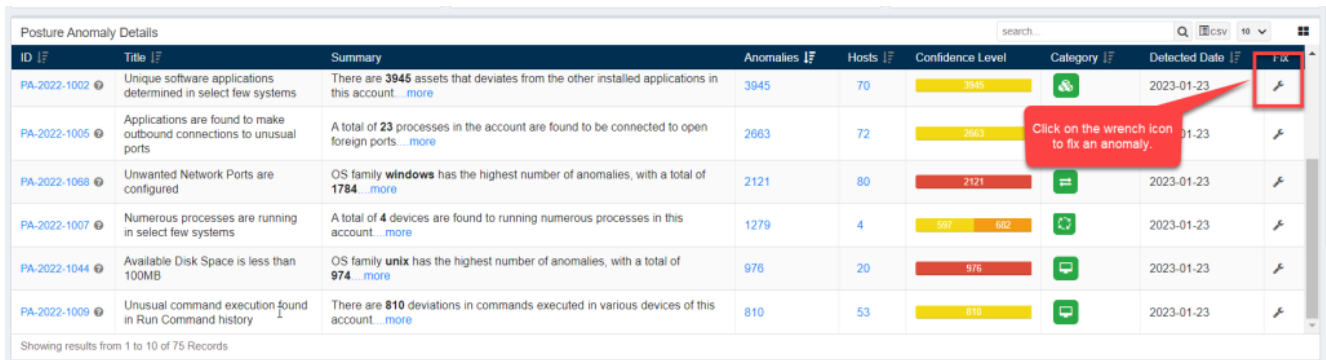


How to fix Anomalies from PA dashboard?

There are Three ways you can fix anomalies detected in your account using PA tool.

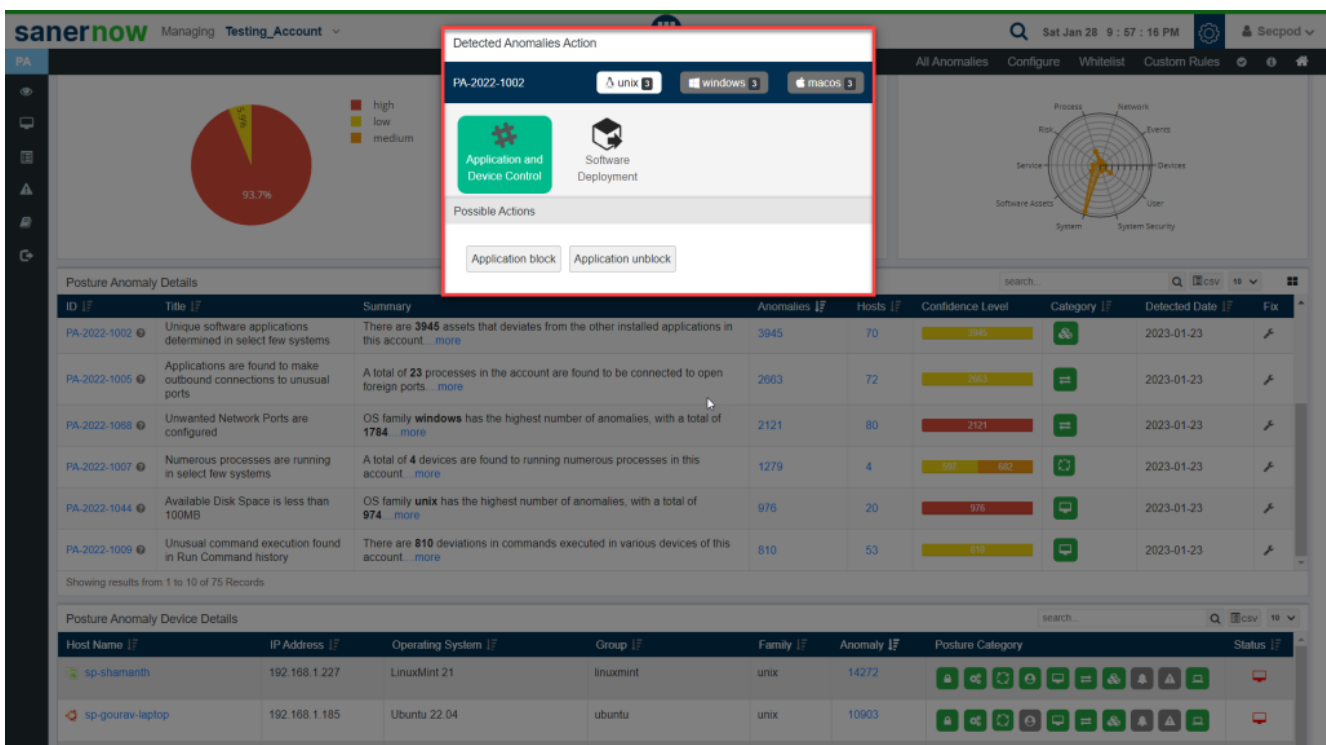
1. Click on the wrench icon displayed under the '**Fix**' column to start fixing anomalies that fall under a particular PA ID.



| ID | Title | Summary | Anomalies | Hosts | Confidence Level | Category | Detected Date | Fix |
|--------------|--|--|-----------|-------|--------------------------------|----------|---------------|-----|
| PA-2022-1002 | Unique software applications determined in select few systems | There are 3945 assets that deviates from the other installed applications in this account. more | 3945 | 70 | <div><div></div></div> 3945 | | 2023-01-23 | |
| PA-2022-1005 | Applications are found to make outbound connections to unusual ports | A total of 23 processes in the account are found to be connected to open foreign ports. more | 2663 | 72 | <div><div></div></div> 2663 | | 2023-01-23 | |
| PA-2022-1058 | Unwanted Network Ports are configured | OS family windows has the highest number of anomalies, with a total of 1784 . more | 2121 | 80 | <div><div></div></div> 2121 | | 2023-01-23 | |
| PA-2022-1007 | Numerous processes are running in select few systems | A total of 4 devices are found to running numerous processes in this account. more | 1279 | 4 | <div><div></div></div> 597 682 | | 2023-01-23 | |
| PA-2022-1044 | Available Disk Space is less than 100MB | OS family unix has the highest number of anomalies, with a total of 974 . more | 976 | 20 | <div><div></div></div> 976 | | 2023-01-23 | |
| PA-2022-1009 | Unusual command execution found in Run Command history | There are 810 deviations in commands executed in various devices of this account. more | 810 | 53 | <div><div></div></div> 810 | | 2023-01-23 | |

Showing results from 1 to 10 of 75 Records

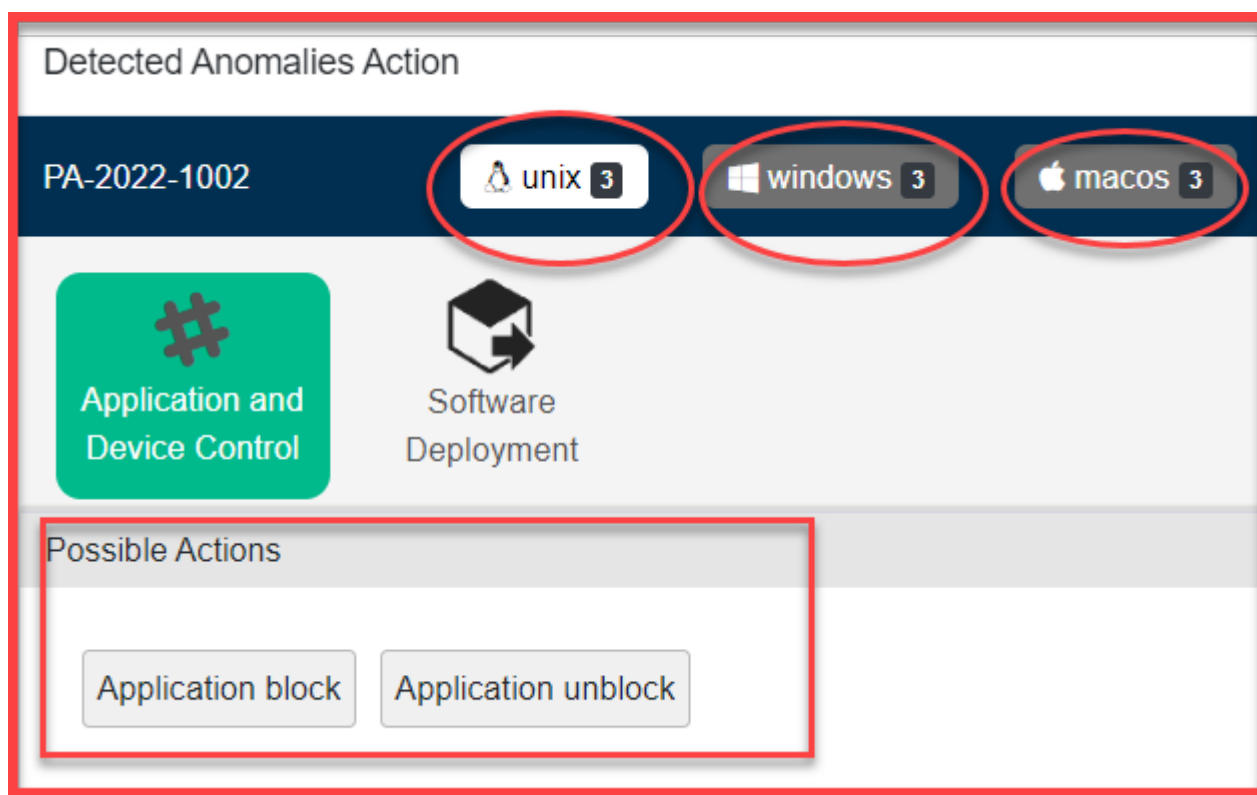
2. You will be presented with a screen that will show possible actions that can be taken to fix the anomaly. These actions will vary depending on the kind of anomaly detected and the operating system running on the devices.



