BigFix
WebUI User's Guide

Special notice

Before using this information and the product it supports, read the information in Notices (on page cccxxxviii).

Edition notice

This edition applies to MCM version 1.1 of BigFix 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Welcome

Welcome to BigFix WebUI. The WebUI delivers a powerful set of functions for BigFix operators. It simplifies BigFix workflows, speeds access to data, and improves flexibility, visibility, and performance.

Only minimal BigFix experience is needed to learn and use the WebUI. A browser, the WebUI URL, and a BigFix username and password are all that is required. Supported browsers include the latest versions of Edge, Safari, Firefox, and Chrome.

Administrators and operators familiar with the BigFix console will find a useful introduction to the WebUI in this guide. For information about installing and administering the WebUI, see the BigFix WebUI Administration Guide.

To open the WebUI, use the URL provided by your administrator and enter your BigFix username and password. Single Sign On users will bypass the BigFix login screen and authenticate through their service provider. After successful login, users are greeted with the BigFix Overview dashboard.

Note: The look of the BigFix interface is changing. We are in the process of updating the graphics in this guide to reflect the new colors and theme. Thank you for your patience as we complete this work.

Chapter 2. Meet the WebUI

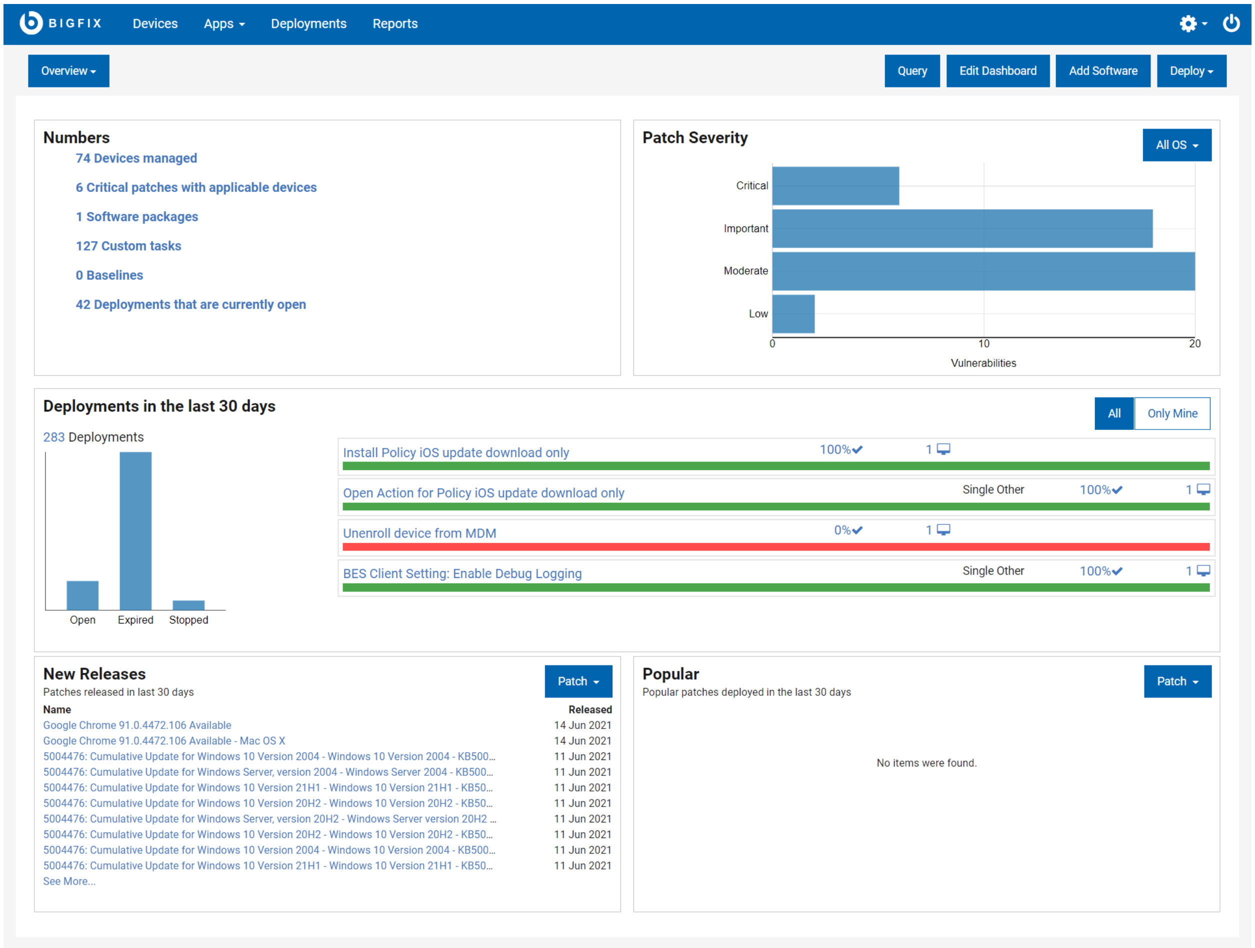
Take a quick tour of the WebUI screens, controls, and workflow.

A detailed description of each of the main WebUI screens, including the Deploy Sequence and its options, begins in Get Started with Devices (on page 23). For an introduction to BigFix terms and concepts, see the Glossary.

Overview Page

The WebUI Overview provides a summary of your environment. Its interactive charts and rich set of links make it easy to move quickly to areas that require immediate attention.

In WebUI, the Overview page is the default landing page. Users can navigate to the overview page from any WebUI screen by clicking the BigFix logo on the navigation bar (on page 12). Links throughout the pages provide shortcuts between views.



Numbers

74 Devices managed

6 Critical patches with applicable devices

1 Software packages

127 Custom tasks

0 Baselines

42 Deployments that are currently open

Deployments in the last 30 days

283 Deployments

Install Policy iOS update download only 100%✓ 1

Open Action for Policy iOS update download only Single Other 100%✓ 1

Unenroll device from MDM 0%✓ 1

BES Client Setting: Enable Debug Logging Single Other 100%✓ 1

New Releases

Patches released in last 30 days

Name	Released
Google Chrome 91.0.4472.106 Available	14 Jun 2021
Google Chrome 91.0.4472.106 Available - Mac OS X	14 Jun 2021
5004476: Cumulative Update for Windows 10 Version 2004 - Windows 10 Version 2004 - KB500...	11 Jun 2021
5004476: Cumulative Update for Windows Server, version 2004 - Windows Server 2004 - KB500...	11 Jun 2021
5004476: Cumulative Update for Windows 10 Version 21H1 - Windows 10 Version 21H1 - KB50...	11 Jun 2021
5004476: Cumulative Update for Windows 10 Version 20H2 - Windows 10 Version 20H2 - KB50...	11 Jun 2021
5004476: Cumulative Update for Windows Server, version 20H2 - Windows Server version 20H2 ...	11 Jun 2021
5004476: Cumulative Update for Windows 10 Version 20H2 - Windows 10 Version 20H2 - KB50...	11 Jun 2021
5004476: Cumulative Update for Windows 10 Version 2004 - Windows 10 Version 2004 - KB500...	11 Jun 2021
5004476: Cumulative Update for Windows 10 Version 21H1 - Windows 10 Version 21H1 - KB50...	11 Jun 2021

See More...

Popular

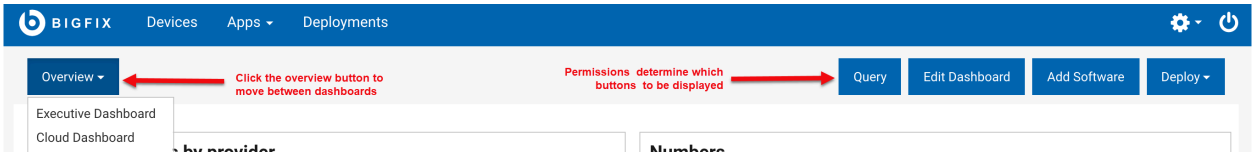
Popular patches deployed in the last 30 days

No items were found.

- Refresh the screen to see the latest data.
- Click the dynamic links to address ongoing changes in your environment
- Click the charts and tallies to drill in for more details

- Mouse over graphic elements to display underlying values
- Filter new releases and popular content by type

Operator permissions and site and role assignments govern which page and data elements are displayed on the WebUI pages. For example, an operator who does not have access to the Software Distribution component cannot see the **Add Software** button on the **Overview**.



Click the overview button to move between dashboards

Permissions determine which buttons to be displayed

Only Master Operators can edit the active dashboard to customize. For more information, see https://help.hcltechsw.com/bigfix/10.0/platform/WebUI/Admin_Guide/c_permission_effects_in_the_webu.html.

- **Overview**: Switch between dashboards by selecting the option under overview dropdown list.
  - Executive Dashboard: The Executive Dashboard provides information of particular interest to IT Officers, Security Officers, and Analysts. To view the Executive Dashboard, click the **Overview** button beneath the navigation bar and select **Executive Dashboard**. Use the **Overview** button to move between dashboards. For more information about the Executive Dashboard and its tiles, see the WebUI Administration Guide.
  - Cloud Dashboard:

    After installing the cloud plugins and discovering the cloud resources, you can see the summary of your cloud devices in WebUI Overview under Cloud Dashboard. To view the Cloud Dashboard, click the **Overview** button beneath the navigation bar and select **Cloud Dashboard**. This dashboard contains tiles for monitoring the amount of cloud resources in your environment, with or without an agent installed, and their distribution by type and region. Click any bar chart to open the Devices page, which lists that subset of resources, where the filters BigFix Agent Status and Managed by are pre-selected.
- **Query:** Click this button to open the Query editor.
- **Edit Dashboard:** Only Master Operators can edit the active dashboard to customize. For more information, see Permissions and Their Effects *(on page 19)*.
- **Add Software:** Click this button to quickly upload software packages.
- **Deploy**: Select an option to under this dropdown to deploy custom content, patch, profile or software.
- **Numbers:** Displays important statistics about your environment. Click on a link to display the filtered list of that specific item.
- **Patch Severity:** Displays the number of patches available for all the operating systems based on the vulnerability, by default. To display data from a specific operating system, select the option from the dropdown. To display the filtered list of patches of a specific type, click on the respective blue bar.
- **Deployments in the last 30 days:** Displays the overview of all the deployments in your environment. Click on the available links to display the details of that item. To display only the overview of your deployments, click **Only Mine**.

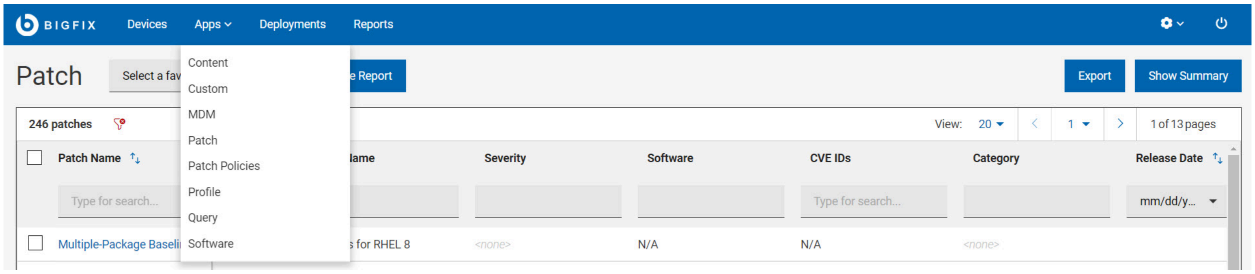
- **New Releases:** Displays the latest 10 new patch releases, by default. You can also display the newly released software or custom content for your environment by selecting the option from the dropdown. Click **See More...** to display the complete list of items.
- **Popular:** Displays popular patches deployed in the last 30 days, by default. You can also display the popular software and custom content deployed in the last 30 days by selecting the option from the dropdown.

WebUI sessions close automatically after a period of inactivity. If your session expires, you will be returned to the page that you were on the next time you log in.

Note: When a tile on a dashboard takes over 10 seconds to load, load time details appear on the tile. Click **Close** to clear the message. Factors that can influence response times include changes to hardware, to the number of endpoints, and the amount of data you have access to.

Navigation Bar

Use the navigation bar to access the Overview, Device, and Deployment pages as well as to access different applications under Apps.

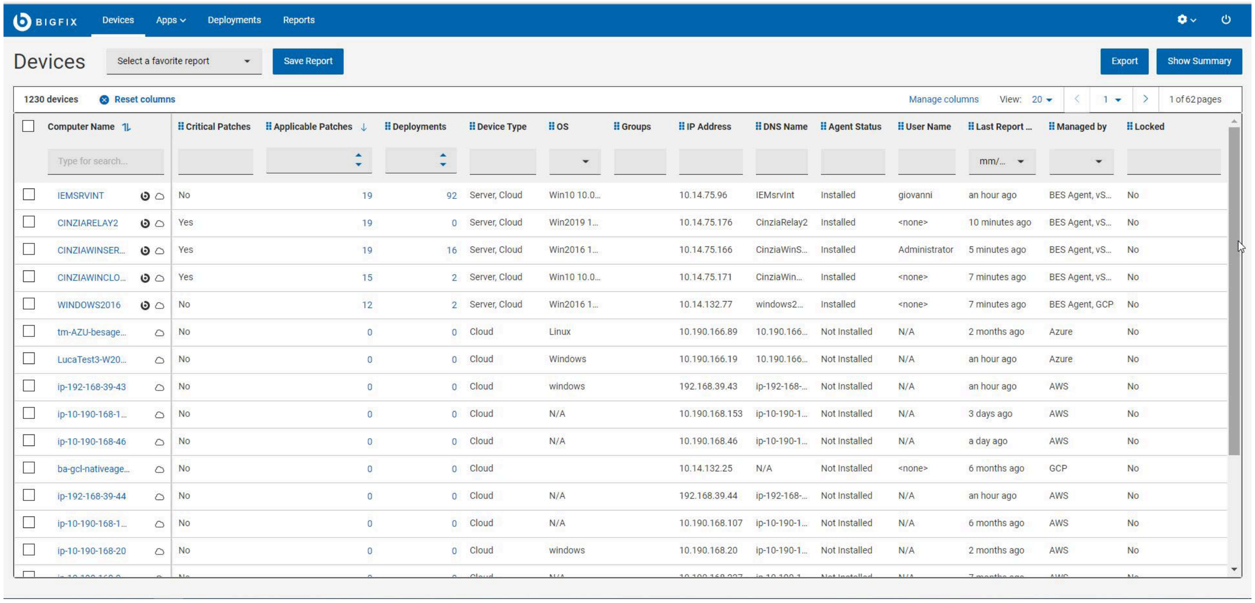


- The BigFix logo and the **Home** icon both open the Overview.
- From the main menu, click **Devices** view a list of reporting BigFix devices and apply actions to them.
- From the main menu, click **Deployments** to view a list of BigFix actions, find more details, or stop open actions.
- From the **Apps** menu, launch the WebUI applications such as Content, Custom, MDM, Patch, Patch Policies, Profile, Query, and Software.
- Click **Reports** to view saved reports and work with reports.
- Click the gear icon to configure WebUI application settings.
- Click the Log out button to log off from WebUI. Hover over the Log out button to see the name of the logged in user.

Grid view

View all the properties in an interactive table where you can customize the columns.

Grid view enables you to quickly view the items in a table. Clicking the link of an item opens the relevant document page. Every column gives an option to search or filter. You can add, remove, and resize columns. You can save the current view as a report (on page 20), export the data, and visualize the data.



□	Computer Name	Critical Patches	Applicable Patches	Deployments	Device Type	OS	Groups	IP Address	DNS Name	Agent Status	User Name	Last Report ...	Managed by	Locked
□	IEMSRVINT	No	19	92	Server, Cloud	Win10 10.0...		10.14.75.96	IEMsrvInt	Installed	giovanni	an hour ago	BES Agent, vS...	No
□	CINZIARELAY2	Yes	19	0	Server, Cloud	Win2019 1...		10.14.75.176	CinziaRelay2	Installed	<none>	10 minutes ago	BES Agent, vS...	No
□	CINZIAWINSER...	Yes	19	16	Server, Cloud	Win2016 1...		10.14.75.166	CinziaWinS...	Installed	Administrator	5 minutes ago	BES Agent, vS...	No
□	CINZIAWINCLO...	Yes	15	2	Server, Cloud	Win10 10.0...		10.14.75.171	CinziaWin...	Installed	<none>	7 minutes ago	BES Agent, vS...	No
□	WINDOWS2016	No	12	2	Server, Cloud	Win2016 1...		10.14.132.77	windows2...	Installed	<none>	7 minutes ago	BES Agent, GCP	No
□	tm-AZU-besage...	No	0	0	Cloud	Linux		10.190.166.89	10.190.166...	Not Installed	N/A	2 months ago	Azure	No
□	LucaTest3-W20...	No	0	0	Cloud	Windows		10.190.166.19	10.190.166...	Not Installed	N/A	an hour ago	Azure	No
□	ip-192-168-39-43	No	0	0	Cloud	windows		192.168.39.43	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
□	ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.153	ip-10-190-1...	Not Installed	N/A	3 days ago	AWS	No
□	ip-10-190-168-46	No	0	0	Cloud	N/A		10.190.168.46	ip-10-190-1...	Not Installed	N/A	a day ago	AWS	No
□	ba-gcl-nativeage...	No	0	0	Cloud			10.14.132.25	N/A	Not Installed	<none>	6 months ago	GCP	No
□	ip-192-168-39-44	No	0	0	Cloud	N/A		192.168.39.44	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
□	ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.107	ip-10-190-1...	Not Installed	N/A	6 months ago	AWS	No
□	ip-10-190-168-20	No	0	0	Cloud	windows		10.190.168.20	ip-10-190-1...	Not Installed	N/A	2 months ago	AWS	No

Note: Operator permission *(on page 19)* settings, connected devices, and site assignments govern the list contents.

Customize devices data grid

You can customize the data grid view by adding, removing, resizing, or changing the positions of the columns. You can also click Reset columns to return back to default view.

- **To resize the column width**
    1. Mouse hover near the desired column border.
    2. Click and hold down the left mouse button, drag the border to the right to widen the column or to the left to make the column narrower, and release the mouse button when the desired width is reached.
- **To change column position**
    1. Mouse hover the desired column name.
    2. Click and hold down the left mouse button, drag and drop it to a desired position in the data grid.

Refine results

- To filter data:
    - From the desired column, select your option from the list.

      or
    - Click in the text field of the desired column and type the search string.

> **Note:** For only a subset of reserved and aggregated computer properties, auto-suggest displays a list of suggested words based on the first few typed letters. For other properties, including user-defined computer properties, auto-suggest does not work, as it impacts the search performance.

- To speed up your search, combine filters.

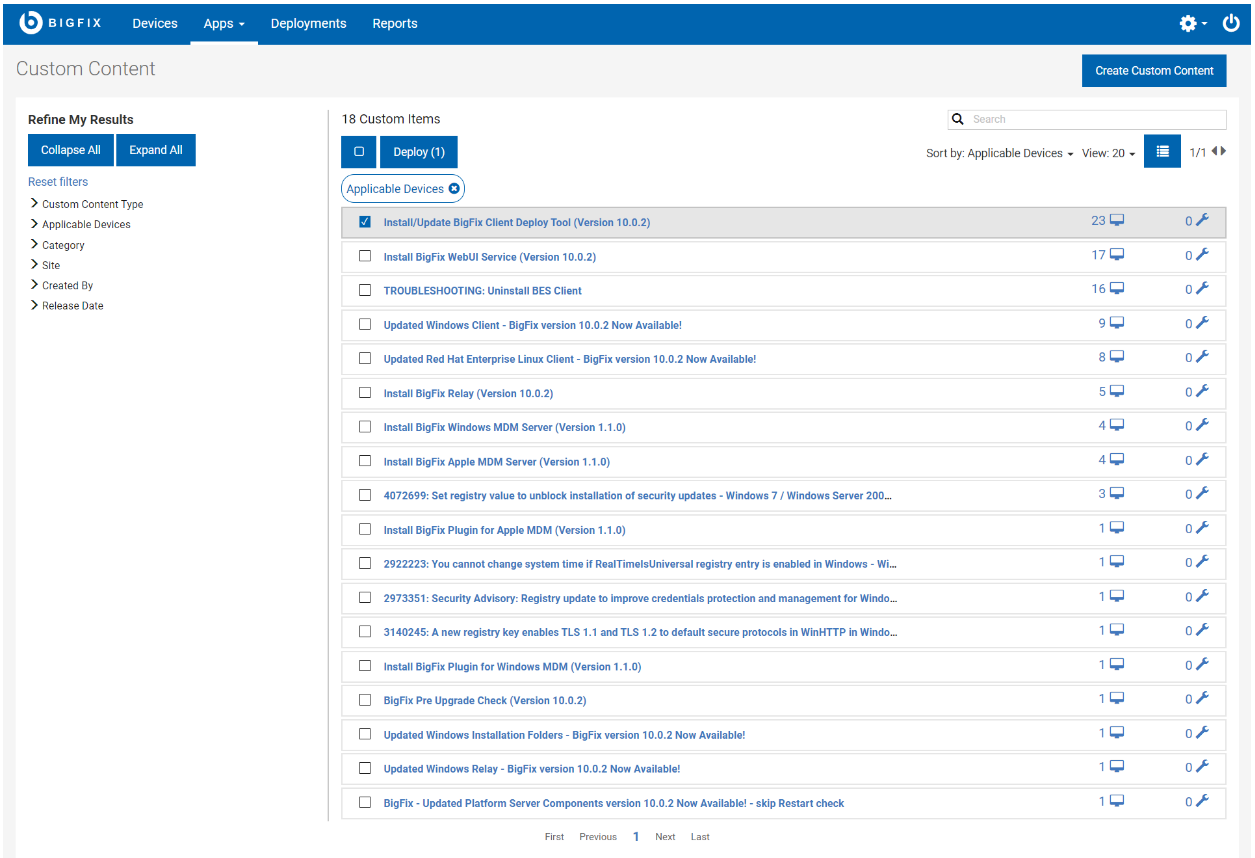
> **Note:** By default, you can combine up to a maximum of five filters to process simultaneously. Exceeding the maximum number of filters affects the performance. The default value can be configured using the setting `_WebUIAppEnv_MAX_FILTERS_NUMBER`.

- To clear all selected filters, click Reset all filters

List view

List views show your BigFix environment in directory form: a flexible, searchable index.

Click the title on a card to open the corresponding document. To take an action, for example, to deploy a custom content on a target device, highlight its card and click the **Deploy** button.



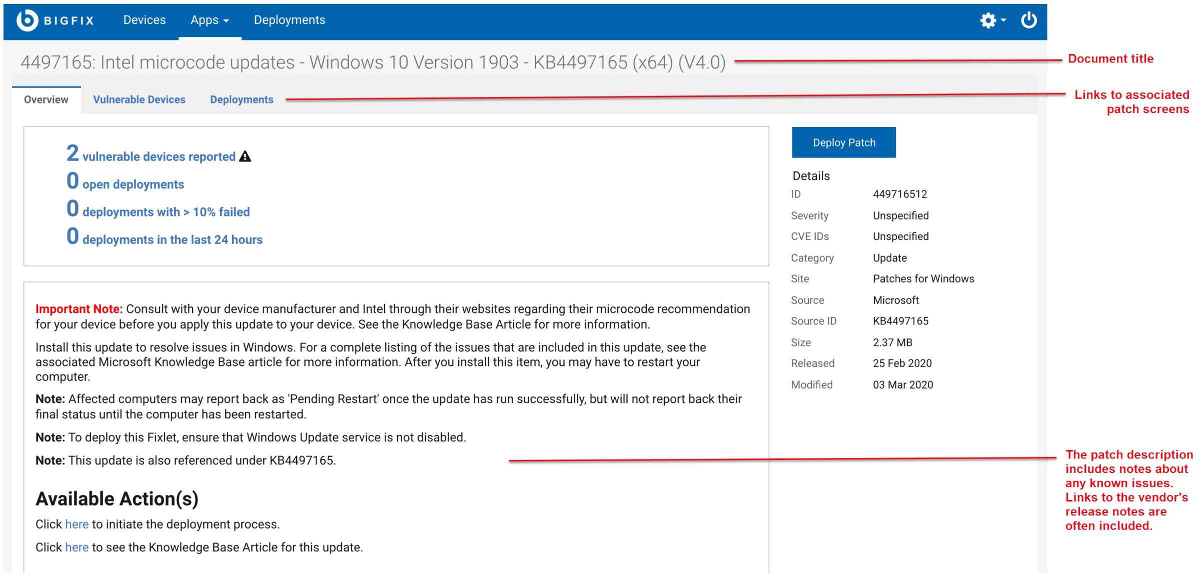
18 Custom Items

☑	Install/Update BigFix Client Deploy Tool (Version 10.0.2)	23	0
□	Install BigFix WebUI Service (Version 10.0.2)	17	0
□	TROUBLESHOOTING: Uninstall BES Client	16	0
□	Updated Windows Client - BigFix version 10.0.2 Now Available!	9	0
□	Updated Red Hat Enterprise Linux Client - BigFix version 10.0.2 Now Available!	8	0
□	Install BigFix Relay (Version 10.0.2)	5	0
□	Install BigFix Windows MDM Server (Version 1.1.0)	4	0
□	Install BigFix Apple MDM Server (Version 1.1.0)	4	0
□	4072699: Set registry value to unblock installation of security updates - Windows 7 / Windows Server 200...	3	0
□	Install BigFix Plugin for Apple MDM (Version 1.1.0)	1	0
□	2922223: You cannot change system time if RealTimeIsUniversal registry entry is enabled in Windows - Wi...	1	0
□	2973351: Security Advisory: Registry update to improve credentials protection and management for Windo...	1	0
□	3140245: A new registry key enables TLS 1.1 and TLS 1.2 to default secure protocols in WinHTTP in Windo...	1	0
□	Install BigFix Plugin for Windows MDM (Version 1.1.0)	1	0
□	BigFix Pre Upgrade Check (Version 10.0.2)	1	0
□	Updated Windows Installation Folders - BigFix version 10.0.2 Now Available!	1	0
□	Updated Windows Relay - BigFix version 10.0.2 Now Available!	1	0
□	BigFix - Updated Platform Server Components version 10.0.2 Now Available! - skip Restart check	1	0

- Click anywhere in a card to select it.
- Click a selected card to clear it.
- Click a card title to display its document.
- To preview a title too long for its card, hover over it with the mouse.

Document view

The WebUI's document views present detailed information about a particular device, deployment, or piece of content. Use document navigation links to drill down into the data on associated views. The diagram shows a patch document.



4497165: Intel microcode updates - Windows 10 Version 1903 - KB4497165 (x64) (V4.0)

2 vulnerable devices reported ⚠
0 open deployments
0 deployments with > 10% failed
0 deployments in the last 24 hours

Important Note: Consult with your device manufacturer and Intel through their websites regarding their microcode recommendation for your device before you apply this update to your device. See the Knowledge Base Article for more information.

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

Note: Affected computers may report back as 'Pending Restart' once the update has run successfully, but will not report back their final status until the computer has been restarted.

Note: To deploy this Fixlet, ensure that Windows Update service is not disabled.

Note: This update is also referenced under KB4497165.

Available Action(s)

Click here to initiate the deployment process.

Click here to see the Knowledge Base Article for this update.

Details

ID	449716512
Severity	Unspecified
CVE IDs	Unspecified
Category	Update
Site	Patches for Windows
Source	Microsoft
Source ID	KB4497165
Size	2.37 MB
Released	25 Feb 2020
Modified	03 Mar 2020

Document title

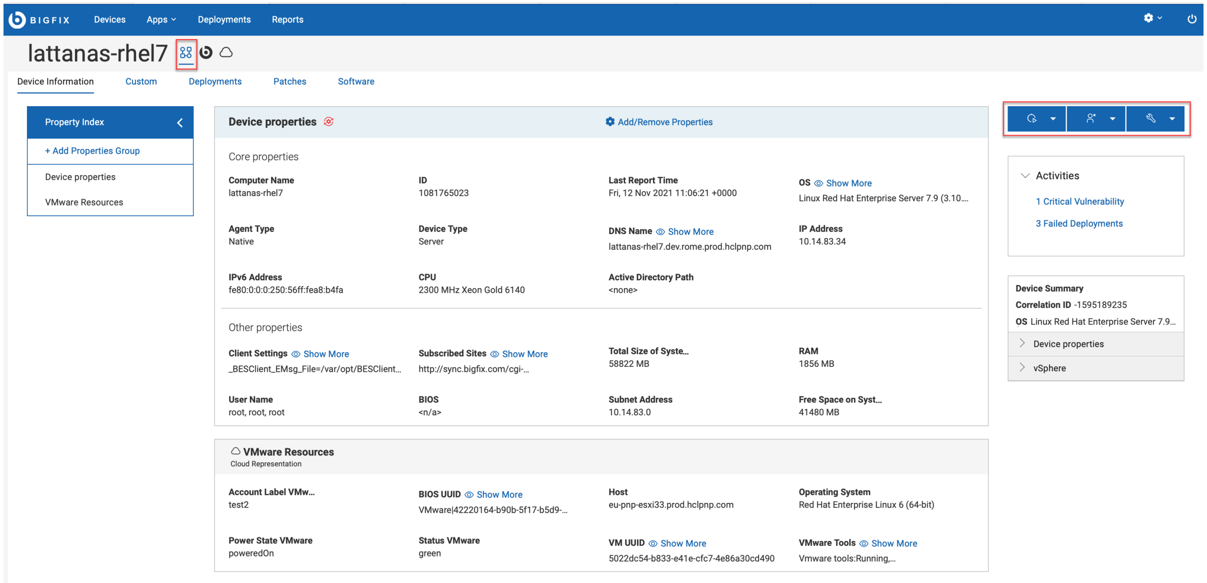
Links to associated patch screens

The patch description includes notes about any known issues. Links to the vendor's release notes are often included.

Key details are summarized in the right side panel; the **Deploy** button appears on all device and content documents.

The following is an image of a device document Device Information view. Use the tabs to display additional views.

- **Deploy**: Click the button to deploy content to the device
- **Configuration**: Click the button to issue a query, send a file, or send a message to this device



Core properties

Computer Name: lattanas-rhel7
ID: 1081765023
Last Report Time: Fri, 12 Nov 2021 11:06:21 +0000
OS: Linux Red Hat Enterprise Server 7.9 (3.10...
Agent Type: Native
Device Type: Server
DNS Name: lattanas-rhel7.dev.rome.prod.hclpnp.com
IP Address: 10.14.83.34
IPv6 Address: fe80:0:0:0:250:56ff:fea8:b4fa
CPU: 2300 MHz Xeon Gold 6140
Active Directory Path: <none>

Other properties

Client Settings: _BESClient_EMsg_File=/var/opt/BESClient...
Subscribed Sites: http://sync.bigfix.com/cgi-...
Total Size of Syste...: 58822 MB
RAM: 1856 MB
User Name: root, root, root
BIOS: <n/a>
Subnet Address: 10.14.83.0
Free Space on Syst...: 41480 MB

VMware Resources
Cloud Representation

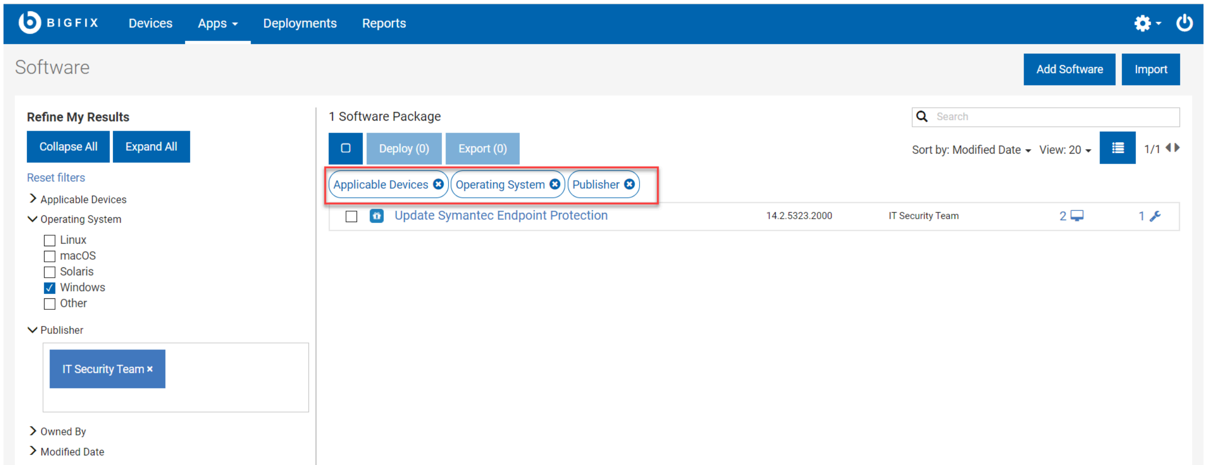
Account Label VMw...: test2
BIOS UUID: VMware|42220164-b90b-5f17-b5d9-...
Host: eu-pnp-esxi33.prod.hclpnp.com
Operating System: Red Hat Enterprise Linux 6 (64-bit)
Power State VMware: poweredOn
Status VMware: green
VM UUID: 5022dc54-b833-e41e-cfc7-4e86a30cd490
VMware Tools: Vmware tools:Running,...

Device Summary
Correlation ID -1595189235
OS Linux Red Hat Enterprise Server 7.9...

Filters and Search Tools

Use the WebUI filters to reduce a long list to a short list of specific items.

For example, filter the Software list by Operating System to see software for OS X computers. Combine filters, for example, to find the software list by Operating System issued by a specific publisher.



Operating System: □ Linux □ macOS □ Solaris ☑ Windows □ Other
Publisher: IT Security Team ×

1 Software Package

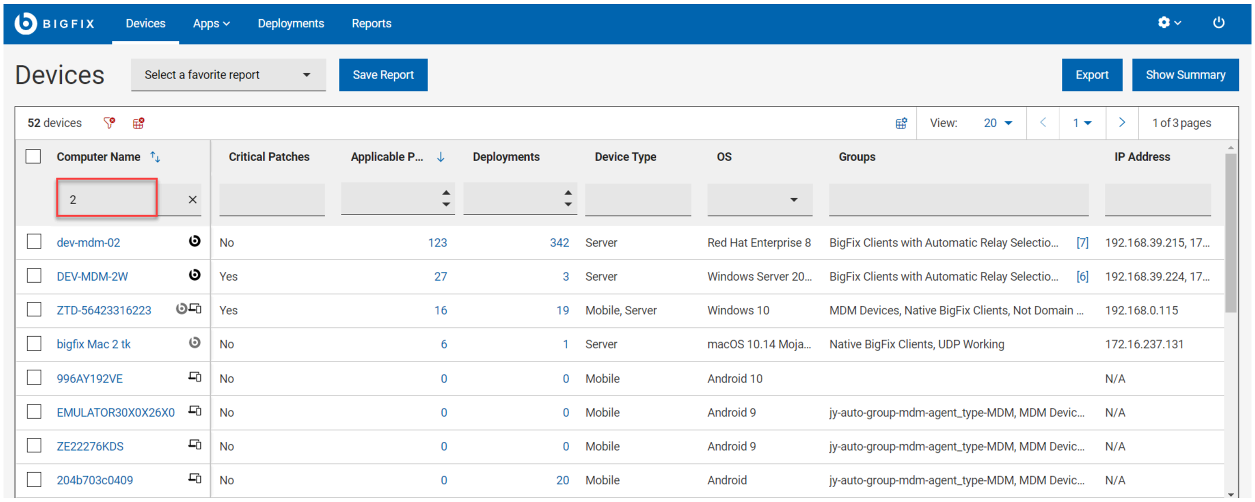
□ Update Symantec Endpoint Protection | 14.2.5323.2000 | IT Security Team | 2 | 1

The list of active filter groups are displayed across the top of the list.

- Click Collapse All to collapse the filters
- Click Expand All to expand the filters and view all the sub filters
- Click Reset Filters to clear all selected filters
- Combine filters to speed up a search
- Click in a text field to select from a list of options or type the first few letters of your search string

Text Search

Use a text search to find items based on words or characters they contain. For example, search the Device list for “2” to find every device with the character “2” in its name.



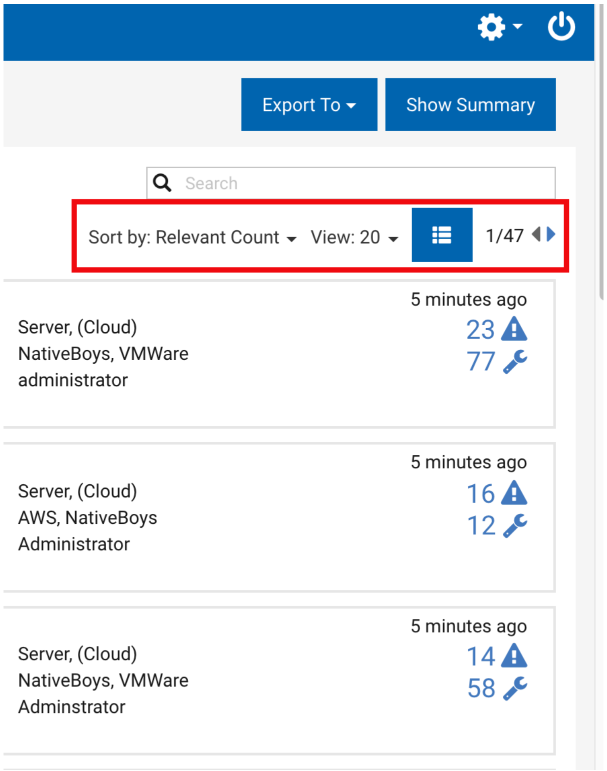
	Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS	Groups		IP Address
	2								
□	dev-mdm-02	No	123	342	Server	Red Hat Enterprise 8	BigFix Clients with Automatic Relay Selectio...	[7]	192.168.39.215, 17...
□	DEV-MDM-2W	Yes	27	3	Server	Windows Server 20...	BigFix Clients with Automatic Relay Selectio...	[6]	192.168.39.224, 17...
□	ZTD-56423316223	Yes	16	19	Mobile, Server	Windows 10	MDM Devices, Native BigFix Clients, Not Domain ...		192.168.0.115
□	bigfix Mac 2 tk	No	6	1	Server	macOS 10.14 Moja...	Native BigFix Clients, UDP Working		172.16.237.131
□	996AY192VE	No	0	0	Mobile	Android 10			N/A
□	EMULATOR30X0X26X0	No	0	0	Mobile	Android 9	jy-auto-group-mdm-agent_type-MDM, MDM Devic...		N/A
□	ZE22276KDS	No	0	0	Mobile	Android 9	jy-auto-group-mdm-agent_type-MDM, MDM Devic...		N/A
□	204b703c0409	No	0	20	Mobile	Android	jy-auto-group-mdm-agent_type-MDM, MDM Devic...		N/A

- Use a multiple word search to find any items that contain those terms. For example, results for a search for *“MS13-035 Vista”* includes the patch *“MS13-035 MSHTML Security Vulnerability Vista”*.
- Searches are not case-sensitive. For example, a patch list search for the word *“advisory”* returns patches with either *“advisory”* or *“Advisory”* in their name.
- Wildcard searches and searches for text within the body of a document are not currently supported.

List Controls

Sort a list, adjust the number and appearance of list items, and move between pages with the list view controls.

- Sort by – Place items you want to see first at the top of the list
- View – Adjust the number of records shown
- Show/Hide Details – Fit more items on a page
- Pagination controls – see the current page number, number of pages, and move between pages



Server, (Cloud)
NativeBoys, VMWare
administrator
5 minutes ago
23
77

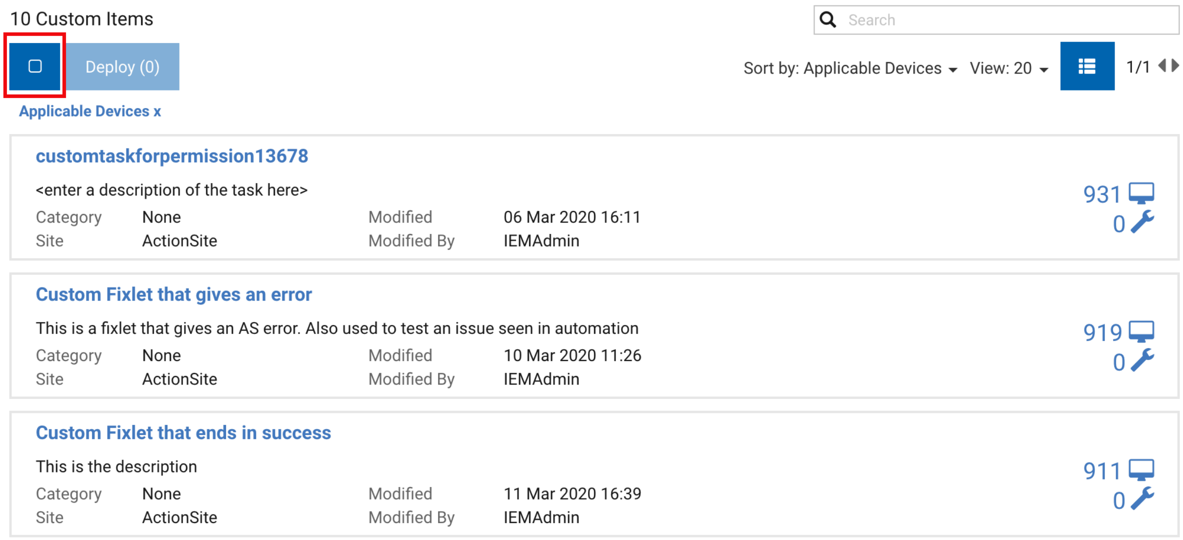
Server, (Cloud)
AWS, NativeBoys
Administrator
5 minutes ago
16
12

Server, (Cloud)
NativeBoys, VMWare
Adminstrator
5 minutes ago
14
58

Select All

The Select All check box selects or clears every item on a page.

- Select or clear all items on a single page
- Select or clear every item on a page
- Deploy button shows your cross-page total
- Selections remain in effect when move between pages



customtaskforpermission13678

<enter a description of the task here>

Category	None	Modified	06 Mar 2020 16:11	931
Site	ActionSite	Modified By	IEMAdmin	0

Custom Fixlet that gives an error

This is a fixlet that gives an AS error. Also used to test an issue seen in automation

Category	None	Modified	10 Mar 2020 11:26	919
Site	ActionSite	Modified By	IEMAdmin	0

Custom Fixlet that ends in success

This is the description

Category	None	Modified	11 Mar 2020 16:39	911
Site	ActionSite	Modified By	IEMAdmin	0

Permissions and Their Effects

The elements that are shown on a WebUI screen reflect the permission levels of the user, and the device, site, and group assignments set for them by the BigFix administrator.

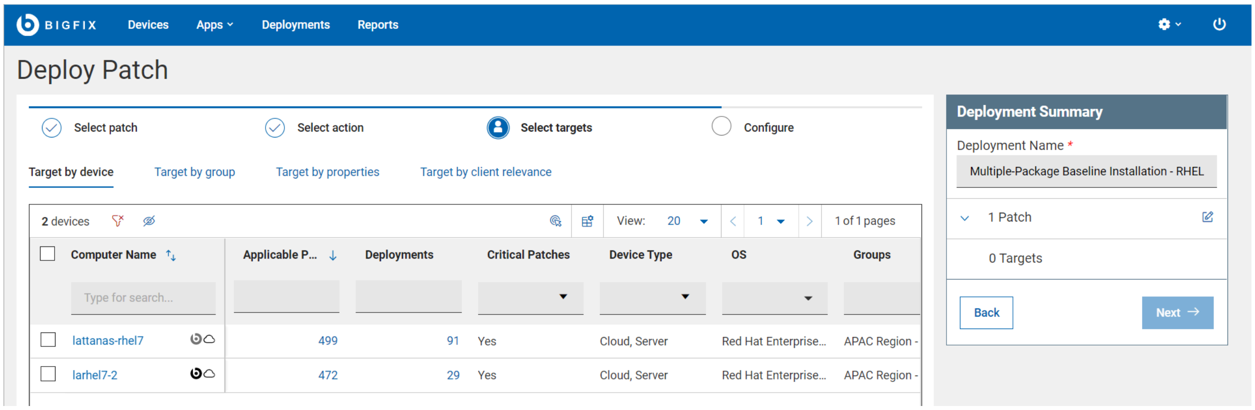
For example, an operator responsible for patching Windows machines might not see Linux patches in their patch list or Linux machines in their device list. An operator who deploys software but does no patching might not see the Patch content or Custom content options in the Content submenu. For more information about permissions and their influence on WebUI screens and data elements, see the BigFix WebUI Administrators Guide.

WebUI Work flow and Deploy Sequence

To deploy means to dispatch content such as applications, modules, updates, and patches to one or more endpoints. For example, by deploying a software package, you install selected software on targeted endpoints. BigFix WebUI enables you to configure the content and the target devices to create a deployment, save the deployment configurations to reuse it as necessary, and monitor the deployment status. The workflow including all the steps, processes, and activities that are required to create a deployment is collectively called as the Deploy Sequence.

You can start a deployment from devices grid or any content screen, or from the Overview page. Deploy Sequence changes as per the entry point.

For further details, see Take Action: The Deploy Sequence (on page 129).



Deploy Patch

2 devices View: 20 1 1 of 1 pages

Computer Name	Applicable P...	Deployments	Critical Patches	Device Type	OS	Groups
lattanas-rhel7	499	91	Yes	Cloud, Server	Red Hat Enterprise...	APAC Region -
larhel7-2	472	29	Yes	Cloud, Server	Red Hat Enterprise...	APAC Region -

Deployment Summary

Deployment Name *: Multiple-Package Baseline Installation - RHEL

1 Patch

0 Targets

- Track your progress through the different tabs of the Deploy sequence
- Use the search, sort, and filtering tools to locate devices and content.
- In the Deployment Summary section, review your selected content and devices and make changes if needed by clicking the Edit button.

Reports

With WebUI Reports, you can create custom reports to obtain more specific information about devices, patches, and deployments of the endpoints.

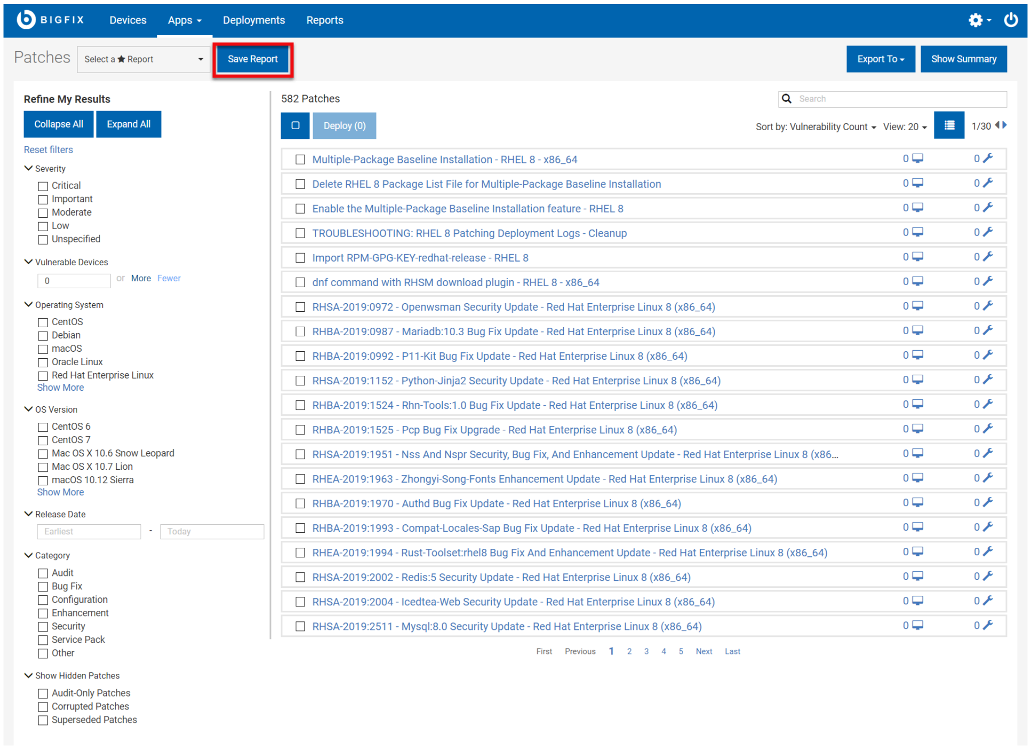
Important:

- Master Operators and Non-Master Operators can create and save reports.
- Master Operators can view/edit/delete all reports, including the private reports created by other users.
- Non-Master Operators can:
  - view all the public reports and their own private reports
  - edit/delete their own reports

Creating a report

To create a new report

1. Open **Devices**, **Deployments** or **Patches** page.
2. Select the desired filters; a list of relevant items matching your filter criteria is displayed.



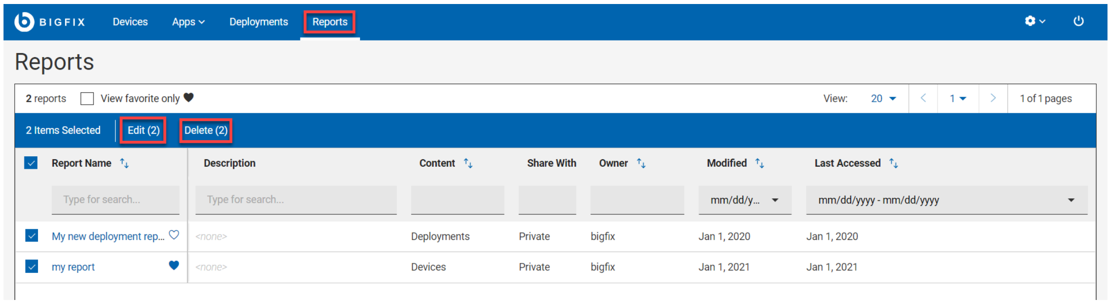
582 Patches

□	Multiple-Package Baseline Installation - RHEL 8 - x86_64	0	0
□	Delete RHEL 8 Package List File for Multiple-Package Baseline Installation	0	0
□	Enable the Multiple-Package Baseline Installation feature - RHEL 8	0	0
□	TROUBLESHOOTING: RHEL 8 Patching Deployment Logs - Cleanup	0	0
□	Import RPM-GPG-KEY-redhat-release - RHEL 8	0	0
□	dnf command with RHSM download plugin - RHEL 8 - x86_64	0	0
□	RHSA-2019:0972 - Openwsman Security Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:0987 - Mariadb:10.3 Bug Fix Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:0992 - P11-Kit Bug Fix Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHSA-2019:1152 - Python-Jinja2 Security Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:1524 - Rhn-Tools:1.0 Bug Fix Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:1525 - Pcp Bug Fix Upgrade - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHSA-2019:1951 - Nss And Nspr Security, Bug Fix, And Enhancement Update - Red Hat Enterprise Linux 8 (x86...	0	0
□	RHEA-2019:1963 - Zhongyi-Song-Fonts Enhancement Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:1970 - Authd Bug Fix Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHBA-2019:1993 - Compat-Locales-Sap Bug Fix Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHEA-2019:1994 - Rust-Toolset:rhel8 Bug Fix And Enhancement Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHSA-2019:2002 - Redis:5 Security Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHSA-2019:2004 - Icedtea-Web Security Update - Red Hat Enterprise Linux 8 (x86_64)	0	0
□	RHSA-2019:2511 - Mysql:8.0 Security Update - Red Hat Enterprise Linux 8 (x86_64)	0	0

3. Click **Save Report**.
4. In the Save Report window:
    a. Enter the **Report Name**.
    b. Enter **Report Description** of the report (optional).
    c. Set the visibility of the report as **Private** or **All Users** to restrict who can view your reports.
    d. A link for the report is auto-generated. Click **Copy Link** to copy the link and directly access the report through a browser.
5. Click **Save**.

Working with saved reports

.



☑	Report Name	Description	Content	Share With	Owner	Modified	Last Accessed
☑	My new deployment rep... ♡	<none>	Deployments	Private	bigfix	Jan 1, 2020	Jan 1, 2020
☑	my report ♥	<none>	Devices	Private	bigfix	Jan 1, 2021	Jan 1, 2021

- View: You can view the list of saved public and private reports depending on the user role. To view, from the WebUI main page, click **Reports**.
- Favorites: Mark a report as your favorite report and quickly access it from the Devices, Deployments or Patch page as applicable. To do that, click ♡ next to the desired report.
- View favorite only: Select this check box to view only the reports that are marked as favorite.
- Sort: You can sort the reports by Name, Content, Owner, Modified, or Last Accessed.
- Filter: You can filter reports by every column. Enter a string or select an option from a column, the respective reports are filtered and displayed.
- Edit: You can edit report name, description, and/or visibility. To edit, select the desired report and click **Edit** . To edit the visibility of multiple reports, select the desired reports and click the **Edit** button.
- Delete: To delete one or more reports, select the desired reports that you want to delete and click **Delete**.
- Undo delete: You can retrieve the last deleted report by clicking ↺ that appears immediately after deleting the report.

  Note: This option appears only for a short time, and you can retrieve only during this time.

- Update:
  1. Click on a report to view it.
  2. Modify the filters, sort by, or view properties; the Update button appears.
  3. Click **Update**. The report is updated and saved.
- Save New:
  1. Click on a report to view it.
  2. Modify the filters, sort by, or view properties; the Save New button appears.
  3. Click **Save New**. The Save Report window appears.
  4. Enter **Report Name**, **Report Description**; select the visibility as **Private** or **All Users** and click **Save**. The modified report is saved as a new report.

Chapter 3. Get Started with Devices

Use the Device screens to view and manage all the devices in your environment as determined by your permission levels. You can find specific devices, access device documents, select devices for deployment, generate and export device reports and do much more.

Cloud devices

BigFix 10 brings you the capability to manage your physical and virtual endpoints on cloud (public, private, and hybrid) securely and cost-effectively. If you have the cloud plugins enabled, you can view cloud resources with or without the native BigFix agent installed.

Modern Client Management (MCM) devices

BigFix 10 enables you to control modern clients in your environment with enhanced security through MCM policies and actions. If you have the MCM plugin enabled, you can enroll the devices for MCM and manage through BigFix WebUI. For more information, refer to Modern Client Management and BigFix Mobile *(on page 173)*.

To avoid duplication and to streamline management of devices, when BigFix discovers a device, it determines if it is unique and adds an icon representing the type of the device (native, cloud, or MCM). If a device has more than one representation or icon, it is called a correlated device. For more information, seeCorrelated devices device.

Related information

The Device List *(on page 23)*

Device Document *(on page 31)*

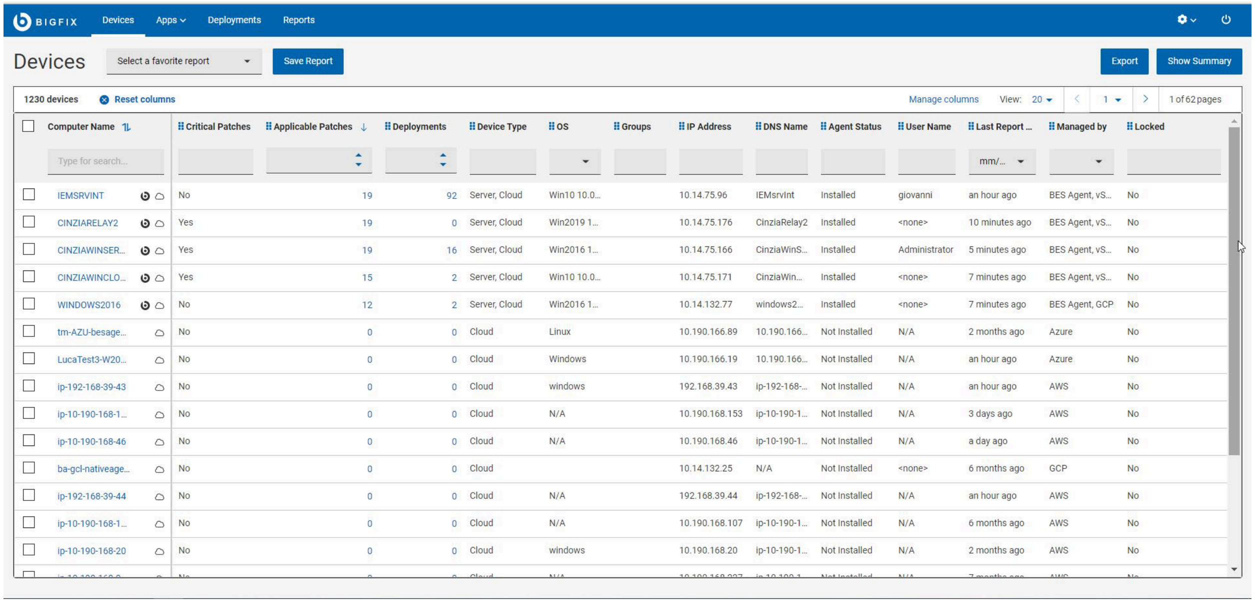
The Device List

View a list of BigFix managed devices, create customized device reports, and review the detailed information about each device to effectively perform actions on and proactively monitor the health of the endpoints.

To access the **Devices** page, from the WebUI main page, click **Devices**.

Important: Operator permission settings, connected devices, and site assignments govern the list contents.

The following image shows the devices data grid with default property columns and their positions (Computer Name, Critical Patches, Applicable Patches, Deployments, Device Type, OS, Groups, IP Address, DNS Name, Agent Status, User Name, Last Report Time, Managed by, Locked). By default, the data is sorted based on the number of Application Patches in descending order.



Computer Name	Critical Patches	Applicable Patches	Deployments	Device Type	OS	Groups	IP Address	DNS Name	Agent Status	User Name	Last Report ...	Managed by	Locked
IEMSRVINT	No	19	92	Server, Cloud	Win10 10.0...		10.14.75.96	IEMsrvInt	Installed	giovanni	an hour ago	BES Agent, vS...	No
CINZIARELAY2	Yes	19	0	Server, Cloud	Win2019 1...		10.14.75.176	CinziaRelay2	Installed	<none>	10 minutes ago	BES Agent, vS...	No
CINZIAWINSER...	Yes	19	16	Server, Cloud	Win2016 1...		10.14.75.166	CinziaWinS...	Installed	Administrator	5 minutes ago	BES Agent, vS...	No
CINZIAWINCLO...	Yes	15	2	Server, Cloud	Win10 10.0...		10.14.75.171	CinziaWin...	Installed	<none>	7 minutes ago	BES Agent, vS...	No
WINDOWS2016	No	12	2	Server, Cloud	Win2016 1...		10.14.132.77	windows2...	Installed	<none>	7 minutes ago	BES Agent, GCP	No
tm-AZU-besage...	No	0	0	Cloud	Linux		10.190.166.89	10.190.166...	Not Installed	N/A	2 months ago	Azure	No
LucaTest3-W20...	No	0	0	Cloud	Windows		10.190.166.19	10.190.166...	Not Installed	N/A	an hour ago	Azure	No
ip-192-168-39-43	No	0	0	Cloud	windows		192.168.39.43	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.153	ip-10-190-1...	Not Installed	N/A	3 days ago	AWS	No
ip-10-190-168-46	No	0	0	Cloud	N/A		10.190.168.46	ip-10-190-1...	Not Installed	N/A	a day ago	AWS	No
ba-gcl-nativeage...	No	0	0	Cloud			10.14.132.25	N/A	Not Installed	<none>	6 months ago	GCP	No
ip-192-168-39-44	No	0	0	Cloud	N/A		192.168.39.44	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.107	ip-10-190-1...	Not Installed	N/A	6 months ago	AWS	No
ip-10-190-168-20	No	0	0	Cloud	windows		10.190.168.20	ip-10-190-1...	Not Installed	N/A	2 months ago	AWS	No

Manage devices

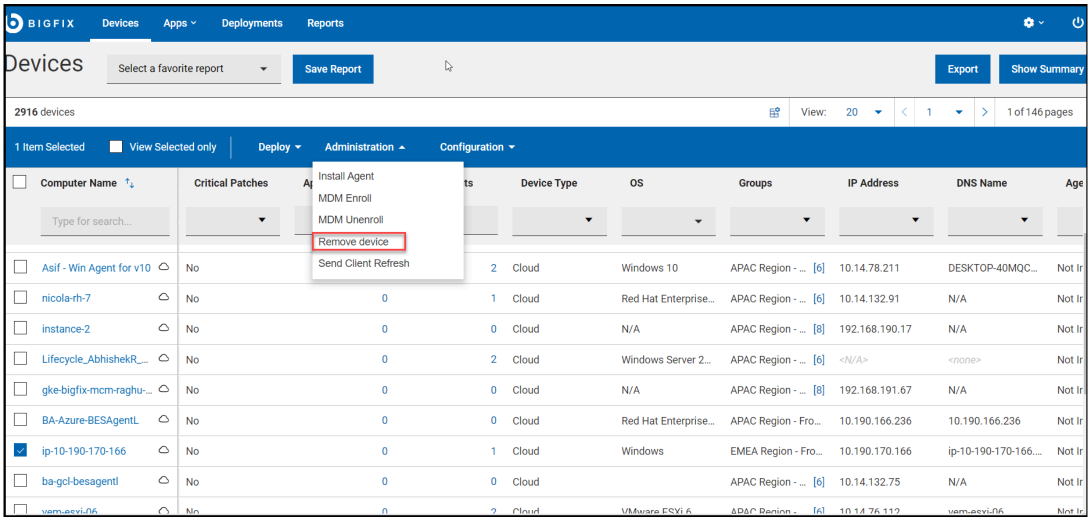
To manage devices, select one or more devices from the list. A blue bar appears with available actions, organized by type. The list of actions may vary according to the installed components in your systems. For example, if you do not have MDM installed, the actions related to MDM do not appear in the Deploy drop down.

- Deploy *(on page 129)*: From this menu, you can deploy content of various types such as custom content, patches, software, MDM policies and actions.

  Note: The option to deploy profiles is getting deprecated.

- Administration: From this menu, you can choose among typical administrative tasks related to the devices, such us enrolling to and unenrolling from MDM server, installing BigFix agent or sending the action for client refresh, and remove device.

  Note: Operators can use the "Remove device" option to delete the selected computers. "Remove device" option from the UI performs a soft delete. When the "Client Removal Tool" runs, it will permanently delete the computer from the database. During that time, if the deleted device reports again then the related entry will be restored in the "Device view".



Devices

Select a favorite report | Save Report | Export | Show Summary

2916 devices | View: 20 | 1 | 1 of 146 pages

1 Item Selected | □ View Selected only | Deploy | Administration | Configuration

Install Agent
MDM Enroll
MDM Unenroll
Remove device
Send Client Refresh

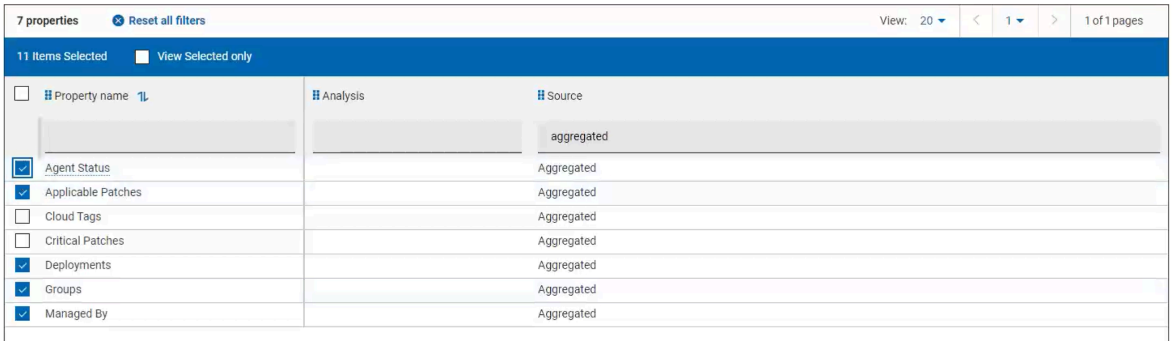
□	Computer Name	Critical Patches	Ap	ts	Device Type	OS	Groups	IP Address	DNS Name	Age
	Type for search...									
□	Asif - Win Agent for v10	No		2	Cloud	Windows 10	APAC Region - ... [6]	10.14.78.211	DESKTOP-40MQC...	Not Ir
□	nicola-rh-7	No	0	1	Cloud	Red Hat Enterprise...	APAC Region - ... [6]	10.14.132.91	N/A	Not Ir
□	instance-2	No	0	0	Cloud	N/A	APAC Region - ... [8]	192.168.190.17	N/A	Not Ir
□	Lifecycle_AbhishekR_...	No	0	2	Cloud	Windows Server 2...	APAC Region - ... [6]	<N/A>	<none>	Not Ir
□	gke-bigfix-mcm-raghu-...	No	0	0	Cloud	N/A	APAC Region - ... [8]	192.168.191.67	N/A	Not Ir
□	BA-Azure-BESAgentL	No	0	0	Cloud	Red Hat Enterprise...	APAC Region - Fro...	10.190.166.236	10.190.166.236	Not Ir
☑	ip-10-190-170-166	No	0	1	Cloud	Windows	EMEA Region - Fro...	10.190.170.166	ip-10-190-170-166....	Not Ir
□	ba-gcl-besagentl	No	0	0	Cloud		APAC Region - ... [6]	10.14.132.75	N/A	Not Ir
□	vem-esxi-06	No	0	2	Cloud	VMware ESXi 6	APAC Region - ... [6]	10.14.76.112	vem-esxi-06	Not Ir

- Configuration: From this menu, you can send a message (if the target machine has SSA installed) or send a file or access Query application.

Computer Properties

These include the standard properties for out-of-the-box BigFix clients and the properties created by BigFix Console users. The computer properties are categorized as follows:

- Reserved: A set of properties that in BigFix Platform are flagged as Reserved and Pre-defined properties. For example, BIOS date, the CPU type, free hard disk drive space, the operating system, memory, and user name.
- Aggregated: A set of properties that WebUI calculates, such as: Applicable Patches, Deployments, Critical Patches, Groups, Agent Status, Cloud Tags and Managed By.



7 properties | Reset all filters | View: 20 | 1 | 1 of 1 pages

11 Items Selected | □ View Selected only

□	Property name	Analysis	Source
			aggregated
☑	Agent Status		Aggregated
☑	Applicable Patches		Aggregated
□	Cloud Tags		Aggregated
□	Critical Patches		Aggregated
☑	Deployments		Aggregated
☑	Groups		Aggregated
☑	Managed By		Aggregated

- All computer properties other than Reserved and Aggregated properties retrieved by BigFix agent.

Note: To improve performance, property values are truncated to the first 5000 characters.

Refine results

- To filter device data:
    - From the desired column, select your option from the list.

      or
    - Click in the text field of the desired column and type the search string.

      Note: For only a subset of reserved and aggregated computer properties, auto-suggest displays a list of suggested words based on the first few typed letters. For other properties, including user-defined computer properties, auto-suggest does not work, as it impacts the search performance.
- To speed up your search, combine filters.

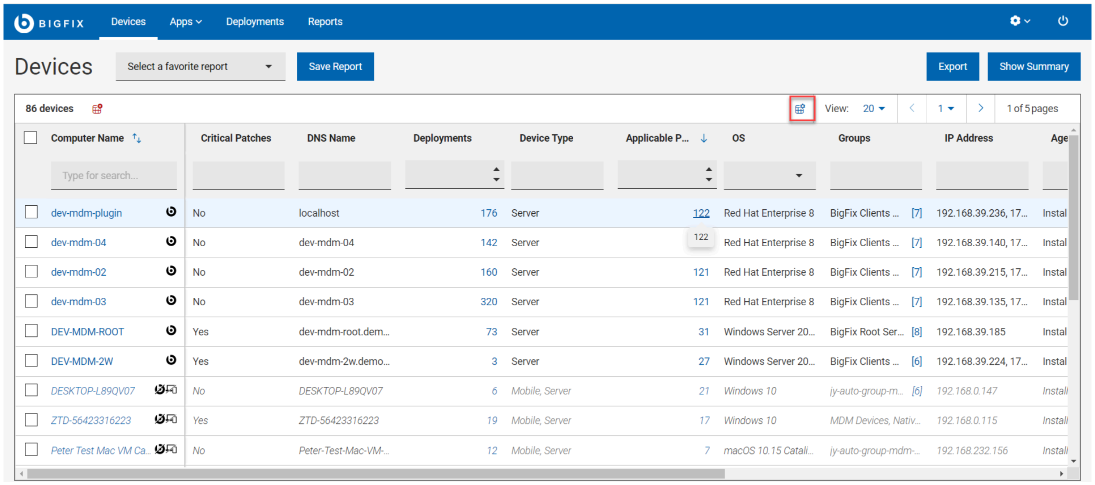
  Note: By default, you can combine up to a maximum of five filters to process simultaneously. Exceeding the maximum number of filters affects the performance. The default value can be configured using the setting `_WebUIAppEnv_MAX_FILTERS_NUMBER`.
- To clear all selected filters, click Reset all filters

Customize devices data grid

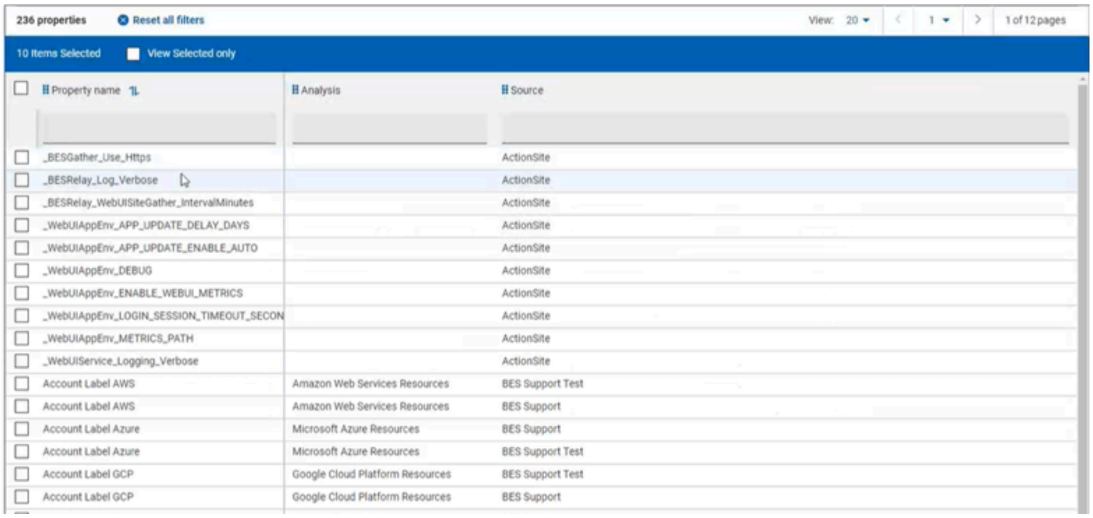
You can customize the data grid view by adding, removing, resizing, or changing the positions of the columns. You can also click Reset columns to return back to default view.

- **To include additional property column to the devices data grid**

1. Click **Manage columns**. The Other Property page appears.

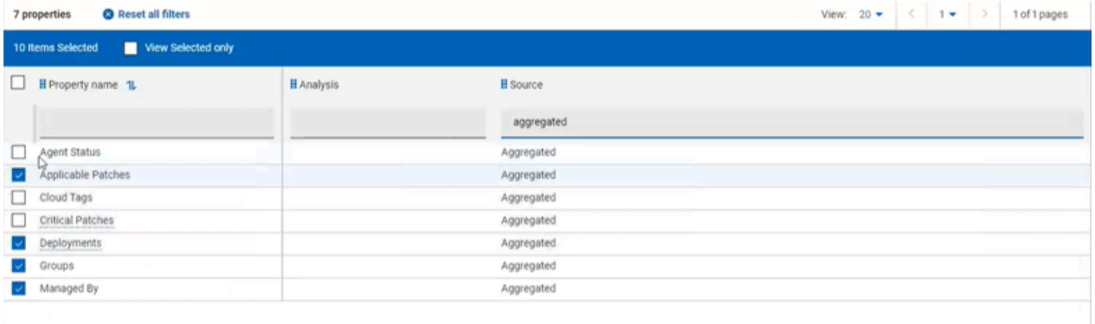


□	Computer Name	Critical Patches	DNS Name	Deployments	Device Type	Applicable P...	OS	Groups		IP Address	Age
□	dev-mdm-plugin	No	localhost	176	Server	122	Red Hat Enterprise 8	BigFix Clients ...	[7]	192.168.39.236, 17...	Instal
□	dev-mdm-04	No	dev-mdm-04	142	Server	122	Red Hat Enterprise 8	BigFix Clients ...	[7]	192.168.39.140, 17...	Instal
□	dev-mdm-02	No	dev-mdm-02	160	Server	121	Red Hat Enterprise 8	BigFix Clients ...	[7]	192.168.39.215, 17...	Instal
□	dev-mdm-03	No	dev-mdm-03	320	Server	121	Red Hat Enterprise 8	BigFix Clients ...	[7]	192.168.39.135, 17...	Instal
□	DEV-MDM-ROOT	Yes	dev-mdm-root.dem...	73	Server	31	Windows Server 20...	BigFix Root Ser...	[8]	192.168.39.185	Instal
□	DEV-MDM-2W	Yes	dev-mdm-2w.demo...	3	Server	27	Windows Server 20...	BigFix Clients ...	[6]	192.168.39.224, 17...	Instal
□	DESKTOP-L89QV07	No	DESKTOP-L89QV07	6	Mobile, Server	21	Windows 10	jy-auto-group-m...	[6]	192.168.0.147	Install
□	ZTD-56423316223	Yes	ZTD-56423316223	19	Mobile, Server	17	Windows 10	MDM Devices, Nativ...		192.168.0.115	Install
□	Peter Test Mac VM Ca...	No	Peter-Test-Mac-VM-...	12	Mobile, Server	7	macOS 10.15 Catali...	jy-auto-group-mdm-...		192.168.232.156	Install



□	Property name	Analysis	Source
□	_BESGather_Use_Https		ActionSite
□	_BESRelay_Log_Verbose		ActionSite
□	_BESRelay_WebUISiteGather_IntervalMinutes		ActionSite
□	_WebUIAppEnv_APP_UPDATE_DELAY_DAYS		ActionSite
□	_WebUIAppEnv_APP_UPDATE_ENABLE_AUTO		ActionSite
□	_WebUIAppEnv_DEBUG		ActionSite
□	_WebUIAppEnv_ENABLE_WEBUI_METRICS		ActionSite
□	_WebUIAppEnv_LOGIN_SESSION_TIMEOUT_SECON		ActionSite
□	_WebUIAppEnv_METRICS_PATH		ActionSite
□	_WebUIService_Logging_Verbose		ActionSite
□	Account Label AWS	Amazon Web Services Resources	BES Support Test
□	Account Label AWS	Amazon Web Services Resources	BES Support
□	Account Label Azure	Microsoft Azure Resources	BES Support
□	Account Label Azure	Microsoft Azure Resources	BES Support Test
□	Account Label GCP	Google Cloud Platform Resources	BES Support Test
□	Account Label GCP	Google Cloud Platform Resources	BES Support

2. Click in the text field of the desired column and type the search string. The search result appears based on the entered string. For example, under Source column, if you enter *Aggregated* the result appears similar to the following image.



□	Property name	Analysis	Source
			aggregated
□	Agent Status		Aggregated
☑	Applicable Patches		Aggregated
□	Cloud Tags		Aggregated
□	Critical Patches		Aggregated
☑	Deployments		Aggregated
☑	Groups		Aggregated
☑	Managed By		Aggregated

3. Select the check box next to the desired **Property name** and click **Save**. The Devices page displays the selected property in a new column.

- **To remove a property column from the devices data grid**
    1. Click **Manage column**.
    2. In the Other Property page, enable **View Selected only** option. The result displays only the properties that are selected for the data grid view.
    3. Deselect one or more properties that you want to remove from the data grid and click **Save**. The Devices page displays the selected properties; the deselected property columns disappear.
- **To resize the column width**
    1. Mouse hover near the desired column border.
    2. Click and hold down the left mouse button, drag the border to the right to widen the column or to the left to make the column narrower, and release the mouse button when the desired width is reached.
- **To change column position**
    1. Mouse hover the desired column name.
    2. Click and hold down the left mouse button, drag and drop it to a desired position in the data grid.

Working with reports

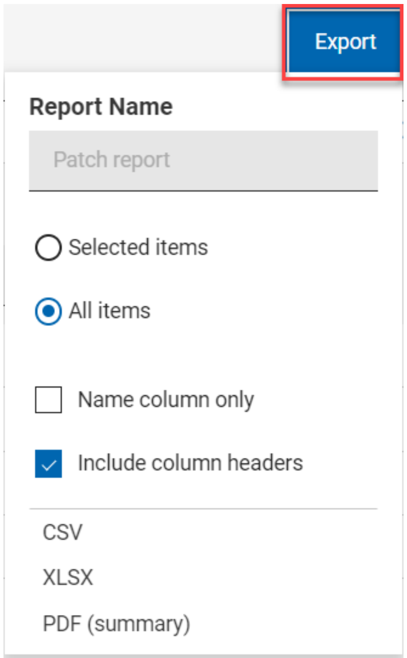
Save reports

You can save the filtered and customized device report for future reference. You can also edit, update, or delete the reports as required. Mark a report as favorite report to access it quickly. For more information about working with reports, see Reports (on page 20).

Export

You can export the filtered report in a `.csv`, `.xlsx`, or `.pdf` format.

1. In the **Devices** page, select the required filters.
2. Click **Export**.



Report Name

Patch report

○ Selected items

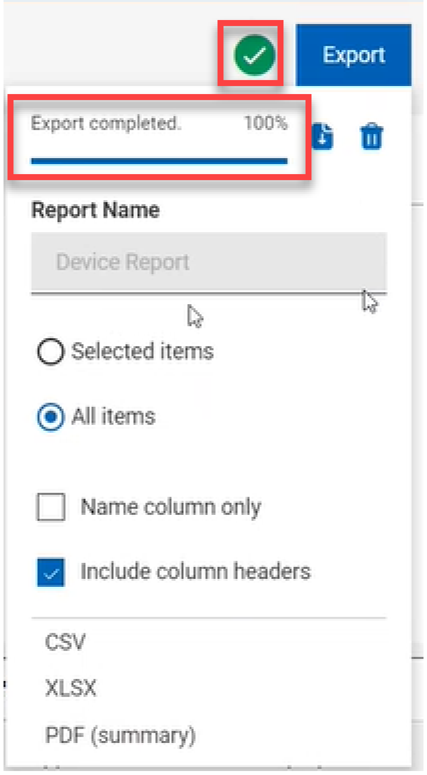
● All items

□ Name column only

☑ Include column headers

3. The option **Selected Items** enables you to select items from the filtered result to export; **All Items** enables you to export all the items from the filtered list. Select the desired option.
4. Name column only: Select this option if you want to export only the names of the filtered items.
5. Include column headers: Select this option if you want to export details of every columns of an item.
6. Select a file format (CSV, XLSX, or PDF) that you want to export to.
   - The export starts and you can see the status in the progress bar.
   - Once export is completed, a green tick mark appears to indicate the report is available to download.
   - Exported report does not get download automatically. You need to click the Download button next to the progress bar to download.
   - If you want to delete the exported report, click Delete button.

- During the export, you can navigate to other pages without interrupting its progress.



Export completed. 100%

Report Name

Device Report

○ Selected items

● All items

□ Name column only

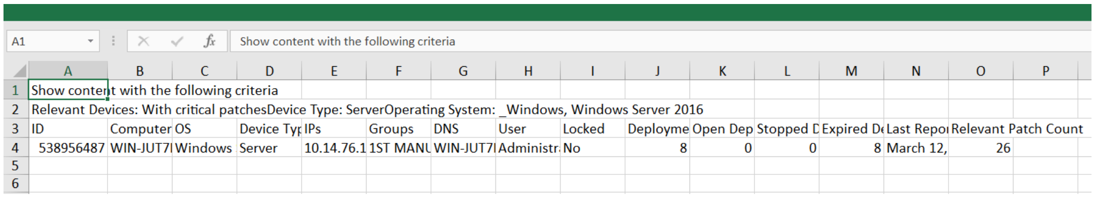
☑ Include column headers

CSV

XLSX

PDF (summary)

- When you download, by default, the report gets downloaded into your Downloads folder with the default file name (Device_Report_mm_dd_yyyy_username). You can change the download settings in your browser to change the file name and download it into a preferred location. You can save the report to review it later and/or share it with interested stakeholders.
- If you have selected PDF format, a `.zip` file gets downloaded which contains a `.csv` file with numerical data and `.pdf` file with visual representation of the data.
- The exported device report contains key details about your managed devices that you have selected through the filters and search criteria. The details include the operating system, device type, IP address along with all the other details that you can see on the screen when you expand every device. A sample report is shown below:



A1 | Show content with the following criteria

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Show content with the following criteria															
2	Relevant Devices: With critical patchesDevice Type: ServerOperating System: _Windows, Windows Server 2016															
3	ID	Computer	OS	Device Typ	IPs	Groups	DNS	User	Locked	Deployme	Open Dep	Stopped D	Expired De	Last Repo	Relevant Patch Count	
4	538956487	WIN-JUT7I	Windows	Server	10.14.76.1	1ST MANU	WIN-JUT7I	Administr	No	8	0	0	8	March 12,	26	
5																
6																

Show summary

1. In the **Devices** page, select the required filters.
2. Click **Show Summary**. You can view the summary of all the filtered devices as charts and tables. Mouse hover the interested areas on the chart to get more details about the respective data point and the percentage data. Mouse hover on any truncated labels to see the full text in the tool tip. Clicking on a clickable area dynamically filters the relevant data, displays in the device list, and displays the summary of the item you clicked on. You can change filters or enter search text and the report dynamically displays the relevant information.
    - **Device Type By Report Time**: Displays the total number of unique devices reported over a period of time against every device type.
    - **By OS Family**: Displays total number of devices from each operating system. The table is sorted alphabetically by OS names.
    - **By Largest Group**: Displays up to the 10 largest computer groups along with the device counts that are relevant as per filter and search criteria.

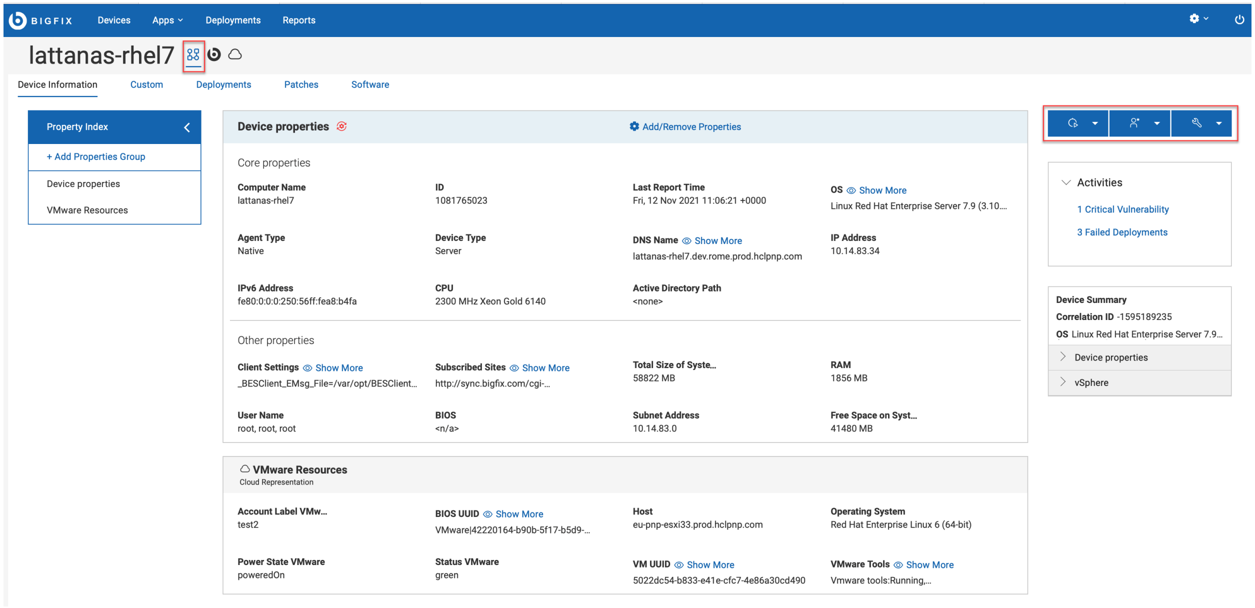
Device Document

Click a device name to get the information related to that device including its properties, status, relevant content, deployment status, history, and much more. Drill further into device details by using the associated views.

As a BigFix Operator, you can view the Device document. Device document provides information gathered from various sources.

Note: To improve performance, property values are truncated to the first 5000 characters.

The following image shows the device document page of a correlated *(on page 23)* device.



lattanas-rhel7

Device properties

Core properties

Computer Name: lattanas-rhel7
ID: 1081765023
Last Report Time: Fri, 12 Nov 2021 11:06:21 +0000
OS: Linux Red Hat Enterprise Server 7.9 (3.10....
Agent Type: Native
Device Type: Server
DNS Name: lattanas-rhel7.dev.rome.prod.hclpnp.com
IP Address: 10.14.83.34
IPv6 Address: fe80:0:0:0:250:56ff:fea8:b4fa
CPU: 2300 MHz Xeon Gold 6140
Active Directory Path: <none>

Other properties

Client Settings: _BESClient_EMsg_File=/var/opt/BESClient...
Subscribed Sites: http://sync.bigfix.com/cgi-...
Total Size of Syste...: 58822 MB
RAM: 1856 MB
User Name: root, root, root
BIOS: <n/a>
Subnet Address: 10.14.83.0
Free Space on Syst...: 41480 MB

VMware Resources
Cloud Representation

Account Label VMw...: test2
BIOS UUID: VMware|42220164-b90b-5f17-b5d9-...
Host: eu-pnp-esxi33.prod.hclpnp.com
Operating System: Red Hat Enterprise Linux 6 (64-bit)
Power State VMware: poweredOn
Status VMware: green
VM UUID: 5022dc54-b833-e41e-cfc7-4e86a30cd490
VMware Tools: Vmware tools:Running,...

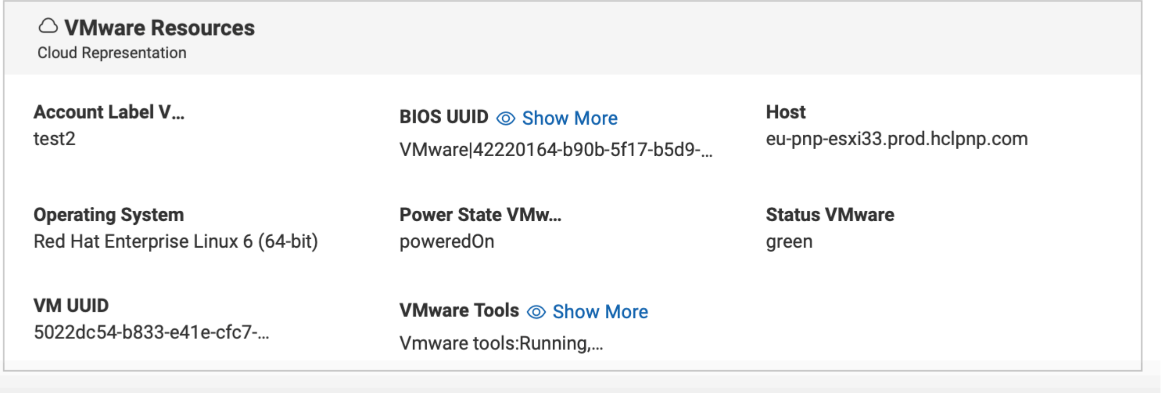
Activities
1 Critical Vulnerability
3 Failed Deployments

Device Summary
Correlation ID -1595189235
OS Linux Red Hat Enterprise Server 7.9...
Device properties
vSphere

Icons and representations

The icons next to the device name indicates the various representation that the device is associated with. To navigate to view the specific properties of a specific representation, click the appropriate icon next to the device name.

- Correlated devices: The icon ⧉ represents that the device is correlated. For correlated devices, you can:
    - view general properties of the device
    - drill down into details of various representations such as BigFix, Cloud, MDM.
- MDM and Cloud devices: For these devices, additional sections are automatically displayed with the default set of properties associated with the representations. You cannot remove these default sections, as they include relevant devices information.



VMware Resources
Cloud Representation

Account Label V...
test2

BIOS UUID Show More
VMware|42220164-b90b-5f17-b5d9-...

Host
eu-pnp-esxi33.prod.hclpnp.com

Operating System
Red Hat Enterprise Linux 6 (64-bit)

Power State VMw...
poweredOn

Status VMware
green

VM UUID
5022dc54-b833-e41e-cfc7-...

VMware Tools Show More
Vmware tools:Running,...

Document views

The tabs in the device document page displays different views as follows:

- **Device Information** – Displays general information of the device.
- **Custom** – Displays custom content relevant to this device.
- **Deployments** – Deployment history for this device.
- **Patches** – Patches relevant to this device.

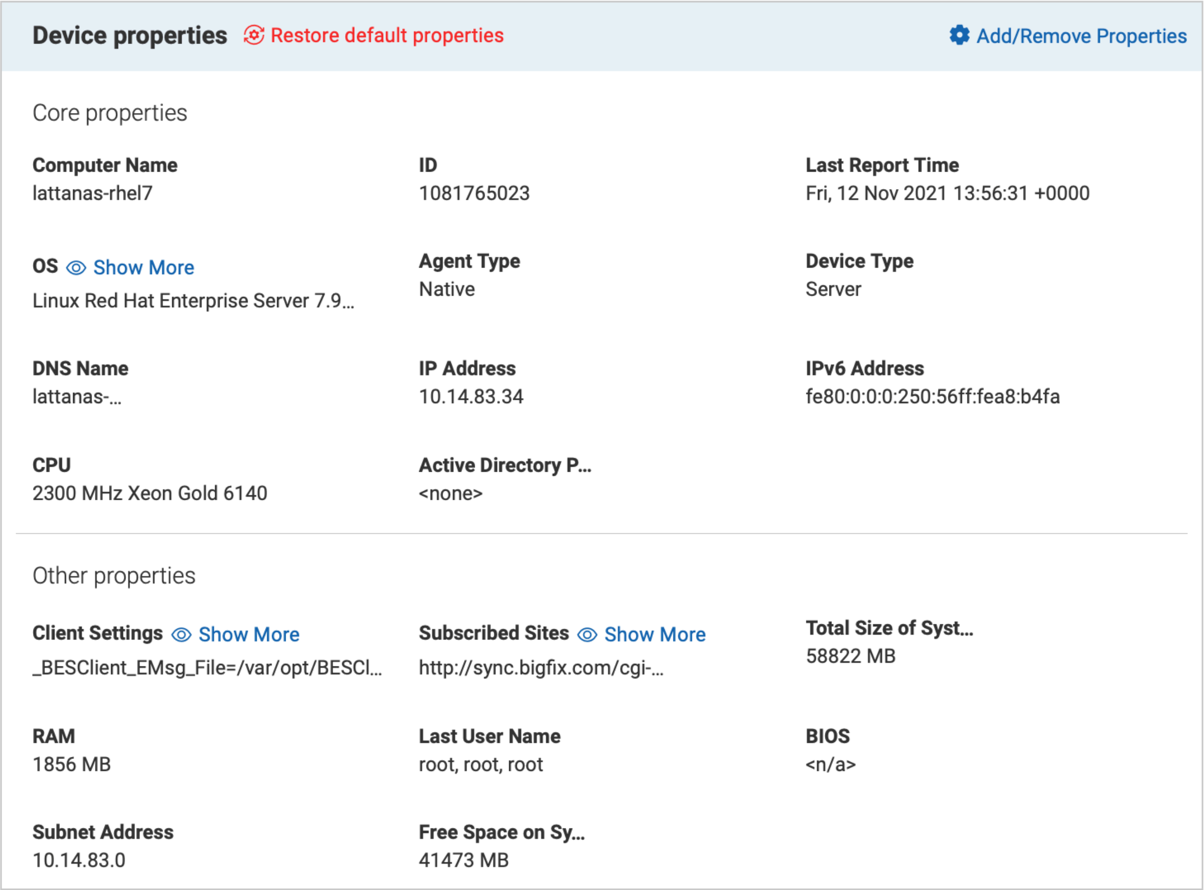
    Note: The tab shows only patches coming from the sites managed in the Patch List *(on page 42)*; other patches can be reached from the Content menu.

- **Software** – Software relevant to this device.

Important: An operator's permission settings govern the views that are displayed. For example, an operator without access to custom content cannot see the **Custom** view.

Customize the layout of the device document page

The default view displays property groups under Property Index and the set of properties in the Device properties box.



Device properties Restore default properties Add/Remove Properties

Core properties

Computer Name
lattanas-rhel7

ID
1081765023

Last Report Time
Fri, 12 Nov 2021 13:56:31 +0000

OS Show More
Linux Red Hat Enterprise Server 7.9...

Agent Type
Native

Device Type
Server

DNS Name
lattanas-...

IP Address
10.14.83.34

IPv6 Address
fe80:0:0:0:250:56ff:fea8:b4fa

CPU
2300 MHz Xeon Gold 6140

Active Directory P...
<none>

Other properties

Client Settings Show More
_BESClient_EMsg_File=/var/opt/BESCl...

Subscribed Sites Show More
http://sync.bigfix.com/cgi-...

Total Size of Syst...
58822 MB

RAM
1856 MB

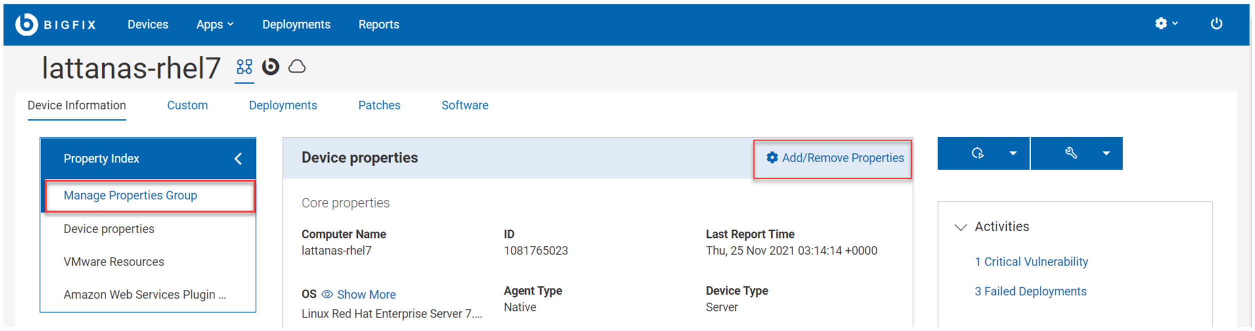
Last User Name
root, root, root

BIOS
<n/a>

Subnet Address
10.14.83.0

Free Space on Sy...
41473 MB

In the correlated view of the device document, you can customize the display of Property Index and Device properties through **Manage property group** or **Add/Remove properties**.



lattanas-rhel7

Device Information Custom Deployments Patches Software

Property Index
Manage Properties Group
Device properties
VMware Resources
Amazon Web Services Plugin ...

Device properties Add/Remove Properties

Core properties

Computer Name
lattanas-rhel7

ID
1081765023

Last Report Time
Thu, 25 Nov 2021 03:14:14 +0000

OS Show More
Linux Red Hat Enterprise Server 7....

Agent Type
Native

Device Type
Server

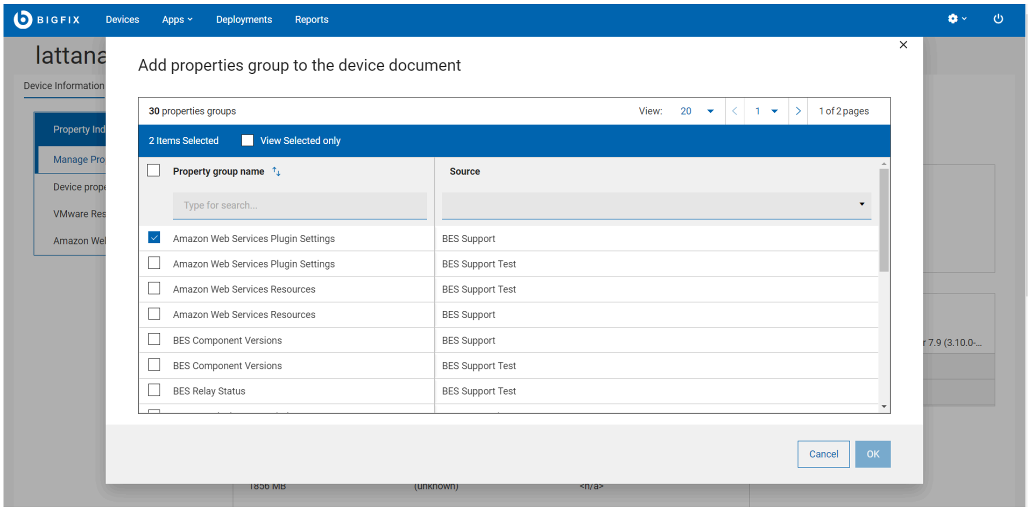
Activities
1 Critical Vulnerability
3 Failed Deployments

The changes are applied throughout all the devices, regardless of their type of associations.

Manage properties group

Click this link to modify the default properties groups displayed under Property Index. You can add as many property groups as you wish. The added property groups are appended to the **Property Index** box. You can expand or collapse Property Index to view the side navigation. If you click on a property group, it automatically scrolls to bring up that property group in focus.

- Add a property group: To add a property group, click the **Manage property group** link, select the checkbox next to a property group, and click OK.



Add properties group to the device document

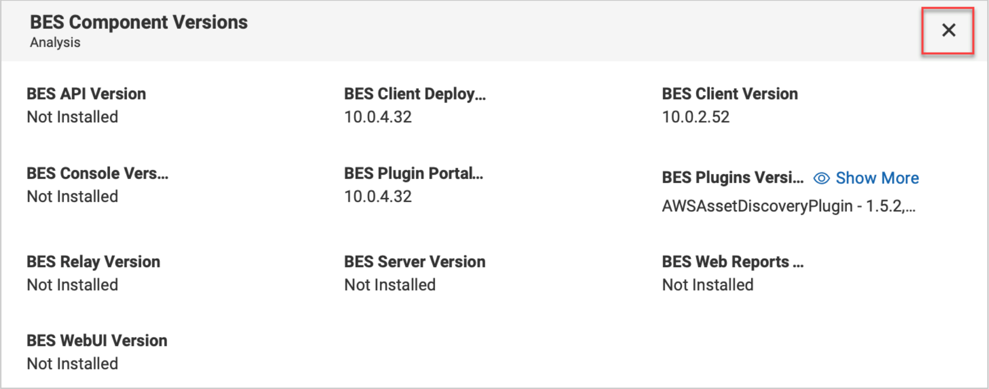
30 properties groups — View: 20 — 1 — 1 of 2 pages

2 Items Selected □ View Selected only

□ Property group name	Source
☑ Amazon Web Services Plugin Settings	BES Support
□ Amazon Web Services Plugin Settings	BES Support Test
□ Amazon Web Services Resources	BES Support Test
□ Amazon Web Services Resources	BES Support
□ BES Component Versions	BES Support
□ BES Component Versions	BES Support Test
□ BES Relay Status	BES Support Test

Cancel OK

- Remove a property group: To remove a property group, click on the X at the top right of that box and click OK for confirmation.

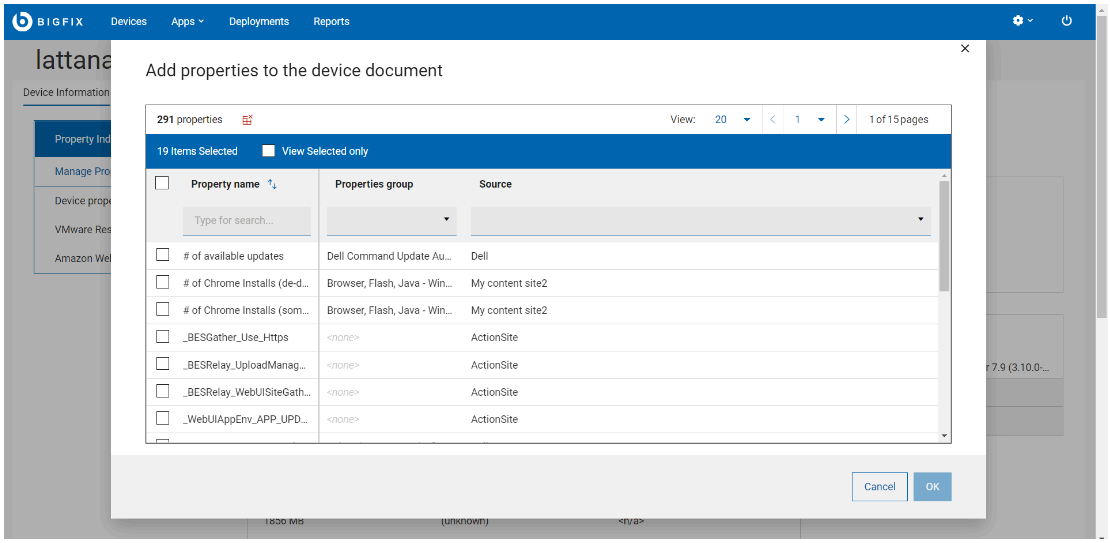


BES Component Versions
Analysis

BES API Version Not Installed	**BES Client Deploy...** 10.0.4.32	**BES Client Version** 10.0.2.52
BES Console Vers... Not Installed	**BES Plugin Portal...** 10.0.4.32	**BES Plugins Versi...** Show More AWSAssetDiscoveryPlugin - 1.5.2,...
BES Relay Version Not Installed	**BES Server Version** Not Installed	**BES Web Reports ...** Not Installed
BES WebUI Version Not Installed		

Add/Remove Properties

Click this link to display the list of available properties and select or deselect the ones that you want to add or remove in the device properties view. From here, you can also add or remove custom properties. If you want to go back to default display, click **Restore default properties**. Upon confirmation, the default view is reset.



Add properties to the device document

291 properties View: 20 1 1 of 15 pages

19 Items Selected □ View Selected only

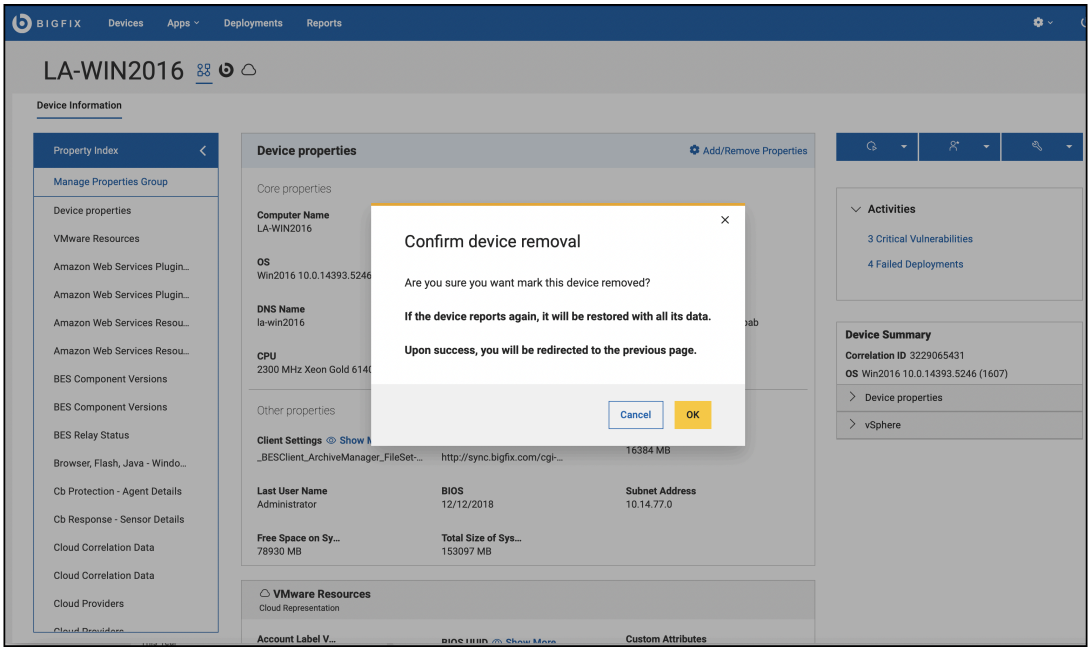
□	Property name	Properties group	Source
	Type for search...		
□	# of available updates	Dell Command Update Au...	Dell
□	# of Chrome Installs (de-d...	Browser, Flash, Java - Win...	My content site2
□	# of Chrome Installs (som...	Browser, Flash, Java - Win...	My content site2
□	_BESGather_Use_Https	<none>	ActionSite
□	_BESRelay_UploadManag...	<none>	ActionSite
□	_BESRelay_WebUISiteGath...	<none>	ActionSite
□	_WebUIAppEnv_APP_UPD...	<none>	ActionSite

Trigger actions

From the device document page, you can trigger actions that are relevant to the device. When you click the action buttons, they display the options based on the type of the device and the permissions of the user. For example, for a cloud device that is not subscribed to MDM, you cannot see “Deploy MDM Action” in the dropdown.

- Deploy: Click the button to deploy custom content, patch, profile, software, or MDM action.
- Administration: Click the button to send refresh, remove device, or install the agent. If you click the "Remove device" option, you can permanently delete the selected computers by clicking "OK".

> **Note:** "Remove device" option from the UI performs a soft delete. When the "Client Removal Tool" runs, it will permanently delete the computer from the database. During that time, if the deleted device reports again then the related entry will be restored in the "Device view".



Confirm device removal

Are you sure you want mark this device removed?

If the device reports again, it will be restored with all its data.

Upon success, you will be redirected to the previous page.

Computer Name: LA-WIN2016

OS: Win2016 10.0.14393.5246

DNS Name: la-win2016

CPU: 2300 MHz Xeon Gold 6140

Client Settings: _BESClient_ArchiveManager_FileSet-...

http://sync.bigfix.com/cgi-...

16384 MB

Last User Name: Administrator

BIOS: 12/12/2018

Subnet Address: 10.14.77.0

Free Space on Sy...: 78930 MB

Total Size of Sys...: 153097 MB

Device Summary

Correlation ID 3229065431

OS Win2016 10.0.14393.5246 (1607)

Account Label V...

BIOS UUID

Custom Attributes

- Configuration: Click the button to issue a query, send a file, or send a message to this device.

Important: When you trigger an action from the correlated view of the device document page, it is targeted to the correlated devices, and it will be up to the correlation engine to dispatch the action to the appropriate representation.

Activities

The Activities section of the device document page provides the links for critical vulnerabilities and failed deployments applicable for the device. Clicking on the links takes you to the pre-filtered list of relevant patches or deployments.

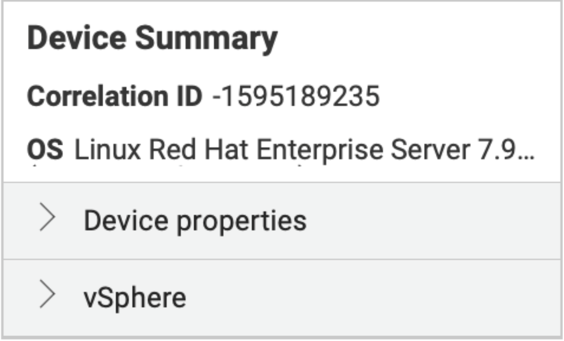
- **Critical Vulnerabilities** – Brings you to the Patches tab pre-filtered by critical and applicable to this device.
- **Failed Deployments –** Brings you to the Deployments tab pre-filtered by deployment status.

Device Summary

The Device Summary section of the device documents provides a recap of the most relevant properties related to the device.

Correlated devices

If the device is correlated it displays the following information



Device Summary

Correlation ID -1595189235

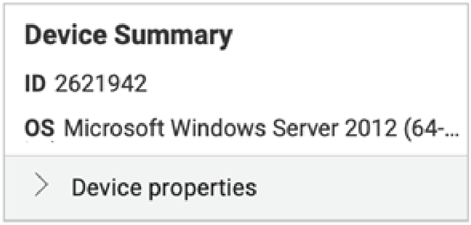
OS Linux Red Hat Enterprise Server 7.9...

- Correlation ID
- OS
- Device Properties section which you can expand or collapse that provides the following details:
  - A fixed set of properties that are useful to be kept in the summary
- Cloud or MDM section (named after the specific source, AWS, MDM etc.)
  - The same fixed list of properties as the master representation, filled in with values reported by the specific representation

For example, Lock property displays the value Yes for the master representation and No for the secondary representation.

Non-correlated devices

If the device is not correlated, the Device Summary section displays the device ID, OS, and Device Properties.



Device Summary

ID 2621942

OS Microsoft Windows Server 2012 (64-...

Send a File

You can upload, list, delete your files and send a file to multiple devices from your file system.

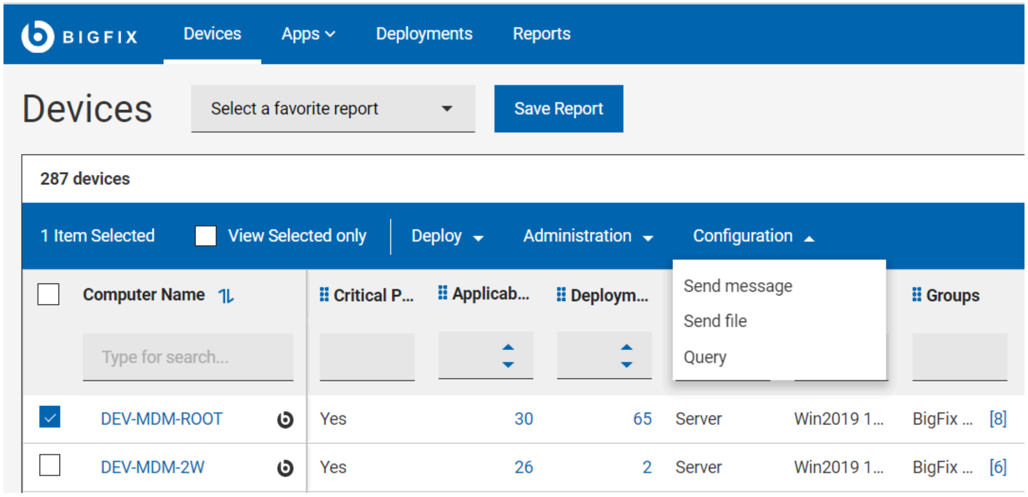
- The operator must have the following permissions:
  - Can Create Actions
  - Custom Content
- SWD must be running and the operator must have access to it.

This section explains you on how to upload a file, send a file to target devices, and delete a file from the list.

Upload files

To upload a new file into the server:

1. From the **Devices** page, select one or more devices. Click **Configuration** and select **Send file**.



Devices

287 devices

	Computer Name	Critical P...	Applicab...	Deploym...			Groups	
☑	DEV-MDM-ROOT	Yes	30	65	Server	Win2019 1...	BigFix ...	[8]
□	DEV-MDM-2W	Yes	26	2	Server	Win2019 1...	BigFix ...	[6]

The **Files** page is displayed that lists all the files that are already uploaded by the user.

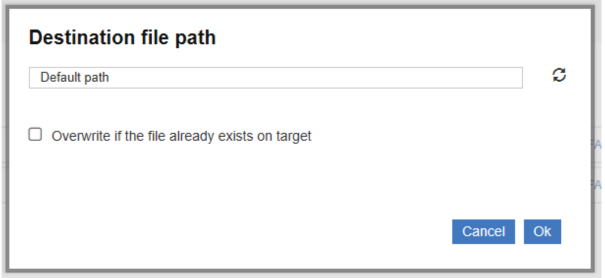
2. Click **Upload**, navigate to and select the file you want to upload, and click **Open**.
   - The file upload starts and you can see the status of the upload in the progress bar.
   - If you want to cancel the upload, click the red x icon next to the progress bar.

Once the file is uploaded, the file list is updated and the uploaded file becomes available to be sent on target devices.

Note: If you are using Microsoft Edge browser to upload a file, ensure you are using the MS Edge version 18.18218 or later. With earlier versions of Microsoft Edge, the progress bar does not show the file upload status; however, the file list gets updated with the uploaded file.

When the file is uploaded, it is saved in the default path. To change the default path:

a. Click the link **DEFAULT_PATH** against the file for which you want to change the default path.
b. In the **Destination file path** window:



Destination file path

Default path

□ Overwrite if the file already exists on target

i. Enter the desired path
ii. Select the option **Overwrite if the file already exists on target** if necessary.

c. Click **Ok**.

The specified path is set as the destination path.

Send a file

You can select a file and send it to one or more selected devices.

Prerequisites: The user permission required to send a file are Create Action and Custom Create

To send a file to one or more destination devices:

1. In the **Devices** *(on page 23)* page, from the list of devices, select one or more destination devices to which you want to send a file.

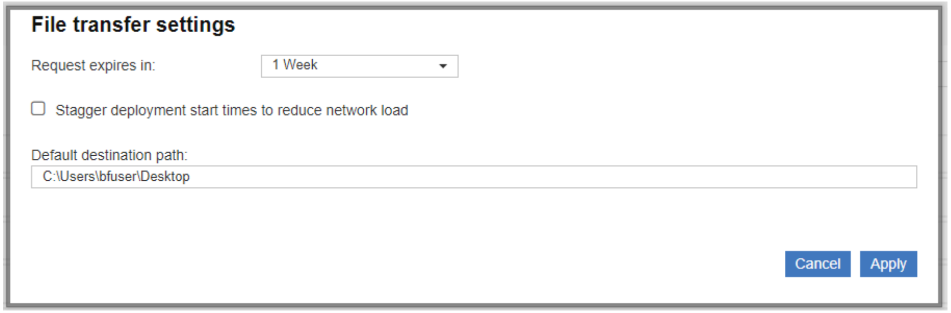
   Important:
   - Select at least one destination device.
   - If you want to select more than one device, then select devices that belong to the same operating system.

2. Click **More** and select **Send file**.
3. From the list of files, select a file to transfer.

   Important: You can send only one file at a time.

   Note: You can search and find a file; sort by upload date, file name, or file size.

   a. **Devices Targeted** – This displays the number of devices selected. Click this button if you want to modify your device selection.
   b. **Settings** – Click this button to define file transfer settings:



File transfer settings

Request expires in: 1 Week

□ Stagger deployment start times to reduce network load

Default destination path: C:\Users\bfuser\Desktop

- **Request expires in** – Select a time period from the drop-down list within which the file can be transferred to the destination devices. After this time period, the file transfer request expires and the file cannot be transferred.
- **Stagger deployment start times to reduce network load** – Select this option if you want to reduce network load.
- **Default destination path** – Specify the default destination path where you want to transfer the file in all selected devices.

4. Click **Send**.

After successful transfer, the file becomes available in the destination devices at the default path set.

Delete

To delete files from the server, from the list of files, select one or more files and click **Delete**.

Note: When a file is removed, only the reference of the file is removed.

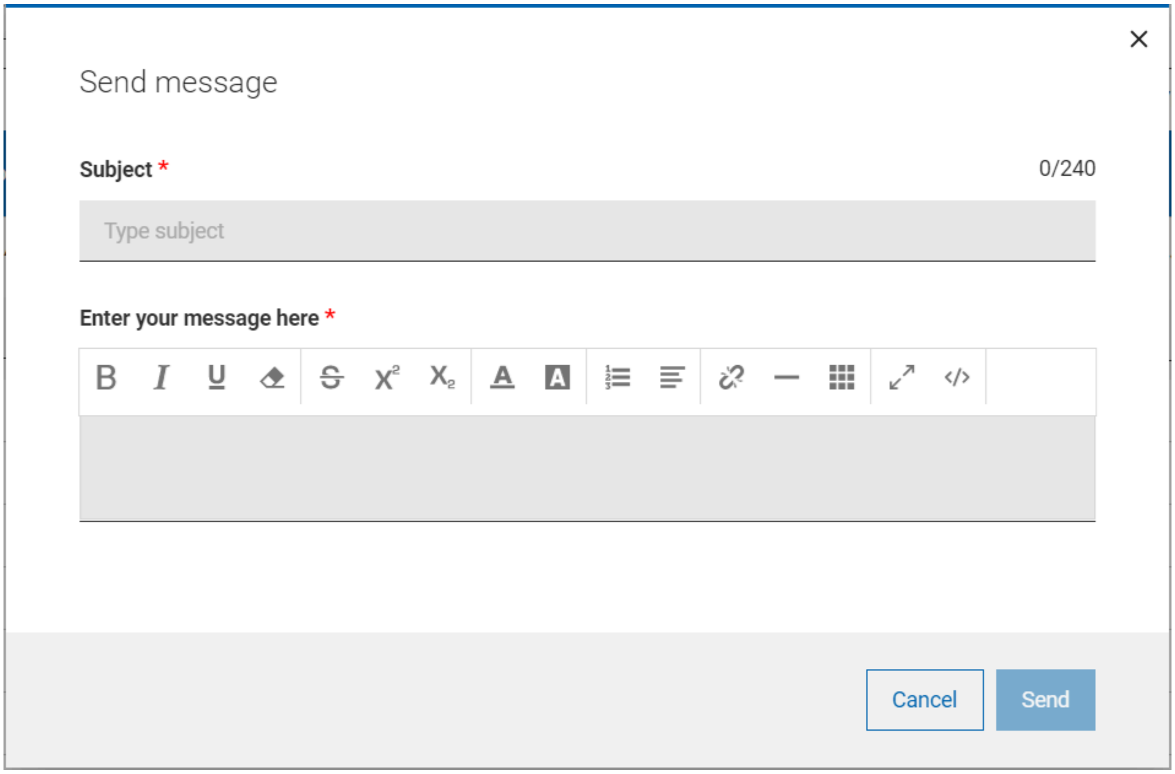
Send Messages to Devices

Using Send Messages feature, you can send a short message notification to multiple selected devices. You can determine if the message is read by the end user and also configure to automatically delete messages from the target devices after a specified number of days.

- The operator must have the following permissions:
  - Can Create Actions
  - Custom Content
- SWD must be running and the operator must have access to it.
- Target devices must have SSA 3.1.0 or later installed with Messages tab setting enabled.

To send message notifications to selected target devices, perform the following steps.

1. Open the **Devices** tab.
2. In the **Devices** page, from the list of devices, select one or more devices to which you want to send the message.
3. Click **Configuration** and select **Send message** from the drop-down.
4. In the **Send message** window, enter your subject and message in the relevant sections.



Note:

- You can enter up to 240 characters including the subject line.
- You can format your content using the formatting options in the toolbar.
- You can copy/paste HTML code into the editor and/or save your message as HTML code.

5. Click **Send**.
    - When the message is sent, a success message is displayed and the relevant action is created for the message sent. If the target device is not installed with SSA 3.1.0 or later, then the message cannot be delivered and the status of this action becomes not relevant.
    - When the user reads the message, the status of the action becomes completed. With this, the operator can determine if the message is read by the end user.
    - To automatically delete messages from the target device user's SSA Message tab after a specified number of days, message expiration days can be set through the WebUI Server setting _WebUIAppEnv_NOTIFICATION_EXPIRATION_DAYS.

Chapter 4. Get Started with Patch

Use the Patch screens to list patches, find specific patches, and view detailed patch information including known issues, vulnerable devices, and deployments.

The Patch List

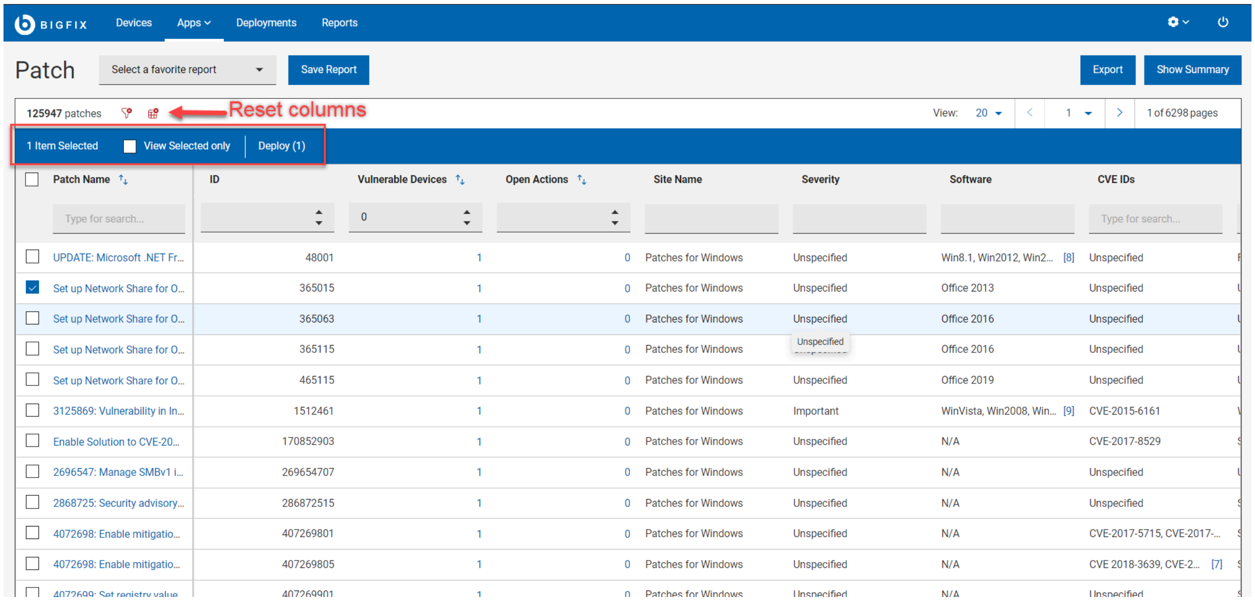
View a list of all patches, create customized patch reports to obtain patching intelligence, make smart patch decisions, report patch compliance, and communicate risks. You can also download and install missing patches using the links in the report.

To access the **Patches** page, from the BigFix WebUI main page, click **Apps > Patch**.

Operator permission settings, connected devices, and site assignments govern the list of contents.

Grid view enables you to quickly view the list of patches in a table. Clicking the patch name navigates to the details of the patch (that is overview, vulnerable devices, and deployment). Every column in the **Patches** page gives an option to search or filter. You can add, remove, and resize columns. You can also click **Reset columns** to return back to default view.

The refine results and customizing the data grid function is similar to those in the device page. For more information, see Grid view (on page 12).



	Patch Name	ID	Vulnerable Devices	Open Actions	Site Name	Severity	Software	CVE IDs
□	UPDATE: Microsoft .NET Fr...	48001	1	0	Patches for Windows	Unspecified	Win8.1, Win2012, Win2... [8]	Unspecified
☑	Set up Network Share for O...	365015	1	0	Patches for Windows	Unspecified	Office 2013	Unspecified
□	Set up Network Share for O...	365063	1	0	Patches for Windows	Unspecified	Office 2016	Unspecified
□	Set up Network Share for O...	365115	1	0	Patches for Windows	Unspecified	Office 2016	Unspecified
□	Set up Network Share for O...	465115	1	0	Patches for Windows	Unspecified	Office 2019	Unspecified
□	3125869: Vulnerability in In...	1512461	1	0	Patches for Windows	Important	WinVista, Win2008, Win... [9]	CVE-2015-6161
□	Enable Solution to CVE-20...	170852903	1	0	Patches for Windows	Unspecified	N/A	CVE-2017-8529
□	2696547: Manage SMBv1 i...	269654707	1	0	Patches for Windows	Unspecified	N/A	Unspecified
□	2868725: Security advisory...	286872515	1	0	Patches for Windows	Unspecified	N/A	Unspecified
□	4072698: Enable mitigatio...	407269801	1	0	Patches for Windows	Unspecified	N/A	CVE-2017-5715, CVE-2017-...
□	4072698: Enable mitigatio...	407269805	1	0	Patches for Windows	Unspecified	N/A	CVE 2018-3639, CVE-2... [7]
□	4072699: Set registry value	407269901	1	0	Patches for Windows	Unspecified	N/A	Unspecified

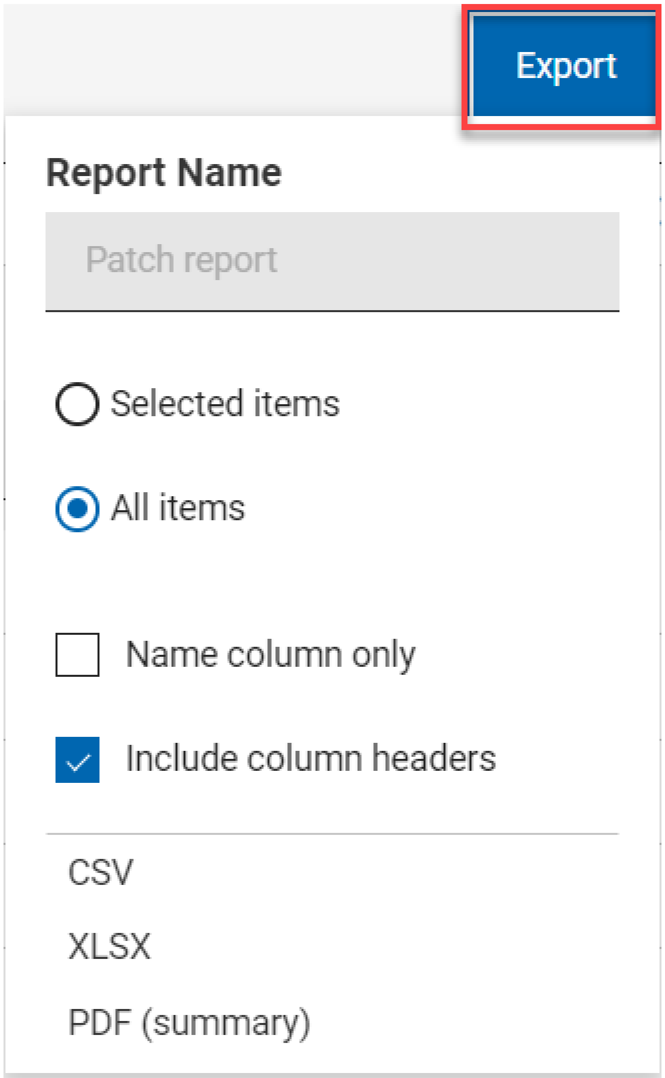
- **Action bar:** Selecting one or more patches from the data grid enables the action bar.
  - **View Selected only:** Check the box to view only the selected patches.
  - **Deploy:** Click **Deploy** to navigate to the Take Action dialog, where you can deploy the patch. The number in the parenthesis indicates the number of patches selected.
- You can use the filters in the headers to refine results:

- See patches required by any number of devices by entering a value in the Vulnerable Devices field.
- See patches which contains open action by entering a value in the Open Action field.
- Use this filter to identify patches by ID.
- Site Name - Only patches from these sites appear in the WebUI:
    - ESU Patching Add-on for Windows 2008 I
    - ESU Patching Add-on for Windows 7
    - Patches for Amazon Linux 2
    - Patches for CentOS 6
    - Patches for CentOS 6 Plugin R2
    - Patches for CentOS 7
    - Patches for CentOS 7 Plugin R2
    - Patches for CentOS 8
    - Patches for Debian 7
    - Patches for Mac OS X
    - Patches for Oracle Linux 6
    - Patches for Oracle Linux 7
    - Patches for Oracle Linux 8
    - Patches for RHEL 5 Extended Support
    - Patches for RHEL 7
    - Patches for RHEL 8
    - Patches for RHEL 8 Extended Support
    - Patches for SLE 11 Native Tools
    - Patches for SLE 12 Native Tools
    - Patches for SLE 12 on System Z
    - Patches for SLE 12 PPC64LE
    - Patches for SLE 15
    - Patches for SLE 15 on System Z
    - Patches for Ubuntu 1404
    - Patches for Ubuntu 1604
    - Patches for Ubuntu 1804
    - Patches for Ubuntu 2004
    - Patches for Windows
    - Updates for Windows Applications
    - Updates for Mac Applications
- See patches for the most critical threats or a specific threat level using the Severity filters. Patch Severity is assigned by the patch vendor (for example, Microsoft), not BigFix.
    - Critical
    - Important
    - Moderate
    - Low
    - Unknown – patch has no vendor-assigned rating.
- Use software filter to see patches that are available for specific software.

