

Suppress detections with tuning parameters

Published: 2024-07-15

Provide information about your network environment so that the ExtraHop system can suppress low-value or redundant detections from ever being generated.

You can add criteria from the [Tuning Parameters](#) page or directly from a detection card. In addition, you can [specify network localities](#), which classify IP address ranges as internal or external to your network.

Learn more about [tuning detections](#).



View the related training: [Configure Tuning Parameters](#)


Specify tuning parameters for detections and metrics

Specify tuning parameters to improve metrics and suppress low-value detections from ever being generated.

If your ExtraHop deployment includes a console, we recommend that you [transfer management](#) of all connected sensors to the console.



Note: The 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 **Tuning 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 such as your firewalls, routers, and NAT gateways.</p> <p>This setting does not affect machine-learning detections.</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>
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</p>

Option	Description
Accelerated Beaconsing Detection	<p>your environment observes substantial incoming Tor traffic.</p> <p>By default, the ExtraHop system detects potential beaconsing events over HTTP and SSL.</p> <p>Select this option to detect beaconsing events faster than the default detection.</p> <p>Note that enabling this option can increase the detection of beaconsing events that are not malicious.</p>
IDS Detections	<p>By default, ExtraHop systems with connected Intrusion Detection System (IDS) sensors only generate detections for traffic inside your network. Select this option to generate IDS detections for traffic that is inbound from an external endpoint.</p> <p>Note that enabling this option can significantly increase the number of IDS detections.</p>
Privileged Active Directory Accounts	<p>Specify regular expressions (regex) that match privileged Active Directory accounts in your environment. The parameter list includes a default list of regular expressions for common privileged accounts that you can edit.</p> <p>The ExtraHop system identifies privileged accounts and tracks account activity in Kerberos records and metrics.</p>
Allowed 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>
Allowed HTTP CONNECT Targets	<p>Specify URIs that your environment can access through the HTTP CONNECT method.</p> <p>URIs must be formatted as <code><hostname>:<port number></code>. 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>
Trusted Domains	<p>Add legitimate known domains to the Trusted Domains list to suppress future detections that target malicious domain activity for that domain.</p> <p>Type a single domain name per field.</p> <p>If you specify a domain name, the tuning parameter suppresses detections for all subdomains. For example, if you add <code>example.com</code> as a trusted domain, detections with <code>vendor.example.com</code> as the offender are</p>

Option

Description

also suppressed. If you add a subdomain such as vendor.example.com, the parameter only suppresses detections where the participant ends with that exact subdomain. In this example, test.vendor.example.com would be suppressed but test.example.com would not.

Wildcards and Regex are not supported.

To add more than one trusted domain name, click **Add Domain**.

For detections that have an associated domain, you can also **add a trusted domain directly from a detection card**.

4. Click **Save**.

Next steps

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

Add a tuning parameter from a detection card

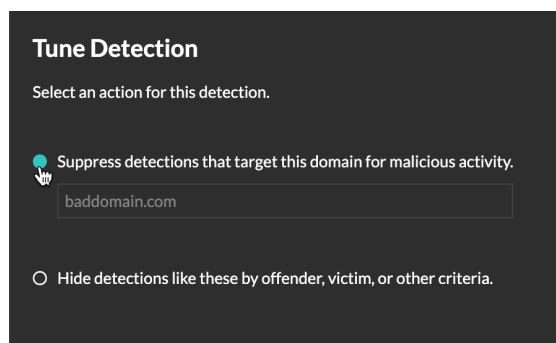
If you encounter a low-value detection, you can add tuning parameters directly from a detection card to keep similar detections from generating.

Before you begin

Users must have full write or higher [privileges](#) to tune a detection.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.
3. Click **Actions** from the lower-left corner of the detection card.
4. Click **Tune Detection...**

If the detection type is associated with a tuning parameter, you will see the option to suppress the detection by adding a tuning parameter. If the detection does not have an associated tuning parameter, you can **hide the detection with a tuning rule**.



5. Click the **Suppress detections...** option and click **Save**.

The Tuning Parameter Added confirmation appears and the new parameter is added to the **Tuning Parameters** page.