



Imperva API Documentation

15 January 2026

Contents

Imperva API Documentation	5
API Overview	6
SaaS API Version 1 Overview	6
SaaS API Version 2/3 Overview	9
On-Premises API Overview	10
OpenAPI (Swagger)	11
Authentication	12
API Lifecycle and Deprecation Policy	13
SaaS API Policy	13
On-Premises API Policy	14
API Reference	17
SaaS Account and User Management	17
User Management	17
Identity Management	17
User and Role Management	35
Account Management	54
Account Management	54
Account Export	76
Export Account Configuration	76
Account Export API Definition	77
Subscription	84
Usage Report	91
Audit Trail	100
Notification Settings	105
SIEM Log Configuration	126
SaaS Website Management	157
Simplified Site Onboarding with an Imperva Site Certificate	157
Advanced Site Onboarding with an Imperva Site Certificate	161
Site Onboarding with a Custom Certificate	166
Website Management API Definition	169
Website Domain Management API Definition	209
Certificate Management	232
SSL Certificates	232
Client Certificate Management	286
Custom Certificates	304
Custom Certificates with HSM Support	307
Tools	310
Troubleshooting	310
Integrations	316
SaaS Application Security	322
Cloud WAF	322
Policy Management	322

Policy Management API Definition	322
Policies API Extended Information	372
Custom Rules	383
Site Management	394
Site Onboarding with an Imperva Account Certificate	394
Site Management	396
Traffic Statistics and Logs	523
Login Protect	546
Login Protect API Overview	546
Login Protect API Definition	547
Settings	562
Session Management	569
Account Takeover Protection	572
Advanced Bot Protection	632
Advanced Bot Protection API Overview	632
Advanced Bot Protection	633
API Security	736
Basic	736
Advanced	828
General	828
Tags	1064
Attack Analytics	1085
Attack Analytics API Overview	1085
Attack Analytics API Definition	1085
Client-Side Protection	1106
Reputation Intelligence	1187
Runtime Protection	1191
SaaS Application Performance	1205
Delivery Settings	1205
Cache Settings	1213
Load Balancing Settings	1229
Load Balancing Monitoring Settings	1234
Website Performance Statistics	1243
Website Performance Statistics API Overview	1243
Website Performance Statistics API Definition	1244
Waiting Rooms	1250
SaaS Network Security	1287
DDoS Protection for Networks and IPs	1287
DDoS Protection for Networks: Test Alerts	1287
DDoS Protection for Networks/IPs: Policy Visibility	1300
DDoS Protection for Individual IPs (over TCP/IP only)	1314
DDoS Protection for Individual IPs (over TCPIP, GRE, IPinIP)	1328
DDoS Protection for Networks: Connections	1342
DDoS Protection for Networks: Flow Exporters	1359
DDoS Protection for Networks: Network Range Diversion	1366

DDoS Protection for Networks: Performance Monitoring	1373
DDoS Protection for Networks and IPs: Asset Migration.....	1377
DDoS Protection for Networks: Access List (ACL) Policies.....	1381
DDoS Protection for Individual IPs: Access List (ACL) Policies	1397
DDoS Protection: Allowlist Policies	1413
DDoS Protection: Asset Management.....	1428
DDoS Protection for Networks: Traffic Statistics and Logs	1431
DNS.....	1454
DNS Protection API Definition	1454
Deprecated SaaS API	1628
Usage Report (Deprecated)	1628
On-Premises Security.....	1635

Imperva API Documentation

Imperva provides customers and partners with the ability to manage your accounts and services via an API. This section provides a reference to all Imperva customer consumable APIs.

SaaS

To learn more about the different API versions, see:

- [API Version 1 Overview](#)
- [API Version 2 Overview](#)

For a full list of the available APIs, see the [API Reference](#) section.

On-Premises

- [On-Premises Security API](#)
- [On-Premises API Overview](#)

SaaS API Version 1 Overview

Imperva provides customers and partners with the ability to manage accounts and sites via an API.

Note: To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your Cloud Application Security sites. For details, see [SaaS API Version 2/3 Overview](#).

Overview

The API has the following characteristics:

- Requests are HTTP POST.
- Parameters are specified in the request body in HTML form style. For example:

```
param1=value1&param2=value2
```

- All requests are in SSL.
- Response content is provided as a JSON document.
- UTF-8 encoding is always used.

General request structure

Account and site identifiers

Most API operations operate on a specific account or site. Use the following parameters to specify the account or site to operate on:

Name	Description
account_id	Numeric identifier of the account to operate on.
site_id	Numeric identifier of the site to operate on.

Pagination

Some API operations may return a list of objects. Use the following parameters to enable paging:

Name	Description	Optional
page_size	The number of objects to return in the response.	Yes

Name	Description	Optional
	Default: 50 Maximum: 100	
page_num	The page to return starting from 0. In order to view the full results, the client needs to run the API call with <code>page_num</code> set to 0, then again with <code>page_num</code> set to 1, and so forth. Default: 0	Yes

Time range specification

Some operations require the user to specify a time range. This is done via the `time_range` parameter, which accepts the following values:

Name	Description
today	Retrieve data from midnight today until the current time.
last_7_days	Retrieve data from midnight of 7 days ago until the current time.
last_30_days	Retrieve data from midnight of 30 days ago until the current time.
last_90_days	Retrieve data from midnight of 90 days ago until the current time.
month_to_date	Retrieve data from midnight of the first day of the month until the current time.
custom	<p>Specify a custom time range using two additional parameters: <code>start</code> and <code>end</code>.</p> <p>Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.</p> <p>For example:</p> <ul style="list-style-type: none"> ▪ A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day. ▪ A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and

Name	Description
	<p>Wednesday - two full days.</p> <ul style="list-style-type: none"> A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

Note:

- If a time range is not specified, `today` is selected by default.
- All dates should be specified as number of milliseconds since midnight 1970 (UNIX time * 1000). For details, see http://en.wikipedia.org/wiki/Unix_time.
- Midnight is based on Coordinated Universal Time (UTC).
- The available time ranges depend on the customer subscription plan.

General response structure

Every response contains the following fields in the returned JSON document:

Name	Description
<code>res</code>	The numeric result code for the operation. A result code of 0 indicates success.
<code>res_message</code>	The textual representation of the result code (for example: "OK" - for success).
<code>debug_info</code>	General information which is not strictly required for using the API, but is helpful to have.

For example:

```
{
  "res": 0,
  "res_message": "OK",
  "debug_info": {}
}
```

General error codes:

Code	Description	Comment
1	Unexpected error	The server has encountered an unexpected error.
2	Invalid input	Input missing or incorrect.
4	Operation timed-out or server unavailable	The server is not available or reached a time-out while processing the operation.

Code	Description	Comment
9411	Authentication missing or invalid	Authentication parameters missing or incorrect.
9403	Unknown/unauthorized account_id	The specified account is unknown or client is not authorized to operate on it.
9413	Unknown/unauthorized site_id	The specified site is unknown or client is not authorized to operate on it.
9414	Feature not permitted	Feature is not available on account's plan.
9415	Operation not allowed	The requested operation is not allowed.

SaaS API Version 2/3 Overview

To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your accounts and services.

The APIs documented in this section either provide an alternative to existing APIs, or provide APIs with new functionality.

All existing version 1 APIs continue to be supported.

What's new in Version 2 and 3?

- Naming and formatting conventions for the HTTP requests are consistent with REST API standards and best practices. For example:
 - The resource to operate on, such as the rule ID, is included in the core HTTP request and not as an additional parameter.
 - Parameters are sent in JSON format in the body of the request, and not as form data.
- In addition to POST, other common HTTP methods are used (GET, POST, PUT, DELETE).
- In addition to reporting error codes in the response body, proper HTTP response status codes are now also returned.

Overview

The API has the following characteristics:

- Authentication parameters are sent as headers.
- All other parameters are specified in JSON format in the request body.
- All requests are in SSL.
- Response content is provided as a JSON document.

-
- UTF-8 encoding is always used.
 - Standard HTTP response error codes are used.

On-Premises API Overview

The REST APIs are for developers who want to access the SecureSphere server directly. The documentation describes various API operations, related request and response structures, and error codes.

For the full list of APIs, see [On-Premises Security API](#)

OpenAPI (Swagger)

OpenAPI definition files are available for many Imperva features and services.

Swagger is a cloud based, interactive API testing and documentation tool. APIs are visually rendered as a fully interactive document, enabling you to:

- visualize and interact with the API resources
- view and download the API documentation
- learn how to use the API
- try out the API before integrating it into your code using your API ID and key

For the full list of available OpenAPI Definition files, see the **API Reference** section.

Authentication

This topic describes the API authentication method for Imperva SaaS products.

In order to use the API, the client must be authenticated by Imperva. To authenticate, send your API ID and API key using the **x-API-Id** and **x-API-Key** request headers. For example:

x-API-Id: 12345

x-API-Key: 123*****789

For example, a curl request might look like this:

```
curl -X 'GET' \
'https://api.imperva.com/policies/v2/policies' \
-H 'accept: application/json' \
-H 'x-API-Id: 2222' \
-H 'x-API-Key: 33333'
```

To create and manage API keys with granular permissions and sub account access, see [API Key Management](#).

The API functionality available for your use is based on the roles and permissions assigned to your user.

API Lifecycle & Deprecation Policy for SaaS

This topic describes the API Lifecycle & Deprecation Policy for Imperva SaaS products.

Changes made to this policy will be communicated in the [Release Notes](#).

API version status

Version Status	Description	Documentation	Support	Release Notes
Active	The current and recommended API version.	Available two weeks prior to general availability release.	Fully supported. Updated with bug fixes and new features.	Notifications published two weeks prior to launch and again on launch date.
Deprecated	<p>The API is planned for removal and has been superseded by a newer version.</p> <p>New customers or new integrations by existing customers are denied access to deprecated APIs.</p>	The version is marked as Deprecated on the day of deprecation.	Supported for six months from the deprecation date (bug fixes).	Notifications published 90 days prior to deprecation and again on deprecation date.
Retired	<p>An API version that was deprecated for more than six months.</p> <p>Any application using a retired API should migrate to an active API version at the earliest opportunity.</p>	The version is marked as Retired on the day of retirement.	No longer supported (six months after deprecation).	Notifications published 90 days prior to retirement and again on retirement date.
Decommissioned	<p>No longer available in production.</p> <p>The version will be decommissioned immediately after the 6-month retirement period.</p>	N/A	None.	Notification published 90 days prior to decommissioning.

Version Status	Description	Documentation	Support	Release Notes
	<p>Note: If an API has no customer usage for 3 months, it may be immediately announced as decommissioned.</p>			

Note: Changes required due to security issues may have a shorter notification and action window.

Time line example

October 1, 2025	January 1, 2026	April 1, 2026	July 1, 2026	October 1, 2026	January 1, 2027
Announcement that API will be deprecated on January 1, 2026.	API status changed to deprecated .	Announcement that API will be retired on July 1, 2026.	API status changed to retired .	Announcement that API will be decommissioned on January 1, 2027.	The API is decommissioned .

API Lifecycle & Deprecation Policy for On-Premises

This topic describes the API Lifecycle & Deprecation Policy for Imperva on-premises products.

The current API Lifecycle & Deprecation Policy is part of our API terms and conditions of use. We may make periodic updates to this Policy, at which time we will notify those who have agreements with us.

This policy is valid only for APIs in GA releases. APIs or features in the beta stage can be changed or retired with no obligations.

There can be breaking changes in some new software versions (changes that break what used to work in older versions). Before upgrading, make sure to check if the new version introduces any changes that might affect your applications.

One way Imperva introduces breaking changes in APIs is by introducing a new version of the API, deprecating the old one and enabling customers to migrate to the new version of the API. After a period of time the old API will

be decommissioned (i.e. no longer available). The deprecation status of an API indicates that you should migrate your application to use the new APIs before upgrading to a newer software version where the old API will not be available. This is a common practice in the industry that allows vendors to enhance the functionality while allowing their customers to adapt to those changes without significant disruption.

Before we explain the policy of deprecation and decommissioning of APIs in On-Prem products in Imperva in more detail, we would like to review the On-Prem product's software lifecycle.

Imperva Product Lifecycle

Imperva On-Prem product versions are denoted as X.Y.Z, where X is the major version, Y is the minor version, and Z is the patch level or maintenance release (version 12.1.1, for example).

Starting with SecureSphere Version 12.0, Imperva provides two different software release types within the release cycle: Feature Pack and Long-Term Support (LTS) Release.

- **Feature Pack:** The most recent GA (generally available) **major** release. A handful of minor releases are usually delivered within the same major release, allowing Imperva to provide new functionality and new APIs. For example, software versions 14.0, 14.1, 14.2, 14.3.
- **Long Term Support:** The last minor release of a major version. Once a new GA comes out, the current Feature Pack moves into LTS. Maintenance Releases may be provided on the LTS for another three years, as needed. LTS releases will have only bug fixes but continue to receive ADC content updates for security vulnerabilities. Threat Radar subscriptions and updates will also be maintained through the life of the LTS release. LTS releases will be supported for three years. (For example, while the current feature pack version may be ver 14.3, the LTS versions might be version 13.5.20 and 12.5.50.)
- **EOS (End Of Support):** An LTS release after three years. It is not supported. Any application using an EOS version must migrate to a newer version. We recommend moving to the feature pack version.
- **EOL (End Of Life):** An EOS release after three months.

API Lifecycle Policy

Imperva's API On-Premises lifecycle and deprecation policy is designed to minimize disruption and provide stability, as follows:

- **In LTS releases, APIs are not deprecated or decommissioned.** This makes sure existing integrations continue working when upgrading to a new minor / patch release.
- In a feature pack major release, an API may change its status once: from active to deprecated or from deprecated to decommissioned.

Let's examine a hypothetical example of an API login/v1 lifecycle:

- login/v1 was created in v12.3
- login/v1 was deprecated in v13.2. In the same release, login/v2 was introduced, allowing customers to migrate to it. login/v1 continues to stay in deprecation status in all the following ver13.x releases including those released once version 13 becomes LTS.

-
- In version 14.1 login/v1 was decommissioned and hence does not work any more.

There might be exceptions to the above policy in rare cases where Imperva has identified a security vulnerability for which the resolution is to update the API. In such cases, Imperva will notify customers about the change through the documentation.

Implications for Customers

Customers who upgrade to a new major release need to check if any APIs they use were deprecated or decommissioned, and act accordingly. When an API is deprecated, it is still supported by Imperva, but it is advised to move to the newer API to allow the smooth upgrade to a newer major release.

Documentation

Each major software release has its own documentation. In addition, different minor releases within the feature pack release have different documentation as more features are added in each release. All documentation can be found on the Imperva documentation website at

<https://docs.imperva.com/bundle?labelkey=version-14.3>.

When drilling down into specific APIs in the API reference guide, users may also see the status of specific APIs in the event that they are deprecated. Decommissioned APIs are not part of the documentation.

For your convenience, the upgrade guide has a page summarizing the deprecated features and APIs. For example, <https://docs.imperva.com/bundle/v14.3-upgrade-guide/page/69357.htm>.

It is in that location that you can see any deprecated or decommissioned APIs.

We suggest you review this section of the upgrade guide prior to upgrading your product, and make sure APIs you are using are not affected by the upgrade.

Imperva Identity Management API

Get a detailed list of your account users, including name, ID, email, and assigned roles. For more details, see [Manage Account Users](#)

Version: 1.0.0

BasePath:/identity-management

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

UserManagement

- post /v3/idm-users/{email}
- post /v3/idm-users
- delete /v3/idm-users/{email}
- get /v3/idm-users
- get /v3/users/list
- get /v3/idm-users/{email}
- patch /v3/idm-users/{email}

UserManagement

```
post /v3/idm-users/{email}
```

Assign user to a specific sub-account (addUserToSubAccount)

Adds user with specified email to a specific subaccount. You can grant different levels of permissions and sub account access to users, based on the level of visibility and control that is required. To do that you can specify a list of roles user will get for specific subaccount. To retrieve the list of available roles, use following API: GET "/user-management/v1/roles"

Path parameters

email (required)

Path Parameter

— User's email

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `ExternalRoleAssignmentsDtoBase` (required)
Body Parameter

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`IdmUsersResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    }],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    }],
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json
- */*

Responses

200

Success [IdmUsersResponse](#)

400

Bad request [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":400,"id":"hfdhfif47bhjf","source":{"pointer":"/v3/idm-users/useremail@imperva.com"},"title":"Failed role request","detail":"Role with ID 111 does not exist on account with ID 1234"}]}
```

401

Unauthorized [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"id":null,"status":401,"source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Unauthorized"}]}
```

409

Conflict [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":409,"id":"24e8ffa30c72f806","source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Resource already exist [USER]","detail":"User ema"}]}
```

```
il@imperva.com already associated with sub-account 54132528"}]}]
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"f7876549b57cf","source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Internal Server Error","detail":"INTERNAL_SERVER_ERROR"}]}
```

```
post /v3/idm-users
```

Create new user (createUser)

Creates a new user with the specified user details. The account administrator or any user with the appropriate permissions can add a new user to the account. When a new user is created in an account, a verification mail is sent to the email address listed for the user. The new user clicks the link in the email to verify their address and set a login password. You can assign roles to a user when creating the user or at a later time. To retrieve the list of available roles, use following API GET "/user-management/v1/roles"

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateIdmUserDto](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[IdmUsersResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json
- */*

Responses

200

Success [IdmUsersResponse](#)

400

Bad request [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":400,"id":"95b356fgj13","source":{"pointer":"/v3/idm-user-s"},"title":"Input validation error for field roleIds","detail":"'roleIds'[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]]: Too many roles"}]}
```

401

Unauthorized APIError

Example data

Content-Type: */*

```
{"errors": [{"id":null,"status":401,"source":{"pointer":"/v3/idm-users"},"title":"Unauthorized"}]}
```

409

Conflict APIError

Example data

Content-Type: */*

```
{"errors": [{"status":409,"id":"7f21c4c098068345","source":{"pointer":"/v3/idm-users"},"title":"Resource already exist [USER]","detail":"User email@imperva.com already exist"}]}
```

500

Internal Server Error APIError

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"f7876549b57cf","source":{"pointer":"/v3/users"},"title":"Internal Server Error","detail":"INTERNAL_SERVER_ERROR"}]}
```

```
delete /v3/idm-users/{email}
```

Delete user by user email (deleteUsersByEmails)

Deletes the specified user and returns the user details. If a sub-account ID was sent in the "caid" request parameter, the user will be unassigned from the sub-account.

Path parameters

email (required)

Path Parameter

— User's email

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[IdmUsersResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

- `*/*`

Responses

200

Success [IdmUsersResponse](#)

400

Bad Request [String](#)

401

Unauthorized [APIError](#)

Example data

Content-Type: `*/*`

```
{"errors": [{"id": null, "status": 401, "source": {"pointer": "/v3/idm-users/email@imperva.com"}, "title": "Unauthorized"}]}
```

404

Entity not found [APIError](#)

Example data

Content-Type: `*/*`

```
{"errors": [{"status": 404, "id": "f41aff1362ac7fb", "source": {"pointer": "/v3/idm-users/email@imperva.com"}, "title": "The requested item was not found", "detail": "User with email email@imperva.com not found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: `*/*`

```
{"errors": [{"status": 500, "id": "f7876549b57cf", "source": {"pointer": "/v3/users"}, "title": "Internal Server Error", "detail": "INTERNAL_SERVER_ERROR"}]}
```

```
get /v3/idm-users
```

Retrieve the list of users for a given account (getAccountUsers)
 Retrieves the list of users for a given account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`IdmUsersResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

- `*/*`

Responses

200

Success [IdmUsersResponse](#)

400

Bad Request [String](#)

401

Unauthorized [APIError](#)

Example data

Content-Type: `*/*`

```
{"errors": [{"id": null, "status": 401, "source": {"pointer": "/v3/idm-users"}, "title": "Unauthorized"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: `*/*`

```
{"errors": [{"status": 500, "id": "f7876549b57cf", "source": {"pointer": "/v3/idm-users"}, "title": "Internal Server Error", "detail": "INTERNAL_SERVER_ERROR"}]}
```

```
get /v3/users/list
```

Retrieve the list of users for a given account ([getCurrentAccountUsers](#))

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

UsersExternalResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "id" : "00Ya56Yb",
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "id" : "00Ya56Yb",
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK UsersExternalResponse

400

Bad Request String

500

Internal Server Error String

```
get /v3/idm-users/{email}
```

Retrieve user details by user email and account ID (getUserByUserEmail)
 Retrieves user details according to the user's email and account ID.

Path parameters

email (required)

Path Parameter

— User's email

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

IdmUsersResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
  }
]
```

```

        "email" : "userEmail@imperva.com"
    } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json
- */*

Responses

200

Success [IdmUsersResponse](#)

400

Bad Request [String](#)

401

Unauthorized [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"id":null,"status":401,"source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Unauthorized"}]}
```

404

Entity not found [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":404,"id":"74rt5144444f5e","source":{"pointer":"/v3/idm-users/email@imperva.info"},"title":"The requested item was not found","detail":"User with email email@imperva.info does not exist"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"f7a400555hjg57cf","source":{"pointer":"/v3/idm-users/email@imperva.info"},"title":"Internal Server Error","detail":"INTERNAL_SERVER_ERROR"}]}
```

```
patch /v3/idm-users/{email}
```

Update list of roles for a user in a specific account (updateUserRoleAssignments)

Updates the list of roles assigned to a user in a specific account or subaccount. To retrieve the list of available roles, use following API: GET "/user-management/v1/roles"

Path parameters

email (required)

Path Parameter

— User's email

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ExternalRoleAssignmentsDtoNew](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[IdmUsersResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  }, {
    "accountId" : 123456,
    "firstName" : "John",
    "lastName" : "Snow",
    "lastLoginTime" : "2021-06-01T16:00:00.3Z",
    "created" : "2021-06-01T16:00:00.3Z",
    "roles" : [ {
      "id" : 1234,
      "name" : "custom_role_1"
    } ],
    "email" : "userEmail@imperva.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json
- */*

Responses

200

Success [IdmUsersResponse](#)

400

Bad request [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":400,"id":"837640108","source":{"pointer":"/v3/idm-users/user_email@imperva.com"},"title":"Failed role request","detail":"Role with ID 1,2,3,4,5,6 does not exist on account with ID 54132520"}]}
```

401

Unauthorized APIError

Example data

Content-Type: */*

```
{"errors": [{"id":null,"status":401,"source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Unauthorized"}]}
```

500

Internal Server Error APIError

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"f7876549b57cf","source":{"pointer":"/v3/idm-users/email@imperva.com"},"title":"Internal Server Error","detail":"INTERNAL_SERVER_ERROR"}]}
```

Models

Methods

Table of Contents

1. APIError
2. CreateIdmUserDto
3. ExternalRoleAssignmentsDtoBase
4. ExternalRoleAssignmentsDtoNew
5. ExternalUserDto
6. IdmUser
7. IdmUsersResponse
8. Role
9. UsersExternalResponse

APIError

status (optional)
Integer
format: int32
id (optional)
String
code (optional)
String
source (optional)
map[String, Object]
title (optional)
String
detail (optional)
String

CreateIdmUserDto

firstName (optional)
String
example: John
lastName (optional)
String
example: Snow
email (optional)
String
example: userEmail@imperva.com
roleIds (optional)
array[Long]
The roles IDs assigned to user. Roles define the user's permissions. format: int64
example: [1,2,3,4]

ExternalRoleAssignmentsDtoBase

roleIds (optional)
array[Long]
The roles IDs assigned to user. Roles define the user's permissions. format: int64
example: [1,2,3,4]

ExternalRoleAssignmentsDtoNew

roleIds (optional)
array[Long]
The roles IDs assigned to user. Roles define the user's permissions. format: int64
example: [1,2,3,4]

ExternalUserDto

id
String
example: 00Ya56Yb
accountId (optional)
Long
format: int64
example: 123456

firstName (optional)
String
example: John
lastName (optional)
String
example: Snow
email (optional)
String
example: userEmail@imperva.com
roles (optional)
array[Role]
example: [{"id":1234,"name":"custom_role_1"}]
lastLoginTime (optional)
Date
The most recent date when the user logged in to Imperva system. format: date-time
example: 2021-06-01T16:00:00.300Z
created (optional)
Date
The date when the user was created. format: date-time
example: 2021-06-01T16:00:00.300Z

IdmUser

accountId (optional)
Long
format: int64
example: 123456
firstName (optional)
String
example: John
lastName (optional)
String
example: Snow
email (optional)
String
example: userEmail@imperva.com
roles (optional)
array[Role]
example: [{"id":1234,"name":"custom_role_1"}]
lastLoginTime (optional)
Date
The most recent date when the user logged in to Imperva system. format: date-time
example: 2021-06-01T16:00:00.300Z
created (optional)
Date
The date when the user was created. format: date-time
example: 2021-06-01T16:00:00.300Z

IdmUsersResponse

data (optional)
array[IdmUser]

Role

id (optional)

Long

Unique identifier of a role. Roles define the user's permissions. format: int64

name (optional)

String

The role name.

UsersExternalResponse

data (optional)

array[ExternalUserDto]

User Management API

This is an API for Imperva User Management

Version: v1

BasePath:/user-management

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

Methods

Models

Table of Contents

UserAndRoleManagement

- `post /v1/roles`
- `post /v1/users`
- `delete /v1/roles/{roleId}`
- `delete /v1/users`
- `get /v1/abilities/accounts/{accountId}`
- `get /v1/roles/{roleId}`
- `get /v1/roles`
- `get /v1/assignments`
- `get /v1/users`
- `post /v1/assignments`
- `post /v1/roles/{roleId}`

UserAndRoleManagement

```
post /v1/roles
```

Create new role (createRole)

Role management APIs for role management

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `createRole` (required)

Body Parameter

— The details required for creating the role.

Return type

[roleDetails](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 1234567,
  "updateDate" : "2019-03-31 14:10:28",
  "isEditable" : true,
  "accountName" : "Example Account",
  "roleId" : 123,
  "roleName" : "viewOnlyRole",
  "userAssignment" : "[{"userEmail": "example_email@imperva.com", "accountId: 12
3"}]",
  "roleAbilities" : "[canManageApiKey, canPurgeCache]",
  "roleDescription" : "Default user role."
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [roleDetails](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
post /v1/users
```

Create new user (createUser)
User management APIs for user management

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `createUser` (required)
Body Parameter
— The details required to create new user.

Return type

User

Example data

Content-Type: application/json

```
{
  "accountId" : 123456,
  "firstName" : "John",
  "lastName" : "Snow",
  "userEmail" : "userEmail@imperva.com",
  "rolesDetails" : [ {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  }, {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  } ],
  "userId" : 112233
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [User](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
delete /v1/roles/{roleId}
```

Delete role by role ID (deleteRoleByRoleId)
Role management APIs for role management

Path parameters

roleId (required)

Path Parameter

— The role ID of the required role. format: int64

Return type

[ApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
  "debug_info" : "{}",  
  "code" : 200,  
  "message" : "OK"
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [ApiSuccessResponse](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
delete /v1/users
```

Delete user by user email (`deleteUserByUserEmail`)
User management APIs for user management

Query parameters

accountId (required)

Query Parameter

— Unique ID of the required account format: int64

userEmail (required)

Query Parameter

— The email of the required user

Return type

[ApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "debug_info" : "{}",
  "code" : 200,
  "message" : "OK"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [ApiSuccessResponse](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
get /v1/abilities/accounts/{accountId}
```

Get account abilities by account ID, according to account type (getAllAvailableAccountAbilitiesByAccountId)
Role management APIs for abilities management

Path parameters

accountId (required)

Path Parameter

— Unique ID of the required account. format: int64

Return type

array[ability]

Example data

Content-Type: application/json

```
[ {
  "abilityDisplayName" : "View sites",
  "isRelevantForSubAccount" : true,
  "abilityKey" : "canViewSite"
}, {
  "abilityDisplayName" : "View sites",
  "isRelevantForSubAccount" : true,
  "abilityKey" : "canViewSite"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
get /v1/roles/{roleId}
```

Get role details by role ID (getRoleDetailsByRoleId)

Retrieve details of roles in the account according to the role ID. Note: If the API key/ID used for authentication are for a subaccount user, results include only users assigned to that specific subaccount.

Path parameters

roleId (required)
Path Parameter

— The role ID of the required role. format: int64

Return type

[roleDetails](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 1234567,
  "updateDate" : "2019-03-31 14:10:28",
  "isEditable" : true,
  "accountName" : "Example Account",
  "roleId" : 123,
  "roleName" : "viewOnlyRole",
  "userAssignment" : "[{"userEmail": "example_email@imperva.com", "accountId": 123"}]",
  "roleAbilities" : "[canManageApiKey, canPurgeCache]",
  "roleDescription" : "Default user role."
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [roleDetails](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
get /v1/roles
```

Get role details by account ID, user email, or role name (getRolesDetails)

Retrieve details of roles in the account. Note: If the API key/ID used for authentication are for a subaccount user, results include only users assigned to that specific subaccount.

Query parameters

accountId (required)

Query Parameter

— Unique ID of the required account format: int64

roleName (optional)

Query Parameter

— The name of the required role

userEmail (optional)

Query Parameter

— The email of the required user

Return type

array[roleDetails]

Example data

Content-Type: application/json

```
[ {
  "accountId" : 1234567,
  "updateDate" : "2019-03-31 14:10:28",
  "isEditable" : true,
  "accountName" : "Example Account",
  "roleId" : 123,
  "roleName" : "viewOnlyRole",
  "userAssignment" : "[{"userEmail": "example_email@imperva.com", "accountId: 123"}]",
  "roleAbilities" : "[canManageApiKey, canPurgeCache]",
  "roleDescription" : "Default user role."
}, {
  "accountId" : 1234567,
  "updateDate" : "2019-03-31 14:10:28",
  "isEditable" : true,
  "accountName" : "Example Account",
  "roleId" : 123,
  "roleName" : "viewOnlyRole",
  "userAssignment" : "[{"userEmail": "example_email@imperva.com", "accountId: 123"}]",
  "roleAbilities" : "[canManageApiKey, canPurgeCache]",
  "roleDescription" : "Default user role."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
get /v1/assignments
```

Get role assignments by user email and account ID (`getUserAssignmentByUserEmail`)
Role management APIs for roles assignment

Query parameters

`accountId` (required)

Query Parameter

— Unique ID of the required account format: int64

`userEmail` (required)

Query Parameter

— The email of the required user

Return type

[User](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 123456,
  "firstName" : "John",
  "lastName" : "Snow",
  "userEmail" : "userEmail@imperva.com",
  "rolesDetails" : [ {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  }, {
    "roleId" : 29,
```

```

    "roleName" : "viewOnlyRole"
} ],
"userId" : 112233
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [User](#)

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

[Internal server error ErrorApiDto](#)

```
get /v1/users
```

Get user details by user email and account ID ([getUserByEmail](#))
 User management APIs for user management

Query parameters

accountId (required)

Query Parameter

— Unique ID of the required account format: int64

userEmail (required)

Query Parameter

— The email of the required user

Return type

[User](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 123456,
  "firstName" : "John",
  "lastName" : "Snow",
  "userEmail" : "userEmail@imperva.com",
  "rolesDetails" : [ {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  }, {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  } ],
  "userId" : 112233
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response User

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

[Internal server error ErrorApiDto](#)

```
post /v1/assignments
```

Assign users to roles or delete existing assignment (updateAssignments)
Role management APIs for roles assignment

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `requestedAssignment` (required)

Body Parameter

— The details required for the new assignments.

Return type

`array[User]`

Example data

Content-Type: application/json

```
[ {
  "accountId" : 123456,
  "firstName" : "John",
  "lastName" : "Snow",
  "userEmail" : "userEmail@imperva.com",
  "rolesDetails" : [ {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  }, {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  } ],
  "userId" : 112233
}, {
  "accountId" : 123456,
  "firstName" : "John",
  "lastName" : "Snow",
  "userEmail" : "userEmail@imperva.com",
  "rolesDetails" : [ {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  }, {
    "roleId" : 29,
    "roleName" : "viewOnlyRole"
  } ],
  "userId" : 112233
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

Legal response

400

Invalid Input [ErrorApiDto](#)

401

Unauthorized [ErrorApiDto](#)

500

Internal server error [ErrorApiDto](#)

```
post /v1/roles/{roleId}
```

Update role details by role ID (updateRole)
Role management APIs for role management

Path parameters

roleId (required)

Path Parameter

— The role ID of the required role. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body updateRole (required)

Body Parameter

— The details required for updating the role.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID

format: int64

Return type

roleDetails

Example data

Content-Type: application/json

```
{  
    "accountId" : 1234567,  
    "updateDate" : "2019-03-31 14:10:28",  
    "isEditable" : true,  
    "accountName" : "Example Account",  
    "roleId" : 123,  
    "roleName" : "viewOnlyRole",  
    "userAssignment" : "[{"userEmail": "example_email@imperva.com", "accountId: 12  
3"}]",  
    "roleAbilities" : "[canManageApiKey, canPurgeCache]",  
    "roleDescription" : "Default user role."  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response roleDetails

400

Invalid Input ErrorApiDto

401

Unauthorized ErrorApiDto

500

Internal server error ErrorApiDto

Models

Methods

Table of Contents

1. `ApiSuccessResponse`
2. `ErrorApiDto`
3. `User`
4. `UserAssignment`
5. `ability`
6. `createRole`
7. `createUser`
8. `requestedAssignment`
9. `roleDetails`
10. `roleShortDetails`
11. `updateRole`

ApiSuccessResponse

Basic API success response
code (optional)

`Long`

Internal response code format: int64

example: 200

`debug_info` (optional)

`map[String, BigDecimal]`

Debug information

example: {}

`message` (optional)

`String`

Response message

example: OK

ErrorApiDto

`description`

`String`

`errorCode`

`Long`

format: int64

User

User Details

`accountId` (optional)

`Long`

ID of the account that was acted on. format: int64

example: 123456

`firstName` (optional)

`String`

The first name of the user.

example: John

lastName (optional)

String

The last name of the user.

example: Snow

rolesDetails

array[roleShortDetails]

userEmail (optional)

String

The email address of the user.

example: userEmail@imperva.com

userId (optional)

Long

The ID of the user that the action was done in. format: int64

example: 112233

UserAssignment

User Assignment Details

accountId (optional)

Long

The account id of user. format: int64

example: 123

userEmail (optional)

String

The email of user assigned to the role.

example: example_email@imperva.com

ability

Ability fields

abilityDisplayName (optional)

String

The name as displayed in the UI.

example: View sites

abilityKey (optional)

String

The internal name of the ability.

example: canViewSite

isRelevantForSubAccount (optional)

Boolean

When true, the ability can apply to roles used in both parent accounts and sub accounts. When false, the ability has no impact when assigned to a user in a sub account.

example: true

createRole

Create role allowed fields

accountId (optional)

Long

ID of the account that was acted on. format: int64

example: 1234567

roleAbilities (optional)

array[String]

The abilities keys that the role contains.

example: {canManageApiKey, canPurgeCache}

roleDescription (optional)

String

Description of the role.

example: Default user role.

roleName (optional)

String

The role name.

example: viewOnlyRole

createUser

Create User Required Details

accountId (optional)

Long

ID of the account that was acted on. format: int64

example: 123456

firstName (optional)

String

The first name of the user that was acted on. It is relevant for the parent account only , but not for subaccounts

example: John

lastName (optional)

String

The last name of the user that was acted on. It is relevant for the parent account only , but not for subaccounts

example: Snow

roleIds (optional)

array[Long]

List of role IDs to add to the user. Use roleIds or roleNames to add roles to the user, but not both. format: int64

example: [11,13]

roleNames (optional)

array[String]

List of role names to add to the user. Use roleIds or roleNames to add roles to the user, but not both

example: [viewOnlyRole]

userEmail (optional)

String

The email address of the user.

example: userEmail@imperva.com

requestedAssignment

Role Assignment Data

accountId (optional)

Long

ID of the account that was acted on. format: int64

example: 123456

roleIds (optional)

array[Long]

The list of role IDs to add for the user. format: int64

example: [11,13]

userEmail (optional)

String

The email of the user that was acted on.

example: email@imperva.com

roleDetails

role details

accountId (optional)

Long

ID of the account that was acted on. format: int64

example: 1234567

accountName (optional)

String

The name of the account that was acted on.

example: Example Account

isEditable (optional)

Boolean

Whether or not the role can be modified.

example: true

roleAbilities (optional)

array[ability]

The abilities that the role contains.

example: [canManageApiKey, canPurgeCache]

roleDescription (optional)

String

Description of the role.

example: Default user role.

roleId (optional)

Long

ID of the role that was acted on. format: int64

example: 123

roleName (optional)

String

The name of the role that was acted on.

example: viewOnlyRole

updateDate (optional)

String

The last update date of this role.

example: 2019-03-31 14:10:28

userAssignment (optional)

array[UserAssignment]

The emails and account ids of users assigned to the role.

example: [{"userEmail": "example_email@imperva.com", "accountId: 123"}]

roleShortDetails

Role Short Details

roleId (optional)

Long

The role ID. format: int64

example: 29

roleName (optional)

String

The role name.

example: viewOnlyRole

updateRole

Update role allowed fields

roleAbilities (optional)

array[String]

The abilities keys that the role contains.
example: {canManageApiKey, canPurgeCache}
roleDescription (optional)

String
The description of the role that was acted on.
example: Default user role.

roleName (optional)
String
The name of the role that was acted on.
example: viewOnlyRole

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountManagement

- `post /api/prov/v1/accounts/add`
- `post /api/prov/v1/subaccounts/add`
- `post /api/prov/v1/accounts/delete`
- `post /api/prov/v1/subaccounts/delete`
- `post /api/prov/v1/account`
- `post /api/prov/v1/accounts/data-privacy/show`
- `post /api/prov/v1/accounts/gettoken`
- `post /api/prov/v1/accounts/list`
- `post /api/prov/v1/accounts/listSubAccounts`
- `post /api/prov/v1/accounts/configure`
- `post /api/prov/v1/accounts/setlog`
- `post /api/prov/v1/accounts/data-privacy/set-region-default`
- `post /api/prov/v1/accounts/subscription`

Account Management

