CYLANCE

CylancePROTECT®

USER API GUIDE

Product: CylancePROTECT

Document: CylancePROTECT Console API Guide. This guide is a succinct resource for analysts, Administrators, and customers who are reviewing or evaluating the product.

Document Release Date: v2.0 rev9, March 2018

About Cylance®: Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs. Visit cylance.com.

Global Headquarters	18201 Von Karman Ave, Suite 700 Irvine, CA 92612
Professional Services Hotline	+1-877-97DEFEND +1-877-973-3336
Corporate Contact	+1-914-CYLANCE +1-914-295-2623
Email	sales@cylance.com
Website	https://www.cylance.com
To Open a Support Ticket	https://support.cylance.com Click on Submit a Ticket
To View Knowledge Base and Announcements	Login to https://support.cylance.com
To Request a Callback from Cylance Support	1-866-699-9689

Table of Contents

Overview

Cylance's award winning next-generation anti-malware product, CylancePROTECT, offers APIs as an alternative way of interacting with the system.

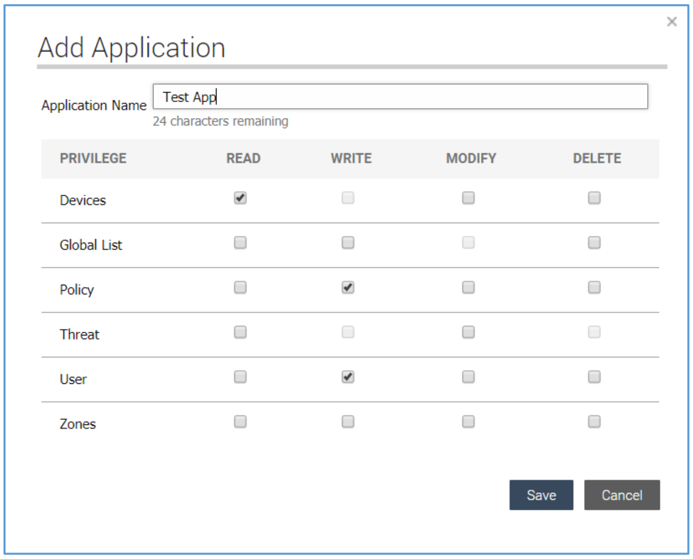
The latest version of Cylance's API allows you to create multiple applications to control access to your Cylance Console data. You can provide Read, Write, Modify, and Delete privileges to each of the API calls. Each API application has unique credentials (ID and Secret) that are used to create a token.

Application Management

CylancePROTECT Administrators can manage multiple API applications, including the access privileges to your CylancePROTECT Console data.

To Add an Application:

1. Log in to the CylancePROTECT Console (https://login.cylance.com/Login) as an Administrator. Only Administrators can create an application integration.
2. Select **Settings > Integrations**.
3. Click **Add Application**.
4. Type an Application Name. This must be unique within your organization.
5. Select the access privilege for a Console data type. Not selecting any checkboxes for a data type means the application does not have access to that data type.



Add Application

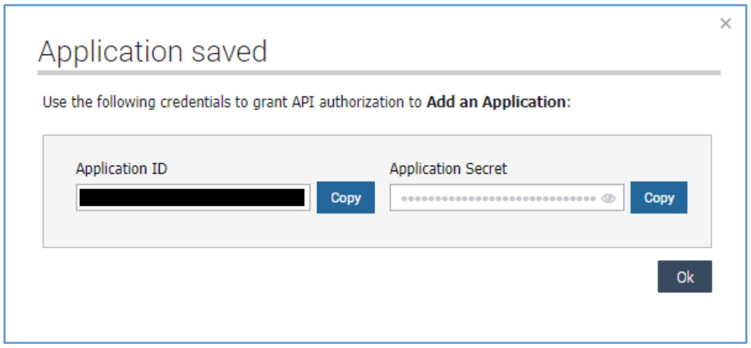
Application Name: Test App

24 characters remaining

PRIVILEGE	READ	WRITE	MODIFY	DELETE
Devices	☑	□	□	□
Global List	□	□	□	□
Policy	□	☑	□	□
Threat	□	□	□	□
User	□	☑	□	□
Zones	□	□	□	□

6. Click **Save**. The credentials to use for the application displays.
7. Copy and paste the Application ID and Application Secret to your API application. Or you can click **OK, got it** 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.



Application saved

Use the following credentials to grant API authorization to **Add an Application**:

Application ID: [redacted]

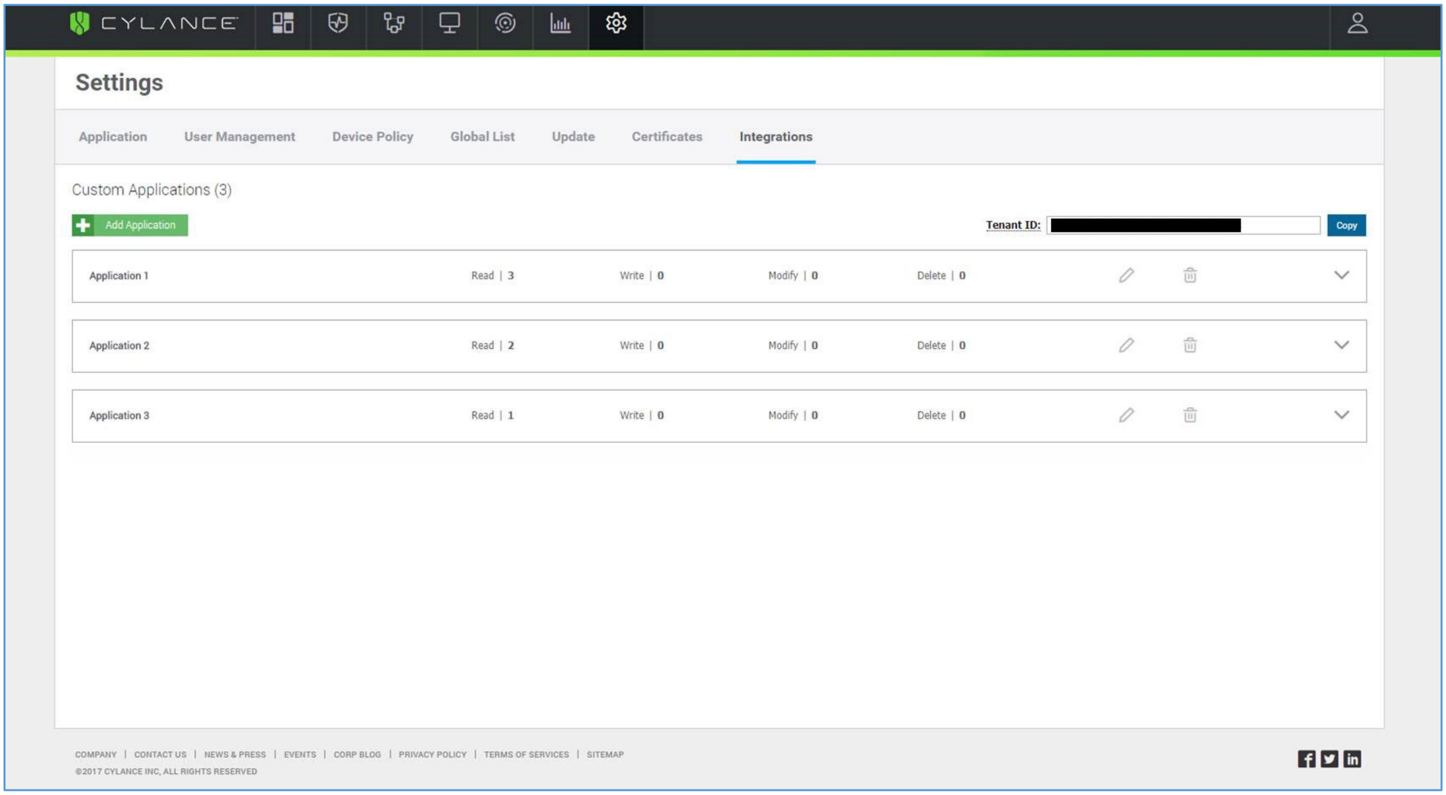
Application Secret: ••••••••••••••••••••••••••••••

Data Type	Description
Devices	Devices are systems with a CylancePROTECT Agent installed. You can get information about devices in your organization. You can also add (Write) or remove (Delete) devices from your organization.
Global List	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.
Policy	Policies contain the protection settings applied to a device. Policies allow adding and removing devices instead of needing to manually update each device when you want to change the protection settings.
Threat	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.
User	Users have access to the data in the Console, based on the role assigned to the User. For example, an Administrator can see everything in the Console, while a User is limited to the zones to which the User is assigned.
Zone	Each device belongs to at least one Zone. Zones are similar to tags and assist in organizing your devices.

Privilege	Description
Read	Ability to read data but cannot create, modify, or delete the data.
Write	Ability to add data to the Console.
Modify	Ability to modify existing data.
Delete	Ability to delete the data.

To Edit an Application:

1. Log in to the CylancePROTECT Console (https://login.cylance.com/Login) as an Administrator. Only Administrators can create an application integration.
2. Select **Settings > Integrations**.
3. Click the edit icon for the application you want to change.
4. Edit the privileges, then click **Save Changes**.



Settings

Application | User Management | Device Policy | Global List | Update | Certificates | Integrations

Custom Applications (3)

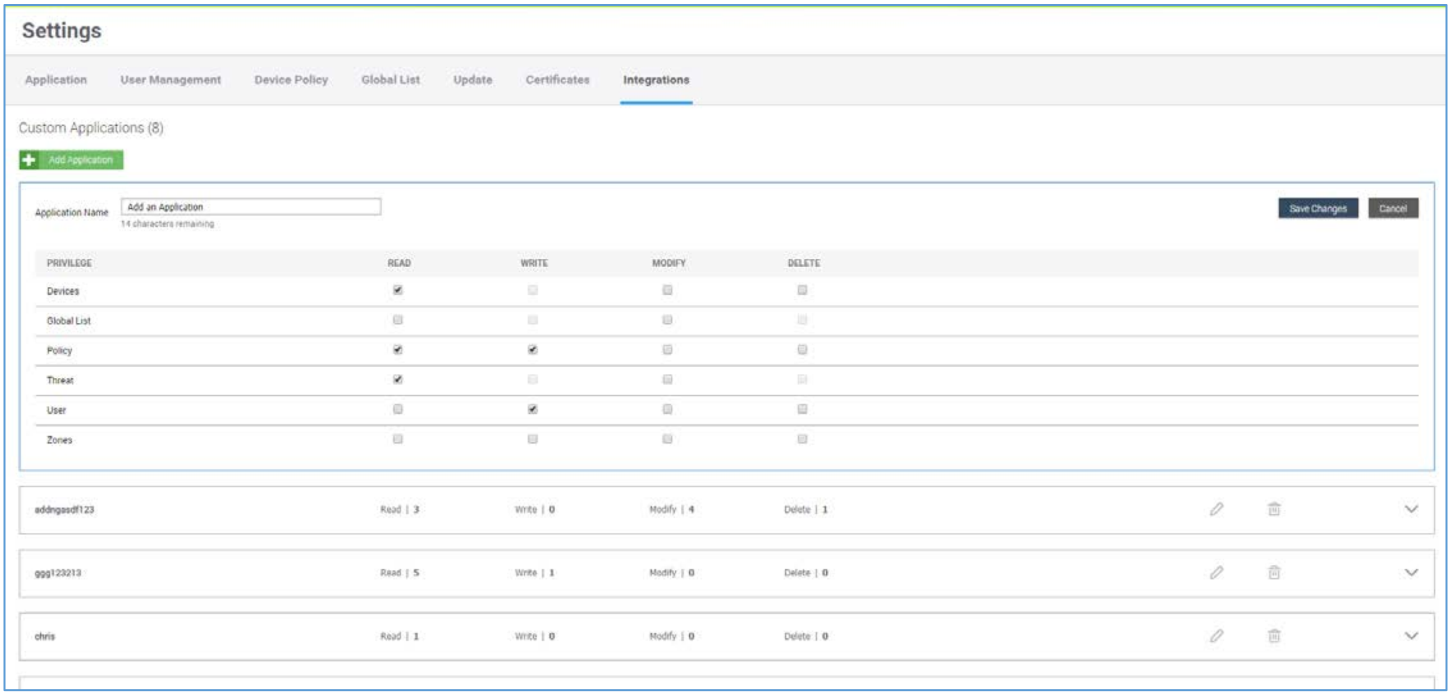
Add Application

Tenant ID: [redacted] Copy

Application 1	Read | 3	Write | 0	Modify | 0	Delete | 0
Application 2	Read | 2	Write | 0	Modify | 0	Delete | 0
Application 3	Read | 1	Write | 0	Modify | 0	Delete | 0

