CylanceOPTICS

Getting Started Guide

Behavioral Detection Engine

Contents

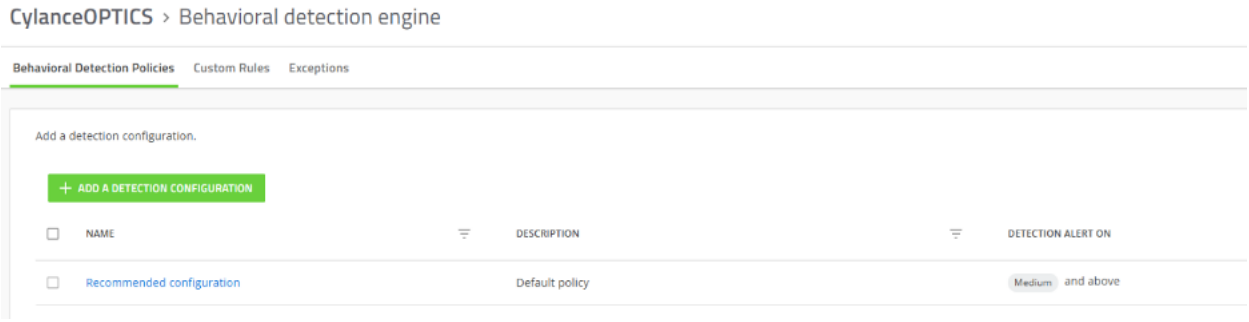
Getting started: Behavioral Detection Engine

The Behavioral Detection Engine (BDE) uses a behavioral detection policy, which aligned with the MITRE framework, to send detection rules to your users' devices. According to the detection rules, alerts are raised based on the alert threshold and remediation steps automatically take place. The BDE eases the burden of configuring and managing CylanceOPTICS when compared to using the legacy rule sets.

In the Cylance console, you can create the detection policy where you configure the alert threshold and the automated remediation steps according to the response threshold. After you configure the BDE policy, you must link it to a device policy and apply the device policy to devices within your organization. This guide provides an overview of the BDE policy, how to link it with a device policy, manage BDE policy content updates, review alerts, and create exceptions. It also includes guidance and best practices for how start using BDE and recommendations related to automated responses.

If you are an existing CylanceOPTICS customer using legacy rule sets, it is recommended that you migrate from using legacy rule sets to BDE policies. For more information, see the Behavioral Detection Engine Migration Guide.

Behavioral detection policies



In the Cylance console, behavioral detection policies are in the **CylanceOPTICS > Behavioral Detection Engine** menu, in the **Behavioral Detection Policies** tab.

The BDE policy defines which MITRE detections to apply to devices, which severity level to alert on, and when to apply automated responses. All tenants have a default policy configured which has all the MITRE detections with Alerts and Observations features enabled. The default policy is configured with an alert threshold of medium and above.

Alert thresholding is a new concept introduced with BDE. It allows easy suppression of alerts that are below a certain level of severity. This means that only alerts at or above the specified threshold level display in the **Alerts** screen and through external interfaces like syslog or the public API. To ensure that there is no loss in information fidelity, the BDE includes support for observations. When **Observations** are enabled, the BDE instructs the CylanceOPTICS agent (version 3.3 or later) to watch for all behaviors that are below the alert threshold, collect any data associated with it, collect any correlated elements along the attack chain, and add the appropriate MITRE TTP tagging to that collected data. Using Alert Thresholds and Observations, the BDE can enact policies with a much lower level of noise without missing important data that may be hiding in low efficacy signal.

Creating a behavioral detection policy

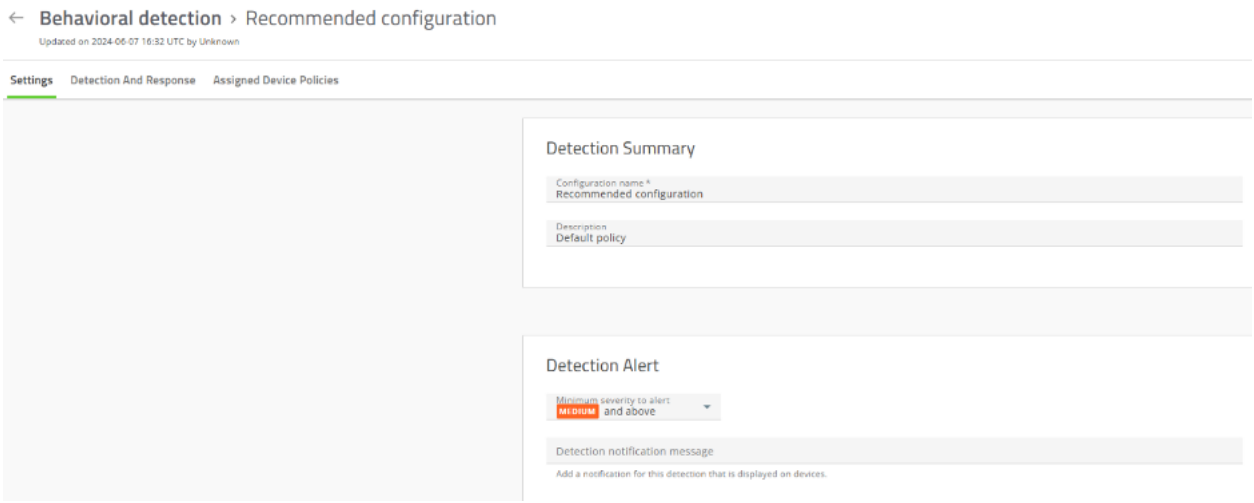
You can create a behavioral detection (BDE) policy from the CylanceOPTICS > Behavioral Detection Engine > Behavioral Detection Policies tab. Click "Add a detection configuration" to create a policy.

Specify this information:

- A name for the configuration.
- A description of the configuration.
- The alert threshold, which is the minimum severity for an alert to be generated and appear in the **Alerts** screen.
- The message to display on the user's device when a detection occurs.

You can configure these settings in the **Settings** tab when you edit a detection policy.

After you create the policy, you need to configure its detection and response settings, and then assign it to device policies.

