BigFix
UI User's Guide

Special notice

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

Contents

Chapter 1. Introduction..... 5

Known limitations..... 7

Chapter 2. Getting Started..... 10

Access and security..... 10

Navigating BigFix UI..... 26

Common Functionalities..... 28

Managing Filters..... 35

Manage Reports..... 42

Managing Tags..... 51

Prescriptive Guidance..... 55

Notification Center..... 58

Chapter 3. Using BigFix UI..... 69

Home..... 69

Explore..... 76

Devices..... 77

Fixlets..... 145

Deployments..... 181

Software..... 193

Sites..... 194

Surveys..... 213

Analyses..... 214

Resolve..... 240

Custom Remediation..... 241

CyberFOCUS..... 277

DEX..... 308

Workflow Builder..... 309

Fixlet Streams..... 311

Integrated Vulnerability..... 350

Patch..... 352

Security Compliance..... 353

License Reclamation.....354
Reporting.....355
All Reports.....355
Scheduled Reports.....366
Report Builder.....384
Scripted Reports.....424
Administration.....433
Application Configuration.....433
Identity management.....447
System configuration.....514
Appendix A. Support.....526
Notices.....dxxvii

Chapter 1. Introduction

BigFix UI is a unified interface that consolidates multiple BigFix capabilities into one modern application. It provides IT operations and security teams with a centralized workspace to manage endpoints, remediate vulnerabilities, and generate reports.

Instead of switching across multiple consoles, you can navigate all essential BigFix features from a single, streamlined UI. When you sign in, the customizable **Welcome to HCL BigFix** home dashboard shows widget cards for the applications and reports that you use most, and the notifications bell in the header alerts you to events raised by your work across the application.

BigFix UI organizes capabilities into four main areas: Explore, Resolve, Reporting, and Administration. This structure helps you move easily between day-to-day endpoint operations, vulnerability management, reporting, and user access tasks.

Explore

Explore gives you a central view of your core BigFix resources. For more information, see Explore *(on page 76)*.

- **Devices** – View, filter, and manage endpoints. Configure properties such as maintenance windows and initiate actions. From the Device Details page, you can also open a remote control session or send a message to a device. You can also group devices into static or dynamic device groups.
- **Fixlets** – Browse and deploy Fixlets such as operating system patches, application updates, or configuration changes. You can also create, edit, and delete your own custom Fixlets.
- **Deployments** – Track the status of active, stopped, or completed deployments, assign tags to deployments, and review the details of each deployment.
- **Software** – Deploy and manage software across all endpoints in your network, with full control, audit visibility, and end-user self-service.
- **Sites** – Review the public and custom sites in your deployment, check how many devices subscribe to each site, and create custom sites to host your own content.
- **Surveys** – Create and track surveys that collect feedback from endpoint users about their digital experience, review the status and score of each survey, and deploy a survey to devices.
- **Analyses** – Collect and review device data. Create analyses, set the devices they apply to, and manage the properties that each analysis reports.

Resolve

Resolve provides the tools to act on identified issues and apply remediation across your environment. For more information, see Resolve *(on page 240)*.

- **Custom Remediation** – Create and run ad hoc remediation actions tailored to your environment, such as deploying a script, installing software, or updating the Windows registry.
- **CyberFOCUS** – Assess exposure using the CISA KEV and MITRE APT reports, and start a remediation flow from the findings.

- **DEX** – Monitor Digital Employee Experience (DEX) scores and historical trends across your environment.
- **Fixlet Streams** – Automate recurring patching by creating streams that deploy Fixlets on a defined schedule, and run ad hoc remediation for urgent issues.
- **Integrated Vulnerability Remediation** – Correlate vulnerability findings from your Tenable Vulnerability Management scanner with BigFix Fixlets and devices, and deploy the remediations from one place.
- **Patch Dashboard** – Get a consolidated, risk-prioritized view of missing patches and vulnerable devices, with drill-down navigation into Fixlets, devices, and deployments.
- **Security Compliance** – Review checklist compliance across your environment and deploy remediation for the checks that fail.
- **License Reclamation** – Find software that is installed but not used, see the savings that you gain when you uninstall it, and reclaim licenses.
- **Protection Level Agreement (PLA)** – Measure patch levels and compliance standards for a set of Fixlets against the service levels that your organization agrees to.
- **Workflow Builder** – Automate multi-step device tasks in a drag-and-drop visual editor, then deploy and monitor the workflows you build.

Reporting

Reporting helps you generate insights from BigFix data and share them with your team. For more information, see Reporting *(on page 355)*.

- **All Reports** – Access existing reports, mark favorites, and manage import/export options. You can also assign tags to reports and generate reports offline.
- **Scheduled Reports** – Run a saved report automatically, email the result, and keep an archive of each run.
- **Report Builder** – Build custom reports from device, Fixlet, deployment, and user data sets, with filters and chart widgets. You can also start from a guided template.
- **Scripted Reports** – Create advanced reports using HTML, Relevance expressions, JavaScript, and CSS.

Administration

Administration is visible only to administrators. For more information, see Administration *(on page 433)*.

- **Application Configuration** – Configure the applications available in BigFix UI, including global DEX settings and IVR settings.
- **Identity management** – Manage users, roles, permissions, account policies, and OIDC single sign-on.
- **System configuration** – Manage SMTP server profiles that BigFix UI uses to send email, such as scheduled report deliveries.

Workspace features

Across all areas, BigFix UI provides a consistent set of workspace features:

- The **Notification Center**, opened from the bell icon in the header, where you can filter, search, and archive notifications from every module.
- The **Account** panel, where you manage your profile and password, review your account activity, and set your language and theme preferences.
- Browser-based navigation, so the browser back and forward buttons, browser tabs, and shareable page links work as you expect.

Benefits of using BigFix UI

- **Single Pane of Glass** – Access all BigFix capabilities in one place.
- **Efficiency** – Reduce effort by consolidating patching, reporting, and remediation.
- **Consistency** – Apply uniform policies across your environment.
- **Visibility** – Monitor vulnerabilities, compliance, and patch health through dashboards and reports.
- **Personalization** – Customize your home dashboard and choose a light, dark, or system default theme.
- **Scalability** – Manage thousands of endpoints through a centralized console.
- **User Experience** – Work with a modern, intuitive UI designed for fast navigation.

About this guide

This guide is for operators and administrators who use BigFix UI day to day. It explains how to navigate the interface, explore devices and Fixlets, deploy content, build reports, and manage users and roles. The chapters follow the structure of the product:

- **Getting Started with BigFix UI** – Sign in, understand access and security, navigate the interface, and use the common functions that appear across the application, such as filters, tags, and notifications.
- **Using BigFix UI** – Work with the Home dashboard and the Explore, Resolve, Reporting, and Administration areas.

This chapter also includes Known limitations *(on page 7)*, which lists the architectural and operational limits that affect how you plan device exploration and remediation. Review these limitations before you deploy content from BigFix UI.

This guide does not cover installing, configuring, or upgrading BigFix UI. For server installation, application configuration settings, and other deployment tasks, see the ***BigFix UI Administration Guide***.

Known limitations

This release of BigFix UI has architectural and operational limits that affect how you plan device exploration and remediation. Review these limitations before you deploy content from BigFix UI.

Correlation is not supported

This release of BigFix UI does not support device correlation. If your environment has correlated devices, you cannot install BigFix UI. The installation does not proceed on an environment where correlation is in place.

To use BigFix UI, remove correlation from your environment first. For more information about correlation, see Correlated devices.

Fixlets that require user input are not supported

You cannot deploy Fixlets and Tasks that ask for user-supplied values at deployment time from BigFix UI. This includes:

- Fixlets that use the `action parameter query` ActionScript command.
- Fixlets that collect input through HTML forms or JavaScript in the Fixlet description.

Console-only Fixlets

You can deploy some Fixlets only from the **BigFix Console**. You cannot deploy them from BigFix UI, BigFix WebUI, or the BigFix REST API.

Note: BigFix UI does not identify these Fixlets, so it does not prevent you from deploying them. If you deploy one of these Fixlets from BigFix UI, the action ends in error. Before you deploy a Fixlet, make sure that it does not require user input.

For more information, see Deploying Fixlets *(on page 167)*.

Stopping other operators' deployments is not supported

BigFix UI does not support the **Stop Other Operators' Actions** permission. A non-master operator can stop only the open deployments that they issued, even if their role grants this permission. To stop a deployment that another operator issued, use the **BigFix Console**.

For more information, see Deployments *(on page 181)*.

Bulk tag assignment does not suggest partially applied tags

When you tag more than one object at once, the **Manage tags** drawer shows only the tags that every selected object already has. Tags that only some of the selected objects have do not appear in the drawer or in the suggestion list. You can still create new tags and assign them to all the selected objects. To give the other objects a tag that only some of them have, tag each of those objects on its own.

For more information, see Managing Tags *(on page 51)*.

Filtering on computer properties that belong to a category is not supported

BigFix UI does not support filtering devices on computer properties that are assigned to a category. This applies to custom properties and to analysis properties, such as **Actionsite Size** in **BES Health Checks Analysis**. If you filter on one of these properties, the results might be incorrect or empty.

For more information, see Devices *(on page 77)*.

Device groups: Server-based groups and client-evaluated manual groups are not supported

BigFix UI does not support server-based groups or manual groups whose membership is determined by client settings (client-evaluated manual groups). These groups are not available in BigFix UI. Use the **BigFix Console** to view and manage them.

For more information, see Device Groups *(on page 94)*.

Related information

Deploying Fixlets *(on page 167)*

Fixlet Explorer Details page *(on page 155)*

Deployments *(on page 181)*

Managing Tags *(on page 51)*

Devices *(on page 77)*

Device Groups *(on page 94)*

Chapter 2. Getting Started

The Getting Started section introduces key features that help users begin working with the BigFix UI. It provides a foundation for understanding how to access the system securely, navigate common features, and apply guided recommendations to improve efficiency and compliance.

The following topics are included in this section:

- Access and security *(on page 10)* – Learn how to securely log in and out of the BigFix UI, manage credentials, update profile details, and understand session timeout controls.
- Navigating BigFix UI *(on page 26)* – Find your way around the side navigation, the application pages, and the common page layout.
- Common Functionalities *(on page 28)* – Explore shared features such as filtering, sorting, and exporting data across modules. This section also covers Managing Filters *(on page 35)*, Manage Reports *(on page 42)*, Managing Tags *(on page 51)*, and Prescriptive Guidance *(on page 55)*.
- Notification Center *(on page 58)* – Review the alerts that BigFix UI raises and how to manage them.

Access and security

Learn how to securely sign in to and out of the BigFix UI application, change your password, update your profile, review your account activity, and set your language and theme.

Learn how to securely log in and out of the BigFix UI application, change your password, and update your profile information. Regularly updating your password and keeping your profile information current helps maintain the security and accuracy of your account. It also covers session handling and password-management features that help maintain account security after setup.

After completing the BigFix UI setup (as outlined in the BigFix UI Administration Guide), users can log in with the credentials created during setup. This topic explains how to access the BigFix UI through the login page, how to sign out securely, and how to change the account password when required.

To manage your account, select the profile icon in the upper-right corner. The **Account** panel opens with four tabs: **Profile**, **Password**, **Account Activity**, and **Settings**. The panel also includes a **Log out** link.

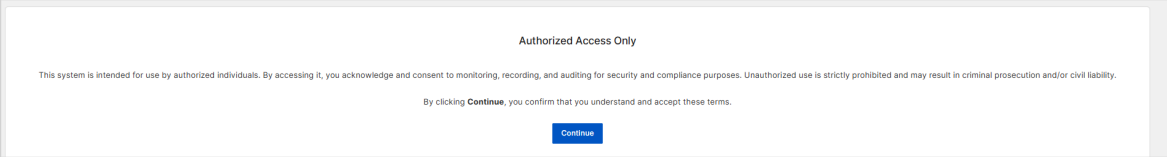
BigFix UI supports two ways to log in:

- **Local credentials**: Enter your **Login Name** and **Password**, and then select **Log in to BigFix**. See Logging In *(on page 10)*.
- **OIDC single sign-on**: Select **Log in via OIDC** and authenticate with your organizational credentials. This option appears only when the instance admin enables OIDC. See Logging In with OIDC Single Sign-On *(on page 13)*.

Logging In

To access the BigFix UI application, follow these steps:

1. Open the BigFix UI application URL: Launch your preferred web browser and navigate to `https://<host>[:port]/ui` to access the BigFix UI application.
2. (Optional) The **Authorized Access Only** page might appear before the login page. This notice confirms that the system is restricted to authorized users. After you read the message, select **Continue** to proceed to the login page.



   - The instance admin controls this notice from the BigFix UI. To change it, expand **Administration** from the side navigation, select **Identity Management**, select the **Admin user and account policy** card, and then select the **Account Policy** tab.
   - On the **User management - account policy** page, the **Legal notice message** section contains a toggle that shows or hides the notice, and the **Authorized access only (required)** field that holds the message text.
   - When the toggle is off, the page does not appear and users go straight to the login page.
   - For the default message text, the field descriptions, and the steps to edit and save the notice, see Account Policy Settings *(on page 488)*.

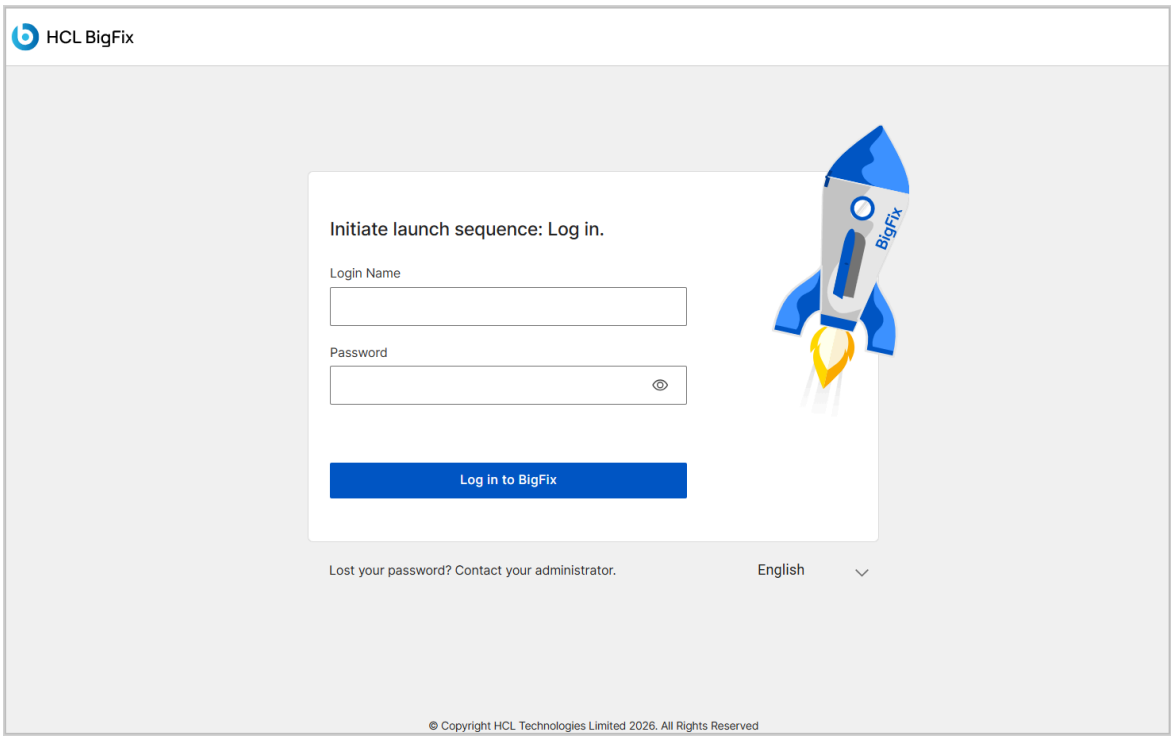
   Note: Only the instance admin can change this message. The **Admin user and account policy** card is not visible to other administrators.

3. (Optional) Select your interface language: In the lower-right corner of the login page, select the language selector, and then choose a language from the list. Use the **Search** box to find a language quickly.

   Note: In the July 2026 release, **English** is the only available language. Additional languages are planned for a future release.

4. Enter your credentials: On the **Initiate launch sequence: Log in.** page, enter your **Login Name** and **Password** in the respective fields. Select the eye icon in the **Password** field to show or hide the password that you typed.

   Note: If you are a first-time user, check the email you received from BigFix for the credentials.



5. After you enter your credentials, select **Log in to BigFix**.

> **Note:** If you forget your password, the login page does not offer a self-service reset. Select **Lost your password? Contact your administrator.** and ask your administrator to reset it.

6. Change the temporary password: A first-time user receives a welcome email containing a temporary password. On first login, the application prompts you to change the temporary password.
7. After you log in successfully, you are taken to Customizable Dashboard, the home page of BigFix UI.
8. The **Login Information** panel appears as a notification overlay in the upper-right corner upon login. It provides essential security details about your account activity:
    - **Last log in**: Displays the date and time of your previous successful login.
    - **Last failed attempt**: Displays the date and time of the most recent unsuccessful login attempt for your account.
    - **Failed attempts since last log in**: Shows the number of incorrect password entries recorded since your last successful session.
    - **Last password change**: Indicates when your account password was last updated.
    - **Last role change**: Displays the date and time of the most recent modification to your assigned user roles or permissions.

> **Note:** You can view these same details any time on the **Account Activity** tab of the **Account** panel. See Viewing Account Activity *(on page 23)*.

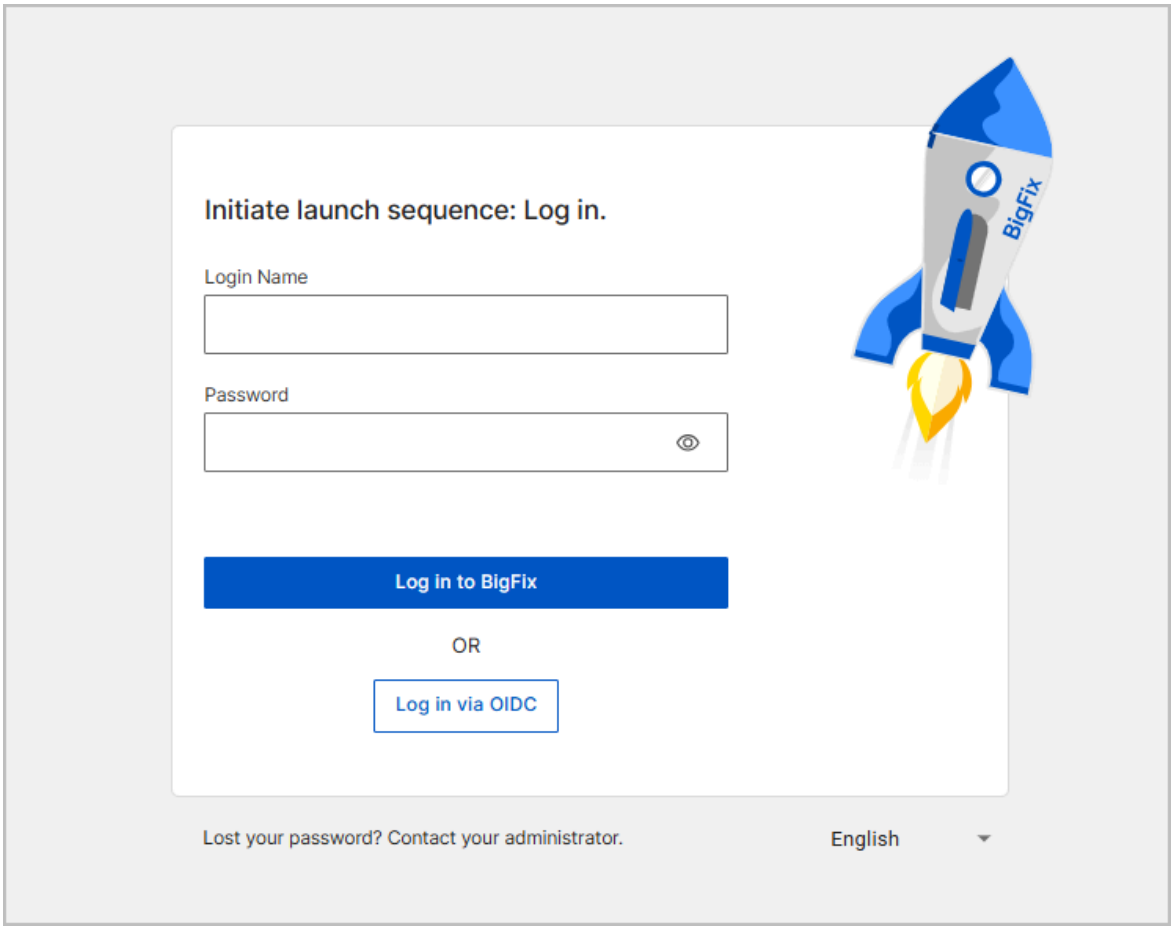
Logging In with OIDC Single Sign-On

If the instance admin enables OpenID Connect (OIDC), the login page shows a **Log in via OIDC** button below **Log in to BigFix**, separated by an **OR** divider. Use this option to log in with the credentials that your organization already issues you, instead of a separate BigFix UI password.

Before you log in with OIDC, your administrator must configure the identity provider and create your account as an **Identity provider (Idp)** user bound to a BigFix operator. For details, see OIDC Configuration *(on page 492)* and Configuring OIDC single sign-on *(on page 506)*.

1. Open the BigFix UI application URL in your browser: `https://<host>[:port]/ui`.
2. If the **Authorized Access Only** page appears, read the message and select **Continue**.
3. Select **Log in via OIDC**.

Note: If the button does not appear, OIDC is not enabled. Ask your instance admin to check the OIDC configuration.



4. The browser redirects you to the login page of your identity provider. Enter your organizational credentials, and complete any other checks that your provider requires, such as multifactor authentication.
5. After the provider authenticates you, the browser returns to BigFix UI. BigFix UI validates the token, creates your session, and opens the Customizable Dashboard with the permissions of the BigFix operator that your account is bound to.

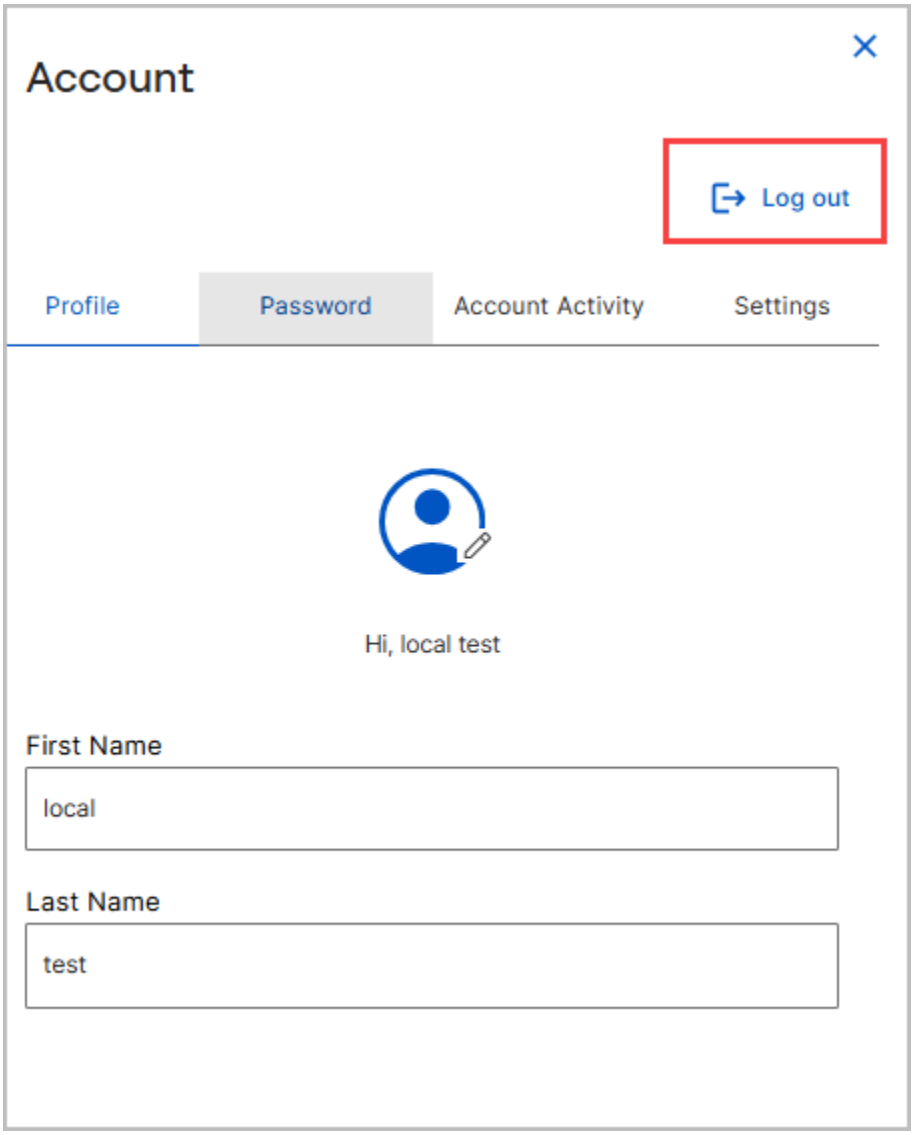
Note: Logging out of BigFix UI ends only your BigFix UI session. It does not log you out of your identity provider. To end the provider session, log out of the provider separately or close the browser.

For the full procedure, including the prerequisites that must be met before your first sign-in, see Logging in with OIDC *(on page 510)*.

Logging Out

To ensure the security of your account, always log out when you are finished using the application:

1. Open the Account panel: Select your profile icon in the upper-right corner of the application window. The **Account** panel opens.
2. Select **Log out**. This securely logs you out of your account and redirects you to the login page.

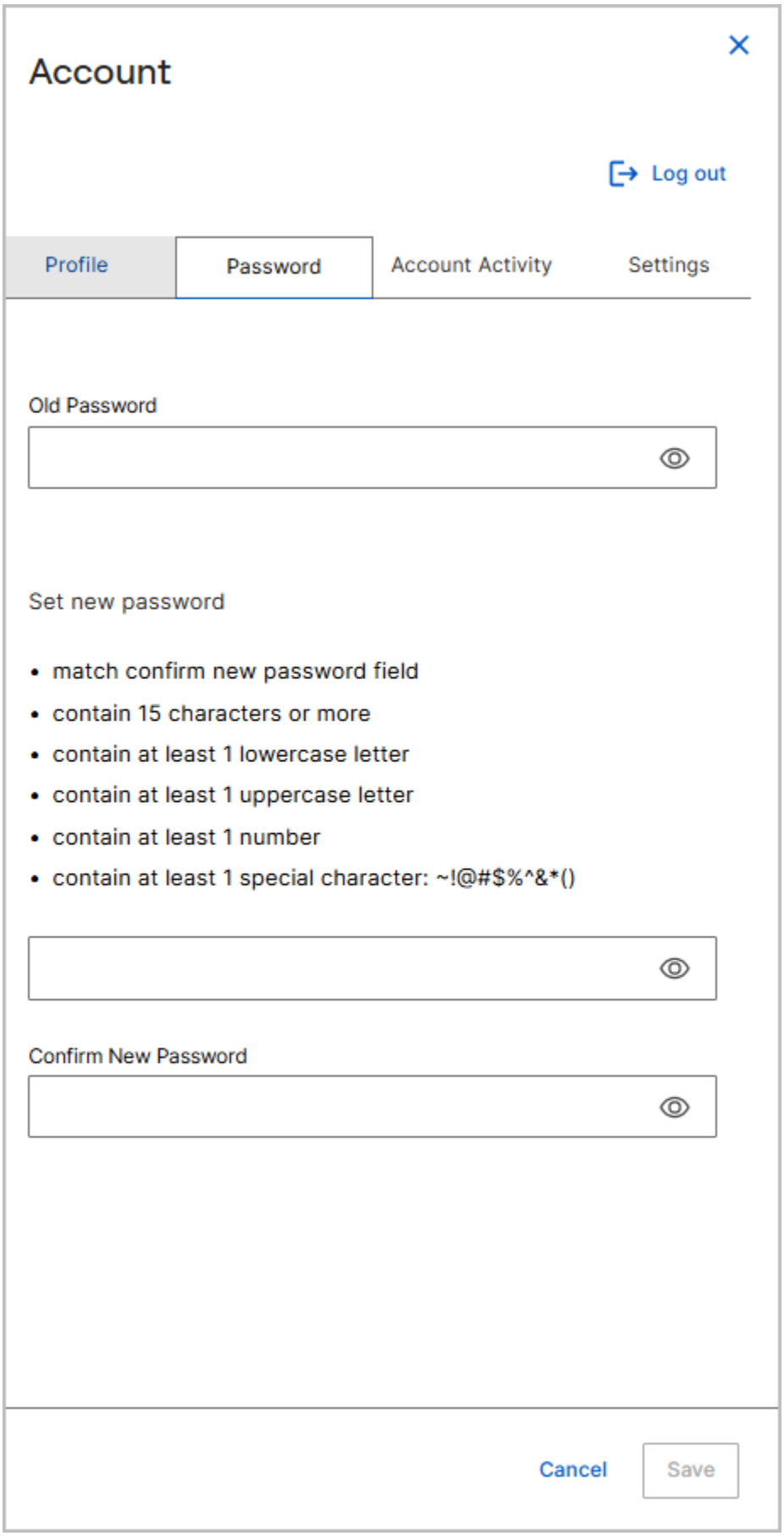


Changing Your Password

If you need to change your password for security reasons or periodic updates, follow these steps:

1. Open the Account panel: Select your profile icon in the upper-right corner to display your account information.
2. Select the **Password** tab.
3. Enter the current password: In the **Old Password** field, enter your current password for verification.
4. Enter the new password: Under **Set new password**, type your new password. The password must meet the following criteria, which the application confirms as you type:

- Match the **Confirm New Password** field.
- Contain 15 characters or more.
- Contain at least one lowercase letter.
- Contain at least one uppercase letter.
- Contain at least one number.
- Contain at least one special character: `~!@#$%^&*()`.

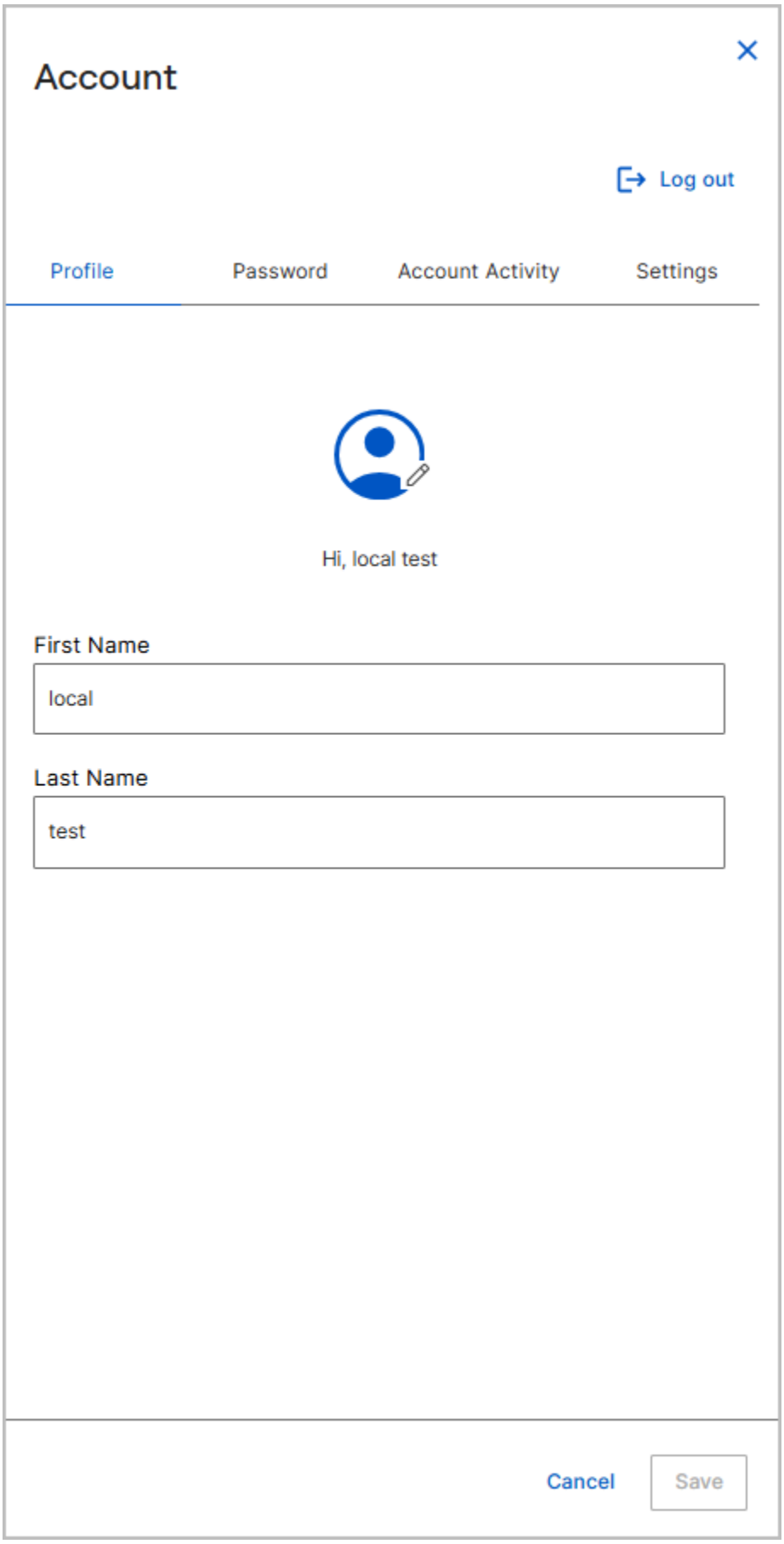

Account
Log out
Profile
Password
Account Activity
Settings
Old Password
Set new password
match confirm new password field
contain 15 characters or more
contain at least 1 lowercase letter
contain at least 1 uppercase letter
contain at least 1 number
contain at least 1 special character: ~!@#$%^&*()
Confirm New Password
Cancel
Save

5. Confirm the new password: In the **Confirm New Password** field, re-enter the new password.
6. Select **Save** to apply the changes. To discard your changes, select **Cancel**. After you change your password, you must log in again with your new password.

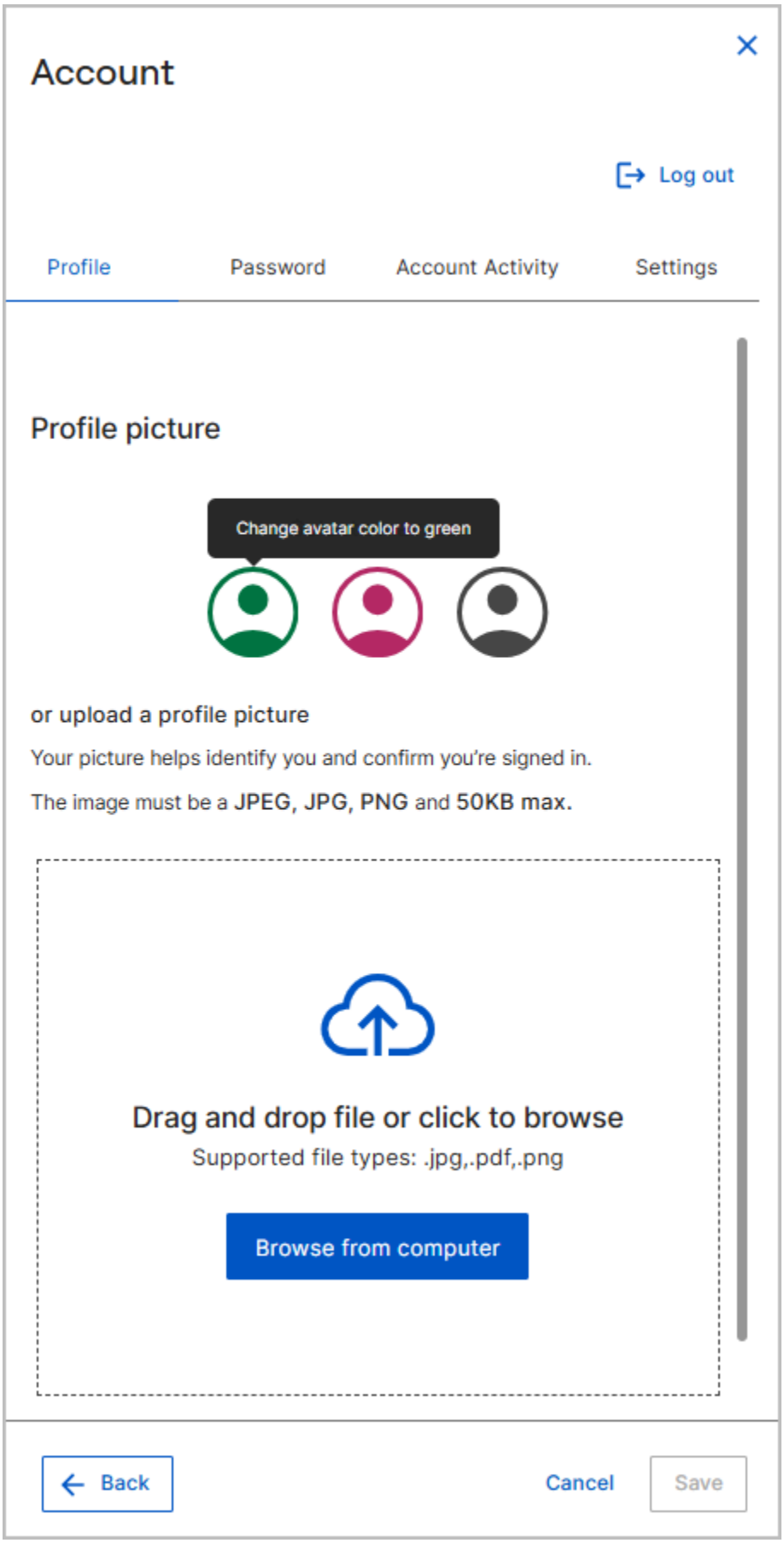
Changing Your Profile Information

To update your profile information, such as your first name, last name, and profile picture:

1. Open the Account panel: Select your profile icon in the upper-right corner, and then select the **Profile** tab.


Account
Log out
Profile
Password
Account Activity
Settings
Hi, local test
First Name
local
Last Name
test
Cancel
Save

2. Update the fields: Modify your **First Name** and **Last Name** as needed. Ensure that the required fields are filled in.
3. (Optional) Change your profile picture:
    a. Select the edit (pencil) icon on the profile avatar. The **Profile picture** window opens.
    b. Do one of the following:
        - Under **Select an avatar**, select one of the provided avatars.
        - To upload your own picture, drag and drop an image onto the upload area, or select **Browse from computer** and choose a file. The image must be a JPEG, JPG, or PNG file, up to 50 KB.
    c. Select **Save**. To return to the Profile tab without changing the picture, select **Back** or **Cancel**.

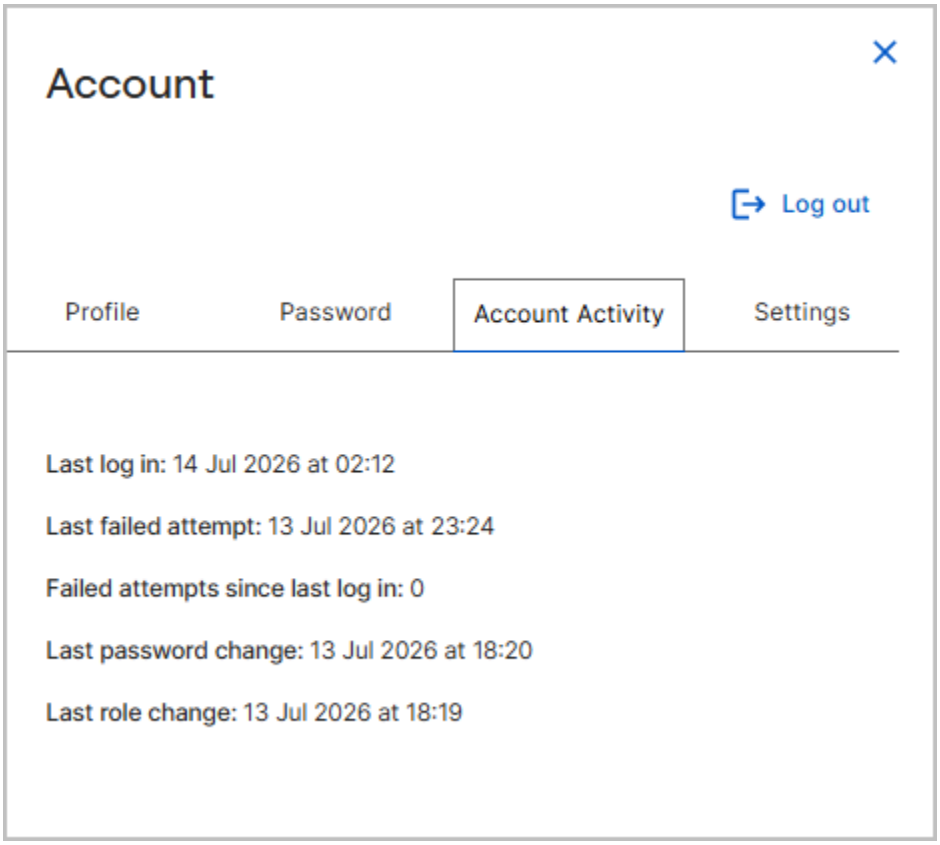

Account
Log out
Profile
Password
Account Activity
Settings
Profile picture
Change avatar color to green
or upload a profile picture
Your picture helps identify you and confirm you're signed in.
The image must be a JPEG, JPG, PNG and 50KB max.
Drag and drop file or click to browse
Supported file types: .jpg,.pdf,.png
Browse from computer
Back
Cancel
Save

4. Select **Save** to save your changes. To discard your changes, select **Cancel**. Your profile information updates immediately.

Viewing Account Activity

The **Account Activity** tab shows recent security details for your account, such as your last sign-in and last password change. Use it to confirm your recent activity and to spot unexpected sign-in attempts.

1. Open the Account panel: Select your profile icon in the upper-right corner. The **Account** panel opens.
2. Select the **Account Activity** tab.



The tab displays the following read-only details:

Table 1. Account Activity fields

Field	Description
Last log in	Date and time of your previous successful login.
Last failed attempt	Date and time of the most recent unsuccessful login attempt for your account.
Failed attempts since last log in	Number of incorrect password entries recorded since your last successful session.

Table 1. Account Activity fields (continued)

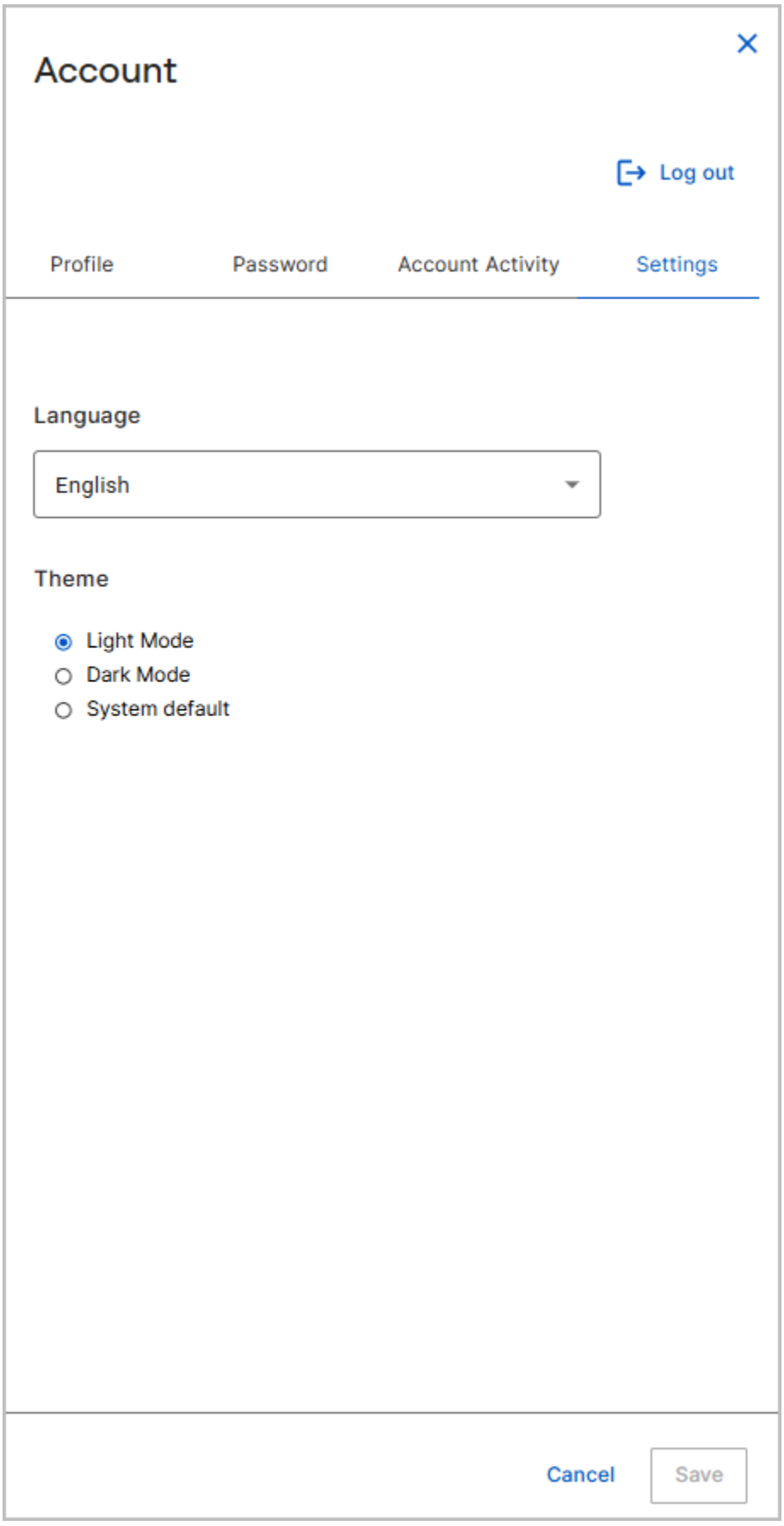
Field	Description
Last password change	Date and time when your account password was last updated.
Last role change	Date and time of the most recent change to your assigned user roles or permissions.

Note: These are the same details that appear in the **Login Information** overlay at sign-in. The **Account Activity** tab lets you review them at any time.

Changing Language and Theme Settings

On the **Settings** tab, you can set the display language and the theme (color mode) for the BigFix UI. These preferences apply to your account.

1. Open the Account panel: Select your profile icon in the upper-right corner. The **Account** panel opens.
2. Select the **Settings** tab.


Account
Log out
Profile
Password
Account Activity
Settings
Language
English
Theme
Light Mode
Dark Mode
System default
Cancel
Save

3. From the **Language** list, select your preferred language.

   Note: In the July 2026 release, **English** is the only available language. Additional languages are planned for a future release.

4. Under **Theme**, select a display mode. The following options are available:
   - **Light Mode**: Displays the interface with a light background. This is the default.
   - **Dark Mode**: Displays the interface with a dark background.
   - **System default**: Matches the theme configured in your operating system.
5. Select **Save** to apply your preferences. To discard your changes, select **Cancel**.

Session Timeout and Re-authentication

To maintain account security, the BigFix UI automatically ends inactive sessions after a predefined timeout period.

- When a session times out, the user is redirected to the login page.
- Users must re-enter their credentials to regain access.
- Unsaved work or in-progress actions might be lost when the session expires.

Note: Avoid leaving the session idle for long periods. If your session expires, log in again with your credentials.

Related information

User & Role Management *(on page 449)*

Logging in with OIDC *(on page 510)*

OIDC Configuration *(on page 492)*

Configuring OIDC single sign-on *(on page 506)*

Navigating BigFix UI

BigFix UI gives every app and page its own web address. As a result, you can move around with your browser's Back and Forward buttons, refresh a page without losing your place, and bookmark or share a link that reopens the exact page you were viewing.

BigFix UI is a single web application made up of several apps, such as Device Explorer, Fixlet Explorer, and Deployment Manager, that you open from the side navigation. As you move between apps, pages, and tabs, the address shown in your browser's address bar updates to match where you are. Because each location has its own address, the browser controls you already know work the way you expect.

Moving between apps and pages

Use the side navigation to open an app. Within an app, use the tabs on a details page (for example, **Overview**, **Relevant Fixlets**, and **Deployments** on a device's details page) to switch between views. Each app and page you open is recorded as a step in your browser history, so you can retrace your path later.

Using the Back and Forward buttons

Your browser's **Back** and **Forward** buttons move you through the pages you have already visited:

- **Back** returns you to the previous page or app.
- **Forward** reopens a page that you stepped back from.

These buttons work across apps as well as within a single app. For example, if you open a device in Device Explorer and then open one of its deployments in Deployment Manager, selecting **Back** returns you to the device you started from.

Refreshing the current page

Refreshing or reloading the page in your browser reloads the view you are currently looking at and keeps you in the same place. You are not sent back to a home page, and you do not lose your position in the app. If your session has expired, you are prompted to sign in again and are then returned to your work.

Bookmarking and sharing pages

Because each page has its own address, you can bookmark it in your browser or copy the link and share it with a colleague. Opening a bookmarked or shared link takes you straight to that page, for example a specific device, fixlet, or deployment, after you sign in if you are not already signed in. A link that opens a specific item in this way is often called a direct link.

Note: Anyone who opens a shared link still needs permission to use the app it points to. If a colleague does not have access to that app, they see a message that access is not allowed. See When a page cannot be opened *(on page 28)*.

Reading the address bar

Addresses in BigFix UI are readable and reflect the app and page you are on. For example, an address that ends in `/ui/deployment-manager` shows the Deployment Manager app, and one that ends in `/ui/deployment-manager/details` shows a details page within it. You do not need to type or edit these addresses by hand. Navigate using the side navigation, tabs, and links in the app, and the address updates automatically.

Opening related items in another app

Some pages contain items that are managed by a different app. When you select such an item, BigFix UI switches to the app that owns it and opens the item directly. For example, selecting a deployment from a device's **Deployments** tab opens that deployment in Deployment Manager. Selecting **Back** returns you to the page you came from.

When a page cannot be opened

If a link points to a page that BigFix UI cannot open, it shows a message instead of the page:

- A page-not-found message appears when the address does not match any app or page. This can happen if a link is mistyped or points to something that no longer exists.
- An access-not-allowed message appears when you open a link to an app that your account is not permitted to use. Contact your administrator if you need access.

To continue, select **Back** or choose another app from the side navigation.

Your starting page after you sign in

When you sign in, BigFix UI opens your default landing app, which is typically **My Dashboard**. The landing app depends on your account and the apps assigned to your role, so it can differ from one user to another.

Common Functionalities

Familiarize yourself with the functionalities that are available across modules. These features work the same way in the BigFix UI applications, such as Devices, Fixlets, Deployments, and CyberFOCUS, so you learn them once and apply them everywhere.

This section describes the controls that BigFix UI shares across its applications. The following features have their own topics:

- Managing Filters *(on page 35)* – Use the global filter, the table filter, and the query filter to narrow the records that you work with.
- Manage Reports *(on page 42)* – Save, load, and organize the custom reports that you generate.
- Managing Tags *(on page 51)* – Attach custom labels to Fixlets, deployments, reports, and analyses so that you can group and track related content.
- Prescriptive Guidance *(on page 55)* – Review actionable recommendations that are based on best practices and the current state of your environment.

The rest of this topic describes the controls that appear directly on list view and overview pages.

Filtering Data

A filter narrows a set of records to the ones that match the conditions you define. You build every filter the same way, from a **Property**, an **Operator**, and a **Value**. BigFix UI provides three filter types, each in a different place and with a different purpose.

Global filter

The global filter is the funnel icon in the upper-right corner of the Devices, Fixlets, CyberFOCUS, and Report Builder pages. It narrows the whole page, including the charts. The panel has **Current filter**, **Saved filters**, and **Favourite filters**

tabs, so you can save a filter under a name of your choice, mark the ones you use most as favourites, and apply them again in a later session. For the steps, see Global filter *(on page 36)*.

Table filter

The table filter is the funnel icon above a data table on the Sites, Analyses, Deployments, All Reports, Scheduled Reports, User Management, and Roles pages. It narrows the rows of that one table. Select **Add filter** to combine conditions with **And** or **Or**, and then select **Apply**. You can't save a table filter. For the steps, see Table filter *(on page 40)*.

Filter by query

The query filter defines a set of devices or Fixlets, so it changes which records an object acts on, not just what you see. You use it wherever BigFix UI asks you to target a set of records: the remediation, Fixlet deployment, and custom remediation flows, the membership criteria of a dynamic device group, the device subscription rule of a custom site, and the device scope of a role. Where the filter targets devices, you can usually filter by **Query**, **Device group**, or **Device list**. For the steps, see Filter by query *(on page 40)*.

Manage Reports

Manage Reports saves, loads, and organizes the custom reports that you generate in BigFix UI. Use it to preserve a view that you use often, such as a set of filter conditions, columns, and charts, and to reopen it later.

Select **Manage Reports** in the upper-right corner of the List View to slide out the panel, which provides a **Save Report** tab and a **Load Report** tab. Reports that you save in one application are listed on the All Reports page, which gives you central management and quick access.

For the steps to save and load a report, see Manage Reports *(on page 42)*.

Columns

Use the column chooser to control which columns appear in the data table.

1. Above the table, select **Column**. The column chooser opens.
2. Optional: In the search box, enter a column name to filter the list.
3. Select the checkbox next to each column you want to show, and clear the checkbox for each column you want to hide. You can display up to 63 columns; the panel shows the current limit as **Max items limit: 63**.
4. Optional: Select **Reset** to restore the default column selection.
5. Select **Apply**. The table updates to show the columns you selected.

Density

Use the density control to set the row spacing of the data table.

1. Above the table, select **Density**. A menu opens.
2. Select the row spacing you want:

- **Compact** – fits the most rows by reducing row height.
- **Standard** – the default row height.
- **Comfortable** – adds space between rows for easier reading.

The table updates immediately to use the spacing that you selected.

Sorting Data

Sorting can be applied to individual columns, allowing users to arrange data according to their current focus or needs. This feature enhances data readability and ensures users can efficiently work with large sets of information by keeping relevant details readily accessible. Sorting organizes your data in ascending or descending order based on a selected column. Each column in the list table includes a **Sort** icon (double arrows) that allows you to organize your data alphabetically or numerically

- **To sort a column**: Select the **Sort** icon in the column header.
  - The first selection sorts the data in **ascending** order (for example, A to Z or 1 to 10).
  - Selecting the icon again sorts the data in **descending** order (for example, Z to A or 10 to 1).
- **To clear a sort**: Select the icon until the arrows return to their default, neutral state.

 **Note:** To identify the current sort order, look for a single upward or downward arrow in the column header.

Exporting Data

The Export Data option is available on Deployments, CyberFOCUS, All reports, Report Builder, and list view pages of Devices, Fixlets. Use this option to download tabular report information from list view pages for offline analysis or record-keeping.

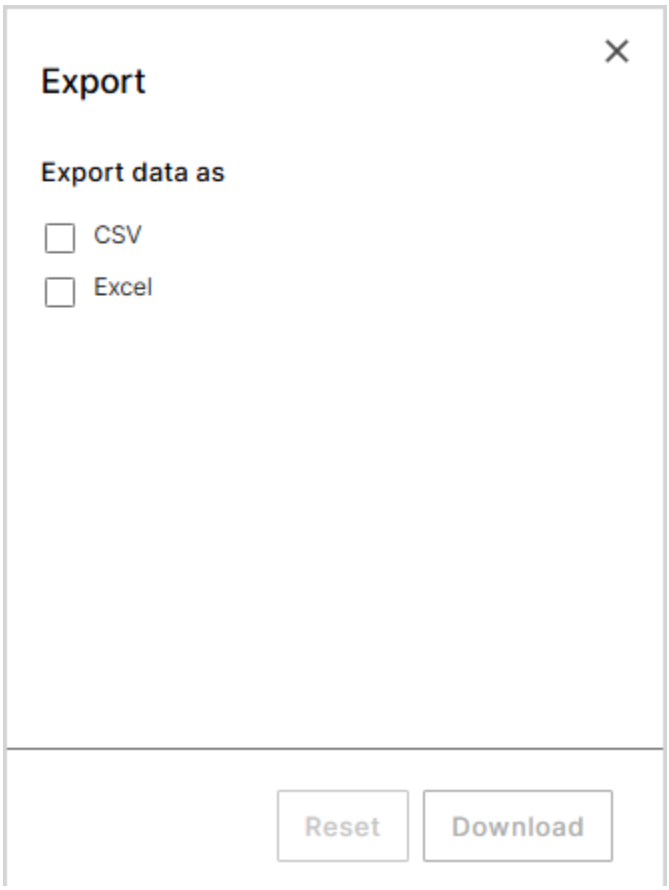
It enables users to export visible report data—filtered, sorted, or customized to commonly used spreadsheet formats like CSV or Excel.

This allows users to review device inventories, fixlet compliance, or deployment summaries outside the BigFix UI environment.

How to Export Data:

1. Click the Export Report icon located in the upper-right corner of the page.

   The **Export** panel slides out and displayed.



2. In the Export panel that appears:
    - Select **CSV** to export raw comma-separated data for importing into other tools.
    - Select **Excel** to export data into a formatted spreadsheet (.xlsx) file.
3. **Choose Data to Export:** Depending on the module and screen you are in, you have the option to export the entire dataset visible on the screen or apply filters to export a specific subset of data.

    Note:
    - If applicable, apply filters or selections within the module to export only the necessary data, reducing file size and focusing on relevant information.
    - Depending on your user role and permissions, access to certain data subsets may be restricted.

4. After selecting the desired format, click **Download**. The file gets generated and downloaded to your device.
5. (Optional) Click **Reset** to clear all selections before downloading again.

Note: In the Report Builder, you can export a report from the **Preview** step of the guided template wizard, or from the report details page by selecting the more options icon and then **Export**. See Report Builder *(on page 384)*.

Exporting Charts

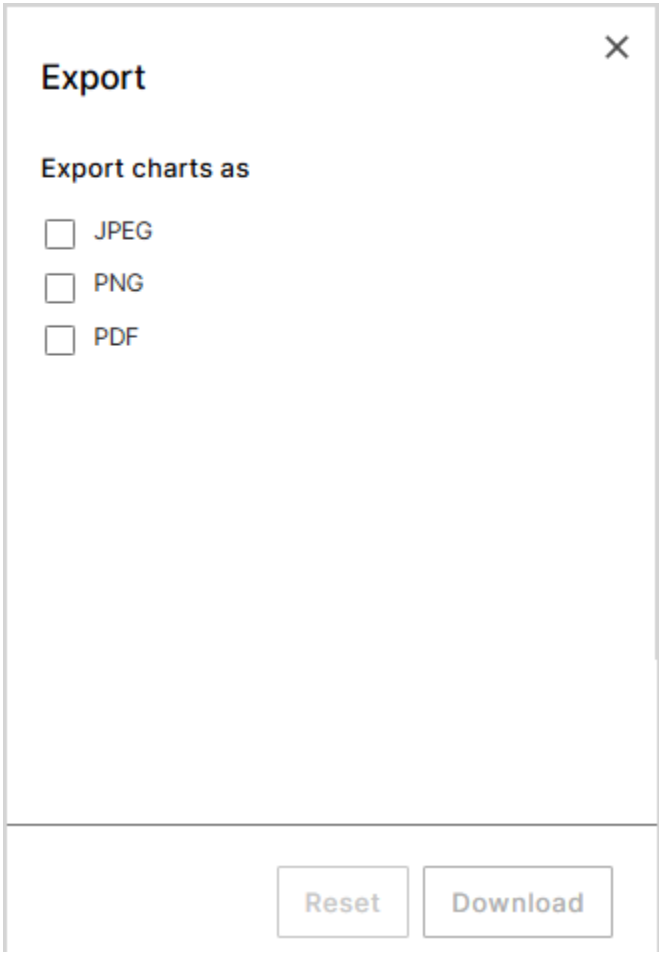
The Export charts option is available on CyberFOCUS and Overview pages of Devices, Fixlets. Use this feature to capture dashboard visualizations from overview pages as image or document files for reporting and presentation purposes. It allows users to download graphical widgets such as bar charts, donut charts, or summary tiles that visualize system compliance, device types, or OS distribution trends.

Charts can be exported as JPEG, PNG, or PDF files, making it easy to include BigFix data visuals in internal reports or external presentations.

How to Export Charts

1. Click the Export Report icon located in the upper-right corner of the page.

   The **Export** panel slides out and displayed.



2. In the Export panel, select one or more of the following options:
    - JPEG – Exports charts as compressed images suitable for quick sharing.
    - PNG – Exports charts in higher resolution for professional documentation.
    - PDF – Consolidates all visible charts into a single report document.
3. **Choose Data to Export:** Depending on the module and screen you are in, you have the option to export the entire dataset visible on the screen or apply filters to export a specific subset of data.

    Note:
    - If applicable, apply filters or selections within the module to export only the necessary data, reducing file size and focusing on relevant information.
    - Depending on your user role and permissions, access to certain data subsets may be restricted.

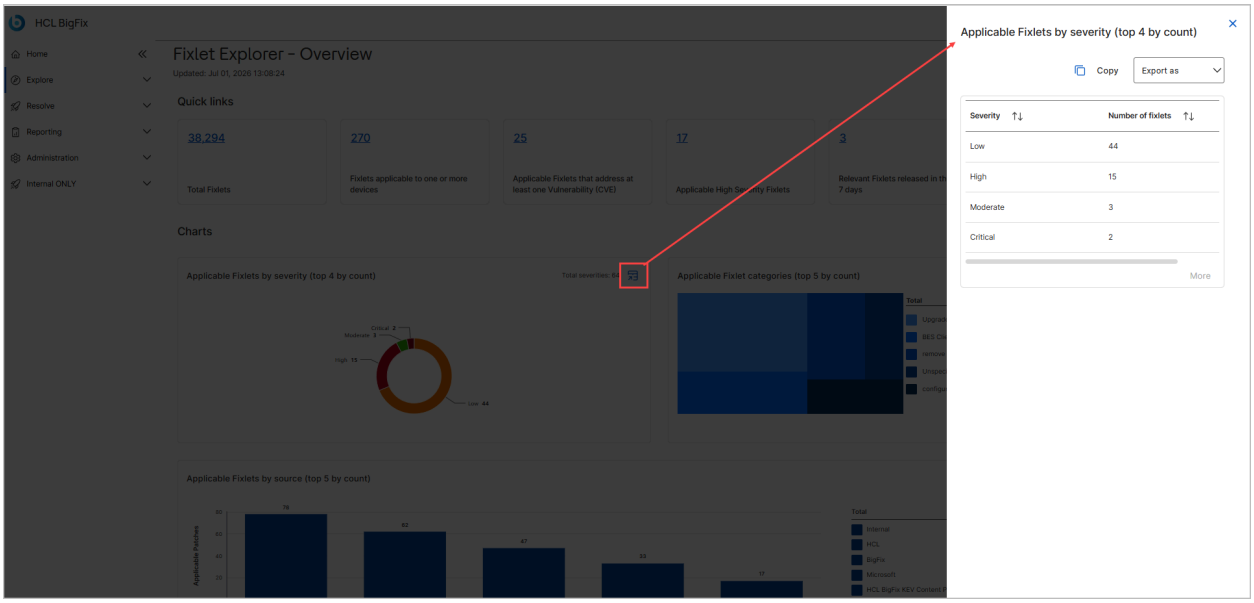
4. **Confirm and Download:** After selecting the desired format click **Download**. The file gets generated and downloaded to your device.

    Note: If you have choosen more than one format to export, the files will be downloaded in a single zip folder.

5. (Optional) Use Reset to deselect all options before making a new export.

Viewing chart data in a table

Each chart has an icon in its top-right corner that opens the chart's data as a table, with options to copy or export it.



Each chart can display its data as a table that you can copy or export

1. Locate the chart that you want, such as **Applicable Fixlets by severity (top 4 by count)**.
2. In the chart's top-right corner, select the **See data in data table format with download options** icon. The chart's data panel opens and displays the data as a table, such as **Severity** and **Number of fixlets**.
3. Optional: To sort the table, select the sort icon in a column header.
4. Optional: If a **More** link appears, select it to load additional rows.
5. To copy the table to the clipboard, select **Copy**.
6. To download the data, select **Export as** and choose a format.
7. To close the panel, select **Close** (X).

Tags

Tags are custom labels that you attach to Fixlets, deployments, reports, and analyses so that you can group, filter, and track related content across BigFix UI. You create tags as you need them and reuse them across objects.

You assign tags from the list view of an application, from an object's detail page, or from the **Summary** step of a remediation flow. The **Tags** column in a data table shows the tags on each row, and you can sort and filter on that column to gather every object that carries the same tag.

Note: Devices don't support tags. To organize devices, use Device Groups *(on page 94)*.

For the objects that support tags, the assignment steps, and the permissions that apply, see Managing Tags *(on page 51)*.

Prescriptive Guidance

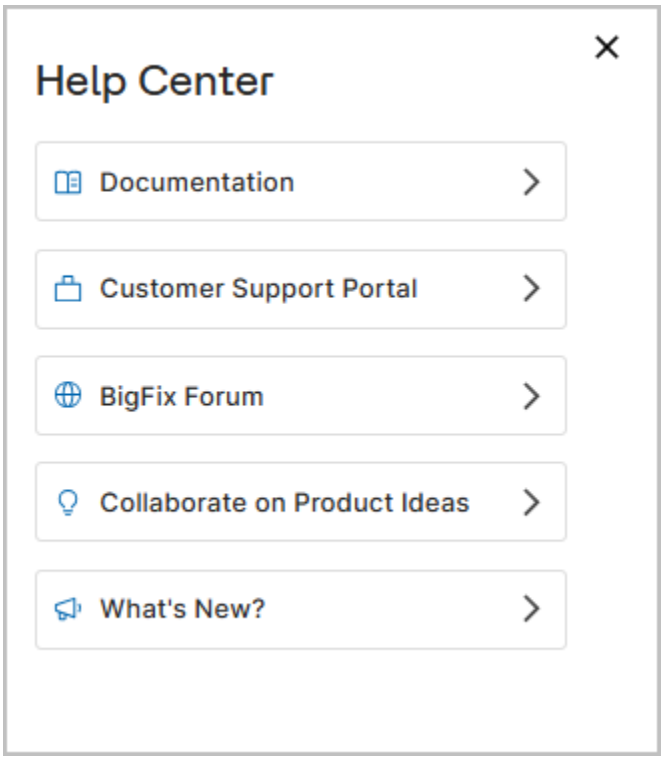
Prescriptive Guidance provides actionable recommendations that are based on best practices, industry standards, and your organizational policies. It identifies devices in your environment that are vulnerable and have no scheduled remediation action, so that you can address the highest risks first.

The feature is available in the Devices, Fixlets, and CyberFOCUS applications. Select the Prescriptive Guidance icon, or select **Prescriptive Guidance** from the **More options** menu, to open the panel. When the panel detects vulnerabilities, the **Remediate** button opens the remediation workflow with the applicable Fixlets and devices already selected.

For the key benefits, use cases, and access steps, see Prescriptive Guidance *(on page 55)*.

Help Center

The Help Center provides quick access to support and documentation resources directly from the BigFix UI. You can open it by clicking the **?** icon located in the upper-right corner of the screen.



The Help Center panel slides out from the right side and includes the following options:

- **Documentation** – Opens the BigFix product documentation site for detailed feature and usage guidance.
- **Customer Support Portal** – Navigates to the official BigFix support site where users can raise tickets or review existing cases.
- **BigFix Forum** – Redirects to the BigFix community discussion forum for peer assistance and technical insights.
- **Collaborate on Product Ideas** – Opens the BigFix idea portal where users can share feature suggestions and vote on proposed enhancements.
- **What's New?** – Displays information about recent updates, new features, and product release notes.

Each option launches an external site in a new browser tab, allowing users to seamlessly access the latest information and resources without leaving the BigFix UI.

Managing Filters

BigFix UI provides three types of filter: the global filter on the Devices, Fixlets, CyberFOCUS, and Report Builder pages, the table filter above a data table, and the query filter that you use wherever you define a set of devices or Fixlets. Learn what each one does and how to use it.

A filter narrows a set of records to the ones that match the conditions you define. BigFix UI provides three filter types, each in a different place and with a different purpose.

Table 2. Filter types

Filter type	Where you find it	What it does
Global filter *(on page 36)*	The funnel icon in the upper-right corner of the Devices, Fixlets, CyberFOCUS, and Report Builder pages.	Narrows the whole page, including the charts. You can save the filter and mark it as a favourite.
Table filter *(on page 40)*	The funnel icon above a data table on the Sites, Analyses, Deployments, All Reports, Scheduled Reports, User Management, and Roles pages.	Narrows the rows of that one table. You can't save it.
Filter by query *(on page 40)*	Anywhere you define a set of devices or Fixlets, such as the remediation and deployment flows, dynamic device groups, site subscriptions, and role device scopes.	Selects the records that the object acts on, rather than changing what the page shows.

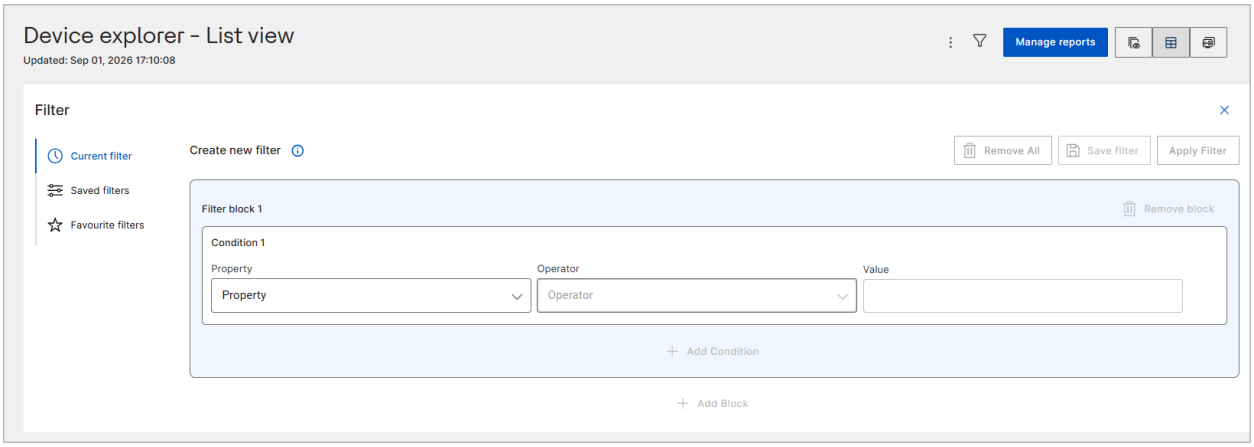
Global filter

The global filter narrows an entire page, including its charts. It is available on the Devices, Fixlets, and CyberFOCUS pages, and in the Report Builder. Unlike the other filter types, you can save a global filter and reuse it in a later session.

In the Report Builder, the filter is available on the **Create Charts** step of the custom configuration wizard, on the **Preview** step of the guided template wizard, and on the report details page. Applying a filter there updates both the configured charts and the content list. See Report Builder *(on page 384)*.

Select the **Filter** icon (funnel) in the upper-right corner of a list view page to open the **Filter** panel. The panel provides three tabs:

- **Current filter** – Build a new filter, or review and change the filter that is applied to the view.
- **Saved filters** – List every filter that you saved for the current page.
- **Favourite filters** – List only the saved filters that you marked as favourites.



Note: Saved filters are private to your account, and BigFix keeps them separate for each page. A filter that you save on the Device Explorer list view applies to devices, so it appears only in the Device Explorer. A filter that you save on the Fixlet Explorer list view appears only in the Fixlet Explorer. A filter that you save in the Report Builder applies to that report. Each of your filter names must be unique within a page.

Building and saving a global filter

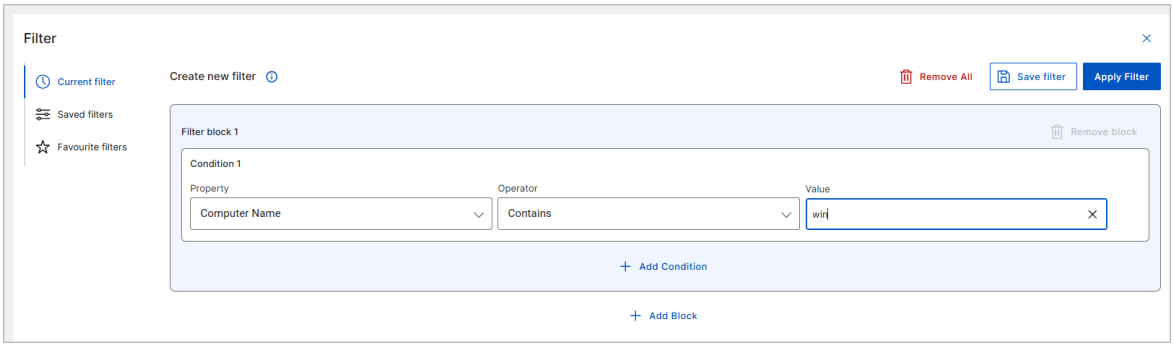
1. On a list view page, select the **Filter** icon (funnel).

   The **Filter** panel opens on the **Current filter** tab.

2. Define the conditions of your filter.

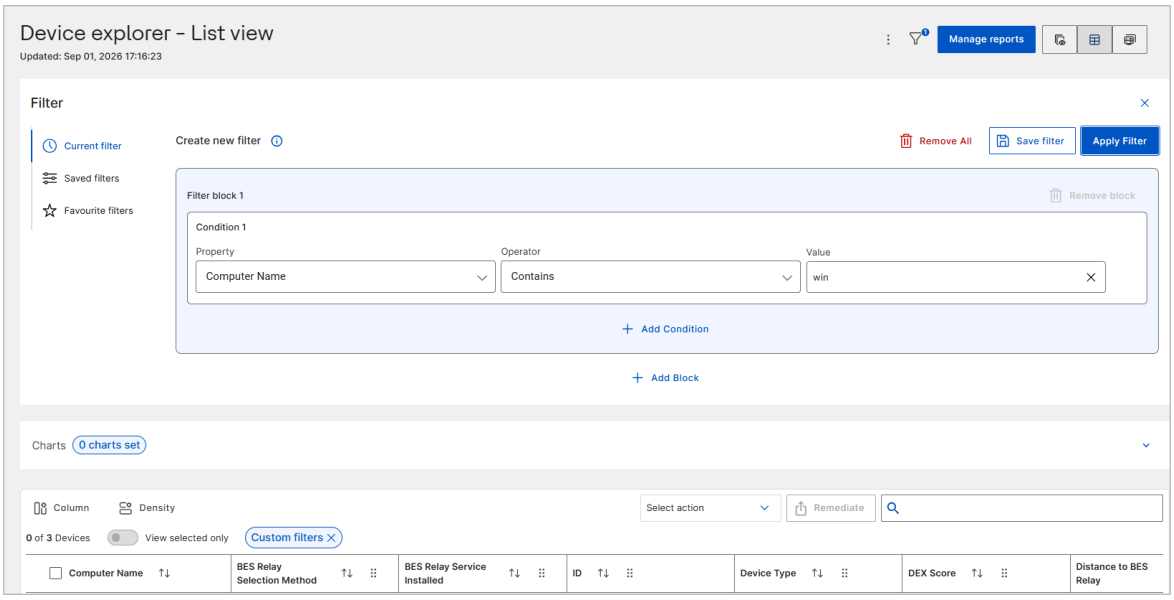
   Select a **Property**, an **Operator**, and a **Value** for each condition. Select **Add Condition** to add another condition to a filter block, or **Add Block** to add another filter block.

   The **Remove All**, **Save filter**, and **Apply Filter** buttons stay dimmed until the filter contains at least one complete condition.



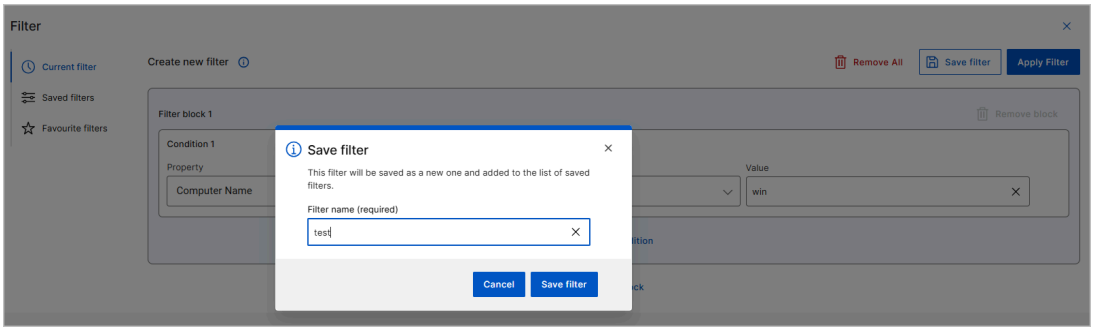
3. Select **Apply Filter** to apply the conditions to the current view.

   The table refreshes to show only the matching records, and the record count updates. A **Custom filters** tag above the table indicates that a filter is active. The **Filter** icon shows a badge with the number of active conditions.



4. To save the filter for later use, select **Save filter**.
    a. In the **Save filter** dialog, enter a **Filter name**.

    The name is required and must be unique among your saved filters for the page. If you enter a name that you already used, BigFix reports a conflict and doesn't save the filter.



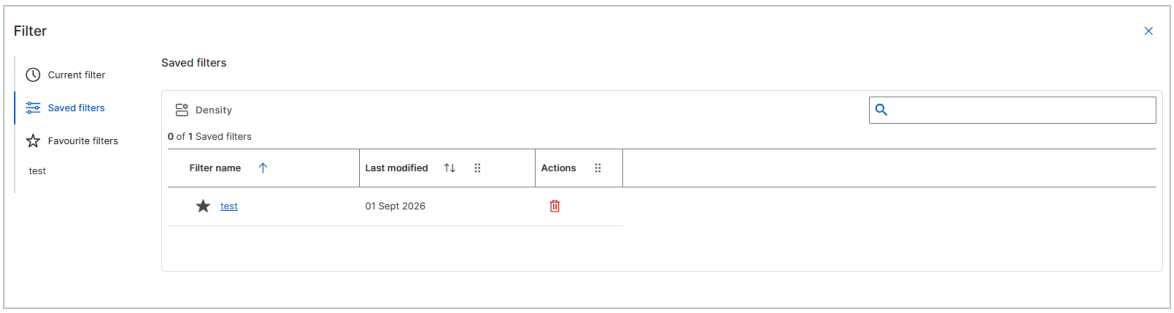
    b. Select **Save filter**.

    A **Filter saved successfully** message confirms the action, and the filter appears on the **Saved filters** tab.

Note: To edit a saved filter, apply it, change its conditions, and save it again under the same name.

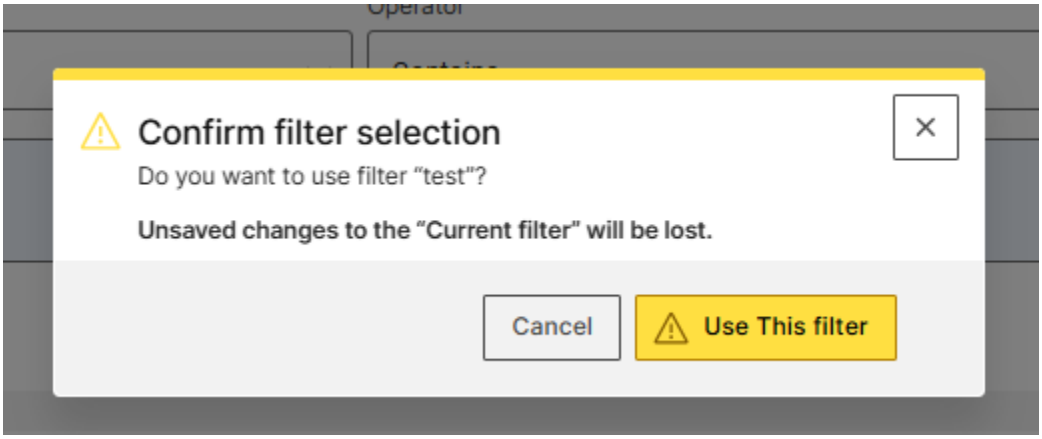
5. To review your saved filters, select the **Saved filters** tab.

    The table lists each saved filter with its **Filter name**, the **Last modified** date, a favourite (star) icon, and the available **Actions**. Use the **Search** box to find a filter by name, the sort icons in the column headers to reorder the list, and **Density** to adjust the row spacing.



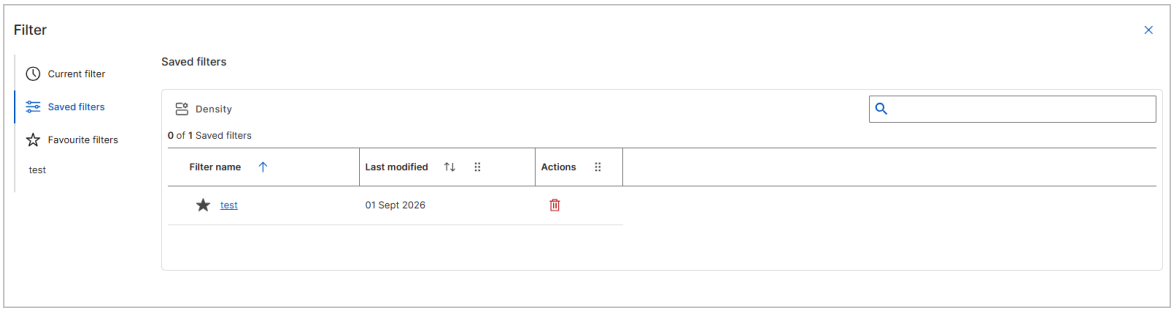
6. To apply a saved filter, select its name.

   The **Confirm filter selection** dialog asks you to confirm the change and warns that unsaved changes to the **Current filter** are lost. Select **Use This filter** to load the saved conditions into the **Current filter** tab and refresh the table, or **Cancel** to keep the current filter.



7. To mark a filter as a favourite, select the star icon next to its name.

   The star fills in, and the filter appears on the **Favourite filters** tab. To remove a filter from your favourites, select the filled star again. The **Favourite filters** tab shows the same information as the **Saved filters** tab.



8. To delete a saved filter, select the **Delete** (bin) icon in the **Actions** column.

   BigFix removes the filter from your saved filters and from your favourites. Deleting a saved filter doesn't change the filter that is currently applied to the view.

Your saved filters stay available for the page until you delete them, so you can apply the same conditions in a later session.

To clear an applied filter, open the **Current filter** tab, select **Remove All**, and then select **Apply Filter**. Removing the conditions from the current filter doesn't delete any of your saved filters.

Table filter

The table filter narrows the rows of a single data table. It is available above the table on the Sites, Analyses, Deployments, All Reports, Scheduled Reports, User Management, and Roles pages. You can't save a table filter; it stays active until you clear it or reload the page.

Select **Filter** (funnel icon) above the table to open the filter panel, and then build each condition from three parts:

- **Property** – The column that you want to test, such as **Name**.
- **Operator** – The comparison to make, such as **Contains**.
- **Value** – The text or value to match.

Filtering a table

1. Above the table, select **Filter** (funnel icon).
2. Select a **Property** and an **Operator**, and then enter a **Value**.
3. Optional: To filter on more than one property, select **Add filter**. A second row appears with an **And** or **Or** list. Select **And** to return only the rows that match every condition, or **Or** to return the rows that match any condition.
4. Optional: To remove one condition, select the minus icon at the end of its row. To clear every condition, select **Remove All**.
5. Select **Apply**.

   The table refreshes to show only the matching rows, and the **Filter** icon shows a badge with the number of conditions that are applied. **Apply** stays dimmed until the condition is complete.



Note: On pages that also provide a search box, such as Sites, the applied filter combines with the text that you type.

Filter by query

The query filter defines a set of devices or Fixlets. Unlike the other filter types, it doesn't just change what you see: it determines which records the object acts on. You use it wherever BigFix UI asks you to target a set of records, for example:

- The **Devices** and **Fixlets** steps of the remediation, Fixlet deployment, and custom remediation flows, to choose what the deployment targets. See Setting-up Remediation Flow *(on page 111)* and Deploying Fixlets *(on page 167)*.
- The membership criteria of a dynamic device group. See Creating and Managing Device Groups *(on page 98)*.
- The device subscription rule of a custom site. See Managing a custom site *(on page 205)*.
- The device scope of a role. See Managing Roles *(on page 467)*.
- The bulk selection of Fixlets when you assign tags. See Managing Tags *(on page 51)*.

The controls differ a little from one context to another, but the conditions always work the same way. Where the filter targets devices, **Filter By** usually offers three methods:

- **Query** – Build conditions that match device properties.
- **Device group** – Select one or more existing device groups.
- **Device list** – Paste a fixed list of devices, identified by name, DNS, or IP address.

Note: Some contexts offer more options. A dynamic device group, for example, can also match devices with a **Relevance expression** that you write, and combines its enabled sections with an **All conditions (Criteria: AND)** or **ANY** top-level condition.

Building a query filter

1. Under **Select top level filter condition**, select **Single condition** to use one filter block, or **Multiple condition (Criteria: OR)** to return the records that match any block.
2. Under **Filter block 1: select condition**, select **Single condition** to use one condition, or **Multiple conditions (Criteria: AND)** to require every condition in the block.
3. For **Condition 1**, select a **Property** and an **Operator**, and then enter a **Value**.

   Some operators, such as **In**, accept several values. Each value that you enter appears as a chip under **Selected Values**. Select the **X** on a chip to remove that value.
4. Optional: Select **Add Block** to add another filter block, or **Remove block** to delete one.
5. Select **Apply**.

   The table or preview below the filter refreshes to show the matching records. In a deployment flow, the footer also shows the running count, such as **Selected 2 Devices**. When you create a dynamic group, the **Preview of dynamically applicable targeted devices** section shows the devices that match.
6. Confirm your selection.

   In a deployment flow, select the checkbox next to each record that you want to include, and then select **Next**. When you define a group, a subscription, or a role scope, the conditions themselves are the definition, so you save the object instead.

Select **Reset Filters** at any point to clear the conditions and start again.

Note: Some contexts evaluate your conditions continuously rather than once. In a deployment flow, turn on **Dynamic targeting device** so that any device matching the conditions later also receives the deployment. A dynamic device group and a site subscription rule behave the same way: membership updates as devices start or stop matching. For more information, see Setting-up Remediation Flow *(on page 111)*.

Related information

Common Functionalities *(on page 28)*

Devices *(on page 77)*

Fixlets *(on page 145)*

CyberFOCUS *(on page 277)*

Report Builder *(on page 384)*

Setting-up Remediation Flow *(on page 111)*

Deploying Fixlets *(on page 167)*

Custom Remediation *(on page 241)*

Creating and Managing Device Groups *(on page 98)*

Managing a custom site *(on page 205)*

Manage Reports

Save, load, and organize the custom reports that you generate in BigFix UI. Use this feature to preserve a view that you use often, such as a set of filter conditions, columns, and charts, and to reopen it later.

The Manage Reports feature preserves frequently used report views or filter conditions in Device Explorer, Fixlet Explorer, Deployment Manager, and the Analyses app. Reports that you save in one application, for example Device Explorer, are listed on the All Reports page, which gives you central management and quick access.

The Manage Reports panel slides out when you select **Manage Reports** from the upper-right corner of the List View. It provides two tabs:

- **Save Report** – Store a new report configuration.
- **Load Report** – View and reopen a report that you saved earlier.

With Manage Reports, you can:

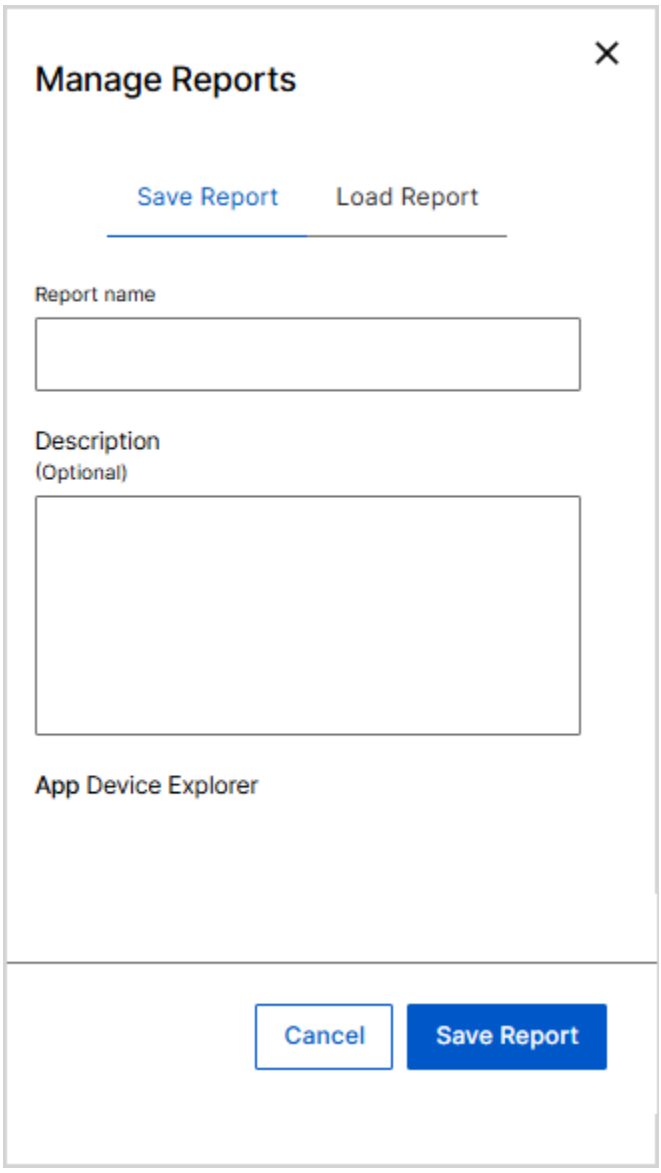
- Save a report with a meaningful name and an optional description.
- Update or overwrite a report that you saved earlier.
- Load an existing report to reapply its saved filters or data views.
- Set or remove a report as your default view for the List View page.

- Manage reports across multiple BigFix UI applications.
- Access your own saved reports for personalized workflows.

Saving a report

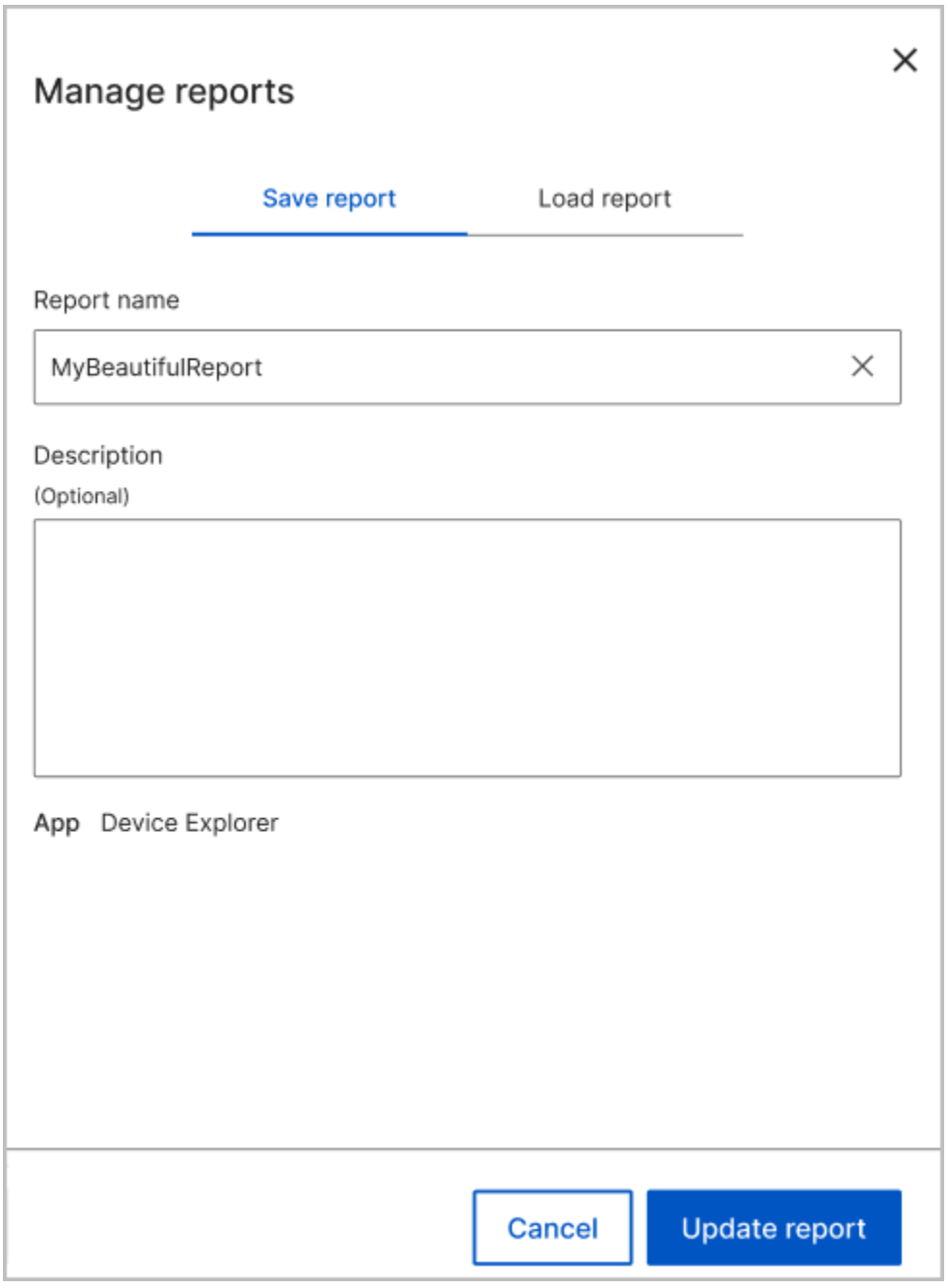
1. In the List View of Device Explorer, Fixlet Explorer, Deployment Manager, or the Analyses app, select **Manage Reports**.

   The Manage Reports panel slides out from the upper-right corner of the List View.



2. Enter a **Report name**.
3. Optional: Provide a **Description** to help identify the report's purpose or filter set.
4. Verify the associated application, for example App Device Explorer.
5. Select **Save report**.

If you opened a saved report and changed it, the button reads **Update report**. Select it to save your changes to the same report.



The report appears on the All Reports page for future access.

Note: If you modify an existing report on the **Save report** tab and try to switch to the **Load report** tab without saving your changes, a dot marks the **Save report** tab and the drawer shows the message `The current report`

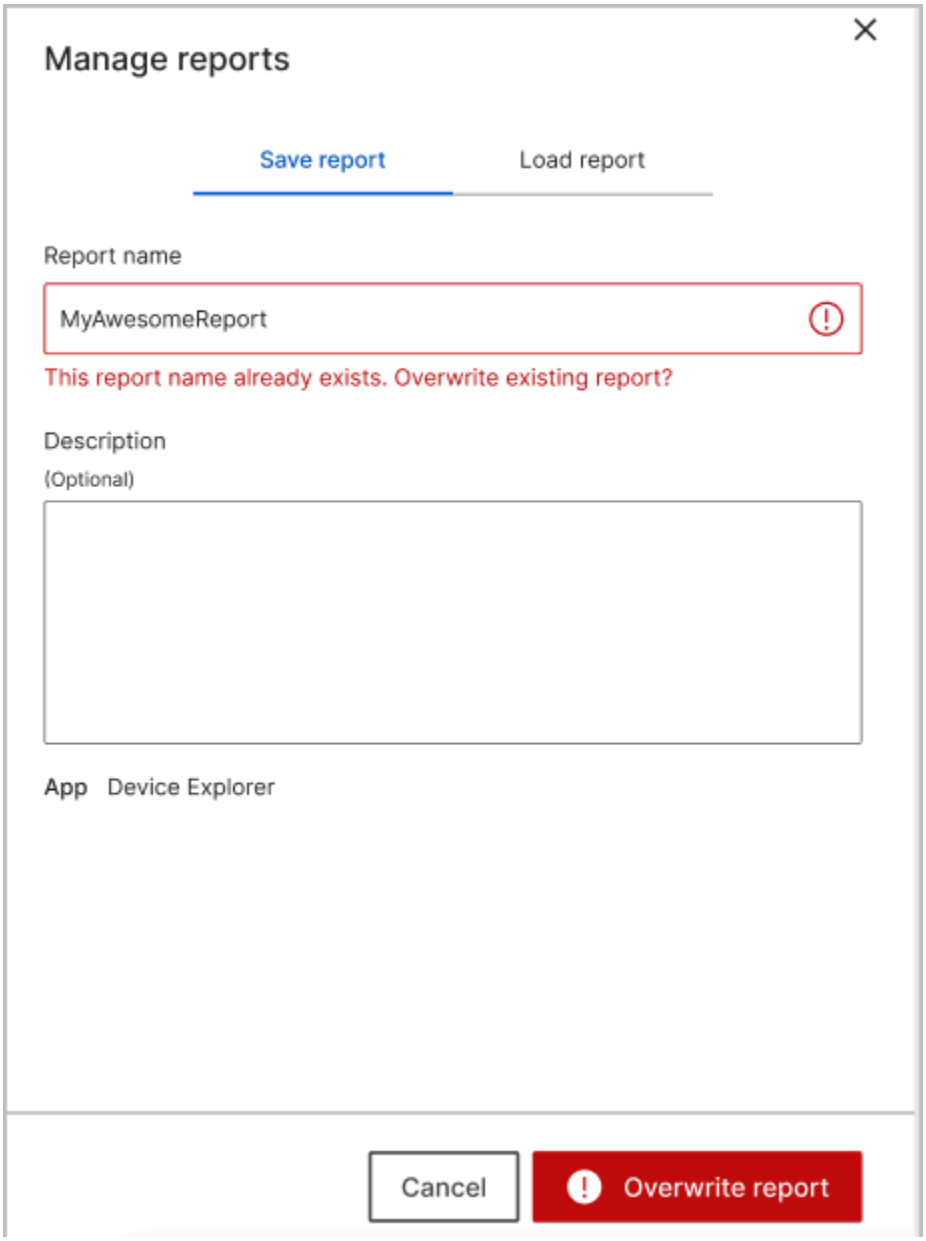
`has unsaved changes`. To keep the changes, return to the **Save report** tab and save the report before you load another one.

Overwriting an existing report

If you enter a report name that is already in use, the field shows the message `This report name already exists. Overwrite existing report?` and the button changes to **Overwrite report**.

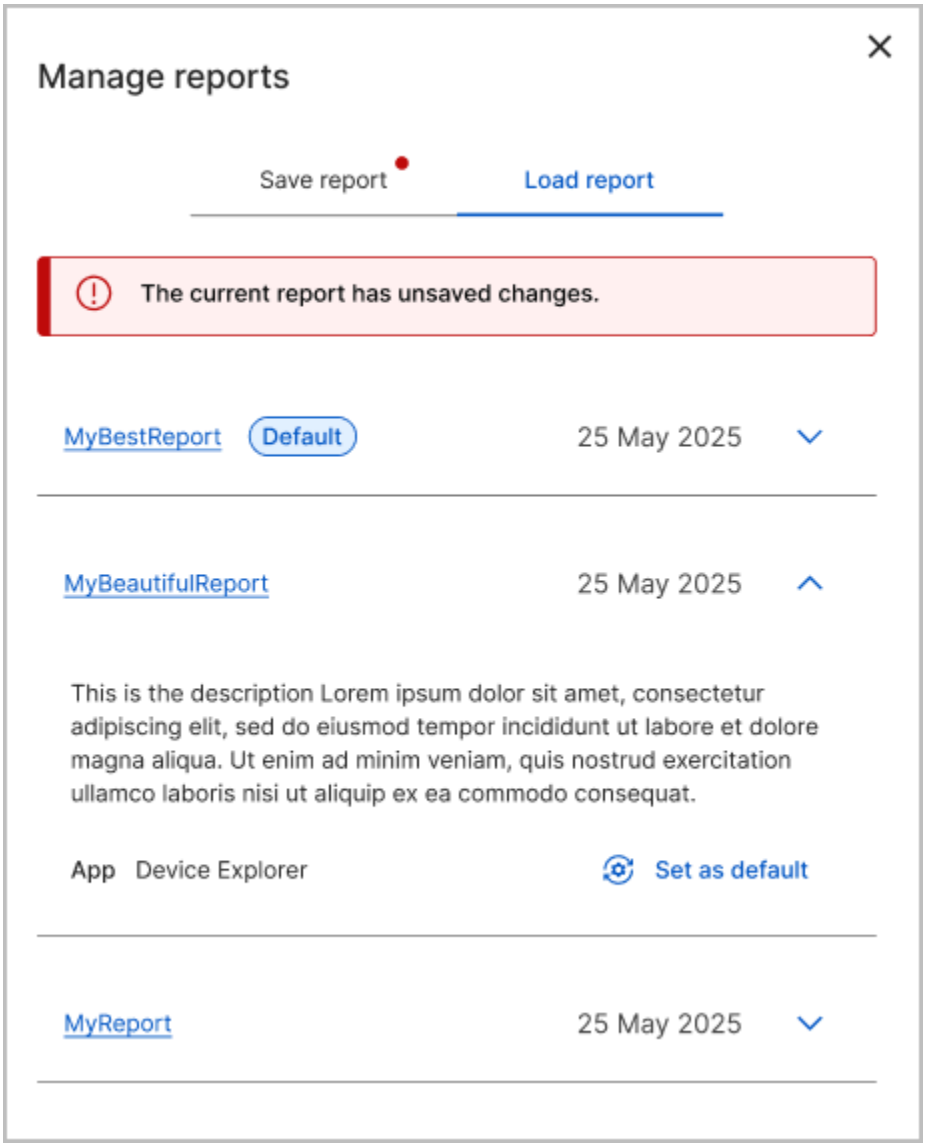
1. On the **Save report** tab, enter the name of the report that you want to replace.
2. Optional: Update the **Description**.
3. Select **Overwrite report**.

The current view replaces the saved report, and the drawer closes.



Loading a report

1. Select **Manage Reports** on the List View toolbar, or open the All Reports page.



2. Select the **Load report** tab.
3. Review the list of available saved reports.

   Each row shows the report name and the date it was last updated. Select the arrow at the end of a row to expand it and view the description, the application, and the default report actions.

4. Select a report name to load it.

   A tooltip opens. If the current report has unsaved changes, the tooltip warns you about them. Select the link in the tooltip to load the selected report.

The associated filters, columns, charts, and view settings are restored.

5. Optional: Edit the filters or sorting, and then save the report again with a new name.

Setting a default report

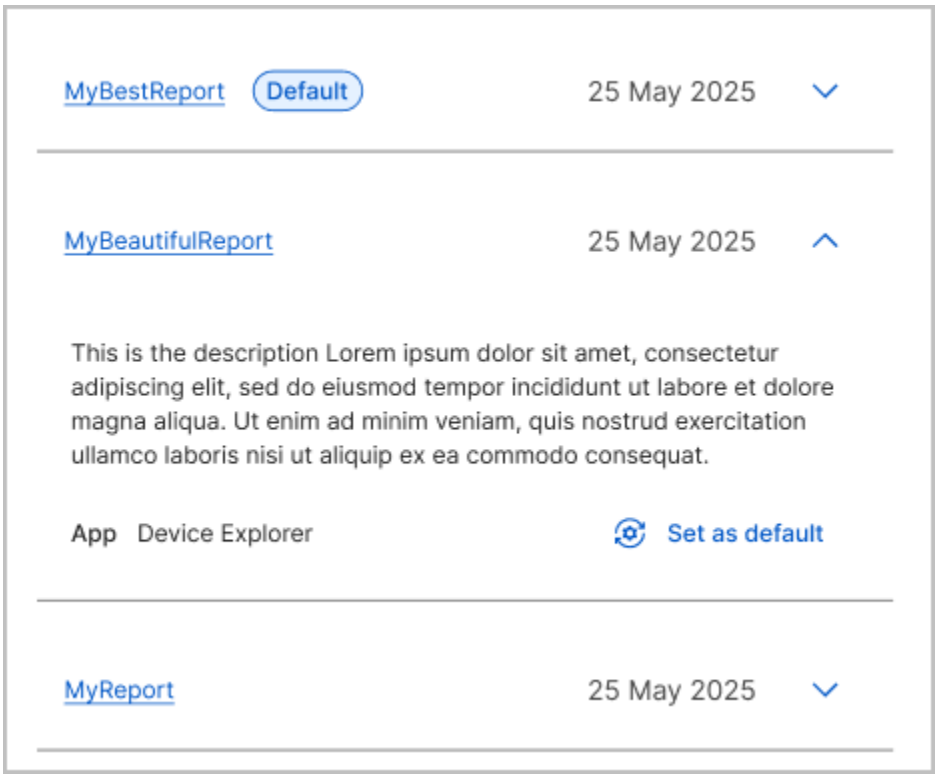
A default report is the view that opens when you go to the List View page of a supported application, such as Device Explorer, Fixlet Explorer, and Deployment Manager apps. The default report restores its saved charts, columns, sorting, and filters. If you do not set a default report, the List View page opens with the standard columns and settings and no charts.

Note: A default report applies only to the List View page. It does not change the Overview page.

To set a default report:

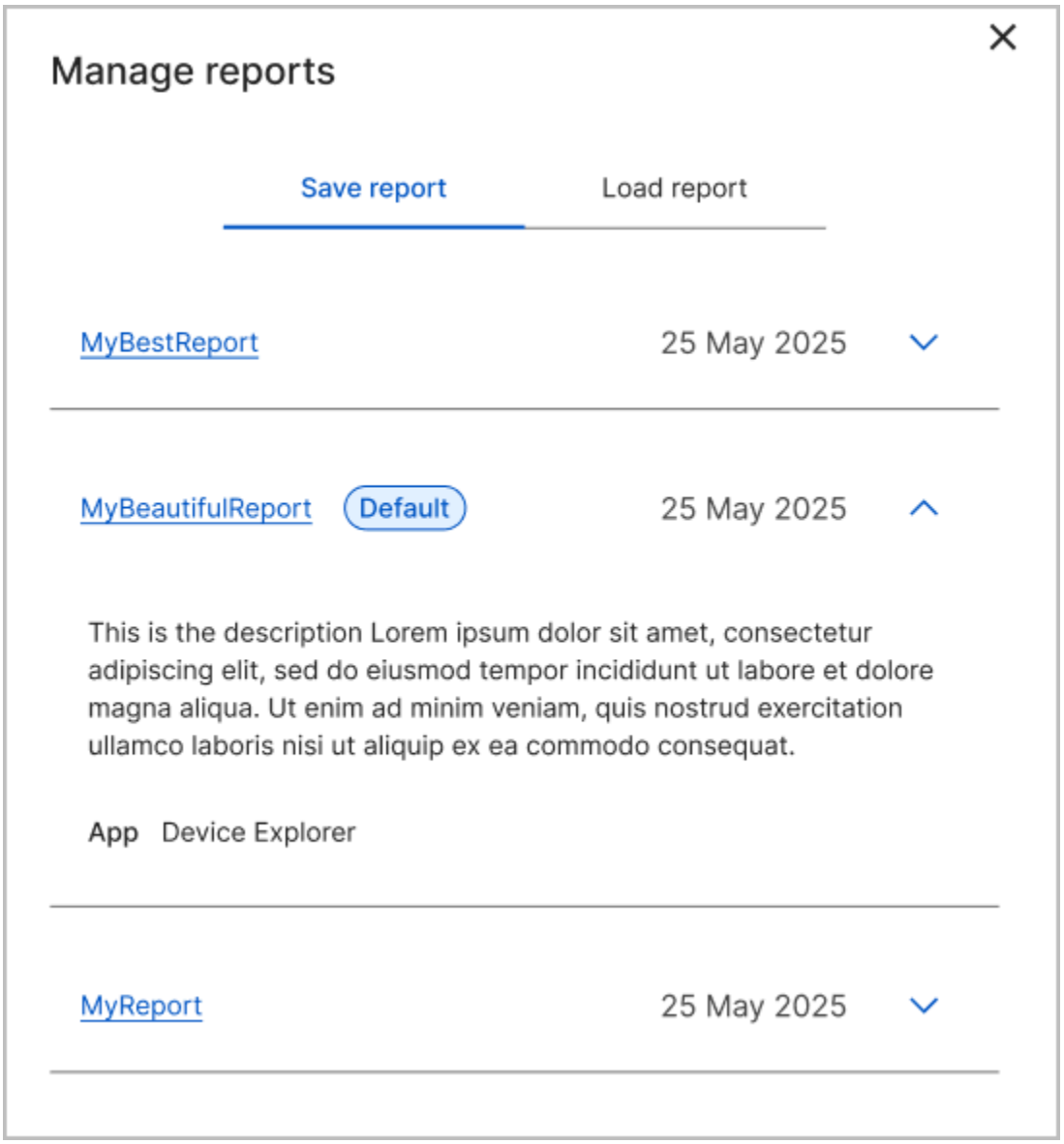
1. On the List View page, select **Manage Reports**, and then select the **Load report** tab.
2. Expand the report that you want to use.
3. Select **Set as default**.

   The setting is saved automatically. A **Default** tag appears next to the report name, and the List View page reloads with that report.



To change the default, repeat these steps for a different report. The **Default** tag moves to the new report, and the previous report loses it. The reports keep their position in the list.

If you edit the default report and save it, the saved report stays the default.

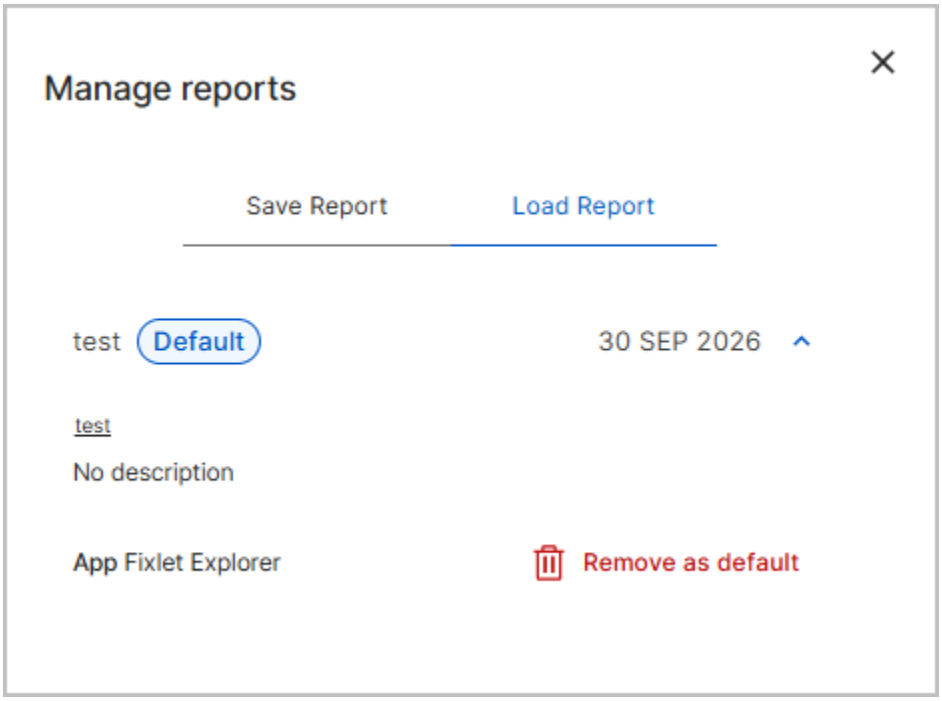


Removing the default setting

You can remove the default setting from a report and keep the report itself.

1. On the List View page, select **Manage Reports**, and then select the **Load report** tab.
2. Expand the report that has the **Default** tag.
3. Select **Remove as default**.

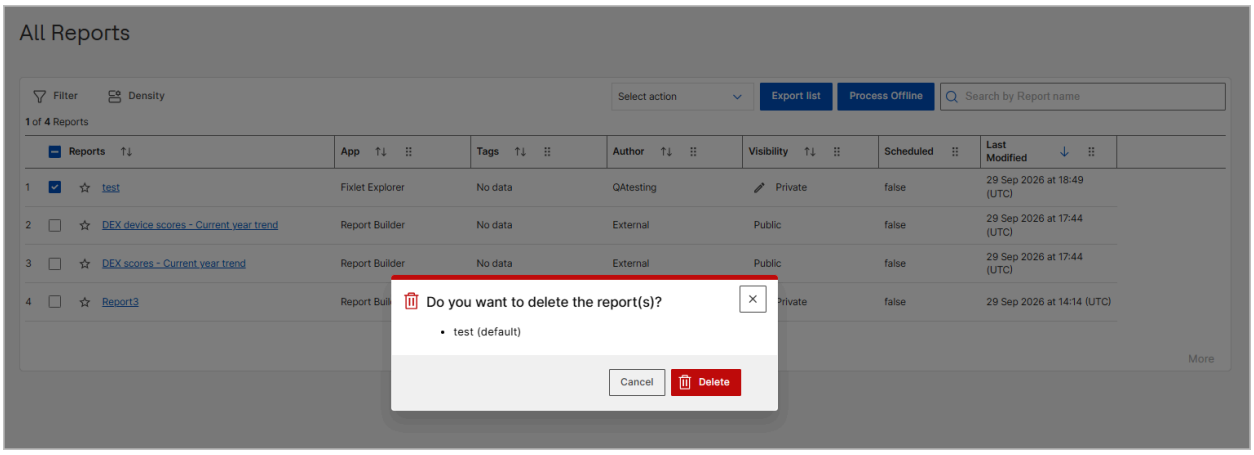
The **Default** tag is removed, and the List View page reloads with the standard columns and settings.



Deleting a default report

When you delete a report that is set as default, the confirmation window warns you that you are deleting the default report.

- Select **Cancel** to keep the report and the default setting.
- Confirm the deletion to remove the report permanently. The List View page then opens with the standard columns and settings.



Things to know

- Reports are saved per user and are not shared globally.
- When you load an older report, make sure that the related data sources, such as devices and Fixlets, are still available in your environment.
- Saved report names must be unique within each application. If you reuse a name, you can overwrite the existing report.
- Only one report can be the default for each application, and the default applies only to your user account.
- The default setting is saved automatically. You do not need to select a save button.

Related information

Common Functionalities *(on page 28)*

All Reports *(on page 355)*

Devices *(on page 77)*

Fixlets *(on page 145)*

Deployments *(on page 181)*

Analyses *(on page 214)*

Managing Tags

Tags are custom labels that you attach to Fixlets, deployments, reports, and analyses so that you can group, filter, and track related content across BigFix UI.

A tag is a short, free-form label, such as *Security*, *Patch-Tuesday*, or *Finance-Servers*. You create tags as you need them and reuse them across objects. Tags carry no built-in meaning, so you decide what each one stands for. Use them to mark ownership, priority, project, or any other grouping that your team follows.

Tags organize content so that you can find and filter it. They don't control what a deployment targets or which devices a policy reaches.

Because the same tag can apply to many objects, you can trace a change from the Fixlet that defines it, through the deployment that runs it, to the report that measures it.

Where you can use tags

The following table lists the objects that support tags and what you can do with each one.

Table 3. Tag support by object

Object	Where you assign tags	Where you view or remove tags
Fixlets	Fixlet Explorer – List View, using **Select action** > **Manage tags**; the Fixlet detail page; and the **Tag** field when you create or edit a custom Fixlet.	The **Tags** column in the list view and the **Tags** widget on the Fixlet detail page.
Deployments	The **Summary** step of the remediation and custom remediation flows.	The **Tags** column in the Deployment Manager and the **Tags** widget on the Deployment Details page. Deployment tags are read-only after the deployment is created.
Reports	The All Reports page, using **Select action** > **Manage tags**, and the **Report details** panel.	The **Tags** column on the All Reports page.
Analyses	The analysis detail page, using **Manage tags**.	The **Tags** column on the **Analyses** tab and the **Tags** field in the analysis details card.

Note: You can't rename a tag. To correct a name, remove the tag from the object and assign a new one.

Devices don't support tags. To organize devices, use Device Groups *(on page 94)*.

The Manage tags drawer

Tag management always opens a single-step drawer from the right side of the screen. The drawer works the same way in Fixlet Explorer, All Reports, and Analyses, from both the list view and the detail page, and whether you tag one object or many. Select your tags, and then select **Save changes**.

When you tag more than one object from a list view, the drawer footer shows the number of objects that receive the tags, for example **4 Fixlets selected**.

The **Select tags** box works the same way everywhere:

- To apply an existing tag, start typing. Matching tags appear in a suggestion list; select the ones you want.
- To create a tag, type a name that doesn't exist yet, and then select **Add**. The tag is created and applied in one step.
- Selected tags appear below the box as chips. To remove a tag, select the **X** on its chip.
- To clear every selection and start over, select **Reset tags**.
- To close the drawer without changing the assigned tags, select **Cancel**.

Note: When you tag more than one object at once, the suggestion list shows only the tags that every selected object already has. Tags that only some of the selected objects have do not appear. You can still create new

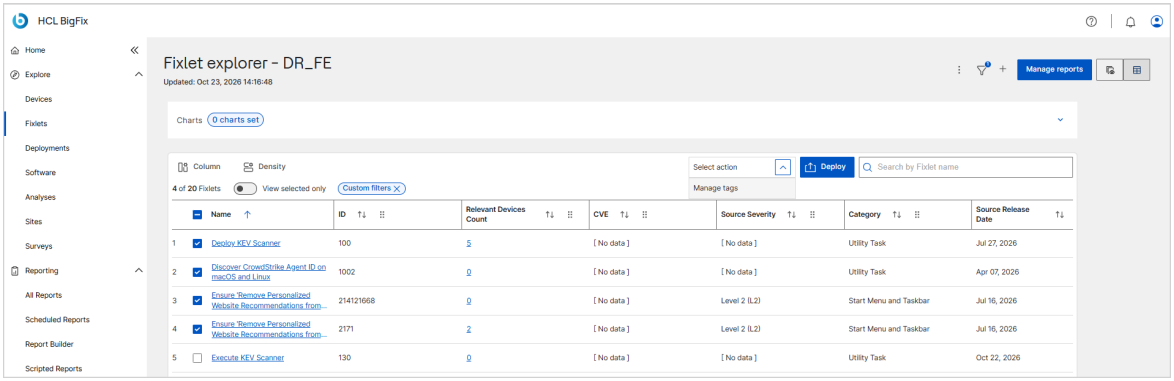
tags and assign them to all the selected objects. To give the other objects a tag that only some of them have, tag each of those objects on its own.

When the assignment finishes, the drawer closes automatically, a success message appears in the top-right corner, and the data table or detail page reloads automatically to show the new tags. You don't need to refresh the page.

Assigning tags to Fixlets in bulk

Tag many Fixlets at once from the Fixlet Explorer – List View. Use this method to label a set of Fixlets that share a CVE, a severity, or a maintenance window.

1. In the side navigation, expand **Explore** and select **Fixlets**. Switch to the list view.



2. Select the checkbox next to each Fixlet that you want to tag.
3. From the **Select action** list above the table, select **Manage tags**. The **Manage tags** drawer opens and shows the tags already assigned to the selected Fixlets. The footer confirms how many Fixlets receive the tags, for example **4 Fixlets selected**.
4. In the **Select tags** box, select existing tags or create new ones.

   Note: The suggestion list does not show tags that only some of the selected Fixlets have. To add one of those tags to the other Fixlets, use the Fixlet detail page or select those Fixlets on their own.

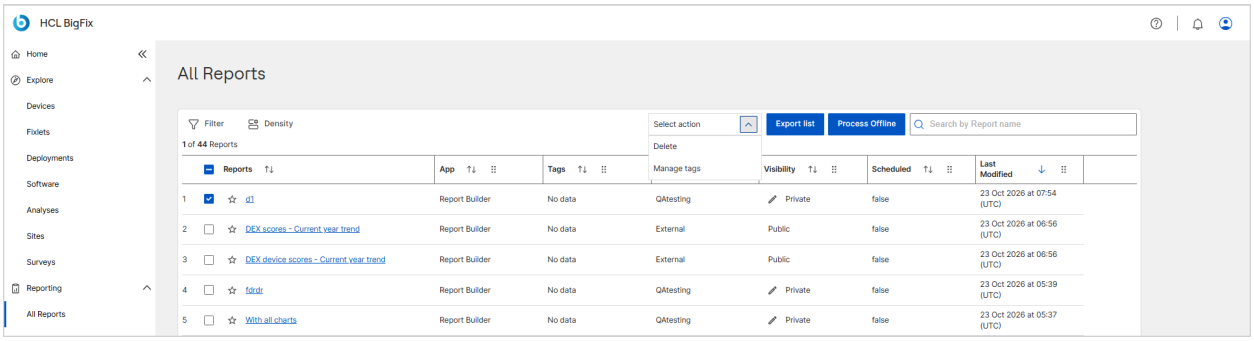
5. Select **Save changes**.

The drawer closes automatically, a success message appears, and the Fixlet table reloads to show the updated **Tags** column for each Fixlet that you tagged. You don't need to refresh the page.

Note: A single request tags a limited number of Fixlets. If you select more Fixlets than the configured limit, split the work into smaller batches.

Assigning tags to reports

On the All Reports page, select one or more reports, and then select **Select action** > **Manage tags**. The single-step drawer opens; select or create your tags, and then select **Save changes**. For the full procedure, see Assigning tags to reports *(on page 357)*.



Assigning tags to analyses

On the analysis detail page, next to **Tags**, select **Manage tags**. The single-step drawer opens. Select or create your tags, and then select **Save changes**. The drawer closes, and the details card refreshes with the new tags. For the full procedure, see Analysis detail page *(on page 217)*.

Assigning tags to deployments

You assign deployment tags while you set up the deployment, not afterward. On the **Summary** step of the remediation or custom remediation flow, use the **Assign tags** field to select or create tags, and then complete the deployment. The tags are saved with the deployment and appear in the Deployment Manager and on the Deployment Details page.

For the flows that support this, see Setting-up Remediation Flow *(on page 111)*, Deploy Script *(on page 243)*, Install Software *(on page 256)*, and Update Windows Registry *(on page 267)*.

How tags appear in data tables

The Fixlet Explorer – List View, the Deployment Manager, the All Reports page, and the **Analyses** tab each include a **Tags** column. The column adapts to the number of tags on each row:

- **No tags** - The cell shows *No data* or a dash.
- **One tag** - The cell shows the tag name as plain text, for example *tag1*.
- **More than one tag** - The cell shows a link with the count, for example *2 tags*. Select the link to open a drawer that lists every tag on that row.

You can sort and filter on the **Tags** column like any other column, which lets you gather all objects that carry the same tag.

Viewing and removing tags

Select a tag count link in a data table, or select **Manage tags** on a detail page, to open the tag drawer. The drawer lists the tags assigned to that object as chips.

For Fixlets, reports, and analyses, you can remove tags from the drawer:

1. Select the **X** on each tag chip that you want to remove.
2. Select **Save changes**.

The tags are unlinked at once, without a confirmation prompt. The drawer closes automatically, a success message appears, and the data table or detail page refreshes to show the updated tag count. You don't need to refresh the page.

To discard your changes instead, select **Cancel**. To restore the tags that were assigned when you opened the drawer, select **Reset tags**.

Removing a tag from one object doesn't affect any other object that uses the same tag.

Note: Deployment tags are read-only. The drawer for a deployment lists its tags but offers no remove control.

Permissions

Tagging follows the permissions that already apply to the object. If your role lets you edit a Fixlet, deploy an action, or manage a report, you can also manage its tags. When you lack the permission, the **Manage tags** action is unavailable.

Related information

Common Functionalities *(on page 28)*

Fixlets *(on page 145)*

Fixlet Explorer Details page *(on page 155)*

Deployments *(on page 181)*

All Reports *(on page 355)*

Analysis detail page *(on page 217)*

Device Groups *(on page 94)*

Prescriptive Guidance

Prescriptive Guidance provides actionable recommendations to users based on best practices, industry standards, and specific organizational policies. This feature enhances operational efficiency, reduces manual effort, and strengthens security posture by guiding users towards optimal configurations and actions tailored to their environment.

Key benefits

- **Standardization of Best Practices:** It helps ensure that all endpoints within an organization adhere to standardized best practices for security, configuration, and compliance.
- **Efficiency and Consistency:** By providing clear, actionable recommendations, prescriptive guidance enables IT teams to efficiently manage a large number of endpoints with consistent policies and configurations.
- **User Empowerment:** It empowers IT administrators and endpoint users by equipping them with the knowledge and tools needed to implement recommended actions effectively. By providing clear, structured recommendations, prescriptive guidance empowers users with the knowledge and tools needed to maintain a secure and efficient endpoint environment.
- **Adaptability to Change:** Prescriptive guidance adapts to evolving threats, regulatory requirements, and technology changes, ensuring that endpoint management practices remain current and effective.
- **Automation and Scalability:** Guidance often includes automated workflows or scripts that enable automated enforcement of policies and configurations, improving scalability and reducing manual effort. The guidance may include automated workflows or scripts that users can deploy to streamline routine tasks such as patching, software updates, or configuration changes.
- **Compliance Assurance:** It supports organizations in meeting regulatory compliance requirements by guiding them towards configurations and practices that align with industry standards and regulations.
- **Ongoing improvement**: It supports ongoing improvement by adapting to new threats, regulatory changes, or operational requirements, ensuring that users stay current with best practices in endpoint management.

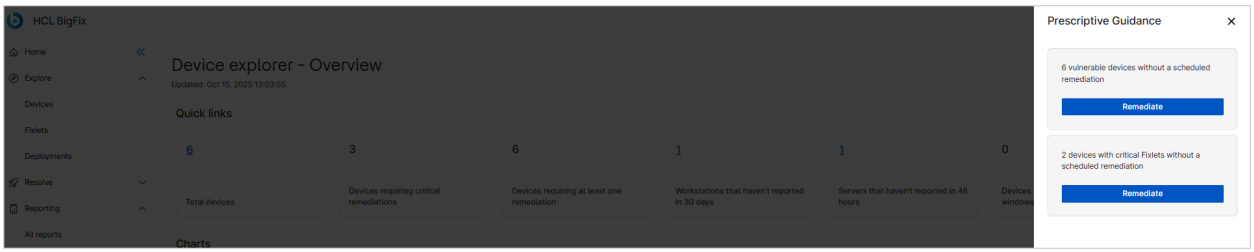
Scenarios and use cases

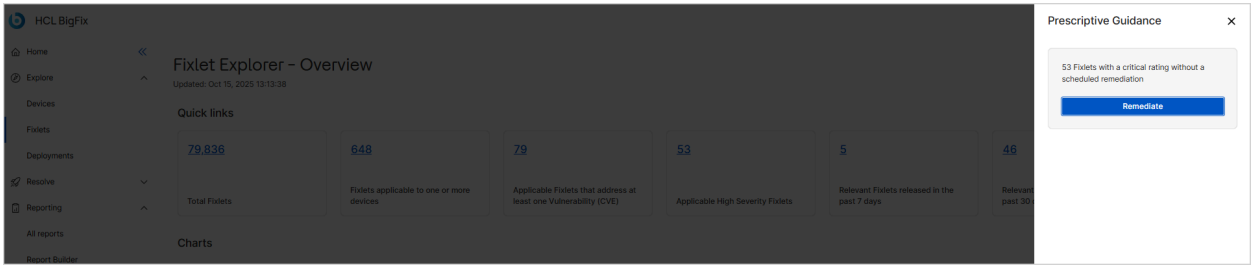
- **Scenario 1: Vulnerability Management**
    - An IT team uses prescriptive guidance to identify and prioritize critical vulnerabilities across their endpoint devices. By following the step-by-step recommendations, they efficiently apply patches and mitigate risks.
- **Scenario 2: Regulatory Compliance**
    - A financial institution leverages prescriptive guidance to align their endpoint configurations with industry regulations. Automated workflows ensure continuous compliance and reduce the burden of manual checks.
- **Scenario 3: Endpoint Standardization**
    - A global enterprise with a diverse set of endpoints utilizes prescriptive guidance to standardize security and configuration practices across all devices. This ensures consistency and reduces the risk of security breaches.

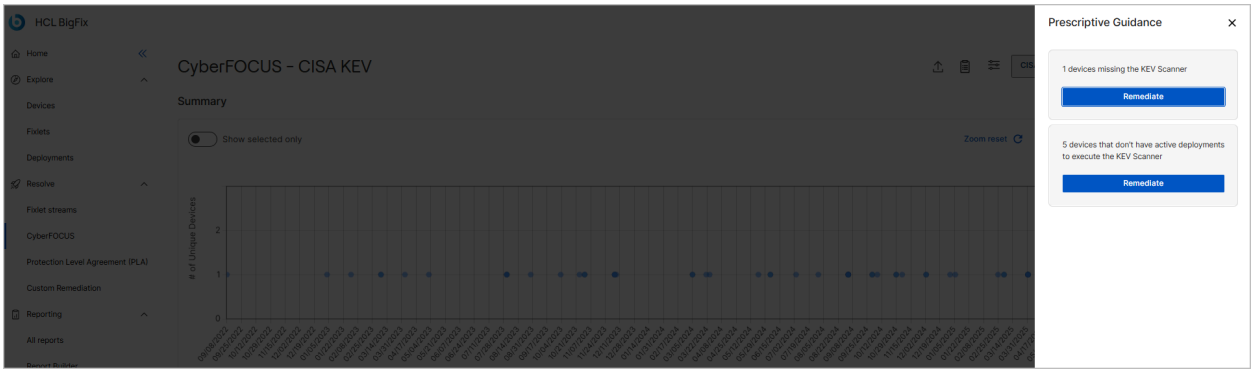
- **Scenario 4: Routine Maintenance**
    - An organization deploys automated scripts provided by prescriptive guidance to streamline routine maintenance tasks such as software updates and configuration changes, enhancing operational efficiency.

How to access

This feature is integrated with the Device Explorer, Fixlet Explorer, and CyberFOCUS apps. When you access these apps, click on the  icon to open the Prescriptive Guidance panel on the right.







The **Prescriptive Guidance** feature automatically identifies devices in your environment that are vulnerable and do not have a scheduled remediation action. It helps you take timely action by highlighting risks and streamlining the remediation process.

- The recommendations are based on your environment's current state.
- The guidance helps prioritize high-risk vulnerabilities and streamlines the remediation steps needed to address them.

- The **Remediate** button appears when vulnerabilities are detected.
- Clicking the **Remediate** button opens the **Remediation Workflow**, where:
  - All applicable fixlets and devices are **pre-selected automatically** based on the prescriptive guidance.
  - You can review and modify the selection before proceeding.

Note: If you close the Prescriptive Guidance window, you need to reload the app to access it again.

Related information

Common Functionalities *(on page 28)*

2. Configuring the remediation steps *(on page 294)*

Devices *(on page 77)*

Fixlets *(on page 145)*

Notification Center

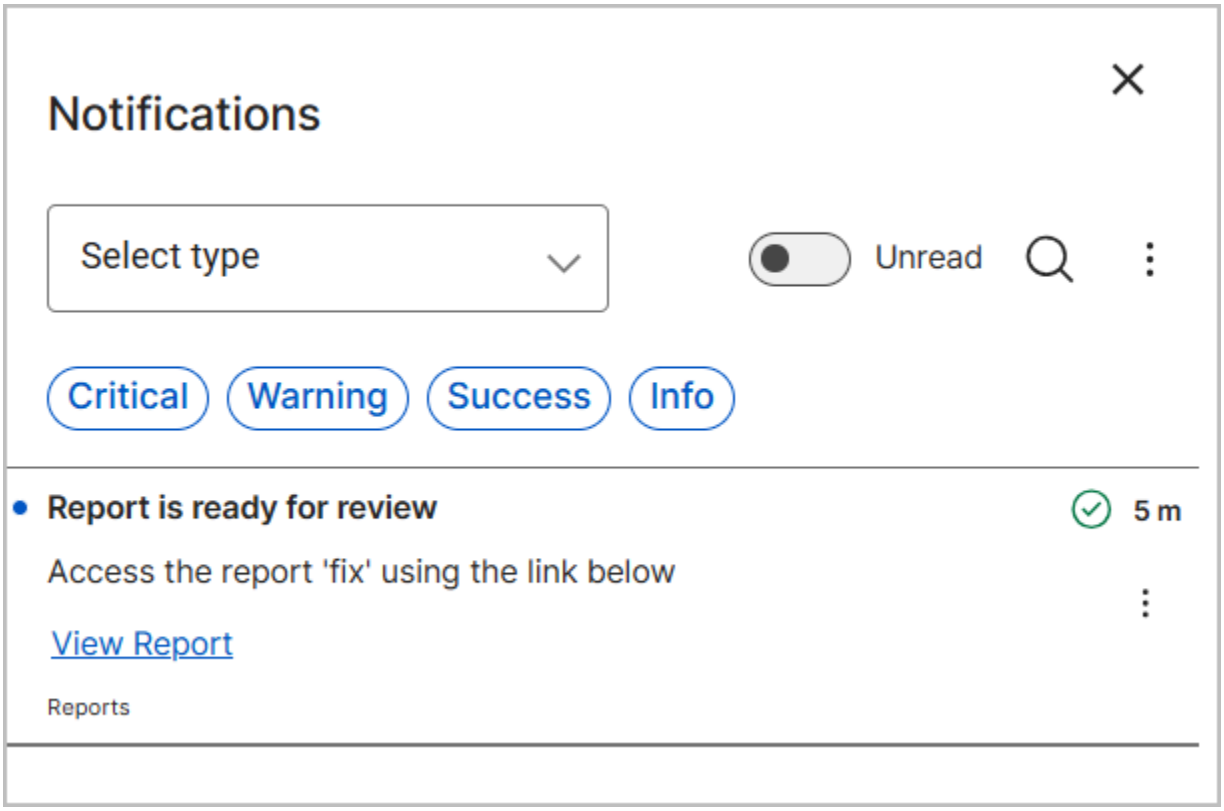
The Notification Center is a central place to view, filter, and manage the real-time notifications that BigFix UI raises about your work across the application. You open it from the bell icon in the upper-right corner of the screen.

Any operation that you perform in BigFix UI can raise a notification, so that you do not need to watch a module to know what happened. For example, you are notified when a report is ready to view, when a deployment finishes, or when a Protection Level Agreement (PLA) is created. Notifications come from across the application, including Analyses, Application Configuration, Applications Versions, Custom Remediation, CyberFOCUS, Deployment Manager, Device Explorer, Fixlet Streams, Identity and Access, My Dashboard, Patch, Reports, Site Management, Software Package, and System Configuration. For the full list in your environment, open the **Select type** list in the Notification Center.

A **bell** icon in the upper-right corner of the screen, next to the Help Center (**?**) icon and your profile icon, gives you access to these notifications from anywhere in the application. When you have unseen notifications, a badge on the bell shows how many there are.



To open the Notification Center, select the **bell** icon. The Notification Center slides out from the right side of the screen and lists your notifications, with the most recent at the top. After you open the Notification Center, the unseen badge on the bell clears. To close it, select the close (**X**) icon.



If you are signed in to BigFix UI in more than one browser session, a notification is delivered to all of your open sessions, so you see it wherever you are working.

Each notification appears as a card. A card shows a status icon for the notification's severity, the title, a short message, and the name of the module that raised it, such as **BigFix Explore**, **Protection Level Agreement (PLA)**, **Integrated Vulnerability Remediation**, **DEX**, or **Reporting**. A card can include a link, such as **View Report**, below the message. A link can also sit inside the message text, for example **Deployment name Cinzia_totale has been successfully completed** or **234 Deployments are expired and not in use**. In both cases, selecting the link opens the related item.

A long message is shortened with an ellipsis on the card. Open the linked item to read the full text.

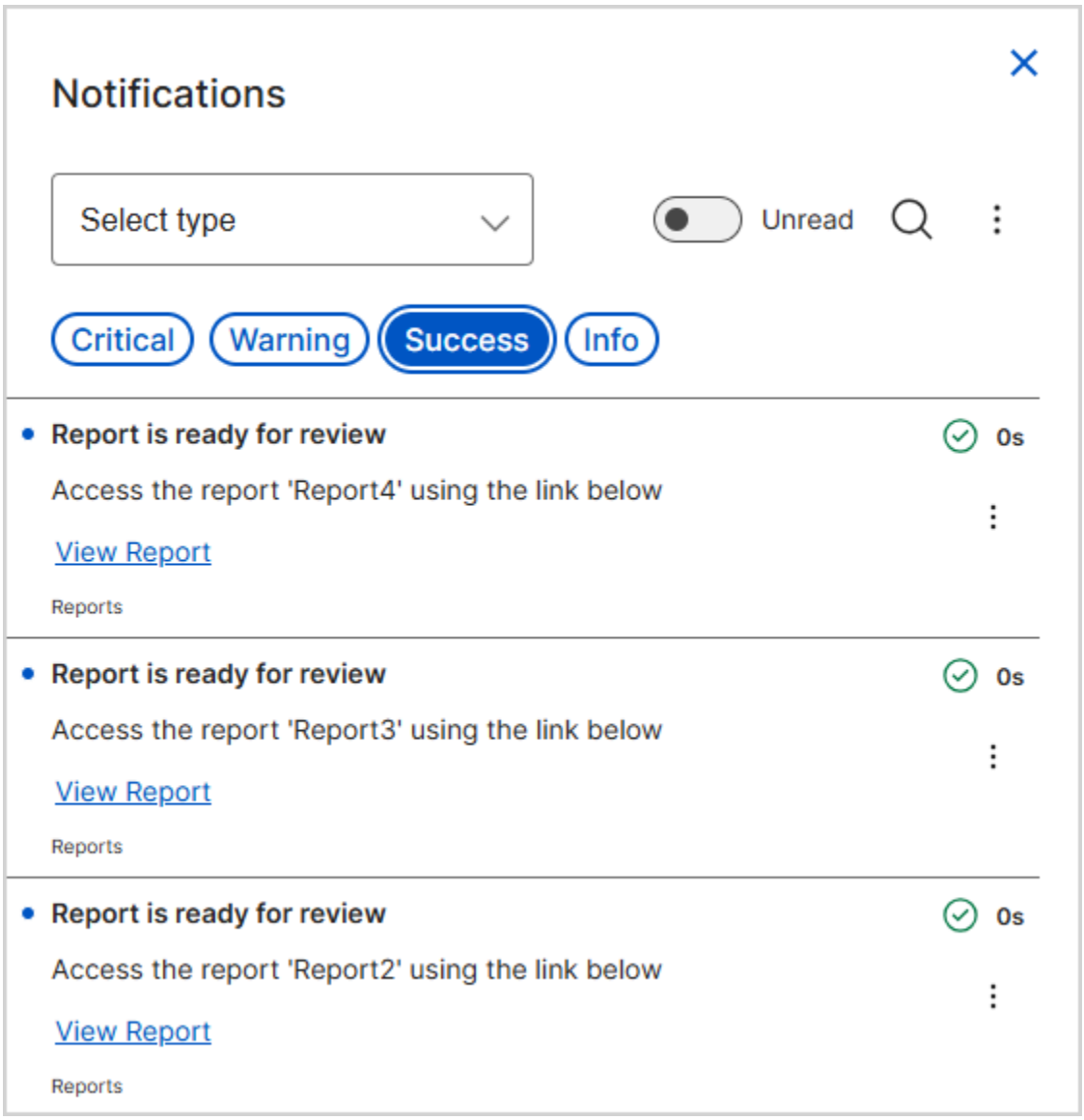
The card shows how long ago the notification arrived as elapsed time in a compact format, such as **15s**, **3 m**, **22 m**, **2h**, or **22h**. Older notifications show a date instead, such as **3 Feb**. Unread notifications are marked with a blue dot.

The following examples show the kinds of notification that can appear, each with the module that raised it:

- **Deployment successful.** Confirms that a named deployment completed. Raised by BigFix Explore, with Success severity.
- **Expired deployments.** Reports deployments that are expired and no longer in use. Raised by BigFix Explore, with Info severity.
- **PLA creation pending.** Reports that a Protection Level Agreement could not be created. Raised by Protection Level Agreement (PLA), with Warning severity.
- **Deployment is not completed.** Reports a remediation deployment that did not finish. Raised by Integrated Vulnerability Remediation, with Warning severity.
- **New security patches available.** Reports critical updates that are ready to deploy. Raised by DEX, with Info severity.
- **Baseline policy updated.** Reports a published change to a security baseline. Raised by BigFix Explore, with Info severity.
- **Multiple devices offline.** Reports endpoints that have not checked in. Raised by Reporting, with Critical severity.

When no notifications match the current view, the Notification Center shows **No notifications to show**. When you have loaded everything available, the end of the list shows **You've caught up on all notifications!**.

A notification can also appear briefly as a pop-up message in the corner of the screen when it arrives. Every notification is also collected in the Notification Center, so you can review it there later even if you miss the pop-up.



Note: Notifications are personal to your account and reflect the modules and items that you have permission to view. The Notification Center is separate from the **Login Information** overlay that appears at sign-in, which reports your recent account activity.

From a generated report to the report itself

The following path shows how a notification takes you from an event to the item it concerns:

1. User opens a report from the **All Reports** page.
2. The badge on the **bell** icon increments as the notification arrives in real time.
3. Select the **bell** icon to open the Notification Center.
4. On the notification card, select **View Report**. The report opens.

A long-running report notifies you when processing finishes, so you do not need to wait on the page.

Notification severity

Each notification has a severity, shown by a colored status icon on the card, that indicates how much attention it needs. You can filter the list by severity using the chips at the top of the Notification Center.

The severity is not conveyed by color alone. Each status icon has a distinct shape and carries a text label that a screen reader announces as **Critical**, **Warning**, **Success**, or **Info**. The unread dot is announced as **Unread**.

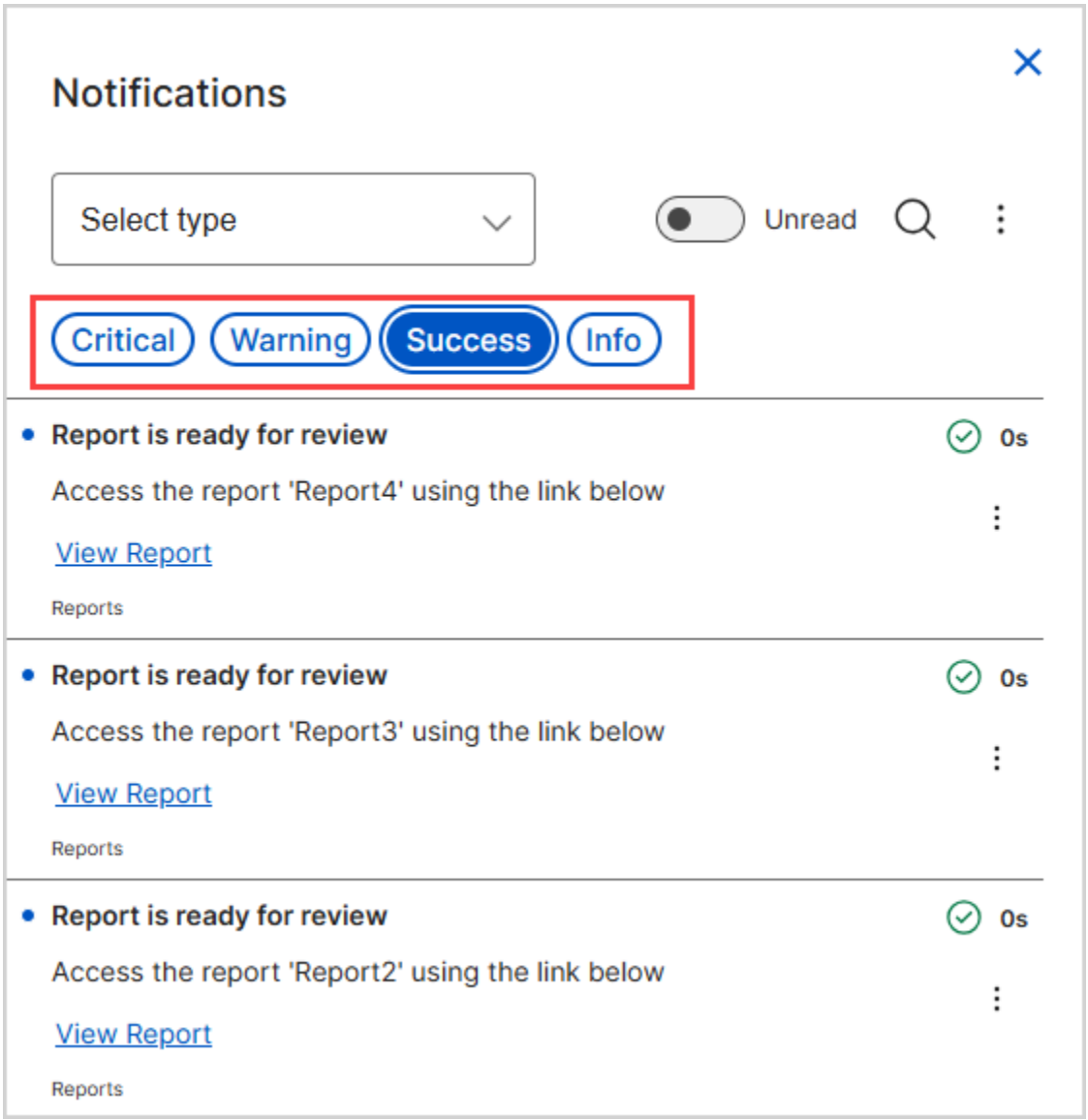


Table 4. Notification severity types

Severity	Description
Critical	Red icon. A problem that needs your immediate attention, such as a report that failed to generate or a deployment that did not complete.
Warning	Amber icon. A condition that might need your attention, such as deployments that are expired and no longer in use.
Success	Green check icon. Confirmation that an operation finished successfully, such as a report that is ready to view or a deployment that completed.
Info	Blue icon. General information, such as a new Protection Level Agreement being created.

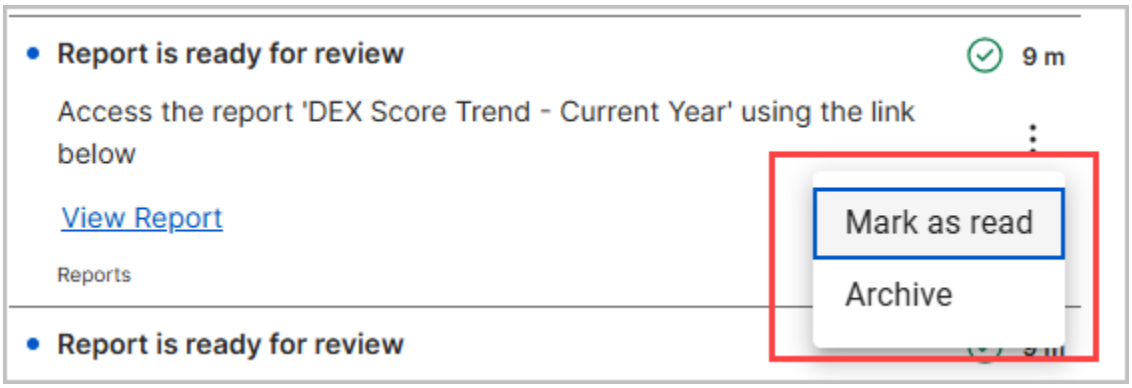
Read and unread notifications

BigFix UI marks a notification that you have not yet read with a blue dot. When you open the Notification Center, the unseen badge on the bell clears, but each notification keeps its dot until you read it. How a notification becomes read depends on its type:

- A notification that contains a link, such as **View Report**, becomes read when you select the link, which also opens the related item.
- A notification that has no link stays unread until you mark it read.

To act on a single notification, select the more-options (three-dot) menu on its card, and then select one of the following:

- **Mark as read** or **Mark as unread** to change whether the notification counts as read.
- **Archive** to move the notification out of the active list without deleting it.



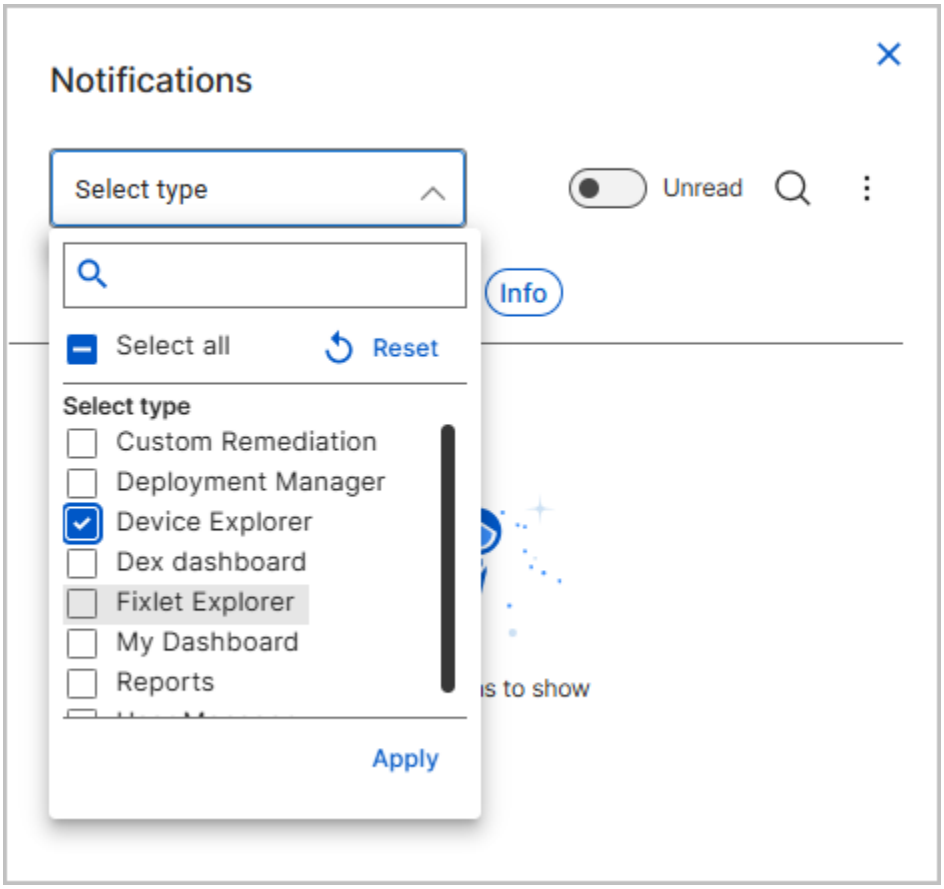
Filter notifications

You can narrow the list by module, by severity, and by keyword, and you can combine these filters.

To filter by the module that raised the notification:

1. Select the **Select type** list.
2. Select the checkbox for each module that you want to include, such as **Analyses**, **CyberFOCUS**, **Deployment Manager**, **Device Explorer**, **Patch**, or **Reports**. The list scrolls, so scroll down to see every module. To find a module quickly, enter its name in the **Search** box. To include every module, select **Select all**; to clear your choices, select **Reset**.
3. Select **Apply**.

The Notification Center shows only notifications from the modules that you selected. Each selected type appears as a chip above the severity chips, for example **Integrated Vulnerability Remediation (IVR)** and **CyberFOCUS**. Select the **X** on a chip to remove that type from the filter. When you select several types, the row ends with a **+N more** indicator.



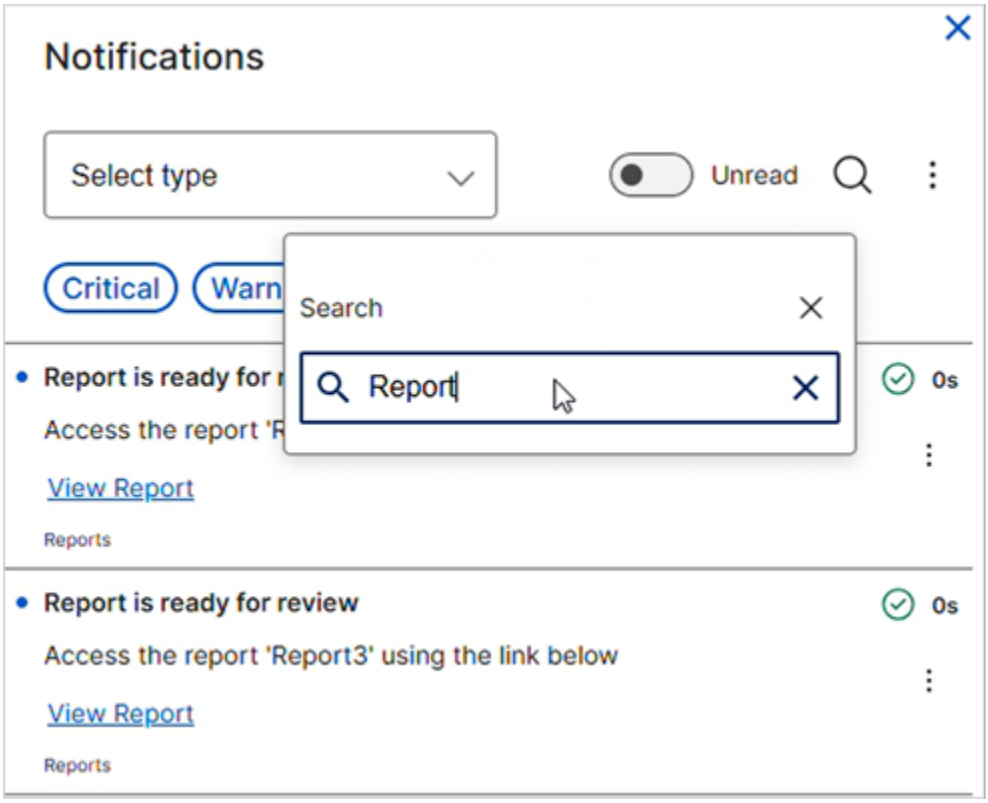
To filter by severity, select one or more of the **Critical**, **Warning**, **Success**, and **Info** chips at the top of the Notification Center. The list shows only notifications of the selected severities. Select a chip again to clear it.

To show only notifications that you have not yet read, turn on the **Unread** toggle.

Search notifications

To find a specific notification by keyword:

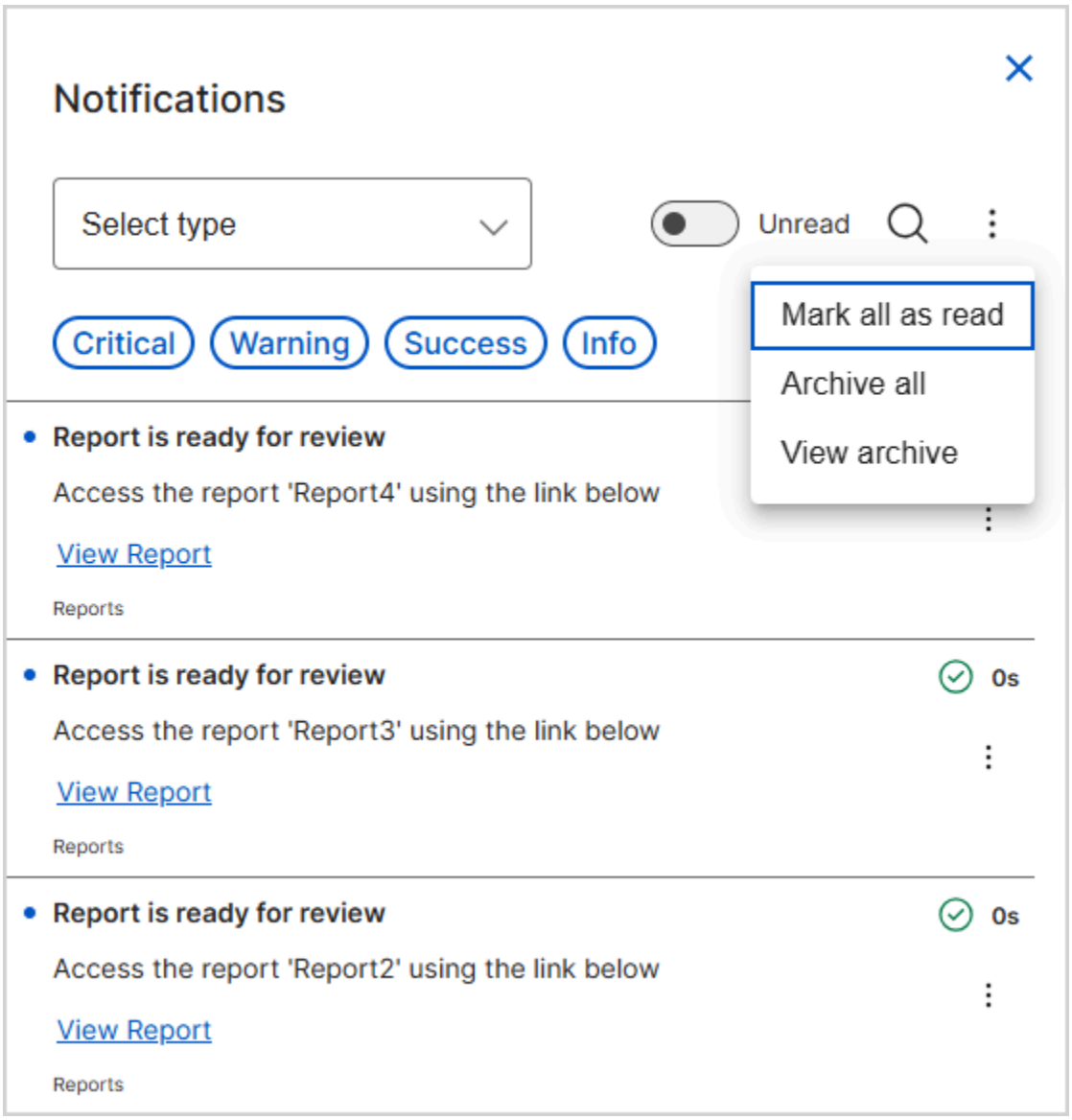
1. Select the **Search** icon.
2. In the **Search** box, enter a word or phrase from the notification title or message. The list updates to show only notifications that match.
3. To close the search box, select the **X**.



Mark and archive all notifications

Use the more-options (three-dot) menu at the top of the Notification Center to act on all notifications at once. The menu provides two actions and a link to the archive:

- **Mark all as read** marks every notification in the list as read.
- **Archive all** moves every notification out of the active list. Archiving removes notifications from the Notification Center without deleting them.



The Notification Center lists 20 notifications at a time. If you have more, select **Load more** at the bottom to load the next 20.

Note: A notification is removed from the Notification Center automatically after a set time. This behavior is managed for you and needs no action.

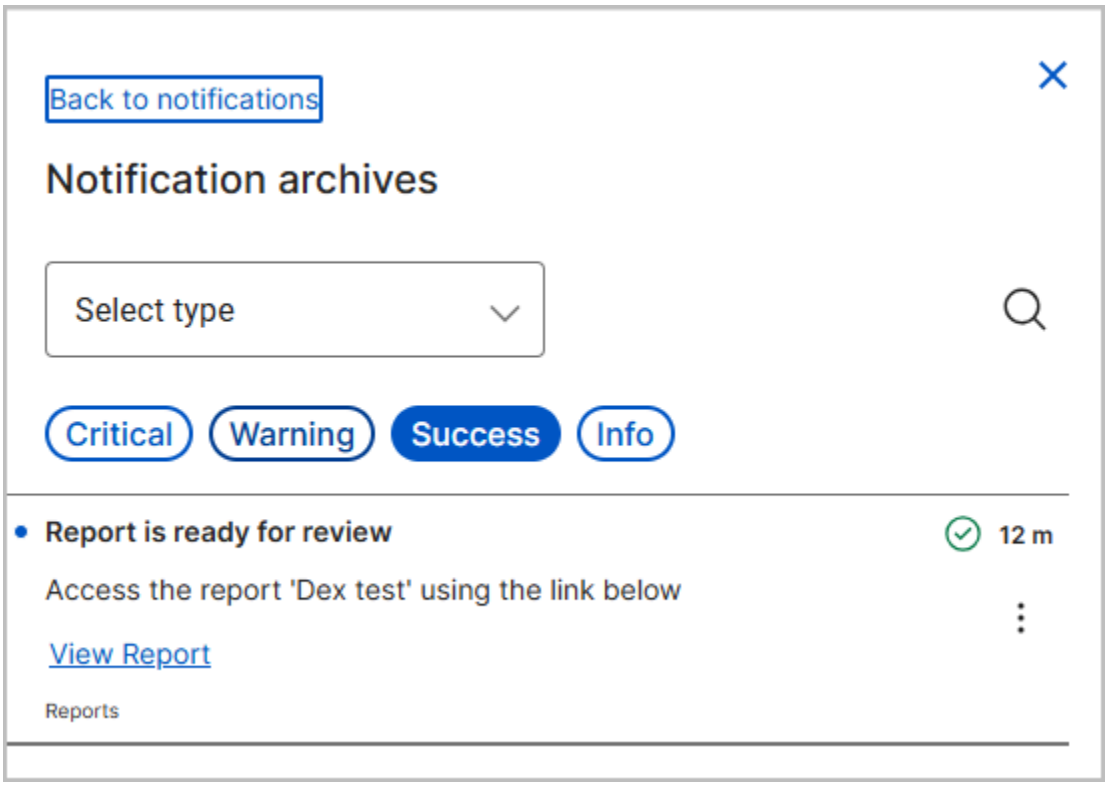
View archived notifications

To review notifications that you archived earlier:

1. Select the more-options (three-dot) menu.
2. Select **View archive**.

BigFix UI opens the **Notification archives** page, which lists the notifications that you archived. You can filter the archive by module and severity and search it by keyword, the same way you work with the Notification Center. To go back, select **Back to notifications**.

The archives page also lists notifications in batches. Select **Load more** at the bottom to load the next batch.



To take a notification back out of the archive:

1. Open the **Notification archives** page.
2. On the notification card, select the more-options (three-dot) menu.
3. Select **Unarchive**. The notification returns to the Notification Center.

The same menu also offers **Mark as unread**.

Notification Center controls

Table 5. Controls in the Notification Center

Control	Description
Select type	Filters the list by the module that raised each notification, and shows every module that can raise one. Includes a search box, **Select all**, **Reset**, and **Apply**.
Type chips	Show the types that you applied in **Select type**. Select the **X** on a chip to remove that type from the filter. A **+N more** indicator appears when you select several types.
Severity chips	Filter the list by **Critical**, **Warning**, **Success**, or **Info**.
Unread	Shows only notifications that you have not yet read.
Search	Finds notifications by a keyword in the title or message.
Panel more-options menu	Provides **Mark all as read**, **Archive all**, and **View archive**.
Notification card more-options menu (Notification Center)	Provides **Mark as read**, **Mark as unread**, and **Archive** for a single notification.
Notification card more-options menu (Notification archives)	Provides **Mark as unread** and **Unarchive** for a single archived notification.
Load more	Loads the next 20 notifications when the list is longer than 20.
Close (**X**)	Closes the Notification Center.

Chapter 3. Using BigFix UI

This guide is for regular users of the BigFix UI.

It provides details of the features that are available when you access the BigFix UI application. For example: navigating through the unified interface, exploring devices, fixlets, and deployments, resolving issues through Custom Remediation, and using tools like DEX.

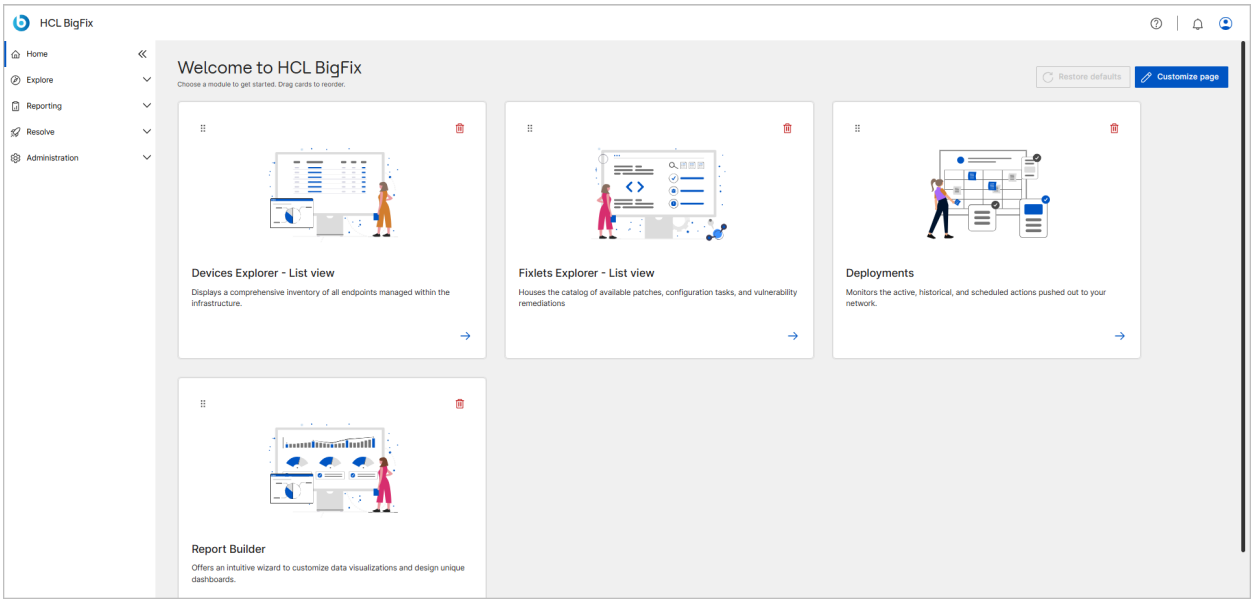
The guide also explains how to access reporting features such as All Reports and Reports Builder, as well as perform administrative tasks such as managing users.

Home

The customizable dashboard is the home page of the BigFix UI. It shows the applications and reports that you use most as a grid of widgets that you can add, remove, and reorder to match your workflow.

After you sign in to the BigFix UI, the customizable dashboard opens as the home page. From the dashboard, you open the application or report that you want, either by selecting its widget or by using the side navigation. To return to the dashboard at any time, select **Home** in the side navigation.

The page opens with the title **Welcome to HCL BigFix** and the prompt **Choose a module to get started. Drag cards to reorder.** Use the **Customise page** button to choose which widgets appear, and the **Restore defaults** button to return to the default layout.



The first time you open the dashboard, the BigFix UI shows a default set of cards. You can then tailor the layout: add or remove cards, and drag them into the order that you want. The BigFix UI saves your layout to your profile, so it persists across sessions.

Note: A card can reference either an application or a report that you have permission to view. If your access to an application or report changes, the BigFix UI updates the dashboard so that you see only the items that you can open.

Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to this application. My Dashboard is a default application, so every role has at least view access to it. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete. For a description of each permission, see Permissions reference *(on page 482)*.

Widget cards

Each application or report on the dashboard appears as a card. A card shows an illustration, the application or report name, and a short description. Each card also provides the following controls. Pause over a control to display its tooltip, which names the card that the control acts on, such as **Drag Devices Explorer - List view**.

Table 6. Card controls

Control	Description
Drag (grid icon, upper-left corner)	Moves the card to a different position in the grid. Select and hold the icon, and then drag the card where you want it.
Delete (trash icon, upper-right corner)	Removes the card from the dashboard. The application or report itself isn't deleted, and you can add the card again from the **Customize page** panel.
Open (arrow icon, lower-right corner)	Opens the application or report that the card represents.

To rearrange the cards on your dashboard by using drag-and-drop:

1. Pause over the **Drag** icon in the upper-left corner of the card that you want to move. A tooltip confirms which card you are about to move, such as **Drag Devices Explorer - List view**.
2. Select and hold the **Drag** icon.
3. Drag the card to the position that you want in the grid. The surrounding cards shift to show where the card will land.
4. Release the card to drop it in the new position.

The BigFix UI saves the new arrangement to your profile automatically, so the layout is the same the next time you open the dashboard.

Note: You can move a card only by its **Drag** icon. Dragging any other part of the card has no effect.

To remove a card from your dashboard:

1. On the card that you want to remove, select the **Delete** icon.

To open an application or report from your dashboard:

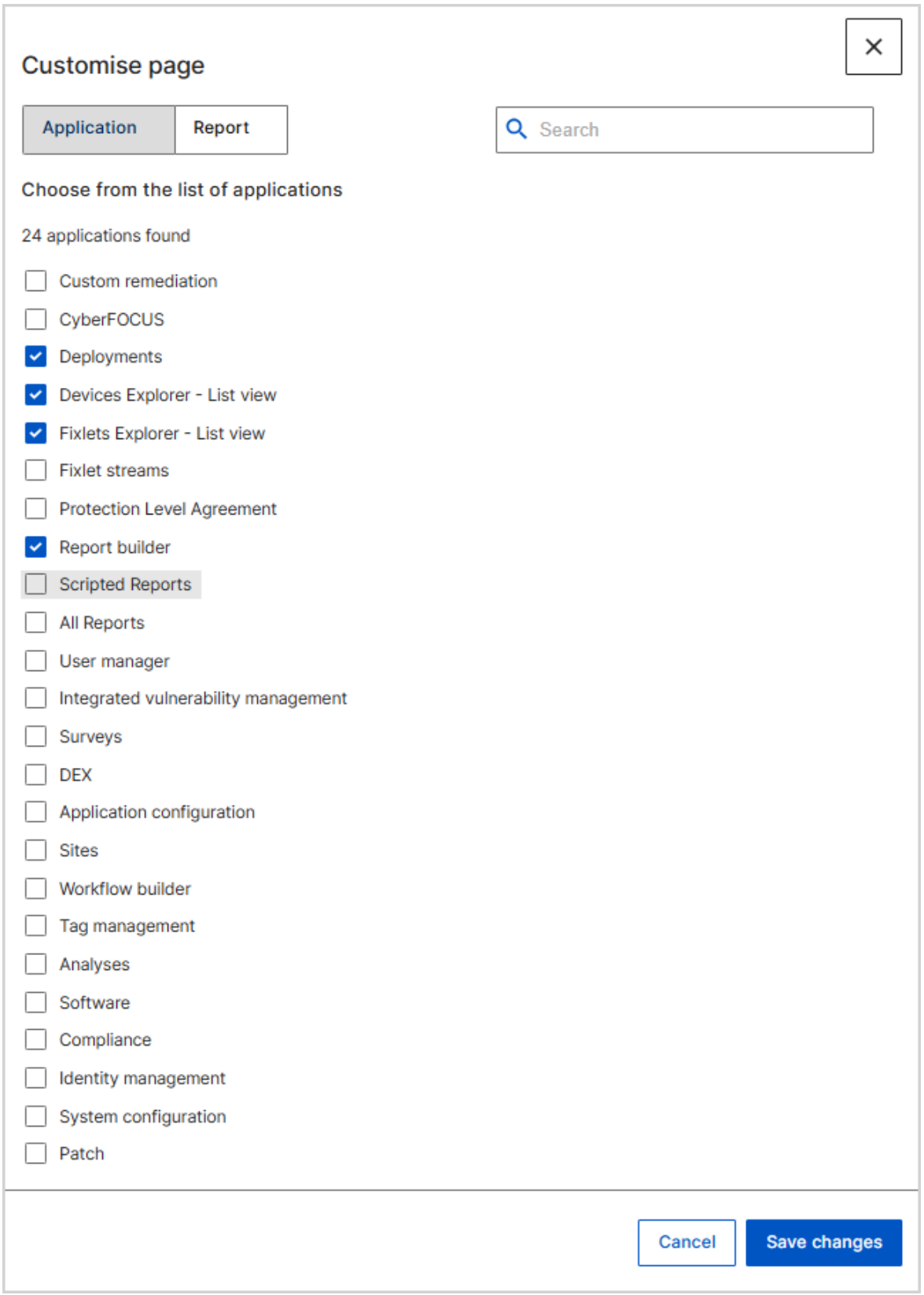
1. On the card that you want to open, select the **Open** icon. The application or report opens.

