

BigFix SaaS User Guide

Contents

Chapter 1. Introduction.....	4
Chapter 2. Getting Started with BigFix SaaS.....	5
Access and security.....	5
Multi-Factor Authentication.....	8
Common Functionalities.....	10
Prescriptive Guidance.....	14
Chapter 3. BigFix SaaS User Guide.....	17
My Dashboard.....	17
Adding devices to BigFix.....	18
Custom Remediation.....	20
Deploy Script.....	20
Install Software.....	23
Update Windows Registry.....	25
CyberFOCUS.....	29
CISA KEV Report.....	30
MITRE APT report.....	33
CyberFOCUS remediation flow.....	35
Deployment Manager.....	38
Deployment Details page.....	39
Device Explorer.....	43
Device Details page.....	47
Setting up remediation flow.....	48
Setting up device maintenance window.....	52
Create Dynamic Device Group.....	55
Create Static Device Group.....	58
On-Prem Relay Deployment.....	61
Client settings management.....	65
Fixlet Explorer.....	68
Fixlet Details page.....	72
Deploying Fixlets.....	76
Fixlet Streams.....	79
Setting up Fixlet Streams.....	80
Fixlet details page.....	84
Create Fixlet Stream.....	85
Troubleshooting.....	86
Common use cases.....	87
Protection Level Agreement (PLA).....	89
Custom PLA.....	92
All Reports.....	94

Migrate.....	96
Start migration.....	100
Add Migration Monitor.....	101
Remove Migration Monitor.....	102
User Management.....	103
Creating a new user.....	105
Editing user profile.....	106
Managing roles.....	107
Integrated Vulnerability Remediation.....	110
IVR Dashboard.....	110
Creating New Datasource.....	127
Manually Importing Vulnerabilities.....	131
IVR Remediation Flow.....	138
Chapter 4. Guides in PDF format.....	152
Index.....	a

Chapter 1. Introduction

BigFix SaaS is an endpoint management platform that automates patch management and inventory across various operating systems and apps. Benefits include cost savings, accessibility, scalability, automatic updates, quick deployment, reliability, high compatibility, SaaS security, and reduced hardware requirements.

BigFix SaaS is an endpoint management platform based on Software as a Service (SaaS). It enables IT operations and security teams to automate and manage patches to hundreds of thousands of endpoints across multiple operating systems and apps, regardless of location, connection type or status as an on-premise, virtual, or cloud endpoint. HCL BigFix automates the management, patching and inventory of nearly 120+ operating systems.

BigFix is a cloud-based service that leverages the BigFix team's decades of experience. The core HCL BigFix platform has the following additional components:

- HCL BigFix for Lifecycle Management (includes Patch Management, Remote Control, Software Distribution, and OS Deployment)
- HCL BigFix for Patch Management (includes vendor patches for Microsoft, UNIX, Linux, and Macintosh operating systems as well as patches for third-party applications by Adobe, Google, and Microsoft)
- HCL BigFix for Security and Compliance (provides common STIG, CIS, and third-party security baselines, network self-quarantine, and removable device control)
- HCL BigFix Inventory (gathers information about installed software and hardware in a customer's infrastructure)
- HCL BigFix for Server Automation (provides hypervisor operations to build and manage virtual machines in a datacenter environment)

Using BigFix has the following benefits:

- Cost savings
- Accessibility
- Scalability
- Automatic updates
- Quick deployment
- Reliability
- High compatibility
- SaaS security
- Decreased hardware requirements for implementation (SaaS version)

Chapter 2. Getting Started with BigFix SaaS

This guide helps you get started with BigFix SaaS solution for managing your endpoints. BigFix SaaS is designed to simplify and streamline the management of users, devices, and deployments within your organization.

Product Overview

BigFix SaaS Endpoint Management Application is a robust platform that enables administrators to efficiently manage user accounts, devices, and software deployments. With a user-friendly interface and powerful functionalities, you can ensure seamless operations and enhanced security for your organization's IT environment.

Feature Overview

User Management

The User Management module allows administrators to create, manage, and monitor user accounts within the organization. Key features include:

- **User Creation:** Add new users with customized roles and permissions.
- **Role-Based Access Control:** Assign roles to users to control their access to various modules and functionalities.

Device Management

The Device Management module provides tools to oversee and maintain all endpoints within the organization. Key features include:

- **Device Enrollment:** Register new devices manually or through automated processes.
- **Device Monitoring:** Monitor the status, performance, and compliance of all registered devices.
- **Remote Management:** Perform remote actions such as restarting, locking, or wiping devices to ensure security.
- **Compliance Policies:** Define and enforce compliance policies for devices to meet organizational standards.

Deployment Management

The Deployment Management module enables administrators to deploy software, updates, and configurations across endpoints. Key features include:

- **Software Deployment:** Distribute software packages to selected devices or groups.
- **Update Management:** Schedule and automate software updates to keep devices up-to-date.
- **Configuration Management:** Apply configuration settings to devices to ensure uniformity and compliance.
- **Deployment Reports:** Generate reports on deployment status and success rates for analysis and troubleshooting.

Access and security

Learn how to securely log in and out of the 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.

Logging In

To access BigFix SaaS application, follow these steps:

1. **Open the BigFix SaaS application URL:** Launch your preferred web browser and navigate to <https://login.bigfix.com> to access BigFix SaaS application.

2. **Enter Your Credentials:** On the login page, enter your user name and password in the respective fields.



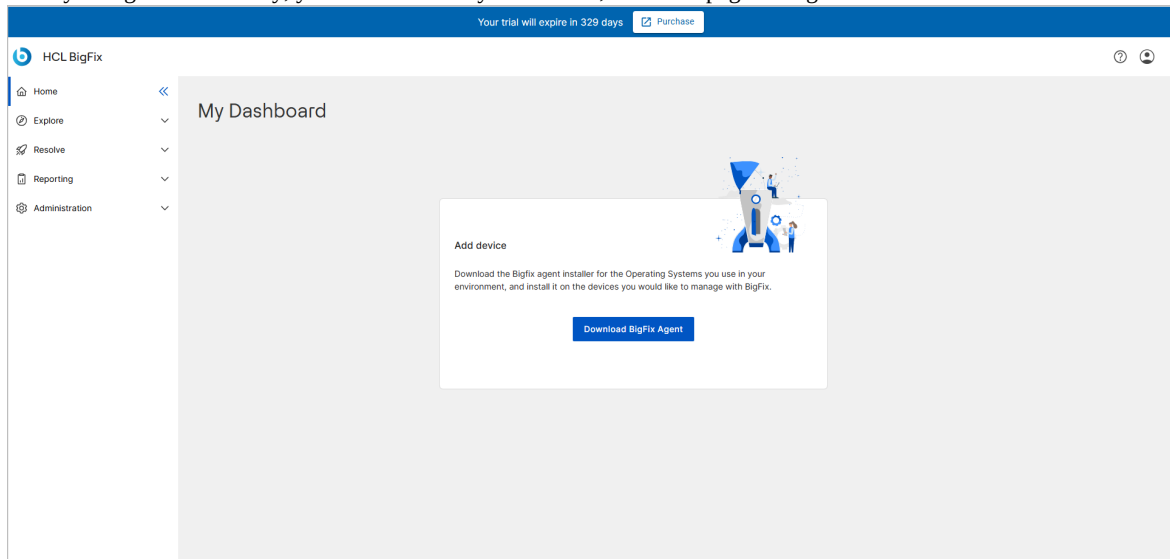
Note: If you are a first time user, check the email you have received from BigFix for the credentials.

3. **Click 'Log in':** Once you have entered your credentials click the 'Log in' button.
4. **Changing temporary password:** First time user receives a **welcome email** containing a temporary password. On first login, the application prompts you to **change the temporary password**.
5. **Multi-factor Authentication:**
 - If the BigFix SaaS admin enforced [Multi-Factor Authentication \(on page 8\)](#) (MFA) for your account, you will be redirected to activate Time-Based One-Time Password (TOTP).
 - If MFA is not enforced, you will be logged in immediately after changing the password.
6. **TOTP Activation**
 - a. When prompted, you will be guided to install an authenticator app (Google Authenticator or Microsoft Authenticator).
 - b. A QR code is shown for easy configuration.
 - c. After scanning the code, you must enter the 6-digit TOTP to complete the set up. On success, you will be logged into BigFox SaaS.



Note: If incorrect TOTP is entered repeatedly, login attempts are temporarily blocked to increase friction for attackers.

7. After you log in successfully, you are taken to My Dashboard, the home page of BigFix.



Logging Out

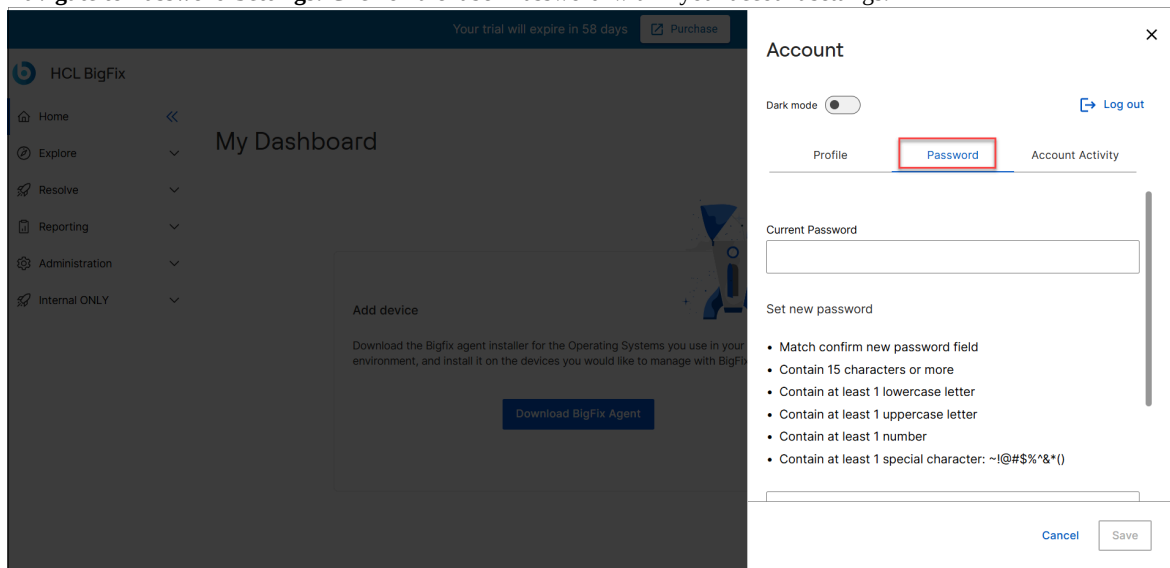
To ensure the security of your account, always log out when you are finished using the application:

1. **Access the User Menu:** Click on your profile icon at the top-right corner of the application window.
2. **Log out:** Click '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 Profile Settings:** Click on your profile icon at the top-right corner to display your account information.
2. **Navigate to Password Settings:** Click on the label 'Password' within your account settings.



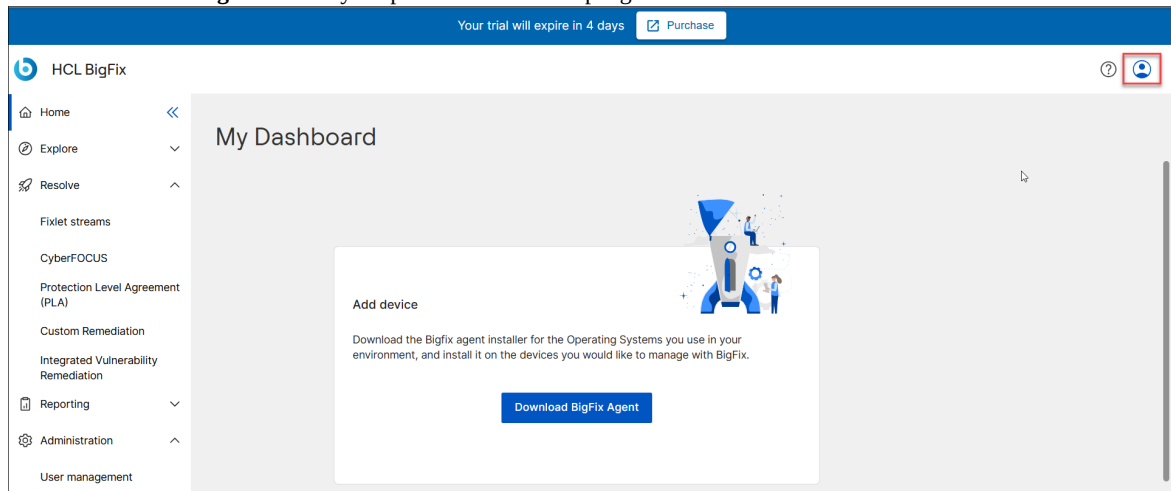
3. **Enter Current Password:** Enter old password for verification.
4. **Enter New Password:** Type your new password in the designated field. Ensure it meets the security requirements specified.

5. **Confirm New Password:** Re-enter the new password to confirm.
6. **Update Changes:** Click the **Save** button to apply the changes. You need to log in again using your new password.

Changing Profile Information

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

1. **Access Profile Settings:** Click on your profile icon at the top-right corner and select 'Profile'.



2. **Update the Fields:** Modify the information as needed. Ensure the required fields are filled in.
3. **Save Changes:** Click the **Save** button to save your changes. Your profile information updates immediately.

Related information

[Multi-Factor Authentication \(on page 8\)](#)

[User Management \(on page 103\)](#)

Multi-Factor Authentication

Secure user access to BigFix SaaS with MFA using authenticator apps.

Overview

MFA adds a second layer of protection during login by requiring both a password and a time-based code from an authenticator app, improving account security. Multi-Factor Authentication (MFA) enhances the security of your BigFix SaaS environment by requiring users to verify their identity with a second factor beyond the password. MFA is especially recommended for business partners managing multiple tenants, each with critical enterprise data, to protect against unauthorized access.



Note: With this release, Time-Based One-Time Password (TOTP) authenticator apps—such as Google Authenticator or Microsoft Authenticator—are supported.

Key Benefits

- Adds an extra layer of security beyond passwords
- Reduces risk of compromised credentials
- Aligns with industry standards (e.g., Microsoft O365)
- Empowers administrators to enforce security policies across all tenant users

Enforcing MFA for All Users

The SaaS Admin creates a new user through the [User Manager \(on page 103\)](#) app.

SaaS Admins can enforce Multi-Factor Authentication (MFA) for all users within a customer account by enabling the **Require multi-factor authentication (MFA) for all users** toggle in the User Manager app.

The screenshot shows the HCL BigFix User management interface. On the left sidebar, the 'Administration' menu is expanded, and 'User management' is selected. In the top right corner, the 'Require MFA' toggle is turned on (indicated by a black circle). Below the toggle, there are tabs for 'Users' and 'Roles'. The main content area displays a table of users with columns for Full name, Email, Roles, Last seen, Status, and Current login. The table shows 4 users, with the first one being disabled and the others enabled.

	Full name	Email	Roles	Last seen	Status	Current login
1	AA abc.abc	abc@b.com	Test_7238554707	No data	Disabled	No d
10	NC Nishant Custom Existing	custom_nks2_saastryandbuytest@yopmail.com	Custom_Nishant	10 Dec, 2025 at 13:56	Enabled	No d
11	NN Nishant New_10Dec	nks2_saastryandbuytest@yopmail.com	Administrator	10 Dec, 2025 at 13:51	Enabled	10 D
12	NS Nishant Soni	nks_saastryandbuytest@yopmail.com	Administrator	16 Dec, 2025 at 16:35	Enabled	No d

Once this option is activated, all users will be prompted to configure MFA the next time they log in. To disable enforcement, the admin can simply turn off the toggle at any time.

MFA Recovery (Lost Authenticator App)

- If a user loses access to their authenticator app:
 1. They must contact their SaaS Admin to reset MFA.
 2. The admin resets MFA for the user in User Manager.
 3. On next login, the user must reconfigure MFA.
- If the only SaaS Admin loses MFA access:
 - Open a support ticket with the vendor to reset MFA via the backend (e.g., Cognito).
 - Admin will be prompted to reconfigure MFA on next login.

Related information

[User Management \(on page 103\)](#)

Common Functionalities

Familiarize yourself with the functionalities that are available across modules. These features help you to effectively manage users, devices, and deployments and enhance your management capabilities.

The **Filter Data Set** feature allows you to refine displayed data by defining filter conditions based on specific properties. Use this feature to quickly locate relevant data by applying one or more conditions with logical operators.

Filtering Data

Filtering allows you to view specific subsets of data based on defined criteria.

- **Access Filters:** Click on the filter icon to define your criteria to filter your data.



- **Filter Conditions:** A filter condition consists of the following elements:
 - **Property** refers to the attribute of the data set that you want to filter on.
 - **Operator** defines how the selected property is evaluated.
 - You can filter a data set using a **single condition** or **multiple conditions**.
 - Conditions are grouped into filter blocks. Each filter block can be combined with other blocks using logical operators such as **AND** and **OR**.
 - You can start with a single condition or create multiple conditions to refine the results. Select **Add Condition** to add more conditions within the same filter block. When multiple conditions are present, use **logical operators** to control how the conditions are evaluated.
- **Filter Blocks:** Filter blocks help you group related conditions and build advanced filter logic. Each filter block is evaluated based on the selected logical operator. Select **Add Block** to create a new filter block.
- **Applying Filters:** After defining the required filter data set conditions, select **Apply** to apply the filter. The data view is updated to display only the results that match the defined conditions.
- **Clearing Filters:**
 - Use **Remove Block** to delete a specific filter block.
 - Select **Remove All** to remove all filter blocks and conditions and reset the filter configuration.

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.

- **How to Sort Data:** Click on the column header to sort. Clicking again toggles between ascending and descending order.

Manage Reports

The **Manage Reports** functionality allows users to save their customized data as a report after applying filtering settings. This feature enables users to quickly access the frequently used data.

This functionality is available across all BigFix SaaS applications that support data filtering, including the following:

- [CyberFOCUS \(on page 29\)](#)
- [Device Explorer \(on page 43\)](#)
- [Fixlet Explorer \(on page 68\)](#)
- [Fixlet Streams \(on page 79\)](#)

Here's how the Manage Reports functionality typically works:

Create a new report

1. **Apply Filters and Sorting:** [Filter \(on page 10\)](#) and [sort \(on page 10\)](#) data as applicable based on desired criteria, adjusting the view to display only the most relevant information.
2. Navigate to an app that supports to manage reports and display the data in a list .
3. On the tool bar, click **Manage Reports**.
4. **Report settings:**
 - a. Provide a unique name and description for the customized report for easy reference.
 - b. Click **Save Report**. The newly created report is listed under All views.

Access a saved report

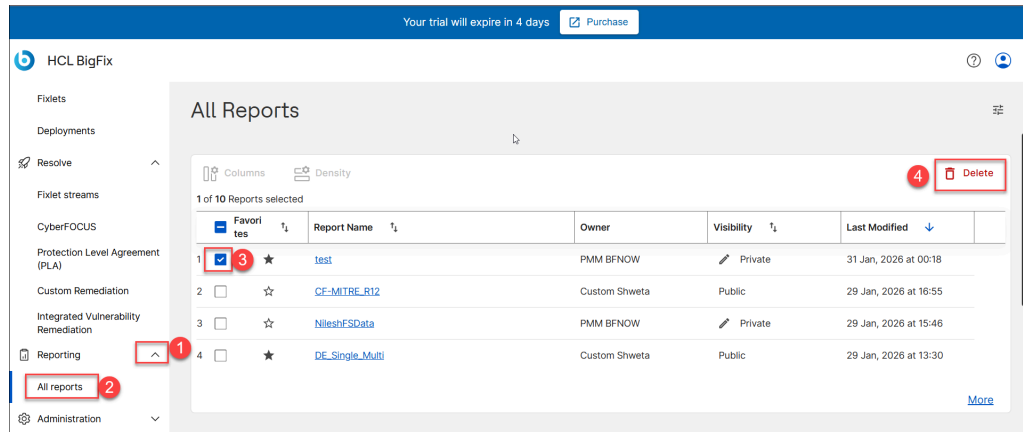
Saved reports are available across sessions, allowing users to load them whenever needed without reapplying the same filters and sorting each time.

1. To load a saved view, expand **Reporting** and click **All reports**.

Delete a report

To remove a saved report:

1. From the **All Reports** page, select a report you wish to delete, then click the delete icon on the top right corner.



2. Confirm the action when prompted.

This permanently removes the selected view from your saved views, and it will no longer be available for future use. This action helps keep your saved views organized by removing outdated or unnecessary configurations.

Exporting Data

The Export Data option is available on Deployments, CyberFOCUS, All reports, 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.

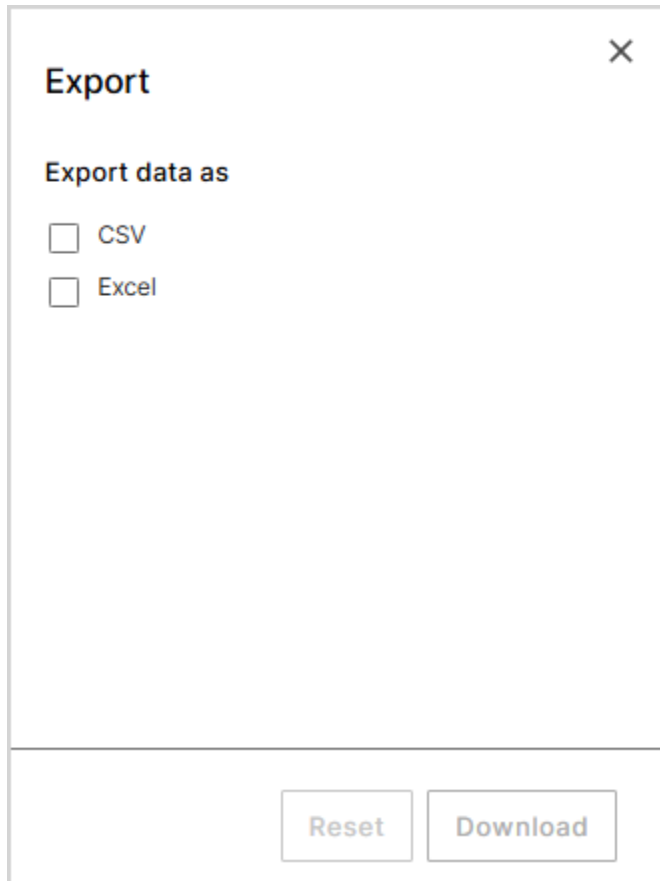
It enables users to export visible report data—filtered, sorted, or customized to commonly used spreadsheet formats like CSV or Excel.

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.



The image shows a modal dialog box titled "Export" with a close button (X) in the top right corner. Below the title, the text "Export data as" is followed by two radio button options: "CSV" and "Excel". At the bottom of the dialog, there are two buttons: "Reset" and "Download".

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.

Exporting Charts

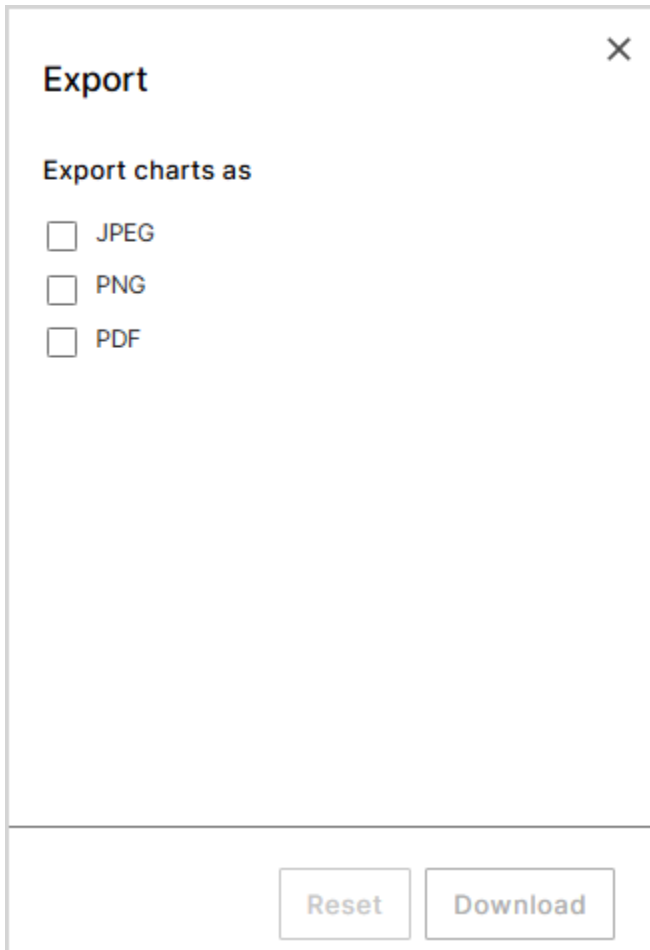
The Export charts option is available on CyberFOCUS and Overview pages of Devices, Fixlets. Use this feature to capture dashboard visualizations from overview pages as image or document files for reporting and presentation purposes. It allows users to download graphical widgets such as bar charts, donut 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.



Export

Export charts as

☐ JPEG

☐ PNG

☐ PDF

Reset Download

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 chosen 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.

Searching Data

The search feature helps you quickly locate specific records.

- **How to Use Search:** Enter keywords or phrases in the search bar. Results update in real-time.
- **Advanced Search:** Use advanced options to refine searches by specifying columns or using logical operators (AND, OR, NOT).

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.
- **Risk Reduction:** It assists in identifying and mitigating security vulnerabilities, reducing the risk of cyber attacks or data breaches across the endpoint environment. It helps users mitigate risks by suggesting actions that address vulnerabilities, security gaps, or non-compliance issues identified across endpoint devices.
- **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 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.

Device explorer - Overview
Updated: Dec 23, 2025 04:56:07

Quick links

24	16	24	0	20	18
Total devices	Devices requiring critical remediations	Devices requiring at least one remediation	Workstations that haven't reported in 30 days	Servers that haven't reported in 48 hours	Devices that lack maintenance windows

Charts

Fixlet Explorer - Overview
Updated: Feb 11, 2026 14:02:18

Quick links

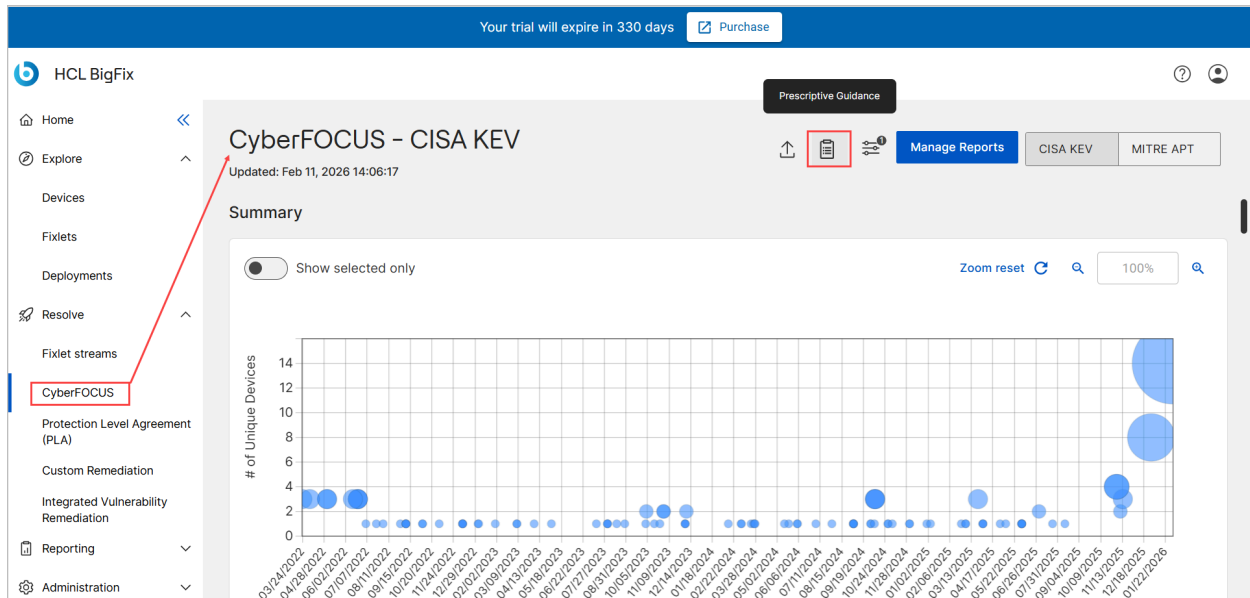
25,580	260	167	114	5	25
Total Fixlets	Fixlets applicable to one or more devices	Applicable Fixlets that address at least one Vulnerability...	Applicable High Severity Fixlets	Relevant Fixlets released in the past 7 days	Relevant Fixlets released in the past 30 days

Charts

Applicable Fixlets by severity (top 4 by count)

Total severities: 154

Applicable Fixlet categories (top 5 by count)



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.

Related information

[CyberFOCUS remediation flow \(on page 35\)](#)

[Setting up remediation flow \(on page 48\)](#)

Chapter 3. BigFix SaaS User Guide

This guide is for the regular users of BigFix SaaS.

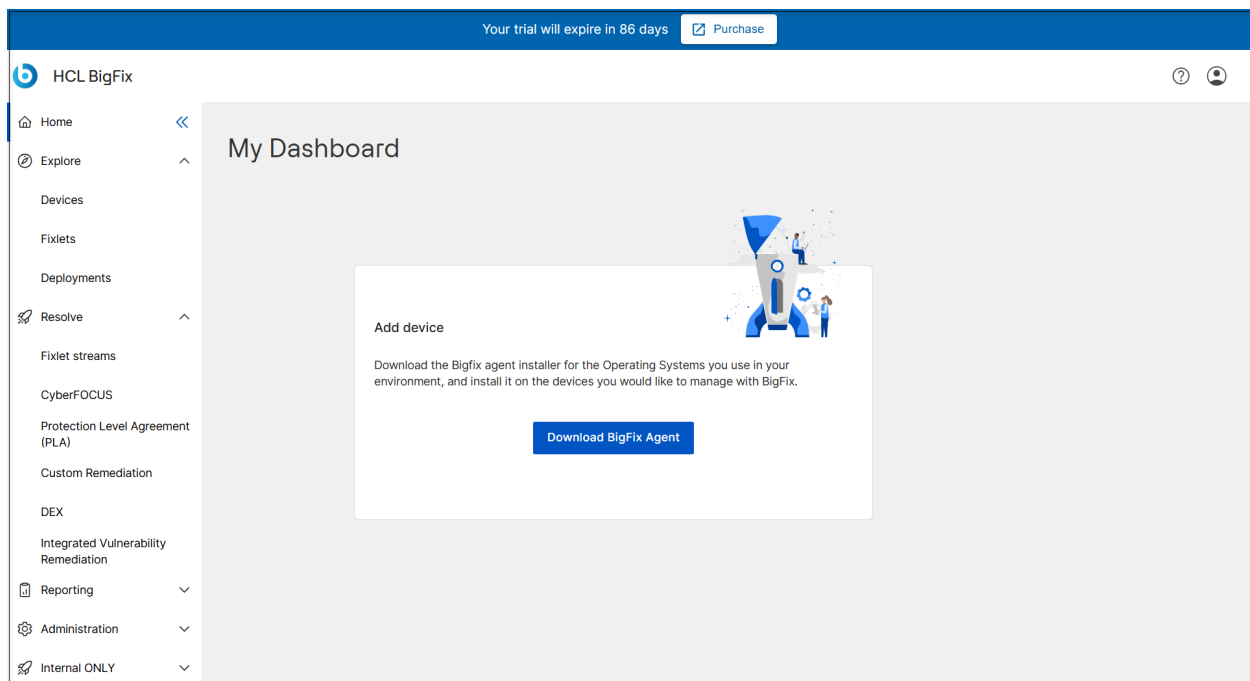
It provides details of the features that are available to a user when they access the SaaS application. For example: accessing BigFix SaaS, creating and managing users, using the available apps - the Deployment Manager, Device Explorer, Fixlet , and User Management.

My Dashboard

My Dashboard is the main page where users can add devices to their deployment and access additional functionality through icons for notifications and user profiles. The platform allows customization with light or dark mode at the account level, affecting all users.

In the top right corner of the Home Page, there are two icons that offer extra features:

- **Notification** icon - where important messages are displayed.
- **User Profile** icon/photo - which takes users to their account management page.



For users with multiple BigFix accounts, each account can choose between light or dark mode.



Note: The Dark Mode feature applies to the entire account, affecting all users and the application.

Click the User Profile icon to access user account profile. click the  switch to toggle between dark and light mode. Click the  icon to view important notifications.

BigFix currently supports the following apps:

- Deployment Manager
- Device Explorer

- Fixlet Explorer
- User Management

Information about these apps and their features can be found in separate sections. To maximize the benefits of BigFix, it is important to add your organization's devices to your BigFix system. Just click **Add device** and follow the instructions on the screen.

Adding devices to BigFix

This task explains how to add devices to BigFix for organizational use. Administrators need to be logged into BigFix to add devices, and the process involves enrolling devices by installing the BigFix agent, which supports various operating systems. BigFix allows managing up to 50,000 devices per deployment and provides tools for device management and removal.

Administrators need to be logged into BigFix platform before adding devices.

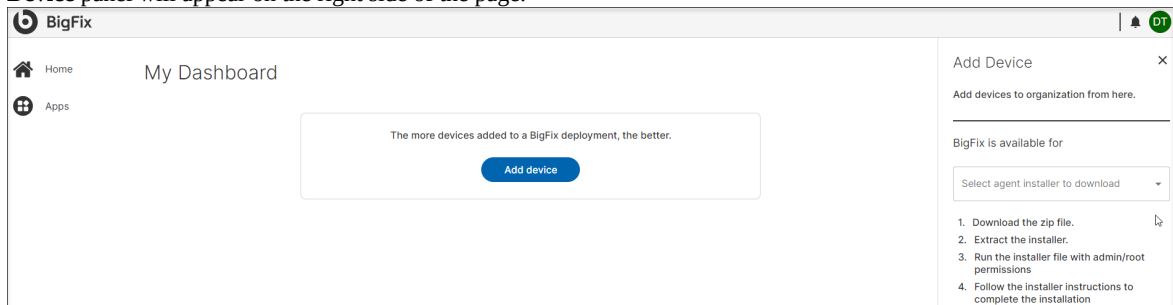


Note: Having at least one device added to your organization's BigFix deployment is essential. Without a device, the BigFix apps cannot be utilized.

The more devices you add to BigFix, the more effective it can be in assisting your organization. All devices added to your BigFix deployment can be viewed in the Device Manager app.

Follow the steps below to add devices:

1. Navigate to **My Dashboard** by clicking the **Home** icon on the left side of the page. Then, click on **Add device**. The **Add Device** panel will appear on the right side of the page.



2. Enrolling a device in your BigFix deployment involves installing the BigFix agent. The agent is a piece of software that runs on the computer and communicates with BigFix server. BigFix SaaS currently supports agents for various operating systems, ensuring compatibility with a wide range of devices.

In the **Add Device** panel, choose the operating system that matches the device to be enrolled in BigFix. For instance, select MacOS for a MacBook or Ubuntu for an Ubuntu server.

3. Once the correct operating system is selected, click the link below the dropdown to download the agent.

BigFix currently supports the following operating systems:

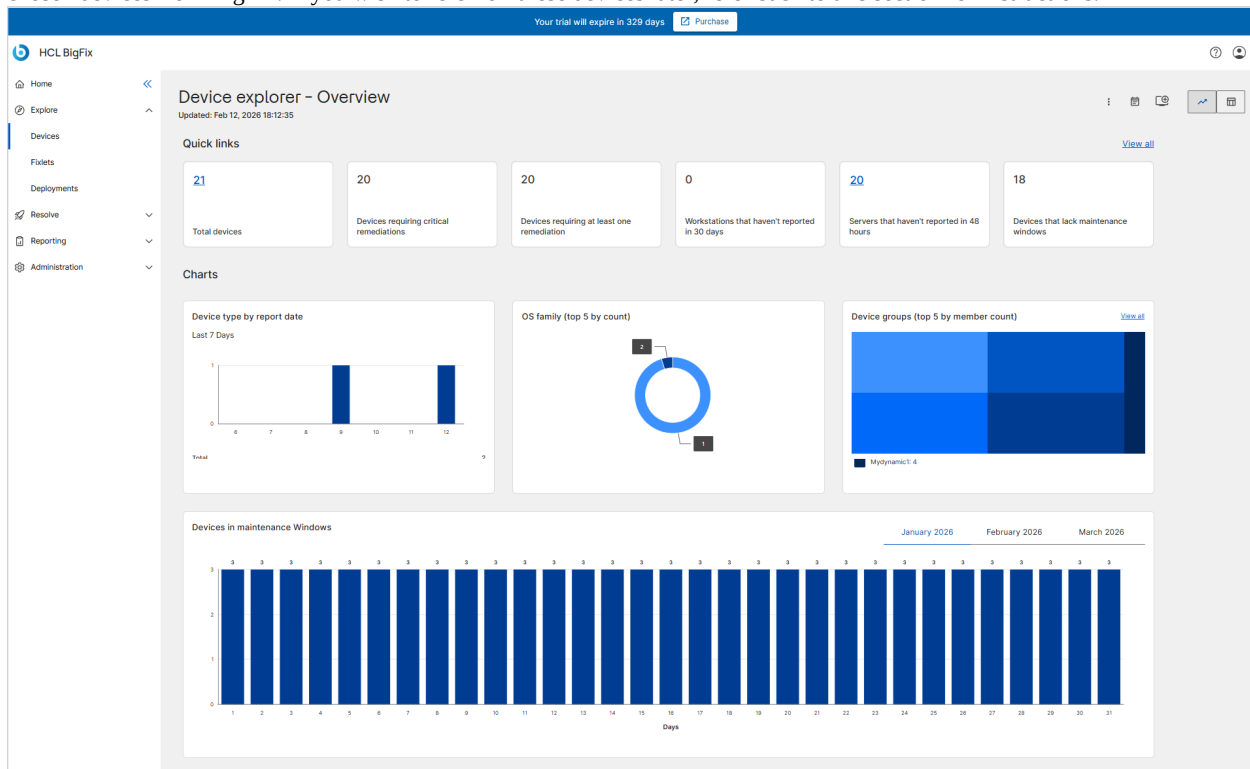
- Windows 10 / 2016 (or greater) (i386)
- Windows 11 (arm64)
- AIX 7.x (ppc64)
- VIOS 3.1.3 (ppc64)
- CentOS 7, 8 (x86_64)
- Debian 10, 11, 12 (x86_64)
- Raspbian 10, 11, 12 (armhf)
- Mac OS (.pkg) 11, 12, 13, 14, 15, 26 (x86_64, arm64)
- Alma Linux 9.5, 9.6, 10 (x86_64)
- Amazon Linux 2, 2023 (x86_64)
- Amazon Linux 2, 2023 (arm64)

- Rocky Linux 8, 9, 10 (x86_64)
- Oracle Enterprise Linux 7, 8, 9 (x86_64)
- Red Hat Enterprise Linux 7, 8, 9, 10 (x86_64)
- Red Hat Enterprise Linux 7, 8, 9 (ppc64le (little-endian))
- Red Hat Enterprise Linux 7, 8, 9 (s390x)
- Solaris 11 (i386)
- Solaris 11 (sparc)
- Solaris (package p5p) 11 (i386)
- Solaris (package p5p) 11 (sparc)
- SUSE Linux Enterprise 12, 15 (ppc64le (little-endian))
- SUSE Linux Enterprise 12, 15 (x86_64)
- SUSE Linux Enterprise 12, 15 (s390x)
- OpenSUSE Leap 15.4, 15.5, 15.6 (x86_64)
- Ubuntu 18, 20, 22, 24 (x86_64)
- Ubuntu 18, 20 (ppc64le (little-endian))
- ESU - Windows 2012 (i386) Windows 10/2016+ (i386)
- MacOS, 11, 12, 13, 14 (x86_64, arm64)
- Amazon Linux 2, 2023 (x86_64)
- RHEL 7, 8, 9 (x86_64)
- Ubuntu 18, 20, 22 (x86_64)

Currently, there is no way to install agents on multiple devices simultaneously; users need to install the agent suitable for each device individually.