```
post /api/prov/v1/accounts/add
```

Add a new managed account (addAccount)

Available for Reseller accounts only

Use this operation to add a new account that should be managed by the account of the API client (the parent account). The new account will be configured according to the preferences set for the parent account by Imperva. Depending on these preferences, an activation e-mail will be sent to the specified e-mail address. The user responds to the activation e-mail, selects a password, and can then log directly into the Imperva console. The same e-mail address can also be used to send system notifications to the account. The new account is identified by a numeric value as provided by Imperva in the response in the field account_id.

Query parameters

email (required)

Query Parameter

— Email address. For example: "joe@example.com".

parent_id (optional)

Query Parameter

— The newly created account's parent id. If not specified, the invoking account will be assigned as the parent.
format: int64

name (optional)

Query Parameter

— The account owner's name. For example: "John Doe".

plan_id (optional)

Query Parameter

— An identifier of the plan to assign to the new account. For example, ent100 for the Enterprise 100

plan.
Example values:
ent100 | ent50 | ent20

ref_id (optional)

Query Parameter

— Customer specific identifier for this operation.

account_name (optional)

Query Parameter

— Account name.

account_description (optional)

Query Parameter

— The account description

user_name (optional)

Query Parameter

— The account owner's name. For example: "John Doe".

log_level (optional)

Query Parameter

— Sets the log reporting level for the site.
Possible values: full | security | none | default
Default value is none
Available only for customers that purchased the Logs Integration SKU.

logs_account_id (optional)

Query Parameter

— Numeric identifier of the account that purchased the logs integration SKU and which collects the logs.
If not specified, operation will be performed on the account identified by the authentication parameters. Available only for customers that purchased the Logs Integration SKU.

Return type

inline_response_200

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1003 - Plan ID invalid
1001 - Email invalid
1010 - Account exists
9403 - Unknown/unauthorized account_id [inline_response_200](#)

Example data

Content-Type: success

```
{"account": {"email": "example@imperva.com", "plan_id": "ent100", "plan_name": "Enterprise 100", "trial_end_date": "Jan 01, 2023 01:00:00 AM", "account_id": 1234, "parent_id": 123, "ref_id": "222", "user_name": "Example Account", "account_name": "Example Account", "logins": [], "support_level": "Standard", "support_all_tls_versions": false, "allow_ssl_validation_delegation": false, "wildcard_san_for_new_sites": "Default", "naked_domain_san_for_new_www_sites": true, "enable_http2_for_new_sites": true, "enable_https2_to_origin_for_new_sites": false}, "email": "example@email.info", "plan_id": "ent100", "plan_name": "Enterprise 100", "account_type": "Reseller Example", "account_id": 1234, "parent_id": 123, "user_name": "Example Account", "account_name": "Example Account", "ref_id": "222", "logins": [], "support_level": "Standard", "support_all_tls_versions": false, "wildcard_san_for_new_sites": "Default", "naked_domain_san_for_new_www_sites": true, "res": 0, "res_message": "OK", "debug_info": {"id-info": "999999"}}
```

Example data

Content-Type: error

```
{"res": 1010, "res_message": "Account exists", "debug_info": {"account_id": 12345, "id-info": "999999"}}
```

```
post /api/prov/v1/subaccounts/add
```

Add a new sub account (addSubAccount)

Use this operation to add a new sub account to be managed by the account of the API client (the parent account).

Query parameters

sub_account_name (required)

Query Parameter

— The name of the sub account.

parent_id (optional)

Query Parameter

— The newly created account's parent id. If not specified, the invoking account will be assigned as the parent account. format: int64

ref_id (optional)

Query Parameter

— Customer specific identifier for this operation.

log_level (optional)

Query Parameter

— Sets the log reporting level for the site.
Possible values: full, security, none, default
Available only for customers that purchased the Logs Integration SKU.

logs_account_id (optional)

Query Parameter

— Numeric identifier of the account that purchased the logs integration SKU and which collects the logs.
If not specified, operation will be performed on the account identified by the authentication parameters.
Available only for customers that purchased the Logs Integration SKU.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9403 - Unknown/unauthorized account_id
9415 - Operation not allowed
1015 - Maximum number of SubAccounts reached
1003 - Plan ID invalid
1010 - Account exists

```
post /api/prov/v1/accounts/delete
```

Delete managed account (deleteAccount)

Available for Reseller accounts only Use this operation to delete an account.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 1 - Unexpected error
 2 - Invalid input
 9415 - Operation not allowed
 ApiResult

```
post /api/prov/v1/subaccounts/delete
```

Delete sub account (deleteSubAccount)

Use this operation to delete a sub account.

Query parameters

sub_account_id (required)

Query Parameter

— Numeric identifier of the sub account to operate on. format: int64

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 1 - Unexpected error
 2002 - Invalid input
 2001 - Object is not empty
 9415 - Operation not allowed [ApiResult](#)

```
post /api/prov/v1/account
```

Get account status (getAccountStatus)
 Use this operation to get account status

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
 If not specified, operation will be performed on the account identified by the authentication parameters.

Return type

[ApiResultAccountStatus](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "account" : {
    "support_all_tls_versions" : true,
    "domains_for_ssl_validation_delegation" : [ "domains_for_ssl_validation_delegation", "domains_for_ssl_validation_delegation" ],
    "naked_domain_san_for_new_www_sites" : true,
    "enable_http2_for_new_sites" : true,
    "user_name" : "Jhon",
    "cname_value_for_ssl_validation_delegation" : "abc.impervadns.net",
    "log_level" : "full",
    "John Account" : "Jhon",
    "trial_end_date" : "2000-01-23T04:56:07.000+00:00",
    "support_level" : "Standard",
    "plan_name" : "Enterprise 100",
    "account_id" : 10,
    "allow_ssl_validation_delegation" : true,
    "parent_id" : 123,
    "wildcard_san_for_new_sites" : "TRUE",
    "enable_http2_to_origin_for_new_sites" : true,
    "logins" : [ {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    }, {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    } ],
    "email" : "example@imperva.com",
    "plan_id" : "ent100"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success ApiResultAccountStatus

```
post /api/prov/v1/accounts/data-privacy/show
```

Get default data storage region (getDefaultRegion)

Use this operation to get the default data region of the account. (Available for Reseller accounts only)

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

res - contains the specific error code:
9403 - Unknown/unauthorized account id
9414 - Feature not permitted
9415 - User is not allowed to change region
1- Unexpected error [ApiResult](#)

```
post /api/prov/v1/accounts/gettoken
```

Get account login token (getToken)

Tokens are used instead of user/password based authentication to log in to the Imperva Cloud Security Console. Use this operation to generate a token for an account. The token is valid for 15 minutes.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

partner_id (optional)

Query Parameter

— Numeric identifier of the parent id to operate on

Return type

[ApiResultGetSsoToken](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "generated_token" : "344ebcaf34dff34"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [ApiResultGetSsoToken](#)

```
post /api/prov/v1/accounts/list
```

List managed accounts (listAccounts)

Available for Reseller accounts only.

Use this operation to get the list of accounts that are managed by account of the API client (the parent account).

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

page_size (optional)**Query Parameter**

— The number of objects to return in the response.
Default: 50
Maximum: 100

page_num (optional)**Query Parameter**

— The page to return starting from 0. Default: '0

Return type

`ApiResultListUsers`

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "accounts" : [ {
    "support_all_tls_versions" : true,
    "domains_for_ssl_validation_delegation" : [ "domains_for_ssl_validation_delegation", "domains_for_ssl_validation_delegation" ],
    "naked_domain_san_for_new_www_sites" : true,
    "enable_http2_for_new_sites" : true,
    "user_name" : "Jhon",
    "cname_value_for_ssl_validation_delegation" : "abc.impervadns.net",
    "log_level" : "full",
    "John Account" : "Jhon",
    "trial_end_date" : "2000-01-23T04:56:07.000+00:00",
    "support_level" : "Standard",
    "plan_name" : "Enterprise 100",
    "account_id" : 10,
    "allow_ssl_validation_delegation" : true,
    "parent_id" : 123,
    "wildcard_san_for_new_sites" : "TRUE",
    "enable_http2_to_origin_for_new_sites" : true,
    "logins" : [ {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    }, {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    } ],
    "email" : "example@imperva.com",
    "plan_id" : "ent100"
  }, {
    "support_all_tls_versions" : true,
    "domains_for_ssl_validation_delegation" : [ "domains_for_ssl_validation_delegation", "domains_for_ssl_validation_delegation" ],
    "naked_domain_san_for_new_www_sites" : true,
    "enable_http2_for_new_sites" : true,
    "user_name" : "John",
    "cname_value_for_ssl_validation_delegation" : "abc.impervadns.net",
    "log_level" : "full",
    "John Account" : "John",
    "trial_end_date" : "2000-01-23T04:56:07.000+00:00",
    "support_level" : "Standard",
    "plan_name" : "Enterprise 100",
    "account_id" : 11,
    "allow_ssl_validation_delegation" : true,
    "parent_id" : 124,
    "wildcard_san_for_new_sites" : "TRUE",
    "enable_http2_to_origin_for_new_sites" : true,
    "logins" : [ {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    }, {
      "login_id" : "demo_account@incapsula.com",
      "email_verified" : true
    } ],
    "email" : "example@imperva.com",
    "plan_id" : "ent100"
  } ]
}
```

```

"naked_domain_san_for_new_www_sites" : true,
"enable_http2_for_new_sites" : true,
"user_name" : "Jhon",
"cname_value_for_ssl_validation_delegation" : "abc.impervadns.net",
"log_level" : "full",
"John Account" : "Jhon",
"trial_end_date" : "2000-01-23T04:56:07.000+00:00",
"support_level" : "Standard",
"plan_name" : "Enterprise 100",
"account_id" : 10,
"allow_ssl_validation_delegation" : true,
"parent_id" : 123,
"wildcard_san_for_new_sites" : "TRUE",
"enable_http2_to_origin_for_new_sites" : true,
"logins" : [ {
    "login_id" : "demo_account@incapsula.com",
    "email_verified" : true
}, {
    "login_id" : "demo_account@incapsula.com",
    "email_verified" : true
} ],
"email" : "example@imperva.com",
"plan_id" : "ent100"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success ApiResultListUsers

```
post /api/prov/v1/accounts/listSubAccounts
```

List account's sub accounts (listSubAccounts)

Use this operation to get a list of sub accounts that are managed by the account of the API client (the parent account).

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

page_size (optional)

Query Parameter

-
- The number of objects to return in the response.
Default: 50
Maximum: 100
page_num (optional)
Query Parameter
— The page to return starting from 0. Default: 0

Return type

array[SubAccountStatus]

Example data

Content-Type: application/json

```
[ {
    "ref_id" : "432",
    "logs_account_id" : 15,
    "sub_account_name" : "My Sub Account",
    "parent_id" : 10,
    "log_level" : "full",
    "support_level" : "Standard",
    "sub_account_id" : 10,
    "logins" : [ {
        "login_id" : "demo_account@incapsula.com",
        "email_verified" : true
    }, {
        "login_id" : "demo_account@incapsula.com",
        "email_verified" : true
    } ]
}, {
    "ref_id" : "432",
    "logs_account_id" : 15,
    "sub_account_name" : "My Sub Account",
    "parent_id" : 10,
    "log_level" : "full",
    "support_level" : "Standard",
    "sub_account_id" : 10,
    "logins" : [ {
        "login_id" : "demo_account@incapsula.com",
        "email_verified" : true
    }, {
        "login_id" : "demo_account@incapsula.com",
        "email_verified" : true
    } ]
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9415 - Operation not allowed
1002 - Account doesn't exist

```
post /api/prov/v1/accounts/configure
```

Modify account configuration (modifyAccountConfiguration)

Use this operation to change the configuration of the account of the API client or one of its managed accounts.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body string (optional)

Body Parameter

Query parameters

param (required)

Query Parameter

— Name of configuration parameter to set.
Possible values for param and value parameters:
name the updated name.email the updated e-mail addressplan_id a plan iderror_page_template a Base64 encoded template for an error page.support_all_tls_versions Use this operation to allow sites in the account to support all TLS versions for connectivity between clients (visitors) and the Imperva service. When this option is set, you can then enable the option per site to support all TLS versions. Possible values: true, false. Note: To remain PCI-compliant, do not enable this option.naked_domain_san_for_new_www_sites Use this option to determine if the naked domain SAN will be added to the SSL certificate for new www sites. Default value: true.wildcard_san_for_new_sites Use this option to determine if the wildcard SAN or the full domain SAN is added to the Imperva SSL certificate for new sites. Possible values: true, false, default (determined by plan) Default value: default.ref_id Sets the Reference ID, a free-text field that enables you to add a unique identifier to correlate an object in our service, such as a protected website, with an object on the customer side.enable_http2_for_new_sites Use this option to enable HTTP/2 for newly created SSL sites.enable_http2_to_origin_for_new_sites Use this option to enable HTTP/2 to Origin for newly created SSL sites. This option can only be enabled once HTTP/2 is enabled for newly created sites.consent_required Blocks Imperva from performing sensitive operations on your behalf. You can then activate consent via the Cloud Security Console UI. Possible values: true, false..inactivity_timeout Account inactivity timeout in millis. Possible values: 900000,1800000,3600000,5400000,7200000.

value (required)

Query Parameter

— According to the configuration parameter used.

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 6001 - Invalid configuration parameter name
 6002 - Invalid configuration parameter value
 6003 - Action required
 6004 - Invalid inactivity timeout value
 2 - Invalid input
 9415 - Operation not allowed
 1 - Unexpected error [inline_response_200](#)

Example data

Content-Type: success

```
{"res":0,"res_message":"OK","debug_info":{"enable_http2_for_new_sites":"false","id-info":"999999"}}
```

Example data

Content-Type: error

```
{"res":6001,"res_message":"Invalid configuration parameter name","debug_info":{"param":"param_not_exist","id-info":"999999"}}
```

```
post /api/prov/v1/accounts/setlog
```

Modify account log level (modifyAccountLogLevel)

Available for Reseller accounts only

Use this operation to change the account log configuration.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
 If not specified, operation will be performed on the account identified by the authentication parameters.

log_level (required)

Query Parameter

— Sets the log reporting level for the site.
Possible values: full | security | none | default
Available only for customers that purchased the Log Integration SKU.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
6001 - Invalid configuration parameter name
1003 - Plan ID invalid
9415 - Operation not allowed
ApiResult

```
post /api/prov/v1/accounts/data-privacy/set-region-default
```

Set default data storage region (setDefaultRegion)

Use this operation to set the default data region of the account for newly created sites. (Available for Reseller accounts only)

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

data_storage_region (optional)

Query Parameter

— The data region to use.
Possible values: US | EU | APAC | AU

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

res - contains the specific error code:
9403 - Unknown/unauthorized account id
9414 - Feature not permitted
1- Unexpected error
2 - Invalid region. [ApiResult](#)

```
post /api/prov/v1/accounts/subscription
```

Get account subscription details (subscription)

Use this operation to get subscription details for an account.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[Success inline_response_200_2](#)

Models

Methods

Table of Contents

1. AccountBandwidth
2. AccountPlanStatus
3. AccountPlanStatus_websiteProtection
4. ApiResult
5. ApiResultAccountStatus
6. ApiResultAccountSubscription
7. ApiResultGetSsoToken
8. ApiResultListUsers
9. ApiResultSubAccountStatus
10. Login
11. PlanSectionRow
12. SubAccountStatus
13. account
14. accounts
15. inline_response_200
16. inline_response_200_1
17. inline_response_200_2

AccountBandwidth

billingCycle (optional)

String

example: Earlier billing cycle

onDemandBandwidth (optional)

String

example: 0bps

alwaysOnBandwidth (optional)

String

example: 7.7kbps

AccountPlanStatus

accountId (optional)

Long

format: int64

example: 12345

accountName (optional)

String

example: demo_account@incapsula.com

websiteProtection (optional)

array[AccountPlanStatus_websiteProtection]

example: {"name": "Website Protection", "planSectionRows": [{"name": "Additional Sites", "purchased": "100", "used": "2"}, {"name": "Load Balancing (old)", "purchased": "0", "used": "0"}, {"name": "Additional Login Protect Users", "purchased": "5", "used": "0"}]}

infrastructureProtection (optional)

array[AccountPlanStatus_websiteProtection]

example: {"name": "Infrastructure Protection", "planSectionRows": [{"name": "On Demand Bandwidth (Clean traffic)", "purchased": "0", "used": ""}, {"name": "GRE Tunnel Pairs", "purchased": "0", "used": "0"}]}

dnsProtection (optional)

array[AccountPlanStatus_websiteProtection]

example: {"name": "DNS Protection", "planSectionRows": [{"name": "Additional DNS Zones", "purchased": "0", "used": "0"}]}

additionalServices (optional)

array[AccountPlanStatus_websiteProtection]

example: {"name": "Additional Services", "planSectionRows": [{"name": "Always On Bandwidth (Clean traffic)", "purchased": "10Mbps", "used": "N/A"}, {"name": "DDoS Protection", "purchased": "None", "used": ""}, {"name": "Support Level", "purchased": "Standard", "used": "Standard"}, {"name": "WAF SIEM Integration", "purchased": "10", "used": "0"}, {"name": "Web Attack Analytics", "purchased": "0", "used": ""}]}

AccountPlanStatus_websiteProtection

name (optional)

String

planSectionRows (optional)

array[PlanSectionRow]

ApiResult

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK
debug_info (optional)
array[map[String, Object]]

ApiResultAccountStatus

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
account (optional)
account

ApiResultAccountSubscription

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
planStatus (optional)
AccountPlanStatus
bandwidthHistory (optional)
array[AccountBandwidth]

ApiResultGetSsoToken

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
generated_token (optional)
String
example: 344ebcaf34dff34

ApiResultListUsers

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)

String
example: OK
debug_info (optional)
array[map[String, Object]]
accounts (optional)
array[accounts]

ApiResultSubAccountStatus

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
sub_account (optional)
SubAccountStatus

Login

login_id (optional)
String
example: demo_account@incapsula.com
email_verified (optional)
Boolean
example: true

PlanSectionRow

name (optional)
String
purchased (optional)
String
used (optional)
String

SubAccountStatus

sub_account_id (optional)
Long
format: int64
example: 10
sub_account_name (optional)
String
example: My Sub Account
ref_id (optional)
String
example: 432
logins (optional)
array[Login]
log_level (optional)
String
example: full

support_level (optional)

String

example: Standard

parent_id (optional)

Long

format: int64

example: 10

logs_account_id (optional)

Long

format: int64

example: 15

account

email (optional)

String

example: example@imperva.com

plan_id (optional)

String

example: ent100

plan_name (optional)

String

example: Enterprise 100

trial_end_date (optional)

Date

format: date-time

account_id (optional)

Long

format: int64

example: 10

parent_id (optional)

Long

format: int64

example: 123

John Account (optional)

String

example: Jhon

user_name (optional)

String

example: Jhon

logins (optional)

array[Login]

log_level (optional)

String

example: full

support_level (optional)

String

example: Standard

support_all_tls_versions (optional)

Boolean

example: true

allow_ssl_validation_delegation (optional)

Boolean

example: true

domains_for_ssl_validation_delegation (optional)

array[String]

cname_value_for_ssl_validation_delegation (optional)

String

example: abc.impervadns.net
wildcard_san_for_new_sites (optional)
String
Enum:
True
False
Default
example: TRUE
naked_domain_san_for_new_www_sites (optional)
Boolean
example: true
enable_http2_for_new_sites (optional)
Boolean
example: true
enable_http2_to_origin_for_new_sites (optional)
Boolean
example: true

accounts

email (optional)
String
example: example@imperva.com
plan_id (optional)
String
example: ent100
plan_name (optional)
String
example: Enterprise 100
trial_end_date (optional)
Date
format: date-time
account_id (optional)
Long
format: int64
example: 10
parent_id (optional)
Long
format: int64
example: 123
John Account (optional)
String
example: Jhon
user_name (optional)
String
example: Jhon
logins (optional)
array[Login]
log_level (optional)
String
example: full
support_level (optional)
String
example: Standard
support_all_tls_versions (optional)
Boolean
example: true
allow_ssl_validation_delegation (optional)

```

Boolean
example: true
domains_for_ssl_validation_delegation (optional)
array[String]
cname_value_for_ssl_validation_delegation (optional)
String
example: abc.impervadns.net
wildcard_san_for_new_sites (optional)
String
Enum:
True
False
Default
example: TRUE
naked_domain_san_for_new_www_sites (optional)
Boolean
example: true
enable_http2_for_new_sites (optional)
Boolean
example: true
enable_http2_to_origin_for_new_sites (optional)
Boolean
example: true

```

`inline_response_200`

`inline_response_200_1`

`inline_response_200_2`

Export Account Configuration

Export your account configuration for the Imperva application security products to facilitate quick and easy onboarding to Terraform.

This can be especially beneficial when your Imperva account is already extensively configured to meet your organization's needs.

The Account Export API exports your configuration from the Imperva platform to a zip file in standard Terraform format.

You can then import the configuration to Terraform and continue to manage and configure your Imperva account using our Terraform provider.

Permissions:

- The **Export configurations** permission is required for exporting your account configuration. This permission is granted to the account admin user by default. The account admin or any user with **Manage users / Manage user roles** permissions can assign this permission to other account users as needed.
- You can only export configurations for which you have access permissions. For example, if you have the **Export configurations** permission but do not have the **View policy** permission, the policy configuration files will not be exported.

Export from Imperva

You can export your configuration at the **account**, **subaccount**, **website**, or **policy** level using the Imperva Account Export API.

The export process includes the following steps:

1. Send an **export request** to initiate the export process. The API response body contains a code for downloading the export file.
2. Send a **download request**, using the code received in the previous response. The code is used to identify the current export process. It can also be used to check the status and retrieve the process results.

The downloaded zip file contains each configuration in a separate file. For example, if you export at the account level, the zip will include separate files for each subaccount, website, and policy.

Note: In the event that downloading the export files fails with an error code 500, it may indicate that the export scope of your account is larger than the API can handle. Try exporting a smaller scope, such as a subaccount, website, or policy.

How to export your account configuration: For instructions on using the Account Export API, see [Account Export API Definition](#). The definition file presents a full, formatted, and interactive version of the APIs that you can use to learn about the APIs, or test them using your API ID and key. You can also download the definition file.

Import to Terraform

You can import the configuration files to Terraform using the import command in the corresponding Imperva resources:

- account resource
- subaccount resource
- website resource
- policy resource

The downloaded zip export file contains an executable file named **import_commands.sh**. Use this file to run the Terraform import command for all exported resources. The result is a Terraform state with the complete existing configuration.

The zip file also contains the **tfvar** file, where you must enter your Imperva API ID and API Key in order to run the Terraform commands.

For more details on the exported resources, see the [Imperva Terraform Provider](#) in the Terraform registry.

Account-Export API

Export account configuration settings from the Imperva platform to a zip file in standard Terraform format. For the full feature documentation, see [Export Account Configuration](#).

Version: 1.0.0

BasePath:/account-export-import

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountConfigurationExport

- `get /v3/export/download/{handler}`
- `post /v3/export`
- `post /v3/export/{resourceType}/{id}`

AccountConfigurationExport

```
get /v3/export/download/{handler}
```

Download the exported zip file after successful export (`downloadAsync`)

This API is used to download the exported zip file after export is complete.

While the export process is in progress the response status will be 202. Once the export process has finished successfully, the response status will be 200 and the file will be served.

Path parameters

`handler` (required)

Path Parameter

— The handler received in the export response. The handler identifies the export process and is used to check the status and retrieve the process zip file when it is ready.

Request headers

Query parameters

`caid` (required)

Query Parameter

— The account to work on. format: int64

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation

202

Export is in progress [AsyncResponse](#)

Example data

Content-Type: */*

```
{handler=1234-abcd-5678-efgh-12qw45rt67ty, status=Export is in progress}
```

404

Resource Not Found [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":404,"id":"20014b504cb97819","source":{"pointer":"/export/download/1234-abcd-5678-efgh-12qw45rt67ty"},"title":"Resource Not Found","detail":"Resource Not Found"}]}
```

500

Something went wrong. Contact support [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"20014b504cb97819","source":{"pointer":"/export/download/1234-abcd-5678-efgh-12qw45rt67ty"},"title":"Internal Server Error","detail":"Something went wrong. Contact support"}]}
```

```
post /v3/export
```

Initiate the export process (exportAsync)

This API initiates the export process for an account (parent or sub account). The process is asynchronous. The response body contains the handler parameter, that is used to identify the current export process. Send this handler in the download request. It can also be used to check the status and retrieve the process results.

Request headers

Query parameters

caid (required)

Query Parameter

— The account ID to work on format: int64

Return type

AsyncResponse

Example data

Content-Type: application/json

```
{
  "handler" : "",
  "status" : ""
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

202

Export is in progress AsyncResponse

Example data

Content-Type: */*

```
{"handler": "1234-abcd-5678-efgh-12qw45rt67ty", "status": "Export is in progress"}
```

401

Authentication missing or invalid [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status": 500, "id": "20014b504cb97819", "source": {"pointer": "/export"}, "title": "Authentication Error", "detail": "Authentication missing or invalid"}]}
```

403

This resource, or one of its associated resources, is currently at work. Please try again later [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status": 403, "id": "20014b504cb97819", "source": {"pointer": "/export"}, "title": "Operation Forbidden", "detail": "This resource, or one of its associated resources, is currently at work. Please try again later"}]}
```

500

Something went wrong. Contact support [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status": 500, "id": "20014b504cb97819", "source": {"pointer": "/export"}, "title": "Internal Server Error", "detail": "Something went wrong. Contact support"}]}
```

```
post /v3/export/{resourceType}/{id}
```

Initiate the export process for a single resource: site or policy. (exportRootResource)
This API initiates the export process for a single resource: site or policy. The process is asynchronous. The

response body contains a code, located in the handler parameter, that is used to identify the current export process. Send this code in the download request. It can also be used to check the status and retrieve the process results.

Path parameters

resourceType (required)

Path Parameter

— The resource type to be exported: SITE or POLICY

id (required)

Path Parameter

— The Imperva ID of the website or policy format: int64

Request headers

Query parameters

caid (required)

Query Parameter

— The account to work on format: int64

exportAsV3 (optional)

Query Parameter

— Indicates whether to export the site resource in v3 format. If true, the export will always use v3 format even if the site's current version is v1. This flag applies only when the resourceType is site. default: false

Return type

AsyncResponse

Example data

Content-Type: application/json

```
{
  "handler" : "",
  "status" : ""
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

202

Export is in progress AsyncResponse

Example data

Content-Type: */*

```
{handler=1234-abcd-5678-efgh-12qw45rt67ty, status=Export is in progress}
```

401

Authentication missing or invalid [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"20014b504cb97819","source":{"pointer":"/export/SITE/1234"},"title":"Authentication Error","detail":"Authentication missing or invalid"}]}
```

403

This resource, or one of its associated resources, is currently at work. Please try again later [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":403,"id":"20014b504cb97819","source":{"pointer":"/export/SITE/1234"},"title":"Operation Forbidden","detail":"This resource, or one of its associated resources, is currently at work. Please try again later"}]}
```

500

Something went wrong. Contact support [APIError](#)

Example data

Content-Type: */*

```
{"errors": [{"status":500,"id":"20014b504cb97819","source":{"pointer":"/export/SITE/1234"},"title":"Internal Server Error","detail":"Something went wrong. Contact support"}]}
```

Models

Methods

Table of Contents

1. APIError
2. AsyncResponse

APIError

code (optional)
 detail (optional)
 id (optional)
 source (optional)
 status (optional)
 format: int32
 title (optional)

AsyncResponse

handler (optional)
 The code provided in the export response. Used to identify the associated zip file when sending the download request.
 status (optional)
 The HTTP response status code indicating the status of the export process.

Imperva Subscription Management API

Access the subscription data for your account using the API. For the full feature documentation, see [Subscription status](#).

Version: 1.0.0

BasePath:/subscription-management

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

[Models](#)

Table of Contents

SubscriptionResources

- `get /v3/subscriptions/{subscription-id}/resources`

Subscriptions

- `get /v3/subscriptions/{subscription-id}`
- `get /v3/subscriptions`

SubscriptionResources

```
get /v3/subscriptions/{subscription-id}/resources
```

Retrieve a subscription's resources (getSubscriptionResources)
 Retrieve a subscription's resources by a subscription ID.

Path parameters

`subscription-id` (required)

Path Parameter

— Subscription ID. Unique identifier of the subscription. Run the GET /v3/subscriptions API to locate the value of the 'id' parameter in the response.

Query parameters

`caid` (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

Return type

`ImpervaApiBodyListSubscriptionResourceDto`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "subscription_id" : "f311512c-2312-4852-877b-73ea6b4daf28",
    "metering_model" : "PERCENTILE",
    "account_id" : 123456,
    "resource_template_id" : "throughput",
    "subscription_resource_value" : "",
    "id" : "f9ae8413-a829-41e4-960d-b39df32fcc99",
    "trial_end_date" : "2024-12-31T00:00:00.000+00:00",
    "resource_template_version" : 1,
    "resource_display_name" : "WAF Bandwidth",
    "resource_status" : "ACTIVE"
  }, {
    "subscription_id" : "f311512c-2312-4852-877b-73ea6b4daf28",
    "metering_model" : "PERCENTILE",
    "account_id" : 123456,
    "resource_template_id" : "throughput",
    "subscription_resource_value" : ""
  }
]
```

```

    "id" : "f9ae8413-a829-41e4-960d-b39df32fcc99",
    "trial_end_date" : "2024-12-31T00:00:00.000+00:00",
    "resource_template_version" : 1,
    "resource_display_name" : "WAF Bandwidth",
    "resource_status" : "ACTIVE"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

[OK ImpervaApiBodyListSubscriptionResourceDto](#)

Subscriptions

```
get /v3/subscriptions/{subscription-id}
```

Retrieve a subscription (get)

Retrieve subscription details by a subscription ID.

Path parameters

subscription-id (required)

Path Parameter

— Subscription ID. Unique identifier of the subscription. Run the GET /v3/subscriptions API to locate the value of the 'id' parameter in the response. format: uuid

Query parameters

caid (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

statusList (optional)

Query Parameter

— Subscription status to return. default: ["ACTIVE","CANCELLED","MIGRATION_INITIATED","EXPIRED"]

Return type

[ImpervaApiBodySubscription](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "payment_gateway" : "EXTERNAL",
    "subscription_status" : "ACTIVE",
    "id" : "efe89e68-8fef-49ed-a14f-714524381122",
    "creation_date" : "2023-10-17T00:00:00.000+00:00",
    "base_plan_sku_display_names" : "App Protect Essentials",
    "usage_cycle_day" : 25,
    "let_expire" : "2024-11-20T00:00:00.000+00:00"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

200

OK. The subscription is returned. [ImpervaApiBodySubscription](#)

```
get /v3/subscriptions
```

Retrieve all subscriptions (getAll)
Retrieve all subscription details of an account.

Query parameters

caid (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

statusList (optional)

Query Parameter

— Subscription status to return. default: ["ACTIVE","CANCELLED","MIGRATION_INITIATED","EXPIRED"]

Return type

[ImpervaApiBodyListSubscription](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "payment_gateway" : "EXTERNAL",
    "subscription_status" : "ACTIVE",
    "id" : "efe89e68-8fef-49ed-a14f-714524381122",
    "creation_date" : "2023-10-17T00:00:00.000+00:00",
    "base_plan_sku_display_names" : "App Protect Essentials",
    "usage_cycle_day" : 25,
    "let_expire" : "2024-11-20T00:00:00.000+00:00"
  }, {
    "payment_gateway" : "EXTERNAL",
    "subscription_status" : "ACTIVE",
    "id" : "efe89e68-8fef-49ed-a14f-714524381122",
    "creation_date" : "2023-10-17T00:00:00.000+00:00",
    "base_plan_sku_display_names" : "App Protect Essentials",
    "usage_cycle_day" : 25,
    "let_expire" : "2024-11-20T00:00:00.000+00:00"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK. The subscriptions are returned. [ImpervaApiBodyListSubscription](#)

Models

Methods

Table of Contents

1. BooleanSubscriptionResourceValueDto
2. EnumSubscriptionResourceValueDto
3. [ImpervaApiBodyListSubscription](#)
4. [ImpervaApiBodyListSubscriptionResourceDto](#)
5. [ImpervaApiBodySubscription](#)
6. NumberSubscriptionResourceValueDto
7. Subscription
8. SubscriptionResourceDto
9. SubscriptionResourceValueDto

BooleanSubscriptionResourceValueDto

A resource value of boolean type

type

String

ordered_value (optional)

Boolean

The purchased quantity of the resource.

trial_value (optional)

Boolean

The trial quantity of the resource.

EnumSubscriptionResourceValueDto

A resource value of enum type

type

String

ordered_value (optional)

String

The purchased quantity of the resource.

trial_value (optional)

String

The trial quantity of the resource.

ImpervaApiBodyListSubscription

data

array[Subscription]

API response data

ImpervaApiBodyListSubscriptionResourceDto

data

array[SubscriptionResourceDto]

API response data

ImpervaApiBodySubscription

data

Subscription

NumberSubscriptionResourceValueDto

A resource value of number type

type

String

ordered_value (optional)

Long

The purchased quantity of the resource. format: int64

example: 50

trial_value (optional)

Long

The trial quantity of the resource. format: int64

example: 100

is_unlimited (optional)

Boolean

Denotes if the purchased quantity is unlimited.

example: true

Subscription

API response data

id (optional)

UUID

Subscription ID. format: uuid

example: efe89e68-8fef-49ed-a14f-714524381122

base_plan_sku_display_names (optional)

array[String]

The name of the subscription plan as displayed in the management console.

example: App Protect Essentials

subscription_status (optional)

String

Indicates the status of the subscription.

Enum:

ACTIVE

EXPIRED

CANCELLED

MIGRATION_INITIATED

example: ACTIVE

usage_cycle_day (optional)

Integer

The start of the period used for calculating usage. For example, the value 10 indicates that the usage period starts on the 10th of the month and ends on the 9th of the following month. format: int32

example: 25

let_expire (optional)

date

The date the subscription or trial period is set to end. format: date

example: Wed Nov 20 00:00:00 UTC 2024

creation_date (optional)

date

Creation date of the subscription. format: date

example: Tue Oct 17 00:00:00 UTC 2023

payment_gateway (optional)

String

Indicates a subscription paid for by credit card.

Enum:

EXTERNAL

NONE

example: EXTERNAL

SubscriptionResourceDto

API response data

id

UUID

Subscription Resource ID. format: uuid

example: f9ae8413-a829-41e4-960d-b39df32fcc99

subscription_id (optional)

UUID

Subscription ID. format: uuid

example: f311512c-2312-4852-877b-73ea6b4daf28

resource_template_id
String
ID of resource template metadata for this subscription resource.
example: throughput
account_id (optional)
Long
Account ID. format: int64
example: 123456
resource_display_name (optional)
String
Display name of this subscription resource.
example: WAF Bandwidth
trial_end_date (optional)
date
Trial expiration date of this subscription resource, specified as an ISO Date Format yyyy-MM-dd. format: date
example: Tue Dec 31 00:00:00 UTC 2024
subscription_resource_value
oneOf:
BooleanSubscriptionResourceValueDto EnumSubscriptionResourceValueDto
NumberSubscriptionResourceValueDto
metering_model
String
Metering model for this subscription resource.
Enum:
PERCENTILE
PERCENTILE_ON_DEMAND
CONSUMPTION
UNIT_BASED
NONE
LIMIT_BASED
example: PERCENTILE
resource_status (optional)
String
Status for this subscription resource.
Enum:
ACTIVE
EXPIRED
PENDING
CANCELLED
example: ACTIVE
resource_template_version
Long
The version of the resource template metadata for this resource. format: int64
example: 1

SubscriptionResourceValueDto

Purchased and/or trial values for this subscription resource.
type
String

Imperva Usage Management API

Access the usage history for your account using the API. For the full feature documentation, see [View Account Usage](#).
Version: 1.0.0
BasePath:/usage-management

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

UsageRecords

- `get /v3/subscription-usage-records/{subscription-usage-record-id}/detailed-usage`
- `get /v3/subscription-usage-records`

UsageRecords