Customise page

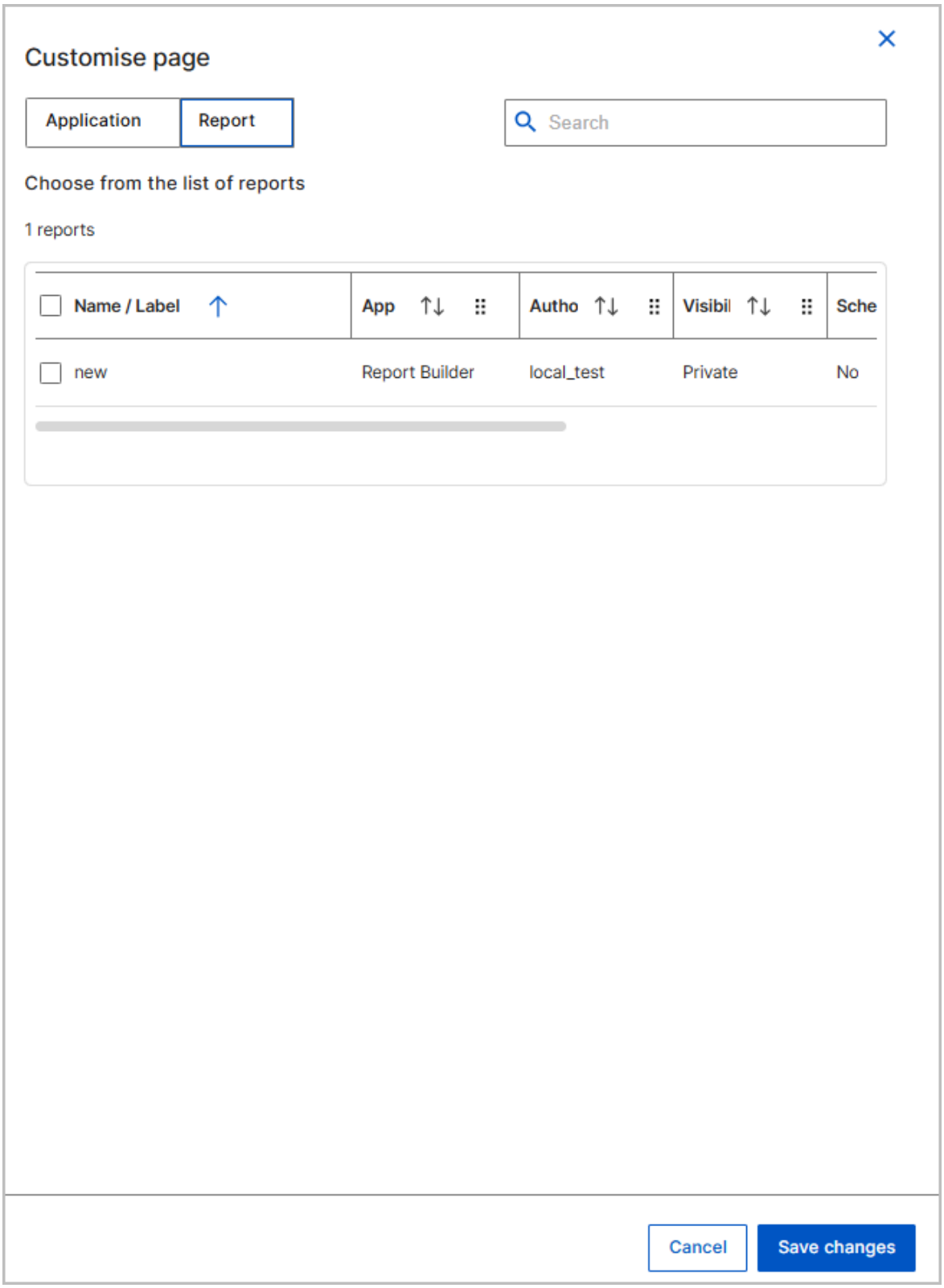
Use the **Customize page** panel to choose which application and report cards appear on your dashboard. The panel lists only the applications and reports that you have permission to view, and it provides an **Application** tab, a **Report** tab, and a **Search** box.

To personalize your dashboard:

1. Select **Customise page** to open the **Customise page** panel.


Customise page
Application
Report
Search
Choose from the list of applications
24 applications found
Custom remediation
CyberFOCUS
Deployments
Devices Explorer - List view
Fixlets Explorer - List view
Fixlet streams
Protection Level Agreement
Report builder
Scripted Reports
All Reports
User manager
Integrated vulnerability management
Surveys
DEX
Application configuration
Sites
Workflow builder
Tag management
Analyses
Software
Compliance
Identity management
System configuration
Patch
Cancel
Save changes

2. On the **Application** tab, select or clear the checkbox next to each application. A selected application appears as a widget; a cleared application is removed. To filter the list, enter a name in the **Search** box.
3. On the **Report** tab, select the checkbox next to each report that you want to add as a widget. Use the columns described in Table 7: Report tab columns *(on page 76)* to identify the correct report.


Customise page
Application
Report
Search
Choose from the list of reports
1 reports
Name / Label
App
Autho
Visibil
Sche
new
Report Builder
local_test
Private
No
Cancel
Save changes

4. Select **Save changes** to apply your selections, or select **Cancel** to close the panel without changing your dashboard.

The dashboard then shows the cards that you selected.

Table 7. Report tab columns

Column	Description
Name / Label	The name of the report.
App	The application that the report belongs to, such as Report Builder or Device Explorer.
Author	The user who created the report.
Visibility	Whether the report is private or shared.
Schedule	Whether the report runs on a schedule.
Last modified	The date and time when the report was last changed.

Restore defaults

The **Restore defaults** button, next to **Customize page** in the top-right corner of the dashboard, discards your personalization and returns the dashboard to the factory default layout. Restoring the defaults removes any cards that you added, brings back any default cards that you removed, and resets the card positions.

To return the dashboard to its default set and arrangement of cards:

1. Select **Restore defaults**.

The dashboard immediately shows the default cards in their default positions, and the BigFix UI saves this layout to your profile. You can personalize the dashboard again at any time.

Note: The **Restore defaults** button is available only when your current layout differs from the default. If you have not changed the dashboard, the button is dimmed.

Note: Restoring the defaults cannot be undone. To rebuild a personalized layout, add and arrange the cards again.

Explore

The Explore section provides a centralized view of core BigFix resources. It helps administrators and operators quickly access devices, fixlets, deployments, sites, and analyses for monitoring and action.

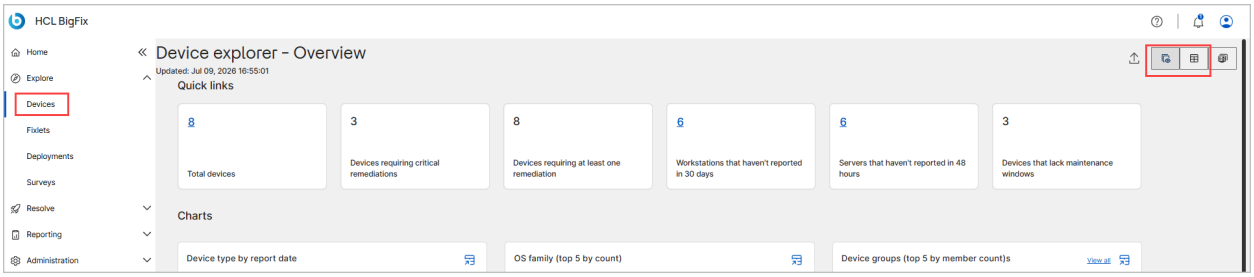
- **Devices** *(on page 77)* – View, monitor, and act on every device connected to your BigFix environment. Use the **Overview** page for a chart-based summary and the **List view** page to work with device inventory in a customizable table. You can also set maintenance windows, update client settings, and group devices.
- **Fixlets** *(on page 145)* – View and manage Fixlets, which are sets of instructions that the BigFix agent runs on devices. Filter and deploy Fixlets, review CVE details, and create your own custom Fixlets.
- **Deployments** *(on page 181)* – Monitor and manage deployments across your environment. View deployment status, filter and search the list, and stop or delete existing deployments.
- **Software** *(on page 193)* – Deploy and manage software across all endpoints in your network. BigFix Software Distribution gives you full control, audit visibility, and end-user self-service from one interface.
- **Sites** *(on page 194)* – Review the public and custom sites in your deployment, check how many devices subscribe to each site, and create custom sites to host your own content.
- **Surveys** *(on page 213)* – Create and track surveys that collect feedback from endpoint users about their digital experience. Review the status and score of each survey, and deploy a survey to devices.
- **Analyses** *(on page 214)* – Collect and review device data. Create analyses, set the devices they apply to, and manage the properties that each analysis reports.

The **Explore** section consolidates these key areas into one streamlined workspace, enabling faster navigation and simplified management.

Devices

The Device Explorer lets you view, monitor, and act on all the devices connected to your BigFix environment. Use the **Overview** page for a high-level, chart-based summary, and the **List view** page to work with device inventory in a customizable table.

To open the Device Explorer, expand **Explore** in the side navigation and select **Devices**. Use the view icons in the top-right corner to switch between the **Overview** (charts) page and the **List view** page. Both pages show an **Updated** timestamp that indicates when the data was last refreshed.



Note: Devices appear in the Device Explorer only if BigFix manages them. A device is managed when the BigFix Agent is installed and reporting. The BigFix UI doesn't support correlation. If your environment has correlated devices, you can't install the BigFix UI. For more information, see Correlation is not supported *(on page 7)* and Correlated devices.

Before you begin

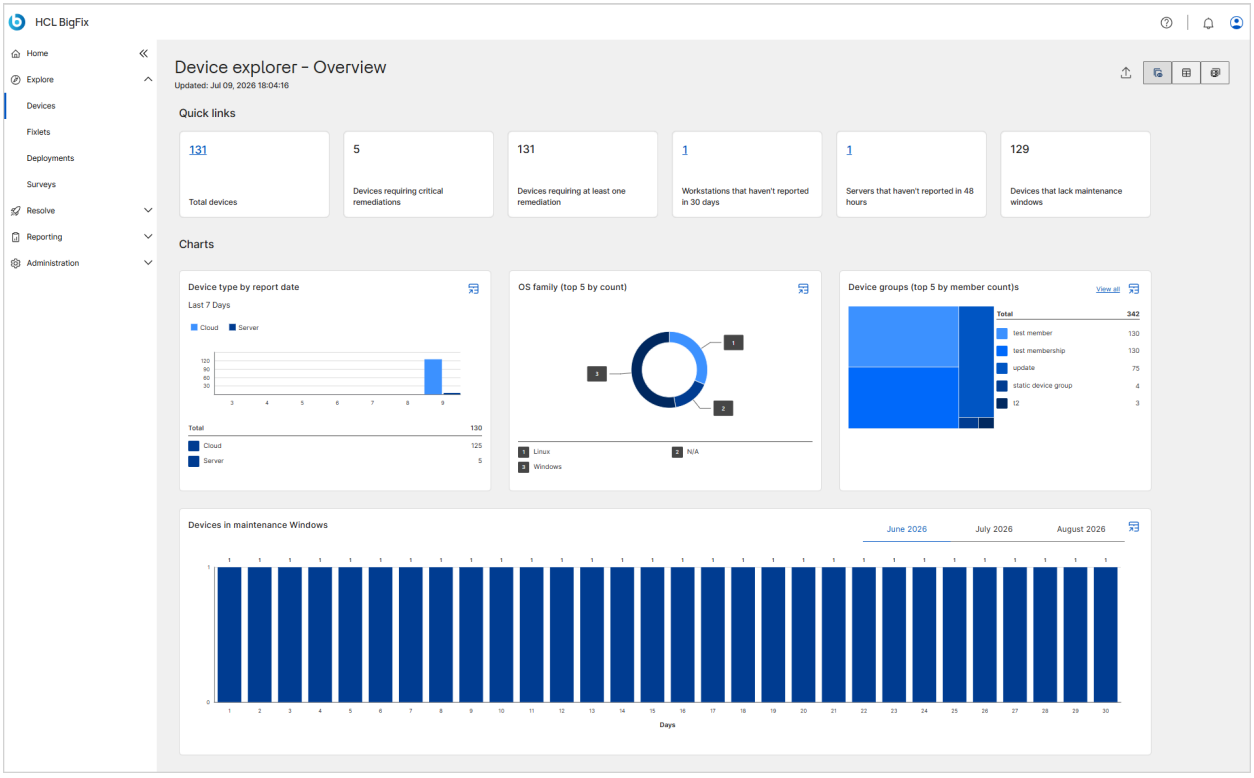
Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to this application. Device Explorer is a default application, so every role has at least view access to it. See Managing Roles *(on page 467)*.
- Your role also defines the device scope, so you see only the devices that your role can manage. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete. For a description of each permission, see Permissions reference *(on page 482)*.

Device Explorer – Overview page

The **Overview** page provides a high-level summary of your device environment through quick links and interactive charts. Use it to monitor device health, reporting status, remediation needs, and group distribution before you drill down into individual device data.

The top-right corner includes an **Export** (share) icon that exports the current page data and a **Device groups** icon that opens the Device Groups page. For more information, see Device Groups *(on page 94)*.



Quick links

The **Quick links** section at the top of the page provides fast access to commonly monitored device conditions. Each tile shows a count.

Table 8. Quick links

Quick link	Description
Total devices	The total number of devices that BigFix currently manages.
Devices requiring critical remediations	The number of devices that are missing security-critical patches or updates and require immediate attention.
Devices requiring at least one remediation	The number of devices that require any remediation, both critical and non-critical.
Workstations that haven't reported in 30 days	Workstation devices that haven't reported to BigFix in the last 30 days.
Servers that haven't reported in 48 hours	Server devices that haven't reported to BigFix in the last 48 hours.
Devices that lack maintenance windows	Devices that don't have an associated maintenance window.

Note: When a tile's count appears as a link, select it to open the Devices table filtered to the matching devices. Counts that aren't links are for reference only. Chart elements, such as segments of a donut or bar chart, are for visualization only and don't filter the table.

Charts

The **Charts** section presents high-level metrics as interactive chart widgets.

Table 9. Overview charts

Chart	Description
Device type by report date	Shows device counts grouped by device type based on their most recent report date, over a selected period such as the last 7 days.
OS family (top 5 by count)	Displays the top five operating system families in your environment, ranked by the number of devices.
Device groups (top 5 by member count)	Shows the five device groups with the most member devices, with the group name and member count. Select **View all** to open the Device Groups page.
Devices in maintenance Windows	Shows the number of devices in active maintenance windows. Select a month tab to view the distribution across the days of that month.

Each chart has a **See data in data table format with download options** icon in its top-right corner. Select it to view the chart's data as a table that you can copy or export. for more information, see Viewing chart data in a table *(on page 33)*.

Device Explorer – List view page

The **List view** page is the central workspace for managing and monitoring the endpoints in your environment. Use it to view inventory data in a customizable table, build charts from device properties, and run administrative actions on one or more devices. The page is organized into a view and utility bar, a collapsible Charts section, a command bar, and the device list table.

View and utility bar

The view and utility bar in the top-right corner manages the overall display and reporting features.

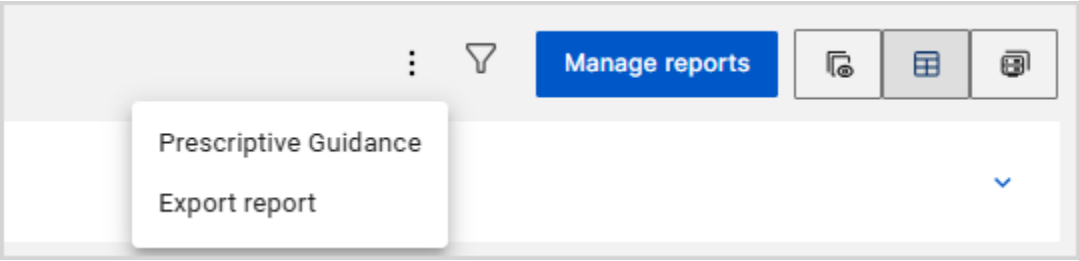


Table 10. View and utility bar controls

Control	Description
More options (three vertical dots)	Opens a menu with **Prescriptive Guidance**, which provides actionable recommendations based on best practices, and **Export report**, which downloads the tabular report for offline analysis. For more information, see Prescriptive Guidance *(on page 55)* and Exporting Data *(on page 30)*.
Filter (funnel icon)	Displays a subset of devices based on criteria that you define. You can also save a filter, mark it as a favourite, and apply it again later. For more information, see Global filter *(on page 36)*.
Manage reports	Saves, loads, and organizes custom reports that you generate in the BigFix UI. For more information, see Manage Reports *(on page 42)*.
Device groups (icon)	Opens the Device Groups page, where you view and manage static and dynamic device groups. For more information, see Device Groups *(on page 94)*.
View icons	Switch between the **Overview** (charts) page and the **List view** page.

Filter

The **Filter** icon (funnel) in the view and utility bar opens the global filter for the page. The global filter narrows the device list table to the devices that match the conditions you define, and it also drives the chart interactions described in Filtering devices from a chart *(on page 87)*.

You can save the filters that you build, so that you can reuse them without defining the same conditions again. From the **Filter** panel, you can save a filter under a name of your choice, list your saved filters, mark the ones you use most as favourites, apply a saved filter to the current view, and delete the filters that you no longer need. Saved filters are private to your account, and the filters that you save here apply to devices only.

For the steps to build, save, apply, and manage your filters, see Global filter *(on page 36)*.

Note: Filtering on computer properties that are assigned to a category is not supported. For more information, see Filtering on computer properties that belong to a category is not supported *(on page 8)*.

Charts

The collapsible **Charts** section creates and displays custom visualizations from device inventory data. A badge next to the title, such as **0 charts set** or **1 chart set**, shows how many charts are defined. For the steps to create a chart and to edit, delete, or export the charts you build, see Configuring and managing device charts *(on page 86)*.

Charts are interactive and work together with the **Global Filter** and the device list table. For the steps to filter the device list table from a chart, see Filtering devices from a chart *(on page 87)*.

Command bar

The command bar, directly above the table, is the primary area for adjusting the table and acting on devices.

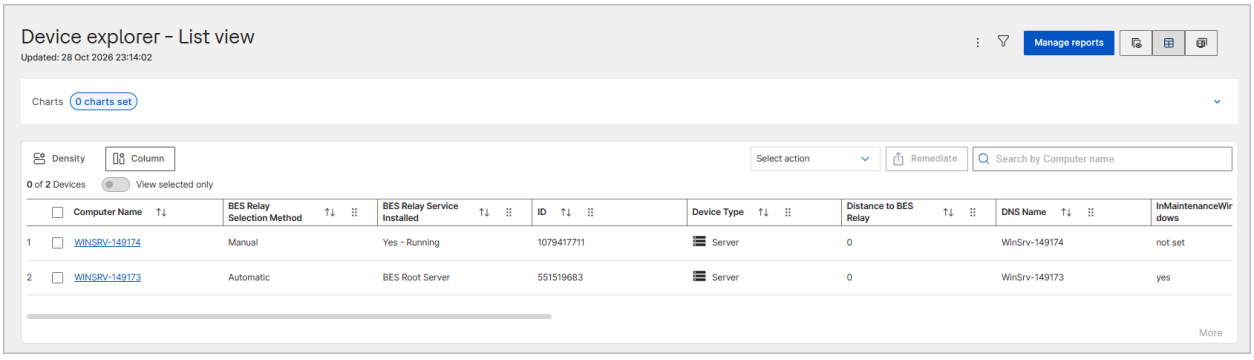


Table 11. Command bar controls

Control	Description
Column	Opens the **Manage columns** drawer, where you choose which device properties appear as columns in the table. For the steps, see Manage columns *(on page 85)*.
Density	Adjusts the row spacing of the table.

Table 11. Command bar controls (continued)

Control	Description
View selected only	When turned on, limits the table to the devices that you selected. A counter, such as **1 of 8 Devices**, shows how many devices are selected.
Select action	Runs a command on the selected devices. Select at least one device checkbox to enable the commands. See Table 12: Select action commands *(on page 82)*.
Remediate	Deploys a fix or configuration task to the selected devices. This button stays dimmed until you select at least one device that requires remediation.
Search	Filters the list as you type a keyword, such as a computer name or ID.

Select action

The **Select action** dropdown provides the following commands for the selected devices.

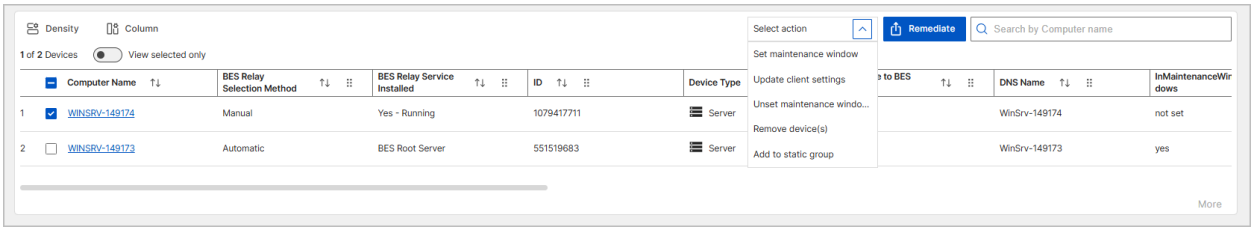


Table 12. Select action commands

Command	Description
Set maintenance window	Defines a period for updates or maintenance on the selected devices. For more information, see Managing Device Maintenance Windows *(on page 126)*.
Update client settings	Modifies configuration settings for the BigFix client on the selected devices. For more information, see Update Client Settings *(on page 135)*.
Unset maintenance window	Removes an existing maintenance schedule from the selected devices. For more information, see Managing Device Maintenance Windows *(on page 126)*.
Remove device(s)	Removes the selected devices from the inventory. Delete devices *(on page 144)*.
Add to static group	Adds the selected devices to an existing static device group, or to a new static group that you name. For more information, see Managing Static Group Membership *(on page 105)*.

Device list table

The device list table displays details about the discovered devices in your environment. Select a device's **Computer Name** to open its Device Details page *(on page 89)*.

Each column header includes a sort icon: select it once to sort ascending, again to sort descending, and again to clear the sort. The table can include the following columns.

Table 13. Device list table columns

Column	Description
Number	The order in which BigFix added the device.
Computer Name	The BigFix computer name assigned to the device. Select it to open the Device Details page.
Active Directory Path	The Active Directory path of the device.
Agent Type	The type of BigFix agent installed on the device.
Agent Version	The version of the BigFix agent installed on the device.
BES Relay Selection Method	How the device selected its relay: **Automatic** (selected by BigFix) or **Manual** (manually configured).
BES Relay Service Installed	Whether a BES Relay service is installed on the device, such as **BES Root Server** or **Not Installed**.
BES Root Server	The BigFix root server that the device reports to.
BIOS	The BIOS version or date reported by the device.
Client Administrators	The administrators defined for the BigFix client on the device.
Client Settings	The client settings applied to the device.
Computer Group	The device groups that the device belongs to.
Computer Type	The hardware type of the device, such as physical or virtual.
CPU	The processor type and speed reported by the device.
Device Type	The type of device, such as Server or Workstation.
Distance to BES Relay	The distance between the device and its assigned relay.
DNS Name	The fully qualified DNS name of the device.
Free Space on System Drive	The available disk space on the system drive of the device.
IDP Computer Groups	The computer groups reported by the identity provider.
IDP User Department	The department of the device user, as reported by the identity provider.
IDP User Display Name	The display name of the device user, as reported by the identity provider.
IDP User Groups	The groups that the device user belongs to, as reported by the identity provider.
IDP User Location	The location of the device user, as reported by the identity provider.
IDP User Principal Name	The principal name of the device user, as reported by the identity provider.

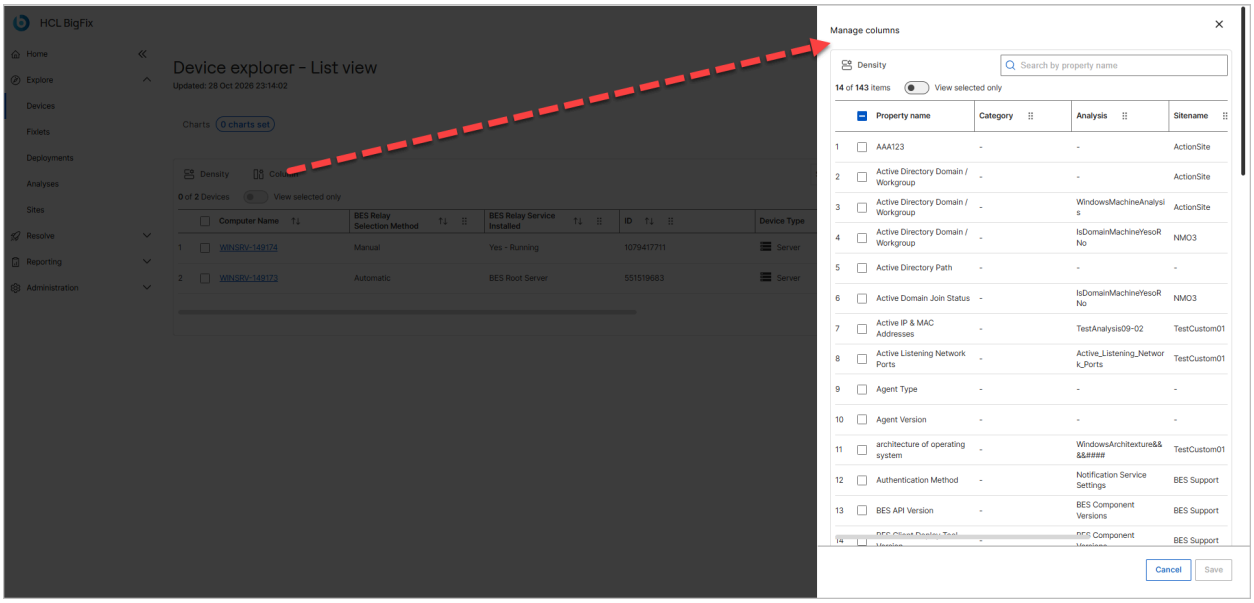
Table 13. Device list table columns (continued)

Column	Description
IDP User Site	The site of the device user, as reported by the identity provider.
InMaintenanceWindows	Whether the device is currently associated with a maintenance window, such as **yes**, **no**, or **not set**.
IP Address	The IP address reported by the device at its last check-in.
IPv6 Address	The IPv6 address reported by the device at its last check-in.
Last Report Time	When the device last reported to BigFix.
LastMaintenanceWindow	The most recent maintenance window that applied to the device.
License Type	The license type that covers the device.
Lock Expiration	When the lock on the device expires.
Locked	Whether the device is locked and excluded from deployments.
MAC Address	The MAC address of the device network interface.
MaintenanceWindowException	Any exception defined for the maintenance window of the device.
MaintenanceWindowProjections	The projected maintenance windows for the device.
NextMaintenanceWindow	The next maintenance window scheduled for the device.
OS	The operating system reported by the device.
OS Family	The operating system family, such as Windows or Linux.
OS Name	The specific operating system installed on the device.
OS Version	The operating system version number.
RAM	The amount of memory installed on the device.
Relay	The relay server currently assigned to the device.
Relay Name of Client	The relay name as reported by the client.
Relevant Fixlet Count	The number of Fixlets that are currently relevant to the device.
Remediated Fixlet Count	The number of Fixlets that have been successfully applied to the device.
Subnet Address	The subnet address of the device.
Subscribed Sites	The sites that the device subscribes to.
Total Size of System Drive	The total capacity of the system drive of the device.
User Name	The user that is logged in to the device.

Note: The columns that appear depend on your **Column** selection. When a value isn't available, the cell shows **No data**.

Manage columns

Select **Column** in the command bar of the **List view** page to open the **Manage columns** drawer. The drawer lists only Reserved, Derived, Custom, Active Analysis, and External properties. For each property, it shows the **Category**, the **Analysis** it comes from, and the **Sitename**.



1. Above the table, select **Column**. The **Manage columns** drawer opens.
2. Optional: In **Search by property name**, enter a property name to narrow the list.
3. Optional: Turn on **View selected only** to list just the properties that you already selected.
4. Select the checkbox next to each property that you want to display as a column, and clear the checkbox for each property that you want to hide. The counter above the list, such as **14 of 143 items**, shows how many properties are selected.

   Note: You can display a maximum of 63 columns.

5. Select **Save**. The table updates to show the columns that you selected.

   To close the drawer without applying your changes, select **Cancel** or the **Close** (X) icon.

Related information

Managing Filters *(on page 35)*

Manage Reports *(on page 42)*

Prescriptive Guidance *(on page 55)*

Device Groups *(on page 94)*

Device Details Page *(on page 89)*

Update Client Settings *(on page 135)*

Managing Device Maintenance Windows *(on page 126)*

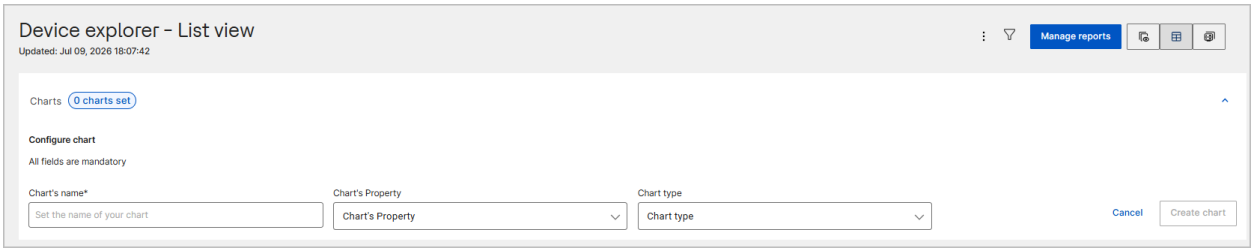
Setting-up Remediation Flow *(on page 111)*

Other Device Actions *(on page 139)*

Configuring and managing device charts

Use the **Configure chart** pane on the Device Explorer – List view page to build custom visualizations from device inventory data. After you create a chart, you can edit it, delete it, view its data as a table, or hide the whole **Charts** section.

The collapsible **Charts** section on the Device Explorer – List view page creates and displays custom visualizations from device inventory data. A badge next to the title, such as **0 charts set** or **1 chart set**, shows how many charts are defined.



1. In the **Charts** section, select **Add chart**.

   The **Configure chart** pane opens. All fields are mandatory.

2. In **Chart's name**, enter a descriptive name that identifies the chart.

3. From the **Chart's Property** dropdown, select the device property to visualize, such as OS, CPU, or device type.

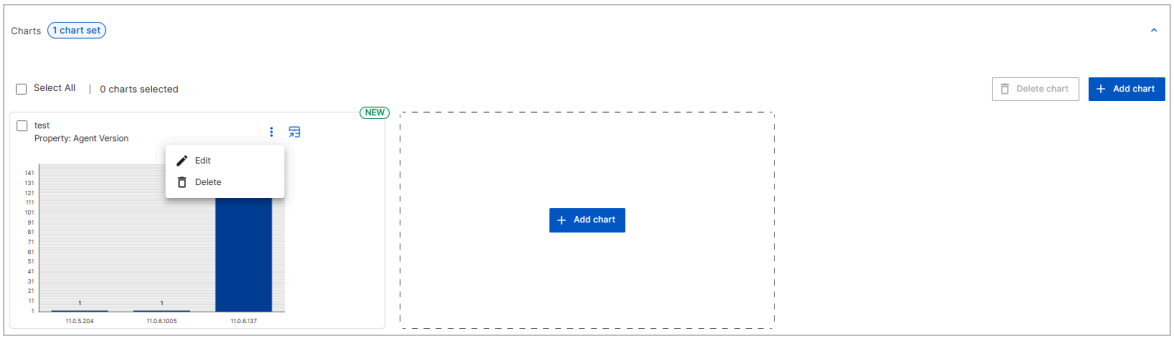
   The dropdown lists all available properties.

4. From the **Chart type** dropdown, select the visual format: **Horizontal chart**, **Vertical chart**, or **Pie chart**.

5. Select **Create chart**.

   This button stays dimmed until you complete all required fields. To close the pane without saving, select **Cancel**.

The chart appears as a tile in the **Charts** section, showing the chart name and the property it visualizes, such as **Property: OS Family**. A **NEW** badge marks a recently added chart. If the selected property has no data, the tile shows **No Data Available**.



The chart is available in the **Charts** section. Charts are interactive and work with the device list table. For the steps to filter the device list table from a chart, see Filtering devices from a chart *(on page 87)*.

After you create a chart, you can manage it in the following ways.

- To add another chart, select **Add chart** or the empty **Add chart** placeholder tile.
- To edit or delete a chart, select the **More options** icon on the chart tile and then select **Edit** or **Delete**.
- To delete several charts, select the checkbox on each tile, or select **Select All**, and then select **Delete chart**.
- To view a chart's data as a table that you can copy or export, select the **See data in data table format with download options** icon in the tile's top-right corner. For more information, see Viewing chart data in a table *(on page 33)*.
- To hide the **Charts** section, select the collapse icon (upward arrow).

Related information

Devices *(on page 77)*

Filtering devices from a chart *(on page 87)*

Common Functionalities *(on page 28)*

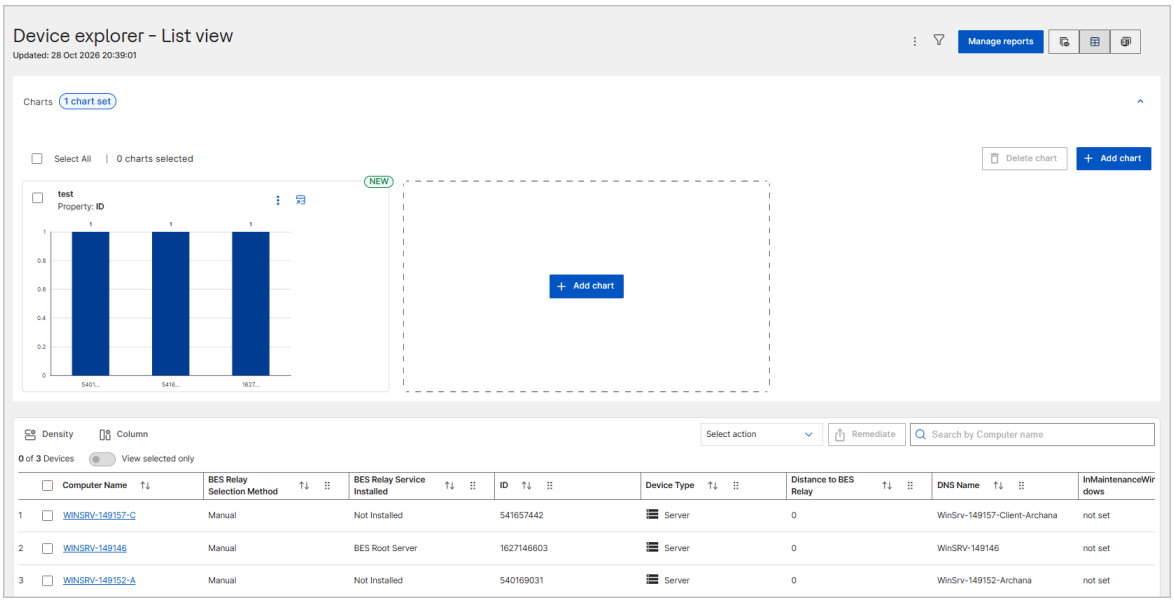
Filtering devices from a chart

Charts on the Device Explorer – List view page are interactive. Select a chart segment to filter the device list table to the matching devices, and clear the filter to return to the default view.

Charts on the Device Explorer – List view page work together with the device list table. When you select a chart segment, BigFix filters the device list table to the matching devices. When you clear the filter, the chart and the table return to their default views.

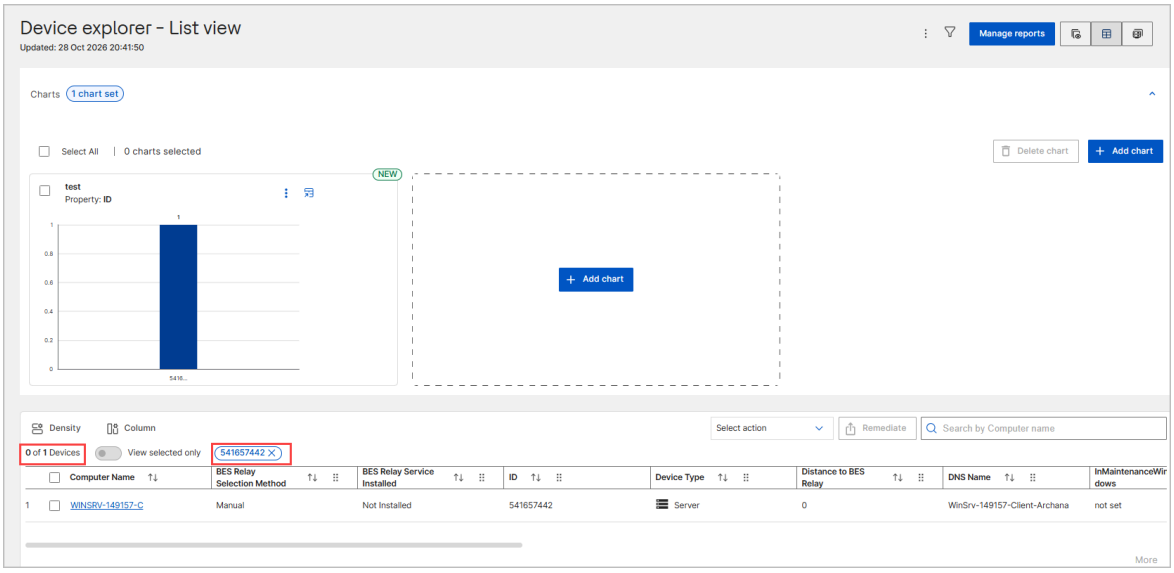
1. Create a chart from a device property, such as **OS Family**.

   The chart appears as a tile that shows each value as a segment, for example Windows, Linux, and N/A, with its device count.



2. Select a segment, such as the **Windows** bar.

   The chart updates to show only the selected segment and hides the rest. For example, the count changes from **0 of 3 Devices** to **0 of 1 Devices**.



3. To clear the selected segment, select the **x** in the chip above the device list table.

The chart returns to its default view and shows all segments, and the device list table shows the complete, unfiltered list. For example, the count returns to **0 of 3 Devices**.

4. **Optional:** Manage the chart: edit it, delete it, add more charts, or hide the **Charts** section.

   For the steps, see Configuring and managing device charts *(on page 86)*.

Note: Use the zoom controls on a chart tile, **Reset Zoom**, zoom in, and zoom out, to adjust how much of the chart is visible. Zooming doesn't filter the table.

Note: To view the chart's values as a table that you can copy or export, select the **See data in data table format with download options** icon in the chart's top-right corner. For the steps, see Viewing chart data in a table *(on page 33)*.

Related information

Devices *(on page 77)*

Configuring and managing device charts *(on page 86)*

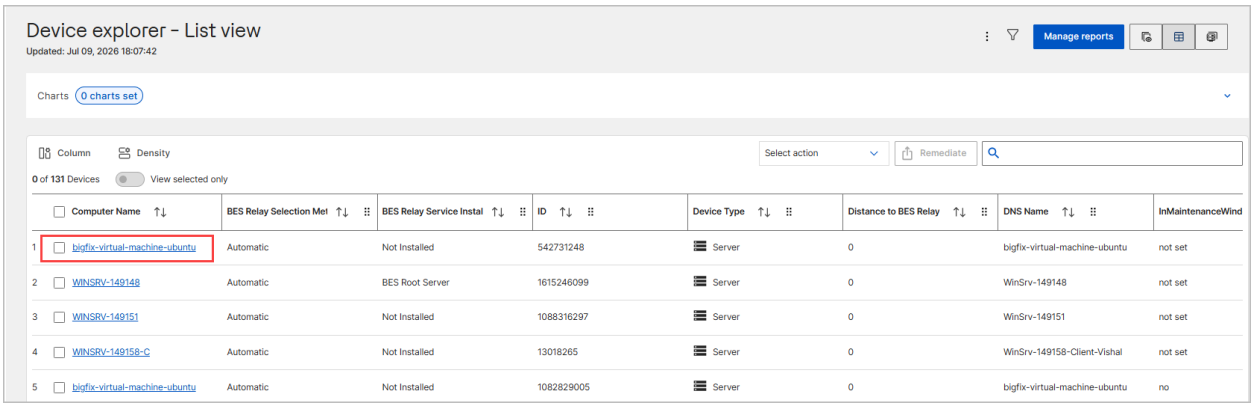
Managing Filters *(on page 35)*

Common Functionalities *(on page 28)*

Device Details Page

The Device Details page provides in-depth information about an enrolled device and lets you act on that device. Use it to review the device's configuration, maintenance settings, group memberships, relevant Fixlets, and deployments, and to run remediation and other device actions.

To open the Device Details page, select a device name in the Device Explorer – List View. The page is divided into three tabs: **Overview**, **Relevant Fixlets**, and **Deployments**. Each tab presents a different aspect of the selected device's status and activity.



Page actions

The device name appears at the top of the page. The following actions are available in the top-right corner of the page on every tab.

Table 14. Device Details page actions

Action	Description
Delete (trash icon)	Removes the device from management. After you delete the device, you can no longer manage or remediate it, and its associated data is removed.
Settings (gear icon)	Opens the device settings, where you configure computer settings for the device.
Other Device Actions	Opens a dropdown of additional actions that you can run on the device, such as **Open Remote Control** and **Send Message**. For more information, see Other Device Actions *(on page 139)*.
Remediate	Opens the Remediate widget so that you can deploy a fix or configuration task to the device. This button appears when relevant content is available for the device.

Note: The actions in the **Other Device Actions** dropdown appear only when the device is eligible for them and you have the required permissions. If an action isn't available for a device, it doesn't appear in the dropdown.

Overview tab

The **Overview** tab summarizes key information about the selected device in the following panels.

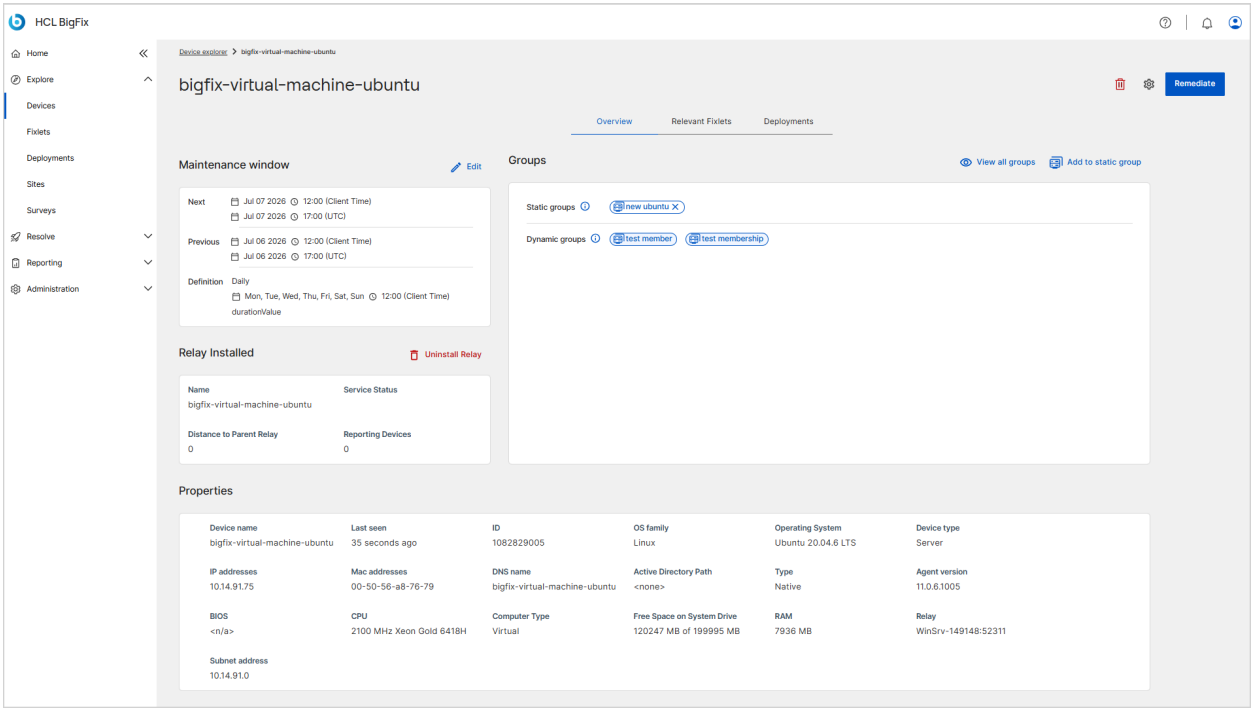


Table 15. Overview tab panels

Panel	Description
Maintenance window	Displays the configured maintenance schedule for the device, including the next and previous windows and the schedule definition. Select **Edit** to change the maintenance window parameters.
Groups	Lists the static and dynamic groups that the device belongs to. Select **View all groups** to see every group, or **Add to static group** to add the device to a static group.
Relay Installed	Indicates whether a BigFix relay is installed on the device and shows the relay name, service status, distance to the parent relay, and number of reporting devices. When a relay is installed, **Uninstall Relay** is available.
Properties	Displays key system information collected from the device to help you identify and assess device health.

The **Properties** panel provides a quick overview of the device's configuration, performance, and connectivity in the BigFix environment. The following fields are available.

Table 16. Device properties

Field	Description
Device name	The name of the device.
Last seen	The time when the device last reported to BigFix.

Table 16. Device properties (continued)

Field	Description
ID	The unique BigFix computer identifier for the device.
OS family	The operating system family, such as Windows, Linux, or Mac.
Operating System	The specific operating system and version, such as Ubuntu 20.04.6 LTS.
Device type	The device role, such as Server or Workstation.
IP addresses	The IP addresses assigned to the device.
Mac addresses	The hardware (MAC) addresses of the device's network interfaces.
DNS name	The fully qualified domain name of the device.
Active Directory Path	The Active Directory path for the device, or **<none>** if the device isn't joined to a domain.
Type	The agent type, such as Native.
Agent version	The version of the BigFix agent installed on the device.
BIOS	The BIOS version or date reported by the device.
CPU	The processor type and speed.
Computer Type	The hardware type, such as Physical or Virtual.
Free Space on System Drive	The available and total space on the system drive.
RAM	The amount of installed memory.
Relay	The relay that the device reports through.
Subnet address	The subnet that the device belongs to.

Note: The fields that appear depend on the device and the information that BigFix collects from it. If a value isn't available, the field shows **<n/a>** or **<none>**.

Relevant Fixlets

The **Relevant Fixlets** tab lists the Fixlets that apply to the selected device. Use this tab to see the pending actions, patches, or configuration changes that the device qualifies for, based on its current state.

Use the toolbar to work with the list:

- **Filter**: Narrows the list to the Fixlets that match the criteria you set. For the steps, see Table filter *(on page 40)*.
- **Column**: Selects which columns appear in the table. For the steps, see Columns *(on page 29)*.
- **Density**: Changes the row height of the table. For the steps, see Density *(on page 29)*.

- **Deploy**: Deploys the Fixlets that you select. This button is available only after you select at least one Fixlet. For the wizard steps, see Deploying Fixlets *(on page 167)*.
- **Search by Fixlet name**: Finds a Fixlet by name.

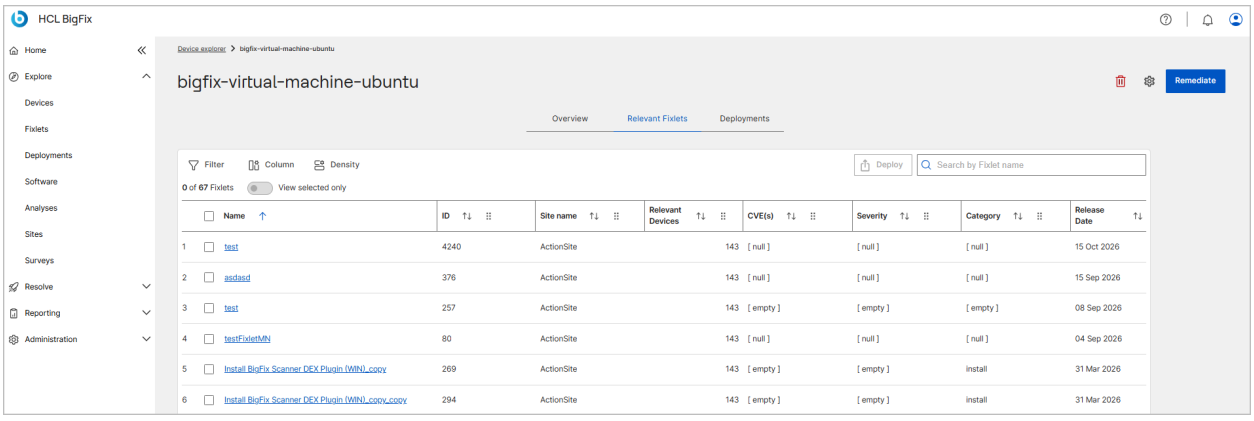
Below the toolbar, a counter shows how many Fixlets you selected out of the total, for example **0 of 67 Fixlets**. Turn on **View selected only** to hide the Fixlets that you did not select.

The table lists each Fixlet with a row number and a checkbox. Select the checkbox in the header row to select every Fixlet in the list. Select a Fixlet name to open its details. Each column header includes a sort control and a column menu. The following columns are available.

Table 17. Relevant Fixlets columns

Column	Description
Name	The name of the Fixlet. Select the name to open the Fixlet details.
ID	The unique identifier of the Fixlet.
Site name	The site that the Fixlet belongs to, such as ActionSite.
Relevant Devices	The number of devices on which the Fixlet is relevant.
CVE(s)	The CVE identifiers that the Fixlet addresses.
Severity	The severity that the Fixlet source assigns.
Category	The type of content, such as install or patch.
Release Date	The date when the Fixlet was released.

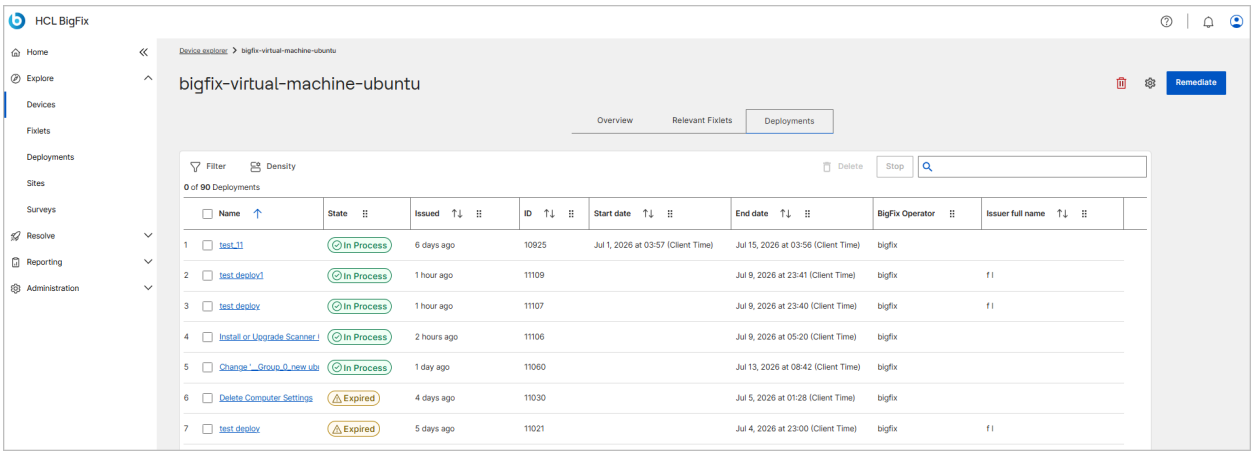
Note: When a value is not available, the column shows **[null]** or **[empty]**.



Deployments

The **Deployments** tab displays the actions and patches that have been deployed to the selected device, along with each deployment's state, issued time, ID, start and end dates, and operator. Use this tab to verify that targeted actions

are applied successfully and to troubleshoot failed deployments. You can filter and search the list, and select a deployment to **Stop** or **Delete** it.



Device Groups

Device groups help you organize devices and target actions, policies, or maintenance settings. BigFix UI supports two types of device groups:

- **Dynamic device groups:** Update memberships automatically as devices start or stop matching the defined conditions. You filter devices by properties, by existing device group membership, or with a relevance expression.
- **Static device groups:** Allow you to manually organize devices by explicitly adding or removing individual devices. Membership in a static group does not change automatically and remains exactly as defined by the user.

Note: Use dynamic groups when you want devices to automatically join or leave a group based on attributes like the operating system or agent type. Use static groups when you need absolute control over the group's membership, such as when selecting a specific set of pilot devices for a patch deployment.

Restriction:

BigFix UI does not support the following types of device groups:

- Server-based groups
- Manual groups whose membership is determined by client settings (client-evaluated manual groups)

These groups are not available in BigFix UI. To view and manage them, use the **BigFix Console**. For more information, see Known limitations *(on page 7)*.

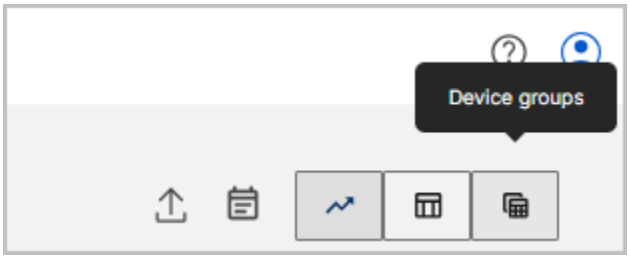
Key Capabilities

- **Visual Insights:** Use interactive donut and pie charts to view the ratio of static to dynamic groups and identify the largest groups by member count.
- **Automatic Updates:** Dynamic groups update memberships automatically as devices start or stop matching defined filter conditions.
- **Centralized Management:** View, edit, or delete existing groups directly from a single dashboard.
- **Targeted Actions:** Organize devices to streamline the deployment of actions, policies, or maintenance windows.
- **Site Ownership:** Every dynamic device group belongs to a site. You select the site when you create a dynamic group, and the **Site Name** and **Site Type** columns in the Device Groups table show which site owns each group. Site selection is not available for static device groups. For more information about sites, see Sites *(on page 194)*.

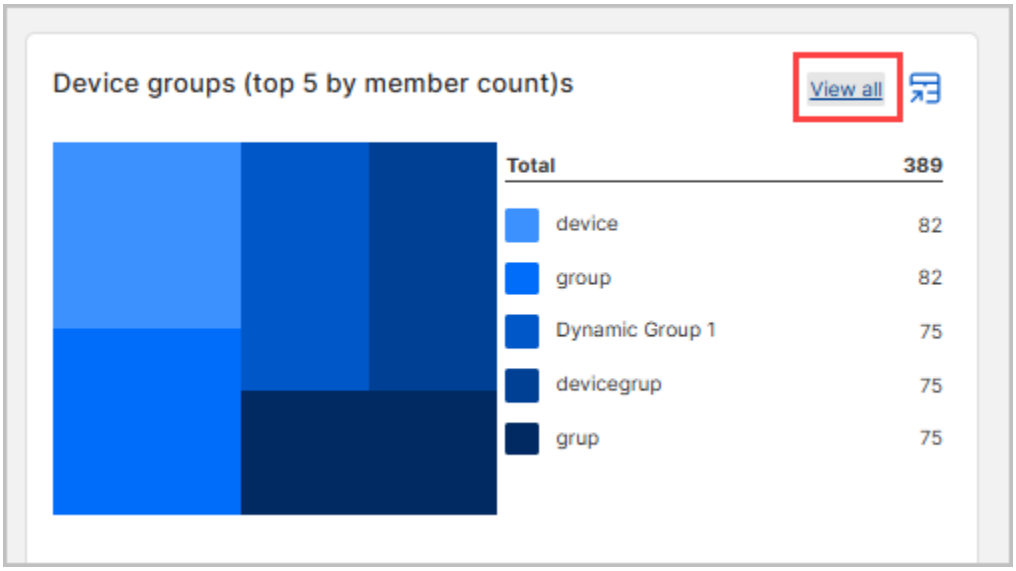
Device Groups Page Interface

You can navigate to the Device Groups page using one of two methods:

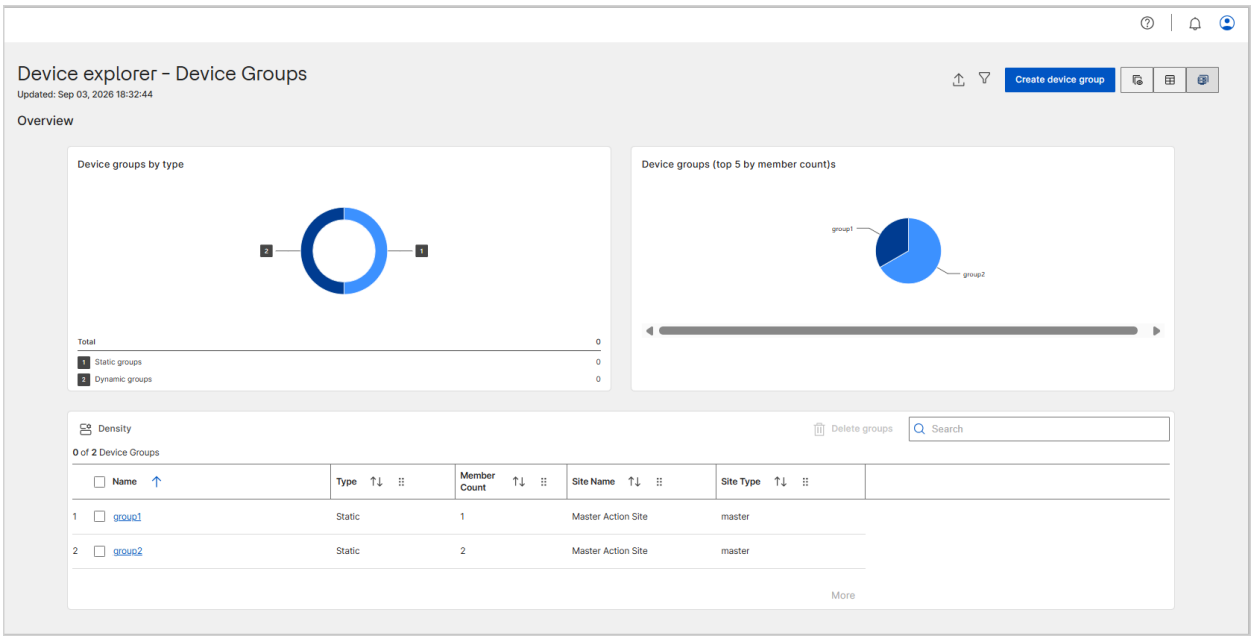
1. Click the **Device groups** icon located in the top-right corner of the **Device explorer - Overview** page.



2. Click the **View all** link next to the **Device groups (top 5 by member count)** chart.

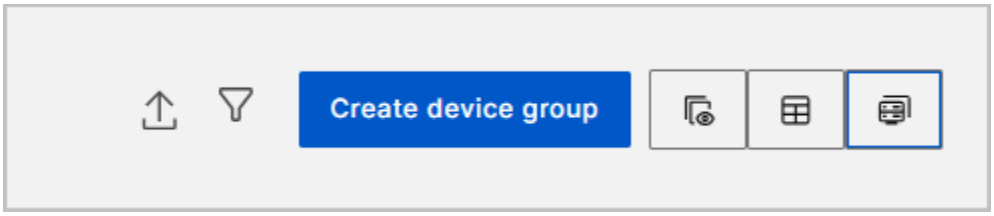


Once on the **Device explorer - Device Groups** page, you can interact with the following elements:



- **Overview Charts:** Includes a "Device groups by type" donut chart and a "Device groups (top 5 by member count)s" pie chart to provide high-level distribution insights.
    - **Device groups by type:** A donut chart that displays the total count and distribution of static versus dynamic device groups in your environment.
    - **Device groups (top 5 by member count):** A pie chart that identifies the five largest device groups based on the number of member devices, allowing you to quickly spot your most populated groups.

- **Device Groups Table:** Lists all available groups, displaying their **Name**, **Type**, **Member Count**, **Site Name**, and **Site Type**. Use the following controls to manage the table view and actions:
    - **Sort:** Click the up or down arrows next to any column header to sort the data in ascending or descending order.
    - **Density:** Click the Density icon to adjust the table row spacing. Choose from **Compact**, **Standard**, or **Comfortable**.
    - **Delete groups:** Select the checkbox next to one or more device groups, then click this button to permanently remove them.
    - **Search:** Enter text in the search bar to quickly filter and find specific device groups.
- **Device Group Details Page:** Clicking a specific group name in the table redirects you to its details page, which contains:
    - **Overview Tab:** Displays core properties (Group name, Group type, Current members, and Site for dynamic groups) and a table listing all current members of the group. You can click the **Manage group** button here to edit the group's conditions or name.
    - **Relevant Fixlets Tab:** Lists the Fixlets that apply to the devices in the group. You can select Fixlets and click **Deploy** directly from this tab.
    - **Deployments Tab:** Shows a history of deployments targeted at this group, allowing you to monitor status or use the **Delete** and **Stop** buttons for active or expired deployments.
- **View and Utility Bar:** Located at the top right of the **Device explorer - Device Groups** page:



    - **Export:** Click the Export icon to download the device groups list in CSV or Excel format for offline analysis or record-keeping. For detailed steps, see Exporting Data *(on page 30)* and Exporting Charts *(on page 32)*.
    - **Filter:** Click the Filter icon to narrow down the device groups displayed in the table based on specific properties and conditions. For detailed steps, see Global filter *(on page 36)*.
    - **Create device group:** Click this button to open the configuration side panel and define a new dynamic or static device group. For detailed steps, see Creating and Managing Device Groups *(on page 98)* and Managing Static Group Membership *(on page 105)*.

- **Overview:** Click the Overview icon (chart symbol) to switch back to the **Device explorer - Overview** page.
- **List:** Click the List icon (table symbol) to switch back to the **Device explorer - List view** page.

Creating and Managing Device Groups

Create new dynamic or static device groups, and edit or delete existing groups to organize your endpoints effectively.

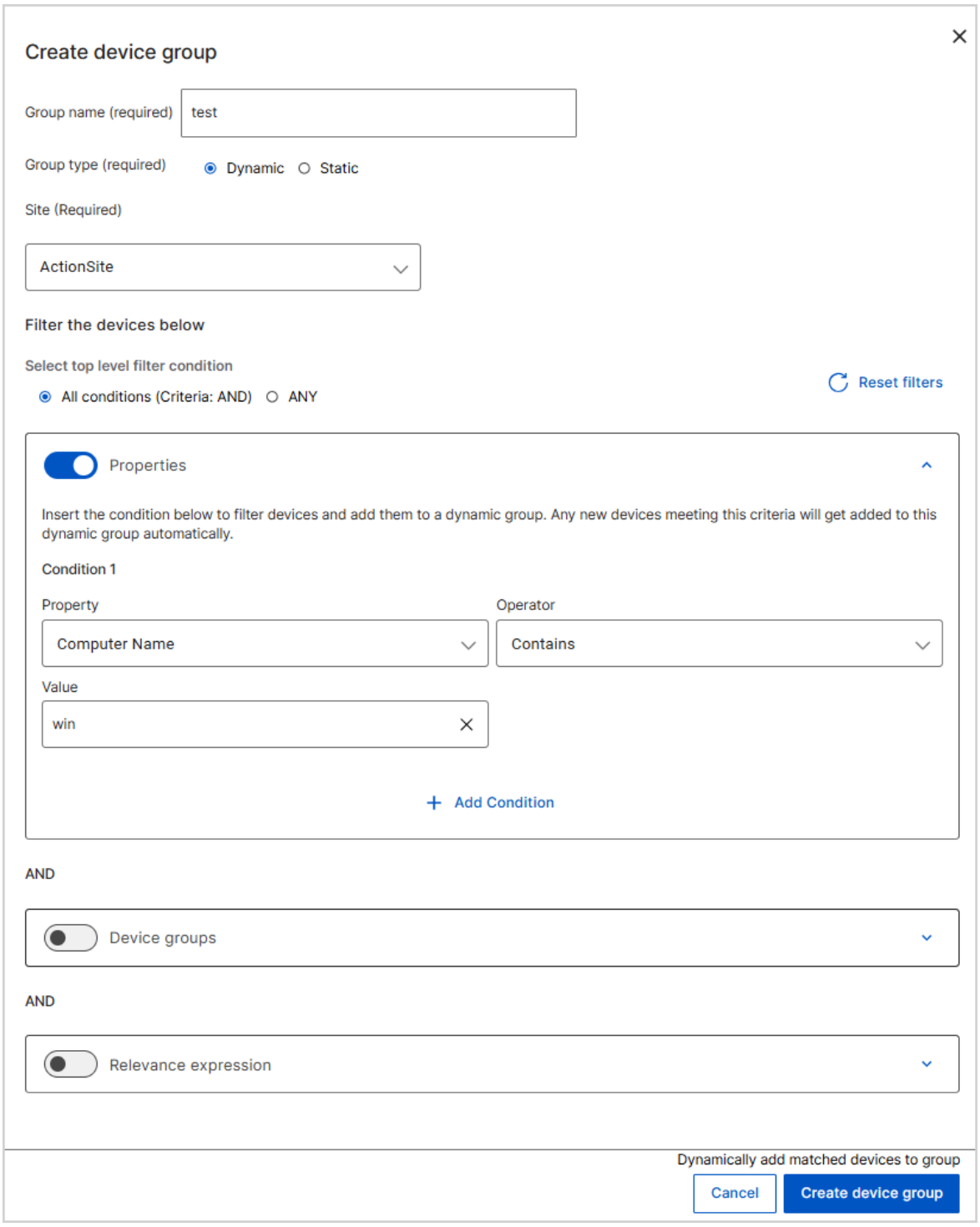
Prerequisites

- You must have the appropriate permissions to manage devices and device groups.
- For dynamic groups, the device properties used for filtering must be reported by the BigFix agent.

Create a Device Group

1. From the BigFix UI side navigation, expand **Explore** and select **Devices**.
2. Navigate to the Device Groups page by clicking the **Device groups** icon in the top-right corner, or by clicking the **View all** link next to the **Device groups (top 5 by member count)** chart.
3. Click **Create device group** in the top-right corner.

   The Create Device Group widget page opens.



4. In the **Group name (required)** field, enter a unique name for the device group.

5. In the **Group type (required)** section, select one of the following options:

- **Dynamic:** Enables filter conditions for automatic membership updates. Devices that match the defined filter conditions are automatically added to the group and updated dynamically over time.
- **Static:** Static device groups allow you to manually organize devices by explicitly adding or removing individual devices. Membership in a static group does not change automatically and remains exactly as defined by the user.

6. Perform the appropriate steps based on your selection:

   - **To configure a Dynamic group:**

     a. From the **Site (Required)** drop-down, select the site that owns the device group.

     The list shows the sites that you have permission to write to, such as **ActionSite** or a custom site. The site determines where BigFix stores the group and who can use it. You cannot change the site after you create the group.

     Note: Site selection is available only for dynamic device groups.

     b. Under **Filter the devices below**, select the top-level filter condition: **All conditions (Criteria: AND)** to add only the devices that match every enabled section, or **ANY** to add the devices that match at least one enabled section.

     c. Turn on the toggle for each section that you want to use. The enabled sections are combined with the top-level condition that you selected.

        - **Properties:** Filters devices by reported device properties.
        - **Device groups:** Filters devices by their membership in existing device groups.
        - **Relevance expression:** Filters devices with a relevance expression that you write.

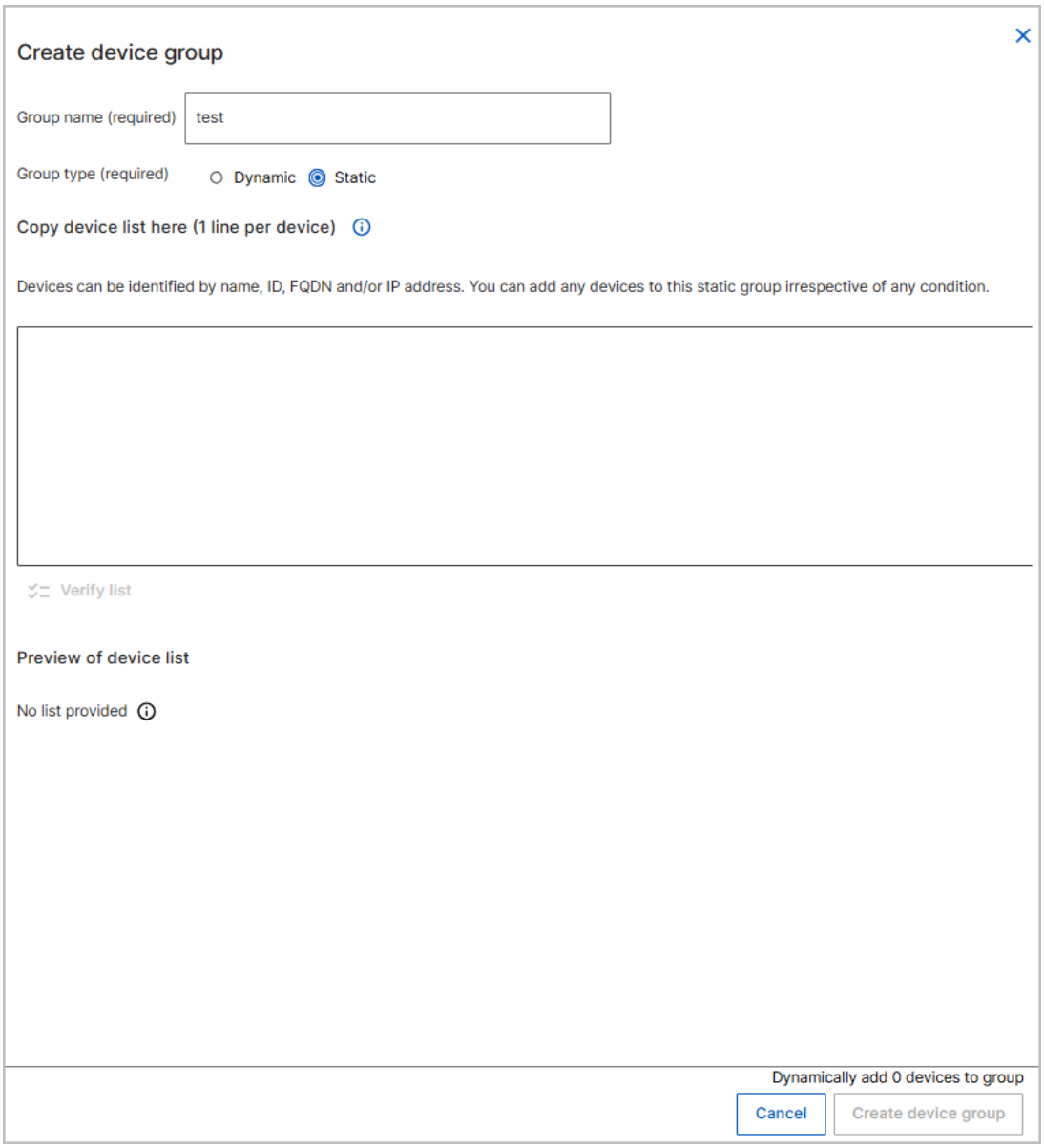
     d. In the **Properties** section, define **Condition 1**: select the **Property**, select the comparison **Operator**, and enter or select the matching **Value**.

     e. *(Optional)* Click **Add Condition** to add more conditions to the section.

     f. *(Optional)* Click **Reset filters** to clear all conditions and start over.

     g. For more information about building filter conditions, see Filter by query *(on page 40)*.

   - **To configure a Static group:**



a. Under **Copy device list here (1 line per device)**, enter the target devices by name, ID, FQDN, and/or IP address. Enter each device on a separate line.

b. Click **Verify list** to review the preview of the device list.

Note: You can also add devices to a static group directly from the device table on the **Device explorer - List view** page. For more information, see Managing Static Group Membership *(on page 105)*.

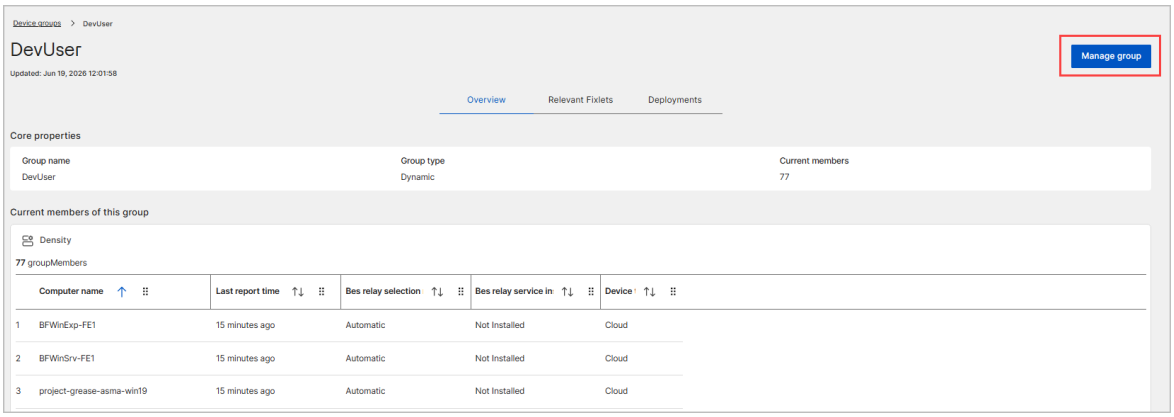
7. Click **Create device group**.

Result The device group is created and appears in the data table. For dynamic groups, the table also shows the **Site Name** and **Site Type** of the site that owns the group.

Edit a Device Group

Modify the properties, filter conditions, or device list of an existing dynamic or static device group to update your targeted endpoints.

1. From the **Device explorer - Device Groups** page, click the name of the group you want to edit.
2. On the group details page, click the **Manage group** button in the top-right corner.

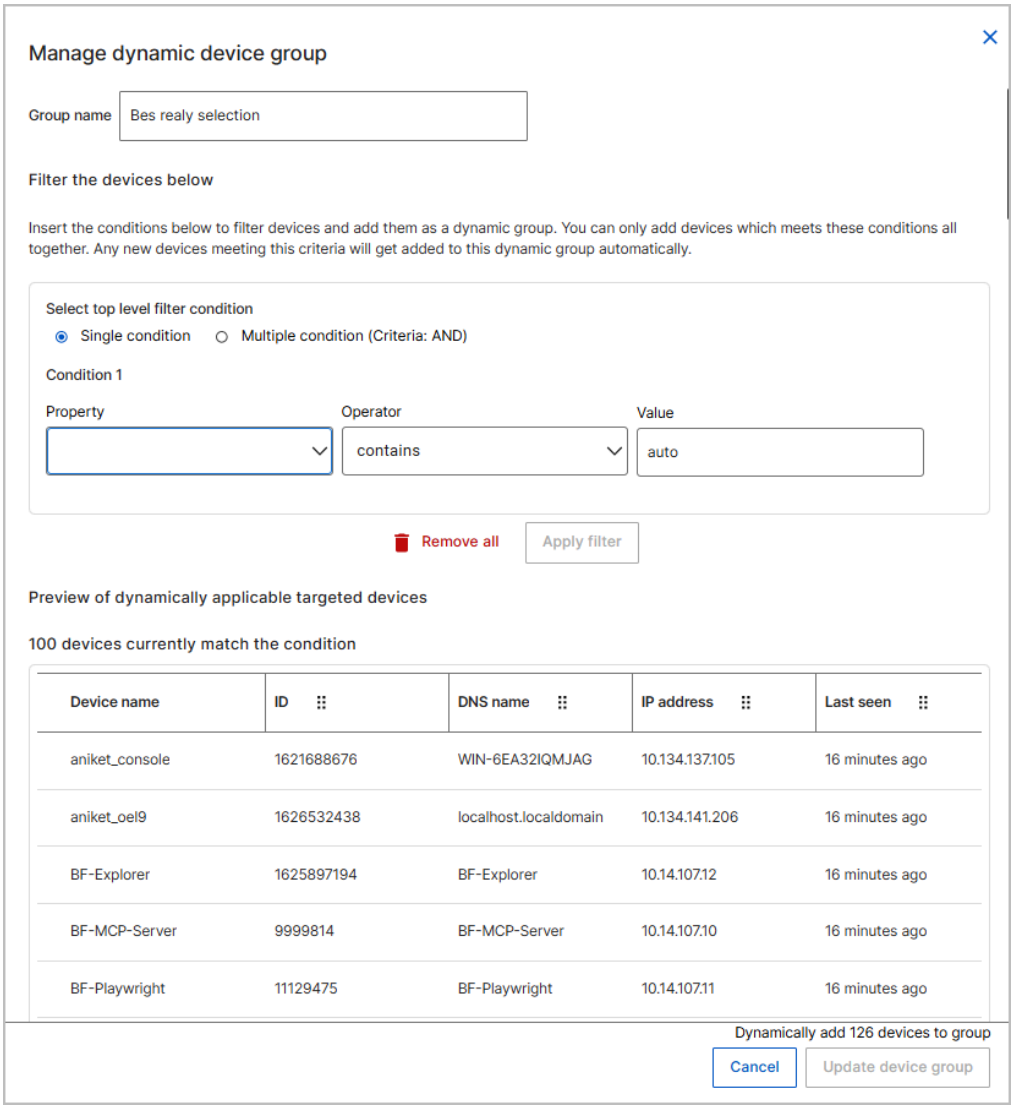


3. In the Manage device group side panel, update the **Group name** if necessary.

> **Note:** You cannot change the **Site** of an existing dynamic device group. To move a group to another site, delete it and create it again in the required site.

4. Update the group membership criteria based on the group type:
    - **If editing a Dynamic group:**
        a. Under **Filter the devices below**, change the top-level filter condition between **All conditions (Criteria: AND)** and **ANY**.
        b. Turn the **Properties**, **Device groups**, and **Relevance expression** toggles on or off to change which sections apply to the group.
        c. Modify the individual conditions by updating the **Property**, **Operator**, and **Value** fields. Click **Add Condition** to add a condition. *(Optional)* Click **Reset filters** to clear the existing conditions and start over.

d. Review the **Preview of dynamically applicable targeted devices** section to ensure the correct devices match your new conditions.



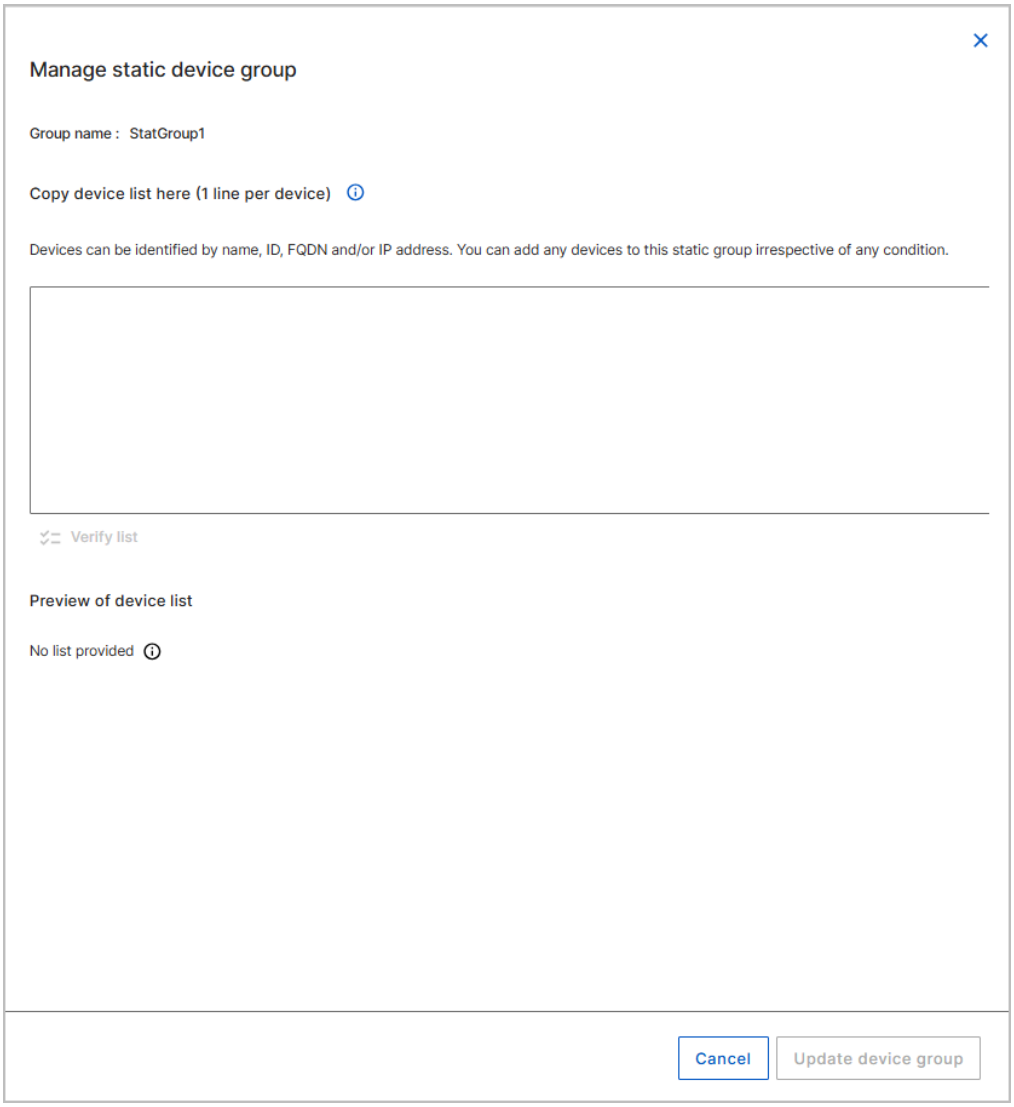
◦ **If editing a Static group:**

a. Locate the **Copy device list here (1 line per device)** text box.

b. Add or remove target devices in the text box. You can identify devices by their name, ID, FQDN, and/or IP address. Ensure each device is entered on a separate line.

c. Click **Verify list** to validate the entered devices.

d. Review the **Preview of device list** section to confirm the endpoints are correctly identified.

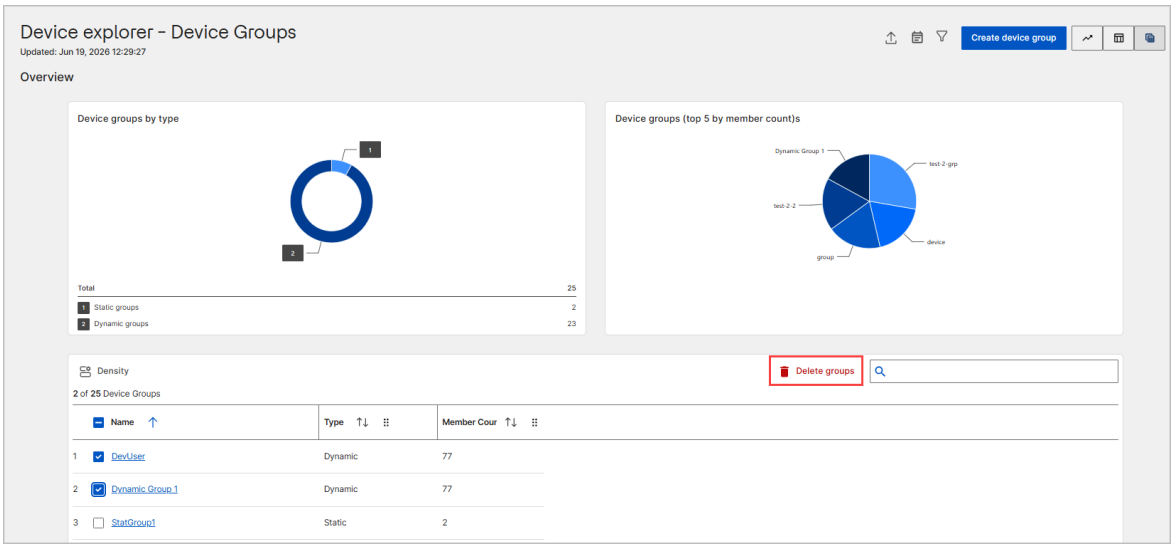


5. Click **Update device group**.

   Result The device group's criteria and properties are updated immediately. For dynamic groups, the BigFix UI automatically recalculates the group's membership based on the new conditions. For static groups, membership is updated to reflect the explicitly defined device list.

Delete a Device Group

1. From the **Device explorer - Device Groups** page, locate the group(s) you want to remove in the data table.
2. Select the checkbox next to the group name(s).



3. Click the **Delete groups** button located above the data table.
4. In the confirmation dialog, review the warning message.

   The dialog indicates that you will no longer be able to manage or remediate the entity, and all associated history will be deleted. This action cannot be undone.
5. Click **Delete device group** to confirm and proceed with the deletion.

Result The device group is permanently removed from the BigFix UI and will no longer appear in the Device Groups data table.

Managing Static Group Membership

Static device groups allow you to manually organize devices by explicitly adding or removing individual devices. Membership in a static group does not change automatically and remains exactly as defined by the user.

In BigFix UI, you can create a static device group directly from a device's details page or add the device to an existing static group. You can also select several devices in the device table and add them to a static group in one action. This approach is useful when you want precise control over which devices are included for administrative actions, testing, or targeted operations.

How Static Device Groups Work

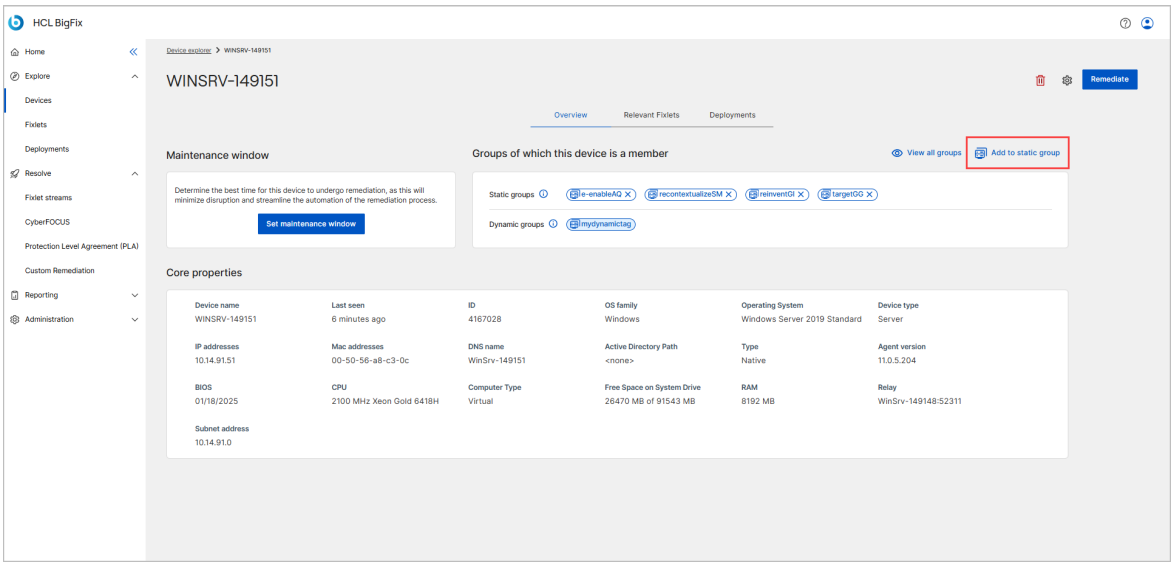
- A static group contains only the devices that you manually add.
- Devices remain members of the group until they are explicitly removed.
- From a device's details page, you can:
  - Create a new static group and add the current device to it.
  - Add the device to one or more existing static groups that it is not already part of.
- From the device table on the **Device explorer - List view** page, you can add one or more selected devices to a static group.

- All static groups associated with a device are displayed in the Groups of which this device is a member section on the device details page.
- Static groups can be managed centrally from the Groups view.

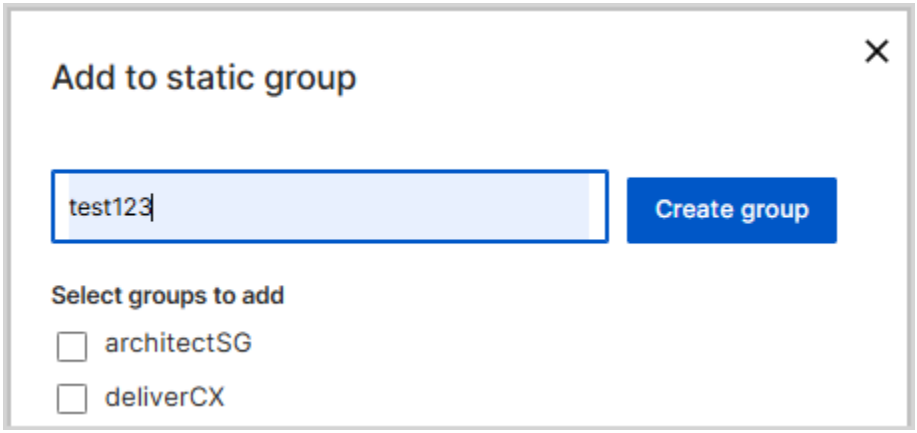
Create a New Static Device Group from a Device

Use this procedure when you want to create a new static group and immediately include the selected device.

1. From the BigFix UI navigation, open **Devices**.
2. Select a device to open the device details page.
3. In the Groups of which this device is a member section, click **Add to static group**.



4. In the Add to static group dialog:



   a. Enter a name for the new static group.
   b. Click **Create group**.

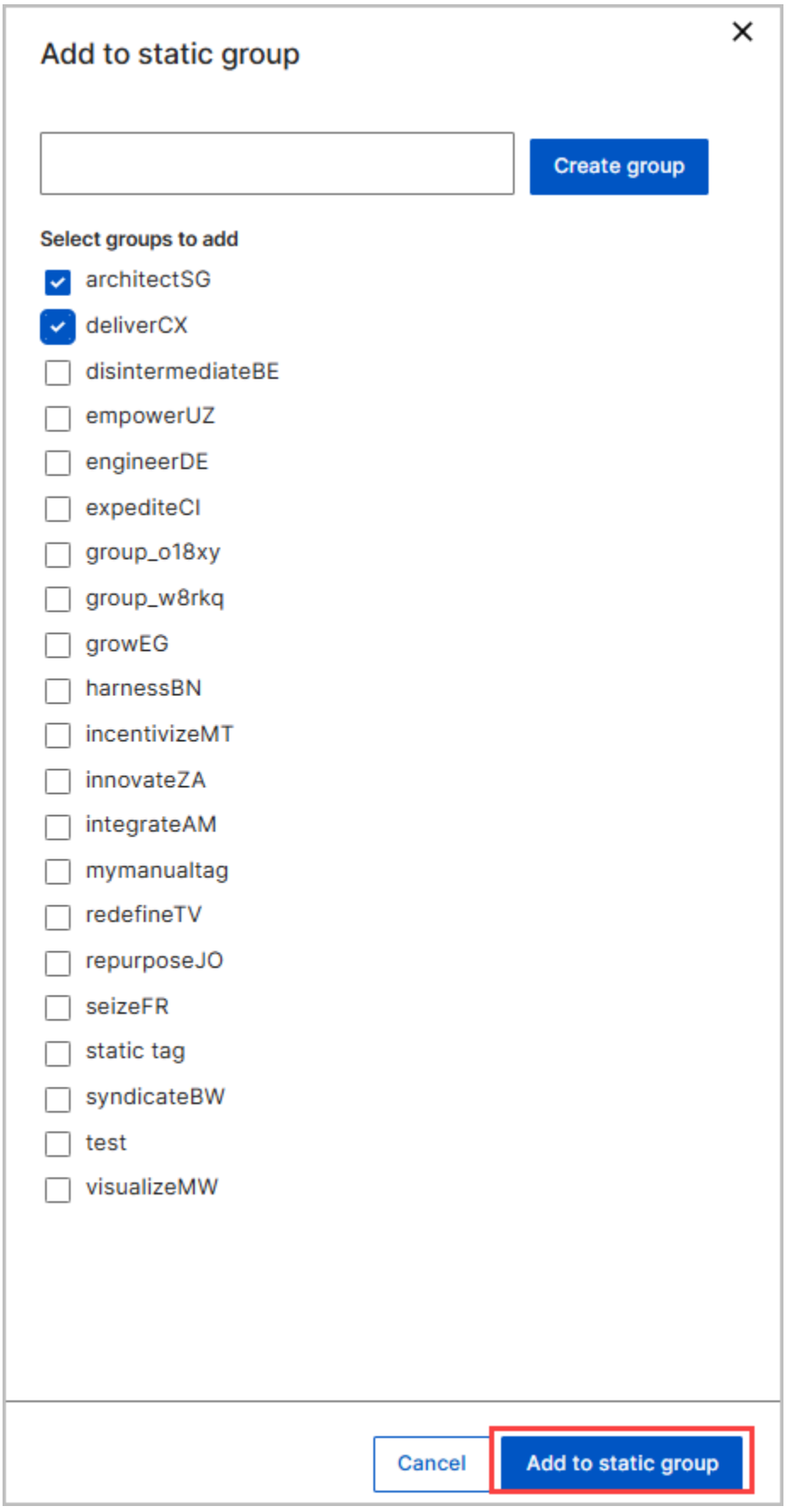
The group appears in the **static groups** membership list.



Add a Device to an Existing Static Device Group

Use this procedure to add the device to one or more static groups that already exist.

1. Open the device details page from device list.
2. Click **Add to static group** from the devices detail page.
3. In the dialog, select one or more static groups from the list.


Add to static group
Create group
Select groups to add
architectSG
deliverCX
disintermediateBE
empowerUZ
engineerDE
expediteCI
group_o18xy
group_w8rkq
growEG
harnessBN
incentivizeMT
innovateZA
integrateAM
mymanualtag
redefineTV
repurposeJO
seizeFR
static tag
syndicateBW
test
visualizeMW
Cancel
Add to static group

Only static groups that the device is not already a member of are available.

4. Click **Add to static group**.

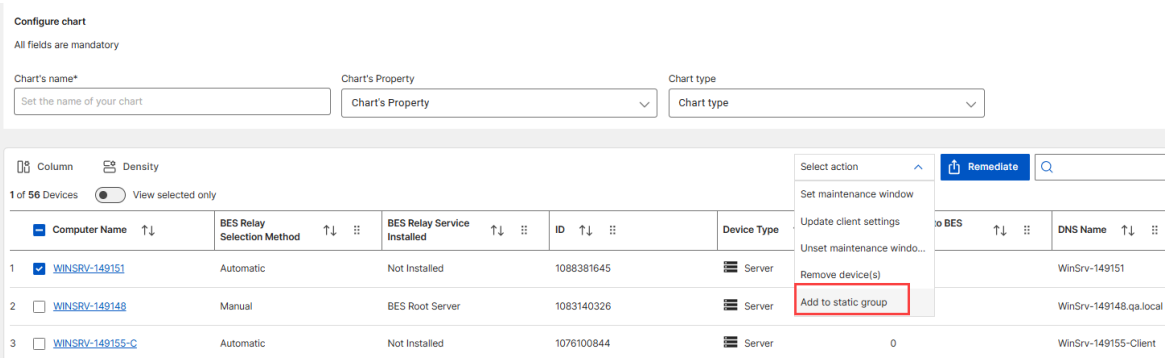
   The device is added to the selected static groups.

   The updated group membership is reflected on the device details page.

Add Devices to a Static Device Group from the Device Table

Use this procedure to add one or more devices to a static group without opening each device details page.

1. From the BigFix UI side navigation, expand **Explore** and select **Devices**.
2. Switch to the **List view** page using the view icons in the top-right corner.
3. In the device table, select the checkbox next to each device that you want to add. A counter above the table, such as **1 of 56 Devices**, shows how many devices you selected.
4. From the command bar, click **Select action** and choose **Add to static group**.



5. In the **Add to static group** dialog, select an existing static group, or enter a name to create a new static group for the selected devices.
6. Click **Add to static group**.

   Result The selected devices are added to the static group. The updated membership appears in the group details page and in the **Groups of which this device is a member** section of each device.

Remove a Device from a Static Device Group

You can remove a device from a static group without affecting other devices in the same group.

1. Open the device details page.
2. In the **Groups of which this device is a member** section, locate the static group.
3. Click the **X** icon next to the static group name to remove the device from the static group.



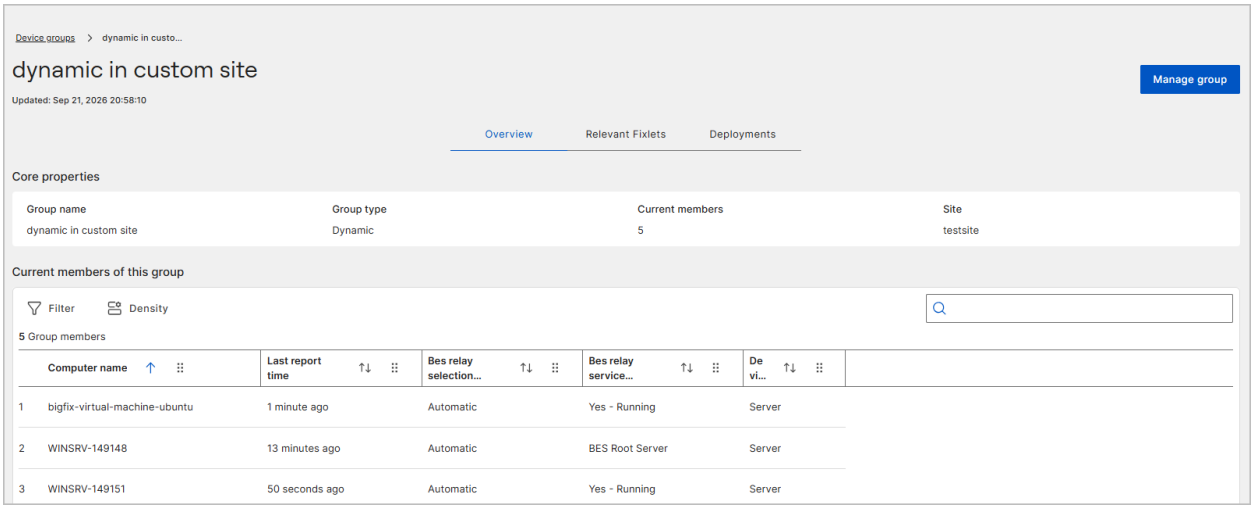
Result The device is no longer a member of the static group. The static group itself remains available for use.

Device Group Details Page

The Device Group Details page provides a comprehensive, focused view of a specific device group. You access this page by clicking a group name from the Device Groups data table. Use this page to review group properties, view member endpoints, identify relevant vulnerabilities, and track deployment history.

The page includes a **Manage group** button in the top-right corner, which allows you to edit the group's name or filter conditions. The information is organized into three tabs: **Overview**, **Relevant Fixlets**, and **Deployments**.

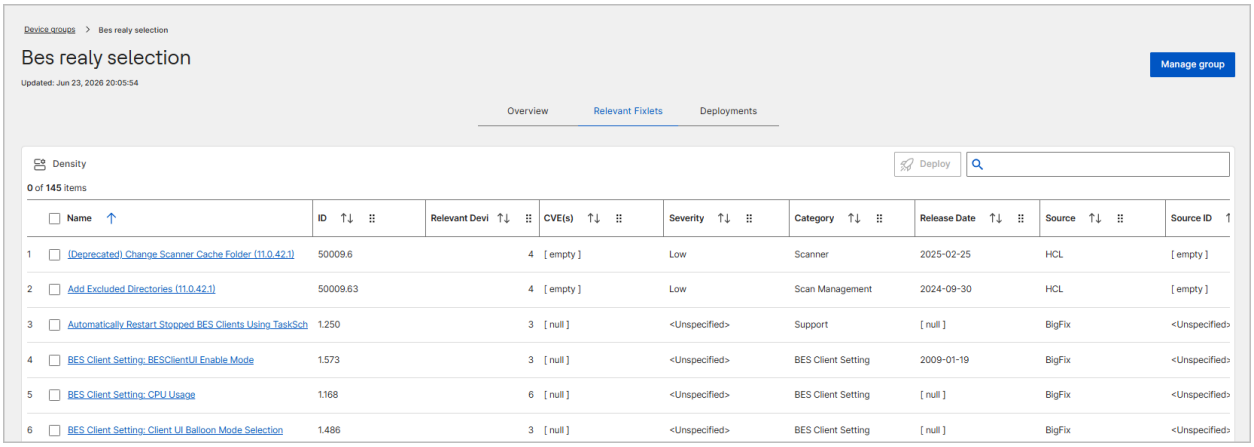
Overview Tab



The Overview tab provides a summary of the group's configuration and a list of its current members.

- **Core properties:** Displays the **Group name**, the **Group type** (Dynamic or Static), the total number of **Current members**, and the **Site** that owns the group. The **Site** property appears only for dynamic device groups.
- **Current members of this group:** A data table that lists all endpoints currently belonging to the group. Use this table to review individual device details, including **Computer name**, **Last report time**, **Bes relay selection**, **Bes relay service in** (installed status), and **Device** (type). You can adjust the row spacing using the **Density** drop-down.

Relevant Fixlets Tab



The Relevant Fixlets tab identifies pending actions, patches, or configuration changes applicable to the devices within the group.

- **Data Table:** Displays all Fixlets relevant to the group's members, including details like the Fixlet **Name**, **ID**, **Relevant Devices** count, **CVE(s)**, **Severity**, and **Category**.
- **Search and Filter:** Use the search bar to quickly locate specific Fixlets by name, ID, or CVE.
- **Deploy Actions:** Select the checkbox next to one or more Fixlets and click the **Deploy** button to initiate a remediation action directly to the devices in this group.

Deployments Tab

The Deployments tab displays the history and current status of actions or patches deployed to the devices in this group.

- **Data Table:** Review deployment records, including the deployment **Name**, **State** (such as Active, Expired, Stopped, or Failed), **Start date**, and **End date**.
- **Manage Deployments:** Select one or more active deployments and click the **Stop** button to halt them. Select expired deployments and click the **Delete** button to remove them from the list.
- **Search and Filter:** Use the search bar to locate specific deployment records quickly.

Setting-up Remediation Flow

The remediation process in BigFix UI is designed to simplify and streamline patch management and vulnerability remediation.

To set up your custom remediation flow and initiate remediation, complete the following steps.

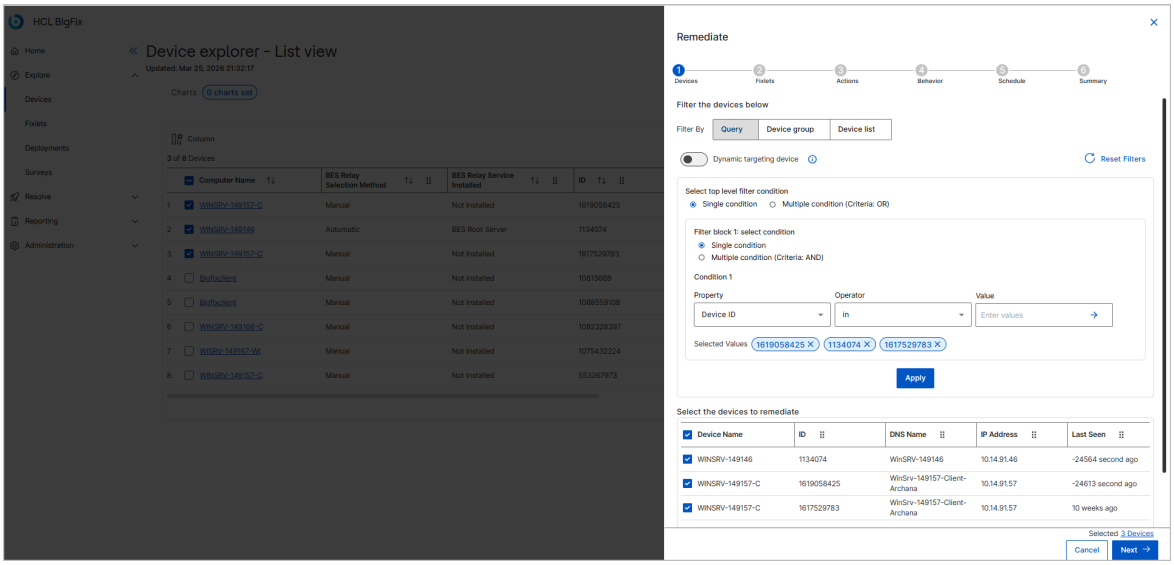
Guidelines for remediation flows

- **Check for input requirements**: Before you add Fixlets to a remediation flow, make sure that none of them require user input, either through the `action parameter query` command or through description forms. These Fixlets end in error when they run.
- **Alternative**: Deploy Fixlets that require user input from the **BigFix Console**.

For more information, see Known limitations *(on page 7)*.

Accessing the Remediate widget

1. Log in to BigFix UI using your Admin credentials.
2. **Go to the Device Explorer Section**
    a. In the BigFix UI application, from the left pane click **Apps** and select **Device Explorer** .
    b. Click the **List** icon to view the devices in list view.
    c. Select the devices that you want to target, the **Remediate** button becomes active.
    d. Click the **Remediate** button to open the Remediate widget.

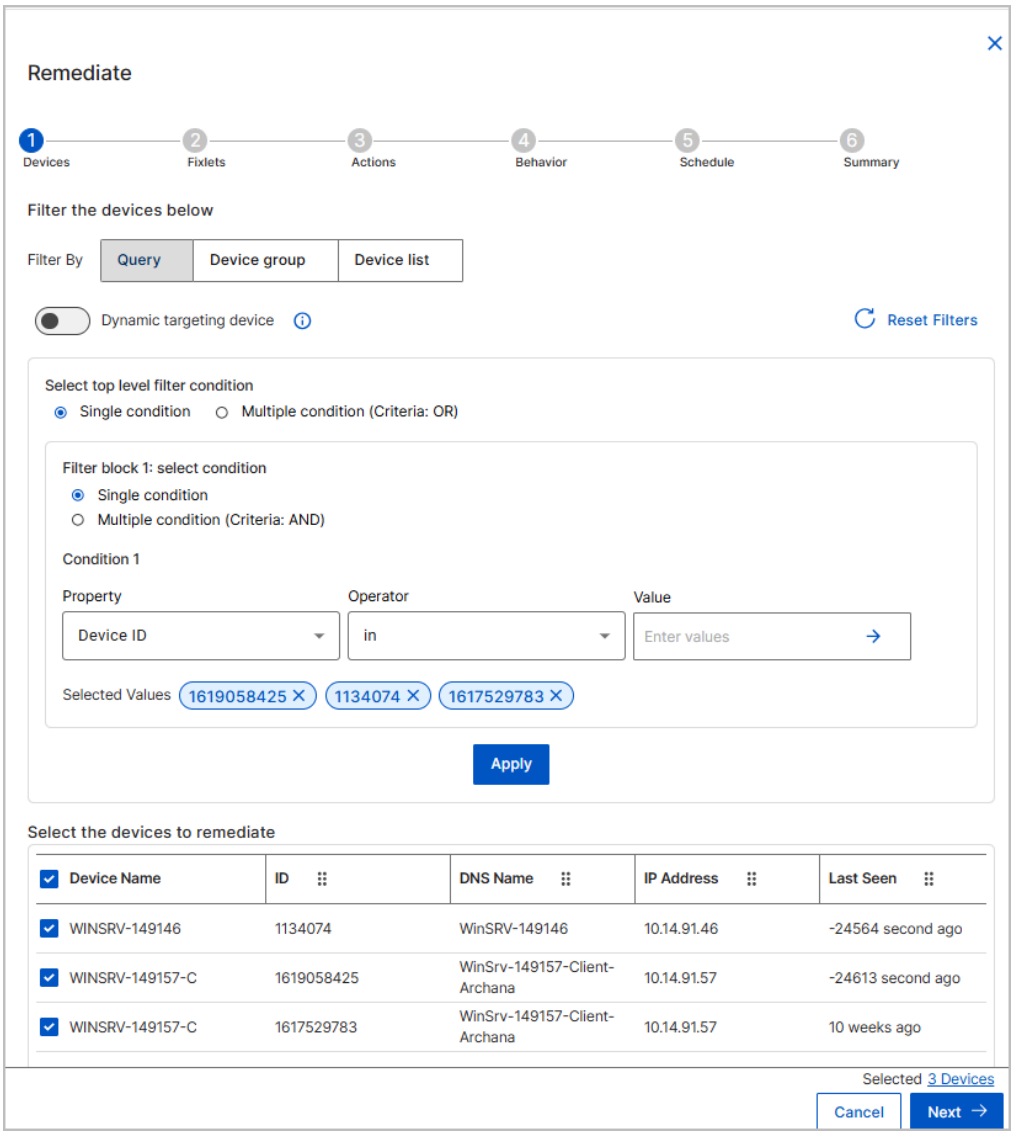


Setting up remediation flow

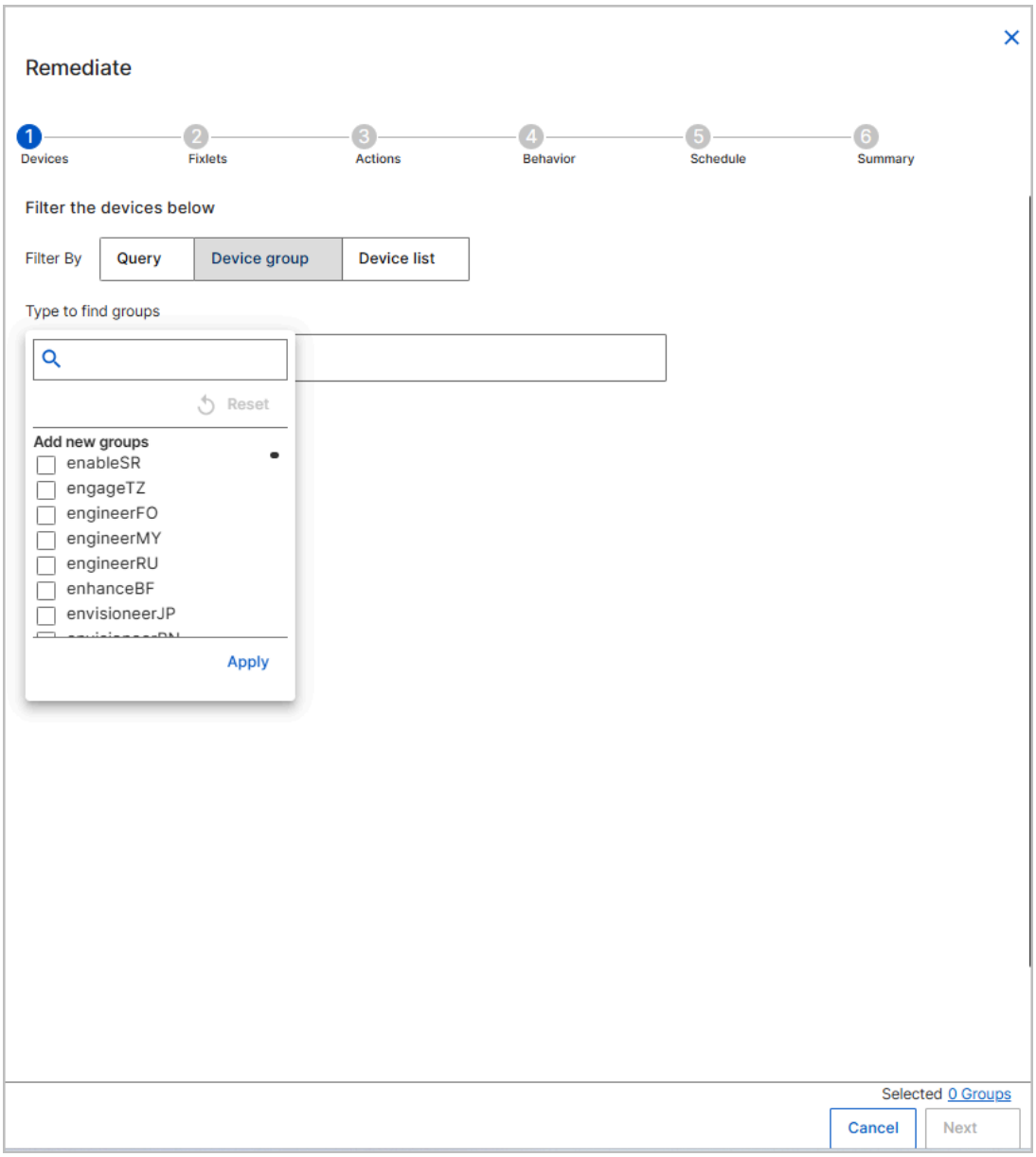
To configure a custom remediation flow, complete the following steps:

1. **Devices**: You can modify the target devices selection using a query to apply the remediation or filter target devices from the device group or device list displayed.
    a. **Filter by Query**
        i. You can apply filters using **Single condition** or **Multiple condition (AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see filtering data *(on page 28)* section.
        ii. By default, the device table displays all devices that match the query, with details such as Device Name, ID, DNS Name, IP Address, Last Seen, OS Family, Operating System, and Device Type.
        iii. Dynamic Targeting device Option:
            - Within this approach, you can enable the **Dynamic Targeting Device** toggle.
            - Dynamic filters define a matching criteria for devices to evaluate continuously until the deployment ends. Any device that matches this filter after the deployment has been created, will have this deployment applied.

- New devices that match the criteria are automatically added.
- A **Preview of dynamically applicable targeted devices** is shown to confirm eligibility.



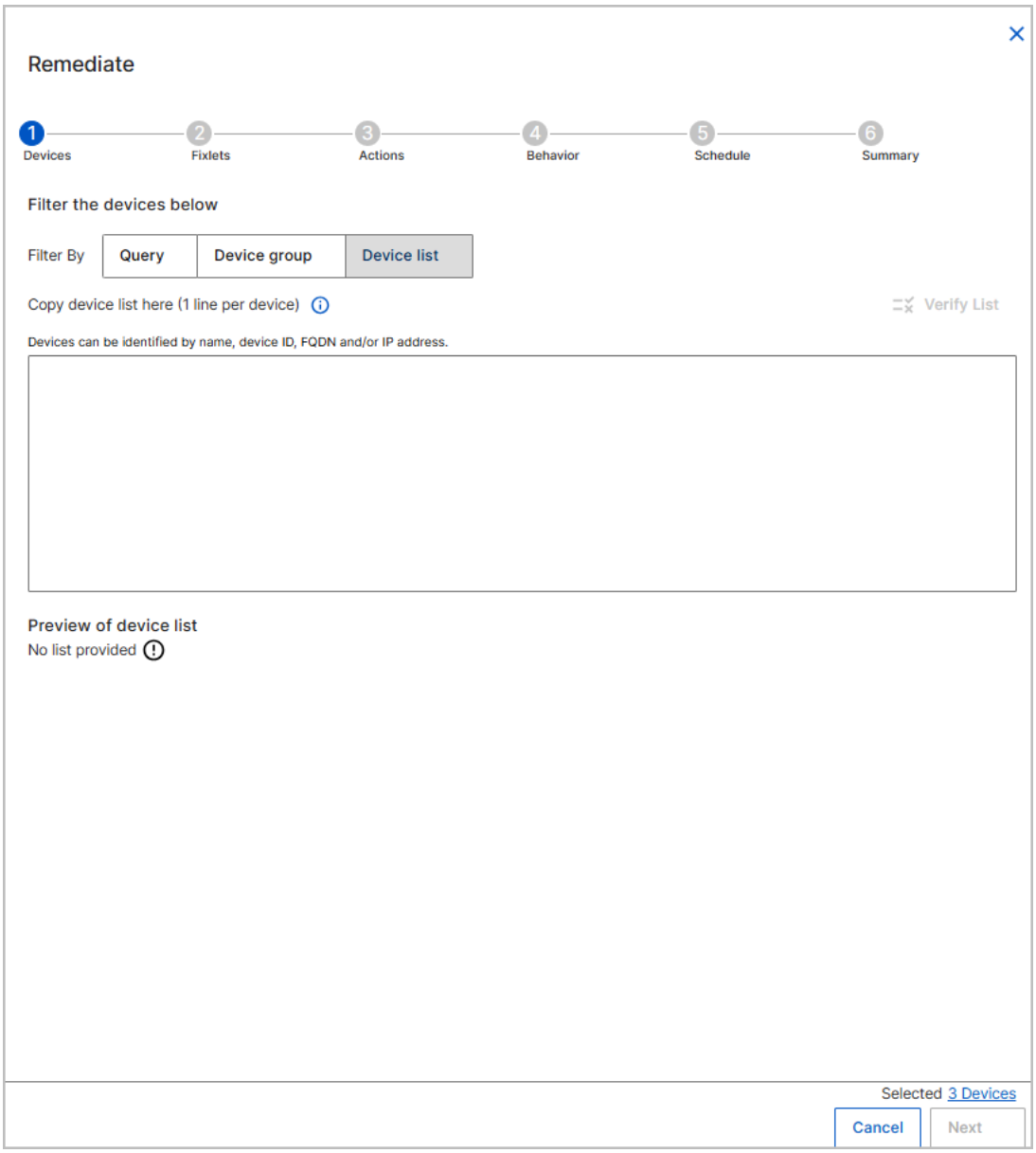
b. **Filter by Device group**- Select a pre-defined device group to target.



i. Locate and select your target groups:

- **Search**: Use the search bar to type and quickly find specific groups by name.
- **Select**: Check the box next to one or more groups under the **Add new groups** list.
- **Reset**: Click **Reset** if you need to clear your current selections within the menu.
- Click **Apply** within the dropdown menu to confirm your group selection.

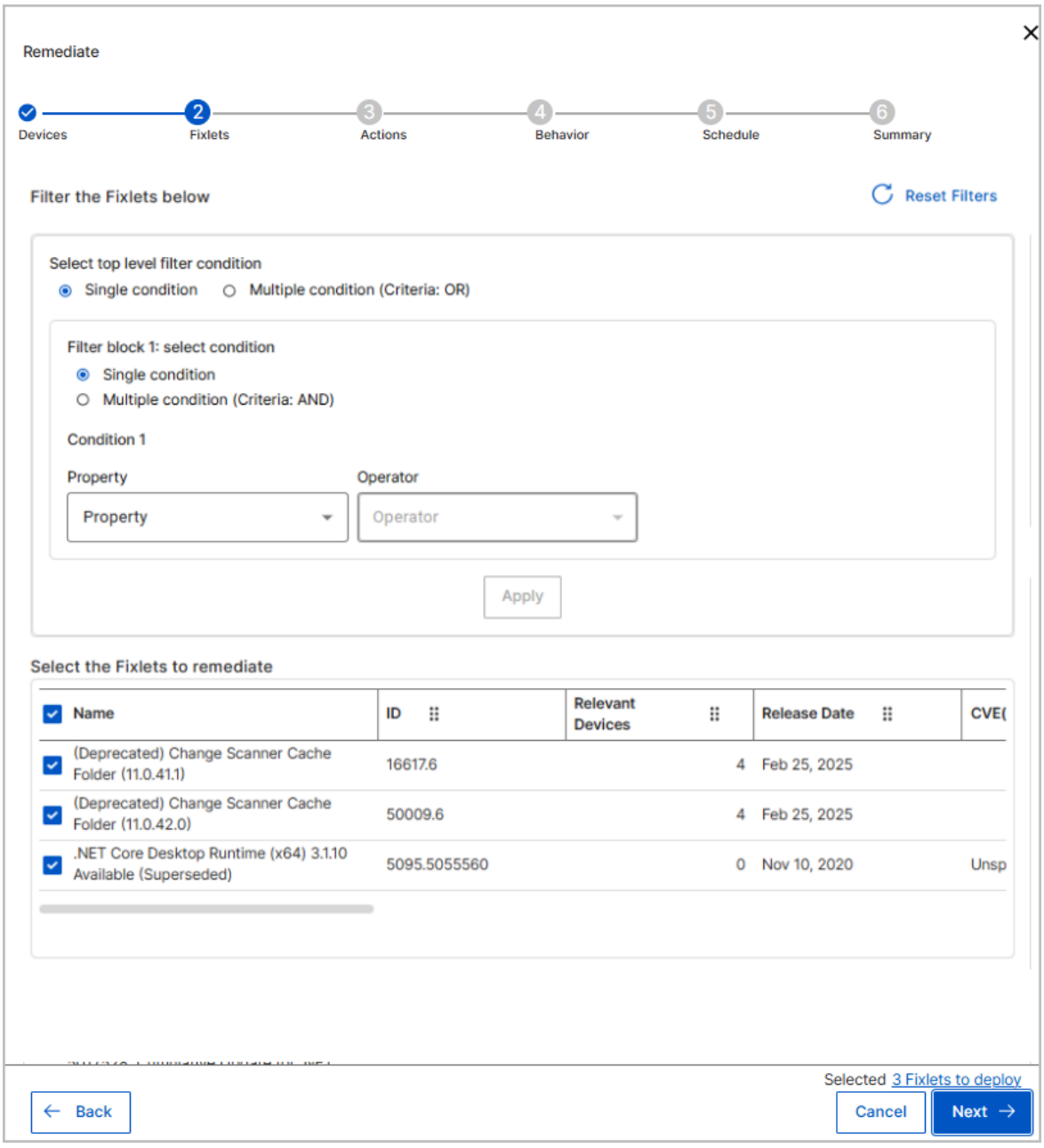
c. **Filter by Device List** - This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.



- Regardless of how they are identified, each device must be in a separate row.
- A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
- Use Verify List to confirm the entries before proceeding.
- The Preview area shows the final static list that will be targeted.

Once the appropriate filters have been selected, or if no filter is needed, click **Next**.

2. **Fixlets**: Configure conditions to filter and select Fixlets to remediate or select the Fixlets from the displayed Fixlets list.



a. All selected Fixlets are listed in a table

b. You can apply filters using **Single condition** or **Multiple condition (Criteria: AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see Filter by query *(on page 40)*.

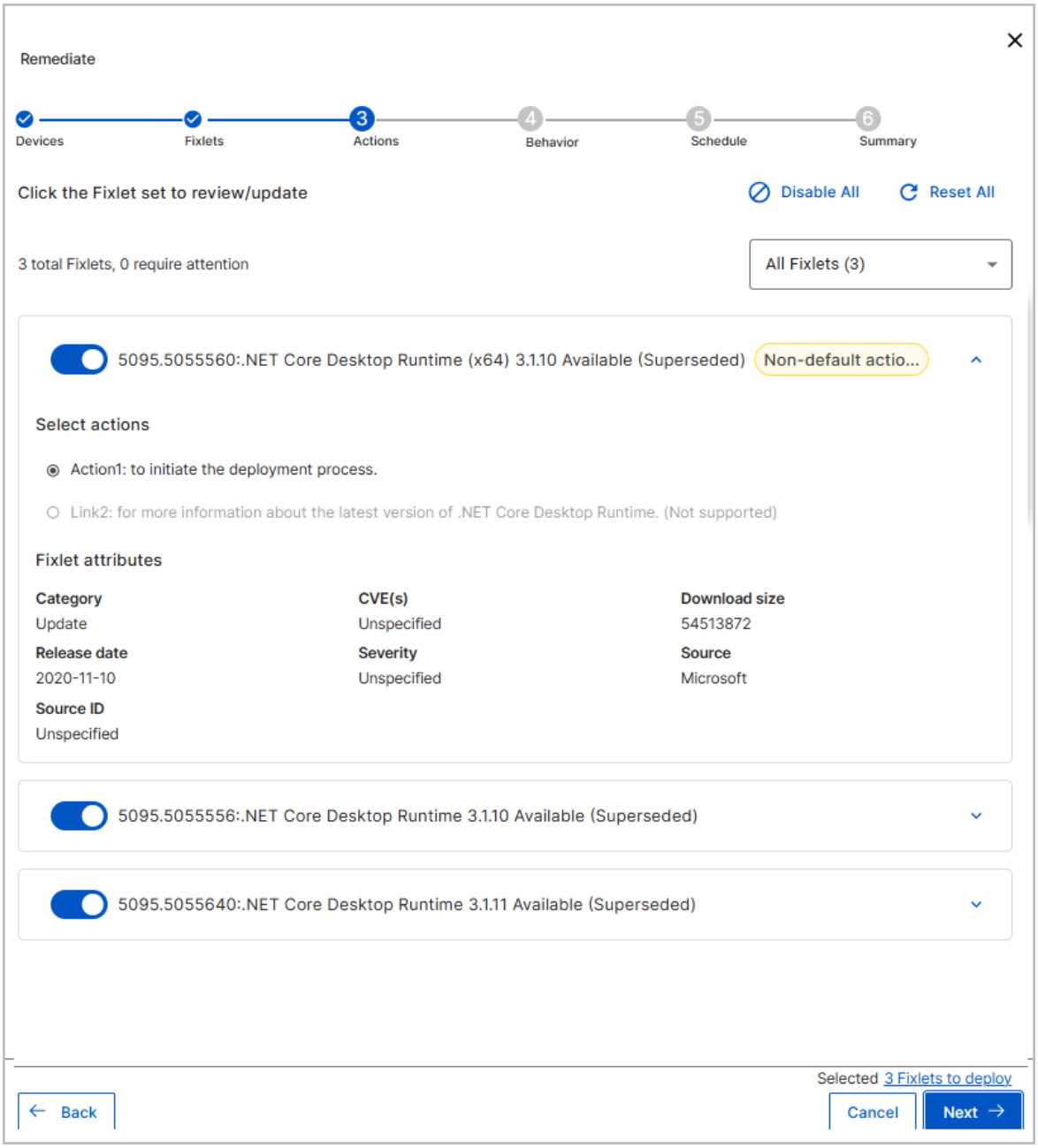
c. Fixlet Table – Review the list of Fixlets.

d. Select Fixlets – Use checkboxes to choose one or more Fixlets for remediation. A counter shows how many are selected.

e. Next/Cancel – Click **Next** to continue to Actions, or **Cancel** to exit.

3. **Actions**: You can review and update the actions for the set of Fixlets with default action and without default action.

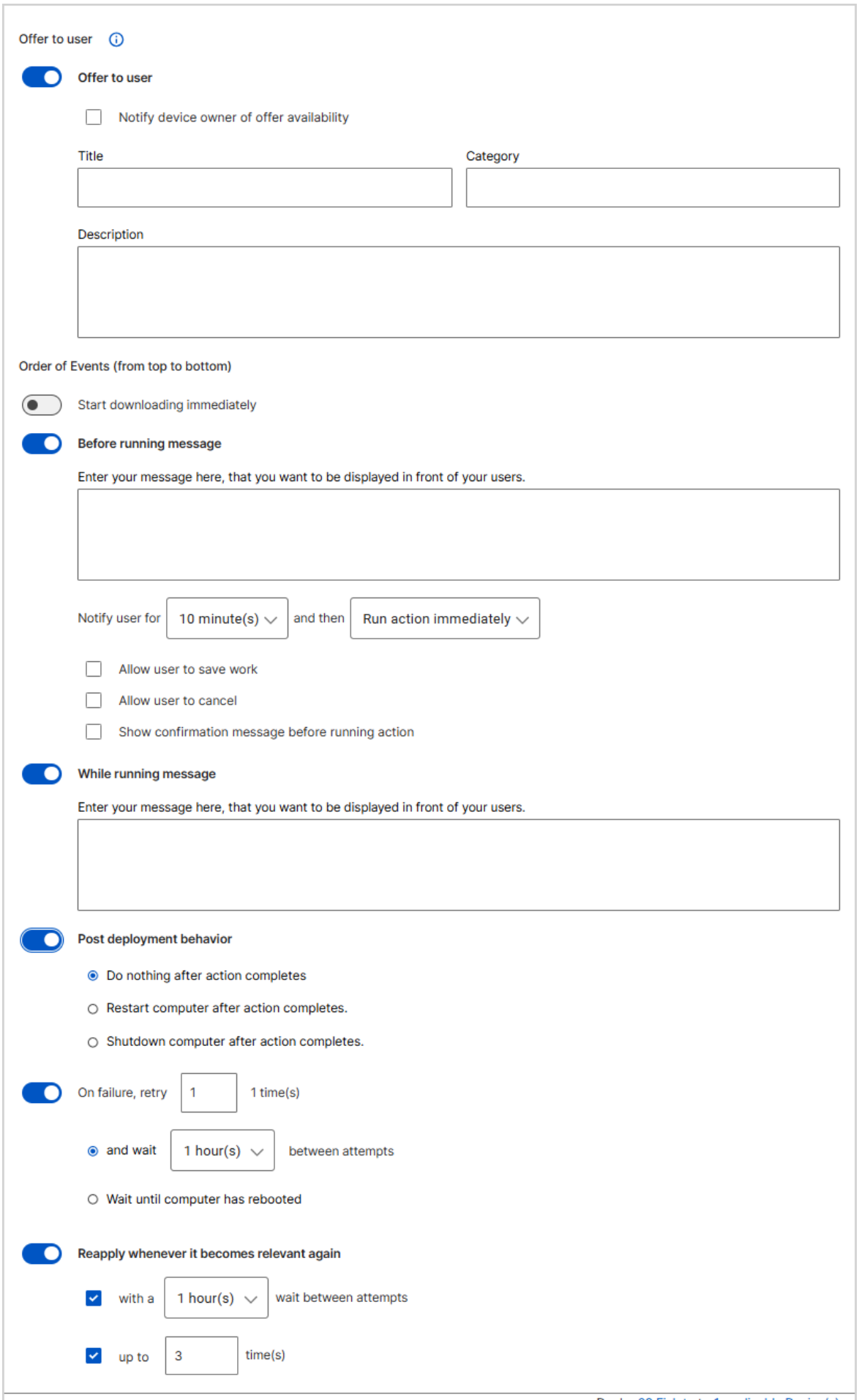
   In this tab, confirm the actions you want the Fixlets you have selected to perform. This is important because not every Fixlet has a single, default action. It is also possible to remove Fixlets that do not have any actions that can be performed on the devices selected in the prior tab.



UI Elements:

a. The Actions step lists all selected Fixlets.
b. Action filter drop-down – Allows you to refine which Fixlets are shown in the list. Available filter options:
    i. All Fixlets – Displays all Fixlets in the remediation set.
    ii. Fixlets that are not actionable – Displays Fixlets that cannot be acted upon.
    iii. Fixlets with no-default action – Shows Fixlets that do not have a predefined default action.
    iv. Action required – Filters Fixlets that require immediate attention.
c. **Actions step**: Review and update the actions for the selected Fixlets.
    i. For Fixlets requiring a choice, select the radio button for the desired action (e.g., **Action1: to initiate the deployment process**).
d. Review the **Fixlet attributes** provided in the details pane to confirm accuracy.
e. Each Fixlet has a toggle switch to enable or disable its deployment.
f. Ensure the toggle switch next to the Fixlet is set to **On**.
g. You can use Disable All or Reset All options as needed.
h. Verify the deployment summary link at the bottom right
i. Once this information is provided, click **Next** to proceed to the Sequence tab.

4. **Behavior**: You can configure the options to deploy the Fixlets from here.


Offer to user
Offer to user
Notify device owner of offer availability
Title
Category
Description
Order of Events (from top to bottom)
Start downloading immediately
Before running message
Enter your message here, that you want to be displayed in front of your users.
Notify user for
10 minute(s)
and then
Run action immediately
Allow user to save work
Allow user to cancel
Show confirmation message before running action
While running message
Enter your message here, that you want to be displayed in front of your users.
Post deployment behavior
Do nothing after action completes
Restart computer after action completes.
Shutdown computer after action completes.
On failure, retry
1
1 time(s)
and wait
1 hour(s)
between attempts
Wait until computer has rebooted
Reapply whenever it becomes relevant again
with a
1 hour(s)
wait between attempts
up to
3
time(s)

a. **Offer to user**: Enable this toggle to deploy the action as a BigFix "Offer".

> **Note:** An Offer allows end-users to choose and install software, patches, or other actions themselves through a self-service application, rather than having them automatically deployed by an administrator.

When you enable this toggle, set the following options:

- **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
- **Title** - Enter the title that identifies the offer to the user.
- **Category** - Enter the category that groups the offer in the self-service application.
- **Description** - Enter the text that explains what the offer does.

b. The **Behavior** tab has a number of toggle switches users can turn on or off. They are presented as an order of events from top to bottom. The sequence order is as follows:

i. Start download immediately - Some Fixlets can contain large files. This option allows users to control whether all applicable devices should begin downloading the Fixlet as soon as the deployment is created.

ii. **Before running message** - As a device may become unresponsive while a Fixlet is being deployed, this gives users the option to display a warning for an amount of time before the Fixlet is applied. This may also be useful if a restart is required, so end users can save work.

Enable the toggle and set the following options:

- Enter the message text to display to the user before the action runs.
- In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Run action immediately**).
- **Allow user to save work** - Select this checkbox to let the user save open work before the action runs.
- **Allow user to cancel** - Select this checkbox to let the user cancel the action.
- **Show confirmation message before running action** - Select this checkbox to prompt the user to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own (for example, *Are you sure you want to run this action now?*).

iii. **While running message** - As a device may be unresponsive while a Fixlet is being deployed, this allows users to write a message that will be displayed on the screen until the deployment is complete. Enable the toggle, and then enter the message text to display to the user.

iv. **Post deployment behavior** - Enable this toggle to control what happens on the device after the action completes. Select one of the following options:

- **Do nothing after action completes** - The device stays in its current state.
- **Restart computer after action completes** - The device restarts when the action finishes.
- **Shutdown computer after action completes** - The device shuts down when the action finishes.

If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:

- **Message title (required)** - Enter a short title (for example, *Shutdown now*).
- **Message text (required)** - Enter the message body that asks the user to save any unsaved work.
- In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Shutdown automatically** or **Restart automatically**).
- **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let the user cancel the shutdown or restart.

v. **On failure, retry** - Occasionally, deployments fail to complete successfully on a device. Should this occur, this allows users to determine if they would like BigFix to automatically try the deployment again. Enable the toggle, enter the number of retries, and then select one of the following options:

- **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.

vi. **Reapply whenever it becomes relevant again** - This option automatically reapplies a Fixlet if it becomes relevant again after the initial deployment. Enable the toggle, and then set the following options:

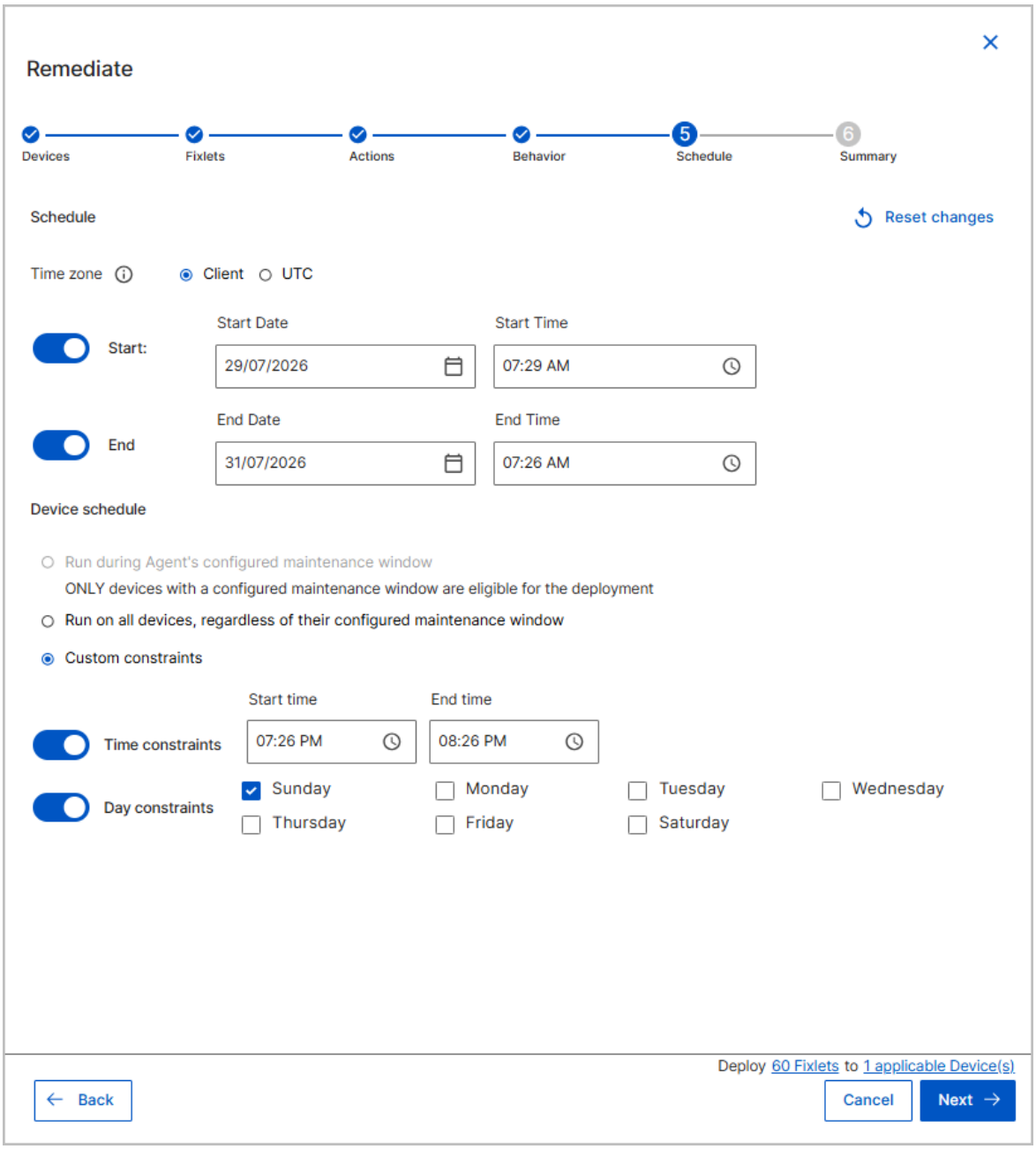
- **with a** - Select this checkbox and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **up to** - Select this checkbox and enter the maximum number of times (for example, **3**) that BigFix reapplies the Fixlet.

After selecting the desired sequence, click **Next** to proceed to the schedule tab.

5. **Schedule**: Configure start date and end date.

Determining a remediation start and end time gives BigFix users a tool to control their deployments. Typically, remediation do not happen immediately. Some devices may be powered down, or disconnected from the Internet, or otherwise unable to have the Fixlet applied. Scheduling allows to control how long BigFix will attempt this particular remediation.

There may be other reasons to control the end time. For example, an organization may wish to ensure that all deployments run overnight to minimize business impact.



- The schedule tab has two options: **Start Time** and **End Time**. In the first, select the calendar date and the start time when BigFix will begin attempting to apply the deployment. You may also select if you want to use client time (e.g., the time zone where the device is located) or UTC.
- In the second, select the calendar date and the start time when BigFix will stop attempting to apply the deployment. You may also select if you want to use client time (e.g., the time zone where the device is located) or UTC.

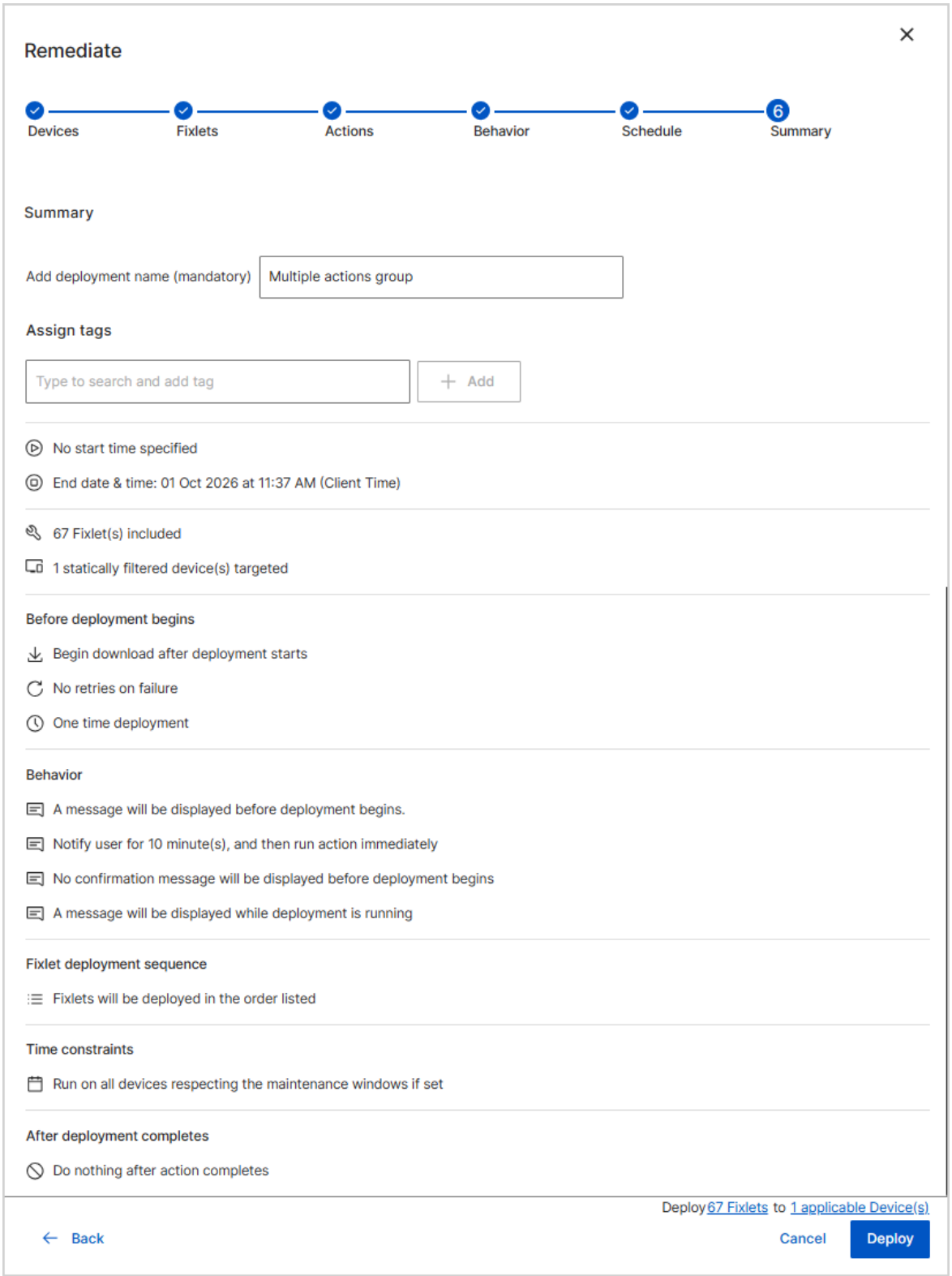
- If no scheduling option is selected, BigFix will begin the remediation immediately.
- **Run during agent's configured maintenance window**: Select this option, if you want to deploy the Fixlet during the set maintenance window *(on page 126)*.
- **Custom Constraints** - The Time Constraint option lets you control when a deployment can run by defining specific time ranges. This ensures Fixlets are applied only during the approved hours or maintenance periods.
    - Time Constraints: Specify the time range (for example, 11:00–23:00) when the deployment is allowed to execute.
    - Day Constraints: Optionally, choose one or more days of the week to further limit deployment (for example, only weekends or weekdays).

After selecting the desired schedule, click **Next** to proceed to the summary tab.

6. **Summary**: Shows all the configured remediation flow settings.
    - **Add deployment name (mandatory)** field is auto-populated with a default name that you can edit on the Summary step. Keep the default, or enter a unique, meaningful name that describes the purpose of the action.
    - In **Assign tags**, add one or more tags:
        - To add an existing tag, type to search for it, select it from the list, and then select **Add**.
        - To create a new tag, type the tag name, and then select **Add**.

      Assigned tags appear as chips below the field. To remove a tag, select the **X** on its chip. Tags are saved with the deployment and appear in the Deployment Manager and on the Deployment Details page; you can't change them after you deploy. For more information, see Managing Tags *(on page 51)*.
    - The Summary step also lists the deployment settings in read-only sections, such as the start and end date and time, the number of Fixlets included, the number of targeted devices, **Before deployment begins**, and **Behavior**.
    - The **Behavior** section confirms the message and notification options that you set on the Behavior step, for example:
        - A message will be displayed before deployment begins.
        - Notify user for 10 minute(s), and then run action immediately.
        - A confirmation message will be displayed before deployment begins.
        - No message will be displayed while deployment is running.

◦ Review the configurations and click **Deploy** to submit the action.



Result: The remediation flow is created and saved.

What to do next: Go to Deployments *(on page 181)* and you can see that the action is deployed. It also displays all the configured remediation flow settings. It shows the devices on which the deployment is being done, and the Fixlets that are deployed.

Related information

Managing Device Maintenance Windows *(on page 126)*

Deployments *(on page 181)*

Managing Tags *(on page 51)*

Managing Device Maintenance Windows

The Device Maintenance Window feature enables administrators to schedule specific time frames for executing actions on devices, ensuring controlled and predictable deployments, updates, and remediations. It supports daily, weekly, and monthly schedules with configurable time zones and execution conditions, minimizing disruptions while allowing flexibility for urgent remediations when needed.

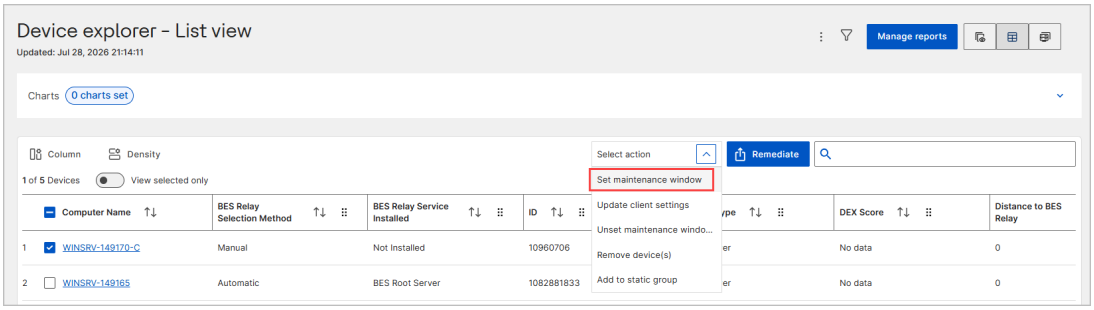
Key capabilities

- **Scheduled Execution**: Define **daily, weekly, or monthly** maintenance windows based on **client time, UTC, or a custom day** to ensure actions run only within designated periods.
- **Time-Based Validation**: Prevent actions from running outside the window unless explicitly configured, ensure accurate execution at the window's start, and handle invalid time entries.
- **Flexible Execution**: Allow scheduled actions to bypass the maintenance window when permitted and enable multiple actions to run simultaneously outside window constraints.
- **End-to-End Workflow Verification**: Validate full remediation behavior with and without maintenance windows, ensuring correct execution in all scenarios.
- **Integration**: Ensure proper application of maintenance window settings within **Fixlet Explorer**, **Fixlet Streams** , and **CyberFocus Remediation workflows**.

Accessing the maintenance window widget

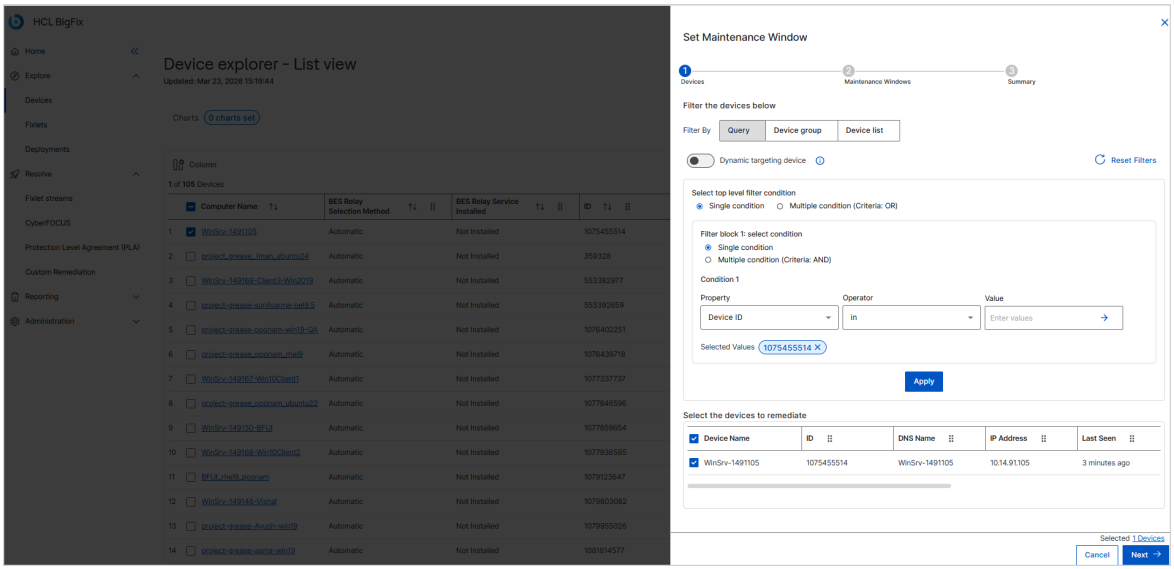
1. Log in to BigFix UI using your Admin credentials.
2. **Go to the Device Explorer Section**
    a. In the BigFix UI application, expand **Explore** from the side navigation, and then select **Devices**.
    b. Click the **List** icon to view the **Device explorer - List View**.

c. Select the devices that you want to target, the **Set maintenance window** becomes active.

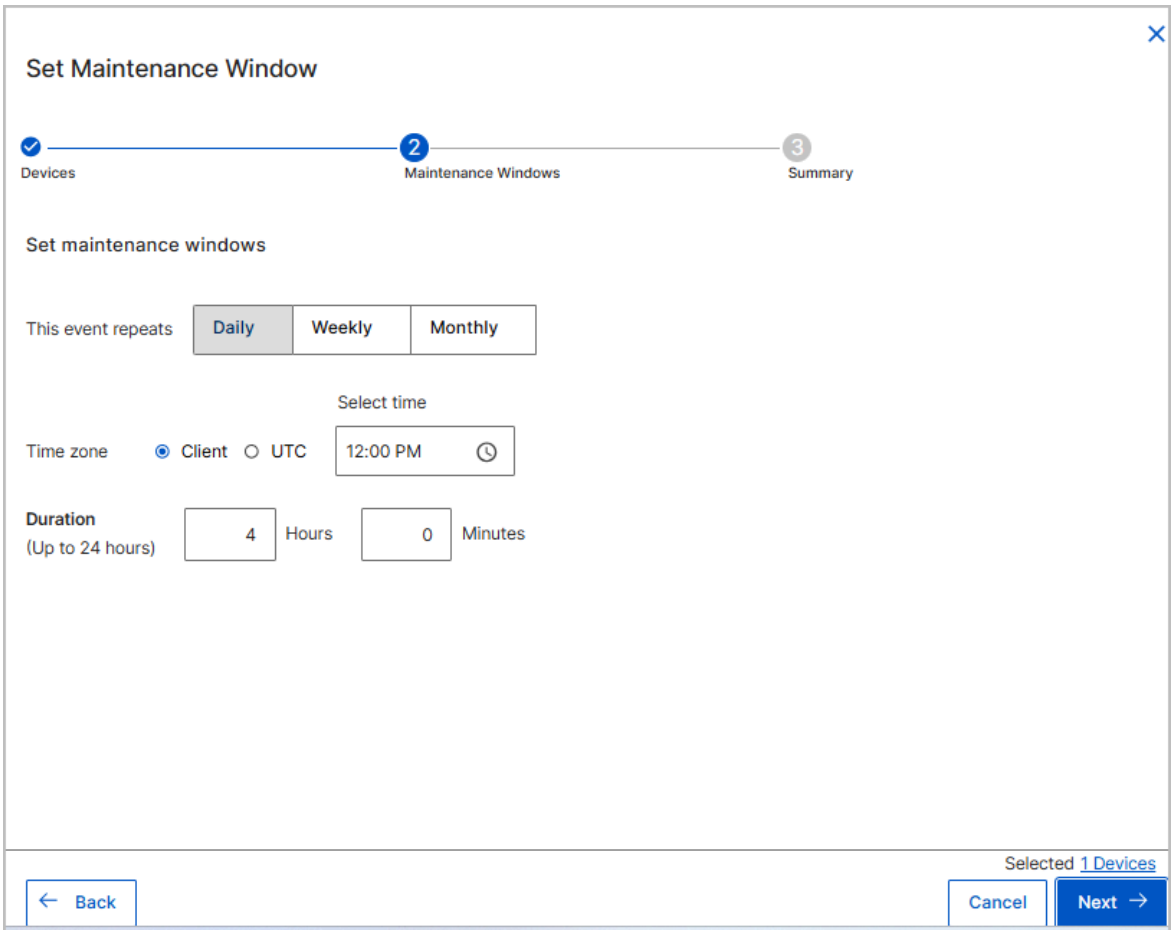


Setting up maintenance window

1. Click the **Select action** drop-down and select the **Set Maintenance Window** to open the widget.



2. **Devices**
    a. Review the selected devices.
    b. Use **Filter By** (**Query**, **Device group**, or **Device list**) to refine your selection.
        i. **Query**: Targets devices dynamically based on defined properties.
        ii. **Device group**: Targets members of existing static or dynamic groups.
        iii. **Device list**: Targets a manually entered, fixed list of devices.
    c. If using **Query**, the **Dynamic targeting device** toggle determines how the list of targeted devices is managed throughout the maintenance period:
        i. When the **Dynamic targeting device** toggle is enabled, the maintenance window uses dynamic filters to evaluate your environment continuously until the scheduled event ends.
        ii. When the **Dynamic targeting device** toggle is disabled, the system applies **static filters**, which define a fixed list of devices at the exact time of creation.
    d. Click **Next**.
3. **Maintenance Windows**



a. **Occurrence:** Choose if the event repeats **Daily**, **Weekly**, or **Monthly**.

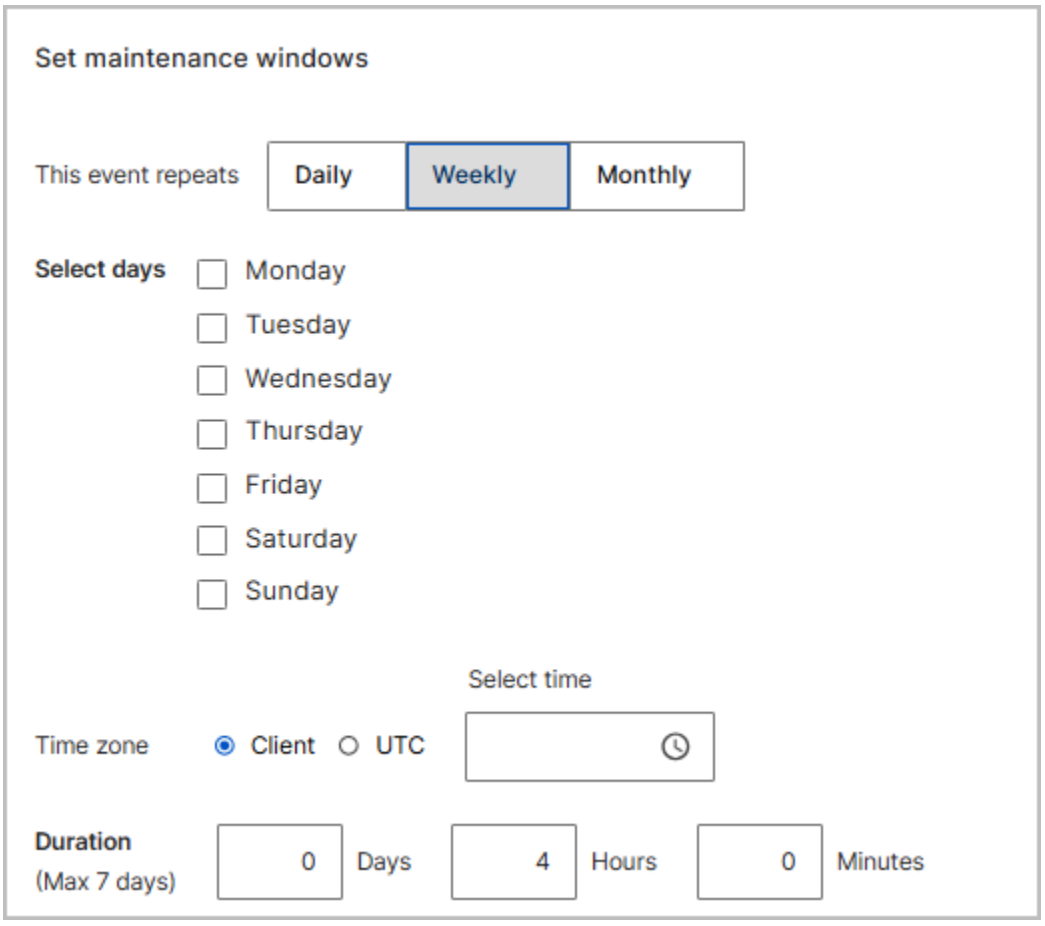
b. If you selected **Daily:** Proceed to select the time and duration.

- **Time zone:** Select **Client** (local endpoint time) or **UTC**.
- **Select time:** Set the window start time.

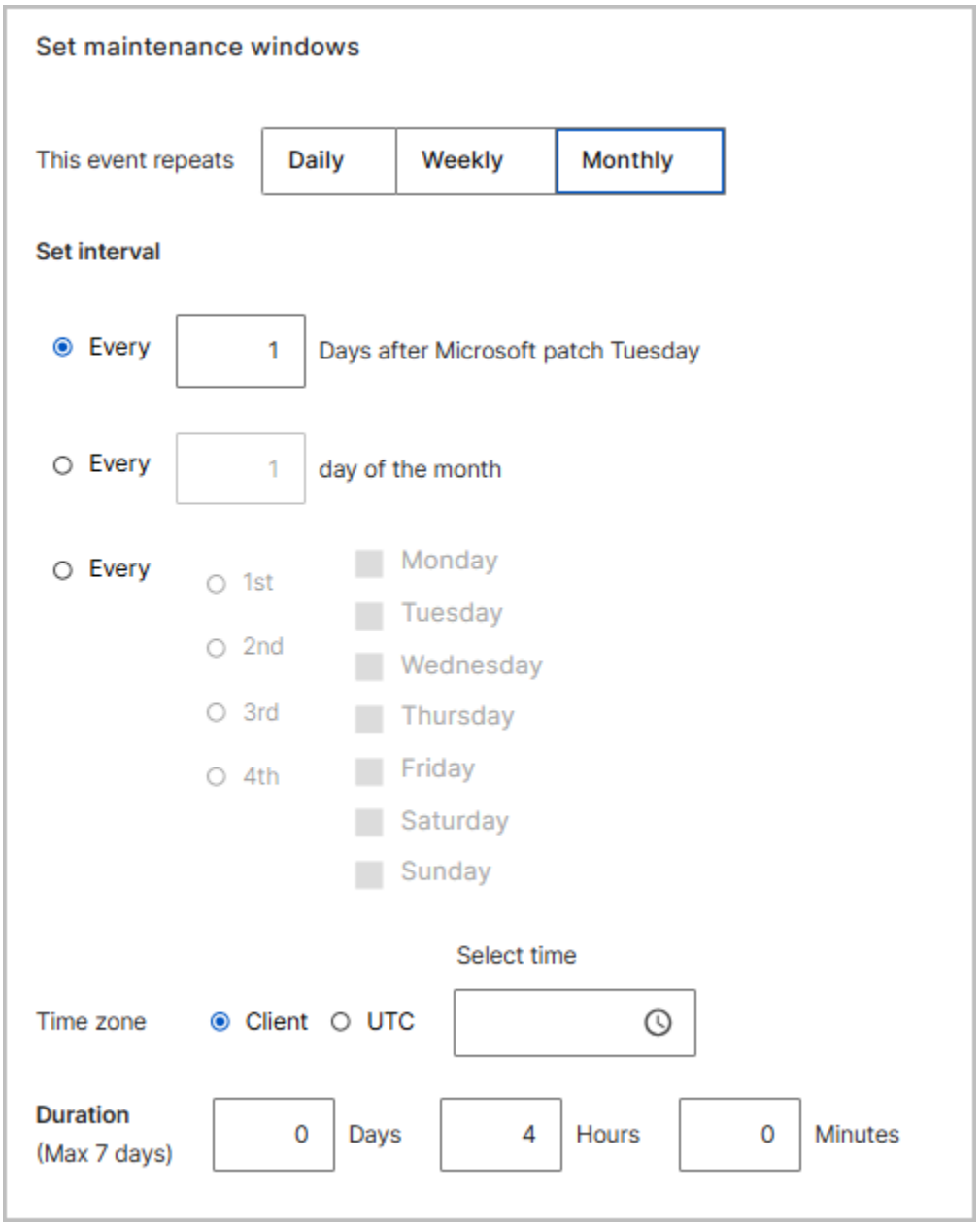
Tip: Click to set time.

- **Duration:** Define the window length in **Hours** and **Minutes** (up to 24 hours).

c. If you selected **Weekly:** In the **Select days** section, select the checkboxes corresponding to the days of the week you want the window to open (for example, Saturday and Sunday).



d. If you selected **Monthly:** In the **Set interval** section, select one of the following radio buttons to define the monthly pattern:



- **Every [X] Days after Microsoft patch Tuesday**: Type the number of days to delay the window after Patch Tuesday.
- **Every [X] day of the month**: Type the exact calendar date (for example, the 15th day of the month).
- **Every [1st / 2nd / 3rd / 4th]**: Select the week of the month, and then select the checkboxes for the specific days of the week (for example, Every 3rd Saturday).

e. In the **Time zone** section, select the time reference used to trigger the window:

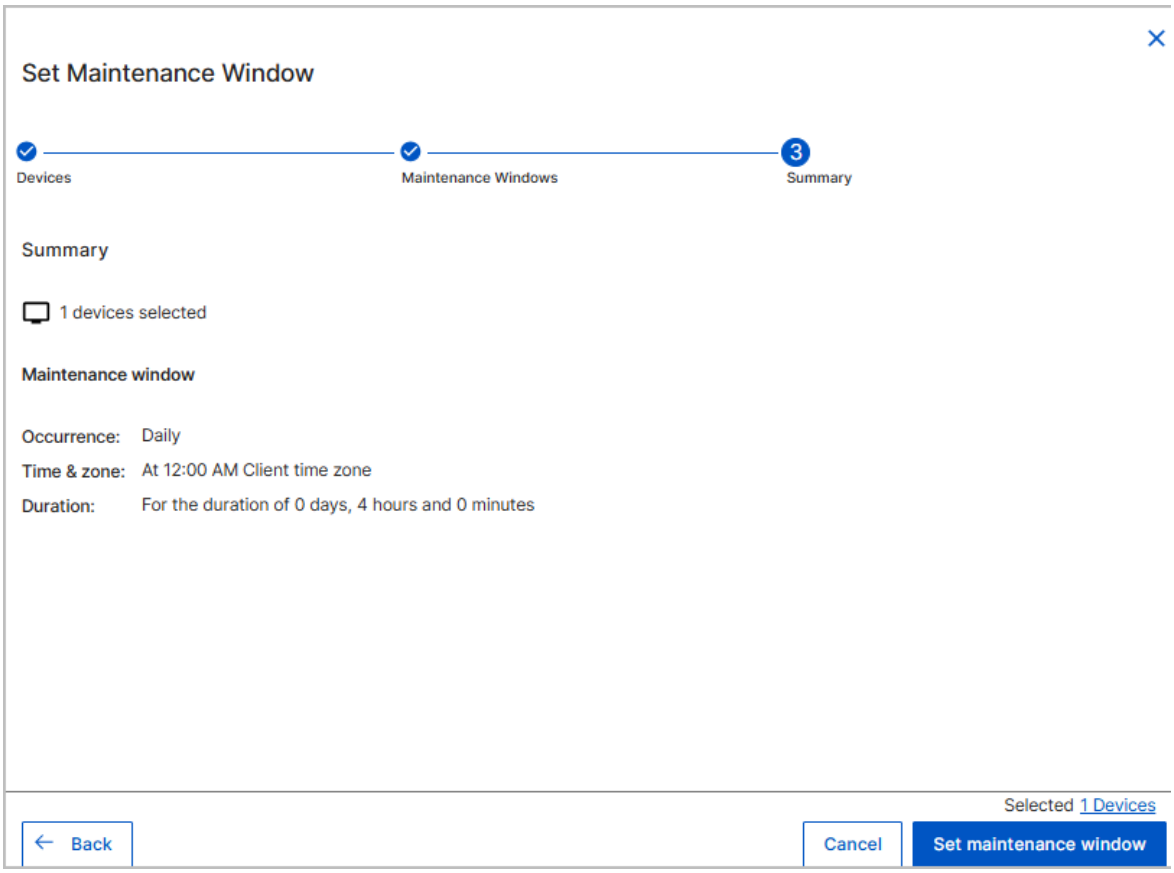
- Select **Client** to use the local time of the targeted endpoint.
- Select **UTC** to use Coordinated Universal Time for simultaneous global execution.

f. In the **Select time** field, click the clock icon to set the exact start time for the maintenance window.

g. In the **Duration (Max 7 days)** section, define how long the maintenance window remains open by typing values in the **Days**, **Hours**, and **Minutes** fields.

h. Click **Next** to proceed to the **Summary** step.

4. **Summary**



a. Review the occurrence, time zone, and duration configuration.

b. Verify the number of selected devices.

5. Click **Set maintenance window**. The maintenance window is successfully created.

6. **Execution Handling**:

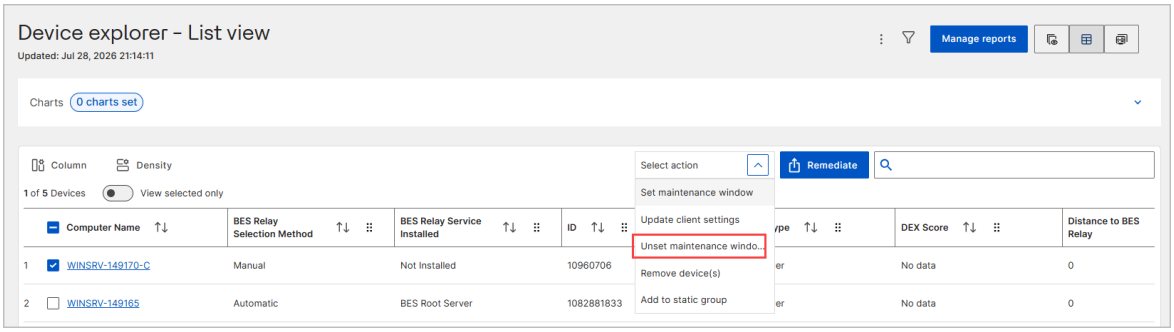
   - Updates and remediations occur within the scheduled window.
   - If a failure occurs, it retries in the next available window.

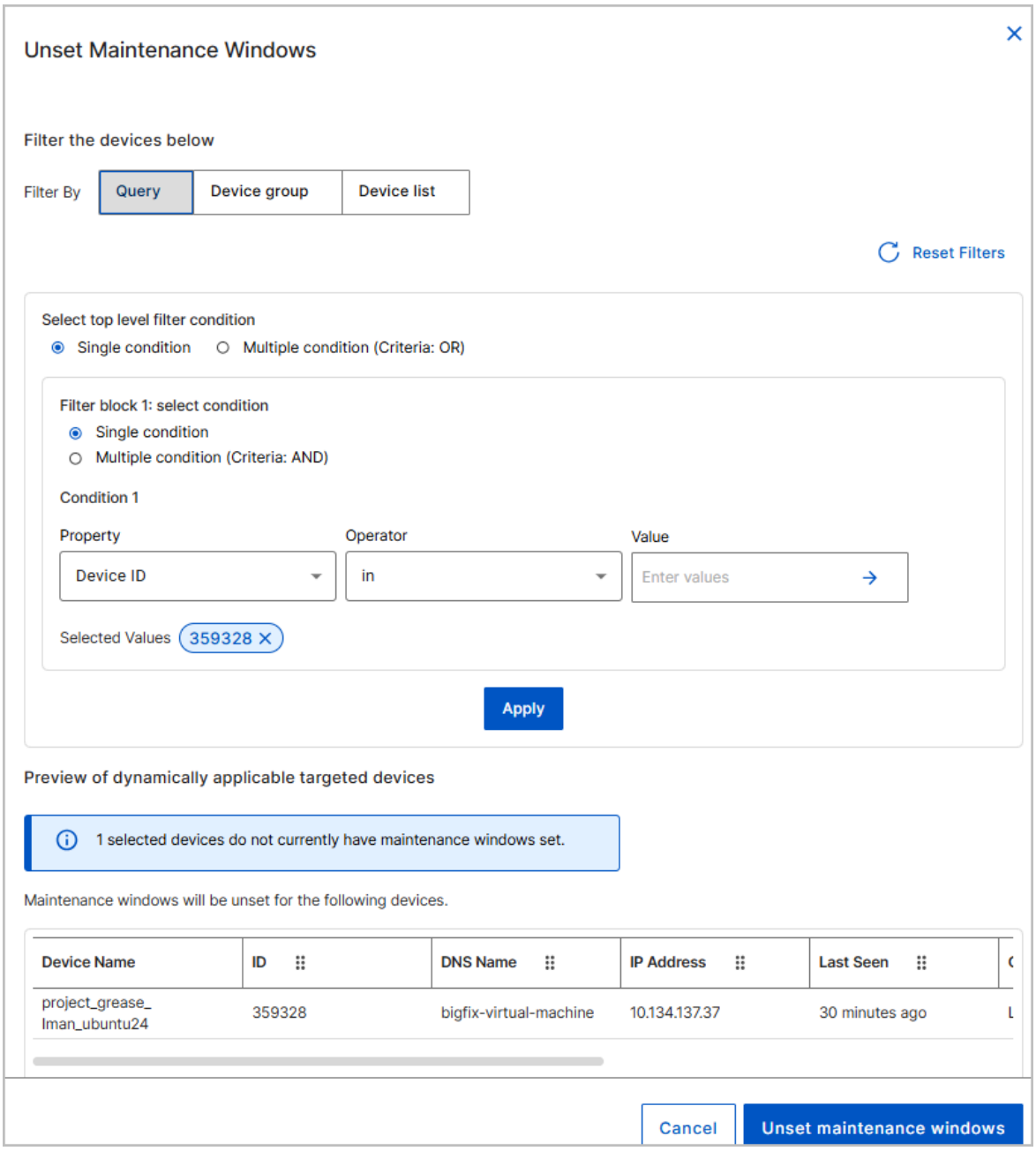
7. **Deployment Integration**:
    - While deploying Fixlet Streams *(on page 311)*, select **"Run during agent's configured maintenance window"**.
    - Verify execution status within the Deployments *(on page 181)*.
8. **Monitor and Modify as Needed**: Adjust schedules based on system needs.