COMPANY | CONTACT US | NEWS & PRESS | EVENTS | CORP BLOG | PRIVACY POLICY | TERMS OF SERVICES | SITEMAP

©2017 CYLANCE INC, ALL RIGHTS RESERVED



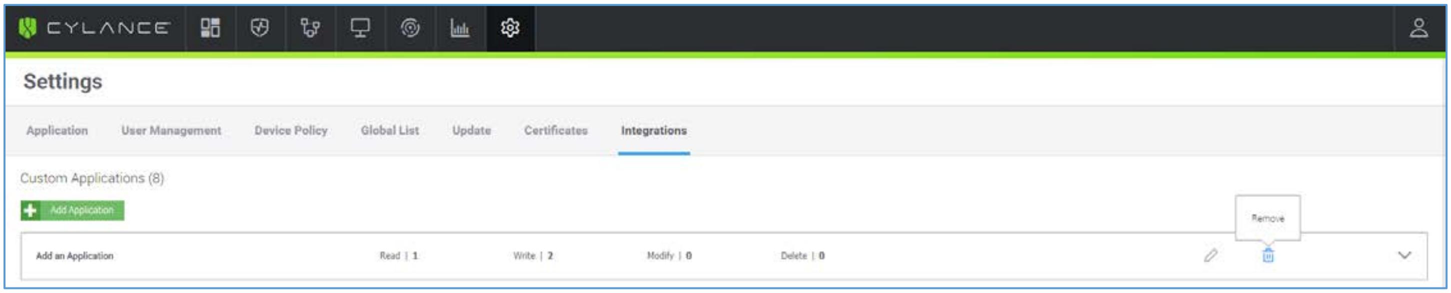
Application Name: Add an Application
14 characters remaining

PRIVILEGE	READ	WRITE	MODIFY	DELETE
Devices	☑	□	□	□
Global List	□	□	□	□
Policy	☑	☑	□	□
Threat	☑	□	□	□
User	□	☑	□	□
Zones	□	□	□	□

addngasdf123	Read | 3	Write | 0	Modify | 4	Delete | 1
ggg123213	Read | 5	Write | 1	Modify | 0	Delete | 0
chris	Read | 1	Write | 0	Modify | 0	Delete | 0

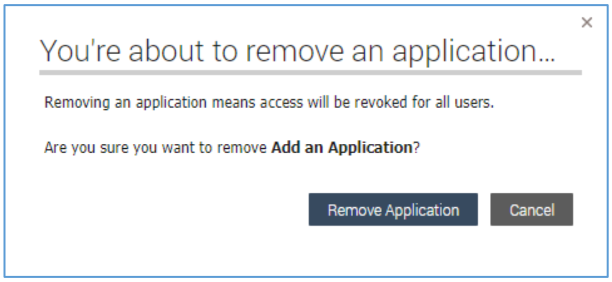
To Delete an Application:

1. Log in to the CylancePROTECT Console (https://login.cylance.com/Login) as an Administrator. Only Administrators can create an application integration.
2. Select **Settings > Integrations**.
3. Click the Remove icon for the application you want to remove.



Add an Application	Read | 1	Write | 2	Modify | 0	Delete | 0

4. Click **Remove Application** to confirm the deletion.



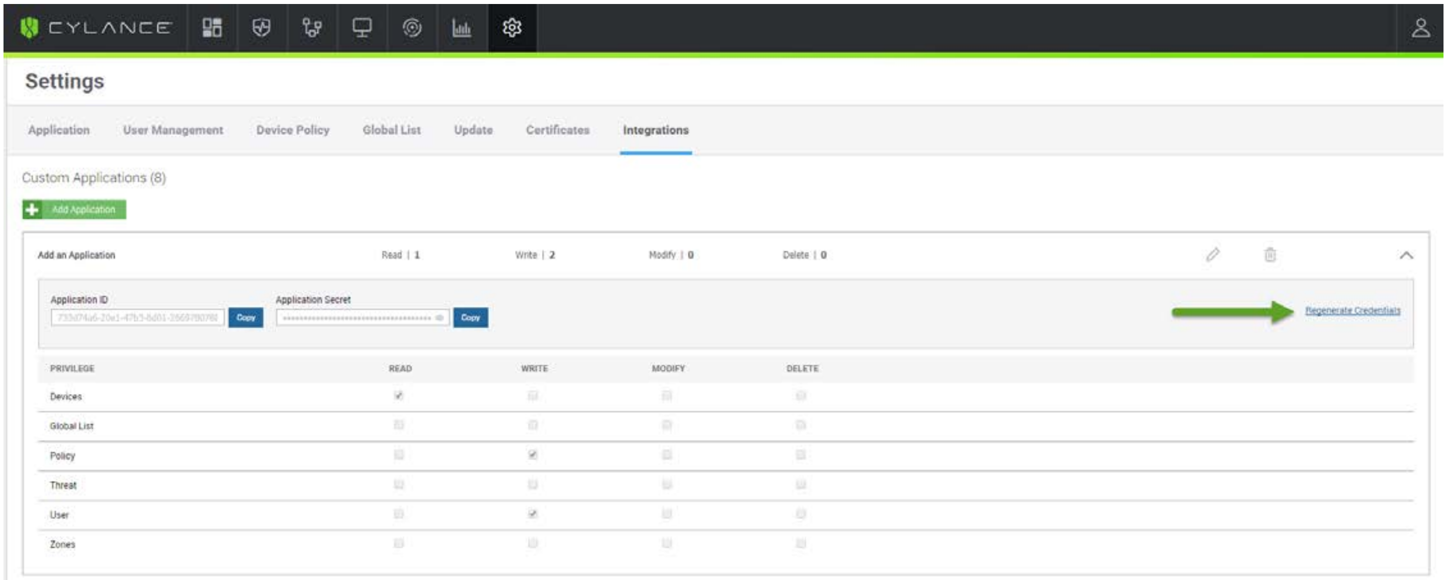
You're about to remove an application...

Removing an application means access will be revoked for all users.

Are you sure you want to remove **Add an Application**?

To Regenerate an Application Credential:

1. Log in to the CylancePROTECT Console (https://login.cylance.com/Login) as an Administrator. Only Administrators can regenerate an application credential.
2. Select **Settings > Integrations**.
3. Click the down arrow to expand the information for the application for which you want to regenerate credentials.



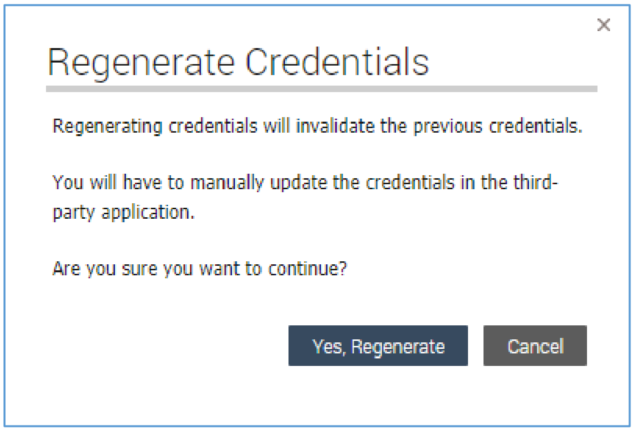
Add an Application — Read | 1 — Write | 2 — Modify | 0 — Delete | 0

Application ID: 733d74a6-20e1-47b5-8d01-256978078l

Application Secret: ••••••••••••••••••••••••••••••••

PRIVILEGE	READ	WRITE	MODIFY	DELETE
Devices	☑	□	□	□
Global List	□	□	□	□
Policy	□	☑	□	□
Threat	□	□	□	□
User	□	☑	□	□
Zones	□	□	□	□

4. Click **Regenerate Credentials**. A confirmation message appears.
5. Click **Yes, Regenerate** to confirm regenerating the credentials.



Regenerate Credentials

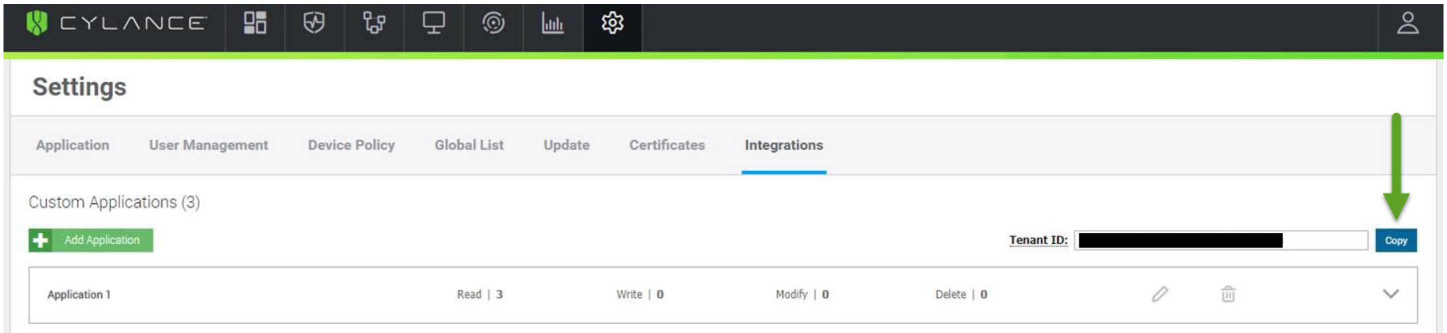
Regenerating credentials will invalidate the previous credentials.

You will have to manually update the credentials in the third-party application.

Are you sure you want to continue?

Copy Tenant ID

The Tenant ID is required for authorization. You can copy your Tenant ID from the Integrations page.



Custom Applications (3)

Tenant ID: [redacted]

Application 1 Read | 3 Write | 0 Modify | 0 Delete | 0

RESTful API

Cylance provides RESTful APIs for registered organizations to manage their resources. To access the CylancePROTECT 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.

Note: Cylance supports CylancePROTECT API resources, including helping Users troubleshoot Cylance API requests. Cylance does not write or train Users on how to create scripts or code (like using Python).

Authentication and Authorization

Application

An Application acts as an integration point between the client system and CylancePROTECT Web 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, as defined in the Application Management section.

Service Endpoint

The Auth API will be accessed via the following base endpoint:

https://protectapi-{region-code}.cylance.com/auth/v2

Authentication

During the step which a client system requests access prior to using CylancePROTECT 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. Cylance 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 flow:

- **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 CylancePROTECT 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. All 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 milliseconds. Note: 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. This is Unix epoch time in milliseconds.
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. In our case, this would hold our Application ID.
		Custom Claims
scp	*String*	Comma delimited scopes requested. This claim is **Optional**.
tid	*String*	Tenant ID (available on the Integrations page in the Console).