    - CentOS
    - Debian
    - OracleLinux
    - Red Hat Enterprise Linux
    - SUSE
    - Ubuntu
    - Unspecified
    - Windows (.NET Core runtimes, Adobe Acrobat, Adobe Flash Player, Adobe Reader, Adobe Shockwave, Google Chrome, GoToMeeting, ImgBurn, Microsoft Edge, Mozilla Firefox, Notepad++, Nullsoft, Oracle, Real Networks, Skype, Webex Meetings, Winamp, Winzip, Zoom)
    - Mac OS
  - Use CVE ID filter to search patches by Common Vulnerabilities and Exposures.
  - See patches associated with a specific task using the Category filters:
    - Audit – Type of BigFix patch that is used to detect conditions that cannot be remediated and require the attention of an administrator.
    - Bug Fix – Apply a change that fixes one or more bugs.
    - Configuration – Apply a change that addresses a configuration issue.
    - Enhancement – Apply a change that provides new features.
    - Other – Apply changes to unspecified patches.
    - Security – Apply a software change to address a vulnerability.
    - Service Pack – Apply patches to installed software. A collection of updates, fixes, or enhancements delivered in a single installable package. Typically used to update existing files, but can also be used to fix bugs, close security holes, or add new features.
  - See the latest patches using the **Release Date** field. Specify a date range to see patches that were issued during a specific time period.
- **Save Report**
  - Save the report for future reference and edit, update, or delete as required. For more information, see Reports *(on page 20)*.
- **Show Summary**
  1. In the **Patches** page, select the required filters.
  2. Click **Show Summary**. You can view the summary of all the filtered patches as charts and tables. Mouse over the interested areas on the chart to get more details about the respective data point and the percentage data. Mouse over on any truncated labels to see the full text in the tooltip. You can change filters or enter search text and the report dynamically displays the relevant information.
      - **Severity By Release Date**: Displays the total number of patches by severity level from the patch release date for a period of time.
      - **By OS Family**: Displays applicable patches for every operating system. The table is sorted alphabetically by OS names.
      - **By Categories**: Displays category wise patch count.
- **Export:**

  You can export the filtered report in a `.csv`, `.xlsx`, or `.pdf` format.

1. In the **Patches** page, select the required filters.
2. Click **Export**.



Report Name

Patch report

○ Selected items

● All items

□ Name column only

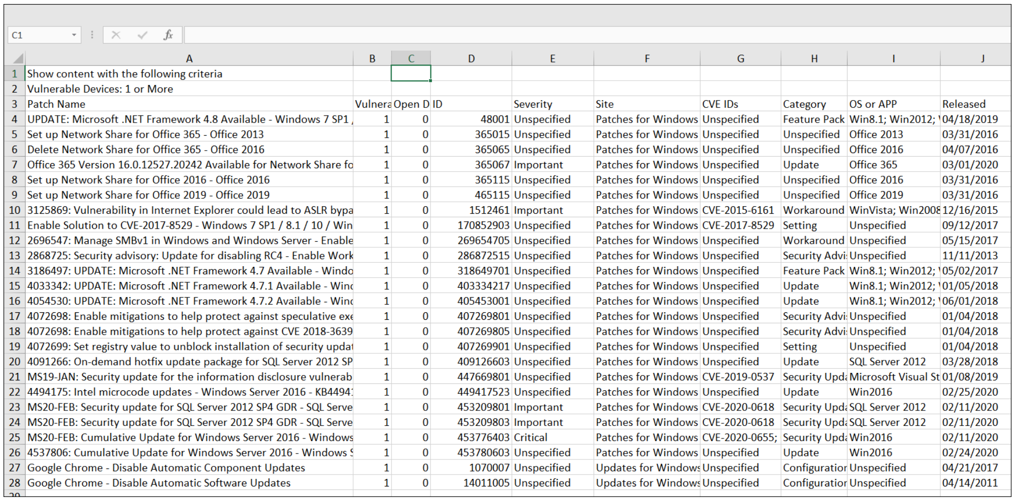
☑ Include column headers

3. The option **Selected Items** allows you to select items from the filtered result to export; **All Items** allows you to export all the items from the filtered list. Select the desired option.
4. Name column only: Select this option if you want to export only the names of the filtered items.
5. Include column headers: Select this option if you want to export details of every default columns of an item.

   Note: If you have displayed columns other than the default columns, you can export name column only.

6. Select a file format (CSV, XLSX, or PDF) that you want to export to.

- By default, the report gets downloaded into your Downloads folder with the default file name (Device_Report_mm_dd_yyyy_username). You can change the download settings in your browser to change the file name and download it into a preferred location. You can save the report to review it later and/or share it with interested stakeholders.
- If you have selected PDF format, a `.zip` file gets downloaded which contains a `.csv` file with numerical data and `.pdf` file with visual representation of the data.
- The exported patch report contains key details about your patches that are displayed after applying the filters and search criteria. The details include the patch name, number of vulnerable devices, severity, CVE IDs along with all the other details that you can see on the screen when you expand every patch. A sample report is shown below:



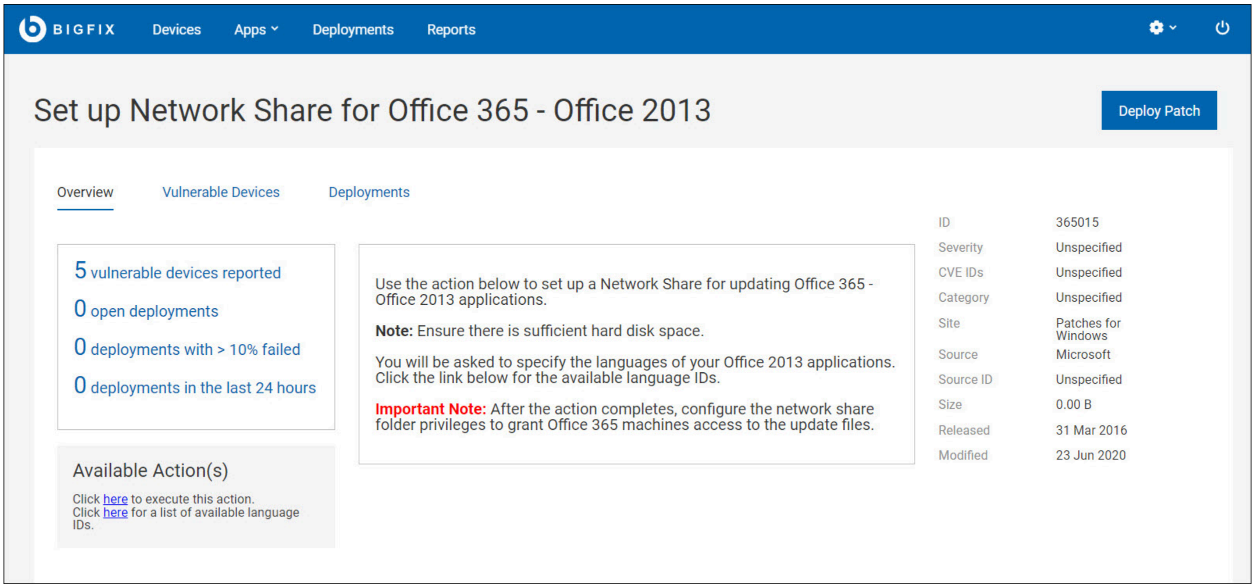
C1

	A	B	C	D	E	F	G	H	I	J
1	Show content with the following criteria									
2	Vulnerable Devices: 1 or More									
3	Patch Name	Vulnera	Open D	ID	Severity	Site	CVE IDs	Category	OS or APP	Released
4	UPDATE: Microsoft .NET Framework 4.8 Available - Windows 7 SP1 /	1	0	48001	Unspecified	Patches for Windows	Unspecified	Feature Pack	Win8.1; Win2012;	04/18/2019
5	Set up Network Share for Office 365 - Office 2013	1	0	365015	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2013	03/31/2016
6	Delete Network Share for Office 365 - Office 2016	1	0	365065	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2016	04/07/2016
7	Office 365 Version 16.0.12527.20242 Available for Network Share fo	1	0	365067	Important	Patches for Windows	Unspecified	Update	Office 365	03/01/2020
8	Set up Network Share for Office 2016 - Office 2016	1	0	365115	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2016	03/31/2016
9	Set up Network Share for Office 2019 - Office 2019	1	0	465115	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2019	03/31/2016
10	3125869: Vulnerability in Internet Explorer could lead to ASLR bypa	1	0	1512461	Important	Patches for Windows	CVE-2015-6161	Workaround	WinVista; Win2008	12/16/2015
11	Enable Solution to CVE-2017-8529 - Windows 7 SP1 / 8.1 / 10 / Win	1	0	170852903	Unspecified	Patches for Windows	CVE-2017-8529	Setting	Unspecified	09/12/2017
12	2696547: Manage SMBv1 in Windows and Windows Server - Enable	1	0	269654705	Unspecified	Patches for Windows	Unspecified	Workaround	Unspecified	05/15/2017
13	2868725: Security advisory: Update for disabling RC4 - Enable Work	1	0	286872515	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	11/11/2013
14	3186497: UPDATE: Microsoft .NET Framework 4.7 Available - Windo	1	0	318649701	Unspecified	Patches for Windows	Unspecified	Feature Pack	Win8.1; Win2012;	05/02/2017
15	4033342: UPDATE: Microsoft .NET Framework 4.7.1 Available - Winc	1	0	403334217	Unspecified	Patches for Windows	Unspecified	Update	Win8.1; Win2012;	01/05/2018
16	4054530: UPDATE: Microsoft .NET Framework 4.7.2 Available - Winc	1	0	405453001	Unspecified	Patches for Windows	Unspecified	Update	Win8.1; Win2012;	06/01/2018
17	4072698: Enable mitigations to help protect against speculative exe	1	0	407269801	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	01/04/2018
18	4072698: Enable mitigations to help protect against CVE 2018-3639	1	0	407269805	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	01/04/2018
19	4072699: Set registry value to unblock installation of security updat	1	0	407269901	Unspecified	Patches for Windows	Unspecified	Setting	Unspecified	01/04/2018
20	4091266: On-demand hotfix update package for SQL Server 2012 SP	1	0	409126603	Unspecified	Patches for Windows	Unspecified	Update	SQL Server 2012	03/28/2018
21	MS19-JAN: Security update for the information disclosure vulnerab	1	0	447669801	Unspecified	Patches for Windows	CVE-2019-0537	Security Upda	Microsoft Visual St	01/08/2019
22	4494175: Intel microcode updates - Windows Server 2016 - KB4494	1	0	449417523	Unspecified	Patches for Windows	Unspecified	Update	Win2016	02/25/2020
23	MS20-FEB: Security update for SQL Server 2012 SP4 GDR - SQL Serve	1	0	453209801	Important	Patches for Windows	CVE-2020-0618	Security Upda	SQL Server 2012	02/11/2020
24	MS20-FEB: Security update for SQL Server 2012 SP4 GDR - SQL Serve	1	0	453209803	Important	Patches for Windows	CVE-2020-0618	Security Upda	SQL Server 2012	02/11/2020
25	MS20-FEB: Cumulative Update for Windows Server 2016 - Windows	1	0	453776403	Critical	Patches for Windows	CVE-2020-0655;	Security Upda	Win2016	02/11/2020
26	4537806: Cumulative Update for Windows Server 2016 - Windows S	1	0	453780603	Unspecified	Patches for Windows	Unspecified	Update	Win2016	02/24/2020
27	Google Chrome - Disable Automatic Component Updates	1	0	1070007	Unspecified	Updates for Windows	Unspecified	Configuration	Unspecified	04/21/2017
28	Google Chrome - Disable Automatic Software Updates	1	0	14011005	Unspecified	Updates for Windows	Unspecified	Configuration	Unspecified	04/14/2011

Patch Document

Click a patch name to see its description, vulnerable devices, and deployment history. Drill further into patch details using the links to associated views.

Pay particular attention to the Notes and Important Notes in a content document: they contain valuable information, including known issues associated with the content.



Set up Network Share for Office 365 - Office 2013

5 vulnerable devices reported
0 open deployments
0 deployments with > 10% failed
0 deployments in the last 24 hours

Use the action below to set up a Network Share for updating Office 365 - Office 2013 applications.

Note: Ensure there is sufficient hard disk space.

You will be asked to specify the languages of your Office 2013 applications. Click the link below for the available language IDs.

Important Note: After the action completes, configure the network share folder privileges to grant Office 365 machines access to the update files.

ID	365015
Severity	Unspecified
CVE IDs	Unspecified
Category	Unspecified
Site	Patches for Windows
Source	Microsoft
Source ID	Unspecified
Size	0.00 B
Released	31 Mar 2016
Modified	23 Jun 2020

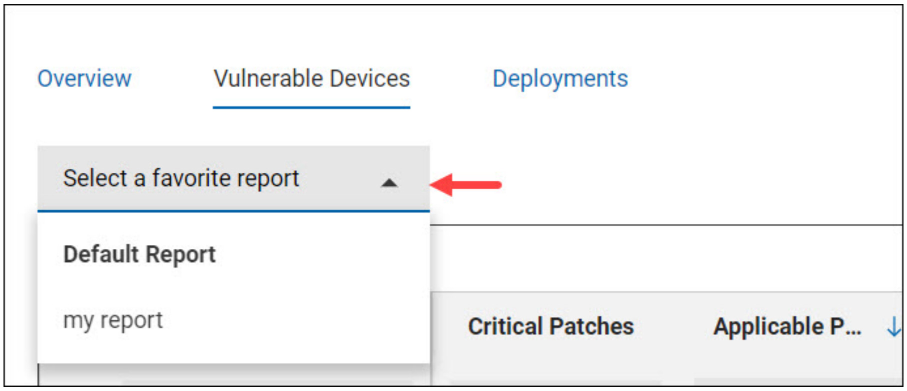
Available Action(s)

Click here to execute this action.
Click here for a list of available language IDs.

The Patch Document views:

- Overview – Detailed description of the patch, including metadata, available actions, and vendor links.
- Vulnerable Devices – List of relevant devices for targeting.
- Deployments – Patch deployment history.

You can load saved reports in the **Vulnerable Devices** and **Deployments** tab. Use the drop-down to select the report.



The information in the Available Actions section is pulled directly from the BigFix database, so options and formatting can vary. A link to the vendor's release notes is often included. For example, "Click here to see the release notes for Windows XP SP3."

Chapter 5. Get Started with Patch Policy

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.

Use the Patch Policy application to establish continuous patching across your enterprise. Create patching schedules for different groups of machines and assign different deployment behaviors to each. 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.

Implement a patching strategy that meets your organization's patching cycles and security guidelines. Use patch policies to establish and maintain a process of continuous security and compliance for your organization. Patch Policies currently supports the sites listed under Supported Patch Sites (on page 43).

Requirements

- BigFix Platform version 9.5.5 or above.
- BigFix WebUI installed and running.
- Subscriptions to all applicable BigFix Patch sites.

From the BigFix console, enable any patch sites that are relevant to your deployment and subscribe all computers to those sites.

Patch Policy Overview

To open the Patch Policy application, from the BigFix WebUI **Apps** menu, select **Patch Policies**.

Perform the following steps to create a patch policy:

1. Enter a name for the policy and select the types of patches it should include. For example, create a policy that includes important service packs for operating system updates.
2. Create a roll out schedule for the policy, including deployment timing, frequency, and behavior.
3. Select policy targets: the devices to be patched.
4. Activate the policy.

   The process is described in detail in Create a Patch Policy (on page 59).

Keeping Policies Current

The Patch Policy app notifies you when new patches that meet policy criteria become available. The delta icon next to a policy name on the Policy List tells you patch content has been added or changed. Refresh a policy to include the new material. Refresh policies manually or use the Auto-refresh option to keep policies up-to-date.

Exclusions

You can exclude patches from a policy that otherwise meet its inclusion criteria. For example, manually exclude a patch you know causes problems in a custom application. Or set a dynamic exclusion to automatically exclude Microsoft Office updates from a policy that updates Windows. Once set, exclusions remain in effect until you remove them. Patch policies never include patches used for auditing, corrupt patches, or patches without a default action.

Use the WebUI Deployment views to monitor policy-based patching results. For more information, see Get Started with Deployments (on page 146).

Permissions and Patch Policy

BigFix master operators (MOs) have full access to all Patch Policy functions. MOs can create, edit, delete, activate, and suspend polices, manage patch rollouts and schedules, and refresh policies when new patches are released. non-master operators (NMOs) can add, edit or delete a policy. NMOs can also add targets to an existing schedule, and remove targets from a schedule if they have relevant permissions.

Patch Policy Category

The following table shows the mapping between the Patch Policy external content categories and Fixlet categories:

WebUI Patch Policy category	Fixlet category
BUG FIX	Bug Fix Bug Fix Advisory Bug
ENHANCEMENT	Definition Update Definition Updates Feature Pack Hotfix Update Updates Product Enhancement Advisory ENHANCEMENT Recommended Optional

WebUI Patch Policy category	Fixlet category
	Upgrade
SERVICE PACK	Rollup Service Pack Update Rollup
SECURITY	Critical Update Critical Updates Security Security Advisory Security Hotfix Security Setting Security Update Security Updates SECURITY Mandatory

Execution behavior

The following table shows the Patch Policy behavior **when using Pre/Post contents** and **when not using Pre/Post contents**:

Table 1. Patch Policy execution behavior

Configuring Pre/Post contents	Execution of MAG order enforced in sequence (MAG1, MAG2, MAG3, and so on)	Using "Force Restart" option available when configuring the schedule	Execution Behavior
When **using** Pre/Post contents	Yes	The restart is only applied at the end of the last MAG execution.	Sequence of MAGs will be executed on all targeted devices, even when patch Fixlets are not relevant. This means any Pre/Post tasks or Post action

Table 1. Patch Policy execution behavior (continued)

Configuring Pre/Post contents	Execution of MAG order enforced in sequence (MAG1, MAG2, MAG3, and so on)	Using "Force Restart" option available when configuring the schedule	Execution Behavior
			restarts will also execute if they are relevant.
When **not using** Pre/Post contents	No[1]	The restart is applied after each MAG because it is unknown which MAG will be the last one to execute.	Each MAG will only execute on targeted devices if the device is applicable to at least one of the Fixlets in the MAG.

Note:

A Fixlet is included in the MAG if it is relevant to at least one endpoint managed by the operator who defined the targets in the schedule.

1. **When not using pre/post content**: MAGs do not necessarily execute in order on the endpoint. The MAGs will execute in order when they become relevant on the endpoint.

Note:

The MAG action issued in Patch Policies through **Target by Property**, **Target by Group**, or **Target by Device** will exclusively consist of fixlets that are relevant to the devices targeted at the time the MAG is issued. If there are no relevant fixlets available, then no MAG will be issued. For more details, see Server Settings.

Operating system updates

The following table shows the mapping between Fixlet sites and the selections available in Patch Policies:

Amazon Linux

Table 2. OS Version and Fixlet site name for Amazon Linux

OS Version	Fixlet Site Name
Amazon Linux 2	Patches for Amazon Linux 2
Amazon Linux 2 with Graviton	Patches for Amazon Linux 2 Graviton

Rocky Linux

Table 3. OS Version and Fixlet site name for Rocky Linux

OS Version	Fixlet Site Name
Rocky Linux 8	Patches for Rocky Linux 8

CentOS

Table 4. OS Version and Fixlet site name for CentOS

OS Version	Fixlet Site Names
CentOS 6	Patches for CentOS 6 Plugin R2
CentOS 7	Patches for CentOS 7 Plugin R2
CentOS 8	Patches for CentOS 8

Debian

Table 5. OS Version and Fixlet site name for Debian

OS Version	Fixlet Site Names
Debian 7	Patches for Debian 7
Debian 11	Patches for Debian 11

Mac OS X

Table 6. OS Version and Fixlet site name for Mac OS X

OS Version	Fixlet Site Name
Any, patches are dynamically filtered from sites	Patches for Mac OS X

Oracle Linux

Table 7. OS Version and Fixlet site name for Oracle Linux

OS Version	Fixlet Site Names
Oracle Linux 6	Patches for Oracle Linux 6
Oracle Linux 7	Patches for Oracle Linux 7
Oracle Linux 8	Patches for Oracle Linux 8

Red Hat Enterprise Linux

Table 8. OS Version and Fixlet site name for Red Hat Enterprise Linux

OS Version	Fixlet Site Names
Red Hat Enterprise 5	Patches for RHEL 5 ESU
Red Hat Enterprise 6	• Patches for RHEL 6 Native Tools • Patches for RHEL RHSM 6 on System Z • Patches for RHEL 6 ESU
Red Hat Enterprise 7	• Patches for RHEL 7 • Patches for RHEL 7 ppc64le • Patches for RHEL 7 ppc64be • Patches for RHEL RHSM 7 on System Z • Patches for RHEL 7 ESU
Red Hat Enterprise 8	• Patches for RHEL 8 • Patches for RHEL 8 ESU • Patches for RHEL 8 ppc64le
Red Hat Enterprise 9	• Patches for RHEL 9

SUSE Linux Enterprise

Table 9. OS Version and Fixlet site name for SUSE Linux Enterprise

OS Version	Fixlet Site Names
SLE 11	Patches for SLE 11 Native Tools
SLE 12	Patches for SLE 12
SLE 12 PPC64LE	Patches for SLE 12 ppc64le
SLE 12 System z	Patches for SLE 12 on System z
SLE 15	Patches for SLE 15
SLE 15 System z	Patches for SLE 15 on System z

Ubuntu

Table 10. OS Version and Fixlet site name for Ubuntu

OS Version	Fixlet Site Names
Ubuntu 14.04	Patches for Ubuntu 1404
Ubuntu 16.04	Patches for Ubuntu 1604
Ubuntu 18.04	Patches for Ubuntu 1804
Ubuntu 20.04	Patches for Ubuntu 2004
Ubuntu 22.04	Patches for Ubuntu 2204

Windows

Table 11. OS Version and Fixlet site name for Windows

OS Version	Fixlet Site Name
Any patches for OS versions selected are dynamically filtered from sites	• Enterprise Security • Patches for Windows (German) • Patches for Windows (French) • Patches for Windows (Polish) • Patches for Windows (Italian) • Patches for Windows (Spanish) • Patches for Windows (Czech) • Patches for Windows (Brazilian Portuguese) • Patches for Windows (Japanese) • Patches for Windows (Simplified Chinese) • Patches for Windows (Korean) • Patches for Windows (Turkish) • Patches for Windows (Hungarian) • Patches for Windows (NLD) • Patches for Windows (CHT) • Patches for Windows (Norwegian) • Patches for Windows (Finnish) • Patches for Windows (Swedish) • Patches for Windows (Greek) • Patches for Windows (Danish) • Patches for Windows (Hebrew) • Patches for Windows (Russian) • Patches for Windows 7 ESU • Patches for Windows 2008 ESU

Operating system application updates

The following table shows the **Operating System** application updates which includes OS, various site names, and applications:

OS Application Updates for Mac OS X and Windows

Table 12. Fixlet site name and Application updates for Mac OS X and Windows

OS	Fixlet Site Names	Applications
Mac OS X	Patches for Mac OS X	• Java • iTunes • Safari
Windows	• Enterprise Security • Patches for Windows (German) • Patches for Windows (French) • Patches for Windows (Polish) • Patches for Windows (Italian) • Patches for Windows (Spanish) • Patches for Windows (Czech) • Patches for Windows (Brazilian Portuguese) • Patches for Windows (Japanese) • Patches for Windows (Simplified Chinese) • Patches for Windows (Korean) • Patches for Windows (Turkish) • Patches for Windows (Hungarian) • Patches for Windows (NLD)	For more information, see System requirements.

Table 12. Fixlet site name and Application updates for Mac OS X and Windows (continued)

OS	Fixlet Site Names	Applications
	• Patches for Windows (CHT) • Patches for Windows (Norwegian) • Patches for Windows (Finnish) • Patches for Windows (Swedish) • Patches for Windows (Greek) • Patches for Windows (Danish) • Patches for Windows (Hebrew) • Patches for Windows (Russian) • Patches for Windows 7 ESU • Patches for Windows 2008 ESU	

Third-party updates

The following table shows the third-party updates which includes OS, various site names, and application/publisher:

Third-party updates for Mac OS X and Windows

Table 13. Fixlet site name and Application/Publisher updates for Mac OS X and Windows

OS	Fixlet Site Names	Applications/Publisher
Mac OS X	Updates for Mac Applications	• Adobe Acrobat • Adobe Air • Adobe Flash • Adobe Reader • Adobe Shockwave • Google Chrome • GoToMeeting • Microsoft • Mozilla Firefox

Table 13. Fixlet site name and Application/Publisher updates for Mac OS X and Windows (continued)

OS	Fixlet Site Names	Applications/Publisher
		• Webex • Zoom
Windows	• Updates for Windows Applications • Advanced Patching • Updates for Windows Applications Extended	See System requirements for more details.

Severity mapping

The following table shows the mapping between the **Patch Policy Severity** categories and **Fixlet Severity Field** categories:

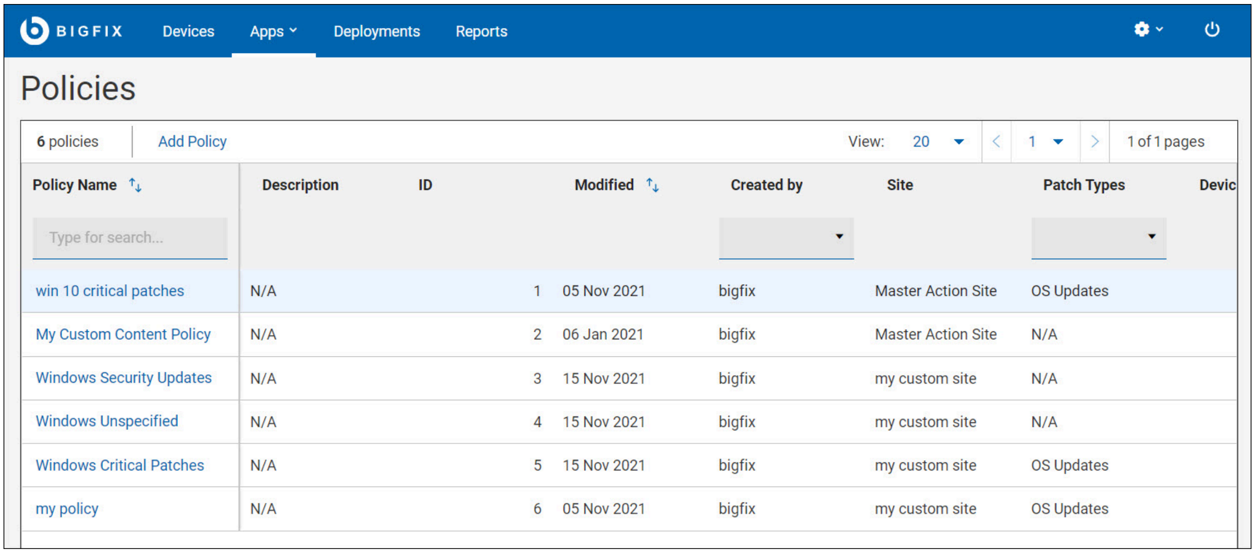
Table 14. Patch Policy Severity and Fixlet Severity Field

Patch Policy Severity	Fixlet Severity Field
CRITICAL	Critical, Mandatory, High
IMPORTANT	Important, Recommended
MODERATE	Moderate
LOW	Low, Optional
UNSPECIFIED	Unspecified, NA, and empty values

The Patch Policy List

The available policies are listed in a grid view. Use the search, sort, and filter option in respective column to find policies quickly. Click a policy name to open its document. Click the **Add Policy** button to create a new policy.

Important: Non-master Operators (NMOs) need relevant permissions to perform different actions in the Patch Policies app. For more information on permissions, see The WebUI Permissions Service.



Policy Name	Description	ID	Modified	Created by	Site	Patch Types	Devic
win 10 critical patches	N/A	1	05 Nov 2021	bigfix	Master Action Site	OS Updates	
My Custom Content Policy	N/A	2	06 Jan 2021	bigfix	Master Action Site	N/A	
Windows Security Updates	N/A	3	15 Nov 2021	bigfix	my custom site	N/A	
Windows Unspecified	N/A	4	15 Nov 2021	bigfix	my custom site	N/A	
Windows Critical Patches	N/A	5	15 Nov 2021	bigfix	my custom site	OS Updates	
my policy	N/A	6	05 Nov 2021	bigfix	my custom site	OS Updates	

Out of Date Policies

Policies can fall out-of-date when there are new patches, or their patches have been modified or replaced. The number of new items are listed in the **Patch Updates** column.

Refresh a policy to include the new content. Active out of date policies continue to run, though they are not particularly effective. For example, say you create a new policy that runs daily at 3 P.M. On the first day it runs, patches are deployed to its designated targets. On the second day new patches become available and the policy falls out of date. On the third and subsequent days the policy runs but does nothing, since the patches it knows about have already been deployed. As soon as you refresh the policy it will deploy the new patches.

Patches that have been superseded by the new content are no longer be deployed.

The following list helps you to understand each individual column in the grid view:

- Patches: Number of patches in the policy.
- Devices: Number of targeted computers and computer groups.
- OS: Operating system of patches in the policy.
- Patch Type: OS update, Application update, or 3rd Party application update.
- Status: Active or Suspended.
- Patch Updates: Number of Fixlets changed since date and time of creation, or last refresh.
- Next Refresh: Date of next scheduled Auto-refresh, if enabled.
- Site: Custom site that contains the patch policy.

Policy Status: Active or Suspended

Patch policies have two states: Active or Suspended. Suspend an Active policy to refresh it, add a new schedule, or make other changes. You do not have to suspend a policy to add or remove targets. New policies remain suspended until you activate them.

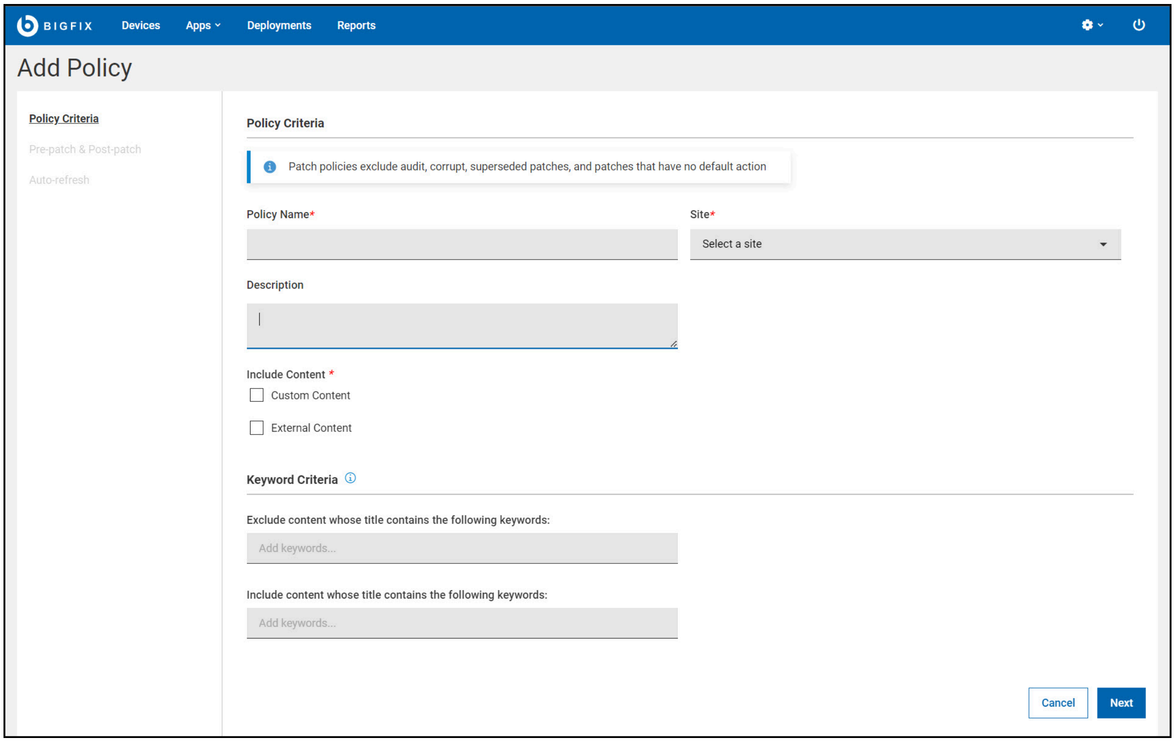
Create a Patch Policy

In this page, steps for creating a patch policy, selecting patches to include, setting deployment options, and designating targets are provided in detail.

To open the application, select **Patch Policies** from the WebUI **Apps** menu. For a summary of Patch Policy tasks, see Patch Policy Operations *(on page 73)*.

1. On the **Policies** page, click **Add Policy**.
   The **Add Policy** page is displayed.

   Note: A non-master operator (NMO) needs Create/Edit Policy and Delete Policy permissions to add, edit or delete policy. For more information on permissions, see The WebUI Permissions Service. NMOs cannot edit definition of the policy stored in the Master Action Site despite having the permission to Create/Edit Policy. Currently, NMOs are not allowed to access the Master Action Site and they can access only their custom site.



Add Policy

Policy Criteria

Patch policies exclude audit, corrupt, superseded patches, and patches that have no default action

Policy Name*

Site*
Select a site

Description

Include Content *
□ Custom Content
□ External Content

Keyword Criteria

Exclude content whose title contains the following keywords:
Add keywords...

Include content whose title contains the following keywords:
Add keywords...

2. Provide the following information under Policy Criteria page:

   Policy Name

   Enter the new policy name.

   Site

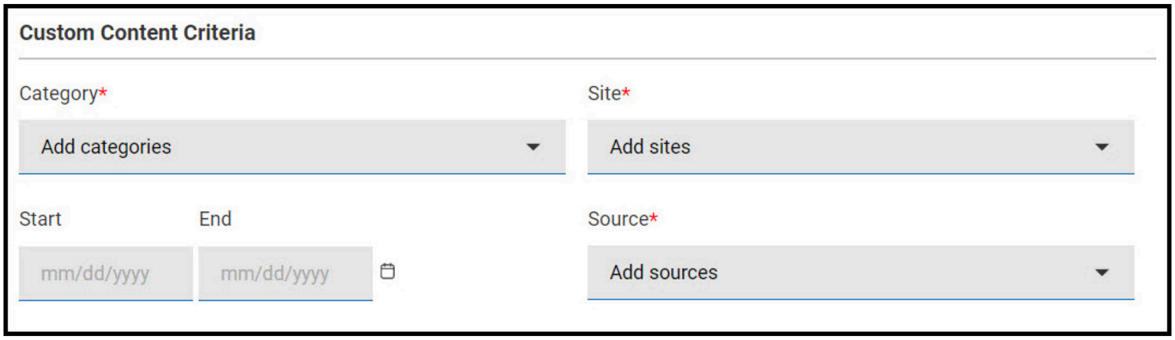
Select the **Master Action Site** or **Custom Site** from the drop-down to store the policy and its schedules.

Description

Enter the description.

3. You can include two types of content: Custom Content and/or External Content.

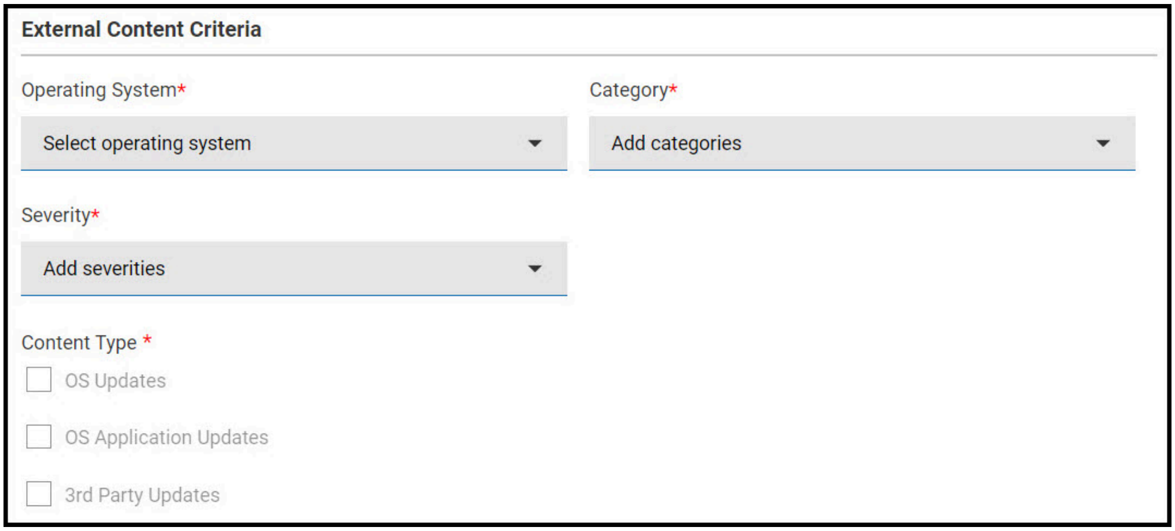
Custom Content:



a. Check this option to include Fixlets from a custom site.
b. Under **Custom Content Criteria**, select the **Category**, **Sites**, **Start/End Date**, and **Sources** dates from the drop-down that the new policy must include.

Note: Custom Fixlets must include the above fields in order to be included in the policy.

External Content:



a. Check this option to include Fixlets from an external site.
b. Under **External Content Criteria**, select the **Operating System**, **Category**, **Severity**, and **Content type**.

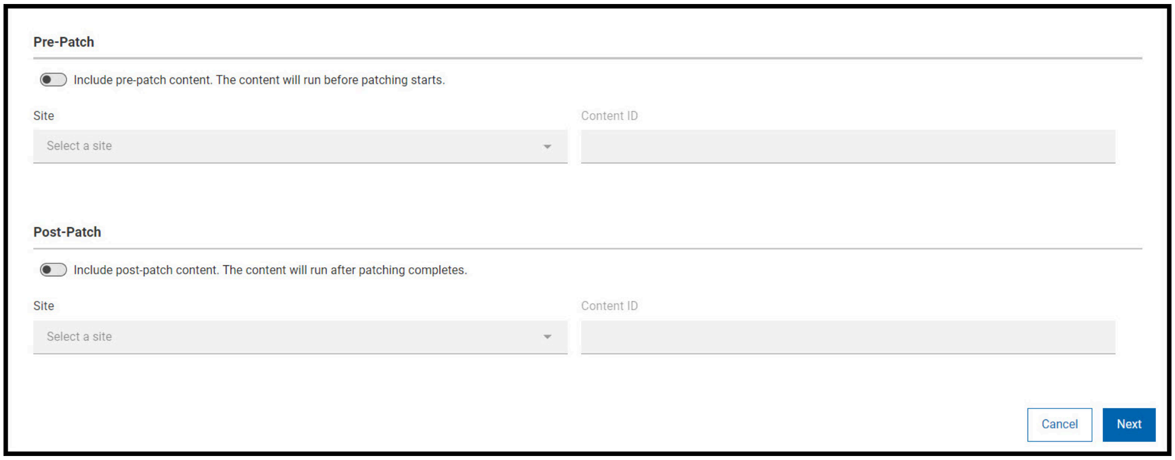
- Operating System (choose one): Amazon Linux, CentOS, Mac OS X, Oracle Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise, Ubuntu, Windows.
- Category: Bug Fix, Enhancement, Security.
- Severity: Critical, Important, Moderate, Low, Unspecified.
- Content Type: OS Updates, OS Application Updates, 3rd Party Updates.

Note: While creating the patch policy, ensure the following:

- Fixlets must have a default action. If not, the Fixlets will not be included in the patch policy.
- Patch policies will only detect Fixlets that has a default action.
- Tasks will not be detected.

4. If required, specify any patch exclusions or inclusions under **Keyword Criteria**. Type a keyword or phrase from the patch title and press **Enter** to add more. These fields are not case-sensitive, so capitalization can be ignored. Use ⊕ and × icons to remove/add a keyword or phrase.
5. Click **Next** to configure the **Pre-Patch and Post-Patch** behaviour of the new policy. For more details on **when using Pre/Post content** and **when not using Pre/Post content**, see Execution behavior *(on page 50)*.

Note: It is not mandatory to configure Pre-patch and Post-patch contents, you can either have Pre-patch content or Post-patch content or both. You can skip this step by clicking **Next** if you do not want Pre-patch and Post-patch content in your new patch policy.



Pre-Patch

○ Include pre-patch content. The content will run before patching starts.

Site: Select a site

Content ID:

Post-Patch

○ Include post-patch content. The content will run after patching completes.

Site: Select a site

Content ID:

a. Click the **toggle switch** to enable Pre-patch or Post-patch.

Note: By default, the Pre-patch and Post-patch is disabled.

b. Select the **Site** from the drop-down.

Note: You can only select a **Custom Site**.

c. Enter the **Content ID**. The name of the Fixlet or Task is displayed below Content ID.

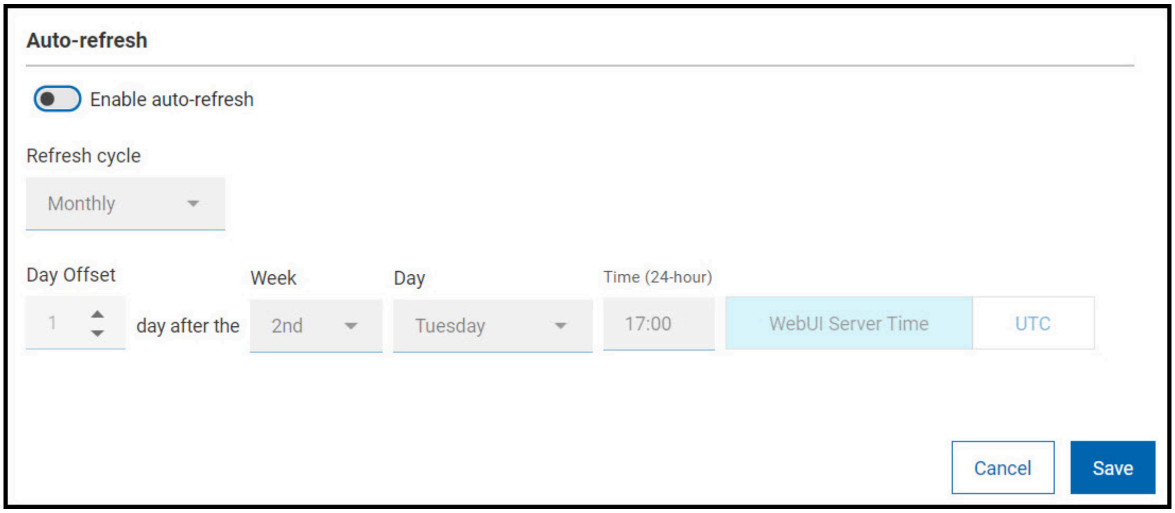
Note: The Content ID field only accepts a single **Fixlet** or **Task**.

Note:

If Pre-Patch or Post-Patch is selected, the following behaviors apply:

- If the resultant policy action contains 200 or fewer Fixlets, the policy action will be executed on targeted devices if the devices are applicable to the pre-task, post-task, or any of the patch Fixlets within the policy.
- If the resultant policy action contains more than 200 Fixlets, the policy action will be executed on all targeted devices, not just the devices that are applicable to the patch Fixlets within the policy. In addition, settings like Offers and Force Restart will be executed on all the targeted devices, if enabled.

6. Click **Next** to configure the Auto-refresh behaviour of the new policy.
7. Use the optional Auto-refresh feature to automatically include new patch content in your policy. To control update timing and frequency, set a refresh interval. Auto-refresh is disabled by default.


Auto-refresh

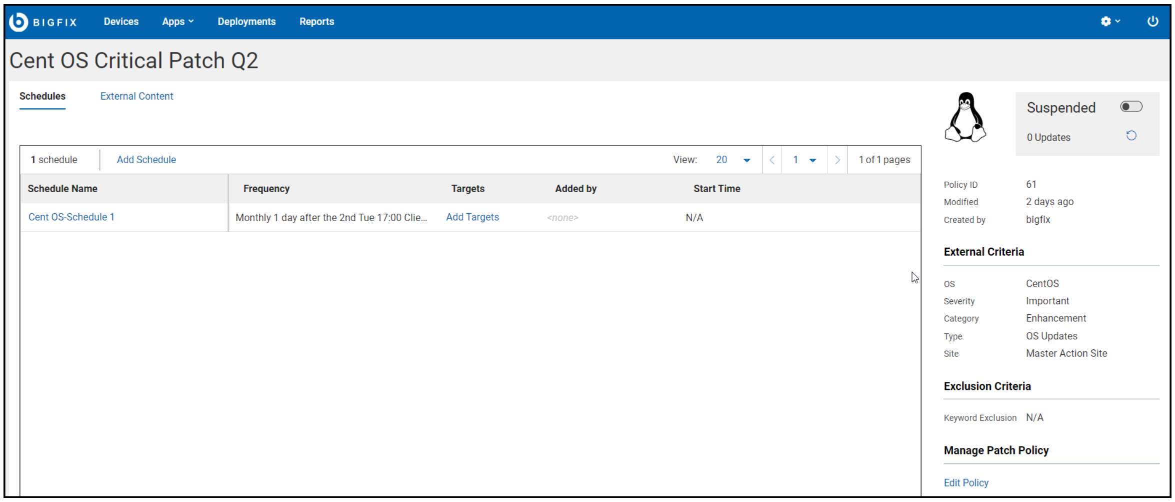
Enable auto-refresh

Refresh cycle: Monthly

Day Offset: 1 day after the Week: 2nd Day: Tuesday Time (24-hour): 17:00 WebUI Server Time UTC

- Refresh cycle (daily, weekly, monthly), on a specific day (of week/month) at (hour).
- Day Offset: Use the optional Day After controls to schedule Auto-refresh updates relative to a monthly event, such as patch Tuesday. The second Tuesday of the month often falls in the second week—but not always. (For example, in August of 2018, Patch Tuesday fell on the 14th.) Use the Day After options to coordinate refreshes with events whose dates change month to month.
- Time Zone: Select the desired time zone (WebUI Server Time or UTC).

8. Click **Save** to save policy settings and display the policy document.



Cent OS Critical Patch Q2

1 schedule

Schedule Name	Frequency	Targets	Added by	Start Time
Cent OS-Schedule 1	Monthly 1 day after the 2nd Tue 17:00 Clie...	Add Targets	<none>	N/A

Policy ID 61
Modified 2 days ago
Created by bigfix

External Criteria

OS CentOS
Severity Important
Category Enhancement
Type OS Updates
Site Master Action Site

Exclusion Criteria

Keyword Exclusion N/A

Manage Patch Policy

Edit Policy

The **Schedules** and **Content** (External/Custom) tabs, appear at the upper left, beneath the policy name. A policy summary appears on the right. Once established, policy schedules will display on the left. The **Edit Policy** control appear at the lower right. The **Added by** column represents the operators who had added targets to the schedule and in the case of Target By Property, it's the operator who had set the condition.

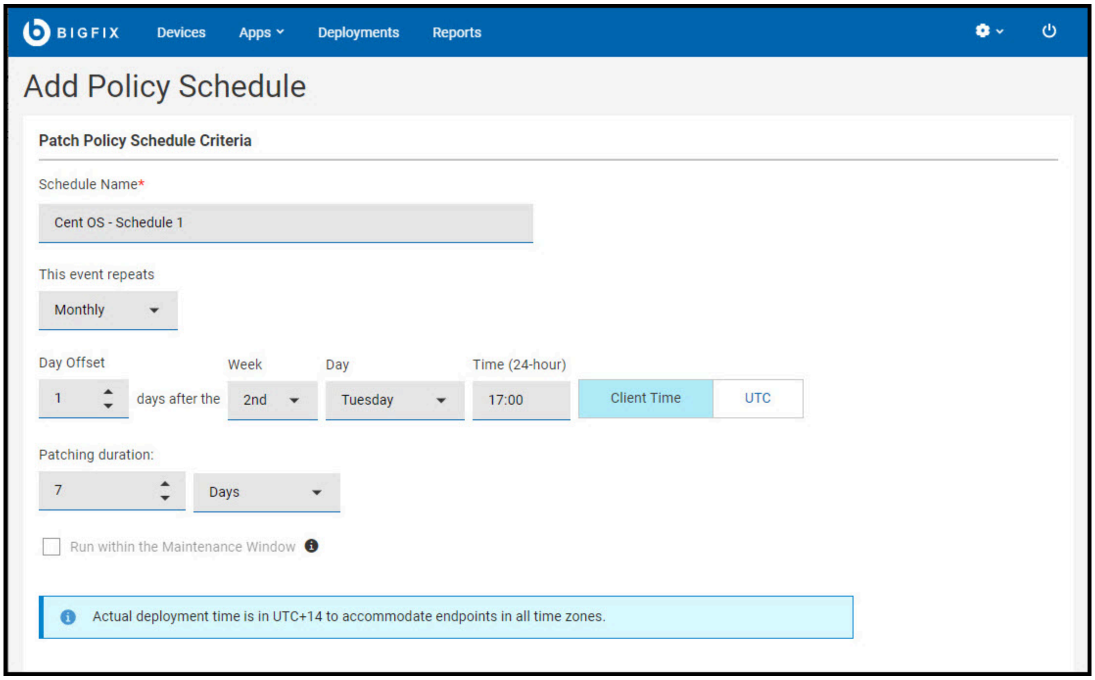
Note: You can delete a policy using the **Delete Policy** action. To delete a policy, click **Edit Policy** and in the Edit Policy page, click **Delete Policy**.

9. Click the **Add Schedule** button to set policy deployment timing, behavior, and targets. A policy can have multiple schedules, each with its own deployment options and targets. A policy without a schedule does not deploy.

   Scheduling adds predictability to patching and can help minimize errors. It also ensures that your environment meets company security policies in time for compliance audits. Some vendors follow a regular patch release schedule, which can tailor your policy schedule to meet. You may want to roll out a policy in a test environment prior to deploying to production. Consider defining separate patch rollouts for Test, QA, and production stages, each with their own timing and duration.

   Note: NMOs need Create/Edit Schedule and Delete Schedule permissions to add, edit, or delete a schedule. For more information on permissions, see The WebUI Permissions Service. NMOs also need write access to the site where the policy is stored to add, edit, or delete a schedule.

a. Enter a name for the schedule and set the deployment interval.



Add Policy Schedule

Patch Policy Schedule Criteria

Schedule Name*: Cent OS - Schedule 1

This event repeats: Monthly

Day Offset: 1 days after the Week: 2nd Day: Tuesday Time (24-hour): 17:00 Client Time UTC

Patching duration: 7 Days

□ Run within the Maintenance Window

Actual deployment time is in UTC+14 to accommodate endpoints in all time zones.

i. This event repeats (daily, weekly, monthly), on (day of week/month).
ii. Day after: Use the optional Day after controls to schedule patching relative to a monthly event, such as Patch Tuesday. The second Tuesday of the month often falls in the second week—but not always. (For example, in August of 2018, Patch Tuesday fell on the 14th.) Use the Day after options to coordinate patching with events whose dates change month to month.
iii. At (Start time).
iv. Time Zone: Use Client time to initiate a process relative to its time zone, for example, to initiate patching in the overnight maintenance window where each endpoint resides. Use UTC time when you want all endpoints to act simultaneously across all time zones.
   - Client Time - the local time on each endpoint; the time on the device where the BigFix agent is installed.
   - Universal Time - Coordinated Universal Time (UTC) is the global standard used to regulate clocks and time worldwide.

   Note: If you specify Client Time, the policy Start time will begin at the specified time in UTC+14 time zone. For more information. See Deployment Time *(on page 69)*

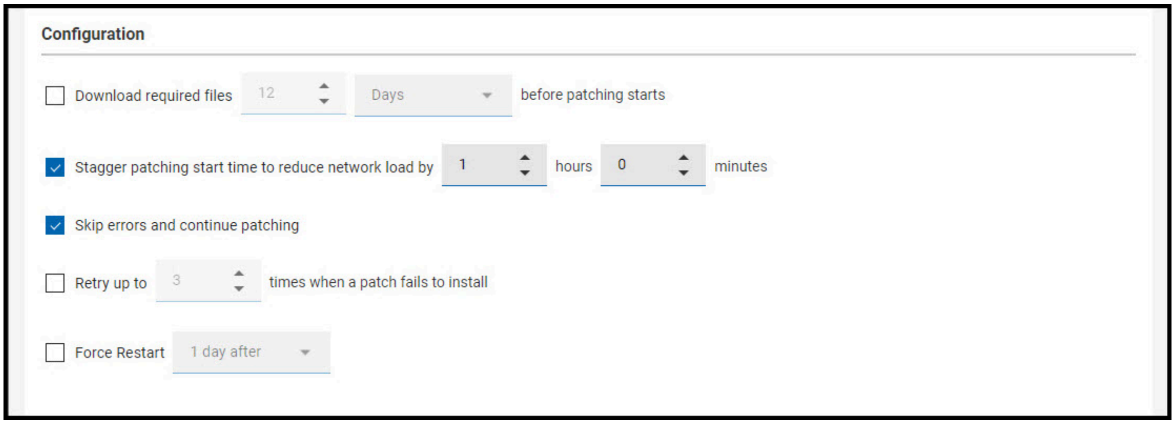
v. Patching Duration (minutes, hours, or days, up to 30 days). The amount of time the policy will attempt to install patches on a target device that is not responding.
vi. Run within the Maintenance Window - This option allows you to run patch policies during maintenance activities. You can use the Maintenance Windows Dashboard to schedule maintenance activities run by BigFix.

> **Note:** To use this feature, a global In Maintenance Window property must exist.

To create the global In Maintenance Window property:

1. From the BigFix console, go to **Tools > Manage Properties**.
2. Select **In Maintenance Window** property from the BES support site, click **Make Custom Copy**, and then click **OK**.

10. Set deployment and post-deployment behavior.



Configuration

☐ Download required files 12 Days before patching starts

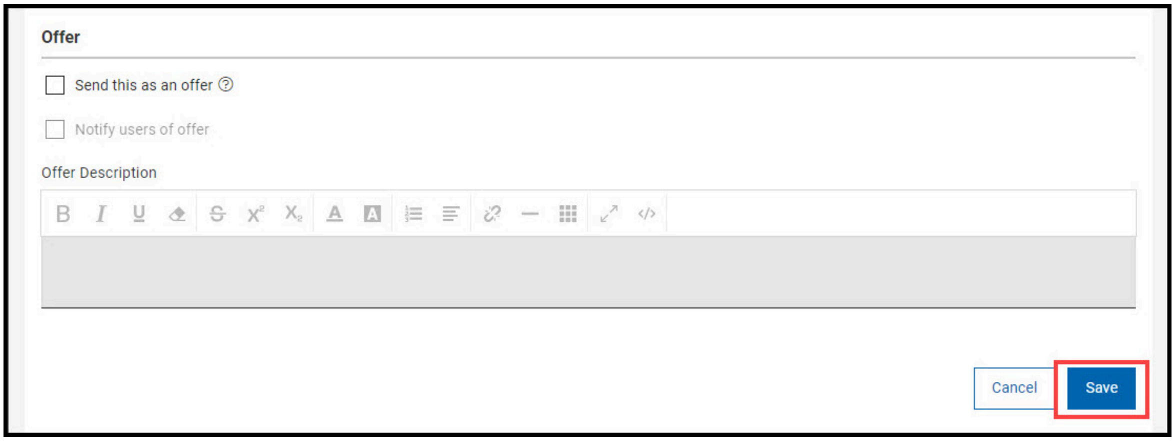
☑ Stagger patching start time to reduce network load by 1 hours 0 minutes

☑ Skip errors and continue patching

☐ Retry up to 3 times when a patch fails to install

☐ Force Restart 1 day after

    - Pre-caching: To download required files before patching starts, set the in minutes, hours, or days up to 5 days.
    - Stagger patching start time, for example, to reduce network load. Set an unlimited number of minutes or hours.
    - Bypass patch errors and continue patching. Patch policies are Multiple Action Groups (MAGs). MAGs run sequentially and stop on the first action that fails. Use the Bypass patch errors option to ignore failures and proceed to the next action. Use this option when the actions in a MAG do not depend on the actions that precede them. For more information about policies and Multiple Action Group (MAG) processing, see Monitoring Deployed Policies *(on page 73)*.
    - Retry up to *n* times (unlimited). If a patch fails to install on a device, for example, due to lack of space on the hard drive, set a retry value and the wait period between attempts.
        - Wait *n* (minutes, hours, up to 30 days) between attempts to install.
        - Wait until device has rebooted to install.
    - Force a Restart - Force a restart on completion. Notify device owners when a restart is required and provide options for restarting at a convenient time. (1, 7, 15 days). Use the default message or type in your own.
11. Use **Offer** feature to send the schedule as an offer which gives the operator an option to accept the schedule if they are interested.



Offer

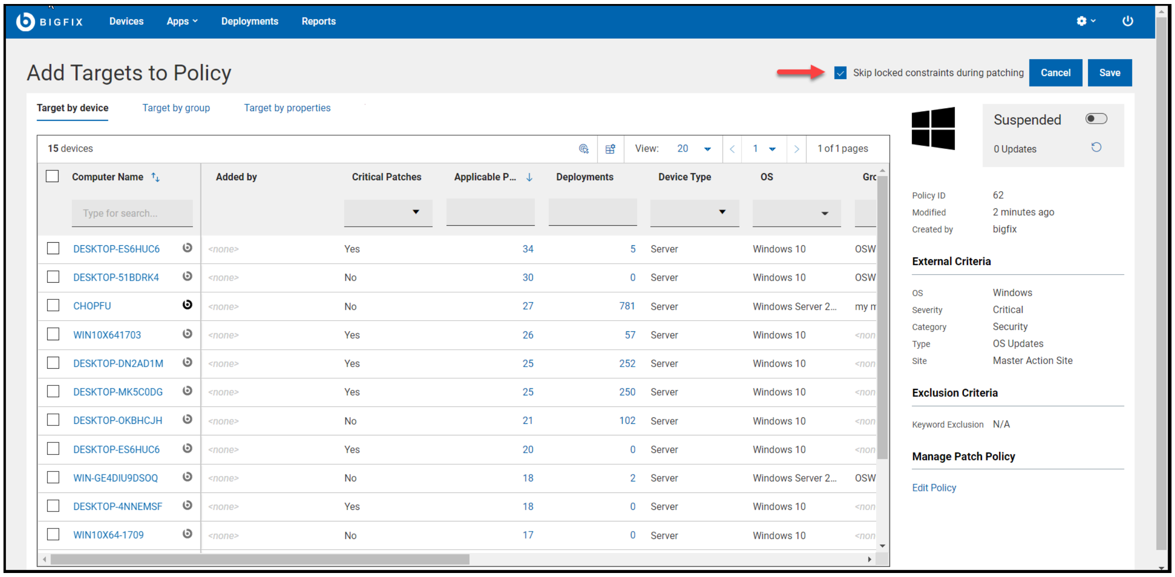
□ Send this as an offer

□ Notify users of offer

Offer Description

a. Check **Send this as an offer**.
b. If required, check **Notify users of offer**.
c. Enter the **Offer Description**.

12. Click **Save** to save the schedule and return to the policy document.
13. The new schedule appears at the top of the list. Click **Add Targets**.



Add Targets to Policy

☑ Skip locked constraints during patching

15 devices

View: 20 | 1 | 1 of 1 pages

Computer Name	Added by	Critical Patches	Applicable P...	Deployments	Device Type	OS	Grc
DESKTOP-ES6HUC6	<none>	Yes	34	5	Server	Windows 10	OSW
DESKTOP-51BDRK4	<none>	No	30	0	Server	Windows 10	OSW
CHOPFU	<none>	No	27	781	Server	Windows Server 2...	my m
WIN10X641703	<none>	Yes	26	57	Server	Windows 10	<non
DESKTOP-DN2AD1M	<none>	Yes	25	252	Server	Windows 10	<non
DESKTOP-MK5C0DG	<none>	Yes	25	250	Server	Windows 10	<non
DESKTOP-OKBHCJH	<none>	No	21	102	Server	Windows 10	<non
DESKTOP-ES6HUC6	<none>	Yes	20	0	Server	Windows 10	<non
WIN-GE4DIU9DSOQ	<none>	No	18	2	Server	Windows Server 2...	OSW
DESKTOP-4NNEMSF	<none>	Yes	18	0	Server	Windows 10	<non
WIN10X64-1709	<none>	No	17	0	Server	Windows 10	<non

Suspended

0 Updates

Policy ID 62
Modified 2 minutes ago
Created by bigfix

External Criteria

OS Windows
Severity Critical
Category Security
Type OS Updates
Site Master Action Site

Exclusion Criteria

Keyword Exclusion N/A

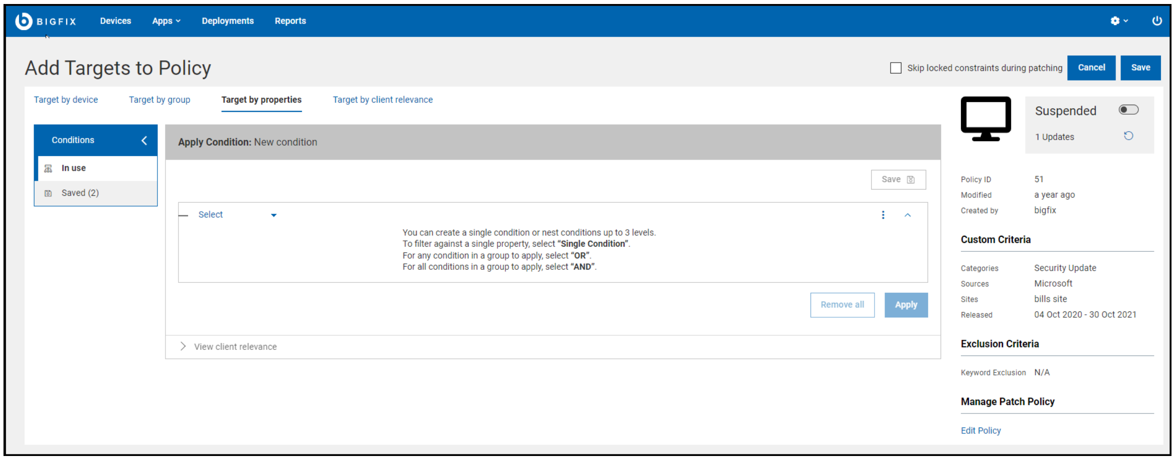
Manage Patch Policy

Edit Policy

Skip locked constraints during patching: Use this feature to deploy patches to locked devices without having to unlock the device. This option is only available to an operator with console lock or unlock permissions, and only applies to targets added by that operator. For information on lock permission, see **Can Lock** - Adding Local Operators.

Note: NMOs need Add/Remove Your Own Targets permission to add or remove the self created targets. NMOs need Remove Other Operator's Targets permission to delete the targets that are created by other operators. NMOs can target only the permitted number of devices and cannot exceed the limit. In case of violation, WebUI app will display an error message and the NMOs cannot proceed further. For more information on permissions, see The WebUI Permissions Service. NMOs need read access to the site where the policy is stored to add/remove the targets.

14. Select devices or computer groups from the **Target by device** or **Target by groups** tabs. Alternatively, you can define a set of property conditions with **Target by properties** and the policy will be issued to the devices that match those conditions. Note that you cannot mix targeting methods in a single schedule. A schedule without targets does not deploy. Check the device to select or deselect it. The numbers in **Applicable Patches** and **Deployments** column refers to the number of patches associated with that device and the deployments information. Use your browser's **Back** button to return to the Patch Policy app.



Apply Condition: New condition

You can create a single condition or nest conditions up to 3 levels.
To filter against a single property, select "Single Condition".
For any condition in a group to apply, select "OR".
For all conditions in a group to apply, select "AND".

Policy ID 51
Modified a year ago
Created by bigfix

Custom Criteria

Categories Security Update
Sources Microsoft
Sites bills site
Released 04 Oct 2020 - 30 Oct 2021

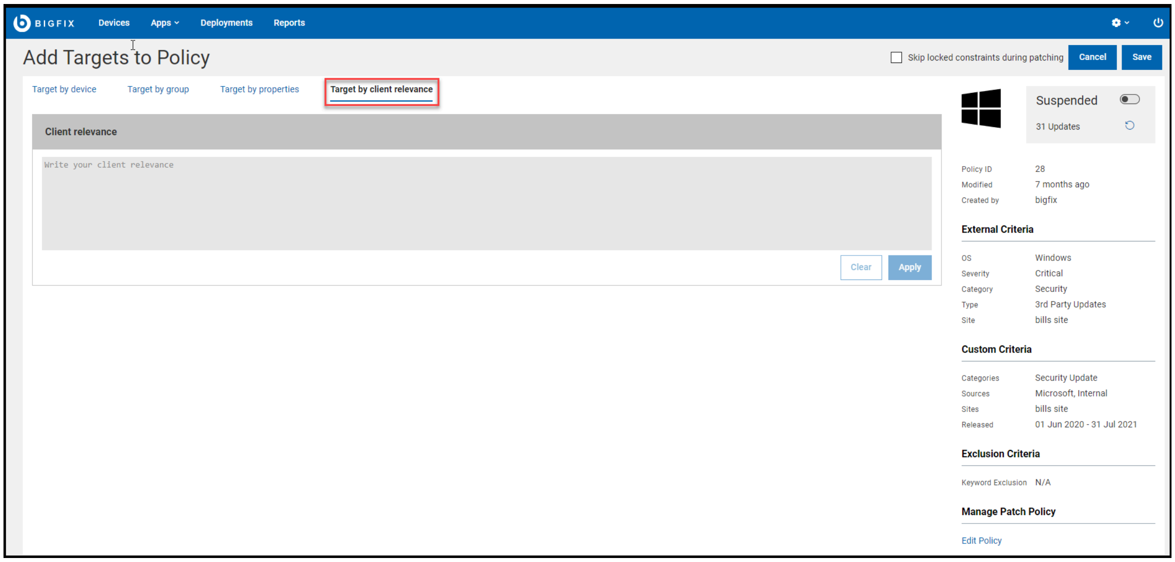
Exclusion Criteria

Keyword Exclusion N/A

Manage Patch Policy

With **Target by properties**, you can define the required condition of the endpoints you intend to target. **Target by properties** is limited to one operator per schedule. For that schedule, the policy will only be issued to the endpoints owned by that operator.

With **Target by client relevance**, you can write your custom relevance that determines the Policy's targets. For example, you can check the versions of specific files. The policy actions will be dynamically targeted. Note that you cannot choose multiple targeting methods at the same time. **Target by client relevance** is limited to one operator per schedule. For that schedule, the policy will only be issued to the endpoints owned by that operator.



Policy ID 28
Modified 7 months ago
Created by bigfix

External Criteria

OS	Windows
Severity	Critical
Category	Security
Type	3rd Party Updates
Site	bills site

Custom Criteria

Categories	Security Update
Sources	Microsoft, Internal
Sites	bills site
Released	01 Jun 2020 - 31 Jul 2021

Exclusion Criteria

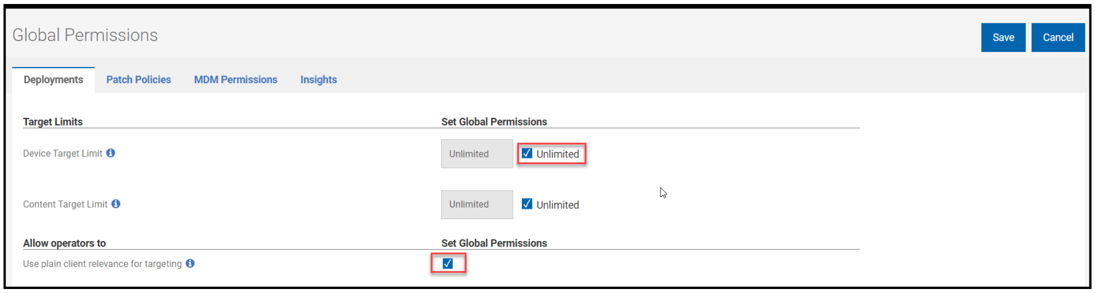
Keyword Exclusion N/A

Manage Patch Policy

If a NMO sets the **Target by properties** or **Target by client relevance** for a given schedule, then only the following operators can edit or change the targeting methods to **Target by device** or **Target by groups**:

- The original NMO who had set **Target by properties** or **Target by client relevance**.
- Master operator (MO).

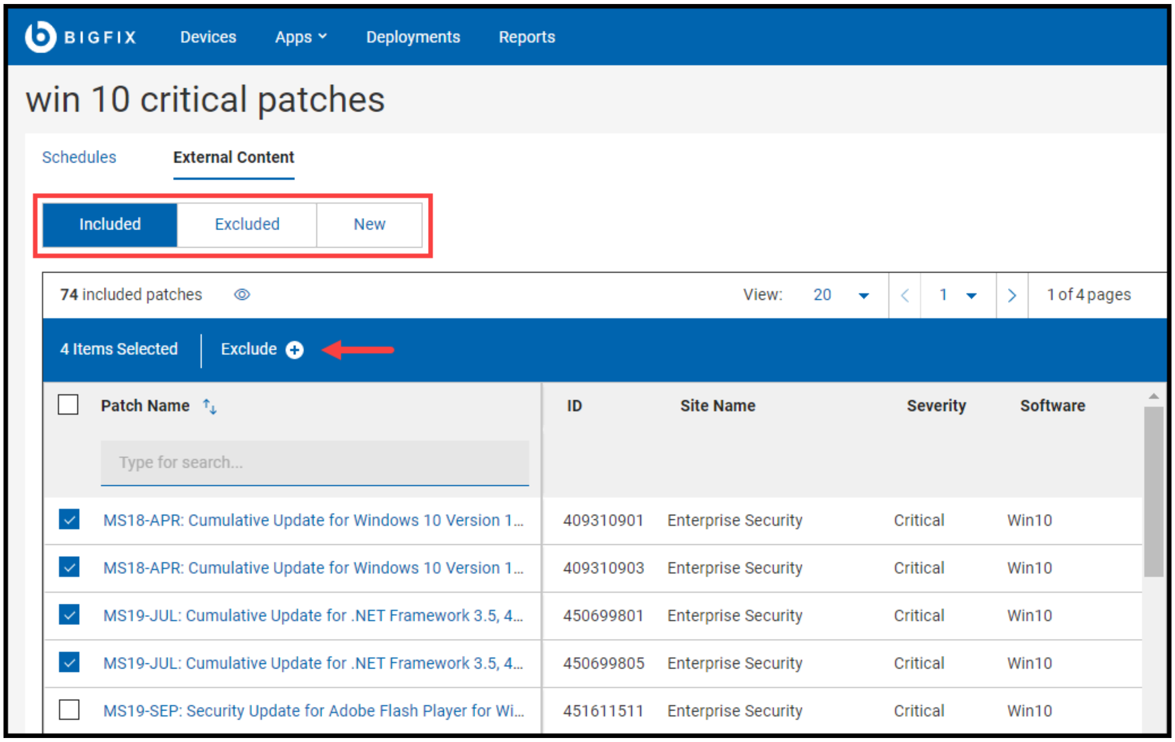
Note: The **Target by properties** or **Target by client relevance** tab will only appear for NMOs whose Device Target Limit permission is set to **Unlimited**. NMOs must click the **Use plain client relevance for targeting** to see the **Target by client relevance** tab. For more information on permissions, see The WebUI Permissions Service.



Target Limits	Set Global Permissions
Device Target Limit	Unlimited ☑ Unlimited
Content Target Limit	Unlimited ☑ Unlimited

Allow operators to	Set Global Permissions
Use plain client relevance for targeting	☑

15. Click **Save** to save targets and return to the Policy document.
16. Click **Content** (External/Custom) tab to Include, Exclude and add New patches in the policy.



win 10 critical patches

74 included patches

	Patch Name	ID	Site Name	Severity	Software
☑	MS18-APR: Cumulative Update for Windows 10 Version 1...	409310901	Enterprise Security	Critical	Win10
☑	MS18-APR: Cumulative Update for Windows 10 Version 1...	409310903	Enterprise Security	Critical	Win10
☑	MS19-JUL: Cumulative Update for .NET Framework 3.5, 4...	450699801	Enterprise Security	Critical	Win10
☑	MS19-JUL: Cumulative Update for .NET Framework 3.5, 4...	450699805	Enterprise Security	Critical	Win10
□	MS19-SEP: Security Update for Adobe Flash Player for Wi...	451611511	Enterprise Security	Critical	Win10

a. Select the patches that you want to exclude.
b. Click **Exclude**.

17. When you are ready, click the **Activate** toggle button to activate the policy and commence patching. Activating a policy activates each of its schedules. Suspend an active policy at any time to halt patch deployment. Click **Refresh Policy** icon to refresh the policy.
To monitor policy-based patching activity, use the WebUI's Deployment views *(on page 146)*

Note:

If you have specified Client Time in your policy schedule, the policy start time will be the specified client time in UTC+14 time zone after activating the policy. This is to ensure that clients in all time zones will be receiving the policy at the specified time.

In WebUI, the start time will be displayed in browser time, after the policy is activated.

- Client time = The time on the endpoint receiving the policy.
- Browser time = The time on the machine on which the browser resides.

The following calculation can be used to convert from UTC+14 time to your browser's time:

- Start_time (in browser time) = <specified_client_time> - 14 hrs + <utc_hour_offset_for_browser_timezone> hrs

Example

You have specified a Client Time of 5 A.M., because you want the policy to be executed at 5 A.M. in each endpoint's timezone, that is 5 A.M. PST, 5 A.M. EST, 5 A.M. IST, etc. This means the policy action will be issued at 5 A.M. in the UTC+14 time zone but the policy will not execute on a client endpoint until it is 5 A.M. in the client's local time.

Consider your browser is in Pacific Daylight Time (PDT). PDT is UTC-7, therefore the UTC offset here is -7.

Start time in PDT = 5 A.M. – 14 hours + (-7 hours) = 5 A.M. – 21 hours = 8 A.M. PDT.

Now let us consider that your browser is in Indian Standard Time (IST). IST is UTC+5:30 so the UTC offset here is +5:30.

Start time in IST = 5 A.M. – 14 hours + (5:30 hours) = 5 A.M. – 8:30 hours = 20:30 IST or 8:30 P.M. IST.

Note: If pre-caching is selected, the policy issue time is offset by the amount of time specified in the pre-cache section.

For example, if you opted to set pre-caching to 1 hour before patching begins, the action will be issued at 7:30 P.M. IST rather than 8:30 P.M. IST.

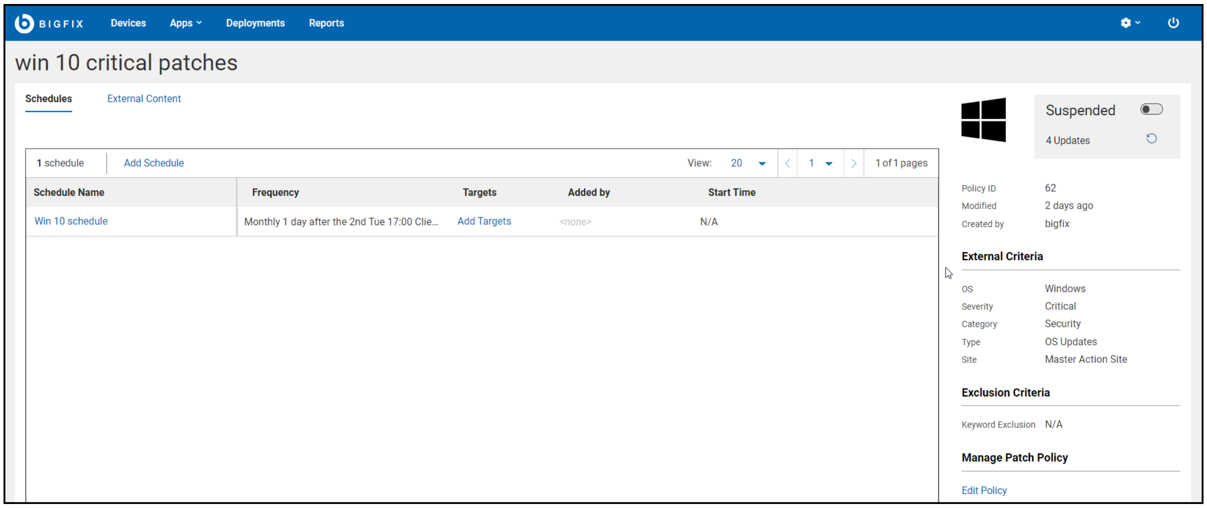
Patch Policy Document

Use the Patch Policy Document to view and manage policy settings. Policy information appears on the right side of the page.

- Status – Active or Suspended.
- Updates – Number of patch updates available.
- Policy ID – Unique identifier for this policy.
- OS, Severity, Category, Type – Inclusion criteria.
- Site - Name of the site where the policy is stored.
- Next Refresh (Active policies) – Time of next auto-refresh, if enabled.
- Modified – Time when the policy was last changed.
- Source: Operator name.
- Refreshed - Date of last policy refresh.
- Keyword Exclusion - Contents with the keyword in the title will be excluded.

Schedules Tab

The Schedules tab displays a list of policy schedules in the order of creation. Click a schedule name to display it's summary page.



win 10 critical patches

Schedules | External Content

1 schedule | Add Schedule | View: 20 | 1 | 1 of 1 pages

Schedule Name	Frequency	Targets	Added by	Start Time
Win 10 schedule	Monthly 1 day after the 2nd Tue 17:00 Clie...	Add Targets	<none>	N/A

Suspended

4 Updates

Policy ID	62
Modified	2 days ago
Created by	bigfix

External Criteria

OS	Windows
Severity	Critical
Category	Security
Type	OS Updates
Site	Master Action Site

Exclusion Criteria

Keyword Exclusion	N/A

Manage Patch Policy

Edit Policy

- Name – Schedule name.
- Frequency – Deployment interval.
- Targets – Number of targeted devices or computer groups. Click the link to display the target list. The **Add Targets** control appears when a schedule has no targets; click the link to add them.
- Added by – This column represents the operators who had added targets to the schedule and in the case of Target By Property It is the operator who had set the condition.
- Next Deployment – The time the schedule's Multiple Action Groups is issued to the BigFix root server. It is subsequently adjusted to accommodate endpoints in all time zones, ensuring the policy executes at the correct time in each location.

Use the toggle switch in the right side panel to **Activate/Suspend** a policy. You cannot refresh or edit an active policy. Some Schedules tab controls are inactive until the policy is Suspended.

Schedules Tab controls:

- **Add Schedule**
- **Activate/Suspend**
- **Refresh Policy**
- **Edit Policy**
- **Delete**

Note: Non-master operators (NMOs) need Activate/Suspend Policy permission to activate or suspend the policy and they need Refresh Policy permission to refresh the policy. For more information on permissions, see The WebUI Permissions Service. NMOs also need write access to the site where the policy is stored to activate/suspend or refresh the policy.

Schedule Summary Page

Click a schedule to display the Schedule summary and its controls. To change the schedule you must suspend its policy. This is not required when adding or removing targets.

- Pre-cache Downloads – The time when policy patches are pre-cached.
- Stagger Start Time – Amount of time to stagger patching time to reduce network load.
- Bypass Errors – Ignore Multiple Action Group (MAG) failures and proceed to the next action. For more information about patch policies and MAG processing, see Monitoring Deployed Policies *(on page 73)*.
- Retry on Failure – number of times to retry if a patch fails to install, and the retry interval.
- Force Restart – Force a restart on completion, and the interval to wait before restarting.

Schedule Summary controls:

- **Add/Edit Targets**
- **Edit Schedule**
- **Delete**

Content (Custom/External) Tab

Displays patches for the selected policy. Patches used for auditing, corrupt patches, and patches with no default action are not included in patch policies. Superseded patches are flagged but not deployed; they will be removed from the patches list once the policy has been refreshed.

To exclude individual patches from the policy, check the **Exclude** box to the left of the title. A device that has been targeted using a computer group (either a manual or dynamic group), cannot be individually excluded.

Filters:

- Included – displays included patches.
- Excluded – displays excluded patches, including both dynamic and manual exclusions.
- New – displays patches that will be added to the policy once it is refreshed.
- Applicable Patches – lists patches associated with the devices the logged in user has permission to operate on. For example, suppose a NMO is authorized to patch Windows machines, but not Linux machines. When viewing a policy that includes both Windows and Linux patches:
    - When the Applicable patches box is checked the NMO will see only Windows patches.
    - When the Applicable box is clear the NMO will see both Windows and Linux patches.
    - Master Operators (MOs), with unlimited permissions, will see the same patches whether the **Applicable Patches** filter is selected or not.

Content (Custom/External) Tab controls:

- **Activate/Suspend**
- **Refresh Policy**

- **Edit Policy**
- **Delete**

Note: Buttons in the policy document appears only when the respective permissions are granted to the NMOs.

Monitoring Deployed Policies

Use the WebUI’s Deployment (on page 146) views to monitor policy-based patching activity.

Working with Multiple Action Groups

A policy is a package of Fixlets and schedules. At the time indicated by the schedule, all patches meeting policy criteria are collected to create a BigFix Multiple Action Group (MAG). If a patch is not relevant on a particular device, no individual action is taken.

A single policy may contain hundreds of patches, and its MAG may contain hundreds of components. To improve performance, when the number of patches in a policy exceeds 200 it is divided into Multiple Action Groups.

Default behavior of a Multiple Action Group (MAG):

- Staggers deployment start time over the course of an hour to reduce network load.
- Retries three times with a one hour interval on each try.
- Uses default action.
- Expires in 2 days (48 hours).
- The targeting method depends on the target type, whether it is: a) a static endpoint, b) a manual computer group, or c) an automatic computer group.

Patch Policy Operations: Task Reference

The Patch Policy operations are summarized in this page. If you suspend an Active policy to make changes, re-activate it when you are done to resume patching.

Add a Policy (on page 74)

Activate a Policy (on page 74)

Suspend a Policy (on page 74)

Refresh a Policy (on page 74)

Edit a Policy (on page 75)

Add a Schedule to a Policy (on page 75)

Edit a Policy Schedule (on page 75)

Add Targets to a Schedule (on page 75)

Add a Policy

1. On the Policy List, click **Add Policy**.
2. Enter a policy name and description.
3. Select a site from the drop-down.
4. Select policy inclusion criteria: Severity, Category, OS, and Content Type.
5. Add dynamic exclusions and set Auto-refresh options, as required. Click **Save**.
6. On the policy document, click **Add Schedule**.
7. Enter a schedule name. Select options for deployment frequency, behavior, and offer. Click **Save**.
8. On the policy document, click the **Add Targets** link for the new schedule.
9. Make sure you have operator visible in **Added by**.
10. Select patching targets from the **Target By Device** or **Target By Group** or **Target by properties** or **Target by client relevance** tab. Click **Save**.
11. On the policy document, Click **Activate** toggle button.

Activate a Policy

1. From the Policy List, open the policy document.
2. Click the **Activate** toggle button.

Suspend a Policy

1. From the Policy List, open the policy document.
2. Click the **Suspend** toggle button.

Refresh a Policy

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click the **Refresh Now** icon.

Edit a Policy

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click the **Edit Policy** link.
4. Make required changes, and click **Save**.

Delete a Policy

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click the **Edit Policy** link.
4. Click **Delete**.

Add a Schedule to a Policy

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click **Add Schedule**.
4. Enter a schedule name, and set scheduling and execution options. Click **Save**.
5. Click the schedule's **Add Targets** link.
6. On the **Target By Device** or **Target By Group** or **Target by properties** or **Target by client relevance** tab, select devices or groups to add. Click **Save**.

Edit a Policy Schedule

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click the schedule name.
4. Click **Edit Schedule**.
5. Make changes and click **Save**.

Add Targets to a Schedule

1. From the Policy List, open the policy document.
2. Click the schedule's Targets link.
3. On the **Target By Device** or **Target By Group** or **Target by properties** or **Target by client relevance** tab, select devices or groups to add. Click **Save**.

Remove Targets from a Schedule

1. From the Policy List, open the policy document.
2. Click the schedule's Targets link.
3. On the **Target By Device** or **Target By Group** or **Target by properties** or **Target by client relevance** tab, select devices or groups to remove. Click **Save**.

Delete a Policy Schedule

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Remove all target devices or groups.
    a. Click the schedule's Targets link.
    b. On the **Target By Device** or **Target By Group** or **Target by properties** or **Target by client relevance** tab, click **Deselect All**. Click **Save**.
4. On the Schedules tab, click the **schedule**.
5. Click **Edit Schedule**.
6. Click **Delete**.

Exclude Individual Patches from a Policy (Manual Exclusions)

1. From the Policy List, open the policy document.
2. If the policy is active, click the **Suspend** toggle button.
3. Click **Content** tab.
4. Click **Included** and select the patches you want to exclude.
5. Click **Exclude** button.

Exclude Patch Types from a Policy (Dynamic Exclusions)

1. From the Policy List, open the policy document.
2. If the policy is active, click **Suspend** toggle button.
3. Click **Edit Policy**.
4. Type a keyword or phrase in the **Exclude** field and press **Enter**; repeat as required. Exclusions keywords are not case-sensitive.
5. Click **Save**.

Enable Auto-refresh

1. From the Policy List, open the policy document.
2. If the policy is active, click **Suspend** toggle button.
3. Click **Edit Policy**.
4. Click **Enable auto-refresh** toggle button, and set refresh timing and frequency.
5. Click **Save**.

Adjust Auto-refresh Schedule

1. From the Policy List, open the policy document.
2. If the policy is active, click **Suspend** toggle button.
3. Click **Edit Policy**.
4. Adjust Auto-refresh timing and frequency.
5. Click **Save**.

Disable Auto-refresh

1. From the Policy List, open the policy document.
2. If the policy is active, click **Suspend** button.
3. Click **Edit Policy**.
4. Click **Disable auto-refresh**.
5. Click **Save**.

Chapter 6. Get started with IVR

Use the **Insights for Vulnerability Remediation** (IVR) application to view a list of all the vulnerabilities, remediate vulnerabilities and create customized IVR reports.

Before you start with WebUI IVR, ensure that your environment meets below prerequisites:

- IVR schema in place
- The minimum version of IVR schema is 1.4
- IVR dataflow run and data correlated to Insights exists
- Insights ETL run

IVR List

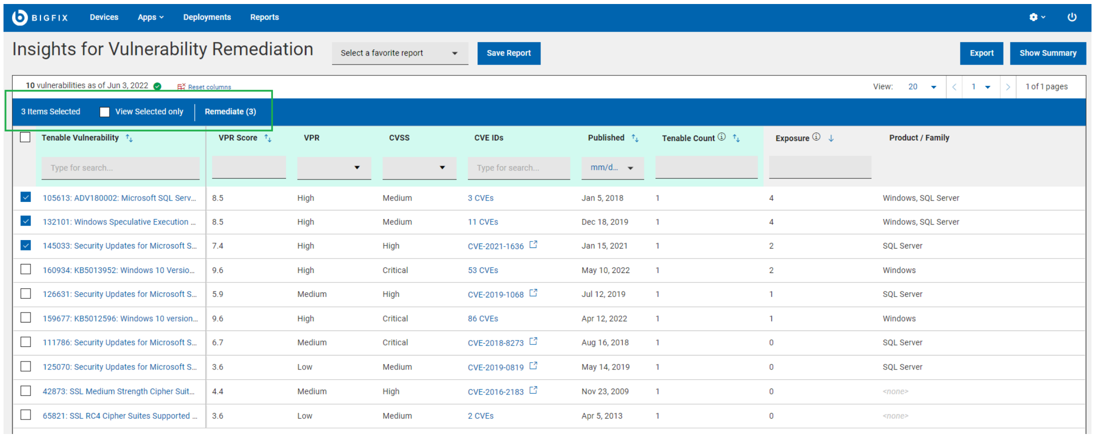
The BigFix Insights for Vulnerability Remediation (IVR) application in the WebUI provides a quick summary of all vulnerabilities in a data grid format. With the application you can remediate vulnerabilities and create custom IVR reports.

To access the **IVR** page, from the WebUI main page, click **Apps > IVR**.

Operator permission settings, connected devices, and site assignments govern the content in the list. With the grid view, you can view the list of vulnerabilities in a table. Click the vulnerability name to navigate to the details of the vulnerability (the overview, vulnerable devices, and deployment). Each column gives an option to search or filter.

The refine results and customizing the data grid function is similar to those in the device page. For more information, see Grid view (on page 12).

Figure 1. IVR App - Overview

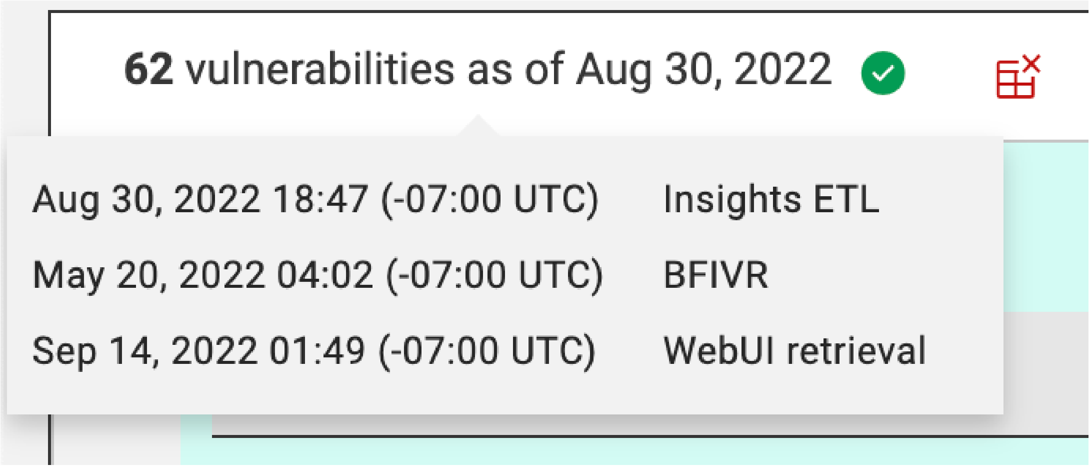


Insights for Vulnerability Remediation

10 vulnerabilities as of Jun 3, 2022

	Tenable Vulnerability	VPR Score	VPR	CVSS	CVE IDs	Published	Tenable Count	Exposure	Product / Family
☑	105613: ADV180002: Microsoft SQL Serv...	8.5	High	Medium	3 CVEs	Jan 5, 2018	1	4	Windows, SQL Server
☑	132101: Windows Speculative Execution ...	8.5	High	Medium	11 CVEs	Dec 18, 2019	1	4	Windows, SQL Server
☑	145033: Security Updates for Microsoft S...	7.4	High	High	CVE-2021-1636	Jan 15, 2021	1	2	SQL Server
□	160934: KB5013952: Windows 10 Versio...	9.6	High	Critical	53 CVEs	May 10, 2022	1	2	Windows
□	126631: Security Updates for Microsoft S...	5.9	Medium	High	CVE-2019-1068	Jul 12, 2019	1	1	SQL Server
□	159677: KB5012596: Windows 10 version...	9.6	High	Critical	86 CVEs	Apr 12, 2022	1	1	Windows
□	111786: Security Updates for Microsoft S...	6.7	Medium	Critical	CVE-2018-8273	Aug 16, 2018	1	0	SQL Server
□	125070: Security Updates for Microsoft S...	3.6	Low	Medium	CVE-2019-0819	May 14, 2019	1	0	SQL Server
□	42873: SSL Medium Strength Cipher Suit...	4.4	Medium	High	CVE-2016-2183	Nov 23, 2009	1	0	<none>
□	65821: SSL RC4 Cipher Suites Supported ...	3.6	Low	Medium	2 CVEs	Apr 5, 2013	1	0	<none>

Hover the mouse over the vulnerability list count to see the dates and times updated upon the most recent **WebUI retrieval**.



62 vulnerabilities as of Aug 30, 2022

Aug 30, 2022 18:47 (-07:00 UTC)	Insights ETL
May 20, 2022 04:02 (-07:00 UTC)	BFIVR
Sep 14, 2022 01:49 (-07:00 UTC)	WebUI retrieval

The date in the vulnerability list count indicates the **Insights ETL** or **BFIVR** date, depending on which is the most recent. It is recommended to have Insights ETL run to completion first and then run an IVR ETL for the most up to date information.

- **Insights ETL** is the time of the most recent and successful completion of an **Insights ETL**. These are determined by the schedules that are setup under Insights. Refer to the link for more information about how to schedule an **Insights ETL**.
- **BFIVR** is the time of the most recent and successful completion of an **IVR ETL**. These are determined by the schedules that are setup upon deployment of the **IVR**. Refer to the link for more information about **IVR ETL** scheduling.
- **WebUI retrieval** is the time of the most recent retrieval of **IVR** data from the broker. By default, WebUI will attempt to pull data daily via the IVR broker. Refer to the link to view IVR settings that can change the frequency of this retrieval. This is also when WebUI updates the **Insights ETL** and **BFIVR** times with the latest metrics.

The IVR App contains the following elements:

- **Action bar:** Select one or more vulnerabilities from the data grid to enable the action bar.
  - **View Selected only:** Select the checkbox to view only the selected vulnerability.
  - **Remediate:** Click **Remediate** to navigate to the **Take Action dialog**, where you can remediate the vulnerability. The number in the parenthesis indicates the number of selected vulnerabilities. For more information, see Take Action: The Deploy Sequence *(on page 129)*.

- **Filters**

Note: Filters in the IVR grid view are presented in green and gray. Green means that information comes from Qualys/Tenable. Gray means that information comes from BigFix Enterprise (BFE) database.

You can use filters in the headers to refine results:

- ◦ **VPR Score**: Vulnerability priority rating score.
- ◦ **VPR**: Vulnerability priority rating.
- ◦ **CVSS**: Common vlnerability scoring system.
- ◦ **CVE IDs**: Use the CVE ID filter to search vulnerabilities by Common Vulnerabilities and Exposures.
- ◦ **Published**: Published date.
- ◦ **Scanner Count**: Tenable/Qualys count - shows the number of vulnerable devices that Tenable/Qualys identified with correlated BigFix content.

Note: Under 2 conditions the grid can show a vulnerability:

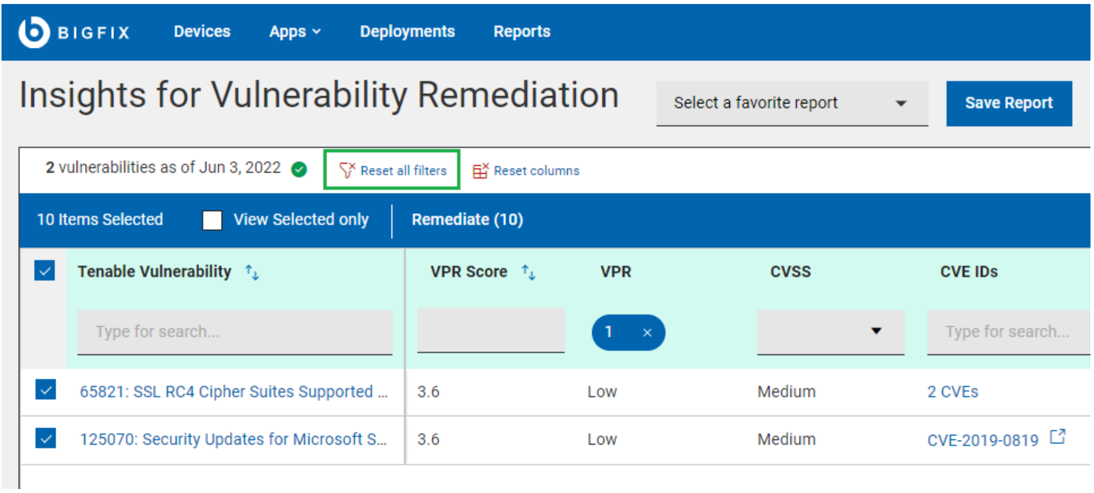
- ▪ The scanner count must be greater than 0
- ▪ The operator must have permission to view to at least one of the fixlets that are associated with that vulnerability

- ◦ **Exposure count**: The aggregate sum of applicable devices for the associated BigFix content.

Note: Exposure count is not a unique count. It is a summation of all applicable devices per Fixlet.

- ◦ **Product/Family**

To clear all the selected filters, click **Reset all filters**.



Insights for Vulnerability Remediation

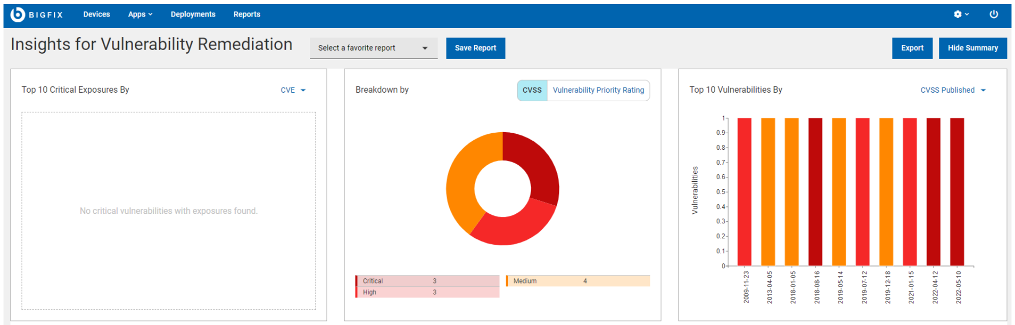
2 vulnerabilities as of Jun 3, 2022

☑	Tenable Vulnerability	VPR Score	VPR	CVSS	CVE IDs
☑	65821: SSL RC4 Cipher Suites Supported ...	3.6	Low	Medium	2 CVEs
☑	125070: Security Updates for Microsoft S...	3.6	Low	Medium	CVE-2019-0819

- **Save Report**
  - ◦ Save the report for reference, edit, update, or delete. For more information, see Reports *(on page 20)*.
- **Show Summary:**
  1. On the **IVR** page, select the required filters.
  2. Click **Show Summary**. You can view the summary of all the filtered vulnerabilities as charts and tables. Hover over of the chart to get more details about a data point and the percentages. Hover over any

truncated labels to see the full text in the tooltip. You can change filters or enter search text and the report dynamically displays the relevant information.

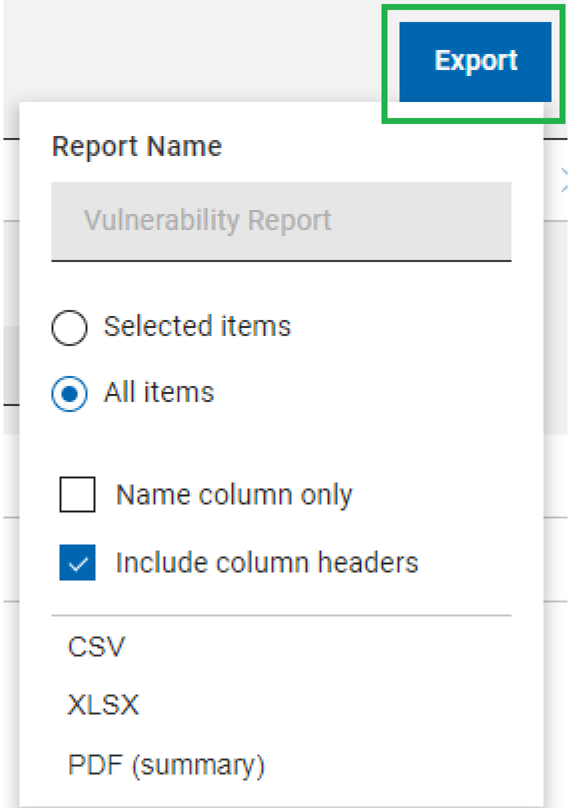
- **Top 10 Critical Exposures by CVE/Vulnerability ID**
- **Breakdown by CVSS/Vulnerability Priority Rating**
- **Top 10 Vulnerabilities by CVSS Published Date/Vulnerability Priority Rating Published Date**



- **Export:**

You can export the filtered report in a `.csv`, `.xlsx`, or `.pdf` format.

1. On the **IVR** page, select the required filters.
2. Click **Export**.



Report Name

Vulnerability Report

○ Selected items

● All items

□ Name column only

☑ Include column headers

CSV

XLSX

PDF (summary)

3. Use the **Selected Items** option to choose items from the filtered result to export; Click **All Items** to export all the items from the filtered list.
4. To export only the names of the filtered items, click **Name column only**
5. To export details of every default column of an item, click **Include column headers**

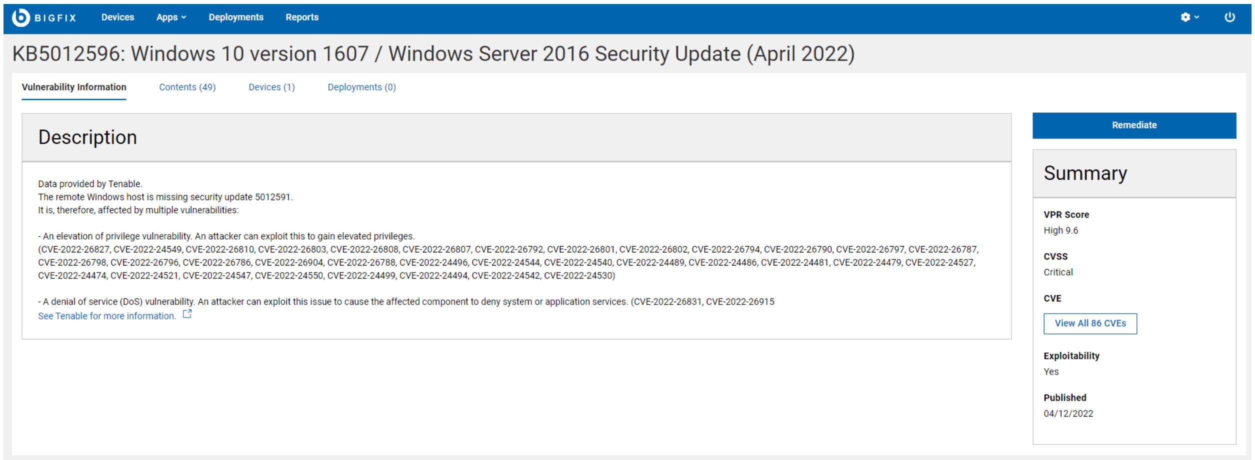
> **Note:** If you are displaying columns other than the default columns, you can export the name column only.

6. Select a file format (CSV, XLSX, or PDF) for exporting the data.

    - By default, the report is saved in the `Downloads` folder with this default file name: `Device_Report_mm_dd_yyyy_username`. You can change the download settings in your browser to change the file name and download it into a different location. You can save the report to review it later or share it with interested stakeholders.
    - If you selected PDF format, a `.zip` file is downloaded, which contains a `.csv` file with numerical data and a `.pdf` file with a visual representation of the data.
    - The exported IVR report contains key details about your vulnerabilities that are displayed after applying the filters and search criteria. The details include the vulnerability name, number of vulnerable devices, severity, CVE IDs and all other details that you can see on the screen when you expand every vulnerability.

IVR document

With the BigFix Insights for Vulnerability Remediation (BFIVR) document you can see the description of the vulnerability, vulnerable devices, and deployment history details. Drill further into vulnerability details by using the links to associated views.



KB5012596: Windows 10 version 1607 / Windows Server 2016 Security Update (April 2022)

Description

Data provided by Tenable.
The remote Windows host is missing security update 5012591.
It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.
(CVE-2022-26827, CVE-2022-24549, CVE-2022-26810, CVE-2022-26803, CVE-2022-26808, CVE-2022-26807, CVE-2022-26792, CVE-2022-26801, CVE-2022-26802, CVE-2022-26794, CVE-2022-26790, CVE-2022-26797, CVE-2022-26787, CVE-2022-26798, CVE-2022-26796, CVE-2022-26786, CVE-2022-26904, CVE-2022-26788, CVE-2022-24496, CVE-2022-24544, CVE-2022-24540, CVE-2022-24489, CVE-2022-24486, CVE-2022-24481, CVE-2022-24479, CVE-2022-24527, CVE-2022-24474, CVE-2022-24521, CVE-2022-24547, CVE-2022-24550, CVE-2022-24499, CVE-2022-24494, CVE-2022-24542, CVE-2022-24530)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-26831, CVE-2022-26915
See Tenable for more information.

Summary

VPR Score
High 9.6

CVSS
Critical

CVE

Exploitability
Yes

Published
04/12/2022

The IVR document includes following views:

- Vulnerability Information – Detailed description of the vulnerability and vendor links
- Contents – List of fixlets associated with the selected vulnerability
- Devices – List of relevant devices for targeting
- Deployments - IVR deployment history

Summary views:

- VPR Score
- CVSS
- CVE
- Exploitability
- Published

Useful links:

Take action: The Deploy Sequence (on page 129)

WebUI IVR Settings

Check the list of BigFix Insights for Vulnerability Remediation (BFIVR) available settings you can change in a configuration file.

Setting name	Default value	Description
`_WebUIAppEnv_INSIGHTS_CONFIG_PATH`	<BigFix Enterprise Path>\BES WebUI\WebUI\insights_db_connection_config.txt	The full path for the configuration file that the broker requires to connect to Insights. This file is automatically created at this location.
`_WebUIAppEnv_INSIGHT_BROKER_PORT`	52318	The port for the broker to listen on.
`_WebUIAppEnv_INSIGHT_BROKER_LOGGING_LEVEL`	Info	You can set up default "Info" to use for debugging and troubleshooting.
`_WebUIAppEnv_INSIGHTS_BROKER_CAPTURE_STDERR`	0	Capture debug logs.
`_WebUIAppEnv_IVR_CACHE_REFRESH_TIME`	Default is 24 hours. Minimum: 5 minutes. Value is in milliseconds.	How often WebUI retrieves data from the IVR broker.
`_WebUIAppEnv_IVR_UPSERT_MAX_TIME`	Default is 1 hour. Minimum: 5 minutes. Value is in milliseconds.	The maximmum time a request to the IVR broker can take during the WebUI retrieval from the IVR broker process.

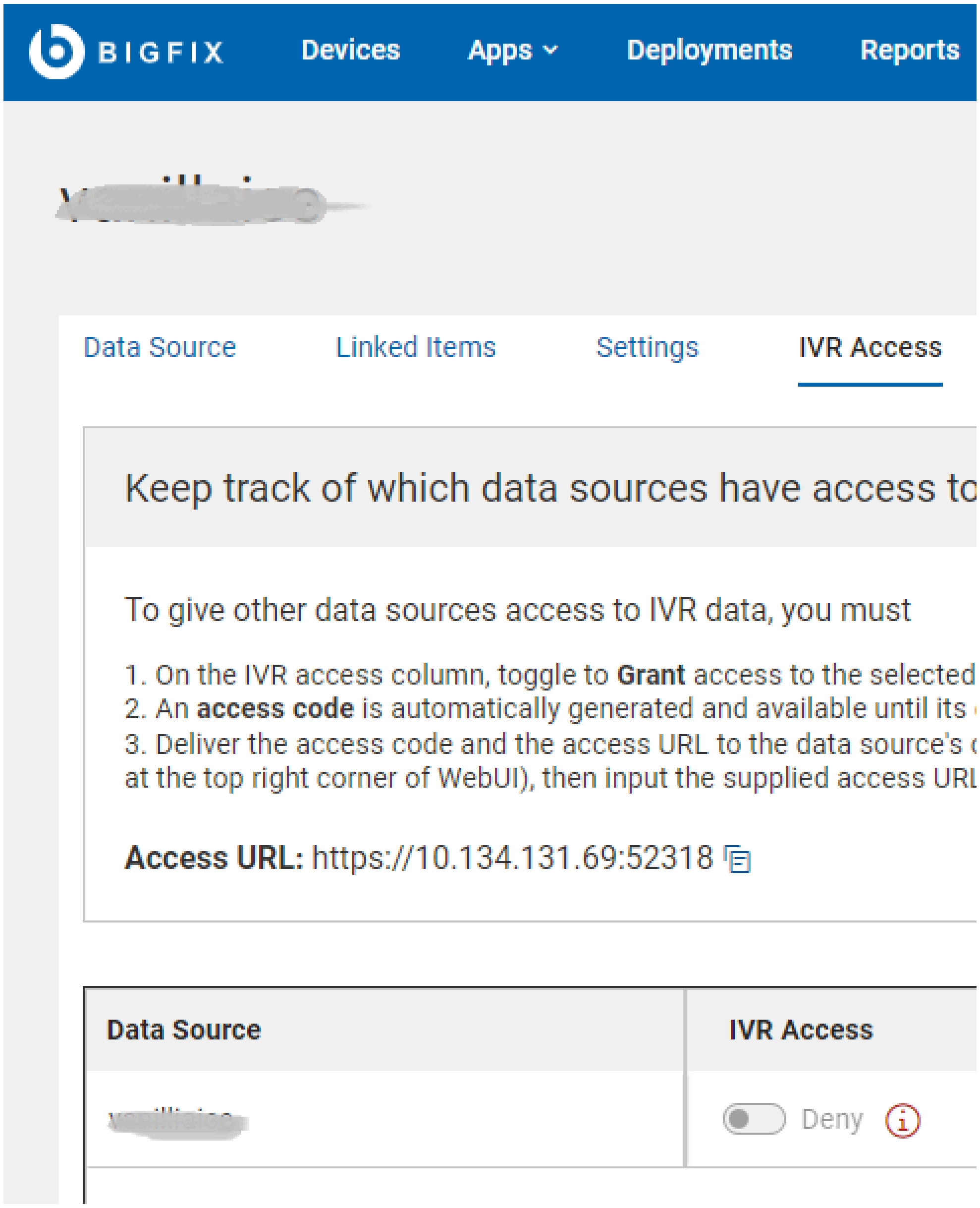
Setting name	Default value	Description
`_WebUIAppEnv_-IVR_MEM_THRESHOLD`	Default and min value is 4000 MB ~ 4 GB	The memory threshold at which IVR restarts - specified in MB.

Troubleshooting IVR

In many instances,you can troubleshooting various issues that you might encounter in the IVR app.

1. Access was not granted to IVR app.

   Hover over the error icon to see error description.



Keep track of which data sources have access to

To give other data sources access to IVR data, you must

1. On the IVR access column, toggle to **Grant** access to the selected
2. An **access code** is automatically generated and available until its
3. Deliver the access code and the access URL to the data source's at the top right corner of WebUI), then input the supplied access URL

Access URL: https://10.134.131.69:52318

Data Source	IVR Access
[redacted]	Deny

Possible errors:

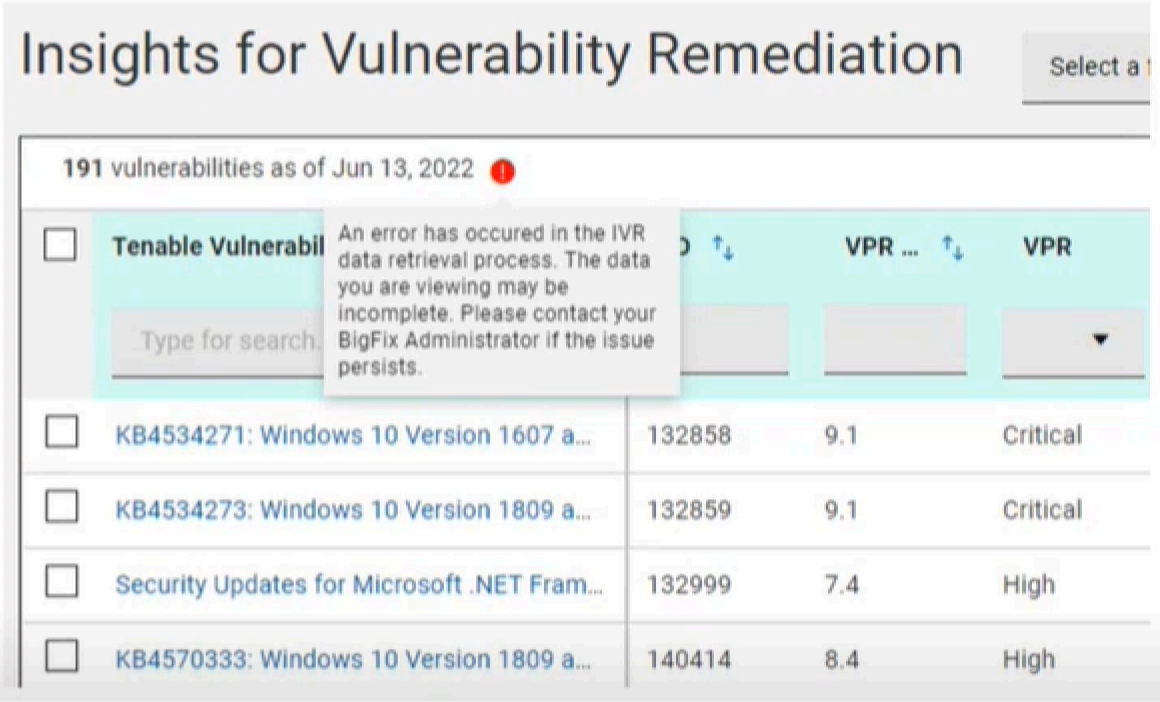
a. Your environment might not meet prerequisites:
   - Ensure that the IVR Schema is in place
   - Ensure that the IVR Dataflow is running (IVR 1.4) and data correlated to Insights exists
   - Ensure that the Insights ETL is running

b. Find whether an error occurred when access was granted/denied

c. Find whether an error occurred during auto-configuration

d. Find whether an error occurred during access code generation

2. An error has occurred in data retrieval process.



Insights for Vulnerability Remediation

191 vulnerabilities as of Jun 13, 2022

An error has occured in the IVR data retrieval process. The data you are viewing may be incomplete. Please contact your BigFix Administrator if the issue persists.

☐	Tenable Vulnerabil		VPR ...	VPR
	Type for search			▾
☐	KB4534271: Windows 10 Version 1607 a...	132858	9.1	Critical
☐	KB4534273: Windows 10 Version 1809 a...	132859	9.1	Critical
☐	Security Updates for Microsoft .NET Fram...	132999	7.4	High
☐	KB4570333: Windows 10 Version 1809 a...	140414	8.4	High

Possible errors:

a. The IVR application didn't connect to insights_broker or access was revoked

b. Check the ivr.log for errors or other information.

c. Check the broker logs on the primary Insights server `<BigFix Enterprise Path>\BES WebUI\WebUI\sites\<WebUI Insights Folder>\insights-app\logs` folder for details regarding an error.

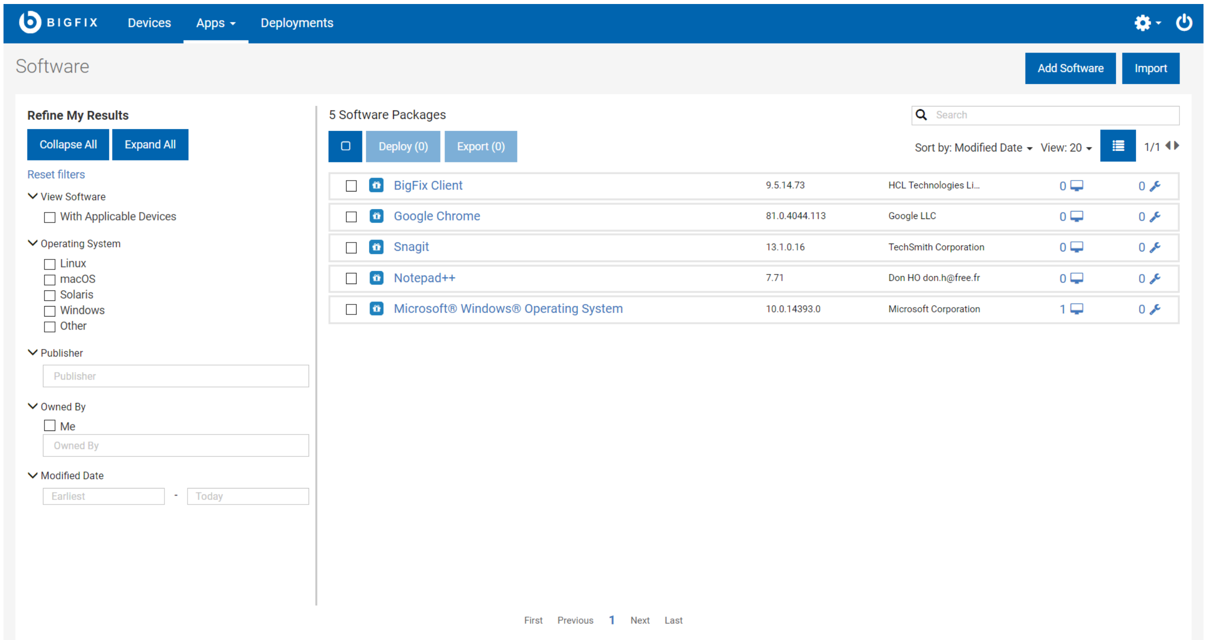
Chapter 7. Get Started with Software

A BigFix software package is the collection of Fixlets used to install software on a device. The package includes the installation files, the Fixlets that install them, and information about the package itself.

Use the Software-related screens to list software packages, find specific software, and view detailed package information.

Use the Software app screens to add, edit, and remove packages from your organization's software catalog. Use the multiple task feature to create packages with more than one action. For example, create a single package that can both install and uninstall a piece of software, or install it multiple ways, using different options.

The Software Package List



5 Software Packages

□ BigFix Client	9.5.14.73	HCL Technologies Li...	0	0
□ Google Chrome	81.0.4044.113	Google LLC	0	0
□ Snagit	13.1.0.16	TechSmith Corporation	0	0
□ Notepad++	7.71	Don HO don.h@free.fr	0	0
□ Microsoft® Windows® Operating System	10.0.14393.0	Microsoft Corporation	1	0

- **List contents reflect the operator's device and site assignments**, and whether a particular package was shared, or marked private by the owner.
- **Add Software to your catalog** with the **Add Software** link. The link does not display if the operator does not have permission to add software.

Use the **Export** and **Import** functions to transfer software packages from one BES server to another. These tools are useful if you are running multiple BigFix deployments or want to make a backup.

- **Export** - Click to export software packages on the BES server as a zip file. The browser will prompt you to specify a directory. Multiple packages selected for export are placed in a single zip file.
- **Import** - Click to import packages created with the **Export** function. Operators who do not have permission to import packages do not see this button.

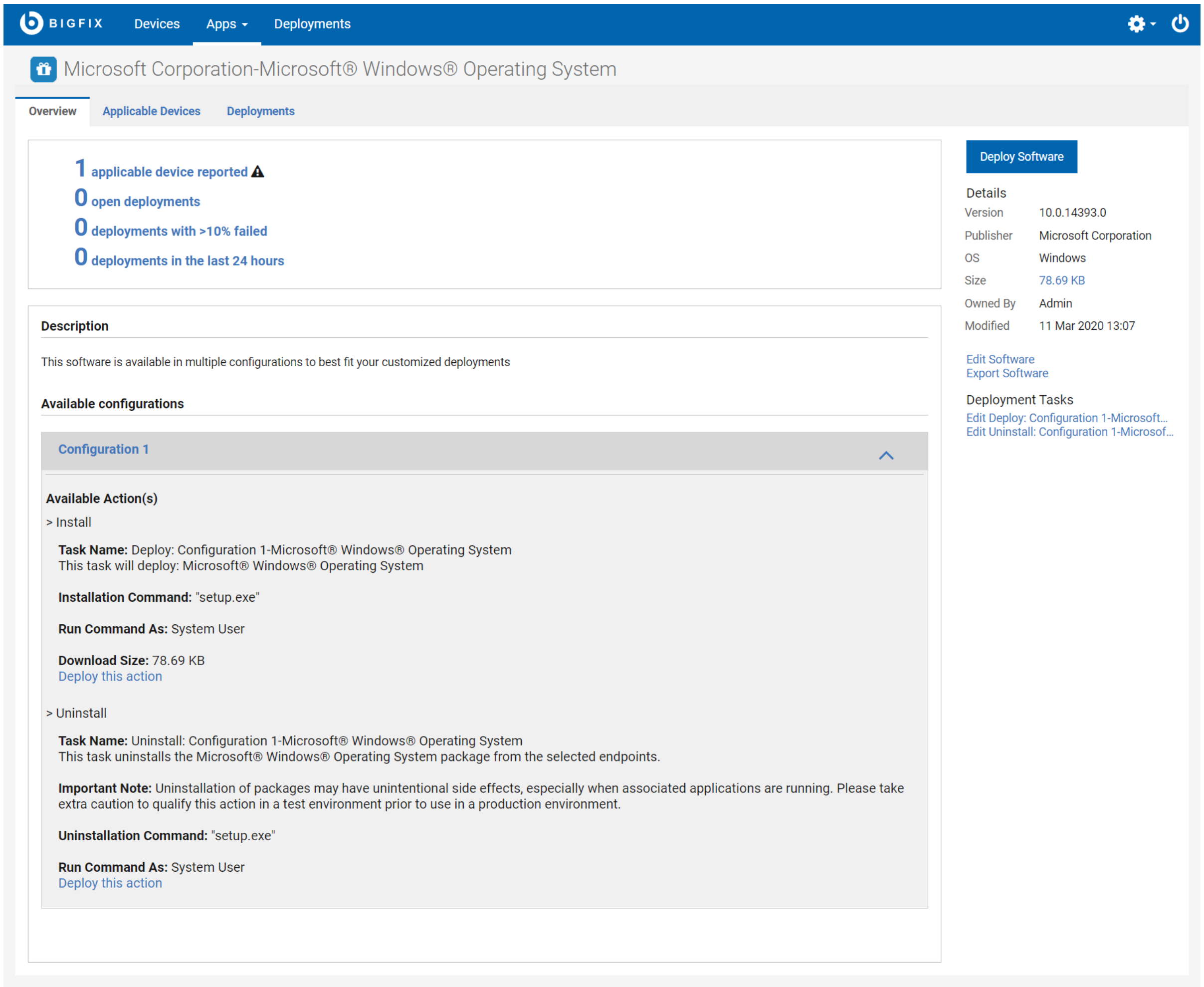
Note: Importing software packages that include text-based files may sometimes fail. The import process can change the file's SHA value and when the SHA validation check fails, the import fails. This is a known BigFix Platform bug.

Software Documents

Click a software package name to see its description, applicable devices, and deployment history. Drill further into package details using the links provided in the sidebar, and associated views.

The Software Document views:

- Overview – Detailed description of software package.
- Applicable Devices – Machines eligible for this software.
- Deployments – Software deployment history.



Microsoft Corporation-Microsoft® Windows® Operating System

1 applicable device reported
0 open deployments
0 deployments with >10% failed
0 deployments in the last 24 hours

Description

This software is available in multiple configurations to best fit your customized deployments

Available configurations

Configuration 1

Available Action(s)

> Install

Task Name: Deploy: Configuration 1-Microsoft® Windows® Operating System
This task will deploy: Microsoft® Windows® Operating System

Installation Command: "setup.exe"

Run Command As: System User

Download Size: 78.69 KB
Deploy this action

> Uninstall

Task Name: Uninstall: Configuration 1-Microsoft® Windows® Operating System
This task uninstalls the Microsoft® Windows® Operating System package from the selected endpoints.

Important Note: Uninstallation of packages may have unintentional side effects, especially when associated applications are running. Please take extra caution to qualify this action in a test environment prior to use in a production environment.

Uninstallation Command: "setup.exe"

Run Command As: System User
Deploy this action

Details

Version	10.0.14393.0
Publisher	Microsoft Corporation
OS	Windows
Size	78.69 KB
Owned By	Admin
Modified	11 Mar 2020 13:07

Edit Software
Export Software

Deployment Tasks
Edit Deploy: Configuration 1-Microsoft...
Edit Uninstall: Configuration 1-Microsof...

- Click **Deploy Software** to deploy the package.
- Edit or remove a software package from your catalog using the **Edit Software** link.
- Export the package using the **Export Software** link.
- Click a deployment task link to edit it. To learn more about task editing see, Editing Custom Content *(on page 98)*.

Software Catalog Operations

This section shows how to add software to your catalog, edit software packages, and delete packages from the catalog.

Note that the permissions used for adding software to the catalog and the permissions used for editing and deleting software are calculated differently.

A single BigFix console setting determines whether or not an operator has permission to add software. Permission to edit and remove software from the catalog is also affected by who owns the software package, whether it was created using the BigFix console or the WebUI, and whether a package created in the WebUI was later modified using the console. If you run into permission issues attempting to edit a software package, talk with your BigFix administrator.

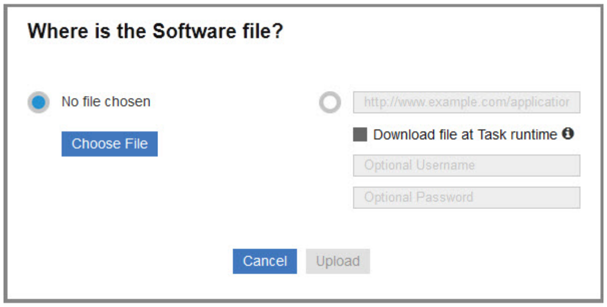
Add a Software Package

To simplify package creation and editing, installation and uninstallation commands are generated automatically for supported file types. Feel free to edit these defaults, or type your own. For unsupported file types, enter the commands you want to use.

- Supported installation file types: .appv, .appx, .bat, dmg, .exe, .msi, .msp, .msu, .pkg (Mac and Solaris), .rpm.
- Supported uninstallation file types: .appv, .msi, .rpm.

