Cylance API

User API Guide

Contents

Application management

Console administrators can manage multiple API applications, including the access privileges to your management console data and services such as CylancePROTECT Desktop and CylanceOPTICS.

An application acts as an integration point between the client system and the User API. Through the application, the client system is granted temporary access to act upon resources. Actions will be limited by the scopes associated to the application itself.

Add an application

A tenant can have up to 10 custom applications.

1. Log in to the management console as an administrator. Only administrators can create an application integration.
2. On the menu bar, click **Settings > Integrations**.
3. Click **Add Application**.
4. Type an application name. This must be unique within your organization.
5. Select the access privileges for a console data type. Not selecting any checkboxes for a data type means the application does not have access to that data type.
6. Click **Save**.
7. Copy and paste the application ID and application secret to your API application, or you can click **OK** to close the dialog box. You can view the application ID and application secret from the integrations page.

   Note: There are some API operations listed in the Add Application matrix that can be enabled (Global List - Read and Modify; Policy - Write, Modify, and Delete) but are not available with the initial release. These API operations are currently under development and will be available in a future release.

Data Type	Description
CylanceOPTICS Commands	The CylanceOPTICS device commands Include device lockdown (locking a device, retrieving history) and file retrieval (requesting, checking, and getting results).
CylanceOPTICS Detections	The CylanceOPTICS detection events triggered by the context analysis engine (CAE) allow further automation of analyzing, triaging, and responding to malicious or suspicious activity prevented or detected by CylanceOPTICS.
CylanceOPTICS Exceptions	The CylanceOPTICS detection exceptions add exceptions to detection rules.
CylanceOPTICS Focus Views	The CylanceOPTICS focus views retrieve an information trail starting with the first event related to an artifact from an InstaQuery result or CylancePROTECT Desktop event.
CylanceOPTICS InstaQueries	The CylanceOPTICS InstaQuery allows searching for system artifacts stored locally by CylanceOPTICS (for example, files, registry key persistence points, processes, and so on).

Data Type	Description
CylanceOPTICS Policies	The CylanceOPTICS settings in a policy require the policy settings to also be enabled.
CylanceOPTICS Rule Sets	The CylanceOPTICS set of rules are applied to a policy.
CylanceOPTICS Rules	The CylanceOPTICS detection rules help monitor an organization for security threats or anomalous behavior.
Devices	Devices are systems with a Cylance agent installed. You can get information about devices in your organization. You can also update or remove devices from your organization.
Global Lists	Global lists include the safe list and the global quarantine list. Each global list operation has its own set of required and optional request fields.
Packages Configuration	The CylanceOPTICS packages are sent and stored on devices. CylanceOPTICS packages are not sent to devices by default. Devices must receive a command to download a package.
Packages Deployment	The CylanceOPTICS packages are executed on devices.
Policies	Policies contain the protection settings applied to devices. Policies allow adding and removing devices instead of needing to manually update each device when you want to change the protection settings.
Threats	Threat details provide information about a file as well as reference information about why a file is considered safe or a threat. Use the threats request to get this information.
Users	Users have access to the data in the console, based on the role assigned to them. For example, an administrator can see everything in the console, while a user is limited to the zones to which the user is assigned.
Zones	Each device belongs to at least one zone. Zones are similar to tags and assist in organizing your devices.

Edit an application

1. Log in to the management console as an administrator. Only administrators can edit an application integration.
2. On the menu bar, click **Settings > Integrations**.
3. Click the edit icon for the application you want to change.
4. Edit the privileges, then click **Save Changes**.

Delete an application

1. Log in to the management console as an administrator. Only administrators can delete an application integration.
2. Select **Settings > Integrations**.
3. Click the remove icon for the application you want to remove.
4. Click **Remove Application** to confirm the deletion.

Regenerate an application control

There may be times when it is necessary to regenerate the credentials for an Integration, like when credentials are compromised or stolen. For BlackBerry Integrations, regenerating credentials creates a new application secret; the application ID remains unchanged.

After regenerating credentials, you must update this information in the application used to generate the API access token.

1. Log in to the management console as an administrator. Only administrators can regenerate an application credential.
2. On the menu bar, click **Settings > Integrations**.
3. Click the down arrow to expand the information for the application for which you want to regenerate credentials.
4. Click **Regenerate Credentials**. A confirmation message appears.
5. Click **Yes, Regenerate** to confirm regenerating the credentials.

API in audit logs

The API calls listed below are included in the console audit log (**My Account > Audit Log**) when something is created or updated. In the audit log, the **Who** field displays the application name, not the username.

- **Policy**: create, update, or delete
- **Global List**: add or delete
- **Zone**: create, update, or delete
- **Tenant User**: create, update, or delete
- **Device**: update device, update device threat, or delete device

RESTful API

BlackBerry provides RESTful APIs for registered organizations to manage their resources. To access the User API resources, the client will need to follow the authentication and authorization flow as defined below. This requires the client to send a request to the Auth endpoint, which will return an access token that the client will use for calling all other endpoints.

BlackBerry supports User API resources, including helping users troubleshoot User API requests. BlackBerry does not write or train users on how to create scripts or code.

Authentication

During the step which a client system requests access prior to using BlackBerry resources, there is an independent web API that will handle the authentication process and grant access to the client system. A token based authentication approach is being taken as a means of data transportation between the parties. BlackBerry has adopted JWT (RFC 7519) as the token format for its simplicity as well as its capabilities for digital signature.

The following actors exist in the authentication workflow:

- Authentication Token: Created and signed by the client system to perform an authentication request, it is in this request where the application is indicated.
- Authentication Endpoint: Part of the BlackBerry Auth web API which will handle the authentication requests coming from client systems, there will be a particular endpoint to handle JWT tokens.
- Access Token: If authentication is successful and the client system is granted access to the requested application, a token representing this identity and some key attributes will be returned as a JWT token.

Authentication token

The authentication token contains the ID of the application to which a client system is requesting access. The application contains two attributes: application ID and application secret, the latter is cryptographic nonce used to sign the token, thus ensuring the authenticity of the caller and therefore, it must be shared between client and server. The authentication endpoint has a mechanism to verify the signature and eventually proceed to grant access to the application, if the client request is indeed allowed.

The client will create the authentication token by indicating the application ID as a claim and sign it using the application secret. The authentication token must have the following claims, which are registered and conform to the JWT standard:

Claim	Type	Description
Registered Claims		
exp	NumericDate	Date and time when the token expires and is no longer valid for processing. This is Unix epoch time in seconds. The longest time-span honored by the service is 30 minutes from the value specified in the iat claim. Specifying a longer time-span will result in an HTTP 400 (Bad Request) response from the server.
iat	NumericDate	Time when the token was issued, measured by Unix epoch time in seconds.

Claim	Type	Description
iss	StringOrUri	Represents the principal issuing the token, which is http://cylance.com.
jti	String	Unique ID for the token, which can be used to prevent reply attacks.
sub	StringOrUri	Principal subject to the claim, which this would hold our application ID.
Custom Claims		
src	String	Include the source API in the token which allows you to audit where API calls originated. this parameter validation requirements: • alphanumeric and double-byte characters are allowed • should remove leading and trailing whitespaces • needs to filter for potential XSS/injection attack strings and other special characters This field can be a source computer name, IP address, or an App ID (Settings > Integrations).
tid	String	Tenant ID (available on the Integrations page in the console).

For example:

Authentication token - adding required token claims

```
DateTime now = DateTime.UtcNow;
long unixTimestamp = now.ToUnixTimestamp();

token.Claims.Add("iss", "http://cylance.com");
token.Claims.Add("iat", now.ToUnixTimestamp()););
token.Claims.Add("exp", now.AddMinutes(1).ToUnixTimestamp());
token.Claims.Add("sub", "k45f6798092hjdhs836h");
token.Claims.Add("jti", "k45f6798092hjdhs836h+d82c7976-
ef46-47b6-80ce-4dda3c91bba3");
token.Claims.Add("tid", "f00e9987-ee61-57b7-80cf-5eeb3d02ccb4”);
token.claims.Add(“src”, “Example_computer_name”)
```

Generate the authentication and access tokens

The authentication token can be generated using Python. You can use the Python example below, adding the required token claims that you need. BlackBerry does have a knowledge base article with an example for installing Python and PyJWT on Windows; this example is provided as is and there is no guarantee the example will work in your environment.

Software requirements:

- Python 3.9 (latest version recommended)
- PyJWT package (pip install PyJWT)
- Requests package (pip install requests)

Note:

- Copying the Python example from the PDF requires proper formatting in Python due to the extra line breaks that can cause an error. Use the example in the HTML version of this guide.
- Example using C# is available upon request.

Python Example

```
# WARNING: Copying this example from the PDF requires proper
# formatting in Python due to the extra lines breaks that
# can cause an error.
# RECOMMENDED: Copy the example using the HTML version of this guide.
# Note: In Python 3.9, encoding does not need the .decode option.
# The .decode option is available as a comment, in case you need it.

import jwt # PyJWT version 1.7.1 as of the time of authoring.
import uuid
import requests # requests version 2.22.0 as of the time of authoring
import json
from datetime import datetime, timedelta

# 30 minutes from now
timeout = 1800
now = datetime.utcnow()
timeout_datetime = now + timedelta(seconds=timeout)
epoch_time = int((now - datetime(1970, 1, 1)).total_seconds())
epoch_timeout = int((timeout_datetime - datetime(1970, 1, 1)).total_seconds())

jti_val = str(uuid.uuid4())
tid_val = "" # The tenant's unique identifier.
app_id = "" # The application's unique identifier.
app_secret = "" # The application's secret to sign the auth token with.

AUTH_URL = "https://protectapi.cylance.com/auth/v2/token"

claims = {
    "exp": epoch_timeout,
    "iat": epoch_time,
    "iss": "http://cylance.com",
    "sub": app_id,
    "tid": tid_val,
    "jti": jti_val
    # The following is optional and is being noted here as an example on how one
 can restrict
    # the list of scopes being requested
    # "scp": ["policy:create","policy:list","policy:read","policy:update"]
}

encoded = jwt.encode(claims, app_secret, algorithm='HS256')
print ('auth_token:\n' + encoded + "\n")

payload = {"auth_token": encoded}
headers = {"Content-Type": "application/json; charset=utf-8"}
resp = requests.post(AUTH_URL, headers=headers, data=json.dumps(payload))

print("http_status_code: " + str(resp.status_code))
print("access_token:\n" + json.loads(resp.text)['access_token'] + "\n")
```

Token lifecycle

An authentication token should be used only once per request. This means the same token should not be usable for more than one request to prevent impersonation attempts. The jti attribute uniquely identifies the token. It can be used to keep track of all the tokens and prevent them from being reused. To ensure that the authentication token can be used only once, an expiration is enforced on the token. This means the token is usable within a few minutes or less.

Request and response model

Service endpoint	/auth/v2/token
Example	https://protectapi.cylance.com/auth/v2/token
HTTP method	POST
Request headers	Accept: application/json Content-Type: application/json Authorization: Bearer *JWT Token returned by Auth API* with the user:create scope encoded.
Request	`{ "title": "Authorization Request", "type": "object" "properties": { "auth_token": { "type": "" "description": "token representing authorization request" } }, "request": ["auth_token"] }`

Service endpoint

The service endpoint address can contain a region code to identify the set of servers to which your organization belongs. North America and US Government have a different format. See service endpoint column below for examples:

Region	Code	Service Endpoint with Region Code
Asia-Pacific - North	apne1	https://protectapi-apne1.cylance.com/
Asia-Pacific - Southeast	au	https://protectapi-au.cylance.com/
Europe - Central	euc1	https://protectapi-euc1.cylance.com/
North America	—	https://protectapi.cylance.com/
South America	sae1	https://protectapi-sae1.cylance.com/

Region	Code	Service Endpoint with Region Code
US Government	us	https://protectapi.us.cylance.com/

Find file checksum

When uploading a Package, the SHA256 hash is required for the checksum.

OS	Steps
Windows	CertUtil is a pre-installed Windows utility. This utility can provide the hash checksum for a file. 1. Open the **Command Prompt**. For Windows 10, click the Start menu, type `cmd`, then click Command Prompt. 2. Type CertUtil -hashfile pathtofile hashtype, then press **Enter**. a. Replace <pathtofile> with the path to the file to check. Example: c:\test \hello_world.py. b. Replace <hashtype> with the hash format. Example: SHA256. Valid hash formats include: MD2, MD4, MD5, SHA1, SHA256, SHA384, and SHA512. c. Example command: `CertUtil -hashfile c:\test\hello_world.py SHA256` 3. Copy the SHA256 hash.
MacOS	Figure - Use CertUtil to Find Checksum 1. Open **Terminal**. Search for Terminal in Spotlight or Launchpad, or open using **Applications > Utilities**. 2. Type shasum -a 256 <pathtofile>, then press **Return**. 3. Copy the SHA256 hash.
Linux	Figure - Use CertUtil to Find Checksum 1. Open **Terminal**. 2. Type sha256sum <pathtofile>, then press **Enter**. 3. Copy the SHA256 hash.

Threat classifications

In the management console, there exists classification information for threats reported in your organization.

The following is a list of possible file status entries that may appear under classification for each threat, along with a brief description of each entry.

File Unavailable: Due to an upload constraint (example: file is too large to upload), the file is unavailable for analysis. If classification is necessary, contact BlackBerry Support for an alternate method to transfer the file for analysis.

Unknown (blank entry): The file has not been analyzed by the BlackBerry Research team. Once the file is analyzed, the classification will be updated with a new status.

Trusted - Local: The file has been analyzed by the BlackBerry Research team and has been deemed safe (not malicious, not a PUP). A file identified as Trusted - Local can be globally safe listed so that the file will be allowed to execute and not generate any additional alerts if found on other devices within your organization. The reason

for the "Local" designation is due to the fact that the file did not come from a trusted source (such as Microsoft or other trusted installers) and therefore cannot be added to our trusted cloud repository.

PUP: The file has been identified as a Potentially Unwanted Program (PUP). This indicates that the program may be unwanted, despite the possibility that users consented to download it. Some PUP's may be permitted to run on a limited set of systems in your organization (example: a VNC application allowed to run on Domain Admin devices). A console administrator can choose to waive or block PUP's on a per device basis or globally quarantine or safe list the file based on company policies. Depending on how much analysis can be performed against a PUP, further subclassification may be possible. Those subclasses are shown below and will aid an administrator in determining whether a particular PUP should be blocked or allowed to run.

Subclass	Definition	Examples
Adware	Adware is a technology that provides advertisements (example: pop-ups) or provide bundled third-party add-ons when installing an application. This usually occurs without adequate notification to the user about the nature or presence of the add-on, control over installation, control over use, or the ability to fully uninstall the add-on.	Gator, Adware Info
Corrupt	This is any executable that is malformed and unable to run.	
Game	These are technologies that create an interactive environment with which a player can play.	Steam Games, League of Legends
Generic	This is any PUP that does not fit into an existing category.	
HackingTool	These are technologies that are designed to assist hacking attempts.	Cobalt Strike, MetaSpl0it
Portable Application	This is a program designed to run on a computer independently, without needing installation.	Turbo
Scripting Tool	This is any script that is able to run as if it were an executable.	AutoIT, py2exe
Toolbar	These are technologies that place additional buttons or input boxes on-screen within a UI.	Nasdaq Toolbar, Bring Me Sports
Other	This is a category for things that don't fit anything else, but are still PUP's. There are a lot of different PUP's, most of which are not malicious but serveral that should still be brought to the attention of the System Administrators through our product. Usually because they have potentially negative uses or negatively impact a system or network.	

Dual Use: Dual Use indicates the file can be used for malicious and non-malicious purposes. Caution should be used when allowing the use of these files in your organization.

Subclass	Definition	Examples
Crack	These are technologies that can alter (or crack) another application in order to bypass licensing limitations or Digital Rights Management (DRM) protection.	

Subclass	Definition	Examples
Generic	This is any Dual Use tool that does not fit into an existing sublcass.	
KeyGen	These are technologies which can generate or recover/ reveal product keys that can be used to bypass Digital Rights Management (DRM) or licensing protection of software and other digital media.	
MonitoringTool	These are technologies that track a user's online activities without awareness of the user by logging and possibly transmitting logs of one or more of the following: • User keystrokes • Email messages • Chat and instant messaging • Web browsing activity • Screenshot captures • Application usage	Veriato 360, Refog Keylogger
Pass Crack	These are technologies that can reveal a password or other sensitive user credentials either by cryptographically reversing passwords or by revealing stored passwords.	l0phtcrack, Cain & Abel
RemoteAccess	These are technologies that can access another system remotely and administer commands on the remote system, or monitor user activities without user notification or consent.	Putty, PsExec, TeamViewer
Tool	These are programs that offer administrative features but can be used to facilitate attacks or intrusions.	Nmap, Nessus, P0f

Malware: The BlackBerry Research team has definitively identified the file as a piece of malware; the file should be removed or quarantined as soon as possible. Verified malware can be further subclassified.

Subclass	Definition	Examples
Backdoor	This is malware that provides unauthorized access to a system, bypassing security measures.	Back Orifice, Eleanor
Bot	This is malware that connects to a central Command and Control (C&C) botnet server.	QBot, Koobface
Downloader	This is malware that downloads data to the host system.	Staged-Downloader
Dropper	This is malware that installs other malware on a system.	—
Exploit	This is malware that attacks a specific vulnerability on the system.	—

Subclass	Definition	Examples
FakeAlert	This is malware that masquerades as legitimate security software to trick the user into fixing fake security problems at a price.	Fake AV White Paper
Generic	This is any malware that does not fit into an existing category.	—
InfoStealer	This is malware that records login credentials and/or other sensitive information.	Snifula
Parasitic	These are parasitic viruses, also known as file viruses, spread by attaching themselves to programs. Typically when you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program.	—
Ransom	This is malware that restricts access to system or files and demands payment for removal of restriction, thereby holding the system for ransom.	CryptoLocker, CryptoWall
Remnant	This is any file that has malware remnants after removal attempts.	—
Rootkit	This is malware that enables access to a computer while shielding itself or other files to avoid detection and/or removal by administrators or security technologies.	TDL, Zero Access Rootkit
Trojan	This is malware that disguises itself as a legitimate program or file.	Zeus
Virus	This is malware that propogates by inserting or appending itself to other files.	Sality, Virut
Worm	This is malware that propagates by copying itself to another device.	Code Red, Stuxnet

Scope values for authentication token

The following are scope values and descriptions related to the Authentication Token. See Authentication token.

Scope	Description
application:create	Create a new application.
application:read	Request a single application.
application:list	Request a list of applications.
application:update	Update an application.
application:regenerate	Regenerate an application secret.

Scope	Description
application:delete	Delete an application.
device:create	Create a new device resource.
device:read	Request a single device resource.
device:list	Request a list of device resources.
device:update	Update a device resource.
device:delete	Delete a device resource.
device:threatlist	Retrieve the list of threats found on a device.
threat:update	Update a threat found on a device.
globallist:create	Add a new entry to the global quarantine list or global safe list.
globallist:list	Request a list of file hashes.
globallist:delete	Remove a convicted threat to either the global quarantine list or the global safe list.
memoryprotection:read	Request a single Memory Protection event.
memoryprotection:list	Request a list of Memory Protection events.
opticscommand:read	Request a single device command resource.
opticscommand:list	Request a list of device command resources.
opticscommand:create	Create a new device command.
opticsdetect:read	Request a single detection resource.
opticsdetect:list	Request a list of detection resources.
opticsdetect:update	Update a detection resource.
opticsdetect:delete	Delete a detection resource.
opticsexception:read	Request a single detection exception.
opticsexception:list	Request a list of detection exceptions.
opticsexception:create	Create a new detection exception.
opticsexception:update	Update a detection exception.
opticsfocus:read	Request a single focus view resource.

Scope	Description
opticsfocus:list	Request a list of focus view resources.
opticsfocus:create	Create a new focus view.
opticspkgconfig:create	Create a new package resource.
opticspkgconfig:read	Request a single package resource.
opticspkgconfig:list	Request a list of package resources.
opticspkgconfig:delete	Delete a package resource.
opticspkgdeploy:create	Create a new package execution resource.
opticspkgdeploy:read	Request a single package execution resource.
opticspkgdeploy:list	Request a list of package execution resources.
opticspkgdeploy:delete	Delete a package execution resource.
opticspolicy:read	Request a single CylanceOPTICS policy resource.
opticspolicy:list	Request a list of CylanceOPTICS policy resources.
opticspolicy:create	Create a new CylanceOPTICS policy.
opticsrule:read	Request a single rule resource.
opticsrule:list	Request a list of rule resources.
opticsrule:create	Create a new rule.
opticsrule:update	Update a rule.
opticsruleset:read	Request a single rule set resource.
opticsruleset:list	Request a list of rule set resources.
opticsruleset:create	Create a new rule set.
opticsruleset:update	Update a rule set.
opticsruleset:delete	Delete a rule set.
opticssurvey:read	Request a single InstaQuery resource.
opticssurvey:list	Request a list of InstaQuery resources.
opticssurvey:update	Update an InstaQuery.

Scope	Description
opticssurvey:delete	Delete an InstaQuery.
policy:read	Request a single policy resource.
policy:list	Request a list of policy resources.
policy:create	Create a new policy.
policy:update	Update a policy.
policy:delete	Delete a policy.
threat:read	Request a single threat resource.
threat:list	Request a list of threat resources.
threat:devicelist	Request a list of devices where a particular threat was convicted.
user:create	Create a new user resource.
user:read	Request a single user resource.
user:list	Request a list of user resources.
user:update	Update a user.
user:delete	Delete a user.
zone:create	Create a new zone resource.
zone:read	Request a single zone resource.
zone:list	Request a list of zone resources.
zone:update	Update a zone.
zone:delete	Delete a zone.

Authorization

In response to the authentication request, the client will receive a response that contains at least the access token. The access token will contain the scopes that will dictate what can or cannot be done. This token is signed by the server and the client will merely echo it on every request as it tries to access resources.

The access token represents the identity of the requester as well as some attributes like scopes. This token will have an expiration and should be sent on every request in the authorization request header. Failing to do so will result in an HTTP/1.1 401 unauthorized response. Should the token be provided and prove to be legitimate but the server finds the action the caller is trying to attempt is not allowed (found in the scopes granted), an HTTP/1.1 403 forbidden will be returned.

Access token

The access token represents a grant to access BlackBerry resources. It contains information about the identity of the caller (application) as well as control information form the token itself, for instance, date it was issued and expiration. This token is also responsible for holding all scopes that would be used by our system to validate actions attempted to be taken against BlackBerry resources.

There is an expiration associated to this token. The expiration time will be set during token creation on the server side. After the token expires, the server will respond with HTTP/1.1 401 unauthorized indicating to the caller to authenticate again with a new access token.

Response status codes

Each API request will receive a response with a JSON payload and a standard HTTP status code. Some API request sections include additional response status descriptions (specific to that request) to help you troubleshoot issues.

Status Code	Description
200 - OK	This was a successful call and operation. The response payload will be JSON, structured according to the nature of the request.
400 - Bad Request	There was a problem with the structure of the request or the payload. If determinable, the response payload will identify the failure in the request. A common case of this type of error is malformed JSON in the request body. A JSON validator can be used to troubleshoot these issues.
401 - Unauthorized	Invalid credentials were passed or some other failure in authentication.
403 - Forbidden	The request has been successfully authenticated, but authorization to access the requested resource was not granted.
404 - Not Found	A request was made for a resource that doesn't exist. Common causes are either an improperly formed URL or an invalid API key.
409 - Conflict	A request was made to create or update an aspect of the resource that conflicts with another. The most common reason for this code is a tenant name or user email that is already in use.
429 - Too Many Requests	Too many requests were made within a given amount of time. This is a rate limiting feature to stop flooding the server with requests. See API Rate Limit below for more information.
500 - Internal Server Error	This is a catch-all code response for any unhandled error that has occurred on the server. Contact BlackBerry Support for help with this issue.
501 - Not Implemented	A request was made against a resource with an operation that has yet to be implemented. Such operations should be identified accordingly in documentation.
Other	Contact BlackBerry Support if you encounter any status codes that are not on this list.

API rate limit

The rate limiting for API endpoints is 100,000 requests per day, or about 20 requests per second. If a tenant exceeds these limits, they will receive a 429 error (too many requests). If you encounter a 429 error, wait 60 seconds before retrying the API request.

The purpose of a rate limit is to maintain a good user experience for all API users. Without a rate limit, API endpoints can flood the server with requests that overwhelm the system and negatively impact all users.

API Tools

The following is information about some REST and JSON tools that might help you when using the User APIs.

BlackBerry supports User API resources, including helping users troubleshoot User API requests. BlackBerry does not write or train users on how to create scripts or code (like using Python).

Tool	Description
REST clients	Although the intent of the User API is to facilitate easy integration of BlackBerry and other systems through the organization's developed code, using or testing the User API doesn't require any specific programming knowledge. Free tools are available for download that allow you to make ad hoc REST requests to the User API. Some examples are: • Fiddler: Free web debugging proxy. Also has an easy-to-use composer and replay features for HTTP requests. • Postman: Google Chrome browser extension designed for testing REST APIs. There are also native Windows, macOS, and Linux clients available.
JSON validators	User API requests and responses use JSON for the body payload. If the body used in the request doesn't conform to proper JSON formatting, it will result in an HTTP response of 400 - Bad Request. To ensure that your JSON is properly formatted, use one of these free, popular tools: • JSON Formatter and Validator: Online, simple interface with options to define and transform the output according to the desired level of white space. Provides highlights and informative descriptions of errors. • Notepad++: Freeware text editor. Supports a wide variety of plug-in extensions, including various JSON formatting and validation tools (like JSTool and JSON Viewer).

About device ID

When attempting to query a CylanceOPTICS API call that utilizes a device ID value, be aware of the following:

See the following table to reference the format for the CylanceOPTICS API device ID value:

Product	Format example
CylanceOPTICS	45E07F34E76B4A9EB167D6D0C510D6BA (upper case without dashes) Passing the device ID value as the CylancePROTECT Desktop format will return an HTTP 200 status, as if the call was successful, but you will receive an incorrect response.
CylancePROTECT Desktop	45e07f34-e76b-4a9e-b167-d6d0c510d6ba (lower case with dashes) To obtain the device ID, you must query the CylancePROTECT Desktop API, then format the device ID to match the CylanceOPTICS format (see example above). This query can be found in the Device API section of this document. Use the Get Devices and Get Device requests from the guide. The device ID value is the field titled "id".

About zone ID

When attempting to query a CylanceOPTICS API call that utilizes a zone ID value, be aware of the following:

See the following table to reference the CylanceOPTICS API zone ID value:

Product	Format example
CylanceOPTICS	D27FF5C45C0D4F56A00DA1FB297E440E (upper case without dashes) Passing the zone ID value as the CylancePROTECT Desktop format will return an HTTP 200 status, as if the call was successful, but you will receive an incorrect response.
CylancePROTECT Desktop	d27ff5c4-5c0d-4f56-a00d-a1fb297e440e (lower case with dashes) To obtain the zone ID, you must query the CylancePROTECT Desktop API, then format the zone ID to match the CylanceOPTICS format (see example above). This query can be found in the zone API section of this document. Use the Get zones and Get zone requests from the guide.

User API

Users have access to the management console and what they can view depends on the permissions they have.

Create user

Create a new console user. This requires a unique email address for the user being created.

Service Endpoint	/users/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/users/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:create encoded.

