BlackBerry Extension for IBM QRadar

Administration Guide

3.0.2

Contents

What is the BlackBerry Extension for QRadar?

The BlackBerry Extension for QRadar enables the following interactions with the Cylance console:

- REST API interaction with the Cylance console (for both CylancePROTECT and CylanceOPTICS)
- Download threat data reports
- Enables SIEM administrators to parse syslog events from CylancePROTECT and CylanceOPTICS
- Supports right-click and hover interactions for log events to provide more information

Note: The extension can be configured to use the Cylance API, the threat data reports, the Cylance syslog, or a combination of these features. The extension does not support integration with a CylanceON-PREM server.

Custom content

The BlackBerry extension contains the following custom content:

- Application (1)
- Custom AQL Function (0)
- Custom Property (7)
- Custom QIDMap Entry (90)
- Custom Rule (4)
- Custom Rule Response (0)
- Dashboard (1)
- Log Source (2)
- Log Source Extension (1)
- Log Source Type (1)
- Reference Data Collection (0)
- Reports (0)
- Saved Search (16)
- Other (0)

Custom properties

The BlackBerry extension includes the following custom properties.

Item	Description
Cylance Event ID	The CylanceOPTICS event ID or detection ID value
Device Name	The name of the device; when the device is created, this is the same as the hostname but can be changed in the Cylance console
Device UUID	The unique ID assigned to the device
More	Generic extra information field that provides different information for different types of events
Operating System	The operating system used by the device

Item	Description
Threat SHA256	The SHA256 value for the threat

Log sources

This extension comes with two log sources, one for live tenants and one for local replay (if needed).

- The live tenant parses a TLS syslog feed
- The local replay parses manually supplied syslogs

Install the extension

To install the BlackBerry extension:

1. In QRadar, navigate to the **Admin** tab.
2. Open **Extension Management**.
3. Click **Add**.
4. Click **Browse**.
5. Choose the downloaded extension file.
6. Click **Open**.
7. Select **Install Immediately**.
8. Click **Add**.
9. Select **Replace existing items**.
10. Click **Install**.
11. Click **OK**.
12. Click **Deploy Changes**.

Create the Application ID and Application Secret

Some of the features in the extension use the Cylance API. Accessing the API requires an application ID and an application secret from the Integrations page in the Cylance console.

1. In the Cylance console, select **Settings > Integrations**.
2. Click **Add Application**.
3. Enter a name for the application.
4. Select the permissions for each privilege you want to grant to the API user. See the table below for required settings.
5. Click **Save**.

Note: Copy the tenant ID, application ID, and application secret. You must provide this information to the API user so they can access data from the Cylance console via the REST API.

Application privileges

The following table summarizes the minimum set of permissions required to make use of all of the available features.

*Security administrators may remove permissions if only a subset of the features are required. If you grant additional permissions, you or other administrators can have access to allow the alteration of data on the Cylance tenant.

Privilege	Permissions
Devices	• Read • Modify*
Global Lists	• Read • Write* • Delete* (required for Remove actions in Global List Actions)

Privilege	Permissions
Policies	• Read • Write* • Modify*
Threats	• Read • Modify*
Zones	• Read • Write* • Modify*
Memory Protection	• Read
CylanceOPTICS Commands	• Read • Write*
CylanceOPTICS Detections	• Read

Syslog configuration in the Cylance console

Before you begin: You need the following information about your QRadar console.

- Protocol (TCP or UDP)
- TLS/SSL enabled or disabled
- IP address or domain address for QRadar
- Listening port for QRadar

1. In the Cylance console, select **Settings > Application**.
2. Enable **Syslog/SIEM**.
3. Select the event types you want to send to your QRadar console.
4. Select IBM QRadar from the SIEM list.
5. Select the protocol, either TCP or UDP.
6. Enable the TLS/SSL feature, if needed.
7. Enter the IP address or domain address of your QRadar console.
8. Enter the listening port for your QRadar console.
9. Optionally, select a severity.
10. Optionally, select a facility.
11. Optionally, enter a custom token.
12. Click **Test Connection** to test the connection between your QRadar console and the Cylance console.
13. Click **Save**.

Get the reports prefix URL and token

The BlackBerry extension allows QRadar users to download the Threat Data Reports from the Cylance console. This requires configuring the Active daily report configuration in the BlackBerry extension by providing the prefix to the Cylance threat report URL and the report token.

1. In the Cylance console, select **Settings > Application**.
2. Copy the threat data report token.
3. Copy the new threat report URL prefix. This is from the https to the V1.
   - Example: https://protect.cylance.com/Reports/ThreatDataReport/V1

     Note: The URL prefix is different by region. The example above is for North America.

Configure the BlackBerry extension for QRadar

1. In QRadar, click Menu > Admin.
2. Click **CylancePROTECT and CylanceOPTICS** under Cylance QRadar App.
3. Click **Add configuration**.
4. Enter the CylancePROTECT API URL for your region.
   The CylancePROTECT API URL varies based on your region.