Unsetting a Maintenance Window

Use this task to remove maintenance window configurations from targeted devices.

1. Navigate to **Explore > Devices** and click the **List**  icon to view the **Device explorer - List View**
2. Select the check box next to the devices from which you want to remove the maintenance window.
3. Click the **Select action** drop-down and choose **Unset maintenance window** to open the widget.





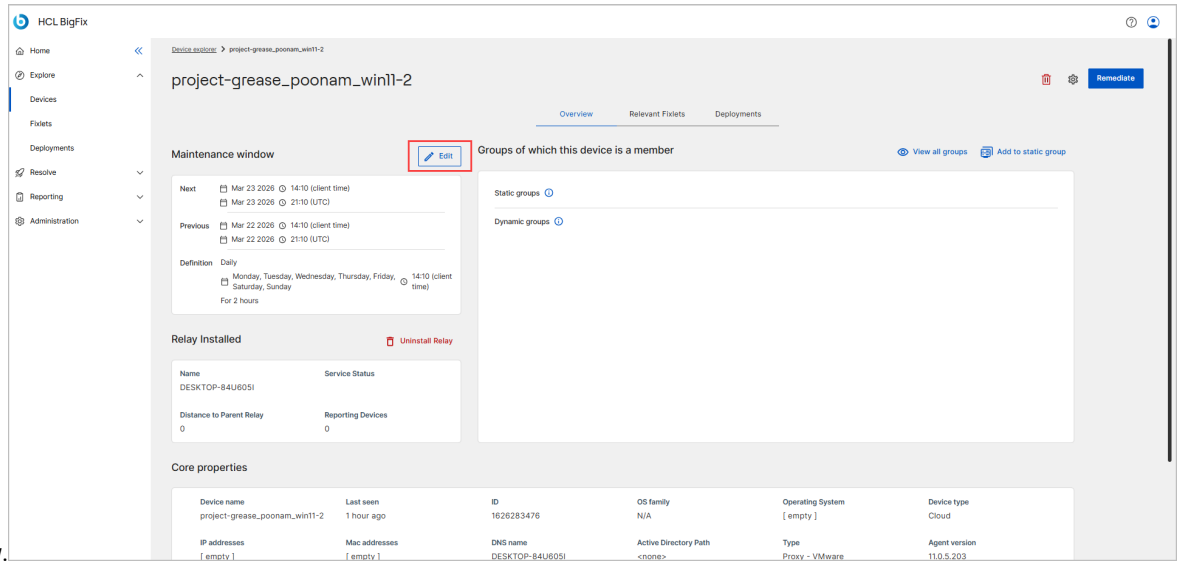
4. Verify the targeted devices in the list.
5. (Optional) Use **Filter By** (**Query**, **Device group**, or **Device list**) to target specific devices for unsetting.
6. Review the info message indicating which selected devices do not currently have a window set.
7. Review the list under "Maintenance windows will be unset for the following devices".
8. Click **Unset maintenance windows**.

   The maintenance window configuration is removed from the selected devices. These devices will no longer defer actions based on a maintenance schedule.

Editing maintenance window

To edit a maintenance window complete these steps:

1. From the list of devices in the Device Explorer, click on the device to which you want to edit the maintenance window.
2. If a maintenance window was previously set, the Maintenance windows section of the device details page displays the **Edit** button. Click the Edit button and make the necessary changes, and click **Set maintenance window**.



Integrations

- Fixlet Streams *(on page 311)*: Configure Fixlet deployments to run only within maintenance windows.
- CyberFOCUS *(on page 277)* Remediation: Align critical security updates within maintenance windows.
- Deployments *(on page 181)*: Monitor action execution and reschedule if needed.
- Fixlets *(on page 145)*: Identify and schedule Fixlets to run within defined maintenance windows for controlled and compliant deployments.

Next steps

- **Monitor and adjust maintenance windows** based on device availability and update requirements.
- **Explore integration with deployment workflows** for better automation.
- **Refer to the detailed configuration guide** for step-by-step instructions on defining maintenance windows.

Frequently Asked Questions

1. **What happens if a device is powered off during a maintenance window?**

If the device is offline, the action will retry in the next available maintenance window as long as the action is still open.

2. **Can I run actions outside the maintenance window?**

   Yes, if the **"Run during agent's configured maintenance window"** option is not selected, actions will execute immediately.

3. **Can I configure different maintenance windows for different devices?**

   Yes, you can apply maintenance windows to individual devices or groups of devices as needed.

4. **What happens if an update fails during the maintenance window?**

   The update will retry in the next scheduled maintenance window, provided the action is still open.

5. **How long does it take for a new maintenance window to take effect?**

   Once set, the maintenance window is applied after the server processes the action, which may take a few minutes.

Update Client Settings

The Update Client Settings feature in BigFix UI allows administrators to modify the configuration of BigFix Agents on one or more devices. This tool provides a streamlined way to manage relay selection methods and apply, edit, or delete custom configuration settings (client settings) directly from the Device Explorer.

Use this feature when you need to reconfigure a group of endpoints to use a specific secondary relay or when you need to deploy a custom configuration tag across multiple devices for reporting and filtering purposes.

Note:

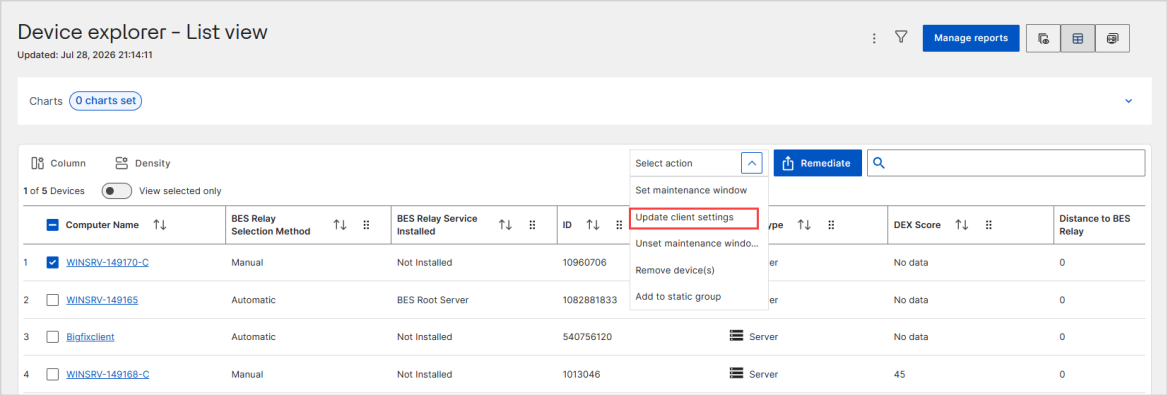
- Changes to client settings are persistent on the endpoint until explicitly modified or deleted.
- When using manual relay selection, you must specify a valid Primary and/or Secondary relay.
- Updating client settings creates a deployment action that can be monitored in the **Deployments** manager.

Key Capabilities

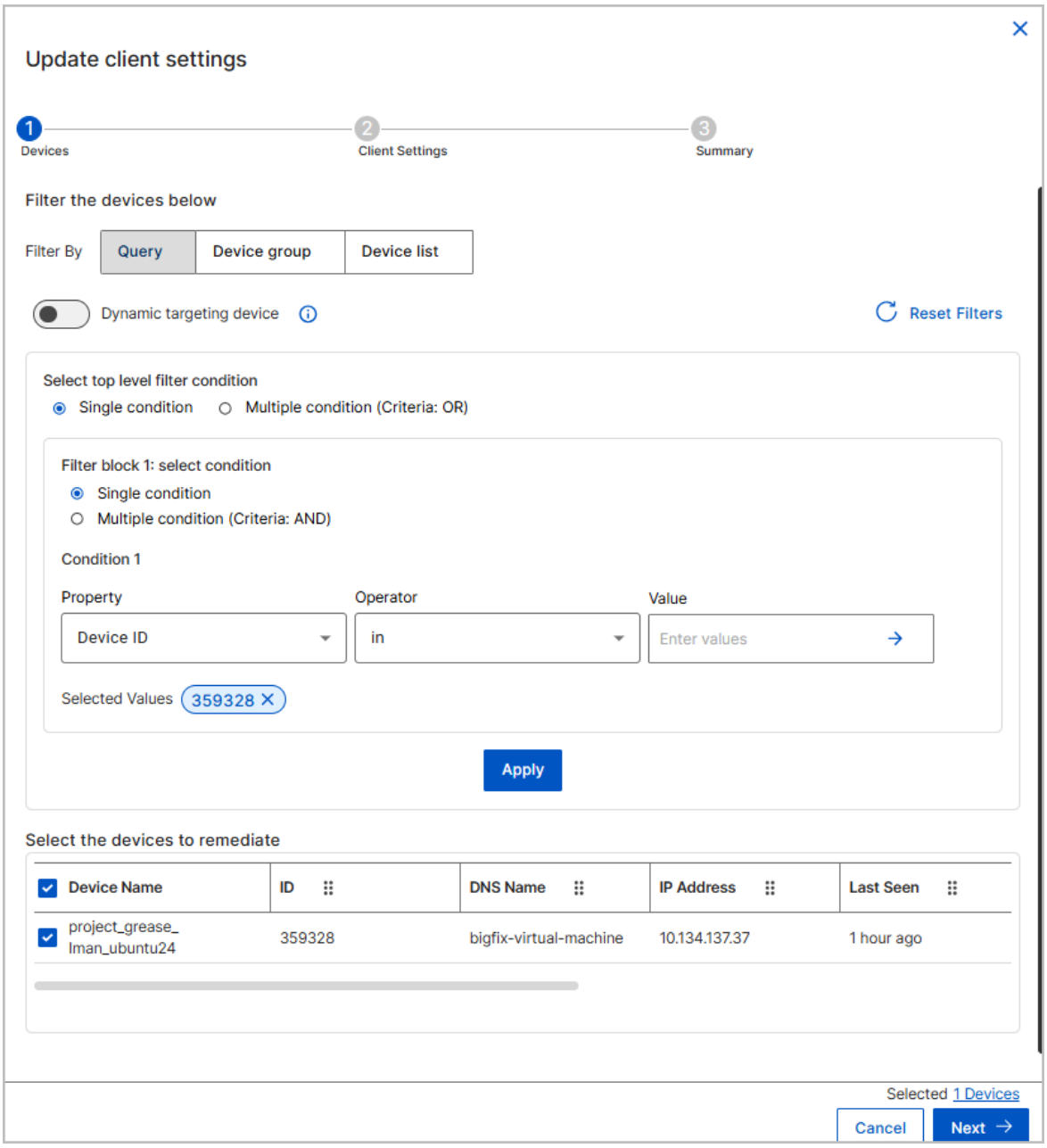
- **Relay Selection Management**: Switch between automatic, manual, or no change for relay selection methods.
- **Custom Settings Deployment**: Add new name-value pairs to configure specific agent behaviors.
- **Settings Modification**: Search for and edit existing client settings on targeted devices.
- **Bulk Deletion**: Identify and remove unnecessary client settings to maintain agent hygiene.
- **Flexible Targeting**: Target devices using specific queries, predefined device groups, or a fixed device list.

Updating Client Settings

1. Expand **Explore** from the side navigation and select **Devices**.
2. In the **Device explorer - List view**, select the checkbox for one or more devices.
3. Click the **Select action** dropdown and choose **Update client settings**.



4. On the **Devices** step, confirm your targets:
    - Use **Filter By** to refine the list by Query, Device group, or Device list.
        - **Query**: Targets devices dynamically based on defined properties.
        - **Device group**: Targets members of existing static or dynamic groups.
        - **Device list**: Targets a manually entered, fixed list of devices.
    - (Optional) Configure the **Dynamic targeting device** toggle based on your deployment need.
        - When the **Dynamic targeting device** toggle is enabled, it will define matching criteria that evaluate devices continuously until the deployment ends. Any device that matches the filter after the deployment is created will have the settings applied automatically.
        - When the **Dynamic targeting device** toggle is disabled, it will define a fixed list of devices at the time of deployment creation. This list remains unchanged for the duration of the deployment; new matching devices are not added, and devices that stop matching the filter will still apply the deployment.
    - Click **Next**.

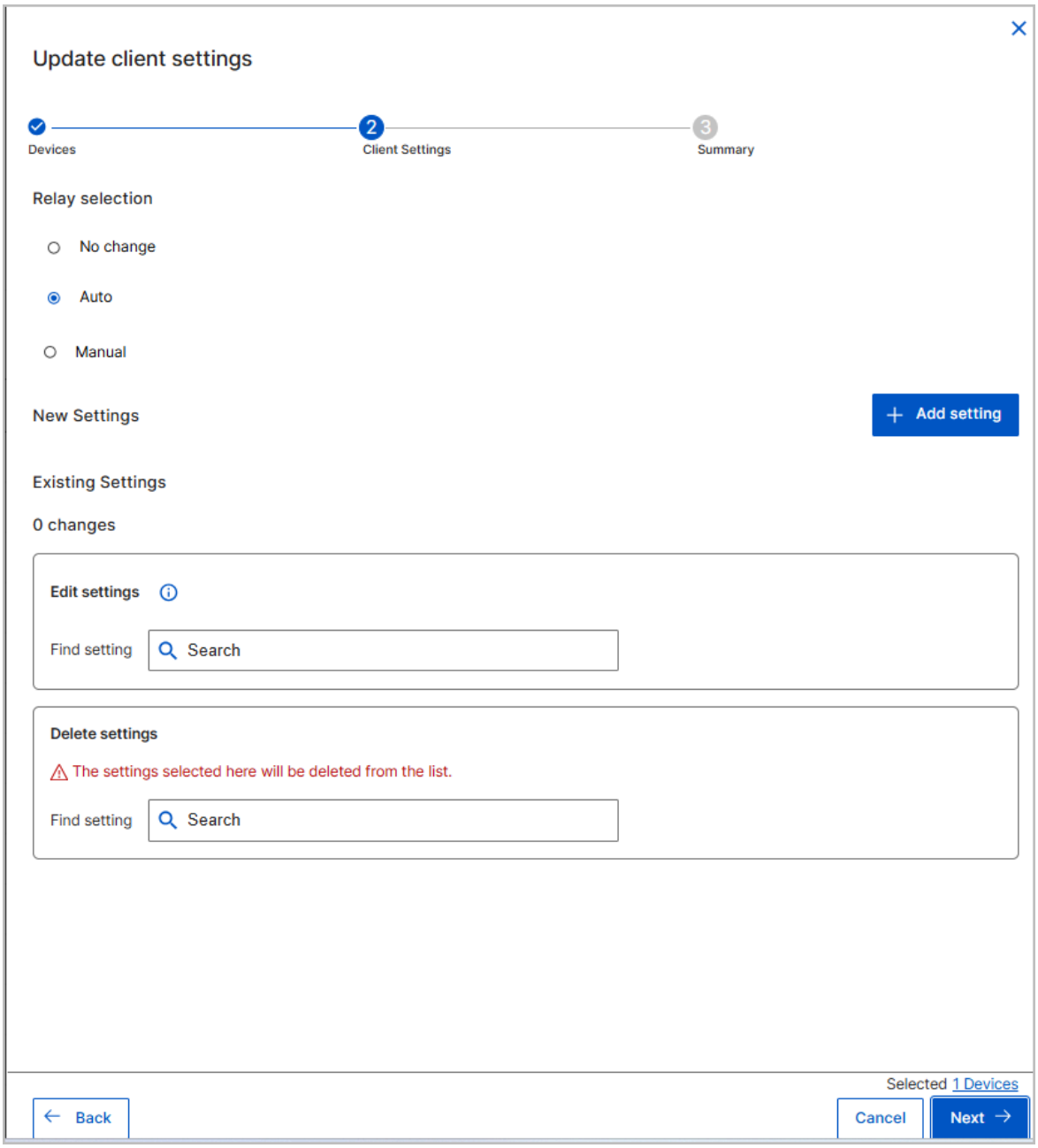


5. On the **Client Settings** step, configure the following:

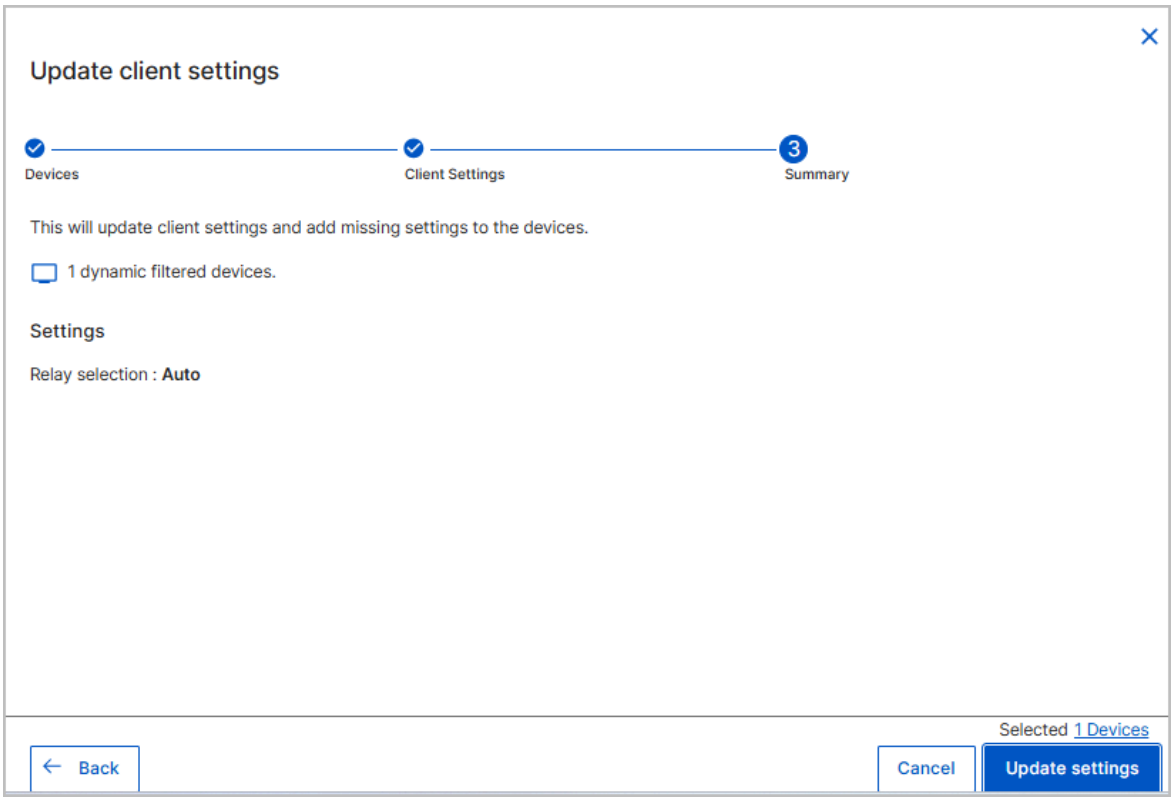
   - **Relay selection**: Select **No change**, **Auto**, or **Manual**. If Manual is selected, choose a Primary and/or Secondary relay from the dropdowns.
   - **New Settings**: Click **Add setting** to enter a **Name** and **Value** for a new configuration pair.

     Note: If user adds a settings name which already exists, an error message is shown below the text box.

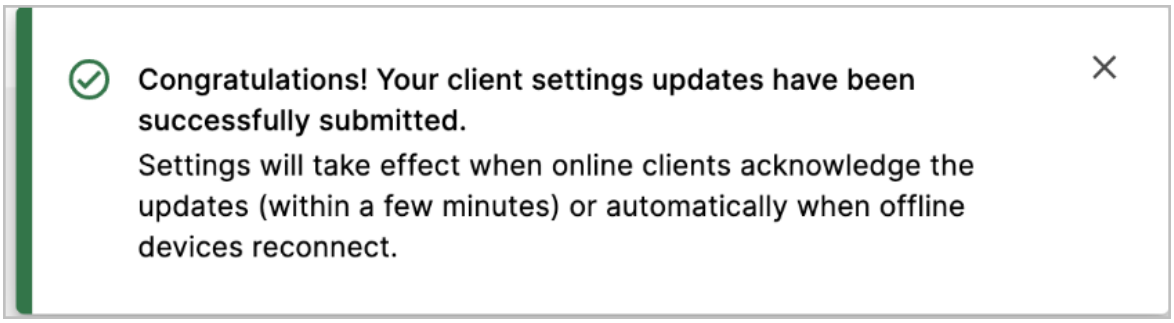
- **Existing Settings**: Use the **Edit settings** search bar to find and modify current settings, or use **Delete settings** to select properties for removal.
- Click **Next**.



6. On the **Summary** step, review your configurations and the number of targeted devices.



7. Click **Update settings** to submit the action. The confirmation will be shown as toast success notification on the main page.



Result

The client settings are sent to the targeted devices. You can monitor the progress of this task by navigating to the **Deployments** page.

Other Device Actions

The **Other Device Actions** dropdown on the Device Details page gives you additional ways to interact with a device without leaving the BigFix UI. Use it to start a remote control session or to send a notification message to the user of the device.

The **Other Device Actions** dropdown is in the top-right corner of the Device Details page, next to the **Settings** icon. Select **Other Device Actions** to display the available actions.

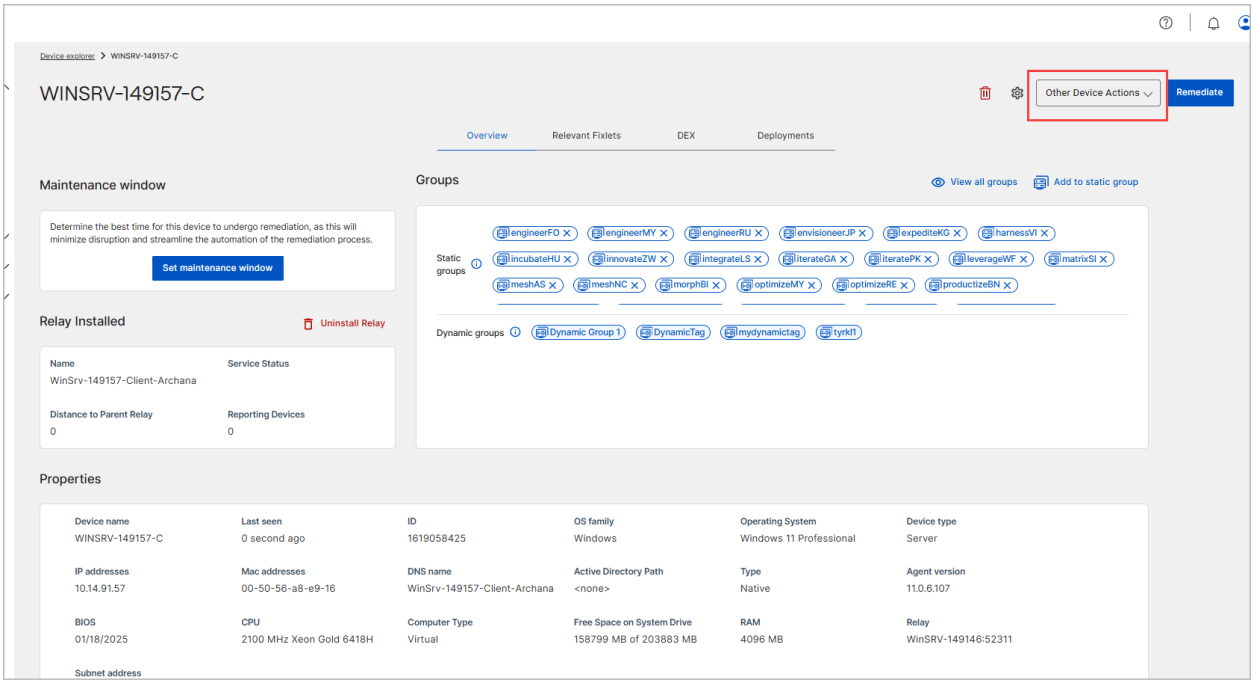


Table 18. Other Device Actions

Action	Description
Open Remote Control	Starts a web-based remote control session with the device. See Open Remote Control *(on page 140)*.
Send Message	Sends a notification message that appears to the user of the device. See Send Message *(on page 141)*.

Note: Each action appears in the dropdown only when the device is eligible for it and you have the required permissions. If a device isn't eligible for an action, or you don't have permission to run it, the action doesn't appear.

Open Remote Control

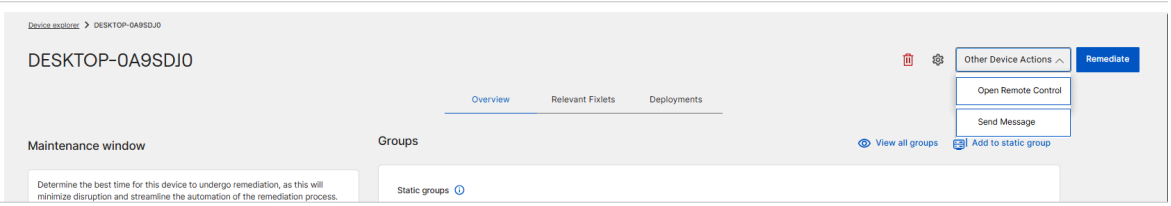
Use **Open Remote Control** to start a remote control session with the device directly from the Device Details page. This action opens the BigFix Remote Control Lite Web Portal in a new browser tab, where you can control the device without installing a standalone controller application.

Open Remote Control appears in the **Other Device Actions** dropdown only when the device is eligible for a remote control session. Eligibility depends on your BigFix environment being configured for Remote Control and on the device being a valid remote control target.

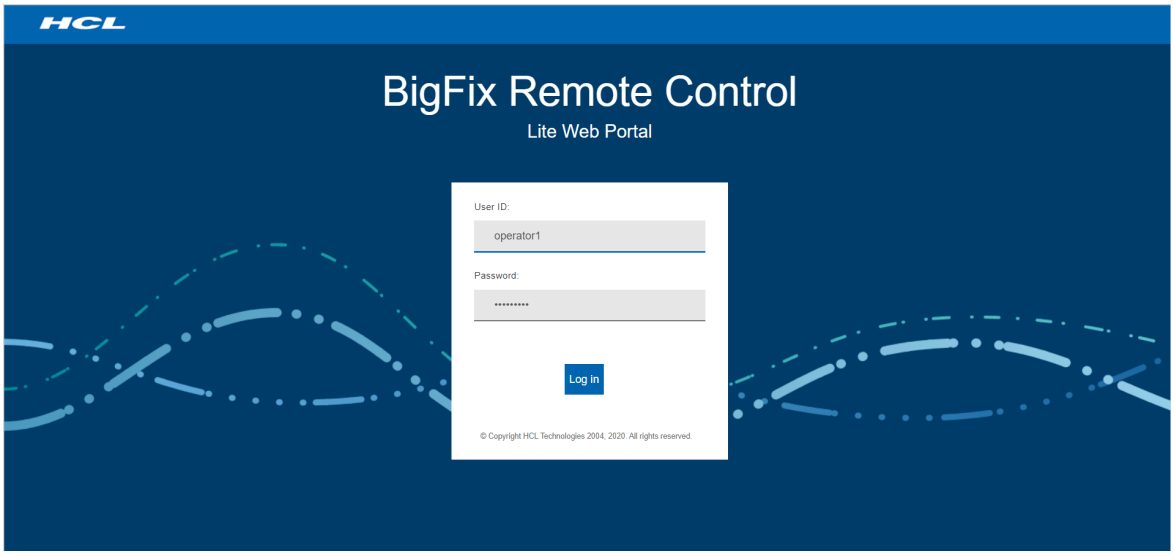
Important: Your Remote Control components (server, broker, and target) must be at version 10.1 FP6 or later. The BigFix Remote Control Lite Web Portal supports Microsoft Edge, Google Chrome, and Mozilla Firefox. Unless your BigFix UI and Remote Control server use single sign-on (SSO) with the same identity provider, you're prompted to sign in to Remote Control with your Remote Control credentials before the session starts.

To start a remote control session

1. Open the Device Details page for the device that you want to control.
2. In the top-right corner, select **Other Device Actions**.



3. Select **Open Remote Control**. The BigFix Remote Control Lite Web Portal opens in a new browser tab.



4. If you're prompted, sign in to Remote Control with your credentials. The remote control session starts for the selected device. For more information about the BigFix Remote Control Lite Web Portal, see Remote Control Lite user guide.

Send Message

Use **Send Message** to send a real-time notification that appears as a pop-up to the user of the device. Send a message to notify users about upcoming maintenance, or to communicate with them during support and troubleshooting, without switching to another tool.

Note: To send a message, you must have the **create custom content** and **create action** permissions in your BigFix environment. **Send Message** appears in the dropdown only when the device supports messaging.

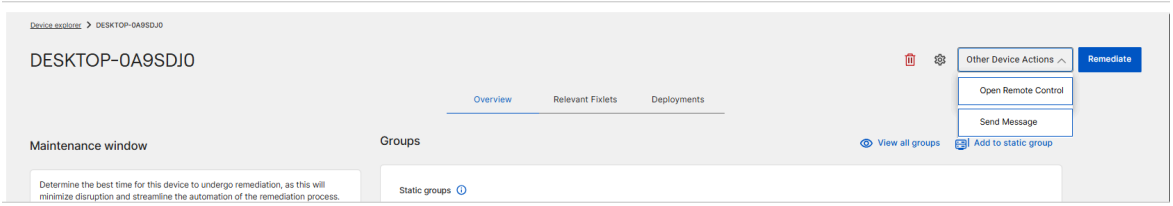
When you select **Send Message**, the **Send Message** dialog opens. The dialog notes that all fields are required and contains the following elements:

Table 19. Send Message dialog fields

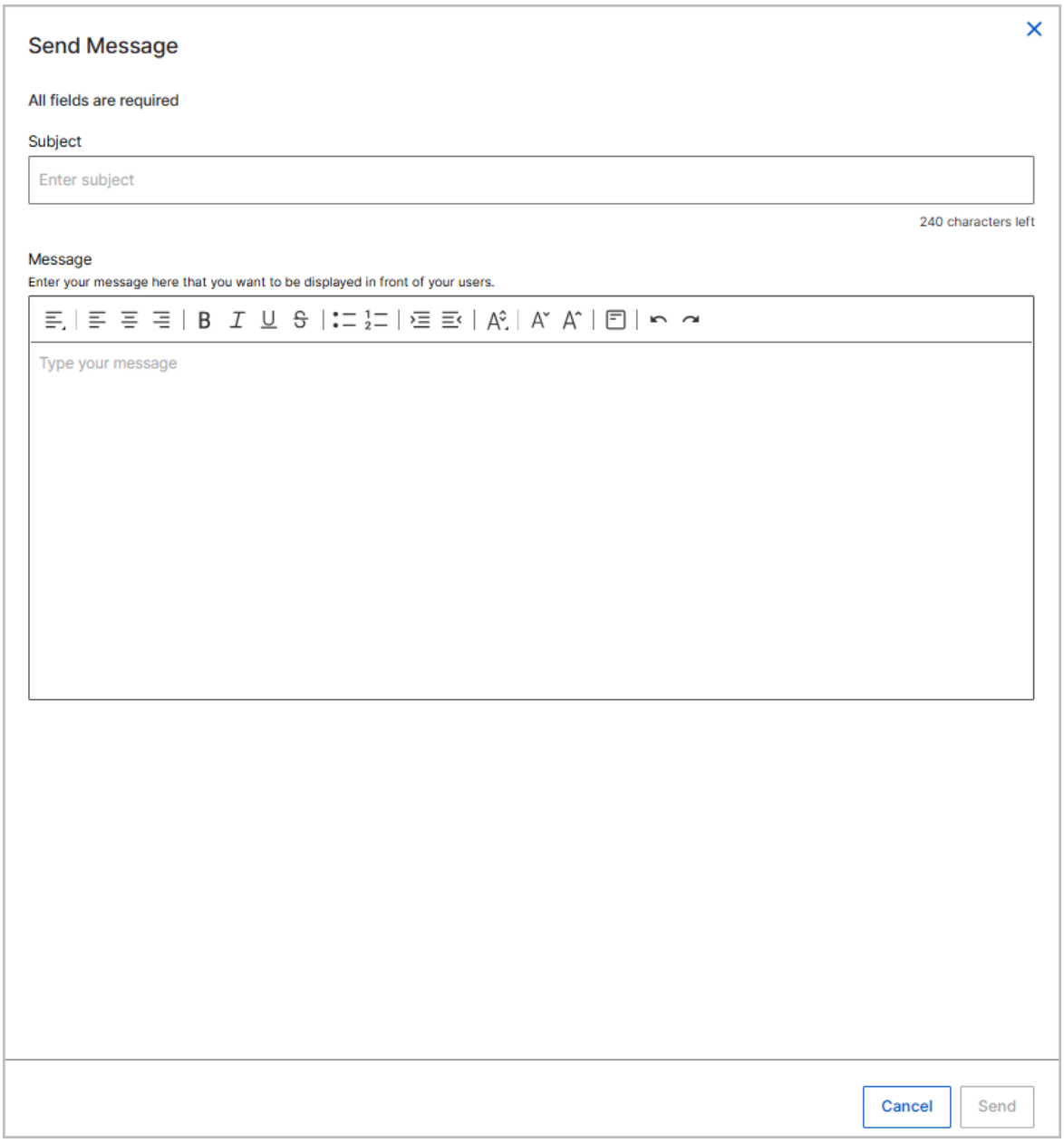
Field	Description
Subject	The title of the notification. Required. Enter up to 240 characters; the dialog shows the number of characters remaining.
Message	The text that appears to the user of the device. Required. Use the formatting toolbar to style the text, including alignment, bold, italic, underline, strikethrough, bulleted and numbered lists, indentation, font size, and undo or redo.
Send	Sends the message to the device. This button is enabled only after you complete both the **Subject** and **Message** fields.
Cancel	Closes the dialog without sending a message.

To send a message to a device

1. Open the Device Details page for the device that you want to send a message to.
2. In the top-right corner, select **Other Device Actions**, and then select **Send Message**.



The **Send Message** dialog opens.



3. In **Subject**, enter a title of up to 240 characters.
4. In **Message**, enter the text to display to the user. Use the formatting toolbar to style the text as needed.
5. Select **Send**. BigFix delivers the message as a pop-up notification on the device, and a confirmation indicates that the message was sent successfully.

Note: If the message can't be sent, BigFix reports the reason. For example, you might not have permission to run actions on the device, or the device might no longer be available. Confirm that you have the required permissions and that the device is still managed, and then try again.

Related information

Device Details Page *(on page 89)*

Delete devices

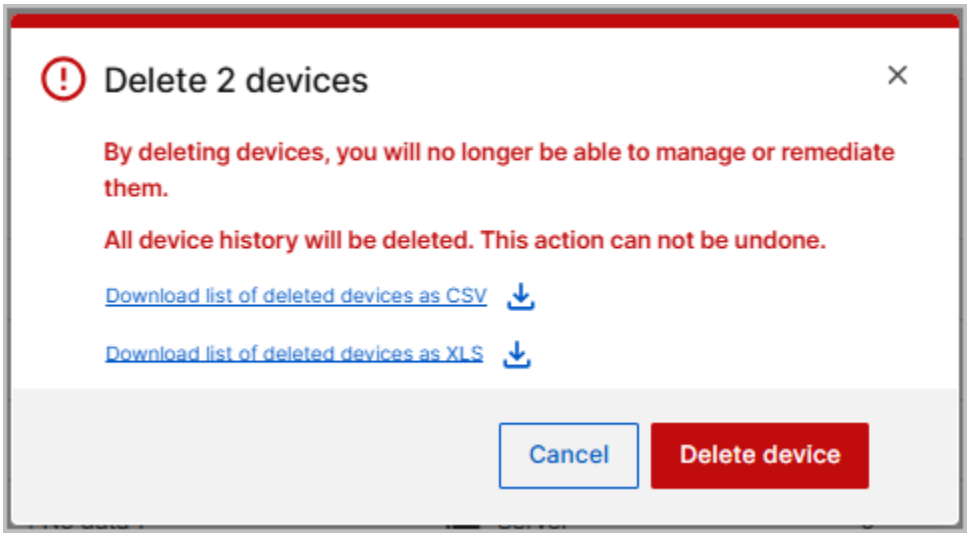
You can delete devices from BigFix using either the device list or the device details page. Deleting a device permanently removes it from management.

1. Delete devices from the device list:

- Open Devices and go to **Device Explorer – List view**.
- Select the check box next to one or more devices.
- Select **Select action** dropdown.
- Select **Delete device(s)**.

  In the confirmation dialog, review the warning message indicating that:

  - The device can no longer be managed or remediated.
  - The action cannot be undone.
  - Ensure to download the list of deleted devices before deleting it.

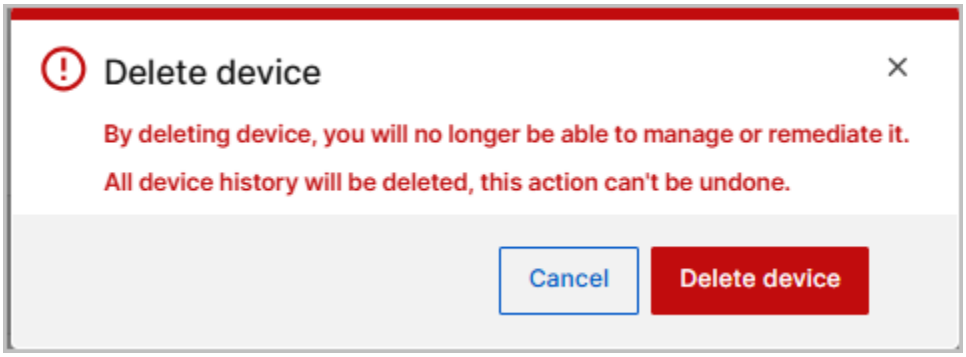


- In the confirmation dialog, select Delete device.

2. Delete a device from the device details page:

- In Device Explorer – List view, select a device name.
- On the device details page, select the Delete (trash) icon.

- In the confirmation dialog, select **Delete device**.



Note:

- Deleting devices is permanent and cannot be undone.
- Deleted devices can no longer be managed or remediated.

Fixlets

Fixlet Explorer enables users to view and manage Fixlets, which are sets of instructions for the BigFix agent to execute on devices. Users can filter and deploy Fixlets, access detailed information on CVEs, and navigate through a data table displaying relevant Fixlet details.

BigFix data is based upon Fixlets. A fixlet is a set of instructions that the BigFix agent executes on an enrolled or onboarded device. Examples include updating installed software, remediating particular CVEs, or removing malware. These are only a very small sample of BigFix's capabilities. BigFix customers benefit from end-to-end security, protection, monitoring, and management delivered through this out-of-the-box content.

Besides using out-of-the-box content, you can create your own custom Fixlets with your own detection rules and actions. For more information, see Managing custom Fixlets *(on page 160)*.

Fixlets are lines of code that contain instructions to perform a set of actions on relevant devices. A Fixlet will also define what those actions are and specify the criteria that determine whether those actions are relevant for a specific device.

After installation, BigFix agents continuously evaluate the relevance criteria on the enrolled device. They then determine whether a Fixlet is relevant to that device, e.g., whether it is relevant or not.

Before you begin

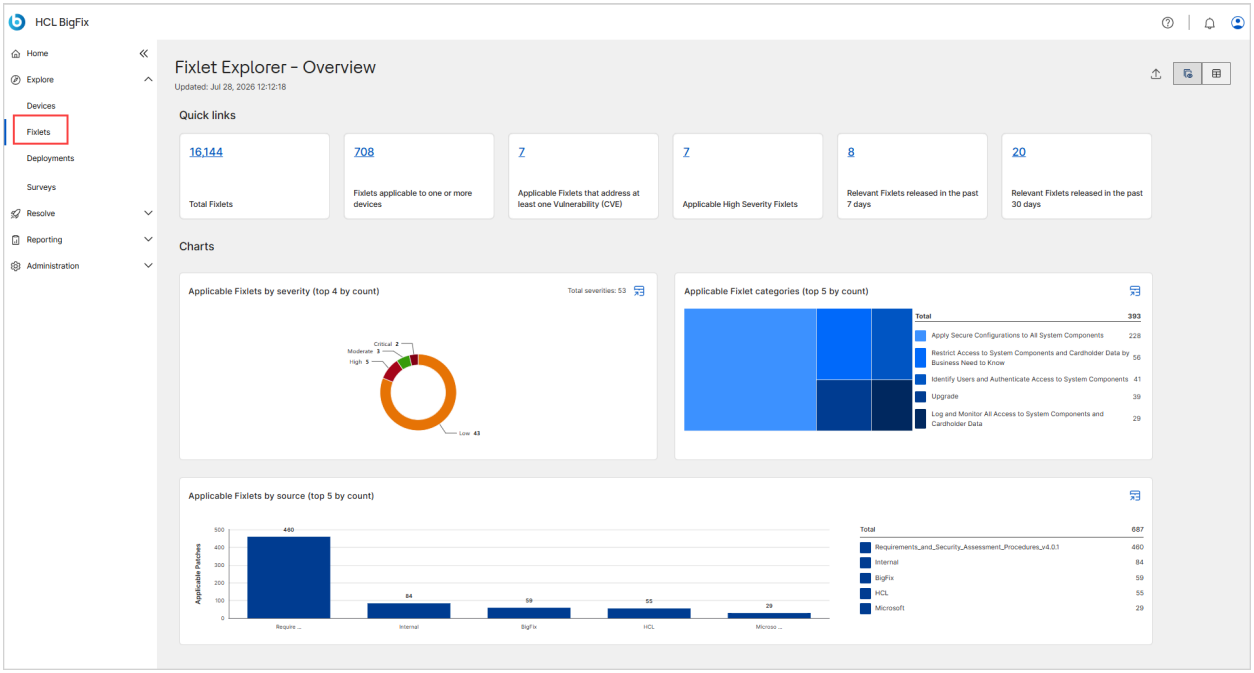
Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to this application. Fixlet Explorer is a default application, so every role has at least view access to it. See Managing Roles *(on page 467)*.
- Your role also defines the sites and devices that you can work with, which determines the Fixlets that you see. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete, such as deploying a Fixlet or creating custom content. For a description of each permission, see Permissions reference *(on page 482)*.

Fixlet Explorer – Overview

The Fixlet Explorer – Overview page provides a consolidated view of all Fixlets in your BigFix environment. At a glance, you can see the patch landscape through summary pallets and detailed charts. From here, you can also drill down into individual Fixlets, view their details, and deploy them directly.

To access the **Fixlet Explorer** app, expand **Explore** from the side navigation, and then select **Fixlets**.



The Overview page is organized into three main areas to help you manage your inventory:

View and utility bar:

Located at the top right, this bar contains Export report icon to manage the overall page. Also, you can toggle between the **List view** and **Chart view**.

Quick links:

The Quick links section presents key Fixlet counts as clickable tiles — total, applicable, CVE-related, high-severity, and recently released Fixlets — each linking to the matching filtered list.

- **Total Fixlets** – Displays the total number of Fixlets available in the environment.
- **Fixlets applicable to one or more devices** – Shows the number of Fixlets that apply to at least one device.
- **Applicable Fixlets that address at least one vulnerability (CVE)** – Displays the number of applicable Fixlets associated with one or more CVEs.
- **Applicable High Severity Fixlets** – Shows the number of applicable Fixlets with high severity.
- **Relevant Fixlets released in the past 7 days** – Displays recently released Fixlets from the last 7 days.
- **Relevant Fixlets released in the past 30 days** – Displays recently released Fixlets from the last 30 days.

Charts:

The Charts section gives visual summaries of applicable Fixlets — by severity, category, and source — and each chart can show its data as a table you can copy or export.

- **Applicable Fixlets by severity (top 4 by count)** – Shows applicable Fixlets grouped by severity levels such as Critical, High, Medium, and Low.
- **Applicable Fixlet categories (top 5 by count)** – Displays the top five Fixlet categories based on the number of applicable Fixlets.
- **Applicable Fixlets by source (top 5 by count)** – Shows the top Fixlet sources or vendors that contribute the most applicable Fixlets.



Note: Each chart has an icon in its top-right corner that opens the chart's data as a table, with options to copy or export it. For more information, see Viewing chart data in a table *(on page 33)*.

Fixlet Explorer – List View

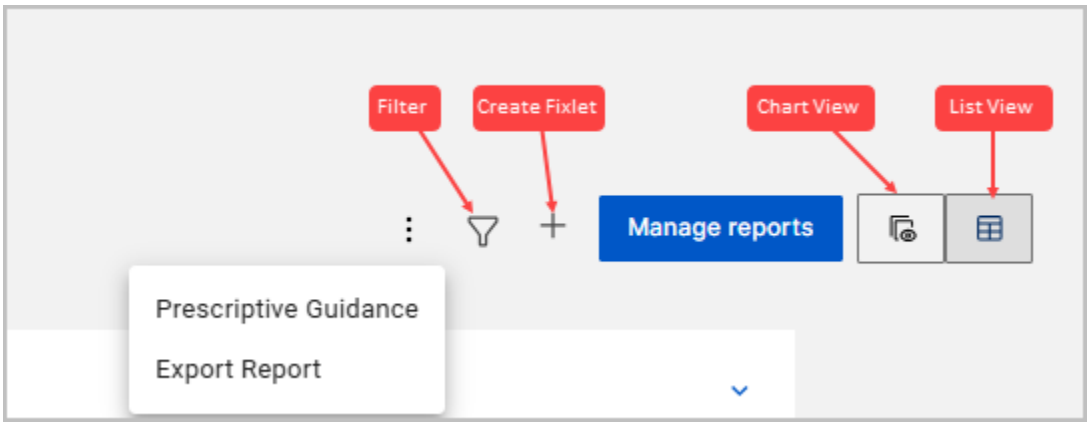
The **Fixlet Explorer – List View** page displays Fixlets in a tabular format, allowing you to review, filter, and manage Fixlets from a single location. This view is designed to help administrators quickly identify Fixlets, examine their properties, and create charts for visual analysis.

The page is organized into four main areas to help you manage your inventory:

- **View and utility bar:** Located at the top right, this bar contains Export report, Prescriptive Guidance, Filter, and Manage report tools to manage the overall page. Also, you can toggle between the **List view** and **Chart view**.
- **Charts section**: Use this collapsible area to create and view visual data summaries.
- **Device list table**: The table displays the available Fixlets in a customizable grid.
- **Command bar**: The **command bar** is located directly above the Fixlet list. It contains tools to act on selected Fixlets.

View and utility bar

Located at the top right of the **Fixlet explorer - List view** page, this bar contains buttons that manage the overall display and reporting features.



- **Prescriptive Guidance (three vertical dots)** provides actionable recommendations to users based on best practices, industry standards, and specific organizational policies. For detailed steps, see Prescriptive Guidance *(on page 55)*.
- **Export report (three vertical dots)**: this export data option used to download tabular report information from list view pages for offline analysis or record-keeping. For detailed steps to export report, see Common functionalities *(on page 28)*.
- The **Filter** icon brings up the filter sidebar. In this sidebar, users can narrow down the displayed Fixlets using a variety of parameters. You can also save a filter, mark it as a favourite, and apply it again later. For more information, see Global filter *(on page 36)*.
- **Create Fixlet**: Select the **Create Fixlet** icon (+ icon) to open the Create fixlet wizard and create a custom Fixlet. For more information, see Managing custom Fixlets *(on page 160)*.
- The **Manage Reports** feature allows users to save, load, and organize custom reports generated within the BigFix UI. For detailed steps, see Manage Reports *(on page 42)*.

Filter

The **Filter** icon (funnel) in the view and utility bar opens the global filter for the page. The global filter narrows the Fixlet table to the Fixlets that match the conditions you define, and it also drives the chart interactions described in Filtering Fixlets from a chart *(on page 153)*.

You can save the filters that you build, so that you can reuse them without defining the same conditions again. From the **Filter** panel, you can save a filter under a name of your choice, list your saved filters, mark the ones you use most as favourites, apply a saved filter to the current view, and delete the filters that you no longer need. Saved filters are private to your account, and the filters that you save here apply to Fixlets only.

For the steps to build, save, apply, and manage your filters, see Global filter *(on page 36)*.

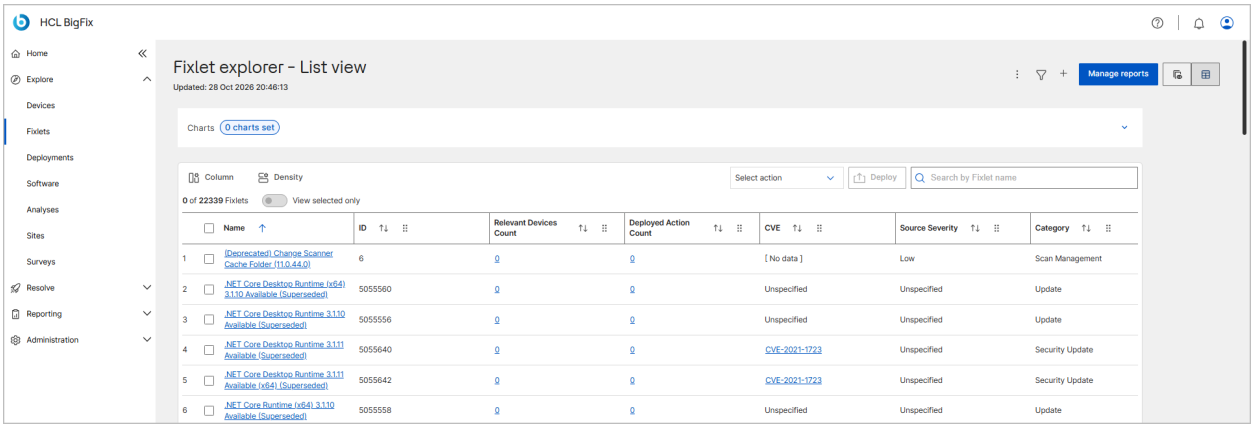
Charts

The collapsible **Charts** section creates visual summaries of Fixlet data. You can define charts based on properties such as **Source Severity**, **Category**, or **Source Release Date** to identify high-priority vulnerabilities at a glance. For the

steps to create a chart and to edit, delete, or export the charts you build, see Configuring and managing Fixlet charts *(on page 151)*.

Charts are interactive and work together with the **Global Filter** and the Fixlet table. For the steps to filter the Fixlet table from a chart, see Filtering Fixlets from a chart *(on page 153)*.

Fixlet List table



When accessing the Fixlet Explorer app, a data table with 100 Fixlets is displayed. Click **More** button to display more fixlets.

There can be thousands of Fixlets relevant to the devices associated with an account. The design focuses on filtering to enable customers to explore the Fixlets relevant to their account and specific associated devices.

Columns in the List View data table:

Table 20. Columns in the Fixlet Explorer – List View data table

Column	Description
Name	The title of the Fixlet. The name is a link; select it to open the Fixlet detail page. This is the primary column and is always shown.
Category	The classification of the Fixlet, such as Update, Security Update, or Configuration.
CVE	The Common Vulnerabilities and Exposures (CVE) identifiers associated with the Fixlet. Each CVE ID is a link to its vulnerability details.
Deployed Action Count	The number of deployed actions that originate from this Fixlet.
Download Size	The size of the patch or update file associated with the Fixlet.
ID	The unique numeric identifier assigned to the Fixlet.
Open Action Count	The number of currently open, active actions for this Fixlet.
Progress	The remediation progress for the Fixlet across its relevant devices.

Table 20. Columns in the Fixlet Explorer – List View data table (continued)

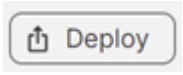
Column	Description
Relevant Devices Count	The number of devices for which the Fixlet is currently relevant.
Remediated Devices Count	The number of relevant devices on which the Fixlet has been successfully applied.
SANS	The SANS security classification associated with the Fixlet.
Site Name	The name of the site that provides the Fixlet.
Source	The origin or vendor of the Fixlet, such as Microsoft, HCL, or BigFix.
Source ID	The vendor-specific reference identifier for the Fixlet.
Source Release Date	The date the Fixlet was released by its source.
Source Severity	The severity level assigned by the source, such as Critical, Important, or Unspecified.
Tags	The tags assigned to the Fixlet. Shows the tag name when one tag is assigned, a count link (for example, *2 tags*) when more than one tag is assigned, or *No data* when no tag is assigned. Select a count link to open the tag drawer, where you can select one or more tags and remove them. After you remove tags, the drawer closes and the table refreshes automatically. For more information, see Managing Tags *(on page 51)*.
Type	The Fixlet type or content type.
Unlocked Devices Count	The number of unlocked devices among those relevant to the Fixlet.

Working with the Fixlet List Table

- The Fixlet Data table only shows a summary of the Fixlet. Click on the Fixlet name to bring up a more focused Fixlet detail page with additional details for the Fixlet. For more information, see Fixlet Explorer Details page *(on page 155)*.
- **Select Fixlets**: Select the checkbox next to a Fixlet name to prepare it for deployment. For more information, see Deploying Fixlets *(on page 167)*.
- **Sort fixlet list:** Each column in the fixlet list table includes a **Sort** icon (double arrows) that allows you to organize your data alphabetically or numerically. for more information, see Sorting Data *(on page 30)*.
- **Column:** Use the column chooser to choose which columns appear in the Fixlet list view and in what combination, showing up to 16 columns at a time. For more information, see Columns *(on page 29)*.
- **Density:** Use the density control to set the row spacing of the Fixlet list view — Compact, Standard, or Comfortable. For more information, see Density *(on page 29)*.

Working with Fixlet List table Command bar

The **command bar** is located directly above the Fixlet list. It contains tools to act on selected Fixlets:

- **Deploy**: Select this 

button to start the deployment process for the selected Fixlets. This button is disabled until you select at least one Fixlet. For users whose local administrators have not granted deployment rights, the Deploy button may remain permanently disabled.
    - The number of Fixlets that have been selected in the data table. The **Deploy** button brings up the deployment menu, which enables users to turn Fixlets into deployments that will be run on relevant devices. Users must select Fixlets by checking the box next to the Fixlet name in order to access the deployment menu. For detailed steps, see Deploying Fixlets *(on page 167)*.
- **Select action**: Choose a bulk action to run on the Fixlets that you selected. Select **Manage tags** to open the **Manage tags** drawer, where you choose or create the tags to apply. The drawer footer confirms how many Fixlets receive the tags, for example **4 Fixlets selected**. This list is unavailable until you select at least one Fixlet. When the assignment finishes, the drawer closes and the table reloads automatically. For the full procedure, see Assigning tags to Fixlets in bulk *(on page 53)*.
- **Search**: Enter keywords, such as a Fixlet name, ID, or CVE number, into the **Search** box to filter the list in real time.

Related information

Managing Filters *(on page 35)*

Manage Reports *(on page 42)*

Prescriptive Guidance *(on page 55)*

Common Functionalities *(on page 28)*

Fixlet Explorer Details page *(on page 155)*

Deploying Fixlets *(on page 167)*

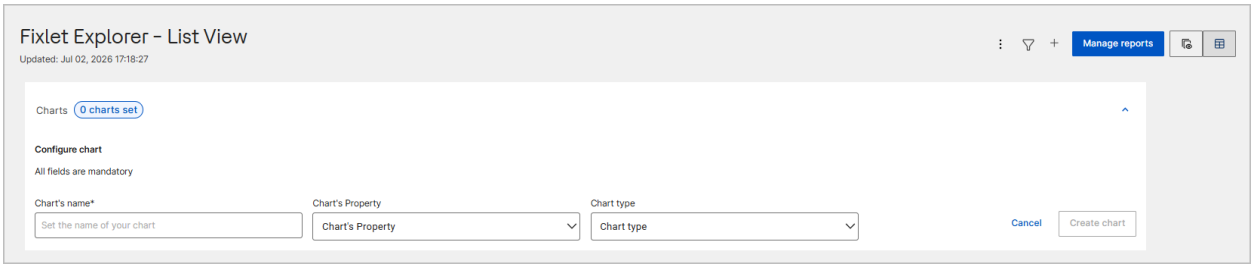
Managing custom Fixlets *(on page 160)*

Managing Tags *(on page 51)*

Configuring and managing Fixlet charts

Use the **Configure chart** pane on the Fixlet Explorer – List View page to build custom visualizations of Fixlet data. After you create a chart, you can edit it, delete it, view its data as a table, or hide the whole **Charts** section.

The collapsible **Charts** section on the Fixlet Explorer – List View page creates visual summaries of Fixlet data. Define charts based on properties such as **Source Severity**, **Category**, or **Source Release Date** to identify high-priority vulnerabilities at a glance.



1. In the **Charts** section, select **Add chart**.

   The **Configure chart** pane opens.

2. In **Chart Name**, enter a descriptive name for the chart.

   A clear name helps you identify the chart later.

3. From the **Chart's Property** dropdown, select the attribute to visualize, such as **CVE**, **Source Severity**, **Category**, or **Source Release Date**.

4. From the **Chart type** dropdown, select the visual format: **Horizontal chart**, **Vertical chart**, or **Pie chart**.

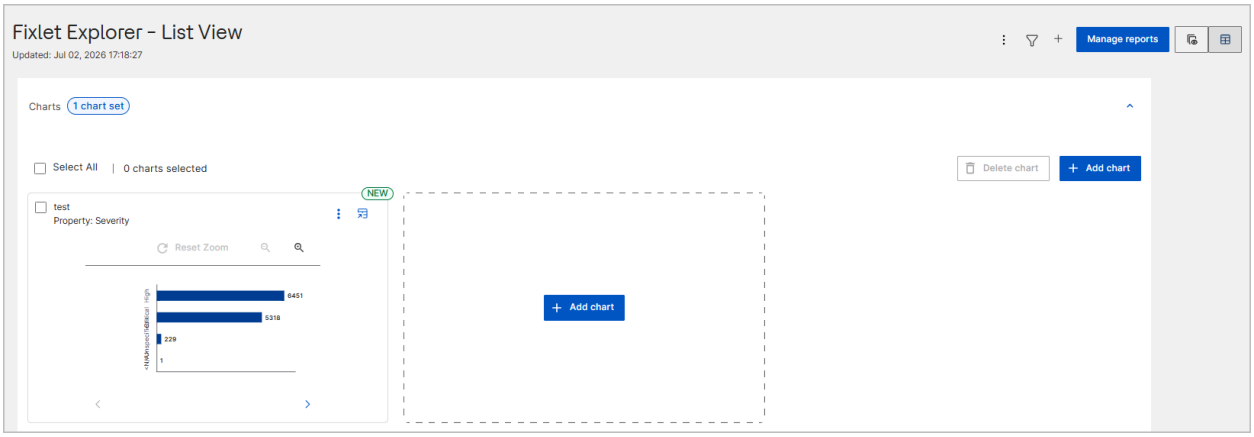
5. Select **Create chart**.

   This button stays dimmed until you provide information for all required fields. To close the pane without saving your changes, select **Cancel**.

   The new chart appears as a tile in the **Charts** section. A **NEW** badge marks a recently added chart, and each tile shows the chart name and the property it visualizes. If the selected property contains no data for the current list, the tile displays **No Data Available**.

The chart is available in the **Charts** section. Charts are interactive and work with the Fixlet table. For the steps to filter the Fixlet table from a chart, see Filtering Fixlets from a chart *(on page 153)*.

After you create a chart, you can modify or remove it from the display.



- To create more charts in the same view, select **Add chart**.
- To edit a chart, select the **More options** icon (three vertical dots) on the chart tile and then select **Edit** or **Delete**.
- To delete several charts, select the checkbox on the specific chart tile, or select **Select All** to choose all charts, and then select **Delete chart**.
- To view a chart's data as a table that you can copy or export, select the icon in the tile's top-right corner. For more information, see Viewing chart data in a table *(on page 33)*.
- To hide the **Charts** section, select the **Collapse** icon (upward arrow) in its top-right corner.

Related information

Fixlets *(on page 145)*

Filtering Fixlets from a chart *(on page 153)*

Common Functionalities *(on page 28)*

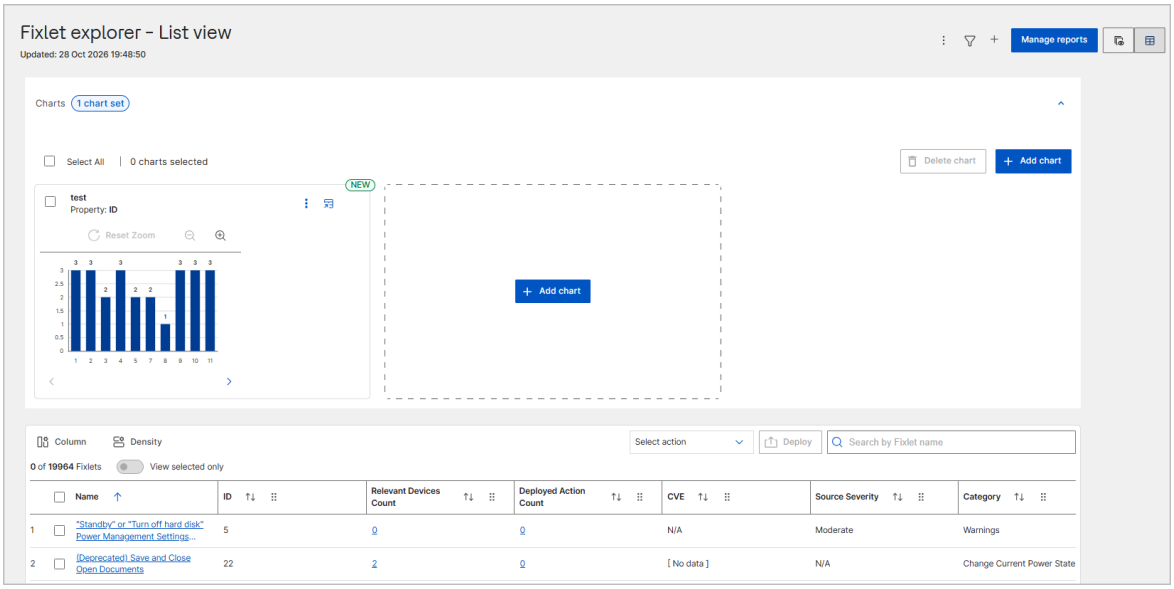
Filtering Fixlets from a chart

Charts on the Fixlet Explorer – List View page are interactive. Select a chart segment to filter the Fixlet table to the matching Fixlets, and clear the filter to return to the default view.

Charts on the Fixlet Explorer – List View page work together with the Fixlet table. When you select a chart segment, BigFix filters the Fixlet table to the matching Fixlets. When you clear the filter, the chart and the table return to their default views.

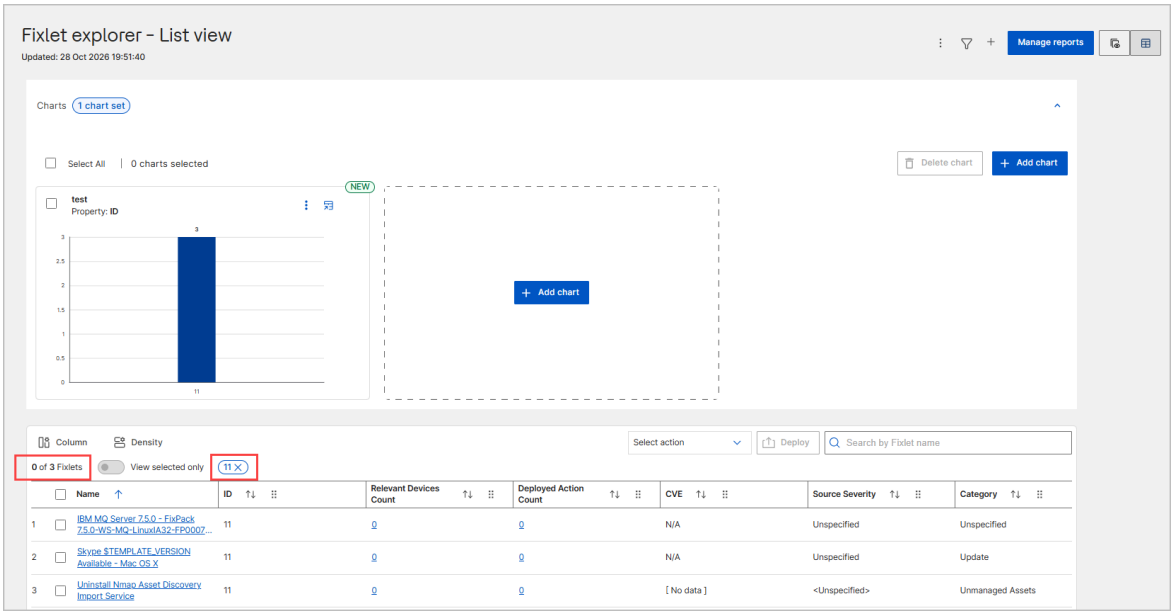
1. Create a chart from a Fixlet property, such as **Severity**.

   The chart appears as a tile that shows each value as a segment, for example High, Critical, and <Unspecified>, with its Fixlet count.



2. Select a segment, such as the **11** bar.

   The chart updates to show only the selected segment and hides the rest. For example, the count changes from **0 of 19964 fixlets** to **0 of 3 fixlets**.



3. To clear the selected segment, select the **x** in the chip above the Fixlet table.

   The chart returns to its default view and shows all segments, and the Fixlet table shows the complete, unfiltered list. For example, the count returns to **0 of 19964 fixlets**.

4. **Optional:** Manage the chart: edit it, delete it, add more charts, or hide the **Charts** section.

   For the steps, see Configuring and managing Fixlet charts *(on page 151)*.

Note: Use the zoom controls on a chart tile, **Reset Zoom**, zoom in, and zoom out, to adjust how much of the chart is visible. Zooming doesn't filter the table.

Note: To view the chart's values as a table that you can copy or export, select the **See data in data table format with download options** icon in the chart's top-right corner. For the steps, see Viewing chart data in a table *(on page 33)*.

Related information

Fixlets *(on page 145)*

Configuring and managing Fixlet charts *(on page 151)*

Managing Filters *(on page 35)*

Common Functionalities *(on page 28)*

Fixlet Explorer Details page

The Fixlet Explorer – Detail Page provides complete information about a selected Fixlet, including its metadata, tags, relevance expressions, actions, applicable devices, and related deployments.

Use this page to understand how a Fixlet works and where it applies. It helps you decide whether to deploy a Fixlet, explore its relevance script, or learn more about its origins.

To open the detail page, select a Fixlet name in the Fixlet Explorer – List View data table. The page opens with three tabs: **Overview**, **Relevant Devices**, and **Deployments**.

From the top-right corner of the Fixlet Explorer – Detail Page, you can deploy, edit, or delete the Fixlet. The **Edit** and **Delete** icons are enabled only for custom Fixlets that you created; they don't appear for out-of-the-box Fixlets.

- **Deploy**: Select **Deploy** to create a deployment for this Fixlet. The deployment wizard opens and guides you through the deployment steps. For more information, see Deploying Fixlets *(on page 167)*.
- **Edit** (custom Fixlets only): To change the Fixlet's details, detection rules, or actions:
  1. In the top-right corner, select the **Edit** icon. The Create fixlet wizard reopens with the Fixlet's current values.
  2. Update the values on the **Details**, **Detection rules**, or **Actions** steps as needed.
  3. On the **Summary** step, review your changes and save the Fixlet.

     For more information, see Managing custom Fixlets *(on page 160)*.

- **Delete** (custom Fixlets only): To remove the Fixlet:
  1. In the top-right corner, select the **Delete** icon. A confirmation dialog opens.
  2. Optional: To keep a copy before you remove it, select the link in the dialog to download the Fixlet's .bes file.
  3. Confirm the deletion. The Fixlet is removed from the Fixlet Explorer – List View table.

     For more information, see Managing custom Fixlets *(on page 160)*.

Overview tab

The **Overview** tab displays Fixlet-level details, including its properties, tags, relevance expressions, and actions. Use it to validate Fixlet logic, understand targeting rules, and preview execution scripts before you deploy.

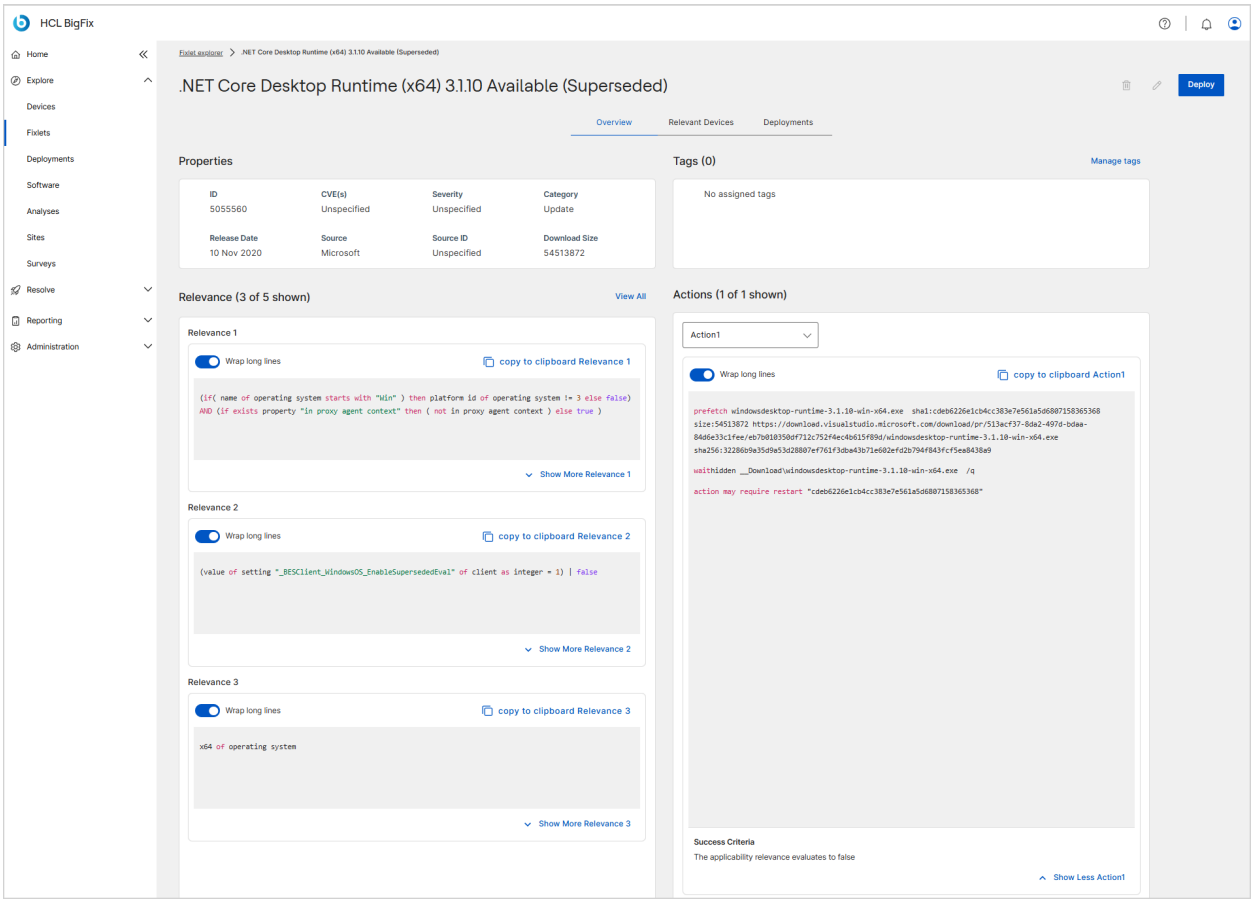


Table 21. Properties

Field	Description
ID	The unique identifier for the Fixlet.
CVE(s)	The Common Vulnerabilities and Exposures (CVE) identifiers linked to the Fixlet.

Table 21. Properties (continued)

Field	Description
Severity	The severity level assigned by the source, such as Critical, Moderate, or Unspecified.
Category	The type of Fixlet, such as Update, Security Advisory, or Scanner.
Release Date	The date the Fixlet was released by its source.
Source	The origin or vendor of the Fixlet, such as Microsoft or HCL.
Source ID	The vendor-specific reference number for the Fixlet.
Download Size	The size of the patch or update file associated with the Fixlet.

The **Tags** panel sits to the right of the **Properties** card and shows the tags assigned to the Fixlet. The heading includes the total, for example **Tags (2)**. When no tags are assigned, the heading shows **Tags (0)** and the panel displays **No assigned tags**.

- Each tag appears as a chip. The panel displays up to two rows of chips; when a Fixlet has more tags than fit, use **View all tags** to see the rest.
- Select **Manage tags** to open the **Manage tags** drawer and apply more tags to this Fixlet. You can select existing tags or create new ones. After you select **Save changes**, the drawer closes and the **Tags** panel refreshes to show the new tags.
- Select **View all tags** to open a drawer that lists every tag assigned to the Fixlet. Select the **X** on one or more tag chips, and then select **Save changes**. The drawer closes, and the **Tags** panel and its count refresh immediately.

Removing a tag from this Fixlet doesn't delete the tag or affect any other object that uses it. For more information, see Managing Tags *(on page 51)*.

- The **Relevance** section shows the relevance expressions that determine whether the Fixlet applies to a device. The header shows how many expressions are displayed, such as **Relevance (3 of 5 shown)**; select **View All** to see every expression. Each expression appears in its own numbered block, such as **Relevance 1**.

- The **Actions** section shows the commands the Fixlet runs on relevant devices. The header shows how many actions are displayed, such as **Actions (1 of 1 shown)**. Select an action from the dropdown list, such as **Action1**, to view its script.
- **Success Criteria** appears below the action script and states the condition that determines when the action is complete, for example **The applicability relevance evaluates to false**.

Each relevance and action block provides the following controls:

Table 22. Relevance and action controls

Control	Description
Wrap long lines	Turn on this toggle to wrap long expressions or scripts in the code viewer.
copy to clipboard	Copies the relevance expression or action script to the clipboard. The control names the block it belongs to, such as **copy to clipboard Relevance 1** or **copy to clipboard Action1**.
Show More / Show Less	Expands or collapses the full code block. The control names the block it belongs to, such as **Show More Relevance 1** or **Show Less Action1**.

Fixlet descriptions in BigFix UI

Descriptions are not displayed: BigFix UI does not display Fixlet descriptions when you explore or deploy Fixlets. You can view the description only when you edit a custom Fixlet.

Description input is not available: Because descriptions are not displayed during deployment, you cannot enter values in input fields that are part of a Fixlet description. To deploy a Fixlet that requires this input, use the **BigFix Console**. For more information, see Known limitations *(on page 7)*.

Relevant Devices tab

The **Relevant Devices** tab lists the devices where the selected Fixlet is currently applicable, so you can confirm coverage across your network. Use **Filter**, **Density**, and the **Search** box to refine the list, select a column header to sort, and select **More** to load additional rows.

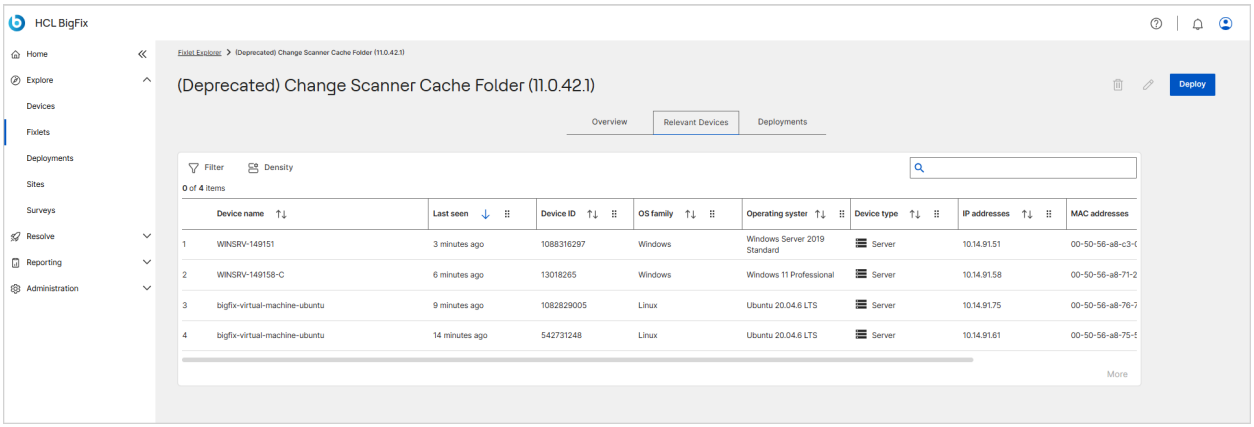


Table 23. Relevant Devices columns

Field	Description
Device name	The host name of the device.
Last seen	The time of the most recent contact received from the device.
Device ID	The unique BigFix-assigned computer identifier.

Table 23. Relevant Devices columns (continued)

Field	Description
OS family	The operating system family, such as Windows or Linux.
Operating system	The specific operating system version installed.
Device type	The device classification, such as Server or Workstation.
IP addresses	The IP address or addresses of the device.
MAC addresses	The hardware MAC address or addresses of the device.
DNS name	The registered DNS name of the device.

Deployments tab

The **Deployments** tab lists all deployments in which the Fixlet has run, giving you a complete history for auditing and tracking remediation progress. Use **Filter**, **Density**, and the **Search** box to refine the list, select a column header to sort, and select **More** to load additional rows.

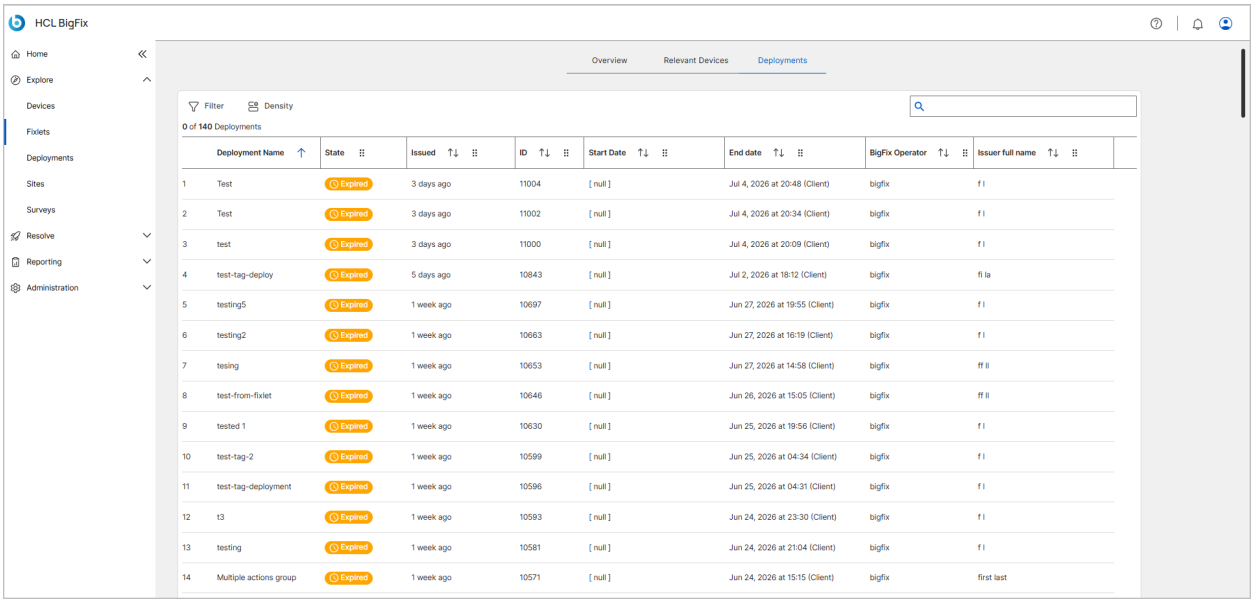


Table 24. Deployments columns

Field	Description
Deployment Name	The name of the deployment.
State	The current state of the deployment, such as Active, Expired, or Stopped.
Issued	When the deployment action was issued.
ID	The unique identifier of the deployment.

Table 24. Deployments columns (continued)

Field	Description
Start Date	The date and time when the deployment started.
End date	The date and time when the deployment ended or is scheduled to end.
BigFix Operator	The operator who initiated the deployment.
Issuer full name	The full name of the user or system that issued the deployment.

Related information

Fixlets *(on page 145)*

Managing Tags *(on page 51)*

Managing custom Fixlets *(on page 160)*

Managing custom Fixlets

Besides using the out-of-the-box content that BigFix provides, you can create your own Fixlets with custom detection rules and actions, and then edit or delete them. What you can create, edit, or delete depends on your operator role and site permissions.

A custom Fixlet contains your own detection criteria and action scripts. You create a custom Fixlet with the Create fixlet wizard from the Fixlet Explorer – List View. After the Fixlet is created, it appears in the List View table; select its name to open the detail page, where the **Edit** and **Delete** icons are available for custom Fixlets.

You can deploy a custom Fixlet in the same way as any other Fixlet. During the remediation flow, you can add tags to the deployment. For more information, see Deploying Fixlets *(on page 167)*.

You can tag a custom Fixlet as you create or edit it, using the **Tag** field on the **Details** step. You can also tag it later from the Fixlet Explorer – List View or its detail page. For more information, see Managing Tags *(on page 51)*.

Permissions for custom Fixlets

Custom Fixlet permissions follow the same approach as the BigFix platform and depend on the BigFix operator that is bound to your BigFix UI user. What you can do is determined by your operator role – master operator or non-master operator – and your site permissions.

Note: You can't edit or delete Fixlets that belong to external sites. This restriction applies to all operators.

For all other sites, the following permissions apply:

Table 25. Custom Fixlet permissions by operator role

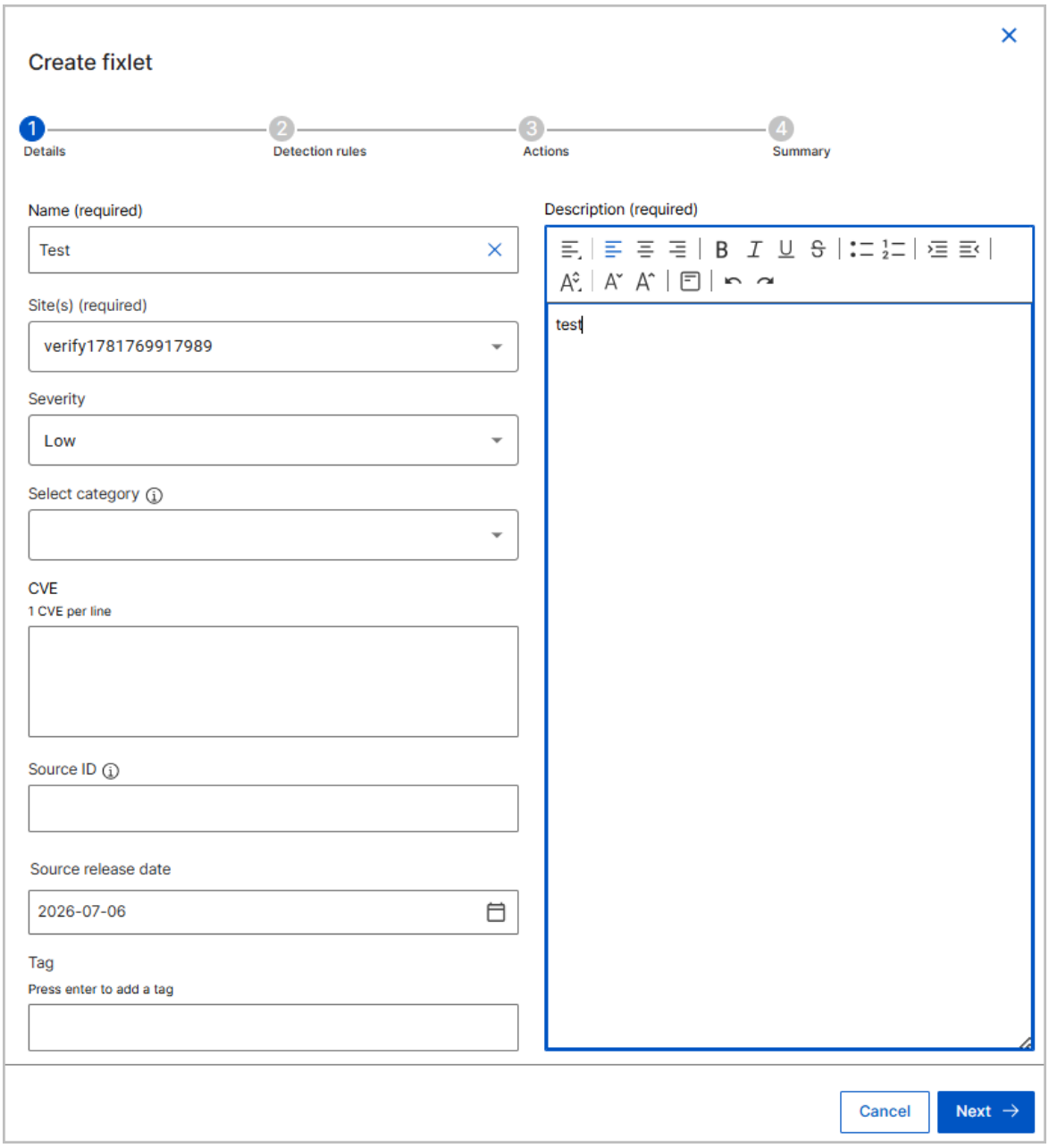
Action	Master operator	Non-master operator
Create	All sites except operator sites (opSites). The **Site(s)** list in the Create fixlet wizard shows only the sites that you can add content to.	Allowed when the **Custom content** permission is set to **Yes** and you have write permission on the site.
Edit	All sites except operator sites (opSites).	Allowed when the **Custom content** permission is set to **Yes** and you have write permission on the site.
Delete	All sites.	Allowed when the **Custom content** permission is set to **Yes** and you have write permission on the site.

Creating a custom Fixlet

Create your own Fixlet to run a custom set of actions on the devices you target. The Create fixlet wizard guides you through four steps: **Details**, **Detection rules**, **Actions**, and **Summary**.

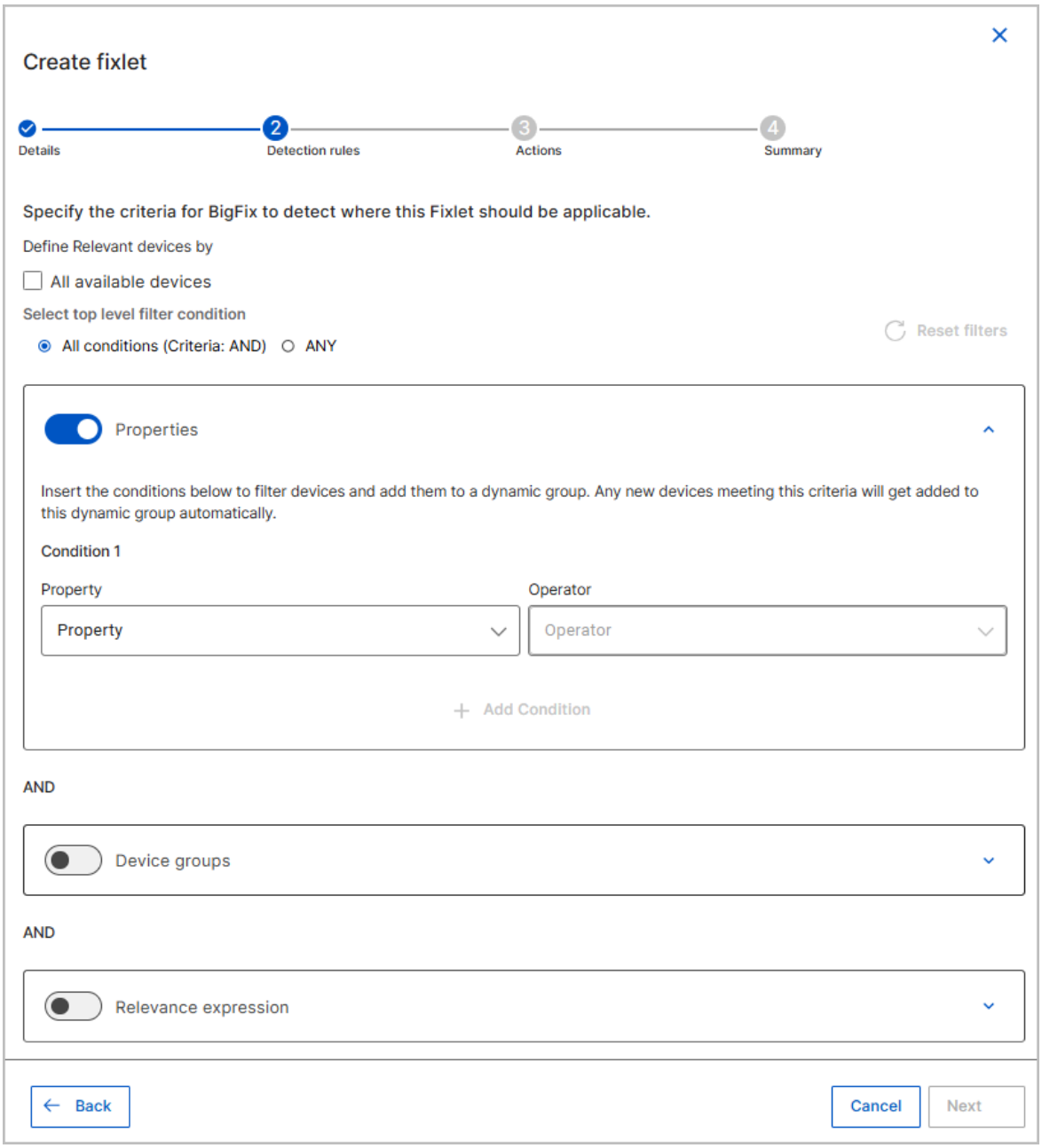
Before you begin, make sure that you have a site that you can add content to, and permission to create custom content in your BigFix environment. The **Site(s)** list shows only the sites where you're allowed to create Fixlets.

1. In the side navigation, expand **Explore** and select **Fixlets** to open the Fixlet Explorer – List View.
2. In the utility bar, select **Create Fixlet** (the plus icon). The **Create fixlet** wizard opens at step 1, **Details**.



3. On the **Details** step, provide the Fixlet information, and then select **Next**:
    - In **Name** (required), enter a unique name.
    - From **Site(s)** (required), select the site that the Fixlet belongs to.
    - In **Description** (required), enter a description. Use the formatting toolbar to style the text.
    - Optional: set **Severity**, **Select category**, **CVE** (one CVE per line), **Source ID**, **Source release date**, and **Tag** (press Enter to add each tag).
4. On the **Detection rules** step, specify the criteria that BigFix uses to detect where the Fixlet is applicable, and then select **Next**. Under **Define Relevant devices by**, select **All available devices** to target every device, or leave it cleared and define conditions:

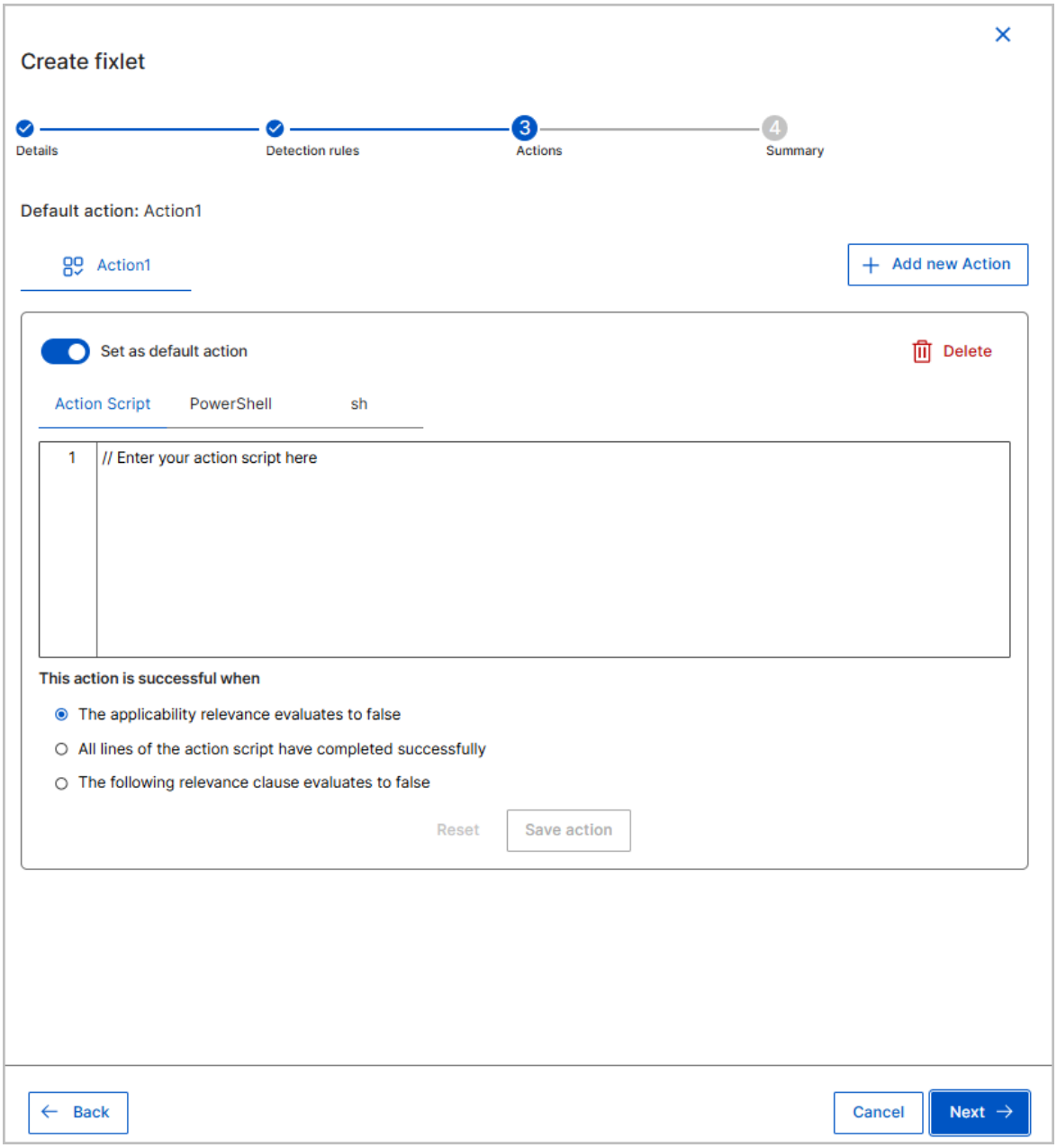
- For **Select top level filter condition**, select **All conditions (Criteria: AND)** or **ANY**.
- Turn on **Properties** to target by device attribute. For each condition, select a **Property** and an **Operator**, enter a **Value**, and select **Add Condition** to add more.
- Turn on **Device groups** to target an existing device group.
- Turn on **Relevance expression** to target by relevance logic. Select **Add Relevance** to add more clauses.
- Select **Reset filters** to clear all conditions.



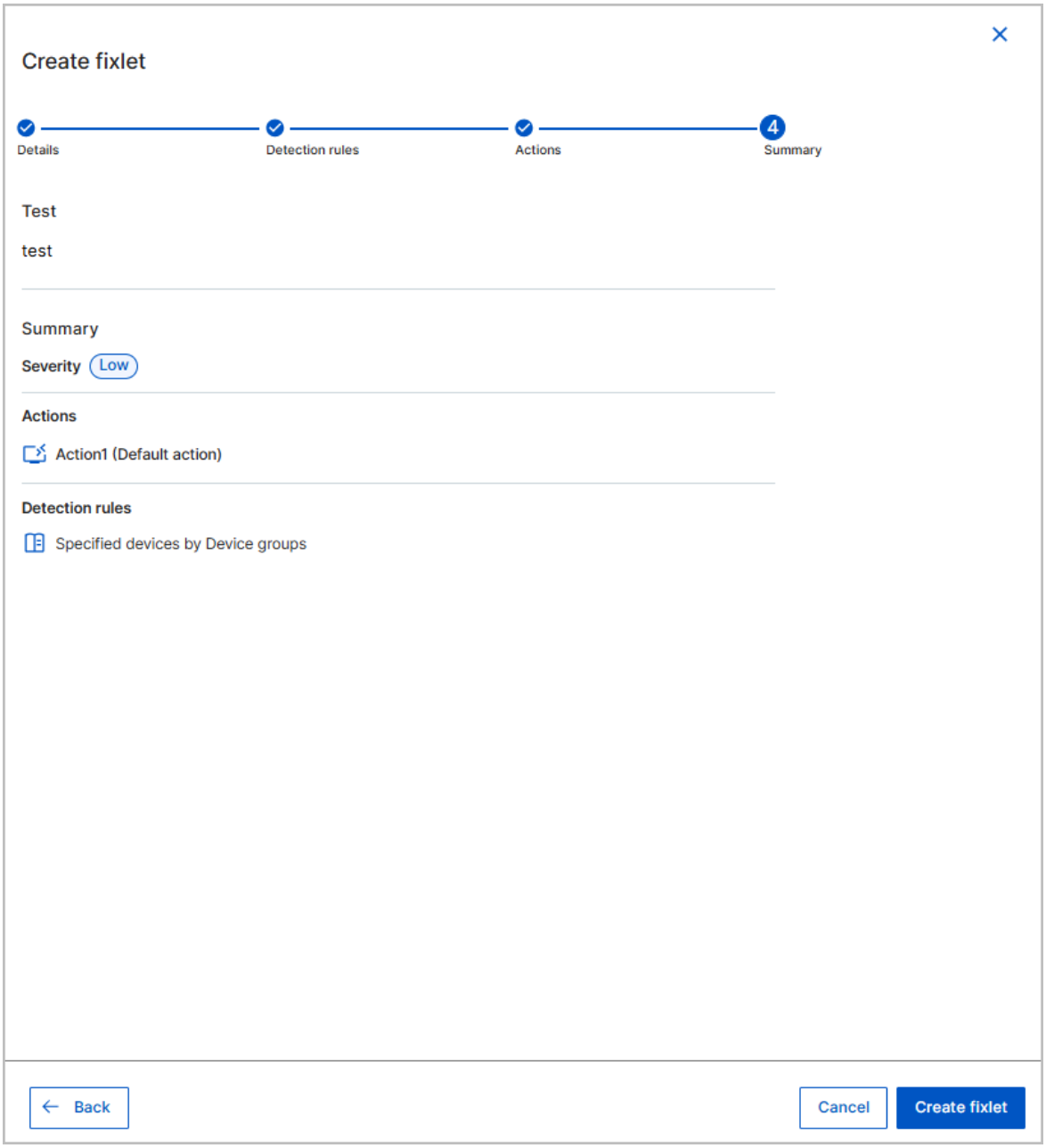
5. On the **Actions** step, define what the Fixlet does on relevant devices, and then select **Next**:
   - Select the script type tab: **Action Script**, **PowerShell**, or **sh**.
   - Enter the action script in the editor.

- Under **This action is successful when**, select a success condition: **The applicability relevance evaluates to false**, **All lines of the action script have completed successfully**, or **The following relevance clause evaluates to false**.
- Select **Save action**.
- To add another action, select **Add new Action**. To set a default, turn on **Set as default action**.

Note: An action is optional. To create a Fixlet without an action, select Delete on the Actions step to remove the action.



6. On the **Summary** step, review the name, description, severity, actions, and detection rules. If the description has more than one paragraph, select **More** to view the full description. To change an entry, select **Back**.



7. Select **Create fixlet**. The message **Your custom fixlet has been successfully created** appears, and the Fixlet is added to the Fixlet Explorer – List View table.

Note: To leave the wizard without creating the Fixlet, select **Cancel** on any step.

Editing a custom Fixlet

Update the details, detection rules, or actions of a custom Fixlet from its detail page. Whether you can edit a Fixlet depends on your operator role and site permissions, as described in Permissions for custom Fixlets.

Note:

- You can't edit Fixlets that belong to external sites.
- A master operator can't edit Fixlets in operator sites (opSites).
- A non-master operator can edit a custom Fixlet only when the **Custom content** permission is set to **Yes** and the operator has write permission on the site.
- You can't change the site of a Fixlet after it's created.

1. In the side navigation, expand **Explore** and select **Fixlets**.
2. In the Fixlet Explorer – List View table, select the name of the custom Fixlet that you want to edit. The Fixlet detail page opens.
3. In the top-right corner of the detail page, select the **Edit** icon. The wizard reopens with the Fixlet's current values.
4. Update the values on the **Details**, **Detection rules**, or **Actions** steps as needed.
5. On the **Summary** step, review your changes and save the Fixlet. The updated Fixlet appears in the Fixlet Explorer – List View table.

Deleting a custom Fixlet

Remove a custom Fixlet that you no longer need from its detail page. Before the Fixlet is removed, you can download its .bes file to keep a copy. Whether you can delete a Fixlet depends on your operator role and site permissions, as described in Permissions for custom Fixlets.

Note: You can't delete Fixlets that belong to external sites. A master operator can delete custom Fixlets from all other sites. A non-master operator can delete a custom Fixlet only when the **Custom content** permission is set to **Yes** and the operator has write permission on the site.

1. In the side navigation, expand **Explore** and select **Fixlets**.
2. In the Fixlet Explorer – List View table, select the name of the custom Fixlet that you want to delete. The Fixlet detail page opens.
3. In the top-right corner of the detail page, select the **Delete** icon. A confirmation dialog opens.
4. Optional: To keep a copy before you remove it, select the link in the dialog to download the Fixlet's .bes file.
5. Confirm the deletion. The Fixlet is removed from the Fixlet Explorer – List View table.

Related information

Managing Tags *(on page 51)*

Deploying Fixlets

Learn how to deploy Fixlets using the Fixlet Explorer deployment wizard. Get to know about the optional customizations that you can configure for each step of the wizard.

A Fixlet comprises instructions executed by the BigFix agent on an enrolled device. At BigFix, the process of executing a Fixlet is termed a **deployment**. BigFix provides numerous customization opportunities for optimizing performance during Fixlet deployment.

This topic elaborates on using the Deploy Wizard within the Fixlet Explorer app. To access the deploy menu, navigate to **Fixlet Explorer - List view** in the app menu.

Fixlet deployment compatibility

Before you deploy a Fixlet from BigFix UI, check the following table for the supported Fixlet types and the alternatives.

Table 26. Supported and unsupported Fixlet types

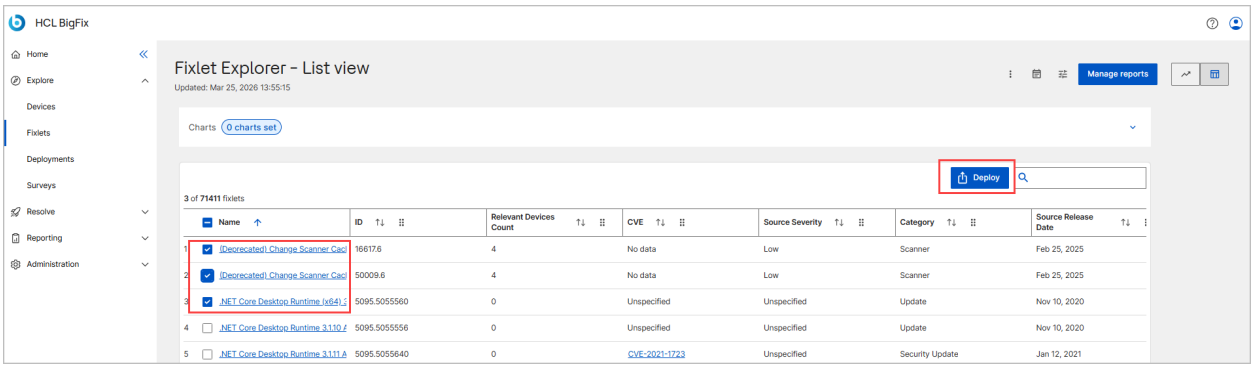
Fixlet or action type	BigFix UI support	Behavior and alternative
Standard Fixlets and Tasks that require no user input	Supported	Deploy directly to the selected target devices.
Fixlets that use the `action parameter query` command	Not supported	Deployment ends in error. Deploy from the **BigFix Console**.
Fixlets that collect input through HTML forms or JavaScript in the description	Not supported	Deployment ends in error. Deploy from the **BigFix Console**.

You can deploy these Fixlets only from the **BigFix Console**. You cannot deploy them from BigFix UI, BigFix WebUI, or the BigFix REST API.

Important: BigFix UI does not identify these Fixlets, so it does not prevent you from deploying them. If you deploy one of these Fixlets from BigFix UI, the action ends in error. Before you deploy a Fixlet, make sure that it does not require user input. For more information, see Known limitations *(on page 7)*.

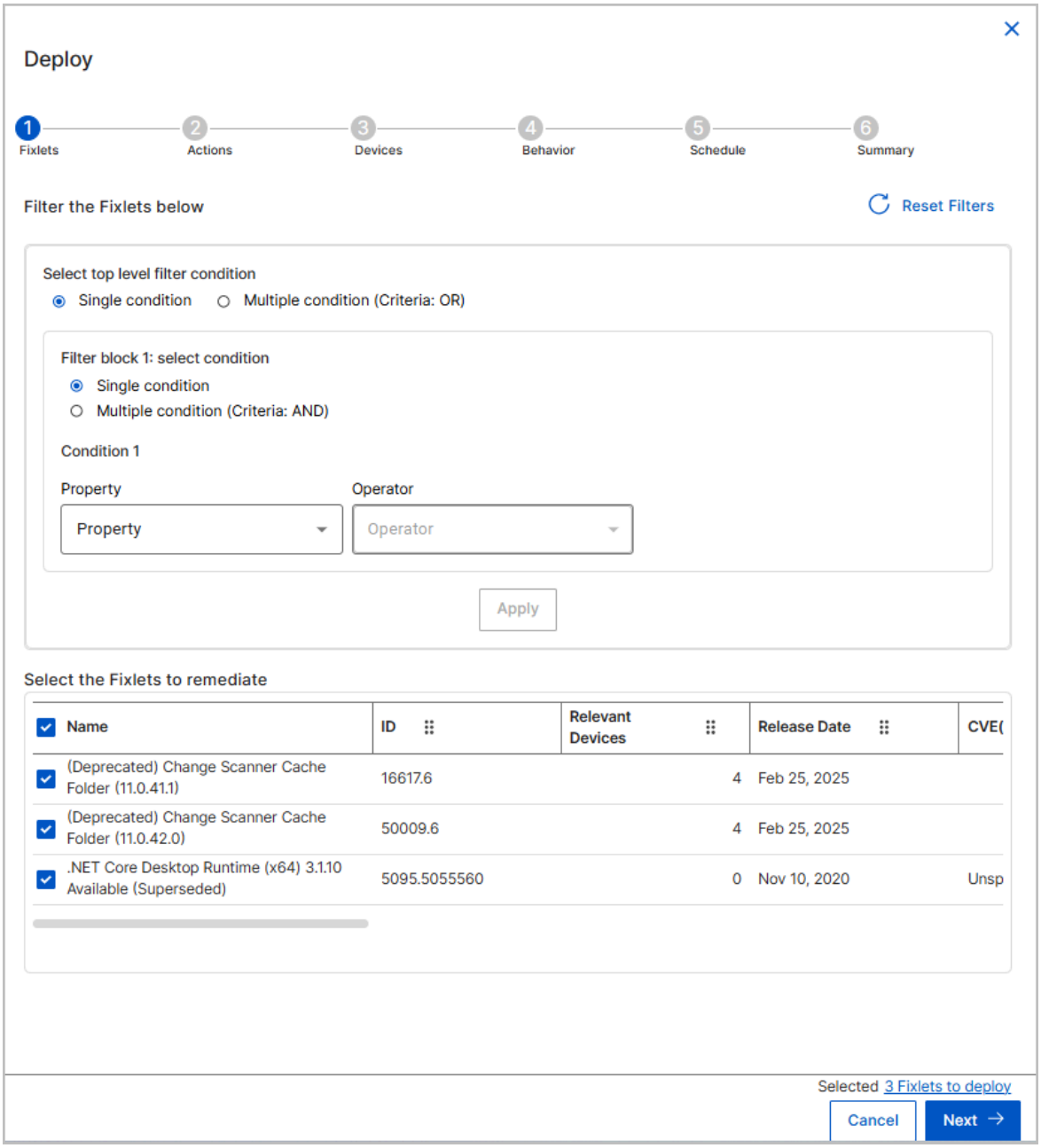
By default, the Deploy Wizard is inactive. It becomes active once Fixlets are selected in the data table. Multiple Fixlets can be selected and combined into a single deployment.

After selecting at least one Fixlet and clicking the **Deploy** button, the Deploy Wizard slides out from the right. The wizard will guide you through the steps to create a new deployment.



The Deploy Wizard allows to customize user deployments; however, these customizations are optional. Use the Deploy Fixlets wizard to create a deployment for one or more Fixlets selected from the Fixlet Explorer list view. The wizard guides you through six steps: Fixlets, Actions, Devices, Sequence, Schedule, and Summary.

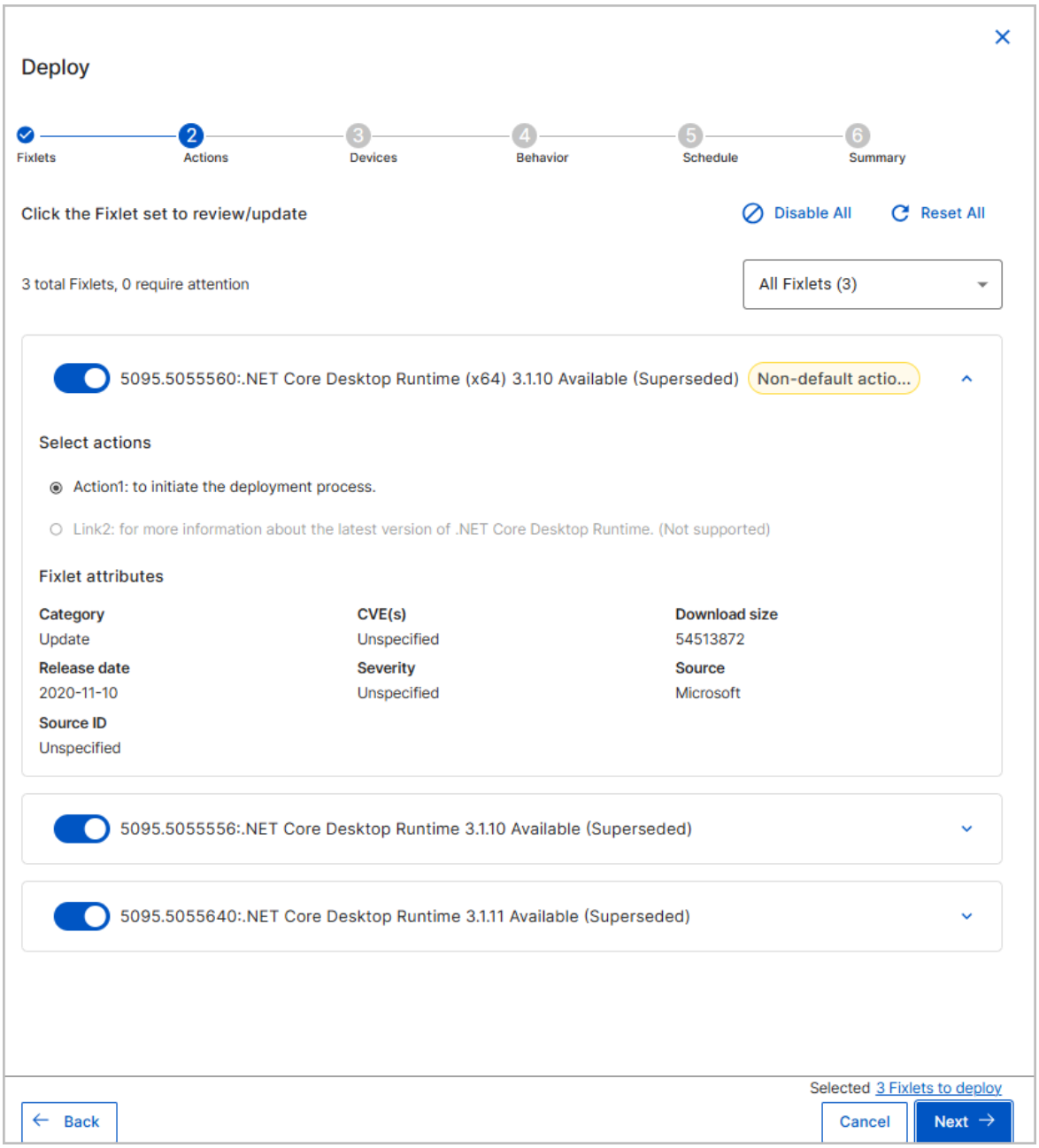
1. **Fixlets** - In this step, you filter and select the Fixlets you want to remediate.



   - All selected Fixlets are listed in a table
   - You can apply filters using **Single condition** or **Multiple condition (Criteria: AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see Filter by query *(on page 40)*.
   - Fixlet Table – Review the list of Fixlets.

- Select Fixlets – Use checkboxes to choose one or more Fixlets for remediation. A counter shows how many are selected.
- Next/Cancel – Click **Next** to continue to Actions, or **Cancel** to exit.

2. **Actions** - Review or update Fixlet actions. In this tab, confirm the actions you want the Fixlets you have selected to perform. This is important because not every Fixlet has a single, default action. It is also possible to remove Fixlets that do not have any actions that can be performed on the devices selected in the prior tab.



- The Actions step lists all selected Fixlets.
- Action filter drop-down – Allows you to refine which Fixlets are shown in the list. Available filter options:
  - All Fixlets – Displays all Fixlets in the remediation set.
  - Fixlets that are not actionable – Displays Fixlets that cannot be acted upon.
  - Fixlets with no-default action – Shows Fixlets that do not have a predefined default action.
  - Action required – Filters Fixlets that require immediate attention.
- **Actions step**: Review and update the actions for the selected Fixlets.
  - For Fixlets requiring a choice, select the radio button for the desired action (e.g., **Action1: to initiate the deployment process**).
- Review the **Fixlet attributes** provided in the details pane to confirm accuracy.
- Each Fixlet has a toggle switch to enable or disable its deployment.
- Ensure the toggle switch next to the Fixlet is set to **On**.
- You can use Disable All or Reset All options as needed.
- Verify the deployment summary link at the bottom right.
- Once this information is provided, click **Next** to proceed to the Devices tab.

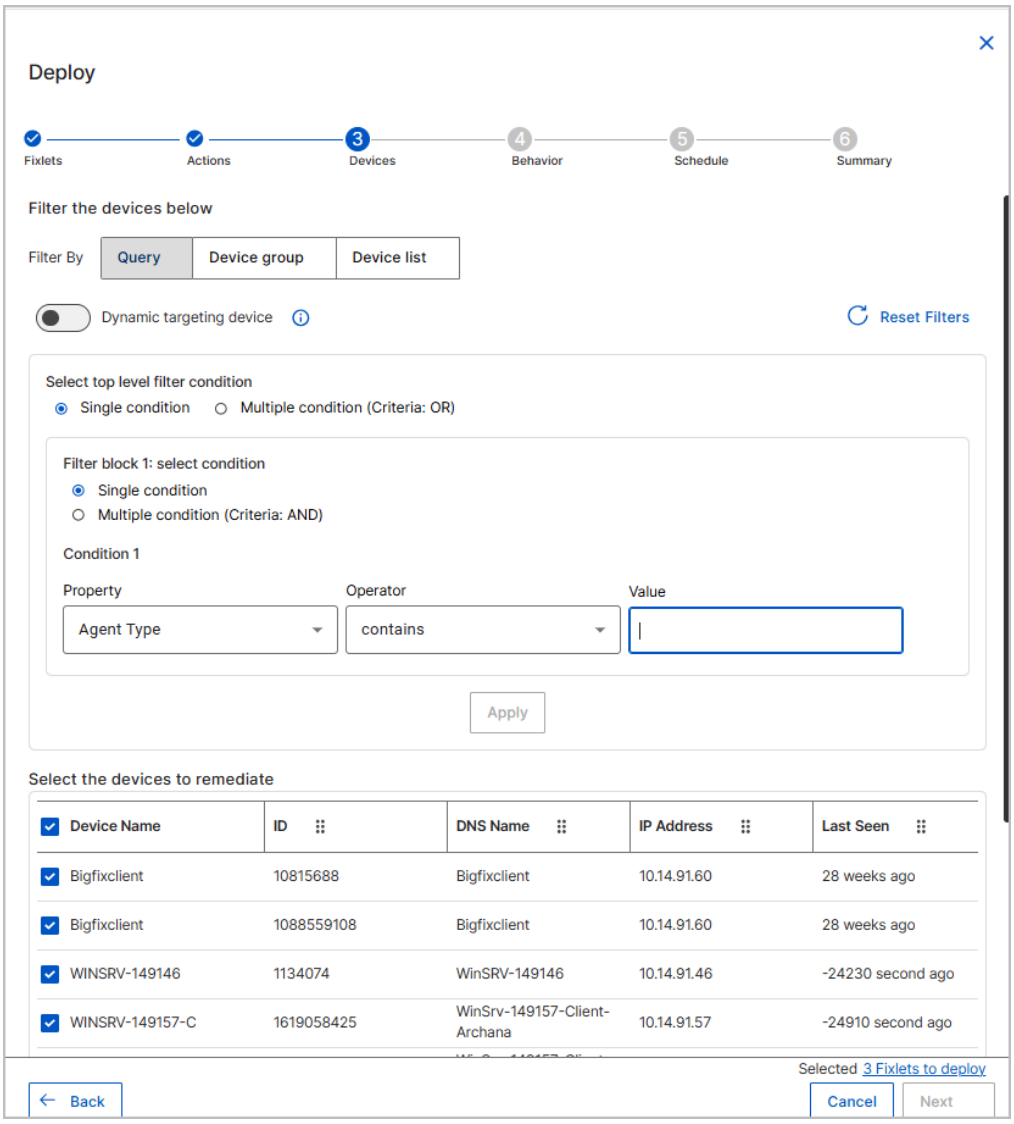
3. **Devices** - This step allows you to confirm the devices for the deployment. Choose to deploy to all applicable devices or utilize various filters to narrow down the deployment size. Since filtering is optional, it is possible to skip this step by clicking **Next**. you select which devices will be included in the deployment. You have three main approaches:

   a. **Filter by Query**

      i. You can apply filters using **Single condition** or **Multiple condition (AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see Filter by query *(on page 40)*.

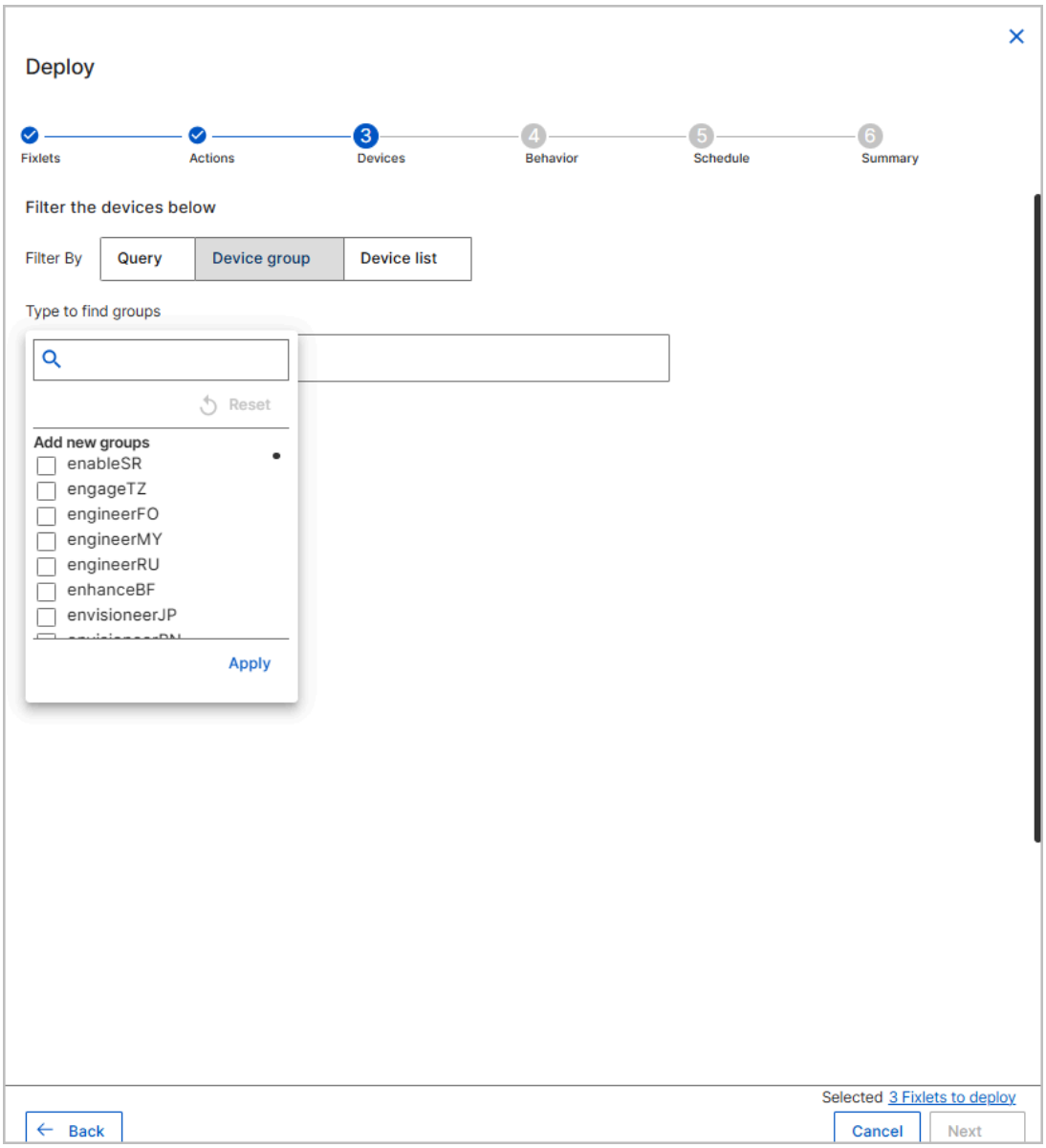
      ii. By default, the device table displays all devices that match the query, with details such as Device Name, ID, DNS Name, IP Address, Last Seen, OS Family, Operating System, and Device Type.

      iii. Dynamic Targeting Option



- Within this approach, you can enable the **Dynamic Targeting Device** toggle.
- Dynamic filters define a matching criteria for devices to evaluate continuously until the deployment ends. Any device that matches this filter after the deployment has been created, will have this deployment applied.
- New devices that match the criteria are automatically added.
- A **Preview of dynamically applicable targeted devices** is shown to confirm eligibility.

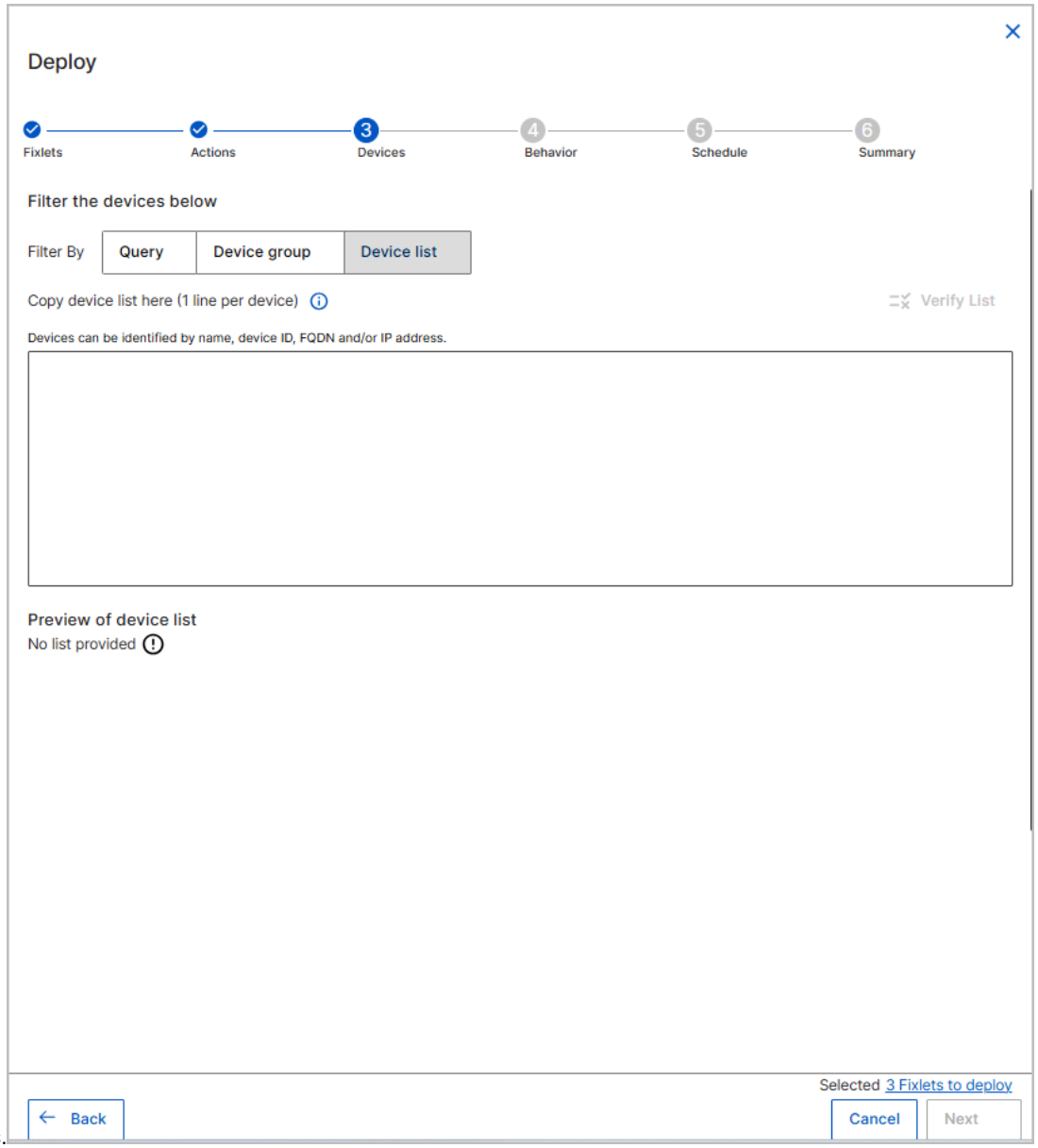
b. **Filter by Device group**- Select a pre-defined device group to target.



i. Locate and select your target groups:

- **Search**: Use the search bar to type and quickly find specific groups by name.
- **Select**: Check the box next to one or more groups under the **Add new groups** list.
- **Reset**: Click **Reset** if you need to clear your current selections within the menu.
- Click **Apply** within the dropdown menu to confirm your group selection.

c. **Filter by Device List** - This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.



   i. Regardless of how they are identified, each device must be in a separate row.
   ii. A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
   iii. Use Verify List to confirm the entries before proceeding.
   iv. The Preview area shows the final static list that will be targeted.
   v. Once the appropriate filters have been selected, or if no filter is needed, click **Next**.

4. **Behavior** - Some deployments can affect many devices simultaneously. The behavior tab provides you with control over deployment timing, display of alerts indicating Fixlet deployment availability for devices, and actions upon deployment completion. Note that selecting any of the provided options is not mandatory.

Offer to user

Offer to user

Notify device owner of offer availability

Title

Category

Description

Order of Events (from top to bottom)

Start downloading immediately

Before running message

Enter your message here, that you want to be displayed in front of your users.

Notify user for 10 minute(s) and then Run action immediately

Allow user to save work

Allow user to cancel

Show confirmation message before running action

While running message

Enter your message here, that you want to be displayed in front of your users.

Post deployment behavior

Do nothing after action completes

Restart computer after action completes.

Shutdown computer after action completes.

On failure, retry 1 1 time(s)

and wait 1 hour(s) between attempts

Wait until computer has rebooted

Reapply whenever it becomes relevant again

with a 1 hour(s) wait between attempts

up to 3 time(s)

Offer to user: Enable this toggle to deploy the action as a BigFix "Offer".

Note: An Offer allows end-users to choose and install software, patches, or other actions themselves through a self-service application, rather than having them automatically deployed by an administrator.

When you enable this toggle, set the following options:

- **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
- **Title** - Enter the title that identifies the offer to the user.
- **Category** - Enter the category that groups the offer in the self-service application.
- **Description** - Enter the text that explains what the offer does.

The behavior tab has a number of toggle switches users can turn on or off. They are presented as an order of events from top to bottom. The sequence order is as follows:

a. Start download immediately - Some Fixlets can contain large files. This option allows users to control whether all applicable devices should begin downloading the Fixlet as soon as the deployment is created.

b. **Before running message** - As a device may become unresponsive while a Fixlet is being deployed, this gives users the option to display a warning for an amount of time before the Fixlet is applied. This may also be useful if a restart is required, so end users can save work.

   Enable the toggle and set the following options:

   - Enter the message text to display to the user before the action runs.
   - In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Run action immediately**).
   - **Allow user to save work** - Select this checkbox to let the user save open work before the action runs.
   - **Allow user to cancel** - Select this checkbox to let the user cancel the action.
   - **Show confirmation message before running action** - Select this checkbox to prompt the user to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own (for example, *Are you sure you want to run this action now?*).

c. **While running message** - As a device may be unresponsive while a Fixlet is being deployed, this allows users to write a message that will be displayed on the screen until the deployment is complete. Enable the toggle, and then enter the message text to display to the user.

d. **Post deployment behavior** - Enable this toggle to control what happens on the device after the action completes. Select one of the following options:

- **Do nothing after action completes** - The device stays in its current state.
- **Restart computer after action completes** - The device restarts when the action finishes.
- **Shutdown computer after action completes** - The device shuts down when the action finishes.

If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:

- **Message title (required)** - Enter a short title (for example, *Shutdown now*).
- **Message text (required)** - Enter the message body that asks the user to save any unsaved work.
- In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Shutdown automatically** or **Restart automatically**).
- **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let the user cancel the shutdown or restart.

e. **On failure, retry** - Occasionally, deployments fail to complete successfully on a device. Should this occur, this allows users to determine if they would like BigFix to automatically try the deployment again. Enable the toggle, enter the number of retries, and then select one of the following options:

- **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.

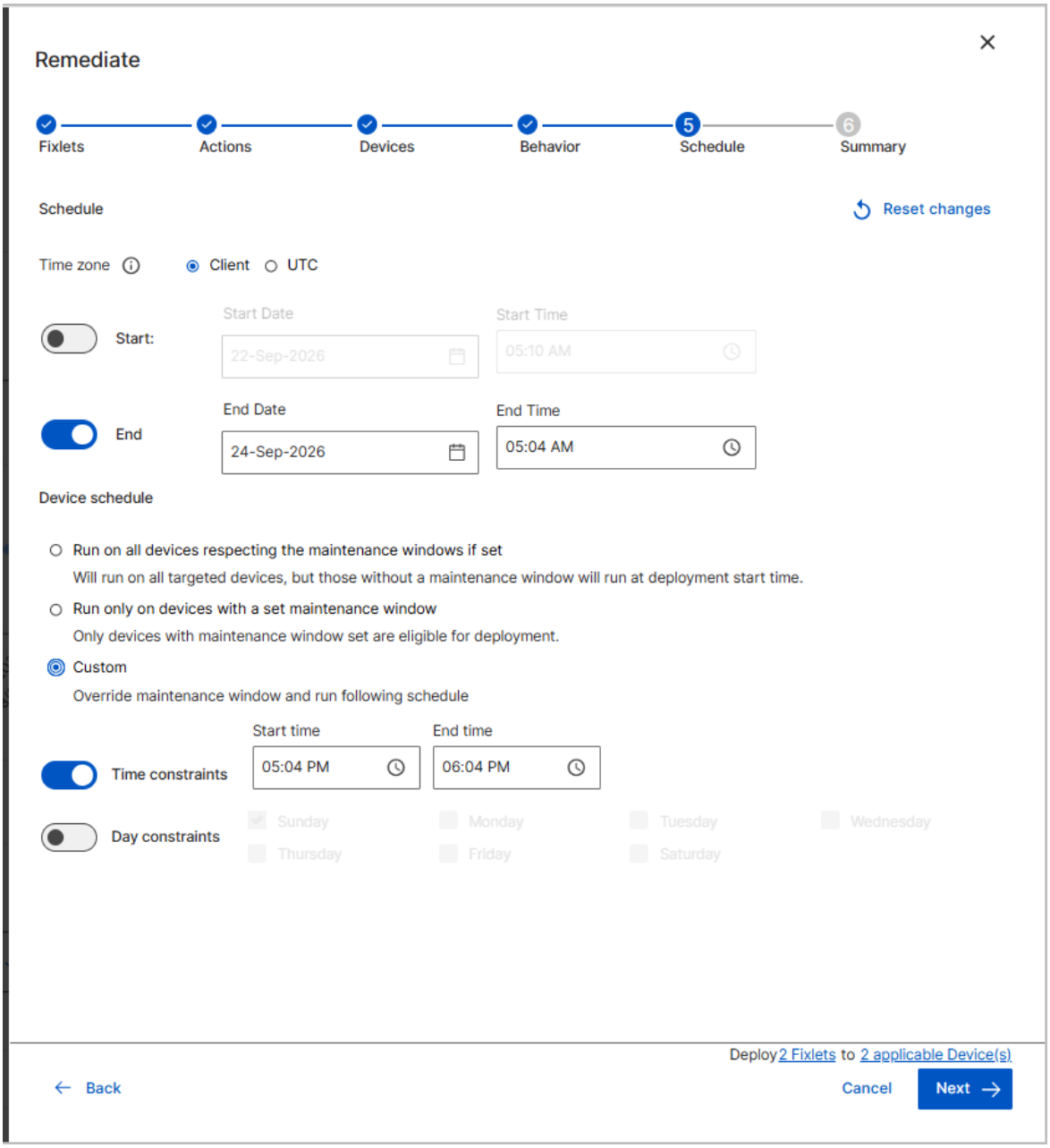
f. **Reapply whenever it becomes relevant again** - This option automatically reapplies a Fixlet if it becomes relevant again after the initial deployment. Enable the toggle, and then set the following options:

- **with a** - Select this checkbox and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **up to** - Select this checkbox and enter the maximum number of times (for example, **3**) that BigFix reapplies the Fixlet.

After selecting the desired sequence, click **Next** to proceed to the schedule tab.

5. **Schedule** - not required. Determining a deployment's start and end time gives BigFix users a tool to control their deployments. Typically, deployments do not happen immediately. Some devices may be powered down, or disconnected from the Internet, or otherwise unable to have the Fixlet applied. Scheduling allows to control how long BigFix will attempt this particular deployment.

   There may be other reasons to control the end time. For example, an organization may wish to ensure that all deployments run overnight to minimize business impact.



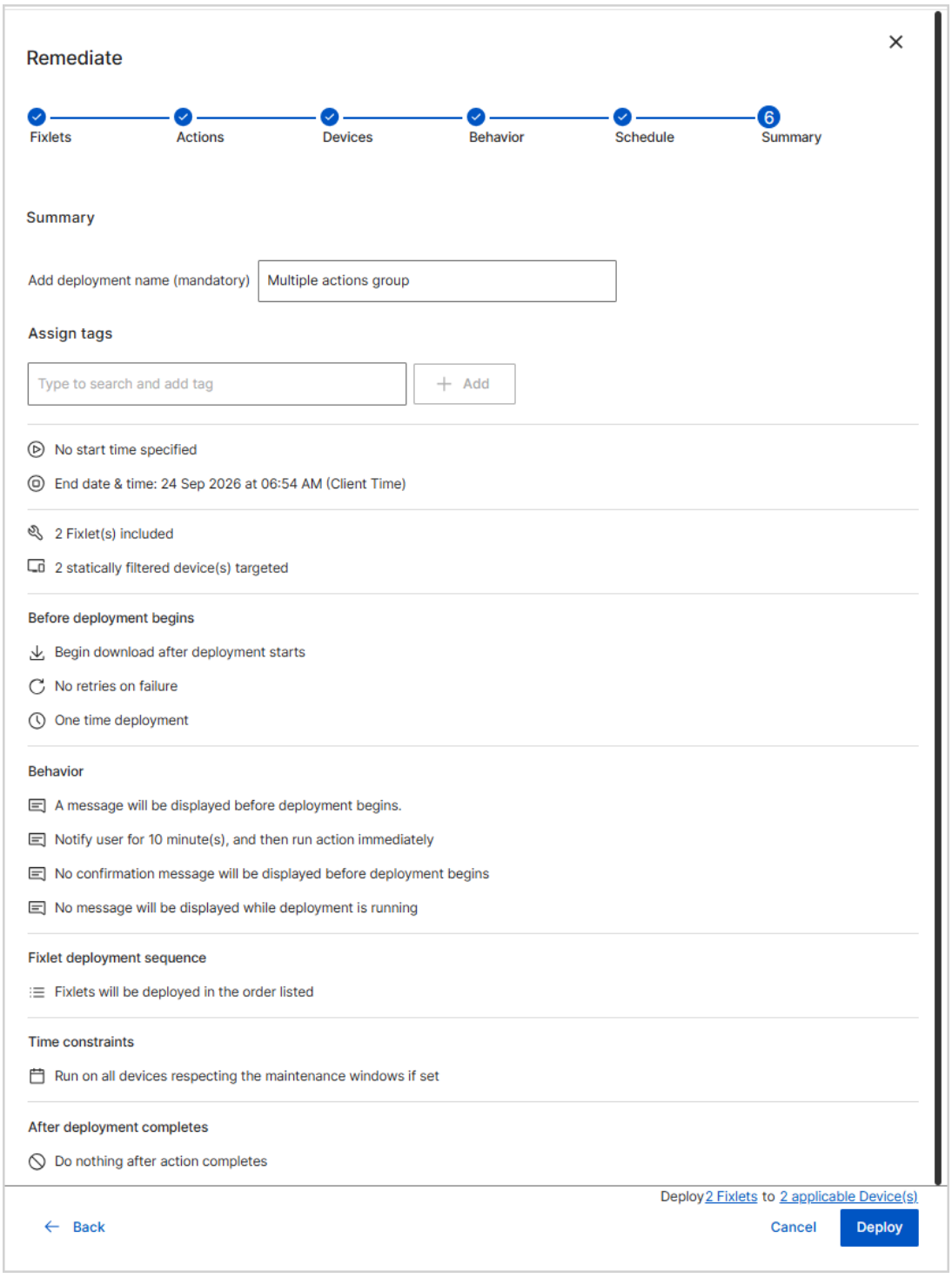
- The schedule tab has two options: **Start Time** and **End Time**. In the first, select the calendar date and the start time when BigFix will begin attempting to apply the deployment. You may also select if you want to use client time (e.g., the time zone where the device is located) or UTC.
- In the second, select the calendar date and the start time when BigFix will stop attempting to apply the deployment. You may also select if you want to use client time (e.g., the time zone where the device is located) or UTC.
- If no scheduling option is selected, BigFix will begin the deployment immediately.
- **Run during agent's configured maintenance window**: Select this option, if you want to deploy the Fixlet during the set maintenance window *(on page 126)*.

- **Custom Constraints** - The Time Constraint option lets you control when a deployment can run by defining specific time ranges. This ensures Fixlets are applied only during the approved hours or maintenance periods.
- Time Constraints: Specify the time range (for example, 11:00–23:00) when the deployment is allowed to execute.
- Day Constraints: Optionally, choose one or more days of the week to further limit deployment (for example, only weekends or weekdays).
- After selecting the desired schedule, click **Next** to proceed to the summary tab.

6. **Summary** - The summary tab shows all of the choices made related to the deployment created. This allows to review all of the things the deployment will do in one location.
    a. **Add deployment name (mandatory)** field is auto-populated with a default name that you can edit on the Summary step. Keep the default, or enter a unique, meaningful name that describes the purpose of the action.
    b. In **Assign tags**, add one or more tags:
        - To add an existing tag, type to search for it, select it from the list, and then select **Add**.
        - To create a new tag, type the tag name, and then select **Add**.

    Assigned tags appear as chips below the field. To remove a tag, select the **X** on its chip.
    c. Review all configuration sections to ensure they match your intended scope. The Summary step lists the start and end date and time, the number of Fixlets included, the number of targeted devices, **Before deployment begins**, and **Behavior**.
    d. The **Behavior** section confirms the message and notification options that you set on the Behavior step, for example:
        - A message will be displayed before deployment begins.
        - Notify user for 10 minute(s), and then run action immediately.
        - A confirmation message will be displayed before deployment begins.
        - No message will be displayed while deployment is running.

    e. (Optional) Click **Back** to navigate to previous steps and modify any settings.



f. Once satisfied with the configuration, click **Deploy** to initiate the remediation flow.

g. Wait for the system to process the request. Once submitted, a confirmation message appears: "**deployment submitted successfully**".

h. Click **OK** to close the deployment wizard and return to the main interface.

Result

The remediation flow is created and submitted to the targeted devices. You can track the real-time status and results of the action in the **Deployments** section of the BigFix UI.

Deployments

Monitor and manage deployments across your environment from the Deployment Manager page - view deployment status, filter and search the list, and stop or delete existing deployments.

The **Deployment Manager** in BigFix UI provides a centralized view to monitor and manage deployments. It enables you to view deployment status, stop or delete existing deployments, and review configuration and device-level details for each deployment.

The Deployment Manager displays all deployments associated with your environment in a table view. Each deployment represents an action initiated on one or more devices. These actions are called deployments. The complexity of a deployment can vary significantly. Some deployments complete in minutes, while others take days to run successfully on all targeted devices.

Before you begin

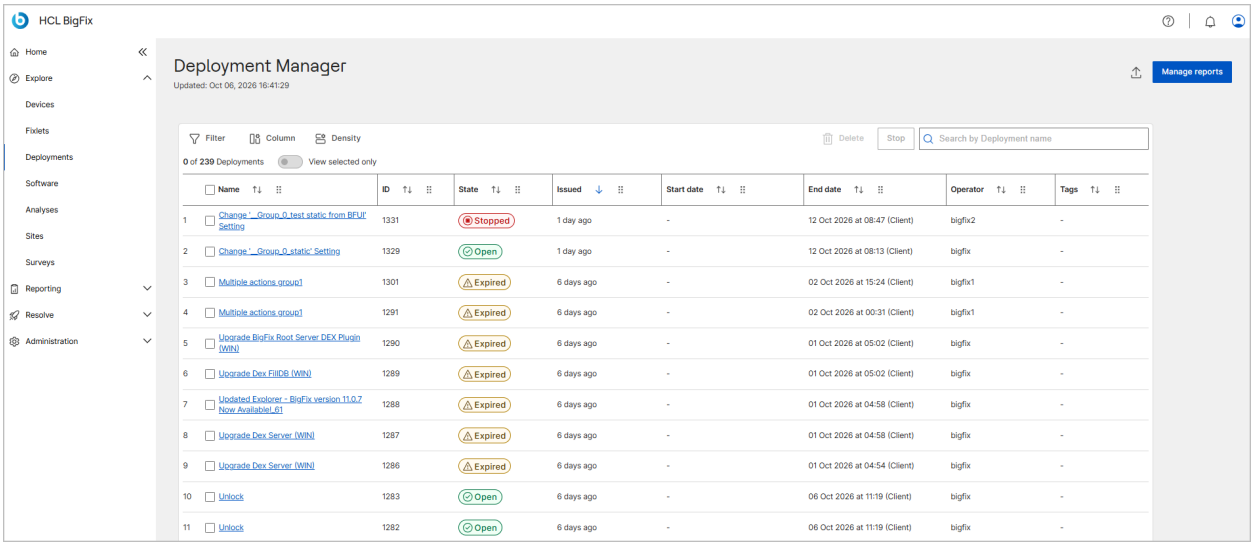
Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to this application. Deployment Manager is a default application, so every role has at least view access to it. See Managing Roles *(on page 467)*.
- Your operator permissions determine which deployments you can see and which actions you can complete, such as stopping or deleting a deployment. For a description of each permission, see Permissions reference *(on page 482)*.

Viewing the Deployment Manager

To access the Deployment Manager app, expand **Explore** from the side navigation, and select **Deployments**.

This page displays a table of all deployments executed in your environment, including open, expired, or stopped ones. Each row represents a single deployment record. The page title shows an **Updated** line with the date and time the table data was last refreshed.



Data table columns:

Table 27. Deployment Manager - data table columns

Column	Description
Name	The deployment title or action name. Select the name to open its detailed page.
Tags	Tags applied to the deployment. Shows a tag value, a count link (for example, *2 tags*) if more than one tag is applied, or *No data* if no tag is applied. Select a count link to open a read-only drawer that lists every tag on the deployment. You assign deployment tags on the **Summary** step of the remediation flow; they can't be changed after the deployment is created. For more information, see Managing Tags *(on page 51)*.
State	Shows the current status of the deployment - **Open**, **Expired**, and **Stopped**.
Issued	Time when the deployment was created, shown relative to now (for example, *1 day ago*).
ID	Unique deployment identifier assigned by BigFix.
Start date	Scheduled start time of the deployment. Shows *[null]* if no start date is scheduled.
End date	Completion or expiration time of the deployment.
BigFix Operator	The operator account that initiated the deployment.
Issuer full name	User who created or owns the deployment.

The upper-right corner of the page offers the following controls:

Table 28. Deployment Manager - page controls

Control	Description
Export icon	Opens the Export panel. Select either **CSV** or **Excel** format, and then select **Download** to export and save the deployment data. For more details, see Exporting Data *(on page 30)*.
Manage reports	Opens the Manage Reports panel. Save the current view, such as the applied filters and columns, as a report, or load a report that you saved earlier. You can also set a report as the default view for this page. For more details, see Manage Reports *(on page 42)*.

The data table offers the following controls:

Table 29. Deployment Manager - toolbar and data table controls

Control	Description
Column	Customizes which columns the data table displays. For more details, see Columns *(on page 29)*.
Density	Adjusts the row height of the data table. For more details, see Density *(on page 29)*.
Filter icon	Opens the filter panel. Using the filter tool makes it possible to reduce the number of deployments displayed in the data table. For more details, see Table filter *(on page 40)*.
Column header sort	Sorts the data table using the values in that column. Move your cursor near the column header name and select it to sort; select again to reverse the sort order. For more details, see Sorting Data *(on page 30)*.
Count line	Shows the number of deployments selected in the data table out of the total associated with your account, in the form *X of Y Deployments* (for example, *0 of 375 Deployments*). Selecting deployments is required for actions such as stopping or deleting them.
Stop	Stops the selected open deployments that you issued.
Delete	Deletes selected deployments from the data table so that they no longer display. You can delete only expired deployments. To delete an open deployment, you must first stop it.
Search box	Filters the deployments list by a keyword, such as a name or ID. The list updates automatically as you type.

Note: The **Stop** and **Delete** buttons are disabled by default and become selectable only after you choose at least one deployment in the data table. User permissions, as assigned by administrators, might restrict some users from stopping or deleting deployments.

Restriction: BigFix UI does not support the **Stop Other Operators' Actions** permission. A non-master operator can stop only the open deployments that they issued, even if their role grants **Stop Other Operators' Actions**. The **Stop** button stays disabled for deployments issued by other operators. To stop a deployment that another operator issued, use the BigFix Console. See Stop Other Operator's Actions feature.

Select the deployment name to drill down to the deployment details page, which has extensive details about that deployment's configuration and status.

When you deploy two or more Fixlets or Tasks together, BigFix creates a **Multiple Action Group (MAG)** along with a member action for each deployed Fixlet. The parent deployment acts as a container action, and each member action carries the Multiple Action Group ID as its parent action ID. The details page of a Multiple Action Group includes a **Components** tab that lists every member action. For more information, see Components tab *(on page 190)*.

Related information

Deployment Details page *(on page 184)*

Managing Tags *(on page 51)*

Managing Filters *(on page 35)*

Manage Reports *(on page 42)*

Deployment Details page

Review a single deployment's configuration, progress, and results across the Overview, Fixlets, Devices, and Components tabs.

The Deployment Details page offers a comprehensive view of a deployment's configuration, progress, and results.

The tabs displayed depend on whether the deployment is a standard single-action deployment or a Multiple Action Group:

- **Standard deployments (single Fixlet, Task, or custom remediation)**: Includes three tabs - **Overview**, **Fixlets**, and **Devices** - to help you analyze outcomes, review script logic, and troubleshoot targeted endpoints.
- **Multiple Action Group (MAG) deployments**: When you deploy two or more Fixlets together, the Deployment Details page provides four tabs - **Overview**, **Fixlets**, **Devices**, and **Components**. Use the **Components** tab to monitor and drill down into each member action in the group.

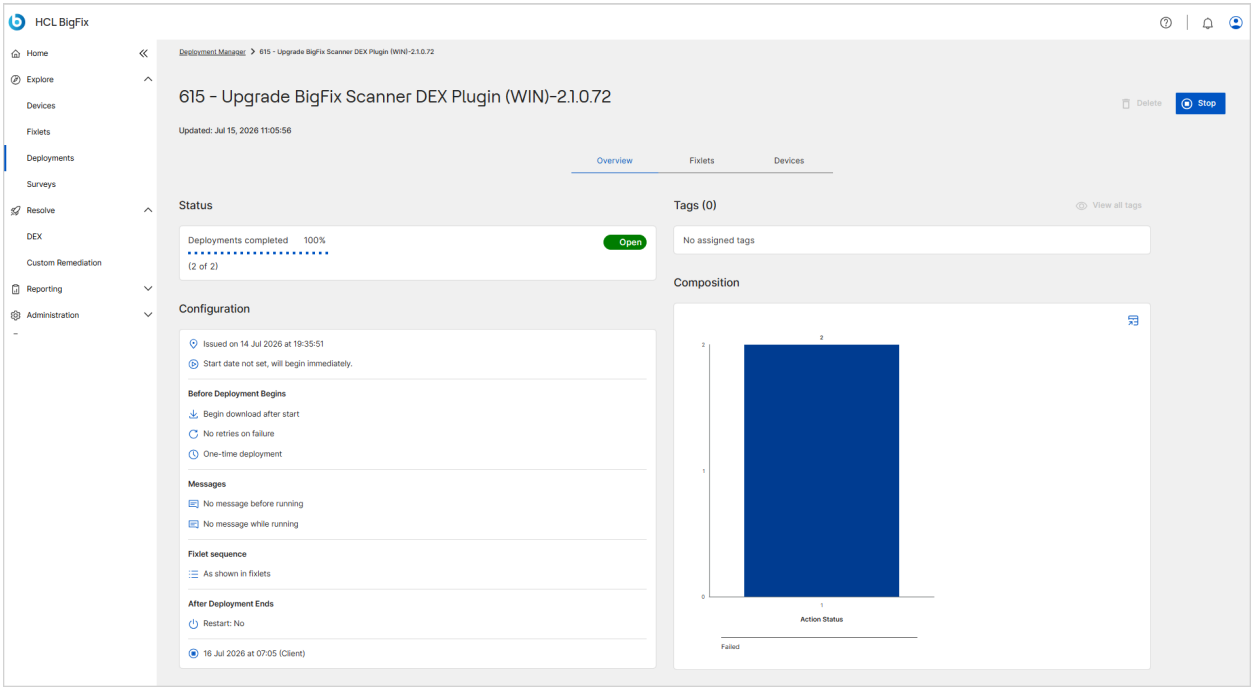
The page features panels and widgets for Status, Tags, Configuration, Composition, Relevance, Action script, Devices, Fixlets, and Components, providing targeted insights that include execution logic and success criteria.

Select the name of the deployment from the Deployment Manager *(on page 181)* table view to drill down to the deployment details page, which has extensive details about that deployment's configuration and status. A breadcrumb at the top of the page (**Deployment Manager** > the deployment name) links back to the deployment list.

The page title shows an **Updated** line with the date and time the page data was last refreshed. The **Delete** and **Stop** buttons also appear at the top of the Deployment Details page, so you can stop or delete this deployment without returning to the Deployment Manager list. The same availability rules apply as in the Deployment Manager: you can delete only an expired deployment, and an open deployment must be stopped before it can be deleted. You can stop only a deployment that you issued. See the restriction in Deployments *(on page 181)*.

Overview tab

The Overview tab provides a summary of the deployment configuration, its progress, and current execution status. It gives you an instant snapshot of a deployment's configuration and completion status.



Sections displayed:

Table 30. Overview tab - sections

Section	Description
Status panel	Shows **Deployments completed** as a percentage with a progress bar and a completed-of-total count (for example, *2 of 2*), and the deployment's current state as a badge - **Open**, **Expired**, **Stopped**, or **Scheduled**.

Table 30. Overview tab - sections (continued)

Section	Description
Tags panel	Shows the number of tags applied to the deployment in the panel heading (for example, *Tags (0)*). Lists the applied tags, or shows *No assigned tags* if none are applied. Select **View all tags** to see the full tag list when there are more tags than fit in the panel. Deployment tags are read-only: you assign them on the **Summary** step of the remediation flow, and you can't add or remove them here. For more information, see Managing Tags *(on page 51)*.
Configuration panel	Lists the key configuration parameters of the deployment. See the parameter table below.
Composition chart	Displays a graphical breakdown of deployment status across devices as a bar chart, plotting the number of devices against **Action Status** (for example, Fixed, Failed, Pending).
Relevance card	Displays the relevance expression that the endpoint evaluates to determine applicability. Includes a **Wrap long lines** toggle, a **copy to clipboard** button, and a **Show More** / **Show Less** link to expand the view. **Note:** For Multiple Action Groups, you view relevance within each member action through the **Components** tab.
Action script card	Displays the script commands that the BigFix Agent runs. Includes a **Wrap long lines** toggle, a **copy to clipboard** button, a **Show More** / **Show Less** link, and the defined **Success Criteria**. **Note:** For Multiple Action Groups, you view the action script within each member action through the **Components** tab.

Configuration panel parameters:

Table 31. Overview tab - configuration panel parameters

Parameter	Description
Issued on	Date and time when the deployment action was created (for example, *Issued on 14 Jul 2026 at 19:35:51*).
Start date	The scheduled start date and time for the deployment. If no start date is scheduled, shows *Start date not set, will begin immediately*.
Before Deployment Begins	Lists pre-deployment settings, such as download timing (for example, *Begin download immediately* or *Begin download after deployment starts*), failure retry

Table 31. Overview tab - configuration panel parameters (continued)

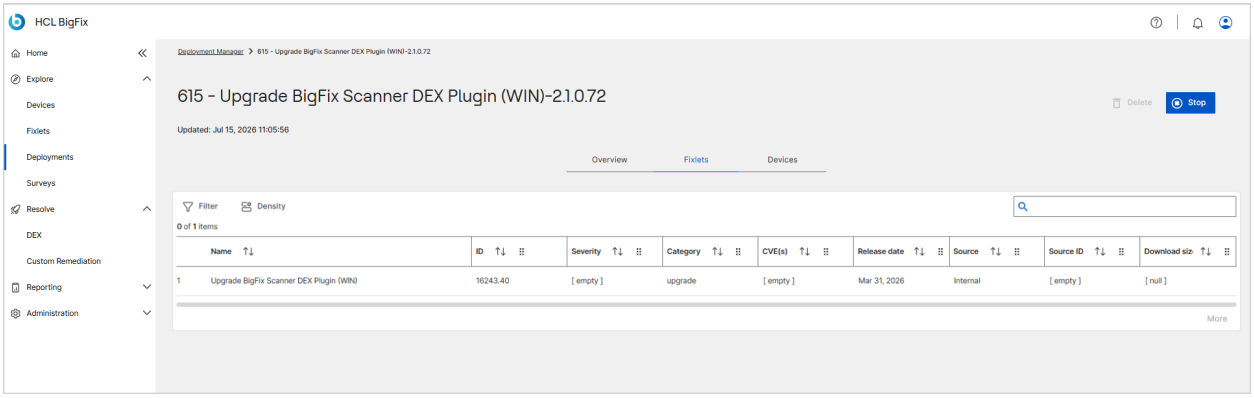
Parameter	Description
	behavior (for example, *No retries on failure*), and deployment frequency (for example, *One-time deployment*).
Messages	Indicates which messages are configured for the deployment. A separate line appears for the before-deployment message, the confirmation message, and the while-running message. For example, *No message will be displayed before deployment begins*, *A confirmation message will be displayed before deployment begins*, and *A message will be displayed while deployment is running*.
Fixlet sequence	Displays the execution order of the deployed fixlets (for example, *As shown in fixlets*).
Time constraints	Specifies when the process can run by setting a time range and restricting execution to selected days of the week. This section displays only if configured during the remediation setup.
After Deployment Ends	Defines post-deployment behavior set on the Behavior step, such as whether the device does nothing, restarts, or shuts down after the action completes (for example, *Restart: No*), and the scheduled end date and time of the deployment (for example, *16 Jul 2026 at 07:05 (Client)*).

For standalone deployments, custom remediation actions, and individual member actions in a Multiple Action Group, the **Overview** tab displays the execution logic and applicability conditions:

- **Relevance**: Displays the relevance expression that client endpoints evaluate. Enable the **Wrap long lines** toggle to fit extended relevance code within the panel without horizontal scrolling. Select **copy to clipboard** to copy the expression, or select **Show More** to expand the view.
- **Action script**: Displays the script commands that the BigFix Agent runs. Includes the **Wrap long lines** toggle and the **copy to clipboard** option.
- **Success Criteria**: Displayed within the **Action script** card, this indicates how BigFix assesses deployment success:
    - *The applicability relevance evaluates to false* - Used for Fixlets. The action succeeds when the relevance no longer matches after execution.
    - *Run to completion* - Used for Tasks and custom scripts. The action succeeds when all commands run without error.
    - *Custom relevance expression* - Evaluates against the custom success criteria that you configured at deployment time.

Fixlets tab

The Fixlets tab lists all fixlets included in the deployment along with their severity, category, source, and release details. Use this view to identify the updates or actions that were deployed.



The Fixlets tab offers the following controls:

Table 32. Fixlets tab - controls

Control	Description
Filter	Opens the filter panel to reduce the number of fixlets displayed in the data table.
Density	Adjusts the row height of the data table.
Search box	Filters the fixlet list by a keyword. The list updates automatically as you type.
Count line	Shows the number of fixlets selected out of the total, in the form *X of Y items* (for example, *0 of 1 items*).
More	Loads additional fixlet rows when the tab has more items than currently displayed.

Columns:

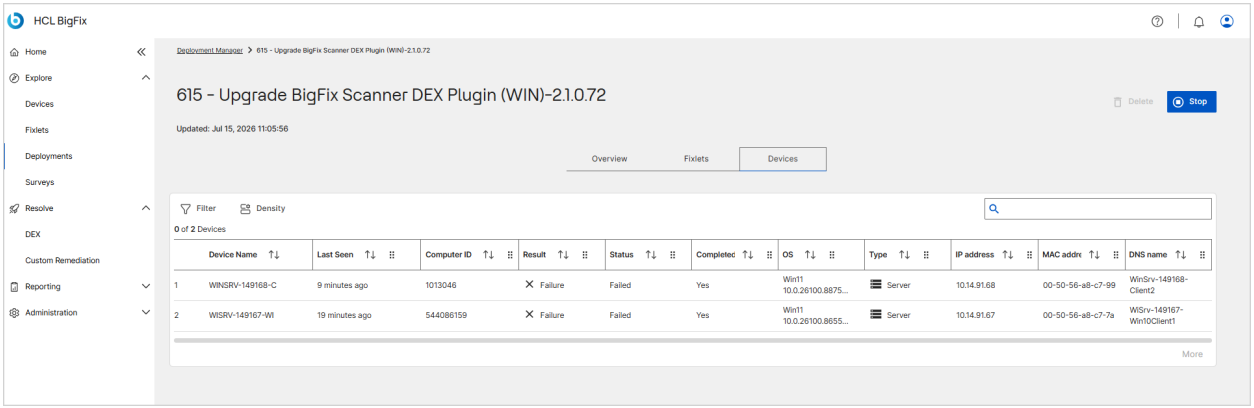
Table 33. Fixlets tab - columns

Column	Description
Name	Fixlet title in the site.
ID	Numeric identifier of the fixlet in the site.
Severity	Vendor severity (for example, Unspecified, Low, Critical).
Category	Functional category (for example, Security Updates, Patch).
CVE(s)	CVE identifier or identifiers associated with the fixlet, if applicable.
Release date	Original publish date of the fixlet.
Source	Publisher/vendor (for example, Microsoft, HCL).
Source ID	Vendor reference such as a KB, CVE, or article ID.
Download size	Size of the payload the fixlet downloads, if applicable.

Note: The data table may include more columns than fit onscreen; scroll horizontally to see additional columns.

Devices tab

The Devices tab shows all endpoints targeted by the deployment, including results such as Success or Failure. You can review each device's operating system, completion status, and DNS name to track success or troubleshoot failed systems.



The Devices tab offers the following controls:

Table 34. Devices tab - controls

Control	Description
Filter	Opens the filter panel to reduce the number of devices displayed in the data table.
Density	Adjusts the row height of the data table.
Search box	Filters the device list by a keyword. The list updates automatically as you type.
Count line	Shows the number of devices selected out of the total, in the form *X of Y Devices* (for example, *0 of 2 Devices*).
More	Loads additional device rows when the tab has more items than currently displayed.

Columns:

Table 35. Devices tab - columns

Column	Description
Device Name	Hostname of the endpoint.

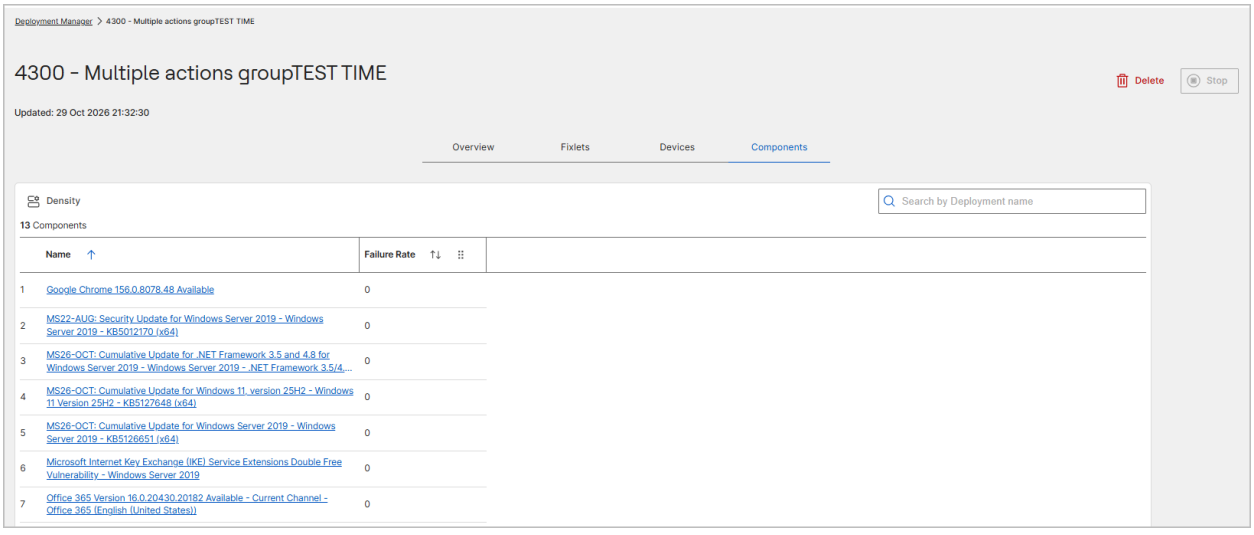
Table 35. Devices tab - columns (continued)

Column	Description
Last Seen	Time the device last reported to BigFix, shown relative to now (for example, *9 minutes ago*).
Computer ID	Unique BigFix identifier.
Result	Action result (for example, Success, Failure).
Status	Fixlet state (for example, Failed, Fixed).
Completed	Yes if the device finished successfully.
OS	Operating system version.
Type	Device type (for example, Server, Workstation).
IP address	Device IP address.
MAC address	Device network interface MAC address.
DNS name	Fully qualified domain name (FQDN).

Components tab

The **Components** tab appears on the Deployment Details page when you view a **Multiple Action Group (MAG)** deployment. BigFix creates a Multiple Action Group whenever you deploy two or more Fixlets or Tasks together in a single remediation. The parent deployment acts as a container action, and each member action carries the Multiple Action Group ID as its parent action ID.

Use the **Components** tab to track the status, failure rates, and details of all member actions in the group.



The Components tab offers the following controls:

Table 36. Components tab - controls

Control	Description
Density	Adjusts the row height of the components table. Choose **Compact**, **Standard**, or **Comfortable**.
Search by Deployment name box	Filters the member actions table by name. The list updates automatically as you type.
Count line	Shows the total number of member actions in the group (for example, *13 Components*).
Column chooser	Customizes which columns the table displays.

Columns:

Table 37. Components tab - columns

Column	Description
#	Index number of the member action.
Name	The name of the member action, which is the Fixlet title. Select the name link to open the **Component Details** page.
Failure Rate	The failure rate, or count, of endpoints where this member action failed. You can sort this column in ascending or descending order.

Component Details page

Select any member action link in the **Components** table to open the **Component Details** page. This drill-down page gives you granular visibility into the execution script, applicability relevance, source Fixlet metadata, and targeted endpoints for that member action.

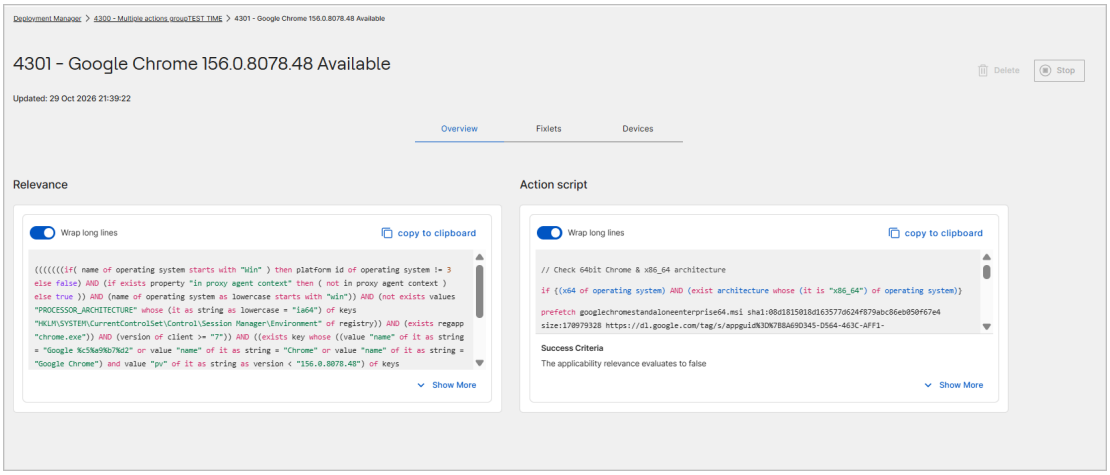
The breadcrumb at the top of the page reflects the full hierarchy: **Deployment Manager** > *[parent MAG ID] - [parent deployment name]* > *[member action ID] - [member action name]*. For example, **Deployment Manager** > *4300 - Multiple actions groupTEST TIME* > *4301 - Google Chrome 156.0.8078.48 Available*.

The page header displays the member action ID and title, the last updated timestamp, and the **Delete** and **Stop** buttons in the upper-right corner.

The Component Details page provides three tabs:

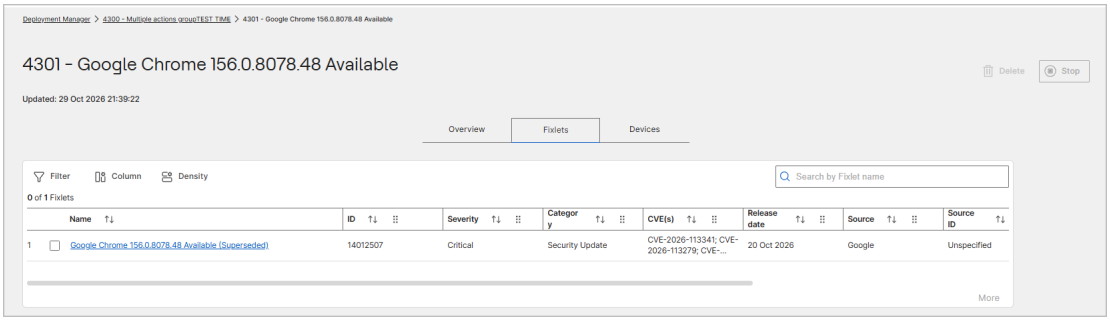
Overview tab

- **Relevance card**: Displays the relevance expression for the member action, with a **Wrap long lines** toggle, a **copy to clipboard** button, and a **Show More** / **Show Less** expansion link.
- **Action script card**: Displays the action script that runs for this member action, with a **Wrap long lines** toggle, a **copy to clipboard** button, a **Show More** / **Show Less** expansion link, and the defined **Success Criteria** (for example, *The applicability relevance evaluates to false*).



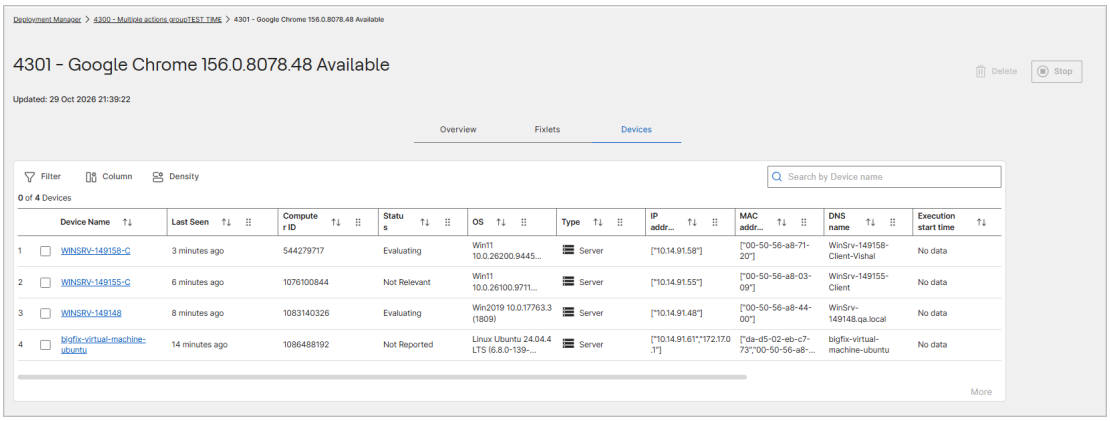
Fixlets tab

- Lists the source Fixlet associated with this member action.
- Includes the **Filter**, **Column**, and **Density** toolbar controls.
- Includes a **Search by Fixlet name** box and an item counter (for example, *0 of 1 Fixlets*).
- Columns: checkbox, **Name**, **ID**, **Severity**, **Category**, **CVE(s)**, **Release date**, **Source**, and **Source ID**.