Request

```
{
    "email": "testuser@email.com",
    "user_role": "00000000-0000-0000-0000-000000000001",
    "first_name": "Test",
    "last_name": "User",
    "zones": [
        {
            "id": "d27ff5c4-5c0d-4f56-a00d-a1fb297e440e",
            "role_type": "00000000-0000-0000-0000-000000000002"
        }
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
email	(Required) This is the user's email address, which must be unique.

Field Name	Description
first_name	(Optional) This is the user's first name, which if specified, must be less than 64 characters.
last_name	(Optional) This is the user's last name, which if specified, must be less than 64 characters.
user_role	(Required) This is the user's role in the console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Read-Only: 00000000-0000-0000-0000-000000000003

zones	These are the zones that the user has access to as an array of elements:
	• id: Unique identifier for the zone
	• role_type: User's role for this particular zone
	  • Zone Manager: 00000000-0000-0000-0000-000000000001
	  • User: 00000000-0000-0000-0000-000000000002
	If the user is an Administrator, the zones array is not required.

To create a zone manager, set the user_role to *User* and assign a zone or zones to the user via the zones parameter. Setting the user_role to *Read-Only* and using the zones parameter will result in a bad request error.

Note that if you are creating a Zone Manager, the 'email' and 'user_role' parameters are mandatory.

Response JSON schema

Field Name	Description
date_created	This is the date and time (in UTC) the console user was created.
date_email_confirmed	This is the date and time (in UTC) when the user confirmed the email provided. This should be null because the user account was recently created.
date_last_login	This is the date and time (in UTC) the user last logged in to the console. This should be null because the user account was recently created.
date_modified	This is the date and time (in UTC) the console user information was last updated.
default_zone_role_name	This is the name of the role for the user in the zone.
default_zone_role_type	This is the unique identifier for the user's default role when assigned to a zone: • None: 00000000-0000-0000-0000-000000000000 • Zone Manager: 00000000-0000-0000-0000-000000000001 • User: 00000000-0000-0000-0000-000000000002
email	This is the user's email address.

Field Name	Description
first_name	This is the user's first name.
has_logged_in	This should be false because the user account was recently created.
id	This is the user's unique identifier for the console.
last_name	This is the user's last name.
role_name	This is the name of the user's role in the console.
role_type	This is the unique identifier defining the user's role in the console: • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Read-Only: 00000000-0000-0000-0000-000000000003 • Zone Manager: 00000000-0000-0000-0000-000000000004 To create a Zone Manager, set the user_role to *User* and assign a zone or zones to the user via the zones parameter. Setting the user_role to *Read-Only* and using the zones parameter will result in a bad request error.

zones	These are the zones that the user has access to as an array of elements:
	• id: Unique identifier for the zone
	• role_type: User's role for this particular zone
	  • None: 00000000-0000-0000-0000-000000000000
	  • Zone Manager: 00000000-0000-0000-0000-000000000001
	  • User: 00000000-0000-0000-0000-000000000002
	• role_name: Name of the user's role in the zone
	If the user is an administrator, the zones array will display empty brackets [ ].

Get users

Request a page with a list of console user resources belonging to a tenant, sorted by the created date, in descending order (most recent user registered listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 10 respectively. The maximum page size that can be specified is 200 entries per page.

Service Endpoint	/users/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	return the first page with up to 100 users: https://protectapi.cylance.com/users/v2?page=1&page_size=100
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
date_created	This is the date and time (in UTC) the console user was created.
date_email_confirmed	This is the date and time (in UTC) when the user confirmed the email provided.
date_last_login	This is the date and time (in UTC) the user last logged in to the console.
date_modified	This is the date and time (in UTC) the console user information was last updated.
default_zone_role_name	This is the name of the role for the user in the zone.
default_zone_role_type	This is the unique identifier for the user's default role when assigned to a zone. • None: 00000000-0000-0000-0000-000000000000 • Zone Manager: 00000000-0000-0000-0000-000000000001 • User: 00000000-0000-0000-0000-000000000002
email	This is the user's email address.
first_name	This is the user's first name.
has_logged_in	This is true if the user has successfully logged in to the console.
last_name	This is the user's last name.
page_number	This is the page number requested.
page_size	This is the the page size requested.
role_type	This is the unique identifier defining the user's role in the console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Read-Only: 00000000-0000-0000-0000-000000000003 • Zone Manager: 00000000-0000-0000-0000-000000000004

Field Name	Description
tenant_id	This is the organization's unique identifier for the console.
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.
user_id	This is the user's unique identifier for the console.

zones	These are the zones that the user has access to as an array of elements.
	• id: Unique identifier for the zone
	• role_type: User's role for this particular zone
	  • None: 00000000-0000-0000-0000-000000000000
	  • Zone Manager: 00000000-0000-0000-0000-000000000001
	  • User: 00000000-0000-0000-0000-000000000002
	• role_name: Name of the user's role in this zone

Get user

Request information for a specific console user resource belonging to a tenant.

Service endpoint	/users/v2/{user_id | user_email_address}
Optional query string parameters	—
Example	• user_id: https://protectapi.cylance.com/users/v2/a2c0ac7a-a63d-4583-b646-ae10db9c9768 • user_email: https://protectapi.cylance.com/users/v2/username@email.com
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
date_created	This is the date and time (in UTC) the console user was created.
date_email_confirmed	This is the date and time (in UTC) when the user confirmed the email provided.
date_last_login	This is the date and time (in UTC) the user last logged in to the console.
date_modified	This is the date and time (in UTC) the console user information was last updated.
default_zone_role_name	This is the name of the role for the user in the zone.
default_zone_role_type	This is the unique identifier for the user's default role when assigned to a zone. • None: 00000000-0000-0000-0000-000000000000 • Zone Manager: 00000000-0000-0000-0000-000000000001 • User: 00000000-0000-0000-0000-000000000002
email	This is the user's email address.
first_name	This is the user's first name.
has_logged_in	This is true if the user has successfully logged in to the console.
id	This is the user's unique identifier for the console.
last_name	This is the user's last name.
role_name	This is the name of the role.
role_type	This is the unique identifier defining the user's role in the console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Read-Only: 00000000-0000-0000-0000-000000000003 • Zone Manager: 00000000-0000-0000-0000-000000000004
tenant_id	This is the organization's unique identifier for the console.
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.

zones	These are the zones that the user has access to as an array of elements.
	• id: unique identifier for the zone
	• role_type: user's role for this particular zone
	  • None: 00000000-0000-0000-0000-000000000000
	  • Zone Manager: 00000000-0000-0000-0000-000000000001
	  • User: 00000000-0000-0000-0000-000000000002
	• role_name: Name of the user's role in this zone.

Update user

Update an existing console user resource.

Service endpoint	/users/v2/{user_id}
Optional query string parameters	—
Example	user_id: https://protectapi.cylance.com/users/v2/a2c0ac7a-a63d-4583-b646-ae10db9c9768
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:update scope encoded

Request

```
{
    "email": "testuser@email.com",
    "user_role": "00000000-0000-0000-0000-000000000001",
    "first_name": "Test",
    "last_name": "User",
    "zones": [
        {
            "id": "d27ff5c4-5c0d-4f56-a00d-a1fb297e440e",
            "role_type": "00000000-0000-0000-0000-000000000002"
        }
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
email	This is the user's email address.
first_name	This is the user's first name.
last_name	This is the user's last name.

Field Name	Description
user_role	This is the unique identifier defining the user's role in the console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Read-Only: 00000000-0000-0000-0000-000000000003

zones	These are the zones to which the user has access as an array of elements.
	• id: Unique identifier for the zone
	• role_type: User's role for this particular zone
	  • None: 00000000-0000-0000-0000-000000000000
	  • Zone Manager: 00000000-0000-0000-0000-000000000001
	  • User: 00000000-0000-0000-0000-000000000002
	Note that administrators have zone management privileges in all zones; trying to use the zones parameter to explicitly set an administrator to be a Zone Manager will result in an error.
	If you are updating a user to a Zone Manager, the zones array is required.

To update a zone manager or change a user to a zone manager, set the user_role to User and set the zones role_type to Zone Manager.

Note that if you are updating a user to a Zone Manager, the 'email' and 'user_role' parameters are mandatory.

Delete user

Delete an existing console user resource.

Service endpoint	/users/v2/{user_id}
Optional query string parameters	—
Example	user_id: https://protectapi.cylance.com/users/v2/a2c0ac7a-a63d-4583-b646-ae10db9c9768
Method	HTTP/1.1 DELETE
Request headers	Authorization: Bearer *JWT Token returned by Auth API* with the user:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Send invite email

Request the console login invitation email to be resent to a user who has not logged into the console yet. The user must already be created, either using the create user API or using the console.

Service endpoint	/users/v2/{user_email_address}/invite
Optional query string parameters	—
Example	https://protectapi.cylance.com/users/v2/username@email.com/invite
Method	HTTP/1.1 POST
Request headers	Authorization: Bearer *JWT Token returned by Auth API* with the user:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Send request password email

Request for the console reset password email to be sent or resent to an existing console user.

Service endpoint	/users/v2/{user_email_address}/resetpassword
Optional query string parameters	—
Example	https://protectapi.cylance.com/users/v2/username@email.com/resetpassword
Method	HTTP/1.1 POST
Request headers	Authorization: Bearer *JWT Token returned by Auth API* with the user:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Device API

Devices are endpoints with Cylance applications installed.

Get devices

Request a page with a list of device resources belonging to a tenant. The page number and page size parameters are optional. When the values are not specified, these default to 1 and 100 respectively. The maximum page size that can be specified is 10000 entries per page.

Service Endpoint	/devices/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	Return the first page with 100 devices: https://protectapi.cylance.com/devices/v2?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
created	This is the date and time (in UTC) when the device record was created.
days_to_deletion	This is the number of days before a device will be deleted. Enable automated device lifecycle management and remove inactive devices must both be enabled under device management. If enable automated lifecycle management is enabled and remove inactive devices is disabled, this field displays Unknown.
deviceCarrier	This is the name of the device's service provider (for example, AT&T or Verizon).
deviceType	This is the the type of device (for example, desktop or mobile).

Field Name	Description
dlcm_status	This is the device lifecycle management status of the device, which shows the device as included or excluded from device lifecycle management. If device lifecycle management is disabled, the status shows as unknown.
id	This is the unique identifier of the endpoint.
ipAddresses	This is the list of IP addresses for the device.
macAddresses	This is the list of MAC addresses for the device.
modelOfDevice	This is the device model (for example, iPhone or Pixel 3 XL).
name	This is the name of the device.
osDescription	This is the operating system running on the device (for example, Windows 10 or iOS 12.3.1).
quarantinedThreatCount	This is the total number of quarantined threats for the device.
safeStatus	This is the status of the device (for example, safe or risk).
unresolvedThreatCount	This is the total number of unresolved threats on the device.

Get devices extended

Request a page with a list of console devices with extended information, belonging to a tenant, sorted by registration (created) date, in descending order (most recent device registered listed first). The page number and page size parameters are optional. When the values are not specified, these default to 1 and 100 respectively. The maximum page size that can be specified is 200 entries per page.

Service endpoint	/devices/v2/extended?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	Return the first page with 100 devices: https://protectapi.cylance.com/devices/v2/extended?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
agent_version	This is the CylancePROTECT Desktop agent version installed on the device.
background_detection	If this is true, the agent is currently running a background threat detection scan.
date_first_registered	This is the date and time (in UTC) when the device record was created.
date_offline	This is the date and time (in UTC) when the device last communicated with the console.
days_to_deletion	This is the number of days before a device will be deleted. Enable automated device lifecycle management and remove inactive devices must both be enabled under device management. If enable automated lifecycle management is enabled and remove inactive devices is disabled, this field displays Unknown.
dlcm_status	This is the device lifecycle management status of the device, which shows the device as included or excluded from device lifecycle management. If device lifecycle management is disabled, the status shows as unknown.
hostname	This is the hostname for the device.
id	This is the endpoint's unique identifier.
ip_addresses	This is the list of IP addresses for the device.
is_safe	If this is true, there are no outstanding threats.
mac_addresses	This is the list of MAC addresses for the device.
name	This is the name of the device.
os_kernel_version	This is the Kernel version for the operating system on the device.
os_version	This is the operating system and version.
page_number	This is the page number requested.
page_size	This is the page size requested.
policy	This is the policy ID and name.
products	This is the name of the product installed on the device, the version number, and status.

Field Name	Description
state	This signals whether the device is online or offline. If device lifecycle management is enabled, the state could be inactive.
total_number_of_items	This is the otal number of resources.
total_pages	This is the otal number of pages that can be retrieved, based on the page size specified.

Get device count

Request a list of products, product versions, and number of devices using a product and product version in a tenant.

Service endpoint	/devices/v2/products
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/products
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
count	This is the total number of devices for a product version.
name	This is the product name.
version	This is the product version.

Get device

Request a specific device resource belonging to a tenant.

Service endpoint	/devices/v2/{{deviceId}}
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/cd5ee717-d6aa-469f-8f7e-7ac6d69a4084
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
agent_version	This is the CylancePROTECT Desktop agent version installed on the device.
background_detection	If this is true, the agent is currently running a background threat detection scan.
date_first_registered	This is the date and time (in UTC) when the device record was created.
date_last_modified	This is the date and time (in UTC) when the device record was last modified.
date_offline	This is the date and time (in UTC) when the device last communicated with the console.
days_to_deletion	This is the number of days before a device will be deleted. Enable automated device lifecycle management and remove inactive devices must both be enabled under device management. If enable automated lifecycle management is enabled and remove inactive devices is disabled, this field displays Unknown.
distinguished_name	This is the unique identifier for the device in the Lightweight Directory Access Protocol (LDAP).

Field Name	Description
dlcm_status	This is the device lifecycle management status of the device, which shows the device as included or excluded from device lifecycle management. If device lifecycle management is disabled, the status shows as unknown.
host_name	This is the hostname for the device.
id	This is the unique identifier for the device.
ip_addresses	This is the list of IP addresses for the device.
is_safe	If this is true, there are no outstanding threats.
last_logged_in_user	This is the ID of the user who logged in last on to the device.
mac_addresses	This is the list of MAC addresses for the device.
name	This is the name of the device.
os_kernel_version	This is the Kernel version for the operating system on the device.
os_version	This is the operating system and version.
policy	This is the name of the policy assigned to the device.
products	This is the name of the product installed on the device, the version number, and status.
state	This is the device is online or offline. If device lifecycle management is enabled, the state could be inactive.
update_available	If this is true, an agent update is available for the device based on the update type (Phase).
update_type	This is the update phase on which the device is scheduled.

Get device by MAC address

Request a specific device resource belonging to a tenant by using the MAC address of the device.

Service endpoint	/devices/v2/macaddress/{mac_address}
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/macaddress/28-F1-0E-45-AB-54
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
agent_version	This is the CylancePROTECT Desktop agent version installed on the device.
background_detection	If this is true, the agent is currently running a background threat detection scan.
date_first_registered	This is the date and time (in UTC) when the device record was created.
date_last_modified	This is the date and time (in UTC) when the device record was last modified.
date_offline	This is the date and time (in UTC) when the device last communicated with the console.
days_to_deletion	This is the number of days before a device will be deleted. Enable automated device lifecycle management and remove inactive devices must both be enabled under device management. If enable automated lifecycle management is enabled and remove inactive devices is disabled, this field displays Unknown.
distinguished_name	This is the unique identifier for the device in the Lightweight Directory Access Protocol (LDAP).
dlcm_status	This is the device lifecycle management status of the device, which shows the device as included or excluded from device lifecycle management. If device lifecycle management is disabled, the status shows as unknown.
host_name	This is the hostname for the device.
id	This is the unique identifier for the device.
ip_addresses	This is the list of IP addresses for the device.
is_safe	If this is true, there are no outstanding threats.
last_logged_in_user	This is the ID of the user who logged in last on to the device.
mac_addresses	This is the list of MAC addresses for the device.

Field Name	Description
name	This is the name of the device.
os_kernel_version	This is the Kernel version for the operating system on the device.
os_version	This is the operating system and version.
policy	This is the name of the policy assigned to the device.
products	This is the name of the product installed on the device, the version number, and status.
state	This is the device is online or offline. If device lifecycle management is enabled, the state could be inactive.
update_available	If this is true, an agent update is available for the device based on the update type (Phase).
update_type	This is the update phase on which the device is scheduled.

Get device by hostname

Request device resources belonging to a tenant by using the hostname (DNS name).

The hostname ("host_name") may not be the same as the name ("name") displayed by Cylance. The hostname is created by the operating system, while the name can be changed in the management console or API. For domain-joined computers, the "host_name" would be "hostname.domain.com". For computers not joined to a domain, it would just be "hostname".

Service endpoint	/devices/v2/hostname/{host_name}
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/hostname/User-Laptop-A123
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
agent_version	This is the CylancePROTECT Desktop agent version installed on the device.
background_detection	If this is true, the agent is currently running a background threat detection scan.
date_first_registered	This is the date and time (in UTC) when the device record was created.
date_last_modified	This is the date and time (in UTC) when the device record was last modified.
date_offline	This is the date and time (in UTC) when the device last communicated with the console.
days_to_deletion	This is the number of days before a device will be deleted. Enable automated device lifecycle management and remove inactive devices must both be enabled under device management. If enable automated lifecycle management is enabled and remove inactive devices is disabled, this field displays Unknown.
distinguished_name	This is the unique identifier for the device in the Lightweight Directory Access Protocol (LDAP).
dlcm_status	This is the device lifecycle management status of the device, which shows the device as included or excluded from device lifecycle management. If device lifecycle management is disabled, the status shows as unknown.
host_name	This is the hostname for the device.
id	This is the unique identifier for the device.
ip_addresses	This is the list of IP addresses for the device.
is_safe	If this is true, there are no outstanding threats.
last_logged_in_user	This is the ID of the user who logged in last on to the device.
mac_addresses	This is the list of MAC addresses for the device.
name	This is the name of the device.
os_kernel_version	This is the Kernel version for the operating system on the device.
os_version	This is the operating system and version.
policy	This is the name of the policy assigned to the device.
products	This is the name of the product installed on the device, the version number, and status. The version number is major, minor, and build number to match the data displayed in the console.

Field Name	Description
state	State of the device (for example, online or offline). If device lifecycle management is enabled, the state could be inactive.
update_available	If this is true, an agent update is available for the device based on the update type (phase).
update_type	This is the update phase on which the device is scheduled.

Update device

Update a specific device resource belonging to a tenant.

Service endpoint	/devices/v2/{unique_device_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/e378dacb-9324-453a-b8c6-5a8406952195
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:update scope encoded • Content-Type: application/json

Request

```
{
    "name": "User-Laptop-A123",
    "policy_id": "d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea",
    "add_zone_ids": [
        "d27ff5c4-5c0d-4f56-a00d-a1fb297e440e"
        ],
    "remove_zone_ids": [
        "639db7f7-c7f9-488d-b834-41c4522b32b6"
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
add_zone_ids	This is the list of zone identifiers which the device is to be assigned.
name	This is the name of the device.
policy_id	This is the unique identifier for the policy to assign to the device (specify as null or leave the string empty to remove the current policy from the device).
remove_zone_ids	This is the list of zone identifiers from which the device is to be removed.

Get device threat

Request a page with a list of threats found on a specific device. The page number and page size parameters are optional. When the values are not specified, these default to 1 and 10 respectively. The maximum page size that can be specified is 200 entries per page.

Service endpoint	/devices/v2/{unique_device_id}/threats?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	https://protectapi.cylance.com/devices/v2/e378dacb-9324-453a-b8c6-5a8406952195/threats?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:threatlist scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
classification	This is the threat classification assigned by Cylance.

Field Name	Description
cylance_score	This is the Cylance score assigned to the threat. The User API returns a raw score of -1 to 1. Threats have a negative raw score, while safe files have a positive raw score. The management console only displays threats and uses a score of 1 to 100. A raw score of -1 equals a console score of 100.
date_found	This is the date and time (in UTC) when the threat was found on the device.
file_path	This is the file path to the threat, which includes the file name.
file_status	This is the current status of the file on the device, which can be one of the following: • Default (0) (Unsafe) • Quarantined (1) • Whitelisted (2) • Suspicious (3) (Abnormal) • File Removed (4) (Delete) - The file was removed from the console. • Corrupt (5) - The file could not be scanned. The file could be corrupt or malformed.
name	This is the name of the threat.
page_number	This is the page number requested.
page_size	This is the page size requested.
sha256	This is the SHA256 hash for the threat.
sub_classification	This is the threat sub-classification assigned by Cylance.
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.
total_number_of_items	This is the total number of resource.

Update device threat

Update the status (waive or quarantine) of a convicted threat. To update a threat on a device requires the modify permission for the threats privilege in an integration. See authorization below.

Service Endpoint	/devices/v2/{unique_device_id}/threats
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/e378dacb-9324-453a-b8c6-5a8406952195/threats

Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the threat:update scope encoded • Content-Type: application/json

Request

```
{
    "threat_id":
 "bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52",
    "event": "Quarantine"
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
event	This is the requested status update for the convicted threat, which can be either quarantine or waive
threat_id	This is the SHA256 hash of the convicted threat

Get zone devices

Request a page with a list of console device resources belonging to a zone, sorted by registration (created) date, in descending order (most recent registered listed first). The page number and page size parameters are optional. When the values are not specified, these default to 1 and 10 respectively. The maximum page size that can be specified is 200 entries per page.

Service endpoint	/devices/v2/{unique_zone_id}/devices?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	https://protectapi.cylance.com/devices/v2/d27ff5c4-5c0d-4f56-a00d-a1fb297e440e/devices?page=1&page_size=100
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
id	This is the unique identifier for the device.
name	This is the name of the device.
page_number	This is the page number requested.
page_size	This is the page size requested.
policy_id	This is the unique identifier for the policy that the policy is currently assigned to (can be assigned as null).
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.

Get agent installer link

Request a secured link to download the Agent installer.

Note: The Build parameter is the full version number of the agent, such as 2.1.1590. To allow existing API calls to continue to work, a fixed number of older partial agent version values are supported as valid values for the build parameter: (1564, 1570, 1574, 1578, 1580, 1584, 1590, 1594)

- If the API call does not have the build parameter passed in, it returns the installer for the latest version of the agent.
- If the API call passes in the build parameter but leaves it with an empty value, the call returns an error.
- If the API call passes in the build parameter and passes a valid integer value of a supported version (such as 1564, 1570, 1574, 1578, 1580, 1584, 1590, 1594) the call return the installer for that agent version.
- If the API call passes in the build parameter and uses a full agent version as the value, the installer for that agent is returned

- If the API call passes in product=ProtectDriver then the build parameter must be the full agent version and the path to the Protect Driver is returned. For example, this will return the path the Protect Driver for version 3.0.1000:

  ```
  /devices/v2/installer?
  product=ProtectDriver&os=Rhel8&architecture=RedHatEnterprise8&build=3.0.1000
  ```

<table>
<tr><td>Service endpoint</td><td>/devices/v2/installer?product=p&os=o&package=k&architecture=a&build=v</td></tr>
<tr><td>Optional query string parameters</td><td>
<table>
<tr><th>Product</th><th>OS</th><th>Package</th><th>Architecture</th><th>Build (optional)</th></tr>
<tr><td>• Protect
• Optics
CylanceOPTICS does not support Linux.</td><td>• AmazonLinux1
• AmazonLinux2
• CentOS7
• Linux
Use Linux as the OS family for CentOS6.
• Mac
• Rhel8
• Suse11
• Suse12
• Ubuntu1404
• Ubuntu1604
• Ubuntu1804
• Windows</td><td>• Exe (Windows only)
• Msi (Windows only)
• Dmg (macOS only)
• Pkg (macOS only)</td><td>• X86
• X64
• AmazonLinux1
• AmazonLinux2
• CentOS6
• CentOS6UI
• CentOS7
• CentOS7UI
• RedHatEnterprise8
• RedHatEnterprise8UI
• Suse11
• Suse11UI
• Suse12
• Suse12UI
• Ubuntu1404
• Ubuntu1404UI
• Ubuntu1604
• Ubuntu1604UI
• Ubuntu1804
• Ubuntu1804UI</td><td>Full version number of the agent, such as 2.1.1590.</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td>https://protectapi.cylance.com/devices/v2/installer?
product=Protect&os=Windows&package=Msi&architecture=X64&build=1510</td></tr>
<tr><td>Method</td><td>HTTP/1.1 GET</td></tr>
<tr><td>Request headers</td><td>• Accept: application/json
• Authorization: Bearer JWT Token returned by Auth API with the device:read scope encoded</td></tr>
</table>

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
url	This is the URL you can use to download the requested agent installer. The API call only provides the URL, it does not download the installer for you.

Delete Devices

Delete one or more devices from a tenant. This is an asynchronous operation and could take up to two hours to delete the devices. If a callback URL is provided, the callback will occur when deletion is complete.

Service endpoint	/devices/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer with the device:delete scope encoded. • Content-Type: application/json

Request

```
{
     "device_ids":
     [
         "e378dacb-9324-453a-b8c6-5a8406952195",
         "a358daac-2394-653a-a9c2-8a8408972163",
         "b248cbba-6367-821b-a7a2-4a3200972163"
     ],
     "callback_url": "https://exampleurl.com"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
callback_url	This is the URL of the callback upon completion (optional). **Note:** • If you are not using a callback URL, then leave it out of the request. An empty callback URL results in an error message. • The URL used in the above Request is just an example. Replace it with your own callback URL.
device_ids	These are the unique identifiers for the devices to be deleted: • All device IDs should be well formed GUIDs. Non-conforming values will be removed from the request. • The maximum number of device IDs per request is 20.

Response JSON schema

Field Name	Description
request_id	This is the unique identifier for the deletion request.

Not all clients support sending a DELETE request. For this instance, use the following POST instead.

- Service Endpoint: /devices/v2/deleteExample: https://protectapi.cylance.com/devices/v2/delete
- Method: HTTP/1.1 POST

Delete this text and replace it with your own content.

Get Device Lifecycle Management settings

Retrieve a tenant's Device Lifecycle Management configuration.

Service endpoint	/devices/v2/inactive/settings
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/inactive/settings
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the devicemanagement:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
enableAutomatedDLCM	Required. Enable or disable Automated DLCM. The default value is disabled (false).
offlineBeforeInactive	Required. Number of days before an Offline device changes to Inactive. The valid value is from 7 to 180 days. The default value is 30 days.
enableRemoveInactiveDevice	Required. Enable or disable removing an inactive device. The default is disabled (false).
inactiveBeforeRemoved	Required. The number of days before inactive devices are removed. The valid value is from 7 to 180 days. The default value is 30 days.

Update Device Lifecycle Management Settings

Update a tenant's Device Lifecycle Management configuration.

Service endpoint	/devices/v2/inactive/settings
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/inactive/settings
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the devicemanagement:update scope encoded

Request

```
{
    "enableAutomatedDLCM": boolean,
    "offlineBeforeInactive": integer,
    "enableRemoveInactiveDevice": boolean,
    "inactiveBeforeRemoved": integer
```

```
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
enableAutomatedDLCM	Required. Enable or disable Automated DLCM. The default value is disabled (false).
offlineBeforeInactive	Required. Number of days before an Offline device changes to Inactive. The valid value is from 7 to 180 days. The default value is 30 days.
enableRemoveInactiveDevice	Required. Enable or disable removing an inactive device. The default value is disabled (false).
inactiveBeforeRemoved	Required. The number of days before inactive devices are removed. The valid value is from 7 to 180 days. The default value is 30 days.

Exempt devices from the Device Lifecycle Management process

Allows a caller to exempt a list of devices belonging to a tenant from the Device Lifecycle Management process.

Service endpoint	/devices/v2/inactive/exemptedDevices
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/inactive/exemptedDevices
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the devicemanagement:update scope encoded

Request

```
{
    "string:{device guid}"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
device guid	Required. The list of device identifiers belonging to a tenant. Maximum size is 1000. You can get the device guid by invoking the Get Device API.

Include devices in the Device Lifecycle Management process

Allows a caller to include a list of devices belonging to a tenant in the Device Lifecycle Management process.

Service endpoint	/devices/v2/inactive/includedDevices
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/inactive/includedDevices
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the devicemanagement:update scope encoded

Request

```
{
    "string:{device guid}"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
device guid	Required. The list of device identifiers belonging to a tenant. The maximum size is 1000. You can get the device guid by invoking the Get Device API.