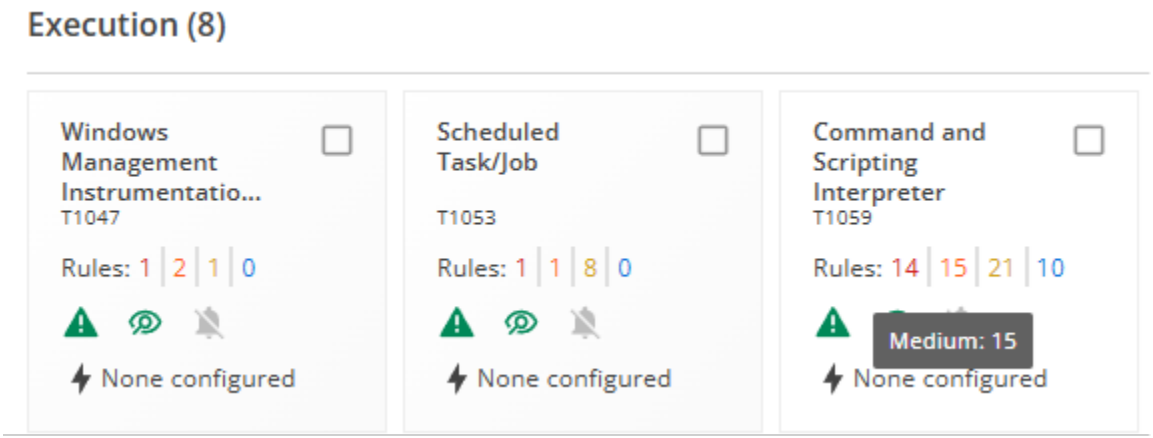


Detection and response tab: Behavioral detection policy

After you create a detection policy, open the policy and configure the settings in the **Detection and Response** tab.

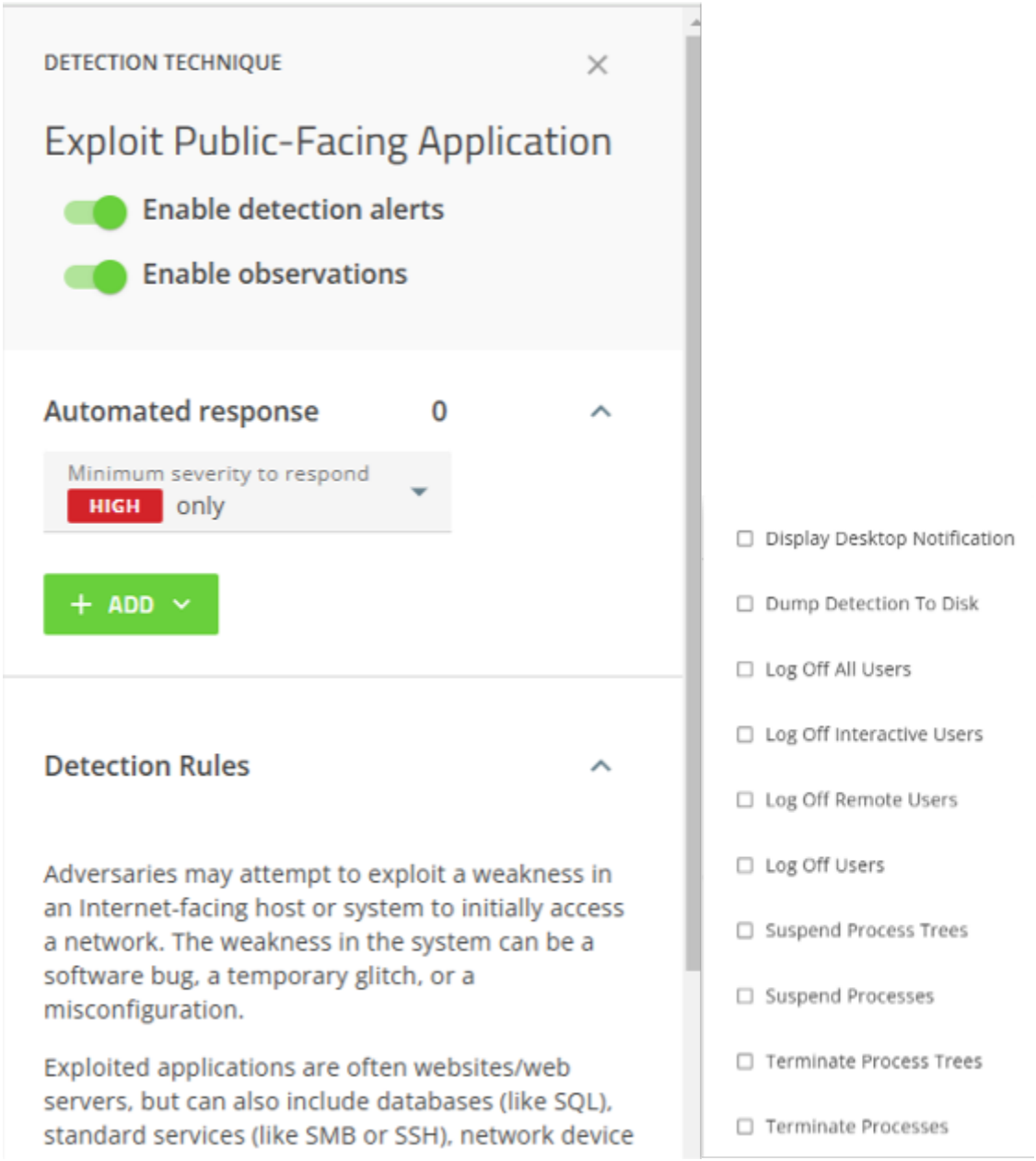
On the **Detection and Response** tab, on the left side of the screen, you can apply filters to help find the detection rules that you are looking for:

- Alerts (On or Off): Filter detection rules by whether detection alerts are enabled.
- Observations (On or Off): Filter detection rules by whether observations are enabled.
- Notifications (On or Off): Filter detection rules by whether notifications are enabled.
- Automated response action: Filter detection rules by the automated response action.
- Platform: Filter detection rules by operating system platform.



On the center of the screen, the detection rules are displayed as cards for specific MITRE techniques aligned from the MITRE framework. Each card includes the rule name, MITRE technique ID, the number of detections rules included at each severity level, and icons that indicate if alerts, observations, notifications and automated responses are configured. Bulk edit options appear above the cards if you use the checkboxes to select them.