Item	Description
API URL	• Asia-Pacific - North: https://protectapi-apne1.cylance.com • Asia-Pacific - Southeast: https://protectapi-au.cylance.com • Europe - Central: https://protectapi-euc1.cylance.com • North America: https://protectapi.cylance.com • South America: https://protectapi-sae1.cylance.com • US Government: https://protectapi.us.cylance.com

5. Enter the Tenant ID for your Cylance tenant.
6. Enter the Application ID for your Cylance tenant.
7. Enter the Application Secret for your Cylance tenant.
8. Enter the Report prefix URL for your threat data reports.
9. Enter the Report token for your threat data reports.
10. Enter a friendly name for your Cylance tenant.
    a) Select Set as default tenant if you want this to be your default tenant when you access the QRadar console.
    b) Select Set as active tenant if you to make this tenant's information available in your QRadar console.

    Note: Only the active tenant is used by the BlackBerry extension for QRadar. If no tenant is marked as active, then the tenant marked as default is used for REST API interactions.
11. Select the **Enable Proxy** check box if a proxy server is required for internet access, which is needed to establish communication with the Cylance tenant.
12. Enter the Proxy URL, Username, and Password .

    Include the correct protocol between https or http in the URL, and specify the proxy port. Use the following format for the Proxy URL: {header}://{proxy domain/IP}:{proxy port} (for example, http://10.3.0.22:3128).
13. Click **Save**.

Syslog configuration in the QRadar console

Use the information in the following table to verify the default CylanceRemoteSyslog settings.

1. Go to **Settings > Admin > Log Sources > CylanceRemoteSyslog > Edit**.
2. The expected CylanceRemoteSyslog log source configuration is as follows.

Item	Setting
Log source name	CylanceRemoteSyslog
Log source description	Cylance: Connection to Cylance Tenant
Log source type	Cylance
Protocol configuration	TLS SyslogLog
Source identifier	sysloghost
TLS listen port	6514
Authentication mode	TLS
Certificate type	Generate Certificate
TLS protocol	TLS 1.2 and above
Enabled	Checked
Credibility	10
Coalescing events	Unchecked
Store event payload	Checked
Log source extension	CylanceCustom_ext
Enable multiline	False

Use the dashboard

After installation is complete, you may need to add the Cylance Dashboard to the appropriate user roles so users who are not in the administrator role can see the dashboard.

Fix saved searches in the dashboard

In the dashboard, there is a known issue that may cause some of the saved searches to lose their accumulated data settings. If you find that some of the dashboards are not populating, try the following to correct the issue.

1. In QRadar, navigate to the **Dashboard** tab.
2. Under **Show Dashboard**, select **Cylance Dashboard**.
3. Click the settings button for the dashboard that is not loading.
4. Select **Capture Time Series Data**.
5. Click **Save**.
6. Refresh the browser page. You may need to clear your browser cache.

Use the sample Pulse dashboard

If you use the QRadar Pulse product in your environment, you can download a sample dashboard, upload it to your environment, and try it out.

1. In QRadar, navigate to the **Admin** tab.
2. Scroll down to **BlackBerry Extension for QRadar** and click the **CylancePROTECT and CylanceOPTICS** icon. The Cylance configuration window opens.
3. Click **Sample Dashboard for QRadar Pulse**. The **Cylance Dashboard.json** file is downloaded to your system.
4. Close the **Cylance configuration** window.
5. Open the **Pulse** tab.
6. Under **Dashboard**, select **New Dashboard**.
7. Click **Import Existing**.
8. Select the **Cylance Dashboard.json** file, or drag and drop the file into the **Import Dashboard** window.
9. Under **Dashboard**, select **Cylance Dashboard**.

Cylance dashboard descriptions

The Cylance dashboard for the Pulse tab contains several widgets with different data and graphs.

Item	Description
Application control events	This is a list of all application control events in your organization.
Cylance: Allowed external device distribution	This is a list of all USB mass storage devices that have been allowed to connect to devices in your organization.
Cylance reported threats (active)	This is a list of all active reported threats in your organization.
Devices needing remediation	This is a list of devices that require an action to be taken, like to quarantine or waive a file.
Devices registered (last 3 days)	This is a list of devices that have registered to the console in your organization in the last three days.

Item	Description
Events table	This is a table list of events that have happened in your organization. • **Event name** is the name of the event • **Low level category** is the category of the event • **Device UUID** is the unique ID for the device • **Source IP** is the IP address used by the device • **Threat SHA256** is the SHA256 hash for the threat • **Cylance Event Id** is the unique ID for the event, created by the console • **Source zone** is the zone the device is assigned to • **Username** is the user who was logged on when the event occurred • **More** provides further details about the event, like which product reported the event
Most recent offenses	This is a list of the most recent threats found in your organization. • **Offense name** is the name of the offense • **Magnitude** is the severity, credibility, and magnitude of the offense
Open offenses	This is the total number of events in the open state in your organization.
Optics events	This is a list of CylanceOPTICS events in your organization.
Overall script interpreter distribution	This is the total number of script control events found in your organization, grouped by the script interpreter (active scripts, Powershell scripts, and macros).
Successful exploits	This is the total number of exploits that have successfully run in your organization.
Syslog: Category distribution	This is a pie chart with the percentage distribution of syslog categories reported on in your organization.
Threats in unsafe state	This is the total number of threats that have not been acted upon in your organization.
Top offense categories	This is a graph of the top offenses in your organization, grouped by threat categories.

Specify Device

When interacting with a device, you must identify the device and select it.

1. In QRadar, select **Cylance**.
2. Select **Devices**.
3. For Device Identity, enter information about the device.
   The device information must match the Identity Type.

   Note: For IP addresses, you can use "*" as a wildcard.
4. For Identity Type, select an identity type.