Reset the inactive period for a list of devices that are included in the Device Lifecycle Management process

Allows a caller to reset the inactive period for a list of devices that are included in the Device Lifecycle Management process.

Service endpoint	/devices/v2/inactive/resetDevices
Optional query string parameters	—
Example	https://protectapi.cylance.com/devices/v2/inactive/resetDevices
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the devicemanagement:update scope encoded

Request

```
{
    "string:{device guid}"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
device guid	Required. The list of device identifiers belonging to a tenant. The maximum size is 1000. You can get the device guid by invoking the Get Device API.

Global list API

The global list allows a file to be marked for quarantine or to allow those files on all devices in the organization.

Get global list

Retrieve a list of items from the global list, based on list type, for a tenant.

Service endpoint	/globallists/v2?listTypeId={{listTypeId}}
Optional query string parameters	• pageNumber: This is the page number to request. • pageSize: This is the number of device records to retrieve per page.
Example	https://protectapi.cylance.com/globallists/v2?listTypeId=[0|1]?pageNumber=1&pageSize=20
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the globallist:list scope encoded

Note: The listTypeId parameter is required and can be either 0 (GlobalQuarantine) or 1 (GlobalSafe).

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
added	This is the date and time the global list item was added.
avIndustry	—
category	—
classification	—
listType	—
md5	This is the MD5 hash for the file.

Field Name	Description
name	This is the name of the global list item.
pageNumber	—
pageSize	—
reason	This is the reason for adding the item to the global list.
sha256	This is the SHA256 hash for the file.
subClassification	—
totalNumberOfItems	—
totalPages	—

Add to global list

Add a convicted threat to either the global quarantine or the global safe list for a particular tenant.

Service endpoint	/globallists/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/globallists/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the globallist:create scope encoded

Request

```
{
    "sha256": "bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52",
    "list_type": "GlobalSafe",
    "category": "CommercialSoftware",
    "reason": "Test"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
category	This field is required only if the *list_type* value is *GlobalSafe*. The value can be one of the following: • AdminTool • CommercialSoftware • Drivers • InternalApplication • OperatingSystem • SecuritySoftware • None There are no spaces in the category name when adding to a global list.
list_type	This is the list type that the threat belongs to (GlobalQuarantine or GlobalSafe).
reason	This is the reason why the file was added to the list.
sha256	This is the SHA256 hash for the threat.

Delete from global list

Remove a convicted threat from either the global quarantine or the global safe list for a particular tenant.

Service endpoint	/globallists/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/globallists/v2
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the globallist:delete scope encoded

Request

```
{
    "sha256": "bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52",
    "list_type": "GlobalSafe"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
list_type	This is the list type that the threat belongs to (GlobalQuarantine or GlobalSafe).
sha256	This is the SHA256 hash for the threat.

Policy API

A policy defines how the agent handles malware it encounters. For example, automatically quarantine malware or ignore it if in a specific folder.

Get policies

Request a page with a list of console policies belonging to a tenant, sorted by modified date, in descending order (most recently modified policy listed first). The page number and page size parameters are optional. When the values are not specified, these default to 1 and 10 respectively. When a policy is created, the modified date is the same as the created date, until the policy is modified.

Service endpoint	/policies/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	Return the first page with up to 100 policies: https://protectapi.cylance.com/policies/v2?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the policy:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
date_added	This is the date and time (in UTC) when the console policy resource was first created.
date_modified	This is the date and time (in UTC) when the console policy resource was last modified.
device_count	This is the number of devices assigned to this policy.
id	This is the unique ID for the policy resource.

Field Name	Description
name	This is the name of the policy.
page_number	This is the page number requested.
page_size	This is the page size requested.
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved based on the page size specified.
zone_count	This is the number of zones assigned to this policy.

Get policy

Get details for a policy, using the policy ID.

Service endpoint	/policies/v2/{policy_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/policies/v2/d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the policy:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description

appcontrol	Application control allows restricting any changes to applications on a device. Only the applications that exist on a device before enabling application control are allowed to execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied.
	The agent updater will also be disabled when application control is enabled.
	• Allowed_folders: allows applications and additions to the specified folders. It must be an absolute path (for example, c:\temp_appcontrol)
	• Changewindow_enabled:
	  • 0 - Closed: No changes can be made to any applications on the device.
	  • 1 - Open: Allow, edit, and run new applications on the device. This includes updating applications.
	• Lockdown:
	  • Action:
	  • The deny action blocks (denies) the lockdown_type.
	  • Lockdown_type:
	  • Executionfromexternaldrives indicates execution of a file from an external drive, like a USB hard drive or USB flash drive.
	  • pechange indicates changes made to existing applications on the device.

checksum	Checksum is used to detect errors that may have occurred during transmission or storage of data.

Field Name	Description

device_control	Device control
	• control_mode:
	  • Block does not allow the selected device_class to connect to the device.
	  • FullAccess allows the selected device_class to connect to the device.
	• device_class:
	  • AndroidUSB is a portable device running Android OS, like a smartphone or tablet.An Android device could connect and be identified as Android, Still Image, or Windows Portable Device (WPD). When blocking Android devices, consider also blocking Still Image and Windows Portable Devices.
	  • iOS is an Apple portable device running iOS, like an iPhone or iPad. iOS devices will not charge when Device Control is enabled and set to Block, unless the iOS device is powered off. Apple includes their charging capability within functions of the device that are required for our iOS device blocking capability.
	  • StillImage is the device class that includes 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 that allows a VMware virtual machine client to access USB devices connected to the host.
	  • WPD is a portable device that uses the Microsoft Windows Portable Device (WPD) driver technology, such as a mobile phone, digital camera, and portable media players.
	• exclusion_list: These are control exclusions that allow full access or block connecting a USB device. The vendor_id is required.
	  • comment: This is optional information about why the exclusion was added.
	  • control_mode:
	  • Block: does not allow the specified vendor_id from connecting to the device.
	  • FullAccess: allows the specified vendor_id to connect to the device.
	  • date_added: This is the date and time the device control exclusion was added to the policy.
	  • product_id: Some manufacturers provide a unique identifier for each USB product they make. This information is optional.
	  • serial_number: Some manufacturers provide a unique serial number for each USB device they make. This information is optional.
	  • vendor_id: This is the unique identifier for the manufacturer of the USB device.

Field Name	Description

file_exclusions	The policy safe list identifies file exclusions specific to the policy, and any devices assigned to the policy will allow the excluded files to run.
	• av_industry:
	  • false: The file hash has not been identified by the anti-virus industry.
	  • true: The file hash has been identified by the anti-virus industry.
	• category_id: This is the category selected when adding the file to the policy safe list.
	  • 1 = None
	  • 2 = Admin Tool
	  • 3 = Internal Application
	  • 4 = Commercial Software
	  • 5 = Operating System
	  • 6 = Drivers
	  • 7 = Security Software
	• cloud_score: This is the Cylance Score displayed in the console. The score can go up to 100.
	• file_hash: This is the SHA256 has for the file. This information is required.
	• file_name: This is the name of the file. This is "null" if the filename is not available.
	• file_type: This is the file scanner type. Should always return *1* for executable.
	• infinity: This is the Cylance Cloud score. This is "null" if no score is available.
	• md5: This is the MD5 hash for the file. This information is optional.
	• reason: This is the reason for adding the file to the policy safe list. The reason must be added when creating the file exclusion.
	• research_class_id: This is the Cylance threat classification. If "infinity" is null, then the research_class_id is not available.
	  • 1 = Trusted
	  • 2 = PUP
	  • 3 = Malware
	  • 4 = File Unavailable
	  • 5 = Possible PUP
	  • 6 = Dual Use
	• research_subclass_id: Some threat classification have sub-classes to help administrators determine if a file should be blocked or allowed to run. See Threat classifications for more information.

filetype_actions	These actions indicate the autoquarantine of unsafe and abnormal files.
	• actions: This is the setting to enable or disable auto quarantine and auto upload.
	  • 0 - AutoQuarantine OFF and AutoUpload OFF
	  • 1 - AutoQuarantine ON and AutoUpload OFF
	  • 2 - AutoQuarantine OFF and AutoUpload ON
	  • 3 - AutoQuarantine ON and AutoUpload ON
	• file_type: The only option is "executable".
	• suspicious_files: These are abnormal files.
	• threat_files: These are unsafe files.

Field Name	Description

logpolicy	These are the Agent log file settings.
	• log_upload: This is the setting to enable or disable uploading log files.
	  • null: Disabled
	  • 1: Enabled
	• maxlogsize: This is the maximum file size (in MB) for a single log file.
	• retentiondays: This is the number of days to save log files. Log files older than the set number of days will be deleted.

memoryviolation_actions	These are the violation types for memory protection. The following 3 rows explain the possible violation types:

Field Name	Description
memory_violations	• lsassread (LSASS read): 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. • outofprocessapc (remote APC scheduled): A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process. • 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).

Field Name	Description
memory_violation_ext	• dyldinjection (DYLD injections): 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_v2	These are the executable files to exclude from memory protection. This must be a relative path to the excluded executable file (for example: \\temp).
policy	Various policy settings are contained within this section. All policy settings must be included in the request. For most policy settings, the possible values will be either 0 (disabled) or 1 (enabled). The remaining cells in this table explain policy settings in detail.
Automatic policy settings	• auto_blocking: This is the setting to auto quarantine unsafe threats. • auto_delete: This is the setting to automatically delete quarantined files after a set number of days. If this feature is enabled, set "days_until_deleted" for the number of days to retain a quarantined file. • auto_uploading: This is the setting to automatically upload files that BlackBerry has not seen before. BlackBerry will perform an analysis on the file and provide details to assist in manual analysis and triage. • autoit_auto_uploading: This setting is currently not in use. • pdf_auto_uploading • powershell_auto_uploading • python_auto_uploading

Field Name	Description

Various policy settings	• days_until_deleted: This is the 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. The "auto-delete" setting must be enabled.
	• device_control: This is the setting to enable or disable the device control feature.
	• docx_auto_uploading: This is the setting currently not in use.
	• full_disc_scan: This is the setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the background threat detection 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: This is the setting to kill processes and children processes regardless of the state when a threat is detected (EXE or DLL).
	• logpolicy: This setting is not used.
	• memory_exploit_detection: This is the setting to enable or disable the memory protection feature. This affects "memory_violation_actions" ("memory_violations" and "memory_violations_ext").
	• sample_copy_path: This is the 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: This is the 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: This is the 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.
	  Example:
	  `{ "name": "scan_max_archive_size", "value": "0" }`
	• script_control: This is the setting to enable or disable the script control feature. Also set the script_control settings (see below in this table).

Field Name	Description

Various policy settings continued	• show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylancePROTECT Desktop events.
	• threat_report_limit: This is the number of threats to upload to the console.
	Example:
	`{ "name": "threat_report_limit", "value": "500" }`
	• trust_files_in_scan_exception_list: This is the setting to allow execution of files in the excluded folders. This is related to the scan_exception_list.
	• watch_for_new_files: This is the setting to analyze new or modified executable files for threats.
	• ole_auto_uploading: This setting is currently not in use.
	• prevent_service_shutdown: This is the setting that protects the Cylance service from being shutdown, either manually or by another process.
	• sample_copy_path: This is the setting to copy all file samples to a network share (CIFS/SMB).
	Example:
	`{ "name": "sample_copy_path", "value": "\\\\server_name\\shared_folder" }`

Field Name	Description
Optics policy settings	• optics: This is the settingto enable or disable CylanceOPTICS. • optics_application_control_auto_upload: This is the setting to allow the automatic uploading of application control related focus data. • optics_malware_auto_upload: This is the setting to allow the automatic uploading of threat related focus data. • optics_memory_defense_auto_upload: This is the setting to allow the automatic uploading of memory protection related Focus Data. • optics_script_control_auto_upload: This is the setting to allow the automatic uploading of script control related focus data. • optics_sensors_advanced_executable_parsing: This is the 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. • optics_sensors_advanced_powershell_visibility: This is the setting to enable recording commands, arguments, scripts, and content entered directly into the Powershell Console and the Powershell Integrated Scripting Environment (ISE). • optics_sensors_advanced_wmi_visibility: This is the setting to enable recording additional Windows Management Instrumentation (WMI) attributes and parameters. • optics_sensors_dns_visibility: This is the setting to enable recording commands and arguments of commands issued directly or indirectly to the Windows Management Instrumentation (WMI) interpreter. • optics_sensors_enhanced_file_read_visibility: This is the setting to enable monitoring file reads within an identified set of directories. • optics_sensors_enhanced_process_hooking_visibility: This is the setting to enable recording process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection. • optics_sensors_private_network_address_visibility: This is the setting to enable recording network connections within the RFC 1918 and RFC 3419 address spaces. • optics_sensors_windows_event_log_visibility: This is the setting to enable recording Windows Security Events and their associated attributes. • optics_set_disk_usage_maximum_fixed: This is the 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. Example: `{ "name": "optics_set_disk_usage_maximum_fixed", "value": "1000" }` • optics_show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylanceOPTICS events. • optics_show_notification: This is the setting to enable or disable CylanceOPTICS desktop notifications on the device.
policy_id	This is the unique identifier for the policy.
policy_name	This is the name of the policy.

Field Name	Description
policy_utctimestamp	This is the date and time the policy was created (in UTC).

script_control	These are the Script Control settings in a policy.
	• activescript_settings:
	  • control_mode: This setting allows or blocks ActiveScript usage.
	  • Allow
	  • Block
	• global_settings:
	  • allowed_folders: This setting specifies folder exclusions, including subfolders, for script control. This setting specifies a relative path.
	  • control_mode: This setting allows or blocks ActiveScript and PowerShell usage with Agent 1370 or lower.
	  • Allow
	  • Block
	• macro_settings:
	  • control_mode: This setting allows or blocks Macro usage. Microsoft Office macros use Visual Basic for Applications (VBA).
	  • Allow
	  • Block
	  Note: The script control macros feature works with agent version 1578 and earlier. For newer agents, use the Dangerous VBA Macros violation type with memory protection. Any macro exclusions created for script control of newer agents must be added to the memory protection exclusions for the Dangerous VBA Macros violation type.
	• powershell_settings:
	  • console_mode: This setting allows or blocks the PowerShell console. This affects PowerShell command usage, including PowerShell one-liners.
	  • Allow
	  • Block
	  • control_mode: This setting allows or blocks PowerShell usage.
	  • Allow
	  • Block

Create policy

Service endpoint	/policies/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/policies/v2

Method	HTTP/1.1 POST
Request headers	• Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the policy:create scope encoded.

Request

The following example creates a policy with most features enabled and includes some sample exclusions. You can copy this example, change the user_id, and this should create an example policy in your tenant.

Note: This example is provided just for testing the API. Do not use this example policy on your devices. Device policies should be tested before applying to a large number of devices in your organization.

```
    "policy_name": "testPolicy",
    "script_control": {
      "activescript_settings": {
        "control_mode": "Alert",
        "control_mode_v2":"BlockAbnormal"
      },
      "global_settings": {
        "allowed_folders": ["/path.py"],
        "allowed_folders_ext": [
          {
            "comment": "any test 200 chars long"
          }
        ],
        "control_mode": "Alert",
        "score_all_scripts": false,
        "upload_script_to_cloud": false,
        "must_obtain_score_from_cloud": false,
        "alert_suspicious_script_exec_only": false
      },
      "macro_settings": {
        "control_mode": "Alert"
      },
      "powershell_settings": {
        "control_mode": "Block",
        "console_mode": "Block",
        "control_mode_v2":"BlockAbnormal"
      }
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
checksum	Checksum is required when creating a policy. This uses an empty value. Example: `"checksum": ""`

Field Name	Description
device_control	Device Control allows or blocks access to USB mass storage devices. device_control must be enabled under **policy**. All device_class entries must be included in the request. • AndroidUSB: This is a portable device running Android OS, like a smartphone or a tablet. 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 Devices as well. • iOS: This is an Apple portable device running iOS, like an iPhone or iPad. 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: This is the device class containing scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers. • USBCDDVDRW: This is a USB optical drive. • USBDrive: This is a USB hard drive or USB flash drive. • VMWareMount: This is a VMware USB Passthrough, which allows a VMware virtual machine client to access USB devices connected to the host. • WPD: This is a Windows Portable Device, which uses the Microsoft Windows Portable Device driver technology, such as mobile phones, digital cameras, and portable media players. Device control exclusion list allows or blocks access to specific USB mass storage devices. • comment: This adds details about the exclusion. This information is optional. • control_mode: This allows or blocks the specific USB mass storage device. • Block: This does not allow the USB mass storage device from connecting to the endpoint. • FullAccess: This allows the USB mass storage device to connect to the endpoint. • product_id: This is the product identifier for the USB mass storage device. This information is optional. • serial_number: This is the serial number for the USB mass storage device. This information is optional. • vendor_id: This is the vendor identifier for the USB mass storage device. This information is required. 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 endpoint, then attach the USB mass storage device to the endpoint. You can view External Device logs in the management 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" } ]`

Field Name	Description

file_exclusions	This adds file exclusions to the policy safe list, under file actions. Policy safe list are file exclusions specific to the policy, and any endpoints assigned to the policy will allow the excluded files to run.
	• category_id: This is 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: This is the SHA256 hash for the file. This information is required.
	• file_name: This is the name of the file being excluded. This information is optional.
	• md5: This is the MD5 hash for the file. This information is optional.
	• reason: This is the reason the file was excluded. This information is required.
	Example:
	`"exclusion_list": [ { "reason": "Test Exclusion", "category_id": "2", "md5": "d41d8cd98f00b204e9800998ecf8427e", "file_hash": "bf17366ee3bb8068a9ad70fc9e68 496e7e311a055bf4ffeeff53cc5d29ccce52", "file_name": "filename" } ]`

filetype_actions	These actions indicate the autoquarantine of unsafe and abnormal files.
	• actions: Set auto-quarantine and auto-upload to enable or disable.
	  • 0: auto-quarantine OFF, auto-upload OFF
	  • 1: auto-quarantine ON, auto-upload OFF\
	  • 2: auto-quarantine OFF, auto-upload OFF
	  • Use 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: The only option is "executable".
	• suspicious_files: Abnormal files
	• threat_files: Unsafe files

Field Name	Description

logpolicy	These are the agent log file settings.
	• log_upload: This is the setting to enable or disable uploading agent log files.
	  • null: Disabled
	  • 1: Enabled
	• maxlogsize: This is the maximum file size (in MB) for a single agent log file.
	• retentiondays: This is the number of days to save agent log files. Log files older than the set number of days will be deleted.

memoryviolation _actions	These are the violation types for memory protection. The following 3 rows explain the possible violation types:

Field Name	Description
memory_violations	• lsassread (LSASS read): 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. • outofprocessapc (remote APC scheduled): A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process. • 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).

Field Name	Description
memory_violations_ext	• dyldinjection (DYLD injections): 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_violations_ext_v2	• childprocessprotect (Memory Permission Changes in Child Processes) - Windows only: A violating process has spawned a child process and has modified memory access permissions in that child process. • dangerouscomobject (Dangerous COM Object) - Windows only: A Malicious code that has a reference to a Component Object Model (COM) object has been detected. • dangerouseenvvariable (Dangerous Environment Variable) - Windows only: An environment variable that may have malicious code attached has been detected. • directsyscall (Direct System Calls) - Windows only: Aan attempt to silently inject malicious code into other processes has been detected. This violation type cannot be blocked. • doppelganger (Doppelganger): A new (malicious) process was started from a file that has not yet been written to the file system. The file writer transaction is usually rolled back after the process start (so the malicious file is never committed to disk), and any attempt to scan the file on disk will only see the unmodified benign file. • maliciouslowintegrity (Low Integrity Process Start) - Windows only: A process has been set to run with a low integrity level. • oopprotect (Memory Permission Changes in Other Processes) - Windows only: A violating process has modified memory access permissions within another process. This is usually done to inject code into another process to make memory executable by modifying memory access permissions. There are few legitimate uses of this. • stolensystemtoken (Stolen System Token) - Windows only: An access token has been modified to allow a user to bypass security access controls. • syscallprobe (System Call Monitoring) - Windows only: A system call made to an application or operating system has been detected. • systemdllwrite (System DLL Overwrite) - Windows only: An attempt to overwrite a system DLL has been detected.

Field Name	Description
memory_exclusion_list_v2	These are the executable files to exclude from Memory Protection. This must be a relative path to the excluded executable file. Example: `"memory_exclusions_list_v2": [ { "violations": [], "path": "C:\\temp\\file1.txt" }, { "violations": [], "path": "C:\\temp\\file2.txt" } ]`
policy	Various policy settings are contained within this section. Some policy settings are enabled under **policy** and configured in a different section, like device_control and logpolicy. For most policy settings, the possible values will be either 0 (disabled) or 1 (enabled). The remaining cells in this table explain policy settings in detail.
Automatic policy settings	• auto_blocking: This is the setting to auto quarantine unsafe threats. • auto_delete: This is the setting to automatically delete quarantined files after a set number of days. If this feature is enabled, set "days_until_deleted" for the number of days to retain a quarantined file. • auto_uploading: This is the setting to automatically upload files that BlackBerry has not seen before. BlackBerry will perform an analysis on the file and provide details to assist in manual analysis and triage. • autoit_auto_uploading: This setting is currently not in use. • pdf_auto_uploading • powershell_auto_uploading • python_auto_uploading

Field Name	Description

Various policy settings	• custom_thumbprint:
	• days_until_deleted: This is the 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. The "auto-delete" setting must be enabled.
	• device_control: This is the setting to enable or disable the device control feature.
	• docx_auto_uploading: This setting is currently not in use.
	• full_disc_scan: This is the setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the background threat detection 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: This is the setting to kill processes and child processes regardless of the state when a threat is detected (EXE or DLL).
	• logpolicy: This setting is not used.
	• memory_exploit_detection: This is the setting to enable or disable the memory protection feature. This affects "memory_violation_actions" ("memory_violations" and "memory_violations_ext").
	• sample_copy_path: This is the setting to copy all file samples to a network share (CIFS/SMB). For Example:
	`{ "name": "sample_copy_path", "value": "\\\\server_name\\shared_folder" }`
	• scan_exception_list: This is the 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. For example:
	`{ "name": "scan_exception_list", "value": [ "c:\\temp" ] }`
	• scan_max_archive_size: This is the 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. For example:
	`{ "name": "scan_max_archive_size", "value": "0" }`
	• script_control: This is the setting to enable or disable the script control feature. Also set the script_control settings (see below in this table).

Field Name	Description

Various policy settings continued	• show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylancePROTECT Desktop events.
	• threat_report_limit: This is the number of threats to upload to the console.
	Example:
	`{ "name": "threat_report_limit", "value": "500" }`
	• trust_files_in_scan_exception_list: This is the setting to allow execution of files in the excluded folders. This is related to the scan_exception_list.
	• watch_for_new_files: This is the setting to analyze new or modified executable files for threats.
	• ole_auto_uploading: This setting is currently not in use.
	• prevent_service_shutdown: This is the setting that protects the Cylance service from being shutdown, either manually or by another process.
	• sample_copy_path: This is the setting to copy all file samples to a network share (CIFS/SMB).
	Example:
	`{ "name": "sample_copy_path", "value": "\\\\server_name\\shared_folder" }`

Field Name	Description
Optics policy settings	• optics: This is the setting to enable or disable CylanceOPTICS. • optics_application_control_auto_upload: This is the setting to allow the automatic uploading of application control related focus data. • optics_malware_auto_upload: This is the setting to allow the automatic uploading of threat related focus data. • optics_memory_defense_auto_upload: This is the setting to allow the automatic uploading of memory protection related Focus Data. • optics_script_control_auto_upload: This is the setting to allow the automatic uploading of script control related focus data. • optics_sensors_advanced_executable_parsing: This is the 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. • optics_sensors_advanced_powershell_visibility: This is the setting to enable recording commands, arguments, scripts, and content entered directly into the Powershell Console and the Powershell Integrated Scripting Environment (ISE). • optics_sensors_advanced_wmi_visibility: This is the setting to enable recording additional Windows Management Instrumentation (WMI) attributes and parameters. • optics_sensors_dns_visibility: This is the setting to enable recording commands and arguments of commands issued directly or indirectly to the Windows Management Instrumentation (WMI) interpreter. • optics_sensors_enhanced_file_read_visibility: This is the setting to enable monitoring file reads within an identified set of directories. • optics_sensors_enhanced_process_hooking_visibility: This is the setting to enable recording process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection. • optics_sensors_private_network_address_visibility: This is the setting to enable recording network connections within the RFC 1918 and RFC 3419 address spaces. • optics_sensors_windows_event_log_visibility: This is the setting to enable recording Windows Security Events and their associated attributes. • optics_set_disk_usage_maximum_fixed: This is used to set the maximum amount of device storage reserved for use by CylanceOPTICS, in MB. The minimum value is 500 and the maximum value is 1000. Example: `{ "name": "optics_set_disk_usage_maximum_fixed", "value": "1000" }` • optics_show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylanceOPTICS events. • optics_show_notification: This is the setting to enable or disable CylanceOPTICS desktop notifications on the device.
policy_name	This is the name of the policy. The name must be unique to your tenant.

Field Name	Description

script_control	The policy settings for script control. script_control must be enabled (set to "1") under policy.
	
	activescript_settings
	
	• control_mode: These are the setting for active script.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	• control_mode_v2:
	  • Allow: The script is allowed to run.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	  • Block UNSAFE: The script will be scored and blocked if found to be unsafe.
	  • Block ABNORMAL and UNSAFE: The script will be scored and blocked if found to be abnormal or unsafe.
	
	global_settings
	
	• allowed_folders: The relative path to scripts that are allowed to run when script control is enabled. Script control folder exclusions apply to all agent versions (agent 1310 or later). For example:
	
	`"allowed_folders": [ "\\temp_scriptcontrol" ]`
	
	• control_mode: This is the setting to enable or disable script control for agent version 1370 or earlier. This works for active scripts and PowerShell. This does not work for macros. 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.
	• score_all_scripts: This boolean setting controls if all scripts are going to be scored, including scripts with the control_mode_v2 setting set to Alert or Block. Scripts with the setting set to Block UNSAFE or Block ANORMARL and UNSAFE will be scored automatically and this setting will be ignored.
	• upload_script_to_cloud: This boolean setting controls if all scripts will be uploaded to BlackBerry services when attempting to obtain the score of a script. If set to "false", Infinity will be searched to see if it already has the score. If it does not, the script will not be uploaded for scanning and will be assigned "UNSCORED".
	• must_obtain_score_from_cloud: This boolean setting allows you to forcefully obtain a score from Infinity before deciding what to do with a script execution. When a cached result is used, this setting will be ignored.
	  • True: When a score can't be obtained from Infinity and control_mode_v2 = Block, Block UNSAFE, or Block ABNORMAL and UNSAFE, the state will be set to "UNSCORED" and "Block".
	  • False: When a score can't be obtained from Infinity, the state will be combined with local classifiers and follow the control_mode_v2 setting. If the local classifier is not available, the score will be set to "UNSCORED".
	• alert_suspicious_script_exec_only: This boolean setting allows you to generate events only for scripts that are suspicious or were not evaluated.

Field Name	Description

	macro_settings
	• control_mode: These are the setting for Microsoft Office macros.
	  • Alert: An alert is sent when an Microsoft Office macro event occurs. The macro is allowed to run.
	  • Block: The Microsoft Office macro is blocked and an alert is sent.
	  Note: The script control macros feature works with agent version 1578 and earlier. For newer agents, use the Dangerous VBA Macros violation type with memory protection. Any macro exclusions created for script control of newer agents must be added to the memory protection exclusions for the Dangerous VBA Macros violation type.
	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. Values can be either Allow or Block
	• control_mode:
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	• control_mode_v2:
	  • Allow: The script is allowed to run.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	  • Block UNSAFE: The script will be scored and blocked if found to be unsafe.
	  • Block ABNORMAL and UNSAFE: The script will be scored and blocked if found to be abnormal or unsafe.