You can click on a detection rule card to open a side panel on the right side. The side panel displays a detailed description of the rule as well as controls to enable alerts, observations, notifications, and automated responses.

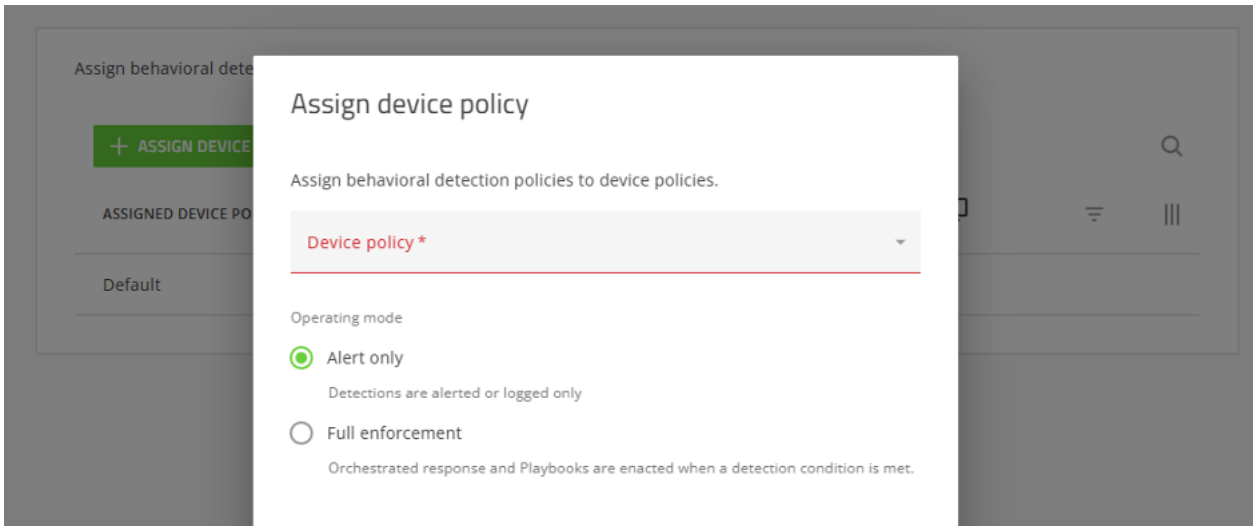


If you want to configure automated responses for a detection rule, you must specify the minimum severity level for the response to apply. In this example, the default minimum severity is set to **High** because this class of rules are the most precise and the easiest to tune. This ensures minimal impact on business continuity due to the lower false positive rate average. Next, add one or more remediation actions from list of available actions. The CylanceOPTICS agent and BDE will take all applicable response actions that are configured based on the context of the detection.

Assigned device policy tab: Behavioral detection policy

After you create a detection policy, assign the BDE policy to device policies from **Assigned Device Policies** tab. Each device policy associated with a BDE policy will be listed by name and include the number of associated devices.

You can add device policies to associate them with the BDE policy. When adding a device policy, in the **Device policy** list field, you can select from the list the device policies that are available in the tenant. You can also specify the operating mode (**Alert only** or **Full enforcement**) which determines whether an alert triggers the automated responses. The operating mode for each device policy can be changed at any time from the **Policies > Device Policy** menu.



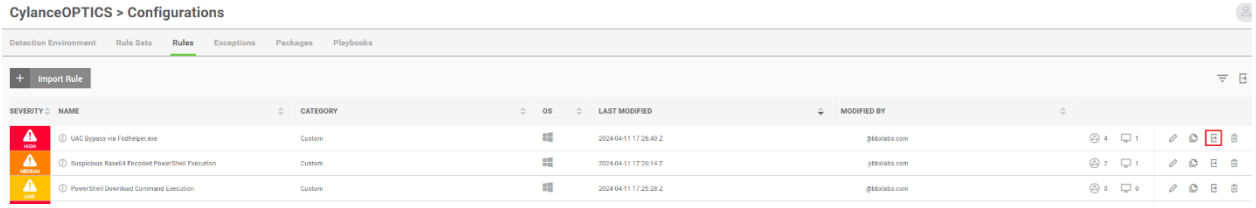
Importing custom rules

The Behavioral Detection Engine supports importing custom detection rules in .json format. In the Cylance console, you can import custom detection rules into custom rule groups from the **CylanceOPTICS > Behavioral Detection Engine > Custom Rules** tab. You can also export legacy rule sets in .json format and import them.

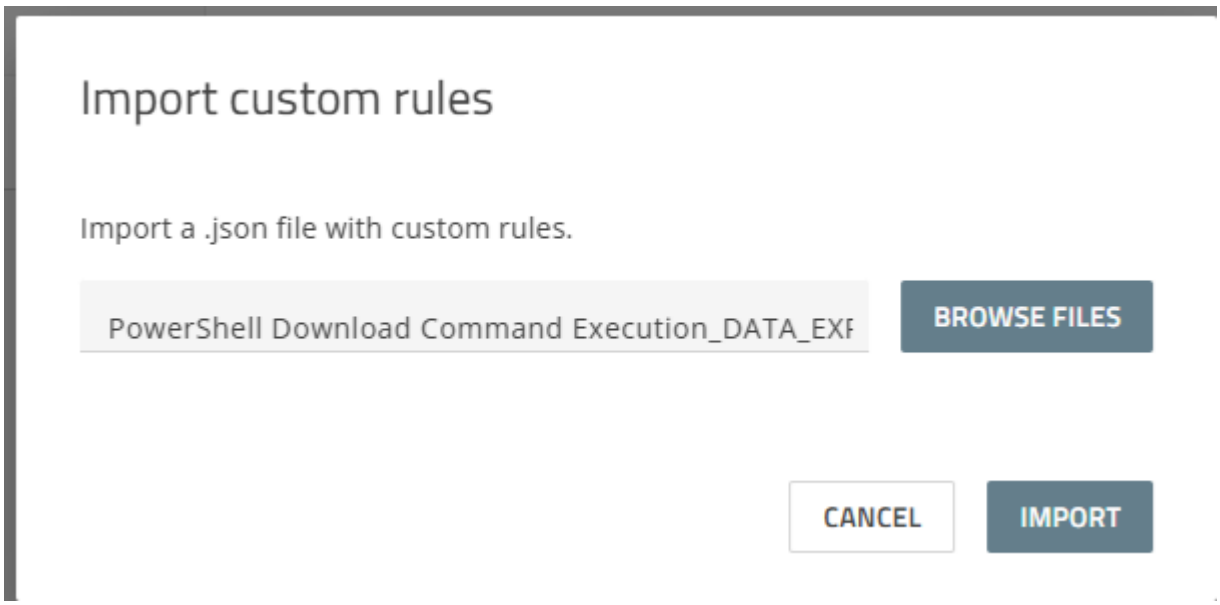
Before you import a custom detection rule, create a custom rule group. The custom rule group that you created appears as a card on the **Custom Rules** screen.