```
get /v3/subscription-usage-records/{subscription-usage-record-id}/detailed-usage
```

Retrieve a usage record's detailed information. (getDetailedUsage)
Retrieve a usage record's detailed information.

Path parameters

subscription-usage-record-id (required)

Path Parameter

— Unique identifier of the subscription usage record. Run the GET /v3/subscription-usage-record API to locate the value of the 'id' parameter in the response.

Query parameters

caid (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

resource (required)

Query Parameter

— Resource ID.

Return type

[ImpervaApiBodyListDetailedSubscriptionUsage](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "resource_usage_records" : [ {
      "bucket_list" : [ {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      }, {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      } ],
      "resource_id" : "throughput",
      "id" : "947bc64b-86f3-43e8-93c4-177ff3f4201f",
      "data_unit" : "Mbps"
    }, {
      "bucket_list" : [ {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      }, {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      } ],
      "resource_id" : "throughput",
      "id" : "947bc64b-86f3-43e8-93c4-177ff3f4201f",
      "data_unit" : "Mbps"
    } ]
  }, {
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "resource_usage_records" : [ {
      "bucket_list" : [ {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      }, {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      } ],
      "resource_id" : "throughput",
      "id" : "947bc64b-86f3-43e8-93c4-177ff3f4201f",
      "data_unit" : "Mbps"
    }, {
      "bucket_list" : [ {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      }, {
        "end_date" : "2023-11-26T01:05:00Z",
        "bucket_value" : 123.45,
        "start_date" : "2023-11-26T01:00:00Z"
      } ],
      "resource_id" : "throughput",
      "id" : "947bc64b-86f3-43e8-93c4-177ff3f4201f",
      "data_unit" : "Mbps"
    } ]
  }
}
```

```

        } ],
        "resource_id" : "throughput",
        "id" : "947bc64b-86f3-43e8-93c4-177ff3f4201f",
        "data_unit" : "Mbps"
    } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK ImpervaApiBodyListDetailedSubscriptionUsage

```
get /v3/subscription-usage-records
```

Retrieve a summary of usage records. (getUsageSummary)

Retrieve a summary of usage records.

Query parameters

caid (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

from (optional)

Query Parameter

— Earliest time boundary, specified as an ISO Date Format yyyy-MM-dd. format: date

to (optional)

Query Parameter

— Latest time boundary, specified as an ISO Date Format yyyy-MM-dd. format: date

resource (optional)

Query Parameter

— Resource ID. Possible values : advanced_bot_protection_connector, api_security_anywhere ,bot_management ,infra_protect_always_on_bandwidth, on_demand_throughput, throughput

Return type

ImpervaApiBodyListSubscriptionUsageRecord

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "subscription_id" : "2c8117e5-c4c7-47cb-91c9-b33d2c793527",
    "account_id" : 1234567,
    "record_status" : "OPEN",
    "cycle_start_date" : "2023-12-25T00:00:00.000+00:00",
    "cycle_end_date" : "2024-12-24T00:00:00.000+00:00",
    "id" : "ccd04cc7-51f5-4532-b623-4d00d14448b2",
    "usage_cycle_day" : 25,
    "base_plan_sku_display_names" : "Enterprise 100",
    "resource_usage_records" : [ {
      "record_status" : "OPEN",
      "overages" : 456.78,
      "unlimited_purchase" : true,
      "used" : 1234.56,
      "unlimited_trial" : false,
      "trial" : 456.78,
      "data_unit" : "Mbps",
      "calculated_for_resources" : "sites",
      "purchased" : 123.45,
      "cycle_start_date" : "2023-11-26T00:00:00.000+00:00",
      "close_term_reason" : "Resource cancelled",
      "resource_id" : "throughput",
      "cycle_end_date" : "2023-12-25T00:00:00.000+00:00",
      "id" : "fe46bed8-ba2b-4a1c-88ea-4998be5df268",
      "resource_name" : "WAF Bandwidth"
    }, {
      "record_status" : "OPEN",
      "overages" : 456.78,
      "unlimited_purchase" : true,
      "used" : 1234.56,
      "unlimited_trial" : false,
      "trial" : 456.78,
      "data_unit" : "Mbps",
      "calculated_for_resources" : "sites",
      "purchased" : 123.45,
      "cycle_start_date" : "2023-11-26T00:00:00.000+00:00",
      "close_term_reason" : "Resource cancelled",
      "resource_id" : "throughput",
      "cycle_end_date" : "2023-12-25T00:00:00.000+00:00",
      "id" : "fe46bed8-ba2b-4a1c-88ea-4998be5df268",
      "resource_name" : "WAF Bandwidth"
    } ]
  }, {
    "subscription_id" : "2c8117e5-c4c7-47cb-91c9-b33d2c793527",
    "account_id" : 1234567,
    "record_status" : "OPEN",
    "cycle_start_date" : "2023-12-25T00:00:00.000+00:00",
    "cycle_end_date" : "2024-12-24T00:00:00.000+00:00",
    "id" : "ccd04cc7-51f5-4532-b623-4d00d14448b2",
    "usage_cycle_day" : 25,
    "base_plan_sku_display_names" : "Enterprise 100",
    "resource_usage_records" : [ {
      "record_status" : "OPEN",
      "overages" : 456.78,
      "unlimited_purchase" : true,
      "used" : 1234.56,
      "unlimited_trial" : false,
      "trial" : 456.78,
      "data_unit" : "Mbps",
      "calculated_for_resources" : "sites",
      "purchased" : 123.45,
      "cycle_start_date" : "2023-11-26T00:00:00.000+00:00",
      "close_term_reason" : "Resource cancelled",
      "resource_id" : "throughput",
      "cycle_end_date" : "2023-12-25T00:00:00.000+00:00",
      "id" : "fe46bed8-ba2b-4a1c-88ea-4998be5df268",
      "resource_name" : "WAF Bandwidth"
    } ]
  }
]
```

```

    "data_unit" : "Mbps",
    "calculated_for_resources" : "sites",
    "purchased" : 123.45,
    "cycle_start_date" : "2023-11-26T00:00:00.000+00:00",
    "close_term_reason" : "Resource cancelled",
    "resource_id" : "throughput",
    "cycle_end_date" : "2023-12-25T00:00:00.000+00:00",
    "id" : "fe46bed8-ba2b-4a1c-88ea-4998be5df268",
    "resource_name" : "WAF Bandwidth"
}, {
    "record_status" : "OPEN",
    "overages" : 456.78,
    "unlimited_purchase" : true,
    "used" : 1234.56,
    "unlimited_trial" : false,
    "trial" : 456.78,
    "data_unit" : "Mbps",
    "calculated_for_resources" : "sites",
    "purchased" : 123.45,
    "cycle_start_date" : "2023-11-26T00:00:00.000+00:00",
    "close_term_reason" : "Resource cancelled",
    "resource_id" : "throughput",
    "cycle_end_date" : "2023-12-25T00:00:00.000+00:00",
    "id" : "fe46bed8-ba2b-4a1c-88ea-4998be5df268",
    "resource_name" : "WAF Bandwidth"
} ]
}
]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

[OK ImpervaApiBodyListSubscriptionUsageRecord](#)

Models

Methods

Table of Contents

1. Bucket
 2. DetailedResourceUsage
 3. DetailedSubscriptionUsage
 4. [ImpervaApiBodyListDetailedSubscriptionUsage](#)
-

-
5. ImpervaApiBodyListSubscriptionUsageRecord
 6. ResourceUsageRecord
 7. SubscriptionUsageRecord

Bucket

List of usage values per a unit of time (bucket).

start_date (optional)

Date

The start datetime of the bucket format: date-time

example: 2023-11-26T01:00Z

end_date (optional)

Date

The end datetime of the bucket format: date-time

example: 2023-11-26T01:05Z

bucket_value (optional)

Double

Usage value of the bucket format: double

example: 123.45

DetailedResourceUsage

List of detailed resource usage records.

id (optional)

UUID

Usage record ID of the resource. format: uuid

example: 947bc64b-86f3-43e8-93c4-177ff3f4201f

resource_id (optional)

String

The measured resource ID.

example: throughput

data_unit (optional)

String

The measurement unit of the data. Possible values: Mbps, Gb, M Requests.

example: Mbps

bucket_list (optional)

array[Bucket]

List of usage values per a unit of time (bucket).

DetailedSubscriptionUsage

API response data

id (optional)

UUID

Usage record ID of the subscription format: uuid

resource_usage_records (optional)

array[DetailedResourceUsage]

List of detailed resource usage records.

ImpervaApiBodyListDetailedSubscriptionUsage

data

array[DetailedSubscriptionUsage]

API response data

ImpervaApiBodyListSubscriptionUsageRecord

data

array[SubscriptionUsageRecord]

API response data

ResourceUsageRecord

a list of the Subscription's resources' usage records.

id (optional)

UUID

Resource Usage Record ID. format: uuid

example: fe46bed8-ba2b-4a1c-88ea-4998be5df268

resource_id (optional)

String

The ID of the resource.

example: throughput

resource_name (optional)

String

The display name of the resource.

example: WAF Bandwidth

record_status (optional)

String

The status of this resource usage record.

Enum:

OPEN

CLOSED

CLOSED_MID_CYCLE

purchased (optional)

Double

The purchased amount of the resource. format: double

example: 123.45

trial (optional)

Double

The trial portion of the resource. format: double

example: 456.78

used (optional)

Double

The amount of the resource that was used, out of the purchased amount. format: double

example: 1234.56

overages (optional)

Double

The amount of monthly usage in excess of the amount included with your plan. format: double

example: 456.78

data_unit (optional)

String

The measurement unit of the data. Possible values: Mbps, Gb, M Requests.

example: Mbps

cycle_start_date (optional)

date

The start date of this resource usage record. format: date

example: Sun Nov 26 00:00:00 UTC 2023

cycle_end_date (optional)

date

The end date of this resource usage record. format: date

example: Mon Dec 25 00:00:00 UTC 2023

close_term_reason (optional)

String

The reason for term closure. Possible values: End of cycle, Quantity changed, Usage cycle day changed, Resource cancelled, Subscription cancelled, SubAccount deleted, Change in services included in calculation.

example: Resource cancelled

calculated_for_resources (optional)

array[String]

Additional resources included in this usage calculation.

example: sites

unlimited_purchase (optional)

Boolean

Indicates if the plan includes unlimited usage of the resource.

example: true

unlimited_trial (optional)

Boolean

Indicates if the trial plan includes unlimited usage of the resource.

example: false

SubscriptionUsageRecord

API response data

id (optional)

UUID

Subscription Usage Record ID. format: uuid

example: ccd04cc7-51f5-4532-b623-4d00d14448b2

subscription_id (optional)

UUID

Subscription ID. format: uuid

example: 2c8117e5-c4c7-47cb-91c9-b33d2c793527

account_id (optional)

Long

Account ID. format: int64

example: 1234567

record_status (optional)

String

Subscription Record Status.

Enum:

OPEN

CLOSED

CLOSED_MID_CYCLE

example: OPEN

usage_cycle_day (optional)

Integer

The start of the period used for calculating usage. For example, the value 10 indicates that the usage period starts on the 10th of the month and ends on the 9th of the following month. format: int32

example: 25

cycle_start_date (optional)

date

The start of the usage cycle. format: date

example: Mon Dec 25 00:00:00 UTC 2023

cycle_end_date (optional)

date

The end of the usage cycle. format: date

example: Tue Dec 24 00:00:00 UTC 2024

resource_usage_records (optional)

array[ResourceUsageRecord]

a list of the Subscription's resources' usage records.

base_plan_sku_display_names (optional)

array[String]

The name of the subscription plan as displayed in the management console.

example: Enterprise 100

Imperva audit-trail

View a log of actions performed in your account by account users, system processes, and Imperva system administrators and support. For full feature documentation, see [Audit Trail](#)

Version: 1.0.0

BasePath:/audit-trail

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AuditTrail

- `get /v2/events`

AuditTrailV1Retired

- `get /v1/events`

AuditTrail

```
get /v2/events
```

Get account audit events (getAuditEventsV2)
 This is a list of audit events of the specified account

Query parameters

`assume` (optional)

Query Parameter

— Is the action performed by Imperva Support logged in as an account user

`caid` (optional)

Query Parameter

— Numeric identifier of the account to operate on. If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

`end` (optional)

Query Parameter

— Latest time boundary (in milliseconds) format: int64

limit (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 50. Maximum is 100 format: int32

offset (optional)

Query Parameter

— Offset is the position of a particular record in the dataset. You can retrieve a subset of records starting with the offset value. The offset and limit parameters work together. Valid values for the offset parameter are multiples of the limit. For example, if you define limit as 50, you can define offset as either 0, 50, 100, 150, or any multiple of 50. format: int32

start (required)

Query Parameter

— Earliest time boundary (in milliseconds) format: int64

type (optional)

Query Parameter

— The action that was performed in the account, such as ACCOUNT_LOGIN

Return type

audit_record_response

Example data

Content-Type: application/json

```
{
  "total" : 1,
  "elements" : [ {
    "account_id" : "285",
    "resource_type_key" : "API",
    "user_id" : "1234",
    "user_details" : "user@test.com",
    "assumed_by_user" : "Imperva support",
    "resource_id" : "4389",
    "time" : 1591860030099,
    "message" : "API (4389) updated",
    "context_key" : "UI",
    "type_description" : "API updated",
    "type_key" : "API_UPDATED"
  }, {
    "account_id" : "285",
    "resource_type_key" : "API",
    "user_id" : "1234",
    "user_details" : "user@test.com",
    "assumed_by_user" : "Imperva support",
    "resource_id" : "4389",
    "time" : 1591860030099,
    "message" : "API (4389) updated",
    "context_key" : "UI",
    "type_description" : "API updated",
    "type_key" : "API_UPDATED"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response `audit_record_response`

500

Error response `error_response_wrapper`

AuditTrailV1Retired

```
get /v1/events
```

Get account audit events (getAuditEvents)

This api is deprecated. This is a list of audit events of the specified account

Query parameters

`assume` (optional)

Query Parameter

— Is the action performed by Imperva Support logged in as an account user

`caid` (optional)

Query Parameter

— Numeric identifier of the account to operate on. If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

`end` (optional)

Query Parameter

— Latest time boundary (in milliseconds) format: int64

`limit` (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 50. Maximum is 100 format: int32

`offset` (optional)

Query Parameter

— Offset is the position of a particular record in the dataset. You can retrieve a subset of records starting with the offset value. The offset and limit parameters work together. Valid values for the offset parameter are multiples of the limit. For example, if you define limit as 50, you can define offset as either 0, 50, 100, 150, or any multiple of 50. format: int32

`start` (required)

Query Parameter

— Earliest time boundary (in milliseconds) format: int64

`type` (optional)

Query Parameter

— The action that was performed in the account, such as ACCOUNT_LOGIN

Return type

array[audit_record]

Example data

Content-Type: application/json

```
[ {
  "account_id" : "285",
  "resource_type_key" : "API",
  "user_id" : "1234",
  "user_details" : "user@test.com",
  "assumed_by_user" : "Imperva support",
  "resource_id" : "4389",
  "time" : 1591860030099,
  "message" : "API (4389) updated",
  "context_key" : "UI",
  "type_description" : "API updated",
  "type_key" : "API_UPDATED"
}, {
  "account_id" : "285",
  "resource_type_key" : "API",
  "user_id" : "1234",
  "user_details" : "user@test.com",
  "assumed_by_user" : "Imperva support",
  "resource_id" : "4389",
  "time" : 1591860030099,
  "message" : "API (4389) updated",
  "context_key" : "UI",
  "type_description" : "API updated",
  "type_key" : "API_UPDATED"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

500

Error response error_response_wrapper

Models

Methods

Table of Contents

1. audit_record
2. audit_record_response
3. error_response_wrapper

audit_record

A single audit record
time (optional)

Long

Time of the audit event format: int64

example: 1591860030099

type_key (optional)

String

The name of the action that was performed in the account, such as ACCOUNT_LOGIN or SITE_ORIGIN_SERVERS_SETTINGS_CHANGED.

example: API_UPDATED

type_description (optional)

String

A description of the action that was performed in the account, such as logging in or changing site settings.

example: API updated

user_id (optional)

String

ID of the user who performed the action

example: 1234

user_details (optional)

String

Email of the user who performed the action

example: user@test.com

account_id (optional)

String

ID of the account that the action was done in

example: 285

resource_type_key (optional)

String

The type of the resource that the action was done on

example: API

resource_id (optional)

String

ID of the resource that the action was done on

example: 4389

message (optional)

String

Detailed description of the audit event

example: API (4389) updated

context_key (optional)

String

The audit activity context. Can be one of the following: UI, API, INTERNAL_API, JOB, NA

example: UI

assumed_by_user (optional)

String

The user who performed the action on behalf of an account user
example: Imperva support

audit_record_response

A object contains collection of audit record

total (optional)

Long

The total number of audit trail entries during the requested time range format: int64

example: 1

elements (optional)

array[audit_record]

collection of audit elements

error_response_wrapper

Object that describes a non valid response

code (optional)

Integer

Internal response code format: int32

example: 1001

message (optional)

String

Response message

example: Required parameter 'start' is missing

id (optional)

String

Unique id to identify the error in the logs

example: Xu09cHAb

Notification Settings API

Create and manage notification settings for your account using the API. For full feature documentation, see

[Notification Settings](#)

Version: 1.0.0

BasePath:/notification-settings

The terms in the absence of an applicable signed agreement between you and Imperva

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true

2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

NotificationPolicies

- `post /v3/policies`
- `delete /v3/policies/{policyId}`
- `get /v3/policies/{policyId}`
- `get /v3/policies/lite`
- `put /v3/policies/{policyId}`
- `put /v3/policy/update`

NotificationSubtypes

- `get /v3/subtypes`

NotificationPolicies

```
post /v3/policies
```

Create a notification policy (create)

Create a notification policy for account and website activity, application security events, and network security updates.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `ImpervaApiDtoNotificationPolicyFull` (required)
Body Parameter

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`ImpervaApiDtoNotificationPolicyFull`

Example data

Content-Type: `application/json`

```
{
  "data" : {
    "accountId" : 645345,
    "subCategory" : "subCategory",
    "policyId" : 2348756345,
    "subAccountPolicyInfo" : {
      "subAccountList" : [ {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      } ],
      "applyToNewSubAccounts" : "FALSE"
    },
    "policyName" : "Default Account notification policy",
    "notificationChannelList" : [ "" ],
    "policyType" : "ACCOUNT",
    "assetList" : [ {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }, {
      "assetId" : 63542345,
      "displayName" : "mysite.com",
      "assetType" : "SITE"
    }
  }
}
```

```

    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, [
    "applyToNewAssets" : "TRUE",
    "status" : "ENABLE"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

201

OK. The request rule is returned. [ImpervaApiDtoNotificationPolicyFull](#)

```
delete /v3/policies/{policyId}
```

Delete a notification policy (delete)

Delete the notification policy as per the specified CAID and policy ID parameters.

Path parameters

policyId (required)

Path Parameter

— The Imperva ID of the policy. To retrieve the policy ID, run the GET /v3/policies/lite API. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ImpervaApiDtoNotificationPolicyFull](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "accountId" : 645345,
    "subCategory" : "subCategory",
    "policyId" : 2348756345,
    "subAccountPolicyInfo" : {
      "subAccountList" : [ {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
      } ],
      "applyToNewSubAccounts" : "FALSE"
    },
    "policyName" : "Default Account notification policy",
    "notificationChannelList" : [ "" ],
  }
}
```

```

"policyType" : "ACCOUNT",
"assetList" : [ {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}, {
  "assetId" : 63542345,
  "displayName" : "mysite.com",
  "assetType" : "SITE"
}], "applyToNewAssets" : "TRUE", "status" : "ENABLE"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

OK. The request rule is returned. [ImpervaApiDtoNotificationPolicyFull](#)

```
get /v3/policies/{policyId}
```

Retrieve a notification policy (get)

Retrieve details of a given policy according to policy ID. To retrieve the policy ID, run the GET /v3/policies/lite API.

Path parameters

policyId (required)

Path Parameter

— The Imperva ID of the policy. To retrieve the policy ID, run the GET /v3/policies/lite API. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ImpervaApiDtoNotificationPolicyFull](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "accountId" : 645345,
    "subCategory" : "subCategory",
    "policyId" : 2348756345,
    "subAccountPolicyInfo" : [
      {
        "subAccountList" : [ {
          "subAccountId" : 32424,
          "displayName" : "Production EMEA Account"
        }, {
          "subAccountId" : 32424,
          "displayName" : "Production EMEA Account"
        }, {
          "subAccountId" : 32424,
          "displayName" : "Production EMEA Account"
        }, {
          "subAccountId" : 32424,
          "displayName" : "Production EMEA Account"
        }, {
          "subAccountId" : 32424,
        }
      ]
    }
  }
}
```



```

    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
  ],
  "applyToNewAssets" : "TRUE",
  "status" : "ENABLE"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK. The request rule is returned. [ImpervaApiDtoNotificationPolicyFull](#)

```
get /v3/policies/lite
```

Get account notification policies (getNotificationPolicyLiteList)
Get a summarized list of all notification policies in your account.

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ImpervaApiDtoListNotificationPolicyLite](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "subCategory" : "ACCOUNT_NOTIFICATIONS",
    "subCategoryDisplayName" : "Account Notifications",
    "categoryDisplayName" : "Account and Site notifications",
    "channelTypeList" : [ {
      "channelTypeDisplayName" : "Email",
      "recipientCount" : 32,
    }
  ]
}
```

```

    "channelType" : "email"
}, {
    "channelTypeDisplayName" : "Email",
    "recipientCount" : 32,
    "channelType" : "email"
} ],
"subAccountsAppliedCount" : 12,
"assetsInUsedCount" : 43,
"accountId" : 523423,
"assetsTotalCount" : 54,
"policyId" : 123123,
"policyType" : "ACCOUNT",
"name" : "Default Account notifications policy",
"category" : "ACCOUNT_AND_SITE",
"subAccountsTotalCount" : 16,
"status" : "ENABLE"
}, {
    "subCategory" : "ACCOUNT_NOTIFICATIONS",
    "subCategoryDisplayName" : "Account Notifications",
    "categoryDisplayName" : "Account and Site notifications",
    "channelTypeList" : [ {
        "channelTypeDisplayName" : "Email",
        "recipientCount" : 32,
        "channelType" : "email"
    }, {
        "channelTypeDisplayName" : "Email",
        "recipientCount" : 32,
        "channelType" : "email"
    } ],
"subAccountsAppliedCount" : 12,
"assetsInUsedCount" : 43,
"accountId" : 523423,
"assetsTotalCount" : 54,
"policyId" : 123123,
"policyType" : "ACCOUNT",
"name" : "Default Account notifications policy",
"category" : "ACCOUNT_AND_SITE",
"subAccountsTotalCount" : 16,
"status" : "ENABLE"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

[OK ImpervaApiDtoListNotificationPolicyLite](#)

```
put /v3/policies/{policyId}
```

Update a notification policy (update)
Overwrite an existing policy (full update)

Path parameters

policyId (required)

Path Parameter

— The Imperva ID of the policy. To retrieve the policy ID, run the GET /v3/policies/lite API. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ImpervaApiDtoNotificationPolicyFull](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ImpervaApiDtoNotificationPolicyFull](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "accountId" : 645345,
    "subCategory" : "subCategory",
    "policyId" : 2348756345,
    "subAccountPolicyInfo" : [
      {
        "subAccountList" : [
          {
            "subAccountId" : 32424,
            "displayName" : "Production EMEA Account"
          },
          {
            "subAccountId" : 32424,
            "displayName" : "Production EMEA Account"
          }
        ]
      }
    ]
  }
}
```

```

        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "subAccountId" : 32424,
        "displayName" : "Production EMEA Account"
    }, {
        "applyToNewSubAccounts" : "FALSE"
    },
    "policyName" : "Default Account notification policy",
    "notificationChannelList" : [ "" ],
    "policyType" : "ACCOUNT",
    "assetList" : [
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        },
        {
            "assetId" : 63542345,
            "displayName" : "mysite.com",
            "assetType" : "SITE"
        }
    ]
}

```

```

    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
}, {
    "assetId" : 63542345,
    "displayName" : "mysite.com",
    "assetType" : "SITE"
} ],
"applyToNewAssets" : "TRUE",
"status" : "ENABLE"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

OK. The request rule is returned. [ImpervaApiDtoNotificationPolicyFull](#)

```
put /v3/policy/update
```

Update notification policy status (updateNonCRUDPolicy)
Enable or disable a notification policy.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body [ImpervaApiDtoNotificationPolicyUpdates](#) (required)
Body Parameter

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API

credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ImpervaApiDtoNotificationPolicyUpdates](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "accountId" : 534522,
    "policyId" : 231121,
    "status" : "ENABLE"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK [ImpervaApiDtoNotificationPolicyUpdates](#)

NotificationSubtypes

```
get /v3/subtypes
```

Retrieve all allowed notification subtypes (getAllowedSubCategoryTemplates)
Retrieves details of the allowed notification subtypes for the specified account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ImpervaApiDtoListSubCategoryDetails](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "connected_asset" : "SITE",
    "sub_category_id" : "SITE_NOTIFICATIONS",
    "category" : "ACCOUNT_AND_SITE",
    "display_name" : "Website Notifications"
  }, {
    "connected_asset" : "SITE",
    "sub_category_id" : "SITE_NOTIFICATIONS",
    "category" : "ACCOUNT_AND_SITE",
    "display_name" : "Website Notifications"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK. A list of notifications sub-types is returned. [ImpervaApiDtoListSubCategoryDetails](#)

Models

Methods

Table of Contents

1. Asset
2. ChannelType
3. ExternalRecipient
4. ImpervaApiDtoListNotificationPolicyLite
5. ImpervaApiDtoListSubCategoryDetails
6. ImpervaApiDtoNotificationPolicyFull
7. ImpervaApiDtoNotificationPolicyUpdates
8. NotificationChannelEmail
9. NotificationChannelInterface
10. NotificationPolicyFull
11. NotificationPolicyLite

-
12. NotificationPolicyUpdates
 13. Recipient
 14. SubAccount
 15. SubAccountPolicyInfo
 16. SubCategoryDetails
 17. UserRecipient

Asset

List of assets to receive notifications (if assets are relevant to the sub category type)

assetType

String

Indicates the type of asset that triggers the notification, such as websites, router connections, network prefixes, individual IPs, Flow exporters, and DNS zones. Example values include: "SITE"

Enum:

SITE

IP_RANGE

EDGE_IP

ORIGIN_CONNECTIVITY

NETFLOW_EXPORTER

DOMAIN

example: SITE

assetId

Long

Indicates a numeric value of the asset. format: int64

example: 63542345

displayName (optional)

String

Indicates name of recipient of the notification.

example: mysite.com

ChannelType

The notification method. For example, email.

channelType (optional)

String

Indicates how recipient receives notifications.

Enum:

email

channelTypeDisplayName (optional)

String

Displayed name of the notification channel.

example: Email

recipientCount (optional)

Integer

The total number of recipients in the account that receive the requested notification type. format: int32

example: 32

ExternalRecipient

displayName (optional)

String

Indicates name of recipient of the notification.

example: John Doe

recipientType (optional)

String

Indicates whether recipient is an external or internal user.

email (optional)

String

Indicates email address of notification recipient.

example: john.doe@imperva.com

ImpervaApiDtoListNotificationPolicyLite

data (optional)

array[NotificationPolicyLite]

API response data

ImpervaApiDtoListSubCategoryDetails

data (optional)

array[SubCategoryDetails]

API response data

ImpervaApiDtoNotificationPolicyFull

The policy to create

data (optional)

NotificationPolicyFull

ImpervaApiDtoNotificationPolicyUpdates

data (optional)

NotificationPolicyUpdates

NotificationChannelEmail

channelType (optional)

String

Enum:

email

recipientToList

array[null]

List of recipients

items oneOf:

ExternalRecipient UserRecipient

NotificationChannelInterface

List of notification channels

channelType (optional)

String

Enum:

email

NotificationPolicyFull

API response data

policyId (optional)

Long

The policy ID. Send a null value when creating a new policy. When updating a policy, send the ID of the relevant policy. format: int64

example: 2348756345

accountId (optional)

Long

The Imperva ID of the account or subaccount. The accountId must be either null, equal to the account id associated with the API key, or equal to the caid. format: int64

example: 645345

policyName

String

The name of the policy

example: Default Account notification policy

status

String

Indicates whether policy is enabled or disabled.

Enum:

ENABLE

DISABLE

subCategory

String

The subtype of the notification policy.

notificationChannelList

array[null]

List of notification channels

items oneOf:

NotificationChannelEmail

assetList (optional)

array[Asset]

List of assets to receive notifications (if assets are relevant to the sub category type)

applyToNewAssets

String

If value is 'TRUE', all newly onboarded assets are automatically added to the notification policy's assets list.

Enum:

TRUE

FALSE

policyType (optional)

String

If value is 'ACCOUNT', the policy will apply only to the current account. If the value is 'SUB_ACCOUNT' the policy applies to the sub accounts only. The parent account will receive notifications for activity in the sub accounts that are specified in the subAccountList parameter. This parameter is available only in accounts that can contain sub accounts.

Enum:

ACCOUNT

SUB_ACCOUNT

subAccountPolicyInfo (optional)

SubAccountPolicyInfo

NotificationPolicyLite

API response data

policyId (optional)

Long

The Imperva ID of the policy. format: int64

example: 123123

accountId (optional)

Long

The Imperva ID of the account. format: int64

example: 523423

name (optional)

String

The name of the policy

example: Default Account notifications policy

status (optional)

String

Indicates whether policy is enabled or disabled.

Enum:

ENABLE

DISABLE

subCategory (optional)

String

The notification policy subtype, such as ACCOUNT_NOTIFICATIONS.

example: ACCOUNT_NOTIFICATIONS

subCategoryDisplayName (optional)

String

Displayed name of the notification policy subtype.

example: Account Notifications

channelTypeList (optional)

array[ChannelType]

List of the channel types of the policy.

assetsInUsedCount (optional)

Integer

The number of assets in the account to which the policy is applied. format: int32

example: 43

assetsTotalCount (optional)

Integer

The total number of assets available in the account. format: int32

example: 54

category (optional)

String

The notification policy type, such as ACCOUNT_AND_SITE.

Enum:

ACCOUNT_AND_SITE

APPLICATION_SECURITY_EVENTS

NETWORK_SECURITY

SYSTEM

example: ACCOUNT_AND_SITE

categoryDisplayName (optional)

String

Displayed name of the notification policy category.

example: Account and Site notifications

subAccountsAppliedCount (optional)

Integer

The number of sub accounts that the parent account will receive notifications for, as specified by the

subAccountList parameter. format: int32

example: 12

subAccountsTotalCount (optional)

Integer

The number of sub accounts in the account. format: int32

example: 16

policyType (optional)

String

If value is 'ACCOUNT', the policy will apply only to the current account. If the value is 'SUB_ACCOUNT' the policy applies to the sub accounts only. The parent account will receive notifications for activity in the sub accounts that are specified in the subAccountList parameter. The 'SUB_ACCOUNT' value is available only in accounts that can contain sub accounts.

Enum:

ACCOUNT
SUB_ACCOUNT

NotificationPolicyUpdates

API response data
accountId (optional)

Long

Numerical value obtained by retrieving from PolicyDetails. format: int64

example: 534522

policyId

Long

Numerical value obtained by retrieving from PolicyDetails. format: int64

example: 231121

status

String

Indicates whether policy is enabled or disabled.

Enum:

ENABLE

DISABLE

Recipient

List of recipients

displayName (optional)

String

Indicates name of recipient of the notification.

example: John Doe

recipientType (optional)

String

Enum:

External

User

SubAccount

The parent account will receive notifications for activity in the specified sub accounts.

subAccountId

Long

Sub account ID. format: int64

example: 32424

displayName (optional)

String

The name of sub account.

example: Production EMEA Account

SubAccountPolicyInfo

If value of policyType is 'SUB_ACCOUNT', then the relevant sub accounts ids will be fill here.

applyToNewSubAccounts (optional)

String

If value is 'TRUE', all newly onboarded sub accounts are automatically added to the notification policy's sub account list.

Enum:

FALSE

TRUE

subAccountList (optional)

array[SubAccount]

The parent account will receive notifications for activity in the specified sub accounts.

SubCategoryDetails

API response data

sub_category_id (optional)

String

The notification policy subtype, such as SITE_NOTIFICATIONS.

example: SITE_NOTIFICATIONS

category (optional)

String

The notification policy type, such as ACCOUNT_AND_SITE.

Enum:

ACCOUNT_AND_SITE

APPLICATION_SECURITY_EVENTS

NETWORK_SECURITY

SYSTEM

example: ACCOUNT_AND_SITE

display_name (optional)

String

The display name of the notification policy subtype.

example: Website Notifications

connected_asset (optional)

String

The asset to receive notifications (if assets are relevant to the sub category type)

Enum:

SITE

IP_RANGE

EDGE_IP

ORIGIN_CONNECTIVITY

NETFLOW_EXPORTER

DOMAIN

example: SITE

UserRecipient

displayName (optional)

String

Indicates name of recipient of the notification.

example: John Doe

recipientType (optional)

String

Indicates whether recipient is an external or internal user.

isUserActive (optional)

Boolean

Indicates whether user is active.

isAccountAdmin (optional)

Boolean

Indicates whether user has Admin privileges for the account.

id (optional)

Long

Indicates the numeric value of the User ID. format: int64
example: 8765

Imperva SIEM Configurations API 3.0

Set up and manage the Imperva SIEM log integration.