Devices tab

- Displays all endpoints targeted by this member action.
- Includes the **Filter**, **Column**, and **Density** toolbar controls.
- Includes a **Search by Device name** box and a selection counter (for example, *0 of 4 Devices*).
- Columns: checkbox, **Device Name**, **Last Seen**, **Computer ID**, **Status** (for example, Evaluating, Not Relevant, Fixed, Failed, Not Reported), **OS**, **Type**, **IP address**, **MAC address**, **DNS name**, and **Execution start time**.



Related information

Deployments *(on page 181)*

Managing Tags *(on page 51)*

BigFix Software Distribution on the BigFix UI

BigFix Software Distribution (SWD) on the BigFix UI (BFUI) is a centralized, enterprise-grade solution for deploying and managing software across all endpoints in your network — providing full control, audit visibility, and end-user self-service through a modernized web interface.

Note: The **Software** page will be visible only if the `Software Distribution` site is licensed and enabled.

Overview

Software Distribution lets you create software packages that can be deployed to managed endpoints. It is available from the **Explorer > Software** menu in BigFix UI. You can also view and deploy pre-built Fixlets created for some common softwares. Moreover you can create configuration tasks for BigFix Self Service Application.

Entitlement

Required:

- Software Distribution entitlement on the BigFix license.
- Optional Software Installer Library for Windows and/or Software Installer Library for macOS entitlements to access pre-built Fixlets.

Check: **Settings > Licensing** shows the entitlement as active.

User permissions

Required role

Software Package application access.

Administrator to access also to the Configure Self Service Application page.

Required scope

Access to a custom site.

Optional access to the `Software Installer Library for Windows` and/or `Software Installer Library for macOS` sites to access pre-built Fixlets.

Prerequisites

BigFix UI installed and connected to the BigFix Server.

Full documentation

To know more about BigFix SWD for BigFix UI, refer to Software Distribution for BigFix UI in the Lifecycle portal.

Related

BigFix Lifecycle Documentation Homepage

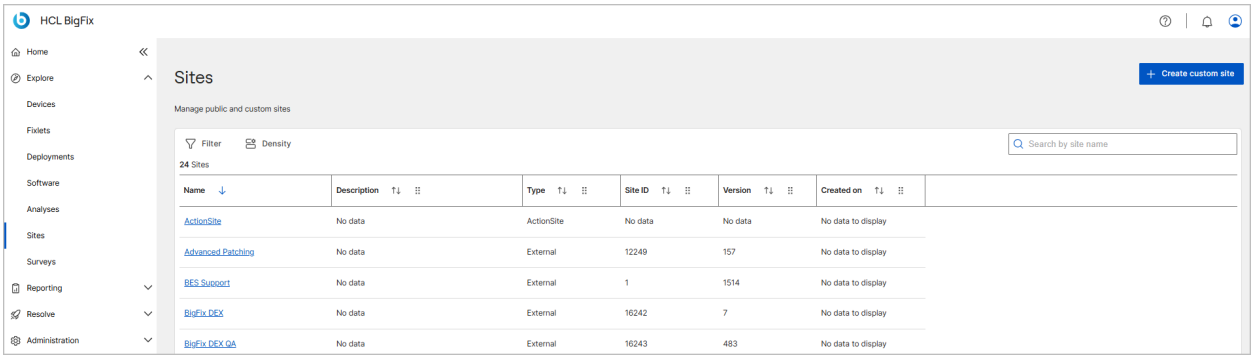
Sites

The Sites page is the central workspace for viewing and managing the BigFix sites in your deployment. Use it to review every public and custom site, check how many devices are subscribed to each site, and create custom sites to host your own content.

A BigFix site is a collection of content, such as Fixlets, tasks, and analyses, that is created by you, by HCL, or by other vendors. Devices subscribe to a site, and the BigFix client on each subscribed device evaluates the content of that site.

To open the **Sites** page, go to **Explore > Sites**. The page header shows the page title, the subtitle **Manage public and custom sites**, and the **Create custom site** button in the upper-right corner. A counter above the data grid, such as **15 Sites**, shows the total number of sites in the list.

Note: Your role controls access to the Sites application. If your role does not allow the application, the **Sites** entry does not appear in the navigation bar.



Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to this application. Site Management is a default application, so every role has at least view access to it. See Managing Roles *(on page 467)*.
- Your role defines the sites that you can access and your permission level on each one, such as Owner, Writer, or Reader. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete, such as creating a custom site. For a description of each permission, see Permissions reference *(on page 482)*.

Site types

The Sites page lists all the site types in your deployment.

Table 38. Site types

Type	Description
ActionSite	The master action site of the deployment. It hosts the content that master operators create. You cannot delete the ActionSite or edit its details.
External	A content site that HCL or another vendor publishes and that BigFix gathers from an external source, such as **BES Support** or **Patches for Windows**. You cannot edit or delete an external site, but users with the required permission can manage its device subscriptions.
Custom	A site that you create in your deployment to organize and host your own content. Users with the required permission can edit the description of a custom site, manage its device subscriptions, add custom content, and delete the site. See Creating a custom site *(on page 203)* and Managing a custom site *(on page 205)*.
Operator	The site that a non-master operator owns and that hosts the content that the operator creates.

Toolbar

The toolbar above the data grid controls how the list of sites appears.

Table 39. Toolbar controls

Control	Description
Filter (funnel icon)	Displays a subset of sites based on criteria that you define, such as a condition on the site name. The active filter combines with any text that you type in the search box. For more information, see Table filter *(on page 40)*.
Density	Adjusts the row spacing of the data grid. Select **Standard** (default), **Compact**, or **Comfortable**.
Search by site name	Filters the list as you type a site name. If you apply a filter, the search combines your text with the filter criteria.
Create custom site	Opens the **Site details** panel to create a custom site. See Creating a custom site *(on page 203)*.

Data grid columns

Each row in the data grid represents one site. Each column header includes a sort icon. Select it once to sort ascending, again to sort descending, and again to clear the sort. Use the handle icon on a column header to reorder the columns. The grid contains the following columns.

Table 40. Sites data grid columns

Column	Description
Name	The name of the site. Select the name to open the site detail page *(on page 197)*, which shows the Fixlets, analyses, and subscribed devices of the site.
Description	The description of the site. For a custom site, this is the text that you entered when you created or last edited the site.
Type	The site type, such as **ActionSite**, **External**, or **Custom**. See Site types *(on page 195)*.
Site ID	The unique numeric identifier that BigFix assigns to the site. For example, the **BES Support** site has Site ID `1`.
Version	The current version of the site content. The version increases each time BigFix updates or gathers the site content.
Subscribed devices	The number of devices that are currently subscribed to the site. Open the site and select the **Subscribed devices** tab to see the device list. See Subscribed devices tab *(on page 201)*.
Created on	The date and time when the site was created, such as **22 Jul 2026 at 06:18**. This value appears for custom sites only.

Note: When a value is not available for a site, the cell shows **No data** or **No data to display**.

Related information

Site detail page *(on page 197)*

Creating a custom site *(on page 203)*

Managing a custom site *(on page 205)*

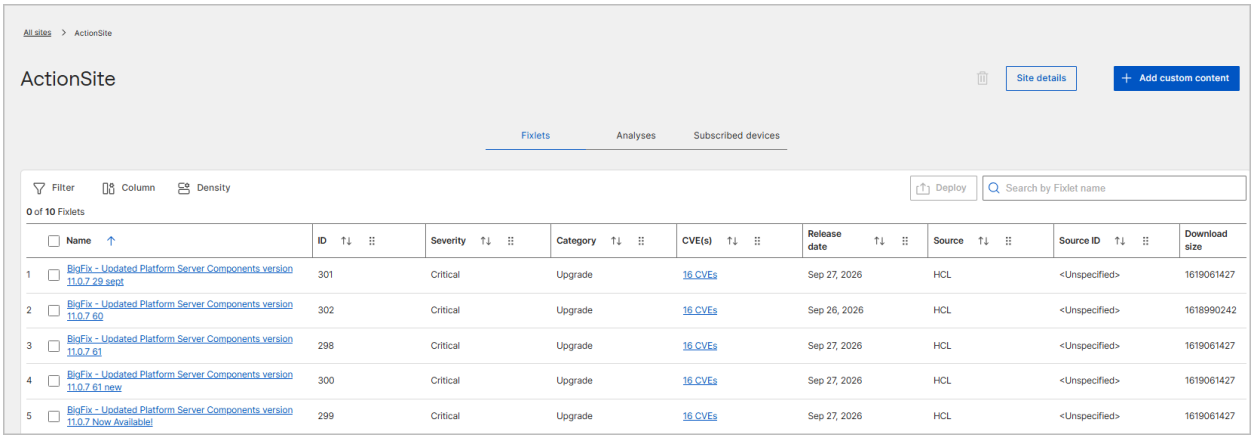
Adding custom content to a site *(on page 206)*

Managing Filters *(on page 35)*

Site detail page

The site detail page shows the content and the subscribed devices of a single site. Use it to review the site properties, deploy Fixlets, work with analyses, manage device subscriptions, and add custom content.

To open a site detail page, go to **Explore > Sites** and select a site name. A breadcrumb trail (**All sites** > site name) at the top of the page returns you to the **Sites** page. See Sites *(on page 194)*.



Page header

The header shows the site name and the following controls.

Table 41. Page header controls

Control	Description
Delete icon (trash can)	Deletes the site. A confirmation dialog opens before the site is deleted. This option is available only for custom sites and requires the appropriate permission. For all other site types, the option is disabled.

Table 41. Page header controls (continued)

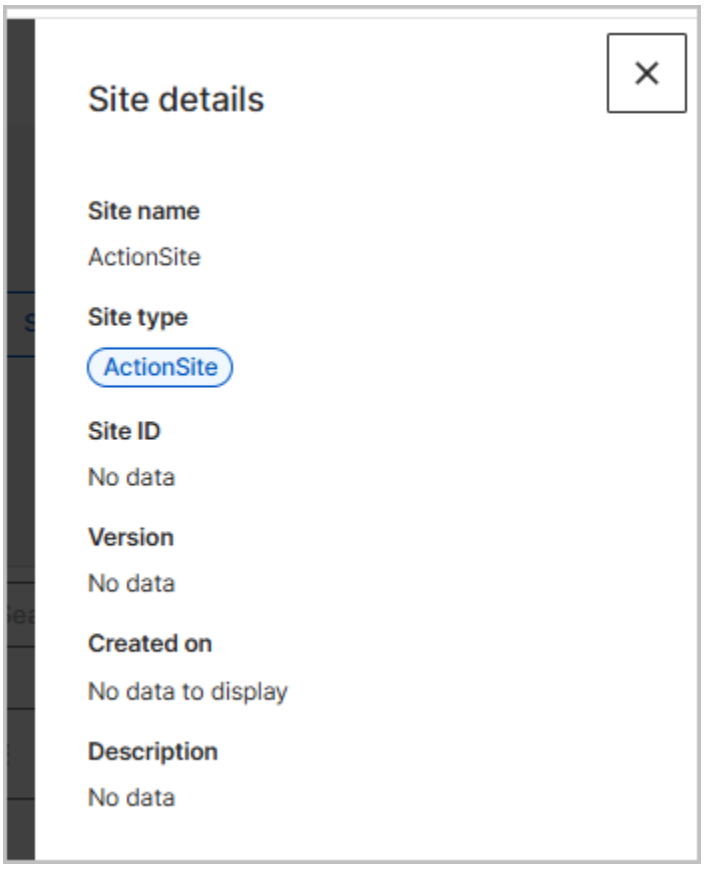
Control	Description
Edit option	Edits the description of the site. This option is available only for custom sites and requires the appropriate permission. You cannot change the site name. For all other site types, the site details are view-only. See Managing a custom site *(on page 205)*.
Site details	Opens the **Site details** panel, which shows the site properties. See Site details panel *(on page 198)*.
Add custom content	Opens the **Create fixlet** wizard to add custom content to the site. This option is enabled only if you have the required access to the site, and your platform permissions allow you to create custom content. See Adding custom content to a site *(on page 206)*.

Site details panel

Select **Site details** to open a panel that shows the following properties. Select the close icon (X) to close the panel.

Table 42. Site details panel fields

Field	Description
Site name	The name of the site. You cannot change the name after you create the site.
Site type	The site type, shown as a badge, such as **ActionSite**, **External**, or **Custom**. See Site types *(on page 195)*.
Site ID	The unique numeric identifier that BigFix assigns to the site.
Version	The current version of the site content.
Created on	The date and time when the site was created. This value appears for custom sites only.
Description	The description of the site. For a custom site, users with the appropriate permission can edit this value.



Fixlets tab

The **Fixlets** tab lists the Fixlets in the site. A counter above the grid, such as **0 of 14 Fixlets**, shows how many Fixlets you selected and the total number in the site. The tab provides the following controls.

Table 43. Fixlets tab controls

Control	Description
Filter	Displays a subset of Fixlets based on criteria that you define.
Column	Chooses which columns appear in the grid. By default, all columns are selected. Clear the check box of a column to hide it, and then select **Apply**.
Density	Adjusts the row spacing of the grid: **Standard** (default), **Compact**, or **Comfortable**.
Deploy	Deploys the selected Fixlets. This button stays dimmed until you select at least one Fixlet check box.
Search by Fixlets name	Filters the list as you type a Fixlet name.

Each column header includes a sort icon. Select a Fixlet name to open its details. The grid contains the following columns.

Table 44. Fixlets grid columns

Column	Description
Name	The title of the Fixlet. Select it to open the Fixlet details.
ID	The unique identifier of the Fixlet in the deployment.
Severity	The severity that the content author assigned to the Fixlet, such as **Critical** or **Low**. If no severity is assigned, the cell shows **<Unspecified>**.
Category	The category of the Fixlet, such as **Upgrade**, **Install**, or **Setup**.
CVE(s)	The Common Vulnerabilities and Exposures (CVE) identifiers that the Fixlet addresses. When a Fixlet addresses multiple CVEs, the cell shows a link with the count, such as **16 CVEs**.
Release date	The date when the source of the Fixlet was released.
Source	The origin of the Fixlet content, such as **HCL** or **Internal**.
Source ID	The identifier that the source assigned to the Fixlet, such as a vendor bulletin number.
Download size	The size of the files that the Fixlet downloads when you deploy it.
Site ID	The unique numeric identifier of the site that hosts the Fixlet.
Type	The type of content, such as **Fixlet** or **Task**.
Relevant Devices Count	The number of subscribed devices on which the Fixlet is relevant.

Note: If the site contains more than 100 Fixlets, select **More** below the grid to load the rest.

Analyses tab

The **Analyses** tab lists the analyses in the site. The tab provides the same **Filter**, **Column**, **Density**, and search controls as the **Fixlets** tab. Select an analysis name to open its details page, where you can activate or deactivate the analysis. The grid contains the following columns.

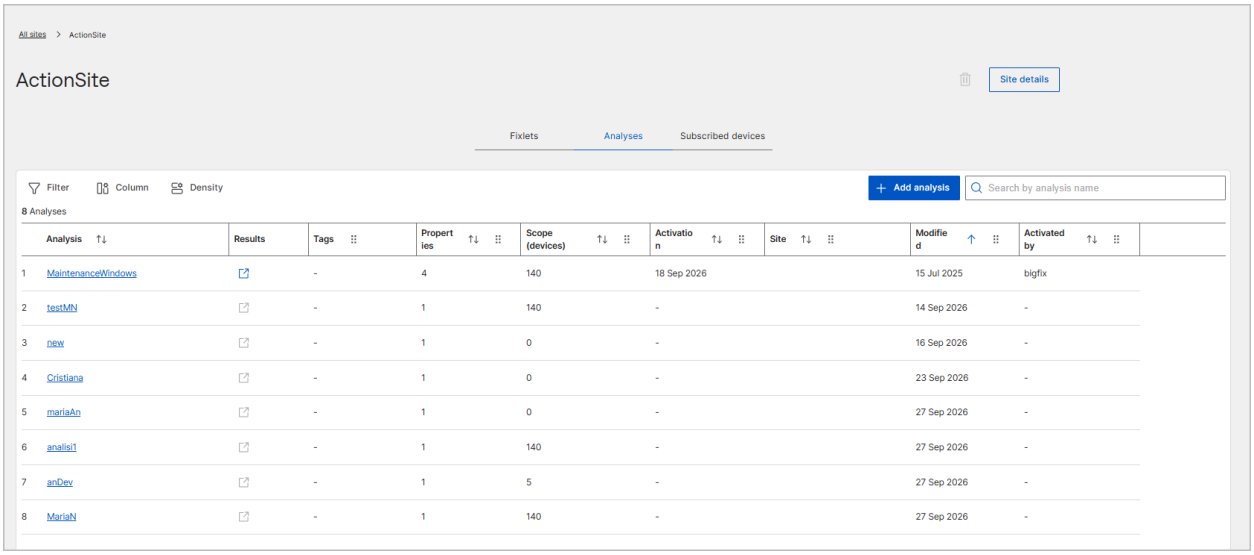


Table 45. Analyses grid columns

Column	Description
Analysis	The name of the analysis. Select it to open the analysis details page.
Results	The results that the analysis reports from the devices on which it is active.
Tags	The tags that are assigned to the analysis.
Properties	The number of properties that the analysis retrieves from the subscribed devices.
Scope (devices)	The devices that are in the scope of the analysis.
Activation	Whether the analysis is active or inactive.
Site	The site that hosts the analysis.
Modified	When the analysis was last modified.
Activated by	The user who activated the analysis.

Note: Only BigFix UI users who are bound to a master operator can globally activate or deactivate an analysis.

Subscribed devices tab

The **Subscribed devices** tab lists the devices that are subscribed to the site. A counter above the grid, such as **0 of 3 Subscribed devices**, shows how many devices you selected and the total number of subscribed devices. The tab provides the same **Filter**, **Column**, and **Density** controls, a search box, and the **Manage subscription** button. The grid contains the following columns.

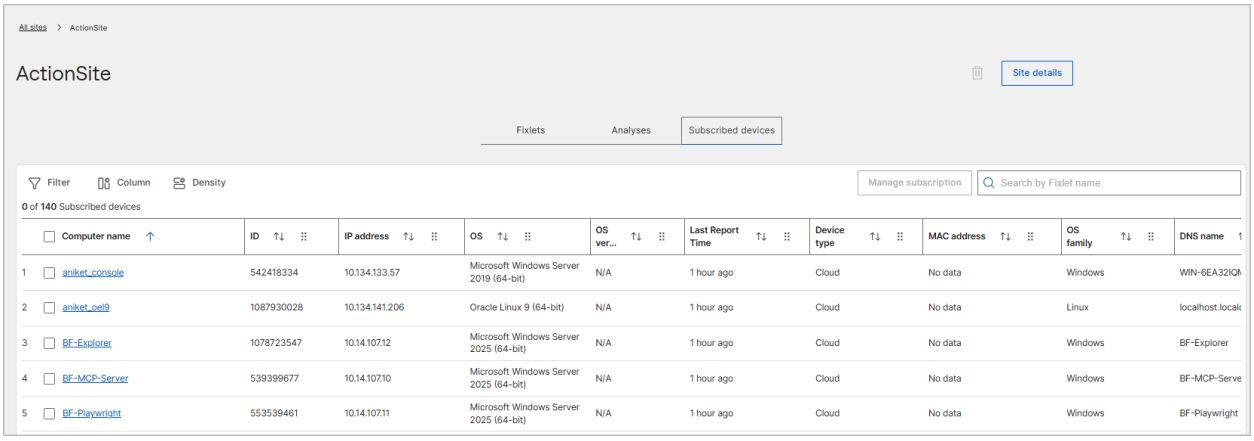


Table 46. Subscribed devices grid columns

Column	Description
Computer name	The BigFix computer name of the device. Select it to open the device details.
ID	The unique BigFix identifier assigned to the device.
IP address	The IP address that the device reported at its last check-in.
OS	The operating system installed on the device, such as **Ubuntu 20.04.6 LTS** or **Windows Server 2022 Standard**.
OS version	The operating system version number.
Last contact	When the device last reported to BigFix.
Status	The status of the device.
Device type	The type of device, such as **Server**.
MAC address	The MAC address of the device network interface.
OS family	The operating system family, such as **Windows** or **Linux**.
DNS name	The DNS name of the device.
Relay	The relay that the device reports through.
Relay name of client	The name of the relay that the BigFix client is assigned to.
BES Relay Selection Method	How the device selects its relay, either automatically or manually.
BES Relay Service Installed	Whether the BigFix relay service is installed on the device.
Distance to BES Relay	The number of network hops between the device and its relay.

Note: The **Manage subscription** option is available only for external and custom sites, and requires the appropriate permission. For the ActionSite, the option is disabled. See Managing a custom site *(on page 205)*.

Note: Subscription changes do not apply in real time. Each client evaluates the subscription criteria and reports back to the server, so the subscribed devices can take a few minutes to appear.

Column display

Note: The columns that appear on each tab depend on your **Column** selection. When a value is not available, the cell shows **No data**.

Related information

Sites *(on page 194)*

Adding custom content to a site *(on page 206)*

Managing a custom site *(on page 205)*

Creating a custom site

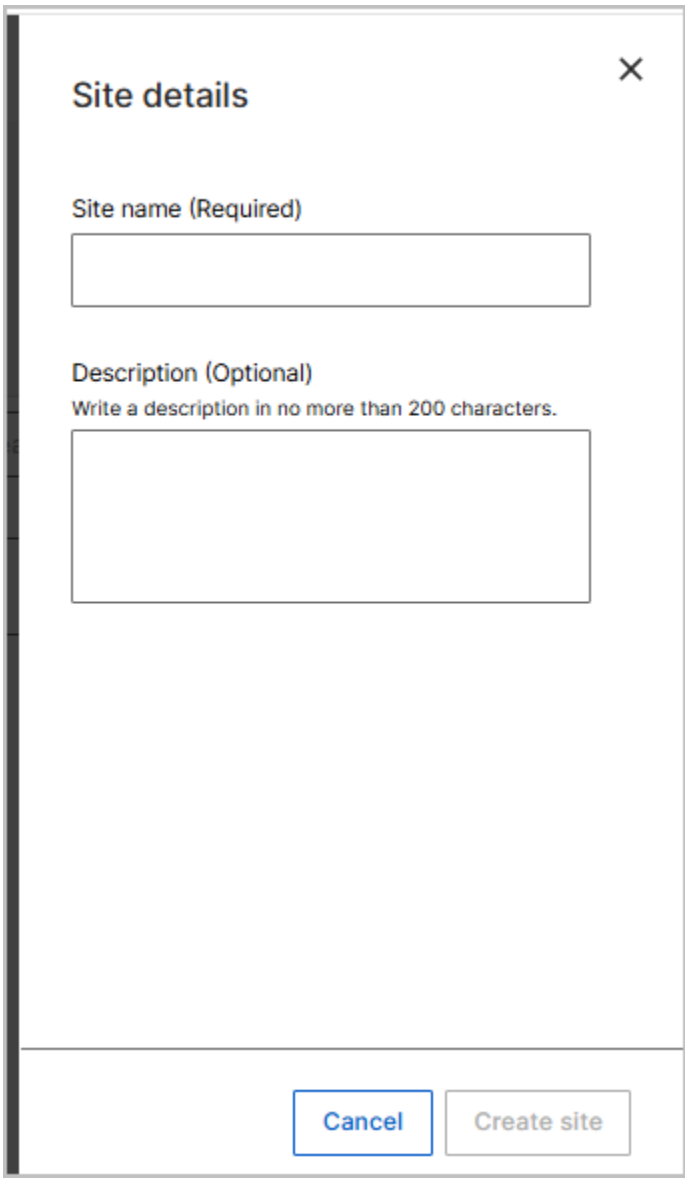
Create a custom site to organize and manage your own content.

You must be a BigFix UI user who is bound to a master operator to create or delete a custom site.

Create a custom site to host your own content, such as Fixlets and analyses, that is pertinent to your network. Custom sites appear on the **Sites** page with the type **Custom**. See Site types *(on page 195)*.

After you create the site, you can add custom content, subscribe devices, and edit the description. You cannot change the site name.

1. Go to **Explore > Sites**.
2. Select **Create custom site**.
   The **Site details** panel opens.



3. In the **Site name** field, enter a name for the site.
   This field is required. You cannot change the name after you create the site.
4. Optional: In the **Description** field, enter a description of no more than 200 characters.
5. Select **Create site**.

The message `Custom site has been successfully created.` appears, and the new site appears on the **Sites** page.

Add custom content to the site and subscribe devices to it. See Adding custom content to a site *(on page 206)* and Managing a custom site *(on page 205)*.

Related information

Sites *(on page 194)*

Site detail page *(on page 197)*

Managing a custom site *(on page 205)*

Adding custom content to a site *(on page 206)*

Managing a custom site

From the site detail page, you can review site properties, add custom content, manage device subscriptions, and delete the site.

You created a custom site. For more information, see Creating a custom site *(on page 203)*.

You must be a BigFix UI user who is bound to a master operator to edit a custom site, manage device subscriptions, activate or deactivate analyses, or delete a custom site.

You perform these tasks on the site detail page. For a description of the page header, the panels, and the tabs, see Site detail page *(on page 197)*.

1. Go to **Explore > Sites**.
2. Optional: Use **Filter** or the **Search by site name** box to find the site.
3. Select the site name to open the site detail page.
4. Perform any of the following management tasks:

Task	Action
Review site properties	Select **Site details** to open the **Site details** panel and review the site name, type, ID, version, creation date, and description. Select the close icon to close the panel. See Site details panel *(on page 198)*.
Edit the site description	Select the edit option in the page header and update the description of the custom site. The change applies immediately. You cannot change the site name or type after you create the site. **Note:** The edit option is available only for custom sites.
Add custom content	Select **Add custom content** and complete the **Create fixlet** wizard. For more information, see Adding custom content to a site *(on page 206)*.

Task	Action
Deploy content	On the **Fixlets** tab, select one or more Fixlets, and then select **Deploy**. See Fixlets tab *(on page 199)*.
Activate or deactivate analyses	On the **Analyses** tab, select an analysis name to open its details page, and activate or deactivate the analysis from there. Activation is global, so the change applies to the whole deployment. The **Activation** and **Activated by** columns show the current state. See Analyses tab *(on page 200)*.
Manage device subscriptions	On the **Subscribed devices** tab, select one or more devices, and then select **Manage subscription**. Device subscriptions use a flat list of conditions - property comparisons, device group membership, or a relevance expression - combined with ALL (AND) or ANY (OR) logic. Nested conditions are not supported. The conditions define a dynamic targeting rule, so any device that meets the criteria is subscribed automatically. Clients can take a few minutes to evaluate the criteria and report back. See Subscribed devices tab *(on page 201)* and Filter by query *(on page 40)*.
Delete the site	Select the delete icon next to **Site details** in the page header, and confirm the deletion in the confirmation dialog. The delete option is available only for custom sites. For other site types, the option is disabled.

Related information

Sites *(on page 194)*

Site detail page *(on page 197)*

Creating a custom site *(on page 203)*

Adding custom content to a site *(on page 206)*

Adding custom content to a site

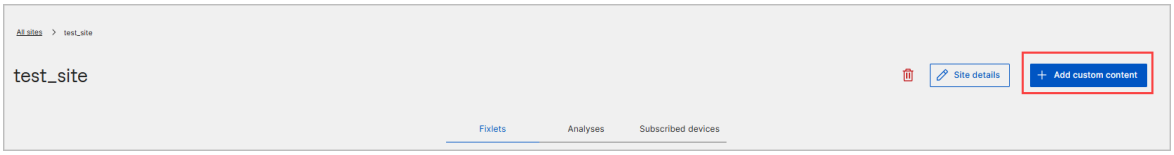
Use the **Create fixlet** wizard to add a custom Fixlet to a site.

The **Add custom content** option is enabled only if you have the required access to the selected site, and your platform permissions allow you to create custom content.

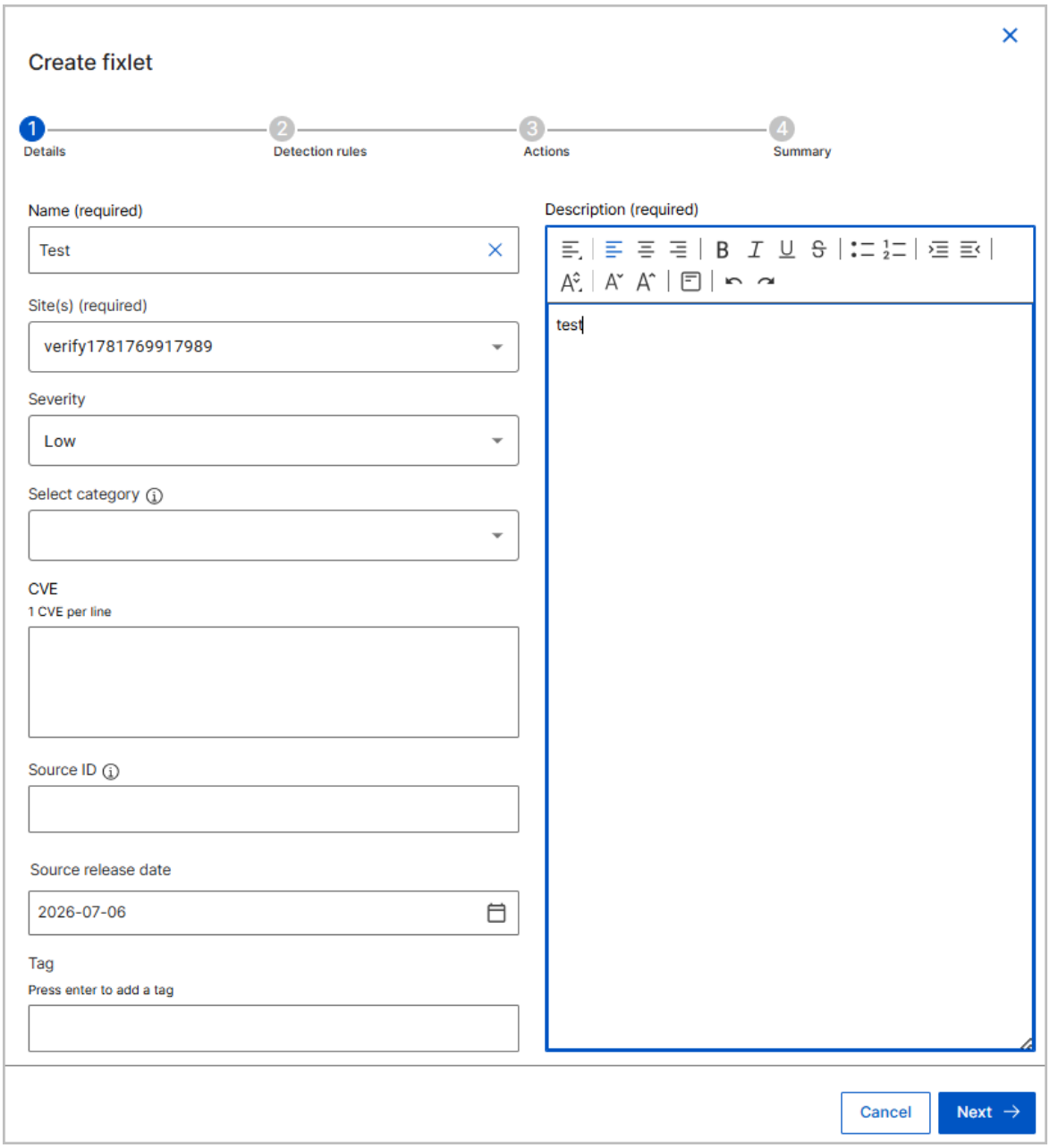
Note: The **Add custom content** option is available only for custom sites.

The **Create fixlet** wizard guides you through four steps, shown in a progress indicator at the top of the wizard: **Details**, **Detection rules**, **Actions**, and **Summary**.

1. Go to **Explore > Sites** and select the site to which you want to add content.



2. Select **Add custom content**.
   The **Create fixlet** wizard opens at the **Details** step.



The **Details** step contains the following fields.

Table 47. Create fixlet - Details step fields

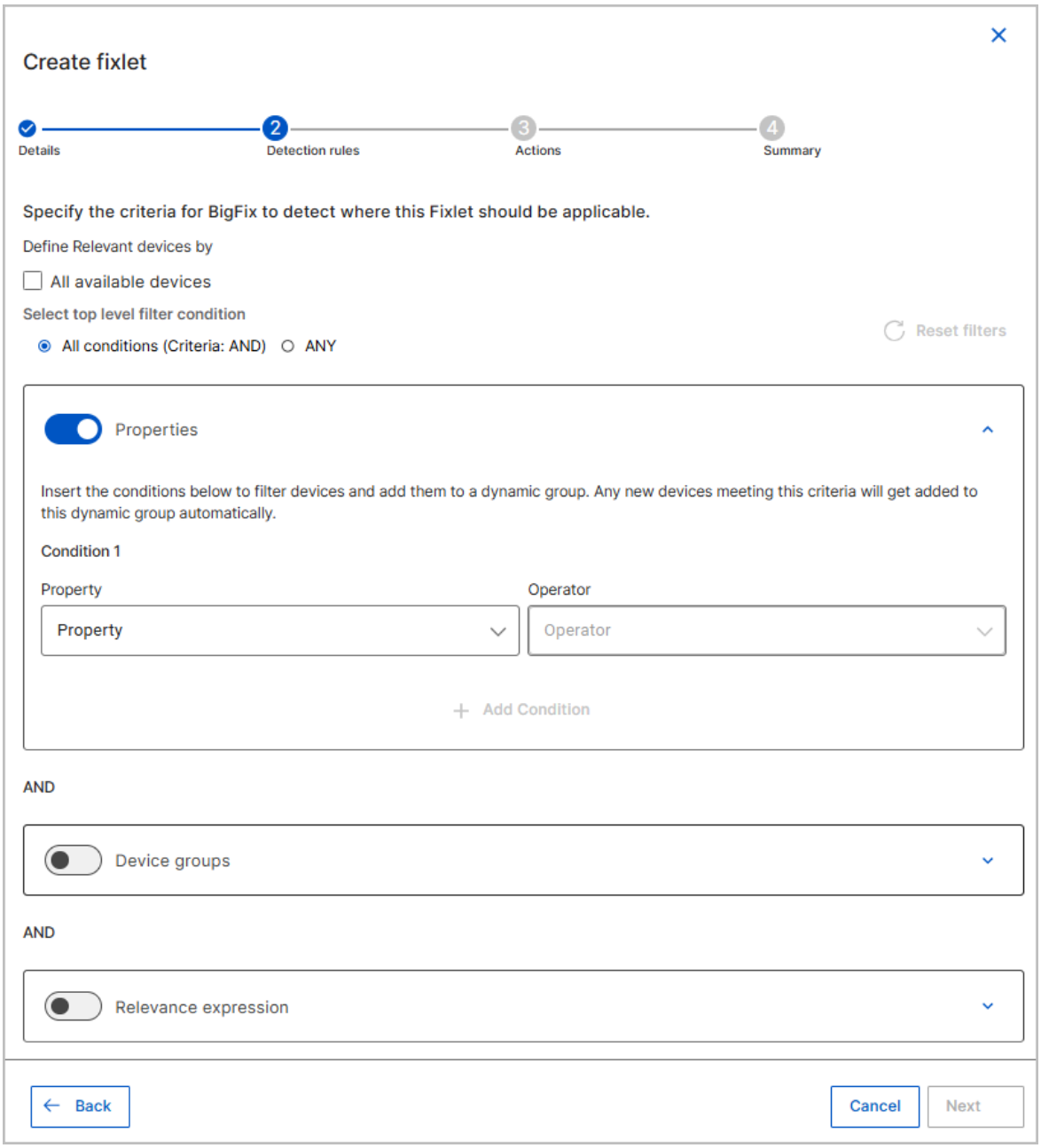
Field	Description
Name	The name of the Fixlet. Required.
Site(s)	The site that hosts the Fixlet. Required. The field is prefilled with the site from which you opened the wizard.
Severity	The severity to assign to the Fixlet, such as **High**.

Field	Description
Select category	The category to assign to the Fixlet, such as **BES Client Setting**.
CVE	The CVE identifiers that the Fixlet addresses. Enter one CVE per line.
Source ID	The identifier that the source assigned to the content, such as a vendor bulletin number.
Source release date	The date when the source of the Fixlet was released. Defaults to the current date.
Tag	One or more tags to assign to the Fixlet. Press **Enter** to add each tag.
Description	The description of the Fixlet. Required. Use the rich-text toolbar to format the text, for example with alignment, bold, italic, underline, strikethrough, lists, and indentation.

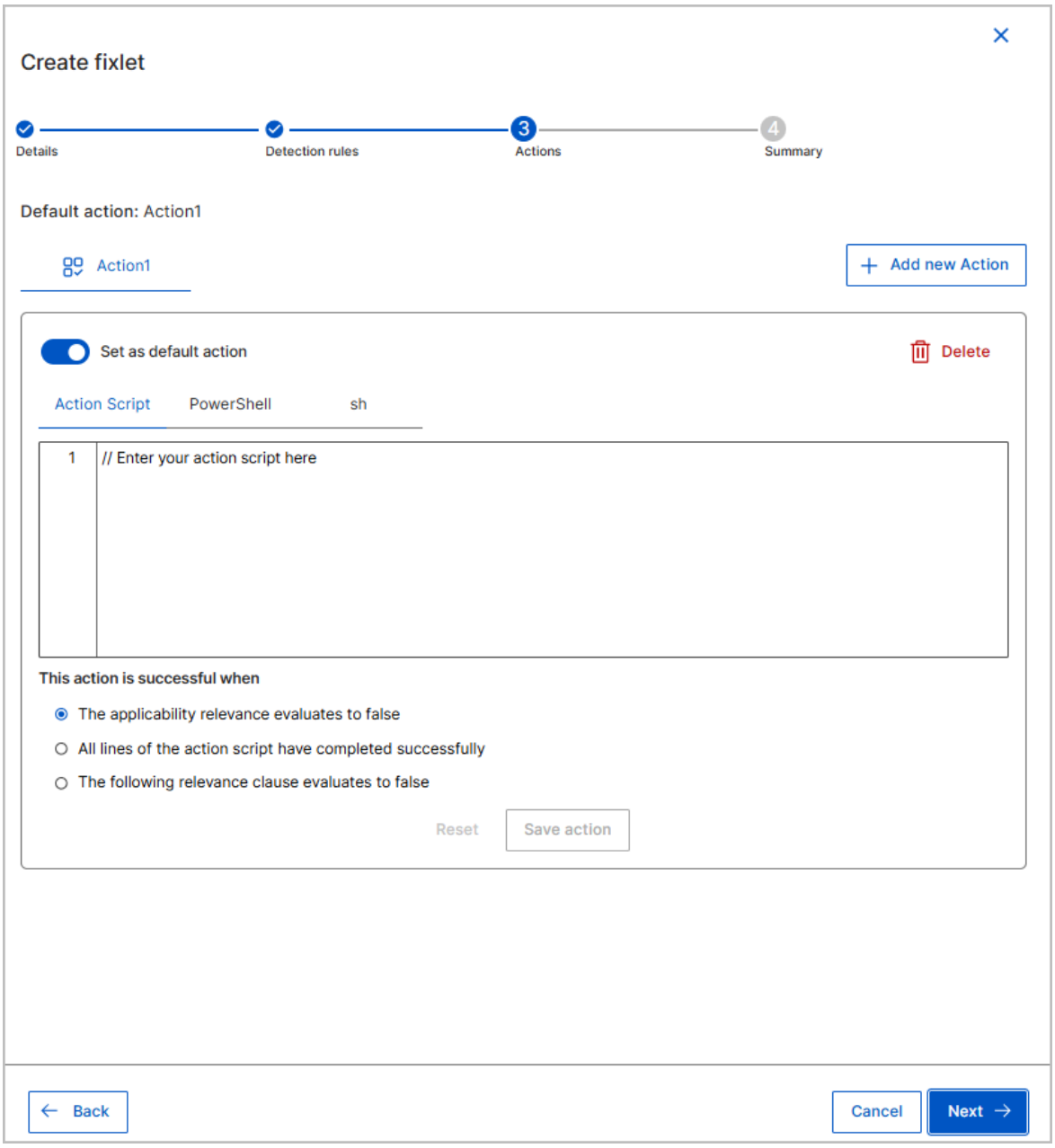
3. On the **Details** step, complete the fields and select **Next**.
    a. In the **Name** field, enter a name for the Fixlet (required).
    b. Verify the site in the **Site(s)** field (required).
    c. Optional: Select a **Severity** and a category from the **Select category** list.
    d. Optional: In the **CVE** field, enter CVE identifiers, one CVE per line.
    e. Optional: Enter a **Source ID**, a **Source release date**, and one or more **Tag** values. Press **Enter** to add a tag.
    f. In the **Description** editor, enter a description (required). You can format the text with the rich-text toolbar.

4. On the **Detection rules** step, specify the criteria that BigFix uses to detect where the Fixlet is applicable, and select **Next**.
    - To target every device, select the **All available devices** check box.
    - To target devices by property, turn on the **Properties** toggle, then define each condition by selecting a **Property**, an **Operator**, and a **Value**. Select **Add Condition** to add more conditions.
    - To target existing device groups, turn on the **Device groups** toggle.
    - To target devices with a relevance expression, turn on the **Relevance expression** toggle.

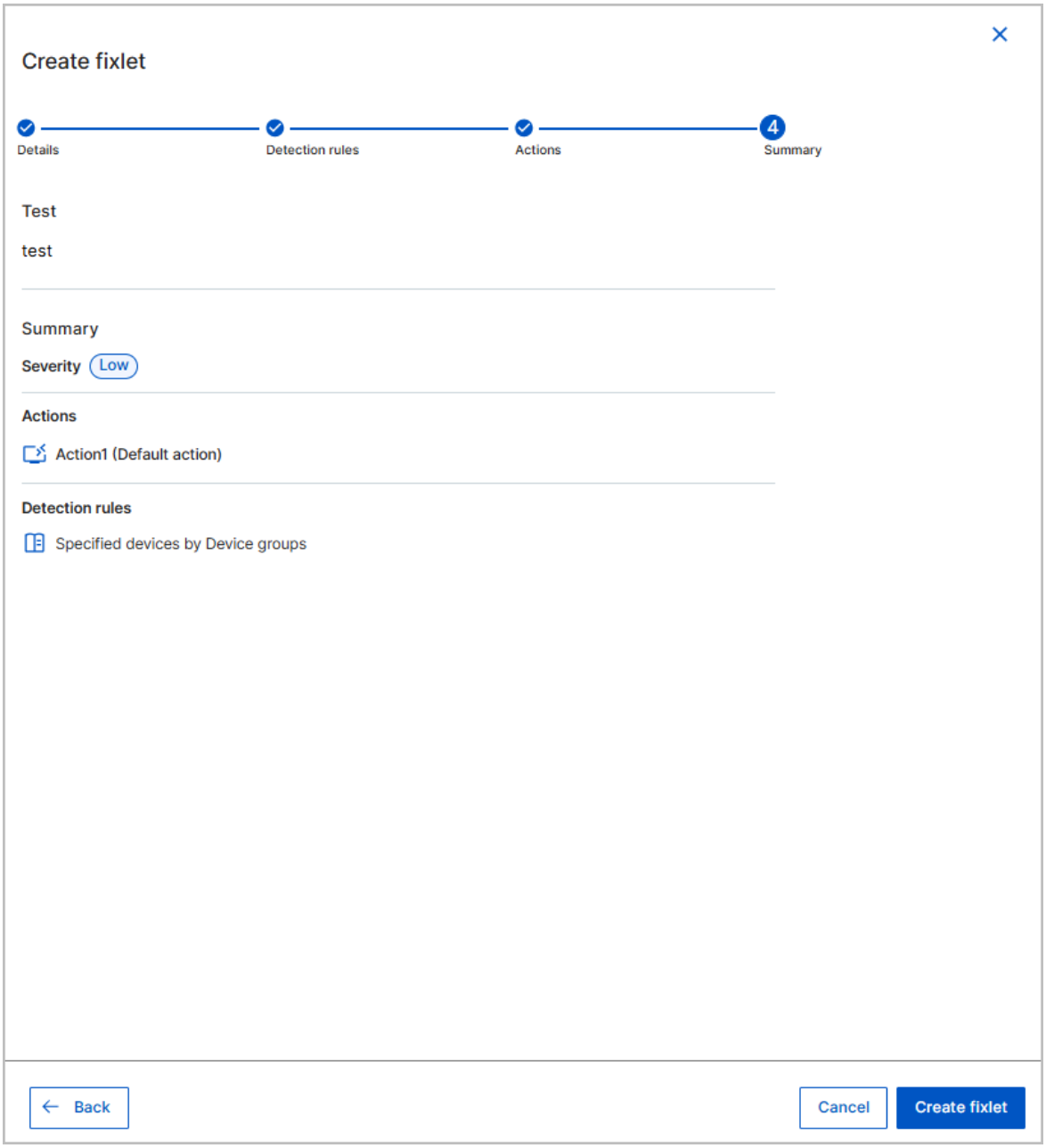
    Use the top-level filter condition to combine the criteria. Select **All conditions (Criteria: AND)** to require every criterion, or **ANY** to require at least one. To clear the criteria, select **Reset filters**.



5. On the **Actions** step, define one or more actions and select **Next**.
    a. Select the script type: **Action Script**, **PowerShell**, or **sh**.
    b. Enter the action script in the editor.
    c. Under **This action is successful when**, select one of the following success criteria: **The applicability relevance evaluates to false**, **All lines of the action script have completed successfully**, or **The following relevance clause evaluates to false**.
    d. Select **Save action**.
    e. Optional: Select **Add new Action** to define another action. Use the **Set as default action** toggle to choose the default action.


Create fixlet
Details
Detection rules
3
Actions
4
Summary
Default action: Action1
Action1
Add new Action
Set as default action
Delete
Action Script
PowerShell
sh
1
// Enter your action script here
This action is successful when
The applicability relevance evaluates to false
All lines of the action script have completed successfully
The following relevance clause evaluates to false
Reset
Save action
Back
Cancel
Next

6. On the **Summary** step, review the Fixlet details, actions, and detection rules, and then select **Create fixlet**.



The message `Your custom fixlet has been successfully created.` appears, and the Fixlet appears on the **Fixlets** tab of the site. See Fixlets tab *(on page 199)*.

Related information

Sites *(on page 194)*

Site detail page *(on page 197)*

Creating a custom site *(on page 203)*

Managing a custom site *(on page 205)*

Surveys

The Surveys page lets you create and track surveys that collect feedback from endpoint users about their digital experience. Use it to review every survey, check its status and score, and deploy a survey to devices.

A survey asks endpoint users a question about their digital environment. Star rating surveys feed the sentiment score. Single choice and multiple choice surveys collect qualitative feedback only.

To open the page, expand **Explore** in the side navigation, and then select **Surveys**. The page header shows the time of the last update, and a counter above the data grid, such as **22 Surveys**, shows the total number of surveys.

Note: Devices can answer a survey only if the BigFix Self-Service Application is installed and the **Survey** tab is enabled.

Entitlement

- **Required:** BigFix Workspace / BigFix DEX entitlement enabled on the BigFix license.
- **Check:** Navigate to **Settings > Licensing** to verify that the DEX entitlement status shows as active.

User permissions

- **Required role:** DEX Operator, Workspace Operator (or Master Administrator).
- **Required scope:** Read/manage access to target Devices, Device Groups, and DEX Dashboards within the BigFix UI.

Prerequisites

- BigFix UI installed, configured, and connected to the BigFix Server.
- BigFix Scanner and the DEX Scanner Plugin deployed to target managed endpoints.
- BigFix Self Service Application version 3.4.4.
- Target endpoints subscribed to the relevant DEX sites and actively collected metrics (CPU/memory usage, crash reports, boot/login times).

Full documentation

Full feature documentation: Survey management

Related

BigFix Workspace

Analyses

The Analyses app lets you collect and review device data in BigFix. Use it to create analyses, define the devices they apply to, and manage the properties that each analysis reports.

An analysis is a collection of one or more properties that BigFix evaluates on the devices that fall within the analysis scope. Use analyses to gather information from devices, such as service status, installed software, or configuration values, and to view the results centrally. Together, these values give you a current view of your environment without deploying an action.

To open the app, expand **Explore** in the side navigation, and then select **Analyses**.

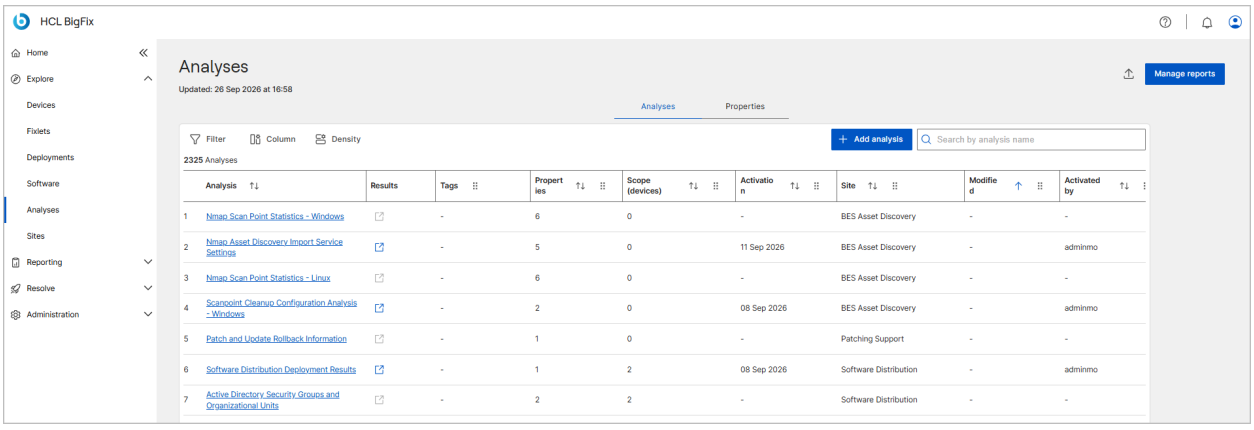
Note: The **Analyses** app is a default app, so it is automatically included in your assigned role. The analyses that you can see, and your ability to create, edit, or delete them, depend on your operator visibility and permissions. Without custom content permissions, you cannot create, edit, or delete analyses. Editing or deleting an analyses also requires write access to the site that hosts it. Analyses that are hosted on external sites cannot be edited or deleted; analyses on custom sites can be edited and deleted.

Key benefits

- Gather device data on a schedule that you control, from every report to once a day.
- Target only the devices that matter by defining a device scope for each analysis.
- Reuse the collected properties in filters, reports, and device investigations.
- Review all analyses and all properties from a single workspace.

Analyses tab

The page opens on the **Analyses** tab and provides a second **Properties** tab.



The **Analyses** tab lists all analyses that are visible to you, along with the total count. The following table describes the columns:

Table 48. Analyses tab columns

Column	Description
Analysis	The analysis name. Select the name to open the analysis detail page.
Results	A link to the results of the analysis. The results open in the device list, where you can review the values that the devices report for the properties of the analysis. Results are available only when the analysis is activated. If an analysis was activated locally, its results are visible only to the operator who activated it.
Tags	The tags assigned to the analysis. Shows the tag name when one tag is assigned, a count link (for example, *2 tags*) when more than one tag is assigned, or *No data* when no tag is assigned. Select a count link to open the tag drawer, where you can view and remove tags. For more information, see Managing Tags *(on page 51)*.
Properties	The number of properties in the analysis.
Scope (devices)	The number of devices in the analysis scope.
Activation	The time when the analysis was activated.
Site	The site that hosts the analysis.
Modified	The date when the analysis was last modified.
Activated by	The operator who activated the analysis.

From this tab, you can select **Add analysis** to create an analysis, or use the search box to find an analysis by name.

Properties tab

The **Properties** tab lists all retrieved properties in the deployment, along with the total count. The following table describes the columns:

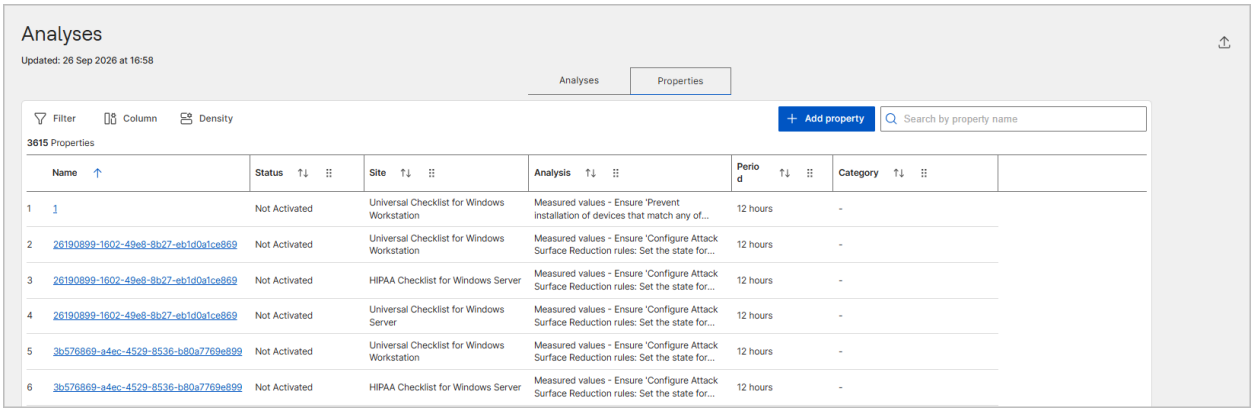


Table 49. Properties tab columns

Column	Description
Name	The property name. Select the name to view or edit the property definition.
Status	The activation status of the property, for example `Not Activated` or `Activated Globally`.
Site	The site that hosts the property.
Analysis	The analysis that the property belongs to.
Period	How often devices evaluate the property, for example `Every Report`, `6 hours`, or `1 day`.
Category	The category of the property, if one is defined.

From this tab, you can select **Add property** to create a property, select a property name to view or edit its definition, or use the search box to find a property by name.

Primary features

- **Add analysis** – Opens a three-step wizard to create an analysis. See Creating an analysis *(on page 220)*.
- **Add property** – Adds a property from the **Properties** tab. See Configuring analysis properties *(on page 234)*.
- **Filter**, **Column**, and **Density** – Narrow the list, choose which columns appear, and set the row spacing. For more information, see Table filter *(on page 40)*, Columns *(on page 29)*, and Density *(on page 29)*.
- **Search** – Finds an analysis by name or a property by name.
- **Export report** and **Manage reports** – Download the table data and save the current view. See Exporting and sharing analysis results *(on page 239)* and Manage Reports *(on page 42)*.
- **Edit analysis** – Reopens the wizard on the details page so that you can change the details, scope, or properties. See Editing and deleting an analysis *(on page 229)*.
- **View results** – Opens the results of an activated analysis in the device list. See Analysis detail page *(on page 217)*.
- **Delete** – Removes an analysis that is hosted on a custom site. See Editing and deleting an analysis *(on page 229)*.

Prerequisites

- Your BigFix operator account must have rights to the site that stores the analysis, such as a custom site or the master action site.
- You need custom content rights to create, edit, or delete an analysis and its properties.
- Reserved properties, such as **Agent Type**, are activated globally and cannot be edited.
- Devices report values only after the analysis is activated and the agent completes its next evaluation.

Related information

Creating an analysis *(on page 220)*

Editing and deleting an analysis *(on page 229)*

Configuring analysis properties *(on page 234)*

Exporting and sharing analysis results *(on page 239)*

Managing Filters *(on page 35)*

Manage Reports *(on page 42)*

Common Functionalities *(on page 28)*

Analysis detail page

The analysis detail page shows the definition of a single analysis: its details, the device scope that determines which devices report on it, and the properties that it evaluates.

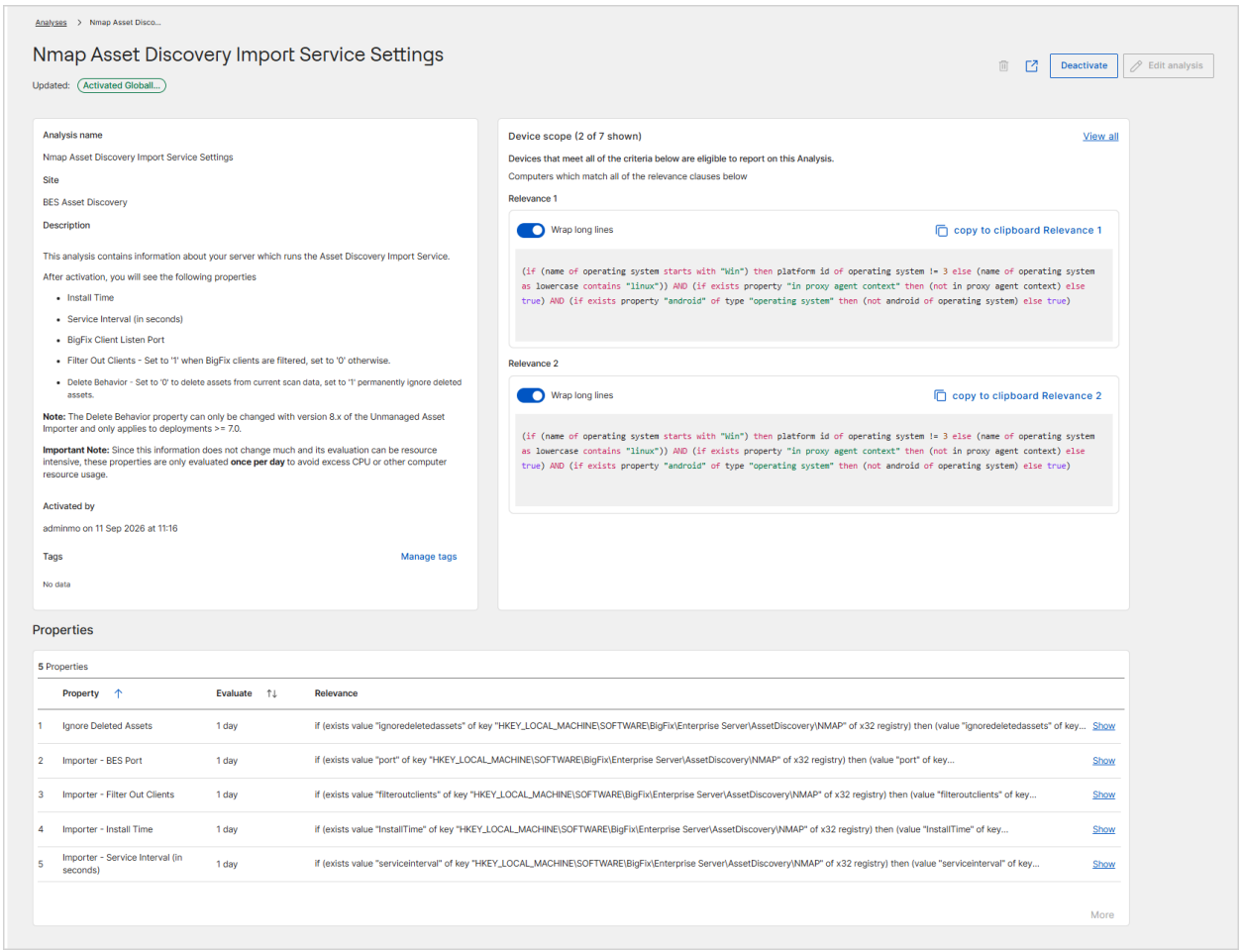
To open the detail page, on the **Analyses** tab, select an analysis name. The page title shows the analysis name, the time of the last update, and a status chip that indicates the activation state, for example `Not Activated`. A breadcrumb at the top of the page returns you to the **Analyses** list.

The actions are in the upper-right corner of the page:

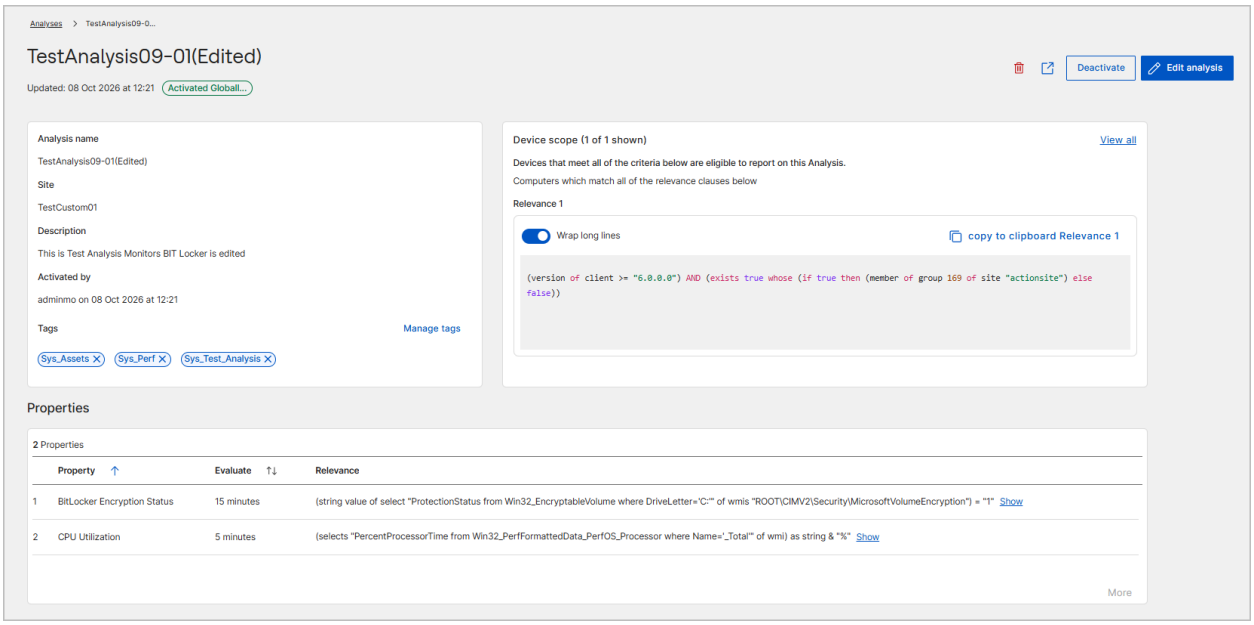
- **Delete** - Removes the analysis from the deployment. Select the delete icon, and then confirm the deletion in the **Delete analysis** dialog. See Editing and deleting an analysis *(on page 229)*.
- **View results** - Opens the results of the analysis in the device list, where you can review the values that the devices report for each property. The icon is enabled only when the analysis is activated. If the analysis was activated locally, the results are visible only to the operator who activated it.
- **Activate** - Activates the analysis so that devices in the scope start to report property values. The button changes to **Deactivate** when the analysis is activated.
- **Edit analysis** - Opens the analysis in the **Edit analysis** wizard, where you can change the details, the device scope, and the properties. See Editing and deleting an analysis *(on page 229)*.

Note: The **Edit analysis** and delete options depend on the type of site that hosts the analyses. Both options are disabled for analyses that are hosted on external sites. Both options are enabled for analyses that are hosted on custom sites, if you have custom content rights and write access to the site.

The following example shows an analysis that is hosted on an external site. The delete icon and **Edit analysis** are dimmed.



The next example shows an analysis that is hosted on the custom site `TestCustom01`. The delete icon and **Edit analysis** are enabled.



Analysis details

The details card shows the following information:

Table 50. Analysis details fields

Field	Description
Analysis name	The name of the analysis.
Site	The site that hosts the analysis.
Description	The description of the analysis, if one was entered.
Activated by	The operator who activated the analysis, and the date and time of the activation. This field is empty until the analysis is activated.
Tags	The tags that are assigned to the analysis. Each tag appears as a chip, for example `Sys_Assets`. Select the close icon on a chip to remove that tag. Select **Manage tags** to open the **Manage tags** drawer and add tags. After you assign or remove tags, the drawer closes and the details card refreshes automatically. If no tag is assigned, the field shows `No data`. For more information, see Managing Tags *(on page 51)*.

Device scope

The **Device scope** panel shows the criteria that determine which devices are eligible to report on the analysis. Devices that meet the criteria report their property values.

Each relevance clause is displayed in a code block. In each block, you can turn on **Wrap long lines** to wrap the expression, select **Copy code** to copy it, or select **Show More** to expand a long expression. When the analysis has

more clauses than the panel shows, the panel heading indicates how many are shown, for example `Device scope (2 of 4 shown)`. Select **View all** to open the **Scope (devices)** panel, where you can view and edit the full scope definition.

Activation

To activate the analysis, select **Activate** at the top of the detail page. You can deactivate an activated analysis from the same page. A confirmation message appears when the analysis is activated or deactivated, and the status chip under the page title is updated. Devices report property values only while the analysis is activated, and the **View results** icon is enabled only when the analysis is activated.

View results

Select the **View results** icon in the upper-right corner of the page to open the analysis results in the device list. The results show the value that each device in the scope reports for every property in the analysis. From there, you can filter the list, choose the columns to display, and export the data. For more information, see Exporting and sharing analysis results *(on page 239)*.

The icon is dimmed until the analysis is activated. If an operator activated the analysis locally, only that operator can view its results.

Properties

The **Properties** section lists the properties in the analysis, along with the total count. Select **More** to view additional properties. The following table describes the columns:

Table 51. Properties columns

Column	Description
Property	The property name.
Evaluate	How often devices evaluate the property, for example `15 minutes` or `7 days`.
Relevance	The relevance expression that produces the property value. Select **Show** to view the full expression.

Related information

Editing and deleting an analysis *(on page 229)*

Exporting and sharing analysis results *(on page 239)*

Managing Tags *(on page 51)*

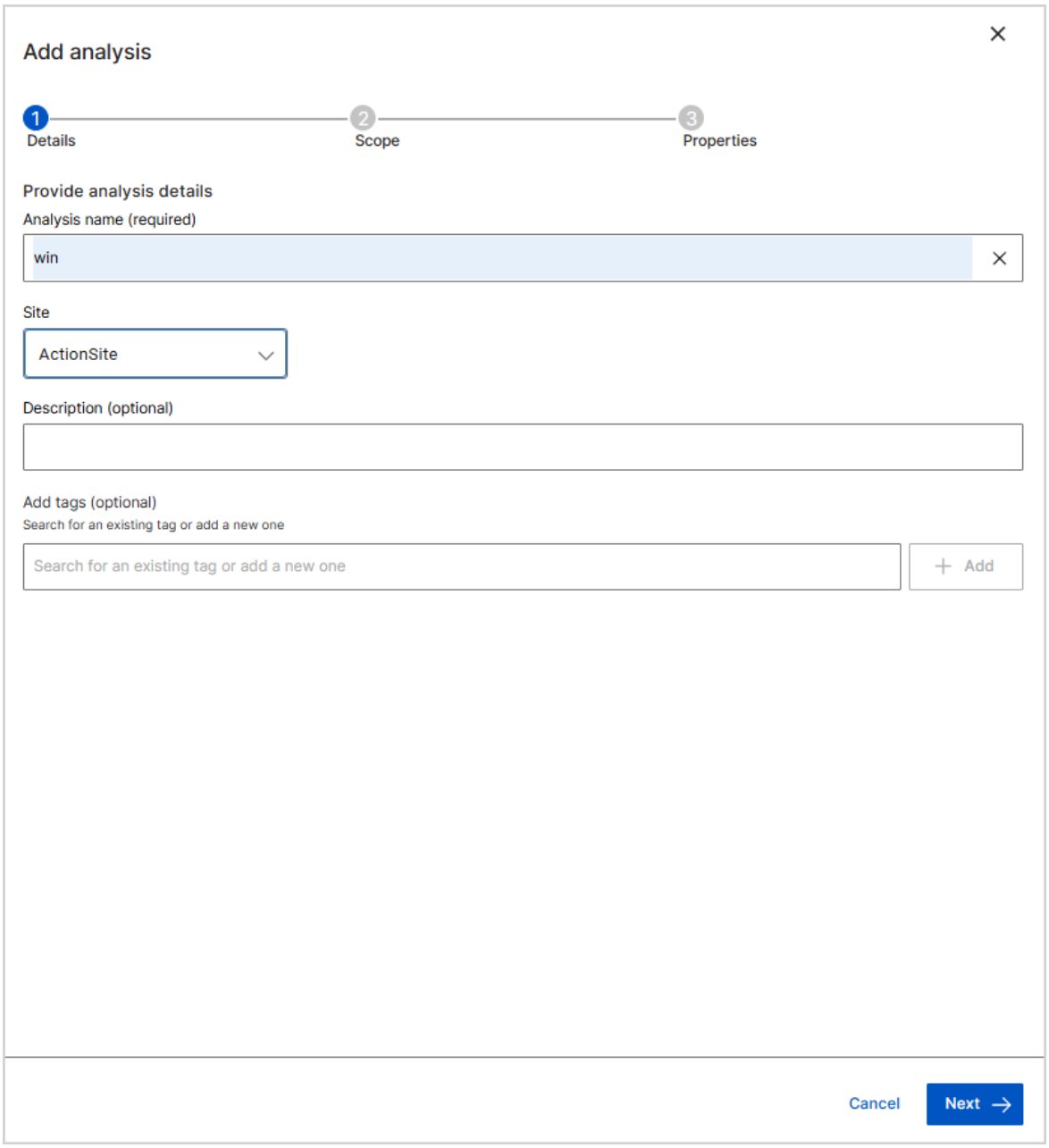
Creating an analysis

Use the **Add analysis** wizard to name an analysis, define the devices it applies to, and add the properties that it reports. You can later edit the analysis, refine its device scope, or assign tags from the analysis detail page.

You need custom content rights and write access to the site that stores the analysis. The sites and properties that you can select depend on your permissions.

The **Add analysis** wizard guides you through three steps: **Details**, **Scope**, and **Properties**.

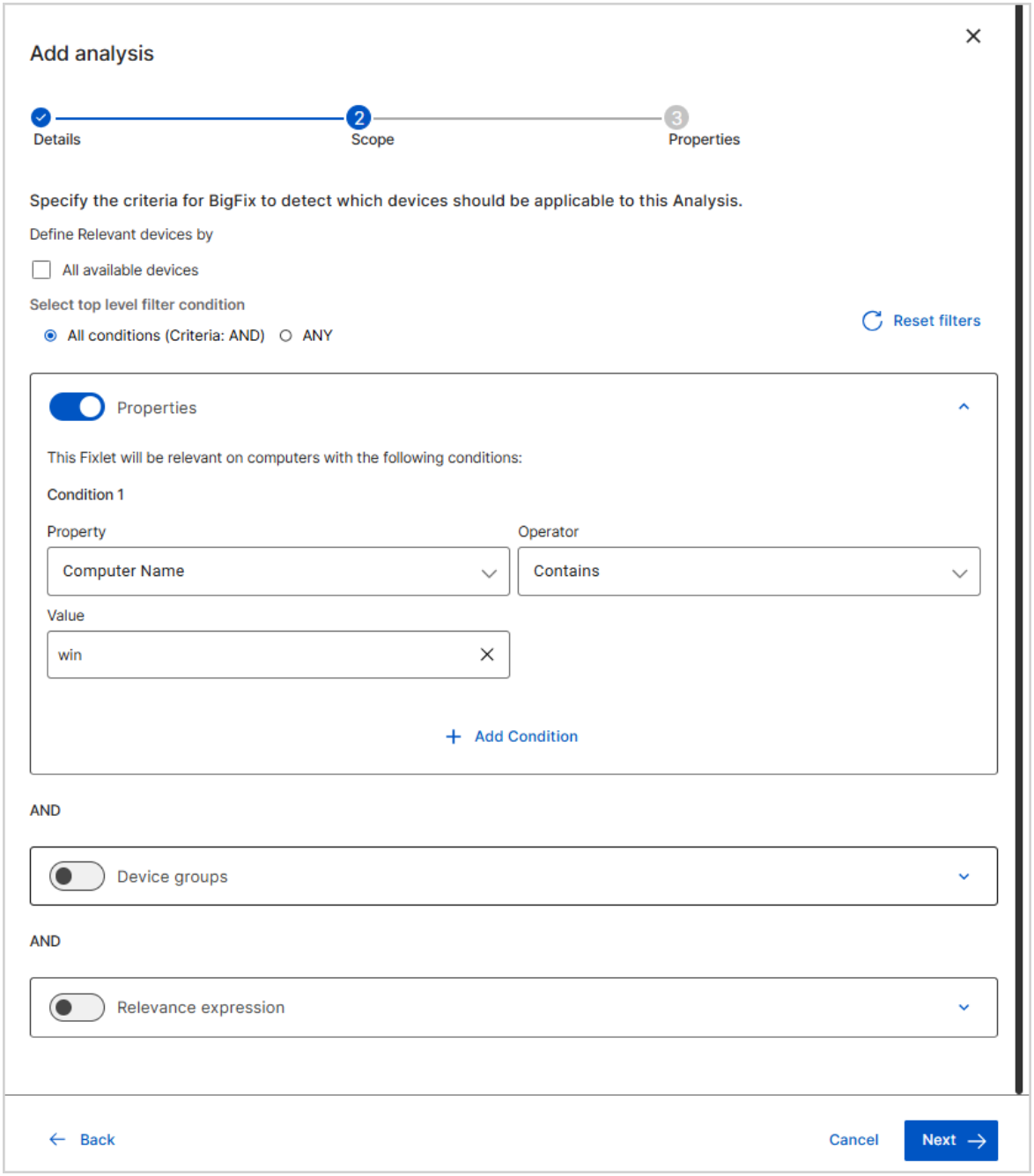
1. Expand **Explore** in the side navigation, and then select **Analyses**.
   The **Analyses** list view opens.
2. Select **Add analysis**.
   The **Add analysis** wizard opens on the **Details** step.
3. Provide the analysis details.



a. In **Analysis name (required)**, enter a name that identifies the data you want to collect.
b. From **Site (required)**, select the site that stores the analysis, such as **ActionSite**.
c. Optional: In **Description**, explain what the analysis collects.
d. Optional: In **Add tags**, search for an existing tag or type a new one, and then select **Add**.

4. Select **Next** to continue to the **Scope** step.

5. Specify the criteria that BigFix uses to detect which devices are applicable to the analysis.



a. To report on every device, select **All available devices**.

b. To target a subset, under **Select top level filter condition**, select **All conditions (Criteria: AND)** or **ANY**.

c. Turn on **Properties**, and then define **Condition 1** by selecting a **Property**, an **Operator**, and a **Value**. Select **Add Condition** to add more conditions.

d. Optional: Turn on **Device groups** or **Relevance expression** to scope the analysis by group membership or by a relevance clause.

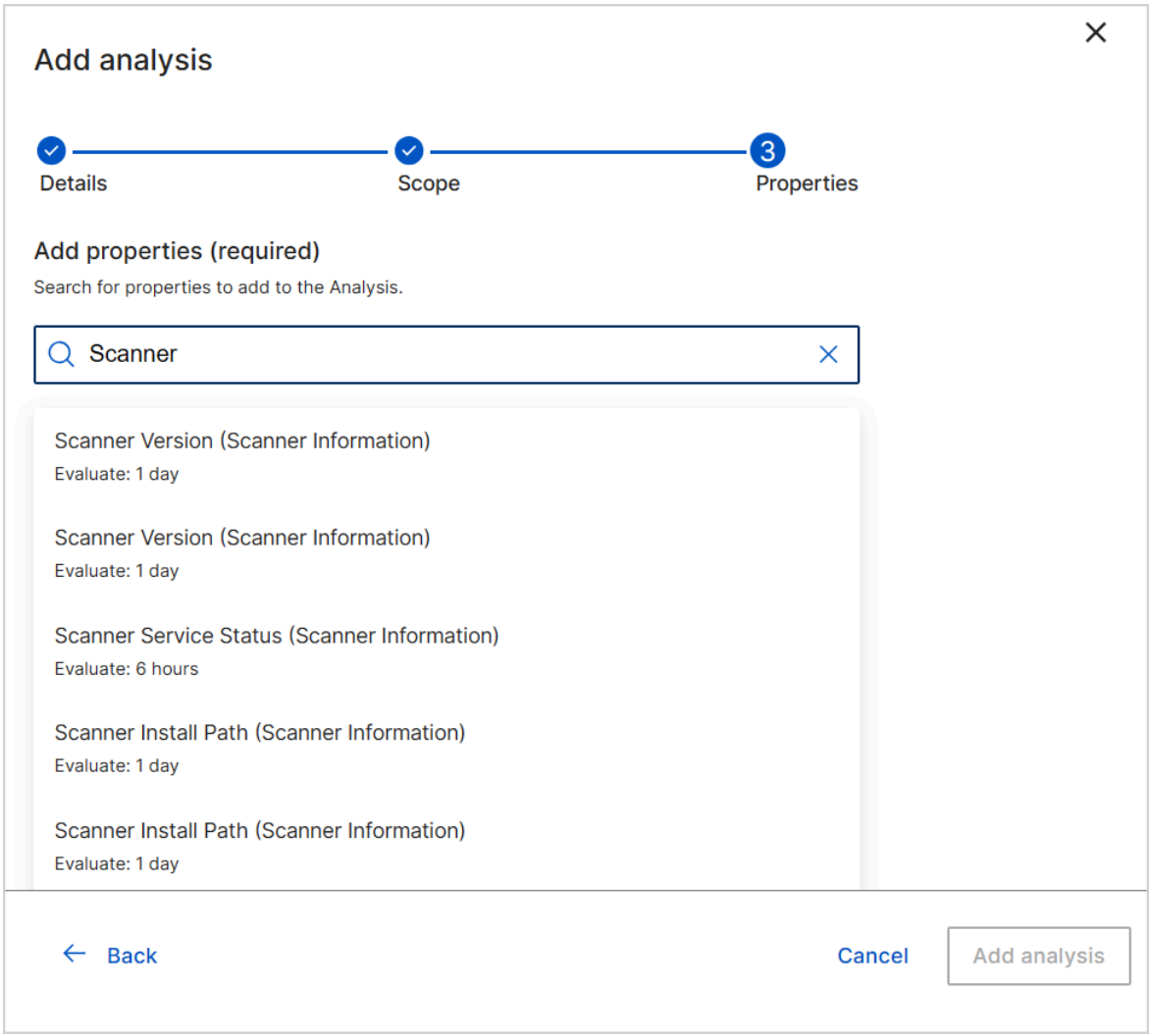
e. Optional: Select **Reset filters** to clear all conditions.

6. Select **Next** to continue to the **Properties** step.
   Select **Back** to return to a previous step.

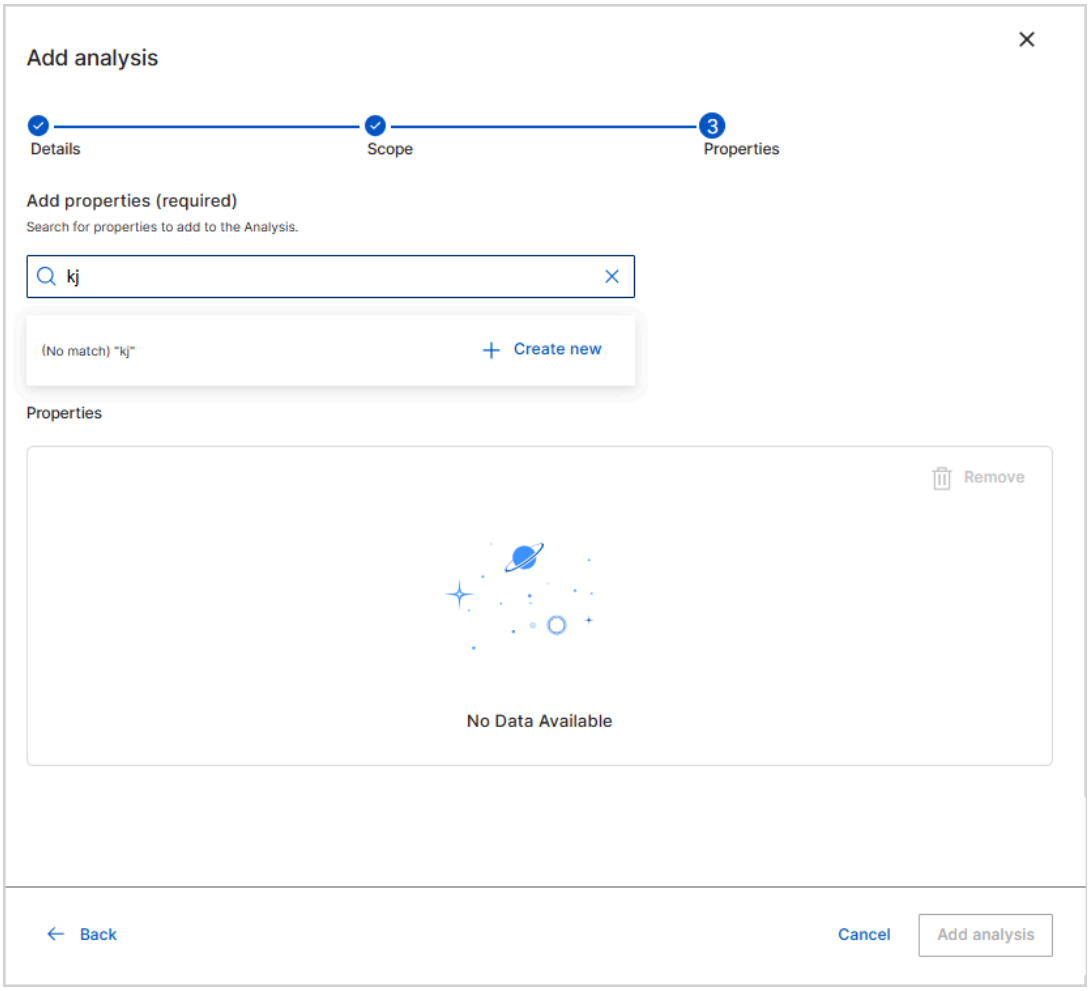
7. In **Add properties (required)**, enter a property name in the search field, and then select a property from the results.

   The results show each matching property with its evaluation period, for example.

   If a property belongs to an analysis, the name of that analysis appears in parentheses after the property name. For example, **Scanner Version (Scanner Information)** is the **Scanner Version** property in the **Scanner Information** analysis. Use the analysis name to tell apart properties that have the same name.

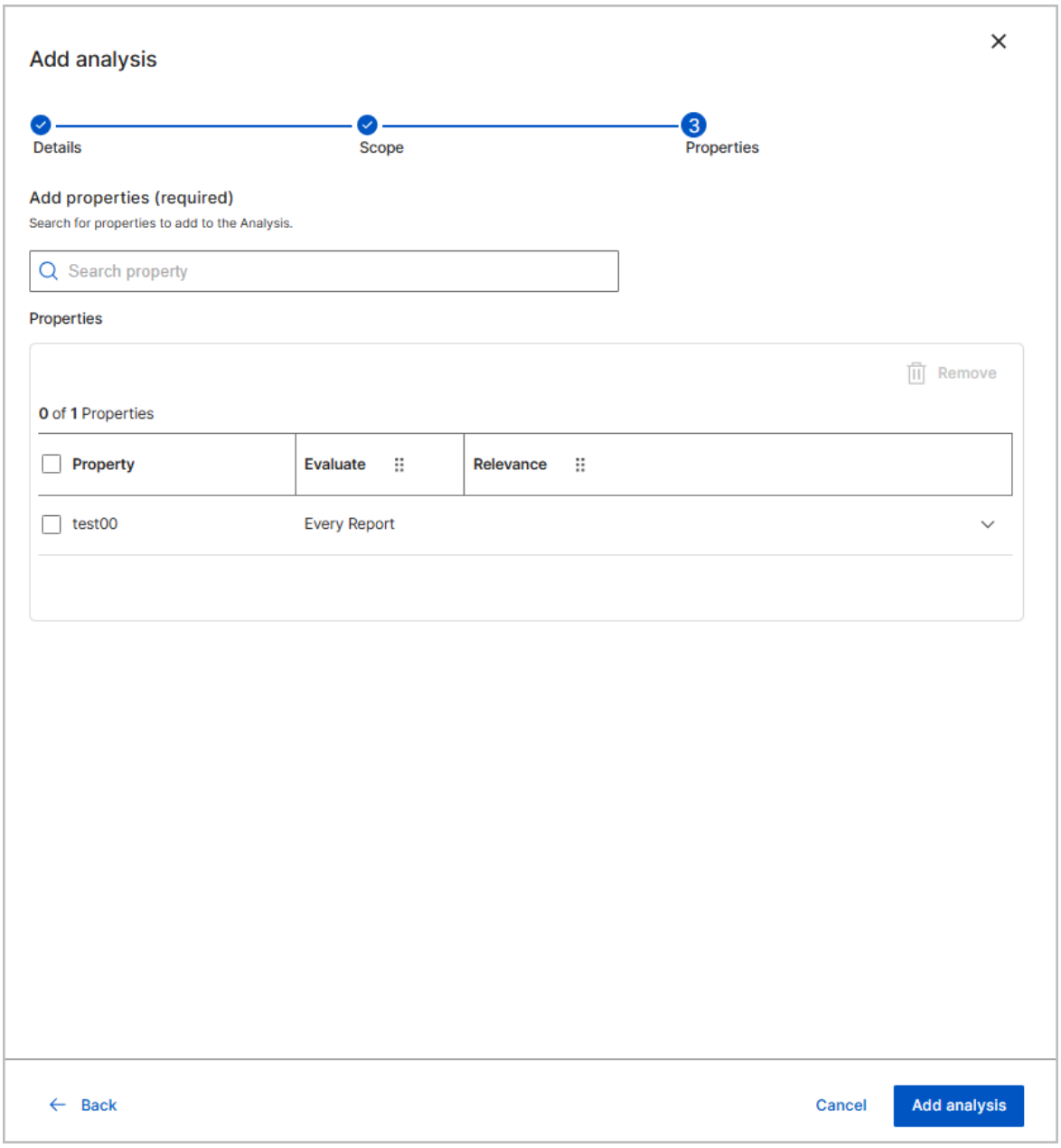


Note: If the search returns **(No match)**, you can create the property without leaving the wizard. Select **Create new**, define the property, and then add it to the analysis.



8. Verify the selections in the **Properties** table.

   The table lists each property with its **Evaluate** period and **Relevance**. Expand a row to review the relevance clause. To remove a property, select its check box and then select **Remove**.



Note: The **Add analysis** button stays dimmed until you add at least one property.

9. Select **Add analysis**.

The message **Analyses created successfully** appears in the upper-right corner, and the analysis appears in the **Analyses** list.



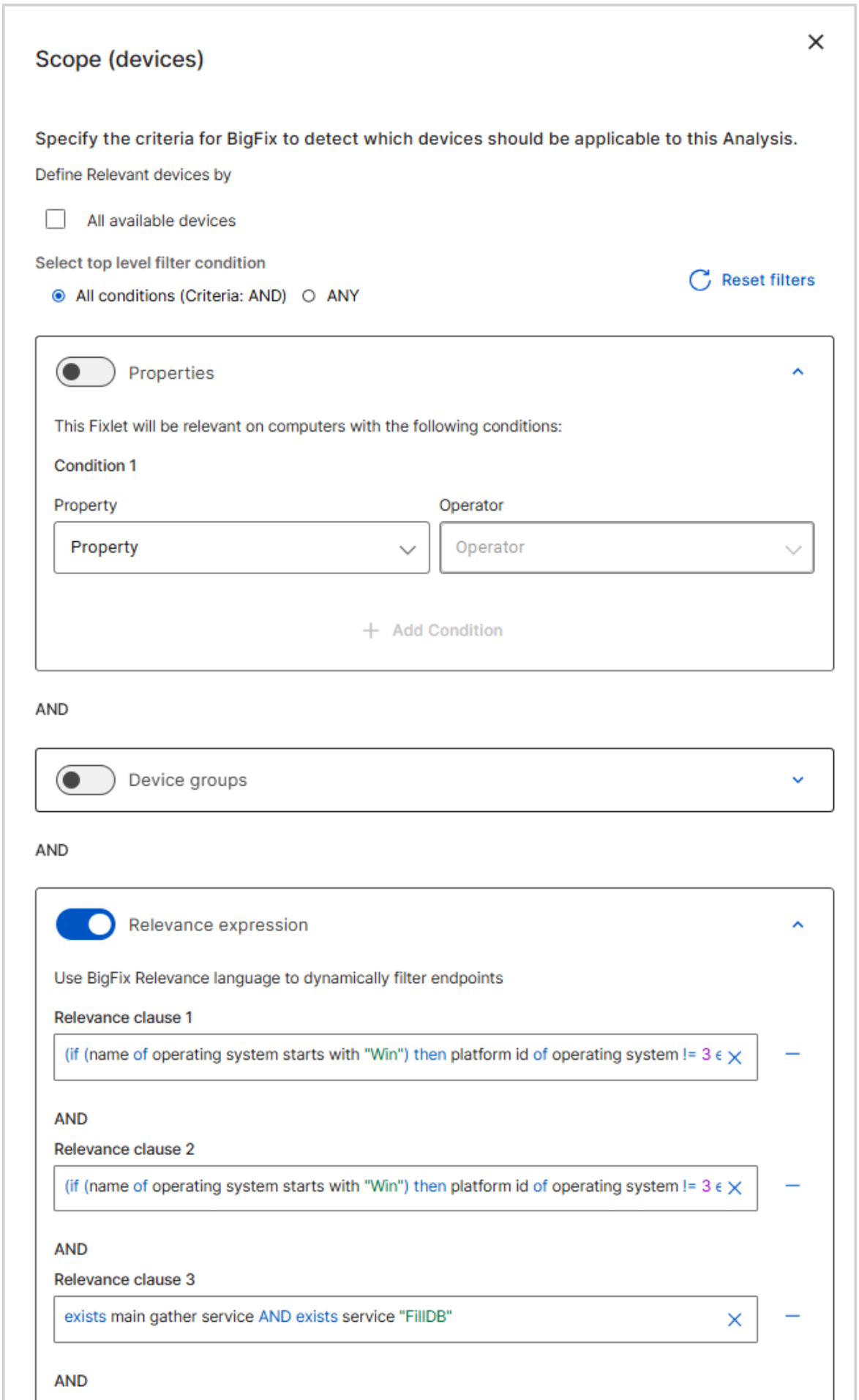
The analysis is saved to the selected site with the state **Not Activated**. Devices report property values after the analysis is activated and the agent completes its next evaluation.

To change the analysis later, open its detail page and select **Edit analysis**. See Editing and deleting an analysis *(on page 229)*.

Note: The **Edit analysis** and delete options depend on the type of site that hosts the analysis. Both options are enabled for analyses that are hosted on custom sites, if you have the required permissions. Both options are disabled for analyses that are hosted on external sites.

After you create an analysis, you can manage it from its detail page:

- To edit the analysis, select **Edit analysis**. The **Edit analysis** wizard opens with the same three steps. You can modify most configuration parameters, but not the hosting site. To delete the analysis, select the delete icon, and then confirm the deletion. See Editing and deleting an analysis *(on page 229)*.
- To view the results of an activated analysis, select the **View results** icon in the upper-right corner of the detail page.
- To view or change the full device scope, in the **Device scope** panel, select **View all**. In the **Scope (devices)** panel, update the criteria, and then select **Save**.


Scope (devices)
Specify the criteria for BigFix to detect which devices should be applicable to this Analysis.
Define Relevant devices by
All available devices
Select top level filter condition
All conditions (Criteria: AND)
ANY
Reset filters
Properties
This Fixlet will be relevant on computers with the following conditions:
Condition 1
Property
Operator
Property
Operator
Add Condition
AND
Device groups
AND
Relevance expression
Use BigFix Relevance language to dynamically filter endpoints
Relevance clause 1
(if (name of operating system starts with "Win") then platform id of operating system != 3 e
AND
Relevance clause 2
(if (name of operating system starts with "Win") then platform id of operating system != 3 e
AND
Relevance clause 3
exists main gather service AND exists service "FillDB"
AND

- To assign tags, next to **Tags**, select **Manage tags**. In the **Manage tags** drawer, search for an existing tag or enter a new one, select **Add**, and then select **Save changes**. The drawer closes, a success message appears, and the **Tags** field updates. For more information, see Managing Tags *(on page 51)*.

Editing and deleting an analysis

Use the **Edit analysis** wizard to change the details, the device scope, or the properties of an analysis. Use the delete icon to remove an analysis that you no longer need.

You need custom content rights and write access to the site that hosts the analysis.

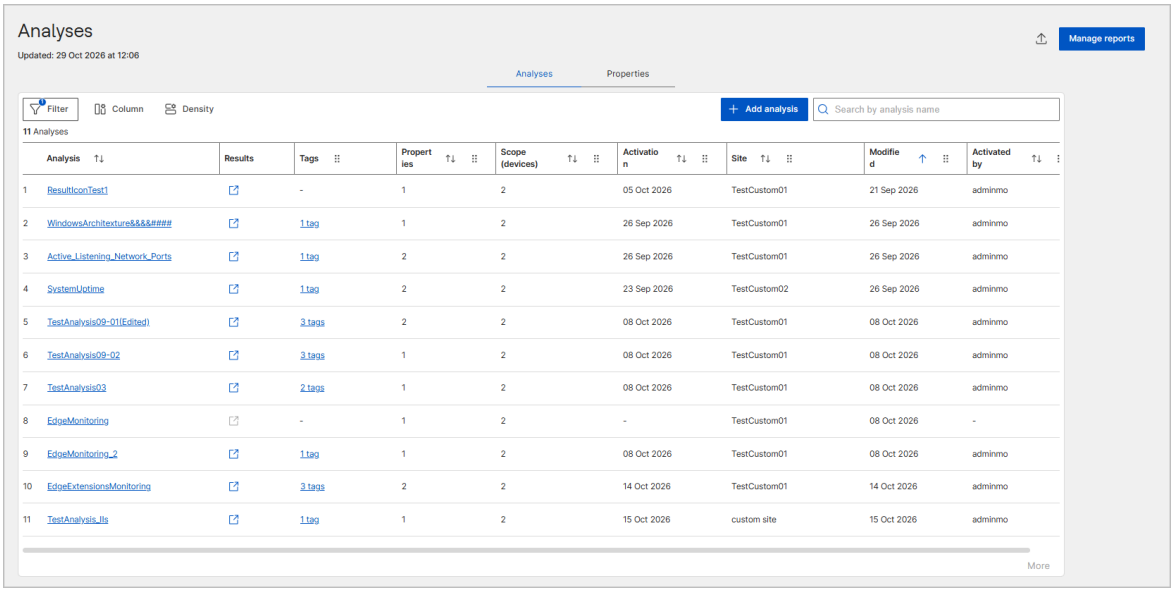
Note: The **Edit analysis** and delete options depend on the type of site that hosts the analysis. Both options are disabled for analyses that are hosted on external sites. Both options are enabled for analyses that are hosted on custom sites, if you have the required permissions.

You edit and delete an analysis from its detail page. The **Edit analysis** wizard uses the same three steps as the **Add analysis** wizard: **Details**, **Scope**, and **Properties**. You can change most configuration parameters, but not the site that hosts the analysis.

1. Expand **Explore** in the side navigation, and then select **Analyses**.
   The **Analyses** list view opens.

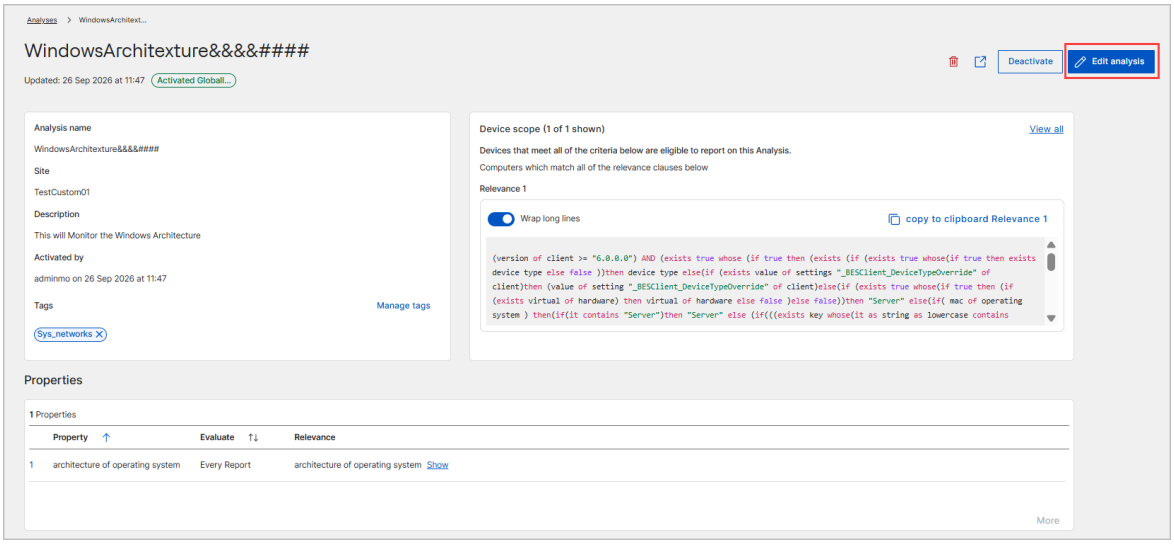
2. Use the table filter to identify the analyses that are hosted on custom sites.

   Above the table, select **Filter** (funnel icon), select the **Site** property and an operator, enter the name of the custom site, and then select **Apply**. The table shows only the analyses on that site, which are the ones that you can edit and delete. For more information, see Table filter *(on page 40)*.



3. Select the name of the analysis that you want to change.

The analysis detail page opens.

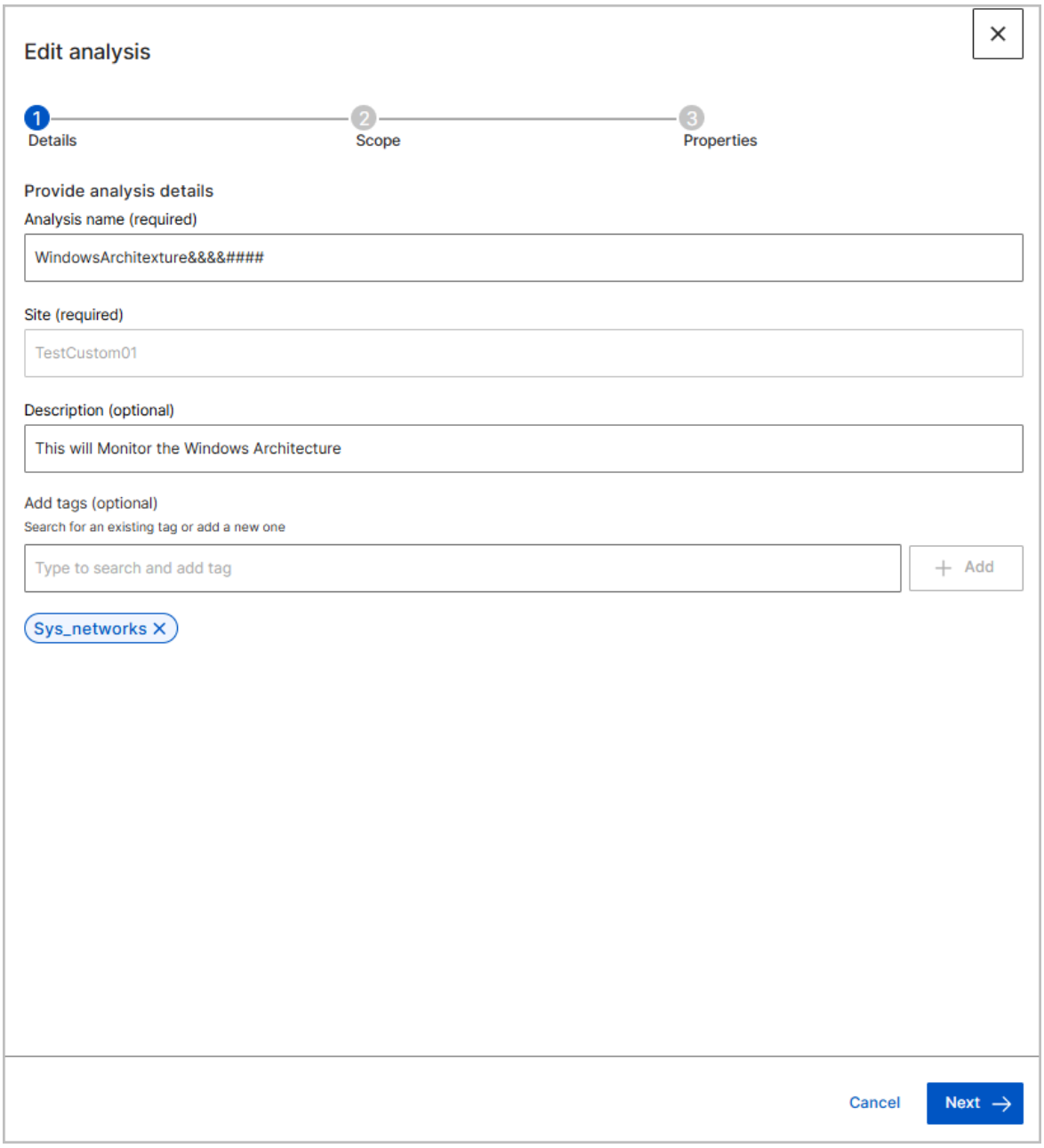


4. In the upper-right corner of the page, select **Edit analysis**.

   If the button is dimmed, the analysis is hosted on an external site or you do not have permission to change it.

   The **Edit analysis** wizard opens on the **Details** step.

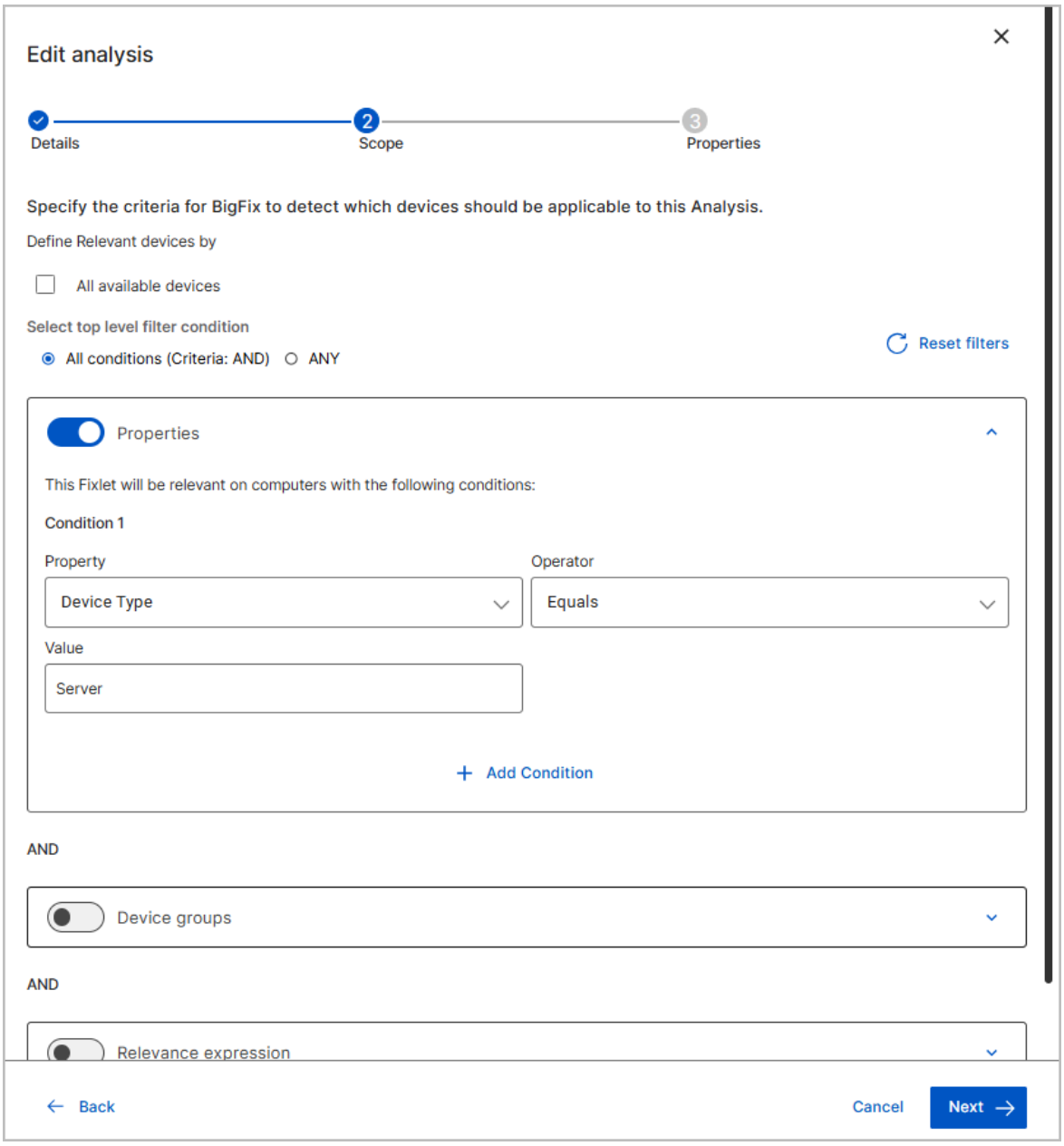
5. On the **Details** step, update the analysis details.



a. In **Analysis name (required)**, change the name.
b. Optional: In **Description**, change the text that explains what the analysis collects.
c. Optional: In **Add tags**, search for an existing tag or type a new one, and then select **Add**.

Note: Site (required) is read only. You cannot move an analysis to another site.

6. Select **Next** to continue to the **Scope** step.

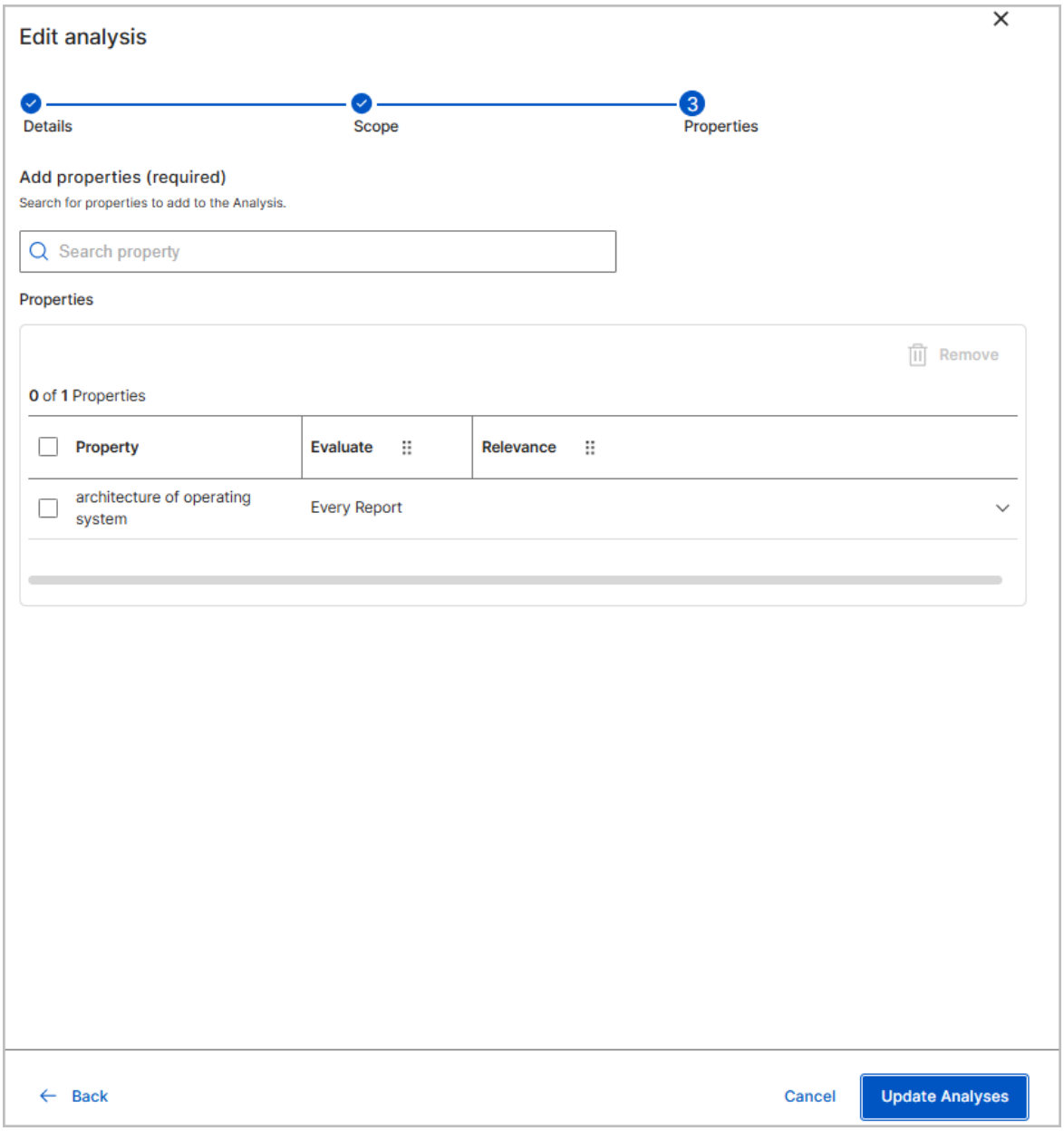


7. On the **Scope** step, update the criteria that BigFix uses to detect which devices are applicable to the analysis.

    a. To report on every device, select **All available devices**.

    b. To target a subset, clear **All available devices**, and then define the filter conditions.
    You can scope the analysis by **Properties**, **Device groups**, or **Relevance expression**. Select **Add Condition** to add more conditions, or **Reset filters** to clear them.

8. Select **Next** to continue to the **Properties** step.



Select **Back** to return to a previous step.

9. On the **Properties** step, update the properties that the analysis reports.
    a. To add a property, enter a property name in **Search property**, and then select a property from the results.
    b. To review a property definition, expand its row in the **Properties** table.
    c. To remove a property, select its check box, and then select **Remove**.

Note: The analysis must keep at least one property.

10. Select **Update Analyses**.

    The message **Analysis Updated successfully** appears, the wizard closes, and the detail page shows the new values.

The analysis is saved with your changes. If the analysis is activated, devices report the updated property values after the agent completes its next evaluation.

Deleting an analysis

Delete an analysis when you no longer need the data that it collects. This action cannot be undone.

1. Expand **Explore** in the side navigation, and then select **Analyses**.
2. Select the name of the analysis that you want to remove.
3. In the upper-right corner of the detail page, select the delete icon.

   The icon is dimmed for analyses that are hosted on external sites. It is enabled for analyses that are hosted on custom sites, if you have the required permissions.

4. In the **Delete analysis** dialog, review the name of the analysis, and then select **Delete**.

   Select **Cancel** or the close icon to keep the analysis.

The analysis is removed from the deployment and no longer appears in the **Analyses** list. Devices stop reporting the properties that belonged to it.

To change only the device scope without opening the wizard, in the **Device scope** panel, select **View all**, update the criteria, and then select **Save**.

Related information

Analysis detail page *(on page 217)*

Creating an analysis *(on page 220)*

Configuring analysis properties *(on page 234)*

Configuring analysis properties

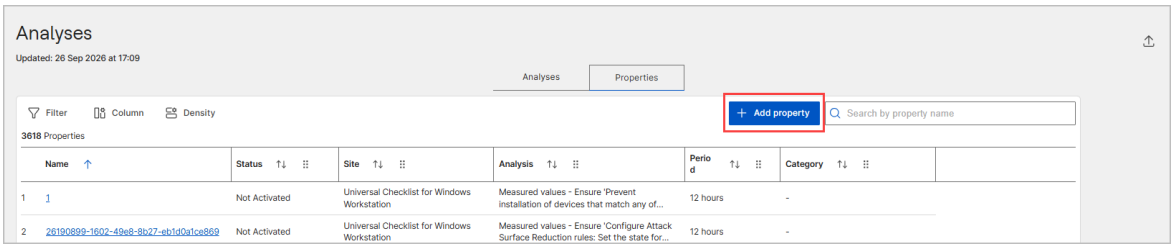
Add a property, change its evaluation period and relevance clause, or remove it from an analysis.

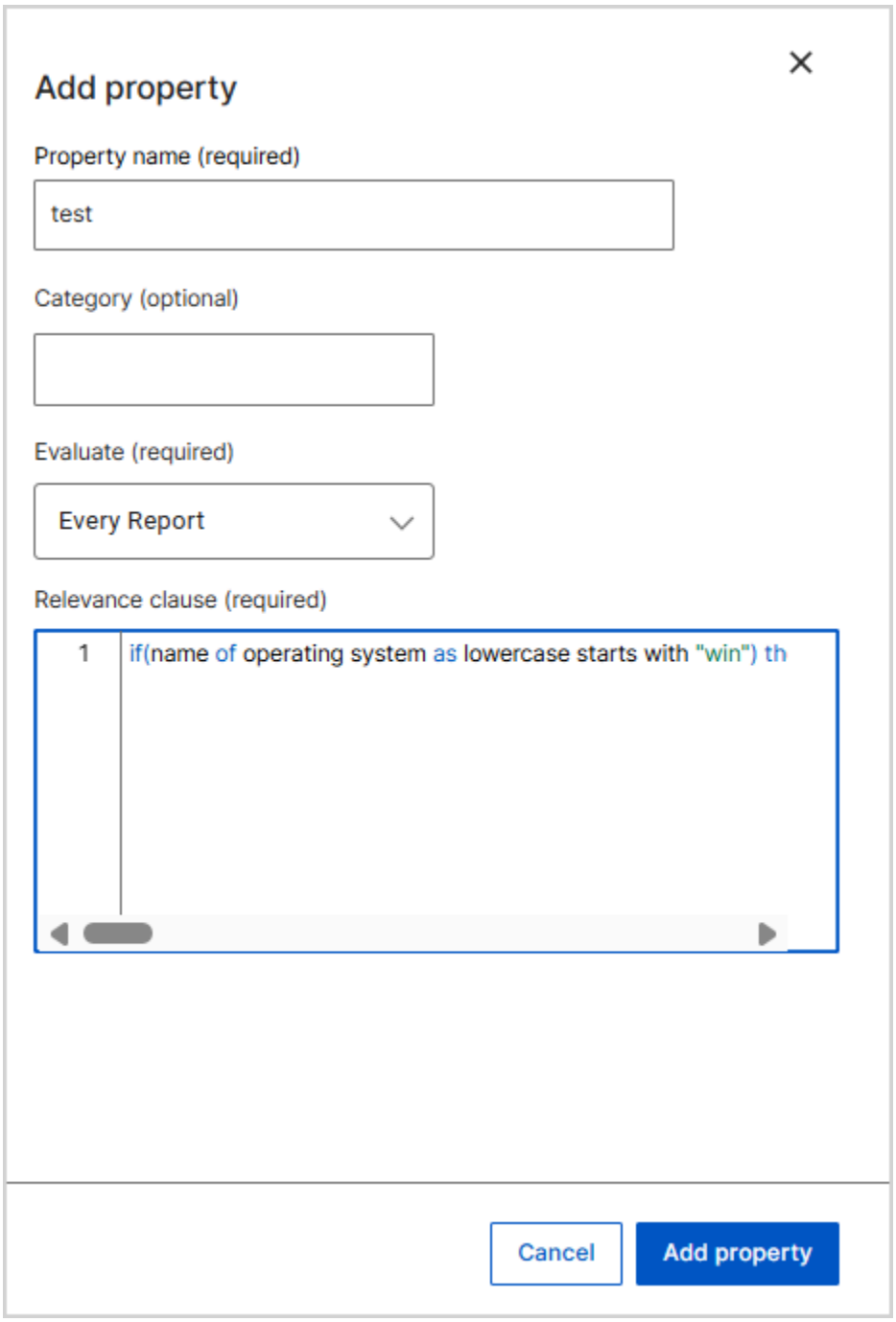
You need custom content rights and write access to the site that stores the analysis. Reserved properties that are activated globally are read-only.

A property defines the data that the BigFix agent collects, how often it evaluates the data, and the relevance clause that returns the value. You can create a property from the **Properties** tab, or edit an existing one from the same tab.

1. Expand **Explore** in the side navigation, select **Analyses**, and then select the **Properties** tab.
   The **Properties** table lists every property with its status, site, parent analysis, evaluation period, and category.

2. To create a property, select **Add property**.





a. In **Property name (required)**, enter a name for the property.

b. Optional: From **Category**, select a category that groups the property.

   Select the field to open the list, and then select one of the following categories: **Hardware**, **Operating System**, **Software**, **Network**, **Ownership**, **Organizational**, **Lifecycle**, **Operational**, **Security**, or **Compliance**. The category appears in the **Category** column of the **Properties** table.

c. From **Evaluate (required)**, select how often the agent evaluates the property.

The list provides **Every Report**, **5 minutes**, **15 minutes**, **30 minutes**, **1 hour**, **6 hours**, **12 hours**, **1 day**, **2 days**, **7 days**, and **30 days**. The default is **Every Report**.



Note: Frequent evaluation returns fresher data but adds load on the device. Use a longer period for values that change rarely.

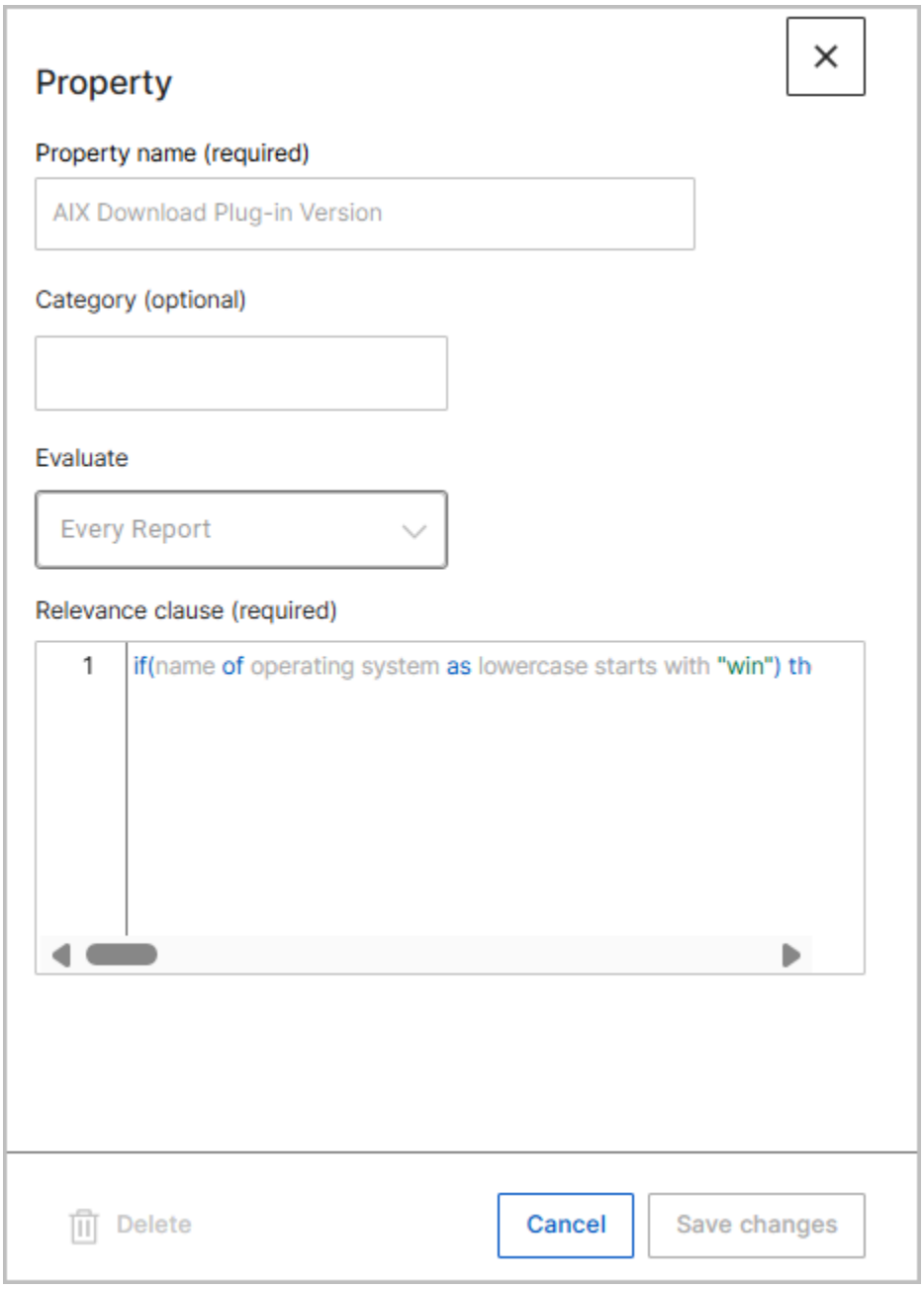
d. In **Relevance clause (required)**, enter the relevance expression that returns the value.

The editor numbers each line and applies syntax colouring to the expression, so that keywords, operators, and string values are easier to tell apart.

e. Select **Add property**.

3. To change an existing property, select its name in the **Properties** table.

The **Property** panel opens on the right and shows the **Property name**, **Category**, **Evaluate**, and **Relevance clause** fields.



4. Update the fields, and then select **Save changes**.

   Note: The **Save changes** button stays dimmed until you change a value. Select **Cancel** to close the panel without saving.

5. Optional: To remove the property, select **Delete** in the panel.

6. Optional: To change the properties of a single analysis, open the analysis details page and select **Edit analysis**.

The **Edit analysis** wizard opens with the same **Details**, **Scope**, and **Properties** steps that you use to create an analysis. Select **Next** to reach the **Properties** step, add or remove properties, and then select **Update Analyses**. To remove the analysis and its properties, select the delete icon on the analysis detail page, and then confirm the deletion. For more information, see Editing and deleting an analysis *(on page 229)*.

The **Properties** table shows the updated evaluation period and relevance. Devices report the new values after the next agent evaluation.

To share the collected values, see Exporting and sharing analysis results *(on page 239)*.

Exporting and sharing analysis results

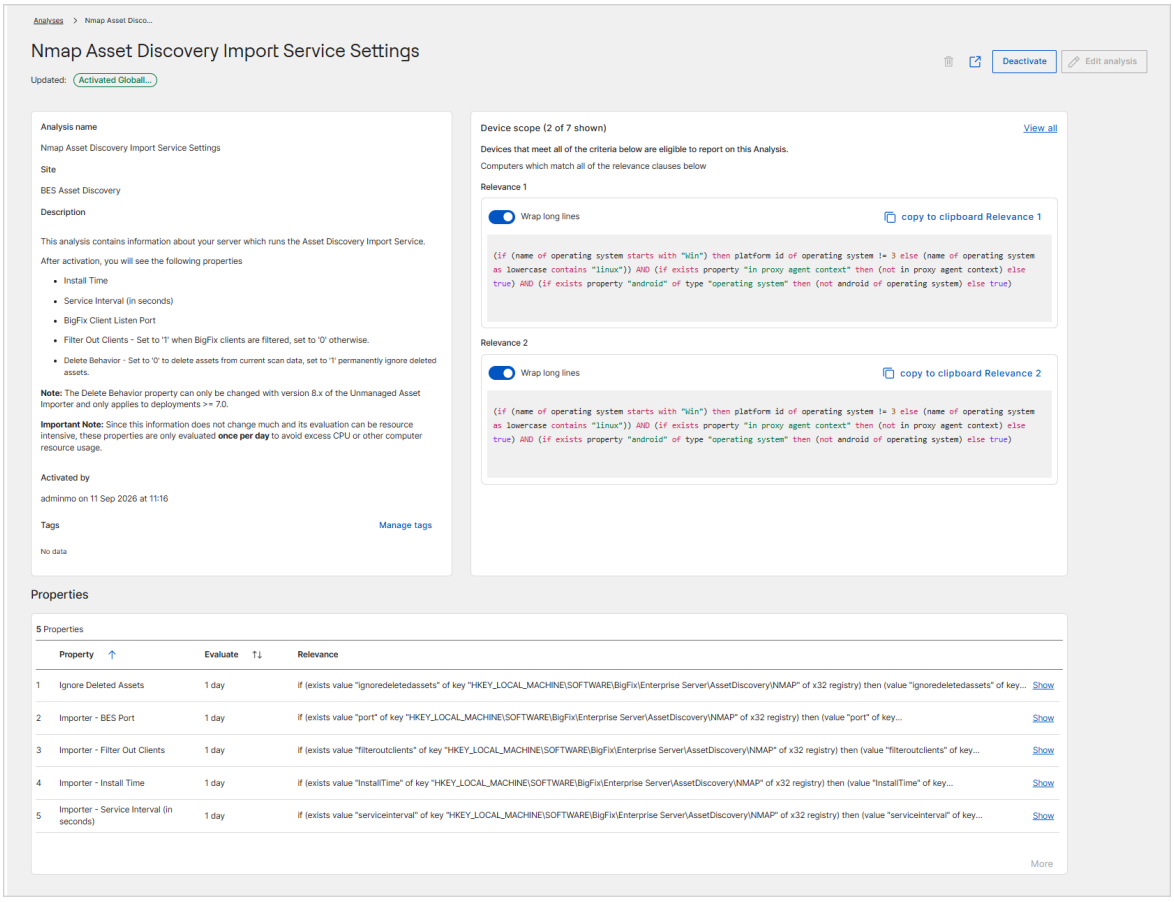
Export the analysis or property list as a report, save the current view for reuse, and copy relevance clauses from the analysis details page.

Devices report values only after the analysis is activated and the agent completes its next evaluation. Until then, the **Results** column is empty.

The **Analyses** page provides an **Export report** icon and a **Manage reports** button in the upper-right corner. Both tabs support these controls. For more information about saving and reopening a view, see Manage Reports *(on page 42)*.

1. Expand **Explore** in the side navigation, and then select **Analyses**.
2. Select the **Analyses** tab or the **Properties** tab, depending on the data that you want to share.
3. Refine the view before you export it.
    a. Select **Filter** to narrow the list to the analyses or properties that you need.
    For the steps, see Table filter *(on page 40)*.
    b. Select **Column** to choose which columns appear.
    For the steps, see Columns *(on page 29)*.
    c. Select **Density** to set the row spacing of the table.
    For the steps, see Density *(on page 29)*.
    d. Optional: Use the search field to find an analysis by name or a property by name.
4. Select the **Export report** icon in the upper-right corner, and then choose the export format.
    The export includes the columns and filters of the current view. For detailed steps, see Common functionalities *(on page 28)*.
    The file downloads to your browser download location.
5. Optional: To save the current view for reuse, select **Manage reports**.
    Saved reports keep your filters and column selections so that you and other operators can open the same view later. For detailed steps, see Common functionalities *(on page 28)*.

6. Optional: To share the results of a single analysis, select the analysis name to open its details page.



   a. In the **Device scope** panel, select **Copy code** to copy a relevance clause.
      Turn on **Wrap long lines** to read a long clause, and select **Show More** to expand it.

   b. Select **View all** to review every device that meets the criteria.

   c. In the **Properties** table, select **More** to load the remaining properties and their relevance values.

You have an exported file, a saved report, or a copied relevance clause that you can share with other operators.

To build a wider report across devices, Fixlets, and deployments, see Report Builder *(on page 384)*.

Resolve

The Resolve section provides tools to act on issues and apply remediations across your environment.

Resolve helps you manage operational risk by letting you act quickly on identified issues. It includes:

- **Custom Remediation** *(on page 241)* – Remediate devices on demand with your own Bash, PowerShell, or Action Scripts. Use it for quick fixes, registry changes, or patching apps that default content does not cover.
- **CyberFOCUS** *(on page 277)* – Combine MITRE ATT&CK intelligence and CISA Known Exploited Vulnerabilities (KEV) data with BigFix Fixlet and device relevance. Assess your security posture and start a remediation flow from the findings.
- **DEX** *(on page 308)* – Monitor digital experience health across managed endpoints. BigFix Digital Employee Experience (DEX) aggregates device performance, application stability, and user sentiment into DEX scores so that you can spot anomalies and act on them.
- **Workflow Builder** *(on page 309)* – Automate multi-step device tasks in a drag-and-drop editor, without writing a Fixlet or Task. Chain check, action, and flow-control steps, then deploy the result as a single BigFix action.
- **Fixlet Streams** *(on page 311)* – Automate recurring remediation, such as patch and update deployments, on a defined schedule. Streams also support ad hoc remediation, so that you can respond fast to urgent issues such as zero-day vulnerabilities.
- **Integrated Vulnerability Remediation** *(on page 350)* – Correlate vulnerability findings from your Tenable Vulnerability Management scanner with BigFix Fixlets and devices, so that you review vulnerabilities and deploy their remediations in one place.
- **Patch** *(on page 352)* – Get a consolidated, risk-prioritized view of missing patches and vulnerable devices. The dashboard shows which Fixlets and devices to address first and links back to the Fixlet explorer for the action.
- **Security Compliance** *(on page 353)* – Review a live, environment-wide view of compliance posture across every checklist deployed in your BigFix environment, and deploy remediation for the checks that fail.
- **License Reclamation** *(on page 354)* – See which software is installed but not used, and the savings that you gain when you uninstall it. Find the software that costs the most and reclaim licenses with one click.
- **Protection Level Agreement (PLA)** – Use baselines that combine device contexts, desired patch levels, and compliance standards for a set of Fixlets, measured against service levels that IT, Security, and the wider organization agree to.

Custom Remediation

Remediate devices on demand using your own Bash, PowerShell, or Action Scripts. Ideal for applying quick fixes, registry changes, or patching apps not covered by default content.

Overview

The Custom Remediation app in BigFix UI gives IT and security teams the flexibility and control to quickly remediate security vulnerabilities and configuration issues, even when standard Fixlets or out-of-the-box content aren't available. You can deploy your own scripts, deploy custom software updates, and apply configuration changes across your endpoints with speed and precision - useful for uncovered vulnerabilities, third-party application risks, and non-standard system configurations.

The Custom Remediation home page shows an **Updated** timestamp under the page title that indicates when the page data was last refreshed.

Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to the Custom Remediation application, which is an optional application. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete, such as creating actions and running script commands on the target devices. For a description of each permission, see Permissions reference *(on page 482)*.

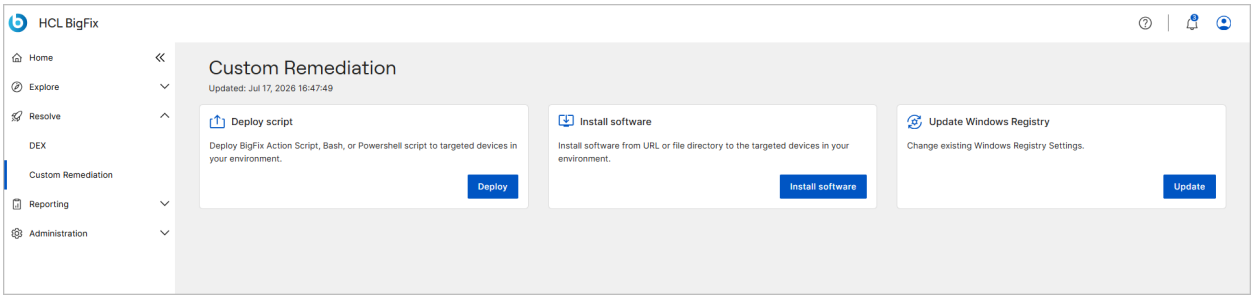
Key features

Deploy Script *(on page 243)*	If predefined remediation workflows don't cover your needs, and you know exactly w scripts are required to fix an issue, you can use this feature to create and deploy you can deploy BigFix Action Script, Bash, or PowerShell script directly to the target devic without waiting for built-in Fixlets.
Install Software *(on page 256)*	Deploy updates or patches for software (that are not included in standard BigFix con rectory to the target devices. Support any software Remediate vulnerabilities in any a not supported out of the box.
Update Windows Registry *(on page 267)*	Make quick changes to system settings, similar to the Windows Registry Wizard. App changes easily: Quickly edit registry values, apply configuration updates, or push env across many devices without waiting for pre-built content.

Note: Supported script types include Bash, PowerShell, and BigFix Action Scri

How to access Custom Remediation

To access the **Custom Remediation** app, expand **Resolve** from the side navigation, and then select **Custom Remediation**.

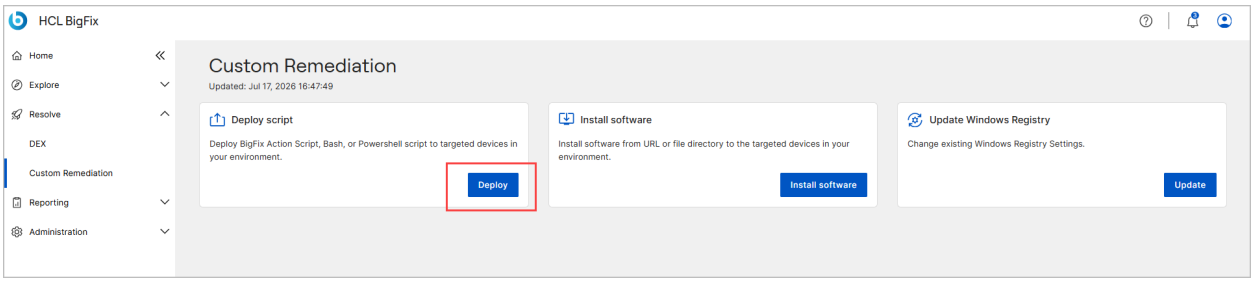


Deploy Script

Run your own scripts to quickly remediate devices. Supported script types include Bash, PowerShell, and BigFix Action Script within the BigFix UI. Target specific devices or OS families for fast and flexible deployments.

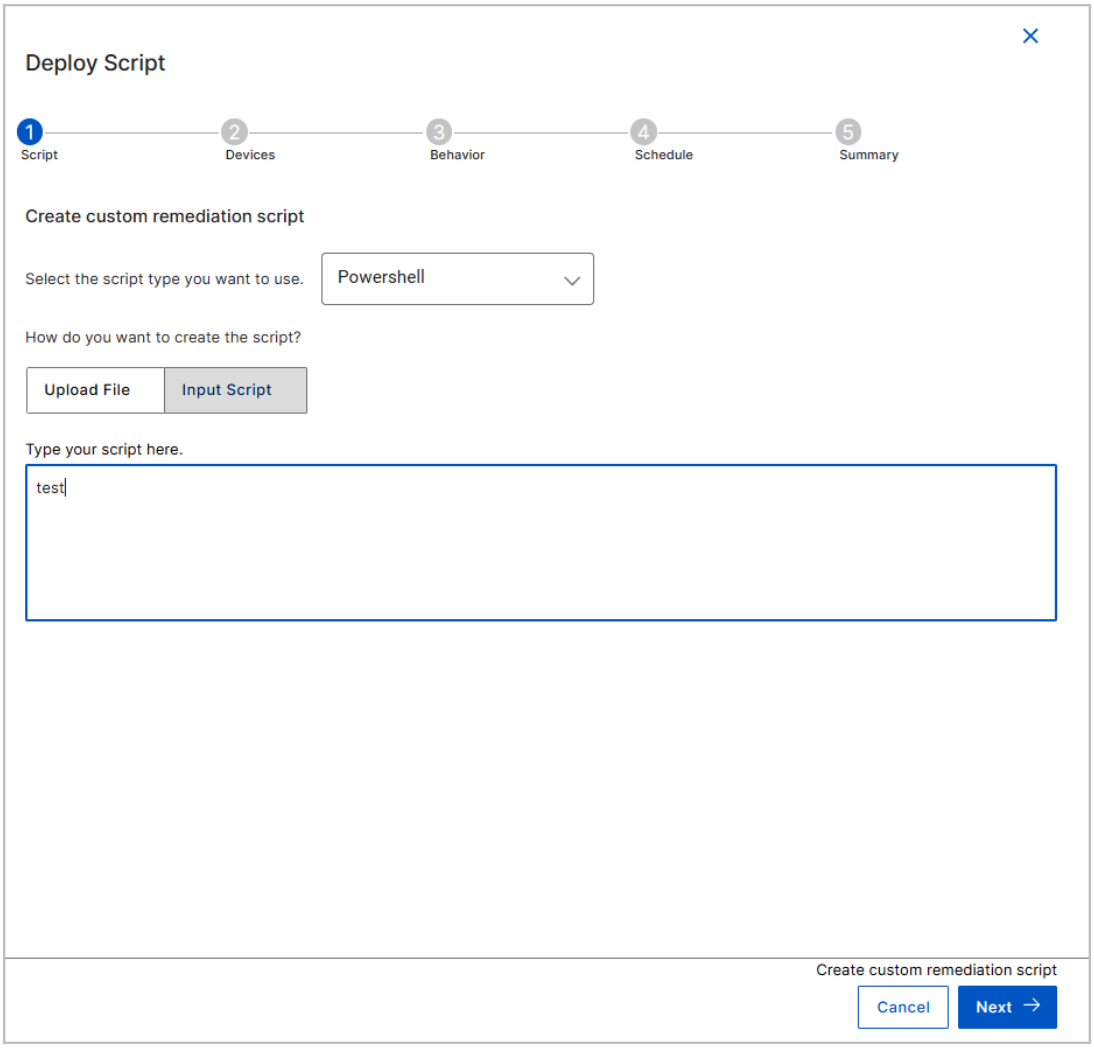
The Deploy Script feature under Custom Remediation lets advanced users (power users) deploy scripts directly to targeted devices for custom remediation. This tool is intended for users who need more control and flexibility than standard remediation tools provide.

From the Custom Remediation app, select **Deploy** on the **Deploy Script** card to open the Deploy Script wizard. The wizard guides you through five steps: **Script**, **Devices**, **Behavior**, **Schedule**, and **Summary**. A footer link, **Create custom remediation script with N applicable devices**, shows the current count of applicable devices on every step.



Deploy a script

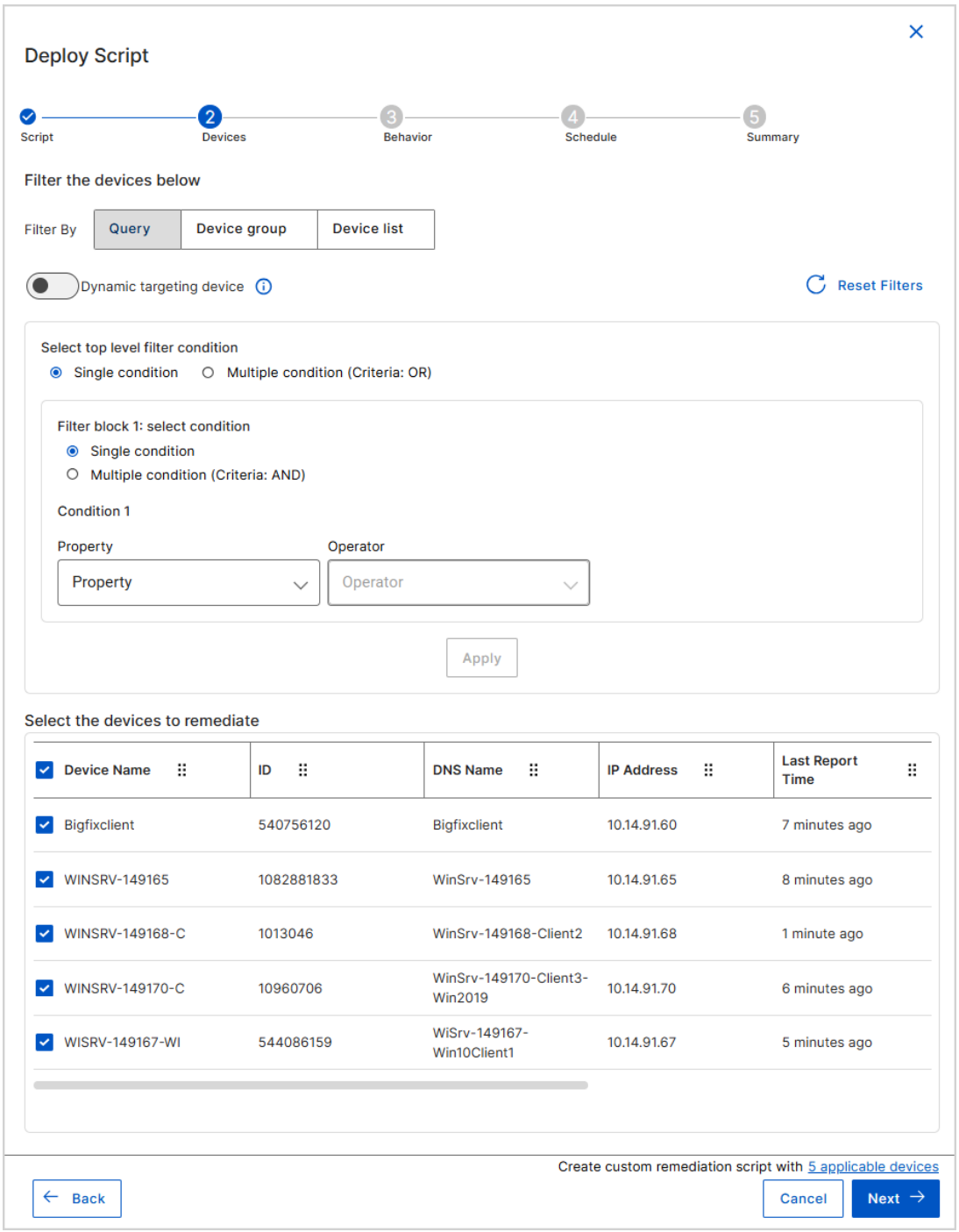
1. On the **Script** step (**Create custom remediation script**), define the script, and then select **Next**:
   - From **Select the script type you want to use**, select a script type, such as **Powershell**, **bash**, or **BigFix Action Script**.
   - For **How do you want to create the script?**, select **Upload File** to upload a script file, or **Input Script** to enter the script in the **Type your script here** box.



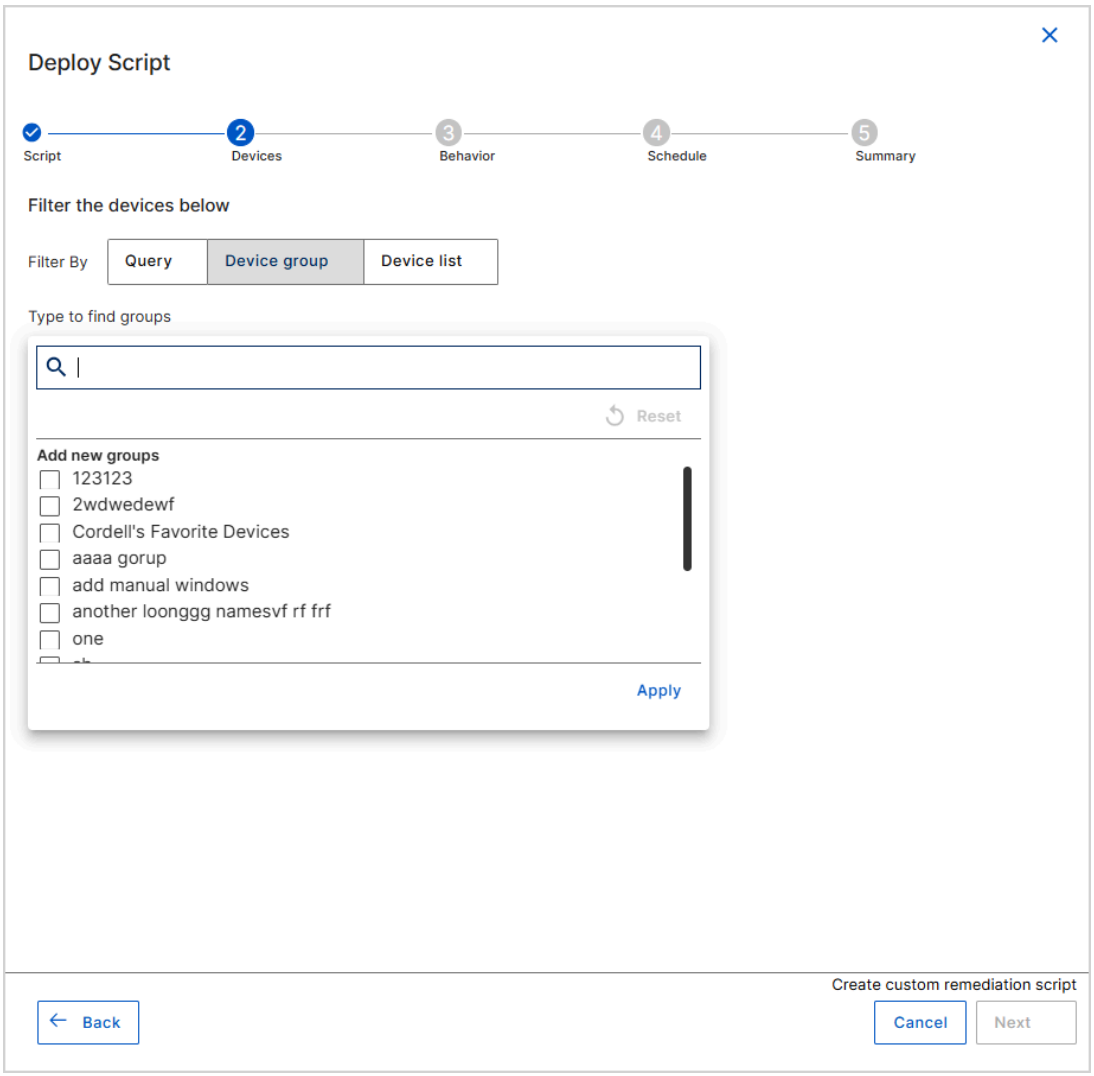
Note: Supported script types include Bash, PowerShell, and BigFix Action Script.

2. On the **Devices** step (**Filter the devices below**), specify how devices are selected, and then select **Next**. For **Filter By**, choose one of the following methods:

- **Query** - Create dynamic filters based on device properties.
  - Apply filters using **Single condition** or **Multiple condition** (Criteria: AND/OR) options. For more information, see Filter by query *(on page 40)*.
  - For each condition, select a **Property**, **Operator**, and **Value**.
  - Select **Reset Filters** to clear the filters.
  - (Optional) Turn on **Dynamic targeting device** toggle button to continuously re-evaluate the targeted devices so that devices matching the criteria are included as they report in.
  - Select **Apply** to evaluate the filters, and then review the **Select the devices to remediate** table to verify which devices match the criteria. The table shows the **Device Name**, **ID**, **DNS Name**, **IP Address**, and **Last Report Time** for each device.

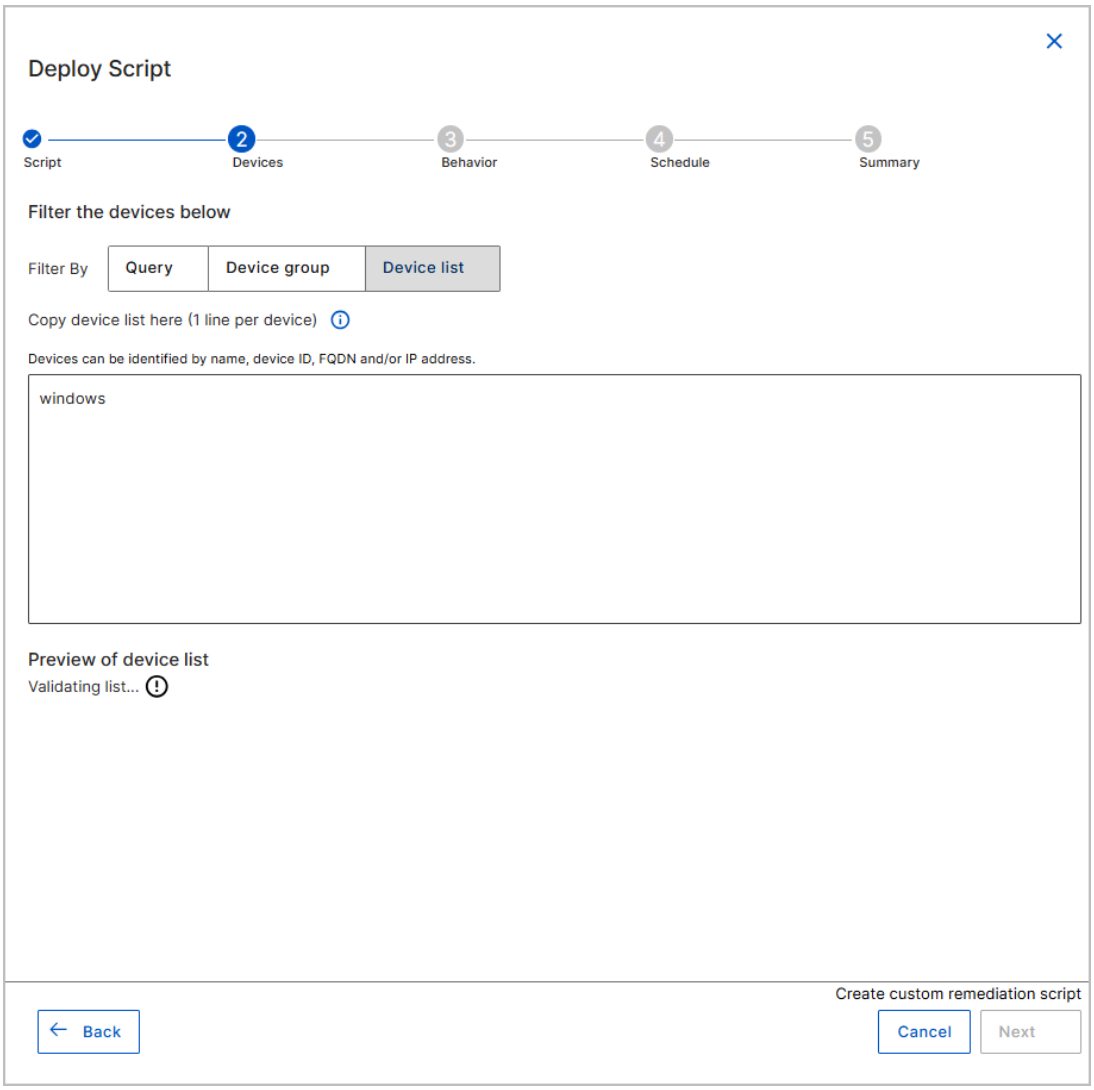


- **Device group** - Target an existing device group.
  - In **Type to find groups**, search for a group.
  - Select one or more groups under **Add new groups**.
  - Select **Apply**. Select **Reset** to clear the selection.

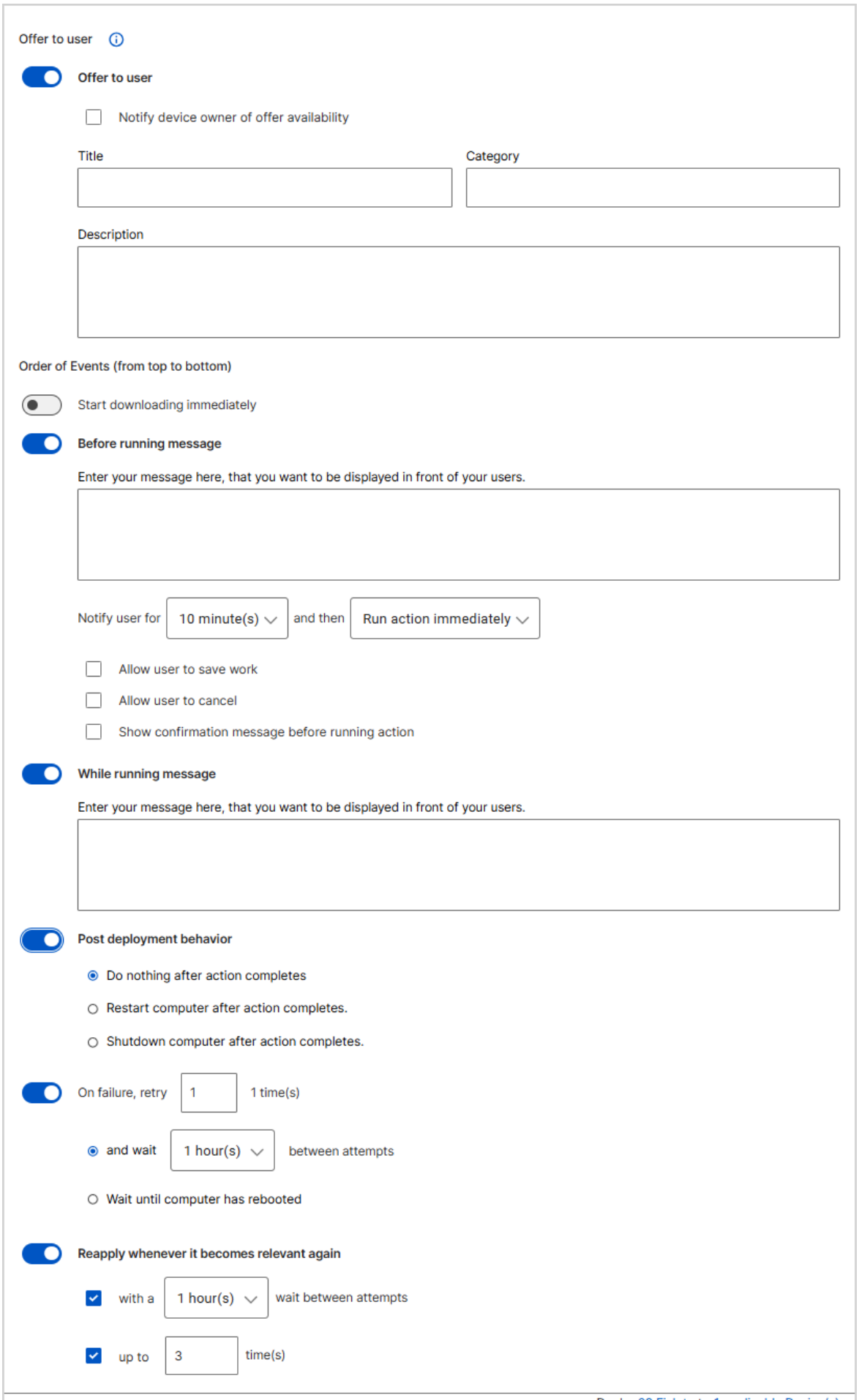


- **Device list** - Select devices manually from the list. This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.

- Identified by name, DNS, or IP address, with each device on a separate row.
- A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
- Select **Verify List** to confirm the entries, and review the preview of the device list to be targeted.



3. On the **Behavior** step, configure how the deployment is delivered, how users are informed, and how failures are handled, and then select **Next**. The options under **Order of Events (from top to bottom)** are processed sequentially:


Offer to user
Offer to user
Notify device owner of offer availability
Title
Category
Description
Order of Events (from top to bottom)
Start downloading immediately
Before running message
Enter your message here, that you want to be displayed in front of your users.
Notify user for
10 minute(s)
and then
Run action immediately
Allow user to save work
Allow user to cancel
Show confirmation message before running action
While running message
Enter your message here, that you want to be displayed in front of your users.
Post deployment behavior
Do nothing after action completes
Restart computer after action completes.
Shutdown computer after action completes.
On failure, retry
1
1 time(s)
and wait
1 hour(s)
between attempts
Wait until computer has rebooted
Reapply whenever it becomes relevant again
with a
1 hour(s)
wait between attempts
up to
3
time(s)

- **Offer to user** - Turn on this toggle to deploy the action as a BigFix Offer.

  Note: An Offer lets end users choose and install software, patches, or other actions themselves through a self-service application, instead of having them deployed automatically by an administrator.

  When you turn on this toggle, set the following options:

  - **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
  - **Title** - Enter the title that identifies the offer to the user.
  - **Category** - Enter the category that groups the offer in the self-service application.
  - **Description** - Enter the text that explains what the offer does.
- **Start downloading immediately** - Some Fixlets contain large files. This option controls whether all applicable devices begin downloading the Fixlet as soon as the deployment is created.
- **Before running message** - A device might become unresponsive while a Fixlet is deployed. Turn on this option to display a warning for a set time before the Fixlet is applied, which is also useful when a restart is required so users can save their work. Enter the message text, and then set the following options:

  - In **Notify user for**, select how long to show the message (for example, **10 minutes**), and in the **and then** list, select the follow-up action, such as **Run action immediately**.
  - **Allow user to save work** - Select this checkbox to let users save open work before the action runs.
  - **Allow user to cancel** - Select this checkbox to let users cancel the action.
  - **Show confirmation message before running action** - Select this checkbox to prompt users to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own, for example *Are you sure you want to run this action now?*
- **While running message** - Turn on this option to display a message on the device until the deployment is complete, and then enter the message text to display to the user.
- **Post deployment behavior** - Turn on this option to control what happens on the device after the action completes, and then select one of the following:

  - **Do nothing after action completes** - The device stays in its current state.
  - **Restart computer after action completes** - The device restarts when the action finishes.
  - **Shutdown computer after action completes** - The device shuts down when the action finishes.

  If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:

  - In **Message title (required)**, enter a short title, for example *Shutdown now*.
  - In **Message text (required)**, enter the message body that asks users to save any unsaved work.

- In **Notify user for**, select how long to show the message, and in the **and then** list, select what happens when that time ends, such as **Shutdown automatically** or **Restart automatically**.
- **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let users cancel the shutdown or restart.

◦ **On failure, retry** - Turn on this option to have BigFix try the deployment again if it fails. Enter the number of retries, and then select one of the following options:

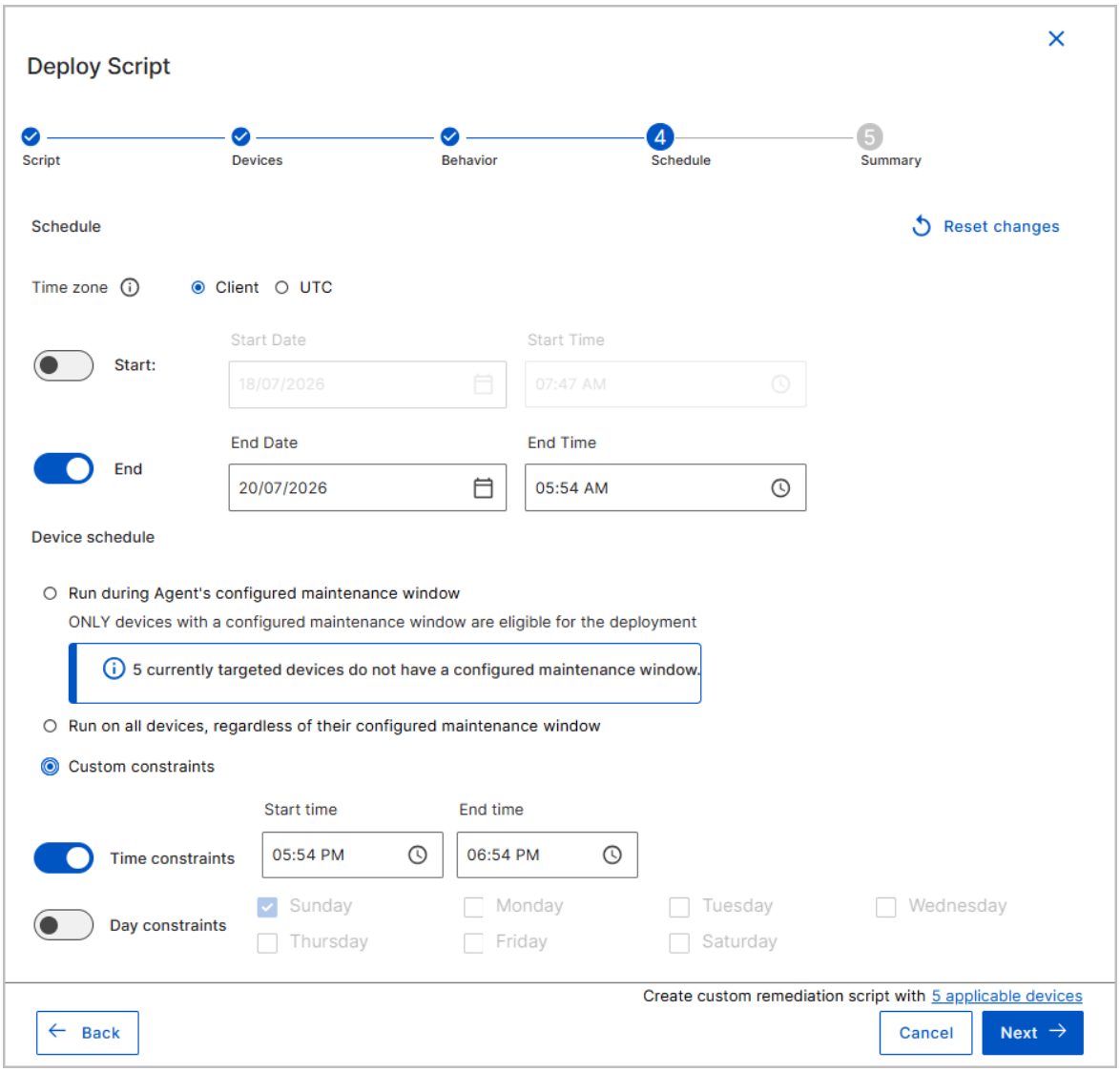
- **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.

◦ **Reapply whenever it becomes relevant again** - Turn on this option to reapply the Fixlet automatically if it becomes relevant again after the initial deployment. Select **with a** to set the wait time between attempts, and **up to** to set the maximum number of times.

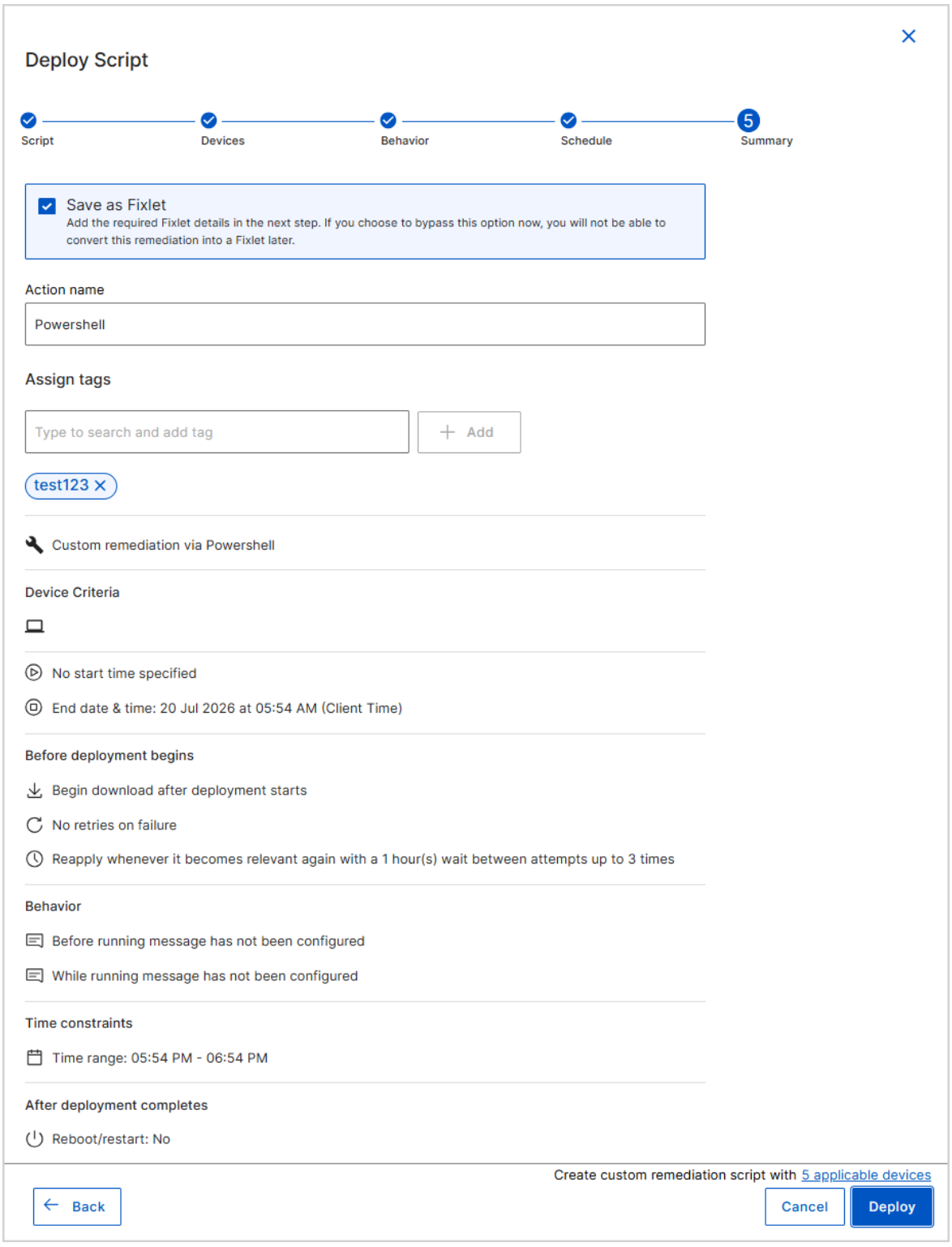


Tip: This setting increases the success rate by accounting for temporary issues such as device disconnection or network latency.

4. On the **Schedule** step, define the window during which the deployment remains in effect, and then select **Next**. For the settings, see Schedule settings *(on page 256)*. Select **Reset changes** to clear all scheduling fields and restore the defaults.



5. On the **Summary** step, review a consolidated, read-only view of every option you selected - device criteria, start and end time, before-deployment settings, behavior, time constraints, and after-deployment settings. This is the final checkpoint before deployment.


Deploy Script
Script
Devices
Behavior
Schedule
5
Summary
Save as Fixlet
Add the required Fixlet details in the next step. If you choose to bypass this option now, you will not be able to convert this remediation into a Fixlet later.
Action name
Powershell
Assign tags
Type to search and add tag
Add
test123
Custom remediation via Powershell
Device Criteria
No start time specified
End date & time: 20 Jul 2026 at 05:54 AM (Client Time)
Before deployment begins
Begin download after deployment starts
No retries on failure
Reapply whenever it becomes relevant again with a 1 hour(s) wait between attempts up to 3 times
Behavior
Before running message has not been configured
While running message has not been configured
Time constraints
Time range: 05:54 PM - 06:54 PM
After deployment completes
Reboot/restart: No
Create custom remediation script with 5 applicable devices
Back
Cancel
Deploy

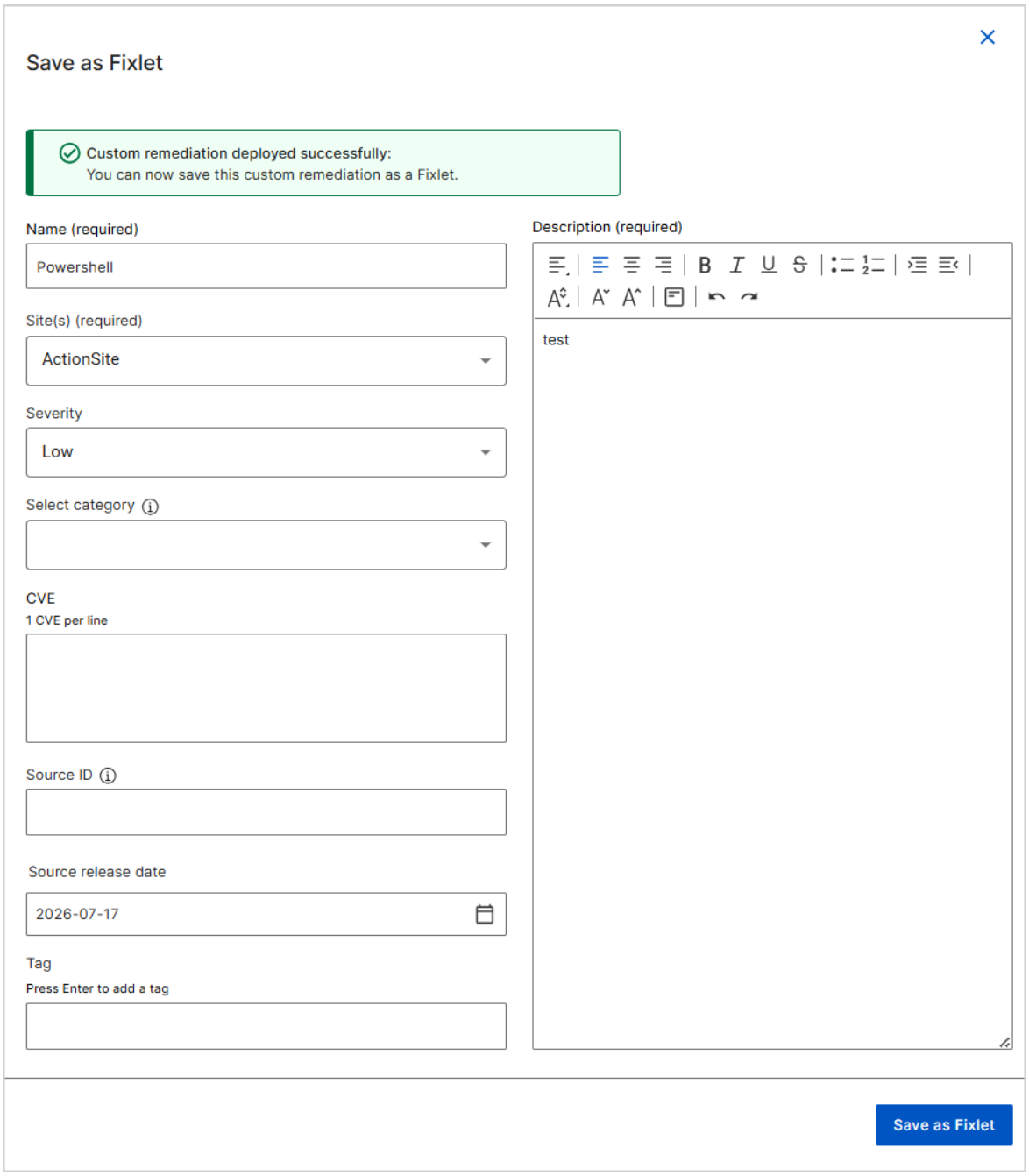
- The **Behavior** section confirms the message and notification options that you set on the Behavior step, for example:
  - A message will be displayed before deployment begins.
  - Notify user for 10 minute(s), and then run action immediately.
  - A confirmation message will be displayed before deployment begins.
  - No message will be displayed while deployment is running.
- To convert this remediation into a Fixlet, select **Save as Fixlet**, and provide the Fixlet details after the deployment succeeds (see step 7).

  Important: If you clear **Save as Fixlet** now, you can't convert this remediation into a Fixlet later.

- **Action name** is auto-populated with a default name that you can edit on the Summary step. Keep the default, or enter a unique, meaningful name that describes the purpose of the action. This name appears in action history, logs, and dashboards, which helps you and your team identify and differentiate actions. Use descriptive terms, such as "Critical patch - May 2026 - Windows devices", for clarity and traceability.
- In **Assign tags**, add one or more tags:
  - To add an existing tag, type to search for it, select it from the list, and then select **Add**.
  - To create a new tag, type the tag name, and then select **Add**.