Field Name	Description
script_control continued	About disabling script control For Agent versions 1430 and later, you can disable script control for active script, PowerShell, or macros. Disabling 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. For example: script control for macros is disabled. `"script_control": { "global_settings": { "allowed_folders": null, "control_mode": "Alert", "score_all_scripts": false, "upload_script_to_cloud":true, "must_obtain_score_from_cloud":true, "alert_suspicious_script_exec_only": false }, "activescript_settings": { "control_mode": "Alert" "control_mode_v2":"Block UnSAFE" }, "powershell_settings": { "control_mode": "Alert", "console_mode": "Allow" "control_mode_v2":"Block UnSAFE" } }`
user_id	This is the unique ID for the user creating the policy. Only administrators can create policies. To get the user_id, use Get users.

Response JSON schema

This table only covers descriptions not covered in the Request JSON Schema Descriptions table (see previous table).

Field Name	Description
policy_id	This is the unique identifier for the policy.
policy_utctimestamp	This is the date and time (in UTC) when the policy was created.

Update policy

Update an existing policy. The request contents for update policy are similar to create policy, except you must include the policy_id in the update policy request.

Service endpoint	/policies/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/policies/v2
Method	HTTP/1.1 PUT
Request headers	• Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the policy:update scope encoded

Request

```
{
   "user_id":"a2c0ac7a-a63d-4583-b646-ae10db9c9769",
   "policy":{
      "memoryviolation_actions":{
         "memory_violations_ext_v2":[
            {
               "violation_type":"syscallprobe",
               "action":"Alert",
               "order":"1"
            },
            {
               "action":"Alert",
               "order":"2",
               "violation_type":"directsyscall"
            },
            {
               "order":"3",
               "violation_type":"systemdllwrite",
               "action":"Alert"
            },
            {
               "order":"4",
               "action":"Alert",
               "violation_type":"dangerouscomobject"
            },
            {
               "order":"5",
               "violation_type":"doppelganger",
               "action":"Alert"
            },
            {
               "violation_type":"dangerousenvvariable",
               "action":"Alert",
               "order":"6"
            },
            {
               "order":"7",
               "violation_type":"oopprotect",
               "action":"Alert"
            },
            {
```

```
            "action":"Alert",
            "order":"8",
            "violation_type":"childprocessprotect"
         },
         {
            "order":"9",
            "action":"Alert",
            "violation_type":"stolensystemtoken"
         },
         {
            "order":"10",
            "violation_type":"maliciouslowintegrity",
            "action":"Alert"
         },
         {
            "violation_type":"injectionviaapc",
            "action":"Alert",
            "order":"11"
         },
         {
            "order":"12",
            "action":"Alert",
            "violation_type":"runmacroscript"
         }
      ],
      "memory_violations":[
         {
            "violation_type":"lsassread",
            "action":"Alert"
         },
         {
            "violation_type":"outofprocessunmapmemory",
            "action":"Alert"
         },
         {
            "violation_type":"stackpivot",
            "action":"Alert"
         },
         {
            "violation_type":"stackprotect",
            "action":"Alert"
         },
         {
            "violation_type":"outofprocessoverwritecode",
            "action":"Alert"
         },
         {
            "action":"Alert",
            "violation_type":"outofprocesscreatethread"
         },
         {
            "violation_type":"overwritecode",
            "action":"Alert"
         },
         {
            "action":"Alert",
            "violation_type":"outofprocesswritepe"
         },
         {
            "violation_type":"outofprocessallocation",
            "action":"Alert"
```

```
            },
            {
               "violation_type":"outofprocessmap",
               "action":"Alert"
            },
            {
               "violation_type":"outofprocesswrite",
               "action":"Alert"
            },
            {
               "action":"Alert",
               "violation_type":"outofprocessapc"
            }
         ],
         "memory_violations_ext":[
            {
               "violation_type":"dyldinjection",
               "action":"Alert"
            },
            {
               "violation_type":"trackdataread",
               "action":"Alert"
            },
            {
               "action":"Alert",
               "violation_type":"zeroallocate"
            },
            {
               "action":"Alert",
               "violation_type":"maliciouspayload"
            }
         ],
         "memory_exclusion_list_v2":[
            {
               "violations":[

               ],
               "path":"\\Application\\TestApp\\MyApp\\program.exe"
            }
         ],
         "memory_exclusion_list":[
            "\\Application\\TestApp\\MyApp\\program.exe"
         ]
      },
      "persona":{
         "mitigation_actions":[
            {
               "action":"alertsOnly",
               "threshold":"70"
            },
            {
               "threshold":"30",
               "action":"promptUsernameAndPassword"
            }
         ],
         "admin_whitelist":[
            {
               "username":"admin"
            }
         ],
         "mode":"1"
```

```
      },
      "device_control":{
         "configurations":[
            {
               "device_class":"AndroidUSB",
               "control_mode":"FullAccess"
            },
            {
               "control_mode":"FullAccess",
               "device_class":"iOS"
            },
            {
               "control_mode":"FullAccess",
               "device_class":"StillImage"
            },
            {
               "device_class":"USBCDDVDRW",
               "control_mode":"FullAccess"
            },
            {
               "control_mode":"FullAccess",
               "device_class":"USBDrive"
            },
            {
               "device_class":"VMWareMount",
               "control_mode":"FullAccess"
            },
            {
               "control_mode":"FullAccess",
               "device_class":"WPD"
            }
         ],
         "exclusion_list":[
            {
               "vendor_id":"1234",
               "comment":"Test external device",
               "serial_number":null,
               "product_id":"5678",
               "control_mode":"FullAccess",
               "date_added":"2022-02-01T23:56:32.479Z"
            }
         ]
      },
      "policy":[
         {
            "value":"1",
            "name":"auto_blocking"
         },
         {
            "value":"1",
            "name":"auto_uploading"
         },
         {
            "value":"500",
            "name":"threat_report_limit"
         },
         {
            "name":"full_disc_scan",
            "value":"2"
         },
         {
```

```
            "value":"1",
            "name":"watch_for_new_files"
         },
         {
            "name":"memory_exploit_detection",
            "value":"1"
         },
         {
            "value":"0",
            "name":"trust_files_in_scan_exception_list"
         },
         {
            "value":"1",
            "name":"logpolicy"
         },
         {
            "name":"script_control",
            "value":"1"
         },
         {
            "name":"prevent_service_shutdown",
            "value":"1"
         },
         {
            "value":"0",
            "name":"scan_max_archive_size"
         },
         {
            "name":"sample_copy_path",
            "value":"\\\\server_name\\shared_folder"
         },
         {
            "name":"kill_running_threats",
            "value":"1"
         },
         {
            "name":"show_notifications",
            "value":"1"
         },
         {
            "name":"optics_set_disk_usage_maximum_fixed",
            "value":"1000"
         },
         {
            "value":"1",
            "name":"optics_malware_auto_upload"
         },
         {
            "name":"optics_memory_defense_auto_upload",
            "value":"1"
         },
         {
            "value":"0",
            "name":"optics_script_control_auto_upload"
         },
         {
            "value":"0",
            "name":"optics_application_control_auto_upload"
         },
         {
            "value":"1",
```

```
            "name":"optics_sensors_dns_visibility"
         },
         {
            "name":"optics_sensors_private_network_address_visibility",
            "value":"1"
         },
         {
            "value":"1",
            "name":"optics_sensors_windows_event_log_visibility"
         },
         {
            "name":"optics_sensors_windows_advanced_audit_visibility",
            "value":"1"
         },
         {
            "name":"optics_sensors_advanced_powershell_visibility",
            "value":"1"
         },
         {
            "name":"optics_sensors_advanced_wmi_visibility",
            "value":"1"
         },
         {
            "name":"optics_sensors_advanced_executable_parsing",
            "value":"1"
         },
         {
            "name":"optics_sensors_enhanced_process_hooking_visibility",
            "value":"1"
         },
         {
            "value":"1",
            "name":"optics_sensors_enhanced_file_read_visibility"
         },
         {
            "value":"1",
            "name":"device_control"
         },
         {
            "name":"optics",
            "value":"1"
         },
         {
            "name":"auto_delete",
            "value":"1"
         },
         {
            "name":"days_until_deleted",
            "value":"14"
         },
         {
            "name":"pdf_auto_uploading",
            "value":"0"
         },
         {
            "name":"ole_auto_uploading",
            "value":"0"
         },
         {
            "name":"docx_auto_uploading",
            "value":"0"
```

```
         },
         {
            "value":"0",
            "name":"python_auto_uploading"
         },
         {
            "value":"0",
            "name":"autoit_auto_uploading"
         },
         {
            "value":"0",
            "name":"powershell_auto_uploading"
         },
         {
            "value":null,
            "name":"custom_thumbprint"
         },
         {
            "name":"scan_exception_list",
            "value":[
               "C:\\Test"
            ]
         },
         {
            "value":"1",
            "name":"optics_show_notifications"
         }
      ],
      "script_control":{
         "powershell_settings":{
            "control_mode":"Alert",
            "console_mode":"Allow"
         },
         "macro_settings":{
            "control_mode":"Alert"
         },
         "global_settings":{
            "control_mode":"Alert",
            "allowed_folders":[
               "/users/*/temp/*"
            ]
         },
         "activescript_settings":{
            "control_mode":"Alert"
         }
      },
      "filetype_actions":{
         "suspicious_files":[
            {
               "actions":"3",
               "file_type":"executable"
            }
         ],
         "threat_files":[
            {
               "actions":"3",
               "file_type":"executable"
            }
         ]
      },
      "logpolicy":{
```

```
         "retentiondays":"30",
         "log_upload":{
            "compress":"True",
            "delete":"False"
         },
         "maxlogsize":"100"
      },
      "file_exclusions":[
         {
            "reason":"SHA256 for testing",
            "category_id":"2",
            "md5":null,
            "research_class_id":"0",

 "file_hash":"443010d98917908efb64a1e8c4a560ec126649bd7e4d0ddd87643356e6f3506f",
            "cloud_score":null,
            "av_industry":false,
            "file_name":"Test file",
            "file_type":1,
            "research_subclass_id":"0",
            "infinity":null
         }
      ],
      "checksum":"",
      "script_control_v2":{
         "python_settings":{
            "control_mode":"Alert"
         },
         "dotnet_dlr_settings":{
            "control_mode":"Alert"
         }
      },
      "policy_name":"Example Policy",
      "policy_id":"52c9f06b-1cef-4837-8001-ca5da50fef32"
   }
}
```


Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
checksum	Checksum is required when you create a policy. Checksum uses an empty value. Example: `"checksum": ""`

Field Name	Description
device_control	Device control allows or blocks access to USB mass storage devices. device_control must be enabled under policy. device_class: All device_class entries must be included in the request. • AndroidUSB is a portable device running Android OS, like a smartphone or a tablet. 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 devices as well. • iOS is an Apple portable device running iOS, like an iPhone or iPad. 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. • VMWareMoun: 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. exclusion_list: Device control exclusion list allows or blocks access to specific USB mass storage devices. • comment: This is optional information about why the exclusion was added. • control_mode: Allows or blocks the specific USB mass storage device. • Block does not allow the USB mass storage device from connecting to the endpoint. • FullAccess allows the USB mass storage device to connect to the endpoint. • product_id: This is the product identifier for the USB mass storage device. This information is optional. • serial_number: This is the serial number for the USB mass storage device. This information is optional. • vendor_id: This is the vendor identifier for the USB mass storage device. This information is required. 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 endpoint, then attach the USB mass storage device to the endpoint. You can view external device logs in the management console, on the protection page or the device details page (external devices tab). For example: `"exclusion_list": [ { "vendor_id": "1234", "comment": "Test device control exclusion", "serial_number": 987654321", "product_id": "5678", "control_mode": "FullAccess" } ]`

Field Name	Description

file_exclusions	This setting adds file exclusions to the policy safe list, under file actions. Policy safe List are file exclusions specific to the policy, and any endpoints assigned to the policy will allow the excluded files to run.
	• category_id: This is the 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: This is the SHA256 hash for the file. This information is required.
	• file_name: This is the name of the file being excluded. This information is optional.
	• md5: This is the MD5 hash for the file. This information is optional.
	• reason: Tis is the reason the file was excluded. This information is required.
	Example:
	`"file_exclusions": [ { "reason": "Test Exclusion", "category_id": "2", "md5": "d41d8cd98f00b204e9800998ecf8427e", "file_hash": "bf17366ee3bb8068a9ad70fc9e68 496e7e311a055bf4ffeeff53cc5d29ccce52", "file_name": "filename" } ]`

<table>
<tr><th>Field Name</th><th>Description</th></tr>
<tr><td>filetype_actions</td><td>This setting is used for the auto-quarantine of unsafe (threat_files) and abnormal (suspicious_files).
actions: This is the setting to enable or disable auto quarantine and auto upload.
0 - auto-quarantine OFF, auto-upload OFF
1 - auto-quarantine ON, auto-upload OFF
2 - auto-quarantine OFF, auto-upload ON
Use 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: The only option is "executable".
suspicious_files: These are abnormal files.
threat_files: These are unsafe files.
Examples of filetype_actions settings and the results in the management console.<table><tr><th colspan="2">filetype_actions settings</th><th colspan="3">Management console results</th></tr><tr><td>threat_files</td><td>suspicious_files</td><td>Unsafe auto-quarantine</td><td>Abnormal auto-quarantine</td><td>Auto upload</td></tr><tr><td>0</td><td>0</td><td>No</td><td>n/a</td><td>No</td></tr><tr><td>2</td><td>2</td><td>No</td><td>n/a</td><td>Yes</td></tr><tr><td>1</td><td>0</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>3</td><td>2</td><td>Yes</td><td>No</td><td>Yes</td></tr><tr><td>1</td><td>1</td><td>Yes</td><td>Yes</td><td>No</td></tr><tr><td>3</td><td>3</td><td>Yes</td><td>Yes</td><td>Yes</td></tr></table></td></tr>
<tr><td>logpolicy</td><td>These are the agent log file settings.
log_upload: The setting to enable or disable uploading agent log files.
null - Disabled
1 - Enabled
maxlogsize: This is the maximum file size (in MB) for a single agent log file.
retentiondays: This is the number of days to save agent log files. Log files older than the set number of days will be deleted.</td></tr>
<tr><td>memoryviolation _actions</td><td>These are the violation types for memory protection. All memory_violations and memory_violations_ext entries must be included in the Request. The following 3 rows explain the possible violation types:</td></tr>
</table>

Field Name	Description
memory_violations	• lsassread (LSASS Read): 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. • outofprocessapc (Remote APC Scheduled): A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process. • 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).

Field Name	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_v2	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_v2": [ "\\temp" ]`
policy	Various policy settings are contained within this section. All policy settings must be included in the request. For most policy settings, the possible values will be either 0 (disabled) or 1 (enabled). The remaining cells in this table explain policy settings in detail.
Automatic policy settings	• auto_blocking: This is the setting to auto quarantine unsafe threats. • auto_delete: This is the setting to automatically delete quarantined files after a set number of days. If this feature is enabled, set "days_until_deleted" for the number of days to retain a quarantined file. • auto_uploading: This is the setting to automatically upload files that BlackBerry has not seen before. BlackBerry will perform an analysis on the file and provide details to assist in manual analysis and triage. • autoit_auto_uploading: This setting is currently not in use. • pdf_auto_uploading • powershell_auto_uploading • python_auto_uploading

Field Name	Description

Various policy settings	• days_until_deleted: This is the 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. The "auto-delete" setting must be enabled.
	• device_contro: This is the setting to enable or disable the device control feature.
	• docx_auto_uploading: This setting is currently not in use.
	• full_disc_scan: This is the setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the background threat detection 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: This is the setting to kill processes and children processes regardless of the state when a threat is detected (EXE or DLL).
	• logpolicy: This setting is not used.
	• memory_exploit_detection: This is the setting to enable or disable the memory protection feature. This affects "memory_violation_actions" ("memory_violations" and "memory_violations_ext").
	• sample_copy_path: This is the setting to copy all file samples to a network share (CIFS/SMB). For example:
	`{ "name": "sample_copy_path", "value": "\\\\server_name\\shared_folder" }`
	• scan_exception_list: This is the 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. For example:
	`{ "name": "scan_exception_list", "value": [ "c:\\temp" ] }`
	• scan_max_archive_size: This is the 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. For example:
	`{ "name": "scan_max_archive_size", "value": "0" }`
	• script_control: This is the setting to enable or disable the script control feature.
	Also set the script_control settings (see below in this table).

Field Name	Description
Various policy settings continued	• show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylancePROTECT Desktop events. • threat_report_limit: This is the number of threats to upload to the console. Example: `{ "name": "threat_report_limit", "value": "500" }` • trust_files_in_scan_exception_list: This is the setting to allow execution of files in the excluded folders. This is related to the scan_exception_list. • watch_for_new_files: This is the setting to analyze new or modified executable files for threats. • ole_auto_uploading: This setting is currently not in use. • prevent_service_shutdown: This is the setting that protects the Cylance service from being shutdown, either manually or by another process.

Field Name	Description
Optics policy settings	• optics: This is the setting to enable or disable CylanceOPTICS. • optics_application_control_auto_upload: This is the setting to allow the automatic uploading of application control related focus data. • optics_malware_auto_upload: This is the setting to allow the automatic uploading of threat related focus data. • optics_memory_defense_auto_upload: This is the setting to allow the automatic uploading of memory protection related Focus Data. • optics_script_control_auto_upload: This is the setting to allow the automatic uploading of script control related focus data. • optics_sensors_advanced_executable_parsing: This is the 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. • optics_sensors_advanced_powershell_visibility: This is the setting to enable recording commands, arguments, scripts, and content entered directly into the Powershell Console and the Powershell Integrated Scripting Environment (ISE). • optics_sensors_advanced_wmi_visibility: This is the setting to enable recording additional Windows Management Instrumentation (WMI) attributes and parameters. • optics_sensors_dns_visibility: This is the setting to enable recording commands and arguments of commands issued directly or indirectly to the Windows Management Instrumentation (WMI) interpreter. • optics_sensors_enhanced_file_read_visibility: This is the setting to enable monitoring file reads within an identified set of directories. • optics_sensors_enhanced_process_hooking_visibility: This is the setting to enable recording process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection. • optics_sensors_private_network_address_visibility: This is the setting to enable recording network connections within the RFC 1918 and RFC 3419 address spaces. • optics_sensors_windows_event_log_visibility: This is the setting to enable recording Windows Security Events and their associated attributes. • optics_set_disk_usage_maximum_fixed: This is the 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. Example: `{ "name": "optics_set_disk_usage_maximum_fixed", "value": "1000" }` • optics_show_notifications: This is the setting to enable or disable desktop notifications on the endpoint for CylanceOPTICS events. • optics_show_notification: This is the setting to enable or disable CylanceOPTICS desktop notifications on the device.
policy_id	This is the unique identifier for the policy.
policy_name	This is the name of the policy. The name must be unique to your tenant.

Field Name	Description

script_control	These are the policy settings for script control. script_control must be enabled (set to "1") under policy.
	
	activescript_settings
	
	• control_mode: These are the settings for active script.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	• control_mode_v2:
	  • Allow: The script is allowed to run.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	  • Block UNSAFE: The script will be scored and blocked if found to be unsafe.
	  • Block ABNORMAL and UNSAFE: The script will be scored and blocked if found to be abnormal or unsafe.
	
	global_settings
	
	• allowed_folders: These are the relative path to scripts that are allowed to run when Script Control is enabled. Script Control Folder Exclusions apply to all Agent versions (Agent 1310 or higher). For example:
	
	`"allowed_folders": [ "\\temp_scriptcontrol"]`
	
	• control_mode: This is the setting to enable or disable script control for agent version 1370 or earlier. This works for active scripts and PowerShell. This does not work for macros. To use script control with macros, use sgent 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.
	• score_all_scripts: This boolean setting controls if all scripts are going to be scored, including scripts with the control_mode_v2 setting set to Alert or Block. Scripts with the setting set to Block UNSAFE or Block ANORMARL and UNSAFE will be scored automatically and this setting will be ignored.
	• upload_script_to_cloud: This boolean setting controls if all scripts will be uploaded to BlackBerry services when attempting to obtain the score of a script. If set to "false", Infinity will be searched to see if it already has the score. If it does not, the script will not be uploaded for scanning and will be assigned "UNSCORED".
	• must_obtain_score_from_cloud: This boolean setting allows you to forcefully obtain a score from Infinity before deciding what to do with a script execution. When a cached result is used, this setting will be ignored.
	  • True: When a score can't be obtained from Infinity and control_mode_v2 = Block, Block UNSAFE, or Block ABNORMAL and UNSAFE, the state will be set to "UNSCORED" and "Block".
	  • False: When a score can't be obtained from Infinity, the state will be combined with local classifiers and follow the control_mode_v2 setting. If the local classifier is not available, the score will be set to "UNSCORED".
	• alert_suspicious_script_exec_only: This boolean setting allows you to generate events only for scripts that are suspicious or were not evaluated.

Field Name	Description

	macro_settings
	• control_mode: These are the settings for Microsoft Office Macros.
	  • Alert: An alert is sent when an Microsoft Office macro event occurs. The macro is allowed to run.
	  • Block: The Microsoft Office macro is blocked and an alert is sent.
	  Note: The script control macros feature works with agent version 1578 and earlier. For newer agents, use the Dangerous VBA Macros violation type with memory protection. Any macro exclusions created for script control of newer agents must be added to the memory protection exclusions for the Dangerous VBA Macros violation type.
	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. Value can either be Allow or Block.
	• control_mode:
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	• control_mode_v2:
	  • Allow: The script is allowed to run.
	  • Alert: The script is allowed to run and an alert is sent when an event occurs.
	  • Block: The script is blocked and an alert is sent.
	  • Block UNSAFE: The script will be scored and blocked if found to be unsafe.
	  • Block ABNORMAL and UNSAFE: The script will be scored and blocked if found to be abnormal or unsafe.

Field Name	Description
script_control continued	For agent versions 1430 and later, you can disable script control for active script, PowerShell, or macros. Disabling 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. For example: script control for macros is disabled. `"script_control": { "global_settings": { "allowed_folders": null, "control_mode": "Alert", "score_all_scripts": false, "upload_script_to_cloud":true, "must_obtain_score_from_cloud":true, "alert_suspicious_script_exec_only": false }, "activescript_settings": { "control_mode": "Alert" "control_mode_v2":"Block UnSAFE" }, "powershell_settings": { "control_mode": "Alert", "console_mode": "Allow" "control_mode_v2":"Block UnSAFE" } }`
user_id	This is the unique ID for the user creating the policy. Only administrators can create policies. To get the user_id, use Get users.

Delete policy

Delete a policy from a tenant.

Service endpoint	/policies/v2/{tenant_policy_id}
Optional query string parameters	—
Example	user_id: https://protectapi.cylance.com/policies/v2/d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea
Method	HTTP/1.1 DELETE
Request headers	Authorization: Bearer *JWT Token returned by Auth API* with the policy:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Delete policies

Delete multiple polices from a tenant.

Service Endpoint	/policies/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/policies/v2
Method	HTTP/1.1 DELETE
Request headers	• Authorization: Bearer *JWT Token returned by Auth API* with the policy:delete scope encoded • Content-Type: application/json

Request

```
{
    "tenant_policy_ids": [
        "d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea",
        "376e21d1-f227-49c4-85fb-d9be1e5d766b",
        "b7a4a177-e385-489b-bcb0-3a4f25276320"
    ]
}
```

Response

Please see the Response status codes for more information.

Zone API

A zone is a way to organize and manage devices.

Create zone

Add a zone to a tenant.

Service endpoint	/zones/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/zones/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the zone:create scope encoded. • Content-Type: application/json

Request

```
{
    "name": "Test Zone",
    "policy_id": "d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea",
    "criticality": "Normal"
}
```

The policy_id or criticality requests can be removed if they are not needed. If the policy_id is removed, the zone is created with the default policy. If the criticality is removed, the zone is created with the normal criticality.

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high). The default setting, normal, is assigned if a value is not included.
name	This is the name of the zone. The maximum character limit for a zone name is 255. The following special characters are invalid: &<>. Zone names are case-preserving, but case-insensitive.

Field Name	Description
policy_id	This is the unique ID for the zone rule created for the zone. Null is displayed if no zone rule exists.

Response JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high).
date_created	This is the date and time (in UTC) when the zone was created.
id	This is the unique ID for the zone.
name	This is the name of the zone.
policy_id	This is the unique ID for the zone rule created for the zone. Null is displayed if no zone rule exists.

Get zones

Request a page with a list of zones resources belonging to a tenant, sorted by the created date, in descending order (most recent user registered listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 10 respectively. The maximum page size that can be specified is 200 entries per page.

Service Endpoint	/zones/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	return the first page with 100 users: https://protectapi.cylance.com/zones/v2?page=1&page_size=100
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:create scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high).
date_created	This is the date and time (in UTC) when the zone was created.
date_modified	This is the date and time (in UTC) when the zone was last modified.
id	This is the unique ID for the zone.
name	This is the name of the zone.
policy_id	This is the unique ID for the policy assigned to the zone.
update_type	This is the update type for the zone (production, pilot, or test).
zone_rule_id	This is the unique ID for the zone rule created for the zone. Null is displayed if no zone rule exists.

Get zone

Request zone information for a specific zone in a tenant.

Service endpoint	/zones/v2/{unique_zone_id}
Optional query string parameters	—
Example	return the first page with 100 users: https://protectapi.cylance.com/zones/v2/d27ff5c4-5c0d-4f56-a00d-a1fb297e440e
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the zone:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high).
date_created	This is the date and time (in UTC) when the zone was created.
date_modified	This is the date and time (in UTC) when the zone was last modified.
id	This is the unique ID for the zone.
name	This is the name of the zone.
policy_id	This is the unique ID for the policy assigned to the zone.
update_type	This is the update type for the zone (production, pilot, or test).
zone_rule_id	This is the unique ID for the zone rule created for the zone. Null is displayed if no zone rule exists.

Get device zones

Request a page with a list of zone resources for a specified device, belonging to a tenant, sorted by the created date, in descending order (most recent user registered listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 10 respectively. The maximum page size that can be specified is 200 entries per page.

Service Endpoint	/zones/v2/{unique_device_id}/zones?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	return the first page with 100 users: https://protectapi.cylance.com/zones/v2/e378dacb-9324-453a-b8c6-5a8406952195/zones?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the zone:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high).
date_created	This is the date and time (in UTC) when the zone was created.
date_modified	This is the date and time (in UTC) when the zone was last modified.
id	This is the unique ID for the zone.
name	This is the name of the zone.
policy_id	This is the unique ID for the policy assigned to the zone.
update_type	This is the update type for the zone (production, pilot, or test).
zone_rule_id	This is the unique ID for the zone rule created for the zone. Null is displayed if no zone rule exists.

Update zone

Update a zone in a tenant.