- Create, view, and edit connections to your log storage repository.
- Configure which logs you want to receive from Imperva, and where to receive them.

For full feature documentation, see [Near Real-Time SIEM Log Integration](#).

Version: 1.0.0

BasePath:/siem-config-service

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Connections

- `post /v3/connections/`
- `delete /v3/connections/{connectionId}`
- `get /v3/connections/{connectionId}`
- `get /v3/connections/`
- `post /v3/connections/test-connection`
- `put /v3/connections/{connectionId}`

LogConfigurations

- `post /v3/log-configurations/`
- `delete /v3/log-configurations/{configurationId}`
- `get /v3/log-configurations/{configurationId}`
- `get /v3/log-configurations/`
- `put /v3/log-configurations/{configurationId}`

Connections

```
post /v3/connections/
```

Create connection (create1)

Define the details of your log storage repository including the path to the repository and the access credentials Imperva needs to push the logs.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ConnectionRequestWrapper (required)

Body Parameter

— JSON body containing connection information. Specify the relevant storage type schema according to the connection type. Possible storage types are: "CUSTOMER_S3"/ "CUSTOMER_S3_ARN"/ "CUSTOMER_SFTP"/ "CUSTOMER_SPLUNK

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

ConnectionResponseWrapper

Example data

Content-Type: application/json

```
{
  "data" : [ "", "" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created ConnectionResponseWrapper

Example data

Content-Type: S3 Basic Auth Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3", "connectionInfo": {"accessKey": "AKIAIOSFODNN7EXAMPLE", "secretKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY", "path": "/mybucket/logs"}}]}]
```

Example data

Content-Type: Splunk Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "Splunk Connection", "assetId": "12345678", "storageType": "CUSTOMER SPLUNK", "connectionInfo": {"host": "splunk.example.com", "port": 8088, "token": "12345678-1234-1234-1234-1234567890ab"}}]}]
```

Example data

Content-Type: SFTP Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "SFTP Connection", "assetId": "123456712138", "storageType": "CUSTOMER_SFTP", "connectionInfo": {"host": "sftp.example.com", "username": "user123", "password": "password123", "path": "/logs"}}]}]
```

Example data

Content-Type: S3 ARN Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 ARN Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3_ARN", "connectionInfo": {"path": "yourBucket/logs"}}]}]
```

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
delete /v3/connections/{connectionId}
```

Delete connection (delete1)

Deletes a connection according to the connection ID.

Path parameters

connectionId (required)

Path Parameter

— The unique ID for the connection, assigned by Imperva. To find the connection ID, run GET /v3/connections

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
get /v3/connections/{connectionId}
```

Retrieve connection (get1)

Retrieves details of a specific connection according to the connection ID.

Path parameters

connectionId (required)

Path Parameter

— The unique ID for the connection, assigned by Imperva. To find the connection ID, run GET /v3/connections

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ConnectionResponseWrapper](#)

Example data

Content-Type: application/json

```
{
  "data" : [ "", "" ]
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ConnectionResponseWrapper

Example data

Content-Type: S3 Basic Auth Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3", "connectionInfo": {"accessKey": "AKIAIOSFODNN7EXAMPLE", "secretKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY", "path": "/my bucket/logs"}}]}]
```

Example data

Content-Type: Splunk Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "Splunk Connection", "assetId": "12345678", "storageType": "CUSTOMER SPLUNK", "connectionInfo": {"host": "splunk.example.com", "port": 8088, "token": "12345678-1234-1234-1234-1234567890ab"}}]}]
```

Example data

Content-Type: SFTP Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "SFTP Connection", "assetId": "123456712138", "storageType": "CUSTOMER_SFTP", "connectionInfo": {"host": "sftp.example.com", "username": "user123", "password": "password123", "path": "/logs"}}]}]
```

Example data

Content-Type: S3 ARN Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 ARN Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3_ARN", "connectionInfo": {"path": "your Bucket/logs"}}]}]
```

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
get /v3/connections/
```

Retrieve all connections (getAll1)
Retrieves details of all connections in the account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ConnectionResponseWrapper](#)

Example data

Content-Type: application/json

```
{
  "data" : [ "", "" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [ConnectionResponseWrapper](#)

Example data

Content-Type: S3 Basic Auth Response

```
{"data": [ { "id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3", "connectionInfo": { "accessKey": "AKIAIOSFODNN7EXAMPLE", "secretKey": "wJalrXUtnFEMI/K7MDENG/bPxRfICYEXAMPLEKEY", "path": "/mybucket/logs" } } ] }
```

Example data

Content-Type: Splunk Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "Splunk Connection", "assetId": "12345678", "storageType": "CUSTOMER_SPLUNK", "connectionInfo": {"host": "splunk.example.com", "port": 8088, "token": "12345678-1234-1234-1234-1234567890ab"}}]}]
```

Example data

Content-Type: SFTP Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "SFTP Connection", "assetId": "123456712138", "storageType": "CUSTOMER_SFTP", "connectionInfo": {"host": "sftp.example.com", "username": "user123", "password": "password123", "path": "/logs"}}]}]
```

Example data

Content-Type: S3 ARN Response

```
{"data": [{"id": "6350f6f8be2e2a10af1d9de9", "connectionName": "S3 ARN Connection", "assetId": "12345678", "storageType": "CUSTOMER_S3_ARN", "connectionInfo": {"path": "yourBucket/logs"}}]}]
```

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status": 400, "id": "2da889aa00000000dea6da80b802440c", "code": "1037", "source": {"pointer": "/siem-config-service/v3/"}, "title": "Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status": 401, "id": "2da889aa00000000dea6da80b802440c", "code": "1031", "source": {"pointer": "/siem-config-service/v3/"}, "title": "Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
post /v3/connections/test-connection
```

Test connection (testConnection)

Test connection to destination storage.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ConnectionRequestWrapper (required)

Body Parameter

— JSON body containing connection information for testing.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
put /v3/connections/{connectionId}
```

Overwrite connection (update1)

Updates a connection according to the connection ID. Overwrites the connection's previous values.

Path parameters

connectionId (required)

Path Parameter

— The unique ID for the connection, assigned by Imperva. To find the connection ID, run GET /v3/connections

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ConnectionRequestWrapper (required)

Body Parameter

— JSON body containing connection information. Specify the relevant storage type schema according to the connection type. Possible storage types are: "CUSTOMER_S3"/ "CUSTOMER_S3_ARN"/ "CUSTOMER_SFTP"/ "CUSTOMER SPLUNK

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

ConnectionResponseWrapper

Example data

Content-Type: application/json

```
{
  "data" : [ "", "" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ConnectionResponseWrapper

Example data

Content-Type: S3 Basic Auth Response

```
{"data": [{"id":"6350f6f8be2e2a10af1d9de9", "connectionName":"S3 Connection", "assetId":"12345678", "storageType":"CUSTOMER_S3", "connectionInfo":{"accessKey":"AKIAIOSFODNN7EXAMPLE", "secretKey":"wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY", "path":"/my bucket/logs"}}]}]
```

Example data

Content-Type: Splunk Response

```
{"data": [{"id":"6350f6f8be2e2a10af1d9de9", "connectionName":"Splunk Connection", "assetId":"12345678", "storageType":"CUSTOMER SPLUNK", "connectionInfo":{"host":"splunk.example.com", "port":8088, "token":"12345678-1234-1234-1234-1234567890ab"}}]}]
```

Example data

Content-Type: SFTP Response

```
{"data": [{"id":"6350f6f8be2e2a10af1d9de9", "connectionName":"SFTP Connection", "assetId":"123456712138", "storageType":"CUSTOMER_SFTP", "connectionInfo":{"host":"sftp.example.com", "username":"user123", "password":"password123", "path":"/logs"}}]}]
```

Example data

Content-Type: S3 ARN Response

```
{"data": [{"id":"6350f6f8be2e2a10af1d9de9", "connectionName":"S3 ARN Connection", "a
```

```
ssetId":"12345678","storageType":"CUSTOMER_S3_ARN","connectionInfo": {"path": "your
Bucket/logs"} } ] }
```

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","s
ource":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","s
ource":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","s
ource":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","s
ource":{"pointer":"/siem-config-service/v3/"},"title":"Server Error"}]}
```

```
ource": {"pointer": "/siem-config-service/v3/"}, "title": "Internal Server Error"}]]}
```

LogConfigurations

```
post /v3/log-configurations/
```

Create log configuration (create)

Define the logs that you want to receive from Imperva, and the connection to use to receive them.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body LogConfigurationDtoResponse (required)

Body Parameter

— JSON body. Schema is identical to the response.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

LogConfigurationDtoResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "logType" : "WAF"
  } ]
}
```

```

    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
} , {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created LogConfigurationDtoResponse

400

Bad Request - Invalid request body or parameters APIError

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials APIError

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
delete /v3/log-configurations/{configurationId}
```

Delete log configuration (delete)

Deletes a log configuration according to the configuration ID.

Path parameters

configurationId (required)

Path Parameter

— The unique ID for the log configuration, assigned by Imperva. To find the configuration ID, run GET /v3/log-configurations

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"}, "title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"}, "title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"}, "title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"}, "title":"Internal Server Error"}]}
```

```
get /v3/log-configurations/{configurationId}
```

Retrieve log configuration (get)

Retrieves details of a specific log configuration according to the configuration ID.

Path parameters

configurationId (required)

Path Parameter

— The unique ID for the log configuration, assigned by Imperva. To find the configuration ID, run GET /v3/log-configurations

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[LogConfigurationDtoResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "logLevel" : "INFO"
  } ]
}
```

```

    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
} , {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK LogConfigurationDtoResponse

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
get /v3/log-configuration/
```

Retrieve all log configurations (getAll)
 Retrieves details of all configurations in the account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[LogConfigurationDtoResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
  }, {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK LogConfigurationDtoResponse

400

Bad Request - Invalid request body or parameters APIError

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"},"title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"},"title":"Internal Server Error"}]}
```

```
put /v3/log-configurations/{configurationId}
```

Overwrite log configuration (update)

Updates a log configuration according to the configuration ID. Overwrites the configuration's previous values.

Path parameters

configurationId (required)

Path Parameter

— The unique ID for the log configuration, assigned by Imperva. To find the configuration ID, run GET /v3/log-configurations

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body LogConfigurationDtoResponse (required)

Body Parameter

— JSON body. Schema is identical to the response.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

LogConfigurationDtoResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
  }, {
    "compressLogs" : true,
    "publicKeyFileName" : "my_public_key.pem",
    "provider" : "CLOUD_WAF",
    "assetId" : "52546656",
    "defaultSiteLogsLevel" : "NONE",
    "format" : "CEF",
    "configurationName" : "ABP configuration",
    "datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
    "id" : "6350f6f8be2e2a10af1d9de9",
    "publicKey" : "publicKey",
    "enabled" : true,
    "publicKeyId" : 0
  } ]
}
```

```

"assetId" : "52546656",
"defaultSiteLogsLevel" : "NONE",
"format" : "CEF",
"configurationName" : "ABP configuration",
"datasets" : [ "WAF_RAW_LOGS", "WAF_RAW_LOGS" ],
"id" : "6350f6f8be2e2a10af1d9de9",
"publicKey" : "publicKey",
"enabled" : true,
"publicKeyId" : 0
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [LogConfigurationDtoResponse](#)

400

Bad Request - Invalid request body or parameters [APIError](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"2da889aa00000000dea6da80b802440c","code":"1037","source":{"pointer":"/siem-config-service/v3/"},"title":"Bad Request"}]}
```

401

Unauthorized - Invalid or missing API credentials [APIError](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"2da889aa00000000dea6da80b802440c","code":"1031","source":{"pointer":"/siem-config-service/v3/"},"title":"Unauthorized"}]}
```

404

Not Found - Resource does not exist [APIError](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":"2da889aa00000000dea6da80b802440c","code":"1005","source":{"pointer":"/siem-config-service/v3/"}, "title":"Not Found"}]}
```

500

Internal Server Error [APIError](#)

Example data

Content-Type: Server Error

```
{"errors": [{"status":500,"id":"2da889aa00000000dea6da80b802440c","code":"1002","source":{"pointer":"/siem-config-service/v3/"}, "title":"Internal Server Error"}]}
```

Models

Methods

Table of Contents

1. [APIError](#)
2. [ArnConnectionInfo](#)
3. [ConnectionDto](#)
4. [ConnectionRequest](#)
5. [ConnectionRequestWrapper](#)
6. [ConnectionResponse](#)
7. [ConnectionResponseWrapper](#)
8. [CustomerS3ArnConnectionDto](#)
9. [CustomerS3BasicAuthDto](#)
10. [LogConfigurationDto](#)
11. [LogConfigurationDtoResponse](#)
12. [S3ConnectionInfo](#)
13. [SftpConnectionDto](#)
14. [SftpConnectionInfo](#)
15. [SplunkConnectionDto](#)
16. [SplunkConnectionInfo](#)

APIError

code (optional)
String
 detail (optional)
String
 id (optional)
String
 source (optional)
map[String, null]
 status (optional)
Integer
 format: int32
 title (optional)
String

ArnConnectionInfo

ARN connection information
 path (optional)
String
 The ARN path for S3.
 example: yourBucket/SIEM

ConnectionDto

assetId (optional)
String
 The Imperva ID for the account.
 example: 52546656
 connectionName
String
 Connection name. NOT required for /test-connection API
 example: Your Connection Name
 id (optional)
String
 Unique connection id.
 example: 6350f6f8be2e2a10af1d9de9
 storageType
String

ConnectionRequest**ConnectionRequestWrapper**

data (optional)
array[ConnectionRequest]
 Array containing a single connection object

ConnectionResponse**ConnectionResponseWrapper**

data (optional)

array[ConnectionResponse]
Array containing connection objects

CustomerS3ArnConnectionDto

Customer S3 Arn Connection details
assetId (optional)
String
The Imperva ID for the account.
example: 52546656
connectionName
String
Connection name. NOT required for /test-connection API
example: Your Connection Name
id (optional)
String
Unique connection id.
example: 6350f6f8be2e2a10af1d9de9
storageType
String
connectionInfo
[ArnConnectionInfo](#)

CustomerS3BasicAuthDto

Customer S3 Connection details
assetId (optional)
String
The Imperva ID for the account.
example: 52546656
connectionName
String
Connection name. NOT required for /test-connection API
example: Your Connection Name
id (optional)
String
Unique connection id.
example: 6350f6f8be2e2a10af1d9de9
storageType
String
connectionInfo (optional)
[S3ConnectionInfo](#)

LogConfigurationDto

assetId (optional)
String
The Imperva ID for the account.
example: 52546656
compressLogs (optional)
Boolean
Logs compression. Available only for Cloud WAF and Attack Analytics services
configurationName
String
Log configuration name.
example: ABP configuration

datasets
array[String]
Enum:
defaultSiteLogsLevel (optional)
String
Logs level for default site. Available only for Cloud WAF services
Enum:
NONE
FULL
SECURITY
enabled
Boolean
Enable / disable the log configuration
format (optional)
String
Optional, allowed only for CLOUD_WAF service
Enum:
W3C
CEF
LEEF
id (optional)
String
Unique log-configuration id.
example: 6350f6f8be2e2a10af1d9de9
provider
String
Provider of the log configuration
Enum:
CLOUD_WAF
ATTACK_ANALYTICS
ABP
NETSEC
AUDIT
ATO
CSP
DNS
DNSMS
API_Security
publicKey (optional)
String
Public key in case of logs encryption. Available only for Cloud WAF and Attack Analytics services
publicKeyFileName (optional)
String
Public key file name in case of adding a public key. Available only for Cloud WAF and Attack Analytics services
example: my_public_key.pem
publicKeyId (optional)
Long
format: int64

LogConfigurationDtoResponse

data (optional)
array[LogConfigurationDto]
Response data items

S3ConnectionInfo

S3 connection information

accessKey (optional)

String

The access key for S3.

example: <YOUR_ACCESS_KEY>

path (optional)

String

The secret key for S3.

example: yourBucket/SIEM

secretKey (optional)

String

The secret key for S3.

example: <YOUR_SECRET_KEY>

SftpConnectionDto

Customer SFTP Connection details

assetId (optional)

String

The Imperva ID for the account.

example: 52546656

connectionName

String

Connection name. NOT required for /test-connection API

example: Your Connection Name

id (optional)

String

Unique connection id.

example: 6350f6f8be2e2a10af1d9de9

storageType

String

connectionInfo

[SftpConnectionInfo](#)

SftpConnectionInfo

The connection info for SFTP.

host (optional)

String

The sftp host

example: sftp.my-company.com

password (optional)

String

The sftp password

example: myPassword123!

path

String

The sftp path

example: yourFolder/SIEM

username (optional)

String

The sftp username

example: myUser

SplunkConnectionDto

Customer Splunk Connection details

assetId (optional)

String

The Imperva ID for the account.

example: 52546656

connectionName

String

Connection name. NOT required for /test-connection API

example: Your Connection Name

id (optional)

String

Unique connection id.

example: 6350f6f8be2e2a10af1d9de9

storageType

String

connectionInfo

SplunkConnectionInfo

SplunkConnectionInfo

Splunk HEC connection information

host

String

Host name or IP address of your Splunk HEC endpoint.

example: splunk.my-company.com

port

Integer

The port number of the Splunk host. Valid values are in the range of 1-65535. format: int32

example: 8088

token

String

The Splunk HEC token in UUID version 4 format.

example: 550e8400-e29b-41d4-a716-446655440000

Simplified Site Onboarding with an Imperva Site Certificate

Easily onboard a new website with a dedicated SSL certificate provided by Imperva.

This simplified API flow for onboarding a site contains a single API call.

Note: To learn more about the benefits of site certificates, see [Imperva Site Certificates](#).

Prerequisites

- Your origin server must support TLS traffic.
- The following permissions are required for using this API:
 - Add sites
 - Manage site's SSL certificate configuration

-
- Edit origin settings

By default, the **Account Admin** user or any user with the default **Administrator** role can use the API.

Onboard a site

When onboarding an apex domain, Imperva automatically onboards its www subdomain as well, if one is detected according to an A or CNAME record in your DNS. Likewise, if the www domain is onboarded, the naked domain is onboarded as well. For example, example.com and www.example.com.

If the specified domain is configured in DNS to point to your website's servers, Imperva automatically identifies the origin servers and associates them with the new site. Alternatively, you can provide the site's origin server addresses (CNAME or IP) using the **servers** parameter.

The API response includes instructions for configuring your DNS. After you complete the DNS configuration and Imperva validates domain ownership, your site is onboard and protected by Imperva.

To onboard a site:

1. **Call the onboarding API:** <https://api.imperva.com/sites-mgmt/v3/sites/onboard>

Note: For full details on using the onboarding API, see the **Simplified Site Onboarding** section here: [Website Management API Definition](#).

For example:

```
curl --request POST 'https://api.imperva.com/sites-mgmt/v3/sites/onboard' \
--header 'x-API-Id: [API-ID]' \
--header 'x-API-Key: [API-KEY]' \
--header 'Content-Type: application/json' \
--data '{
    "domain": "example.com"
    "servers": ["1.2.3.4", "1.2.3.5"]
}'
```

To onboard a website to a subaccount, make sure to specify the sub account ID using the `caid` parameter.

2. **Complete domain validation:** Follow the **SSL instructions** returned in the API response to configure your DNS and complete the domain validation process. By default, Imperva validates your domain ownership using a CNAME record.

Validation may take several minutes.

You can confirm that validation is complete by polling the /v3/certificates API. For details, see [SSL Certificates API Definition](#).

You can also view the status on the Cloud Security Console **SSL Certificates** page. For details, see [Manage SSL Certificates](#).

You can then verify that SSL support was added for the domain as follows:

- a. Add the Imperva proxy IP address and the domain name to your local hosts file. You can identify the proxy IP according to the CNAME address that was provided by Imperva for the primary (onboarded) domain.
- b. In a browser, open <https://<added domain>> and check if there is a secure connection to confirm the process is complete.

3. Direct your domain's traffic to the Imperva network:

Follow the **Network instructions** returned in the API response to configure your DNS to reroute your domain's traffic through the Imperva network.

Note: By default, port 443 is used for SSL traffic. If your origin server supports SSL traffic on a different port, you can use the **Port Forwarding** option in **Delivery Settings** to redirect incoming requests **before** redirecting your traffic to Imperva.

Sample response

```
{
  "data": [
    {
      "site": {
        "id": 123456,
        "name": "www.example.com",
        "type": "CLOUD_WAF",
        "accountId": 10,
        "creationTime": 1673186130,
        "cname": "asdasd.ng.impervadns.net"
      },
      "domains": [
        {
          "id": 123456,
          "name": "www.example.com",
          "protectionStatus": "BYPASSED"
        }
      ],
      "servers": {
        "ips": [
          "1.2.3.4",
          "3.2.2.2"
        ]
      },
      "certificateSettings": {
        "validationMethod": "CNAME"
      },
    }
  ]
}
```

```

"instructions": {
  "SSL": [
    {
      "description": "Add the following record to your DNS provider",
      "recordType": "CNAME",
      "value": "qweqwe.ng.impervadns.net",
      "host": "_delegate_validation.example.com"
    }
  ],
  "Network": [
    {
      "description": "Add the following record to your DNS provider",
      "recordType": "A",
      "value": "1.2.3.4",
      "host": "example.com"
    },
    {
      "description": "Add the following record to your DNS provider",
      "recordType": "A",
      "value": "5.6.7.8",
      "host": "example.com"
    },
    {
      "description": "Add the following record to your DNS provider",
      "recordType": "CNAME",
      "value": "asdasd.ng.impervadns.net",
      "host": "www.example.com"
    }
  ]
}
}

```

After onboarding

Manage sites and certificates

After onboarding, you can view and manage the site in the Cloud Security Console.

- The newly configured site is displayed on the **Websites** page. For details, see [Web Protection - Websites](#).
- The certificate details are displayed on the **SSL Certificates** page. For details, see [Manage SSL Certificates](#).

Support for multiple domains

When a site certificate is issued, it initially covers only the site's domain. After the certificate is issued, you can manually add other domains to the site. When you add new domains, the certificate will automatically extend its coverage to include them.

You must explicitly add domains to your website configuration to ensure they're covered by your Site Certificate. Domains using the Imperva-provided CNAME but not explicitly adding the domain to the website configuration will not have SSL coverage.

For details on adding domains, see [Site Certificate Support for Multiple Domains](#).

Limitations and known issues

Functional limitations

- The simplified onboarding API initially supports a single domain, though additional domains can be added later through the API. For details, see [Site Certificate Support for Multiple Domains](#).
- Sites created using the simplified onboarding API do not support non-SNI client connections.
- The simplified onboarding API only supports site certificates. Custom certificates can be added later.
- Sites created using the v3 API do not support account certificates.
- IPv6 is not currently supported by the simplified API.
- After onboarding: Sites created using the v3 API do not support managed account certificates. As a result, when calling the `https://my.imperva.com/api/prov/v1/sites/configure` endpoint, you cannot use parameters related to account certificates:
 - `domain_validation`
 - `naked_domain_san`
 - `wildcard_san`

UI limitations

Configuration instructions are not available on the Cloud Security Console **Websites** page.

When a site is not yet fully configured, the configuration instructions are typically displayed when clicking on the icon in the **Status** column. For sites created using the simplified onboarding API, these instructions are not provided.

Known issues

- Using the simplified API to onboard an apex domain that does not have a www subdomain, and then completing the DNS configuration reports an incorrect status for the site. The status remains as **partially configured** when it is actually **fully configured**.
- In some cases, when the parent domain was already validated by Imperva, SSL instructions are still returned in the API response, even though they are not required. This can occur, for example, if the account is set up for automatic domain validation. For more details on automatic validation, see [Automatic Domain Validation for Imperva-Generated Certificates](#).

Advanced Site Onboarding with an Imperva Site Certificate

Onboard a new website with a dedicated SSL certificate provided by Imperva.

Use the Imperva version 3 RESTful APIs to onboard your site with high flexibility and control over the process.

Note: To learn more about the benefits of site certificates, see [Imperva Site Certificates](#).

Prerequisites

- Your origin server must support TLS traffic.
- The following permissions are required for using this API:
 - Add sites
 - Manage site's SSL certificate configuration
 - Edit origin settings

By default, the **Account Admin** user or any user with the default **Administrator** role can use the API.

Onboard a site

Onboarding a site includes creating and configuring the following entities:

1. Create a site
2. Create a domain
3. Create a data center
4. Create a certificate configuration
5. Complete certificate validation
6. Direct your domain traffic to the Imperva network

The following code snippets include executable examples:

Create a site

Sites are configured to support only SNI traffic. For more details, see [Create site in the Website Management API Definition](#).

```
curl --request POST 'https://api.imperva.com/sites-mgmt/v3/sites?caid=[ACCOUNT_ID]' \
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{"name": "MyDemoSite",
  "type": "CLOUD_WAF"}'
# Example response:
#
# {"data": [
#   {"id":373884525,
#    "name":"MyDemoSite",
#    "type":"CLOUD_WAF",
#    "accountId": [ACCOUNT_ID],
#    "creationTime":1713095076247,
#    "cname":"wgpctvw.ng.impervadns.net"} ]}
```

Create a domain

Create a domain entity to manage multiple domains with shared website settings and a single site certificate.

You can also add support for additional domains after onboarding the site. For details, see [Support for multiple domains](#).

The site will serve requests from the domains that are explicitly defined using this API. Certificate coverage will be provided only after domain ownership is validated. It can take up to 5 min for the certificate to be issued after the domain is added.

For more details, see [Add domain in the Website Domain Management API Definition](#).

```
curl -request POST 'https://api.imperva.com/site-domain-manager/v2/sites/{site_id}/domains?c...
--header 'x-api-key: [API_ID]' \
--header 'x-api-id: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{
    "domain": "mysite.example.com"
}'
# Example response:
#
#{
#    "id": 325066699,
#    "siteId": 375300046,
#    "domain": "mysite.example.com",
#    "managed": true,
#    "validationCode": "z55fqnl.ng.impervadns.net",
#    "cnameRedirectionRecord": "z55fqnl.ng.impervadns.net",
#    "status": "BYPASSED",
#    "creationDate": 1749389230371,
#    "aRecords": null
#}
```

Create a data center

This endpoint enables you to define your origin servers to which legitimate requests are directed.

For more details, see [Set site's data center configuration](#) in the Site Management API Definition.

```
curl --request PUT 'https://my.imperva.com/api/prov/v3/sites/[SITE_ID]/data-centers-configuration
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data ' {"data": [{"dataCenters": [
        {"name": "MyDataCenter",
         "servers": [{"address": "1.2.2.4"}]}]}]}'
```

Create a certificate configuration

This API call enables the managed certificate feature and configures the method used for validating domain ownership of the site. Once you create the domain (see the next step) the process of issuing the certificate is triggered.

For more details, see [Overwrite site certificate settings](#) in the SSL Certificates API Definition.

```
curl --request POST 'https://api.imperva.com/certificates-ui/v3/sites/[SITE_ID]/certificates
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{"siteId": [SITE_ID],
```

```

"defaultValidationMethod": "CNAME" },
"siteCertificateEnabled": true'
# Example response:
#
# {"data": [
#     {"siteId": [SITE_ID],
#      "defaultValidationMethod":
#      "CNAME", "certificateDetails": []} ]}
```

Complete certificate validation

If using the CNAME or DNS validation methods, the instructions for validating the domain are returned by the /v3/instructions API. The instructions become available only after the certificate is issued (up to 5 min after domain addition). Invoking the API before that will return an empty response.

For more details, see [Get domain validation instructions](#) in the SSL Certificates API Definition.

```

curl --request GET 'https://api.imperva.com/certificates-ui/v3/instructions?caid=[ACCOUNT_ID]
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{
    "caid": [ACCOUNT_ID],
    "extSiteId": [SITE_ID]
}'

# {"data": [{"domain": "delegate_validation.mysite1704352668.877465.incapitest.co",
#             "validationMethod": "CNAME",
#             "recordType": "CNAME",
#             "verificationCode": "5g9juwj.ng.impervadnsstage.net",
#             "verificationCodeExpirationDate": 1706944763000,
#             "lastNotificationDate": 1704352883000,
#             "relatedSansDetails": [{"sanId": 389842, "sanValue": "mysite1704352668.877465.incapitest.co"}]}}
```

Note: The site is only published after you have added the data center and domain.

For sites using CNAME validation, the domain is validated only after data center is added.

Direct your domain traffic to Imperva

Use the information returned in the domain creation API response to configure your DNS to reroute your domain's traffic through the Imperva network.

Note: By default, port 443 is used for SSL traffic. If your origin server supports SSL traffic on a different port, you can use the **Port Forwarding** option in [Delivery Settings](#) to redirect incoming requests **before** redirecting your traffic to Imperva.

For more details, see [Create a domain](#) above, or [Website Domain Management API Definition](#).

After onboarding

Manage sites and certificates

After onboarding, you can view and manage the site in the Cloud Security Console.

- The newly configured site is displayed on the **Websites** page. For details, see [Web Protection - Websites](#).
- The certificate details are displayed on the **SSL Certificates** page. For details, see [Manage SSL Certificates](#).

Support for multiple domains

When a site certificate is issued, it covers all domains that were previously added to the site. After the certificate is issued, you can manually add other domains to the site. When you add new domains, the certificate will automatically extend its coverage to include them.

You must explicitly add domains to your website configuration to ensure they're covered by your Site Certificate. Domains using the Imperva-provided CNAME but not explicitly adding the domain to the website configuration will not have SSL coverage.

For details on adding domains, see [Site Certificate Support for Multiple Domains](#).

Limitations and known issues

Functional limitations

- A site onboarded using this API configures a site certificate for the site. No other certificate type is supported during the onboarding process. After the certificate is issued and onboarding is complete, you can upload a custom certificate for the site if needed. Account certificates are not supported.
- Sites created using this v3 onboarding API do not support non-SNI client connections.
- IPv6 is not currently supported.
- The v1/v2 data center APIs are not supported.
- Apex domains:
 - Using the v3 API to onboard an apex domain that does not have a www subdomain, and then completing the DNS configuration reports an incorrect status for the site. The status remains as **partially configured** when it is actually **fully configured**.
 - You may be required to configure a CNAME record on the apex domain's www subdomain, in addition to configuring an A record on the apex domain. If the apex domain is the first one added to the site, or the apex domain is the apex of a www domain that was added as the first domain, an A record on the apex domain should be sufficient.
- Mock entities: Newly created sites are not associated with any domain or data center. Due to technical limitations, Imperva associates mock entities with the site. They are visible in some APIs and UI screens, but are replaced when you created your actual domain and data centers.
- After onboarding: Sites created using the v3 API do not support managed account certificates. As a result, when calling the `https://my.imperva.com/api/prov/v1/sites/configure` endpoint, you cannot use parameters related to account certificates:
 - `domain_validation`
 - `naked_domain_san`

-
- wildcard_san

UI limitations

Configuration instructions are not available on the Cloud Security Console **Websites** page.

When a site is not yet fully configured, the configuration instructions are typically displayed when clicking on the icon in the **Status** column. For sites created using the simplified onboarding API, these instructions are not provided.

Site Onboarding with a Custom Certificate

Onboard a new website with a custom certificate using the Imperva version 3 RESTful APIs. This method allows you to onboard your site with high flexibility and control over the process.

Prerequisites

- The certificate must meet certain requirements. For details, see [Upload a Custom Certificate for Your Website on Imperva](#).
- Your origin server must support TLS traffic.
- The following permissions are required for using this API:
 - Add sites
 - Edit origin settings
 - Upload custom certificate

By default, the **Account Admin** user or any user with the default **Administrator** role can use the API.

Onboard a site

Onboarding a site includes creating and configuring the following entities:

1. Create a site
2. Create a domain
3. Create a data center
4. Upload a custom certificate
5. Direct your domain traffic to the Imperva network

The following code snippets include executable examples:

Create a site

Sites are configured to support only SNI traffic. For more details, see [Website Management API Definition](#).

```
curl --request POST 'https://api.imperva.com/sites-mgmt/v3/sites?caid=[ACCOUNT_ID]' \
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{"name": "MyDemoSite", "type": "CLOUD_WAF"}'
# Example response:
#
# {"data": [
#   {"id":373884525, "name": "MyDemoSite", "type": "CLOUD_WAF", "accountId": [ACCOUNT_ID], "creationTime": 1713095076247, "cname": "wgpcvww.ng.impervadns.net"} ]}
```

Create a domain

Only a single domain can be added (although you can add both an apex domain and its www subdomain).

The site will serve requests only from the domain that is explicitly defined using this API. Certificate coverage will be provided only after domain ownership is validated. It can take up to 5 min for the certificate to be issued after the domain is added.

For more details, see [Website Domain Management API Definition](#).

```
curl --request POST 'https://api.imperva.com/site-domain-manager/v2/sites/[SITE_ID]/domains?' \
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data '{
      "domain": "shiri3.incapcwfteam.net"
    }'
# Example response:
#
# {
#   "id": 48367189,
#   "siteId": [SITE_ID],
#   "domain": "shiri3.incapcwfteam.net",
#   "mainDomain": true,
#   "managed": true,
#   "validationCode": "wgpcvww.ng.impervadns.net",
#   "cnameRedirectionRecord": "wgpcvww.ng.impervadns.net",
#   "status": "BYPASSED",
#   "creationDate": 1713096303954,
#   "aRecords": ["45.223.102.204", "45.223.117.204"]
# }
```

Create a data center

This endpoint enables you to define your origin servers to which legitimate requests are directed.

For more details, see [/api/prov/v3/sites/{extSiteId}/data-centers-configuration here](#).[Site Management API](#).

```
curl --request PUT 'https://my.imperva.com/api/prov/v3/sites/[SITE_ID]/data-centers-configurations' \
--header 'x-API-Id: [API_ID]' \
--header 'x-API-Key: [API_KEY]' \
--header 'Content-Type: application/json' \
--data ' {"data": [{"dataCenters": [
    {"name": "MyDataCenter",
     "servers": [{"address": "1.2.2.4"}]}]}]}'
```

Upload your custom certificate

This endpoint enables you to upload your own SSL certificate to Imperva so it can be presented to your website visitors. Custom certificates are presented to SNI-supporting clients only.

Before you begin, make sure that your certificate meets all the requirements listed here: [Upload a Custom Certificate for Your Website on Imperva](#).

For more details on this API, see [Custom Certificates API Definition](#).