Type	Description
Hostname	This is the DNS hostname for the device. **Note:** While the hostname and device name may match, these are separate and can be different. The hostname is created by the operating system, while the device name can be changed in the Cylance console or API.
MAC Address	This is the MAC address for the device.
Cylance UUID	This is the unique identifier for the device, assigned by the console when the device registered.
IP Address	This is the IP address for the device.

5. Click **Search**.
   This generates a list of devices for Threat Remediation, Exploits Info, and Config & Misc.

Threat Remediation

Use threat remediation to isolate a device from the network or add a file to the waived or quarantined lists on a device.

Note: If the threat remediation device list is empty, you must specify a device first.

1. In QRadar, select **Cylance**.
2. Select **Devices**.
3. Select **Threat Remediation**.
4. Select a device from the Devices list.
5. Select a threat from the Threats list.
6. Select an action from the Remediation list
   You can select the following actions for a threat.

   Tip: If a file has already been remediated, "Quarantined" or "Waived" appears after the file name.

Remediation	Description
Isolate device	This disables network connectivity on the device for the specified amount of time. This includes LAN ports and WiFi adapters. • Expiry Timer is the amount of time the device is isolated from network activity. • Choose is a list that allows you to select minutes or days for the amount of time the device is isolated from network activity. • When specifying a time for the Expiry Timer, the minimum is 5 minutes, the maximum is 3 days. **Note:** To isolate a device, the CylanceOPTICS agent must be installed on that device. This is also known as Lockdown Device.
Waive Threat on Device	This adds the file to the waived list on the selected device.
Quarantine Threat on Device	This adds the file to the quarantine folder on the selected device.

7. Click **Apply Remediation Action**.

   Important: If the Modify permission was granted (see Application privileges), administrators can remove any supported device from the network. Before granting this permission, ensure that all administrators in your organization understand the risks involved.

Exploits Information

Use exploit information to see exploit events on a device.

Note: If the exploits info device list is empty, you must specify a device first.

Item	Description
Pie chart	This pie chart shows the exploit events found on the device and the percentage of occurrences for each event type.
Event Id	This is the unique ID for an exploit event occurrence on the device.
Artifact Name	This is the file name and path associated with the event.
Artifact SHA256 Hash	This is the SHA256 hash for the file.

Click on any of the table rows to get more information about the exploit.

Item	Description
Back to event list	Go back to the table view
Created On	The date and time the memory protection event was created
Name	The path and the name of the file that triggered the event

Item	Description
File Hash ID	The SHA256 hash for the threat
File Version	The version number of the file that triggered the event
DLL Version	The agent version that identified the memory protection event
Process ID	The process ID for the memory protection event
OS Security ID	The security identifier for the user, group, or other security principal; this is generated by the operating system
User Name	The name of the user who was logged in to the device when the memory protection event occurred
Groups	The groups the user belongs to

Configuration and miscellaneous

Use Configuration & miscellaneous to change some device properties and see some device details.

Properties

The properties section displays some device properties, like the device name, zones the device is assigned to, and the device policy.

1. In QRadar, select **Cylance**.
2. Select **Devices**.
3. Specify a device.
4. Click **Configuration & miscellaneous**.
5. Under Properties, select a device from the device list.
6. Click **Get Lockdown History** to view the lockdown history for the device.
   If there is no lockdown history, then nothing will display.
7. To change the device name, enter a new name in the Name field.

   Note: It is recommended to leave the device name as is, unless the field is empty.
8. Select a zone from the zone list.
   You can select multiple zones for a device.
9. Select a policy from the policy list.

   Note: Only one policy can be assigned to a device.
10. Click **Update**.

State & Details

The state and details section displays information related to the device. For example, the lockdown history for the device displays here.

Item	Description
Lockdown History	• **User ID** shows the user ID for the administrator who locked down the device. • **Timestamp** shows the date and time the device was locked down. • **Command** shows the lockdown command that was issued. • **Back to device state** returns you to the device status.

Status	• **ON** displays if the device is online. Click the icon to display the device details.
	• **OFF** displays if the device is offline. Click the icon to display the device details.
	• **?** displays if a device has not been selected. Select a device from the device list.
	• **Last Modified** shows the date and time the device information was last modified.
	• **Hostname** shows the hostname for the device.
	• **IP Addresses** provides a list of all IP address associated with the device.
	• **MAC Addresses** provides a list of all MAC addresses associated with the device.
	• **OS Version** shows the operating system for the device.
	• **Is Safe** shows if a device has no threats or all threats have been mitigated.
	  • **true** means there are not threats on the device that need to be acted upon.
	  • **false** means there are threats on the device that need to be acted upon.
	• **Last User** shows the username of the user who last logged on the device.
	• **Back to device status** returns you to the device status.

Action Log

The action log displays all actions taken and the results while on the devices page.

Note: The action log resets when you navigate away from the page.

Item	Description
No.	This is the action number so you can see the sequence of actions taken.
Context	This provides some information related to the action. For example, when getting device information, the device ID displays in this column.
Action	This is the action taken. For example, "Search device" displays when you search for a device.
Result	This is the result of the action. For example, "OK" means the action was successful.

Global List Actions

Use global list actions to add a file to the global quarantine list or the global safe list.

Note: Adding a file to a global list affects all devices in your organization, unless the file is quarantined or waived at the device-level.