Service endpoint	/zones/v2/{unique_zone_id}
Optional query string parameters	—
Example	return the first page with 100 users: https://protectapi.cylance.com/zones/v2/d27ff5c4-5c0d-4f56-a00d-a1fb297e440e
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the zone:update scope encoded

Request

```
{
    "name": "Test Policy",
    "policy_id": "d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea",
    "criticality": "Normal"
```

```
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
criticality	This is the value of the zone (low, normal, or high).
name	This is the name of the zone.
policy_id	This is the unique ID for the policy assigned to the zone.

Delete zone

Delete a zone in a tenant.

Service endpoint	/zones/v2/{unique_zone_id}
Optional query string parameters	—
Example	return the first page with 100 users: https://protectapi.cylance.com/zones/v2/d27ff5c4-5c0d-4f56-a00d-a1fb297e440
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the zone:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Threat API

CylancePROTECT Desktop can do more than simply classify files as unsafe or abnormal. It can provide details on the static and dynamic characteristics of files.

Get threats

Get a list of threats detected in a tenant.

Service endpoint	threats/v2?page=m&page_size=n&start_time=t1&end_time=t2
Optional query string parameters	—
Example	https://protectapi.cylance.com/threats/v2/?page=1&page_size=20&start_time=2023-11-14T21:07:10&end_time=2023-11-24T21:07:10
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the device:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
avIndustry	This is the threat data from the AV industry.
certIssuer	This is the certificate issuer.
certPublisher	This is the certificate publisher.
certTimestamp	This is the date and time when the certificate was created.
classification	This is the classification of the threat (For example, PUP indicates a potentially unwanted program).
dateDetected	This is the date and time the threat was detected on the device. Note that the date parameters filter on dateDetected.

Field Name	Description
dateFirstDetected	This is the date and time when the threat was first detected.
detectedBy	This is the product features that detected the threat.
deviceId	This is the unique ID for the device.
deviceName	This is the name of the device.
end_time	The end of the time range in ISO-8601 date/time format (optional) (default value: now)
fileSize	This is the size of the file, in bytes (for example, 1000 is 1KB).
globalQuarantined	—
md5	This is the MD5 hash information for the threat.
mostRecentDetection	This is the date and time of the most recent detection of the threat.
name	This is the name of the threat.
page	The page number to request. (optional) (default value: 1)
page_size	The number of device records to retrieve per page. (optional) (default value: 10, maximum value: 200)
safelisted	—
sha256	This is the SHA256 hash information for the file.
signed	—
start_time	The start of the time range in ISO-8601 date/time format (required if using end_time)
subClassification	—
threatHistory	—
uniqueToCylance	—

Get threat

Request threat details for a specific threat.

Service endpoint	/threats/v2/{threat_sha256}

Optional query string parameters	—
Example	https://protectapi.cylance.com/threats/v2/bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the threat:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
auto_run	This setting indicates if the file is set to automatically run on system startup. • false: The file is not set to automatically run on system startup. • true: The file is set to automatically run on system startup.
av_industry	This is the score provided by the antivirus industry. If there is no antivirus industry score, then null is displayed.
cert_issuer	This is the ID for the certificate issuer.
cert_publisher	This is the ID for the certificate publisher.
cert_timestamp	This is the date and time (in UTC) when the file was signed using the certificate.
classification	This is the threat classification for the threat. See Threat classifications for more information.
cylance_score	This is the Cylance score assigned to the threat. The User API returns a raw score of -1 to 1. Threats have a negative raw score, while safe files have a positive raw score. The management console only displays threats and uses a score of 1 to 100. A raw score of -1 equals a Console score of 100.
detected_by	This is the name of the module that detected the threat.
file_size	This is the size of the file, in bytes.

Field Name	Description
global_quarantine	This setting identifies if the threat is on the global quarantine list. • false: The file is not on the global quarantine list. • true: The file is on the global quarantine list.
md5	This is the MD5 hash for the threat.
name	This is the name of the threat.
running	This setting identifies if the threat is executing, or another executable loaded or called it. • false: The threat is not running. • true: The threat is running.
safelisted	This setting identifies if the threat is on the safe list. • false: The file is not on the safe list. • true: The file is on the safe list.
sha256	This is the SHA256 hash for the threat.
signed	This setting identifies if the file is signed or not signed.
sub_classification	This is the threat sub-classification for the threat. See Threat classifications for more information.
unique_to_cylance	This setting identifies that the threat was identified by Cylance but not by other antivirus sources. • false: The file has been identified by other antivirus sources. • true: The file has only been identified as a threat by Cylance.

Get threat devices

Request a list of devices affected by a specific threat. Only one file_path is listed per page_item, therefore the same device could have multiple entries, one entry per file_path.

Service endpoint	/threats/v2/{threat_sha256}/devices?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page. • threat_sha256: This is the SHA256 hash for the threat.
Example	return the first page with 100 devices that have the specified threat: https://protectapi.cylance.com/threats/v2/bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52/devices?page1&page_size=100
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the threat:devicelist scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
agent_version	This is the CylancePROTECT Desktop agent version installed on the device.
date_found	This is the date and time (in UTC) when the threat was found on the device.
file_path	This is the path where the file was found on the device. Only one file_path is listed per page_item, therefore the same device could have multiple entries, one entry per file_path.
file_status	This is the current quarantine status of the file on the device. • Default (unsafe) • Quarantined • Whitelisted • Suspicious (abnormal) • File Removed (delete): The file was removed from the console • Corrupt: The file could not be scanned, it could be corrupt or malformed.
id	This is the endpoint's unique identifier.
ip_addresses	This is the list of IP addresses for the device.
mac_addresses	This is the list of MAC addresses for the device.
name	This is the name of the device.
page_number	This is the page number requested.
page_size	This is the page size requested.
policy_id	This is the unique identifier for the policy assigned to the device, or null if no policy is assigned.

Field Name	Description
state	This is the state of the device. • Offline • Online
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.

Get threat download URL

Request a download link for a given file. Use the download link to download the file.

Service endpoint	/threats/v2/download/{threat_sha256}
Optional query string parameters	—
Example	https://protectapi.cylance.com/threats/v2/download/bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the threat:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
url	This is the URL you can use to download the file. The API call only provides the URL, it does not download the file for you.

Memory protection API

Memory protection provide different options for handling memory exploits, including process injections and escalations.

Get memory protection events

Request a list of memory protection events.

Service endpoint	/memoryprotection/v2?page=m&page_size=n&start_time=t1&end_time=t2
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page. • start_time: This is the start of the time range. Format is YYYY-MM-DDThh:mm:ss.SSSZ (ISO 8601 date/time format). Required if using an end_time. • end_time: This is the end of the time range. Format is: YYYY-MM-DDThh:mm:ss.SSSZ (ISO 8601 date/time format). Optional. The default value is now. • device_id: This adds a device ID to reduce the set of memory protection events. Default is null.
Example	https://protectapi.cylance.com/memoryprotection/v2?page=1&page_size=100&start_time=2019-11-01T12:00:00& end_time:2019-11-30T12:00:00
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the memoryprotection:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
action	This is the action take on the memory protection event. • 0: None • 2: Block • 3: Terminate
agent_event_id	This is the unique identifier for the memory protection event, created by the Agent.
created	This is the date and time the memory protection event was created.
device_id	This is the unique identifier for the device.
device_image_file_event_id	This is the unique identifier for the memory protection event. Use this information for get memory protection event.
dll_version	This is the agent version that identified the memory protection event.
file_hash_id	This is the SHA256 hash for the threat.
file_version	This is the version number of the file that caused the memory protection event.
groups	This is the groups the user belongs to.
image_name	This is the path and name of the file that triggered the memory protection event.
process_id	This is the process ID of the memory protection event. It is generated by the operating system.
sid	This is the security identifier for the user, group, or other security principal. It is generated by the operating system.
username	This is the name of the user who was logged in to the device when the memory protection event occurred.
violation_type	This is the violation type number for the memory protection event. See Memory violation types for more information.

Get memory protection event

Request details for a specific memory protection event.

Service endpoint	/memoryprotection/v2/{device_image_file_event_id}
Optional query string parameters	—

Example	https://protectapi.cylance.com/memoryprotection/v2/40d04bf5-c5d7-495f-805a-28c6fc8ac12chttps://protectapi.cylance.com/users/v2
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the memoryprotection:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
action	This is the action take on the memory protection event. • 0: None • 2: Block • 3: Terminate
agent_event_id	This is the unique identifier for the memory protection event, created by the agent.
created	This is the date and time the memory protection event was created.
device_id	This is the unique identifier for the device.
device_image_file_event_id	This is the unique identifier for the memory protection event. Use this information for get memory protection event.
dll_version	This is the agent version that identified the memory protection event.
file_hash_id	This is the SHA256 hash for the threat.
file_version	This is the version number of the file that caused the memory protection event.
groups	These are the groups the user belongs to.
image_name	This is the path and name of the file that triggered the memory protection event.
process_id	This is the process ID of the memory protection event. It is generated by the operating system.

Field Name	Description
sid	This is the security identifier for the user, group, or other security principal. It is generated by the operating system.
username	This is the name of the user who was logged in to the device when the memory protection event occurred.
violation_type	This is the violation type number for the memory protection event. See Memory violation types for more information.

Memory violation types

The following table provides a description of each violation type, the operating system on which the violation type is applied, and the violation type number returned by the User API.

#	Violation Type	Description	Applies To
1	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).	Windows macOS Linux
2	Stack protect	The memory protection of a thread's stack has been modified to enable execution permissions. 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).	Windows macOS Linux
3	Overwrite code	Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass data execution prevention (DEP).	Windows
4	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.	macOS

#	Violation Type	Description	Applies To
5	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.	macOS
6	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.	Windows macOS
7	Remote write PE to 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.	Windows
8	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.	Windows
9	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.	Windows
10	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.	Windows macOS
11	Remote APC scheduled	A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process.	Windows

#	Violation Type	Description	Applies To
12	LSASS read	Memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.	Windows
13	RAM scraping	A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS).	Windows
22	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.	Windows macOS
23	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, that cause their modules to be loaded automatically when an application starts.	macOS Linux
24	Malicious payload	A generic shellcode and payload detection associated with exploitation has been detected.	Windows
25	Dangerous VBA macro	A dangerous action by an Office Visual Basic for applications (VBA) macro. This includes starting a shell, deleting files, calling certain COM objects, and referencing functions from external libraries.	Windows
26	Doppelganger	A process using a portable executable (PE) file that exists in an unfinalized state so the file can be manipulated to look like a different PE.	Windows
27	Memory permission changes in other processes	A process modifying memory permissions in another process that it did not create (not a child process).	Windows

#	Violation Type	Description	Applies To
28	Memory permission changes child processes	A process modifying memory permissions in another process that was not created by it (not a parent process).	Windows
30	System call monitoring	An attempt to set up the monitoring of system calls done by another process.	Windows
31	Direct system calls	An attempt to use undocumented and unstable system calls directly without going through the documented system interfaces.	Windows
32	System DLL overwrite	An overwrite of the system library (ntdll).	Windows
34	Stolen system token	A privilege escalation by stealing an authentication token of a system process with the highest privileges.	Windows
35	Dangerous environment variable	A process is reading an environment variable that has high abuse potential and may have been set by an attacker.	Windows
36	Low integrity process start	An executable file that is dropped and subsequently loaded by a low integrity process in a temp directory.	Windows
37	Dangerous COM object	A potentially dangerous COM object is being created.	Windows
38	Injection via APC	A process is using an Asynchronous Procedure Call (APC) or start remote thread to call LoadLibrary or similar function in order to inject arbitrary code into target process.	Windows

Detections API

The CylanceOPTICS detection API allows users to interact with detection events triggered by the CylanceOPTICS context analysis engine (CAE). CAE allows users to take automated response actions against malicious or suspicious behavior detected on devices utilizing both machine learning models and static behavior-based rules.

The CylanceOPTICS detection API enables further automation of analyzing, triaging, and responding to malicious or suspicious activity prevented or detected by CylanceOPTICS. The workflows currently available through this API include:

- Gathering a summary detection events that have occurred in a tenant including a detection event's ID, severity, description, occurrence time, associated device, and status.
- Gathering the specific detection details of detection events that have occurred in a tenant, including the artifacts associated with a detection event, the status of automated response actions that have been taken against a detection event, and other granular details that compose the detection event.
- Deleting a single or multiple detection events from a tenant.
- Updating a detection event's status and comments in a tenant.

Get detections

Request a page with a list of detections belonging to a tenant, sorted in descending order (most recent detection listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 20 respectively.

Service endpoint	/detections/v2?page=m&page_size=n

Optional query string parameters	• page: This is the page number to request.
	• page_size: This is the number of device records to retrieve per page.
	• start: This is the start date-time of the query range.
	• end: This is the end date-time of the query range.
	• severity: This is the detection severity filter. Values are informational, low, medium, high.
	• detection_type: This is the detection type filter.
	• event_number: This is the event number filter.
	• device: This is the device name filter.
	• status: This is the status for the detection event, values are new, in progress, follow up, reviewed, done, false positive.
	• sort: This sorts by the following fields (adding "-" in front of the value denotes descending order):
	  • Severity
	  • OccurrenceTime
	  • Status
	  • Device
	  • PhoneticId
	  • Description
	  • ReceivedTime

Example	retrieve the first page with up to 100 Detections, with a High severity, and sorted by Occurrence Time: https://protectapi.cylance.com/detections/v2?page=1&page_size=100&severity=High&sort=OccurrenceTime
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
CylanceId	This is the ID for the device.
DetectionDescription	This is the description of the detection.
Device	This is the device information that contains the device ID and device name.
Id	This is the unique ID for the detection.
name	This is the name of the device.
OccurrenceTime	This is the time when the detection occurred according to the associated endpoint agent.
page_number	This is the page number requested.
page_size	This is the page size requested.
PhoneticId	This is the easy-to-read version of the ID that is probabilistically unique.
ReceivedTime	This is the time when the detection was received by Cylance's cloud services.
Severity	This is the criticality of an observance of a detection.
Status	This is the status of the detection workflow.
total_number_of_items	This is the total number of resources.

Field Name	Description
total_pages	This is the total number of pages that can be retrieved, based on the page size specified.

Get detection

Request a specific detection resource belonging to a tenant. Use get detections to obtain the unique detection ID.

Service endpoint	/detections/v2/{detection_id}/details
Optional query string parameters	—
Example	https://protectapi.cylance.com/detections/v2/f2d6c020-53e2-4300-9005-2e006d9a0f57/details
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
ActivationTime	This is the time that this particular detection first started to occur.
AppliedExceptions	These are the exceptions that were applied to the detection. • Id: This is the unique identifier for the exception. • Version: This is the version number for the exception.

Field Name	Description

ArtifactsOfInterest	This is the artifact associated with the rule that triggered the exception. This is a dynamic object.
	• Artifact:
	  • Type: This is the type of artifact.
	  • Uid: This is the unique identifier for the artifact.
	• Source: This is the source for the artifact.
	• StateA: This is this is the name of the artifact of interest.

AssociatedArtifacts	This is the list of artifacts that were involved in this detection. These are dynamic objects.
Comment	This is the comment on the detection.
Context	This is the context of the detection.
DetectionRule	This is the description of the rule from which this detection originated. • Category: This is the category of the rule. • Description: This is the description of the rule. • Id: This is the ID of the rule. • Name: This is the name of the rule. • Version: This is the version of the rule.
Detector	This is the description of the plugin that originated the detection. • Name: This is the name of the detector. • Version: This is the version of the detector.
Device	This is a capture of the current state of the device. • CylanceId: This is the unique ID for the device. • Name: This is the name of the device.
Id	This is the unique identifier for the detection.
InvolvedArtifacts	These are the artifacts involved in this detection.
Name	This is the name of the detection.
ObjectType	This is the object type for the detection.
OccurrenceTime	This is the time at which the detection occurred.
PhoneticId	This is the easy-to-read version of the ID that is probabilistically unique.
Product	This is the description of the Cylance product that originated the detection. • Name: This is the name of the Cylance product. • Version: This is the version of the Cylance product.

Field Name	Description
ReceivedTime	This is the time when the detection was received.

Responses	These are the responses to the detection.
	• Status: This is the status of the response.
	• Comment: This is the comment on the response.
	• TenantId: This is the tenant ID to which the response belongs.
	• PhoneticId: This is the easy-to-read version of the ID that is probabilistically unique.
	• DetectionId: This is the ID for the detection event that warranted the response.
	• OccurrenceTime: This is the time at which the response actions were taken.
	• ActionResults:
	  • HandlingResponderVersion: This is the version of the responder plugin that performed the response.
	  • HandlingResponderName: This is the name of the responder plugin that performed the response.
	  • Results:
	  • Status: This is the status of the result.
	  • Message: This is the message of the result.
	  • Code:
	  • Ordinal: This is the indicator code for the success of the action.
	  • Reason: This is the detailed description explaining the indicator code.
	  • Name: This is the friendly name of the status code.
	• AssociatedArtifacts: These are the artifacts upon which the action occurred.
	• ResponseRuleId: This is the ID of the response rule that triggered the response.
	• SchemaVersion: This is the version of the response rule.
	• ResponseRuleVersion: This is the version of the response rule.
	• ReceivedTime: This is the time the response was received.
	• ObjectType: This is the type of the object for the response.

SchemaVersion	This is the version of the schema to which the object conforms.
Severity	This is the criticality of an observance of the detection.
SeveritySortLevel	This is the sort level for the severity.
Status	This is the status of the detection in the workflow.
StatusSortLevel	This is the sort level for the status.
Trace	This is the trace information. • Event: This is the CylanceOPTICS Event that triggered the state. • StateName: This is the name of a state that was traversed.
TenantId	This is the ID for the tenant.
ZoneIds	This is the list of IDs for the zones associated with the detection.

Get recent detections

Request a count of recent CylanceOPTICS detection resources belonging to a tenant.

Service endpoint	/detections/v2/recent?since={recent_detection_datetime}
Optional query string parameters	—
Example	https://protectapi.cylance.com/detections/v2/recent?since=2018-07-26T01:20:07.596Z
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
num_after	This is the number of detections after the {recent_detection_datetime}.
num_unaddressed	This is the number of unaddressed detections after the {recent_detection_datetime}.

Get detections .csv

Request a list of CylanceOPTICS detection resources belonging to a tenant, in .csv format. Any provided filters will be applied, but limit/offset parameters will not. All detections for the tenant will be exported.

Service endpoint	/detections/v2/csv

Optional query string parameters	• start: This is the start date-time of the query range.
	• end: This is the end date-time of the query range.
	• severity: This is the detection severity filter. Values are informational, low, medium, high.
	• detection_type: This is the detection type filter.
	• detected_on: This is the detected on filter.
	• event_number: This is the event number filter.
	• device: This is the device name filter.
	• status: The values for this are new, in progress, follow up, reviewed, done, false positive.
	• page: This is the page number to request.
	• page_size: This is the number of detection records to retrieve per page.
	• sort: This sorts by the following fields (adding "-" in front of the value denotes descending order):
	  • Severity
	  • OccurrenceTime
	  • Status
	  • Device
	  • PhoneticId
	  • Description
	  • ReceivedTime

Example	retrieve the first page with up to 100 detections, with a high severity, and sorted by occurrence time: https://protectapi.cylance.com/detections/v2/csv?page=1&page_size=100&severity=High&sort=OccurrenceTime
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
Cylance Id	This is the ID for the device.
Device	This is the name of the device.

Field Name	Description
Detected On	This is the time when the detection occurred according to the associated endpoint agent.
Detection	This is the description of the detection.
Detection Id	This is the easy-to-read version of the ID that is probabilistically unique.
Id	This is the unique ID for the detection.
ReceivedTime	This is the time when the detection was received by Cylance's cloud services.
Severity	This is the criticality of an observance of a detection.
Status	This is the status of the detection workflow.

Get detections by severity

Request a list of CylanceOPTICS aggregated detection resources by severity for a tenant. This is useful for making histograms.

Service endpoint	/detections/v2/severity?start={detection_start_timestamp}&end{detection_end_timestamp} &interval={detection_interval}
Optional query string parameters	• start: This is the start date-time of the query range. • end: This is the end date-time of the query range. • interval: This is the timer interval used for grouping detection resources. • detection_type: This is the detection type filter. • detected_on: This is the detected on filter. • event_number: This is the event number filter. • device: This is the device name filter. • status: The values for this are new, in progress, follow up, reviewed, done, false positive.
Example	https://protectapi.cylance.com/detections/v2/severity?start=2019-09-13T00:00:00Z&end=2019-09-15T23:59:59Z&interval=1d
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
counts	This is the number of detections found, grouped by severity (informational, medium, and high).
detected_on	This is the time when the detection was received by Cylance's cloud services.
facet	This is the facet used for the search. This is severity.
filters	This is the list of filters used on the request.

Update detection

Update the status or comment fields for an existing detection for a tenant.

Service endpoint	/detections/v2/update
Optional query string parameters	—
Example	https://protectapi.cylance.com/detections/v2/update
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:update scope encoded

Request

Request with Status:

```
[
    {
        "detection_id": "f2d6c020-53e2-4300-9005-2e006d9a0f57",
        "field_to_update": {
            "status": "Done"
        }
    }
]
```

Request with Comment:

```
[
```

```
    {
        "detection_id": "f2d6c020-53e2-4300-9005-2e006d9a0f57",
        "field_to_update": {
            "comment": "Add comment"
        }
    }
]
```

When creating the request JSON, include the status or comment string, but not both in the same request. Attempting to send the request with the status and comment strings included will result in a 400 bad request error.

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
comment	This is the comment of the detection.
status	This is the status of the detection. • Done: All actions are complete for this detection. • False Positive: The detection is considered a false positive. • Follow Up: This detection requires someone to follow-up on it. • In Progress: The detection is currently being reviewed and worked on. • New: The detection is new. • Reviewed: The detection has been reviewed, but no actions have been taken.

Delete detection

Soft delete a specific CylanceOPTICS detection resource belonging to a tenant. Use get detections to obtain the unique ID for the detection.

Service endpoint	/detections/v2/{detection_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/detections/v2/f2d6c020-53e2-4300-9005-2e006d9a0f57
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Delete detections

Delete CylanceOPTICS detection resources for a specific tenant.

Service endpoint	/detections/v2/
Optional query string parameters	—
Example	https://protectapi.cylance.com/detections/v2/
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:delete scope encoded

Request

```
{
    "ids": [
        "f2d6c020-53e2-4300-9005-2e006d9a0f57",
        "23f22a53-e656-4253-8bc5-e40b13e980d4"
    ]
}
```

Response

Please see the Response status codes for more information.

Package deployment API

CylanceOPTICS users can now interact with a hardened Python interpreter that is present locally on each endpoint that is running CylanceOPTICS v2.3.1000 or later. This new feature allows users to interact with their endpoints in an efficient and technical manner to accomplish tasks on endpoints in an automated fashion. By default, Cylance is supporting 5 capabilities to collect different forensic artifacts from targeted endpoints. These capabilities include:

- Collecting master file table (MFT) artifacts from NTFS volumes.
- Collecting entire Windows registry hives from endpoints.
- Collecting entire Windows event log files from endpoints.
- Collecting web browser history databases from Chrome, Firefox, Internet Explorer, Edge, Opera, and Safari.
- Collecting common application execution records, including Amcache, Prefetch, and Shimcache.

Users can also configure and deploy custom packages to conduct custom, scripted actions against endpoints. This allows customers to upload in-house or third-party scripts and applications to Cylance's cloud services and deploy them to endpoints. This scripting is done via interacting with the local Python interpreter built into CylanceOPTICS, allowing for an easily extensible set of capabilities.

After packages have been deployed and executed on endpoints, users can automatically upload the resulting data to SMB shares or SFTP servers for centralized collection and analysis by other forensic or incident response tools. Users can also configure packages to store the results locally on the endpoints for retrieval at a later time.

The CylanceOPTICS package deployment supports up to 20 packages for your organization. Each package has a maximum file size of 70MB. These capabilities and workflows around the package deployment feature are exposed via Cylance's API.

Create package

Create a new CylanceOPTICS package resource for a tenant.

Service endpoint	/packages/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgconfig:create scope encoded

Request

```
{
    "checksum":
 "bf17366ee3bb8068a9ad70fc9e68496e7e311a055bf4ffeeff53cc5d29ccce52",
    "packageDescriptor": {
        "name": "Test Package",
        "description": "This is a test package",
```

```
        "examples": [],
        "packageInfo": {
            "fileType": "python",
            "fileName": "hello_world.py",
            "entryPoint": ""
        },
        "version": 1
    }
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
checksum	This is the SHA256 hash for the package.
description	This is a description of what the package does.
examples	This is a list of examples of how to use the package. This information is optional. • description: A description of what the example does. • invocationString: An example of how to invoke the package.
name	This is the name of the package.
packageInfo	This is the package level documentation and annotation. • entryPoint: The point of execution for the package. • fileName: The name of the package file. • fileType: The file type of the package. Only Python is supported.
version	This is the version of the package, which must be 1 or higher.

Response JSON schema

Field Name	Description
packageId	This is the unique identifier for the package.
packageUrl	This is the URL to retrieve the package (after the actual package has been uploaded).
uploadTo	This is the URL used to upload the package.

Get packages

Request a page with a list of packages belonging to a tenant, sorted by the uploaded date, in descending order (most recent uploaded package listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 20 respectively.

Service endpoint	/packages/v2?page=m&page_size=n

Optional query string parameters	• page: This is the page number to request.
	• page_size: This is the number of device records to retrieve per page.
	• sort: This sorts by the following fields (adding "-" in front of a value denotes descending order).
	  • packageId: Filter by package ID
	  • uploadedOn: Filter by the uploaded timestamp (in UTC)
	  • uploadedBy.id: Filter by the user ID of the user who uploaded the package
	  • uploadedBy.login: Filter by the email of the user who uploaded the package
	  • size: Filter by the size of the package (in bytes)
	  • status: Filter by the status of the package upload process, values are started, success, failed, or timeout
	  • timeout: Filter by the amount of time (in seconds) for the package to upload before the status changes to timeout
	  • packageDescriptor.name: Name of the package
	• category: This filters by the package category. The values are custom or cylance.

Example	retrieve the first page with up to 100 Packages, sorted by a success status: https://protectapi.cylance.com/packages/v2?page=1&page_size=100&status=success
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgconfig:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
category	This is the category of the package. The values are custom or cylance.

Field Name	Description
downloadUrl	This is the URL to download the package from.

packageDescriptor	This is the package metadata, provided by the user.
	• description: This is the description of the package.
	• examples: This is the list of examples of how to use the package.
	  • invocationString: This is an example of how to invoke the package.
	  • description: This is a description of what the example does.
	• name: This is the name of the package.
	• packageId: This is the unique ID for the package.
	• packageInfo: This is the package level documentation or annotation.
	  • fileType: This is the file type of the package, only Python is supported.
	  • fileName: This is the name of the package file.
	  • entryPoint: This is the point of execution for the package.
	• version: This is the version of the package.

packageId	This is the unique identifier for the package.
page_number	This is the page number requested.
page_size	This is the page size requested.
playbookCount	This is the number of playbooks to which the package is associated.
size	This is the size of the package (in bytes).
status	This is the status of the package in the upload process.
timeout	This is the amount of time (in seconds) for the package to upload before the status changes to timeout.
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved based on the page size specified.
uploadedBy	This is the unique identifier of the user who uploaded the package. • id: The unique ID for the user. • login: The email address of the user.
uploadedOn	This is the date and time (in UTC) when the package was uploaded.

Get package

Request a specific package resource belonging to a tenant. Use get packages to obtain the unique package ID.

Service endpoint	/packages/v2/{unique_package_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2/e378dacb-9324-453a-b8c6-5a8406952195
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgconfig:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
category	This is the category of the package. The values are custom or cylance.
downloadUrl	This is the URL to download the package from.

packageDescriptor	This is the package metadata, provided by the user.
	• description: This is the description of the package.
	• examples: This is a list of examples of how to use the package.
	  • description: This is a description of what the example does.
	  • invocationString: This is an example of how to invoke the package.
	• name: This is the name of the package.
	• packageInfo: This is the package level documentation or annotation.
	  • entryPoint: This is the point of execution for the package.
	  • fileName: This is the name of the package file.
	  • fileType: This is the file type of the package. Only Python is supported.
	• packageId: This is the unique identifier for the package.
	• version: This is the version of the package.

packageId	This is the unique identifier for the package.
playbookCount	This is the number of playbooks that the package is associated with.