```
curl --request PUT 'https://my.impervaservices.com/api/prov/v2/sites/[SITE_ID]/customCertificates' \
--header 'X-API-Key: [API_KEY]' \
--header 'X-API-Id: [API_ID]' \
--header 'Content-Type: application/json' \
--data ' {"certificate": "[CUSTOM_CERT_CONTENT]", \
         "private_key": "[PRIVATE_KEY]", \
         "auth_type": "RSA"}'
```

Direct your domain traffic to Imperva

Use the information returned in the domain creation API response to configure your DNS to reroute your domain's traffic through the Imperva network.

For more details, see [Create a domain](#) above, or [Website Domain Management API Definition](#)

After onboarding

After onboarding, you can view and manage the site in the Cloud Security Console.

- The newly configured site is displayed on the **Websites** page. For details, see [Web Protection - Websites](#).
- The certificate details are displayed on the **SSL Certificates** page. For details, see [Manage SSL Certificates](#).

Note: By default, port 443 is used for SSL traffic. Once the new site is fully configured and the certificate has been issued, you can use the **Port Forwarding** option to redirect incoming requests to a different port. For details, see [Delivery Settings](#).

Limitations and known issues

Functional limitations

- Only a single domain can be added (although you can add both an apex domain and its www subdomain).
- IPv6 is not currently supported.
- A site onboarded using these APIs can have a site certificate or a custom certificate. Account certificates are not supported.
- The v1/v2 data center APIs are not supported.
- Using the v3 API to onboard an apex domain that does not have a www subdomain, and then completing the DNS configuration reports an incorrect status for the site. The status remains as **partially configured** when it is actually **fully configured**.
- Mock entities: Newly created sites are not associated with any domain or data center. Due to technical limitations, Imperva associates mock entities with the site. They are visible in some APIs and UI screens, but are replaced when you created your actual domain and data centers.
- After onboarding: Invoking the <https://my.imperva.com/api/prov/v1/sites/configure> endpoint with the following parameters is not supported:
 - domain_validation
 - naked_domain_san
 - wildcard_san

UI limitations

Configuration instructions are not available on the Cloud Security Console **Websites** page. When a site is not yet fully configured, the configuration instructions are typically displayed when clicking on the icon in the **Status** column. For sites created using the simplified onboarding API, these instructions are not provided.

Sites management API Documentation

Get details of your websites configured in Imperva.

Version: 1.0.0

BasePath:/sites-mgmt

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountTLSConfiguration

- `get /v3/accounts/settings/default-tls-configuration`
- `put /v3/accounts/settings/default-tls-configuration`

SPA API

- `get /v3/sites/{siteId}/site-settings`
- `get /v3/sites/spa/{siteId}`
- `put /v3/sites/{siteId}/site-settings`
- `put /v3/sites/spa/{siteId}`

Simplified Site Onboarding

- `post /v3/sites/onboard`

Site Management

- `delete /v3/sites/{siteId}`
- `get /v3/sites/extended`
- `get /v3/sites/{siteId}`
- `get /v3/sites`
- `post /v3/sites`

Website TLS Configuration

- `get /v3/sites/{siteId}/settings/TLSConfiguration`
- `patch /v3/sites/{siteId}/settings/TLSConfiguration`

AccountTLSConfiguration

```
get /v3/accounts/settings/default-tls-configuration
```

Get account default TLS configuration settings. (getAccountDefaultInboundTLSConfiguration)
Get account default TLS configuration settings by account ID.

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AccountInboundTLSConfigurationRequest](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "tlsConfiguration" : [ {
      "tlsVersion" : "TLS_1_0",
      "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
    }, {
      "tlsVersion" : "TLS_1_0",
      "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
    } ],
    "configurationProfile" : "CUSTOM"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AccountInboundTLSConfigurationRequest](#)

Example data

Content-Type: InboundTlsSettingsDto

```
{"data": [{"configurationProfile": "CUSTOM", "tlsConfiguration": [{"tlsVersion": "TLS_1_3", "ciphersSupport": ["TLS_AES_128_GCM_SHA256", "TLS_CHACHA20_POLY1305_SHA256"]}] } ] }
```

400Bad Request [ErrorResponse](#)**401**Unauthorized [ErrorResponse](#)**404**Not Found [ErrorResponse](#)**500**Internal Error [ErrorResponse](#)

```
put /v3/accounts/settings/default-tls-configuration
```

Define account default TLS configuration settings. (setAccountDefaultInboundTLSConfiguration)

Update the account default TLS configuration. This configuration will be applied to new websites created directly under the specified account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request bodybody [AccountInboundTLSConfigurationRequest](#) (required)

Body Parameter

—

example: {

```
"description" : "Sets custom ciphers profile with support for just TLS v1.3 and specific list of ciphers.",
"value" : {
  "data" : [ {
    "configurationProfile" : "CUSTOM",
    "tlsConfiguration" : [ {
      "tlsVersion" : "TLS_1_3",
      "ciphersSupport" : [ "TLS_AES_128_GCM_SHA256", "TLS_CHACHA20_POLY1305_SHA256" ]
    } ]
  } ]
}
```

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation

Example data

Content-Type: SPA

```
{"data": [{"configurationProfile": "CUSTOM", "tlsConfiguration": [{"tlsVersion": "TLS_1_3", "ciphersSupport": ["TLS_AES_128_GCM_SHA256", "TLS_CHACHA20_POLY1305_SHA256"]}]}]}
```

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

SPAAPI

```
get /v3/sites/{siteId}/site-settings
```

Get site SPA settings (getSiteSpaDataFull)
Retrieves the SPA settings for a given website.

Path parameters

siteld (required)
Path Parameter
— The Imperva site ID of your website. format: int64

Query parameters

caid (optional)
Query Parameter
— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

SiteSpaFullSettingsV3ResponseDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "urlList" : [ "/url1", "/url2", "/url3" ],
    "state" : "SPA_FOR_SPECIFIC_URLS"
  }, {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "urlList" : [ "/url1", "/url2", "/url3" ],
    "state" : "SPA_FOR_SPECIFIC_URLS"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation [SiteSpaFullSettingsV3ResponseDto](#)

400

Bad Request [ErrorResponse](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":null,"source":{"pointer":"/v3/sites/16612920 /settings/spa"},"title":"Bad Request","detail":"Failed to get site spa info. Message: Bad Request"}]}
```

401

Unauthorized [ErrorResponse](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"ba34a964fe9a1887","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Unauthorized","detail":"Failed to verify permissions"}]}
```

404

Not Found [ErrorResponse](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":null,"source":{"pointer":"/v3/sites/16/settings/spa"},"title":"Not Found","detail":"Failed to get site spa info. Message: Not Found"}]}
```

500

Internal Server Error [ErrorResponse](#)

Example data

Content-Type: Internal Server Error

```
{"errors": [{"status":500,"id":"1dce2fbdec3e60e2","source":{"pointer":"/v3/sites/16612922/settings/spa"},"title":"Internal Server Error","detail":"Internal Server Error"}]}
```

```
get /v3/sites/spa/{siteId}
```

Get site SPA settings (getSiteSpaSettings)
Retrieves the SPA settings for a given website.

Path parameters

siteld (required)

Path Parameter

— The Imperva site ID of your website. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

SiteSpaSettingsApiResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "state" : true
  }, {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "state" : true
  } ]
}
```

```

        "state" : true
    } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation [SiteSpaSettingsApiResponse](#)

400

Bad Request [ErrorResponse](#)

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":null,"source":{"pointer":"/v3/sites/16612920 /settings/spa"},"title":"Bad Request","detail":"Failed to get site spa info. Message: Bad Request"}]}
```

401

Unauthorized [ErrorResponse](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"ba34a964fe9a1887","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Unauthorized","detail":"Failed to verify permissions"}]}
```

404

Not Found [ErrorResponse](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status": 404, "id": null, "source": {"pointer": "/v3/sites/16/settings/spa"}, "title": "Not Found", "detail": "Failed to get site spa info. Message: Not Found"}]}
```

500

Internal Server Error [ErrorResponse](#)

Example data

Content-Type: Internal Server Error

```
{"errors": [{"status": 500, "id": "1dce2fbdec3e60e2", "source": {"pointer": "/v3/sites/16612922/settings/spa"}, "title": "Internal Server Error", "detail": "Internal Server Error"}]}
```

```
put /v3/sites/{siteId}/site-settings
```

Update site SPA settings ([modifySiteSpaDataFull](#))
Updates the SPA settings for a given website.

Path parameters

siteld (required)

Path Parameter

— The Imperva site ID of your website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body SiteSpaFullSettingsDto (required)

Body Parameter

example: {

```
"description" : "Defines the whole site as a single-page application.",
"value" : {
    "state" : "SPA"
}
```

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[SiteSpaFullSettingsV3ResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "urlList" : [ "/url1", "/url2", "/url3" ],
    "state" : "SPA_FOR_SPECIFIC_URLS"
  }, {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "urlList" : [ "/url1", "/url2", "/url3" ],
    "state" : "SPA_FOR_SPECIFIC_URLS"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Successful operation [SiteSpaFullSettingsV3ResponseDto](#)

Example data

Content-Type: SPA

```
{"data": [{"state": "SPA"}]}
```

Example data

Content-Type: SPA_FOR_SPECIFIC_URLS

```
{"data": [{"state": "SPA_FOR_SPECIFIC_URLS", "urlList": ["/test1", "/test2"]}]}
```

400

Bad Request ErrorResponse

Example data

Content-Type: Null state

```
{"errors": [{"status": 400, "id": "787d252e08cd99ad", "source": {"pointer": "/v3/sites/16612920/settings/spa"}, "title": "Invalid Input Error", "detail": "state State must not be null!"} ]}
```

Example data

Content-Type: NOT_SPA state with not empty url list

```
{"errors": [{"status": 400, "id": "0949bee81d4bce3f", "source": {"pointer": "/v3/sites/16612920/settings/spa"}, "title": "Bad Request", "detail": "Url list must be empty when site state is NOT_SPA"}]}
```

Example data

Content-Type: Bad Request

```
{"errors": [{"status": 400, "id": null, "source": {"pointer": "/v3/sites/16612920/settings/spa"}, "title": "Bad Request", "detail": "Failed to get site spa info. Message: Bad Request"}]}
```

Example data

Content-Type: Null value for url

```
{"errors": [{"status": 400, "id": "358eebec0102e42c", "source": {"pointer": "/v3/sites/16612920/settings/spa"}, "title": "Bad Request", "detail": "Invalid value for URL, exp"}]}
```

```
ecting a not null string surrounded by quotes"}]} }
```

401

Unauthorized [ErrorResponse](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"ba34a964fe9a1887","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Unauthorized","detail":"Failed to verify permissions"}]} }
```

404

Not Found [ErrorResponse](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":null,"source":{"pointer":"/v3/sites/16/settings/spa"},"title":"Not Found","detail":"Failed to get site spa info. Message: Not Found"}]} }
```

500

Internal Server Error [ErrorResponse](#)

Example data

Content-Type: Internal Server Error

```
{"errors": [{"status":500,"id":"1dce2fbdec3e60e2","source":{"pointer":"/v3/sites/16612922/settings/spa"},"title":"Internal Server Error","detail":"Internal Server Error"}]} }
```

```
put /v3/sites/spa/{siteId}
```

Update site SPA settings (modifySiteSpaSettings)
Updates the SPA settings for a given website.

Path parameters

siteld (required)

Path Parameter

— The Imperva site ID of your website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body SiteSpaSettingsDto (required)

Body Parameter

example: {

```
"description" : "Defines the whole site as a single-page application.",
"value" : {
    "state" : "SPA"
}
}
```

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

SiteSpaSettingsApiResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "state" : true
  }, {
    "prodVersion" : "1.1",
    "preProdSettings" : {
      "headers" : [ "header1", "header2", "header3" ],
      "preProdVersion" : "1.1"
    }
  } ]
}
```

```

        "preProdVersion" : "1.1"
    },
    "allowedSpaDomains" : [ "allowedSpaDomains", "allowedSpaDomains" ],
    "state" : true
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation SiteSpaSettingsApiResponse

Example data

Content-Type: SPA

```
{"data": [{"state": "SPA"}]}
```

Example data

Content-Type: SPA_FOR_SPECIFIC_URLS

```
{"data": [{"state": "SPA_FOR_SPECIFIC_URLS", "urlList": ["/test1", "/test2"]}]}
```

400

Bad Request ErrorResponse

Example data

Content-Type: Null state

```
{"errors": [{"status": 400, "id": "787d252e08cd99ad", "source": {"pointer": "/v3/sites/16612920/settings/spa"}, "title": "Invalid Input Error", "detail": "state State must not be null!"}]}
```

Example data

Content-Type: NOT_SPA state with not empty url list

```
{"errors": [{"status":400,"id":"0949bee81d4bce3f","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Bad Request","detail":"Url list must be empty when site state is NOT_SPA"}]}
```

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":null,"source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Bad Request","detail":"Failed to get site spa info. Message: Bad Request"}]}
```

Example data

Content-Type: Null value for url

```
{"errors": [{"status":400,"id":"358eebec0102e42c","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Bad Request","detail":"Invalid value for URL, expecting a not null string surrounded by quotes"}]}
```

401

Unauthorized [ErrorResponse](#)

Example data

Content-Type: Unauthorized

```
{"errors": [{"status":401,"id":"ba34a964fe9a1887","source":{"pointer":"/v3/sites/16612920/settings/spa"},"title":"Unauthorized","detail":"Failed to verify permissions"}]}
```

404

Not Found [ErrorResponse](#)

Example data

Content-Type: Not Found

```
{"errors": [{"status":404,"id":null,"source":{"pointer":"/v3/sites/16/settings/spa"},"title":"Not Found","detail":"Failed to get site spa info. Message: Not Found"}]}
```

500

Internal Server Error [ErrorResponse](#)

Example data

Content-Type: Internal Server Error

```
{"errors": [{"status":500,"id":"1dce2fbdec3e60e2","source":{"pointer":"/v3/sites/16612922/settings/spa"},"title":"Internal Server Error","detail":"Internal Server Error"}]}]
```

SimplifiedSiteOnboarding

```
post /v3/sites/onboard
```

Simplified site onboarding (postSiteController)
Quickly onboard a website with a single API call.

If the specified domain is configured in DNS to point to your website's servers, Imperva automatically identifies the origin servers and associates them with the new site. If the specified domain is not configured in your DNS, you must provide the site's origin server addresses using the servers parameter. The created website automatically receives SSL coverage served by an Imperva-managed certificate dedicated to this site.

The API response includes all the REST entities that are created during the onboarding process (site, domains, servers, and certificate settings). The response also includes instructions comprised of 2 parts: SSL and Network.

The SSL instructions describe how to configure your DNS in order to complete the domain ownership validation process. By default, domain ownership validation is done using a CNAME record.

The Network section provides instructions on how to direct your domain's traffic to the Imperva network.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [SiteOnboardingRequest](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

CollectionSiteOnboardResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "instructions" : {
      "Network" : [ {
        "description" : "Add the following record to your DNS provider",
        "host" : "example.com",
        "recordType" : "A",
        "value" : "1.2.3.4"
      }, {
        "description" : "Add the following record to your DNS provider",
        "host" : "example.com",
        "recordType" : "A",
        "value" : "5.6.7.8"
      }, {
        "description" : "Add the following record to your DNS provider",
        "host" : "www.example.com",
        "recordType" : "CNAME",
        "value" : "asdasd.ng.impervadns.net"
      } ],
      "SSL" : [ {
        "description" : "Add the following record to your DNS provider",
        "host" : "_delegate_validation.example.com",
        "recordType" : "CNAME",
        "value" : "qweqwew.ng.impervadns.net"
      } ]
    },
    "certificateSettings" : {
      "validationMethod" : "CNAME"
    },
    "site" : {
      "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
      "accountId" : 10,
      "creationTime" : 1673186130,
      "isDefaultSite" : false,
      "siteStatus" : "CONFIGURED",
      "cname" : "sdh5s.example.com",
      "name" : "www.example.com",
      "active" : true,
      "id" : 123456,
      "refId" : "123abc",
      "type" : "CLOUD_WAF"
    },
    "servers" : {
      "ips" : [ "1.2.3.4", "3.2.2.2" ]
    },
    "domains" : [ {
      "name" : "www.example.com",
      "protectionStatus" : "BYPASSED",
      "id" : 123456
    }
  }
}
```

```

}, {
  "name" : "www.example.com",
  "protectionStatus" : "BYPASSED",
  "id" : 123456
} ]
}, {
  "instructions" : [
    "Network" : [ {
      "description" : "Add the following record to your DNS provider",
      "host" : "example.com",
      "recordType" : "A",
      "value" : "1.2.3.4"
    }, {
      "description" : "Add the following record to your DNS provider",
      "host" : "example.com",
      "recordType" : "A",
      "value" : "5.6.7.8"
    }, {
      "description" : "Add the following record to your DNS provider",
      "host" : "www.example.com",
      "recordType" : "CNAME",
      "value" : "asdasd.ng.impervadns.net"
    }],
    "SSL" : [ {
      "description" : "Add the following record to your DNS provider",
      "host" : "_delegate_validation.example.com",
      "recordType" : "CNAME",
      "value" : "qweqwew.ng.impervadns.net"
    }]
},
  "certificateSettings" : {
    "validationMethod" : "CNAME"
  },
  "site" : {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  },
  "servers" : {
    "ips" : [ "1.2.3.4", "3.2.2.2" ]
  },
  "domains" : [ {
    "name" : "www.example.com",
    "protectionStatus" : "BYPASSED",
    "id" : 123456
  }, {
    "name" : "www.example.com",
    "protectionStatus" : "BYPASSED",
    "id" : 123456
  }]
}
]
}

```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [CollectionSiteOnboardResponse](#)

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

SiteManagement

```
delete /v3/sites/{siteId}
```

Delete site (deleteSite)

Delete an existing site

Path parameters

siteId (required)

Path Parameter

— Numeric identifier of the site. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

CollectionSite

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  }, {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [CollectionSite](#)

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

```
get /v3/sites/extended
```

Extended get sites (extendedGetSites)

Retrieve details of all websites associated with the current account.

To filter for a subset of the account's websites, provide website IDs and website names.

If multiple filters are provided, an AND operation is applied and the API will return all websites matching the filters.

Query parameters

sitelds (optional)

Query Parameter

— A list of website ids. If this parameter is provided, only websites matching one of these IDs will be returned.

format: int64

names (optional)

Query Parameter

— A list of website names. If this parameter is provided, only websites matching one of these names will be returned.

siteTypes (optional)

Query Parameter

— A list of website types. Indicates if the website is onboarded to Imperva Cloud WAF or configured for Imperva WAF Anywhere. If this parameter is provided, only websites with type matching one of these types will be returned.

subAccIds (optional)

Query Parameter

— A list of sub account IDs. When provided, the API returns websites corresponding to the specified sub account IDs. This parameter is ignored if the API call is authenticated as a sub account. format: int64

page (optional)

Query Parameter

— The page to return starting from 0. default: 0 format: int32

size (optional)

Query Parameter

— Page size used to determine the first object to be returned and the number of objects to be returned. default:

10 format: int32

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

PaginatedCollectionSite

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  }, {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  } ],
  "meta" : {
    "size" : 6,
    "totalPages" : 5,
    "page" : 0,
    "totalElements" : 1
  },
  "links" : {
    "key" : "links"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [PaginatedCollectionSite](#)

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

```
get /v3/sites/{siteId}
```

Get site (getSite)
Retrieve details of a website according to its Imperva ID

Path parameters

siteId (required)

Path Parameter

— Numeric identifier of the site. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

CollectionSite

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  }, {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation CollectionSite

400

Bad Request ErrorResponse

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

[Internal Error ErrorResponse](#)

```
get /v3/sites
```

Get sites (getSites)

Retrieve details of all websites associated with the current account.

To filter for a subset of the account's websites, provide website IDs and website names.

If multiple filters are provided, an AND operation is applied and the API will return all websites matching the filters.

Query parameters

sitelds (optional)

Query Parameter

— A list of website ids. If this parameter is provided, only websites matching one of these IDs will be returned.

format: int64

names (optional)

Query Parameter

— A list of website names. If this parameter is provided, only websites matching one of these names will be returned.

siteTypes (optional)

Query Parameter

— A list of website types. Indicates if the website is onboarded to Imperva Cloud WAF or configured for Imperva WAF Anywhere. If this parameter is provided, only websites with type matching one of these types will be returned.

subAccts (optional)

Query Parameter

— A list of sub account IDs. When provided, the API returns websites corresponding to the specified sub account IDs. This parameter is ignored if the API call is authenticated as a sub account. format: int64

page (optional)

Query Parameter

— The page to return starting from 0. default: 0 format: int32

size (optional)

Query Parameter

— Page size used to determine the first object to be returned and the number of objects to be returned. default:

10 format: int32

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[PaginatedCollectionSite](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  }, {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  } ],
  "meta" : {
    "size" : 6,
    "totalPages" : 5,
    "page" : 0,
    "totalElements" : 1
  },
  "links" : {
    "key" : "links"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation PaginatedCollectionSite

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

```
post /v3/sites
```

Create site (postSite)

Create site associated with the current account

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [Site](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[CollectionSite](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  }, {
    "deploymentKeys" : "4d0654aa-8d16-46f6-8158-a42a1b48e48b",
    "accountId" : 10,
    "creationTime" : 1673186130,
    "isDefaultSite" : false,
    "siteStatus" : "CONFIGURED",
    "cname" : "sdh5s.example.com",
    "name" : "www.example.com",
    "active" : true,
    "id" : 123456,
    "refId" : "123abc",
    "type" : "CLOUD_WAF"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [CollectionSite](#)

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500[Internal Error ErrorResponse](#)

WebsiteTLSConfiguration

```
get /v3/sites/{siteId}/settings/TLSConfiguration
```

Get website TLS configuration settings (getSiteTLSConfiguration)
 Get website tls configuration settings by website id

Path parameters

siteId (required)
 Path Parameter
 — Numeric identifier of the website. format: int64

Query parameters

caid (optional)
 Query Parameter
 — The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[SiteTLSConfigurationRequest](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "disablePQCSupport" : false,
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
      "subDomainsIncluded" : false,
      "preLoaded" : false
    },
    "inboundTlsSettings" : {
      "tlsConfiguration" : [ {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      }, {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      } ],
      "configurationProfile" : "CUSTOM"
    }
  } ]
```

```
    } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [SiteTLSConfigurationRequest](#)

Example data

Content-Type: SPA

```
{"data": [{"hstsConfiguration": {"preLoaded": false, "maxAge": 7543, "subDomainsInclude": false, "isEnabled": true}, "inboundTlsSettings": {"configurationProfile": "CUSTOM", "tlsConfiguration": [{"tlsVersion": "TLS_1_3", "ciphersSupport": ["TLS_AES_128_GCM_SHA256", "TLS_CHACHA20_POLY1305_SHA256"]}], "disablePQCSupport": false}}]}
```

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

[Internal Error](#) [ErrorResponse](#)

```
patch /v3/sites/{siteId}/settings/TLSConfiguration
```

Modify website TLS configuration settings (partial update) ([setSiteTLSConfiguration](#))
Update TLS settings of an existing website. Only fields that are sent in the request will be updated.

Path parameters

`siteld` (required)
 Path Parameter
 — Numeric identifier of the website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SiteTLSConfigurationRequest` (required)
 Body Parameter

example: {

```

    "description" : "Enables and configure HSTS and sets custom ciphers profile w
ith support for just TLS v1.3 and specific list of ciphers.",
    "value" : {
        "data" : [ {
            "hstsConfiguration" : {
                "preLoaded" : false,
                "maxAge" : 7543,
                "subDomainsIncluded" : false,
                "isEnabled" : true
            },
            "inboundTlsSettings" : {
                "configurationProfile" : "CUSTOM",
                "tlsConfiguration" : [ {
                    "tlsVersion" : "TLS_1_3",
                    "ciphersSupport" : [ "TLS_AES_128_GCM_SHA256", "TLS_CHACHA20_POLY130
5_SHA256" ]
                } ]
            },
            "disablePQCSupport" : false
        } ]
    }
}
```

Query parameters

`caid` (optional)
 Query Parameter
 — The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`CollectionSiteTLSConfiguration`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "disablePQCSupport" : false,
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
      "subDomainsIncluded" : false,
      "preLoaded" : false
    },
    "inboundTlsSettings" : {
      "tlsConfiguration" : [ {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      }, {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      } ],
      "configurationProfile" : "CUSTOM"
    }
  }, {
    "disablePQCSupport" : false,
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
      "subDomainsIncluded" : false,
      "preLoaded" : false
    },
    "inboundTlsSettings" : {
      "tlsConfiguration" : [ {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      }, {
        "tlsVersion" : "TLS_1_0",
        "ciphersSupport" : [ "ciphersSupport", "ciphersSupport" ]
      } ],
      "configurationProfile" : "CUSTOM"
    }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [CollectionSiteTLSConfiguration](#)

400

Bad Request [ErrorResponse](#)

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

500

Internal Error [ErrorResponse](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [AccountInboundTLSConfigurationRequest](#)
 3. [CertificateSettings](#)
 4. [CollectionSite](#)
 5. [CollectionSiteOnboardResponse](#)
 6. [CollectionSiteTLSConfiguration](#)
 7. [DnsOnboardingInstructionDto](#)
 8. [Domain](#)
 9. [ErrorResponse](#)
 10. [InboundTlsSettings](#)
 11. [PaginatedCollectionSite](#)
 12. [PaginationMetadata](#)
 13. [Servers](#)
 14. [Site](#)
 15. [SiteHstsConfiguration](#)
 16. [SiteOnboardResponse](#)
 17. [SiteOnboardingRequest](#)
-

-
18. SiteSpaFullSettingsDto
 19. SiteSpaFullSettingsV3ResponseDto
 20. SiteSpaPreProdSettingsDto
 21. SiteSpaSettingsApiResponse
 22. SiteSpaSettingsDto
 23. SiteTLSConfiguration
 24. SiteTLSConfigurationRequest
 25. TLSVersion

APIError

code (optional)
String
 detail (optional)
String
 id (optional)
String
 source (optional)
map[String, Object]
 status (optional)
Integer
 format: int32
 title (optional)
String

AccountInboundTLSConfigurationRequest

data (optional)
array[InboundTlsSettings]

CertificateSettings

Certificate Settings entity
 validationMethod (optional)
String
 The method used by Imperva to validate domain ownership.
 example: CNAME

CollectionSite

data (optional)
array[Site]

CollectionSiteOnboardResponse

data (optional)
array[SiteOnboardResponse]

CollectionSiteTLSConfiguration

data (optional)

array[SiteTLSConfiguration]

DnsOnboardingInstructionDto

site onboarding DNS instruction
description (optional)

String

instruction's description

host (optional)

String

DNS record host

example: www.example.com

recordType (optional)

String

DNS record type

example: CNAME

value (optional)

String

DNS record value

example: abc.impervadns.net

Domain

Domain entity

id (optional)

Long

The ID of the domain format: int64

example: 123456

name (optional)

String

The domain name

example: www.example.com

protectionStatus (optional)

String

The domain ownership verification status. Possible values: BYPASSED, MISCONFIGURED, VERIFIED, PROTECTED

example: BYPASSED

ErrorResponse

errors (optional)

array[APIError]

InboundTlsSettings

configurationProfile (optional)

String

TLS configuration profile is an enumeration of predefined configuration profiles. It can also be set to CUSTOM, for setting custom TLS configuration.

Enum:

CUSTOM

DEFAULT

ENHANCED_SECURITY

tlsConfiguration (optional)

array[TLSVersion]

List of supported TLS versions and ciphers related to the specific version. This list holds the CUSTOM

configuration that is going to be used in the communication between the client and Imperva. If the list is empty a predefined configuration profile should be used.

PaginatedCollectionSite

data
array[Site]
 API paginated response data
 links (optional)
map[String, String]
 API pagination links
 meta (optional)
PaginationMetadata

PaginationMetadata

API pagination metadata
 page (optional)
Integer
 format: int32
 size (optional)
Integer
 format: int32
 totalElements (optional)
Long
 format: int64
 totalPages (optional)
Integer
 format: int32

Servers

Server entity
 ips (optional)
array[String]
 Data Center's origin server IPs/CNAMEs
 example: ["1.2.3.4", "3.2.2.2"]

Site

Site entity
 accountId (optional)
Long
 The account ID of the site format: int64
 example: 10
 active (optional)
Boolean
 Whether the site is active or bypassed by the Imperva network
 example: true
 cname (optional)
String
 The CNAME provided by Imperva that is used for pointing your website traffic to the Imperva network. This is not relevant for site type of LOCAL or PUBLIC_CLOUD.
 example: sdh5s.example.com
 creationTime (optional)
Long

The creation date of the site format: int64

example: 1673186130

deploymentKeys (optional)

array[UUID]

Deployment keys format: uuid

example: 4d0654aa-8d16-46f6-8158-a42a1b48e48b

id (optional)

Long

The ID of the site. format: int64

example: 123456

isDefaultSite (optional)

Boolean

Default anywhere site

example: false

name

String

Friendly name of the site.

example: www.example.com

refId (optional)

String

Sets the Reference ID, a free-text field that enables you to add a unique identifier to correlate a website in our service with an object on the customer side

example: 123abc

siteStatus (optional)

String

The status

Enum:

CONFIGURED

PARTIALLY_CONFIGURED

NOT_CONFIGURED

UNKNOWN

example: CONFIGURED

type

String

The website type. Indicates which kind of website is created, e.g. CLOUD_WAF for a website onboarded to Imperva Cloud WAF.

Enum:

CLOUD_WAF

LOCAL

PUBLIC_CLOUD

example: CLOUD_WAF

SiteHstsConfiguration

HTTP Strict transport security (HSTS) ensures that any attempt by visitors to use the unsecure version (`http://`) of a page will be forwarded automatically to the secure version (`https://`).

isEnabled (optional)

Boolean

Enable/disable HSTS support for this website

maxAge (optional)

Long

(TTL) The amount of time in seconds to apply HSTS in the browser before attempting to load the page using `http://`. format: int64

example: 7543

preLoaded (optional)

Boolean

The most secure way to enforce HSTS. Ensures the first request goes out in a secure tunnel, since the browser already has that URL in the pre-load list. The domain needs to be listed at <https://hstspreload.appspot.com/>.

subDomainsIncluded (optional)

Boolean

Enforce HSTS on sub-domains. For example, a page listed on xxx.ddd.com uses resources from images.ddd.com. If HSTS for sub-domains is enabled, the images are also covered. Make sure that the site and all sub-domains support HTTPS so that HSTS does not break an internal resource when rendering the page.

SiteOnboardResponse

Site onboarding response entity

certificateSettings (optional)

CertificateSettings

domains (optional)

array[Domain]

instructions (optional)

map[String, array[DnsOnboardingInstructionDto]]

Site onboarding instructions list

example: {"Network": [{"description": "Add the following record to your DNS provider", "host": "example.com", "recordType": "A", "value": "1.2.3.4"}, {"description": "Add the following record to your DNS provider", "host": "example.com", "recordType": "A", "value": "5.6.7.8"}, {"description": "Add the following record to your DNS provider", "host": "www.example.com", "recordType": "CNAME", "value": "asdasd.ng.impervadns.net"}], "SSL": [{"description": "Add the following record to your DNS provider", "host": "_delegate_validation.example.com", "recordType": "CNAME", "value": "qweqweng.impervadns.net"}]}

servers (optional)

Servers

site (optional)

Site

SiteOnboardingRequest

Site onboarding request entity

domain

String

The domain of the site

example: my.domain.com

generateCertificate (optional)

Boolean

Indicates whether to automatically generate an SSL certificate. When set to false, SSL certificate generation is disabled.

example: false

name (optional)

String

The name of the site. If not specified, the domain name is used.

example: my site

servers (optional)

array[String]

List of your origin server IP addresses or CNAMEs.

example: ["1.2.3.4", "3.2.2.2"]

type (optional)

String

The website type. Indicates which kind of website is created, e.g. CLOUD_WAF for a website onboarded to Imperva Cloud WAF.

Enum:

CLOUD_WAF

LOCAL

PUBLIC_CLOUD

example: CLOUD_WAF

SiteSpaFullSettingsDto

allowedSpaDomains (optional)

array[String]

List of allowed cross-origin domains for the SPA site. The SPA script is allowed to add SPA-specific request headers when the application makes requests to these domains.

preProdSettings (optional)

SiteSpaPreProdSettingsDto

prodVersion (optional)

String

The SPA script version to be used for the website. This parameter is optional. If not specified, the latest version is used.

example: 1.1

state

String

<p>The SPA configuration option for the specified website. Possible values: SPA, SPA FOR_SPECIFIC_URLS, SPA_EXCEPT_URLS, NOT_SPA.</p> <p>Imperva recommends configuring SPA support for the entire website. The other options should be used only for rare cases where SPA functionality is seen to interfere with specific pages, and in consultation with Imperva.</p>

Enum:

NOT_SPA

SPA_EXCEPT_URLS

SPA_FOR_SPECIFIC_URLS

SPA

example: SPA_FOR_SPECIFIC_URLS

urlList (optional)

array[String]

The list of URLs to be used together with either the SPA FOR_SPECIFIC_URLS or SPA_EXCEPT_URLS parameter to define SPA support for only a subset of your website.

example: ["/url1","/url2","/url3"]

SiteSpaFullSettingsV3ResponseDto

data (optional)

array[SiteSpaFullSettingsDto]

SiteSpaPreProdSettingsDto

The pre-production SPA settings to be used for the website. This parameter is optional.

headers (optional)

array[String]

The list of headers to be used together with the preProdVersion parameter to provide execution of a specific spa version.

example: ["header1","header2","header3"]

preProdVersion (optional)

String

The pre production SPA script version to be used for the website. This parameter is optional. If not specified, the latest version is used.

example: 1.1

SiteSpaSettingsApiResponse

data (optional)

array[SiteSpaSettingsDto]

SiteSpaSettingsDto

allowedSpaDomains (optional)

array[String]

List of allowed cross-origin domains for the SPA site. The SPA script is allowed to add SPA-specific request headers when the application makes requests to these domains.

preProdSettings (optional)

SiteSpaPreProdSettingsDto

prodVersion (optional)

String

The SPA script version to be used for the website. This parameter is optional. If not specified, the latest version is used.

example: 1.1

state

Boolean

<p>The SPA configuration state for the specified website.</p> <p>Imperva recommends configuring SPA support for the entire website. The other options should be used only for rare cases where SPA functionality is seen to interfere with specific pages, and in consultation with Imperva.</p>

example: true

SiteTLSConfiguration

disablePQCSupport (optional)

Boolean

Disable Post-Quantum Cryptography support for SNI traffic.

hstsConfiguration (optional)

SiteHstsConfiguration

inboundTlsSettings (optional)

InboundTlsSettings

SiteTLSConfigurationRequest

data (optional)

array[SiteTLSConfiguration]

TLSVersion

List of supported TLS versions and ciphers related to the specific version. This list holds the CUSTOM configuration that is going to be used in the communication between the client and Imperva. If the list is empty a predefined configuration profile should be used.

ciphersSupport (optional)

array[String]

List of RFC cipher names supported for the specified TLS version. This configuration is used when the CUSTOM configuration profile is selected. Please refer to <https://docs.imperva.com/bundle/cloud-application-security/page/cipher-suites.htm> for the list of ciphers.

tlsVersion (optional)

String

TLS version name. For example: TLS_1_2

Enum:

TLS_1_0

TLS_1_1

TLS_1_2

TLS_1_3

Imperva Website Domain Management

Manage the domains that are sharing the CNAME of an onboarded website.

All domains that are using the same CNAME share the website configuration settings and policies of the onboarded website.

For full feature documentation, see [Website General Settings](#).

Version: 1.0.0

BasePath:/site-domain-manager

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Domains

- `post /v2/sites/{siteId}/domains`
- `delete /v2/sites/{siteId}/domains/{domainId}`
- `get /v2/sites/{siteId}/domains/{domainId}`
- `get /v2/sites/{siteId}/domains/extradetails`
- `get /v2/sites/{siteId}/domains/status/{uuid}`
- `get /v2/sites/{siteId}/domains`
- `put /v2/sites/{siteId}/domains`

DomainsV3

- `post /v3/sites/{siteId}/domains`
- `delete /v3/sites/{siteId}/domains/{domainId}`
- `get /v3/domains`
- `get /v3/sites/{siteId}/domains`

Domains

```
post /v2/sites/{siteId}/domains
```

Add domain to a given website (addSiteDomain1)

Adds a domain to an onboarded website.

Path parameters

`sitId` (required)
 Path Parameter
 — The Imperva ID of the onboarded website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `AddSiteDomainDetails` (required)
 Body Parameter

Query parameters

`caId` (optional)
 Query Parameter
 — The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`SiteDomainDetails`

Example data

Content-Type: `application/json`

```
{
  "cloudWafSite" : true,
  "mainDomain" : false,
  "validationCode" : "xjkschvver.impervadnsstage.net",
  "creationDate" : 1655140751000,
  "aRecords" : [ "aRecords", "aRecords" ],
  "validationMethod" : "CNAME",
  "managed" : false,
  "domain" : "a.example.com",
  "autoDiscovered" : true,
  "subDomains" : [ {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  }, {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
  }
]
```

```

    "id" : 320
} ],
"siteId" : 66575115,
"domainSslStatus" : "SSL_COVERAGE_EXIST",
"id" : 440,
"cnameRedirectionRecord" : "xjkschvver.impervadnsstage.net",
"status" : "BYPASSED"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

400

[Bad Request APIErrors](#)

500

[Internal Error APIErrors](#)

200

successful operation [SiteDomainDetails](#)

```
delete /v2/sites/{siteId}/domains/{domainId}
```

Delete a domain from a website (deleteSiteDomain1)
Deletes a domain from an onboarded website.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

domainId (required)

Path Parameter

— The Imperva ID of the domain. You can retrieve the domain ID using the GET /domains call. format: int64

Query parameters

deleteLastDomain (optional)

Query Parameter

— Delete last domain

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

200

successful operation

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v2/sites/{siteId}/domains/{domainId}
```

Retrieve details of a given domain (getSiteDomain)

Retrieve details of a domain associated with an onboarded website.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

domainId (required)

Path Parameter

— The Imperva ID of the domain. You can retrieve the domain ID using the GET /domains call. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[SiteDomainDetails](#)

Example data

Content-Type: application/json

```
{
  "cloudWafSite" : true,
  "mainDomain" : false,
  "validationCode" : "xjkschvver.impervadnsstage.net",
  "creationDate" : 1655140751000,
  "aRecords" : [ "aRecords", "aRecords" ],
  "validationMethod" : "CNAME",
  "managed" : false,
  "domain" : "a.example.com",
  "autoDiscovered" : true,
  "subDomains" : [ {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  }, {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  }],
  "siteId" : 66575115,
  "domainSslStatus" : "SSL_COVERAGE_EXIST",
  "id" : 440,
  "cnameRedirectionRecord" : "xjkschvver.impervadnsstage.net",
  "status" : "BYPASSED"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

400

[Bad Request APIErrors](#)

500

[Internal Error APIErrors](#)

200

successful operation SiteDomainDetails

```
get /v2/sites/{siteId}/domains/extraDetails
```

Get site extra details. (getSiteExtraDetails)

Returns additional site details, related to domain management.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

SiteDomainsExtraDetailsResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "numberOfAutoDiscoveredDomains" : 10,
    "maxAllowedDomains" : 1000
  }, {
    "numberOfAutoDiscoveredDomains" : 10,
    "maxAllowedDomains" : 1000
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [SiteDomainsExtraDetailsResponse](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v2/sites/{siteId}/domains/status/{uuid}
```

Get status for asynchronous request (`getStatusForDomainsForSiteRequest`)

Use this API in order to get status for any domain management asynchronous API using a unique id. Status can be one of the following: IN_PROGRESS, COMPLETED_SUCCESSFULLY or FAILED

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

`uuid` (required)

Path Parameter

— The uuid of the asynchronous request

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[AsyncResponseData](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "handler" : "cf0c2380-21e7-4e52-b6e9-57c746af3b83",
    "status" : "IN_PROGRESS"
  }, {
    "handler" : "cf0c2380-21e7-4e52-b6e9-57c746af3b83",
    "status" : "COMPLETED_SUCCESSFULLY"
  } ]
}
```

```

    "handler" : "cf0c2380-21e7-4e52-b6e9-57c746af3b83",
    "status" : "IN_PROGRESS"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AsyncResponseData](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v2/sites/{siteId}/domains
```

List domains for a given website (listSiteDomains)

Lists all domains associated with an onboarded website.