  Assigned tags appear as chips below the field. To remove a tag, select the **X** on its chip. Tags are saved with the deployment and appear in the Deployment Manager; you can't change them after you deploy. For more information, see Managing Tags *(on page 51)*.

6. Select **Deploy** to deploy the action.
7. If you selected **Save as Fixlet**, the **Save as Fixlet** dialog opens after the message **Custom remediation deployed successfully** appears. Provide the Fixlet details, and then select **Save as Fixlet**. The Name is auto-populated with the same name entered for the action; the remaining fields start blank:



- In **Name** (required), keep the auto-populated action name or enter a different name.
- In **Description** (required), enter a description. Use the formatting toolbar to style the text.
- From **Site(s)** (required), select the site that the Fixlet belongs to, such as **ActionSite**.
- Optional: set **Severity**, **Select category**, **CVE** (one CVE per line), **Source ID**, **Source release date**, and **Tag** (press Enter to add each tag).

8. Select **Save as Fixlet**. A success message reading **"Your custom fixlet has been successfully created."** will appear in the top-right corner.

Schedule settings

Use the following settings on the **Schedule** step to control when the deployment runs.

Setting	Description
Time zone	Select the time zone that applies to the start and end times: **Client** uses each endpoint's local time; **UTC** uses Coordinated Universal Time.
Start	Turn on **Start** to set when the deployment begins, and then select the **Start Date** and **Start Time**. If **Start** is off, the deployment can begin immediately.
End	Turn on **End** to set when the deployment window closes, and then select the **End Date** and **End Time**.
Run during Agent's configured maintenance window	Restrict the deployment to devices that have a configured maintenance window. The deployment runs only within those windows. The wizard notes how many currently targeted devices don't have a configured maintenance window; those devices are excluded.
Run on all devices, regardless of their configured maintenance window	Override maintenance window restrictions. The deployment runs on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Control when a deployment can run by defining specific times and days. Turn on **Time constraints** to specify a **Start time** and **End time** when the deployment is allowed to run. Turn on **Day constraints** to limit the deployment to one or more days of the week.

Related information

Managing Tags *(on page 51)*

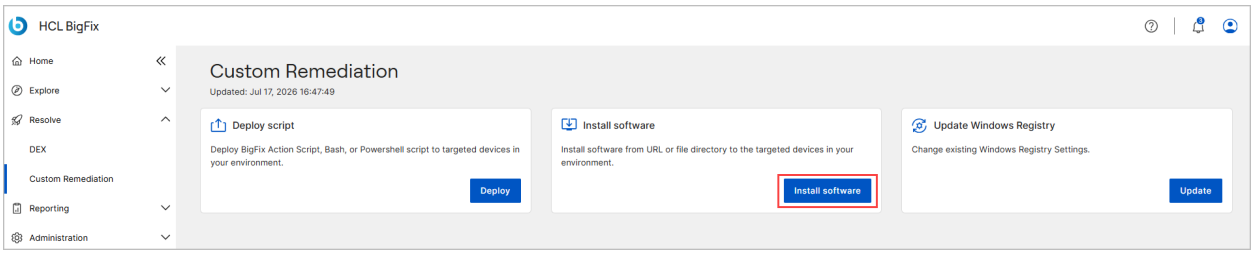
Install Software

Deploy software to specific devices by providing a download link and targeting filtered devices. This is a flexible way to deliver software without uploading packages manually.

Use the Install Software feature in the Custom Remediation app when you have a publicly accessible or internal URL for a software installer, you want to deploy that software to a subset of devices filtered by OS, name, group, or other criteria, and you need a lightweight, quick remediation workflow.

Install software

From the Custom Remediation app, select **Install Software** to open the Install Software wizard. The wizard guides you through five steps: **Software**, **Devices**, **Behavior**, **Schedule**, and **Summary**. A footer link, **Install software package to N applicable devices**, shows the current count of applicable devices.



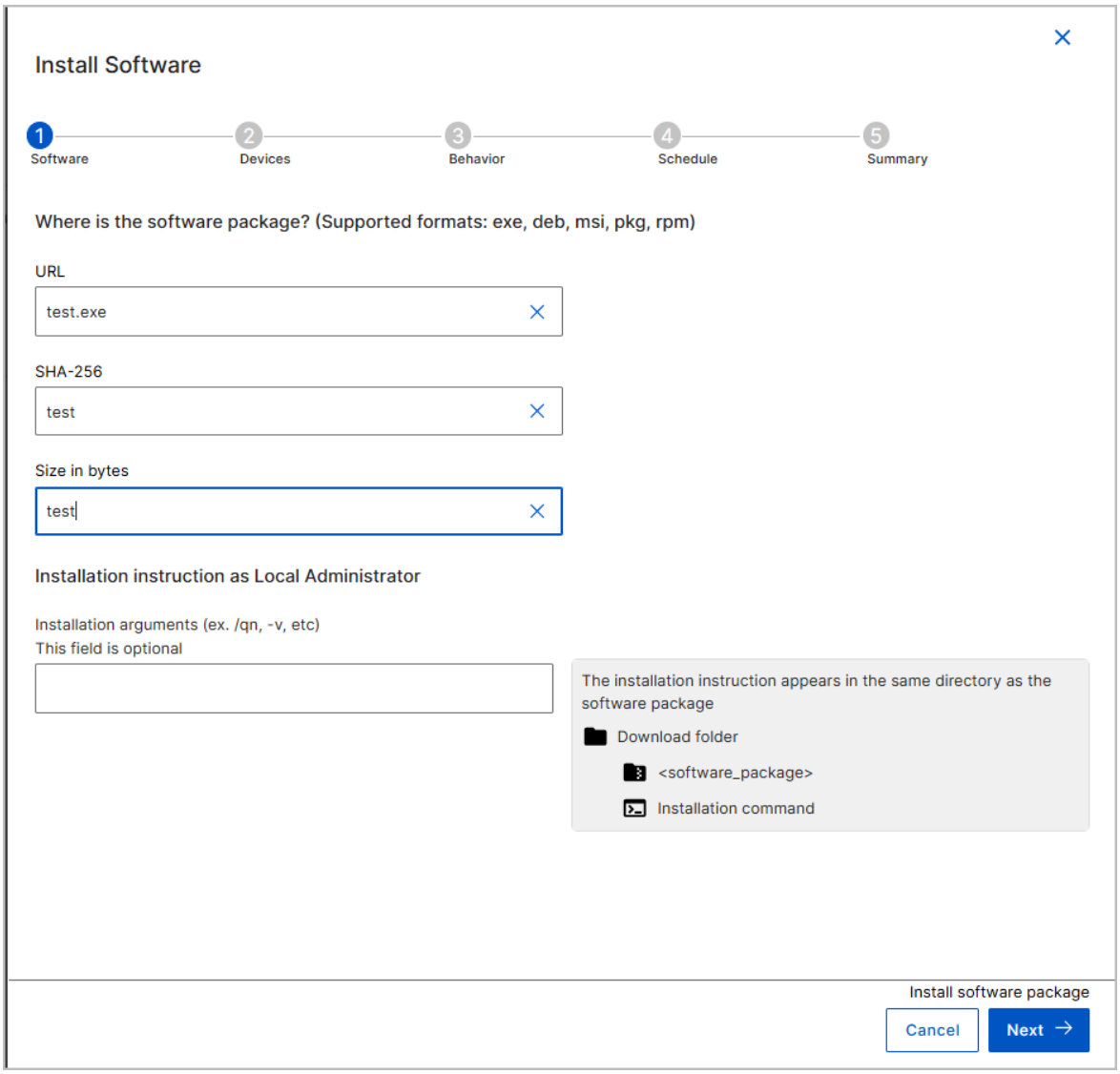
1. On the **Software** step (**Where is the software package? (Supported formats: exe, deb, msi, pkg, rpm)**), provide the software details, and then select **Next**:
    - In **URL**, enter the direct link to the software package hosted online. Supported file extensions are .deb, .exe, .msi, .pkg, and .rpm.
    - In **SHA-256**, enter the secure hash used to verify the integrity of the downloaded file.
    - In **Size in bytes**, enter the exact file size to validate the download.
    - **Installation instructions as Local Administrator**: This field is optional. Optionally enter **Installation arguments (ex. /qn, -v, etc)**. BigFix generates the base installation command from the file type in the URL, so you only need to enter optional arguments, such as silent-install flags.

      Example: If you're installing an MSI and want a silent install, just enter `/qn`.

      BigFix will generate the full command automatically, e.g., `msiexec.exe /i myApp.msi /qn`.

      If you leave the field blank, BigFix will still send the appropriate base command, such as

      ```
      msiexec.exe /i
              myApp.msi
      ```

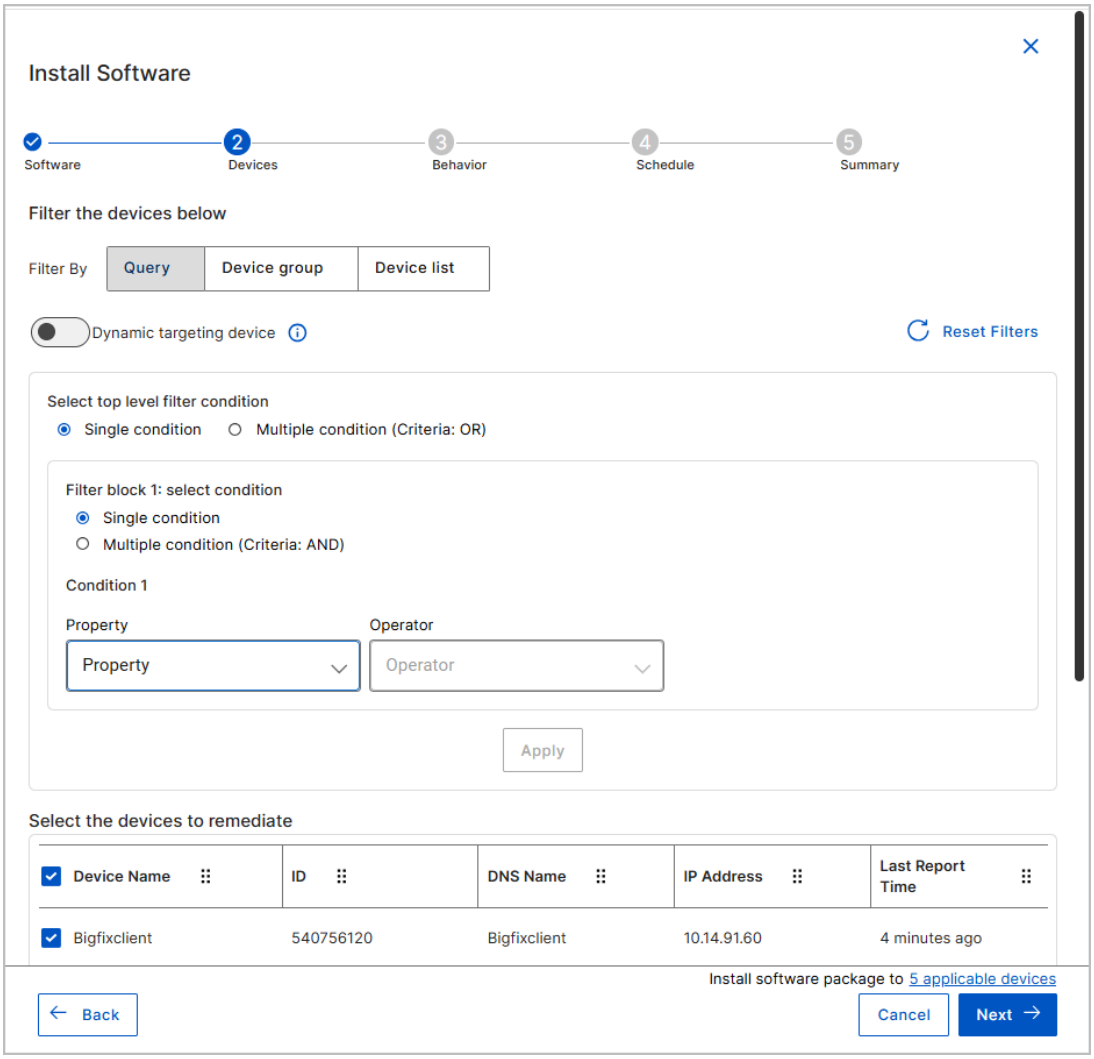


Note: The installation instruction is placed in the same directory as the software package. On the device, the download folder contains the software package and the generated installation command.

Table 52. Example configuration

Field	Example value
URL	https://example.com/software/app.msi
SHA-256	3a1f34e... (64-character hash)
Size in bytes	10485760
Software command	app.msi
Installation command	msiexec.exe /i app.msi /qn

2. On the **Devices** step (**Filter the devices below**), select the target devices, and then select **Next**. For **Filter By**, choose one of the following methods:
    - **Query** - Create dynamic filters based on device properties.
        - Apply filters using **Single condition** or **Multiple condition** (Criteria: AND/OR) options. For more information, see Filter by query *(on page 40)*
        - For each condition, select a **Property**, **Operator**, and **Value**.
        - Select **Reset Filters** to clear the filters.
        - (Optional) Turn on **Dynamic targeting device** toggle button to continuously re-evaluate the targeted devices so that devices matching the criteria are included as they report in.
        - Select **Apply** to evaluate the filters, and then review the **Select the devices to remediate** table to verify which devices match the criteria. The table shows the **Device Name**, **ID**, **DNS Name**, **IP Address**, and **Last Report Time** for each device.



    - **Device group** - Target an existing device group.

        - In **Type to find groups**, search for a group.
        - Select one or more groups under **Add new groups**.
        - Select **Apply**. Select **Reset** to clear the selection.
    - **Device list** - Select devices manually from the list. This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.
        - Identified by name, DNS, or IP address, with each device on a separate row.
        - A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
        - Select **Verify List** to confirm the entries, and review the preview of the device list to be targeted.

    - Enter a fixed list of devices, identified by name, DNS, or IP address, with each device on a separate row. A single device list supports a maximum of 1,000 devices; to target more, create separate deployments. Select **Verify List** to confirm the entries, and review the preview of the static list to be targeted.
3. On the **Behavior** step, configure how the deployment is delivered, how users are informed, and how failures are handled, and then select **Next**. The options under **Order of Events (from top to bottom)** are processed sequentially:

Offer to user

Offer to user

Notify device owner of offer availability

Title

Category

Description

Order of Events (from top to bottom)

Start downloading immediately

Before running message

Enter your message here, that you want to be displayed in front of your users.

Notify user for 10 minute(s) and then Run action immediately

Allow user to save work

Allow user to cancel

Show confirmation message before running action

While running message

Enter your message here, that you want to be displayed in front of your users.

Post deployment behavior

Do nothing after action completes

Restart computer after action completes.

Shutdown computer after action completes.

On failure, retry 1 1 time(s)

and wait 1 hour(s) between attempts

Wait until computer has rebooted

Reapply whenever it becomes relevant again

with a 1 hour(s) wait between attempts

up to 3 time(s)

- **Offer to user** - Turn on this toggle to deploy the action as a BigFix Offer.

  Note: An Offer lets end users choose and install software, patches, or other actions themselves through a self-service application, instead of having them deployed automatically by an administrator.

  When you turn on this toggle, set the following options:

  - **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
  - **Title** - Enter the title that identifies the offer to the user.
  - **Category** - Enter the category that groups the offer in the self-service application.
  - **Description** - Enter the text that explains what the offer does.
- **Start downloading immediately** - When on, targeted endpoints begin downloading the required payloads as soon as the action is deployed.
- **Before running message** - When on, the configured message appears to the end user before the action starts, to provide context, warnings, or a request for confirmation. Enter the message text, and then set the following options:

  - In **Notify user for**, select how long to show the message (for example, **10 minutes**), and in the **and then** list, select the follow-up action, such as **Run action immediately**.
  - **Allow user to save work** - Select this checkbox to let users save open work before the action runs.
  - **Allow user to cancel** - Select this checkbox to let users cancel the action.
  - **Show confirmation message before running action** - Select this checkbox to prompt users to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own, for example *Are you sure you want to run this action now?*
- **While running message** - When on and a message is configured, the message appears during execution to show that the remediation is in progress. Enter the message text to display to the user.
- **Post deployment behavior** - When on, controls what happens on the device after the action completes. Select one of the following:

  - **Do nothing after action completes** - The device stays in its current state.
  - **Restart computer after action completes** - The device restarts when the action finishes.
  - **Shutdown computer after action completes** - The device shuts down when the action finishes.

  If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:

  - In **Message title (required)**, enter a short title, for example *Shutdown now*.
  - In **Message text (required)**, enter the message body that asks users to save any unsaved work.

- In **Notify user for**, select how long to show the message, and in the **and then** list, select what happens when that time ends, such as **Shutdown automatically** or **Restart automatically**.
- **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let users cancel the shutdown or restart.

◦ **On failure, retry** - When on, BigFix reattempts a failed action. Enter the number of retries, and then select one of the following options:

- **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.

◦ **Reapply whenever it becomes relevant again** - When on, BigFix reapplies the action automatically if it becomes relevant again after the initial deployment. Select **with a** to set the wait time between attempts, and **up to** to set the maximum number of times.



Tip: Reapplying increases the success rate by accounting for temporary issues such as device disconnection or network latency.

4. On the **Schedule** step, define the window during which the deployment remains in effect, and then select **Next**. For the settings, see the Schedule settings table. Select **Reset changes** to clear all scheduling fields and restore the defaults.

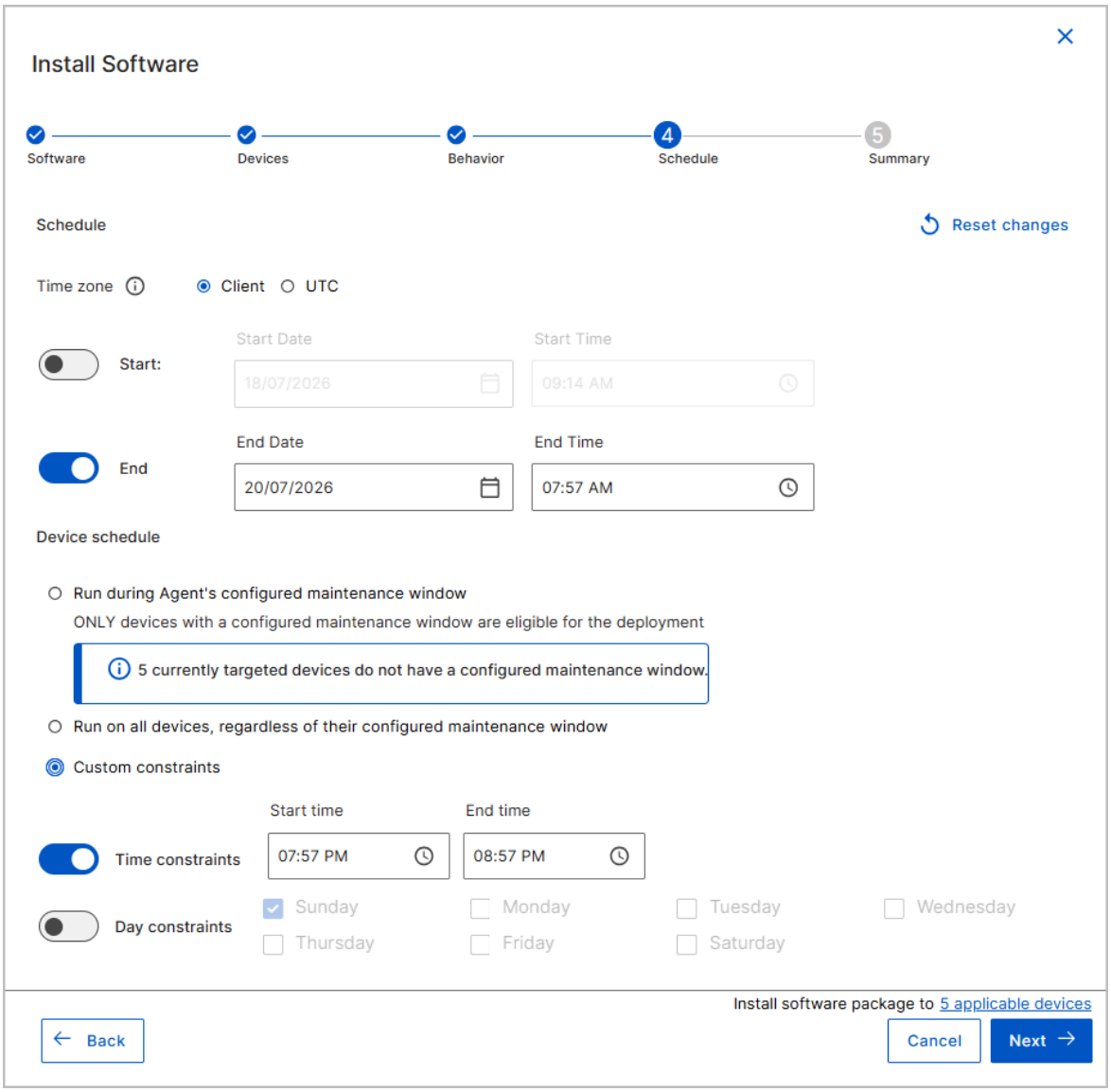
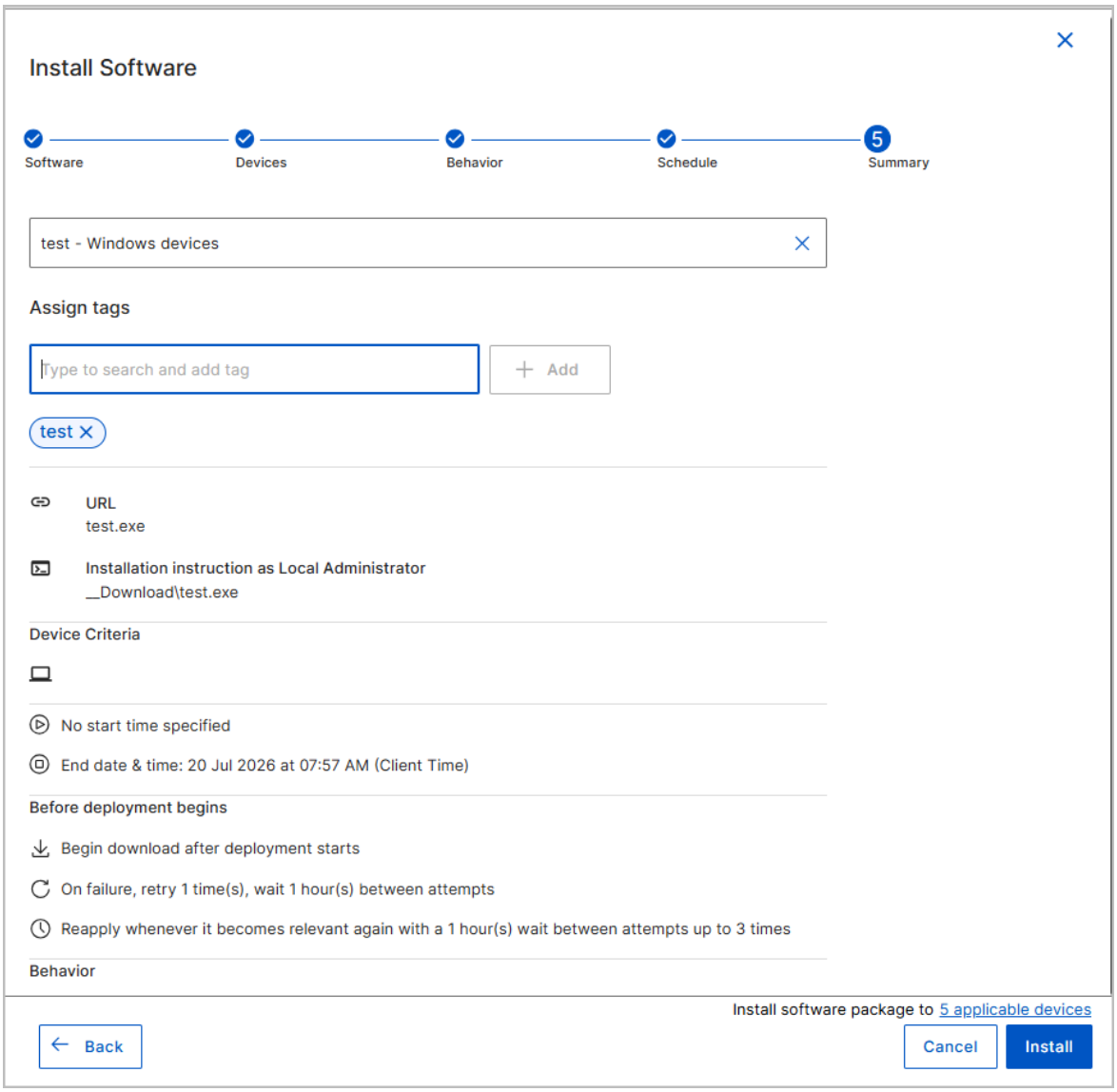


Table 53. Schedule settings

Settings	Description
Time zone	Select the time zone that applies to the start and end times: **Client** uses each endpoint's local time; **UTC** uses Coordinated Universal Time.
Start	Turn on **Start** to set when the deployment begins, and then select the **Start Date** and **Start Time**. If **Start** is off, the deployment can begin immediately.
End	Turn on **End** to set when the deployment window closes, and then select the **End Date** and **End Time**.

Settings	Description
Run during Agent's configured maintenance window	Restrict the deployment to devices that have a configured maintenance window. The deployment runs only within those windows. The wizard notes how many currently targeted devices don't have a configured maintenance window; those devices are excluded.
Run on all devices, regardless of their configured maintenance window	Override maintenance window restrictions. The deployment runs on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Control when a deployment can run by defining specific times and days. ◦ Turn on **Time constraints** to specify a **Start time** and **End time** when the deployment is allowed to run. ◦ Turn on **Day constraints** to limit the deployment to one or more days of the week.

5. On the **Summary** step, review a consolidated, read-only view of every option you selected - URL, installation instruction, device criteria, start and end time, before-deployment settings, and behavior. This is the final checkpoint before deployment.



- The **Behavior** section confirms the message and notification options that you set on the Behavior step, for example:
  - A message will be displayed before deployment begins.
  - Notify user for 10 minute(s), and then run action immediately.
  - A confirmation message will be displayed before deployment begins.
  - No message will be displayed while deployment is running.
- In **Action name**, enter a unique, meaningful name that describes the purpose of the action. This name appears in action history, logs, and dashboards, which helps you and your team identify and differentiate actions. Use descriptive terms, such as "Critical patch - May 2026 - Windows devices", for clarity and traceability.
- In **Assign tags**, add one or more tags:

- To add an existing tag, type to search for it, select it from the list, and then select **Add**.
- To create a new tag, type the tag name, and then select **Add**.

Assigned tags appear as chips below the field. To remove a tag, select the **X** on its chip. Tags are saved with the deployment and appear in the Deployment Manager; you can't change them after you deploy. For more information, see Managing Tags *(on page 51)*.

6. Select **Install** to install the software. The message **Deployment submitted successfully** confirms that the deployment was submitted.

Related information

Managing Tags *(on page 51)*

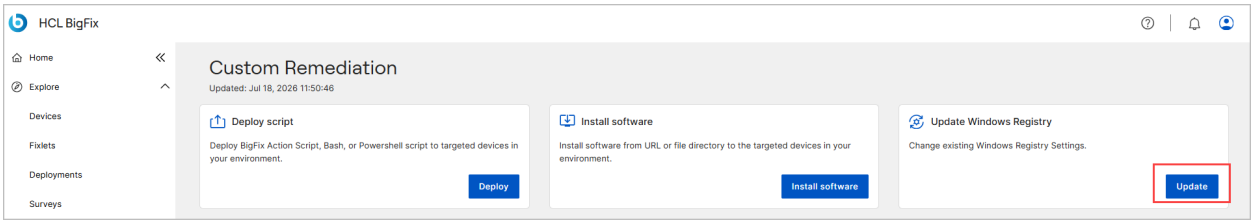
Update Windows Registry

Apply Windows Registry changes to one or more devices using Custom Remediation. Upload a Windows Registry (.reg) file or specify registry keys directly - ideal for applying system policies, security settings, or configuration changes at scale.

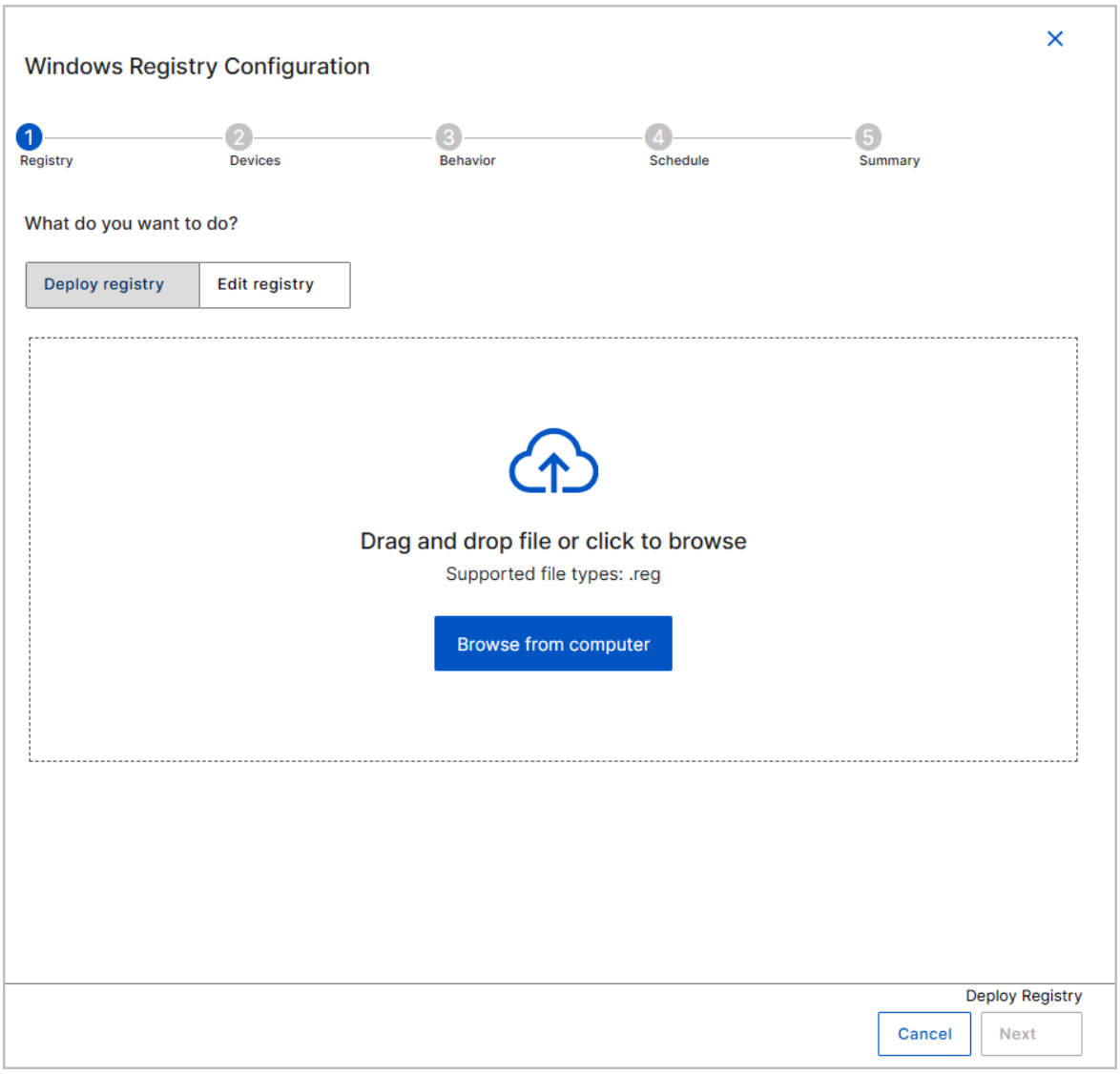
The Update Windows Registry feature lets IT administrators apply registry changes to one or more Windows devices quickly and securely, without creating a Fixlet or waiting for official content updates. You can import a .reg file or define registry keys directly; BigFix converts the changes into a script that runs silently on targeted devices that meet the targeting criteria.

Update the Windows Registry

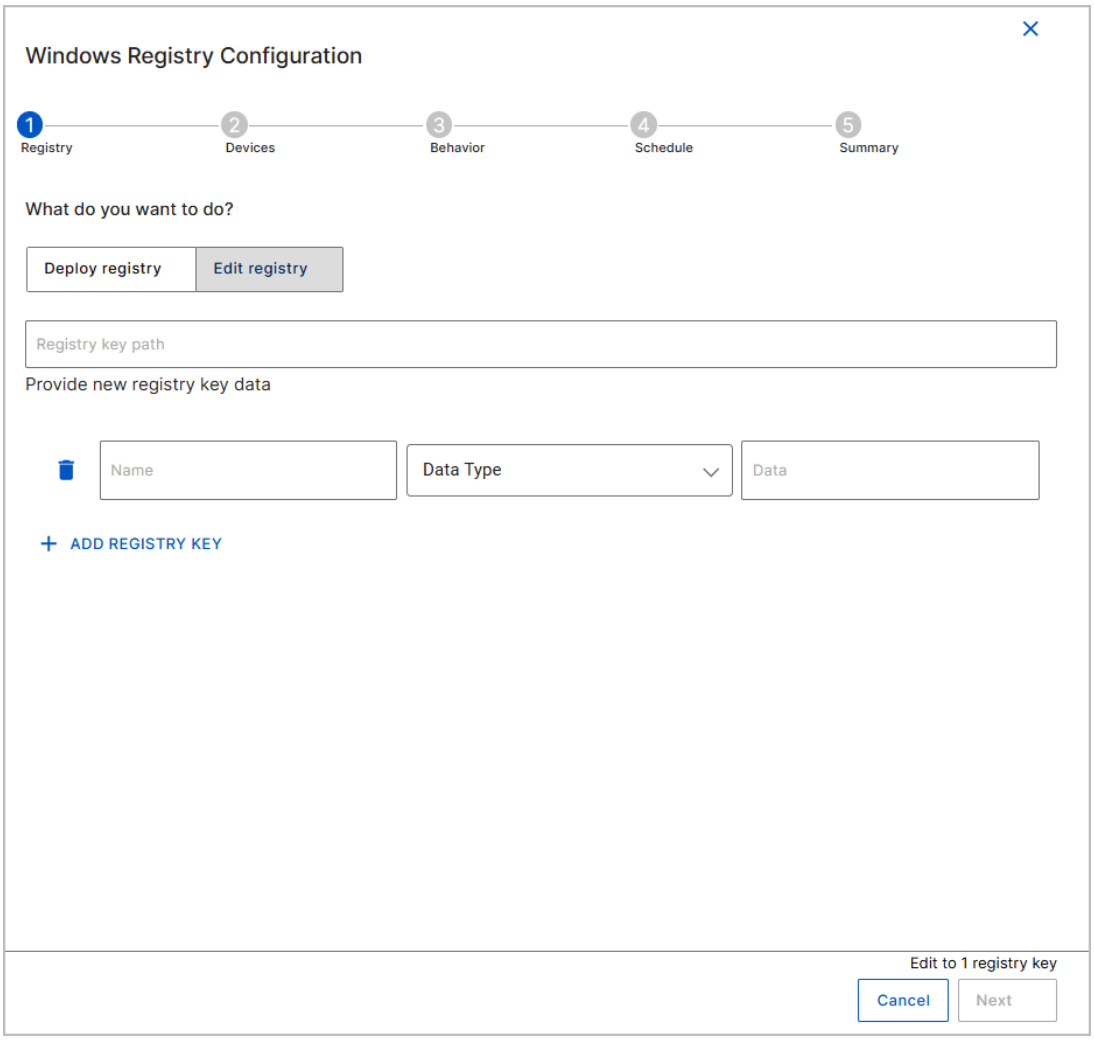
From the Custom Remediation app, select **Update** on the **Update Windows Registry** card to open the **Windows Registry Configuration** wizard. The wizard guides you through five steps: **Registry**, **Devices**, **Behavior**, **Schedule**, and **Summary**.



1. On the **Registry** step, under **What do you want to do?**, select how to provide the registry changes, and then select **Next**:



   - **Deploy registry** - Upload a .reg file. Drag and drop the file into the upload area, or select **Browse from computer** to select the file from your system. Supported file type: .reg.
   - **Edit registry** - Specify the registry changes directly:

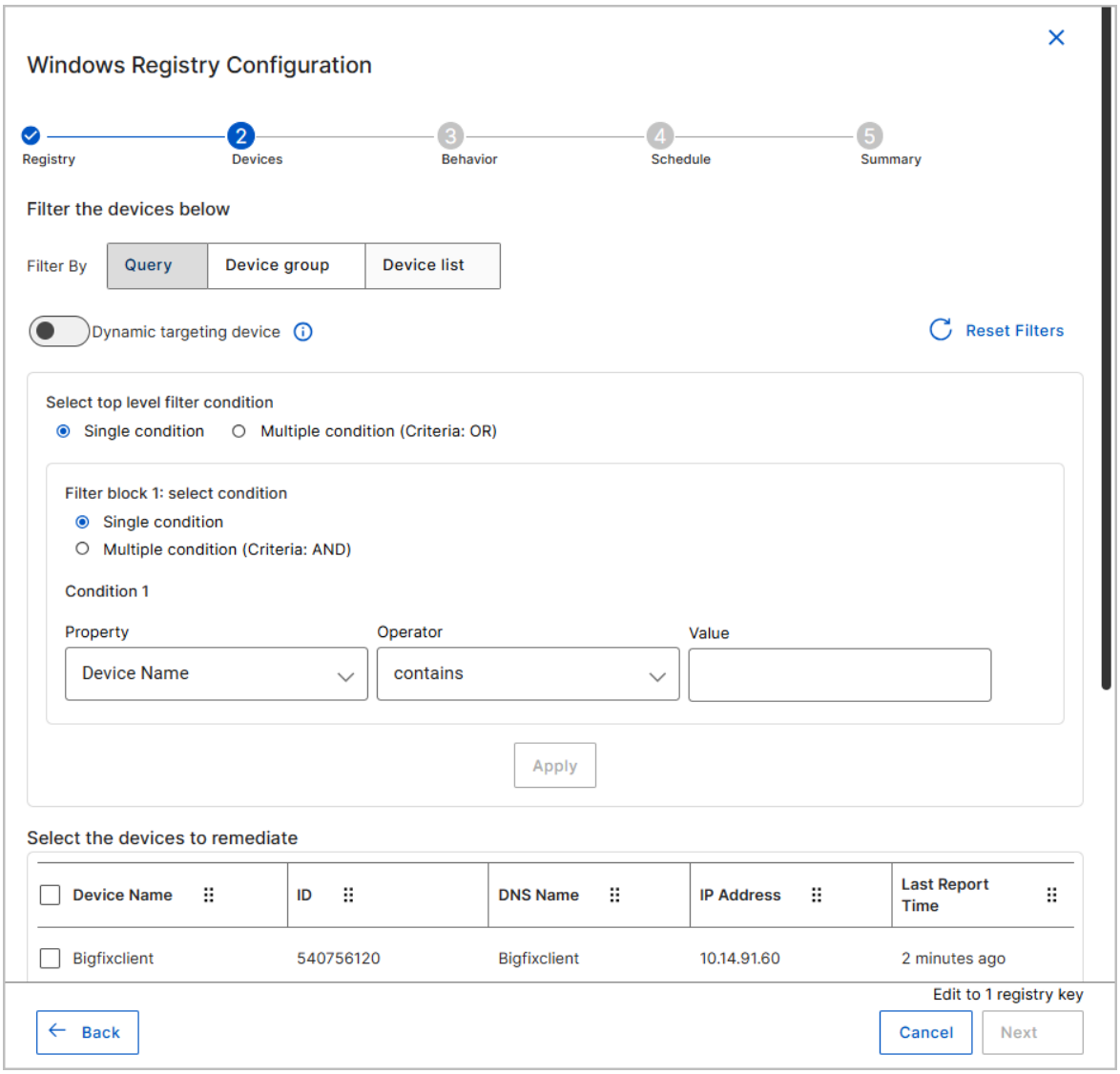


- Enter the registry key path - the full path to the registry key to modify, for example `HKEY_LOCAL_MACHINE\Software\YourCompany\Settings`.
- Under **Provide new registry key data**, enter the data name (for example, EnableFeatureX), select the data type (for example, **String**), and enter the data value.
- Select **ADD REGISTRY KEY** to add the key-value pair. To add more entries, select **ADD REGISTRY KEY** again; to remove an entry, select the delete (trash) icon next to it. All keys run in a single execution sequence on the endpoint.

Table 54. Example: multiple registry keys

Registry path	Name	Type	Value
`HKEY_LOCAL_MACHINE\Software\MyApp`	`AutoStart`	`REG_DWORD`	`1`
`HKEY_LOCAL_MACHINE\Software\MyApp\Config`	`ServerURL`	`REG_SZ`	`https://example.com`

2. On the **Devices** step (**Filter the devices below**), select the target devices, and then select **Next**.



For **Filter By**, choose one of the following methods:

- **Query** - Create dynamic filters based on device properties.
  - Apply filters using **Single condition** or **Multiple condition** (Criteria: AND/OR) options. For more information, see Filter by query *(on page 40)*.
  - For each condition, select a **Property**, **Operator**, and **Value**.
  - Select **Reset Filters** to clear the filters.
  - (Optional) Turn on **Dynamic targeting device** toggle button to continuously re-evaluate the targeted devices so that devices matching the criteria are included as they report in.
  - Select **Apply** to evaluate the filters, and then review the **Select the devices to remediate** table to verify which devices match the criteria. The table shows the **Device Name**, **ID**, **DNS Name**, **IP Address**, and **Last Report Time** for each device.

- **Device group** - Target an existing device group.
  - In **Type to find groups**, search for a group.
  - Select one or more groups under **Add new groups**.
  - Select **Apply**. Select **Reset** to clear the selection.
- **Device list** - Select devices manually from the list. This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.
  - Identified by name, DNS, or IP address, with each device on a separate row.
  - A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
  - Select **Verify List** to confirm the entries, and review the preview of the device list to be targeted.

3. On the **Behavior** step, configure how the deployment is delivered, how users are informed, and how failures are handled, and then select **Next**. The options under **Order of Events (from top to bottom)** are processed sequentially:

   - **Offer to user** - Turn on this toggle to deploy the action as a BigFix Offer.

     Note: An Offer lets end users choose and install software, patches, or other actions themselves through a self-service application, instead of having them deployed automatically by an administrator.

     When you turn on this toggle, set the following options:

     - **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
     - **Title** - Enter the title that identifies the offer to the user.
     - **Category** - Enter the category that groups the offer in the self-service application.
     - **Description** - Enter the text that explains what the offer does.
   - **Start downloading immediately** - When on, targeted endpoints begin downloading the required payloads as soon as the action is deployed.
   - **Before running message** - When on, the configured message appears to the end user before the action starts, to provide context, warnings, or a request for confirmation. Enter the message text, and then set the following options:
     - In **Notify user for**, select how long to show the message (for example, **10 minutes**), and in the **and then** list, select the follow-up action, such as **Run action immediately**.
     - **Allow user to save work** - Select this checkbox to let users save open work before the action runs.
     - **Allow user to cancel** - Select this checkbox to let users cancel the action.
     - **Show confirmation message before running action** - Select this checkbox to prompt users to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own, for example *Are you sure you want to run this action now?*
   - **While running message** - When on and a message is configured, the message appears during execution to show that the remediation is in progress. Enter the message text to display to the user.

- **Post deployment behavior** - When on, controls what happens on the device after the action completes. Select one of the following:
  - **Do nothing after action completes** - The device stays in its current state.
  - **Restart computer after action completes** - The device restarts when the action finishes.
  - **Shutdown computer after action completes** - The device shuts down when the action finishes.

  If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:
  - In **Message title (required)**, enter a short title, for example *Shutdown now*.
  - In **Message text (required)**, enter the message body that asks users to save any unsaved work.
  - In **Notify user for**, select how long to show the message, and in the **and then** list, select what happens when that time ends, such as **Shutdown automatically** or **Restart automatically**.
  - **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let users cancel the shutdown or restart.
- **On failure, retry** - When on, BigFix reattempts a failed action. Enter the number of retries, and then select one of the following options:
  - **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
  - **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.
- **Reapply whenever it becomes relevant again** - When on, BigFix reapplies the action automatically if it becomes relevant again after the initial deployment. Select **with a** to set the wait time between attempts, and **up to** to set the maximum number of times.

  Tip: Reapplying increases the success rate by accounting for temporary issues such as device disconnection or network latency.

Offer to user

Offer to user

Notify device owner of offer availability

Title

Category

Description

Order of Events (from top to bottom)

Start downloading immediately

Before running message

Enter your message here, that you want to be displayed in front of your users.

Notify user for 10 minute(s) and then Run action immediately

Allow user to save work

Allow user to cancel

Show confirmation message before running action

While running message

Enter your message here, that you want to be displayed in front of your users.

Post deployment behavior

Do nothing after action completes

Restart computer after action completes.

Shutdown computer after action completes.

On failure, retry 1 1 time(s)

and wait 1 hour(s) between attempts

Wait until computer has rebooted

Reapply whenever it becomes relevant again

with a 1 hour(s) wait between attempts

up to 3 time(s)

4. On the **Schedule** step, define the window during which the deployment remains in effect, and then select **Next**. For the settings, see the Schedule settings table. Select **Reset changes** to clear all scheduling fields and restore the defaults.

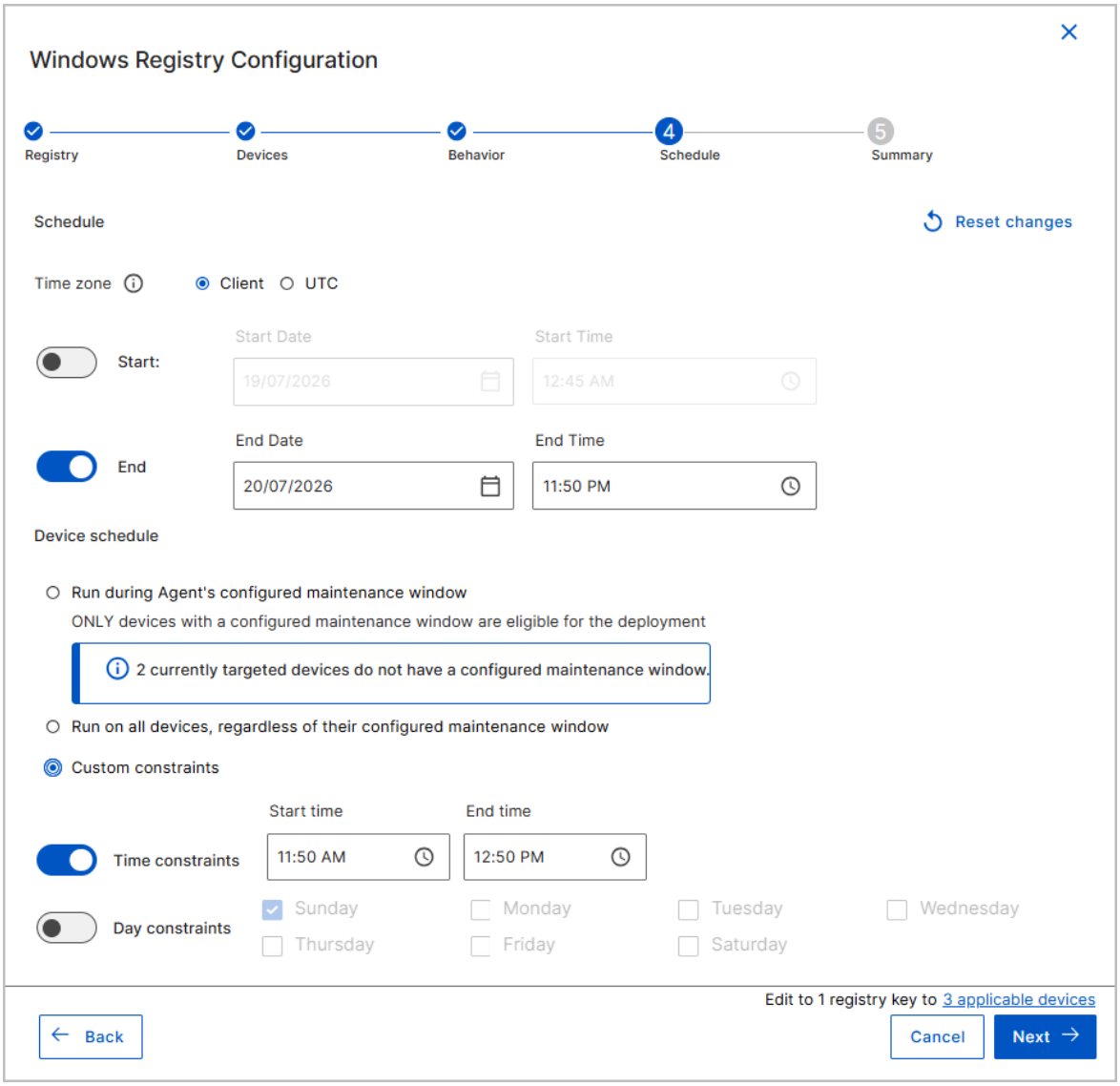


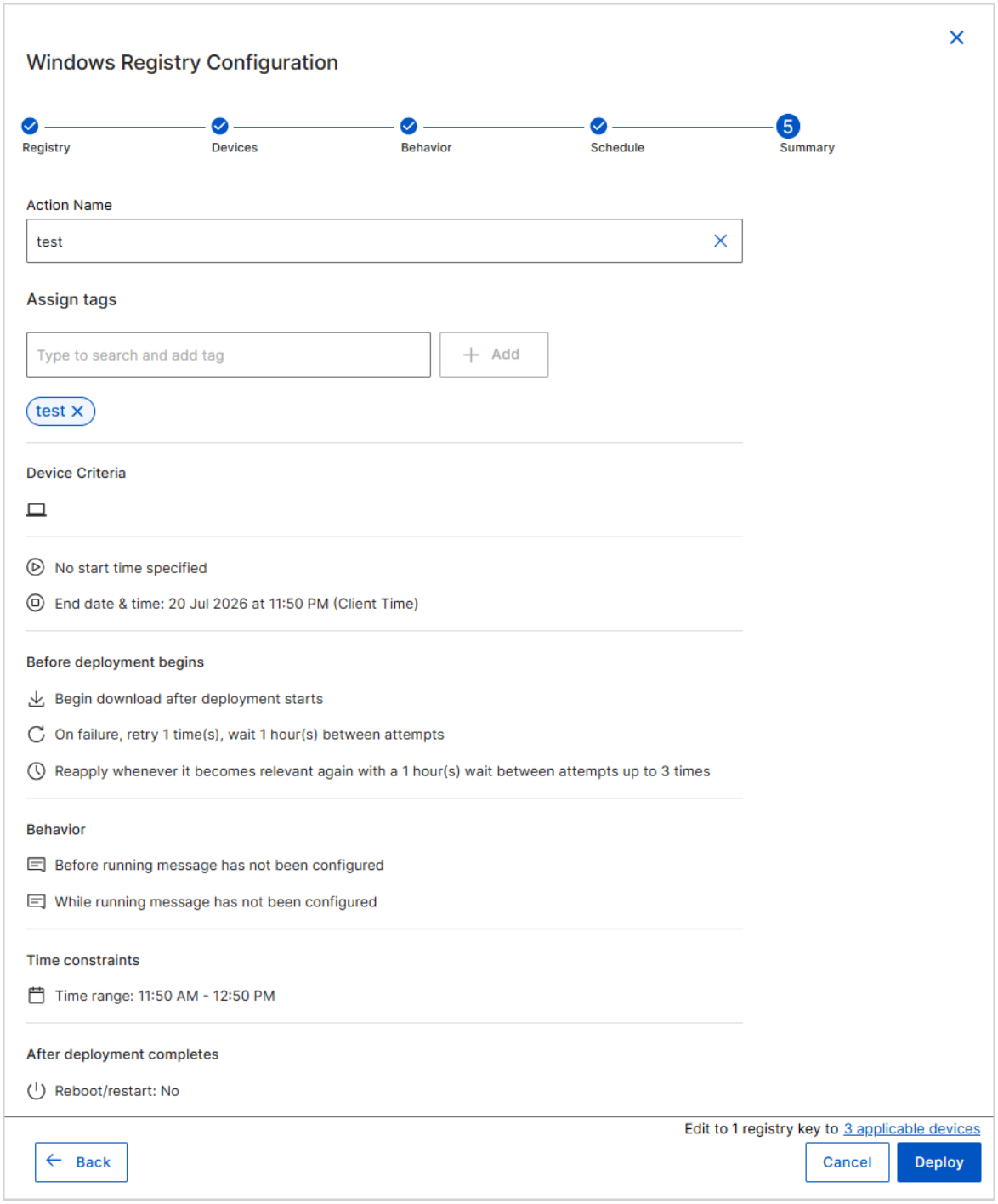
Table 55. Schedule settings

Settings	Description
Time zone	Select the time zone that applies to the start and end times: **Client** uses each endpoint's local time; **UTC** uses Coordinated Universal Time.
Start	Turn on **Start** to set when the deployment begins, and then select the **Start Date** and **Start Time**. If **Start** is off, the deployment can begin immediately.

Settings	Description
End	Turn on **End** to set when the deployment window closes, and then select the **End Date** and **End Time**.
Run during Agent's configured maintenance window	Restrict the deployment to devices that have a configured maintenance window. The deployment runs only within those windows. The wizard notes how many currently targeted devices don't have a configured maintenance window; those devices are excluded.
Run on all devices, regardless of their configured maintenance window	Override maintenance window restrictions. The deployment runs on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Control when a deployment can run by defining specific times and days. ◦ Turn on **Time constraints** to specify a **Start time** and **End time** when the deployment is allowed to run. ◦ Turn on **Day constraints** to limit the deployment to one or more days of the week.

5. On the **Summary** step, review a consolidated, read-only view of every option you selected - device criteria, start and end time, before-deployment settings, and behavior. This is the final checkpoint before deployment.
    - The **Behavior** section confirms the message and notification options that you set on the Behavior step, for example:
        - A message will be displayed before deployment begins.
        - Notify user for 10 minute(s), and then run action immediately.
        - A confirmation message will be displayed before deployment begins.
        - No message will be displayed while deployment is running.
    - In **Action Name**, enter a unique, meaningful name that describes the purpose of the action. This name appears in action history, logs, and dashboards, which helps you and your team identify and differentiate actions. Use descriptive terms, such as "Critical patch - May 2026 - Windows devices", for clarity and traceability.
    - In **Assign tags**, add one or more tags:
        - To add an existing tag, type to search for it, select it from the list, and then select **Add**.
        - To create a new tag, type the tag name, and then select **Add**.

      Assigned tags appear as chips below the field. To remove a tag, select the **X** on its chip. Tags are saved with the deployment and appear in the Deployment Manager; you can't change them after you deploy. For more information, see Managing Tags *(on page 51)*.



6. Select **Deploy** to deploy the action. The message **Deployment submitted successfully** confirms that the deployment was submitted.

Related information

Managing Tags *(on page 51)*

CyberFOCUS

CyberFOCUS is a threat intelligence and remediation feature within BigFix UI that combines MITRE ATT&CK intelligence with CISA Known Exploited Vulnerabilities (KEV) metadata and BigFix Fixlet and device relevance data. It enables users to assess their security posture and take proactive remediation actions based on real-world threat intelligence.

Note: To access the CyberFOCUS application, the user must enable the CyberFOCUS site, the BigFix Scanner site, and the platform-specific Known Exploited Vulnerabilities sites from the BigFix Console.

CyberFOCUS combines MITRE ATT&CK intelligence with CISA Known Exploited Vulnerabilities (KEV) metadata and BigFix Fixlet and device relevance data in a single dashboard, providing interactive filtering, correlation of vulnerabilities with attack tactics, and detailed reporting to help organizations prioritize and act on critical threats efficiently. It enables organizations to act swiftly on critical threats, minimizing the risk of exploitation. By leveraging CyberFOCUS, security teams can streamline vulnerability management, improve compliance with regulatory frameworks, and strengthen their overall security posture through detailed reporting and audit-ready insights.

Prerequisites for CyberFOCUS

Complete the required licensing, operator access, and role assignments to enable the CyberFOCUS application for users in the BigFix UI.

Note:

- You must have administrator rights in the BigFix Console to update license entitlements and operator permissions.
- You must be logged in as an administrator in the BigFix UI to assign roles.

To grant a user access to the CyberFOCUS application, you must complete the following three-step procedure:

1. Entitle the BigFix license to the **CyberFOCUS** site, the **BigFix Scanner** site, and the required platform-specific Known Exploited Vulnerabilities (KEV) sites. For full coverage, enable all of the following sites:
    - `http://sync.bigfix.com/cgi-bin/bfgather/bigfixscanner`
    - `http://sync.bigfix.com/cgi-bin/bfgather/kevcontentwindows`
    - `http://sync.bigfix.com/cgi-bin/bfgather/kevcontentnix`
    - `http://sync.bigfix.com/cgi-bin/bfgather/kevcontentmacos`
    - `http://sync.bigfix.com/cgi-bin/bfgather/kevcontentmobile`

2. Grant the BigFix operator account permission to access the CyberFOCUS site, the BigFix Scanner site, and the enabled platform-specific KEV site or sites.
3. Grant the user role access to the CyberFOCUS application in the BigFix UI:
    - Navigate to **Administration** > **Identity management** > **User & Role Management**. For more information, see Identity management *(on page 447)*.
    - When creating a new user or editing an existing role, navigate to the **Applications** step.
    - Turn on the toggle for the **CyberFOCUS** application.
    - Save the role configuration.

Result:

The user can now view and access the **CyberFOCUS** application under the **Resolve** menu in the BigFix UI.

Note: If the license is not entitled, the operator lacks site permissions, or the CyberFOCUS role is not assigned, the **CyberFOCUS** option will remain hidden from the user.

Vulnerability management

- CyberFOCUS correlates published threat intelligence with BigFix remediation content and device relevance data to provide actionable vulnerability reporting.
- The CISA KEV report uses the CISA Known Exploited Vulnerabilities catalog metadata. The MITRE APT report gets ATT&CK group-to-CVE mappings from MITRE ATT&CK data and enriches those CVEs with vulnerability metadata such as CVSS score, severity, due date, and remediation guidance from the CISA KEV catalog.
- Each vulnerability is linked to Fixlets, enabling automated remediation of affected devices. Additionally, correlations with MITRE ATT&CK tactics help security teams understand exploitation methods and take proactive defense measures.

Reports

CyberFOCUS in BigFix UI includes two key reports:

- CISA KEV Report *(on page 281)* – A collection of known exploited vulnerabilities. The CISA Known Exploited Vulnerabilities (KEV) web report uses the catalog metadata published by the Cybersecurity & Infrastructure Security Agency (CISA) and the associated CISA due dates, analyses and compares them with the patch levels of the devices in your BigFix environment, and visualizes the vulnerability intelligence as a bubble chart to assess and prioritize the vulnerabilities.

- MITRE APT report *(on page 286)* – Maps adversary groups and ATT&CK techniques to related CVEs using MITRE ATT&CK data, then correlates those CVEs with CISA KEV metadata and BigFix Fixlet and device exposure data to help prioritize mitigation. The report visualizes the analysis as a bar chart to help you take an informed decision to mitigate the security threat.

Both reports share one page layout: a heading with an **Updated** stamp that shows when the data was last refreshed, a **Summary** section that holds the chart, and a **CVEs** section that holds the table. Switch between the reports with the **CISA KEV** and **MITRE APT** buttons in the upper right of the page; the active report is highlighted. Selecting a CVE in either table opens its CVE details page *(on page 290)*.

Note:

- Both CISA KEV and MITRE reports are visualized using tables and charts.
- By default, the dashboard displays the CISA KEV report.
- The MITRE APT CVE view shows the intersection of MITRE ATT&CK CVE mappings, CISA KEV metadata, and BigFix exposure data. As a result, the report can contain fewer CVEs than a raw MITRE ATT&CK source list.

What the reports show by default

Each report applies a filter that keeps only the CVEs with an exposure count greater than zero, so the list reflects the work that remains rather than the whole published catalog. A CVE that no device is exposed to is filtered out rather than shown with a count of zero, and a CVE drops out of the report once it is fully remediated. The CISA KEV report also opens sorted by **N° exposures** in descending order, so the vulnerabilities that create the most work appear first.

Note: A report can list fewer CVEs than the published catalog contains. That is the default filter at work, not missing data.

How CyberFOCUS counts Fixlets, devices, and exposures

CyberFOCUS counts Fixlets, devices, and exposures in specific ways, and labels the same quantity differently on the report and on the details page. Use these definitions to read the counts correctly.

Table 56. CyberFOCUS counting terms

Term	Definition	Labels in the UI
Applicable Fixlet	A Fixlet that addresses the CVE, whether or not it is currently relevant to any of your devices. Answers "how many Fixlets exist for this vulnerability". Because a device that is already patched no longer makes a Fixlet relevant, the applicable count can be higher than the relevant count.	**N° applicable Fixlets** (CISA KEV table); **# of applicable Fixlets** (MITRE APT table); **Applicable fixlet content** (details)

Table 56. CyberFOCUS counting terms (continued)

Term	Definition	Labels in the UI
Relevant Fixlet	An applicable Fixlet that is relevant to at least one device, which means it still needs to be applied. Answers "how much work is left". As you remediate, this count falls while the applicable count stays the same.	**N° relevant Fixlets** (CISA KEV table); **# of relevant Fixlets** (MITRE APT table); **Relevant fixlet count** (details)
Unique device	A distinct device that the CVE affects, counted once however many Fixlets it needs.	**N° unique devices** (CISA KEV table); **Unique device count** (details); **# of Unique Devices** (CISA KEV chart axis)
Exposure	One mapping between a relevant Fixlet and an affected device. One device that needs three Fixlets is 3 exposures; two devices that each need the same three Fixlets are 6.	**N° exposures** (CISA KEV table); **# of exposures** (MITRE APT table and chart axis); **Exposure count** (details)

Operations teams work from the relevant count, because it is the work to schedule. Security teams work from the applicable count, because compliance is measured against how many of the applicable Fixlets have been satisfied.

For example, a CVE in the CISA KEV report that shows **N° applicable Fixlets** 8, **N° relevant Fixlets** 2, **N° unique devices** 2, and **N° exposures** 2 has eight Fixlets that address it, six of which your devices already satisfy. Two devices are still affected, and two Fixlet-to-device mappings remain. Remediating both mappings drops the exposure count to zero, and the CVE then falls out of the default view.

Note: The two reports label these counts differently. The CISA KEV **CVEs** table uses the `N°` form, for example `N° exposures`. The MITRE APT table, the chart axes, the chart tooltips, and the chart data table panels all use the `#` form, for example `# of exposures`. The labels differ, but the quantity is the same.

Fixlet Creation & Cyber Focus Content Pack

- The BigFix content team creates Fixlets.
- The CISA KEV content pack provides Fixlets for vulnerabilities at no additional cost for those with CyberFOCUS.
- Users can view vulnerability details in the BigFix Console or API.

Insights Gained from CyberFOCUS

By analyzing the CyberFOCUS dashboard, users can:

- Identify high-risk vulnerabilities currently exploited in the wild.
- Understand the impact on their organization based on affected devices.
- Assess the urgency of patching based on severity and exploitation status.

- Monitor remediation progress over time.
- Correlate threats with MITRE ATT&CK tactics to understand attack techniques used by adversaries.

Actions Users Can Take

CyberFOCUS allows users to take direct remediation actions, including:

- Automated Patching: Remediate *(on page 294)* vulnerable software and devices by deploying relevant Fixlets.
- Isolation of Compromised Systems: Quarantine affected endpoints to prevent lateral movement.
- Policy Enforcement: Apply security configurations to reduce exposure.
- Threat Hunting: Investigate indicators of compromise (IoCs) linked to KEV vulnerabilities.
- Reporting & Compliance: Generate reports for audits and compliance tracking.

Related information

Prescriptive Guidance *(on page 55)*

Managing Filters *(on page 35)*

CyberFOCUS remediation flow *(on page 294)*

CISA KEV Report

The CISA Known Exploited Vulnerabilities (KEV) Catalog is a curated list maintained by the Cybersecurity and Infrastructure Security Agency (CISA). It includes vulnerabilities actively exploited in the wild and requiring immediate remediation. Organizations can use this intelligence to prioritize patching efforts and reduce exposure to cyber threats.

Key Benefits of CISA KEV

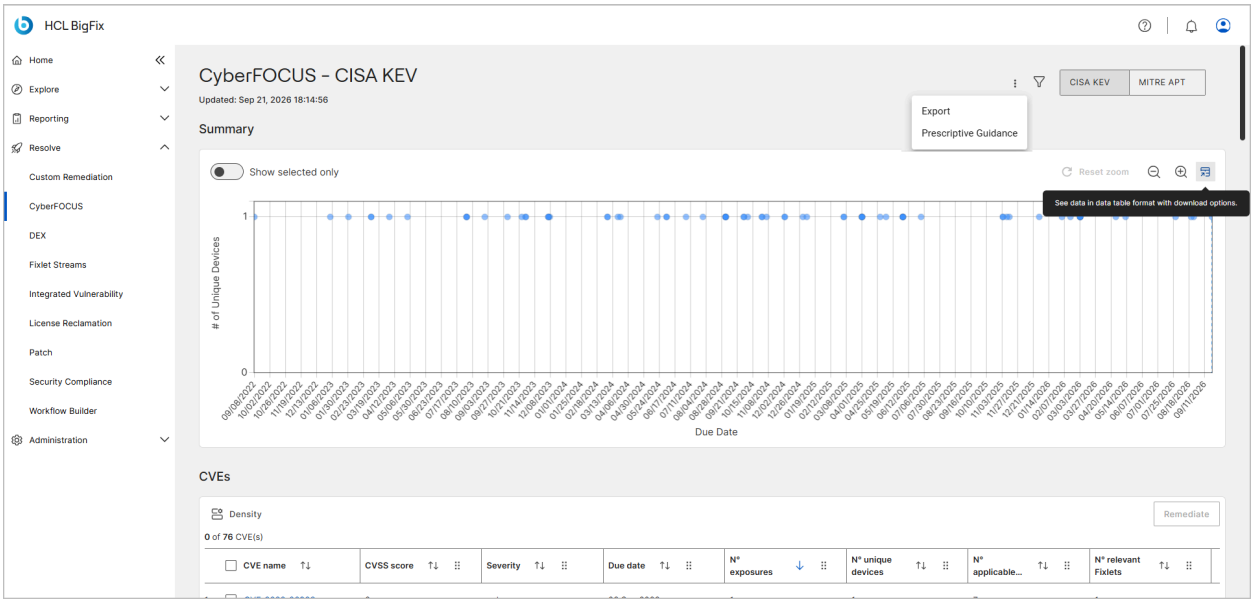
- Identifies vulnerabilities with confirmed exploitation in real-world attacks.
- Provides mandated patching deadlines (for U.S. federal agencies).
- Helps organizations prioritize security patches effectively.

Use Cases

- **Security Teams**: Helps in vulnerability management by focusing on critical threats.
- **Compliance**: U.S. federal agencies must comply with KEV patching deadlines.
- **Threat Intelligence**: Organizations can proactively monitor and defend against known exploited vulnerabilities.

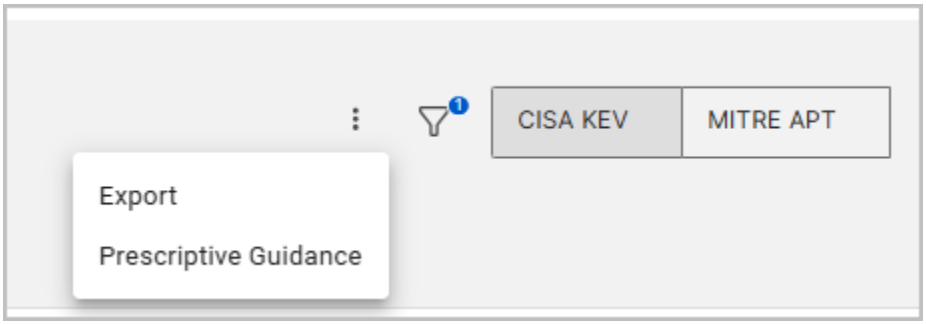
Accessing CISA KEV report

To access the **CyberFOCUS** app, expand **Resolve** from the side navigation, and then select **CyberFOCUS**. By default, the dashboard displays the CISA KEV report.



CISA KEV View and Utility Controls

The CISA KEV page includes utility controls that allow you to navigate between vulnerability reports, filter data, export information, and access remediation guidance.



- **Report Toggle (CISA KEV / MITRE APT)**Click the buttons to switch the dashboard view between the CISA KEV and MITRE APT reports.
- Click the 3-dot ⋮ menu to access the **Export** and **Prescriptive Guidance** tools.
  - **Export** – Click the ⋮ menu and select **Export** to open the Export panel. Select your preferred format (CSV, Excel, JPEG, PNG, or PDF), and click **Download** to save the CVE data. For detailed steps, see Exporting Data *(on page 30)* and Exporting Charts *(on page 32)*.
  - **Prescriptive Guidance** – Click the ⋮ menu and select **Prescriptive Guidance** to view actionable remediation recommendations. For more information, see Prescriptive Guidance for CISA KEV Scanner *(on page 284)* and Prescriptive Guidance *(on page 55)*.

- **Filter** – Click the Filter icon to open the filter panel. Use this tool to refine and reduce the number of CVEs displayed in the data table. For detailed steps, including how to save a filter and mark it as a favourite, see Global filter *(on page 36)*.



Note: By default, the system applies a filter where the **Property** is set to `N° exposures`, the **Operator** is `Greater than`, and the **Value** is `0`. The table is also sorted by `N° exposures` in descending order, so the vulnerabilities that create the most work in your environment appear first.

CISA KEV Report Data Representation and Interactions

CyberFOCUS displays CISA KEV data in an **interactive table and chart**, offering insights into an organization's exposure to known threats and take actions.

CISA KEV Chart Representation

- CyberFOCUS uses a **bubble chart** to visualize CISA KEV data:
  - **X-axis:** Due date of the CVE.
  - **Y-axis:** Number of unique affected devices.
  - **Bubble Size:** Exposure count (larger bubbles indicate higher exposure).
  - **Bubble Color:** CVSS3 severity (darker color = higher severity).
  - **today marker:** A labeled vertical line at the current date, separating deadlines that have passed from those still ahead.
  - **Behavior:**
    - Shrinking bubbles indicate that the vulnerabilities are partially remediated.
    - Fully remediated vulnerabilities disappear from the chart.

CISA KEV Chart Interactions

- **Hover for Details**: Hover over a bubble to view a tooltip with the `CVE name`, `Due date`, `# of unique devices`, and `# of exposures`. The tooltip shows the due date in `MM/DD/YYYY` format, for example `12/07/2023`.
- **Show Selected Only**: Filter the chart to display only the CVEs selected from the table.
- **Zoom Controls**: Zoom in or out to focus on specific data points, with an option to reset the zoom level.
- **Detailed CVE Insights**: Click on any bubble in the chart to open the CVE details page *(on page 290)*, which shows the CVE description, the affected devices, and the Fixlets that remediate it.
- **Chart Data Table**: Click the data table icon at the right end of the chart toolbar to open the plotted values as text. The icon tooltip reads **See data in data table format with download**

options. The panel is titled **CyberFOCUS CISA KEV** and lists `CVE name`, `Due date`, `# of unique devices`, and `# of exposures`, each sortable, with the due date in `MM/DD/YYYY` format. Select **Copy** to put the values on the clipboard, or choose **CSV**, **PDF**, or **XLS** from the **Export as** list to download them. Use this view when bubbles overlap too tightly to read, or with a screen reader. This is the chart's data, not the **CVEs** table. For detailed steps, see Viewing chart data in a table *(on page 33)*.

CISA KEV Table Representation

The table provides a structured list of vulnerabilities with key details. Above the table, Density *(on page 29)* sets the row spacing, the counter shows selected rows against the total (for example `0 of 135 CVE(s)`), and the header checkbox selects every CVE. For how the counts are calculated, see How CyberFOCUS counts Fixlets, devices, and exposures *(on page 279)*.

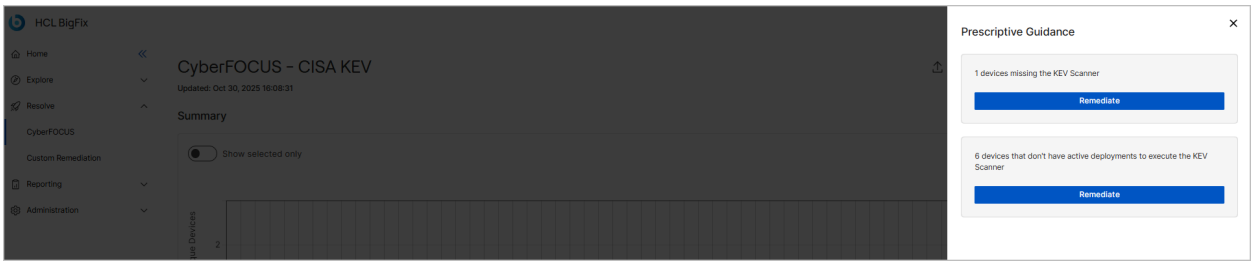
Column Name	Description
CVE name	The unique identifier for the vulnerability, sourced from the CISA KEV catalog.
CVSS score	The severity rating from the CISA KEV catalog, based on the Common Vulnerability Scoring S tem (CVSS).
Severity	The severity band that corresponds to the CVSS score (Critical, High, Medium, or Low). A CV no published score shows `unknown`.
Due date	The CISA remediation deadline, for example `12 May 2026`.
N° exposures	The total number of Fixlet-to-device mappings required to remediate the vulnerability. The ta sorted by this column by default.
N° unique devices	The number of unique devices in your environment affected by the CVE.
N° applicable Fixlets	Fixlets that address the CVE, whether or not they are currently relevant to a device.
N° relevant Fixlets	The subset of Fixlets that still need to be applied (after some patches have been deployed).

CISA KEV Table Interactions

- **Click for More Information**: Click on a CVE name in the table to open the CVE details page *(on page 290)*, which provides the description, the affected devices, the relevant Fixlets, and a direct link to the National Vulnerability Database (NVD).
- **Sort Functionality**: Sort vulnerabilities by any column in the table to quickly identify and prioritize threats.
- **Start Remediation**: Select one or more CVEs from the table and click the **Remediate** button to initiate the CyberFOCUS remediation flow *(on page 294)*.

Prescriptive Guidance for CISA KEV Scanner

Prescriptive Guidance *(on page 55)* on the CyberFOCUS app helps identify and remediate endpoints that are missing the required CISA KEV scanner and/or not actively running the KEV scanner.



You will see a device count in each prescriptive guidance. This data is retrieved using the corresponding **Site ID** and **Fixlet ID**.Click on the respective Remediate button to:

- Deploy the scanner to devices that do not have it installed.
- Execute the scanner on applicable devices.

How the Remediation Flow Works

Each remediate action is tied to a specific **Site ID** and **Fixlet ID**.

1. User clicks on the Remediate button to install KEV scanner or run the KEV scanner.
2. The **side panel** opens and automatically triggers the **remediation flow**.
3. The flow deploys the corresponding Fixlet depending on the action:
   - **Install or upgrade the scanner:** Deploys Fixlet ID `103` (Install or Upgrade Scanner) from the BigFix Scanner site (Site ID `16617`).
   - **Execute the scanner:** Deploys Fixlet ID `130` (Execute KEV Scanner) from the applicable platform-specific KEV site (for example, Site IDs `50045`–`50048`).
4. The user completes the wizard by providing a deployment name and confirming the deployment.
5. The deployment status can be viewed in the **Deployment Manager**.

With this, you can easily **install** and **run** the KEV scanner across your deployment, ensuring continuous vulnerability assessment and compliance.

Related information

CyberFOCUS *(on page 277)*

MITRE APT report *(on page 286)*

CyberFOCUS remediation flow *(on page 294)*

MITRE APT report

The **MITRE APT Report** in CyberFOCUS helps organizations understand and mitigate vulnerabilities by mapping them to adversary tactics and techniques. It provides valuable insights for security teams, enabling proactive defense strategies.

The MITRE APT report maps adversary groups and ATT&CK techniques to related CVEs using MITRE ATT&CK® data, then correlates those CVEs with CISA KEV metadata and BigFix Fixlet and device exposure data to help prioritize mitigation. It visualizes the analysis as a bar chart to help you take an informed decision to mitigate the security threat.

Important: The MITRE APT CVE view shows the intersection of MITRE ATT&CK CVE mappings, CISA KEV metadata, and BigFix exposure data. As a result, the report can contain fewer CVEs than a raw MITRE ATT&CK source list.

The **MITRE ATT&CK® Framework** documents real-world attack techniques used by Advanced Persistent Threat (APT) groups. For more details, visit MITRE ATT&CK.

Key Benefits of MITRE APT Report

- **MITRE APT Report** maps vulnerabilities to the **MITRE ATT&CK framework**, which tracks adversary tactics and techniques.
- The report analyses the data within MITRE ATT&CK and correlates the tactics, techniques, and procedures leveraged by APT groups to the BigFix Patch content based on the CVEs.
- It enriches those CVEs with vulnerability metadata such as CVSS score, severity, due date, and remediation guidance from the CISA KEV catalog.
- It highlights vulnerabilities linked to **known adversary techniques**.
- It helps security teams **understand attack vectors** and prepare defense strategies.

What the report includes

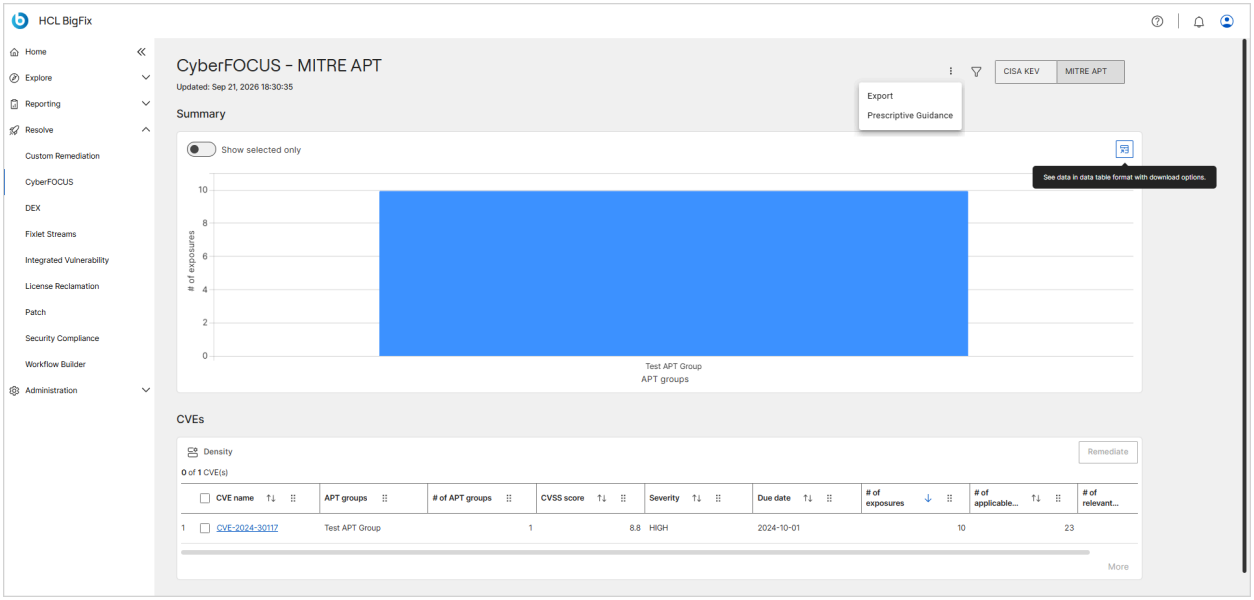
A CVE appears in this report only if it satisfies all three of the following:

- MITRE ATT&CK associates it with at least one APT group.
- It appears in the CISA KEV catalog, which supplies its CVSS score, severity, vector, due date, required action, vendor, and product.
- Fixlets exist for it that apply to the devices in your environment.

Because a CVE must clear all three tests, this report normally lists far fewer CVEs than the CISA KEV Report *(on page 281)*. A short list is the expected result, not a sign that data is missing.

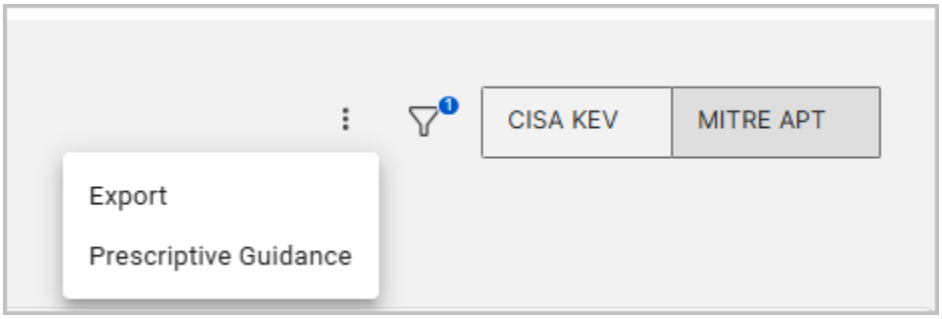
Accessing MITRE APT report

To view the MITRE APTs report, expand **Resolve** from the side navigation, select **CyberFOCUS**, and then click the **MITRE APT** tab.



MITRE APT View and Utility Controls

The MITRE APT page provides utility controls that enable you to toggle between vulnerability reports, refine the displayed data, export information, and access remediation guidance.



- **Report Toggle (CISA KEV / MITRE APT)** – Click the buttons to switch the dashboard view between the MITRE APT and CISA KEV reports.
- Click the 3-dot ⋮ menu to access the **Export** and **Prescriptive Guidance** tools.
  - **Export** – Click the ⋮ menu and select **Export** to open the Export panel. Select your preferred format (CSV, Excel, JPEG, PNG, or PDF), and click **Download** to save the CVE data. For detailed steps, see Exporting Data *(on page 30)* and Exporting Charts *(on page 32)*.
  - **Prescriptive Guidance** – Click the ⋮ menu and select **Prescriptive Guidance** to view actionable remediation recommendations. For more information, see Prescriptive Guidance *(on page 55)*.

- **Filter** – Click the Filter icon to open the filter panel. Use this tool to refine and reduce the number of CVEs displayed in the data table. For detailed steps, including how to save a filter and mark it as a favourite, see Global filter *(on page 36)*.



Note: By default, the system applies a filter where the **Property** is set to `N° exposures`, the **Operator** is `Greater than`, and the **Value** is `0`.

MITRE APT Report Data Representation and Interactions

CyberFOCUS displays MITRE APT data in an **interactive table and chart**, offering insights into an organization's exposure to known threats.

MITRE APT Chart Representation

The chart visualizes the exposure each adversary group represents:

- The stacked bars on the chart indicate different CVE's that have been associated to a given APT group.
- Colour of the bar indicates the unique CVE. The same colour on the different bars indicates that the same CVE can be leveraged by different APT groups.
- X-axis is labeled **APT groups** and lists the adversary groups.
- Y-axis is labeled **# of exposures** and measures the exposure each group represents.
- When a group is associated with a single CVE, its bar is one solid block rather than a stack.



Note: Unlike the CISA KEV chart, the MITRE APT chart has no zoom controls.

MITRE APT Chart Interactions

- **Hover for Details**: Hover over a bars in the graph to view additional details about the associated CVE and its impact on the applicable environment below the chart.
- **Show Selected Only**: Filter the chart to display only the CVEs selected from the table.
- **Chart Data Table**: Click the data table icon at the upper right of the chart to open the plotted values as text. The icon tooltip reads **See data in data table format with download options.** The panel is titled **CyberFOCUS MITRE APT**. Its first column is **APT groups**, and it then shows one sortable column per plotted CVE, headed by the CVE identifier, holding the exposure count that CVE contributes to each group. Select **Copy** to put the values on the clipboard, or choose **CSV**, **PDF**, or **XLS** from the **Export as** list to download them. A **More** button loads further rows. For detailed steps, see Viewing chart data in a table *(on page 33)*.
- **Missing device data**: When no device data is available, an information icon and this message appear in place of the bars, and the **CVEs** table shows an empty state. The axes still render.

MITRE APT Table Representation

The table provides a structured list of vulnerabilities with key details. It offers the same Density *(on page 29)* control, **Remediate** button, record counter, header checkbox, and sortable, reorderable columns as the CISA KEV table. A **More** button below the table loads further rows, and the table scrolls horizontally when the columns exceed the width of the page. When no CVEs are available, it shows an empty state. For how the counts are calculated, see How CyberFOCUS counts Fixlets, devices, and exposures *(on page 279)*.

Note: Unlike the CISA KEV table, which uses the `N°` form, the MITRE APT table column headings use the `#` form, for example `# of exposures`.

Column Name	Description
CVE name	Unique identifier for the vulnerability from the National Vulnerability Database (NVD). Select it to open the CVE details page.
APT groups	List of APT groups known to exploit the vulnerability, for example `Test APT Group`.
# of APT groups	Number of APT groups associated with the CVE.
CVSS score	Severity rating based on the Common Vulnerability Scoring System (CVSS), enriched from the CISA KEV catalog.
Severity	The severity band that corresponds to the CVSS score (Critical, High, Medium, or Low), enriched from the CISA KEV catalog.
Due date	The CISA remediation deadline for the vulnerability, enriched from the CISA KEV catalog.
# of exposures	The total number of Fixlet-to-device mappings required to remediate the vulnerability. The table is sorted by this column by default.
# of applicable Fixlets	Fixlets that address the CVE, whether or not they are currently relevant to a device.
# of relevant Fixlets	The subset of Fixlets that still need to be applied (after some patches have been deployed).

MITRE APT Table Interactions

- **Click for More Information**: Click on a CVE in the table to open the CVE details page *(on page 290)*, which provides the description, the affected devices, the relevant Fixlets, and a direct link to the National Vulnerability Database (NVD).
- **Sort Functionality**: Sort vulnerabilities by any column in the table to quickly identify and prioritize threats.

- **Start Remediation**: Select one or more CVEs from the table and click the **Remediate** button to initiate the CyberFOCUS remediation flow *(on page 294)*. The flow works the same way as it does from the CISA KEV report: the six steps are **Fixlets**, **Actions**, **Devices**, **Behavior**, **Schedule**, and **Summary**, and the **Fixlets** step opens pre-filtered with **Property** set to **CVE**, **Operator** set to **In**, and the CVEs you selected listed under **Selected Values**.

  Note: If no Fixlets match the selected CVEs, **Select the Fixlets to remediate** shows **No Data Available**, the counter reads `Selected 0 Fixlets to deploy`, and **Next** stays dimmed. A CVE can appear in the report with applicable Fixlets that are not relevant to any device, which leaves nothing to deploy.

Related information

CISA KEV Report *(on page 281)*

CyberFOCUS *(on page 277)*

CyberFOCUS remediation flow *(on page 294)*

CVE details page

The CVE details page answers the three questions that follow from spotting a vulnerability in a CyberFOCUS report: what is it, which of my devices have it, and what fixes it.

Open the page by selecting a CVE name in the **CVEs** table of either report, or by selecting a bubble in the CISA KEV chart. The heading reads **Details: *CVE ID***, for example `Details: CVE-2022-26923`, with an **Updated** stamp below it. A breadcrumb above the heading links back to the report.

The three tabs

Table 57. CVE details tabs

Tab	What it shows
Overview	Opens first. A **Description** card with the published description of the vulnerability and a **View at NVD** link, and a **Properties** card with the scoring, dates, affected product, and the Fixlet and device counts.
Devices	The devices in your environment that this CVE affects, with the identity and operating system of each one.
Fixlets	The relevant Fixlets that remediate this CVE, with the severity, category, and source of each one.

The **Devices** and **Fixlets** tabs each provide a Filter *(on page 40)* control, a Density *(on page 29)* control, a counter of selected rows against the total (for example `0 of 1 items`), sortable and reorderable columns, and a **More** button

that loads further rows. **More** is dimmed when every row is already shown. Both tables scroll horizontally when the columns exceed the width of the page.

Overview tab properties

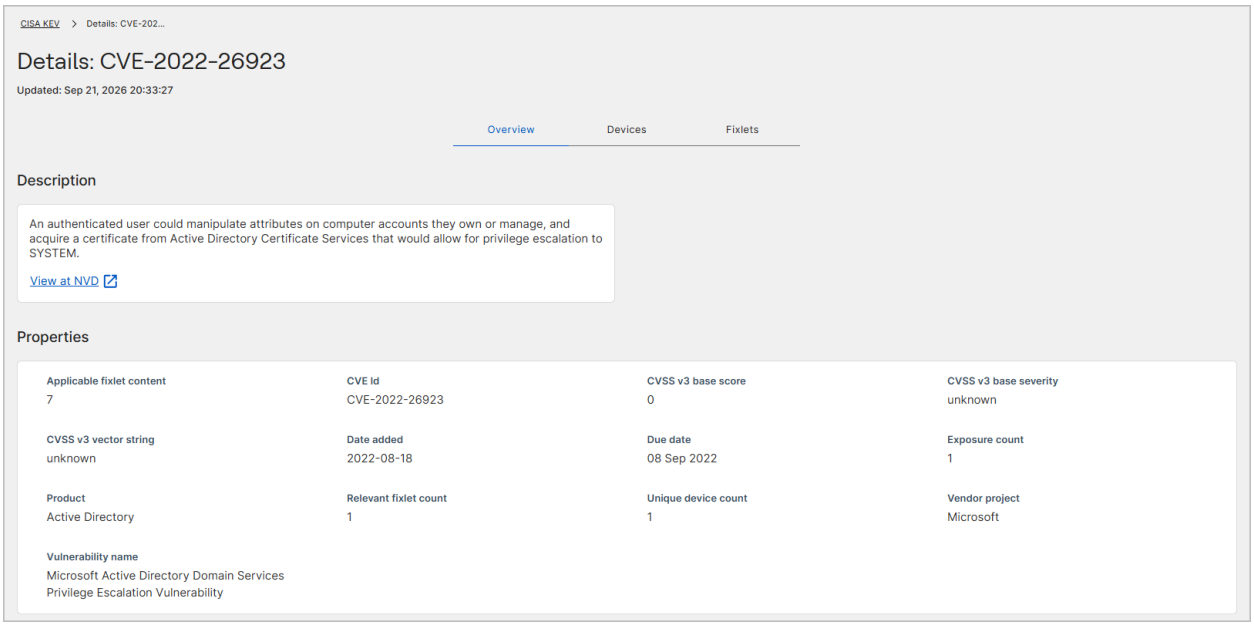


Table 58. CVE properties

Field	Description
Applicable fixlet content	The number of Fixlets that address this CVE, whether or not they are currently relevant to a device in your environment.
CVE Id	The Common Vulnerabilities and Exposures identifier, for example `CVE-2022-26923`.
CVSS v3 base score	The Common Vulnerability Scoring System version 3 base score published for the CVE.
CVSS v3 base severity	The severity band that corresponds to the base score.
CVSS v3 vector string	The CVSS version 3 vector that records how the base score was calculated.
Date added	The date the CVE was added to the source catalog, for example `2022-08-18`.
Due date	The remediation deadline published by CISA, for example `08 Sep 2022`.
Exposure count	The number of Fixlet-to-device mappings that remain to remediate the CVE.
Product	The affected product, for example `Active Directory`.
Relevant fixlet count	The number of Fixlets that are relevant to at least one device, and so still need to be applied.
Unique device count	The number of distinct devices in your environment that the CVE affects.
Vendor project	The vendor or project that owns the affected product, for example `Microsoft`.

Table 58. CVE properties (continued)

Field	Description
Vulnerability name	The descriptive name published for the vulnerability.

The **View at NVD** link opens the National Vulnerability Database record for the CVE in a new browser tab. Use it to confirm the published scoring or to read the full technical write-up.

Devices tab columns

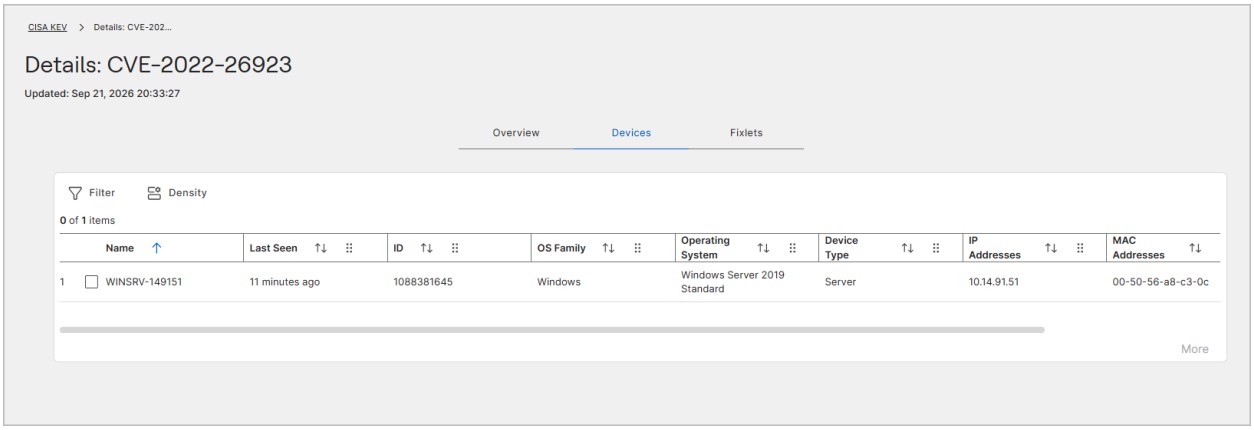


Table 59. Devices tab columns

Column	Description
Name	The name of the affected device.
Last Seen	How long ago the device last reported, for example `5 minutes ago`.
ID	The computer identifier of the device.
OS Family	The operating system family, for example `Windows`.
Operating System	The specific operating system and edition, for example `Windows Server 2019 Standard`.
Device Type	The device category, for example `Server`.
IP Addresses	The IP addresses reported by the device.
MAC Addresses	The hardware addresses reported by the device.
DNS Name	The DNS name of the device. Scroll the table horizontally to see this column.

Fixlets tab columns

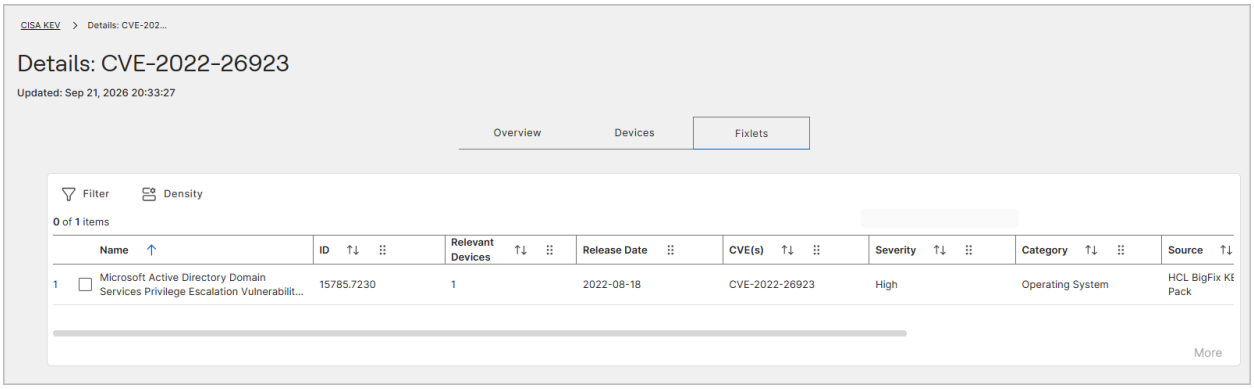


Table 60. Fixlets tab columns

Column	Description
Name	The title of the Fixlet.
ID	The Fixlet identifier, for example `50045.7230`.
Relevant Devices	The number of devices on which the Fixlet is currently relevant.
Release Date	The date the Fixlet was published, for example `2022-08-18`.
CVE(s)	The CVE identifiers that the Fixlet addresses.
Severity	The severity rating of the Fixlet, for example `High`.
Category	The content category of the Fixlet, for example `Operating System`.
Source	The content site that published the Fixlet, for example `Known Exploited Vulnerabilities Content Pack for Windows`. Sites are split into per-operating-system content packs, so this value can also name the NIX, macOS, or Mobile pack.
Source ID	The identifier the source site uses for the content, which for KEV content is the CVE identifier.
Download Size	The size of the payload the Fixlet downloads. Shows `[ null ]` when the Fixlet has no download.

Why the Fixlets tab can show fewer Fixlets than you expect

The **Fixlets** tab lists **relevant** Fixlets, which means the ones that still need to be applied to at least one device. The count of every Fixlet that addresses the CVE, including the ones your devices already satisfy, appears on the **Overview** tab as **Applicable fixlet content**.

The two numbers answer different questions. Operations teams use the relevant count, because it is the work that remains. Security teams use the applicable count, because compliance is measured against how many of the applicable Fixlets have been satisfied. See How CyberFOCUS counts Fixlets, devices, and exposures *(on page 279)*.

Related information

CISA KEV Report *(on page 281)*

MITRE APT report *(on page 286)*

CyberFOCUS *(on page 277)*

CyberFOCUS remediation flow

The **CyberFOCUS remediation flow** streamlines the process of identifying and addressing security vulnerabilities (CVEs) efficiently.

From the CyberFOCUS dashboard, to initiate remediation and set up your custom remediation flow, complete the following steps.

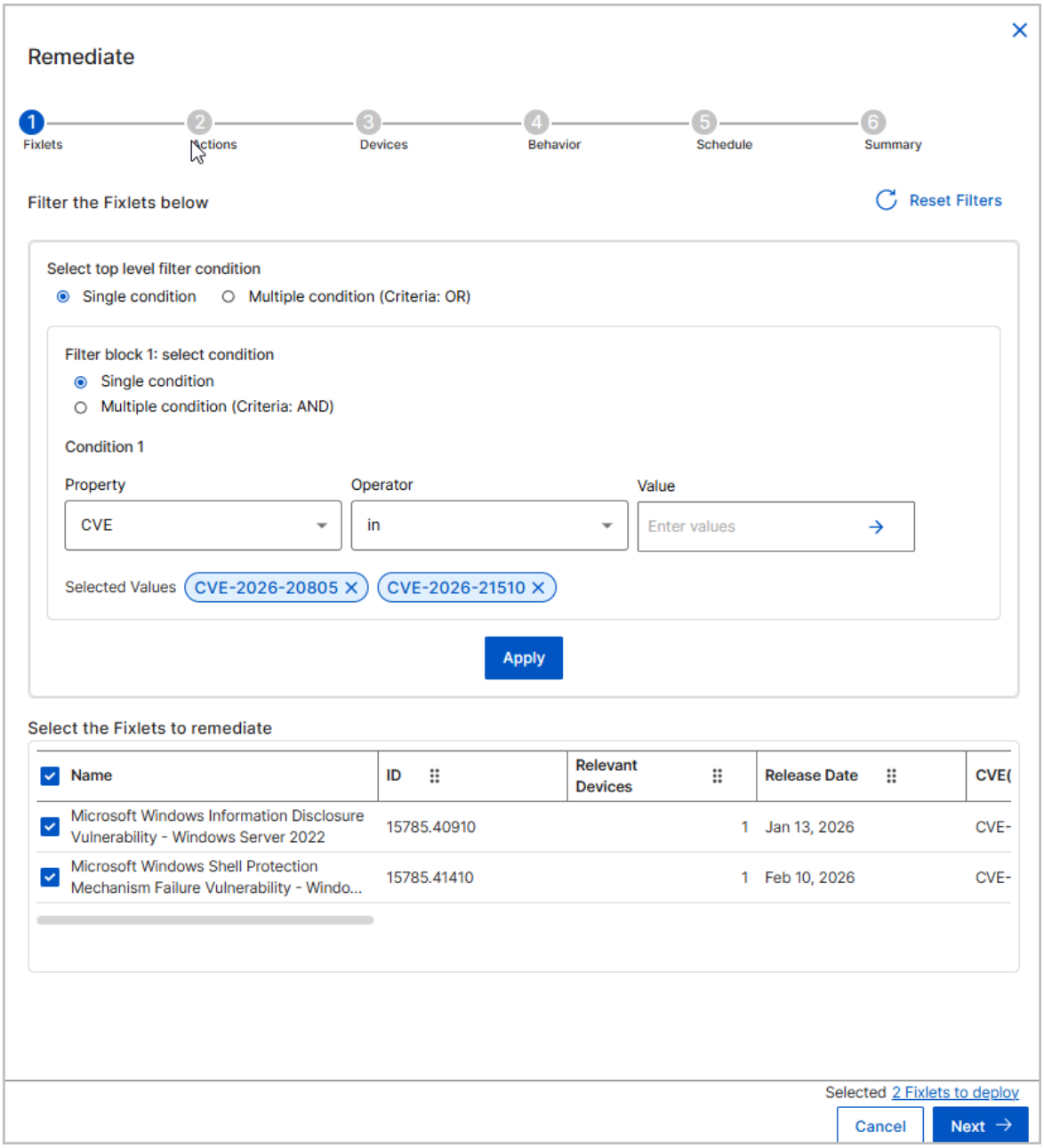
1. Accessing the Remediate widget from CyberFOCUS dashboard

1. From the **CVEs** table of either the CISA KEV Report *(on page 281)* or the MITRE APT report *(on page 286)*, select one or more CVEs. The **Remediate** button becomes active. It stays dimmed while nothing is selected.
2. Click the **Remediate** button to open the Remediate widget.

2. Configuring the remediation steps

To configure a custom remediation flow, complete the following steps:

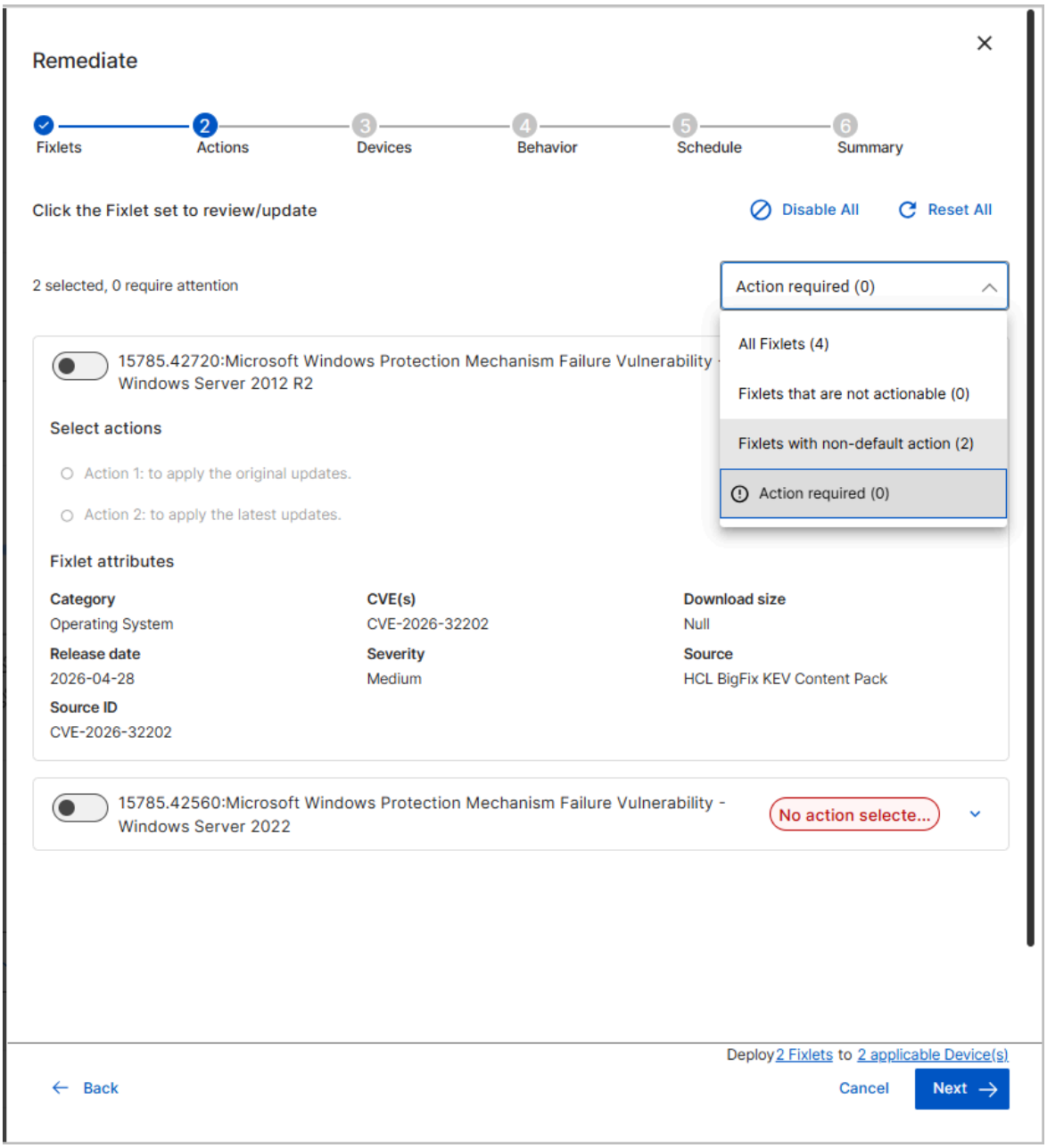
1. **Fixlets** - In this step, you filter and select the Fixlets you want to remediate.



   - All selected Fixlets are listed in a table with the columns **Name**, **ID**, **Relevant Devices**, **Release Date**, and **CVE(s)**.
   - To narrow the list to specific vulnerabilities, set **Property** to **CVE** and **Operator** to **In**, then enter the CVE identifiers. Each one appears as a chip under **Selected Values**, which you can remove individually.
   - You can apply filters using **Single condition** or **Multiple condition (Criteria: AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see Filter by query *(on page 40)*.

- Fixlet Table – Review the list of Fixlets.
- Select Fixlets – Use checkboxes to choose one or more Fixlets for remediation. A counter shows how many are selected.
- Next/Cancel – Click **Next** to continue to Actions, or **Cancel** to exit.

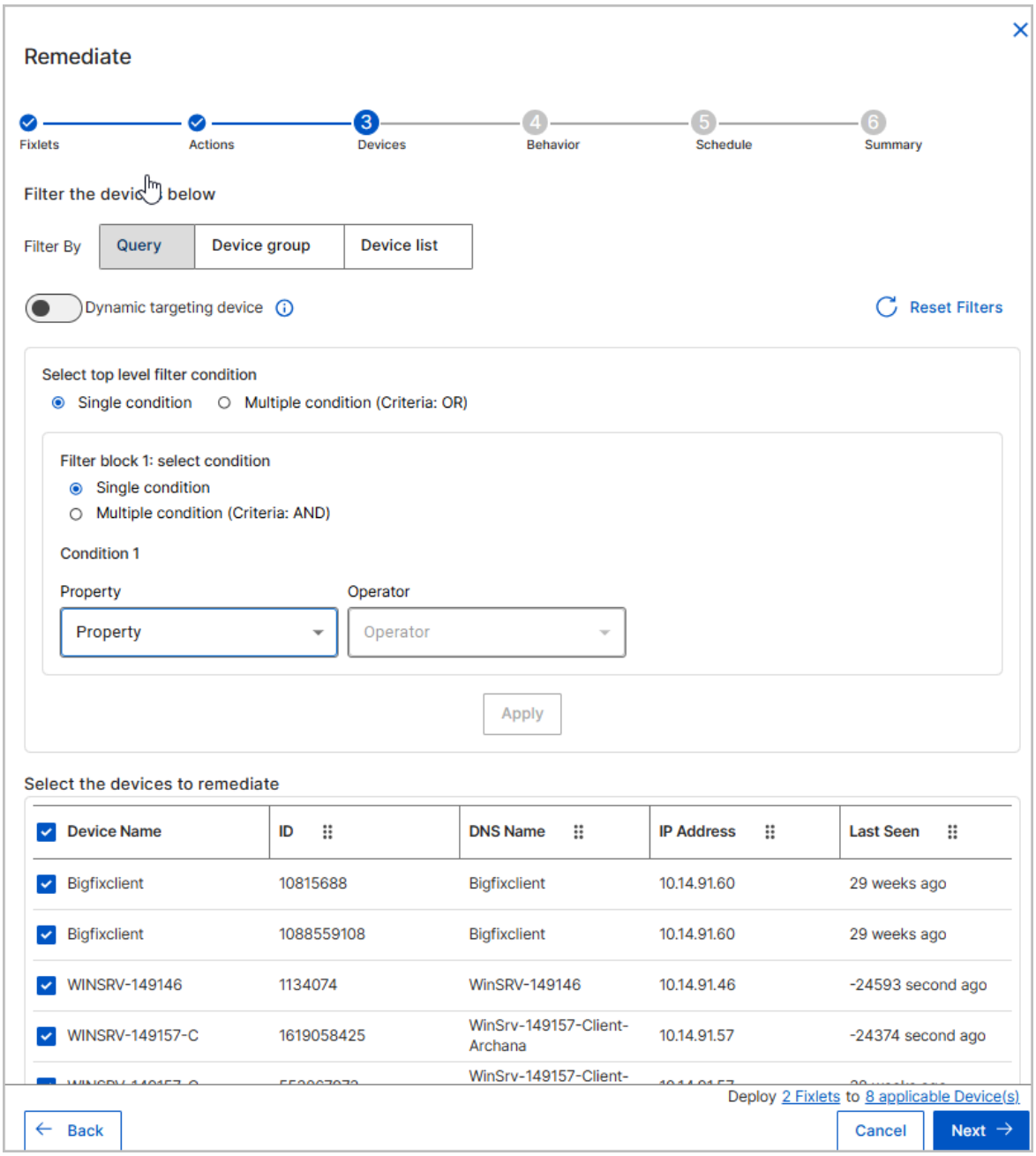
2. **Actions** - Review or update Fixlet actions. In this tab, confirm the actions you want the Fixlets you have selected to perform. This is important because not every Fixlet has a single, default action. It is also possible to remove Fixlets that do not have any actions that can be performed on the devices selected in the prior tab.



- The Actions step lists all selected Fixlets, with a status line above them such as `2 selected, 0 require attention`.
- Action filter drop-down – Allows you to refine which Fixlets are shown in the list. Each option shows a count in parentheses. Available filter options:
  - **All Fixlets** – Displays all Fixlets in the remediation set.
  - **Fixlets that are not actionable** – Displays Fixlets that cannot be acted upon.
  - **Fixlets with non-default action** – Shows Fixlets that do not have a predefined default action.
  - **Action required** – Filters Fixlets that require immediate attention.
- Under **Select actions**, choose the appropriate radio button for the remediation:
  - **Action 1**: To apply the original updates.
  - **Action 2**: To apply the latest updates.
- Review the **Fixlet attributes** provided in the details pane to confirm accuracy. The attributes are **Category**, **CVE(s)**, **Download size**, **Release date**, **Severity**, **Source**, and **Source ID**.
- A Fixlet for which you have not yet chosen an action shows a **No action selected** badge. Select an action for it before you continue.
- Each Fixlet has a toggle switch to enable or disable its deployment.
- Ensure the toggle switch next to the Fixlet is set to **On**.
- You can use Disable All or Reset All options as needed.
- Verify the deployment summary link at the bottom right, which reads `Deploy 2 Fixlets to 2 applicable Device(s)` once actions are selected.

Once this information is provided, click **Next** to proceed to the Devices tab.

3. **Devices** - This step allows you to confirm the devices for the deployment. Choose to deploy to all applicable devices or utilize various filters to narrow down the deployment size. Since filtering is optional, it is possible to skip this step by clicking **Next**. you select which devices will be included in the deployment. You have three main approaches:



a. **Filter by Query**

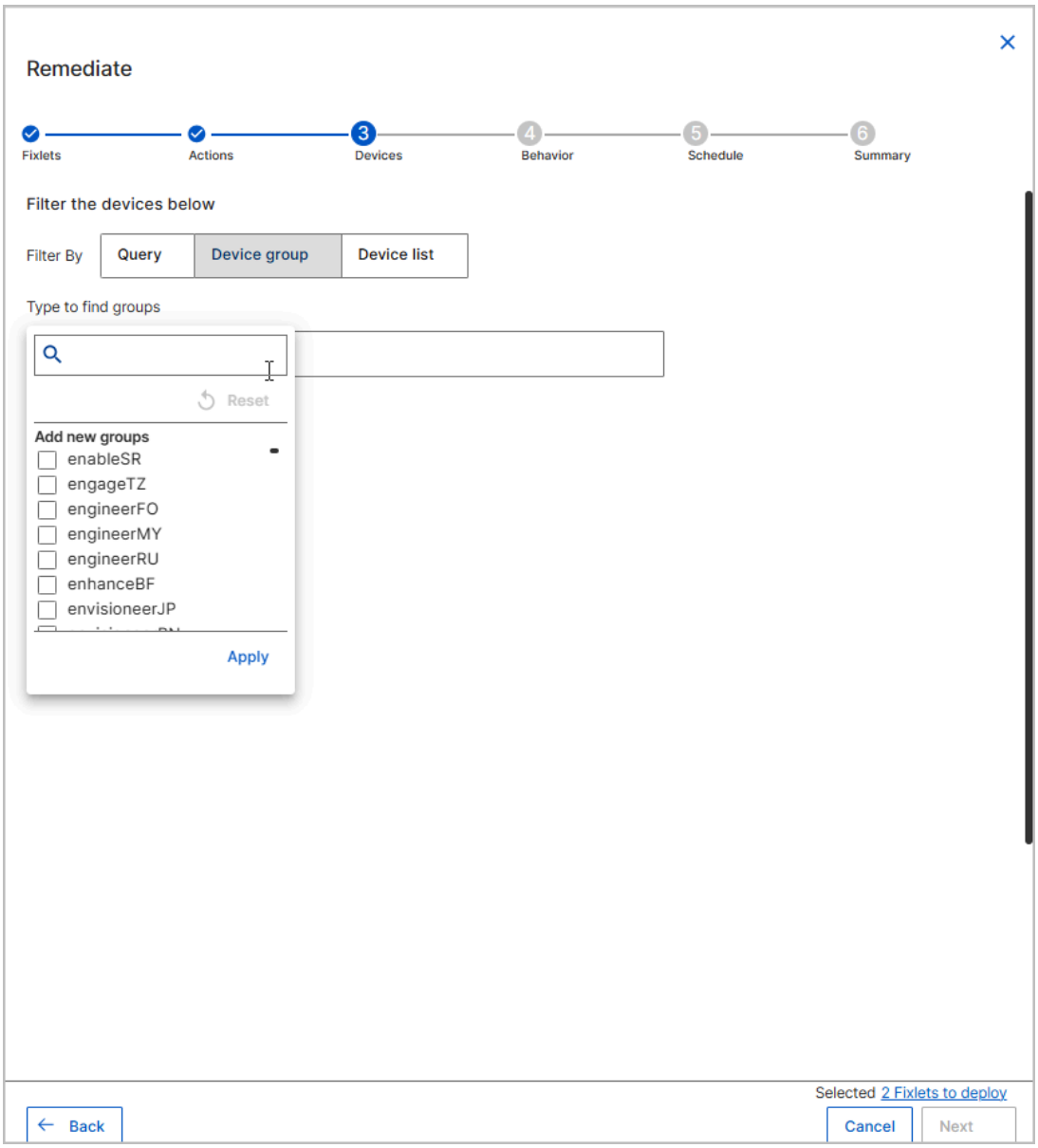
   i. You can apply filters using **Single condition** or **Multiple condition (Criteria: AND/OR)** options to refine the Fixlet list. You can click on **Reset Filters** to clear filters. For more information, see Filter by query *(on page 40)*.

   ii. By default, the device table displays all devices that match the query, with the columns **Device Name**, **ID**, **DNS Name**, **IP Address**, and **Last Report Time**.

   iii. Dynamic Targeting device Option:

- Within this approach, you can enable the **Dynamic Targeting Device** toggle.
- Dynamic filters define a matching criteria for devices to evaluate continuously until the deployment ends. Any device that matches this filter after the deployment has been created, will have this deployment applied.
- New devices that match the criteria are automatically added.
- A **Preview of dynamically applicable targeted devices** is shown to confirm eligibility.

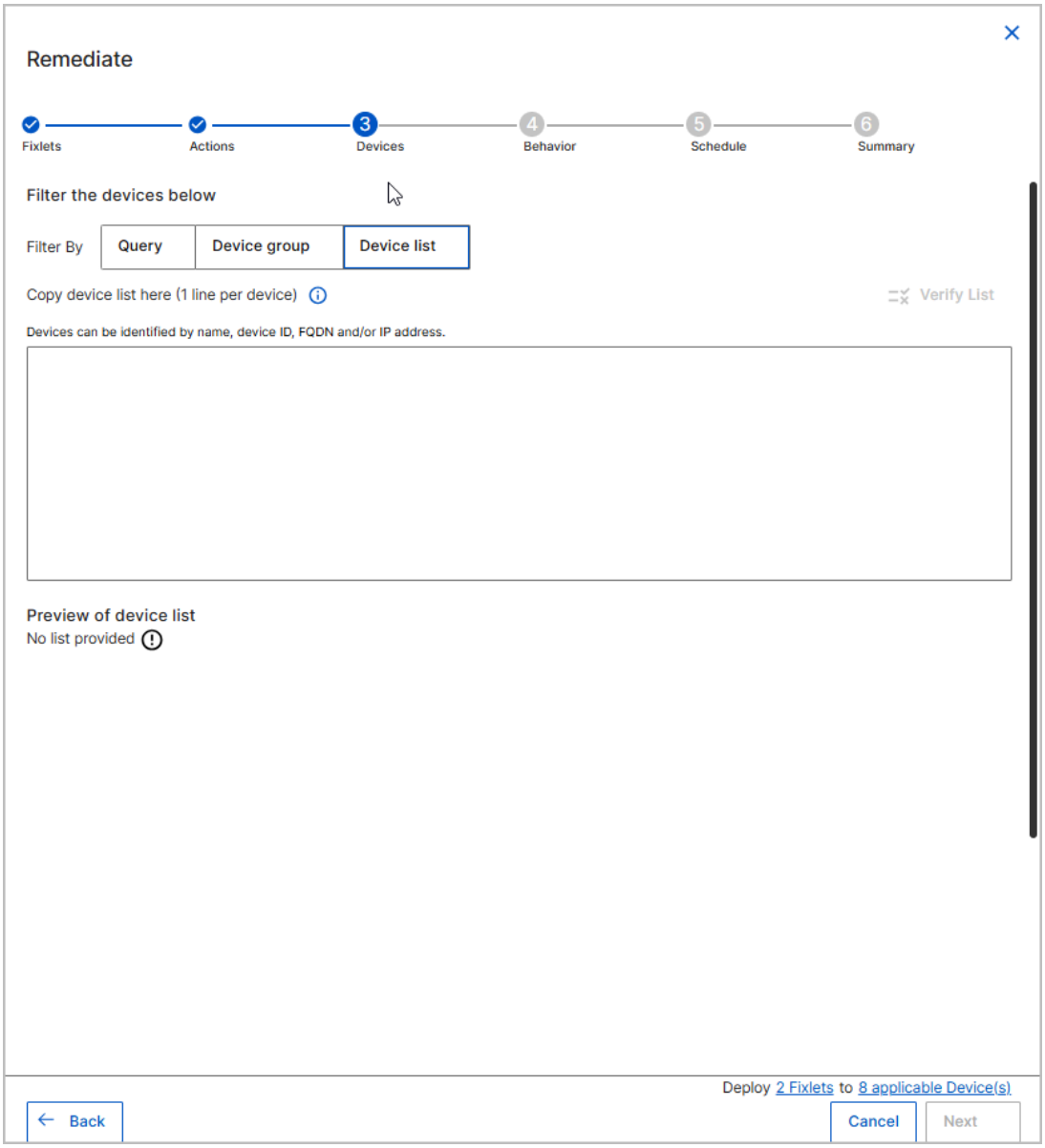
b. **Filter by Device group**- Select a pre-defined device group to target.



i. Locate and select your target groups:

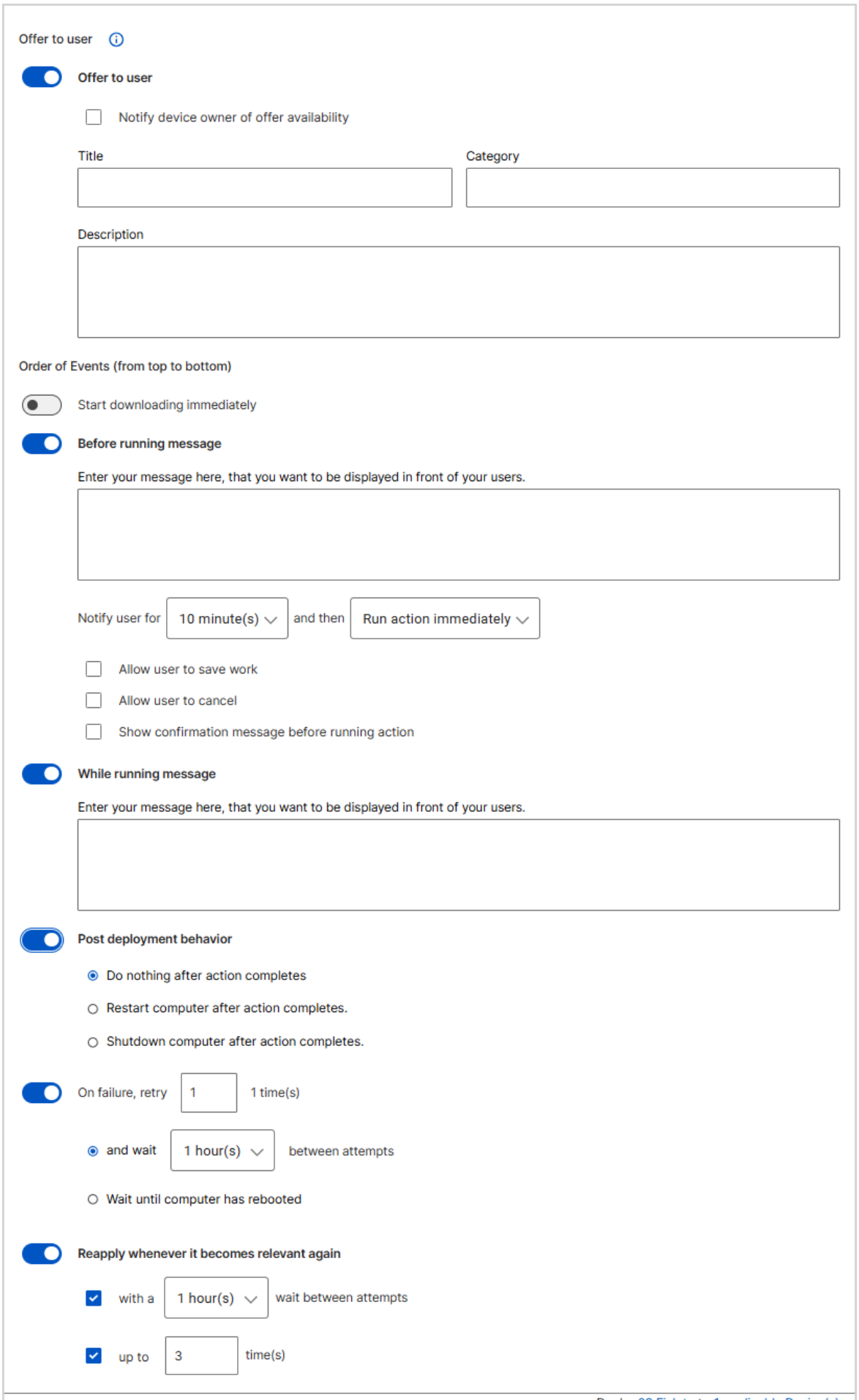
- **Search**: Use the search bar to type and quickly find specific groups by name.
- **Select**: Check the box next to one or more groups under the **Add new groups** list.
- **Reset**: Click **Reset** if you need to clear your current selections within the menu.
- Click **Apply** within the dropdown menu to confirm your group selection.

c. **Filter by Device List** - This option allows to input a fixed list of devices where the deployment will be applied. Devices can be identified using their name, DNS, and IP address.



   i. Regardless of how they are identified, each device must be in a separate row.
   ii. A maximum of 1,000 devices can be added in a single device list. If you intend to target more than 1,000 devices using device lists for filtering, create separate deployments.
   iii. Use Verify List to confirm the entries before proceeding.
   iv. The Preview area shows the final static list that will be targeted.
   v. Once the appropriate filters have been selected, or if no filter is needed, click **Next**.

4. **Behavior** - Some deployments can affect many devices simultaneously. The sequence tab provides you with control over deployment timing, display of alerts indicating Fixlet deployment availability for devices, and actions upon deployment completion. Note that selecting any of the provided options is not mandatory.


Offer to user
Offer to user
Notify device owner of offer availability
Title
Category
Description
Order of Events (from top to bottom)
Start downloading immediately
Before running message
Enter your message here, that you want to be displayed in front of your users.
Notify user for
10 minute(s)
and then
Run action immediately
Allow user to save work
Allow user to cancel
Show confirmation message before running action
While running message
Enter your message here, that you want to be displayed in front of your users.
Post deployment behavior
Do nothing after action completes
Restart computer after action completes.
Shutdown computer after action completes.
On failure, retry
1
1 time(s)
and wait
1 hour(s)
between attempts
Wait until computer has rebooted
Reapply whenever it becomes relevant again
with a
1 hour(s)
wait between attempts
up to
3
time(s)

Offer to user: Enable this toggle to deploy the action as a BigFix "Offer".

Note: An Offer allows end-users to choose and install software, patches, or other actions themselves through a self-service application, rather than having them automatically deployed by an administrator.

When you enable this toggle, set the following options:

- **Notify device owner of offer availability** - Select this checkbox to alert the device owner when the offer becomes available.
- **Title** - Enter the title that identifies the offer to the user.
- **Category** - Enter the category that groups the offer in the self-service application.
- **Description** - Enter the text that explains what the offer does.

Under **Order of Events (from top to bottom)**, the behavior tab presents the following controls in the order in which they take effect:

a. **Start downloading immediately** - Some Fixlets can contain large files. This option allows users to control whether all applicable devices should begin downloading the Fixlet as soon as the deployment is created.

b. **Before running message** - As a device may become unresponsive while a Fixlet is being deployed, this gives users the option to display a warning for an amount of time before the Fixlet is applied. This may also be useful if a restart is required, so end users can save work.

   Enable the toggle and set the following options:

   - Enter the message text to display to the user before the action runs.
   - In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Run action immediately**).
   - **Allow user to save work** - Select this checkbox to let the user save open work before the action runs.
   - **Allow user to cancel** - Select this checkbox to let the user cancel the action.
   - **Show confirmation message before running action** - Select this checkbox to prompt the user to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own (for example, *Are you sure you want to run this action now?*).

c. **While running message** - As a device may be unresponsive while a Fixlet is being deployed, this allows users to write a message that will be displayed on the screen until the deployment is complete. Enable the toggle, and then enter the message text to display to the user.

d. **Post deployment behavior** - Enable this toggle to control what happens on the device after the action completes. Select one of the following options:

- **Do nothing after action completes** - The device stays in its current state.
- **Restart computer after action completes** - The device restarts when the action finishes.
- **Shutdown computer after action completes** - The device shuts down when the action finishes.

If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:

- **Message title (required)** - Enter a short title (for example, *Shutdown now*).
- **Message text (required)** - Enter the message body that asks the user to save any unsaved work.
- In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends (for example, **Shutdown automatically** or **Restart automatically**).
- **Allow user to cancel shutdown** or **Allow user to cancel restart** - Select this checkbox to let the user cancel the shutdown or restart.

e. **On failure, retry** - Occasionally, deployments fail to complete successfully on a device. Should this occur, this allows users to determine if they would like BigFix to automatically try the deployment again. Enable the toggle, enter the number of retries, and then select one of the following options:

- **and wait** - Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **Wait until computer has rebooted** - Select this option to retry the action only after the device restarts.

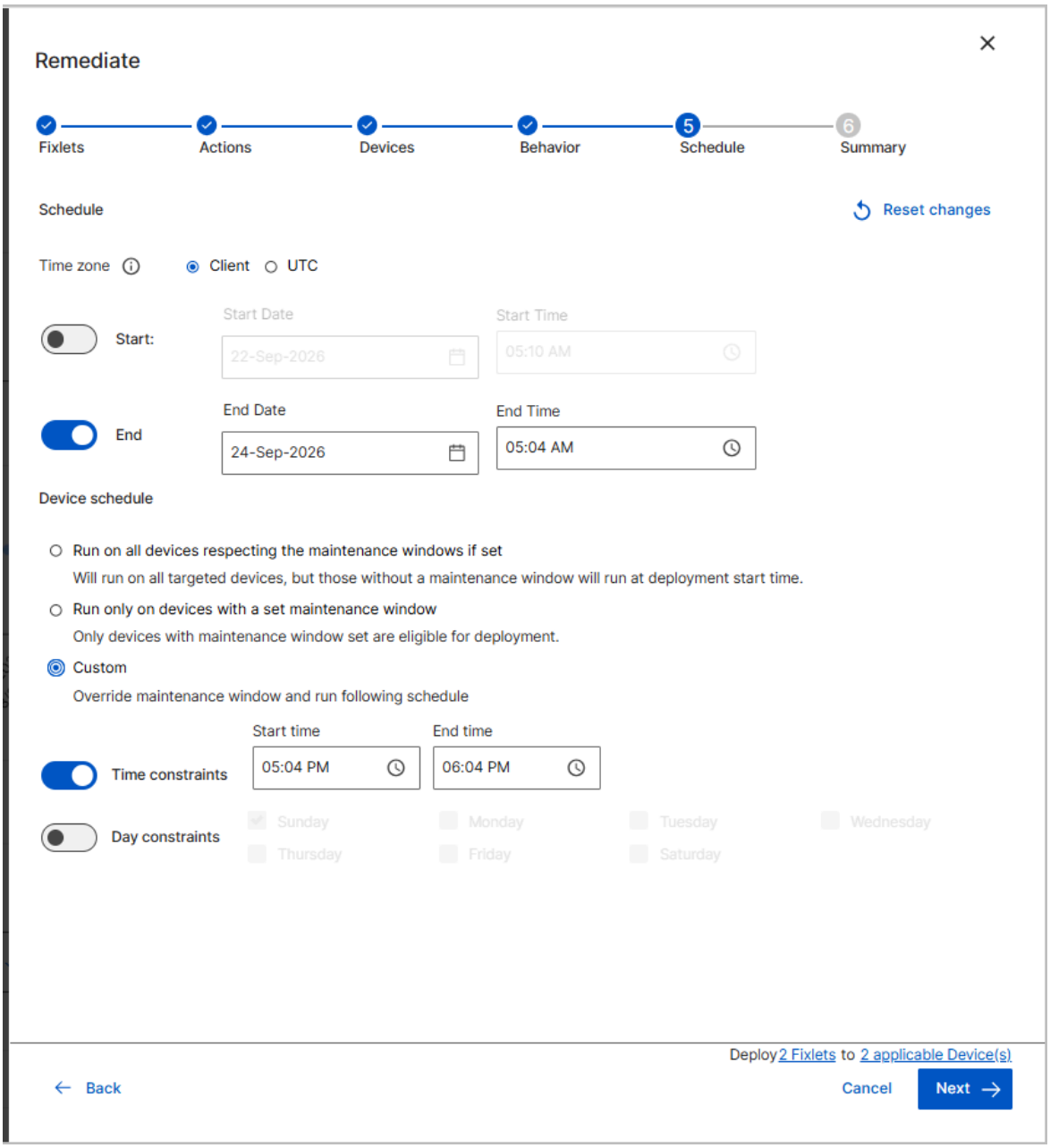
f. **Reapply whenever it becomes relevant again** - This option automatically reapplies a Fixlet if it becomes relevant again after the initial deployment. Enable the toggle, and then set the following options:

- **with a** - Select this checkbox and set the interval (for example, **1 hour**) that BigFix waits between attempts.
- **up to** - Select this checkbox and enter the maximum number of times (for example, **3**) that BigFix reapplies the Fixlet.

After selecting the desired sequence, click **Next** to proceed to the schedule tab.

5. **Schedule** - not required. Determining a deployment's start and end time gives BigFix users a tool to control their deployments. Typically, deployments do not happen immediately. Some devices may be powered down, or disconnected from the Internet, or otherwise unable to have the Fixlet applied. Scheduling allows to control how long BigFix will attempt this particular deployment.

   There may be other reasons to control the end time. For example, an organization may wish to ensure that all deployments run overnight to minimize business impact.



- **Time zone**: Select **Client** to use the time zone where each device is located, or **UTC**.
- **Start**: Turn on this toggle and select the **Start Date** and **Start Time** when BigFix begins attempting to apply the deployment.
- **End**: Turn on this toggle and select the **End Date** and **End Time** when BigFix stops attempting to apply the deployment.
- If no start time is set, BigFix begins the deployment immediately.
- **Reset changes** returns the schedule to its default state.

Under **Device schedule**, select one of the following:

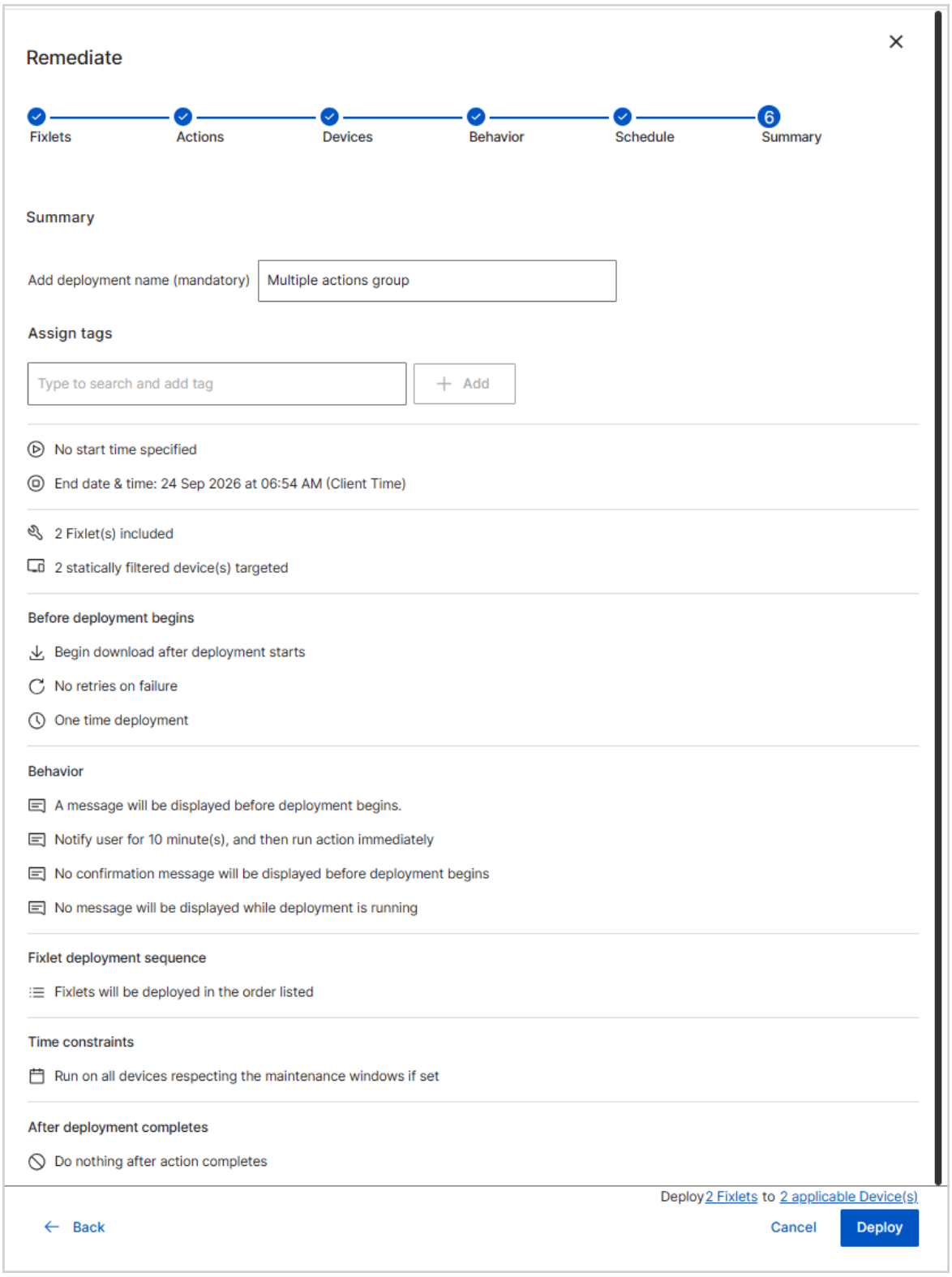
- **Run on all devices respecting the maintenance windows if set** - Runs on all targeted devices. Devices without a maintenance window *(on page 126)* run at the deployment start time.
- **Run only on devices with a set maintenance window** - Only devices that have a maintenance window set are eligible for deployment.
- **Custom** - Overrides the maintenance window and runs on the schedule you define below.

Selecting **Custom** enables these constraints:

- **Time constraints**: Specify the **Start time** and **End time** range when the deployment is allowed to run, for example 05:04 PM to 06:04 PM.
- **Day constraints**: Optionally, choose one or more days of the week to further limit deployment, for example only weekends or weekdays.

After selecting the desired schedule, click **Next** to proceed to the summary tab.

6. **Summary** - The summary tab shows all of the choices made related to the deployment created. This allows to review all of the things the deployment will do in one location.


Remediate
Fixlets
Actions
Devices
Behavior
Schedule
6
Summary
Summary
Add deployment name (mandatory)
Multiple actions group
Assign tags
Type to search and add tag
Add
No start time specified
End date & time: 24 Sep 2026 at 06:54 AM (Client Time)
2 Fixlet(s) included
2 statically filtered device(s) targeted
Before deployment begins
Begin download after deployment starts
No retries on failure
One time deployment
Behavior
A message will be displayed before deployment begins.
Notify user for 10 minute(s), and then run action immediately
No confirmation message will be displayed before deployment begins
No message will be displayed while deployment is running
Fixlet deployment sequence
Fixlets will be deployed in the order listed
Time constraints
Run on all devices respecting the maintenance windows if set
After deployment completes
Do nothing after action completes
Deploy 2 Fixlets to 2 applicable Device(s)
Back
Cancel
Deploy

- **Add deployment name (mandatory)**: Enter a name for the deployment. This field is required.
- **Assign tags**: Optionally, search for a tag and select **Add** to assign it to the deployment. See Managing Tags *(on page 51)*.

Below these fields, the summary lists the start and end times, the number of Fixlets included, the number of devices targeted, and the download, retry, and behavior settings you chose.

After reviewing your selections, click **Deploy**.

Result: The remediation flow is created and saved.

What to do next: Go to Deployments *(on page 181)* and you can see that the action is deployed. It also displays all the configured remediation flow settings. It shows the devices on which the deployment is being done, and the Fixlets that are deployed.

Related information

CyberFOCUS *(on page 277)*

CISA KEV Report *(on page 281)*

MITRE APT report *(on page 286)*

CVE details page *(on page 290)*

DEX

BigFix Digital Employee Experience (DEX) is an endpoint experience management application that gives IT and Workplace administrators a real-time, environment-wide view of digital experience health across managed endpoints. It aggregates device performance, application stability, and user sentiment into actionable DEX scores to proactively identify anomalies, optimize productivity, and automate issue remediation.

Entitlement

- **Required:** BigFix Workspace / BigFix DEX entitlement enabled on the BigFix license.
- **Check:** Navigate to **Settings > Licensing** to verify that the DEX entitlement status shows as active.

User permissions

- **Required role:** DEX Operator, Workspace Operator (or Master Administrator).
- **Required scope:** Read/manage access to target Devices, Device Groups, and DEX Dashboards within the BigFix UI.

Prerequisites

- BigFix UI installed, configured, and connected to the BigFix Server.
- BigFix Scanner and the DEX Scanner Plugin deployed to target managed endpoints.
- Target endpoints subscribed to the relevant DEX sites and actively collected metrics (CPU/memory usage, crash reports, boot/login times).

Full documentation

Full feature documentation: BigFix DEX

Related

BigFix Workspace

Workflow Builder

Workflow Builder lets you automate multi-step device tasks without writing a Fixlet or Task: you chain predefined check, action, and flow-control steps in a drag-and-drop editor, and deploy the result as a single BigFix action tagged `bf-workflow`.

Workflow Builder is available from **Resolve** > **Workflow Builder** in BigFix UI, where the **Workflows** tab holds the workflows and the **Deployments** tab tracks their results. Version 1.0 supports Windows target devices only.

Note: This topic provides a summary of Workflow Builder entitlement, permissions, and prerequisites, with a map to the full procedures. For complete instructions on installing, building, deploying, and troubleshooting workflows, see the *BigFix Workflow Builder User Guide*, which links back to this page.

Entitlement

Required:

- A BigFix license that includes the **BigFix WorkFlow Builder** external content site.

Check:

- In the BigFix Console, **BigFix Management** > **License Overview** lists the **BigFix WorkFlow Builder** site as enabled (refresh the license first if it is missing). See Get the BigFix content in the *BigFix Workflow Builder User Guide*.
- In BigFix UI, **Workflow Builder** appears in the list of role applications only when the site is enabled with a site version greater than zero. See Grant user access in the *BigFix Workflow Builder User Guide*.

User permissions

Required role:

- A BigFix UI role with the **Workflow Builder** application assigned (User & Role Management). Assigning the application enforces the **Custom Content** permission, so assign it only to operators who may create custom content. Master and non-master operators are supported.
- Your operator permissions determine which actions you can complete. For a description of each permission, see Permissions reference *(on page 482)*.
- There is no per-workflow permission: every user who is assigned the application can manage all workflows, including the sample workflows.
- For installation and configuration: a BigFix UI administrator account; command-line access to the BigFix UI server; site permissions on the **BigFix WorkFlow Builder** site for the operators who install and configure it; and a SQL Server login with administrative access to the `BFEnterprise` database for the one-time permission setup.
- Deployment targets: Windows devices with BigFix Agent 9.5.11 or later (version 11 recommended), selected by query, device group, or device list.
- Site subscription: at a minimum, the computer that hosts the BigFix Workflow Service; optionally, all computers for future use.

Prerequisites

- BigFix Platform environment in place (BigFix Platform 11 recommended).
- BigFix UI installed, running, and connected to the BigFix Server. The BigFix UI requires BigFix Platform 11.0.7 or later and Microsoft SQL Server 2025 for its own database. See BigFix UI System Requirements.
- **BigFix WorkFlow Builder** site enabled, gathered, and subscribed (*BigFix Workflow Builder User Guide*).
- Least-privilege database login prepared in `BFEnterprise` with `mssql-init.sql` (Prepare the database login), and hardened after the first service start (Harden the database login).
- BigFix Workflow Service (Windows service `BigFixWorkFlow`) installed on a Windows host with the *Install BigFix WorkFlow Builder Acceptor <version> (WIN)* task (Deploy the BigFix Workflow Service).
- Network connectivity between the BigFix UI server and the BigFix Workflow Service host on the basic authentication port (default 8089) and the mTLS port (default 9087).
- Application activated with `BFUI.exe --configure-wfb` on the BigFix UI server (mTLS setup), followed by a BigFix UI service restart (Activate the application in the BigFix UI).

Important: Before you go live: the service ports are set at installation and cannot be changed afterwards. Backup and restore of the BigFix Workflow Service is not available, and uninstalling the service removes the HMAC key that protects stored workflows, so saved workflows can no longer be accessed. Export workflows as JSON files before you uninstall or rebuild. See *BigFix Workflow Builder User Guide*.

Where to go for full instructions

Full feature documentation: the *BigFix Workflow Builder User Guide*, with a link back to this page.

Related

- Platform Documentation
- BigFix UI User's Guide
- BigFix UI Administration Guide

Fixlet Streams

Fixlet Streams help to automate the process of remediating endpoint vulnerabilities, such as patch and update deployments, while offering flexibility for manual intervention when critical issues arise. The feature ensures routine security and compliance tasks are handled efficiently, freeing up IT teams to focus on strategic initiatives. Additionally, it allows for ad-hoc remediation, enabling swift responses to urgent issues like zero-day vulnerabilities.

It offers a unique blend of routine automation and emergency flexibility, which is not fully available in existing BigFix features. It adds real-time response capabilities, more efficient emergency patch handling, and enhanced time-saving measures, making it a powerful tool for modern IT and security teams.

Key Benefits

- **Increased Efficiency**: Automates routine patch and update deployments, reducing the manual effort required and allowing IT teams to focus on higher-priority tasks.
- **Faster Response to Emergencies**: Provides the flexibility to deploy critical patches and updates immediately in response to urgent threats, such as zero-day vulnerabilities.
- **Improved Security and Compliance**: Ensures endpoints are consistently updated with the latest security patches, reducing the risk of vulnerabilities being exploited.
- **Strategic Focus**: By handling the majority of remediation tasks automatically, IT teams can dedicate more time and resources to strategic initiatives that add value to the organization.
- **Reduced Risk of Human Error**: Automation reduces the likelihood of manual errors in patch deployment, ensuring consistency and reliability across the organization's endpoints.

Content requirements

Fixlet Streams work only with patch content from external patch content sites. An external patch content site is an external site whose name begins with *Patches for*, *Updates for*, *ESU Patching*, or *Known Exploited Vulnerabilities Content Pack for*.

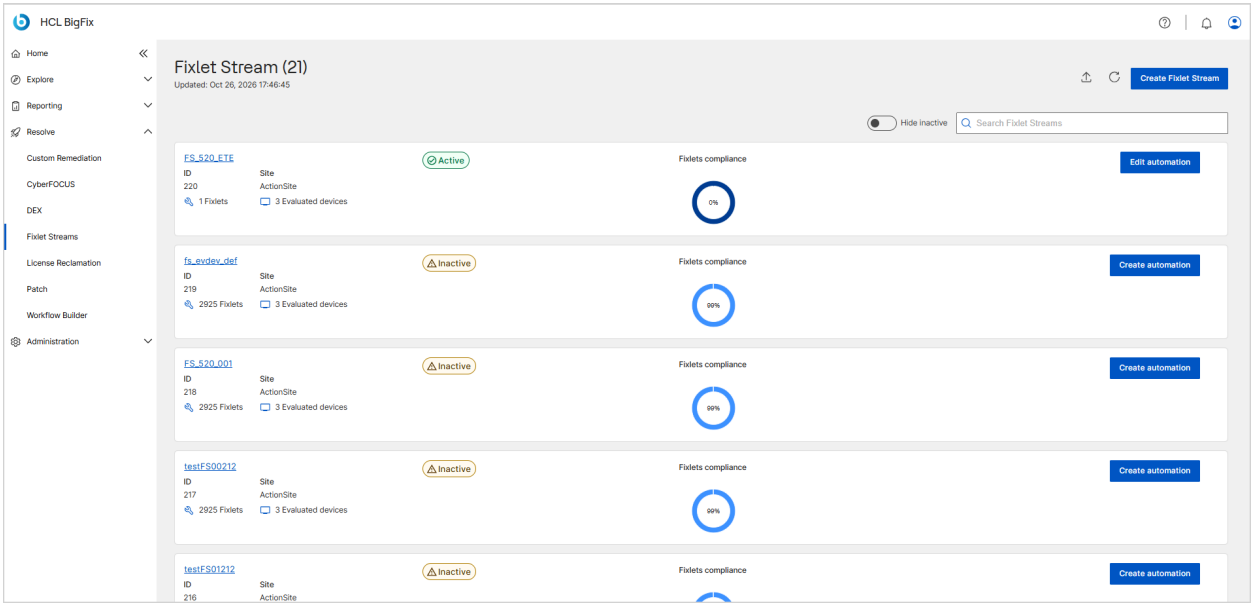
A Fixlet is included in a stream only when all of the following are true:

- It is a Fixlet, not a task.
- It has a default action.
- It is not superseded.
- It comes from an external patch content site.

Note: Access to the Fixlet Streams application and access to patch content sites are granted separately. A role can include the Fixlet Streams application without any external patch content sites. In that case, the application is available, but you cannot complete the Create Fixlet Stream wizard because no sites are listed. See Managing Roles *(on page 467)*.

The Fixlet Streams landing page

To open the landing page, expand **Resolve** from the side navigation, and then select **Fixlet Streams**.



The page heading shows the total number of streams and the time the list was last updated. Each stream appears as a card that shows:

- **Name** of the Fixlet Stream, as a link to its details page.
- **Status**, either **Active** or **Inactive**.
- **ID** and **Site** that the stream draws its Fixlets from.
- The number of **Fixlets** and **Devices** in the stream.
- **Fixlets compliance**, shown as a percentage in a ring chart.
- An action button, either **Create automation** for an inactive stream or **Edit automation** for an active one. See Creating an automation for a Fixlet Stream *(on page 322)* and Editing a Fixlet Stream automation *(on page 335)*.

Note: The **Create automation** button is unavailable on a card until the stream has at least one subscribed device.

Use the following controls to manage the view:

- **Hide inactive**: Turn on this toggle to list only active streams. Turn it off to show all streams again. The setting applies to the current session only.
- **Search fixlet streams**: Type all or part of a stream name to filter the cards as you type. Clear the field to restore the full list.
- **Export**: Click the export icon to download the list as CSV or Excel. The export always includes every Fixlet Stream, both active and inactive. The **Hide inactive** toggle and the search filter change only what the page displays, not what the file contains. See Exporting Data *(on page 30)*.
- **Refresh**: Click the refresh icon to reload the list with the latest stream data, such as status, Fixlet and device counts, and compliance. The **Updated** timestamp below the page heading changes to the time of the refresh.
- **Create Fixlet Stream**: Start the wizard that builds a new stream. See Create Fixlet Stream *(on page 314)*.

To open a stream and review its devices, Fixlets, and deployments, click its name. See Fixlet Stream Details Page *(on page 339)*.

Device subscription

You define which devices a Fixlet Stream targets on the **Devices** step of the Create Fixlet Stream wizard. The conditions you set there form a dynamic filter that BigFix evaluates continuously. For step-by-step information, read Create Fixlet Stream *(on page 314)*.

Key Notes:

- **Dynamic Filters**: Filters will continuously evaluate device subscriptions, ensuring that newly added devices meeting the criteria are included in the deployment automatically.
- **Multiple Conditions**: You can refine your subscriptions by adding multiple conditions, creating complex filters to target specific device groups.

The **Device subscription** panel on the stream's Overview tab shows the conditions that are in force. See Fixlet Stream Details Page *(on page 339)*.

Monitoring

- **Fixlet Compliance**: The **Fixlet compliance percentage** shows the proportion of devices that have successfully applied the patch or update from the Fixlet Stream. Regular monitoring of this metric ensures that devices are keeping up with your desired compliance levels. If the compliance percentage is lower than expected, investigate why certain devices are not compliant. This could be due to errors in the deployment or devices that didn't meet the dynamic filter criteria.

  Note: If a Fixlet in the stream is a dynamic Fixlet, the Fixlet compliance percentage does not change after a deployment. A dynamic Fixlet is one that can be applied to the same device again and again, so it stays relevant on the device even after the action succeeds. For example, the **Fixlets compliance** ring chart can continue to show 0% while the **Deployment progress** ring chart shows 100%. This

behavior is expected and does not indicate a failed deployment. To confirm the outcome, review the deployment state on the **Deployments** tab.

- **Deployment Progress**: The **Deployment progress** ring chart on the stream's Overview tab shows how far the deployment has advanced.
  - **Track status**: Use the chart to monitor the deployment and to spot delays or issues during roll out.
  - **Adjust Deployment Timing**: If you see that deployment is not progressing as planned, you can adjust future schedules or rerun the deployment for specific device groups.

Important: Reflecting correct metrics takes time. The device count, the relevant Fixlet count, and the compliance percentage are based on the state that devices report to the server, not on the deployment result. A stream updates these values only after the affected devices report again, so a new stream can take several minutes to show its first device count, and a count can stay unchanged for a while after a deployment succeeds. See Device Count and Relevant Fixlet Count Take Time to Update *(on page 345)*.

Best Practices

- **Regularly Review Device Subscriptions**: Ensure that new devices matching your criteria are automatically subscribed and that conditions remain relevant over time.
- **Monitor Compliance Metrics**: Stay proactive by checking Fixlet compliance and deployment progress to address issues early.
- **Keep Automation Up to Date**: Revisit and refine automation definitions as organizational needs evolve.

Automation States

A Fixlet Stream is either **Active** or **Inactive**. The state controls which management actions are available.

Important: You must deactivate a Fixlet Stream before you can edit or delete it. Deactivating a stream also deletes the automation created for it, so you must create the automation again after you finish your changes. For step-by-step information, see Managing Fixlet Streams *(on page 332)*.

Additional Resources

- Creating an automation for a Fixlet Stream *(on page 322)*
- Managing Fixlet Streams *(on page 332)*
- Common use cases *(on page 348)*
- Troubleshooting *(on page 344)*

Create Fixlet Stream

The Create Fixlet Stream feature enables you to set up custom Fixlet streams to meet specific organizational needs by defining conditions and selecting targeted devices for updates. The guided workflow helps you specify Fixlet

criteria, scope target devices, and review the configuration before creating the stream, which can later be automated for continuous remediation.

Before you begin:

- You must have permission to create Fixlet Streams.
- Your role must have access to at least one external patch content site. An external patch content site is an external site whose name begins with one of the following:
  - Patches for
  - Updates for
  - ESU Patching
  - Known Exploited Vulnerabilities Content Pack for
- Device properties used for filtering must be reported by agents.

Important:

Fixlet Streams can include only content that meets all of the following conditions:

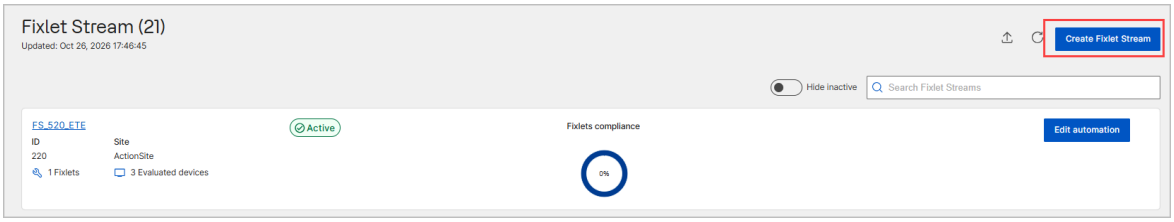
- The content is a Fixlet, not a task.
- The content has a default action.
- The content is not superseded.
- The content comes from an external patch content site.

Content that does not meet every condition is not added to the stream, even if it matches the Fixlet criteria that you define. BigFix UI restates these conditions in the **Fixlet Streams criteria** dialog each time you start the wizard.

Steps to Create a Fixlet Stream

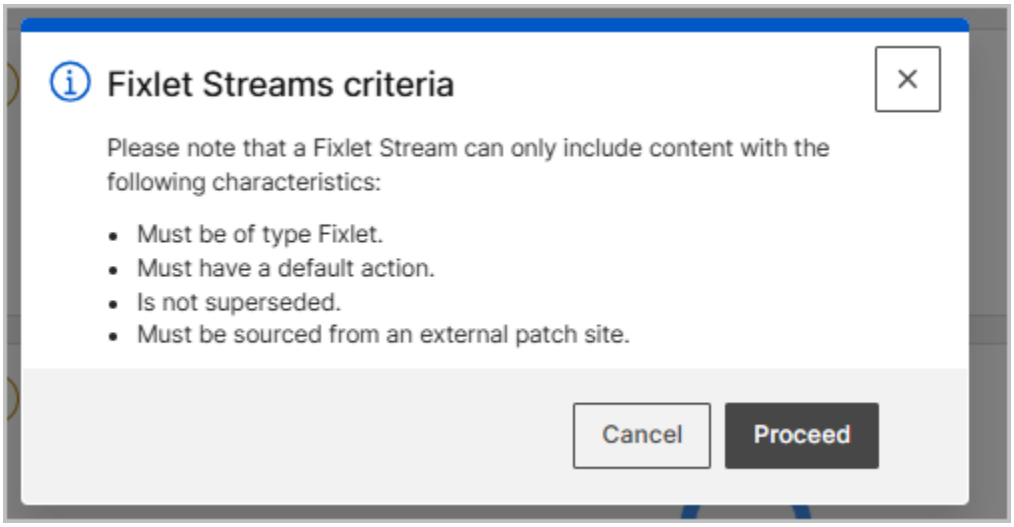
1. **Open the Create Fixlet Stream Widget**

   From the BigFix UI navigation, go to Resolve # Fixlet Streams.



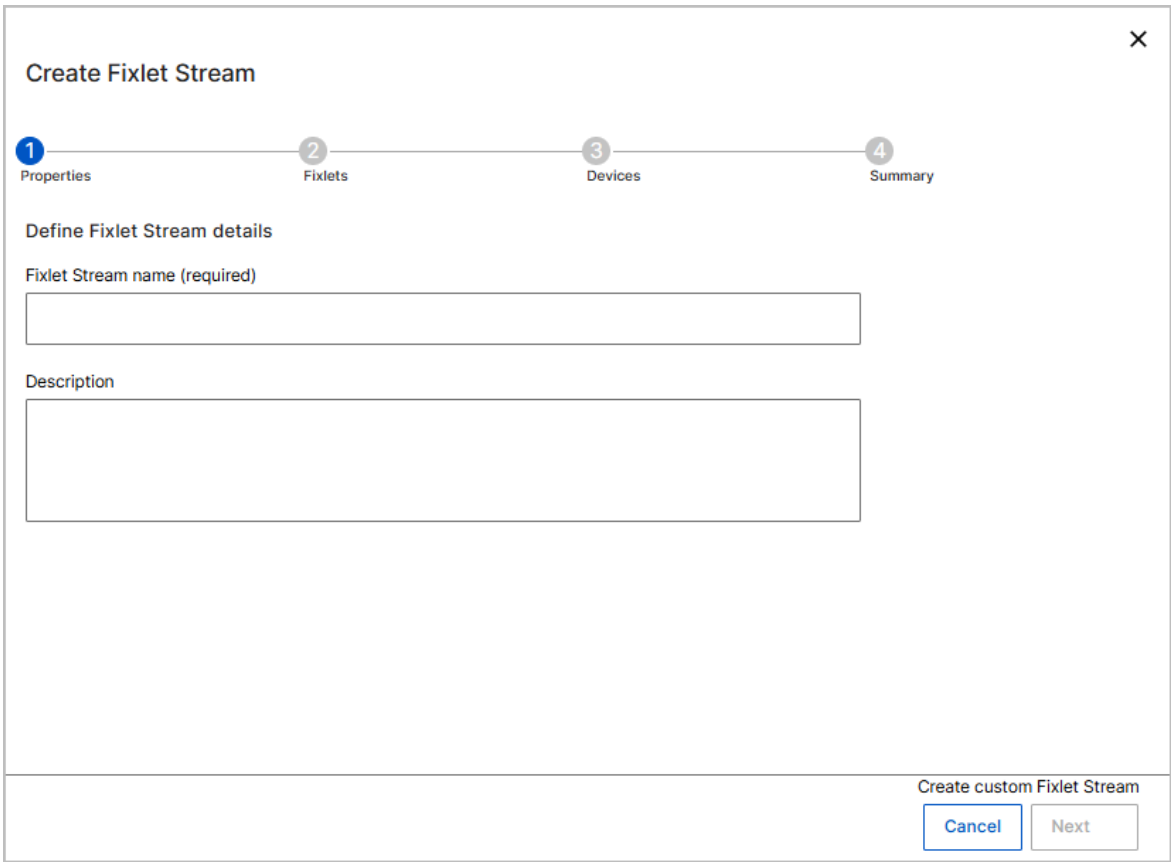
   Click **Create Fixlet Stream** in the top-right corner.

   The **Fixlet Streams criteria** dialog opens and lists the characteristics that content must have to join a stream.



Review the conditions, and then click **Proceed** to open the wizard, or **Cancel** to return to the landing page.

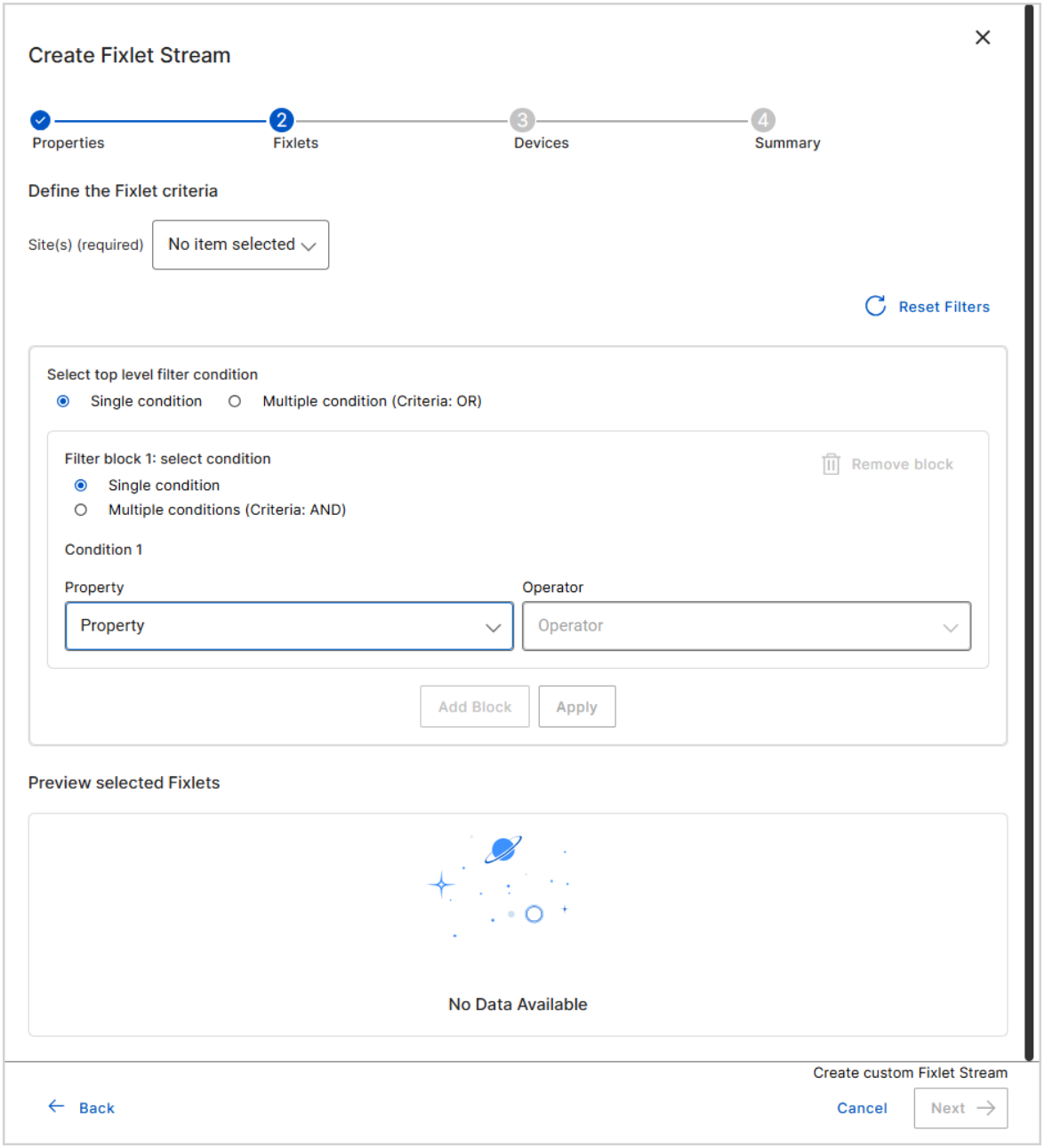
The Create Fixlet Stream wizard opens on the Properties step.



2. **Properties**: Define Fixlet Stream properties.

- In Fixlet Stream name, enter a meaningful name for the stream. For example: Windows Critical Security Updates.
- (Optional) In Description, enter additional details to explain the purpose of the stream.
- Click **Next** to continue.

3. **Fixlets**: Select Fixlets for the stream.



- On the Fixlets step, click the **Site(s)** list and select one or more sites that supply the Fixlets. This field is required.

  The list opens as a panel of checkboxes, one for each site that your role can access, for example:

- Known Exploited Vulnerabilities Content Pack for Windows
- Patches for Windows
- Updates for Windows Applications
- Updates for Windows Applications Extended

Work with the panel as follows:

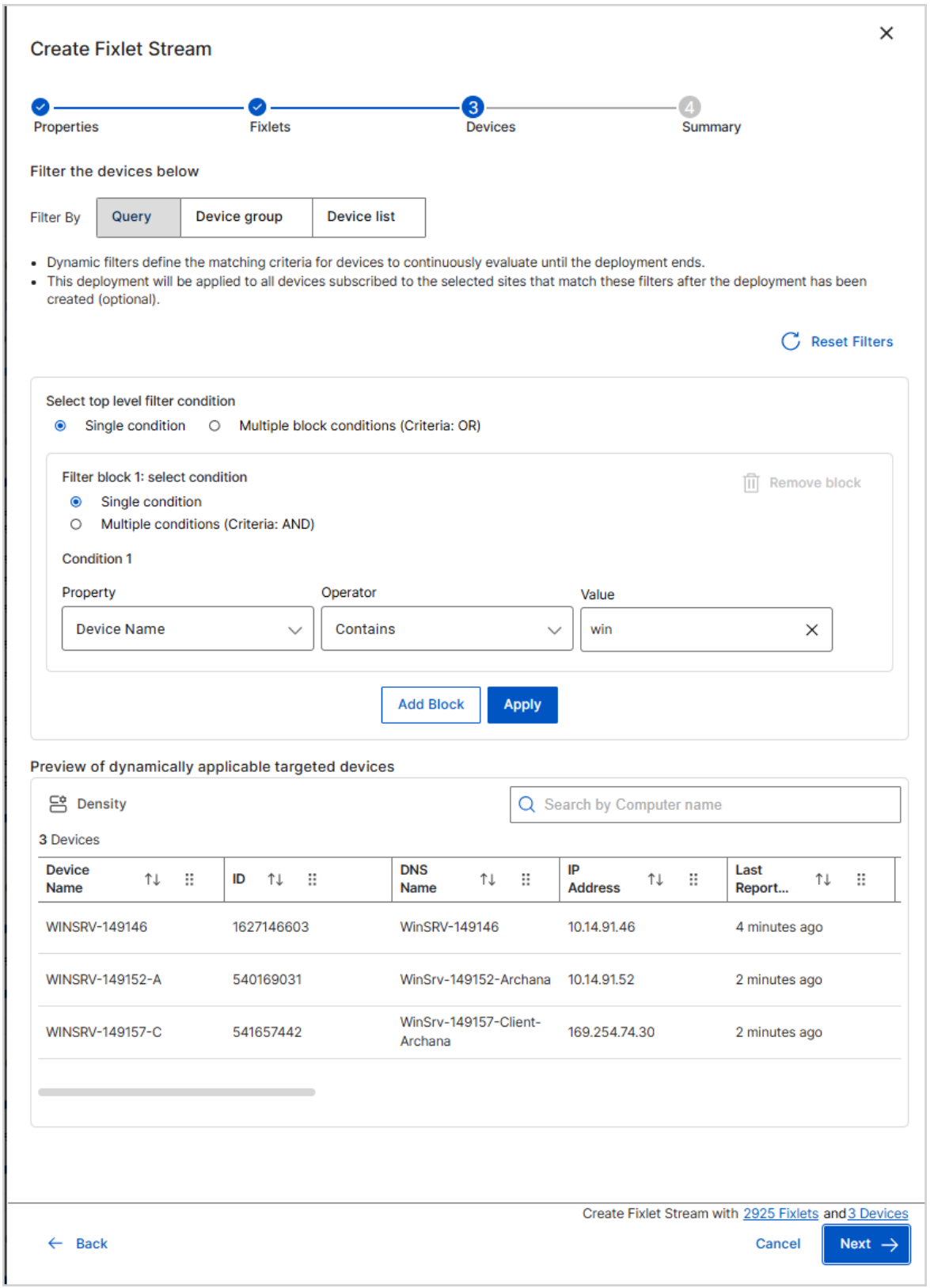
- Type in the search box at the top of the panel to find a site by name.
- Select the checkbox of each site that you want to include. The panel shows **Max items limit: 10**, so you can select up to 10 sites.
- Click **Reset** to clear the selection and start again.
- Click **Apply** to confirm the selection and close the panel.

The field label reports how many sites you chose, for example **1 items selected**, and the **Selected values** row lists them. Click **Reset Filters** to clear the site selection and the Fixlet criteria together.

Important: The **Site(s)** list shows only the external patch content sites that your role can access, such as Patches for Windows. If the list is empty, your role does not have access to any external patch content site, and you cannot continue creating the stream. Ask your administrator to grant your role access to at least one external patch content site. See Managing Roles *(on page 467)*.