Use these steps to export the legacy rule sets from the Cylance console, create a custom rule group, and then import the legacy rule sets to the custom rule group:

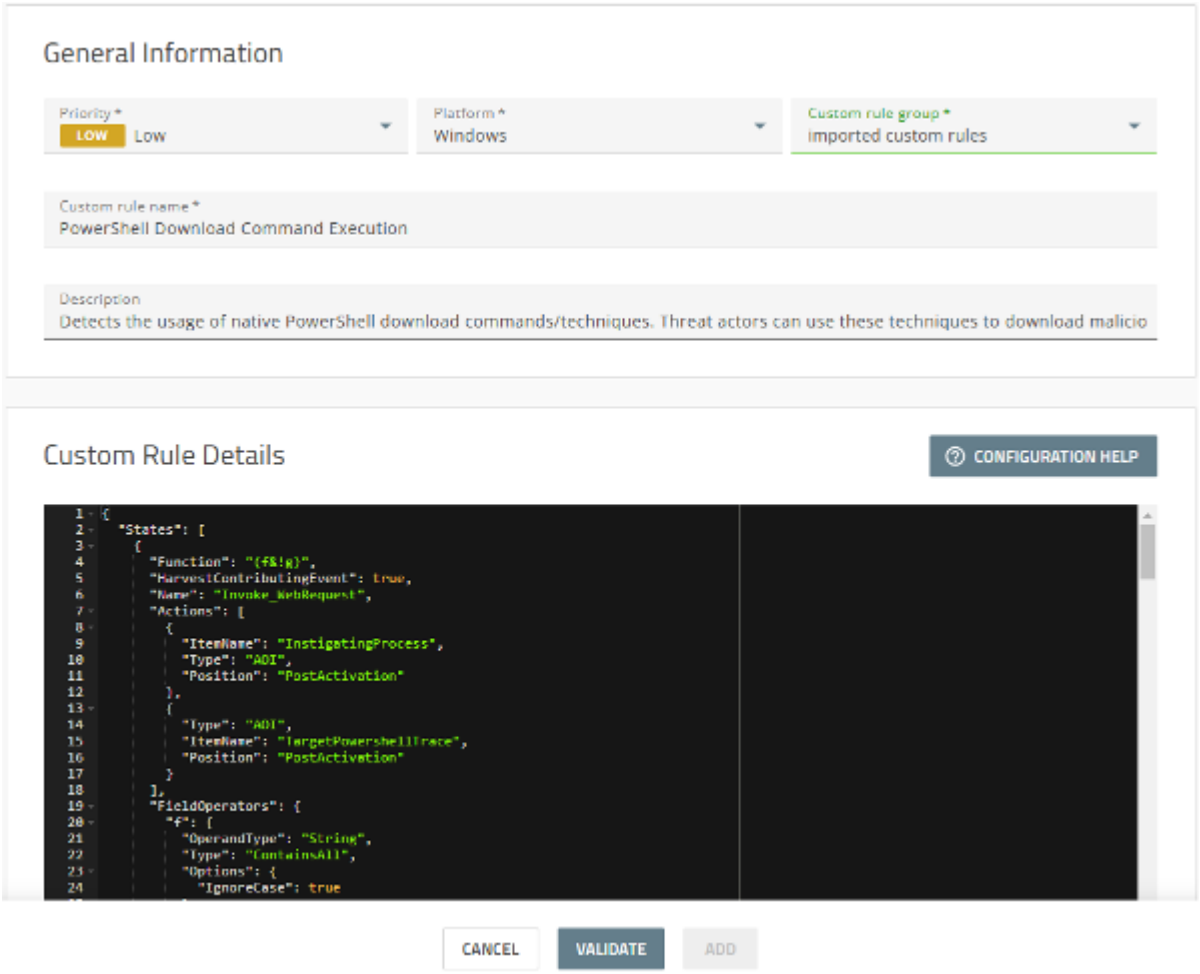
1. Navigate to **CylanceOPTICS > Configurations > Rules**.
2. Beside the rule that you want to export, click **Export** and save the .json file with the rule conditions.



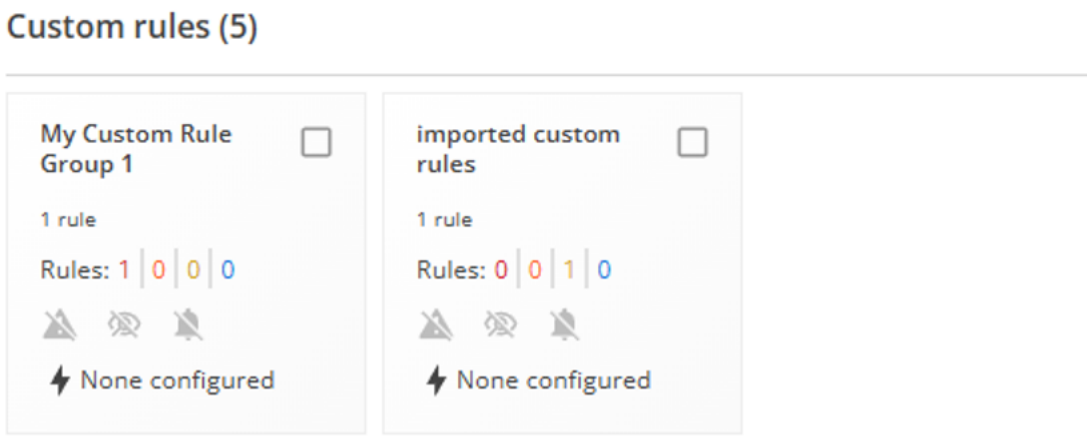
3. Navigate to **CylanceOPTICS > Behavioral Detection Engine > Custom Rules**.
4. In the **Custom Rule** tab, click **Add** and then add a new custom rule group.
5. Click the custom rule group, and then on the right side, click **Add > Import custom rules**, and specify the .json file.