Path parameters

`sitId` (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

Query parameters

`pageNumber` (optional)

Query Parameter

— The page to return starting from 0.

In order to view the full results, run the API call with `page_num` set to 0,
then again with `page_num` set to 1, and so forth.

Default: 0 format: int32

`pageSize` (optional)

Query Parameter

— The number of objects to return in the response.

Default: 50

Maximum: 100 format: int32

`excludeAutoDiscovered` (optional)

Query Parameter

— Auto discovered domains are included by default.

Set this parameter to true to get only manually configured domains.

Default: false

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetSiteDomainsDetails](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "cloudWafSite" : true,
    "mainDomain" : false,
    "validationCode" : "xjkschvver.impervadnsstage.net",
    "creationDate" : 1655140751000,
    "aRecords" : [ "aRecords", "aRecords" ],
    "validationMethod" : "CNAME",
    "managed" : false,
    "domain" : "a.example.com",
    "autoDiscovered" : true,
    "subDomains" : [ {
      "creationTime" : 1655140751000,
      "subDomain" : "sub.domain.example.com",
      "lastDiscoveredTime" : 1655140751000,
      "id" : 320
    }, {
      "creationTime" : 1655140751000,
      "subDomain" : "sub.domain.example.com",
      "lastDiscoveredTime" : 1655140751000,
      "id" : 320
    } ],
    "siteId" : 66575115,
    "domainSslStatus" : "SSL_COVERAGE_EXIST",
    "id" : 440,
    "cnameRedirectionRecord" : "xjkschvver.impervadnsstage.net",
    "status" : "BYPASSED"
  }, {
    "cloudWafSite" : true,
    "mainDomain" : false,
    "validationCode" : "xjkschvver.impervadnsstage.net",
    "creationDate" : 1655140751000,
    "aRecords" : [ "aRecords", "aRecords" ],
    "validationMethod" : "CNAME",
    "managed" : false,
    "domain" : "a.example.com",
    "autoDiscovered" : true,
    "subDomains" : [ {
      "creationTime" : 1655140751000,
      "subDomain" : "sub.domain.example.com",
      "lastDiscoveredTime" : 1655140751000,
      "id" : 320
    }, {
      "creationTime" : 1655140751000,
      "subDomain" : "sub.domain.example.com",
      "lastDiscoveredTime" : 1655140751000,
      "id" : 320
    } ]
  }
}
```

```

    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  } ],
  "siteId" : 66575115,
  "domainSslStatus" : "SSL_COVERAGE_EXIST",
  "id" : 440,
  "cnameRedirectionRecord" : "xjkschvver.impervadnsstage.net",
  "status" : "BYPASSED"
} ],
"meta" : {
  "totalPages" : 5
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

successful operation [GetSiteDomainsDetails](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
put /v2/sites/{siteId}/domains
```

Bulk update domains for a given website. (updateDomainsToSite)

An asynchronous API for adding and removing domains to an onboarded website using a single bulk operation. The call will immediately return a response with a location header specifying a GET request url for a status check using a unique id

Path parameters

`siteId` (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [BulkAddSiteDomainsBody](#) (required)
Body Parameter

Query parameters

includeAutoDiscovered (optional)

Query Parameter

— should the system consider also auto discovered domains

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[AsyncResponseData](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "handler" : "cf0c2380-21e7-4e52-b6e9-57c746af3b83",
    "status" : "IN_PROGRESS"
  }, {
    "handler" : "cf0c2380-21e7-4e52-b6e9-57c746af3b83",
    "status" : "IN_PROGRESS"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

202

Accepted successfully [AsyncResponseData](#)

DomainsV3

```
post /v3/sites/{siteId}/domains
```

Add domain to a given website (addSiteDomain)
Adds a domain to an onboarded website.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CollectionSiteDomainDto](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[SiteDomainDetails](#)

Example data

Content-Type: application/json

```
{
  "cloudWafSite" : true,
  "mainDomain" : false,
  "validationCode" : "xjkschvver.impervadnsstage.net",
  "creationDate" : 1655140751000,
  "aRecords" : [ "aRecords", "aRecords" ],
  "validationMethod" : "CNAME",
  "managed" : false,
  "domain" : "a.example.com",
  "autoDiscovered" : true,
  "subDomains" : [ {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  }, {
    "creationTime" : 1655140751000,
    "subDomain" : "sub.domain.example.com",
    "lastDiscoveredTime" : 1655140751000,
    "id" : 320
  }],
  "siteId" : 66575115,
  "domainSslStatus" : "SSL_COVERAGE_EXIST",
  "id" : 440,
  "cnameRedirectionRecord" : "xjkschvver.impervadnsstage.net",
  "status" : "BYPASSED"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

400

[Bad Request APIErrors](#)

500

[Internal Error APIErrors](#)

200

successful operation [SiteDomainDetails](#)

```
delete /v3/sites/{siteId}/domains/{domainId}
```

Delete a domain from a website (deleteSiteDomain)
Deletes a domain from an onboarded website.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

domainId (required)

Path Parameter

— The Imperva ID of the domain. You can retrieve the domain ID using the GET /domains call. format: int64

Query parameters

deleteLastDomain (optional)

Query Parameter

— Delete last domain

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[CollectionSiteDomainDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "domain" : "a.example.com",
    "cname" : "xjkschvver.impervadnsstage.net",
    "arecords" : [ "arecords", "arecords" ],
    "siteId" : 66575115,
    "id" : 440,
    "creationDate" : 1655140751000,
    "status" : "CONFIGURED"
  }, {
    "domain" : "a.example.com",
    "cname" : "xjkschvver.impervadnsstage.net",
    "arecords" : [ "arecords", "arecords" ],
    "siteId" : 66575115,
    "id" : 440,
    "creationDate" : 1655140751000,
  } ]
```

```

        "status" : "CONFIGURED"
    } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

successful operation [CollectionSiteDomainDto](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v3/domains
```

List domains for a given account ([getAccountDomainsByFilter](#))

Lists all domains associated with an onboarded website of a given account.

Query parameters

`domainIds` (optional)

Query Parameter

— A list of domains ids. If this parameter is provided, only domains matching one of these ids will be returned.

`format: int64`

`names` (optional)

Query Parameter

— A list of domains names. If this parameter is provided, only domains matching one of these names will be returned.

`sitIds` (optional)

Query Parameter

— A list of website ids. If this parameter is provided, only domains of websites matching one of these IDs will be returned. `format: int64`

`page` (optional)

Query Parameter

— The page to return starting from 0. `default: 0` `format: int32`

`size` (optional)

Query Parameter

— Page size used to determine the first object to be returned and the number of objects to be returned. `default: 20` `format: int32`

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

PaginatedCollectionSiteDomainDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "domain" : "a.example.com",
    "cname" : "xjkschvver.impervadnsstage.net",
    "arecords" : [ "arecords", "arecords" ],
    "siteId" : 66575115,
    "id" : 440,
    "creationDate" : 1655140751000,
    "status" : "CONFIGURED"
  }, {
    "domain" : "a.example.com",
    "cname" : "xjkschvver.impervadnsstage.net",
    "arecords" : [ "arecords", "arecords" ],
    "siteId" : 66575115,
    "id" : 440,
    "creationDate" : 1655140751000,
    "status" : "CONFIGURED"
  } ],
  "meta" : {
    "size" : 1,
    "totalPages" : 0,
    "page" : 5,
    "totalElements" : 6
  },
  "links" : {
    "key" : "links"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

successful operation PaginatedCollectionSiteDomainDto

400

Bad Request APIErrors

500

Internal Error APIErrors

```
get /v3/sites/{siteId}/domains
```

List domains for a given website (getSiteDomains)

Lists all domains associated with an onboarded website. The status field indicates the domain's overall configuration status, including SSL coverage and DNS configuration.

Path parameters

sitelid (required)

Path Parameter

— The Imperva ID of the onboarded website. format: int64

Query parameters

pageNumber (optional)

Query Parameter

— The page to return starting from 0.

In order to view the full results, run the API call with page_num set to 0,
then again with page_num set to 1, and so forth.

Default: 0 default: 0 format: int32

pageSize (optional)

Query Parameter

— The number of objects to return in the response.

Default: 50

Maximum: 100 format: int32

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PaginatedCollectionSiteDomainDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "domain" : "a.example.com",
    "cname" : "xjkschvver.impervadnsstage.net",
    "arecords" : [ "arecords", "arecords" ],
    "siteId" : 66575115,
    "id" : 440,
    "creationDate" : 1655140751000,
    "status" : "CONFIGURED"
  }
]
```

```

}, {
  "domain" : "a.example.com",
  "cname" : "xjkschvver.impervadnsstage.net",
  "arecords" : [ "arecords", "arecords" ],
  "siteId" : 66575115,
  "id" : 440,
  "creationDate" : 1655140751000,
  "status" : "CONFIGURED"
} ],
"meta" : {
  "size" : 1,
  "totalPages" : 0,
  "page" : 5,
  "totalElements" : 6
},
"links" : {
  "key" : "links"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

successful operation [PaginatedCollectionSiteDomainDto](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [APIErrors](#)
 3. [AddSiteDomainDetails](#)
-

-
4. AsyncResponse
 5. AsyncresponseData
 6. BulkAddSiteDomainDetails
 7. BulkAddSiteDomainsBody
 8. CollectionSiteDomainDto
 9. GetEntitiesDetailsMeta
 10. GetSiteDomainsDetails
 11. PaginatedCollectionSiteDomainDto
 12. PaginationMetadata
 13. SiteDomainDetails
 14. SiteDomainDto
 15. SiteDomainsExtraDetails
 16. SiteDomainsExtraDetailsResponse
 17. WildCardSubDomainDetails

APIError

status (optional)
Integer
format: int32
id (optional)
String
code (optional)
String
source (optional)
map[String, Object]
title (optional)
String
detail (optional)
String

APIErrors

errors (optional)
array[APIError]

AddSiteDomainDetails

domain
String
The name of the domain to add
example: full.alternative.domain.incaptest.co
strictMode (optional)
Boolean
Internal use for Terraform.
In strict mode, add/delete of hostname is allowed only if it does not affect other hosts in the site. For example, adding a wildcard hostname is forbidden in strict mode if a subdomain of the wildcard already exists as a siteDomain, while in loose mode, the subdomain is converted to a WildCardSubDomain.
example: true

AsyncResponse

Asynchronous response.

handler (optional)

String

The code provided in the asynchronous response.

example: cf0c2380-21e7-4e52-b6e9-57c746af3b83

status (optional)

String

The status of the process.

Enum:

IN_PROGRESS

COMPLETED_SUCCESSFULLY

FAILED

example: IN_PROGRESS

AsyncResponseData

data (optional)

array[**AsyncResponse**]

Asynchronous response.

BulkAddSiteDomainDetails

Domains to add for a given website

name (optional)

String

The name of the domain to add

example: my-website.example.com

BulkAddSiteDomainsBody

data (optional)

array[**BulkAddSiteDomainDetails**]

Domains to add for a given website

CollectionSiteDomainDto

data (optional)

array[**SiteDomainDto**]

API request data

GetEntitiesDetailsMeta

totalPages (optional)

Integer

The total number of pages format: int32

example: 5

GetSiteDomainsDetails

data (optional)

array[**SiteDomainDetails**]

meta (optional)
GetEntitiesDetailsMeta

PaginatedCollectionSiteDomainDto

data (optional)
array[SiteDomainDto]
API paginated response data
meta (optional)
PaginationMetadata
links (optional)
map[String, String]
API pagination links

PaginationMetadata

API pagination metadata
totalPages (optional)
Integer
format: int32
totalElements (optional)
Long
format: int64
size (optional)
Integer
format: int32
page (optional)
Integer
format: int32

SiteDomainDetails

id (optional)
Long
The ID of the alternative domain format: int64
example: 440
siteld (optional)
Long
The Imperva ID of the onboarded website. format: int64
example: 66575115
domain (optional)
String
The name of the domain to add
example: a.example.com
autoDiscovered (optional)
Boolean
CNAME reuse domain that was discovered automatically by Imperva proxy
example: true
mainDomain (optional)
Boolean
Indicates if the domain is primary domain or alternative domain
example: false
managed (optional)
Boolean
Indicates that the primary domain does not have any alternative domains
example: false

subDomains (optional)
array[WildCardSubDomainDetails]
validationMethod (optional)
String
The method used to validate ownership of the domain. Possible values: CNAME, TXT, A
example: CNAME
validationCode (optional)
String
The code that should be used to validate ownership of the domain
example: xjkschvver.impervadnsstage.net
cnameRedirectionRecord (optional)
String
The CNAME value that should be used for CNAME reuse for the alternative domains.
example: xjkschvver.impervadnsstage.net
status (optional)
String
The domain ownership verification status. Possible values: BYPASSED, MISCONFIGURED, VERIFIED, PROTECTED
example: BYPASSED
creationDate (optional)
Long
The date of the domain creation format: int64
example: 1655140751000
aRecords (optional)
array[String]
cloudWafSite (optional)
Boolean
domainSslStatus (optional)
String
Enum:
SSL_COVERAGE_EXIST
SSL_COVERAGE_NOT_EXIST
NOT_ACCEPTABLE

SiteDomainDto

API request data
id (optional)
Long
The ID of the domain format: int64
example: 440
siteld (optional)
Long
The Imperva ID of the onboarded website. format: int64
example: 66575115
domain
String
The domain
example: a.example.com
status (optional)
String
The domain protection status.
Enum:
CONFIGURED
NOT_CONFIGURED
UNKNOWN
NOT_SUPPORTED
example: CONFIGURED

cname (optional)
String
 Site cname
 example: xjkschvver.impervadnsstage.net
 creationDate (optional)
Long
 The date of the domain creation format: int64
 example: 1655140751000
 arecords (optional)
 array[String]

SiteDomainsExtraDetails

Site domain extra details response.
 numberOfAutoDiscoveredDomains (optional)
Integer
 Number of current Auto Discovered domains in the site. format: int32
 example: 10
 maxAllowedDomains (optional)
Integer
 Maximum allowed domains for a given website. format: int32
 example: 1000

SiteDomainsExtraDetailsResponse

data (optional)
 array[SiteDomainsExtraDetails]
 Site domain extra details response.

WildCardSubDomainDetails

id (optional)
Long
 The Imperva Id of the wild card subdomain details format: int64
 example: 320
 subDomain (optional)
String
 The name of the subdomain
 example: sub.domain.example.com
 lastDiscoveredTime (optional)
Long
 For auto-discovered domains, indicates the last time the domain was discovered. format: int64
 example: 1655140751000
 creationTime (optional)
Long
 The creation time of the wildcard subdomain details format: int64
 example: 1655140751000

SSL Certificate Management

View and manage certificates for all websites in your account.

Version: 1.0.0

BasePath:/certificates-ui

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

HSMCertificates

- `get /v3/certificates/hsm/latency`

MTLSImpervaToOriginCertificates

- `put /v3/mtls/origin/{certificateId}/associated-sites/{siteId}`
- `get /v3/mtls/origin/{certificateId}`
- `get /v3/mtls/origin`
- `get /v3/mtls/origin/{certificateId}/associated-sites/{siteId}`
- `delete /v3/mtls/origin/{certificateId}`
- `delete /v3/mtls/origin/{certificateId}/associated-sites/{siteId}`
- `put /v3/mtls/origin/{certificateId}`
- `post /v3/mtls/origin`

SSLAccountSettings

- `post /v3/account/ssl-settings/delegation/domain/{domain}`
- `delete /v3/account/ssl-settings`
- `get /v3/account/ssl-settings`
- `patch /v3/account/ssl-settings`
- `delete /v3/account/ssl-settings/delegation/domain/{domainId}`
- `post /v3/account/ssl-settings`
- `post /v3/account/ssl-settings/delegation/domain/{domainId}/status`

SSLCertificates

- `put /v3/certificates/{certificateId}/sans/{sanId}/validationMethod`
- `get /v3/certificates`
- `get /v3/instructions`

SSL Site Certificate Settings

- `delete /v3/sites/{siteId}/certificates/managed`
- `get /v3/sites/{siteId}/certificates/managed`
- `post /v3/sites/{siteId}/certificates/managed`

HSM Certificates

```
get /v3/certificates/hsm/latency
```

Get HSM latency (getLatency)

Get the latest HSM latency between a given Imperva data center (PoP) and a specific Fortanix region. This operation returns the time it takes for Imperva to get the private key from Fortanix. It does not include the session creation time.

Query parameters

`pop` (required)

Query Parameter

— The code of the Imperva data center (PoP) to check latency for. For the full list of PoPs and codes, see [Imperva Data Centers](https://docs.imperva.com/bundle/cloud-application-security/page/more/pops.htm).

`hsmHostName` (required)

Query Parameter

— The URI (host name) of the Fortanix region. Possible values: amer, uk, eu, apac, au in the required format, e.g. `api.amer.smartkey.io`

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`HsmLatencyDetailsResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "requestTime" : 1677144366,
    "hsmHostName" : "api.amer.smartkey.io",
    "latency" : 146
  }, {
    "requestTime" : 1677144366,
    "hsmHostName" : "api.amer.smartkey.io",
    "latency" : 146
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [HsmLatencyDetailsResponse](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

504

Gateway Timeout [APIErrors](#)

MTLSImpervaToOriginCertificates

```
put /v3/mtls/origin/{certificateId}/associated-sites/{siteId}
```

Assign an mTLS client certificate to websites (assignCertificateToSite)

Assign an mTLS client certificate to websites in your account. This defines which certificate is served during the TLS handshake between the Imperva proxy and your website's origin server. This overrides an existing certificate-site association.

Path parameters

`certificateId` (required)

Path Parameter

— The mTLS certificate id you want to assign to your site. format: int64

`siteId` (required)

Path Parameter

— Site id to assign to a given mTLS client certificate format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

DataResponse

Example data

Content-Type: application/json

```
{  
    "data" : [ { }, { } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation DataResponse

400

Bad Request APIErrors

404

Not Found APIErrors

500

Internal Error APIErrors

```
get /v3/mtls/origin/{certificateId}
```

Get mTLS client certificate details (getCertificateById)
Retrieve details of a specific mTLS client certificate.

Path parameters

certificateId (required)

Path Parameter

— format: int64

Query parameters

caId (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

MtlsCertificateDetailsResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
      "expirationDateValid" : true,
      "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
  }, {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us"
  }
}
```

```

    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
        "expirationDateValid" : true,
        "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [MtlsCertificateDetailsResponse](#)

400

Bad Request [APIErrors](#)

404

Not Found [APIErrors](#)

500

[Internal Error APIErrors](#)

```
get /v3/mtls/origin
```

Get details of all mTLS client certificates (getCertificates)

Retrieve details of all mTLS client certificates in your account or assigned to a specific website.

Query parameters

`sitId` (optional)

Query Parameter

— The Imperva ID of the onboarded website. format: int64

`caId` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`MtlsCertificateDetailsResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
      "expirationDateValid" : true,
      "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
  }, {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ]
  }
}
```

```

        "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
        "expirationDateValid" : true,
        "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [MtlsCertificateDetailsResponse](#)

400

Bad Request [APIErrors](#)

404

Not Found [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v3/mtls/origin/{certificateId}/associated-sites/{siteId}
```

Check association between specific mTLS certificate and site. (isCertificateAssociatedToSite)
Check if a specific mTLS client certificate id is associated to a specific site id.

Path parameters

certificateId (required)

Path Parameter

— mTLS certificate id. format: int64

siteld (required)

Path Parameter

— Site id. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

DataResponse

Example data

Content-Type: application/json

```
{
  "data" : [ { }, { } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation. Association exist DataResponse

400

Bad Request APIErrors

404

Not Found. Association does not exist DataResponse

500

Internal Error APIErrors

```
delete /v3/mtls/origin/{certificateId}
```

Delete mTLS client certificate (removeCertificate)

Delete an existing mTLS client certificate that is uploaded to your account. Deleting the certificate may cause outages for applications that still use it. Before deleting the certificate, we strongly advise you to ensure that these applications are not using it.

Path parameters

`certificateId` (required)

Path Parameter

— The mTLS certificate id you want to delete. format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

DataResponse

Example data

Content-Type: application/json

```
{
  "data" : [ { }, { } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation DataResponse

400

Bad Request [APIErrors](#)

404

Not Found [APIErrors](#)

500

[Internal Error APIErrors](#)

```
delete /v3/mtls/origin/{certificateId}/associated-sites/{siteId}
```

Remove mTLS client certificate from website (unAssignCertificateFromSite)

When the mTLS certificate is unassigned from the website, the certificate is not served to the website's origin server.

Path parameters

certificateId (required)

Path Parameter

— The mTLS certificate id you want to un assign your site. format: int64

sitId (required)

Path Parameter

— Site id to un assign from a given mTLS client certificate format: int64

Query parameters

caId (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

DataResponse

Example data

Content-Type: application/json

```
{
  "data" : [ { }, { } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

Successful operation [DataResponse](#)

400

Bad Request [APIErrors](#)

404

Not Found [APIErrors](#)

500

Internal Error [APIErrors](#)

```
put /v3/mtls/origin/{certificateId}
```

Replace mTLS client certificate (updateCertificate)

Replace an existing mTLS client certificate that is uploaded to your account. The Imperva certificate ID remains the same after replacement. Body should be provided in multipart/form-data.

Path parameters

certificateId (required)

Path Parameter

— The mTLS certificate id you want to edit. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Form parameters

certificateFile (optional)

Form Parameter

— format: binary
certificateName (optional)
Form Parameter

— passphrase (optional)
Form Parameter

— privateKeyFile (optional)
Form Parameter
— format: binary

Return type

MtlsCertificateDetailsResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
      "expirationDateValid" : true,
      "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
  }, {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ]
  }
}
```

```

        "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
        "expirationDateValid" : true,
        "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [MtlsCertificateDetailsResponse](#)

400

Bad Request [APIErrors](#)

404

Not Found [APIErrors](#)

500

Internal Error [APIErrors](#)

```
post /v3/mtls/origin
```

Upload mTLS client certificate (uploadCertificate)

Upload an mTLS certificate to your account. Body should be provided in multipart/form-data.

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Form parameters

certificateFile (optional)

Form Parameter

— format: binary

certificateName (optional)

Form Parameter

—

passphrase (optional)

Form Parameter

—

privateKeyFile (optional)

Form Parameter

— format: binary

Return type

MtlsCertificateDetailsResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    }, {
      "accountId" : 22222,
      "name" : "my.domain.org",
      "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
  }
]
```

```

    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
        "expirationDateValid" : true,
        "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
}, {
    "chain" : "my.company.org, example intermediate CA, example root CA",
    "appliedSitesDetails" : [ {
        "accountId" : 22222,
        "name" : "my.domain.org",
        "externalId" : 11111
    }, {
        "accountId" : 22222,
        "name" : "my.domain.org",
        "externalId" : 11111
    } ],
    "issuedTo" : "CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us",
    "serialNumber" : "1234abcd",
    "certificateId" : 1,
    "issuedBy" : "CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us",
    "validFrom" : 1655140751000,
    "creationDate" : 1693415951000,
    "accountId" : 1,
    "lastUpdate" : 1693415951000,
    "name" : "example-certificate",
    "validUntil" : 1693415951000,
    "errors" : {
        "expirationDateValid" : true,
        "chainValid" : true
    },
    "hash" : "bdf252eb5fc9ec468a966de1e9e83db676d1851c"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [MtlsCertificateDetailsResponse](#)

400Bad Request [APIErrors](#)**404**Not Found [APIErrors](#)**500**[Internal Error APIErrors](#)

SSLAccountSettings

```
post /v3/account/ssl-settings/delegation/domain/{domain}
```

Add domain to the SSL validation delegation settings (addDomainToSSLValidationDelegationSettings)
 Add domain to the SSL validation delegation settings of your account. Delegating a domain enables Imperva to perform domain ownership validation on your behalf during website onboarding and certificate renewal.

Path parameters

domain (required)
 Path Parameter

Query parameters

caid (optional)
 Query Parameter
 — The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

AccountSSLSettingsResponseDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
```

```
"allowedDomainsForCNAMEValidation" : [ {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
}, {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
} ],
"allowCNAMEValidation" : true
}
},
{
"allowSupportOldTLSVersions" : true,
"enableHSTSForNewSites" : true,
"impervaCertificate" : {
    "useWildCardSanInsteadOfFQDN" : true,
    "addNakedDomainSanForWWWSites" : true,
    "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        }, {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
    }
}
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AccountSSLSettingsResponseDto](#)

400

Bad Request [APIErrors](#)

500

[Internal Error APIErrors](#)

```
delete /v3/account/ssl-settings
```

Reset SSL settings to default (deleteSSLValidationDelegationSettings)
Resets SSL settings for your account to the default values.

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AccountSSLSettingsResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
```

```
"allowedDomainsForCNAMEValidation" : [ {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
}, {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
} ],
"allowCNAMEValidation" : true
}
},
{
"allowSupportOldTLSVersions" : true,
"enableHSTSForNewSites" : true,
"impervaCertificate" : {
    "useWildCardSanInsteadOfFQDN" : true,
    "addNakedDomainSanForWWWSites" : true,
    "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        }, {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
    }
}
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AccountSSLSettingsResponseDto](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v3/account/ssl-settings
```

Get account SSL settings (getSSLValidationDelegationSettings)
Get SSL settings for your account.

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AccountSSLSettingsResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
```

```
"allowedDomainsForCNAMEValidation" : [ {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
}, {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
} ],
"allowCNAMEValidation" : true
}
},
{
"allowSupportOldTLSVersions" : true,
"enableHSTSForNewSites" : true,
"impervaCertificate" : {
    "useWildCardSanInsteadOfFQDN" : true,
    "addNakedDomainSanForWWWSites" : true,
    "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        }, {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
    }
}
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AccountSSLSettingsResponseDto](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
patch /v3/account/ssl-settings
```

Modify SSL settings (partial update) (patchSSLValidationDelegationSettings)
Updates the SSL settings that you send in the request. Other settings remain as is.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AccountSettingsDto](#) (required)
Body Parameter

—

Query parameters

caid (optional)
Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AccountSSLSettingsResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
          "cnameRecordValue" : "abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        }, {
          "cnameRecordValue" : "abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
      }
    }
  }, {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
          "cnameRecordValue" : "abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        }, {
          "cnameRecordValue" : "abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        } ]
      }
    }
  }
]
```

```
        "name" : "example.com",
        "id" : 123,
        "statusSince" : 1663446207139,
        "creationDate" : 1663446207139,
        "status" : "CONFIGURED"
    } ],
    "allowCNAMEValidation" : true
}
}
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation AccountSSLSettingsResponseDto

400

Bad Request API Errors

500

Internal Error API Errors

Remove domain from the SSL validation delegation settings (removedDomainToSSLValidationDelegationSettings)
Remove domain from the SSL validation delegation settings of your account. Certificate renewal may require you to revalidate domain ownership.

Path parameters

domainId (required)

domainId (Required) Path Parameter

— domainId can be getting from this api ([GET /v3/account/ssl-settings](#)) format: int64.

Query parameters

caid (optional)

cauld (optional) Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API.

credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

AccountSSLSettingsResponseDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
          "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        }, {
          "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
          "creationDate" : 1663446207139,
          "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
      }
    }
  }, {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : {
        "allowedDomainsForCNAMEValidation" : [ {
          "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
          "lastStatusCheck" : 1663446207139,
          "cnameRecordHost" : "_delegate_validation.example.com",
          "inherited" : false,
          "name" : "example.com",
          "id" : 123,
          "statusSince" : 1663446207139,
        }
      }
    }
  }
]
```

```
        "creationDate" : 1663446207139,
        "status" : "CONFIGURED"
    }, {
        "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
        "lastStatusCheck" : 1663446207139,
        "cnameRecordHost" : "_delegate_validation.example.com",
        "inherited" : false,
        "name" : "example.com",
        "id" : 123,
        "statusSince" : 1663446207139,
        "creationDate" : 1663446207139,
        "status" : "CONFIGURED"
    } ],
    "allowCNAMEValidation" : true
}
}
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation AccountSSLSettingsResponseDto

400

Bad Request APIErrors

500

Internal Error APIErrors

```
post /v3/account/ssl-settings
```

Overwrite SSL settings (full update) (updateSSLValidationDelegationSettings)
Update SSL settings for your account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AccountSettingsDto](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AccountSSLSettingsResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "allowSupportOldTLSVersions" : true,
    "enableHSTSForNewSites" : true,
    "impervaCertificate" : {
      "useWildCardSanInsteadOfFQDN" : true,
      "addNakedDomainSanForWWWSites" : true,
      "delegation" : [
        {
          "allowedDomainsForCNAMEValidation" : [ {
            "cnameRecordValue" : "abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
          }, {
            "cnameRecordValue" : "abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
          } ],
          "allowCNAMEValidation" : true
        }
      ]
    },
    "allowSupportOldTLSVersions" : true
  }
}
```

```
"enableHSTSForNewSites" : true,
"impervaCertificate" : [
    "useWildCardSanInsteadOfFQDN" : true,
    "addNakedDomainSanForWWWSites" : true,
    "delegation" : [
        "allowedDomainsForCNAMEValidation" : [ {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        }, {
            "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
            "lastStatusCheck" : 1663446207139,
            "cnameRecordHost" : "_delegate_validation.example.com",
            "inherited" : false,
            "name" : "example.com",
            "id" : 123,
            "statusSince" : 1663446207139,
            "creationDate" : 1663446207139,
            "status" : "CONFIGURED"
        } ],
        "allowCNAMEValidation" : true
    }
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation AccountSSLSettingsResponseDto

400

Bad Request APIErrors

500

Internal Error APIErrors

```
post /v3/account/ssl-settings/delegation/domain/{domainId}/status
```

Check the configuration status of a domain that appears in the domain delegation list
(verifyDomainToSSLValidationDelegationSettings)

Check if the CNAME record has been added to the domain's DNS zone.

Path parameters

domainId (required)

Path Parameter

— domainId can be getting from this api (GET /v3/account/ssl-settings) format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[AllowDelegationDomainWithInheritanceResponseDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
  }, {
    "cnameRecordValue" : "_abc.a1234.validation.imperva.com",
    "lastStatusCheck" : 1663446207139,
    "cnameRecordHost" : "_delegate_validation.example.com",
    "inherited" : false,
    "name" : "example.com",
    "id" : 123,
    "statusSince" : 1663446207139,
    "creationDate" : 1663446207139,
    "status" : "CONFIGURED"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AllowDelegationDomainWithInheritanceResponseDto](#)

400

Bad Request [APIErrors](#)

500

[Internal Error APIErrors](#)

SSL Certificates

```
put /v3/certificates/{certificateId}/sans/{sanId}/validationMethod
```

Change SAN validation method (changeSanValidationMethod)

Changes the SAN validation method and value used for certificate revalidation.

Path parameters

certificateId (required)

Path Parameter

— The Imperva ID assigned to the certificate. Use the GET /v3/certificates API call to retrieve the IDs of certificates in your account. format: int64

sanId (required)

Path Parameter

— The Imperva ID assigned to the SAN. Use the GET /v3/certificates API call to retrieve the SAN IDs of certificates in your account. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ChangeValidationMethodRequest](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[ChangeValidationMethodExternalResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "validationMethod" : "DNS",
    "recordType" : "TXT",
    "domain" : "example.imperva.com",
    "verificationCodeExpirationDate" : 1633380421000,
    "validationEmail" : "example@imperva.com",
    "lastNotificationDate" : 1633180421000,
    "expirationDate" : 1633180421000,
    "verificationCode" : "globalsign-domain-verification=1234"
  }, {
    "validationMethod" : "DNS",
    "recordType" : "TXT",
    "domain" : "example.imperva.com",
    "verificationCodeExpirationDate" : 1633380421000,
    "validationEmail" : "example@imperva.com",
    "lastNotificationDate" : 1633180421000,
    "expirationDate" : 1633180421000,
    "verificationCode" : "globalsign-domain-verification=1234"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ChangeValidationMethodExternalResponse](#)

400

Bad Request APIErrors

500

Internal Error APIErrors

```
get /v3/certificates
```

Get certificate details (getCertificates1)
 Get details for certificates in your account.