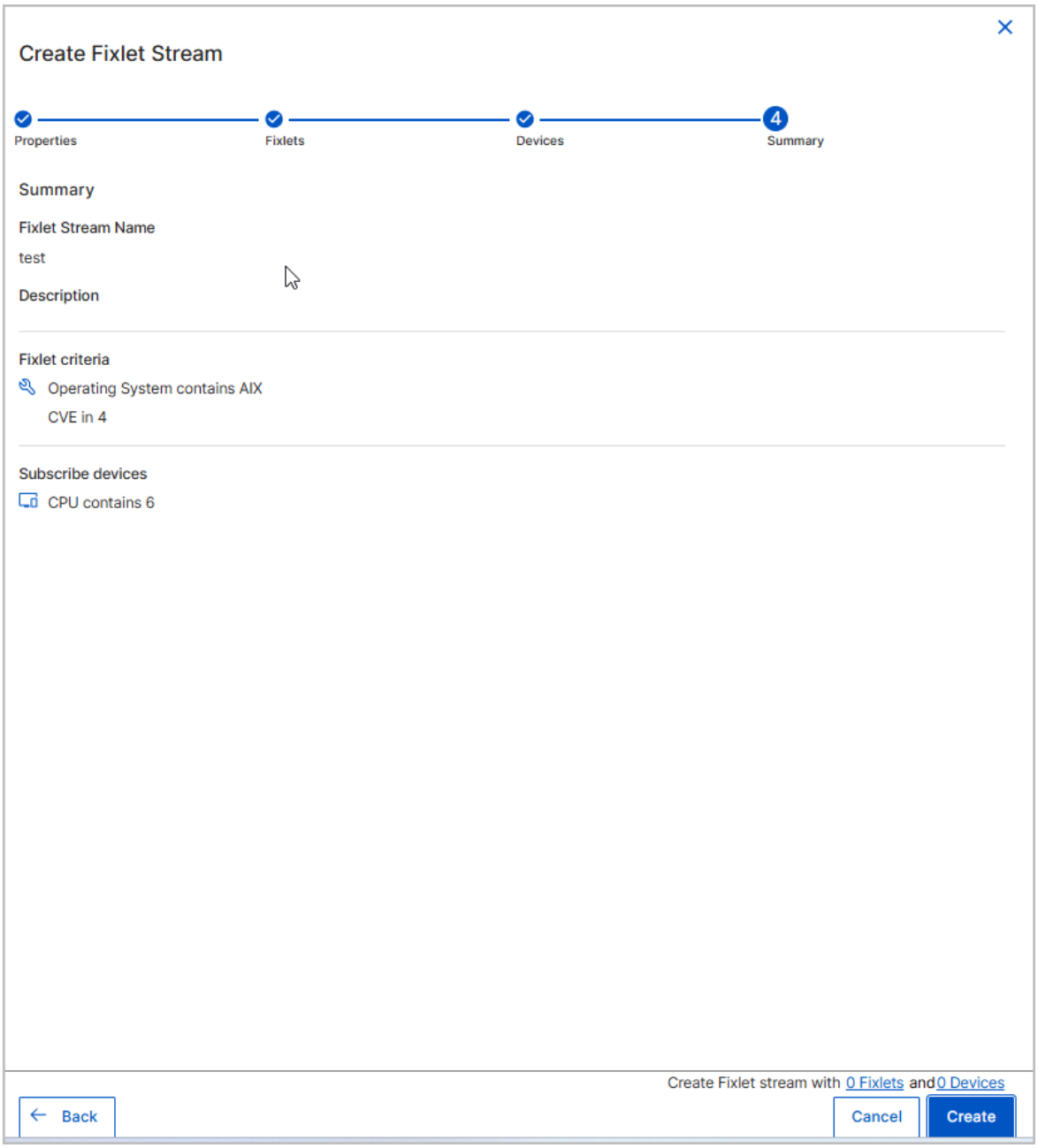
- Under **Define the Fixlet criteria**, build the conditions that select the Fixlets. Select a **Property** such as **Name**, **Severity**, or **CVE**, an **Operator**, and a **Value**. The controls work the same way as the query filter elsewhere in BigFix UI, including the **Single condition** and **Multiple condition** options and **Add Block**. See Filter by query *(on page 40)*.
- Click **Apply**. The system evaluates the criteria and identifies matching Fixlets.
- Review the **Preview selected Fixlets** section to confirm that the expected Fixlets are included. The footer shows the running count, for example **Create Fixlet stream with 7 Fixlets**.
- Click **Next**.

4. **Devices**: Define target devices.


Create Fixlet Stream
Properties
Fixlets
3
Devices
4
Summary
Filter the devices below
Filter By
Query
Device group
Device list
Dynamic filters define the matching criteria for devices to continuously evaluate until the deployment ends.
This deployment will be applied to all devices subscribed to the selected sites that match these filters after the deployment has been created (optional).
Reset Filters
Select top level filter condition
Single condition
Multiple block conditions (Criteria: OR)
Filter block 1: select condition
Remove block
Single condition
Multiple conditions (Criteria: AND)
Condition 1
Property
Operator
Value
Device Name
Contains
win
Add Block
Apply
Preview of dynamically applicable targeted devices
Density
Search by Computer name
3 Devices
Device Name
ID
DNS Name
IP Address
Last Report...
WINSRV-149146
1627146603
WinSRV-149146
10.14.91.46
4 minutes ago
WINSRV-149152-A
540169031
WinSrv-149152-Archana
10.14.91.52
2 minutes ago
WINSRV-149157-C
541657442
WinSrv-149157-Client-Archana
169.254.74.30
2 minutes ago
Create Fixlet Stream with 2925 Fixlets and 3 Devices
Back
Cancel
Next

- On the Devices step, use **Filter By** to choose how devices are selected:
  - **Query** – Build conditions from device properties, such as **Device Name**.
  - **Device group** – Select an existing device group.
  - **Device list** – Select individual devices.
- Build the conditions that select the devices. The controls work the same way as the query filter elsewhere in BigFix UI. See Filter by query *(on page 40)*. Use the following controls to shape the dynamic filter:
  - **Single condition**: Matches devices on one condition.
  - **Multiple condition (AND)**: Requires every condition in the block to match.
  - **Multiple condition (OR)**: Matches devices that satisfy any block.
  - **Property**: Select the device attribute to test, such as **Device Name**, **OS Family**, or **ID**.
  - **Operator**: Select the comparison, such as **equals** or **contains**.
  - **Value**: Enter one or more values to match.
  - **Add Block**: Adds another block of conditions.
  - **Remove block**: Deletes a block that you no longer need.
  - **Reset Filters**: Clears all the conditions so that you can start again.
- Click **Apply** to evaluate the filters.
- Review the **Preview of dynamically applicable targeted devices** section to verify which devices match the criteria.
- Click **Next**.

5. **Summary**: Review and create the Fixlet Stream:



- On the Summary step, review all configured details
  - Fixlet Stream name and description
  - Fixlet selection criteria
  - Device filtering criteria
- Confirm that the configuration matches your intended scope. Click **Create**.

- The Fixlet Stream is created and appears on the Fixlet Streams landing page.
- The stream does not deploy Fixlets until devices are subscribed and automation is configured.
- You can now proceed to set up the Fixlet Stream for remediation.

6. **Edit Fixlet Stream**
   - To adjust conditions, click your Fixlet Stream on the landing page to open the Fixlet Stream Details Page *(on page 339)*, and then edit the settings as needed.
   - If the stream is active, deactivate it first. The **Edit Fixlet Stream** button is unavailable while a stream is active. See Editing a Fixlet Stream *(on page 334)*.

What to do next

- Confirm that the devices you defined on the **Devices** step appear on the **All targeted devices** tab. See Fixlet Stream Details Page *(on page 339)*.
- Create automation to schedule and control Fixlet deployments. See Creating an automation for a Fixlet Stream *(on page 322)*.
- Activate the stream, and manage it later from the details page. See Managing Fixlet Streams *(on page 332)*.
- Monitor compliance and deployments from the Fixlet Stream details page.

Related information

Creating an automation for a Fixlet Stream *(on page 322)*

Managing Fixlet Streams *(on page 332)*

Troubleshooting *(on page 344)*

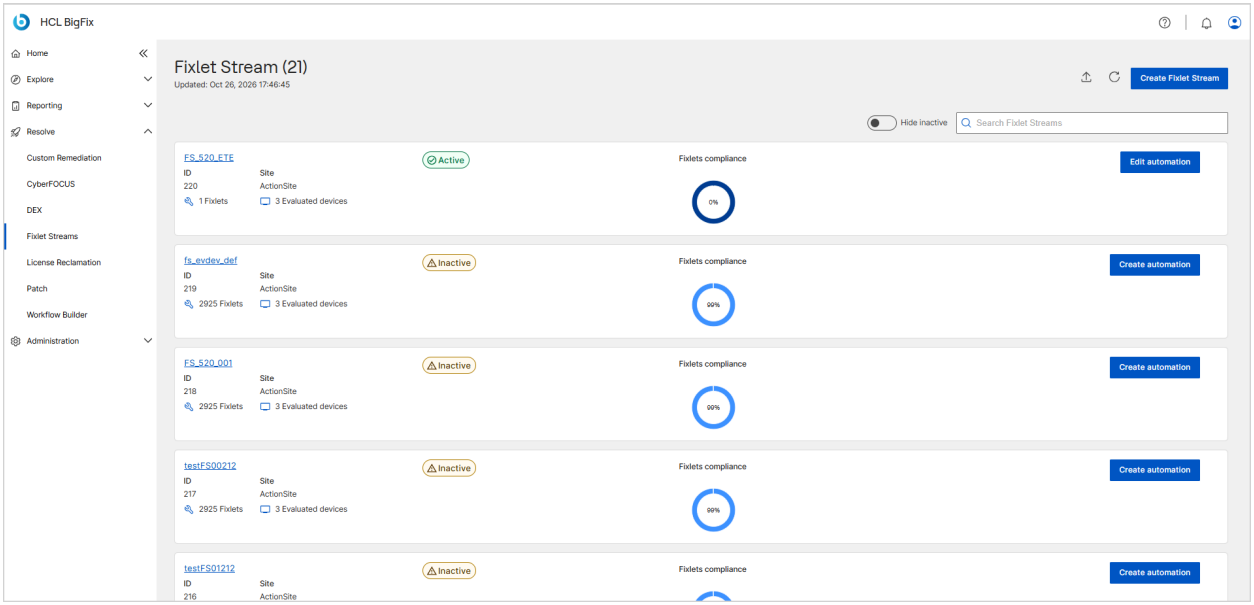
Common use cases *(on page 348)*

Creating an automation for a Fixlet Stream

An automation defines when and how a Fixlet Stream deploys Fixlets to its subscribed devices. Use the Create automation wizard to set the device schedule, the execution sequence, and the activation date. When you create the automation, the stream becomes active and starts continuous remediation.

- You must have permission to manage Fixlet Streams.
- The Fixlet Stream must already exist. See Create Fixlet Stream *(on page 314)*.
- The stream must have at least one subscribed device. The **Create automation** button stays unavailable until devices are subscribed.
- The stream must be inactive. An active stream shows **Edit automation** instead.

Expand **Resolve** from the side navigation, and then select **Fixlet Streams**. Each stream appears as a card with its status, ID, site, Fixlet and device counts, and Fixlets compliance.



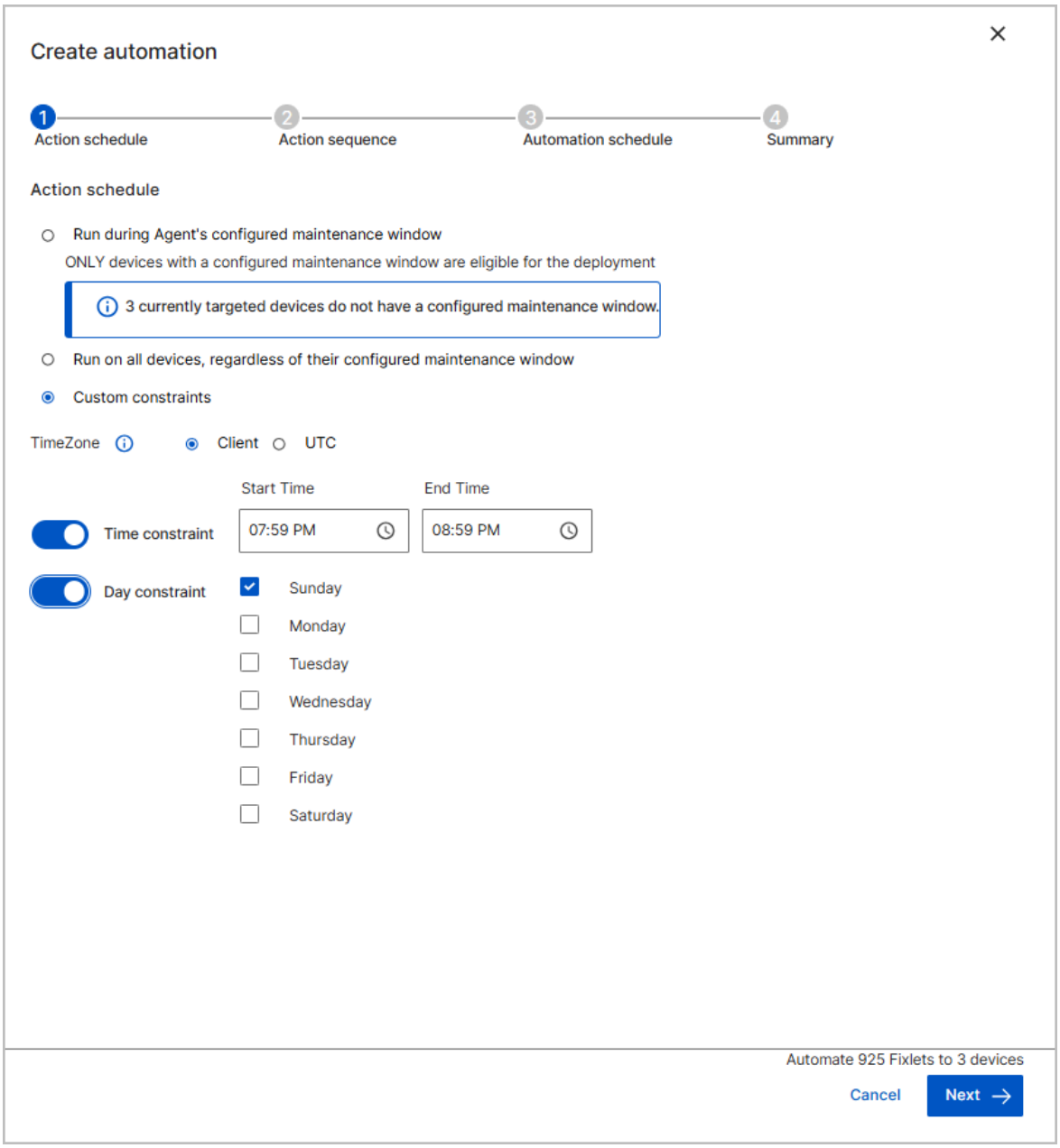
The wizard has four steps: **Action schedule**, **Action sequence**, **Automation schedule**, and **Summary**. The footer of every step reports the scope of the automation, for example **Automate 925 Fixlets to 3 devices**. Click **Back** to revise an earlier step, or **Cancel** to close the wizard without saving.

Note: The **Edit automation** action opens the same four steps in an **Edit automation** wizard, with your current settings in place. See Editing a Fixlet Stream automation *(on page 335)*.

1. On the card of the Fixlet Stream, click **Create automation**.

   The Create automation wizard opens on the **Action schedule** step.

2. On the **Action schedule** step, select when the Fixlets can run.

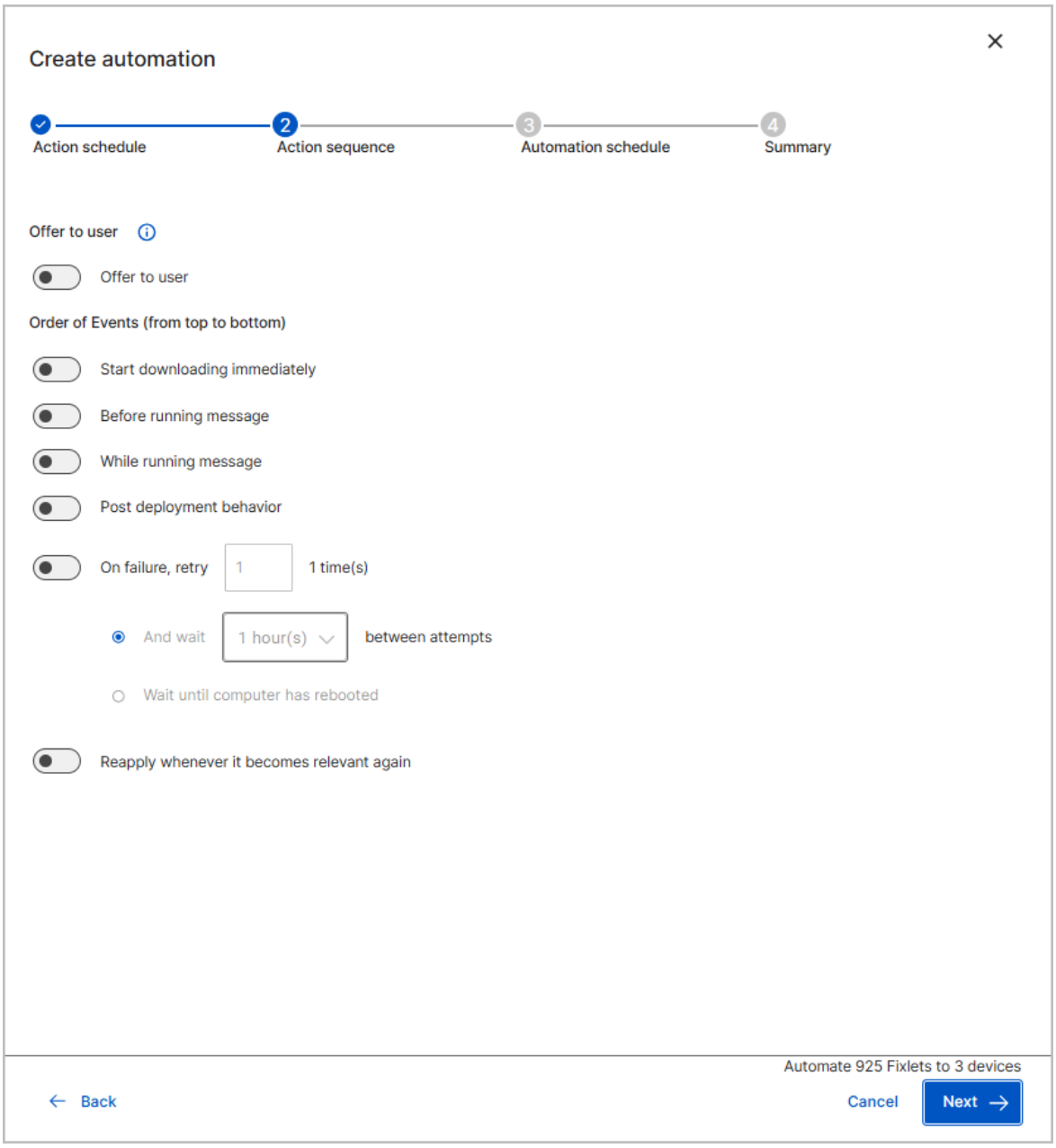


- **Run during Agent's configured maintenance window**: Only devices with a configured maintenance window are eligible for the deployment. The wizard reports how many targeted devices have no maintenance window, for example **3 currently targeted devices do not have a configured maintenance window**. To set windows for those devices, see Managing Device Maintenance Windows *(on page 126)*.
- **Run on all devices, regardless of their configured maintenance window**: Deploys to every subscribed device.
- **Custom constraints**: Defines your own deployment window. This option enables the time zone, time, and day controls.

3. **Optional:** If you selected **Custom constraints**, define the window.
    a. For **TimeZone**, select **Client** to use each device's local time, or **UTC** to use a single reference time.
    b. Turn on **Time constraint**, and then set the **Start Time** and **End Time**.
    c. Turn on **Day constraint**, and then select the days on which the deployment can run.

4. Click **Next**.

    The **Action sequence** step opens.



5. **Optional:** Turn on **Offer to user** to let users start the deployment themselves instead of running it silently.

- **Notify device owner of offer availability**: Select this checkbox to alert the device owner when the offer becomes available.
- **Title**: Enter the title that identifies the offer to the user.
- **Category**: Enter the category that groups the offer in the self-service application.
- **Description**: Enter the text that explains what the offer does.

6. Under **Order of Events (from top to bottom)**, configure how the Fixlets run on the devices.
   - **Start downloading immediately**: Downloads the payload before the deployment starts. If this option is off, the download begins after the deployment starts.
   - **Before running message**: Shows a message to users before the action runs. Turn on the toggle, enter the message text, and then set the following options:
     - In **Notify user for**, select how long the message is displayed (for example, **10 minutes**), and in **and then**, select what happens when that time ends, such as **Run action immediately**.
     - **Allow user to save work**: Select this checkbox to let users save open work before the action runs.
     - **Allow user to cancel**: Select this checkbox to let users cancel the action.
     - **Show confirmation message before running action**: Select this checkbox to prompt users to confirm before the action runs. In **Confirmation message**, keep the default text or enter your own, for example *Are you sure you want to run this action now?*
   - **While running message**: Shows a message to users while the action runs. Turn on the toggle, and then enter the message text to display to the user.
   - **Post deployment behavior**: Turn on this toggle to control what happens on the device after the action completes, and then select one of the following:
     - **Do nothing after action completes**: The device stays in its current state.
     - **Restart computer after action completes**: The device restarts when the action finishes.
     - **Shutdown computer after action completes**: The device shuts down when the action finishes.

     If you select **Restart computer after action completes** or **Shutdown computer after action completes**, configure the message shown to the user:
     - In **Message title (required)**, enter a short title, for example *Shutdown now*.
     - In **Message text (required)**, enter the message body that asks users to save any unsaved work.
     - In **Notify user for**, select how long the message is displayed, and in **and then**, select what happens when that time ends, such as **Shutdown automatically** or **Restart automatically**.
     - **Allow user to cancel shutdown** or **Allow user to cancel restart**: Select this checkbox to let users cancel the shutdown or restart.
   - **On failure, retry**: Turn on this toggle to have BigFix try the deployment again if it fails. Enter the number of retries, and then select one of the following options:

        - **and wait**: Select this option and set the interval (for example, **1 hour**) that BigFix waits between attempts.
        - **Wait until computer has rebooted**: Select this option to retry the action only after the device restarts.
    - **Reapply whenever it becomes relevant again**: Turn on this toggle to run the action again each time the Fixlet becomes relevant on the device. Select **with a** to set the wait between attempts, and **up to** to cap the number of times.

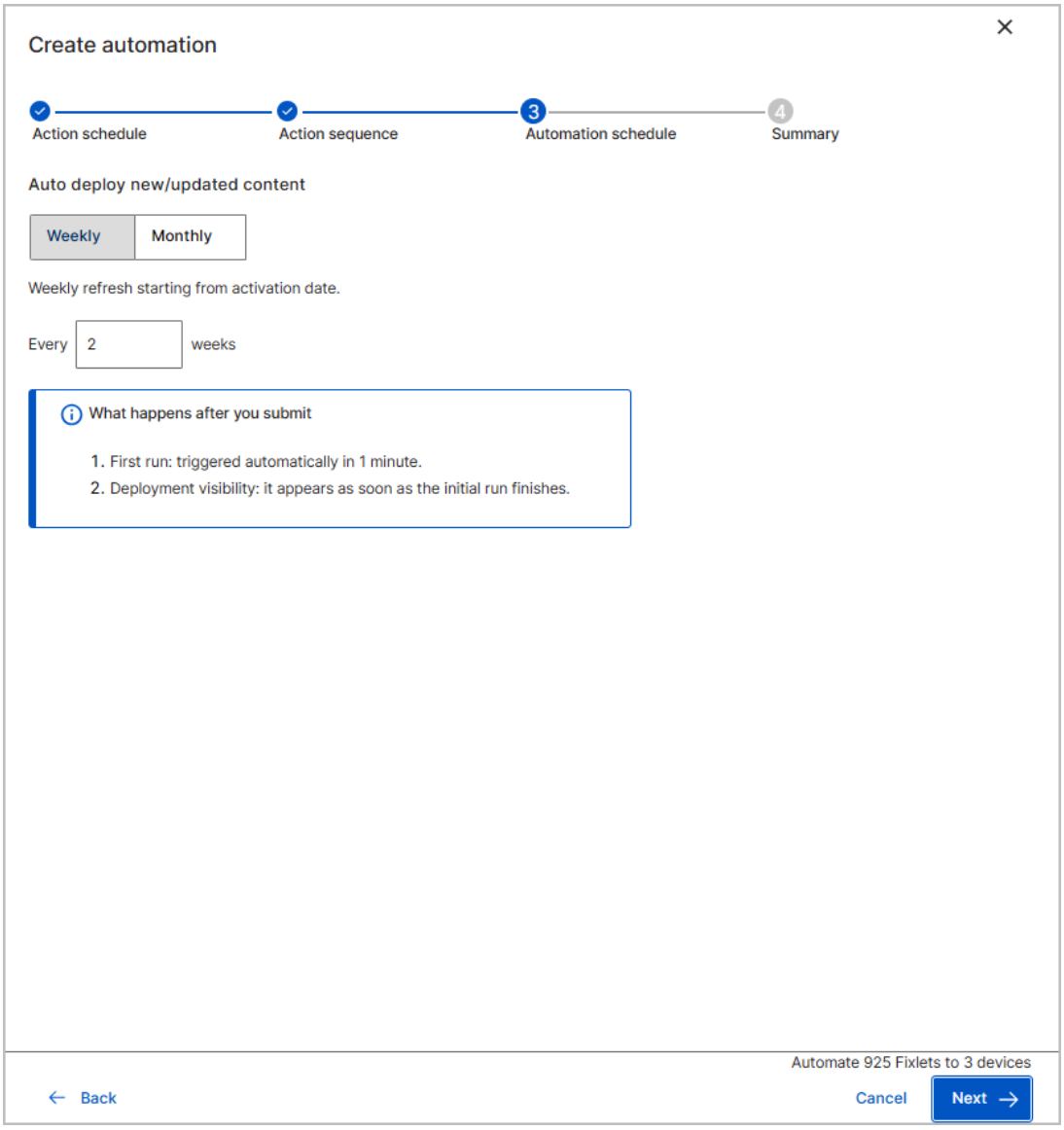
7. Click **Next**.

   The **Automation schedule** step opens.

8. On the **Automation schedule** step, under **Auto deploy new/updated content**, set how often the stream picks up new and updated Fixlets.

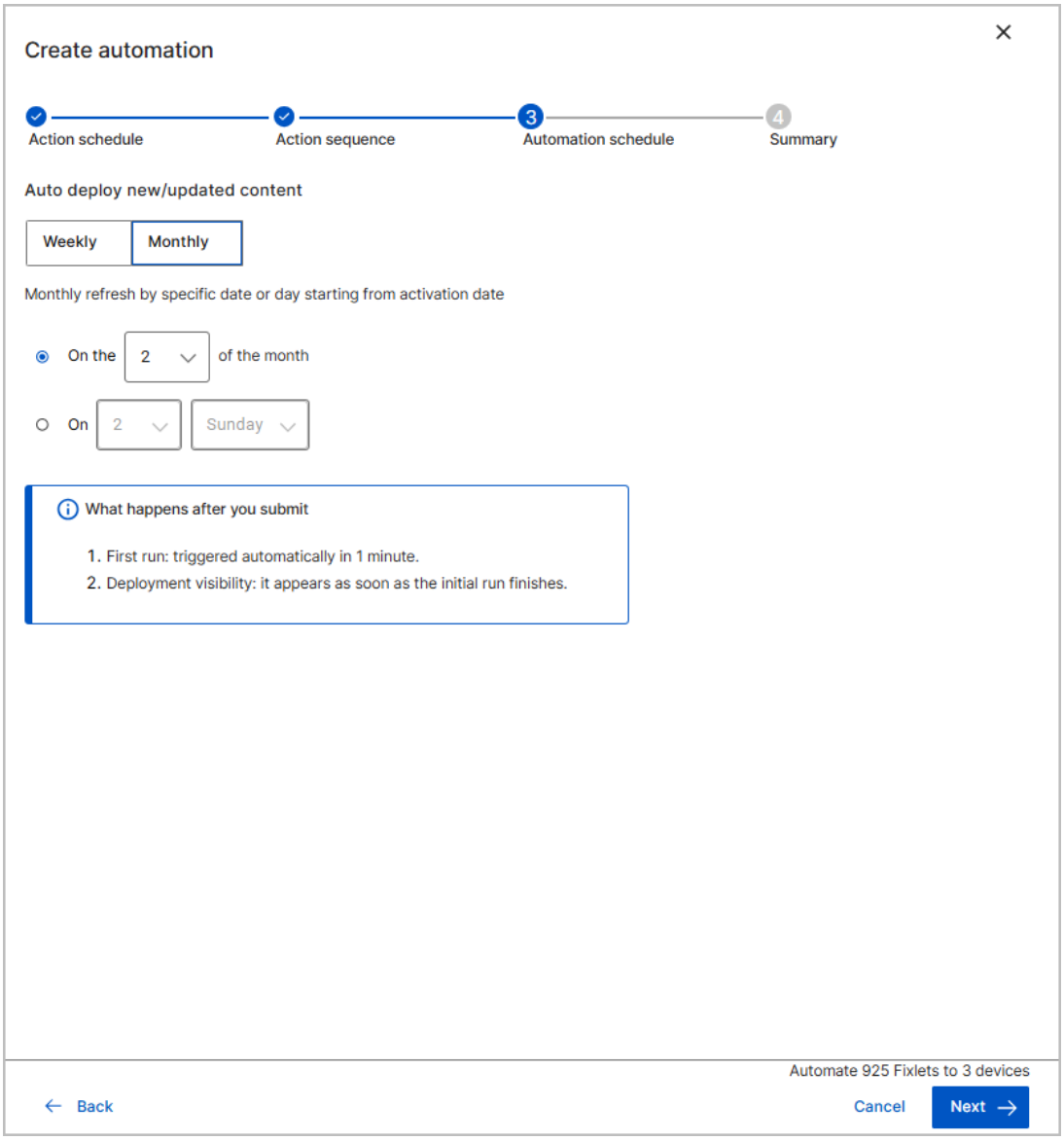
   Select **Weekly** or **Monthly**, and then set the interval. Both schedules start from the activation date.

◦ **Weekly**: In the **Every** field, enter the number of weeks between refreshes, for example 2 weeks.



◦ **Monthly**: Refresh by a specific date or a specific day of the month. Select one of the following options:

- **On the [date] of the month**: Select the day of the month, for example the 2nd.
- **On [occurrence] [weekday]**: Select the occurrence and the weekday, for example the second Sunday.



Note:

The **What happens after you submit** panel explains how the automation starts:

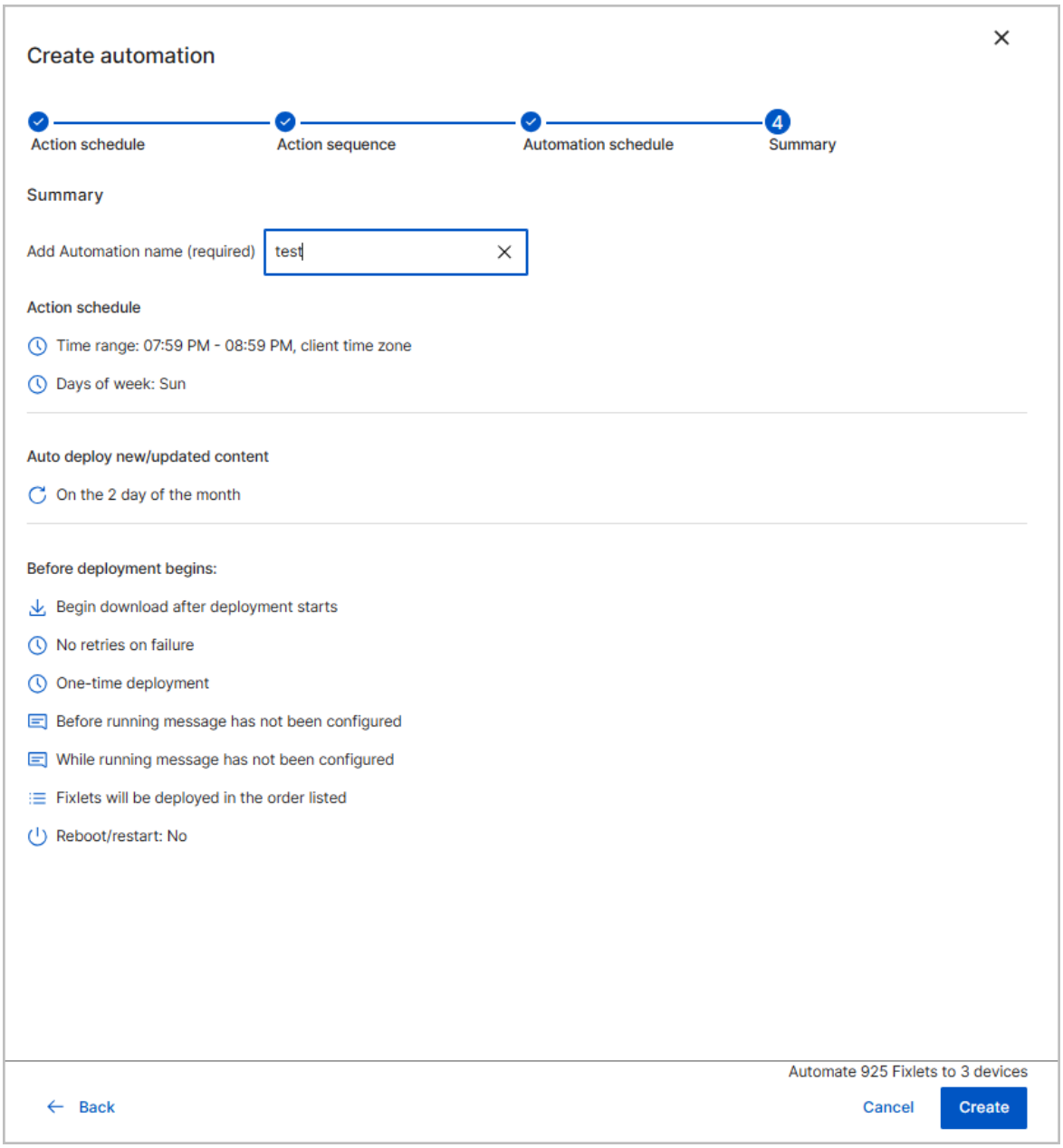
a. The first run is triggered automatically in 1 minute.
b. When the automation runs, BigFix creates an action in the BigFix console, and the deployment appears on the **Deployments** tab after the action is created. BigFix creates the action only if the Fixlets in the stream are relevant to at least one subscribed device. If none of the

subscribed devices needs the Fixlets, the automation still runs, but it finds no targeted devices, so no action and no deployment are created. In that case, the **Deployments** tab stays empty, and the reason is recorded only in the orchestration log.

9. Click **Next**.

   The **Summary** step opens.

10. On the **Summary** step, in **Add Automation name**, enter a name for the automation. This field is required.



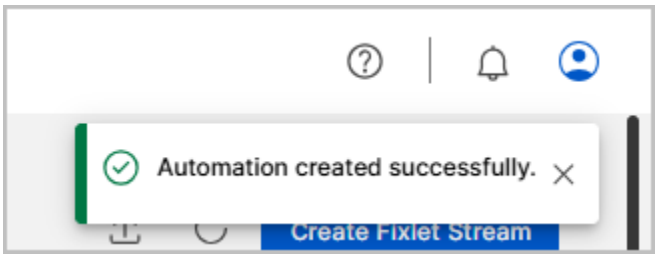
11. Review the settings that the summary reports.

- **Action schedule**: The maintenance window option or the custom constraints that you set, reported as a time range and the days of the week, for example **Time range: 07:59 PM - 08:59 PM, client time zone** and **Days of week: Sun**.
- **Auto deploy new/updated content**: The refresh interval, for example **On the 2 day of the month**.
- **Before deployment begins**: The download, retry, reapply, message, order, and reboot settings, for example **Begin download after deployment starts**, **No retries on failure**, **One-time deployment**, **Fixlets will be deployed in the order listed**, and **Reboot/restart: No**.

To correct a setting, click **Back** until you reach the relevant step.

12. Click **Create**.

    The message **Automation created successfully** appears, and the stream status changes to **Active**. The card action changes to **Edit automation**.



- The first run is triggered automatically about 1 minute after you submit.
- Fixlets deploy to the subscribed devices on the defined schedule.
- New and updated Fixlets that match the stream criteria deploy automatically at the refresh interval.
- Deployment activity appears on the **Deployments** tab of the stream after BigFix creates an action for the relevant devices. If no subscribed device needs the Fixlets, no deployment appears.

- Click the name of the Fixlet Stream to open the Fixlet Stream Details Page *(on page 339)*, and then monitor compliance on the **Overview** tab and progress on the **Deployments** tab.
- To change the schedule, activate the stream, or deactivate it, see Managing Fixlet Streams *(on page 332)*.

Related information

Create Fixlet Stream *(on page 314)*

Managing Fixlet Streams *(on page 332)*

Editing a Fixlet Stream automation *(on page 335)*

Fixlet Stream Details Page *(on page 339)*

Troubleshooting *(on page 344)*

Managing Fixlet Streams

After you create a Fixlet Stream and its automation, you manage the stream from its details page. You can activate or deactivate the stream, change its criteria, change the deployment schedule, or delete the stream.

To open the details page of a stream, expand **Resolve** from the side navigation, select **Fixlet Streams**, and then click the name of the stream.

Fixlet Stream states

The status toggle in the upper-right corner of the details page shows whether the stream is **Active** or **Inactive**. The state controls which management actions are available.

- **Active**: The **Edit Fixlet Stream** button and the delete icon are unavailable. You can click **Edit automation** to change the deployment schedule.
- **Inactive**: The **Edit Fixlet Stream** button and the delete icon become available, and the **Automate remediation schedule** panel shows **Create automation**.

Important: Deactivating a Fixlet Stream deletes the automation created for it. The stream, its Fixlet criteria, and its device subscription remain intact, but you must create the automation again before deployments resume.

Management tasks

- Activating and deactivating a Fixlet Stream *(on page 332)*
- Editing a Fixlet Stream *(on page 334)*
- Editing a Fixlet Stream automation *(on page 335)*
- Deleting a Fixlet Stream *(on page 338)*

Related information

Create Fixlet Stream *(on page 314)*

Creating an automation for a Fixlet Stream *(on page 322)*

Fixlet Stream Details Page *(on page 339)*

Troubleshooting *(on page 344)*

Activating and deactivating a Fixlet Stream

Activate a Fixlet Stream to start deploying Fixlets on the schedule defined in its automation. Deactivate a stream to stop deployments and to unlock the edit and delete actions.

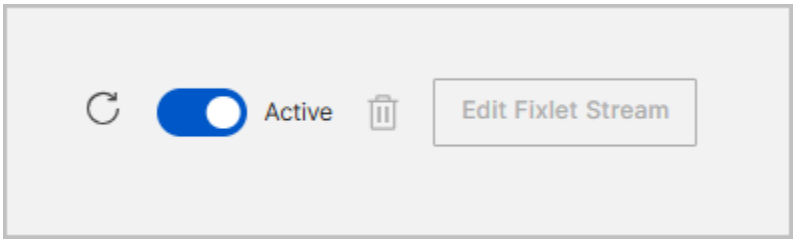
- You must have permission to manage Fixlet Streams.
- The Fixlet Stream must already have an automation defined. See Creating an automation for a Fixlet Stream *(on page 322)*.

Expand **Resolve** from the side navigation, select **Fixlet Streams**, and then click the name of the stream. The status toggle in the upper-right corner of the details page shows the current state.

Important: Deactivating a Fixlet Stream deletes the automation created for it. The stream, its Fixlet criteria, and its device subscription remain intact, but you must create the automation again before deployments resume.

1. To activate the stream, set the status toggle to **Active**.

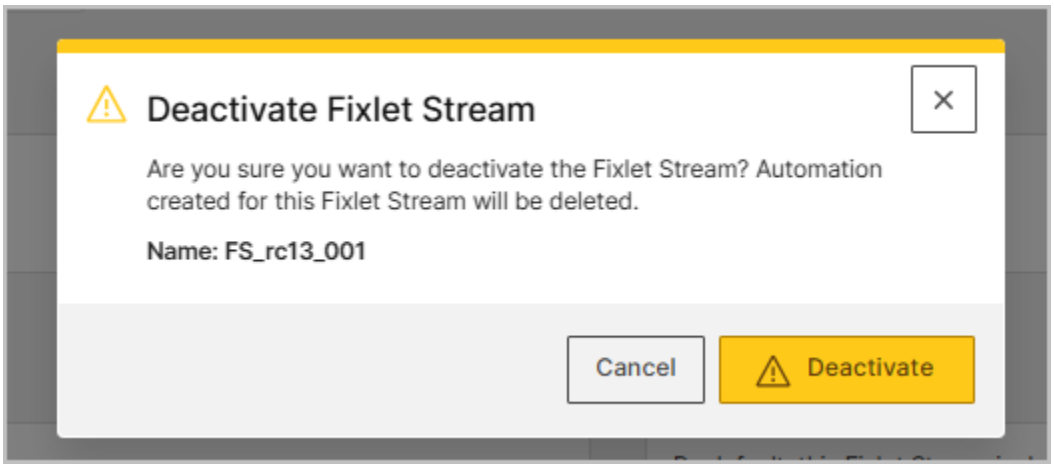
   The toggle is available only when the stream already has an automation. If no automation is defined, click **Create automation** on the stream card or in the **Automate remediation schedule** panel instead. Creating an automation also activates the stream. See Creating an automation for a Fixlet Stream *(on page 322)*.

   The stream starts deploying Fixlets to subscribed devices on the schedule defined in the automation.

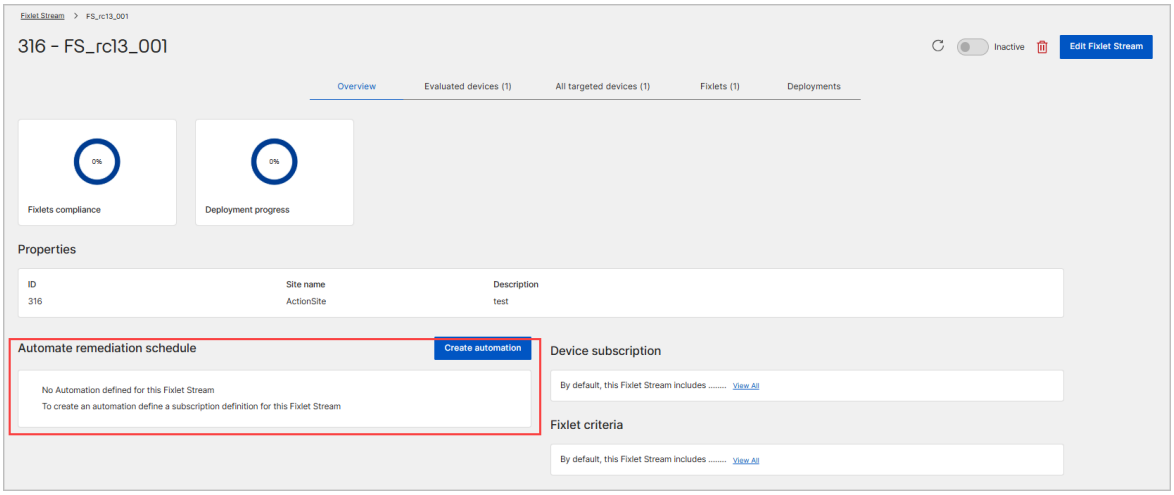
2. To deactivate the stream, set the status toggle to **Inactive**.

   a. In the **Deactivate Fixlet Stream** dialog, review the stream name and the warning that the automation will be deleted.

   b. Click **Deactivate** to confirm, or **Cancel** to keep the stream active.

The status changes to **Inactive**, the **Automate remediation schedule** panel reports that no automation is defined, and the edit and delete controls become available.



After you activate a stream, monitor progress from the **Overview** and **Deployments** tabs of the Fixlet Stream Details Page *(on page 339)*.

Related information

Managing Fixlet Streams *(on page 332)*

Editing a Fixlet Stream *(on page 334)*

Deleting a Fixlet Stream *(on page 338)*

Creating an automation for a Fixlet Stream *(on page 322)*

Editing a Fixlet Stream

Edit a Fixlet Stream to change its name, description, Fixlet criteria, or device criteria. A stream must be inactive before you can edit it.

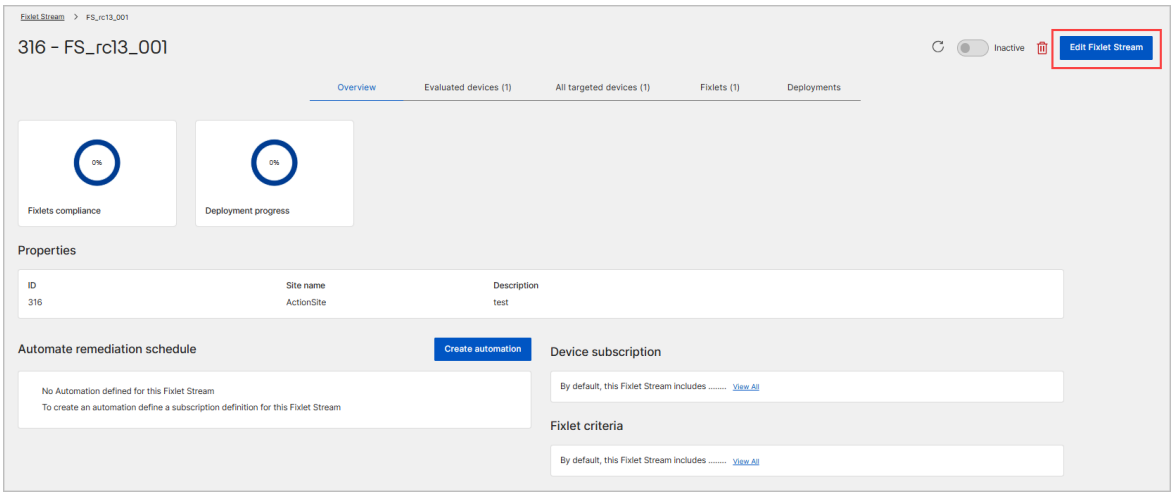
- You must have permission to manage Fixlet Streams.
- The stream must be inactive. The **Edit Fixlet Stream** button is unavailable while a stream is active. See Activating and deactivating a Fixlet Stream *(on page 332)*.

Expand **Resolve** from the side navigation, select **Fixlet Streams**, and then click the name of the stream.

1. Deactivate the stream if it is active.

   See Activating and deactivating a Fixlet Stream *(on page 332)*.

2. Click **Edit Fixlet Stream**.



The Create Fixlet Stream wizard reopens with your current settings.

3. Update the properties, Fixlet criteria, or device criteria.

   For what each step of the wizard controls, see Create Fixlet Stream *(on page 314)*.

4. Click **Edit** on the Summary step to save your changes.

   If the Fixlets, Evaluated devices, or All targeted devices tab still shows the previous results after you edit a filter, click the refresh icon in the top-right corner of the Fixlet Streams landing page, or reload the browser page. See Troubleshooting *(on page 344)*.

Editing a stream does not restore the automation that was deleted when you deactivated it. Create the automation again to resume deployments. See Creating an automation for a Fixlet Stream *(on page 322)*.

Related information

Managing Fixlet Streams *(on page 332)*

Create Fixlet Stream *(on page 314)*

Activating and deactivating a Fixlet Stream *(on page 332)*

Troubleshooting *(on page 344)*

Editing a Fixlet Stream automation

Edit the automation of an active Fixlet Stream to change when and how it deploys Fixlets, without changing the Fixlet criteria or the device subscription.

- You must have permission to manage Fixlet Streams.
- The Fixlet Stream must already have an automation defined. See Creating an automation for a Fixlet Stream *(on page 322)*.

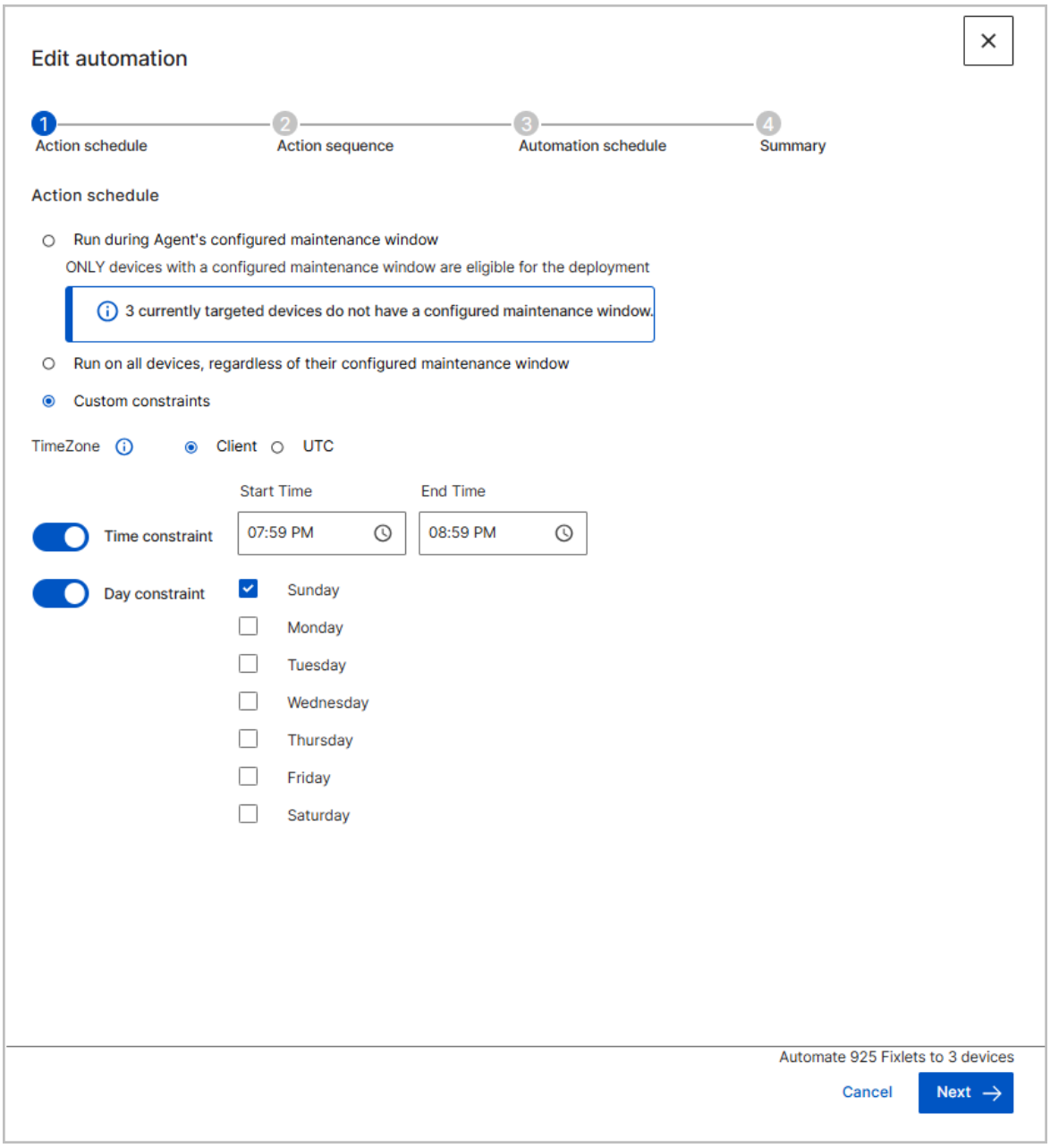
Expand **Resolve** from the side navigation, select **Fixlet Streams**, and then click the name of the stream. You can also click **Edit automation** directly on the stream card on the landing page.



Note: Editing an automation does not require you to deactivate the stream. To change the Fixlet criteria or the device subscription instead, see Editing a Fixlet Stream *(on page 334)*.

1. In the **Automate remediation schedule** panel, click **Edit automation**.

   The **Edit automation** wizard opens at the **Action schedule** step, with the current settings in place.



2. Update the settings on the **Action schedule**, **Action sequence**, and **Automation schedule** steps as required.

   For what each setting controls, see Creating an automation for a Fixlet Stream *(on page 322)*.

3. On the **Summary** step, review the settings, and then click **Create** to save the new schedule.

The stream deploys Fixlets on the updated schedule. Deployment activity appears on the **Deployments** tab of the stream.

Related information

Managing Fixlet Streams *(on page 332)*

Creating an automation for a Fixlet Stream *(on page 322)*

Editing a Fixlet Stream *(on page 334)*

Fixlet Stream Details Page *(on page 339)*

Deleting a Fixlet Stream

Delete a Fixlet Stream when you no longer need it. A stream must be inactive before you can delete it.

- You must have permission to manage Fixlet Streams.
- The stream must be inactive. The delete icon is unavailable while a stream is active. See Activating and deactivating a Fixlet Stream *(on page 332)*.

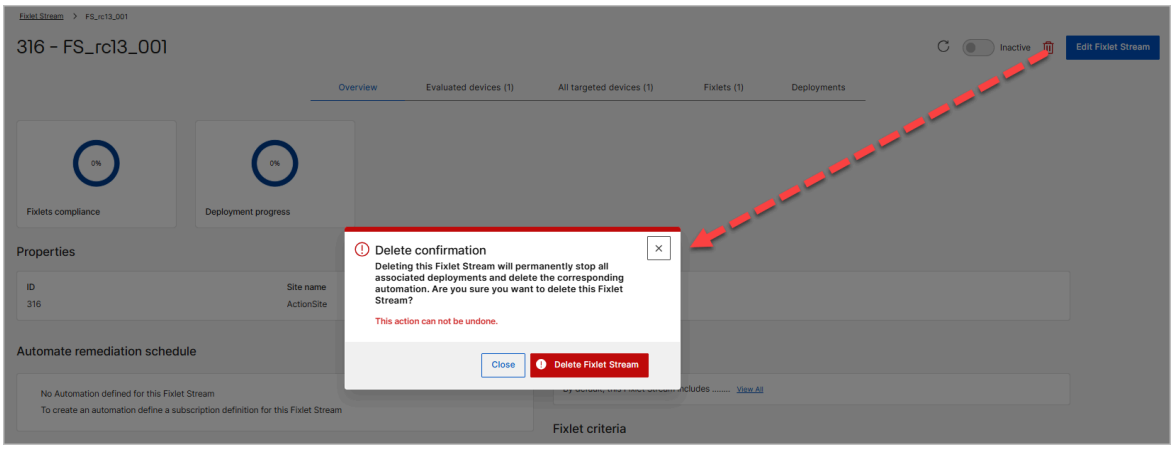
Expand **Resolve** from the side navigation, select **Fixlet Streams**, and then click the name of the stream.

CAUTION: Deleting a Fixlet Stream permanently stops all deployments associated with the stream that are still running, and deletes the corresponding automation. The stream's criteria and device subscription are also removed. You cannot undo this action. Deployments that already ran are not reversed, and historical deployment records remain available from **Explore** > **Deployments**.

1. Deactivate the stream if it is active.

   See Activating and deactivating a Fixlet Stream *(on page 332)*.

2. Click the delete icon next to the status toggle.
3. In the **Delete confirmation** dialog, review the message, and then click **Delete Fixlet Stream** to confirm. To keep the stream, click **Close**.



The stream is removed from the Fixlet Streams landing page. Any deployments of the stream that are still running stop, and its automation is deleted.

Related information

Managing Fixlet Streams *(on page 332)*

Activating and deactivating a Fixlet Stream *(on page 332)*

Editing a Fixlet Stream *(on page 334)*

Fixlet Stream Details Page

The Fixlet Stream details page provides a centralized view of a specific Fixlet Stream, including its configuration, subscribed devices, selected Fixlets, and deployment activity. From this page, you can monitor compliance, review automation settings, and activate, edit, or delete the stream.

Note:

- A Fixlet Stream remains inactive until automation is created and activated.
- Once automation is active, deployment activity appears in the Deployments tab.
- Automation status is reflected immediately in the Overview tab.
- Compliance and count values are not immediate. They update after the subscribed devices report their state again. See Device Count and Relevant Fixlet Count Take Time to Update *(on page 345)*.

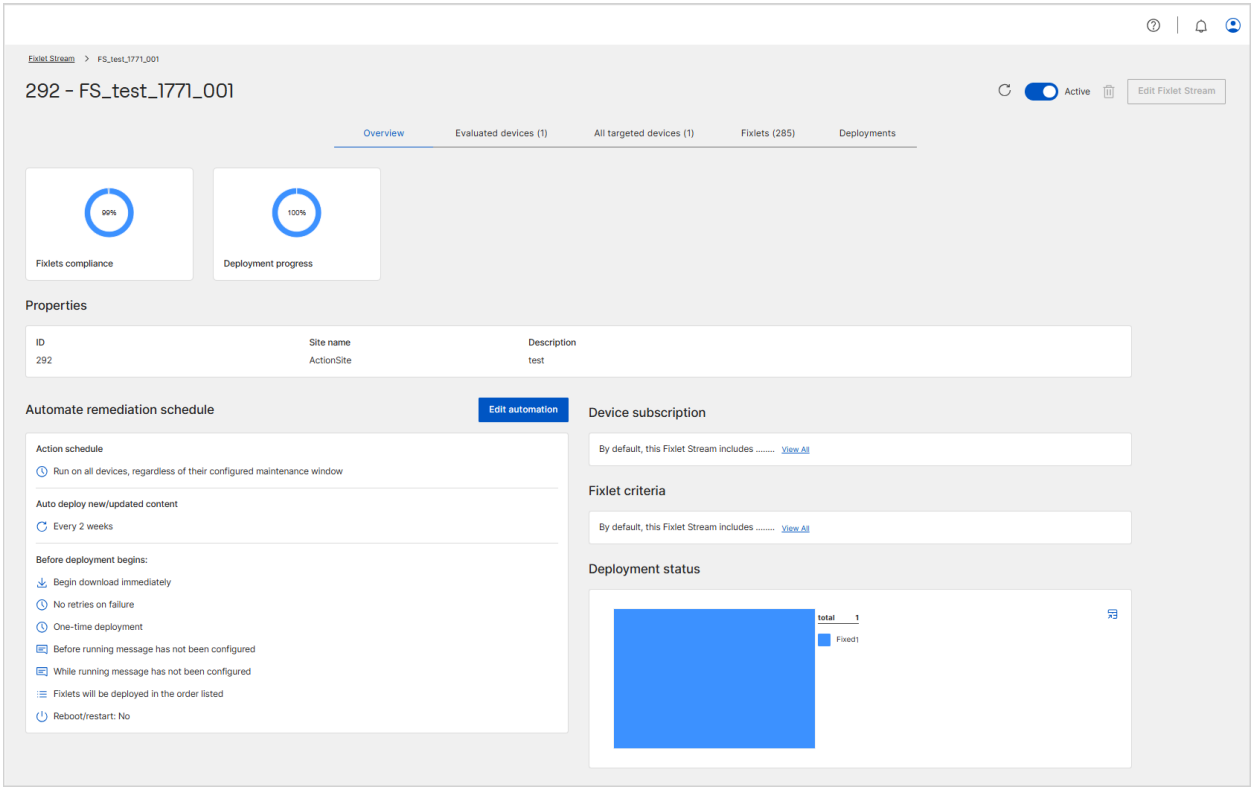
To monitor the fixlet streams, expand **Resolve** from the side navigation, and then select **Fixlet streams**. Click the required Fixlet Stream card. The Fixlet Stream details page opens.

The page header shows the stream ID and name, for example **292 - FS_test_1771_001**, and the page has the following tabs:

- **Overview**
- **Evaluated devices**
- **All targeted devices**
- **Fixlets**
- **Deployments**

Overview tab

The Overview tab displays a high-level summary of the Fixlet Stream's status and configuration.



Fixlets compliance: Shows the overall compliance percentage for Fixlets included in the stream, as a ring chart.

Deployment progress: Displays the current deployment status for the stream, as a ring chart. If no deployments have occurred, the card shows **No data available**.

Automate remediation schedule:

Displays the configured automation settings, including:

- **Action schedule**: The deployment time range and the days of the week, for example **Time range: 07:59 PM - 08:59 PM, client time zone** and **Days of week: Sun**.
- **Auto deploy new/updated content**: The refresh frequency, for example **On the 2 day of the month**.
- **Before deployment begins**: The download, retry, message, order, and reboot behavior.

If automation has not been configured, this section indicates that no automation is defined.

Device subscription:

Shows the device conditions that were defined for the Fixlet Stream, for example **Name contains 46, ID = 1612992728**. To change these conditions, deactivate the stream and then click **Edit Fixlet Stream**.

Fixlet criteria: Shows the conditions that select the Fixlets for the stream, for example **DefaultAction is not, Title not contains**. Select **View All** to read the full set of conditions.

Deployment status: Summarizes the outcome of the deployments that the stream generated, broken down by state with a total. If the stream has not deployed anything yet, the panel shows **No deployment data found**.

Status: The toggle in the upper-right corner shows whether the Fixlet Stream is **Active** or **Inactive**. Use it to activate or deactivate the stream. A delete icon and the **Edit Fixlet Stream** button appear next to the toggle.

Important: The **Edit Fixlet Stream** button and the delete icon are unavailable while a stream is active. Deactivate the stream first. Deactivating deletes the automation created for the stream, so you must create the automation again afterward. See Activating and deactivating a Fixlet Stream *(on page 332)*.

Properties: Displays the **ID**, **Site name**, and **Description** of the Fixlet Stream.

- **Edit Options**:
  - **Edit automation**: Change the automation settings, including the action schedule, the action sequence, and the automation schedule. See Editing a Fixlet Stream automation *(on page 335)*.
  - **Edit Fixlet Stream**: Opens the Fixlet Stream configuration so you can update its details and criteria. Available only when the stream is inactive. See Editing a Fixlet Stream *(on page 334)*.

If you edit a filter and the tabs still show the previous results, refresh the data. On the Fixlet Streams landing page, click the refresh icon in the top-right corner, or reload the browser page. See Troubleshooting *(on page 344)*.

Working with the data tables

The **Evaluated devices**, **All targeted devices**, **Fixlets**, and **Deployments** tabs each present their records in a data table with the same set of controls:

- **Filter**: Narrows the rows of the table. Build each condition from a **Property**, an **Operator**, and a **Value**. See Table filter *(on page 40)*.
- **Density**: Sets the row spacing to **Compact**, **Standard**, or **Comfortable**. See Density *(on page 29)*.
- **Search**: Finds records in the table. Type in the search box above the table to filter the rows as you type.
- **Sort**: Orders the rows by a column. Select the sort icon in a column header to switch between ascending and descending order. See Sorting Data *(on page 30)*.
- **Column options**: Select the options icon in a column header to change how that column is displayed.

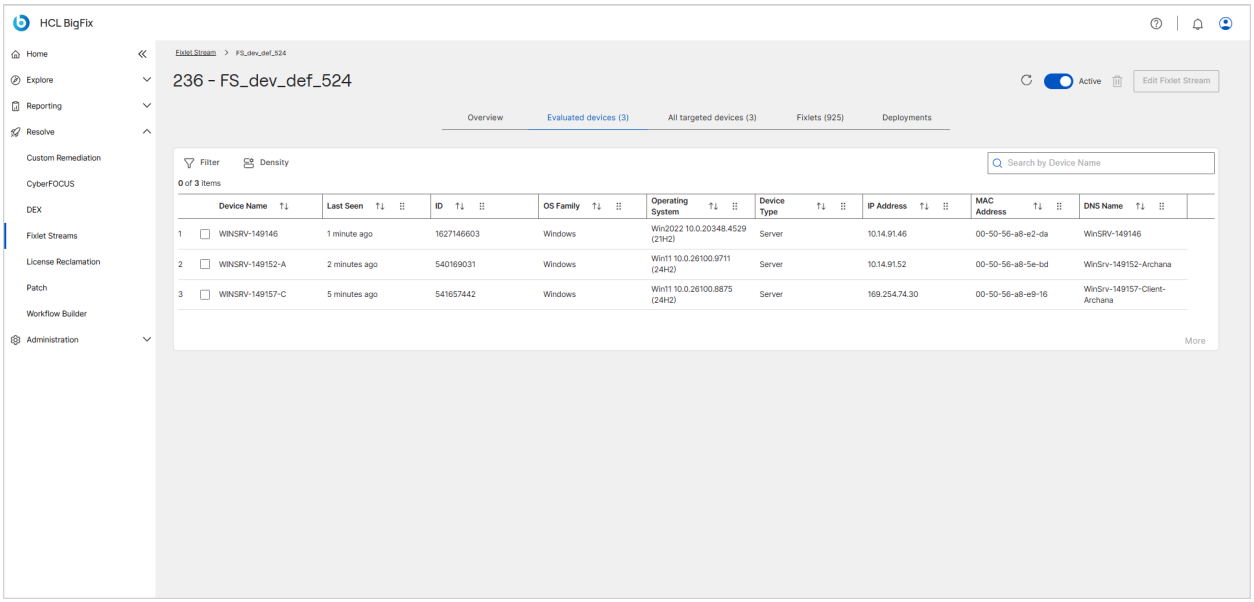
Above each table, an item count shows how many rows you selected out of the total, for example **0 of 2 items**. If the table holds more rows than the page shows, select **More** at the lower right to load further rows.

Note: The tab labels include the current record count, for example **Evaluated devices (3)** and **Fixlets (925)**. This count reflects the stream definition, so it can differ from the number of rows in the table when a filter or search is active.

Evaluated devices tab

The **Evaluated devices** tab lists the targeted devices that have reported to the BigFix server since the Fixlet Stream was created. A device that matches the device subscription but has not reported since then does not appear on this tab. For example, a device that has not reported for a month is listed on **All targeted devices** only. As each targeted device reports, it is added to this tab, and the list updates as reporting devices begin or stop matching the subscription criteria. To see newly reported devices, click the refresh icon in the upper-right corner of the details page.

The table reports **Device Name**, **Last Seen**, **ID**, **OS Family**, **Operating System**, **Device Type**, **IP Address**, **MAC Address**, and **DNS Name**. On this tab, the **Operating System** column reports the build that the device last sent, for example **Win11 10.0.26100.9711 (24H2)**.

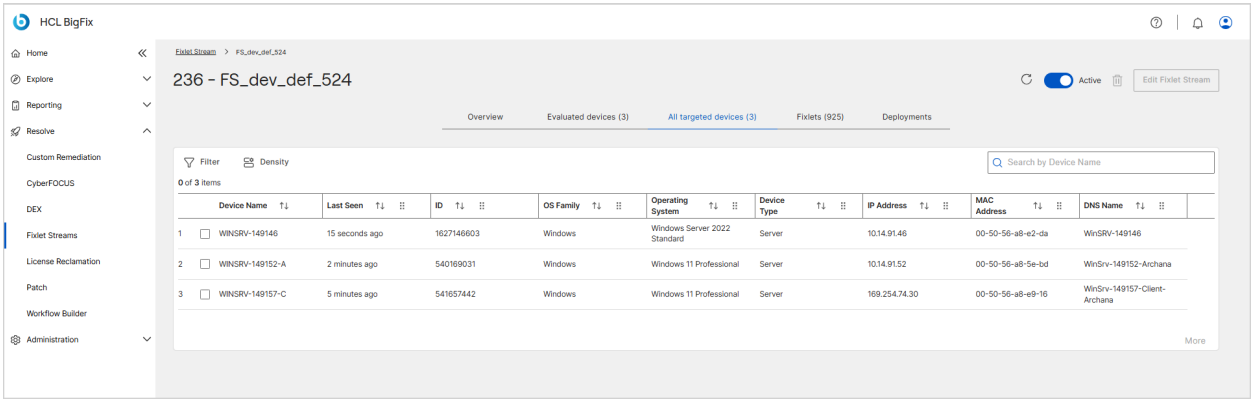


All targeted devices tab

The All targeted devices tab lists every device that the device subscription targets, whether or not the stream has evaluated it yet.

The table reports the same columns as the **Evaluated devices** tab, but the **Operating System** column reports the product name, for example **Windows Server 2022 Standard** or **Windows 11 Professional**.

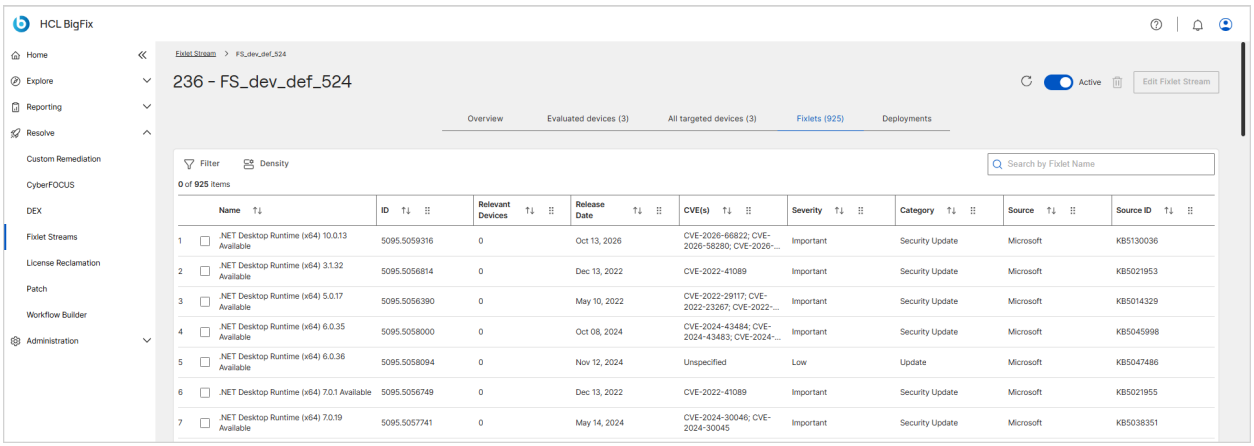
Compare the two tabs to confirm that every targeted device is reporting. A device that appears on **All targeted devices** but not on **Evaluated devices** has not reported since the stream was created. To check, review the device's **Last Seen** value on this tab. A device whose **Last Seen** value is recent, for example a few seconds or a minute ago, also appears on **Evaluated devices** after you refresh the page. See Device Count and Relevant Fixlet Count Take Time to Update *(on page 345)*.



Fixlets tab

The Fixlets tab displays all Fixlets included in the Fixlet Stream. This list is continuously updated as new Fixlets match the stream criteria or existing Fixlets become irrelevant.

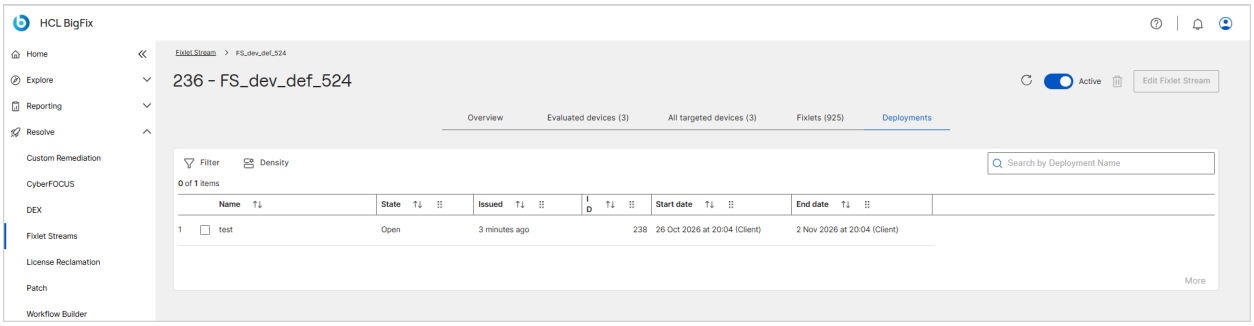
The table reports **Name**, **ID**, **Relevant Devices**, **Release Date**, **CVE(s)**, **Severity**, **Category**, **Source**, and **Source ID**. A column shows **[null]** or **[empty]** when the Fixlet carries no value for it.



Deployments tab

The Deployments tab displays deployment activity generated by the Fixlet Stream automation. A deployment appears only after the automation creates an action, which happens only when the Fixlets are relevant to at least one subscribed device. If no deployments have occurred, the page displays **No data available**.

The table reports **Name**, **State**, **Issued**, **ID**, **Start date**, and **End date**. The **Name** column shows the automation name that you entered on the Summary step of the wizard. The start and end dates report the client time zone, for example **26 Oct 2026 at 20:04 (Client)**. An open deployment that has no fixed schedule shows **[null]** as its start and end date.



Related information

Managing Fixlet Streams *(on page 332)*

Create Fixlet Stream *(on page 314)*

Managing Filters *(on page 35)*

Common Functionalities *(on page 28)*

Troubleshooting *(on page 344)*

Troubleshooting

Understand these common issues and their resolutions, so that you can effectively troubleshoot and resolve problems encountered while managing and monitoring Fixlet Streams, ensuring smooth and efficient deployment processes.

No sites appear in the Site(s) list

Issue: On the Fixlets step of the Create Fixlet Stream wizard, the **Site(s)** list is empty, and you cannot continue.

Cause: Your role has access to the Fixlet Streams application but not to any external patch content site. The list shows only external sites whose names begin with *Patches for*, *Updates for*, *ESU Patching*, or *Known Exploited Vulnerabilities Content Pack for*.

Resolution: Ask your administrator to edit your role and turn on access to at least one external patch content site on the **Sites** step, under **External sites (read only access)**. See Editing a role *(on page 480)*.

Expected Fixlets are missing from the stream

Issue: Fixlets that match your criteria are not included in the stream.

Cause: The stream includes only Fixlets that have a default action and are not superseded. Tasks are never included.

Resolution: Confirm that the content meets the requirements in Create Fixlet Stream *(on page 314)*.

Edited Filter Results Do Not Appear

Issue: After you edit a filter on an existing Fixlet Stream and save the change, the Fixlets or Devices tab still lists the previous results. The counts on the stream card and on the details page also stay unchanged.

Cause: The page does not reload the results automatically after a filter change.

Resolution:

- **Refresh the list**: On the Fixlet Streams landing page, click the refresh icon in the top-right corner to reload the stream data. Your saved changes are not lost, only the displayed results are stale.
- **Refresh the browser page**: If the results are still stale, press F5, or use the browser reload button, to load the updated Fixlet and device lists.
- **Confirm the new criteria**: After the page reloads, check the Fixlet count and device count on the stream card to confirm that the edited filter produced the scope you expected.

Device Count and Relevant Fixlet Count Take Time to Update

Issue: The counts and compliance figures on a Fixlet Stream do not change as soon as you expect. For example:

- A new stream shows **0 Devices** for several minutes, even though devices already match the subscription criteria.
- The **Relevant Fixlets** count stays unchanged after a deployment finishes, even when the deployment reports 100% successful.
- The **Fixlets compliance** ring chart continues to show the earlier percentage.

Cause: These metrics are derived from the state that devices report to the server. A Fixlet Stream does not recalculate them from the deployment result. Instead, it waits for each device to report its latest state in the next reporting cycle. Until that report arrives, the stream shows the values from the previous cycle.

What to expect: Reflecting correct metrics takes time. In a small environment, the first device count on a new stream can take about five minutes to appear. The relevant Fixlet count and the compliance percentage update after the affected devices report again, so the delay depends on your reporting interval and on how many devices the stream targets.

Resolutions:

- **Allow time for the next report**: Wait for the subscribed devices to report their state before you judge the counts. The stream is working as designed during this interval.
- **Refresh the data**: Click the refresh icon on the Fixlet Streams landing page, or reload the browser page, to pick up the latest reported values. A refresh does not force the devices to report.
- **Confirm the deployment outcome**: To check whether a Fixlet was applied, open the **Deployments** tab and review the deployment state instead of the relevant Fixlet count. A successful deployment with an unchanged count means the device has not reported yet.

Long Load Times for Complex Queries

Issue: A Fixlet Stream takes a long time to display results, or the page stops responding while it evaluates criteria. This is most common when a stream spans a large number of Fixlets, for example when you validate compliance across more than 100 Fixlets.

Cause: Complex relevance queries evaluate a large amount of content across many devices. Broad criteria, many sites, or many conditions increase the processing time.

What to expect: Loading can take more than one minute. In some cases the request stops before results appear.

Resolutions:

- **Allow extra time**: Wait for the query to finish before you retry. Repeated attempts add load and slow the result further.
- **Narrow the criteria**: Reduce the number of selected sites, or add conditions such as severity or category, so that the stream evaluates fewer Fixlets.
- **Split the stream**: Create several smaller Fixlet Streams instead of one broad stream. Smaller streams load faster and are easier to monitor.
- **Run during off-peak hours**: Schedule large evaluations when fewer operators are using the system.

Slow Response When Creating an Automation Right After Deactivating

Issue: You deactivate a Fixlet Stream and immediately click **Create automation**. The wizard is slow to open, or the automation is not created.

Cause: The system is still removing the previous automation when the new request arrives.

Resolutions:

- **Wait before you retry**: Allow the deactivation to finish, click the refresh icon, and confirm that the status shows **Inactive** and that the schedule panel reports no automation.
- **Create the automation again**: Start the wizard once the stream is confirmed inactive.
- **Check for duplicates**: Review the **Automate remediation schedule** panel to confirm that only the intended automation exists.

Error Fetching Devices

Issue: When attempting to apply dynamic filters, you may encounter the error message: "**Error fetching devices. Please try again.**"

Causes:

- Incorrectly defined filter conditions.
- Attributes or values that do not exist in the device database.
- Network connectivity issues preventing the system from querying devices.

Resolutions:

- **Validate Conditions**: Review the conditions you set for the dynamic filters. Ensure that attributes, conditions, and values are correctly specified and applicable to your devices.
- **Test with Simplified Filters**: Temporarily simplify your conditions to isolate the problematic parameter. Start with broad filters and then narrow down to identify the issue.
- **Check Network Connectivity**: Ensure that the system has access to the necessary network resources to fetch device information.

Low Fixlet Compliance Percentage

Issue: The Fixlet compliance percentage is lower than expected after a deployment.

Causes:

- Devices may not meet the dynamic filter criteria.
- There may be compatibility issues preventing devices from applying the Fixlet.
- Some devices may be offline or not connected during deployment.
- The stream includes dynamic Fixlets. A dynamic Fixlet stays relevant after it is applied, so it does not raise the compliance percentage. See Monitoring *(on page 313)*.

Resolutions:

- **Review Filter Conditions**: Check if the dynamic filters are too restrictive. Adjust conditions to include more devices if necessary.
- **Investigate Compatibility**: Ensure that the Fixlet is compatible with the targeted devices (e.g., OS version, hardware requirements).
- **Check Device Status**: Confirm that all intended devices are online and connected. Consider scheduling the deployment during a time when devices are most likely to be active.

Deployment Progress Stalled

Issue: The deployment progress bar shows little to no movement over an extended period.

Causes:

- High network traffic or bandwidth limitations.
- Issues with the Fixlet itself, such as improper configuration.
- Large numbers of devices being targeted, causing slow processing.

Resolutions:

- **Monitor Network Performance**: Check network traffic and performance to ensure it can support the deployment. Consider deploying during off-peak hours.
- **Verify Fixlet Configuration**: Ensure that the Fixlet is configured correctly without any errors that could cause it to stall.
- **Segment Deployments**: If targeting a large group of devices, consider segmenting the deployment into smaller groups to expedite the process.

Related information

Create Fixlet Stream *(on page 314)*

Managing Fixlet Streams *(on page 332)*

Common use cases

Fixlet Streams provide a versatile solution for managing patch deployments and updates across a range of device environments. Below are some common use cases illustrating how organizations can effectively utilize Fixlet Streams:

Automating Regular Patch Management

Description: Organizations can set up Fixlet Streams to automate the deployment of regular patches and updates for operating systems and applications.

Scenario:

- A company schedules monthly patch deployments for all Windows devices using a built-in Fixlet Stream.
- Dynamic filters are set to include only devices running specific OS versions to ensure compatibility.
- The automation runs automatically each month, reducing manual effort and ensuring all devices are up-to-date.

Addressing Critical Vulnerabilities

Description: In response to emerging security threats, organizations can quickly deploy Fixlet Streams to address critical vulnerabilities (0-day vulnerabilities).

Scenario:

- A cybersecurity team identifies a critical vulnerability affecting a widely used application.
- They create a temporary Fixlet Stream that targets all devices running the vulnerable application and applies the necessary patches.
- Dynamic filters can be adjusted to ensure rapid deployment to affected devices, minimizing risk exposure.

Managing Compliance with Regulatory Requirements

Description: Organizations in regulated industries can use Fixlet Streams to ensure that devices comply with necessary security standards and regulations.

Scenario:

- A healthcare organization must adhere to HIPAA regulations and maintain compliance on all devices accessing patient data.
- They set up a Fixlet Stream that automates the deployment of security updates and compliance patches specifically tailored for healthcare applications.
- Regular monitoring of Fixlet compliance percentages helps ensure that all devices remain compliant.

Testing Software Updates Before Full Deployment

Description: Before rolling out updates to all devices, organizations can use Fixlet Streams to test software updates on a small group of devices.

Scenario:

- An IT department wants to verify a new version of an internal application.
- They create a Fixlet Stream to target only a limited number of devices for testing purposes.
- After monitoring the test deployment, feedback is gathered, and adjustments are made before a full-scale rollout.
- Because a stream must be inactive before it can be edited, plan a pause between the test run and the adjusted rollout. Deactivating the stream deletes its automation, so recreate the automation after you revise the criteria.

Segmenting Deployments Based on Device Attributes

Description: Organizations can create tailored deployments by segmenting devices based on specific attributes, such as department, location, or hardware specifications.

Scenario:

- A global organization has different device types used in various departments (e.g., HR, Finance, and Engineering).
- They set up multiple Fixlet Streams with dynamic filters that match devices based on department-specific software requirements.
- This ensures that each department receives the appropriate updates relevant to their operations without unnecessary deployments to unrelated devices.

Regular Maintenance for End-of-Life Devices

Description: For devices that are approaching end-of-life status, organizations can manage their maintenance using Fixlet Streams to extend their lifecycle while preparing for replacement.

Scenario:

- An organization has a number of legacy devices still in operation.
- A Fixlet Stream is created specifically for these devices to apply critical updates and patches, ensuring they remain secure while planning for replacements.
- Dynamic filters can target these legacy devices, allowing the IT team to manage resources effectively.

Related information

Create Fixlet Stream *(on page 314)*

Managing Fixlet Streams *(on page 332)*

Integrated Vulnerability Remediation

Integrated Vulnerability Remediation (IVR) correlates the vulnerability findings from your Tenable Vulnerability Management scanner with BigFix Fixlets and devices, so that you can review vulnerabilities and deploy their remediations from one place.

Overview

It is available from the **Resolve** > **Integrated Vulnerability Remediation** menu in BigFix UI. You can review vulnerabilities by vulnerability or by device, and start remediation from either view. Administrators set up and maintain IVR from **Administration** > Application Configuration *(on page 433)*. IVR refreshes scanner data every 12 hours by default.

Entitlement

Required:

- A BigFix license that includes the BigFix Insights for Vulnerability Remediation site: BigFix Remediate, BigFix Lifecycle, BigFix Compliance, BigFix Workspace or Workspace+, or BigFix Enterprise or Enterprise+.

Check:

- In the BigFix Console, the BigFix License Overview dashboard shows **BigFix Insights for Vulnerability Remediation** in the **Compliance/Lifecycle** panel.
- In BigFix UI, the **Integrated Vulnerability Remediation** tile appears on Administration > Application Configuration *(on page 433)*.

User permissions

Required role:

- **To use IVR:** a BigFix UI role that includes the IVR application, assigned in **Administration** > **Identity and Access** > User & Role Management *(on page 449)*.
- **To configure IVR:** a BigFix UI administrator account mapped to a BigFix operator. Only administrators can access Application Configuration *(on page 433)*.
- **To install IVR:** a BigFix Console operator who can enable external sites, activate analyses, and take actions.
- **To register IVR with BigFix UI (one time):** a local Windows administrator on the BigFix UI server, and the BigFix UI instance admin credentials.

Required scope:

- **To remediate:** the devices that the user's mapped BigFix operator can target.
- **Site subscription:** computers subscribed to the BigFix Insights for Vulnerability Remediation site. **All computers** is recommended.

Prerequisites

- **BigFix platform:** BigFix UI installed and connected to a Windows-based BigFix Server, version 11.0.7.61 or later.
- **BigFix content:** the BigFix Insights for Vulnerability Remediation site enabled (site version greater than 0), and the **IVR Vulnerability Scanner Host ID** analysis activated globally.
- **IVR backend:** the BES IVR Retriever Service, installed with the **Download BigFix IVR Retriever v5.0.0.0** Task on the BigFix UI server or on a separate computer.
  - Operating system: Windows Server 2016, 2019, 2022, or 2025.
  - Hardware: at least 2 CPU cores (4 recommended). In addition to the operating system, 2 GB of RAM and 4 GB of disk space per 20,000 endpoints.
- **IVR database:** an IVR schema that IVR creates in the BigFix UI database on Microsoft SQL Server 2025. The database user must have permission to create a schema. Back up the BigFix UI database before you configure IVR.
- **Network:**
  - Inbound to the IVR host from BigFix UI on ports 8088 and 9022.
  - Outbound from the IVR host to Tenable on port 443 (a proxy is supported) and to the BigFix UI database on port 1433.

- **Scanner:** a Tenable Vulnerability Management account with an administrator role to generate API keys. IVR supports one data source.
- **Earlier IVR versions:** uninstalled before you install IVR v.5.

Full documentation

For full feature documentation, see BigFix Integrated Vulnerability Remediation (IVR) v.5.

Related

- Remediate Documentation
- Platform Documentation
- BigFix UI User's Guide
- BigFix UI Administration Guide

Patch

The **Patch dashboard** tells you which Fixlets and devices to look at first and links back to the **Fixlet explorer** for the action.

Overview

It is available from the **Resolve** > **Patch** menu in BigFix UI.

Entitlement

Required:

- A BigFix license that includes the Patch entitlement.

Check:

- In the BigFix Console, the BigFix License Overview dashboard shows the Patch entitlement as active.
- In BigFix UI, **Settings > Licensing** shows the entitlement as active.

User permissions

Required role:

- Patch Operator (or Administrator).

Required scope:

- Access to the devices or device groups and patch sites targeted by the deployment.

Prerequisites

- BigFix UI installed and connected to the BigFix Server.
- At least one managed endpoint with the Patch content sites enabled and subscribed.

Full documentation

Full feature documentation: Patch on BigFix UI in the Patch Portal, with a link back to this page.

Related

- Patch portal landing page
- BigFix UI portal landing page
- Explore *(on page 76)*.

Security Compliance

Security Compliance gives Security and Compliance administrators a live, environment-wide view of compliance posture across every Checklist deployed in the BigFix environment.

Overview

It is available from the **Resolve** > **Security Compliance** menu in BigFix UI.

Entitlement

Required:

- A BigFix license that includes the Compliance Distribution entitlement.

Check:

- In the BigFix Console, the BigFix License Overview dashboard shows the Compliance entitlement as active.
- In BigFix UI, **Settings > Licensing** shows the entitlement as active.

User permissions

Required role:

- Compliance Reporting Operator (or Administrator).

Required scope:

- Access to the Checklists, Devices, and Device Groups.

Prerequisites

- BigFix UI installed and connected to the BigFix Server.
- At least one managed endpoint subscribed to an enabled compliance reporting site.

Full documentation

Full feature documentation: Security Compliance on BigFix UI in the Compliance Portal, under **SCM**, with a link back to this page.

Related

- Security compliance dashboard under SCM.
- Compliance portal landing page
- BigFix UI portal landing page
- Explore *(on page 76)*.

License Reclamation

The License Reclamation page shows which software is installed but not used, and the savings that you gain when you uninstall it. Use it to find the software that costs the most, to see where you can save money, and to reclaim licenses with one click. For more information, see Support for BFUI License Reclamation with mTLS.

To open the page, expand **Resolve** in the side navigation, and then select **License Reclamation**.

Entitlement

- **Required:** BigFix Workspace / BigFix DEX entitlement enabled on the BigFix license.
- **Check:** Navigate to **Settings > Licensing** to verify that the DEX entitlement status shows as active.

User permissions

- **Required role:** DEX Operator, Workspace Operator (or Master Administrator).
- **Required scope:** Read/manage access to target Devices, Device Groups, and DEX Dashboards within the BigFix UI.

Prerequisites

- BigFix UI installed, configured, and connected to the BigFix Server.
- BigFix Scanner and the DEX Scanner Plugin deployed to target managed endpoints.
- Target endpoints subscribed to the relevant DEX sites and actively collected metrics (CPU/memory usage, crash reports, boot/login times).

Full documentation

Full feature documentation: Support for BFUI License Reclamation with mTLS

Related

BigFix Workspace

Reporting

The Reporting section provides tools to create, view, and manage reports for analysis and decision-making.

Reporting allows you to generate insights from BigFix data and share them across your team. It includes:

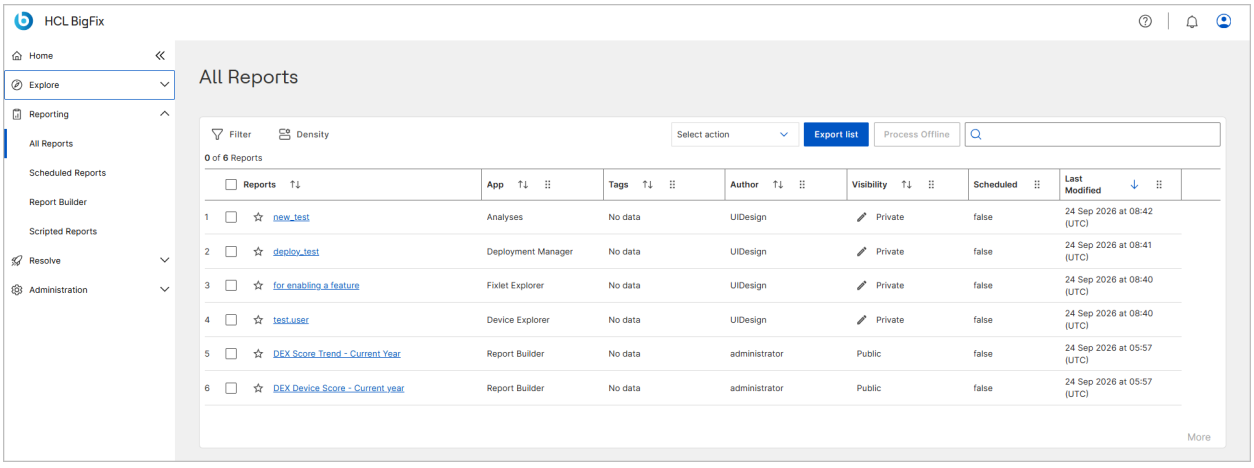
- **All Reports** *(on page 355)* – View, manage, and organize every report available in BigFix UI from one page. Apply filters, export data, generate a report offline, delete reports, assign tags, manage report visibility, and mark reports as favorites.
- **Scheduled Reports** *(on page 366)* – Run a saved report automatically at a time that you choose, send the result by email, and keep an archive of each run. The page lists every schedule that you can access and shows its status and next run.
- **Report Builder** *(on page 384)* – Create visual reports from the data in your BigFix environment with a wizard. Start from a pre-built template or build a report from scratch with full manual control.
- **Scripted Reports** *(on page 424)* – Write reports in HTML with embedded BigFix Relevance expressions and optional JavaScript or CSS. Use them to design advanced, interactive reports beyond the standard Report Builder charts.

All Reports

The All Reports page is a central location to view, manage, and organize all reports available in BigFix UI. From this page, you can apply filters, export data, generate a report offline, delete reports, assign tags, and manage report visibility. You can also mark reports as favorites to find them quickly.

The All Reports page lists every report you create in BigFix UI. Because all of your reports are collected in one place, you can view, manage, and organize them without switching between apps.

To open the All Reports page, expand **Reporting** from the side navigation, and then select **All reports**.



Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to the Reports application, and your access level (**Admin**, **Users**, or **Read only**) determines what you can do here. See Managing Roles *(on page 467)*.
- Your operator permissions determine which actions you can complete, such as deleting a report or assigning tags. For a description of each permission, see Permissions reference *(on page 482)*.

Reports table

The reports table lists your reports and their details. It contains the following columns:

Table 61. All Reports columns

Column	Description
Favorites	A star control on each row. Select the star to mark or clear a report as a favorite.
Reports	The title of the report. Select the name to open the report.
App	The application associated with the report, such as **Device Explorer**, **Analyses**, or **Report Builder**.
Tags	The tags applied to the report. Shows the tag name, a count link (for example, *2 tags*) if more than one tag is applied, or *No data* if no tag is applied. Select a count link to open the tag drawer, where you can select one or more tags and remove them. After you remove tags, the drawer closes and the table refreshes automatically. To assign tags, see Assigning tags to reports *(on page 357)*.
Author	The user who created the report.
Visibility	Indicates whether the report is **Public** or **Private**. Select the edit icon next to the value to change the report's visibility.
Scheduled	Shows whether the report is scheduled to run automatically.
Last Modified	The date and time the report was last updated.

Toolbar controls

The toolbar above the table provides the following controls:

Table 62. All Reports toolbar controls

Control	Description
Search	Enter a report name or keyword to filter the list, and then press **Enter**. The list updates only after you press **Enter**.
Select action	Choose an action to run on the selected reports: **Delete** to remove the reports, or **Manage tags** to open the **Manage tags** drawer. Both actions are available only when at least one report is selected.
Export list	Download the report data for offline use or external sharing. For the full procedure, see Exporting reports *(on page 361)*.
Process Offline	Generate the selected report in the background so that you can keep working. This control is available only when you select a report. For the full procedure, see Generating a report offline *(on page 361)*.
Density	Adjust the row spacing of the table between compact and comfortable.
Filter	Open the filter panel to narrow the reports shown. For the filter properties, see Filtering reports *(on page 360)*.

Note: The **Delete** and **Manage tags** actions are disabled until you select at least one report. User permissions, as assigned by administrators, might restrict some users from deleting reports or assigning tags.

About report tags

Tags are custom labels that you assign to reports to group and find them quickly. You assign tags to a report after the report is created; you cannot add tags while creating a report in the Report Builder, scheduled reports, or scripted reports.

Assigned tags appear in the **Tags** column. When a report has one tag, the tag name appears. When a report has more than one tag, a count link appears, such as *2 tags*. Select the count link to open the tag drawer. To remove tags, select the **X** on each tag chip, and then select **Save changes**. The drawer closes automatically, and the **Tags** column updates without a page refresh.

Note: Report tagging uses the same access controls as the earlier labels feature. If you could manage labels for a report, you can manage its tags.

Tags also apply to Fixlets, deployments, and analyses. For an overview of tagging across BigFix UI, see Managing Tags *(on page 51)*.

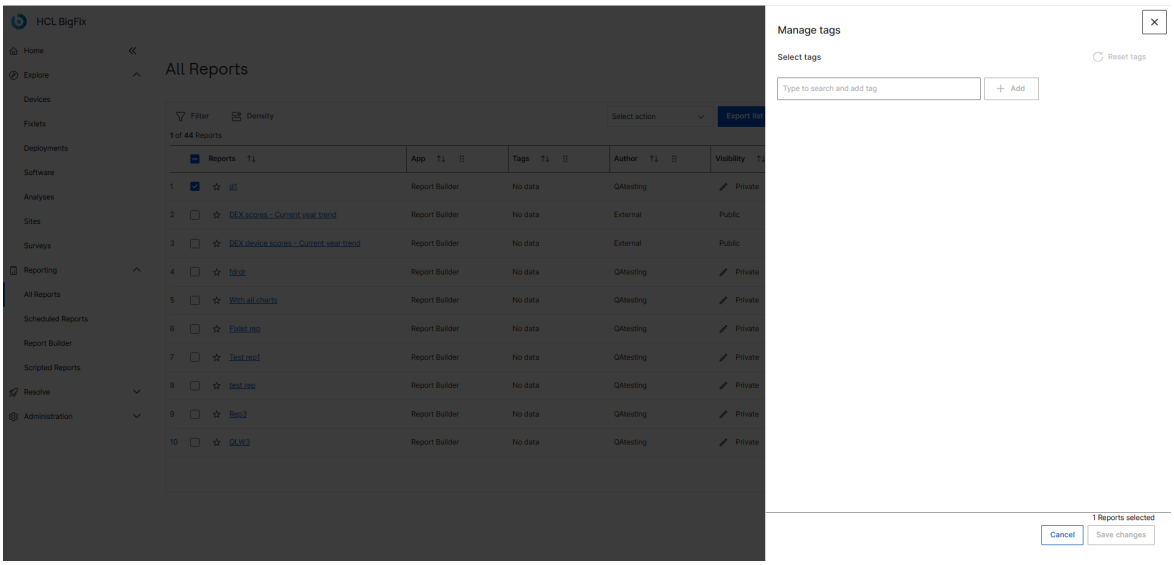
Assigning tags to reports

Assign one or more tags to reports so that you can group and locate them from the All Reports page. You can create new tags or apply existing ones, and you can assign tags to several reports at once.

To assign tags to reports:

1. On the All Reports page, select one or more reports.
2. Select **Select action** > **Manage tags**.

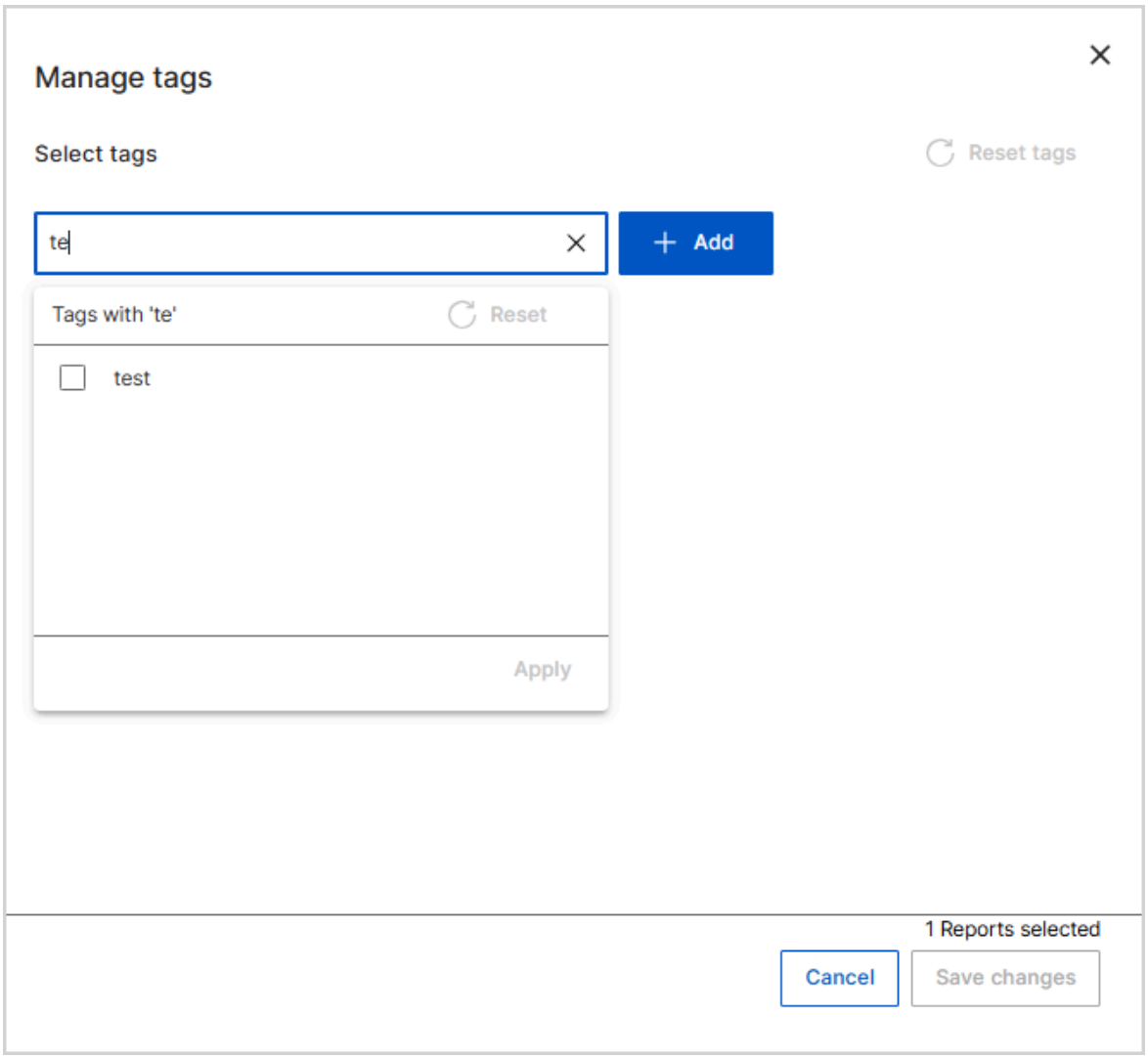
   The **Manage tags** drawer opens from the right side of the screen. If you selected one report, the drawer lists the tags on that report. If you selected several reports, the drawer lists only the tags that all of them share. For example, if you select two reports and only one of them has the *Security* tag, the drawer does not list *Security*.



3. To create a tag, enter a name in the **Select tags** box, and then select **Add**.

   The new tag is added to the list of selected tags. The tag is not created and applied until you select **Save changes**.

4. To apply existing tags, enter text in the **Select tags** box to filter the **Tags with '<text>'** suggestion list, select the check box for each tag you want, and then select **Apply**.



Note: When you select several reports, the **Tags with '<text>'** list leaves out any tag that some of those reports already have. You can still create a new tag and apply it to every report you selected. To copy such a tag to the reports that are missing it, open each of those reports one at a time and add the tag there.

5. To remove a tag from the selection, select the **X** on its chip. To restore the tags that were assigned when you opened the drawer, select **Reset tags**.

   The tag is removed from the report only after you select **Save changes**.

6. Select **Save changes**.

Important: Adding and removing tags takes effect only when you select **Save changes**. If you close the drawer or select **Cancel**, BigFix UI discards the tags that you added or removed.

The drawer closes automatically, a success message appears, for example **Tag(s) Assigned - 2 tags has been assigned to 1 report**, and the All Reports table reloads to show the assigned tags in the **Tags** column. You don't need to refresh the page.

Important: If a tag cannot be created, the message **Tag could not be created - There was an internal error creating the tag** appears. Wait a moment, and then try to add the tag again.

The following table describes the controls in the **Manage tags** drawer.

Table 63. Manage tags drawer controls

Control	Description
Select tags	Enter text to create a tag or to filter the suggestion list of existing tags. Select the **X** in the box to clear the text.
Add	Create a tag from the text you entered and add it to the selected tags.
Tag chips	The tags currently selected. Select the **X** on a chip to remove that tag from the selection.
Tags with '<text>'	The suggestion list of existing tags that match your text. Select a check box to include a tag, and then select **Apply**.
Reset tags	Restore the tags that were assigned when you opened the drawer.
Save changes	Apply the selected tags to the selected reports. The drawer closes and the table reloads automatically.
Cancel	Close the drawer without changing the assigned tags.

Filtering reports

Use the **Filter** icon to open the **Filter data** panel and narrow the reports shown on the All Reports page. You build one or more conditions on report properties, and the list shows only the reports that match.

The available filter properties are:

- **Favorites**
- **Reports**
- **App**
- **Tags**
- **Author**
- **Visibility**
- **Scheduled**
- **Last Modified**

To filter reports:

1. Select the **Filter** icon to open the **Filter data** panel.
2. Under **Select top level filter condition**, select **Single condition** to use one filter block, or **Multiple condition (Criteria: OR)** to combine several blocks so that a report matches when it meets any block.
3. In **Filter block 1**, select **Single condition** to set one condition, or **Multiple condition (Criteria: AND)** to require a report to meet every condition in the block.
4. For each condition, select a **Property**, select an **Operator** (for example, **Contains**), and enter a **Value**.
5. To add another filter block, select **Add Block**. To delete a block, select **Remove block**.
6. Select **Apply**.

To clear every condition, select **Remove all**. For more about filtering across BigFix UI, see Table filter *(on page 40)*.

Exporting reports

Use **Export list** to download report data for offline use or external sharing. You can export the data in either of the following formats:

- **CSV** - A lightweight, text-based format suitable for data processing.
- **Excel** - A spreadsheet format suitable for analysis and visualization.

The file is saved to your local system. For the full procedure, see Exporting Data *(on page 30)*.

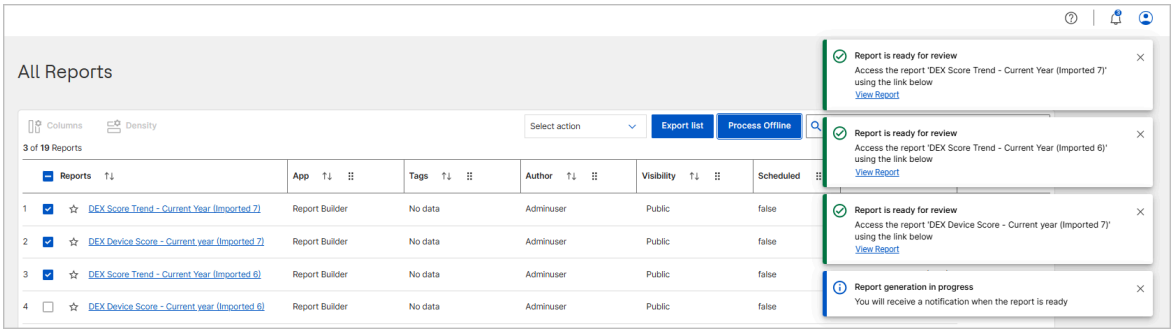
Generating a report offline

Use **Process Offline** to generate a report in the background so that you can keep working while BigFix UI prepares it. BigFix UI notifies you when the report is ready to review.

To generate a report offline:

1. On the All Reports page, select a report.
2. Select **Process Offline**.

   A notification confirms that report generation is in progress: **Report generation in progress - You will receive a notification when the report is ready.**



3. When the report is ready, select **View Report** in the **Report is ready for review** notification to open it.

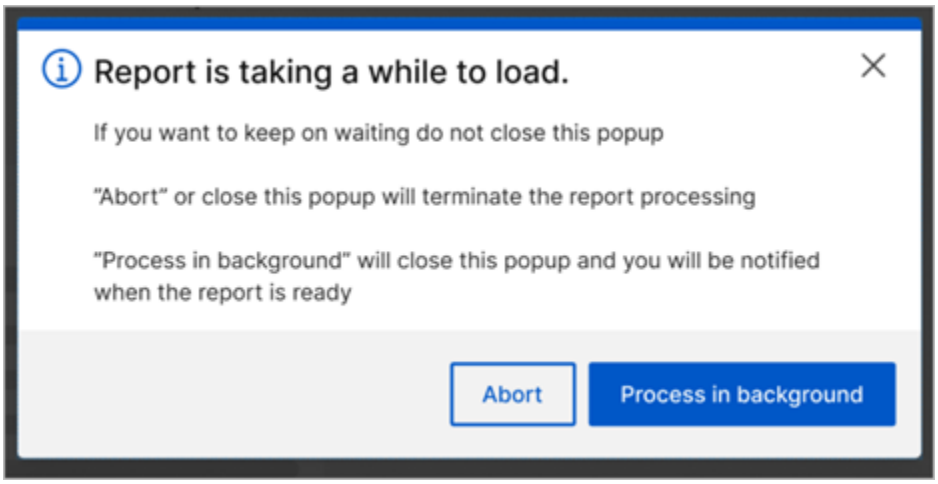
Note: If you dismiss the notification, you can still open the report. Select the notification (bell) icon in the upper-right corner of BigFix UI, and then select **View Report** for the report in the Notification Center. For more details, see Notification Center *(on page 58)*.

Working with a report

When you select a report name on the All Reports page, the report opens on its own page. The page header shows the report name, prefixed by the app that built it (for example, **Report Builder - test**), and the date and time the report was last updated. The page presents the report's **Quick link** cards and **Charts**.

If a report takes more than three seconds to load, the **Report is taking a while to load** message appears. Choose how to proceed:

- To keep waiting, leave the message open.
- Select **Process in background** to close the message and keep working. BigFix UI notifies you when the report is ready.
- Select **Abort** to stop processing the report. Closing the message also stops processing.



Note: This message appears only for device reports, fixlet reports, analyses reports, and Report Builder reports.

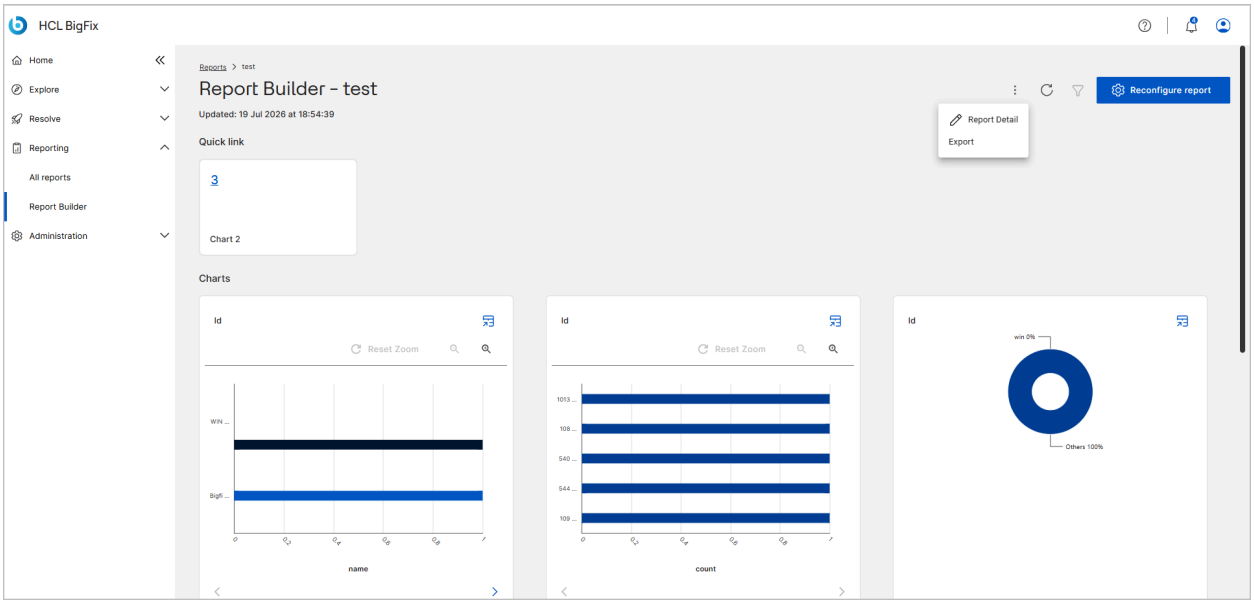
From the report page, you can edit the report's details, export it, refresh its data, and reconfigure it. The page header provides the following controls:

Restriction: The **Reconfigure report** control and the **Report details** panel apply only to reports that you build in Report Builder. Other apps that support reporting, such as Device Explorer, Fixlet Explorer, Deployment

Manager, and Analyses, use a simpler editing flow. In those apps, you change a report by updating the view and saving it again from the **Manage Reports** panel. For the steps, see Manage Reports *(on page 42)*.

Table 64. Report page controls for Report Builder reports

Control	Description
More options icon	Opens a menu with two actions: • **Report Detail** to open the Report details panel. For more details, see Editing report details *(on page 363)*. • **Export** to export the report. For the export formats and steps, see Exporting Data *(on page 30)*.
Refresh	Reloads the report with the latest data.
Reconfigure report	Opens the report in its builder so that you can change its configuration. For the steps, see Reconfigure a report *(on page 404)*.



Editing report details

Use the **Report details** panel to change a report's name, description, visibility, and tags. This panel is available only for Report Builder reports.

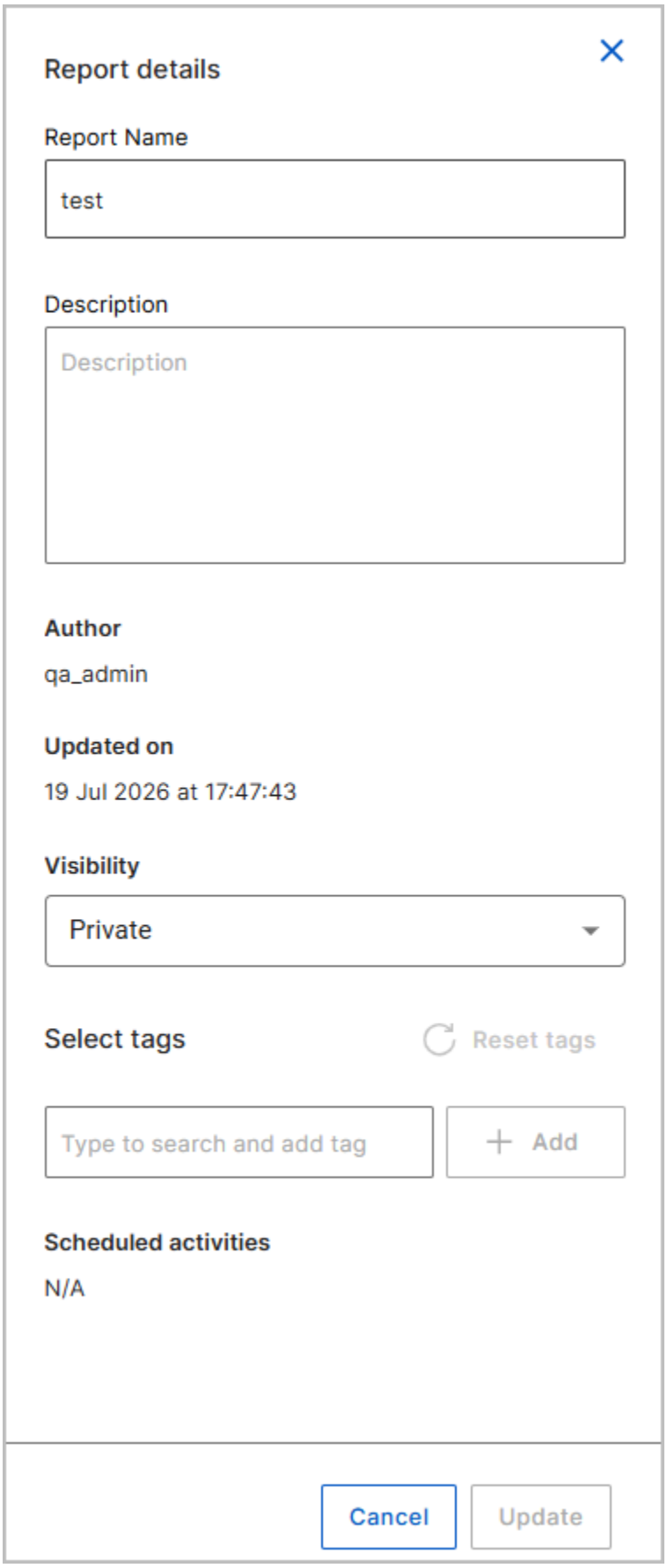
To edit a report's details:

1. On the All Reports page, select the report name to open the report.
2. Select the more options icon, and then select **Report Detail**.

   The **Report details** panel slides in from the right.

3. Edit any of the following: **Report Name**, **Description**, or **Visibility** (**Public** or **Private**).
4. To add a tag, enter text in **Select tags**, and then select **Add**. To clear the tags you added, select **Reset tags**.
5. Select **Update** to save your changes, or **Cancel** to close the panel without saving.

 **Note:** The **Author**, **Updated on**, and **Scheduled activities** fields are read-only.


Report details
Report Name
test
Description
Description
Author
qa_admin
Updated on
19 Jul 2026 at 17:47:43
Visibility
Private
Select tags
Reset tags
Type to search and add tag
Add
Scheduled activities
N/A
Cancel
Update

The following table describes the fields in the **Report details** panel of a Report Builder report.

Table 65. Report details panel fields

Field	Description
Report Name	The report's title. Editable.
Description	Optional text that describes the report. Editable.
Author	The user who created the report. Read-only.
Updated on	The date and time the report was last updated. Read-only.
Visibility	Sets whether the report is **Public** or **Private**. Editable from the dropdown.
Select tags	Adds tags to the report. Enter text to search for an existing tag, and then select **Add**. Select **Reset tags** to clear the tags you added.
Scheduled activities	Any scheduled runs for the report, or **N/A** if none are scheduled. Read-only.

Related information

Managing Tags *(on page 51)*

Manage Reports *(on page 42)*

Managing Filters *(on page 35)*

Scheduled Reports

Use Scheduled Reports to run a saved report automatically at a time that you choose, send the result by email, and keep an archive of each run. The Scheduled Reports page lists every schedule that you have access to and shows its status and next run.

A schedule (also called a scheduled activity) links one existing report to a recurrence pattern. Each time the schedule runs, BigFix UI generates the report, compresses the output and stores it as an archive, and sends an email notification if you configured one.

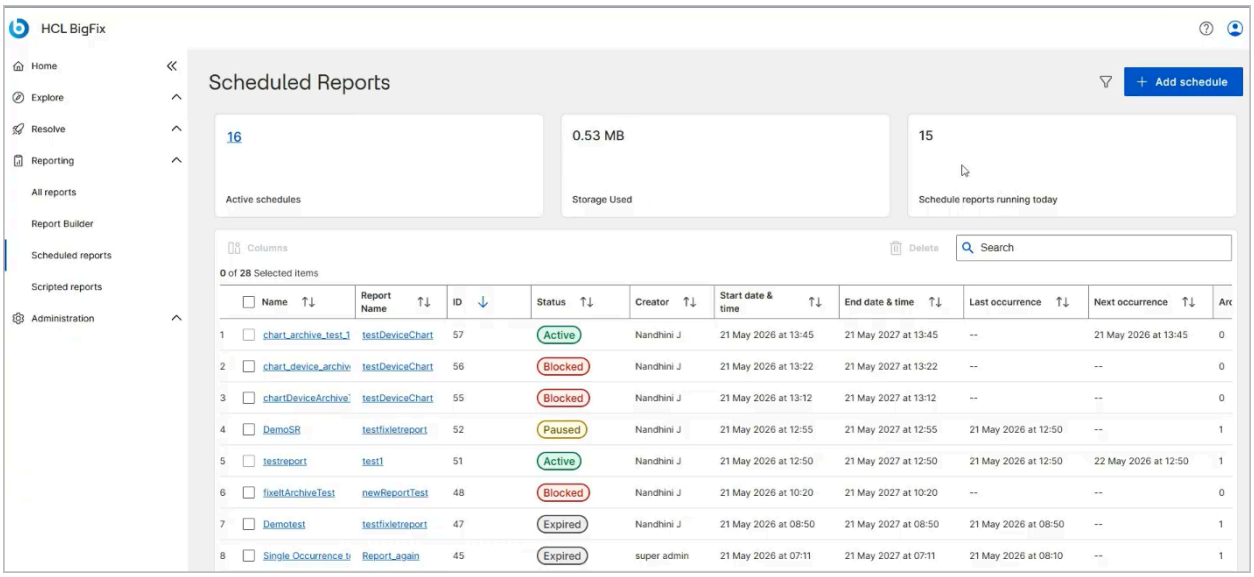
You can schedule a report only if the report is listed on the **All Reports** page and you are its owner, that is, you created the report. You cannot schedule reports that other users own. Scheduling supports reports from the following sources:

- Device Explorer
- Fixlet Explorer
- Analyses
- Deployment
- Report Builder

A schedule is independent of the report that it runs. Deleting a schedule does not delete the report, and you can create more than one schedule for the same report.

To open the page, expand **Reporting** in the side navigation, and then select **Scheduled Reports**.

Note: Email notifications require a configured SMTP profile. See the ***BigFix UI Administration Guide***.



Note: A schedule runs with the permissions of the user who created it. If that user account is deactivated, BigFix UI stops any run in progress and removes the user's schedules.

Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to the Reports application with the **Users** or **Admin** access level. With **Read only** access, Scheduled Reports is not available to you. See Managing Roles *(on page 467)* and Scheduled Reports with Read only access *(on page 368)*.
- Your operator permissions determine which actions you can complete. For a description of each permission, see Permissions reference *(on page 482)*.

Summary cards

Three cards above the table summarize your schedules:

- **Active schedules** – The number of schedules in the **Active** status. Select the number to filter the table so that it shows only those schedules.
- **Storage used** – The total size of the compressed report archives that are kept for your schedules, for example `0.53 MB`. Deleting schedules or archives frees this storage.
- **Schedule reports running today** – The number of schedules that have a run planned for the current day.

Note: Each user has a storage quota for scheduled report archives. The default quota is 10 MB per user. Your administrator sets the quota in the **ScheduledReportsQuotaPerUser** configuration setting, in bytes, and the value applies to all users. If you exceed the quota, BigFix UI sets your schedules to the **System Paused** status. Delete archives that you no longer need. For the full list of statuses, see Schedule statuses *(on page 381)*. For the setting, see the ***BigFix UI Administration Guide***, Configuration Variables.

Toolbar and table

The toolbar above the table contains **Filter** to narrow the list and **Density** to set the row height to **Standard**, **Compact**, or **Comfortable**. It also contains a selection counter such as **0 of 5 List of scheduled reports**, **Delete**, which is enabled when you select one or more schedules that are not active, and **Search**. For more information about filters, see Table filter *(on page 40)*.

The page header contains the page title and **+ Add schedule**.

Each row is one schedule. Select the value in the **Name** column to open the schedule details page, or select the value in the **Report Name** column to open the report itself. Select a column heading to sort the table. For the description of each column and status, see Scheduled Reports reference *(on page 380)*.

Scheduled Reports with Read only access

The Scheduled Reports page lists only the schedules that you created. It is not a view of every schedule on the system.

If your role grants **Read only** access to the Reporting application, the Scheduled Reports application is not available to you. **Scheduled Reports** is not shown under **Reporting** in the side navigation, so you cannot open the page or create a schedule.

You can still open an archived report if you have a valid report link, for example the **View Report** link in a notification email that was sent or forwarded to you. The link works until it expires. See Email notifications *(on page 380)*.

To create and manage schedules, ask your administrator for the **Users** or **Admin** access level for the Reporting application. For more information about access levels, see User & Role Management *(on page 449)*.

What you can do

- Create a schedule with the four-step **Add schedule** wizard. See Add a schedule *(on page 369)*.
- Review the configuration, the runs, and the archives of one schedule. See Schedule details page *(on page 373)*.

- Pause, resume, edit, or delete a schedule, and open or delete its archives. See Manage scheduled reports *(on page 375)*.
- Look up the table columns, the statuses, and the wizard fields. See Scheduled Reports reference *(on page 380)*.

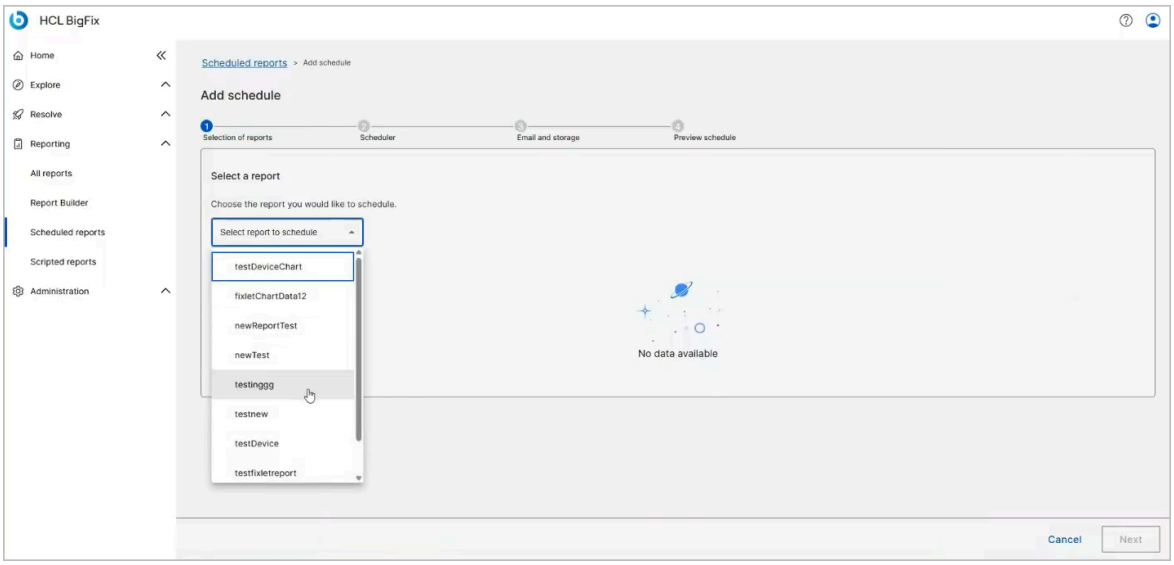
Add a schedule

Create a schedule that runs an existing report once or on a daily, weekly, or monthly basis, emails the result, and keeps an archive of each run.

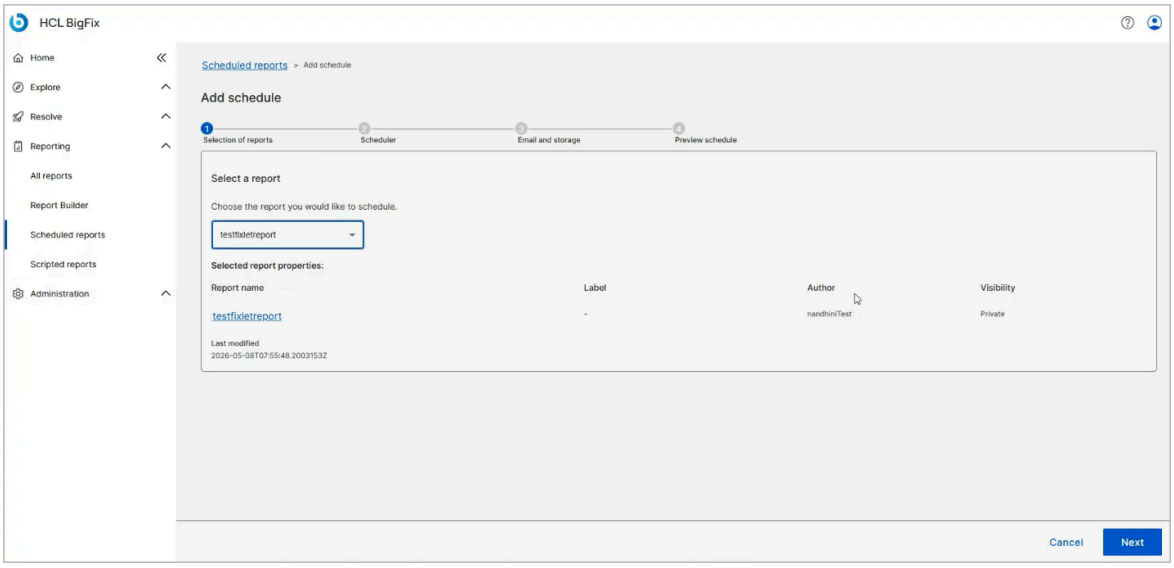
The report that you want to schedule must already exist on the **All Reports** page, and you must have created it (you must be the owner of the report). To create a report, see Create a report with custom configuration *(on page 397)*.

The **Add schedule** wizard has four steps: **Selection of reports**, **Scheduler**, **Email and storage**, and **Preview schedule**. A progress bar at the top of the wizard shows the current step. Select **Previous** to return to an earlier step, or **Cancel** to discard the schedule.

1. Expand **Reporting** in the side navigation, and then select **Scheduled Reports**.
2. Select **Add schedule**.
   The wizard opens at step 1, **Selection of reports**.
3. In the **Select report to schedule** list, select the report.



   The **Selected report properties** table shows the **Report name**, **Tags**, **Author**, and **Last modified** values of the report, and **Next** becomes available.



4. Select **Next**.
   Step 2, **Scheduler**, opens.

5. Under **Configure schedule**, define when the report runs.

   a. For **This event occurs**, select **Once**, **Daily**, **Weekly**, or **Monthly**.

   b. Under **Start conditions**, for **Time zone** select **Client** to use the time zone of the device that runs the report, or **UTC**.

   c. In **Select date**, pick the date of the first run.

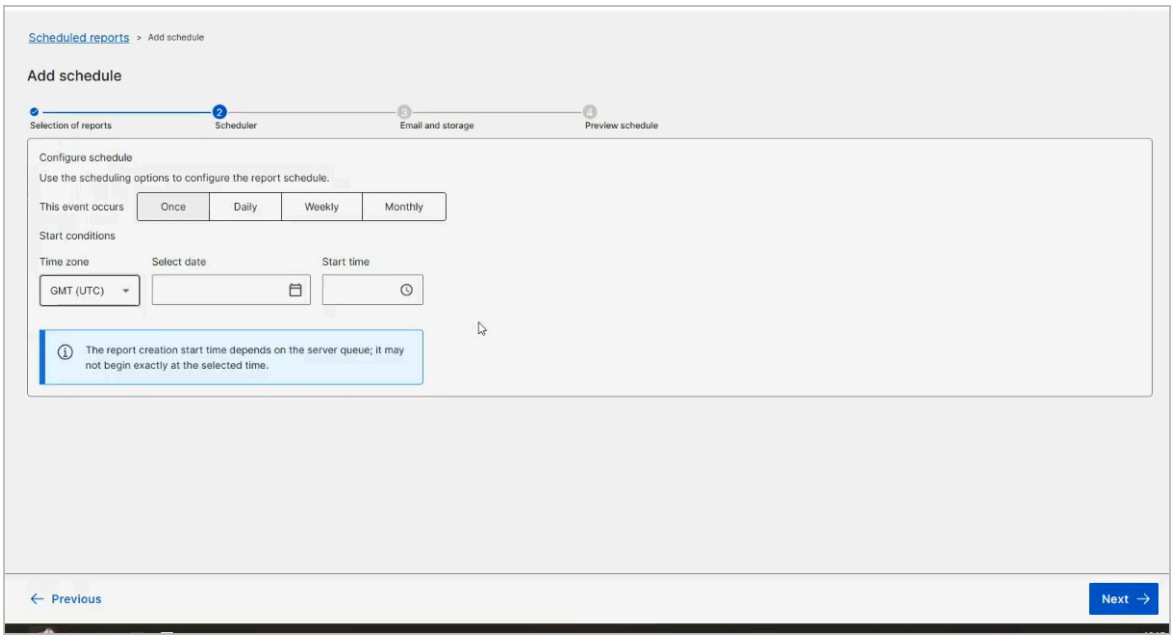
   d. In **Start time**, pick the time of the first run.

   e. Under **End conditions**, select **Never** to run the schedule indefinitely, **On** to stop it at a date and time that you choose, or **After** to stop it after a number of runs.

      If you select **On**, set **Select date** and **End time**. If you select **After**, enter the number of occurrences. The **End date & time** column and the schedule details page then show the computed end, for example `After 10 occurrences on 30 Sep 2026 at 16:50 (Client).`

Note: The report generation start time depends on the server queue. A run might not begin exactly at the selected time.

Note: All schedule dates in the list, on the details page, and in the preview are displayed with their time zone in brackets, for example `21 Sep 2026 at 14:58 (Client).`



6. Select **Next**.
   Step 3, **Email and storage**, opens.

7. Optional: Under **Notifications**, turn on **Email notifications** and complete the email fields.

   a. In **Email subject**, enter a subject. If you leave it empty, the default subject is used.

   b. In **Email to**, type a recipient name or address, select it, and then select **Add**. Repeat for each recipient. Each recipient appears as a chip below the field. Select the **X** on a chip to remove that recipient, or the clear (**X**) control in the input to empty it. You can add up to 50 recipients. Your administrator can change this limit in the **EmailMaxIndividualRecipients** configuration setting. See the ***BigFix UI Administration Guide***, Configuration Variables.

   c. To also notify the BigFix UI administrator, select **Notify the administrator about this schedule**.

   d. In **Body text (Optional)**, enter the message body. If you leave it empty, the default body text is used.

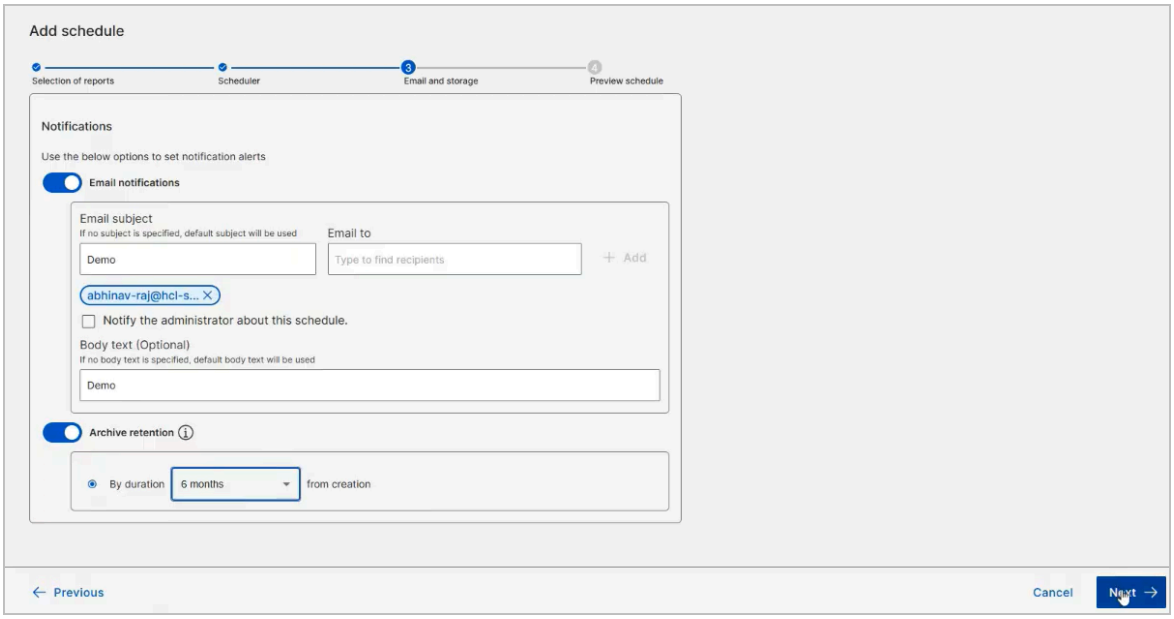
Note: The notification contains a report card and a **View Report** link that opens the archived report. By default, the link works for 30 days. Your administrator can change this period in the **ScheduledReportAccessTokenExpirationHours** configuration setting. See the ***BigFix UI Administration Guide***, Configuration Variables. Any user who has a valid BigFix UI account can open the link while it is valid, including a user who received it by forwarding. For the full contents, see Email notification contents *(on page 382)*.

Note: Email notifications require a configured SMTP profile. See the ***BigFix UI Administration Guide***.

8. Optional: Turn on **Retention**, and then select how long to keep each archive in the **By duration** list, for example **1 month** from creation.

   When the retention period ends, BigFix UI deletes the archive automatically.

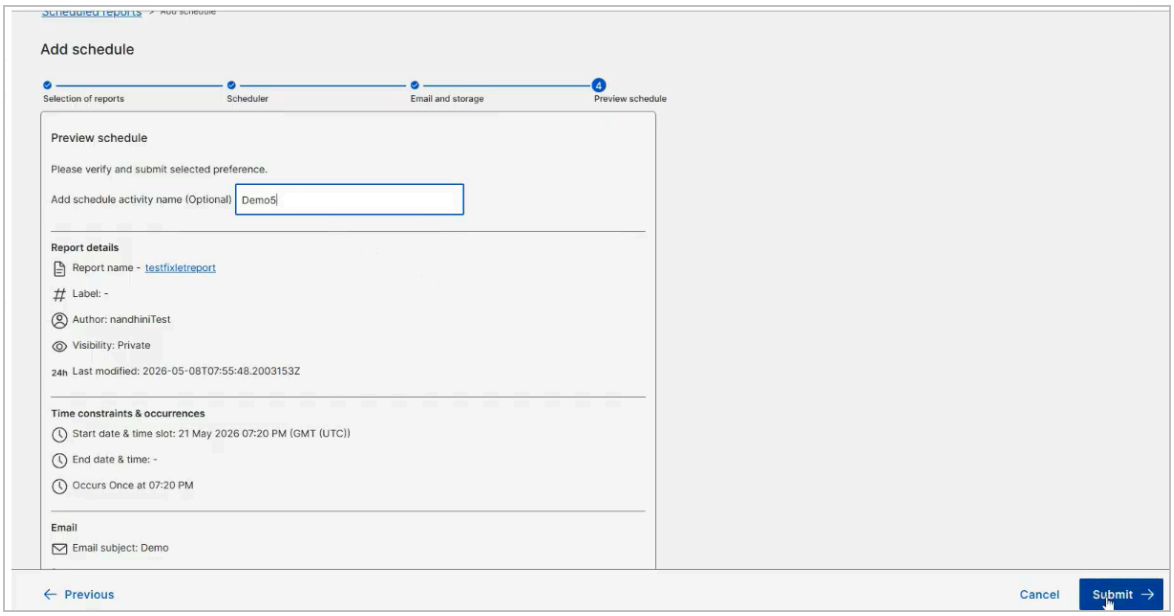
   Important: In this release, BigFix UI keeps every archive for 3 months, regardless of the period that you select in the **By duration** list and whether you turn on **Retention**.



9. Select **Next**.
   Step 4, **Preview schedule**, opens and summarizes the **Report details**, **Time constraints & occurrences**, **Email**, and **Retention** settings.

10. In **Add schedule activity name (Mandatory)**, enter a name for the schedule.

    This name appears in the **Name** column of the Scheduled Reports page. Choose a name that tells the recipients what the schedule delivers.



11. Verify the summary, and then select **Submit**.

The message `Schedule submitted successfully` confirms the action.

The schedule appears as a new row on the Scheduled Reports page with a new **ID** and the **Active** status. The **Next occurrence** column shows the first run. After each run, the generated report is listed on the **Archives** tab of the schedule details page, and the email is sent if you turned on notifications.

To change an active schedule, pause it first. See Manage scheduled reports *(on page 375)*.

Schedule details page

The schedule details page shows the configuration and run history of one schedule on the Overview tab, and the generated report archives on the Archives tab. From this page you pause, resume, edit, or delete the schedule.

To open the page, select the schedule in the **Name** column of the Scheduled Reports page. The breadcrumb **Scheduled Reports** > *schedule name* returns you to the list.

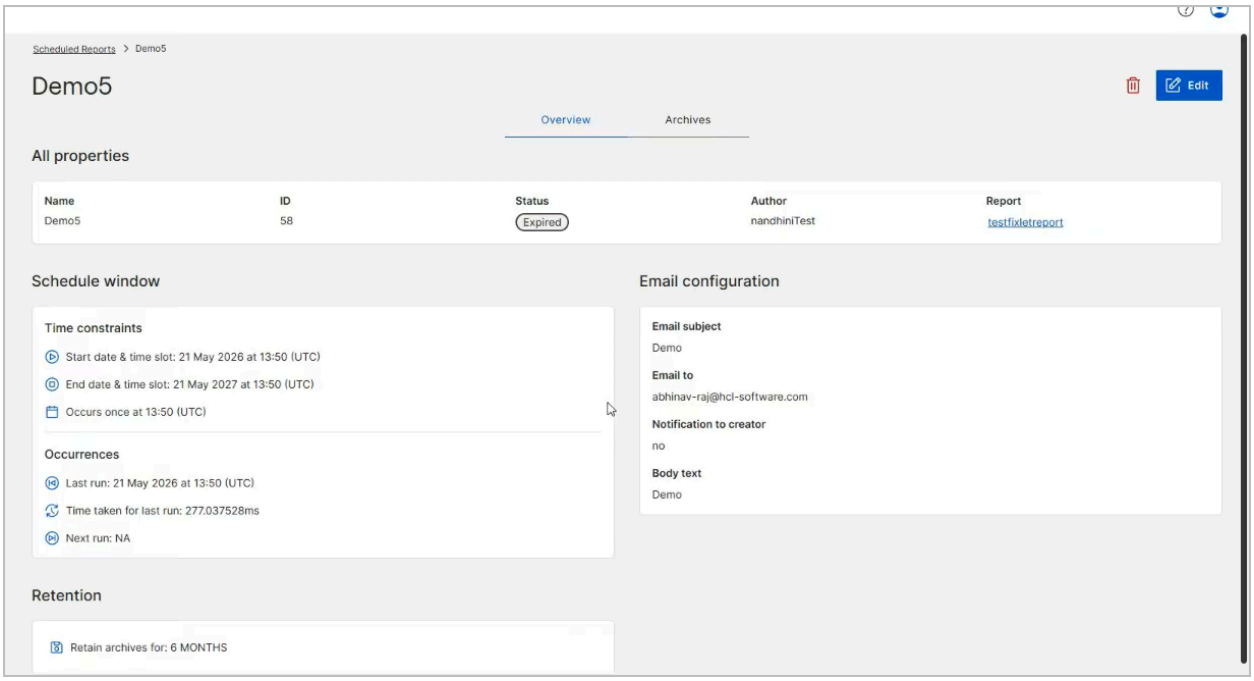
Page header

The header shows the schedule name and the following controls in the upper-right corner:

- Delete (trash icon) – Deletes the schedule and all of its archives after you confirm. Enabled only when the schedule is not active.
- **Pause** or **Resume** – Suspends an active schedule or restarts a paused one. The button that is shown depends on the current status.
- **Edit** – Opens the schedule in the wizard. Enabled only when the schedule is not active.

Note: When you point to a disabled **Edit** or delete control, the tooltip *"To edit / delete an active schedule, please pause it first before making any changes."* is shown.

Overview tab



The **Overview** tab groups the schedule settings into four panels:

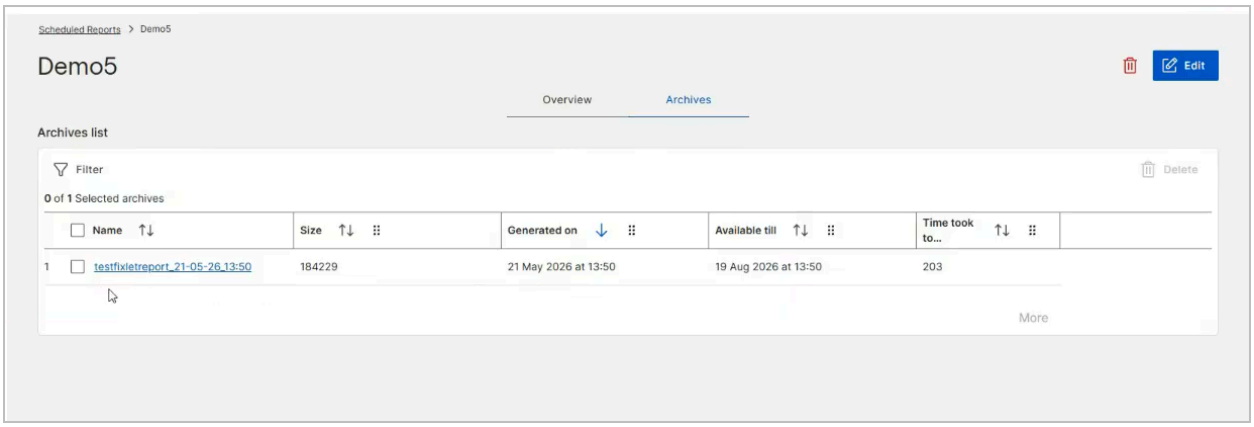
Table 66. Overview tab panels

Panel	Fields
All properties	**Name**, **ID**, **Status**, **Author**, and **Report**. Select the report name to open the report.
Schedule window	**Time constraints**: **Start date & time slot**, **End date & time slot**, and the recurrence, for example **Occurs once at 13:50 (UTC)**. The **End date & time slot** shows the end condition of the schedule, for example **After 10 occurrences on 30 Sep 2026 at 16:50 (Client)**. **Occurrences**: **Last run**, **Time taken for last run**, and **Next run**. **Time taken for last run** shows **N/A** before the first run, and **Next run** shows **NA** when no further run is planned.
Email configuration	**Email subject**, **Email to**, **Notification to creator** (**yes** or **no**), and **Body text**.
Retention	**Retain archives for**, for example **6 MONTHS**.

Archives tab

The **Archives** tab lists one archive for each completed run of the schedule, together with the time that the run took and the date on which the archive is deleted according to the retention period.

Select an archive name to open the archived report. The report opens in the standard report view, with the report name prefixed by the app that created it, such as **Report Builder - testfixletreport** or **Device explorer - Device Report with chart**, an **Updated** date and time, and the report content below. A report that contains charts also shows a **Charts** panel.



The toolbar contains **Filter**, a selection counter such as **0 of 1 Selected archives**, and **Delete**, which is enabled when you select one or more archives. A view selector labeled **Archives** sits above **Archives list**. Select **More** below the table to load additional archives. To delete archives, see View and delete report archives *(on page 379)*.

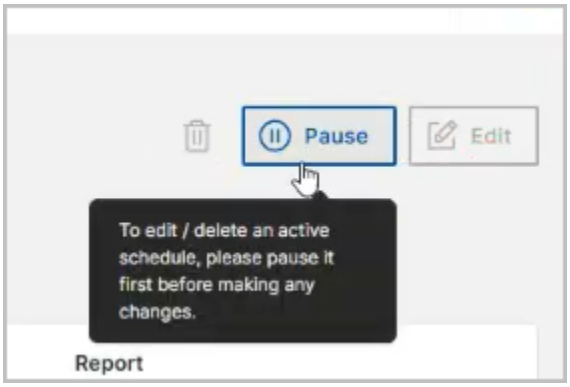
Table 67. Archives list columns

Column	Description
Name	The archive name, built from the report name and the execution date and time, for example `testfixletreport_21-05-26_13:50`. The date and time are always recorded in UTC, even when the schedule uses client time. Select the name to open the archived report.
Size	The size of the compressed archive, shown in the most appropriate unit, such as B, kB, or MB. The sum of these values is reported in the **Storage used** card on the Scheduled Reports page.
Generated on	The date and time when the run completed.
Available till	The date and time after which the archive is no longer available, according to the retention setting of the schedule.
Time took to...	The time that the run took to generate the report. The value is displayed using the most appropriate unit, such as milliseconds, seconds, or minutes.

Manage scheduled reports

After you create a schedule, you can pause it, resume it, change its settings, delete it, and work with the report archives that it generates. You perform these actions on the schedule details page. On the Scheduled Reports page, you can only delete schedules that are not active.

A schedule must not be active when you change or delete it. While a schedule is active it can run at any time, so BigFix UI disables the **Edit** and delete controls and shows the tooltip *"To edit / delete an active schedule, please pause it first before making any changes."*



Which actions are available depends on the status of the schedule. BigFix UI sets the **Blocked** and **System Paused** statuses automatically. For the cause of each one, see Schedule statuses *(on page 381)*.

Table 68. Available actions by status

Status	Pause or resume	Edit	Delete
Active	Pause	Not available	Not available
Paused	Resume	Available	Available
System Paused	Resume	Available	Available
Blocked	Not available	Available	Available
Expired	Not available	Available	Available

Pause or resume a schedule

Pause a schedule to suspend its runs temporarily, for example while you change the report that it uses. While a schedule is paused, no reports are generated and no emails are sent. The archives that the schedule already produced are kept.

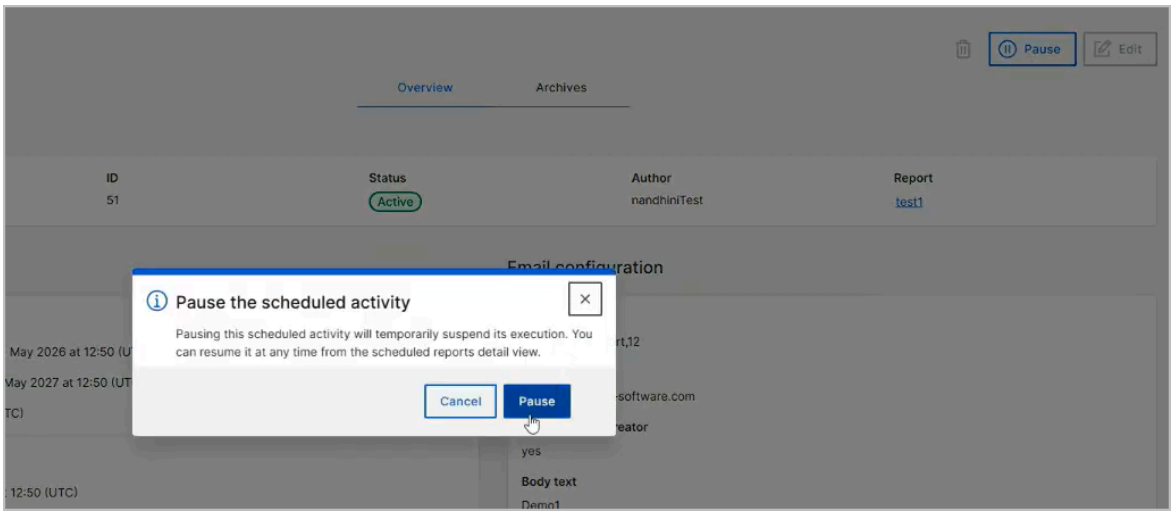
1. On the Scheduled Reports page, select the schedule in the **Name** column.

   The schedule details page opens.

2. In the upper-right corner, select **Pause**.

   The **Pause the scheduled activity** dialog opens.

3. Select **Pause** to confirm.



The message `Scheduled report paused successfully` confirms the change. The status changes to **Paused**, the **Pause** button changes to **Resume**, and the **Edit** and delete controls become available.

4. To start the schedule again, select **Resume** on the same page.

   The status returns to **Active**, and the **Next run** value is updated.

Edit a schedule

Editing reuses the same four-step wizard as Add a schedule *(on page 369)*, with the current values filled in. The wizard title reads **edit schedule**. You can change the report, the recurrence, the notification settings, and the retention period.

1. If the schedule is active, pause it as described in the previous section.
2. On the schedule details page, select **Edit**.

   The wizard opens at step 1, **Selection of reports**, with the current report selected.



3. Change the settings in each step as needed, and then select **Next** to move to the next step.

   For the description of each field, see Scheduled Reports reference *(on page 380)*.

4. In step 4, **Preview schedule**, verify the summary, and then select **Submit**.
5. Select **Resume** to make the schedule active again.

Note: Editing and submitting a schedule that has expired makes the schedule active again with the new settings.

Delete schedules

Delete a schedule when you no longer need the report to run automatically. Deleting a schedule does not delete the report itself: the report stays on the **All Reports** page and you can schedule it again.

Important: Deleting a schedule permanently deletes all past archives that belong to it and frees the storage that they used. You cannot recover the archived reports.

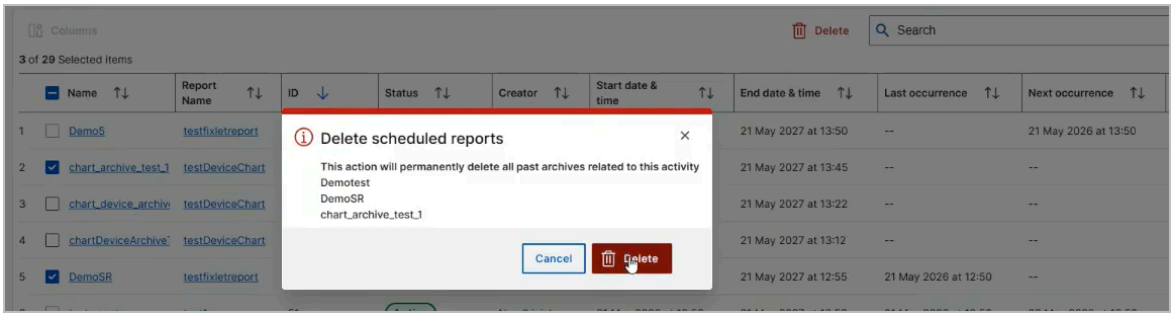
On the **Scheduled Reports** page, you can delete one or more schedules that are not active at the same time. You cannot select an active schedule. To delete an active schedule, pause it on the schedule details page first.

1. On the Scheduled Reports page, select the check box of each schedule that you want to delete.

   The selection counter, for example **3 of 29 List of scheduled reports**, and the **Delete** button in the toolbar are updated.

2. Select **Delete**.

The **Delete scheduled reports** dialog lists the names of the selected schedules.



3. Select **Delete** to confirm.

   The message `Scheduled reports successfully deleted` confirms the action, and the rows are removed from the table.

To delete a single schedule from its details page, select the delete (trash) icon in the upper-right corner, and then select **Delete** in the **Delete scheduled reports** dialog.

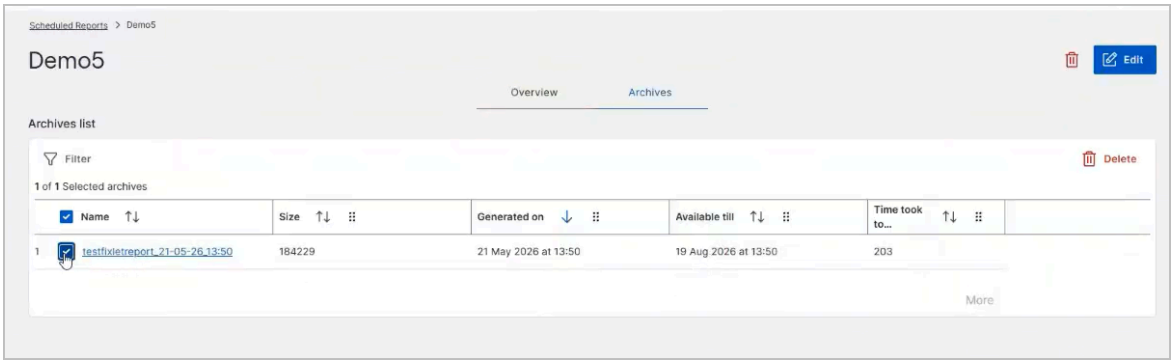
View and delete report archives

Each completed run of a schedule produces one archive. The **Archives** tab of the schedule details page lists the archives, how long each run took, when it ran, and when the archive is removed according to the retention period. For the description of each column, see Archives tab *(on page 374)*.

1. On the Scheduled Reports page, select the schedule in the **Name** column, and then select the **Archives** tab.
2. To open an archived report, select the archive name, for example `testfixletreport_21-05-26_13:50`. The name contains the report name and the execution date and time, always in UTC.

   The archived report opens in the standard report view. The page header shows the report name prefixed by the app that created it, such as **Report Builder - testfixletreport** or **Device explorer - Device Report with chart**, the **Updated** date and time, and the report content below.

3. To remove archives that you no longer need, select the check box of each archive, and then select **Delete** in the **Archives list** toolbar.



The **Delete archives** dialog opens with the message `This action will permanently delete selected archives.` followed by the archive name.

4. Select **Delete** to confirm.

   The message `Archives successfully deleted` confirms the action. The archives are removed and the storage that they used is freed. The **Storage used** card on the Scheduled Reports page is updated. If you deleted every archive, the **Archives** tab shows **No Data Available**.

Note: Archives are also removed automatically when they reach the date in the **Available till** column.

Email notifications

If you turned on email notifications for a schedule, each recipient receives an email when a run finishes. The email contains a report card and a **View Report** link that opens the archived report in BigFix UI. For the description of each field, see Email notification contents *(on page 382)*.

Important: Any user who has a valid BigFix UI account can open a forwarded report link. Access depends on possession of the link and a valid login, not on whether the user was in the original email recipient list. Forward the link only to users who are allowed to see the report data.

By default, the link stops working 30 days after the report is generated. Your administrator can change this period in the **ScheduledReportAccessTokenExpirationHours** configuration setting. See the ***BigFix UI Administration Guide***, Configuration Variables. The email shows the expiry date as **Link Expires On**. After the link expires, open the archive on the **Archives** tab of the schedule details page.

Scheduled Reports reference

Reference information for Scheduled Reports: the columns and statuses of the Scheduled Reports table and the fields of the Add schedule wizard.

Scheduled Reports table columns

Table 69. Scheduled Reports columns

Column	Description
Name	The activity name that you entered in step 4 of the wizard. Select it to open the schedule details page.
Report name	The report that the schedule runs. Select it to open the report.
ID	The numeric identifier of the schedule. The table is sorted by **ID** in descending order by default, so the newest schedule is listed first.
Status	The current state of the schedule. See Schedule statuses *(on page 381)*.

Table 69. Scheduled Reports columns (continued)

Column	Description
Creator	The user who created the schedule. The schedule runs with this user's permissions.
Start date & time	The date and time of the first run, with the time zone, for example `21 Sep 2026 at 14:58 (Client)`.
End date & time	The end condition of the schedule. For a schedule that ends after a number of runs, the computed end is shown, for example `After 10 occurrences on 30 Sep 2026 at 16:50 (Client)`. See End conditions *(on page 382)*.
Last occurrence	The date and time of the most recent run. Shows `--` if the schedule has not run yet.
Next occurrence	The date and time of the next planned run. Shows `--` if no further run is planned, for example for a paused, blocked, or expired schedule.
Archive	The number of archives that the schedule has produced, for example `0` or `1`.
Email	**Yes** or **No**, to show whether email distribution is configured for the schedule.

All dates are displayed with their time zone in brackets.

Schedule statuses

Table 70. Schedule statuses

Status	Meaning
Active	The schedule runs as configured. You must pause it before you can edit or delete it.
Paused	You suspended the schedule. No runs occur until you select **Resume**. You can edit or delete a paused schedule.
Expired	The schedule reached its end date, or it was a one-time schedule that has already run. No further runs are planned. Editing and submitting an expired schedule makes it active again.
Blocked	The schedule does not run. No last or next occurrence is shown. BigFix UI blocks a schedule in either of the following cases: • Report execution encounters integrity issues. • Three or more previous executions failed. You can edit or delete a blocked schedule.
System Paused	BigFix UI paused the schedule automatically. No runs occur until the cause is corrected. BigFix UI pauses a schedule in either of the following cases:

Table 70. Schedule statuses (continued)

Status	Meaning
	• The scheduled-report storage quota of the user who owns the schedule is exceeded. • Email delivery fails three consecutive times. You can edit or delete a system-paused schedule.

End conditions

The **End conditions** group in step 2 of the wizard sets when the schedule stops running.

Table 71. End condition options

Option	Description
Never	Default. The schedule runs indefinitely.
On	The schedule stops at a date and time that you choose. Selecting this option enables **Select date** and **End time**.
After	The schedule stops after a number of runs. Enter the number of occurrences in the stepper.

The **End date & time** column and the schedule details page show the computed end, for example `After 10 occurrences on 30 Sep 2026 at 16:50 (Client).`

Email notification contents

When a run finishes, each recipient receives an email that contains the following information.

Table 72. Email notification fields

Field	Description
Report Name	The generated report, with the execution date and time appended in UTC.
Schedule Name	The schedule activity name.
Generated On	The date and time of the run, with the time zone.
Link Expires On	The date and time after which **View Report** stops working, 30 days after generation by default. Your administrator sets this period in the **ScheduledReportAccessTokenExpirationHours** configuration setting. See Configuration Variables.
Report ID	The numeric identifier of the report.
View Report	Opens the archived report in BigFix UI.

The email footer shows the root server identifier.

Important: Any user who has a valid BigFix UI account can open a forwarded report link. Access depends on possession of the link and a valid login, not on whether the user was in the original email recipient list. Forward the link only to users who are allowed to see the report data.

Add schedule wizard fields

Table 73. Add schedule wizard fields

Step	Field	Description
1. **Selection of reports**	**Select report to schedule**	Required. The report to run. The list contains the reports on the **All Reports** page that you own and can schedule.
	Selected report properties	Read-only. **Report name**, **Tags**, **Author**, and **Last modified**.
2. **Scheduler**	**This event occurs**	Required. **Once**, **Daily**, **Weekly**, or **Monthly**.
	Time zone	Radio buttons. Select **Client** to use the time zone of the device that runs the report, or **UTC**. All schedule dates are displayed with their time zone in brackets.
	Select date	Required. The date of the first run.
	Start time	Required. The time of the first run. The actual start depends on the server queue and might be later than the selected time.
	End conditions	**Never** (default), **On**, or **After**. See End conditions *(on page 382)*.
3. **Email and storage**	**Email notifications**	Toggle. Turn on to email the generated report. Turning it on shows the email fields.
	Email subject	Optional. If empty, the default subject is used.
	Email to	Required when notifications are on. Type to find a recipient, and then select **Add**. Each recipient is shown as a removable chip. Select the clear (**X**) control to empty the input. The maximum is 50 recipients by default (**EmailMaxIndividualRecipients**, see Configuration Variables). For the contents of the notification, see Email notification contents *(on page 382)*.
	Notify the administrator about this schedule	Check box. Also sends the notification to the administrator. The preview shows this setting as **Notification to admin**.
	Body text (Optional)	Optional. If empty, the default body text is used.
	Retention	Toggle. Turn on to set how long each archived report is kept. In this release, archives are always kept for 3 months, regardless of this setting.

Table 73. Add schedule wizard fields (continued)

Step	Field	Description
	By duration	The retention period counted from the creation of each archive, for example **1 month**. In this release, the selected period is not applied; archives are kept for 3 months.
4. **Preview schedule**	**Add schedule activity name (Mandatory)**	Required. The name that is shown in the **Name** column and in the schedule details page header.
	Report details	Read-only summary of step 1. Includes **Visibility** (**Private** or **Public**).
	Time constraints & occurrences	Read-only summary of step 2: **Start date & time slot**, **End date & time**, and **Occurs**, for example **Occurs Once at 07:20 PM**.
	Email	Read-only summary of the notification settings.
	Retention	Read-only summary of the retention period, for example **Retain archives for: 1 month**.

Report Builder

The Report Builder is a wizard-based feature that you use to create visual reports from the data available in your BigFix environment. You can start from a pre-built template or build a report from scratch with full manual control.

To open the Report Builder, expand **Reporting** in the side navigation, and then select **Report Builder**.

Before you begin

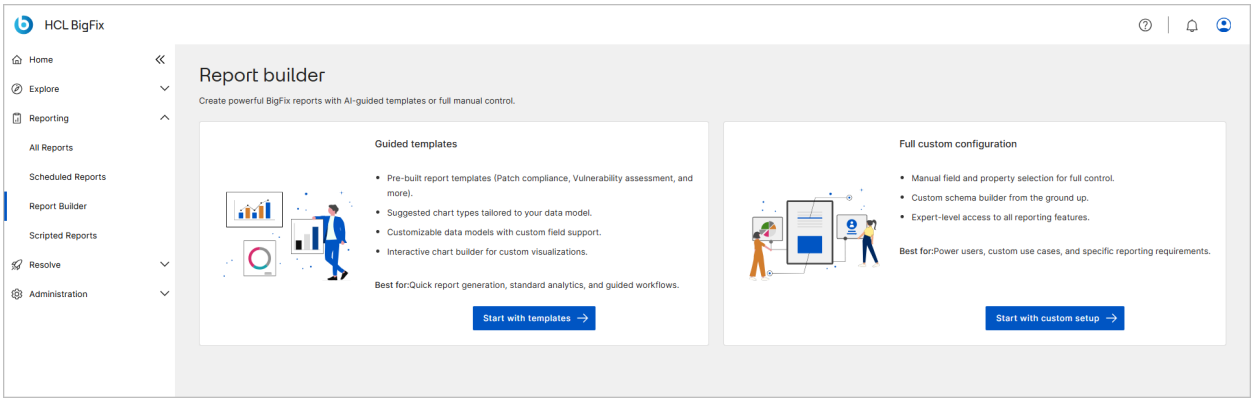
Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to the Reports application, and your access level (**Admin**, **Users**, or **Read only**) determines what you can do here. See Managing Roles *(on page 467)*.
- The data sets and visualization options that are available depend on your permissions and on the data sources configured for the UI. For a description of each permission, see Permissions reference *(on page 482)*.

Ways to create a report

The **Report builder** page presents two cards. Each card starts a different report creation method:

- **Guided templates** – Start from a pre-built report template, customize its data model, and choose a variation. Select **Start with templates**.
- **Full custom configuration** – Select the data set, properties, and chart widgets yourself. Select **Start with custom setup**.



Guided templates

A guided template is a pre-built report definition that you customize instead of building a report from scratch. Each template supplies a data model, suggested fields, and a set of variations that narrow the report to a specific focus. The **Guided templates** card offers:

- Pre-built report templates, such as patch compliance and vulnerability assessment.
- Suggested chart types that suit the data model.
- Customizable data models with custom field support.
- An interactive chart builder for custom visualizations.

This method is best for quick report generation, standard analytics, and guided workflows.

When you select **Start with templates**, the **Report templates** page lists the templates that are available to you. After you select a template, the wizard creates the report in three steps: **Customize**, **Variations**, and **Preview**.

For a description of the templates page and the wizard steps, see Guided templates *(on page 388)*. For the procedure, see Create a report from a template *(on page 389)*.

Full custom configuration

Full custom configuration gives you manual control over every part of the report. The **Full custom configuration** card offers:

- Manual field and property selection for full control.
- A custom schema builder from the ground up.
- Expert-level access to all reporting features.

This method is best for power users, custom use cases, and specific reporting requirements.

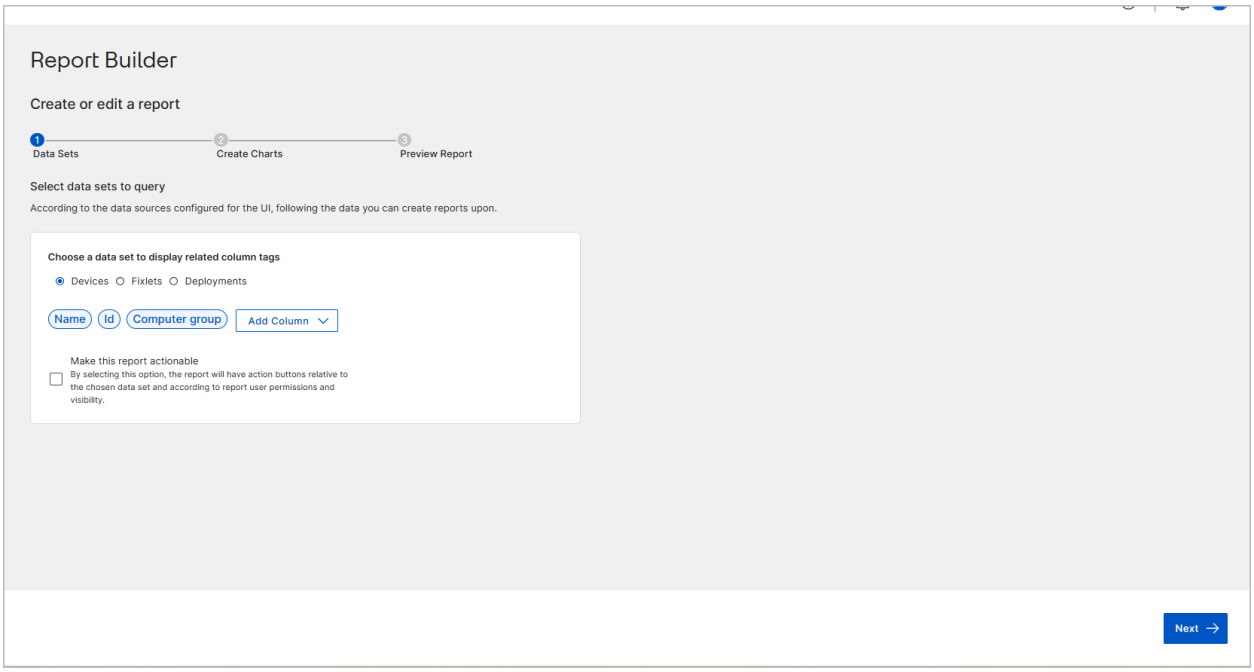
When you select **Start with custom setup**, the Report Builder creates a report in a three-step process:

- **Data Sets** – Choose the source data set and the properties that you want to include in your report.
- **Create Charts** – Design one or more visualization widgets based on the selected properties.
- **Preview Report** – Enter a name and description, review the final layout, and generate the report.

For the procedure, see Create a report with custom configuration *(on page 397)*.

Data sets

Each data set corresponds to a data category within BigFix. The data set that you select in the **Data Sets** step determines which columns, filters, and data types are available in your report:



- **Devices** – Data related to managed endpoints, such as hostname, IP addresses, and operating system.
- **Fixlets** – Information about Fixlets, tasks, and baselines.
- **Deployments** – Details about deployment operations, targets, and results.

The **Name**, **Id**, and **Computer group** columns are included by default and cannot be removed.

For the complete list of properties that you can add as report columns for each data set, see Report Builder settings reference *(on page 413)*.

Chart widgets

The **Create Charts** step provides four widget categories, or five when the selected columns include DEX properties:

- **Distribution over time** – Displays how a DEX property changes over a selected time range, as a vertical bar or line chart. This widget category is available only when the selected columns include DEX properties, such as Dex Score or Dex Device Score. Set the reporting period with **Time range**. On the **Preview Report** step, you can also categorize the metric with **Group By** and change the aggregation interval with the **View by** list. See Working with Distribution over time charts *(on page 407)*.
- **Percentage of a whole** – Displays proportional data as a donut, gauge, or pie chart.
- **Quick link** – Displays a KPI as a link to a filtered view of the data. The link label is the count of the elements that match the filter criteria that you define.
- **Composition** – Displays how values compose a whole as a horizontal bar, pie, treemap, or vertical bar chart.
- **Category breakdown** – Shows how the values of a second property are distributed within each value of a first property, as a grouped or stacked bar chart with horizontal or vertical orientation. For example, Agent type broken down by Operating system.

For the visual formats and configuration settings of each widget category, see Report Builder settings reference *(on page 413)*.

Chart data table

Every chart provides a **See data in data table format with download options** icon in its upper-right corner, which opens the chart data as a table that you can copy or export. This control works the same way across BigFix UI. See Viewing chart data in a table *(on page 33)*.

For a **Distribution over time** chart, the table additionally provides the **Aggregated data** and **Details by (Historical property)** tabs. See Working with Distribution over time charts *(on page 407)*.

Report management

When you generate a report, it is automatically added to the **All Reports** page, where you can mark it as a favorite, set its visibility to **Public** or **Private**, reconfigure it, or delete it.

To open a report, select its name on the **All Reports** page. On the report details page, you can:

- Refresh the report data.
- Filter the report. See Global filter *(on page 36)*.
- Limit the report to selected device groups with **View by group**. This list is displayed only for reports that were created from a guided template.
- Export the report data. See Exporting Data *(on page 30)*.
- Duplicate the report. See Duplicate a report *(on page 406)*.
- Reconfigure the report. See Reconfigure a report *(on page 404)*.

Filtering and exporting behave the same way as they do elsewhere in BigFix UI. For more information, see Global filter *(on page 36)* and Exporting Data *(on page 30)*.

Note: The data sets and visualization options that are available depend on your user permissions and the data sources configured for the UI.

Related information

Guided templates *(on page 388)*

Create a report from a template *(on page 389)*

Create a report with custom configuration *(on page 397)*

Reconfigure a report *(on page 404)*

Global filter *(on page 36)*

Duplicate a report *(on page 406)*

Exporting Data *(on page 30)*

Report Builder settings reference *(on page 413)*

Guided templates

Guided templates are pre-built report definitions that you customize instead of building a report from scratch. Each template supplies a data model, suggested fields, and a set of variations that narrow the report to a specific focus.

To use a guided template, open the Report Builder and select **Start with templates** on the **Guided templates** card. The **Report templates** page lists the templates that are available to you.

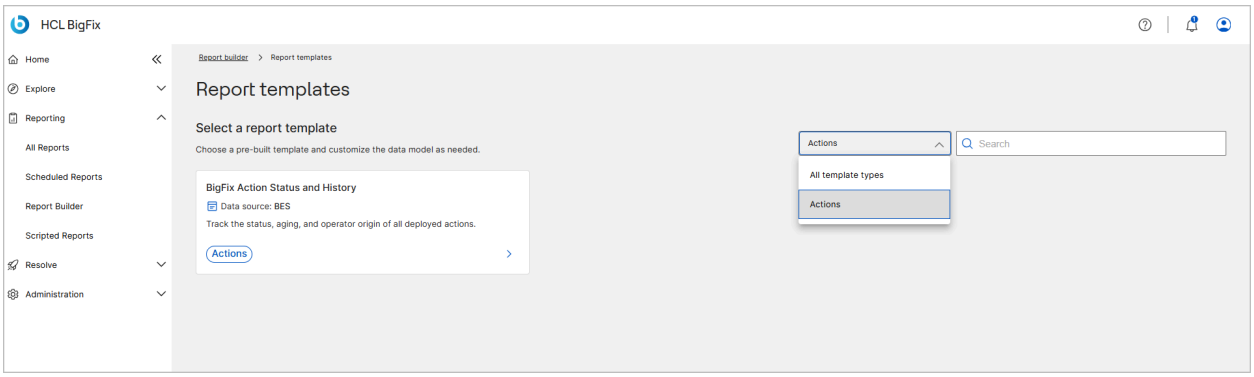
Guided templates are best for quick report generation, standard analytics, and guided workflows. If you need full manual control over the data set, properties, and chart widgets, use the full custom configuration method instead. See Full custom configuration *(on page 385)*.