Field Name	Description
size	This is the size of the package, in bytes.
status	This is the status of the package in the upload process. The statuses are started, success, failed, and timeout.
timeout	This is the amount of time (in seconds) for a package upload before the status changes to timeout.
uploadedBy	These are the unique identifiers of the user who uploaded the package. • id: This is the unique ID for the user. • login: This is the email address of the user.
uploadedOn	This is the date and time (in UTC) when the package was uploaded.

Delete package

Delete a specific package resource belonging to a tenant. Use get packages to obtain the unique package ID.

Service endpoint	/packages/v2/{unique_package_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2/e378dacb-9324-453a-b8c6-5a8406952195
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgconfig:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Create package execution

Create a new CylanceOPTICS package execution resource for a specific tenant, which triggers a package to execute on the device or on devices in a specific zone.

Service Endpoint	/packages/v2/executions
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2/executions
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgdeploy:create scope encoded
Notes	• To create a package execution, either provide a list of devices or a list of zones. • For "devices" or "zones", use a format that is all upper case with the dashes removed. Example: "E378DACB9324453AB8C65A8406952195" • For "package" use the UUID4 format. Example: "61d8944e-d900-4724-87eb-d10078b90a41"

Request

Request with device ID and destination local:

```
{
    "execution": {
        "name": "Package Execution",
        "target": {
            "devices": [
                "E378DACB9324453AB8C65A8406952195"
            ]
        },
        "destination": "",
        "packageExecutions": [
            {
                "arguments": [
                    "-browser ALL"
                ],
                "package": "61d8944e-d900-4724-87eb-d10078b90a41"
            }
        ],
        "keepResultsLocally": true
    }
}
```

Request with zone ID and destination FTP:

```
{
    "execution": {
        "name": "Package Execution",
        "target": {
            "devices": [
                "E378DACB9324453AB8C65A8406952195"
            ]
        },
        "destination": "",
```

```
        "packageExecutions": [
            {
                "arguments": [
                    "-browser ALL"
                ],
                "package": "61d8944e-d900-4724-87eb-d10078b90a41"
            }
        ],
        "keepResultsLocally": true
    }
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
destination	This is the FTP, SFTP, or SAMBA URL for saving the results. If saving the results to the local disk drive, leave this empty ("").
keepResultsLocally	This is the setting to save the results to the local disk drive. If true, the results are saved to file://[Cylance Data Directory]/Optics.
name	This is the name of the execution.
packageExecutions	This is the list of packages to execute. • arguments: This is the list of arguments for the package. See examples from packageDescriptor. • package: This is the packageID for the package. As an example, you can get the packageID for a package through the “Get Packages” query.
target	These are the devices or zones to execute the packages against. • devices: This is the list of device IDs to execute the packages against. • zones: This is the list of zone IDs to execute the packages against. Target devices only or zones only per request, not both. Device IDs and zone IDs must be uppercase letters and no hyphens.

Response JSON schema

Field Name	Description
createdAt	This is the date and time (in UTC) when the execution was requested.

Field Name	Description
createdBy	This is the user who requested the execution. • id: This is the unique ID for the user. • login: This is the email address of the user.
destination	This is the FTP, SFTP, or SAMBA URL for saving the results.
deviceCount	This is the number of online devices at the moment the package execution request was made.
deviceStatuses	These are the statuses of the package executions on the devices. • acked (acknowledged): This is the number of devices that receive the package execution command but have not yet responded. • failed: This is the number of devices that failed to execute the packages. • succeeded: This is the number of devices that have successfully executed the packages.
id	This is the ID of the execution resource.
keepResultsLocally	This is the setting to save the results to the local disk drive. If true, the results are saved to file//[Cylance Data Directory]/Optics.
name	This is the name of the execution.
packageExecutions	This is the list of packages to execute. • arguments: This is the list of arguments for the package. See examples from packageDescriptor. • package: This is the packageID for the package. As an example, you can get the packageID for a package through the “Get Packages” query.
target	These are the devices and/or zones to execute the packages against. • devices: This is the list of device IDs to execute the packages against. • zones: This is the list of zone IDs to execute the packages against.

Get package executions

Request a page with a list of package executions belonging to a tenant, sorted by the uploaded date, in descending order (most recent uploaded package execution listed first). The page number and page size parameters are optional. When the values are not specified, the default values are 1 and 20 respectively.

Service endpoint	/packages/v2/executions?page=m&page_size=n

Optional query string parameters	• page: This is the page number to request.
	• page_size: This is the number of package records to retrieve per page.
	• sort: This sorts by the following fields (adding "-" in front of a value denotes descending order).
	  • id: Filter by unique ID of the execution
	  • name: Filter by name of the execution
	  • createdAt: Filter by date and time (in UTC) when the execution was requested
	  • createdBy.Id: Filter by ID of the user who requested the execution
	  • createdBy.Login: Filter by the email address of the user who requested the execution
	  • deviceCount: Filter by the number of online devices at the moment the package execution request was made

Example	retrieve the first page with up to 100 Detections, filtered by ID, and sorted by ID: https://protectapi.cylance.com/packages/v2/executions?page=1&page_size=100&id=1C04-1C2D&sort=id
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgdeploy:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
createdAt	This is the date and time (in UTC) when the execution was requested.
createdBy	This is the user who requested the execution. • id: This is the unique identifier of the user who requested the execution. • login: This is the email address of the user who requested the execution.
destination	This is the FTP, SFTP, or SAMBA URL for saving the results.
deviceCount	This is the number of online devices at the moment the package execution request was made.

Field Name	Description
deviceStatuses	These are the statuses of the package executions on the device. • acked (acknowledged): This is the number of devices that received the package. • failed: This is the number of devices that failed to execute the packages. • succeeded: This is the number of devices that have successfully executed the packages.
id	This is the unique identifier of the execution resource.
keepResultsLocally	This is the setting to save the results to the local disk drive. If true, the results are saved to file://[Cylance Data Directory]/Optics.
name	This is the name of the execution.
packageExecutions	This is the list of packages to execute. • arguments: This is the list of arguments for the package. See examples from packageDescriptor. • package: This is the URL from which to download the package resource.
page_number	This is the page number requested.
page_size	This is the page size requested.
target	These are the devices and/or zones to execute the packages against. • devices: This is the list of device IDs to execute the packages against. • The list of zone IDs to execute the packages against.
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved based on the page size specified.

Get package execution

Request a specific package execution resource belonging to a tenant. Use Get Package Executions to obtain the unique package execution ID.

Service endpoint	/packages/v2/executions/{unique_execution_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2/executions/abebf88c-f283-4edc-834b-aa8ad3bc682c
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgdeploy:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
createdAt	This is the date and time (in UTC) when the execution was requested.
createdBy	This is the user who requested the execution. • id: This is the unique ID for the user. • login: This is the email address of the user.
destination	This is the FTP, SFTP, or SAMBA URL for saving the results.
deviceCount	This is the number of online devices at the moment the package execution request was made.
deviceStatuses	These are the statuses of the package executions on the devices. • acked (acknowledged): This is the number of devices that received the package execution. • failed: This is the number of devices that failed to execute the packages. • succeeded: This is the number of devices that have successfully executed the packages.
id	This is the ID of the execution resource.
keepResultsLocally	This is the setting to save the results to the local disk drive. If true, the results are saved to file://[Cylance Data Directory]/Optics.
name	This is the name of the execution.
packageExecutions	This is the list of packages to execute. • arguments: This is the list of arguments for the package. See examples from packageDescriptor. • package: This is the URL to download the package resource from.

Field Name	Description
target	These are the devices and/or zones to execute the package against. • devices: This is the list of device IDs to execute the packages against. • zones: This is the list of zone IDs to execute the packages against.

Delete package execution

Delete a specific package resource belonging to a tenant. Use Get Package executions to obtain the unique package ID.

Service endpoint	/packages/v2/executions/{unique_execution_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/packages/v2/executions/abebf88c-f283-4edc-834b-aa8ad3bc682c
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspkgdeploy:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
createdAt	This is the date and time (in UTC) when the execution was requested.
createdBy	This is the user who requested the execution. • id: This is the unique ID for the user. • login: This is the email address of the user.
destination	This is the FTP, SFTP, or SAMBA URL for saving the results.

Field Name	Description
deviceCount	This is the number of online devices at the moment the package execution request was made.
deviceStatuses	These are the statuses of the package executions on the devices. • acked (acknowledged): This is the number of devices that received the package execution. • failed: This is the number of devices that failed to execute the packages. • succeeded: This is the number of devices that have successfully executed the packages.
id	This is the ID of the execution resource.
keepResultsLocally	This is the setting to save the results to the local disk drive. If true, the results are saved to file://[Cylance Data Directory]/Optics.
name	This is the name of the execution.
packageExecutions	This is the list of packages to execute. • arguments: This is the list of arguments for the package. See examples from packageDescriptor. • package: This is the URL to download the package resource from.
target	These are the devices and/or zones to execute the package against. • devices: This is the list of device IDs to execute the packages against. • zones: This is the list of zone IDs to execute the packages against.

Detection rule API

The CylanceOPTICS Detection Rules API allows users to create or update rules to help monitor an organization for security threats or anomalous behavior. The flexibility of detection rules allows users to monitor for broad behavior characteristics (for example, files being created with certain naming patterns) or search for a targeted series of events (for example, a process with a certain file signature thumbprint that then creates files and initiates network connections).

The CylanceOPTICS Detection Rules API includes:

- Getting the content of a detection rule.
- Getting a list of detection rules for a tenant.
- Getting a list of detection rules as a .csv file.
- Validating a detection rule.
- Creating a detection rule.
- Updating a detection rule.
- Deactivating (or soft deleting) a detection rule.
- Getting a natural language representation of a detection rule.
- Getting a count of how many detection rules exist in a tenant.

Get Detection Rule List

Retrieve a list of Detection rules available in a tenant.

Service Endpoint	/rules/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page.
Example	Return the first page with 100 devices: https://protectapi.cylance.com/rules/v2?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Category	This is the category of rule grouping that the detection rule belongs to. Possible values include: • Custom: These are custom rules that users have uploaded to a tenant. • Cylance rules: These are the rules from Cylance. • Cylance experimental: These are the rules from Cylance that are deemed to be experimental.
Description	This is the description of the detection rule.
DeviceCount	This is the number of devices that have the detection rule applied.
Id	This is the unique ID of the detection rule.
LastModified	This is the timestamp (in UTC) of the last time that the detection rule was modified.
ModifiedBy	This is an object detailing the last user to modify the detection rule. It includes the following fields: • id: This is the unique ID of the user who modified the detection rule. • login: This is the email address of the user who modified the detection rule.
Name	This is the name of the detection rule.
OperatingSystems	This is an object detailing the operating systems that the detection rule can be applied to. It will include the "name" field. This can consist of: • "Windows" • "MacOS"
page_number	This is the current page number of results.
page_size	This is the number of items on the page.
RulesetCount	This is the number of detection rule sets that have the detection rule enabled.
Severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
total_number_of_items	This is the total number of detection rules in the tenant.
total_pages	This is the total number of pages of this size.
Version	This is the version of the detection rule.

Get detection rule .csv list

Retrieve a .csv file where every line represents a detection rule available in the tenant.

Service endpoint	/rules/v2/csv
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/csv
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Category	This is the category that the detection rule belongs to.
Description	This is the description of the detection rule.
Device Count	This is the number of devices that have the detection rule applied.
Id	This is the unique ID of the detection rule.
Last Modified	This is the timestamp (in UTC) of the last time that the detection rule was modified.
Modified By	This is the email address of the user who last modified the detection rule.
Name	This is the name of the detection rule.
Ruleset Count	This is the number of detection rule sets that have the detection rule enabled.
Severity	This is the severity of the detection rule.
Version	This is the version of the detection rule.

Get detection rule

Retrieve the content of a detection rule in its native JSON structure.

Service Endpoint	/rules/v2/{rule_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/008ece50-49af-472a-b0d8-3c3700883738
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsdetect:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
ActivationCanUtlize DeviceStateEvents	This indicates if state events (historical rundowns) should be considered when evaluating for matches.
ActivationLifetimeLimit	This is the amount of time a rule is active. If the rule has been active past this duration, then the instance of the rule will be removed.
AllowMultipleActivations PerContext	This indicates if the rule can be activated multiple times, simultaneously.
Description	This is the description for the detection rule.
Id	This is the unique identifier for the detection rule.
MaximumConcurrent Activations	This indicates the maximum number of concurrently executing instances of this rule.
Name	This is the name of the detection rule.

Field Name	Description
NotValidAfter	This is the date and time (in UTC) after which the detection rule is not valid.
NotValidBefore	This is the date and time (in UTC) before which the detection rule is not valid.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	These are the affected operating systems. • Name: The name of the type of operating system (like Windows, macOS, or Linux).
Paths	This defines the paths by which this deterministic finite automata (DFA) can be iterated.
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
RuleSource	This is the source of the rule (for example, Cylance).
RuleSourceGrouping	This is the classification or designator for the rule source (for example, CylanceOPTICS).
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the detection rule.
TerminateActiveDfaIf ActivatingProcessesEnd	If the activating process (and, if applicable, all other processes that have been absorbed as activating processes) end, then this will terminate the active DFA.
Version	This is the version of the detection rule.

Validate detection rule

Allows a user to validate a detection rule's JSON by sending the native JSON structure of a detection rule to a validation service.

Service endpoint	/rules/v2/validate
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/validate
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:read scope encoded

Request

```
{
    "Name": "Name of Detection Rule",
    "Description": "Description of Detection Rule",
    "Severity": "Medium",
    "ObjectType": "DetectionRule",
    "OperatingSystems": [
        {
            "Name": "Windows",
        }
    ],
    "Plugin": {
        "Name": "OpticsDetector"
    },
    "Product": {
        "Name": "CylanceOPTICS"
    },
    "SchemaVersion": 1,
    "States": [
        {
            "Name": "MaliciousApp",
            "Scope": "Global",
            "Function": "Function",
            "FieldOperators": {
                "Function": {
                    "Type": "EqualsAny",
                    "Operands": [
                        {
                            "Source": "LiteralSet",
                            "Data": "badapp.exe"
                        }
                    ],
                    "OperandType": "string",
                    "Options": {
                        "IgnoreCase": true
                    }
                }
            },
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
```

```
                    "Position": "PostActivation"
                }
            ],
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "Process",
                        "SubCategory": "",
                        "Type": "*"
                    }
                }
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
Description	This is the description for the detection rule.
Name	This is the name of the detection rule.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	This is the affected operating systems. • Name: This is the name of the type of operating system (like Windows, macOS, or Linux).
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational

Field Name	Description
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the Detection Rule.

Response JSON schema

Field Name	Description
errors	This is a list of error messages that will prevent the Detection Rule from validating and operating correctly.
valid	This returns "true" if the Detection Rule passes validation. It returns "false" if the Detection Rule does not pass validation.
warnings	This is a list of warning message strings that may impact the performance or validity of the Detection Rule.

Create detection rule

Allows a caller to create a new detection rule by sending the native JSON structure of a detection rule.

Service endpoint	/rules/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:create scope encoded

Request

```
{
    "Name": "Name of Detection Rule",
    "Description": "Description of Detection Rule",
    "Severity": "Medium",
    "ObjectType": "DetectionRule",
    "OperatingSystems": [
        {
            "Name": "Windows"
        }
    ],
```

```
    "Plugin": {
        "Name": "OpticsDetector"
    },
    "Product": {
        "Name": "CylanceOPTICS"
    },
    "SchemaVersion": 1,
    "States": [
        {
            "Name": "MaliciousApp",
            "Scope": "Global",
            "Function": "Function",
            "FieldOperators": {
                "Function": {
                    "Type": "EqualsAny",
                    "Operands": [
                        {
                            "Source": "LiteralSet",
                            "Data": "badapp.exe"
                        }
                    ],
                    "OperandType": "string",
                    "Options": {
                        "IgnoreCase": true
                    }
                }
            },
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                }
            ],
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "Process",
                        "SubCategory": "",
                        "Type": "*"
                    }
                }
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
Description	This is the description for the detection rule.
Name	This is the name of the detection rule.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	These are the affected operating systems. • Name: This is the name of the type of operating system (like Windows, macOS, or Linux).
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the detection rule.

Response JSON schema

Field Name	Description
Description	This is the description for the detection rule.
Id	This is the unique identifier for the detection rule.
Name	This is the name of the detection rule.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule

Field Name	Description
OperatingSystems	This is the affected operating systems. • Name: This is the name of the type of operating system (like Windows, macOS, or Linux).
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
RuleSourceGrouping	This is the classification or designator for the rule source (for example, CylanceOPTICS).
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. The possible values are: • High • Medium • Low • Informational
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the detection rule.
Version	This is the version of the detection rule.

The response JSON schema contains the entirety of the Detection Rule Logic.

The "id" and "version" fields are automatically populated when the request is submitted.

Update detection rule

Update a detection rule by sending a new JSON structure.

Service endpoint	/rules/v2/{rule_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/c407f28a-3805-4014-b32c-0c2553ac1e10
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:update scope encoded

Request

```
{
    "Name": "Name of Detection Rule",
    "Description": "Description of Detection Rule",
    "Severity": "High",
    "ObjectType": "DetectionRule",
    "OperatingSystems": [
        {
            "Name": "Windows"
        }
    ],
    "Plugin": {
        "Name": "OpticsDetector"
    },
    "Product": {
        "Name": "CylanceOPTICS"
    },
    "SchemaVersion": 1,
    "States": [
        {
            "Name": "MaliciousApp",
            "Scope": "Global",
            "Function": "Function",
            "FieldOperators": {
                "Function": {
                    "Type": "EqualsAny",
                    "Operands": [
                        {
                            "Source": "LiteralSet",
                            "Data": "badapp.exe"
                        }
                    ],
                    "OperandType": "string",
                    "Options": {
                        "IgnoreCase": true
                    }
                }
            },
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                }
            ],
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "Process",
                        "SubCategory": "",
                        "Type": "*"
                    }
                }
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
```

```
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
Description	This is the description for the detection rule.
Name	This is the name of the detection rule.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	These are the affected operating systems. • Name: This is the name of the type of operating system (like Windows, macOS, or Linux).
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the detection rule.

Response JSON schema

Field Name	Description
Description	This is the description for the detection rule.
Id	This is the unique identifier for the detection rule.

Field Name	Description
Name	This is the name of the detection rule.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	These are the affected operating systems. • Name: This is the name of the type of operating system (like Windows, macOS, or Linux).
Plugin	This is the CylanceOPTICS plugin associated with the detection rule.
Product	This is the name of the product associated with the detection rule.
RuleSourceGrouping	This is the classification or designator for the rule source (for example, CylanceOPTICS).
SchemaVersion	This is the version of the schema.
Severity	This is the severity assigned to the detection rule. The possible values are: • High • Medium • Low • Informational
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is a list of tags associated with the detection rule.
Version	This is the version of the detection rule.

The response JSON schema contains the entirety of the detection rule Logic.

The "id" and "version" fields are automatically populated when the request is submitted.

Deactivate or delete detection rule

"Soft delete" a detection rule and remove it from the detection rule dets.

Service endpoint	/rules/v2/{rule_id}/deactivate
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/c407f28a-3805-4014-b32c-0c2553ac1e10/deactivate

Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:update scope encoded

Request

None

Response

Please see the Response status codes for more information.

Detection rule sets are not automatically communicated to all endpoints when updates to detection rules are made. To ensure that the latest logic is applied to endpoints in the quickest manner, re-save any affected detection rule sets (either via the UI or API).

Get detection rule natural language representation

Retrieve the "natural language" representation of a rule. This process converts the detection rule logic into a series of 'AND's, 'OR's, and 'NOT's to describe what the detection rule looks for. The underlying logic extracts from the JWT specified as the bearer value in the authorization request header the tenant's unique identifier to associated the detection rule resource with.

Service endpoint	/rules/v2/{rule_id}/natlang
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/c407f28a-3805-4014-b32c-0c2553ac1e10/natlang
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Get detection rule counts

Retrieve counts of how many devices, detection rule sets, and policies that have a particular detection rule applied.

Service endpoint	/rules/v2/{rule_id}/counts
Optional query string parameters	—
Example	https://protectapi.cylance.com/rules/v2/c407f28a-3805-4014-b32c-0c2553ac1e10/counts
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsrule:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
DeviceCount	This is the number of devices that have the requested detection rule applied.
PolicyCount	This is the number of device policies that have the requested detection rule applied.
RulesetCount	This is the number of detection rule sets that have the requested detection rule enabled.

Detection rule sets API

The CylanceOPTICS detection rule set API allows users to create a set of rules and apply that set to device policies.

The CylanceOPTICS detection rule set API includes:

- Getting content for a detection rule set
- Getting a list of detection rule sets
- Creating a detection rule set
- Retrieving a default detection rule set (retrieving a default template)
- Updating a detection rule set
- Deleting a detection rule set
- Deleting multiple detection rule sets
- Getting a list of detection rule sets as a .csv file

Get detection rule set list

Retrieve a list of detection rule sets available in a tenant.

Service endpoint	/rulesets/v2?page=m&page_size=n
Optional query string parameters	• page: This is the page number to request. • page_size: This is the number of device records to retrieve per page. You can also append any of the following to filter the results: • description: This is the case-insensitive query parameter to filter or sort by the description field. • last_modified: This is the case-insensitive query parameter to filter or sort by the Last Modified field, for example, the date/time format: 2019-04-10T21:39:54Z. Partial information will return matching results, for example, if 2019-04-10, 21:39:54, or 2019-04-10T21 is used, 2019-04-10T21:39:54Z will return, along with any other matching results. • modified_by.id: This is the case-insensitive query parameter to filter or sort by a user's unique ID. • modified_by.login: This is the case-insensitive query parameter to filter or sort by a user's email address. • device_count: This filters or sort the list by the number of applied devices. • sort: This sorts by field (adding '-' in front of the value denotes descending order).
Example	return the first page with 100 devices: https://protectapi.cylance.com/rulesets/v2?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Content-Type: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the user:create scope encoded.

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
page_size	This is the number of items on the page.
total_pages	This is the total number of pages of this size.
total_number_of_items	This is the total number of detection rules in the tenant.
page_number	This is the current page number of results.
page_items	This is a list of exception objects that are available in the tenant that will contain the following fields.
name	This is the name of the detection rule.
description	This is the description of the detection rule.
id	This is the unique ID of the detection rule.
last_modified	This is the timestamp (in UTC) of the last time that the detection rule was modified.
modified_by	This is an object detailing the last user to modify the detection rule. It includes the following fields: • id: This is the unique ID of the user who modified the detection rule. • login: This is the email address of the user who modified the detection rule.
policies	This is a list of policy IDs that a detection rule set is applied to.
device_count	This is the number of devices that have the detection rule applied.
category	This is the category of rule grouping that the detection rule belongs to. Possible values include: • Custom: These are custom rules that users have uploaded to a tenant. • Cylance rules: These are the rules from Cylance. • Cylance experimental: These are the rules from Cylance that are deemed to be experimental.

Get detection rule set .csv list

Retrieve a .csv where every line represents a detection rule set available in a tenant.

Service endpoint	/rulesets/v2/csv
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/csv
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Id	This is the unique ID of the exception.
Last Modified	This is the timestamp (in UTC) of the last time the detection rule set was modified.
Modified By	This is the email address of the user who last modified the detection rule set.
Name	This is the name of the detection rule set.
Description	This is the description of the detection rule set.
Notification	This is the notification message to display on a device if the detection rule triggers.
Category	This is the category of the detection rule set.
Device Count	This is the number of devices that have the detection rule set applied.

Get detection rule set

Retrieve the content of a detection rule set, including detection rules, response actions, detection exceptions, package playbooks, and the policies where the detection rule set is applied.

Service endpoint	/rulesets/v2/{ruleset_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/c407f28a-3805-4014-b32c-0c2553ac1e17
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
name	This is the name of the detection rule set.
description	This is the description of the detection rule set.
notification_message	This is the message to display on the endpoint when a detection rule is triggered.
id	This is the unique ID of the detection rule set.
last_modified	This is the timestamp (in UTC) of the last time that the detection rule set was modified.
modified_by	This is an object detailing the last user to modify the detection rule. It includes the following fields: • id: This is the unique ID of the user who modified the detection rule. • login: This is the email address of the user who modified the detection rule.
rules	This is a list of detection rule objects and their associated response actions, detection exceptions, and package playbooks.

Field Name	Description
detection_rule_id	This is the unique ID of the detection rule.
detection_rule_version	This is the version of the detection rule.
detection_name	This is the name of the detection rule.
detection_description	This is the description of the detection rule set.
category	This is the category of the detection rule.
severity	This is the severity assigned to the detectionrule. Possible values are: • High • Medium • Low • Informational
operating_systems	This is an object detailing the operating systems to which the detection rule can be applied. It will include the "name" field. This can consist of: • "Windows" • "MacOS"
date_added	This is the timestamp (in UTC) when the detection rule was added to the tenant.
enabled	This determines whether or not a detection rule is enabled in the detection rule set. When viewing the content of a detection rule set, this should always be set to 'true'.
notification_enabled	This determines whether or not the message defined in the 'notification_message' field should display on the device when the detection rule is triggered. To enable display desktop notification on device using the API, set notification_enabled and DisplayDesktopNotification to "true". To disable, set both to "false". The DisplayDesktopNotification setting enables or disables the feature. The notification_enabled setting affects the display desktop notification on device checkbox in the console as enabled (checked) or disabled (unchecked).
responses	This is a list of response objects for each response action enabled for a particular detection rule. each object will include the following fields: • template_id: This is the ID of the response template to use (this is provided by Cylance). • response_rule_id: This is the ID of the response rule to enable (this is provided by Cylance). • response_rule_version: This is the version of the response rule to enable (this is provided by Cylance). • description: This is the description/name of the response rule. • value: This is a currently unused field. • enabled: This will always be 'true' when viewing a detection rule set. • created: This is the date that the response rule was added to the tenant.

Field Name	Description
exceptions	This is a list of exception rule objects that should be applied to the detection rule. Each object will include the following fields: • exception_id: This is the unique ID of the exception rule. • enabled: This will always be 'true' when viewing a detection rule set. • name: This is the name of the exception rule.
playbooks	This is a list of package playbook unique IDs that will be executed when the detection rule is triggered on the device.

Create detection rule set

Create a new detection rule set. Detection rule sets can require a large number of fields and unique IDs to function properly. It is recommended to make a GET request to '/rulesets/v2/default' to obtain a properly formatted template prior to submitting a POST request described below.