Query parameters

extSiteId (optional)

Query Parameter

— The Imperva ID of the onboarded website. Retrieves certificate details for a specific website. If not specified, this API retrieves details of all certificates in the account. format: int64

certType (optional)

Query Parameter

— The type of certificate to provide details for

caId (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

ExternalCertificateResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "level" : "SITE",
    "sans" : [ {
      "sitesIds" : [ 2, 2 ],
      "statusDate" : 7,
      "autoValidation" : true,
      "cnameValidationValue" : "cnameValidationValue",
      "approverFqdn" : "approverFqdn",
      "numSitesCovered" : 5,
      "verificationCode" : "verificationCode",
      "domainIds" : [ 6, 6 ],
      "caIssue" : {
        "rawDetails" : "Request rejected by CA: caa: example.com.: issue=example-
ca.com",
        "domain" : "example.com",
        "message" : "The CAA record for the domain must contain GlobalSign CA",
      }
    } ]
  } ]
}
```

```

        "type" : "CAA_CONFIG_ISSUE"
    },
    "sanValue" : "sanValue",
    "validationMethod" : "validationMethod",
    "sanId" : 5,
    "validationEmail" : "validationEmail",
    "expirationDate" : 1,
    "status" : "status"
}, {
    "sitesIds" : [ 2, 2 ],
    "statusDate" : 7,
    "autoValidation" : true,
    "cnameValidationValue" : "cnameValidationValue",
    "approverFqdn" : "approverFqdn",
    "numSitesCovered" : 5,
    "verificationCode" : "verificationCode",
    "domainIds" : [ 6, 6 ],
    "caIssue" : {
        "rawDetails" : "Request rejected by CA: caa: example.com.: issue=example-
ca.com",
        "domain" : "example.com",
        "message" : "The CAA record for the domain must contain GlobalSign CA",
        "type" : "CAA_CONFIG_ISSUE"
    },
    "sanValue" : "sanValue",
    "validationMethod" : "validationMethod",
    "sanId" : 5,
    "validationEmail" : "validationEmail",
    "expirationDate" : 1,
    "status" : "status"
} ],
"renewalCertOrderId" : "ATLAS_47_3483659225",
"siteName" : "Site Name",
"type" : "ATLAS",
"customCertificateDetails" : {
    "inputHash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbcd3",
    "hsmType" : "FORTANIX",
    "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
    "hasMismatchSite" : true,
    "isHsm" : true,
    "fingerprint" : "SHA1 Fingerprint=FE:AB:F3:B4:93:0C:56:CF:4B:EC:E0:29:1C:C
5:8A:9E:47:78:4E:A9",
    "validations" : [ {
        "field" : "field",
        "validationType" : "validationType",
        "statusDetails" : "statusDetails",
        "value" : { },
        "status" : "OK"
    }, {
        "field" : "field",
        "validationType" : "validationType",
        "statusDetails" : "statusDetails",
        "value" : { },
        "status" : "OK"
    } ],
    "authType" : "authType",
    "eccCurve" : "eccCurve",
    "expirationDate" : 0
}
,
```

```

    "name" : "ATLAS_47_3483659225",
    "siteId" : 9,
    "inRenewal" : true,
    "originCertOrderId" : "ATLAS_47_3483659225",
    "id" : 2674,
    "authType" : "RSA",
    "extSiteId" : 856963,
    "expirationDate" : 1633180421000,
    "status" : "IN_PROCESS"
}, {
    "level" : "SITE",
    "sans" : [ {
        "sitesIds" : [ 2, 2 ],
        "statusDate" : 7,
        "autoValidation" : true,
        "cnameValidationValue" : "cnameValidationValue",
        "approverFqdn" : "approverFqdn",
        "numSitesCovered" : 5,
        "verificationCode" : "verificationCode",
        "domainIds" : [ 6, 6 ],
        "caIssue" : {
            "rawDetails" : "Request rejected by CA: caa: example.com.: issue=example-
ca.com",
            "domain" : "example.com",
            "message" : "The CAA record for the domain must contain GlobalSign CA",
            "type" : "CAA_CONFIG_ISSUE"
        },
        "sanValue" : "sanValue",
        "validationMethod" : "validationMethod",
        "sanId" : 5,
        "validationEmail" : "validationEmail",
        "expirationDate" : 1,
        "status" : "status"
    }, {
        "sitesIds" : [ 2, 2 ],
        "statusDate" : 7,
        "autoValidation" : true,
        "cnameValidationValue" : "cnameValidationValue",
        "approverFqdn" : "approverFqdn",
        "numSitesCovered" : 5,
        "verificationCode" : "verificationCode",
        "domainIds" : [ 6, 6 ],
        "caIssue" : {
            "rawDetails" : "Request rejected by CA: caa: example.com.: issue=example-
ca.com",
            "domain" : "example.com",
            "message" : "The CAA record for the domain must contain GlobalSign CA",
            "type" : "CAA_CONFIG_ISSUE"
        },
        "sanValue" : "sanValue",
        "validationMethod" : "validationMethod",
        "sanId" : 5,
        "validationEmail" : "validationEmail",
        "expirationDate" : 1,
        "status" : "status"
    } ],
    "renewalCertOrderId" : "ATLAS_47_3483659225",
    "siteName" : "Site Name",
    "type" : "ATLAS",

```

```

"customCertificateDetails" : {
    "inputHash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
    "hsmType" : "FORTANIX",
    "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
    "hasMismatchSite" : true,
    "isHsm" : true,
    "fingerprint" : "SHA1 Fingerprint=FE:AB:F3:B4:93:0C:56:CF:4B:EC:E0:29:1C:C
5:8A:9E:47:78:4E:A9",
    "validations" : [ {
        "field" : "field",
        "validationType" : "validationType",
        "statusDetails" : "statusDetails",
        "value" : { },
        "status" : "OK"
    }, {
        "field" : "field",
        "validationType" : "validationType",
        "statusDetails" : "statusDetails",
        "value" : { },
        "status" : "OK"
    } ],
    "authType" : "authType",
    "eccCurve" : "eccCurve",
    "expirationDate" : 0
},
"name" : "ATLAS_47_3483659225",
"siteId" : 9,
"inRenewal" : true,
"originCertOrderId" : "ATLAS_47_3483659225",
"id" : 2674,
"authType" : "RSA",
"extSiteId" : 856963,
"expirationDate" : 1633180421000,
"status" : "IN_PROCESS"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ExternalCertificateResponse](#)

400

Bad Request [APIErrors](#)

500

Internal Error APIErrors

```
get /v3/instructions
```

Get domain validation instructions (sanInstructionsForAccount)
Get validation instructions for all pending SANs in the account

Query parameters

`extSiteId` (optional)

Query Parameter

— The Imperva ID of the onboarded website. format: int64

`validationMethod` (optional)

Query Parameter

— The methods that can be used to validate ownership of the domain.

`certificateType` (optional)

Query Parameter

— The type that can be used to get san instructions.

`caId` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`ExternalSanInstructionsResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "relatedSansDetails" : 1633180421000,
    "validationMethod" : "DNS",
    "certificateLevel" : "SITE",
    "recordType" : "TXT",
    "domain" : "example.imperva.com",
    "verificationCodeExpirationDate" : 1633180421000,
    "validationEmail" : "example@imperva.com",
    "lastNotificationDate" : 1633180421000,
    "expirationDate" : 1633180421000,
    "verificationCode" : "856963"
  }, {
    "relatedSansDetails" : 1633180421000,
    "validationMethod" : "DNS",
    "certificateLevel" : "SITE",
    "recordType" : "TXT",
    "domain" : "example.imperva.com",
    "verificationCodeExpirationDate" : 1633180421000,
    "validationEmail" : "example@imperva.com",
    "lastNotificationDate" : 1633180421000,
    "expirationDate" : 1633180421000
  } ]
}
```

```

    "expirationDate" : 1633180421000,
    "verificationCode" : "856963"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ExternalSanInstructionsResponse](#)

401

Unauthorized [APIErrors](#)

500

Internal Server Error [APIErrors](#)

SSLSiteCertificateSettings

```
delete /v3/sites/{siteId}/certificates/managed
```

Remove site certificate coverage. ([deleteSiteSSLCertificateSettings](#))

Removes site certificate coverage for a specific website according to the site ID.

Warning: This API was deprecated. To remove site certificate coverage for a specific website, use POST [/v3/sites/{siteId}/certificates/managed](#) API.

Path parameters

siteId (required)

Path Parameter

— format: int64

Return type

[SiteSSLCertificatesSettings](#)

Example data

Content-Type: application/json

```
{
  "defaultValidationMethod" : "CNAME",
  "siteCertificateEnabled" : true,
  "siteId" : 856963
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [SiteSSLCertificatesSettings](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
get /v3/sites/{siteId}/certificates/managed
```

Get site certificate settings (getSiteSSLCertificateSettings)

Retrieves site certificate settings for a specific website according to the site ID.

Path parameters

`siteld` (required)

Path Parameter

— format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

[SiteSSLCertificatesSettings](#)

Example data

Content-Type: application/json

```
{
  "defaultValidationMethod" : "CNAME",
  "siteCertificateEnabled" : true,
  "siteId" : 856963
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [SiteSSLCertificatesSettings](#)

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

```
post /v3/sites/{siteId}/certificates/managed
```

Overwrite site certificate settings (full update) (`updateSiteSSLCertificateSettings`)

Enables/disables a site certificate for a specific website and updates its settings. The site certificate is issued for all domains that are added manually to the website configuration in Imperva (“managed domains”).

Path parameters

`siteld` (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SiteSSLCertificatesSettings` (required)
 Body Parameter

Query parameters

`preventCoverageLack` (optional)

Query Parameter

— When set to true: If the site has both a site certificate and the customer's custom certificate, setting this parameter to true ensures that there is no coverage loss.
 When enabling site certificate support (`SiteCertificateEnabled=true`), the request will fail if there is an existing custom certificate that contains SANs that will not be covered by the site certificate.
 When disabling site certificate support (updating the settings with `SiteCertificateEnabled=false`), the request will fail if there is an existing custom certificate and the site certificate contains SANs that do not exist in the custom certificate. default: false

`skipAutoDiscoveredDomainsCheck` (optional)

Query Parameter

— When set to true, the request will succeed even if the site contains auto-discovered domains. default: false

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

`SiteSSLCertificatesSettings`

Example data

Content-Type: application/json

```
{
  "defaultValidationMethod" : "CNAME",
  "siteCertificateEnabled" : true,
  "siteId" : 856963
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation `SiteSSLCertificatesSettings`

400

Bad Request [APIErrors](#)

500

Internal Error [APIErrors](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [APIErrors](#)
 3. [AccountDtoSSLDelegationSettingsDto](#)
 4. [AccountSSLSettingsResponseDto](#)
 5. [AccountSettingsDto](#)
 6. [AllowDelegationDomainWithInheritanceResponseDto](#)
 7. [AllowDomainDelegationWithInheritance](#)
 8. [CaIssueDetails](#)
 9. [Certificate](#)
 10. [CertificateSanDetails](#)
 11. [CertificateValidation](#)
 12. [ChangeValidationMethodDTO](#)
 13. [ChangeValidationMethodExternalResponse](#)
 14. [ChangeValidationMethodRequest](#)
 15. [CustomCertificateDetails](#)
 16. [DataResponse](#)
 17. [ExternalCertificateResponse](#)
 18. [ExternalSanInstructionsResponse](#)
 19. [HsmLatencyDetailsResponse](#)
 20. [HsmLatencyDto](#)
 21. [ImpervaGeneratedCertificateSettingsDto](#)
 22. [MtlsCertificateBaseDetails](#)
 23. [MtlsCertificateDetailsResponse](#)
 24. [MtlsCertificateErrorsDto](#)
 25. [RelatedSansDetails](#)
 26. [SanInstructionsDto](#)
 27. [SiteExternalDetails](#)
 28. [SiteSSLCertificatesSettings](#)
 29. [mtls_origin_body](#)
 30. [origin_certificateId_body](#)
-

APIError

code (optional)
String
detail (optional)
String
id (optional)
String
source (optional)
map[String, Object]
status (optional)
Integer
format: int32
title (optional)
String

APIErrors

errors (optional)
array[APIError]

AccountDtoSSLDelegationSettingsDto

allowCNAMEValidation (optional)
Boolean
Enable Imperva to automatically perform domain ownership validation on your behalf for domains in the allowedDomainsForCNAMEValidation list.
example: true
allowedDomainsForCNAMEValidation (optional)
array[AllowDomainDelegationWithInheritance]

AccountSSLSettingsResponseDto

data (optional)
array[AccountSettingsDto]

AccountSettingsDto

allowSupportOldTLSVersions (optional)
Boolean
When true, sites under the account or sub-accounts can allow support of old TLS versions traffic. This can be configured only on the parent account level.
example: true
enableHSTSForNewSites (optional)
Boolean
When true, enables HSTS support for newly created websites.
example: true
impervaCertificate (optional)
ImpervaGeneratedCertificateSettingsDto

AllowDelegationDomainWithInheritanceResponseDto

data (optional)
array[AllowDomainDelegationWithInheritance]

AllowDomainDelegationWithInheritance

The list of domains delegated to Imperva for purposes of domain ownership validation. Subdomains of the domains in the list are also automatically validated by Imperva. Wildcards are not allowed.

cnameRecordHost (optional)

String

The CNAME record host to use.

example: _delegate_validation.example.com

cnameRecordValue (optional)

String

The CNAME record value to use to configure this domain for delegation.

example: _abc.a1234.validation.imperva.com

creationDate (optional)

Long

The domain creation date. format: int64

example: 1663446207139

id (optional)

Long

The domain id. format: int64

example: 123

inherited (optional)

Boolean

CNAME validation is automatically inherited from a parent domain that is delegated to Imperva. When domain delegation configured (true) for a specific subdomain, its CNAME value overrides the current setting of the parent domain.

example: false

lastStatusCheck (optional)

Long

The date the domain status was last verified. format: int64

example: 1663446207139

name (optional)

String

The domain name.

example: example.com

status (optional)

String

The domain status. Possible values: CONFIGURED, NOT_CONFIGURED

example: CONFIGURED

statusSince (optional)

Long

The date the domain status was last modified. format: int64

example: 1663446207139

CaIssueDetails

domain (optional)

String

The domain to which the CA issue applies

example: example.com

message (optional)

String

A general description about the issue

example: The CAA record for the domain must contain GlobalSign CA

rawDetails (optional)

String

The error response from the CA

example: Request rejected by CA: caa: example.com.: issue=example-ca.com

type (optional)

String

DNS issues reported to Imperva by the CA during the certificate validation process

Enum:

CAA_CONFIG_ISSUE

SERVFAIL

INVALID_CNAME_CONFIG

DNSSEC_CHAIN_ERROR

example: CAA_CONFIG_ISSUE

Certificate

authType (optional)

String

The authentication type of the certificate

Enum:

RSA

ECC

example: RSA

customCertificateDetails (optional)

CustomCertificateDetails

expirationDate (optional)

Long

Certificate expiration date format: int64

example: 1633180421000

extSiteId (optional)

Long

The Imperva ID of the onboarded website covered by the certificate format: int64

example: 856963

id (optional)

Long

The Imperva ID of the certificate. format: int64

example: 2674

inRenewal (optional)

Boolean

Is certificate under renewal process

example: true

level (optional)

String

The level of the certificate (SITE or ACCOUNT)

Enum:

SITE

ACCOUNT

example: SITE

name (optional)

String

For an Imperva-generated certificate, indicates the certificate name and the ID of the Imperva request to the CA.

example: ATLAS_47_3483659225

originCertOrderId (optional)

String

The order ID of the Imperva request to the CA for a certificate that is set to expire in the near future and must be renewed. This certificate will be replaced by the certificate specified by renewalCertOrderId.

example: ATLAS_47_3483659225

renewalCertOrderId (optional)

String

The order ID of the Imperva request to the CA for a new certificate that will replace an expiring certificate. This certificate will replace the certificate specified by originCertOrderId.

example: ATLAS_47_3483659225

sans (optional)

array[CertificateSanDetails]

List of Subject Alternative Names found on the certificate

siteId (optional)

Long

The id of the site format: int64

siteName (optional)

String

The name of the onboarded website covered by the certificate

example: Site Name

status (optional)

String

Certificate status Possible values for Imperva generated certificate: ISSUED, IN_PROCESS, UNDER_RENEWAL

Possible values for Custom Certificate: ACTIVE, NEAR_EXPIRATION, EXPIRED, SITE_MISMATCH

example: IN_PROCESS

type (optional)

String

Certificate type

Enum:

ATLAS

CUSTOM_CERT

MANUAL

MANAGED

example: ATLAS

CertificateSanDetails

List of Subject Alternative Names found on the certificate

approverFqdn (optional)

String

autoValidation (optional)

Boolean

caIssue (optional)

CaIssueDetails

cnameValidationValue (optional)

String

domainIds (optional)

array[Long]

format: int64

expirationDate (optional)

Long

format: int64

numSitesCovered (optional)

Integer

format: int32

sanId (optional)

Long

format: int64

sanValue (optional)

String

sitesIds (optional)

array[Long]

format: int64

status (optional)

String

statusDate (optional)

Long

format: int64

validationEmail (optional)

String
validationMethod (optional)
String
verificationCode (optional)
String

CertificateValidation

field (optional)
String
status (optional)
String
Enum:
OK
WARNING
ERROR
statusDetails (optional)
String
validationType (optional)
String
value (optional)
Object

ChangeValidationMethodDTO

Validation instructions.
domain (optional)
String
Validation domain
example: example.imperva.com
expirationDate (optional)
Long
SAN expiration date format: int64
example: 1633180421000
lastNotificationDate (optional)
Long
Last date an email was sent format: int64
example: 1633180421000
recordType (optional)
String
validation record type
Enum:
TXT
CNAME
A
NONE
example: TXT
validationEmail (optional)
String
Validation email
example: example@imperva.com
validationMethod (optional)
String
SAN Validation method
Enum:
EMAIL
DNS

CNAME
METATAG
URL
HTTP
NONE
example: DNS
verificationCode (optional)
String
SAN Verification code
example: globalsign-domain-verification=1234
verificationCodeExpirationDate (optional)
Long
Verification code expiration date format: int64
example: 1633380421000

ChangeValidationMethodExternalResponse

data (optional)
array[ChangeValidationMethodDTO]
Validation instructions.

ChangeValidationMethodRequest

validationEmail (optional)
String
Validation email. Required only when the EMAIL validation method is used.
example: example@imperva.com
validationMethod
String
SAN Validation method
Enum:
DNS
EMAIL
CNAME
METATAG
example: EMAIL

CustomCertificateDetails

authType (optional)
String
eccCurve (optional)
String
expirationDate (optional)
Long
format: int64
fingerprint (optional)
String
The certificate fingerprint
example: SHA1 Fingerprint=FE:AB:F3:B4:93:0C:56:CF:4B:EC:E0:29:1C:C5:8A:9E:47:78:4E:A9
hasMismatchSite (optional)
Boolean
Return true if domain is covered by the certificate
example: true
hsmType (optional)
String

The name of the HSM provider

example: FORTANIX

inputHash (optional)

String

Internal use for terraform

example: a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

isHsm (optional)

Boolean

If certificate private key is managed in an HSM, this will return true

example: true

serialNumber (optional)

String

The certificate serialNumber

example: FB:4B:BD:4B:1B:7D:7C:CF

validations (optional)

array[CertificateValidation]

DataResponse

data (optional)

array[Object]

ExternalCertificateResponse

data (optional)

array[Certificate]

ExternalSanInstructionsResponse

data (optional)

array[SanInstructionsDto]

HsmLatencyDetailsResponse

data (optional)

array[HsmLatencyDto]

HSM latency response.

HsmLatencyDto

HSM latency response.

hsmHostName (optional)

String

The URI (host name) of the Fortanix region.
Possible values: amer, uk, eu, apac, au in the required format,

e.g. api.amer.smartkey.io

example: api.amer.smartkey.io

latency (optional)

Long

The last latency in the pop format: int64

example: 146

requestTime (optional)

Long

The time the latency request was recorded.
 Unix epoch time, in milliseconds. format: int64

example: 1677144366

ImpervaGeneratedCertificateSettingsDto

addNakedDomainSanForWWWSites (optional)

Boolean

For sites with the www prefix, adds the naked domain SAN to the Imperva SSL certificate. The value you assign is used as the default option when onboarding new websites.

example: true

delegation (optional)

AccountDtoSSLDelegationSettingsDto

useWildCardSanInsteadOfFQDN (optional)

Boolean

Adds the wildcard SAN to the Imperva SSL certificate instead of the full domain SAN. The value you assign is used as the default option when onboarding new websites.

example: true

MtlsCertificateBaseDetails

mTLS certificate response.

accountId (optional)

Long

The ID of the Account that owns the certificate. format: int64

example: 1

appliedSitesDetails (optional)

array[SiteExternalDetails]

List of the sites attached to the current certificate.

certificateId (optional)

Long

The Imperva ID of the Certificate. format: int64

example: 1

chain (optional)

String

The certification path, from the uploaded certificate back to the root certificate, where each certificate has been signed by the next one in the chain.

example: my.company.org, example intermediate CA, example root CA

creationDate (optional)

Long

The date the certificate was uploaded. In epoch format: int64

example: 1693415951000

errors (optional)

MtlsCertificateErrorsDto

hash (optional)

String

State representation. For Terraform provider use

example: bdf252eb5fc9ec468a966de1e9e83db676d1851c

issuedBy (optional)

String

The Certificate Authority that issued the certificate.

example: CN=example ca,OU=internal ca,O=ca,L=example city,ST=california,C=us

issuedTo (optional)

String

The domain that the certificate applies to.

example: CN=example company,OU=dev,O=IT,L=example city,ST=california,C=us

lastUpdate (optional)

Long

The date the certificate was updated. In epoch format: int64

example: 1693415951000

name (optional)

String

The name you assign to the certificate, and the unique identifier assigned by Imperva.

example: example-certificate

serialNumber (optional)

String

The certificate serial number that was assigned by the CA that signed the certificate.

example: 1234abcd

validFrom (optional)

Long

The date the certificate was issued. In epoch format: int64

example: 1655140751000

validUntil (optional)

Long

The date the certificate expires. In epoch format: int64

example: 1693415951000

MtlsCertificateDetailsResponse

data (optional)

array[MtlsCertificateBaseDetails]

mTLS certificate response.

MtlsCertificateErrorsDto

chainValid (optional)

Boolean

Is the chain of trust valid. False indicates that the signatures in the certificate are not valid.

expirationDateValid (optional)

Boolean

Indicates if the certificate expired or not.

RelatedSansDetails

List of related SANs using the same domain for validation

domainIds (optional)

array[Long]

List of domain ids that are being SSL covered by this SAN format: int64

example: 1

expirationDate (optional)

Long

format: int64

sanId (optional)

Long

format: int64

sanValue (optional)

String

SanInstructionsDto

certificateLevel (optional)

String

The level of the certificate (SITE or ACCOUNT)

Enum:

SITE

ACCOUNT

example: SITE

domain (optional)

String
 Domain to validate
 example: example.imperva.com
 expirationDate (optional)
Long
 SAN expiration date format: int64
 example: 1633180421000
 lastNotificationDate (optional)
Long
 Last date an email was sent format: int64
 example: 1633180421000
 recordType (optional)
String
 Record type for the validation
 Enum:
 TXT
 CNAME
 A
 NONE
 example: TXT
 relatedSansDetails (optional)
array[RelatedSansDetails]
 List of related SANs using the same domain for validation
 example: 1633180421000
 validationEmail (optional)
String
 Validation email
 example: example@imperva.com
 validationMethod (optional)
String
 Validation method of the SAN
 Enum:
 EMAIL
 DNS
 CNAME
 METATAG
 URL
 HTTP
 NONE
 example: DNS
 verificationCode (optional)
String
 Verification code of the SAN
 example: 856963
 verificationCodeExpirationDate (optional)
Long
 Verification code expiration date format: int64
 example: 1633180421000

SiteExternalDetails

List of the sites attached to the current certificate.
 accountId (optional)
Long
 The Imperva ID of the account. format: int64
 example: 22222
 externalId (optional)
Long

The Imperva ID of the website. format: int64

example: 11111

name (optional)

String

The name of the website.

example: my.domain.org

SiteSSLCertificatesSettings

defaultValidationMethod (optional)

String

The default validation method that will be used as part of the domain SSL validation process.

Enum:

DNS

CNAME

EMAIL

example: CNAME

siteCertificateEnabled (optional)

Boolean

Indicates whether the site certificate is enabled or not. When enabled, a site certificate is issued for all domains that are added manually to the website configuration in Imperva (“managed domains”).

example: true

siteld (optional)

Long

The Imperva ID of the onboarded website covered by the certificate format: int64

example: 856963

mtls_origin_body

certificateFile (optional)

byte[]

Your mTLS client certificate file. Supported formats: PEM, DER and PFX. Only RSA certificates are currently supported. The certificate RSA key size must be 2048 bit or less. The certificate must be issued by a certificate authority (CA) and cannot be self-signed. format: binary

certificateName (optional)

String

A descriptive name for your mTLS client certificate.

passphrase (optional)

String

Your private key passphrase. Leave empty if the private key is not password protected.

privateKeyFile (optional)

byte[]

Your private key file. supported formats: PEM, DER. If PFX certificate is used, then this field can remain empty. format: binary

origin_certificateId_body

certificateFile (optional)

byte[]

Your mTLS client certificate file. Supported formats: PEM, DER and PFX. Only RSA certificates are currently supported. The certificate RSA key size must be 2048 bit or less. The certificate must be issued by a certificate authority (CA) and cannot be self-signed. format: binary

certificateName (optional)

String

A descriptive name for your mTLS client certificate.

passphrase (optional)

String

Your private key passphrase. Leave empty if the private key is not password protected.

privateKeyFile (optional)**byte[]**

Your private key file. supported formats: PEM, DER. If PFX certificate is used, then this field can remain empty.
format: binary

Certificate Manager API

Configure client certificate support for your websites or web applications.

Manage and upload a Certificate Revocation List (CRL) file to verify whether certificates are valid and trustworthy.

For full feature documentation, see [Client Certificate Support](#).

Version: 1.0

BasePath:/certificate-manager

Imperva License Agreement

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

CRL

- `post /sites/{siteId}/CRL`
- `put /sites/{siteId}/CRL/{crlId}`
- `get /sites/{siteId}/CRL`
- `delete /sites/{siteId}/CRL/{crlId}`

ClientCertificates

- `post /v2/accounts/{accountId}/client-certificates`
- `post /v2/sites/{siteId}/client-certificates/{certId}`
- `delete /v2/sites/{siteId}/client-certificates/{certId}`
- `delete /v2/accounts/{accountId}/client-certificates/{certId}`
- `put /v2/sites/{siteId}/configuration/client-certificates`
- `get /v2/sites/{siteId}/client-certificates`
- `get /v2/sites/{siteId}/configuration/client-certificates`
- `get /v2/accounts/{accountId}/client-certificates`
- `get /v2/accounts/{accountId}/client-certificates/{certId}`
- `post /v2/sites/{siteId}/configuration/client-certificates`

CRL

```
post /sites/{siteId}/CRL
```

Add CRL to site (addCRL)

Path parameters

`siteId` (required)
 Path Parameter
 — The Imperva ID for the website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

`crl_file` (optional)
 Form Parameter
 — format: binary
`name` (optional)
 Form Parameter

Return type

CRLDetails

Example data

Content-Type: application/json

```
{
  "name" : "CRL Name",
  "siteId" : 1,
  "id" : 1,
  "creationDate" : "2023-07-18"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success CRLDetails

406

Invalid CRL file name, file limit exceeded, failed to read CRL file, unauthorized siteld

500

server error

```
put /sites/{siteId}/CRL/{crlId}
```

Update existing CRL on site (fullUpdateCRL)
Replaces the CRL currently uploaded to the website

Path parameters

siteld (required)

Path Parameter

— The Imperva ID for the website. format: int64

crlId (required)

Path Parameter

— The Imperva ID for the CRL. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

crl_file (optional)

Form Parameter

— format: binary

name (optional)

Form Parameter

—

Return type

CRLDetails

Example data

Content-Type: application/json

```
{
  "name" : "CRL Name",
  "siteId" : 1,
  "id" : 1,
  "creationDate" : "2023-07-18"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success CRLDetails

406

Invalid CRL file name, file limit exceeded, failed to read CRL file, unauthorized sitelid

500

server error

```
get /sites/{siteId}/CRL
```

List site CRLs (listCRLs)

Path parameters

sitelid (required)

Path Parameter

— The Imperva ID for the website. format: int64

Return type

CRLDetails

Example data

Content-Type: application/json

```
{
  "name" : "CRL Name",
```

```

    "siteId" : 1,
    "id" : 1,
    "creationDate" : "2023-07-18"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success CRLDetails

406

unauthorized siteld

500

failed to send CRL

```
delete /sites/{siteId}/CRL/{crlId}
```

Remove CRL from site (removeCRL)

Path parameters

siteld (required)

Path Parameter

— The Imperva ID for the website. format: int64

crlId (required)

Path Parameter

— The Imperva ID for the CRL. format: int64

Responses

200

success

406

unauthorized siteld

500server error

ClientCertificates

```
post /v2/accounts/{accountId}/client-certificates
```

Add client CA certificate to account (addClientCACert)

Path parameters

accountId (required)

Path Parameter

— The Imperva ID for the account. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

ca_file (optional)

Form Parameter

— format: byte

name (optional)

Form Parameter

—

Return type

[ClientCACertificateDetails](#)

Example data

Content-Type: application/json

```
{
  "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
  "name" : "Cert name",
  "id" : 1,
  "validFrom" : "2000-01-23T04:56:07.000+00:00",
  "creationDate" : "2023-07-18",
  "issuer" : "EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US",
  "hash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
  "validTo" : "2000-01-23T04:56:07.000+00:00"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateDetails

401

unauthorized account

406

bad request

500

failed to add ca certificate

```
post /v2/sites/{siteId}/client-certificates/{certId}
```

Assign client CA certificate of the account to site (assignSiteToCertificate)

Path parameters

siteId (required)

Path Parameter

— The Imperva ID for the website. format: int64

certId (required)

Path Parameter

— The Imperva ID assigned to an uploaded certificate.
Run GET method to locate the certificate ID. format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success

401

unauthorized site

406

bad request

500

failed to assign ca certificate to site

```
delete /v2/sites/{siteId}/client-certificates/{certId}
```

Remove client CA certificate from site (deassignCertFromSite)

Path parameters

siteId (required)

Path Parameter

— The Imperva ID for the website. format: int64

certId (required)

Path Parameter

— The Imperva ID assigned to an uploaded certificate.
Run GET method to locate the certificate ID. format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success

401

unauthorized site

406

bad request

500

failed to remove ca certificate from site

```
delete /v2/accounts/{accountId}/client-certificates/{certId}
```

Delete client CA certificate from account (deleteClientCaCert)

Path parameters

accountId (required)

Path Parameter

— The Imperva ID for the account. format: int64

certId (required)

Path Parameter

— The Imperva ID assigned to an uploaded certificate.
Run GET method to locate the certificate ID. format: int64

Responses

200

success

401

unauthorized account

406

bad request

500

Could not delete certificate

```
put /v2/sites/{siteId}/configuration/client-certificates
```

Overwrite the client CA certificate configuration (full update) (fullUpdateSiteConfiguration)

Path parameters

siteId (required)

Path Parameter

— The Imperva ID for the website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ClientCACertificateSiteConfiguration (required)

Body Parameter

— configuration to update

Return type

ClientCACertificateSiteConfiguration

Example data

Content-Type: application/json

```
{
  "isDisableSessionResumption" : true,
  "headerName" : "Full-Cert",
  "hosts" : [ "imperva.com", "imprevaservices.com" ],
  "isPortsException" : false,
  "headerValue" : "FULL_CERT",
  "ports" : [ 80, 9000 ],
  "mandatory" : true,
  "isHostsException" : false,
  "forwardToOrigin" : true,
  "fingerprints" : "F009B2EABECCBE9BFBE23B8C57A684650B8564A9"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateSiteConfiguration

401

unauthorized account

406

invalid Json

500

server error

```
get /v2/sites/{siteId}/client-certificates
```

List all client CA certificates assigned to site (getAllCertsForSite)

Path parameters

siteId (required)

Path Parameter

— The Imperva ID for the website. format: int64

Return type

ClientCACertificateDetails

Example data

Content-Type: application/json

```
{
  "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
  "name" : "Cert name",
  "id" : 1,
  "validFrom" : "2000-01-23T04:56:07.000+00:00",
  "creationDate" : "2023-07-18",
  "issuer" : "EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US",
  "hash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
  "validTo" : "2000-01-23T04:56:07.000+00:00"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateDetails

401

unauthorized site

406

bad request

```
get /v2/sites/{siteId}/configuration/client-certificates
```

Get client CA certificate configuration for site (getSiteConfiguration)

Path parameters

siteld (required)

Path Parameter

— The Imperva ID for the website. format: int64

Return type

ClientCACertificateSiteConfiguration

Example data

Content-Type: application/json

```
{
  "isDisableSessionResumption" : true,
  "headerName" : "Full-Cert",
  "hosts" : [ "imperva.com", "imprevaservices.com" ],
  "isPortsException" : false,
  "headerValue" : "FULL_CERT",
  "ports" : [ 80, 9000 ],
  "mandatory" : true,
  "isHostsException" : false,
  "forwardToOrigin" : true,
  "fingerprints" : "F009B2EABECCBE9BFBE23B8C57A684650B8564A9"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateSiteConfiguration

401

unauthorized account

```
get /v2/accounts/{accountId}/client-certificates
```

List client CA certificates in account (listClientCACertsByAccount)

Path parameters

accountId (required)

Path Parameter

— The Imperva ID for the account. format: int64

Return type

array[ClientCACertificateDetails]

Example data

Content-Type: application/json

```
[ {
    "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
    "name" : "Cert name",
    "id" : 1,
    "validFrom" : "2000-01-23T04:56:07.000+00:00",
    "creationDate" : "2023-07-18",
    "issuer" : "EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US",
    "hash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
    "validTo" : "2000-01-23T04:56:07.000+00:00"
}, {
    "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
    "name" : "Cert name",
    "id" : 1,
    "validFrom" : "2000-01-23T04:56:07.000+00:00",
    "creationDate" : "2023-07-18",
    "issuer" : "EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US",
    "hash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
    "validTo" : "2000-01-23T04:56:07.000+00:00"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success

401

unauthorized account

403

forbidden access

```
get /v2/accounts/{accountId}/client-certificates/{certId}
```

Get client CA certificate information including assigned sites (listSitesByCert)

Path parameters

accountId (required)

Path Parameter

— The Imperva ID for the account. format: int64

certId (required)

Path Parameter

— The Imperva ID assigned to an uploaded certificate.
Run GET method to locate the certificate ID. format: int64

Return type

ClientCACertificateDetails

Example data

Content-Type: application/json

```
{
  "serialNumber" : "FB:4B:BD:4B:1B:7D:7C:CF",
  "name" : "Cert name",
  "id" : 1,
  "validFrom" : "2000-01-23T04:56:07.000+00:00",
  "creationDate" : "2023-07-18",
```

```

    "issuer" : "EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US",
    "hash" : "a94a8fe5ccb19ba61c4c0873d391e987982fbbd3",
    "validTo" : "2000-01-23T04:56:07.000+00:00"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateDetails

401

unauthorized account

406

bad request

```
post /v2/sites/{siteId}/configuration/client-certificates
```

Modify the client CA certificate configuration (partial update) (partialUpdateSiteConfiguration)

Path parameters

siteId (required)

Path Parameter

— The Imperva ID for the website. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ClientCACertificateSiteConfiguration (required)

Body Parameter

— configuration sections to update

Return type

ClientCACertificateSiteConfiguration

Example data

Content-Type: application/json

```
{
  "isDisableSessionResumption" : true,
  "headerName" : "Full-Cert",
  "hosts" : [ "imperva.com", "imprevaservices.com" ],
  "isPortsException" : false,
  "headerValue" : "FULL_CERT",
  "ports" : [ 80, 9000 ],
  "mandatory" : true,
  "isHostsException" : false,
  "forwardToOrigin" : true,
  "fingerprints" : "F009B2EABECCBE9BFBE23B8C57A684650B8564A9"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

success ClientCACertificateSiteConfiguration

401

unauthorized account

406

invalid Json

500

server error

Models

Methods

Table of Contents

1. CRLDetails
2. CRL_crlId_body
3. ClientCACertificateDetails
4. ClientCACertificateSiteConfiguration
5. accountId_clientcertificates_body
6. siteId_CRL_body

CRLDetails

id (optional)
Long
format: int64
example: 1
name (optional)
String
example: CRL Name
creationDate (optional)
String
example: 2023-07-18
siteId (optional)
Long
format: int64
example: 1

CRL_crlId_body

crl_file (optional)
byte[]
Upload a Certificate Revocation List (CRL) file for your website.
The CRL file must be in PEM format, using Base64 encoding and cannot be larger than 1MB.
Replaces a CRL currently uploaded to the website. format: binary
name (optional)
String
CRL name

ClientCACertificateDetails

id (optional)
Long
format: int64
example: 1
name (optional)
String
example: Cert name
serialNumber (optional)
String
example: FB:4B:BD:4B:1B:7D:7C:CF
issuer (optional)
String
example: EMAILADDRESS@example@email.com, CN=My-company, OU=Support, O=My-company, ST=California, C=US
validFrom (optional)

Date
 format: date-time
 validTo (optional)

Date
 format: date-time
 creationDate (optional)
String
 example: 2023-07-18
 hash (optional)
String
 example: a94a8fe5ccb19ba61c4c0873d391e987982fbcd3

ClientCACertificateSiteConfiguration

mandatory (optional)

Boolean

When set to true, the end user is required to present the client certificate in order to access the site. By default, set to false.

example: true

ports (optional)

array[Long]

The ports on which client certificate authentication is supported. If left empty, client certificates are supported on all ports. format: int64

example: [80,9000]

isPortsException (optional)

Boolean

When set to true, client certificates are not supported on the ports listed in the Ports field ('blacklisted'). By default, set to false.

example: false

hosts (optional)

array[String]

The hosts on which client certificate authentication is supported. If left empty, client certificates are supported on all hosts.

example: ["imperva.com", "imprevervices.com"]

isHostsException (optional)

Boolean

When set to true, client certificates are not supported on the hosts listed in the Hosts field ('blacklisted'). By default, set to false.

example: false

fingerprints (optional)

array[String]

Permitted client certificate fingerprints. If left empty, all fingerprints are permitted.

example: F009B2EABECCBE9BFBE23B8C57A684650B8564A9

forwardToOrigin (optional)

Boolean

When set to true, the contents specified in headerValue are sent to the origin server in the header specified by headerName. By default, set to false.

example: true

headerName (optional)

String

The name of the header to send header content in. By default, the header name is 'clientCertificateInfo'.

example: Full-Cert

headerValue (optional)

String

The content to send in the header specified by headerName. One of the following: FULL_CERT (for full certificate in Base64) COMMON_NAME (for certificate's common name (CN)) FINGERPRINT (for the certificate fingerprints in SHA1) SERIAL_NUMBER (for the certificate's serial number)

Enum:

FULL_CERT
COMMON_NAME
FINGERPRINT
SERIAL_NUMBER
example: FULL_CERT
isDisableSessionResumption (optional)
Boolean

accountId_clientcertificates_body

ca_file
byte[]
Upload a client certificate for your website.
The certificate must be in PEM format.
Supported file extensions include .pem, .crt and .cer. format: byte
name (optional)
String
CA certificate file name

siteId_CRL_body

crl_file (optional)
byte[]
Upload a Certificate Revocation List (CRL) file for your website.
The CRL file must be in PEM format, using Base64 encoding and cannot be larger than 1MB.
Replaces a CRL currently uploaded to the website. format: binary
name (optional)
String
CRL name

Imperva API2 WAF

To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your Cloud Application Security account and websites. These APIs provide either an alternative to existing APIs, or provide APIs with new functionality. For more details about Imperva APIs, see [Imperva API Documentation](#).