Note: QRadar uses Cylance's "Add to Global List" and "Delete from Global List" APIs. For details on functionality and success/error messaging, see the Cylance API User Guide.

1. In QRadar, select **Cylance**.
2. Select **Threats & global list**.
3. Enter the SHA256 hash for the file.
4. Select an action.

Action	Description
Move to Safe List	This action adds the SHA256 hash for a file to the global safe list. This allows the file to run on any device in your organization.
Move to Quarantine List	This action adds the SHA256 hash for a file to the global quarantine list. This will quarantine the file if it is found on any device in your organization.
Remove from Safe List	This action removes the SHA256 hash from the global safe list.
Remove from Quarantine List	This action removes the SHA256 from the global quarantine list.

5. Click **Apply**.

   Important: If the Write/Delete permissions were granted (see Application privileges), administrators can write to or clear global lists at any time. Before granting this permission, ensure that all administrators in your organization understand the risks involved.

Threat Info Center

The Threat Info Center allows you to enter the SHA256 hash for a file and retrieve information about it. You can also get a list of devices that are impacted by this file.

Item	Description
Enter threat (SHA256)	Enter the SHA256 hash for a file
Get threat info	Displays the threat details
Get devices impacted by threat	Displays a list of devices where the SHA256 hash has been found

Get CylanceOPTICS event details

The extension allows you to view details about a specific CylanceOPTICS event.

1. In QRadar, get a CylanceOPTICS event ID.
   a) Select **Log Activity**.
   b) Click **Quick Searches**.
   c) Select a Cylance preset query.
   d) Hover over **Cylance Event Id (custom)**.
   e) Copy the CylanceOPTICS event ID.
2. Select **Cylance**.
3. Select **CylanceOPTICS events**.
4. Paste the CylanceOPTICS event ID.
5. Click **Get event details**.

CylanceOPTICS detection event details

The CylanceOPTICS detection event details provides the following information.

Item	Description
Name	The name of the event
Severity	The severity level of the event
Detection started	The date and time the detection started collecting data for the event
Detection occurred	The date and time the detection event occurred
Detection received	The date and time the detection event was sent to the console
Instigating process	The process that triggered the detection
Target object	The object targeted by the instigating process
Rule name	The name of the rule that triggered the detection
Rule category	The category the rule belongs to
Rule description	The description for the rule
Rule policy group	The ruleset the rule belongs to
Detector	The product feature that detected the event
Device ID (Impacted)	The unique console ID for the device

Item	Description
Logged on users	A list of logged on users on the impacted device
Applied exceptions	A list of exceptions applied to the detection event
Associated artifacts	The JSON content of the detection rule
Trace	The JSON content for the sensor of the rule
Responses	The JSON of any actions taken by the rule

Zone interactions

Zone summary

The Zone summary is a list of zones created in the console.

Item	Description
Zone name	The name of the zone
Update type	The update type for the zone (Production, Pilot, Test)
Criticality	The criticality of the zone (High, Normal, Low)
Policy	The name of the policy assigned to the zone

View and update zone details

Click on a zone name in the Zone summary table to view details about the zone.

Item	Description
Name	The name of the zone; enter a new zone name to change it
Creation date	The date and time the zone was created
Modified date	The date and time the zone information was last modified
Update type	The update type for the zone (Production, Pilot, Test)
Rule ID	The unique ID for the zone rule
Criticality	The criticality of the zone (High, Normal, Low); select the criticality from the list
Policy	The name of the policy assigned to the zone; you can select a different policy from the list
Update zone info	Updates the zone information

Update a zone

You can update some of the zone information.

1. In QRadar, select **Cylance**.
2. Select **Zones**.
3. Select a zone from the zone list.
4. Under **View/update zone details**, you can update the name, criticality, and policy for the zone.

Task	Steps
Update the zone name	Type a new name for the zone.
Select a different criticality	Select a criticality from the list.
Select a different policy	Select a policy from the list.

5. Click **Update zone info**.

   Important: If the Write/Modify permissions were granted (see Application privileges), administrators can add or modify any existing zone. Before granting this permission, ensure that all administrators in your organization understand the risks involved.

Policy summary

The Policy summary is a list of policies available in your organization.

Item	Description
Policy name	The name of the policy
Number of devices	The number of devices using the policy
Date added	The date the policy was created
Date modified	The date the policy was last updated

Create a policy

You can create a policy and then use that policy on devices. A policy defines how the agent handles malware it encounters. For example, automatically quarantine malware or ignore it if in a specific folder.

Note: This task covers using the create policy Basic view. See JSON view for information on creating a policy using JSON.

1. In QRadar, select **Cylance**.
2. Select **Device policies**.
3. Click **Create policy**.
4. Enter a name for the policy.
5. Enter your console user ID.
6. Select the policy settings. See Policy settings for information about each setting.
7. Click **Create policy**.

   Important: If the Write/Modify permissions were granted (see Application privileges), administrators can add or modify any existing policy. Before granting this permission, ensure that all administrators in your organization understand the risks involved.