4. Once downloaded, install the agent following the standard procedures for the device's operating system. Admin/root privileges are required for successful installation. Proceed with the installer steps until completion.

After installing the agent on a device, it will automatically connect to the BigFix service and appear in the Device Explorer page. BigFix permits managing up to 50,000 devices per deployment. Users can utilize the filter tool to search for devices in their deployment. To remove device(s) from a deployment, select the device(s) and click the **Delete** button. This action eliminates the chosen devices from BigFix. If you wish to re-enroll these devices later, refer back to this section for instructions.



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 SaaS gives IT and security teams enhanced flexibility and control to quickly remediate security vulnerabilities and configuration issues—even when standard Fixlets or out-of-the-box content are unavailable. This feature lets you deploy your own scripts, deploy custom software updates, and apply manual configuration changes. It's ideal for addressing uncovered vulnerabilities, third-party application risks, and non-standard system configurations across your endpoints with speed and precision.

Key features

[Deploy Script \(on page 20\)](#)

If predefined remediation workflows don't cover your needs, and you know exactly what content is required to fix an issue, you can use this feature to create and deploy your own custom script. You can deploy an Action Script, Bash, or PowerShell script directly to the target devices and resolve issues with standard Fixlets.

[Install Software \(on page 23\)](#)

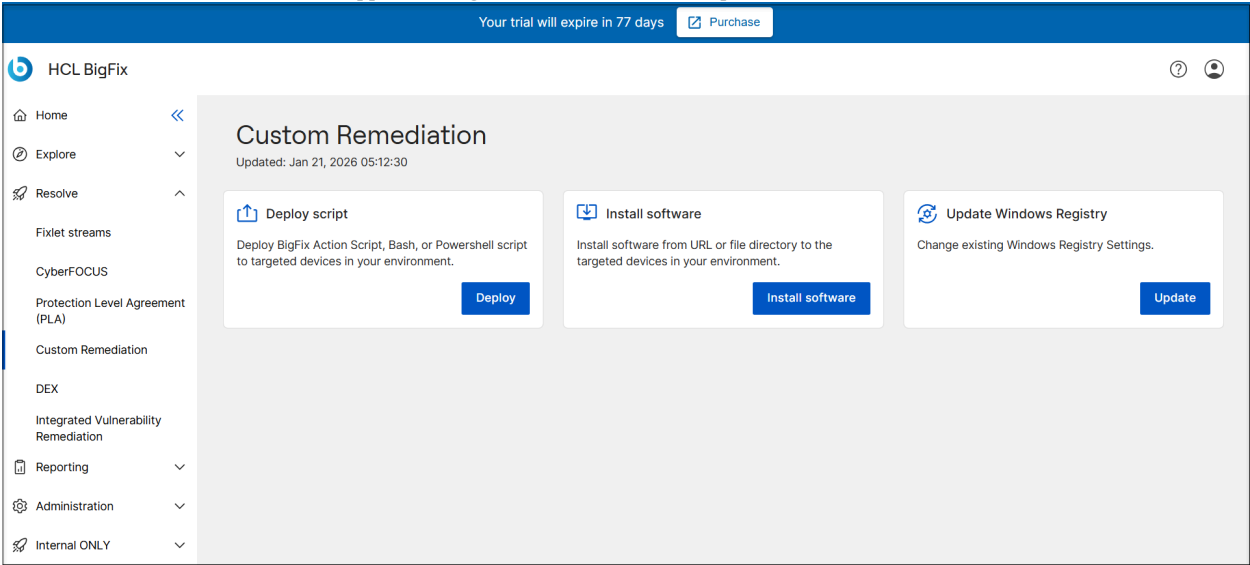
Deploy updates or patches for software (that are not included in standard BigFix content) from the target devices. Support any software Remediate vulnerabilities in any application, even if they are not in the box.

[Update Windows Registry \(on page 25\)](#)

Make quick changes to system settings, similar to the Windows Registry Wizard. Apply configuration changes. Quickly edit registry values, apply configuration updates, or push environment changes across your endpoints waiting for pre-built content

How to access Custom Remediation

To access the Custom Remediation app, from **BigFix SaaS Remediate**, expand **Resolve** and select **Custom Remediation**.



Deploy Script

Run your own scripts to quickly remediate devices. Currently supports bash script, PowerShell, and BigFix Action Scripts. Target specific devices or OS families for fast and flexible deployments.

The **Deploy Script** feature under **Custom Remediation** allows advanced users (power users) to directly deploy scripts to targeted devices for custom remediation purposes. This tool is intended for users who need more control and flexibility than what is available through standard remediation tools.

To open the Deploy Script widget, from the **Custom Remediation** app, on the **Deploy Script** card, click **Deploy**.

The screenshot shows the Custom Remediation app interface. On the left, the 'Custom Remediation' section is visible with a 'Deploy script' card. The 'Deploy' button on this card is highlighted. On the right, the 'Deploy Script' modal is open, showing a progress bar with five steps: Script, Devices, Sequence, Schedule, and Summary. The 'Script' step is currently active. Below the progress bar, there is a section for 'Create custom remediation script'. It includes a dropdown menu to 'Select the script type you want to use.' and a section titled 'How do you want to create the script?' with two buttons: 'Upload File' and 'Input Script'. Below these buttons is a large dashed box with a cloud upload icon and the text 'Drag and drop file or click to browse' and 'File type supported .ps1, .sh, .as'. At the bottom of the modal, there is a 'Browse from computer' button. At the very bottom right of the modal, there are 'Cancel' and 'Next' buttons.

1. **Script:**

- Select a script type from the available options (such as **Powershell**, **bash**, **BigFix Action Script**).
- Upload File** or **Input Script**: Upload a script file or enter the script content directly in the provided field.
- Click **Next**.

2. **Devices:** [Filter target devices \(on page 49\)](#) and click **Next**.

3. **Sequence:** The configured options are processed **sequentially from top to bottom**, giving you precise control over how deployments are delivered, how users are informed, and how failures are handled.

a. **Start downloading immediately**

When enabled, targeted endpoints begin downloading the required payloads as soon as the remediation action is deployed.

b. **Before running message**

When enabled, the configured message is displayed to the end user before the action starts. This can be used to provide context, warnings, or request user confirmation.

c. **While running message**

When enabled and a message is configured, during execution of the action, the notification message is shown to indicate that the remediation is currently in progress. This helps maintain user awareness and reduce support inquiries.

d. **Reboot/restart devices on completion of deployment**

After the remediation completes, targeted devices are automatically rebooted if required by the fixlet. This step ensures that changes are properly applied and system integrity is maintained.

e. **On failure: retry x time and wait x hour between attempts**

If the action fails, you can configure:

- **Number of retries:** how many times the system should reattempt the action.
- **Wait time between retries:** the number of hours to wait between each retry.

This setting increases the success rate by accounting for temporary issues like device disconnection or network latency.

f. **Reapply whenever it becomes relevant again**

Click **Next** to proceed.

4. **Schedule:** Select a time range for the scheduled activity. This setting defines the window during which the schedule remains in effect. After configuring the schedule, click **Next** to proceed.

Field Label	Description
Start Date	Select the calendar date when the remediation deployment should begin.
Start Time	Select the time (hh:mm) at which the remediation should start.
Time Zone (Start)	Choose the time zone to apply for the start time: - Client: Uses each endpoint's local time. - UTC: Uses Coordinated Universal Time.
End Date	Select the calendar date by which the remediation deployment should be completed.
End Time	Select the time (hh:mm) at which the deployment window ends.
Run During Agent's Configured Maintenance Window	Enable this option to restrict the deployment to devices that have a maintenance window configured. The remediation will only run within those windows. ! Note: Devices without a maintenance window will be excluded from the deployment.
Run on All Devices, Regardless of Their Configured Maintenance Window	Enable this option to override maintenance window restrictions. The remediation will run on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Enable this option to apply custom constraints, allowing the selection of a specific date, time, and day of the week.
Reset	Click to clear all current scheduling fields and revert the section to its default state. Use this to start over if needed.

5. **Summary:** The Summary section provides a consolidated view of all the configuration options selected in the remediation flow. It acts as the final checkpoint before deployment, allowing you to review and confirm your settings.

Action name:

- **Enter a unique and meaningful name** that clearly describes the purpose of the action.
- This name will appear in action history, logs, and dashboards, helping you and your team quickly identify and differentiate actions.
- Use descriptive terms (e.g., "*Critical Patch – May 2025 – Windows Devices*") to ensure clarity and traceability.

6. **Deploy the Script:** After verifying the configured information, click **Deploy** to deploy the action.

Related information

[Install Software \(on page 23\)](#)

[Update Windows Registry \(on page 25\)](#)

Install Software

The **Install Software** feature in the **Custom Remediation** app allows you to deploy software to specific devices by simply providing a download link and targeting filtered devices. This is a powerful and flexible way to deliver software without needing to upload packages manually.

Use this feature 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.
- You need a lightweight and quick remediation workflow.

To open the Install Software widget, from the **Custom Remediation** app, click the **Install Software** button.

The screenshot shows the HCL BigFix Custom Remediation app interface. On the left is a sidebar with navigation options: Home, Explore, Resolve, Fixlet streams, CyberFOCUS, Protection Level Agreement (PLA), Custom Remediation (selected), DEX, Integrated Vulnerability Remediation, Reporting, Administration, and Internal ONLY. The main area displays the 'Custom Remediation' app with a 'Deploy script' button and a 'Deploy' button. Overlaid on this is the 'Install Software' widget. The widget has a progress bar with five steps: 1. Software, 2. Devices, 3. Behavior, 4. Schedule, and 5. Summary. The 'Software' step is active. The form includes fields for 'URL', 'SHA-256', and 'Size in bytes'. Below these is a section for 'Installation instruction as Local Administrator'. At the bottom right are 'Cancel' and 'Next' buttons.

1. Enter Software Details:

- **URL:** Provide the direct link to the software package hosted online.



Note: Supported file extensions are **.deb**, **.exe**, **.msi**, **.pkg**, and **.rpm**.