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");
         o  token.claims.Add("scp", "policy:create, policy:list, policy:read,
            policy:update")
```

Generating 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.

Software Requirements:

- Python 2.7 (latest version is recommended)
- PyJWT package (pip install PyJWT)
- Requests package (pip install requests)

Examples using C# are available upon request.

Python Example:

```
import jwt  # PyJWT version 1.5.3 as of the time of authoring.
import uuid
import requests  # requests version 2.18.4 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/Response Model

Service Endpoint	https://protectapi-{region-code}.cylance.com/auth/v2/token
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	Authentication Request Schema
	{
	"title":"Authentication Request",
	"type":"object",
	"properties": {
	"auth_token":{
	"type":"string",
	"description":"Token representing authentication request"
	}
	},
	"required":["auth_token"]
	}

Response

Authentication Response Schema

```
{
  "title":"Authentication Response",
  "type":"object",
  "properties": {
    "access_token":{
      "type":"string",
      "description":"Access token granted by the Server"
    }
  },
  "required":["access_token"]
}
```

401 Unauthorized – Returned for the following reasons:

- The authentication token provided failed to authorize.
- The application ID supplied in the “sub” claim could not be found in the system.

403 Forbidden – The authentication token provided is requesting invalid or unavailable scopes.

500 InternalServerError – An unforeseeable error has occurred.

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 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 CylancePROTECT Resources. It contains information about the identity of the caller (Application) as well as control information for 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 CylancePROTECT 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.

Response Status Codes

Each API request will receive a response with a JSON payload and a standard HTTP status code.

Note: Some API request sections include additional response status descriptions (specific to that request) to help you troubleshoot issues.

Status Code	Description
200 – OK	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 cause 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	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.
500 – Internal Server Error	A catch-all code response for any unhandled error that has occurred on the server. Contact Cylance 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 Cylance Support if you encounter any status codes that are not on this list.

Region Codes

The service endpoint address includes a region code, to identify the set of servers to which your organization belongs. **Example**: http://protectapi-euc1.cylance.com/devices/v2

Region Code	Description	Notes
Asia-Pacific – North	apne1	
Asia-Pacific – Southeast	au	
Europe – Central	euc1	
Government	us	
North America		No code required.
South America	sae1	

User API

Create User

Create (add) a new Console User. This requires a unique email address for the User being created.

Service Endpoint	https://protectapi-{region-code}.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 scope encoded.

Request	Post User Request Schema
	{
	  "email": "string",
	  "user_role": "string",
	  "first_name": "string",
	  "last_name": "string",
	  "zones": [
	   {
	    "id": "string",
	    "role_type": "string"
	   }
	  ]
	}

Response

201 Created

Post User Response Schema

```
{
  "id": "string",
  "tenant_id": "string",
  "first_name": "string",
  "last_name": "string",
  "email": "string",
  "has_logged_in": true,
  "role_type": "string",
  "role_name": "string",
  "default_zone_role_type": "string",
  "default_zone_role_name": "string",
  "zones": [
   {
    "id": "string",
    "role_type": "string",
    "role_name": "string"
   }
  ],
  "date_last_login": "2017-09-13T22:33:26.098Z",
  "date_email_confirmed": "2017-09-13T22:33:26.098Z",
  "date_created": "2017-09-13T22:33:26.098Z",
  "date_modified": "2017-09-13T22:33:26.098Z"
}
```

400 BadRequest – Returned for the following reasons:

- The User create request was empty.
- The Tenant ID cannot be retrieved from the JWT token.
- The User’s email address specified is not a proper email address.
- The User application role specified is not one of the accepted values.
- The zones array is empty when the User application role is not Administrator.
- The email provided is already in use.

401 Unauthorized – The JWT token is not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

	500 InternalServerError – An unforeseeable error has occurred.

The request JSON schema contains the following fields:

Field Name	Description
email	The User's email address. This must be unique.
first_name	The User's first name. Maximum of 64 characters.
last_name	The User's last name. Maximum of 64 characters.
user_role	The User's role in your Console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Zone Manager: 00000000-0000-0000-0000-000000000003
zones	The zones to which the User has access. This is an array of elements. • id: The unique identifier for the zone. • role_type: The User's role for this particular zone. o Zone Manager: 00000000-0000-0000-0000-000000000001 o User: 00000000-0000-0000-0000-000000000002 • role_name: The name of the User's role in this zone. Note: If the User is an Administrator, this array is not required and the elements specified will be ignored.

The response JSON schema contains the following fields:

Field Name	Description
date_created	The date and time (in UTC) the Console User was created.
date_email_confirmed	The date and time (in UTC) when the User confirmed the email provided.
date_last_login	The date and time (in UTC) the User last logged in to the Console.
date_modified	The date and time (in UTC) the Console User information was last updated.

default_zone_role_type	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
default_zone_role_name	The name of the role for the User in the zone.
email	The User's email address.
first_name	The User's first name.
has_logged_in	True if the User has successfully logged in to the Console.
id	The User's unique identifier for the Console.
last_name	The User's last name.
tenant_id	The organization's unique identifier for the Console.
role_type	The unique identifier defining the User's role in the Console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Zone Manager: 00000000-0000-0000-0000-000000000003
role_name	The name of the User's role in the Console.
zones	The zones to which the User has access. This is an array of elements. • id: The unique identifier for the zone. • role_type: The User's role for this particular zone. o None: 00000000-0000-0000-0000-000000000000 o Zone Manager: 00000000-0000-0000-0000-000000000001 o User: 00000000-0000-0000-0000-000000000002 • role_name: The name of the User's role in this zone. Note: If the User is an Administrator, this array is not required and the elements specified will be ignored.

Get Users

Allows a caller to 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	https://protectapi-{region-code}.cylance.com/users/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 user:list scope encoded.
Request	Append the following optional query string parameters: • page: The page number to request. • page_size: The number of device records to retrieve per page.

Response	200 OK
	Get Users Response Schema
	{
	 "page_number": 0,
	 "page_size": 0,
	 "total_pages": 0,
	 "total_number_of_items": 0,
	 "page_items": [
	  {
	   "id": "string",
	   "tenant_id": "string",
	   "first_name": "string",
	   "last_name": "string",
	   "email": "string",
	   "has_logged_in": true,
	   "role_type": "string",
	   "role_name": "string",
	   "default_zone_role_type": "string",
	   "default_zone_role_name": "string",
	   "zones": [

```
        {
          "id": "string",
          "role_type": "string",
          "role_name": "string"
        }
      ],
      "date_last_login": "2017-09-26T05:21:01.943Z",
      "date_email_confirmed": "2017-09-26T05:21:01.943Z",
      "date_created": "2017-09-26T05:21:01.943Z",
      "date_modified": "2017-09-26T05:21:01.943Z"
    }
  ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID cannot be retrieved from the JWT token.
- The page number or page size specified is less than or equal to zero, or the page size is greater than 200.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
date_created	The date and time (in UTC) the Console User was created.
date_email_confirmed	The date and time (in UTC) when the User confirmed the email provided.
date_last_login	The date and time (in UTC) the User last logged in to the Console.
date_modified	The date and time (in UTC) the Console User information was last updated.
default_zone_role	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	The User's email address.
first_name	The User's first name.
has_logged_in	True if the User has successfully logged in to the Console.
last_name	The User's last name.
page_number	The page number requested.
page_size	The page size requested.
tenant_id	The organization's unique identifier for the Console.
total_pages	The total number of pages that can be retrieved, based on the page size specified.
user_id	The User's unique identifier for the Console.
user_role	The unique identifier defining the User's role in the Console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Zone Manager: 00000000-0000-0000-0000-000000000003
zones	The zones to which the User has access. This is an array of elements. • id: The unique identifier for the zone. • role_type: The User's role for this particular zone. o None: 00000000-0000-0000-0000-000000000000 o Zone Manager: 00000000-0000-0000-0000-000000000001 o User: 00000000-0000-0000-0000-000000000002 • role_name: The name of the User's role in this zone. Note: If the User is an Administrator, this array is not required and the elements specified will be ignored.

Get User

Allows a caller to request a specific Console User resource belonging to a Tenant.

Service Endpoint	https://protectapi-{region-code}.cylance.com/users/v2/{user_id | user_email_address}
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	200 OK

Get User Response Schema

```
{
  "user_id": "string",
  "tenant_id": "string",
  "first_name": "string",
  "last_name": "string",
  "email": "string",
  "has_logged_in": true,
  "user_role": "string",
  "default_zone_role": "string",
  "zones": [
   {
    "id": "string",
    "role_type": "string",
    "role_name: "string"
   }
  ],
  "date_last_login": "2017-05-22T23:35:56.705Z",
  "date_email_confirmed": "2017-05-22T23:35:56.705Z",
  "date_created": "2017-05-22T23:35:56.705Z",
  "date_modified": "2017-05-22T23:35:56.705Z"
 }
```

	400 BadRequest – Returned for the following reasons: • The Tenant ID cannot be retrieved from the JWT token. • The User's unique identifier is not valid (when using a unique User ID). • The User's email address specified is not a proper email address (when using User's email address). 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The User resource cannot be found by the unique User ID or email address specified in the URL. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
date_created	The date and time (in UTC) the Console User was created.
date_email_confirmed	The date and time (in UTC) when the User confirmed the email provided.
date_last_login	The date and time (in UTC) the User last logged in to the Console.
date_modified	The date and time (in UTC) the Console User information was last updated.
default_zone_role	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	The User's email address.
first_name	The User's first name.
has_logged_in	True if the User has successfully logged in to the Console.
last_name	The User's last name.
tenant_id	The organization's unique identifier for the Console.

user_id	The User’s unique identifier for the Console.
user_role	The unique identifier defining the User’s role in the Console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002 • Zone Manager: 00000000-0000-0000-0000-000000000003
zones	The zones to which the User has access. This is an array of elements. • id: The unique identifier for the zone. • role_type: The User’s role for this particular zone. o None: 00000000-0000-0000-0000-000000000000 o Zone Manager: 00000000-0000-0000-0000-000000000001 o User: 00000000-0000-0000-0000-000000000002 • role_name: The name of the User’s role in this zone. Note: If the User is an Administrator, this array is not required and the elements specified will be ignored.

Update User

Allows a caller to update an existing Console User resource.

Service Endpoint	https://protectapi-{region-code}.cylance.com/users/v2/{user_id}
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	Put User Request Schema
	{
	  "email": "string",
	  "user_role": "string",
	  "first_name": "string",
	  "last_name": "string",