For the procedure, see Create a report from a template *(on page 389)*.

Report templates page

Each template card shows the template name, the data source that supplies the data (for example, BES), a short description of what the report tracks, and a template type chip such as **Operations**, **Security**, **Compliance**, **Inventory**, or **Actions**.

To narrow the list, select a type from the template type dropdown list, which is set to **All template types** by default, or enter text in the **Search** field.



Template wizard steps

After you select a template, the wizard creates the report in three steps:

- **Customize** – Review the base fields of the template, add optional properties to the data model, and choose whether the report is actionable. The **Schema overview** shows the number of base fields, and the collapsible **Data model** section shows the total number of fields in the schema definition.
- **Variations** – Choose a sub-template that narrows the report to a specific focus, such as an age range, a state, or an operator type. The number of available variations is displayed on the right of the step, for example **17 available**.
- **Preview** – Review the resulting content list, adjust the columns and the row density, search the list, build a filter, export the data, and save the report with a name and description.

A breadcrumb trail at the top of the page shows **Report builder** > **Report templates** > **Create report**. Use it to return to an earlier page at any point in the wizard.

Note: The templates and variations that are available depend on your user permissions and the data sources configured for the UI.

Related information

Create a report from a template *(on page 389)*

Report Builder *(on page 384)*

Report Builder settings reference *(on page 413)*

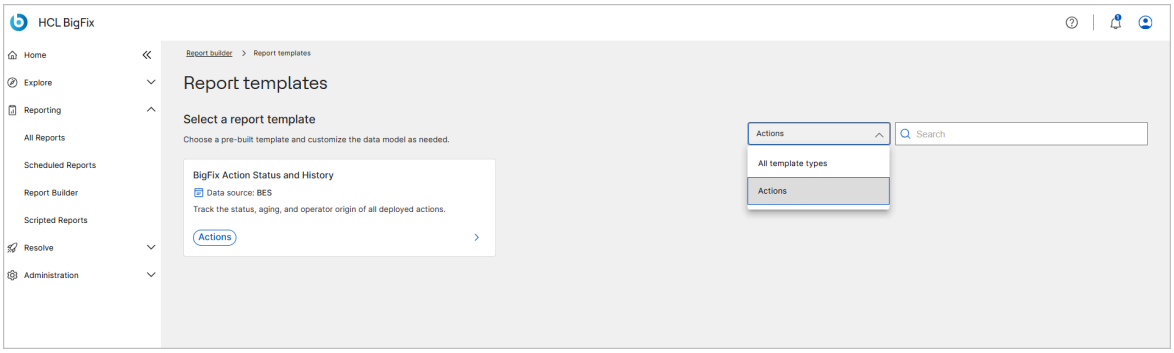
Create a report from a template

Use a guided template to create a report: customize the data model of a pre-built template, choose a variation, and save the report.

The templates, variations, and properties that are available depend on your user permissions and the data sources configured for the UI.

The template wizard guides you through three steps: **Customize**, **Variations**, and **Preview**.

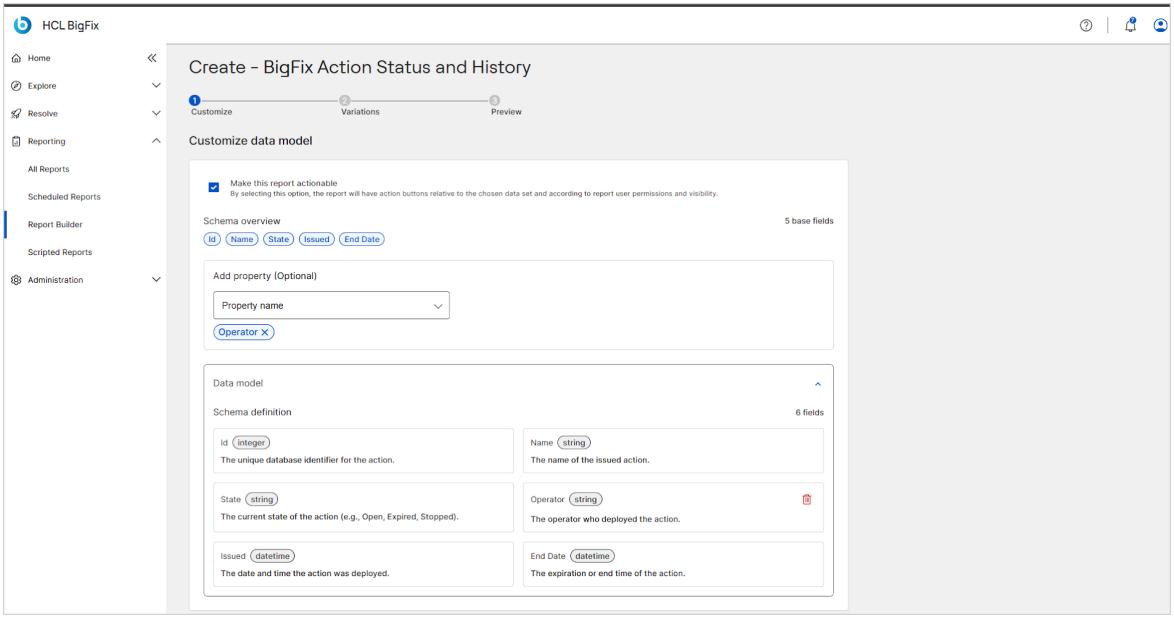
1. Expand **Reporting** in the side navigation, and then select **Report Builder**.
2. On the **Guided templates** card, select **Start with templates**.
   The **Report templates** page opens and lists the available templates.
3. Optional: To narrow the list, select a type from the template type dropdown list or enter text in the **Search** field.



4. Select the template that you want to use.
   The **Create** page opens at the **Customize** step and displays the data model of the template.
5. Optional: Select **Make this report actionable** to add action buttons to the report.
   The action buttons that are displayed depend on the chosen data set and on the permissions and visibility of the report user.
6. Review the base fields of the template under **Schema overview**.

   The base fields are included in every report that is created from the template and cannot be removed. The number of base fields is displayed on the right of **Schema overview**.

   Expand the **Data model** section to view the full **Schema definition**. The number of fields in the schema is displayed on the right of the section. Each field shows its data type, such as **string**, **integer**, **number**, **datetime**, **content**, or **boolean**, and a description.



7. Optional: To add more fields to the report, select the **Property name** dropdown list under **Add property (Optional)**.

    a. Use the search field to locate properties quickly.

    b. Select the check box of each property that you want to add.

    Note: You can add a maximum of 16 optional properties.

    c. Optional: Select **Reset** to clear all selected properties.

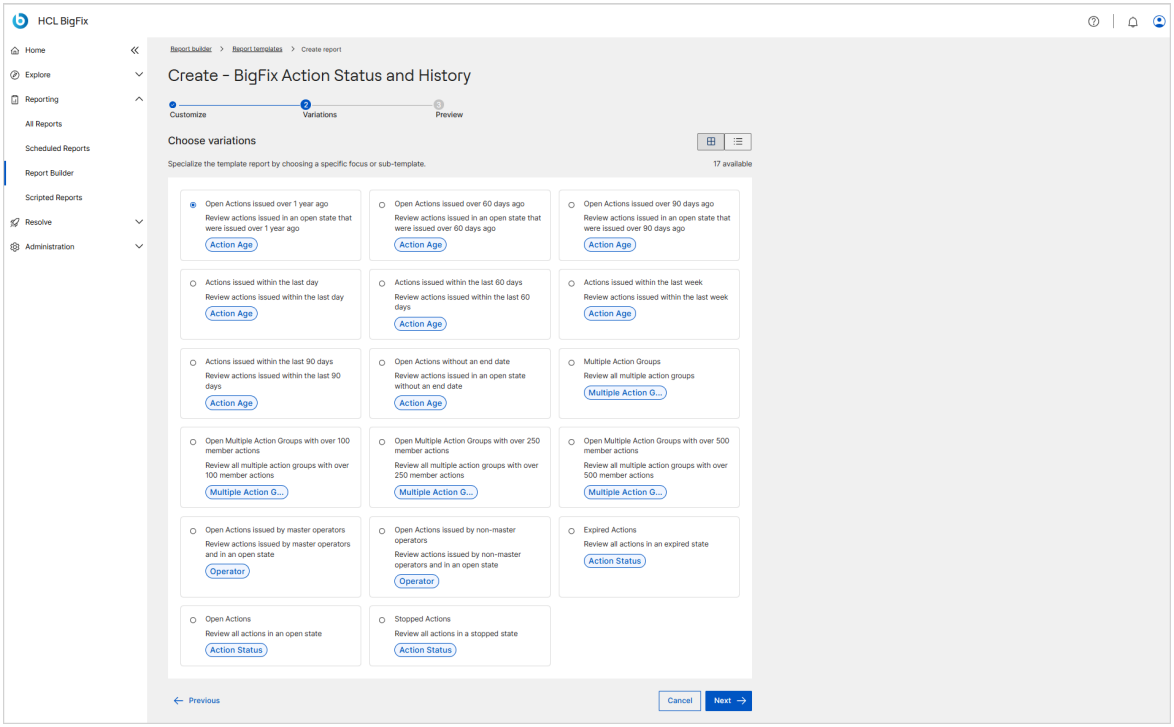
    d. Select **Apply**.
    The selected properties appear as tags under **Add property (Optional)** and as fields in the **Data model** section.

8. Optional: To remove an optional property, select the delete icon on its field in the **Data model** section, or select the remove icon on its tag.

9. Select **Next**.
The **Variations** step opens and lists the available variations of the template.

10. Select the variation that matches the focus that you want to report on.

    Each variation card shows a name, a description, and a category chip, such as **Action Age**, **Action Status**, **Multiple Action Groups**, or **Operator**. The number of available variations is displayed on the right of the page. Select the grid or list icon in the upper-right corner to change how the variations are displayed.

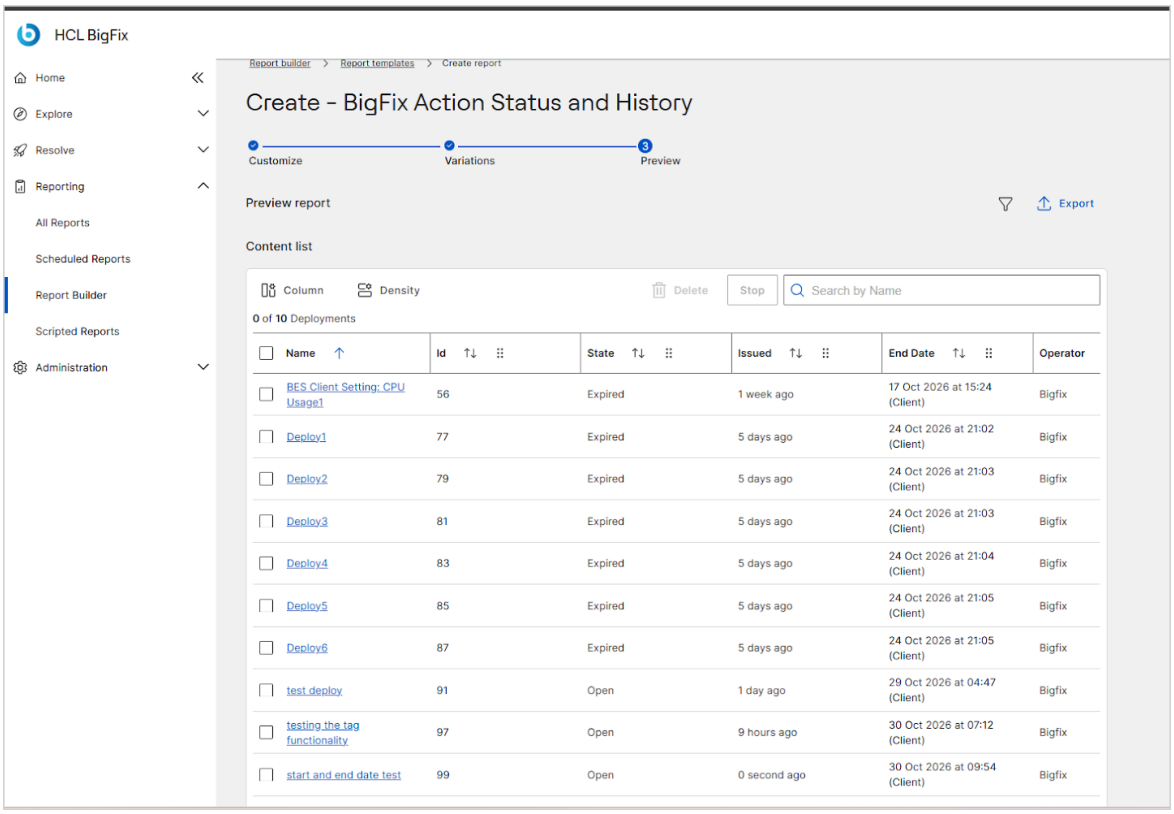


11. Select **Next**.

    The **Preview** step opens and displays the **Content list** with the data that the report returns.

12. Review the report data in the **Content list**.

    You can use the column headers to sort the data. The number of selected rows and the total number of rows are displayed above the table.



13. Optional: Use the **Content list** toolbar to change how the data is displayed.
    - Select **Column** to show or hide columns.
    - Select **Density** to change the row height.
    - Use the **Search by Name** field to find a specific row.

    If the report is actionable, select the check box of one or more rows to enable the action buttons, such as **Delete** and **Stop**.

14. Optional: To refine the data, select the filter icon in the upper-right corner of the page.

    The **Filter** panel opens on the **Current filter** tab and displays **Create new filter**.

    a. In **Filter block 1**, define **Condition 1**: select a **Property**, select an **Operator**, and enter a **Value**.
    The **Operator** list and the **Value** field become available after you select a property.

    b. Optional: Select **Add Condition** to add another condition to the same block.

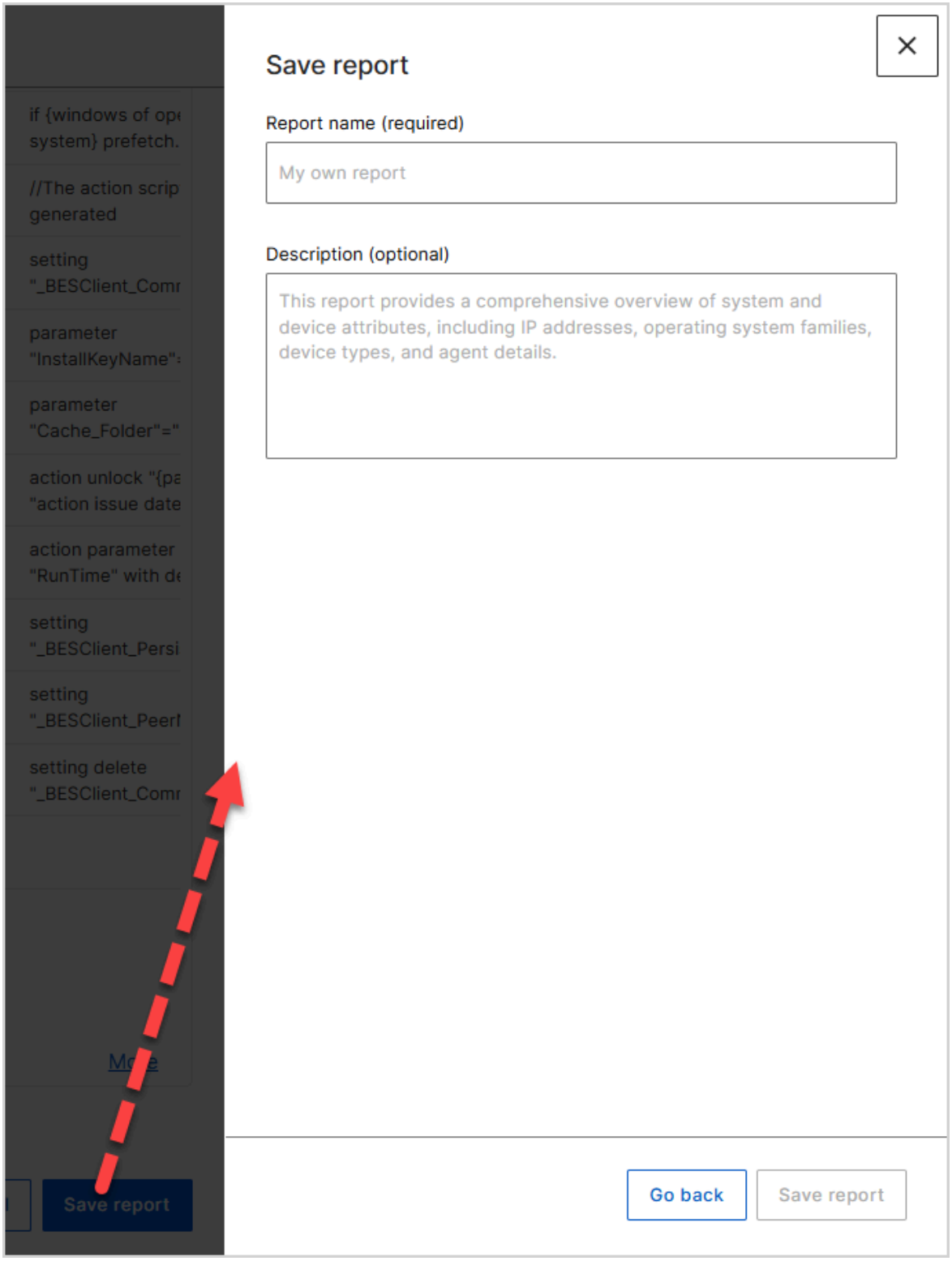
    c. Optional: Select **Add Block** to add another filter block.

    d. Optional: Select **Remove block** to delete a single block, or **Remove All** to delete all blocks.

    e. Select **Apply Filter**.
    The **Content list** displays only the rows that match the filter.

15. Optional: To download the data, select **Export**.
    In the **Export** panel, select the **CSV** check box, the **Excel** check box, or both, and then select **Download**. For more information, see Exporting Data *(on page 30)*.

16. Select **Save report**.
    The **Save report** panel opens.

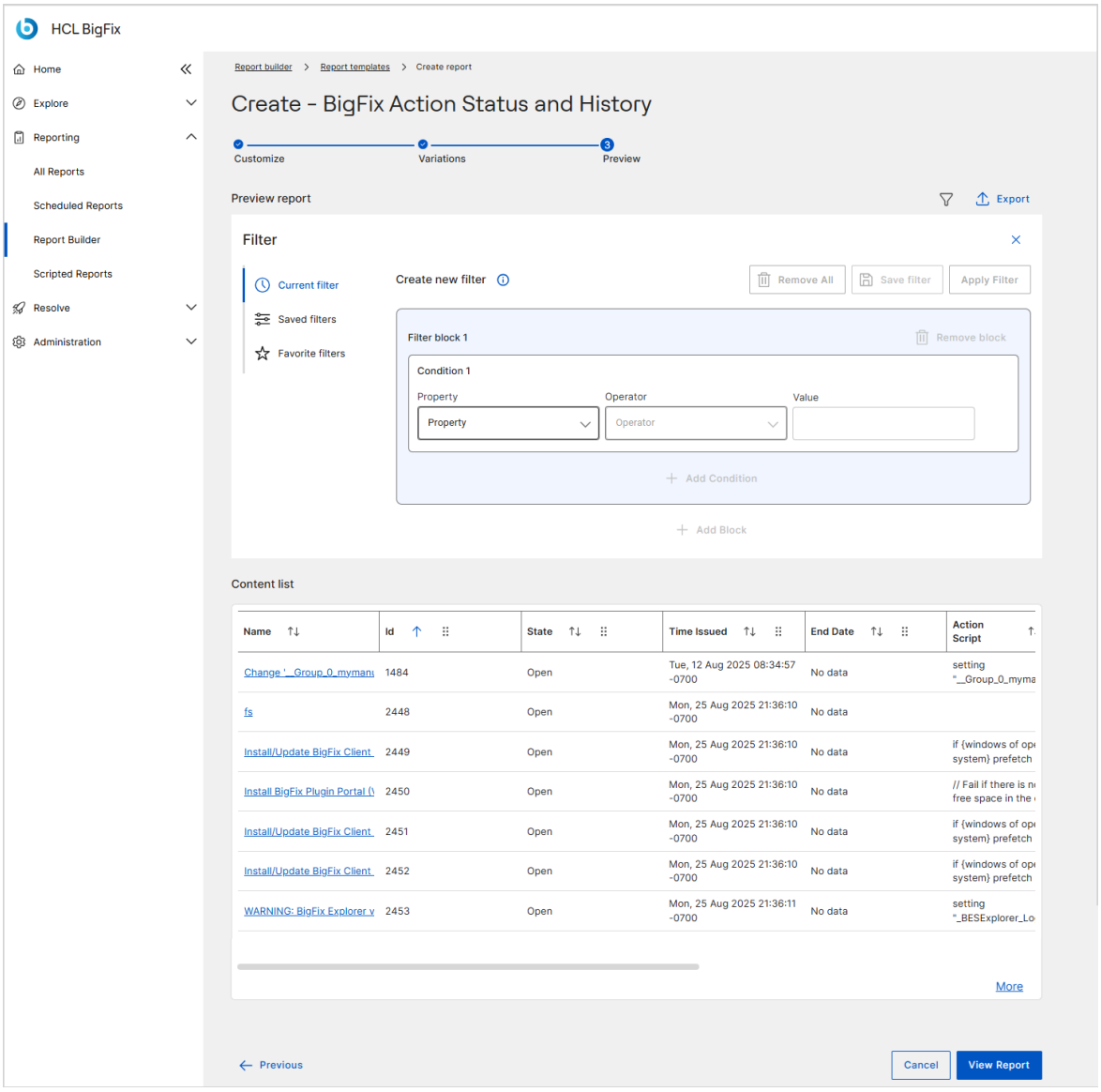


17. Enter a **Report name** and, optionally, a **Description**.

Note: The report name is required. To return to the preview without saving, select **Go back**.

18. Select **Save report**.
    A success message "Congratulations! You have successfully created a new report" appears in the upper-right corner of the UI.

19. Select **View Report**.



The **Save report** button is replaced by **View Report** after the report is saved.
The report is added to the **All Reports** page.

To change a saved report, reconfigure it from the report details page. See Reconfigure a report *(on page 404)*.

Create a report with custom configuration

Use the Report Builder wizard to select a data set, design chart widgets, and generate a custom report. Use this method when you want full manual control over the properties and charts in the report.

The data sets and visualization options that are available depend on your user permissions and the data sources configured for the UI.

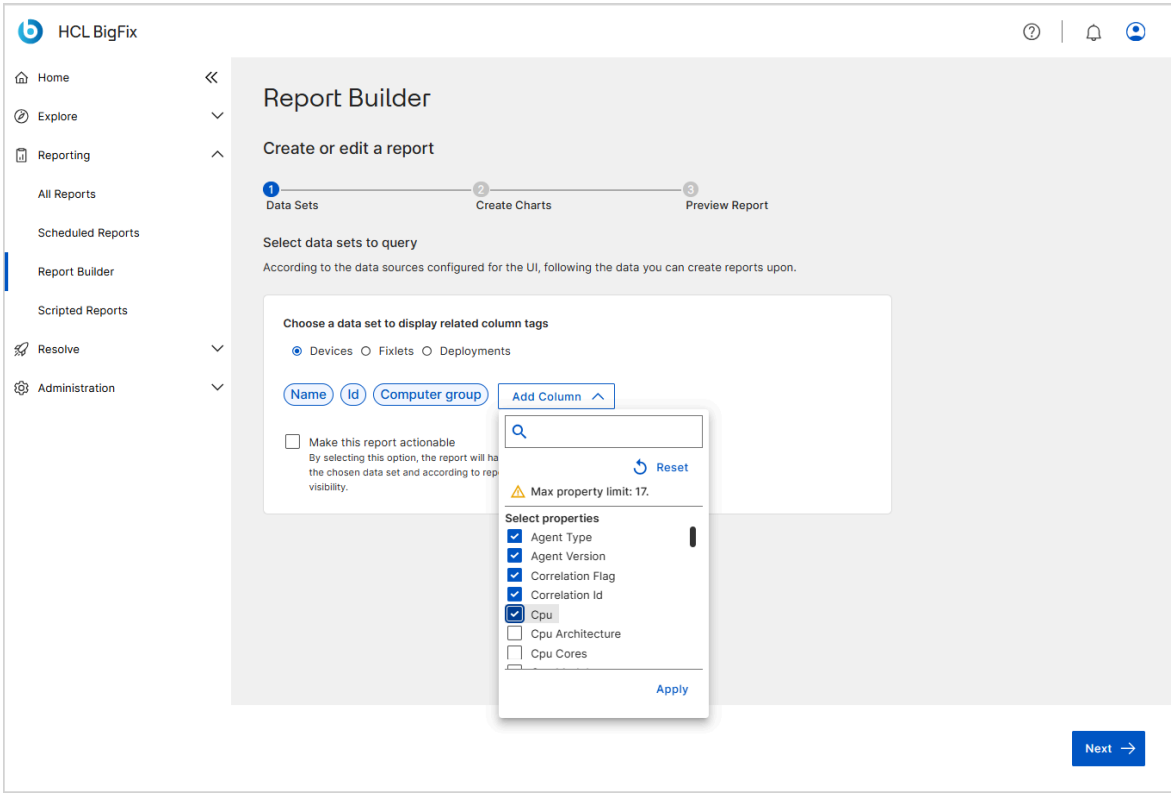
The Report Builder guides you through three steps: **Data Sets**, **Create Charts**, and **Preview Report**.

1. Expand **Reporting** in the side navigation, and then select **Report Builder**.
2. On the **Full custom configuration** card, select **Start with custom setup**.
   The **Data Sets** step opens.
3. Under **Choose a data set to display related column tags**, select one data set: **Devices**, **Fixlets**, or **Deployments**.

   For the properties available in each data set, see Report Builder settings reference *(on page 413)*.

   Note: The **Name**, **Id**, and **Computer group** columns are included by default and cannot be removed.

4. Select **Add Column** to open the property selection panel.



a. Use the search field to locate properties quickly.

b. Under **Select properties**, select the check box of each property that you want to include as a report column.

Note:

- Only the columns that you select in this step appear in the property dropdown lists during chart creation.
- You can select up to a maximum property limit of 18.

c. Optional: Select **Reset** to clear all selected properties.

d. Select **Apply** to confirm your selections.
The selected properties appear as column tags next to **Name**.

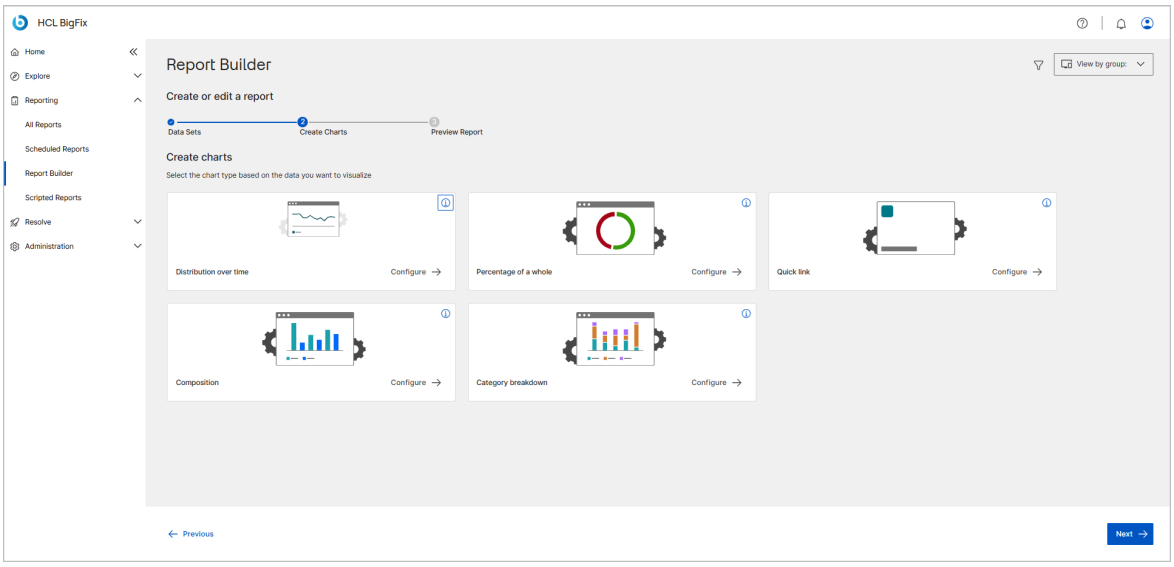
5. Optional: Select **Make this report actionable** to add action buttons to the report.
The action buttons that are displayed depend on the chosen data set and on the permissions and visibility of the report user.

6. Select **Next** to continue to the **Create Charts** step.

7. On the **Create Charts** page, select **Configure** on the card of each widget type that you want to add: **Distribution over time**, **Percentage of a whole**, **Quick link**, **Composition**, or **Category breakdown**.

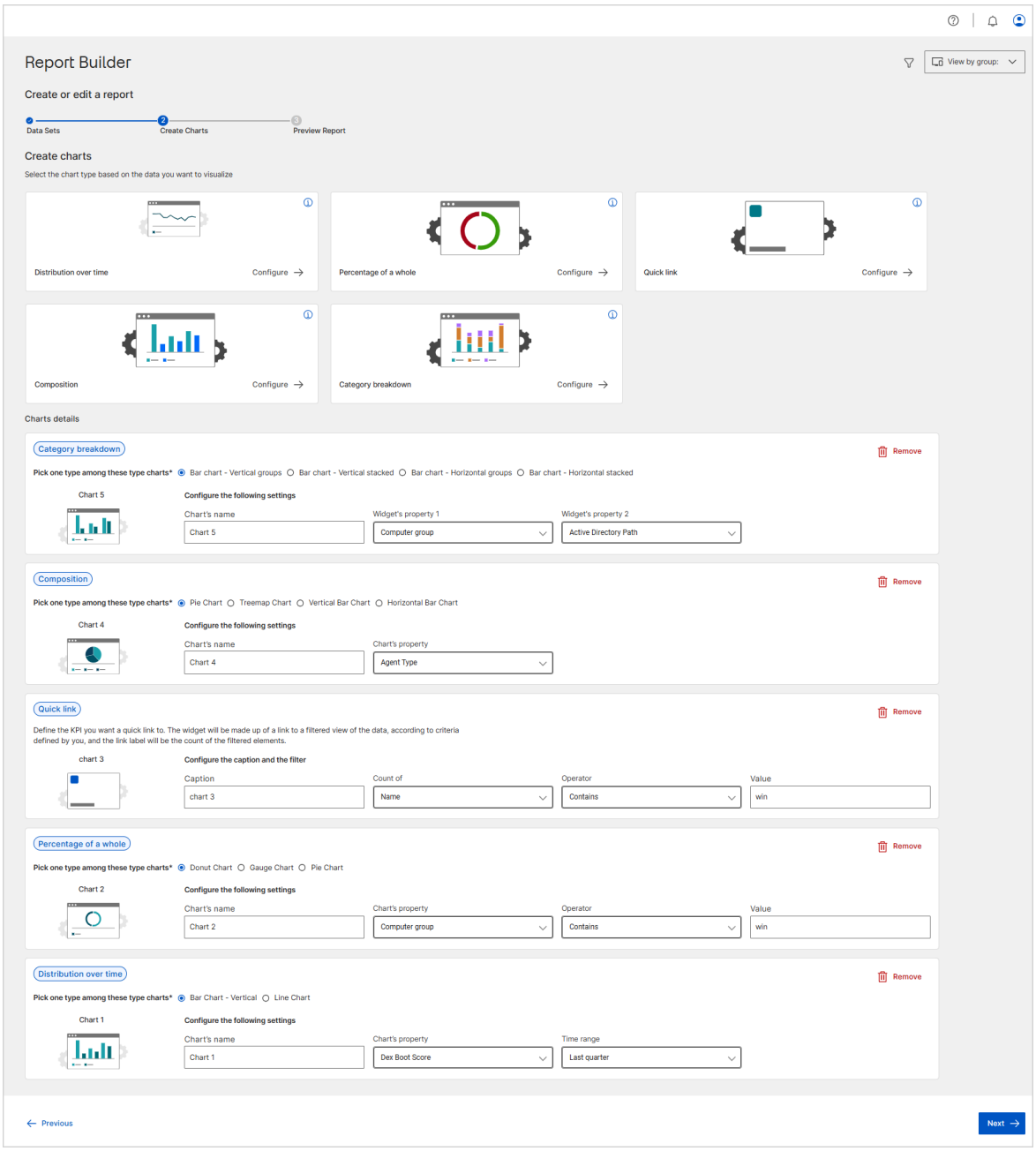
Each widget that you configure is added to the **Charts details** list. Newly added widgets appear at the top of the list.

Note: The page displays four widget cards. The **Distribution over time** card is displayed as a fifth card only when the columns that you selected in the **Data Sets** step include DEX properties, such as Dex Score or Dex Device Score.



8. In each configuration panel under **Charts details**, select the visual format next to **Pick one type among these type charts**, and then complete the settings.

   The settings differ by widget category. For the complete list of visual formats and settings, see Report Builder settings reference *(on page 413)*.



Note: The property dropdown lists display only the columns that you selected in the **Data Sets** step.

a. For a **Distribution over time** chart, select **Bar Chart - Vertical** or **Line Chart**, and then enter a **Chart's name**, select the DEX property to visualize in **Chart's property**, and select a **Time range**.

   The **Time range** list provides **Last month**, **Last quarter**, **Last year**, **Current month** (the default), **Current quarter**, **Current year**, and **Custom**. Select **Custom** to set the start and end dates in the calendar.

Note: The **Chart's property** list displays only the DEX properties that you selected in the **Data Sets** step.

For the grouping and interval controls that this chart provides on the **Preview Report** step, see Working with Distribution over time charts *(on page 407)*.

b. For a **Percentage of a whole** chart, select **Donut Chart**, **Gauge Chart**, or **Pie Chart**, and then enter a **Chart's name** and select a **Chart's property**, an **Operator**, and a **Value**.
The chart shows the proportion of records that match the operator and value that you define, against the rest of the records.

c. For a **Quick link** widget, enter a **Caption** and select a **Count of** property, an **Operator**, and a **Value**.
The widget displays the count of the matching elements as a link to a filtered view of the data, with the caption below the count.

d. For a **Composition** chart, select **Horizontal Bar Chart**, **Pie Chart**, **Treemap Chart**, or **Vertical Bar Chart**, and then enter a **Chart's name** and select a **Chart's property**.
The chart groups the records by the values of the selected property and shows the count of each value.

e. For a **Category breakdown** chart, select **Bar chart - Horizontal groups**, **Bar chart - Horizontal stacked**, **Bar chart - Vertical groups**, or **Bar chart - Vertical stacked**, and then enter a **Chart's name** and select **Widget's property 1** and **Widget's property 2**.

Widget's property 1 sets the categories on the primary axis. **Widget's property 2** sets how the records in each category are broken down, shown as groups or stacked segments in the legend.

Note: Records with no value for the selected property are shown as N/A.

9. Optional: To delete a widget configuration, select **Remove** in the upper-right corner of its panel.
10. Optional: To refine the data displayed in the report, select the filter icon in the upper-right corner of the page. The **Filter** panel provides the **Current filter**, **Saved filters**, and **Favourite filters** tabs. For detailed steps, see Global filter *(on page 36)*.
11. Optional: To limit the report to specific device groups, select **View by group** in the upper-right corner of the page, select the check box of each group, and then select **Apply**.

    In the **Select Device group** list, you can search for a group, select **Select all**, or select **Reset** to clear your selection.

    Note: The **View by group** list is available on the **Create Charts** and **Preview Report** steps. On the report details page, it is displayed only for reports that were created from a guided template.

12. Select **Next** to continue to the **Preview Report** step.

    Note: The **Next** button remains disabled until you provide all the required chart information. For example, the button remains disabled if two charts have the same name.

13. In the **Configure Report Properties** section, enter a report **Name** and, optionally, a **Description** that summarizes the report's purpose.

    Note: The **Generate Report** button stays dimmed until you enter a name.

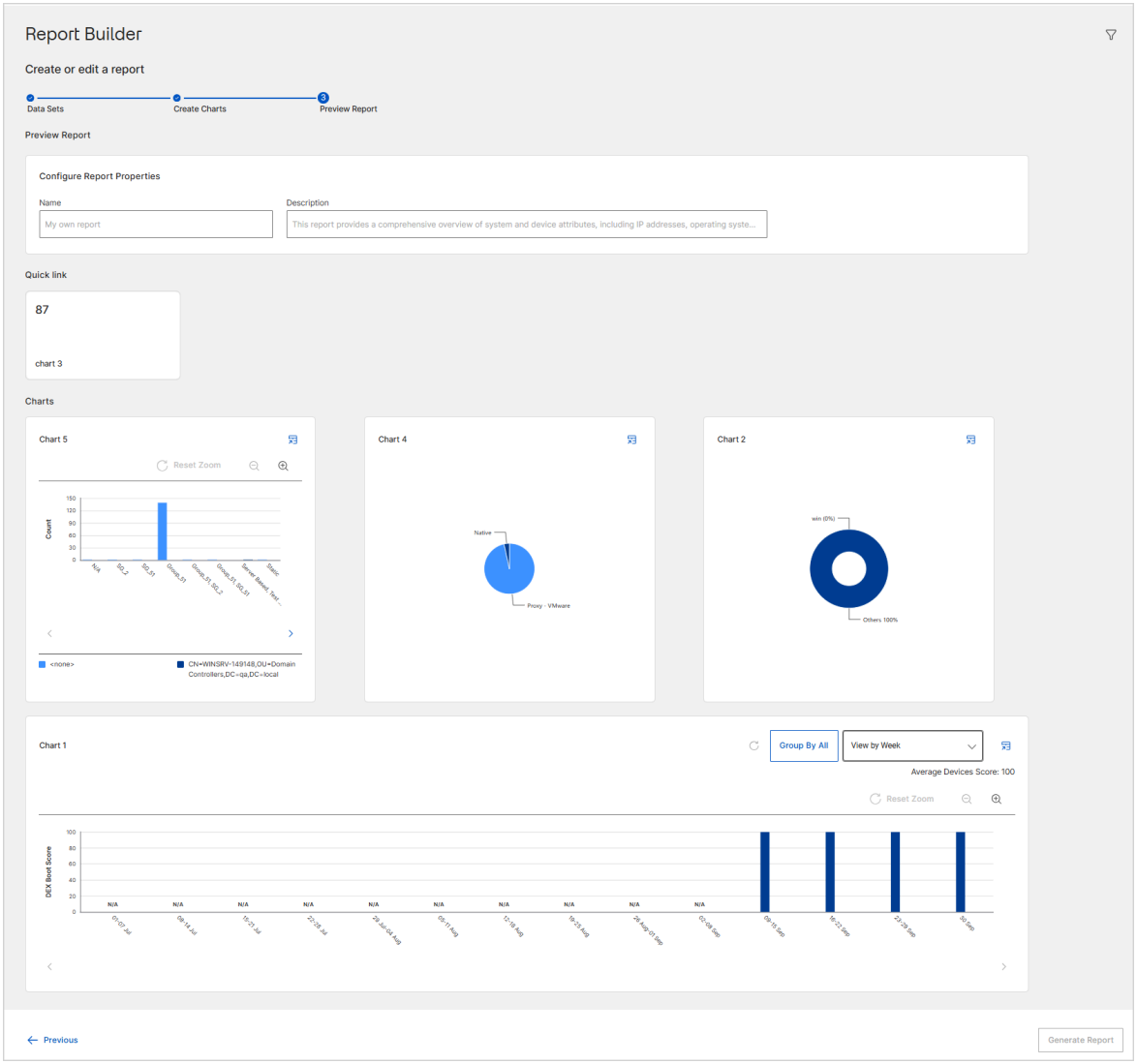
14. Verify that the report content appears correctly.

    The preview page displays the following sections:

    - **Quick link** – Displays each configured quick link widget with the count of matching elements and its caption.
    - **Charts** – Displays a visual preview of the configured charts, with the chart name in the upper-left corner and the **See data in data table format with download options** icon in the upper-right corner. In a bar chart, you can zoom in, zoom out, and select **Reset Zoom**. Where a chart has more values than it can display at one time, use the arrows below the chart to page through them.
    - **Content list** – Displays a preview of the report columns and sample data rows. You can use the column headers to sort the data, and select **More** to load more rows.

    Note: If the report includes a **Distribution over time** chart, the **Content list** is not displayed for any of the charts in the report.

    A **Distribution over time** chart provides additional controls in its header: a refresh icon, the **Group By** button, the **View by** list, and the **Average Devices Score** benchmark. See Working with Distribution over time charts *(on page 407)*.



15. Optional: To review the values behind a chart, select the **See data in data table format with download options** icon in the upper-right corner of the chart.

    The chart data opens as a table that you can sort, copy, or export. For the steps, see Viewing chart data in a table *(on page 33)*.

    Note: For a **Distribution over time** chart, the table also provides the **Aggregated data** and **Details by (Historical property)** tabs and its own **View by** list. See Working with Distribution over time charts *(on page 407)*.

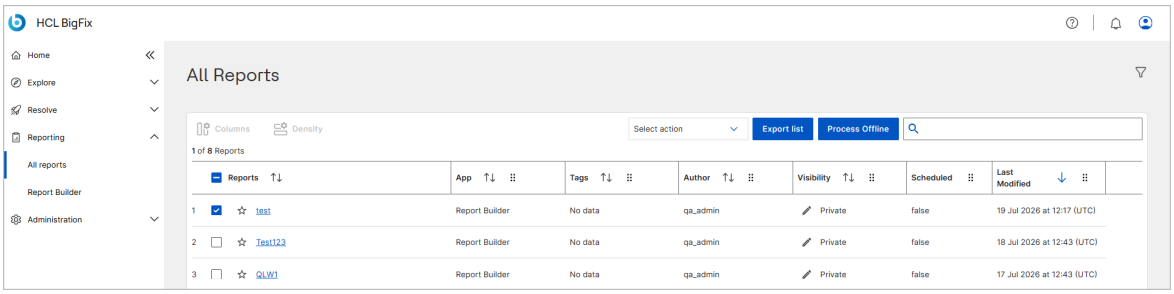
16. Select **Generate Report**.

    A success message "Congratulations! You have successfully created a new report" appears in the upper-right corner of the UI. The page stays on the **Preview Report** step, and **Generate Report** is replaced by **View Report**.

17. Select **View Report**.

    The report is added to the **All Reports** page, where you can:

    - Mark the report as a favorite with the star icon
    - Change its visibility between **Public** and **Private** with the edit icon in the **Visibility** column
    - Assign tags, change the visibility of several reports at a time, or delete reports from the **Select action** list
    - Select the report name to open the report details page, where you can reconfigure the report



To modify a saved report, reconfigure it from the **All Reports** page. See Reconfigure a report *(on page 404)*.

Reconfigure a report

Reconfigure an existing custom report to update its data sets, charts, or filters.

You must start the edit from the **All Reports** page. You cannot open a report for editing directly from the **Report Builder** menu.

Note:

- You can edit or delete saved reports anytime under **Reporting** > **All Reports**.
- The data sets and visualization options that are available depend on your user permissions and configured data sources.

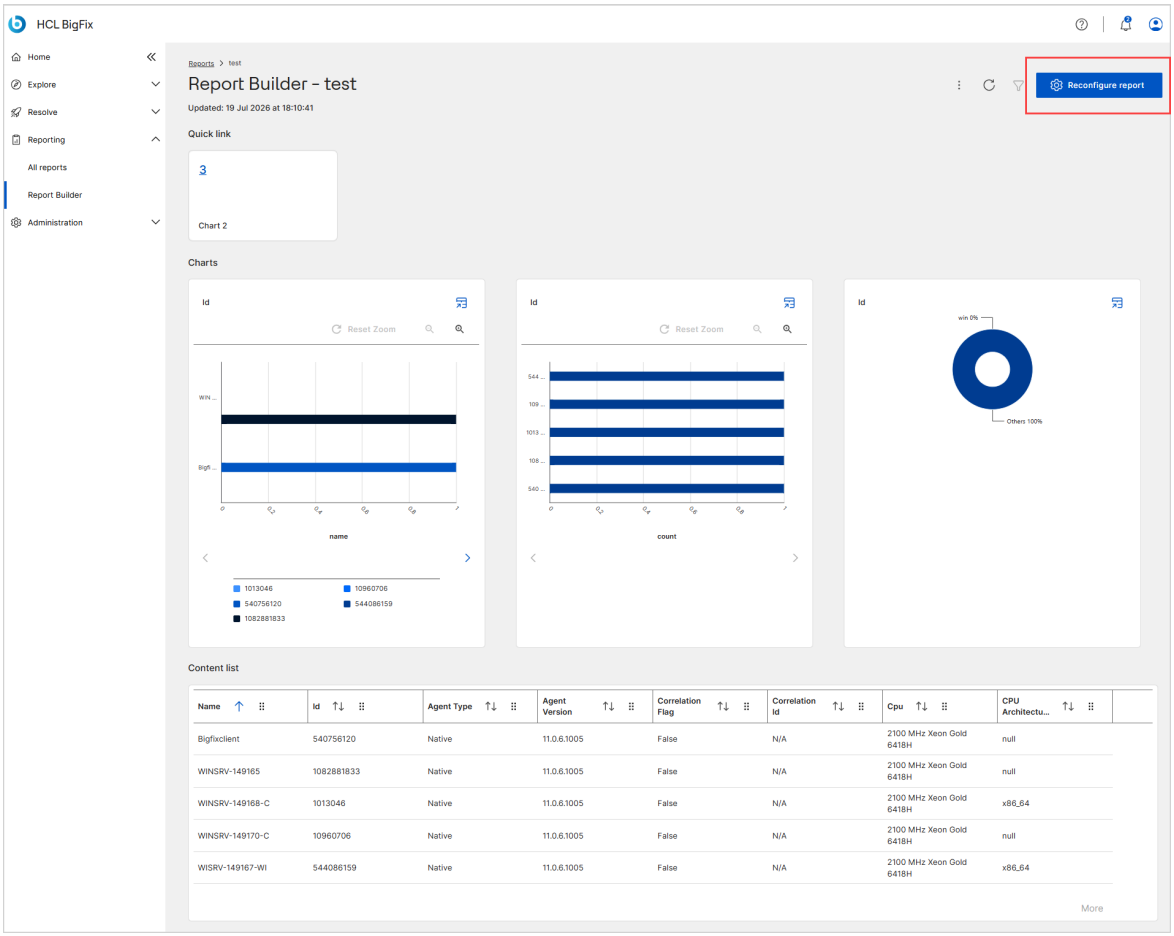
1. Go to **Reporting** > **All Reports**.
2. Select the name of the report that you want to modify.

   The report details page opens. It displays the report content, the time when the report was last updated, and the **Reconfigure report** button in the upper-right corner.

   The sections that are displayed depend on how the report was created. A report that you built with full custom configuration displays the **Quick link** and **Charts** sections that you configured, followed by the **Content list**. A report that you created from a guided template displays only the **Content list**.

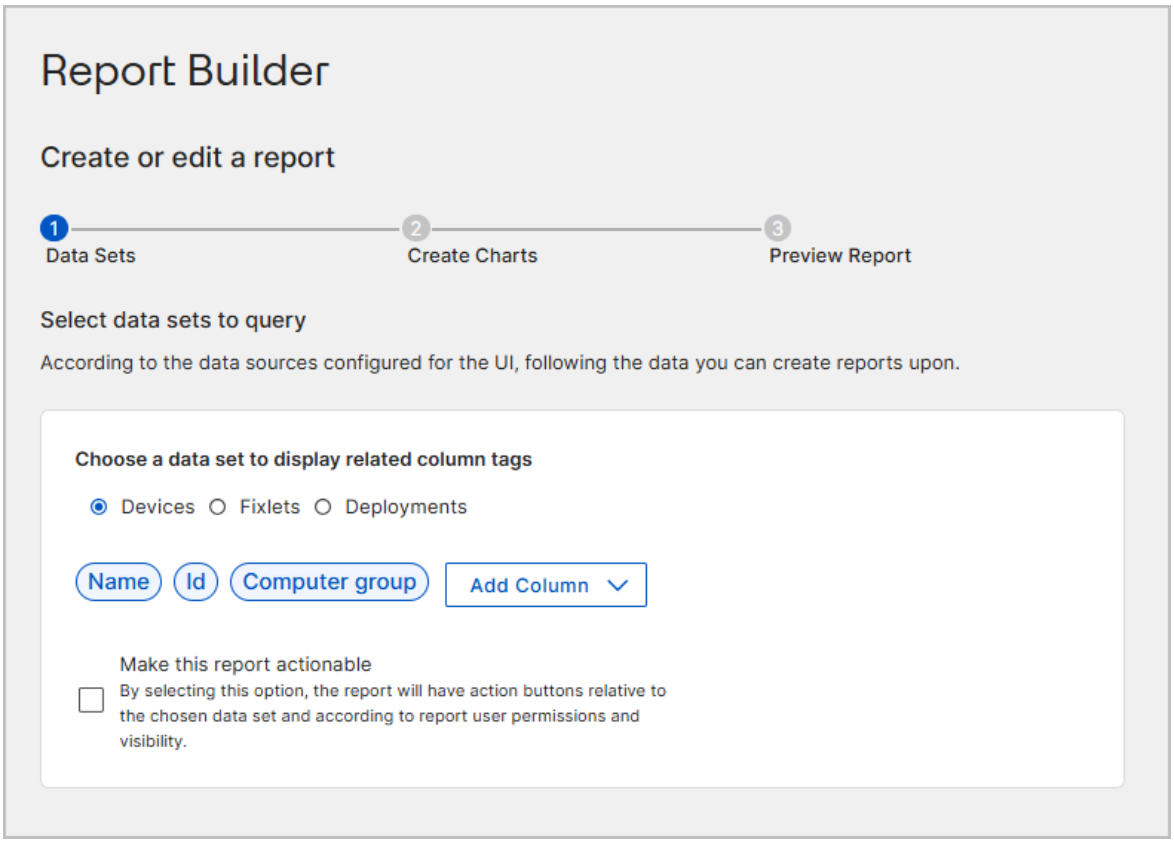
The toolbar next to the **Reconfigure report** button also provides a refresh icon, a filter icon, and a more options icon that contains the **Export** and **Duplicate report** actions. For these actions, see Global filter *(on page 36)*, Exporting Data *(on page 30)*, and Duplicate a report *(on page 406)*.

Note: The **View by group** list is displayed only for reports that were created from a guided template. Use it to limit the report to the selected device groups. See Create a report from a template *(on page 389)*.



3. Select **Reconfigure report**.

   The Report Builder opens in edit mode and displays your existing configuration.



4. To modify your data set, go to the **Data Sets** step and select **Add Column** to open the property selection panel.

    a. Select a check box to add a new property.

    b. Clear a check box to remove an existing property.

    Note: You cannot remove a property from the data set if a chart or filter currently uses it. Remove or reconfigure the associated chart or filter first.

5. Go through the **Create Charts** and **Preview Report** steps to update your widgets, filters, or report details.

6. Select **Update Report** on the preview page to save your changes.

Duplicate a report

Create a copy of an existing report to use as the starting point for a new report.

Duplicating a report keeps the original report unchanged. Reconfigure the copy to adjust its data set, charts, or filters.

1. Go to **Reporting** > **All Reports**.

2. Select the name of the report that you want to copy.
   The report details page opens.

3. Select the more options icon next to **Reconfigure report**.
4. Select **Duplicate report**.

   A message confirms that the report was duplicated. For example, "Report duplicated successfully. Report "DOT3" has been successfully duplicated to "DOT3 (COPY)"."

   The copy is added to the **All Reports** page with "(COPY)" appended to the original report name.

To change the copy, open it from the **All Reports** page and select **Reconfigure report**. See Reconfigure a report *(on page 404)*.

Working with Distribution over time charts

A Distribution over time chart tracks how a DEX property changes across your managed endpoints over a selected period. Use the chart controls to set the time range, change the aggregation interval, group the metric by a device attribute, and open the underlying data.

The **Distribution over time** card is displayed on the **Create Charts** step only when the columns that you selected in the **Data Sets** step include at least one DEX property, such as Dex Score, Dex Boot Score, Dex Device Score, or Dex Application Score. If the report includes no DEX property, the card is hidden.

You can render the chart as a **Bar Chart - Vertical**, which shows the score for each time interval as a separate bar, or as a **Line Chart**, which shows the trend as a continuous line.

Time range

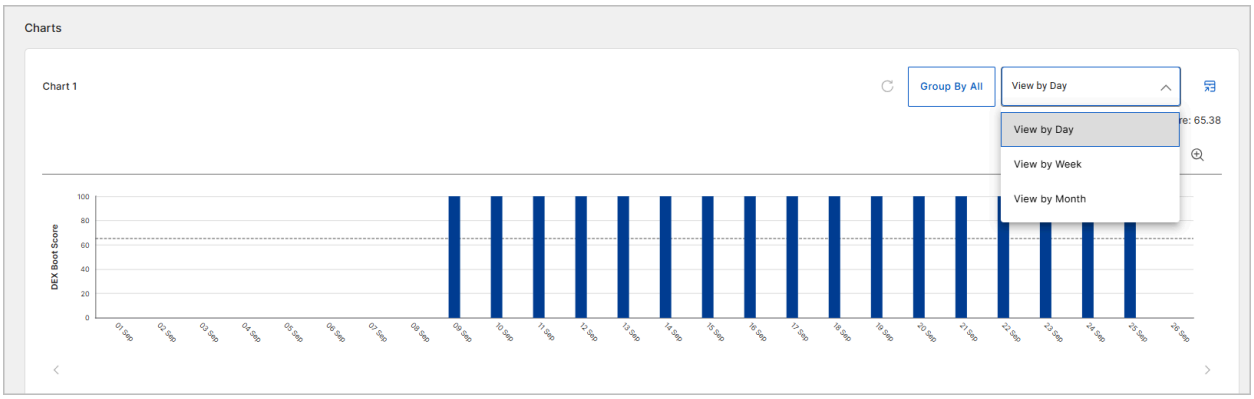
Set **Time range** on the **Create Charts** step to define the period that the chart reports on. Select one of the following values:

- **Last month**
- **Last quarter**
- **Last year**
- **Current month** – the default value.
- **Current quarter**
- **Current year**
- **Custom** – select the start and end dates in the calendar.

Aggregation interval

On the **Preview Report** step and on the report details page, use the **View by** list in the chart header to set the interval that the chart aggregates the scores into:

- **View by Day** – one value for each day.
- **View by Week** – one value for each seven-day window, for example 01 - 07 Sep. This is the default value.
- **View by Month** – one value for each month.



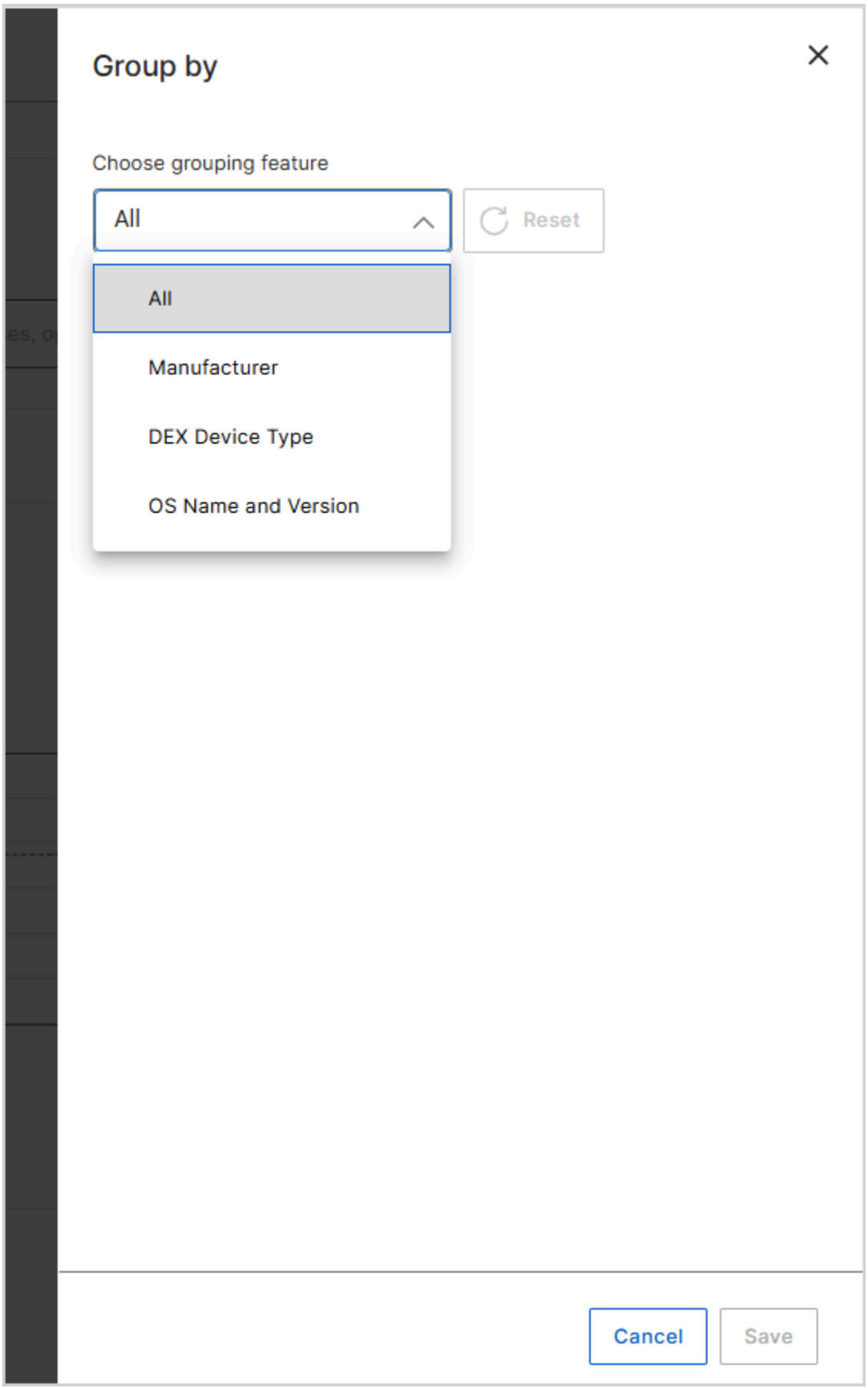
Group the metric by a device attribute

By default the chart aggregates the scores of all contributing devices into a single series, and the button in the chart header is labeled **Group By All**. Group the metric to compare the scores of different device categories against each other.

1. In the chart header, select **Group By**. The **Group by** drawer opens.
2. From the **Choose grouping feature** list, select **All**, **Manufacturer**, **DEX Device Type**, or **OS Name and Version**.
3. If you select a feature other than **All**, the **Select values to chart** list opens. Select the check box of each value that you want the chart to plot as a separate series, and then select **Apply**.
    - Use the search field to locate a value quickly.
    - Select **Reset** in the list to clear the selected values.
4. Select **Save** to apply the grouping, or **Cancel** to close the drawer without applying it.

Note: Selecting the values is required, and you can select a maximum of five. The drawer displays the message "You can only choose: 5" and **Save** stays dimmed until you apply at least one value.

To restore the default grouping, open the drawer again and select **Reset** next to the **Choose grouping feature** list.


Group by
Choose grouping feature
All
Reset
All
Manufacturer
DEX Device Type
OS Name and Version
Cancel
Save

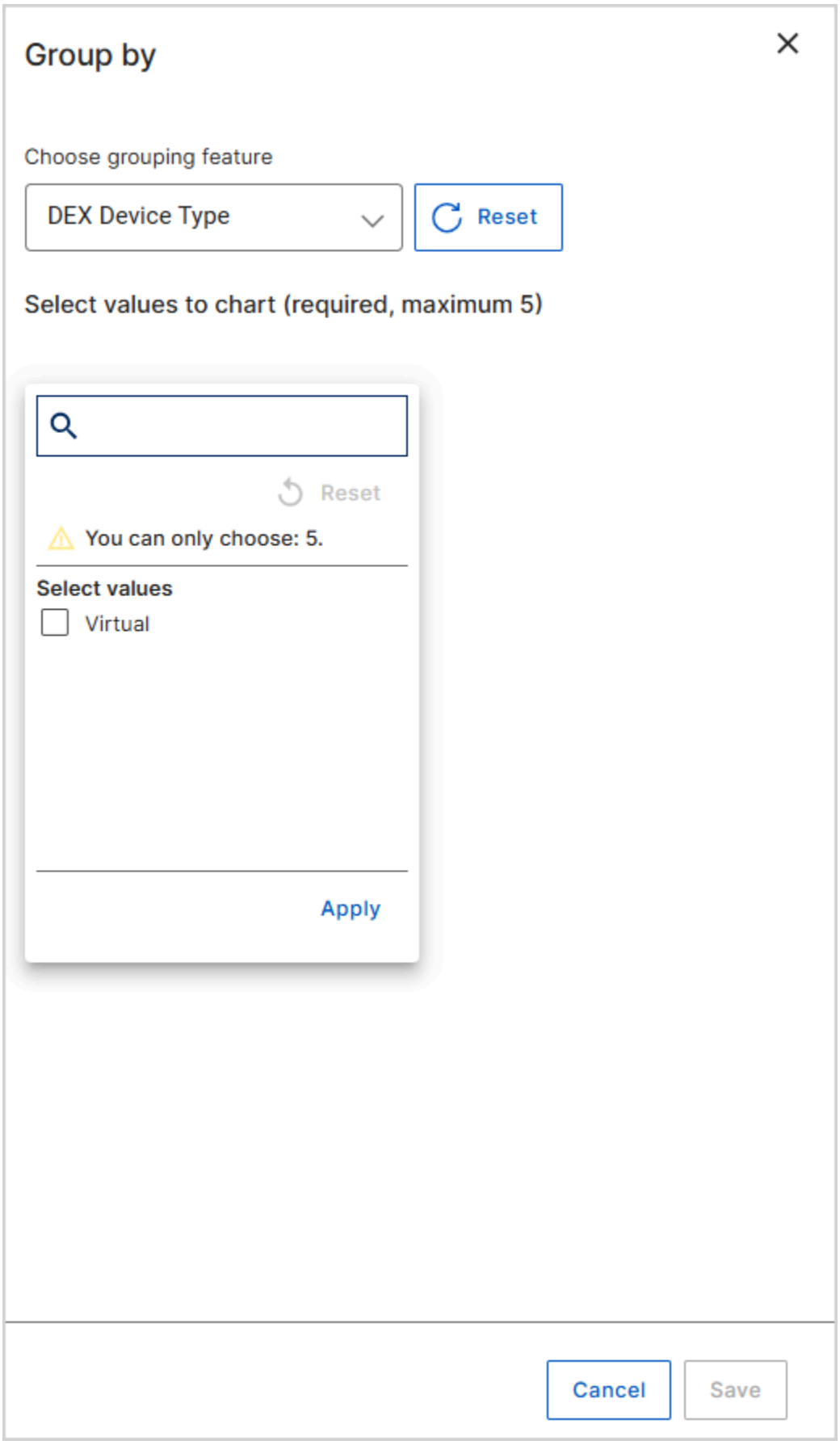

Group by
Choose grouping feature
DEX Device Type
Reset
Select values to chart (required, maximum 5)
Reset
You can only choose: 5.
Select values
Virtual
Apply
Cancel
Save

Chart controls

The chart header and canvas provide the following controls:

- Refresh icon – reloads the latest scores from the server.
- **Average Devices Score** – the benchmark average across the contributing endpoints, displayed above the chart and drawn on the canvas as a dotted line.
- Zoom in, zoom out, and **Reset Zoom** – adjust the magnification of the horizontal axis to focus on a shorter period.
- Left and right arrows – page through the intervals that do not fit on the canvas at one time.

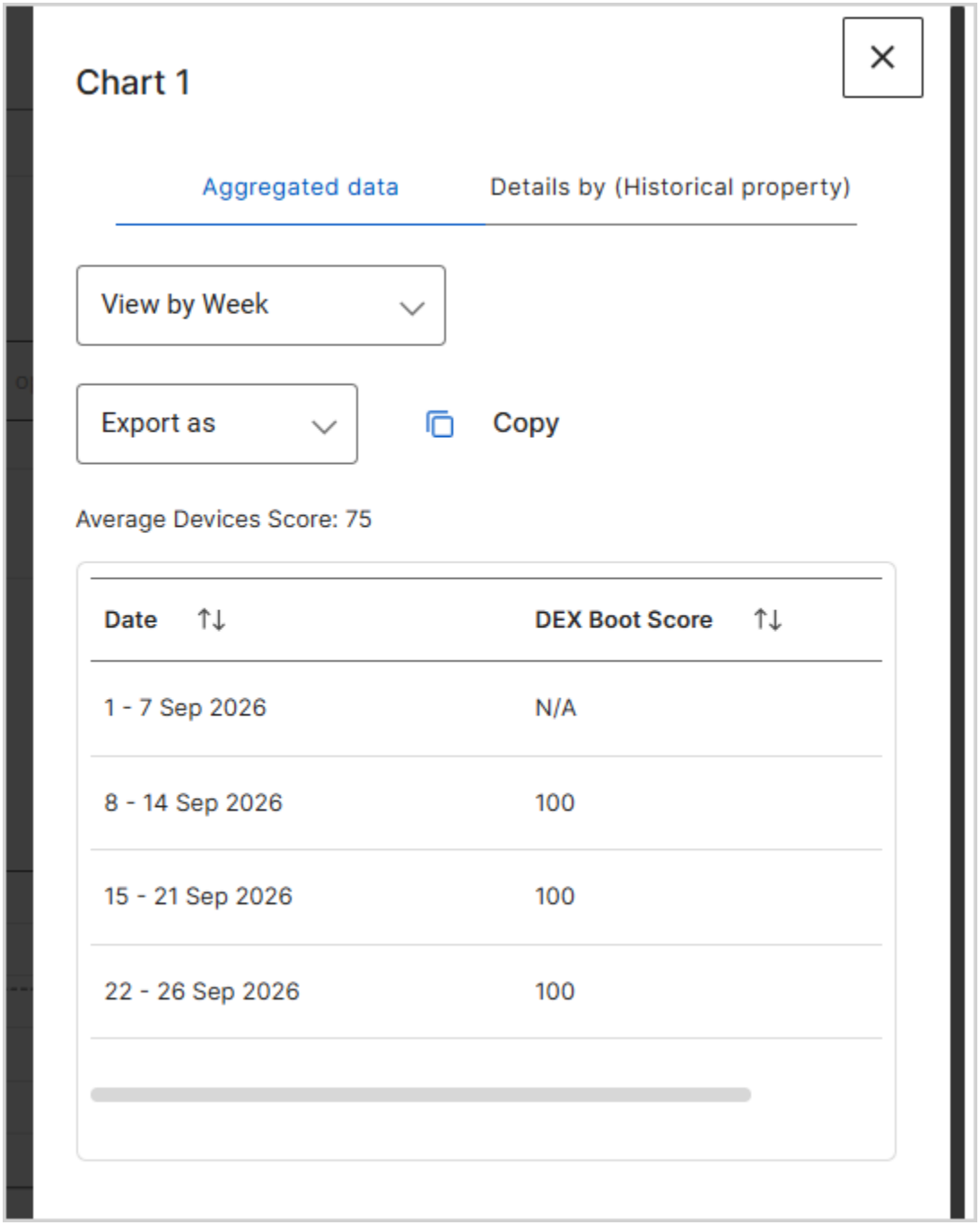
Chart data table

Select the **See data in data table format with download options** icon in the upper-right corner of the chart to open the data drawer. The drawer provides two tabs:

- **Aggregated data** – lists the aggregated score for each interval in the selected time range, in a **Date** column and a column named after the charted DEX property. The benchmark **Average Devices Score** is displayed above the table. Intervals with no reported data show N/A.
- **Details by (Historical property)** – lists the devices that contributed to the selected interval, with their individual scores, so that you can trace a change back to specific endpoints.

The drawer provides its own **View by** list, so you can change the interval without closing it.

Sorting, copying, and exporting the table work the same way as they do for any chart in BigFix UI. For the steps, see Viewing chart data in a table *(on page 33)*.



Content list behavior

Note: When a report includes a **Distribution over time** chart, the **Content list** table is not displayed on the **Preview Report** step or on the report details page, for any of the charts in the report. Review the endpoint records in the **Details by (Historical property)** tab of the chart data drawer instead.

Related information

Create a report with custom configuration *(on page 397)*

Report Builder settings reference *(on page 413)*

Global filter *(on page 36)*

Viewing chart data in a table *(on page 33)*

Exporting Data *(on page 30)*

Report Builder settings reference

Reference information for the Report Builder: the visual formats and configuration settings of each chart widget category, and the properties that you can add as report columns for each data set.

Chart widget categories and settings

The following table lists the visual formats and configuration settings for each widget category on the **Create Charts** page.

Table 74. Chart widget configuration settings

Widget category	Visual formats	Configuration settings
Distribution over time	• Bar Chart - Vertical • Line Chart	Displays how a DEX property changes over a selected time range. • **Chart's name** – A descriptive title for the chart. • **Chart's property** – The DEX property to visualize (for example, DEX Boot Score). The drop-down displays only the DEX properties that you selected in the **Data Sets** step; non-DEX properties are not displayed. • **Time range** – The reporting period for the chart: **Last month**, **Last quarter**, **Last year**, **Current month** (the default), **Current quarter**, **Current year**, or **Custom**. • **View by** – The aggregation interval, set in the chart header on the **Preview Report** step: **View by Day**, **View by Week** (the default), or **View by Month**. • **Group by** – The device attribute that the metric is categorized by, set in the **Group by** drawer: **All**, **Manufacturer**, **DEX Device Type**, or **OS**

Table 74. Chart widget configuration settings (continued)

Widget category	Visual formats	Configuration settings
		Name and Version. For any feature other than **All**, you must also select the values to chart, to a maximum of five. **Note:** This widget category is available only when the selected columns include DEX properties, such as Dex Score or Dex Device Score. If the report includes a Distribution over time chart, the **Content list** is not displayed on the **Preview Report** page for any of the charts. For the chart controls and the two-tab data drawer, see Working with Distribution over time charts *(on page 407)*.
Percentage of a whole	• Donut Chart • Gauge Chart • Pie Chart	• **Chart's name** – A descriptive title for the chart. • **Chart's property** – The data set column to visualize. • **Operator** – The comparison operator (for example, **Equals**). • **Value** – The matching criteria.
Quick link	Link widget with a count as the link label	Defines the KPI that you want a quick link to. The widget is made up of a link to a filtered view of the data, according to criteria that you define, and the link label is the count of the filtered elements. The BigFix properties that you selected in the **Data Sets** step are converted into explorer-compatible properties for use in the Report Builder widgets and configurations. • **Caption** – The label displayed under the count. • **Count of** – The data set column to count. • **Operator** – The comparison operator (for example, **Contains**). • **Value** – The matching criteria.

Table 74. Chart widget configuration settings (continued)

Widget category	Visual formats	Configuration settings
Composition	• Horizontal Bar Chart • Pie Chart • Treemap Chart • Vertical Bar Chart	• **Chart's name** – A descriptive title for the chart. • **Chart's property** – The data set column to visualize.
Category breakdown	• Bar chart - Horizontal groups • Bar chart - Horizontal stacked • Bar chart - Vertical groups • Bar chart - Vertical stacked	Shows the breakdown of one property within each value of another property from the same BigFix object. • **Chart's name** – A descriptive title for the chart. • **Widget's property 1** – The data set column that defines the categories (primary axis). • **Widget's property 2** – The data set column whose values are broken down within each category (legend). **Note:** Records with no value for the selected property are shown as N/A.

Note: The property dropdown lists display only the columns that you selected in the **Data Sets** step.

Note: Every chart provides a **See data in data table format with download options** icon in its upper-right corner, which opens the chart data as a table that you can copy or export. See Viewing chart data in a table *(on page 33)*.

Template wizard settings

The following table lists the settings of the **Customize** step of the guided template wizard.

Setting	Description
Make this report actionable	Adds action buttons to the report. The buttons that are displayed depend on the chosen data set and on the permissions and visibility of the report user.
Schema overview	Lists the base fields that the template always includes. The field count is displayed on the right. Base fields cannot be removed.

Setting	Description
Add property (Optional)	Adds more fields to the data model. Select properties from the **Property name** dropdown list, and then select **Apply**. You can add a maximum of 16 optional properties. Select **Reset** to clear the selection.
Data model	Displays the schema definition of the report. Each field shows its name, data type (**string**, **integer**, **number**, **datetime**, **content**, or **boolean**), and a description. Optional fields that you added include a delete icon.
Variations	Sub-templates that narrow the report to a specific focus. Each variation card shows a name, a description, and a category chip. Select the grid or list icon to change how the variations are displayed.
Content list toolbar	On the **Preview** step, provides **Column** to show or hide columns, **Density** to change the row height, and **Search by Name** to find a specific row. The number of selected rows and the total number of rows are displayed below the toolbar. For an actionable report, select one or more rows to enable the action buttons, such as **Delete** and **Stop**.

Note: On the **Report templates** page, each template card shows the template name, its data source, a description, and a template type chip, such as **Operations**, **Security**, **Compliance**, **Inventory**, or **Actions**. Use the template type dropdown list or the **Search** field to narrow the list.

Report details page controls

The following table lists the controls that are available when you open a saved report from the **All Reports** page.

Control	Description
Reconfigure report	Opens the report in the Report Builder wizard in edit mode.
More options icon	Provides the **Export** and **Duplicate report** actions.
Refresh icon	Reloads the report data and updates the "Updated" timestamp below the report title.
Filter icon	Opens the **Filter** panel, where you can create, save, and apply filters.
View by group	Limits the report to the selected device groups. Search for a group, select **Select all** or individual check boxes, and then select **Apply**. Select **Reset** to clear the selection. A badge on the control shows the number of selected groups. This list is displayed only for reports that were created from a guided template.
See data in data table format with download options icon	Opens the chart data as a table that you can sort, copy, or export. See Viewing chart data in a table *(on page 33)*. For a **Distribution over time** chart, the

Control	Description
	table also provides the **Aggregated data** and **Details by (Historical property)** tabs and a **View by** list.
Chart time grouping list	For a **Distribution over time** chart, sets the interval used on the chart: **View by Day**, **View by Week** (the default), or **View by Month**.
Group By	For a **Distribution over time** chart, opens the **Group by** drawer, where you categorize the metric by a device attribute. Select a value in **Choose grouping feature**. For any feature other than **All**, select the values to chart in the **Select values to chart** list, to a maximum of five, and then select **Apply**. Select **Save** to apply the grouping. Select **Reset** to restore the default grouping.
Average Devices Score	For a **Distribution over time** chart, the benchmark average score across the contributing endpoints. The value is displayed above the chart and drawn on the canvas as a dotted line.
Reset Zoom, zoom in, and zoom out	Adjust the magnification of the horizontal axis to focus on a shorter period.

Note: In the custom configuration wizard, the filter icon and the **View by group** list are available on the **Create Charts** and **Preview Report** steps. The **Preview Report** step also provides the chart data drawer icon and the chart zoom controls. A **Distribution over time** chart provides a refresh icon, the **Group By** button, and the **View by** list in its chart header.

Data set properties

In the **Data Sets** step, select **Add Column** to add properties as report columns. You can select up to a maximum property limit of 18. The **Name**, **Id**, and **Computer group** columns are included by default and cannot be removed. The following tables list the properties available for each data set.

Devices properties

Property	Description
Agent Type	Type of agent that manages the device (for example, Native).
Agent Version	Version of the BigFix agent that is installed on the device.
Correlation Flag	Indicates whether the device record is correlated with other records that represent the same device.
Correlation Id	Identifier that links correlated device records.
Cpu	Processor description of the device, including speed and model.
Cpu Architecture	Processor architecture of the device (for example, x86_64).
Cpu Cores	Number of processor cores on the device.

Property	Description
Cpu Model	Model name of the device processor.
Database Id	Identifier of the database that stores the device record.
Database Name	Name of the database that stores the device record.
Device Type	Type of the device (for example, server, desktop, or laptop).
Dex Application Score	DEX (digital employee experience) score that rates software performance and reliability on the device.
Dex Boot Score	DEX score that rates the boot speed of the device.
Dex Cpu Score	DEX score that rates the CPU utilization of the device.
Dex Das Score	DEX device analytics score reported for the device.
Dex Device Score	Endpoint DEX score that rates the device experience, based on device reliability and performance.
Dex Disk Score	DEX score that rates the disk health of the device.
Dex Gpu Score	DEX score that rates the GPU health of the device.
Dex Last Report Time	Time when the device last reported DEX data.
Dex Logon Score	DEX score that rates the logon speed on the device.
Dex Memory Score	DEX score that rates the memory utilization of the device.
Dex Partition Score	DEX score that rates the disk partition usage of the device.
Dex Reliability Score	DEX score that rates the device reliability, based on crashes and hard resets.
Dex Score	Overall DEX score of the device.
Dex Sentiment Score	DEX score based on user sentiment feedback.
Dex Wi-fi Score	DEX score that rates the Wi-Fi connectivity of the device.
Extension Flag	Indicates whether the device record originates from an agent extension.
Gpu Dedicated Capacity	Dedicated memory capacity of the device GPU.
Gpu Shared Capacity	Shared memory capacity of the device GPU.
Hostname	Host name of the device.
Id	Unique identifier of the device.
Ip Addresses	IP addresses that are assigned to the device.
Last Report Time	Time when the device last reported to the BigFix server.
License Type	BigFix license type that applies to the device.

Property	Description
Link Href	URL of the device resource in the REST API.
Locked Flag	Indicates whether the device is locked and cannot run actions.
Number Of Gpus	Number of GPUs that are installed on the device.
Operating System	Operating system that runs on the device.
Ram Capacity	Amount of RAM that is installed on the device.
Ram Manufacturer	Manufacturer of the RAM that is installed on the device.
Ram Type	Type of the RAM that is installed on the device (for example, DDR4).
Relay Distance	Number of network hops between the device and its relay.
Relay Hostname	Host name of the relay that the device connects to.
Relay Selection Method	Method that the device uses to select its relay (automatic or manual).
Relay Server	Relay server that the device reports to.
Relay Server Flag	Indicates whether the device acts as a relay.
Relevant Fixlet Count	Number of Fixlets that are currently relevant to the device.
Remediated Fixlet Count	Number of Fixlets that were remediated on the device.
Root Server	BigFix root server that the device reports to.
Root Server Flag	Indicates whether the device is the BigFix root server.
Wi-fi Manufacturer	Manufacturer of the wireless network adapter of the device.

Fixlets properties

Property	Description
Analysis Flag	Indicates whether the content item is an analysis.
Applicable Computer Count	Number of computers where the Fixlet is currently applicable.
Baseline Flag	Indicates whether the content item is a baseline.
Category	Category that is assigned to the Fixlet.
Charset	Character set of the Fixlet content.
Components Xml	XML definition of the components included in a baseline.
Creation Time	Time when the Fixlet was created.
Custom Flag	Indicates whether the Fixlet is custom content.
Custom Site Flag	Indicates whether the Fixlet belongs to a custom site.

Property	Description
Cve Id List	CVE identifiers that are associated with the Fixlet.
Digest File Name	File name of the Fixlet digest.
Display Category	Category label that is displayed in the UI.
Display Name	Name of the Fixlet that is displayed in the UI.
Display Source	Source label that is displayed in the UI.
Display Source Id	Source identifier that is displayed in the UI.
Display Source Severity	Source severity that is displayed in the UI.
Download Size	Total size of the files that the Fixlet downloads.
Evaluation Period	Period over which the agent evaluates the Fixlet relevance.
Fixlet Flag	Indicates whether the content item is a Fixlet.
Globally Visible Flag	Indicates whether the Fixlet is visible to all operators.
Group Flag	Indicates whether the content item is a group.
Id	Unique identifier of the Fixlet.
Link Href	URL of the Fixlet resource in the REST API.
Locally Visible Flag	Indicates whether the Fixlet is visible only to the owning operator.
Master Site Flag	Indicates whether the Fixlet belongs to the master action site.
Modification Time	Time when the Fixlet was last modified.
Open Action Count	Number of open actions that were created from the Fixlet.
Operator Site Flag	Indicates whether the Fixlet belongs to an operator site.
Parent Relevances	Relevance expressions that are inherited from the parent content.
Relevance	Relevance expression that determines where the Fixlet applies.
Relevance Clauses	Individual relevance clauses of the Fixlet.
Remediated Computer Count	Number of computers where the Fixlet was remediated.
Sans Id List	SANS identifiers that are associated with the Fixlet.
Source	Source site or vendor of the Fixlet.
Source Id	Identifier that is assigned by the Fixlet source.
Source Release Date	Date when the source released the Fixlet.
Source Severity	Severity level that is assigned by the Fixlet source.
Task Flag	Indicates whether the content item is a task.

Property	Description
Type	Content type of the item (for example, Fixlet or task).
Unlocked Computer Count	Number of applicable computers that are not locked.
Visible Flag	Indicates whether the Fixlet is visible in the UI.
Wizard Link	Link to the wizard that created the Fixlet.
Wizard Name	Name of the wizard that created the Fixlet.

Deployments properties

Property	Description
Action Script	Script that the deployment runs on the target devices.
Action Script Type	Type of the action script (for example, BigFix action script).
Applicability Relevance	Relevance expression that determines where the deployment applies.
Computer Group Flag	Indicates whether the deployment targets a computer group.
Constrain By Property Name	Name of the property that constrains the deployment targets.
Constrain By Property Relation	Relation that is used in the property constraint.
Constrain By Property Value	Value that is used in the property constraint.
Continue On Errors Flag	Indicates whether a multiple-action group continues to run when a component fails.
Custom Success Relevance	Custom relevance expression that defines when the deployment is successful.
Database Id	Identifier of the database that stores the deployment record.
Database Name	Name of the database that stores the deployment record.
Date Range End	End of the date range in which the deployment can run.
Date Range Start	Start of the date range in which the deployment can run.
End Date	Date when the deployment ends.
End Flag	Indicates whether an end date is set for the deployment.
End Time_of_day	Time of day when the deployment stops running.
Expiration Flag	Indicates whether the deployment expires.
Expiration Time	Time when the deployment expires.
Group Member Flag	Indicates whether the deployment is a member of an action group.

Property	Description
Hidden Flag	Indicates whether the deployment is hidden.
Id	Unique identifier of the deployment.
Link Href	URL of the deployment resource in the REST API.
Management Rights Flag	Indicates whether the deployment is restricted by management rights.
Message Action Button Flag	Indicates whether the user message includes an action button.
Message Allow Cancel Flag	Indicates whether users can cancel the deployment from the message.
Message Postpone Delay	How long users can postpone the deployment from the message.
Message Text	Text of the message that is displayed to users before the deployment runs.
Message Timeout Delay	How long the user message is displayed before it times out.
Message Title	Title of the message that is displayed to users before the deployment runs.
Multiple Flag	Indicates whether the deployment is a multiple-action group.
Offer Category	Category of the offer, if the deployment is presented as an offer.
Offer Flag	Indicates whether the deployment is presented to users as an offer.
Operator Site Flag	Indicates whether the deployment was issued from an operator site.
Postaction Allow Cancel Flag	Indicates whether users can cancel the post-action, such as a restart.
Postaction Force Delay	Delay before the post-action is forced to run.
Postaction Message Text	Text of the message that is displayed before the post-action.
Postaction Message Title	Title of the message that is displayed before the post-action.
Postaction Postpone Delay	How long users can postpone the post-action.
Precache Flag	Indicates whether downloads are cached before the deployment runs.
Reapplication Interval	Interval between reapplications of the deployment.
Reapplication Limit	Maximum number of times that the deployment reapplies.
Reapply Flag	Indicates whether the deployment reapplies when it becomes relevant again.
Require User Absence	Indicates whether the deployment runs only when no active user is present.
Require User Presence	Indicates whether the deployment runs only when an active user is present.
Restart Flag	Indicates whether the target device restarts after the deployment completes.
Retry Delay	Wait time between retry attempts.
Retry Limit	Maximum number of retry attempts.
Retry Wait For Reboot Flag	Indicates whether the deployment waits for a restart before it retries.

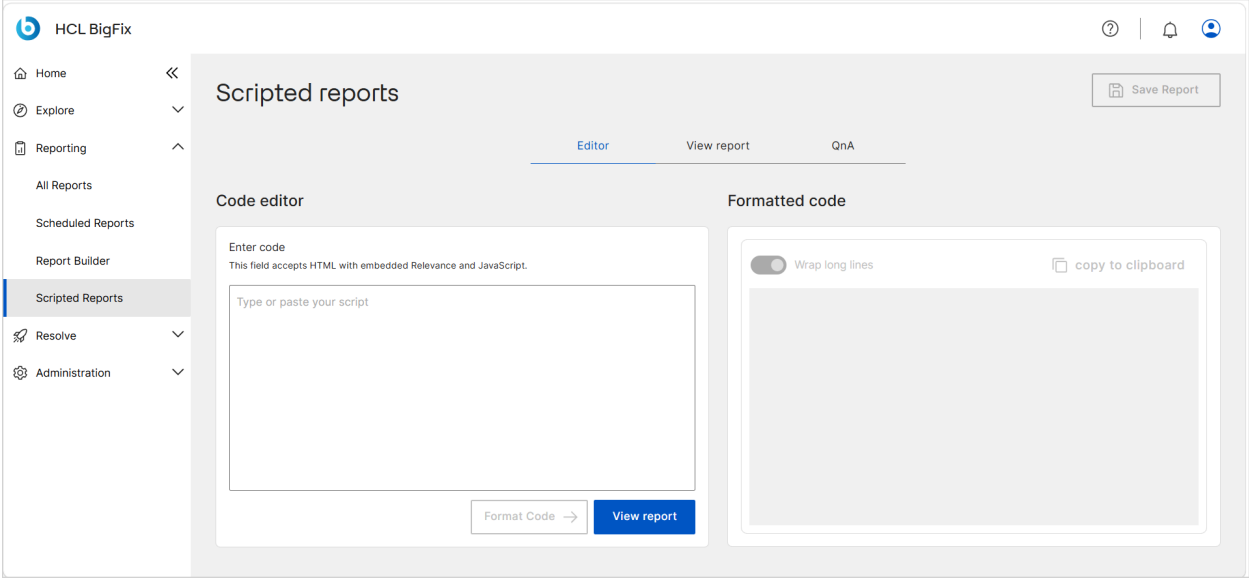
Property	Description
Running Message Text	Text of the message that is displayed while the deployment runs.
Running Message Title	Title of the message that is displayed while the deployment runs.
Secure Parameter Flag	Indicates whether the deployment parameters are stored securely.
Selected Groups String	Computer groups that are selected as deployment targets.
Settings Flag	Indicates whether custom settings are applied to the deployment.
Show Message Flag	Indicates whether a message is displayed to users before the deployment runs.
Show Running Message Flag	Indicates whether a message is displayed while the deployment runs.
Shutdown Flag	Indicates whether the target device shuts down after the deployment completes.
Single Flag	Indicates whether the deployment is a single action.
Source Relevance	Relevance expression from the source Fixlet.
Start Date	Date when the deployment starts.
Start Flag	Indicates whether a start date is set for the deployment.
Start Time_of_day	Time of day when the deployment starts running.
State	Current state of the deployment (for example, Open, Stopped, or Expired).
Subscription Flag	Indicates whether the deployment relates to a site subscription.
Success On Custom Relevance	Indicates whether success is evaluated by a custom relevance expression.
Success On Original Relevance	Indicates whether success is evaluated by the original relevance becoming false.
Success On Run To Completion	Indicates whether success is evaluated by the action script running to completion.
Targeted By Id Flag	Indicates whether the deployment targets devices by identifier.
Targeted By List Flag	Indicates whether the deployment targets devices from a list.
Targeted By Property Flag	Indicates whether the deployment targets devices by property values.
Targeted List	List of the deployment targets.
Targeted Names	Names of the targeted devices.
Targeting Method	Method that is used to target the deployment.
Targeting Relevance	Relevance expression that is used to target the deployment.
Temporal Distribution	Time window over which the deployment start is staggered across devices.

Property	Description
Time Issued	Time when the deployment was issued.
Time Range End	End of the time range in which the deployment can run.
Time Range Start	Start of the time range in which the deployment can run.
Time Stopped	Time when the deployment was stopped.
Top Level Flag	Indicates whether the deployment is the top-level action of a group.
Untargeted Flag	Indicates whether the deployment has no specific targets.
Urgent Flag	Indicates whether the deployment is sent with urgent priority.
Utc Time Flag	Indicates whether the deployment schedule uses UTC time.

Scripted Reports

With Scripted Reports, you create scripted reports: reports that you write in HTML with embedded BigFix Relevance expressions and optional JavaScript or CSS. Scripted reports let you design advanced, interactive reports beyond the standard Report Builder charts.

To open Scripted Reports, expand **Reporting** in the side navigation, and then select **Scripted Reports**.



Note: Scripted Reports features are disabled by default. To enable these features, you must set several `Settings` values in the `AppConfig.yaml` file. For the list of settings, see Scripted Reports reference *(on page 431)*.

Before you begin

Access to this application is controlled by the role that your administrator assigns to you. If your role does not grant the application, it does not appear in the side navigation, and the actions described in this topic are unavailable or dimmed.

- Your role must grant access to the Reports application with the **Can use scripted reports** option selected. See Managing Roles *(on page 467)*.
- Scripted Reports features are disabled by default. Your administrator must enable them in the `AppConfig.yaml` file. See Scripted Reports reference *(on page 431)*.
- Your operator permissions determine which actions you can complete. For a description of each permission, see Permissions reference *(on page 482)*.

Tabs

Scripted Reports include three key sections within the BigFix UI:

- **Editor** – Create and edit scripted reports by using your own code.
- **View report** – Preview and verify your report output.
- **QnA** – Evaluate Relevance expressions in real time before embedding them.

Editor panes

The **Editor** tab is divided into two panes:

- **Code editor** – The **Enter code** field where you type or paste your script.
- **Formatted code** – A read-only pane that displays the formatted version of your script after you click **Format Code**.

Until you enter code, the **Save Report**, **Format Code**, and **View report** buttons remain disabled.

For a description of every control on these panes, see Scripted Reports reference *(on page 431)*.

Report management

When you save a scripted report, it is added to the **All Reports** page and is listed with **Scripted Report** in the **App** column. Reports that you create here are stored in the BigFix UI database and are managed as part of All Reports, where you can modify or delete them at any time.

For the procedure, see Create and manage a scripted report *(on page 426)*.



Note: Scripted Reports are intended for advanced users who are familiar with HTML and Relevance.

Related information

Create and manage a scripted report *(on page 426)*

Scripted Reports reference *(on page 431)*

All Reports *(on page 355)*

Create and manage a scripted report

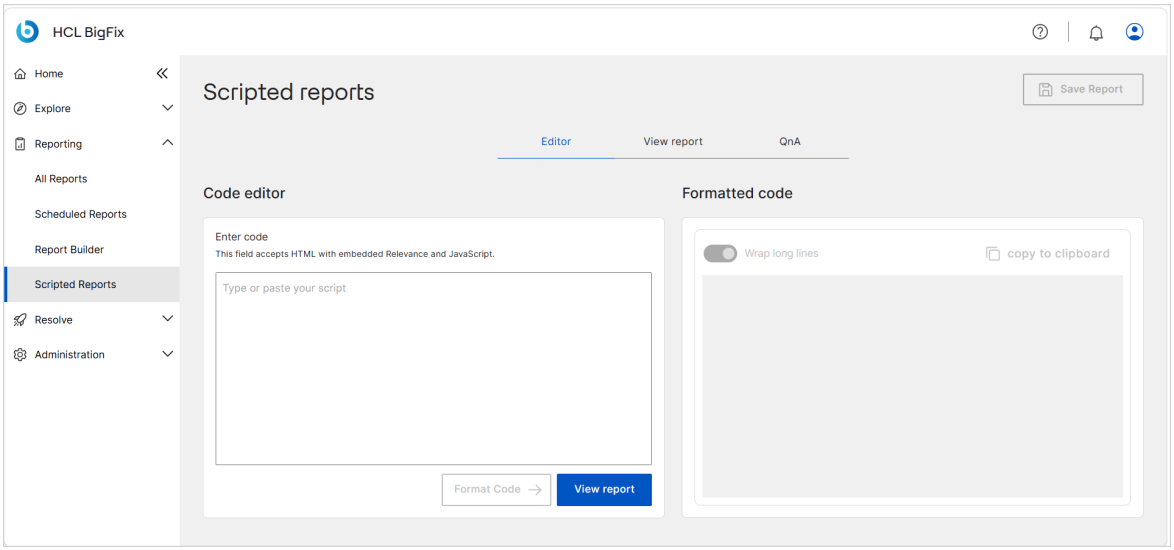
Write custom HTML and Relevance-based scripts to create tailored reports that fetch and display BigFix data dynamically, preview the output, and save the report to the All Reports page.

Scripted Reports features are disabled by default. Before you begin, make sure that these features are enabled in the `AppConfig.yaml` file. See Scripted Reports *(on page 424)*.

Scripted Reports are intended for advanced users who are familiar with HTML and Relevance.

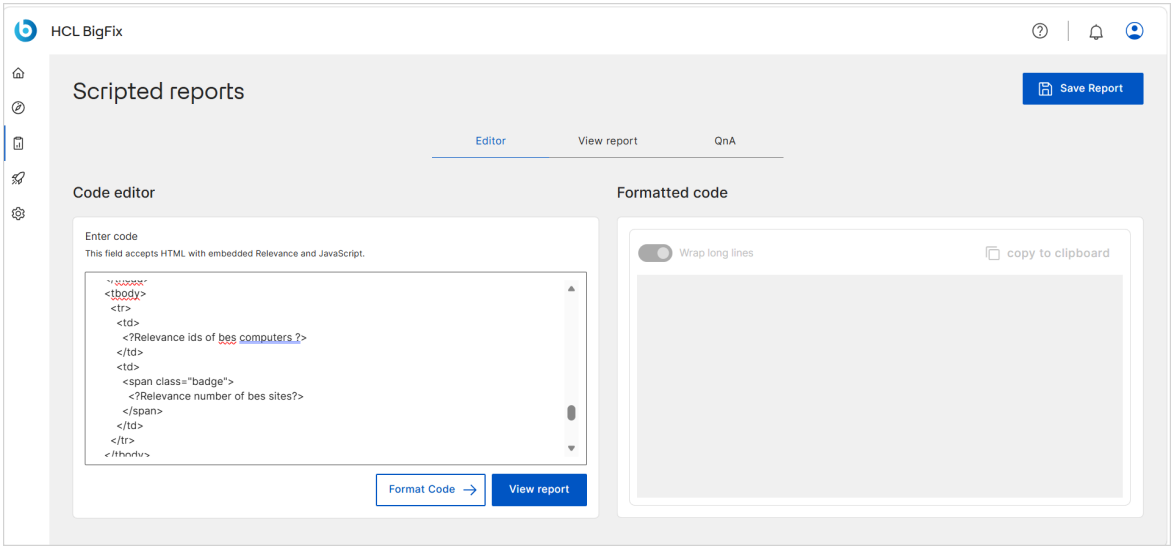
1. Expand **Reporting** in the side navigation, and select **Scripted Reports**.

   The **Editor** tab opens with the **Code editor** pane on the left and the **Formatted code** pane on the right.



2. In the **Enter code** field, type or paste your script.

   This field accepts HTML with embedded Relevance and JavaScript.



To embed a Relevance expression in your code, enclose the expression in a relevance tag. Use the following format:

```
<?relevance <relevance expression> ?>
```

For example:

```
<?relevance ids of bes computers ?>
```

The tag identifies the enclosed text as a Relevance expression. If you enter an expression without the tag, it is not evaluated.

Example: The following sample report shows BigFix data in a table. Each table cell uses a relevance tag to retrieve the data, and a script counts the table rows and displays the total below the table.

```
<!DOCTYPE html>
<html>
<head>
  <title>BigFix BES Overview</title>
  <style>
    body { font-family: sans-serif; margin: 20px; }
    table { width: 100%; border-collapse: collapse; margin-bottom: 10px; }
    th, td { border: 1px solid #ccc; padding: 8px; text-align: left; }
    th { background-color: #005A9C; color: white; }
  </style>
</head>
<body>
  <h2>BES Details Overview</h2>
  <table id="besTable">
```

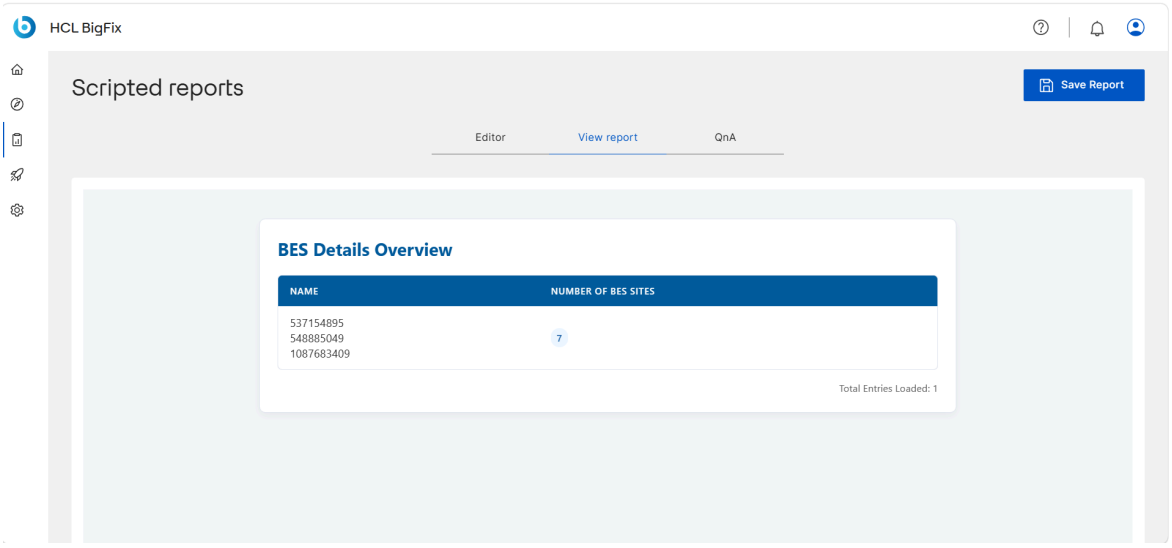
```
    <thead>
      <tr>
        <th>Name</th>
        <th>Number of BES Sites</th>
      </tr>
    </thead>
    <tbody>
      <tr>
        <td><?Relevance ids of bes computers ?></td>
        <td><?relevance number of bes sites ?></td>
      </tr>
    </tbody>
  </table>
  <p id="rowCountDisplay"></p>
  <script>
    const rows = document.querySelectorAll("#besTable tbody tr").length;
    document.getElementById("rowCountDisplay").innerText = "Total Entries: " + rows;
  </script>
</body>
</html>
```

3. **Optional:** Click **Format Code** to auto-indent your script.

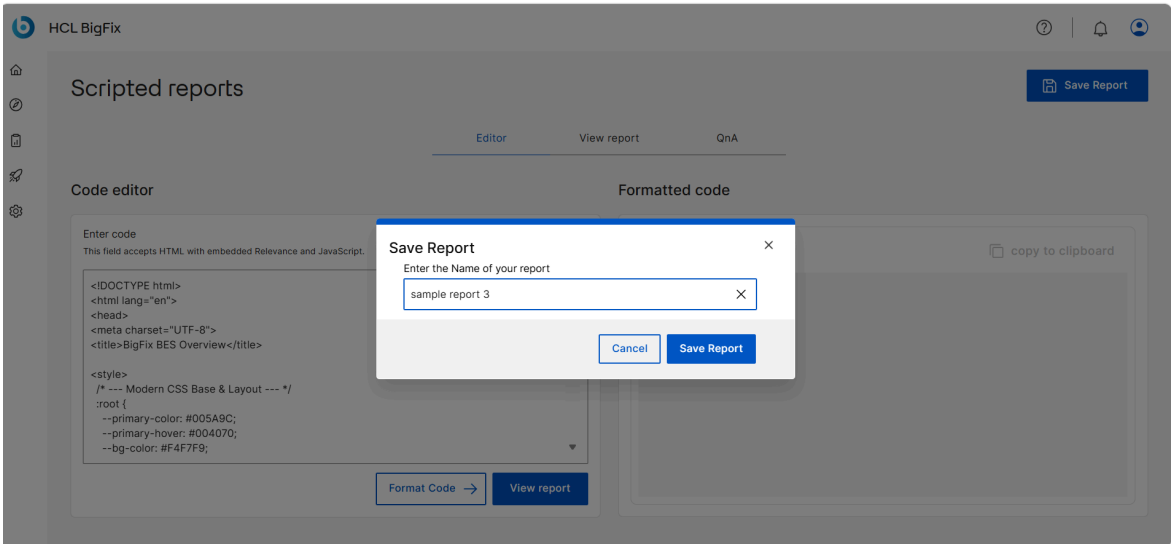
   The formatted script appears in the **Formatted code** pane. In that pane, you can turn on **Wrap long lines** to read long lines without scrolling sideways, or click **copy to clipboard** to copy the formatted script.

4. Click **View report** to generate and preview the report output.

   Validate that the data renders correctly. Relevance errors are displayed inline in the preview.

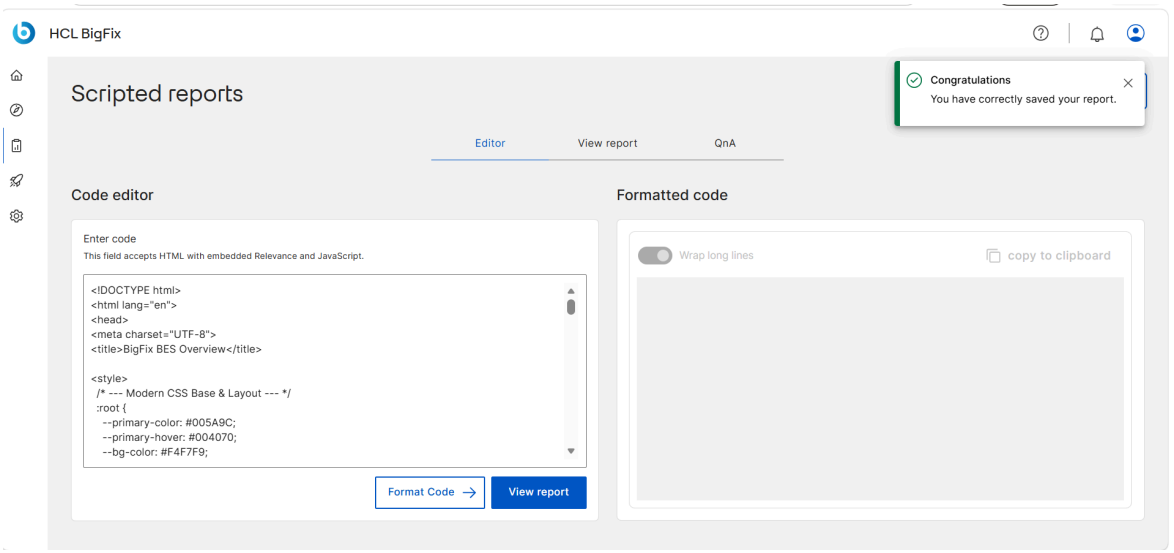


5. Click **Save Report**.



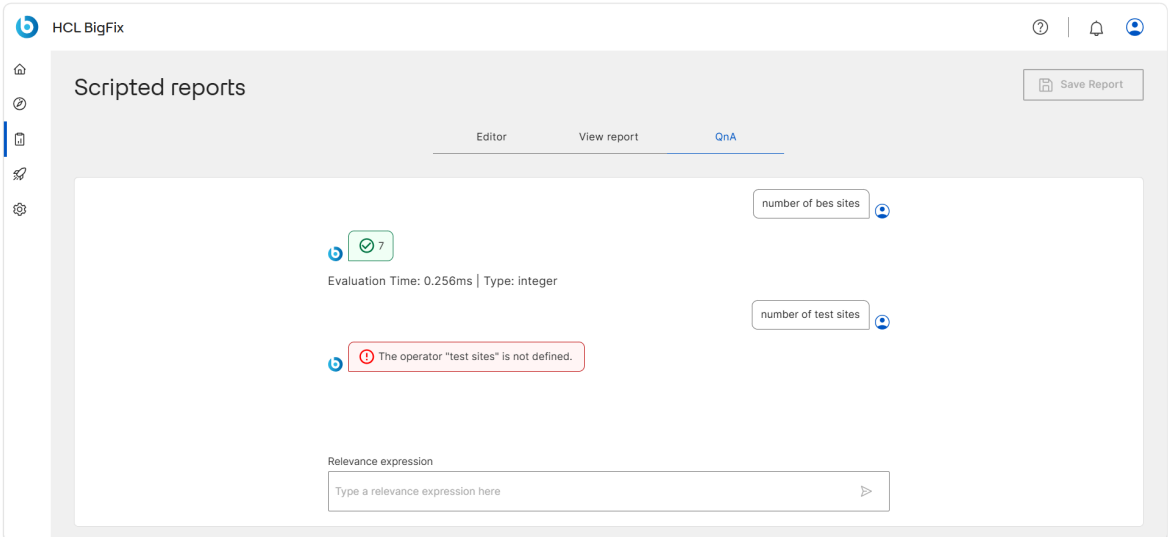
   a. In the **Save Report** dialog box, enter a name for your report.
   b. Click **Save Report** again.

A success message appears in the upper-right corner: "Congratulations You have correctly saved your report."

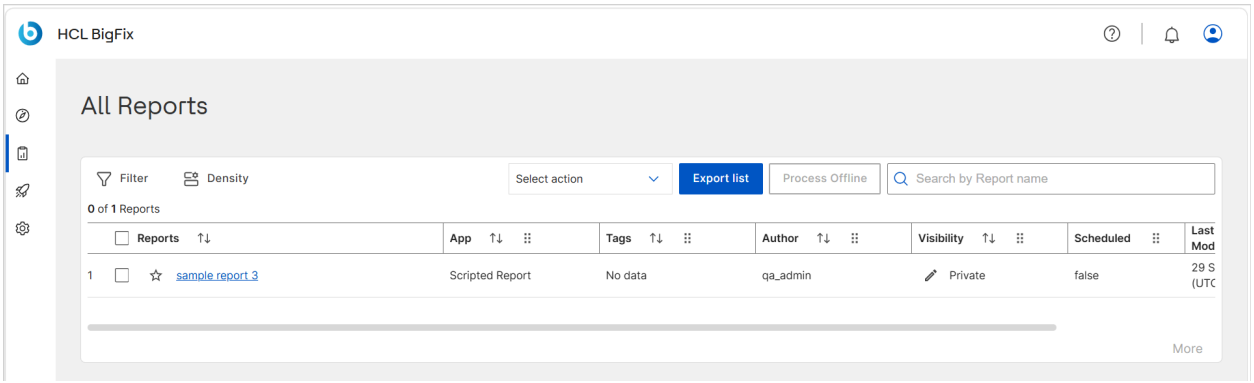


6. **Optional:** Select the **QnA** tab to test individual Relevance expressions.

Enter a Relevance expression in the **Relevance expression** box and click the arrow icon to run it. The result is displayed in real time with its evaluation time and result type. If the expression is not valid, an error message appears in place of the result.



The saved report is added to the **All Reports** page and is listed with **Scripted Report** in the **App** column.



You can modify or delete your scripted reports at any time from the **All Reports** page. See All Reports *(on page 355)*.

Related information

Scripted Reports *(on page 424)*

Scripted Reports reference *(on page 431)*

All Reports *(on page 355)*

Scripted Reports reference

Reference information for Scripted Reports: the configuration settings that enable its features, the controls on each tab, and usage considerations.

Configuration settings

Scripted Reports features are disabled by default. To enable these features, add the following settings to the `Settings` section of the `AppConfig.yaml` file and set them to `true`.

Table 75. AppConfig.yaml settings for Scripted Reports

Setting	Description
`AllowCustomJsonDefinitionReportsView`	Shows the **View report** tab and the **View report** button, where you preview the output of a scripted report. Works together with `AllowCustomJsonDefinitionReportsExecution`. If either setting is `false`, the tab and the button are hidden. If this flag is `false` then "reports created from scripted reports app" will be excluded from report list in all reports page.
`AllowCustomJsonDefinitionReportsCreation`	Lets you save or edit scripted reports. If this setting is `false`, the **Save Report** button stays disabled.
`AllowCustomJsonDefinitionReportsExecution`	If the flag is `true`, Shows the **View report** tab and the **View report** button, where you preview the output of a scripted report. Works together with `AllowCustomJsonDefinitionReportsView`. If either setting is `false`, the tab and the button are hidden.
`AllowUseQna`	Shows the **QnA** tab, where you evaluate Relevance expressions. If this setting is `false`, the **QnA** tab is hidden.

Note: To use the **View report** tab and button, set both `AllowCustomJsonDefinitionReportsView` and `AllowCustomJsonDefinitionReportsExecution` to `true`. If either setting is `false`, the **View report** tab and button are hidden.

These settings are documented in the ***BigFix UI Administration Guide***. For more information, see Configuration Variables.

Note: After adding, removing, or modifying these flags in the AppConfig.yaml file, save your changes and restart the BES UI service; the updates will not take effect until the service has been restarted.

Editor tab controls

The **Editor** tab is divided into the **Code editor** pane and the **Formatted code** pane. The following table lists the controls on this tab.

Table 76. Editor tab controls

Control	Pane	Description
Enter code	**Code editor**	The field where you type or paste your script. It accepts HTML with embedded Relevance and JavaScript.
Format Code	**Code editor**	Auto-indents and formats your script for readability. The result appears in the **Formatted code** pane. Disabled until you enter code.
View report	**Code editor**	Switches to preview mode to display the report output. Disabled until you enter code. Hidden if `AllowCustomJsonDefinitionReportsView` or `AllowCustomJsonDefinitionReportsExecution` is `false`.
Wrap long lines	**Formatted code**	Wraps long lines so that you can read them without scrolling sideways.
copy to clipboard	**Formatted code**	Copies the formatted script to your clipboard.
Save Report	Page header	Opens the **Save Report** dialog box, where you name and save the report. Disabled until you enter code, or if `AllowCustomJsonDefinitionReportsCreation` is `false`.

QnA tab results

The **QnA** tab evaluates a single Relevance expression and returns the result with the following details:

- **Result** – The value that the expression returns.
- **Evaluation Time** – The time in milliseconds that the server took to evaluate the expression.
- **Type** – The data type of the result, for example, `integer`.

If the expression is not valid, an error message appears in place of the result. For example, `The operator "test sites" is not defined.`

Usage considerations

- Scripted Reports are intended for advanced users who are familiar with HTML and Relevance.
- Relevance errors are displayed inline when you preview reports.
- Reports that you create here are stored in the BigFix UI database and are managed as part of All Reports.
- You can modify or delete reports at any time from the **All Reports** page.

Related information

Scripted Reports *(on page 424)*

Create and manage a scripted report *(on page 426)*

Configuration Variables

Administration

The Administration section helps you manage users and access control in BigFix UI.

Note: Administration section visible only to administrators. Ensure you are logged in as an administrator to access this app.

Administration provides the tools needed to securely manage access to the BigFix UI. It includes:

- **Application Configuration** *(on page 433)* – Manage the modular applications and integrations that BigFix UI hosts, such as global DEX settings and IVR settings. The page lists each application as a card and shows whether it is configured, so that you can open the configuration page that the application team owns.
- **Identity management** *(on page 447)* – Manage users, roles, permissions, account policies, and identity provider configuration from one central place.
- **System configuration** *(on page 514)* – Manage the global settings that every application in BigFix UI shares. In this release, System configuration contains the SMTP settings that BigFix UI uses to send email, such as scheduled report deliveries.

Note: Identity management replaces the earlier User management app. User and role management capabilities are now available from the **User & Role Management** card in Identity management.

Related information

Identity management *(on page 447)*

Application Configuration

The Application Configuration page is a central administrative hub for the modular applications and integrations that BigFix UI hosts. It lists each application as a card and shows whether the application is configured, so that you can open the configuration page that the application team owns.

Use the Application Configuration page to set up a newly integrated application or to reach the settings of an application that is already configured. The page groups every hosted application into a **Not Configured** section and a **Configured** section, so you can see at a glance which applications still need attention.

Note:

- The page is a configuration directory, not an application launcher.
- Each application team owns and implements its own configuration page. The options that you see depend on the application.
- The cards that appear depend on your site subscriptions, your environment setup, and your role. An application that is not installed or not entitled does not appear.

Key capabilities:

- Lists every hosted application configuration in one directory.
- Sorts applications by their current setup status, Configured or Not Configured.
- Opens the configuration page of each application directly from its card.
- Manages integration parameters and feature policies for modular applications from a single place.

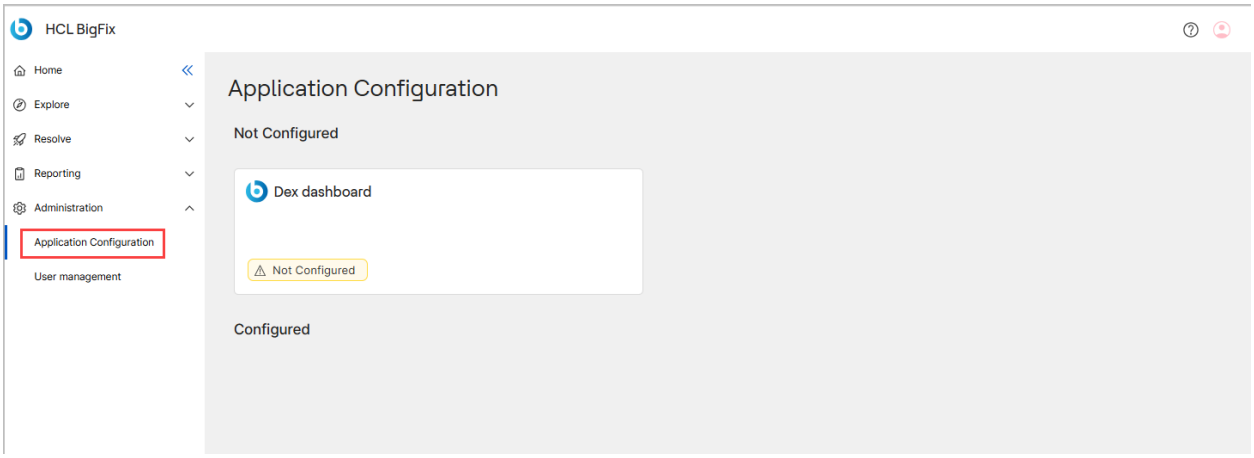
Open the Application Configuration page

Open the page to review the status of the hosted applications and manage their settings.

Note: You must be logged in to BigFix UI with administrator privileges. For more information, see Access control and role permissions *(on page 436)*.

1. In the side navigation, expand **Administration**.
2. Select **Application Configuration**.

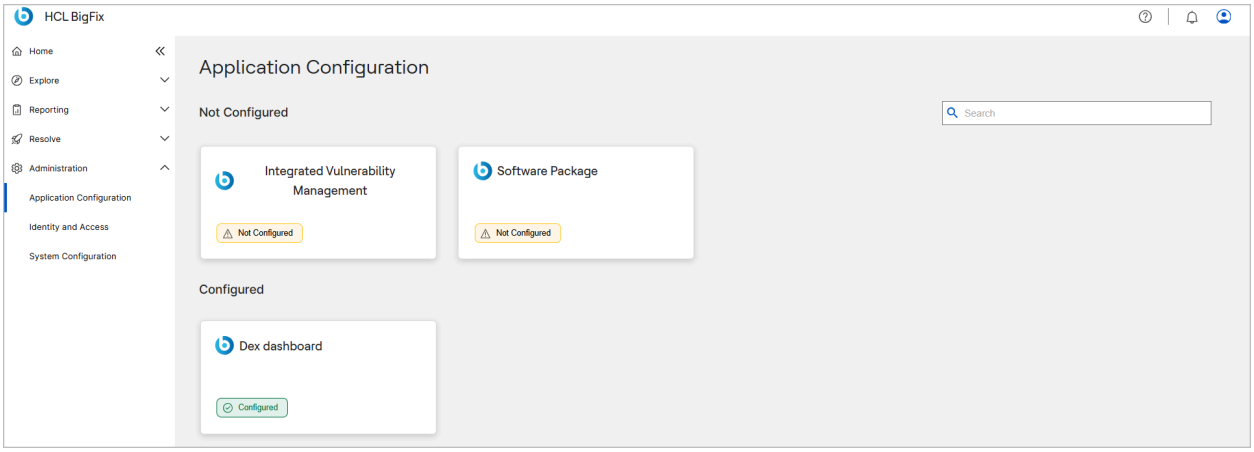
The page opens and loads the list of application configurations. Use the search box in the upper-right corner to find an application by name.



Configure an application

Select an application card to open the configuration page of that application.

1. To set up a new application, select a card in the **Not Configured** section. Complete the settings that the application requires. When the setup is complete, the card moves to the **Configured** section.
2. To review or change an existing setup, select a card in the **Configured** section. BigFix UI opens the configuration page of that application.



Applications that you can configure

The cards that appear depend on your site subscriptions and your environment. The hub can host the following applications and integrations. More applications are added in each release.

Table 77. Applications in the Application Configuration hub

Application	What you configure
Software Package	Software Distribution and BigFix Self-Service Application (SSA) settings. Migrate legacy software packages that were created in the BigFix Console or the classic WebUI into BigFix UI. Define the allowed download and source URLs, the whitelist, that packages can use to add external files. Set the platform-level SSA options, such as branding, client name, custom tabs, and support links, and the notification and user prompt rules. BigFix UI creates or updates the SSA configuration Fixlets that send these settings to all entitled endpoints.
Integrated Vulnerability Management	Settings and connectivity for BigFix Insights for Vulnerability Remediation (IVR). The card appears only when the IVR site is enabled. It shows the configuration status and links to the administrator setup. See IVR settings *(on page 437)*.

Table 77. Applications in the Application Configuration hub (continued)

Application	What you configure
Dex dashboard	Global settings for BigFix Digital Employee Experience (DEX). See Global DEX settings *(on page 437)*.

Other hosted applications and external integrations, such as the Compliance dashboard, Patch, Software Explorer, Workflow Builder, and Remote Control parameters, expose a card here as they become available. The card appears when the matching site is enabled in your deployment.

Interface reference

The page groups the application cards by configuration status. Use the following table to understand the elements of the interface.

Table 78. Application Configuration interface reference

UI element	Description
Not Configured	A section that lists the applications that need setup before you can use them. Each card carries a warning icon and a **Not Configured** label.
Configured	A section that lists the applications that are set up. Each card carries a check icon and a **Configured** label.
Application card	A tile that shows the application name and its status. Select the card to open the configuration page of the application.
Search	Filters the cards as you type an application name.

Access control and role permissions

Access to the page is limited to administrators.

- Master operators and local administrators can open the page. A custom role can open it when the role has explicit access to the Application Configuration app.
- To grant access, expand **Administration**, select **Identity Management**, and then select the **User & Role Management** card. When you create or edit a role, turn on **Application Configuration** in the **Applications** step, under **What applications should this role access?**. See Creating a new role *(on page 468)*.
- If your role does not have this access, the **Application Configuration** entry does not appear in the navigation.

Related information

Global DEX settings *(on page 437)*

IVR settings *(on page 437)*

Managing Roles *(on page 467)*

Identity management *(on page 447)*

Global DEX settings

The Global DEX settings page shows the custom global DEX settings that apply to your entire environment. Use it to review the settings that control how DEX collects and scores data on your devices.

The **Dex dashboard** card on the Application Configuration *(on page 433)* page opens the **Global DEX settings** page. The card appears in the **Configured** section when DEX is set up in your deployment.

Note: The settings on this page are read-only. To change them, run the **Update Global Profile Settings** Fixlet of the DEX site from the BigFix Console.

More information

For the full list of global DEX settings and their values, see Global DEX settings.

Related information

Application Configuration *(on page 433)*

Global DEX settings

IVR settings

The **Integrated Vulnerability Management** card in Application Configuration connects BigFix UI to BigFix Insights for Vulnerability Remediation (IVR). Use it to run the initial setup, to review the saved server, application, and database settings, and to manage the scanner datasources that IVR imports vulnerability data from.

BigFix Insights for Vulnerability Remediation correlates vulnerability findings from a third-party scanner with the devices that BigFix manages, so that you can remediate those findings from BigFix UI. Before IVR can do that, it needs to know which database to write to, how to reach its own service, and which scanner to import from. You supply all of that from the **Integrated Vulnerability Management** card on the **Application Configuration** page.

The card appears only when the BigFix Insights for Vulnerability Remediation site is enabled in your deployment. For the wider role of the page that hosts the card, see Application Configuration *(on page 433)*.

What must be in place first

The card and the application are both gated. Three conditions must be met before an operator sees IVR at all:

- The **BigFix Insights for Vulnerability Remediation** site is enabled for a user who has compliance access, and the deployment holds an active license for it.
- The version of that site is greater than 0. A site that is subscribed but not yet gathered reports version 0, and IVR stays hidden until the first gather completes.
- The role that is assigned to the user grants access to the application. An administrator turns the application on in the Applications step when creating or editing a role, in **User & Role Management**. A role created without it hides IVR from every user who holds that role.

Note: Enabling a site and creating roles are platform tasks rather than IVR tasks. For the procedures, see the site management and role management topics of this guide.

Configuration statuses

The **Application Configuration** page sorts every application card into a **Not Configured** group or a **Configured** group, and the card itself carries a matching status chip. For IVR, the status reports the outcome of the setup, not merely whether you filled in the form:

- **Not Configured** – Either you have not run the setup, or you ran it and one of the background processes that it starts did not finish. The setup screens stay available so that you can correct the values and run it again.
- **Configured** – The setup finished and every background process that it started completed successfully. Selecting the card now opens the **IVR Configuration** page in its **View Configuration** state instead of the setup wizard.

Until the status is **Configured**, the IVR pages under **Resolve** open but return no data, and report that the application is not yet configured.

The IVR Configuration page

Selecting the **Integrated Vulnerability Management** card opens the **IVR Configuration** page. What the page shows depends on the status.

When IVR is not yet configured, the page presents the setup as a sequence of steps. See Configure IVR *(on page 439)*.

When IVR is configured, the page opens on **View Configuration**, which summarizes the saved settings in three panels and lists the scanner datasources below them:

- **Server configuration** – The address, ports, and subject alternative names of the IVR service. This panel is read-only.
- **Application configuration** – The web protocol, local web server port, cross-origin policy, Windows service option, and proxy settings. Select **Edit** to change them.
- **Database Configuration** – The host, port, credentials, connection string, and schema of the database that holds the IVR data. Select **Edit** to change them.

For every value in these panels, see IVR configuration reference *(on page 443)*.

Why server configuration is read-only

Earlier releases let you enter the server settings yourself. The installer and the IVR service now derive those values and write them for you, so the **Server configuration** panel reports them but does not offer an **Edit** control. To change a server value, change it at the service and reopen the page.

Scanner datasources

A datasource is one connection to a vulnerability scanner. IVR imports findings from each datasource that you add, then matches them against the devices that BigFix manages. The **Datasource** section of **View Configuration** lists every connection, identified by its **Type**, **Target** URL, and **Alias**. Use **Add datasource** to connect another scanner, and the controls in the **Action** column to change or remove one.

You add the first datasource during setup. You can add more at any time afterward.

What becomes available after setup

Once the status is **Configured**, IVR appears under **Resolve** as **Integrated Vulnerability Remediation**, with its overview, vulnerability, and device views. Separately, enabling the site adds a **Vulnerability** tab to the device details page in Device Explorer, which lists the vulnerabilities found on that one device. If the site is not enabled, that tab does not appear at all.

Related information

Configure IVR *(on page 439)*

IVR configuration reference *(on page 443)*

Application Configuration *(on page 433)*

Configure IVR

Run the setup on the **IVR Configuration** page to point BigFix Insights for Vulnerability Remediation at its database, set the options that its service runs with, and connect the first scanner datasource. BigFix UI reports the application as **Configured** only after the background processes that the setup starts finish successfully.

Confirm that the prerequisites in IVR settings *(on page 437)* are met: the BigFix Insights for Vulnerability Remediation site is enabled and licensed, its version is greater than 0, and your role grants access to the application.

Collect the following before you start:

- The host, port, database name, and schema name of the BigFix UI database, and the credentials of a database user who can create a schema in it. Alternatively, an ADO.NET connection string for that database.
- The protocol, local web server port, and permitted cross-origin values that the IVR service runs with.

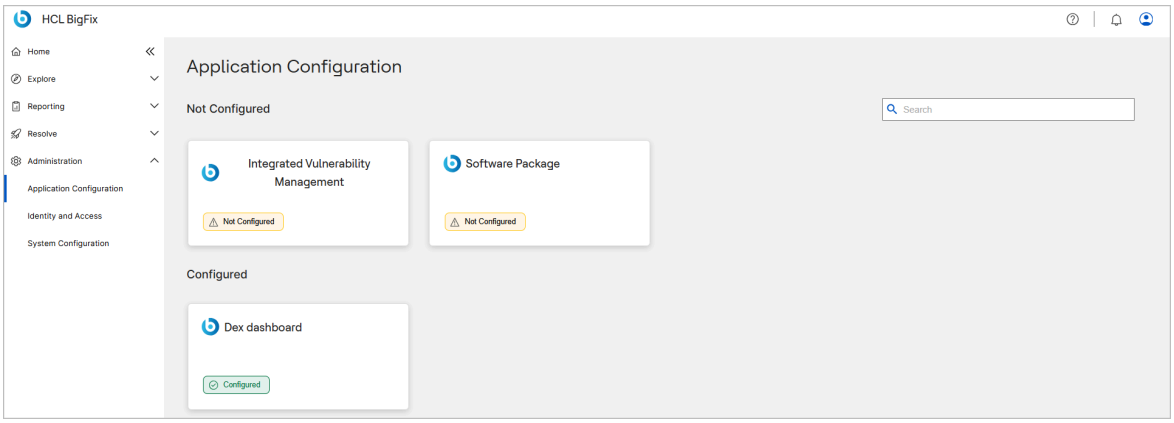
- The host, port, and credentials of your outbound proxy, if IVR reaches the scanner through one.
- The cloud URL, access key, and secret key of the scanner that you want to import from.

Important: The setup creates a new schema inside the existing BigFix UI database. The database user that you supply must hold the privilege to create a schema, or the connection test fails.

The setup has four steps: **Database Configuration**, **Application configuration**, **Scanner Datasource configuration**, and **Summary**. A stepper at the top of the page shows which step you are on. You do not configure the server here; the IVR service sets those values itself.

Each step validates against the system it describes before it lets you continue. Use **Verify Connection** on a step to test the values that you entered, and correct them there rather than at the end. Every field on a step is required, as the page states.

1. Expand **Administration** in the side navigation, and then select **Application Configuration**.



2. In the **Not Configured** group, select the **Integrated Vulnerability Management** card.

   Use the search box in the upper right to find the card by name.

   The **IVR Configuration** page opens on the first setup step.

3. On the **Database Configuration** step, read the **IVR schema setup in BFUI Database** banner.

   The banner states what this step does: the setup creates a new IVR schema inside the database that BigFix UI already uses. You are not creating a database here, and you are not pointing IVR at a database of its own. You are naming the BigFix UI database and the new schema to add to it.

   The page also states that all fields are required.

4. From the **Database Type** list, select how you want to identify the database.

- **Microsoft SQL Server** – Enter the server, port, credentials, and database name in separate fields. Choose this if you know these values individually.
- **Provide your own DSN** – Enter one ADO.NET connection string. Choose this if your database administrator gave you a connection string, or if you need Windows authentication, which the separate fields do not offer.

The fields below the list change to match your choice. If you switch between the two options, re-check the fields that remain.

5. **Optional:** If you selected **Microsoft SQL Server**, enter the connection values.

   a. In **SQL Server**, enter the host name or IP address of the server that hosts the BigFix UI database.

      Use the same server that BigFix UI itself connects to. Pointing IVR at a different server creates the schema in the wrong place, and IVR finds no BigFix data to correlate its findings against.

   b. In **SQL Server Port**, enter the port that the database server listens on.

      The default for Microsoft SQL Server is `1433`. If your deployment uses a named instance or a non-default port, ask your database administrator.

   c. In **Database User** and **Database User Password**, enter the credentials that IVR connects with.

      This account must be able to create a schema in the BigFix UI database. An account with read-only or data-only rights passes a plain login test but fails when the setup tries to create the schema.

      IVR stores these credentials and reuses them for every connection, so use a service account rather than a personal one.

   d. In **Database Name**, enter the name of the existing BigFix UI database.

      This database must already exist. The setup does not create it.

6. **Optional:** If you selected **Provide your own DSN**, enter an ADO.NET connection string in the **DSN** field.

   Only Microsoft SQL Server connection strings are supported, and the database that the string names must already exist. The help text above the field gives two examples, one for SQL Server authentication and one for Windows authentication:

   - SQL Server authentication:

     ```
     server=192.168.0.5;database=myDataBase;user=myUsername;password=myPassword;port=1433
     ```

   - Windows authentication: `Server=192.168.0.5;Database=myDataBase;Integrated Security=True;Trusted_Connection=True`

   Note: The connection string contains the password in plain text. Follow your organization's handling rules when you copy it from another system.

7. In **Database Schema Name**, enter a name for the schema that the setup creates.

This field appears for both database types. Use a name that identifies the schema as belonging to IVR, and keep a record of it: administrators need it later when they query or back up the IVR data.

Use a name that does not already exist in the database. Reusing the name of an existing schema can cause the setup to fail.

8. Select **Verify Connection**.

   The control stays unavailable until every required field holds a value. Always verify before you continue: a wrong value that you carry forward surfaces later as a failed background process, which is harder to trace back to its cause.

   BigFix UI connects to the database server with the values that you entered and reports whether it succeeded. If the test fails, check the following before you try again:

   - The server name and port are correct, and the database server accepts connections from the BigFix UI server.
   - The database that you named exists on that server.
   - The credentials are valid and the account can create a schema.
   - For a DSN, the string is well formed and names a Microsoft SQL Server database.

   If the test keeps failing with values that you believe are correct, a firewall between the BigFix UI server and the database server is a common cause. Confirm that the port is open in that direction.

9. Select **Next**.
10. On the **Application configuration** step, set the options that the IVR service runs with.
    a. In **Web protocol**, enter the protocol that the service serves on.
    b. In **Local web server port**, enter the port that the service listens on.
    c. In **CORS allowed origins**, enter the origins that may call the service.
    d. To run IVR as a Windows service, select **Install the application as a Windows Service**.

       Installing the application as a Windows service requires administrative privileges.

    e. If IVR reaches the scanner through a proxy, turn on **Setup proxy**, and then enter the proxy host, port, user name, and password.

       The proxy host and port are required when the toggle is on. Leave the toggle off for a direct connection.

    f. Select **Verify Connection**.
11. Select **Next**.
12. On the **Scanner Datasource configuration** step, connect the scanner that IVR imports findings from.

a. From the **Create a New Datasource** list, select **Tenable IO**.

b. In **Tenable cloud url**, enter the URL of your Tenable instance.

c. In **Tenable access key** and **Tenable secret key**, enter the API keys of the Tenable account that IVR reads with.

Generate the keys in Tenable, from the API keys section of your user profile. IVR stores them; it cannot retrieve them from Tenable for you.

d. In **Alias**, enter a name that identifies this datasource in the datasource list.

e. Select **Verify Connection**.
BigFix UI calls the scanner with the credentials that you entered and reports whether the connection succeeded.

You can add more datasources later from the **View Configuration** page.

13. Select **Next**.

14. On the **Summary** step, review every value that you entered.

The summary groups the values as **Server Configuration**, **Database Configuration**, and **Application Configuration**, and lists the datasources beneath them. To correct a value, return to the step that holds it by selecting that step in the stepper at the top of the page.

15. Select **Finish**.

BigFix UI saves the configuration and starts three background processes that build the IVR data set. The page returns to **Application Configuration**.

When all three background processes complete successfully, the **Integrated Vulnerability Management** card moves to the **Configured** group and its status chip reads **Configured**. IVR then appears under **Resolve** and returns data.

If a process does not complete, the card stays in the **Not Configured** group and BigFix UI displays a message telling you to check the BigFix UI and IVR logs and then select **Finish** again to restart the service. Reopen the card, correct any values that the logs identify, and run the setup again.

To review or change the saved values, or to connect another scanner, reopen the card and work from **View Configuration**. For a description of every value, see IVR configuration reference *(on page 443)*.

IVR configuration reference

Descriptions of the values on the **IVR Configuration** page, the fields on each setup step, the columns of the datasource list, and the configuration statuses.

Configuration statuses

Table 79. Status of the Integrated Vulnerability Management card

Status	Meaning
Not Configured	The setup has not run, or it ran and at least one of the background processes that it started did not complete. Selecting the card opens the setup so that you can correct the values and run it again.
Configured	The setup ran and every background process completed successfully. Selecting the card opens **View Configuration**.

Steps of the setup

The **IVR Configuration** page runs the setup as four steps. A stepper at the top of the page shows the current step. There is no server configuration step; the IVR service sets those values itself.

Table 80. Setup steps

Step	What you supply
1. **Database Configuration**	The database that IVR writes its schema into, given either as individual values or as a DSN connection string, and the name of the schema to create.
2. **Application configuration**	The options that the IVR service runs with, including the web protocol, the local web server port, the cross-origin policy, the Windows service option, and the proxy settings.
3. **Scanner Datasource configuration**	The first scanner that IVR imports vulnerability findings from.
4. **Summary**	Nothing. The step lists every value that you entered so that you can review it before you complete the setup.

Cancel and **Next** appear at the foot of each step. **Verify Connection** appears on the steps that connect to another system, and tests the values that you entered before you continue.

Server configuration panel

The IVR service sets these values. The panel reports them and offers no **Edit** control.

Table 81. Server configuration values

Value	Description
IVR Server address	Host name or IP address of the server that runs the IVR service.
Basic Auth port	Port on which the service accepts basic authentication.
mTLS port	Port on which the service accepts mutual TLS authentication.

Table 81. Server configuration values (continued)

Value	Description
SANs	Subject alternative names on the certificate that the service presents.

Application configuration panel

Select **Edit** on the panel to change these values. The panel labels each value with the key that the IVR service uses.

Table 82. Application configuration values

Key in the panel	Field in the setup	Description
webProtocol	**Web protocol**	Protocol that the IVR service serves on, for example `https`.
localWebServerPort	**Local web server port**	Port that the IVR web server listens on.
cors	**CORS allowed origins**	Origins that are permitted to call the service across origins. A value of `*` permits all origins.
windowsService	**Install the application as a Windows Service**	Reports whether IVR is installed as a Windows service. Installing it as a service requires administrative privileges.
isProxyEnabled	**Setup proxy**	Reports whether IVR reaches the scanner through a proxy. When `false`, the remaining proxy values are empty.
proxyServerHost	**Proxy server host**	Host name or IP address of the proxy. Required when the proxy is enabled.
proxyServerPort	**Proxy server port**	Port that the proxy listens on. Required when the proxy is enabled.
proxyUsername	**Proxy server username**	User name that IVR authenticates to the proxy with. The matching password is stored but not displayed.

Database Configuration panel

Select **Edit** on the panel to change these values.

Table 83. Database configuration values

Key in the panel	Field in the setup	Description
dbType	**Database Type**	Type of the database server that holds the BigFix UI database. The list offers **Microsoft SQL Server** and **Provide your own DSN**. The remaining fields on the step change to match your choice.
dbHost	**SQL Server**	Host name or IP address of the database server.
dbPort	**SQL Server Port**	Port that the database server listens on.

Table 83. Database configuration values (continued)

Key in the panel	Field in the setup	Description
dbUser	**Database User**	User that IVR connects to the database as. This user must hold the privilege to create a schema. The matching password, **Database User Password**, is stored but not displayed.
dbName	**Database Name**	Name of the existing BigFix UI database that IVR writes its schema into.
schemaName	**Database Schema Name**	Schema that the setup creates inside the BigFix UI database to hold the IVR data.
dsn	**DSN**	The connection string that IVR uses. BigFix UI assembles it from the other values, or uses the ADO.NET connection string that you supply when you select **Provide your own DSN** in **Database Type**. Only Microsoft SQL Server DSN strings are supported, and the database must already exist.

Important: The setup creates a *new* schema inside the *existing* BigFix UI database. It does not create a database.

When you select **Provide your own DSN**, the step shows only the **DSN** and **Database Schema Name** fields. The page gives two example strings, one using SQL Server authentication and one using Windows authentication.

Scanner datasource fields

These fields appear on the **Scanner Datasource configuration** step and when you select **Add datasource** on **View Configuration**. All of them are required.

Table 84. Datasource fields for Tenable IO

Field	Description
Create a New Datasource	Type of scanner to connect to. The fields below it change to match the type that you select.
Tenable cloud url	URL of your Tenable instance, for example `https://cloud.tenable.com`.
Tenable access key	Access key of the Tenable account that IVR reads with. Generate it in Tenable, from the API keys section of your user profile.
Tenable secret key	Secret key that pairs with the access key. Generated at the same time and in the same place.
Alias	Name that identifies this datasource in the datasource list.
Verify connection	Calls the scanner with the values that you entered and reports whether the connection succeeded.

Datasource list

Table 85. Columns of the Datasource list

Column	Description
Type	Scanner type of the connection, for example `TENABLE IO`.
Target	URL of the scanner instance that IVR imports from.
Alias	Identifier of the connection.
Action	Holds an edit control, which reopens the datasource fields, and a delete control, which removes the connection.

Select **Add datasource** above the list to connect another scanner.

Messages

Table 86. Messages that the configuration can return

Message	Where it appears	What to do
A message reporting that a background process stopped unexpectedly and directing you to the BigFix UI and IVR logs.	The **IVR Configuration** page, after you select **Finish**.	Review the logs, correct any values that they identify, and select **Finish** again to restart the service.
IVR unavailable – Something went wrong, please contact your administrator.	An IVR page under **Resolve**.	Confirm that the application shows as **Configured** in Application Configuration and that the IVR service is running.

Identity management

The Identity management app in BigFix UI is the central place to manage global settings for all applications running within BigFix UI. From here, administrators manage users, roles, account policies, and identity provider configuration.

Note: The Identity management app is visible only to administrators. Ensure you are logged in as an administrator to access this app.

Accessing Identity management

To open the app, expand **Administration** from the side navigation, and then select **Identity Management**. The Identity management landing page displays the **Identity and access** group of cards.

The cards and the side navigation items that you see depend on the account you log in with.

Figure 1. Identity management as the instance admin



Figure 2. Identity management as an administrator



Use the **Search all settings** field to find a setting by name. Turn on **Open list view** to display the cards as a list.

Identity and access

Select a card to open the corresponding settings area. The cards that are displayed depend on how you are logged in. The instance admin sees the **Admin user and account policy** and **OIDC Configuration** cards. Administrators see the **User & Role Management** card.

Table 87. Identity and access cards

Card	Description	Visible to
User & Role Management	Create and manage users and roles to control access to BigFix applications. For details, see User & Role Management *(on page 449)*.	Administrators
Admin user and account policy	Create the primary site administrator and configure account security policies. For details, see Admin user and account policy *(on page 484)*.	Instance admin only
OIDC Configuration	Configure OpenID Connect (OIDC) for single sign-on authentication with your identity provider. For details, see OIDC Configuration *(on page 492)*.	Instance admin only

Note: The **Admin user and account policy** and **OIDC Configuration** cards appear only when you are logged in as the instance admin.

Related information

User & Role Management *(on page 449)*

Creating a new user *(on page 454)*

Managing Roles *(on page 467)*

Admin user and account policy *(on page 484)*

OIDC Configuration *(on page 492)*

User & Role Management

The User & Role Management area of Identity management provides administrators with a centralized interface to manage user accounts, roles, permissions, and activities. This section walks you through the process of creating new users, disabling or deleting existing users, setting passwords, managing roles, and more.

Note: User & Role Management is visible only to administrators. Ensure you are logged in as an administrator to access this area.

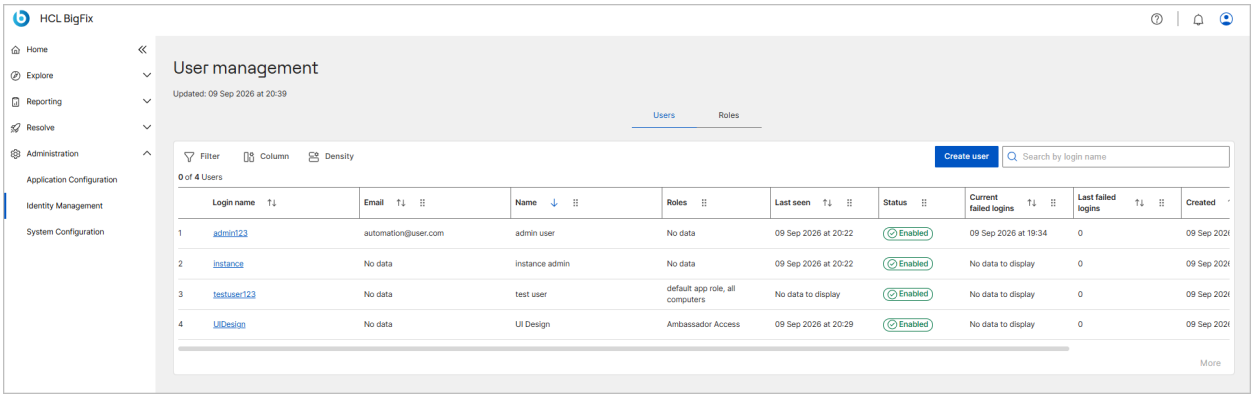
Key features

- **User account management**
  - **User Creation and Registration**: Admins can create new user accounts manually.
  - **Account Activation/Deactivation**: Admin users can enable or disable user accounts as needed.
  - **User Activity Insights**: Track login history, failed login attempts, and access status.
  - **BigFix operator binding**: Bind each user to a BigFix operator from which the user inherits device and platform permissions.
- **Role-based application access**:
  - **Role Assignment:** Assign one or more custom roles to users, granting them access to appropriate applications, devices, and sites.
  - **Granular Permission:** Configure specific access levels (**Admin**, **Users**, or **Read only**) and feature rights for the Reporting application when creating or editing a role.
  - **Operational permissions:** Define what a role or user can do on the platform, such as creating actions or using the Console, WebUI, or REST API. See Permissions reference *(on page 482)*.
- **Authentication and Security**
  - **Authentication Management**: Support for both Local and Identity Provider (IdP) authentication methods
  - **Password Requirements**: Enforce strong password, including complexity requirements and expiration periods.
  - **Profile Customization**: Users can view or edit their personal information and update passwords securely.

User management

The User management page provides administrators with a centralized view of all users who have access to the BigFix UI.

To access the page, expand **Administration** from the side navigation, select **Identity Management**, and then select the **User & Role Management** card. By default the **Users** tab is displayed:



Use the **Filter**, **Column**, and **Density** controls above the user grid to narrow down the list of users, customize the columns that are displayed, and adjust the row spacing. Use the **Search by login name** field to quickly locate a specific user. For more information, see Table filter *(on page 40)*, Columns *(on page 29)*, and Density *(on page 29)*.

The user grid displays the following details for each user:

Table 88. Users grid columns

Column	Description
Login Name	The name the user signs in with. Click a login name to open the user details page.
Email	The email address of the user.
Name	The full name of the user.
Roles	The roles assigned to the user.
Last seen	The date and time when the user last accessed BigFix UI.
Status	Indicates whether the user account is **Enabled** or **Disabled**.
Current failed logins	The date and time of the most recent failed login attempt in the current observation window.
Last failed logins	The number of failed login attempts recorded before the last successful login.
Created	The date and time when the user account was created.

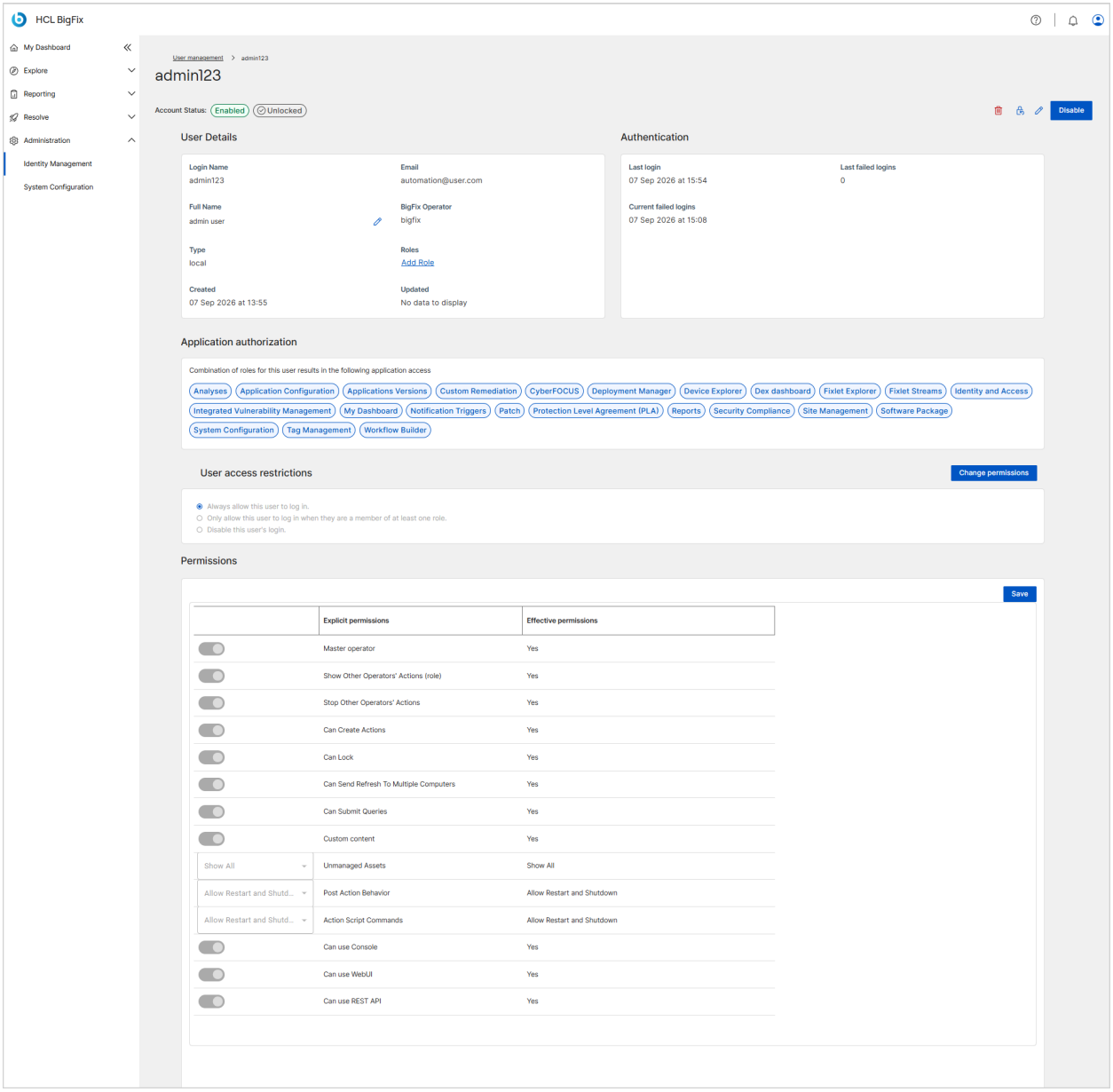
Administrators can create new users directly from the **Users** tab by selecting **Create user**. The guided flow allows you to:

- Select an authentication method (Identity provider (Idp) or Local).
- Add the user's basic information and, for local users, the password.
- Define the user as Administrator or Non Administrator, bind the user to a BigFix operator, and assign one or more roles.
- Review and confirm access permissions.

After creation, users appear in the main table where administrators can manage roles, enable/disable access, or delete accounts. For detailed steps, see Creating a new user *(on page 454)*.

User details and actions

From the **Users** tab, clicking a **Login Name** opens the user details page, where administrators can view and manage individual user information.



The **Account Status** badges indicate whether the account is Enabled or Disabled, and Locked or Unlocked. The actions in the upper-right corner let you **Delete** the user, **Reset password**, **Edit user profile**, and **Disable** or **Enable** the account. For details, see Editing user profile *(on page 463)*.

The user details page is organized in the following sections:

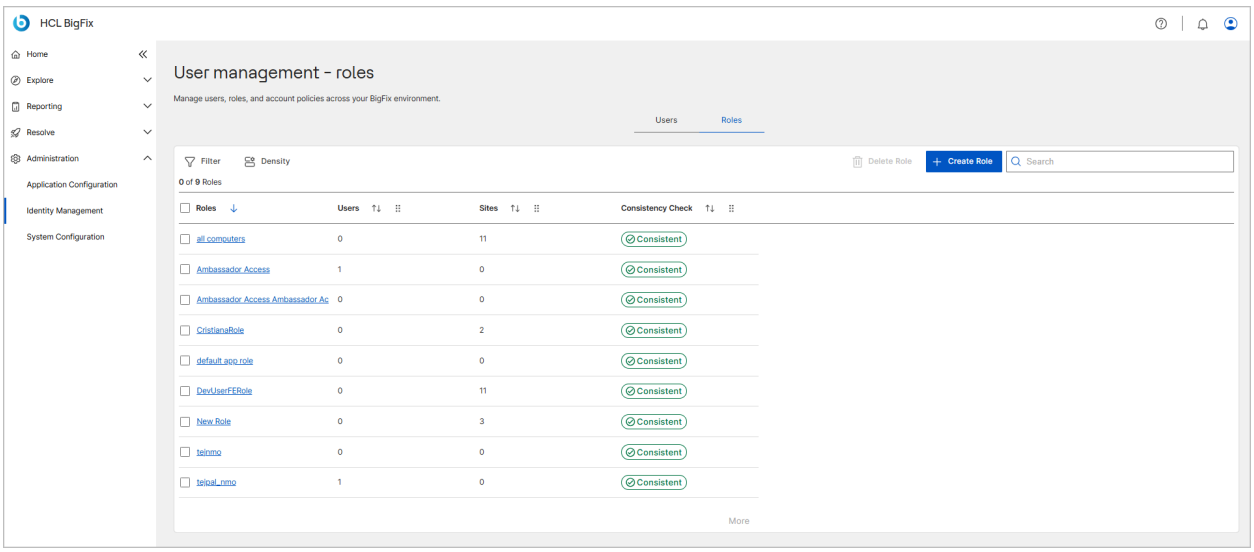
Table 89. User details page sections

Section	Description
User Details	Login Name, Email, Full Name (click the pencil icon to edit it inline), BigFix Operator bound to the user, Type (for example, local), Roles, and the Created and Updated timestamps. Click **Add Role** under **Roles** to assign a role to the user.
Authentication	Last login, Last failed logins, and Current failed logins.
Application authorization	The combination of roles for this user results in the listed application access. Each application the user can open is shown as a tag.
User access restrictions	Controls when the user can log in: **Always allow this user to log in**, **Only allow this user to log in when they are a member of at least one role**, or **Disable this user's login**. Click **Change permissions** to modify the selection.
Permissions	A table of **Explicit permissions** that you can grant to the user directly, next to the resulting **Effective permissions**. Click **Save** to apply changes. For the list of permissions, see Permissions reference *(on page 482)*.

Role management

The **Roles** tab provides a centralized interface for managing access control across the BigFix environment. Administrators can create new roles, modify existing ones, and associate users based on their operational responsibilities. Each role defines access to specific applications, devices, sites, and permissions.

To access this page, open **User & Role Management** and select the **Roles** tab. The **User management - roles** page is displayed:



The roles grid displays the following details for each role:

Table 90. Roles grid columns

Column	Description
Roles	The role name. Click a role name to open the role details page.
Users	The number of users assigned to the role.
Sites	The number of sites the role has access to.
Consistency Check	Indicates whether the role definition on the BigFix platform and its application permissions in BigFix UI are in sync. A **Consistent** badge means no discrepancy was found.

From this page, administrators can:

- Create new roles through a guided wizard that includes Devices, Applications, Permissions, Sites, and Summary steps.
- View and manage existing role details, including users, devices, applications, permissions, and sites.
- Select one or more roles using checkboxes and click **Delete Role** to delete them, if required.

For detailed steps, see Managing Roles *(on page 467)*.

Related information

Identity management *(on page 447)*

Creating a new user *(on page 454)*

Managing Roles *(on page 467)*

Editing user profile *(on page 463)*

Permissions reference *(on page 482)*

Creating a new user

Use the Create user wizard in User & Role Management to add new users in BigFix UI. You define how users authenticate, bind them to a BigFix operator, assign their roles, and review the applications they can access.

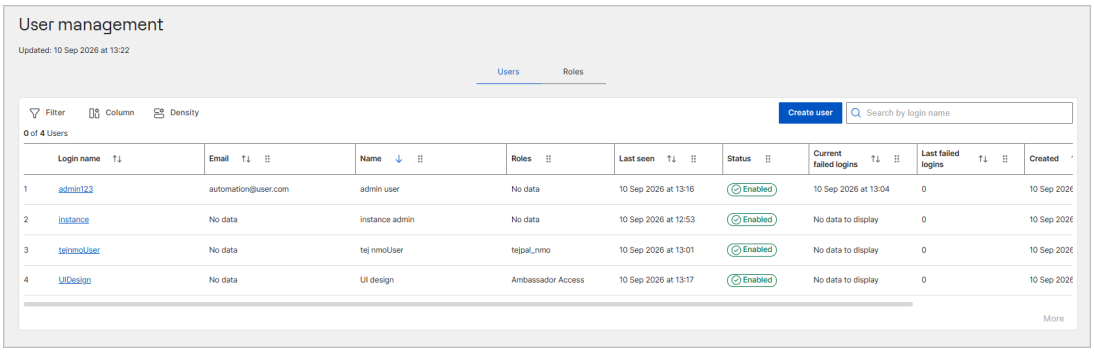
- User & Role Management is visible only to administrators. Ensure you are logged in as an administrator.
- A BigFix operator must exist for each user that you create. The user is bound to the operator and inherits its permissions.

Administrators create new users from the **Users** tab of User & Role Management. Clicking **Create user** opens a guided three-step wizard: **User**, **Role**, and **Summary**. In the first step you select the authentication method and enter the user details. In the second step you define whether the user is an Administrator or Non Administrator, bind the user to a BigFix operator, and assign roles. In the final step you review the information and click **Create**.

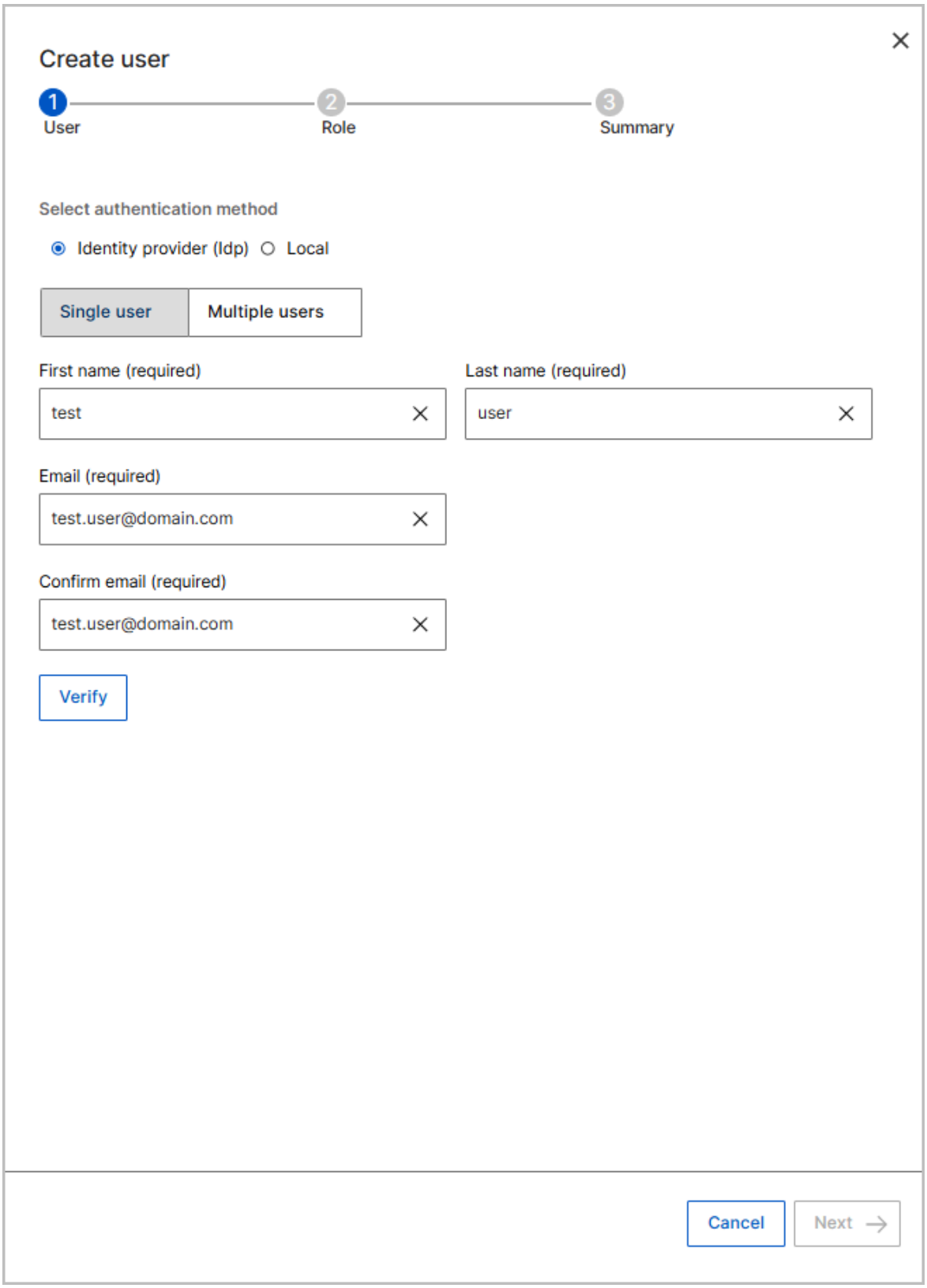
The fields on the **User** step change with the authentication method that you select. This topic describes both the **Identity provider (Idp)** method and the **Local** method.

To create a new user, complete the following steps:

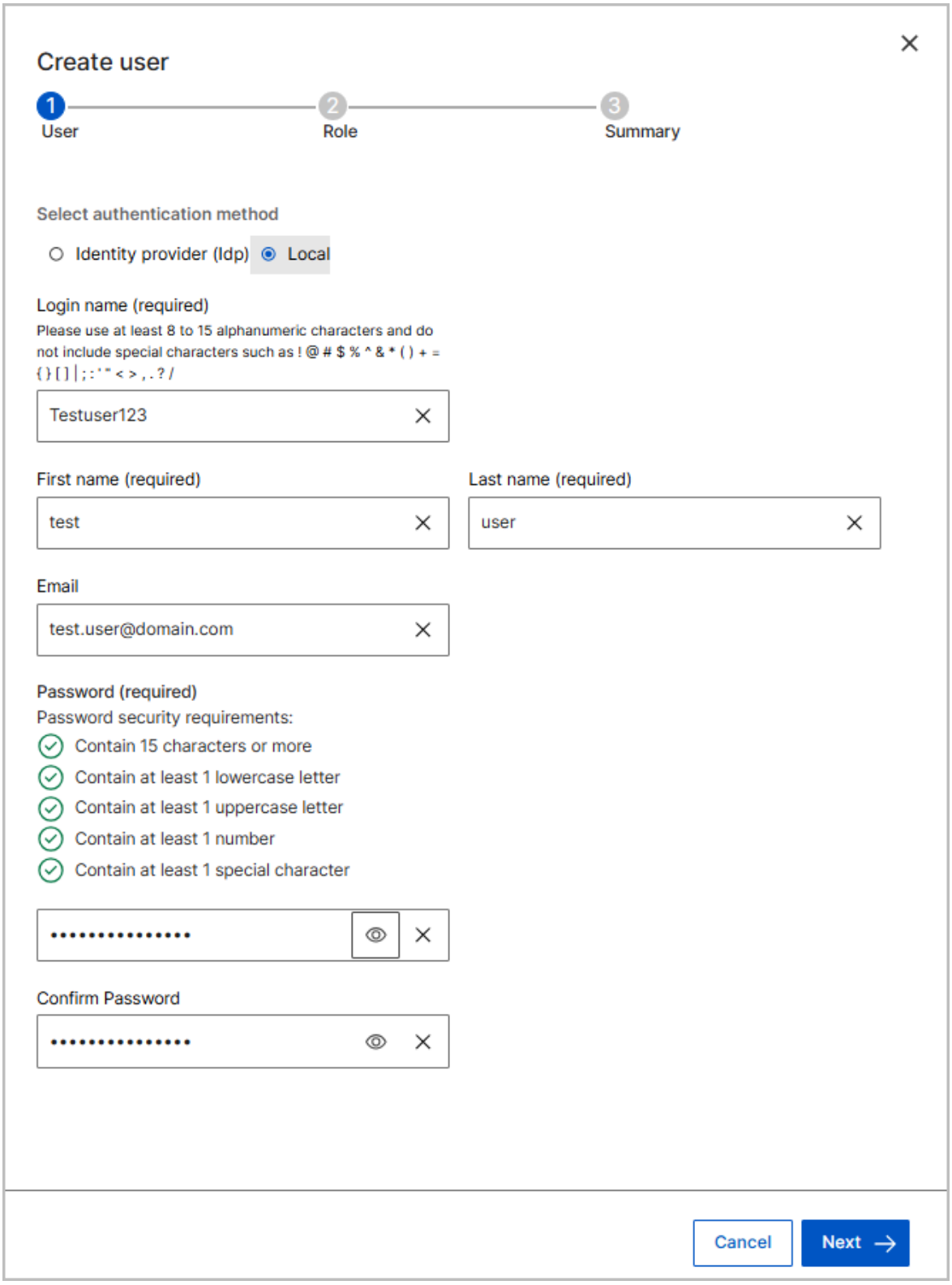
1. Access the **Create user** wizard.
    a. Log in to BigFix UI as an administrator.
    b. Expand **Administration** from the side navigation, select **Identity Management**, and then select the **User & Role Management** card.
    c. On the **Users** tab, click **Create user**. The **Create user** wizard opens on the **User** step.



2. On the **User** screen, under **Select authentication method**, select the method for the new user.
    - **Identity provider (Idp)**: Select this option if your organization manages users through an external identity provider that is configured in OIDC Configuration. The identity provider authenticates the user, so you do not set a password in BigFix UI.
    - **Local**: Select this option to create a user account that BigFix UI manages directly. You set the login name and the initial password.


Create user
1
User
2
Role
3
Summary
Select authentication method
Identity provider (Idp)
Local
Single user
Multiple users
First name (required)
test
Last name (required)
user
Email (required)
test.user@domain.com
Confirm email (required)
test.user@domain.com
Verify
Cancel
Next

3. If you selected **Local**, enter the user details.



a. Complete the following fields.

Table 91. Local user fields

Field	Description
Login Name (required)	Use at least 8 to 15 alphanumeric characters. Do not include special characters such as ! @ # $ % ^ & * ( ) + = { } [ ] | ; : ' " < > , . ? /
First name (required)	The first name of the user.
Last name (required)	The last name of the user.
Email	The email address of the user.
Password (required)	The initial password for the user. The **Password security requirements** list above the field is marked as met while you type. The password must: ▪ Contain 15 characters or more ▪ Contain at least 1 lowercase letter ▪ Contain at least 1 uppercase letter ▪ Contain at least 1 number ▪ Contain at least 1 special character
Confirm Password	Re-enter the password. Both entries must match.

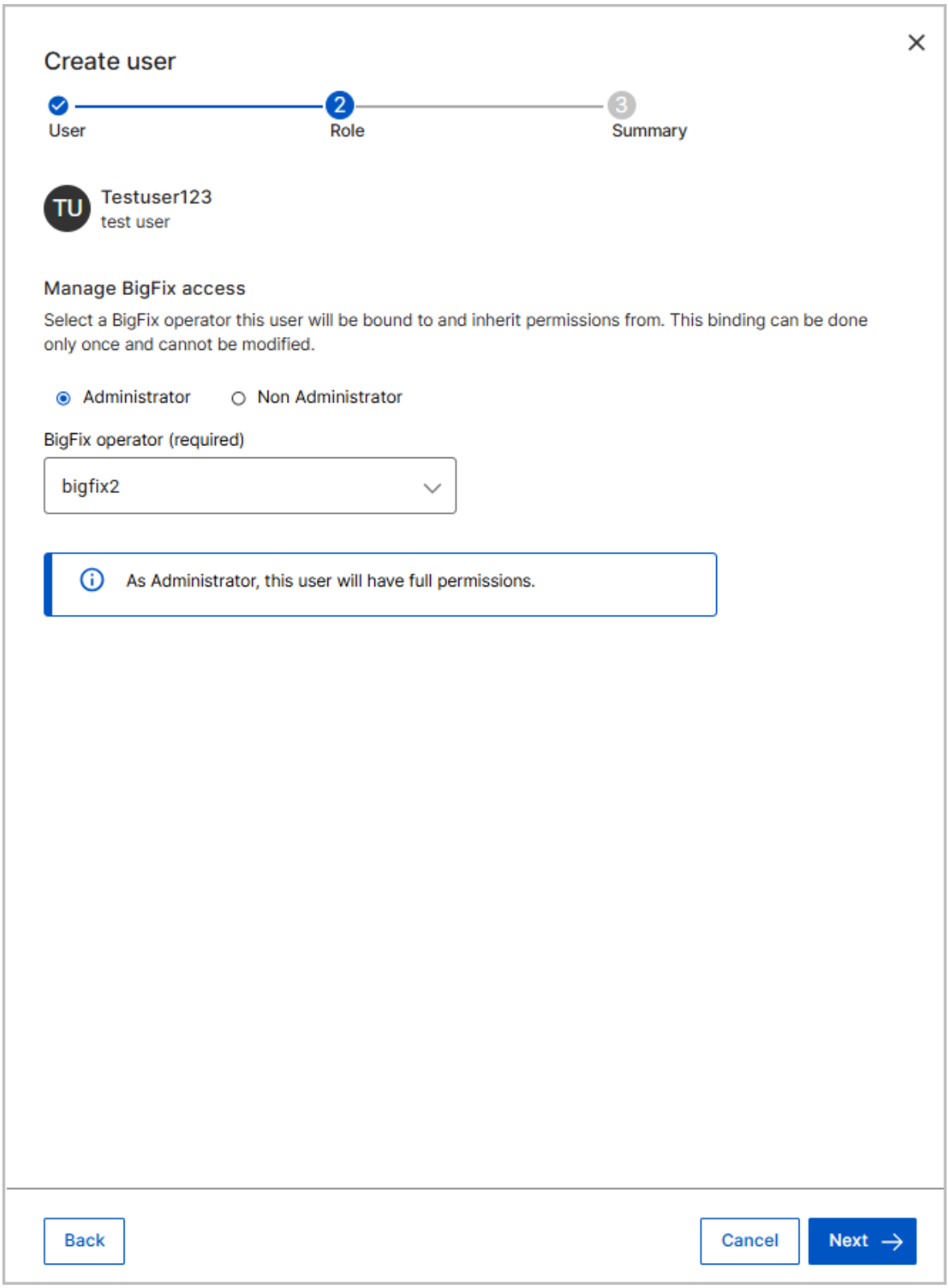
To check what you typed, click the eye icon next to a password field. To clear a field, click the **X** icon.

b. Click **Next** to open the **Role** screen.



Note: Next stays disabled until you complete all required fields and the password meets every security requirement.

4. On the **Role** screen, define BigFix access and assign roles.



The login name and full name that you entered appear at the top of the window.

a. Under **Manage BigFix access**, select **Administrator** or **Non Administrator**.

   Your choice controls which operators appear in the **BigFix operator (required)** list. In both cases, the list shows only operators that are not already bound to another user.

   - **Administrator**: The list shows only master operators. The user gets full permissions in BigFix UI and keeps master operator permissions in the platform.
   - **Non Administrator**: The list shows all available operators, including master operators. The user inherits the permissions of the operator that you select.

b. From the **BigFix operator (required)** list, select the BigFix operator that this user is bound to and inherits permissions from.

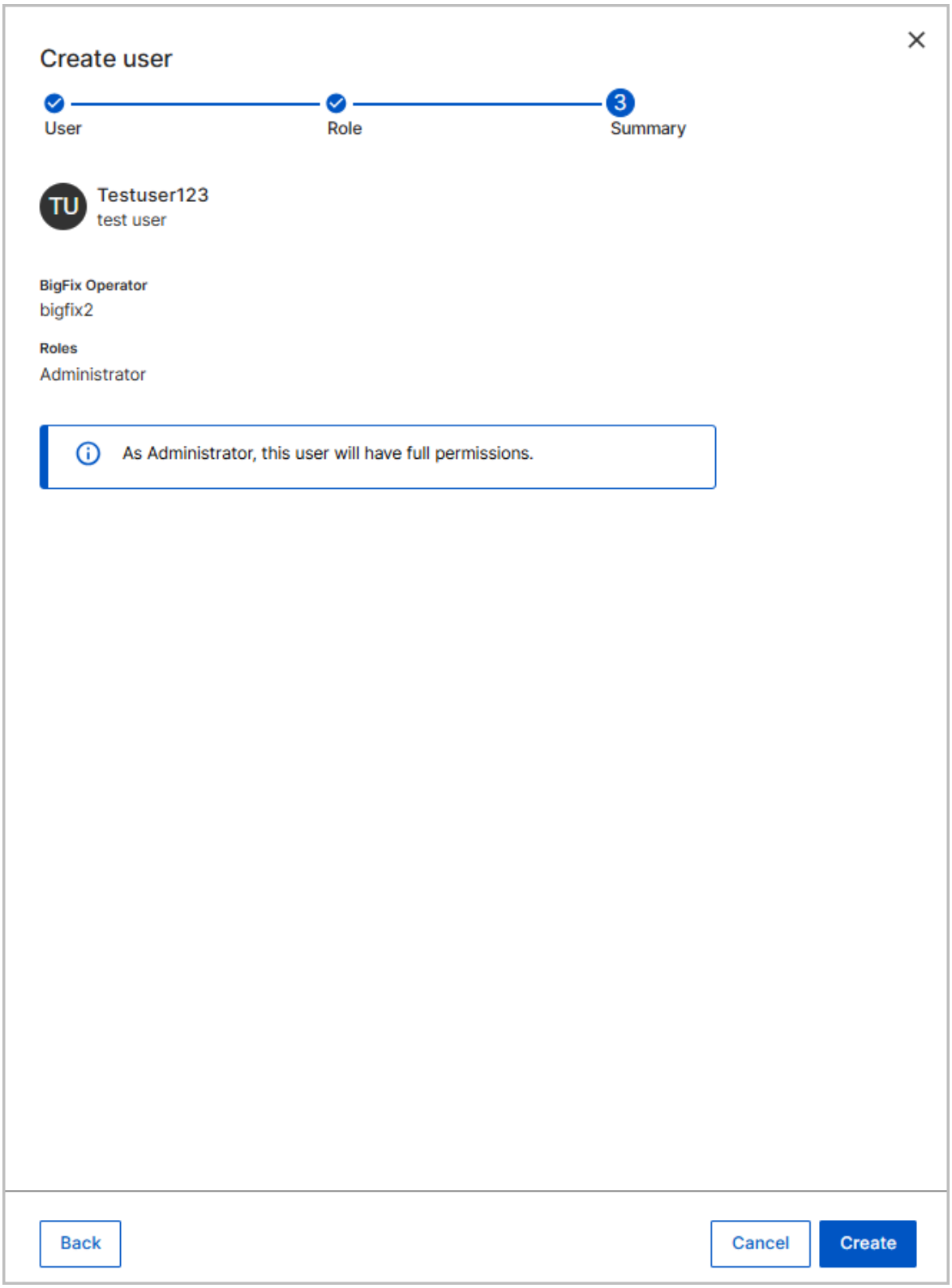
   Important: This binding can be done only once and cannot be modified after the user is created.

c. Under **Select desired role**, select the check box next to each role to assign to the user. The list shows the roles defined in your environment.

d. Review the **What applications should this role access?** section. It lists the applications the user can access based on the selected operator and roles.