Add a Software Package

1. On the **Software Package List** click **Add Software** to open the **Upload Software Package** dialog.

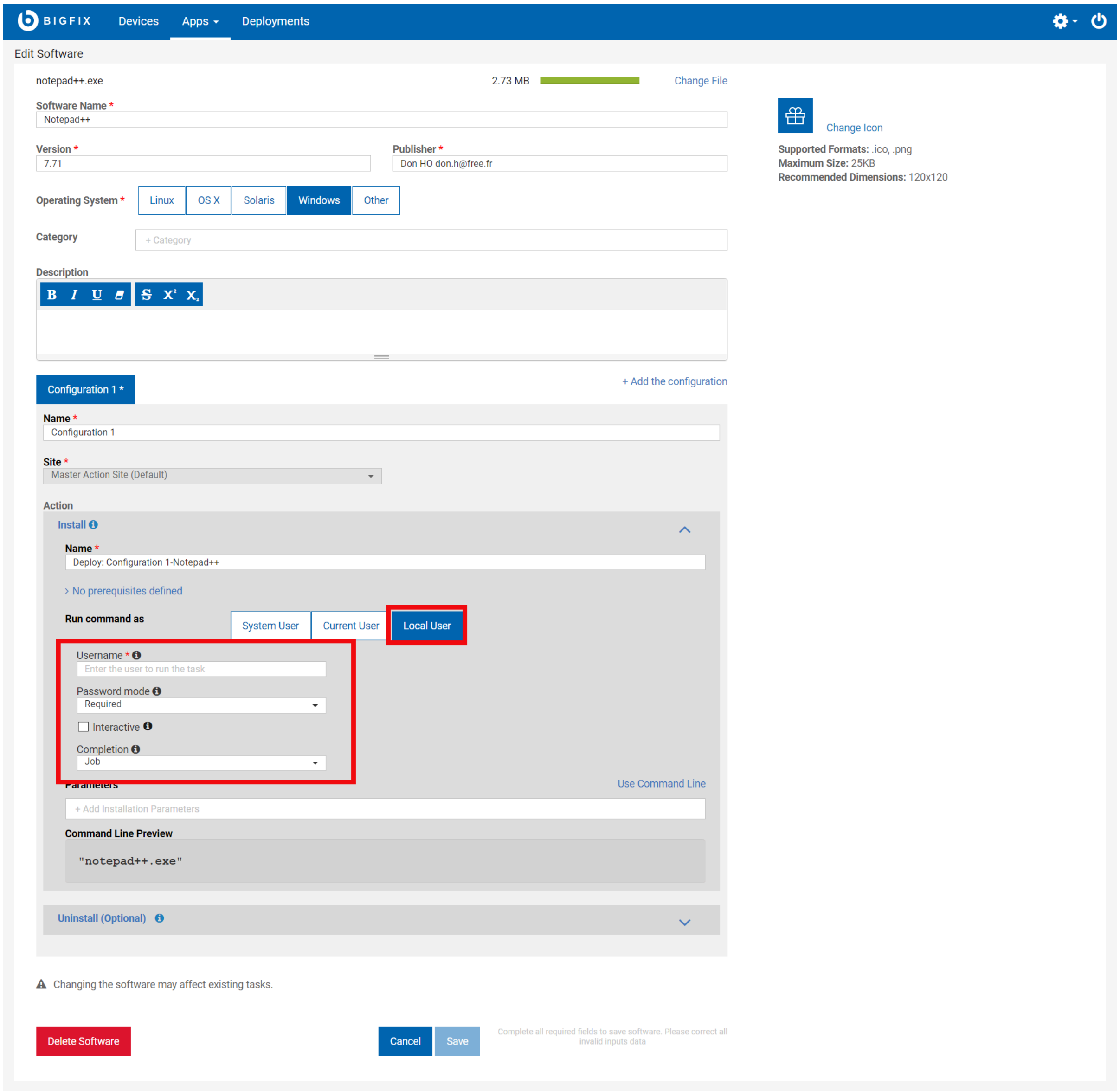

Where is the Software file?
● No file chosen
Choose File
○ http://www.example.com/applicatior
■ Download file at Task runtime ℹ
Optional Username
Optional Password
Cancel
Upload

2. Choose a local file or enter a URL to download a package. Upload the file to place it on the BigFix server, where it will remain until the package is deleted. Check the **Download file at Task runtime** box to have the file cached when the package is deployed, a useful alternative if you do not want to permanently store the file.
3. Click **Upload**.
4. Complete the catalog record. Verify, enter, or select:
    - Software Name
    - Version number
    - Publisher
    - Package Icon - To replace the default icon for the package click **Change icon**, and upload a .ico or .png file.
    - Operating System - Linux, OS X, Solaris, Windows, or Other.
    - Category - Type of software. Select one or more existing categories or type a new category name to create one.
    - Description - Describe the package and any instructions that will aid others responsible for deploying it.
    - Configuration - Configuration in this context includes two operations: Install and Uninstall (optional).

        - To add a configuration:
            a. Click **+ Add the configuration**.
            b. Enter the **Name** of the configuration.
            c. From the **Site** list, select the BigFix site where the Fixlet is stored.
        - To remove the configuration, select the configuration tab you want to remove and click **Delete**. The **Delete** button will be hidden if there is only one configuration tab.
    - On Windows systems, you can run the commands as a System User, Current User, or as a Local User. Commands that are run by BigFix Clients default to System User (On OS X, UNIX, and Linux computers, the software is installed as root). In some cases, you might want to install by using the credentials and local context of the Current User or a Local User. For details on how to set various parameters associated with Local User, see Running deployment commands as a Local User *(on page 90)*.
    - Select from the list of installation parameters provided, or click **Use Command Line** to edit the installation command. Use the **Command Line Preview** to verify that it is correct and complete.
5. Click **Save** to add the package.

Running deployment commands as a Local User

This section explains the various parameters you can configure when you run a command as a local user that is different than the logged-in user.



Edit Software

notepad++.exe 2.73 MB

Software Name *: Notepad++

Version *: 7.71

Publisher *: Don HO don.h@free.fr

Operating System *: Windows

Category: + Category

Description

Supported Formats: .ico, .png
Maximum Size: 25KB
Recommended Dimensions: 120x120

Configuration 1 *

Name *: Configuration 1

Site *: Master Action Site (Default)

Action

Install

Name *: Deploy: Configuration 1-Notepad++

› No prerequisites defined

Run command as: Local User

Username *: Enter the user to run the task

Password mode: Required

□ Interactive

Completion: Job

Parameters: + Add Installation Parameters

Command Line Preview

```
"notepad++.exe"
```

Uninstall (Optional)

Changing the software may affect existing tasks.

Complete all required fields to save software. Please correct all invalid inputs data

- **Username**: Name of a user who is different than the user that is currently logged in, in either of the following formats:
    1. user@domain. Example: "myname@tem.test.com"
    2. domain\user. Example: "TEM\myname"
- **Password mode**: Defines the mode of authentication. The following options are available:
    1. **Required**: The application prompts you to enter a password, and the value you enter is passed on to the agent as a Secure Parameter.
    2. **Impersonate**: The agent searches for a session running for the user specified in **Username** and runs the command in the session of that user.
    3. **System**: The command is run as the local system account. For this option to work, the user specified in **Username** must be logged in to the system when the command is run.

- **Interactive**: Select the checkbox. The command opens the user interface of the user specified in **Username** and runs in that user's session.
- **Target user**: Optional. This option becomes active when you select **Interactive**. The command opens the user interface in the session of the user you specify in this field and runs in that session. The command runs with the primary user privileges, but the target user must be logged in to the system for the command to work.
- **Completion**: specifies whether the command must wait for the process to end.
    1. **None**: The command does not wait for the process to end. The user must be logged in to the system before the command starts running. The `SWD_Download` folder is retained if this option is selected. Deploy the `SWD_Download` folder cleanup Fixlet to clean up the client computer, after the process ends.
    2. **Process**: The command waits for the process to end. This option does not require the specified user to be logged in to the system.
    3. **Job**: The command waits for the process to end. This option expects the process to do its own job control management and does not require the specified user to be logged in to the system.

Enable Uninstallation

Learn how to enable uninstallation option in the software package that you have added.

To enable the option to uninstall:

1. Complete the steps 1 through 4 under Add a Software Package *(on page 89)*
2. In your configuration tab, under **Action**, click **Uninstall** and select **On**.
3. **Run command as**: Select an available option.
    - System User
    - Current User
    - Local User
4. Click **Use Command Line**.

   Automatic: If the server and the client have the same operating systems, the string in the command line is automatically generated. Hence, after you save this configuration and deploy uninstall action in the client machine, uninstallation takes place automatically.

   Manual: If the client has a different operating system than the server (for example, Windows client and Linux server) and that supports two different extension files (for example: *.rpm and *.msi), then enter the string manually. If not entered manually, after you save this configuration and deploy uninstall action in a client machine, uninstallation does not take place automatically even if the status of this action on the console shows 'Completed.'
5. Click **Save**.

   The uninstallation configuration is saved to uninstall the software.

Edit a Software Package

To simplify package creation and editing, installation and uninstallation commands are generated automatically for supported file types. Feel free to edit these defaults, or type your own. For unsupported file types, enter the commands you want to use.

- Supported installation file types: .appv, .appx, .bat, dmg, .exe, .msi, .msp, .msu, .pkg (Mac and Solaris), .rpm.
- Supported uninstallation file types: .appv, .msi, .rpm.

Edit a Software Package

1. Open the software package document that you want to update.
2. Click the **Edit Software** link in the right side panel.
3. Make any wanted changes to the package data or deployment options. For more information about each field and its options, see Add Software Package *(on page 89)*.
4. Click **Save**.

Note: Packages edited in the SWD Dashboard such that the package no longer contains a file or Fixlet, cannot be edited in the WebUI.

Delete a Software Package

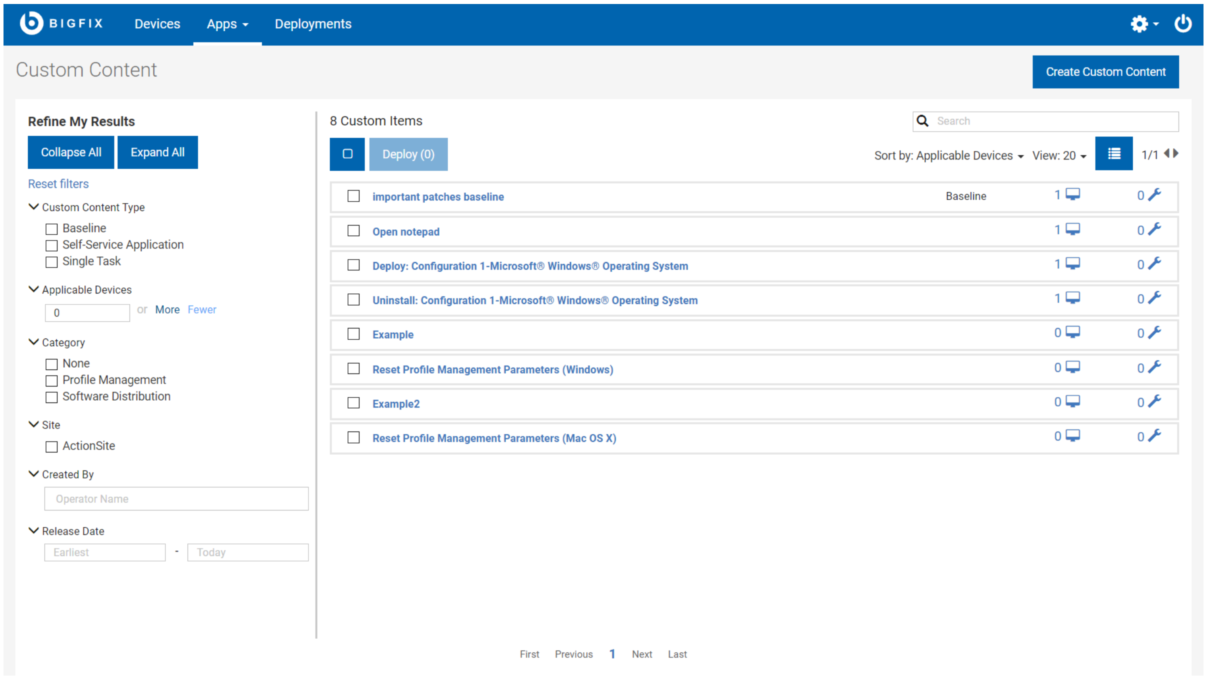
1. Open the Software Package document you want to delete.
2. Click the **Edit Software** link, located in the right side panel.
3. Click **Delete** in the lower left corner of the dialog, and confirm at the prompt.

Chapter 8. Get Started with Custom Content

Use the Custom Content pages to view custom content, edit tasks, and view related information, including applicable devices and deployments.

The Custom Content List

Use the filters to see specific types of content. Click a title to open a content document.

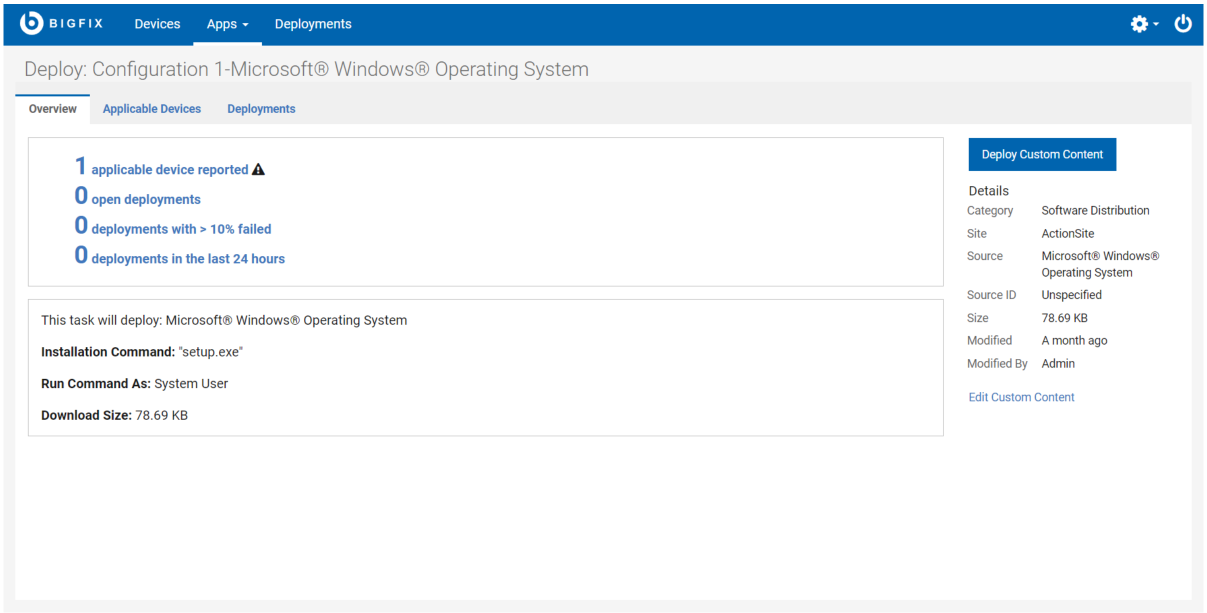


□ important patches baseline	Baseline	1	0
□ Open notepad		1	0
□ Deploy: Configuration 1-Microsoft® Windows® Operating System		1	0
□ Uninstall: Configuration 1-Microsoft® Windows® Operating System		1	0
□ Example		0	0
□ Reset Profile Management Parameters (Windows)		0	0
□ Example2		0	0
□ Reset Profile Management Parameters (Mac OS X)		0	0

Common categories often include installation, configuration, software distribution, security updates, and uninstallation. The site filters display content stored in a particular site.

Custom Content Documents

Click a custom content name to see its description, list of applicable devices, and deployment history. Use the links to see details provided in the associated views.



Deploy: Configuration 1-Microsoft® Windows® Operating System

1 applicable device reported ⚠

0 open deployments

0 deployments with > 10% failed

0 deployments in the last 24 hours

This task will deploy: Microsoft® Windows® Operating System

Installation Command: "setup.exe"

Run Command As: System User

Download Size: 78.69 KB

Details

Category	Software Distribution
Site	ActionSite
Source	Microsoft® Windows® Operating System
Source ID	Unspecified
Size	78.69 KB
Modified	A month ago
Modified By	Admin

The Custom Content views:

- Overview - detailed description of custom content.
- Applicable Devices - machines eligible for this content.
- Deployments - list of deployments for this piece of content.

If a piece of custom content involves multiple actions, as for a baseline, for example, the names of its components are listed in the Overview. For information about the differences between Single tasks and Baselines, see the Glossary.

Creating Custom Content

Use the Custom Content Wizard screen to create custom content.

The WebUI application allows operators with the appropriate permissions to create new Fixlet content within the WebUI. The operator can create custom content by filling the required fields in the custom content creation wizard. The below listed fields in the custom content creation wizard are mandatory to create custom content:

- Name: Enter a desired name for the custom content.
- Relevance: Enter the required relevance.
- Action: Enter the action script.
- Site: Enter the site to which you want to deploy the custom content.

Note: Though all the fields are not mandatory, it is recommended to enter the details in non-mandatory fields.

Creating Custom Content

- To get to the custom content creation page in the global navigation, click **Apps** > select **Custom** from the drop-down, and then click **Create Custom Content** button.
- On the Create Custom Content Wizard screen, enter the name, add the task description, relevance, and actionscript accordingly.

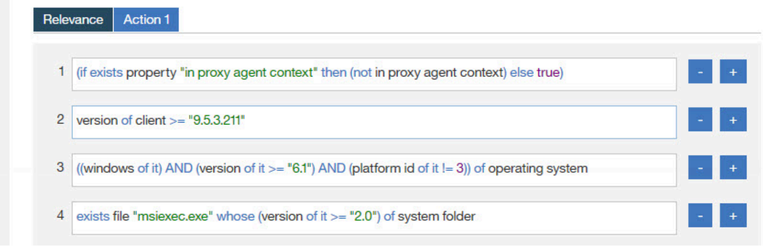
Add Task Descriptions

Add task descriptions using the Rich Text Format (RTF) or HTML editors; the **Use HTML Editor/ Use Rich Text Editor** link toggles between them. The two editors are not kept in sync. In other words, changes made in one will not be replicated when you switch to the other. Click **Save** to save the contents of the active editor; any changes made in the other editor will be lost.

To protect against cross-site scripting attacks, text entered in the Rich Text editor is checked before it is saved. For example, style and script tags will be removed, and URLs and class/ ID values might be modified or removed. Content that is created in the console is rendered accurately in the HTML editor, but might not be rendered accurately by the Rich Text editor.

Add Task Relevance

Click the boxed **+** and **–** controls to insert or remove a clause. An asterisk next to a tab name indicates that a change was made on that tab. Changes made on this page to Relevance created in the BigFix console using the Conditional Relevance option will subsequently appear in the console as Relevance clauses.

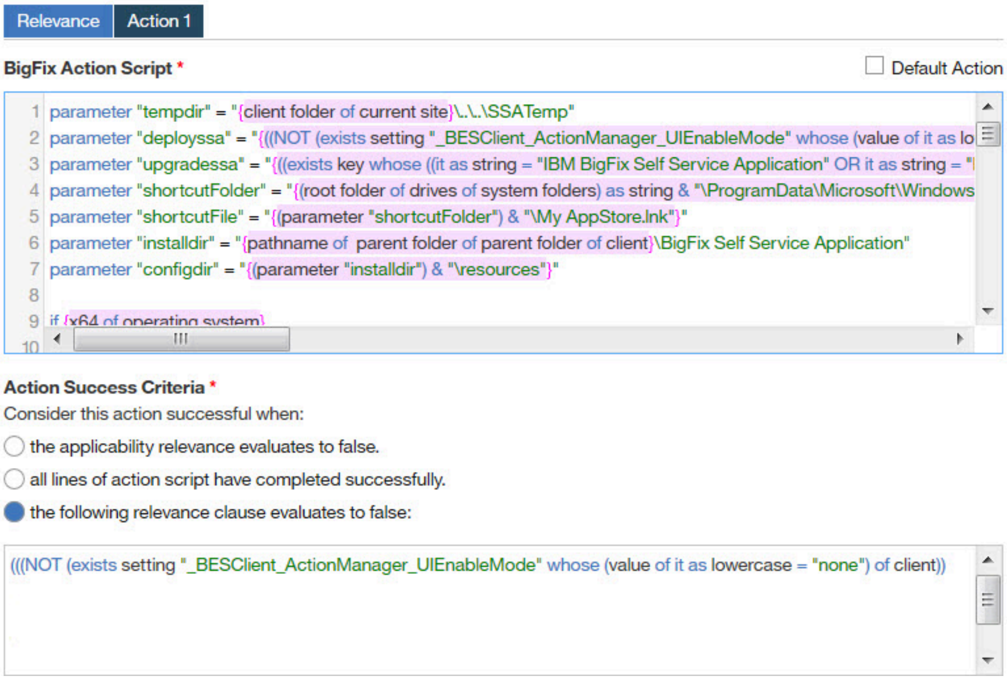


```
1 (if exists property "in proxy agent context" then (not in proxy agent context) else true)
2 version of client >= "9.5.3.211"
3 ((windows of it) AND (version of it >= "6.1") AND (platform id of it != 3)) of operating system
4 exists file "msiexec.exe" whose (version of it >= "2.0") of system folder
```

For more information about adding Relevance, see the BigFix Console Operators Guide.

Add Task Actions

Use the editor on the **Custom Content Wizard** page to modify an action. A bolded tab name marks the default action. Actions cannot be added or removed using this editor.



BigFix Action Script *

☐ Default Action

```
parameter "tempdir" = "{client folder of current site}\..\..\SSATemp"
parameter "deployssa" = "{((NOT (exists setting "_BESClient_ActionManager_UIEnableMode" whose (value of it as lo
parameter "upgradessa" = "{((exists key whose ((it as string = "IBM BigFix Self Service Application" OR it as string = "
parameter "shortcutFolder" = "{(root folder of drives of system folders) as string & "\ProgramData\Microsoft\Windows
parameter "shortcutFile" = "{(parameter "shortcutFolder") & "\My AppStore.lnk"}"
parameter "installdir" = "{pathname of  parent folder of parent folder of client}\BigFix Self Service Application"
parameter "configdir" = "{(parameter "installdir") & "\resources"}"

if {x64 of operating system}
```

Action Success Criteria *

Consider this action successful when:

○ the applicability relevance evaluates to false.

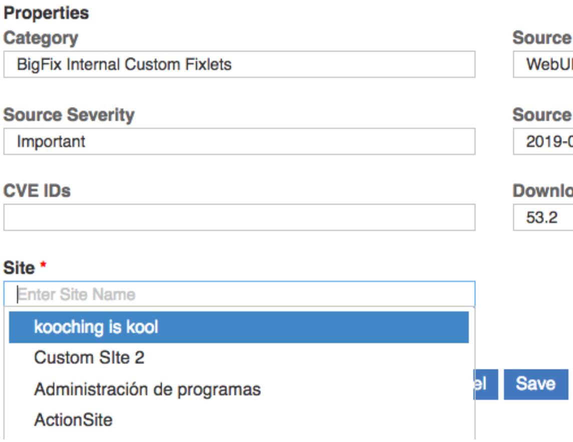
○ all lines of action script have completed successfully.

● the following relevance clause evaluates to false:

```
(((NOT (exists setting "_BESClient_ActionManager_UIEnableMode" whose (value of it as lowercase = "none") of client))
```

Add Task Properties

Use the property fields on the **Custom Content Wizard** page to add or change property information. Add information appropriate to the task, for example, Common Vulnerabilities and Exposures (CVE) ID for patch-related tasks.


Properties

Category: BigFix Internal Custom Fixlets	Source: WebUI
Source Severity: Important	Source Release Date: 2019-03-11 ✖
CVE IDs:	Download Size: 53.2 MB

Site *

Enter Site Name

- koocheng is kool
- Custom SIte 2
- Administración de programas
- ActionSite

- Category - Type of task, for example, patch or software distribution.
- Download size - Used when a file is distributed with the task (as for software, or a patch).
- Source - Source of associated file, for example, a patch from Microsoft.
- Source Release Date - Date a piece of software or patch was released.
- Source Severity - Describes the level of risk associated with the problem fixed by a patch.
- CVE IDs - The CVE ID system number of a patch.
- Site – Custom content is saved to the selected site.

Important: Non-Master Operators can only save to their operator site and to the custom content sites that they have write permission.

Important: Master Operators can only save to custom site and the master action site.

Editing Custom Content

Use the Edit Task screen to edit custom content.

You can also,

- Add or change an icon.
- Edit Relevance - add and remove Relevance clauses.
- Edit Action Script - add or change an action and success criteria.
- Delete a task.

The link to the **Edit Task** page appears on custom content and software package documents when an operator has permission to edit tasks. The **Edit Task** page does not currently provide the full editing capabilities of the BigFix console. For example, it cannot be used to add actions, change script type, or include action setting locks. Use the BigFix console to edit baselines. Tasks that are created in the Profile Management application must be edited by using the Profile Management application.

Edit Task Descriptions

Edit task descriptions using the Rich Text Format (RTF) or HTML editors; the **Use HTML Editor/Use Rich Text Editor** link toggles between them. The two editors are not kept in sync. In other words, changes made in one will not be replicated when you switch to the other. Click **Save** to save the contents of the active editor; any changes made in the other editor will be lost.

To protect against cross-site scripting attacks, text entered in the Rich Text editor is checked before it is saved. For example, style and script tags will be removed, and URLs and class/ID values might be modified or removed. Content that is created in the console is rendered accurately in the HTML editor, but might not be rendered accurately by the Rich Text editor.

Edit Task Relevance

Use the editor on the **Edit Task** page to edit Relevance. Click the boxed **+** and **–** controls to insert or remove a clause. An asterisk next to a tab name indicates that a change was made on that tab. Changes made on this page to Relevance created in the BigFix console using the Conditional Relevance option will subsequently appear in the console as Relevance clauses.

For more information about editing Relevance, see the BigFix Console Operators Guide.

Edit Task Actions

Use the editor on the **Edit Task** page to modify an action. A bolded tab name marks the default action. Actions cannot be added or removed using this editor.

Edit Task Properties

Use the property fields on the **Edit Task** page to add or change property information. Add information appropriate to the task, for example, Common Vulnerabilities and Exposures (CVE) ID for patch-related tasks.

- Category - Type of task, for example, patch or software distribution.
- Download size - Used when a file is distributed with the task (as for software, or a patch).
- Source - Source of associated file, for example, a patch from Microsoft.
- Source Release Date - Date a piece of software or patch was released.
- Source Severity - Describes the level of risk associated with the problem fixed by a patch.
- CVE IDs - The CVE ID system number of a patch.

Chapter 9. Get Started with BigFix Query

Use the BigFix Query feature to retrieve data from endpoints through a dedicated query channel, where the memory available on each Relay minimizes the impact to normal BigFix processing.

You can use BigFix Query to:

- Query individual computers, manual computer groups, and dynamic computer groups
- Build Relevance and use it in building a query
- Find Relevance from the BES sites
- Test Relevance expressions as you develop the content
- Export query results to a comma-separated value (.csv) file
- Create a library of custom queries and keep the collections private or share them with others

Users and roles

The Master Operator creates custom sites to host queries, and assigns access to BigFix Query Operators and Content Creators. This allows Content Creators to save queries on the custom site, group queries into categories, and make them available to operators.

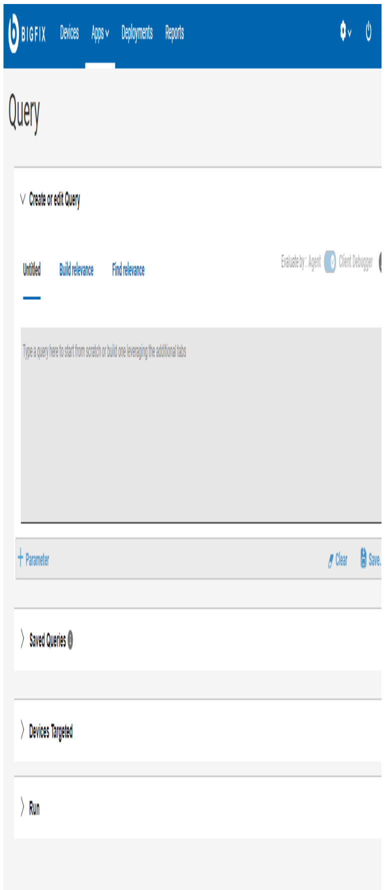
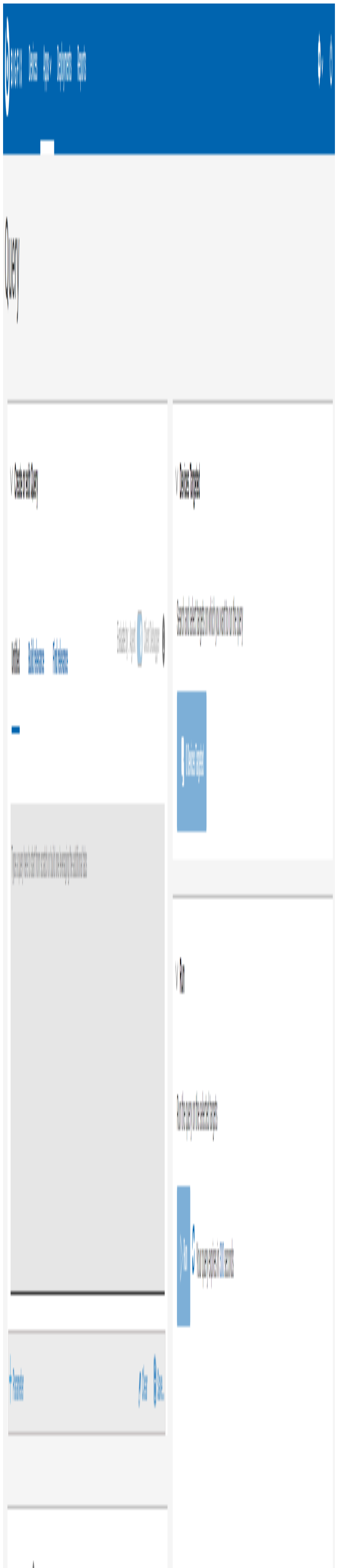
Content Creator

As a Content Creator, you can use BigFix Query to do the following tasks:

- Filter queries by selecting or unselecting system and local queries
- Load, hide, delete, or reload sample queries into your operator site
- Customize queries and build your own queries
- Build Relevance and use it in building a query
- Find Relevance from the BES sites
- Save queries on a new site or with a new name and make them available to the operators to access it
- Select and filter target devices to run the query
- Click on **Switch to run view** to enter values for the parameters used in the Relevance expression of a query
- View the results of the query and save them to a `.csv` file
- Open a device document from query results to investigate or apply a fix
- Choose to run a query to be evaluated by the agent or by the local QnA
- Change the default timeout value for the query results to be gathered
- View the results of the last 5 queries run, through the result tabs

Query app supports resolutions between range: 1024 x 768 (minimum) and 1920 x1080 (maximum). The following graphics show the main Query editor page for a Content Creator or Master Operator for different resolutions:

Table 15.

Figure 2. 1024x768 resolution	Figure 3. 1920x1080 resolution
	

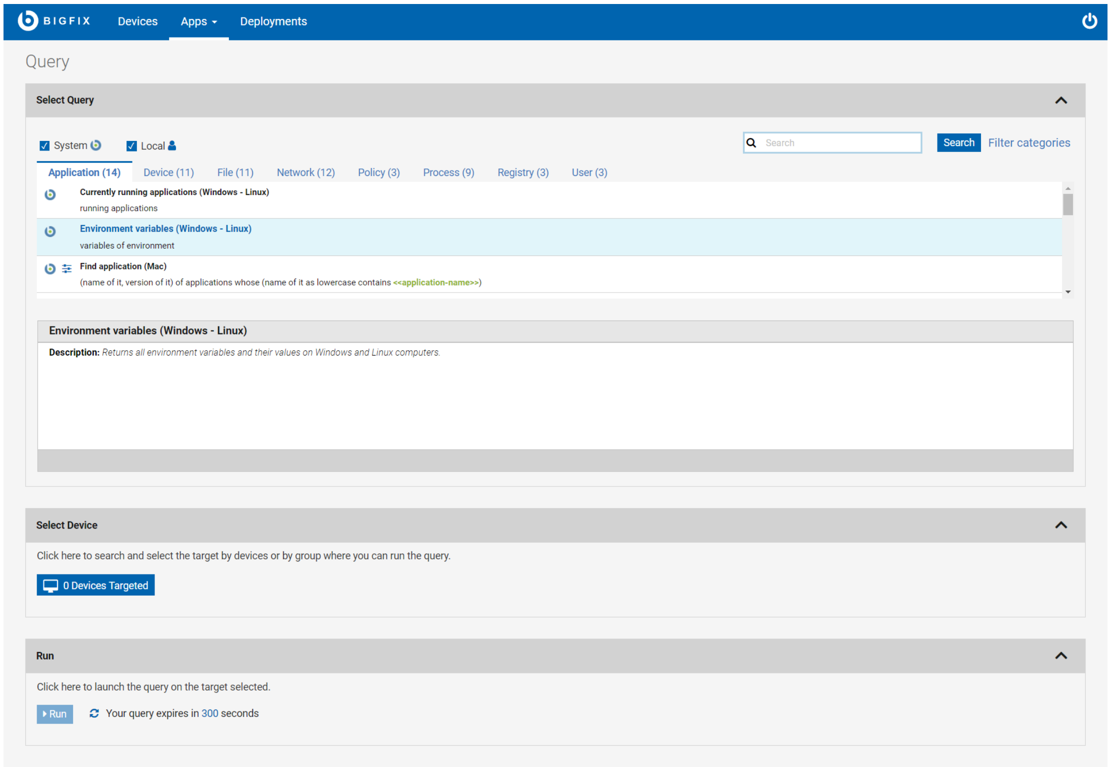
Operator

As an Operator, you can use BigFix Query to do the following tasks:

- View the queries that a Content Creator shared with you
- Filter, search, or select a query
- View query descriptions
- Filter and select target devices
- Run a query
- Choose to run a query to be evaluated by the agent or by the local QnA
- Enter values for the parameters used in the Relevance expression of a query
- View the results of the last 5 queries run, through the result tabs
- Change the default timeout value for the query results to be gathered
- View query results and save them to a .csv file, if you have the required permission
- Open a device document from query results to investigate or apply a fix

Operators cannot create or delete queries and cannot view Relevance expressions.

The following graphic shows the main Query editor page for a Non-Master Operator:



Currently running applications (Windows - Linux)
running applications

Environment variables (Windows - Linux)
variables of environment

Find application (Mac)
(name of it, version of it) of applications whose (name of it as lowercase contains <<application-name>>)

Environment variables (Windows - Linux)

Description: *Returns all environment variables and their values on Windows and Linux computers.*

Click here to search and select the target by devices or by group where you can run the query.

Click here to launch the query on the target selected.

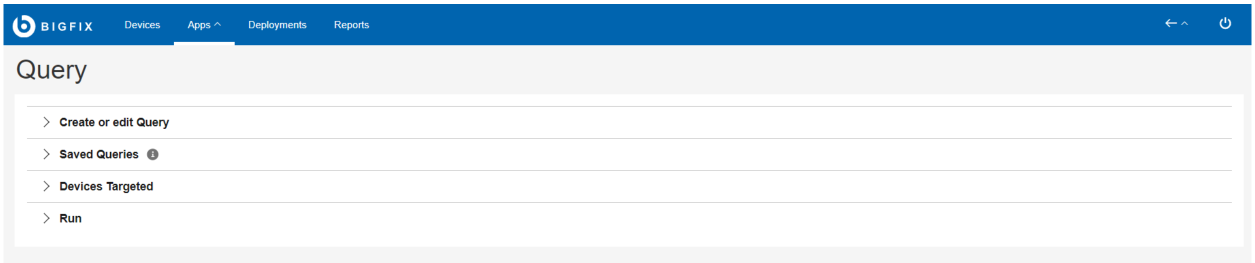
Your query expires in 300 seconds

For details on the editor and how to use custom queries, see Building a query (on page 109).

For information about the different types of users that can use BigFix Query, see Permissions for BigFix Query.

About Accordions

The sections in BigFix Query page is organized with accordions to provide a better visibility of the tasks to retrieve data from devices. You can expand or collapse the view.



Query

- Create or edit Query
- Saved Queries
- Devices Targeted
- Run

- **Create or edit Query**: This section allows you to view, edit, and create a query. This section has the following tabs.
    - Untitled tab *(on page 111)*
    - Build relevance *(on page 113)*
    - Find relevance *(on page 125)*
- **Saved Queries**: This section allows you to view saved local and custom queries. It shows all the queries that BigFix provides (System queries) and those saved by operators (Local queries). If you are looking for a relevance content in general, run a search in Find relevance *(on page 125)* Tab.
    - System
    - Local
    - Filter by query type (System or Local)
    - Search
    - Filter Categories to narrow down the search
- **Devices Targeted**: This section allows you to select your targets/endpoints. To enable the Devices targeted button in this section, select a query to run on the targets. Click the Devices targeted button to select the target devices. It displays the device data in a grid. You can use the filters and search options available in this grid to identify your devices and select them to run the query.
    - Target by device
    - Target by group

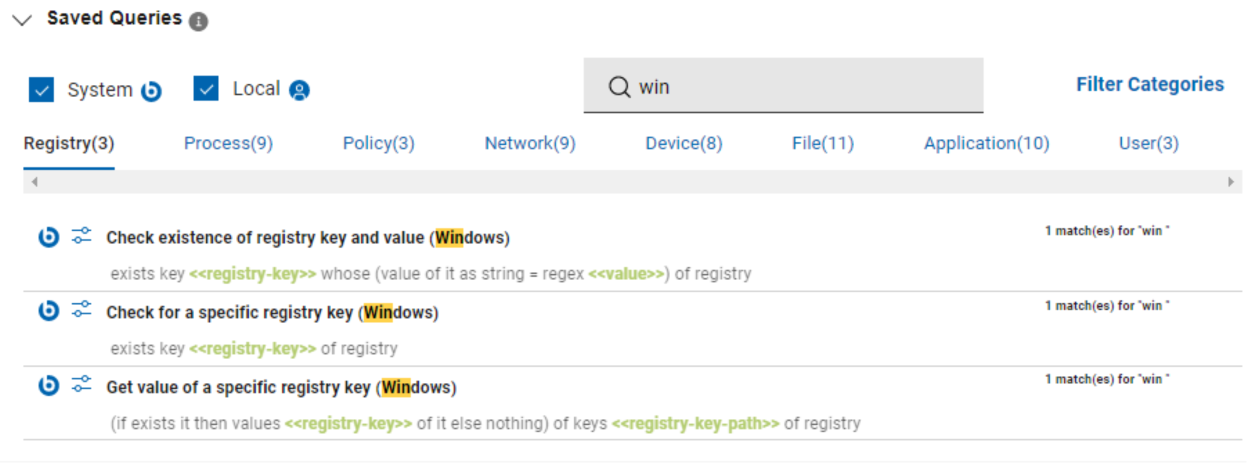
    Note: *Only devices identified with the BigFix icon will be capable of responding properly to the Query requests.*

- **Run**: This section allows you to run a query *(on page 106)* on the selected target. It fetches the results and displays in a grid. To enable the Run button in this section, select a query and the target devices.

About Search

You can search for queries by using **Search** feature.

To perform a basic search, enter a search string and click **Enter**. This lists the queries that contain the specified string highlighted in the query title.



Saved Queries

☑ System ☑ Local

win

Filter Categories

Registry(3) Process(9) Policy(3) Network(9) Device(8) File(11) Application(10) User(3)

Check existence of registry key and value (Windows) 1 match(es) for "win "

exists key <<registry-key>> whose (value of it as string = regex <<value>>) of registry

Check for a specific registry key (Windows) 1 match(es) for "win "

exists key <<registry-key>> of registry

Get value of a specific registry key (Windows) 1 match(es) for "win "

(if exists it then values <<registry-key>> of it else nothing) of keys <<registry-key-path>> of registry

About Filters

You can filter queries based on their creation type and or based on their categories.

To filter based on the creation type:

- Select the **System** check box to view only the sample queries loaded from the database.
- Select the **Local** check box to view only the custom queries.

Note:

- To view both sample and custom queries, select both **System** and **Local** check boxes.
- If you clear both **System** and **Local** check boxes, the query app displays both sample and custom queries.

To filter based on the categories:

1. Enter the search string, and click **Filter categories**.
2. Select the categories from the list to refine the search.

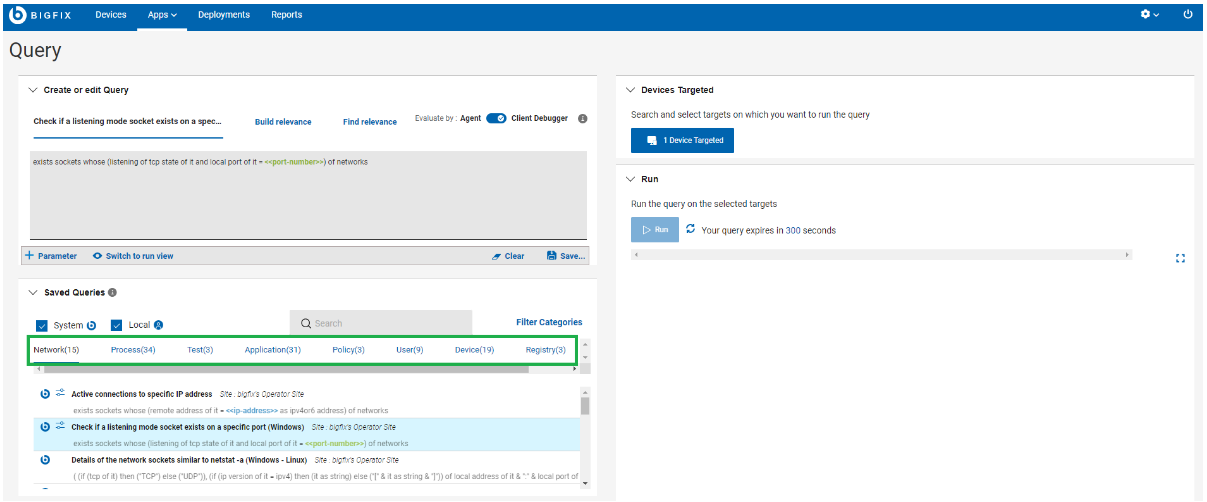
   Note: All categories are selected by default. To refine your search, clear check boxes against unwanted categories.

3. Click **Save** to save your selection for future searches.

This lists the queries that contain the specified string in the query titles and/or in the Relevance expressions.

About Categories

With Categories, Content Creators can group queries according to their needs. Content Creators can create, populate and delete categories, while Operators can only show or hide categories.



Check if a listening mode socket exists on a spec...

```
exists sockets whose (listening of tcp state of it and local port of it = <<port-number>>) of networks
```

☑ System ☑ Local

Network(15) Process(34) Test(3) Application(31) Policy(3) User(9) Device(19) Registry(3)

Active connections to specific IP address *Site : bigfix's Operator Site*

```
exists sockets whose (remote address of it = <<ip-address>> as ipv4or6 address) of networks
```

Check if a listening mode socket exists on a specific port (Windows) *Site : bigfix's Operator Site*

```
exists sockets whose (listening of tcp state of it and local port of it = <<port-number>>) of networks
```

Details of the network sockets similar to netstat -a (Windows - Linux) *Site : bigfix's Operator Site*

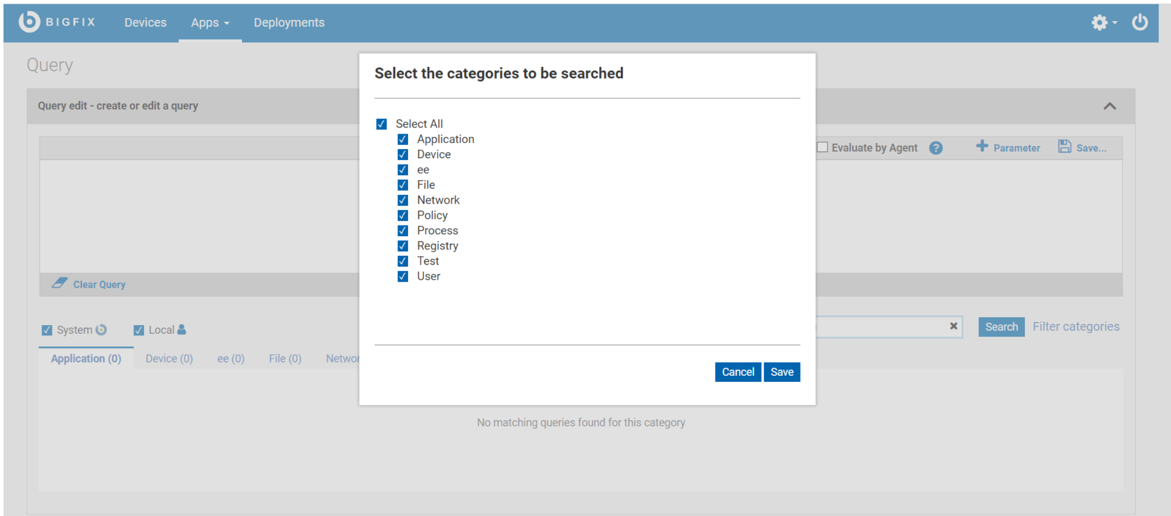
```
( (if (tcp of it) then ("TCP") else ("UDP")), (if (ip version of it = ipv4) then (it as string) else ("[" & it as string & "]")) of local address of it & ":" & local port of
```

Search and select targets on which you want to run the query

Run the query on the selected targets

Your query expires in 300 seconds

- The category tabs are displayed alphabetically from left-to-right, row by row. Query titles are listed alphabetically in each category.
- Each query must be saved in at least one category and each category can contain queries hosted by different sites.
- To delete a category, a Content Creator must delete all queries in the category.
- To create a category, a Content Creator must specify a name for the category name when saving a query.
- To filter queries by category, click Filter categories, select the desired categories, and click Save. Only queries that are relevant to the selected categories are displayed.



Select the categories to be searched

☑ Select All
☑ Application
☑ Device
☑ ee
☑ File
☑ Network
☑ Policy
☑ Process
☑ Registry
☑ Test
☑ User

□ Evaluate by Agent

No matching queries found for this category

About queries and sites

Each query is uniquely identified by the combination of its title and the name of the site that is hosting the query. If you change either of these two values, a copy of the query is automatically created. If you create a copy of a query in a different site, you must apply subsequent updates to each copy individually.

You can save queries only to sites to which you have access as assigned by a Master Operator. These sites can be either of the following:

- Custom sites created by a Master Operator to share it with Operators.
- Operator sites, if the Content Creator is a Non-Master Operator.

Note: Preexisting queries are not automatically imported into the current BigFix Query release. However, they are still available as dashboard variables. You can access them using the REST API dashboard variable resource, as documented on the following page https://developer.bigfix.com/rest-api/api/dashboardvariable.html.

To learn more about BigFix Query, visit the following links:

- Getting client information by using BigFix Query
- BigFix Query requirements
- BigFix Query restrictions
- Who can use BigFix Query
- How to run BigFix Query from the WebUI
- How BigFix manages BigFix Query requests

Running a sample query

System queries are sample queries that are marked with the BigFix icon. As Content Creators, you can load, hide, delete, and reload sample queries in operator sites.

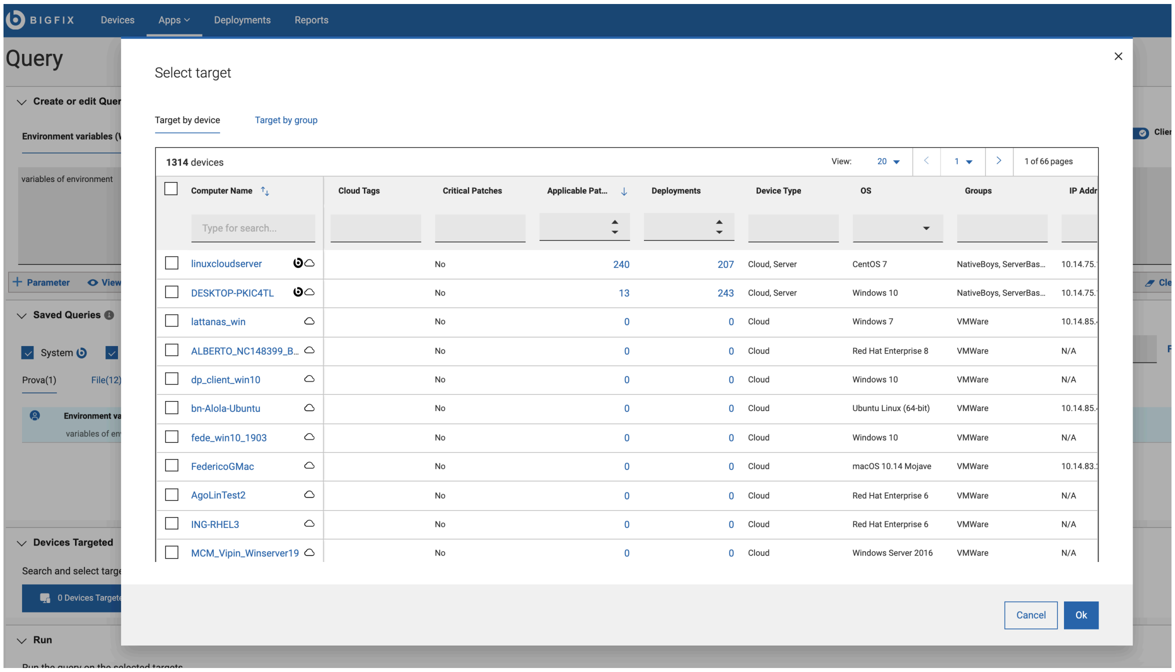
BigFix provides sample queries under the categories Applications, Files, Devices, Networks, Processes, Registry, Policies, and Users.

Note: If multiple content creators save a copy of query with the same name and category in different sites, the application creates multiple instances of the query.

To run a sample query, do the following steps:

1. Click on a category *(on page 105)* tab.
2. From the listed queries, select a query to display it in the editor. You can also use search and filter functions to locate a specific query.

3. If the query has parameters, enter the parameter values or accept the default values, if provided. You must use the Operator View to specify parameter values at run time. For more information, see Managing parameters in queries *(on page 127)*.
4. In the **Device Targeted** section, click **Devices Targeted** to open the target list. To select the list of targets to display, click either **Target By Device** or **Target By Group**.



Select target

Target by device | Target by group

1314 devices — View: 20 — 1 — 1 of 66 pages

☐ Computer Name	Cloud Tags	Critical Patches	Applicable Pat...	Deployments	Device Type	OS	Groups	IP Addr
☐ linuxcloudserver		No	240	207	Cloud, Server	CentOS 7	NativeBoys, ServerBas...	10.14.75.
☐ DESKTOP-PKIC4TL		No	13	243	Cloud, Server	Windows 10	NativeBoys, ServerBas...	10.14.75.
☐ lattanas_win		No	0	0	Cloud	Windows 7	VMWare	10.14.85.
☐ ALBERTO_NC148399_B...		No	0	0	Cloud	Red Hat Enterprise 8	VMWare	N/A
☐ dp_client_win10		No	0	0	Cloud	Windows 10	VMWare	N/A
☐ bn-Alola-Ubuntu		No	0	0	Cloud	Ubuntu Linux (64-bit)	VMWare	10.14.85.
☐ fede_win10_1903		No	0	0	Cloud	Windows 10	VMWare	N/A
☐ FedericoGMac		No	0	0	Cloud	macOS 10.14 Mojave	VMWare	10.14.83.
☐ AgoLinTest2		No	0	0	Cloud	Red Hat Enterprise 6	VMWare	N/A
☐ ING-RHEL3		No	0	0	Cloud	Red Hat Enterprise 6	VMWare	N/A
☐ MCM_Vipin_Winserver19		No	0	0	Cloud	Windows Server 2016	VMWare	N/A

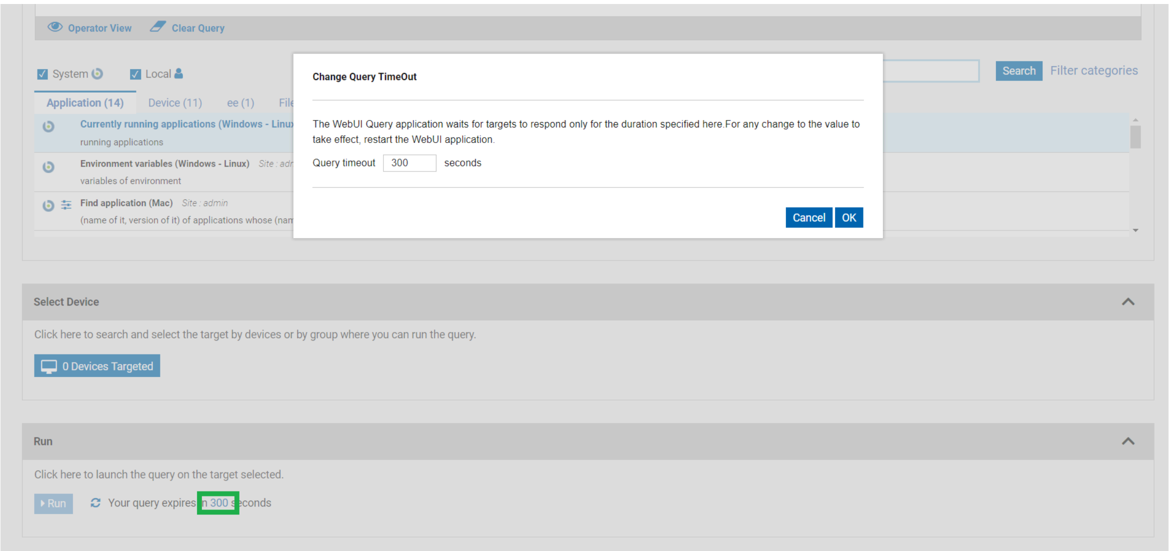
Cancel | Ok

5. Select one or more target devices in which you want to run the query.
   - You can select individual devices or groups. The targets are listed as per the permissions of the user. Master Operators see all devices and groups. Non-Master Operators might see a subset of the complete list. Use the sort, search, and filtering *(on page 10)* functions to quickly locate target devices.
     - To find a specific device or group, enter its name in the **Search** field for the name column.
     - Use filters to locate devices with specific properties.

   When the device or group selection is complete click **OK** to return to the editor. The **Devices Targeted** button displays the total number of devices selected.

   Note: When pairing queries and targets, keep in mind that queries that are concise and limited in scope run most efficiently. Broad queries return larger data sets and use more resources and affect the query performance.

6. To limit the polling time taken by the server to fetch the results, you can set Query timeout. The default time is 300 sec and the maximum limit is 900 sec. To change the default time, click the link on the default time, and in the **Change Query TimeOut** popup, enter the required number of seconds. For broader queries, server stops polling the results when it reaches the specified polling time.



Change Query TimeOut

The WebUI Query application waits for targets to respond only for the duration specified here.For any change to the value to take effect, restart the WebUI application.

Query timeout 300 seconds

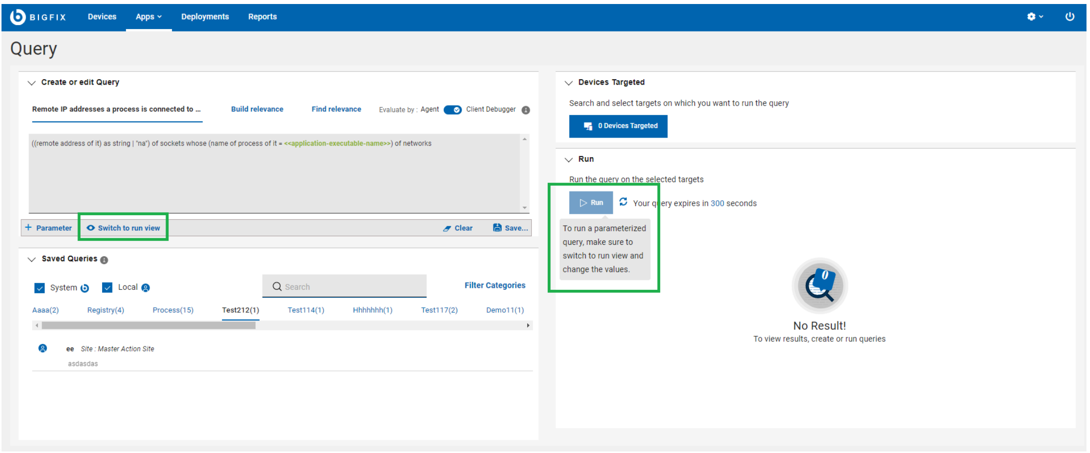
Click here to search and select the target by devices or by group where you can run the query.

Click here to launch the query on the target selected.

Your query expires in 300 seconds

7. To run the query, click **Run**. If you want to cancel the query, you can do it while the results are loading.

Note: To run a parameterized query make sure to switch to run view and change the values.



```
((remote address of it) as string | "na") of sockets whose (name of process of it = <<application-executable-name>>) of networks
```

Search and select targets on which you want to run the query

Run the query on the selected targets

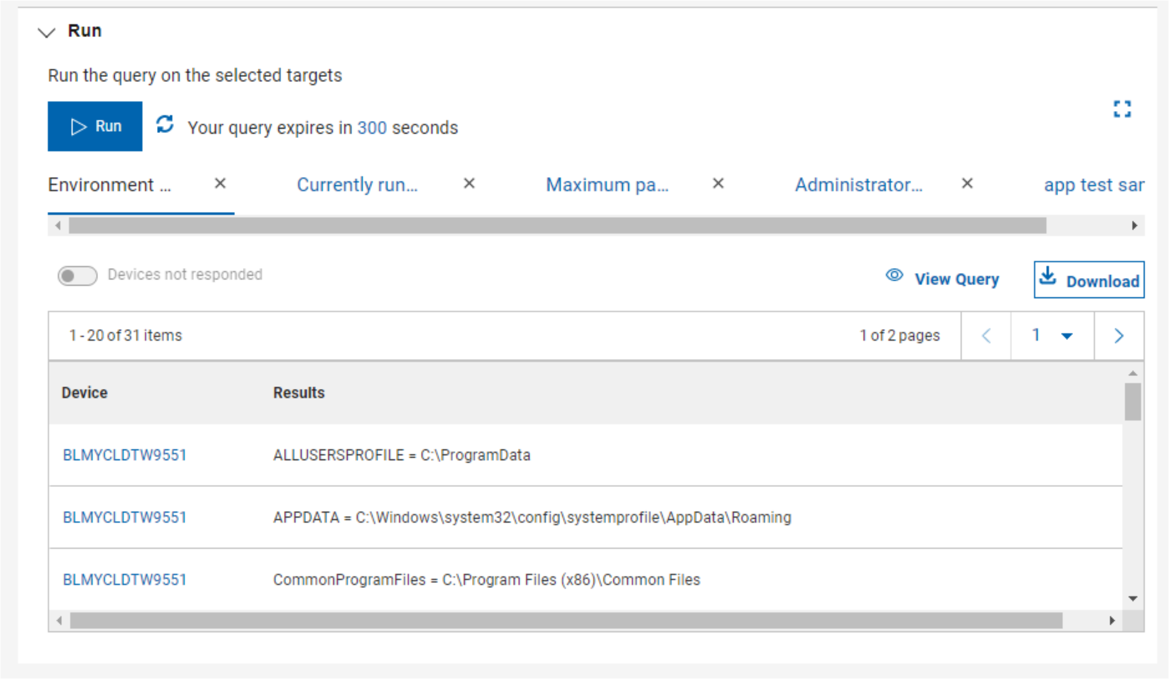
Your query expires in 300 seconds

To run a parameterized query, make sure to switch to run view and change the values.

No Result!

To view results, create or run queries

8. Review your results. Devices report in real time, and new arrivals are appended to the list as clients report in within the set time limit.



Run the query on the selected targets

Your query expires in 300 seconds

1 - 20 of 31 items 1 of 2 pages 1

Device	Results
BLMYCLDTW9551	ALLUSERSPROFILE = C:\ProgramData
BLMYCLDTW9551	APPDATA = C:\Windows\system32\config\systemprofile\AppData\Roaming
BLMYCLDTW9551	CommonProgramFiles = C:\Program Files (x86)\Common Files

- To switch to full screen mode and see more results, click the **Expand** icon. Click the icon again, or press the **Escape** key, to exit from full screen mode.
- Left corner of the list show the total number of rows, and the number of devices that reported so far.
- You can view the total number of resultant pages and navigate between pages by selecting the page number or using < previous and > next navigation buttons.
- You can view the report of five recent query runs. To see the query details click on **View Query** icon.
- Select the report and click **Download** button to download the report as a `.csv` file.
- Click the clock icon to see the titles of the recent 10 query runs.
- To save the results to a file in comma-separated values (.csv) format, click the **Download** button.

Building a query

Working with local/custom queries. The queries created by Content Creators are local/custom queries and are marked with the operator icon. Content Creators can create, load, run, hide, delete, and reload local queries in their operator sites.

Creating or editing a query

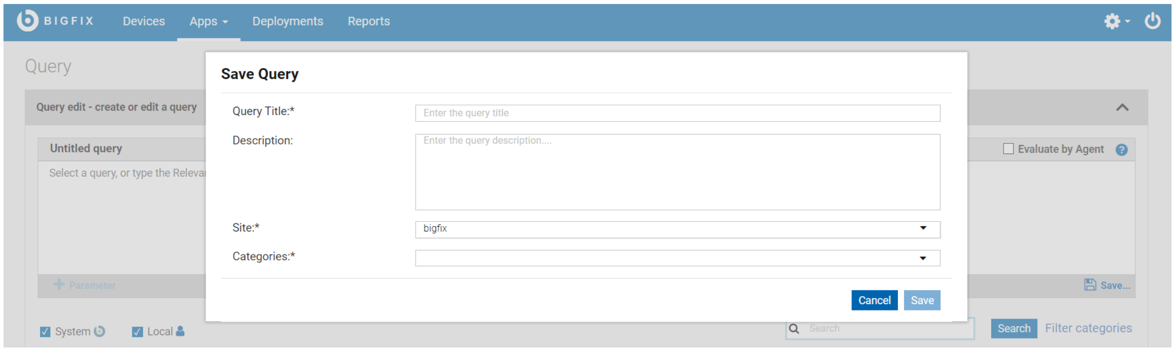
A Content Creator can create a new query in the following ways:

- Build Relevance expression through the Build relevance *(on page 113)* tab and save it as a query.
- Find an existing Relevance expression through the Find relevance *(on page 125)* tab to use it in the query editor in the Untitled tab *(on page 111)*

- Enter Relevance expression in the Query editor and save it.
- Create a copy of an existing query, edit it as needed, and save it with a different name or save it to a different site.

To create or edit a query:

1. In the Untitled tab *(on page 111)* ensure you are in Edit View *(on page 100)*.
2. Enter the Relevance expression in the Query editor.
    a. To edit an existing query, select the desired query under a category. This displays the title of the query and Relevance expression in the editor which you can edit. You can also click **Clear Query** to enter your Relevance expression afresh.
    b. You can build Relevance expression from the Build relevance *(on page 113)* tab or find an existing Relevance expression from the Find relevance *(on page 125)* tab and copy and paste it in the Query editor.
3. Add parameters to the Relevance expression, if required. For details about parameters, see Managing parameters in queries *(on page 127)*
4. Click **Save**.



Save Query

Query Title:* Enter the query title

Description: Enter the query description....

Site:* bigfix

Categories:*

☑ System ☑ Local

    a. Enter a descriptive title for the query.

    Note: It is recommended to keep the query title short up to a maximum of 23 characters. If the query title is longer than that, the title is truncated on the title tab.

    b. Select a site that you are allowed to access and host the query on.
    c. Specify at least one category for the query.
        - If you specify more than one category, the query appears in all the specified categories.
        - If you enter a new name in the Categories field, a new category is created.
    d. Click **Save**.

Note:

- Writing Relevance expression in the query editor is similar to writing Fixlets in the BigFix Console using the Relevance language. It is recommended to be familiar with the Relevance language to build queries. To learn more about the Relevance language, see BigFix Developer. However, you can build

Relevance expressions with limited knowledge of Relevance language through Build relevance *(on page 113)* tab using proper filters.

- Concise queries that are limited in scope run most efficiently. Broad, general queries that return large data sets consume more resources and impact the performance. Problems associated with poorly performing Relevance in the Console can also occur in the Query editor.

Create copy of an existing query

A query is uniquely identified by its title and the site on which it is saved. To create a copy of a query, change either the title or the site of the query.

Note: If multiple content creators save a copy of a query with the same name and category in different sites, Master Operators might see multiple instances of the same query under a category.

To see who last edited a query, hover the cursor over the operator icon of the query.

Deleting a query

To delete a query, select the query and click the **Delete Query** icon next to it.

Note:

- Operators cannot delete queries.
- Master operators/Content Creators can delete the custom queries only and not the system queries.

Using Client Context

As a content creator, you can enable the **Evaluation by Agent** flag to save a specific query and use the client context. Enabling the **Evaluation by Agent** flag and running a query helps you to retrieve accurate data from the client.

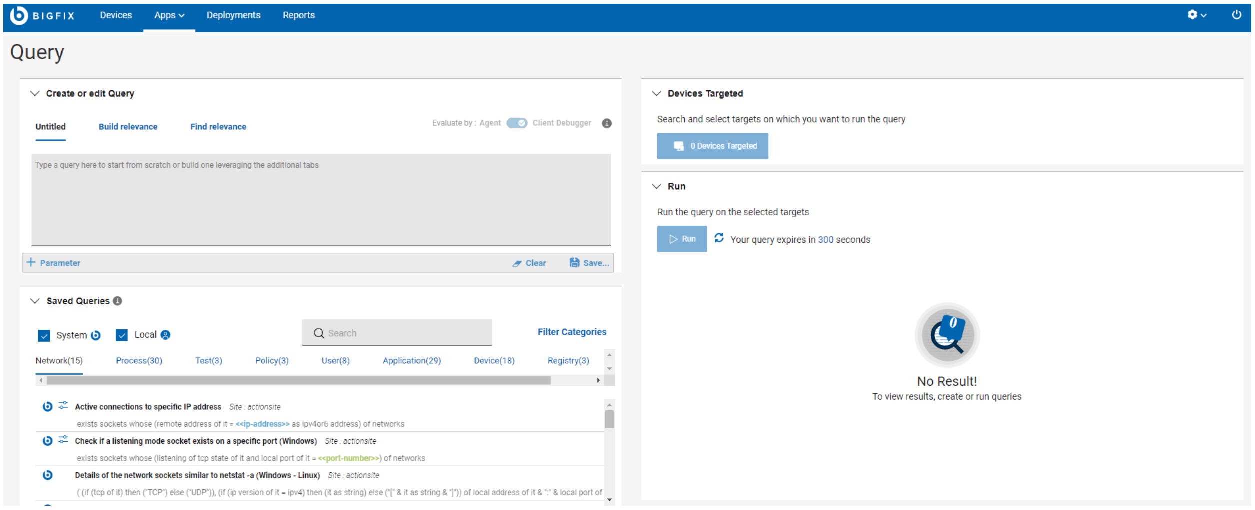
By default, the Queries are evaluated by Client Debugger. You can change it by using the `_WebUIAppEnv_USE_CLIENT_CONTEXT` client setting. If this setting is set to 1, the **Evaluate by Agent** flag is enabled. The value for each query can be overwritten only by the content creator. You can save the individual query by enabling the **Evaluation by Agent** flag, which allows an operator to use the client context.

Note: Evaluation by Agent flag is available only in BigFix Platform version 9.5.13 and later.

Untitled tab

This is the initial view when you log in to the Query app. When no query is selected, the tab in the Create or edit Query section is displayed as Untitled tab. When you select a saved query, this tab displays the title of the selected Query.

Note: Depending on your device resolution, the layout of the Query tabs differs. Refer to the link *(on page 101)* to find more information on supported resolutions.



Type a query here to start from scratch or build one leveraging the additional tabs

Active connections to specific IP address *Site : actionsite*

```
exists sockets whose (remote address of it = <<ip-address>> as ipv4or6 address) of networks
```

Check if a listening mode socket exists on a specific port (Windows) *Site : actionsite*

```
exists sockets whose (listening of tcp state of it and local port of it = <<port-number>>) of networks
```

Details of the network sockets similar to netstat -a (Windows - Linux) *Site : actionsite*

```
( (if (tcp of it) then ("TCP") else ("UDP")), (if (ip version of it = ipv4) then (it as string) else ("[" & it as string & "]")) of local address of it & ":" & local port of
```

Search and select targets on which you want to run the query

Run the query on the selected targets

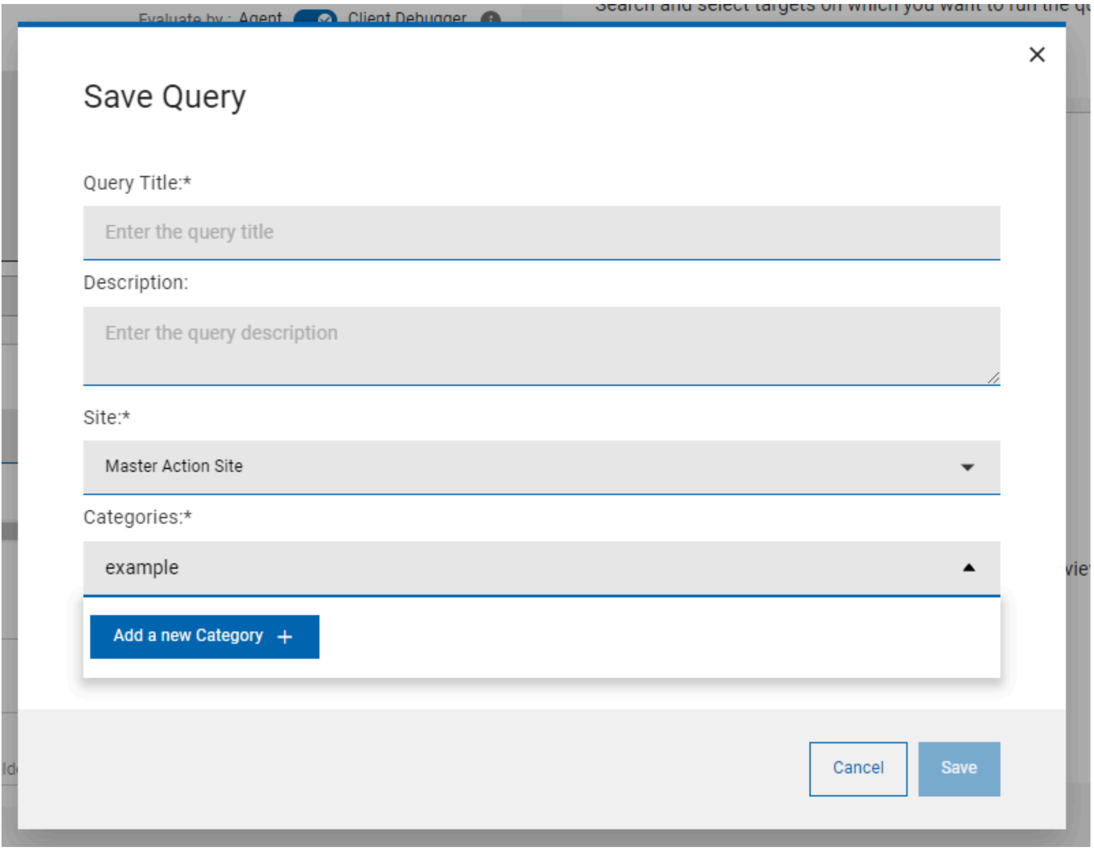
Your query expires in 300 seconds

To view results, create or run queries

If you have logged in as an Administrator or Master Operator or Content creator, you can see the following functions through this tab.

- **Parameter**: Click this button to add a parameter to your query. See Managing parameters in queries *(on page 127)* to learn more about managing parameters.
- **View**: This is a toggle button that helps to toggle between Operator view and Edit view. If an Admin runs a parametrized query, to input the value for the parameter in the query, the Admin must switch over to the operator view.
- **Clear**: Click this button to clear the Relevance statement in the Query editor.
- **Save**: Click this button to save a new query or updates to the existing query. When saving the new query you will be aksed to fill in a fields like:
    - Query Title
    - Description

  - Site
  - Categories. You can create new category by clicking on **Add a new Category** button



Save Query

Query Title:*

Description:

Site:* Master Action Site

Categories:* example

- **Evaluate by: Agent Client Debugger** *(on page 111)*: Enabling the **Evaluate by Agent** flag and running a query helps you to retrieve accurate data from the client.
- **Edit**: If you have switched over to Operator view, click this button to return to Edit view.

If you have logged in as an Operator, you can only view the description of the Query and cannot see the Relevance expression. Also, the above buttons are disabled. If you run a parametrized query as an operator, you can enter the value for the parameter from this tab.

Build relevance

As a Content Creator, you can build Relevance expressions with just few clicks through the Build relevance tab in the Query app.

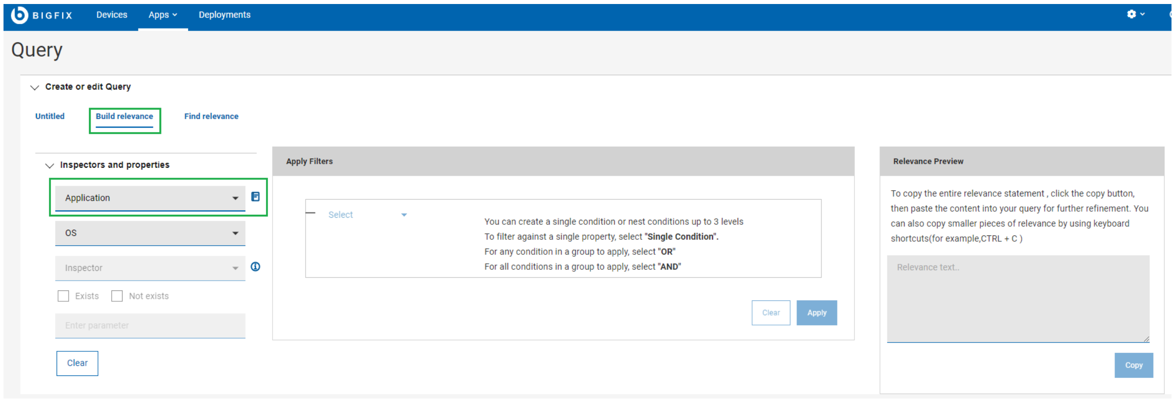
You can select inspectors and properties and apply filters to build Relevance expressions. You can click Copy to copy this Relevance expression and paste it in the Query editor to build a new query.

Build Relevance expression

Note: Please note that depending on your device resolution, layout of the Query tabs may differ. Refer to the link *(on page 101)* to find more information on supported resolutions.

To build Relevance expressions from the Build relevance tab, do the following:

1. From the WebUI main page, click **Apps > Query.**
2. In the **Create or edit Query** section, click **Build relevance**.
3. In the **Inspectors and properties** section, do the following:



You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select **"Single Condition"**.
For any condition in a group to apply, select **"OR"**
For all conditions in a group to apply, select **"AND"**

To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

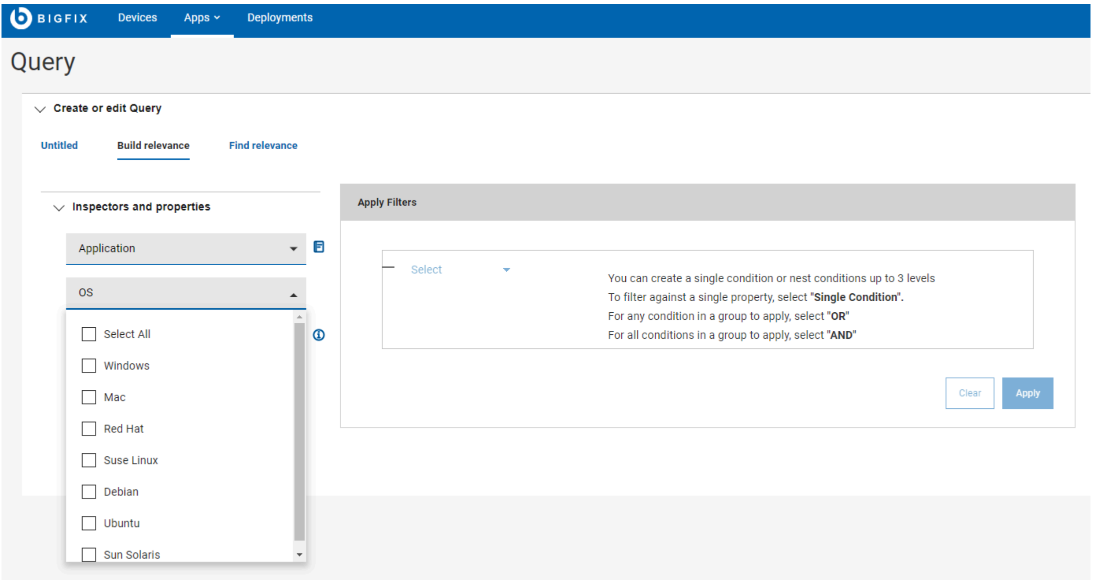
   a. From the first dropdown, select an Inspector type.

   To learn more about inspectors click on the 🗎 icon. It will help you understand the meaning of inspectors when buidling relevance expressions.

   List of currently supported Inspector types:

   - Active device
   - Application
   - Drive
   - File
   - Folder
   - Language
   - Network IP Interface
   - Operating system
   - Process
   - Processor
   - RAM
   - Registry Key
   - Running Task
   - Scheduled task
   - Service
   - User

b. From the second dropdown, select an operating system. You can select one or multiple operating systems.

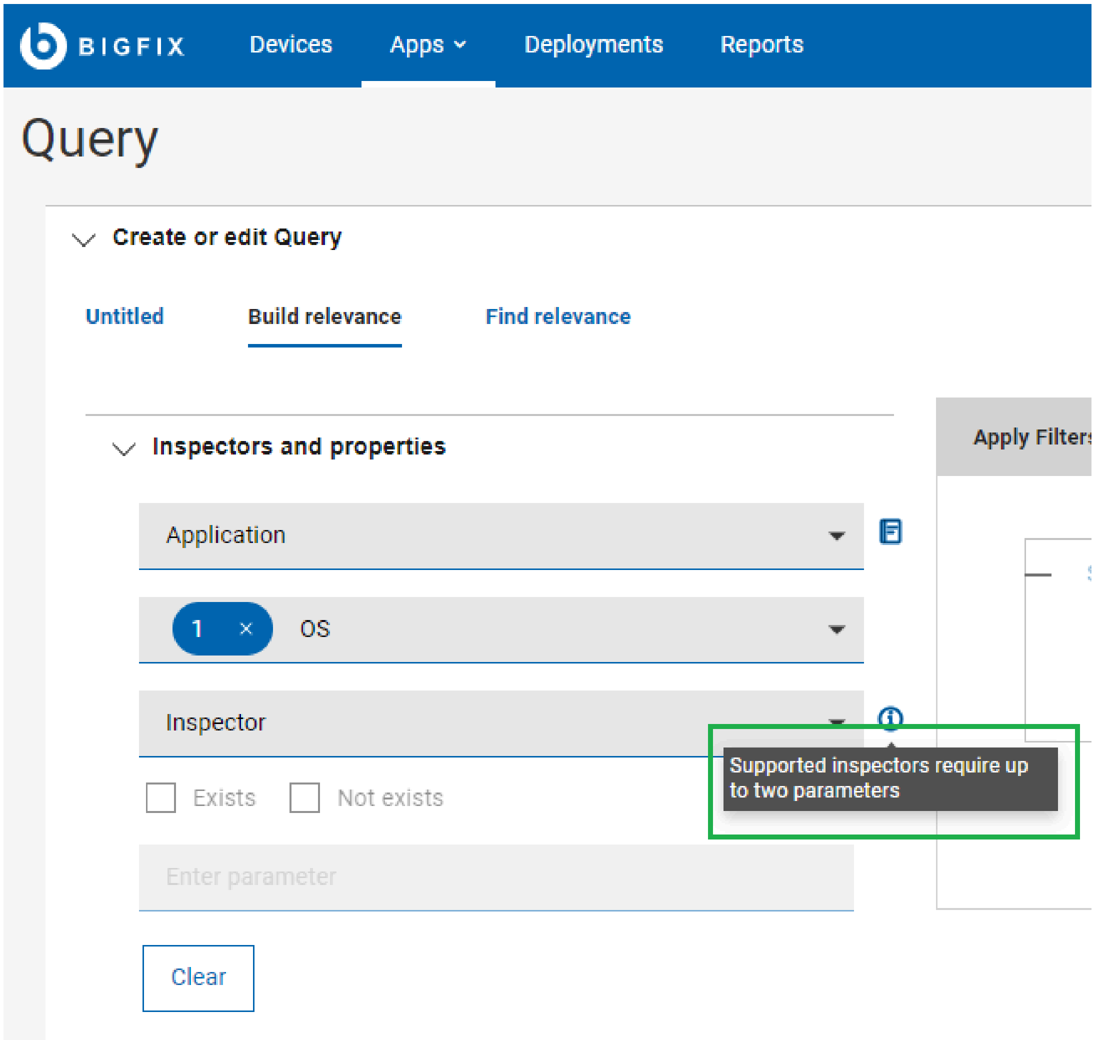


Application

OS

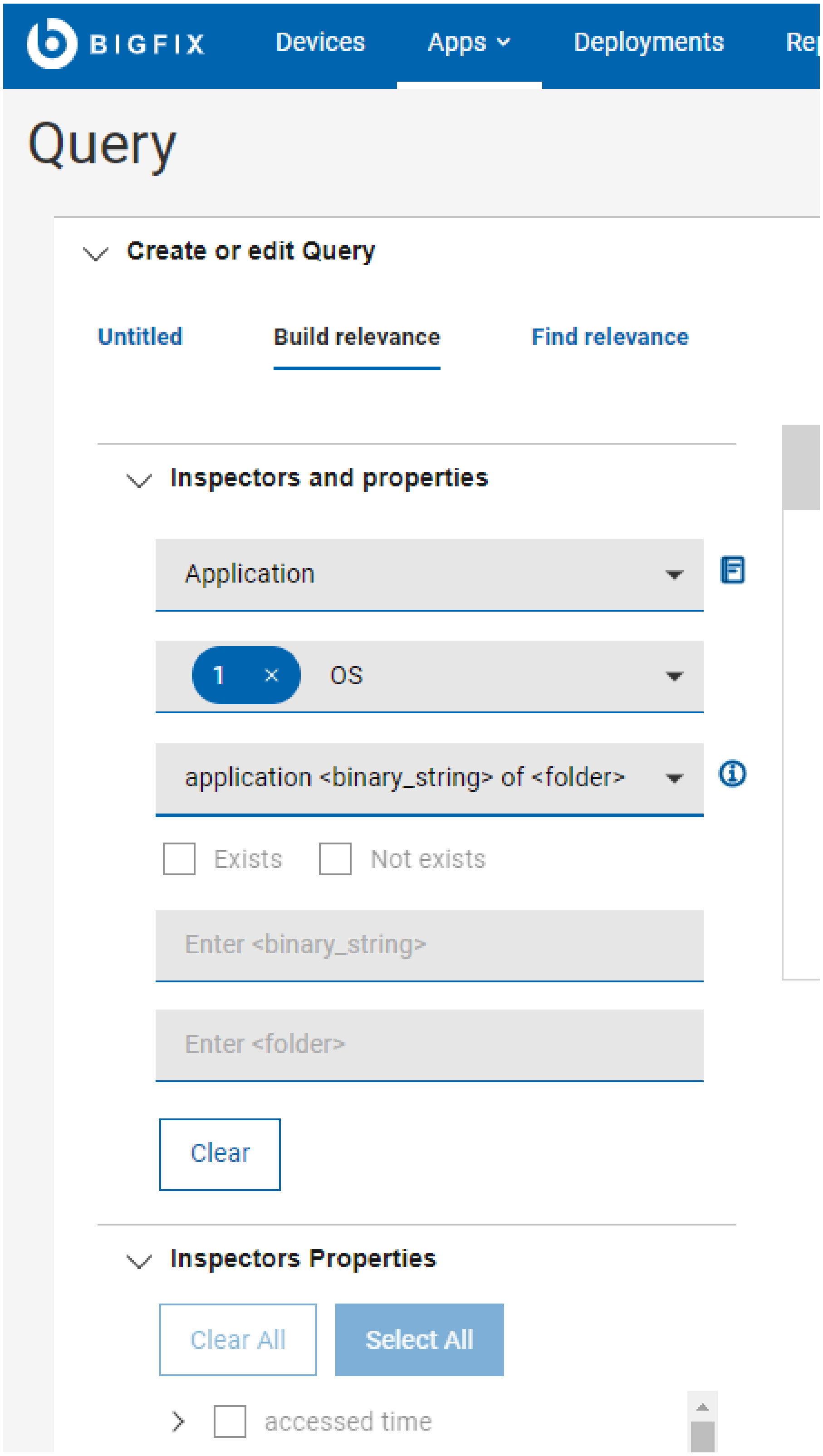
You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**"
For all conditions in a group to apply, select "**AND**"

c. Based on selected Inspector type and operating system, the applicable inspectors are filtered out. From the third drop down, select the inspector value.



- If the selected inspector is parameterized, you can enter the value of the parameter in the **Enter Parameter** text box.

Note: Currently Inspectors with maximum 2 parameters are supported.



Application

OS

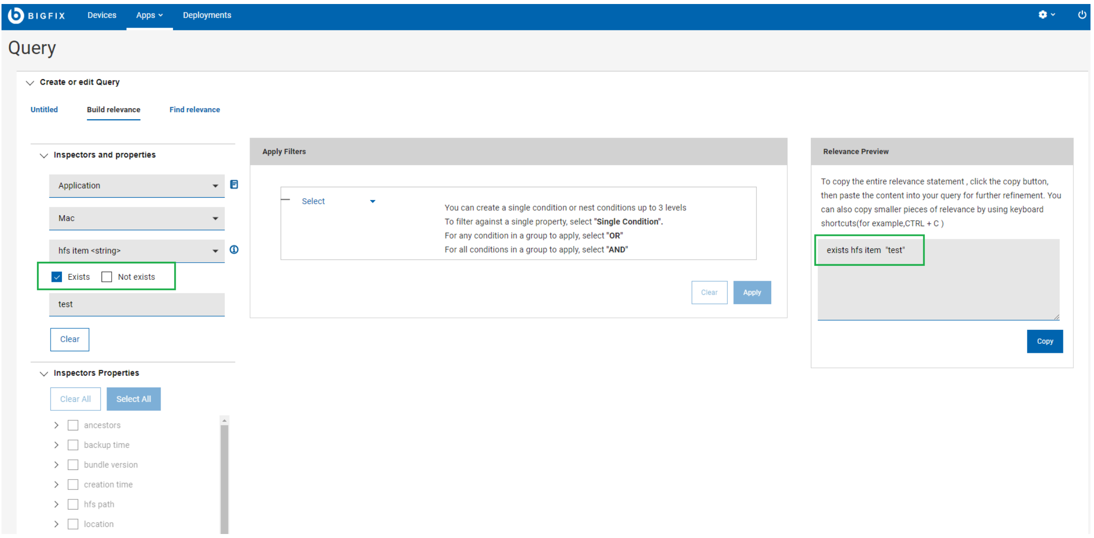
application <binary_string> of <folder>

- If the selected inspector is not parameterized, the **Enter Parameter** text box is disabled.

d. **Exist** and **Not Exist** keywords are supported in build relevance. The usage is supported in three different positions in Buid relevance:

- Inspectors and properties section: supports adding Exist/Not Exist to Inspectors
- Inspectors Properties section: supports adding Exist/Not Exist to Inspector Properties
- Apply Filter section: supports adding Exist/Not Exist to Filters

Selecting one of the checkboxes enables Apply Filters and disables Inspectors Properties as it is shown in the following image .

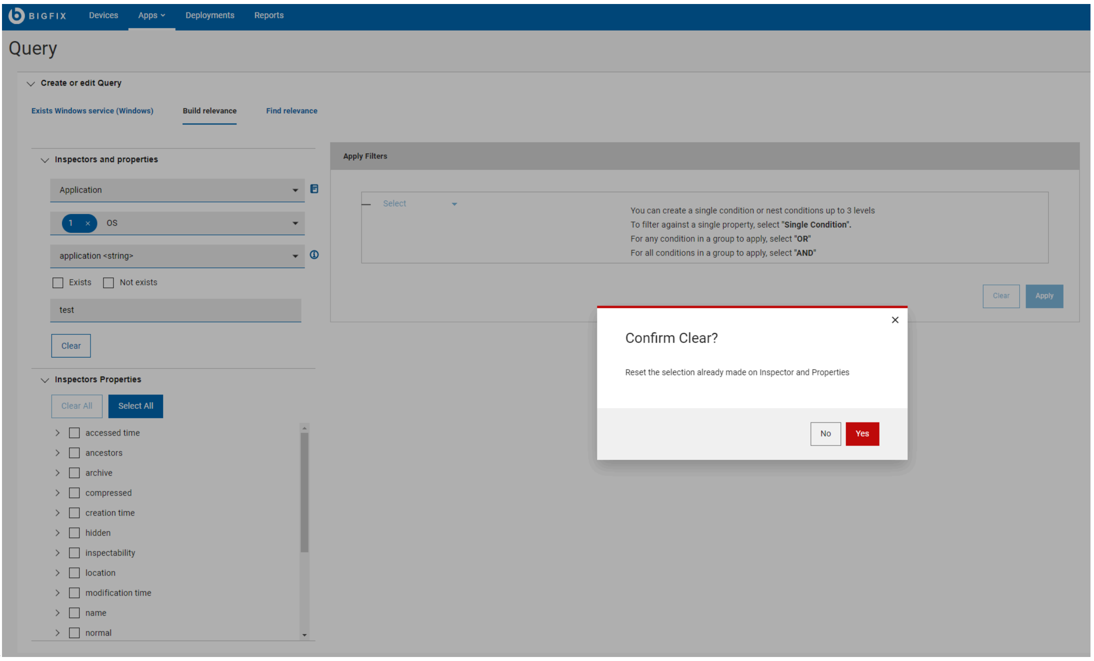


You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**"
For all conditions in a group to apply, select "**AND**"

To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

exists hfs item "test"

e. To remove the parameters, click **Clear** button and confirm clear.



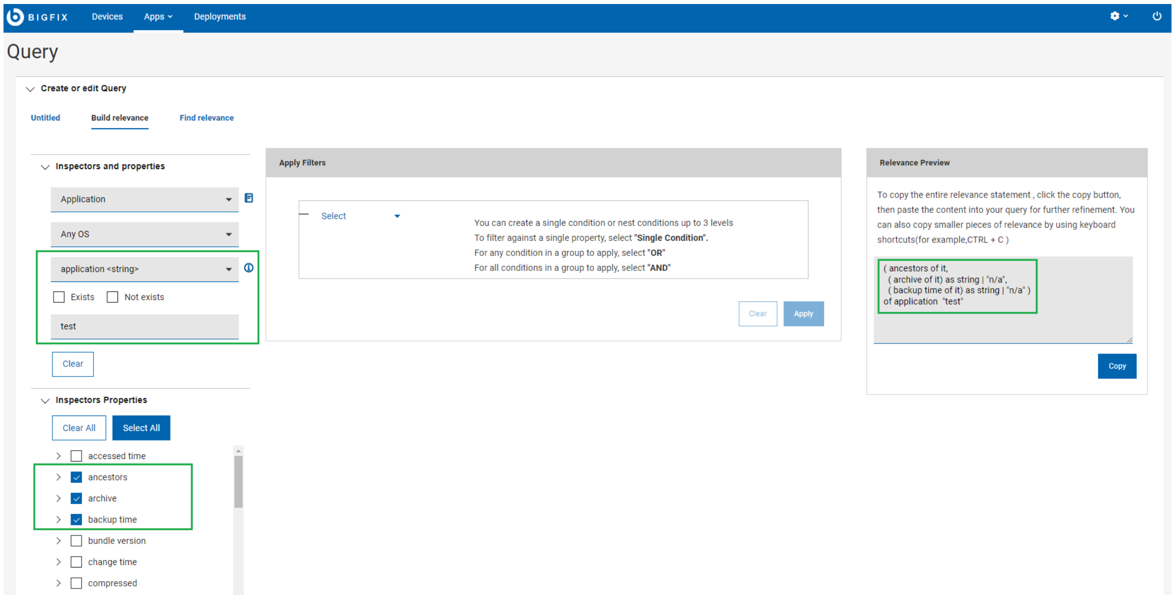
You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**"
For all conditions in a group to apply, select "**AND**"

Confirm Clear?

Reset the selection already made on Inspector and Properties

4. Based on the selected Inspectors value, the list of **Inspectors Properties** is populated. Select the properties you want the build relevance to return.

Note: Inspectors Properties dropdown list is enabled only when **Exists** or **Not Exists** checkbox is not selected.

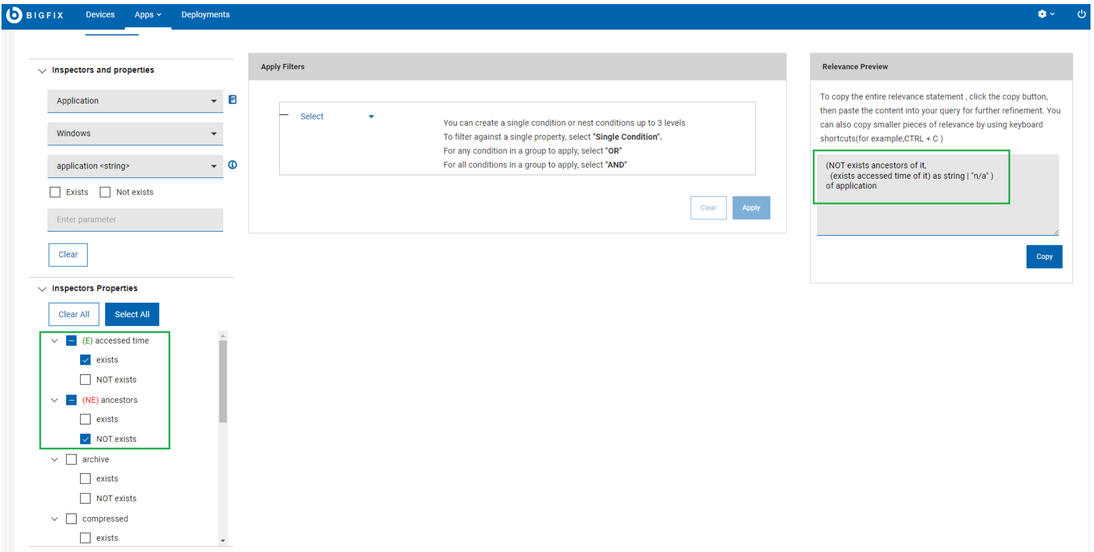


You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**"
For all conditions in a group to apply, select "**AND**"

To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

```
( ancestors of it,
  ( archive of it) as string | "n/a",
  ( backup time of it) as string | "n/a" )
of application  "test"
```

- Each of the Property has **Exist** and **Not Exist** as options. Once you select **Exist** or **Not Exist** , **E** (for Exist) or **NE** (Not Exist) appears next to the Property.



You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**"
For all conditions in a group to apply, select "**AND**"

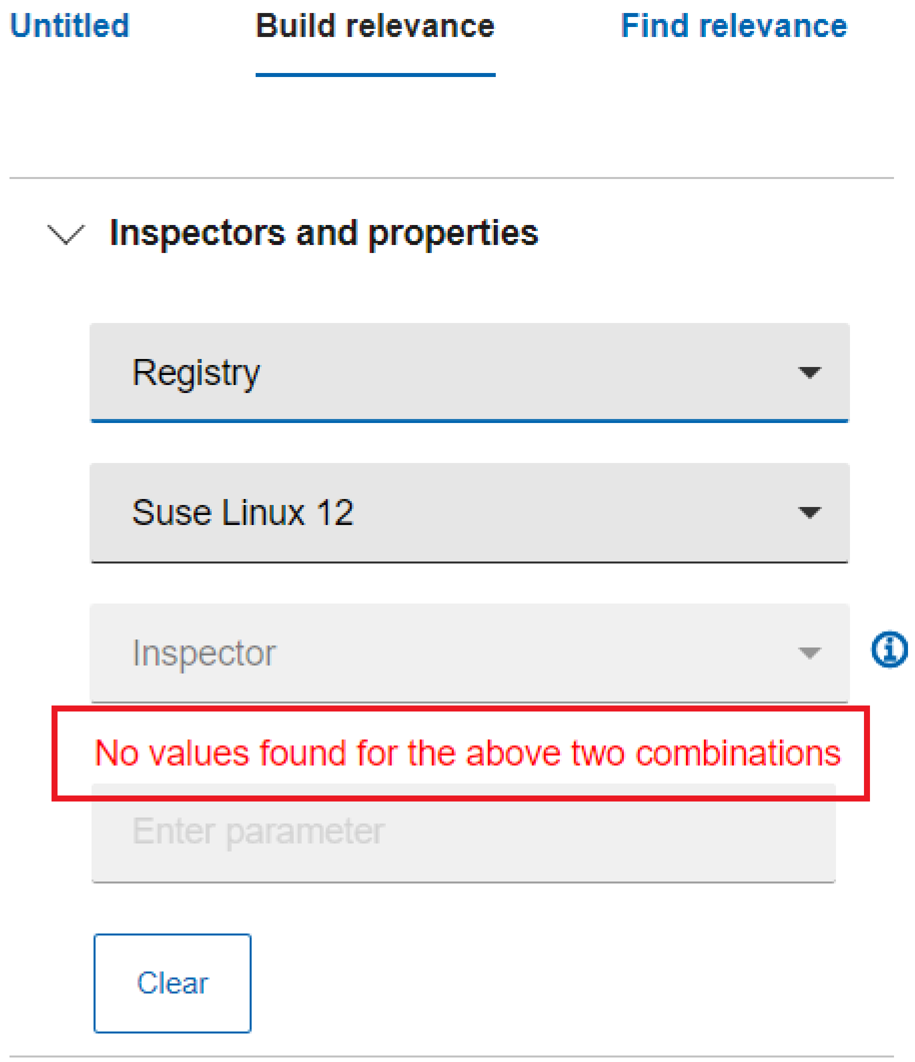
To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

```
(NOT exists ancestors of it,
  (exists accessed time of it) as string | "n/a" )
of application
```

- To select all the properties, click **Select All**
- To clear all the selected properties, click **Clear All**

Note:

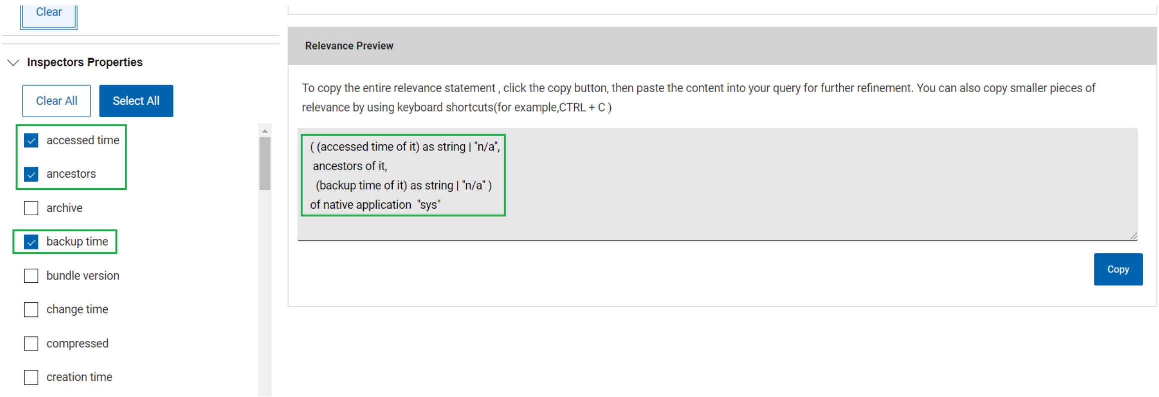
- Changing the selection of inspector type or operating system results in fetching new Inspectors values. Thus, results in generating new Inspectors Properties.
- If the selected combination of inspector type and operating system does not have any relevant Inspector value, the following message appears:



No values found for the above two combinations

Note: There is no validation of the correctness of inspector parameter.

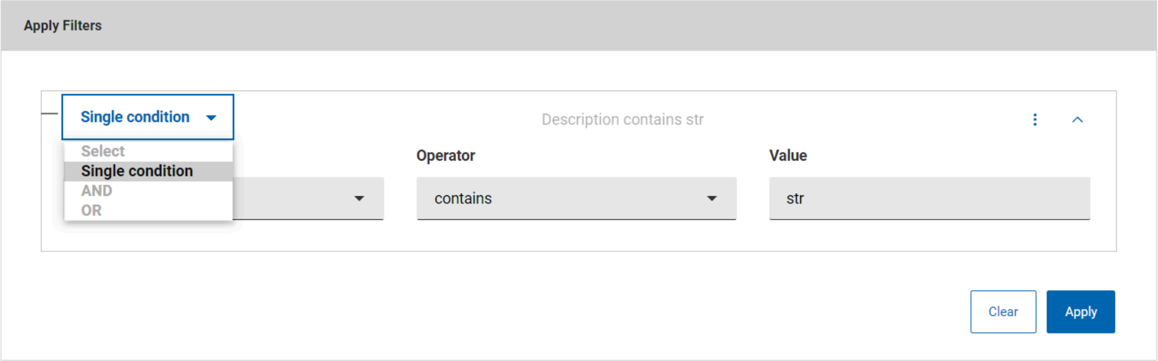
5. Select the checkboxes from Inspectors Properties. In the **Relevance Preview** box you can see the Relevance expression for the selected combination of inspectors and properties.



To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

```
( (accessed time of it) as string | "n/a",
 ancestors of it,
  (backup time of it) as string | "n/a" )
of native application  "sys"
```

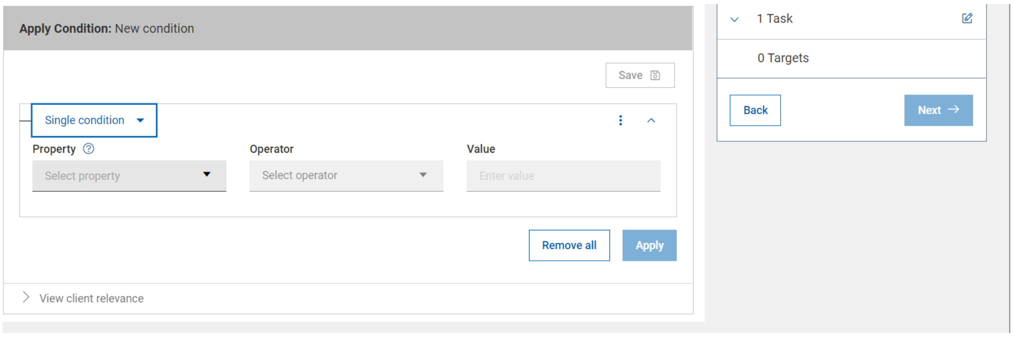
6. **Apply filters**: You can also combine conditions to filter your search and build the Relevance expression. You can create a single condition or nested conditions **up to 3 levels**.



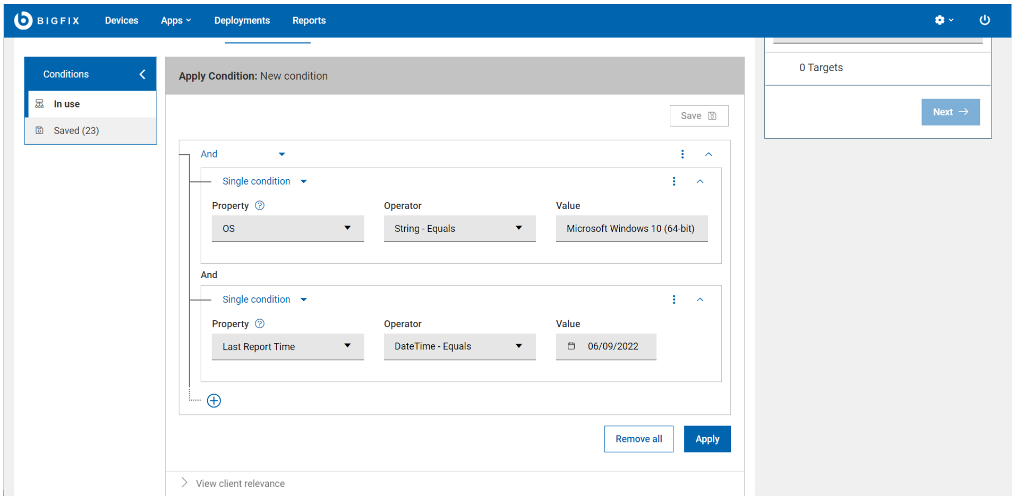
To add condition to the selected Inspectors and Properties to build Relevance expression:

a. From the **Apply Filters** section, select:

- **Single condition**: to define a single condition and filter against a single property.



- **AND**: To define multiple conditions where **all** of the specified conditions need to match.



Apply Condition: New condition

And

Single condition

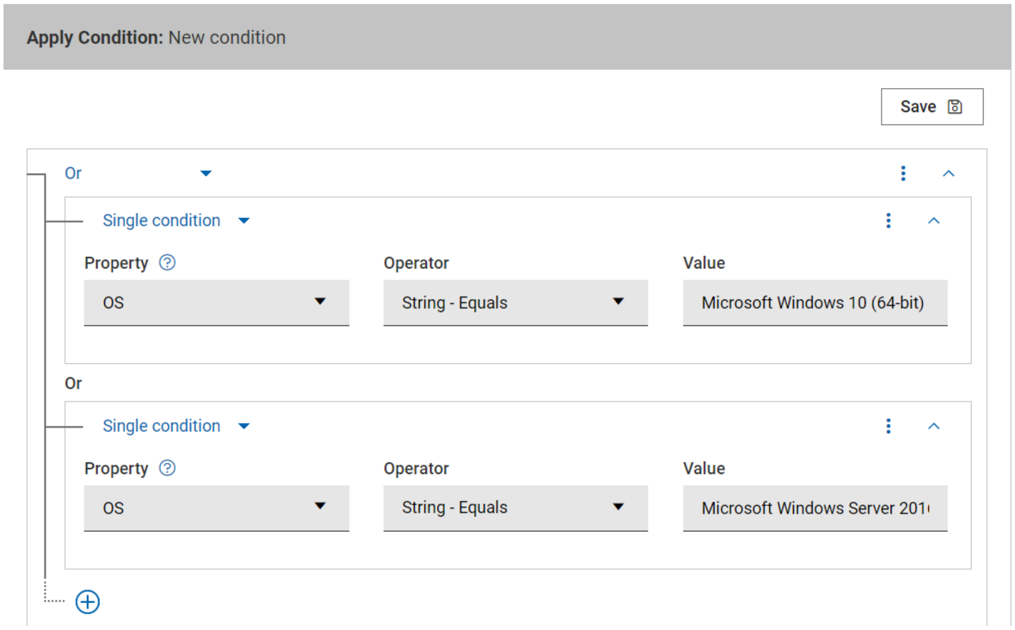
Property	Operator	Value
OS	String - Equals	Microsoft Windows 10 (64-bit)

And

Single condition

Property	Operator	Value
Last Report Time	DateTime - Equals	06/09/2022

- **OR** : To define multiple conditions where **any** of the specified conditions can match.



Apply Condition: New condition

Or

Single condition

Property	Operator	Value
OS	String - Equals	Microsoft Windows 10 (64-bit)

Or

Single condition

Property	Operator	Value
OS	String - Equals	Microsoft Windows Server 201

Note: You can add/remove conditions with the kebab menu on the top right corner

⋮

.

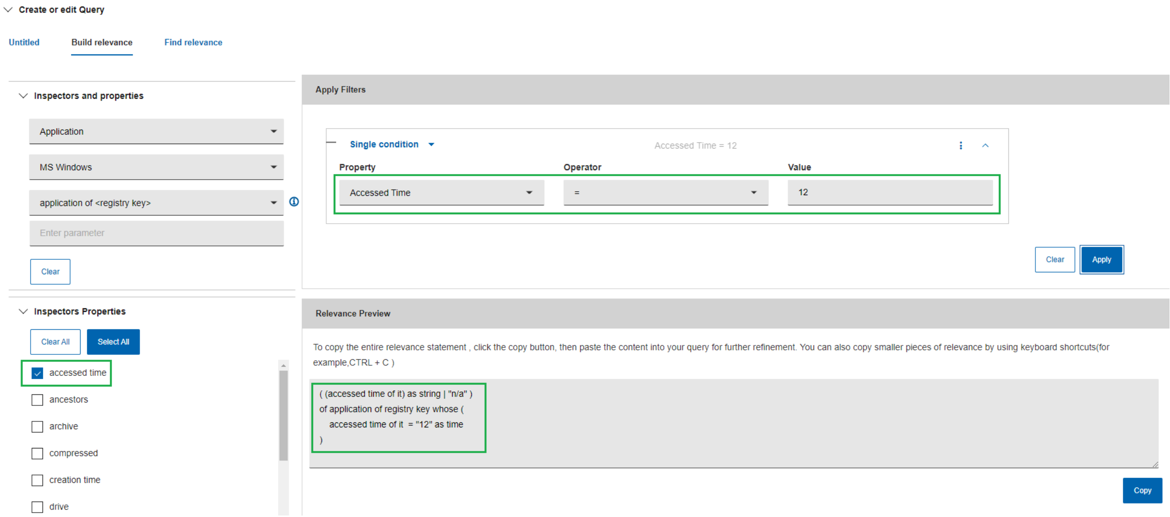
Note: Depending on the property value, number of operators available for the filtering conditions may differ:

- Operators available for integer values: =, <, >, >=, <=, Exist, Not Exist
- Operators available for boolean values: =, Exist, Not Exist

- Operators available for time values: =, contains, starts with, Exist, Not Exist
- Operators available for string values: =, contains, starts with, Exist, Not Exist

b. Click **Apply**.

In the **Relevance Preview** box, you can see the Relevance expression for the selected combination of inspectors and properties combined with the filters applied. You can click **Copy** to copy this Relevance expression and paste it in the Query editor to build a new query. To clear the filters, click **Clear** button. Click **Yes** to confirm clear in the pop up window.



Application

MS Windows

application of <registry key>

Enter parameter

☑ accessed time
□ ancestors
□ archive
□ compressed
□ creation time
□ drive

Property: Accessed Time
Operator: =
Value: 12

To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

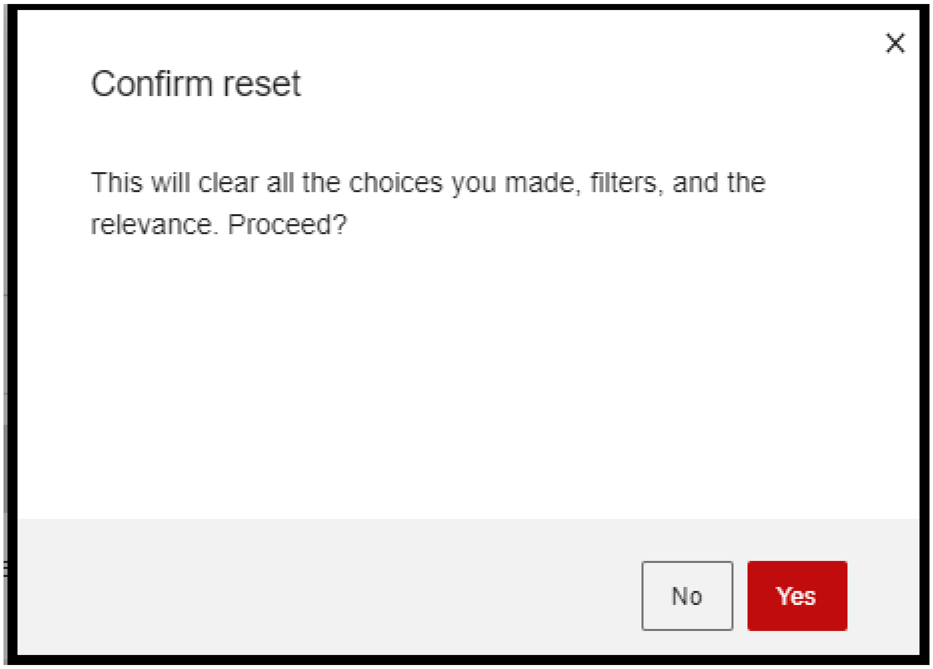
```
( (accessed time of it) as string | "n/a" )
of application of registry key whose (
   accessed time of it  = "12" as time
)
```

Note: There is no validation of the correctness of the final relevance syntax.

Clear Relevance expression

You can clear the Relevance expression from the preview box in the following ways:

- Click **Reset** button under **Relevance Preview** window. Click **Yes** to confirm reset when the pop up window appears.

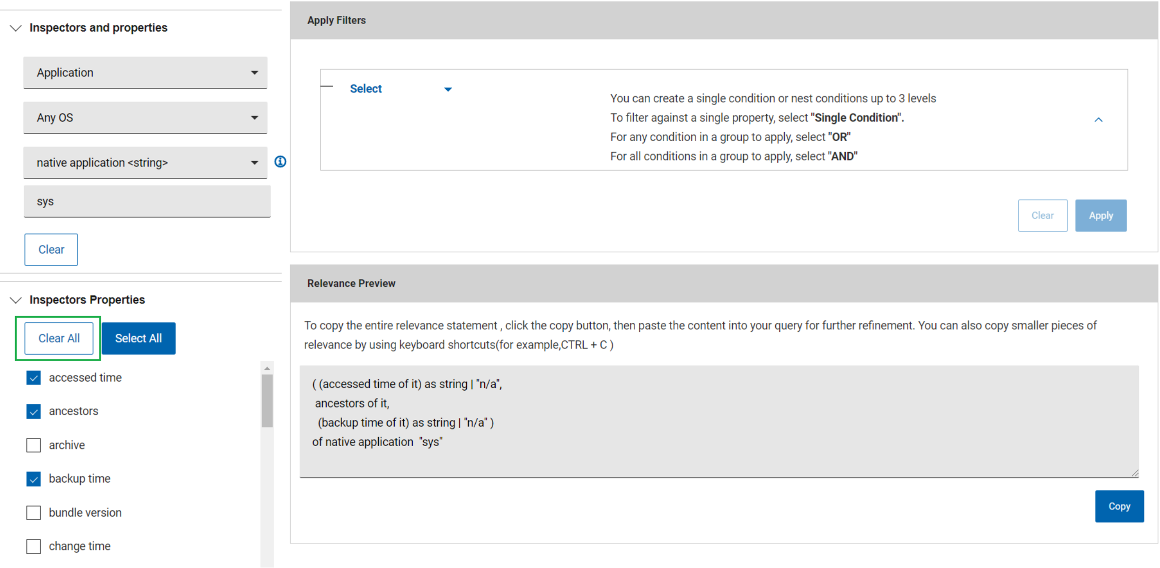


Confirm reset

This will clear all the choices you made, filters, and the relevance. Proceed?

Note: Reset button clears Relevance preview, Inspector Properties and Apply filters.

- Deselect checkboxes in the **Inspectors Properties**
- Click **Clear All** button to remove all the Inspectors Properties and thereby the Relevance statement from the Relevance Preview window.



You can create a single condition or nest conditions up to 3 levels
To filter against a single property, select **"Single Condition"**.
For any condition in a group to apply, select **"OR"**
For all conditions in a group to apply, select **"AND"**

To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

```
( (accessed time of it) as string | "n/a",
 ancestors of it,
  (backup time of it) as string | "n/a" )
of native application  "sys"
```

Find relevance

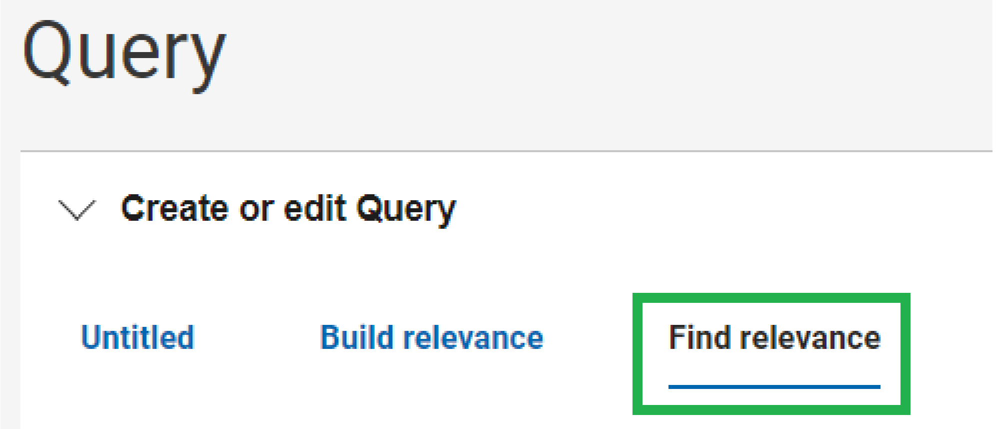
From the Find relevance tab, you can fetch the Relevance content from BES server. Master Operators/Content Creators can search for the properties or fixlets and tasks from the BES server with the key words.

Important: Web reports must be up and running to view and work with **Find relevance**.

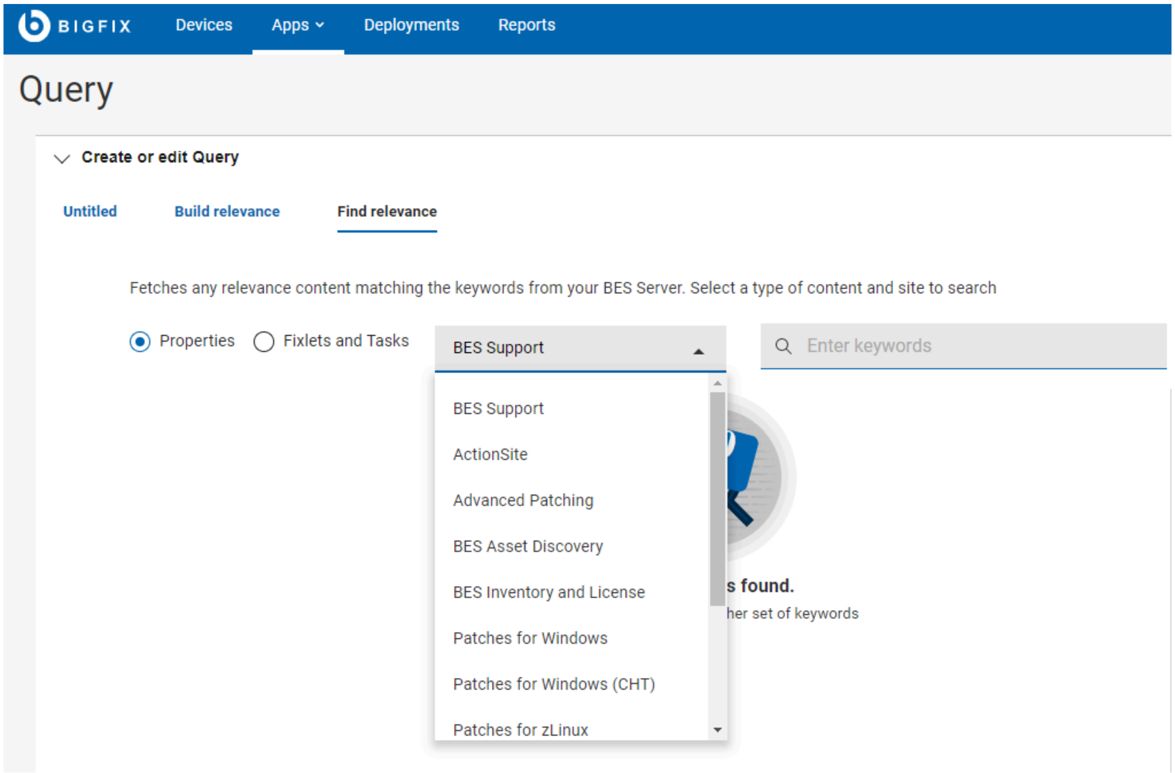
Note: Depending on your device resolution, the layout of the Query tabs differs. Refer to the link *(on page 101)* to find more information on supported resolutions.

To find the relevance, do the following:

1. In the Query editor, go to **Find relevance** tab.



2. Select **Properties** or **Fixlets and Tasks**.
3. Select a **Site** from the dropdown list. By default, the site is set to BES Support. The search includes the custom sites.



Fetches any relevance content matching the keywords from your BES Server. Select a type of content and site to search

● Properties ○ Fixlets and Tasks

BES Support

Enter keywords

- BES Support
- ActionSite
- Advanced Patching
- BES Asset Discovery
- BES Inventory and License
- Patches for Windows
- Patches for Windows (CHT)
- Patches for zLinux

s found.

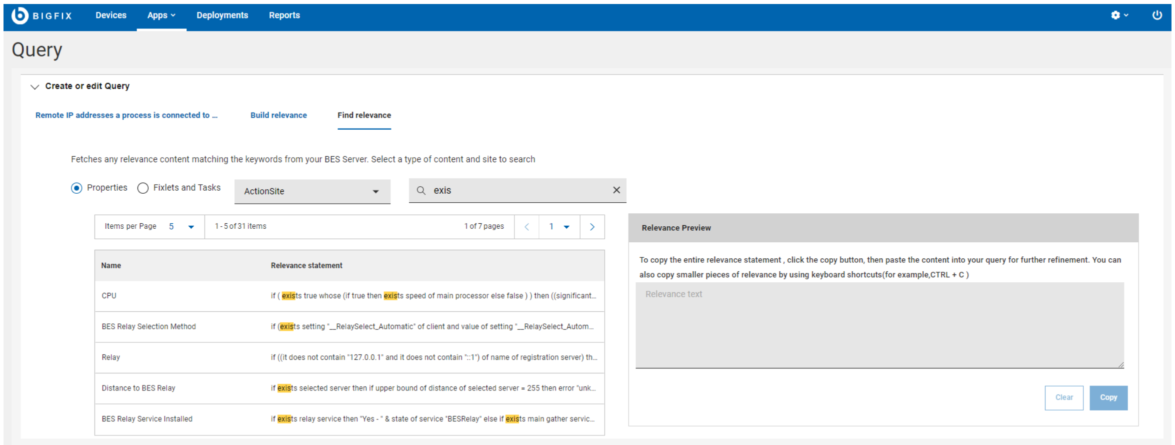
her set of keywords

Note: The sites available in the drop down are all the available external BigFix sites the Content Creator is entitled to see, plus the ActionSite if the operator is a Master Operator.

4. Enter any keyword in the search box and press **Enter** to see the results. All matching **Fixlets and Tasks** or **Properties** (as selected) along with the Relevance statements appear in a result set with the specified string highlighted.

   To see the Relevance preview, click the associated row.

   You can also copy the Relevance statement from the Relevance preview text box and paste it in the **Untitled** tab in the Query editor to save as a new query or run the query.



Fetches any relevance content matching the keywords from your BES Server. Select a type of content and site to search

● Properties ○ Fixlets and Tasks ActionSite exis

Items per Page 5 1 - 5 of 31 items 1 of 7 pages 1

Name	Relevance statement
CPU	if (exists true whose (if true then exists speed of main processor else false)) then ((significant...
BES Relay Selection Method	if (exists setting "__RelaySelect_Automatic" of client and value of setting "__RelaySelect_Autom...
Relay	if ((it does not contain "127.0.0.1" and it does not contain "::1") of name of registration server) th...
Distance to BES Relay	if exists selected server then if upper bound of distance of selected server = 255 then error "unk...
BES Relay Service Installed	if exists relay service then "Yes - " & state of service "BESRelay" else if exists main gather servic...

Relevance Preview

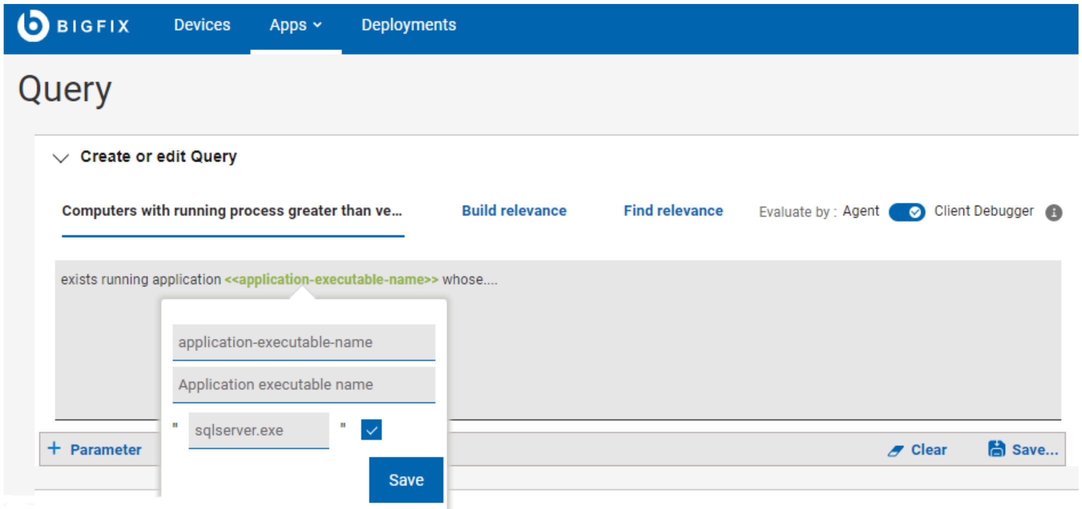
To copy the entire relevance statement , click the copy button, then paste the content into your query for further refinement. You can also copy smaller pieces of relevance by using keyboard shortcuts(for example,CTRL + C)

Note: In case a property belongs to an analysis, the Name column for **Properties** is formatted in the following way: *(name_of_the_analysis) name_of_the_property*. In other cases, it is just the name of the property. For **Fixlets and Tasks** it is always the name of the fixlet/task.

Managing parameters in queries

As a Content Creator, you can add parameters to a query to customize it at run time. Operators are prompted to assign values to the parameters when they run the query, but they cannot see the Relevance expression.

- To add a parameter, do the following steps:
    1. In the query editor, ensure you are in Edit view for the **+Parameter** button to be enabled.
    2. In the Query editor, place the cursor at the point where you want to add the parameter in the Relevance expression and click **Parameter**.



exists running application <<application-executable-name>> whose....

application-executable-name

Application executable name

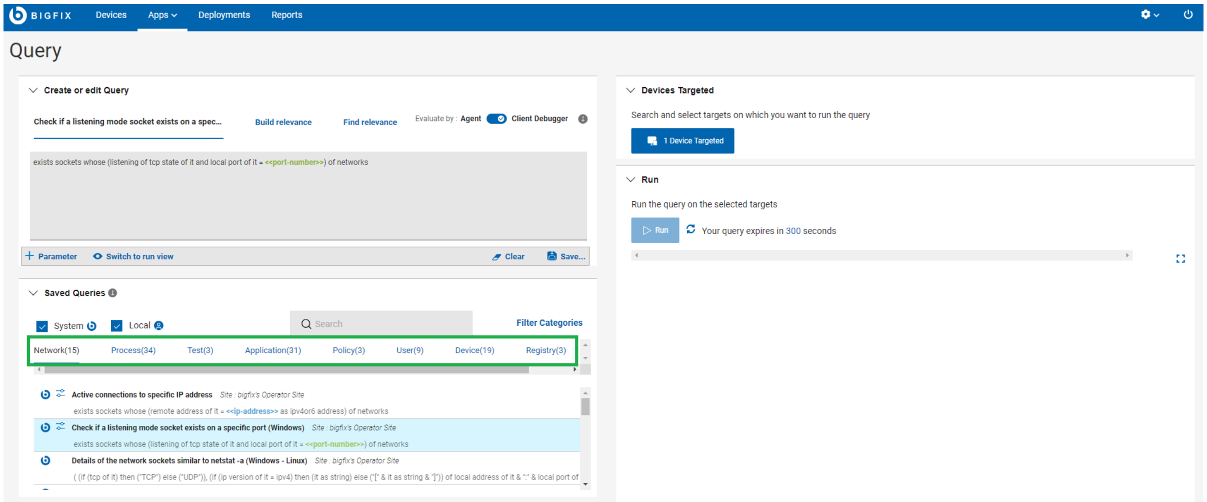
" sqlserver.exe " ☑

3. Enter **Parameter ID**, **Parameter Label**, and **Default Value** and click **Save**.

The parameter is added to the Relevance expression.

- To reuse a parameter, do the following steps:
    1. Click **+Parameter** and enter the Parameter ID that you want to reuse; the Parameter Label and Default Value fields are populated automatically.
    2. To insert that parameter into the Relevance expression, click **Save** .
- To see the definition of a parameter, click on the parameter in the query editor.
- To delete a parameter from a query, select the parameter in the query editor, and press the Backspace or Delete key.
- To assign a value to a parameter (that does not have a default value) at run time as a Content Creator, click **Operator View**.