```
  "zones": [
   {
    "id": "string",
    "role_type": "string"
   }
  ]
}
```

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID cannot be retrieved from the JWT token. • The User ID is invalid or not specified. • The User's email address specified is not a proper email address. • The User application role specified is not one of the accepted values. • The zones array is empty when the User application role is not Administrator. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The User ID does not exist. 500 Server Error – The server encountered something it did not expect and was unable to complete the request.

The request JSON schema contains the following fields:

Field Name	Description
email	The User's email address.
first_name	The User's first name.
last_name	The User's last name.
user_role	The unique identifier defining the User's role in the Console. • User: 00000000-0000-0000-0000-000000000001 • Administrator: 00000000-0000-0000-0000-000000000002

	• Zone Manager: 00000000-0000-0000-0000-000000000003
zones	The zones to which the User has access. This is an array of elements. • id: The unique identifier for the zone. • role_type: The User's role for this particular zone. o None: 00000000-0000-0000-0000-000000000000 o Zone Manager: 00000000-0000-0000-0000-000000000001 o User: 00000000-0000-0000-0000-000000000002

Delete User

Allows a caller to delete an existing Console User resource.

Service Endpoint	https://protectapi-{region-code}.cylance.com/users/v2/{user_id}
Method	HTTP/1.1 DELETE
Request Headers	Authorization: Bearer <JWT Token returned by Auth API> with the user:delete scope encoded.
Request	None
Response	200 OK - The User was deleted successfully. 400 BadRequest – Returned for the following reasons: • The Tenant ID cannot be retrieved from the JWT token. • The User ID is invalid or not specified. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound– The User specified by unique User ID was not found. 500 InternalServerError – An unforeseeable error has occurred.

Send Invite Email

Allows a caller to request for the Console login invitation email to be sent or resent to an existing User.

Service Endpoint	https://protectapi-{region-code}.cylance.com/users/v2/{user_email_address}/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	200 OK– The email was successfully sent. 400 BadRequest – Returned for the following reasons: • The Tenant ID cannot be retrieved from the JWT token. • The unique ID of the User triggering the invitation email to be sent cannot be retrieved from the JWT token. • The User's email address specified is not a proper email address. • The User to whom the invite email is to be sent has already logged in to the Console. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound– The User resource to send or resend the invitation email to is not found.

Send Reset Password Email

Allows a caller to request for the Console reset password email to be sent or resent to an existing User.

Service Endpoint	https://protectapi-{region-code}.cylance.com/users/v2/{user_email_address}/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	200 OK – The email was successfully sent. 400 BadRequest – Returned for the following reasons: • The Tenant ID cannot be retrieved from the JWT token. • The User's email address specified is not a proper email address. • The User to whom the reset password email is to be sent has not confirmed the email provided. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound– The User resource to send or resend the invitation email to is not found. 500 InternalServerError – An unforeseeable error has occurred.

Device API

Get Devices

Allows a caller to request a page with a list of Console device resources 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 10 respectively.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/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 device:list scope encoded.
Request	Append the following optional query string parameters: • page: The page number to request. • page_size: The page number of device records to retrieve per page.

Response	200 OK
	Get Devices Response Schema
	{
	"page_number": 0,
	"page_size": 0,
	"total_pages": 0,
	"total_number_of_items": 0,
	"page_items": [
	{
	"id": "string",
	"name”: “string",
	"state": “string",
	"agent_version": "string",
	"policy": {
	“id": "string",
	“name": "string"
	},
	"date_first_registered": "2017-07-28T16:35:46.081Z",
	“ip_addresses”: [

```
      “string1”,
      “string2” ],
    “mac_addresses”: [
      “string1”,
      “string2” ]
  }
 ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The page number or page size specified is less than or equal to zero.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 NotFound – The device resources page requested doesn’t exist.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
agent_version	The CylancePROTECT Agent version installed on the device.
date_first_registered	The date and time (in UTC) when the device record was created.
id	The device’s unique identifier.
ip_addresses	The list of IP addresses for the device.
mac_addresses	The list of MAC addresses for the device.
name	The device’s name.
page_number	The page number requested.
page_size	The page size requested.
policy	The policy ID and name.

state	Signals whether the device is online or offline.
total_number_of_items	Total number of resources.
total_pages	The total number of pages that can be retrieved, based on the page size specified.

Get Device

Allows a caller to request a specific device resource belonging to a Tenant.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/v2/{unique_device_id}
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	200 OK
	Get Device Response Schema
	{
	  "id": "string",
	  "name": "string",
	  "host_name": "string",
	  "os_version": "string",
	  "state": "string",
	  "agent_version": "string",
	  "policy": {
	    “id": "string",
	    “name": "string"
	  },
	  "last_logged_in_user": "string",
	  "update_type": "string",
	  "update_available": true,
	  "background_detection": true,
	  "is_safe": true,
	  "date_first_registered": "2017-06-15T18:02:45.714Z",

```
    "date_offline": "2017-06-15T18:02:45.714Z",
    "date_last_modified": "2017-06-15T18:02:45.714Z",
     “ip_addresses”: [
       “string1”,
       “string2” ],
     “mac_addresses”: [
       “string1”,
       “string2” ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The device’s unique identifier is not valid.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 NotFound – The device resources page requested doesn’t exist.

500 InternalServerError – An unforeseeable error has occurred.

Field Name	Description
agent_version	The CylancePROTECT Agent version installed on the device.
background_detection	If true, the Agent is currently running.
date_first_registered	The date and time (in UTC) when the device record was created.
date_last_modified	The date and time (in UTC) when the device record was last modified.
date_offline	The date and time (in UTC) when the device last communicated with the Console.
host_name	The hostname for the device.
id	The unique identifier for the device.
ip_addresses	The list of IP addresses for the device.
is_safe	If true, there are no outstanding threats.
last_logged_in_user	The ID of the User who logged in last on to the device.

mac_addresses	The list of MAC addresses for the device.
name	The name of the device.
os_version	The operating system and version.
policy	The name of the policy assigned to the device.
state	The device is online or offline.
update_available	If true, an Agent update is available for the device based on the update type (Phase).
update_type	The update phase the device is scheduled on.

Update Device

Allows a caller to update a specific Console device resource belonging to a Tenant.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/v2/{unique device id}
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	Put Device Response Schema
	{
	"name”: “string",
	"policy_id": "string",
	"add_zone_ids": [
	“string"
	],
	“remove_zone_ids": [
	“string"
	]
	}

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT. • The device's unique identifier is not valid. • The device update data failed validation. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – Returned if the device resource to update doesn't exist. 500 InternalServerError – An unforeseeable error has occurred.

The request JSON schema contains the following fields:

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

Get Device Threats

Allows a caller to 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	https://protectapi-{region-code}.cylance.com/devices/v2/{unique device id}/threats?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 device:threatlist scope encoded.

Request

Append the following optional query string parameters:

- page: The page number to request.
- page_size: The page number of device records to retrieve per page.

Response

200 OK

Get Device Threat Response Schema

```
{
   "page_number": 0,
   "page_size": 0,
   "total_pages": 0,
   "total_number_of_items": 0,
   "page_items": [
     {
       "name": "string",
       "sha256”: “string",
       "file_status": 0,
       "file_path": "string",
       "cylance_score": 0,
       "classification": "string",
       "sub_classification": "string",
       "date_found": "2017-06-15T18:02:45.714Z"
     }
   ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The device’s unique identifier is not valid.
- The page number or page size specified is less than or equal to zero, or the page size is greater than 200.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 NotFound – The identifier specified doesn’t belong to a device resource in the system.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
classification	The threat classification assigned by Cylance.
cylance_score	The Cylance score assigned to the threat.
date_found	The date and time (in UTC) when the threat was found on the device.
file_path	The file path where the threat was found on the device.
file_status	The current status of the file on the device. This can be one of the following: • Default (0) • Quarantined (1) • Whitelisted (2) • Suspicious (3) • FileRemoved (4) • Corrupt (5)
name	The name of the threat.
page_number	The page number requested.
page_size	The page size requested.
sha256	The SHA256 hash for the threat.
sub_classification	The threat sub-classification assigned by Cylance.
total_pages	The total number of pages that can be retrieved, based on the page size specified.
total_number_of_items	Total number of resources.

Update Device Threat

Allows a caller to update the status (waive or quarantine) of a convicted threat.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/v2/{unique device id}/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": “string”,
	  "event": “string”
	}

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The device’s unique identifier is not valid. • The page number or page size specified is less than or equal to zero, or the page size is greater than 200. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The identifier specified doesn’t belong to a device resource in the system. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
event	The requested status update for the convicted threat. • Quarantine

	• Waive
threat_id	The SHA256 hash of the convicted threat.

Get Zone Devices

Allows a caller to 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	https://protectapi-{region-code}.cylance.com/devices/v2/{unique zone id}/devices?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 device:threatlist scope encoded.
Request	Append the following optional query string parameters: • page: The page number to request. • page_size: The page number of device records to retrieve per page.

Response	200 OK
	Get Device Threat Response Schema
	{
	"page_number": 0,
	"page_size": 0,
	"total_pages": 0,
	"total_number_of_items": 0,
	"page_items": [
	{
	"id": "string",
	"name”: “string",
	"policy_id": "string"
	}
	]
	}

	400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The device's unique identifier is not valid. • The page number or page size specified is less than or equal to zero, or the page size is greater than 200. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The zone resource requested is not a valid ID. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
id	The unique identifier for the device.
name	The name of the device.
policy_id	The unique identifier for the policy to which the policy is currently assigned. Can be null.

Get Agent Installer Link

Allows a caller to request a secured link to download the Agent installer.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/v2/installer?product=p&os=o&package=k&architecture=a&build=v
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	Append the following optional query string parameters:
	• product: Specify the Cylance product installer to download. The allowed values are:
	  o Protect
	  o Optics
	• os: Specify the operating system (OS) family. The allowed values are:
	  o CentOS7
	  o Linux
	  o Mac
	  o Ubuntu1404
	  o Ubuntu1604
	  o Windows
	• architecture (required for Windows and macOS): Specify the target architecture. The allowed values are:
	  o X86
	  o X64
	  o CentOS6
	  o CentOS6UI
	  o CentOS7
	  o CentOS7UI
	  o Ubuntu1404
	  o Ubuntu1404UI
	  o Ubuntu1604
	  o Ubuntu1604UI
	• package (required for Windows and macOS): Specify the installer format. The allowed values are:
	  o Exe (Windows only)
	  o Msi (Windows only)
	  o Dmg (macOS only)
	  o Pkg (macOS only)
	• build (optional): Specify the build name for the installer.

Response	200 OK
	Get Agent Installer Link Response Schema
	{
	  "url": "string"
	}

	400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The requested payload failed validation. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The requested link resource does not exist. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
url	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

Allows a caller to delete one or more devices from an organization.

Note: 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	https://protectapi-{region-code}.cylance.com/devices/v2/
Method	HTTP/1.1 DELETE Note: For clients who do not support DELETE, see the not below.
Request Headers	Accept: application/json Authorization: Bearer <JWT Token returned by Auth API> with the device:read scope encoded. Content-Type: application/json

Request

Delete Device Request Schema

```
{
  "device_ids":
  [
    “string"
  ],
  "callback_url”: “string"
}
```

Response

202 Accepted

Delete Device Response Schema

```
{
  "request_id": "string"
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The device IDs are not valid.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 NotFound – The devices do not exist.

413 PayloadTooLarge – The number of resources specified in the request is too large.

500 InternalServerError – An unforeseeable error has occurred.

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

- Service Endpoint: https://protectapi-{region-code}.cylance.com/devices/v2/delete
- Method: HTTP/1.1 POST

The request JSON schema contains the following fields:

Field Name	Description
device_ids	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.
callback_url (*Optional*)	The URL of the callback upon completion.

The response JSON schema contains the following fields:

Field Name	Description
request_id	The unique identifier of the deletion request.

Get Device by MAC Address

Allows a caller to request a specific device resource belonging to a Tenant, by using the MAC address of the device.

Service Endpoint	https://protectapi-{region-code}.cylance.com/devices/v2/macaddress/{mac_address}
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	From URI: • mac_address: The MAC address of the device. Acceptable MAC address formats are: o 00-00-00-00-00-00 o 00:00:00:00:00:00

Response

200 OK

Get Device By MAC Address Response Schema

```
[
  {
    "id": "string",
    "name": "string",
    "host_name": "string",
    "os_version": "string",
    "state": "string",
    "agent_version": "string",
    "policy": {
      "id": "string",
      "name": "string"
    },
    "last_logged_in_user": "string",
    "update_type": "string",
    "update_available": "string",
    "background_detection": "string",
    "is_safe": "string",
    "date_first_registered": "2017-06-15T18:02:45.714Z",
    "date_offline": "2017-06-15T18:02:45.714Z",
    "date_last_modified": "2017-06-15T18:02:45.714Z",
    "ip_addresses": [
      "strings1",
      "string2" ],
    "mac_addresses": [
      "strings1",
      "string2" ]
  }
]
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The MAC address is not valid.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

	403 Forbidden – The JWT token did not contain the proper scope to perform this action. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
agent_version	The CylancePROTECT Agent version installed on the device.
background_detection	The response is True if the CylancePROTECT Agent is running.
date_first_registered	The date and time (in UTC) when the device record was created.
date_last_modified	The date and time (in UTC) when the device record was last modified.
date_offline	The date and time (in UTC) when the device last communicated with the Cylance Console.
host_name	The host name for the device.
id	The unique identifier for the device.
ip_addresses	The list of IP addresses for the device.
is_safe	The response is True if there are not outstanding threats on the device. An outstanding threat is a threat that is not waived, safelisted, or quarantined.
last_logged_in_user	The ID of the User who last logged in to the device.
mac_addresses	The list of MAC addresses for the device.
name	The name for the device.
os_version	The operating system running on the device.
policy	The policy name and policy ID assigned to the device.
state	The current status of the device, which is either online or offline.
update_available	The response is True if there is an Agent update available for the device, according to the update type (phase).
update_type	The update phase on which the device is scheduled.