Policy settings

Item	Description
Policy name	The name of the policy
User ID	Your unique console ID To get your user ID, do one of the following: • Use the Cylance API (Get Users) • In the console, go to User Management, view your user details, your user ID is at the end of the URL

Item	Description
Prevent unsafe files from executing before they can potentially do damage	Automatically quarantine unsafe files
Prevent abnormal files from executing before they potentially do damage	Automatically quarantine abnormal files **Note:** Prevent unsafe files must be selected before you can select Prevent abnormal files.
Allow auto-deletion of quarantined files	Automatically deletes quarantined files after the set number of days • **Auto-delete after X days (days range 14-365 days)**: Sets the number of days a quarantined file will be retained; the number of days can be between 14 and 365.
Enable auto-upload	Automatically uploads unsafe or abnormal portable executable files (PE) that Cylance has not analyzed before
Enable memory protection	Used to detect or block exploit attempts on the device
Prevent service shutdown from device	Protects the Cylance service from being shutdown manually or by another process
Kill unsafe running processes and their sub-processes	Terminates processes, and their sub-processes, regardless of state when a threat is detected
Background threat detection	Performs a full disk scan to detect and analyze any dormant threats on disk
Watch for new files	The agent will detect and analyze new or modified files for dormant threats
Exclude specific folders (includes subfolders)	Exclude folders, including subfolders, from Background threat detection and Watch for new files • Example for Windows: C:\Test • Example for macOS: /Applications/SampleApplication.app • Example Linux: /opt/application/
Set maximum archive file size to scan: X MB (size range 0-150MB)	Set the maximum archive file size the agent will scan
Enable script control	Alerts or blocks active script and PowerShell scripts from running • Alert: Monitors scripts running in your environment • Block: Blocks scripts from running on devices in your environment

Item	Description
Enable device control	Protects devices by controlling USB mass storage devices connecting to devices
External storage exclusion list	Exclude USB mass storage devices from the device control feature
Add an exclusion	Add an exclusion for a USB mass storage device; vendor ID is required

Policy JSON view

The JSON view displays the policy as a JSON file. This is the same format used for the Policy API.

user_id

Your unique console ID. To get your user ID, do one of the following:

- Use the Cylance API (Get Users)
- In the console, go to User Management, view your user details, your user ID is at the end of the URL

checksum

Use an empty value. This is required when creating a policy.

device_control

Device control allows or blocks access to USB mass storage devices.

Item	Description
control_mode	• **Block** blocks the USB device from connecting to the endpoint • **FullAccess** allows the USB device to connect to the endpoint

Item	Description
device_class	**Note:** All device_class entries must be included in the request. • **AndroidUSB** is a portable device running Android OS, like a smartphone or tablet **Note:** An Android device could connect and be identified as Android, Still Image, or Windows Portable Device. If you want to block Android devices, consider blocking Still Image and Windows Portable Device as well. • **iOS** is an Apple portable device running iOS, like an iPhone or iPad **Note:** iOS devices will not charge when Device Control is enabled and set to Block, unless the Apple device is powered off. Apple includes their charging capability within functions of the device that are required for our iOS device blocking capability. Non-Apple devices do not bundle their charging capability in this manner and are not impacted. • **StillImage** is the device class containing scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers • **USBCDDVDRW** is a USB optical drive • **USBDrive** is a USB hard drive or USB flash drive • **VMWareMount** is the VMware USB Passthrough, which allows a VMware virtual machine client to access USB devices connected to the host • **WPD** is a Windows Portable Device, which uses the Microsoft Windows Portable Device driver technology, such as mobile phones, digital cameras, and portable media players

Item	Description

exclusion_list	The device control exclusion list that allows or blocks access to specific USB mass storage devices
	• **comment** adds detail about the exclusion; this information is optional
	• **control_mode** allows or blocks the specific USB mass storage device
	  • **Block** blocks the USB mass storage device from connecting to the endpoint
	  • **FullAccess** allows the USB mass storage device to connect to the endpoint
	• **product_id** is the product identifier for the USB mass storage device; this information is optional
	• **serial_number** is the serial number for the USB mass storage device; this information is optional
	• **vendor_id** is the vendor identifier for the USB mass storage device; this information is optional
	Note: One way to find the Vendor ID for a USB mass storage device is to enable device control in a policy, assign that policy to an device, then attach the USB mass storage device to the device. You can view external device logs in the Cylance console, on the Protection page or the Device Details page (External Devices tab).

Example	`"exclusion_list": [ { "vendor_id": "1234", "comment": "Test device control exclusion", "serial_number": "987654321", "product_id": "5678:, "control_mode": "FullAccess" } ]`

file_exclusions

Adds file exclusions to the Policy Safe List, under File Actions. The policy safe list are file exclusions specific to the policy, and any devices assigned to the policy will allow the excluded files to run.

Item	Description
category_id	A list of categories to identify the type of file; this information is optional • 1 - None • 2 - AdminTool • 3 - InternalApplication • 4 - CommercialSoftware • 5 - OperatingSystem • 6 - Drivers • 7 - SecuritySoftware
file_hash	The SHA256 hash for the file; this information is optional
file_name	The name of the file being excluded; this information is optional

Item	Description
md5	The MD5 hash for the file; this information is optional
reason	The reason the file was excluded; this information is optional

Example	<pre>"file_exclusions": [
	{
	"reason": "Test Exclusion",
	"category_id": "2",
	"md5": "d41d8cd98f00b204e9800998ecf8427e",
	"file_hash":
	"bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52",
	"file_name": "filename"
	}
	]</pre>

filetype_action

The auto-quarantine of unsafe (threat_files_) and abnormal (suspicious_files)

Item	Description
actions	Allows setting auto-quarantine and auto-upload to enabled or disabled • 0 - Auto-quarantine OFF, auto-upload OFF • 1 - Auto-quarantine ON, auto-upload OFF • 2 - Auto-quarantine OFF, auto-upload OFF **Note:** Use 2 for suspicious_files when threat_files is set to 3 and auto-quarantine for suspicious_files is disabled. • 3 - Auto-quarantine ON, auto-upload ON
file_type	Only has "executable" as an option
suspicious_files	These are abnormal files
threat_files	These are unsafe files

logpolicy

The agent log file settings.