- **SHA-256:** Secure hash used to verify the integrity of the downloaded file.
- **Size in bytes:** Exact file size to validate the download.
- **Installation instructions as Local Administrator:** This field is optional. BigFix automatically generates the base installation command based on the file type (for example, **.msi**, **.exe**) provided in the URL. 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
```

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 Instructions as Local Administrator	/qn

Click **Next**.

2. **Devices:** [Filter target devices \(on page 49\)](#) and click **Next**.

3. **Behavior:** The configured options are processed **sequentially from top to bottom**, giving you precise control over how deployments are delivered, how users are informed, and how failures are handled.

a. **Start downloading immediately**

When enabled, targeted endpoints begin downloading the required payloads as soon as the remediation action is deployed.

b. **Before running message**

When enabled, the configured message is displayed to the end user before the action starts. This can be used to provide context, warnings, or request user confirmation.

c. **While running message**

When enabled and a message is configured, during execution of the action, the notification message is shown to indicate that the remediation is currently in progress. This helps maintain user awareness and reduce support inquiries.

d. **Reboot/restart devices on completion of deployment**

After the remediation completes, targeted devices are automatically rebooted if required by the fixlet. This step ensures that changes are properly applied and system integrity is maintained.

e. **On failure: retry x time and wait x hour between attempts**

If the action fails, you can configure:

- **Number of retries:** how many times the system should reattempt the action.
- **Wait time between retries:** the number of hours to wait between each retry.

This setting increases the success rate by accounting for temporary issues like device disconnection or network latency.

f. **Reapply whenever it becomes relevant again**

Click **Next** to proceed.

4. **Schedule:** Select a time range for the scheduled activity. This setting defines the window during which the schedule remains in effect. After configuring the schedule, click **Next** to proceed.

Field Label	Description
Start Date	Select the calendar date when the remediation deployment should begin.
Start Time	Select the time (hh:mm) at which the remediation should start.

Field Label	Description
Time Zone (Start)	Choose the time zone to apply for the start time: - Client : Uses each endpoint's local time. - UTC : Uses Coordinated Universal Time.
End Date	Select the calendar date by which the remediation deployment should be completed.
End Time	Select the time (hh:mm) at which the deployment window ends.
Run During Agent's Configured Maintenance Window	Enable this option to restrict the deployment to devices that have a maintenance window configured. The remediation will only run within those windows. ! Note: Devices without a maintenance window will be excluded from the deployment.
Run on All Devices, Regardless of Their Configured Maintenance Window	Enable this option to override maintenance window restrictions. The remediation will run on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Enable this option to apply custom constraints, allowing the selection of a specific date, time, and day of the week.
Reset	Click to clear all current scheduling fields and revert the section to its default state. Use this to start over if needed.

5. **Summary:** The Summary section provides a consolidated view of all the configuration options selected in the remediation flow. It acts as the final checkpoint before deployment, allowing you to review and confirm your settings.

Action name:

- **Enter a unique and meaningful name** that clearly describes the purpose of the action.
 - This name will appear in action history, logs, and dashboards, helping you and your team quickly identify and differentiate actions.
 - Use descriptive terms (e.g., *"Critical Patch – May 2025 – Windows Devices"*) to ensure clarity and traceability.
6. **Install:** After verifying the configured information, click **Install** to install the software.

Related information

[Deploy Script \(on page 20\)](#)

[Update Windows Registry \(on page 25\)](#)

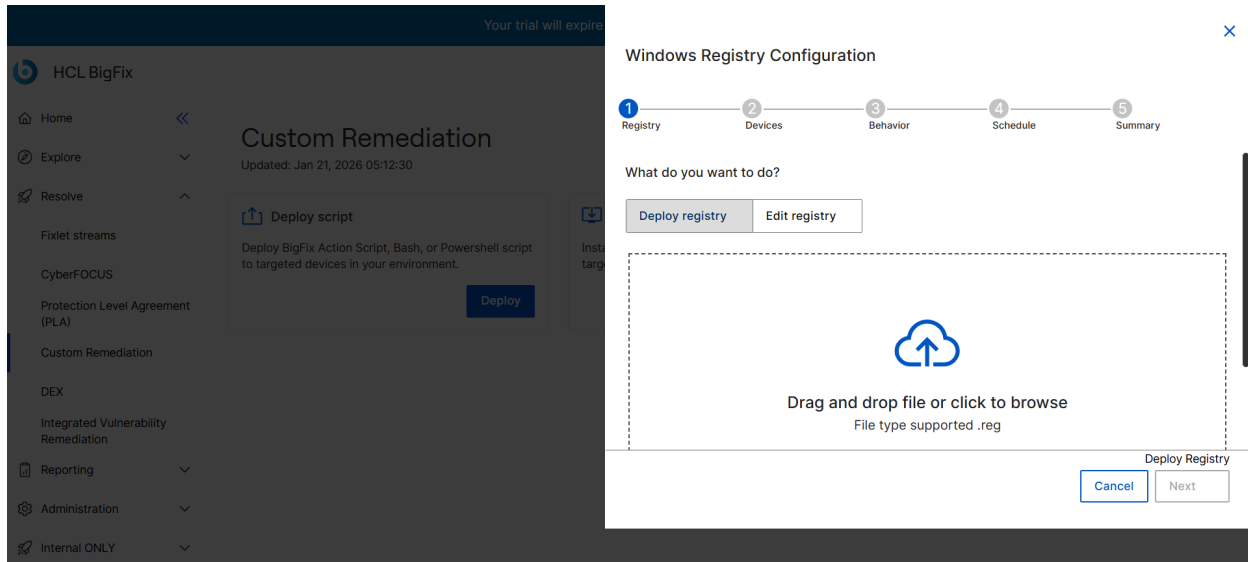
Update Windows Registry

Upload and deploy Windows Registry (.reg) files to one or more devices using Custom Remediation. Ideal for applying system policies, security settings, or config changes at scale.

The **Upload Windows Registry File** feature lets IT admins apply registry changes to one or more Windows devices quickly and securely — without creating a Fixlet or waiting for official content updates.

- **Import a .reg file** directly into the Custom Remediation wizard.
- Automatically converts the registry file into a script that runs silently on targeted devices.
- Supports deploying to any number of Windows endpoints that meet targeting criteria.

To open the Windows Registry Configuration widget, from the **Custom Remediation** app, on the **Windows Registry Configuration** card, click **Update**.



1. Registry:

- You can **upload a .reg file** by:
 - Dragging and dropping the file into the upload area, or
 - Clicking **Browse Files** to select the file from your system.
- If you prefer to specify registry changes directly:
 - a. Enter Registry Key Path, specify the full path to the registry key you want to modify.
 Example:

HKEY_LOCAL_MACHINE\Software\YourCompany\Settings
 - b. Provide New Registry Key Data
 - **Data Name:** The name of the registry value to be created or modified.
 Example: **EnableFeatureX**
 - **Data Type:** Choose from supported types:
 - **Data Value:** Enter the value associated with the key.
 Example: **1** (for enabling a feature)
 - c. Click **Add Registry Key**. This adds the key-value pair to the list of changes to be deployed.
 - d. Add Multiple Registry Keys (Optional)
 - You can repeat Step 2 to add **multiple registry entries** under different or the same paths.
 - All keys will be written in a single execution sequence on the endpoint.

Example:

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. **Devices:** [Filter target devices \(on page 49\)](#) and click **Next**.
3. **Behavior:** The configured options are processed **sequentially from top to bottom**, giving you precise control over how deployments are delivered, how users are informed, and how failures are handled.

- a. **Start downloading immediately**

When enabled, targeted endpoints begin downloading the required payloads as soon as the remediation action is deployed.

- b. **Before running message**

When enabled, the configured message is displayed to the end user before the action starts. This can be used to provide context, warnings, or request user confirmation.

- c. **While running message**

When enabled and a message is configured, during execution of the action, the notification message is shown to indicate that the remediation is currently in progress. This helps maintain user awareness and reduce support inquiries.

- d. **Reboot/restart devices on completion of deployment**

After the remediation completes, targeted devices are automatically rebooted if required by the fixlet. This step ensures that changes are properly applied and system integrity is maintained.

- e. **On failure: retry x time and wait x hour between attempts**

If the action fails, you can configure:

- **Number of retries:** how many times the system should reattempt the action.
- **Wait time between retries:** the number of hours to wait between each retry.

This setting increases the success rate by accounting for temporary issues like device disconnection or network latency.

Click **Next** to proceed.

4. **Sequence:** The configured options are processed **sequentially from top to bottom**, giving you precise control over how deployments are delivered, how users are informed, and how failures are handled.

- a. **Start downloading immediately**

When enabled, targeted endpoints begin downloading the required payloads as soon as the remediation action is deployed.

- b. **Before running message**

When enabled, the configured message is displayed to the end user before the action starts. This can be used to provide context, warnings, or request user confirmation.

- c. **While running message**

When enabled and a message is configured, during execution of the action, the notification message is shown to indicate that the remediation is currently in progress. This helps maintain user awareness and reduce support inquiries.

- d. **Reboot/restart devices on completion of deployment**

After the remediation completes, targeted devices are automatically rebooted if required by the fixlet. This step ensures that changes are properly applied and system integrity is maintained.

- e. **On failure: retry x time and wait x hour between attempts**

If the action fails, you can configure:

- **Number of retries:** how many times the system should reattempt the action.
- **Wait time between retries:** the number of hours to wait between each retry.

This setting increases the success rate by accounting for temporary issues like device disconnection or network latency.

f. **Reapply whenever it becomes relevant again**

Click **Next** to proceed.

5. **Schedule:** Select a time range for the scheduled activity. This setting defines the window during which the schedule remains in effect. After configuring the schedule, click **Next** to proceed.

Field Label	Description
Start Date	Select the calendar date when the remediation deployment should begin.
Start Time	Select the time (hh:mm) at which the remediation should start.
Time Zone (Start)	Choose the time zone to apply for the start time: - Client: Uses each endpoint's local time. - UTC: Uses Coordinated Universal Time.
End Date	Select the calendar date by which the remediation deployment should be completed.
End Time	Select the time (hh:mm) at which the deployment window ends.
Run During Agent's Configured Maintenance Window	Enable this option to restrict the deployment to devices that have a maintenance window configured. The remediation will only run within those windows. ! Note: Devices without a maintenance window will be excluded from the deployment.
Run on All Devices, Regardless of Their Configured Maintenance Window	Enable this option to override maintenance window restrictions. The remediation will run on all targeted devices, whether or not they have a maintenance window configured.
Custom constraints	Enable this option to apply custom constraints, allowing the selection of a specific date, time, and day of the week.
Reset	Click to clear all current scheduling fields and revert the section to its default state. Use this to start over if needed.

6. **Summary:** The Summary section provides a consolidated view of all the configuration options selected in the remediation flow. It acts as the final checkpoint before deployment, allowing you to review and confirm your settings.

Action name:

- **Enter a unique and meaningful name** that clearly describes the purpose of the action.
- This name will appear in action history, logs, and dashboards, helping you and your team quickly identify and differentiate actions.
- Use descriptive terms (e.g., "*Critical Patch – May 2025 – Windows Devices*") to ensure clarity and traceability.

7. **Deploy:** After verifying the configured information, click **Deploy** to deploy the action.

Related information

[Deploy Script \(on page 20\)](#)

[Install Software \(on page 23\)](#)

CyberFOCUS

CyberFOCUS is a threat intelligence and remediation feature within BigFix SaaS Remediate that provides visibility into CISA KEV (Known Exploited Vulnerabilities) and MITRE ATT&CK reports. It enables users to assess their security posture and take proactive remediation actions based on real-world threat intelligence.

CyberFOCUS enhances cybersecurity visibility by integrating CISA KEV and MITRE ATT&CK intelligence into 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.

Vulnerability management

- NVD (National Vulnerability Database) and MITRE ATT&CK maintain comprehensive databases of global vulnerabilities and attack techniques.
- BigFix SaaS Remediate pulls vulnerabilities from both NVD and MITRE ATT&CK, integrating them into its system for comprehensive threat intelligence.
- 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 SaaS includes two key reports:

- [CISA KEV Report \(on page 30\)](#) – A collection of known exploited vulnerabilities. Displays known exploited vulnerabilities based on NVD data. CISA Known Exploited Vulnerabilities (KEV) web report utilizes the data provided by the Cybersecurity & Infrastructure Security Agency (CISA) KEV Catalog 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 \(on page 33\)](#) – Follows a similar structure but is based on the MITRE ATT&CK framework. Another framework for tracking vulnerabilities. MITRE Advanced Persistent Threat Groups (MITRE APTs) web report obtains data published through the MITRE ATT&CK® Framework, analyses and compares it with the patch levels of the devices in your BigFix environment, and visualizes the analysis as a bar chart to help you take informed decision to mitigate the security threat.



Note:

- Both CISA KEV and MITRE reports are visualized using tables and charts.
- By default, the dashboard displays the CISA KEV report.

Toolbar Icons



- **Export**: Exports the current view data or charts.
 - Use this option to download tabular data as CSV or Excel, or export visualizations as JPEG, PNG, or PDF formats.
 - For detailed steps, see [Common Functionality \(on page 10\)](#) > Export Data and Charts.



- **Prescriptive Guidance**: Opens the Prescriptive Guidance panel, which identifies configuration gaps or missing actions and provides direct remediation options.

- From this panel, you can review affected devices and select Remediate to take corrective action.
- For more information, see [Prescriptive Guidance \(on page 14\)](#).



- **Filter**: Filters the data displayed in the current view based on selected criteria.

- You can apply single or multiple conditions to narrow results using properties, operators, and values.
- For detailed steps, see [Common Functionality \(on page 10\)](#) > Filter Data.

Understanding Fixlets and Exposures

- The system tracks affected devices and Fixlets required for remediation.
- Exposure represents the mapping between relevant Fixlets and affected devices.
- For example, if a device requires three Fixlets, its exposure count is 3; If two devices require three Fixlets each, the exposure count is 6. The total exposure is calculated based on relevant Fixlets and affected devices.

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.

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:

- Patching: [Remediate \(on page 35\)](#) vulnerable software and devices by deploying relevant Fixlets.

For detailed, step-by-step instructions on executing this action, see [Remediate \(on page 35\)](#)

Related information

[Prescriptive Guidance \(on page 14\)](#)

[CyberFOCUS remediation flow \(on page 35\)](#)

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

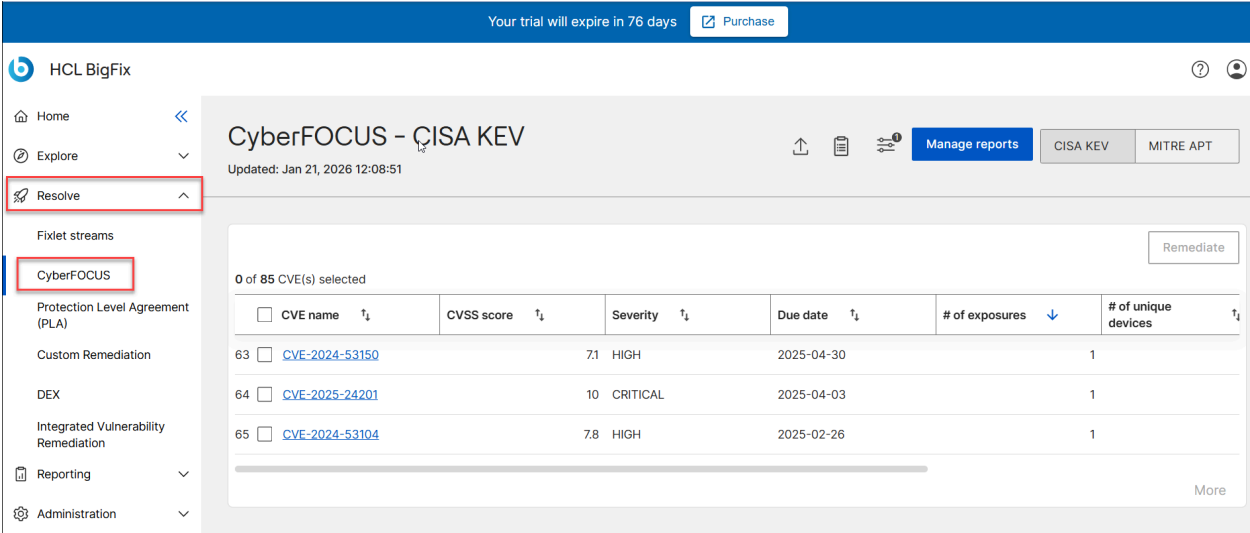
- Identifies vulnerabilities with confirmed exploitation in real-world attacks.
- Provides mandated patching deadlines (for U.S. federal agencies).
- Helps organizations prioritize security patches effectively.

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 view the CISA KEV report, from **BigFix SaaS** , expand **Resolve** and select **CyberFOCUS**. By default, the dashboard displays the CISA KEV report.



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).
 - **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 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.
- **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 view specific information, such as CVE details, Fixlet details, and other relevant content.

CISA KEV Table Representation

The table provides a structured list of vulnerabilities with key details:

Column Name	Description
CVE ID	The unique identifier for the vulnerability, sourced from NVD.
CVSS Score	The severity rating from NVD, based on the Common Vulnerability Scoring System (CVSS).
Severity	The risk level assigned to vulnerability (Critical, High, Medium, Low).
Due Date	The deadline by which the vulnerability should be remediated, as per CISA.
Exposure Count	The total number of Fixlet-device mappings required to remediate the vulnerability.
Unique Devices Affected	The number of unique devices in your environment affected by the CVE.
Applicable Fixlets	Fixlets that can be used to patch the affected devices.
Relevant Fixlets	The subset of Fixlets that still need to be applied (after some patches have been deployed).

CISA KEV Table Interactions

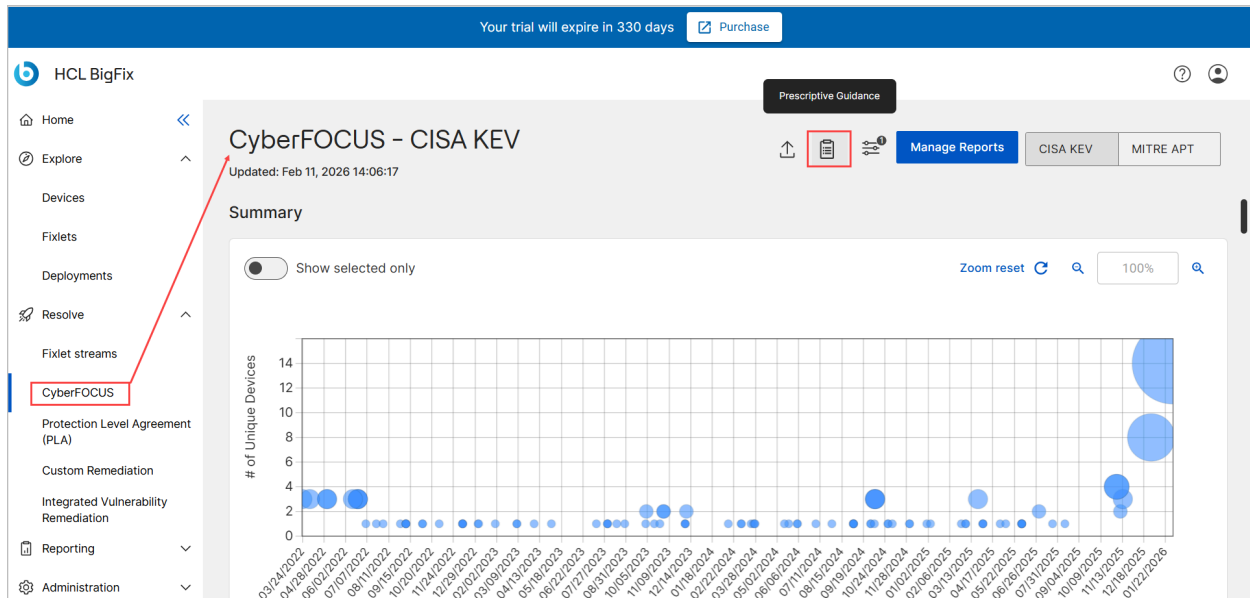
- **Click for More Information:** Click on a CVE in the table to access in-depth details, including a description, applicable Fixlets, and affected devices. A direct link to the National Vulnerability Database (NVD) is available on the details page for further reference.
- **Sort Functionality:** Sort 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 \(on page 35\)](#).

Prescriptive Guidance for CISA KEV Scanner

[Prescriptive Guidance \(on page 14\)](#) 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 using:
 - **Site ID:** Example – **15785**
 - **Fixlet ID:** Example – **100**
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 \(on page 29\)](#)

[MITRE APT report \(on page 33\)](#)

[CyberFOCUS remediation flow \(on page 35\)](#)

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.

MITRE Advanced Persistent Threat Groups (MITRE APTs) web report obtains data published through the MITRE ATT&CK[®] Framework, analyses and compares it with the patch levels of the devices in your BigFix environment, and visualizes the analysis as a bar chart to help you take informed decision to mitigate the security threat.

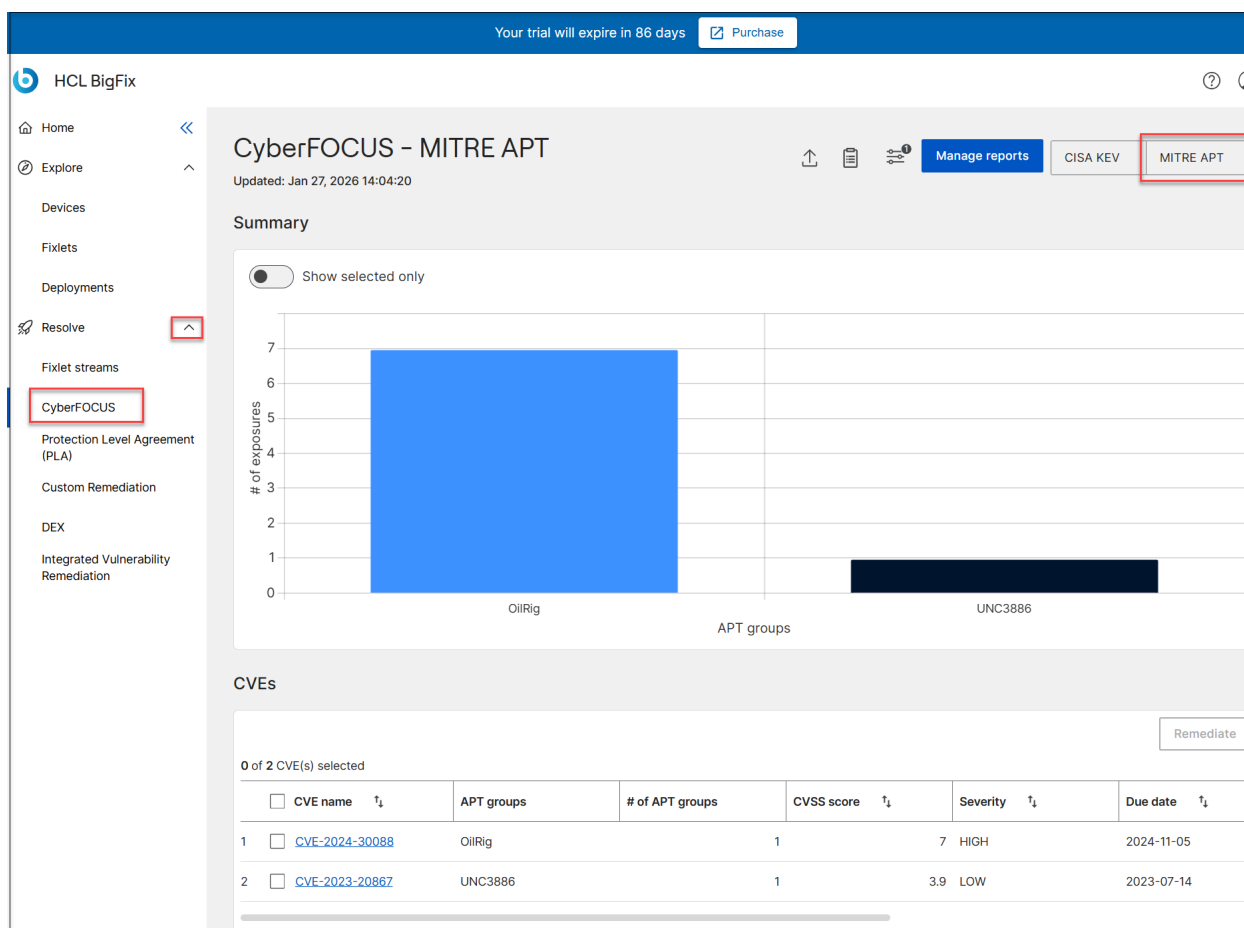
The **MITRE ATT&CK[®] Framework** documents real-world attack techniques used by Advanced Persistent Threat (APT) groups. For more details, visit [MITRE ATT&CK](#).

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's to the BigFix Patch content based on the CVEs.
- It highlights vulnerabilities linked to **known adversary techniques**.
- It helps security teams **understand attack vectors** and prepare defense strategies.

Accessing MITRE APT report

To view the CISA KEV report, from **BigFix SaaS** , expand **Resolve**, select **CyberFOCUS**, and click **MITRE APT**.



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 table provides a structured list of vulnerabilities with key details:

- 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 indicates APT group
- Y-axis indicates number of exposures

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.

MIRTE APT Table Representation

The table provides a structured list of vulnerabilities with key details:

Column Name	Description
CVE ID	Unique identifier for the vulnerability from the National Vulnerability Database (NVD).
CVE Name	Common name for the vulnerability.
APT Groups	List of APT groups known to exploit the vulnerability.
# of APT Groups	Number of APT groups associated with the CVE.
CVSS Score	Severity rating based on the Common Vulnerability Scoring System (CVSS).
Severity	Severity rating based on the impact categorized as High, Medium, or Low.
Due Date	The deadline by which the vulnerability should be remediated.
# of exposures	The total number of Fixlet-device mappings required to remediate the vulnerability.
# of applicable Fixlets	Total number of Fixlets that can be used to patch the affected devices.
# 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 access in-depth details, including a description, applicable Fixlets, and affected devices. A direct link to the National Vulnerability Database (NVD) is available on the details page for further reference.
- **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 \(on page 35\)](#).

Related information

[CISA KEV Report \(on page 30\)](#)

[CyberFOCUS \(on page 29\)](#)

[CyberFOCUS remediation flow \(on page 35\)](#)

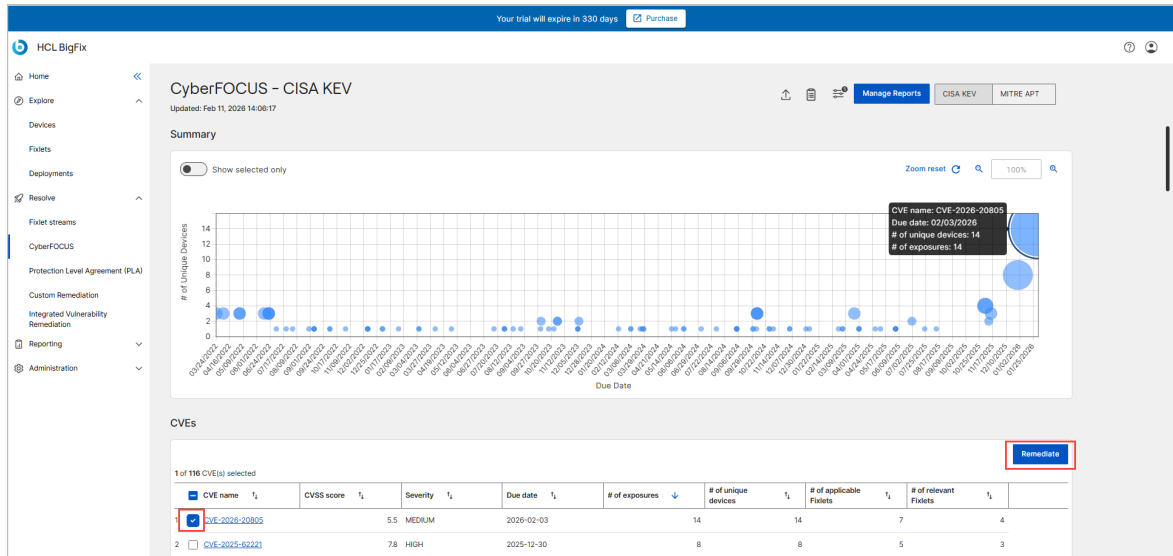
CyberFOCUS remediation flow

The **CyberFOCUS Remediation Flow** streamlines the process of addressing the most urgent security vulnerabilities (CVEs) quickly and efficiently.

From the CyberFOCUS dashboard, to initiate a remediation, complete the following steps.

1. Accessing the Remediate widget from CyberFOCUS dashboard

- From either the CISA KEV or MITRE APT tabs available in CyberFOCUS, select one or more CVEs. You can select CVEs either from the table or from the charts themselves. Once a CVE is selected the **Remediate** button becomes active.



- Click the **Remediate** button to open the Remediate widget.

The screenshot shows the Remediate widget with a progress bar indicating the current step is 'Fixlets'. The 'Filter the Fixlets below' section is active, showing a single condition filter: 'CVE' in 'in' with the value 'CVE-2025-24990'. The 'Apply' button is visible. Below the filter section, there is a 'Select the Fixlets to remediate' section with a 'Next' button.

2. Configure the remediation

To configure a remediation from CyberFOCUS, complete the following steps:

- Fixlets:** The selected CVEs are auto filtered to fetch relevant Fixlets. You can modify the filter further as needed. For information on how to modify the filter, refer to [Setting up remediation flow \(on page 49\)](#).
- Actions:** You can review and update the actions for the set of Fixlets with default action and without default action.
- Devices:** Relevant devices are automatically filtered. You can modify the filtering using a query and enable or disable dynamic targeting. Alternatively, you can select devices from the group or list to adjust the filtering.

Remediate

Fixlets Actions **Devices** Behavior Schedule Summary

Filter the devices below

Filter By **Query** Device group Device list

☐ Dynamic targeting device ☒ Single condition

☒ Single condition ☐ Multiple condition (OR)

☒ Single condition ☐ Multiple condition (AND)

Property Operator

Property Operator

Apply

Deploy 1 Fixlets to 1 applicable Device(s)

Back Cancel Next

4. **Behavior:** You can configure deployment options for the remediation from here.

Remediate

Fixlets Actions Devices **Behavior** Schedule Summary

Order of Events (from top to bottom)

☐ Start downloading immediately

☐ Before running message

☐ While running message

☐ Reboot/Restart devices on completion of deployment

☐ On failure, retry 1 time, and wait 1 hour between attempts

☐ Reapply whenever it becomes relevant again

Deploy 1 Fixlets to 1 applicable Device(s)

Back Cancel Next

- **Start downloading immediately:** Select this option to instruct the targeted BigFix Agents to download deployment files immediately regardless of the start time schedule. You can save time when working with large files or a tight maintenance window by completing this part of the job first.
- **Before running message:** To display a message on target computers before the deployment runs, select this option and enter your message.
- **While running message:** Select this option to display the message on targeted computers while the deployment is running.
- **Reboot/Restart devices on completion of deployment:** Select this option to restart the computer after the action is run.
- **On failure, retry:** Select this option to configure when to retry deployment on failure.
- **Reapply:** Select this option to reapply the action. By default, whenever it becomes relevant again, you can reapply with 1-hour wait between attempts, up to 3 times. You can configure the wait time and the number of attempts as needed.

5. **Schedule:** Configure start date and end date.
6. **Summary:** Shows all the configured remediation flow settings. Provide a unique **Deployment Name**.

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

Result: A remediation deployment is created.

What to do next: Go to [Deployment Manager \(on page 38\)](#) and you can see the remediate deployment that was created. It also displays all the configured deployment settings. It shows the devices on which the deployment is being done, and the Fixlets that are deployed.

Related information

[CyberFOCUS \(on page 29\)](#)
[CISA KEV Report \(on page 30\)](#)
[MITRE APT report \(on page 33\)](#)

Deployment Manager

The Deployment Manager in BigFix streamlines the process of executing actions on devices within a deployment. It allows users to initiate and monitor deployments, which can range in complexity from quick tasks completed in minutes to more involved processes that may take days to finish on all targeted devices.

Your trial will expire in 86 days

Purchase

HCL BigFix

Home

Explore

Devices

Fixlets

Deployments

Resolve

Fixlet streams

CyberFOCUS

Protection Level Agreement (PLA)

Custom Remediation

DEX

Integrated Vulnerability Remediation

Deployment Manager

Updated: Jan 27, 2026 16:19:33

0 of 307 Deployments selected

Delete

Stop

	Name	State	Issued	ID	Start date	End date
1	lk	Expired	1 week ago	2778	[null]	22 Jan 2026 at C
2	vanji_auto	Expired	1 week ago	2770	[null]	21 Jan 2026 at 1
3	a_cinzia_8_stress	Expired	1 week ago	2626	[null]	20 Jan 2026 at 1
4	auto1	Expired	1 week ago	2605	[null]	20 Jan 2026 at 1

More

BigFix allows users to perform actions on devices included in a BigFix deployment. These actions are called Deployments. The complexity of a deployment can vary significantly. Some deployments may complete in minutes, while others may take days to successfully run on all targeted devices.

The Deployment Manager application allows users to see, manage, and control active and completed deployments. To see active or expired Deployments, click **Deployment Manager**. This table view allows users to take basic actions on displayed deployments, including stopping and deleting the deployment.

Click the deployment name to drill down to the deployment details page which has extensive details about that deployment’s configuration and status.

BigFix to showcases critical information to help leaders to support their business. Each application features a row of key performance indicators (KPIs) at the top, providing a real-time snapshot of the deployment and its status. We designed these KPIs to help users optimize their BigFix experience.

The Deployment Manager app currently has the following KPIs:

- Count of all deployments
- Count of active deployments
- Count of fixlets associated with active and/or scheduled deployments
- Average number of fixlets per active or pending deployments

The Deployment Manager app displays all deployments associated with your organization — both active and expired — in a table.

The deployment data table includes filtering, detail drill down, and deleting deployments.

- Click the **Filter** icon to view the filter panel. Using the [filter tool \(on page 10\)](#) makes it possible to reduce the number of deployments displayed in the data table.
- The data table also supports the [sorting \(on page 10\)](#) of each column. To do so, move your cursor near the column header name and then click. This will sort the data table using the values in that column. Reverse sorting requires clicking again.
- A count of the total of deployments associated with your account.
- A count of the deployments that the user has selected in the data table. Selecting deployments in the data table is required for actions such as stopping or deleting deployments.
- The **Stop** button stops the selected active deployments.
- The **Delete** button deletes selected deployments from the data table so that they will no longer be displayed. Only Expired deployments may be deleted. To delete an Active deployment, it must first be stopped.
- You can [save the view \(on page 10\)](#) of the filtered and sorted data and access it back whenever necessary.



Note: The **Stop** and **Delete** buttons are disabled by default and become selectable only after at least one deployment is chosen in the data table. User permissions, as assigned by administrators, may restrict some users from stopping or deleting deployments.

The data table provides a comprehensive view of all your deployments. For detailed information on specific deployments, such as relevance code, current status, and other fields, users can access the Deployment Details page. To do this, click on the Name field of the desired deployment.

Related information

[Protection Level Agreement \(PLA\) \(on page 89\)](#)

Deployment Details page

The Deployment Details page provides detailed information on a deployment, allowing for tracking of status, troubleshooting of failures, and performance monitoring. It includes widgets for Status, Composition, Configuration, Device, and Fixlets, each providing specific insights such as real-time statuses, device compositions, configuration details, device lists, and fixlet information.

The screenshot shows the HCL BigFix Deployment Manager interface. At the top, a blue banner indicates 'Your trial will expire in 86 days' with a 'Purchase' button. The left sidebar contains navigation links: Home, Explore, Devices, Fixlets, Deployments, Resolve, Fixlet streams, CyberFOCUS, Protection Level Agreement (PLA), Custom Remediation, DEX, and Integrated Vulnerability Remediation. The main content area displays the deployment details for '2011 - Testing_Issue_BFNOW-9625_Disabling', updated on Jan 27, 2026 at 16:33:45. It includes tabs for Overview, Fixlets, and Devices. The Status section shows 'Deployments completed 100%' with a progress bar and an 'Expired' label. The Configuration section lists deployment settings: Issued on 06 Dec 2025 at 17:20:08, Start date not set, will begin immediately, Before Deployment Begins (Begin download after start, No retries on failure, One-time deployment), Messages (No message before running, No message while running), Fixlet sequence (As shown in fixlets), and After Deployment Ends (Restart: No). The Composition section shows a bar chart with a value of 1 for 'Action Status'.

The Deployment Detail page contains various pieces of information displayed in widgets.

Status

The Status widget displays real-time information about the statuses related to devices in the deployment. It includes the deployment progress and failure rate. Example statuses are pending restart, complete, and failed.

The screenshot shows the Status widget. It features a title 'Status' with a mouse cursor icon. Below the title, a white box displays 'Deployments completed 100%' with a progress bar consisting of 10 blue squares. Below the progress bar, it says '(1 of 1)'. To the right of the progress bar, there is a yellow button with the text 'Expired'.

Composition

Besides the high-level status of completed or failed, a device can have multiple statuses like pending restart, waiting to download, etc. The Composition widget displays a treemap of all statuses for devices in the deployment being viewed. This information is particularly helpful for troubleshooting.

Configuration

The Configuration widget summarizes how users set up the initial deployment. At a glance, it shows all customizable parameters such as start time, end time, and pre- and post-actions.

Configuration

 Issued on Apr 17, 2024 13:14:03

 Start date not set, will begin immediately.

Before Deployment Begins

 Begin download after start

 No retries on failure

 One-time deployment

Messages

☐ Before running message identified

☐ No while running message

Fixlet sequence

 As shown in fixlets

After Deployment Ends

 Restart: No

☒ End date not set, will continue running until stopped

Device

The Device tab displays a subset of all devices in the selected deployment. To see the full list of devices click **Show All**.

Devices: (3 of 3 shown)

No.	Name	Last seen	Computer ID	Result	Status	Completed
1	VINOYW10EDU1809	16 hours ago	6234322	-	Not Relevant	Yes
2	W2016-BOB2	5 weeks ago	1614089656	-	Not Relevant	Yes
3	CINZIAWINCLOUD3	8 weeks ago	553541953	-	Not Relevant	Yes

If there is only one device in the deployment, then the device properties are displayed in the widget.

Device

All Properties

Search property name or value

Name	Last seen	Computer ID	OS family
W2016-BOB2	5 weeks ago	1614089656	Windows
Operating system	Device type	IP address	MAC address
Win2016	Server	10. 5	00-5-09
DNS name			
W2 2			

Fixlets

The Fixlet tab lists a subset of all fixlets included in the selected deployment. To view the full list of Fixlets, click **Show All**.

Fixlets: (2 of 2 shown)

No.	Name	ID	Severity	Category
1	BES Client Setting: CPU Usage	1-168	<Unspecified>	BES Client Setting
2	BES Client Setting: Download Throttling	1-167	<Unspecified>	BES Client Setting

If there is only one fixlet in the deployment, then the fixlet properties are displayed in the widget.

Fixlet

All Properties

Search property name or value

Q

Name	ID	CVE(s)	Severity
Create file	12505-3	Unspecified	Important
Category	Release date	Source	Source ID
Security Update	Jun 28, 2024	Microsoft	KB328131
Download size	[null]		

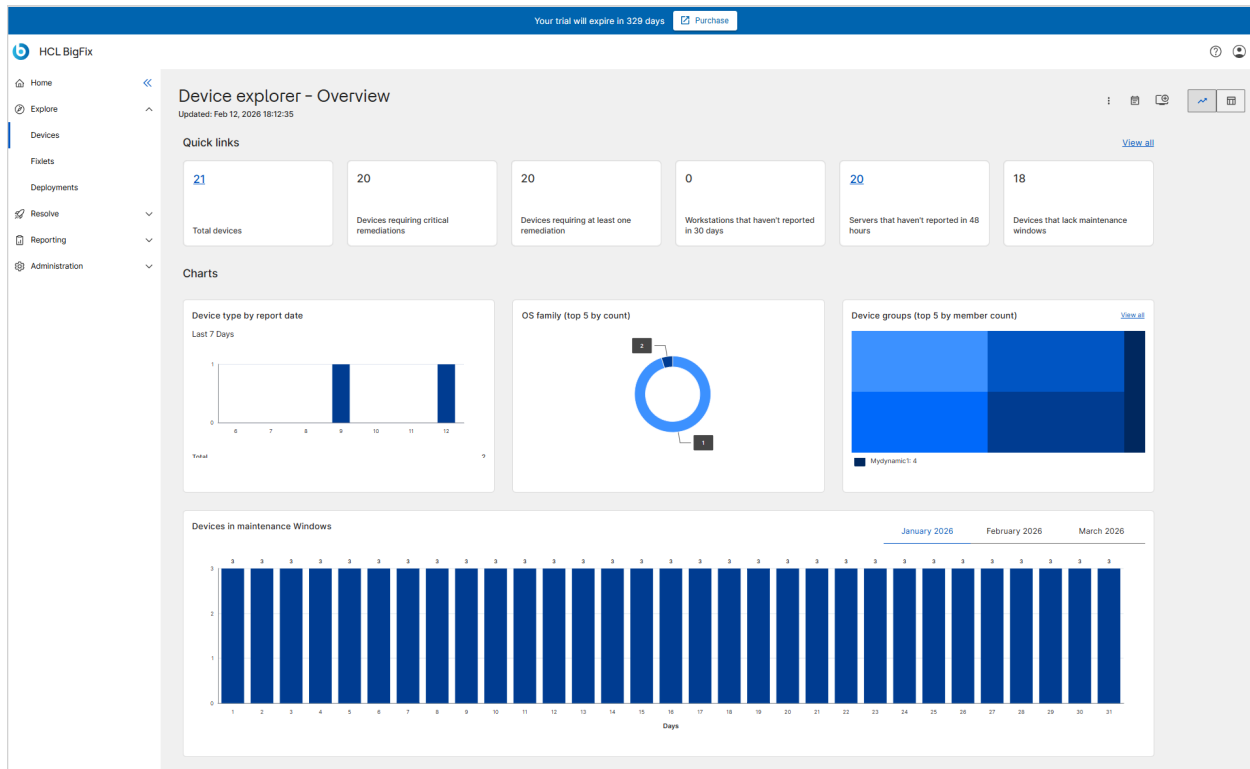
Device Explorer

Use the Device Explorer Dashboard in BigFix to explore all connected devices in table and chart formats. Filter, sort, add devices, perform remediation, schedule maintenance, and export reports—all from one unified view.

Device Explorer - Overview

The **Device Explorer Dashboard** is a unified application within BigFix SaaS Remediate that allows administrators to view, manage, and take actions on all devices connected to their account. Whether you're filtering for a subset of devices, exploring details of a specific device, or preparing for remediation or reporting, this dashboard provides an interactive, visual-first interface to handle it all.

 **Note:** Devices only appear in this dashboard if the **BigFix agent is installed** and reporting.



BigFix currently supports up to **50,000 linked devices per account**, with performance optimized for both large and small environments.

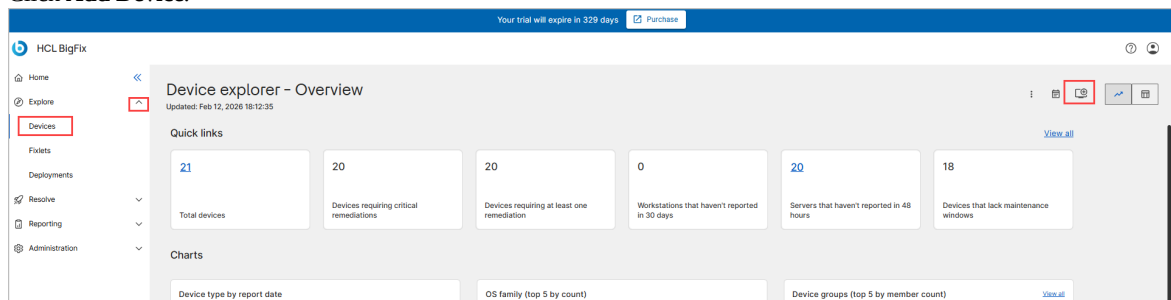
The Device Explorer app in BigFix allows to view and explore their linked devices in a table format, displaying important details like device name, last connection time, OS information, and device type. To simplify device exploration use filter or device search. Click on specific device to access more details.

The Device Explorer app displays all devices linked to your BigFix account. BigFix currently allows adding up to 50,000 devices.

Add Device

To add new devices

1. Click **Add Device**.



2. Use the dropdown to choose the target OS (Windows, macOS, Linux, etc.).
3. Download the corresponding agent installer.
4. Follow guided steps to install the agent on the target device.



Note: For the devices to appear in the dashboard, you need to install the BigFix agent and the device needs to check in.

Overview - Top-level charts

The dashboard provides quick access to high-level metrics through interactive chart widgets:

- **Top 5 by Device Type:** Displays the most common device types such as desktops, laptops, or servers.
- **Top 5 by OS Family:** Breaks down the device count by operating system family—e.g., Windows, macOS, Linux.
- **Top 5 by Tags:** Shows top organizational or functional tags applied to devices.
- **Devices in Maintenance Window:** Visualizes the number of devices currently in active maintenance windows.
- **Devices Requiring Critical Remediations:** Highlights devices missing security-critical patches or updates.
- **Devices Requiring At Least One Remediation:** Broader view of any device that needs updates or patches.



Note: Clickable count showing the full inventory. Clicking any section of these charts will automatically update the device table with the filtered list.

List - Device table

This is the main area for in-depth device exploration. The table supports sorting, filtering, and quick action on device records.

Displayed Columns

Displayed Columns Include:

- **Number:** Assigned by BigFix to indicate the order in which the device was added.
- **Device Name:** Local name of the device (sortable and searchable).
- **Last seen:** Indicates when the device last checked in with BigFix.
- **ID:** Unique identifier of the device.
- **OS family:** High-level OS classification, such as “Red Hat” or “macOS”.
- **Operating System:** The specific OS version (Example, Windows 10, Ubuntu 22.04).
- **Device Type:** Such as laptop, desktop, or server.
- **IP Address / MAC Address:** Captured during the device’s last connection.
- **DNS Name:** Helpful for network-based tracking.
- **Relay:** Shows the current relay server.
- **Relay Selection / Relay Installed:** Indicates if a relay is installed and if it was manually or automatically selected.
- **Distance to Relay:** Useful for understanding latency and proximity for patch distribution.
- **Maintenance Window Definition / In Maintenance Window / Next Maintenance Window:** Shows configuration and current/next window status.

💡 The table displays **100 devices without pagination**.

The app also showcases these devices in a table and enables in-depth exploration of each device.

The table includes various fields that help to view and investigate all devices associated with the account.

The table presents the following details:

- **Device Number** - Assigned by BigFix to show the order of device addition to the user’s account.
- **Device Name** - The local name of the device.
- **Date and Time Device Last Seen** - The last connection time of the device’s agent to the BigFix service.
- **Device ID** - A unique device identifier.
- **Device OS Family** - The operating system running on the device, for example, Mac OS or Red Hat Linux.
- **Operating System Installed on the Device** - The specific operating system version on the device.
- **Device Type** - Indicates if the device is a computer or server.
- **Device IP Address** - The IP address from the device's last connection to the BigFix service.



Note: When a device is removed from Device Explorer, it stops sending or receiving data via BigFix. To resume using BigFix on that device, reinstall the BigFix agent.

BigFix customers may have thousands of devices linked to their account. To use the filter in the Device Explorer app, click the **Filter** button at the top left of the device table. The filter panel will slide out from the right side of the screen. Various device properties, such as device name, operating system, and IP address, can be used to filter.

The Device Explorer app supports [filter \(on page 10\)](#), [sorting \(on page 10\)](#), and [saving views \(on page 10\)](#) to refine data and narrow down displayed results to only the most relevant items, save them, and access back quickly.

Click on a specific device to be redirected to the [Device Details page \(on page 47\)](#) for more information about the selected device.

Filtering and Search

- Click the **Filter** button to open the filter panel.
- The panel slides in from the right and supports filtering on:
 - Device Name
 - Operating System
 - IP Address
 - Device Type
 - Maintenance Status
 - And more

Filters help you **narrow down to only relevant devices**, and you can **save filtered views** for future use.

Remediate Devices

- Select one or more devices from the list.
- Click the **Remediate** button to launch patching or Fixlet deployment.

Devices not in a maintenance window or otherwise restricted will be eligible for action.

Set Maintenance Window

To set maintenance window:

1. Select devices and from the **Select action** menu, select **Set Maintenance Window**.
2. In the Set Maintenance Window widget, do the following:
 - a. Set the maintenance window frequency - Daily, Weekly, or Monthly.
 - b. Select time format, set time and duration
 - c. Click **Set maintenance window**
 - d. Define start time, end time, and recurrence.
 - e. Devices in this window will defer actions until outside the window.
 - f. This helps prevent disruption during critical business hours.

Related information

[Setting up remediation flow \(on page 48\)](#)

[Setting up device maintenance window \(on page 52\)](#)

[Protection Level Agreement \(PLA\) \(on page 89\)](#)

Device Details page

The Device Details page in BigFix provides in-depth information about enrolled devices, aiding in troubleshooting by displaying device attributes and location. Users can access this page by selecting a device from the Device Explorer table and view unique properties, activity feed, applicable fixlets, device properties, and tags.

The Device Details Page provides detailed information about a device enrolled in a BigFix account. This information is helpful for fixing problems on specific devices by displaying the device’s location and attributes.

When you click a **Device Name** from the **Device Explorer – List View**, the Device Details page opens. This page is divided into three sections: Overview, Relevant Fixlets, and Deployments. Each section presents different aspects of the selected device’s status and activity.

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Device explorer – List view

Updated: Feb 13, 2026 11:13:25

Charts 0 charts set

0 of 21 Devices selected

	Device Name	Last seen	ID	OS family	Operating Systems	Device type	IP addresses	Mac addresses
1	WIN11	4 minutes ago	548417685	Windows	Windows 11 Professional	Server	192.168.1.106	4e-b2-ed-f4-f5-4c
2	DESKTOP-692UFC6	4 days ago	550381058	Windows	Windows 10 Pro N	Server	10.134.133.85	00-50-56-a8-9f-c3
3	nashu	2 weeks ago	1074585973	macOS	macOS Monterey	Server	172.16.75.130	00-0c-29-1f-04-bb
4	VINQYWIOPRO1803	2 weeks ago	1075282637	Windows	Windows 10 Pro	Server	10.190.70.49	00-50-56-a8-2f-27
5	LUNAFREYA	2 weeks ago	12310227	Windows	Windows 10 Pro	Server	10.134.146.216, 10.134.156.10	00-50-56-a8-2b-8e, a8-9f-47
6	AYMERIC	2 weeks ago	1623982284	Windows	Windows Server 2016 Datacenter	Server	10.134.156.14	00-50-56-a8-4d-eb
7	CINZIA-WIN10-4	2 weeks ago	1622964558	Windows	Windows 10 Enterprise	Server	10.134.135.128	00-50-56-a8-a1-88

Overview Tab

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Device explorer > WIN11

WIN11

OverviewRelevant FixletsDeployments

Maintenance window

Determine the best time for this device to undergo remediation, as this will minimize disruption and streamline the automation of the remediation process.

Set maintenance window

Groups of which this device is a member

Static groups 23-01-2026 static... X

Dynamic groups DeviceGroupTestin...DynamicDevicePentestDynamicGro...WindowsGroupTesti...

Core properties

Device name	Last seen	ID	OS family	Operating System	Device type
WIN11	9 minutes ago	548417685	Windows	Windows 11 Professional	Server
IP addresses	Mac addresses	DNS name	Active Directory Path	Type	Agent version
192.168.1.106	4e-b2-ed-f4-f5-4c	Win11.d.domain.home	CN=WIN11,CN=Computers,DC=d,DC=domain,DC=home	Native	11.0.5.204
BIOS	CPU	Computer Type	Free Space on System Drive	RAM	Relay
02/15/2024	3400 MHz Common KVM processor	Virtual	18567 MB of 60716 MB	8160 MB	bigfix-relay-top-0.sbx0010.play.hclsofy.dev:52311
Subnet address					
192.168.1.0					

The **Overview** tab summarizes key information about the selected device. It contains the following panels:

- **Maintenance window** – Displays the configured maintenance schedule for the device.
You can click **Edit** to modify the maintenance window parameters.
- **Groups of which this device is a member** – Lists all static and dynamic groups that include this device.

You can **View all groups** or **Add to static group** directly from this section.

- **Relay installed** – Shows whether the BigFix relay is installed on the device, the relay name, its parent relay, and reporting devices.

If the relay is installed, the Service Status and Uninstall Relay options appear.

- **Core properties** – The Core Properties panel displays key system information collected from the BigFix to help identify and assess device health. This information provides a quick overview of the device’s configuration, performance, and connectivity within the BigFix environment.

Relevant Fixlets

The **Relevant Fixlets** tab lists all Fixlets that apply to the selected device. It provides visibility into pending actions, patches, or configuration changes that the device qualifies for based on its current state. You can use this view to monitor outstanding compliance issues and plan remediation actions.

Your trial will expire in 328 days

Purchase

HCL BigFix

Device Explorer > WIN11

WIN11

OverviewRelevant FixletsDeployments

Name	ID	Relevant Devices	CVE(s)	Severity	Category	Release Date	Source
Google Chrome 145.0.7632.46 Available	5095.14011754		1 Unspecified	Unspecified	Update	2026-02-10	Google
Update: Microsoft Visual Studio Code x64 v1.109.2 - Windows (x64)	15658.5802501		1 [empty]	[empty]	Update	2026-02-10	Microsoft
Mozilla Firefox (x64) 147.0.3 Available	5095.6082248		1 Unspecified	Unspecified	Update	2026-02-04	Mozilla
Mozilla Firefox (x64) 147.0.2 Available	5095.6082246		1 CVE-2026-24868; CVE-2026-24869	High	Security Update	2026-01-27	Mozilla
Notepad++ (x64) 8.9.1 Available	5095.4001340		1 Unspecified	Unspecified	Update	2026-01-26	Notepad++
Update: Microsoft Visual C++ 2017-2026 Redistributable (x64) v14.50.30719.0 - Windows (x64)	15658.5802201		1 [empty]	[empty]	Update	2025-11-23	Microsoft
Microsoft Windows Privilege Escalation Vulnerability - Windows 11	15785.39800		1 CVE-2021-43226	None	Operating System	2025-10-06	HCL BigFix KEV Content Pack

You can scroll the list to locate a specific Fixlet and take relevant actions such as viewing details.

Deployments

The Deployments tab displays details of actions or patches that have been deployed to the selected device. It helps track the execution and outcome of tasks initiated from the BigFix environment. This information helps you verify that targeted actions are applied successfully and troubleshoot any failed deployments.

Your trial will expire in 328 days

Purchase

HCL BigFix

Device Explorer > WIN11

WIN11

OverviewRelevant FixletsDeployments

Name	State	Issued	ID	Start date	End date	Issuer
check1202	Active	20 hours ago	953	[null]	Feb 15, 2026 at 02:32 (Client)	rcpentest+3@yopmail.com
Uninstall Relay on device WIN11	Active	1 day ago	947	[null]	[null]	rcpentest+3@yopmail.com
Uninstall Relay on device WIN11	Active	1 day ago	945	[null]	[null]	rcpentest+3@yopmail.com
ff 147.0.1 walker	Expired	3 weeks ago	823	[null]	Jan 24, 2026 at 00:23 (Client)	rcpentest+3@yopmail.com
Firefox update - walker	Expired	3 weeks ago	821	[null]	Jan 24, 2026 at 00:17 (Client)	rcpentest+3@yopmail.com
test action with dynamic download	Expired	3 weeks ago	813	[null]	Jan 20, 2026 at 00:08 (Client)	[null]

More

Setting up remediation flow

The remediation process in BigFix SaaS 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.

1. Accessing the Remediate widget

1. Logging in

Log in to BigFix SaaS using your Admin credentials.

2. Go to the Device Explorer Section

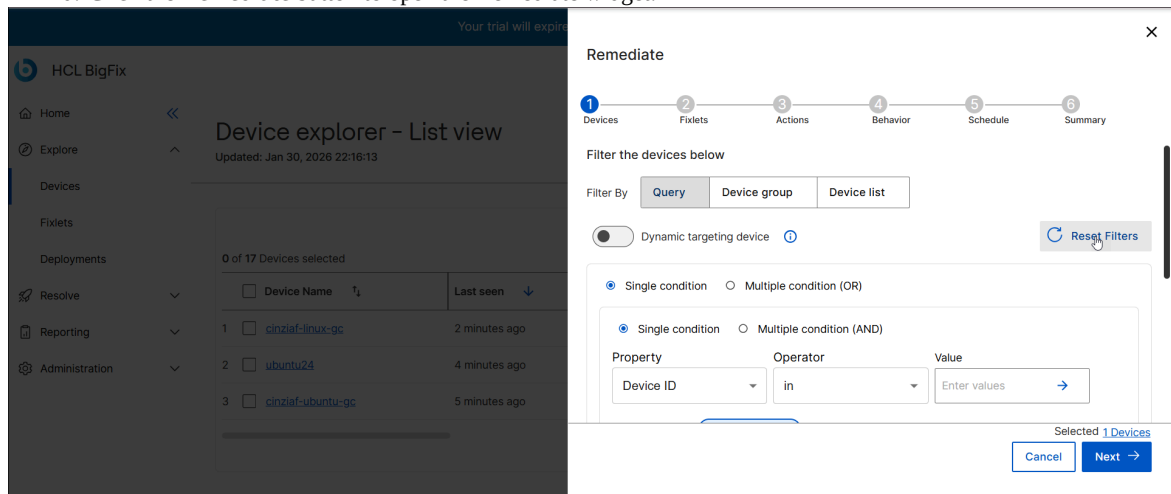
a. In the BigFix SaaS application, from the left pane expand **Explore** and select **Devices**.



b. Click the **List** button 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.



2. 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 list displayed.

a. Filter Devices

i. Filter by query:

- **Dynamic or static targeting device:** Toggle the option to select static or dynamic targeting devices.
 - **Static:** This is the default option. Applies the deployment to devices that match the defined filters *at the time of deployment creation*.
 - This list remains unchanged for the duration of the deployment.
 - Devices that match the filter *after* deployment creation will not be included.
 - Devices that stop matching the filter will still receive the deployment.
 - Best for predictable targeting where the scope should not change.
 - **Dynamic:**

- Defines matching criteria that is continuously evaluated for the entire duration of the deployment.
- Devices that match the filter at any time while the deployment is active will automatically be included.
- Ideal for ongoing remediation where new or reclassified devices need to be captured.

▪ **Single condition:** Enables you to define one condition.

▪ **Multiple condition (OR):** The device group that meets at least one condition will qualify for subscription.

- **Add Group:** Creates a **nested group** of conditions. Useful for combining AND/OR logic together.

▪ Example:

▪ Match any:

▪ Group 1 (Match all):

- OS = Windows
- Device ID contains "abc"

▪ Group 2 (Match all):

- OS = macOS
- Device ID contains "xyz"

Matches devices that are either **Windows with a Device ID containing "abc"** or **macOS with a Device ID containing "xyz"**.

▪ **Multiple condition (AND):** Filters devices that meet every condition specified based on the following parameters.

- **Attribute:** Device attributes like OS, RAM, software version.
- **Condition:** Criteria such as equals, greater than, contains.
- **Value:** The specific value for the condition. Example: To subscribe all Windows devices, set the attribute to "OS", the condition to "equals", and the value to "Windows".
- **Add Condition:** You can **Add** multiple conditions to ensure that they reflect the criteria relevant to your deployment needs. For example, you can add conditions based on geography, software version, or device type. Example:

▪ Condition 1: Operating System equals Windows

▪ Condition 2: Device ID contains 1234

Only devices that are **Windows** and with device ID that contains 1234 will match.

▪ **Filter by Device List:** Alternatively, you can also select devices from **Filter by device list** to select the target devices.

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

a. Click the **Attribute** dropdown to choose an attribute. For each attribute, specify a condition and add a value. You can define multiple conditions.

- **CVE:** Add relevant CVEs by typing them and click **Add**.



Note:



- To enter multiple CVE entries at once, you can copy paste a list of CVEs separated by comma, semicolon or a space. For example: CVE-123-1234,CVE-123-1256, CVE-123-1278
- View All button is displayed when there are more than eight CVE values. Click the **View All** button to view the list in detail, review, search, or remove a specific CVE.

- **Category:** Select categories from the list of categories dynamically displayed based on your system's database and click **Add**. This displays all the available categories with the ones that you have selected in blue. You can also modify your selection from here.
- **Name:** Select the "contains" or "not contains" condition and for the value, enter your string, and click **Add**. This displays all the strings that you have entered. You can also modify your selection from here, inserting or deleting values.
- **Severity:** Select the "in" or "not in" condition; for the value, choose the level of severity for the Fixlet. Modify selection by adding or removing as required.
- **Source:** Select the "in" or "not in" condition; for the value, select one or more vendors from the available option, and click **Add**. This displays all the available options for vendors with the ones that you have selected in blue. You can also modify your selection from here.



Note:

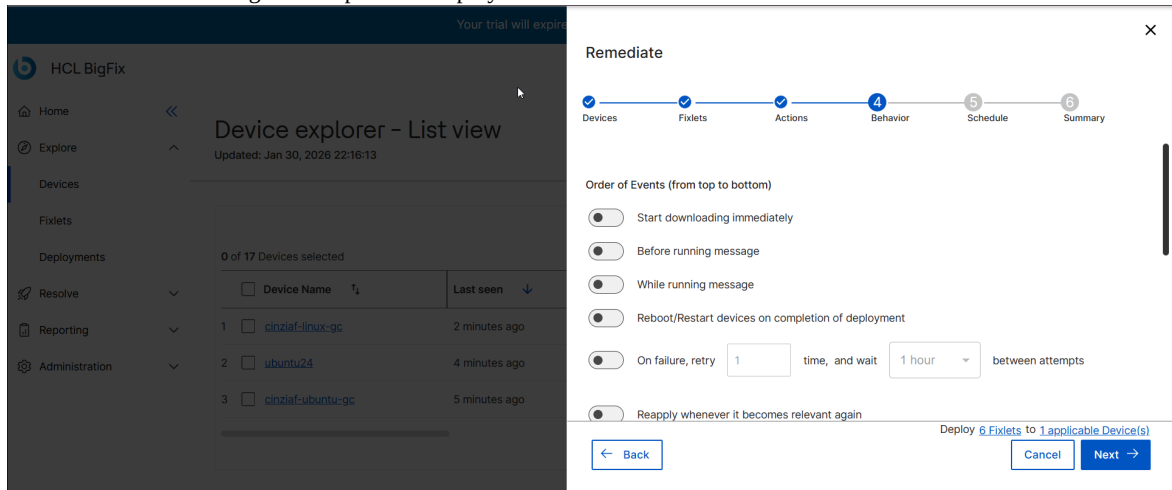


- To remove all entries in a section, click .
- The **Attribute** dropdown dynamically displays the attributes available to you.
- The **Value** text box dynamically fetches data from your database for you to select.

b. Once the conditions are defined, click **Next** to proceed.

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

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



You can control the sequence by selecting which events to run. The system follows the list from top to bottom, running only the selected ones.

- **Start downloading immediately:** Select this option to download deployment files immediately regardless of the start time schedule. Pre-cache deployment-related files, transferring them from a vendor's server to a BigFix server before deployment. You can save time when working with large files or a tight maintenance window by completing this part of the job first.
- **Before running message:** To display a message on target computers before the deployment runs, select this option and enter your message.

- **While running message:** Select this option to display the message on targeted computers while the deployment is running.
- **Reboot/Restart devices on completion of deployment:** Select this option to restart the computer after the action is run.
- **On failure, retry:** Select this option to configure when to retry deployment on failure.
- **Reapply:** Select this option to reapply the action. By default, whenever it becomes relevant again, you can reapply with 1-hour wait between attempts, up to 3 times. You can configure the wait time and the number of attempts as needed.

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

Run during agent's configured maintenance window: Select this option, if you want to deploy the remediation during the set [maintenance window \(on page 52\)](#).

6. **Summary:** Shows all the configured remediation flow settings. Provide a unique **Deployment Name**.

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

Result: The remediation flow is created and saved.

What to do next: Go to [Deployment Manager \(on page 38\)](#) 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.

Setting up device maintenance window

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. Logging in

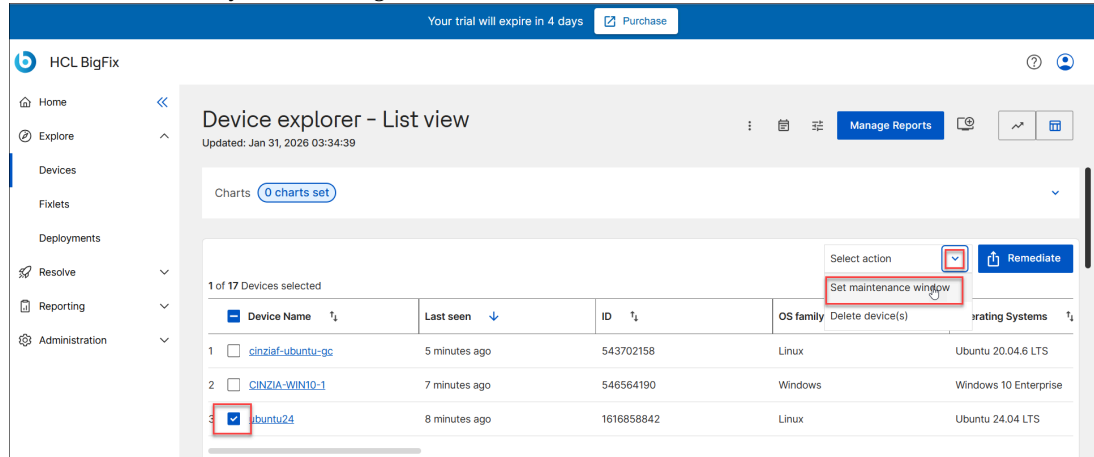
Log in to BigFix SaaS using your Admin credentials.

2. Go to the Device Explorer Section

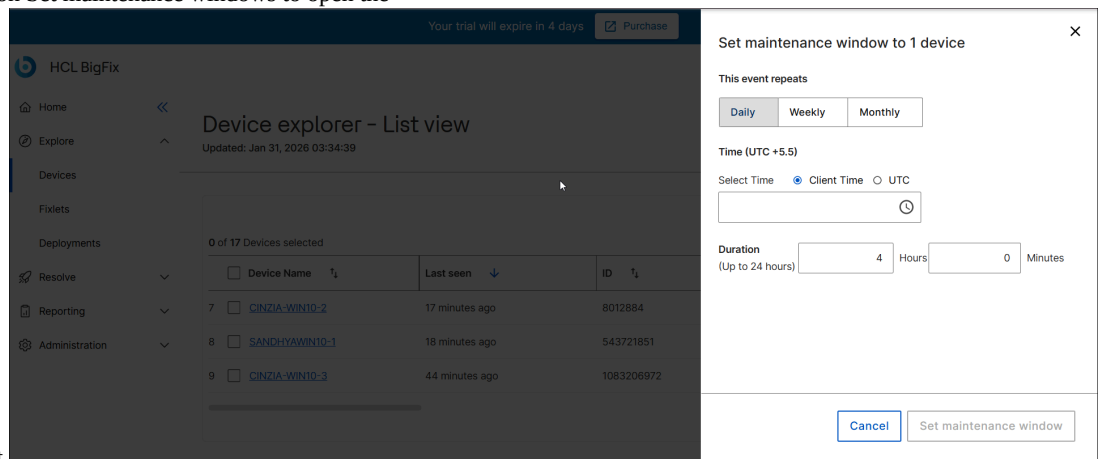
- a. In the BigFix SaaS application, from the left pane expand **Explore** and select **Device**.



- b. Click the **List** button to view the devices in list view.
c. Select the devices that you want to target, the **Set maintenance windows** button becomes active.



- d. Click on Set maintenance windows to open the



widget.

Setting up maintenance window

1. **Define a Maintenance Window:** Choose frequency (daily, weekly, or monthly) and configure time, duration, and interval as necessary.



Tip: Click  to set time.

2. Click **Set Maintenance Window**. The maintenance window is successfully created.
3. **Execution Handling:**
 - Updates and remediations occur within the scheduled window.
 - If a failure occurs, it retries in the next available window.
4. **Deployment Integration:**

- While deploying [Fixlet Streams \(on page 79\)](#), select "**Run during agent's configured maintenance window**".
- Verify execution status within the [Deployment Manager \(on page 38\)](#).

5. **Monitor and Modify as Needed:** Adjust schedules based on system needs.



Note: Maintenance Windows take effect only after the targeted endpoints receive and run the deployment containing the Maintenance Window configuration. Until the endpoint processes the change and reports back, the Maintenance Window will not be enforced. This may take several hours depending on the endpoint reporting cycle.

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**.

The screenshot shows the HCL BigFix console interface. At the top, a blue banner indicates "Your trial will expire in 4 days" and a "Purchase" button. The left sidebar contains navigation links: Home, Explore, Devices, Fixlets, Deployments, Resolve, Reporting, and Administration. The main content area is titled "AYMERIC" and shows the "Device explorer" path. The "Maintenance window" section is highlighted with a red box, containing a "Set maintenance window" button. Below this, the "Core properties" section displays a table of system details for the device AYMERIC.

Device name	Last seen	ID	OS family	Operating System	Device type
AYMERIC	20 hours ago	1080826623	Windows	Windows Server 2016 Datacenter	Server
IP addresses	Mac addresses	DNS name	Active Directory Path	Type	Agent version
10.134.156.14	00-50-56-a8-4d-eb	aymeric	<none>	Native	11.0.5.204
BIOS	CPU	Computer Type	Free Space on System Drive	RAM	Relay
11/12/2020	2600 MHz Xeon Gold 6142	Virtual	50572 MB of 101897 MB	8192 MB	bigfix-relay-top-0.sbx0224.play.hclsof y.dev:52311
Subnet address					
10.134.156.0					

Integrations

- [Fixlet Streams \(on page 79\)](#): Configure Fixlet deployments to run only within maintenance windows.
- [CyberFOCUS \(on page 29\)](#) Remediation: Align critical security updates within maintenance windows.
- [Deployment Manager \(on page 38\)](#): Monitor action execution and reschedule if needed.
- [Fixlet Explorer \(on page 68\)](#) 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.

Create Dynamic Device Group

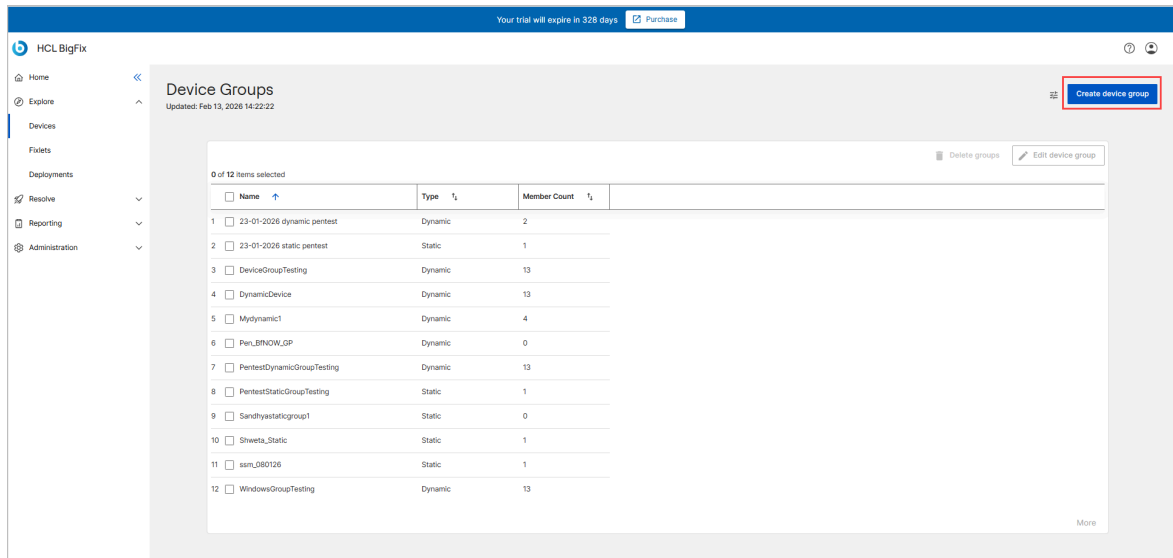
Device groups help you organize devices and target actions, policies, or maintenance settings. A dynamic device group updates automatically as devices start or stop matching the defined conditions.

Use this task to create a dynamic device group by defining filter conditions that automatically include devices matching specific criteria.

Procedure

1. From the BigFix SaaS side navigation, expand **Explore** and select **Devices**.
2. Click the **Device groups** icon next to the **Device Groups (Top 5 by Member Count)** chart.

The **Device Groups** page opens.



The screenshot displays the HCL BigFix web interface. At the top, a blue header bar contains the HCL BigFix logo, a navigation menu (Home, Explore, Devices, Fixlets, Deployments, Resolve, Reporting, Administration), and a trial status indicator: "Your trial will expire in 328 days" with a "Purchase" button. The main content area is titled "Device Groups" and shows a list of 12 items. A "Create device group" button is highlighted in the top right corner. Below the list, there are buttons for "Delete groups" and "Edit device group".

	Name	Type	Member Count
1	23-01-2026 dynamic pentest	Dynamic	2
2	23-01-2026 static pentest	Static	1
3	DeviceGroupTesting	Dynamic	13
4	DynamicDevice	Dynamic	13
5	Mydynamic1	Dynamic	4
6	Pen_BN0W_GP	Dynamic	0
7	PentestDynamicGroupTesting	Dynamic	13
8	PentestStaticGroupTesting	Static	1
9	Sandhyastaticgroup1	Static	0
10	Sheetta_Static	Static	1
11	ssm_080126	Static	1
12	WindowsGroupTesting	Dynamic	13

3. Select **Create device group** on the Device Groups page.

The **Create device group** widget opens.

Create device group ✕

Group name (required)

Filter the devices below

☒ Single condition
 ☐ Multiple condition (AND)

Property

Property ▾

Operator

Operator ▾

Remove all

Apply filter

Preview of dynamically applicable targeted devices

ⓘ

Insert a condition to dynamically add devices.

Dynamically add 0 devices to group

Cancel

Create device group

4. In **Group name (required)**, enter a unique name for the device group.
5. Under Filter the devices below, choose one of the following:
 - Single condition to define one filter rule.
 - Multiple condition (AND) to combine multiple filter rules.
6. Define the filter condition:
 - From **Property**, select the device property to filter by (for example, Active Directory Path).
 - From **Operator**, select the comparison operator (for example, contains).
 - In **Value**, enter the value to match.
7. (Optional) Add additional conditions if you selected Multiple condition (AND).
8. Select **Apply filter** to preview the targeted devices.
9. Review the **Preview of dynamically applicable targeted devices** section.
 - If devices match the conditions, they are listed in the preview.
 - If no devices match, the preview displays No Data Available.

10. Review the message at the bottom of the widget indicating how many devices will be dynamically added to the group.
11. Select **Create device group**.

The device group is created. Devices that match the defined filter conditions are automatically added to the group and updated dynamically over time.



Note:

- To remove all filter conditions and start over, select Remove all.
- Changes in device properties may cause devices to be added to or removed from the group automatically.

Create Static Device Group

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. This approach is useful when you want precise control over which devices are included for administrative actions, testing, or targeted operations.

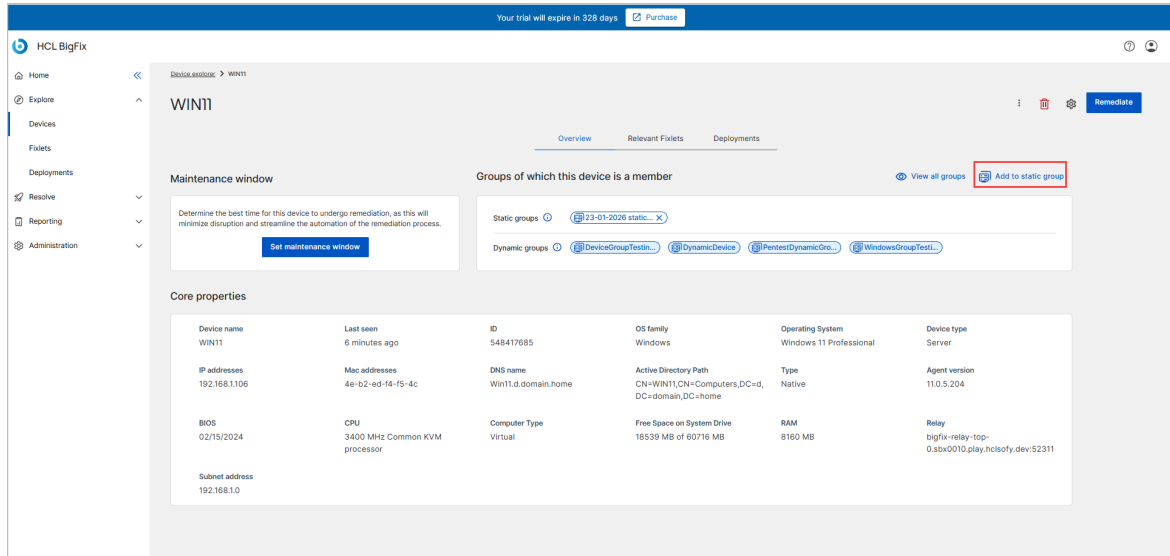
How Static Device Groups Work

- 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.
- 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**.

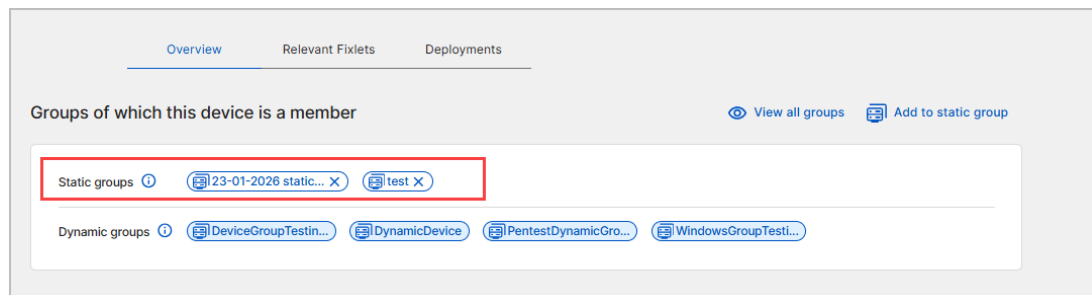


4. In the Add to static group dialog:



- Enter a name for the new static group.
- 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.

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

Add to static group ×

Create group

Select groups to add

☒ PentestStaticGroupTesting

☒ Sandhyastaticgroup1

☐ Shweta_Static

☐ ssm_080126

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**.

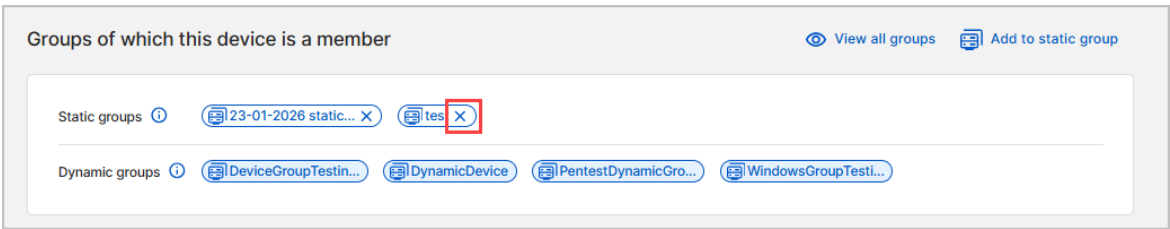
The device is added to the selected static groups.

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

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. Remove the device from the static groups.



The device is no longer a member of the static group.

The static group itself remains available for use.

On-Prem Relay Deployment

Enable BigFix SaaS customers to deploy, configure, and manage on-premises Relays that report to the cloud-based Top-Level Relays (TLRs), improving network efficiency and endpoint management in hybrid environments.

Overview

BigFix SaaS supports the deployment of **on-prem Relays**, allowing customers to create a hybrid Relay infrastructure. These Relays report back to the SaaS-hosted Top-Level Relays (TLRs), enabling optimized bandwidth usage, custom Relay selection hierarchies, and better support for geographically distributed environments.

BigFix SaaS users with appropriate permissions can:

- Deploy and configure on-prem Relays to report back to SaaS TLRs.
- Define Relay hierarchies, including leaf/child Relays within on-prem infrastructure.
- Configure Relay selection settings for endpoints using [Relay Assignment settings](#).
- Monitor Relay-related properties on endpoints via list view of the Device Explorer:
 - Relay installed
 - Relay selection
 - Distance to Relay
 - Relay

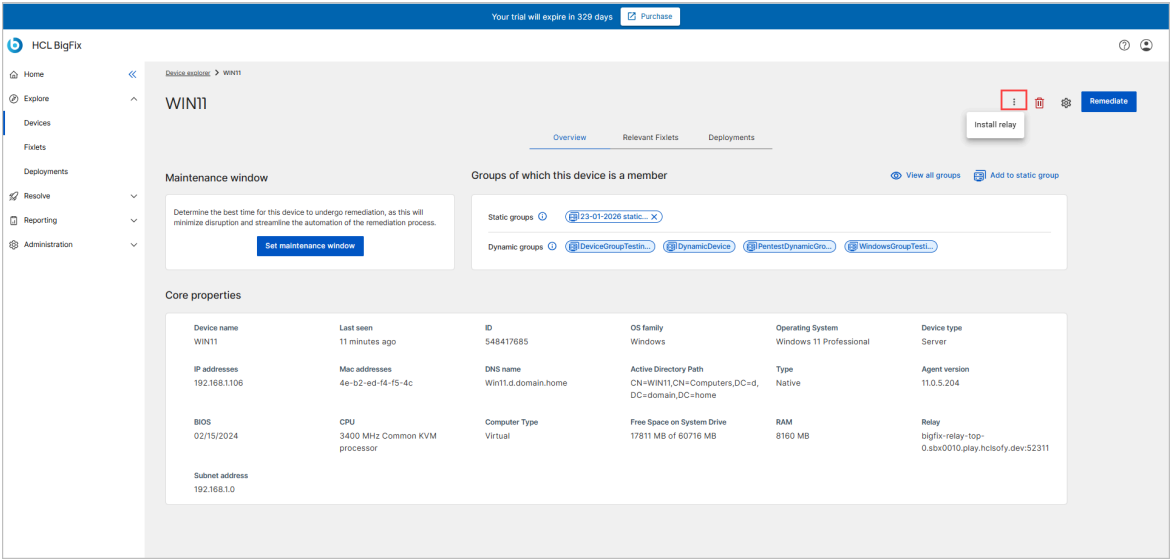
Relay Deployment Permissions

Action	Who Can Perform
Install Relay	Admin only
Uninstall Relay	Admin only
View Relay Status	All users

View Relay Hierarchy All users

Installing a Relay

- 1. Expand **Explore** from the side navigation, and then select **Devices**.
- 2. Go to **Device Explorer – List View**. When you click a **Device Name** from the table, the Device Details page opens.



- 3. From the **Overview** tab of the selected device, click on the **Install relay**  icon to open the Install Relay wizard.



Note: The **Install Relay** and **Uninstall Relay** buttons are visible only for admin users.

×

Install Relay

Relay Name

The Relay name is what will be used by BigFix Agents to find and connect to the Relay on the network. You can override this value to a different fully qualified domain name or IP address.

Win11.d.domain.home

Install location

Please specify the desired full path for the Relay service.

C:\Program Files\BigFix Enterprise\BES Relay

Relay selection

Primary Relay
Select the desired parent Relay to which this new Relay will connect (useful to define a tiered Relay hierarchy).

Cloud Relay (bigfix-relay-top-0.sbx0010.play.hclsofy.dev) ▼

Secondary Relay (optional)

Cloud Relay (bigfix-relay-top-0.sbx0010.play.hclsofy.dev) ▼

Authentication ☒

Relay authentication is recommended for internet-facing Relays.

Cancel

Install Relay

4. In the Install Relay wizard, provide the required details:

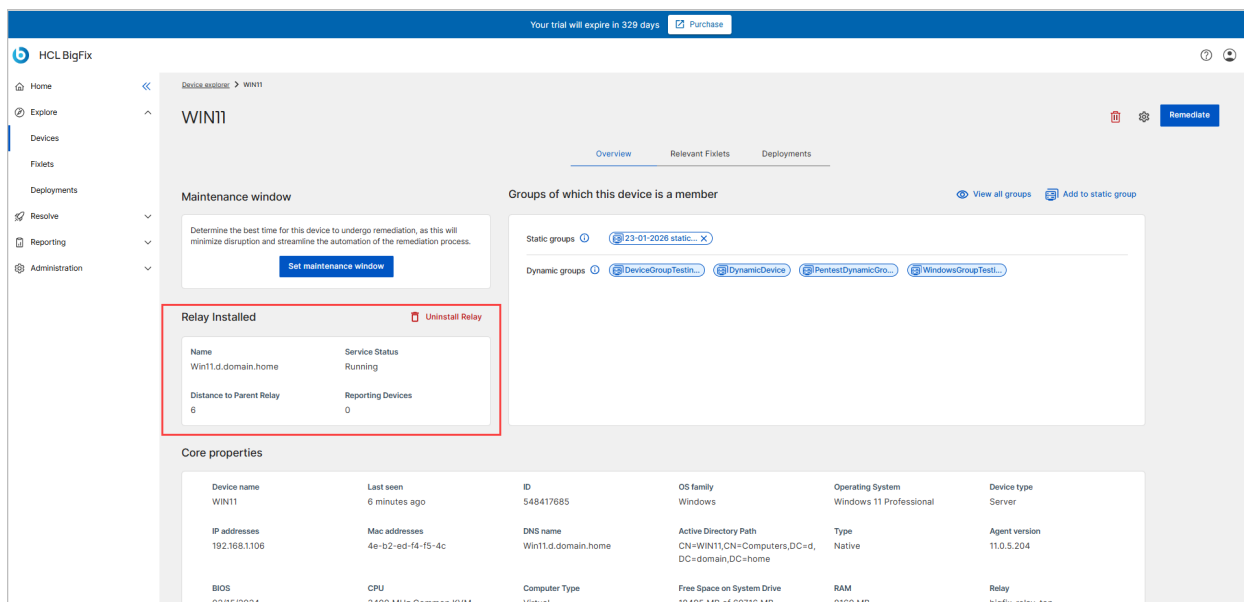
- **Relay Name:** Auto-suggested based on the client's host name (FQDN or IP), customizable by the user.
- **Install Location:**
 - For Linux, it is set by default.
 - For Windows, users can configure the path during installation.
- **Relay Selection:**
 - Choose the **Primary Relay** (default is the SaaS Cloud Relay).
 - Optionally, you can set another device as the **Secondary Relay** to act as a fallback if the Primary Relay becomes unavailable.
- **Authentication** (for internet-facing Relays): Enables protection against unauthorized use.

5. Click **Install Relay**.

The action is listed in the **Deployments** tab of the selected device and in the **Deployment Manager** after a few minutes.

Manage an Existing Relay

For devices where a Relay is already installed, the device **Overview** page displays the following changes:



- The **Install Relay** button is hidden.
- A **Relay Installed** section is shown, which includes:
 - Relay name
 - Relay status
 - Distance to Parent Relay
 - Reporting Devices
- **Uninstall Relay** button is shown.

Uninstalling a Relay

At any point in time, as an Admin, to uninstall a relay, complete the following.

1. Expand **Explore** from the side navigation, and then select **Devices**.
2. Go to **Device Explorer – List View**.
3. Click on the device which is a Relay.
4. From the device **Overview** tab of the selected device, in the **Relay Installed** section, click **Uninstall Relay**.

The action is listed in the **Deployments** tab of the selected device and in the **Deployment Manager** after a few minutes.

Best Practices for Relay Management

- **Avoid circular hierarchies:** Ensure each Relay has a single, clear parent Relay.
- **Monitor Relay load:** Balance endpoint connections to prevent performance issues.
- **Use Distance to Relay** to identify optimal Relay placement.
- **Deploy incrementally:** Start with a single layer of child Relays and expand based on bandwidth needs and endpoint locations

Client settings management

Configure, modify, or remove BigFix client (Platform) settings for individual or multiple devices using Device Explorer in BigFix SaaS.

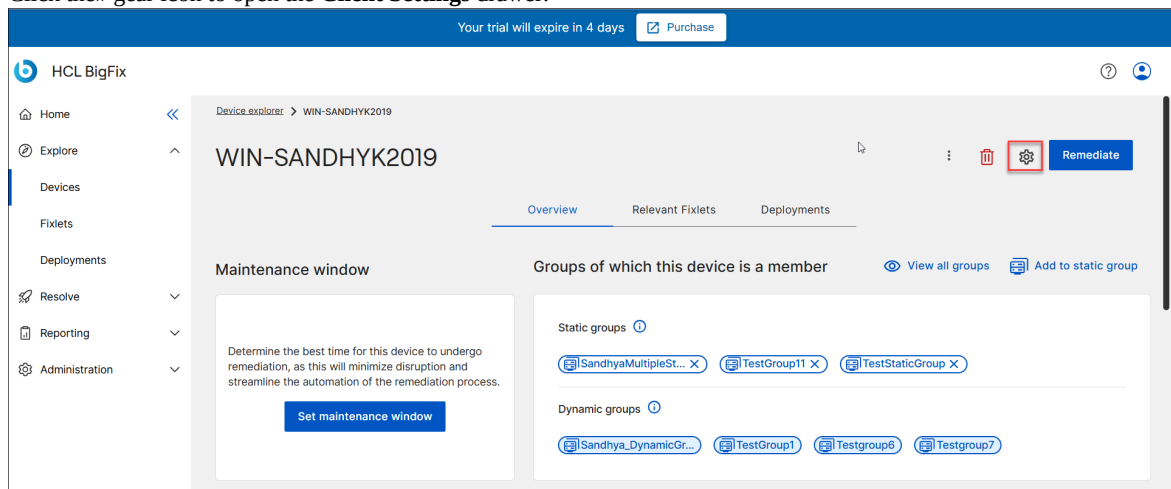
BigFix SaaS enables you to manage **client (Platform) settings** directly from the web-based interface without using the BES Console. These settings control client behavior such as CPU usage limits, relay selection, and action execution policies.

This feature allows you to:

- View current settings for a device.
- Add, edit, or delete client settings.
- Configure relay selection (automatic/manual).
- Apply settings across multiple devices using targeting options.
- Search, filter, and validate settings.
- Track pending changes before deployment.
- Prevent invalid or duplicate entries.

Accessing Client Settings

1. From the BigFix SaaS application, expand **Explore** and select **Devices**.
2. Change to list view and select the device you want to configure.
3. Click the **gear icon** to open the **Client Settings** drawer.



The **Update client settings** opens.

Update client settings [X]

Relay selection

☒ Auto

☐ Manual Select Primary Relay Select Secondary Relay

Cloud Relay (bigfix-relay-top-0rslb) Cloud Relay (bigfix-relay-top-0rslb)

New settings [+ Add setting](#)

Existing settings

0 updates [Expand all](#) [Collapse all](#)

Others [v]

_BESClient_ActionManager_HistoryKeepDays	1095	
_BESClient_ArchiveManager_LastArchive	444954f5e18b8685fd438da079f5f8eacd34b0bc6f9...	
_BESClient_Comm_EnableConnectionTriggers	1	
_BESClient_Comm_ForceHttpsOnRelay	1	

[Cancel](#) [Update settings](#)

Viewing and editing existing settings

- All existing BigFix Platform client settings of the selected device are listed in collapsible categories (For example, Action execution, Action management, Archiving client files and so on).
- Each category includes:
 - **Name** and editable **Value** fields of every client setting under the category
 - **Documentation link** that contains specific information of the client setting

- Button to **expand or collapse**
 - **Delete icon** to remove the client setting (changes to Undo icon when deleted). The input field is disabled when the setting is deleted.
 - **Undo icon** to revert a delete or edit and restore the original value (changes to Delete icon when restored)
- All edits, additions, and deletions are tracked and displayed as a total count of updates, as well as grouped under each affected category.

Search and navigation

- Use the **search bar** to find settings by name.
- Matching settings are listed as per the search.
- Use **Expand All** or **Collapse All** for quick navigation.

Configuring Relay Selection

Under the **Relay Selection** section:

- Choose **Automatic** or **Manual**.
- For Manual:
 - Select a **Primary Relay** (Cloud or On-Prem).
 - Optionally add a **Secondary Relay** as fallback.



Note: Apply relay settings carefully to avoid connectivity issues.

Adding a new setting

A. Defining a new setting

1. Click **Add Setting**.
2. Enter a **key name** and **value**.



Note:

- Avoid overwriting platform-defined settings unless necessary.
- Use clear, consistent naming for custom settings.
- For structured data (like JSON), validate syntax before saving.

3. Repeat to add more key-value pairs.
4. Duplicate or empty fields are not allowed; errors are shown inline.



Note: Long values are fully visible via tooltips and support horizontal scrolling for editing. You can enter JSON strings, which are accepted as plain text.

B. Submitting Changes

1. Click **Update Settings** to deploy changes.
2. A **BigFix Action** is generated and visible in the **Deployment Manager**.

Related information

[Device Explorer \(on page 43\)](#)

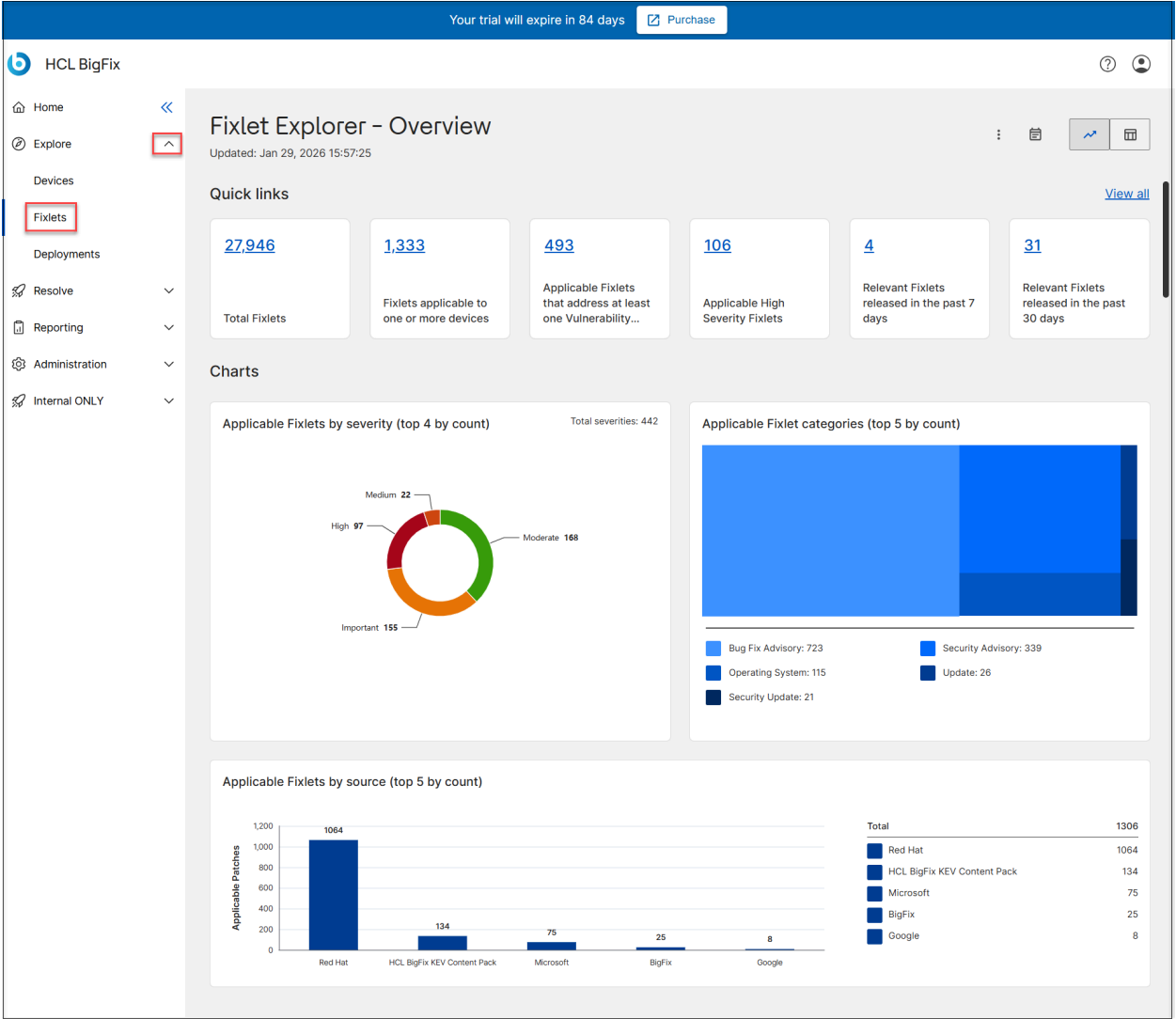
Fixlet Explorer

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. 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.

To access the **Fixlet Explorer** app, expand **Explore** and select **Fixlets** .



By default, the data is displayed in chart view. Click  to view the data in a table.

Fixlet Explorer – List view

Updated: Jan 29, 2026 16:26:45

0 of 1333 fixlets selected

☐	Title	SiteID	ID	Severity	Category
☐	Linux Kernel Use-After-Free Vulner	15785	30240	High	Operating System
☐	List enabled modules to file on clie	15763	501	Unspecified	Support
☐	Manage KEY Scanner Settings	15785	120	No data	Utility Task

[More](#)



Note: Fixlet Explorer shows only the top 100 Fixlets for a filter and does not support pagination or endless scrolling.

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.

The Fixlet Explorer data table contains the following fields:

- **Title** – Displays the title of the Fixlet.
 - The Fixlet name is a clickable hyperlink. Selecting it opens the Fixlet Explorer – Detail Page, where you can view complete information about that Fixlet, including applicable devices, associated CVEs, and metadata.
- **Site ID** –
- **ID** – Shows the unique numeric identifier assigned to each Fixlet in the BigFix environment.
- **Relevant Devices Count** – Displays the number of devices currently relevant for that Fixlet, helping you quickly gauge its impact or applicability within your environment.
- **CVE IDs** – Lists any associated Common Vulnerabilities and Exposures (CVE) identifiers linked to the Fixlet.
 - If any CVE identifiers are linked to the Fixlet, each CVE ID is a clickable hyperlink. Selecting it opens the CVE IDs panel, which displays detailed vulnerability references related to that Fixlet.
- **Severity** – Indicates the severity level of the Fixlet as classified by the source (for example, Critical, Important, or Unspecified).
- **Category** – Describes the type or classification of the Fixlet, such as Update, Security Advisory, or Undo Workaround.
- **Source Release Date** – Displays the release date of the Fixlet as provided by its source, indicating when it became available.
- **Source** - Origin or vendor of the Fixlet (for example, Microsoft, Apache).
- **Source ID** - Vendor-specific reference number.
- **Download Size** - Size of any related patch or update file.

Let's go through the top row of the Fixlet Explorer table, from left to right:



- The **Filter** icon brings up the [filter \(on page 10\)](#) sidebar. In this sidebar, users can narrow down the displayed Fixlets using a variety of parameters.
- The total number of Fixlets relevant to the devices enrolled in your account
- 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.



Note:

By default, the **Deploy** button is disabled and can only be clicked when at least one Fixlet is selected in the data table. For users whose local administrators have not granted deployment rights, the Deploy button may remain permanently disabled.

- The Fixlet Explorer data table supports [sorting \(on page 10\)](#) by clicking a column header label. Click again to reverse sort.
- For more details about filtering, sorting, managing reports, and exporting, see [Common Functionalities \(on page 10\)](#).

The Fixlet Data table only shows a summary of the Fixlet. Click on the Fixlet name to bring up a more focused Fixlet Explorer page with additional details for the Fixlet.

Your trial will expire in 84 days

Purchase

HCL BigFix

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Internal ONLY

Fixlet Explorer > 4072699: Set registry value to unblock installation of security updates - Windows 7 / Windows Server 2008 R2 / Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 / Windows 10...

4072699: Set registry value to unblock installation of security updates - Windows ...

Overview

Relevant Devices

Deployments

Properties

ID	CVE(s)	Severity	Category
2.407269901	N/A	Unspecified	Setting
Release Date	Source	Source ID	Download Size
Jan 04, 2018	Microsoft	KB4072699	0

Relevance (3 of 4 shown)

View All

Actions (1 of 1 shown)

Relevance 1

Wrap long lines

Copy code