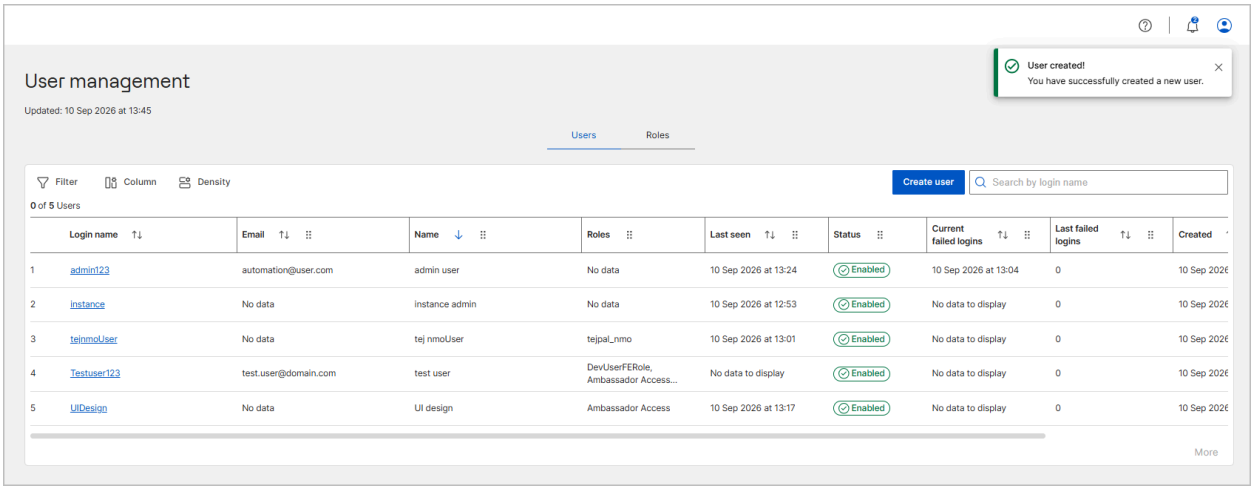
e. Click **Next** to open the Summary screen.

5. On the **Summary** screen, review and confirm the user details.


Create user
User
Role
3
Summary
TU
Testuser123
test user
BigFix Operator
bigfix2
Roles
Administrator
As Administrator, this user will have full permissions.
Back
Cancel
Create

a. Verify the login name, full name, **BigFix Operator**, **Roles**, and the applications listed under **What applications should this role access?**.
b. Click **Create**.

A **User created!** message is displayed, confirming that you have successfully created a new user. The wizard closes and the new account appears in the **Users** grid with the status **Enabled**. The user count above the grid increases by one.



The grid row shows the login name, email, name, assigned roles, status, and creation date. Click the login name to open the user details page, where you can review the application authorization, user access restrictions, and permissions.

For local users, authentication uses the password that you set in the wizard.

For IdP users, no password is set or managed in BigFix UI. Authentication is handled by the configured identity provider (IdP).

If you created a local user, share the login URL and the password with the user through a secure channel.

If you created an IdP user, the user can sign in to BigFix UI using their existing IdP credentials.

To change roles later, open the user details page and click **Add Role**, or edit the role itself. See Managing Roles *(on page 467)*.

Related information

User & Role Management *(on page 449)*

Managing Roles *(on page 467)*

Permissions reference *(on page 482)*

Editing user profile

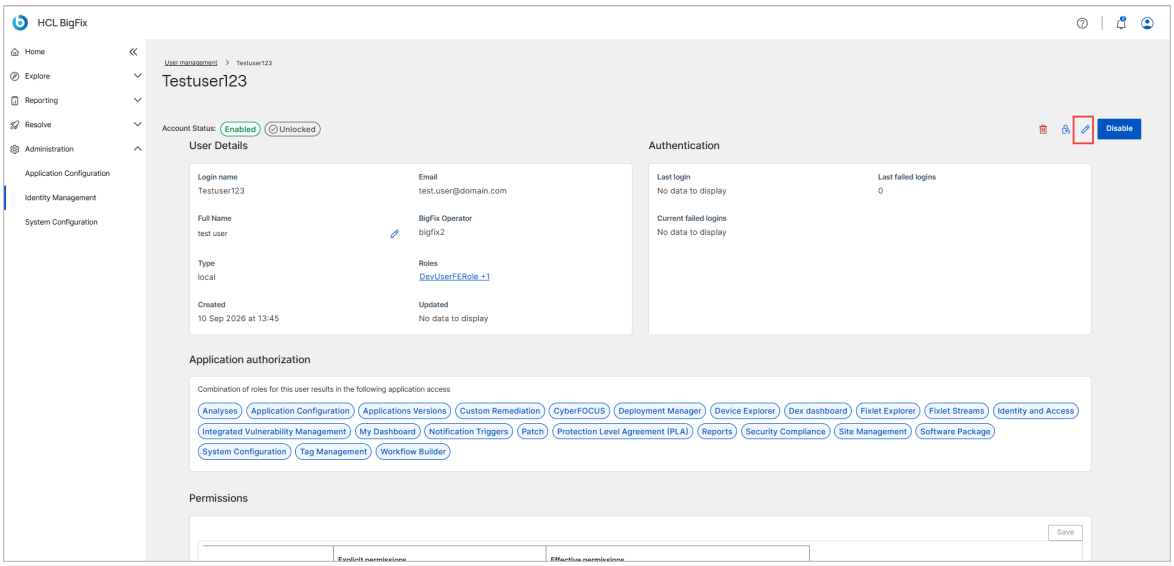
Administrators can edit user details, such as login name, email, and full name, and reset passwords directly from the user details page in User & Role Management.

Note: You must be logged in as an administrator.

Edit User Details

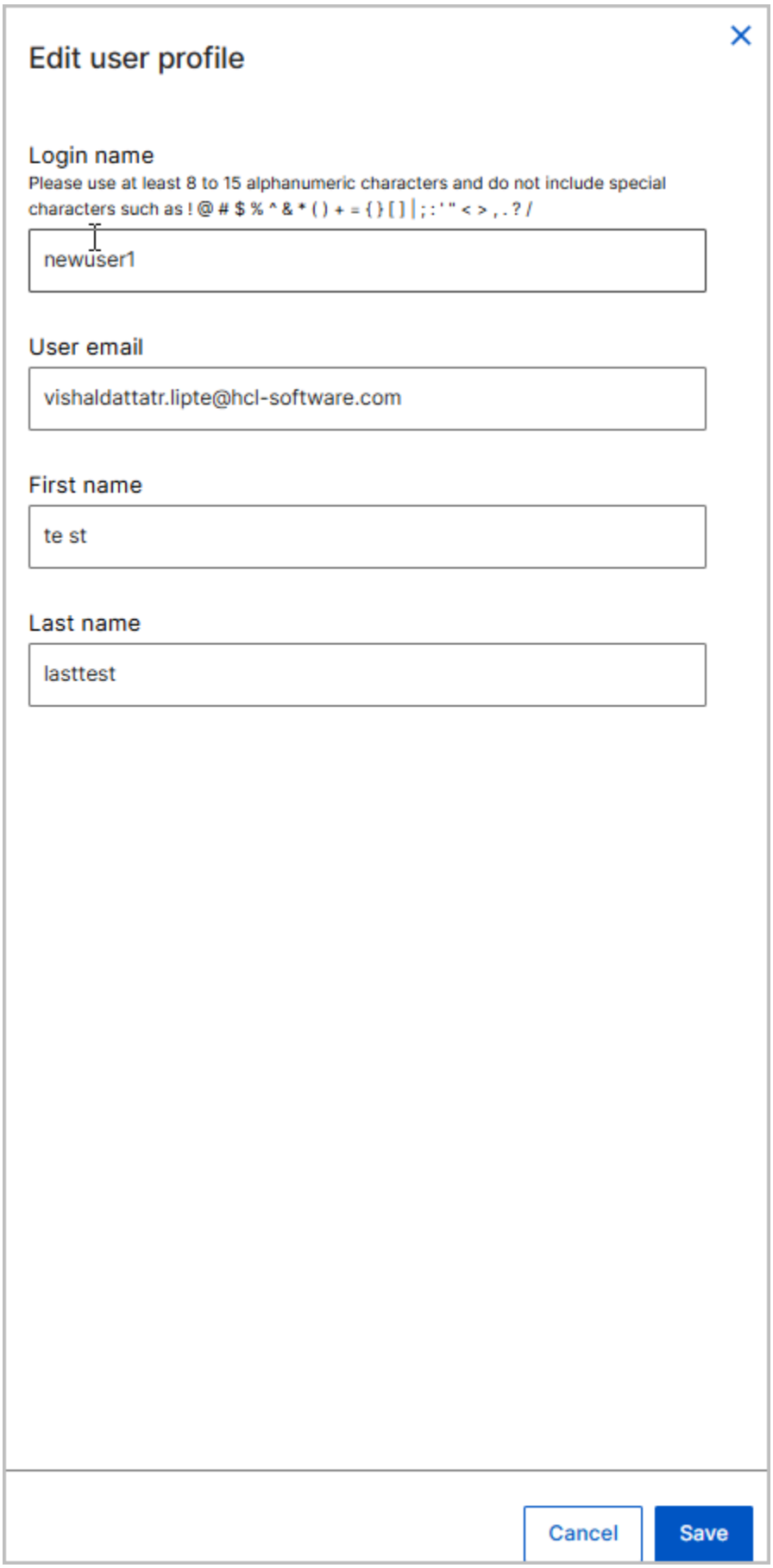
Follow these steps to modify a user's basic profile information:

1. Log in to BigFix UI with your credentials.
2. Expand **Administration**, select **Identity Management**, and then select the **User & Role Management** card.
3. On the **Users** tab, click the **login name** of the user you want to edit.
4. On the user details page, click the **Edit user profile** (pencil) icon in the top right corner.



Note: To change only the full name, you can also click the pencil icon next to **Full Name** in the **User Details** card.

5. In the **Edit user profile** panel, update the following fields as needed:


Edit user profile
Login name
Please use at least 8 to 15 alphanumeric characters and do not include special characters such as ! @ # $ % ^ & * ( ) + = { } [ ] | ; : ' " < > , . ? /
newuser1
User email
vishaldattatr.lipte@hcl-software.com
First name
te st
Last name
lasttest
Cancel
Save

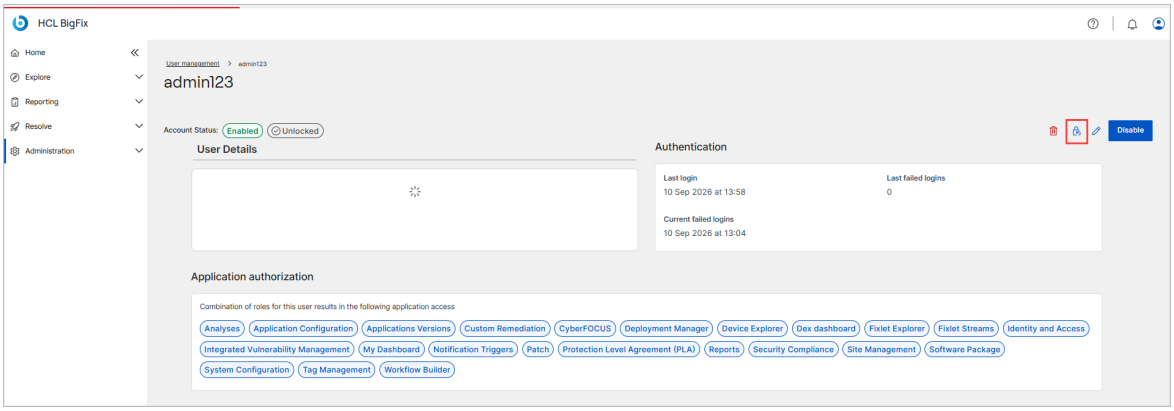
- **Login name**: Enter a name using at least 8 to 15 alphanumeric characters. Do not include special characters such as ! @ # $ % ^ & * ( ) + = { } [ ] | ; : ' " < > , . ? /.
- **User email**: Enter the user's email address.
- **First name**: Enter the user's first name.
- **Last name**: Enter the user's last name.

6. Click **Save**. The user's profile information is updated immediately.

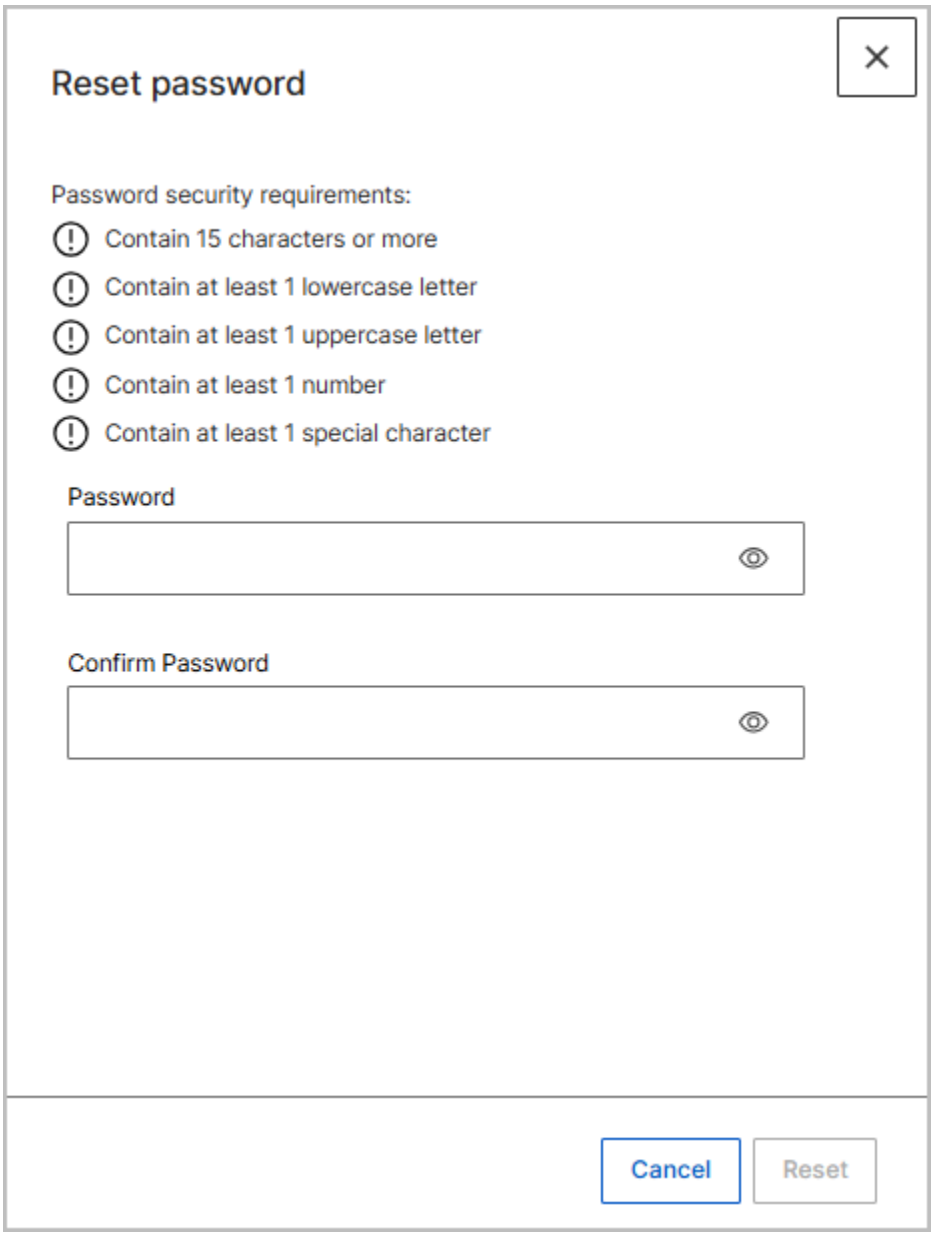
Reset a User Password

Follow these steps to manually reset a local user's password:

1. Expand **Administration**, select **Identity Management**, and then select the **User & Role Management** card.
2. On the **Users** tab, click the login name of the user whose password you need to reset.
3. On the user details page, click the **Reset password** icon in the top right corner.



4. In the **Reset password** panel, enter a new password in the **Password** field.



The panel lists the password security requirements. Each requirement is marked as met while you type. Ensure the new password meets the following criteria:

- Contains 15 characters or more
- Contains at least 1 lowercase letter
- Contains at least 1 uppercase letter
- Contains at least 1 number
- Contains at least 1 special character

5. Re-enter the password in the **Confirm Password** field.
6. Click **Reset**. The **Reset** button is enabled only after the password meets all security requirements and both entries match. The user's password is changed. The user must use the new password upon their next login.

Related information

User & Role Management *(on page 449)*

Managing Roles

Create, edit, and manage user roles with customizable access to applications, devices, sites, and permissions in the BigFix UI environment. You can customize each role by specifying app-level permissions, ensuring users have secure and appropriate access based on their responsibilities.

Note: You must be logged in as an administrator.

Roles

Roles are user-defined in BigFix UI and allow administrators to tailor permissions and access based on specific organizational requirements. Each role controls which applications, devices, and sites are accessible, and which operational permissions are granted. Roles can be edited, assigned to users, or deleted (if no users are assigned).

Roles are BigFix platform roles. The BigFix platform is the single source of truth for role definitions: roles that you create, edit, or delete in BigFix UI are created, edited, or deleted on the platform, and roles created on the BigFix Console are automatically discovered and listed in BigFix UI. Role assignment works through the BigFix operator that each user is bound to.

Administrator access is not a role. You define a user as **Administrator** or **Non Administrator** when you create the user. See Creating a new user *(on page 454)*.

A user can have multiple roles. The user's effective permissions combine all assigned roles by taking the most permissive setting for each platform permission and the highest access level for each application. See Permissions reference *(on page 482)*.

Note: When you edit or delete a role, users assigned to that role are logged out so that the updated permissions take effect at their next login.

Default and Non-Removable Applications

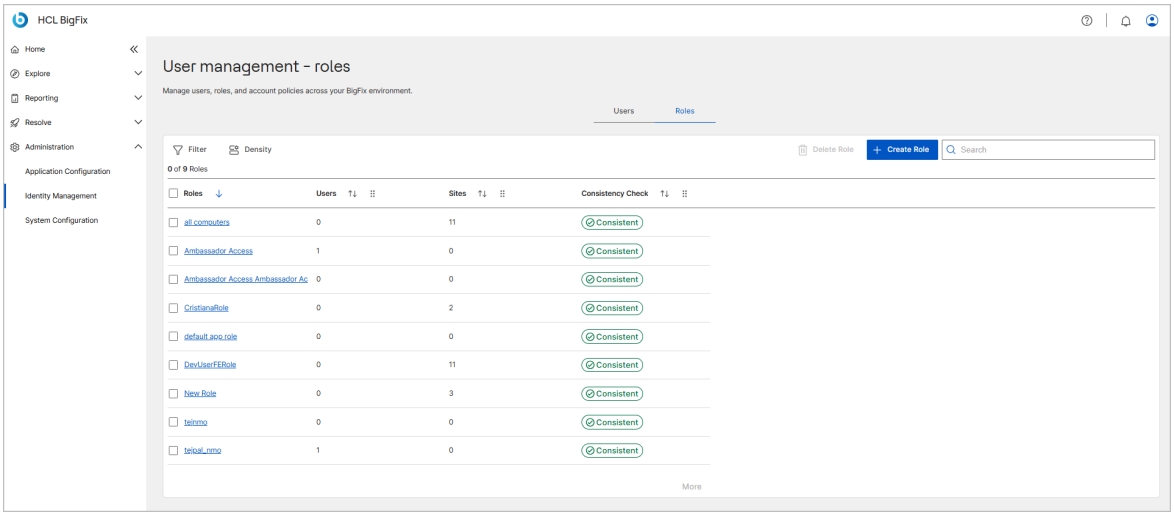
Certain applications are marked as **Default app** and are automatically assigned to every role with view access. These apps **cannot be unselected** during role creation or editing. By default, all new roles have view access to:

- Analyses
- Deployment Manager (expand **Explore** and select **Deployments**)
- Device Explorer (expand **Explore** and select **Devices**)
- Fixlet Explorer (expand **Explore** and select **Fixlets**)
- My Dashboard (home screen)
- Site Management

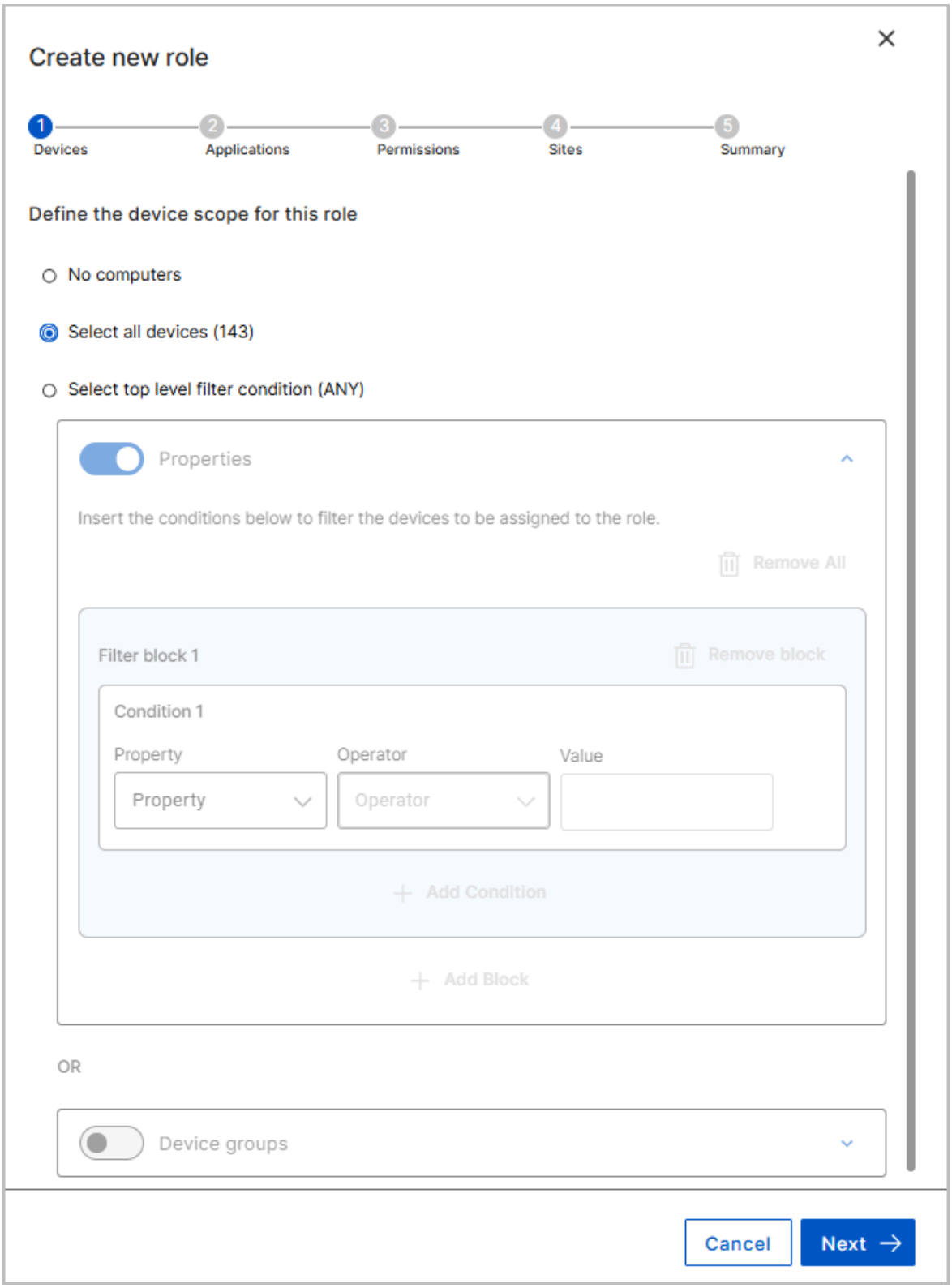
Creating a new role

Follow these steps to create a role that defines the devices, applications, permissions, and sites available to the users assigned to it:

1. Expand **Administration**, select **Identity Management**, select the **User & Role Management** card, and then select the **Roles** tab.



2. Click **Create Role**. The **Create new role** wizard opens with five steps: **Devices**, **Applications**, **Permissions**, **Sites**, and **Summary**.
3. **Devices**: Under **Define the device scope for this role**, select the devices the role can manage.



Select one of the following options:

- **No computers**: The role manages no devices.
- **Select all devices**: The role manages every device in the environment. The option shows the current device count in brackets, for example **Select all devices (143)**.
- **Select top level filter condition (ANY)**: The role manages the devices that match the filter you build. A device qualifies if it matches **any** of the sources you define.

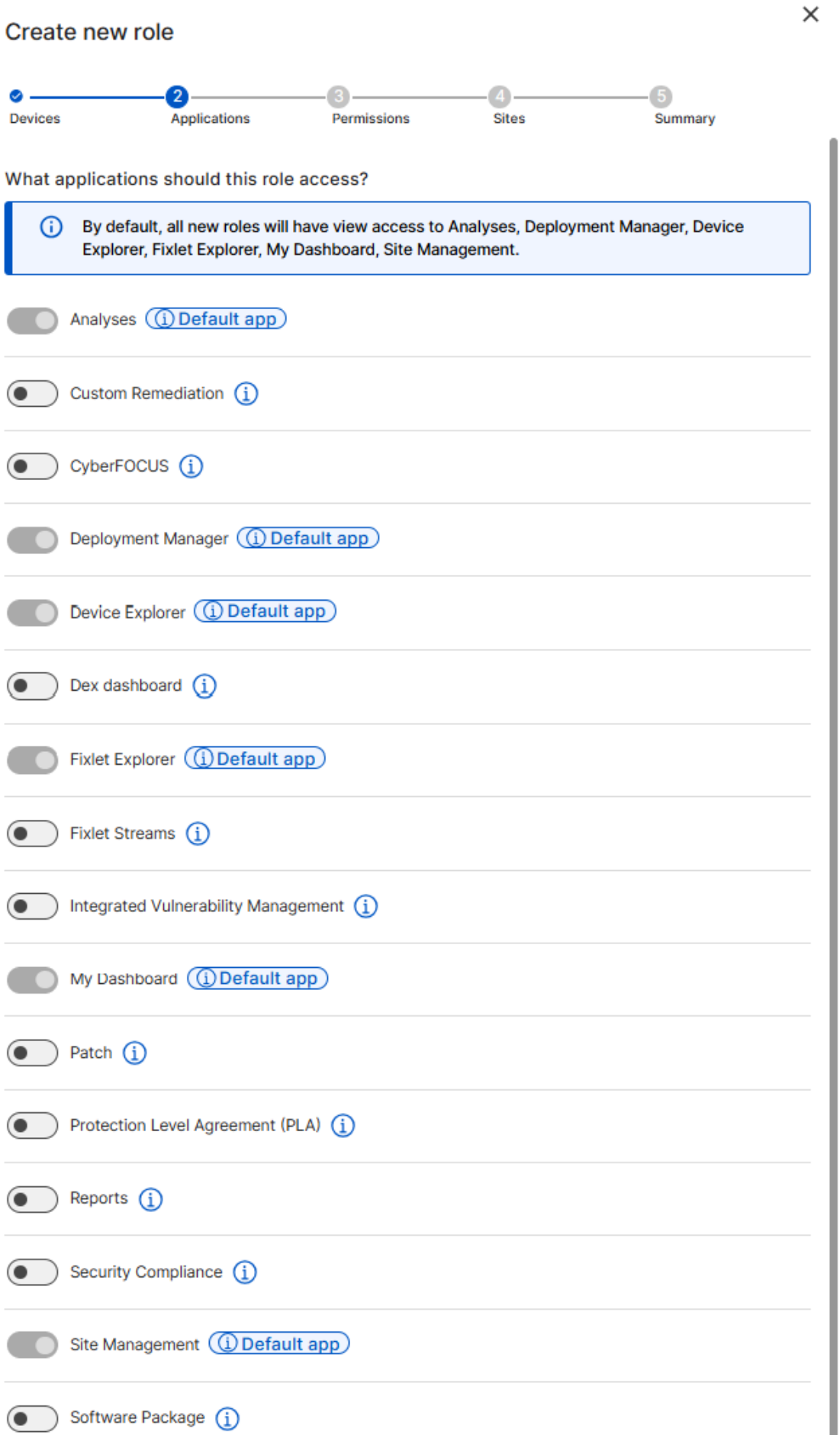
If you select **Select top level filter condition (ANY)**, build the filter with the **Properties** and **Device groups** sources. The two sources combine with **OR** logic.

- Turn on **Properties** to filter by device property. For each condition, select a **Property** and an **Operator**, and then enter a **Value**. Click **Add Condition** to add another condition to the block, or **Add Block** to add another filter block. To delete a single block, click **Remove block**. To delete every block, click **Remove All**.
- Turn on **Device groups** to filter by existing device group, and then expand the section to select the groups.

For more information about building filter conditions, see Filter by query *(on page 40)*.

Click **Next**.

4. **Applications**: Under **What applications should this role access?**, turn on the toggle for each application the role should access.


Create new role
Devices
2
Applications
3
Permissions
4
Sites
5
Summary
What applications should this role access?
By default, all new roles will have view access to Analyses, Deployment Manager, Device Explorer, Fixlet Explorer, My Dashboard, Site Management.
Analyses
Default app
Custom Remediation
CyberFOCUS
Deployment Manager
Default app
Device Explorer
Default app
Dex dashboard
Fixlet Explorer
Default app
Fixlet Streams
Integrated Vulnerability Management
My Dashboard
Default app
Patch
Protection Level Agreement (PLA)
Reports
Security Compliance
Site Management
Default app
Software Package

Note: By default, all new roles have view access to Analyses, Deployment Manager, Device Explorer, Fixlet Explorer, My Dashboard, and Site Management. The wizard repeats this information in a banner at the top of the step. The toggle for each default app is dimmed, so you cannot turn it off.

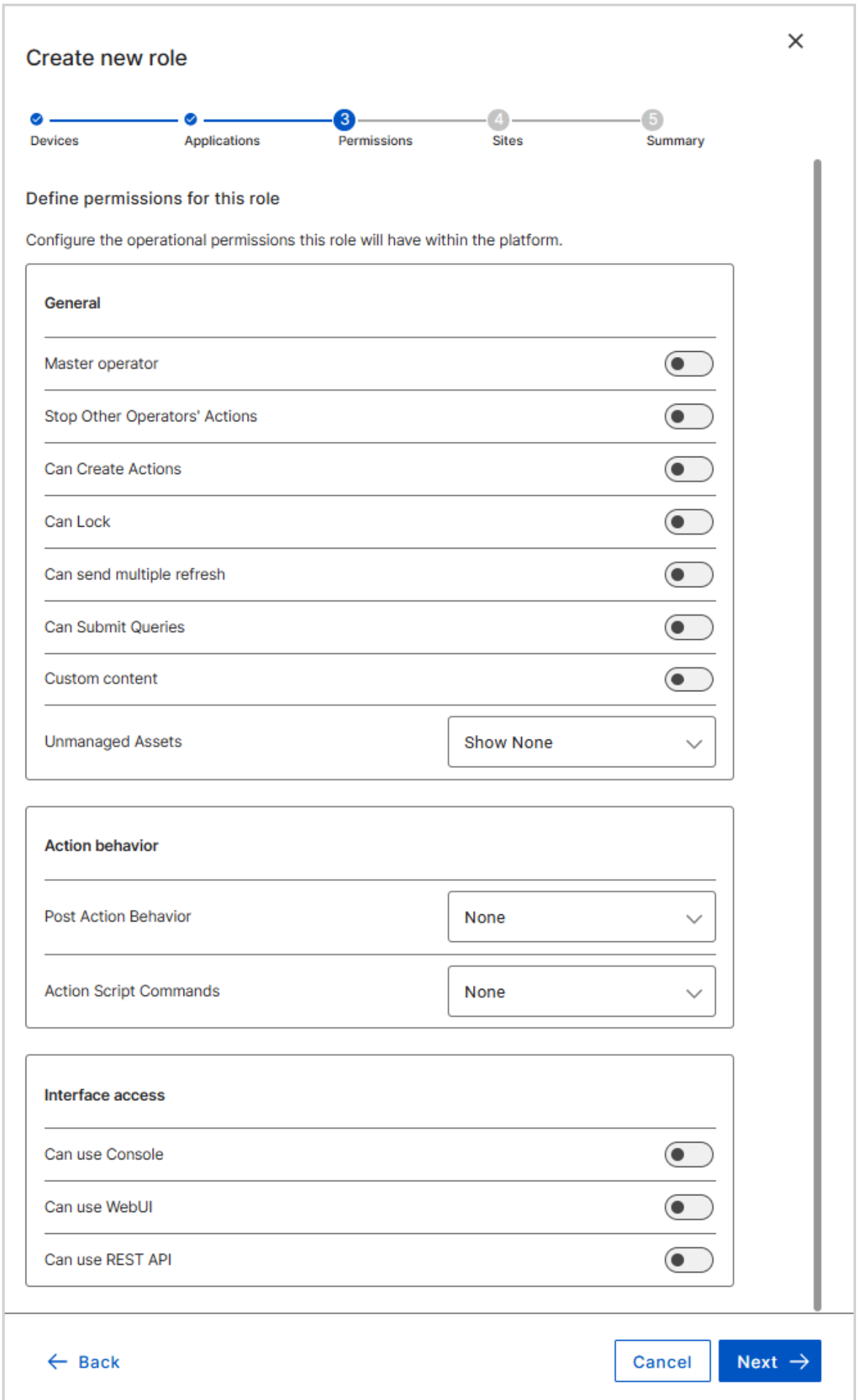
The following applications are available:

Table 92. Applications available in the role wizard

Application	Access
Analyses	Default app. Cannot be turned off.
Custom Remediation	Optional
CyberFOCUS	Optional
Deployment Manager	Default app. Cannot be turned off.
Device Explorer	Default app. Cannot be turned off.
Dex dashboard	Optional
Fixlet Explorer	Default app. Cannot be turned off.
Fixlet Streams	Optional. Users also need access to at least one external patch content site, which you grant on the **Sites** step. Otherwise, they cannot create a Fixlet Stream.
Integrated Vulnerability Management	Optional
My Dashboard	Default app. Cannot be turned off.
Patch	Optional
Protection Level Agreement (PLA)	Optional
Reports	Optional. When turned on, select an access level: **Admin**, **Users**, or **Read only**. Select **Can use scripted reports** to grant access to custom scripted reports.
Security Compliance	Optional
Site Management	Default app. Cannot be turned off.
Software Package	Optional
Tag Management	Optional
Workflow Builder	Optional

Each default app carries a **Default app** label. Hover over the information icon next to an application to read its description. Click **Next**.

5. **Permissions**: Under **Define permissions for this role**, configure the operational permissions this role has within the platform.


Create new role
Devices
Applications
3
Permissions
4
Sites
5
Summary
Define permissions for this role
Configure the operational permissions this role will have within the platform.
General
Master operator
Stop Other Operators' Actions
Can Create Actions
Can Lock
Can send multiple refresh
Can Submit Queries
Custom content
Unmanaged Assets
Show None
Action behavior
Post Action Behavior
None
Action Script Commands
None
Interface access
Can use Console
Can use WebUI
Can use REST API
Back
Cancel
Next

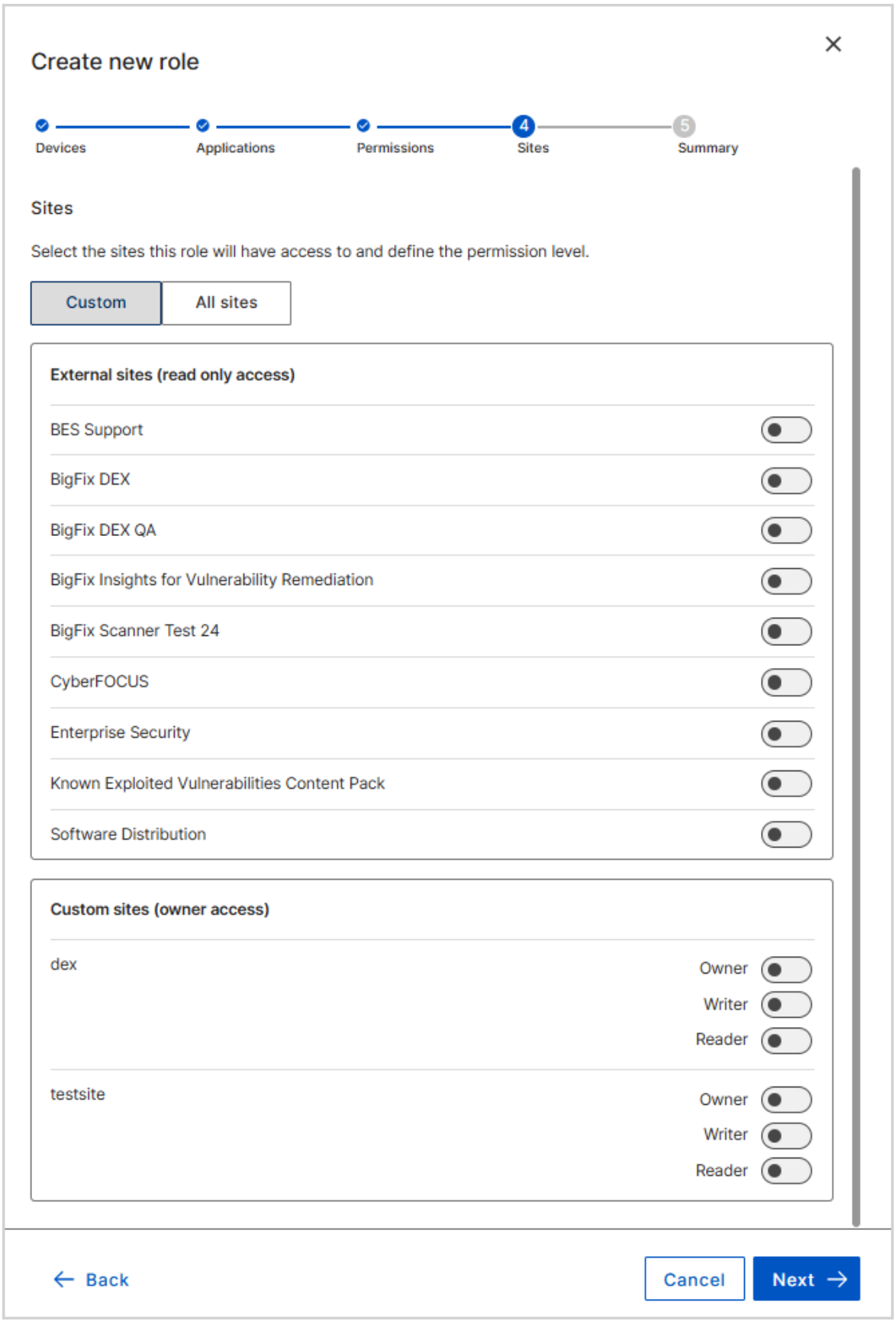
The permissions are grouped in three sections.

- **General**: Turn on the toggle for each permission to grant: **Master operator**, **Stop Other Operators' Actions**, **Can Create Actions**, **Can Lock**, **Can send multiple refresh**, **Can Submit Queries**, and **Custom content**. From the **Unmanaged Assets** list, select **By Scan Point**, **Show All**, or **Show None**.
- **Action behavior**: From the **Post Action Behavior** list, select **Allow Restart and Shutdown**, **Allow Restart Only**, or **None**. From the **Action Script Commands** list, select the level of script command access to grant.
- **Interface access**: Turn on the toggle for each interface the role can use: **Can use Console**, **Can use WebUI**, and **Can use REST API**.

All toggles are off and both lists are set to **None** by default, except **Unmanaged Assets**, which is set to **Show None**.

For a description of each permission, see Permissions reference *(on page 482)*. Click **Next**.

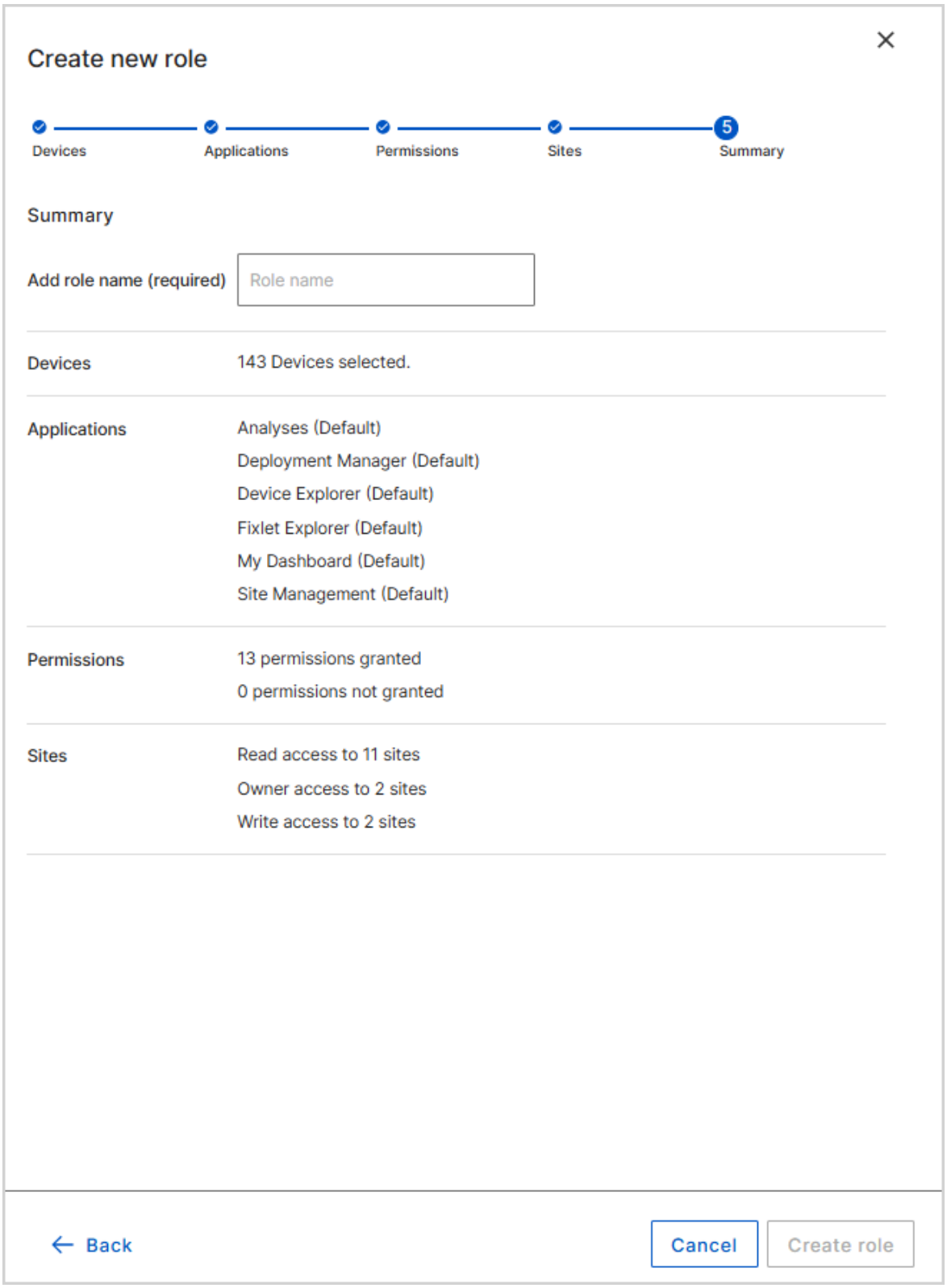
6. **Sites**: Select the sites this role has access to and define the permission level.


Create new role
Devices
Applications
Permissions
4
Sites
5
Summary
Sites
Select the sites this role will have access to and define the permission level.
Custom
All sites
External sites (read only access)
BES Support
BigFix DEX
BigFix DEX QA
BigFix Insights for Vulnerability Remediation
BigFix Scanner Test 24
CyberFOCUS
Enterprise Security
Known Exploited Vulnerabilities Content Pack
Software Distribution
Custom sites (owner access)
dex
Owner
Writer
Reader
testsite
Owner
Writer
Reader
Back
Cancel
Next

- Select **All sites** to grant access to every site, or **Custom** to choose sites individually. **Custom** is selected by default.
- Under **External sites (read only access)**, turn on the toggle for each external site the role can read.
- Under **Custom sites (owner access)**, for each custom site turn on **Owner**, **Writer**, or **Reader** to set the permission level.

Click **Next**.

7. On the **Summary** step, enter a **Role name (required)** and review the configuration.


Create new role
Devices
Applications
Permissions
Sites
5
Summary
Summary
Add role name (required)
Role name
Devices
143 Devices selected.
Applications
Analyses (Default)
Deployment Manager (Default)
Device Explorer (Default)
Fixlet Explorer (Default)
My Dashboard (Default)
Site Management (Default)
Permissions
13 permissions granted
0 permissions not granted
Sites
Read access to 11 sites
Owner access to 2 sites
Write access to 2 sites
Back
Cancel
Create role

The summary reports the number of devices selected, the applications the role can access with their default status, the count of permissions granted and not granted, and the site access by permission level.

To correct any setting, click **Back** to return to the relevant step.

Note: Provide a unique name for the role. You cannot edit the role name once it is created.

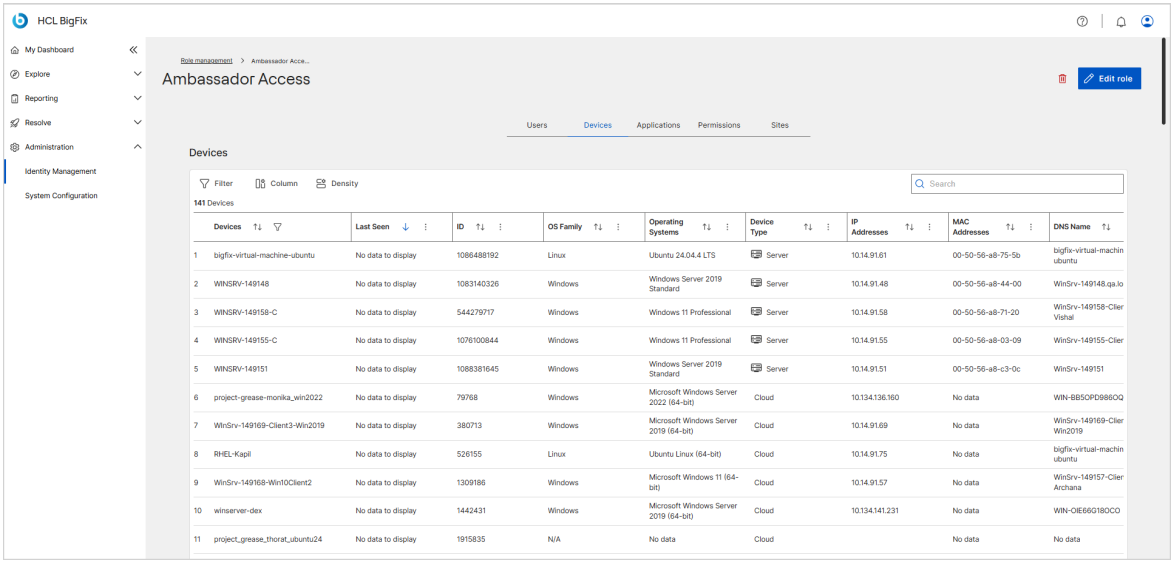
8. Click **Create role**. The button stays disabled until you enter a role name.

   Result: The new role appears on the **Roles** tab. Click the role to view its details.

Viewing role details

Follow these steps to view the users, devices, applications, permissions, and sites associated with a specific role:

1. Open **User & Role Management** and select the **Roles** tab.
2. Click a role name from the **Roles** column. The role details page appears.



3. Select a tab to view the corresponding information.

Table 93. Role details tabs

Tab	Description
Users	Lists the users assigned to the role. Use **Filter**, **Density**, and **Search** to locate a user. For more information, see Table filter *(on page 40)*.
Devices	Lists the devices the role can manage, with Last Seen, ID, OS Family, Operating Systems, Device Type, IP Addresses, MAC Addresses, and DNS Name. Use **Filter**, **Column**, **Density**, and **Search** to refine the list.

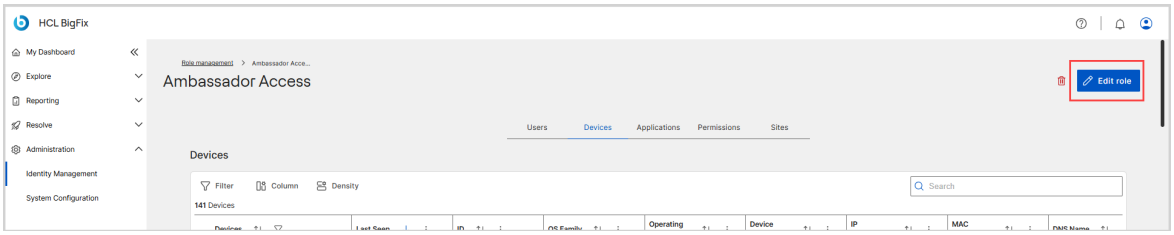
Tab	Description
Applications	Lists each application the role can access, its **Version**, and the **Access level** (for example, **Full access**, or **user** for Reports).
Permissions	Shows the **Permissions details** for the role, grouped as General, Action behavior, and Interface access. A **Granted** badge marks each permission the role grants. See Permissions reference *(on page 482)*.
Sites	Lists the sites the role has access to.

Editing a role

Follow these steps to modify the device scope, applications, permissions, and sites for an existing role:

Restriction: You cannot edit a role whose computer assignment is set to `byActiveDirectory`. BigFix UI does not support this computer assignment type and cannot change it. Use the BigFix Console to edit them.

1. Open **User & Role Management** and select the **Roles** tab.
2. Click the name of the role you want to edit.
3. Click **Edit role** in the top right corner. The **Edit role** wizard appears with the same **Devices**, **Applications**, **Permissions**, **Sites**, and **Summary** steps as the Create Role wizard.



4. Update the device scope, applications, permissions, and sites as described in Creating a new role *(on page 468)*. The wizard opens with the current settings of the role. Click **Next** to move forward and **Back** to return to an earlier step.
5. On the **Summary** step, review your changes and confirm to apply the new configuration. The role name is read-only.

   The role permissions update immediately. Assigned users will experience the modified access levels upon their next action.

Note: You cannot change the role name after the role is created.

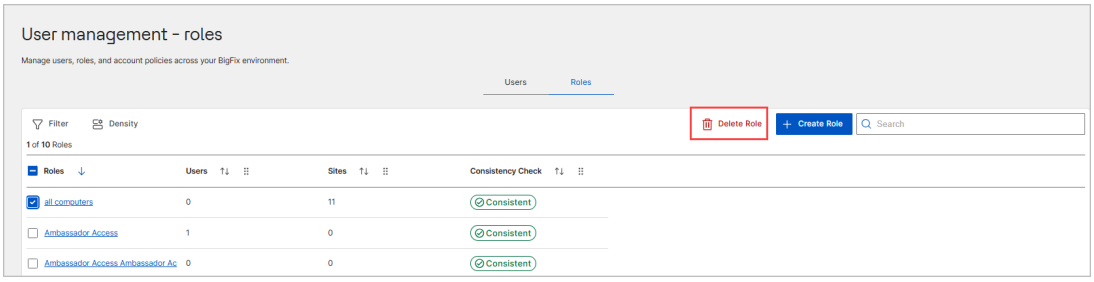
Deleting a role

Follow these steps to permanently remove a role from the BigFix UI.

Note: A role can only be deleted if zero users are currently assigned to it. Unassign all users from the role before attempting deletion.

You can delete a role using either of the following methods:

1. **Method 1:** Delete from the Roles list
    a. Open **User & Role Management** and select the **Roles** tab.
    b. Select the check box next to the role or roles you want to delete.
    c. Click **Delete Role** at the top right of the table.

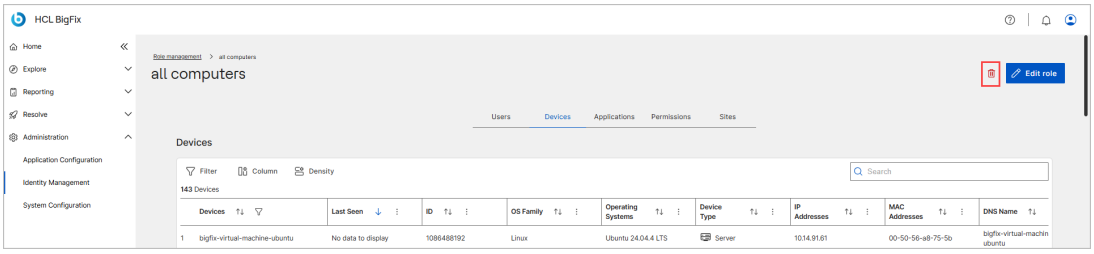


2. **Method 2:** Delete from the role details page

    a. Open **User & Role Management** and select the **Roles** tab.

    b. Click the name of the role you want to delete.

    c. Click the **Delete** (trash can) icon in the top right corner.

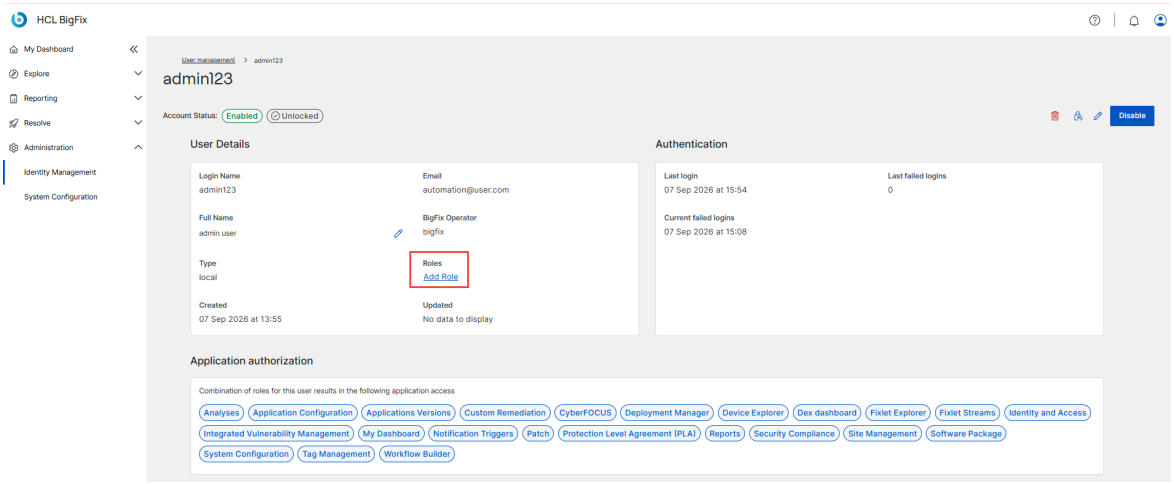


Assigning roles to users

As an administrator, when creating a new user *(on page 454)*, you assign one or more roles to ensure they have the appropriate level of access from their first login. You can add roles to an existing user at any time to adapt to organizational changes, evolving operational needs, and updated security policies.

To add a role to an existing user:

1. Open **User & Role Management**. On the **Users** tab, click the login name of the user.
2. On the user details page, under **Roles**, click **Add Role** and select the role.



3. Verify the change in the **Application authorization** section of the user details page and in the **Roles** column of the Users grid.

Related information

User & Role Management *(on page 449)*

Creating a new user *(on page 454)*

Permissions reference *(on page 482)*

Permissions reference

Permissions define the operational actions that a role or a user can perform within the platform. The same set of permissions appears on the **Permissions** step of the Create Role and Edit role wizards, on the **Permissions** tab of the role details page, and in the **Permissions** section of the user details page.

Explicit and effective permissions

On the user details page, the **Permissions** table shows two columns:

- **Explicit permissions**: Permissions that you grant directly to the user by using the toggles and lists in the first column. Click **Save** to apply your changes.
- **Effective permissions**: The resulting permissions for the user, combining the explicit permissions with the permissions inherited from the assigned roles and the bound BigFix operator.

On the role details page, a **Granted** badge next to a permission indicates that the role grants that permission.

When a user has multiple roles, the effective value of each toggle permission is the most permissive value across all assigned roles, and the effective access level for each application is the highest level granted by any assigned role.

Available permissions

Table 94. Permissions

Group	Permission	Control and values
General	Master operator	Toggle (on/off)
	Show Other Operators' Actions (role)	Toggle (on/off). Shown on the user details page and the role details page.
	Stop Other Operators' Actions	Toggle (on/off). BigFix UI saves this permission to the platform role, but enforces it only in the BigFix Console. In BigFix UI, operators can stop only their own deployments. For more information, see Deployments *(on page 181)*.
	Can Create Actions	Toggle (on/off)
	Can Lock	Toggle (on/off)
	Can Send Refresh To Multiple Computers (labeled **Can send multiple refresh** in the role wizard)	Toggle (on/off)
	Can Submit Queries	Toggle (on/off)
	Custom content	Toggle (on/off)
	Unmanaged Assets	List. For example, **Show All**.
Action behavior	Post Action Behavior	List: **Allow Restart and Shutdown**, **Allow Restart Only**, or **None**.
	Action Script Commands	List: **Allow Restart and Shutdown**, **Allow Restart Only**, or **None**.
Interface access	Can use Console	Toggle (on/off)
	Can use WebUI	Toggle (on/off)
	Can use REST API	Toggle (on/off)



Note: Hover over the information icon next to a permission in the UI to read its description.

Related information

Managing Roles *(on page 467)*

User & Role Management *(on page 449)*

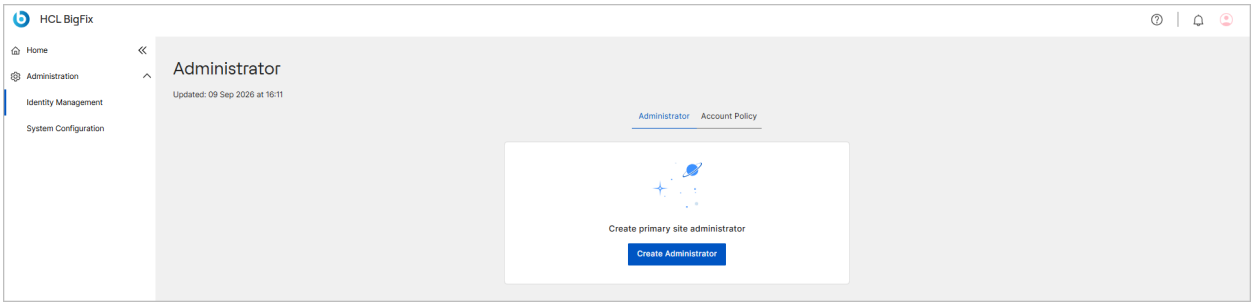
Admin user and account policy

The Admin user and account policy area of Identity management lets the instance admin create the primary site administrator and define the account security policies that govern how all users authenticate and maintain their sessions in BigFix UI.

Note: The **Admin user and account policy** card is visible only to the instance admin. It does not appear for other administrators.

Accessing Admin user and account policy

To open this area, expand **Administration** from the side navigation, select **Identity Management**, and then select the **Admin user and account policy** card. The page opens on the **Administrator** tab.



Tabs

The page is organized in two tabs.

Table 95. Admin user and account policy tabs

Tab	Description
Administrator	Shows the primary site administrator. Until an administrator exists, the tab displays **Create primary site administrator** with a **Create Administrator** button. For details, see Creating the primary site administrator *(on page 485)*.
Account Policy	Defines the legal notice message, session settings, password policy, and account lockout settings that apply to all users. For details, see Account Policy Settings *(on page 488)*.

Typical workflow

After the BigFix UI setup, the instance admin completes the following tasks from this area:

1. On the **Administrator** tab, create the primary site administrator and bind it to a BigFix Master operator. See Creating the primary site administrator *(on page 485)*.
2. On the **Account Policy** tab, configure the session, password, and lockout policies to match your organization's security standards. See Account Policy Settings *(on page 488)*.
3. Share the login URL and password with the primary site administrator through a secure channel. The administrator can then use **User & Role Management** to create users and roles. See User & Role Management *(on page 449)*.

Related information

Identity management *(on page 447)*

Creating the primary site administrator *(on page 485)*

Account Policy Settings *(on page 488)*

User & Role Management *(on page 449)*

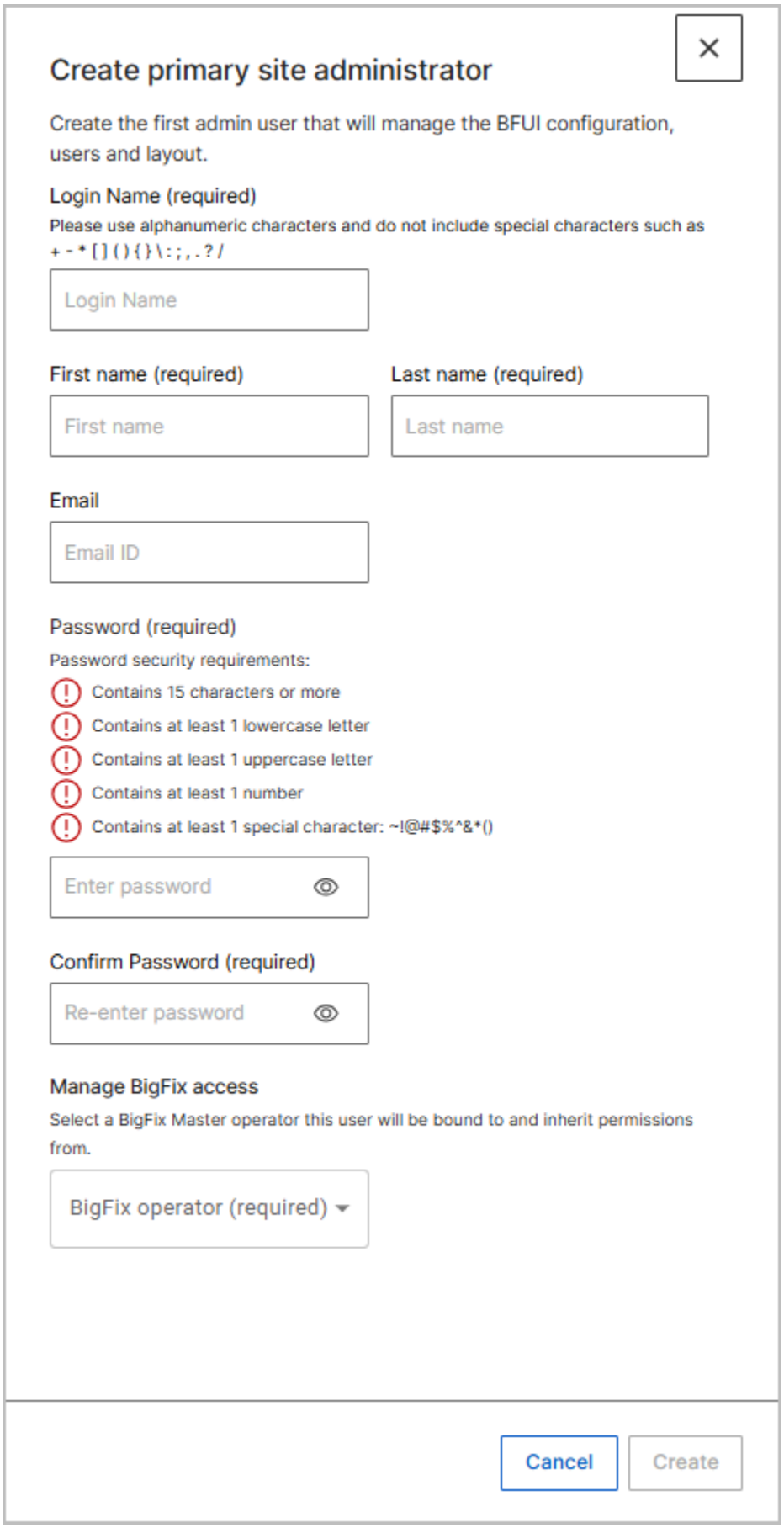
Creating the primary site administrator

As the instance admin, create the first admin user that manages the BigFix UI configuration, users, and layout. The primary site administrator is bound to a BigFix Master operator and inherits its permissions.

- You must be logged in as the instance admin. The **Admin user and account policy** card is visible only to the instance admin.
- A BigFix Master operator must exist on the BigFix platform to bind the administrator to.

The **Administrator** tab of the Admin user and account policy area shows the primary site administrator. Until an administrator is created, the tab displays **Create primary site administrator** with a **Create Administrator** button.

1. Expand **Administration** from the side navigation, select **Identity Management**, and then select the **Admin user and account policy** card.
   The **Administrator** page opens on the **Administrator** tab.
2. Click **Create Administrator**.


Create primary site administrator
Create the first admin user that will manage the BFUI configuration, users and layout.
Login Name (required)
Please use alphanumeric characters and do not include special characters such as + - * [ ] ( ) { } \ : ; , . ? /
Login Name
First name (required)
First name
Last name (required)
Last name
Email
Email ID
Password (required)
Password security requirements:
Contains 15 characters or more
Contains at least 1 lowercase letter
Contains at least 1 uppercase letter
Contains at least 1 number
Contains at least 1 special character: ~!@#$%^&*()
Enter password
Confirm Password (required)
Re-enter password
Manage BigFix access
Select a BigFix Master operator this user will be bound to and inherit permissions from.
BigFix operator (required)
Cancel
Create

The **Create primary site administrator** panel opens.

3. Complete the following fields.

Table 96. Create primary site administrator fields

Field	Description
Login Name (required)	Use alphanumeric characters. Do not include special characters such as + - * [ ] ( ) { } \ : ; , . ? /
First name (required)	The first name of the administrator.
Last name (required)	The last name of the administrator.
Email	The email ID of the administrator.
Password (required)	The initial password. The **Password security requirements** list is marked as met while you type. The password must: ◦ Contain 15 characters or more ◦ Contain at least 1 lowercase letter ◦ Contain at least 1 uppercase letter ◦ Contain at least 1 number ◦ Contain at least 1 special character: ~!@#$%^&*()
Confirm Password (required)	Re-enter the password.
BigFix operator (required) (under **Manage BigFix access**)	Select the BigFix Master operator this user is bound to and inherits permissions from.

4. Click **Create**.
   The **Create** button is enabled only after all required fields are complete and the password meets the security requirements.

The primary site administrator is created and appears on the **Administrator** tab. The administrator can log in to BigFix UI and use **User & Role Management** to create users and roles.

Share the login URL and password with the administrator through a secure channel. To configure session, password, and lockout policies, select the **Account Policy** tab. See Account Policy Settings *(on page 488)*.

Related information

Admin user and account policy *(on page 484)*

Account Policy Settings *(on page 488)*

User & Role Management *(on page 449)*

Account Policy Settings

The Account policy settings feature enables the instance admin to configure and enforce account security policies directly through the BigFix UI. By managing these settings, administrators can ensure the environment complies with organizational security standards, such as NIST 800-53, and enforce custom password complexity requirements.

Use this feature when you need to align your BigFix UI environment with strict corporate security policies, regulatory compliance frameworks, or when you want to mitigate unauthorized access risks by enforcing strong passwords and session limits.

Note:

- **Immediate Effect:** Any changes made to security settings apply immediately to all new authentication attempts.
- **Active Sessions:** Existing user sessions remain valid until their natural expiration or inactivity timeout.
- **Password Updates:** New password complexity rules apply only to password changes or resets that occur after the policy update.
- **Audit Logging:** All modifications to account security settings are recorded in the audit log, capturing the administrator's ID, timestamp, old/new values, and a request ID for traceability.

Key Capabilities

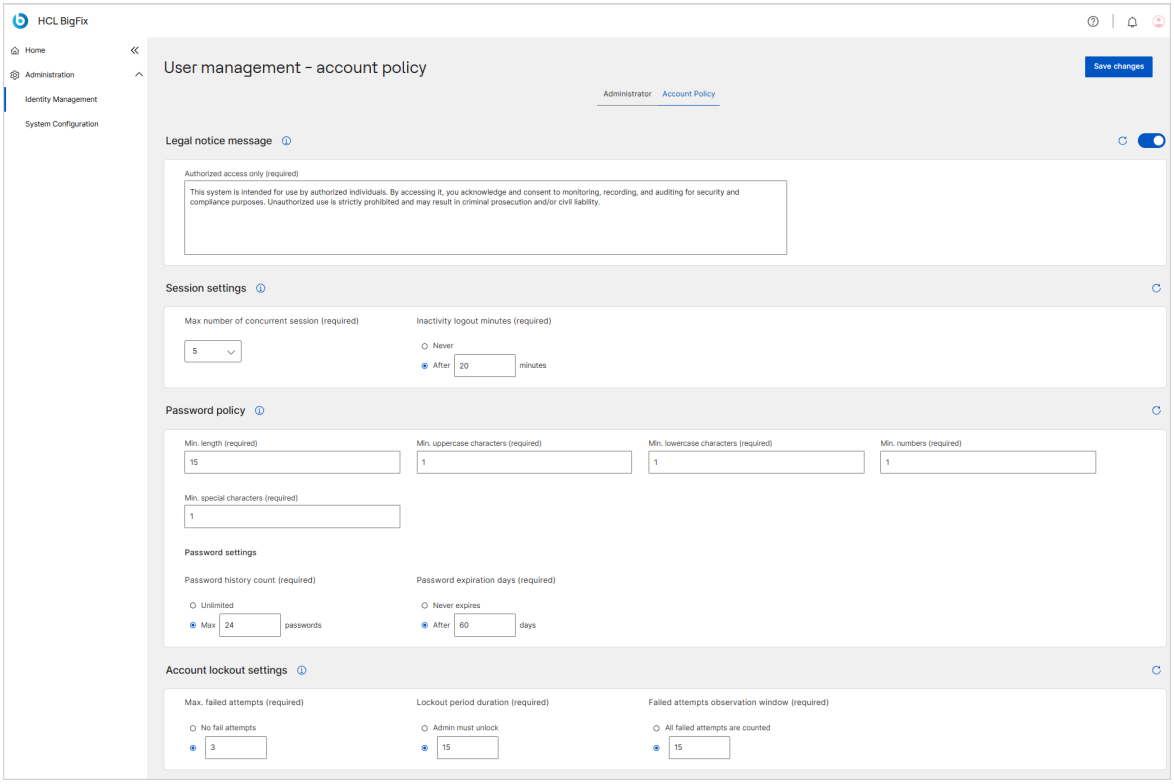
- **Access Control Policies:** Define parameters for concurrent sessions and inactivity timeouts.
- **Account Lockout Configuration:** Prevent unauthorized access by setting limits on failed login attempts and configuring lockout durations.
- **Password Complexity:** Enforce strict password rules, including minimum length, character types, expiration days, and password history tracking.
- **Pre-Login Legal Notice:** Display a customizable legal notice or warning message to users before they log in.

Configure Account Security Policies

1. From the BigFix UI navigation menu, expand **Administration**, select **Identity Management**, and then select the **Admin user and account policy** card.

   Note: You must be logged in as the instance admin. The **Admin user and account policy** card is not visible to other administrators.

2. Click the **Account Policy** tab. The **User management - account policy** page is displayed.



3. In the **Legal notice message** section, click the toggle to enable the pre-login message and enter your text in the **Authorized access only (required)** field.

> **Note:** The **Restore default** icon reverts the settings within a specific policy section to their factory default values. This icon is located in the upper-right corner of each section header (for example, Legal notice message, Session settings, or Password policy).

4. In the **Session settings** section, configure the **Max number of concurrent session (required)** and **Inactivity logout minutes (required)**.
5. In the **Password policy** section, define the character requirements, **Password history count (required)**, and **Password expiration days (required)**.
6. In the **Account lockout settings** section, configure the **Max. failed attempts (required)**, **Lockout period duration (required)**, and **Failed attempts observation window (required)**.
7. Click **Save changes**.

Result

The updated security policies take effect immediately for all new logins. Password complexity rules will be enforced the next time a user creates or resets their password.

Account Policy Settings Reference

The Account policy page categorizes security settings into logical sections. Use the following tables to understand the available configuration parameters, their behaviors, and default values. You can modify existing values, but you cannot create new settings or delete existing ones.

Table 97. Account Policy Actions

Action	Description
Restore default icon	Restores the settings within a specific policy section to their factory default values, rather than acting as a simple reset. This icon is located in the upper-right corner of each section header (for example, Legal notice message, Session settings, or Password policy).
Save changes	Applies and enforces the configured account policies across the BigFix UI environment.

Table 98. Legal Notice Message

UI Field / Setting	Description	Default Value
Toggle Switch	Enables or disables the display of a pre-login message on the login screen.	Off
Authorized access only (required)	The custom text displayed to users before logging in.	This system is intended for use by authorized individuals. By accessing it, you acknowledge and consent to monitoring, recording, and auditing for security and compliance purposes. Unauthorized use is strictly prohibited and may result in criminal prosecution and/or civil liability.

Table 99. Session Settings

UI Field / Setting	Description	Default Value
Max number of concurrent session (required)	The maximum number of simultaneous sessions allowed per user. Select a value from the dropdown list.	5
Inactivity logout minutes (required)	The time period of user inactivity before the system automatically trig-	After 20 minutes

Table 99. Session Settings (continued)

UI Field / Setting	Description	Default Value
	gers a logout. Can be set to **Never** or **After [X] minutes**. **Note:** A warning popup appears 60 seconds before the session officially ends.	

Table 100. Password Policy

UI Field / Setting	Description	Default Value
Min. length (required)	The minimum number of characters required for a valid password.	15
Min. uppercase characters (required)	The minimum number of uppercase letters required.	1
Min. lowercase characters (required)	The minimum number of lowercase letters required.	1
Min. numbers (required)	The minimum numerical digits required.	1
Min. special characters (required)	The minimum special characters required.	1
Password history count (required)	The number of previous passwords that cannot be reused. Can be set to **Unlimited** or **Max [X] passwords**.	Max 24 passwords
Password expiration days (required)	The number of days before a user is forced to change their password. Can be set to **Never expires** or **After [X] days**.	After 60 days

Table 101. Account Lockout Settings

UI Field / Setting	Description	Default Value
Max. failed attempts (required)	The maximum number of failed login attempts allowed before the account is locked. Select **No fail attempts** or enter a count.	3

Table 101. Account Lockout Settings (continued)

UI Field / Setting	Description	Default Value
Lockout period duration (required)	The duration, in minutes, an account remains locked. Select **Admin must unlock** or enter a number of minutes.	15 minutes
Failed attempts observation window (required)	The observation window, in minutes, for counting failed attempts. Select **All failed attempts are counted** or enter a window duration.	15 minutes

Related information

Admin user and account policy *(on page 484)*

Creating the primary site administrator *(on page 485)*

OIDC Configuration

OIDC Configuration lets the instance admin connect BigFix UI to an external identity provider by using the OpenID Connect (OIDC) protocol, so that users can log in with single sign-on (SSO) using their existing organizational credentials.

Note: OIDC Configuration is available only to the instance admin. Open it from **Administration** > **Identity Management** > **OIDC Configuration**.

Overview

With OIDC enabled, the BigFix UI login page shows an additional **Log in via OIDC** button. When a user clicks it, BigFix UI redirects the user to the identity provider's login page. After the identity provider authenticates the user, it redirects the browser back to BigFix UI, which validates the ID token, creates a BigFix UI session, and opens the dashboard.

Logging out of BigFix UI ends only the BigFix UI session; it does not log the user out of the identity provider.

OIDC authentication succeeds only for users that already exist in BigFix UI as Identity provider (Idp) users and are bound to a BigFix operator. See Creating a new user *(on page 454)*.

Configuration workflow

Setting up OIDC single sign-on spans the identity provider, the BigFix Console, and BigFix UI. Complete the following tasks in order:

1. Register BigFix UI as a client application in your identity provider, and collect the Provider URL, client ID, and client secret. See Registering BigFix UI with your identity provider *(on page 495)*.
2. Add the identity provider to the BigFix Console and create the identity provider operators. See Configuring the identity provider on the BigFix Console *(on page 503)*.
3. Enter the provider details in BigFix UI, test the connection, and save the configuration. See Configuring OIDC single sign-on *(on page 506)*.
4. Create the matching Identity provider (Idp) users in BigFix UI. See Creating a new user *(on page 454)*.
5. Verify that a user can sign in. See Logging in with OIDC *(on page 510)*.

Supported OIDC providers

BigFix UI supports the following identity providers for OIDC authentication:

- Active Directory Federation Services (ADFS)
- Microsoft Azure Entra ID
- Okta

The Provider URL format, the **Scope** value, and the client ID and client secret differ for each provider. For the Provider URL and Scope values, see OIDC provider settings reference *(on page 512)*. Obtain the client ID and client secret from the application that you register with your provider. See Registering BigFix UI with your identity provider *(on page 495)*.

Restriction: For Okta, the Provider URL (issuer) must have `okta.com` as its domain suffix. Custom Okta domains are not supported in this release.

Prerequisites

Before you configure OIDC in BigFix UI, register BigFix UI as a client application in your identity provider and collect the following values from it:

- **Provider URL**: The OIDC discovery endpoint, or issuer, of the provider.
- **Client ID**: The client ID registered for BigFix UI in the provider.
- **Client Secret**: The client secret registered for BigFix UI in the provider.
- **Scope** (optional): The scope value that your provider requires.

You must also register the BigFix UI redirect URL in the provider, and the provider must be reachable over HTTPS with a trusted certificate from both the BigFix UI server and the client browser. See Registering BigFix UI with your identity provider *(on page 495)* and OIDC provider settings reference *(on page 512)*.

Important: Treat the client secret as a credential. BigFix UI never displays a saved client secret in the user interface.

The Setup single sign-on (SSO) page

The **OIDC Configuration** card opens the **Setup single sign-on (SSO)** page. When a configuration exists, the page shows the **OIDC enabled** toggle and the **OIDC details** (ADFS/OIDC Providers URL and Client ID), together with the following actions.

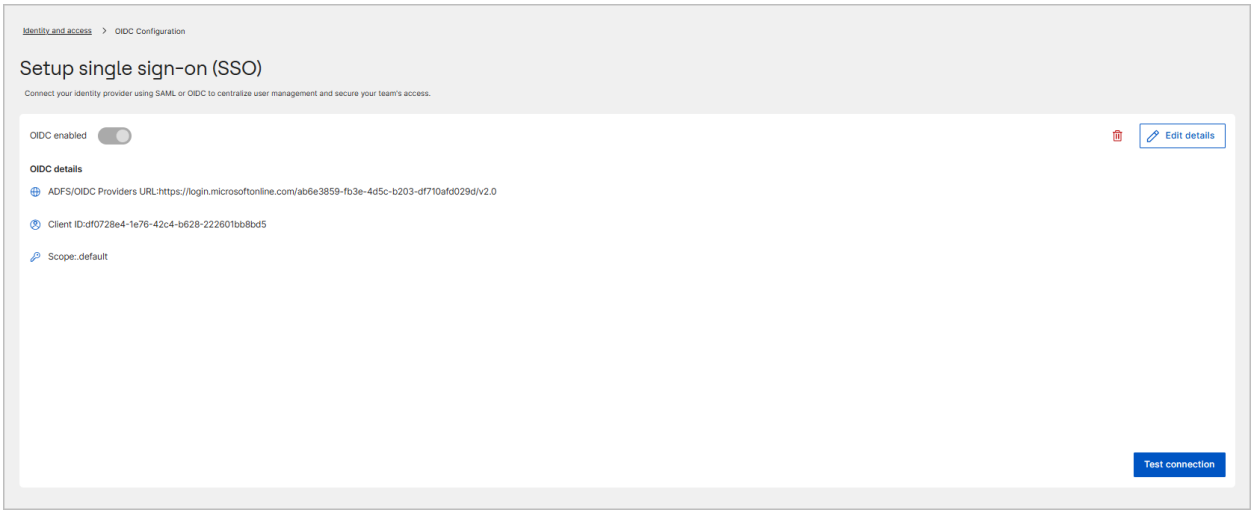


Table 102. OIDC Configuration actions

Control	Description
OIDC enabled	Turns OIDC authentication on or off. When off, the **Log in via OIDC** option is not available on the login page.
Edit details	Opens the configuration fields for editing. See Configuring OIDC single sign-on *(on page 506)*.
Delete (trash can icon)	Removes the OIDC configuration. After deletion, the provider is no longer available for OIDC authentication.
Test connection	Verifies that BigFix UI can connect to the provider with the saved (or entered) configuration.
Reset inputs	Available while editing. Clears the values you entered in the fields.

Note: To change the Provider URL, disable the existing configuration and create a new configuration with the new Provider URL and its credentials.

Related information

Registering BigFix UI with your identity provider *(on page 495)*

Configuring the identity provider on the BigFix Console *(on page 503)*

Configuring OIDC single sign-on *(on page 506)*

Logging in with OIDC *(on page 510)*

OIDC provider settings reference *(on page 512)*

Identity management *(on page 447)*

Creating a new user *(on page 454)*

Registering BigFix UI with your identity provider

Before you configure OIDC in BigFix UI, register BigFix UI as a client application in your identity provider and collect the Provider URL, client ID, and client secret that the configuration requires.

- You must have administrator rights in the identity provider to register an application.
- Decide the redirect URL for your BigFix UI server. See Redirect URL *(on page 513)*.

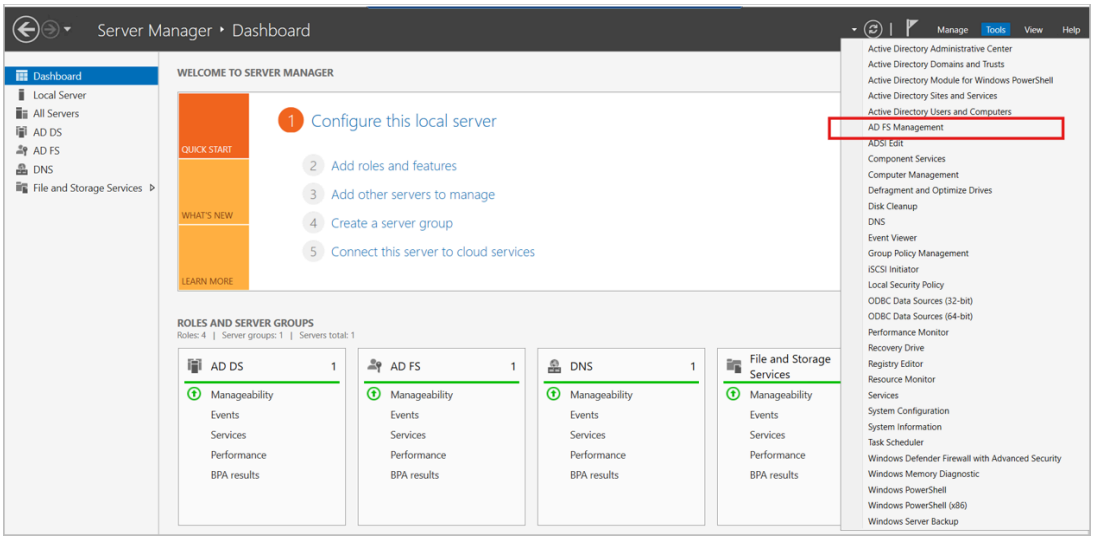
BigFix UI supports ADFS, Microsoft Azure Entra ID, and Okta. Whichever provider you use, the registration produces the same three values that you later enter in BigFix UI:

- **Provider URL**: The OIDC discovery endpoint, or issuer, of the provider.
- **Client ID**: The identifier that the provider assigns to the BigFix UI application.
- **Client Secret**: The secret that the provider generates for the application.

In every provider, you must also register the redirect URL that ends with `/oidc/callback`. Complete the procedure for your provider.

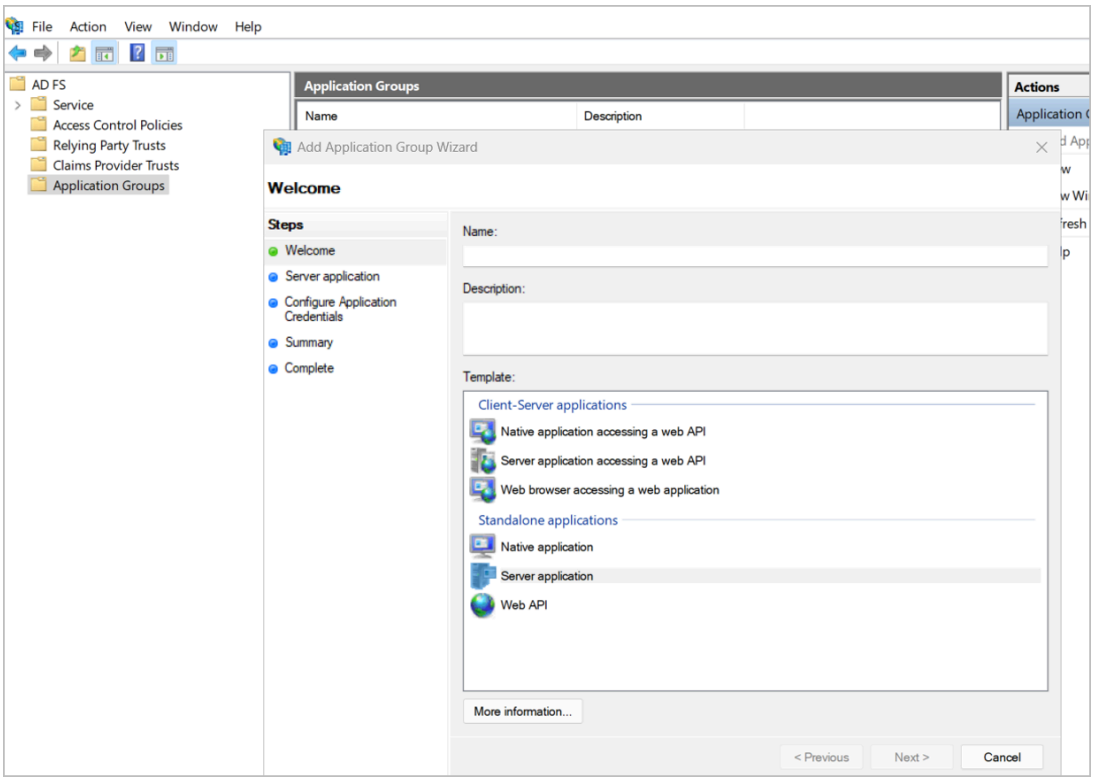
1. To register BigFix UI in ADFS, create an application group on the ADFS server.

    a. On the Windows server, open **Server Manager** and select **Tools > AD FS Management**.



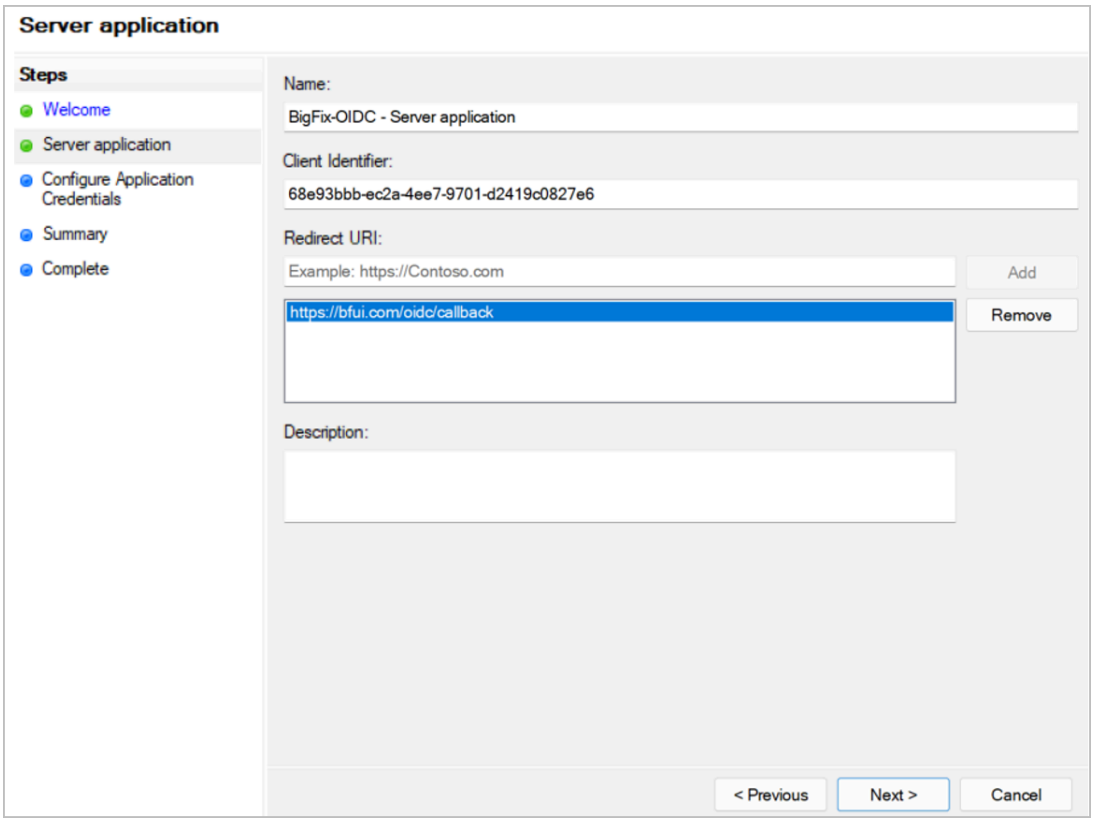
b. Select **Application Groups**, and then click **Add Application Group**.

c. In the **Add Application Group Wizard**, type a name for the group, for example `BigFix-OIDC`, select the **Server application** template under **Standalone applications**, and click **Next**.



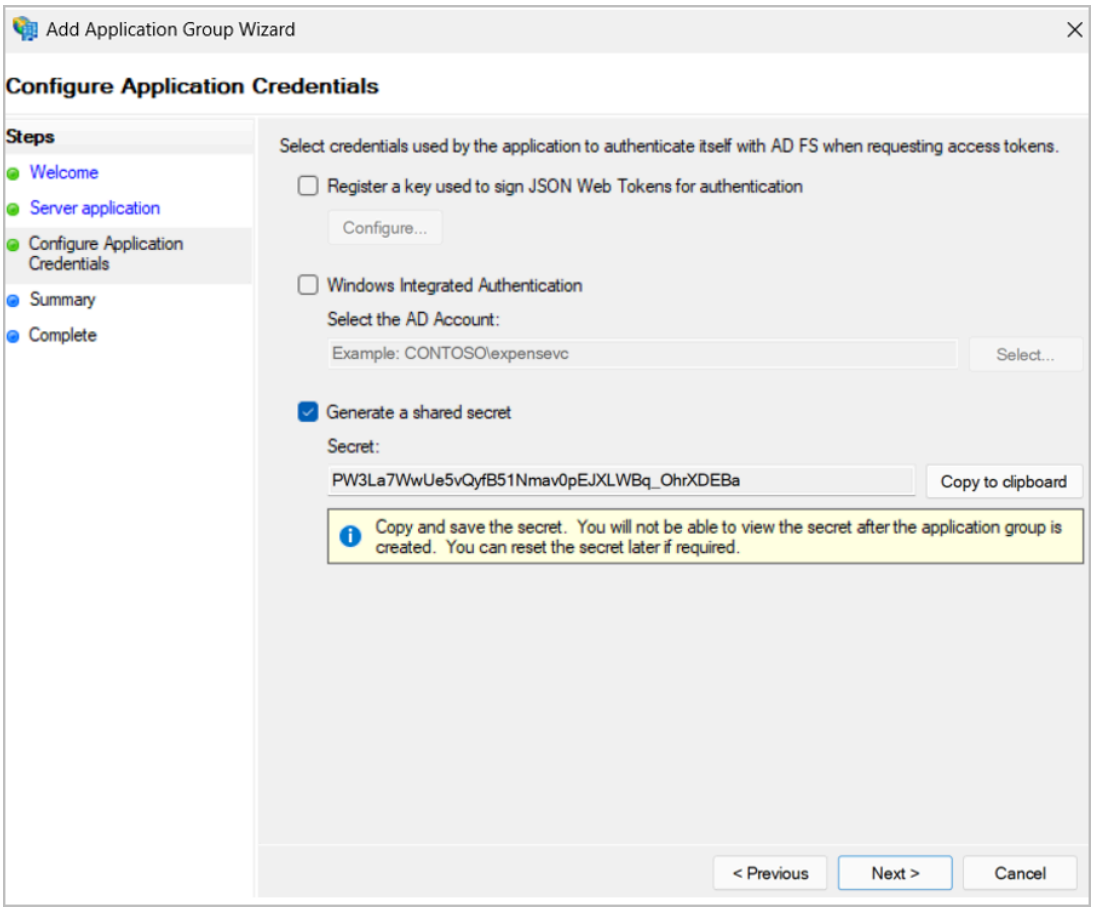
d. On the **Server application** page, note the generated **Client Identifier**, type the redirect URL in **Redirect URI**, click **Add**, and then click **Next**.

The client identifier is the client ID that you enter in BigFix UI.

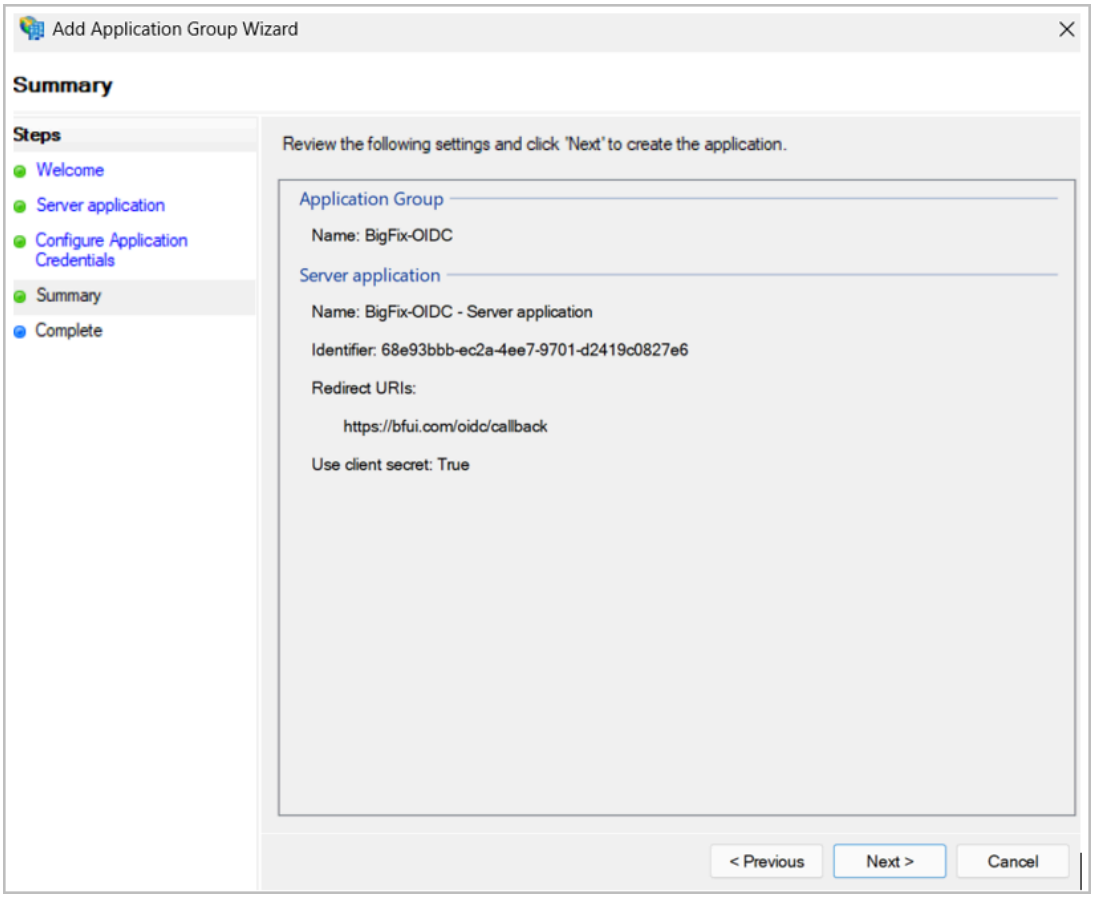


e. On the **Configure Application Credentials** page, select **Generate a shared secret**, copy the secret, and click **Next**.

Important: Save the secret in a secure location. ADFS does not display it again after the application group is created. If you lose it, reset the secret.


Add Application Group Wizard
Configure Application Credentials
Steps
Welcome
Server application
Configure Application Credentials
Summary
Complete
Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.
Register a key used to sign JSON Web Tokens for authentication
Configure...
Windows Integrated Authentication
Select the AD Account:
Example: CONTOSO\expensevc
Select...
Generate a shared secret
Secret:
PW3La7WwUe5vQyfB51Nmav0pEJXLWBq_OhrXDEBa
Copy to clipboard
Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.
< Previous
Next >
Cancel

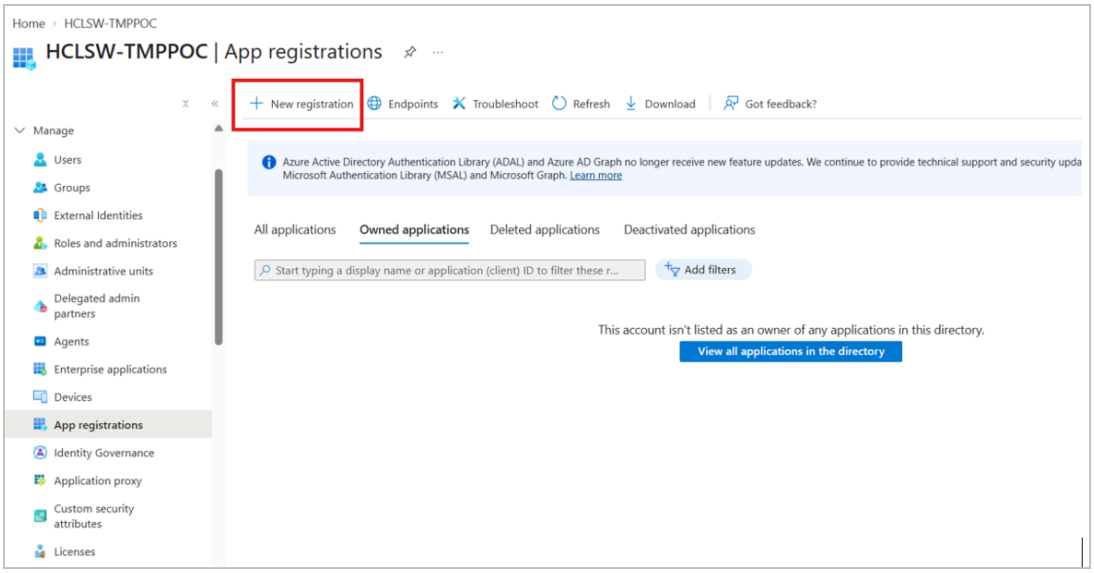
f. Review the settings on the **Summary** page and click **Next** to create the application group.



The application group is created. The Provider URL for BigFix UI is the ADFS server domain followed by `/adfs`. See Provider URL *(on page 512)*.

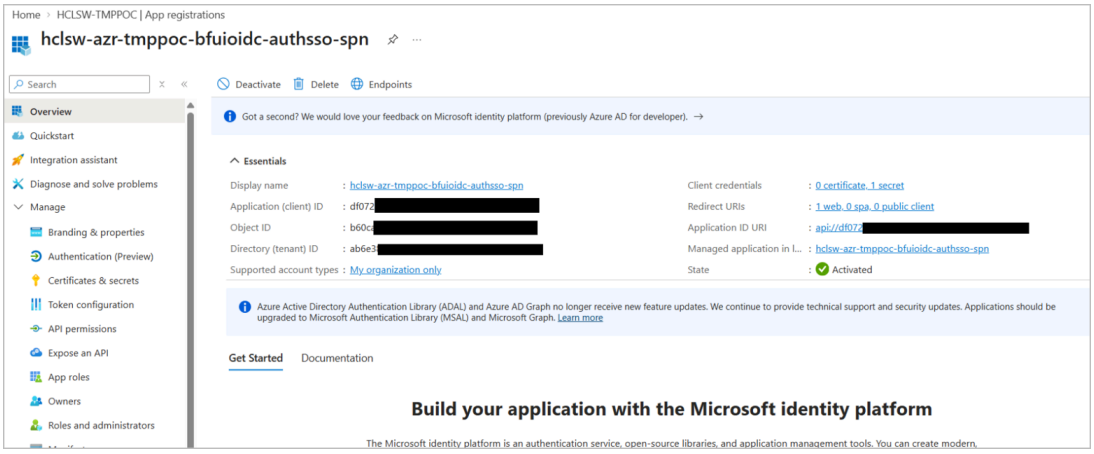
2. To register BigFix UI in Microsoft Azure Entra ID, create an app registration in your tenant.

a. In the Microsoft Entra admin center, open **App registrations** for your tenant and click **New registration**.



b. From the **Overview** page of the new application, note the **Application (client) ID** and the **Directory (tenant) ID**.

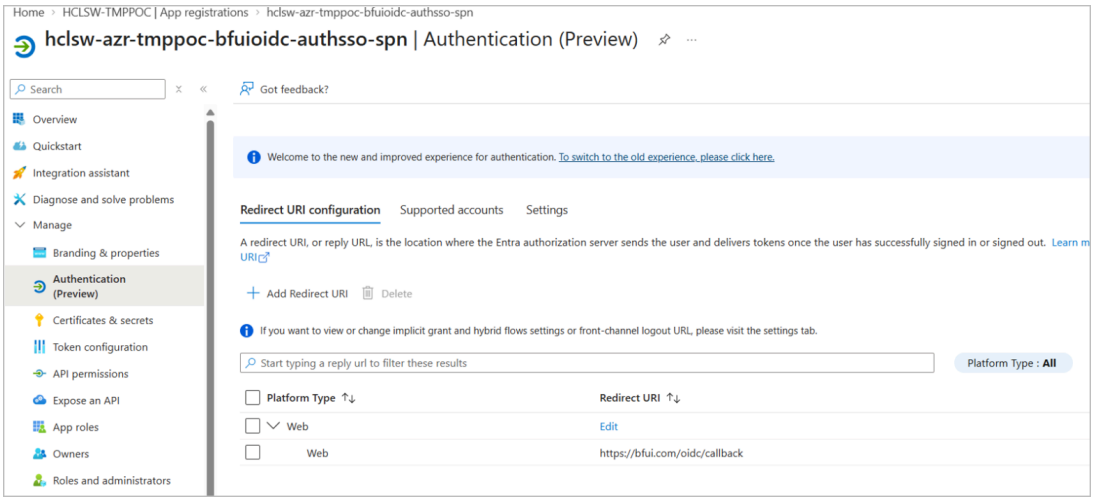
The tenant ID forms part of the Provider URL.



c. Under **Certificates & secrets**, create a client secret and copy its value.

Important: Copy the secret value immediately. Entra ID hides it after you leave the page.

d. Under **Authentication**, add a redirect URI of platform type **Web** and set it to the BigFix UI redirect URL.

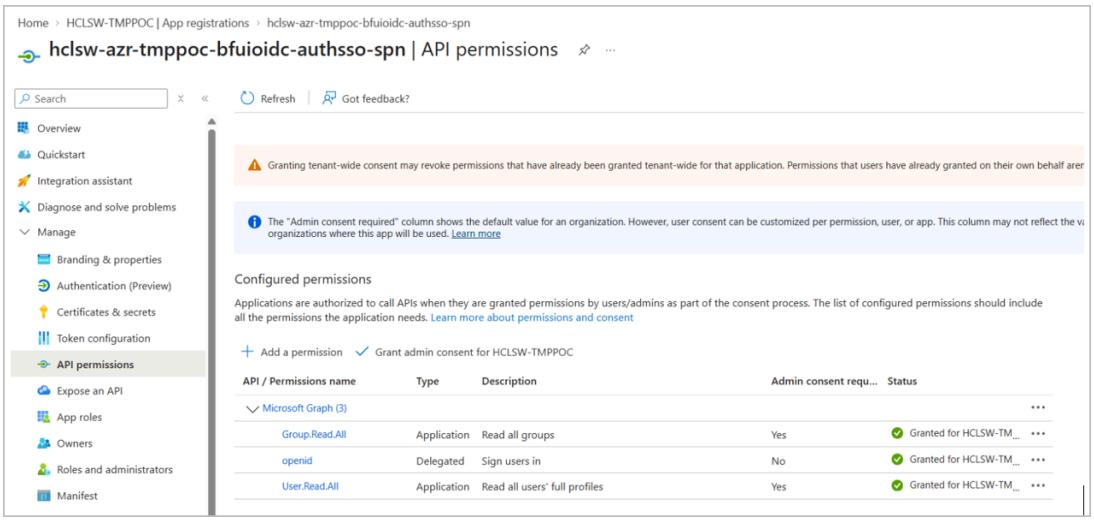


e. Under **API permissions**, add the Microsoft Graph permissions that BigFix UI requires, and then grant admin consent for the tenant.

BigFix UI reads user and group membership so that Entra ID users can sign in and receive the expected privileges.

Table 103. Required Microsoft Graph permissions

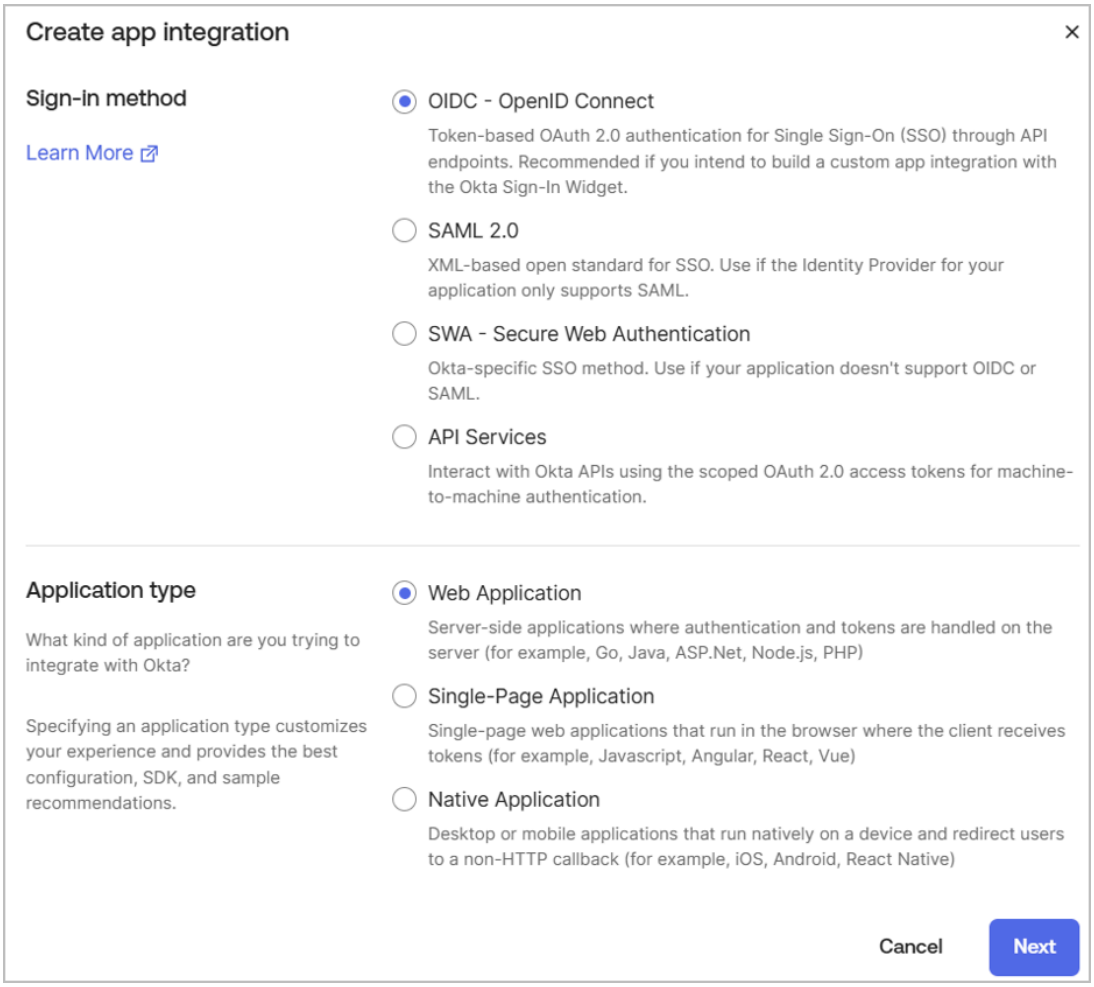
Permission	Type	Description
`Group.Read.All`	Application	Read all groups. Requires admin consent.
`User.Read.All`	Application	Read all users' full profiles. Requires admin consent.
`openid`	Delegated	Sign users in.



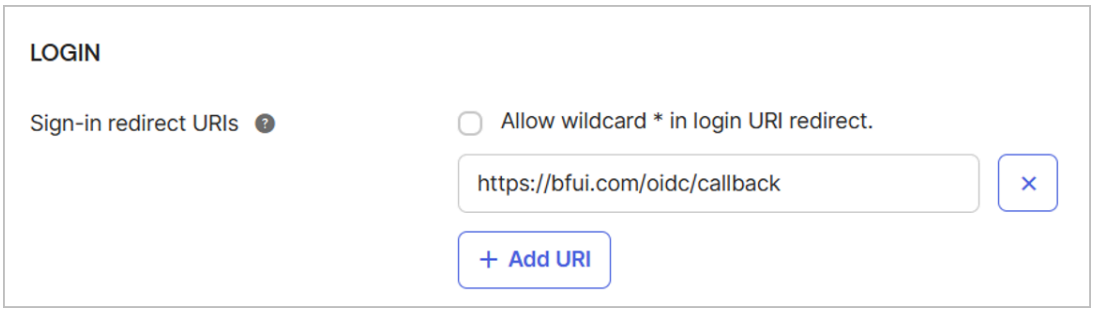
The app registration is complete. Build the Provider URL from the tenant ID as described in Provider URL *(on page 512)*.

3. To register BigFix UI in Okta, create an app integration in your Okta organization.

    a. In the Okta Admin Console, create an app integration with the sign-in method **OIDC - OpenID Connect** and the application type **Web Application**, and click **Next**.



    b. Under **LOGIN**, set **Sign-in redirect URIs** to the BigFix UI redirect URL, and complete the remaining fields according to the policies of your organization.



c. Save the integration and note the client ID and client secret from the general settings of the application.

The app integration is complete. The Provider URL is the Okta organization URL, which must end with `okta.com`. See Provider URL *(on page 512)*.

BigFix UI is registered with your identity provider, and you have the Provider URL, client ID, and client secret that the OIDC configuration requires.

Configure the same identity provider on the BigFix Console so that operators exist for the users who sign in through OIDC. See Configuring the identity provider on the BigFix Console *(on page 503)*.

Related information

OIDC provider settings reference *(on page 512)*

Configuring the identity provider on the BigFix Console *(on page 503)*

Configuring OIDC single sign-on *(on page 506)*

Register an application with the Microsoft identity platform

Create OIDC app integrations in Okta

Configuring the identity provider on the BigFix Console

OIDC authenticates a user, but the user still needs a BigFix operator to work with BigFix resources. Add your identity provider to the BigFix Console, create the identity provider operators, and then create the matching users in BigFix UI.

Why the Console configuration is needed

When a user signs in with **Log in via OIDC**, the identity provider verifies the credentials of the user. BigFix UI then matches that user with an existing identity provider user, which is bound to a BigFix operator. The operator determines which sites, devices, and actions the user can work with.

Therefore, the identity provider must be defined on the BigFix Console, and an operator must exist for each user who signs in through OIDC.

Important: Configure the identity provider operators on the BigFix Console and create the corresponding users in BigFix UI before anyone signs in with OIDC. If the operator or the BigFix UI user does not exist, the user can authenticate at the provider but cannot access the expected resources or functions.

Adding the identity provider to the BigFix Console

The procedure depends on the provider that you use for OIDC.

Table 104. Identity provider configuration on the BigFix Console

Provider	What to do
ADFS	Add the existing Active Directory to the BigFix Console. See Integrating the BigFix Windows server with Active Directory.
Microsoft Azure Entra ID	Add Microsoft Entra ID as an identity provider. See Adding Microsoft Entra ID as Identity Provider.
Okta	The BigFix Console does not integrate with Okta directly. See Using Okta with the BigFix Console *(on page 504)*.

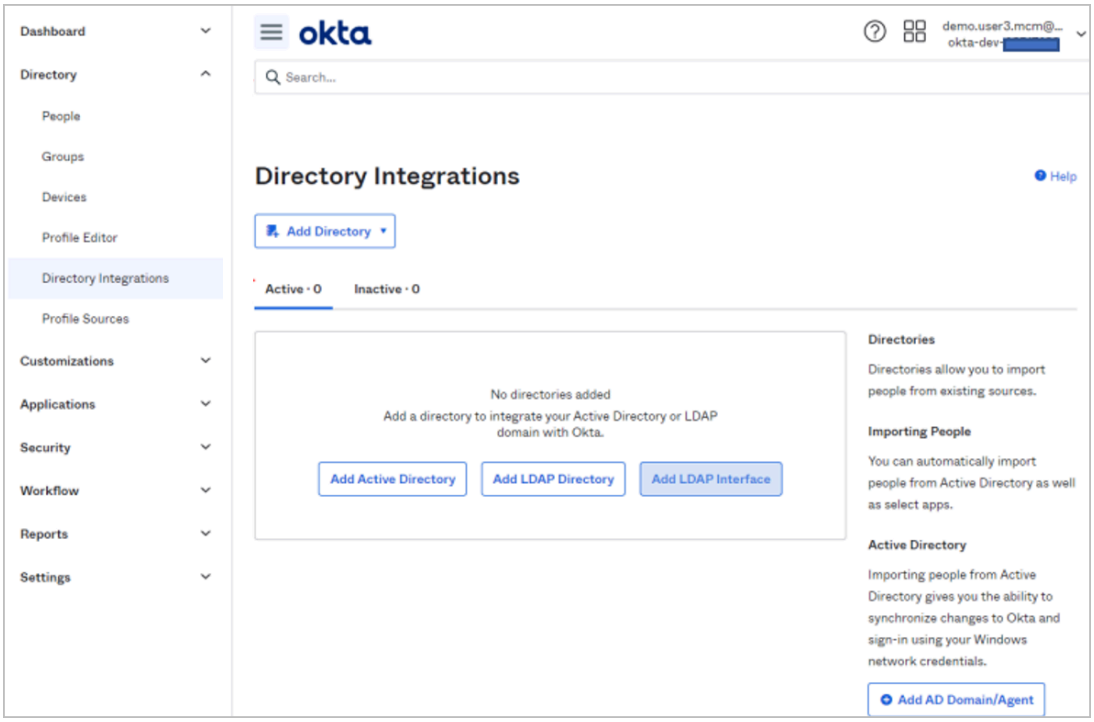
Using Okta with the BigFix Console

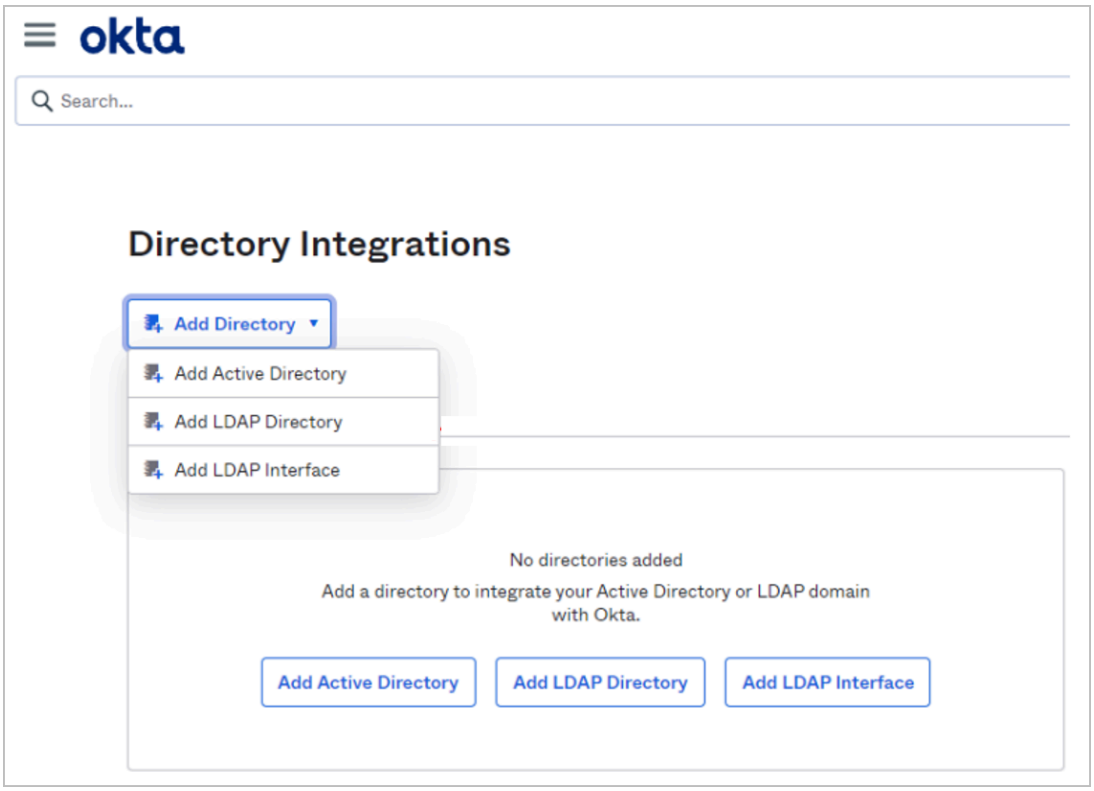
The BigFix Console does not provide direct integration with Okta. Connect Okta to an Active Directory or LDAP directory, and then add that directory to the BigFix Console:

1. In the Okta Admin Console, open **Directory > Directory Integrations** and click **Add Directory**.
2. Select **Add Active Directory**, **Add LDAP Directory**, or **Add LDAP Interface**, and complete the integration.
3. Add the same Active Directory or LDAP directory to the BigFix Console in the standard way. See Integrating the BigFix Windows server with Active Directory.

Note: If Okta uses an external directory such as Active Directory or LDAP, make sure that the directory integration and the corresponding Okta agent are configured and that the required users are imported or synchronized into the Okta organization before you attempt an OIDC login. Also make sure that the users are active and assigned to the BigFix UI OIDC application.

Figure 3. Directory Integrations in the Okta Admin Console





Adding identity provider operators

Create Console operator accounts from your Active Directory, LDAP, or Microsoft Entra ID account. When you select this option, an operator with the same name as the one in the identity provider directory is added under the operators node in the Domain Panel of the BigFix Console.

For details, see Adding Identity Provider Operators.

Creating the identity provider users in BigFix UI

For each operator, create a user in BigFix UI with the authentication method **Identity provider (Idp)** and bind it to the operator. No password is set or managed in BigFix UI for these users, because the identity provider authenticates them. See Creating a new user *(on page 454)*.

Related information

Registering BigFix UI with your identity provider *(on page 495)*

Configuring OIDC single sign-on *(on page 506)*

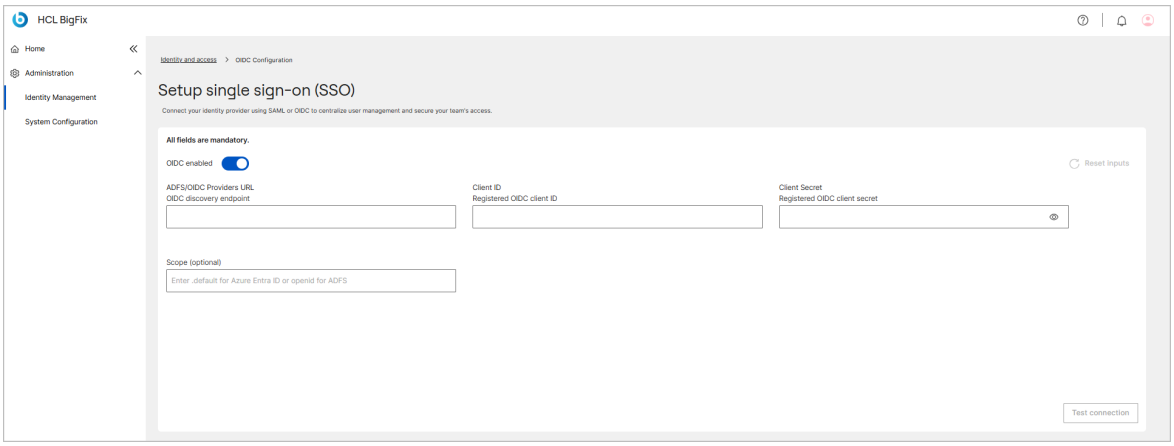
Creating a new user *(on page 454)*

Configuring OIDC single sign-on

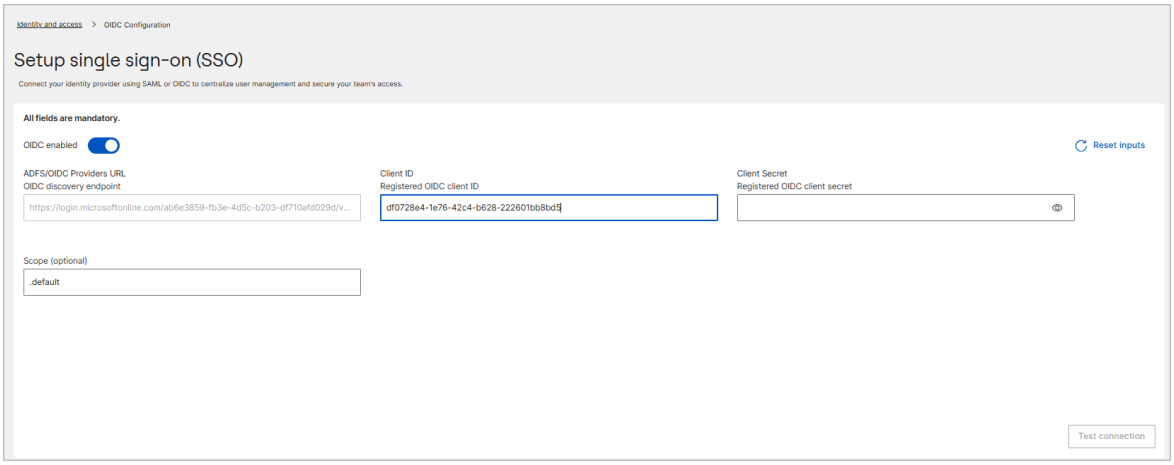
Connect BigFix UI to your OIDC identity provider, test the connection, and enable single sign-on so that users can log in with **Log in via OIDC**.

- You must be logged in as the instance admin.
- BigFix UI is registered as a client application in your identity provider, with the redirect URL set to `<scheme>://<bfui-host>:<port>/oidc/callback`. You have the Provider URL, Client ID, and Client Secret. See Registering BigFix UI with your identity provider *(on page 495)*.
- The provider is reachable over HTTPS from the BigFix UI server and from the client browser, with a trusted certificate. See Provider URL accessibility *(on page 513)*.
- The identity provider is configured on the BigFix Console, and the identity provider operators exist. See Configuring the identity provider on the BigFix Console *(on page 503)*.

1. Expand **Administration** from the side navigation, select **Identity Management**, and then select the **OIDC Configuration** card.
   The **Setup single sign-on (SSO)** page opens.



2. If a configuration already exists, click **Edit details**. Otherwise, continue with the next step.



All fields are mandatory unless marked optional.

3. Turn on the **OIDC enabled** toggle.

4. Complete the configuration fields.

Table 105. OIDC configuration fields

Field	Description
ADFS/OIDC Providers URL	The OIDC discovery endpoint of your provider, for example `https://adfs.corpdemo.local/adfs`. The format depends on the provider. See Provider URL *(on page 512)*. The Provider URL identifies the configuration and cannot be changed afterwards.
Client ID	The registered OIDC client ID for BigFix UI.
Client Secret	The registered OIDC client secret for BigFix UI. Click the eye icon to show or hide the value.

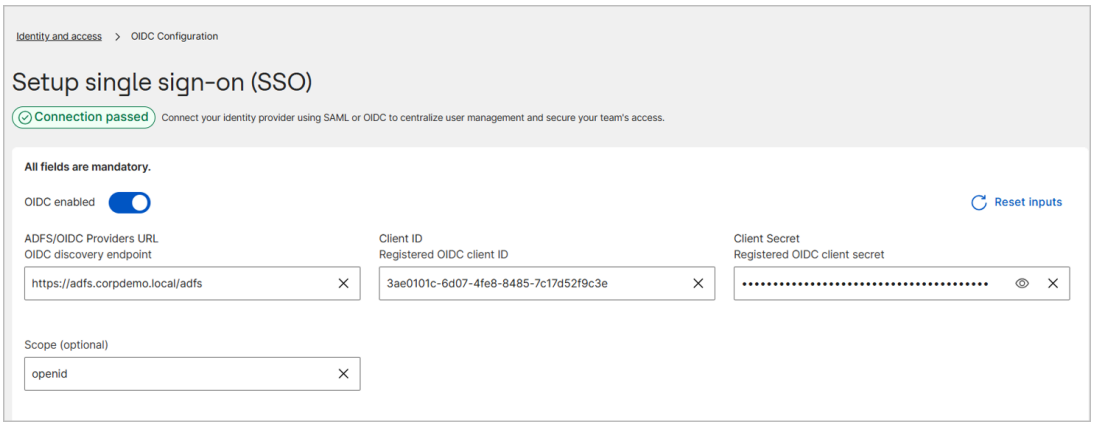
Field	Description
Scope (optional)	Enter `.default` for Azure Entra ID or `openid` for ADFS. Leave empty for Okta. The scope is mandatory for Azure Entra ID. See Scope *(on page 512)*.

To clear the values you entered, click **Reset inputs**.

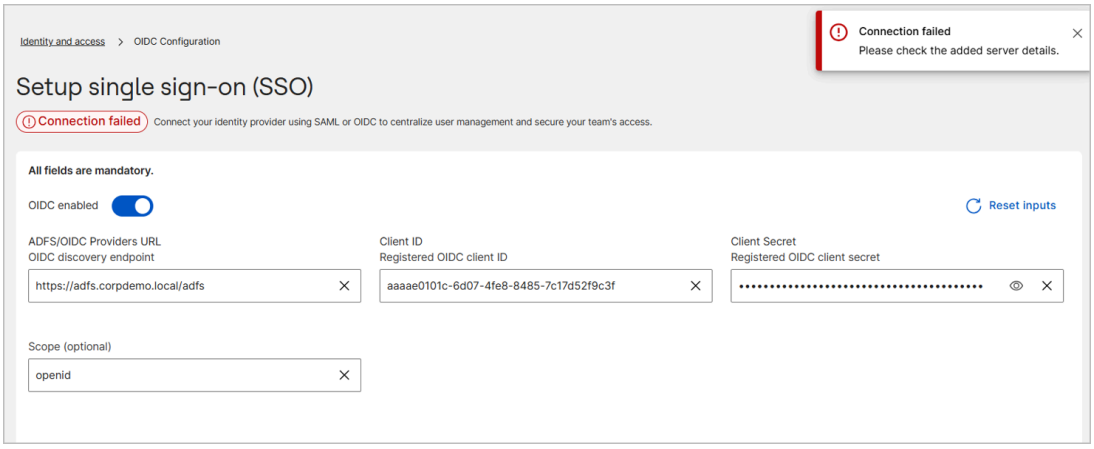
5. Click **Test connection**.

   The button is enabled after all mandatory fields are complete. BigFix UI attempts to connect to the provider with the values that you entered.

   - If the values are valid, the **Connection passed** status is displayed next to the page title. Continue with the next step.

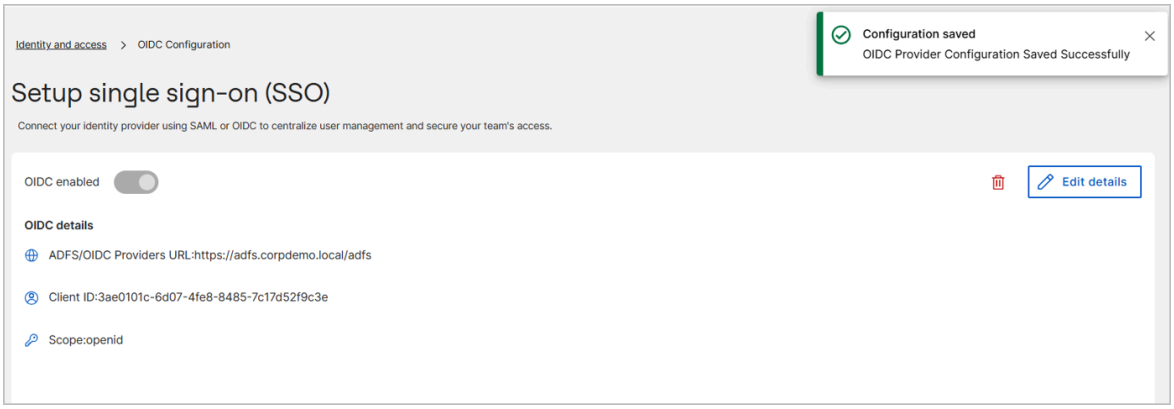


   - If the values are not valid or the provider cannot be reached, the **Connection failed** status is displayed. Correct the Provider URL, the credentials, the certificate trust, or the network access, and test again.

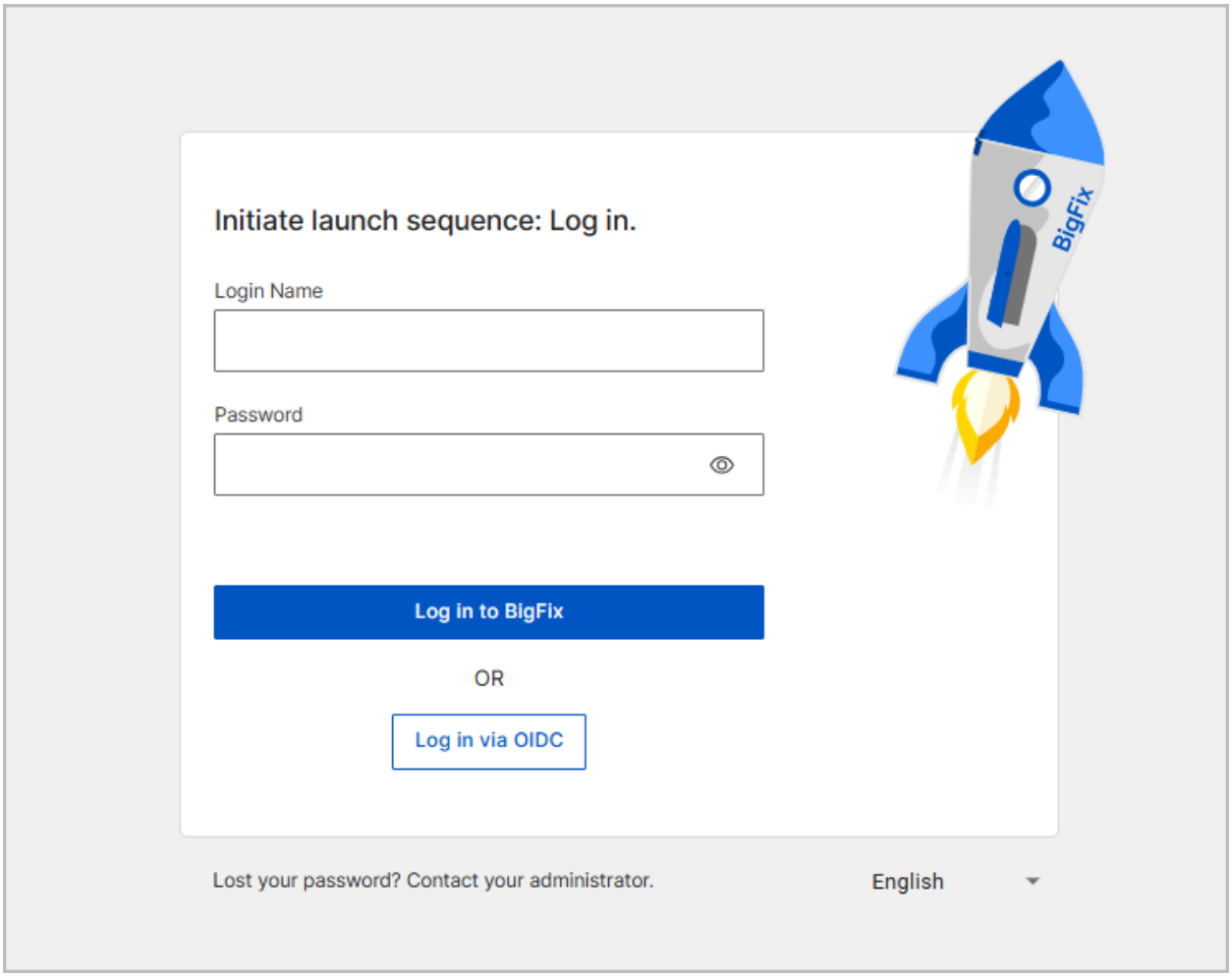


6. Save the configuration.

The **Configuration saved** message confirms that the OIDC provider configuration is saved. The **Setup single sign-on (SSO)** page shows the **OIDC details** with the Provider URL, Client ID, and scope. The client secret is not displayed.



The BigFix UI login page now shows the **Log in via OIDC** button below **Log in to BigFix**.



- Create the users that will sign in through the provider as Identity provider (Idp) users in User & Role Management, bound to a BigFix operator. See Creating a new user *(on page 454)*.
- Ask a test user to click **Log in via OIDC**, authenticate at the provider, and confirm that the BigFix UI dashboard opens. See Logging in with OIDC *(on page 510)*.
- To temporarily stop OIDC logins without losing the configuration, turn off the **OIDC enabled** toggle. To remove the configuration, click the **Delete** (trash can) icon.

Related information

OIDC Configuration *(on page 492)*

OIDC provider settings reference *(on page 512)*

Registering BigFix UI with your identity provider *(on page 495)*

Configuring the identity provider on the BigFix Console *(on page 503)*

Logging in with OIDC *(on page 510)*

Identity management *(on page 447)*

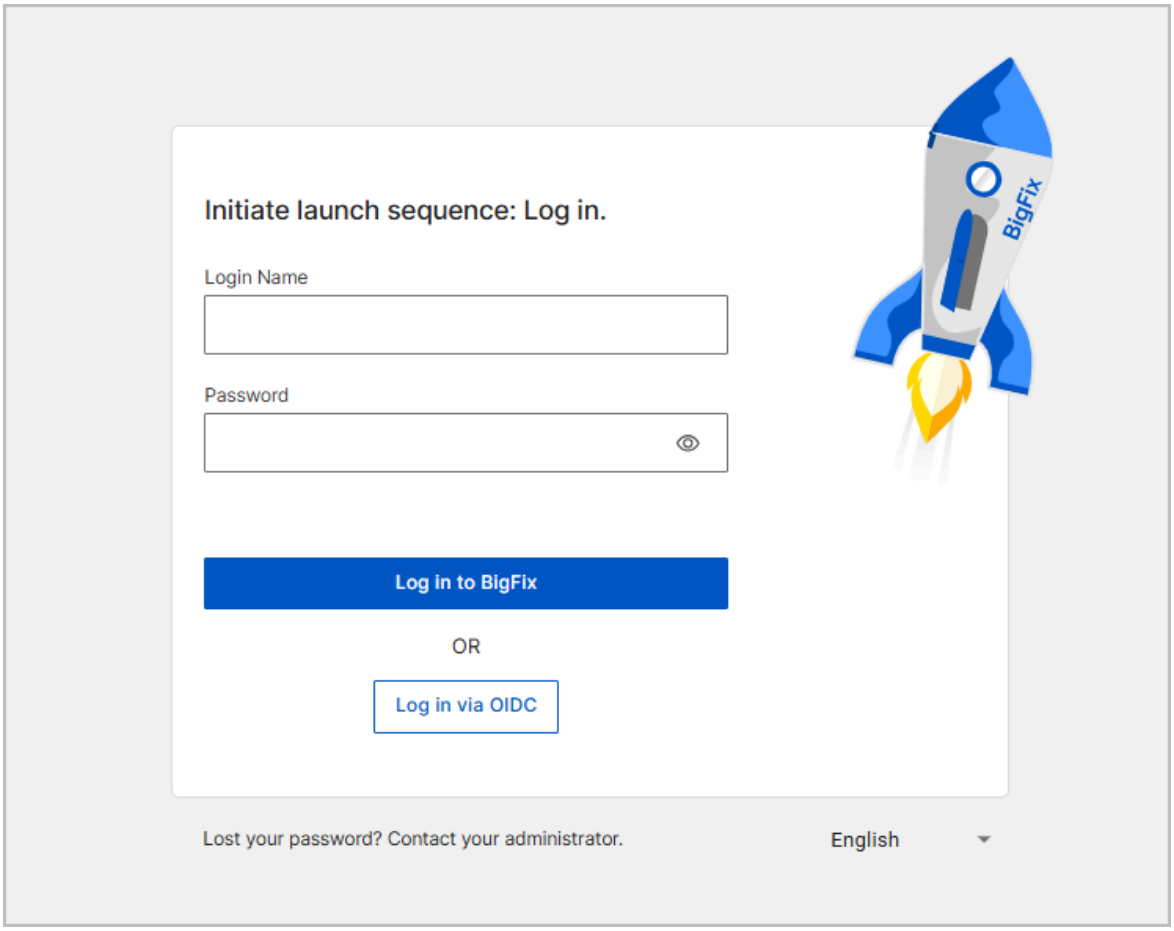
Logging in with OIDC

After OIDC is configured and enabled, users sign in to BigFix UI with their organizational credentials by clicking **Log in via OIDC** on the login page.

Before you log in with OIDC, verify that all of the following are complete:

- BigFix UI is registered with the identity provider, and the redirect URL is configured. See Registering BigFix UI with your identity provider *(on page 495)*.
- The identity provider is configured on the BigFix Console, and an identity provider operator exists for the user. See Configuring the identity provider on the BigFix Console *(on page 503)*.
- The OIDC configuration is saved in BigFix UI, and the **OIDC enabled** toggle is on. See Configuring OIDC single sign-on *(on page 506)*.
- A BigFix UI user with the authentication method **Identity provider (Idp)** exists for the user and is bound to the operator. See Creating a new user *(on page 454)*.

1. Open the BigFix UI login page in a browser.



2. Click **Log in via OIDC**.

   Note: If the button is not displayed, OIDC is not enabled. Ask the instance admin to check the OIDC configuration.

   The browser is redirected to the login page of the identity provider.

3. Authenticate with the credentials of your identity provider.
   Complete any additional checks that your provider requires, such as multifactor authentication.

The identity provider redirects the browser back to BigFix UI. BigFix UI validates the token, creates a session, and opens the dashboard with the permissions of the BigFix operator that the user is bound to.

Logging out of BigFix UI ends only the BigFix UI session. It does not log you out of the identity provider.

Related information

OIDC Configuration *(on page 492)*

Configuring OIDC single sign-on *(on page 506)*

Creating a new user *(on page 454)*

OIDC provider settings reference

The Provider URL, scope, and redirect URL values that BigFix UI requires differ for each supported identity provider. Use this reference when you register BigFix UI with your provider and when you complete the OIDC configuration fields.

Provider URL

The Provider URL is the base URL of the OIDC identity provider. BigFix UI uses it to discover the OIDC endpoints of the provider and to authenticate users. The format depends on the provider.

Table 106. Provider URL format by identity provider

Provider	Format	Example
ADFS	The ADFS server domain followed by `/adfs`: `https://{domain-name}/adfs`	`https://adfs.corpdemo.local/adfs`
Azure Entra ID	The Microsoft login URL with the tenant ID of your Entra ID tenant: `https://login.microsoftonline.com/{tenant-id}/v2.0`	`https://login.microsoftonline-.com/ab223859-234e-4efg-b123-1a2b3c4d5e6f/v2.0`
Okta	The Okta organization URL of your Okta account: `https://{okta-org-name}.okta.com`	`https://integrator-234567.okta.com`

Restriction: For Okta, the Provider URL (issuer) must have `okta.com` as its domain suffix. Custom Okta domains are not supported in this release.

Scope

The value to enter in the **Scope (optional)** field depends on the provider.

Table 107. Scope value by identity provider

Provider	Scope	Required
ADFS	`openid`	Optional
Azure Entra ID	`.default`	Mandatory
Okta	Not applicable	Leave the field empty

Client ID and client secret

The client ID and client secret are the credentials of the OIDC application that is registered for BigFix UI with the identity provider. Obtain these values from your identity provider administrator or from the owner of the application. BigFix UI does not generate them. See Registering BigFix UI with your identity provider *(on page 495)*.

Redirect URL

Configure the redirect URL, also called the redirect URI or reply URL, in the identity provider. It must point to the BigFix UI server address that the browser uses, in the following format:

```
<scheme>://<bfui-host>:<port>/oidc/callback
```

For example:

- `https://bfui.example.com/oidc/callback`
- `https://10.134.85.110:8080/oidc/callback`

Apply the following rules:

- The host name or IP address must resolve from the browser that is used to access BigFix UI, and it must point to the BigFix UI server.
- The redirect URL must end with the `/oidc/callback` path.
- The redirect URL that is configured in the provider must match the URL that BigFix UI uses. A mismatch in the scheme, host name, IP address, port, or callback path causes authentication to fail.
- If, during the BigFix UI setup, the host name is configured with a DNS name, use the DNS name in the redirect URL. If it is configured with an IP address, use the IP address.
- Omit the default ports, `80` for HTTP and `443` for HTTPS. Specify only non-default ports.

For example, if users access BigFix UI at `https://bfui.example.com`, the redirect URL is `https://bfui.example.com/oidc/callback`. If they access it at `https://10.134.85.110:8080`, the redirect URL is `https://10.134.85.110:8080/oidc/callback`.

Provider URL accessibility

The Provider URL must be reachable from both the BigFix UI server and the client browser:

- The provider must be reachable over HTTPS from the BigFix UI server.
- The provider must present a valid, trusted SSL/TLS certificate. The certificate must not be expired, and its host name must match the configured Provider URL.
- If the provider uses a private or internal certificate authority (CA), add the CA certificate to the trusted certificate store on the BigFix UI server. For example, if ADFS uses a local CA, the BigFix UI server must trust that CA.
- Network and firewall rules must not block traffic between the BigFix UI server and the provider.
- The client browser must also reach the provider, because the user is redirected to the provider during authentication.

Related information

OIDC Configuration *(on page 492)*

Registering BigFix UI with your identity provider *(on page 495)*

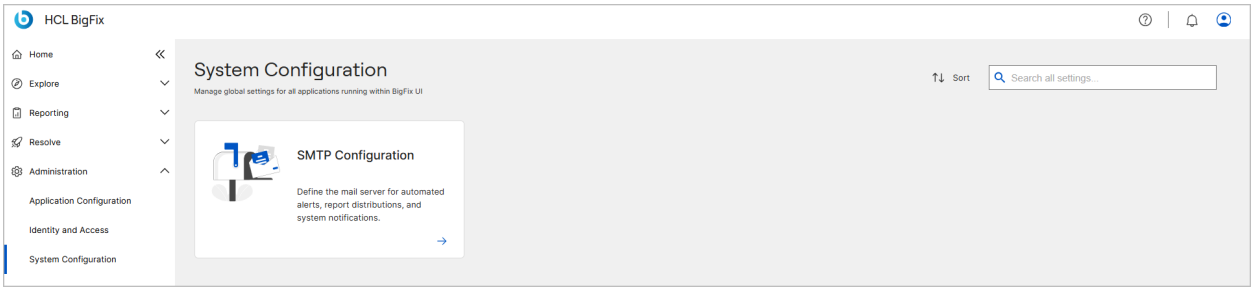
Configuring OIDC single sign-on *(on page 506)*

System configuration

Use System configuration to manage the global settings that every application in BigFix UI shares. In this release, System configuration contains the SMTP settings that BigFix UI uses to send email.

A global setting applies to the whole product rather than to one application. Because BigFix UI sends scheduled reports, alerts, and system notifications by email, it needs a mail server to relay those messages. You define that mail server in System configuration, and every application then uses it.

To open the page, expand **Administration** in the side navigation, and then select **System Configuration**.



Settings catalog

The page shows one card for each group of global settings that you can manage. Select the arrow on a card to open its settings. Use **Search all settings** to find a card by name, and **Sort** to change the order of the cards.

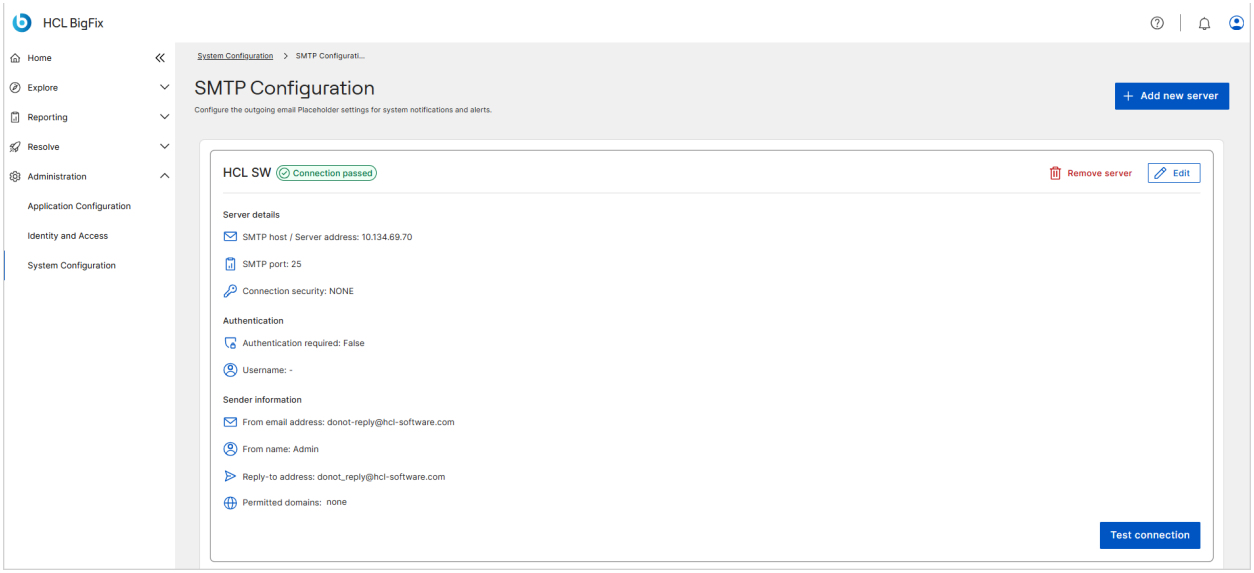
This release provides one card:

- **SMTP Configuration** – Define the mail server for automated alerts, report distributions, and system notifications.

SMTP Configuration page

The **SMTP Configuration** page holds the mail server profiles that BigFix UI can use. A profile is one named set of server, authentication, and sender settings. You can configure more than one profile, which lets you relay mail for different recipient domains through different servers.

Each saved profile appears as a card. The card heading is the profile name, and a status shows whether the last connection test succeeded. The card summarizes the profile in three groups: **Server details**, **Authentication**, and **Sender information**. For a description of every field, see SMTP configuration reference *(on page 522)*.



Note: The page subtitle in the current build contains a placeholder word. Ignore it; the settings on the page behave as described in this topic.

Connection tests

BigFix UI does not save a profile until you test it. When you select **Test connection**, BigFix UI sends a message from the address in **From email address** to that same address and reports the result. If the test succeeds, the profile shows **Connection passed** and you can save it. You can run the test again at any time from the profile card.

The test confirms that BigFix UI can relay mail through the server. It does not confirm that a mailbox exists for the sender address.

Permitted domains

A profile can restrict the recipient domains that it serves. Add one or more domains under **Permitted domains**, and the profile sends mail only to addresses in those domains. If you add no domains, the profile allows all domains.

What you can do

- Add a mail server profile and test it before you save it. See Add an SMTP server profile *(on page 516)*.
- Edit, retest, or remove an existing profile. See Manage SMTP server profiles *(on page 519)*.
- Look up each field, its allowed values, and its default. See SMTP configuration reference *(on page 522)*.

Add an SMTP server profile

Add a mail server profile so that BigFix UI can send scheduled reports, alerts, and system notifications by email. Test the connection before you save the profile.

Collect the following information from your mail administrator:

- The host name or IP address of the SMTP server, and the port that it listens on.
- The connection security that the server requires.
- The user name and password, if the server requires authentication.
- The sender address that the server accepts.

You can add more than one profile. BigFix UI does not enable **Save changes** until a connection test succeeds, so complete every field before you run the test.

1. Expand **Administration** in the side navigation, and then select **System Configuration**.
2. On the **SMTP Configuration** card, select the arrow.
   The **SMTP Configuration** page opens.
3. Select **Add new server**.
   A blank profile form opens above the existing profile cards.
4. Under **Server details**, identify the mail server.
   a. In **Profile name**, enter a name for the profile.

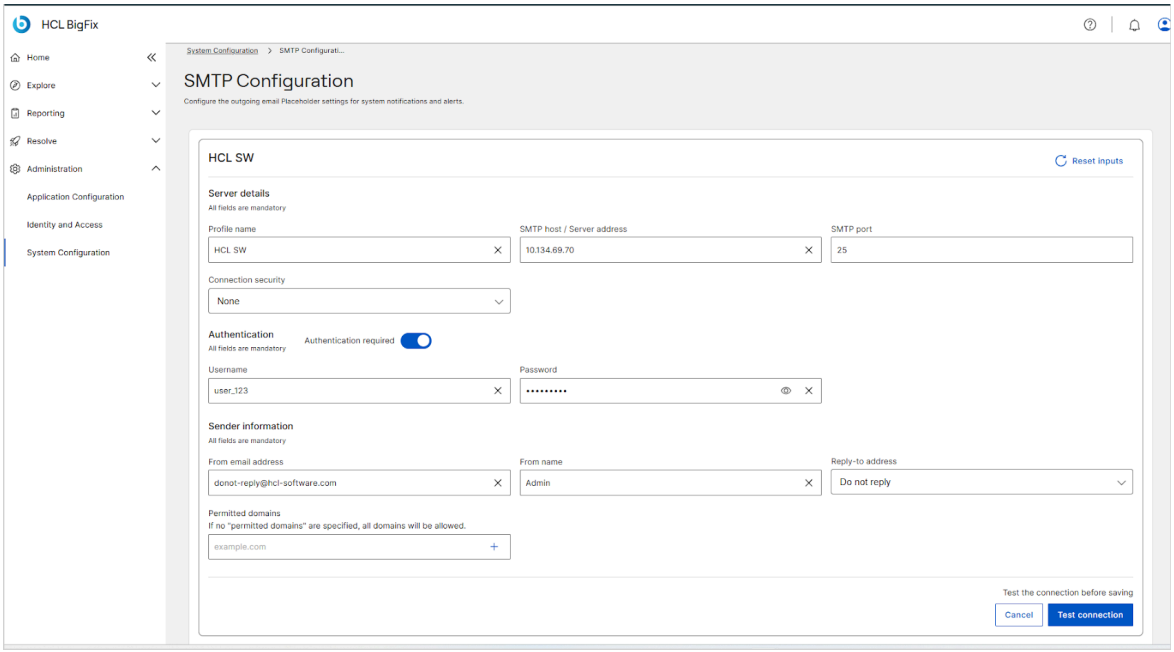
      The name becomes the heading of the profile card. Use a name that identifies the server or the domain that it serves.

   b. In **SMTP host / Server address**, enter the host name or IP address of the server.

   c. In **SMTP port**, enter the port that the server listens on.

   d. From the **Connection security** list, select **TLS** or **None**.

      Note: Select **TLS** if you turn **Authentication required** on in the next step, or if you entered port 465. BigFix UI does not save a profile that pairs authentication with an unencrypted connection. See SMTP authentication requires TLS *(on page 521)*.



5. Under **Authentication**, set **Authentication required**.
   - If the server requires credentials, leave the toggle on, and then enter the **Username** and **Password**. Select the eye icon to show or hide the password.
   - If the server accepts unauthenticated relay, turn the toggle off. BigFix UI hides the **Username** and **Password** fields.

   Note: BigFix UI encrypts the password before it sends it. The password is never transmitted or stored in plain text.

   Restriction: If you leave the toggle on while **Connection security** is **None**, the **Connection security** field shows `Select TLS when authentication is enabled` and you cannot save the profile. Return to the previous step and select **TLS**. See SMTP authentication requires TLS *(on page 521)*.

6. Under **Sender information**, define the sender.

   a. In **From email address**, enter the address that recipients see in the From header.

   b. In **From name**, enter the display name that accompanies the address.

   c. From the **Reply-to address** list, select **Do not reply**, **Same as sender**, or **Custom address**.

   If you select **Custom address**, enter the address that receives replies.

7. **Optional:** Under **Permitted domains**, restrict the recipient domains that this profile serves.

a. Enter a domain, for example `example.com`.

b. Select the plus sign.
   The domain is added as a chip below the field. To remove a domain, select the **X** on its chip.

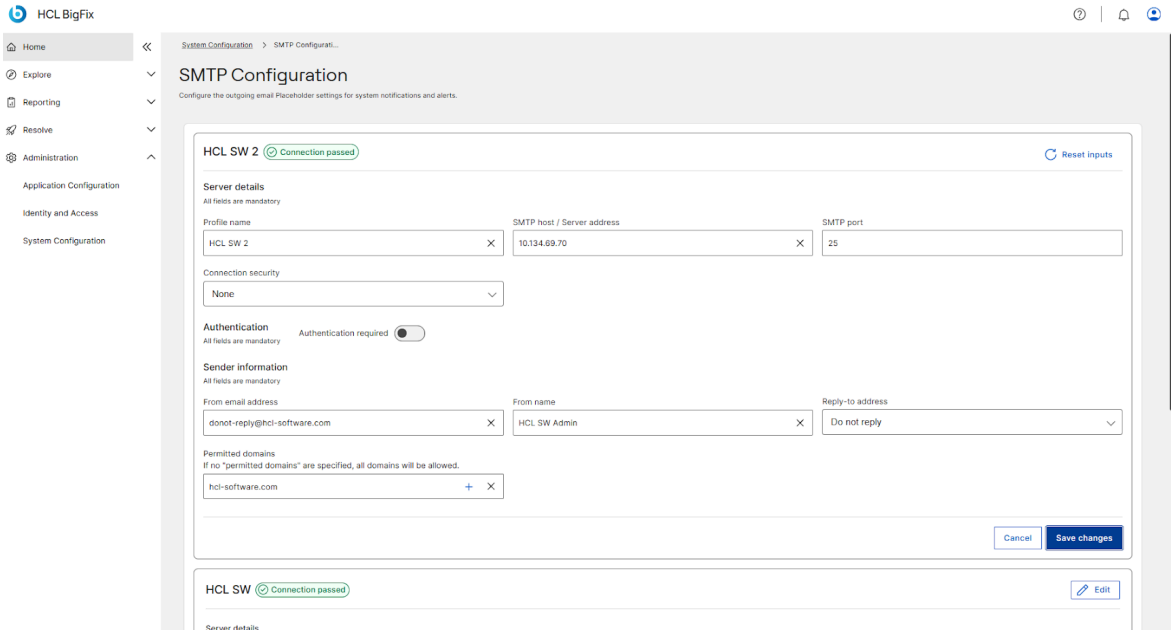
c. Repeat for each domain that the profile serves.

If you add no domains, the profile allows all domains.

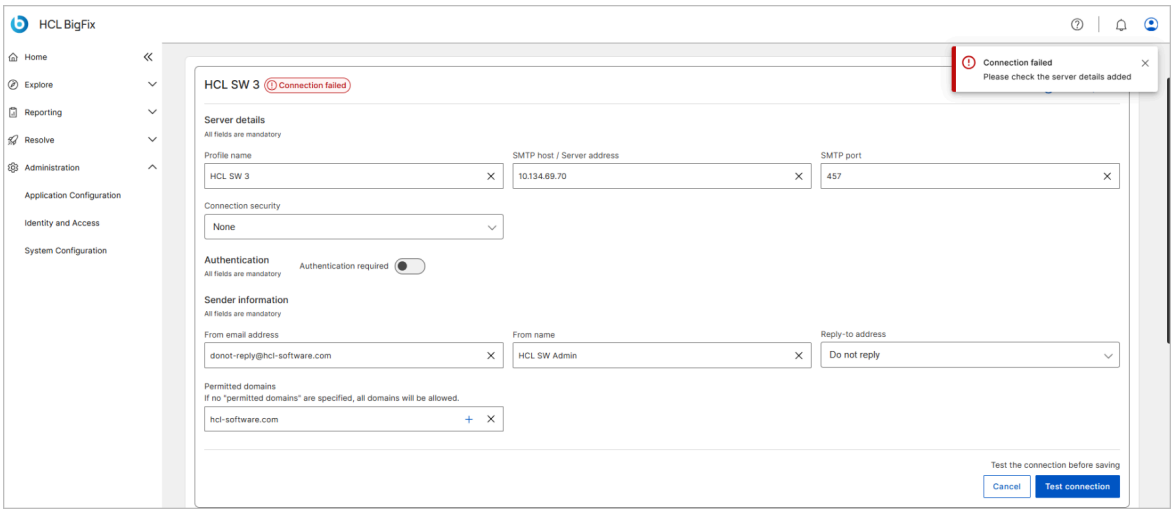
8. Select **Test connection**.

   BigFix UI sends a message from the address in **From email address** to that same address.

   If the test succeeds, **Connection passed** appears next to the profile name, and **Test connection** is replaced by **Save changes**.



If the test fails, **Connection failed** appears next to the profile name, and a notification in the upper right corner asks you to check the server details. Correct the values, and then select **Test connection** again. You cannot save the profile until the test succeeds.



A failed test usually points to a wrong server address, a port that does not match the connection security, missing or invalid credentials, or a sender address that the server rejects. See Connection status *(on page 524)*.

If the profile uses **TLS** and the test still fails, the mail server certificate might not be trusted by the machine certificate store on the BigFix UI server. See SMTP authentication requires TLS *(on page 521)*.

9. Select **Save changes**.

The profile is saved and appears as a card on the **SMTP Configuration** page with the **Connection passed** status. BigFix UI can now send email through this server.

To discard the profile before you save it, select **Cancel**. To clear every field and start again, select **Reset inputs**.

Related information

System configuration *(on page 514)*

Manage SMTP server profiles *(on page 519)*

SMTP authentication requires TLS *(on page 521)*

SMTP configuration reference *(on page 522)*

Manage SMTP server profiles

Edit a saved mail server profile, retest its connection, or remove a profile that you no longer need.

At least one SMTP server profile must exist. To add one, see Add an SMTP server profile *(on page 516)*.

Each saved profile appears as a card on the **SMTP Configuration** page. Open the page by expanding **Administration** in the side navigation, selecting **System Configuration**, and then selecting the arrow on the **SMTP Configuration** card.

- To edit a profile, select **Edit** on its card.

  The card is replaced by the profile form. Change the values that you need, select **Test connection**, and then select **Save changes**. As with a new profile, BigFix UI does not enable **Save changes** until the test succeeds.

  To return the form to the last saved values, select **Reset inputs**. To leave the profile unchanged, select **Cancel**.

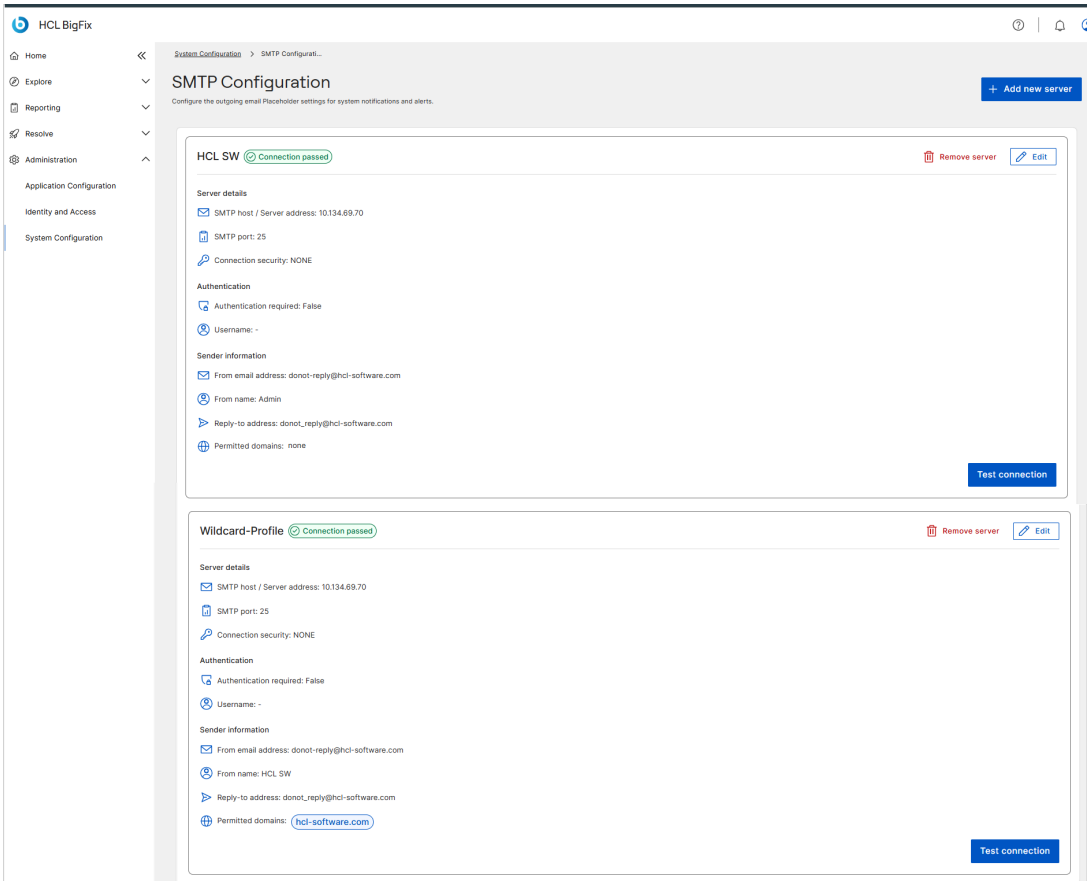
- To verify that a saved profile still works, select **Test connection** at the bottom of its card.

  Retest a profile after your mail administrator changes the server, the credentials, or the connection security. The status next to the profile name reflects the result of the most recent test: **Connection passed** or **Connection failed**.

  If the status is **Connection failed**, a notification asks you to check the server details. Select **Edit**, correct the values, and test the connection again. For the values to check, see Connection status *(on page 524)*.

- To remove a profile, select **Remove server** on its card.

  Restriction: BigFix UI requires at least one SMTP server profile. **Remove server** appears only when two or more profiles are configured. If only one profile exists, you cannot remove it. To replace it, select **Edit** and change its values, or add the replacement profile first and then remove the original.



Related information

System configuration *(on page 514)*

Add an SMTP server profile *(on page 516)*

SMTP configuration reference *(on page 522)*

SMTP authentication requires TLS

A profile that turns on **Authentication required** must use **TLS** for **Connection security**. BigFix UI rejects the combination of authentication and an unencrypted connection, because credentials must never travel in cleartext.

The limitation

SMTP authentication sends a user name and password to the mail server. On an unencrypted connection, those credentials cross the network in cleartext, where anyone on the path can read them. For this reason, BigFix UI does not support a profile that sets **Authentication required** to on and **Connection security** to **None**.

The limitation is a security rule, not a defect. There is no setting that turns it off. If your mail server accepts credentials only on an unencrypted port, ask your mail administrator to enable TLS on the server, or configure the profile for unauthenticated relay instead.

How BigFix UI handles it

BigFix UI enforces the rule in the profile form and again in the backend, so an unsupported profile cannot be saved.

The form flags the combination

If you turn **Authentication required** on and leave **Connection security** set to **None**, the **Connection security** field turns red and shows the message `Select TLS when authentication is enabled`. Change **Connection security** to **TLS** to clear the message.

The backend blocks the save

The backend applies the same rule when it receives the profile, so the combination is rejected even if the form is bypassed. A profile that pairs authentication with an unencrypted connection never reaches storage.

The mail server certificate must be trusted

When a profile uses **TLS**, the certificate that the mail server presents must be trusted by the machine certificate store on the BigFix UI server. Self-signed certificates and certificates from an internal certificate authority fail the connection test until someone adds them to that store. Ask your administrator to import the certificate, and then run the test again.

Port 465 always requires TLS

Port 465 is an implicit TLS port. A profile that uses port `465` must set **Connection security** to **TLS**, whether or not **Authentication required** is on.

What to do

- To authenticate to the mail server, select **TLS** and enter a port that accepts an encrypted connection, such as 465.
- To relay mail without credentials on an unencrypted port, turn **Authentication required** off. BigFix UI then hides **Username** and **Password**, and **None** is a valid connection security.
- If the connection test fails after you select **TLS**, check that the mail server certificate is in the machine certificate store on the BigFix UI server.

Related information

Add an SMTP server profile *(on page 516)*

SMTP configuration reference *(on page 522)*

SMTP configuration reference

Descriptions of the controls on the SMTP Configuration page, the fields in the server profile form, and the connection status values.

Page and card controls

Table 108. SMTP Configuration page controls

Control	Description
Add new server	Opens a blank profile form above the existing profile cards.
Edit	Replaces the profile card with the profile form so that you can change the saved values.
Remove server	Deletes the profile. Appears only when two or more profiles are configured, because BigFix UI requires at least one profile.
Test connection	Sends a message from the address in **From email address** to that same address and reports whether the configuration is valid. Available on a saved profile card and in the profile form.
Save changes	Saves the profile. Replaces **Test connection** in the form after a test succeeds. Not available until then.
Reset inputs	Returns every field in the form to its last saved value, or clears the form for a new profile.
Cancel	Closes the form and discards unsaved changes.

Server details

All fields in this group are required.

Table 109. Server details fields

Field	Description	Value
Profile name	Identifies the profile. Becomes the heading of the profile card.	Text
SMTP host / Server address	Host name or IP address of the mail server that relays the message.	Text
SMTP port	Port that the mail server listens on. Port `465` is an implicit TLS port and always requires **Connection security** to be **TLS**, whether or not authentication is on.	Number. Default: `465`. Enter the port that matches the connection security that the server requires. A port that the server does not accept causes the connection test to fail.
Connection security	Encryption that BigFix UI uses to reach the mail server. Select **None** only when the server accepts unencrypted connections and **Authentication required** is off. With authentication on, **None** is invalid and the field shows `Select TLS when authentication is enabled`. When you select **TLS**, the mail server certificate must be trusted by the machine certificate store on the BigFix UI server. See SMTP authentication requires TLS *(on page 521)*.	**TLS** (default) or **None**

Authentication

Table 110. Authentication fields

Field	Description	Value
Authentication required	Controls whether BigFix UI signs in to the mail server. When the toggle is off, BigFix UI hides **Username** and **Password**, and the profile card shows **Authentication required: False**. When the toggle is on, **Connection security** must be **TLS**, because credentials must never travel in cleartext.	Toggle. Default: on
Username	Account that BigFix UI uses to sign in to the mail server. Required when **Authentication required** is on.	Text
Password	Password for the account. Masked by default; select the eye icon to show or hide it. BigFix UI encrypts the password before it sends it, so the password is never transmitted in plain text. Required when **Authentication required** is on.	Text

Sender information

Table 111. Sender information fields

Field	Description	Value
From email address	Address that appears in the From header of every message that this profile sends. The connection test also sends its message to this address.	Email address
From name	Display name that accompanies the sender address.	Text
Reply-to address	Address that receives replies. **Do not reply** composes a no-reply address on the permitted domain, **Same as sender** reuses **From email address**, and **Custom address** lets you enter any address.	**Do not reply** (default), **Same as sender**, or **Custom address**
Permitted domains	Recipient domains that this profile serves. Enter a domain and select the plus sign to add it as a chip; select the **X** on a chip to remove it. If you specify no domains, the profile allows all domains.	One or more domain names. Optional

Connection status

Table 112. Connection status values

Status	Meaning
Connection passed	The most recent connection test succeeded. BigFix UI reached the mail server and relayed the test message. The status does not confirm that a mailbox exists for the sender address.
Connection failed	The most recent connection test failed. BigFix UI could not reach the mail server or the server rejected the request. A **Connection failed** notification also appears in the upper right corner with the message `Please check the server details added`. Select the **X** to close the notification. **Save changes** stays unavailable until a test succeeds.

When the status is **Connection failed**, check the following values, and then select **Test connection** again:

- **SMTP host / Server address**. The host name or IP address must resolve and the server must be reachable from BigFix UI.
- **SMTP port**. The port must match the port that the mail server listens on.
- **Connection security**. The setting must match what the server requires. Select **None** only when the server accepts unencrypted connections and authentication is off.
- **Authentication required**. Turn the toggle on and enter valid credentials when the server requires them. With the toggle on, select **TLS**.

- The mail server certificate, when the profile uses **TLS**. A self-signed certificate or a certificate from an internal certificate authority fails until it is added to the machine certificate store on the BigFix UI server.
- **From email address**. The server must accept this sender address.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

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.