Global List API

Get Global List

Allows a caller to request a page with a list of global list resources for a Tenant, sorted by the date when the hash was added to the Global List, in descending order (most recent 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. The maximum page size that can be specified is 200 entries per page. The listTypeId parameter is required and can be either 0 (GlobalQuarantine) or 1 (GlobalSafe).

Service Endpoint	https://protectapi-{region-code}.cylance.com/globallists/v2?listTypeId=[0|1]&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 globallist:list scope encoded.
Request	Append the following optional query string parameters: • listTypeId: The type of the list to retrieve the hashes for. • page: The page number to request. • page_size: The number of policy records to retrieve per page.
Response	200 OK Get Threats Response Schema { "page_number": 0, "page_size": 0, "total_pages": 0, "total_number_of_items": 0, "page_items": [{ "name": "string", "sha256": "string", "md5": "string", "cylance_score": 0, "av_industry": 0, "classification": "string", "sub_classification": "string",

```
      "list_type": "string",
      "category": "string",
      "added": "2017-05-22T23:35:56.705Z",
      "added_by": "string",
      "reason": "string"
    }
  ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The page number or page size specified is less than or equal to zero.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 Not Found – The global list page requested doesn't exist.

500 Internal Server Error – Generic server error.

The response JSON schema contains the following fields:

Field Name	Description
added	The timestamp when the file was added to the list.
added_by	The Tenant User ID who added the file to the list.
av_industry	The score provided by the antivirus industry.
category	The category for the list specified (for the Global Safe list only).
classification	The threat classification assigned by Cylance.
cylance_score	The Cylance score assigned to the threat.
list_type	The list type to which the threat belongs (GlobalQuarantine or GlobalSafe).
md5	The MD5 has for the threat.
name	The name of the threat.

page_number	The page number requested.
page_size	The page size requested.
reason	The reason why the file was added to the list.
sha256	The SHA256 hash for the threat.
sub_classification	The threat sub-classification assigned by Cylance.
total_pages	The total number of pages that can be retrieved, based on the page size specified.
total_number_of_items	Total number of resources.

Add To Global List

Allows a caller to add a convicted threat to either the Global Quarantine or the Global Safe list for a particular Tenant.

Service Endpoint	https://protectapi-{region-code}.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. Content-Type: application/json

Request	Post Global List Entry Request Schema
	{
	"sha256": "string",
	"list_type": "string",
	"category": "string",
	"reason": "string"
	}

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The page number or page size specified is less than or equal to zero. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 409 Conflict – The threat specified already exists in the intended list. 500 Internal Server Error – Generic server error.

The response JSON schema contains the following fields:

Field Name	Description
category	This field is required only if the list_type value is Global Safe. The value can be one of the following: • Admin Tool • Commercial Software • Drivers • Internal Application • Operating System • Security Software • None
list_type	The list type to which the threat belongs (GlobalQuarantine or GlobalSafe).
reason	The reason why the file was added to the list.
sha256	The SHA256 hash for the threat.

Delete From Global List

Allows a caller to remove a convicted threat from either the Global Quarantine or the Global Safe list for a particular Tenant.

Service Endpoint	https://protectapi-{region-code}.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. Content-Type: application/json

Request	Post Global List Entry Request Schema
	{
	  "sha256": "string",
	  "list_type": "string"
	}

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The provided SHA256 is invalid. • The provided list type is not supported. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The threat specified does not exist in the intended list. 500 Internal Server Error – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

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

Policy API

Get Policy

Allows the caller to get details for a single policy.

Service Endpoint	https://protectapi-{region-code}.cylance.com/policies/v2/{policy_id}
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	Append the Tenant policy ID to the service endpoint. Requires policy:read scope.
Response	200 OK Get Policy Response Schema

```
{
  "file_exclusions": {
    "checksum": "",
    "error_rate": "0",
    "exclusionlisthash": "",
    "exclusionlisthash_secondary": "",
  },
  "filetype_actions": {
    "suspicious_files": [
      {
        "actions": "string",
        "file_type": "executable",
      }
    ],
    "threat_files": [
      {
        "actions": "string",
        "file_type": "executable",
      }
    ]
  },
  "memoryviolation_actions": {
    "memory_exclusion_list": [],
    "memory_violations": [
      {
        "actions": "string",
        "violation_type": "string",
      }
    ],
    "memory_violations_ext": [
      {
        "actions": "string",
        "violation_type": "string",
      }
    ]
  },
  "policy": [
    {
      "name": "string",
      "value": "string",
    }
    {
      "name": "scan_exception_list",
      "value": [
        ""
      ]
    }
  ],
 "policy_id": "string",
 "policy_name": "string",
 "policy_utctimestamp": "9/15/2017 8:41:15 PM"
}
```

404 Not Found – The Tenant policy ID specified is valid, but no such record exists.

The request JSON schema contains the following fields:

Field Name	Description
file_exclusions	Policy Safe List are file exclusions specific to the policy, and any endpoints assigned to the policy will allow the excluded files to run. • checksum • error_rate • exclusionlisthash • exclusionlisthash_secondary • size
filetype_actions	The Auto-Quarantine of Unsafe (threat_files) and Abnormal (suspicious_files). • actions – Set Auto-Quarantine to Enable or Disable. o 0 – Disabled o 1 – Enabled • file_type – The only option is "executable". • suspicious_files – Abnormal files • threat_files – Unsafe files
logpolicy	The Agent log file settings. • log_upload – The setting to enable or disable uploading log files. o 0 – Disabled o 1 – Enabled • maxlogsize – The maximum file size (in MB) for a single log file. • retentiondays – The number of days to save log files. Log files older than the set number of days will be deleted.
memory_exclusion_list	The executable files to exclude from Memory Protection. This must be a relative path to the excluded executable file.
memoryviolation_actions	The Violation Types for Memory Protection. **Note**: All Violation Types must be included in the Request. • 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, that cause their modules to be loaded automatically when an application starts. • 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. • maliciouspayload (Malicious Payload) – A generic shellcode and payload detection associated with exploitation has been detected.

- 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 Threat 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). • 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.
policy	Various policy settings are contained within this section. **Note**: All policy settings must be included in the Request. • auto_blocking – Setting to Auto Quarantine Unsafe threats. o 0 – Disabled o 1 – Enabled • auto_delete – 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. o 0 – Disabled o 1 – Enabled • auto_uploading – Setting to automatically upload files that Cylance has not seen before. Cylance will perform an analysis on the file and provide details to assist in manual analysis and triage. o 0 – Disabled o 1 – Enabled • days_until_deleted – Setting for the number of days to retain a quarantined file. Quarantined files older than the set number of days will be automatically deleted. The minimum number of days is 14, the maximum number of days is 365. The "auto-delete" setting must be enabled. • device_control – Setting to enable or disable the Device Control feature. o 0 – Disabled o 1 – Enabled • full_disc_scan – Setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the Background Threat Detection setting. o 0 – Disabled

  - 1 – Run Recurring (performs a scan every nine days)
  - 2 – Run Once (runs a full disk scan upon installation only)
- kill_running_threats – Setting to kill processes and children processes regardless of the state when a threat is detected (EXE or DLL).
  - 0 – Disabled
  - 1 – Enabled
- logpolicy – Setting to enable or disable the Agent logging feature.
- low_confidence_threshold – Setting to adjust the Cylance Score threshold between Unsafe and Abnormal threats. The default is -600, therefore:
  - A Cylance Score of -600 to -1000 is Unsafe.
  - A Cylance Score of 0 to -599 is Abnormal.
  - A Cyalnce Score greater than 0 is Safe.
- memory_exploit_detection – Setting to enable or disable the Memory Protection feature. This affects "memory_violation_actions" ("memory_violations" and "memory_violations_ext").
- optics – Setting to enable or disable CylanceOPTICS®.
  - 0 – Disabled
  - 1 – Enabled
- optics_application_control_auto_upload – Setting to allow the automatic uploading of Application Control related Focus Data.
  - 0 – Disabled
  - 1 – Enabled
- optics_malware_auto_upload – Setting to allow the automatic uploading of Threat related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_memory_defense_auto_upload – Setting to allow the automatic uploading of Memory Protection related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_script_control_auto_upload – Setting to allow the automatic uploading of Script Control related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_set_disk_usage_maximum_fixed – Setting the maximum amount of device storage reserved for use by CylanceOPTICS, in MB. The minimum amount is 500MB and the maximum is 1000MB.
- prevent_service_shutdown – Setting that protects the Cylance service from being shutdown, either manually or by another process.

	• sample_copy_path – Setting to copy all file samples to a network share (CIFS/SMB). Use the fully qualified path. Example: \\server_name\shared_folder. • scan_exception_list – Setting to exclude specific folders and subfolders from being scanned by “full_disc_scan” and “watch_for_new_files”. Set the value to the absolute path for the excluded files. • scan_max_archive_size – Setting for the maximum archive file size (in MB) to be scanned. The value can be 0 to 150. If set to 0, then archive files will not be scanned. • script_control – Setting to enable or disable the Script Control feature. o 0 – Disabled o 1 – Enabled • show_notifications – Setting to enable or disable Desktop Notifications on the endpoint. o 0 – Disabled o 1 – Enabled • threat_report_limit – The number of threats to upload to the Console. • trust_files_in_scan_exception_list – Setting to exclude executable files from Memory Protection actions. The value is the relative path to the excluded executable files. • watch_for_new_files – Setting to analyze new or modified executable files for threats.
policy_name	The name of the policy.
policy_id	The unique identifier for the policy.
policy_utctimestamp	The date and time the policy was created, in UTC.

Get Policies

Allows the caller to get a list of Tenant policies where the Tenant ID is retrieved from the JWT token provided in the request.

Service Endpoint	https://protectapi-{region-code}.cylance.com/policies/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 policy:list scope encoded.
Request	Append the following optional query string parameters: - page: The page number to request. - page_size: The number of policy records to retrieve per page.

Response	200 OK
	Get Policies Response Schema
	{
	"page_number": 0,
	"page_size": 0,
	"total_pages": 0,
	"total_number_of_items": 0,
	"page_items": [
	{
	"id": "string",
	"name": "string",
	"device_count": "string",
	"zone_count": "string",
	"date_added": "2017-05-22T23:35:56.705Z",
	"date_modified": "2017-05-22T23:35:56.705Z"
	}
	]
	}
	400 BadRequest – Returned for the following reasons:
	- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.

	• The page number or page size specified is less than or equal to zero. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 Not Found – No policy resources available. 500 Internal Server Error – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
page_items	The list of policies belonging to the requested page, each displaying the following information: • date_added: The date and time (in UTC) when the Console policy resource was first created. • date_modified: The date and time (in UTC) when the Console policy resource was last modified. • device_count: The number of devices assigned to this policy. • id: The unique ID for the policy resource. • name: The name of the policy. • zone_count: The number of zones assigned to this policy.
page_number	The page number requested.
page_size	The page size requested.
total_number_of_items	The total number of resources.
total_pages	The total number of pages that can be retrieved based on the page size specified.

Create Policy

Allows the caller to create a policy.

Service Endpoint	https://protectapi-{region-code}.cylance.com/policies/v2
Method	HTTP/1.1 POST
Request Headers	Authorization: Bearer < JWT Token returned by Auth API> with the policy:create scope encoded. Content-Type: application/json

Request

Create Policy Request Schema