```
((if( name of operating system starts with "Win" ) then platform id of operating system != 3 else false) AND (if exists property "in proxy agent context" then ( not in proxy agent context ) else true )
```

Show More

Relevance 2

Wrap long lines

Copy code

```
not ia64 of operating system
```

Show More

Relevance 3

Wrap long lines

Copy code

```
((name of it = "Win7" OR name of it = "Win2008R2") OR name of it = "Win8.1" OR name of it = "Win10" OR name of it = "Win8" OR name of it = "Win2012" OR name of it = "Win2012R2" OR name of it = "Win2016") of operating system
```

Show More

Action1

Wrap long lines

Copy code

```
regset "[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityC" "cadca5fe-87d3-4b96-b7fb-a231484277cc"=dword:0
```

Show Less

To learn more about the CVE(s) associated with a Fixlet, click the blue highlighted CVE number in the CVE column. This will cause the CVE panel to slide out from the right side of the screen, providing additional information about the CVE.

0 of 260 Fixlets selected

	Title	Size	ID	Severity	Category	CVE
8	40726988: Additional instructions for...	2	407269881	Unspecified	Security Advisory	3 CVEs
9	40726989: Enable instructions for...	2	407269897	Unspecified	Security Advisory	8 CVEs
10	40726990: Enable instructions for...	2	407269905	Unspecified	Security Advisory	7 CVEs
11	40726991: Enable instructions for...	2	407269908	Unspecified	Security Advisory	CWE-2018-3639
12	40726992: Enable instructions for...	2	407269901	Unspecified	Security Advisory	2 CVEs
13	40726993: Set registry value to...	2	407269907	Unspecified	Setting	N/A
14	40731118: Additional instructions for...	2	407311190	Unspecified	Security Advisory	11 CVEs
15	40731119: Enable instructions for...	2	407311904	Unspecified	Security Advisory	CVE-2017-5753
16	40731120: Enable instructions for...	2	407311905	Unspecified	Setting	N/A
17	40731121: Enable instructions for...	2	407311906	Unspecified	Security Advisory	CVE-2018-3639
18	40731122: Enable instructions for...	2	407311901	Unspecified	Setting	N/A
19	44029300: Update for Active...	2	440293007	Unspecified	Update	N/A

CVE IDs

Fixlet

- CVE-2018-1135
- CVE-2018-11091
- CVE-2018-12126
- CVE-2018-12127
- CVE-2018-12130
- CVE-2017-5753
- CVE-2017-5715
- CVE-2018-3639
- CVE-2018-3615
- CVE-2018-3620
- CVE-2018-3646

Related information

[Adding devices to BigFix \(on page 18\)](#)

[Protection Level Agreement \(PLA\) \(on page 89\)](#)

Fixlet Details page

Learn about the various widgets present on the Fixlet Details page. Widgets help you learn more about a deployment, Fixlet, specific relevance script, or understanding a Fixlet's origins.

The Fixlet Details page allows to drill down into a Fixlet for its specific information. These details can be especially useful when evaluating whether to deploy a particular Fixlet, explore the specific relevance script, or understand more about the Fixlet's origins.

To access the Fixlet Details page, click on the Fixlet name from the data table. Once loaded, the Fixlet Details page has several widgets that display properties that are unique to the selected device.

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Internal ONLY

Your trial will expire in 83 days

Purchase

HCL BigFix

Fixlet Explorer > 2696547: Manage SMBv1 in Windows and Windows Server - Disable Workaround (Remove SMB v1 completely) - Windows 8.1 / Windows 10 / Windows Server 2012 R2 / Windows Server 201...

2696547: Manage SMBv1 in Windows and Windows Server - Disable Workaround (...)

Overview

Relevant Devices

Deployments

Properties

ID	CVE(s)	Severity	Category
2.269654707	N/A	Unspecified	Undo Workaround
Release Date	Source	Source ID	Download Size
May 15, 2017	Microsoft	KB2696547	[null]

Relevance (3 of 4 shown)

View All

Actions (1 of 1 shown)

Relevance 1

Wrap long lines

Copy code

```
(if( name of operating system starts with "Win" ) then platform id of operating system != 3 else false) AND (if exists property "in proxy agent context" then ( not in proxy agent context ) else true )
```

Show More

Relevance 2

Wrap long lines

Copy code

```
not ia64 of operating system
```

Show More

Relevance 3

Wrap long lines

Copy code

```
(((((name of it = "Win2012" AND value "CurrentVersion" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as string is "6.3") OR name of it = "Win2012R2")) OR (name of it = "Win2016" OR name of it starts with "Win20" AND (exists value "CurrentMajorVersionNumber" of it AND
```

Show More

Action1

Wrap long lines

Copy code

```
if {(((name of it = "Win8" AND value "CurrentVersion" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as string is "6.3") OR name of it = "Win8.1") AND service pack major version of it = 0) OR name of it = "Win10" OR (it starts with "Win" AND it does not start with "Win20") of name of it AND (exists value "CurrentMajorVersionNumber" of it AND value "CurrentMajorVersionNumber" of it as integer = 10) of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry) of operating system}

// Disable wow64 redirection on x64 OSes

action uses wow64 redirection {not x64 of operating system}

delete __createfile

// CREATEFILE

createfile until END_OF_FILE

Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

END_OF_FILE

delete powershell.ps1

move __createfile powershell.ps1

waithidden { pathname of file ((it as string) of value "Path" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft of native registry) } -ExecutionPolicy Bypass -File powershell.ps1

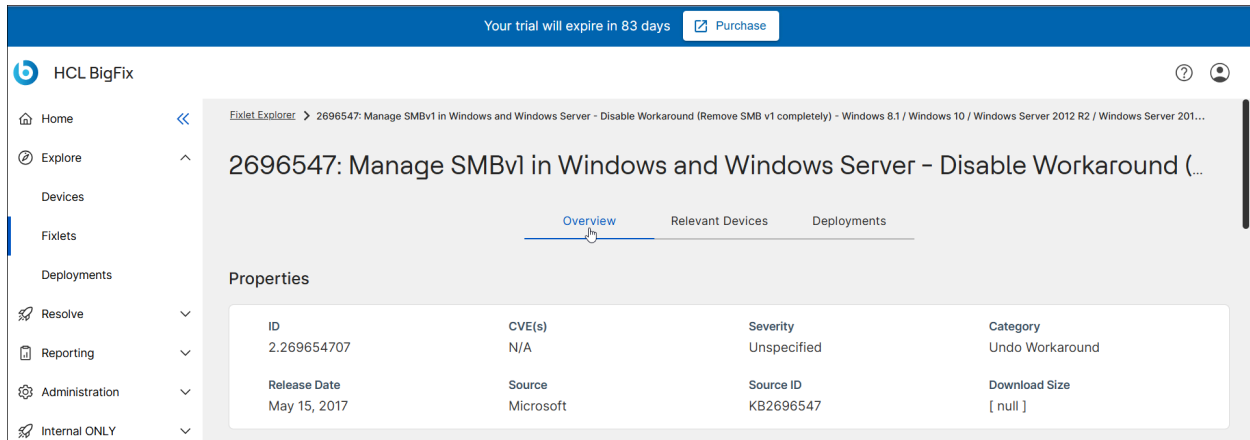
else

action uses wow64 redirection {not x64 of operating system}
```

Show Less

Overview - Fixlet Properties

The Fixlet Properties widget is located in the center of the page. The Fixlet Properties widget displays properties associated with the Fixlet, such as its severity, author, and release date.



Your trial will expire in 83 days [Purchase](#)

HCL BigFix

Home << Fixlet Explorer > 2696547: Manage SMBv1 in Windows and Windows Server - Disable Workaround (Remove SMB v1 completely) - Windows 8.1 / Windows 10 / Windows Server 2012 R2 / Windows Server 201...

2696547: Manage SMBv1 in Windows and Windows Server - Disable Workaround (...)

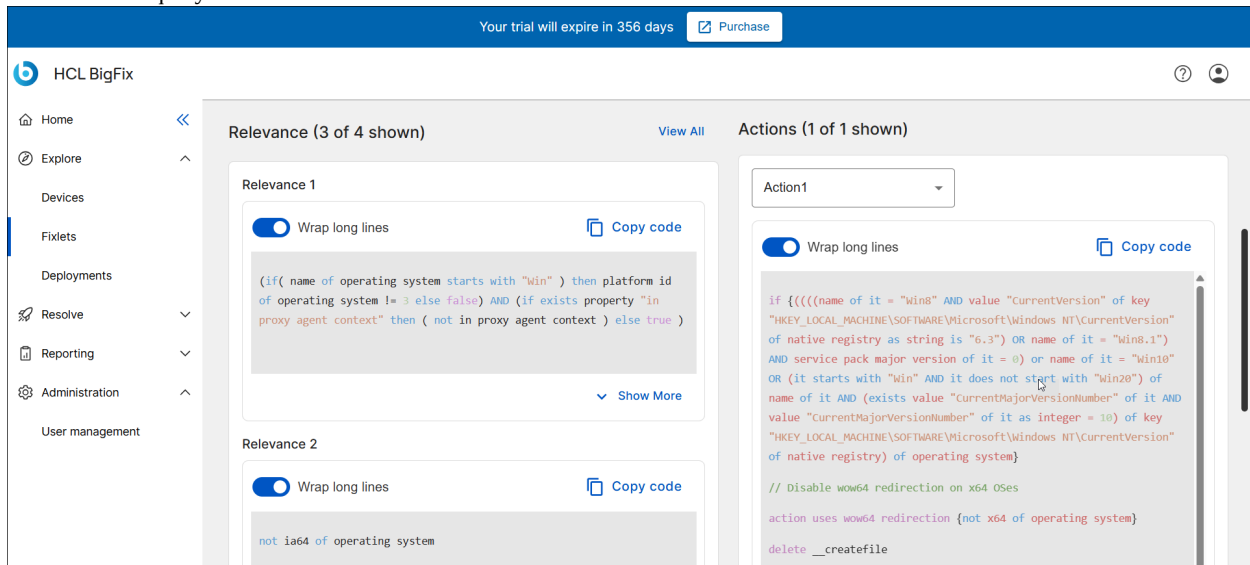
Overview Relevant Devices Deployments

Properties

ID	CVE(s)	Severity	Category
2.269654707	N/A	Unspecified	Undo Workaround
Release Date	Source	Source ID	Download Size
May 15, 2017	Microsoft	KB2696547	[null]

Relevance

Relevance is a scripting language used by BigFix to create Fixlets. While it is not required to learn Relevance, understanding the relevance definitions and the criteria that the Fixlet satisfies can be beneficial. Click **View All** in the widget's header to see the full Relevance query.



Your trial will expire in 356 days [Purchase](#)

HCL BigFix

Home << Explore > Relevance (3 of 4 shown) View All Actions (1 of 1 shown)

Relevance 1

☒ Wrap long lines [Copy code](#)