6. Review the imported rule conditions, verify the target custom rule group, and then click **Validate**. After validation, click **Add** to complete the import.



7. On the **Behavioral Detection Engine** screen, **open the BDE policy > Detection And Response** tab where you can enable alerts, observations, and automated responses for your custom rules. The custom rule group will appear as a new card at the bottom of the **Detection And Response** tab when editing a BDE policy, under the **Custom rules** section.



Adding exceptions

In some cases, alerts may be triggered by legitimate business applications installed on your users' devices. If this occurs an exception is required to ensure business continuity and to prevent unnecessary alerts from being reported to the console.

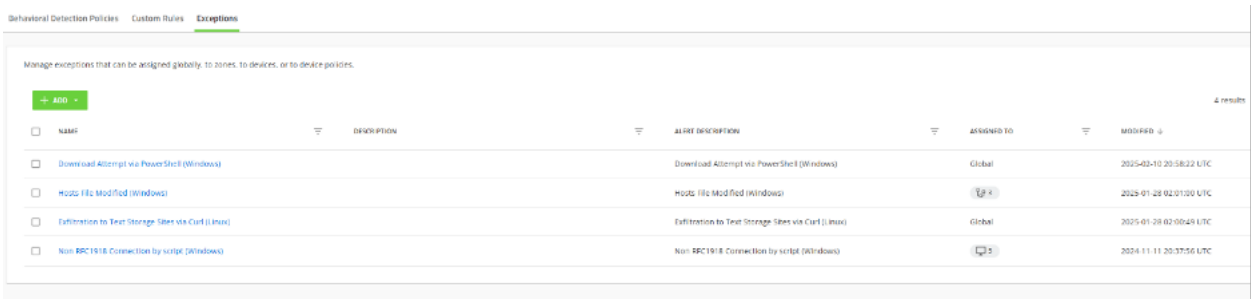
Exceptions can be added in two ways:

- From the **CylanceOPTICS > Behavioral Detection Engine > Exceptions** tab
- From the **Alerts** view

Regardless of where the exception was created, the **Exceptions** tab displays a list of all exceptions for the tenant, including the name, description, alert description, assignment, and the date the exception was last modified.

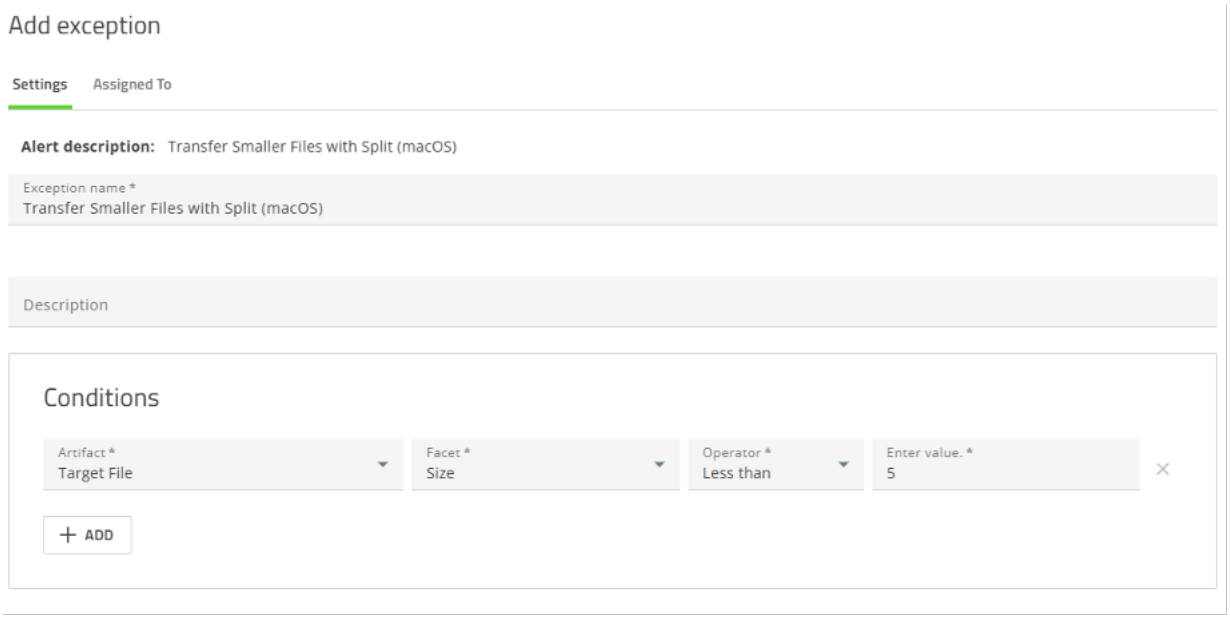
Adding exceptions from the Exceptions tab

You can add exceptions from the **CylanceOPTICS > Behavioral Detection Engine > Exceptions** tab.



When adding an exception from the **Exceptions** tab, specify the MITRE tactic and technique for which you want to create an exception along with an appropriate alert description.

Next, specify one more conditions, including the artifact, facet, operator, and value for each condition.

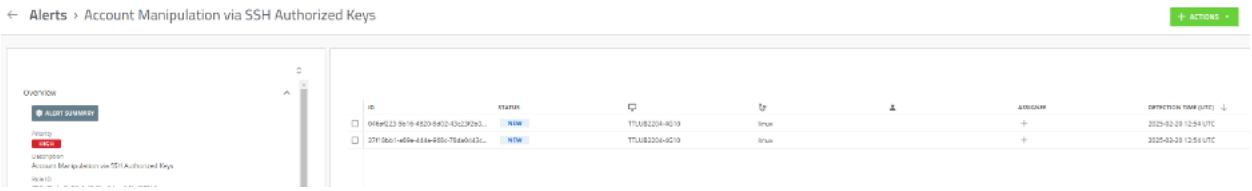


In the **Assigned To** tab, assign the exceptions appropriately using one of the options. For more information, see the next section on "Assigning exceptions globally, to zones, to devices, or to device policies" in this guide.