Item	Description
log_upload	• null - Disabled • 1 - Enabled
maxlogsize	The maximum file size (in MB) for a single agent log file
retentiondays	The number of days to save agent log files; log files older than the set number of days will be deleted

memoryviolation_actions

The violation types for memory protection.

Note: All memory_violations and memory_violations_ext must be included in the request.

Item	Description
Action	• **None** means no action is taken when a memory violation is triggered • **Alert** means an alert will display in the console but no action is taken on the memory violation • **Block** means the memory violation is blocked and an alert will display in the console; the process that triggered the memory violation is not terminated • **Terminate** means the memory violation is blocked, the process that triggered the memory violation is terminated, and an alert will display in the console

Item	Description
memory_violations	• **lsassread** (LSASS Read) - The memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords. • **outofprocessallocation** (Remote Allocation of Memory) - A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system. • **outofprocesscreatethread** (Remote Thread Creation) - A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process. • **outofprocessmap** (Remote Mapping of Memory) - A process has introduced code and/or data into another process. This may indicate an attempt to begin executing code in another process and thereby reinforce a malicious presence. • **outofprocessoverwritecode** (Remote Overwrite Code) - A process has modified executable memory in another process. Under normal conditions, executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process. • **outofprocessunmapmemory** (Remote Unmap of Memory) - A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution. • **outofprocesswrite** (Remote Write to Memory) - A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation), but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose. • **outofprocesswritepe** (Remote Write PE to Memory) - A process has modified memory in another process to contain an executable image. Generally, this indicates that an attacker is attempting to execute code without first writing that code to disk. • **overwritecode** (Overwrite Code) - The code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP). • **stackpivot** (Stack Pivot) - The stack for a thread has been replaced with a different stack. Generally, the system will only allocate a single stack for a thread. An attacker would use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP). • **stackprotect** (Stack Protect) - The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).

Item	Description
memory_violations_ext	• **dyldinjection** (DYLD Injection) - An environment variable has been set that will cause a shared library to be injected into a launched process. Attacks can modify the plist of applications like Safari or replace applications with bash scripts, causing their modules to be loaded automatically when an application starts. • **maliciouspayload** (Malicious Payload) - A generic shellcode and payload detection associated with exploitation has been detected. • **trackdataread** (RAM Scraping) - A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS). • **zeroallocate** (Zero Allocate) - A null page has been allocated. The memory region is typically reserved, but in certain circumstances, it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.
memory_exclusion_list	These are the executable files to exclude from memory protection. This must be a relative path to the excluded executable file.

Example	`"memory_exclusion_list": [`
	`  "\\temp"`
	`]`

policy

Various policy settings are contained within this section. Some policy settings are enabled under the policy section and configured in a different section, like device_control and logpolicy.

Item	Description
auto_blocking	Enables or disables the Auto Quarantine setting for Unsafe and Abnormal files. • 0 - Disabled • 1 - Enabled **Note:** filetype_actions must also be set for unsafe (threat_files) and abnormal (suspicious_files) files.
auto_delete	Setting to automatically delete quarantined files after a set number of days. • 0 - Disabled • 1 - Enabled **Note:** If this feature is enabled, set days_until_deleted for the number of days to retain a quarantined file.

Item	Description
auto_uploading	Setting to automatically upload files that Cylance has not seen before. Cylance will perform an analysis on the file and provide details to assist in manual analysis and triage. • 0 - Disabled • 1 - Enabled **Note:** filetype_actions must also be set for unsafe (threat_files) and abnormal (suspicious_files) files for Auto-Upload.
autoit_auto_uploading	The value is 0.
custom_thumbprint	The vaule is null.
days_until_deleted	Setting for the number of days to retain a quarantined file. Quarantined files older than the set number of days will be automatically deleted. • The minimum number of days is 14 • The maximum number of days is 365. **Note:** To use the days_until_deleted feature, the auto_delete setting must be enabled.
device_control	Setting to enable or disable the device control feature.
docx_auto_uploading	The value is 0.
full_disc_scan	Setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the Background Threat Detection (BTD) setting. • 0 - Disabled • 1 - Run recurring (performs a scan every nine days) • 2 - Run once (runs a full disk scan upon installation only)
kill_running_threats	Setting to kill processes and sub-processes regardless of the state when a threat is detected (exe or dll).
logpolicy	The value is 0.
low_confidence_threshold	Setting to adjust the score threshold between unsafe and abnormal files. The default is -600. • A score of -600 to -1000 is unsafe. • A score of 0 to -599 is abnormal. • A score greater than 0 is safe.

Item	Description
memory_exploit_detection	Setting to enable or disable the memory protection feature. • 0 - Disabled • 1 - Enabled **Note:** Also set the memoryviolation_actions (memory_violations, memory_violations_ext, and memory_exclusion_list).
ole_auto_uploading	The value is 0.
optics	Setting to enable or disable CylanceOPTICS. • 0 - Disabled • 1 - Enabled **Note:** Also set the other CylanceOPTICS settings (optics_).
optics_application_control_auto_upload	Setting to allow the automatic uploading of application control related to focus data. • 0 - Disabled • 1 - Enabled
optics_malware_auto_upload	Setting to allow the automatic uploading of threat related focus data. • 0 - Disabled • 1 - Enabled
optics_memory_defense_auto_upload	Setting to allow the automatic uploading of memory protection related focus data. • 0 - Disabled • 1 - Enabled
optics_script_control_auto_upload	Setting to allow the automatic uploading of script control related focus data. • 0 - Disabled • 1 - Enabled
optics_sensors_advanced_executable_parsing	Setting to enable recording data fields associated with portable executable (PE) files, such as file version, import functions, and packer types. This is Enhanced Portable Executable Parsing in the policy settings. • 0 - Disabled • 1 - Enabled

Item	Description
optics_sensors_advanced_powershell_visibility	Setting to enable recording commands, arguments, scripts, and content entered directly into the Powershell console and the Powershell Integrated Script Environment (ISE). • 0 - Disabled • 1 - Enabled
optics_sensors_advanced_wmi_visibility	Setting to enable recording additional Windows Management Instrumentation (WMI) attributes and parameters. • 0 - Disabled • 1 - Enabled
optics_sensors_dns_visibility	Setting to enable recording commands and arguments of commands issued directly or indirectly to the Windows Management Instrumentation (WMI) interpreter. • 0 - Disabled • 1 - Enabled
optics_sensors_enhanced_process_hooking_visibility	Setting to enable recording process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection. • 0 - Disabled • 1 - Enabled
optics_sensors_private_network_address_visibility	Setting to enable recording network connections within the RFC 1918 and RFC 3419 address spaces. • 0 - Disabled • 1 - Enabled
optics_sensors_windows_event_log_visibility	Setting to enable recording Windows Security Events and their associated attributes. • 0 - Disabled • 1 - Enabled
optics_sensors_intel_cryptomining_detection	Setting to enable recording CPU activity using hardware registers for potential cryptomining and cryptojacking activites. • 0 - Disabled • 1 - Enabled
optics_set_disk_usage_maximum_fixed	Setting the maximum amount of device storage reserved for use by CylanceOPTICS, in MB. The minimum value is 500 and the maximum value is 1000.

Item	Description
optics_show_notifications	Setting to enable or disable desktop notifications on the device for CylanceOPTICS events. • 0 - Disabled • 1 - Enabled
pdf_auto_uploading	The value is 0.
powershell_auto_uploading	The value is 0.
prevent_service_shutdown	Setting that protects the Cylance service from being shutdown, either manually or by another process. • 0 - Disabled • 1 - Enabled
python_auto_uploading	The value is 0.
sample_copy_path	Setting to copy all file samples to a network share (CIFS/SMB). Example `{ "name": "sample_copy_path", "value": "\\\\server_name\ \shared_folder" }`
scan_exception_list	Setting to exclude specific folders and subfolders from being scanned by full_disc_scan and watch_for_new_files. Set the value to the absolute path for the excluded files. Example `{ "name": "scan_exception_list", "value": [ "c:\\temp" ] }`
scan_max_archive_size	Setting for the maximum archive file size (in MB) to be scanned. • The value can be 0 to 150. • If set to 0, then archive files will not be scanned.
script_control	Setting to enable or disable the script control feature. • 0 - Disabled • 1 - Enabled

Item	Description
show_notifications	Setting to enable or disable desktop notifications on the device for CylancePROTECT Desktop events. • 0 - Disabled • 1 - Enabled
threat_report_limit	The number of threats to upload to the console.
trust_files_in_scan_exception_list	Setting to allow execution of files in the excluded folders. This is related to the scan_exception_list. • 0 - Disabled • 1 - Enabled
watch_for_new_files	Setting to analyze new or modified executable files for threats. • 0 - Disabled • 1 - Enabled

policy_name

This is the name of the policy. The name must be unique in your tenant.

script_control

These are the policy settings for script control.

Note: script_control must be enabled (set to 1) under policy.

Item	Description

activescript_settings	• **control_mode** - These are the settings for active script.
	  • **Alert** - An alert is sent when an active script event occurs. The active script is allowed to run.
	  • **Block** - The active script is blocked and an alert is sent.

global_settings	• **allowed_folders** - The relative path to scripts that are allowed to run when script control is enabled. Example:
	`"allowed_folders": [ "\\temp_scriptcontrol" ]`
	• **control_mode** - Setting to enable or disable script control for agent version 1370 or lower. To use script control with macros, use agent version 1380 or later.
	  • **Allow** - An alert is sent when an active script or Powershell event occurs. The script is allowed to run.
	  • **Block** - The active script or Powershell is blocked and an alert is sent.

Item	Description

macro_settings	• **control_mode** - Settings for Microsoft Office macros.
	  • **Alert** - An alert is sent when an Office macro event occurs. The macro is allowed to run.
	  • **Block** - The Office macro is blocked and an alert is sent.

powershell_settings	• **console_mode** - The Powershell console is blocked to prevent Powershell command usage, including one-liners. To use this feature, the Powershell control_mode must be set to block.
	• **control_mode**
	  • **Alert** - An alert is sent when a Powershell script event occurs. The Powershell script is allowed to run.
	  • **Block** - The Powershell script is blocked and an alert is sent.