```
(if( name of operating system starts with "win" ) then platform id of operating system != 3 else false) AND (if exists property "in proxy agent context" then ( not in proxy agent context ) else true )
```

[Show More](#)

Relevance 2

☒ Wrap long lines [Copy code](#)

```
not ia64 of operating system
```

Action1

☒ Wrap long lines [Copy code](#)

```
if {(((name of it = "win8" AND value "CurrentVersion" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as string is "6.3") OR name of it = "win8.1") AND service pack major version of it = 0) or name of it = "win10" OR (it starts with "win" AND it does not start with "win20") of name of it AND (exists value "CurrentMajorVersionNumber" of it AND value "CurrentMajorVersionNumber" of it as integer = 10) of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry) of operating system}

// Disable wow64 redirection on x64 OSes

action uses wow64 redirection (not x64 of operating system)

delete __createfile
```

This widget presents the Fixlet relevance code, allowing comprehension of the relevance definitions and criteria fulfilled by the Fixlet. Click **View All** in this widget to display the entire relevant statement for the selected Fixlet.

< Fixlet Explorer: Details

Updated: Jun 26, 2024 20:13:13

2.269654707 - 2696547: Manage SMBv1 in Windows and Windows Server - Disable Workarou...

Relevance (4 of 4 shown)

Relevance 1

```
(if( name of operating system starts with "Win" ) then platform id of operating system != 3 else false) AND (if exists property "in proxy agent context" then ( not in proxy agent context ) else true )
```

Relevance 2

```
not ia64 of operating system
```

Relevance 3

```
((((name of it = "Win2012" AND value "CurrentVersion" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as string is "6.3") OR name of it = "Win2012R2")) or (name of it = "Win2016" OR name of it starts with "Win20" AND (exists value "CurrentMajorVersionNumber" of it AND value "CurrentMajorVersionNumber" of it as integer = 10) of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry) or (((name of it = "Win8" AND value "CurrentVersion" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as string is "6.3") OR name of it = "Win8.1") AND service pack major version of it = 0) or (name of it = "Win10" OR (it starts with "Win" AND it does not start with "Win20") of name of it AND (exists value "CurrentMajorVersionNumber" of it AND value "CurrentMajorVersionNumber" of it as integer = 10) of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry)) of operating system
```

Relevance 4