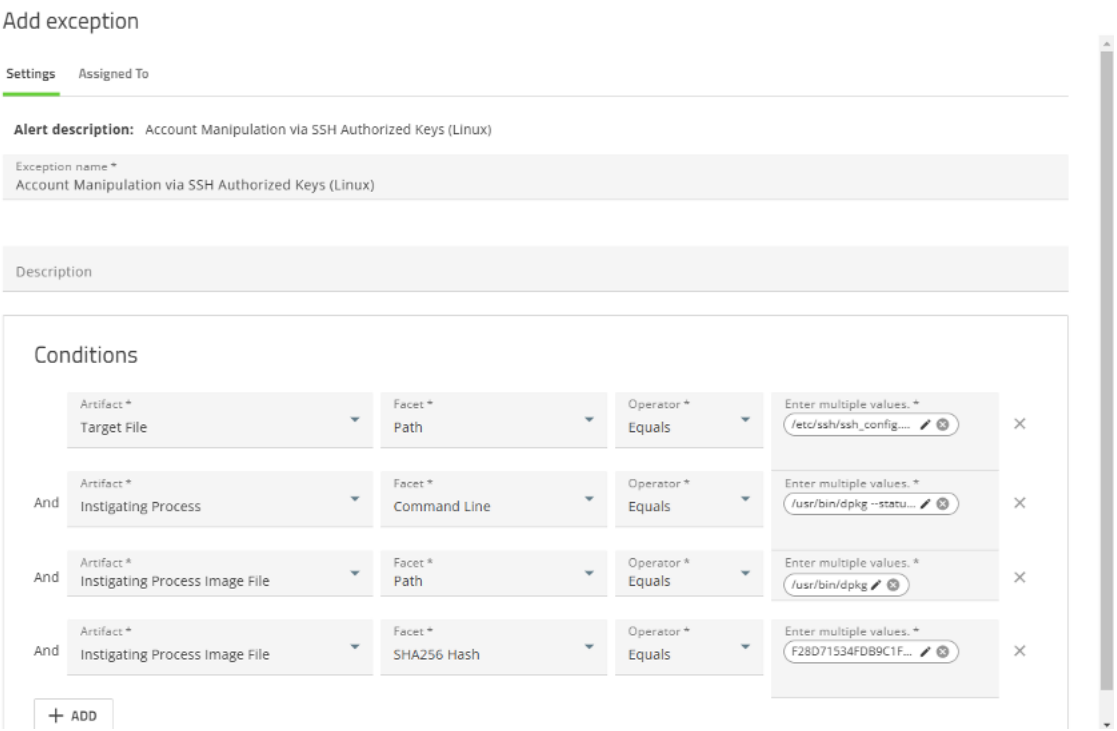
Adding exceptions from the Alerts view

If you observe an alert for a legitimate business application in the Alerts view, you can use AI to add exceptions. The details of the exception, including the conditions, are automatically defined by AI based on the alert.

To add an exception in the Alerts view, simply open the alert and use the **Actions** menu on the top right of the screen.



In the **Add exception** dialog box, review the details of the exception, and then make changes if necessary.

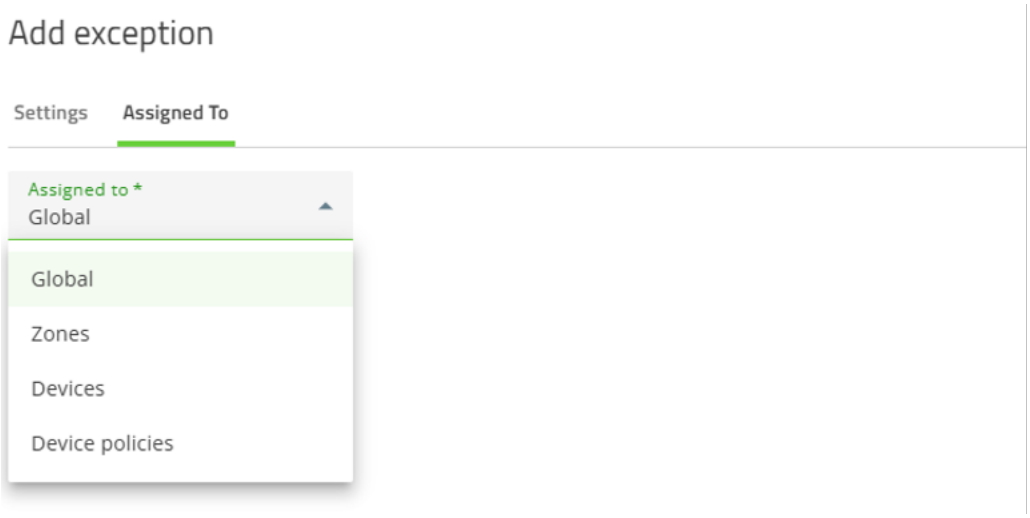


In the **Assigned To** tab, assign the exceptions appropriately using one of the options. For more information, see the next section on "Assigning exceptions globally, to zones, to devices, or to device policies" in this guide.

Assigning exceptions globally, to zones, to devices, or to device policies

Regardless of how you add a detection exception, you must specify how to assign them to devices. When configuring an exception, in the **Assigned To** tab, you can specify whether to assign the exceptions globally, to zones, to devices, or to device policies.