About disabling script control

For agent version 1430 and later, you can disable script control for active script, Powershell, or macros. Disable script control allows the selected script type to run and does not send an alert to the console.

To disable script control for a specific script type, do not include the script type in the Create Policy API request.

Example: Script control for macros is disabled

```
"script_control": {
  "powershell_settings: {
    "control_mode": "Block",
    "console_mode": "Block"
  },
  "global_settings": {
    "control_mode": "Alert",
    "allowed_folders: [
      "\\temp_scriptcontrol"
    ]
  },
  "activescript_settings: {
    "control_mode": "Alert"
  }
}
```

Overview report

The overview report provides some summary details for the console.

Item	Description
Devices (count)	The total number of devices with the agent installed
Threats (count)	The total number of threats found in your tenant
Detections (count)	The total number of detections found in your tenant
Policies (count)	The total number of policies available in your tenant
Zones (count)	The total number of zones available in your tenant
Recent Devices	A list of recently added devices to your tenant
Recent Threats	A list of recent threats discovered in your tenant
Recent Detections	A list of recent detections discovered in your tenant

Daily reports

The daily reports page allows you to download reports from the console in .csv format.

Report	Description
Threat report	This report lists all threats discovered in the organization. This information includes the file name and file status (unsafe, abnormal, waived, and quarantined).
Device report	This report lists all devices in the organization that have an agent installed. This information includes the device name, OS version, agent version, and policy applied.
Events report	This report lists all events related to the threat events graph on the dashboard in the console, for the last 30 days. This information includes the file hash, device name, file path, and the date the event occurred.
Indicators report	This report lists each threat and the associated threat characteristics.
Cleared report	This reports lists threats that were found by CylancePROTECT Desktop but where cleared when: • An administrator deleted the quarantined threats from the console. • A user deleted the threat that was on the disk. This includes if an application other than Cylance deleted the threat.
Policies report	This report lists each policy in your organization and includes the policy settings.

Report	Description
External devices report	This report lists all external device information. This information includes the device type, vendor ID, product ID, serial number, the date when the external device was used, action, and the device name the external devices was used on.
Memory protection events report	This report lists all memory protection related events. This includes the device name, process name, and the action taken, for the last seven days.

Use Log Activity

Use the Log Activity window to view Cylance event information.

1. In QRadar, select **Log Activity**.
2. Click **Quick Searches**, then select a predefined search.
   - Compliance: Source IP's Involved in Compliance Rules - Last 6 Hours
   - Compliance: Username Involved in Compliance Rules - Last 6 Hours
   - Cylance: All Events (Local Replay) - Last 6 Hours
   - Cylance: Allowed Application Control Events - Last 6 Hours
   - Cylance: Devices Needing Remediation - Last 6 Hours
   - Cylance: Top Devices - Last 6 Hours
   - Cylance: Top Optics Events - Last 6 Hours
   - Cylance: Top Successful Exploit Events - Last 6 Hours
   - Cylance: Top Threats - Last 6 Hours
3. Hover over or right-click any of the following fields to view more details.
   - Any IP address
   - Cylance event ID
   - Device ID
   - Device name

     Note: Right-clicking or hovering over the device name to get the device information could return empty if the device name was changed to be different from the hostname.
   - Device UUID
   - File SHA256
   - Host MAC addresses
   - Host IP addresses
   - Instigating Process ImageFileSha256
   - Optics event ID
   - Source MAC
   - Target File Sha256
   - Target Process ImageFileSha256
   - Threat SHA256

Troubleshooting

While this section contains some valuable items to review when experiencing issues with your installation, it is recommended that you review our knowledge base articles for the latest identified issues.

Syslog consumption

Troubleshoot Cylance data from the log activities not populating.

1. Ensure searches are filtered by Log Source Type of Cylance and/or Log Source of CylanceRemoteSyslog.
2. Ensure the CylanceRemoteSyslog Log Source is configured following syslog configuration.
3. Ensure proper network configuration.
   - Click **Test Connection** hyperlink in the Cylance tenant. You should see Test Connection Successful.
   - Ensure port is open to receive syslog data. For example, assuming 6514 is being used, `netstat - an | grep 6514`.
   - Ensure no network or host firewalls are blocking traffic. Layer 7 firewalls may need to be told to expect TLS/SSL traffic.
     - Use a packet sniffer such as Wireshark to verify the connection is made and data is passed.
     - Inspect QRadar error logs in `/var/log/qradar.error` to look for any TLS and/or network related messages.

Cylance application

Use the following troubleshooting steps when there are Cylance application call errors or when no results are found.

1. Ensure at least one tenant configuration has been populated, otherwise an error 500 page will be shown when trying to access the web application. In QRadar, **Settings > Admin > CylancePROTECT and CylanceOPTICS**. Make sure at least one tenant configuration is present.
2. Ensure communication with the Cylance tenant is successful. When creating or editing a tenant configuration, a test connection is made when the configuration is saved. Pay attention to the result notification as it would clearly indicate whether communication is successful.
3. Ensure proper network configuration. Ensure port is open to communicate over port 443 (i.e. HTTPS). Make sure no network or host firewalls are blocking traffic over this port.

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 http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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