Service endpoint	/rulesets/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:create scope encoded

Request

```
{
    "name": "Test Rule Set",
    "description": "Test Detection Rule Set",
    "notification_message": "",
    "category": "Custom",
    "rules": [
        {
            "detection_rule_id": "008ece50-49af-472a-b0d8-3c3700883738",
            "detection_rule_version": 1,
            "detection_name": "Gatekeeper Bypass (MITRE)",
            "detection_description": "Detects on usage to bypass Gatekeeper",
            "category": "Custom",
            "severity": "Low",
            "operating_systems": [
                {
                    "Name": "macOS"
                }
            ],
            "date_added": "2018-11-20T17:58:49Z",
```

```
            "enabled": false,
            "notification_enabled": false,
            "responses": [
                {
                    "template_id": "9686d82e-1b1d-45a9-977a-cf86f1063b15",
                    "response_id": "c6a26a8b-edce-4a68-8e18-4d16df74e455",
                    "response_rule_version": 1,
                    "description": "DisplayNotification",
                    "value": {},
                    "enabled": false,
                    "created": "2018-11-20T17:58:49Z"
                }
            ],
            "exceptions": [
                {
                    "exception_id": "",
                    "enabled": ,
                    "name": ""
                }
            ],
            "playbooks": [
                ""
            ]
        }
    ]
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
name	This is the name of the detection rule set.
description	This is the description of the detection rule set.
notification_message	This is the message to display on the endpoint when a detection rule is triggered.
id	This is the unique ID of the detection rule set.
last_modified	This is the timestamp (in UTC) of the last time that the detection rule set was modified.
modified_by	This is an object detailing the last user to modify the detection rule. It includes the following fields: • id: This is the unique ID of the user who modified the detection rule. • login: This is the email address of the user who modified the detection rule.
rules	This is a list of detection rule objects and their associated response actions, detection exceptions, and package playbooks.

Field Name	Description
detection_rule_id	This is the unique ID of the detection rule.
detection_rule_version	This is the version of the detection rule.
detection_name	This is the name of the detection rule.
detection_description	This is the description of the detection rule set.
category	This is the category of the detection rule.
severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
operating_systems	This is an object detailing the operating systems to which the detection rule can be applied. It will include the "name" field. This can consist of: • "Windows" • "MacOS"
date_added	This is the timestamp (in UTC) when the detection rule was added to the tenant.
enabled	This determines whether or not a detection rule is enabled in the detection rule set. When viewing the content of a detection rule set, this should always be set to 'true'.
notification_enabled	This determines whether or not the message defined in the 'notification_message' field should display on the device when the detection rule is triggered. To enable display desktop notification on device using the API, set notification_enabled and DisplayDesktopNotification to "true". To disable, set both to "false". The DisplayDesktopNotification setting enables or disables the feature. The notification_enabled setting affects the display desktop notification on device checkbox in the console as enabled (checked) or disabled (unchecked).
responses	This is a list of response objects for each response action enabled for a particular detection rule. Each object will include the following fields: • template_id: This is the ID of the response template to use (this is provided by Cylance). • response_rule_id: This is the ID of the response rule to enable (this is provided by Cylance). • response_rule_version: This is the version of the response rule to enable (this is provided by Cylance). • description: This is the description/name of the response rule. • value: This is a currently unused field. • enabled: This will always be 'true' when viewing a detection rule set. • created: This is the date that the response rule was added to the tenant.

Field Name	Description
exceptions	This is a list of exception rule objects that should be applied to the detection rule. Each object will include the following fields: • exception_id: This is the unique ID of the exception rule. • enabled: This will always be 'true' when viewing a detection rule set. • name: This is the name of the exception rule.
playbooks	This is a list of package playbook unique IDs that will be executed when the detection rule is triggered on the device.

Retrieve default detection rule set

Retrieve a properly formatted default detection rule set template that includes all detection rules, exceptions, playbooks, and response actions available in a tenant. The output of this request can be modified and submitted as a POST request to 'ruleset/v2' to create a new detection rule set.

Service endpoint	/rulesets/v2/default
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/default
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
name	This is the name of the detection rule set.
description	This is the description of the detection rule set.
notification_message	This is the message to display on the endpoint when a detection rule is triggered.

Field Name	Description
rules	This is a list of detection rule objects and their associated response actions, detection exceptions, and package playbooks.
detection_rule_id	This is the unique ID of the detection rule.
detection_rule_version	This is the version of the detection rule.
detection_name	This is the name of the detection rule.
detection_description	This is the description of the detection rule set.
category	This is the category of the detection rule.
severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
operating_systems	This is an object detailing the operating systems to which the detection rule can be applied. It will include the "name" field. This can consist of: • "Windows" • "MacOS"
date_added	This is the timestamp (in UTC) when the detection rule was added to the tenant.
enabled	This determines whether or not a detection rule is enabled in the detection rule set. When viewing the content of a detection rule set, this should always be set to 'true'.
notification_enabled	This determines whether or not the message defined in the 'notification_message' field should display on the device when the detection rule is triggered. To enable display desktop notification on device using the API, set notification_enabled and DisplayDesktopNotification to "true". To disable, set both to "false". The DisplayDesktopNotification setting enables or disables the feature. The notification_enabled setting affects the display desktop notification on device checkbox in the console as enabled (checked) or disabled (unchecked).

Field Name	Description
responses	This is a list of response objects for each response action enabled for a particular detection rule. Each object will include the following fields: • template_id: This is the ID of the response template to use (this is provided by Cylance). • response_rule_id: This is the ID of the response rule to enable (this is provided by Cylance). • response_rule_version: This is the version of the response rule to enable (this is provided by Cylance). • description: This is the description/name of the response rule. • value: This is a currently unused field. • enabled: This will always be 'true' when viewing a detection rule set. • created: This is the date that the response rule was added to the tenant.
exceptions	This is a list of exception rule objects that should be applied to the detection rule. Each object will include the following fields: • exception_id: This is the unique ID of the exception rule. • enabled: This will always be 'true' when viewing a detection rule set. • name: This is the name of the exception rule.
playbooks	This is a list of package playbook unique IDs that will be executed when the detection rule is triggered on the device.

Update detection rule set

Update a detection rule set by sending a new JSON structure.

Service endpoint	/rulesets/v2/{ruleset_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/c407f28a-3805-4014-b32c-0c2553ac1e17
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:update scope encoded

Request

```
{
    "name": "",
    "description": "",
    "notification_message": "",
```

```
    "category": "Custom",
    "rules": [
        {
            "detection_rule_id": "998ece50-49af-472a-b0d8-3c3700883736",
            "detection_rule_version": 1,
            "detection_name": "Gatekeeper Bypass (MITRE)",
            "detection_description": "Detects on usage of xattr or spctl to bypass
 Gatekeeper, by a non-root user (MITRE1144)",
            "category": "Cylance MITRE ATT&CK Rules",
            "severity": "High",
            "operating_systems": [
                {
                    "Name": "macOS"
                }
            ],
            "date_added": "2018-11-20T17:58:49Z",
            "enabled": false,
            "notification_enabled": false,
            "responses": [
                {
                    "template_id": "9986d82e-1b1d-45a9-977a-cf86f1063b14",
                    "response_id": "95947b5c-71ce-4a7e-a5e0-df5043402b5c",
                    "response_rule_version": 1,
                    "description": "DisplayDesktopNotification",
                    "value": {},
                    "enabled": false,
                    "created": "2018-11-20T17:58:49Z"
                }
            ],
            "exceptions": [
                {
                    "exception_id": "9f12a426-a956-4f4e-a698-df732ba1b295",
                    "enabled": false,
                    "name": "AO Exception"
                }
            ],
            "playbooks": []
        }
    ]
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
name	This is the name of the detection rule set.
description	This is the description of the detection rule set.
notification_message	This is the message to display on the endpoint when a detection rule is triggered.

Field Name	Description
rules	This is a list of detection rule objects and their associated response actions, detection exceptions, and package playbooks.
detection_rule_id	This is the unique ID of the detection rule.
detection_rule_version	This is the version of the detection rule.
detection_name	This is the name of the detection rule.
detection_description	This is the description of the detection rule set.
category	This is the category of the detection rule.
severity	This is the severity assigned to the detection rule. Possible values are: • High • Medium • Low • Informational
operating_systems	This is an object detailing the operating systems to which the detection rule can be applied. It will include the "name" field. This can consist of: • "Windows" • "MacOS"
date_added	This is the timestamp (in UTC) when the detection rule was added to the tenant.
enabled	This determines whether or not a detection rule is enabled in the detection rule set. When viewing the content of a detection rule set, this should always be set to 'true'.
notification_enabled	This determines whether or not the message defined in the 'notification_message' field should display on the device when the detection rule is triggered. To enable display desktop notification on device using the API, set notification_enabled and DisplayDesktopNotification to "true". To disable, set both to "false". The DisplayDesktopNotification setting enables or disables the feature. The notification_enabled setting affects the display desktop notification on device checkbox in the console as enabled (checked) or disabled (unchecked).

Field Name	Description
responses	This is a list of response objects for each response action enabled for a particular detection rule. Each object will include the following fields: • template_id: This is the ID of the response template to use (this is provided by Cylance). • response_rule_id: This is the ID of the response rule to enable (this is provided by Cylance). • response_rule_version: This is the version of the response rule to enable (this is provided by Cylance). • description: This is the description/name of the response rule. • value: This is a currently unused field. • enabled: This will always be 'true' when viewing a detection rule set. • created: This is the date that the response rule was added to the tenant.
exceptions	This is a list of exception rule objects that should be applied to the detection rule. Each object will include the following fields: • exception_id: This is the unique ID of the exception rule. • enabled: This will always be 'true' when viewing a detection rule Set. • name: This is the name of the exception rule.
playbooks	This is a list of package playbook unique IDs that will be executed when the detection rule is triggered on the device.

Delete detection rule set

Delete a detection rule set.

Service endpoint	/rulesets/v2/{ruleset_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/c407f28a-3805-4014-b32c-0c2553ac1e17
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:delete scope encoded

Request

None

Response

Please see the Response status codes for more information.

Delete multiple detection rule sets

Delete multiple detection rule sets in a single request.

Service endpoint	/rulesets/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2
Method	HTTP/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsruleset:delete scope encoded

Request

```
{
    "ids": [
        "c407f28a-3805-4014-b32c-0c2553ac1e17",
        "998ece50-49af-472a-b0d8-3c3700883736"
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
ids	This is a list of detection rule set IDs to be deleted.

Response JSON schema

Field Name	Description
id	This is a detection rule set ID that was attempted to be deleted.
success	This is a boolean field denoting whether or not the detection rule set was deleted.

Field Name	Description
message	This is a string containing any error, success, or warning messages.

Detection exceptions API

The CylanceOPTICS detection exceptions API allows users to add exceptions to their detection rules. Users can create a detection exception from a false positive detection, from the detection summary page, and from the detection details page.

The CylanceOPTICS detection exceptions API includes:

- Getting the content for a detection exception
- Getting a list of detection exceptions for a tenant
- Getting a list of detection exceptions as a .csv file
- Creating a detection exception
- Updating a detection exception
- Deactivating (or soft deleting) a detection exception

Get detection exceptions list

Retrieve a list of detection exception rules available in a tenant.

Service endpoint	/exceptions/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/exceptions/v2
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
page_size	This is the number of items on the page.
total_pages	This is the total number of pages of this size.

Field Name	Description
total_number_of_items	This is the total number of exceptions in the tenant.
page_number	This is the current page number of results.
page_items	This is a list of exception objects that are available in the tenant.
Id	This is the unique ID of the exception.
Name	This is the name of the exception.
Description	This is the description of the exception.
DeviceCount	This is the number of devices that have the exception applied.
LastModified	This is the timestamp (in UTC) of the last time that the exception was modified.
ModifiedBy	This is the last user to modify the exception. • id: This is the unique ID of the user who modified the exception. • login: This is the email address of the user who modified the exception.
OperatingSystem	These are the operating systems that the exception can be applied to. The "name" field can consist of: • "Windows" • "MacOS"
PolicyCount	This is the number of policies that have the exception applied.
RulesetCount	This is the number of detection rule sets that have the exception applied.
Version	This is the version of the exception.

Get detection exception .csv list

Retrieve a .csv where every line represents an exception rule available in the tenant.

Service endpoint	/rulesets/v2/csv
Optional query string parameters	—
Example	https://protectapi.cylance.com/rulesets/v2/csv
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Name	This is the name of the exception.
Id	This is the unique ID of the exception.
Version	This is the version of the exception.
Description	This is the description of the exception.
Last Modified	This is the timestamp (in UTC) of the last time the exception was modified.
Modified By	This is the email address of the user who last modified the exception.
Device Count	This is the number of devices that have the exception applied.
Ruleset Count	This is the number of detection rule sets that have the exception enabled.

Get detection exception content

Retrieve the content of an Exception in its native JSON structure.

Service endpoint	/exceptions/v2/{exception_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/exceptions/v2/24eff732-4d39-47df-b246-f7dbb8a8fd87
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Description	This is the description for the detection exception.
Id	This is the unique identifier for the detection exception.
Name	This is the name of the detection exception.
ObjectType	This is the object type for the detection.
OperatingSystems	This is the list of operating systems to which the detection exception applies.
Plugin	This is the name of the product feature to which the detection exception applies.
Product	This is the name of the Cylance product to which the detection exception applies.
SchemaVersion	This is the version of the schema to which the object conforms.
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is the list of tags associated with the detection exception.
Version	This is the version number for the detection exception.

Create detection exception

Create a new detection exception by sending the native JSON structure of a detection exception.

Service endpoint	/exceptions/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/exceptions/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:create scope encoded

Request

```
{
    "Name": "My Exception",
    "Description": "My Exception Description",
    "ObjectType": "ExceptionRule",
    "OperatingSystems": [
        {
            "Name": "Windows"
        }
    ],
    "Plugin": {
        "Name": "OpticsDetector"
    },
    "Product": {
        "Name": "CylanceOPTICS"
    },
    "SchemaVersion": 1,
    "States": [
        {
            "Name": "UnsignedProc",
            "Scope": "Global",
            "Function": "Function",
            "FieldOperators": {
                "Function": {
                    "Type": "EqualsAny",
                    "Operands": [
                        {
                            "Source": "LiteralSet",
                            "Data": iexplore.exe"
                        }
                    ],
                    "OperandType": "string",
                    "Options": {
                        "IgnoreCase": true
                    }
                }
            },
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                }
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS, Exception"
    ]
}
```

Response

Please see the Response status codes for more information.

Request and Response JSON schema

Field Name	Description
Description	This is the description for the detection exception.
Id	This is the unique identifier for the detection exception. Part of the response, after the detection exception is created.
Name	This is the name of the detection exception.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	This is the list of operating systems to which the detection exception applies.
Plugin	This is the name of the product feature to which the detection exception applies.
Product	This is the name of the Cylance product to which the detection exception applies.
SchemaVersion	This is the version of the schema.
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is the list of tags associated with the detection exception.
Version	This is the version number for the detection exception. It is part of the response, after the detection exception is created.

The "id" and "version" fields are automatically populated when the request is submitted.

Update detection exception

Update a detection exception by sending a new JSON structure.

Service endpoint	/exceptions/v2/{exception_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/exceptions/v2/24eff732-4d39-47df-b246-f7dbb8a8fd87
Method	HTTP/1.1 PUT

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:update scope encoded

Request

```
{
    "Name": "My Exception",
    "Description": "My Exception Description",
    "ObjectType": "ExceptionRule",
    "OperatingSystems": [
        {
            "Name": "Windows"
        }
    ],
    "Plugin": {
        "Name": "OpticsDetector"
    },
    "Product": {
        "Name": "Optics"
    },
    "SchemaVersion": 1,
    "States": [
        {
            "Name": "UnsignedProc",
            "Scope": "Global",
            "Function": "Function",
            "FieldOperators": {
                "Function": {
                    "Type": "EqualsAny",
                    "Operands": [
                        {
                            "Source": "LiteralSet",
                            "Data": iexplore.exe"
                        }
                    ],
                    "OperandType": "string",
                    "Options": {
                        "IgnoreCase": true
                    }
                }
            },
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                }
            ]
        }
    ],
    "Tags": [
        "Optics, Exception"
    ]
}
```

Response

Please see the Response status codes for more information.

Request or response JSON schema

Field Name	Description
Description	This is the description for the detection exception.
Id	This is the unique identifier for the detection exception. Part of the response, after the detection exception is updated.
Name	This is the name of the detection exception.
ObjectType	This is the type of object defined in this rule. • DetectionRule • ResponseRule
OperatingSystems	This is the list of operating systems to which the detection exception applies.
Plugin	This is the name of the product feature to which the detection exception applies.
Product	This is the name of the Cylance product to which the detection exception applies.
SchemaVersion	This is the version of the schema.
States	This is the list of all available states. If no paths are specified, the states are transitioned in the order they are specified.
Tags	This is the list of tags associated with the detection exception.
Version	This is the version number for the detection exception. Part of the response, after the detection exception is updated.

The "id" and "version" fields are automatically populated when the request is submitted.

Deactivate or delete detection exception

Deactivate (or "soft delete") a detection exception and remove it from the detection rule sets list.

Service endpoint	/exceptions/v2/{exception_id}/deactivate
Optional query string parameters	—
Example	https://protectapi.cylance.com/exceptions/v2/24eff732-4d39-47df-b246-f7dbb8a8fd87/deactivate

Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsexception:update scope encoded

Request

None

Response

Please see the Response status codes for more information. Detection rule sets are not automatically communicated to all endpoints when updates to detection exceptions are made. To ensure that the latest logic is applied to endpoints in the quickest manner, re-save any affected detection rule sets (either via the UI or API).

Device commands API

The CylanceOPTICS device commands API allows users to perform actions on the endpoint. For example, locking down an endpoint or retrieving a file from an endpoint.

The CylanceOPTICS device commands API includes:

- Locking down an endpoint
- Getting device lockdown history for a tenant
- Requesting a file retrieval from an endpoint
- Checking the file retrieval status for an endpoint
- Getting the retrieved file results

Lockdown device command

Create a CylanceOPTICS device lockdown command resource for a specific device.

Service endpoint	/devicecommands/v2/{{device_id}}/lockdown?value=true&expires=d:hh:mm
Optional query string parameters	• value: The value specifies whether to lockdown or not. The default value is 'true'. • expires: This is the duration of the lockdown. The Format is 'd:hh:mm', where the maximum is 3 days and the minimum is 5 minutes.
Example	https://protectapi.cylance.com/devicecommands/v2/45E07F34E76B4A9EB167D6D0C510D6BA/lockdown?value=true&expires=0:00:05
Method	HTTP/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticscommand:create scope encoded

Note: The format of the device ID must be in all caps with no hyphens.

Request

```
{
    "lockdown_config_id": 1,
    "lockdown_type": "Lockdown",
    "expires": "0:00:05",
    "parameters": {
        "Network": {}
    }
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
hostname	This is the hostname of the device that the lockdown command was issued to.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
connection_status	This displays whether or not the device is connected to Cylance's cloud services.
optics_device_version	This returns the numerical version of CylanceOPTICS running on the device.
password	This is the password required to unlock the device.
lockdown_expiration	This is the timestamp (in UTC) of when the current device lockdown is set to expire.
lockdown_initiated	This is the timestamp (in UTC) of when the current device lockdown was initiated.
lockdown_history	This is a list of historical device lockdown commands issued to this particular device.
user_id	This is the unique ID of the user who locked down the device.
timestamp	This is the timestamp (in UTC) of when the command was initiated.
command	This is the command that was executed.

Get device lockdown history

Request the current lockdown state and lockdown history for a specific device.

Service endpoint	/devicecommands/v2/{{device_id}}/lockdown
Optional query string parameters	—
Example	https://protectapi.cylance.com/devicecommands/v2/45E07F34E76B4A9EB167D6D0C510D6BA/lockdown
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticscommand:read scope encoded

Note: The format of the device ID must be in all caps with no hyphens.

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
hostname	This is the hostname of the device that the lockdown command was issued to.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
connection_status	This displays whether or not the device is connected to Cylance's cloud services.
optics_device_version	This returns the numerical version of CylanceOPTICS running on the device.
password	This is the password required to unlock the device.
lockdown_expiration	This is the timestamp (in UTC) of when the current device lockdown is set to expire.
lockdown_initiated	This is the timestamp (in UTC) of when the current device lockdown was initiated.
lockdown_history	This is a list of historical device lockdown commands issued to this particular device.
user_id	This is the unique ID of the user who locked down the device.
timestamp	This is the timestamp (in UTC) of when the command was initiated.
command	This is the command that was executed.

Get retrieved file results

Obtain a history of file retrieval requests for all devices in the tenant.

Service endpoint	/devicecommands/v2/retrieved_files?page=m&page_size=n

Optional query string parameters	• q: This is the case-insensitve search term. • page: This is the page number to request. Defaults to 1. • page_size: This is the number of file retrieval records to retrieve per page. Defaults to 20. • sort: This is used to sort by field (adding '-' in front of the value denotes descending order).
Example	https://protectapi.cylance.com/devicecommands/v2/retrieved_files?page=1&page_size=100
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticscommand:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
data	This is an object containing the various fields associated with the file retrieval request.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
user_id	This is the unique ID of the user who locked down the device.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
created_at	This is the timestamp (in UTC) of when the file retrieval was requested.
filepath	This is the file path of the requested file.
download_url	This is the unique URL and parameters required to download the retrieved file.

Field Name	Description
file_status	This is the status of the file retrieval. This will always be "PENDING" for newly created file retrievals. • REQUEST: The file retrieval has not been requested, but the user may issue a request for it. • RETRY_REQUEST: The file retrieval has been requested previously but no results were received. It can be requested again. • PENDING: The file retrieval has been requested but has not yet been completed. • DOES_NOT_EXIST: The file retrieval has been requested but is not present on the device. • AVAILABLE: The file is available for download. A download link (download_url) is generated and valid for the next 10 minutes. • UNAVAILABLE: The file is not available. This status may indicate that the requested device is not online, or the requested device failed to upload the file. This status will become RETRY_REQUEST after an hour.
file_status_description	This displays any errors or status messages associated with the retrieval request.
password	This is the password required to decrypt the retrieved file.
md5	This is the MD5 hash of the retrieved file.
sha1	This is the SHA1 hash of the retrieved file.
sha256	This is the SHA256 hash of the retrieved file.
correlation_id	This is the correlation ID associated with this action.
user_login	This is the email address of the user who initiated the file retrieval request.
hostname	This is the hostname of the device that the file retrieval was requested on.

Request file retrieval from device

Request that the specified file be retrieved from a specified device and stored in the management console for later analysis.

Service endpoint	/devicecommands/v2/{{device_id}}/getfile
Optional query string parameters	—
Example	https://protectapi.cylance.com/devicecommands/v2/45E07F34E76B4A9EB167D6D0C510D6BA/getfile
Method	HTTP/1.1 POST

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticscommand:read scope encoded

Note: The format of the device ID must be in all caps with no hyphens.

Request

```
{
    "file_path": "C:\path\to\file.txt"
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
data	This is an object containing the various fields associated with the file retrieval request.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
user_id	This is the unique ID of the user who locked down the device.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
created_at	This is the timestamp (in UTC) of when the file retrieval was requested.
filepath	This is the file path of the requested file.
download_url	This is the unique URL and parameters required to download the retrieved file.
file_status	This is the status of the file retrieval. This will always be "PENDING" for newly created file retrievals.
file_status_description	This displays any errors or status messages associated with the retrieval request.
password	This is the password required to decrypt the retrieved file.
md5	This is the MD5 hash of the retrieved file.
sha1	This is the SHA1 hash of the retrieved file.
sha256	This is the SHA256 hash of the retrieved file.

Field Name	Description
correlation_id	This is the correlation ID associated with this action.
user_login	This is the email address of the user who initiated the file retrieval request.
hostname	This is the hostname of the device that the file retrieval was requested on.

Check file retrieval status from device

Check the status of a previously requested file retrieval operation.

Service endpoint	/devicecommands/v2/{{device_id}}/getfile:get
Optional query string parameters	—
Example	https://protectapi.cylance.com/devicecommands/v2/45E07F34E76B4A9EB167D6D0C510D6BA/getfile:get
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticscommand:read scope encoded

Note: The format of the device ID must be in all caps with no hyphens.

Request

```
{
    "file_path": "C:\path\to\file.txt"
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
data	This is an object containing the various fields associated with the file retrieval request.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.

Field Name	Description
user_id	This is the unique ID of the user who locked down the device.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
created_at	This is the timestamp (in UTC) of when the file retrieval was requested.
filepath	This is the file path of the requested file.
download_url	This is the unique URL and parameters required to download the retrieved file.
file_status	This is the status of the file retrieval. This will always be "PENDING" for newly created file retrievals. • REQUEST: The file retrieval has not been requested, but the user may issue a request for it. • RETRY_REQUEST: The file retrieval has been requested previously but no results were received. It can be requested again. • PENDING: The file retrieval has been requested but has not yet been completed. • DOES_NOT_EXIST: The file retrieval has been requested but is not present on the device. • AVAILABLE: The file is available for download. A download link (download_url) is generated and valid for the next 10 minutes. • UNAVAILABLE: The file is not available. This status may indicate that the requested device is not online, or the requested device failed to upload the file. This status will become RETRY_REQUEST after an hour.
file_status_description	This displays any errors or status messages associated with the retrieval request.
password	This is the password required to decrypt the retrieved file.
md5	This is the MD5 hash of the retrieved file.
sha1	This is the SHA1 hash of the retrieved file.
sha256	This is the SHA256 hash of the retrieved file.
correlation_id	This is the correlation ID associated with this action.
user_login	This is the email address of the user who initiated the file retrieval request.
hostname	This is the hostname of the device that the file retrieval was requested on.

Focus view API

The CylanceOPTICS focus view API allows users to retrieve an information trail starting with the first event related to an artifact from an InstaQuery result or a CylancePROTECT Desktop event.

The CylanceOPTICS focus view API includes:

- Searching for focus view results
- Generating a focus view
- Getting a summary of a focus view
- Getting the results of a focus view
- Getting a list of focus views that have been made in a tenant

Get focus view list

Retrieve a list of focus views that have been made in the tenant.

Service endpoint	/foci/v2?page=m&page_size=n
Optional query string parameters	The 'q' request parameter was replaced with multiple request parameters to provide more flexibility when filtering the Focus View List. Any Get Focus View List requests that contain the 'q' request parameter will not return any results. Requests should use the following parameters: • artifact_type: This is the type of Artifact for the Focus View. Types include Protect, Process, File, and NetworkConnection. The artifact type is case-insensitive. • created_at: This is the date when the file retrieval was requested. The date format is YYYY-MM-DD. The results are for a 24 hour period. For example, using "&created_at=2019-11-01" will return results that occurred from 2019-11-01:00:00:00 to 2019-11-01:23:59:59. • description: This is the human-readable description for the Focus View. The description is case-insensitive. • hostname: This is the hostname of the device for which the retrieval was requested. The hostname is case-insensitive. • status: This is the status of the Focus View request or result. Statuses include AVAILABLE, DOES_NOT_EXIST, PENDING, REQUEST, RETRY_REQUEST, UNAVAILABLE, and UNKNOWN_DEVICE. The statuses are case-sensitive. • page: This is the page number to request. The default is 1. • page_size: This is the number of file retrieval records to retrieve per page. The default is 20. • sort: This is used to sort by field (adding '-' in front of the value denotes descending order).
Example	https://protectapi.cylance.com/foci/v2?page=1&page_size=100
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsfocus:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
page_size	This is the number of items per page.
total_pages	This is the total number of pages of this page size.
total_number_of_items	This is the total number of Focus Views available in the tenant.
page_number	This is the current page number.
page_items	This is a list of Focus View objects.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
artifact_type	This is the type of Artifact for the focus view. • Protect: Request a focus view for a CylancePROTECT Desktop-generated event. • Process: Request a focus view for a process artifact to visualize how a process interacts with the device. This is the most common option. • File: Request a focus view for a file artifact to visualize how the file has been interacted with. • NetworkConnection: Request a focus view for a network artifact to visualize communications associated with an IP address.
artifact_subtype	This field should always be "Uid" at this time.
value	This is the UID of the Artifact used to gather the focus view.
threat_type	This is an option field to use with a "Protect" artifact_type to denote the type of threat that a focus view is being generated for.
description	This is the human-readable description for the focus view.
id	This is the unique ID of the focus view.

Field Name	Description
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
created_at	This is the timestamp (in UTC) of when the file retrieval was requested.
hostname	This is the hostname of the device that the file retrieval was requested on.
status	This is the status of the focus view result or request. Possible values are: • AVAILABLE: A focus view has been generated and is available for viewing. • DOES_NOT_EXIST: The focus view requested on the device cannot be completed because the requested parameters do not exist on the device. • PENDING: The focus view has been requested. • REQUEST: The focus view has not been generated, but it can be requested. • RETRY_REQUEST: The focus view has not been generated. It was previously requested but no results were received. It can be requested again. • UNAVAILABLE: The focus view is not available, and the associated device is not online to fulfill the request. It can be requested at a later time. • UNKNOWN_DEVICE: The F focus view is not available, and the associated device is no longer known.
relations	This is a list of objects that are related to this focus view. The following fields can be contained: • Object: The URL of a focus view, InstaQuery, or Detection Event that is linked to this focus view. • Relationship: How the relationship was established.