```
{
  "user_id" : "string",
  "policy" : {
  "device_control": {
    "configurations": [
      {
        "control_mode": "string",
        "device_class": "string"
      }
    ],
    "exclusion_list": [
      {
        "control_mode": "string",
        "product_id": "string",
        "serial_number": "string",
        "vendor_id": "string"
      }
    ]
  },
  "file_exclusions": [
    {
      "file_hash": "string",
      "md5": "string",
      "file_name": "string",
      "category_id": "string",
      "reason": "string"
    }
  ],
  "memoryviolation_actions": {
    "memory_violations": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_violations_ext": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_exclusion_list": "[]"
  },
  "policy": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "policy_name": "string",
  "script_control": {
    "activescript_settings": {
      "control_mode": "string"
    },
    "global_settings": {
      "allowed_folders": "",
      "control_mode": "string"
    },
    "macro_settings": {
      "control_mode": "string"
    },
    "powershell_settings": {
      "console_mode": "string",
      "control_mode": "string"
    }
  },
  "filetype_actions": {
    "suspicious_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ],
    "threat_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ]
  },
  "logpolicy": {
    "log_upload": "string",
    "maxlogsize": "string",
    "retentiondays": "string"
  }
 }
}
```

Response

Create Policy Response Schema

```
{
  "device_control": {
    "configurations": [
      {
        "control_mode": "string",
        "device_class": "string"
      }
    ],
    "exclusion_list": [
      {
        "control_mode": "string",
        "product_id": "string",
        "serial_number": "string",
        "vendor_id": "string"
      }
    ]
  },
  "file_exclusions": [
    {
      "file_hash": "string",
      "md5": "string",
      "file_name": "string",
      "category_id": "string",
      "reason": "string",
      "cloud_score": "string",
      "av_industry": "string",
      "file_type": "string",
      "research_class_id": "string",
      "research_subclass_id": "string"
    }
  ],
  "memoryviolation_actions": {
    "memory_violations": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_violations_ext": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_exclusion_list": []
  },
  "policy": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "policy_name": "string",
  "script_control": {
    "activescript_settings": {
      "control_mode": "string"
    },
    "global_settings": {
      "allowed_folders": "string",
      "control_mode": "string"
    },
    "macro_settings": {
      "control_mode": "string"
    },
    "powershell_settings": {
      "console_mode": "string",
      "control_mode": "string"
    }
  },
  "filetype_actions": {
    "suspicious_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ],
    "threat_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ]
  },
  "logpolicy": {
    "log_upload": "string",
    "maxlogsize": "string",
    "retentiondays": "string"
  },
    "policy_id": "e1b44f3c-5a47-4d7f-b97d-1e63f792c0b9",
    "policy_utctimestamp": "9/22/2017 4:23:51 PM"
}
```

409 Conflict – The policy name specified already exists.

The request JSON schema contains the following fields:

Field Name	Description
device_control	Device Control allows or blocks access to USB Mass Storage devices. **Note**: All Device Classes must be included in the Request. Control Mode (control_mode): • Block – Blocks the USB Mass Storage device from connecting to the endpoint. • FullAccess – Allows the USB Mass Storage device to connect to the endpoint. Device Class (device_class): • AndroidUSB – A portable device running Android OS, like a smartphone or tablet. • iOS – An Apple portable device running iOS, like an iPhone or iPad. **Note**: iOS devices will not change when Device Control is enabled and set to Block, unless the 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 – The device class containing scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers. • USBCDDVDRW – A USB optical drive. • USBDrive – A USB hard drive or USB flash drive. • VMWareMount – VMWare USB Passthrough, which allows a VMware virtual machine client to access USB devices connected to the host. • WPD – 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. • control_mode – Allows or blocks the specific USB Mass Storage device. o Block - Blocks the USB Mass Storage device from connecting to the endpoint. o FullAccess – Allows the USB Mass Storage device to connect to the endpoint. • product_id – The product identifier for the USB Mass Storage device. This information is optional. • Serial_number – The serial number for the USB Mass Storage device. This information is optional. • vendor_id – The vendor identifier for the USB Mass Storage device. This information is required. **Note**: One way to find the Vendor ID for a USB Mass Storage device is to enable Device Control in a policy, assign that policy to an endpoint, then attach the USB Mass Storage device to the endpoint. You can view External Device logs in the Cylance Console, on the Protection page or the Device Details page (External Devices tab).

file_exclusions	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 – A list of categories to identify the type of file. This information is optional.
	  o 1 – None
	  o 2 – Admin Tool
	  o 3 – Internal Application
	  o 4 – Commercial Software
	  o 5 – Operating System
	  o 6 – Drivers
	  o 7 – Security Software
	• file_hash – The SHA256 hash for the file. This information is required.
	• file_name – The name of the file being excluded. This information is required.
	• md5 – The MD5 hash for the file. This information is optional.
	• reason – The reason the file was excluded. This information is required.

filetype_actions	The Auto-Quarantine of Unsafe (threat_files) and Abnormal (suspicious_files). • actions – Set Auto-Quarantine to Enable or Disable. o 0 – Disabled o 1 – Enabled • file_type – The only option is "executable". • suspicious_files – Abnormal files • threat_files – Unsafe files

logpolicy	The Agent log file settings. • log_upload – The setting to enable or disable uploading log files. o 0 – Disabled o 1 – Enabled • maxlogsize – The maximum file size (in MB) for a single log file. • retentiondays – The number of days to save log files. Log files older than the set number of days will be deleted.
memory_exclusion_list	The executable files to exclude from Memory Protection. This must be a relative path to the excluded executable file.
memoryviolation_actions	The Violation Types for Memory Protection. **Note**: All Violation Types must be included in the Request. • 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, that cause their modules to be loaded automatically when an application starts. • 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. • maliciouspayload (Malicious Payload) – A generic shellcode and payload detection associated with exploitation has been detected. • 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 Threat 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). • 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.
policy	Various policy settings are contained within this section. **Note**: All policy settings must be included in the Request. • auto_blocking – Setting to Auto Quarantine Unsafe threats.

- 0 – Disabled
  - 1 – Enabled
- auto_delete – 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.
  - 0 – Disabled
  - 1 – Enabled
- auto_uploading – Setting to automatically upload files that Cylance has not seen before. Cylance will perform an analysis on the file and provide details to assist in manual analysis and triage.
  - 0 – Disabled
  - 1 – Enabled
- days_until_deleted – Setting for the number of days to retain a quarantined file. Quarantined files older than the set number of days will be automatically deleted. The minimum number of days is 14, the maximum number of days is 365. The “auto-delete” setting must be enabled.
- device_control – Setting to enable or disable the Device Control feature.
  - 0 – Disabled
  - 1 – Enabled
- full_disc_scan – 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 – Setting to kill processes and children processes regardless of the state when a threat is detected (EXE or DLL).
  - 0 – Disabled
  - 1 – Enabled
- logpolicy – Setting to enable or disable the Agent logging feature.
- low_confidence_threshold – Setting to adjust the Cylance Score threshold between Unsafe and Abnormal threats. The default is -600, therefore:
  - A Cylance Score of -600 to -1000 is Unsafe.
  - A Cylance Score of 0 to -599 is Abnormal.
  - A Cyalnce Score greater than 0 is Safe.
- memory_exploit_detection – Setting to enable or disable the Memory Protection feature. This affects “memory_violation_actions” (“memory_violations” and “memory_violations_ext”).
- optics – Setting to enable or disable CylanceOPTICS.
  - 0 – Disabled

  - 1 – Enabled
- optics_application_control_auto_upload – Setting to allow the automatic uploading of Application Control related Focus Data.
  - 0 – Disabled
  - 1 – Enabled
- optics_malware_auto_upload – Setting to allow the automatic uploading of Threat related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_memory_defense_auto_upload – Setting to allow the automatic uploading of Memory Protection related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_script_control_auto_upload – Setting to allow the automatic uploading of Script Control related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_set_disk_usage_maximum_fixed – Setting the maximum amount of device storage reserved for use by CylanceOPTICS, in MB. The minimum amount is 500MB and the maximum is 1000MB.
- prevent_service_shutdown – Setting that protects the Cylance service from being shutdown, either manually or by another process.
- sample_copy_path – Setting to copy all file samples to a network share (CIFS/SMB). Use the fully qualified path.
  Example: \\server_name\shared_folder.
- scan_exception_list – Setting to exclude specific folders and subfolders from being scanned by “full_disc_scan” and “watch_for_new_files”. Set the value to the absolute path for the excluded files.
- scan_max_archive_size – Setting for the maximum archive file size (in MB) to be scanned. The value can be 0 to 150. If set to 0, then archive files will not be scanned.
- script_control – Setting to enable or disable the Script Control feature.
  - 0 – Disabled
  - 1 – Enabled
- show_notifications – Setting to enable or disable Desktop Notifications on the endpoint.
  - 0 – Disabled
  - 1 – Enabled
- threat_report_limit – The number of threats to upload to the Console.

	• trust_files_in_scan_exception_list – Setting to exclude executable files from Memory Protection actions. The value is the relative path to the excluded executable files. • watch_for_new_files – Setting to analyze new or modified executable files for threats.
policy_name	The name of the policy.
script_control	The policy settings for Script Control. • activescript_settings – Setting for Active Script. o control_mode ▪ Alert – An alert is sent when an Active Script event occurs. The Active Script is allowed to run. ▪ Block – The Active Script is blocked and an alert is sent. • global_settings o allowed_folders – The relative path to scripts that are allowed to run when Script Control is enabled. o control_mode – Setting to enable or disable Script Control. ▪ 0 – Disable ▪ 1 – Enable • macro_settings – Setting for Microsoft Office Macros. o control_mode ▪ Alert – An alert is sent when an Office Macro event occurs. The Macro is allowed to run. ▪ Block – The Office Macro is blocked and an alert is sent. • powershell_settings – Settings for PowerShell scripts. o console_mode – The PowerShell Console is blocked to prevent PowerShell command usage, including one-liners. The PowerShell control_mode must be set to Block. o control_mode ▪ Alert – An alert is sent when a PowerShell Script event occurs. The PowerShell Script is allowed to run. ▪ Block – The PowerShell Script is blocked and an alert is sent.
user_id	The unique ID for the User creating the policy. Only Administrators can create policies. To get the user_id, use Get User.

The response JSON schema contains most of the fields from the request schema, with the following additional fields:

Field Name	Description
policy_id	The unique identifier for the policy.
policy_utctimestamp	The date and time the policy was created, in UTC.

Update Policy

Allows the caller to update an existing policy.

Service Endpoint	https://protectapi-{region-code}.cylance.com/policies/v2
Method	HTTP/1.1 PUT
Request Headers	Authorization: Bearer < JWT Token returned by Auth API> with the policy:update scope encoded. Content-Type: application/json
Request	Update Policy Request Schema

```
{
  "device_control": {
    "configurations": [
      {
        "control_mode": "string",
        "device_class": "string"
      }
    ],
    "exclusion_list": [
      {
        "control_mode": "string",
        "product_id": "string",
        "serial_number": "string",
        "vendor_id": "string"
      }
    ]
  },
  "file_exclusions": [
    {
      "file_hash": "string",
      "md5": "string",
      "file_name": "string",
      "category_id":"string",
      "reason": "string"
    }
  ],
  "memoryviolation_actions": {
    "memory_violations": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_violations_ext": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_exclusion_list": "[]"
  },
  "policy": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "policy_id": "string",
  "policy_name": "string",
  "policy_utctimestamp": "6/17/2017 4:49:36 AM",
  "script_control": {
    "activescript_settings": {
      "control_mode": "string"
    },
    "global_settings": {
      "allowed_folders": "string",
      "control_mode": "string"
    },
    "macro_settings": {
      "control_mode": "string"
    },
    "powershell_settings": {
      "console_mode": "string",
      "control_mode": "string"
    }
  },
  "filetype_actions": {
    "suspicious_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ],
    "threat_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ]
  },
  "logpolicy": {
    "log_upload": "string",
    "maxlogsize": "string",
    "retentiondays": "string"
 }
}
```

Response

Update Policy Response Schema

```
{
  "device_control": {
    "configurations": [
      {
        "control_mode": "string",
        "device_class": "string"
      }
    ],
    "exclusion_list": [
      {
        "control_mode": "string",
        "product_id": "string",
        "serial_number": "string",
        "vendor_id": "string"
      }
    ]
  },
  "file_exclusions": [
    {
      "file_hash": "string",
      "md5": "string",
      "file_name": "string",
      "category_id": "string",
      "reason": "string"
    }
  ],
  "memoryviolation_actions": {
    "memory_violations": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_violations_ext": [
      {
        "action": "string",
        "violation_type": "string"
      }
    ],
    "memory_exclusion_list": []
  },
  "policy": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "policy_id": "string",
  "policy_name": "string",
  "policy_utctimestamp": "6/17/2017 4:50:42 AM",
  "script_control": {
    "activescript_settings": {
      "control_mode": "string"
    },
    "global_settings": {
      "allowed_folders": "string",
      "control_mode": "string"
    },
    "macro_settings": {
      "control_mode": "string"
    },
    "powershell_settings": {
      "console_mode": "string",
      "control_mode": "string"
    }
  },
  "filetype_actions": {
    "suspicious_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ],
    "threat_files": [
      {
        "actions": "string",
        "file_type": "executable"
      }
    ]
  },
  "logpolicy": {
        "log_upload": "string",
        "maxlogsize": "string",
        "retentiondays": "string"
    }
}
```

204 No Content

The request and response JSON schemas contains the following fields:

Field Name	Description
device_control	Device Control allows or blocks access to USB Mass Storage devices. **Note**: All Device Classes must be included in the Request. Control Mode (control_mode): • Block – Blocks the USB Mass Storage device from connecting to the endpoint. • FullAccess – Allows the USB Mass Storage device to connect to the endpoint. Device Class (device_class): • AndroidUSB – A portable device running Android OS, like a smartphone or tablet. • iOS – An Apple portable device running iOS, like an iPhone or iPad. **Note**: iOS devices will not change when Device Control is enabled and set to Block, unless the 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 – The device class containing scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers. • USBCDDVDRW – A USB optical drive. • USBDrive – A USB hard drive or USB flash drive. • VMWareMount – VMWare USB Passthrough, which allows a VMware virtual machine client to access USB devices connected to the host.

	• WPD – 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. • control_mode – Allows or blocks the specific USB Mass Storage device. o Block - Blocks the USB Mass Storage device from connecting to the endpoint. o FullAccess – Allows the USB Mass Storage device to connect to the endpoint. • product_id – The product identifier for the USB Mass Storage device. This information is optional. • Serial_number – The serial number for the USB Mass Storage device. This information is optional. • vendor_id – The vendor identifier for the USB Mass Storage device. This information is required. **Note**: One way to find the Vendor ID for a USB Mass Storage device is to enable Device Control in a policy, assign that policy to an endpoint, then attach the USB Mass Storage device to the endpoint. You can view External Device logs in the Cylance Console, on the Protection page or the Device Details page (External Devices tab).
file_exclusions	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 – A list of categories to identify the type of file. This information is optional. o 1 – None o 2 – Admin Tool o 3 – Internal Application o 4 – Commercial Software o 5 – Operating System o 6 – Drivers o 7 – Security Software • file_hash – The SHA256 hash for the file. This information is required. • file_name – The name of the file being excluded. This information is required. • md5 – The MD5 hash for the file. This information is optional. • reason – The reason the file was excluded. This information is required.

filetype_actions	The Auto-Quarantine of Unsafe (threat_files) and Abnormal (suspicious_files). • actions – Set Auto-Quarantine to Enable or Disable. o 0 – Disable o 1 – Enable • file_type – The only option is “executable”. • suspicious_files – Abnormal files • threat_files – Unsafe files
logpolicy	The Agent log file settings. • log_upload – The setting to enable or disable uploading log files. o 0 – Disabled o 1 – Enabled • maxlogsize – The maximum file size (in MB) for a single log file. • retentiondays – The number of days to save log files. Log files older than the set number of days will be deleted.
memory_exclusion_list	The executable files to exclude from Memory Protection. This must be a relative path to the excluded executable file.
memoryviolation_actions	The Violation Types for Memory Protection. **Note**: All Violation Types must be included in the Request. • 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, that cause their modules to be loaded automatically when an application starts. • 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. • maliciouspayload (Malicious Payload) – A generic shellcode and payload detection associated with exploitation has been detected. • 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 Threat 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).
- 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.
policy	Various policy settings are contained within this section. **Note**: All policy settings must be included in the Request. • auto_blocking – Setting to automatically block found threats. • auto_delete – 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. o 0 – Disabled o 1 – Enabled • auto_uploading – Setting to automatically upload files that Cylance has not seen before. Cylance will perform an analysis on the file and provide details to assist in manual analysis and triage. o 0 – Disabled o 1 – Enabled • days_until_deleted – Setting for the number of days to retain a quarantined file. Quarantined files older than the set number of days will be automatically deleted. The minimum number of days is 14, the maximum number of days is 365. The “auto-delete” setting must be enabled. • device_control – Setting to enable or disable the Device Control feature. o 0 – Disabled o 1 – Enabled • full_disc_scan – Setting to have Cylance analyze all executable files on disk to detect any dormant threats. This is the Background Threat Detection setting. o 0 – Disabled o 1 – Run Recurring (performs a scan every nine days) o 2 – Run Once (runs a full disk scan upon installation only) • kill_running_threats – Setting to kill processes and children processes regardless of the state when a threat is detected (EXE or DLL). o 0 – Disabled o 1 – Enabled • logpolicy – Setting to enable or disable the Agent logging feature. • low_confidence_threshold – Setting to adjust the Cylance Score threshold between Unsafe and Abnormal threats. The default is -600, therefore:

- A Cylance Score of -600 to -1000 is Unsafe.
  - A Cylance Score of 0 to -599 is Abnormal.
  - A Cyalnce Score greater than 0 is Safe.
- memory_exploit_detection – Setting to enable or disable the Memory Protection feature. This affects “memory_violation_actions” (“memory_violations” and “memory_violations_ext”).
- optics – Setting to enable or disable CylanceOPTICS.
  - 0 – Disabled
  - 1 – Enabled
- optics_application_control_auto_upload – Setting to allow the automatic uploading of Application Control related Focus Data.
  - 0 – Disabled
  - 1 – Enabled
- optics_malware_auto_upload – Setting to allow the automatic uploading of Threat related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_memory_defense_auto_upload – Setting to allow the automatic uploading of Memory Protection related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_script_control_auto_upload – Setting to allow the automatic uploading of Script Control related Focus data.
  - 0 – Disabled
  - 1 – Enabled
- optics_set_disk_usage_maximum_fixed – Setting the maximum amount of device storage reserved for use by CylanceOPTICS, in MB. The minimum amount is 500MB and the maximum is 1000MB.
- prevent_service_shutdown – Setting that protects the Cylance service from being shutdown, either manually or by another process.
- sample_copy_path – Setting to copy all file samples to a network share (CIFS/SMB). Use the fully qualified path.
  Example: \\server_name\shared_folder.
- scan_exception_list – Setting to exclude specific folders and subfolders from being scanned by “full_disc_scan” and “watch_for_new_files”. Set the value to the absolute path for the excluded files.
- scan_max_archive_size – Setting for the maximum archive file size (in MB) to be scanned. The value can be 0 to 150. If set to 0, then archive files will not be scanned.

	• script_control – Setting to enable or disable the Script Control feature. o 0 – Disabled o 1 – Enabled • show_notifications – Setting to enable or disable Desktop Notifications on the endpoint. o 0 – Disabled o 1 – Enabled • threat_report_limit – The number of threats to report to the Console. • trust_files_in_scan_exception_list – Setting to exclude executable files from Memory Protection actions. The value is the relative path to the excluded executable files. • watch_for_new_files – Setting to analyze new or modified executable files for threats.
policy_id	The unique identifier for the policy.
policy_name	The name of the policy.
policy_utctimestamp	The date and time the policy was created, in UTC.
script_control	The policy settings for Script Control. • activescript_settings – Setting for Active Script. o control_mode ▪ Alert – An alert is sent when an Active Script event occurs. The Active Script is allowed to run. ▪ Block – The Active Script is blocked and an alert is sent. • global_settings o allowed_folders – The relative path to scripts that are allowed to run when Script Control is enabled. o control_mode – Setting to enable or disable Script Control. ▪ 0 – Disabled ▪ 1 – Enabled • macro_settings – Setting for Microsoft Office Macros. o control_mode ▪ Alert – An alert is sent when an Office Macro event occurs. The Macro is allowed to run. ▪ Block – The Office Macro is blocked and an alert is sent.

- powershell_settings – Settings for PowerShell scripts.
  - console_mode – The PowerShell Console is blocked to prevent PowerShell command usage, including one-liners. The PowerShell control_mode must be set to Block.
  - control_mode
    - Alert – An alert is sent when a PowerShell Script event occurs. The PowerShell Script is allowed to run.
    - Block – The PowerShell Script is blocked and an alert is sent.

Delete Policy

Delete a policy from the Console.

Service Endpoint	https://protectapi-{region-code}.cylance.com/policies/v2/<tenant_policy_id>
Method	HTTP/1.1 DELETE
Request Headers	Authorization: Bearer < JWT Token returned by Auth API> with the policy:delete scope encoded.
Request	Append the Tenant Policy ID to the Service Endpoint.
Response	204 No Content

Delete Policies

Delete multiple policies from the Console.

Service Endpoint	https://protectapi-{region-code}.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	Delete Tenant Policies Request Schema
	{
	"tenant_policy_ids": [
	"string",
	"string",
	"string",
	"string",
	"string"
	]
	}

Response	204 No Content

The request JSON schema contains the following fields:

Field Name	Description
string	Replace "string" with the Tenant Policy ID. Example: "012a3456-78b9-0c12-3d4e-f56g78hijklm"

Zone API

Create Zone

Create (add) a zone to your Console.

Service Endpoint	https://protectapi-{region-code}.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	Post Zone Request Schema
	{
	"name": "string",
	"policy_id": "string",
	"criticality": "string"
	}

Response	201 Created
	Post Zone Response Schema
	{
	"id": "string",
	"name": "string",
	"criticality": "string",
	"policy_id": "string",
	"date_created": "2017-06-15T21:35:11.994Z"
	}
	400 BadRequest – The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.

- The zone name value provided is not a valid value for a name.
- The zone criticality provided is not a valid value for criticality.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

409 Conflict – The zone name provided already exists in your organization.

500 InternalServerError – An unforeseeable error has occurred.

The request JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
name	The name of the Zone.
policy_id	The unique ID for the policy assigned to the Zone.

The response JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
date_created	The date and time (in UTC) when the Zone was created.
id	The unique ID for the Zone.
name	The name of the Zone.
policy_id	The unique ID for the policy assigned to the Zone.

Get Zones

Request zone information for your organization. This will return the top 100 records.

<table>
<tr><td>Service Endpoint</td><td>https://protectapi-{region-code}.cylance.com/zones/v2?page=m&page_size=n</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 zone:list scope encoded.</td></tr>
<tr><td>Request</td><td>Append the following (optional) query string parameters:

• page: The page number to request.
• page_size: The number of zone records to retrieve per page.</td></tr>
<tr><td>Response</td><td>200 OK

Get Zones Response Schema
<pre>
{
  "page_number": 0,
  "page_size": 0,
  "total_pages": 0,
  "total_number_of_items": 0,
  "page_items": [
    {
      "id": "string",
      "name": "string",
      "criticality": "string",
      "zone_rule_id": "string",
      "policy_id": "string",
      “update_type”: “string”,
      "date_created": "2017-06-15T21:35:11.994Z",
      "date_modified": "2017-06-15T21:35:11.994Z"
    }
  ]
}
</pre></td></tr>
</table>

	400 BadRequest – The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
date_created	The date and time (in UTC) when the zone was created.
date_modified	The date and time (in UTC) when the zone was last modified.
id	The unique ID of the zone.
name	The name of the zone.
policy_id	The unique ID of the policy assigned to the zone.
update_type	The update type for the zone.
zone_rule_id	The unique ID for the zone rule created for the zone.

Get Device Zones

Request zone information for a specified device in your organization. This will return the top 100 records.

Service Endpoint	https://protectapi-{region-code}.cylance.com/zones/v2/{unique device id}/zones?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 zone:list scope encoded.
Request	Append the following (optional) query string parameters: • page: The page number to request.

- page_size: The number of zone records to retrieve per page.

Response

200 OK

Get Zones Response Schema