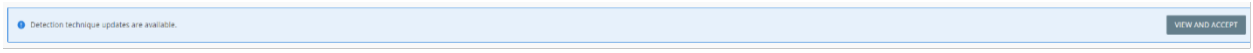
- Global: Applies the exception to your organization's entire tenant
- Zones: Applies the exception to the zones that you select and all devices assigned to those zones.
- Devices: Applies the exception to the selected devices
- Device Policies: Applies the exception to all devices that are assigned to the selected device policies



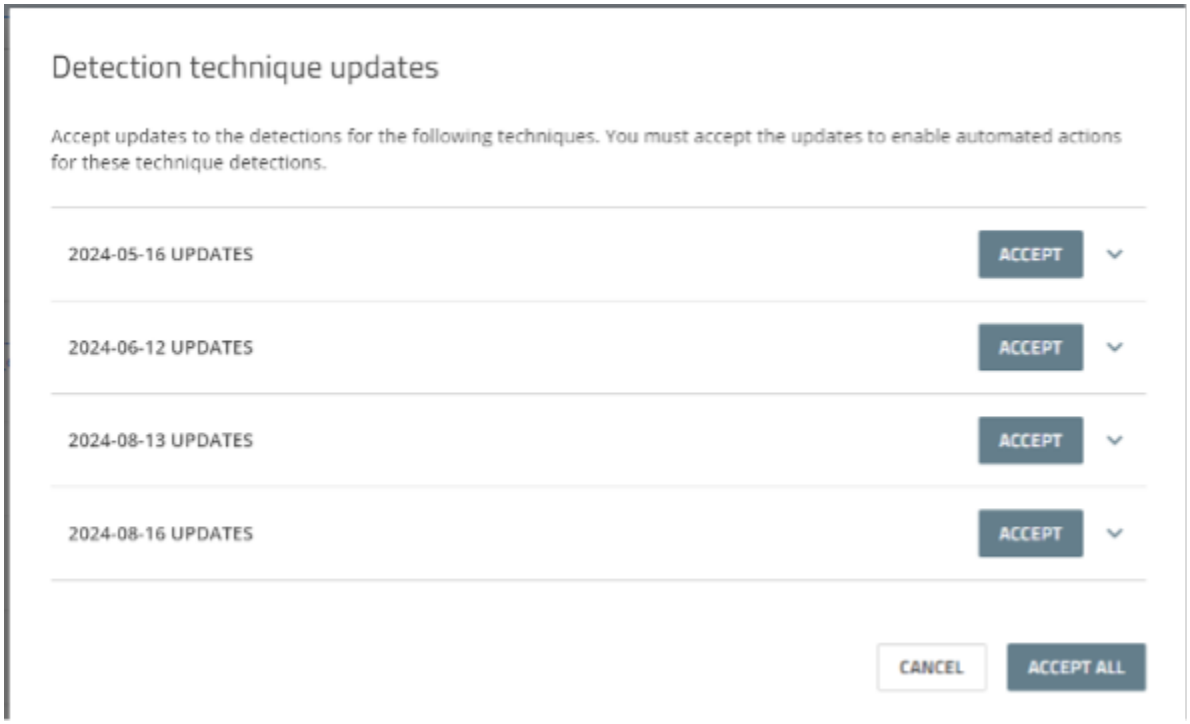
Managing detection rule updates

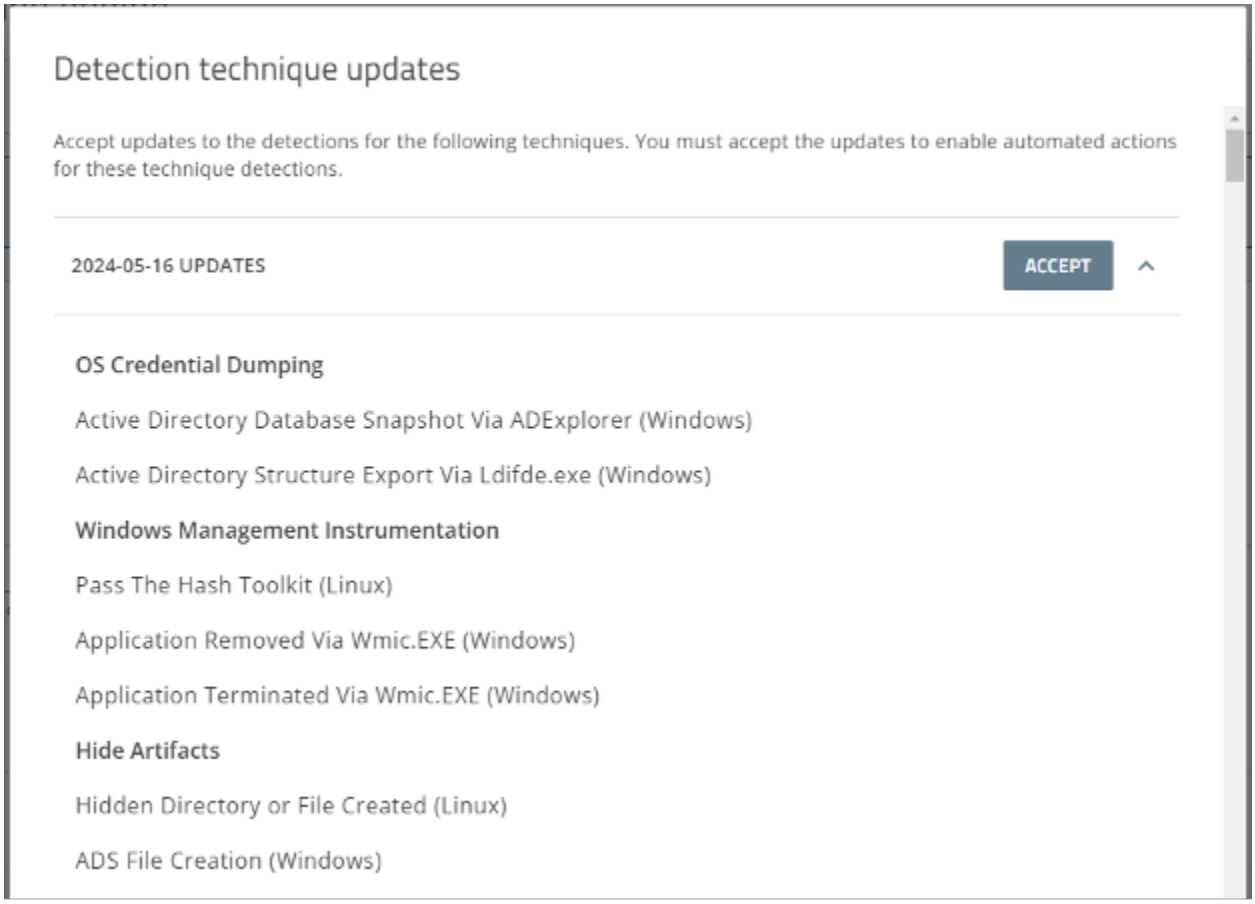
Cylance continues to develop CylanceOPTICS detection rules for new and emerging threats. To streamline the time to value, and minimize the overhead required to benefit from the new rules, we have automated the deployment process.

