

Specify custom parameters for detections


Published: 2020-05-15

By providing information about your network environment, you can help improve the quality and accuracy of rules-based detections, which are authored by ExtraHop. Some rules-based detections rely on custom parameters and these detections are not generated if the custom parameters are left empty.

If your ExtraHop deployment includes a Command appliance, we recommend that you configure these settings on the Command appliance, and then transfer management from connected Discover appliances to the Command appliance.



Note: Parameter fields on this page might be added, deleted, or modified over time by ExtraHop.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon  and then click **Custom Parameters**.
3. Specify values for any of the following parameters available on the page.

Option	Description
Gateway Devices	<p>By default, gateway devices are ignored by rules-based detections because they can result in redundant or frequent detections.</p> <p>Select this option to identify potential issues with gateway devices like your firewalls or routers.</p>
Inbound Tor Nodes	<p>By default, inbound connections from known Tor nodes are ignored by rules-based detections because they can result in low-value detections in environments with minimal Tor traffic.</p> <p>Select this option to identify detections on inbound connections from known Tor nodes if your environment observes substantial incoming Tor traffic.</p>
Outbound Tor Nodes	<p>By default, outbound connections to known Tor nodes are ignored by rules-based detections because they can result in low-value detections in environments with minimal Tor traffic.</p> <p>Select this option to identify detections on outbound connections to known Tor nodes if your environment observes substantial outgoing Tor traffic.</p>
Related Records	<p>By default, transactions that directly result in a rules-based detection are committed as records that you can investigate. However, transactions related to the detection that might provide context and deeper insight are not committed.</p> <p>Select this option to commit records for transactions related to rules-based detections. Note that this can significantly increase the number of records committed.</p>

Option	Description
Approved Public DNS Servers	<p>Specify public DNS servers allowed in your environment that you want rules-based detections to ignore.</p> <p>Specify a valid IP address or CIDR block.</p> <p>If you do not specify a value for this parameter or for Approved Internal DNS Servers, detections that rely on this parameter might not be generated.</p>
Approved Internal DNS Servers	<p>Specify internal DNS servers allowed in your environment that you want rules-based detections to ignore.</p> <p>From the drop-down list, start typing the name of the device, and then select a device from the filtered list.</p> <p>If you do not specify a value for this parameter or for Approved Public DNS Servers, detections that rely on this parameter might not be generated.</p>
Allowed HTTP CONNECT Targets	<p>Specify URIs that your environment can access through the HTTP CONNECT method.</p> <p>URIs must be formatted as <hostname>:<port number>. Wildcards and Regex are not supported.</p> <p>If you do not specify a value, detections that rely on this parameter are not generated.</p>
Approved HTTP Ports	<p>Specify non-standard server ports in your environment that you want rules-based detections to ignore when HTTP traffic is observed on these ports.</p> <p>Type a single HTTP port number per field.</p> <p>If you do not specify a value, detections that rely on this parameter are not generated.</p>
Approved SSH Ports	<p>Specify non-standard server ports in your environment that you want rules-based detections to ignore when SSH traffic is observed on these ports.</p> <p>Type a single SSH port number per field.</p> <p>If you do not specify a value, detections that rely on this parameter are not generated.</p>
Approved User Agents	<p>Specify HTTP user agents in your environment that you want rules-based detections to ignore.</p> <p>Type a single user agent per field.</p>

4. Click **Save**.

Next steps

Click **Detections** from the top navigation menu to [view detections](#).