```
{
  "page_number": 0,
  "page_size": 0,
  "total_pages": 0,
  "total_number_of_items": 0,
  "page_items": [
    {
      "id": "string",
      "name": "string",
      "criticality": "string",
      "zone_rule_id": "string",
      "policy_id": "string",
      “update_type”: “string”,
      "date_created": "2017-06-15T21:35:11.994Z",
      "date_modified": "2017-06-15T21:35:11.994Z"
    }
  ]
}
```

400 BadRequest – The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
date_created	The date and time (in UTC) when the zone was created.

date_modified	The date and time (in UTC) when the zone was last modified.
id	The unique ID of the zone.
name	The name of the zone.
policy_id	The unique ID of the policy assigned to the zone.
update_type	The update type for the zone.
zone_rule_id	The unique ID for the zone rule created for the zone.

Get Zone

Request zone information for a specific zone in your organization.

Service Endpoint	https://protectapi-{region-code}.cylance.com/zones/v2/{unique_zone_id}
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	200 OK
	Get Zone Response Schema
	{
	"id": "string",
	"name": "string",
	"criticality": "string",
	"zone_rule_id": "string",
	"policy_id": "string",
	"date_created": "2017-06-15T21:35:11.994Z",
	"date_modified": "2017-06-15T21:35:11.994Z"
	}
	400 BadRequest – Returned for the following reasons:
	• The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.

	- The zone unique identifier is not valid. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The zone requested doesn't exist. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
date_created	The date and time (in UTC) when the zone was created.
date_modified	The date and time (in UTC) when the zone was last modified.
id	The unique ID of the zone.
name	The name of the zone.
policy_id	The unique ID of the policy assigned to the zone.
zone_rule_id	The unique ID for the zone rule created for the zone.

Update Zone

Update a zone in your organization.

Service Endpoint	https://protectapi-{region-code}.cylance.com/zones/v2/{unique_zone_id}
Method	HTTP/1.1 PUT
Request Headers	Accept: application/json Authorization: Bearer < JWT Token returned by Auth API> with the zone:update scope encoded. Content-Type: application/json
Request	

	Put Zone Request Schema
	{
	"name": "string",
	"policy_id": "string",
	"criticality": "string"
	}

Response	200 OK 400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The zone name provided is not a valid value for a name. • The zone criticality provided is not a valid value for criticality. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The zone requested doesn’t exist. 409 Conflict – The zone name provided already exists in the organization. 500 InternalServerError – An unforeseeable error has occurred.

The request JSON schema contains the following fields:

Field Name	Description
criticality	The value of the Zone – Low, Medium, or High.
name	The name of the zone.
policy_id	The unique ID of the policy assigned to the zone.

Delete Zone

Delete (remove) a zone from your Console.

Service Endpoint	https://protectapi-{region-code}.cylance.com/zones/v2/{unique zone id}
Method	HTTP/1.1 DELETE
Request Headers	Authorization: Bearer < JWT Token returned by Auth API> with the zone:delete scope encoded.
Request	None
Response	200 OK 400 BadRequest – The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The zone requested doesn’t exist. 500 InternalServerError – An unforeseeable error has occurred.

Threat API

Get Threat

Request threat details for a specific threat.

Service Endpoint	https://protectapi-{region-code}.cylance.com/threats/v2/{hash}
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	Append the SHA256 for the threat to the service endpoint.
Response	200 OK Get Threat Response Schema

Get Threat Response Schema

```
{
   "name": "string",
   "sha256": "string",
   "md5": "string",
   "signed": true,
   "cylance_score": 0,
   "av_industry": 0,
   "classification": "string",
   "sub_classification": "string",
   "global_quarantine": true,
   "safelisted": true,
   "cert_publisher": "string",
   "cert_issuer": "string",
   "cert_timestamp": "2017-06-15T21:35:11.994Z",
   "file_size": 0,
   "unique_to_cylance": true,
   "running": "string",
   "auto_run": true,
   "detected_by": "string"
}
```

	400 BadRequest – Returned for the following reasons: • The Tenant ID could not be retrieved from the JWT token specified in the Authorization header. • The Threat Hash ID specified is invalid. 401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid. 403 Forbidden – The JWT token did not contain the proper scope to perform this action. 404 NotFound – The threat requested doesn't exist. 500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
auto_run	Indicates if the file is set to automatically run on system startup.
av_industry	The score provided by the antivirus industry.
cert_issuer	The ID for the certificate issuer.
cert_publisher	The ID for the certificate publisher.
cert_timestamp	The date and time (in UTC) when the file was signed using the certificate.
classification	The threat classification for the threat.
cylance_score	The Cylance Score assigned to the threat.
detected_by	The name of the Cylance module that detected the threat.
file_size	The size of the file.
global_quarantine	Identifies if the threat is on the Global Quarantine list.
md5	The MD5 hash for the threat.
name	The name of the threat.
running	Identifies if the threat is executing, or another executable loaded or called it.
safelisted	Identifies if the threat is on the Safe List.
sha256	The SHA256 hash for the threat.

signed	Identifies the file as signed or not signed.
sub_classification	The threat sub-classification for the threat.
unique_to_cylance	The threat was identified by Cylance but not by other antivirus sources.

Get Threats

Allows a caller to request a page with a list of Console threat resources belonging to a Tenant, sorted by the last found date, in descending order (most recent policy 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	https://protectapi-{region-code}.cylance.com/threats/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 threat:list scope encoded.
Request	Append the following optional query string parameters: • page: The page number to request. • page_size: The number of device records to retrieve per page.
Response	200 OK Get Threats Response Schema

```
{
  "page_number": 0,
  "page_size": 0,
  "total_pages": 0,
  "total_number_of_items": 0,
  "page_items": [
    {
      "name": "string",
      "sha256": "string",
      "md5": "string",
      "cylance_score": 0,
      "av_industry": 0,
      "classification": "string",
      "sub_classification": "string",
      "global_quarantined": true,
      "safelisted": true,
      "file_size": 0,
      "unique_to_cylance": true
      "last_found": "2017-06-15T21:35:11.994Z"
    }
  ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The Threat Hash ID specified is invalid.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

404 NotFound – The threat requested doesn't exist.

429 TooManyRequests – The rate limit has been reached.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
av_industry	The score provided by the antivirus industry.
cert_issuer	The ID for the certificate issuer.
cert_publisher	The ID for the certificate publisher.
cert_timestamp	The date and time (in UTC) when the file was signed using the certificate.
classification	The threat classification for the threat.
cylance_score	The Cylance Score assigned to the threat.
file_size	The size of the file.

global_quarantined	Identifies if the threat is on the Global Quarantine list.
md5	The MD5 hash for the threat.
name	The name of the threat.
safelisted	Identifies if the threat is on the Safe List.
sha256	The SHA256 hash for the threat.
signed	Identifies the file as signed or not signed.
sub_classification	The threat sub-classification for the threat.
unique_to_cylance	The threat was identified by Cylance but not by other antivirus sources.

Get Threat Devices

Request threat details for a specific threat.

Service Endpoint	https://protectapi-{region-code}.cylance.com/threats/v2/{hash}/devices?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 threat:devicelist scope encoded.
Request	Append the following (optional) query string parameters: • page: The page number to request. • page_size: The number of device records to retrieve per page.
Response	200 OK Get Threat Devices Response Schema { "page_number": 0, "page_size": 0, "total_pages": 0, "total_number_of_items": 0, "page_items": [{

```
          "id": "string",
          "name": "string",
          "state": "Offline",
          "agent_version": "string",
          "policy_id": "string",
          "date_found": "2017-06-15T21:35:11.994Z",
          "file_status": "Quarantined",
          "file_path": "string",
          "ip_addresses": [
            "string1",
            "string2" ],
          "mac_addresses": [
            "string1”,
            "string2” ]
      }
    ]
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The Threat Hash ID specified is invalid.
- The page number or page size specified is less than or equal to zero, or the page size is greater than 200.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

Field Name	Description
agent_version	The agent version installed on the device.
date_found	The date and time (in UTC) when the threat was found on the device.
fie_path	The path where the file was found on the device.

file_status	Current quarantine status of the file on the device. • 0 – Default • 1 – Quarantined • 2 – Whitelisted • 3 – Suspicious • 4 – FileRemoved • 5 – Corrupt
id	The device ID.
ip_addresses	The list of IP addresses for the device.
mac_addresses	The list of MAC addresses for the device.
name	The device name for the device.
policy_id	The unique identifier of the policy assigned to the device, or null if no policy is assigned.
serial_number	The API key of the device.
state	The state of the device. • 0 – Offline • 1 – Online

Get Threat Download URL

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

Service Endpoint	https://protectapi-{region-code}.cylance.com/threats/v2/{sha256}
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	Append the following (optional) query string parameters: • sha256: The SHA256 hash for the file.
Response	200 OK

Get Threat Download URL Schema

```
{
  "url": "string"
}
```

400 BadRequest – Returned for the following reasons:

- The Tenant ID could not be retrieved from the JWT token specified in the Authorization header.
- The provided SHA256 hash is invalid.
    - Not associated with the Tenant.
    - Agent reported SHA1 and MD5 hashes do not match values in the Console.
    - SHA1 or MD5 hash is empty.
- The page number or page size specified is less than or equal to zero, or the page size is greater than 200.

401 Unauthorized – The JWT token was not specified, has expired, or is otherwise invalid.

403 Forbidden – The JWT token did not contain the proper scope to perform this action.

500 InternalServerError – An unforeseeable error has occurred.

The response JSON schema contains the following fields:

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

API Tools

Information about some REST and JSON tools that might help you when using the CylancePROTECT APIs.

Note: Cylance supports CylancePROTECT API resources, including helping Users troubleshoot Cylance API requests. Cylance does not write or train Users on how to create scripts or code (like using Python).

REST Clients

Although the intent of the CylancePROTECT API is to facilitate easy integration of Cylance and other systems through the organization's developed code, using or testing the CylancePROTECT 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 CylancePROTECT API. Some examples are:

- Fiddler (http://www.telerik.com/fiddler) – Free web debugging proxy. Also has an easy-to-use composer and replay features for HTTP requests.
- Postman (https://www.getpostman.com) – Google Chrome browser extension designed for testing REST APIs. There are also native Windows, macOS, and Linux clients available.

JSON Validators

CylancePROTECT 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 (http://jsonformatter.curiousconcept.com) – Online, simple interface with options to define/transform the output according to the desired level of white space. Highlights and provides informative descriptions of errors.
- Notepad++ (https://notepad-plus-plus.org) – Freeware text editor. In addition to being a powerful replacement for Microsoft Notepad, it supports a wide variety of plug-in extensions, including various JSON formatting and validation tools (like JSTool and JSON Viewer).