When updates are available for detection rules, a notification appears in the Cylance console on the **CylanceOPTICS > Behavioral Detection Engine** screen.



You can click the notification to view the details of each update available. For each update, you can expand it to view the changes, grouped by the detection technique. Knowledge base (KB) articles are available for more information about some of the updates.



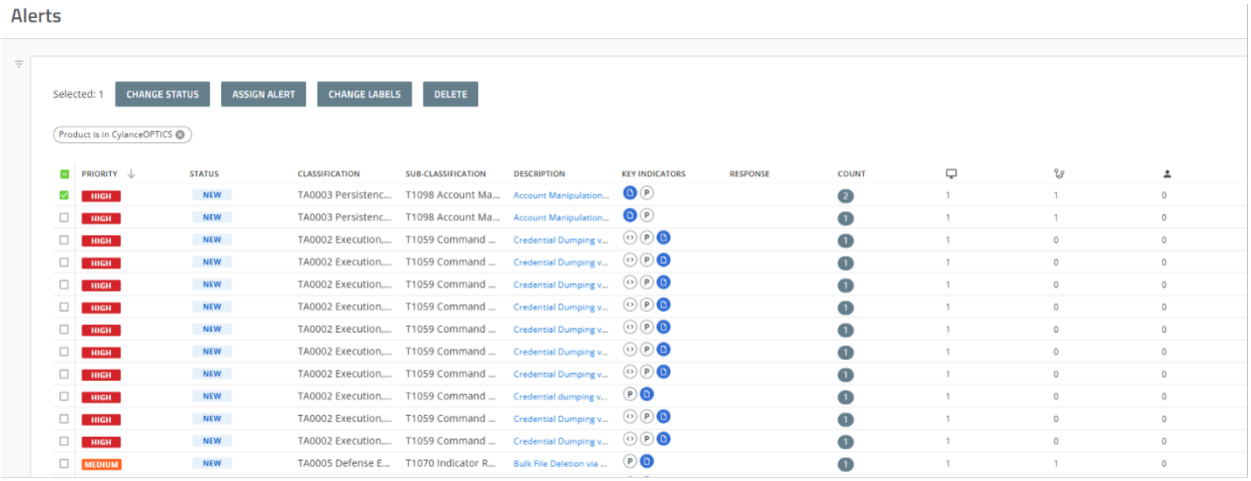


As soon as an update is available, the new rules are automatically pushed to devices according to the BDE policy that is already assigned to those devices. Until the rules are accepted, the rules will operate in Alert Only mode. Users and devices will not be impacted due to potentially untuned false positives. This allows administrators to observe the performance and impact of the new rules, and provides an opportunity for any tuning or exception creation prior to accepting the rules and enforcing them. Enforcement means any defined automated responses are applied when the detection rule is triggered.

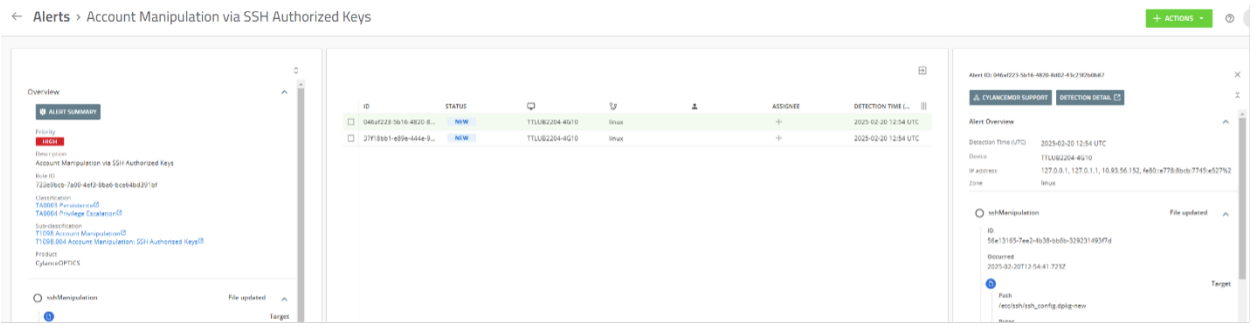
If business continuity issues arise at any point during enforcement, you can change the BDE policy to Alert Only mode to allow administrators to review alerts and tune their environments without impacting users before enforcing the rules again.

Viewing alerts

Alerts raised from the BDE will appear in the Cylance console on the **Alerts** screen. The initial Alerts view is a summary that groups similar alerts based on criteria such as priority, alert classification, configured responses, and other key alert attributes. Each alert has a priority, status, classification and sub-classification as well as a description and some key indicators. For more information about the data displayed in the **Alerts** screen, see the Alerts documentation.



On the **Alerts** screen, you can change the status of the alert, assign it for triage, add or edit labels, or delete the alert. You can click an alert group to display second level alert information, such as the individual alerts within the group, and use AI to generate an alert summary. You can use the **Actions** menu within the alert to create exceptions using AI to define the exception conditions automatically.



Best practice: Tuning your environment

1. As a best practice, start with assigning the default BDE policy to devices and monitor the alerts prior to enabling automated responses. During this observation period, identify any alerts triggered by legitimate business applications and then add exceptions for them so that business continuity can be maintained when you enable automated responses. You can easily add exceptions from the Alerts view using the **Actions** menu.
2. Continue to monitor and review all alerts with **High** severity to determine if additional exceptions are required to remove unwanted alerts. You can apply filters in the **Alerts** screen to quickly find these alerts. For example, click the **Product** column heading, and then filter for **CylanceOPTICS** alerts. By default, the alerts with the highest severity are displayed at the top of the filter results.
3. After the recommended observation period of seven to ten days has passed without any alerts triggered by legitimate business applications and no unwanted alerts, you are ready to enable automated responses and start enforcement.
    - If you want to enable automated responses for a detection technique, set the **Automated response severity** setting to **High only**. For the remediation actions, add **Display Desktop Notification**, **Log Off Remote Users** and **Terminate Process Tree**.
    - To start enforcement, edit the device policy to change the BDE policy operating mode from **Alert only** to **Full enforcement**.

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at .https://www.blackberry.com/us/en/legal/third-party-software

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada