## How to configure Posture Anomaly tool for custom detection?

1. Go to Posture Anomaly dashboard and click on **Configure**.



2. In here, you can perform checks to detect unwanted services, ports, processes, start-up applications, devices, and environment variables.

You can perform checks to detect unwanted services,	0		Windows	Linux	MacOS		Others	^	0	0	0	0
<ul> <li>ports, processes, start-up applications, devices and environment viraibles. You can initiate these detections by configuring allowed values in your organization for a comprehensible anomaly calculation. The checked values will be whitelisted within the account.</li> <li>Steps to configure.</li> <li>Go to the appropriate section by clicking on the vertical menu</li> <li>Select the entities you want to whitelist in each of the sections.</li> <li>If an entity is not already present in the list, you can create by entering its name in the Add New field</li> <li>At the end, save your changes by clicking on the Save button on the top.</li> <li>Saving will thigher recalculation of PA with the new changes.</li> <li>Indicates configuration is performed on any family in the section.</li> <li>Indicates section has been edited from the previously</li> </ul>	vanted Ports	Reset           10143           445           10243           10533           12120           1351           1351           1593           1565           1593           1649           17590           17594	Add New		2	search		Q	vanted Services	vanted Process	vanted Startup Applications	vanted Devices
saved state.	PA-2022-1068 - Um	<ul> <li>18412</li> <li>19010</li> <li>2179</li> <li>22</li> <li>23419</li> <li>24642</li> </ul>							PA-2022-1069 - Unv	PA-2022-1070 - Unv	PA-2022-1071 - Unv	PA-2022-1072 - Unv

3. PA Tool provides a total of 6 configurable PA ID's that can be used for custom detection.

1. PA 2022-1068 - Unwanted Ports

- 2. PA 2022 -1069 Unwanted Services
- 3. PA 2022- 1070 Unwanted Processes
- 4. PA 2022 1071 Unwanted Startup Applications
- 5. PA 2022-1072 Unwanted Devices
- 6. PA 2022-1073 Unwanted Environment variables

Each of these PA IDs allow you to provide inputs that are OS specific – Windows, Linux, MacOS. Also, you can provide inputs for Network Devices under 'Others' tab.

4. Provide values for any of these configurable PA ID's, the PA tool will initiate a scan and the values provided by you will be whitelisted within the account.

Note: Users need to mandatorily configure each of these six configurable PA ID's. This means that the user needs to explicitly tell which ports, services, processes, startup applications, devices, and environment variables are allowed within the account.

Now you know how to configure PA tool for custom detection.