```
not exists key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10" of native registry
```

Actions

This widget displays the actions that the selected Fixlet will execute when it is run on targeted, relevant devices. These actions are the actual commands that are run on the devices. Some Fixlets include multiple actions. You can view all available actions for a Fixlet by selecting the **Action** dropdown menu.

Relevant Devices

This tab displays information about the relevant devices, including their names, dates last seen, IDs, OS family, operating systems, device types, associated IP addresses, DNS name, and associated MAC addresses.

Your trial will expire in 83 days [Purchase](#)

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Internal ONLY

<<

>>

	Device name	t ₁		Last seen	t ₁	ID	t ₁	OS family	t ₁	Operating system	t ₁
14	SAASNILESHWIN1			7 weeks ago		1619320885		Windows		Windows Server 2019 Standard	
15	SAASNILESHWIN1			7 weeks ago		538730224		Windows		Windows Server 2019 Standard	
16	SANDHYAWIN2019			7 weeks ago		16180985		Windows		Windows Server 2019 Standard	
17	VANJI-WINDOWS			7 weeks ago		538064145		Windows		Windows 11 Professional	
18	SAASNILESHWIN1			7 weeks ago		1078901487		Windows		Windows Server 2019 Standard	
19	DESKTOP-84U605I			7 weeks ago		1083309832		Windows		Windows 11 Professional	
20	DESKTOP-84U605I			7 weeks ago		1623151053		Windows		Windows 11 Professional	

More

Deployments

This tab shows a chronological list of every deployment in which this Fixlet has been included.

Your trial will expire in 83 days [Purchase](#)

HCL BigFix

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Internal ONLY

Name	State	Issued	ID	Start date	End date
22 FixleExsp_xdeHvtONUWb mENskPaPaoSuRBW1764...	Expired	8 weeks ago	1341	[null]	Dec 3, 2025 at 06:55 (Client)
23 Test	Expired	8 weeks ago	1237	[null]	Dec 1, 2025 at 06:03 (Client)
24 Testing_TestCase1	Expired	8 weeks ago	1235	[null]	Dec 1, 2025 at 05:38 (Client)
25 123	Expired	9 weeks ago	1082	[null]	Nov 25, 2025 at 07:24 (Client)
26 test 2	Expired	10 weeks ago	1012	[null]	Nov 23, 2025 at 08:50 (Client)
27 FixleExp_sfNbHumxELVQeg fDcslJDRQRrJ176311190...	Expired	11 weeks ago	907	[null]	Nov 16, 2025 at 06:55 (Client)
28 FixleExpsp_MBcSwdclQUP QmRQDSmqllVFCod1763...	Expired	11 weeks ago	899	[null]	Nov 15, 2025 at 06:55 (Client)

More

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 how to deploy a Fixlet from the Fixlet Explorer.

To access the deploy menu, expand **Explore** and click **Fixlet**.

From the Fixlet list view, select at least one Fixlet. The **Deploy** button is enabled. Click **Deploy** that slides out from the right. The wizard will guide you through the steps to create a new deployment.

Your trial will expire in 83 days [Purchase](#)

HCL BigFix

Home

Explore

Devices

Fixlets

Deployments

Resolve

Reporting

Administration

Internal ONLY

Fixlet Explorer - List view

Updated: Jan 30, 2026 15:21:37

Charts 0 charts set

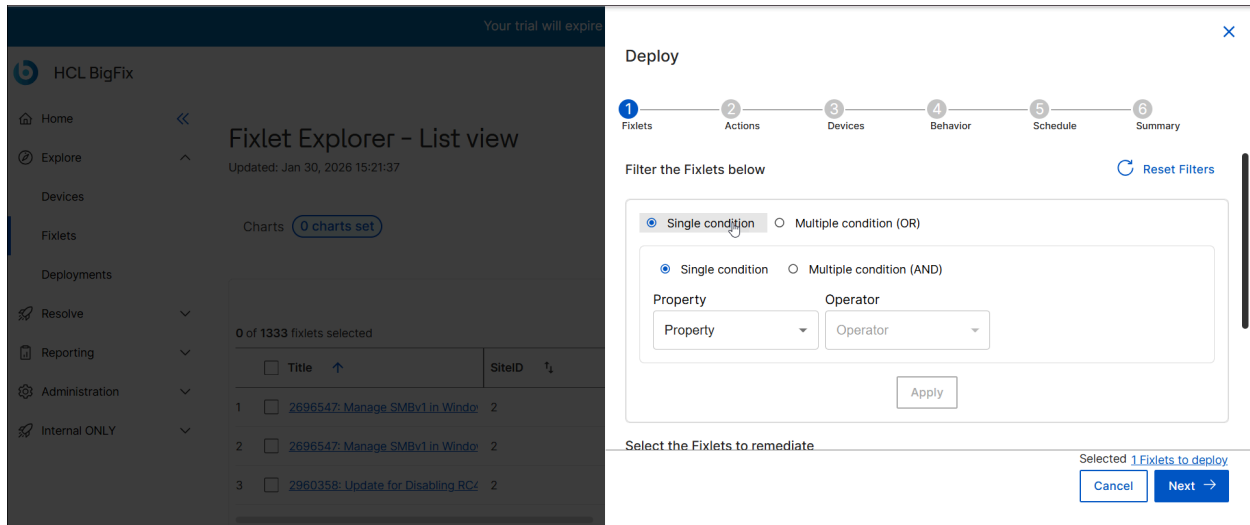
1 of 1333 fixlets selected

Title	SiteID	ID	Severity	Category
2696547: Manage SMBv1 in Window	2	269654707	Unspecified	Undo Workaround
2696547: Manage SMBv1 in Window	2	269654705	Unspecified	Workaround
2960358: Update for Disabling RC	2	296035803	Unspecified	Security Update

Deploy

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

The Deploy Wizard allows to customize user deployments; however, these customizations are optional.



1. **Fixlets:** The selected Fixlets are considered for remediation. You can modify the Fixlet selection in this step.
2. **Actions:** In this step, 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.

There are two different types of Fixlets that may require attention before deployment:

- **Attention required** - requires input from the user to be able to deploy successfully. To aid with visual identification, attention required Fixlets are highlighted in red and are marked with a cross icon. Some Fixlets require attention because they cannot run without some input from the user, such as a password.
- **Attention recommended** - requires user input to select the action the Fixlet should perform. To aid with visual identification, attention recommended Fixlets are highlighted in orange and are marked with a warning icon. Some Fixlets have multiple possible actions and users must select which action they wish for the deployment to perform. Users must select at least one action per Fixlet.

Once the necessary information is provided for all Fixlets to run correctly, a green checkmark will appear and the highlighting will be removed.

Until you provide the required information for all attention required and attention recommended Fixlets, you cannot proceed with their deployment. Once this information is provided, click **Next** to proceed to the sequence tab.

3. **Devices:** This step prompts 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**.

To access the filter menu, click the **Add Filter** button. BigFix supports three types of filtering: static, dynamic, and device list.

- **Static Filter** - a static filter reduces the number of devices using information that is known about a device when the deployment is created. In the static filter tab, it is required to first select an attribute to filter devices. Examples of attributes include computer type, BIOS, and Agent Version. Then, specify the condition, such as "contains", "equals", or "starts with". Finally, input a value in free text that is used for purposes of filtering.

To add additional static filter groups, click **Add Group**.

- **Dynamic Filter** - While static filtering is a subset of a list of applicable devices at the time when the deployment is created, dynamic filtering continuously evaluates whether a device is applicable as long as the deployment is active. When using dynamic filtering, the Deploy Wizard displays the number of applicable devices at that time. That number, however, may go up if additional devices become eligible for the deployment.

In the dynamic filter tab, first select an attribute to filter devices. Examples of attributes include computer type, BIOS, and Agent Version. Then, specify the condition, such as "contains", "equals", or "starts with". Finally, input a value in free text that is used for purposes of filtering.

To add additional dynamic filter groups, click **Add Group**.

- **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. 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.

The sequence 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.
- 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.
- d. **Reboot/restart device on deployment completion** - This determines whether the device will be forced to restart after the deployment is complete.
- 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. Users may also specify the maximum number of retries and the time interval between retry attempts.
- f. **Reapply whenever it becomes relevant again.**

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 \(on page 52\)](#).

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

6. **Summary** - This step 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. It is also required to input a name for the deployment on the summary page.

After reviewing your selections, click **Deploy**.

Related information[Fixlet Explorer \(on page 68\)](#)

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.

Setting Up Automated Remediation

The **Fixlet Stream** feature allows users to automate patch and update deployments across devices by utilizing pre-built or [custom \(on page 85\)](#) Fixlet streams. The Fixlet streams are displayed as **cards** showing the stream's name, status (Active/Inactive), and a brief description.

You need to **Subscribe Devices** to a Fixlet Stream. This is done by creating dynamic filters that continuously match devices based on defined criteria. You can group devices by specifying conditions based on attributes, such as OS or software version, and then applying or resetting these conditions. Once applied, devices are subscribed to the stream, and you can proceed to **Create automation** for deployment. Throughout the process, you'll also be able to monitor **Fixlet compliance** and **Deployment progress** for the active stream. For step-by-step information, read [Setting up Fixlet Streams \(on page 80\)](#).

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.

Filtering

The **Filtering Capability** in Fixlet Streams enables users to refine their search based on specific criteria, making it easier to quickly find relevant updates and patches. This feature includes the following filters, each targeting a key aspect of every Fixlet stream:

- **Name:** Filters Fixlet streams by searching for specific strings within the Fixlet stream's name.
- **Description:** Filters Fixlet streams by searching for specific strings within each Fixlet stream's description.
- **CVE Name:** Filters Fixlets based on Common Vulnerabilities and Exposures (CVE) identifiers, aiding in locating security patches for particular vulnerabilities.
- **Type:** Filters Fixlets based on selected types, whether built-in or custom.
- **Vendor:** Filters Fixlets by vendor, enabling targeted patch management for software from specific providers.
- **Category:** Allows filtering by category, such as security or updates, within the Fixlet streams.
- **Severity:** Filters Fixlets by severity level (e.g., critical, high, medium, low), helping prioritize patches that require immediate attention.

Saving a view

Fixlet Streams support [saving a view \(on page 10\)](#) of the filtered and sorted data and access the saved view quickly when needed.

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.
- **Deployment Progress:** The system also provides a **deployment progress bar** for the active Fixlet Stream, allowing you to track how far along the deployment process is.
 - **Real-Time Updates:** Use the progress bar to monitor the deployment status in real time. This can help you spot any 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.

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.

Additional Resources

- [Common use cases \(on page 87\)](#)
- [Troubleshooting \(on page 86\)](#)

Setting up Fixlet Streams

Setting up Fixlet Streams involves accessing the built-in streams displayed as cards and subscribing devices based on dynamic filters. You can create targeted subscriptions by specifying conditions based on attributes, ensuring that the right devices

receive necessary updates. Once devices are subscribed, you can create automation for seamless patch deployments and monitor compliance and progress in real time.

To set up your Fixlet Stream, complete the following steps.

1. Accessing the Fixlet Stream

1. Logging in

Log in to BigFix SaaS using your Admin credentials.

2. Go to the Fixlet Stream Section

In the BigFix SaaS application, from the left pane expand **Resolve** and select **Fixlet Stream**. This opens the list of available streams. All built-in Fixlet Streams are presented as **cards**. Each card provides:

- The **name** of the Fixlet Stream.
- Its **status** (Active/Inactive).
- A brief **description** of the Fixlet Stream.
- Actions to **Create subscriptions** or **Create automation**.

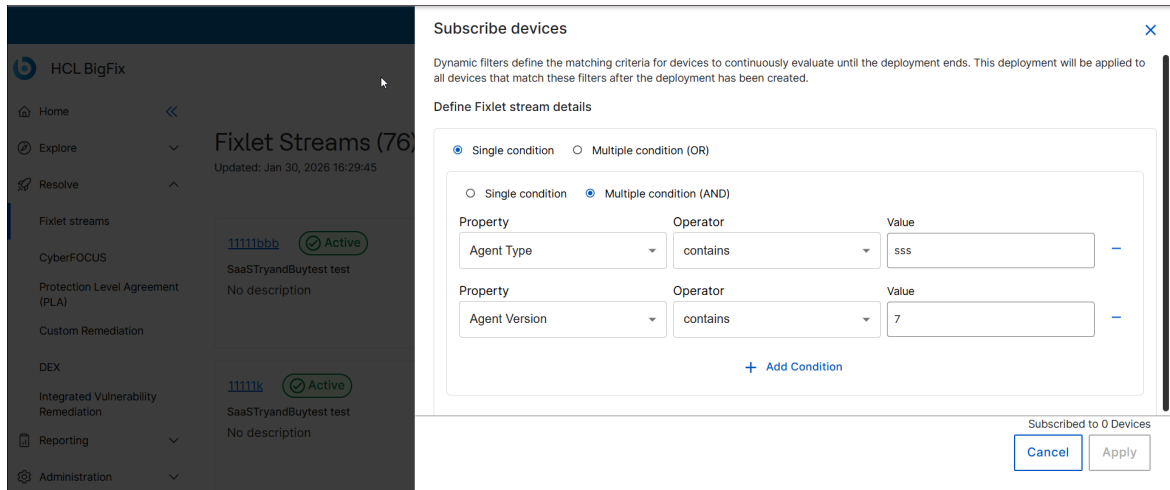
3.

2. Subscribing Devices to a Fixlet Stream

To deploy a Fixlet Stream, you need to subscribe devices using dynamic filters. To do that, complete the following steps:

1. On the desired Fixlet Stream card, click **Create subscription**.

2. On the Subscribe devices page, define the conditions to filter devices to subscribe.



- You can group devices that match conditions based on the following parameters:
 - **Property:** Device attributes like OS, RAM, software version.
 - **Operator:** Criteria such as equals, greater than, contains.
 - **Value:** The specific value for the condition.
 - **Single condition:** Allows you to define parameters for one condition. Example: To subscribe all Windows devices, set the attribute to "OS", the condition to "equals", and the value to "Windows".
 - **Multiple condition (AND):** Allows you to define multiple conditions and filters devices that match all the defined conditions. You can add multiple conditions, to ensure that they reflect the criteria relevant to your deployment needs. For example, you can add conditions based on geography, software version, or device type.
 - **Multiple condition (OR):** Allows you to define multiple conditions and filters devices that match at least one condition that qualify for subscription.
3. Review the device count. As per the dynamic filters, the system automatically displays the total number of **dynamically filtered devices** that are eligible for subscription.
 4. Click **Apply** to subscribe devices to the Fixlet Stream. This triggers a continuous evaluation of matching devices.

“

Note: If an error occurs, you will see the message "**Error fetching devices. Please try again.**" Review your conditions and try again.



Tip: If you want to modify the conditions or start over, click **Edit subscriptions** to clear the current filters.

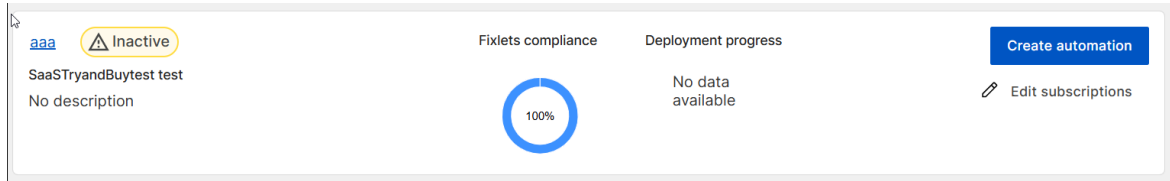
”

Once the devices are subscribed, the **Subscription definition** status of the Fixlet Stream changes to "Set", and the **Create automation** button is enabled to perform the next step.

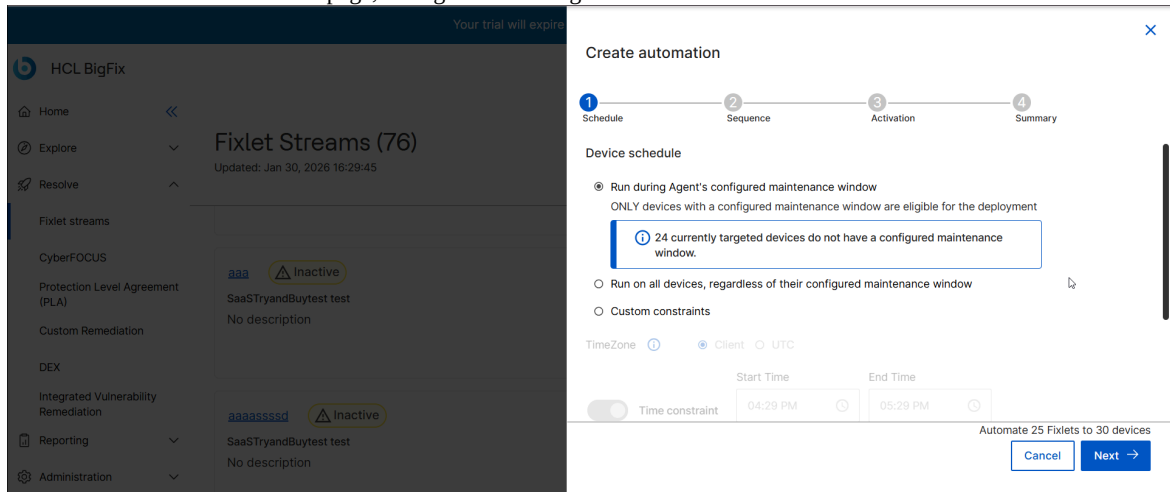
3. Creating Automation

After subscribing devices, to create an automation definition, complete the following steps:

1. On the desired Fixlet Stream card, click **Create automation**.



2. On the Automation Remediation page, configure the settings.



- a. Configure automation schedule and click **Next**.
 - **Device schedule:** Select an option as per the requirement.
 - Run during Agent's configured maintenance window. Only devices with configured maintenance window are eligible for the deployment. It also displays how many devices from the currently targeted devices do not have a configured maintenance window.
 - Run on all devices, regardless of their configured maintenance window.
 - Custom constraints. Specify the constraints for the execution window.
 - **Start Time:** Select the time when the automation should begin.
 - **End Time:** Define when the automation should conclude.
 - **Time Zone:** Select the appropriate option:
 - Client - start and end time of the maintenance window is based on the local time of the BigFix client device. Use this when devices are in different time zones and you want them to start maintenance at the same local time.
 - UTC - The start and end time is based on Coordinated Universal Time (UTC). Use this when you want all devices to enter maintenance mode at the same exact moment globally, for example, during a worldwide patch rollout.
 - **Day of the Week:** Choose which day(s) the automation will run.
 - Choose how frequently you want the newly updated remediation content to refresh: For example, **Weekly, Monthly, or Every 2 Weeks**.
- b. Define the **Sequence** by setting the order of events for the automation and click **Next**.
- c. Specify a future **Activation** date for the automation to begin and click **Next**.
- d. Review the **Summary** page.
- e. Review the applicable **Fixlets** and the **Dynamically Targeted Devices**. These numbers appear as links that you can click to see the list of applicable Fixlets and the list of targeted devices.
- f. Once everything is configured to your satisfaction, click the **Create** button. A message will display: **"Congratulations! Automation created successfully."** Click **OK** to acknowledge the message.

Result: On the selected Fixlet Stream card, the **Automation Definition** status changes to **Set**, and the Fixlet Stream becomes active.

What to do next: As deployments occur, data appears dynamically for monitoring. If there are any issues or concerns, click on the name of the Fixlet Stream to access the [detailed information \(on page 84\)](#).

Fixlet details page

The Fixlet Details Page provides comprehensive information about the status and configuration of your Fixlet Stream.

Your trial will expire in 83 days

Purchase

HCL BigFix

Home

Explore

Resolve

Fixlet streams

CyberFOCUS

Protection Level Agreement (PLA)

Custom Remediation

DEX

Integrated Vulnerability Remediation

Reporting

Administration

Fixlet Stream > 11111bbb

11111bbb

Updated: Jan 30, 2026 16:45:17

Edit Fixlet Stream

Overview

Devices

Fixlets

Deployments

100%

Fixlets Compliance

No data available

Deployment Progress

0

Devices

1027

Fixlets

Automate remediation schedule

Edit Automation

Subscription definition

Edit subscriptions

Device schedule

Time range: 10:25 AM - 10:46 AM, client time zone

Days of week: Sunday

Auto deploy new/updated content

Every 2 weeks

Before deployment begins:

Begin download after deployment starts

No retries on failure

One time deployment

Reboot/restart: No

Before running message has not been configured

While running message has not been configured

Activation

Start date & time: 05 Dec 2025 at 11:53 AM client time zone

Subscription definition

Agent Type contains "sss" and Agent Version contains "7"

Status

No description

Active

Composition

No deployment data found

Properties

ID	Stream Name	Description
221184a9-e547-4a7d-92cb-65ca3812beb3	11111bbb	[null]
Stream Source	Content Type	Operating System
HCL BigFix	fixlet	Windows 3rd party, Win23H2, Win20H2, Win2022, ...

Here’s what you can find:

- **Status:** Displays whether the Fixlet Stream is **Active** or **Inactive**. Users can toggle this status as needed.
- **Edit Options:**
 - **Edit Subscription:** Modify the device subscriptions associated with the Fixlet Stream.
 - **Edit Automation:** Change the automation settings, including the schedule or conditions.
- **Activity Feed:**

- Shows a list of **Recent, Scheduled, In Progress, Expired, and Stopped Deployments**.
- Displays **Fixlet Compliance** data, indicating the percentage of compliant devices.
- Provides **Deployment Progress Data**, allowing users to track the success of the current deployment.
- **Overview:** Displays real-time data to monitor Fixlet Compliance and Deployment Progress.
- **Composition:** Shows the composition of the results.
- **Subscription definition:** Shows the dynamic filter conditions that you have defined to subscribe devices to the Fixlet Stream.
- **Properties:** Displays critical information about the Fixlet Stream such as its category, ID, severity.
- **Fixlets:** Lists all the applicable Fixlets along with some critical information about the Fixlets in a grid.
- **Subscribed devices:** Lists all the devices that are subscribed to the Fixlet Stream along with their details in a grid.

Related information

[Troubleshooting \(on page 86\)](#)

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.

Steps to Create a Fixlet Stream

1. Open the Create Fixlet Stream Widget

- On the Fixlet Streams page, click the **Create Fixlet Stream** to open the "Create Fixlet Stream" widget.

2. **Properties:** Define the name and description for the Fixlet stream and click **Next**.
3. **Fixlets:** Select Fixlets for the Fixlet stream by using the conditions.
 - a. Select the Operating System: Mandatory. Click on the **Select Operating Systems** dropdown and choose one or more operating systems and versions from the available options in the tree view. You can add or remove the selected OS choices.
4. **Configure Fixlet Conditions**
 - Click the **Property** dropdown to choose an attribute and define a condition for the Fixlet stream. For each attribute, specify a condition and add values. You can define multiple conditions. The **Attribute** dropdown dynamically displays the attributes available to you.
 - **CVE:** Filters Fixlets based on the associated Common Vulnerabilities and Exposures (CVE) ID. Use this property to target specific security vulnerabilities.
 - **Category:** Filters Fixlets by their classification type (for example, Audit, Bug Fix Advisory, Critical Update, Configuration, or Definition Update). Select one or more categories to include only those types of Fixlets in the stream. Use Select all to include all categories or Reset to clear your selection.
 - **Name:** Select the "contains" or "not contains" condition and for the value, enter your string, and click **Apply** button. This displays all the strings that you have entered.

- **Severity:** Select the "in" or "not in" condition; for the value, choose the level of severity for the Fixlet stream. Modify selection by adding or removing as required.
- **Source:** Filters Fixlets based on the content provider or vendor (for example, 7-Zip, 3CX, 8x8, or other supported publishers). Select one or more sources to include only Fixlets published by those vendors in the stream. Use Select all to include all sources or Reset to clear your selection.
- Select the **Operator**.
- The **Value** text box dynamically fetches data from your database for you to select.
 - **CVE:** Add relevant CVEs to the stream by typing them and click **Add**.

**Note:**

- To enter multiple CVE entries at once, you can copy paste a list of CVEs separated by comma, semicolon or a space. For example: CVE-123-1234,CVE-123-1256, CVE-123-1278
 - View All button is displayed when there are more than eight CVE values. Click the **View All** button to view the list in detail, review, search, or remove a specific CVE.
- 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.
 - Once the conditions are defined, click **Next** to proceed.

5. Devices

- [Define device filters \(on page 82\)](#) by selecting attributes, conditions, and values to determine which devices need to be included in the Fixlet stream.
- Click **Next** to continue.

6. Review Summary and Create

- The **Summary** page displays all the details that you have configured for your Fixlet stream.
- Provide a meaningful name for your Fixlet stream, review the summary, and click **Create**.
- Upon creation, the custom Fixlet stream appears at the top of your list with the icon **Custom Fixlet Stream** to distinguish it from built-in Fixlet streams.

7. Edit Fixlet Stream

- To adjust conditions, click on your custom Fixlet stream card to access the [Fixlet details page \(on page 84\)](#) and edit any attribute settings as needed.

Related information

[Troubleshooting \(on page 86\)](#)

[Common use cases \(on page 87\)](#)

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.

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.

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

[Setting up Fixlet Streams \(on page 80\)](#)

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.

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.

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

[Setting up Fixlet Streams \(on page 80\)](#)

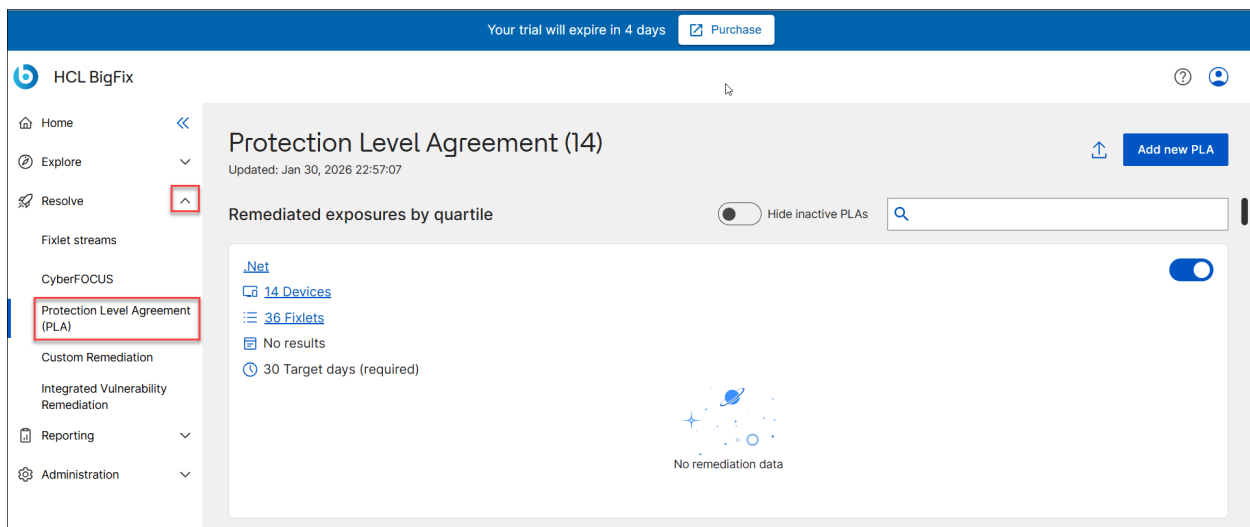
Protection Level Agreement (PLA)

Protection Level Agreements are a set of baselines that combine device contexts, and desired patch levels and compliance standards for a given set of Fixlets against agreed-to organisational service levels by key stakeholders including IT, Security, and the overall organization.

With PLAs, organizations can ensure consistent and enforceable security measures for devices by making informed business decisions to reduce risk.

How to access PLA report

To view the PLA report in the BigFix SaaS application, from the left pane expand **Resolve** and select **Protection Level Agreement**.



What PLAs show

The **25% quartile (25th percentile), median, and 75% quartile (75th percentile)** of PLAs provide actionable insights into the update cadence of devices. By analyzing these metrics, users can prioritize remediation, track progress, set and manage goals, and allocate resources effectively.

Median

- This is the middle value of a dataset when all data points are arranged in ascending order.
- It represents the **typical or average performance level**, splitting the dataset into two equal halves:

- 50% of the endpoints perform below this value.
- 50% of the endpoints perform above this value.
- For example: If the median remediation time is 4 days, it means half of the vulnerabilities are remediated in 4 days or fewer, and the other half take longer than 4 days.

25% Quartile (Lower Quartile)

- This is the value below which 25% of the data lies.
- It represents the shorter remediation timelines, showing the endpoints or vulnerabilities remediated quickly.
- **Example:** If the 25% quartile is 3 days, it means that 25% of remediations are completed within 3 days.

75% Quartile (Upper Quartile)

- This is the value below which 75% of the data lies.
- It reflects the majority of remediation timelines, showing the endpoints or vulnerabilities remediated with longer timelines.
- **Example:** If the 75% quartile is 8 days, it means that 75% of the remediations are completed in 8 days or fewer, while the remaining 25% take longer than 8 days.

Example in a PLA context

Assume a PLA report analyzes the **patch compliance** of 1,000 endpoints. The results might look like this:

- **25% Quartile:** 3 days (25% of remediations are completed within 3 days)
- **Median:** 4 days (50% of remediations are completed in 4 days or fewer)
- **75% Quartile (Q3):** 8 days (75% of remediations are completed within 8 days)

These statistics provide a comprehensive view of the distribution of remediation timelines, allowing organizations to identify trends, outliers, and areas for improvement in the remediation process.

Activating or deactivating a PLA

The **Activate/Deactivate PLA (Protection Level Agreement)** feature allows administrators to enable or disable specific security and compliance policies within a system or application. This feature provides flexibility in managing protection levels based on operational needs while ensuring compliance with security standards.

When to Activate PLA?

Activating PLA enforces security controls to protect sensitive data and maintain compliance. Consider enabling PLA in the following situations:

- **Protecting sensitive data** – Prevents unauthorized access to critical information.
- **Ensuring compliance** – Aligns with legal and regulatory requirements such as GDPR, HIPAA, or ISO 27001.
- **Mitigating security threats** – Strengthens defenses when potential vulnerabilities or attacks are detected.
- **Enforcing enterprise-wide security policies** – Standardizes protection measures across the organization.

When to Deactivate PLA?

In certain scenarios, disabling PLA may be necessary to improve performance, enable troubleshooting, or support system transitions. Consider deactivating PLA in the following cases:

- **Optimizing performance** – Reduces resource consumption in low-risk environments.
- **Conducting system maintenance or debugging** – Temporarily removes security restrictions for troubleshooting.

- **Supporting non-production environments** – Allows flexible testing and development without strict security controls.
- **Transitioning to a new security framework** – Simplifies policy adjustments during system upgrades or migrations.

How to activate or deactivate a PLA

You can activate or deactivate a PLA using either of the following methods:

1. **From the PLA List:** Toggle the activation button next to the PLA to enable or disable it directly from the list view, or
2. **From the PLA Details Page:** Click on a PLA to open its details page, then use the activation toggle to enable or disable it.

View all or hide inactive PLAs

This feature enhances visibility and management by allowing users to toggle between viewing all PLAs or filtering out inactive ones.

-  **View all PLAs** – Displays both active and inactive PLAs.
-  **Hide inactive PLAs** – Filters out deactivated PLAs, allowing administrators to focus only on currently enforced security and compliance policies.

Custom PLA report

A custom PLA is a user-defined report that helps organizations implement a proactive patching strategy while ensuring compliance and security align with their specific needs. For instructions on creating and editing a custom PLA, refer to [Custom PLA \(on page 92\)](#).

Export PLA report

Users can export the PLA report as a CSV or excel file. For more information, refer to [Exporting Data \(on page 11\)](#).

Insights gained from the PLA report

- **Device Vulnerability Distribution:**
 - Spot devices with minimal vulnerabilities, showing those that are remediated relatively quickly (remediations completed in 3 days or fewer).
 - Understand the typical state of devices in the environment, reflecting the average remediation time (remediations typically closed in 4 days).
 - Identify clusters of devices with high vulnerability counts, indicating devices that are not being remediated quickly (remediations taking longer than 8 days).
- **Vulnerability Trends:**
 - Compare the quartiles over time to see if the security posture is improving or deteriorating, with a focus on whether the median and upper quartile remediation times are decreasing, and the lower quartile is showing improvement.
 - Highlight areas needing urgent attention (for example, devices consistently taking longer than 8 days for remediation).
- **Performance Gaps:**

Analyze the disparity between the 25% and 75% quartiles to measure variability in device security.

- A **smaller gap** suggests consistent security across devices, with remediations being resolved in a similar time frame.
- A **larger gap** indicates uneven protection levels, with some devices being addressed quickly, while others take longer to remediate.

Decisions a user can make using the PLA report

1. Prioritize Remediation Efforts:

- Focus first on the highest risk devices (devices with remediation times longer than 8 days).
- Allocate resources effectively by targeting the most vulnerable devices that take the longest to remediate.

2. Set Realistic Security Goals:

- Use the **median** to establish achievable remediation baselines for the organization (for example, 50% of devices remediated within 4 days).
- Gradually aim to shift more devices towards the **75% quartile** for better overall security (for example, reducing the number of devices that take longer than 8 days to remediate).

3. Monitor Progress and Effectiveness:

- Track changes in quartile metrics over time to measure the impact of patching, configuration changes, or other security measures.
- Use the report to validate whether security initiatives are improving the posture of the devices, ensuring remediation times are reduced.

4. Segment and Tailor Strategies:

- Use the quartiles to segment devices by performance levels and apply different strategies to each group:
 - **Low performers:** Intensive remediation and stricter monitoring to quickly address vulnerabilities.
 - **Median performers:** Routine updates and maintenance to ensure continued compliance.
 - **High performers:** Focus on maintaining compliance and ensuring ongoing protection.

5. Identify Outliers and Exceptions:

- Spot devices significantly outside the normal range (for example, remediation times lower than 3 days or above 8 days) and investigate unusual patterns.
- Determine if certain device types, configurations, or departments consistently under perform and require focused attention.

6. Justify Resource Allocation and Investments:

- Present quartile data to stakeholders to justify funding for tools, staff, or processes that improve endpoint security.

Custom PLA

A Custom PLA is a user-defined PLA report that help organizations maintain a proactive patching strategy while ensuring compliance and security are tailored to their specific needs.

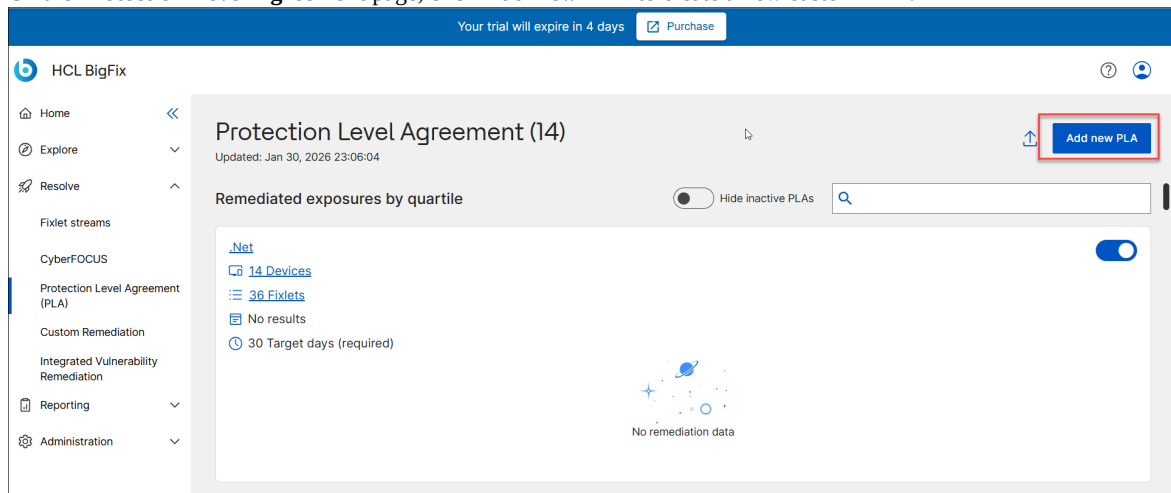
Custom PLAs provide:

- **Flexibility:** Allows organizations to define patching policies based on their security and compliance needs.
- **Granular Control:** Enables selection of patches based on CVE, category, vendor, and severity.
- **Targeted Deployment:** Ensures patches are applied only to relevant devices by using specific rules.
- **Optimized Compliance Management:** Custom time frames for patch application ensure alignment with internal policies.

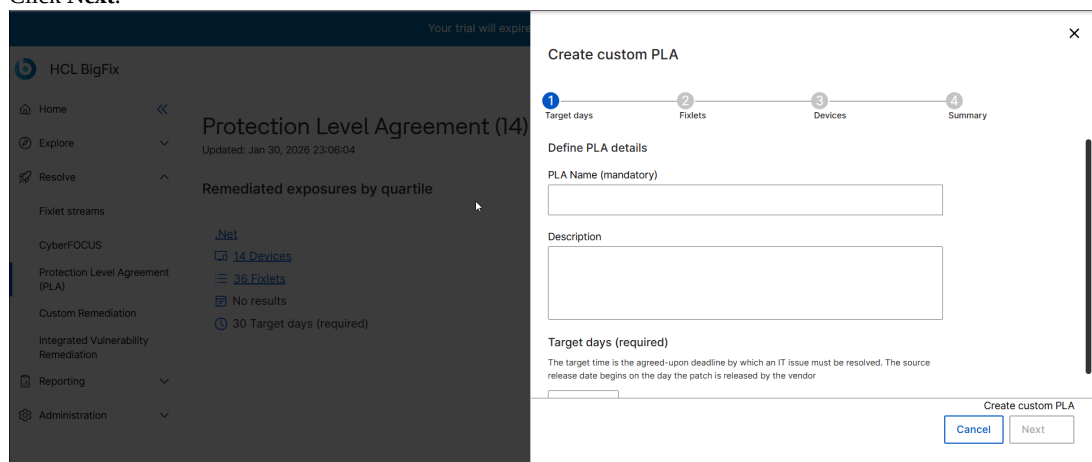
Creating custom PLA

To create a new custom PLA, complete these steps:

1. On the **Protection Level Agreement** page, click **Add New PLA** to create a new custom PLA.



2. The **Create Custom PLA** wizard appears. Complete the following steps:
 - a. Enter a name and description for the PLA.
 - b. Specify the target days.
 - c. Click **Next**.



3. Define the Fixlets Criteria:
 - a. Select an Operating System
 - b. You can group Fixlets that match conditions based on the following parameters:
 - **Property:** Fixlet attributes like CVE, category, Name, Severity, and Source.
 - **Operator:** Criteria such as *in* and *not in*.
 - **Value:** The specific value for the condition.
 - c. **Single condition:** Allows you to define parameters for one condition.
 - d. **Multiple condition (AND):** Allows you to define multiple conditions and filters Fixlets that match all the defined conditions. You can add multiple conditions, to ensure that they reflect the criteria relevant to your deployment needs.
 - e. **Multiple condition (OR):** Allows you to define multiple conditions and filters Fixlets that match at least one condition that qualify.
 - f. Preview selected Fixlets to ensure the correct ones are selected.
 - g. Click **Next**.
4. Define target devices

- a. Filter target devices using rule-based conditions through **Filter by Query** or **Filter by device list**.
 - i. **Filter by Query:**
 1. [Define device filters \(on page 82\)](#) by selecting attributes, conditions, and values to determine which devices need to be included.
 2. Review the filtered target devices under **Preview of dynamically applicable targeted devices**.
 - ii. **Filter by device list:**
 1. You can manually enter one or more device names, device IDs, FQDNs, or IP addresses to select as targets.
 2. Click  **Verify List** to review the filtered target devices.
- b. Click **Next**.
5. Review the **PLA Name, Description, Fixlet Criteria, Devices Criteria** and modify if needed before finalizing.
6. Click **Create** to create the custom PLA.
7. A success message is displayed. Click **Done**.

The custom PLA will be stored on the server and listed on the **Protection Level Agreement** page. Custom PLAs are not activated by default. [Activate \(on page 90\)](#) the PLA as needed.

Editing Custom PLA

 **Important:** You can edit only custom PLAs. System-defined PLAs cannot be edited.

1. From the **Protection Level Agreement** page, click on a custom PLA that you want to edit.
2. **Deactivate custom PLA:** If the custom PLA is [activate \(on page 90\)](#), you must deactivate before making changes.
3. Click **Edit**.
4. **Modify PLA Details:** You can update description of the PLA, target days, Fixlet selection, and target device selection as needed.



Note: You cannot rename a custom PLA. To use a different name, create a new custom PLA

5. **Review:** Carefully review the **Summary**, then click **Update > Done**. The changes will be reflected on the Protection Level Agreement page.
6. **Reactivate PLA:** Once edits are complete, [reactivate \(on page 90\)](#) the PLA to enforce the updated PLA.

Deleting Custom PLA

 **Important:** You can delete only custom PLAs. System-defined PLAs cannot be deleted.

1. From the **Protection Level Agreement** page, click on a custom PLA that you want to delete.
2. From the details page on the right side, click **Delete**.



CAUTION: The action cannot be undone. All associated data will be permanently deleted.

3. Click **Delete** to confirm. The custom PLA will be permanently deleted.

All Reports

The All Reports page provides a central location to view, manage, and organize all reports available in BigFix SaaS. From this page, you can apply filters, delete reports, and manage report visibility. You can also mark reports as Favorites.

To access the **All reports** page, expand **Reporting** from the side navigation, and then select **All reports**.

Your trial will expire in 75 days [Purchase](#)

HCL BigFix
?
👤

Home
<<

Explore

Devices

Fixlets

Deployments

Analyses

Resolve

Reporting

Administration

All Reports

Columns

Density

Delete

0 of 91 Reports

	☐ Favorites	Report Name	App	Owner	Visibility	
1	☐ ☆	Test_61721	Fixlet Streams	Steve Irwin	Public	5
2	☐ ☆	Test_67149	Fixlet Streams	Steve Irwin	Private	5
3	☐ ☆	Test_82928	Unknown app	Steve Irwin	Public	5
4	☐ ☆	Test_97299	Fixlet Streams	Steve Irwin	Public	5
5	☐ ☆	Test_16123	Fixlet Streams	Steve Irwin	Public	5

The All Reports table contains the following sections and controls:

- **Favorites** – You can toggle the favorite status on or off as needed.
- **Report Name** – The title of the report.
- **App** – The BigFix SaaS application associated with the report.
- **Owner** – The user who created the report.
- **Visibility** – Indicates whether the report is Private or Shared.
- **Last Modified** – Displays the date and time of the last update.

The toolbar above the table includes the following controls:

- **Columns** – Show or hide report columns. (This feature currently disabled)
- **Density** – Adjust the table view between compact or comfortable. (This feature currently disabled)
- **Delete** – Remove selected reports.



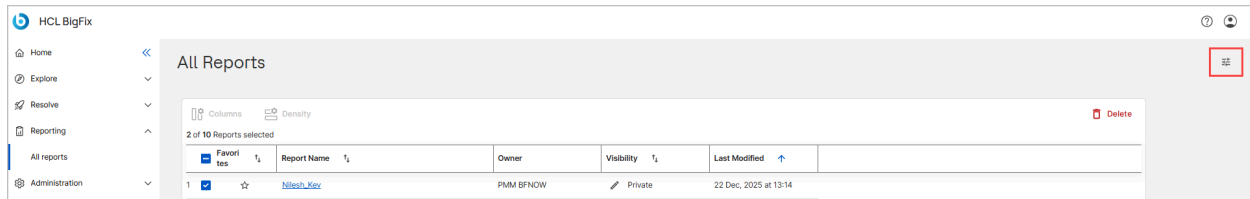
Note: These options are inactive until you select one or more reports.

Filtering Reports

The Filter option allows you to narrow down the reports displayed in the All Reports page. You can apply single or multiple conditions using logical operators (AND/OR). Available filter properties include:

- Favorites
- Report Name
- Visibility

This feature helps you quickly locate reports based on specific criteria. For detailed steps, see Filtering Data in [Common Functionalities \(on page 10\)](#).



Edit a Saved Report

Follow the steps below to edit an existing report:

1. Go to **Reporting > All Reports**.
2. Click on the report you want to edit.
3. Once the report opens, click **Manage Report**.
4. Make the required changes.
5. Click **Save** to apply your updates.

How Edits are Saved Based on Ownership

The system handles report edits differently depending on who owns the report.

If you are the report owner:

- The original report is updated with your changes.
- No duplicate report is created.

If you are not the report owner:

- The original report remains unchanged.
- The system creates a new copy of the report.
- Your changes are saved in the copied report.

This ownership-based behavior ensures that original reports are not accidentally modified by other users.

Migrate

The Agent Migration feature allows you to seamlessly migrate your devices from BigFix on-premises to BigFix SaaS. This process utilizes a universal Fixlet for deployment and allows users to track the migration status through the migration dashboard.

Supported Platforms

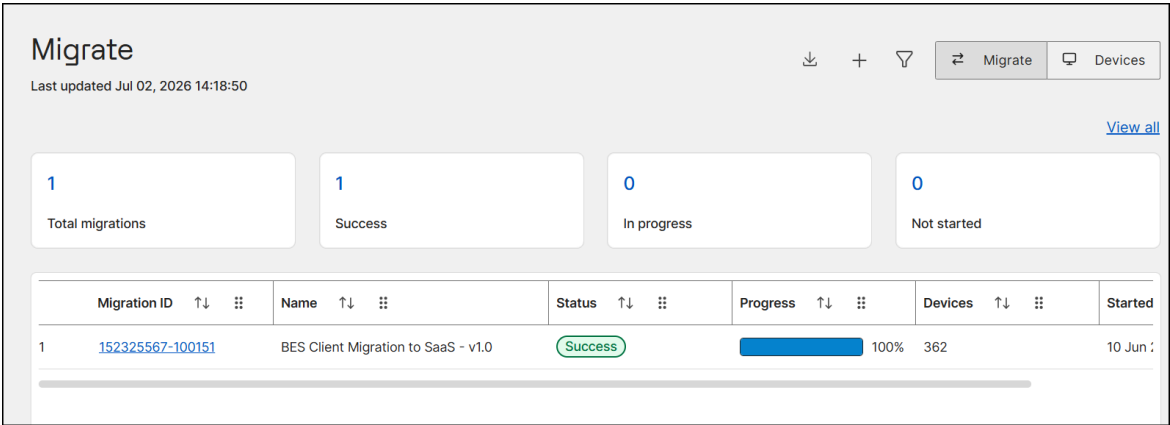
The migration supports a wide range of operating systems, including:

- Windows
- RHEL
- Ubuntu
- Mac OS
- Debian
- Amazon Linux 2
- Amazon Linux 2023
- CentOS

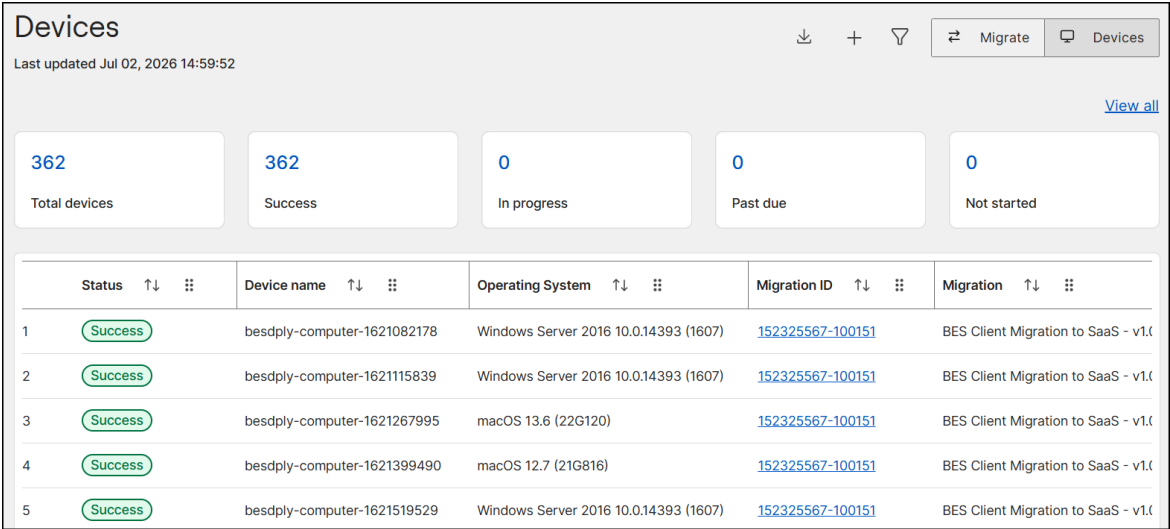
Migration Metrics Dashboard

The Migration Metrics Dashboard tracks the transition of your endpoints from on-premises BigFix environments to the BigFix SaaS platform. The dashboard provides two views that you switch between with the Migrate / Devices toggle at the top right:

- **Migrate view:** Lists every migration action and its overall progress.



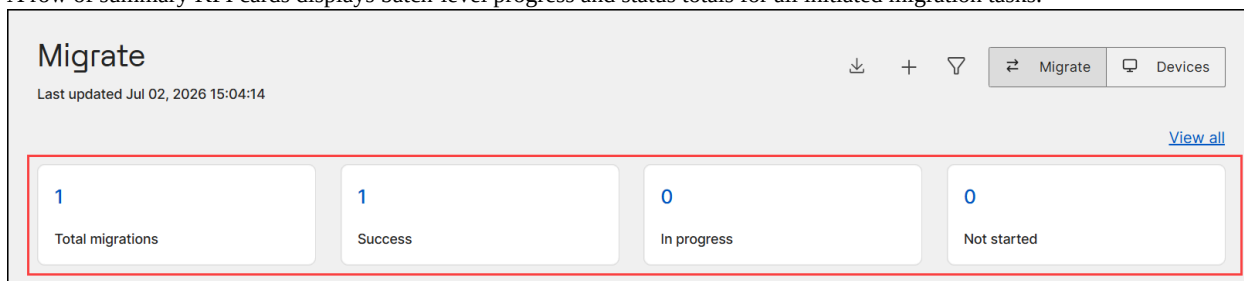
- **Devices view:** Lists every device across all migrations and the migration task to which each device belongs.



Note: The system enforces a maximum limit of 15 simultaneous migration uploads per user to ensure system stability.

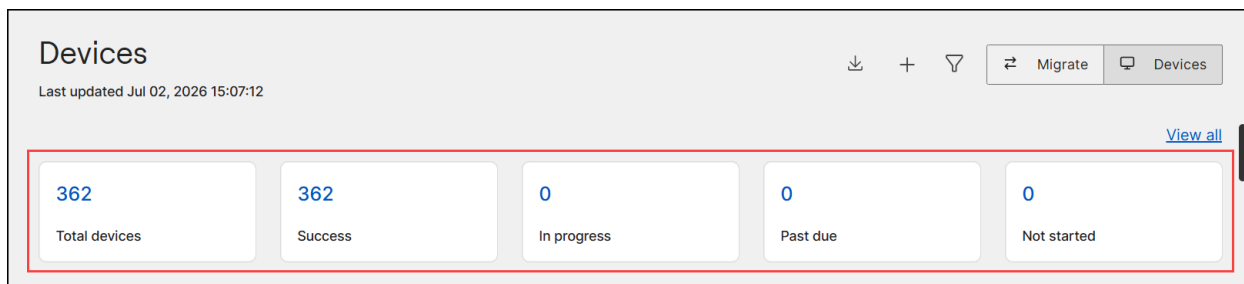
Core Metrics

A row of summary KPI cards displays batch-level progress and status totals for all initiated migration tasks.



- **Total migrations** — total number of migration actions.
- **Success** — migrations in which the targeted devices completed migration and are reporting.
- **In progress** — migrations that are currently running.
- **Not started** — migrations that have been created but have not begun reporting activity yet.

The **Devices view** and the migration detail view show device-level cards:



- **Total devices** — total number of endpoints targeted for migration.
- **Success** — devices that completed migration and are actively reporting.
- **In progress** — devices that are currently running the migration Fixlet.
- **Past due** — devices that did not complete migration before the migration's end date passed. You set this end date when you create the migration in the on-premises console; after that date, any device that has not reported a successful migration is marked past due. A device is typically past due because it was powered off, went offline, or hit a technical error mid-process and did not check back in with the SaaS console. Use this count to find machines to investigate, extend deadlines for, or re-trigger.
- **Not started** — devices that are targeted but have not yet begun the migration Fixlet.

Migration list (Migrate view)

The Migrate view lists each migration in a sortable table with these columns:

Column	Description
Migration ID	Unique identifier for the migration. Select it to open the migration detail view.
Name	Name of the migration action.
Status	Overall status of the migration (for example, Success or Past due).
Progress	Completion bar and percentage for the migration.
Devices	Number of devices targeted by the migration.
Started	Date and time the migration started.

Devices list (Devices view)

The Devices view lists every device across all migrations, with these columns:

Column	Description
Status	Migration status of the device.
Device name	Name of the endpoint.
Operating System	Operating system and build of the endpoint.
Migration ID	Migration the device belongs to. This column is new in the Devices view. Select it to open the migration detail view.
Migration	Name of the migration the device belongs to.
Last report	Date and time the device last reported to the server.

Migration detail view

From either the **Migrate** or **Devices** view, select a **Migration ID** to open the Migration Details page. This page displays summary metrics and a device data table (**Status**, **Device name**, **Operating System**, **Last report**) filtered specifically for that migration.

The breadcrumb link at the top returns you to the list you came from: it reads Migrate when you open the detail view from the Migrate view, and Devices when you open it from the Devices view. Both lead to the same migration data.

The detail view supports Key Performance Indicator (KPI) cards, the View all link, column sorting, and the Remove migration monitor action. Filters are not available on the detail view.



Note:

- If no data has been imported, the dashboard shows a **No Data Available** state and all counters remain at 0.
- Pagination controls appear when the number of records exceeds 100.
- After the migration file is uploaded, the **Last report time** field is blank. The field is populated only after the device has been successfully migrated and reports to the server.

Migration Dashboard Controls

- **Start migration (on page 100)** – Opens the migration work flow to create a new migration.
- **Add Migration Monitor (on page 101)** – Adds a new migration monitor to the dashboard.
- **Filter** – Filters the dashboard view based on the selected criteria.
- **Migrate / Devices** toggle – switches between the migration list and the device list.
- **View All / View Less** – Expands or collapses the dashboard metrics to show all or a summarized view.

Frequently Asked Questions

- **Q: What is the maximum number of devices I can migrate in one action?**
 - **A:** Each migration action is limited to a maximum of 10,000 devices.
- **Q: Will the root server or relays be migrated?**
 - **A:** No, the migration Fixlet's relevance criteria are specifically designed to exclude relays and servers from being applicable for migration.
- **Q: How long does the migration take for my devices to report status?**
 - **A:** Online devices are expected to report their status approximately 10 minutes after deployment. The total process for online devices is expected to take at least 10 minutes.
 - **Device Limit:** Each migration action is limited to a maximum of **10,000 devices**.
- **Q: Can I delete a migration after it has been created?**
 - **A:** Yes. Open the migration detail view (select a Migration ID from the Migrate or Devices view) and select Remove migration monitor. This removes the migration and all of its devices from the dashboard, and updates the KPI cards: the total migrations count decreases by one, and the total devices count decreases by that

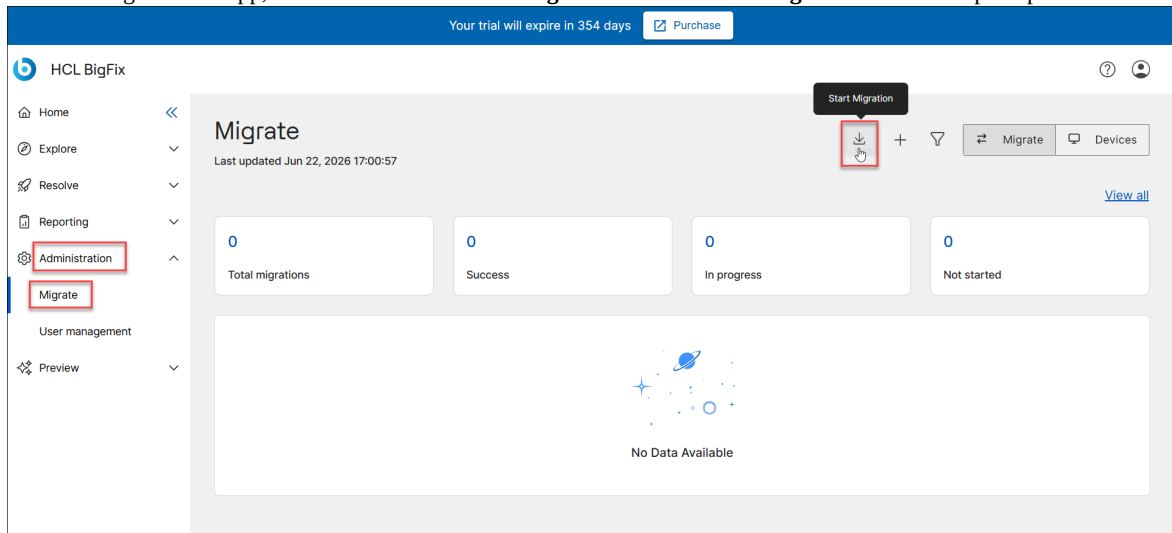
migration's device count. You remove one migration at a time; there is no multi-select. The action takes effect immediately, with no confirmation prompt, and returns you to the dashboard. For details, see [Remove Migration Monitor \(on page 102\)](#).

Start migration

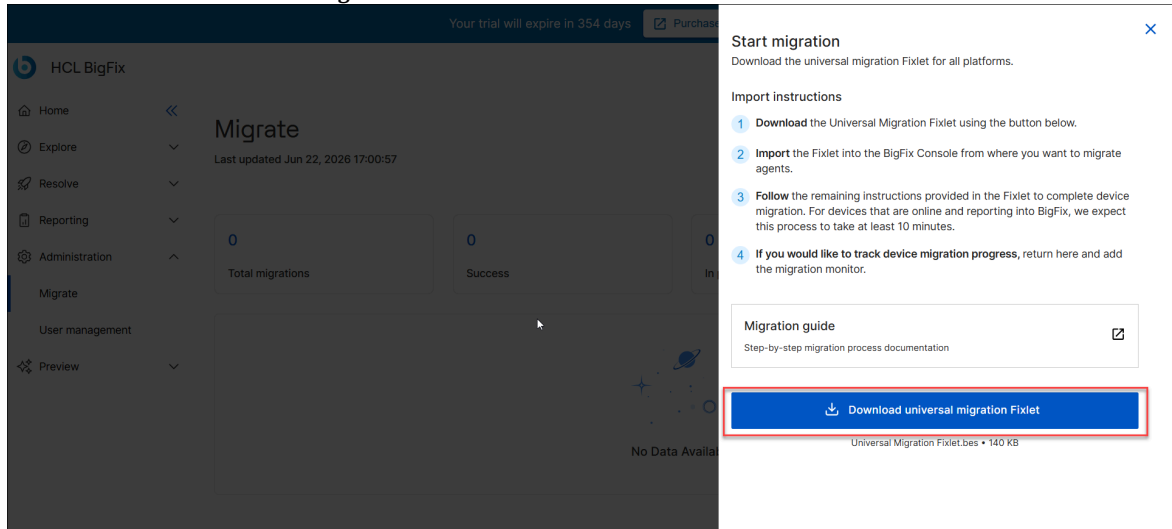
BigFix on-premises to SaaS migration is performed using the **Universal Migration Fixlet**, which deploys the migration tool to your on-premises endpoints. Click **Start Migration** to launch a guided, step-by-step work flow for downloading and deploying the Universal Migration Fixlet to your on-premises endpoints.

To initiate device migration, follow these steps:

1. From the BigFix SaaS app, select **Administration > Migrate**. Click the **Start migration** button to open up the wizard.



2. Click the **Download universal migration Fixlet** button.



- **File Name:** Universal Migration Fixlet.bes (about 140 KB)
- This universal Fixlet supports all available operating systems.

3. Import the downloaded .bes file into the on-premises BigFix Console to migrate your existing agents.

4. Deploy and Target Devices:

- Follow the embedded instructions in the Universal Migration Fixlet description to execute the migration.

Add Migration Monitor

Add migration monitor allows you to track and monitor your device migration progress by importing data directly from your on-premises BigFix Console. To track migration progress, select **Add migration monitor**.

You must export a migration monitor file from BigFix Console and upload it to the BigFix SaaS Migrate app to track real-time progress. To export data from BigFix Console:

1. Open on-premises BigFix Console and navigate to the Universal Migration Fixlet.
2. Right-click inside the Fixlet description and select **Reload** to refresh the data.

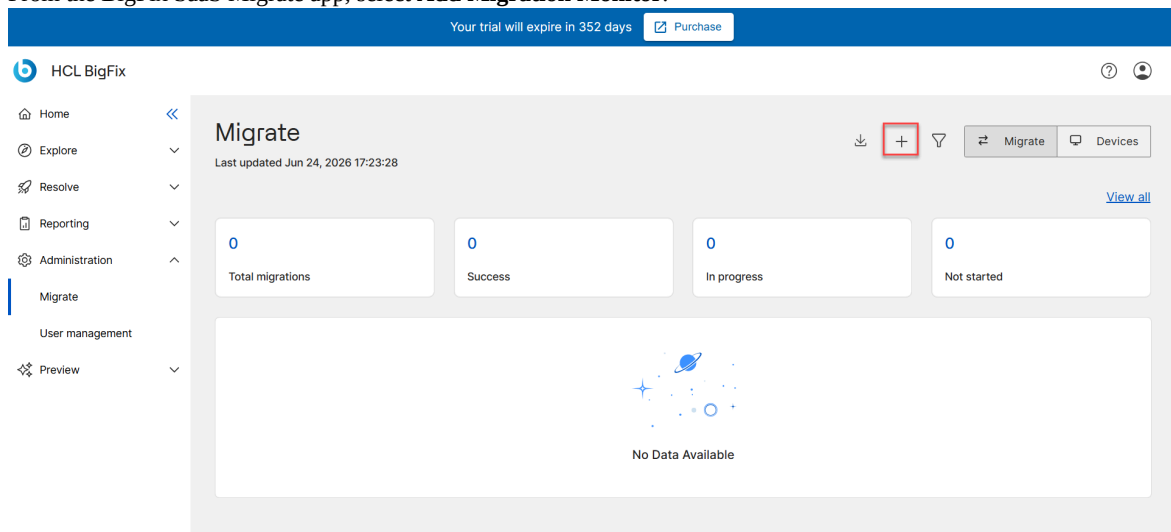


Note: If the **Reload** option is not visible, switch between the different console views (for example, Tasks, Computers, or other tree nodes). The **Reload** option then becomes available.

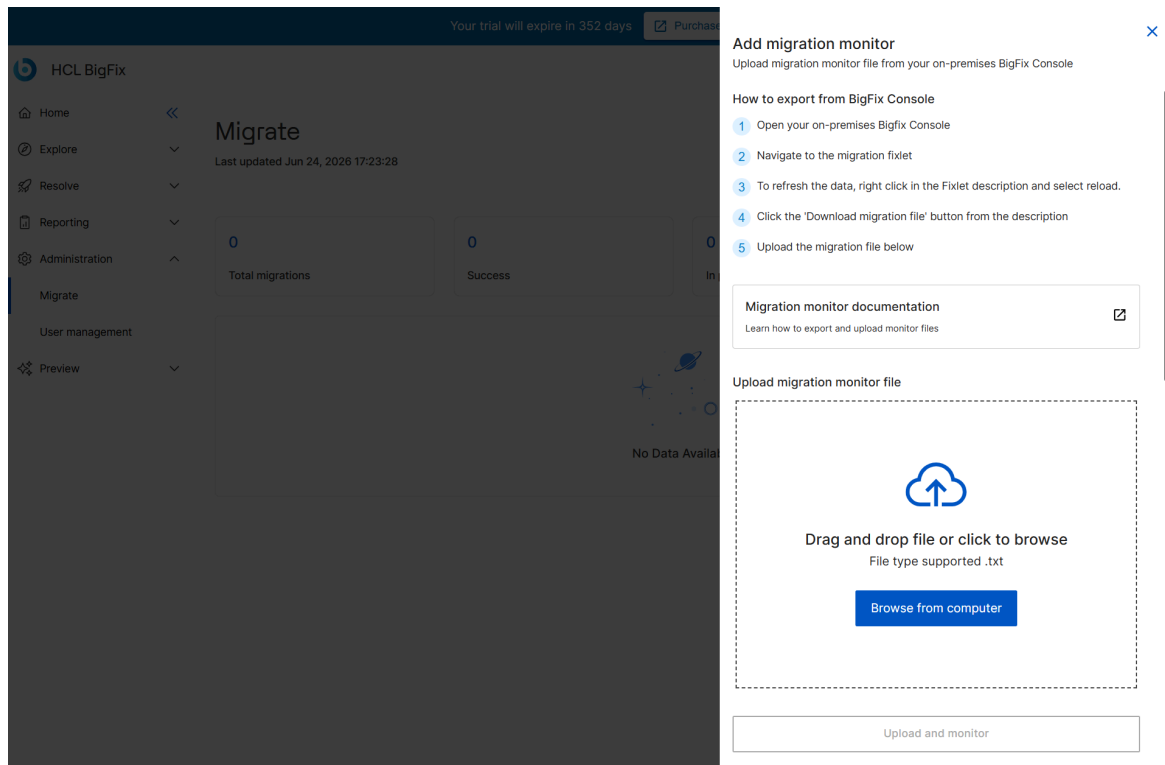
3. Select **Download migration file** within the description and save the resulting file.

To add migration monitor and track the progress of the migration:

1. From the BigFix SaaS Migrate app, select **Add Migration Monitor**.



The wizard opens up.



2. Select **Browse from computer** and upload the migration monitor file (must be a **.txt** file) downloaded from the BigFix Console. You can also drag and drop the file in that space.
3. Select **Upload and monitor** to process the data and update your migration dashboard.

**Note:**

- Online devices are expected to report their status within approximately 10 minutes after deployment.
- Action Limit: You can perform a maximum of **15 migration actions** per customer. Each migration action initiated from the console is displayed as a single migration in the BigFix SaaS UI.

Remove Migration Monitor

Remove migration monitor lets you stop tracking a migration and delete it from the **Migrate** dashboard. Removing a migration deletes the migration and its associated devices from the Devices view, and updates the dashboard metrics. You can remove one migration at a time.

You must have at least one migration on the **Migrate** dashboard. If no data has been imported, the dashboard displays a **No Data Available** state and there is nothing to remove.

Remove a migration and its device records from the dashboard when you no longer need to track them.

1. From the **Migrate** or **Devices** view, select the **Migration ID** you want to remove. The migration detail view opens.

Migrate > 152325567-10015...

152325567-100151 - BES Client Migration to SaaS - v1.0

Last updated Jul 02, 2026 13:46:30

[View all](#)

362 Total devices

362 Success

0 In progress

0 Past due

0 Not started

	Status	Device name	Operating System	Last report
1	Success	besdply-computer-1621082178	Windows Server 2016 10.0.14393 (1607)	10 Jun 2026 at 13:44:15
2	Success	besdply-computer-1621115839	Windows Server 2016 10.0.14393 (1607)	10 Jun 2026 at 13:44:15
3	Success	besdply-computer-1621267995	macOS 13.6 (22G120)	10 Jun 2026 at 13:44:15
4	Success	besdply-computer-1621399490	macOS 12.7 (21G816)	10 Jun 2026 at 13:44:15
5	Success	besdply-computer-1621519529	Windows Server 2016 10.0.14393 (1607)	10 Jun 2026 at 13:44:15

2. Select **Remove migration monitor**.

The migration and all of its devices are removed immediately, with no confirmation prompt, and you return to the dashboard. The KPI cards update: the total migrations count decreases by one, and the total devices count decreases by that migration's device count. The removed migration no longer appears in either the **Migrate** or the **Devices** view.



Note: Removing a migration monitor cannot be undone. Because there is no confirmation prompt, make sure you have selected the correct migration before you select Remove migration monitor.

User Management

The User Manager application in BigFix SaaS provides administrators with a robust interface to efficiently manage user accounts, roles, permissions, and activities in BigFix SaaS. This guide walks you through the process of creating new users, disabling or deleting existing users, setting passwords, managing roles, and more, ensuring you have a smooth and efficient experience.



Note: The User Management app is visible only to administrators. Ensure you are logged in as an administrator to access this app.

Key features

User Account Management

- **User Creation and Registration:** Admins can create and onboard new user accounts.
- **Account Status Management:** Enable, disable, or unlock user accounts to control access.
- **User Activity Insights:** Monitor login history, failed attempts, and account status.
- **User Deletion:** Permanently remove user accounts and revoke all associated access.

Role-Based Application Access

- **Role Assignment:** Assign predefined roles (example - Admin) or create custom roles to control feature access.

Authentication and Security

- **Authentication Management:** Supports multifactor authentication for enhanced security.
- **Password Enforcement:** Enforce strong password requirements, including complexity and expiration.
- **Profile and Credential Management:** Allow users to securely update personal information and passwords.

Creating and managing users

- [Creating a new user \(on page 105\)](#)
- **Details:** Click on a user to view details such as role, creation date, email, last login, and failed login attempts.
- **Disabling/enabling a user:** To disable a user, click on the disable option. If needed, re-enable a user by clicking the enable option.
- **Unlocking a user:** Restore access to users locked due to failed login attempts.
- **Deleting a user:** Permanently remove a user and revoke all access. To delete a user, disable the user first, and then proceed with deletion.

Managing user profile

- **Updating Username:** Users can update their username by clicking on the profile icon in the header and accessing the Profile Manager.
- **Updating Password:** To update the password, navigate to the Profile Manager and follow the prompts to change it.

Manage Reports

The **Reporting Feature** within User Management allows administrators and operators to filter, save, and quickly re-apply specific views of user data. This functionality is designed to be consistent with reporting features across other BigFix SaaS applications.

How to create a report

To create a new report with the current filtered view of the user list:

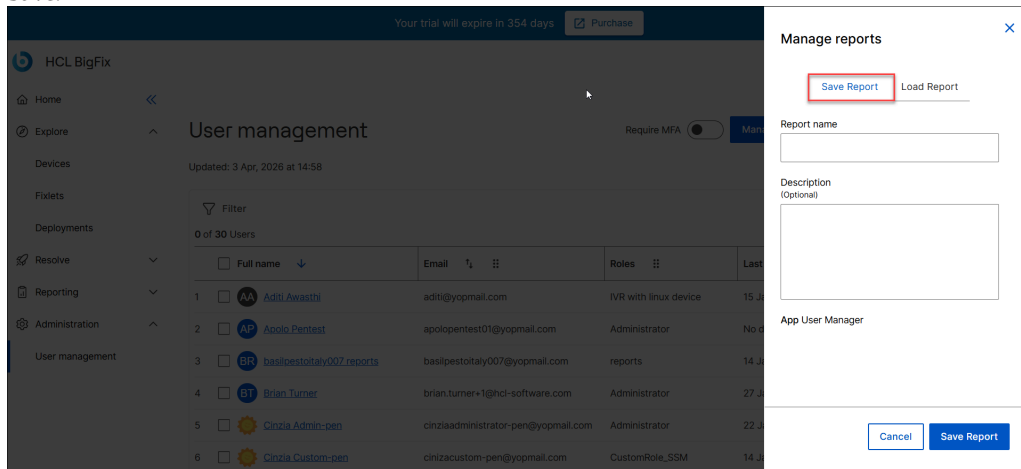
1. Apply desired criteria to the user list using the **Filter** tool.
 - For example, a filter might be used to:
 - Narrow down the user list based on a specific string in their name.
 - Isolate users based on a role, such as "administrator" status.

Identify inactive users by setting a criterion on the **Last seen** date (e.g., users not seen in the last 30 days).
2. Click **Manage Reports**.

The screenshot shows the HCL BigFix User management interface. At the top, there's a blue header with the HCL BigFix logo and a trial expiration notice. The main content area is titled 'User management' and includes a 'Require MFA' toggle and a 'Manage reports' button (highlighted with a red box). Below this, there's a 'Filter' section and a table of users. The table has columns for 'Full name', 'Email', 'Roles', 'Last seen', 'Status', and 'Last login'. The table lists 6 users, including Aditi Awasthi, Apolo Pentest, basilestoitaly007 reports, Brian Turner, Cinzia Admin-pen, and Cinzia Custom-pen.

	Full name	Email	Roles	Last seen	Status	Last login
1	Aditi Awasthi	aditi@yopmail.com	IVR with linux device	15 Jan, 2026 at 13:57	Enabled	No d.
2	Apolo Pentest	apolopentest01@yopmail.com	Administrator	No data	Enabled	No d.
3	basilestoitaly007 reports	basilestoitaly007@yopmail.com	reports	14 Jan, 2026 at 09:31	Enabled	14 Ja
4	Brian Turner	brian.turner+1@hcl-software.com	Administrator	27 Jan, 2026 at 06:18	Enabled	13 Ja
5	Cinzia Admin-pen	cinziaadministrator-pen@yopmail.com	Administrator	22 Jan, 2026 at 22:48	Enabled	No d.
6	Cinzia Custom-pen	cinziacustom-pen@yopmail.com	CustomRole_SSM	14 Jan, 2026 at 15:53	Enabled	No d.

3. On the Manage Reports page, **Save Report** tab, enter a unique name and an optional description and click **Save**.



How to view/access an existing user management report

Saved reports can be accessed as follows:

- **Within the User Management app:** Use the **Manage Reports** control in the User Management action bar, switch to **Load Report** tab, and click on an existing report to view.
- **Centralized View:** Access [All Reports \(on page 94\)](#), which is a central hub for managing reports across applications. Loading a report automatically re-applies all its saved filters.

Permissions for creating and deleting reports

- **Creation:** Any user (operator) with access to the User Management application can create and save reports.
- **Deletion:** Only the **Owner** (the user who created the report) can delete their own reports. Non-owners cannot delete reports owned by other users. Furthermore, when a user account is removed from the system, any reports owned by that user are also automatically removed.

Usage limitations

- **Role-Based Reports:** There is currently no support for generating reports based on roles.
- **Exporting Data:** Exporting saved reports is not supported due to the presence of sensitive data within User Management.

Creating a new user

Creating a new user in BigFix SaaS user management application involves a series of steps to ensure proper access and security.

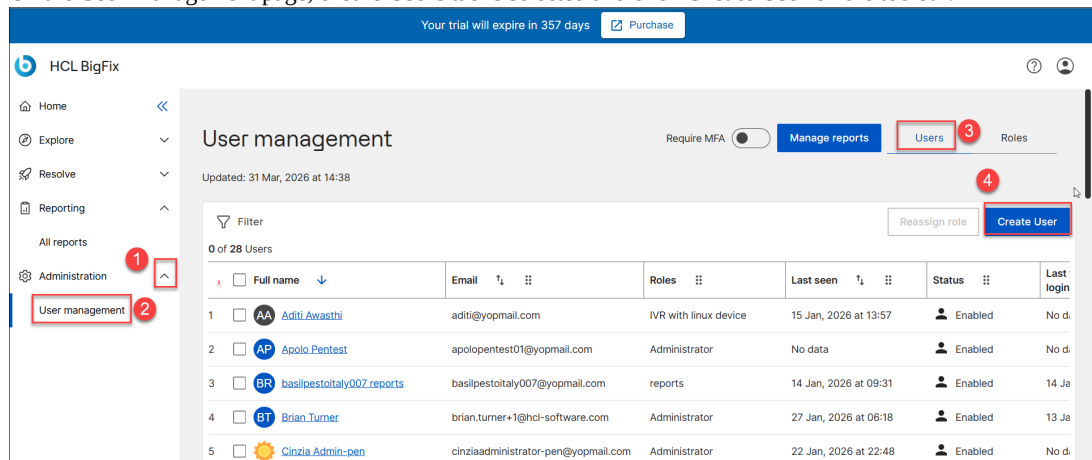
The User Management app is visible only to administrators. Ensure you are logged in as an administrator to access this app.

First, an administrator logs into the user management dashboard. From there, the admin selects the option to add a new user, which typically prompts a form requiring essential details such as the user's name, email address, and role within the organization. Once the information is submitted, BigFix sends a confirmation email to the new user with a link to login, set password, and complete the account setup. This process ensures that the new user has access to appropriate features and resources while maintaining security protocols.

To create a new user, complete the following steps:

1. Accessing the User Manager

- Log in to BigFix SaaS as an administrator.
- To navigate to the User Manager section, expand **Administration** and click **User Management**.
- On the User Management page, ensure **Users** tab is selected and click **Create User** on the toolbar.



- Entering User Information:** In the Create User popup, enter the user's first name, last name, email address, and confirm email. Click **Next**.
- Assigning Roles:** The [roles \(on page 107\)](#) determine the BigFix SaaS applications and the devices the user can access. Select a role for the user from the available list and click **Next**.
- Summary:**
 - Verify user email ID, role, and application access.
 - Read the information about welcome mail and the password security requirements.
 - Click **Create**.

User is successfully created. Upon BigFix SaaS account creation, the user receives a welcome email with the log in link and temporary password. When logging in, the user can set up a new password.

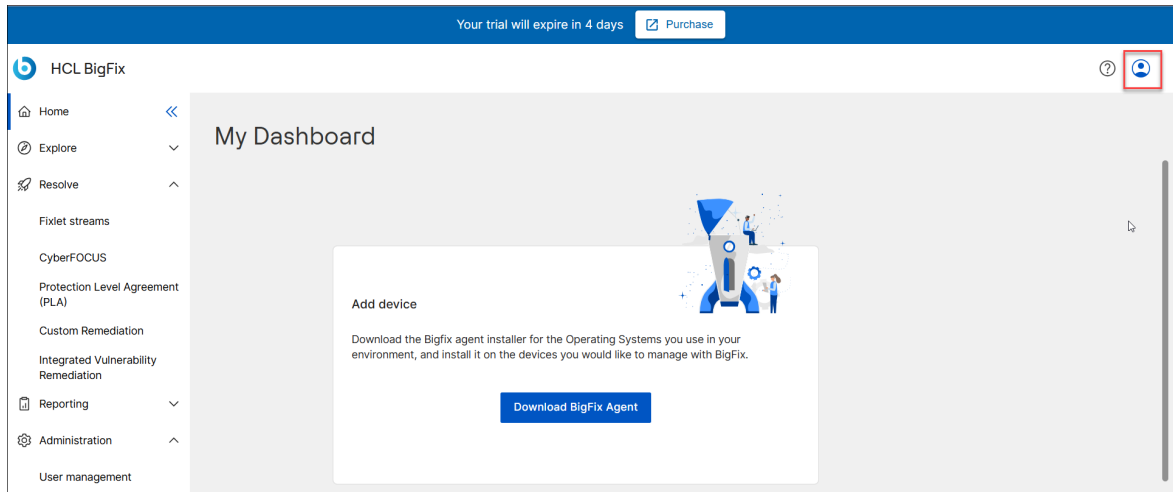
- The user receives credentials through email and can log in to BigFix SaaS application.
- When the user logs in for the first time, BigFix SaaS prompts the user to change the password. The user can set password according to the password rule, confirm new password, and click change password.
- After the password is changed, the user is redirected to the log in page. Once logged in, the dashboard is displayed.

Editing user profile

You can edit your own profile to keep your information up to date. Here's how you can easily edit your profile from the BigFix SaaS home page.

Only logged-in users can edit their own profiles. Admins do not have the capability to edit user profiles.

- Log in to BigFix SaaS with your credentials.
- On the home page, click on the user icon on the top right corner.



3. Update user's first name and last name and click **Save**.

Managing roles

Create, edit, and manage user roles with customizable access to applications in the SaaS environment. You can customize each role by specifying app-level permissions, ensuring users have secure and appropriate access based on their responsibilities.

Built-in role

A built-in role is predefined role provided by BigFix SaaS to streamline user and access management.

- **Administrator:** This role comes with default configurations and permissions that address common administrative and operational needs. Administrators have access to all available applications. They have the ability to create, delete, and edit users.



Important: The Administrator role is a built-in role that you cannot modify or delete.

Custom roles

Custom roles are user-defined roles in BigFix SaaS that allow administrators to tailor permissions and access based on specific organizational requirements. These roles provide flexibility to control which users, devices, and applications are accessible within the environment. These roles can be edited, reassigned, or deleted (if no users are assigned).

Create a custom role

Creating a custom role involves defining a user role with specific permissions and access tailored to your organization's unique requirements. Unlike built-in roles, which have fixed configurations, custom roles allow flexibility in managing devices, applications, and user assignments. For detailed steps, read [Creating a new role \(on page 108\)](#).



Note: Users can create a maximum of 20 custom user roles.

Modify a custom role

1. From the User Manager app, click **Roles**.
2. Open an existing custom role and modify the following as necessary.
 - Role name
 - Assigned apps (excluding default apps which remain fixed)
 - Assigned users

- Assigned computer groups (e.g., All Computers, Filtered Groups)
- Admin status

Example: Update a dynamic filter to refine device selection, such as filtering by **Device Properties**.

3. Save changes.



Note: Role updates affect permissions in real time after a user logs in.

Delete a custom role

You can delete a role only if:

- The role is **not assigned to any users**.
- The role is **not marked as an admin role**.

To delete a custom role:

1. Unassign all users from the role.
 2. Click **Delete**.
- If no users are assigned to a role, click the **Delete** button to remove it.

Default and Non-Removable Applications

Certain applications are marked as **default** in the backend and are automatically assigned to every role. These apps **cannot be unselected** during role creation or editing.

Examples include:

- Deployment Manager (depending on product configuration)
- Device Explorer
- Fixlet Explorer
- My Dashboard (home screen)
- Reports

Assigning a role to users

As an administrator, when creating [a new user \(on page 105\)](#), you can assign a role to ensure they have the appropriate level of access from their first login. You can reassign the roles at any time to adapt to organizational changes, evolving operational needs, and updated security policies.

To reassign users roles:

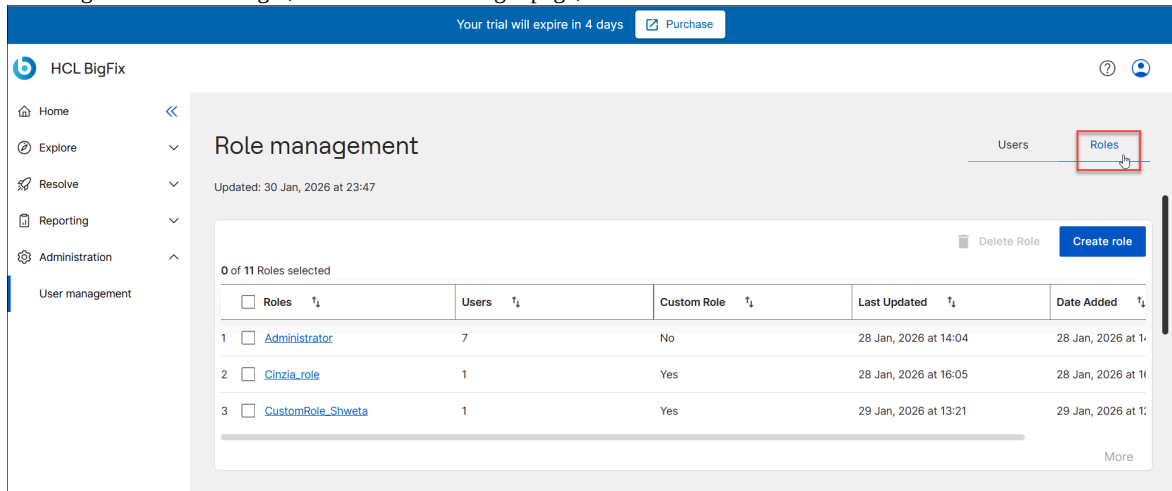
1. In the User Management section, go to the **Users** tab.
2. Select one or more users from the grid.
3. Click **Reassign** and select a new role from the available options.
4. To verify the action, from the User Manager grid, check the **Roles** column to see the associated role displayed next to the selected users.

Creating a new role

Create a custom role to define specific permissions and access tailored to your organizational needs. Assign a name, configure dynamic filters for device assignments, and specify access levels. Save the role to manage users, devices, and applications efficiently.

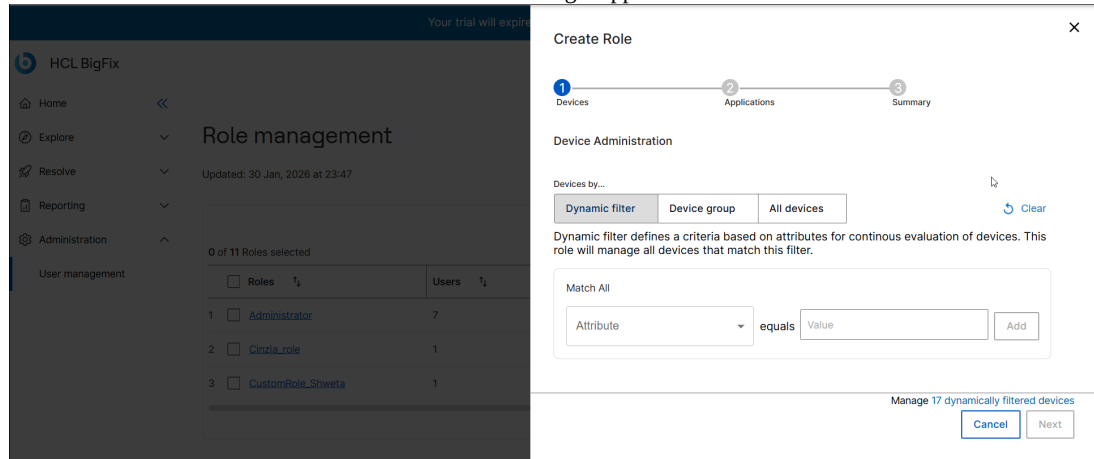
You must be an Administrator to create a new role.

1. To navigate to Role Manager, from the User Manager page, click **Roles**.



2. Create a Role

- a. Click **Create role** to add a new role. The Create Role widget appears.



- b. **Devices:** Administrators can manage device assignments for roles by setting conditions or selecting devices directly:

- **Dynamic filter:** To dynamically filter and assign devices to a role's scope:
 - i. Select an attribute to filter devices (e.g., OS Family).
 - ii. Specify the desired value for the attribute (e.g., Windows).
 - iii. Click Add to add the condition to the filter.
 - Example: The condition "**OS Family Equals Windows**" assigns all Windows devices to the role.
 - Click + **Add Condition** to define more conditions and refine the scope further, ensuring only the intended devices are included.
 - If you want to delete a condition that you have defined, click the **Delete** icon next to the condition.
 - If you want to delete all the conditions that you have defined, click **Clear**.
 - The system automatically displays the total number of devices matching your conditions.
- **# Device tag:** Manually choose specific devices by their unique IDs for targeted assignments.
- **All Devices:** Include all available devices in the scope of the role for broader access.

- c. Once the scope is set, click **Next** to proceed.

- d. **Applications:** Select applications this role should have access to.

- The list includes all available apps.
 - Hover over each app for a short description.
 - Some apps (**My Dashboard**, **Reports**, **Deployment Manager**, **Device Explorer**, **Fixlet Explorer**) are pre-selected and cannot be unselected.
- e. On the next step, enter a name for the role.



Note: Provide a unique name for the role. You cannot edit the role name once it is created.

- f. Verify the number of devices and the number of applications to access. Click **Create**. The role is successfully created. Click **OK** to exit the widget.

The new role appears on the **Role Manager** page. Click the role to view its details, including:

- **Overview:** Displays key information about the role.
- **Application Access:** Lists the applications the role can access.
- **Associated Devices:** Shows details of the devices assigned to the role.
- **Configurations:** Displays all the conditions that are defined to filter and associate to the role.

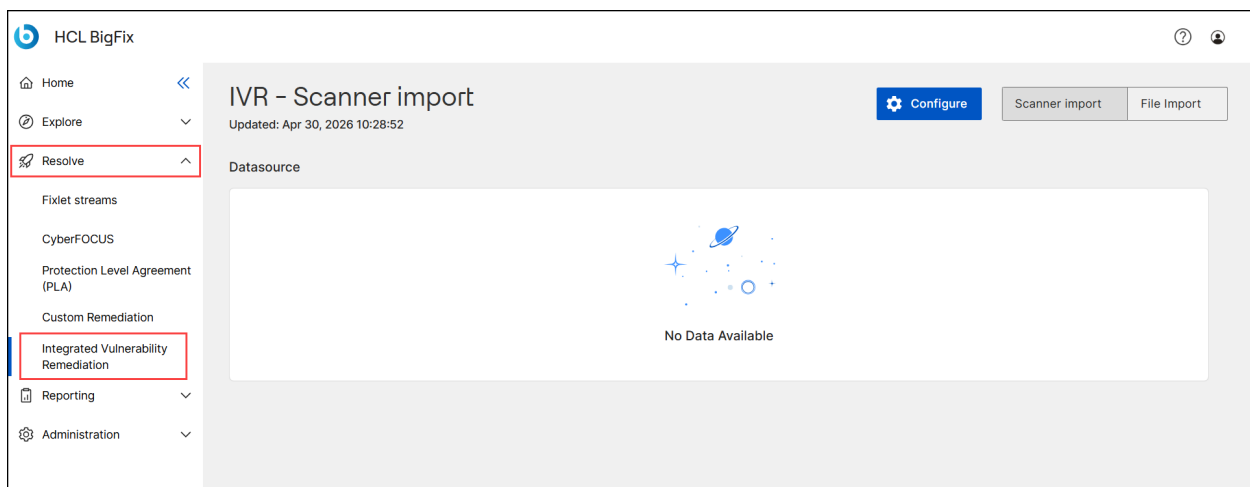
Integrated Vulnerability Remediation

Integrated Vulnerability Remediation (IVR) provides a real-time overview of security vulnerabilities categorized by severity, using both the Common Vulnerability Scoring System (CVSS) and the Vulnerability Priority Rating (VPR). Use this feature to configure data sources, visualize vulnerability data in charts, and manage individual vulnerabilities in a detailed table. You can also manually import vulnerability data from external sources using the Universal Vulnerability Ingestion (UVI) feature. You can remediate vulnerabilities directly from the dashboard and export the data.

To access the IVR dashboard from **BigFix SaaS**, go to **Resolve > Integrated Vulnerability Remediation**.



Note: The **Integrated Vulnerability Remediation** link appears in the navigation pane only if your user role includes permission to access the IVR application. If you do not see this option, contact your BigFix administrator. For more details, see [User Management \(on page 103\)](#).



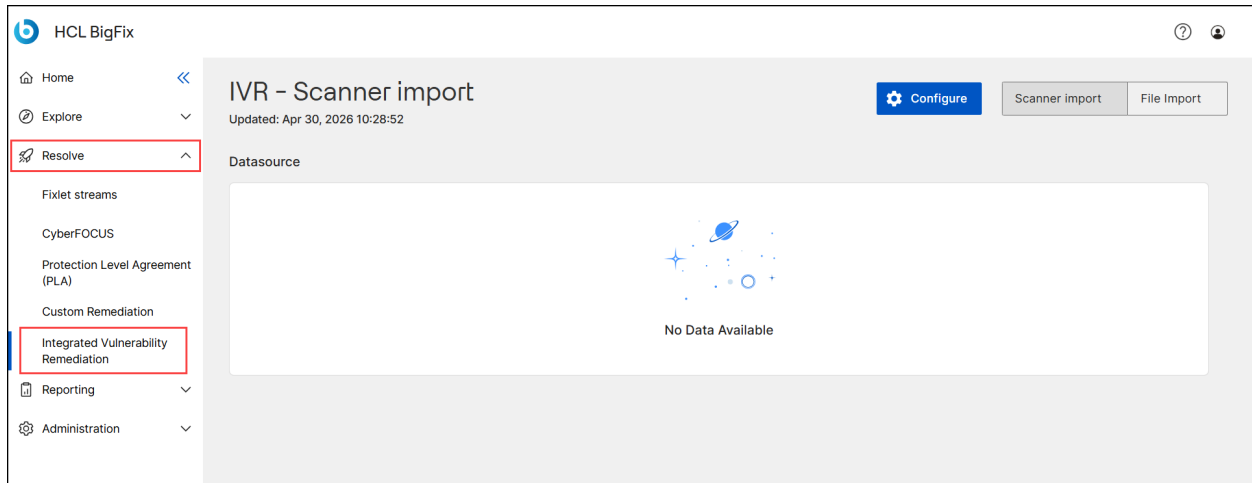
IVR Dashboard

The **Integrated Vulnerability Remediation (IVR)** dashboard provides a centralized, dynamic interface to view, analyze, and remediate vulnerabilities within your environment. The dashboard adapts to display data whether it is directly synced from external scanners (such as Tenable) or manually uploaded through CSV spreadsheets. This consolidated view supports the correlation of external scanner data with BigFix content, enabling you to efficiently process the remediation flow.

Initial Dashboard Setup and Data Synchronization

When you navigate to the IVR dashboard by expanding **Resolve** and selecting **Integrated Vulnerability Remediation** on the left navigation menu, the system automatically loads the **IVR - Scanner import** page.

If you have not yet configured a data source, the dashboard indicates that no data is available. You must establish a connection to an external vulnerability scanner (for example, Tenable) to populate the dashboard grids and charts.



You can consolidate your vulnerability data into a single view by integrating multiple scanners. For instructions on configuring initial or additional data sources, see [Creating New Datasource \(on page 127\)](#).

Once a data source is successfully configured and the initial synchronization is complete, the dashboard populates with your active vulnerability data.



Note: The system checks for newly configured data sources every 10 minutes and refreshes data from existing sources every 12 hours. To import data immediately, use the manual file import feature.

Dashboard Layout

The IVR dashboard is divided into two primary functional areas: the header section for global controls and the main workspace for data analysis and remediation.

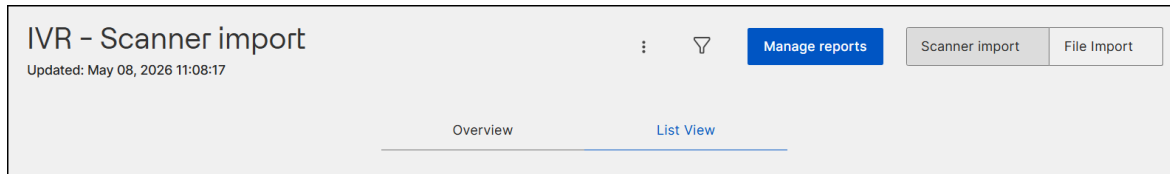
Header controls: The top section of the dashboard contains global tools to manage your overall view. The available buttons and features vary depending on whether you have a data source configured:

- **When a data source is not configured:**

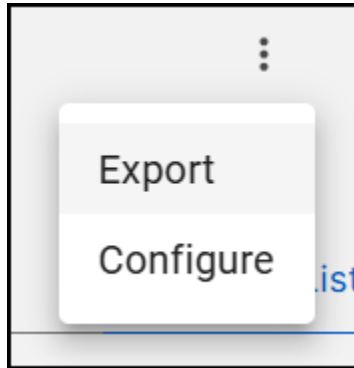


- **Configure:** Select to set up your initial vulnerability data source.
- **Scanner import and File Import toggle:** Switch between the automated scanner data view and the manual file import view.

- **When a data source is configured:**



- **Vertical Ellipsis icon (three vertical dots):** Select to reveal a menu with the following options:



- **Export:** Export the vulnerability data. The exported file is in JPEG, PNG, or PDF format for the Overview charts, and in CSV or XLSX format for the List View data.
- **Configure:** Open the configuration settings to add additional data sources.



- **Filter icon:** Select to open the Filter data widget, which allows you to set multiple levels of filtering conditions based on selected vulnerability properties. You can filter data using the following properties:

- **Tenable Vulnerability:** Filter by the specific name of the vulnerability.
- **ID:** Filter by the unique numeric identifier.
- **CVE(s):** Filter by the Common Vulnerabilities and Exposures identifiers.
- **VPR:** Filter by the Vulnerability Priority Rating score.

- **Published:** Filter by the date the vulnerability was disclosed.
- **CVSS:** Filter by the Common Vulnerability Scoring System score.

Filter data

Set conditions on properties

Select top level filter condition

☐ Single condition ☒ Multiple condition (Criteria: AND)

Condition 1

Property

Property

Operator

Operator

AND

Condition 2

Property

Tenable Vulnerability

ID

CVE(s)

VPR

Published

CVSS

Operator

Operator

+ Add Block

Remove all

Apply

- **Manage reports:** Select to open the Manage Reports widget. Use this to save your current dashboard view for quick access later, or reload a previously saved report.
 - **Save Report:** Select to save your current grid data (in List view) as a named report.

×

Manage reports

Save Report

Load Report

Report name

Description
(Optional)

App Integrated Vulnerability Remediation

Cancel

Save Report

- **Load report:** Select to view a list of all previously saved reports. Selecting a specific report loads it into the data grid (in List view).

×

Manage reports

Save Report

Load Report

VPR-critical-12-SI	11 JUN 2026	▼
234046_9_FI	11 JUN 2026	▼
18 from FI	11 JUN 2026	▼
65- SI	11 JUN 2026	▼
238080_6 - FI	11 JUN 2026	▼
Scanner_Import_Default_Report	11 JUN 2026	▼
Default_File_Import	11 JUN 2026	▼

- **Scanner import and File import toggles:** Switch between the automated scanner data view and the manual file import view.
- **Overview and List View toggles:** Switch between the visual analytics summary and the tabular list of vulnerabilities.
- **Main workspace:** The main area of the dashboard adapts its content based on your selected data context. It serves as the primary location to analyze vulnerability metrics and initiate the remediation workflow.
 - **Scanner import view:** When viewing automated scanner data, the workspace displays the content for either the **List View** tab (a detailed grid of active vulnerabilities) or the **Overview** tab (visual analytics and charts).

IVR - Scanner import
Updated: May 01, 2026 11:54:49

Overview List View

Scanner Import Summary

0 of 365 Vulnerabilities

☐ Tenable Vulnerability	ID	VPR	CVSS	CVE(s)	Published
☐ Adobe Flash Player <= 29.0.0.140 (APSB18-16)	109601	Medium	Critical	CVE-2018-4944	2018-05-08T00:00
☐ Adobe Flash Player <= 32.0.0.171 (APSB19-26)	125056	Medium	High	CVE-2019-7837	2019-05-14T00:00
☐ Adobe Flash Player <= 32.0.0.192 (APSB19-30)	125815	High	High	CVE-2019-7845;CVE-20	2019-06-11T00:00
☐ Adobe Flash Player <= 32.0.0.238 (APSB19-46)	128633	High	Critical	CVE-2019-8069;CVE-20	2019-09-10T00:00
☐ Adobe Flash Player <= 32.0.0.321 (APSB20-06)	133607	Medium	High	CVE-2020-3757	2020-02-11T00:00
☐ Adobe Flash Player <= 32.0.0.371 (APSB20-30)	137253	Medium	Critical	CVE-2020-9633	2020-06-09T00:00
☐ Adobe Flash Player <= 32.0.0.433 (APSB20-58)	141494	Medium	High	CVE-2020-9746	2020-10-16T00:00

- **File import view:** When viewing manual data, the workspace displays the **File Import Summary** tab (a grid of manually uploaded vulnerabilities) and the **Import Log** tab (historical import metrics).

IVR - File import
Updated: Jun 22, 2026 11:00:55

File Import Summary Import Log

File Import Summary

0 of 401 Vulnerabilities

☐ Vulnerabilities	ID	Severity	Severity Score	CVSS	CVE(s)	Published	Scanner Count
☐ KB5055519: Windows 10 version 1809 / Windows Sx	234046	4	10	10	CVE-2025-24073;CVE-2	2025-04-08T00:00:00Z	1
☐ KB5058392: Windows 10 version 1809 / Windows Sx	235845	4	10	10	CVE-2025-29959;CVE-2	2025-05-13T00:00:00Z	1
☐ KB5060531: Windows 10 version 1809 / Windows Sx	238080	4	10	10	CVE-2025-33050;CVE-2	2025-06-10T00:00:00Z	1
☐ KB5062557: Windows 10 version 1809 / Windows Sx	241548	2	6.8	6.8	CVE-2025-36350;CVE-2	2025-07-08T00:00:00Z	1
☐ KB5063877: Windows 10 version 1809 / Windows Sx	249130	4	10	10	CVE-2025-50155;CVE-2	2025-08-12T00:00:00Z	1
☐ KB5065428: Windows 10 version 1809 / Windows Sx	261799	4	10	10	CVE-2025-54110;CVE-2	2025-09-09T00:00:00Z	1
☐ KB5065429: Windows 10 version 21H2 / Windows 11	261804	4	10	10	CVE-2025-54099;CVE-2	2025-09-09T00:00:00Z	1
☐ KB5066586: Windows 10 version 1809 / Windows Sx	270378	3	7.5	7.5	CVE-2025-23004;CVE-2	2025-10-14T00:00:00Z	1
☐ KB5066791: Windows 10 version 21H2 / Windows 11	270379	3	7.5	7.5	CVE-2025-58722;CVE-2	2025-10-14T00:00:00Z	1

Analyzing and Remediating Vulnerability Lists

The data grids in the main workspace (**List View** for scanner imports and **File Import Summary** for manual imports) display critical identifying information about the vulnerabilities in your environment. You can interact directly with your vulnerability data from these grids.

The specific columns available depend on the data view you are currently accessing:

- **Scanner import:** When you view automated data synced from an integrated vulnerability scanner on the **List View** tab, the data grid displays the following columns:

Column Name	Data Type	Description
(Selection Checkbox)	Interactive Checkbox	A control that allows you to select one or multiple rows to perform actions (like Remediate). A master checkbox at the table header enables bulk selection.
Tenable Vulnerability	Text Link (Hyperlink)	The descriptive name of the security vulnerability as identified by the vulnerability scanner (Tenable). This text is hyperlinked, leading to more details about the specific vulnerability displayed under the following tabs: ◦ Vulnerability Information: This includes a brief summary, a detailed description, and a solution for the specific vulnerability. You can also fix the vulnerability from here by clicking Remediate and following the steps given in the IVR Remediate flow page (on page 138). ◦ Contents: It shows the Fixlets that are related to this specific vulnerability. Select a Content Name to open more details about a specific Fixlet on the Fixlet details page (on page 72). ◦ Devices: It shows the devices that the specific Fixlet can be applied to. Click on Devices to go to Device Details page (on page 47). ◦ Deployment: It shows the deployment data. To learn how to deploy the Fixlet, go to Deploying Fixlets page (on page 76).
ID	Numeric	A unique numeric identifier assigned to the specific vulnerability instance within the system for tracking and reference purposes.
VPR	Categorical Text	Vulnerability Priority Rating. A dynamic rating (e.g., Low, Medium, High) that helps prioritize remediation by combining technical severity with threat intelligence (specific to Tenable's scoring).
CVSS	Categorical Text	Common Vulnerability Scoring System. An industry-standard score (e.g., Critical, High) that reflects the intrinsic

Column Name	Data Type	Description
CVE(s)	Alphanumeric Link	sic severity of the vulnerability based on its technical characteristics. Common Vulnerabilities and Exposures. A list of standardized identifiers (e.g., CVE-2019-7837) that reference the vulnerability in the public National Vulnerability Database (NVD). These are hyperlinked for external reference.
Published	Date/Time (Timestamp)	The date and time (in ISO 8601 format) when the vulnerability was publicly disclosed or added to the database.
Tenable Count	Numeric	Displays the number of vulnerable devices identified by Tenable.

- **File import:** When you view manually uploaded data on the **File Import Summary** tab, the data grid displays the columns mapped during the Universal Vulnerability Ingestion (UVI) process:

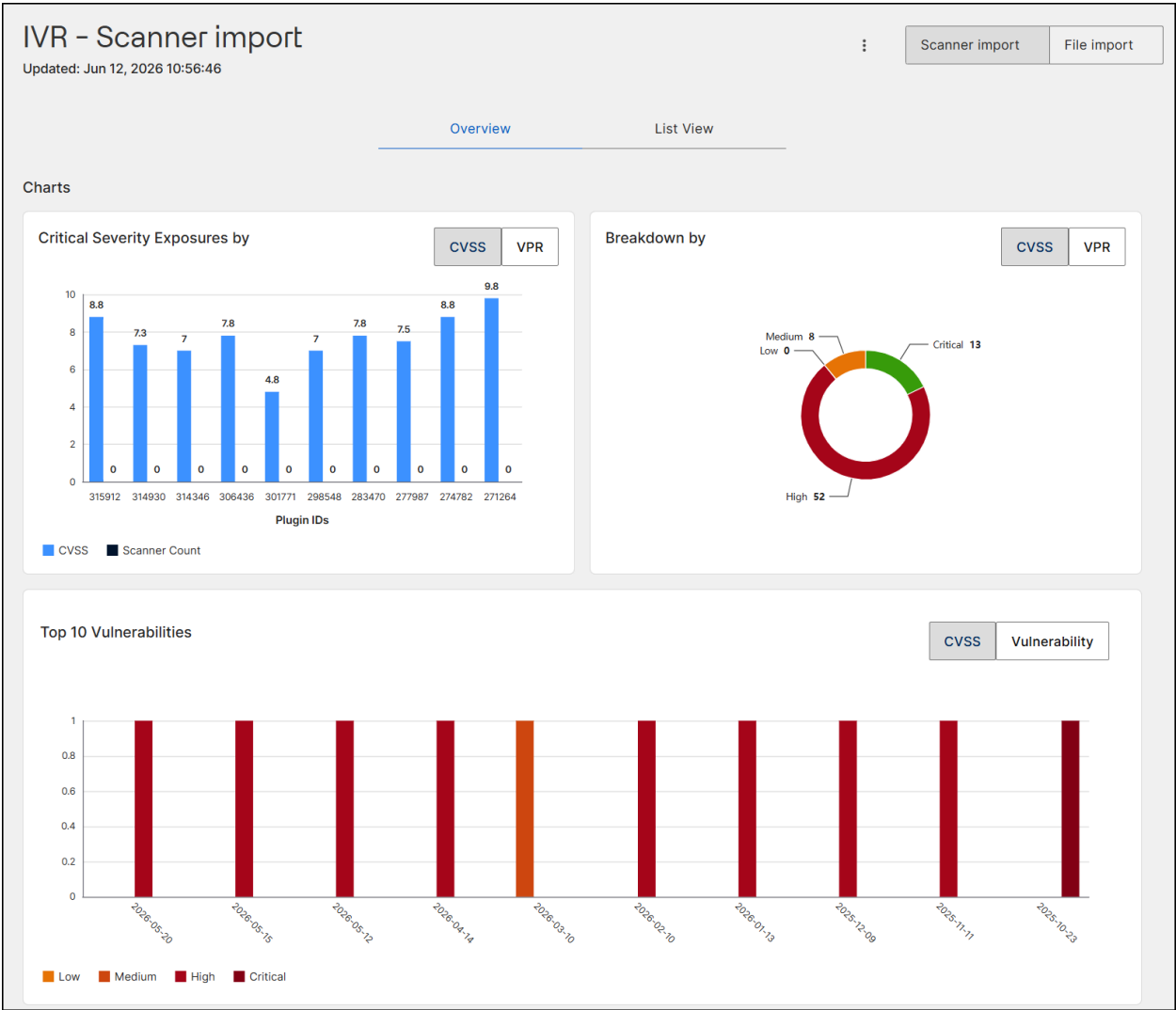
Column Name	Data Type	Description
(Selection Checkbox)	Interactive Checkbox	A control that allows you to select one or multiple rows to perform actions (like Remediate). A master checkbox at the table header enables bulk selection.
Vulnerabilities	Text Link (Hyperlink)	Displays the name or title of the vulnerability as mapped from your imported CSV file. This text is hyperlinked, leading to more details about the specific vulnerability displayed under the following tabs: ◦ Vulnerability Information: This includes a brief summary, a detailed description, and a solution for the specific vulnerability. You can also fix the vulnerability from here by clicking Remediate and following the steps given in the IVR Remediate flow page (on page 138). ◦ Contents: It shows the Fixlets that are related to this specific vulnerability. Select a Content Name to open more details about a specific Fixlet on the Fixlet details page (on page 72). ◦ Devices: It shows the devices that the specific Fixlet can be applied to. Click on Devices to go to Device Details page (on page 47). ◦ Deployment: It shows the deployment data. To learn how

Column Name	Data Type	Description
		to deploy the Fixlet, go to Deploying Fixlets page (on page 76) .
ID	Numeric	A unique numeric identifier assigned to the specific vulnerability instance within the system for tracking and reference purposes.
Severity	String	Displays the categorical severity level of the vulnerability (for example, Critical, High, Medium, or Low) based on your imported data.
Severity Score	Numeric	Displays the numerical severity score of the vulnerability based on your imported data.
CVSS	Categorical Text	Common Vulnerability Scoring System. An industry-standard score (e.g., Critical, High) that reflects the intrinsic severity of the vulnerability based on its technical characteristics.
CVE(s)	Alphanumeric Link	Common Vulnerabilities and Exposures. A list of standardized identifiers (e.g., CVE-2019-7837) that reference the vulnerability in the public National Vulnerability Database (NVD). These are hyperlinked for external reference.
Published	Date/Time (Timestamp)	The date and time (in ISO 8601 format) when the vulnerability was publicly disclosed or added to the database.
Scanner Count	Numeric	Displays the number of vulnerable devices based on your imported data.

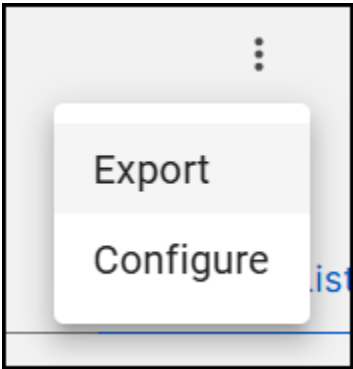
From either of these grid views, you can select one or more specific vulnerabilities using the checkboxes and select **Remediate** to initiate the standard IVR remediation flow and deploy fixlets to your endpoints. For more information, see [IVR Remediation Flow \(on page 138\)](#).

Visualizing data on the Overview tab

In the Scanner Import view, selecting the **Overview** toggle changes the interface to visual analytics. These refined charts are designed to help you quickly prioritize remediation efforts.



- **Header Section:** The header in the **Overview** view displays the following elements:
 - **Vertical Ellipsis icon (three vertical dots):** Select to reveal a menu with the following options:



- **Export:** Select **Export** to download graphical reports as a JPEG, PNG, or PDF file.
- **Configure:** Select **Configure** to open the Configure Datasource page, where you can manage datasource integrations.
- **Scanner import and File import toggles:** Switch between the automated scanner data view and the manual file import view.
- **Overview and List View toggles:** Switch between the visual analytics summary and the tabular list of vulnerabilities.



Note: The **Filter** icon and **Manage Reports** button are hidden in this view.

- **Workspace:** The workspace presents vulnerability trends using interactive charts:
 - **Critical Severity Exposures by:** This clustered bar chart visualizes vulnerabilities based on their Plugin IDs. For each ID, it plots the **Severity Score** (Light Blue) and **Scanner Count** (Dark Blue) side-by-side, allowing you to correlate the risk level with its detection frequency. You can toggle the view to base the analysis on either **CVSS** or **VPR** scoring models.
 - **Breakdown by:** A donut chart that shows the distribution of vulnerabilities by severity level (for example, *Critical* vs. *High*). You can toggle the view by **CVSS** or **VPR**.
 - **Top 10 Vulnerabilities:** This timeline bar chart visualizes the most significant security risks in your environment. It plots vulnerability counts against publication dates using a bar chart color-coded by severity (from **Low** to **Critical**). The timeline focuses exclusively on the dates associated with the ten highest-ranked risks (based on severity and frequency). You can toggle the view between **CVSS** and **Vulnerability** to analyze the distribution by severity score or specific threat.

Filtering Vulnerabilities

Apply advanced filters to quickly locate specific security flaws across large datasets by multiple properties simultaneously, including Tenable Vulnerability, ID, CVE(s), VPR, Published, and CVSS.

To filter vulnerability data:



1. Select the **Filter** icon in the header controls to open the Filter data widget.

Filter data

Set conditions on properties

Select top level filter condition

☐ Single condition
 ☒ Multiple condition (Criteria: AND)

Condition 1

Property

Operator

Property

Operator

AND

Condition 2

Property

Operator

Property

Operator

Tenable Vulnerability

ID

CVE(s)

VPR

Published

CVSS

+ Add Block

Remove all

Apply

2. Set your desired filtering conditions based on the available vulnerability properties.

3. Select **Apply**.

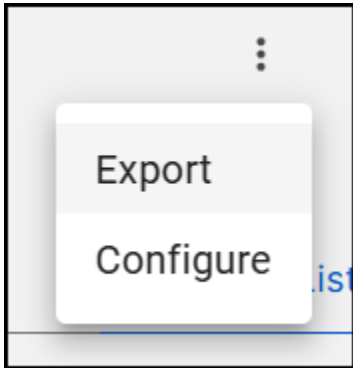
When filters are active, visual indicators appear above the main workspace grid. You can use these indicators to easily identify and clear specific filters as needed.

Exporting Dashboard Data

You can export data from the dashboard to share with external stakeholders, generate reports, or conduct offline analysis.

To export vulnerability data:

1. Select the **Ellipsis** icon (three vertical dots) in the header controls.
2. Select **Export**.



The available file formats depend on your active view:

- **List View:** Download the grid data as a CSV or Excel file.

×

Export

Export data as

☒ CSV

☐ Excel

Reset

Download

- **Overview:** Download the data charts as a JPEG, PNG, or PDF file.

×

Export

Export charts as

☐ JPEG

☐ PNG

☒ PDF

Reset

Download

Creating New Datasource

This module explains how to add a new data source to the Integrated Vulnerability Remediation (IVR) SaaS application.

Prerequisites

IVR does not scan devices directly. It ingests vulnerability data either from an integrated external scanner (such as Tenable) or through manual CSV uploads using the Universal Vulnerability Ingestion (UVI) feature. The following prerequisites apply

specifically to configuring a Tenable data source. If you are importing vulnerability data manually, see [Manually Importing Vulnerabilities \(on page 131\)](#).

1. BigFix Management:

- Ensure the **BigFix Agent** is installed on the target devices. For instructions on enrolling devices in the SaaS environment, see [Adding devices to BigFix \(on page 18\)](#).
- Verify that these devices are reporting correctly to your BigFix deployment.

2. Tenable Vulnerability Management:

Ensure the following actions are completed within your Tenable Vulnerability Management instance:

- **Install Scanners:** Ensure Tenable Nessus Scanners or Agents are installed on the target devices.
- **Create & Launch Scan:** Create a scan profile (e.g., *Basic Network Scan*) that targets the IP addresses of your BigFix-managed devices. Refer to [Create a Scan](#) in the Tenable documentation.
- **Verify Completion:** Launch the scan and wait for the status to reach **Completed**. IVR can only import finalized scan results.

3. API User Permissions:

- The Tenable user account associated with the API keys must have **Viewer** or **Auditor** permissions at a minimum.
- Ensure that your user account has the necessary permissions (e.g., **Basic User** with "Can View" access to assets, or **Administrator**) to retrieve vulnerability data. Refer to [Generate API Keys](#) in the Tenable documentation.

Procedure

- Navigate to Create New Datasource page.
 - On the left navigation pane, go to **Resolve > Integrated Vulnerability Remediation** to access the IVR application dashboard.
 - Perform one of the following actions based on your current setup:
 - **New Users:** You are automatically directed to the **Configure Datasources** page.
 - **Existing Users:** To add an additional source, click **Configure**. The **Configure Datasources** page opens.
 - On the **Configure Datasources** page, click **Create Datasource**.

Integrated Vulnerability Remediation

Updated: Jan 22, 2026 16:24:52

Datasource

Type	User	Target	Port	Alias	Status	Actions
Tenable IO	la-newuser2@yopmail.com	https://cloud.tenable.com	443	f591cc43-2f8d-4a97-b27d-8f2a977bbf9e	Running	 
Tenable IO	la-newuser2@yopmail.com	https://cloud.tenable.com	443	e1b3388e-77f1-490c-923c-fd464f1376cb	New	 

The **Create New Datasource** widget opens on the right side.

2. Fill in required information.
 - a. Enter the following details:

Field	Description
Tenable URL	The API endpoint for the Tenable instance (e.g., https://cloud.tenable.com).
Access Key	Unique key generated from the user's Tenable account.
Secret Key	Secret pair for the access key, also retrieved from Tenable.
Port	443 by default.



Note: Ensure the access and secret keys are copied accurately and securely stored. These are required for authentication and data retrieval.

- b. Click **Verify credentials**. If verification succeeds, a **UUID** is generated for the data source. Click **Save**.

On success:

- The data source appears in a datasource table.
- The initial status of the datasource is **New**. The system checks for new datasources every 10 minutes. As soon as the scheduler picks up the new datasource, the status changes to **Running** and the system

starts fetching vulnerabilities from the external scanner. When the import process completes, the status updates to **Finished**.



Note: Once the automation starts, it cannot be stopped. You cannot edit or delete a data source while it is in the **Running** status. Additionally, you cannot edit the data source if the resulting UUID is different (i.e., you cannot change the data source to a different tenant).

Type	User	Target	Port	Alias	Status	Actions
Tenable IO	la-newuser2@yopmail.com	https://cloud.tenable.com	443	f591cc43-2f8d-4a97-b27d-8f2a977bbf9e	Finished	 
Tenable IO	la-newuser2@yopmail.com	https://cloud.tenable.com	443	e1b3388e-77f1-490c-923c-fd464f1376cb	Finished	 

To edit a datasource:



1. Click the **Pencil** icon under the **Actions** field to open the **Update Datasource** widget.

Update Datasource

Tenable Cloud URL*

https://cloud.tenable.com

Tenable Access Key*

Navigate to your profile and locate the API Keys section

Tenable Secret Key*

Find keys in Tenable UI's API section

Verify Credentials

Container UUID

f591cc43-2f8d-4a97-b27d-8f2a977bbf9e

Type

Tenable IO

Port

443

Cancel

Save



Note: It is mandatory to re-enter both **Access Key** and **Secret Key**, even if unchanged.

2. Make the necessary changes and click **Save**.

To delete a datasource:



1. Click the **Delete** icon to remove the data source entry.



Note: You cannot delete a datasource that is in the Running status.

Manually Importing Vulnerabilities

The Universal Vulnerability Ingestion (UVI) feature allows you to manually upload vulnerability data into the Integrated Vulnerability Remediation (IVR) application in the Bigfix SaaS using a CSV file.

Manual imports are useful for integrating vulnerability data from external scanners or custom sources. By default, the Integrated Vulnerability Remediation dashboard opens the **Scanner Import** view. You can toggle to the **File Import** view to manually upload your file.

During the import process, you choose whether to merge the new vulnerabilities with your manual data or replace your previously imported data entirely. You must map the columns in your CSV file to the mandatory system fields.



Note: The maximum supported file size is 50 MB for a single CSV file and 250 MB in total for multiple files per tenant. Concurrently, tenants can only upload a maximum of 2 files.

Prerequisites

Before you import vulnerability data, ensure that the following conditions are met:

1. Your endpoints are registered to the root server provisioned for you in SaaS. For more information, see [Adding devices to BigFix \(on page 18\)](#).
2. Your devices are scanned by the relevant scanners so that you can download the vulnerability information as a CSV file.

Importing and Mapping Vulnerability Data

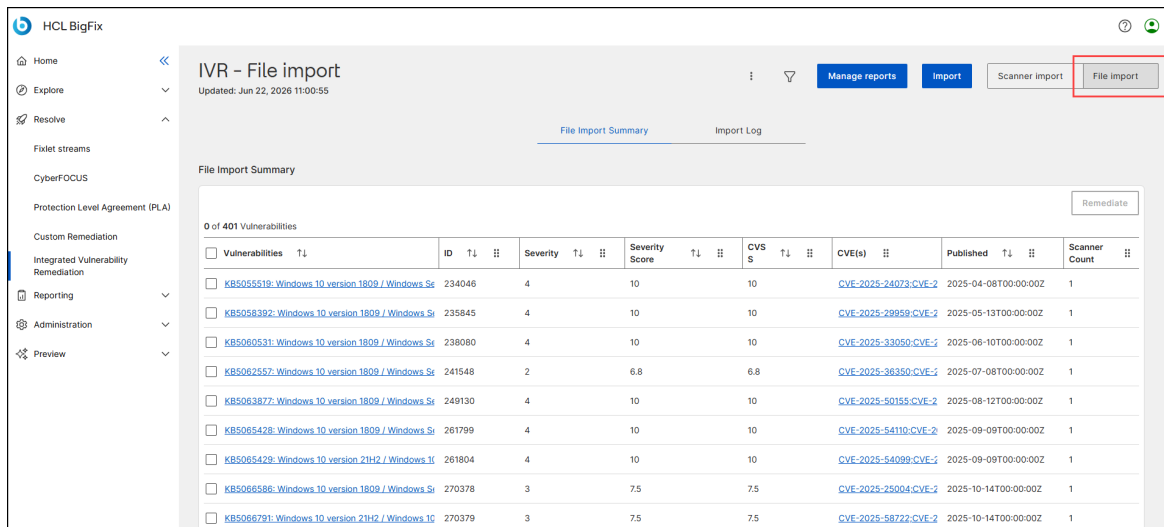
Use the following steps to upload your CSV file, choose whether to merge or replace existing data, and map your spreadsheet columns to the required system fields using the **Import Data** wizard.

1. On the left navigation pane, go to **Resolve > Integrated Vulnerability Remediation** to access the IVR application dashboard.



Note: By default, the dashboard displays the **IVR - Scanner Import** view.

2. In the upper-right corner of the dashboard, select **File Import** to switch to the **IVR - File Import** page.



IVR - File Import
Updated: Jun 22, 2026 11:00:55

Manage reports Import Scanner import **File Import**

File Import Summary Import Log

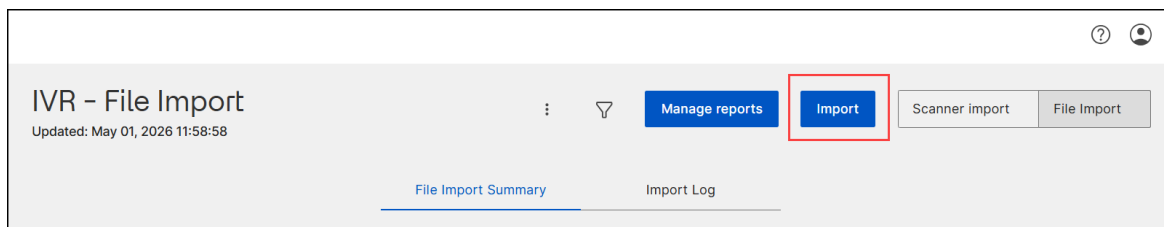
0 of 401 Vulnerabilities

Vulnerabilities	ID	Severity	Severity Score	CVSS	CVE(s)	Published	Scanner Count
KB5055519: Windows 10 version 1809 / Windows Se	234046	4	10	10	CVE-2025-24073 CVE-2	2025-04-08T00:00:00Z	1
KB5058392: Windows 10 version 1809 / Windows Se	235845	4	10	10	CVE-2025-29959 CVE-2	2025-05-13T00:00:00Z	1
KB5060531: Windows 10 version 1809 / Windows Se	238080	4	10	10	CVE-2025-33050 CVE-2	2025-06-10T00:00:00Z	1
KB5062557: Windows 10 version 1809 / Windows Se	241548	2	6.8	6.8	CVE-2025-36350 CVE-2	2025-07-08T00:00:00Z	1
KB5063877: Windows 10 version 1809 / Windows Se	249130	4	10	10	CVE-2025-50155 CVE-2	2025-08-12T00:00:00Z	1
KB5065428: Windows 10 version 1809 / Windows Se	261799	4	10	10	CVE-2025-54110 CVE-2	2025-09-09T00:00:00Z	1
KB5065429: Windows 10 version 21H2 / Windows 1f	261804	4	10	10	CVE-2025-54099 CVE-2	2025-09-09T00:00:00Z	1
KB5066586: Windows 10 version 1809 / Windows Se	270378	3	7.5	7.5	CVE-2025-25004 CVE-2	2025-10-14T00:00:00Z	1
KB5066791: Windows 10 version 21H2 / Windows 1f	270379	3	7.5	7.5	CVE-2025-58722 CVE-2	2025-10-14T00:00:00Z	1

3. Select **Import** to launch the **Import Data** wizard.



Note: The **Import** button is only available in the **File Import** view. Manual imports are not supported in the **Scanner Import** view.



IVR - File Import
Updated: May 01, 2026 11:58:58

Manage reports **Import** Scanner import File Import

File Import Summary Import Log

4. In the **Upload File** step, configure the following import settings:

Import Data

1 Upload File 2 Select Header 3 Map Column Row 4 Confirm

Select Import Mode (required)

☐ Replace ☐ Merge

Select the source of data to import (required)

☐ Tenable ☐ General CSV File

Upload File (max file size: 250 MB)

Drag and drop file or click to browse

File type supported .csv

Browse from computer

Cancel Next →

a. **Select Import Mode:** Choose how the system handles the incoming data:

- **Replace:** Deletes your previously imported data and replaces it entirely with the new file.
- **Merge:** Appends new vulnerabilities to your existing data.



Note: You can only select **Merge** if the new source of data matches your existing, configured data source. If the data sources do not match, you must select **Replace**.

b. **Select the source of data to import:** Choose either **Tenable** or **General CSV File** depending on your data origin.

c. Drag and drop your **.csv** file into the upload area, or select **Browse from computer** to locate the file. Select **Next**.

5. In the **Select Header** step, review the data preview table. Select the checkbox next to the row that contains your column headers. This ensures the system does not import your header row as a vulnerability record. Select **Next**.

Import Data

1

Upload File

2

Select Header

3

Map Column Row

4

Confirm

Select Header

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	
☒ Name	Plugin Id	Severity Score	Severity	CVSS	CVE IDs	Published	Scanner Count	
☐ Security Updates for Microsoft SQL...	182956	4.4	Medium	Medium	CVE-2023-36728	2023-10-12T00:00:00Z	1	
☐ KB5043050: Windows 10 versi...	206898	7.4	High	Critical	CVE-2024-21416,CVE-2024-...	2024-09-10T00:00:00Z	1	
☐ Security Updates for Microsoft SQL...	207065	7.4	High	Critical	CVE-2024-37341,CVE-2024-...	2024-09-12T00:00:00Z	1	
☐ Security Updates for Microsoft SQL...	207067	7.4	High	High	CVE-2024-26186,CVE-2024-...	2024-09-12T00:00:00Z	1	
☐ Security Updates for Microsoft SQL...	207070	3.6	Low	High	CVE-2024-43474	2024-09-12T00:00:00Z	1	
☐ KB5044277: Windows 10 versi...	208285	9.6	Critical	Critical	CVE-2024-20659,CVE-2024-...	2024-10-08T00:00:00Z	1	
☐ Security Updates for Microsoft .NET...	208757	4.4	Medium	High	CVE-2024-43483,CVE-2024-...	2024-10-11T00:00:00Z	1	
☐ KB5046615: Windows 10 versi...	210860	10	Critical	Critical	CVE-2024-38203,CVE-2024-...	2024-11-12T00:00:00Z	1	

Back

Cancel

Next →

6. In the **Map Column Row** step, map the columns from your CSV file to the IVR system fields using the dropdown menus. You must map the following required fields marked with an asterisk (*) to proceed:

- **ID**
- **Vulnerability Name**
- **CVE IDs**

Select **Next** when mapping is complete.

Import Data

1

2

3

4

Upload File

Select Header

Map Column Row

Confirm

Select Header Row

Field Mapping

ID*	String	182956	Plugin Id
Vulnerability Name*	String	Security Updates for Microsoft SQL Serv...	Name
CVE IDs*	String: CVE-####-####, ...	CVE-2023-36728	CVE IDs
Severity Score	Double from 0 to 10	4.4	Severity Score
Severity	String: Critical, High, Medium, or Low	Medium	Severity
CVSS	Double from 0 to 10	Medium	CVSS
Description	String	<None Selected>	Select
Published	Datetime	2023-10-12T00:00:00Z	Published

Back

Cancel

Next →

7. In the **Confirm** step, review the final preview of your mapped data.



Note: Rows with duplicate IDs may be consolidated, and rows with invalid values will be removed. Only column headers mapped to IVR fields are displayed.

Import Data

1

2

3

4

Upload File

Select Header

Map Column Row

Confirm

4. Confirm

Final data preview

Below is a final preview of your mapped data.

This is only a preview, the data will undergo further processing. Rows with duplicate ids may be consolidated. Rows with invalid values will be removed.

The preview may not exactly reflect the final result. After processing, only vulnerabilities that map to fixlets will be shown.

The column headers from your file are displayed in teal tags below each IVR column header.

Only IVR column headers will be shown in the IVR app.

ID	Vulnerability Name	CVE IDs	Severity Score	Severity
182956	Security Updates for Microsoft SQL Server (October 2023)	CVE-2023-36728	4.4	Medium
206898	KB5043050: Windows 10 version 1809 / Windows Server 2019 Security Update...	CVE-2024-21416,CVE-2024-30073,CVE-2024-38014,CVE-2024-38045,CVE-202...	7.4	High
207065	Security Updates for Microsoft SQL Server Elevation of Privilege (September 2024)	CVE-2024-37341,CVE-2024-37965,CVE-2024-37980	7.4	High
207067	Security Updates for Microsoft SQL Server (September 2024)	CVE-2024-26186,CVE-2024-26191,CVE-2024-37335,CVE-2024-37337,CVE-202...	7.4	High
207070	Security Updates for Microsoft SQL Server (CVE-2024-43474) (September 2024)	CVE-2024-43474	3.6	Low
208285	KB5044277: Windows 10 version 1809 / Windows Server 2019 Security Update...	CVE-2024-20659,CVE-2024-30092,CVE-2024-37976,CVE-2024-37979,CVE-202...	9.6	Critical
208757	Security Updates for Microsoft .NET Framework (October 2024)	CVE-2024-43483,CVE-2024-43484	4.4	Medium
210850	KB5046615: Windows 10 version 1809 /	CVE-2024-38203,CVE-2024-43449,CVE-	10	Critical

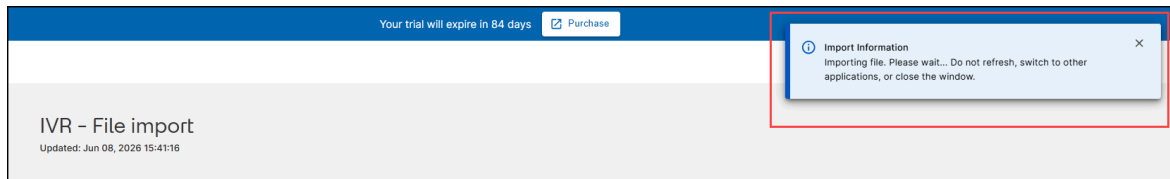
Back

Cancel

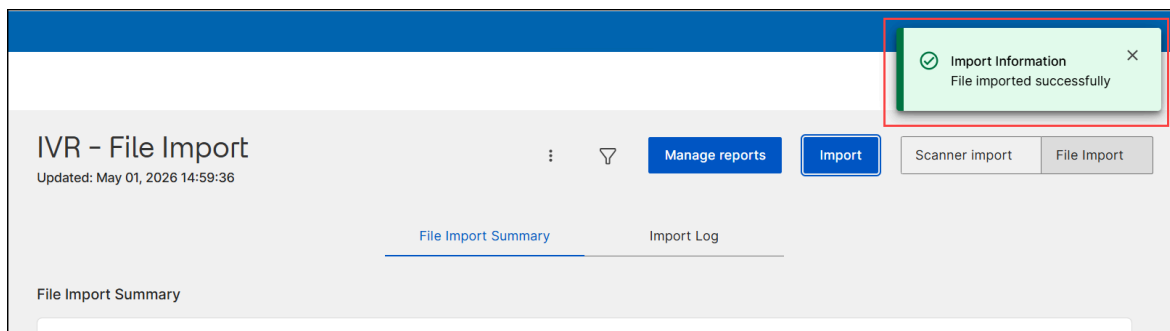
Import

8. Select **Import** to finalize the process. An **Import Information** toast notification appears stating, *"Please wait... Do not refresh, switch to other applications, or close the window."*

 **Important:** Do not navigate away from the page while this notification is displayed. Interrupting the session may cause the import to fail.



When the import completes successfully, a confirmation toast notification appears.



After the import is complete, the vulnerability data populates the **File Import Summary** section on the page. From this view, you can select the newly imported vulnerabilities and select **Remediate** to initiate the [IVR Remediation Flow \(on page 138\)](#).

Monitoring Import Logs

You can track the processing status and view historical import metrics for all manually uploaded files. The Import Log also allows you to cancel an import that is still in progress.

1. On the **IVR - File Import** page, select the **Import Log** tab.

IVR - File import
Updated: Jun 16, 2026 10:01:56

[Import](#) [Scanner import](#) [File import](#)

[File Import Summary](#) [Import Log](#)

Import Log

File Name	Processed File Rows	Date	Records Skipped	Initiated By	Status	Action
tenable 11.csv	1962	2026-06-10T13:09:12.694399Z	307	gelatoitaly007@yopmail.com	Completed	⊗
Gelato_Original_1_Windows - Gelato.csv	1748	2026-06-12T16:45:52.984881Z	118	gelatoitaly007@yopmail.com	Completed	⊗
Gelato_Original_1_Windows - Gelato.csv	1748	2026-06-11T16:58:23.192483Z	118	gelatoitaly007@yopmail.com	Completed	⊗
TenableVM1.csv	27	2026-06-10T12:10:00.160663Z	2	gelatoitaly007@yopmail.com	Completed	⊗
TenableVM1.csv	19	2026-06-11T15:30:48.878456Z	10	gelatoitaly007@yopmail.com	Completed	⊗
TenableVM1.csv	19	2026-06-10T12:05:00.155605Z	10	gelatoitaly007@yopmail.com	Completed	⊗
TenableVM1.csv	19	2026-06-08T06:33:41.165145Z	10	gelatoitaly007@yopmail.com	Completed	⊗
Replace_File_New.csv	0	2026-06-12T16:43:45.575359Z	9	gelatoitaly007@yopmail.com	Completed	⊗

2. Review the grid to monitor your imports. The grid provides the following information for each file:

Column	Description
File Name	The original name of the uploaded CSV spreadsheet.
Processed File Rows	The total number of valid vulnerability records successfully parsed and imported from the file.
Date	The timestamp indicating when the import was initiated.
Records Skipped	The number of duplicate or invalid records that the system skipped during the import process.
Initiated By	The username or email address of the user who started the import.
Status	The current state of the import. Values include Inprogress (the system is actively processing the data) and Completed (the data is fully imported and available in the dashboard), Failed (the import could not be completed), and Cancelled (the import was manually stopped before completion).
Action	Displays a cancel icon (⊗) for each import entry. For imports with a status of Inprogress , the icon is active and allows you to cancel the import. For completed or failed imports, the icon is disabled.

3. To cancel an **Inprogress** Import:
 - a. Locate the import with a status of **Inprogress**.
 - b. Select the cancel icon (⊗) in the **Action** column.
 - c. In the **Cancel import** confirmation dialog, select one of the following:

	Processed File Rows	↑↓	⋮	Date	↑↓	⋮	Records Skipped	↑↓	⋮	Initiated By	↑↓	⋮	Status	↑↓	⋮	Action	⋮
Purging2.cs	2238			2026-06-			112			rcpentest+12@vopmail.com			Inprogress			⊗	
Purging2.cs	2229									mail.com			Completed			⊗	
Purging2.cs	2229									mail.com			Completed			⊗	
	2229									@yopmai			Completed			⊗	
	2229			2026-06-			121			rc1zpentestivruvni@yopmai			Completed			⊗	
				05T11:00:06.3257837						User							

- **Cancel:** Cancels the import and stops further processing.
- **Keep Import:** Dismisses the dialog and allows the import to continue.

IVR Remediation Flow

The remediation workflow in Integrated Vulnerability Remediation (IVR) allows you to address vulnerabilities by deploying relevant Fixlets to affected devices. This process is managed through a unified wizard that guides you through selecting content, targeting devices, configuring behavior, and scheduling the deployment. You can initiate the remediation process for multiple vulnerabilities at once from the **List View** or **File Import Summary** tab in the main dashboard, or focus on a specific vulnerability from its details page.

Initiating the Remediate Wizard

Perform one of the following actions based on your remediation scope:

• **From the IVR Dashboard (Bulk Remediation):**

IVR - Scanner import

Updated: Jun 16, 2026 11:05:42

Manage reports Scanner import File import

Overview List View

Scanner Import Summary

2 of 73 Vulnerabilities

Remediate

☒ Tenable Vulnerability ↓	ID ↑↓	VPR ↑↓	CVSS ↑↓	CVE(s)	Published ↑↓	Tenable Count
☒ Adobe Flash Player <= 32.0.0.171 (APSB19-26)	125056	Medium	High	CVE-2019-7837	2019-05-14T00:00:00Z	1
☒ Adobe Flash Player <= 32.0.0.192 (APSB19-30)	125815	High	High	CVE-2019-7845 ; CVE-2019-7846	2019-06-11T00:00:00Z	1
☐ Adobe Flash Player <= 32.0.0.238 (APSB19-46)	128633	High	Critical	CVE-2019-8069 ; CVE-2019-8070	2019-09-10T00:00:00Z	1
☐ Adobe Flash Player <= 32.0.0.321 (APSB20-06)	133607	Medium	High	CVE-2020-3757	2020-02-11T00:00:00Z	1
☐ Adobe Flash Player <= 32.0.0.371 (APSB20-30)	137253	Medium	Critical	CVE-2020-9633	2020-06-09T00:00:00Z	1
☐ Adobe Flash Player <= 32.0.0.433 (APSB20-58)	141494	Medium	High	CVE-2020-9746	2020-10-16T00:00:00Z	1
☐ KB4467694: Security update for Adobe Flash Player (Now)	118917	Medium	High	CVE-2018-15978	2018-11-13T00:00:00Z	1

1. Navigate to the IVR Dashboard.
2. Select either the **List View** tab (for scanner-imported vulnerabilities) or the **File Import Summary** tab (for manually imported vulnerabilities).
3. Select the checkbox(es) for the vulnerabilities you want to remediate.
4. Click **Remediate** in the upper-right corner.

• **From the Vulnerability Details Page (Single Vulnerability):**

1. Click the name of a specific vulnerability in the dashboard to open its details page.
2. You can manage the vulnerability using the following tabs:

- **Vulnerability Information:** View high-level details (CVEs, severity). Click **Remediate** in the page header to initiate the wizard for all applicable content and devices.

The screenshot shows the 'Vulnerability Information' page for 'Adobe Flash Player <= 32.0.0.238 (APSB19-46)'. The page header includes a breadcrumb 'Integrated Vulnera... > Adobe Flash Play...' and a 'Remediate' button. Below the header is a navigation bar with 'Vulnerability Information', 'Contents', 'Devices', and 'Deployment'. The main content area is divided into two sections: 'Synopsis' and 'Description'. The 'Synopsis' section contains the text: 'The remote Windows host has a browser plugin installed that is affected by multiple arbitrary code execution vulnerabilities.' The 'Description' section contains the text: 'The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 32.0.0.238. It is therefore affected by multiple arbitrary code execution vulnerabilities.' Below the description is a link: 'See Tenable for more information'. To the right of the description is a 'Summary' table with the following data:

Severity	CPEs
Critical	cpe:/a:adobe:flash_player
Plugin Id	Exploit Ease
128633	
Version	Patch Publication Date
1.8	2019-09-10T00:00:00Z
Plugin Family	CVE IDs
Windows	CVE-2019-8069, CVE-2019-8070
VPR Score	Published

- **Contents:** Lists specific Fixlets correlated to this vulnerability. Select the content name to view its details on the Fixlet Explorer page. Select specific Fixlets and click **Deploy** to launch the wizard.

Integrated Vulnerability > KB4467694: Security update for Adobe Flash Player (November 2018)

Updated: Feb 02, 2026 14:27:57

Vulnerability Information **Contents** Devices Deployment

 Deploy

3 of 10 Fixlets selected

☒ Content Name ↑	ID ↑↓	Relevant Devices ↑↓	Site ↑↓	CVE(s)
☒ MS19-SEP: Security Update for Adobe Flash Player for Windows	2.451611511	1	Enterprise Security	CVE-2019-8069
☒ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032529	0	Enterprise Security	CVE-2020-9746
☒ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032503	0	Enterprise Security	CVE-2020-9746
☐ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032517	0	Enterprise Security	CVE-2020-9746
☐ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032535	0	Enterprise Security	CVE-2020-9746
☐ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032525	0	Enterprise Security	CVE-2020-9746
☐ MS20-OCT: Security Update for Adobe Flash Player for Windows	2.458032521	0	Enterprise Security	CVE-2020-9746

- **Devices:** Lists the specific endpoints affected by this vulnerability. Select the device name to view its details on the Device details page. Select target devices and click **Remediate** to launch the wizard for those endpoints.

Integrated Vulnerability > KB4467694: Security update for Adobe Flash Player (November 2018)

Updated: Feb 02, 2026 20:48:21

Remediate

Vulnerability InformationContentsDevicesDeployment

1 of 1 Devices selected

Device Name ↑IDLast Report Time ↑↓OS FamilyDevice Type

DESKTOP-692UFG6

16264343674 weeks agoWin10 10.0.15063.1418 (1703)Server

Remediate

- **Deployment:** Displays the history of all remediation actions previously taken for this specific vulnerability. It lists the *Deployment Name*, *Status* (e.g., Active, Completed, Expired), *Start Time*, and *User* who initiated the action. Select a specific deployment to view its details on the Deployment details page.

Integrated Vulnerability > KB4467694: Security update for Adobe Flash Player (November 2018)

Updated: Feb 05, 2026 18:04:19

Remediate

Vulnerability InformationContentsDevicesDeployment

Deployment Name ↑	State	Issued ↑↓	ID ↑↓	Start Date ↑↓	End Date ↑↓
Backend Regression Deployment 1	Active	3 weeks ago	159 [null]		[null]
IVR >> Message Testing	Expired	4 weeks ago	151 [null]		Jan 9, 2026 at 11:
IVR Deploy	Expired	4 weeks ago	157 [null]		Jan 11, 2026 at 05
IVR:Testing	Expired	4 weeks ago	149 [null]		Jan 9, 2026 at 11:

The **Remediate** wizard opens, displaying the progression steps: Fixlets, Actions, Devices, Behavior, Schedule, and Summary.

Configuring the Remediation Flow

Follow these steps to configure and submit your remediation deployment:

Step 1: Select Fixlets

Remediate

1

2

3

4

5

6

Fixlets

Actions

Devices

Behavior

Schedule

Summary

Filter the Fixlets below

Reset Filters

Select top level filter condition

☒ Single condition
 ☐ Multiple condition (Criteria: OR)

Filter block 1: select condition

☒ Single condition
 ☐ Multiple condition (Criteria: AND)

Condition 1

Property

Operator

Property

Operator

Apply

Select the Fixlets to remediate

☒	Name	ID	Relevant Devices	Release Date	CVE(
☒	MS26-JUN: Cumulative Update for Windows 10 Version 1809 - Windows 10...	2.509412301	0	Jun 09, 2026	CVE-2026
☒	MS26-JUN: Cumulative Update for Windows 10 Version 1809 - Windows 10...	2.509412303	0	Jun 09, 2026	CVE-2026
☒	MS26-JUN: Cumulative Update for Windows Server 2019 - Windows Server...	2.509412305	0	Jun 09, 2026	CVE-2026
☒	RHBA-2025:20605 - Avahi Bug Fix And Enhancement Update - Red Hat Enterpri...	15763.25206051	1	Nov 11, 2025	
☒	RHBA-2025:20616 - Bubblewrap Bug Fix And Enhancement Update - Red Hat...	15763.25206161	1	Nov 11, 2025	
☒	RHBA-2025:20736 - Emacs Bug Fix And Enhancement Update - Red Hat Enterpri...	15763.25207361	1	Nov 11, 2025	
☒	RHBA-2026:18596 - Grub2 Bug Fix And	15763.25208596	1	Nov 11, 2026	

Selected 40 Fixlets to deploy

Cancel

Next →

The wizard automatically filters the content to show Fixlets relevant to the selected CVEs.

- Review Content:** Check the **Select the Fixlets to remediate** table. This displays the details (such as *Name*, *ID*, count of *Relevant Devices*, CVE, and Severity) for each Fixlet.
- Filter (Optional):** If the list is extensive, use the **Filter the Fixlets below** section to refine the view.
 - Select **Single condition** or **Multiple condition (OR / AND)** to define complex logic.
 - Choose a *Property* and *Operator* to set your criteria, then click **Apply**.

3. Ensure the checkboxes are selected for all Fixlets you intend to include in this deployment.
4. Click **Next** to proceed.

Step 2: Configure Actions

Remediate

1

2

3

4

5

6

Fixlets

Actions

Devices

Behavior

Schedule

Summary

Click the Fixlet set to review/update

Disable All

Reset All

40 total Fixlets, 0 require attention

All Fixlets (40)

2.509412301:MS26-JUN: Cumulative Update for Windows 10 Version 1809 - Windows 10 Version 1809 LTSC - KB5094123

2.509412303:MS26-JUN: Cumulative Update for Windows 10 Version 1809 - Windows 10 Version 1809 LTSC - KB5094123 (x64)

2.509412305:MS26-JUN: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5094123 (x64)

15763.25206051:RHBA-2025:20605 - Avahi Bug Fix And Enhancement Update - Red Hat Enterprise Linux 9 (x86_64)

15763.25206161:RHBA-2025:20616 - Bubblewrap Bug Fix And Enhancement Update - Red Hat Enterprise Linux 9 (x86_64)

15763.25207361:RHBA-2025:20736 - Emacs Bug Fix And Enhancement Update - Red Hat Enterprise Linux 9 (x86_64)

15763.26185961:RHBA-2026:18596 - Grub2 Bug Fix And Enhancement Update - Red Hat Enterprise Linux 9 (x86_64)

15763.26186191:RHBA-2026:18619 - Gcc Bug Fix And Enhancement Update - Red Hat Enterprise Linux

Selected 40 Fixlets to deploy

Back

Cancel

Next

Review and update the specific actions associated with the selected Fixlets.

1. View the list of Fixlets. Use the toggle switch next to each Fixlet to include or exclude it from this specific deployment.
2. (Optional) Use the **Disable All** or **Reset All** buttons to manage the selection in bulk.
3. Click **Next**.

Step 3: Target Devices

Remediate

✓

✓

3

4

5

6

Fixlets

Actions

Devices

Behavior

Schedule

Summary

Filter the devices below

Filter By

Query

Device group

Device list

☐ Dynamic targeting device ⓘ
 [Reset Filters](#)

Select top level filter condition

☒ Single condition
 ☐ Multiple condition (Criteria: OR)

Filter block 1: select condition

☒ Single condition
 ☐ Multiple condition (Criteria: AND)

Condition 1

Property

Operator

Property

Operator

Apply

Select the devices to remediate

☒ Device Name	ID ⓘ	DNS Name ⓘ	IP Address ⓘ	Last Seen ⓘ
☒ localhost.localdomain	1087534649	localhost	10.134.131.171	2 weeks ago

← Back

Deploy [40 Fixlets](#) to [1 applicable Device\(s\)](#)

Cancel

Next →

Define which endpoints will receive the remediation. The wizard automatically filters for devices relevant to the selected vulnerability and fixlet(s).

1. **Refine Targets:** Use one of the following filter tabs to adjust the scope:
 - **Query:** Apply logical conditions (Single or Multiple) to target devices based on properties.
 - **Device group:** Select pre-defined device groups existing in your BigFix environment.
 - **Device list:** Manually select specific devices from a list.
2. **Dynamic Targeting:**
 - Toggle **Dynamic targeting device** to **On** if you want the deployment to automatically target any new devices that meet your criteria in the future (e.g., if a new device scans positive for this vulnerability later).
3. Review the **Select the devices to remediate** table to confirm the final list of target endpoints.
4. Click **Next** to proceed.

Step 4: Set Behavior

Remediate

✓

Fixlets

✓

Actions

✓

Devices

4

Behavior

5

Schedule

6

Summary

Order of Events (from top to bottom)

☒
Start downloading immediately

☐
Before running message

☒

While running message

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

☒
Reboot/Restart devices on completion of deployment

☐
On failure, retry time, and wait between attempts

☐
Reapply whenever it becomes relevant again

← Back

Deploy [40 Fixlets](#) to [1 applicable Device\(s\)](#)

Cancel

Next →

Configure the user experience and post-deployment actions. You can control the sequence by selecting which events to run. The system follows the list from top to bottom, running only the selected ones.

1. **Start downloading immediately:** Select this option to download deployment files immediately regardless of the start time schedule. Pre-cache deployment-related files, transferring them from a vendor's server to a BigFix server before deployment. You can save time when working with large files or a tight maintenance window by completing this part of the job first.
2. **User Messages:**

- **Before running message:** Select this option to set a message to display on targeted devices before the deployment runs.
 - **While running message:** Select this option to set a message to display on targeted devices while the deployment is running.
3. **Reboot/Restart devices on completion of deployment:** Select this option if the remediation requires a system restart.
 4. **On failure, retry:** Select this option to configure automatic retry attempts. Specify the number of retries and the wait time between attempts.
 5. **Reapply whenever it becomes relevant again:** Select this option to reapply the action. By default, whenever it becomes relevant again, you can reapply with 1-hour wait between attempts, up to 3 times. You can configure the wait time and the number of attempts as needed.
 6. Click **Next**.

Step 5: Schedule Deployment

Remediate

✓

Fixlets

✓

Actions

✓

Devices

✓

Behavior

5

Schedule

6

Summary

Schedule

Reset changes

Time zone ⓘ

☒ Client
 ☐ UTC

Start

Start date (dd/mm/yyyy)

23/06/2026

Start time

12:13 AM

End

End date (dd/mm/yyyy)

25/06/2026

End time

12:02 AM

Device schedule

☐ Run during Agent's configured maintenance window
 ONLY devices with a configured maintenance window are eligible for the deployment

☒ Run on all devices, regardless of their configured maintenance window

☐ Custom constraints

Time constraints

Start time

12:02 PM

End time

01:02 PM

Day constraints

☒ Sunday
 ☐ Monday
 ☐ Tuesday
 ☐ Wednesday
 ☐ Thursday
 ☐ Friday
 ☐ Saturday

Deploy 40 Fixlets to 1 applicable Device(s)

← Back

Cancel

Next →

Define the timeframe and constraints for the deployment.

1. **Time Zone:** Select **Client** to use the local time of the device or **UTC** to use Coordinated Universal Time for all devices simultaneously.
2. **Duration:** Use the **Start** and **End** toggles to set a specific window. Enter the dates and times in the respective fields.
3. **Device Schedule:** Select one of the following options:

- **Run during Agent's configured maintenance window:** Restricts deployment to the device's defined maintenance hours. See [Setting up device maintenance window \(on page 52\)](#) for more details.
- **Run on all devices, regardless of their configured maintenance window:** Overrides local maintenance windows to ensure immediate remediation.
- **Custom constraints:** Select this to define specific *Time constraints* (e.g., 10:00 PM - 11:00 PM) or *Day constraints* (e.g., Saturday only) specifically for this deployment.

4. Click **Next**.

Step 6: Review and Deploy

×

Remediate

✓

✓

✓

✓

✓

6

Fixlets

Actions

Devices

Behavior

Schedule

Summary

Summary

Add deployment name (mandatory)

⏮ No start time specified

⏭ End date & time: 25 Jun 2026 at 12:02 AM (Client Time)

🔍 40 fixlets will be included in this deployment

📁 1 statically filtered device will be explicitly targeted

Before deployment begins

⬇ Begin download immediately

🔄 No retries on failure

🕒 One time deployment

Behavior

📄 Before running message has not been configured

📄 While running message has been configured

Fixlet deployment sequence

☰ Fixlets will be deployed in the order listed

Time constraints

📅 Run on all devices, regardless of their configured maintenance window

After deployment completes

(!) Reboot/restart: Yes

Deploy 40 Fixlets to 1 applicable Device(s)

← Back

Cancel

Deploy

Finalize the configuration.

1. Enter a unique name for the operation in the **Add deployment name (mandatory)** field.
2. Review the summary sections (Fixlets, Devices, Behavior) to ensure all settings are correct.
3. Click **Deploy**.

Result: The remediation action is submitted. You can monitor the status of the action (e.g., Active, Expired) and view details by navigating to the **Deployment** tab on the Vulnerability Details page.

What to do next: Go to [Deployment Manager \(on page 38\)](#) 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.

Chapter 4. Guides in PDF format

This section contains links to PDF versions of all the BigFix SaaS product guides.

BigFix SaaS guides

[BigFix SaaS User Guide](#)

Index

A

- Ad-hoc patch deployment
 - 79
- admin role protection
 - 107
- app permissions
 - 107
- Authenticator app
 - 8
- Automated Fixlet Stream
 - 79
- Automated patch management
 - 79
- Automated remediation
 - 79
- Automated security updates
 - 79
- Automated threat remediation
 - 79
- Automated vulnerability management
 - 79
- Automated workflows
 - 14

B

- Bash script BigFix
 - 20
- Best practices for security
 - 14
- BigFix Action Script
 - 20
- BigFix custom fix
 - 20
- BigFix custom remediation
 - 20, 23
- BigFix endpoint management
 - 20

C

- client configuration
 - 65
- client settings
 - 65
- configuration settings
 - 65
- custom remediation
 - 20
- custom roles
 - 107
- custom settings
 - 65
- custom software deployment
 - 23

D

- default apps
 - 107

- default settings
 - 65
- deploy script
 - 20
- deploy script BigFix
 - 20
- deploy third-party software
 - 23
- Device health monitoring
 - 89
- Device protection levels
 - 89
- device remediation BigFix
 - 20
- Device security analytics
 - 89
- device targeting
 - 65
- Disable MFA
 - 8

E

- Enable MFA
 - 8
- Endpoint compliance reports
 - 89
- Endpoint configuration
 - 14
- Endpoint data security
 - 89
- Endpoint device monitoring
 - 89
- Endpoint incident response
 - 89
- Endpoint Management Fixlet Deployment
 - 79
- Endpoint management security
 - 89
- Endpoint protection compliance
 - 89
- Endpoint risk management
 - 89
- Endpoint security best practices
 - 89
- Endpoint security metrics
 - 89
- Endpoint vulnerability assessment
 - 89
- Endpoint vulnerability statistics
 - 89

F

- fix devices with scripts
 - 20

I

- install software on endpoints

- 23
- IT management solutions
- 14
- M**
- MFA
- 8
- MFA recovery
- 8
- MFA setup
- 8
- Multi-Factor Authentication
- 8
- O**
- on-demand remediation
- 20
- Operational efficiency
- 14
- P**
- Patch compliance reporting
- 89
- platform settings
- 65
- PowerShell deploy BigFix
- 20
- PowerShell script deployment
- 20
- Prescriptive Guidance
- 14
- Protection Level Agreement (PLA)
- 89
- R**
- RBAC
- 107
- Regulatory compliance
- 14
- relay settings
- 65
- Remediate with Bash script BigFix
- 20
- Remediate with BigFix Action Script
- 20
- Risk mitigation
- 14
- role management
- 107
- role-based access control
- 107
- run script BigFix
- 20
- S**
- SaaS security
- 8
- SaaS-based endpoint management
- 14
- Security posture
- 14
- silent install with PowerShell
- 23
- software installation automation

- 23
- T**
- TOTP
- 8
- TOTP setup
- 8
- Two-step verification
- 8
- U**
- unsupported app patching
- 20
- update registry, .reg file deployment, custom remediation, apply registry changes, windows registry patch, deploy regedit file, windows configuration update, bigfix registry deployment, bigfix remediation tools, registry tweaks, apply reg file bigfix
- 25
- User authentication
- 8
- User Manager
- 8
- user roles
- 107
- Z**
- zero-day patch management
- 79