The following graphic shows how a Content Creator sees a query with parameters in the Edit view:



```
exists sockets whose (listening of tcp state of it and local port of it = <<port-number>>) of networks
```

Search and select targets on which you want to run the query

Run the query on the selected targets

Your query expires in 300 seconds

Active connections to specific IP address *Site : bigfix's Operator Site*
exists sockets whose (remote address of it = <<ip-address>> as ipv4or6 address) of networks

Check if a listening mode socket exists on a specific port (Windows) *Site : bigfix's Operator Site*
exists sockets whose (listening of tcp state of it and local port of it = <<port-number>>) of networks

Details of the network sockets similar to netstat -a (Windows - Linux) *Site : bigfix's Operator Site*
((if (tcp of it) then ("TCP") else ("UDP")), (if (ip version of it = ipv4) then (it as string) else ("[" & it as string & "]")) of local address of it & ":" & local port of

To review what Operators see when they select the query, click View.

To return to the Edit view, click Edit.

Chapter 10. Take Action: The Deploy Sequence

To deploy means to dispatch content such as applications, modules, updates, and patches to one or more endpoints. For example, by deploying a software, you install the software in the targeted endpoints. BigFix WebUI enables you to configure the content and the target devises to create a deployment and monitor the deployment status. The work flow including all the steps, processes, and activities that are required to create a deployment is collectively called as the Deploy Sequence.

Deploy Sequence Summary

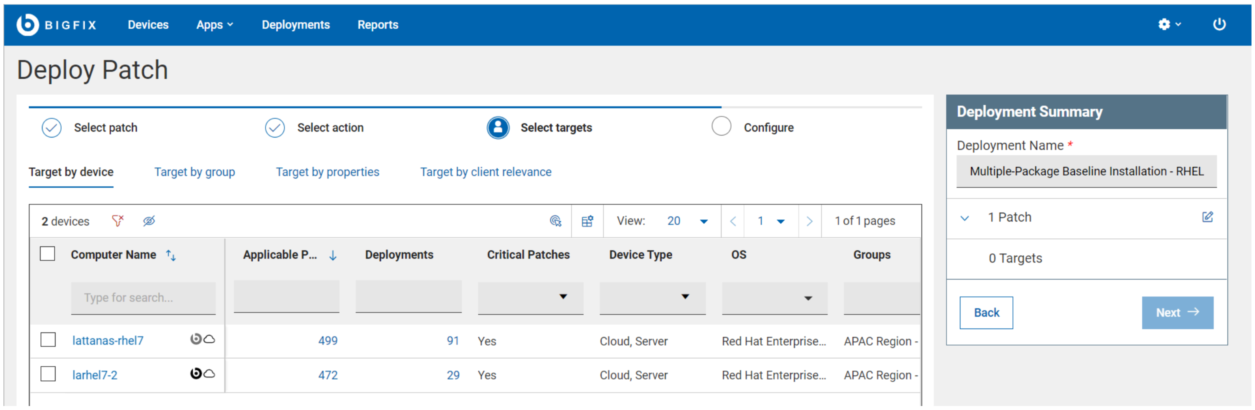
Deploy Sequence changes as per the entry point.

For example, if you start your deployment from the devices list, the sequence is as follows:

1. Select target devices.
2. Select content such as custom content, MDM action or policy, patch, software, or profile
3. Select action
4. Configure deployment options
5. Review and deploy

If you start your deployment from a content page, for example the Patch page, the sequence is as follows:

1. Select patch (or any other content)
2. Select action
3. Select target devices
4. Configure deployment options
5. Review and deploy



Deploy Patch

2 devices

View: 20 | 1 | 1 of 1 pages

Computer Name	Applicable P...	Deployments	Critical Patches	Device Type	OS	Groups
Type for search...						
lattanas-rhel7	499	91	Yes	Cloud, Server	Red Hat Enterprise...	APAC Region -
larhel7-2	472	29	Yes	Cloud, Server	Red Hat Enterprise...	APAC Region -

Deployment Summary

Deployment Name *

Multiple-Package Baseline Installation - RHEL

1 Patch

0 Targets

- The deploy sequence wizard consists of all the actions in different tabs. You can navigate between tabs at any point in time.
  - 👤 indicates the current action
  - ✓ indicates the completed actions
  - ○ indicates the actions that are yet to be completed.

Deployment Summary gives the overall summary of the deployment. It gives the complete details about the selected targets, contents, actions, and the configurations. You can click the edit button at any time to change the selections. The Next button lets you to move to the next step in the sequence. When all the steps are completed as per the requirements, the Deploy button is enabled. If you see disabled Deploy button review your selections and edit to fix the issues.

Prompts, status information, and selection tallies are shown in the Deployment Summary section. The status bar reflects your progress in the deploy sequence. Embedded help (question mark icon) is available for some options.

- **Target Limits**. An administrator can limit the amount of content that can be deployed at one time, and the number of devices you can deploy to or query at the same time. If you exceed it, a message displays until you reduce your selections to within the acceptable range. The message includes the target limit, for example, *"You have exceeded the maximum of 3 devices per deployment."*

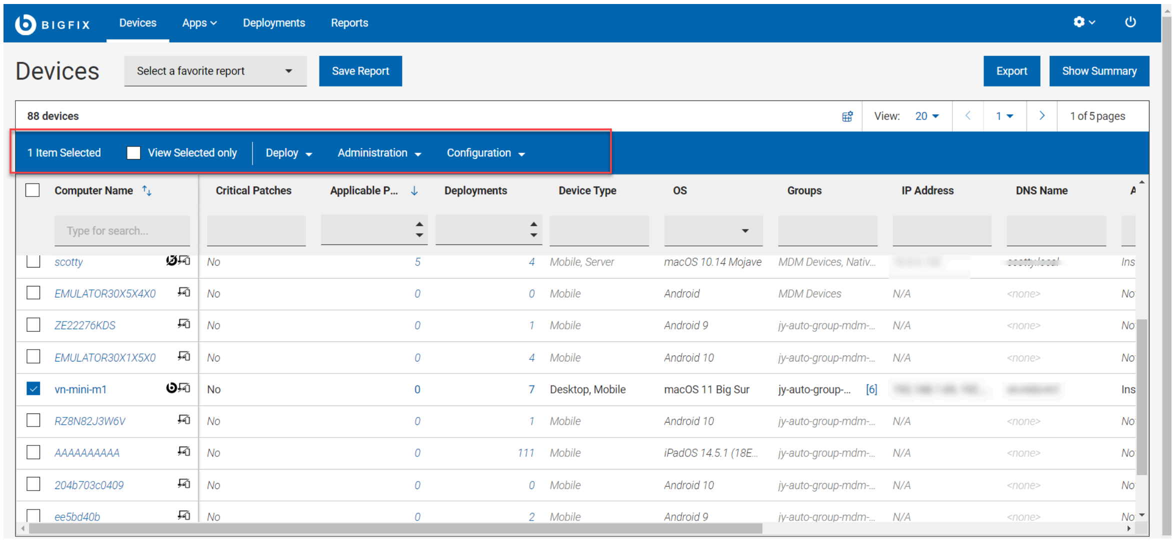
  Note: If there is a target limit defined, the Non-Master Operators (NMOs) affected cannot deploy actions using the *Target by Group* option.

- **Not all content can be deployed.** If non-deployable content (such as an audit action) is selected, you will be prompted to remove it from the deployment.
- **No Default Action** – If content without a default action is selected, you will be prompted to choose one.
- **Action Parameters Required** – If content that requires a parameter is selected, you will be prompted to supply one.

Deploy Procedure

Read this section to learn the steps to deploy content onto the devices.

1. Select devices or content for deployment; the blue action bar appears.

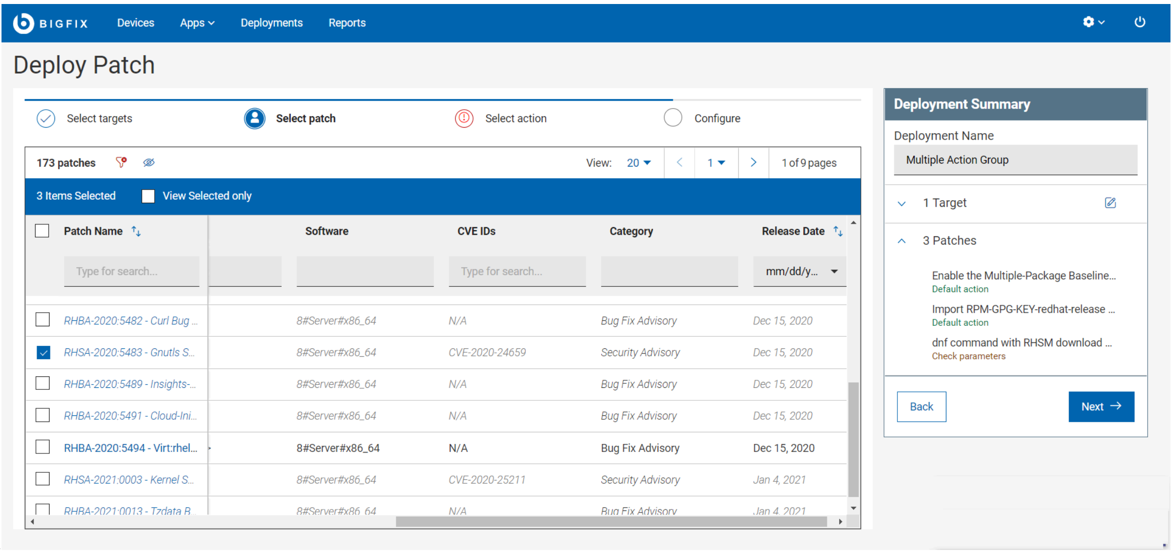


88 devices

1 Item Selected □ View Selected only

□	Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS	Groups	IP Address	DNS Name	A
	Type for search...									
□	scotty	No	5	4	Mobile, Server	macOS 10.14 Mojave	MDM Devices, Nativ...	[redacted]	[redacted]	Ins
□	EMULATOR30X5X4X0	No	0	0	Mobile	Android	MDM Devices	N/A	<none>	No
□	ZE22276KDS	No	0	1	Mobile	Android 9	jy-auto-group-mdm-...	N/A	<none>	No
□	EMULATOR30X1X5X0	No	0	4	Mobile	Android 10	jy-auto-group-mdm-...	N/A	<none>	No
☑	vn-mini-m1	No	0	7	Desktop, Mobile	macOS 11 Big Sur	jy-auto-group-... [6]	[redacted]	[redacted]	Ins
□	RZ8N82J3W6V	No	0	1	Mobile	Android 10	jy-auto-group-mdm-...	N/A	<none>	No
□	AAAAAAAAAA	No	0	111	Mobile	iPadOS 14.5.1 (18E...	jy-auto-group-mdm-...	N/A	<none>	No
□	204b703c0409	No	0	0	Mobile	Android 10	jy-auto-group-mdm-...	N/A	<none>	No
□	ee5bd40b	No	0	2	Mobile	Android 9	jy-auto-group-mdm-...	N/A	<none>	No

2. Select content or device targets, respectively; click **Next**.



173 patches

3 Items Selected □ View Selected only

□	Patch Name	Software	CVE IDs	Category	Release Date
	Type for search...		Type for search...		mm/dd/y...
□	RHBA-2020:5482 - Curl Bug ...	8#Server#x86_64	N/A	Bug Fix Advisory	Dec 15, 2020
☑	RHSA-2020:5483 - Gnutls S...	8#Server#x86_64	CVE-2020-24659	Security Advisory	Dec 15, 2020
□	RHBA-2020:5489 - Insights-...	8#Server#x86_64	N/A	Bug Fix Advisory	Dec 15, 2020
□	RHBA-2020:5491 - Cloud-Ini...	8#Server#x86_64	N/A	Bug Fix Advisory	Dec 15, 2020
□	RHBA-2020:5494 - Virt:rhel...	8#Server#x86_64	N/A	Bug Fix Advisory	Dec 15, 2020
□	RHSA-2021:0003 - Kernel S...	8#Server#x86_64	CVE-2020-25211	Security Advisory	Jan 4, 2021
□	RHBA-2021:0013 - Tzdata B...	8#Server#x86_64	N/A	Bug Fix Advisory	Jan 4, 2021

Deployment Summary

Deployment Name: Multiple Action Group

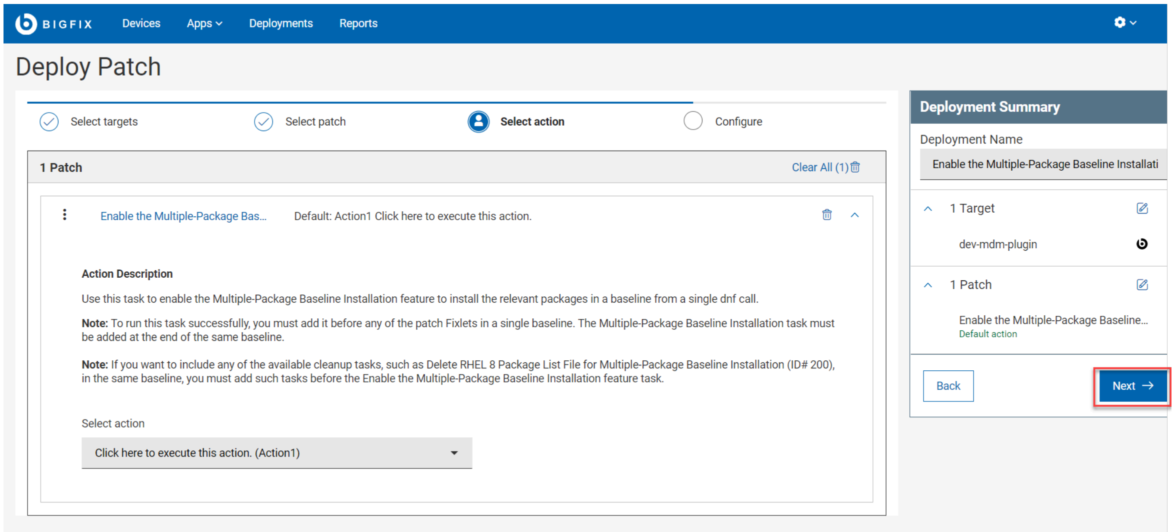
1 Target

3 Patches

- Enable the Multiple-Package Baseline...
  Default action
- Import RPM-GPG-KEY-redhat-release ...
  Default action
- dnf command with RHSM download ...
  Check parameters

   - Use the List views, filter, and search tools to find the records you want.
   - Review the device and documents to ensure that you understand their effects.
   - Alternatively, you can deploy an action directly from the Software Document as described in Software Documents *(on page 87)*.

3. The Select actions tab displays Tasks, Patches or Software depending on the App you are working with. To expand and see the complete description, click the caret symbol.



Deploy Patch

Select targets | Select patch | Select action | Configure

1 Patch — Clear All (1)

Enable the Multiple-Package Bas... Default: Action1 Click here to execute this action.

Action Description

Use this task to enable the Multiple-Package Baseline Installation feature to install the relevant packages in a baseline from a single dnf call.

Note: To run this task successfully, you must add it before any of the patch Fixlets in a single baseline. The Multiple-Package Baseline Installation task must be added at the end of the same baseline.

Note: If you want to include any of the available cleanup tasks, such as Delete RHEL 8 Package List File for Multiple-Package Baseline Installation (ID# 200), in the same baseline, you must add such tasks before the Enable the Multiple-Package Baseline Installation feature task.

Select action: Click here to execute this action. (Action1)

Deployment Summary

Deployment Name: Enable the Multiple-Package Baseline Installati

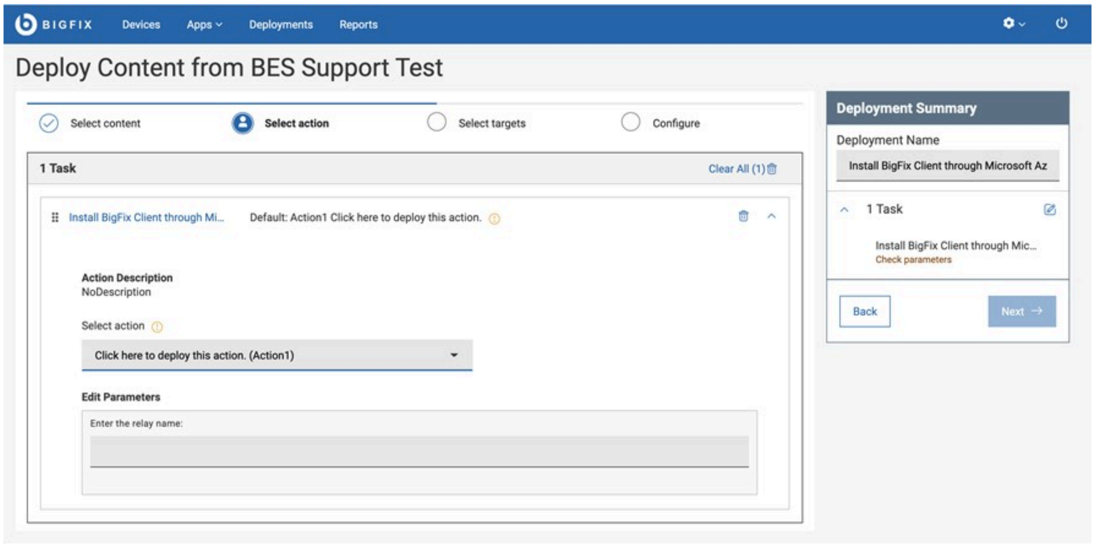
1 Target: dev-mdm-plugin

1 Patch: Enable the Multiple-Package Baseline... Default action

Back | Next →

4. If the "Require decision" or "Non-deployable" prompts display, one or more actions require input.
   - One or more actions require attention

   a. Click the **Selected** actions link (Tasks, Patches, or Software) to open the Decision dialog.



Deploy Content from BES Support Test

Select content | Select action | Select targets | Configure

1 Task — Clear All (1)

Install BigFix Client through Mi... Default: Action1 Click here to deploy this action.

Action Description
NoDescription

Select action: Click here to deploy this action. (Action1)

Edit Parameters

Enter the relay name:

Deployment Summary

Deployment Name: Install BigFix Client through Microsoft Az

1 Task: Install BigFix Client through Mic... Check parameters

Back | Next →

Note: Multiple Action Groups can be reordered by clicking and dragging individual actions. This is a feature of the BigFix® WebUI that cannot be performed in the traditional BigFix® console.

i. Specify any missing default actions.
   - Fixlets with no default and multiple actions: Select an action from the drop-down list. For example, a single software package might be used to both install and uninstall an application.
   - Fixlets with no default and a single action:

1. Review the content document. The Fixlet® author is saying, "Proceed with caution." Pay close attention to any Notes®, Warnings, or Known Issues in the document and make an informed decision.
2. To remove the action, click the x next to its name. To deploy the action, select "Click here to initiate the deployment process" from the drop-down list.

ii. Enter action parameters as required.

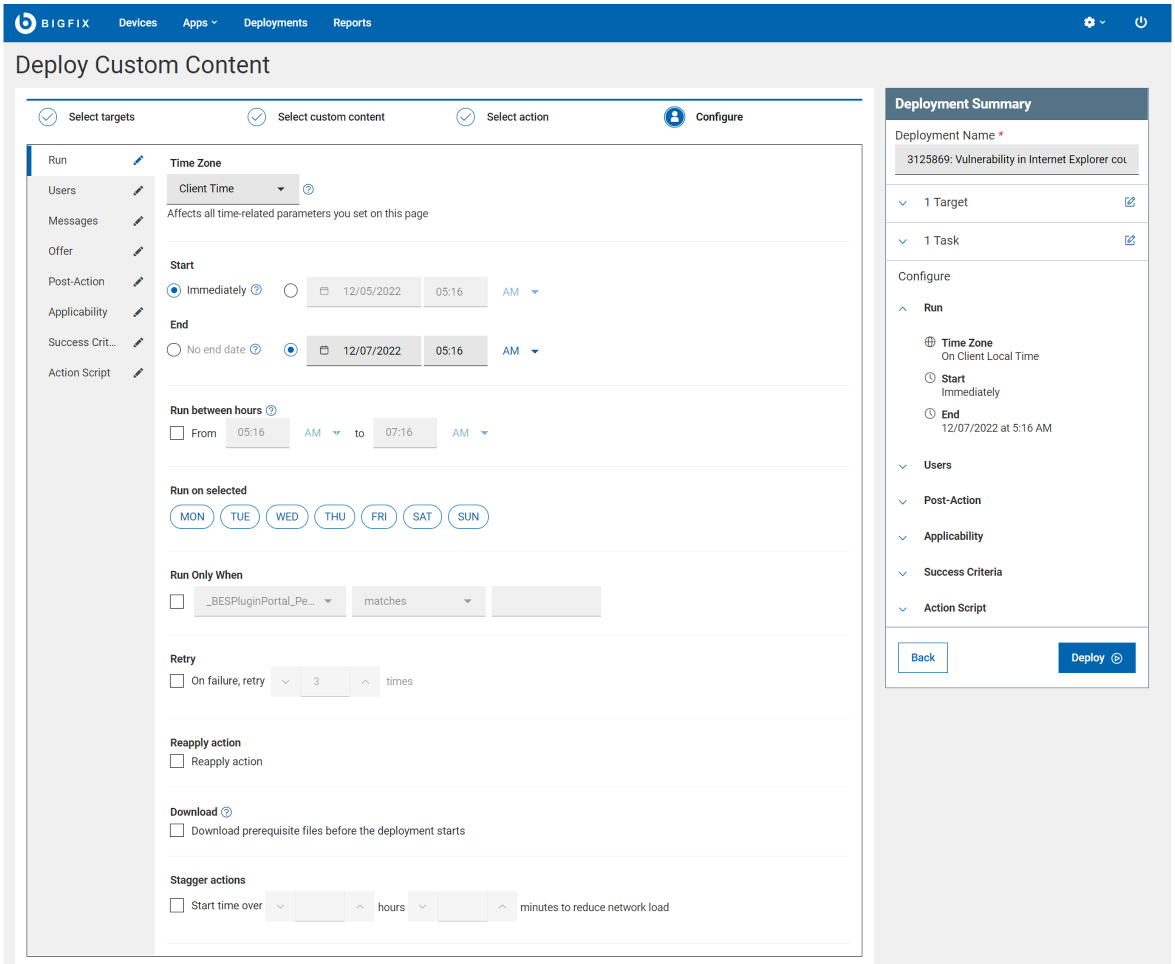
1. Select the action that is presented in the drop-down list to display the **Enter Parameters** link.
2. Click **Enter Parameters** and type in the required information, such as a path name or service name.

iii. Remove any non-deployable actions, such as audits or superseded patches.

b. Click **Apply** to return to the deploy sequence.

c. Click **Next** to open the Configuration page.

5. Select configuration options for the deployment; click **Next**. See Configuration Options *(on page 140)* for descriptions of each option.



Deploy Custom Content

Time Zone: Client Time
Affects all time-related parameters you set on this page

Start
● Immediately ○ 12/05/2022 05:16 AM

End
○ No end date ● 12/07/2022 05:16 AM

Run between hours
□ From 05:16 AM to 07:16 AM

Run on selected

Run Only When
□ _BESPluginPortal_Pe... matches

Retry
□ On failure, retry 3 times

Reapply action
□ Reapply action

Download
□ Download prerequisite files before the deployment starts

Stagger actions
□ Start time over hours minutes to reduce network load

Deployment Summary

Deployment Name *
3125869: Vulnerability in Internet Explorer cou

1 Target

1 Task

Configure

Run
Time Zone
On Client Local Time
Start
Immediately
End
12/07/2022 at 5:16 AM

Users

Post-Action

Applicability

Success Criteria

Action Script

6. Review your selections from the Deployment Summary. Use the **Edit** icon to make any adjustments.

> **Note:** Deploy button is enabled only if all the steps have correct and compatible data. Otherwise, it is disable, review and correct it to proceed with deployment.

7. Click **Deploy**.

8. Monitor deployment results from The Deployment List *(on page 146)*.

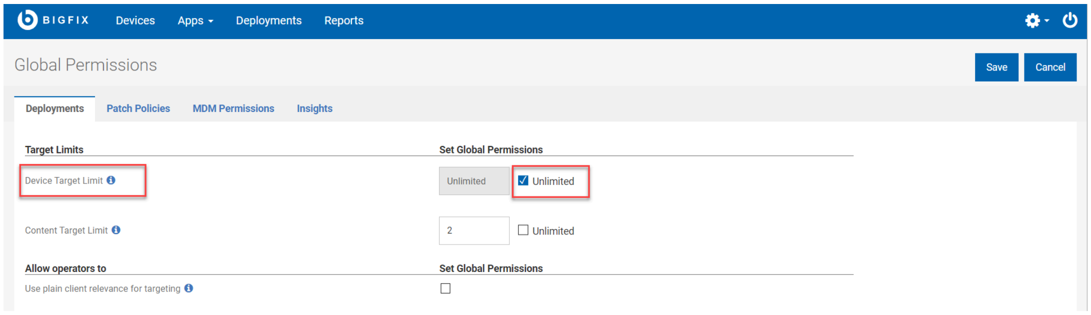
Selecting targets

You can select targets in several ways to deploy patches or content through WebUI.

In the **Deployment sequence** wizard, when your current action is **Select targets**, the following tabs are displayed that correspond to target selection methods:

- **Target by device**. Select target devices from the device grid.
- **Target by group**. Select one or more groups of target devices.
- **Target by properties**. Dynamically filter and select only a specific set of target devices that satisfy one or more conditions defined based on their BigFix properties. For the procedure, see Targeting devices by properties *(on page 135)*.

  > **Important:** This tab is visible only for users who have the Permission `Device Target Limit` set to `unlimited` in the Global Permissions or in the Permissions of user's assigned role.



Global Permissions

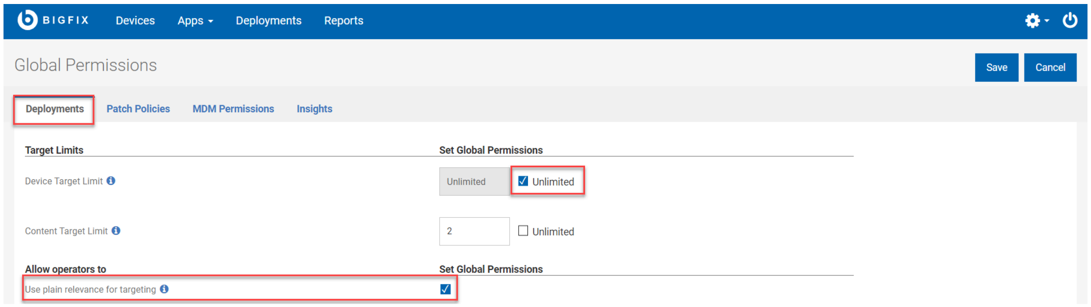
Target Limits	Set Global Permissions	
Device Target Limit	Unlimited	☑ Unlimited
Content Target Limit	2	☐ Unlimited

Allow operators to	Set Global Permissions
Use plain client relevance for targeting	☐

- **Target by relevance**. Use a plain client relevance that you trust for your targeting. For the procedure, see Targeting devices by relevance *(on page 139)*.

  > **Important:** This tab is visible only for users who have the following permissions enabled in the Global Permissions or in the Permissions of user's assigned role:

- `Device Target Limit` set to `Unlimited`.
- Allow operators to `Use plain relevance for targeting`



Device Target Limit: Unlimited ☑ Unlimited

Content Target Limit: 2 □ Unlimited

Use plain relevance for targeting ☑

Related information

Configuration Options *(on page 140)*

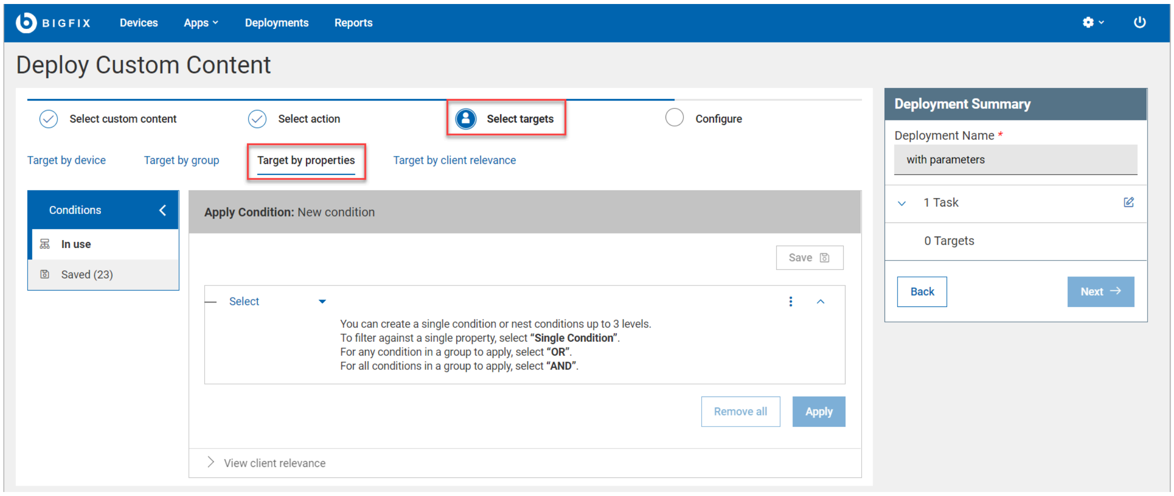
Targeting devices by properties

You can dynamically filter and select a specific set of target devices that satisfy one or more defined conditions based on their BigFix properties.

You can create a Target by properties condition with reserved properties (already present in BigFix) and also with custom properties (created by users). You can define a single condition or build nested conditions using AND and OR statements.

To define conditions:

1. On the deploy sequence, when you are in **Select targets** action, select the **Target by properties** tab.



Deployment Name *: with parameters

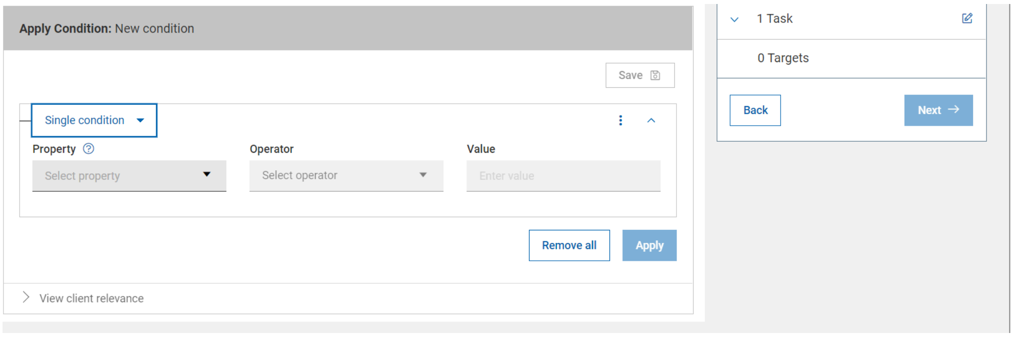
You can create a single condition or nest conditions up to 3 levels.
To filter against a single property, select "**Single Condition**".
For any condition in a group to apply, select "**OR**".
For all conditions in a group to apply, select "**AND**".

2. Click **Apply Condition**. You can filter targets based on their properties by defining a single condition or by combining conditions using AND and OR operators.

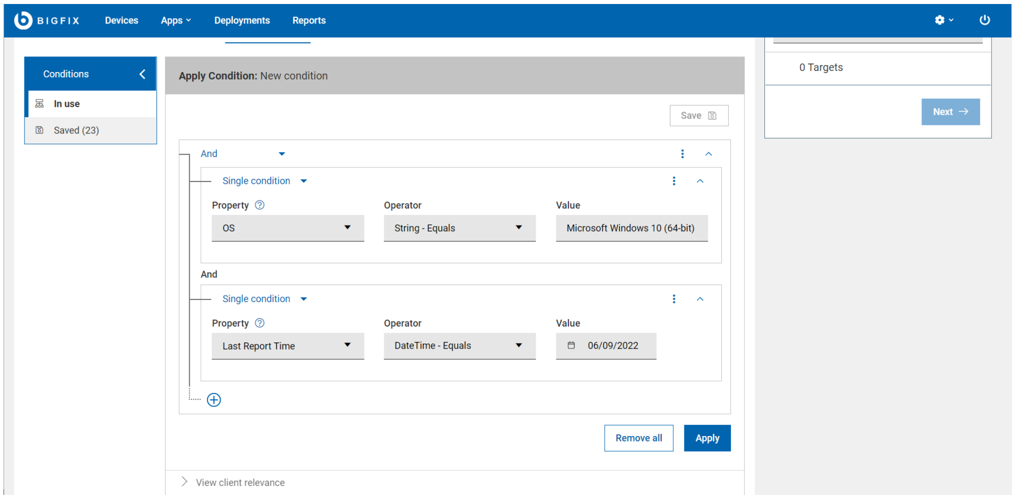
3. To add conditions:

    a. From the **Apply Condition** section, open the **Select** menu. Use the following menu options:

    - **Single condition**: Select this option to define a single condition to filter by a single property.



    - **And**: Select this option to define multiple conditions where **all** the specified conditions must match.

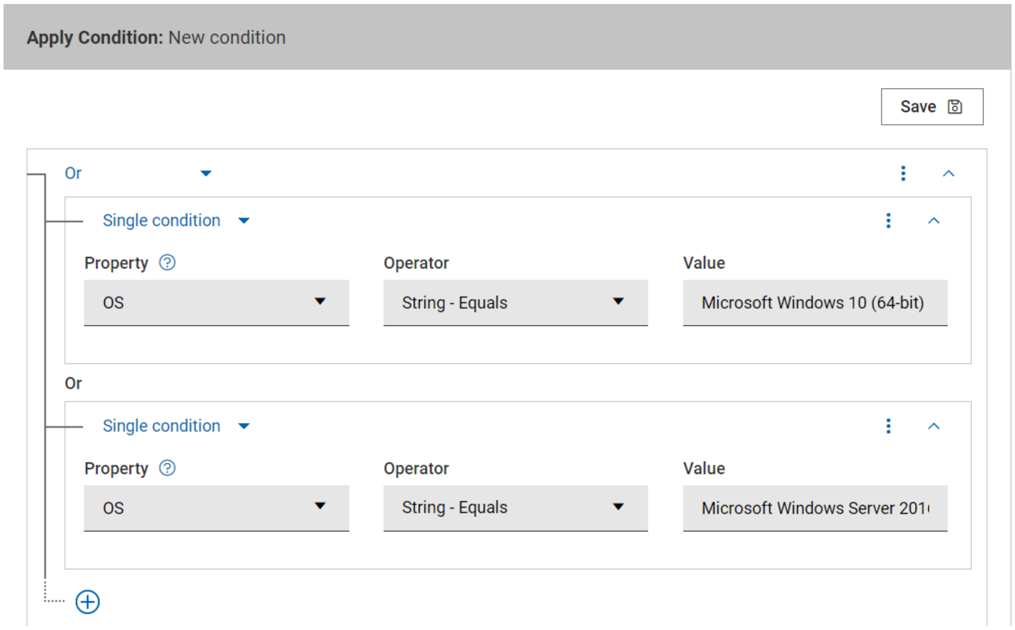


Property: OS | Operator: String - Equals | Value: Microsoft Windows 10 (64-bit)

And

Property: Last Report Time | Operator: DateTime - Equals | Value: 06/09/2022

    - **or**: Select this option to define multiple conditions where **any** of the specified conditions must match.



Apply Condition: New condition

Save

Or

Single condition

Property: OS | Operator: String - Equals | Value: Microsoft Windows 10 (64-bit)

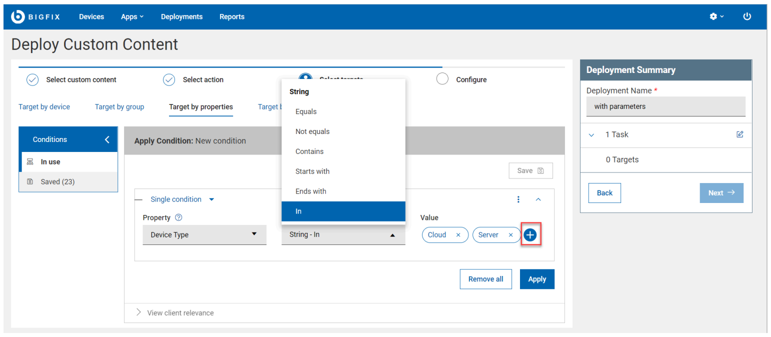
Or

Single condition

Property: OS | Operator: String - Equals | Value: Microsoft Windows Server 201

Note: The operator menu item works differently from the others.

- **Operator**:
  - Depending on the selected **Property**, the **Operator** options are displayed dynamically.
  - With *In* operator you can add a list of values. Click the **+** symbol to add values to the list.



Deploy Custom Content

Select custom content | Select action | Select targets | Configure

Target by device | Target by group | Target by properties | Target b

Conditions: In use | Saved (23)

Apply Condition: New condition

Save

Single condition

Property: Device Type | String - In | Value: Cloud × Server ×

String: Equals | Not equals | Contains | Starts with | Ends with | In

Remove all | Apply

View client relevance

Deployment Summary

Deployment Name *: with parameters

1 Task

0 Targets

Back | Next

  - You can have as many conditions as you want at the same level, but you can have a maximum of three nested conditions.

  - You can also define a condition with a value that is not in your database yet.

- In the **Property** menu, if a property is not listed, click **Add property**, select the a property, and click **Add**.

- You can add, clear, or remove a condition with the three-dots menu ⋮ in the upper-right corner.
- To remove all the conditions, click **Remove All**.

4. Click **Apply**. This button is available only after you defining conditions correctly.
   - The Deployment Summary section shows the total number applicable devices.

     Note: The target estimation does not include the fixlet relevance but only those that match with properties combination.

   - You must have web reports installed and active to use session relevance, because BigFix dynamically evaluates and estimates the number of devices that match the condition based on information in the database. The **Next** button is enabled only after you click the **Apply** button and BigFix completes estimating the targets. With this estimate, you can avoid submitting unwanted or large deployments by mistake.

     Note: If you have "Allow operators to use plain relevance for targeting enabled" permission you can bypass the evaluation of targets in targeting by properties in case web reports is not installed or is temporarily not available

5. **Optional:** To view the Relevance statement for the defined condition by clicking **View client relevance**.
6. **Save**: To save the defined conditions and reuse later, click **Save**, and in the Save condition window, complete the following steps:

   a. In **Condition name**, enter a name for the condition to be saved.

   b. In **Share mode**, select one of these options:
      - **Private**: To save this condition for your use only, select this option.
      - **Public**: To share the saved condition with others, select this option, enter a label, and click tick [is that a check mark?] sign.

   c. **Optional:** To add another label click the **plus** icon (+).

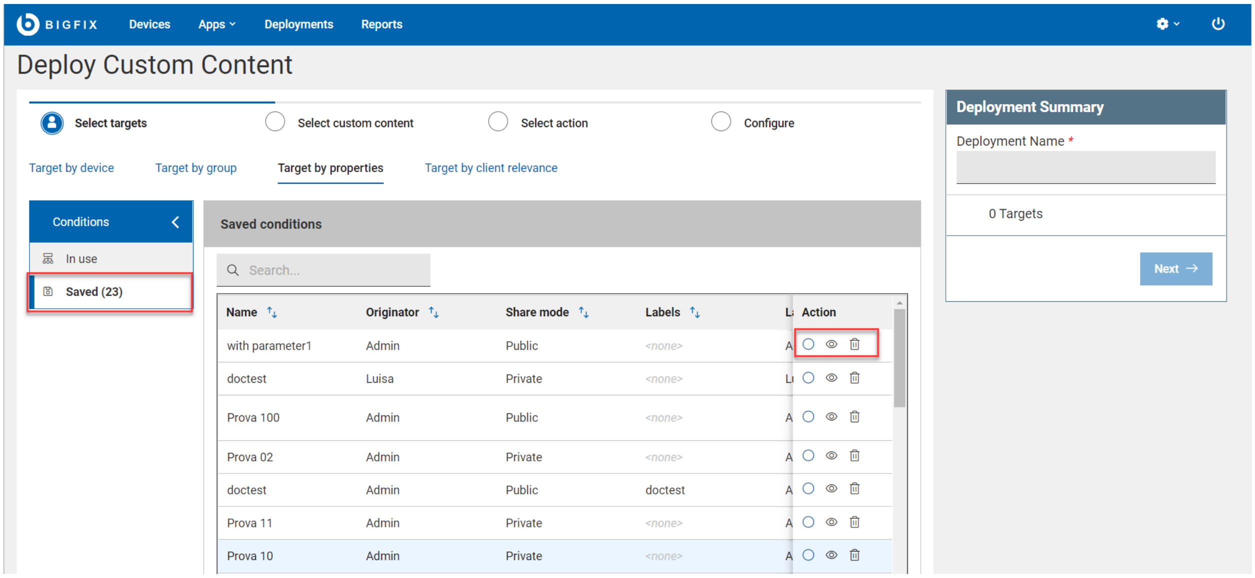
   d. Click **OK**.

To access the saved conditions, click **Conditions > Saved**[A click path is never a noun or a location. The elements of the path are objects of the transitive verb, "click" or "select"]. The following restrictions apply to saved conditions:

- Anybody can save private or public conditions.
- Only master operators have full access to all the saved conditions.
- If you do not have permissions for one or more of the properties used in a condition that another user created, you cannot reuse that condition. In this case, you get an error message.

- If you do not have permission to delete a private or public condition, the **Delete** icon is disabled.
- Conditions saved as public can be deleted only by master operators or by the originator.

You can select a condition to load and view its details, view the client relevance, or delete it. You can also search the saved conditions by name, labels, originators, or last modifier.



Name	Originator	Share mode	Labels	L	Action
with parameter1	Admin	Public	<none>	A	○ 👁 🗑
doctest	Luisa	Private	<none>	Lu	○ 👁 🗑
Prova 100	Admin	Public	<none>	A	○ 👁 🗑
Prova 02	Admin	Private	<none>	A	○ 👁 🗑
doctest	Admin	Public	doctest	A	○ 👁 🗑
Prova 11	Admin	Private	<none>	A	○ 👁 🗑
Prova 10	Admin	Private	<none>	A	○ 👁 🗑

In the window, you can use the following options:

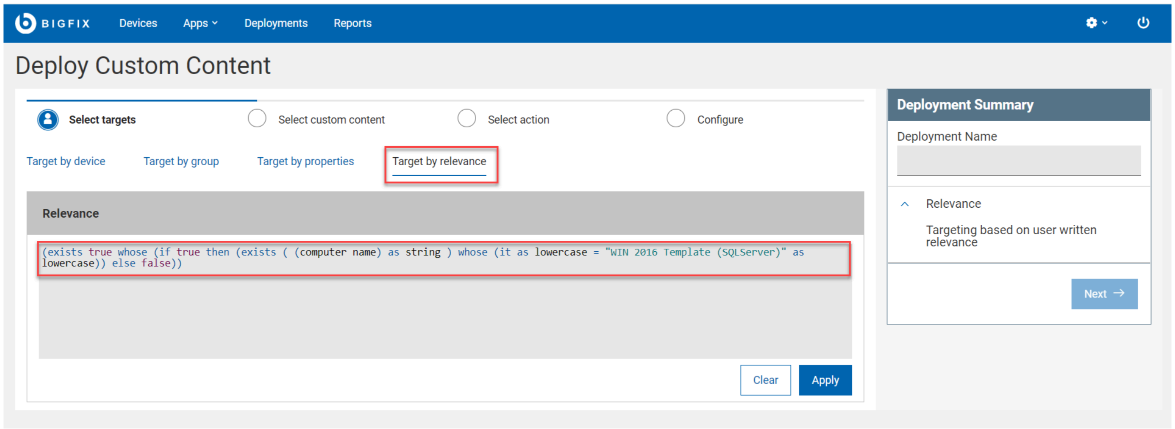
- **Load**: Click to load a filter.
- **View client relevance**: Click to view the corresponding client relevance in a window.
- **Delete**: Click to delete the filter, and then click **Delete** in the confirmation window.

Note: If you do not have the permission to delete a private or public filter, the **Delete** icon is disabled.

Targeting devices by relevance

To use trusted plain client relevance for your targeting, use the **Target by relevance** tab. In Target by relevance tab, you have only syntax highlighting. No evaluation of the number of targets is done.
To target devices by using the relevance statement:

1. In the deploy sequence in **Select targets** action, open the **Target by relevance** tab and enter the relevance statement.



```
(exists true whose (if true then (exists ( (computer name) as string ) whose (it as lowercase = "WIN 2016 Template (SQLServer)" as
lowercase)) else false))
```

Note:

- You can copy and paste the relevance that the "Target by properties" builder generates and can change it here.
- The text box for the relevance statement uses syntax highlighting. The relevance statement that you write here is not evaluated. For more information about writing correct relevance statement, read the Relevance Guide

2. Click **Apply**.

Configuration Options

The configuration options enable you to set the deployment options. The options available for you depends on how your BigFix administrator has configured it.

On the left pane you can navigate to the configuration categories to set the available configurations. Click the ? icon to know some information about a configuration. The Deployment Summary shows the summary of all the configurations you have set, which you can review before deploying. The deployment options are listed below.

Run

You can configure the time zone, time, date, day, and much more from here.

- **Time Zone**: You can select Client time or UTC time. Client Time is the local time on a BigFix client's device. Coordinated Universal Time is the primary standard for regulating clocks and time worldwide. This selection affects all the time-related parameters.
- Set**Start** and**End** Time: Schedule a deployment to start or end at a specific time; for example, to reduce network load a0nd device-holder inconvenience. When scheduling across time zones you can schedule actions to start in the past, relative to your own time zone. The option**Immediately** starts the deployment immediately after you click the deploy button. The option No end date creates open-ended deployment which does not have expiry date and

runs continuously and checks whether endpoints comply. For more information, see the Glossary.

- **Run between hours**: Defines a period during which the action can be run. This functionally starts at the specified time, only if all the other conditions are valid.
- **Run on selected**: You can select one or more days in a week to run this deployment regularly.
- **Run all member actions**: This option is only visible when you have multiple actions. Actions in a multiple action group run sequentially and stop on the first action that fails. Select this option to instruct the MAG to ignore a failure and proceed to the next action. Use this option when the actions in a MAG do not depend on the actions that precede them.

  Note: This option appears only when you have multiple actions.

- **Run Only When** Select the check box to set a condition. Select the condition from the dropdown lists and specify a value for the condition .
- **Retry**: Select the check box to configure when to retry deployment on failure.
- **Reapply action**: Select the check box to configure when to reapply the action.
- **Download:** Select this check box to download deployment files immediately regardless of the start time schedule. Pre-cache deployment-related files, transferring them from a vendor's server to a BigFix server before deployment. You can save time when working with large files or a tight maintenance window by completing this part of the job first.
- **Stagger deployment times to reduce network load**: Enter an interval in hours and minutes.

Users

Allows you to specify#whether or not#you require a logged-on user (or specified group of users) to be present before running the#Action.

- **Run action**: Select an option to run the deployment depending on the log in status.
- **Select users**: Select if the deployment needs to be run for all users, users in a local session, or users in a group. If you select group, enter the name of the group and click Insert.

Messages

Specify informative messages to be displayed on the targeted Clients, along with options for user interaction.

- **Before running action**: Select this option to display the message on targeted computers before the deployment running.
- **While running action**: Select this option to display the message on targeted computers while the deployment is running.

Send a Notification

Trigger an email alert when a deployment fails or completes. Enter one or more recipients in the **To:** field, separating multiple addresses with a comma.

- Send on Failure - enter a threshold value (1 - 250,000) to receive an email if the deployment fails on the specified number of devices.
- Send on Completion - check the box to receive an email when the deployment completes on all targets. Note: this notification option is not available when targeting computer groups.

Offer

Configure to enable the device owners to accept or decline an action and to control when the deployment can run. For example, whether or not to install an application, or to run an installation at night rather than during the day. An action that is made into an 'Offer' becomes available in the list of offers in the client UI on applicable machines. Users can browse through the list of available offers and apply those that they are interested in. Offers will only be visible to users selected on the 'Users' tab and on machines where the client Offer UI is enabled. To configure, select the**Send this as an offer** check box, enter the offer description. Select the**Notify me of offers**check box to notify when there is an offer.

Note: Do not send an offer as an open-ended deployment. Open-ended offers can cause problems for device owners, such as an optional piece of software they cannot permanently remove.

Offer options:

- **ONLY to the Software Distribution Client dashboard** - Display software offers on the Client UI’s Software Distribution Client Dashboard when it is enabled on the device, and the Self-Service Application is not enabled. When the Self-Service Application is enabled, all offers display there.
- **Notify users of offer availability** - Include a notification on the endpoint that a new offer is available.
- **Offer Description** - Enter a description of the action in the box provided. The description will be presented to users. You can change fonts, sizes, styles, numbering, and formatting to customize the description. If the offer contains multiple actions the name of each component is included by default.

Post-Action

Specify a follow-up behavior for the Action.

- **Do nothing**: Select this option to do nothing after the action is run.
- **Restart the computer**: Select this option to restart the computer after the action is run.

  - ◦ **Prompt before restarting**: Displays the message to the active user. Send the default message or enter the message title and text in the text boxes.
  - ◦ **Allow me to cancel restart**: Allows the user to cancel the restart after the deployment.
  - ◦ Set a deadline in minutes, hours, or days from the drop down and select an option to restart automatically at deadline or show the action message at the top until the user accepts.
- **Shut down the computer**: Select this option to shut down the computer after the action is run.
  - ◦ **Prompt before shut down**: Displays the message to the active user before shutting down the computer. Send the default message or enter the message title and text in the text boxes.
  - ◦ **Allow me to cancel shut down**: Allows the user to cancel the shutdown after the deployment.
  - ◦ Set a deadline in minutes, hours, or days from the drop down and select an option to shut down automatically at deadline or show the action message at the top until the user accepts.

Applicability relevance

This tab is also available from the following dialogs from the console:

- Take action
- Take multiple actions
- Edit Computer Settings

Specify the criteria to use to judge the relevance of a Fixlet action.

- **When the relevance from the original Fixlet or Task Message evaluates to true**: Select this option to confirm the relevance expression set in the default action. It is strongly recommended that you use the original Relevance expression. However, you can also customize it to better suit your needs.
- **When the following custom relevance evaluates to true**: Select this option to modify the existing relevance expression or to specify a new relevance expression to suite your needs.

Success criteria

Define the conditions under which the action is considered to be successful. Select one of the following options:

- **When the applicability relevance evaluates to false**

  This is the default success criteria, requiring that the Relevance statement that made the action applicable is no longer TRUE. Because the Relevance statement notices a problem and the action fixes it, this is generally sufficient to establish success.

- **When all lines in the action script are correctly completed**

  You can make success dependent on completing all steps of the action script.
- **When the following custom relevance evaluates to false**

  You can use a special Relevance clause to ensure that the action has accomplished it goals. In this case, the text box in the screen becomes editable, and you can create a new or revise an existing Relevance clause.

Action script

In general you are recommended to use the action script provided with the Fixlet or task. However, sometimes it might be useful to align the action script to your environment and business needs. The **Action Script** tab of the **Take Action** dialog allows you to modify the action script. There are two options in this dialog:

- **From the original Fixlet or Task message**

  This is the default for most Fixlet actions and is the recommended option.
- **From the custom action script**

  You can select one of the following options and either modify the existing script or enter a new script in the text area. Select the type of action script that you want to use for this script:

  - **BigFix Action Script**

    This is the BigFix standard scripting language for actions. For more information about the action language, see https://developer.bigfix.com/action-script/ the *Action Script Language* section in the BigFix Developer web site (*https:// developer.bigfix.co m*).
  - **AppleScript**

    This is the scripting language of Apple for controlling computer resources.
  - **SH**

    The action is a shell script to be run by a Linux or a UNIX or a bsd shell.
  - **PowerShell**

    Starting from version 10.0.4, BigFix gives you the possibility to run PowerShell scripts too.

    You can run on a selected Windows Client the script that you write in the **Action Script** text box. The script runs on the PowerShell installed by default by your Windows operating system in the C:\Windows \System32\WindowsPowerShell\v1.0 directory, if available, or in C:\Windows\SysWOW64\WindowsPowerShell\v1.0.

The script is executed by default using the **-ExecutionPolicy Bypass** option. To avoid using this option, you can use the `_BESClient_PowerShell_DisableExecPolicyBypass` client setting described in the Miscellaneous section of the List of settings and detailed descriptions page.

Since they are executed in hidden mode, PowerShell scripts requiring user interaction or showing pop-up windows or dialog boxes are not supported and might cause the action to remain in running status or the script to display an error in the log file.

Note: By default, actions cannot be undone. Make sure to test your action on a small scale before you deploy it in your entire network.

Pre/Post Execusion script

This option becomes available when you deploy a baseline. You can write the action script in BigFix Action Script, AppleScript, SH, or PowerShell *(on page 144)*.

- **Pre-execution**: Write the script to run before excuting this multiple action group.
- **Post-execution**: Write the script to run after excuting this multiple action group.

Chapter 11. Get Started with Deployments

Use the Deployment views to monitor and verify completion of BigFix deployments.

The Deployment List

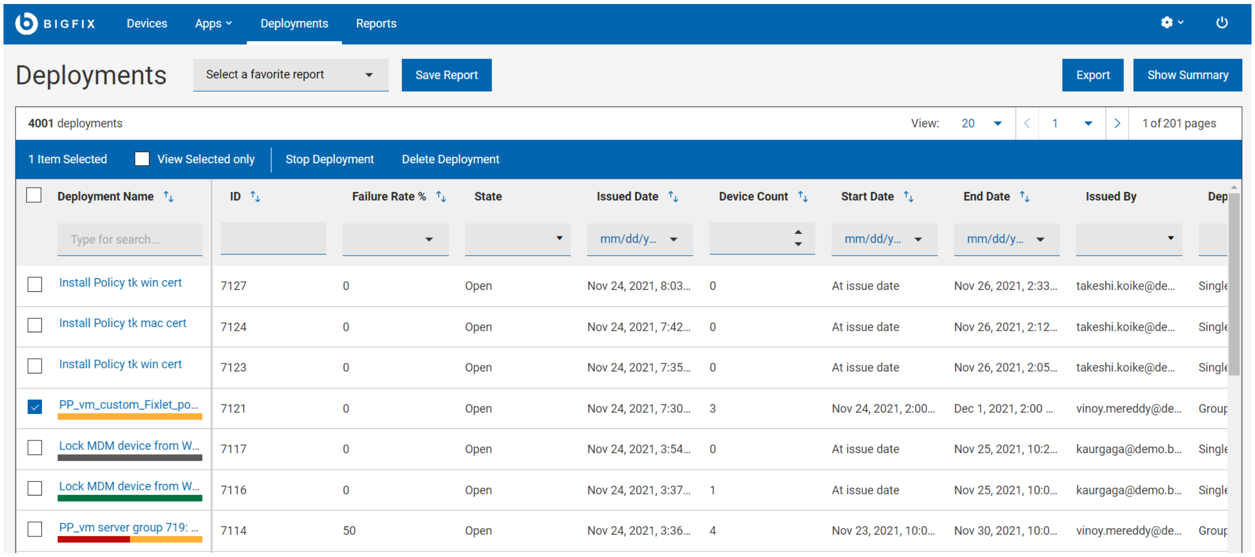
View the list of all deployments, create customized deployment summary reports to review the detailed information about each deployment.

To access the **Deployments** page, from the WebUI main page, select **Deployments**.

WebUI deployment screens list every deployment irrespective of the permission settings. While operators can see all deployments, permissions continue to govern the actions they can take. For example, an operator who cannot access the WebUI patch screens can see all patch deployments, but cannot stop a patch deployment that is running.

The WebUI displays all actions initiated from the WebUI, the BigFix console, and external sites, including BES Support.

The following image shows the Deployments data grid with default columns order. By default, the data is sorted based on the “issue date” in descending order. This view cannot be customized if not reordering the columns.



4001 deployments

□	Deployment Name	ID	Failure Rate %	State	Issued Date	Device Count	Start Date	End Date	Issued By	Dep
□	Install Policy tk win cert	7127	0	Open	Nov 24, 2021, 8:03...	0	At issue date	Nov 26, 2021, 2:33...	takeshi.koike@de...	Single
□	Install Policy tk mac cert	7124	0	Open	Nov 24, 2021, 7:42...	0	At issue date	Nov 26, 2021, 2:12...	takeshi.koike@de...	Single
□	Install Policy tk win cert	7123	0	Open	Nov 24, 2021, 7:35...	0	At issue date	Nov 26, 2021, 2:05...	takeshi.koike@de...	Single
☑	PP_vm_custom_Fixlet_po...	7121	0	Open	Nov 24, 2021, 7:30...	3	Nov 24, 2021, 2:00...	Dec 1, 2021, 2:00 ...	vinoy.mereddy@de...	Group
□	Lock MDM device from W...	7117	0	Open	Nov 24, 2021, 3:54...	0	At issue date	Nov 25, 2021, 10:2...	kaurgaga@demo.b...	Single
□	Lock MDM device from W...	7116	0	Open	Nov 24, 2021, 3:37...	1	At issue date	Nov 25, 2021, 10:0...	kaurgaga@demo.b...	Single
□	PP_vm server group 719: ...	7114	50	Open	Nov 24, 2021, 3:36...	4	Nov 23, 2021, 10:0...	Nov 30, 2021, 10:0...	vinoy.mereddy@de...	Group

Manage deployments

To manage deployments, select one or more deployments from the list. A blue bar appears; according to the user permissions, you can do the following possible actions:

- Stop Deployment *(on page 153)* that are in `Open` state.
- Delete deployments that are in `Expired` or `Stopped` state.

Deployment status bar

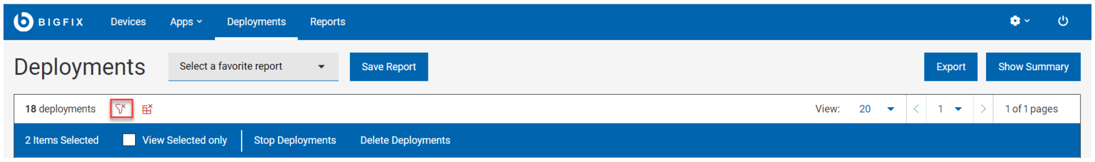
The deployment name cell also displays a colored bar that gives a quick summary of the Deployment Status (on page 152) of each deployment.

Refine results

- **Sort by:** You can sort the list by:
    - Deployment Name
    - ID
    - Failure Rate
    - Issued Date
    - Device Count
    - Start Date
    - End Date
- **Filter**: To filter deployments data, click in the text field of the desired column and type the search string; or from the desired column, select your option from the list.
    - To speed up your search, combine filters.
        - **Deployment Name**: Filter the deployments containing the entered search string.
        - **ID**: Filter the deployments containing the entered numbers in their ID.
        - **Failure Rate %**: Filter deployments with specified failure rate range.
        - **State**: Filter all expired, open, or stopped deployments.
        - **Issued Date**: Filter deployments issued within a day, week, month, quarter, or within a specific date or date range.
        - **Device Count**: Filter the deployments that are applicable or issued on the specified minimum number of devices.
        - **Start Date**: Filter all the deployments that start within a day, week, month, quarter, or within a specific date or date range.
        - **End Date**: Filter all the deployments that end within a day, week, month, quarter, or within a specific date or date range.
        - **Issued By**: Filter the deployments issued by the logged in user or a specified user.
        - **Deployment Type**: Filter all deployments targeted for a single content (Fixlet, software, task) or a group (multiple action group, baseline).
        - **Behaviors**: Filter deployments with a specific behavior such as deployments with user message, offer type deployments, open-ended deployments, or deployments that restart endpoints.
        - **Application Type**: Filter deployments that belong to a particular application type.
        - **Source Site**: Filter all the deployments that belong to a specific site.

Note: By default, you can combine up to a maximum of five filters to process simultaneously. Exceeding the maximum number of filters affects the performance. The default value can be configured using the setting `_WebUIAppEnv_MAX_FILTERS_NUMBER`.

- To clear all selected filters, click Reset all filters

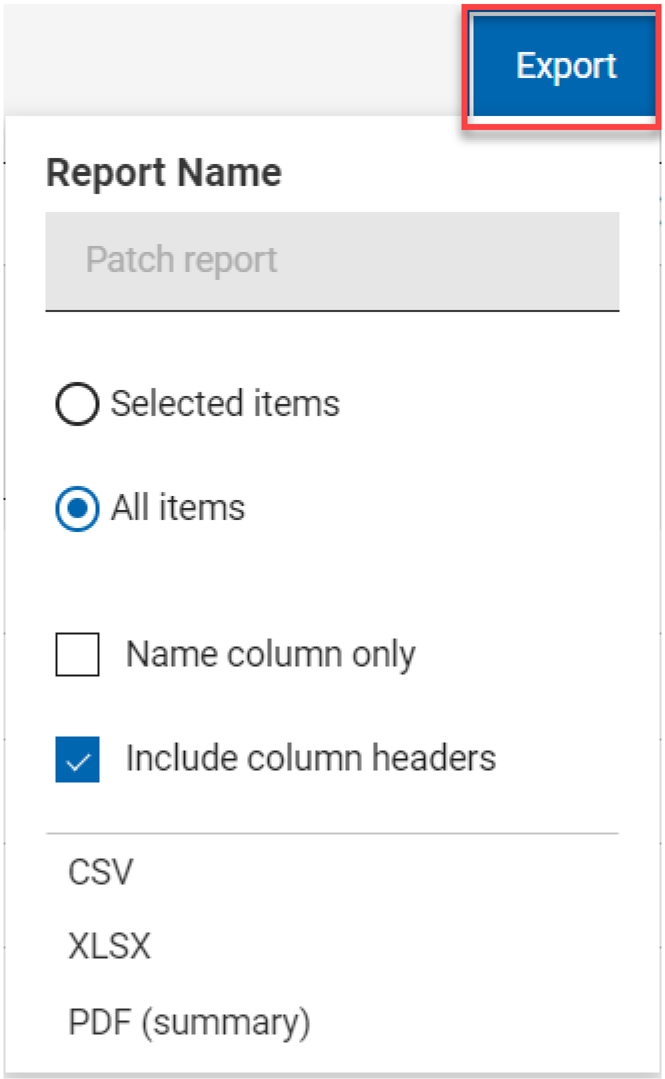


Deployment reports

- **Save Report**: Save the report for future reference and edit, update, or delete as required. For more information, see Reports *(on page 20)*.
- **Show Summary:**
  1. In the **Deployments** page, select the required filters.
  2. Click **Show Summary**. You can view the deployment data as charts and tables. Mouse over the interested areas on the chart to get more details about the respective data point and the percentage data. Mouse over on any truncated labels to see the full text in the tool tip. You can change filters or enter search text and the report dynamically displays the relevant information.
  3. **Deployment State By Deployment Date**: Displays total number of deployments and their deployment state since the start date of deployment for a period of time.
  4. **By Failure Rate (%)**: Displays total number of deployments and their failure rate under different categories from 0 to 100.
  5. **By Application Type**: Displays total number of deployments for each application type.
- **Export:**

  You can export the filtered report in a `.csv`, `.xlsx`, or `.pdf` format.

  1. In the **Devices** page, select the required filters.
  2. Click **Export To**.



Report Name

Patch report

○ Selected items

● All items

□ Name column only

☑ Include column headers

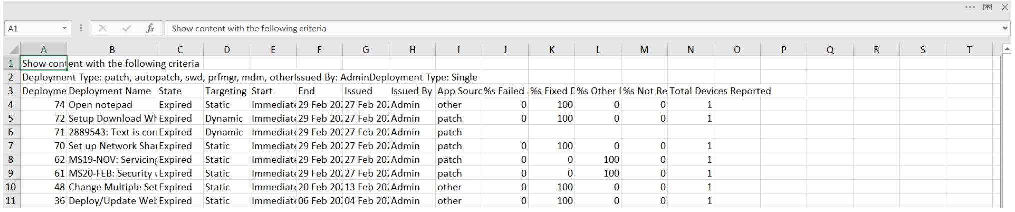
3. The option **Selected Items** allows you to export select items from the filtered result; **All Items** allows you to export all the items from the filtered list. Select the desired option.
4. Name column only: Select this option if you want to export only the names of the filtered items.
5. Include column headers: Select this option if you want to export details of every default columns of an item.

Note: If you have displayed columns other than the default columns, you can export name column only.

6. Select a file format (CSV, XLSX, or PDF) that you want to export to.

    - By default, the report gets downloaded into your Downloads folder with the default file name (Device_Report_mm_dd_yyyy_username). You can change the download settings in your browser to change the file name and download it into a preferred location. You can save the report to review it later and/or share it with interested stakeholders.

- If you have selected PDF format, a `.zip` file gets downloaded which contains a `.csv` file with numerical data and `.pdf` file with visual representation of the data.
- The exported deployment report contains key details about your deployments that you have selected through the filters and search criteria. The details include such as deployment ID, deployment name, state of the deployment along with all the other details that you can see on the screen when you expand every deployment. A sample report is shown below:



A1 | Show content with the following criteria

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Show content with the following criteria													
2	Deployment Type: patch, autopatch, swd, prfmgr, mdm, otherIssued By: AdminDeployment Type: Single													
3	Deployme	Deployment Name	State	Targeting	Start	End	Issued	Issued By	App Sourc	%s Failed	%s Fixed D	%s Other I	%s Not Re	Total Devices Reported
4	74	Open notepad	Expired	Static	Immediate	29 Feb 20	27 Feb 20	Admin	other	0	100	0	0	1
5	72	Setup Download Wh	Expired	Dynamic	Immediate	29 Feb 20	27 Feb 20	Admin	patch	0	100	0	0	1
6	71	2889543: Text is cor	Expired	Dynamic	Immediate	29 Feb 20	27 Feb 20	Admin	patch					
7	70	Set up Network Shar	Expired	Static	Immediate	29 Feb 20	27 Feb 20	Admin	patch	0	100	0	0	1
8	62	MS19-NOV: Servicing	Expired	Static	Immediate	29 Feb 20	27 Feb 20	Admin	patch	0	0	100	0	1
9	61	MS20-FEB: Security u	Expired	Static	Immediate	29 Feb 20	27 Feb 20	Admin	patch	0	0	100	0	1
10	48	Change Multiple Set	Expired	Static	Immediate	20 Feb 20	13 Feb 20	Admin	other	0	100	0	0	1
11	36	Deploy/Update Wel	Expired	Static	Immediate	06 Feb 20	04 Feb 20	Admin	other	0	100	0	0	1

Deployment Documents

Click a deployment name to see its deployment status, behavior (set at configuration), and targeting information. Drill further into deployment details using the links to associated views.

The Deployment Document views:

- Overview – detailed description of the selected deployment: status, behavior, targeting, and more.
- Device Results – target status – the state of the deployment on each endpoint.
- Component Results – for content with multiple actions: the deployment status of each component on targeted devices, expressed as a percentage of success.

Note: For performance reasons, the deployment status of each component is not retrieved if the action contains more than 200 items.

Monitoring Deployments: State, Status, and Result

Interpret deployment results correctly by understanding the difference between Device Results, Deployment Status, and Deployment State.

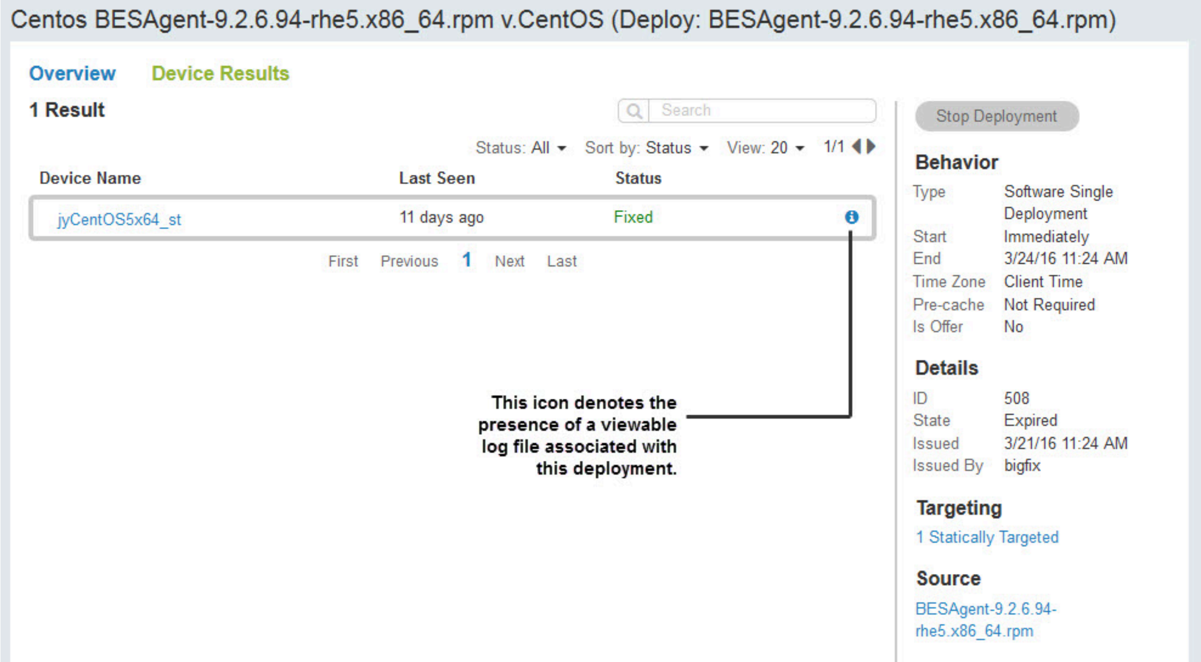
Device Results

Device Results describe the state of a deployment on a particular endpoint. There are many different BigFix Device Result codes. The most common ones seen in the WebUI include:

- Fixed or Completed – The deployment succeeded (on this device).
- Failed – The deployment failed (on this device).
- Pending Restart – Eventual success is implied.
- Not Relevant – The action is not relevant to this device.
- Running

- Evaluating
- Pending Download

Software deployments might have an associated log file. This log can be viewed in the Device Results screen. The presence of a viewable log file is denoted by an icon. Note that log files are only available for software deployments.



Centos BESAgent-9.2.6.94-rhe5.x86_64.rpm v.CentOS (Deploy: BESAgent-9.2.6.94-rhe5.x86_64.rpm)

1 Result

Status: All ▾ Sort by: Status ▾ View: 20 ▾ 1/1

Device Name	Last Seen	Status
jyCentOS5x64_st	11 days ago	Fixed

This icon denotes the presence of a viewable log file associated with this deployment.

Behavior

Type	Software Single Deployment
Start	Immediately
End	3/24/16 11:24 AM
Time Zone	Client Time
Pre-cache	Not Required
Is Offer	No

Details

ID	508
State	Expired
Issued	3/21/16 11:24 AM
Issued By	bigfix

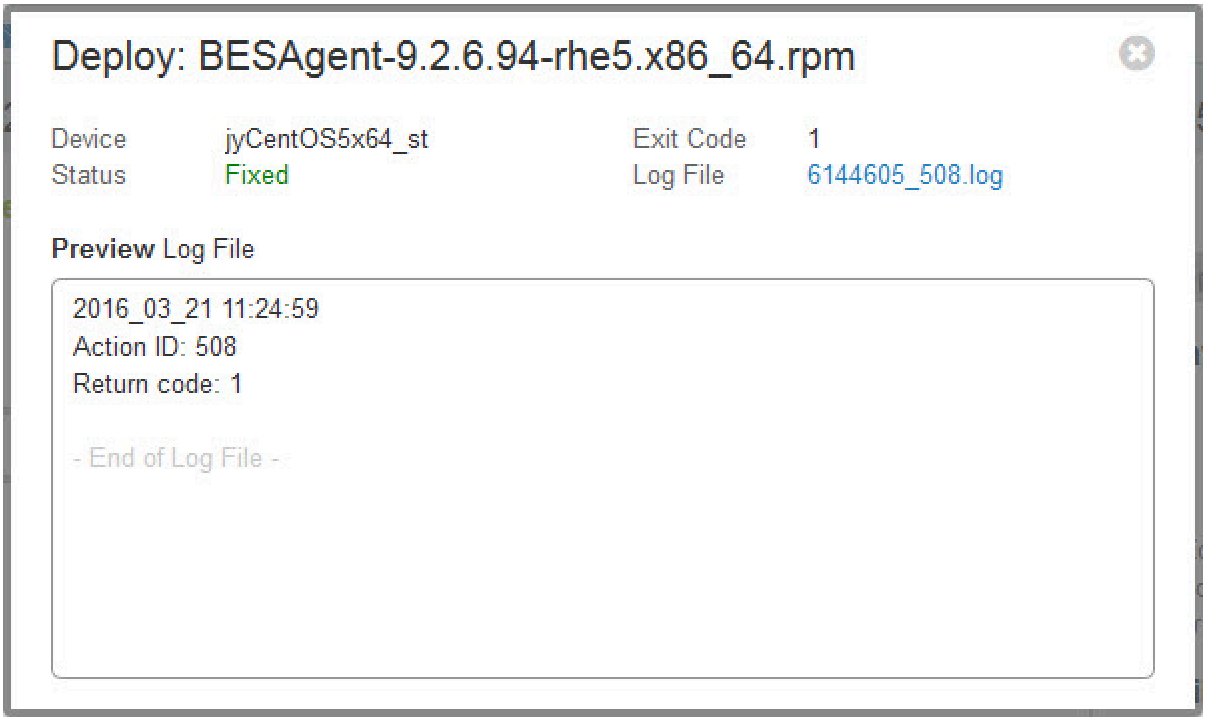
Targeting

1 Statically Targeted

Source

BESAgent-9.2.6.94-rhe5.x86_64.rpm

Click the log icon to display the associated log data. The entire log can be downloaded by clicking the log file name.



Deploy: BESAgent-9.2.6.94-rhe5.x86_64.rpm

Device	jyCentOS5x64_st	Exit Code	1
Status	Fixed	Log File	6144605_508.log

Preview Log File

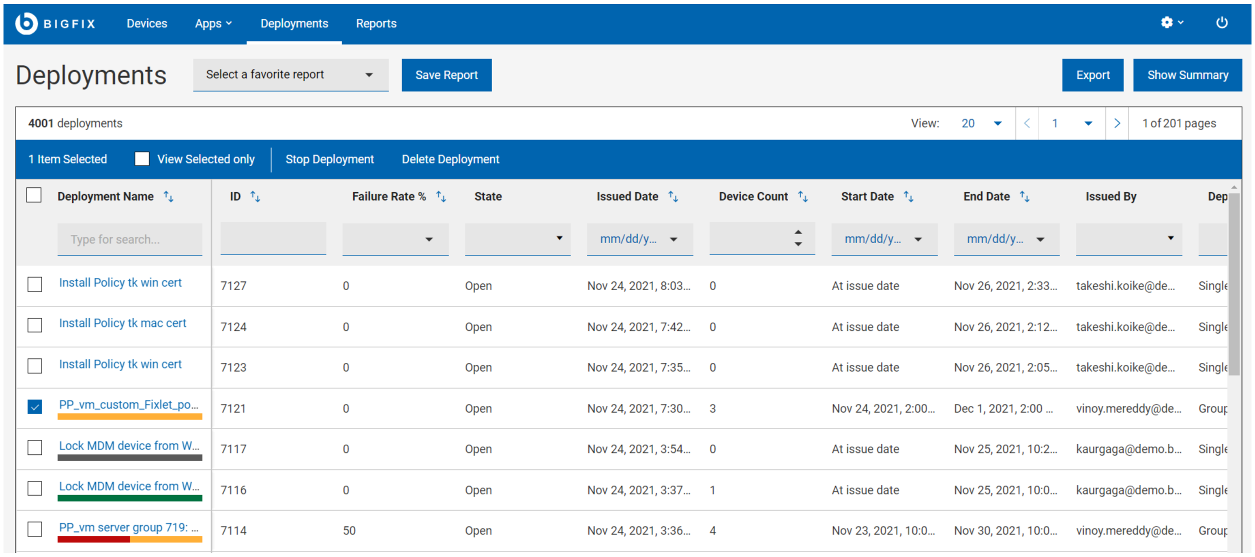
```
2016_03_21 11:24:59
Action ID: 508
Return code: 1

- End of Log File -
```

Note: Log files can only be viewed for software deployments. In addition, to view log files in the BigFix WebUI, the current user must be subscribed to the Software Distribution Site in the traditional BigFix Console, and Analysis 11 of the Software Distribution Site must be activated.

Deployment Status

Deployment Status is formulated using Device Results.

- For deployments with single actions, Deployment Status is the cumulative deployment status of each targeted device, expressed as a percentage of success.
- For deployments with multiple actions, Deployment Status is the cumulative deployment status of each component on each targeted device, expressed as a percentage of success.



4001 deployments   View: 20   1   1 of 201 pages

1 Item Selected   ☐ View Selected only   Stop Deployment   Delete Deployment

☐	Deployment Name	ID	Failure Rate %	State	Issued Date	Device Count	Start Date	End Date	Issued By	Dep
	Type for search...				mm/dd/y...		mm/dd/y...	mm/dd/y...		
☐	Install Policy tk win cert	7127	0	Open	Nov 24, 2021, 8:03...	0	At issue date	Nov 26, 2021, 2:33...	takeshi.koike@de...	Single
☐	Install Policy tk mac cert	7124	0	Open	Nov 24, 2021, 7:42...	0	At issue date	Nov 26, 2021, 2:12...	takeshi.koike@de...	Single
☐	Install Policy tk win cert	7123	0	Open	Nov 24, 2021, 7:35...	0	At issue date	Nov 26, 2021, 2:05...	takeshi.koike@de...	Single
☑	PP_vm_custom_Fixlet_po...	7121	0	Open	Nov 24, 2021, 7:30...	3	Nov 24, 2021, 2:00...	Dec 1, 2021, 2:00 ...	vinoy.mereddy@de...	Group
☐	Lock MDM device from W...	7117	0	Open	Nov 24, 2021, 3:54...	0	At issue date	Nov 25, 2021, 10:2...	kaurgaga@demo.b...	Single
☐	Lock MDM device from W...	7116	0	Open	Nov 24, 2021, 3:37...	1	At issue date	Nov 25, 2021, 10:0...	kaurgaga@demo.b...	Single
☐	PP_vm server group 719: ...	7114	50	Open	Nov 24, 2021, 3:36...	4	Nov 23, 2021, 10:0...	Nov 30, 2021, 10:0...	vinoy.mereddy@de...	Group

- Green – Fixed (patches), or Completed (software, custom content) deployments.
- Gray – Not yet reported or not relevant.
- Red – For deployments with error and failed deployments.
- Yellow – For all the other conditions including Pending Restart, Running, Evaluating, Pending Download.
- No Status Bar – No relevant devices.

Deployment State

Deployment State describes the eligibility of a deployment to run on endpoints. It is not involved in calculating Deployment Status.

Deployment State has three values:

- Open – The deployment is eligible to be run by endpoints.
- Expired – The deployment is no longer eligible to run because the end time has passed for all possible endpoints in all time zones. The default expiration time for an action is 2 days.
- Stopped – The deployment is no longer eligible to run because an operator or administrator stopped it.

In summary: Device Result is the result of a particular deployment on a specific device. Deployment State describes the eligibility of a deployment to run. Deployment Status provides the cumulative results of a deployment on targeted endpoints.

Evaluating Deployments With Multiple Actions

To obtain an accurate picture of the state of a deployment with multiple actions, such as those involving a group or baseline, check the status of its individual components. In other words, if a deployment group's status is less than 100%, check to see which of its components has not yet completed.

1. Open the Deployments list.
2. Use the Deployment Type filter to display a list of Group deployments.
3. Select the Deployment that you want and open its document.
4. Click **Component Results**.

Note: For performance reasons, the deployment status of each component is not retrieved if the action contains more than 200 items.

Stop Deployment

Not every deployment completes successfully the first time. Use the **Stop Deployment** button on any Deployment list or document view to terminate a deployment, if needed.

Reasons to stop a deployment include:

- Starting to see failures on many devices.
- Starting to get blue screens on the targeted devices.
- You have updated a baseline (or Fixlet) and need to stop the old one.

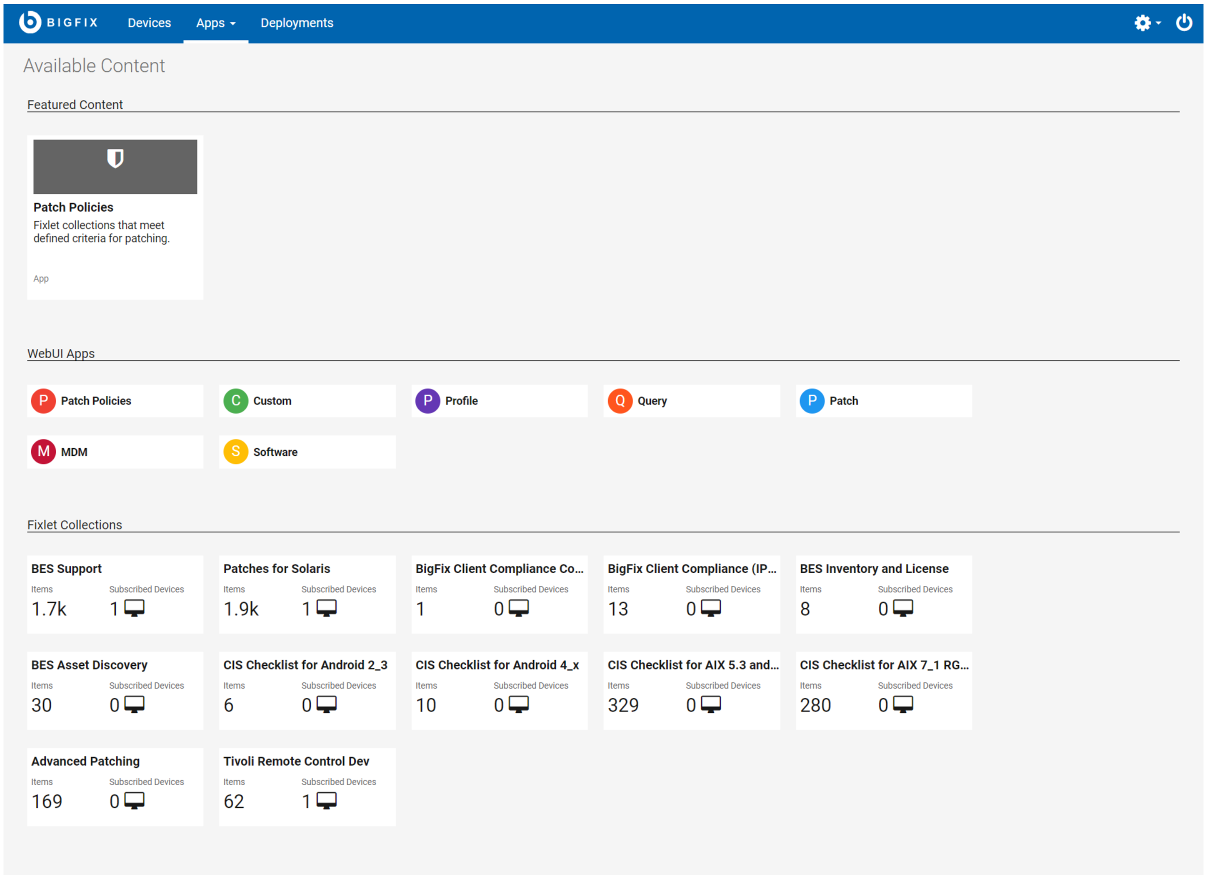
Use the Deployment views and the custom tools provided by your BigFix administrator to diagnose and fix deployment problems. Work with them to learn more about why deployments fail and effective methods for resolving issues when they arise. Reasons a deployment can fail include:

- A computer is offline.
- A computer is being rebuilt or reimaged.
- A computer has insufficient disk space.
- A computer is not communicating with the BigFix update server.

- The BigFix agent is not running on the computer.
- The computer is missing some dependent software.

Chapter 12. Get Started with the Content App

Use the Content App to work with Fixlets, tasks, and baselines on the BigFix sites. Search, filter, and deploy content using standard WebUI tools.



Available Content

Featured Content

Patch Policies
Fixlet collections that meet defined criteria for patching.
App

WebUI Apps

P Patch Policies
C Custom
P Profile
Q Query
P Patch
M MDM
S Software

Fixlet Collections

Collection	Items	Subscribed Devices
BES Support	1.7k	1
Patches for Solaris	1.9k	1
BigFix Client Compliance Co...	1	0
BigFix Client Compliance (IP...	13	0
BES Inventory and License	8	0
BES Asset Discovery	30	0
CIS Checklist for Android 2_3	6	0
CIS Checklist for Android 4_x	10	0
CIS Checklist for AIX 5.3 and...	329	0
CIS Checklist for AIX 7_1 RG...	280	0
Advanced Patching	169	0
Tivoli Remote Control Dev	62	1

Note:

- The sites listed in the Content App depends on the sites subscribed and the permissions given to the logged in user.
- It also lists the sites that are not yet associated with a WebUI application.

New sites, new applications, and apps with new features are highlighted in the Featured Content section. Click the tiles in the WebUI Apps section to open WebUI applications. Operators see sites on the Content application's white list of permissible sites. Master operators see all sites that are not part of the WebUI App collection.

Note: Not all Fixlets are deployable. Do not use the Content App to deploy Fixlets that:

- Contain or employ JavaScript, for example, JavaScript that takes action or secure action.
- Use Session Relevance.
- Use specialized Console APIs.

The Fixlets will not run, and you will receive no errors or any other indication that something is wrong until devices start reporting back that there is a problem. If you are not sure whether a Fixlet is deployable or not, run it from the BigFix Console to avoid unpredictable behavior.

Operator Access

The below list associates the activities that an operator can perform with the type of operator.

- Non-master operators cannot access BES support in the WebUI application as it is intended only for the Master Operators.
- Master operators can view all the external sites, except for the two below listed sites in Table 1.
- Non-master operator can only access the external sites that they have visibility. See the accessible Whitelist sites listed in Table 2.

Table 16. List of external sites that cannot be accessed by the Master operator

Site ID	Site Name
8361	OS Deployment and Bare Metal Imaging
8363	OS Deployment and Bare Metal Imaging Beta

Table 17. List of whitelist sites that can be accessed by the Non-master operator

Site ID	Site Name
12249	Advanced Patching
3107	BES Asset Discovery
3073	BigFix Client Compliance (IPSec Framework)
3043	BigFix Client Compliance Configuration
9287	BigFix Labs
8253	BitLocker Management (Labs)
11316	CIS Checklist for AIX 5.3 and 6.1
11316	CIS Checklist for AIX 5.3 and 6.1
11522	CIS Checklist for AIX 7.1 - RG03
12070	CIS Checklist for Apache HTTP Server 2.2 on Linux

Site ID	Site Name
12391	CIS Checklist for CentOS Linux 6
12410	CIS Checklist for CentOS Linux 7
11535	CIS Checklist for DB2 on Linux
11536	CIS Checklist for DB2 on Windows
15106	CIS Checklist for Internet Explorer 10
12337	CIS Checklist for Internet Explorer 11
12339	CIS Checklist for Mac OS X 10.10
12354	CIS Checklist for Mac OS X 10.11
12425	CIS Checklist for Mac OS X 10.12
11313	CIS Checklist for Mac OS X 10.6
12389	CIS Checklist for Mac OS X 10.8
11566	CIS Checklist for MS IIS 7
12509	CIS Checklist for MS IIS 8
11568	CIS Checklist for MS SQL Server 2005
11570	CIS Checklist for MS SQL Server 2008 R2
11574	CIS Checklist for MS SQL Server 2012 DB Engine
11539	CIS Checklist for Oracle Database 11-11g R2 on Linux
11540	CIS Checklist for Oracle Database 11-11g R2 on Windows
11537	CIS Checklist for Oracle Database 9i-10g on Linux
11538	CIS Checklist for Oracle Database 9i-10g on Windows
12373	CIS Checklist for Oracle Linux 6
12364	CIS Checklist for Oracle Linux 7
11318	CIS Checklist for RHEL 5
11366	CIS Checklist for RHEL 6
12181	CIS Checklist for RHEL 7

Site ID	Site Name
12187	CIS Checklist for SLES 10
12518	CIS Checklist for SLES 11
11317	CIS Checklist for Solaris 10
11526	CIS Checklist for Solaris 11 - RG03
12465	CIS Checklist for SUSE 12
12453	CIS Checklist for Ubuntu 12.04 LTS Server
12439	CIS Checklist for Ubuntu 14.04 LTS Server
12429	CIS Checklist for Ubuntu 16.04 LTS Server
12288	CIS Checklist for
11356	CIS Checklist for Windows 2003 DC
11358	CIS Checklist for Windows 2003 MS
13083	CIS Checklist for Windows 2008 DC - RG03
13085	CIS Checklist for Windows 2008 MS - RG03
13075	CIS Checklist for Windows 2008 R2 DC
13077	CIS Checklist for Windows 2008 R2 MS
12064	CIS Checklist for Windows 2012 DC
12066	CIS Checklist for Windows 2012 MS
12057	CIS Checklist for Windows 2012 R2 DC
12061	CIS Checklist for Windows 2012 R2 MS
12469	CIS Checklist for Windows 2016 DC
12471	CIS Checklist for Windows 2016 MS
11491	CIS Checklist for Windows 7
12093	CIS Checklist for Windows 8
15107	CIS Checklist for Windows 8.1
11360	CIS Checklist for Windows XP
9342	Client Manager Builder

Site ID	Site Name
8151	Client Manager for Application Virtualization
75	Client Manager for Endpoint Protection
9318	Client Manager for TPMfOSD
11035	DISA STIG Checklist for AIX 5.1
11036	DISA STIG Checklist for AIX 5.2
11434	DISA STIG Checklist for AIX 53 - RG03
11436	DISA STIG Checklist for AIX 61 - RG03
11354	DISA STIG Checklist for AIX 7.1
11040	DISA STIG Checklist for HPUX 11.11
11460	DISA STIG Checklist for HPUX 11.23 - RG03
11462	DISA STIG Checklist for HPUX 11.31 - RG03
11458	DISA STIG Checklist for Internet Explorer 10 - RG03
12068	DISA STIG Checklist for Internet Explorer 11 - RG03
11454	DISA STIG Checklist for Internet Explorer 8 - RG03
11456	DISA STIG Checklist for Internet Explorer 9 - RG03
12309	DISA STIG Checklist for Mac OS X 10.10
12427	DISA STIG Checklist for Mac OS X 10.11
12225	DISA STIG Checklist for Mac OSX 10.8
12346	DISA STIG Checklist for Mac OSX 10.9
12497	DISA STIG Checklist for Oracle Linux 6
11042	DISA STIG Checklist for RHEL 3
11043	DISA STIG Checklist for RHEL 4
11430	DISA STIG Checklist for RHEL 5 - RG03

Site ID	Site Name
11440	DISA STIG Checklist for RHEL 6 RG03, CentOS Linux 6 RG03
12412	DISA STIG Checklist for RHEL 7, CentOS Linux 7
11432	DISA STIG Checklist for Solaris 10 - RG03
12281	DISA STIG Checklist for Solaris 11
11045	DISA STIG Checklist for Solaris 8
11046	DISA STIG Checklist for Solaris 9
11048	DISA STIG Checklist for SUSE 10
11059	DISA STIG Checklist for SUSE 11
11058	DISA STIG Checklist for SUSE 9
12289	DISA STIG Checklist for Windows 10
11141	DISA STIG Checklist for Windows 2003 DC
11142	DISA STIG Checklist for Windows 2003 MS
11143	DISA STIG Checklist for Windows 2008 DC
11144	DISA STIG Checklist for Windows 2008 MS
11145	DISA STIG Checklist for Windows 2008 R2 DC
11146	DISA STIG Checklist for Windows 2008 R2 MS
11575	DISA STIG Checklist for Windows 2012 DC
11577	DISA STIG Checklist for Windows 2012 MS
12467	DISA STIG Checklist for Windows 2016
11140	DISA STIG Checklist for Windows 7
11564	DISA STIG Checklist for Windows 8
11147	DISA STIG Checklist for Windows Vista
11148	DISA STIG Checklist for Windows XP

Site ID	Site Name
11120	FDCC Checklist for Internet Explorer 7
11123	FDCC Checklist for Windows Vista
11124	FDCC Checklist for Windows Vista Firewall
11121	FDCC Checklist for Windows XP
11122	FDCC Checklist for Windows XP Firewall
13013	IBM License Reporting (ILMT) v9
8506	MaaS360 Mobile Device Management
12380	Managed Vulnerabilities
8150	Patching Support
8102	Power Management
15105	QRadar Vulnerabilties
8110	Remote Control
6113	SCM Reporting
9188	Software Distribution
8032	Tivoli Endpoint Manager for Software Usage Analysis v1.3
9072	Trend Common Firewall
9095	Trend Core Protection Module for Mac
11119	USGCB Checklist for Internet Explorer 7
11113	USGCB Checklist for Internet Explorer 8
12106	USGCB Checklist for RHEL 5
11110	USGCB Checklist for Windows 7
11112	USGCB Checklist for Windows 7 Energy
11111	USGCB Checklist for Windows 7 Firewall
11116	USGCB Checklist for Windows Vista
11114	USGCB Checklist for Windows Vista Energy
11115	USGCB Checklist for Windows Vista Firewall

Site ID	Site Name
11118	USGCB Checklist for Windows XP
11117	USGCB Checklist for Windows XP Firewall
8346	Virtual Endpoint Manager
5040	Vulnerabilities to Windows Systems
9112	Windows 7 Migration
9173	Windows Point of Sale
8232*	Updates for Mac Applications
5095*	Updates for Windows Applications

Attention: * The content from these sites is available in the **Patches** app.

Chapter 13. Get Started with Extensions Management Application

BigFix Extension Management application provides you the possibility to extend WebUI features beyond what is delivered in the products that you are currently entitled to. You can address specific use cases that are not currently fulfilled by the product by adding ad-hoc extensions to WebUI.

Developing extensions

With this release, to accelerate the customization of the interface to your needs, the development of extensions is limited to HCL personnel. Future releases of this feature will enable organizations to develop extensions on their own via a public toolkit that HCL delivers.

High-level process flow

The high-level steps to develop a customized extension and manage it is as follows:

1. Organizations contact their HCL representative to define business requirements and engage with the appropriate team within HCL to develop an extension.
2. HCL team develops a WebUI extension to add a new capability that is not available on the WebUI to address the customer request and delivers the extension by publishing it on an external site or by sharing the extension file.
3. WebUI Administrator enables the capability of Extension Management in WebUI.
4. WebUI user (Master operator or Content creator with read and write permissions to the necessary custom sites) from your organization receives or downloads the extension application file (`*.webui)` and installs it on to the custom sites.
5. After the extension is installed, it becomes accessible from WebUI under Extension Management. Users with appropriate site access and permissions can use them seamlessly together with the rest of the applications and manage the extensions from WebUI.

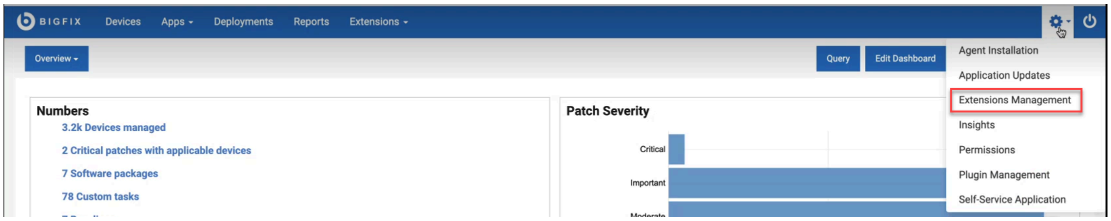
Access Extension Management

By default, Extension Management is not added to WebUI. To add it, contact your WebUI Administrator to configure the server setting `_WebUIAppEnv_ENABLE_EXTENSIONS_MANAGEMENT`. For the changes in the server setting to take effect, restart the WebUI after configuring.

Users and roles

Master operator and Content creators

Master Operators and Content Creators can install, manage, and use the extension management applications.



They can manage the extension applications as follows:

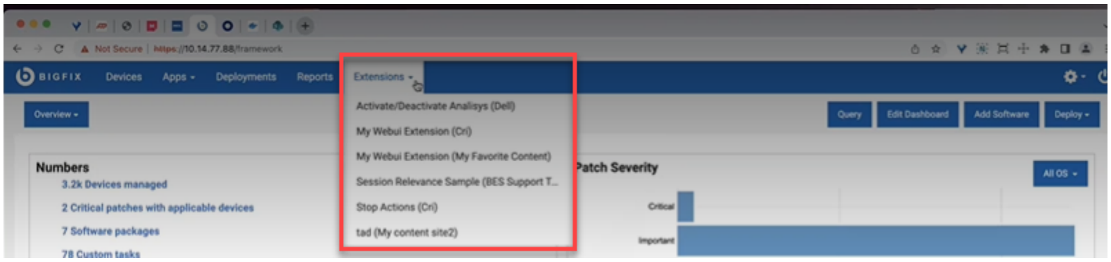
- Install a new extension from an external site or from an extension file (`*.webui)` as indicated by the HCL representative.
- Launch an extension
- Repair an extension
- Update an extension
- Search, sort, filter, and navigate through extensions
- Uninstall or remove an old obsolete extension

Note:

- Master operators can manage all the extensions available to an organization as they have access to all the custom sites. Content Creators can only manage the extensions available within the sites accessible to them.
- External sites are read only sites for both Master Operators and Content Creators, and they cannot remove any extensions from the external site.

Non-Master Operators

NMOs can view the extensions installed on the custom sites visible to them. They can launch an extension application from the Extensions menu and work with it. They cannot manage or perform any administrative actions on the extensions.



:

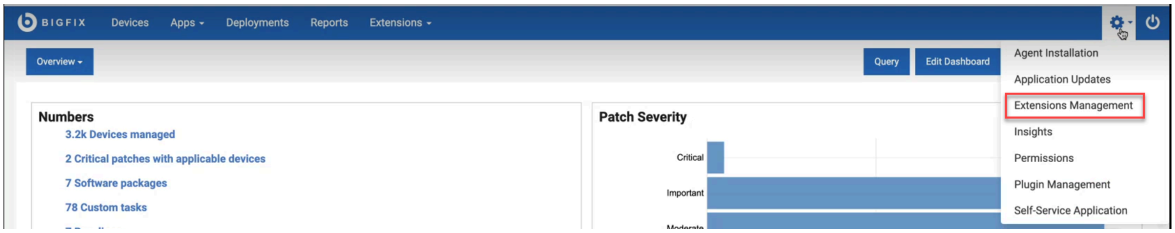
Installing an extension from a site

Read this page to learn how to install an extension from an external site.

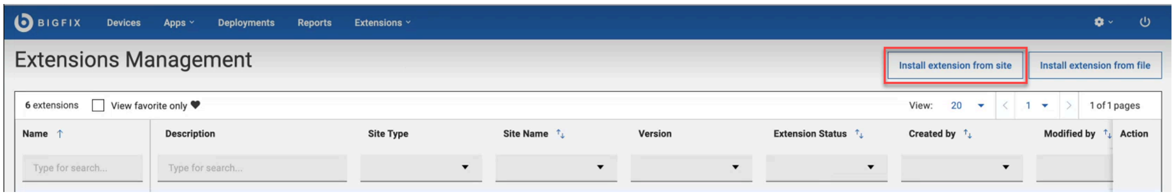
- You must be a Master Operator or a Content Creator with read and write access to the required custom site to perform this task.
- Ensure the extension is already made available on the external site.

To install an extension from an external site, complete the following steps:

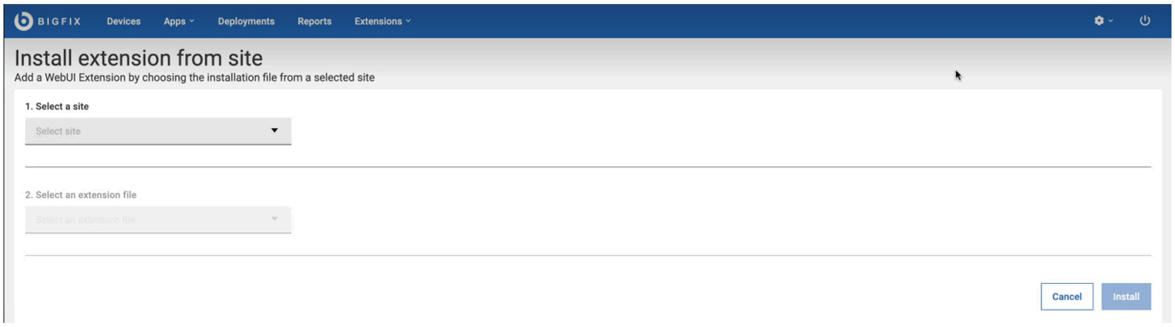
1. Log in to WebUI with appropriate credentials.
2. From the menu bar click settings and select **Extensions Management**.



3. On the Extension Management page, click **Install extension from site**.



4. The following page appears.


BIGFIX
Devices
Apps
Deployments
Reports
Extensions
Install extension from site
Add a WebUI Extension by choosing the installation file from a selected site
1. Select a site
Select site
2. Select an extension file
Select an extension file
Cancel
Install

From the drop-down:

   a. Select a site in which the extension file is available.

   Note: You can view only the sites that you have access to.

   b. Select an extension file. You can view all the extensions that are published to the selected site.
5. Click **Install**.
6. Once the extension is successfully installed, it is listed on the Extension Management page.

Related information

[Working with extensions *(on page 167)*](#)

[Updating an extension *(on page 169)*](#)

[Uninstalling an extension *(on page 171)*](#)

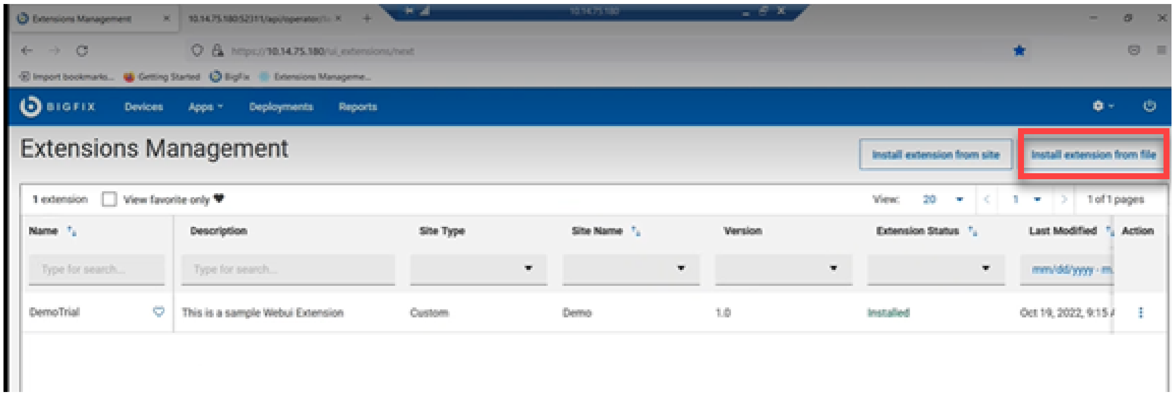
Installing an extension from file

Read this page to learn how to install an extension from a file.

You must be a Master Operator or a Content Creator with read and write access to the custom site to perform this task.

To install an extension from a file, complete the following steps:

1. Log in to WebUI with appropriate credentials.
2. From the menu bar, click **Extension Management**.
3. Click **Install extension from file**.

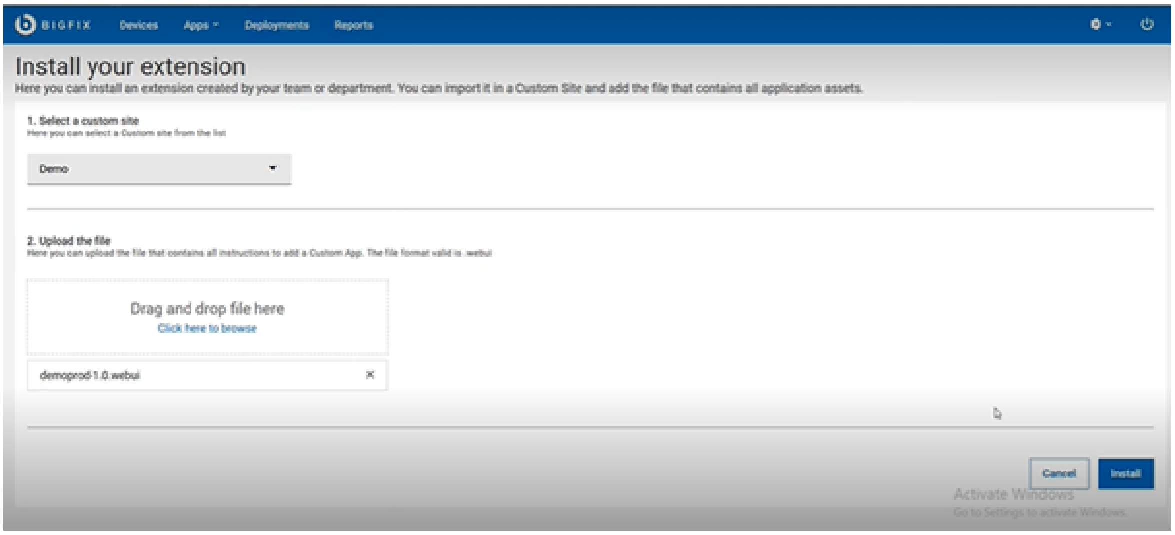


Extensions Management

1 extension

Name	Description	Site Type	Site Name	Version	Extension Status	Last Modified	Action
DemoTrial	This is a sample Webui Extension	Custom	Demo	1.0	Installed	Oct 19, 2022, 9:15	⋮

4. Select a custom site where the extension will be installed.
5. Upload the file that contains all instructions to add a custom app. The valid file format is `.webui`.



Install your extension

Here you can install an extension created by your team or department. You can import it in a Custom Site and add the file that contains all application assets.

1. Select a custom site
Here you can select a Custom site from the list

Demo

2. Upload the file
Here you can upload the file that contains all instructions to add a Custom App. The file format valid is .webui

Drag and drop file here
Click here to browse

demoprod-1.0.webui ×

6. Click **Install**.
7. Once the extension is successfully installed, a success message is displayed and the extension is listed on the Extension Management grid.

Related information

[Working with extensions *(on page 167)*]

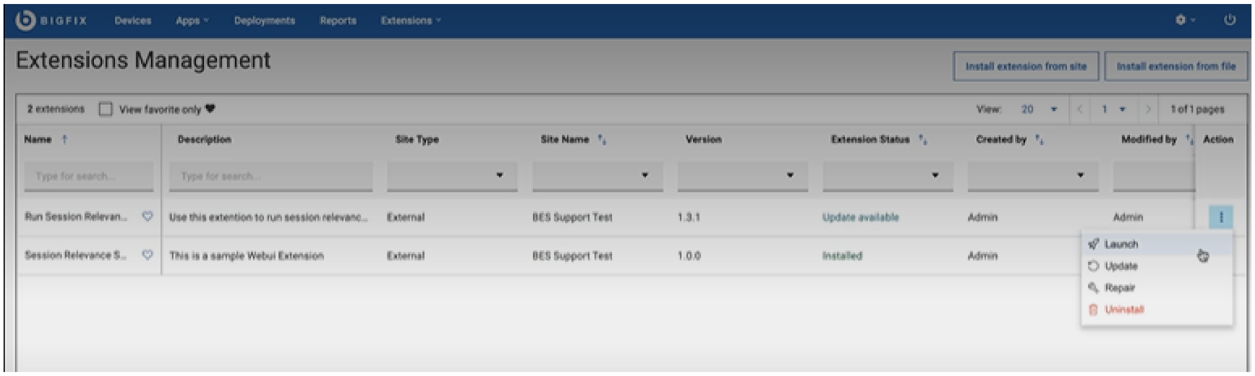
[Updating an extension *(on page 169)*]

[Uninstalling an extension *(on page 171)*]

Working with extensions

Read this page to learn to work with the extensions.

After installing an extension, it is listed in the Extension Management grid.



Extensions Management

2 extensions □ View favorite only ♥ View: 20 1 1 of 1 pages

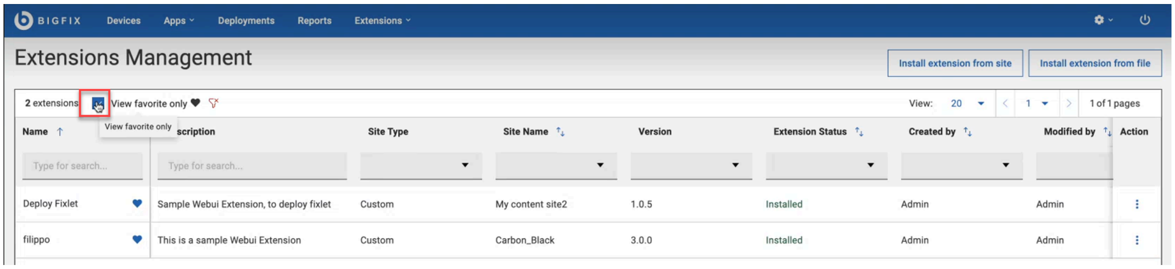
Name	Description	Site Type	Site Name	Version	Extension Status	Created by	Modified by	Action
Type for search...	Type for search...							
Run Session Relevan...	Use this extention to run session relevanc...	External	BES Support Test	1.3.1	Update available	Admin	Admin	⋮
Session Relevance S...	This is a sample Webui Extension	External	BES Support Test	1.0.0	Installed	Admin		

You can perform the following actions from the menu under Actions column:

- **Launch *(on page 168)***: Once an extension is installed, you can launch that extension to work with it.
- **Update** *(on page 169)*: Update your extensions when a newer version is available in the external site. For more information refer to the link *(on page 169)*.
- **Repair**: When the Extension Status of an extension application displays *To Repair* it means that the extension application file needs a repair. Click the To Repair link to repair and reinstall the extension for the application to work as intended.
- **Uninstall *(on page 171)***: You can uninstall an extension that is no longer needed.

You can also perform the following actions from the Extensions Management grid:

- **Favorite**: Click the favorite icon ♡ to mark an extension as your favorite. When you select the View favorite only checkbox, the grid displays only the extensions that are marked as favorite.



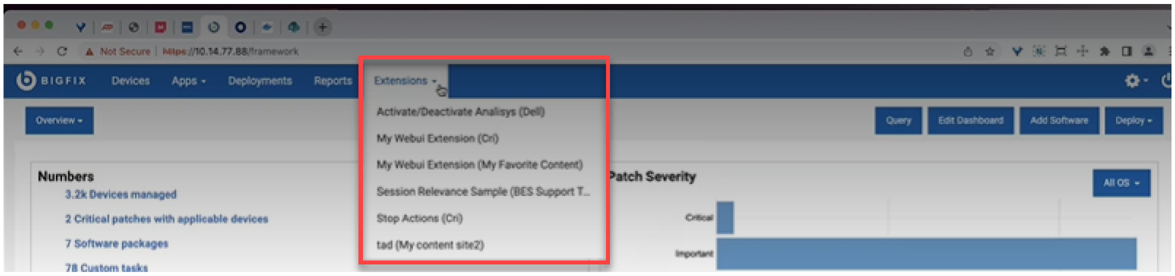
Name ↑	scription	Site Type	Site Name ↑↓	Version	Extension Status ↑↓	Created by ↑↓	Modified by ↑↓	Action
Deploy Fixlet ♥	Sample Webui Extension, to deploy fixlet	Custom	My content site2	1.0.5	Installed	Admin	Admin	⋮
filippo ♥	This is a sample Webui Extension	Custom	Carbon_Black	3.0.0	Installed	Admin	Admin	⋮

- **Filter**: You can filter the extensions by Name, Description, Site Type, Site Name, Versions, Extension Status, Created by, Modified by, Last Modified Time. You can search by text or select an option under a column as applicable to filter the required data.
- **Sort**: You can sort the extensions by Name, Site Name, Extension Status, Created by, Modified by, and Last Modified Time columns.
- **Paginate and navigate**: You can select a number from the View dropdown to set the number of extensions that can be displayed on a page. Using the left and right arrows, you can navigate through the pages.

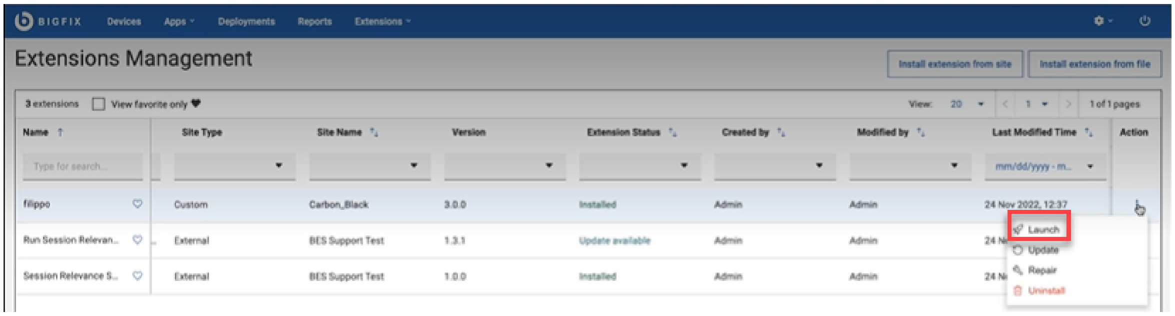
Launch

If you have signed in as a Master Operator or a Content Creator, you can launch an extension in the following ways:

- Launch an extension directly from the Extensions menu. The Extensions menu displays a list of all installed extension applications that are already installed. When you launch an extension from here, the relevant extension application is opened in the same page. You can work with one extension application at a time from here.



- Launch an extension application from the **Actions** sub-menu. To do that, under the Actions column, click the menu icon for a desired extension and select Launch. This opens the extension application in a new window. You can open one or more extensions and every extension application opens in a new tab.



Extensions Management

3 extensions □ View favorite only View: 20 1 1 of 1 pages

Name	Site Type	Site Name	Version	Extension Status	Created by	Modified by	Last Modified Time	Action
filippo	Custom	Carbon_Black	3.0.0	Installed	Admin	Admin	24 Nov 2022, 12:37	
Run Session Relevan...	External	BES Support Test	1.3.1	Update available	Admin	Admin	24 N	
Session Relevance S...	External	BES Support Test	1.0.0	Installed	Admin	Admin	24 N	

If you have signed in as a NMO, the extension applications installed on the sites accessible to you are displayed under Extensions menu. You can select an extension application to launch it directly from there.

Related information

Updating an extension *(on page 169)*

Updating an extension

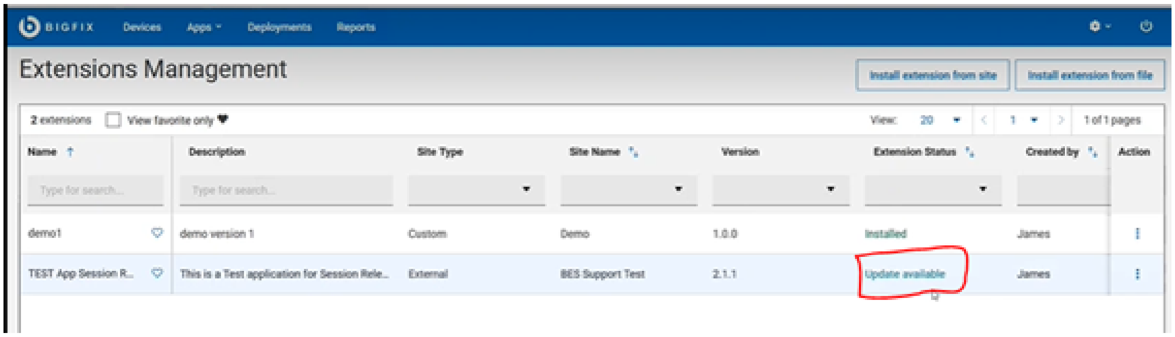
You can update an extension when a newer version of the extension is available.

Before you begin: You must be a Master Operator or a Content Creator with read and write access to the required custom site to perform this task.

Update from external site

If an extension is installed through the "Install from site" option, whenever a newer version of that extension is published in the respective external site, the Extension Status displays the status as "Update available". To update the extension, complete the following steps:

1. Check the **Extension Status** for available update.

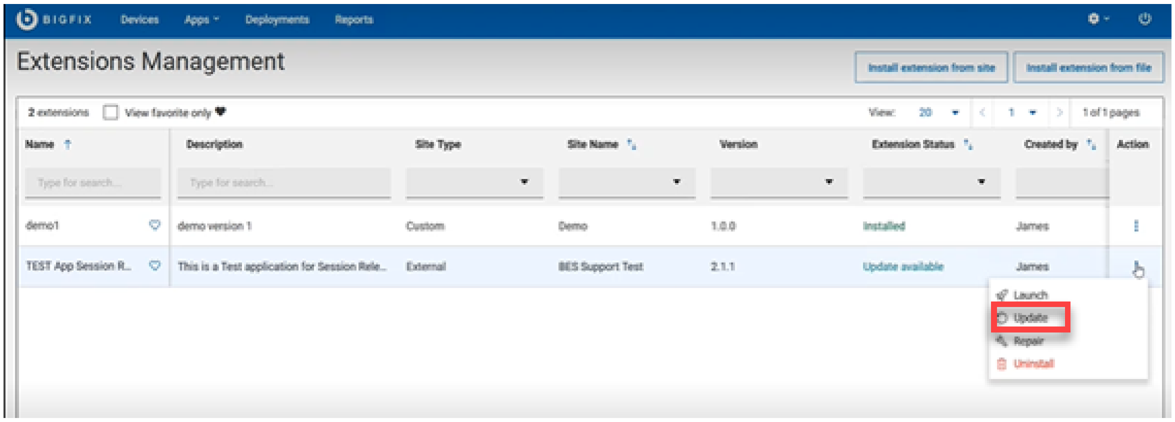


Extensions Management

2 extensions □ View favorite only View: 20 1 1 of 1 pages

Name	Description	Site Type	Site Name	Version	Extension Status	Created by	Action
demo1	demo version 1	Custom	Demo	1.0.0	Installed	James	⋮
TEST App Session R...	This is a Test application for Session Rele...	External	BES Support Test	2.1.1	Update available	James	⋮

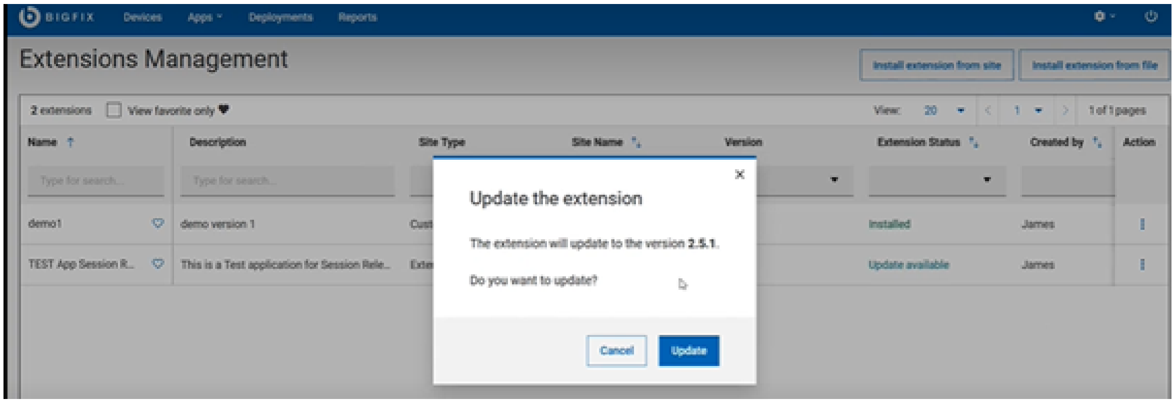
2. Click the **Update available** link to update. Alternatively, you can also click the menu icon under **Actions** column corresponding to the extension and select **Update**.



Name	Description	Site Type	Site Name	Version	Extension Status	Created by	Action
demo1	demo version 1	Custom	Demo	1.0.0	Installed	James	⋮
TEST App Session R...	This is a Test application for Session Rele...	External	BES Support Test	2.1.1	Update available	James	⋮

Note: For the extensions installed from site, the Update option in the dropdown is enabled only when the Extension Status shows Update available.

3. Confirm update.



Update the extension

The extension will update to the version **2.5.1**.

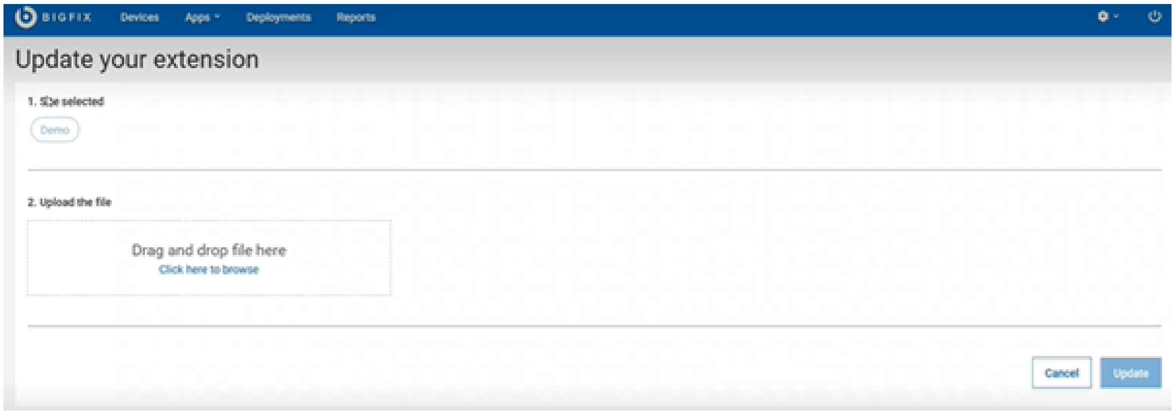
Do you want to update?

Success message is displayed and the Extension status is changed to "Installed".

Update from custom site

If an extension is installed through "Install extension from file" option, you can update an extension to a newer version by navigating to the extension file uploaded on the custom site. To do that, complete the following steps:

1. Click the menu icon under **Actions** column corresponding to an extension and select **Update**.
2. On the Update your extension page, drag and drop the newer version of extension file or click the "click here to browse" link to navigate and locate the newer version of the extension file from the custom site.



Update your extension

1. Site selected

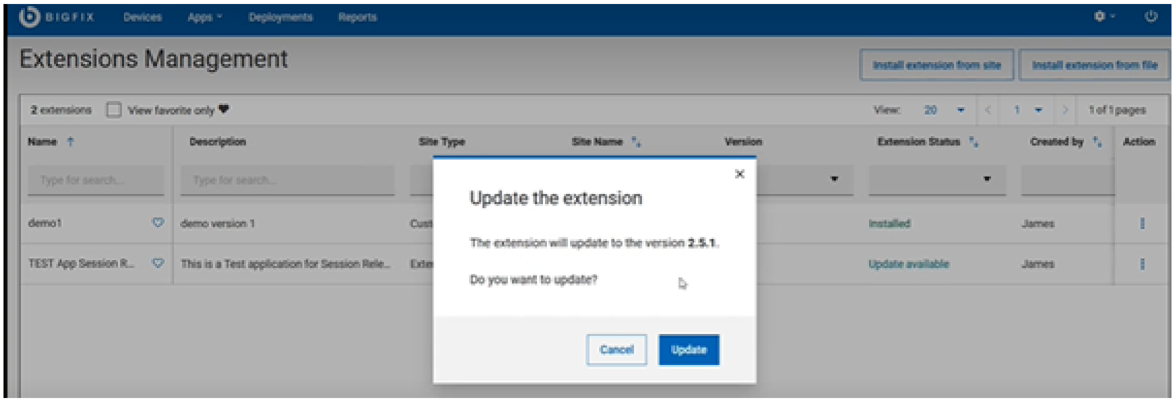
Demo

2. Upload the file

Drag and drop file here
Click here to browse

Note: "Site selected" automatically picks up and displays the site from which the extension was initially installed. You cannot change this while updating an extension.

3. Confirm update.



Extensions Management

2 extensions

Name	Description	Site Type	Site Name	Version	Extension Status	Created by	Action
demo1	demo version 1	Cust			Installed	James	⋮
TEST App Session R...	This is a Test application for Session Rele...	Exte			Update available	James	⋮

Update the extension

The extension will update to the version **2.5.1**.

Do you want to update?

Extension status is now changed to Installed.

Downgrade an extension

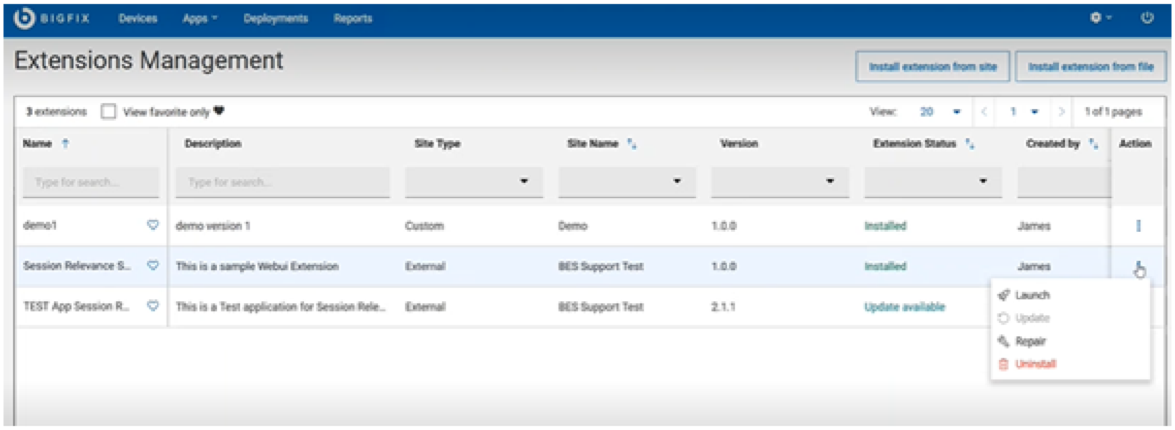
You can also downgrade an extension from the current version to an older version. To do that, while updating an extension, select an older version of the extension file from an external site or from a custom site as applicable.

Uninstalling an extension

You can uninstall an extension that is no longer needed.

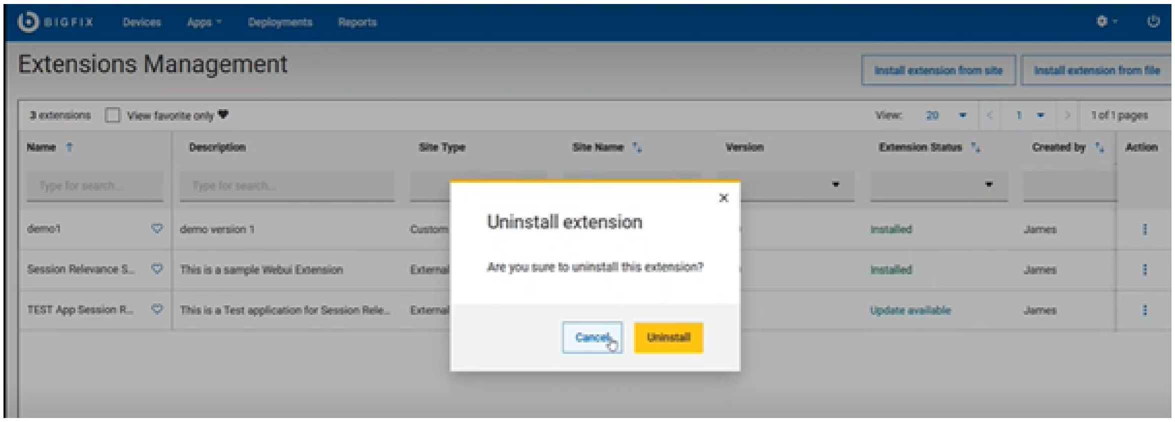
To uninstall an extension complete the following steps:

1. From the Extension management page, click the drop-down menu corresponding to an extension that you want to uninstall and from the menu, select **Uninstall**.



Name	Description	Site Type	Site Name	Version	Extension Status	Created by	Action
demo1	demo version 1	Custom	Demo	1.0.0	Installed	James	⋮
Session Relevance S...	This is a sample Webui Extension	External	BES Support Test	1.0.0	Installed	James	⋮
TEST App Session R...	This is a Test application for Session Rele...	External	BES Support Test	2.1.1	Update available		

2. In the pop-up window, click **Uninstall** to confirm uninstalling.



Uninstall extension

Are you sure to uninstall this extension?

Note: If you are uninstalling an extension from a custom site, you can also remove the extension file uploaded to that site.

Chapter 14. Modern Client Management and BigFix Mobile

This section guides you through BigFix Modern Client Management (MCM) and BigFix Mobile to understand the MCM concepts, terminologies, features, and functionality. You can find detailed instructions for managing the complete lifecycle of your MDM managed endpoints here.

Overview

- BigFix delivers an agent capability to endpoint management that dynamically provides visibility to every endpoint. BigFix WebUI facilitates to manage modern devices that do not have a BigFix agent installed as well as to manage traditional devices that have BigFix agent installed. BigFix agent initiates downloads, patches, configurations, and other content to the endpoint in real-time; initiates actions and performs continuous self-assessment and policy enforcement. BigFix also provides agentless management for Windows, macOS, iOS, and Android endpoints.
- For architecture overview and other detailed information on MDM on-premises , see On premises deployments.
- BigFix extends management to corporate-owned and BYOD devices running Windows, macOS, iOS, iPadOS, and Android by delivering important actions and out-of-the-box policies to effectively manage the endpoints.

BigFix MCM

With BigFix MCM you can extend the management capabilities to modern laptops with Windows and macOS operating systems by leveraging MDM technology.

BigFix Mobile

BigFix Mobile extends endpoint management to iOS, iPadOS, and Android devices.

Prerequisites

For complete details, see Prerequisites and requirements.

Feature overview

Modern Client Management and BigFix Mobile facilitates the management of modern clients in your environment in the following ways:

Device enrollment

BigFix MCM supports various enrollment methods for devices with different operating systems based on the organization’s need. For more details, see Device Enrollment.

MCM Dashboard

BigFix Modern Client Management dashboard (on page 175) provides:

- Insights about the MCM managed devices in your environment and the health of the overall MCM deployment.
- Quick glance of statistics on every aspect of device management, device security, and device encryption.
- Notifications on important statistics such as number of reporting and non-reporting devices, number of succeeded and failed actions.
- An overview on the total number of devices enrolled, number of devices with each operating system, and type of device such as mobile or desktop.
- A quick access to your daily tasks, help information, and the link to create support ticket.

Deploy BigFix agent (MCM only)

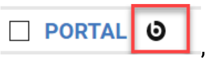
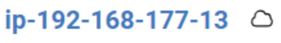
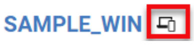
With MCM, you can deploy the BigFix agent on enrolled macOS or Windows devices through WebUI. Enrolled MCM devices that also have the BigFix agent installed benefit from the capabilities of both management capabilities, and users see one consolidated representation of the device. Actions from both the BigFix agent and MDM APIs are available to these correlated devices.

Device inventory (MCM and BigFix Mobile)

With MCM and BigFix Mobile, you can view critical device information in the device list *(on page 23)*, regardless of whether the information is pulled from the native BigFix agent, MDM, or cloud instances.

Note: Non-Master Operators must have the access permission to the mobile site (BESUEM Mobile) to access the mobile related content in WebUI.

Simplified Device Representations (MCM and BigFix Mobile)

On the WebUI, an icon indicates the type of each device on your network (native  □ PORTAL, cloud  ip-192-168-177-13, or MDM  SAMPLE_WIN). When an endpoint has more than one representation, it shows multiple icons. A device that has multiple representations is called a correlated device.

Device Management (MCM and BigFix Mobile)

MCM and BigFix Mobile provides additional capabilities and policies to help manage modern desktops such as macOS and Windows and mobile devices such as Android, iOS, and iPadOS. It supports actions such as lock, wipe, restart, shutdown, You can apply capabilities that are captured in BigFix artifacts called *Policies*.

Device Security

MCM and BigFix Mobile facilitates enforcement of security policies on managed devices. With this, IT admins can ensure that all managed devices have the right settings set for passwords, restrictions, and more.

Application Management (MCM and BigFix Mobile)

MCM enables you to pre-stage applications on the MDM server to distribute them to macOS and Windows endpoints through policy groups. BigFix Mobile enables you distribute basic store applications from Play store and App store.

Policy Management (MCM and BigFix Mobile)

BigFix MCM and BigFix Mobile enables you to set common passcode policies and restriction policies across your Apple (macOS, iOS, and iPadOS), Windows, and Android devices. You can also upload custom policies suitable for your organization and the device's operating system. For a list of policies available for different operating systems, see Manage policies *(on page 267)*.

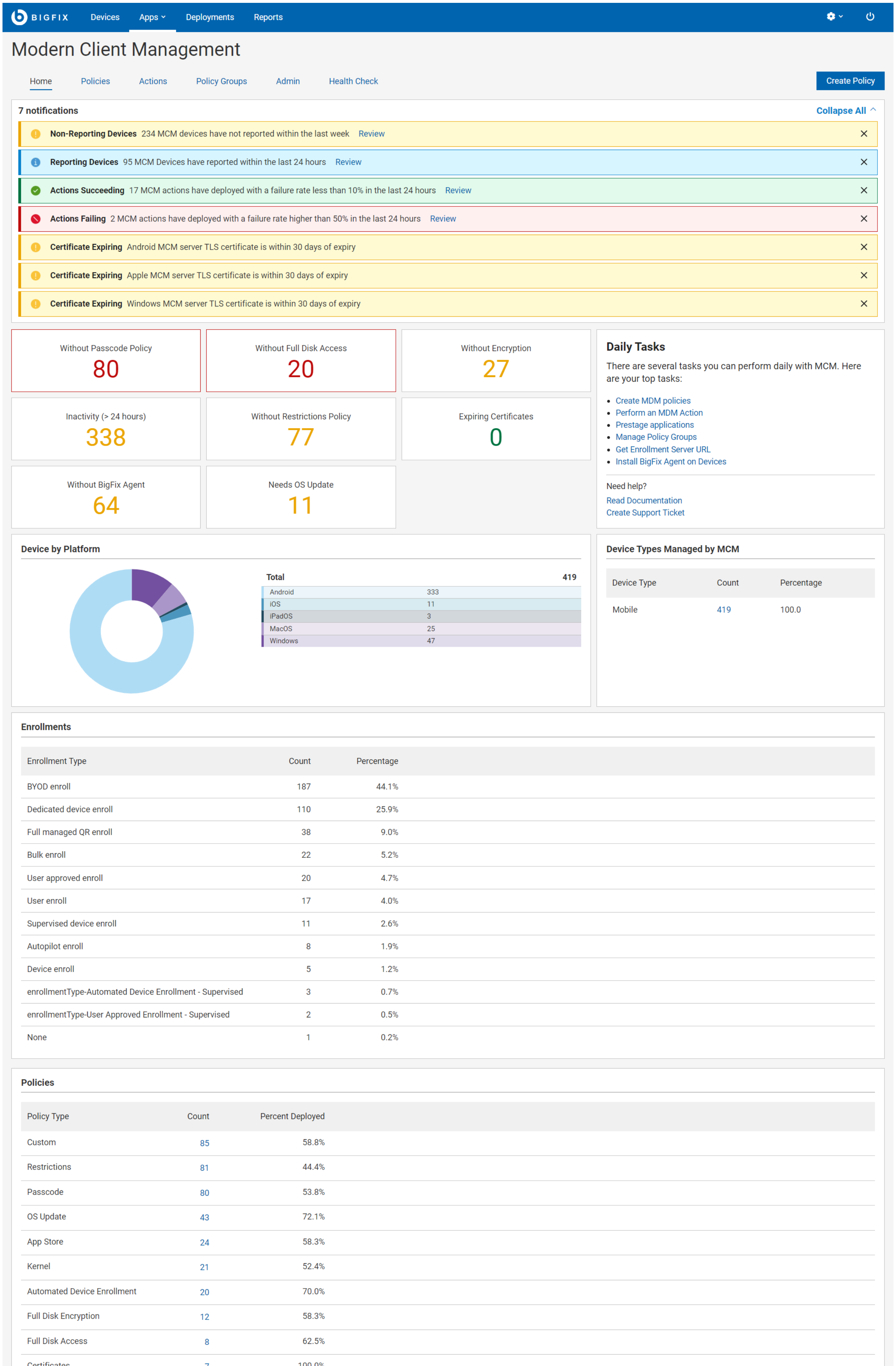
License requisite

- You can manage Laptops via MDM API's and the WebUI with BigFix MCM, BigFix Lifecycle, and BigFix Compliance licenses.
- Managing Mobile devices in BigFix requires a BigFix Mobile license.

Modern Client Management dashboard

The MCM dashboard is the home page of the MCM application. It provides insights into every aspect of device management, device security, and device encryption of MDM managed devices.

To view MCM dashboard, from the WebUI main page, click **Apps > MCM**.



Modern Client Management

7 notifications

- **Non-Reporting Devices** 234 MCM devices have not reported within the last week Review
- **Reporting Devices** 95 MCM Devices have reported within the last 24 hours Review
- **Actions Succeeding** 17 MCM actions have deployed with a failure rate less than 10% in the last 24 hours Review
- **Actions Failing** 2 MCM actions have deployed with a failure rate higher than 50% in the last 24 hours Review
- **Certificate Expiring** Android MCM server TLS certificate is within 30 days of expiry
- **Certificate Expiring** Apple MCM server TLS certificate is within 30 days of expiry
- **Certificate Expiring** Windows MCM server TLS certificate is within 30 days of expiry

Without Passcode Policy 80

Without Full Disk Access 20

Without Encryption 27

Inactivity (> 24 hours) 338

Without Restrictions Policy 77

Expiring Certificates 0

Without BigFix Agent 64

Needs OS Update 11

Daily Tasks

There are several tasks you can perform daily with MCM. Here are your top tasks:

- Create MDM policies
- Perform an MDM Action
- Prestage applications
- Manage Policy Groups
- Get Enrollment Server URL
- Install BigFix Agent on Devices

Need help?
Read Documentation
Create Support Ticket

Device by Platform

Total	419
Android	333
iOS	11
iPadOS	3
MacOS	25
Windows	47

Device Types Managed by MCM

Device Type	Count	Percentage
Mobile	419	100.0

Enrollments

Enrollment Type	Count	Percentage
BYOD enroll	187	44.1%
Dedicated device enroll	110	25.9%
Full managed QR enroll	38	9.0%
Bulk enroll	22	5.2%
User approved enroll	20	4.7%
User enroll	17	4.0%
Supervised device enroll	11	2.6%
Autopilot enroll	8	1.9%
Device enroll	5	1.2%
enrollmentType-Automated Device Enrollment - Supervised	3	0.7%
enrollmentType-User Approved Enrollment - Supervised	2	0.5%
None	1	0.2%

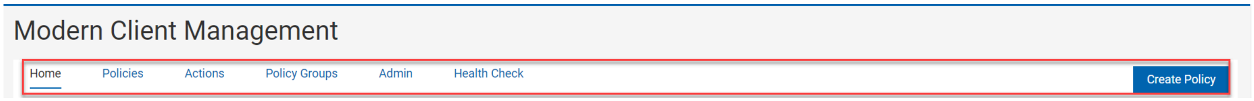
Policies

Policy Type	Count	Percent Deployed
Custom	85	58.8%
Restrictions	81	44.4%
Passcode	80	53.8%
OS Update	43	72.1%
App Store	24	58.3%
Kernel	21	52.4%
Automated Device Enrollment	20	70.0%
Full Disk Encryption	12	58.3%
Full Disk Access	8	62.5%
Certificates	7	100.0%

Important: Ensure under Health Check *(on page 186)* all analyses are activated to view expected data in the MCM dashboard**.**

Navigation bar

The navigation bar is displayed at the top of the page throughout the MCM application. It helps you to navigate to any feature page with ease.



- Home – From any page in the application, clicking on Home tab takes you to the MCM dashboard page.
- Policies *(on page 267)* – From this tab, you can create and manage policies.
- Actions *(on page 304)* – From this tab, you can initiate MCM actions on your devices including lock, wipe, restart, shut down, remove policy and much more.
- Policy Groups *(on page 269)* – From this tab, you can create and manage policy groups.
- Admin – From this tab, you can set up your MCM components *(on page 189)*, prestage installers and apps, configure enrollment settings, and set up recovery key.
- Health Check *(on page 186)* – From this tab, you can monitor the statuses of all MCM components for different operating systems in your environment.
- Clicking the **Create Policy** button opens the Policies *(on page 267)* page, where you can see the list of policy types. You can click on a policy type according to your operating system and the requirement to create a policy.

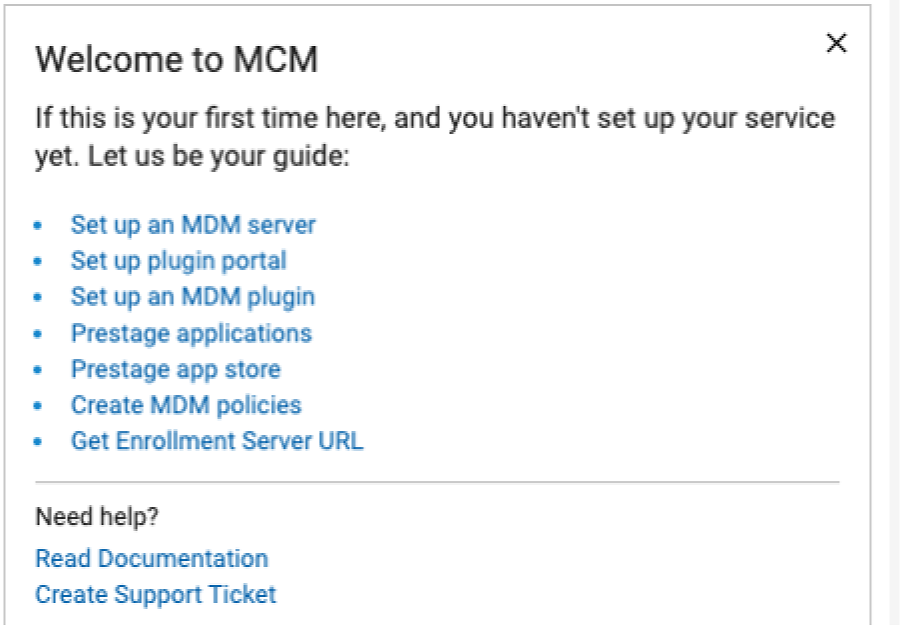
Overview

The dashboard displays various information and statistics. The statistics in each section of the dashboard depends on the access permission of the logged in user and the overall license level of the deployment. For example, organizations without BigFix Mobile license cannot view data related to iOS, iPadOS, or Android devices. Also the numbers displayed differs for a master operator and a non-master operators depending on the device ownership permissions configured through the BigFix Console.

Clicking on any clickable statistical item in the dashboard takes you to the filtered list of that specific item, which enables you to take any necessary action on that list of items.

Welcome To MCM

For the first time Master Operators, this section provides quick links to set up the MDM server and other administrative tasks. You can also go to MCM documentation page for help information or create support ticket from here.



Welcome to MCM

If this is your first time here, and you haven't set up your service yet. Let us be your guide:

- Set up an MDM server
- Set up plugin portal
- Set up an MDM plugin
- Prestage applications
- Prestage app store
- Create MDM policies
- Get Enrollment Server URL

Need help?

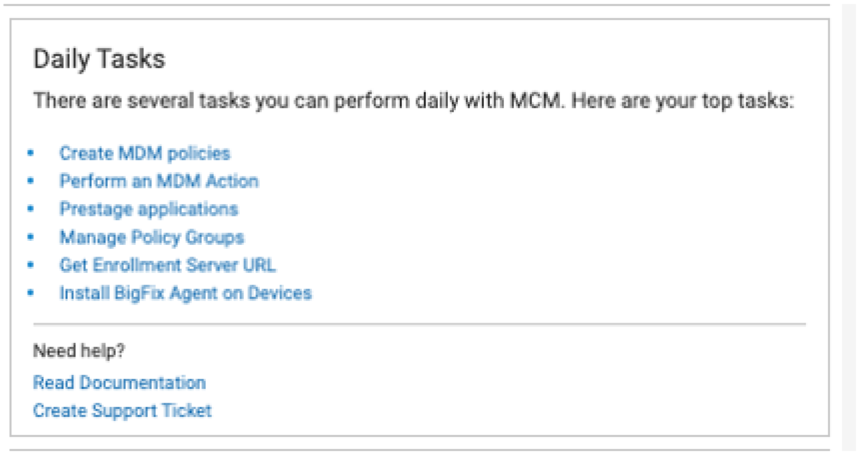
Read Documentation

Create Support Ticket

Daily Tasks

Once a Master Operator dismisses the Welcome to MCM, the Daily Tasks appears going forward on all subsequent visits to the MCM dashboard. This section provides quick links to the tasks to manage your devices. You can also go to MCM Admin Guide for help information or create support ticket from here.

Note: Non Master Operators visiting the MCM Dashboard can only see the Daily Tasks tile.



Daily Tasks

There are several tasks you can perform daily with MCM. Here are your top tasks:

- Create MDM policies
- Perform an MDM Action
- Prestage applications
- Manage Policy Groups
- Get Enrollment Server URL
- Install BigFix Agent on Devices

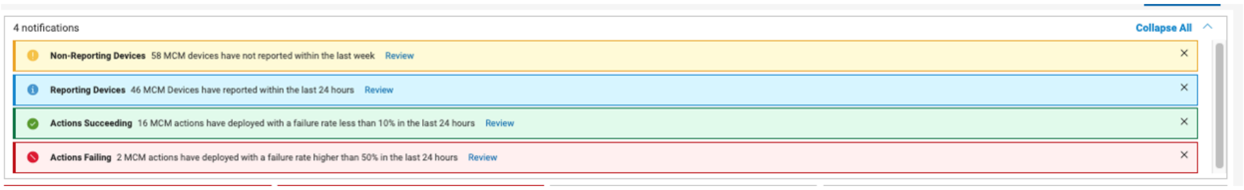
Need help?

Read Documentation

Create Support Ticket

Notifications

The **notifications** section provides quick information, warnings, and alerts about the overall MDM Deployment.



4 notifications

Non-Reporting Devices 58 MCM devices have not reported within the last week

Reporting Devices 46 MCM Devices have reported within the last 24 hours

Actions Succeeding 16 MCM actions have deployed with a failure rate less than 10% in the last 24 hours

Actions Failing 2 MCM actions have deployed with a failure rate higher than 50% in the last 24 hours

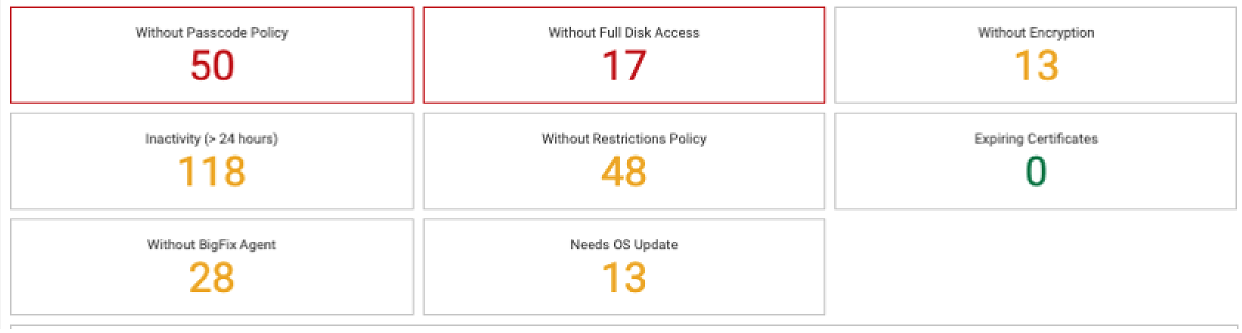
It displays:

- MDM devices reported within 24 hours
- MDM devices that did not report within 24 hours
- Recent succeeded deployments (with less than 10% failure in 24 hours)
- Recent failed deployments (with greater than 50% failure in 24 hours)
- Warnings and errors about various MDM certificates (warning when certificates are within 30 days of expiry; errors when certificates expire). The following certificates are evaluated:
  - Apple Push certificate
  - Auth CA certificate
  - Auth certificate
  - TLS certificate

Click the **Review** link next to a notification to view the filtered list of devices specific to that notification. You can expand or collapse the notification section by clicking the **Collapse All** toggle.

Number Tiles

The widgets in the dashboard provide an overview about the policies applied on the managed devices.



Without Passcode Policy 50	Without Full Disk Access 17	Without Encryption 13
Inactivity (> 24 hours) 118	Without Restrictions Policy 48	Expiring Certificates 0
Without BigFix Agent 28	Needs OS Update 13	

It counts the policies deployed through the following methods:

- A policy deployed individually through Policies *(on page 267)*
- A policy deployed by targeting a device through a policy group action
- A default policy deployed at the time of enrollment through a policy group

The following Number Tiles are shown in the dashboard:

- **Without Passcode Policy** - Number of devices without Passcode policy *(on page 275)* applied. This counts all the devices with different operating systems in the MDM environment.
- **Without Full Disk Access** - Number of macOS devices without Full Disk Access *(on page 284)* policy applied
- **Without Encryption** - Number of macOS and Windows devices without Disk Encryption Policy *(on page 288)* policy applied
- **Inactivity (> 24 hours)** - Number of devices that did not report to MDM for more than 24 hours, including the correlated devices.
- **Without Restrictions Policy** - Number of devices without Restrictions Policy *(on page 284)* applied. This counts all the devices with different operating systems in the MDM environment.
- **Expiring Certificates** - Number of macOS/iOS/iPadOS devices with certificates set to expire within 30 days. This widget also counts the number of devices that have already had their device certificate expire.

  Note:
  - Devices that have their device certificate expired must re-enroll in MDM to report to MDM properly again.
  - To update Apple enrollment certificates, run Fixlet 3000 in BESUEM on relevant devices. Fixlet 3000 can be run as an open-ended policy action that applies to all devices that become relevant when they get close to their expiration time.

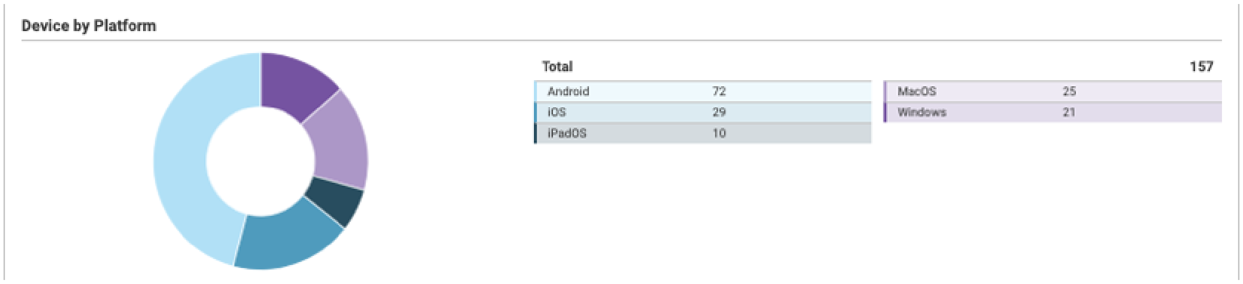
- **Without BigFix Agent** - Number of macOS and Windows devices that do not have BigFix agent installed.
- **Needs OS Update** - Number of devices that need their OS to be updated.

  Note: Currently this is limited to iOS/iPad counts only.

Device by Platform

This section shows the total number of devices enrolled to MCM and BigFix Mobile. It shows a pie chart and a table with a breakdown on enrolled devices' operating systems.

Clicking on the pie chart or the individual rows on the table leads to a device list filtered with the selected MDM operating system.



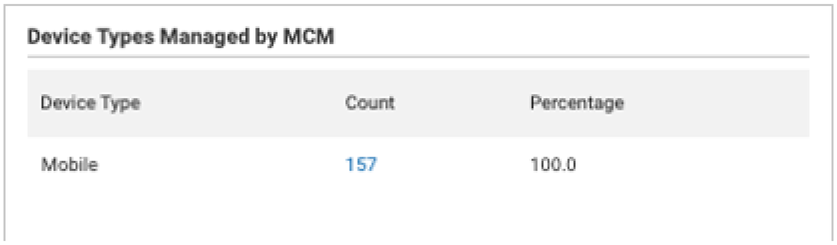
Device by Platform

Total			157
Android	72	MacOS	25
iOS	29	Windows	21
iPadOS	10		

Device Types Managed by MCM

This section shows the total number of devices of every device type managed by MCM and BigFix Mobile in your environment. It also shows the data in percentage.

Clicking on the count corresponding to a device type leads to the list of devices filtered with that device type.



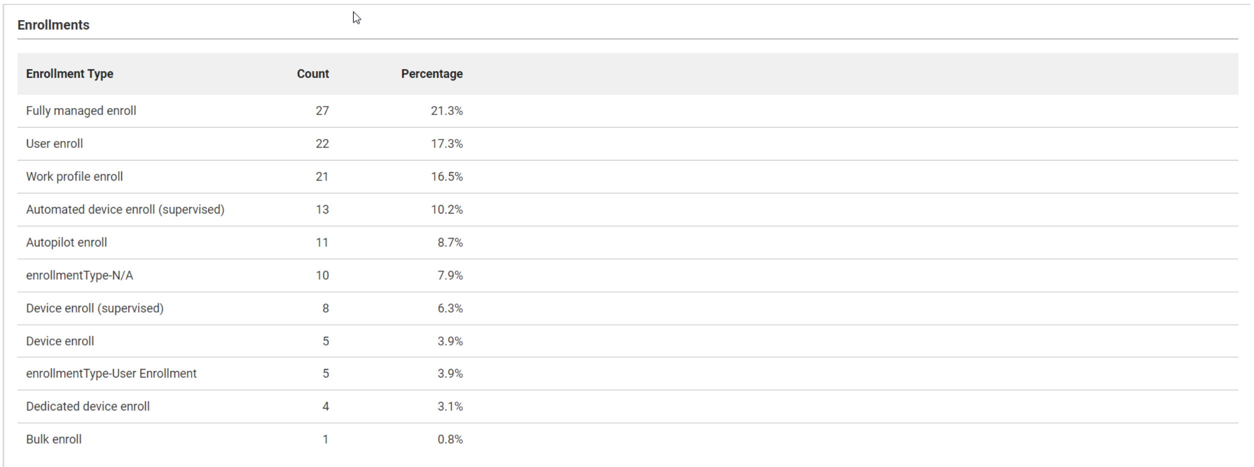
Device Types Managed by MCM

Device Type	Count	Percentage
Mobile	157	100.0

Enrollments

This section shows the total number of enrollments by every enrollment type and their respective percentages in overall enrollments.

Clicking on the count corresponding to an enrollment type leads to the filtered list of devices enrolled with that enrollment type.



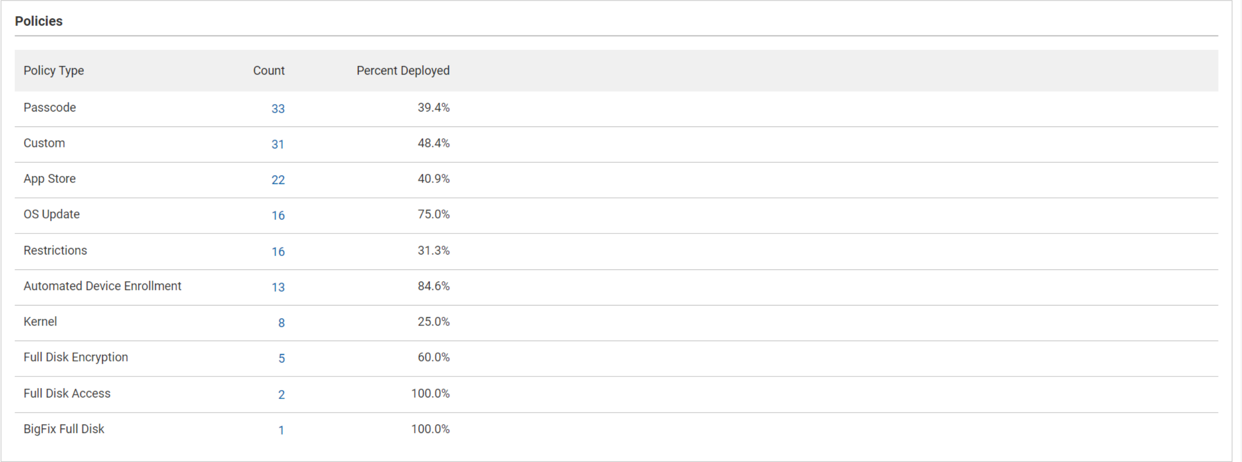
Enrollments

Enrollment Type	Count	Percentage
Fully managed enroll	27	21.3%
User enroll	22	17.3%
Work profile enroll	21	16.5%
Automated device enroll (supervised)	13	10.2%
Autopilot enroll	11	8.7%
enrollmentType-N/A	10	7.9%
Device enroll (supervised)	8	6.3%
Device enroll	5	3.9%
enrollmentType-User Enrollment	5	3.9%
Dedicated device enroll	4	3.1%
Bulk enroll	1	0.8%

Policies

This section shows the total number of policies created and the percentage of policies deployed in every policy type.

Clicking on the count corresponding to a policy type leads to the list of policies filtered with that policy type.



Policies

Policy Type	Count	Percent Deployed
Passcode	33	39.4%
Custom	31	48.4%
App Store	22	40.9%
OS Update	16	75.0%
Restrictions	16	31.3%
Automated Device Enrollment	13	84.6%
Kernel	8	25.0%
Full Disk Encryption	5	60.0%
Full Disk Access	2	100.0%
BigFix Full Disk	1	100.0%

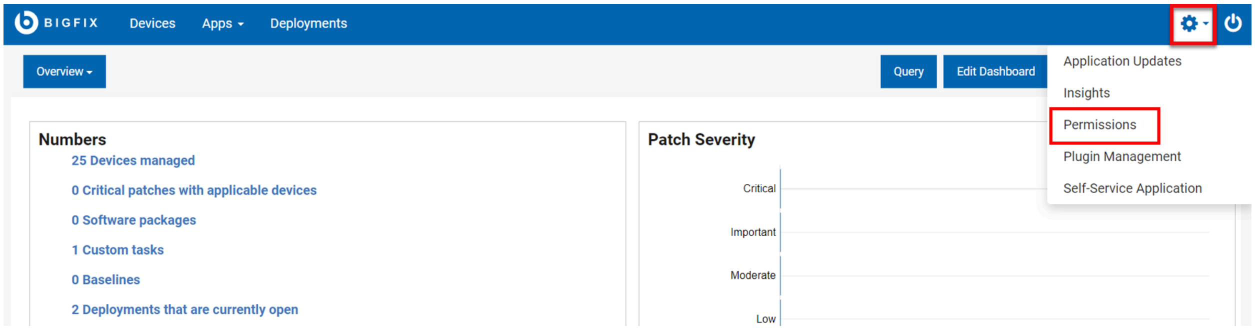
Related information

Install and manage MCM and BigFix Mobile components - On-premises only *(on page 189)*

MCM roles and permissions

Use the WebUI Permissions service to take advantage of fine-grained control over permissions and preferences for users and groups of users in WebUI MDM.

To go to the Permissions page, as a Master Operator click on the gear icon, and from the dropdown menu, select Permissions.



Numbers

25 Devices managed

0 Critical patches with applicable devices

0 Software packages

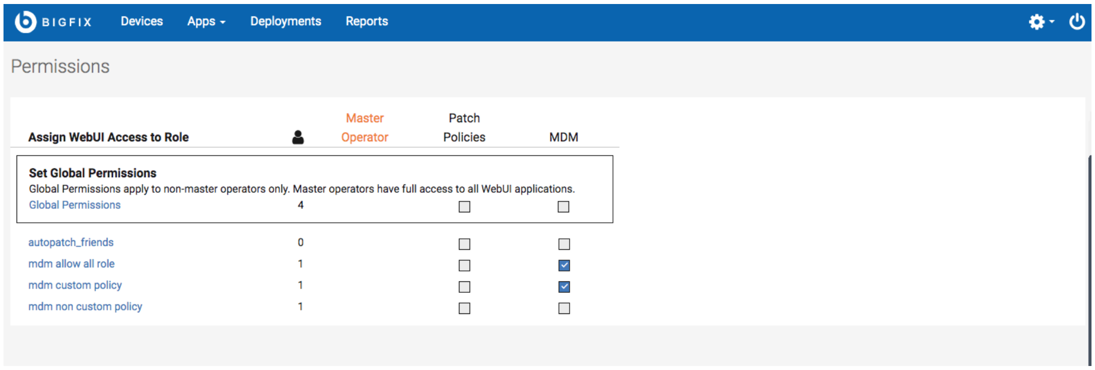
1 Custom tasks

0 Baselines

2 Deployments that are currently open

Master Operator can configure two things with the Permissions and Preferences Services (PPS) with MDM:

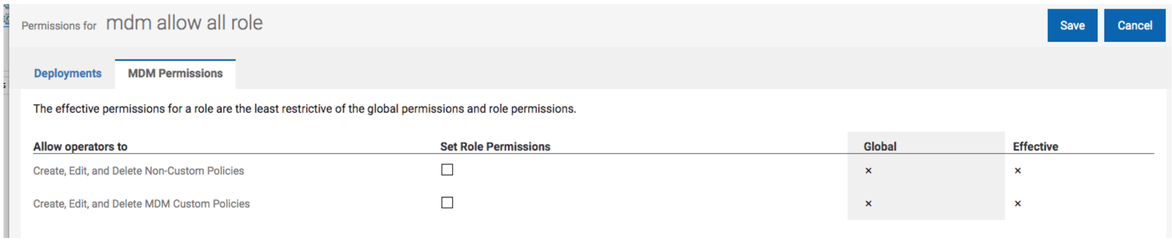
1. Configure visibility of the MCM app based on the user role
    - For example, users with *mdm allow all role* and *mdm custom policy* roles can see the MCM application; but users not in those roles do not have access to MCM application.



Permissions

Assign WebUI Access to Role	👤	Master Operator	Patch Policies	MDM
Set Global Permissions Global Permissions apply to non-master operators only. Master operators have full access to all WebUI applications. Global Permissions	4		☐	☐
autopatch_friends	0		☐	☐
mdm allow all role	1		☐	☑
mdm custom policy	1		☐	☑
mdm non custom policy	1		☐	☐

2. Configure specific MCM permissions



Permissions for mdm allow all role

The effective permissions for a role are the least restrictive of the global permissions and role permissions.

Allow operators to	Set Role Permissions	Global	Effective
Create, Edit, and Delete Non-Custom Policies	☐	×	×
Create, Edit, and Delete MDM Custom Policies	☐	×	×

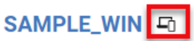
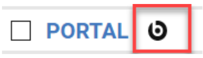
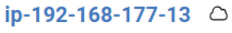
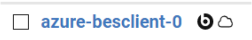
- *Create, Edit and Delete Non-Custom Policies* permission allows users to modify policies (passcode policies, kernel policies, certificate policies, restrictions policies, and full disk access policies) that WebUI natively supports.
- *Create, Edit, and Delete MCM Custom Policies* permission allows users to modify custom policies that users define and upload on their own.

Permissions in WebUI work just like console permissions in that a user's permissions is the union of all of their role permissions and global permissions. For example: If a user is part of four different roles and only one of them has access to MCM specific permission, that user has access to MCM. If a user is not part of any role that has any MCM specific permissions, but the Global Permissions of MCM has been set, that user also has access to MCM despite not having access through roles.

Device inventory

After the devices are enrolled to MDM successfully, the devices report to BigFix WebUI, and they are listed on the **Devices** page. You can use the Devices page in BigFix WebUI to view the list of all devices (as determined by permission levels). The devices list shows all the devices in the BigFix environment including the devices managed by MCM.

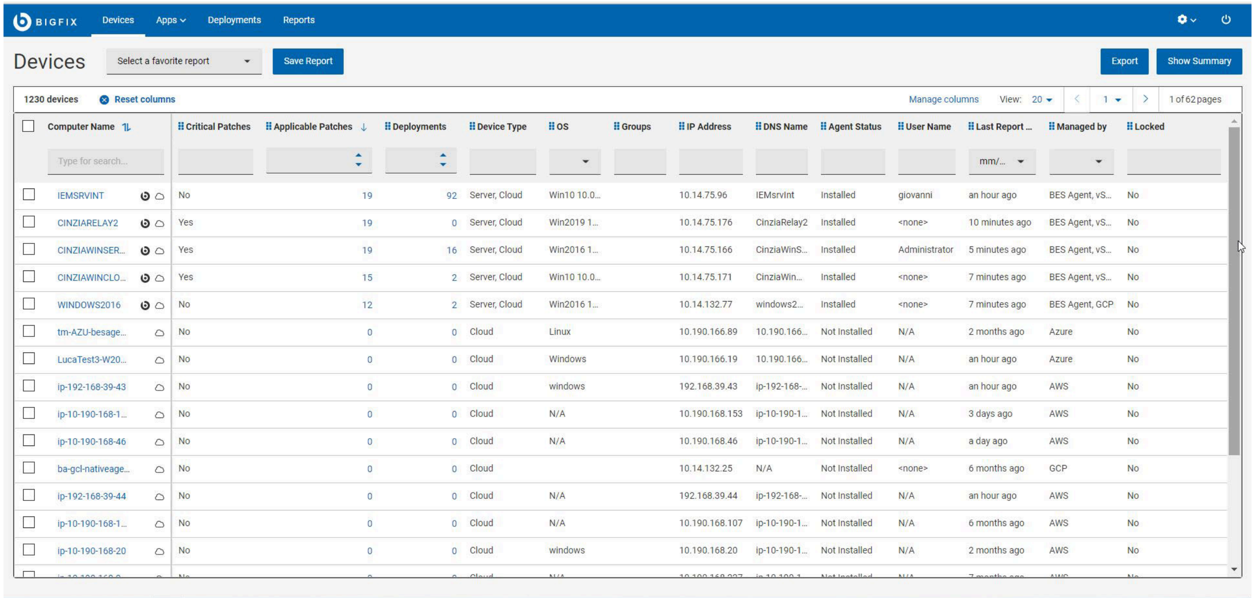
Note:

- The laptop and Mobile Phone icon  SAMPLE_WIN next to the device name indicates that the device is managed by MDM. You can deploy MDM actions, MDM policies, Send Client Refresh, and Deploy BigFix Agent only on these devices.
- Non-Master Operators must have the access permission to the mobile site (BESUEM Mobile) to access the mobile related content in WebUI.
- BigFix icon  □ PORTAL next to the device name indicates that the device is managed by BigFix native agent. You can also send client refreshes to BigFix native agent devices.
- The Cloud icon  ip-192-168-177-13 next to the device name indicates that the device is managed by the cloud.
- If you find more than one icon  □ azure-besclient-0 next to the device name, it indicates that the device is correlated and can be managed in multiple ways.

With MDM, additional deployment options appear on the Deploy dropdown menu. Non-master operators require the Can Create Actions permission to be able to see this dropdown menu. For more information about User permissions, see the BigFix Platform Guide.

The users who have visibility to the WebUI MDM App *(on page 182)* have the following options that are available with WebUI MDM:

- Deploy MDM Action: Allows users to deploy MDM specific actions like the lock, wipe, restart, and more.
- Deploy MDM Policy: Allows users to deploy MDM policies to lock down password settings, add kernel or full disk access exceptions, restriction policies, and certificate policies to the MCM enrolled devices as applicable.
- Deploy MDM Policy Group: Allows users to deploy MDM Policy Groups that can deploy sets of MDM policies and applications to selected MDM endpoints.
- Deploy BigFix Agent: Allows users to deploy the BigFix agent on MDM devices that do not have the BigFix agent deployed on it.
- MDM Enroll and MDM Unenroll: Allows user to enroll devices to MDM and unenroll from MDM.



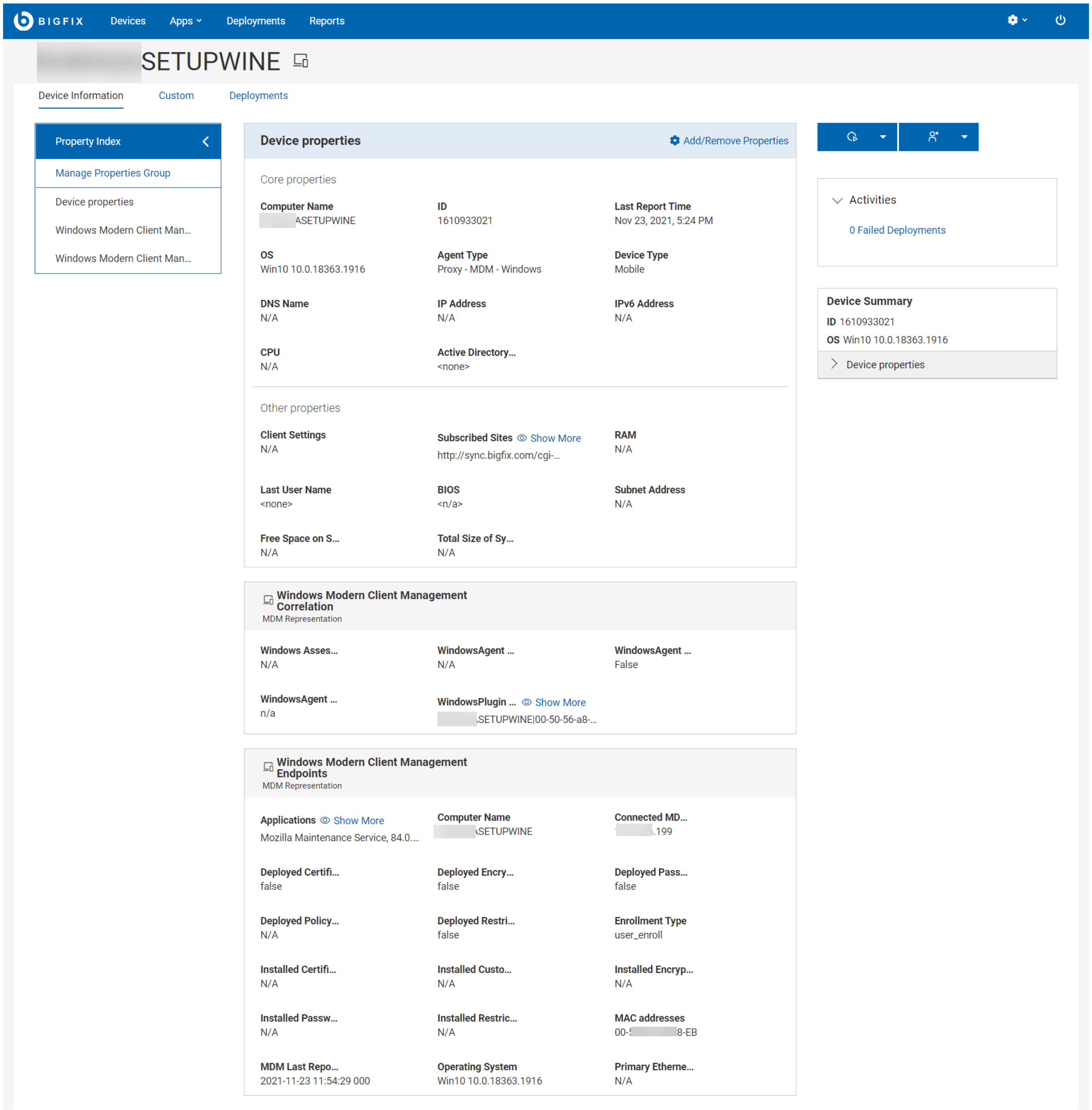
1230 devices

1 of 62 pages

Computer Name	Critical Patches	Applicable Patches	Deployments	Device Type	OS	Groups	IP Address	DNS Name	Agent Status	User Name	Last Report ...	Managed by	Locked
IEMSRVINT	No	19	92	Server, Cloud	Win10 10.0...		10.14.75.96	IEMsrvInt	Installed	giovanni	an hour ago	BES Agent, vS...	No
CINZIARELAY2	Yes	19	0	Server, Cloud	Win2019 1...		10.14.75.176	CinziaRelay2	Installed	<none>	10 minutes ago	BES Agent, vS...	No
CINZIAWINSER...	Yes	19	16	Server, Cloud	Win2016 1...		10.14.75.166	CinziaWinS...	Installed	Administrator	5 minutes ago	BES Agent, vS...	No
CINZIAWINCLO...	Yes	15	2	Server, Cloud	Win10 10.0...		10.14.75.171	CinziaWin...	Installed	<none>	7 minutes ago	BES Agent, vS...	No
WINDOWS2016	No	12	2	Server, Cloud	Win2016 1...		10.14.132.77	windows2...	Installed	<none>	7 minutes ago	BES Agent, GCP	No
tm-AZU-besage...	No	0	0	Cloud	Linux		10.190.166.89	10.190.166...	Not Installed	N/A	2 months ago	Azure	No
LucaTest3-W20...	No	0	0	Cloud	Windows		10.190.166.19	10.190.166...	Not Installed	N/A	an hour ago	Azure	No
ip-192-168-39-43	No	0	0	Cloud	windows		192.168.39.43	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.153	ip-10-190-1...	Not Installed	N/A	3 days ago	AWS	No
ip-10-190-168-46	No	0	0	Cloud	N/A		10.190.168.46	ip-10-190-1...	Not Installed	N/A	a day ago	AWS	No
ba-gcl-nativeage...	No	0	0	Cloud			10.14.132.25	N/A	Not Installed	<none>	6 months ago	GCP	No
ip-192-168-39-44	No	0	0	Cloud	N/A		192.168.39.44	ip-192-168-...	Not Installed	N/A	an hour ago	AWS	No
ip-10-190-168-1...	No	0	0	Cloud	N/A		10.190.168.107	ip-10-190-1...	Not Installed	N/A	6 months ago	AWS	No
ip-10-190-168-20	No	0	0	Cloud	windows		10.190.168.20	ip-10-190-1...	Not Installed	N/A	2 months ago	AWS	No

Click a device in the device list to view the device doc that includes properties, status, relevant content items, and deployment history of the device. Additionally, if the device is an MDM device or if the device is a correlated device that has an MDM representation, you can view additional analysis information about MDM devices.

Note: If the device is correlated, the device document generates different device reports that contain common properties like IP address, Name, and Operating System name, Analysis and more. BigFix displays properties from the native agent over property information that originates from MDM. For some fields like device type, BigFix WebUI displays the aggregation of different device reports.



[redacted]SETUPWINE

Device properties

Core properties

Computer Name [redacted]ASETUPWINE	ID 1610933021	Last Report Time Nov 23, 2021, 5:24 PM
OS Win10 10.0.18363.1916	Agent Type Proxy - MDM - Windows	Device Type Mobile
DNS Name N/A	IP Address N/A	IPv6 Address N/A
CPU N/A	Active Directory... <none>	

Other properties

Client Settings N/A	Subscribed Sites Show More http://sync.bigfix.com/cgi-...	RAM N/A
Last User Name <none>	BIOS <n/a>	Subnet Address N/A
Free Space on S... N/A	Total Size of Sy... N/A	

Windows Modern Client Management Correlation
MDM Representation

Windows Asses... N/A	WindowsAgent ... N/A	WindowsAgent ... False
WindowsAgent ... n/a	WindowsPlugin ... Show More [redacted]SETUPWINE|00-50-56-a8-...	

Windows Modern Client Management Endpoints
MDM Representation

Applications Show More Mozilla Maintenance Service, 84.0....	Computer Name [redacted]SETUPWINE	Connected MD... [redacted].199
Deployed Certifi... false	Deployed Encry... false	Deployed Pass... false
Deployed Policy... N/A	Deployed Restri... false	Enrollment Type user_enroll
Installed Certifi... N/A	Installed Custo... N/A	Installed Encryp... N/A
Installed Passw... N/A	Installed Restric... N/A	MAC addresses 00-[redacted]8-EB
MDM Last Repo... 2021-11-23 11:54:29 000	Operating System Win10 10.0.18363.1916	Primary Etherne... N/A

Device Summary
ID 1610933021
OS Win10 10.0.18363.1916

Device properties

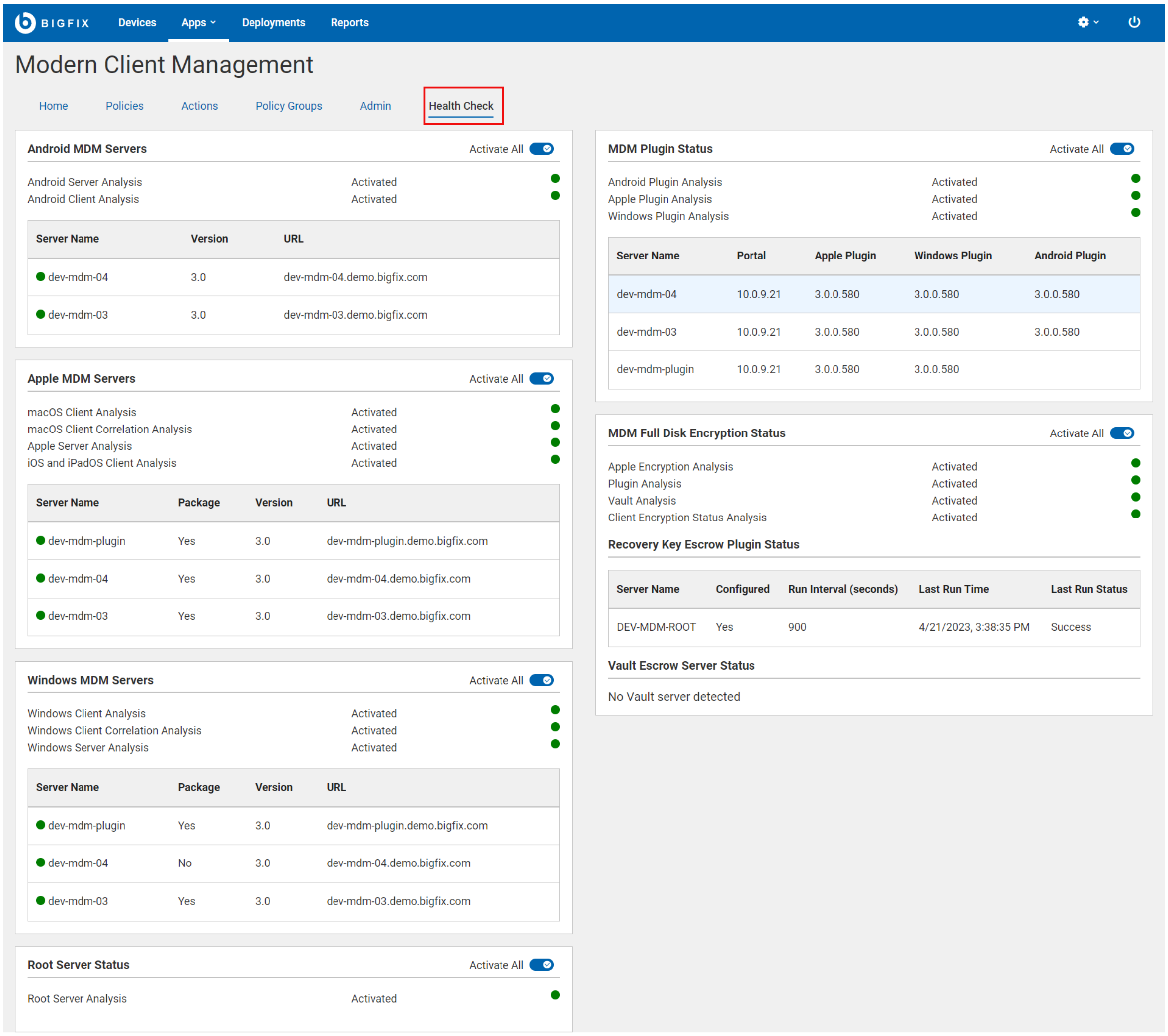
Health Check

As a Master Operator, use the Health Checks page in the MCM application to monitor the health of your MCM deployments.

Note: This functionality is not applicable for Non-Master Operators.

To access the Health Checks page:

1. Login to the WebUI as a Master Operator.
2. From the WebUI main page, select **Apps > MCM**.
3. On the Modern Client Management home page, click **Health Check**. The Health Check page is displayed as follows.



Modern Client Management

Android MDM Servers

Android Server Analysis Activated ●
Android Client Analysis Activated ●

Server Name	Version	URL
● dev-mdm-04	3.0	dev-mdm-04.demo.bigfix.com
● dev-mdm-03	3.0	dev-mdm-03.demo.bigfix.com

Apple MDM Servers

macOS Client Analysis Activated ●
macOS Client Correlation Analysis Activated ●
Apple Server Analysis Activated ●
iOS and iPadOS Client Analysis Activated ●

Server Name	Package	Version	URL
● dev-mdm-plugin	Yes	3.0	dev-mdm-plugin.demo.bigfix.com
● dev-mdm-04	Yes	3.0	dev-mdm-04.demo.bigfix.com
● dev-mdm-03	Yes	3.0	dev-mdm-03.demo.bigfix.com

Windows MDM Servers

Windows Client Analysis Activated ●
Windows Client Correlation Analysis Activated ●
Windows Server Analysis Activated ●

Server Name	Package	Version	URL
● dev-mdm-plugin	Yes	3.0	dev-mdm-plugin.demo.bigfix.com
● dev-mdm-04	No	3.0	dev-mdm-04.demo.bigfix.com
● dev-mdm-03	Yes	3.0	dev-mdm-03.demo.bigfix.com

Root Server Status

Root Server Analysis Activated ●

MDM Plugin Status

Android Plugin Analysis Activated ●
Apple Plugin Analysis Activated ●
Windows Plugin Analysis Activated ●

Server Name	Portal	Apple Plugin	Windows Plugin	Android Plugin
dev-mdm-04	10.0.9.21	3.0.0.580	3.0.0.580	3.0.0.580
dev-mdm-03	10.0.9.21	3.0.0.580	3.0.0.580	3.0.0.580
dev-mdm-plugin	10.0.9.21	3.0.0.580	3.0.0.580	

MDM Full Disk Encryption Status

Apple Encryption Analysis Activated ●
Plugin Analysis Activated ●
Vault Analysis Activated ●
Client Encryption Status Analysis Activated ●

Recovery Key Escrow Plugin Status

Server Name	Configured	Run Interval (seconds)	Last Run Time	Last Run Status
DEV-MDM-ROOT	Yes	900	4/21/2023, 3:38:35 PM	Success

Vault Escrow Server Status

No Vault server detected

This page is organized into different sections as follows to track important health indicators:

- **Android MDM Servers**
- **Apple MDM Servers**
- **Windows MDM Servers**
- **Root Server Status**
- **MDM Plugin Status**
- **MDM Full Disk Encryption Status**

Activate or deactivate all the relevant BESUEM/BESUEM Mobile analyses by clicking the **Activate All** or **Deactivate All** toggle button depending on the activation status. When activated, a green tick mark is displayed next to the relevant analysis.

Important: Ensure all analyses are activated for MCM app to work as expected**.**

Android MDM Status

- Server Name: Reports the list of Android MDM servers that are detected. If there are no Android MDM servers, displays ‘No servers detected’. For information on setting up Android MDM Server, see Install BigFix MDM Service for Android *(on page 196)*.
- Version: Shows the current version of the Android MDM server installed.

Apple MDM Servers

- Server Name: Reports the list of Apple MDM servers that are detected. If there are no Apple MDM servers, ‘No servers detected’ is displayed. For information on setting up the Apple MDM Server, seeInstall BigFix MDM Service for Apple *(on page 194)*.
- Package: Indicates whether a BigFix Agent macOS installer package has been pre-staged on the MDM server. This is needed to successfully deploy a BigFix agent on OSX devices via MDM. If the package has been pre-staged correctly, users can see a green tick mark. If the package is missing and if you want to add the package, see Prestage macOS BigFix installer *(on page 235)*.
- Version: Shows the current version of the Apple MDM server installed.
- URL: Displays the MDM URL of the configured sever. If the server URL is not detected, ensure the server is set up properly. To set up the server, see Install BigFix MDM Service for Apple *(on page 194)*.

Windows MDM Servers

- Server Name: Reports the list of Windows servers that are detected. If there are no Windows servers, displays ‘No servers detected’. For information on setting up the Windows MDM Server, see Install BigFix MDM Service for Windows *(on page 191)*.
- Package: Indicates whether a BigFix Agent Windows .msi installer package has been pre-staged on the MDM server. This is needed to successfully deploy a BigFix agent on Windows devices via MDM. If a package has been pre-staged correctly, the check shows a green tick mark against the relevant sever. If the package is missing and if you want to add the package, see Prestage Windows BigFix Installer *(on page 236)*.
- Version: Shows the current version of the Windows MDM server installed.
- URL: Displays the MDM URL of the configured sever. If the server URL is not detected, ensure the server is set up properly. To set up the server, see Install BigFix Windows MDM Server *(on page 191)*.

Root Server Status

This analysis checks the BES Server to find if there are any PPKG files created.

Note: PPKG created on BES Server is automatically moved to MDM Servers and is used from MDM servers when PPKG actions are taken.

MDM Plugin Status

Reports the list of all the installed Plugin Portal names, versions along with the versions of the installed Apple MDM Plugin, Windows MDM Plugin, and Android Plugin. If component is not installed, it displays 'None.'

MDM Full Disk Encryption Status

Reports the Full Disk Encryption status.

- It shows if the FDE analysis is activated or not.
- Recovery key escrow plugin status: It displays if the Recovery key escrow plugin is configured; if yes, in which server, and the time interval in which it prompts. If not configured, it displays a link through which you can configure.
- Vault Escrow Server Status: It shows if the Vault Escrow Server is configured or not. If configured, it shows the name of the Vault Escrow Server.

Related reference

Health Check MDM Plugin Status is not displayed properly

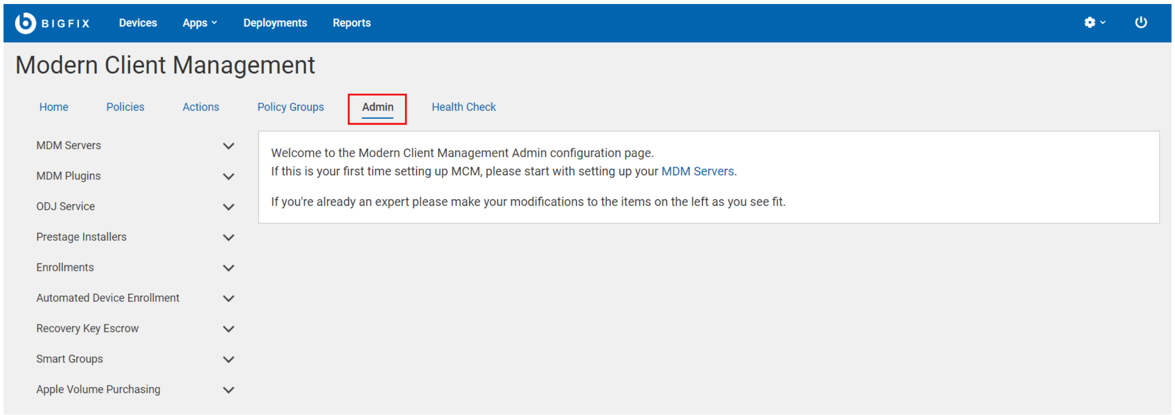
Install and manage MCM and BigFix Mobile components - On-premises only

MDM on-premises requires you to perform one-time MDM Server setup. You must have the required hardware and software set up prior to deploying MDM on-premises. Set up your environment through BigFix WebUI.

For details on prerequisites, setup instructions, and other information seeOn-premises deployment setup section of the Installation and Configuration Guide.

To set up and manage MDM components through BigFix WebUI:

- Ensure that you are a Master Operator (MO)
- From WebUI main page, click **Apps > MCM** and from the Modern Client Management page, click **Admin**



Welcome to the Modern Client Management Admin configuration page.
If this is your first time setting up MCM, please start with setting up your MDM Servers.

If you're already an expert please make your modifications to the items on the left as you see fit.

Install MDM server

Install MDM server: You can install standalone versions of Windows™, Apple®, or Android MDM server. You can also add capabilities to the MDM server to manage a combination of these operating systems. Before installing MDM server, do the following:

- Install Docker Engine, Docker Compose, and OpenSSL.
- Install BES client on the target computer in which you want to install MDM server. This is because you need to install MDM server through WebUI or Fixlets.

Note: With MCM v3.0, you do not have to configure LDAP at the time of installing the MDM Server. You can configure this through the Manage Capability screen. This gives you the options to select your identity server and authentication method after installing the MDM Server.

Manage capability

For MDM servers with only one component installed (Windows, Apple, or Android), you can add the additional component. You can also configure the identity service. See Manage MDM server capability (on page 200).

Install MDM Plugin

Install MDM Plugin: Installing MDM Plugins is required to set up a connection between the MDM Servers and the BigFix Plugin Portal. MDM Plugins communicate with the MDM Server through REST APIs and the AMQP protocol using client certificates. MDM Plugins are available to manage Apple, Windows, and Android devices.

Before installing MDM Plugin:

- Ensure that the server host is running the Plugin Portal version 10.0.2 or later.

  Note:

- To install any version of MDM Plugin, you need at least Plugin Portal v10.0.2.
- For all the features from the latest MDM version to work, you need Plugin Portal v10.0.8 or greater.

- Ensure BigFix agent version 10.0.2 or later is running locally. For details about installing the BigFix Client, see Installing the BigFix components.
- Ensure you have the required credentials, specifically the CA cert, the client cert, and the client key that is generated from BESAdmin.sh. For details, see MDM SSL certificates.
- Ensure you have a Trusted CA TLS certificate and MDM Push credentials of various forms for Apple, Windows and Android servers.

Manage server and client credentials

You need an appropriate set of server and client certificates and keys for the client applications (MDM Plugin, WebUI, ID Service) to securely communicate with a specific MDM Server. You can generate these certificates and keys through BESAdmin and upload them at the time of MDM server installation. After the initial installation, if you want to add, modify, or remove these credentials, you can do it through WebUI. For more information on how to add, update, or remove server and client credentials, see:

- Add Credentials *(on page 210)*
- Update Credentials *(on page 211)*
- Remove Credentials *(on page 212)*

Update

Update MDM servers and Plugins as necessary. See update MDM components (on page 206).

Uninstall

At any point in time, you can uninstall MDM components (on page 207) from WebUI. Note that uninstalling MDM components removes the capability to manage some or all the enrolled devices.

Install BigFix MDM Service for Windows

Learn how to install BigFix MDM Service for Windows to provide MDM service on Windows through WebUI.

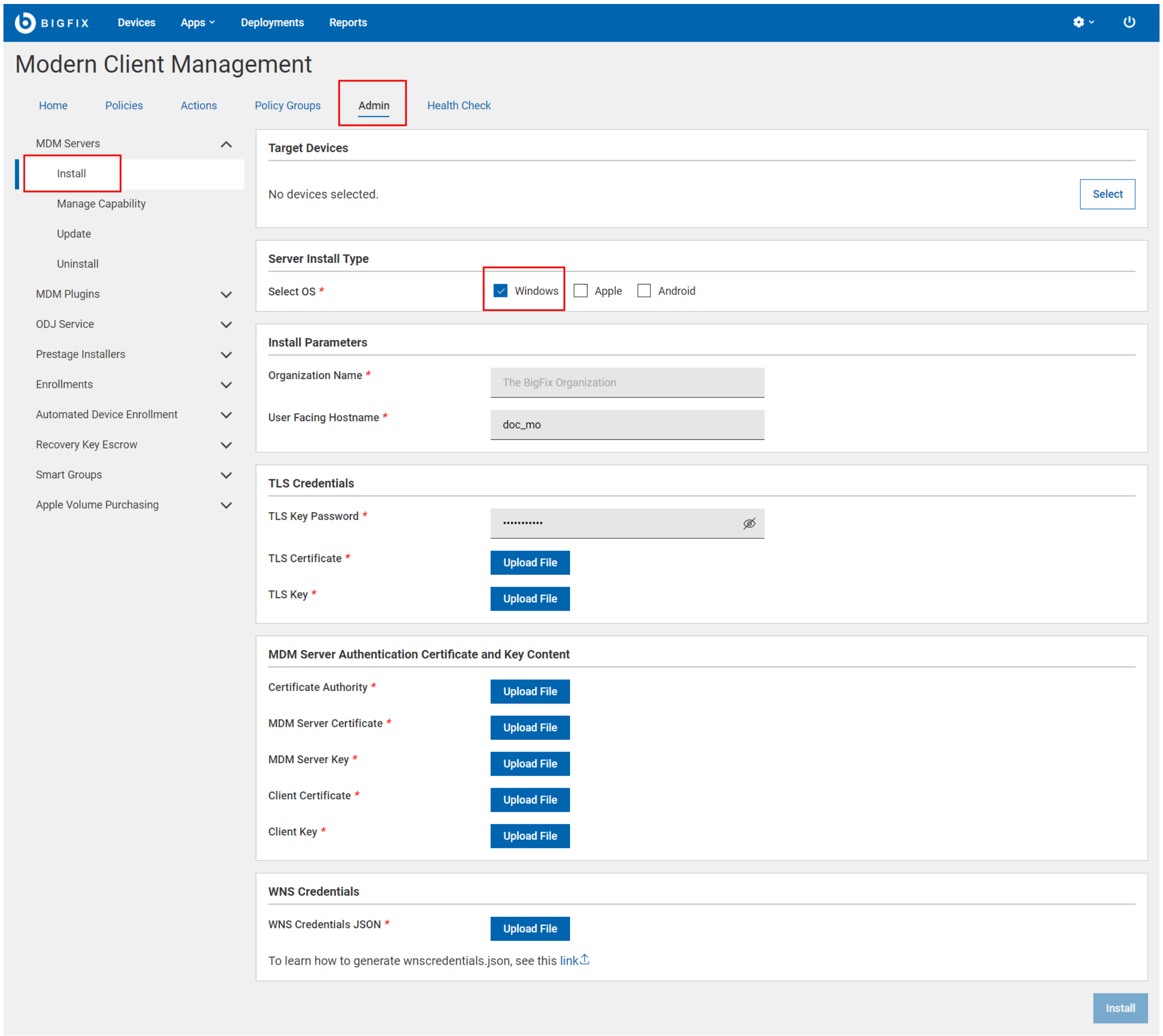
This procedure is for a first time installation of an MDM Service on the MDM Server. If you have already installed one of the MDM Services, use Manage MDM server capability *(on page 200)* option to add an additional MDM service, as some of the configuration is common to all MDM Services and should not be re-supplied for each MDM Service installed.

These prerequisites must be met to install the BigFix MDM Service for Windows:

- You must be a Master Operator to perform this task through WebUI.
- You must have the `wnscredentials.json` file ready to upload. For the work flow to create this file, see Generating WNS credentials.
- You must have a Trusted CA TLS certificate.
- You must have the required credentials, specifically from the CA cert, the client cert, and the client key that is generated from BESAdmin.sh. For details, seeMDM SSL certificates.

To install BigFix MDM Service for Windows:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin.**
3. On the Admin page, from the left navigation, under **MDM Servers**, select **Install**.



Modern Client Management

Home | Policies | Actions | Policy Groups | Admin | Health Check

- MDM Servers
  - Install
  - Manage Capability
  - Update
  - Uninstall
- MDM Plugins
- ODJ Service
- Prestage Installers
- Enrollments
- Automated Device Enrollment
- Recovery Key Escrow
- Smart Groups
- Apple Volume Purchasing

Target Devices

No devices selected. Select

Server Install Type

Select OS * ☑ Windows ☐ Apple ☐ Android

Install Parameters

Organization Name * The BigFix Organization

User Facing Hostname * doc_mo

TLS Credentials

TLS Key Password * ••••••••••••

TLS Certificate * Upload File

TLS Key * Upload File

MDM Server Authentication Certificate and Key Content

Certificate Authority * Upload File

MDM Server Certificate * Upload File

MDM Server Key * Upload File

Client Certificate * Upload File

Client Key * Upload File

WNS Credentials

WNS Credentials JSON * Upload File

To learn how to generate wnscredentials.json, see this link

Install

4. Select Target Device. Click **Select** and select an appropriate target on which you want to install the MDM server.

5. Server Install Type: For Select OS, select **Windows** to manage Windows devices.
6. Install Parameters:
    - **Organization Name**: Enter a string. While enrolling a device, the organization name entered here is displayed to the end users.
    - **User Facing Hostname**: For over the air enrolls, this is the hostname of the server where users can visit to enroll in MDM. The value must be a valid FQDN that is accessible from the Internet. For example, `mdmserver.deploy.bigfix.com`.

      Note: `htt:s//` should not be included here.
7. TLS Credentials: Upload the MDM Server TLS certificate and key files.
    a. TLS Key Password: Enter a string to set TLS key password.
    b. TLS Certificate: Click Upload File and browse through the location to select the TLS `.crt` file.
    c. TLS Key: Click Upload File and browse through the location to select the TLS `.key` file.
8. MDM Server Authentication Certificate and Key Content: Upload the MDM Server authentication certificate and key files.
    a. For **Certificate Authority**, click Upload File and browse through the file location to select the `ca.cert.pem` file.
    b. For **MDM Server Certificate**, click Upload File and browse through the file location to select the `server.cert.pem` file.
    c. For **MDM Server Key**, click Upload File and browse through the file location to select the `server.key` file.

       Tip: For more information on how to generate `.pem` and `.key` files, see MDM SSL certificates.
    d. For **Client Certificate**, click Upload File and navigate and select `client.cert.pem` file.
    e. For **Client Key**, click Upload File and navigate and select `client.key` file.
9. WNS Credentials: This field appears when you select Windows as the operating system. Click Upload File and browse through the file location to select the `wnscredentials.json` file.

   Tip: For more information on how to generate `wnscredentials.json` file, see Generating WNS credentials.
10. Click **Install**.

Results: This action completes these activities:

1. Downloads a set of docker images from software.bigfix.com which is needed for the MDM installation.
2. Installs the services and certificates including the Plugin certificates and the TLS certificate on which the server runs.
3. Applies all required configurations.

Install BigFix MDM Service for Apple

Learn how to install BigFix MDM Service for Apple through WebUI.

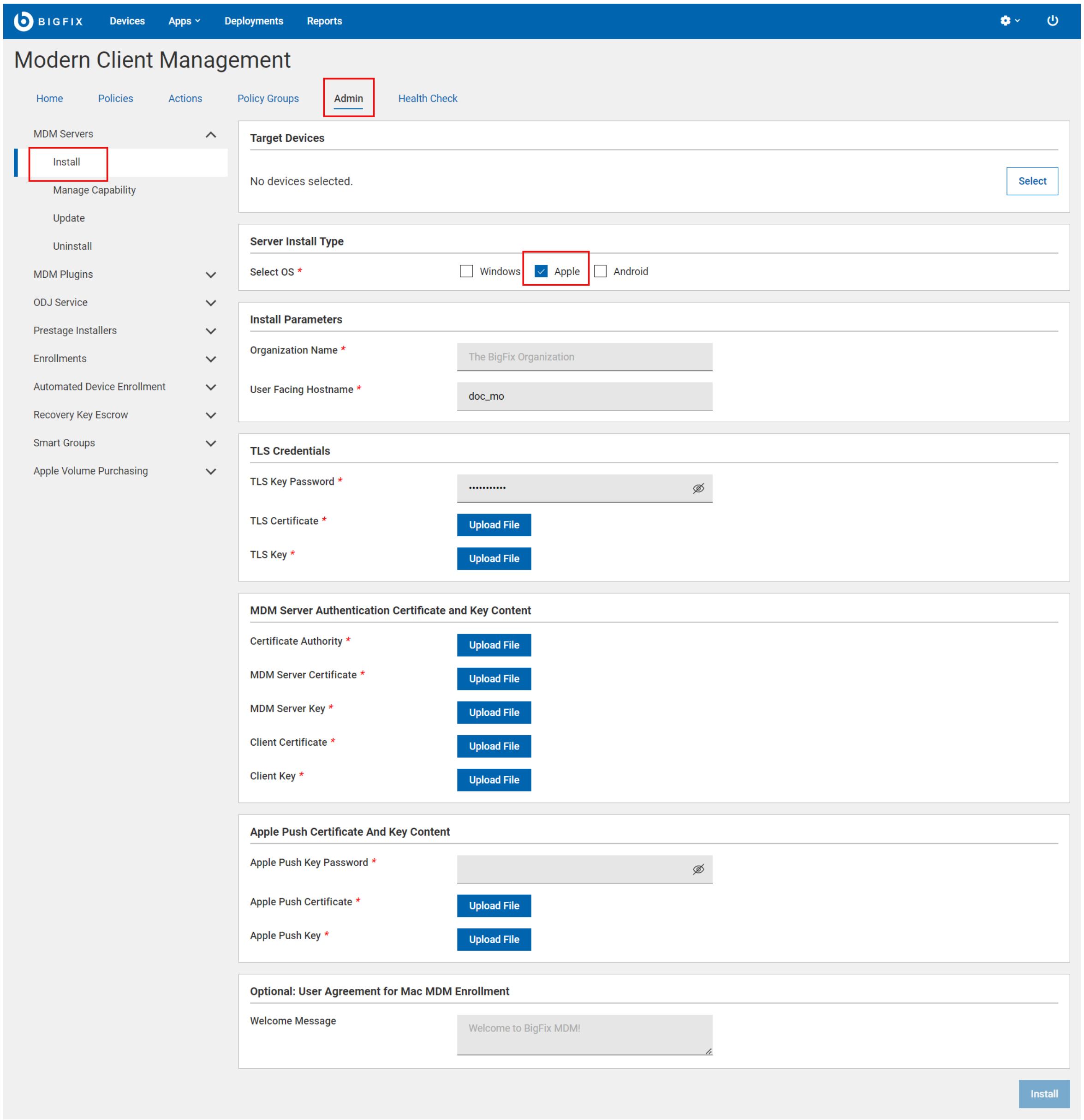
This procedure is for a first time installation of an MDM Service on the MDM Server. If you have already installed one of the MDM Services, use Manage MDM server capability *(on page 200)* option to add an additional MDM service, as some of the configuration is common to all MDM Services and should not be re-supplied for each MDM Service installed.

These prerequisites must be met to install the BigFix MDM Service for Apple:

- You need an Apple Push Notification certificates `PEM` file that is obtained through the HCL vendor signing process and processed by Apple for this MDM Server deployment.
- You must have the necessary certificates and keys. See, MDM SSL certificates.
- You must have the BigFix Agent version 10.0.2 or later running on the MDM Server target.
- You must be a Master Operator to perform this task through WebUI.

To install BigFix MDM server for Apple endpoints:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin.**
3. On the Admin page, from the left navigation, under **MDM Servers**, select **Install**.
4. Select Target Device. Click **Select** and select an appropriate target to install the MDM server on.
5. Server Install Type: For Select OS, select **Apple**.



Modern Client Management

Target Devices

No devices selected.

Server Install Type

Select OS * □ Windows ☑ Apple □ Android

Install Parameters

Organization Name * The BigFix Organization

User Facing Hostname * doc_mo

TLS Credentials

TLS Key Password * ············

TLS Certificate *

TLS Key *

MDM Server Authentication Certificate and Key Content

Certificate Authority *

MDM Server Certificate *

MDM Server Key *

Client Certificate *

Client Key *

Apple Push Certificate And Key Content

Apple Push Key Password *

Apple Push Certificate *

Apple Push Key *

Optional: User Agreement for Mac MDM Enrollment

Welcome Message Welcome to BigFix MDM!

6. Install Parameters:
   - Organization Name: Enter a string. While enrolling a device, the organization name entered here displayed to the end users.
   - User Facing Hostname: For over the air enrolls, this is the hostname of the server where users can visit to enroll in MDM. The value must be a valid FQDN that is accessible from the Internet. For example, `mdmserver.deploy.bigfix.com`.

     Note: `htt:s//` should not be included here.

7. TLS Credentials: Enter the details of the MDM Server TLS certificate and key contents.

   a. TLS Key Password: Enter a string to set TLS key password.
   b. TLS Certificate: Click Upload File and browse through the location to select the TLS `.crt` file.
   c. TLS Key: Click Upload File and browse through the location to select the TLS `.key` file.

8. MDM Server Authentication Certificate and Key Content: Upload the MDM Server authentication certificate and key files.
   a. For **Certificate Authority**, click Upload File and browse through the file location to select the `ca.cert.pem` file.
   b. For **MDM Server Certificate**, click Upload File and browse through the file location to select the `server.cert.pem` file.
   c. For **MDM Server Key**, click Upload File and browse through the file location to select the `server.key` file.

   Tip: For more information on how to generate `.pem` and `.key` files, see MDM SSL certificates.

   d. For **Client Certificate**, click Upload File and navigate and select `client.cert.pem` file.
   e. For **Client Key**, click Upload File and navigate and select `client.key` file.
9. Apple Push Certificate and Key Content:
   - Apple Push Key password: Enter the Apple Push key password.
   - Apple Push Certificate: Click Upload File and browse through the file location to select the `Push PEM` file.
   - Apple Push Key: Click Upload File and browse through the file location to select the `Push key` file.
10. User Agreement for Mac MDM Enrollment: This is optional. Enter a welcome message text for users to see prior to accepting enrollment into MDM. The message entered here is displayed to the end users to accept to proceed with enrollment of Apple devices through the enrollment process. This allows the organization to notify or warn device users of the terms and conditions of enrolling their devices. This message can include, for example, a warning about allowing remote management of the device or helpdesk contact information.
11. Click **Install**.

Results: The action completes these activities:

1. Downloads a set of docker images from software.bigfix.com which is needed for the MDM installation.
2. Installs the services and certificates including the Plugin certificates, the TLS certificate, and the Apple Push certificate on which the server runs.
3. Applies all required configurations.

Install BigFix MDM Service for Android

Learn how to install BigFix MDM Service for Android through WebUI.

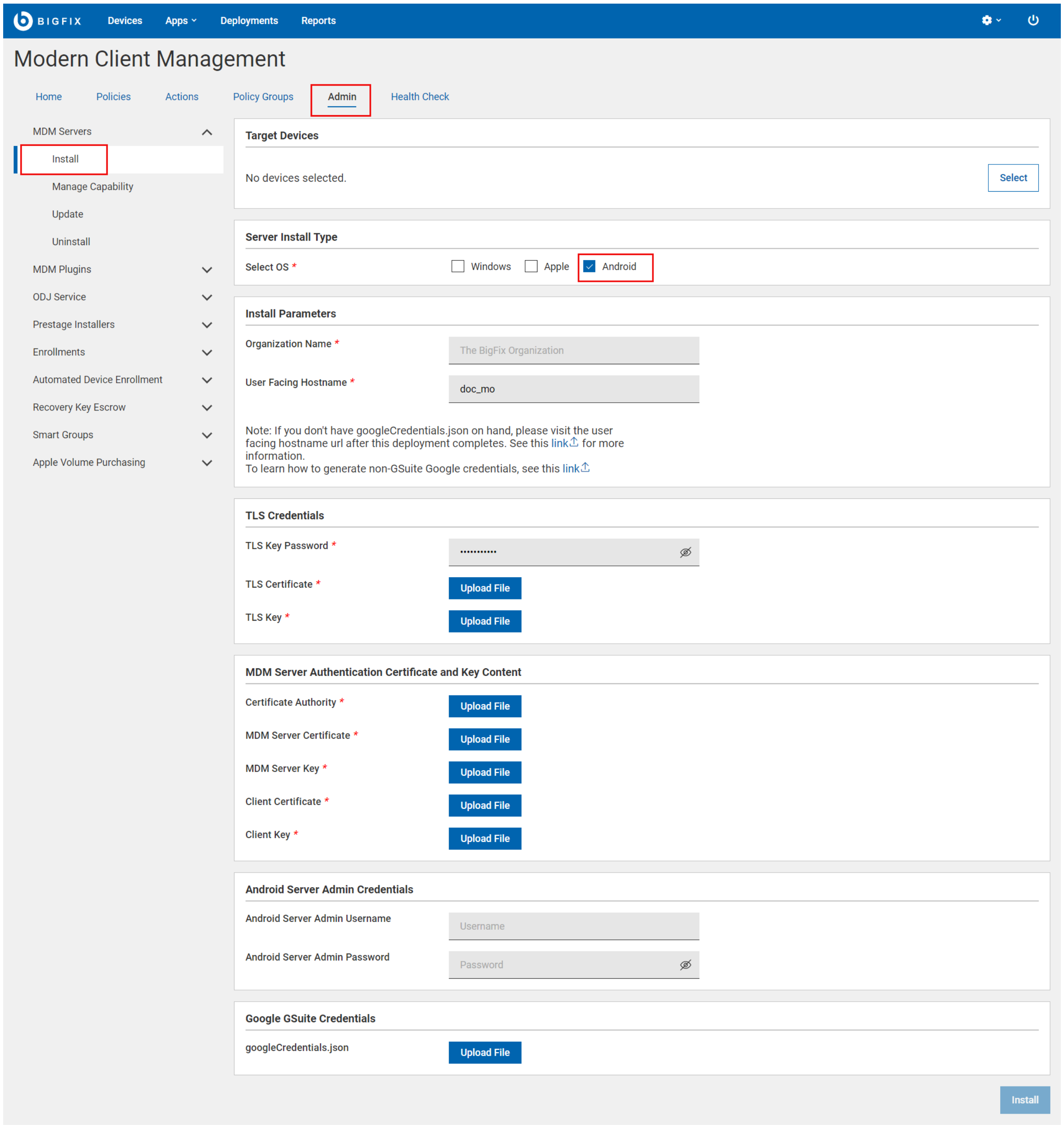
This procedure is for a first time installation of an MDM Service on the MDM Server. If you have already installed one of the MDM Services, use Manage MDM server capability *(on page 200)* option to add an additional MDM service, as some of the configuration is common to all MDM Services and should not be re-supplied for each MDM Service installed.

These prerequisites must be met to install the BigFix MDM Server for Android endpoints:

- You must have the necessary certificates and keys. See, BigFix PlugIn and MDM SSL certificates and keys.
- You must have the BigFix Agent running on the MDM Server target.
- You must be a Master Operator to perform this task through WebUI.

To install BigFix MDM server for Android endpoints:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin.**
3. On the Admin page, from the left navigation, under MDM Servers, select **Install**.
4. Select Target Device. Click **Select** and select an appropriate target to install the MDM server on.
5. Server Install Type: For Select OS, select Android.



Target Devices

No devices selected.

Server Install Type

Select OS * ☐ Windows ☐ Apple ☑ Android

Install Parameters

Organization Name * The BigFix Organization

User Facing Hostname * doc_mo

Note: If you don't have googleCredentials.json on hand, please visit the user facing hostname url after this deployment completes. See this link for more information.
To learn how to generate non-GSuite Google credentials, see this link

TLS Credentials

TLS Key Password * ••••••••••••

TLS Certificate *

TLS Key *

MDM Server Authentication Certificate and Key Content

Certificate Authority *

MDM Server Certificate *

MDM Server Key *

Client Certificate *

Client Key *

Android Server Admin Credentials

Android Server Admin Username Username

Android Server Admin Password Password

Google GSuite Credentials

googleCredentials.json

6. Install Parameters:
   - Organization Name: Enter a string. While enrolling a device, the organization name entered here displayed to the users along with the rest of the profile information.
   - User Facing Hostname: For over the air enrolls, this is the hostname of the server where users can visit to enroll in MDM. For over the air enrolls, this is the hostname of the server where users can visit to enroll in MDM. The value must be a valid FQDN that is accessible from the Internet. For example, `mdmserver.deploy.bigfix.com`.

Note: `htt:s//` should not be included here.

This is also where some Android Admin configuration takes place. See Enroll to Managed Google Play Accounts enterprise.

7. TLS Credentials: Enter the details of the MDM Server TLS certificate and key contents.
    a. TLS Key Password: Enter a string to set TLS key password.
    b. TLS Certificate: Click Upload File and browse through the location to select the TLS `.crt` file.
    c. TLS Key: Click Upload File and browse through the location to select the TLS `.key` file.
8. MDM Server Authentication Certificate and Key Content: Upload the MDM Server authentication certificate and key files.
    a. For **Certificate Authority**, click Upload File and browse through the file location to select the `ca.cert.pem` file.
    b. For **MDM Server Certificate**, click Upload File and browse through the file location to select the `server.cert.pem` file.
    c. For **MDM Server Key**, click Upload File and browse through the file location to select the `server.key` file.

    Tip: For more information on how to generate `.pem` and `.key` files, see MDM SSL certificates.

    d. For **Client Certificate**, click Upload File and navigate and select `client.cert.pem` file.
    e. For **Client Key**, click Upload File and navigate and select `client.key` file.
9. For non G-Suite accounts, Android Server Admin Credentials are required. For G-Suite accounts, the Google Gsuite Credentials are required.

    Note: Either the Android Server Admin Credentials or the Google Gsuite Credentials are required, not both. The UI stops you if you try to enter both.

    Android Server Admin Credentials:

    a. Android Server Admin Username: Enter a string to set the Admin UI user name.
    b. Android Server Admin Password: Enter a string to set the Admin UI password.

    Important: Set a strong and complex password (For example, at least 12 characters long - the longer, the better; has a combination of upper and lowercase letters, numbers, punctuation, and special symbols) for better application security.

    For more information on how to generate `googlecredentials.json` file, see Enroll to Managed Google Play Accounts enterprise.

    or

Google GSuite Credentials: Click Upload file and browse through the file location to select the `googlecredentials.json` file.

10. Click **Install**.

Results: This action completes these activities:

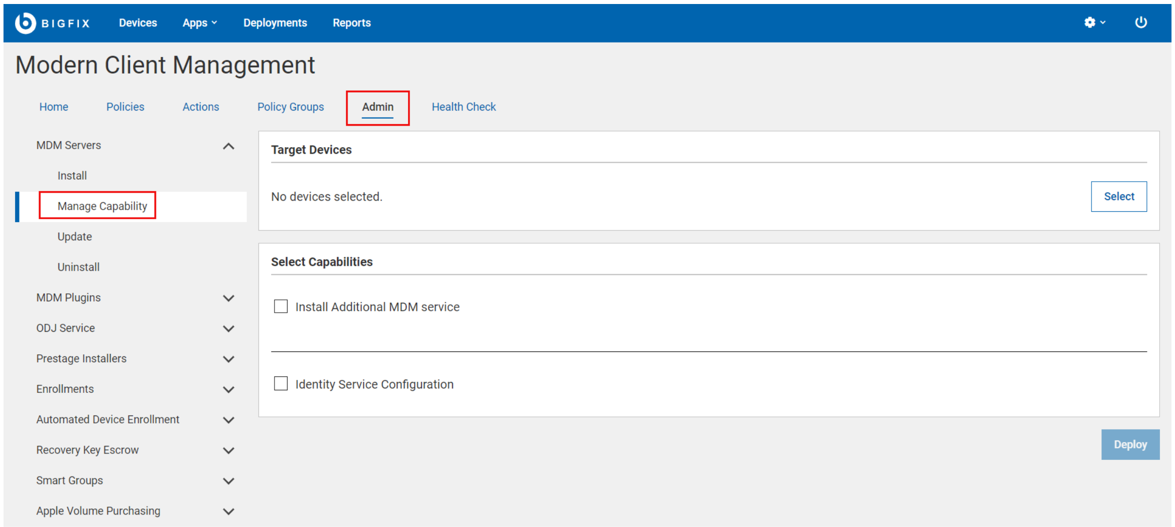
1. Downloads a set of docker images from software.bigfix.com which is needed for the MDM installation.
2. Installs the services and certificates including the Plugin certificates and the TLS certificate on which the server runs.
3. Applies all required configurations.

Manage MDM server capability

Read this topic to learn how to install additional MDM services such as Windows, Apple, Android and to configure the identity service.

For MDM servers that do not have all the three MDM components installed (Windows, Apple, or Android), you can add the missing component. For example, a Windows MDM server can use this work flow to add Apple MDM and / or Android MDM server capabilities and vice versa. You can also configure the authentication method used by the identity service for your organization through this screen.

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, select **MDM Servers > Manage Capability**. The following page appears:



Modern Client Management

Target Devices

No devices selected.

Select Capabilities

□ Install Additional MDM service

□ Identity Service Configuration

4. Click **Select** to select an MDM server on which you want to install additional MDM service and/or configure the identity service. You must select at least one option to deploy on an MDM server.
5. **Install Additional MDM Service**

a. Under the Select Capabilities section, select the **Install Additional MDM Service** check box.

b. Select the Operating System.

   - Windows

     WNS Credentials: This field appears when you select Windows as the operating system. Click Upload File and browse through the file location to select the `wnscredentials.json` file.

     Tip: For more information on how to generate `wnscredentials.json` file, see Generating WNS credentials.

   - Apple
     - Apple Push Certificate and Key Content:
       - Apple Push Key password: Enter the Apple Push key password.
       - Apple Push Certificate: Click Upload File and browse through the file location to select the `Push PEM` file.
       - Apple Push Key: Click Upload File and browse through the file location to select the `Push key` file. For information on how to obtain an Apple Push Certificate for your MDM Server, see Generating APNs certificate.
     - User Agreement for Mac MDM Enrollment: This is optional. Enter welcome message text for an end user agreement. The message entered here is displayed to the end users to accept to proceed with enrollment of Apple devices through the enrollment process. This allows the organization to notify or warn device users of the terms of enrolling their devices. This message can include, for example, a warning about allowing remote management of the device or helpdesk contact information.
   - Android

     - For non G-Suite accounts, Android Server Admin Credentials are required. For G-Suite accounts, the Google G-Suite Credentials are required.

       Note: Either the Android Server Admin Credentials or the Google Gsuite Credentials are required, not both. The UI stops you if you try to enter both.

       Android Server Admin Credentials:

       - Android Server Admin Username: Enter the user name
       - Android Server Admin Password: Enter the password

       For more information on how to generate `googlecredentials.json` file, see Enroll to Managed Google Play Accounts enterprise.

       or

       Google GSuite Credentials: Click Upload file and browse through the file location to select the `googlecredentials.json` file.

6. **Identity Service Configuration**

    a. Under the Select Capabilities section, select the **Identity Service Configuration** checkbox. ID Service options appear for you to select.

    b. Select ID Service

    - No Auth: Select this option if you do not want any authentication. This means anyone can enroll for MCM service without having to identify themselves through user credentials.
    - AD/Open LDAP
        - Enable SAML: This is optional. Select this check box to enable SAML-authentication configuration.

            Note: With MCM v3.0, Okta is supported. Instructions below pertain to Okta-specific setup.

            - SAML Credentials: upload the JSON file with issuer and signOnUrl information in the following format:

                ```
                { "issuer" : "http://www.okt.......ndV5d7",
                "signOnUrl" : "https://dev-12345...........WIBUg5d7/aln7rix.....FK5d7" }
                ```

                Note: See Step 2: Create SAML credentials file for detailed information on how to create the `.json` file.

            - SAML Identity Provider Certificate: Upload the `okta.cert` file that you have downloaded in Step 3: Download SAML Identity Provider certificates from Okta server
        - LDAP URL: This is mandatory. Valid format is https://<server>:<port>. For more information on LDAP URL formats, see https://ldap.com/ldap-urls/
        - LDAP Base DN: This is mandatory. Valid format "dc=example,dc=org"

            Note: Configuring multiple Base DNs is not supported.

        - LDAP Bind User: This is mandatory. The root point to bind to the server. For example, DC=mydomain,DC=mycompany,DC=com. "user@example.org"
        - LDAP Bind Password: This is mandatory. Enter a string.
    - Azure AD
        - Enable SAML: This is optional. Select this checkbox to enable SAML-authenticated enrollment *(on page 202)*.
        - Azure Credentials: This is mandatory. Upload the `.json` file with Azure AD credentials in the following format:

```
{ "client_id": "06b6d920-xxxx-xxxx-xxxx-73792306xxxx",
  "tenant_id": "31ac2431-xxxx-xxxx-xxxx-6215b1c2xxxx",
  "client_secret": "d7bc6b2e-xxxx-xxxx-xxxx-b5c681e5xxxx"
 }
```

For information on how to fetch this information, refer to the BigFix Wiki documentation at Azure AD registration and configuration.

7. Click **Deploy**.

Note: The Deploy button is enabled only when all the required parameters for the selected capabilities are provided without errors.

On top of the existing capabilities of the targeted MDM server, the capabilities of the selected operating system are added. Authentication method and the identity service are configured.

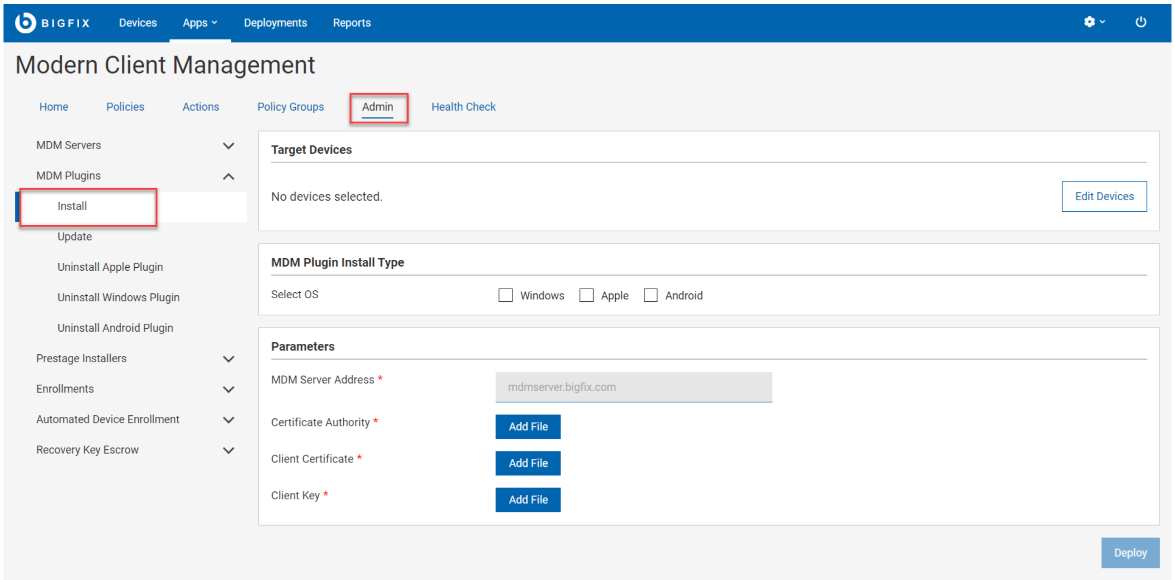
Install MDM Plugin for Windows

To deploy any of the supported MDM Plugins (Windows, Apple, and/or Android) on a Plugin Portal (Windows or Linux), complete the following steps.

The targeted server host must have the BigFix client running and Plugin Portal installed.

To install MDM plugins on a Windows or Linux Plugin Portal:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation under **MDM Plugins**, click **Install** ,



Target Devices

No devices selected.

MDM Plugin Install Type

Select OS ☐ Windows ☐ Apple ☐ Android

Parameters

MDM Server Address * mdmserver.bigfix.com

Certificate Authority *

Client Certificate *

Client Key *

4. In the Target Device section, click **Edit Devices** and select the Windows or Linux Plugin Portal in which you want to install the MDM plugin.
5. Under MDM **Plugin Install Type**, select the required operating system.
   You can select more than one operating system to install MDM Plugins for the selected operating systems simultaneously.
6. Under Parameters, in the **MDM Server Address** field, enter the FQDN or IP address of the MDM Server that can be reached from the Plugin Portal to connect to the MDM Server in the DMZ.
7. For **Certificate Authority**, click Add File and navigate and select `ca.cert.pem` file.
8. For **Client Certificate**, click Add File and navigate and select `client.cert.pem` file.
9. For **Client Key**, click Add File and navigate and select `client.key` file.

You can find the MDM plugin files at this location:

- Windows — `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux
  - Binaries — `/opt/BESPluginPortal/Plugins`
  - Data files — `/var/opt/BESPluginPortal`

You can manage *(on page 257)* the enrolled Windows endpoints.

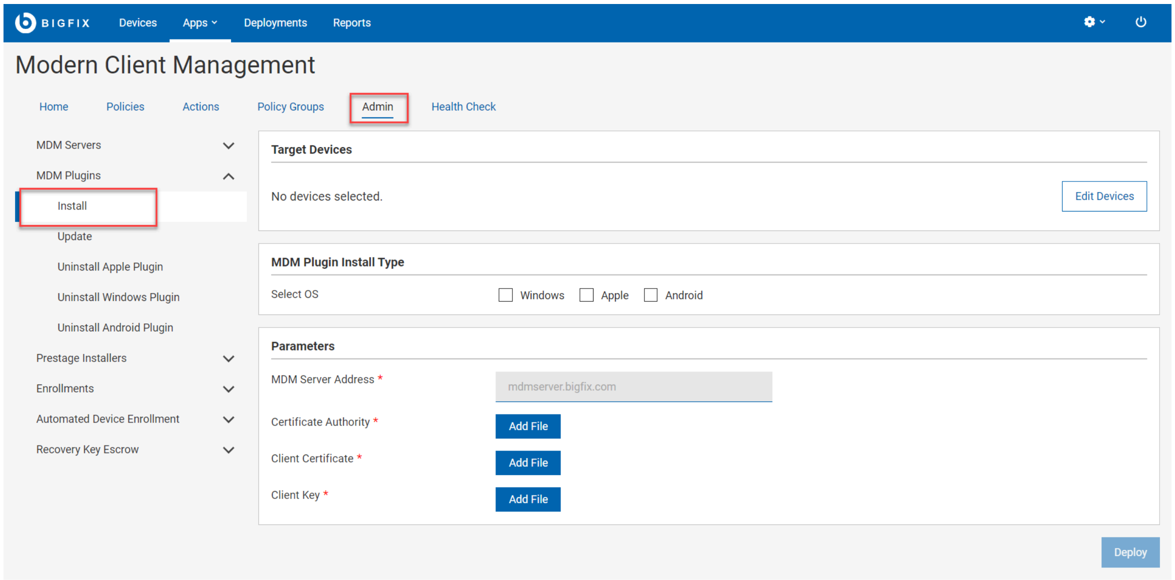
Install MDM Plugin for Apple

Learn how to deploy MDM Plugin on a Windows or Linux Plugin Portal to manage Apple devices.

The targeted server host must have a BigFix client running and Plugin Portal installed.

To deploy MDM plugin for Apple devices:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation under MDM Plugins, click **Install** ,



4. In the Target Device section, click **Edit Devices** and select the MDM server in which you want to install the MDM plugin.
5. Under MDM Plugin Install Type, select Apple for the Operating System.
   You can select more than one operating system to install MDM Plugins for the selected operating systems simultaneously.
6. Under Parameters, in the **MDM Server Address** field, enter the same MDM Server hostname or IP address that you have entered to Install BigFix MDM Service for Apple *(on page 194)*.
7. For **Certificate Authority**, click Add File and navigate and select `ca.cert.pem` file.
8. For **Client Certificate**, click Add File and navigate and select `client.cert.pem` file.
9. For **Client Key**, click Add File and navigate and select `client.key` file.

You can find the MDM plugin files at this location:

- Windows — `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux
  - Binaries — `/opt/BESPluginPortal/Plugins`
  - Data files — `/var/opt/BESPluginPortal`

You can manage *(on page 257)* the enrolled Apple endpoints.

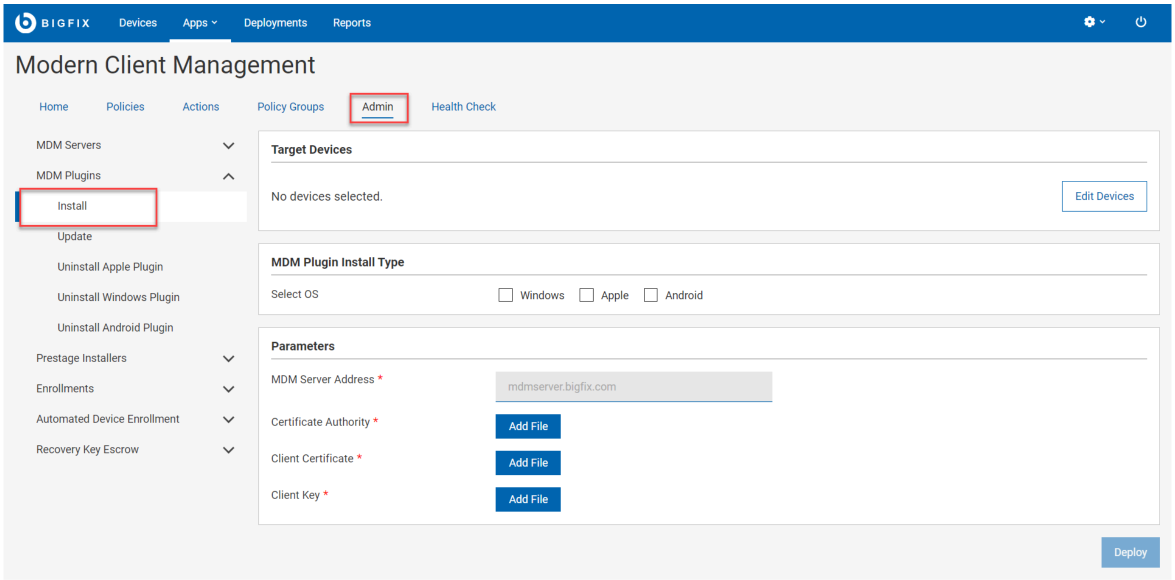
Install MDM Plugin for Android

Learn how to deploy any of the supported MDM Plugins on an Android Plugin Portal.

The targeted server host must have a BigFix client running and Plugin Portal installed.

To install MDM plugins for Android:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation under MDM Plugins, click **Install** ,



4. In the Target Device section, click **Edit Devices** and select the MDM server in which you want to install the MDM plugin.
5. Under MDM Plugin Install Type, select for the Operating System.

   You can select more than one operating system to install MDM Plugins for the selected operating systems simultaneously.
6. Under Parameters, in the **MDM Server Address** field, enter the same MDM Server hostname or IP address that you have entered to Install MDM Server *(on page 191)*.
7. For **Certificate Authority**, click Add File and navigate and select `ca.cert.pem` file.
8. For **Client Certificate**, click Add File and navigate and select `client.cert.pem` file.
9. For **Client Key**, click Add File and navigate and select `client.key` file.

You can find the MDM plugin files at this location:

- Windows — `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux
  - Binaries — `/opt/BESPluginPortal/Plugins`
  - Data files — `/var/opt/BESPluginPortal`

You can manage *(on page 257)* the enrolled Windows endpoints.

Update MDM Components

Learn how to update MDM components.

Before you begin:

- You must be a Master Operator to perform this task through WebUI.
- You need PlugIn Portal version 10.0.2 or later to update the MDM Plugins to the latest version.

Update MDM Server

To update MDM Server:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation, under MDM Server, click **Update**
4. In the Target Devices section, click **Edit Devices**. A list of the available servers that need an update is displayed. Select the required servers and click **OK**.
5. Review the number of servers selected and click **Deploy**. WebUI runs the update on the targeted servers.

Update MDM Plugins

To update MDM Plugins:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation, under MDM Plugins, click **Update**
4. In the Target Devices section, click **Edit Devices**. A list of the available devices that need an update is displayed. Select the required devices and click **OK**.
5. Review the number of servers selected and click **Deploy**. WebUI runs the update on the targeted servers.

Uninstall MDM components

Learn how to uninstall MDM components.

Before you begin: You must be a Master Operator to perform this task through WebUI.

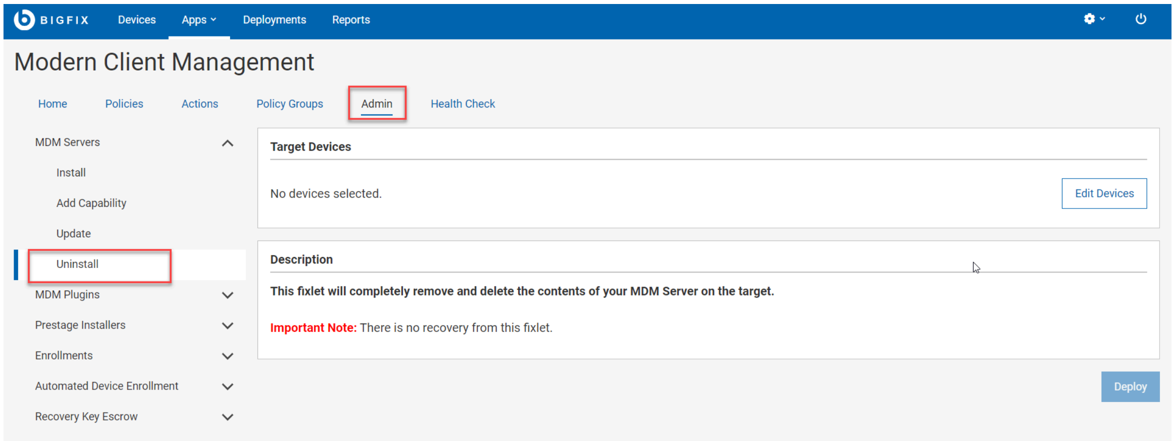
Uninstall MDM server

Uninstalling MDM server removes BigFix MDM from the server and you cannot use MDM services any longer from that server. There is no recovery from an MDM Server Uninstall. For the MDM devices to enroll and properly report again, MDM must be reinstalled.

To uninstall MDM server:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.

3. On the Admin page, from the left navigation, under MDM Server, click **Uninstall**



No devices selected.

This fixlet will completely remove and delete the contents of your MDM Server on the target.

Important Note: There is no recovery from this fixlet.

4. Click **Edit Devices** and select the MDM server that you want to uninstall.

5. Click **Deploy**.

Uninstall MDM Plugin for Apple

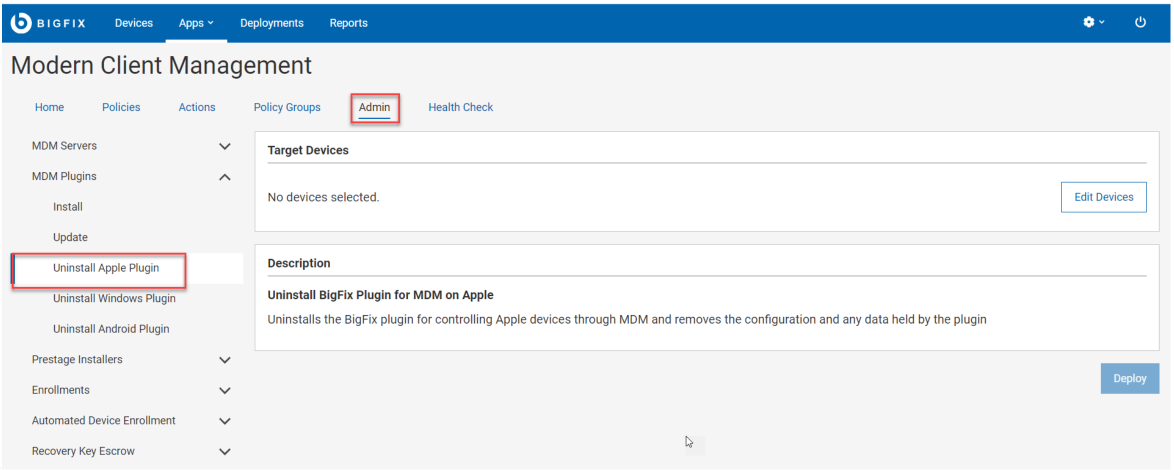
After uninstalling MDM Plugin for Apple from a device, you cannot manage Apple devices from that server.

To uninstall:

1. From the WebUI main page, click **Apps > MCM**.

2. On the Modern Client Management page, click **Admin**

3. On the Modern Client Management page, from the left pane under MDM Plugins, click **Uninstall Apple Plugin**.



No devices selected.

Uninstall BigFix Plugin for MDM on Apple

Uninstalls the BigFix plugin for controlling Apple devices through MDM and removes the configuration and any data held by the plugin

4. Click **Edit Devices** and select the server you want to uninstall the MDM plugin.

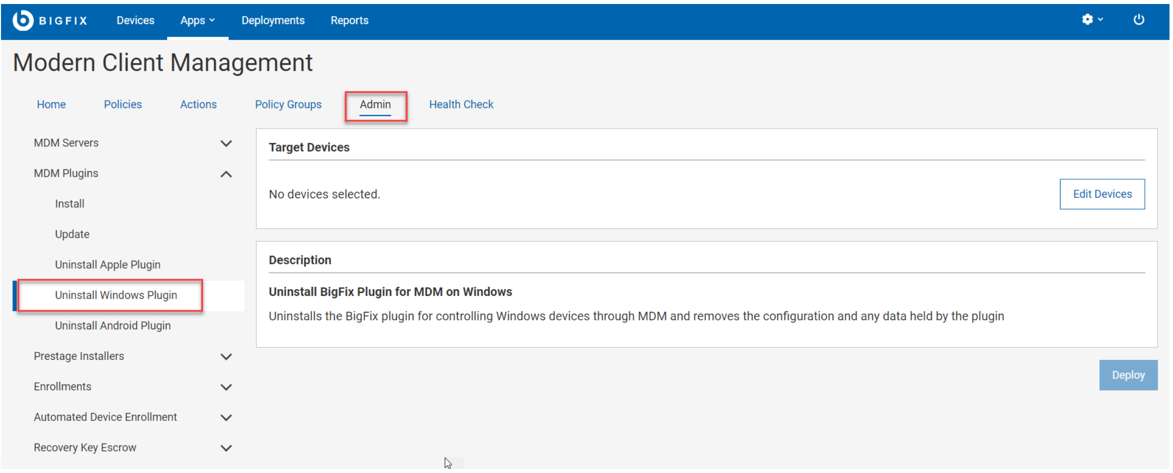
5. Click **Deploy**.

Uninstall MDM Plugin for Windows

After uninstalling MDM plugin for Windows from a device, you cannot manage Windows devices from that Plugin Portal.

To uninstall:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Modern Client Management page, from the left pane under MDM Plugins, click **Uninstall Windows Plugin**



No devices selected.

Uninstall BigFix Plugin for MDM on Windows

Uninstalls the BigFix plugin for controlling Windows devices through MDM and removes the configuration and any data held by the plugin

4. Click **Edit Devices** and select the devices you want to uninstall Windows MDM plugin.
5. Click **Deploy**.

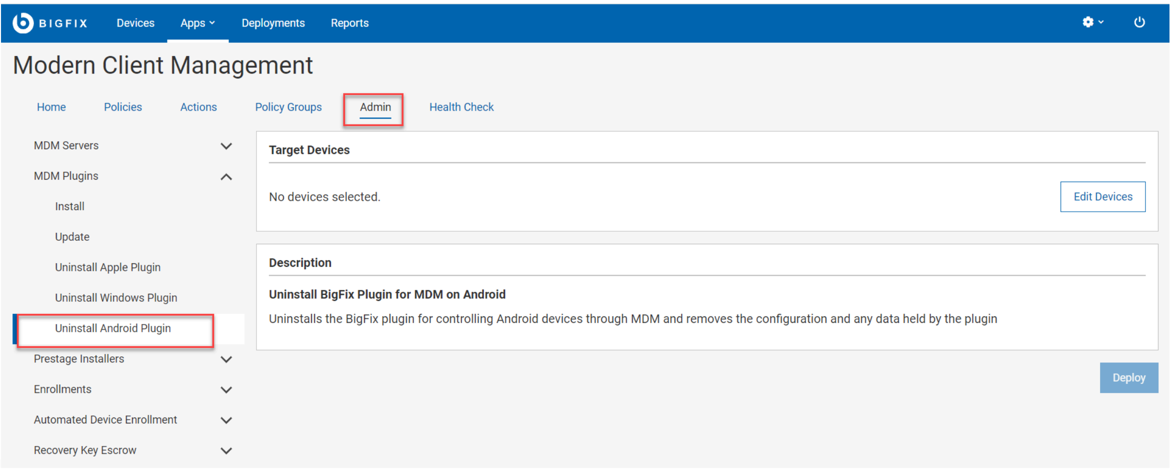
Uninstall MDM Plugin for Android

After uninstalling MDM Plugin for Android from a device, you cannot manage Android devices from that Plugin Portal.

To uninstall:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.

3. On the Modern Client Management page, from the left pane under MDM Plugins, click **Uninstall Android Plugin**



No devices selected.

Uninstall BigFix Plugin for MDM on Android

Uninstalls the BigFix plugin for controlling Android devices through MDM and removes the configuration and any data held by the plugin

4. Click **Edit Devices** and select the devices you want to uninstall Android MDM Plugin.
5. Click **Deploy**.

Related reference

Error while reinstalling MDM server

Add Credentials

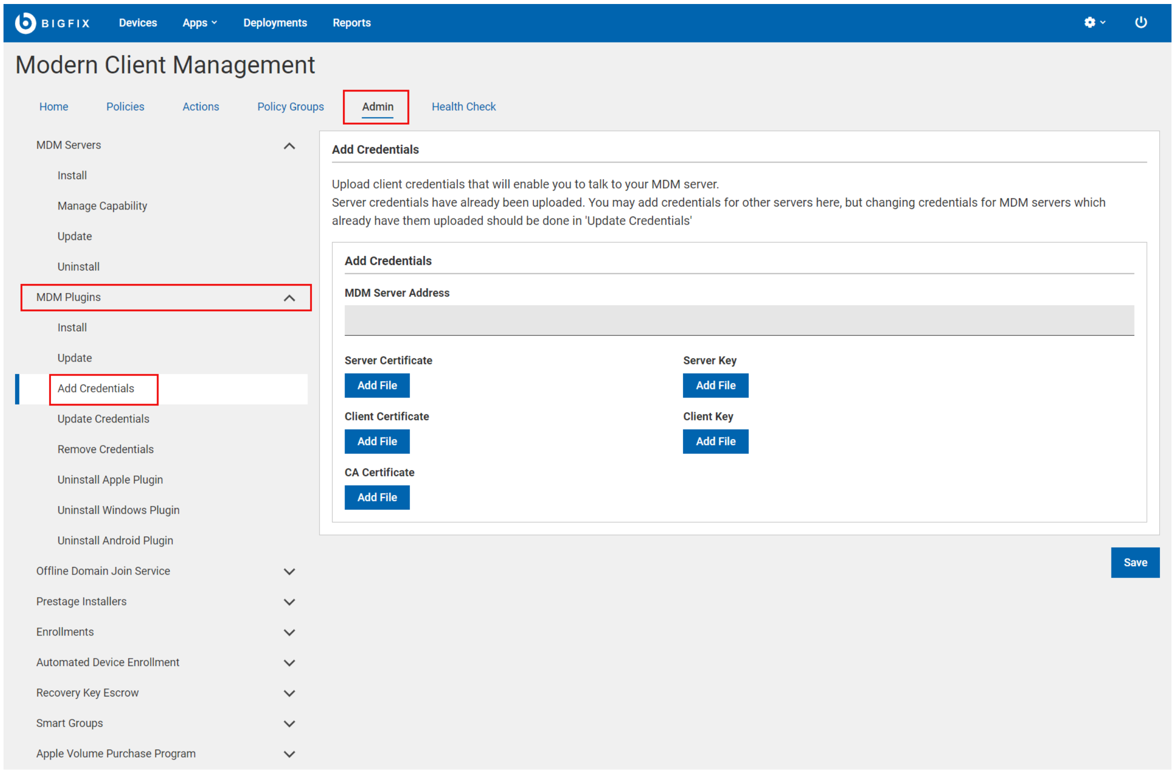
After the initial MDM server installation, at any point in time, if you want to add credentials for additional servers, you can do that from WebUI **Add Credentials** page.

To add server and client credentials, complete the following steps.

Note:

- For upgrading MCM from 2.x to 3.x, to establish direct connectivity between WebUI and the MDM Server, you must upload the same set of server credentials and client credentials that were originally obtained through BESAdmin tool and uploaded while installing MDM server and MDM Plugin.
- For adding more MDM services (Windows MDM, Android MDM, or Apple MDM) to the initial set up, upload only the fresh credentials.
- For updating existing credentials that were added before, go to Update Credentials *(on page 211)*.

1. From MCM Admin page, expand **MDM Plugins** and click **Add Credentials**.



Upload client credentials that will enable you to talk to your MDM server.
Server credentials have already been uploaded. You may add credentials for other servers here, but changing credentials for MDM servers which already have them uploaded should be done in 'Update Credentials'

2. **MDM Server Address**: Enter the address of the MDM server for which you want to add the credentials. For example, `mdmserver.deploy.bigfix.com`.
3. Click **Add File** next to a certificate or key that you want to upload, navigate to the folder, and select the respective file.

   Note: Upload the appropriate certificate and key files. If the files that you uploaded do not match, an error message is displayed.

4. Click **Save**.

The uploaded credentials are stored in WebUI. These credentials are used to establish communication between the MDM server and the client applications (MDM Plugin, WebUI).

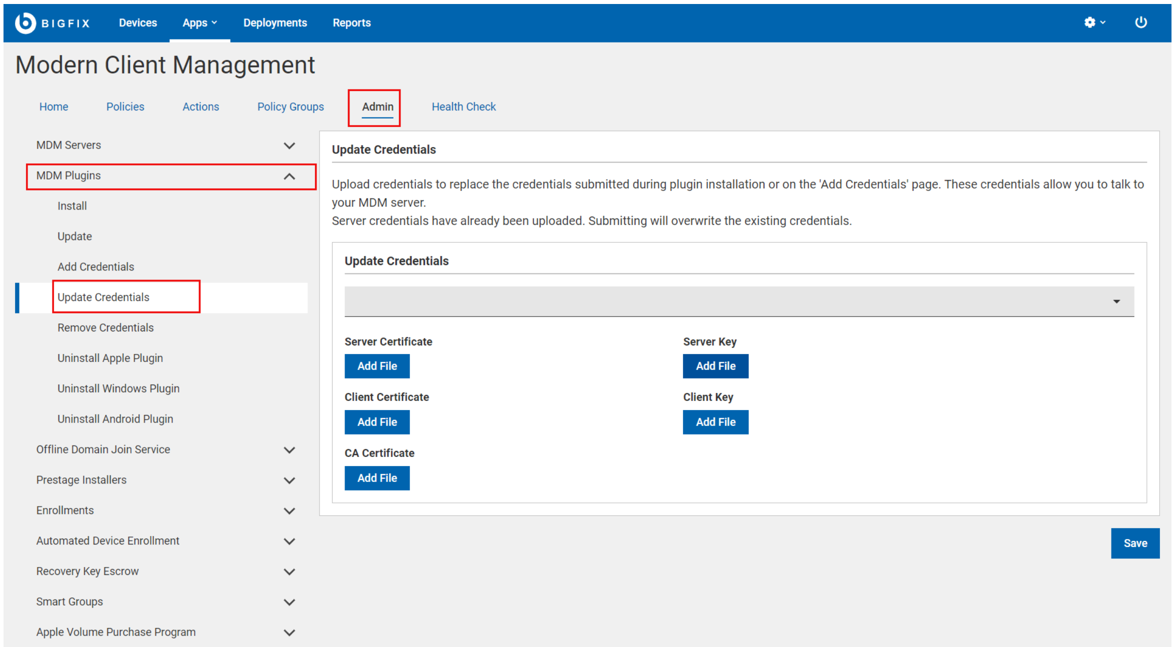
Update Credentials

You can replace the server and client credentials that you have uploaded at the time of initial MDM server installation and those added later through the "Add credentials" page.

To update server and client credentials, complete the following steps.

Note: Uploading credentials overwrites the previously uploaded credentials.

1. From MCM Admin page, expand **MDM Plugins** and click **Update Credentials**.



Update Credentials

Upload credentials to replace the credentials submitted during plugin installation or on the 'Add Credentials' page. These credentials allow you to talk to your MDM server.
Server credentials have already been uploaded. Submitting will overwrite the existing credentials.

Update Credentials

2. The Upload Credentials drop-down lists the MDM servers in your environment. Select an MDM server for which you want to upload the credentials. For example, `mdmserver.deploy.bigfix.com`.
3. Click **Add File** next to a certificate or key that you want to upload, navigate to the folder, and select the respective file.

   Note: Upload the appropriate certificate and key files. If the files that you uploaded do not match, an error message is displayed.

4. Click **Save**.

The previously uploaded credentials are replaced in the credential store with the ones that you have uploaded now.

Note: Uploading to the credential store does not automatically redeploy these credentials to the various servers.

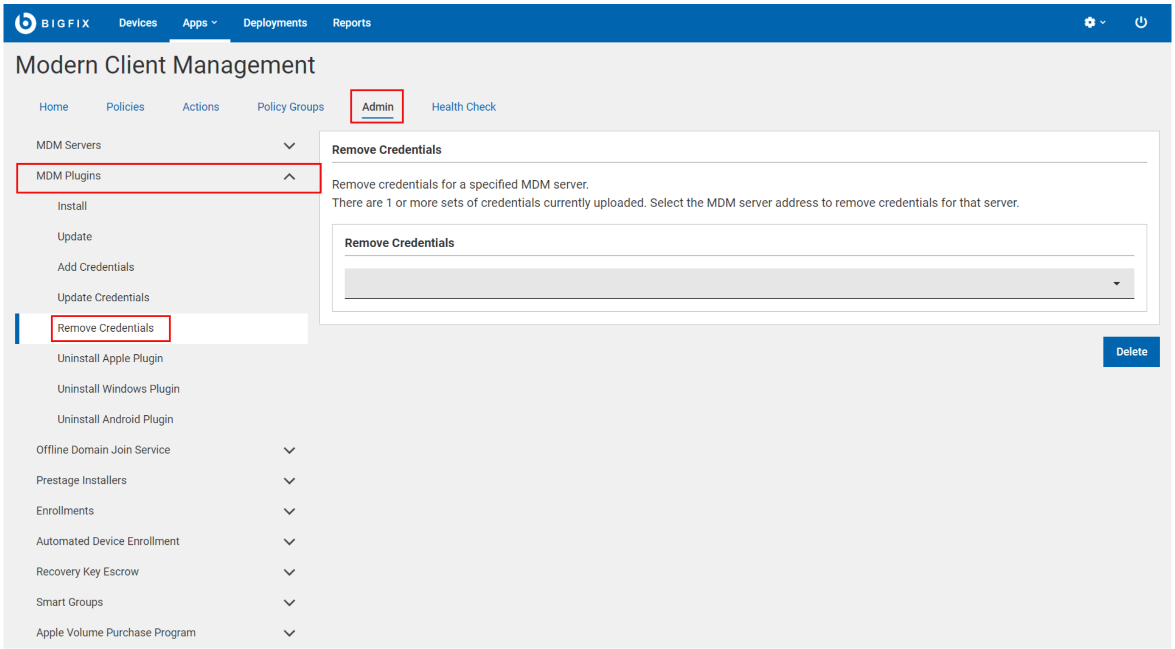
Remove Credentials

You can remove the server and client credentials that you have uploaded previously from WebUI **Remove Credentials** page.

To remove credentials for an MDM server, complete the following steps.

Note: If you remove credentials, you cannot establish a communication between the MDM server and other client applications such as WebUI, MDM Plugin, Identity Service. To establish connection again, you need to upload the credentials again.

1. From MCM Admin page, expand **MDM Plugins** and click **Remove Credentials**.



Remove Credentials

Remove credentials for a specified MDM server.
There are 1 or more sets of credentials currently uploaded. Select the MDM server address to remove credentials for that server.

Remove Credentials

2. From the **Remove Credentials** drop-down, select an MDM server from which you want to remove the credentials.
3. Click **Delete**.

All the credentials for the selected MDM server are deleted. Refresh the browser so that the relevant MDM server is deleted from the Remove Credentials drop-down.

Install and manage ODJ service

Offline Domain Join (ODJ) service is an "Add-on" service and is installed through WebUI after completing the initial MDM server installation.

For a detailed information about the ODJ service, prerequisites and initial setup to prepare for ODJ service installation, refer to Domain join installation and configuration.

For a detailed information about the ODJ service architecture and the enrolment flow, refer to Autopilot enrollment with Offline Domain Join service.

Install

Learn how to install ODJ service through WebUI.

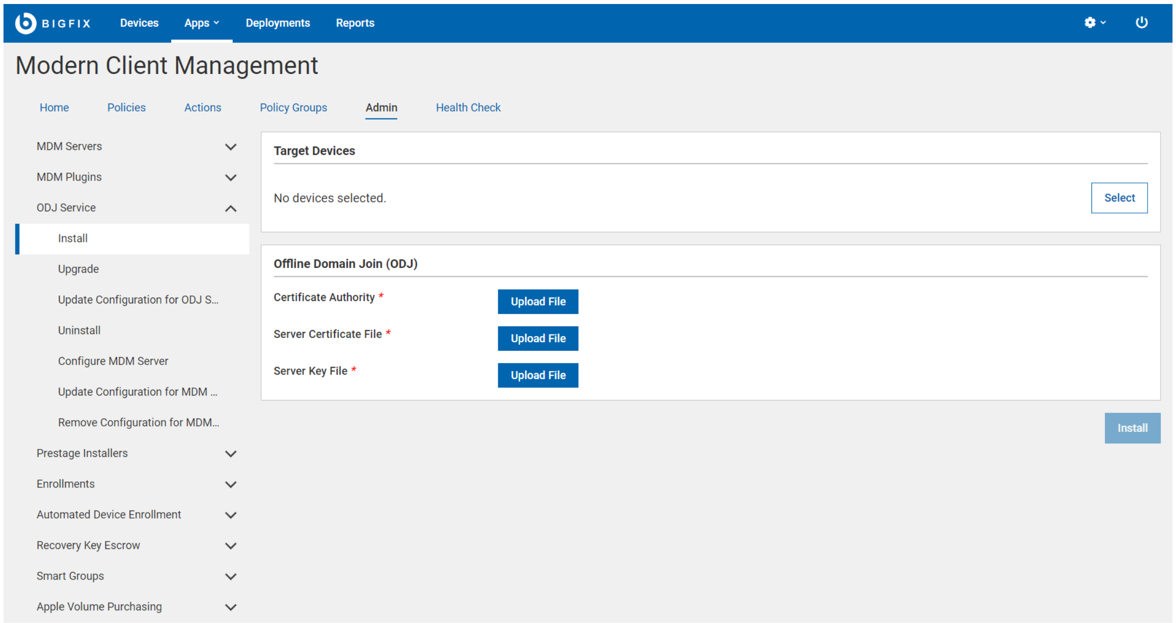
To install the ODJ service, you must fulfill these requirements:

- You must be a Master Operator to perform this task through WebUI.
- The target on which the ODJ service needs to be installed must run Windows 10 or later.
- BESclient must be installed on the target Windows device.
- The target must be already connected to Active Directory (AD).

> **Note:** For more detailed information, refer to Prerequisites for hybrid domain join.

To install ODJ service on a Windows target complete the following steps.

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation, under **ODJ Services**, select



Install.
4. Click **Select**. The eligible Windows devices are listed. Select a target to install the ODJ service .
5. Upload the appropriate certificate files that you have created for ODJ server. See ODJ and MDM SSL certificates and keys.
   a. For Certificate Authority, click **Upload File** and browse through the file location to select the `ca.cert.pem` file.
   b. For Server Certificate File, click **Upload File** and browse through the file location to select the `server.cert.pem` file.
   c. For Server Key File, click **Upload File** and browse through the file location to select the `server.key` file.
6. Click **Install**.

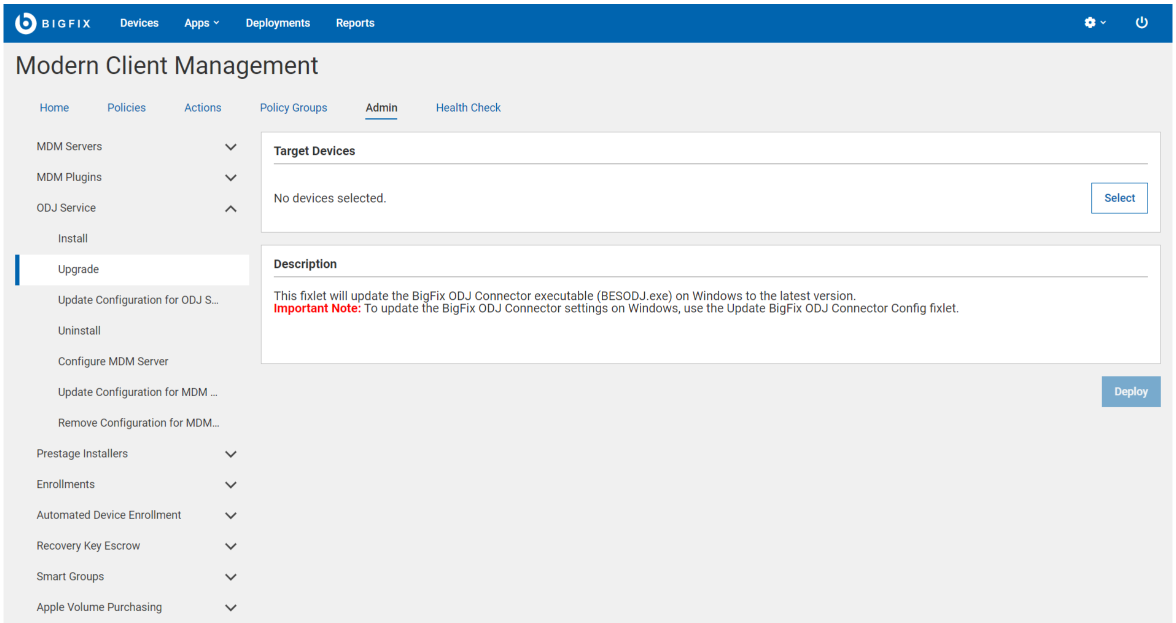
This action installs the ODJ service on the target Windows machine.

Upgrade

Upgrade becomes relevant whenever there is a new version of the ODJ service is released.

To upgrade ODJ service to the latest version, complete the following steps.

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation, under ODJ Service, click **Upgrade**.



No devices selected.

This fixlet will update the BigFix ODJ Connector executable (BESODJ.exe) on Windows to the latest version.
Important Note: To update the BigFix ODJ Connector settings on Windows, use the Update BigFix ODJ Connector Config fixlet.

4. In the Target Devices section, click **Select**. The Select Target page displays a list of Windows devices that have an older version of the ODJ service installed. Select a target and click **OK**.
5. Review the number of targets selected and click **Deploy**.

This action updates the ODJ service to the latest available version.

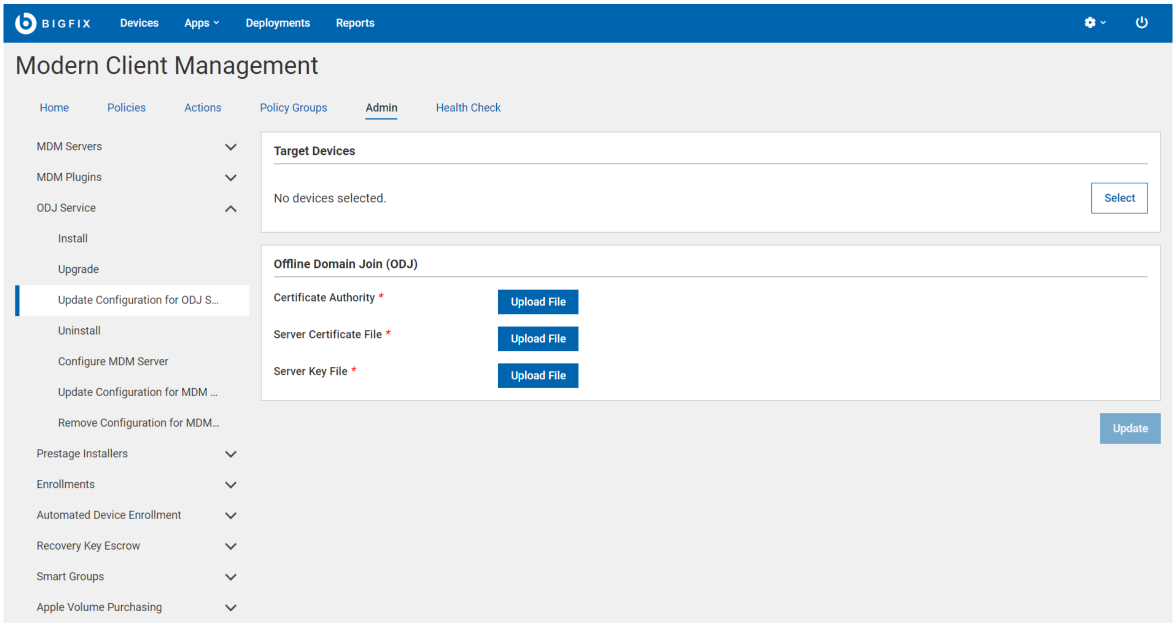
Update configuration for ODJ Service

Learn how to update ODJ Service.

If you want to replace ODJ server certificates, you can do it by updating the configuration for ODJ. To do that, complete the following steps:

1. From the WebUI main page, select **Apps > MCM**
2. On the Modern Client Management page, click **Admin**.

3. On the Admin page, from the left navigation, under **ODJ Services**, select **Update Configuration for ODJ Service**.



No devices selected.

4. Click **Select** to select the target Windows machine where the ODJ Service is installed and that needs update.
5. Upload the appropriate certificate files that you have created for ODJ server. See ODJ and MDM SSL certificates and keys.
    a. For Certificate Authority, click **Upload File** and browse through the file location to select the `ca.cert.pem` file.
    b. For Server Certificate file, click **Upload File** and browse through the file location to select the `server.cert.pem` file.
    c. For Server Key, click **Upload File** and browse through the file location to select the `server.key` file.
6. Click **Update**.

This action updates the ODJ service on the selected Windows machine.

Uninstall

Learn how to uninstall ODJ service.

You must be a Master Operator to perform this task through WebUI.

Uninstalling ODJ service removes the service from the target Windows machine. You cannot use the ODJ service any longer from that machine.

To uninstall ODJ service:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. On the Admin page, from the left navigation, under ODJ Service, click **Uninstall**.

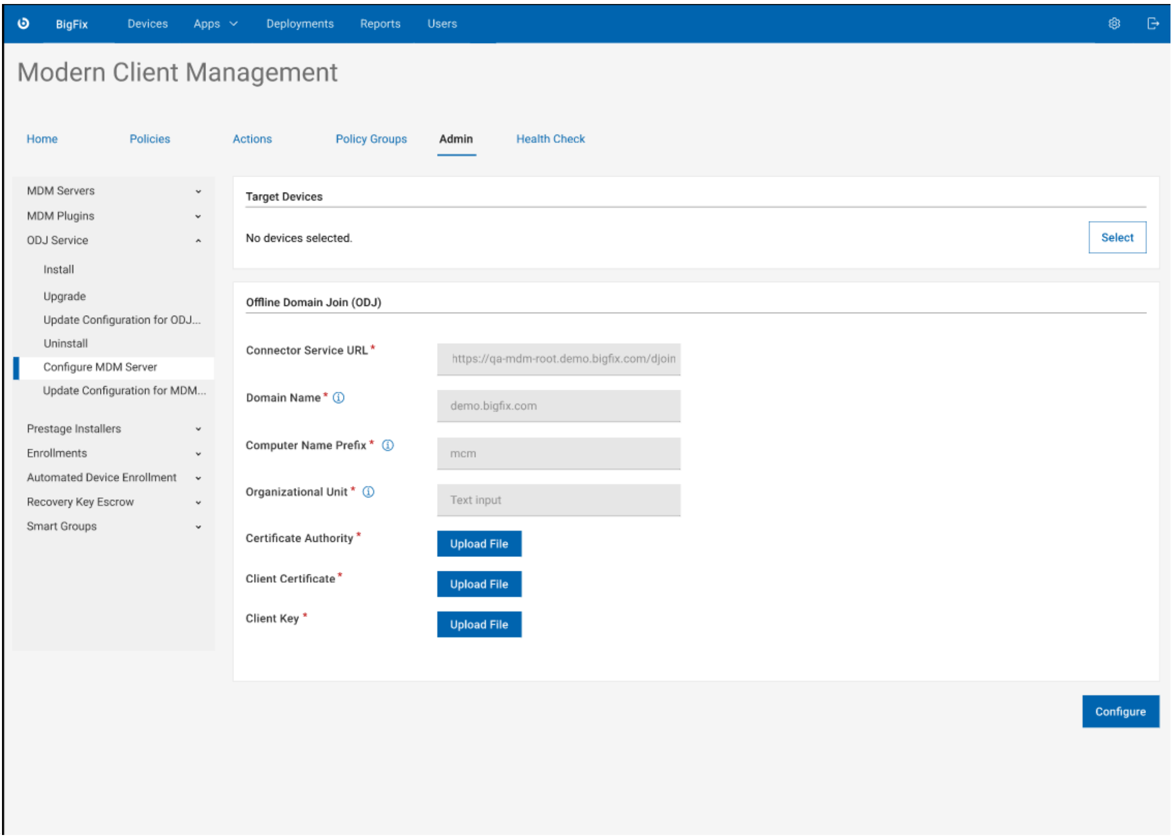
4. On the Target Devices section, click **Select** to target one or more Windows machine in which you want to remove the ODJ service.
5. Click **Deploy**.

ODJ service is uninstalled from the selected targets. There is no recovery from an ODJ service uninstall. To get the Autopilot-enrolled Windows devices to join the Active Directory again, ODJ service must be reinstalled.

Configure MDM Server for ODJ Service

Learn how to configure MDM Server to utilize ODJ service.

1. On the MCM Admin page, from the left navigation, under **ODJ Services**, select **Configure MDM Server**.



Target Devices

No devices selected.

Offline Domain Join (ODJ)

Connector Service URL * https://qa-mdm-root.demo.bigfix.com/djoin

Domain Name * demo.bigfix.com

Computer Name Prefix * mcm

Organizational Unit * Text input

Certificate Authority *

Client Certificate *

Client Key *

2. Click **Select** to select an MDM server.
3. In the Offline Domain Join (ODJ) section, do the following:
    - **Connector Service URL**: Provide the URL in the format: https://<ODJ_connector_host>/djoin

      Where <ODJ_connector_host> is the hostname or IP address of the server hosting the ODJ service.

      For example: https://172.xx.xxx.xxx/djoin, https://odj.example.com/djoin.
    - **Domain Name**: Provide the Fully Qualified Domain Name (FQDN) of your Active Directory (AD) domain to which the computers are to join.

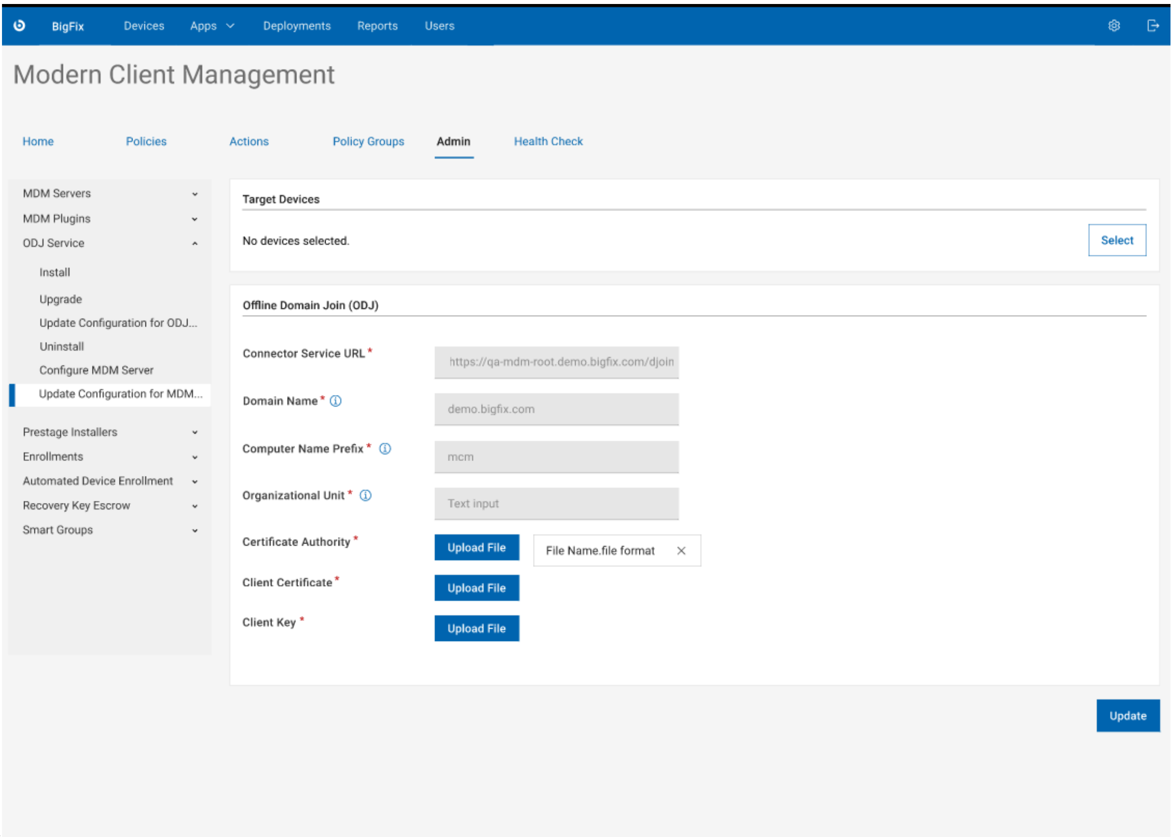
- **Computer Name Prefix**: Provide an appropriate prefix for the computer name. Computer names are 15 characters long. After the prefix, random characters are automatically added to generate 15-character computer names.
- **Organizational Unit:** Provide the distinguished name of the Organizational Unit (OU) where the computer accounts need to be created. If not specified, the default OU in your Active Directory domain is used.
- Upload the appropriate certificate files that you have created for ODJ server. See ODJ and MDM SSL certificates and keys.
    - **Certificate Authority**: Click **Upload File** and navigate and select `ca.cert.pem` file.
    - **Client Certificate**: Click **Upload File** and navigate and select `client.cert.pem` file.
    - **Client Key**: Click **Upload File** and navigate and select `client.key` file.

4. Click **Configure**.

Update configuration for MDM Server

You can modify the ODJ configuration done previously on the MDM Server to update the configuration.

1. On the MCM Admin page, from the left navigation, under **ODJ Services**, select **Configure MDM Server**.



Target Devices

No devices selected.

Offline Domain Join (ODJ)

Connector Service URL * https://qa-mdm-root.demo.bigfix.com/djoin

Domain Name * demo.bigfix.com

Computer Name Prefix * mcm

Organizational Unit * Text input

Certificate Authority * File Name.file format

Client Certificate *

Client Key *

2. Click **Select** to select an MDM Server.
3. In the Offline Domain Join (ODJ) section, to the following:

- **Connector Service URL**: Provide the URL in the format: https://<ODJ_connector_host>/djoin

  Where <ODJ_connector_host> is the hostname or IP address of the server hosting the ODJ service.

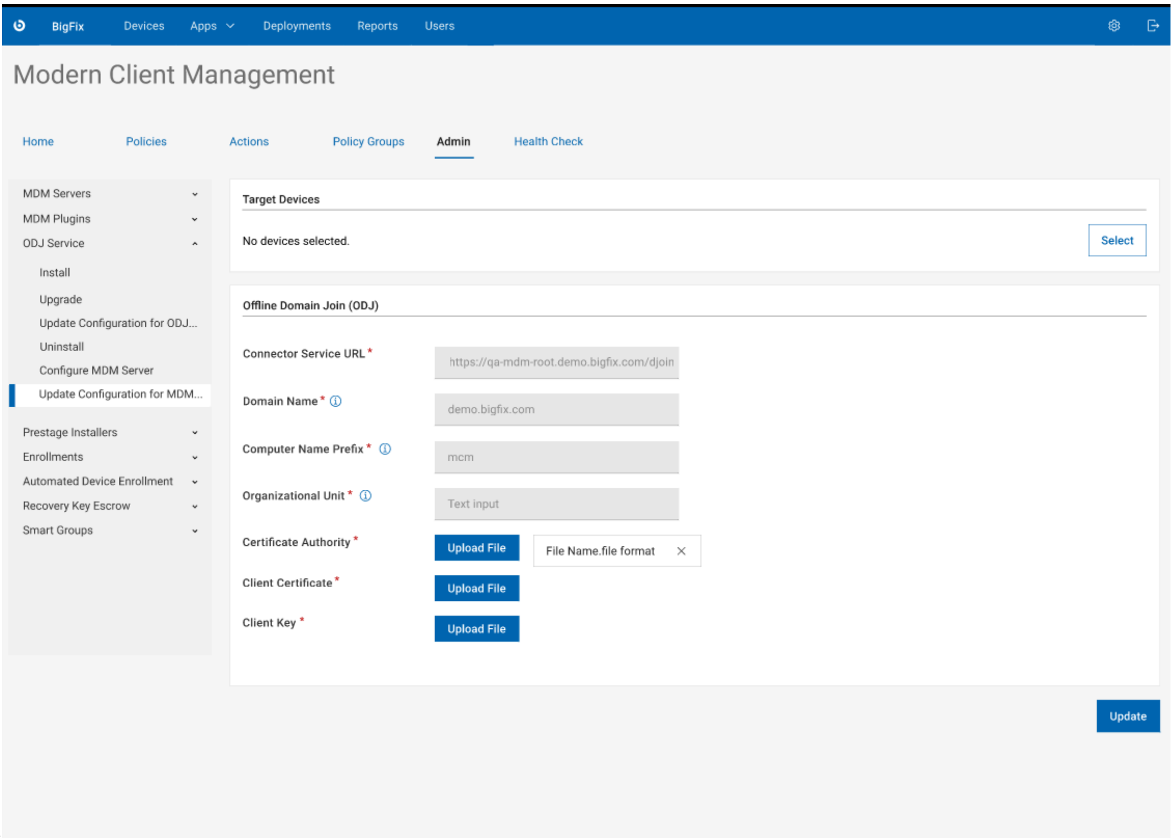
  For example: https://172.xx.xxx.xxx/djoin, https://odj.example.com/djoin.
- **Domain Name**: Provide the Fully Qualified Domain Name (FQDN) of your Active Directory (AD) domain to which the computers are to join.
- **Computer Name Prefix**: Provide an appropriate prefix for the computer name. Computer names are 15 characters long. After the prefix, random characters are automatically added to generate 15-character computer names.
- **Organizational Unit:** Optional. Provide the distinguished name of the Organizational Unit (OU) where the computer accounts need to be created. If not specified, the default OU in your Active Directory domain is used.
- Upload the appropriate certificate files that you have created for ODJ server. See ODJ and MDM SSL certificates and keys.
  - **Certificate Authority**: Click **Upload File** and navigate and select `ca.cert.pem` file.
  - **Client Certificate**: Click **Upload File** navigate and select `client.cert.pem` file.
  - **Client Key**: Click **Upload File** and navigate and select `client.key` file.

4. Click **Update**.

Remove configuration for MDM Server

You can remove the ODJ configuration from the MDM Server.

1. On the MCM Admin page, from the left navigation, under **ODJ Services**, select **Configure MDM Server**.



Target Devices

No devices selected.

Offline Domain Join (ODJ)

Connector Service URL * https://qa-mdm-root.demo.bigfix.com/djoin

Domain Name * demo.bigfix.com

Computer Name Prefix * mcm

Organizational Unit * Text input

Certificate Authority * File Name.file format

Client Certificate *

Client Key *

2. Click **Select** to select an MDM Server.
3. In the Offline Domain Join (ODJ) section, to the following:
    - **Connector Service URL**: Provide the URL in the format: https://<ODJ_connector_host>/djoin

      Where <ODJ_connector_host> is the hostname or IP address of the server hosting the ODJ service.

      For example: https://172.xx.xxx.xxx/djoin, https://odj.example.com/djoin.
    - **Domain Name**: Provide the Fully Qualified Domain Name (FQDN) of your Active Directory (AD) domain to which the computers are to join.
    - **Computer Name Prefix**: Provide an appropriate prefix for the computer name. Computer names are 15 characters long. After the prefix, random characters are automatically added to generate 15-character computer names.
    - **Organizational Unit:** Optional. Provide the distinguished name of the Organizational Unit (OU) where the computer accounts need to be created. If not specified, the default OU in your Active Directory domain is used.
    - Upload the appropriate certificate files that you have created for ODJ server. See ODJ and MDM SSL certificates and keys.

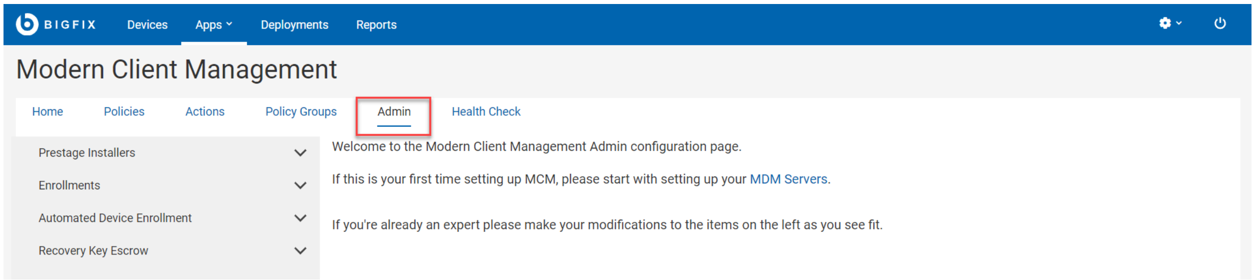
   - **Certificate Authority**: Click **Upload File** and navigate and select `ca.cert.pem` file.
   - **Client Certificate**: Click **Upload File** and navigate and select `client.cert.pem` file.
   - **Client Key**: Click **Upload File** and navigate and select `client.key` file.

4. Click **Update**.

Configuring BigFix MCM and BigFix Mobile

After the MCM components are set up, there are additional configuration options available to enable features like Bulk Enrollment for Windows, DEP policies for macOS, or prestage installers for Windows and MacOS MDM endpoints.

To configure MCM, from the WebUI main page, click **Apps > MCM** and from the Modern Client Management page, select **Admin**.



Welcome to the Modern Client Management Admin configuration page.

If this is your first time setting up MCM, please start with setting up your MDM Servers.

If you're already an expert please make your modifications to the items on the left as you see fit.

Depending on the operating system and enrollment type, you can navigate to the configuration option to complete these configuration tasks:

- Prestage macOS BigFix installer *(on page 235)*
- Prestage Windows BigFix Installer *(on page 236)*
- Prestage an Application *(on page 229)*
- Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations *(on page 230)*
- Create Windows Provisioning Package *(on page 240)*
- Designate Provisioning Package Generation Point *(on page 239)*
- Configure Windows Autopilot Terms of Service *(on page 249)*
- Generate Encryption Recovery Key Escrow Certificate *(on page 260)*
- Setup Recovery Key Escrow Plugin *(on page 261)*
- Manage Automated Device Enrollment Policies *(on page 256)*

Smart Groups

Smart groups are dynamic user groups created and managed based on Active Directory group, user attributes, and device attributes. The members of a smart group are defined dynamically in WebUI, rather than being manually defined by an administrator. You can target multiple devices using smart groups that a user or a device is subscribed to and you can manage apps, device access, group membership and so on.

Advantages

Smart groups facilitate scalable management of MDM-enrolled devices via user-based enrollment and device targeting. If you have defined a smart group, you can:

- Deploy customized policies such as passcode policy, restriction policy, certificate policy for a specific set of devices.
- Trigger customized actions such as lock, wipe as applicable on specific set of devices.

Smart groups can also be used as an effective access control system to provide access permissions to resources based on user attributes, such as job title, department, or location, and device attributes, such as operating system. For example, you can create a smart group to include all users who belong to "Engineering" department, located in "the United States", using iOS mobile phones, and you can grant access to specific engineering-related resources applicable to iOS mobile phones compliant to the United States.

With Smart Group, you can manage users where you can store user and attribute data.

Best practices

Consider the following while you create a smart group:

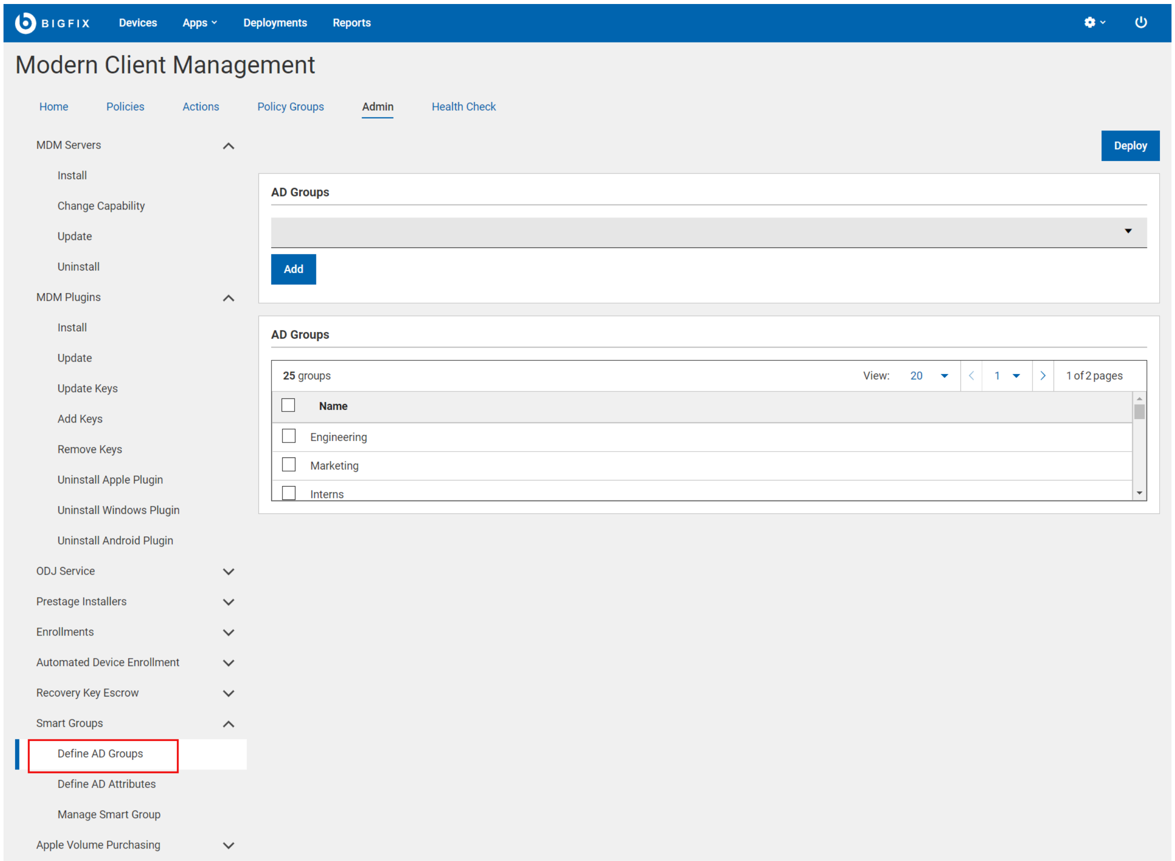
- Create Smart Groups to define either user or device criteria that must be met by a new enrollment to match a specific Policy Group and associated configuration.
- Smart Group name:
  - It should reflect the set of criteria defined in the smart group.
  - Avoid any specific device type references unless the smart group contains device criteria that identifies a specific device and/or specific OS criteria.
  - Avoid any application or policy references, as those are not defined within a Smart Group.
- The same Smart Group can apply to any number of Policy Groups.

Define Groups

You can add a subset of user groups from the Active Directory in WebUI. The groups added here can be associated to Smart Groups. so that you can target devices by the defined group names.

To define a group name, complete the following steps:

1. From the MCM **Admin** page expand **Smart Groups** and click **Define Groups**.



2. In the **AD Groups** drop-down menu, group names from the master list of Active Directory are listed. Select one or more desired user groups.

   Note: As you type in the search box, WebUI provides suggestions or auto-complete options, based on the letters or words you have entered so far.

3. Click **Add**. The user group is added to the grid.

   Note: You can add a maximum of 64 groups.

4. Click **Deploy** to deploy all the user groups added to the grid on to the MDM server.

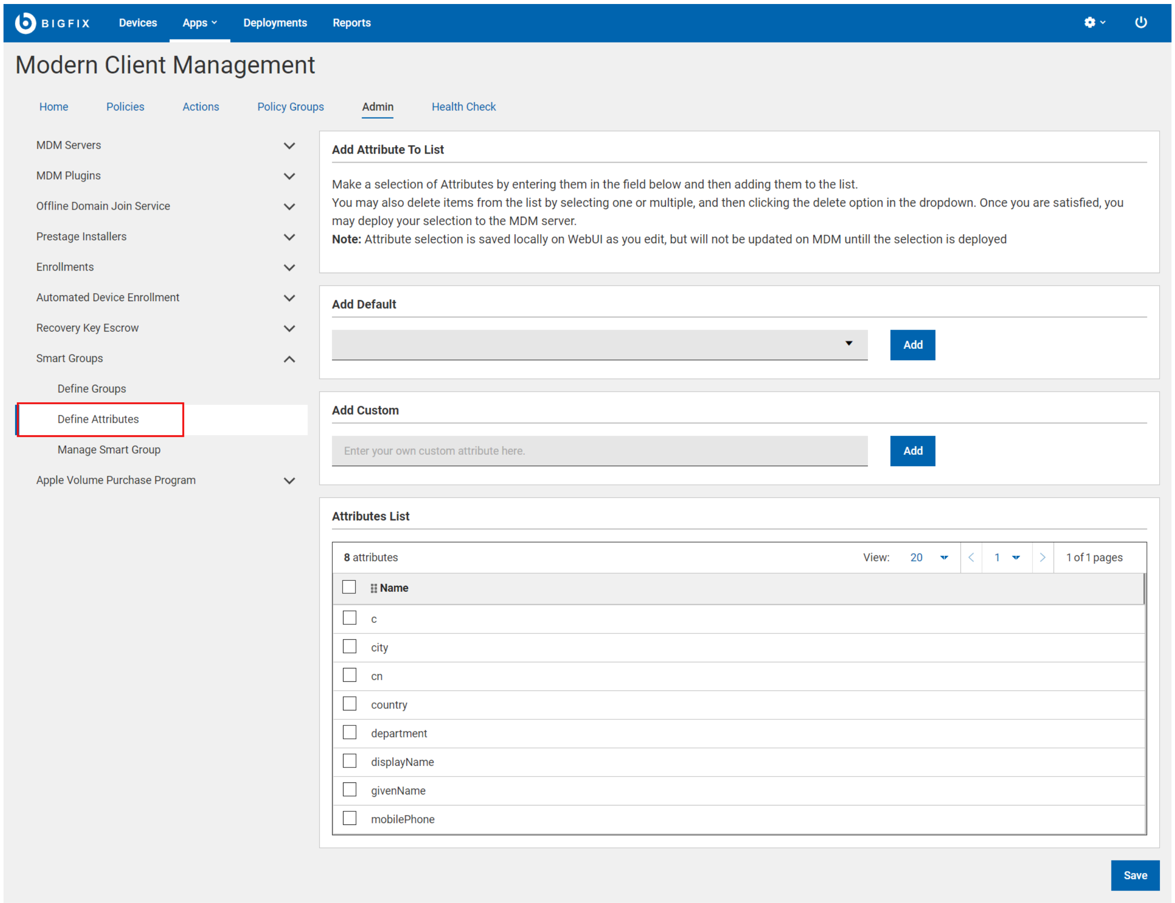
   If you want to delete a group from the grid before deploying it on to the MDM server, select one or more user groups that you want to delete and from the blue action bar, select **Delete**.

Define Attributes

You can define attributes in WebUI, so that you can target devices by the defined attributes.

To define attributes, complete the following steps:

1. From the MCM **Admin** page, explore **Smart Groups** and click **Define Attributes**.



Add Attribute To List

Make a selection of Attributes by entering them in the field below and then adding them to the list.
You may also delete items from the list by selecting one or multiple, and then clicking the delete option in the dropdown. Once you are satisfied, you may deploy your selection to the MDM server.
Note: Attribute selection is saved locally on WebUI as you edit, but will not be updated on MDM untill the selection is deployed

Attributes List

8 attributes View: 20 1 1 of 1 pages

□	Name
□	c
□	city
□	cn
□	country
□	department
□	displayName
□	givenName
□	mobilePhone

2. **Add Default**: Click this drop down list to view the list of attributes available in the Active Directory and select one from the list. Click **Add** to add it to the Attributes List.

   or

   Add Custom: Enter a string and click **Add** to add a custom attribute to the Attributes List.
3. Click **Save** to deploy all the attributes added to the grid on to the MDM server.

   If you want to delete an attribute from the grid before deploying it on to the MDM server, select the attribute that you want to delete and from the blue action bar, select **Delete**.

Manage Smart Groups

Read this section to learn how to create, edit, or delete a smart group.

- Create Smart Group *(on page 225)*
- Edit Smart Group *(on page 227)*
- Delete Smart Group *(on page 228)*

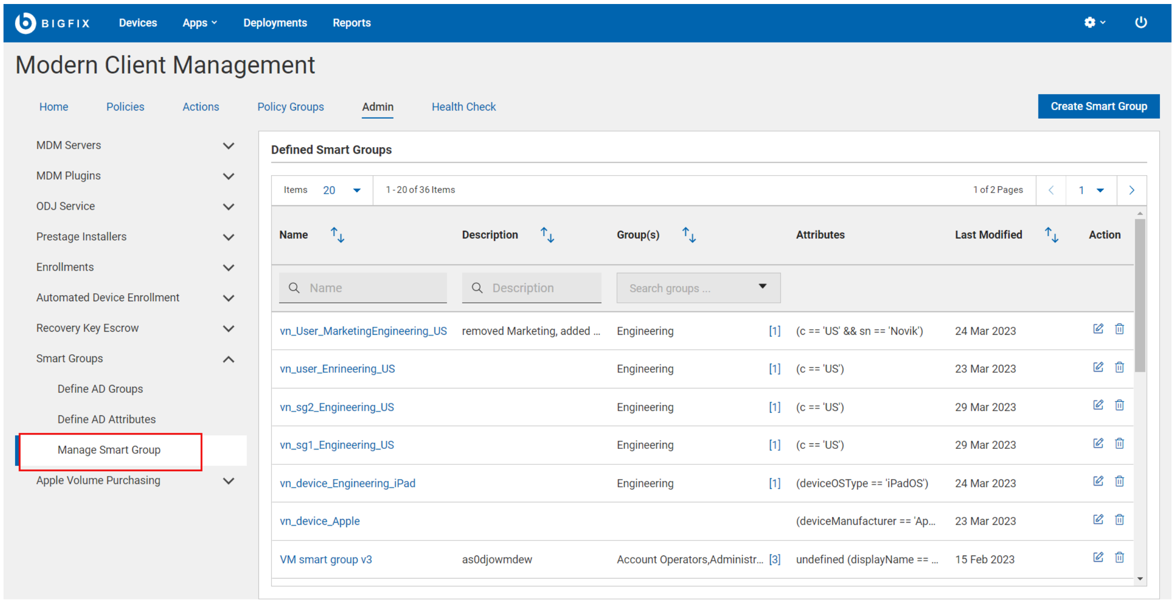
Create Smart Group

Read this topic to learn how to create a smart group.

Ensure AD groups *(on page 222)* and AD attributes *(on page 223)* are defined already to associate them to a smart group.

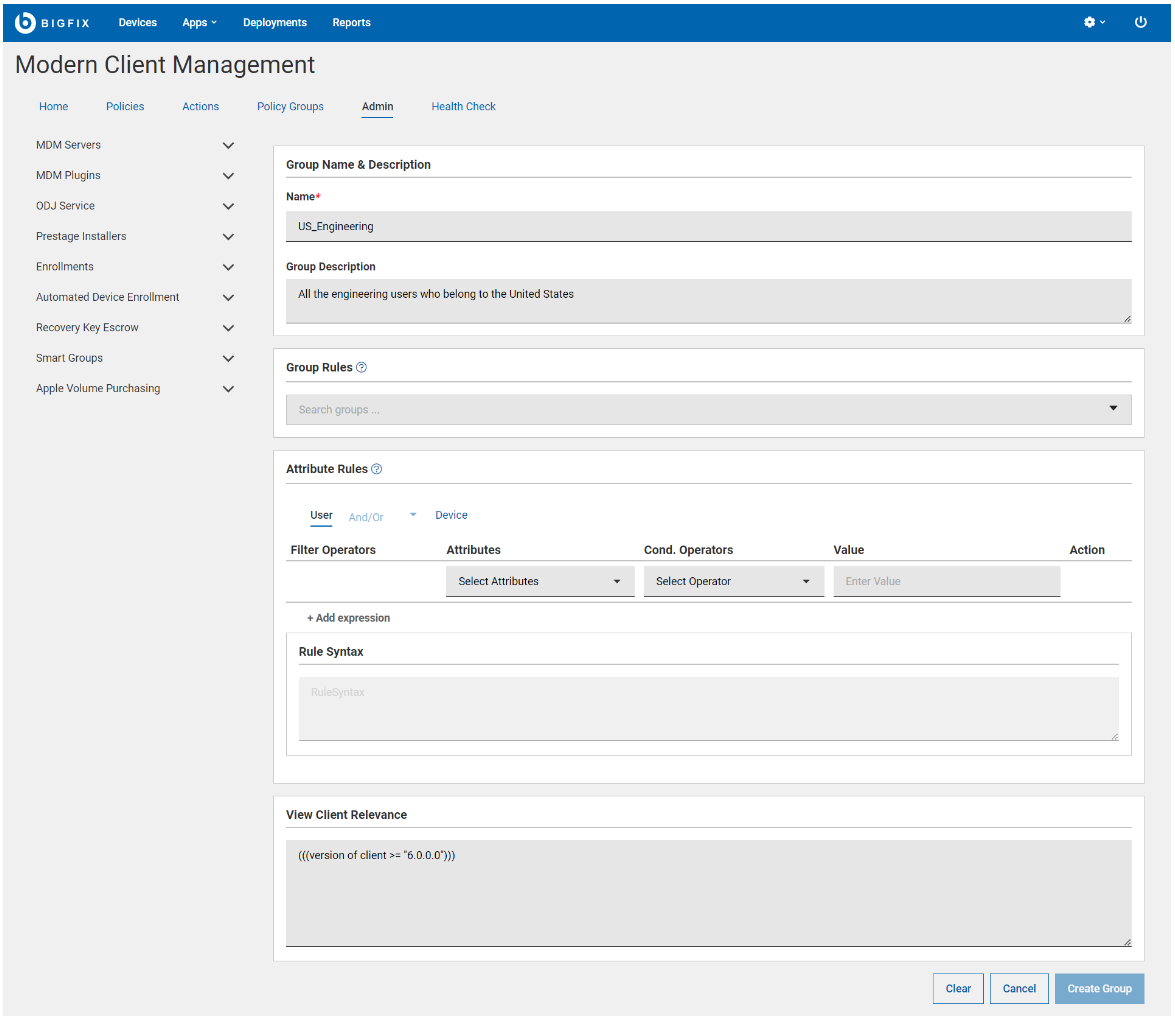
To create a smart group, complete the following:

1. From the MCM **Admin** page expand **Smart Groups** and click **Manage Smart Groups**.



Name	Description	Group(s)	Attributes	Last Modified	Action
vn_User_MarketingEngineering_US	removed Marketing, added ...	Engineering [1]	(c == 'US' && sn == 'Novik')	24 Mar 2023	
vn_user_Enrineering_US		Engineering [1]	(c == 'US')	23 Mar 2023	
vn_sg2_Engineering_US		Engineering [1]	(c == 'US')	29 Mar 2023	
vn_sg1_Engineering_US		Engineering [1]	(c == 'US')	29 Mar 2023	
vn_device_Engineering_iPad		Engineering [1]	(deviceOSType == 'iPadOS')	24 Mar 2023	
vn_device_Apple			(deviceManufacturer == 'Ap...	23 Mar 2023	
VM smart group v3	as0djowmdew	Account Operators,Administr... [3]	undefined (displayName == ...	15 Feb 2023	

2. On the top right corner, click **Create Smart Group**.
3. On the next page, for **Group Name & Description**, define the following:



Name*

US_Engineering

Group Description

All the engineering users who belong to the United States

View Client Relevance

(((version of client >= "6.0.0.0")))

- **Name**: It is a mandatory field. Enter a name for your smart group.
- **Group Description**: Provide a meaningful description for your smart group.
- **Group Rules**: The drop-down lists a maximum of 64 groups that were previously defined on the Define Groups *(on page 222)* page. Select one or more groups to define the group rules.
  - Select one or more groups from the list.
  - To add more groups to the rule, click ⊕.
  - To delete a group from the rule, click **X** next to a selected group.
- **Attribute Rules**: You can define one or more rules with combinations of attributes, conditional operators, and values.

  To add a rule and to build Relevance expression:

  - From the **Attribute Rules** section, do the following:
    - Select **User** tab to define user attribute rules.
    - Select **And/Or** to mutually include or exclude user attribute rules with device attribute rules.

> **Note:** And/Or is enabled after you define at least one User or Device attribute rule.

- Select **Device** tab to define device attribute rules.
- Select the Attributes, conditional operator, and value.
- To add another rule, click **+ Add expression**.

For example, "Department" = "Engineering" fetches all the users whose department is engineering.

The **View Client Relevance** section dynamically displays the relevance statement according to your rule definition.

4. Click **Create Group** to create the smart group.

You have created a Smart Group that defines the applicable groups and attributes and filters the applicable devices.

Example: If you have created a Smart Group named "USENGINEERS" for US Engineering users only, and add a restrictions policy named "USENGINEERRESTRICTIONS" targeted to USENGINEERS group, all endpoints that evaluate as being in the US and in the Engineering group get that specific restrictions policy.

You can target specific devices using the created smart group. You can also associate the smart group with policy group to deploy policies to specific set of devices.

Edit Smart Group

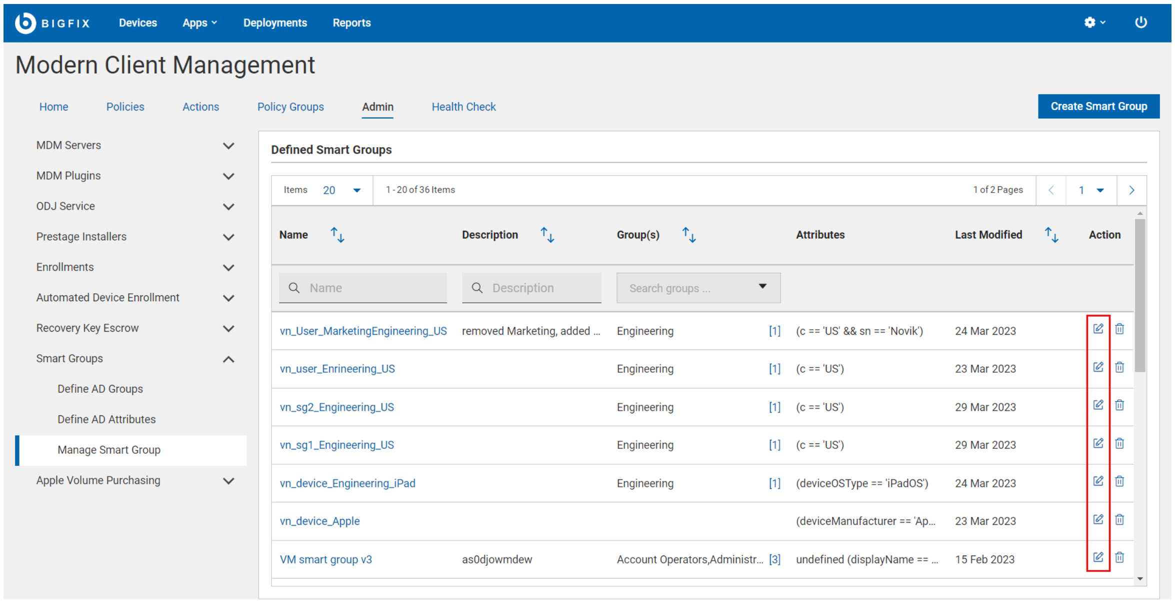
Read this section to learn how to edit and modify a smart group that you have already created.

When an existing smart group is modified:

- Any policy or policy group that has been assigned to devices, that was relevant before, is removed.
- The policy or policy group assignment is retained for the modified smart group.
- Policies or policy groups are reapplied to all relevant devices with correct policies applied.

To edit a smart group, do the following:

1. From the MCM **Admin** page expand **Smart Groups** and click **Manage Smart Groups**.
2. Click the edit button next to the smart group that you want to modify.



Name	Description	Group(s)		Attributes	Last Modified	Action
vn_User_MarketingEngineering_US	removed Marketing, added ...	Engineering	[1]	(c == 'US' && sn == 'Novik')	24 Mar 2023	
vn_user_Enrineering_US		Engineering	[1]	(c == 'US')	23 Mar 2023	
vn_sg2_Engineering_US		Engineering	[1]	(c == 'US')	29 Mar 2023	
vn_sg1_Engineering_US		Engineering	[1]	(c == 'US')	29 Mar 2023	
vn_device_Engineering_iPad		Engineering	[1]	(deviceOSType == 'iPadOS')	24 Mar 2023	
vn_device_Apple				(deviceManufacturer == 'Ap...	23 Mar 2023	
VM smart group v3	as0djowmdew	Account Operators,Administr...	[3]	undefined (displayName == ...	15 Feb 2023	

3. In the next screen, make changes in the description, group rule, attribute rule as needed. The client relevance is dynamically updated as you make changes.

   Note: You cannot change the smart group name once created.

4. Click **Save**.

The Smart Group definition is changed, and all the devices re-evaluate themselves against the latest Smart Group criteria.

Example:

- If you change the definition of the Smart Group by adding an attribute criterion to limit the policy to only those who do not have an AWSAdmin attribute and deploy a passcode policy to USENGINEERS, the policy will be deployed only to those devices which belong to US Engineering users without AWSAdmin attribute. Rest of the devices do not get this passcode policy.
- With the above attribute criteria, a subset of US Engineers who have the AWSAdmin attribute are no longer eligible for some of the policies deployed before making the change. Also, some policies that are not applicable for AWSAdmin group will still remain in place, unless that policy is removed from the appropriate devices.

Delete Smart Group

Read this section to learn how to delete a smart group.

When you delete a smart group:

- <TBU>

To delete a smart group, do the following:

1. From the MCM **Admin** page expand **Smart Groups** and click **Manage Smart Groups**.
2. Click the **Delete** button next to the smart group that you want to delete.
3. Click **OK** to confirm.

Manage applications

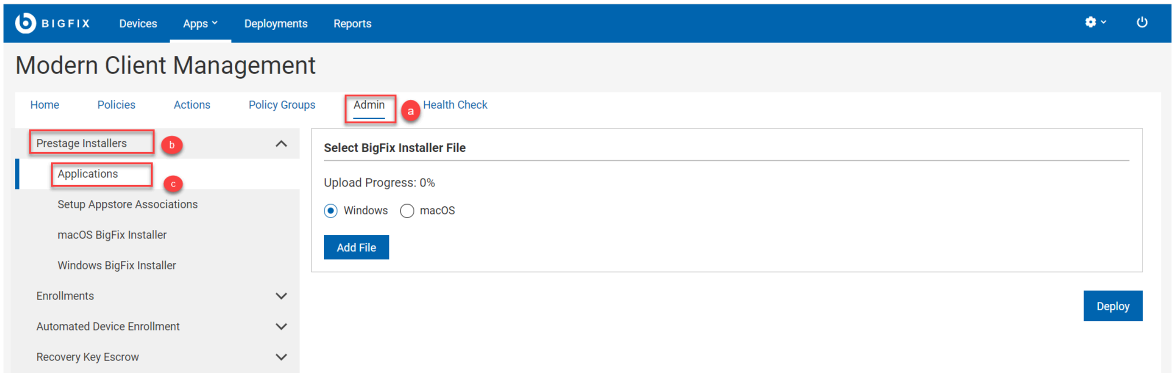
You can configure MDM server to install the BigFix agent and any other applications on and macOS devices at the time of enrollment or after devices have already enrolled.

Prestage an Application

Learn how to prestage an application in the MDM server to install on Windows and macOS devices on enrollment.

To prestage an application in the MDM server, do the following:

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin > Prestage Installers > Applications**. The following screen appears.



Upload Progress: 0%

● Windows ○ macOS

3. Select the Target Operating System.
4. Click **Add File** and browse through an `.msi` file for Windows applications or a `.pkg` file for macOS applications.
5. Click **Deploy**.

The application from the installer package becomes available in all the available MDM servers to be deployed into the compatible devices when enrolled.

Note:

Note: It might take some time for the MDM server to recognize that an application has been prestaged. The analysis that populates available packages to install updates every 15 minutes.

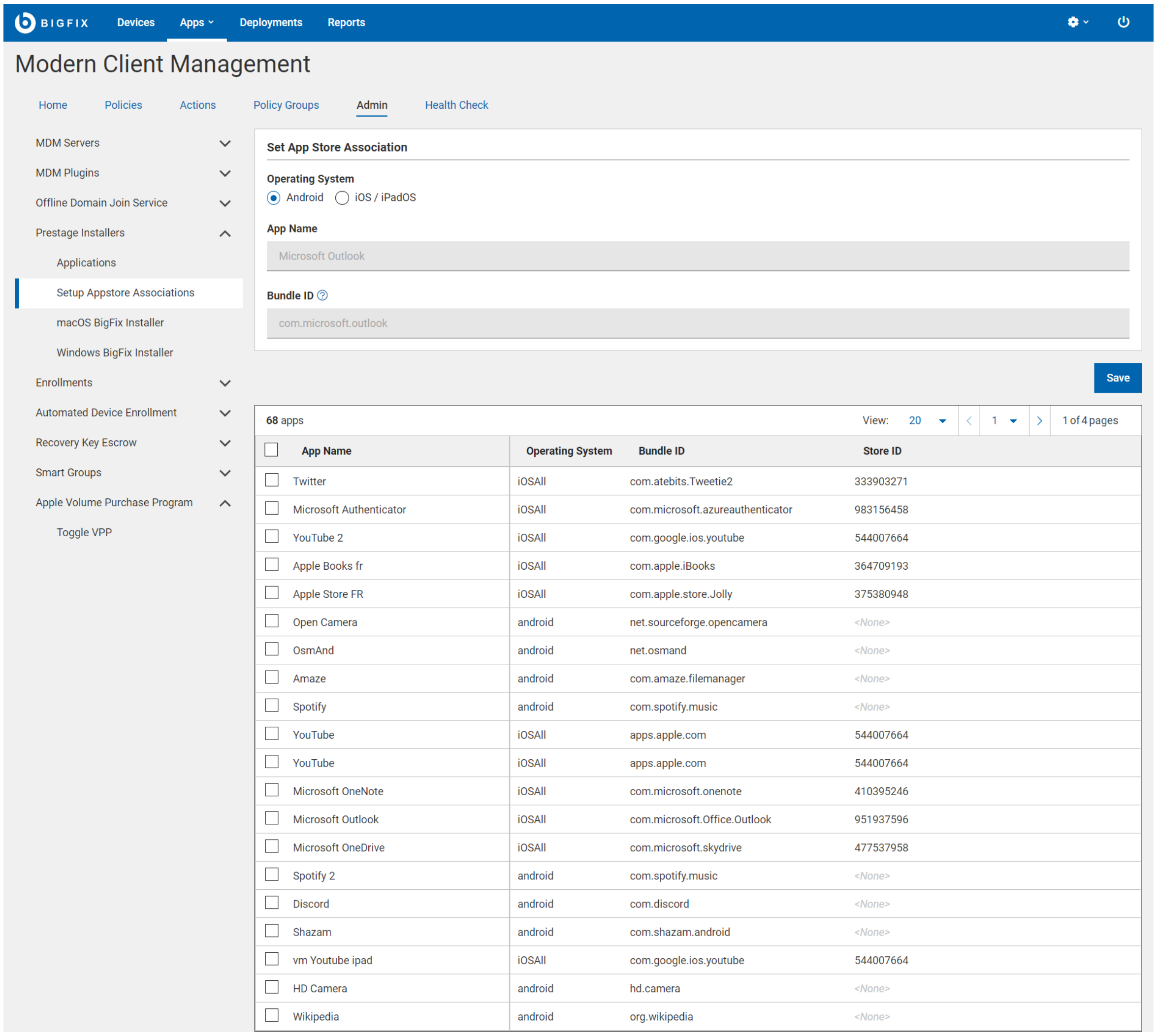
Important: macOS packages must be signed and notarized to be delivered to recent macOS versions. They also must be compatible to run on the target OS version. For example, you must install Rosetta software as a prerequisite on Apple Silicon (M1 chips) devices to run macOS packages. See https://support.apple.com/en-us/HT211861 for more details. To successfully install a macOS package, the package must be delivered to a device that has a compatible target OS.

Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations

You can create an app catalog of the apps approved by the organization and facilitate distribution to the enrolled Android, iOS, and iPadOS devices. Apps from the Apple App store (iOS and iPadOS) and Google Play Store (Android) can be included to the catalog.

To include an app from the Apple App store or Google Play Store to the app catalog approved by the organization and add approved apps into the Appstore App Policy *(on page 292)*, do the following:

1. From the WebUI main page, click **Apps > MCM**
2. On the Modern Client Management page, click **Admin > Prestage Installers > Setup Appstore Associations**. The following screen appears.



Set App Store Association

Operating System
● Android ○ iOS / iPadOS

App Name
Microsoft Outlook

Bundle ID
com.microsoft.outlook

68 apps View: 20 1 1 of 4 pages

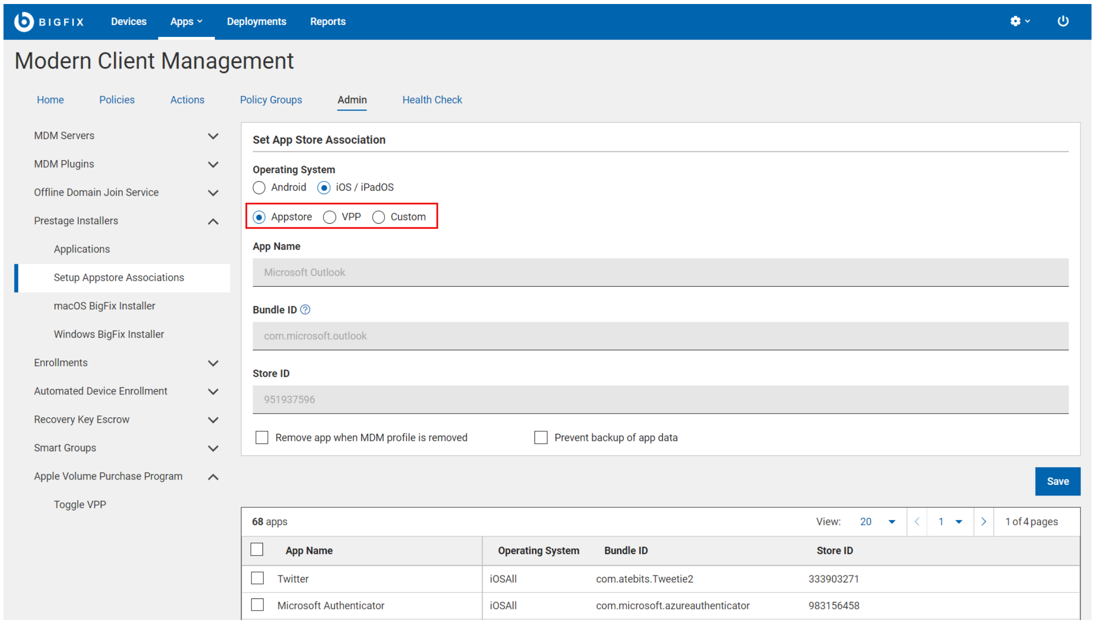
□ App Name	Operating System	Bundle ID	Store ID
□ Twitter	iOSAll	com.atebits.Tweetie2	333903271
□ Microsoft Authenticator	iOSAll	com.microsoft.azureauthenticator	983156458
□ YouTube 2	iOSAll	com.google.ios.youtube	544007664
□ Apple Books fr	iOSAll	com.apple.iBooks	364709193
□ Apple Store FR	iOSAll	com.apple.store.Jolly	375380948
□ Open Camera	android	net.sourceforge.opencamera	<None>
□ OsmAnd	android	net.osmand	<None>
□ Amaze	android	com.amaze.filemanager	<None>
□ Spotify	android	com.spotify.music	<None>
□ YouTube	iOSAll	apps.apple.com	544007664
□ YouTube	iOSAll	apps.apple.com	544007664
□ Microsoft OneNote	iOSAll	com.microsoft.onenote	410395246
□ Microsoft Outlook	iOSAll	com.microsoft.Office.Outlook	951937596
□ Microsoft OneDrive	iOSAll	com.microsoft.skydrive	477537958
□ Spotify 2	android	com.spotify.music	<None>
□ Discord	android	com.discord	<None>
□ Shazam	android	com.shazam.android	<None>
□ vm Youtube ipad	iOSAll	com.google.ios.youtube	544007664
□ HD Camera	android	hd.camera	<None>
□ Wikipedia	android	org.wikipedia	<None>

3. Under Operating System, select the OS.

    a. **Android**

        - **App Name**: Enter an appropriate name for the app.
        - **Bundle ID**:
            - Bundle ID of an app from Google Play: Find the app in Google Play and click on it to go to the app's page. The app ID is shown in the URL after `?id=`. For example, the URL for outlook is https://play.google.com/store/apps/details?id=com.microsoft.office.outlook and the bundle ID is `com.microsoft.office.outlook`.
            - Bundle ID of a private app: To know the bundle ID, from Admin Configuration UI, under Private Apps Configuration, click the desired private app icon; you can find the Bundle ID next to the **APK file** label.

    b. **IOS/iPadOS**



Set App Store Association

Operating System

○ Android ● iOS / iPadOS

● Appstore ○ VPP ○ Custom

App Name: Microsoft Outlook

Bundle ID: com.microsoft.outlook

Store ID: 951937596

□ Remove app when MDM profile is removed □ Prevent backup of app data

68 apps — View: 20 — 1 — 1 of 4 pages

□	App Name	Operating System	Bundle ID	Store ID
□	Twitter	iOSAll	com.atebits.Tweetie2	333903271
□	Microsoft Authenticator	iOSAll	com.microsoft.azureauthenticator	983156458

- Select the type of App:
  - **Appstore**: Select this option to add a normal Appstore App.
  - **VPP**: Select this option to set up the Apps that the organization has purchased in bulk through Apple's Volume Purchase Program (VPP).
  - **Custom**: Select this option to set up the customized apps that are created by the organization for unique needs of the business.

  Important: In MCM v3.0, to get the App Name, Bundle ID, and Store ID for the VPP and Custom apps, run Fixlet ID 421 Retrieve Available VPP and Custom Apps from Apple Business Manager *(on page 233)*.

- **App Name**: Enter an appropriate name for the app.
- **Bundle ID**: Bundle ID of the app from the App Store. If you know the Store ID, you can download the metadata of the app from the URL *http://itunes.apple.com/lookup?id=*<enter the storeID of the app> and search for “bundleId” in the downloaded file to get the bundle ID.

  For example, for Microsoft Outlook, the store ID is 951937596, you can download the metadata file from the URL https://itunes.apple.com/lookup?id=951937596; and if you search for “bundleId” in the downloaded file, you get “com.microsoft.Office.Outlook”.

  Alternatively, there are also few web pages that make the bundle ID lookup easier; you can try one of them.

- **Store ID**: You can find Store ID from the App Store URL. For example, the App Store URL for Microsoft Outlooks is *https://apps.apple.com/us/app/microsoft-outlook/id951937596* and the Store ID is *951937596*. Store ID must include only the numerical part.

        - **Remove app when MDM profile is removed**: Select this checkbox if you want to remove the app when MDM profile is removed.
        - **Prevent backup of app data**: Select this checkbox to prevent backup of app data.
        - **Assume Management**: This option appears if you have selected **VPP** as the type of App.

          Note: Select this option for delivering apps to supervised Apple devices only. Do not select this option if the app is to be delivered to an Apple user enrolled device, as that option is not allowed for BYOD enrollments. For more information, see Known limitations.

4. Click **Save**.

The app is added to the catalogue and listed on the Setup Appstore Associations page. Also when you create anAppstore App Policy *(on page 292)*, you can view the app listed, if you select the relevant operating system.

To delete an app from the catalogue and disassociate:

1. On the **Setup Appstore Associations** page, from the apps data grid, select one or more apps.

   The blue action bar appears.
2. Click **Delete**.

While creating an Appstore app policy, you can select one or more apps from this app catalogue to add to the policy and in turn add the policy to a policy group *(on page 269)* to distribute the applications to eligible mobile devices.

Retrieve Available VPP and Custom Apps from Apple Business Manager

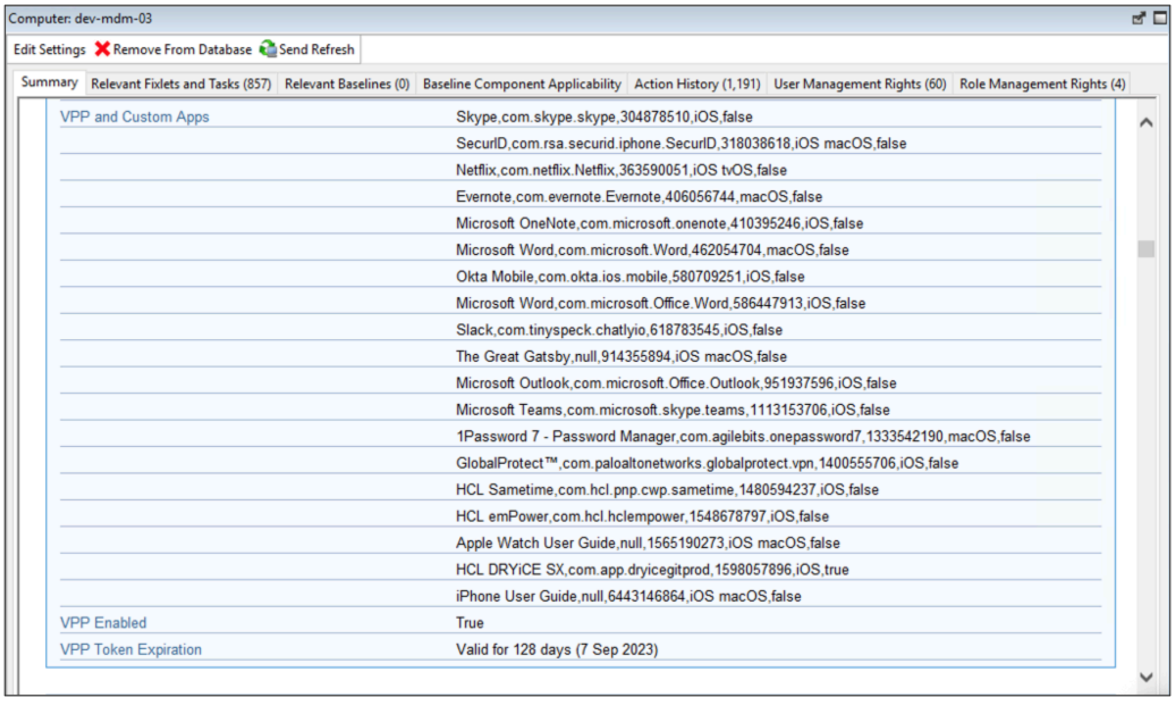
In MCM v3.0, to get the VPP and Custom Apps information such as App name, Bundle ID, Store ID to set up an App, run Fixlet 421 from the BigFix Mobile site.

The MDM Server analysis shows each of the available apps in VPP. Fixlet 421 to Retrieve Available VPP and Custom Apps from Apple Business Manager must be run to seed this analysis.

1. Log in to the BigFix console.
2. Open the **Fixlets and Tasks** icon in the Domain Panel.
3. In the search bar, enter "Retrieve Available VPP and Custom Apps".
4. Select the Fixlet named **Retrieve Available VPP and Custom Apps from Apple Business Manager**.
5. Click **Take Action**.
6. On the **Target** tab, select the MDM Server.
7. Click **OK**.
8. After the Fixlet runs successfully, MDM Server analysis shows each of the available VPP and custom apps.

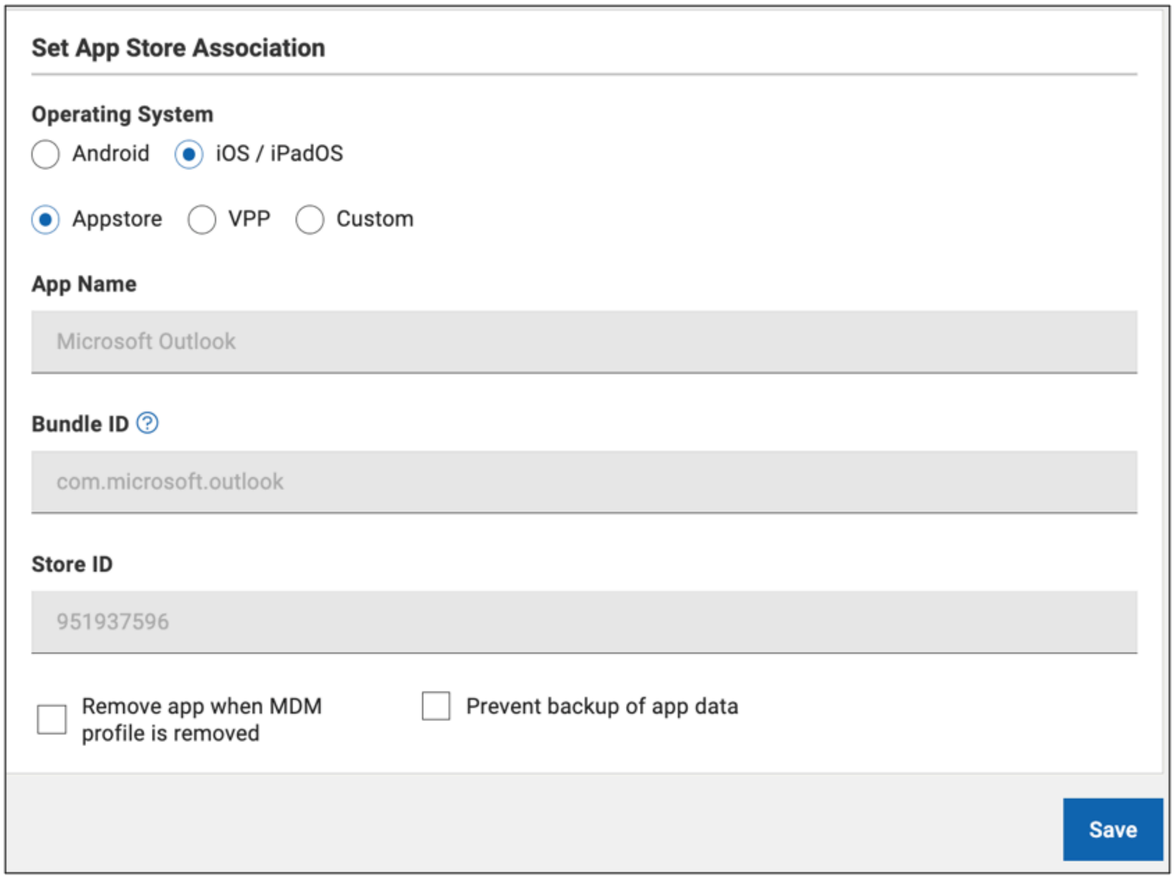
   Format of each line is as follows:

   ```
   <application name>,<bundle ID>,<store ID>,<OS Type>,<is Custom>
   ```


Computer: dev-mdm-03
Edit Settings
Remove From Database
Send Refresh
Summary
Relevant Fixlets and Tasks (857)
Relevant Baselines (0)
Baseline Component Applicability
Action History (1,191)
User Management Rights (60)
Role Management Rights (4)

VPP and Custom Apps	Skype,com.skype.skype,304878510,iOS,false
	SecurID,com.rsa.securid.iphone.SecurID,318038618,iOS macOS,false
	Netflix,com.netflix.Netflix,363590051,iOS tvOS,false
	Evernote,com.evernote.Evernote,406056744,macOS,false
	Microsoft OneNote,com.microsoft.onenote,410395246,iOS,false
	Microsoft Word,com.microsoft.Word,462054704,macOS,false
	Okta Mobile,com.okta.ios.mobile,580709251,iOS,false
	Microsoft Word,com.microsoft.Office.Word,586447913,iOS,false
	Slack,com.tinyspeck.chatlyio,618783545,iOS,false
	The Great Gatsby,null,914355894,iOS macOS,false
	Microsoft Outlook,com.microsoft.Office.Outlook,951937596,iOS,false
	Microsoft Teams,com.microsoft.skype.teams,1113153706,iOS,false
	1Password 7 - Password Manager,com.agilebits.onepassword7,1333542190,macOS,false
	GlobalProtect™,com.paloaltonetworks.globalprotect.vpn,1400555706,iOS,false
	HCL Sametime,com.hcl.pnp.cwp.sametime,1480594237,iOS,false
	HCL emPower,com.hcl.hclempower,1548678797,iOS,false
	Apple Watch User Guide,null,1565190273,iOS macOS,false
	HCL DRYiCE SX,com.app.dryicegitprod,1598057896,iOS,true
	iPhone User Guide,null,6443146864,iOS macOS,false
VPP Enabled	True
VPP Token Expiration	Valid for 128 days (7 Sep 2023)

9. Copy the corresponding values for each application to define it in the Set App Store Association WebUI page.



Set App Store Association

Operating System

○ Android ● iOS / iPadOS

● Appstore ○ VPP ○ Custom

App Name

Microsoft Outlook

Bundle ID

com.microsoft.outlook

Store ID

951937596

□ Remove app when MDM profile is removed □ Prevent backup of app data

- Operating System: Select the Operating System. In the MDM Server analysis, you can find it at <OS Type>
- Custom: Select this to define custom app. In the MDM Server analysis, you can find the value as true or false at <is Custom>
- App Name: <application name>
- Bundle ID: <bundle ID>
- Store ID: <store ID>

For example, to define Skype as a VPP app for iOS, copy the values from the MDM Server analysis as follows:

- Operating System: Select iOS/iPadOS
- VPP: Select this option.
- App Name: Skype
- Bundle ID: com.skype.skype
- Store ID: 304787510

10. Complete the rest of the steps to set up App Store Association as per Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations *(on page 230)*.

Prestage macOS BigFix installer

Learn how to prestage and deploy the latest version of the BigFix agent for macOS on the MDM Server.

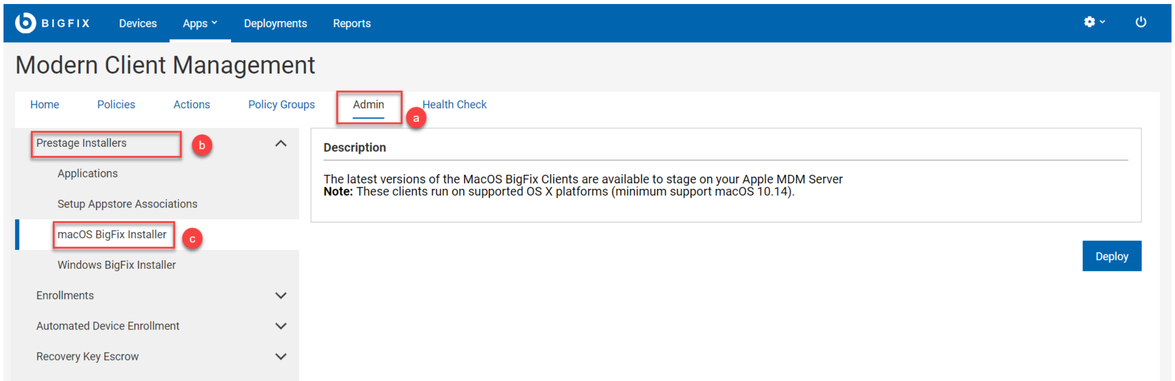
Only Master operators can prestage MacOS Agents on the MDM Server.

If the BigFix installer package is prestaged on the MDM server, after the endpoints are enrolled to MDM, you can also deploy BES agent on the enrolled devices.

BigFix provides an installation package for every released version of the BigFix agent for macOS. Every time an updated version of the package becomes available, prestage this package against the MDM Server through WebUI. When prestaged, the WebUI displays a list of available BigFix packages to deploy in the “Deploy BigFix Agent” Action when MacOS devices are selected as targets to deploy BigFix agents to.

To prestage BigFix installer for macOS devices:

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin > Prestage Installers > macOS BigFix Installer**. The following page appears:



Description

The latest versions of the MacOS BigFix Clients are available to stage on your Apple MDM Server
Note: These clients run on supported OS X platforms (minimum support macOS 10.14).

3. Click **Deploy**.

This action deploys the latest BigFix installer for macOS on all the available MDM servers.

Note:

- Only a signed macOS package that is compatible with the OS version on the target devices gets successfully installed.
- Also, the pre-requisites (if any) must be met to successfully install the macOS packages. For example, to install the macOS packages on devices with Apple Silicon (M1 chips), the pre-requisite Rosetta software must be installed on those devices. See https://support.apple.com/en-us/HT211861 for more details.
    - It might take some time for the MDM server to recognize that an application has been prestaged. The analysis that populates available packages to install updates the information every 15 minutes.

Prestage Windows BigFix Installer

Learn how to prestage and deploy the latest version of the BigFix agent for Windows on the MDM Server.

If the Windows BigFix installer package is prestaged on the MDM server, after for Windows endpoints are enrolled to MDM, you can also deploy the BigFix agent on enrolled devices.

Before you begin: Before prestaging, you must create a custom MSI package. This is because, for installing the BES server installation on Windows, the installer copies a BigFix agent in to the `BigFix Enterprise\BES Installers\ClientMSI` folder, but without a masthead (configuration profile for the BigFix agent). After a general BigFix installation, you can find the base MSI on the BigFix server. You must customize this MSI package by including the site masthead, and if required, set the Authenticating Relay information insider the installer to deploy the BigFix agent through WebUI.

A. Prepare custom BigFix agent MSI package

To prepare a custom BigFix agent MSI package, complete the following steps:

1. Locate the BigFix agent `.msi` file that is installed with the server component. (By default, it is in `BES Installers\ClientMSI\BigFixAgent.msi)`.
2. Copy the `masthead.afxm` file and the `BigFixAgent.msi` file into a new folder on a Windows machine to add the masthead to the `BigFixAgent.msi` file.
3. Run the `BESClientSetupMSI.exe` command and follow the instructions from the installer to add the masthead.
4. Optionally add authenticating relay command details if you have an authenticating relay `BESClientSetupMSI.exe /secureregistration <RELAY_PASSWORD> /relayserver1 http://<RELAY_HOST>:52311/bfmirror/downloads/ <TARGET_MSI>` to the `BigFixAgent.msi` file.

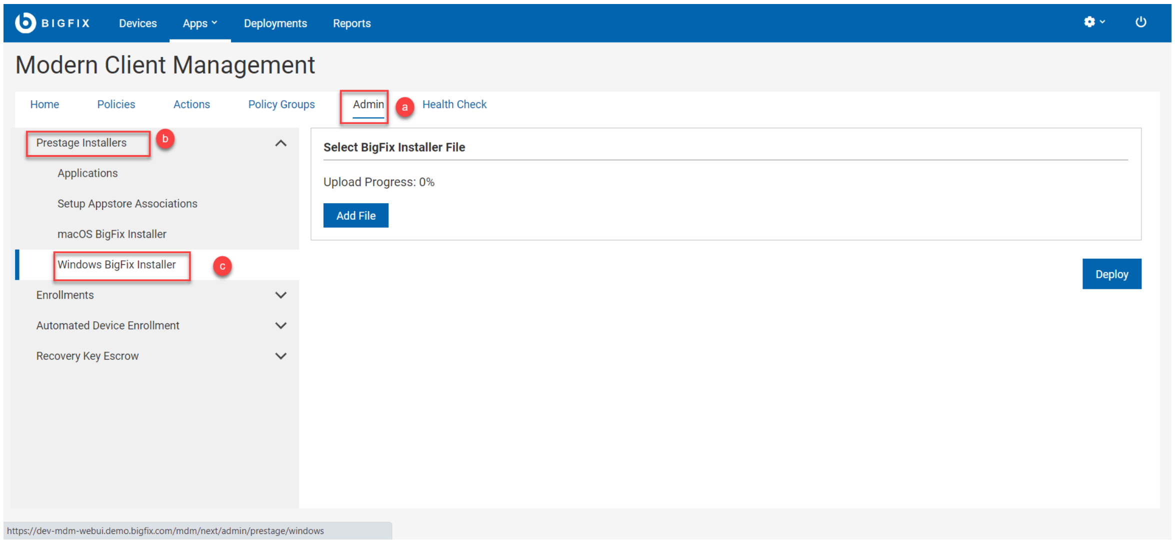
   Result: Customized `BigFixAgent.msi` file ready to be prestaged becomes available on the Windows machine at the folder you have selected.

B. Prestage BigFix installer for Windows

To pre-stage Bigfix installer for , complete the following steps:

1. From the WebUI main page, click **Apps > MCM**.

2. On the Modern Client Management page, click **Admin > Prestage Installers > Windows BigFix Installer**. The following page appears:



3. Click **Add File** and select the prepared custom `BigFixAgent.msi` file from the Windows machine.

4. Click **Deploy**.

Results: This action deploys the latest BigFix installer for Windows on all the available MDM servers. You can find the pre-staged `BigFixAgent.msi` file at `/var/opt/BESUEM/packages` on the MDM Server.

Note: It might take some time for the MDM server to recognize that an application has been prestaged. The analysis that populates available packages to install updates the information every 15 minutes.

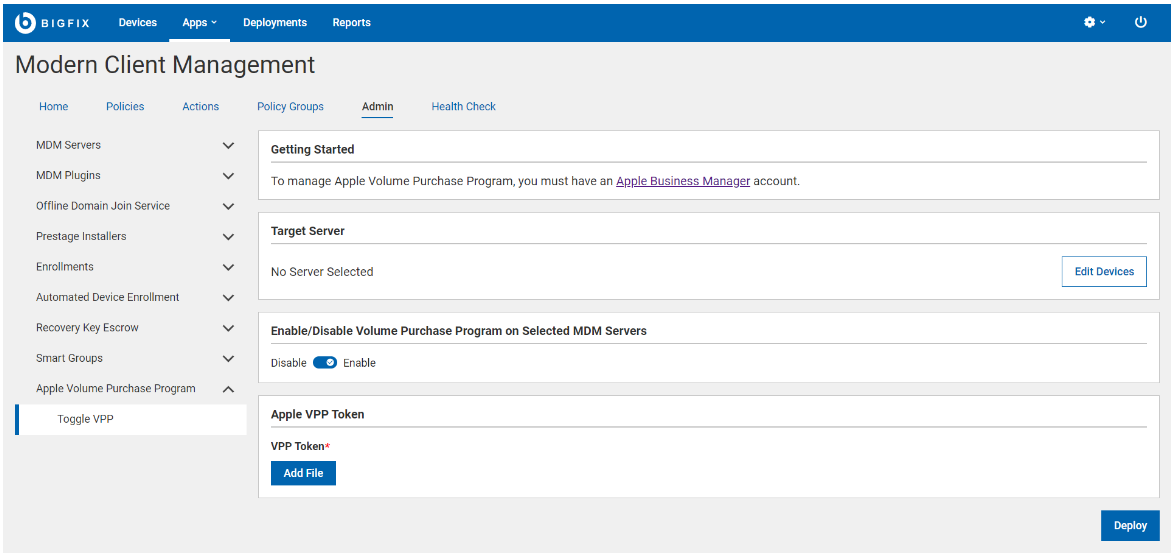
Apple Volume Purchase Program

Learn how to enable or disable Apple Volume Purchase Program (VPP) on selected MDM Servers.

You must download the Apple VPP token from Apple School Manager or Apple Business Manager using your Apple ID associated with your organization that is enrolled in the Volume Purchase Program.

The VPP token is required to link your organization's Apple Business Manager or Apple School Manager account to BigFix Mobile, which is used to distribute apps and books to devices within your organization.

1. To enable VPP, log in to WebUI as a Master Operator.
2. Navigate to **Apps > MCM**.
3. From the Admin tab, select **Apple Volume Purchase Program > Toggle VPP**.



Modern Client Management

Getting Started

To manage Apple Volume Purchase Program, you must have an Apple Business Manager account.

Target Server

No Server Selected

Enable/Disable Volume Purchase Program on Selected MDM Servers

Disable ● Enable

Apple VPP Token

VPP Token*

4. Click **Edit Devices** and select the MDM servers in which you want to enable Apple VPP.
5. Click the toggle button to Enable VPP.
6. Under **Apple VPP Token**, click **Add Files** to navigate and locate the downloaded `.vpptoken` file.
7. Click **Deploy**.

The VPP is enabled in the selected MDM server. You can set up Appstore associations *(on page 230)* to add and distribute VPP apps.

Enroll devices

You must enroll your devices to BigFix MCM to get them listed in WebUI and manage them through MDM.

BigFix MCM supports multiple enrollment methods based on the device’s operating system and the requirements in an organization. See Device Enrollment to learn various enrollment methods for different operating systems supported by BigFix MCM.

Bulk enrollment - Windows

Read this section to understand the step-by-step procedure of Windows bulk enrollment.

Prerequisites:

- Ensure the Windows devices that you target for bulk enrollment have BigFix agent installed.
- From the BigFix Console, enable Analysis 15 - `Modern Client Management Root Server Analysis`.
- In the BES root server, at `C:\Program Files (x86)\BigFix Enterprise\BES Server\Mirror Server\Config,` in the `DownloadWhitelist.txt` file, add the following:

  ```
  http://localhost.*
  ```

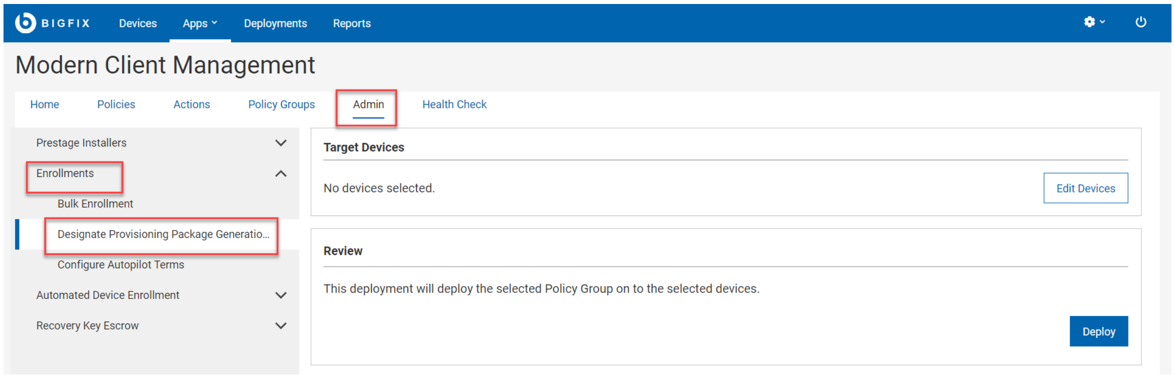
About this task: The workflow of bulk enrollment is as follows:

1. Designate Provisioning Package Generation Point: WebUI Master operator designates one or more devices to generate Windows provisioning package (`.ppkg`) file. This configuration task sets the client setting on the designated Windows endpoint to designate it as the device that creates the `.ppkg` file that is later used to enroll devices to MCM.
2. Create Windows PPKG artifact: Master operator generates `.ppkg` file using the endpoint designated in Step-1. After this step, the `.ppkg` file becomes available in the MDM server to facilitate bulk enrollment on deployment.
3. Bulk enroll: After triggering the MDM enroll action, the targeted Windows devices that have the BigFix agent installed are enrolled to MCM automatically with the pre-configured `.ppkg` artifact without user intervention.
4. Assign primary user: The primary user names for the Windows devices enrolled with `.ppkg` file must be overwritten with appropriate primary user names using the User Assignment *(on page 313)* action. Otherwise, all the enrolled Windows devices report in with the default primary user information as hardcoded in the `.ppkg` file and cannot use user and group management through Smart Groups *(on page 221)*.

Designate Provisioning Package Generation Point

To designate a device as the Windows provisioning package generation point, do the following:

1. Log in to BigFix WebUI as a Master operator.
2. On the WebUI main page, click **App > MCM**
3. On the Modern Client Management page, click **Admin > Enrollments > Designate Provisioning Package Generation Point**.



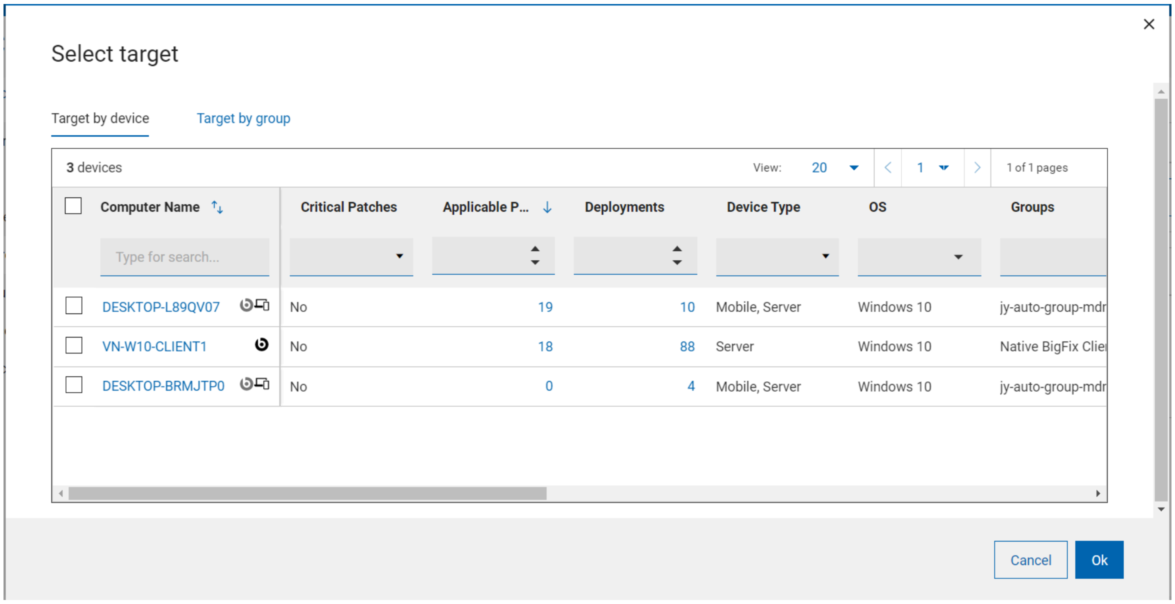
Target Devices

No devices selected.

Review

This deployment will deploy the selected Policy Group on to the selected devices.

4. On the Designate Provisioning Package Generation Point page, in the Target Device section, click **Edit Devices**.
5. On the Target By Device page, select one or more devices in one of which you want to generate the `.ppkg` file and click **OK**.



3 devices

☐	Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS	Groups
☐	DESKTOP-L89QV07	No	19	10	Mobile, Server	Windows 10	jy-auto-group-mdr
☐	VN-W10-CLIENT1	No	18	88	Server	Windows 10	Native BigFix Clie
☐	DESKTOP-BRMJTP0	No	0	4	Mobile, Server	Windows 10	jy-auto-group-mdr

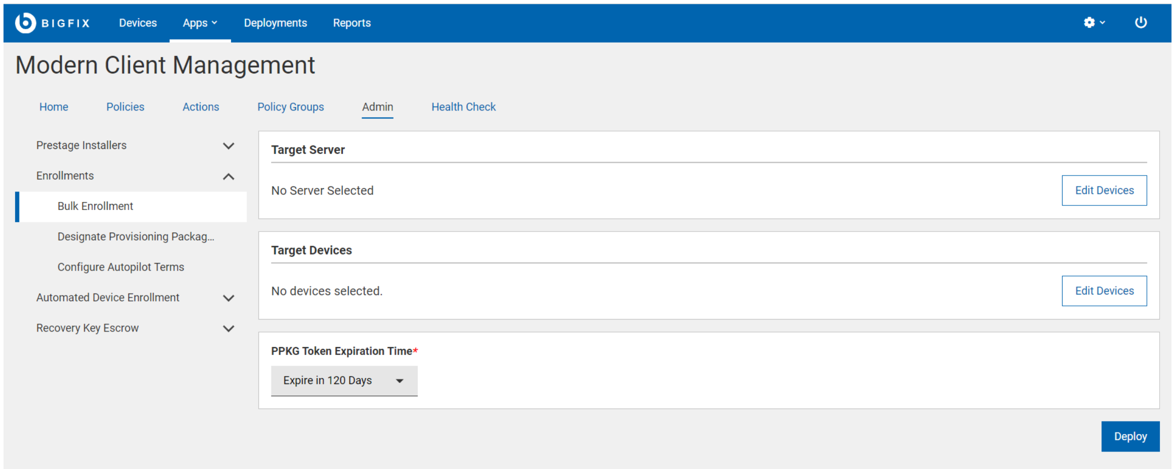
6. Verify the information in the Target Device and click **Deploy**.

Result: The selected devices become `.ppkg` generation point in one of which you can create `.ppkg` file. The client setting `MCM_WIN10_BULK_ENROLLMENT_ENDPOINT = 1` is set on the targeted devices.

Create Windows Provisioning Package

To create a Windows provisioning package (`.ppkg`) and make it available for bulk enrollment in the MDM server, do the following:

1. Login to the WebUI as a Master operator.
2. Click **App > MCM**
3. On the Modern Client Management page, click **Admin**.
4. On the Admin page, click **Enrollments > Bulk Enrollment**.



Target Server

No Server Selected

Target Devices

No devices selected.

PPKG Token Expiration Time*

Expire in 120 Days

5. The **Target Server** section displays the MDM server in which the ppkg file is deployed on successful completion of this task. To make any changes, click **Edit Devices**.
6. The **Target Device** section displays the number of devices as designated in Designate Provisioning Package Generation Point *(on page 239)*). To make any changes, click **Edit Devices**.

Note: Windows device that you select here uses ArchiveNow to upload ppkg content on to the root MDM server. If you have any specific workflow around the selected Windows endpoint and ArchiveNow, that is overwritten after this action.

7. **PPKG Token Expiration Time**: This field is mandatory. Select an option from the drop down menu to set the validity period for your ppkg. After expiry, you cannot use that ppkg to enroll Windows devices. The default expiration time is 120 days. The available options are:
   - Expire in 120 Days
   - Expire in 1 Year
   - Never Expire: If this option is selected, the ppkg does not have any expiration time.

Tip: WebUI internally creates a unique token for every PPKG. With this, you can prevent any unauthorized use of PPKG by creating and deploying a new one when you feel it is necessary. If the PPKG token on the MDM server and the enrolling device do not match, then the enrollment cannot be completed.

Important:

- If you want to deploy timestamped PPKG on to an MDM server, ensure the MDM server is upgraded to v2.1.1 or later.
- PPKG files created without expiration time (created through older version of BigFix MCM) do not work as expected in MDM server v2.1.1 or later. Therefore, you need to create PPKG again and deploy.

8. Click **Deploy**.

   Note: It takes several minutes to complete the process. To speed up the process, restart the `ppkg` generating Windows device a few times.

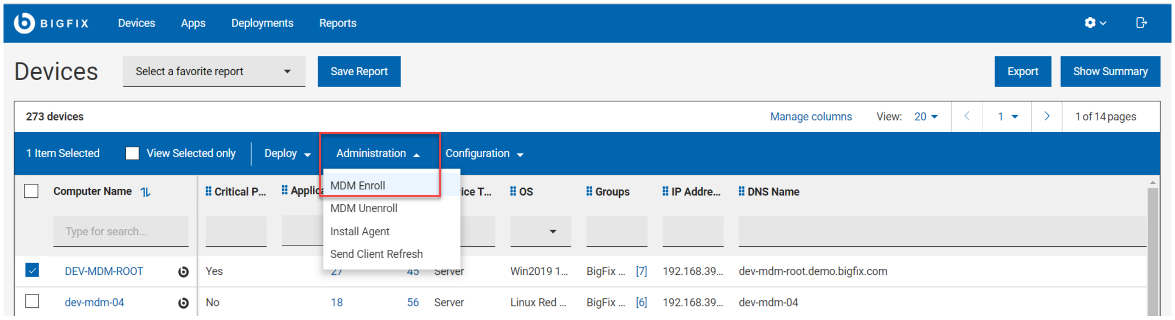
Results: After this action is completed:

- Windows `ppkg` file is created in the targeted Windows device at `C:\MCMPPKG`.
- The created `ppkg` file is transferred to the target MDM server at `/var/opt/BESUEM/packages` to facilitate enrollment.

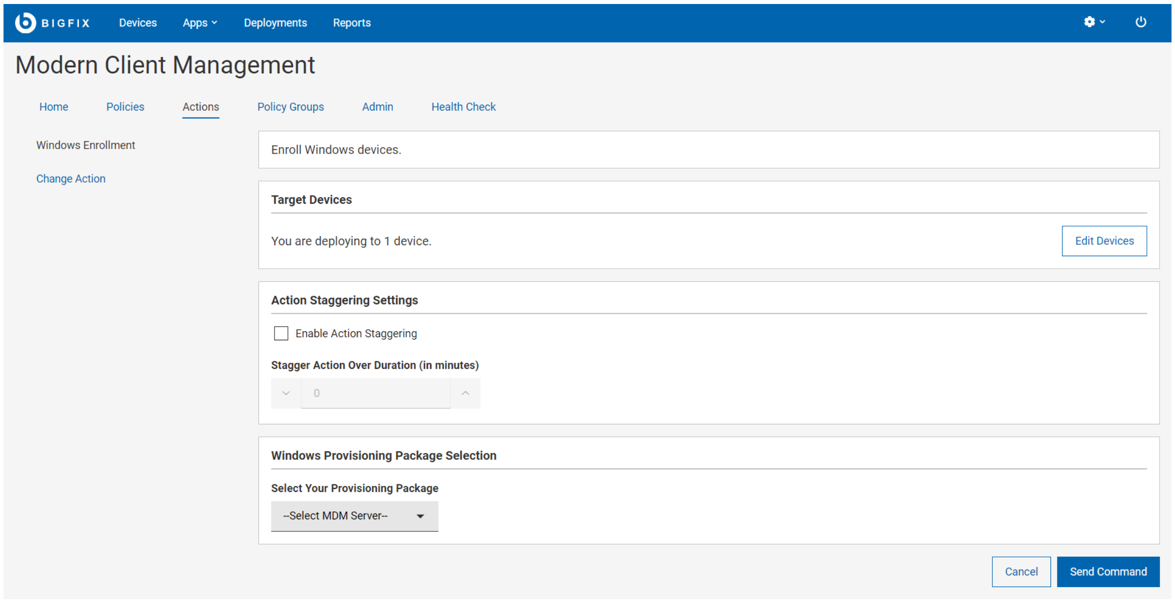
Bulk enroll

To enroll devices through bulk enrollment using the `.ppkg` artifacts that was created in the previous steps, do the following:

1. Log in to BigFix WebUI.
2. On the Devices *(on page 23)* page filter devices with native BigFix agent installed. To do that, in the **OS** column, select `Windows` and in the **Agent** column, select `Yes`.
3. From the devices list select all or a subset of devices for bulk enrollment.
4. Click **Administration > MDM Enroll**.



The **Windows Enrollment** page appears.



Modern Client Management

Enroll Windows devices.

Target Devices

You are deploying to 1 device.

Action Staggering Settings

□ Enable Action Staggering

Stagger Action Over Duration (in minutes)

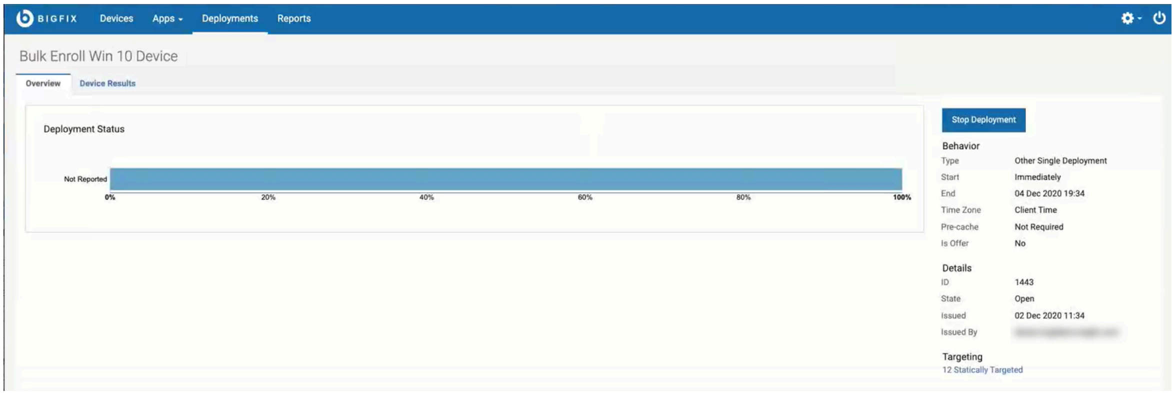
0

Windows Provisioning Package Selection

Select Your Provisioning Package

--Select MDM Server--

5. In the Target Devices section, the number of targeted devices is displayed. If you want to change the targeted devices, click **Edit Devices**.
6. Action Staggering Settings: Select **Enable Action Staggering** and enter **Stagger Action Over Duration** in minutes. Use this setting to spread out the load on the MDM server and network to prevent all the targeted endpoints attempting to enroll at the same time. Staggering enrolling endpoints normalizes the amount of traffic generated by newly enrolled devices over a broader more manageable period of time. When this is set, each endpoint selects a random time within the specified time interval to enroll.
7. For **Select Your Provisioning Package**, select the MDM server to which you want to enroll the selected devices.
8. Click **Send Command**.
    - A BigFix deployment is generated that initiates MDM enrollment on the selected devices.
    - The deployment document *(on page 150)* with information on devices targeted and device results is displayed.
    - The targeted devices start the enrollment processes.
    - At any point, to stop the deployment, click **Stop Deployment**.



Bulk Enroll Win 10 Device

Behavior

Type	Other Single Deployment
Start	Immediately
End	04 Dec 2020 19:34
Time Zone	Client Time
Pre-cache	Not Required
Is Offer	No

Details

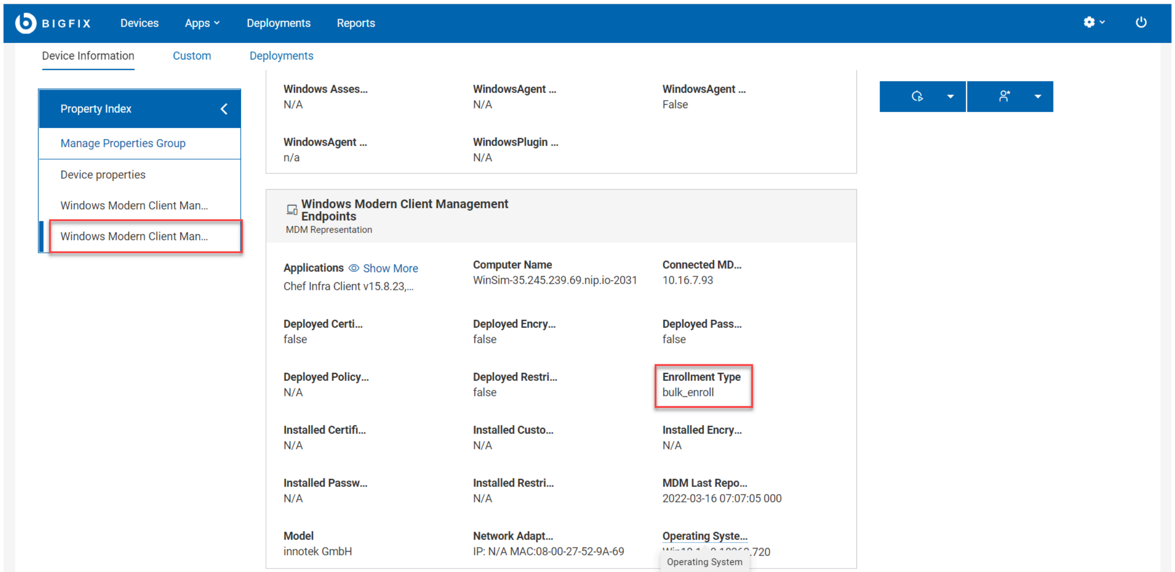
ID	1443
State	Open
Issued	02 Dec 2020 11:34
Issued By	[redacted]

Targeting

12 Statically Targeted

Results:

- After running the action, the targeted devices get enrolled to the selected MDM server.
- The enrolled devices report with MDM icon SAMPLE_WIN in The Device List *(on page 23)*.
- When you click on a bulk enrolled device from the Device List, the Device Information page shows Enrollment Type as bulk_enroll under the section Windows Modern Client Management Endpoints.



Windows Asses...
N/A

WindowsAgent ...
N/A

WindowsAgent ...
False

WindowsAgent ...
n/a

WindowsPlugin ...
N/A

Windows Modern Client Management Endpoints
MDM Representation

Applications Show More
Chef Infra Client v15.8.23,...

Computer Name
WinSim-35.245.239.69.nip.io-2031

Connected MD...
10.16.7.93

Deployed Certi...
false

Deployed Encry...
false

Deployed Pass...
false

Deployed Policy...
N/A

Deployed Restri...
false

Enrollment Type
bulk_enroll

Installed Certifi...
N/A

Installed Custo...
N/A

Installed Encry...
N/A

Installed Passw...
N/A

Installed Restri...
N/A

MDM Last Repo...
2022-03-16 07:07:05 000

Model
innotek GmbH

Network Adapt...
IP: N/A MAC:08-00-27-52-9A-69

Operating Syste...
Win10.1 [illegible] 0.19262.720
Operating System

- As a Device User, to view the configured provisional package details in the enrolled device, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package.

  For some reason, if you want to enroll this device again through bulk enrollment, do the following:

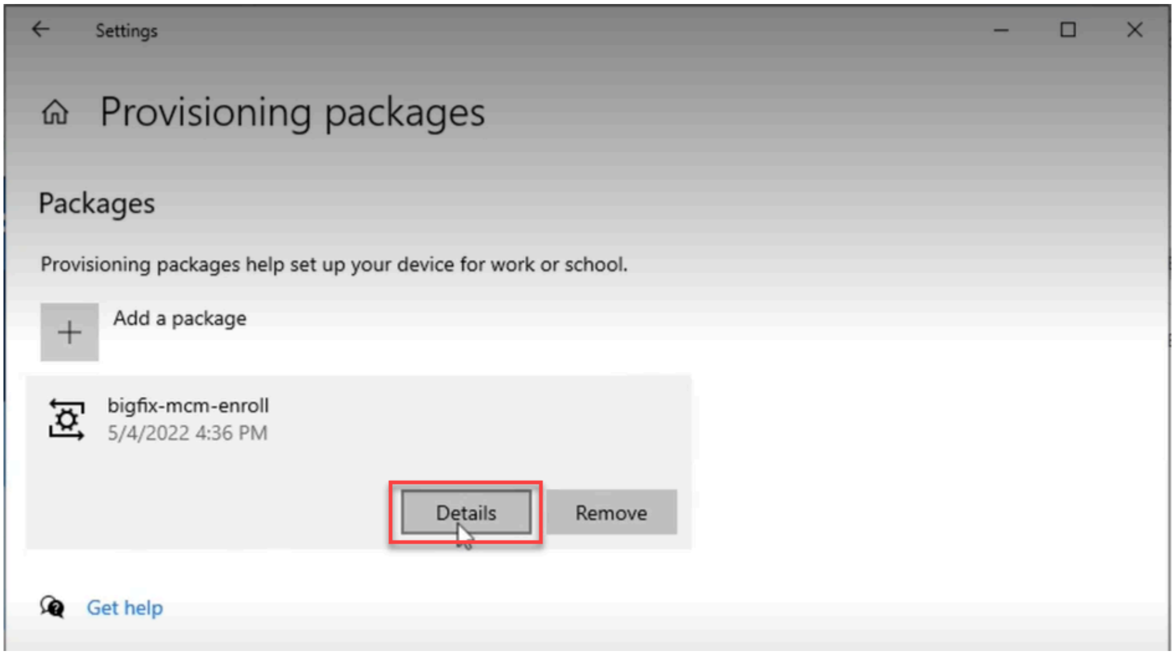
  1. Delete the provisioning package in the device.
  2. Disconnect the MDM profile under Settings > Accounts > Access work or school.
  3. From the WebUI, initiate Windows Enrollment.

Troubleshooting

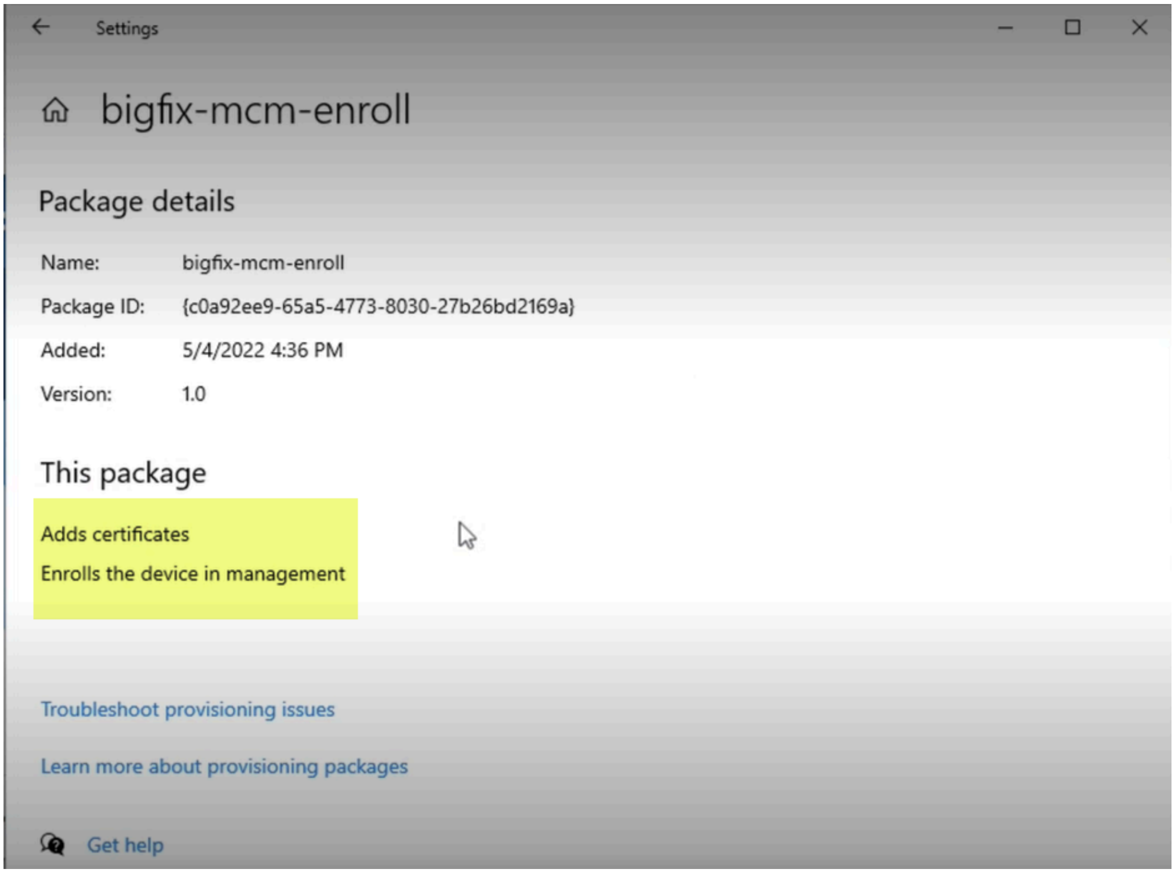
You can use the `.ppkg` file for bulk enrollment, Over-The-Air enrollment (on page 247), or Enrollment via E-mail or link to download PPKG file (on page 247).

In all these scenarios, after successful enrollment, Device User can view the configured provisional package details in the enrolled device. To do that:

1. On the Windows device, navigate to **Settings > Accounts > Access work or school > Add or remove a provisioning package.**
2. To view the details, click on the provisioning package and click **Details**.



The .ppkg details as per the configuration is displayed as shown in the following image, for example:


Settings
bigfix-mcm-enroll
Package details
This package
Troubleshoot provisioning issues
Learn more about provisioning packages
Get help

Name: bigfix-mcm-enroll

Package ID: {c0a92ee9-65a5-4773-8030-27b26bd2169a}

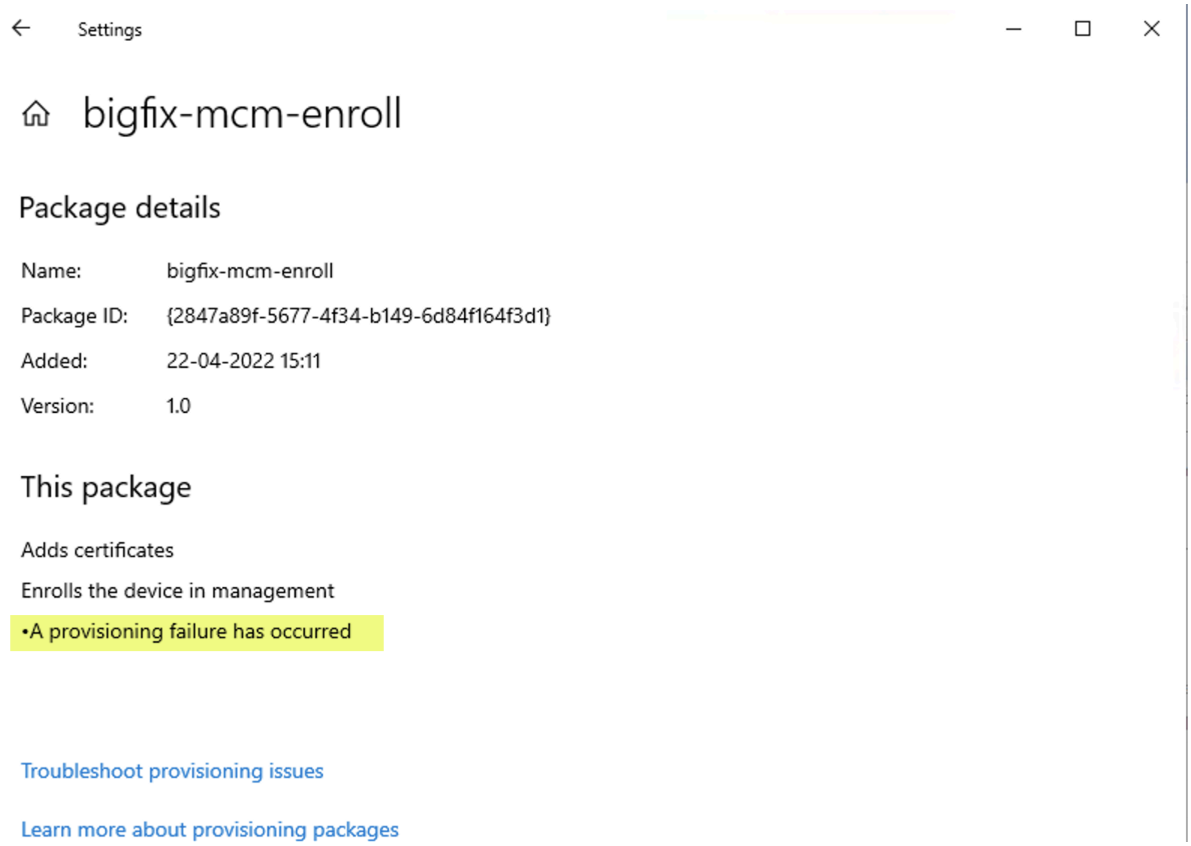
Added: 5/4/2022 4:36 PM

Version: 1.0

Adds certificates

Enrolls the device in management

In case of failure, it displays the failure message as shown the following image.



bigfix-mcm-enroll

Package details

Name: bigfix-mcm-enroll

Package ID: {2847a89f-5677-4f34-b149-6d84f164f3d1}

Added: 22-04-2022 15:11

Version: 1.0

This package

Adds certificates

Enrolls the device in management

•A provisioning failure has occurred

Troubleshoot provisioning issues
Learn more about provisioning packages

It means that the enrollment through the `.ppkg` is not successful.

There can be many reasons for `.ppkg` enrollment failure, including but not limited to the following:

- The `.ppkg` is expired. If the set PPKG Token Expiration Time *(on page 241)* is expired, enrollment through the respective `.ppkg` fails.
- The `.ppkg` on the MDM server and the one on the device are different.

Contact Admin to get an appropriate `.ppkg` file to proceed with enrollment.

Important: Before you re-attempt to enroll through another `.ppkg` file, ensure to remove the previously downloaded `.ppkg` file from the device.

User-initiated enrollment - Windows

Read this section to learn how to enroll Windows devices as a Device User.

If Windows provisioning package is present in the MDM server, Admin can share the `.ppkg` file with the Device Users to enroll Windows devices through user-initiated enrollment.

For information on how to create and deploy Windows provisioning package, see Bulk enrollment - Windows *(on page 239)*.

Important: Ensure that Windows provisioning package (`.ppkg` file) is not already present in the targeted devices before enrollment. If you are re-enrolling a Windows device, ensure the `.ppkg` file is manually deleted.

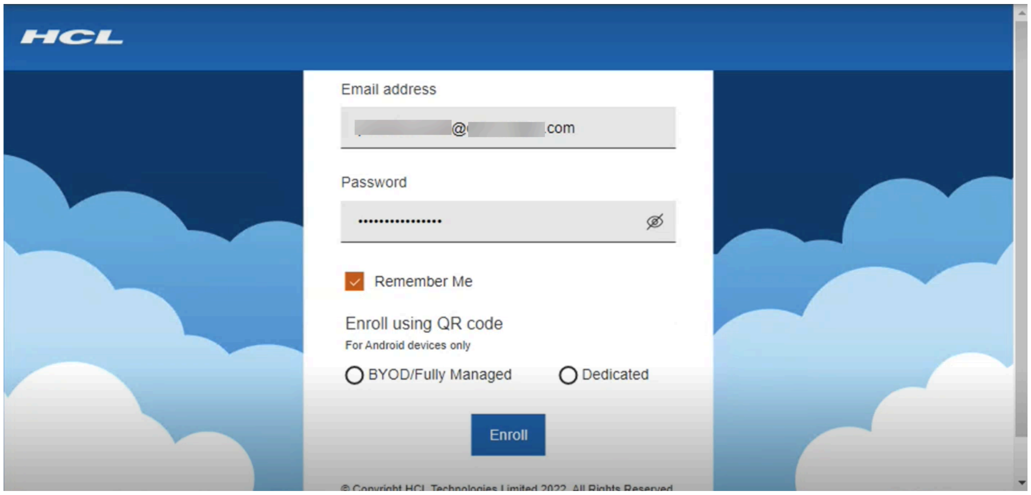
User-initated enrollments can be done in the following ways:

Over-The-Air enrollment

If the MDM server has a Windows provisioning package, when the users on devices hit the MDM Server's Enrollment URL, the `.ppkg` file is presented upon successful authentication. Users can use this `.ppkg` file to automatically enroll with MDM. To do this, complete the following:

1. Ensure the prerequisites met. On a Windows device which needs to be enrolled, launch a web browser and go to the MDM server URL. If a `ppkg` package is present on the MDM server and bulk enroll had been configured as TRUE, the following screen appears.
   - If LDAP Authentication is on, enter an email address and Password that is associated with a valid AD set of credentials and click **Enroll**.
   - If LDAP authentication is off, just click **Enroll**.

   A `ppkg` file gets downloaded.



Email address

[redacted]@[redacted]com

Password

••••••••••••••••

☑ Remember Me

Enroll using QR code

For Android devices only

○ BYOD/Fully Managed ○ Dedicated

© Copyright HCL Technologies Limited 2022. All Rights Reserved

2. Click the downloaded `ppkg` file; the enrollment process begins.

Enrollment via E-mail or link to download PPKG file

If the admin shares the `.ppkg` file with the device user via E-mail, downloadable link, or any other means, and if the device user double clicks that `.ppkg` file, MDM enrollment profile is added to the endpoint.

For troubleshooting information see, Troubleshooting (on page 244).

Autopilot enrollment

Windows Autopilot helps an administrator to automatically enroll new or factory reset Windows devices that have been preconfigured to enroll in MDM on first boot.

Autopilot configuration is done through Microsoft Endpoint Manager. For detailed information see, the BigFix Wiki page Windows Autopilot configuration guide.

Through WebUI, you can configure the following for Autopilot enrollments:

- Default Windows profile through policy groups *(on page 248)*
- Windows Autopilot Terms of Service *(on page 249)*

Configure Default Windows Profile for Autopilot enrollment

Learn how to configure a default Windows profile in the MDM server that can be deployed to Windows endpoints on enrollment.

A Policy Group is a collection of MDM policies and applications that can apply to MDM endpoints at enrollment time.

The following is the workflow to create a policy group that will apply a set of policies at enrollment time for Autopilot devices:

1. Prestage applications: The applications pre-staged on the MDM server are listed here. For information on how to pre-stage applications, see Prestage an Application *(on page 229)*.
2. Upload Custom Policy *(on page 290)*. Upload the `.xml` file that contains custom policy code as required.

   Note: Optionally you can upload a Custom policy to restrict device users from unenrolling fully-managed (company-owned) devices *(on page 249)*

3. Create other MDM policy types as required such as Passcode policy *(on page 275)*, Restrictions Policy *(on page 284)*, Certificates Policy *(on page 287)*, and save the policies.

   Note: Disk Encryption policies for Windows are not allowed to be part of policy groups for now.

4. Create a policy group *(on page 269)*
   a. Select OS: Select the operating system as Windows
   b. Add Policy: Click the + button and add the required custom policies and other MDM policies into the policy group.

      Note: Only one passcode or restriction policy is available at any given time, but multiple certificate policies are allowed.

   c. Add Application: Add the required pre-staged applications to the policy group.

d. Add BigFix Agent

e. Assign To Group: Select Autopilot Enrollment to deploy this policy group to all the Autopilot enrolled devices on enrollment by default.

f. Save the policy group.

5. Select the policy group and Deploy the Policy Group on MDM Server.

The default policy group is created and deployed on the MDM server. When Windows files are enrolled through Autopilot enrollment, the policies and applications added into this policy group are deployed onto the enrolled devices.

Custom policy to restrict device users from unenrolling fully-managed (company-owned) devices

To restrict the Windows device users from unenrolling the fully-managed (company-owned) device from MDM, upload a custom policy `.xml` file with the following code and add it to the policy group to be deployed onto the MDM server.

```
<Replace>
<CmdID>20</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/Experience/AllowManualMDMUnenrollment</LocURI>
</Target>
<Meta>
<Format>int</Format>
<Type>text/plain</Type>
</Meta>
<Data>0</Data>
</Item>
</Replace>
```

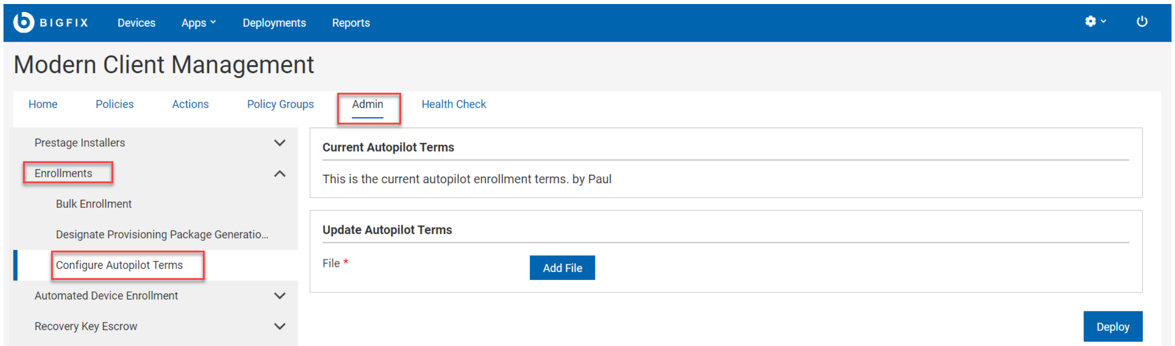
Configure Windows Autopilot Terms of Service

Learn how to customize end user agreement screen while enrolling through Windows Autopilot by adding your company’s logo and terms of service.

Create a customized terms of service HTML file.

Note: This HTML file must meet certain requirements to present certain buttons to perform specific actions for the end user. For more information on the protocol semantics, go to https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-active-directory-integration-with-mdm#terms-of-use-protocol-semantics. Autopilot Terms of Service HTML files that do not meet these requirements will prevent users from properly enrolling correctly on startup.

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, click **Admin > Enrollments > Configure Autopilot Terms**. The following page appears:



This is the current autopilot enrollment terms. by Paul

3. Under Update Autopilot Terms, click **Add File** and select the HTML file where you have the customized Terms of Service for your organization.
4. Click **Deploy**.

The configured Terms of Service page is displayed on the Windows devices when the devices are enrolled through Windows Autopilot.

Apple Automated Device Enrollment

MCM and BigFix Mobile supports the Apple Automated Device Enrollment Program (DEP) — an online service to automate the enrollment and configuration of Apple devices.

Through Apple Automated Device Enrollment, you can enroll a large number of Apple devices effortlessly without user intervention. On the Apple Business Manager portal, BigFix administrators can preconfigure which devices can be assigned to which MDM Servers, so that as part of initial device setup, devices can automatically enroll in MCM and BigFix Mobile.

For more information on Apple Automated Device Enrollment such as how to qualify for the program and links for Apple Business Manager, see Apple support site.

All Apple devices, as part of initial configuration, reach out to Apple Business Manager to see if they have been preassigned to a specific MDM Server to get enrolled. If Apple Business Manager finds configuration for a device that maps to a specific profile, it sends that profile to the device. The device processes the enrollment info, make the required settings, and then reaches out to the defined MDM Server within the profile to do an MDM enrollment. If there is no specific device to Apple Automated Device Enrollment profile mapping, a device gets the Automated Device Enrollment profile assigned to the MDM Server that is marked as an auto-assigner.

For instructions on configuring ABM or MCM server for Automated Device Enrollment, see the BigFix Wiki page Apple Business Manager Quick Start Guide for DEP

Note: All the Automated Device Enrollment profile configuration files (`.crt, .key, .enc,` and `.p7M`) are stored in the `/var/opt/BESUEM/certs` directory on the MDM server.

Once all these configurations are done, when a user powers up the Apple device for the initial OS setup and connects to Internet, Apple server receives a notification, recognizes the Automated Device Enrollment profile account, and redirects the device to the appropriate MDM server. The Setup Assistant on the Apple devices takes the users through the activation process.

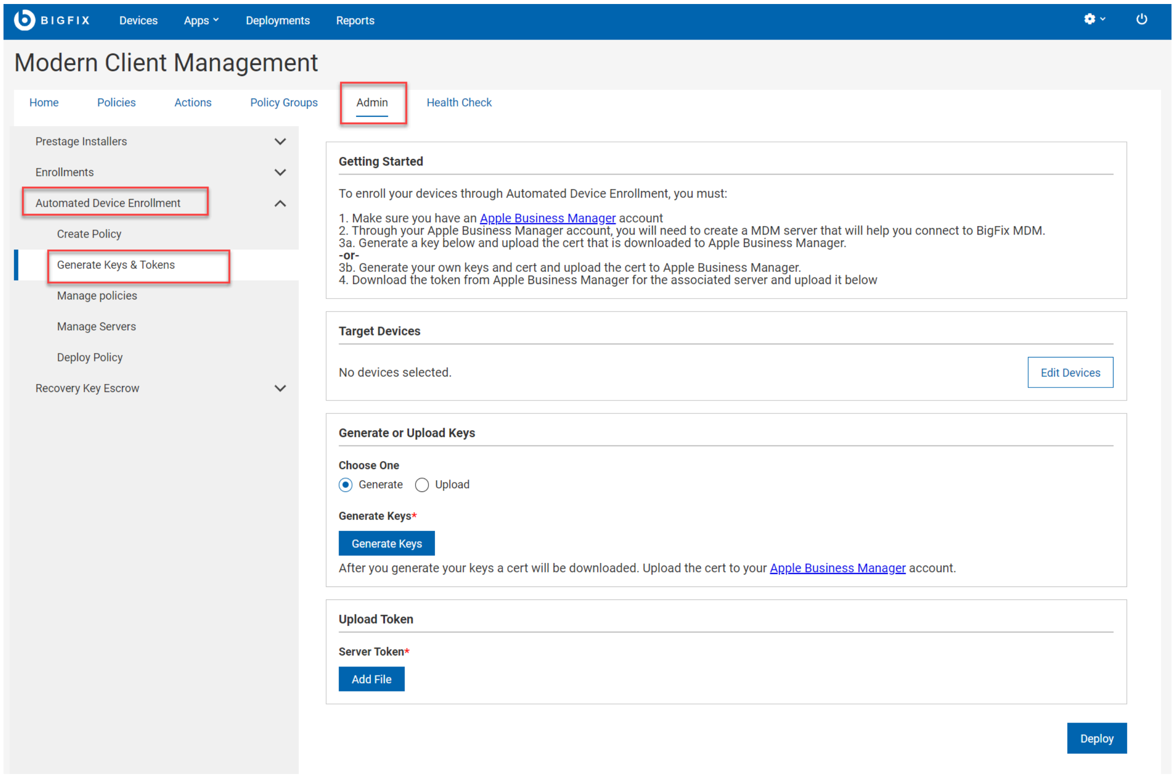
After the devices are enrolled, you can manage MDM devices through WebUI (on page 257).

Generate or upload public key

You need the key in `.pem` format to define your MDM server in Apple Business Manager.

To create the public key for the MDM server that you want to define in Apple Business Manager:

1. Log in to BigFix WebUI as a Master Operator.
2. From the WebUI main page, click **Apps > MCM**.
3. On the Modern Client Management page, click **Admin > Automated Device Enrollment > Generate Keys & Tokens**. The following page appears:



Getting Started

To enroll your devices through Automated Device Enrollment, you must:

1. Make sure you have an Apple Business Manager account
2. Through your Apple Business Manager account, you will need to create a MDM server that will help you connect to BigFix MDM.
3a. Generate a key below and upload the cert that is downloaded to Apple Business Manager.
-or-
3b. Generate your own keys and cert and upload the cert to Apple Business Manager.
4. Download the token from Apple Business Manager for the associated server and upload it below

Target Devices

No devices selected.

Generate or Upload Keys

Choose One

● Generate ○ Upload

Generate Keys*

After you generate your keys a cert will be downloaded. Upload the cert to your Apple Business Manager account.

Upload Token

Server Token*

4. Target Device: Click **Edit Devices** and select the MDM server that you want to define in Apple Business manager.
5. Generate or Upload keys:

- **Generate**: Select this option to indicate that you want to generate keys from BigFix.
- **Upload**: Select this option to browse and locate the keys of a CA-signed certificate, if you already have one.
- **Generate Keys**: Click this button when you are ready to create your own certificate to upload to Apple Business Manager account.

The public key in `.pem` format gets downloaded at your default download location.

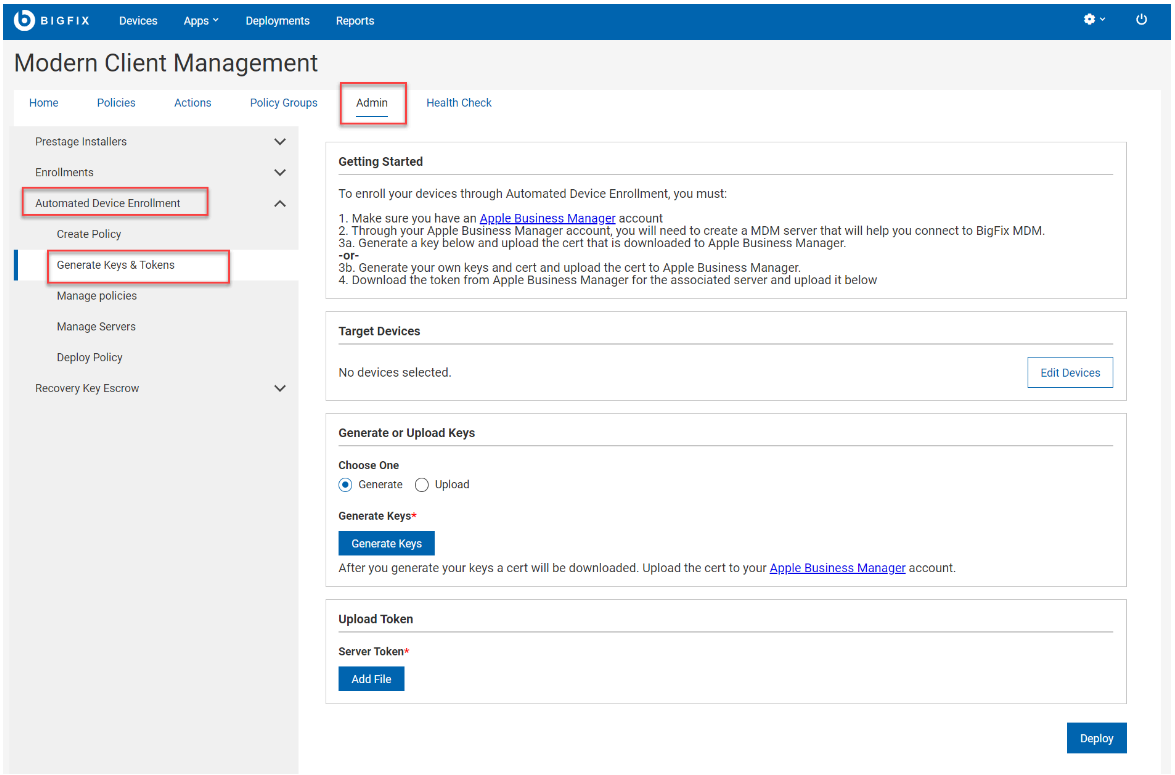
Next steps: Upload the generated `.pem` file to define the server in Apple Business Manager.

Upload MDM server token

Through WebUI, you need to upload the server token (`.p7m`) obtained from Apple Business Manager to establish the communication and enroll Apple devices by Automated Device Enrollment.

To create the public/private key for the MDM server that you want to define in Apple Business Manager:

1. Log in to BigFix WebUI as a Master Operator.
2. From the WebUI main page, click **Apps > MCM**.
3. On the Modern Client Management page, click **Admin > Automated Device Enrollment > Generate Keys & Tokens**. The following page appears:



Getting Started

To enroll your devices through Automated Device Enrollment, you must:

1. Make sure you have an Apple Business Manager account
2. Through your Apple Business Manager account, you will need to create a MDM server that will help you connect to BigFix MDM.
3a. Generate a key below and upload the cert that is downloaded to Apple Business Manager.
-or-
3b. Generate your own keys and cert and upload the cert to Apple Business Manager.
4. Download the token from Apple Business Manager for the associated server and upload it below

Target Devices

No devices selected.

Generate or Upload Keys

Choose One
● Generate ○ Upload

Generate Keys*

After you generate your keys a cert will be downloaded. Upload the cert to your Apple Business Manager account.

Upload Token

Server Token*

4. Under **Target Device**, click **Edit Devices** and select the MDM server that you want to define in Apple Business Manager.

5. Under **Upload Token**, click **Add File**, browse through the MDM server token `.p7m` created via Apple Business Manager.
6. Click **Deploy**.

The connection gets established between the target MDM server and Apple Business Manager. This MDM server acts as the DEP server in which devices can be enrolled automatically.

Next step: Assign devices in ABM

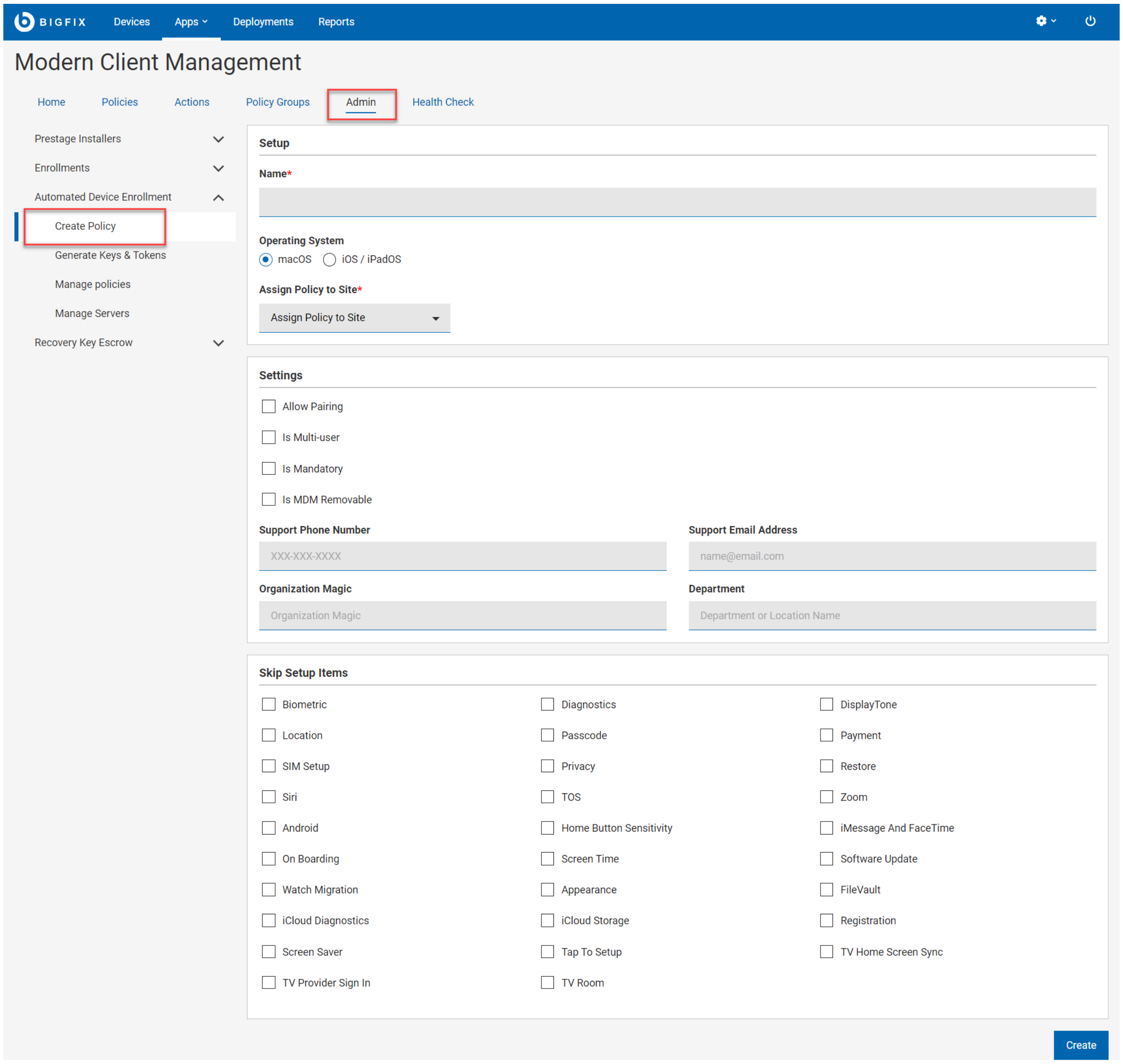
Create Automated Device Enrollment Policy

Learn how to create default policy for DEP enrollments.

Create the required policies that you want to configure for automated device enrollment. See Manage policies *(on page 267)* for detailed information on different types of policies and the steps to create them.

To create automated device enrollment policy:

1. Log in to BigFix WebUI as a Master Operator.
2. From the WebUI main page, click **Apps > MCM**.
3. On the Modern Client Management page, click **Admin > Automated Device Enrollment > Create Policy**. The following page appears that lists all the relevant policies:



Setup

Name*

Operating System

● macOS ○ iOS / iPadOS

Assign Policy to Site*

Assign Policy to Site

Settings

□ Allow Pairing

□ Is Multi-user

□ Is Mandatory

□ Is MDM Removable

Support Phone Number: XXX-XXX-XXXX

Support Email Address: name@email.com

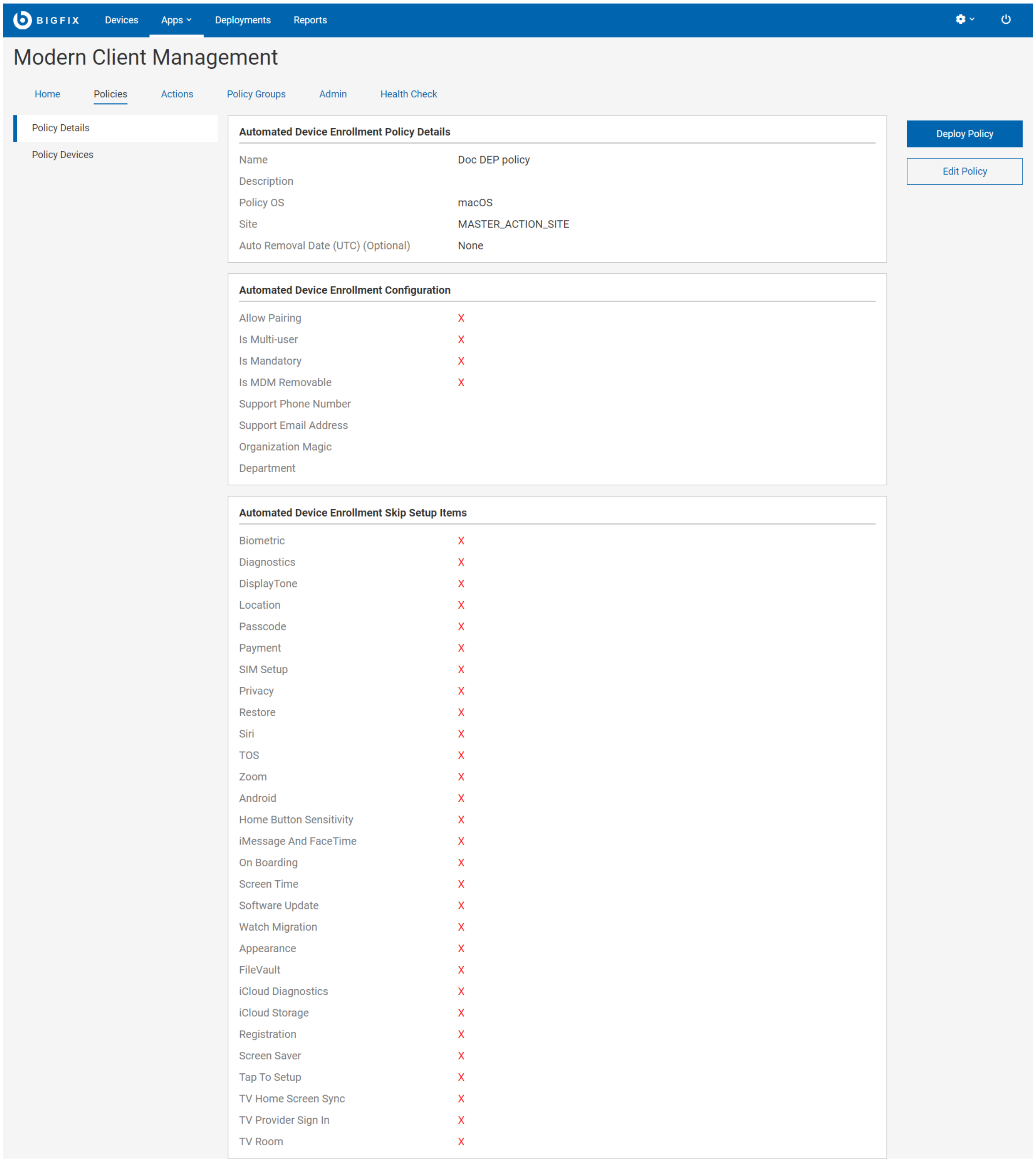
Organization Magic: Organization Magic

Department: Department or Location Name

Skip Setup Items

□ Biometric	□ Diagnostics	□ DisplayTone
□ Location	□ Passcode	□ Payment
□ SIM Setup	□ Privacy	□ Restore
□ Siri	□ TOS	□ Zoom
□ Android	□ Home Button Sensitivity	□ iMessage And FaceTime
□ On Boarding	□ Screen Time	□ Software Update
□ Watch Migration	□ Appearance	□ FileVault
□ iCloud Diagnostics	□ iCloud Storage	□ Registration
□ Screen Saver	□ Tap To Setup	□ TV Home Screen Sync
□ TV Provider Sign In	□ TV Room	

4. Enter the required details and select appropriate check boxes to create a policy.
   Note: For more details about profile properties and their values, see https://developer.apple.com/documentation/devicemanagement/profile. BigFix MCM supports only a subset of the profile properties listed on this page.
5. Click **Save**. The configured policy is saved.



Modern Client Management

Automated Device Enrollment Policy Details

Name	Doc DEP policy
Description	
Policy OS	macOS
Site	MASTER_ACTION_SITE
Auto Removal Date (UTC) (Optional)	None

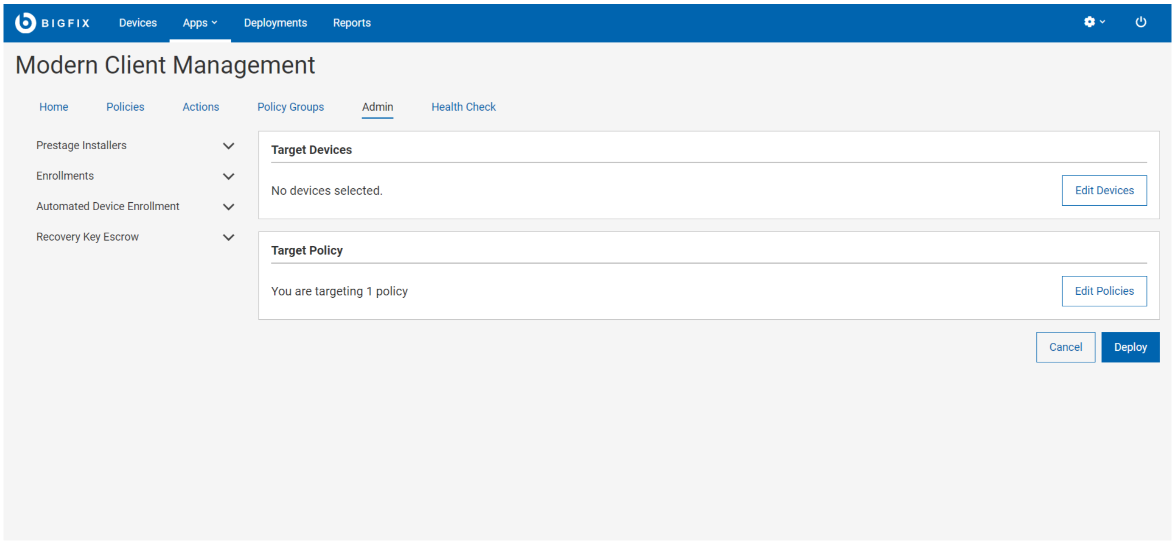
Automated Device Enrollment Configuration

Allow Pairing	X
Is Multi-user	X
Is Mandatory	X
Is MDM Removable	X
Support Phone Number	
Support Email Address	
Organization Magic	
Department	

Automated Device Enrollment Skip Setup Items

Biometric	X
Diagnostics	X
DisplayTone	X
Location	X
Passcode	X
Payment	X
SIM Setup	X
Privacy	X
Restore	X
Siri	X
TOS	X
Zoom	X
Android	X
Home Button Sensitivity	X
iMessage And FaceTime	X
On Boarding	X
Screen Time	X
Software Update	X
Watch Migration	X
Appearance	X
FileVault	X
iCloud Diagnostics	X
iCloud Storage	X
Registration	X
Screen Saver	X
Tap To Setup	X
TV Home Screen Sync	X
TV Provider Sign In	X
TV Room	X

6. Click **Deploy Policy**.
7. On the Deploy Policy page, to select the target devices, click **Edit Devices**. From the next pop up window select the devices in which you want to deploy the policy.



Target Devices

No devices selected.

Target Policy

You are targeting 1 policy

8. Review the selected policy and the devices and click **Deploy**.

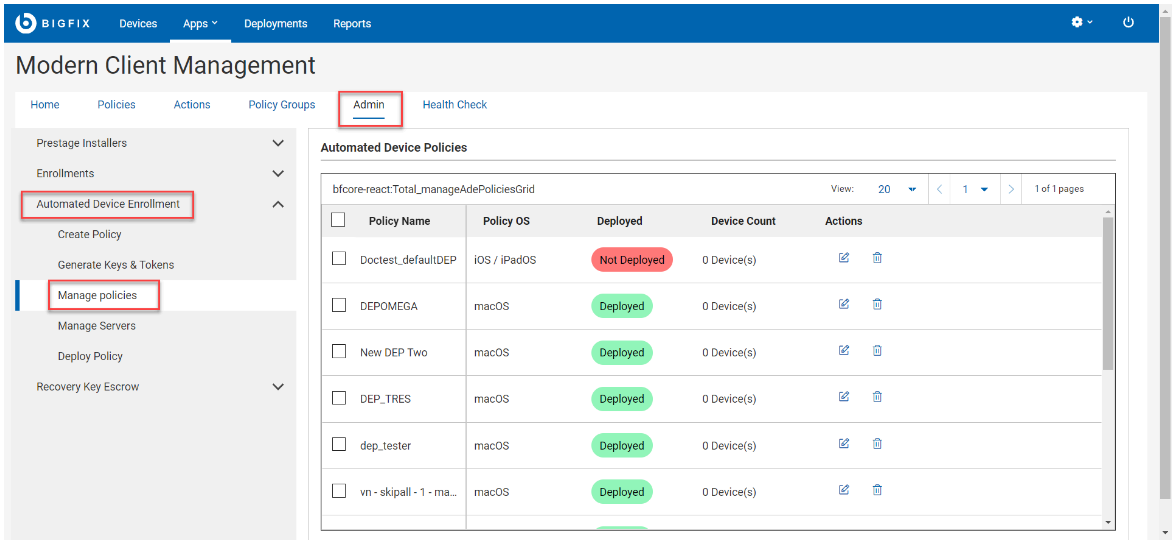
> **Note:** Only the most recently deployed DEP policy on the MDM server takes effect, replacing any policy deployed earlier. All devices going through DEP enrollment get the same profile and options, assuming the profile has been enabled for the OS of the enrolling device.

Manage Automated Device Enrollment Policies

Learn how to manage DEP policies.

To manage DEP policies:

1. Log in to BigFix WebUI as a Master Operator.
2. From the WebUI main page, click **Apps > MCM**.
3. On the Modern Client Management page, click **Admin > Automated Device Enrollment > Manage Policies**. The following page appears that lists all the relevant policies:



Automated Device Policies

bfcore-react:Total_manageAdePoliciesGrid View: 20 1 1 of 1 pages

□	Policy Name	Policy OS	Deployed	Device Count	Actions
□	Doctest_defaultDEP	iOS / iPadOS	Not Deployed	0 Device(s)	
□	DEPOMEGA	macOS	Deployed	0 Device(s)	
□	New DEP Two	macOS	Deployed	0 Device(s)	
□	DEP_TRES	macOS	Deployed	0 Device(s)	
□	dep_tester	macOS	Deployed	0 Device(s)	
□	vn - skipall - 1 - ma...	macOS	Deployed	0 Device(s)	

4. Manage policies:
    - To refine the resultant list of policies, select appropriate filters.
    - To edit an existing policy, click the pen icon next to the desired policy, make the changes, and click **Save**.
    - To delete a policy, click the trash icon next to the desired policy, and click **Delete** to confirm.
    - To create a new policy *(on page 253)*, click **Create Policy**.
    - To deploy a policy to the DEP server, select a policy from the list and click **Deploy**.

Manage devices

After the devices are enrolled to MDM successfully, the devices report to BigFix WebUI, and they are listed on the **Devices** page. Use the MCM application in the WebUI to view, manage, and control these MCM and BigFix Mobile devices.

To access the MCM page, from the WebUI main page, select **Apps > MCM**.

Note: A Master Operator can configure access to the MCM application for a user by using WebUI Permission *(on page 182)*. Only users who have access to the MCM application through BigFix WebUI and have the permissions *Can create actions* and *Can see custom content* can create native MCM policies *(on page 267)*.

Full Disk Encryption

With BigFix MCM, you can centrally manage the native full-disk encryption (FDE) technologies from Windows (BitLocker) and macOS (FileVault2) to secure data at rest.

For more information on Full Disk encryption feature in BigFix MCM, see Full Disk Encryption.

Workflow to configure and deploy Full Disk Encryption

1. Set up the BES Server Plugin Service (Fixlet 708 in BES Support)
2. Configure Recovery Key Escrow *(on page 259)*
3. Create Disk Encryption policy *(on page 288)*
4. Deploy FDE Policy *(on page 262)*

Health Check

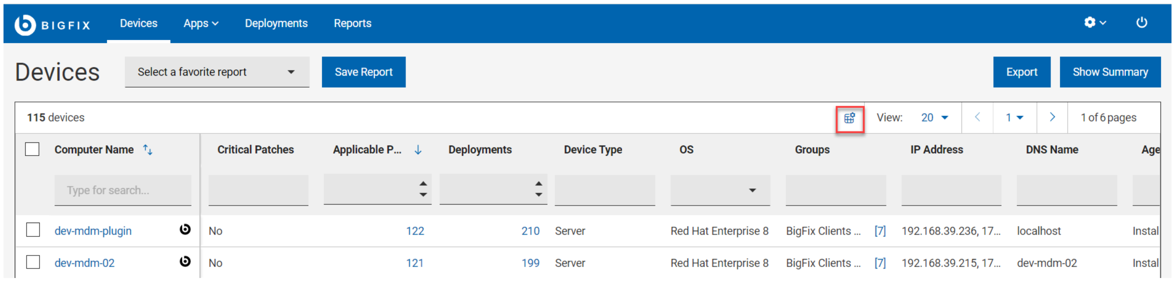
After configuring Full Disk Encryption, to view the MDM Full Disk Encryption Status (on page 189), on the Modern Client Management page click **Health Check.**

Building a saved report for encryption status

Using the properties from the "Full Disk Encryption Status" analysis, you can enable columns that allow filtering to look for devices that are not encrypted, missing recovery key, and so on.

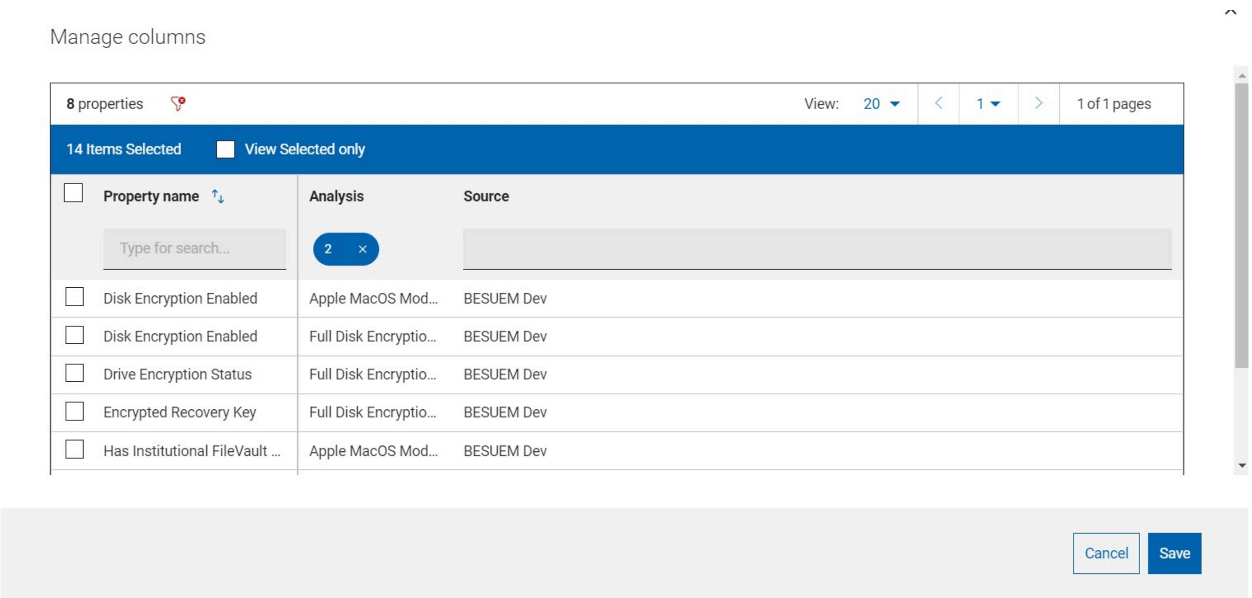
To include the Full Disk Encryption specific device properties in the device data grid:

1. From the device list *(on page 23)*, click manage column icon.



	Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS	Groups	IP Address	DNS Name	Age
□	dev-mdm-plugin	No	122	210	Server	Red Hat Enterprise 8	BigFix Clients ... [7]	192.168.39.236, 17...	localhost	Instal
□	dev-mdm-02	No	121	199	Server	Red Hat Enterprise 8	BigFix Clients ... [7]	192.168.39.215, 17...	dev-mdm-02	Instal

2. In the Manage columns window, search by string in the Property name field or in the Analysis column, select Full Disk Encryption.


Manage columns

8 properties

View: 20 ▾ | < | 1 ▾ | > | 1 of 1 pages

14 Items Selected □ View Selected only

□	Property name	Analysis	Source
	Type for search...	2 ×	
□	Disk Encryption Enabled	Apple MacOS Mod...	BESUEM Dev
□	Disk Encryption Enabled	Full Disk Encryptio...	BESUEM Dev
□	Drive Encryption Status	Full Disk Encryptio...	BESUEM Dev
□	Encrypted Recovery Key	Full Disk Encryptio...	BESUEM Dev
□	Has Institutional FileVault ...	Apple MacOS Mod...	BESUEM Dev

Property	Description
Encrypted	If the endpoint is encrypted, shows the encrypted recovery key. **Note:** If the endpoint is encrypted, but if it does not show recovery key, that it might have been target for key regeneration.
Drive encryption status	Disk Encryption shows overall encryption status for system drive.
Disk encryption status	Drive encryption shows for Windows per drive encryption status and method.
TPM status	TPM status shows for Windows whether the TPM has been detected and if Ready, values here are "Ready" "Not Ready" "Not Detected"

Note:

- After selecting properties and configuring the datagrid the way you want it to look, you can save the view in a Report by clicking on "Save Report *(on page 28)*" in the Devices Page.
- After filling in a Report Name and Report Description and hitting save, the view will be available under "Reports (on page 20)" in the Global Navigation bar for later viewing and reference.

Configure Recovery Key Escrow

Key escrow is a method of storing important cryptographic keys. By using key escrow, organizations can ensure that in the case of crisis, such as security breach, lost or forgotten keys, natural disaster, or otherwise, their critical keys are safe and can be recovered.

Some of the scenarios where recovery key escrow becomes necessary are as follows:

- The desk-side support person moving a disk from a broken laptop to a new laptop.
- A laptop being sent to legal for safe keeping after an employee leaves the company.
- Laptop recycle.

Recovery Key Escrow Configuration involves the following steps:

1. Creating certificates – Create a certificate and key pair for encrypting the recovery key through WebUI MDM app. This certificate is used in Windows actions and in macOS escrow payload. The key is placed in BES server plugin folder for decrypting.
2. Setting up Vault – Specify an existing Vault server (URL, access keys), or you can also deploy Vault with self-signed certificates. You can access the Vault directory to get the unseal keys and access keys that were generated, and configure Vault settings in WebUI.
3. Setting up Escrow plugin – Trigger the action to deploy the plugin, and then configure with details of the key and Vault details, so that the private key is stored in the 'Applications' directory of the BES server.
4. Manual device task to escrow recovery key – If recovery key is missing or out of date, you can retrieve it by regenerating it.

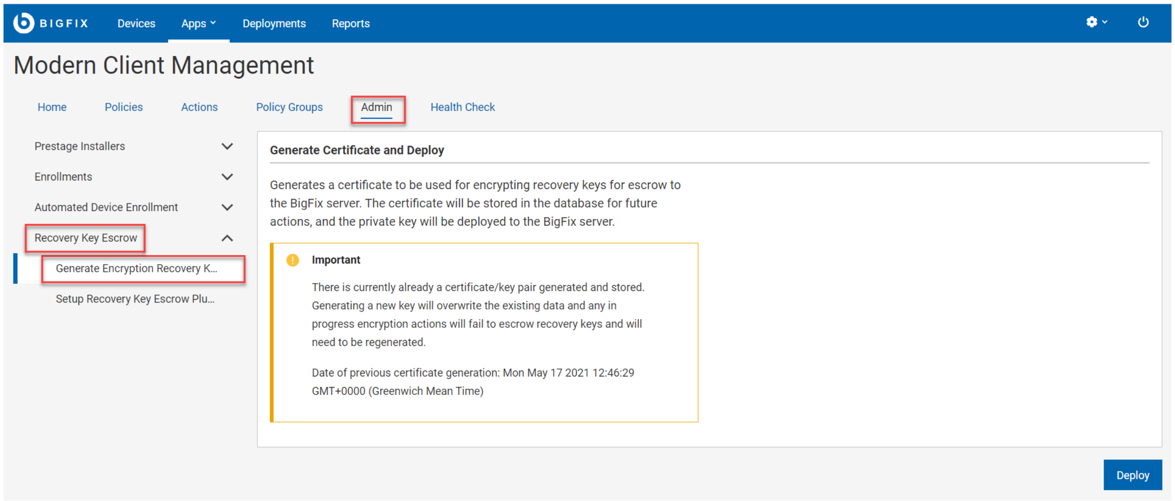
Note:

- It involves user interaction to continue with setup, enter password at start up to start encryption process, or to start OS after the forced restart.
- On macOS, encrypting secondary drives or enforcement of encryption of removable drives is not supported.

Generate Encryption Recovery Key Escrow Certificate

To generate the certificate and key pair complete the following steps:

1. From the WebUI main page, click **Apps** **> MCM > Admin**.
2. On the **Admin** page, expand **Recovery Key Escrow** and click **Generate Encryption Recovery Key Escrow Certificate**.
3. In the next screen, click **Deploy**



Generate Certificate and Deploy

Generates a certificate to be used for encrypting recovery keys for escrow to the BigFix server. The certificate will be stored in the database for future actions, and the private key will be deployed to the BigFix server.

Important

There is currently already a certificate/key pair generated and stored. Generating a new key will overwrite the existing data and any in progress encryption actions will fail to escrow recovery keys and will need to be regenerated.

Date of previous certificate generation: Mon May 17 2021 12:46:29 GMT+0000 (Greenwich Mean Time)

.

Now, the certificate and key pair to be used to create the recovery keys are generated, stored in the WebUI database for future actions. The key will be used when deploying Windows or macOS Encryption Policies.

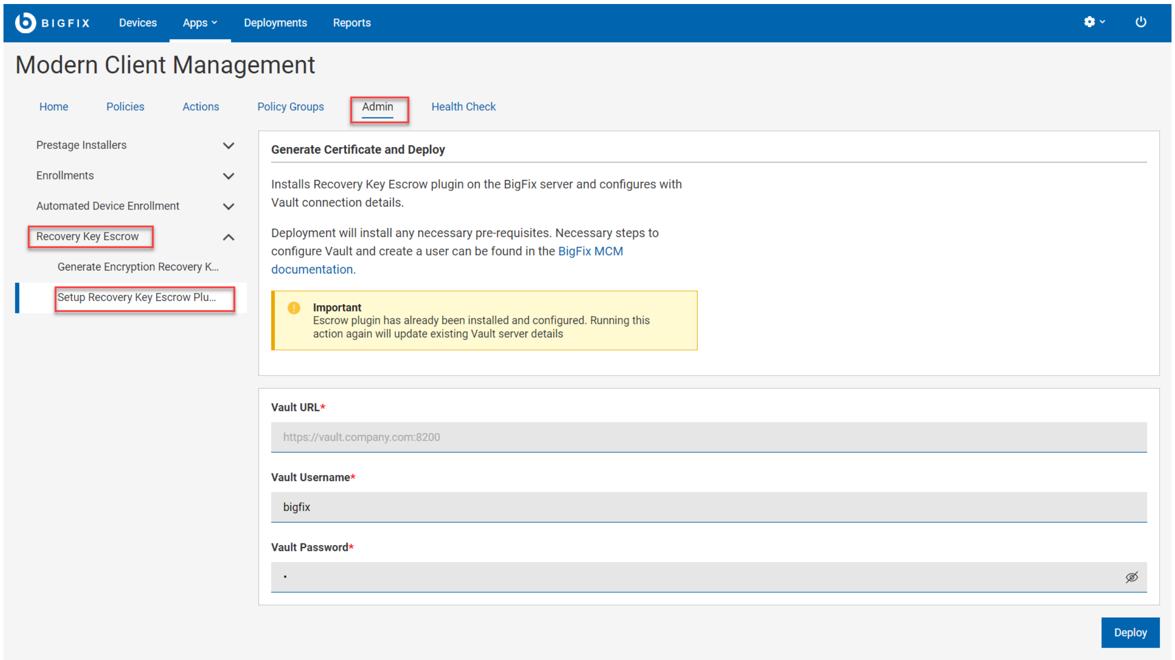
Important: You can also regenerate the certificate/key pair from this page. However, generating a new set of keys will have adverse effects. Any in progress encryption actions will fail to escrow recovery key as they will be encrypting using outdated certificate. To avoid that, it is recommended to re-deploy MacOS full disk encryption policies, as that will update the escrow certificate stored on the devices for a future update or regeneration of the recovery key.

Setup Recovery Key Escrow Plugin

Ensure the BES Server Plugin Service is already installed.

To install the Encryption plugin on the BES server, complete the following steps.

1. From the WebUI main page, click **Apps > MCM**.
2. On the Modern Client Management page, click **Admin**.
3. From the following screen select **Recovery Key Escrow > Setup Recovery Key Escrow Plugin**.



Generate Certificate and Deploy

Installs Recovery Key Escrow plugin on the BigFix server and configures with Vault connection details.

Deployment will install any necessary pre-requisites. Necessary steps to configure Vault and create a user can be found in the BigFix MCM documentation.

Important
Escrow plugin has already been installed and configured. Running this action again will update existing Vault server details

Vault URL*
https://vault.company.com:8200

Vault Username*
bigfix

Vault Password*
•

4. Enter **Vault URL**, **Vault Username** and **Vault Password** that has write access to the 'bigfix' Secret Engineas set up previously.
5. Click **Deploy**.

By default, the Recovery Key Escrow Plugin tries to talk with Vault (https://www.hashicorp.com/products/vault) as it’s secure secrets repository. Vault must be configured separately for Recovery Keys storage and retrieval to work properly. For more information, see Set up Vault.

Once configured, users that have specific access to Vault directly can obtain recovery keys for all keys that have been escrowed properly.

Note: User access to Vault is separate from BigFix users and operators and needs to be configured separately.

To learn how to create a full disk encryption policy, see Disk Encryption Policy (on page 288).

Deploy FDE Policy

To deploy the created FDE policy do the following steps.

1. From the Devices page, select one or more devices and click **Deploy > MDM Policy**.
2. On the Deploy Policy page, select the options as needed. If you select the option Restart Devices immediately, the endpoint gets restarted regardless of the end user restarts or not.
3. Windows options: For Windows, show notification is the default. If you do not select Show Notification, the endpoint restarts immediately after the action runs.

Regenerate Encryption Recovery Key

Learn how to regenerate the encryption recovery key for Windows or macOS devices.

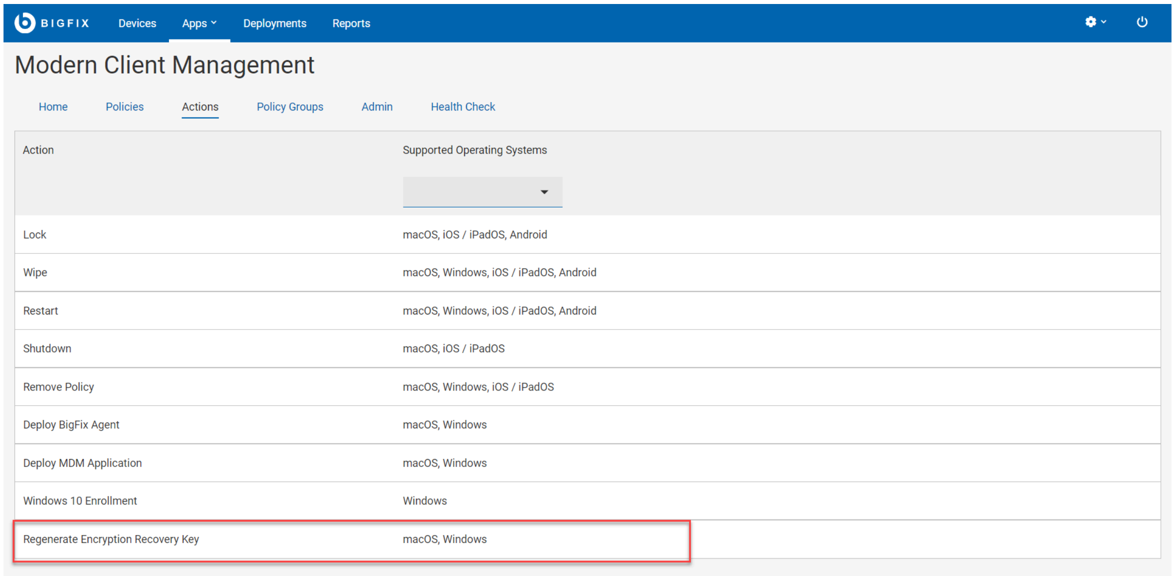
Recovery key regeneration requires the BigFix agent to perform the action and can not be done through just MDM. On Mac devices, the device user is prompted by a utility to enter the username and password of a privileged user to regenerate recovery key.

On Mac devices, the end user will be prompted by a small utility to enter the username and password of a privileged user in order for regeneration of the recovery key to occur.

To retrieve escrowed recovery keys, operator or support person must log in directly to the Vault server interface (if you have set up Vault with the provided Fixlet, you can use the read user that was created). The 'bigfix' secret engine contains the recovery keys. Recovery keys are stored with identifiers based on the BigFix computer ID, computer name and last logged in user and can be searched in the Vault interface. The name of the entry in Vault has these values as of the time the recovery key was escrowed.

To regenerate full disk encryption recovery key, complete these steps.

1. From WebUI, click **Apps > MCM**
2. On the Modern Client Management page, click **Action**
3. On the available list of actions, click **Regenerate Encryption Recovery Key**.



Action	Supported Operating Systems
Lock	macOS, iOS / iPadOS, Android
Wipe	macOS, Windows, iOS / iPadOS, Android
Restart	macOS, Windows, iOS / iPadOS, Android
Shutdown	macOS, iOS / iPadOS
Remove Policy	macOS, Windows, iOS / iPadOS
Deploy BigFix Agent	macOS, Windows
Deploy MDM Application	macOS, Windows
Windows 10 Enrollment	Windows
Regenerate Encryption Recovery Key	macOS, Windows

4. On the following page, click **Edit Devices** to select the target Windows or macOS devices.
5. Review your selection and click **Deploy**.

Deploy MCM policies

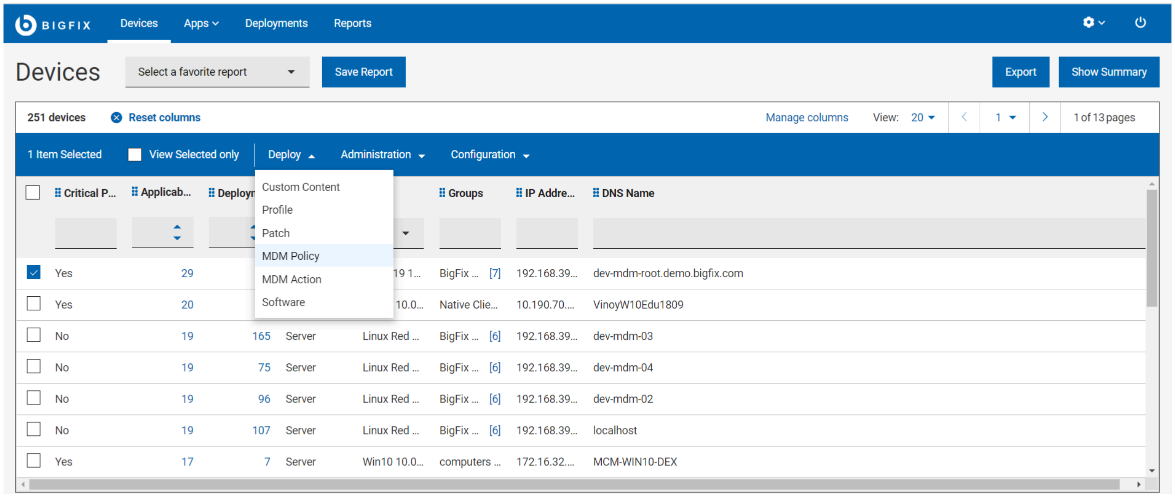
Deploying MCM policies enables administrators to configure and manage MCM devices.

Note:

- Master Operators can perform all actions. The following notes applies only to users other than Master Operators:
  - Only users having access to the MDM application via BigFix WebUI can deploy MDM policies. Master Operator can configure access permissions through WebUI Permission *(on page 182)* service.
  - Only non-master operators with the permission *Create,Edit, and Delete Non-Custom Policies* can create native MDM policies (Kernel Extensions, Passcode Policy, Certificate policies, Restrictions policies, Full Disk Access).
  - Only users with the permission *Can Create Actions* in the BigFix Console can deploy MDM policies. These users also need permissions in the BigFix custom sites associated with view/edit/deploy the policies unless the policies were created in the master action site. For more information about permissions, see MDM Permissions *(on page 182)*.
  - You can deploy an MDM policy only to MDM managed endpoints. Deploying MDM policies to device groups with non-MDM devices will fail.
  - WebUI will prevent users generating actions that do not apply to the right device type. For example, WebUI prevents deploying MDM policies to native BigFix agent devices or cloud devices.
  - If you attempt to deploy an MDM policy on a correlated device with both a native BigFix representation and an MDM representation, it will result in deploying the MDM policy only to the MDM device.

Follow these steps to deploy MDM policies:

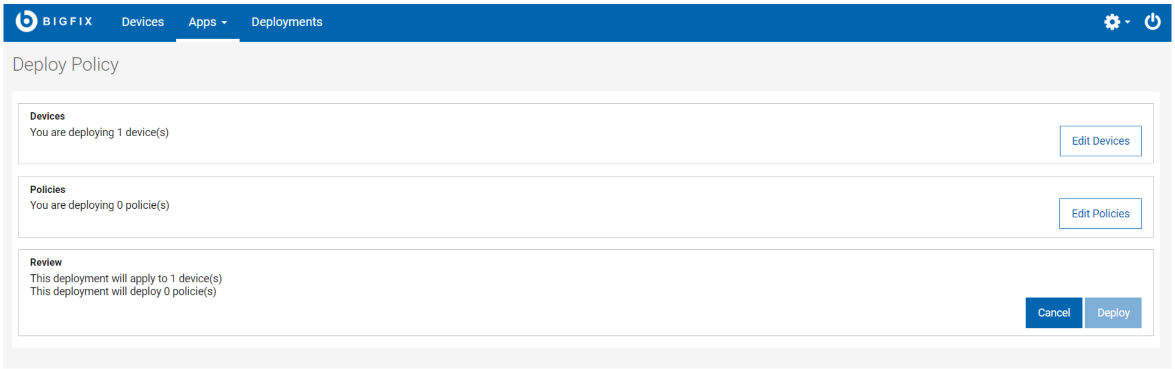
1. Go to the **Devices** list.
2. Select one or more devices to which you want to deploy the MDM policies.
3. Click **Deploy** button.
4. Select **Deploy MDM Policy** from the drop down list.



☐	Critical P...	Applicab...	Deploym...			Groups		IP Addre...	DNS Name
☑	Yes	29			19 1...	BigFix ...	[7]	192.168.39...	dev-mdm-root.demo.bigfix.com
☐	Yes	20			10.0...	Native Clie...		10.190.70....	VinoyW10Edu1809
☐	No	19	165	Server	Linux Red ...	BigFix ...	[6]	192.168.39...	dev-mdm-03
☐	No	19	75	Server	Linux Red ...	BigFix ...	[6]	192.168.39...	dev-mdm-04
☐	No	19	96	Server	Linux Red ...	BigFix ...	[6]	192.168.39...	dev-mdm-02
☐	No	19	107	Server	Linux Red ...	BigFix ...	[6]	192.168.39...	localhost
☐	Yes	17	7	Server	Win10 10.0...	computers ...		172.16.32....	MCM-WIN10-DEX

5. Click **Edit Policies** to select the policy you want to deploy.
6. Click **Deploy** to deploy the MDM policy to the selected devices.

> **Note:** Non-master operators need visibility on the sites where policies were created to deploy them. If non-master operators do not see the right MDM policies in this deployment workflow, they must check their BigFix site permissions.



Deploy Policy

Devices
You are deploying 1 device(s)

Policies
You are deploying 0 policie(s)

Review
This deployment will apply to 1 device(s)
This deployment will deploy 0 policie(s)

Related information

Manage policies *(on page 267)*

Deploy BigFix Agent

By deploying the BigFix agent to devices, BigFix administrators can use all the capabilities of BigFix on those devices.

> **Important:** BigFix agent can be installed only on macOS and Windows devices. BigFix agent cannot be installed on IOS, iPadOS, or Android devices. Additionally, macOS and Windows BigFix Agent installation packages need to be prestaged on the MDM server before the Deploy BigFix Agent action to work. To learn how to prestage, see Prestage macOS BigFix installer *(on page 235)* and Prestage Windows BigFix Installer *(on page 236)*.

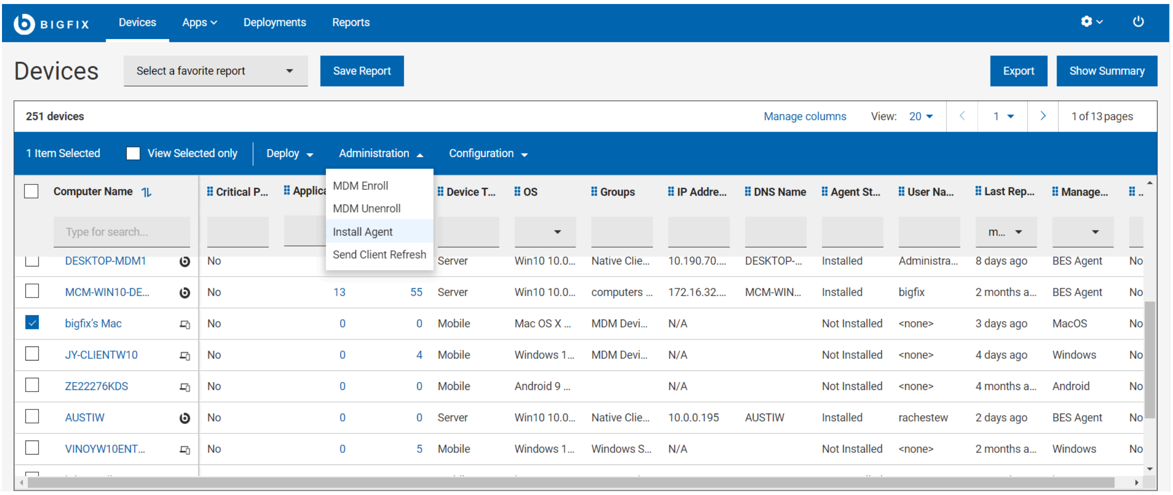
- Master operators can deploy BigFix agent on an MCM device
- Non-Master Operators (NMO) who have the *Can use WebUI*, *Can Create Actions*, and *Custom Content* permissions can deploy BigFix agent on MCM devices.

To deploy the BigFix agent, follow these steps:

1. Select at least one macOS or Windows device that is managed only by MCM. (From the device list, users can filter devices that do not have BigFix agent installed by using the **Agent Status > No** filter.

   Note: The devices that are managed only by MCM are indicated by the MCM symbol SAMPLE_WIN 🖳 next to it.

2. From the blue action bar, click **Administration > Install Agent**.

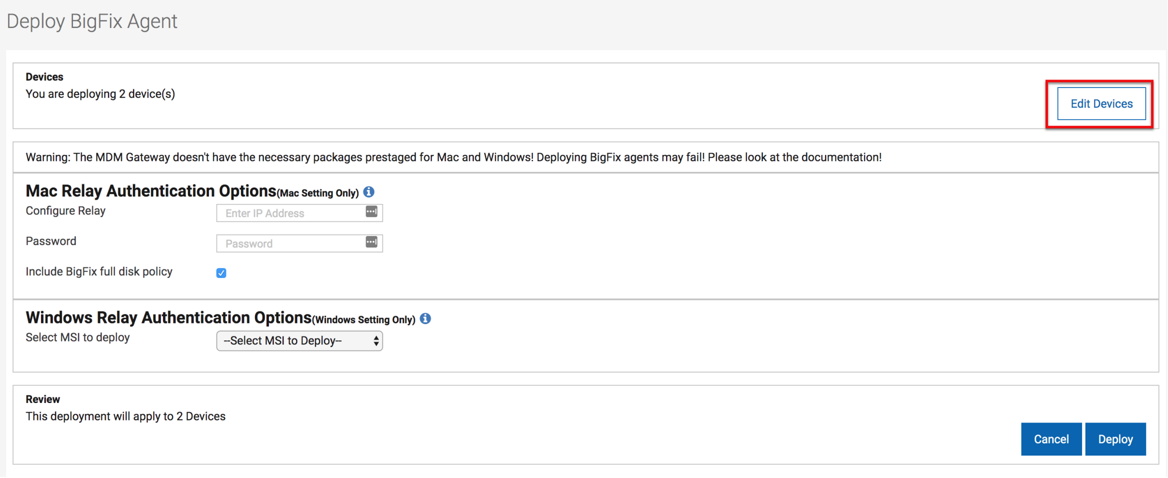


Devices

251 devices

☐	Computer Name	Critical P...	Applica...		Device T...	OS	Groups	IP Addre...	DNS Name	Agent St...	User Na...	Last Rep...	Manage...	...
☐	DESKTOP-MDM1	No			Server	Win10 10.0...	Native Clie...	10.190.70....	DESKTOP-...	Installed	Administra...	8 days ago	BES Agent	No
☐	MCM-WIN10-DE...	No	13	55	Server	Win10 10.0...	computers ...	172.16.32....	MCM-WIN...	Installed	bigfix	2 months a...	BES Agent	No
☑	bigfix's Mac	No	0	0	Mobile	Mac OS X ...	MDM Devi...	N/A		Not Installed	<none>	3 days ago	MacOS	No
☐	JY-CLIENTW10	No	0	4	Mobile	Windows 1...	MDM Devi...	N/A		Not Installed	<none>	4 days ago	Windows	No
☐	ZE22276KDS	No	0	0	Mobile	Android 9 ...		N/A		Not Installed	<none>	4 months a...	Android	No
☐	AUSTIW	No	0	0	Server	Win10 10.0...	Native Clie...	10.0.0.195	AUSTIW	Installed	rachestew	2 days ago	BES Agent	No
☐	VINOYW10ENT...	No	0	5	Mobile	Windows 1...	Windows S...	N/A		Not Installed	<none>	2 months a...	Windows	No

3. To add or remove devices, on the **Deploy BigFix Agent** page, click **Edit Devices**.



Deploy BigFix Agent

Devices
You are deploying 2 device(s)

Warning: The MDM Gateway doesn't have the necessary packages prestaged for Mac and Windows! Deploying BigFix agents may fail! Please look at the documentation!

Mac Relay Authentication Options (Mac Setting Only)
Configure Relay: Enter IP Address
Password: Password
Include BigFix full disk policy ☑

Windows Relay Authentication Options (Windows Setting Only)
Select MSI to deploy: --Select MSI to Deploy--

Review
This deployment will apply to 2 Devices

4. Configure Relay authentication options.
   a. **Mac Relay Authentication Options**: This section is displayed if Mac endpoints are selected.
      - **Configure Relay**: Enter an IP address or a DNS name.
      - **Passphrase**: Enter the passphrase.
      - **Include BigFix full disk policy**: Select this check box to grant full-disk access privileges to BigFix.

b. **Windows Relay Authentication Options**: This section is displayed if Windows endpoints are selected.
   - **Select MSI to deploy**: From this list, select the msi file that you have pre-staged on the MDM server.

5. To deploy the BigFix Agent, click **Deploy**.

Note:

- After the action is complete, both MDM and the BigFix Agent can manage the device.
- The IP address and passphrase that are entered as part of configuring a relay are used only by macOS MDM endpoints. Windows MDM devices must have a prestaged MSI with a relay authorization that is already configured as part of the MSI.
- Deploying the BigFix Agent works only if the installers for BigFix Agents are pre-staged on the MDM server. The BigFix WebUI requires at least one .pkg file for macOS and one .msi file for Windows™ devices. If installation packages are not on the MDM server, users receive a warning that says BigFix Agent actions will fail." The WebUI checks for .msi and .pkg files in the `/var/opt/BESUEM/packages` folder on the MDM server by default to see whether BigFix Agent packages are pre-staged correctly.

Manage policies

You can create and manage policies specific to Windows, Apple (macOS/iOS/iPadOS), and Android devices through BigFix WebUI.

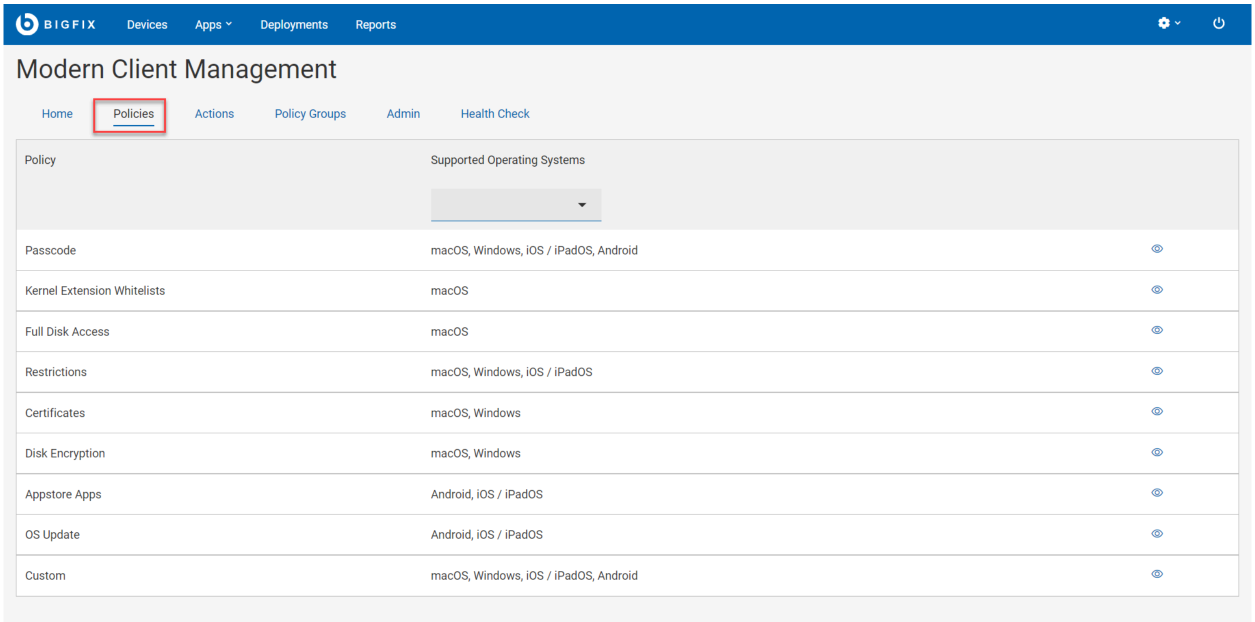
Note:

- Master operators and non-master operators that have the WebUI permission to view the MCM application, and permissions to *Create, Edit, and Delete Non-Custom Policies* can create or manage the following policies:
   - Passcode policy *(on page 275)*
   - Kernel Extension Whitelists *(on page 279)*
   - Full Disk Access *(on page 284)*
   - Restrictions Policy *(on page 284)*
   - Certificates Policy *(on page 287)*

  Users who have the *Create, Edit, and Delete MDM Custom Policies* permission will see an additional option when creating policies to help them create custom policies.
- Only Master Operators can manage DEP policies.
- Non-master operators must have the following permissions to manage MCM and BigFix Mobile policies and actions:
   - Appropriate permissions to create, edit and delete MCM custom and non-custom policies
   - The "custom content" and "can create actions" permissions to deploy MCM actions and policies

- Write permissions to specific custom content sites to have them be an option in the site drop down when associating an MDM policy with a custom site.
- Read permissions or be part of a role that has read permissions to the BESUEM site to get accurate device counts of the policies.

The following are the policies that can be configured using BigFix WebUI:



Modern Client Management

Policy	Supported Operating Systems
Passcode	macOS, Windows, iOS / iPadOS, Android
Kernel Extension Whitelists	macOS
Full Disk Access	macOS
Restrictions	macOS, Windows, iOS / iPadOS
Certificates	macOS, Windows
Disk Encryption	macOS, Windows
Appstore Apps	Android, iOS / iPadOS
OS Update	Android, iOS / iPadOS
Custom	macOS, Windows, iOS / iPadOS, Android

Certain policy types are operating system specific. Each policy type has the applicable operating system logos underneath to notify the users. If you find more than one logo, it represents that the policy can be applied to more than one operating system, specific to those logos.

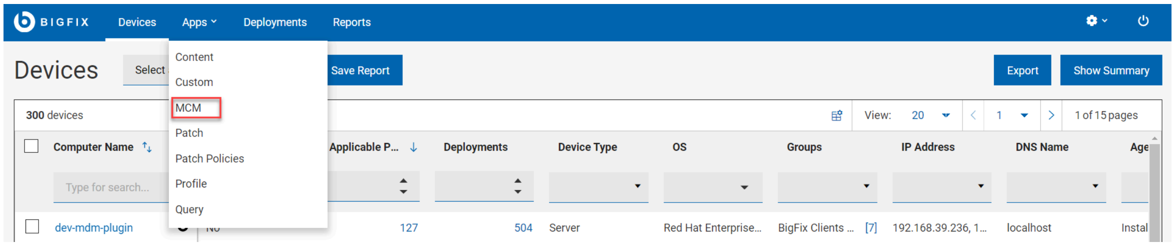
Policy type	Scope	Available for the OS
Passcode policy *(on page 275)*	Create passcode policy for low security requirement	macOS / iOS / iPadOS, , Android
Kernel Extension Whitelists (on page 279)	Create kernel extension whitelist policy to load code dynamically into the macOS Kernel	macOS
Full Disk Access *(on page 284)*	Create policy to encrypt disc space	macOS
Upload Custom Policy *(on page 290)*	Create custom policy	macOS / iOS / iPadOS, , Android

Policy type	Scope	Available for the OS
Restrictions Policy *(on page 284)*	Create restriction policy	macOS / iOS / iPadOS, , Android
Certificates Policy *(on page 287)*	Create policy certificates	macOS,
Disk Encryption Policy *(on page 288)*	Create policy to apply disc encryption	macOS,
Appstore App Policy *(on page 292)*	Create policy to deploy app store apps on MDM endpoints	iOS / iPadOS, Android
OS Update Policy *(on page 294)*	Create policy to manage OS updates	iOS / iPadOS, Android

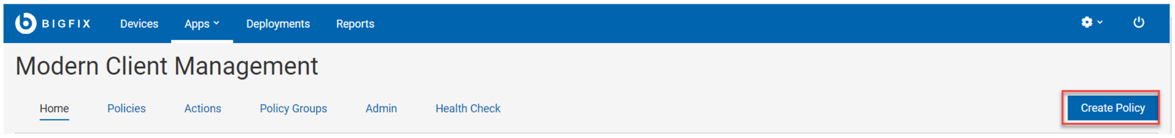
You cannot deploy multiple non-custom polices of same type to the targeted devices. You can deploy multiple custom policies to the targeted devices in one action.

To create a policy, follow these steps:

1. Open the MCM app.



2. Click **Create Policy**.



3. On the page where the policies are listed, select the Supported Operating Systems to display only the policy types that are supported for the selected operating systems. From the filtered list, select the policy type that you want to create.

Policy Groups

Policy Groups enable you to combine policies, apps, and a BigFix Agent in a single group and deploy it onto the MDM server or onto enrolled devices.

You can assign an enrollment type specific to an operating system and deploy onto the MDM server, the policies in the deployed policy group becomes default enrollment policy for those specific devices.

You can assign an enrollment type specific to an operating system and deploy onto eligible devices to override the default enrollment policy.

A policy group can contain the following:

- MDM Policies (Passcode policy *(on page 275)*, Restrictions Policy *(on page 284)*, Certificates Policy *(on page 287)*, Appstore App Policy *(on page 292)*, Kernel Extension Whitelists *(on page 279)*, Full Disk Access *(on page 284)*, Custom policy *(on page 290)*)

  Note: OS Update Policy *(on page 294)* for iOS and Disk Encryption Policy *(on page 288)* for Windows are not supported in policy groups)

- Prestaged applications (on page 229)
- BigFix Agents (on page 265)

Before you Begin: You must be a master operator to perform policy group related tasks such as creating, adding policies and applications, deleting, deploying and so on. As a non-master operator, you can only create policies to be included in the policy group.

Working with Policy Groups

- Create Policy Group *(on page 270)*
- Deploy Policy Group *(on page 273)*
- Associate Policy Group to Smart Group
- Edit a Policy Group *(on page 275)*
- Delete a Policy Group *(on page 275)*

Create Policy Group

To create a policy group:

1. From BigFix WebUI main page, click **Apps > MCM**
2. From the Modern Client Management home page, click **Policy Group.**
3. On the **Policy Groups** page, click **Create Policy Group**.
4. On the **Create Policy Group** page, do the following:
   a. Enter **Policy Group Name** and **Description**
   b. Select OS.
   c. **Assign To Group**. If this policy group is deployed on to MDM servers, assign to group specifies what types of enrolling devices are eligible to get the policies and applications defined within this policy group.

Note: If you do not assign any group here, you can only deploy this policy group to one or more already enrolled devices or BigFix Device Groups. On enrollment, devices do not get the policies and applications from any unassigned policy group.

These are the available Enrollment Groups:

Operating System	**Enrollment Group**
Android	▪ Work profile enrollment: Assigns this policy group to BYOD Android devices. On fresh enrollment, BYOD Android devices receive the policies added in this group. ▪ Fully managed enrollment: Assigns this policy group to fully-managed Android devices. On fresh enrollment, fully-managed Android devices receive the policies added in this group. ▪ Dedicated device enrollment: Assigns this policy group to Dedicated Android devices. On fresh enrollment, Dedicated Android devices receive the policies added in this group. **Note:** For Android, you can provision policies only through the policy groups feature; you cannot provision an individual policy that is not added to any policy group directly onto the MDM server or enrolled devices.
IOS	▪ Over the Air Enrollment: Assigns this policy group to the iOS devices that are enrolled over the air. On fresh enrollment, iOS devices that are enrolled over the air receive the policies added in this group. ▪ User Enrollment (BYOD): Assigns this policy group to BYOD iOS devices. On fresh enrollment, BYOD iOS devices receive the policies added in this group. ▪ Automated Device Enrollment: Assigns this policy group to the iOS devices that are enrolled through Automated Device Enrollment.
iPadOS	▪ Over the Air Enrollment: Deploys the policies in the policy group to all iPadOS devices that are enrolled over the air. On fresh enrollment, iPadOS devices that are enrolled over the air receive the policies added in this group. ▪ User Enrollment (BYOD): Assigns this policy group to BYOD iPadOS devices. On fresh enrollment, BYOD iPadOS devices receive the policies added in this group. ▪ Automated Device Enrollment: Deploys the policies in the policy group to all iPadOS devices that are enrolled through Automated Device Enrollment.

Operating System	**Enrollment Group**
macOS	▪ Over the Air Enrollment: Deploys the policies in the policy group to all macOS devices that are enrolled over the air. On fresh enrollment, macOS devices that are enrolled over the air receive the policies added in this group. ▪ User Enrollment (BYOD): Assigns this policy group to BYOD macOS devices. On fresh enrollment, BYOD macOS devices receive the policies added in this group. ▪ Automated Device Enrollment: Deploys the policies in the policy group to all macOS devices that are enrolled through Automated Device Enrollment.
Windows	▪ Over the Air Enrollment: Deploys the policies in the policy group to all Windows devices that are enrolled over the air. ▪ Bulk Enrollment: Deploys the policies in the policy group to all Windows devices that are enrolled through bulk enrollment. ▪ Autopilot Enrollment: Deploys the policies in the policy group to all Windows devices that are enrolled through Autopilot Enrollment.

5. To add an application or a policy, on the left navigation pane, click the + sign next to the desired item. Then select the desired policies and/or applications. Then click **Save** to save your changes and close the module.
    - **Add Policy**: This option allows users to add policies to their policy group. The policies listed are prefiltered by the selected operating system of the policy group. Select a policy from the list and click OK to add that policy to the policy group. You can add multiple policies of different types. Ensure that you do not add any contradicting policies. In case of certain policies (like passcode and restrictions policies), you can add only one policy of its type in a policy group.

        Note: Before saving the group policy, if you want to remove a policy that you have added, go back to the policy list and deselect the policies you want to remove.

        Important: For Android dedicated devices, ensure to add a policy with kiosk mode setting to the policy group. Otherwise, the dedicated device works as just a fully-managed device.

    - **Add Application** (macOS and Windows only): This option allows users to add prestaged applications to their policy group. The applications listed are prefiltered by the selected operating system of the policy group. Select one or more applications and click OK to add them to the policy group.

> **Important:** Only Mac and Windows Policy Groups can add applications from this page. To add applications on Android, iOS, or iPadOS devices, you must create an Appstore App Policy *(on page 292)* and add it to the policy group via **Add Policy**.

    - **Add BigFix Agent** (MCM only): This lists all the available pre-staged BigFix Agent versions for the selected OS (Windows and macOS only).

6. To save the current selection of policies to your policy group, click the **Save** button in the bottom right to save your policy group.

> **Note:** Ensure you have added at least one policy and one application to your policy group. If you attempt to save a policy group without any application or policy selected, WebUI will prompt you to add at least one policy or application.

Result: A policy group is created and listed in the policy groups. The created policy is displayed in a data grid. You can filter and sort as required to find a specific policy group.

Deploy Policy Group

You can deploy a Policy Group to the MDM server to push the contents of the policy group to eligible devices at the time of enrollment. You can also directly deploy the contents of the policy group onto already enrolled devices.

Default policies - Deploy Policy Group on MDM Server

Policy groups can be deployed on to MDM servers, so that enrolling devices automatically get the contents of the policy group. A policy group can target specific operating system (Android, iOS, iPadOS, macOS, Windows) and specific MDM enrollment type (such as OTA, DEP, Bulk enrollment, Autopilot enrollment, BYOD enrollment, and fully-managed enrollment).

To deploy a policy group to MDM server:

1. From the **Policy Groups** page, select a Policy group. The blue action bar appears.
2. From the **Deploy** dropdown, select **On MDM Server**.
3. If you want to associate Smart Groups to the Policy Group, on the next page, click **Edit Smart Groups** and select the Smart Groups *(on page 221)*.
4. Review the selected Smart Groups and the Policy Group and click **Deploy**.

Result:

- This deploys the policy group onto all the MDM servers in your BigFix environment.
- If you have selected Smart Groups *(on page 221)* at the time of deploying the Policy Group on MDM servers, on enrollment, the contents of the Policy Group deployed on the MDM server are deployed onto eligible devices as default policies as per the specified operating system, enrollment type, and Smart Group definition *(on page 225)*.

Note:

- You can only deploy one policy group at a time to devices or to the MDM server. However, you can run the “Deploy Policy Group to MDM Server” multiple times to deploy policy groups that affect different operating systems and enrollment groups. The latest policy group of a specific operating system and enrollment group combination takes effect on enrollment. For example:
    - If you create a macOS Over The Air Enrollment Policy Group "First Policy Group" and deploy it to MDM servers, newly enrolled OTA macOS devices get the contents of "First Policy Group"

      .
    - If you then create a macOS Over The Air Enrollment Policy Group "Second Policy Group" and deploy it to MDM servers, newly enrolled OTA macOS devices get the contents of "Second Policy Group"
    - You cannot select both “First Policy Group” and "Second Policy Group" at a time to deploy them onto the MDM server. You can only deploy them one at a time.

Update policies on enrolled devices - Policy Group Action

You can update the policies on enrolled MDM devices by deploying a Policy Group to the selected devices or device groups.

Note: When you do not select an enrollment type while creating a Policy Group, you can deploy that policy group onto selected eligible devices or device groups.

To deploy a Policy Group onto selected eligible devices or device groups:

1. From the **Policy Groups** page, select a policy group. The blue action bar appears.
2. Click **Policy Group Action**.
3. In the Deploy Policy Group page, click **Edit Devices** to select the devices or device groups.
4. Review the selected policy and the devices and click **Deploy**.

Result: This deploys the policy group onto all the MDM servers in your environment.

Important: Dedicated Android devices: After the enrollment, when a policy group is deployed, policies in the deployed policy group overwrites previous policies if any.

Smart Group and Policy Group Association

When you associate Smart Groups *(on page 221)* to Policy Group, the policies are deployed based on the criteria defined in the Smart Group (such as primary user membership to the Active Directory group *(on page 222)*, Active Directoryuser attribute rules, and device attributes rules *(on page 223)*) along with the OS type and enrollment type.

Note: You can associate multipe Policy Groups to a Smart Group and vise versa.

Edit a Policy Group

To edit a policy group, click on the name of a policy group. From here, you can change the selected policies and applications, change the name, description and other details. Saving the policy group with changes overwrites the old policy group, so be sure about the changes you want to make. You can click the save button once you are done with your changes to save and go back to the display page. You can also select the cancel button to return without saving your changes.

Delete a Policy Group

To delete a policy group:

1. From the Policy Group page, select a policy group that you want to delete.
2. Use the horizontal scroll bar to move towards the right end of the page and click the delete icon present for the selected policy group.

Note: You can also delete a policy group from the edit policy group page by clicking the red **Delete** button in the bottom right of the page.

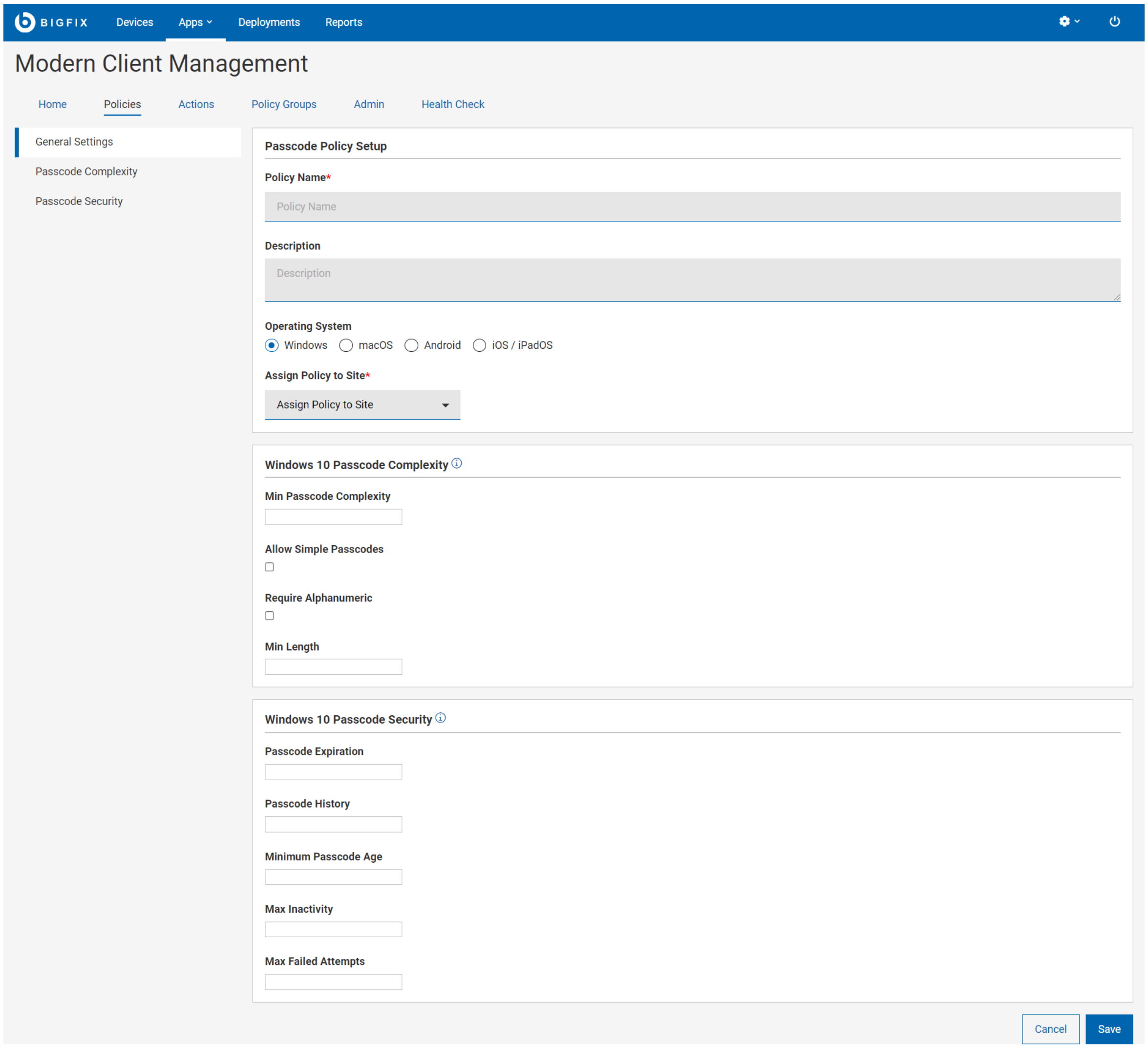
Result: The selected policy group is deleted. The policies deployed previously through this policy group on the devices do not get affected.

Passcode policy

Passcode policies allow BigFix administrators to lock down various password/inactivity settings on Windows, macOS, iOS, iPadOS, and Android MDM devices.

To create a Passcode policy:

1. Log in to WebUI.
2. From the WebUI main page, click **Apps > MCM**.
3. Click **Create Policy**.
4. Select **Passcode** to create a passcode policy.
5. Click **General Settings** from the left navigation bar.



Modern Client Management

Passcode Policy Setup

Policy Name*: Policy Name

Description: Description

Operating System: ● Windows ○ macOS ○ Android ○ iOS / iPadOS

Assign Policy to Site*: Assign Policy to Site

Windows 10 Passcode Complexity ⓘ

Min Passcode Complexity

Allow Simple Passcodes □

Require Alphanumeric □

Min Length

Windows 10 Passcode Security ⓘ

Passcode Expiration

Passcode History

Minimum Passcode Age

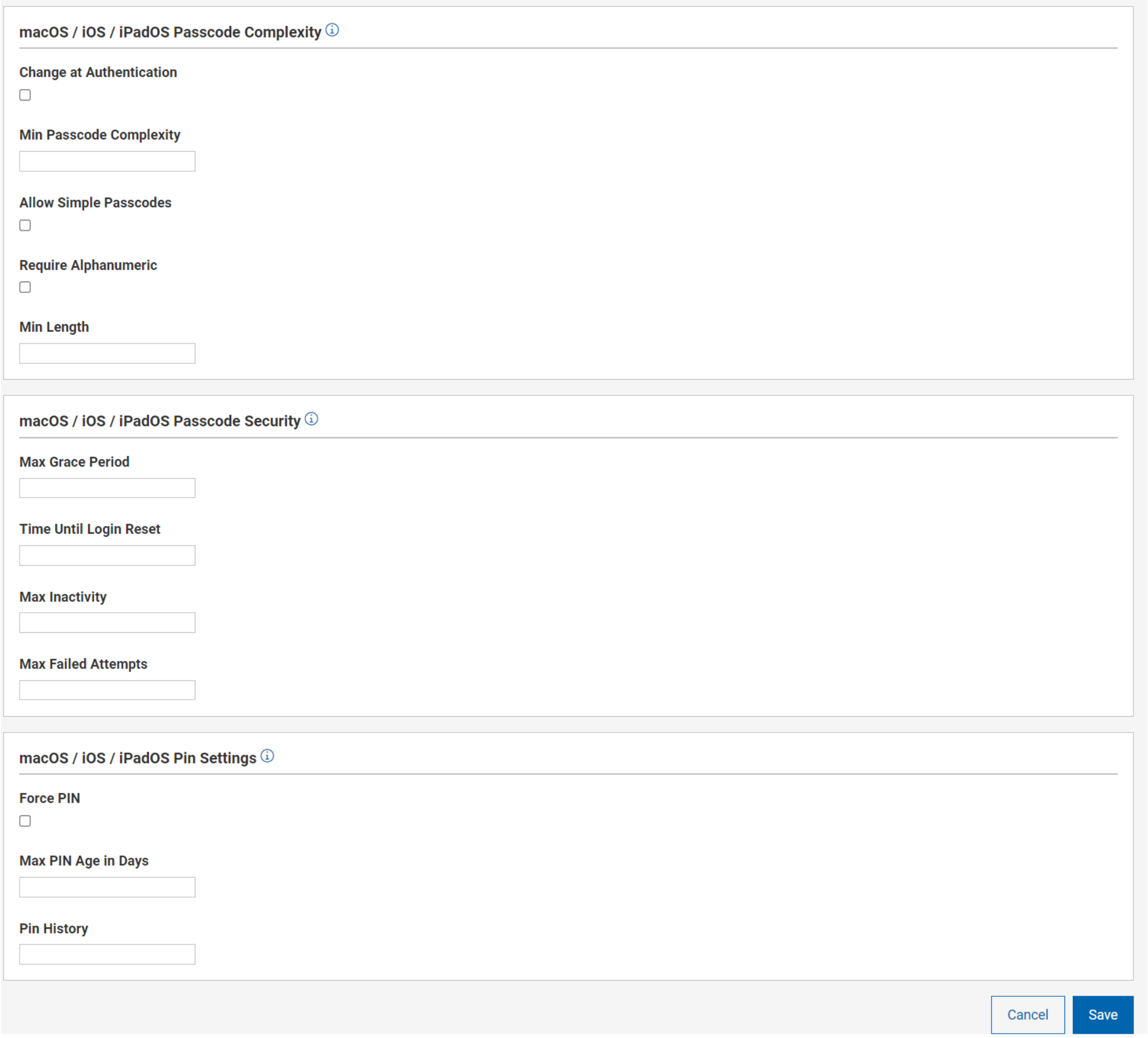
Max Inactivity

Max Failed Attempts

6. Enter the details in **General Settings**.
    a. Enter **Policy Name**.
    b. Enter **Description** of the policy.
    c. Select the operating system. Once you select the operating system, additional fields specific to that operating system appear.
    d. To assign a policy to site, select a site from the **Assign Policy to Site**drop down. Non-master operators can see only those sites in the dropdown to which they have access.
7. Configure the settings specific to the selected OS (Windows, macOS, Android, iOS/iPadOS). Mouse over the information icon ⓘ for description of every setting.
8. Click **Save**. The passcode policy is created and is ready to deploy.

Optional Settings

- macOS and iOS/iPadOS specific settings:



macOS / iOS / iPadOS Passcode Complexity ⓘ

Change at Authentication

□

Min Passcode Complexity

Allow Simple Passcodes

□

Require Alphanumeric

□

Min Length

macOS / iOS / iPadOS Passcode Security ⓘ

Max Grace Period

Time Until Login Reset

Max Inactivity

Max Failed Attempts

macOS / iOS / iPadOS Pin Settings ⓘ

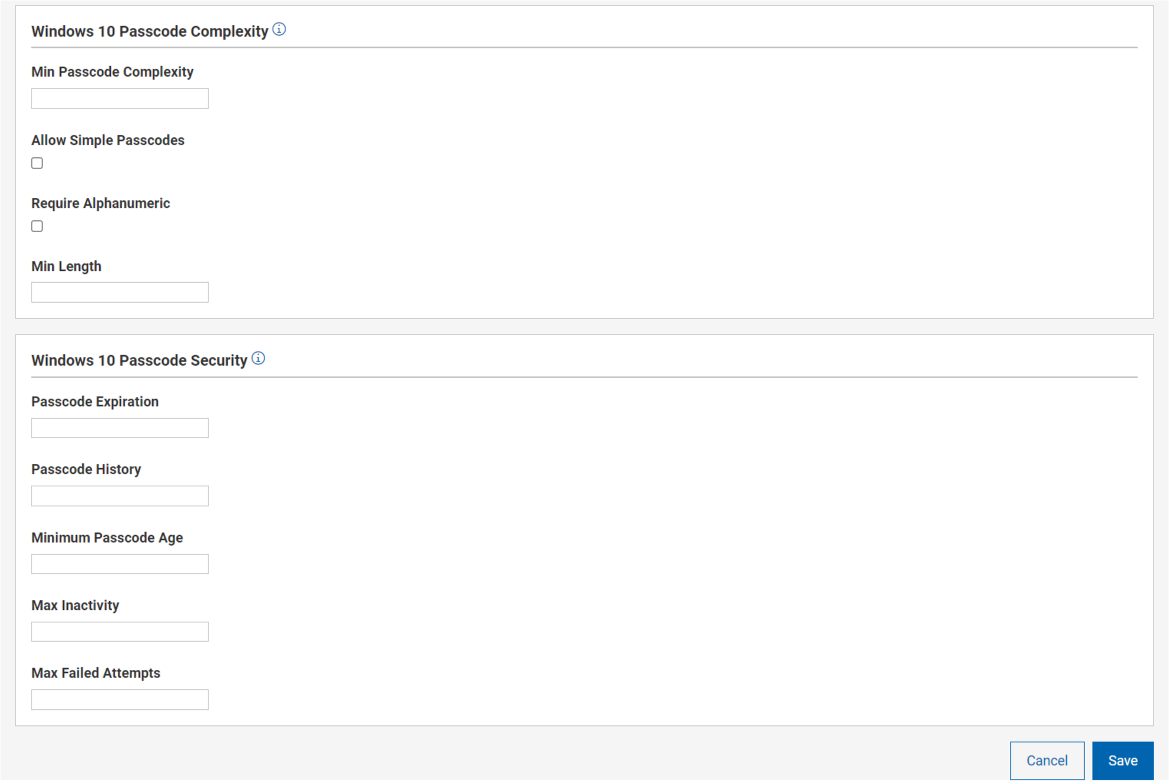
Force PIN

□

Max PIN Age in Days

Pin History

- Windows specific settings:



Windows 10 Passcode Complexity ⓘ

Min Passcode Complexity

Allow Simple Passcodes
□

Require Alphanumeric
□

Min Length

Windows 10 Passcode Security ⓘ

Passcode Expiration

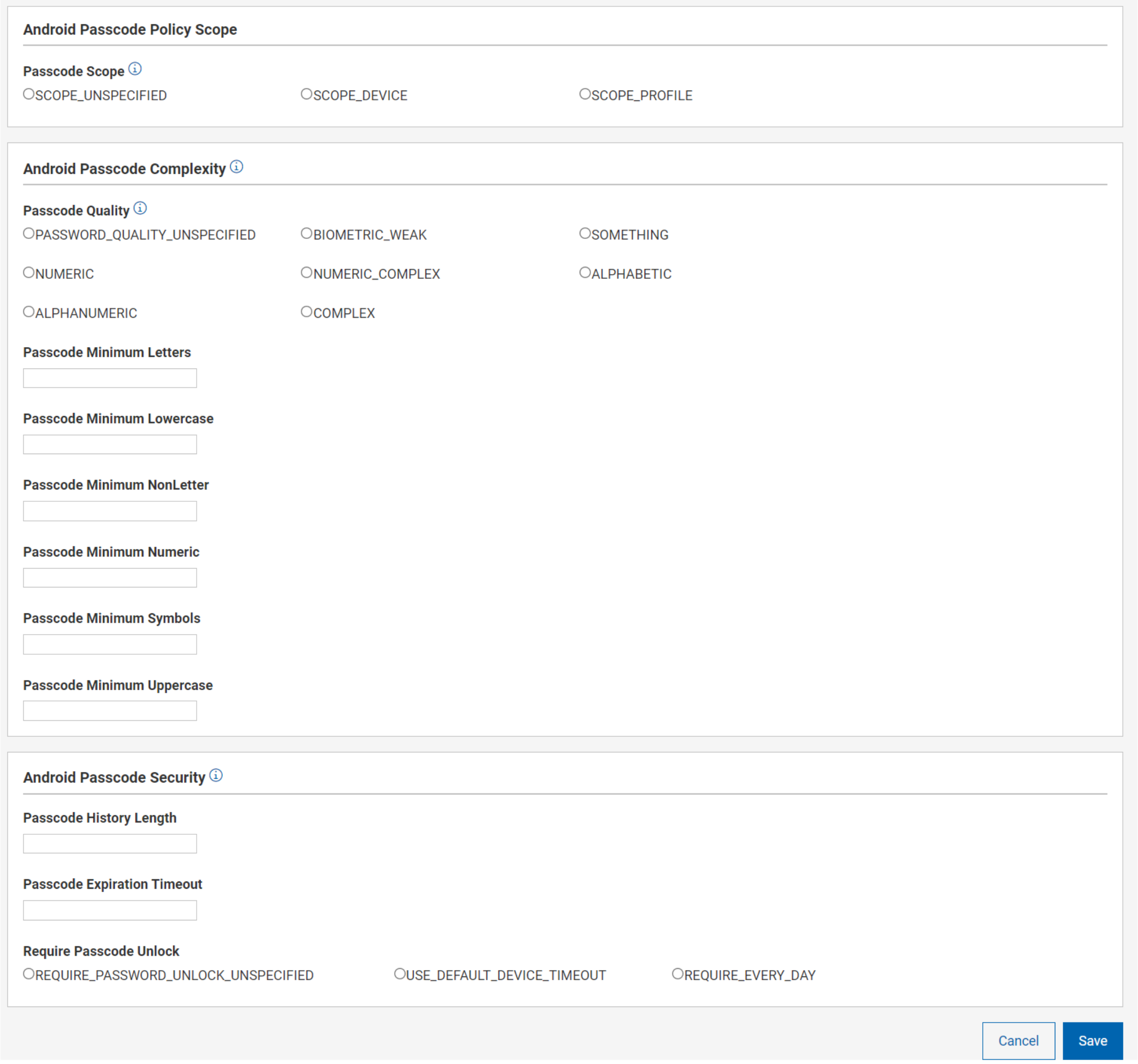
Passcode History

Minimum Passcode Age

Max Inactivity

Max Failed Attempts

- Android specific settings



Android Passcode Policy Scope

Passcode Scope

○SCOPE_UNSPECIFIED ○SCOPE_DEVICE ○SCOPE_PROFILE

Android Passcode Complexity

Passcode Quality

○PASSWORD_QUALITY_UNSPECIFIED ○BIOMETRIC_WEAK ○SOMETHING

○NUMERIC ○NUMERIC_COMPLEX ○ALPHABETIC

○ALPHANUMERIC ○COMPLEX

Passcode Minimum Letters

Passcode Minimum Lowercase

Passcode Minimum NonLetter

Passcode Minimum Numeric

Passcode Minimum Symbols

Passcode Minimum Uppercase

Android Passcode Security

Passcode History Length

Passcode Expiration Timeout

Require Passcode Unlock

○REQUIRE_PASSWORD_UNLOCK_UNSPECIFIED ○USE_DEFAULT_DEVICE_TIMEOUT ○REQUIRE_EVERY_DAY

Kernel Extension Whitelists

Kernel Extensions provide developers the ability to load code dynamically into the macOS Kernel. This allows access to internal kernel interfaces allowing complex apps to function properly.

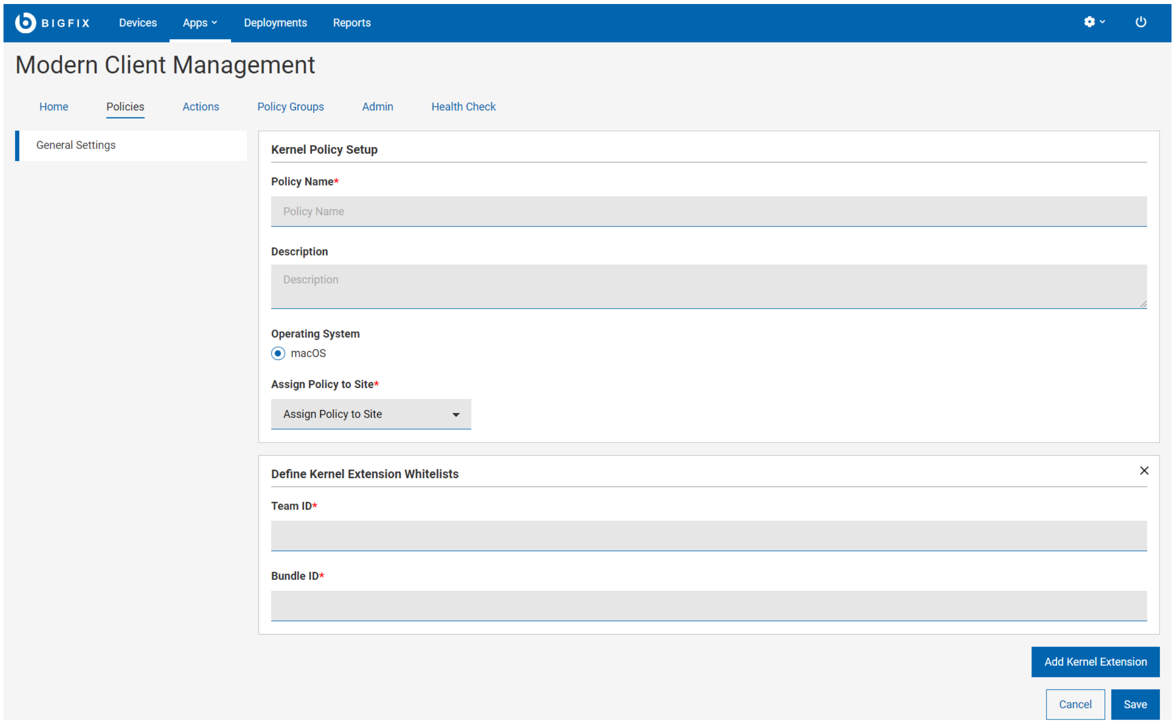
For more information on Kernel Extensions, see Kernel Extension Overview.

If the Kernel Extensions associated with specific applications are whitelisted via macOS MDM, those applications can be installed seamlessly without user intervention or approval.

You can create macOS MDM policies for Kernel Extension Whitelisting of specific applications. You must apply the created Kernel Extension Whitelisting policies before attempting to install those specific applications with kernel extensions.

To create a Kernel Extension Whitelisting policy:

1. Open the MDM app.
2. Click **Create Policy**.
3. From the list of policy types, select **Kernel Extension Whitelists**. The following page appears.



4. Under **Generic Settings**, enter the following details.
   - **Policy Name**: Enter a name for the kernel extension whitelisting policy.
   - **Description**: Enter a description for your policy.
   - **Operating System**: Cannot be changed as this is applicable only to macOS.
   - **Assign Policy to Site**: Select a site from the dropdown menu to assign the policy to the selected site. Non-master operators can see only those sites in the dropdown menu to which they have access.
5. Under **Define Kernel Extension Whitelists**, enter the Team ID and the Bundle ID.
   - **Team ID**: Team ID is unique to a specific development team. It is an alphanumeric string, which is the developer's or vendor's Developer ID for signing KEXTs certificate identifier.
   - **Bundle IDs**: Bundle ID is an alphanumeric string that uniquely identifies an application from a specific vendor. You can specify more than one Bundle ID separated by a comma for any given Team ID.

   To identify Team ID and Bundle IDs using sqlite3:

   a. Install the target product on a machine running a supported macOS version.

   b. Let the user manually approve installation of any extensions that are flagged.

   c. Check the SQLite database with the following commands to get Team ID and Bundle ID:

   ```
   sqlite3 /var/db/SystemPolicyConfiguration/KextPolicy
   SELECT * FROM kext_policy;
   ```

This command will show all the kernel extensions in effect on the machine across all products. You need to locate the ones of interest for whitelisting and create a policy or policies that cover everything you wish to whitelist.

The output might look similar to: `EQHXZ8M8AV|com.google.dfsfuse.filesystems.dfsfuse|1|Google, Inc.|8"`

Where `EQHXZ8M8AV` is the Team ID and `com.google.dfsfuse.filesystems.dfsfuse` is the bundle ID.

Note:

- To whitelist the kernel extension of an application from a specific vendor, you must specify both the Team ID and the Bundle ID.
- Do not add multiple entries with the same Team ID, as only the last one in the list will actually be used. If you have multiple apps to whitelist with the same Team ID, add all the Bundle IDs in one entry separated by commas. For example:

```
Bundle IDs: BundleID1,BundleID2,BundleID3
```

6. **Add Kernel Extension**: If you want to whitelist more than one product from different vendors within a single policy, click Add Extension to add additional Team ID and Bundle IDs to the same policy.
7. Click **Save**. The kernel extension whitelisting is created.

System Extension Whitelists

System extensions allow software like network extensions and endpoint security solutions to extend the functionality of macOS without requiring kernel-level access.

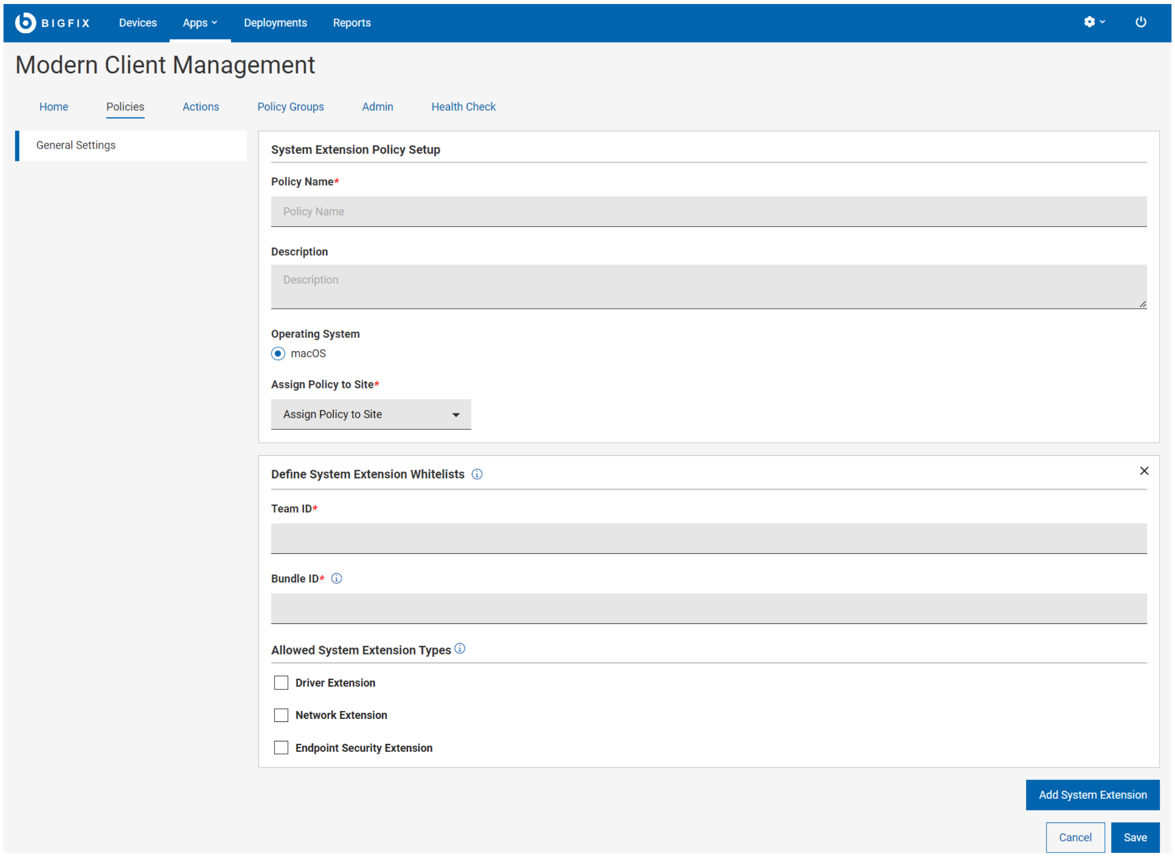
Once installed, the whitelisted extensions become available to all users on the macOS system and can perform tasks that are previously reserved for kernel extensions. Learn more about system extensions.

Note:

- Multiple system extension whitelists can be specified in a single policy itself.
- Multiple system extension whitelists policies can be added to a policy group *(on page 269)* and deployed.

To create a System Extension Whitelist policy:

1. Open the MDM app.
2. Click **Create Policy**.
3. From the list of policy types, select **System Extension Whitelists**. The following page appears.



4. Enter the following details.
    - **Policy Name**: Enter a name for the policy.
    - **Description**: Enter description for your policy.
    - **Operating System**: Cannot be changed as this is applicable only to macOS.
    - **Assign Policy to Site**: Select a site from the dropdown menu to assign the policy to the selected site. Non-master operators can see only those sites in the dropdown menu to which they have access to.
5. Under **Define System Extension Whitelists**, enter the Team ID and the Bundle ID.
    - **Team ID**: Team ID is unique to a specific development team. It is a 10-digit alphanumeric string, which Apple generates and associates with the developer's or vendor's Developer ID.
    - **Bundle IDs**: Bundle ID is an alphanumeric string that uniquely identifies a system extension policy. You can specify more than one Bundle ID separated by a comma for any given Team ID.

    To identify Team ID and Bundle IDs, obtain a list of system extensions that are present on the machine via terminal using the following command:

    ```
    systemextensionsctl list
    ```

    This command will show all the system extensions in effect on the machine across all products. You need to locate the ones of interest for whitelisting and create a policy or policies that cover everything you wish to whitelist.

The output might look similar to the following:

```
bigfixmdm@LP2-US-xxxxxxxx mdm % systemextensionsctl list

1 extension(s)

--- com.apple.system_extension.network_extension

enabledactiveteamIDbundleID (version)name[state]

**PXPZ95SK77com.paloaltonetworks.GlobalProtect.client.extension
 (5.2.6-87/1)GlobalProtectExtension[activated enabled]
```

Where `PXPZ95SK77` is the Team ID and `com.paloaltonetworks.GlobalProtect.client.extension` is the Bundle ID.

Note:

- To whitelist the system extension of an application from a specific vendor, you must specify both the Team ID and the Bundle ID.
- Do not add multiple entries with the same Team ID, as only the last one in the list will actually be used. If you have multiple system extensions to whitelist with the same Team ID, add all the Bundle IDs in one entry separated by commas. For example:

  ```
  Bundle IDs: BundleID1,BundleID2,BundleID3
  ```

- If you do not specify any extension type, the policy assumes all system extensions associated with the TeamID are allowed.

6. **Allowed System Extension Types:**
   - **Driver Extension**: Select this to use the DriverKit framework and create drivers for USB, Serial, NIC, and HID devices that users can install in macOS. Learn more about DriverKit.
   - **Network Extension**: Select this to distribute network extension apps such as content filters, DNS proxies, and VPN clients as system extensions to macOS. Learn more about NetworkExtension.
   - **Endpoint Security Extension**: Endpoint security clients, including Endpoint Detection and Response software, antivirus software, can leverage the new EndpointSecurity API to monitor and even block system events to better conform with security policies and protect from potential malicious activity. Learn more about Endpoint Security.
7. **Add System Extension**: If you want to whitelist more than one product from different vendors within a single policy, click Add Extension to add additional Team ID and Bundle IDs to the same policy.
8. Click **Save**. The system extension whitelisting is created.

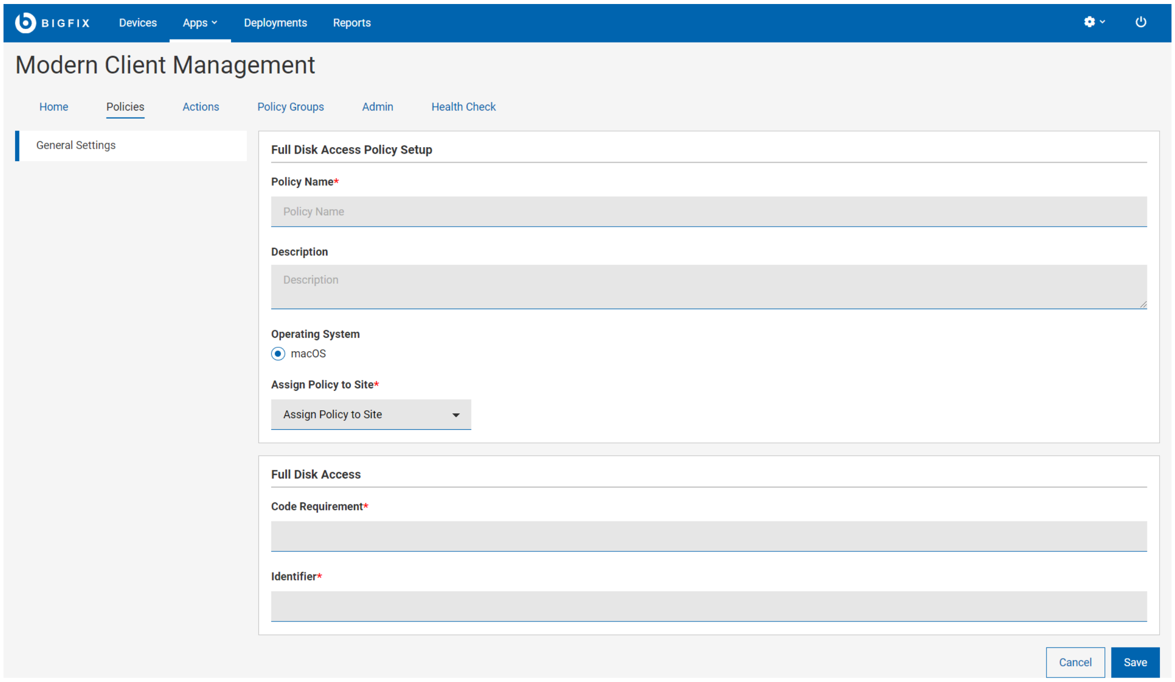
A System Extension Whitelist policy is created and is ready to be deployed.

Add the created policy to a policy group *(on page 269)* and deploy onto the MDM server or eligible devices.

Full Disk Access

You can create a Full Disk Access policy using this section. Creating a Full Disk policy allows the BigFix Agent (and other applications) to function smoothly on OSX devices. Applications configured with a full disk policy are granted complete disk access on OSX.

1. From the list of policy types, select **Full Disk Access**.



Full Disk Access Policy Setup

Policy Name*
Policy Name

Description
Description

Operating System
● macOS

Assign Policy to Site*
Assign Policy to Site

Full Disk Access

Code Requirement*

Identifier*

2. In **Generic Settings**, enter policy name and description.
3. To Assign Policy to Site, select a site from the dropdown.

Note: Non-master operator can see only those sites in the dropdown to which they have access.

4. Under **Full Disk Access**, enter Code Requirement and Identifier.
5. Click **Save**.
6. Add the policy to a policy group to deploy.

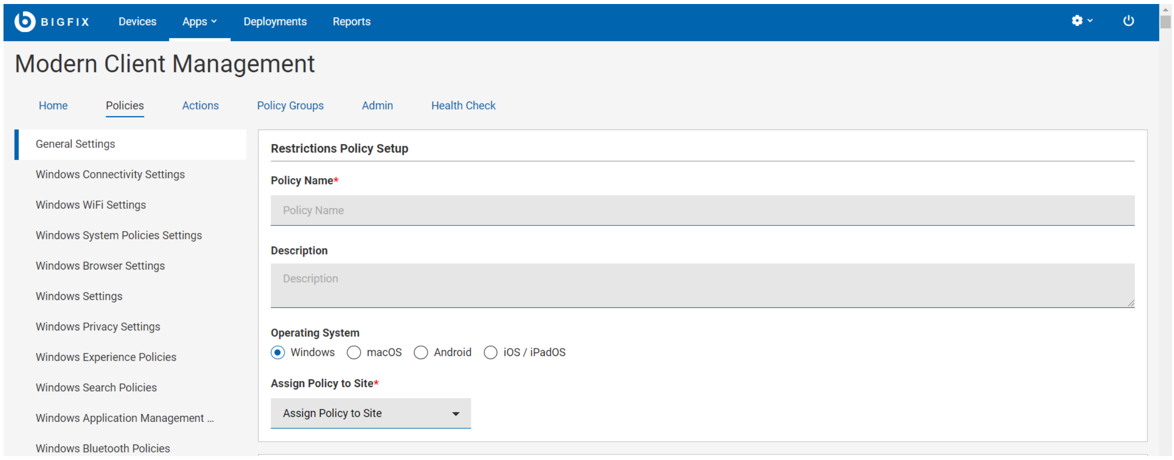
Restrictions Policy

With restriction profiles, you can control (enable or disable) many device capabilities of corporate devices and prevent many potential security threats. This prevents end users from using certain device features, such as using the camera. This is supported on MacOS, iOS, iPadOS, Android, and Windows.

To create a restrictions policy, complete the following steps.

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, on the right side corner, click the **Create Policy** button.

3. From the list of policy types, select **Restrictions**. The following page appears.



Restrictions Policy Setup

Policy Name*

Policy Name

Description

Description

Operating System

● Windows ○ macOS ○ Android ○ iOS / iPadOS

Assign Policy to Site*

Assign Policy to Site

4. In the **Generic Settings** section, do the following:
    a. Enter name and description of the policy.
    b. Select operating system.
    c. All operating systems have specific set of restrictions policies. Navigate to the specific settings for each of the operating systems selected on the left side navigation panel. Once there, you can set the operating system specific settings for your restrictions policy.
    d. In the **Assign Policy to Site** dropdown, select Master action site.
5. Click **Save**. The restriction policy is created.

    You can verify your policy and can click **Deploy Policy** to deploy it to selected devices.

A restriction policy is created for the selected operating system with the configured settings.

Add the created restriction policy to a policy group *(on page 269)* to deploy onto the eligible devices.

Android restriction settings

As an administrator, you can control users access and interaction with their Android device by applying restriction policy settings.

Some settings are available only for company-owned devices. For details, see Add company owned devices to the inventory.

Click a settings category and a setting. Learn about the restriction settings in the following section.

https://support.google.com/a/answer/6328708?hl=en#top&zippy=%2Cavailable-apps%2Cusb-file-transfer%2Cphysical-media

Related information

Android hardware security

iOS and iPadOS restriction settings

You can set restrictions, including modifying a device and its features, on iPhone and iPad devices enrolled in a mobile device management (MDM) solution.

For details on MDM restrictions for iPhone and iPad devices, see https://support.apple.com/en-in/guide/deployment/dep0f7dd3d8/web

Certain restrictions are available only for Apple devices that are supervised and enrolled in a mobile device management (MDM) solution. For details, see https://support.apple.com/en-in/guide/deployment/dep6b5ae23e9/1/web/1.0

macOS restriction settings

You can set restrictions to modify a device and its features, for MDM enrolled macOS devices.

For details about the settings, see https://developer.apple.com/documentation/devicemanagement/restrictions

Windows restriction settings

Windows operating system provides various restriction settings to control the access and behavior of users on a particular computer. IT Administrators can configuring Windows restriction settings through policies and ensure that the systems are secure and that users are not able to access or modify sensitive information.

: Some of the restrictions settings on Windows may not apply correctly depending on the edition and service pack level of the Windows endpoints. If one of those settings is edited, users receive a warning. To find more about what specific editions and versions of Windows are required, visit Microsoft documentation at

https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider.

The following are the restriction settings that you can configure:

- configureAdditionalSearchEngines
- enterpriseModeSiteList
- configureTaskbarCalendar
- letAppsAccessCalendar
- letAppsAccessCalendar_ForceAllowTheseApps
- letAppsAccessCalendar_ForceDenyTheseApps
- letAppsAccessCalendar_UserInControlOfTheseApps
- allowTailoredExperiencesWithDiagnosticData
- allowThirdPartySuggestionsInWindowsSpotlight
- disablePrintingOverHTTP
- allowWindowsSpotlightOnSettings
- turnOffFileHistory
- showLockOnUserTile
- allowWindowsSpotlight
- allowWindowsSpotlightOnActionCenter

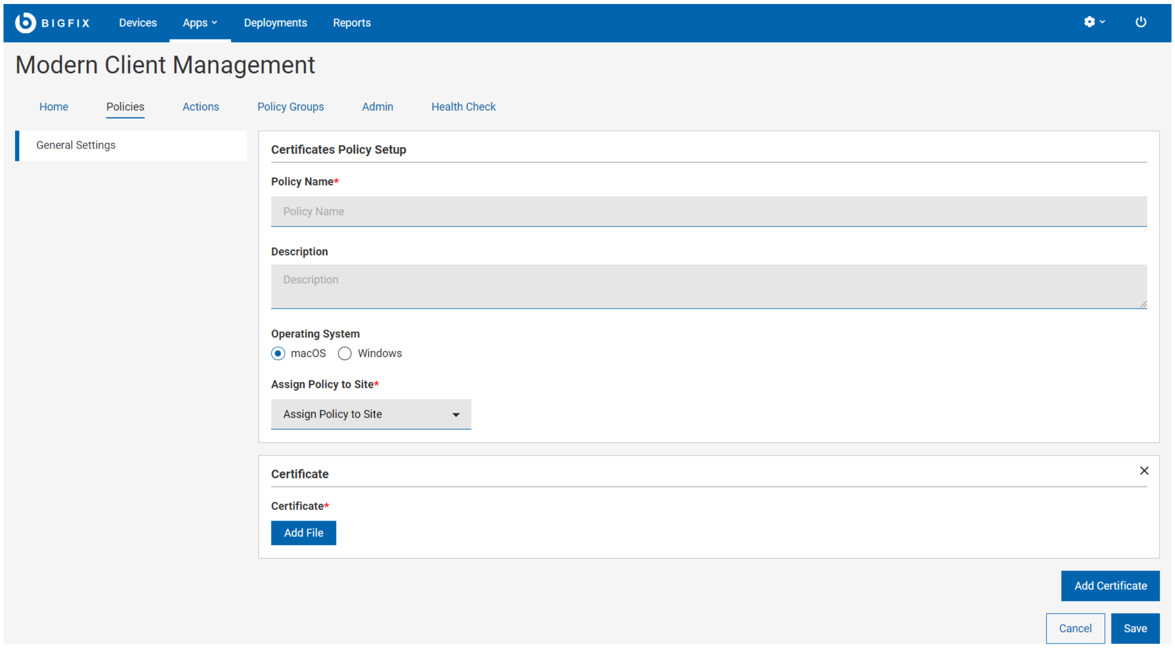
- allowWindowsSpotlightWindowsWelcomeExperience
- configureWindowsSpotlightOnLockScreen
- winsetMinimumEncryptionKeySize
- letAppsAccessBackgroundSpatialPerception
- letAppsAccessBackgroundSpatialPerception_ForceAllowTheseApps
- letAppsAccessBackgroundSpatialPerception_ForceDenyTheseApps
- letAppsAccessBackgroundSpatialPerception_UserInControlOfTheseApps

Certificates Policy

Learn how to upload `.pem` and `.der` certificates to MDM server and deploy them on MDM endpoints.

To create or edit certificates policy:

1. From the WebUI main page, select **Apps > MCM**.
2. On the MDM page, click **Create Policy**.
3. From the list of policy types, select **Certificates**. The following page appears.



Modern Client Management

Certificates Policy Setup

Policy Name*

Policy Name

Description

Description

Operating System

● macOS ○ Windows

Assign Policy to Site*

Assign Policy to Site

Certificate

Certificate*

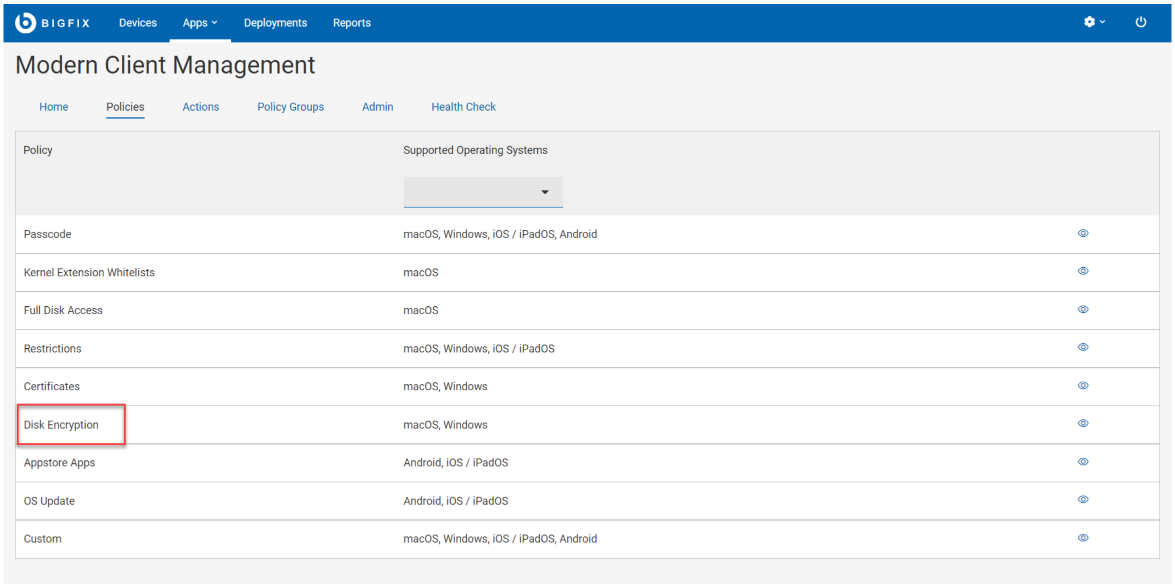
4. In the **Generic Settings** section, do the following:
   a. Enter name and description of the policy.
   b. Select operating system. Additional fields appear when you select the operating system.
   c. In the **Assign Policy to Site** dropdown, select **Master** action site.
5. Under **Certificate** section do the following:
   a. If you have selected Windows as operating system, select the **Certificate Type**
   b. Click **Add File** and select the `.pem` or `.der` certificate file.
6. Click **Add Certificate** to upload another certificate.
7. Click **Save**. Certificate policy is created.

Disk Encryption Policy

User can create and deploy a Full Disk Encryption (FDE) policy just like any other MDM policy.

For details on FDE, see Full Disk Encryption. To create a FDE policy complete the following steps:

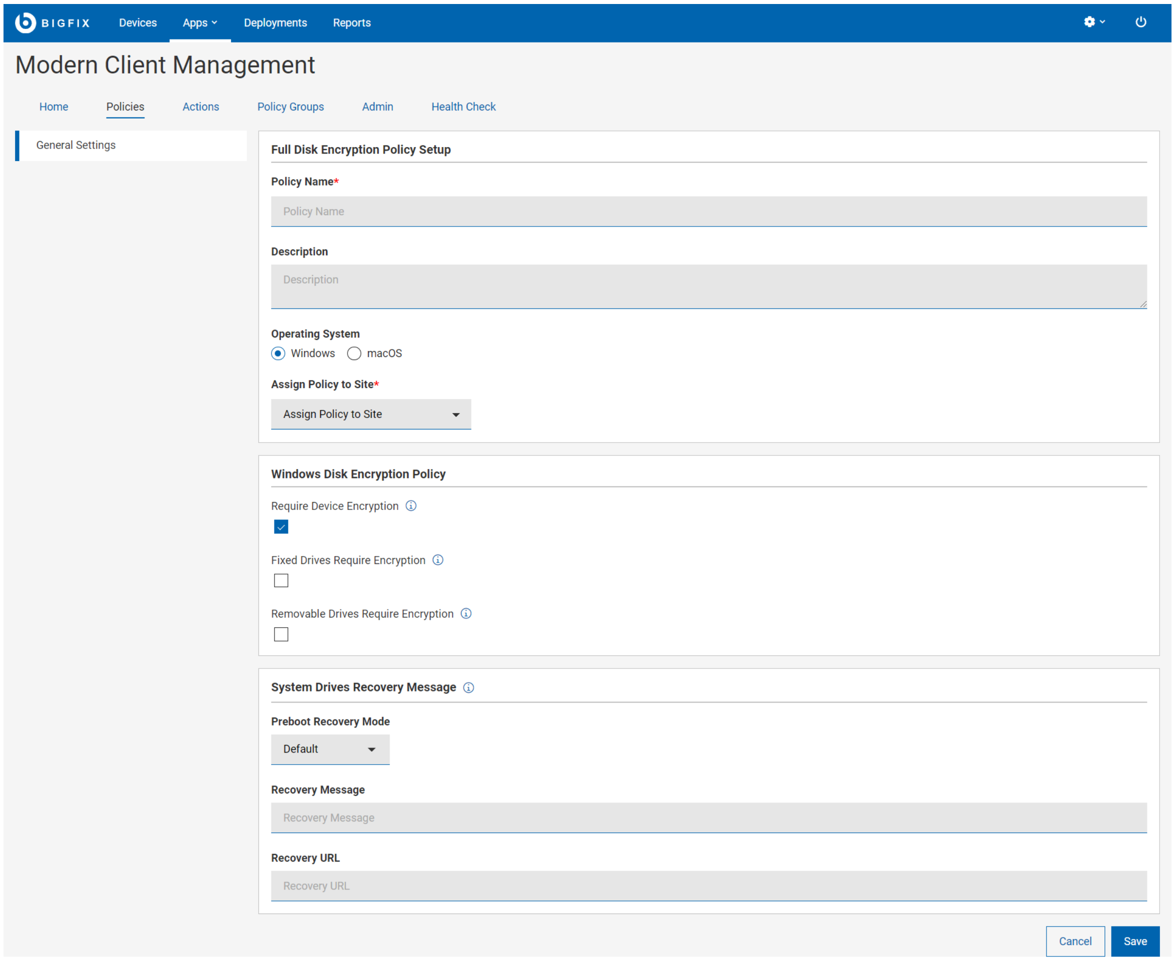
1. From the WebUI main screen, click **Apps > MCM** and on the top right corner, click **Create Policy**
2. From the list of policy types, select **Disk Encryption**



Modern Client Management

Policy	Supported Operating Systems
Passcode	macOS, Windows, iOS / iPadOS, Android
Kernel Extension Whitelists	macOS
Full Disk Access	macOS
Restrictions	macOS, Windows, iOS / iPadOS
Certificates	macOS, Windows
Disk Encryption	macOS, Windows
Appstore Apps	Android, iOS / iPadOS
OS Update	Android, iOS / iPadOS
Custom	macOS, Windows, iOS / iPadOS, Android

3. On the Disk Encryption Policy page, enter the required information.



Modern Client Management

Full Disk Encryption Policy Setup

Policy Name*: Policy Name

Description: Description

Operating System: ● Windows ○ macOS

Assign Policy to Site*: Assign Policy to Site

Windows Disk Encryption Policy

Require Device Encryption ☑

Fixed Drives Require Encryption □

Removable Drives Require Encryption □

System Drives Recovery Message

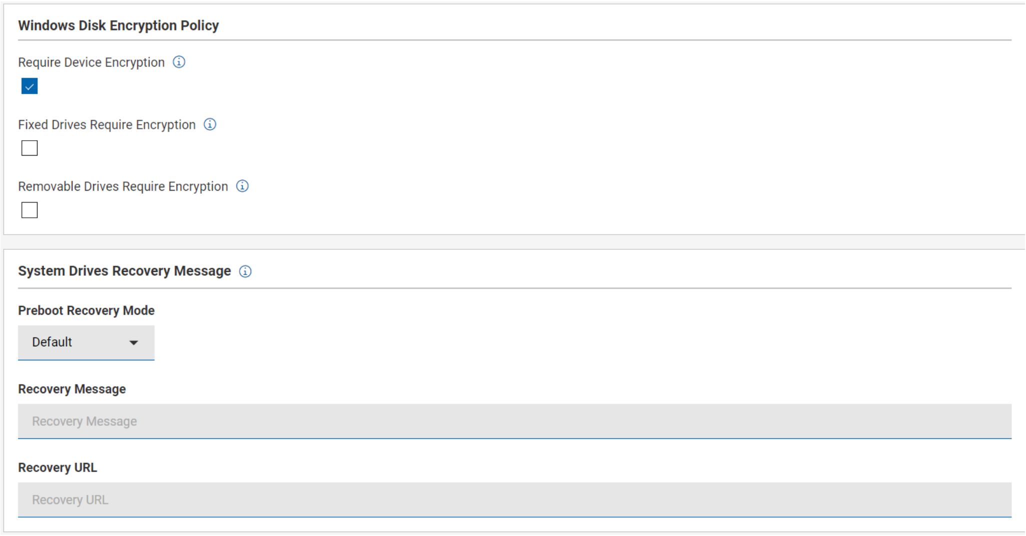
Preboot Recovery Mode: Default

Recovery Message: Recovery Message

Recovery URL: Recovery URL

Windows

If you select Windows for Operating System, provide the following information. You must configure if you want a Client UI offer (if available) or to just restart immediately.



Windows Disk Encryption Policy

Require Device Encryption ☑

Fixed Drives Require Encryption □

Removable Drives Require Encryption □

System Drives Recovery Message

Preboot Recovery Mode: Default

Recovery Message: Recovery Message

Recovery URL: Recovery URL

- Windows Disk Encryption Policy
  - **Require Device Encryption**: Select this to enforce disk encryption. This is selected by default.
  - **Fixed Drives Require Encryption**: This setting determines whether BitLocker protection is required for fixed data drives to be writable on a computer. If not encrypted, the fixed drives remain Read-Only.
  - **Removable Drives Require Encryption**: This setting configures whether BitLocker protection is required for a computer to be able to write data to a removable data drive. If not encrypted, the removable drives remain Read-Only.
- System Drives Recovery Message: This setting lets you configure the entire recovery message or replace the existing URL that are displayed on the pre-boot key recovery screen when the OS drive is locked.
  - Preboot Recovery Mode
    - Disabled
    - Default
    - Custom Message
    - Custom URL
  - Recovery Message: Recovery message is displayed in the BitLocker recovery page.
  - Recovery URL

macOS

If you select macOS for Operating System provide the following information:

- MacOS Disk Encryption Policy
  - **Recovery Key Output Path** which is an optional field where you can provide a path where the recovery key information is stored.
  - **Recovery Key Escrow Location**: The description of the location where the recovery key will be escrowed. This text will be inserted into the message the user sees when enabling FileVault. Required field. Enter a message that can be displayed to the user about from where to get the recovery key. For example, support helpdesk.

Note: Enabling full disk encryption on macOS devices disables auto-login. For more information, read Apple official documentation at https://support.apple.com/en-us/HT201476 and https://support.apple.com/en-us/HT204837.

4. Click **Save**.

Upload Custom Policy

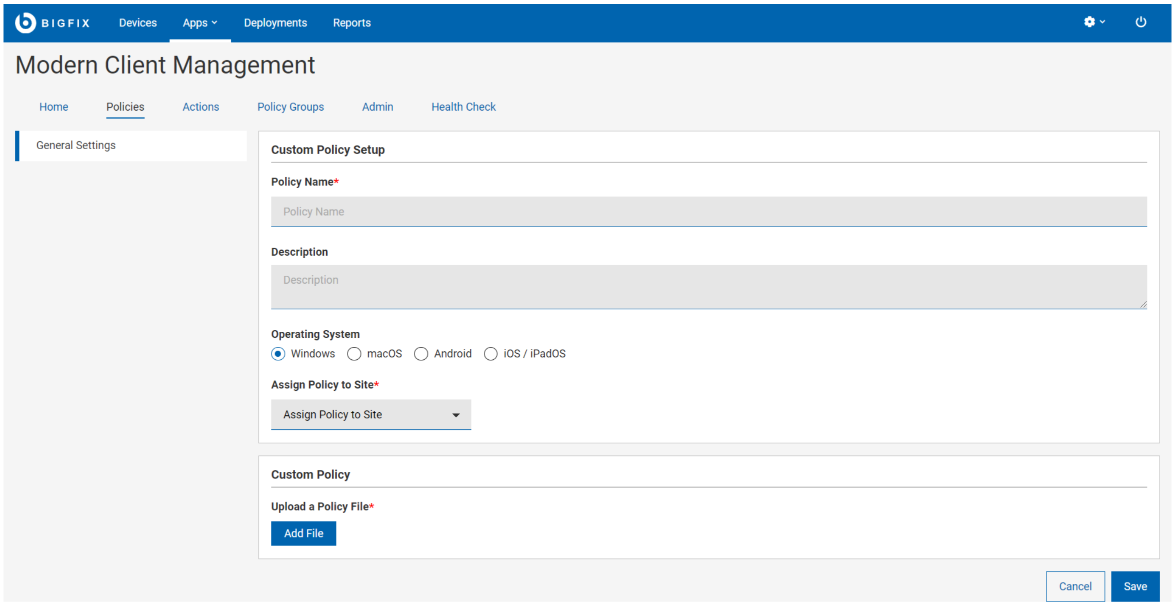
You can upload your custom policy file in `.xml`, `.mobileconfig`, or `syncML` format.

You can create a custom policy using this wizard.

Note:

- For macOS/ iOS / iPadOS, you can use profile creator to create custom policy and upload the `.mobileConfig` file to Custom Policy Wizard.
- For Windows, see https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference for all the potential CSPS that are available for use in a custom policy for Windows.
- For Android, see https://developers.google.com/android/management/reference/rest/v1/enterprises.policies for more information on the available settings you can use to construct a custom policy.
- Once an appropriate .syncml or .xml file has been created using the Microsoft docs as a reference, users can upload the file in the Custom Policy Wizard.

1. From the WebUI main page, select **Apps > MCM**.
2. On the Modern Client Management page, on the right side corner, click the **Create Policy** button.
3. From the list of policy types displayed, select **Custom**. The following page appears



Modern Client Management

Custom Policy Setup

Policy Name*

Policy Name

Description

Description

Operating System

● Windows ○ macOS ○ Android ○ iOS / iPadOS

Assign Policy to Site*

Assign Policy to Site

Custom Policy

Upload a Policy File*

.

4. Under **General Settings**, enter the name and description of the policy.
5. Select the operating system.
6. In the Assign Policy to Site dropdown, select a site to assign the policy. Non-master operator can see only those sites in the dropdown to which they have access.
7. **Note:**

- You can select only one operating system checkbox at a time.
- You can only create policies and assign them to sites where you have the write permission.

8. Under Custom Policy, click **Add File** to upload a `.xml` or `.mobileconfig` or `.syncml` policy file.

   Note: If the policy file is not in the supported format or if it contains binary characters, WebUI displays the error message "Unable to parse UUID from file.” For more information, see Unable to parse UUID from file.

9. Click **Save**.
10. Add the saved custom policy to a policy group to deploy it to the MDM server or applicable devices.

Appstore App Policy

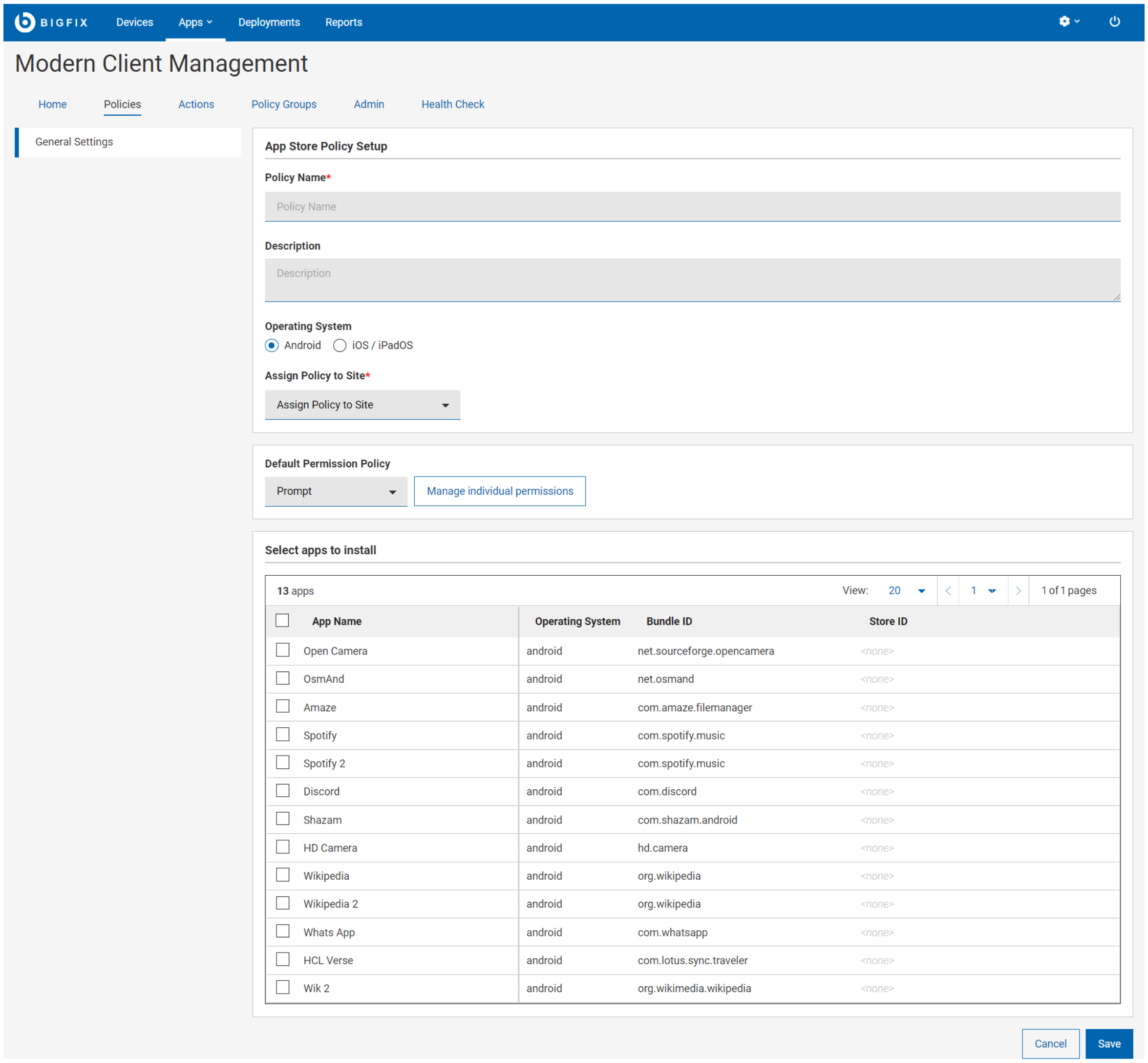
BigFix Mobile enables you to configure application policies to install applications from the App store on the Android, iOS, and iPadOS devices.

Before creating the Appstore App policy, set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) associations *(on page 230)* to make an app available to include in the Appstore app policy.

Creating an Appstore app policy

To create an appstore app policy, perform these steps:

1. Log in to BigFix WebUI.
2. Go to **Apps > MCM**.
3. Click **Create Policy** on the top right corner.
4. From the list of policy types, select **Appstore Apps**. The following page page appears.



Modern Client Management

App Store Policy Setup

Policy Name* Policy Name

Description Description

Operating System ● Android ○ iOS / iPadOS

Assign Policy to Site* Assign Policy to Site

Default Permission Policy Prompt | Manage individual permissions

Select apps to install

13 apps View: 20 | 1 | 1 of 1 pages

□ App Name	Operating System	Bundle ID	Store ID
□ Open Camera	android	net.sourceforge.opencamera	<none>
□ OsmAnd	android	net.osmand	<none>
□ Amaze	android	com.amaze.filemanager	<none>
□ Spotify	android	com.spotify.music	<none>
□ Spotify 2	android	com.spotify.music	<none>
□ Discord	android	com.discord	<none>
□ Shazam	android	com.shazam.android	<none>
□ HD Camera	android	hd.camera	<none>
□ Wikipedia	android	org.wikipedia	<none>
□ Wikipedia 2	android	org.wikipedia	<none>
□ Whats App	android	com.whatsapp	<none>
□ HCL Verse	android	com.lotus.sync.traveler	<none>
□ Wik 2	android	org.wikimedia.wikipedia	<none>

Cancel | Save

5. Under the **General Settings** section, enter Appstore Apps Policy Name and Description.
6. Select the Operating System.
7. From the **Assign Policy to Site** dropdown, select the site.
8. Configure the operating system specific settings. In the **Default Permission Policy** field, select the permission type; Prompt, Grant or Deny.

Android

Default Permission Policy: The permission set here is applicable globally for all the applications that are installed through the policy. Admins can choose from the following options when setting a default runtime permission policy for the managed Android apps.

- Prompt - prompt the user to grant permission to install apps. This is the default option. Device users can either choose to allow installation of the apps or cancel it.
- Grant - automatically grant permission to install the managed apps without user intervention

  - Deny - automatically deny permission to prevent unauthorized app installation
  - Manage individual permissions: IT admins can remotely set permissions to prevent applications from gaining access to data or control over a device. For example, the ability to read the user's contacts, external storage or location are runtime permissions. The user has to explicitly grant these permission for the application. However, for managed Google Play applications, administrators can configure and enforce these permissions from WebUI. Select Prompt, Grant, or Deny for individual permissions. For more details on the permissions listed, see the official Android documentation at https://developer.android.com/reference/android/Manifest.permission

  - The permissions configured through this policy are applicable globally to all the apps included in this policy. If you want to configure per-app permissions, you must configure them through a custom policy.
  - Deployment of this Appstore policy removes any previously deployed work profile applications that are not specified in this policy.

9. **Select apps to install**: Lists all the available apps specific to Android or iOS/iPadOS. Select the apps as desired.
10. Click **Save**.

Appstore app policy is created and is ready to deploy.

When the policy is deployed, the device receives a notification that a set permission or action is being performed on the device by the device manager. The permission manager in the device shows the permission that are applied.

Note: Android:

- Per-app permissions are not yet available.
- Policy deployment will remove any past work profile apps not specified in the new policy.

OS Update Policy

Through the OS update policy you can manage system updates for the Android and iOS/iPadOS devices.

This allows you to install system updates without user interaction.

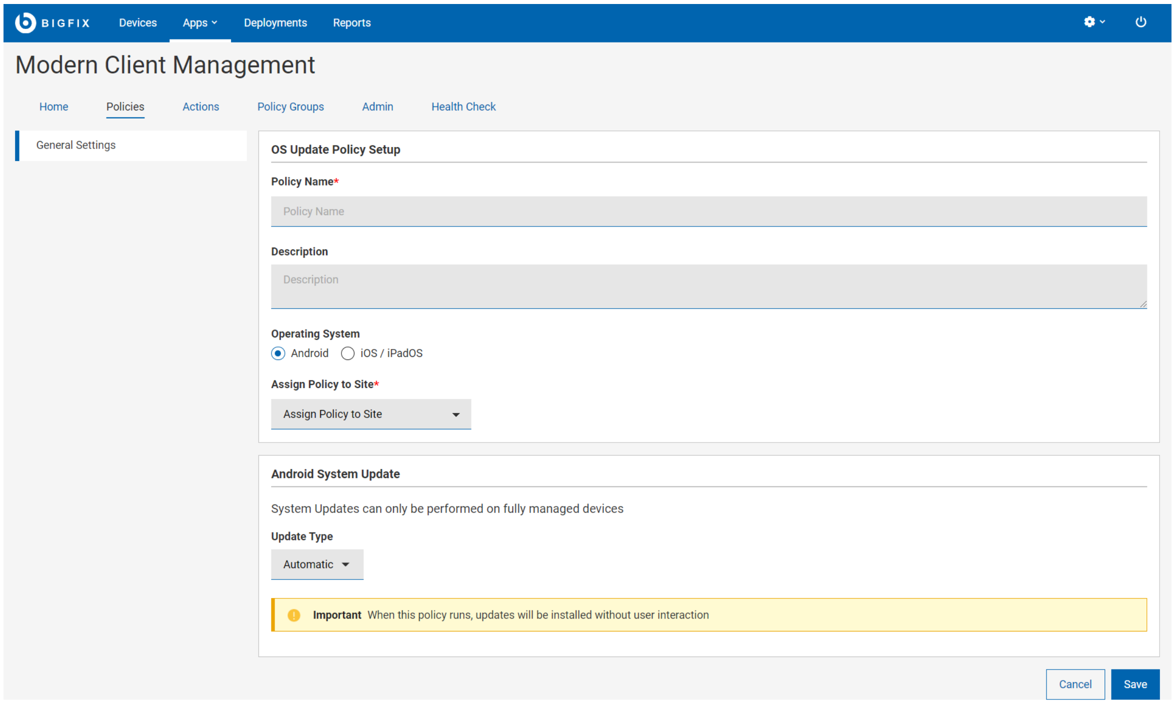
Prerequisite for the iOS/iPadOS devices to support OS update

- On iOS 10.3 and later, supported Software Update commands require supervision but not DEP enrollment. That means the device could either be OTA enrolled or DEP enrolled. If there is a passcode on the device, a user must enter it to start a software update.
- Prior to iOS 10.3, the supervised devices need to be DEP-enrolled and have no passcode
- Updates will not be installed if the battery level falls below 50% unless plugged in.

Creating an OS update policy

To create an OS update policy, perform the following steps:

1. Log in to BigFix WebUI.
2. Go to **Apps > MCM**.
3. Click **Create Policy** on the top right corner.
4. From the list of policy types, select **OS Update Policy**. The **OS Update Policy** page appears.



OS Update Policy Setup

Policy Name*

Policy Name

Description

Description

Operating System

● Android ○ iOS / iPadOS

Assign Policy to Site*

Assign Policy to Site

Android System Update

System Updates can only be performed on fully managed devices

Update Type

Automatic

Important When this policy runs, updates will be installed without user interaction

5. Under the **General Settings** section, enter the OS update policy name and description.
6. Select the **Operating System**.
7. From the **Assign Policy to Site** dropdown, select the desired site.
8. Configure the OS specific settings.

   Android System Update

   This section appears when you have selected Android as operating system. For Android, system updates can only be performed on fully managed devices. Select the required **Update Type**.

   - **Automatic**: Installs system updates (without user interaction) once they become available. Setting this policy type immediately installs any pending updates that might be postponed or waiting for a maintenance window.
   - **Windowed**: Installs system updates during a daily maintenance window (without user interaction). Set the start time and end time of the daily maintenance window to create a windowed policy.
   - **Postponed**: Postpones the installation of system updates for 30 days. After the 30-day period, the system prompts the device user to install the update.

iOS/iPadOS System Update

This section appears when you have selected iOS/iPadOS as operating system. For iOS/iPadOS, system updates can only be performed on supervised devices. An open action is created when deploying this policy that will periodically perform the selected update type.

- **Version**: This lists available versions found in the environment for updating to specific versions, or can chose "Latest" to update to latest regardless of version.
- **Update Type**:
    - **Download and Install**: Downloads or installs the system update depending on state of device. Two applications of the policy action will be required for the update to be installed.
    - **Download Only**: Download the software update without installing it.
    - **Install Only:** : Installs a downloaded update.

    > **Note:** : If no passcode is set on the device, the device restarts without prompting end user when performing an install. If passcode is set, device user is prompted to install the update; user also can decline.

- **Apply Frequency (Days)**: Select an option from the dropdown to set the frequency in which you want to run the system updates.

9. Click **Save**.

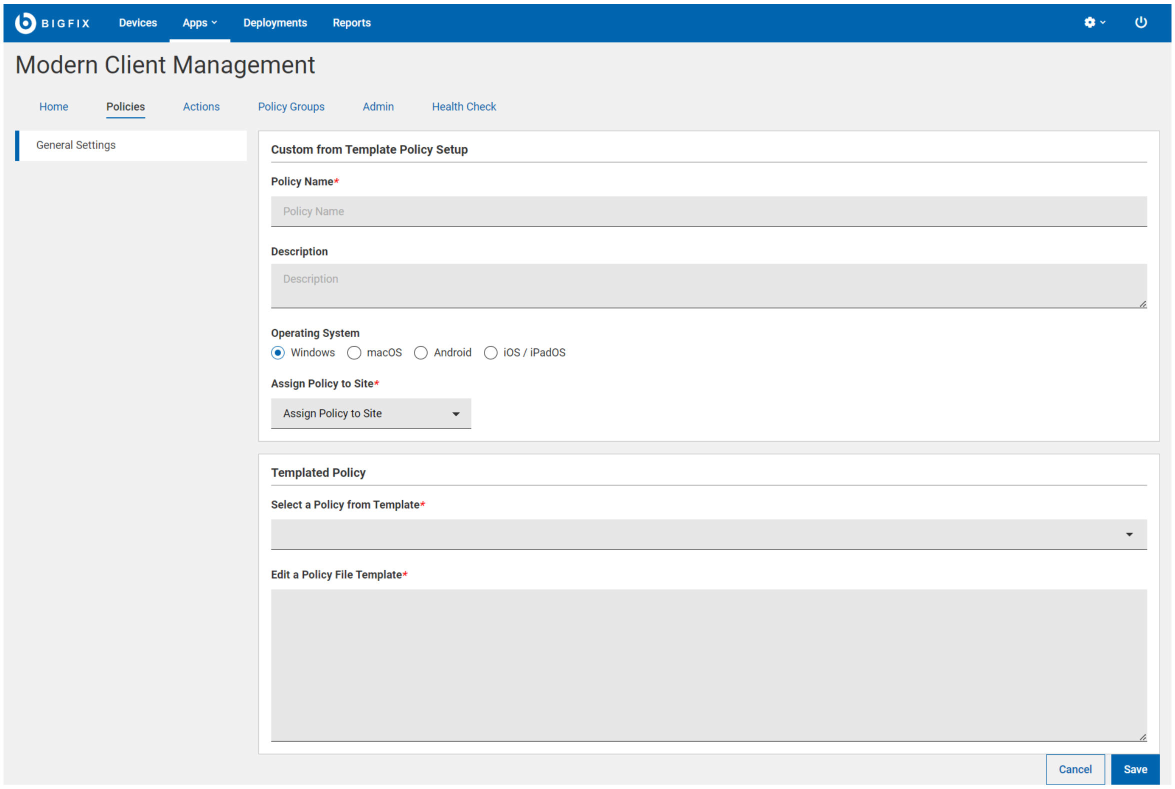
The OS update policy is created and can be deployed on Android or iOS/iPadOS devices as applicable.

Custom from Template

WebUI provides a set of custom policy templates that you can directly save or edit and save as a custom policy and then include in a Policy Group.

To access the custom template page and to create a custom policy from a pre-existing template for an operating system, do the following:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.



Modern Client Management

Custom from Template Policy Setup

Policy Name*

Policy Name

Description

Description

Operating System

● Windows ○ macOS ○ Android ○ iOS / iPadOS

Assign Policy to Site*

Assign Policy to Site

Templated Policy

Select a Policy from Template*

Edit a Policy File Template*

3. Select an **Operating System**. As per the selected operating system, applicable custom policy templates are displayed in the **Select a Policy from Templates** drop-down.

   Note: You cannot delete any default custom policy example template.

4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. Edit the selected policy template to customize it as per your needs.
6. Click **Save**.
7. The saved custom template is displayed under the **Policies** tab. Add this custom policy to a policy group or deploy on to an individual device as applicable.

For operating system specific custom policy templates and for the modifiable content, refer to the following pages.

Windows

- Windows SCEP DeviceID template *(on page 298)*
- Windows SCEP Username template *(on page 298)*
- Windows Private Firewall Enable Template *(on page 299)*
- Windows Public Firewall Enable Template *(on page 299)*
- Windows Offline Domain Join Template *(on page 299)*

MacOS, iOS, and iPadOS

- Apple SCEP Template *(on page 300)*

Android

- Dedicated Device Example Template *(on page 300)*
- Verify Application Enforcement Example Template *(on page 302)*
- Verify Application with User Choice Example Template *(on page 303)*

Windows custom policies

Read this section to find information about custom templates available for Windows custom policies.

Windows SCEP DeviceID template

This custom template is intended for creating SCEP policy to be deployed on to Windows devices based on the device ID.

To create a custom policy from the Windows SCEP DeviceID template, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Windows as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select **Windows SCEP DeviceID Template**.
6. Click **Save** to save the custom Windows SCEP DeviceID policy.
7. Add the custom policy to an appropriate Policy Group.

Note: At the time of deploying the policy, the necessary parameters are replaced as per the Simple Certificate Enrollment Protocol (SCEP) configuration.

Windows SCEP Username template

This custom template is intended for creating SCEP policy to be deployed on to Windows devices based on the device user name for OTA enrollments.

To create a custom policy from the Windows SCEP Username template, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Windows as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Windows SCEP Username policy.
6. Click **Save** to save the custom Windows SCEP Username policy.

7. Add the custom policy to an appropriate Policy Group.

Note: At the time of deploying the policy, the necessary parameters are replaced as per the Simple Certificate Enrollment Protocol (SCEP) configuration.

Windows Private Firewall Enable Template

This custom template is intended for creating private firewall policy to be deployed on to Windows devices. By enforcing this policy, you can ensure that the target Windows device has the Windows Firewall enabled and that you are controlling the inbound and outbound connections.

To create a custom policy from the Windows Private Firewall template, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Windows as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Windows Private Firewall Enable Template.
6. Click **Save** without changing any settings.

Windows Public Firewall Enable Template

This custom template is intended for creating public firewall policy to be deployed on to Windows devices. Through this policy, you can ensure that the target Windows device has the Windows Firewall enabled and that you are controlling the inbound and outbound connections.

To create a custom policy from the Windows Public Firewall template, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Windows as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Windows Public Firewall Enable Template.
6. Click **Save** without changing any settings.

Windows Offline Domain Join Template

A custom ODJ policy template for Windows is available in WebUI. You can modify and add it to a Policy Group like any other policy to deploy it to the MDM server. You can also deploy this custom ODJ policy on to individual devices.

To create acustom policy from the Windows Offline Domain Join template, complete the following steps:

1. From the WebUI select **Apps > MCM**
2. The WebUI MCM dashboard appears. Click **Create Policy**.
3. From the list of available policy options, select **Custom from Template**.

4. On the General Settings page, do the following:
    a. Enter **Policy Name** and **Description**.
    b. For **Operating System**, select Windows.
    c. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
    d. In the **Templated Policy** section, under **Select a Policy from Template** drop-down, select **Windows Offline Domain Join Template**.
    e. Click **Save** to save the Custom ODJ policy.
5. Add the saved ODJ policy to a policy group for Windows with “Autopilot” enrolment type and deploy to MDM Server.

MacOS custom policies

Read this section to find information about custom templates available for macOS custom policies.

Apple SCEP Template

This custom template is intended for creating SCEP policy to be deployed on to Apple devices.

To create custom policy with Apple SCEP template, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select macOS as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Apple SCEP Template.
6. Click **Save** to save the custom Apple SCEP DeviceID policy. At the time of deploying the policy, the necessary parameters are replaced as per the Simple Certificate Enrollment Protocol (SCEP) configuration.

Add the policy to an appropriate Policy Group to deploy onto the Apple devices.

Android custom policies

Read this section to find information about custom templates available for Android custom policies.

Dedicated Device Example Template

This custom template is intended for creating Dedicated Device policy to be deployed on to Android devices.

Dedicated devices are company-owned devices that fulfill a single use case, such as digital signage, ticket printing, or inventory management. This allows admins to further lock down the usage of a device to a single app or small set of apps, and prevents users from enabling other apps or performing other actions on the device. For more information on Dedicated Devices, see

Android Kiosk management.

To modify the custom template to personalize, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Android as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Dedicated Device Example Template.
6. This policy snippet includes the recommended device settings for a dedicated device with minimal access. Edit the *packageName* and *installType* to customize the applications that needs to be installed through this policy.

```
{
 "safeBootDisabled": true,
 "screenCaptureDisabled": true,
 "factoryResetDisabled": true,
 "cameraDisabled": true,
  "systemUpdate": {
  "type": "WINDOWED",
  "startMinutes": 120,
  "endMinutes": 240
 },
 "kioskCustomLauncherEnabled": true,
 "keyguardDisabled": true,
 "applications": [
 {
         "packageName":"com.olacabs.oladriver",
         "installType":"FORCE_INSTALLED",
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"com.screencast",
         "installType":"FORCE_INSTALLED"
      },
      {
         "packageName":"com.android.chrome",
         "installType":"FORCE_INSTALLED",
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"org.mozilla.firefox",
         "installType":"FORCE_INSTALLED",
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"com.ubercab",
         "installType":"FORCE_INSTALLED",
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"com.jio.media.jiobeats",
         "installType":"FORCE_INSTALLED",
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"com.microsoft.office.outlook",
         "installType":"FORCE_INSTALLED",
         "managedConfiguration":{
            "com.microsoft.outlook.EmailProfile.EmailAddress":"johndoe@hcl.com",
            "com.microsoft.outlook.EmailProfile.EmailAccountName":"John Doe",
            "com.microsoft.outlook.EmailProfile.ServerHostName":"outlook.office365.com",
   "com.microsoft.outlook.EmailProfile.EmailUPN": "prod\\John Doe"
        }
      }
 ]
}
```

Verify Application Enforcement Example Template

This custom template is intended for creating App enforcement policy for Android devices.

Verify Apps enforcement feature enables Google Play Protect to scan all the apps installed on Android device for harmful software before and after they are installed to ensure that malicious apps cannot compromise corporate data. This setting is optional.

To modify the custom template to personalize, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Android as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Verify Application Enforcement Example Template.
6. Edit the *packageName* and *installType* to customize the applications that need to be installed through this policy.

```
{
  "advancedSecurityOverrides": {
    "developerSettings": "DEVELOPER_SETTINGS_ALLOWED",
    "untrustedAppsPolicy": "DISALLOW_INSTALL",
    "googlePlayProtectVerifyApps": "VERIFY_APPS_ENFORCED"
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "AVAILABLE"
    }
   ]
}
```

7. Click **Save**.

Verify Application with User Choice Example Template

This custom template is intended for creating App enforcement policy with user choice for Android devices.

Verify Apps enforcement feature enables Google Play Protect to scan all the apps installed on Android device for harmful software before and after they are installed to ensure that malicious apps cannot compromise corporate data. With this custom policy, IT admins can provide device users an option to turn the setting `Scan apps with Play Protect` on or off. This allows the user to choose whether to enable app verification or not. This setting is optional.

To modify the custom template to personalize, complete the following steps:

1. From the MCM application click **Create Policy** and select **Custom from Template**.
2. On the **General Settings** page, enter the **Policy Name** and **Description**.
3. Select Android as the **Operating System**.
4. From the **Assign Policy to Site** drop-down, select a site to assign the policy.
5. From the **Select a policy from template** drop-down, select Verify Application user Choice Example Template.
6. Edit the *packageName* and *installType* to customize the applications that needs to be installed through this policy.

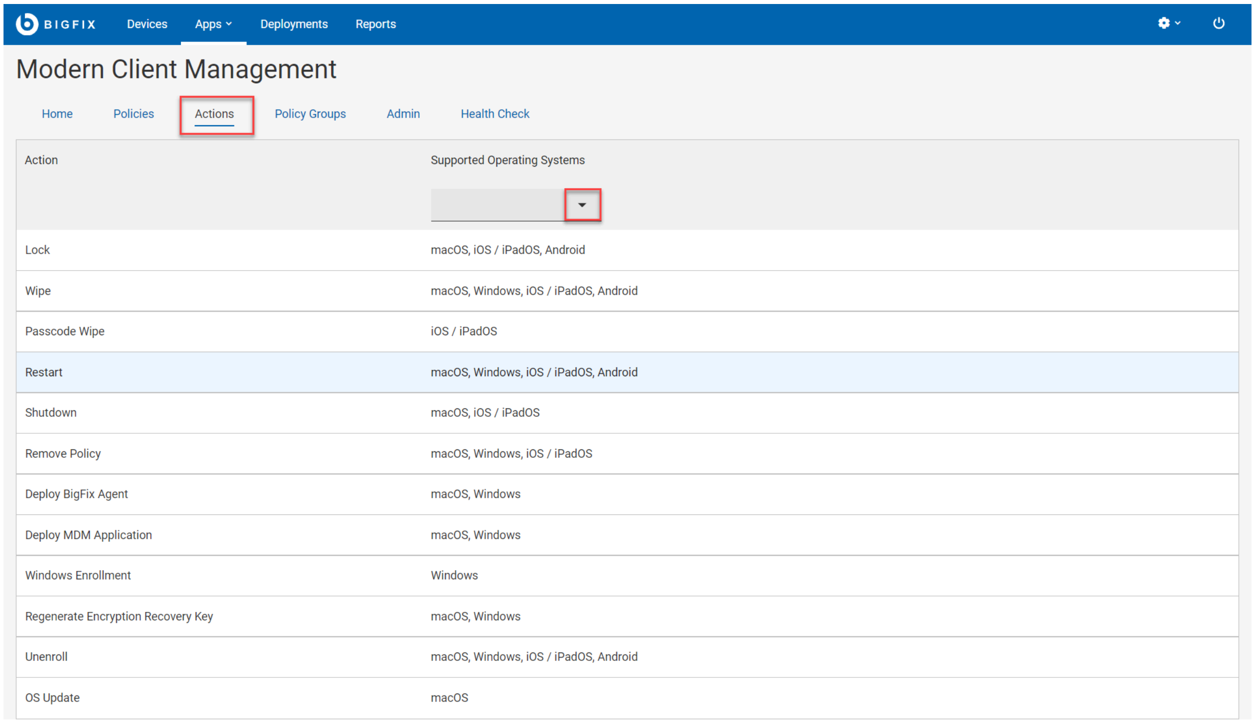
```
{
  "advancedSecurityOverrides": {
    "developerSettings": "DEVELOPER_SETTINGS_ALLOWED",
    "untrustedAppsPolicy": "DISALLOW_INSTALL",
    "googlePlayProtectVerifyApps": "VERIFY_APPS_USER_CHOICE"
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "AVAILABLE"
    },
    {
      "packageName": "com.spotify.music",
      "installType": "AVAILABLE"
    }
   ]
}
```

7. Click **Save**.

Deploy MCM actions

With MCM and BigFix Mobile, you can perform the following MDM-specific actions:

- Lock
- Wipe
- Passcode Wipe
- Restart
- Shutdown
- Remove Policy
- Deploy BigFix Agent
- Deploy MDM Application
- Windows Enrollment
- Regenerate Encryption Recovery Key
- Unenroll
- OS Update
- User Assignment



Action	Supported Operating Systems
Lock	macOS, iOS / iPadOS, Android
Wipe	macOS, Windows, iOS / iPadOS, Android
Passcode Wipe	iOS / iPadOS
Restart	macOS, Windows, iOS / iPadOS, Android
Shutdown	macOS, iOS / iPadOS
Remove Policy	macOS, Windows, iOS / iPadOS
Deploy BigFix Agent	macOS, Windows
Deploy MDM Application	macOS, Windows
Windows Enrollment	Windows
Regenerate Encryption Recovery Key	macOS, Windows
Unenroll	macOS, Windows, iOS / iPadOS, Android
OS Update	macOS

Note:

- You can deploy MDM actions only to the MCM and BigFix Mobile managed devices.
- You can also deploy MDM actions to correlated devices that have MCM and BigFix Mobile representation.
- Certain actions are operating system specific, and each action has an operating system logo on it to indicate which operating system it applies to. If you find more than one logo for an action, it represents that action can be applied to each operating system depicted.
- Deploying the *Deploy BigFix Agent* action requires installer packages to be pre-staged to work properly. For macOS, see Prestage macOS BigFix installer *(on page 235)*. For Windows, see Prestage Windows BigFix Installer *(on page 236)*.

To perform different MDM actions, follow these steps:

1. Login to the WebUI.
2. Click **Apps** and select **MCM**.
3. From the Modern Client Management page, click **Actions**.
4. The MDM Actions page displays all the possible actions along with the supported operating system for every action. You can also filter applicable actions by using the Supported Operating Systems filter. Click on the specific MDM action you want to deploy on MDM endpoints.

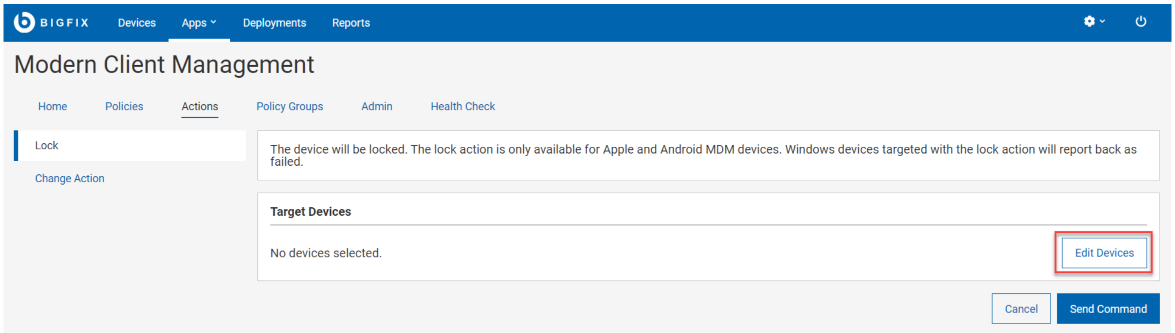
Lock Device

Use this action to remotely lock devices that are lost or stolen. Lock helps protect the data stored on devices when they are lost or stolen. If after initiating a lock action the device is recovered, the device can be unlocked using the recovery pin set initially by the action launched from the WebUI.

Note:

- Lock action is applicable for macOS, iOS, iPadOS, and Android devices.
- Lock action is not applicable to Windows devices. The lock action deployed on Windows MDM devices does not lock those Windows devices, and this action reports as failed.

1. From the list of available actions, select **Lock**.
2. On the following screen, click **Edit Devices** to add or remove the devices.



Modern Client Management

The device will be locked. The lock action is only available for Apple and Android MDM devices. Windows devices targeted with the lock action will report back as failed.

Target Devices

No devices selected.

3. Click **Send Command** to deploy the action to the targeted devices.

   Result: The targeted devices are locked.

   Note: Different operating systems prompt users for different options during the lock operation. For Android devices, users can enter the Android Command duration (in seconds). The command expires if not executed within the time specified.

Wipe

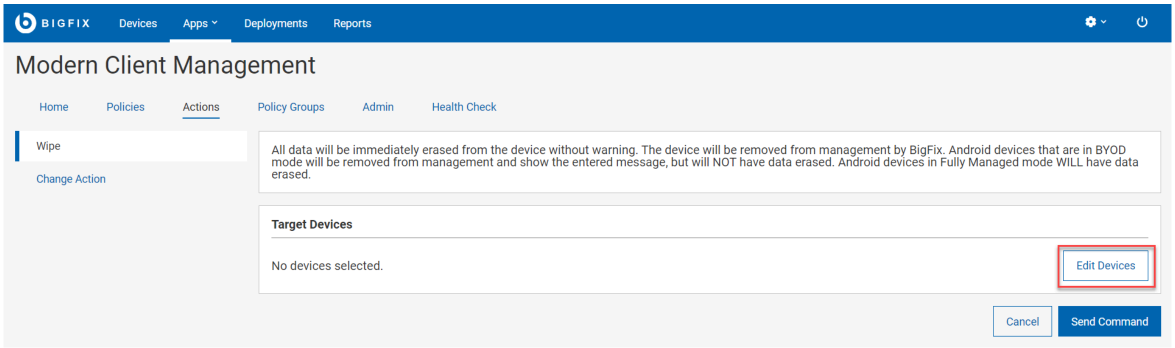
Use this action to erase the data on the remote device, even if the device is locked. The Wipe action helps you to completely erase the data from the targeted devices from the BigFix management without warning the end-user.

Note:

- The recovery code applies only to macOS devices. Windows devices will execute the Wipe action while ignoring the recovery pin.
- Users can wipe only one device at a time and cannot execute wipe on device groups.

- When targeting Android devices, the following options are available to specify the level of wipe on the Android device:
  - WIPE DATA UNSPECIFIED: This value is ignored.
  - PRESERVE RESET PROTECTION DATA: Preserve the factory reset protection data on the device.
  - WIPE EXTERNAL STORAGE: Additionally wipe the external storage of the device.

1. From the list of available actions, select **Wipe**.
2. On the following screen, click **Edit Devices** to add or remove devices.



All data will be immediately erased from the device without warning. The device will be removed from management by BigFix. Android devices that are in BYOD mode will be removed from management and show the entered message, but will NOT have data erased. Android devices in Fully Managed mode WILL have data erased.

Target Devices

No devices selected.

3. If you select macOS devices to wipe, set a six-digit recovery PIN. This PIN is required to reinstall the operating system on the device. Ensure to record it and share it with the device owner.
4. Click **Send Command** to deploy the action to the targeted devices.

   Result: Once the deployment is complete, the targeted devices are wiped from MDM.

Passcode Wipe

Use this action to remove passcode from the targeted iOS, iPadOS, and Android devices.

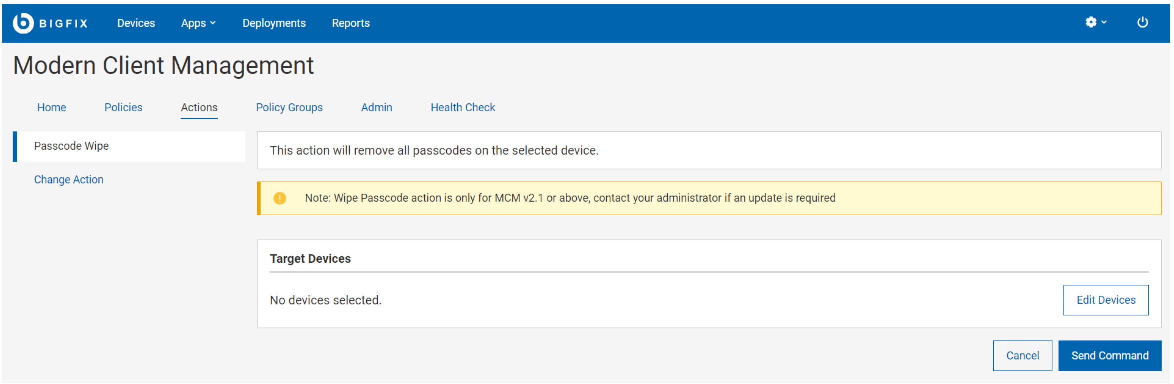
Note:

- The target iOS or iPadOS device must be a supervised device for this action to be successful.
- All the iOS 15 or later are supervised.

If an iOS, iPadOS, or Android device user forgets the passcode, an IT Admin can remotely remove the passcode from the device, so that the device user can get back access to the device.

To wipe passcode on selected devices, complete the following steps.

1. From the list of available actions, select **Passcode Wipe**.
2. On the following screen, click **Edit Devices** to add or remove devices.



This action will remove all passcodes on the selected device.

Note: Wipe Passcode action is only for MCM v2.1 or above, contact your administrator if an update is required

No devices selected.

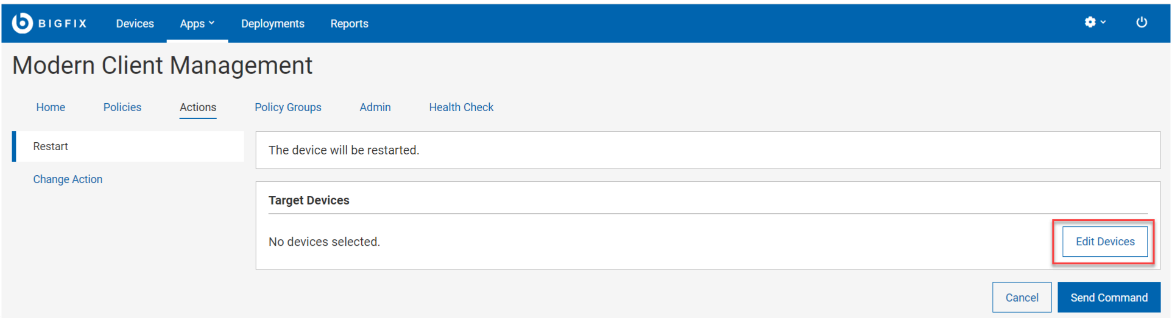
3. Click **Send Command** to deploy the action to the targeted devices.

- When the action is completed, it removes Passcode, PIN, patterns from the targeted mobile devices.
- If the target is an Android device with Personal and Work profiles, the passcode is removed only for the Work Profile.

Restart

Use this action to restart the targeted devices.

1. From the list of available actions, select **Restart**.
2. On the following screen, click **Edit Devices** to add or remove devices.



The device will be restarted.

No devices selected.

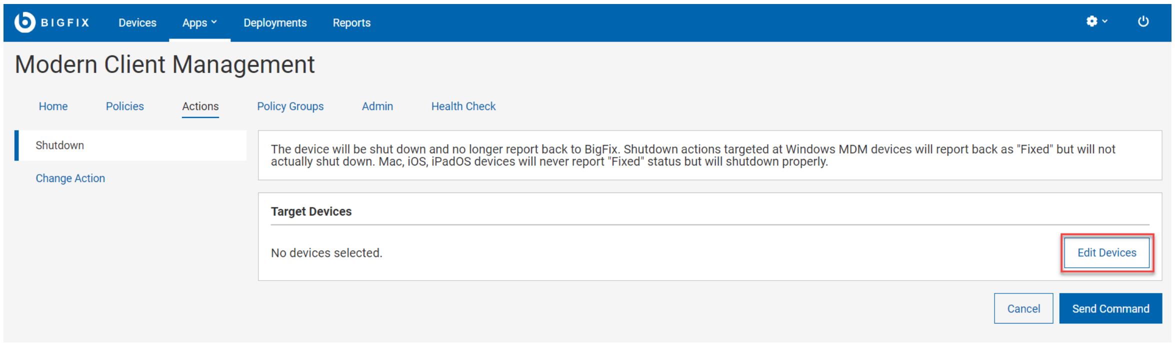
3. Click **Send Command** to deploy the action to the targeted device.

Note: The restart action is only available for Apple DEP devices. Non-supervised Apple devices targeted with the restart action will ignore the restart command.

Shutdown

Use this action to shut down the targeted devices.

1. From the list of available actions, select **Shutdown**.
2. From the following screen, click **Edit Devices** to add or remove devices.



The device will be shut down and no longer report back to BigFix. Shutdown actions targeted at Windows MDM devices will report back as "Fixed" but will not actually shut down. Mac, iOS, iPadOS devices will never report "Fixed" status but will shutdown properly.

No devices selected.

3. Click **Send Command** to deploy the action to the targeted devices.

Note:

- The restart action is only available for Apple DEP devices. Non supervised Apple devices targeted with the restart action will ignore the restart command.
- Shutdown action is available only for macOS/iOS/iPadOS and not for Windows.

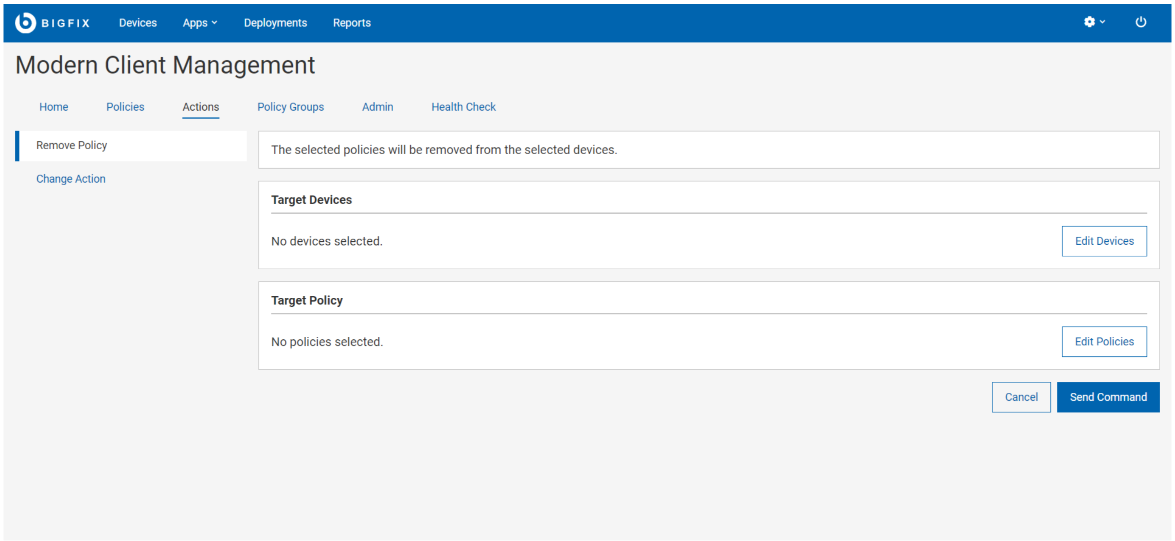
Remove Policy

You can remove policies from selected devices using this action. You can only remove policies on devices that are enrolled in MCM and BigFix Mobile.

Note:

- If remove policy action is sent to macOS devices that do not have the selected policy, the action fails.
- You cannot remove Android policy. You can only overwrite Android policy by deploying another policy through Policy Groups *(on page 269)*.

1. From the list of available actions, select **Remove Policy**.
2. From the following screen, click **Edit Devices** to add or remove devices.



The selected policies will be removed from the selected devices.

Target Devices

No devices selected.

Target Policy

No policies selected.

3. Click **Edit Policies** to select the policy that needs to be removed from the targeted devices.
4. Click **Send Command** to deploy the action to the targeted devices.

Deploy BigFix Agent

See Deploy BigFix Agent (on page 265).

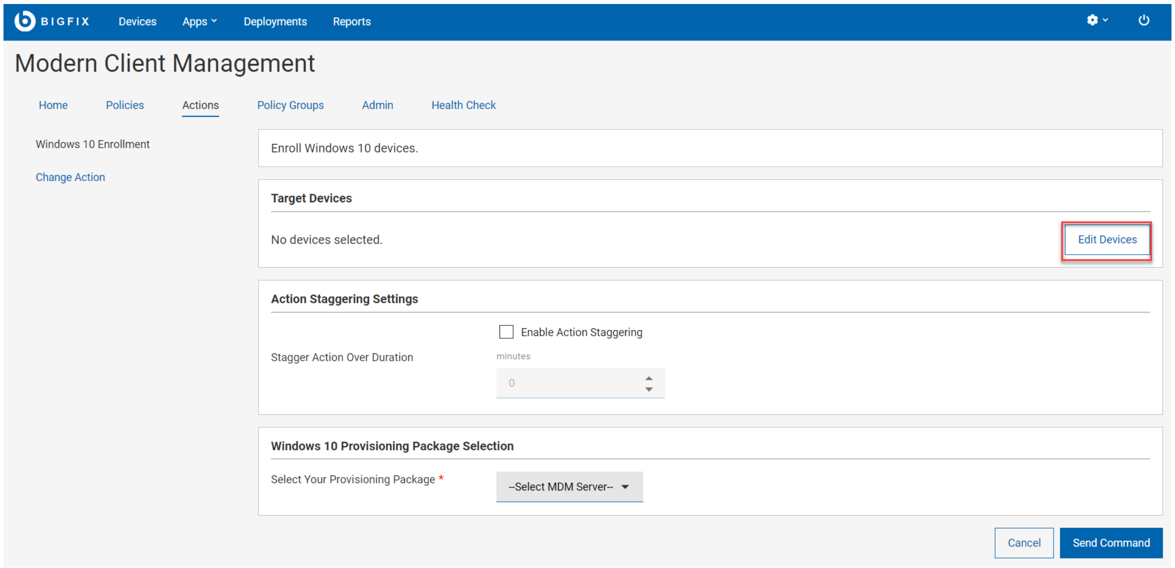
Deploy MDM Application

See Deploy BigFix Agent (on page 265).

Windows Enrollment

If `ppkg` file is present in your MDM server, then you can also initiate Windows bulk enrollment *(on page 239)* via this page. To do that:

1. From the list of available actions, select **Windows Enrollment**.
2. From the following screen, click **Edit Devices** to select devices in your environment that have BigFix agent installed.



Modern Client Management

Windows 10 Enrollment

Change Action

Enroll Windows 10 devices.

Target Devices

No devices selected.

Action Staggering Settings

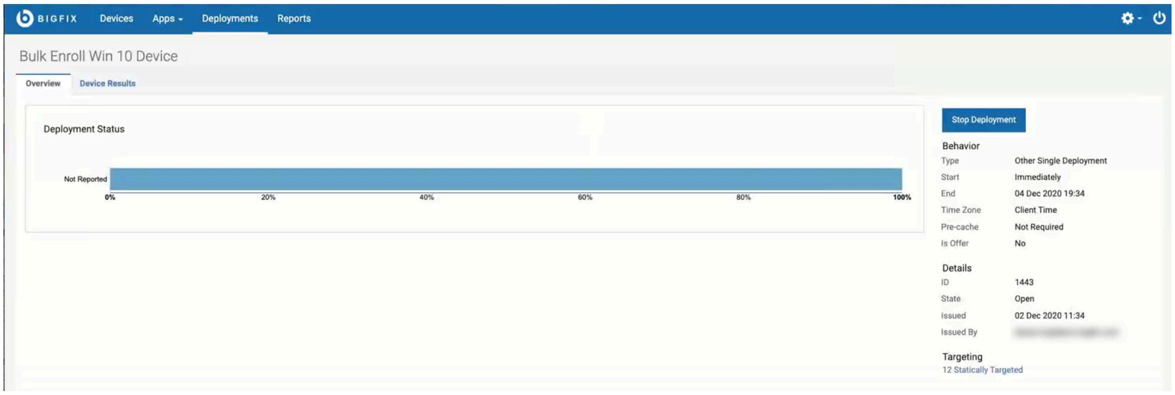
□ Enable Action Staggering

Stagger Action Over Duration: minutes 0

Windows 10 Provisioning Package Selection

Select Your Provisioning Package *: --Select MDM Server--

3. Action Staggering Settings: Select **Enable Action Staggering** and enter **Stagger Action Over Duration** in minutes. Use this setting to spread out the load on the MDM server and network to prevent all the targeted endpoints attempting to enroll at the same time. Staggering enrolling endpoints normalizes the amount of traffic generated by newly enrolled devices over a broader more manageable period of time. When this is set, each endpoint selects a random time within the specified time interval to enroll.
4. For **Select Your Provisioning Package**, select the MDM server to which you want to enroll the selected devices.
5. Click **Send Command**.
    - A BigFix deployment is generated that initiates MDM enrollment on the selected devices.
    - The deployment document *(on page 150)* with information on devices targeted and device results is displayed.
    - The targeted devices start the enrollment processes.
    - At any point, to stop the deployment, click **Stop Deployment**.



Bulk Enroll Win 10 Device

Behavior

Type	Other Single Deployment
Start	Immediately
End	04 Dec 2020 19:34
Time Zone	Client Time
Pre-cache	Not Required
Is Offer	No

Details

ID	1443
State	Open
Issued	02 Dec 2020 11:34
Issued By	[redacted]

Targeting

12 Statically Targeted

Regenerate Encryption Recovery Key

See Regenerate Encryption Recovery Key (on page 263).

Unenroll

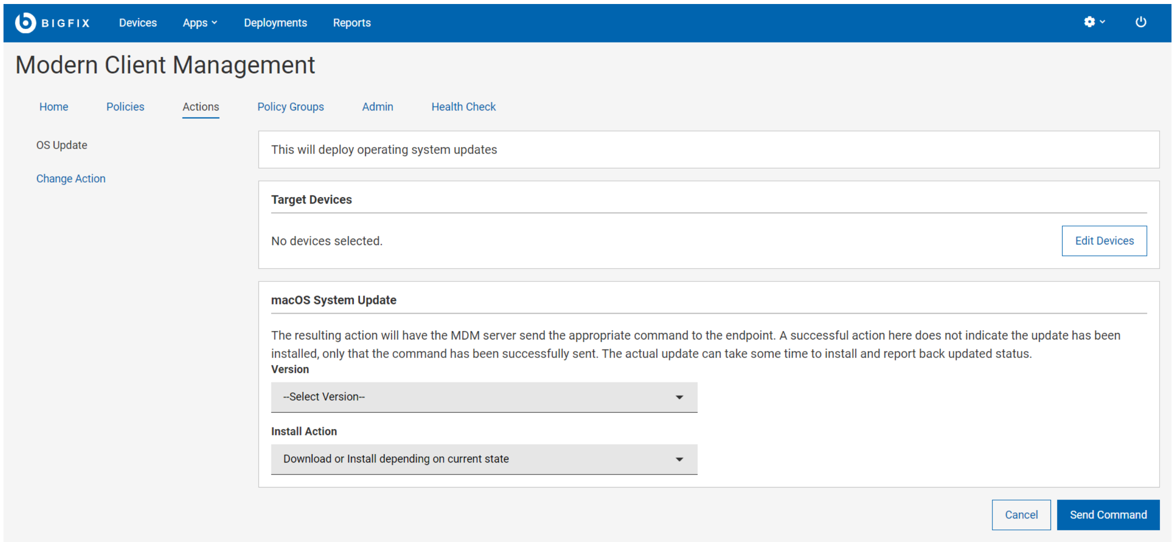
See Unenroll devices (on page 314)

OS Update

Use this action to update the system software in macOS devices. This is similar to OS Update Policy (on page 294) for the Android and iOS/iPadOS devices.

To update system software in macOS devices, complete the following steps:

1. From the list of available actions for macOS, select **OS Update**.
2. On the OS Update page, under **Target Devices**, click **Edit Devices** and select the applicable target devices or group.



This will deploy operating system updates

No devices selected.

The resulting action will have the MDM server send the appropriate command to the endpoint. A successful action here does not indicate the update has been installed, only that the command has been successfully sent. The actual update can take some time to install and report back updated status.

Version: --Select Version--

Install Action: Download or Install depending on current state

3. Under macOS System Update, select a macOS **Version** to update. This drop-down dynamically lists the security patches, minor and major versions, and all other software updates applicable to the macOS devices in your environment.

   Important:

   - ***Supported***: Only Big Sur and Monterey are supported for macOS updates.
   - ***Not supported***: Catalina OS upgrades (10.15.X) are not supported.

4. Select the **Install Action**. According to the action selected, WebUI displays appropriate messages to consider.
5. Click **Send Command**.

Note:

- This action will only be relevant and run on endpoints that have the specified update listed as available.
- Successful action indicates only sending the update to the MDM server and notifying the operating system to schedule the update according to rules of the operating system. This does not indicate actual system update on the OS.
- If the update was applicable before, but after successfully sending the OS update command, becoming unavailable indicates the update was installed on the OS. It will reflect in the analysis only after a refresh.

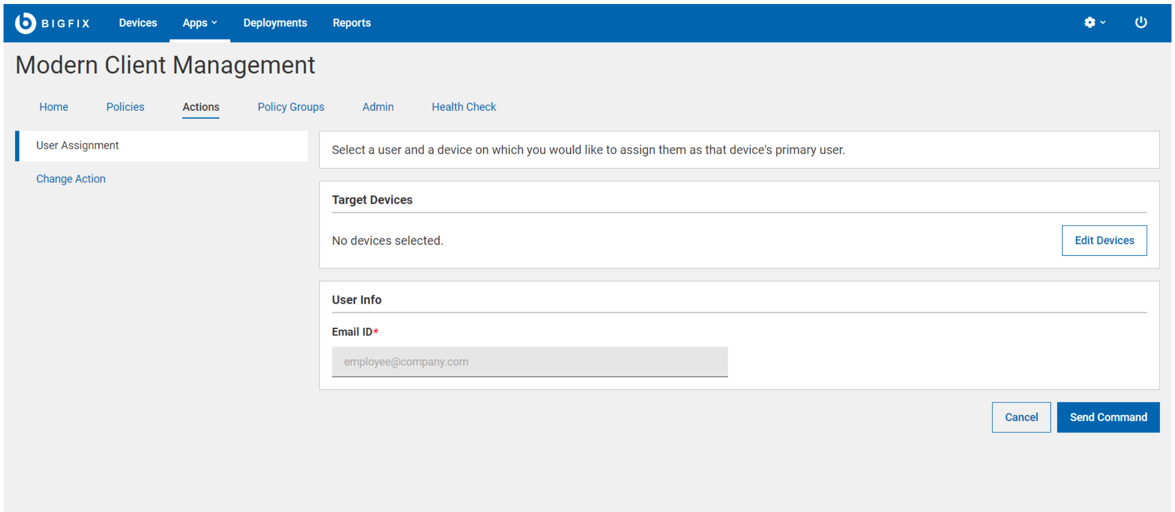
User Assignment

Use this action to assign a user to an MCM enrolled device. You can set or change the primary user that was assigned to a device during enrollment. If a user is already assigned to a device, this action overrides and assigns the specified user as the primary device user. If a user is not assigned previously, this action assigns the primary device user afresh.

Note: With MCM v3.0, this action allows you to assign primary user for one device at a time. If you want to assign primary users for huge number of devices, contact HCL Support at `BigFixServices@hcl.in`

To assign a user to a device, complete the following steps:

1. From the list of available actions, select **User Assignment**.
2. On the User Assignment page, under **Target Devices**, click **Edit Devices** and select a device.



Select a user and a device on which you would like to assign them as that device's primary user.

No devices selected.

employee@company.com

3. Under User Info, enter the **Email ID** of the user to whom you want to assign the target device.
4. Click **Send Command**.

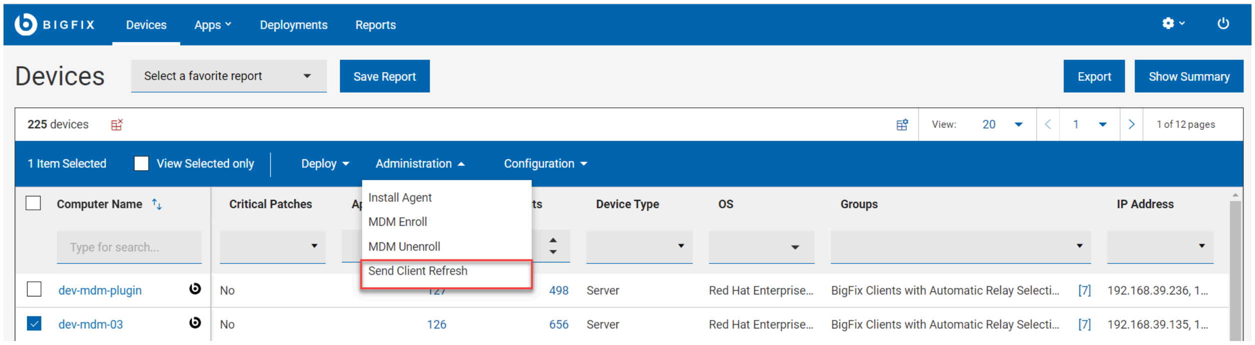
Note: When the action is successful, WebUI registers the primary user with the entered email ID.

Send Client Refresh

Use this action to send client refresh to devices.

This action is available for all BigFix managed devices, regardless of whether the device is managed by MDM, by BigFix Native agent, or through cloud plugins.

Send Client Refresh action becomes available under Administration menu, when you select one or more devices from the Device List *(on page 23)*.



☐	Computer Name	Critical Patches	Ap…	…ts	Device Type	OS	Groups		IP Address
☐	dev-mdm-plugin	No	127	498	Server	Red Hat Enterprise...	BigFix Clients with Automatic Relay Selecti...	[7]	192.168.39.236, 1...
☑	dev-mdm-03	No	126	656	Server	Red Hat Enterprise...	BigFix Clients with Automatic Relay Selecti...	[7]	192.168.39.135, 1...

By deploying the *Send Client Refresh* action, you can send a full client refresh request to devices. It is equivalent to performing Send Refresh on the BigFix Console.

In BigFix 9.5, send client refresh creates an action against targeted devices with the ActionScript notify client ForceRefresh.

In MCM and BigFix Mobile, WebUI sends a direct API call to force clients to perform full refresh.

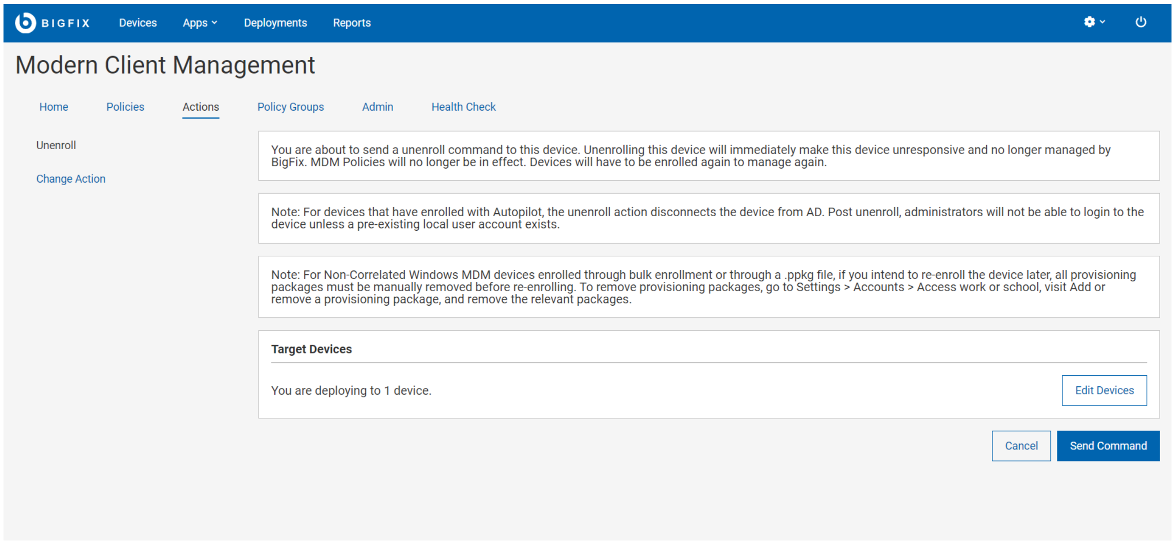
Unenroll devices

After unenrolling from MDM, you can no longer manage the device through BigFix MCM. MDM policies become ineffective on the unenrolled devices.

Unenrollment through WebUI

To unenroll devices through WebUI:

1. From the WebUI main page, click **Devices**.
2. From the listed devices, select the devices to unenroll.
3. From the action bar that appears in blue, select **Administration > MDM Unenroll**.The following page appears.



You are about to send a unenroll command to this device. Unenrolling this device will immediately make this device unresponsive and no longer managed by BigFix. MDM Policies will no longer be in effect. Devices will have to be enrolled again to manage again.

Note: For devices that have enrolled with Autopilot, the unenroll action disconnects the device from AD. Post unenroll, administrators will not be able to login to the device unless a pre-existing local user account exists.

Note: For Non-Correlated Windows MDM devices enrolled through bulk enrollment or through a .ppkg file, if you intend to re-enroll the device later, all provisioning packages must be manually removed before re-enrolling. To remove provisioning packages, go to Settings > Accounts > Access work or school, visit Add or remove a provisioning package, and remove the relevant packages.

Target Devices

You are deploying to 1 device.

4. If you want to change the target, click **Edit Devices**. Review the information and click **Send Command**. The device gets unenrolled.

Note:

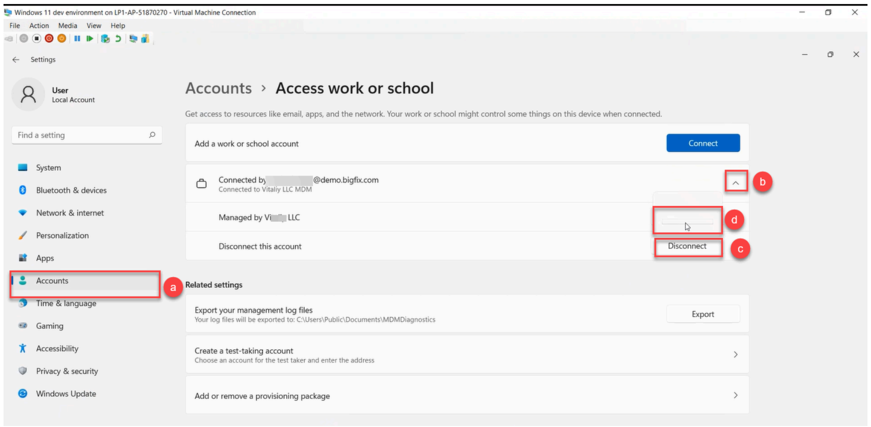
- If you have installed BigFix Platform version earlier than 10.0.8, when you unenroll and later re-enroll an MDM device, WebUI and the Console show multiple devices with unique computer IDs. To avoid this, upgrade BigFix Platform version to 10.0.8 or later, which deletes the unenrolled device from the root server, Console, and WebUI.
- An endpoint that is enrolled with an ODJ policy, when unenrolled, does not get disconnected from Active Directory. To fix this issue, see Endpoint not disconnected from AD after unenrollment.

Unenrollment by device user

Windows

- By default, MCM allows user-initiated unenrollment on all the enrolled Windows devices.
  - As a device user, to unenroll a Windows device, do the following steps:
    - a. Select **Account** from the left navigation pane.
    - b. Click the caret symbol next to **Connected by**
    - c. Click **DisconnectAccess work or school** and click **Disconnect**. The device gets unenrolled from MDM service.

- d. Additionally in Windows 11 devices, to unenroll, click the popup button (that is displayed as a blank line) that appears after clicking **Disconnect**.



Windows 11 dev environment on LP1-AP-51870270 - Virtual Machine Connection

Accounts › Access work or school

Get access to resources like email, apps, and the network. Your work or school might control some things on this device when connected.

Add a work or school account

Connected by [redacted]@demo.bigfix.com
Connected to Vitaly LLC MDM

Managed by Vi[redacted] LLC

Disconnect this account

Related settings

Export your management log files
Your log files will be exported to: C:\Users\Public\Documents\MDMDiagnostics

Create a test-taking account
Choose an account for the test taker and enter the address

Add or remove a provisioning package

- If an organization wants to prevent users from unenrolling company-owned devices, that can be done through a custom policy. Add the custom policy to a policy group and deploy onto the MDM server. For code, see Custom policy to restrict device users from unenrolling fully-managed (company-owned) devices *(on page 249)*.

Apple

The ability for a user to unenroll themselves is configured in the DEP profile that was applied on the device. While configuring through Configure Automated Device Enrollment Policy page, if the `Is MDM Removable` option is selected, the Apple device user can unenroll. Otherwise, the option is disabled and the user cannot unenroll. After user-initiated unenrollment, the items under the sections Apps and Restrictions become empty.

To unenroll an iPhone or iPad device:

1. Open **Settings** on the device.
2. Go to **General** **> Device Management**.
3. Select the MDM profile.
4. Select **Remove Management**.

To unenroll a macOS device:

1. Open **System Preferences**.
2. Go to the **Profiles** section.
3. Select the main MDM profile.
4. Click the "-" button and follow the prompts to confirm the unenrollment.

Android

Users cannot unenroll company owned devices (New or factory reset devices).

Users can unenroll BYOD Android device by deleting the work profile. To delete your work profile:

1. Go to **Settings** > **Accounts** > **Remove work profile**.
2. Tap **Delete** to confirm the removal of all apps and data within your work profile.
3. Ensure that the policy app ("Device Policy") is uninstalled and not present on your device.

After the work profile is deleted, all local data on the device within that profile is deleted.

You can also remove all apps and data (both personal and work) by factory-resetting your device.

Chapter 15. Extending BigFix management capabilities

BigFix 10 delivers a few significant new functions for enhancing the visibility and management of devices on your network regardless of whether the devices are physical or virtual.

Challenges faced in managing modern IT infrastructures

Managing their infrastructures is growing more and more challenging and complex for IT organizations. With the advent of multiple types of servers, different operating systems, software, cloud computing and services, and technology that is changing almost every minute, it becomes difficult to track, control, and manage the IT environments.

- Technologies such as cloud computing and mobility change the IT landscapes fast and it becomes difficult to stay current.
- Catering to new compliance and regulatory requirements while still complying with the old ones has mandated the need for a cost-effective solution.
- As IT organizations continue to increase operations around latest technologies, security becomes a major concern.
- Sophisticated IT infrastructures that support high computing and data analysis need efficient and cost-effective data extraction and data storage techniques.

BigFix 10 features

To achieve transparency across your heterogeneous IT environments, you need a more automated, comprehensive, and robust solution like BigFix 10. This all-new version of BigFix provides you with an accurate view of the resources in your network, key analytics, and detailed insights that can enable your decision makers to make faster and informed decisions about IT management.

Related information

Managing cloud resources

Managing cloud plugins in WebUI *(on page 324)*

Modern Client Management

Insights

Managing cloud plugins

BigFix 10 Platform includes a plugin for every cloud provider supported, namely Amazon Web Services (AWS), Microsoft Azure, VMware and Google Cloud Platform (GCP). Each of these cloud providers has its own uniqueness, capabilities, and ways to interface with an external program and they handle access to data and capabilities differently.

To be able to install the plugin portal and the cloud plugins, Master Operator (MO) privilege is required.

The multicloud management features are available for use in both BigFix Console and WebUI.

Related information

Installing the plugin portal *(on page 319)*

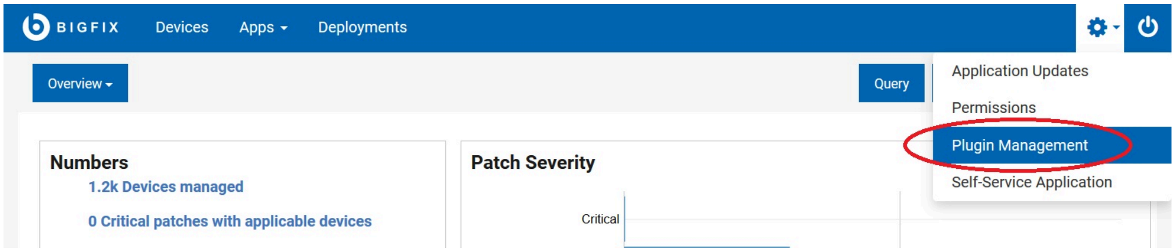
Installing cloud plugins *(on page 320)*

Installing the plugin portal

The Plugin Portal is a new component introduced in BigFix 10 to help manage cloud devices as well as modern devices such as Windows 10 and MacOS endpoints enrolled to BigFix. For details on modern client management, see the Modern Client Management documentation.

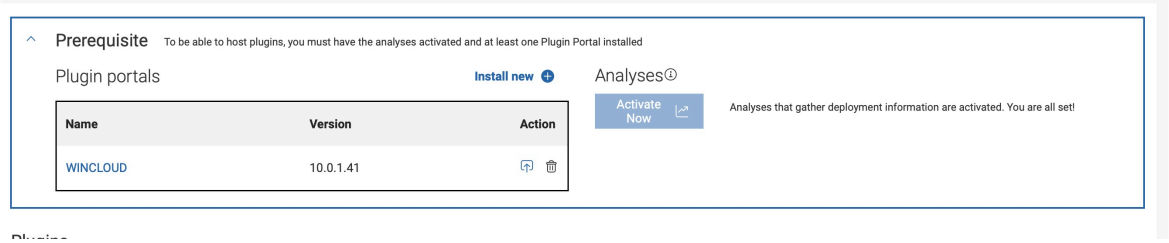
Plugin portal is a scalable component introduced in BigFix 10 for supporting the management of cloud instances and modern clients.

1. Click the gear icon at the top right corner.
2. Click **Plugin Management**.



The Plugin Management page opens.

3. The Preprequisite section helps ensuring the right components are available and started in order to proceed with the Plugins installation.



To be able to host plugins, you must have the analyses activated and at least one Plugin Portal installed

Name	Version	Action
WINCLOUD	10.0.1.41	

Analyses that gather deployment information are activated. You are all set!

a. Install a new plugin portal if you have not done so yet.
   - Click Install in the Plugin portals section. The Install BigFix Plugin Portal opens.
   - Click **Deploy Content**.

b. Check if Analyses have been activated. If not, press the button to ensure that the discovered data are reported correctly in the BigFix database.

Installing cloud plugins

Install and manage cloud plugins.

To install cloud plugins, complete the following steps.

1. Click **Install new** in the Plugins section. Choose the provider in the dropdown menu.
2. The Install cloud plugin page opens. There are two or more sections, each one includes configuration parameters.
3. The **General** section displays.
4. Specify the Hosting Portal.
5. Specify a value, in minutes, for the Discovery frequency.
6. The **Provider specific settings** section displays. This section is for AWS only and here you must specify the default region.
7. The **Authentication** section displays.
8. While installing the plugin, one credential set must be specified. Over time you can add as many as you need. See the Working with cloud plugins *(on page 324)* section. Each credential has a label for easier management, enter a name you can use to retrieve the credential and simplify the management. The field is named **Account label**. Depending on which cloud provider you are using (AWS, Azure, VMware or GCP), the list of the following required parameters changes.
    - If you specified Microsoft Azure as Cloud Provider , you must enter the following information: Tenant ID, Subscription ID, Client ID (Application ID) and Password (Client Secret).
    - If you specified vSphere as Cloud Provider, you must enter the following information : vCenter Server, Username, Passoword.
    - If you specified GCP you must enter the service account key by uploading the .json file you receive from your GCP cloud administrator.
    - If you specified AWS the authentication parameters are: AWS user region, Access key ID, secret access key. To simplify maintenance of the credentials, BigFix allows you to optionally add roles that this credentials can use in order to execute actions in the cloud through the API such as the discovery. By leveraging roles, you can simplify and shorten the list of credentials to be used and configured in the AWS plugin. This is only possible if you have this configuration in place in AWS. In addition, for each role an external ID can be also specified. For more details on the usage of roles and external IDs, refer to the AWS documentation. To add roles and external IDs simply press the **Add new** button and a table is displayed where you can input the values in the rows. Roles must be specified with their fully qualified name (for example "arn:aws:iam::123456789012:root"). You can add as many as you need.
9. The **Advanced Settings** section displays.
10. Microsoft Azure and AWS have an advanced settings section, where you can specify:
    - For Microsoft Azure, the Log Path and Log verbose.
    - For AWS, in addition to the logging information, you can also specify the proxy settings such as proxy url, proxy username and proxy password.
11. Click **Install**.
12. Click **Install**.

IAM roles support

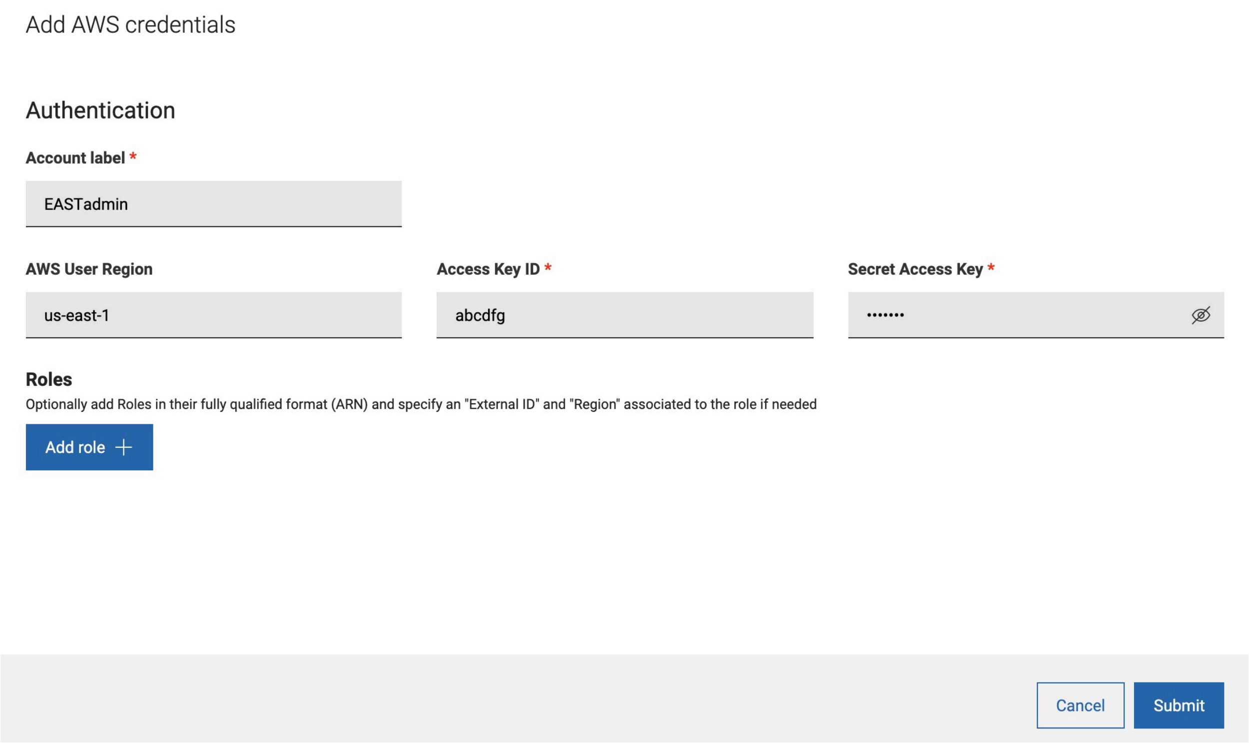
With version 10.0.4, BigFix has introduced the support of IAM roles to simplify the management of AWS credentials.

In fact, BigFix can discover cloud instances based on what provider specific credentials are entitled to see or manage. This means that potentially a very large number of credentials need to be specified in the Plugin settings, with the related burden of keeping them current. Having the possibility to also use roles, this number significantly decreases since BigFix will start discovering by impersonating those roles and as such avoiding the need for multiple credentials to be managed since the discovery will be based on roles.

Of course in this case, the AWS cloud needs to be configured so that some users are given multiple roles to be able to discover the entire cloud environment. The roles must be provided to BigFix in their fully qualified name, called ARN (Amazon Resource Name). These information are usually exchanged between the Cloud administrator and the BigFix MO.

Note: Once AWS Roles are inserted, the AWS plugin will use them during its discovery, instead of the credential from which they derive. You must ensure that these roles include all the AWS devices that you want to discover in your cloud environment: otherwise, some machines may not be discovered.

For AWS, here is how the user can specify the roles while installing the plugin or when adding / editing credentials:



Add AWS credentials

Authentication

Account label *

EASTadmin

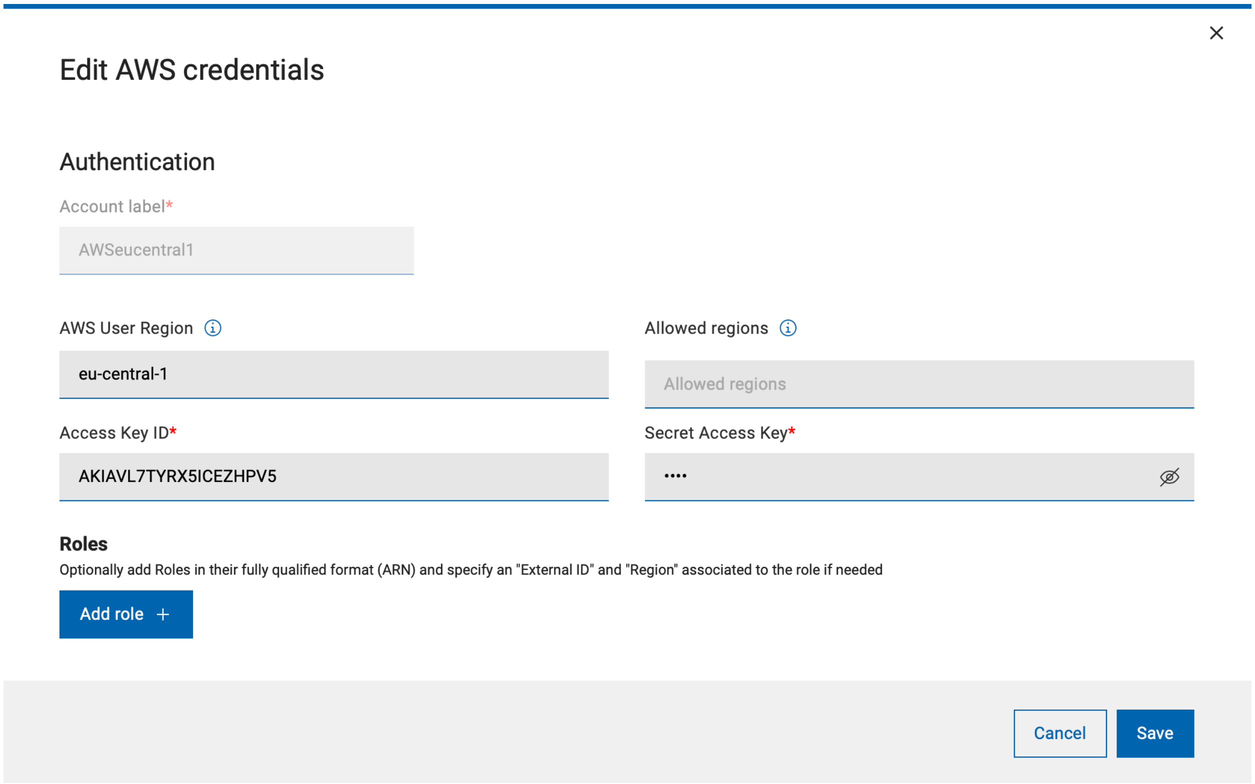
AWS User Region	Access Key ID *	Secret Access Key *
us-east-1	abcdfg	•••••••

Roles

Optionally add Roles in their fully qualified format (ARN) and specify an "External ID" and "Region" associated to the role if needed

By pressing **Add role**, a table is displayed to include the fully qualified ARN for the role, an External ID if provided by the cloud administrator and a default region, required by the AWS APIs, to start the discovery. All of these fields are optional but if External ID or Region is specified, they must have an ARN.

With BigFix Platform version 10.0.5, user can also limit scan at credential level.



Edit AWS credentials

Authentication

Account label*: AWSeucentral1

AWS User Region: eu-central-1

Allowed regions: Allowed regions

Access Key ID*: AKIAVL7TYRX5ICEZHPV5

Secret Access Key*: ••••

Roles

Optionally add Roles in their fully qualified format (ARN) and specify an "External ID" and "Region" associated to the role if needed

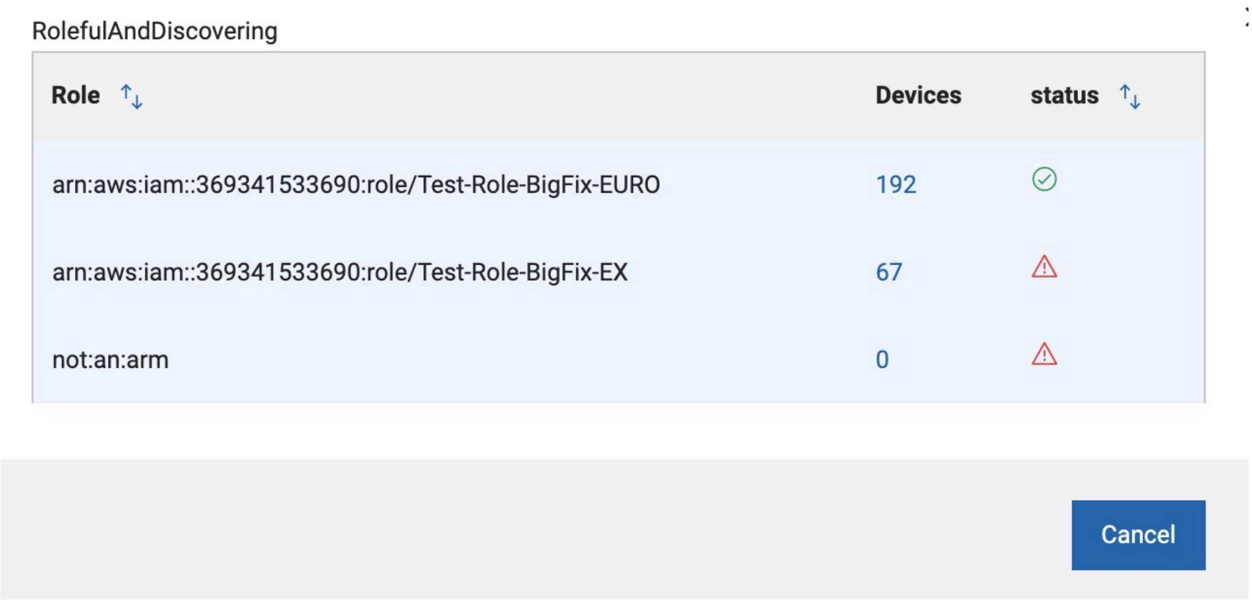
Once the plugins are installed, the main **Plugin Management** page can be used to keep under control the plugins behavior.

Each provider has a dedicated horizontal tab, and once in the tab the sidebar on the left will have one entry per plugin, if in your environment there are multiple portals, therefore multiple plugins. In fact, there can be only one plugin of a specific provider installed on each portal.

The icon next to the plugin name is a quick indicator whether the plugin is working properly or not. In case there is a yellow or red icon, go to the **Authentication** table to spot the credential set that is causing troubles.

The table includes the credential information, the roles if specified, the status, number of devices discovered using the credentials, possibility to edit and to remove.

The “eye” icon opens a modal window with details on the roles.

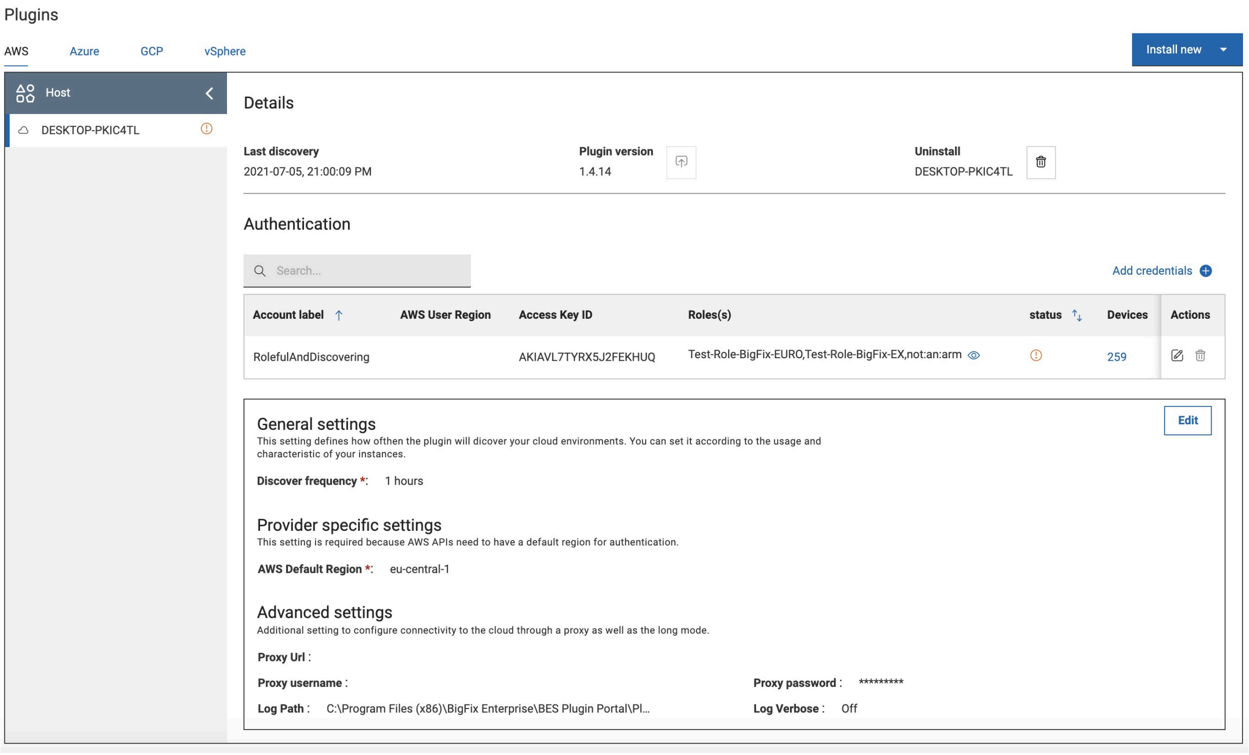


RolefulAndDiscovering

Role ↑↓	Devices	status ↑↓
arn:aws:iam::369341533690:role/Test-Role-BigFix-EURO	192	✓
arn:aws:iam::369341533690:role/Test-Role-BigFix-EX	67	⚠
not:an:arm	0	⚠

The page includes information such as:

- Last time a discovery was performed.
- The plugin version plus possibility to upgrade if a new version is available.
- Possibility to uninstall the Plugin.



Details

Last discovery
2021-07-05, 21:00:09 PM

Plugin version
1.4.14

Uninstall
DESKTOP-PKIC4TL

Authentication

Account label ↑	AWS User Region	Access Key ID	Roles(s)	status ↑↓	Devices	Actions
RolefulAndDiscovering		AKIAVL7TYRX5J2FEKHUQ	Test-Role-BigFix-EURO,Test-Role-BigFix-EX,not:an:arm	!	259	

General settings

This setting defines how ofthen the plugin will dicover your cloud environments. You can set it according to the usage and characteristic of your instances.

Discover frequency *: 1 hours

Provider specific settings

This setting is required because AWS APIs need to have a default region for authentication.

AWS Default Region *: eu-central-1

Advanced settings

Additional setting to configure connectivity to the cloud through a proxy as well as the long mode.

Proxy Url :

Proxy username :

Proxy password : *********

Log Path : C:\Program Files (x86)\BigFix Enterprise\BES Plugin Portal\Pl...

Log Verbose : Off

After the initial installation, more credentials can be added or existing credentials can be edited or removed. In the **General settings** section, provider specific information such as discovery frequency, logging and proxy can be set.

Working with cloud plugins

If you have the cloud plugins enabled and they have discovered cloud instances in your environment, you can access those cloud devices from the Devices page and work with them.

The **Devices** page enumerates all the devices in your environment, indicates whether they are physical or virtual, how many in either category, and whether they have BigFix agent installed or not.

The data grid view can be customized easily and columns can be added / removed / reorganized.

The objective of device correlation is to avoid duplication of resources and streamline the device management. When BigFix discovers devices on the cloud (either private or public), it determines whether these are already known or tracked in the system. The advantage of asset correlation is that if there are multiple representations of a single endpoint, they are all aggregated and presented on the **Devices** page as a single endpoint. You as an operator can then select any group (of such representations) to target actions, and then any representation within the group as target for each specific action. You can also limit the operators' access to only manage specific representations of a device.

After installing the cloud plugins and discovering the cloud resources, you can see the summary of your cloud devices in WebUI Overview under Cloud Dashboard. To view the Cloud Dashboard, click the **Overview** button beneath the navigation bar and select **Cloud Dashboard**. This dashboard contains tiles for monitoring the amount of cloud resources in your environment, with or without an agent installed, and their distribution by type and region. Click any bar chart to open the Devices page, which lists that subset of resources, where the filters BigFix Agent Status and Managed by are pre-selected.

As a BigFix Operator, you can view the Device document. Device document provides information gathered from various sources.

If it is a cloud instance, you see data related to cloud as well on this page. To narrow down the search to cloud devices, you can use filters such as BigFix Agent Status (Installed or Not installed) or Managed by (Cloud and which Cloud provider).

Plugin settings

The following configurations are set using the `SetPluginSettingsIntoStore` function exported by the Plugin Portal common header. These settings retrieve all the plugin store settings that are used to populate the console dashboards and the dashboard in WebUI.

Table 18. SetPluginSettingsIntoStore Settings

Plugin Name	Description
`Credentials_LoginSuccess`<useralias>	Avoids credential locking if lockout policies are in place.

Table 18. SetPluginSettingsIntoStore Settings (continued)

Plugin Name	Description
	Values: Set to “1” when the login succeeds. Set to “0” if the cloud provider refuses the credentials. For example, HTTP error 401 sets this setting to “0” that indicates that a password is no longer valid. If the login fails for something different form HTTP 401 (for example, network error or any other HTTP error code) nothing is set.
`Discovery_LastScan`	Contains the timestamp (unix time) of the last discovery attempt.
`Discovery_LastScanNoErrors`	Contains the timestamp (unix time) of the last discovery attempt completed with no errors. This is to support multicredentials. For example, if you have 10 credential sets, the discovery is attempted for each one. If one credential set fails due to password expiration, the `LastScan` is set because one discovery is already done, but `LastScanNoErrors` is not set. If no error occurred, `LastScanNoErrors` and `LastScan` are set to the same value.
`Discovery_LastError`	Contains the last error message (whatever it is) that a full discovery finds during its execution. It is reset when the full discovery terminates with no errors. In other words, this is set if `LastScanNoErrors` != `LastScan`; this is set to “” when `LastScanNoErrors` == `LastScan.`

Limit AWS Regions to restrict the scope of device discovery

AWS organizes the data centers and virtual instances by region. This property of a cloud instance is reported in AWS Region by the `Amazon Web Services Resources` analyses.

AWS Region

An AWS Region is a collection of AWS resources in a geographic area. The resources that you create in one Region do not exist in any other Region unless you explicitly use a replication feature offered by an AWS service. When you enable a Region, AWS performs actions to prepare your account in that Region. For more information, see the AWS official documentation at https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

Limit scan regions

For faster discovery, it is recommended to limit scanning only the AWS regions that you use. If not specified, after logging into the cloud environment, discovery is performed to all the AWS managed regions retrieved in the login phase, regardless of the authority that the additional credentials defined in the plugin have for the various regions.

For example, if the IAM User credentials specified at plugin install time have authority only to access `us-west1` region, when the plugin logins, it tries to retrieve all the AWS account managed regions and starts the discovery. At this point, the AWS plugin tries to use the IAM User credentials to login to all AWS managed regions. This causes failed logins as the credential is not authorized to access any regions other than `us-west1`.

BigFix Platform 10.0.5 introduces the possibility to limit the regions that are used for discovery through the parameter Allowed regions. If specified, it restricts the scope of the discovery, optimizing the network traffic and minimizing errors.

You can customize Allowed region setting by editing the AWS settings or by adding new AWS credentials.

The following table summarizes the usage of parameters and what happens if not specified.

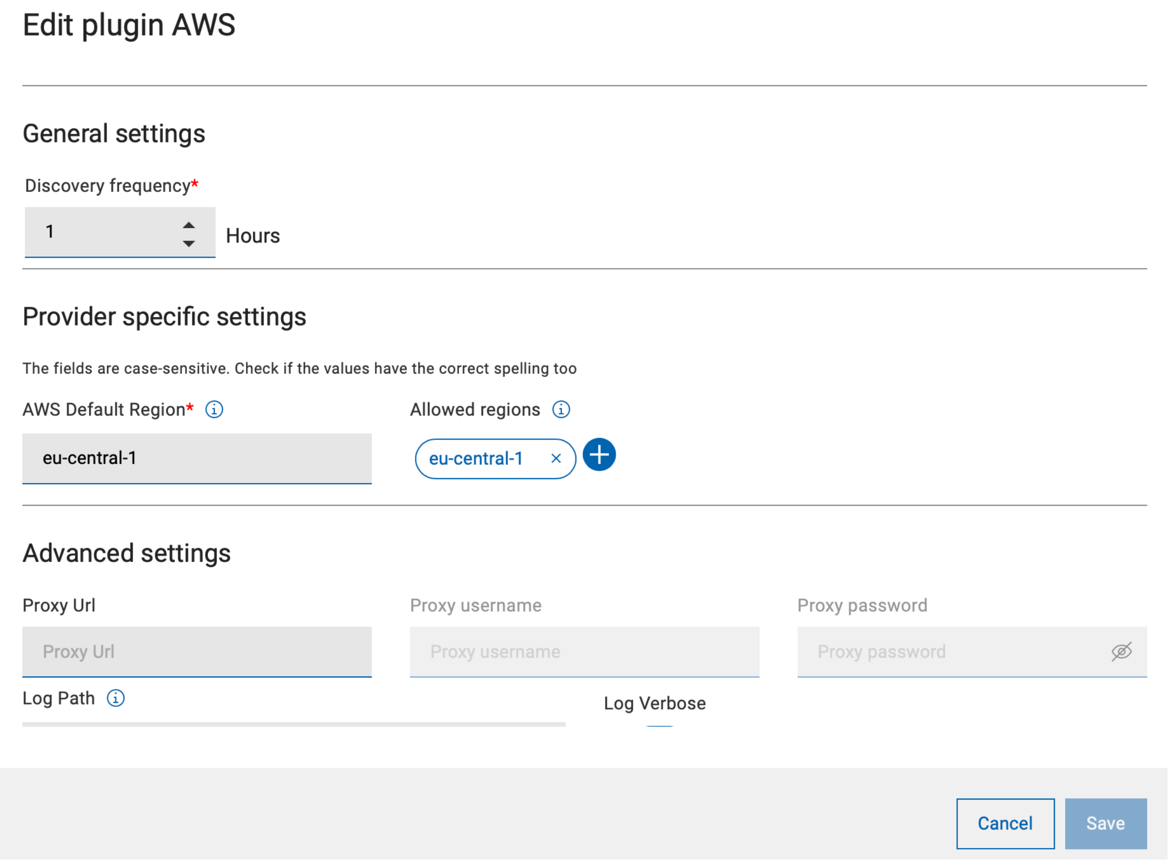
Applicability	Parameter name	Used for	What if not used?
PLUGIN	**AWS Default region ***	Login (to open the session through API)	MANDATORY at install time
	Allowed regions (1)	Narrows down the scope of the plugin discovery by listing the only regions where the discovery should run among the complete list of entitled regions for the users	Discovery spans every managed region
ACCOUNT LABEL	**AWS User region** (Regions for account label)	Login and, if specified, overrides **AWS Default region**	**AWSDefaultregion** Is used instead
	Allowed regions (for account label)	Overrides Plugin **Allowed regions**(1) if present Narrow down the scope of the account discovery by listing the only regions where the discovery should run among the com-	Plugin **Allowed regions**(1) is used

		plete list of entitled regions for the users	
	Region (Role region)	Used for login and it overrides **AWS User region** and **AWS Default region** in cascade	**AWS User region** or in cascade **AWS Default region** is used

Limit AWS Regions at plugin level

To set AWS regions at plugin level, complete the following steps:

1. Click the **AWS** tab.
2. In the **Plugin Management** page, edit the plugin **General settings**



Edit plugin AWS

General settings

Discovery frequency* 1 Hours

Provider specific settings

The fields are case-sensitive. Check if the values have the correct spelling too

AWS Default Region*: eu-central-1

Allowed regions: eu-central-1

Advanced settings

Proxy Url: Proxy Url

Proxy username: Proxy username

Proxy password: Proxy password

Log Path

Log Verbose

.

- Add one or more regions to limit the discovery. The added regions are listed as pills.

  Important: Enter the correct spelling for the region names, because BigFix cannot check the name of the region for correctness. Refer name and code of AWS Regions.

- You can also remove a region easily.

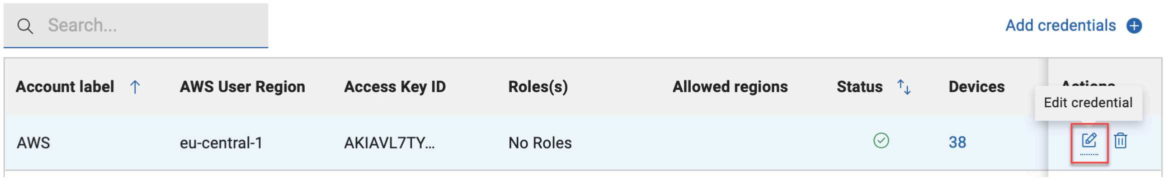
After you have added all the regions you want, click **Save**. This deploys the Fixlet to apply the configuration change.

Limit AWS Regions at credential level

To limit AWS Regions at credential level, complete the following steps:

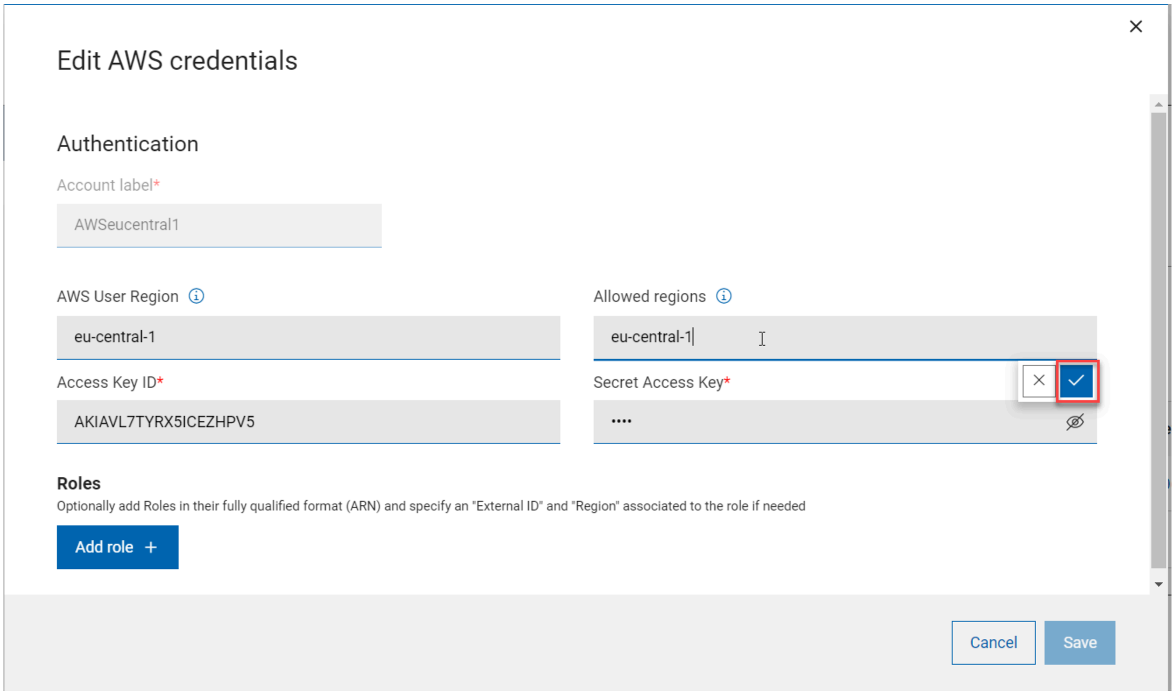
1. In the Authentication table, click **Edit credential** in the specific credential line.

   Authentication



Account label	AWS User Region	Access Key ID	Roles(s)	Allowed regions	Status	Devices	Actions
AWS	eu-central-1	AKIAVL7TY...	No Roles		✓	38	

2. On the **Edit AWS credentials** page, enter AWS Region and click the tick mark to add it. Add one or more regions as needed.



Edit AWS credentials

Authentication

Account label*: AWSeucentral1

AWS User Region: eu-central-1

Allowed regions: eu-central-1

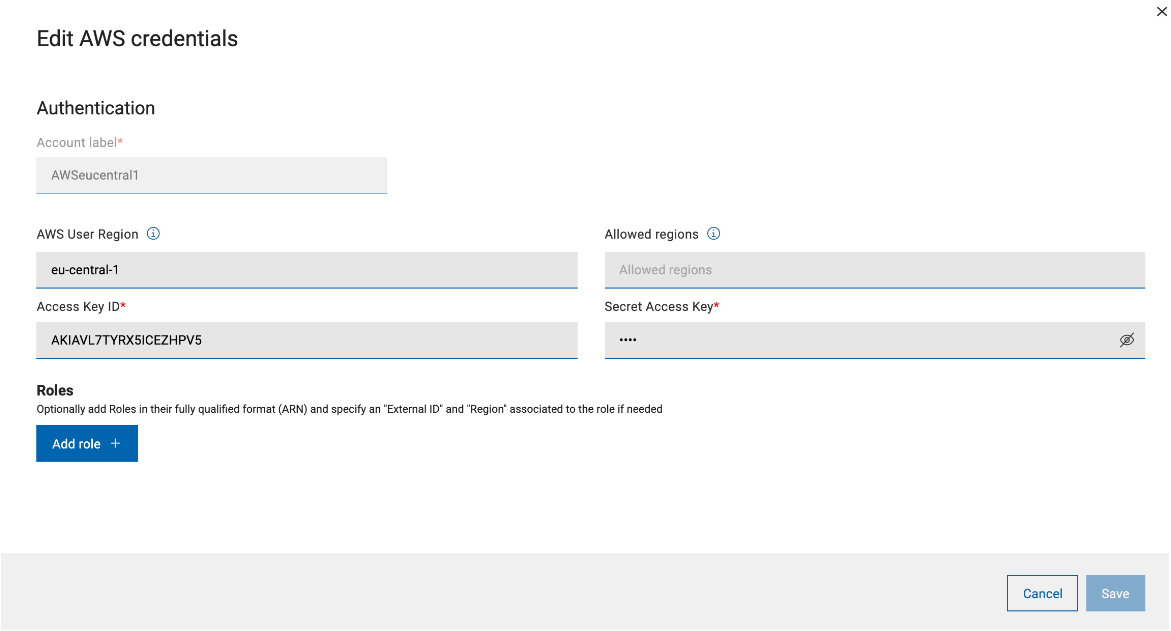
Access Key ID*: AKIAVL7TYRX5ICEZHPV5

Secret Access Key*: ••••

Roles

Optionally add Roles in their fully qualified format (ARN) and specify an "External ID" and "Region" associated to the role if needed

- **Important:** Enter the correct spelling for the region names, because you cannot check the name of the region for correctness.
- You can also remove a region easily as needed by clicking ‘x’ mark.



Edit AWS credentials

Authentication

Account label*

AWSeucentral1

AWS User Region: eu-central-1

Allowed regions: Allowed regions

Access Key ID*: AKIAVL7TYRX5ICEZHPV5

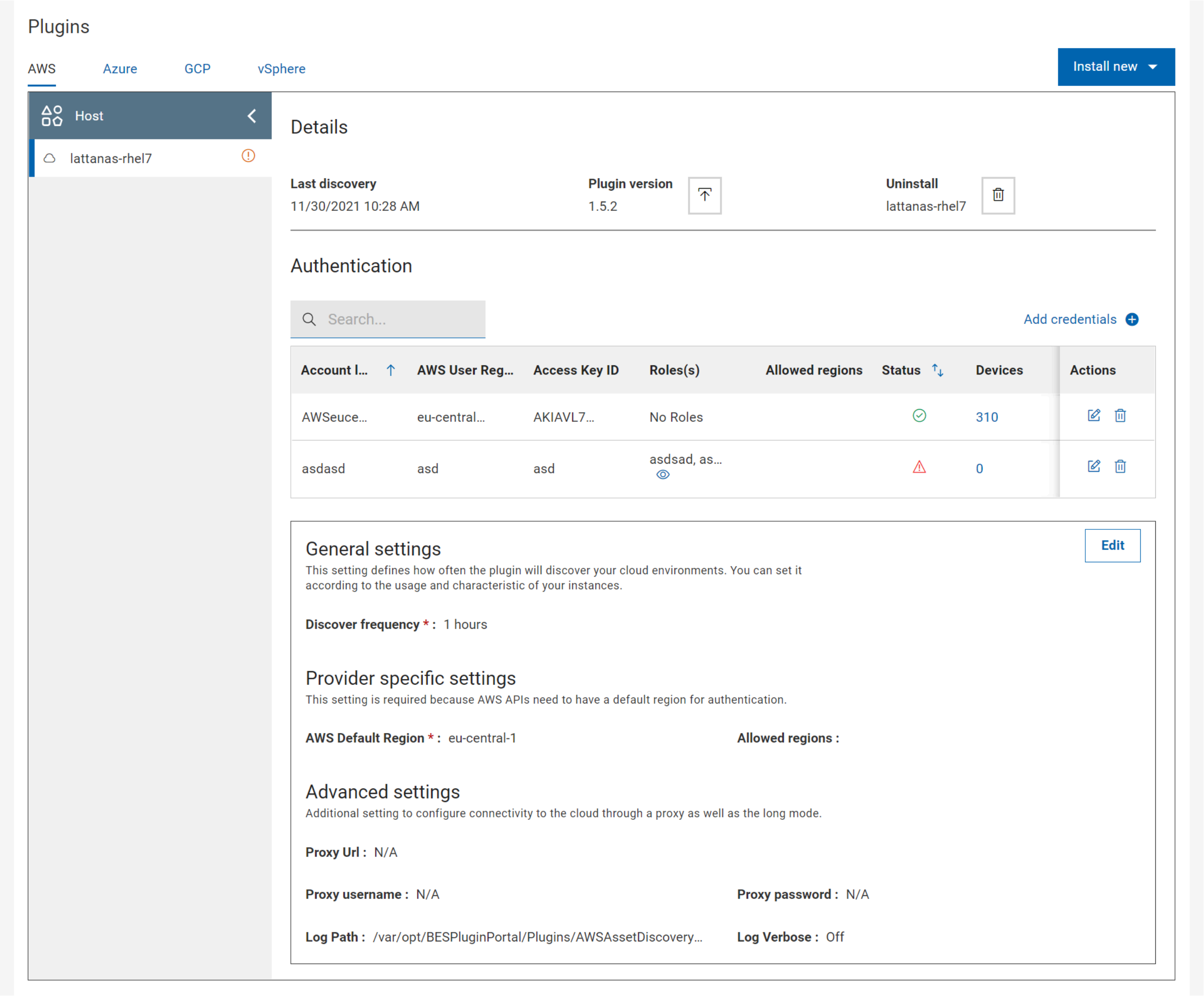
Secret Access Key*: ••••

Roles

Optionally add Roles in their fully qualified format (ARN) and specify an "External ID" and "Region" associated to the role if needed

3. After you have added all the regions you want, click **Submit**. This deploys the fixlet to apply the configuration change.

When changes are applied, they are visible in the related section of the AWS plugin tab, either in the Authentication table column "Allowed regions" or in the General Settings section.



Details

Last discovery 11/30/2021 10:28 AM

Plugin version 1.5.2

Uninstall lattanas-rhel7

Authentication

Account I...	AWS User Reg...	Access Key ID	Roles(s)	Allowed regions	Status	Devices	Actions
AWSeuce...	eu-central...	AKIAVL7...	No Roles		✓	310	
asdasd	asd	asd	asdsad, as...		⚠	0	

General settings

This setting defines how often the plugin will discover your cloud environments. You can set it according to the usage and characteristic of your instances.

Discover frequency * : 1 hours

Provider specific settings

This setting is required because AWS APIs need to have a default region for authentication.

AWS Default Region * : eu-central-1

Allowed regions :

Advanced settings

Additional setting to configure connectivity to the cloud through a proxy as well as the long mode.

Proxy Url : N/A

Proxy username : N/A

Proxy password : N/A

Log Path : /var/opt/BESPluginPortal/Plugins/AWSAssetDiscovery...

Log Verbose : Off

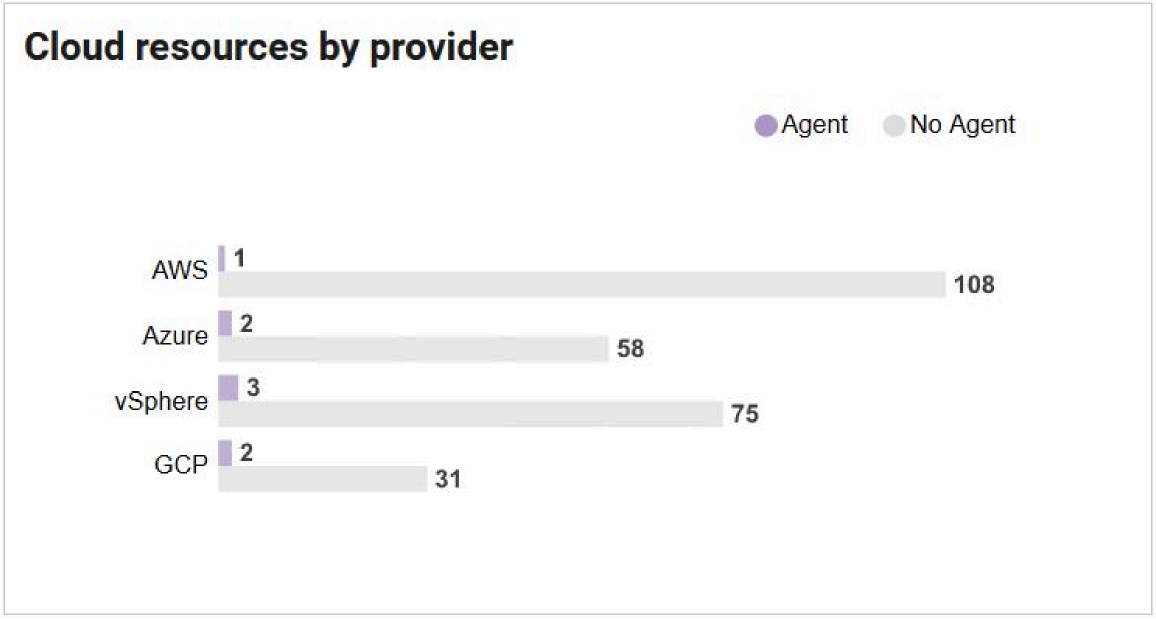
Installing BigFix Agent on cloud discovered devices

From BigFix WebUI, you can install the BigFix Agent code on the devices that have been discovered by cloud plugins.

- You can install BigFix Agent on the cloud discovered devices if only they have Windows or Linux x86 64bit Operating System.
- You need to have a CDT infrastructure set up. CDT documentation and log files can also be used for troubleshooting. For more information, see https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Installation/c_using_the_cdt.html

WebUI leverages the Client Deployment Tool (CDT) technology that is already available in BigFix. Compared to the CDT wizard, WebUI offers a simplified and streamlined process. To deploy BigFix Agent through WebUI perform the following steps:

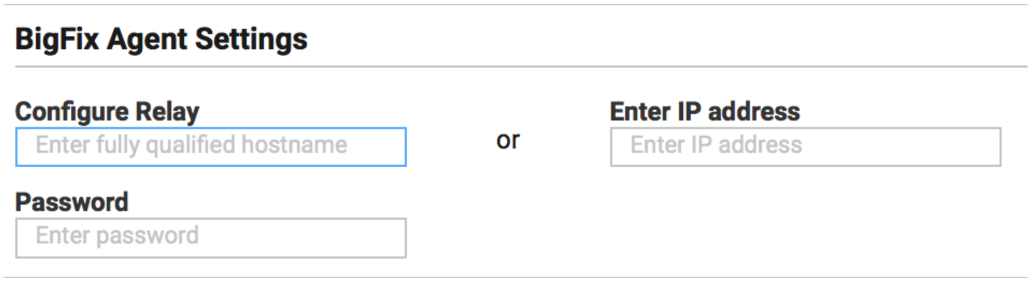
1. From the landing page of the WebUI, click **Overview** and from the dropdown menu select **Cloud Dashboard**.
2. The **Cloud resources by provider** dashboards summarizes all the devices discovered with and without the BigFix Agent. Click on the bar that represents the devices without BigFix Agent that belong to a desired cloud provider.



   Now, the **Device** *(on page 23)* page is displayed filtered by the following properties:
    - **Managed by**: <the selected cloud provider>
    - **BigFix Agent Status**: `Not installed`
3. Select one or more devices from the filtered list in which you want to install the BigFix Agent.
4. Click the **Deploy** dropdown button and select **Deploy BigFix Agent**. Now, you can customize the parameters required to install the BigFix Agent through the existing CDT infrastructure. Before specifying the settings, you can still revise and modify the list of target devices by clicking the **Edit Devices** button on top right of the page.

   Deployment settings

   BigFix Agent Settings: This setting is optional, and it is related to the relay connection. If not specified, once the BigFix Agent starts, it connects to the root server or top level Relay, according to the deployment configuration. If a Relay is specified, either with the hostname or the IP, there is also the possibility to include the password in case the selected Relay is configured for authentication.



BigFix Agent Settings

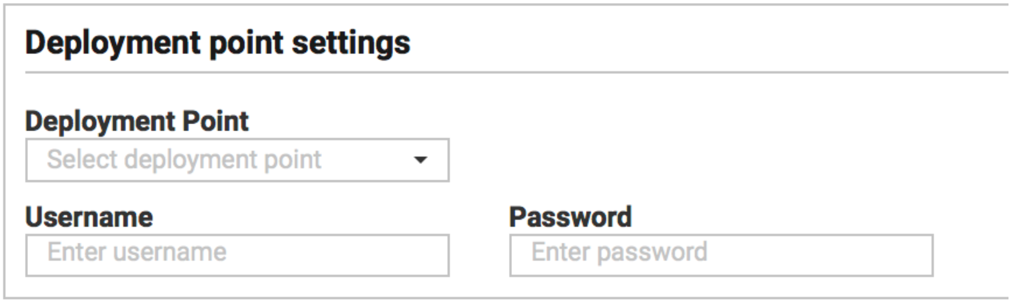
Configure Relay: Enter fully qualified hostname

or

Enter IP address: Enter IP address

Password: Enter password

Deployment point settings: This setting enables you to choose the CDT Deployment Point (among the available Windows Deployment points) from which you want to distribute the agent code to the targets.



Deployment point settings

Deployment Point: Select deployment point

Username: Enter username

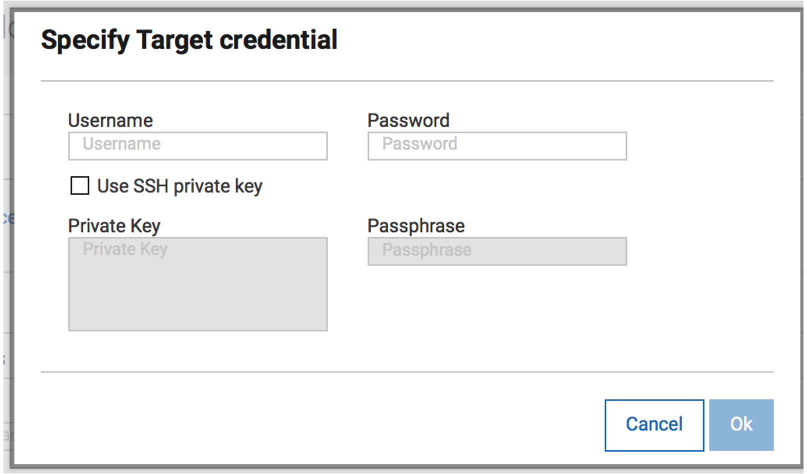
Password: Enter password

Note: You can have only one Deployment Point for all the distributions. You cannot assign multiple Deployment points to different buckets of targets. Username and Password of the computer is also required.

When you select the Deployment Point, ensure that the target device and the deployment point ping each other (can connect), because unlike the CDT wizard in the BigFix Console, here it is not possible to set a proxy to guarantee the communication.

The process installs a predefined version of the BigFix Agent. If newer versions are available, agent can then be upgraded via the usual upgrade fixlets available in BigFix Support site.

Specify Target credentials: This setting enables you to set credentials for the target machines to allow the installation of the BigFix Agent code. You can select multiple devices at the same time and assign the same credentials (if required) or do it one by one to assign different credentials. Devices are identified by their IPs (this is why even if you have selected computers by names, CDT connects to these devices through the IP). If the computer has multiple IPs, CDT tries to connect to all of them until the first response.


Specify Target credential

Search field lets the user to look for a specific machine in this list, if needed.

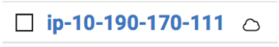
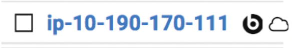
Once the selection is done, click **Set credentials** to include either the username/password combination or an SSH private key in the popup.

5. Once all the required configuration is done, click **Deploy** button to begin the deployment.

   Now, the **Deployment** page appears to indicate the status of the action to start CDT processing.

   Note: When this action is successful, it only means that the CDT has successfully started the process and not that the agent is successfully installed on the target devices.

   Once BigFix Agent is successfully installed on the devices:

   - The devices connect to the BigFix Server through the BigFix Agent
   - The device entries are correlated with the existing ones related to the cloud discovery
   - The visualization of the device in the Device page canges from showing cloud icon to showing BigFix logo and cloud icon. For example,  ☐ ip-10-190-170-111 to  ☐ ip-10-190-170-111

You can also install the BigFix Agent on cloud devices from the Devices page by carefully selecting the appropriate **Managed by** and **BigFix Agent Status** filters.

Note: The system returns an appropriate error message:

- If you choose a mixed set of cloud discovered and MDM devices to the deploy BigFix Agent.
- If you choose a device that already has a BigFix Agent installed and if you try to deploy BigFix Agent through the Deploy dropdown action.

Installing the BigFix agent on cloud-native devices

From BigFix WebUI, you can install the BigFix agent on the AWS and Azure environments and use the cloud provider services.

This task is available starting with BigFix Platform Version 10 Patch 2. You must install this patch before you start this task.

WebUI uses native cloud API services.

To deploy the BigFix agent through the WebUI:

1. From the landing page of the WebUI, click the gear icon at the top right corner and from the dropdown menu select **Install Agent**.
2. The **Install BigFix agent** page displays allowing you to install the agent on devices already discovered and registered in BigFix using one of the available installation methods:

   AWS native API

   This method deploys the agent using the Amazon Web Services native cloud API services and requires AWS access with execution privileges.

   Azure native API

   This method deploys the agent using the Microsoft Azure native cloud API services and requires Azure access with execution privileges.

   Note: These choices are displayed in brackets and link to the devices that meet these criteria:

   - Devices that are relevant to the installation Fixlet.
   - Devices that satisfy the prerequisites required by the installation.

   You might have more devices discovered in your cloud platforms but, without the prerequisites needed for leveraging the native API services, they are not displayed.

Note: For more details about the native agent installation errors (exit codes) and suggested actions, see BigFix Agent installation on cloud resources.

Agent installation from the Devices page

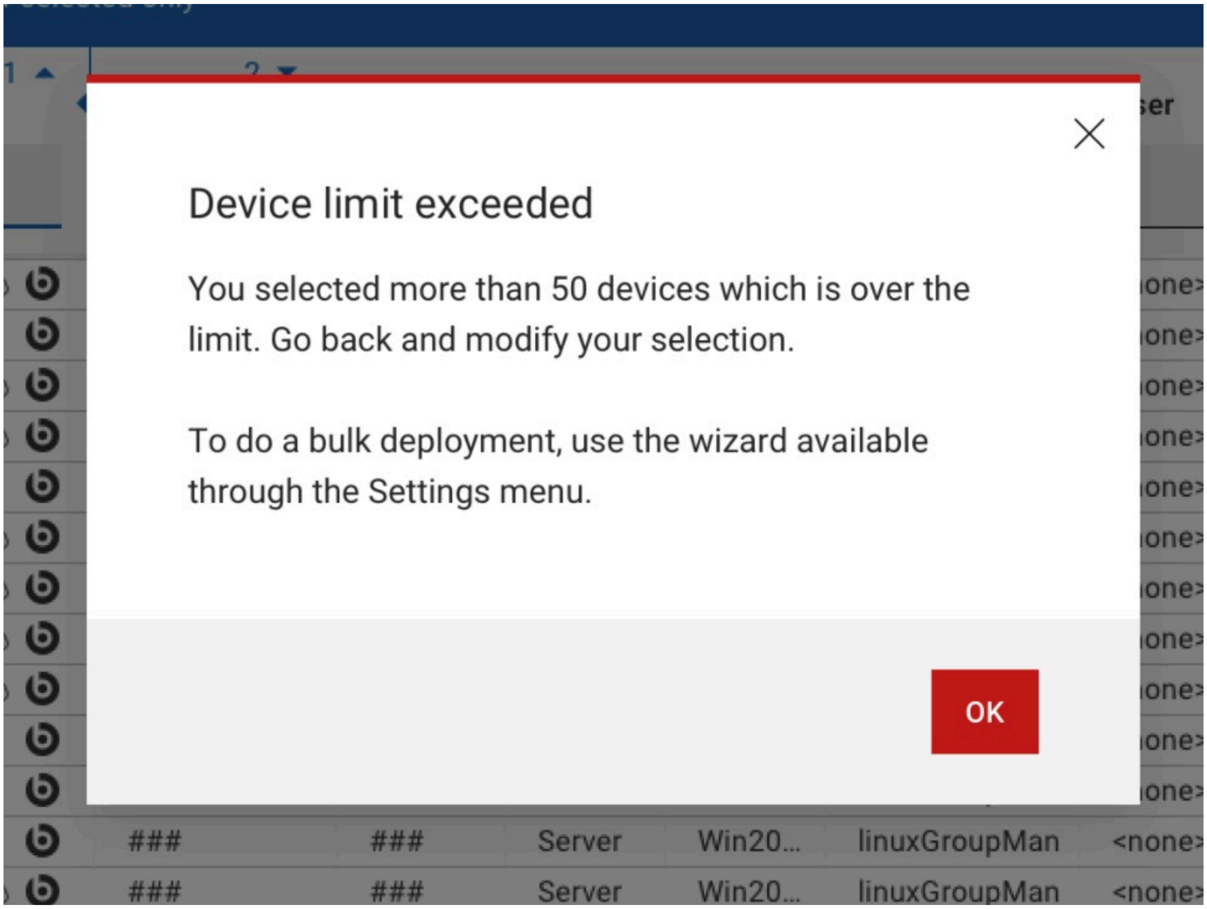
After you select devices, you can install the agent from the **Administration** menu of the Devices page.

Under **Administration**, select **Install Agent**.

Depending on the combination of the devices that you selected, some messages are displayed, that warn you about or prevent you from completing the action.

Scenario 1

You selected more than 50 devices. For the best performance, use the wizard instead and the action is not submitted.



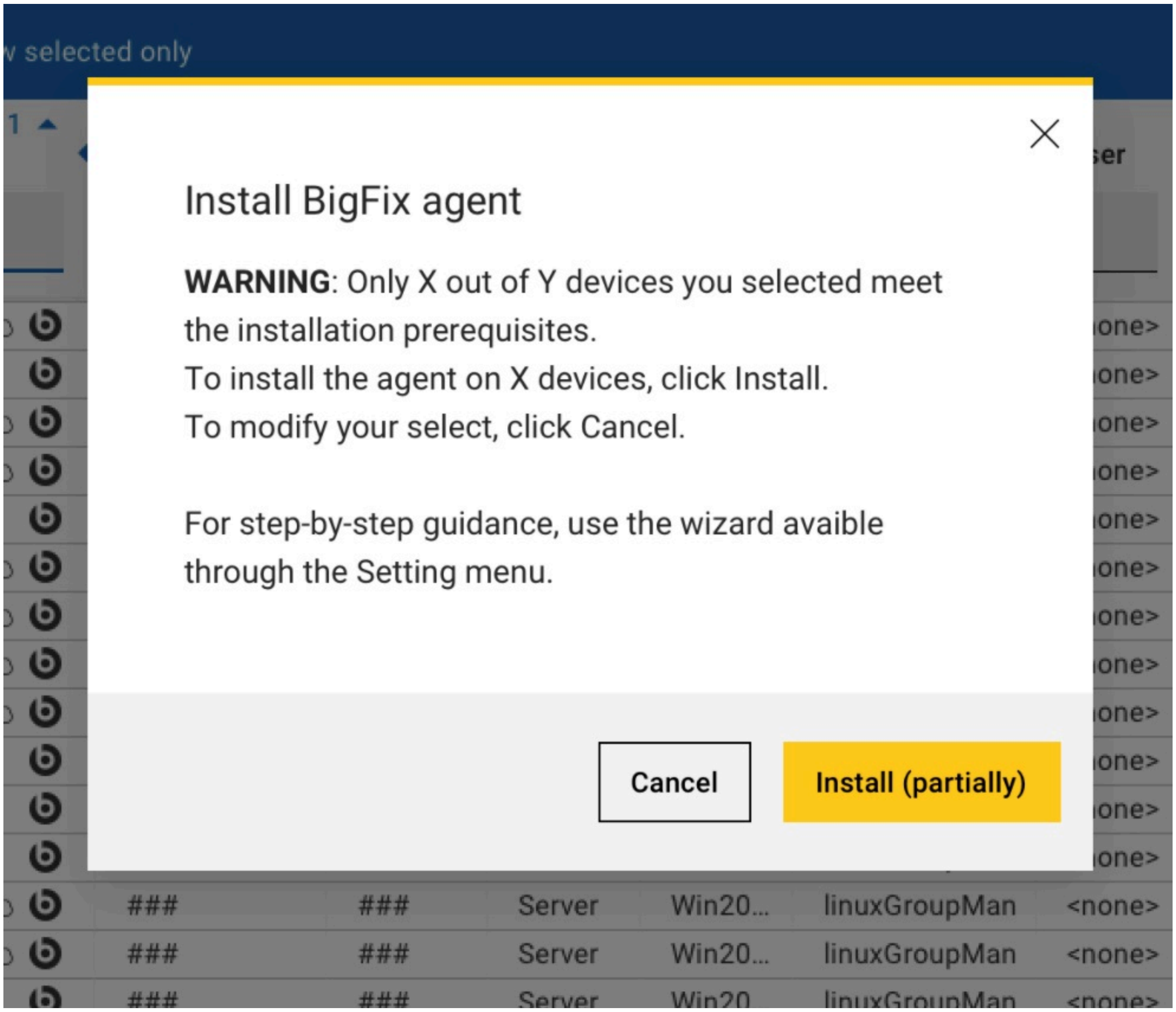
Device limit exceeded

You selected more than 50 devices which is over the limit. Go back and modify your selection.

To do a bulk deployment, use the wizard available through the Settings menu.

Scenario 2

Only a subset of the devices that you selected meet the prerequisite for a native installation. Therefore, when you run the action, it is submitted against only a subset of devices.



Install BigFix agent

WARNING: Only X out of Y devices you selected meet the installation prerequisites.
To install the agent on X devices, click Install.
To modify your select, click Cancel.

For step-by-step guidance, use the wizard avaible through the Setting menu.

Scenario 3

The devices that you selected are mixed. For example, you selected devices that MDM and Cloud manage. In this case, the WebUI blocks the installation of those mixed devices that do not already have an agent installed.

Appendix A. Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

Terms and conditions for product documentation

Applicability

Personal use

Commercial use

Rights

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.