Search for focus view results

Search for focus views by a list of device ID and CylancePROTECT Desktop event ID pairs, up to 200 at a time. The request requires both a CylancePROTECT Desktop event ID and device ID to determine whether or not a focus view can be created.

Service endpoint	/foci/v2/search
Optional query string parameters	—
Example	https://protectapi.cylance.com/foci/v2/search
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsfocus:list scope encoded

Request

```
[
    {
        "uid": "59F849F29BBE4F1F889AAF50F9153618",
        "device_id": "E378DACB9324453AB8C65A8406952195"
    }
]
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
uid	This is the unique ID of a CylancePROTECT Desktop event. This is "value" from Get focus view list.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.

Response JSON schema

Field Name	Description
uid	This is the unique ID of a CylancePROTECT Desktop event.
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
status	This is the status of the focus view result or request. Possible values are: • AVAILABLE: A focus view has been generated and is available for viewing. • PENDING: The focus view has been requested. • REQUEST: The focus view has not been generated, but it can be requested. • RETRY_REQUEST: The focus view has not been generated. It was previously requested but no results were received. It can be requested again. • DOES_NOT_EXIST: The focus view requested on the device cannot be completed because the requested parameters do not exist on the device. • UNAVAILABLE: The focus view is not available, and the associated device is not online to fulfill the request. It can be requested at a later time. • UNKNOWN_DEVICE: The focus view is not available, and the associated device is no longer known.
focus_id	This is the unique ID of the focus view.

Request a focus view

Request a focus view from a specified device.

Service endpoint	/foci/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/foci/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsfocus:create scope encoded

Request

```
{
    "device_id": "E378DACB9324453AB8C65A8406952195",
    "artifact_type": "Process",
    "artifact_subtype": "Uid",
    "value": "59F849F29BBE4F1F889AAF50F9153618",
    "threat_type": "THREAT",
    "description": "Focus View Example"
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.

Field Name	Description
artifact_type	This is the type of artifact for the focus view. • Protect: Request a focus view for a CylancePROTECT Desktop-generated event. • Process: Request a focus view for a process artifact to visualize how a process interacts with the device. This is the most common option. • File: Request a focus view for a file artifact to visualize how the file has been interacted with. • NetworkConnection: Request a focus view for a Network artifact to visualize communications associated with an IP address. • RegistryKey: Request a focus view for a registry artifact to visualize how the registry key or path has been interacted with.
artifact_subtype	This field should always be "Uid" at this time.
value	This is the UID of the artifact to gather a focus view about. This can be obtained from InstaQuery results, another focus view, the details/associated artifacts of a detection event, or anywhere else an artifact is referenced.
threat_type	This is an optional field to use with a "Protect" artifact_type to denote the type of threat that a focus view is being generated for.
description	This is the human-readable description for the focus view.

Response JSON schema

Field Name	Description
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
artifact_type	This is the type of artifact for the focus view. • Protect: Request a focus view for a CylancePROTECT Desktop-generated event. • Process: Request a focus view for a process artifact to visualize how a process interacts with the device. This is the most common option. • File: Request a focus view for a file artifact to visualize how the file has been interacted with. • NetworkConnection: Request a focus view for a network artfiact to visualize communications associated with an IP address. • RegistryKey: Request a focus view for a registry artifact to visualize how the registry key or path has been interacted with.
artifact_subtype	This field should always be "Uid" at this time.
value	This is the UID of the artifact to gather a focus view about. This can be obtained from InstaQuery results, another focus view, the details/associated artifacts of a detection event, or anywhere else an artifact is referenced.

Field Name	Description
threat_type	This is an optional field to use with a "Protect" artifact_type to denote the type of threat that a focus view is being generated for.
description	This is the human-readable description for the focus view.
id	This is the unique ID of the focus view.
tenant_id	This is the unique ID of the tenant associated with the focus view.
create_at	This is the timestamp (in UTC) of when the focus view was created.
hostname	This is the hostname of the device that the focus view was requested from.
status	This is the status of the focus view result or request. Possible values are: • AVAILABLE: A focus view has been generated and is available for viewing. • PENDING: The focus view has been requested. • REQUEST: The focus view has not been generated, but it can be requested. • RETRY_REQUEST: The focus view has not been generated. It was previously requested but no results were received. It can be requested again. • DOES_NOT_EXIST: The focus view requested on the device cannot be completed because the requested parameters do not exist on the device. • UNAVAILABLE: The focus view is not available, and the associated device is not online to fulfill the request. It can be requested at a later time. • UNKNOWN_DEVICE: The focus view is not available, and the associated device is no longer known.
relations	This is a list of objects that are related to this focus view. The following fields can be contained: • Object: This is the URL of a focus view, InstaQuery, or detection event that is linked to this focus view. • Relationship: This shows how the relationship was established.

Get a focus view summary

Get the results of an existing focus view.

Service endpoint	/foci/v2/{{focus_id}}
Optional query string parameters	—
Example	https://protectapi.cylance.com/foci/v2/A0AC3D2117C40D0576CED0D99069E96G
Method	HTTP/1.1 GET

Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsfocus:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
device_id	This is the unique device ID that the lockdown command was issued to. See About device ID for device ID formatting.
artifact_type	This is the type of artifact for the focus view. • Protect: Request a focus view for a CylancePROTECT Desktop-generated event. • Process: Request a focus view for a process artifact to visualize how a process interacts with the device. This is the most common option. • File: Request a focus view for a file artifact to visualize how the file has been interacted with. • NetworkConnection: Request a focus view for a network artifact to visualize communications associated with an IP address.
artifact_subtype	This field should always be "Uid" at this time.
value	This is the UID of the Artifact used to gather the focus view.
threat_type	This is an optional field to use with a "Protect" artifact_type to denote the type of threat that a focus view is being generated for.
description	This is the human-readable description for the focus view.
id	This is the unique ID of the focus view.
tenant_id	This is the unique tenant ID of the tenant that the device belongs to.
created_at	This is the timestamp (in UTC) of when the file retrieval was requested.
hostname	This is the hostname of the device that the file retrieval was requested on.

Field Name	Description
status	This is the status of the focus view result or request. The possible values are: • AVAILABLE: A focus view has been generated and is available for viewing. • PENDING: The focus view has been requested. • REQUEST: The focus view has not been generated, but it can be requested. • RETRY_REQUEST: The focus view has not been generated. It was previously requested but no results were received. It can be requested again. • DOES_NOT_EXIST: The focus view requested on the device cannot be completed because the requested parameters do not exist on the device. • UNAVAILABLE: The focus view is not available, and the associated device is not online to fulfill the request. It can be requested at a later time. • UNKNOWN_DEVICE: The focus view is not available, and the associated device is no longer known.
relations	This is a list of objects that are related to this focus view. The following fields can be contained: • Object: This is the URL of a focus view, InstaQuery, or detection event that is linked to this focus view. • Relationship: This shows how the relationship was established.

Get focus view results

Get the details of an existing focus view that is used to generate the chart and table in the UI.

Service endpoint	/foci/v2/{{focus_id}}/results
Optional query string parameters	—
Example	https://protectapi.cylance.com/foci/v2/A0AC3D2117C40D0576CED0D99069E96G/results
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticsfocus:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
id	This is the unique ID of the focus view.
status	This is the status of the focus view result or request. The possible values are: • AVAILABLE: A focus view has been generated and is available for viewing. • PENDING: The focus view has been requested. • REQUEST: The focus viewhas not been generated, but it can be requested. • RETRY_REQUEST: The focus view has not been generated. It was previously requested but no results were received. It can be requested again. • DOES_NOT_EXIST: The focus view requested on the device cannot be completed because the requested parameters do not exist on the device. • UNAVAILABLE: The focus view is not available, and the associated device is not online to fulfill the request. It can be requested at a later time. • UNKNOWN_DEVICE: The focus view is not available, and the associated device is no longer known.
result	This is the large structure of data that is used to generate the focus view chart and table in the UI. This field will only be populated if the status field is *AVAILABLE*. Parsing this data is beyond the scope of this guide.

InstaQuery API

The CylanceOPTICS InstaQuery API allows users to search for system artifacts stored locally by CylanceOPTICS - files, registry key persistence points, processes, etc. Users can investigate incidents, or hunt for potential threats, and then take appropriate remediation actions.

InstaQuery searches are zone based; unzoned endpoints cannot be searched via InstaQuery.

The CylanceOPTICS InstaQuery API includes:

- Creating an InstaQuery
- Getting a list of InstaQueries in a tenant
- Getting a specific InstaQuery
- Getting the results of an InstaQuery
- Archiving an InstaQuery

Get InstaQueries

Request a page with a list of CylanceOPTICS InstaQuery resources belonging to a tenant, sorted by occurrence time, in descending order (most recent occurred InstaQuery listed first). The page number and page size parameters are optional, when the values are not specified, they default to 1 and 20 respectively.

Service endpoint	/instaqueries/v2?page=m&page_size=n
Optional query string parameters	• q: This is the case-insensitive search term (e.g. name, zones, artifact). • archived: Include archived surveys. • originated-from: Limit the query by the relationship. • page: This is the page number to request. Defaults to 1. • page_size: This is the number of detection records to retrieve per page. Defaults to 20. • sort: Sort by field (adding '-' in front of the value denotes descending order).
Example	https://protectapi.cylance.com/instaqueries/v2?page=m&page_size=n
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticssurvey:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
page_number	This is the page number requested.
page_size	This is the page size requested.
total_number_of_items	This is the total number of resources.
total_pages	This is the total number of pages that can be retrieved based on the page size specified.
page_items	This is the list of detections belonging to the requested page.
name	This is the name of the InstaQuery.
description	This is the description of the InstaQuery.
artifact	This is the artifact type that was queried.
match_value_type	This is the type (or Facet) of the artifact that was queried.
match_values	This is the list of values that were queried for.
case_sensitive	This value indicates whether or not the InstaQuery should take case into account.
match_type	This is the match type configured for the query, either "fuzzy" or "exact."
zones	This is the list of zones queried.
filters	This is the list of filters applied to the InstaQuery.
relations	This is the list of objects (e.g.: Focus Views) that the InstaQuery is related to.
id	This is the unique ID of the InstaQuery.
archived	This is the timestamp of when the InstaQuery was archived.
results_available	This determines if the InstaQuery has returned any results.
progress	This provides the number of devices queried and the number of devices that have responded.

Create InstaQuery

Update CylanceOPTICS InstaQuery resources for a specific tenant.

Service endpoint	/instaqueries/v2

Optional query string parameters	—
Example	https://protectapi.cylance.com/instaqueries/v2
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticssurvey:create scope encoded

Request

```
{
    "name": "InstaQuery Name",
    "description": "Test InstaQuery",
    "artifact": "File",
    "match_value_type": "Path",
    "match_values": [
        "exe"
    ],
    "case_sensitive": true,
    "match_type": "Fuzzy",
    "zones": [
        "D27FF5C45C0D4F56A00DA1FB297E440F"
    ],
    "filters": [
        {
            "aspect": "OS",
            "value": "Windows"
        }
    ],
    "relations": [
        {
            "object": "/focus/focus_id",
            "relationship": "originated-from"
        }
    ]
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
name	This is the name of the InstaQuery.
description	This is the description of the InstaQuery.

Field Name	Description
artifact	This is the type of artifact to search. Possible values are "File", "Process", "NetworkConnection", and "RegistryKey".

match_value_type	This is the type of value (also known as a facet) to search. Possible values are dependent on the selected artifact type. Valid selections for each are as follows:
	• File
	  • Path
	  • Md5
	  • Sha2
	  • Owner
	  • CreationDateTime
	• Process
	  • Name
	  • Commandline
	  • PrimaryImagePath
	  • PrimaryImageMd5
	  • StartDateTime
	• NetworkConnection
	  • DestAddr
	  • DestPort
	• RegistryKey
	  • ProcessName
	  • ProcessPrimaryImagePath
	  • ValueName
	  • FilePath
	  • FileMd5
	  • IsPersistencePoint

match_values	This is a list of strings to be matched against for the InstaQuery.
case_sensitive	This determines whether to consider case sensitivity when matching values.
match_type	This determines whether or not to use an exact or "fuzzy" match. The default behavior of InstaQuery is to use a "fuzzy" match. Possible values are: • Fuzzy • Exact
zones	This is a list of zone IDs to perform the InstaQuery against.
filters	This is a list of filters when performing the InstaQuery.
aspect	This is the aspect (or type) of filters (for example, "OS").
value	This is the value to filter for (for example,. "Windows").

Field Name	Description
relations	This is a list of objects (for example, Focus View URLs) that are related to the InstaQuery. This is similar to the "Pivot Query" functionality in the Console.
object	This is the URL of the focus view that the InstaQuery relates to.
relationship	This is how the InstaQuery relates to the URL. This should almost always be "originated-from".

Response JSON schema

Field Name	Description
name	This is the name of the InstaQuery.
description	This is the description of the InstaQuery.
artifact	This is the type of artifact to search. Possible values are "File", "Process", "NetworkConnection", and "RegistryKey".

match_value_type	This is the type of value (also known as a facet) to search. Possible values are dependent on the selected artifact type. Valid selections for each are as follows:
	• File
	  • Path
	  • Md5
	  • Sha2
	  • Owner
	  • CreationDateTime
	• Process
	  • Name
	  • Commandline
	  • PrimaryImagePath
	  • PrimaryImageMd5
	  • StartDateTime
	• NetworkConnection
	  • DestAddr
	  • DestPort
	• RegistryKey
	  • ProcessName
	  • ProcessPrimaryImagePath
	  • ValueName
	  • FilePath
	  • FileMd5
	  • IsPersistencePoint

Field Name	Description
match_values	This is a list of strings to be matched against for the InstaQuery.
case_sensitive	This determines whether to consider case sensitivity when matching values.
match_type	This determines whether or not to use an exact or "fuzzy" match. The default behavior of InstaQuery is to use a "fuzzy" match. Possible values are: • Fuzzy • Exact
zones	This is a list of zone IDs to perform the InstaQuery against.
filters	This is a list of filters when performing the InstaQuery.
aspect	This is the aspect (or type) of filters (for example, "OS").
value	This is the value to filter for (for example, "Windows").
relations	This is a list of objects (for example, Focus View URLs) that are related to the InstaQuery. This is similar to the "Pivot Query" functionality in the Console.
object	This is the URL of the focus view that the InstaQuery relates to.
relationship	This is how the InstaQuery relates to the URL. This should almost always be "originated-from".
id	This is the unique identifier of the created InstaQuery.
created_at	This is the date and time that the InstaQuery was created.
progress	This is the progress of the InstaQuery.

Get InstaQuery

Request a specific InstaQuery resource belonging to a tenant.

Service endpoint	/instaqueries/v2{queryID}
Optional query string parameters	—
Example	https://protectapi.cylance.com/instaqueries/v2/AF593F38EDC1B743BDC0A6FCC53A03CE
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticssurvey:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
name	This is the name of the InstaQuery.
description	This is the description of the InstaQuery.
artifact	This is the type of artifact to search. Possible values are "File", "Process", "NetworkConnection", and "RegistryKey".

match_value_type	This is the type of value (also known as a facet) to search. Possible values are dependent on the selected artifact type. Valid selections for each are as follows:
	• File
	  • Path
	  • MD5
	  • SHA256
	  • Owner
	  • CreationDateTime
	• Process
	  • Name
	  • CommandLine
	  • PrimaryImagePath
	  • PrimaryImageMd5
	  • StartDateTime
	• NetworkConnection
	  • DestAddr
	  • DestPort
	• RegistryKey
	  • ProcessName
	  • ProcessPrimaryImagePath
	  • ValueName
	  • FilePath
	  • FileMd5
	  • IsPersistencePoint

match_values	This is a list of strings to be matched against for the InstaQuery.
case_sensitive	This determines whether to consider case sensitivity when matching values.

Field Name	Description
match_type	This determines whether or not to use an exact or "fuzzy" match. The default behavior of InstaQuery is to use a "fuzzy" match. Possible values are: • Fuzzy • Exact
zones	This is a list of zone IDs to perform the InstaQuery against.
filters	This is a list of filters when performing the InstaQuery.
aspect	This is the aspect (or type) of filters (for example, "OS").
value	This is the value to filter for (for example, "Windows").
relations	This is a list of objects (for example, Focus View URLs) that are related to the InstaQuery. This is similar to the "Pivot Query" functionality in the Console.
object	This is the URL of the focus view that the InstaQuery relates to.
relationship	This is how the InstaQuery relates to the URL. This should almost always be "originated-from".
id	This is the unique identifier of the created InstaQuery.
archived	This is the timestamp of when the InstaQuery was archived.
results_available	This determines if the InstaQuery has returned any results.
created_at	This is the date and time that the InstaQuery was created.
progress	This is the progress of the InstaQuery.

Get InstaQuery results

Request a CylanceOPTICS InstaQuery resource results belonging to a tenant.

Service endpoint	/instaqueries/v2{queryID}/results
Optional query string parameters	—
Example	https://protectapi.cylance.com/instaqueries/v2/AF593F38EDC1B743BDC0A6FCC53A03CE/results
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticssurvey:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
Id	This is the unique ID of the InstaQuery.
Status	This is the status of the InstaQuery.
Result	This is the list of responses to the InstaQuery.
@timestamp	This is the timestamp that the result was reported in Unix epoch time.
HostName	This is the hostname of the device that returned the result.
DeviceID	This is the unique ID of the device that returned the result.
@version	This is the version format of the result.
CorrelationID	This is the unique correlation ID of the result object.
Result	This is the object containing response data.
FirstObservedTime	This is the timestamp that the result was first observed on the system (for example, when a file was first observed on the system as in a file being created) .
LastObservedTime	This is the timestamp that the result was last observed on the system (for example, when a file was last observed as in the last time a file was interacted with). This value will be the same as the FirstObservedTimestamp for NetworkConnection and process artifacts.
Uid	This is the unique ID of the result.
Type	This is the type of artifact that the result's "properties" contain.
Properties	This is the object containing the individual elements of the result. This will vary depending on the artifact and type that was queried. The following 4 cells outline the possible property values:

Field Name	Description
File	• Path: This is the full path to the file. • CreationDateTime: This is the timestamp (in UTC) of when the file was created on the responding system. • Md5: This is the MD5 hash of the file result (where applicable). • Sha256: This is the SHA256 hash of the file result (where applicable). • Owner: This is the owner of the file. • SuspectedFileType: This is the suspected file type of the file object (where applicable). • FileSignature: This is a set of information derived about the file's signature status. • Size: This is the size of the file object (in bytes). • OwnerUid: This is the unique ID of the owner of the file.
Process	• Name: This is the name of the process. • CommandLine: This is the command line arguments that the process was executed with. • StartDateTime: This is the timestamp (in UTC) of when the process was executed on the responding system. • PrimaryImagePath: This is the image file path of the process. • PrimaryImageMd5: This is the MD5 hash of the image file of the process. • PrimaryImageSha256: This is the SHA256 hash of the image file of the process. • PrimaryImageUid: This is the unique ID of the image file of the process. • Owner: This is the user who owns the process. • OwnerUid: This is the unique ID of the user who owns the process. • SuspectedFileType: This is the suspected file type of the image file of the process. • FileSignature: This is a set of information derived about the image file's siganture status. • IsBeingDebugged: This is a Boolean value to determine if the process has a debugger attached to it.
Network	• DestinationAddress: This is the IP address that the connection was destined to. • DestinationPort: This is the port associated with the remote IP address. • ProcessName: This is the process name that was associated with the connection. • ProcessPrimaryImageUid: This is the unique ID of the process associated with the connection. • ProcessPrimaryImagePath: This is the image file path of the process associated with the connection. • ProcessImageMd5: This is the MD5 hash of the image file of the process associated with the connection. • ProcessImageSha256: This is the SHA256 hash of the image file of the process associated with the connection. • SuspectedFileType: This is the suspected file type of the image file of the process associated with the connection.

Field Name	Description
Registry	• IsPersistencePoint: This is a binary value (1 or 0) to determine if the resulting Registry item is a common persistence location. • ValueName: This is the name of the Registry Value that was interacted with. • Path: This is the full path of the Registry Key. • FilePath: This is the full path of the file referenced in the Registry Value (where applicable). • FileMd5: This is the MD5 hash of the file referenced in the Registry Value (where applicable). • FileSha256: This is the SHA256 hash of the file referenced in the Registry Value (where applicable). • FileUid: This is the unique ID of the file referenced in the Registry Value (where applicable). • SuspectedFileType: This is the suspected file type of the file referenced in the Registry Value (where applicable). • FileSignature: This is a set of information derived about a file's signature status that is referenced in the Registry Value (where applicable).

Archive InstaQuery

Archive a CylanceOPTICS InstaQuery resource belonging to a tenant. Surveys are archived instead of deleted so that user activity history can be maintained.

Service endpoint	/instaqueries/v2{queryID}/archive
Optional query string parameters	—
Example	https://protectapi.cylance.com/instaqueries/v2/AF593F38EDC1B743BDC0A6FCC53A03CE/archive
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticssurvey:update scope encoded

Request

None

Response

Please see the Response status codes for more information.

CylanceOPTICS policy API

The CylanceOPTICS policy API allows administrators to get a list of all polices and if a detection rule set is assigned to each policy. Administrators can also assign or unassign a detection rule set to a policy.

Get detection rule sets to policy mapping

Get a list of Cylance policies, the unique ID of the detection rule set currently assigned to the policy, and a list of all detection rule sets available to the policy.

Service endpoint	/opticsPolicies/v2/configurations
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsPolicies/v2/configurations
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspolicy:list scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
configuration_id	This is the unique ID for the detection rule set. Matching this number to the DETECTION number gives you the name of the detection rule set assigned to the policy.
DETECTION	This is the unique ID for the detection rule set assigned to the policy.
device_count	This is the number of devices assigned to the policy.
display_name	This is the detection rule set name.
page_number	This is the page number displayed.
page_size	This is the number of items to list per page.

Field Name	Description
policy_id	This is the unique ID for the policy.
total_number_of_items	This is the total number of policies in a tenant.
total_pages	This is the total number of pages, based on the page_size selected.
type	This is the configuration type. For detection rule sets, this is DETECTION.

Get detection rule set for a policy

Get the detection rule set assigned to a policy.

Service Endpoint	/opticsPolicies/v2/configurations/{policy_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsPolicies/v2/configurations/d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea
Method	HTTP/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspolicy:read scope encoded

Request

None

Response

Please see the Response status codes for more information.

Response JSON schema

Field Name	Description
configuration_id	This is the unique ID for the Detection Rule Set. Matching this number to the DETECTION number gives you the name of the Detection Rule Set assigned to the policy.
DETECTION	This is the unique ID for the Detection Rule Set assigned to the policy.
device_count	This is the number of devices assigned to the policy.

Field Name	Description
display_name	This is the Detection Rule Set name.
policy_id	This is the unique ID for the policy.
type	This is the configuration type. For Detection Rule Sets, this is DETECTION.

Update a detection rule set in a policy

Update the detection rule set assigned to a policy.

Service endpoint	/opticsPolicies/v2/configurations
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsPolicies/v2/configurations
Method	HTTP/1.1 POST
Request headers	• Accept: application/json • Authorization: Bearer *JWT Token returned by Auth API* with the opticspolicy:create scope encoded

Request

```
{
    "configuration_type": "DETECTION",
    "configuration_id": "d23198bd-2725-4660-969c-971f1548ffc3",
    "link": [d5c6d6a3-0599-4fb5-96bc-0fdc7eacb6ea],
    "unlink": []
}
```

Response

Please see the Response status codes for more information.

Request JSON schema

Field Name	Description
configuration_id	This is the detection rule set unique identifier (ID). Use get all detection rule sets or get single detection rule set requests to get this ID.
configuration_type	This is the configuration type. For detection rule sets, this is DETECTION.

Field Name	Description
link	This adds the policy ID to assign the detection rule set to the policy.
unlink	This adds the policy ID to remove the detection rule set from the policy.

Response JSON schema

Field Name	Description
id	This is the policy ID.
message	This displays the assignment of the detection rule set to the policy. • link: This is the detection rule set is assigned to the policy. • unlink: This is the detection rule set was removed from the policy.
success	This displays if the update was successful or not. • false: The process of updating the detection rule set in the policy failed. • true: The process of updating the detection rule set in the policy succeeded.

Lockdown configurations API

The CylanceOPTICS lockdown configurations API allows users to perform actions by partially locking an infected device. The CylanceOPTICS lockdown configurations API includes:

- Getting a list of custom partial lockdown profiles
- Creating a custom partial lockdown profile
- Updating a custom partial lockdown profile
- Deleting a custom partial lockdown profile

For more information about custom lockdown profiles, see Lock a device in the Cylance Endpoint Security Administration content.

Get lockdown configurations

Request custom partial lockdown profiles.

Service endpoint	/opticsLockdownConfigurations/
Optional query string parameters	count: This is a boolean to include the count of devices currently locked with this configuration
Example	https://protectapi.cylance.com/opticsLockdownConfigurations/v2
Method	Http/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer JWT Token

Response

Please see the Response status codes for more information.

Response JSON schema

```
{
   "lockdown_config_id":123,
   "name":"Test Config",
   "description":"Optional Description",
   "date_added":"DateTime",
   "date_modified":"DateTime",
   "default_config":0,
   "count":(optional)
}
```

Get lockdown configuration

Request a custom partial lockdown profile.

Service endpoint	/opticsLockdownConfigurations/v2/{lockdown_config_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsLockdownConfigurations/v2/123
Method	Http/1.1 GET
Request headers	• Accept: application/json • Authorization: Bearer JWT Token

Response

Please see the Response status codes for more information.

Response JSON schema

```
{
   "lockdown_config_id":123,
   "name":"Test Config",
   "description":"Optional Description",
   "parameters":{
      "WhitelistedAddresses":[
         {
            "ip_address":"192.168.0.10",
            "direction":1
         }
      ],
      "WhitelistedPorts":[
         {
            "port":"22",
            "direction":1
         }
      ]
   }
}
```

Create lockdown configuration

Create a custom partial lockdown profile.

Service endpoint	/opticsLockdownConfigurations/v2
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsLockdownConfigurations/v2
Method	Http/1.1 POST

Request headers	• Accept: application/json • Authorization: Bearer JWT Token

Request

```
{
   "name":"Test Config",
   "description":"Optional Description",
   "parameters":{
      "WhitelistedAddresses":[
         {
            "ip_address":"192.168.0.10",
            "direction":1
         }
      ],
      "WhitelistedPorts":[
         {
            "port":"22",
            "direction":1
         }
      ]
   }
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

There is no response JSON schema.

Update lockdown configuration

Update a custom partial lockdown profile.

Service endpoint	/opticsLockdownConfigurations/v2/{lockdown_config_id}
Optional query string parameters	—
Example	https://protectapi.cylance.com/opticsLockdownConfigurations/v2/123
Method	Http/1.1 PUT
Request headers	• Accept: application/json • Authorization: Bearer JWT Token

Request

```
{
   "name":"Test Config",
   "description":"Optional Description",
   "parameters":{
      "WhitelistedAddresses":[
         {
            "ip_address":"192.168.0.10",
            "direction":1
         }
      ],
      "WhitelistedPorts":[
         {
            "port":"22",
            "direction":1
         },
         {
            "port":"3268",
            "direction":2
         }
      ]
   }
}
```

Response

Please see the Response status codes for more information.

Response JSON schema

There is no response JSON schema.

Delete lockdown configuration

Delete a custom partial lockdown profile.

Service endpoint	/opticsLockdownConfigurations/v2/{lockdown_config_id}
Optional query string parameters	-
Example	https://protectapi.cylance.com/opticsLockdownConfigurations/v2/123
Method	Http/1.1 DELETE
Request headers	• Accept: application/json • Authorization: Bearer JWT Token

Response

Please see the Response status codes for more information.

Response JSON schema

There is no response JSON schema.

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