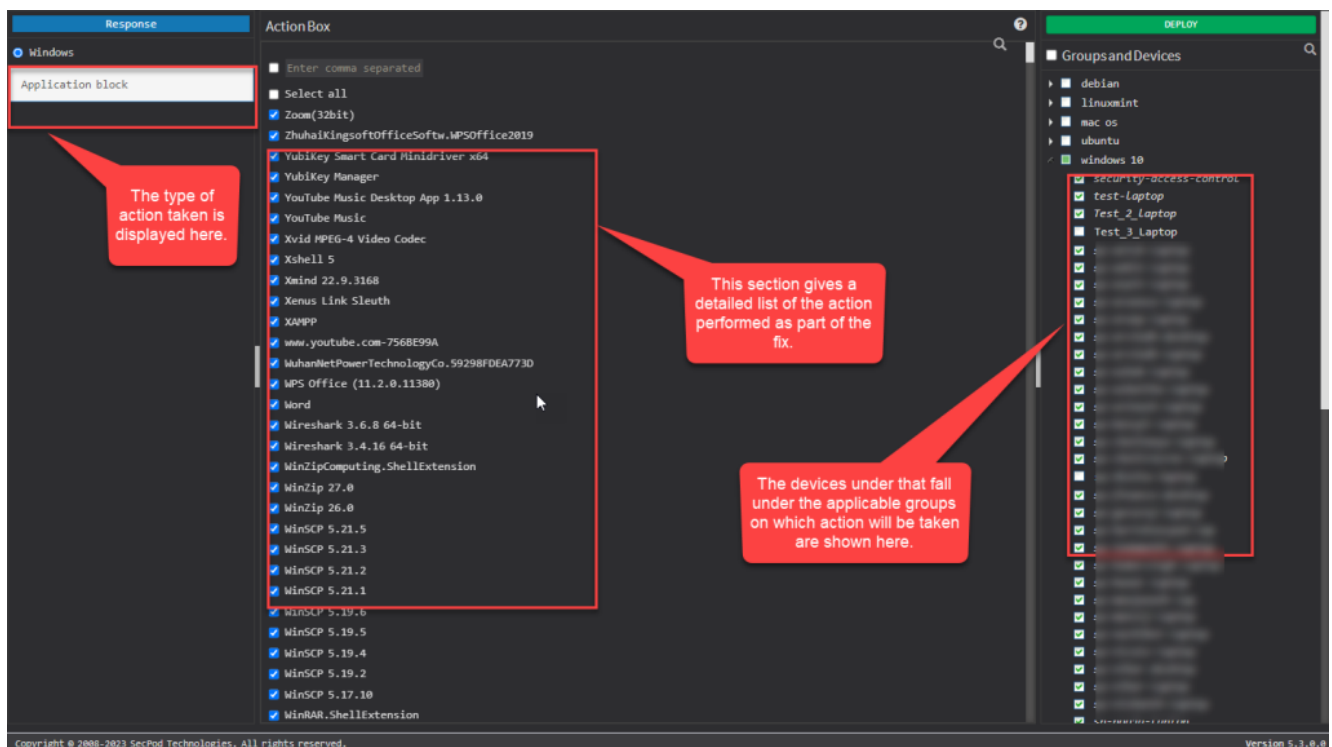
The screenshot shows the SanerNow interface. On the left, there's a sidebar with navigation icons. The main area displays a dashboard with a pie chart showing '93.7%' and a legend for 'high', 'low', and 'medium' risk levels. Below the chart is a table titled 'Posture Anomaly Details' with columns: ID, Title, Summary, Anomalies, Hosts, Confidence Level, Category, Detected Date, and Fix. The table lists several anomalies, including PA-2022-1002, PA-2022-1005, PA-2022-1058, PA-2022-1007, PA-2022-1044, and PA-2022-1009. A modal window titled 'Detected Anomalies Action' is open, showing details for PA-2022-1002. It includes tabs for 'unix', 'windows', and 'macos'. The modal displays two main action categories: 'Application and Device Control' and 'Software Deployment'. Under 'Possible Actions', there are buttons for 'Application block' and 'Application unblock'. The background also shows a 'Posture Anomaly Device Details' table with columns: Host Name, IP Address, Operating System, Group, Family, Anomaly, Posture Category, and Status.

3. The Detected Anomalies Action screen will show you all available possible actions for operating

systems on which anomalies were detected. The number of possible actions available to fix the anomaly on individual operating systems is displayed right next to the operating system label.



4. Once you click on any of the Possible Actions buttons, you will be directed to the **Response and Deploy** page.



5. Here, you can see the kind of action being performed on the top left page. Under the **Action Box**, you can see the details of the actions. This information displayed in the Action Box will change depending on the type of action being performed as part of the remediation of the anomaly. And under the Deploy page, you can see all the devices on which the Action will be performed.

Now you know how to fix anomalies from PA dashboard.