Version: 2.0.0
BasePath:/api/prov/v2
All rights reserved
<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

CustomCertificate

- `delete /sites/{extSiteId}/customCertificate`
- `put /sites/{extSiteId}/customCertificate`

CustomCertificate

```
delete /sites/{extSiteId}/customCertificate
```

Remove custom certificate (sitesExtSiteIdCustomCertificateDelete)

Remove the custom certificate uploaded to Imperva for a specified website.

Path parameters

`extSiteId` (required)

Path Parameter

— The Imperva ID of your website.

Query parameters

`auth_type` (required)

Query Parameter

—

Responses

200

OK

500

Internal Server Error

```
put /sites/{extSiteId}/customCertificate
```

Upload custom certificate (sitesExtSiteIdCustomCertificatePut)

Upload your own SSL certificate to Imperva for a specified website. This certificate is presented to SNI-supporting clients only.

Supported file formats: PFX, PEM, CER. The certificate and private key must be in Base64 format.

Path parameters

`extSiteId` (required)

Path Parameter

— The Imperva ID of your website.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `customCertificateBody` (required)
Body Parameter

Responses

200

OK

400

Bad Request

401

Unauthorized siteld

500

Internal Server Error

Models

Methods

Table of Contents

1. `customCertificateBody`

`customCertificateBody`

certificate (optional)

String

The certificate content in base64 format.

example: LS0tLS1CRUdJTiBDRVJU...WS1BFZU1LbUk9Ci0tLS0tRU5EIENFUlJRkIDQVRFLS0tLS0=

private_key (optional)

String

The private key of the certificate in base64 format.

example: LS0tLS1CRUdJTiBQUkIW...VRFIFhSXp0bUcvN3RSTkJZY3NFMnpXZmtFZ0VOSzUyajNvcTYKTzVnNjhoTm1PQTk1dlpacIRTekJYa2M9Ci0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K

passphrase (optional)

String

The passphrase used to protect your SSL certificate.

example: 1234

auth_type (optional)

String

The authentication type of the certificate (RSA or ECC)

example: RSA or ECC

Imperva API2 WAF

To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your Cloud Application Security account and websites. These APIs provide either an alternative to existing APIs, or provide APIs with new functionality. For more details about Imperva APIs, see [Imperva API Documentation](#).

Version: 2.0.0

BasePath:/api/prov/v2

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

CustomCertificateWithHMSupport

- `get /sites/{extSiteId}/hsmCertificate/connectivityTest`
- `delete /sites/{extSiteId}/hsmCertificate`
- `put /sites/{extSiteId}/hsmCertificate`

CustomCertificateWithHMSupport

```
get /sites/{extSiteId}/hsmCertificate/connectivityTest
```

Test connectivity between Imperva and HSM provider (`sitesExtSiteIdHsmCertificateConnectivityTestGet`)
Test connectivity between Imperva and your HSM service provider. This endpoint also validates the integrity between the certificate and the private key, provided by the HSM service.

Path parameters

`extSiteId` (required)

Path Parameter

— The Imperva ID of your website.

Responses

200

OK

400

Bad Request

500

Internal Server Error

```
delete /sites/{extSiteId}/hsmCertificate
```

Remove custom certificate and HSM credentials (sitesExtSitIdHsmCertificateDelete)
Remove custom certificate and HSM credentials.

Path parameters

extSitId (required)

Path Parameter

— The Imperva ID of your website.

Responses

200

OK

500

Internal Server Error

```
put /sites/{extSiteId}/hsmCertificate
```

Upload custom certificate and HSM credentials (sitesExtSitIdHsmCertificatePut)
Upload a custom certificate without the private key. Provide credentials for the HSM service that is managing your private key.

Path parameters

extSitId (required)

Path Parameter

— The Imperva ID of your website.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **hsmBody** (required)

Body Parameter

— The private key asset details in your HSM service.

Responses

200

OK

401

Unauthorized siteld

400

Bad Request

500

Internal Server Error

Models

Methods

Table of Contents

1. **hsmBody**
2. **hsmBody_data**
3. **hsmBody_data_hsmDetails**

hsmBody

data (optional)

hsmBody_data

hsmBody_data

An object that contains the certificate string and the hsmDetails object

certificate (optional)

String

The certificate content in base64 format.

example: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSLofd4d6gjFsRENDQW55Z0F3SUJBZ0IKQU1sSDZPNzB3b2FvTUEwR0NTcUdTSWlzRFFFQkN3VUFNR2t4Q3pBSkJnTIYKQkFZVEFrB1NUTh3RFFZRFZRUUIEQVpKYzNKaFpXd3hFREFPQmdOVkJBY01CM0psYUc5MmlzUXhFakFRQmdOVgpCQW9NQ1UxNVEyOXRjR0Z1ZVRFTU1Bb0dBMVVFQ3d3RFpHVjJNUIV3RxZRFZRUUREQXhwYm1OaGNIUmjM1F1ClkyOHdlaGNOTWpFd09EQXINRGt6TURJNVdoY05Nak13T0RBeU1Ea3pNREk1V2pCcE1Rc3dUVIEViFRR0V3SkokVERFUE1BMEdBMVVFQ0F3R1NYTn1ZV1ZzTVJBd0RnWURWUVFIREFkeVpXaHZkbTkWTVJJd0VBWURWUVFLREFsTgplVU52YlhCaGJua3hEREFLQmdOVkJBc01BIMJsZGpFV1CTUdBMVVFQX3dTWFXNWpZWEIwWhOMExtTnZNSUICClqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUICQ2dLQ0FRRUE3M2JGcXI3bTRtNmMvenc0dDREK2IINMKYmdzenExTnZqcFArOG01NDk2U01RNlh3dCsyN21SWIM4TGRqbDBC2VFVWCtHTUITUkc0aElPa0hYMkpTUIBScAozdUUrOXFOaVhOQ3lwZkxiZENSZHVDRL0MER6WmtlUVRPZXZpL3JsN0p6ZXREZGZDd2R4dFIHNG40ZzM0VnFDCIY2NKZHWXkvRFU0WERkeW5neFhscVRZ0VRMGd5eThnUm9VR2Vlb2N2Mi8wdFgxOudWOFI5Q0FlaVIWOURGMHQZ1VqY0VwcEJ3NDlwTG4wOW9JN2JEbjNYdFJMYWVZbk4vRytnbW5TVWp6NjByMTg2ZVVCV2MrK3N2dXc3Tmt3MwpsUTgwdGw2UTZOUV4vbjhqY0ZPczgvOGNpVDVxM0VxcXILdIRhSXdJYVJZUEpEUjRZS1NYb3UvZ0IBZ1RYUUIECkFRQUJvejh3UFRBTEJnTIZIUThFQkFNQ0JEQXdFd1IEVIIwbEJBd3dDZ1JS3dZQkJRVUhBd0V3R1FZRFZSMFIKQkJd0VJSU9LaTVwYm1OaGNIUmjM1F1WTI4d0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dFQkFLT0xVUkZodldzZwpYeis1aUkwWTZaSnk2c0FOaGZIWTM5TTFrcytwMXBkZ1pkOHhKMFplenZNT000Yi80QjVmTWR5eXp2QUdMemgvCmtlZFFEU3NQUIRkcDVJT1RQd1VSNW9SN3owYjZpV2JWTTVBTW5SbHhkUHFydWhMc0JuZncxVG5MaIVrYWtRSUgKS3hPenczdZdSZ24xaEsxZHVrUVc3WTdnem0vWnJuTXUwYkkvUnhrc1JLbIhleGpnZXNyBWXWGrSEowQXAxNQpEcjF3OTVrL1ZPbVBcjViYTRIK1dkTURnTDhRYUpndGprZjdyd01MdKJDU1piR1FIQVarU2QyOEoyNVlwSXVrCjN2Y0dLMHM4UFoxeGFtU1BWU2VLaVZHNVU4OXdjB0FXTEewS24zSVJDczRvNnptODE2QUNXb3pQM2g3bGIVSGUKaG9WS1BFZU1LbUk9Ci0tLS0tRU5EIENFUJRk1dQVRFLS0tLS0=

hsmDetails (optional)

array[hsmBody_data_hsmDetails]

An array of your private key asset details in your HSM service

hsmBody_data_hsmDetails

keyId (optional)

String

The key ID for the private key in your HSM service.

example: 257r65d8-9d62-8l16-91g2-7g64345278n2

apiKey (optional)

String

The API_key for the private key in your HSM service.

example: MTAyRVdmMzBsZGRmOC00NzRmLWFmNWltMjk4MmU3YWMYTkWOnQzMXRNZUE4dHhjYmtVTjZoWURRSldY2w3WINmVExtGXkzSJ0Z24SMzB1D3k2NDNGbnEwdkVQcnkDUXhGcGdsR1dPcrKFSTyaBBjSnJmTndwTkdn

hostName (optional)

String

The address (URI) of your assets in your HSM service.

example: api.amer.smartkey.io

Imperva Troubleshooting Page API

Gain more visibility into connectivity issues that occur when Imperva data centers cannot reach your origin web servers. For full feature documentation, see [Troubleshoot Website Errors](#).

Version: 1.0.0

BasePath:/troubleshooting-center

The terms in the absence of an applicable signed agreement between you and Imperva

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

ConnectivityTests

- `post /v3/connectivityTests/{assetType}/{assetId}`

ConnectivityTests

```
post /v3/connectivityTests/{assetType}/{assetId}
```

Retrieve connectivity tests for a given website. (getConnectivityCheckApiResult)
Retrieves details of connectivity tests of a given website.

Path parameters

`assetType` (required)
Path Parameter

—
`assetId` (required)
Path Parameter
— Numeric identifier of the site to retrieve. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

`body ConnectivityTestSearch` (required)
Body Parameter
— Filters

Return type

`ApiResult`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "timeStamp" : 1672841491000,
    "pop" : {
      "popId" : "ast",
      "popName" : "AST, London"
    },
    "tcpPort" : 8080,
    "accountId" : 15,
    "connectivityTestId" : "3",
    "originCNAME" : "my-test.site.net",
    "siteId" : 10,
    "errorCode" : "20",
    "connectivityTestsList" : [ {
      "checkType" : "PING",
      "check" : "PING 8.8.8.8 (8.8.8.8): 56 data bytes..."
    }, {
      "checkType" : "MTR",
      "check" : "Start: 2021-03-10T14:02:24+0200..."
    }, {
      "checkType" : "MTR_TCP",
      "check" : "Start: 2021-03-10T14:02:24+0200..."
    }],
    "originIP" : "192.5.10.41"
  }, {
    "timeStamp" : 1672841491000,
    "pop" : {
      "popId" : "ast",
      "popName" : "AST, London"
    },
    "tcpPort" : 8080,
    "accountId" : 15,
    "connectivityTestId" : "3",
    "originCNAME" : "my-test.site.net",
    "siteId" : 10,
    "errorCode" : "20",
    "connectivityTestsList" : [ {
      "checkType" : "PING",
      "check" : "PING 8.8.8.8 (8.8.8.8): 56 data bytes..."
    }, {
      "checkType" : "MTR",
      "check" : "Start: 2021-03-10T14:02:24+0200..."
    }, {
      "checkType" : "MTR_TCP",
      "check" : "Start: 2021-03-10T14:02:24+0200..."
    }],
    "originIP" : "192.5.10.41"
  }],
  "meta" : {
    "limit" : 50,
    "totalPages" : 20,
    "page" : 1
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

401

Unauthorized [ErrorResponse](#)

404

Not Found [ErrorResponse](#)

200

Successful operation [ApiResult](#)

500

Internal Error [ErrorResponse](#)

400

Bad Request [ErrorResponse](#)

Models

Methods

Table of Contents

1. [APIError](#)
2. [ApiResult](#)
3. [Check](#)
4. [ConnectivityTest](#)
5. [ConnectivityTestSearch](#)
6. [ErrorResponse](#)
7. [Meta](#)
8. [Pop](#)

APIError

[status \(optional\)](#)

Integer
format: int32
id (optional)
String
code (optional)
String
source (optional)
map[String, Object]
title (optional)
String
detail (optional)
String

ApiResult

meta (optional)
Meta
data (optional)
array[ConnectivityTest]

Check

Output of connectivity test performed against origin server
check_type (optional)
String
Enum:
PING
MTR
MTR_TCP
check (optional)
String

ConnectivityTest

connectivityTestId (optional)
String
Numeric identifier of the connectivity test that was performed against the origin server.
example: 3
sitId (optional)
Long
Numeric identifier of the site the test was performed on. format: int64
example: 10
accountId (optional)
Long
Numeric identifier of the account the site belongs to. format: int64
example: 15
originIP (optional)
String
The IP of the origin server (that was resolved when the test was performed).
example: 192.5.10.41
originCNAME (optional)
String
The CNAME of the origin server.
example: my-test.site.net
timeStamp (optional)
Long

The timestamp in which the connectivity test was performed. format: int64

example: 1672841491000

pop (optional)

Pop

errorCode (optional)

String

The error code that triggered the connectivity test.

example: 20

tcpPort (optional)

Integer

The port the MTR over TCP test is performed against. format: int32

example: 8080

connectivityTestsList (optional)

array[Check]

Output of connectivity test performed against origin server

example: [{"checkType": "PING", "check": "PING 8.8.8.8 (8.8.8.8): 56 data bytes...", "start": "2021-03-10T14:02:24+0200..."}, {"checkType": "MTR", "check": "Start: 2021-03-10T14:02:24+0200...", "start": "2021-03-10T14:02:24+0200..."}]

ConnectivityTestSearch

start

Long

Start of search time range (in milliseconds) format: int64

example: 1672841491000

end (optional)

Long

End of search time range (in milliseconds) format: int64

example: 1672841591000

limit (optional)

Integer

The number of objects to return in the response.
Default: 100
Possible values: 10, 25, 50, 100 format:

int32

example: 50

page (optional)

Integer

The page to return starting from 1. format: int32

example: 1

connectivityTestIds (optional)

array[Long]

format: int64

errorCodesList (optional)

array[Integer]

format: int32

popsIdsList (optional)

array[String]

originIPsList (optional)

array[String]

originCNAMEsList (optional)

array[String]

ErrorResponse

errors (optional)

array[APIError]

Meta

page (optional)

Long

The page returned format: int64

example: 1

limit (optional)

Long

The number of connectivity test returned per page format: int64

example: 50

totalPages (optional)

Long

The total number of pages in search result format: int64

example: 20

Pop

popId (optional)

String

example: ast

popName (optional)

String

example: AST, London

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Integrations

- post /api/integration/v1/clapps
 - post /api/integration/v1/geo
 - get /api/integration/v1/ips
 - post /api/integration/v1/ips
 - post /api/integration/v1/texts
-

Integrations

```
post /api/integration/v1/clapps
```

Get client applications info (getClappsInfo)
 Use this operation to retrieve a list of all the client applications.

Return type

ApiResultGetClappsInfo

Example data

Content-Type: application/json

```
{
  "clientApps" : {
    "1" : "Firefox"
  },
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  },
  {
    "key" : { }
  } ],
  "clientAppTypes" : {
    "1" : "Browser"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success ApiResultGetClappsInfo

```
post /api/integration/v1/geo
```

Get geographical info (getGeoInfo)
 Use this operation to retrieve a list of all the countries and continents codes.

Return type

[GeoInfo](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "continentsCodes" : {
    "AF" : "Africa"
  },
  "countriesCodes" : {
    "BD" : "Bangladesh",
    "BE" : "Belgium"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[Success GeoInfo](#)

```
get /api/integration/v1/ips
```

Get Imperva IP ranges (getIPRanges)

Use this operation to get the updated list of Imperva IP ranges. This list may be used to define firewall rules that restrict access to customers sites from non-Imperva IPs.

Query parameters

resp_format (optional)

Query Parameter

— Response format.
Possible values: json | apache | nginx | iptables | text
Default: json

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
14001 - Format invalid [inline_response_200](#)

```
post /api/integration/v1/ips
```

Get Imperva IP ranges (getIPRangesWithPost)

Use this operation to get the updated list of Imperva IP ranges. This list may be used to define firewall rules that restrict access to customers sites from non-Imperva IPs.

Query parameters

resp_format (optional)

Query Parameter

— Response format.
Possible values: json | apache | nginx | iptables | text
Default: json

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
14001 - Format invalid inline_response_200

```
post /api/integration/v1/texts
```

Get texts (getTexts)

Use this operation to retrieve a list of all text messages that may be part of API responses. For each message a key and a value are provided. The key is the unique identifier of the message and the value is the message text itself, in the API's default locale (English).

Return type

[ApiResultGetTexts](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "texts" : {
    "api.stats.visits_timeseries.human" : "Human visits",
    "api.stats.visits_timeseries.bot" : "Bot visits",
    "api.threats.followup.view" : "View Incidents"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success `ApiResultGetTexts`

Models

Methods

Table of Contents

1. `ApiResult`
2. `ApiResultGetClappsInfo`
3. `ApiResultGetTexts`
4. `ApiResultIncapsulaRanges`
5. `GeoInfo`
6. `inline_response_200`

`ApiResult`

res (optional)

`Integer`

res - contains specific error code format: int32

example: 0

res_message (optional)

`String`

example: OK

debug_info (optional)

`array[map[String, Object]]`

`ApiResultGetClappsInfo`

res (optional)

`Integer`

res - contains specific error code format: int32

example: 0

res_message (optional)

`String`

example: OK

debug_info (optional)

`array[map[String, Object]]`

clientApps (optional)

`array[map[String, Object]]`

example: {"1":"Firefox"}

clientAppTypes (optional)

`array[map[String, Object]]`

example: {"1":"Browser"}

ApiResultGetTexts

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
array[map[String, Object]]
 texts (optional)
array[map[String, Object]]
 example: {"api.stats.visits_timeseries.human":"Human visits","api.stats.visits_timeseries.bot":"Bot visits","api.threats.followup.view":"View Incidents"}

ApiResultIncapsulaRanges

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
array[map[String, Object]]
 ipRanges (optional)
array[Object]
 ipv6Ranges (optional)
array[Object]

GeoInfo

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
array[map[String, Object]]
 countriesCodes (optional)
array[map[String, Object]]
 example: {"BD":"Bangladesh","BE":"Belgium"}
 continentsCodes (optional)
array[map[String, Object]]
 example: {"AF":"Africa"}

inline_response_200**Imperva API Documentation****Imperva API Documentation**

Version: 1.0.0

BasePath:/policies

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

PolicyManagement

- `get /v2/policies/{policyId}/assets/{assetType}/{assetId}`
- `post /v2/policies`
- `delete /v2/policies/{policyId}`
- `get /v3/policies`
- `get /v2/policies`
- `get /v2/policies/{policyId}`
- `post /v2/policies/{policyId}`
- `put /v2/policies/{policyId}`
- `patch /v2/policies/{policyId}/{assetType}/{assetId}`

PolicyManagementAccountApplication

- `post /v2/accounts/{subAccountId}/policies/{policyId}`
- `get /v3/accounts/associated-policies`
- `get /v2/accounts/policies/{policyId}`
- `patch /v3/accounts/associated-policies`
- `put /v3/accounts/associated-policies`
- `delete /v2/accounts/{subAccountId}/policies/{policyId}`
- `put /v2/accounts/policies/{policyId}`

PolicyManagementAssetApplication

- `post /v2/assets/{assetType}/{assetId}/policies/{policyId}`
- `get /v2/assets/policies/{policyId}`
- `get /v2/assets/{assetType}/{assetId}/policies`
- `delete /v2/assets/{assetType}/{assetId}/policies/{policyId}`
- `put /v2/assets/{assetType}/{assetId}/policies/{policyId}`

PolicyManagement

```
get /v2/policies/{policyId}/assets/{assetType}/{assetId}
```

Check whether the policy is applied on the asset (checkIfPolicyIsAppliedOnAsset)
True if the policy is applied on the asset

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

assetType (required)

Path Parameter

— The type of asset on which the policy is applied

assetId (required)

Path Parameter

— Asset ID format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the check is performed for an asset that belongs to the account (A) associated with the API credentials used for authentication. To check for an asset that belongs to a different account (an account under the account (A)), specify the account ID. format: int64

Return type

GetPolicyResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "accountId" : 10,
    "policySettings" : [ {
      "data" : {
        "geo" : {
          "countries" : [ "AE", "AC" ],
          "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
          "pattern" : "EQUALS",
          "url" : "/test"
        }, {
          "pattern" : "EQUALS",
          "url" : "/test"
        } ],
        "ips" : [ "ips", "ips" ]
      }
    }
  }
}
```

```

},
"policyId" : 10,
"policySettingType" : "IP/GEO/URL",
"policyDataExceptions" : [ {
  "data" : [ {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  } ],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
}, {
  "data" : [ {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  } ],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
}, {
  "data" : {
    "geo" : {
      "countries" : [ "AE", "AC" ],
      "continents" : [ "APAC", "US" ]
    },
    "urls" : [ {
      "pattern" : "EQUALS",
      "url" : "/test"
    }, {
      "pattern" : "EQUALS",
      "url" : "/test"
    } ],
    "ips" : [ "ips", "ips" ]
  },
  "policyId" : 10,
  "policySettingType" : "IP/GEO/URL",
  "policyDataExceptions" : [ {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    }, {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
}, {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
} ]
}

```

```

        "values" : [ "values", "values" ]
    } ,
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
} ],
"policySettingsId" : 55,
"comment" : "exclude all ips for pen tests",
"id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
} ],
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [ {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
}, {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
} ],
"description" : "This is policy blocks all requests from Europe",
"enabled" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [GetPolicyResponse](#)

404

Not found [PolicyBaseFailureResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
post /v2/policies
```

Add a new policy or copy an existing policy (createNewPolicy)

When copying an existing policy the body is ignored but nevertheless needs to be sent. A good approach is to send an empty JSON as the request body, e.g {}

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body PolicyDto (required)

Body Parameter

Query parameters

sourcePolicyId (optional)

Query Parameter

— Optional to clone full policy data format: int64

caid (optional)

Query Parameter

— By default, the policy is created for the account (A) associated with the API credentials used for authentication.

To create the policy for a different account (an account under the account (A)), specify the account ID. format:

int64

Return type

GetPolicyResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "accountId" : 10,
    "policySettings" : [ {
      "data" : {
        "geo" : {
          "countries" : [ "AE", "AC" ],
          "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
          "pattern" : "EQUALS",
          "url" : "/test"
        }, {
          "pattern" : "EQUALS",
          "url" : "/test"
        } ],
        "ips" : [ "ips", "ips" ]
      }
    }
  }
}
```

```

},
"policyId" : 10,
"policySettingType" : "IP/GEO/URL",
"policyDataExceptions" : [ {
  "data" : [ {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  } ],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
}, {
  "data" : [ {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  } ],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
}, {
  "data" : {
    "geo" : {
      "countries" : [ "AE", "AC" ],
      "continents" : [ "APAC", "US" ]
    },
    "urls" : [ {
      "pattern" : "EQUALS",
      "url" : "/test"
    }, {
      "pattern" : "EQUALS",
      "url" : "/test"
    } ],
    "ips" : [ "ips", "ips" ]
  },
  "policyId" : 10,
  "policySettingType" : "IP/GEO/URL",
  "policyDataExceptions" : [ {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    }, {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
}, {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
} ]
}

```

```

        "values" : [ "values", "values" ]
    } ,
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
} ],
"policySettingsId" : 55,
"comment" : "exclude all ips for pen tests",
"id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
} ],
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [ {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
}, {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
} ],
"description" : "This is policy blocks all requests from Europe",
"enabled" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [GetPolicyResponse](#)

400

Bad Request [SimpleTextErrorResponse](#)

500

Internal Error [SimpleTextErrorResponse](#)

```
delete /v2/policies/{policyId}
```

Delete an existing policy (deletePolicy)

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the policy is deleted for the account (A) associated with the API credentials used for authentication.

To delete the policy for a different account (an account under the account (A)), specify the account ID. format:

int64

uiContext (optional)

Query Parameter

Return type

PolicyResult

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : { }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Success PolicyResult

400

Bad Request SimpleTextErrorResponse

500

Internal Error SimpleTextErrorResponse

```
get /v3/policies
```

Get account policies by filter (getAccountPoliciesByFilter)

Get Policies for the account based on the provided filters. If no filters are provided, all policies for the account will be returned according to the page size.

Query parameters

policyIds (optional)

Query Parameter

— A list of policy ids. If this parameter is provided, only policies matching one of these ids will be returned. format: int64

names (optional)

Query Parameter

— A list of policy names. If this parameter is provided, only policies matching one of these names will be returned.

types (optional)

Query Parameter

— A list of policy types. If this parameter is provided, only policies matching one of these types will be returned.

assetIds (optional)

Query Parameter

— A list of website ids. If this parameter is provided, only websites matching one of these IDs will be returned.

format: int64

subAccIds (optional)

Query Parameter

— A list of sub account ids. If this parameter is provided, websites corresponding to the sub account ids will be returned.

</br> Else it will default to return all sites corresponding to the acc id in user jwt format: int64

page (optional)

Query Parameter

— The page to return starting from 0. default: 0 format: int32

size (optional)

Query Parameter

— Page size used to determine the first object to be returned and the number of objects to be returned. default:

20 format: int32

extended (optional)

Query Parameter

— Extended parameter is used to determine whether to return a more detailed policies dto. default: false

caid (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

Return type

PaginatedCollectionPolicyDtoWithAssetsAndSubAccountsAssignment

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 10,
    "assetIds" : [ 0, 0 ],
    "policySettings" : [ {
      "data" : {
        "geo" : {
          "countries" : [ "AE", "AC" ],
          "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
          "pattern" : "EQUALS",
          "url" : "/test"
        }, {
          "pattern" : "EQUALS",
          "url" : "/test"
        } ],
        "ips" : [ "ips", "ips" ]
      },
      "policyId" : 10,
      "policySettingType" : "IP/GEO/URL",
      "policyDataExceptions" : [ {
        "data" : [ {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        }, {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        } ],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
      }, {
        "data" : [ {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        }, {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        } ],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
      }, {
        "id" : 10,
        "settingsAction" : "BLOCK"
      }, {
        "data" : {
          "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
          },
          "urls" : [ {
            "pattern" : "EQUALS",
            "url" : "/test"
          }, {
            "pattern" : "EQUALS",
            "url" : "/test"
          } ],
        }
      }
    }
  }
}
```

```

        "ips" : [ "ips", "ips" ]
    },
    "policyId" : 10,
    "policySettingType" : "IP/GEO/URL",
    "policyDataExceptions" : [
        {
            "data" : [
                {
                    "exceptionType" : "GEO",
                    "values" : [ "values", "values" ]
                },
                {
                    "exceptionType" : "GEO",
                    "values" : [ "values", "values" ]
                }
            ],
            "policySettingsId" : 55,
            "comment" : "exclude all ips for pen tests",
            "id" : 10
        },
        {
            "data" : [
                {
                    "exceptionType" : "GEO",
                    "values" : [ "values", "values" ]
                },
                {
                    "exceptionType" : "GEO",
                    "values" : [ "values", "values" ]
                }
            ],
            "policySettingsId" : 55,
            "comment" : "exclude all ips for pen tests",
            "id" : 10
        }
    ],
    "id" : 10,
    "settingsAction" : "BLOCK"
},
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [
    {
        "accountId" : 10,
        "policyId" : 8,
        "id" : 10,
        "assetType" : "WEBSITE"
    },
    {
        "accountId" : 10,
        "policyId" : 8,
        "id" : 10,
        "assetType" : "WEBSITE"
    }
],
"description" : "This is policy blocks all requests from Europe",
"subaccountIds" : [ { }, { } ],
"enabled" : true
},
{
    "accountId" : 10,
    "assetsIds" : [ 0, 0 ],
    "policySettings" : [
        {
            "data" : [
                {
                    "geo" : [
                        "countries" : [ "AE", "AC" ],
                        "continents" : [ "APAC", "US" ]
                    },
                    "urls" : [
                        {
                            "pattern" : "EQUALS",
                            "url" : "/test"
                        }
                    ]
                }
            ]
        }
    ]
}

```

```

        "pattern" : "EQUALS",
        "url" : "/test"
    } ],
    "ips" : [ "ips", "ips" ]
},
"policyId" : 10,
"policySettingType" : "IP/GEO/URL",
"policyDataExceptions" : [ {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
}, {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
}, {
    "data" : {
        "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
            "pattern" : "EQUALS",
            "url" : "/test"
        }, {
            "pattern" : "EQUALS",
            "url" : "/test"
        }],
        "ips" : [ "ips", "ips" ]
},
"policyId" : 10,
"policySettingType" : "IP/GEO/URL",
"policyDataExceptions" : [ {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",

```

```

        "id" : 10
    }, {
        "data" : [ {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        }, {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        }],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
    ],
    "id" : 10,
    "settingsAction" : "BLOCK"
},
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [ {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
}, {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
}],
"description" : "This is policy blocks all requests from Europe",
"subaccountIds" : [ { }, { } ],
"enabled" : true
},
"meta" : {
    "size" : 1,
    "totalPages" : 5,
    "page" : 6,
    "totalElements" : 5
},
"links" : {
    "key" : "links"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[Success PaginatedCollectionPolicyDtoWithAssetsAndSubAccountsAssignment](#)

404

Not Found [APIError](#)

500

Internal Server Error [APIError](#)

```
get /v2/policies
```

Retrieve all policies in account (getAllPoliciesByAccount)

Query parameters

extended (optional)

Query Parameter

— Optional to get full policy data. Default is false. When set to false, the response returns basic policy details such as name, ID, and policy type, according to GetLeanPoliciesResponse. This is the default value. If set to true, the response returns full policy details, including current configuration and settings, according to GetPoliciesResponse.

caid (optional)

Query Parameter

— By default, the policies are retrieved for the account (A) associated with the API credentials used for authentication. To retrieve the policies for a different account (an account under the account (A)), specify the account ID. format: int64

Return type

[GetLeanPoliciesResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  }, {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 11
  } ]
}
```

```

    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [GetLeanPoliciesResponse](#)

404

Not Found [SimpleTextErrorResponse](#)

500

Internal Error [SimpleTextErrorResponse](#)

```
get /v2/policies/{policyId}
```

Retrieve policy details (getPolicyById)

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Query parameters

extended (optional)

Query Parameter

— Optional to get full policy data. Default is false. When set to false, the response returns basic policy details such as name, ID, and policy type, according to GetLeanPoliciesResponse. This is the default value. If set to true, the response returns full policy details, including current configuration and settings, according to GetPoliciesResponse.

caid (optional)

Query Parameter

— By default, the policy is retrieved for the account (A) associated with the API credentials used for authentication. To retrieve the policy for a different account (an account under the account (A)), specify the

account ID. format: int64

Return type

[GetLeanPoliciesResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  }, {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [GetLeanPoliciesResponse](#)

404

Not Found [SimpleTextErrorResponse](#)

500

Internal Error SimpleTextErrorResponse

```
post /v2/policies/{policyId}
```

Modify an existing policy (partial update) (modifyPolicy)

When sending the content in the "data" attribute, it will be appended and not overwritten. When updating an existing policy settings or exceptions, the relevant id (policy settings or exception id) must be provided.

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body UpdatePolicyDto (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— By default, the policy is updated for the account (A) associated with the API credentials used for authentication. To update the policy for a different account (an account under the account (A)), specify the account ID. format: int64

Return type

GetPolicyResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "accountId" : 10,
    "policySettings" : [ {
      "data" : {
```

```

"geo" : {
    "countries" : [ "AE", "AC" ],
    "continents" : [ "APAC", "US" ]
},
"urls" : [ {
    "pattern" : "EQUALS",
    "url" : "/test"
}, {
    "pattern" : "EQUALS",
    "url" : "/test"
} ],
"ips" : [ "ips", "ips" ]
},
"policyId" : 10,
"policySettingType" : "IP/GEO/URL",
"policyDataExceptions" : [ {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
}, {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
}, {
    "data" : {
        "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
            "pattern" : "EQUALS",
            "url" : "/test"
        }, {
            "pattern" : "EQUALS",
            "url" : "/test"
        } ],
        "ips" : [ "ips", "ips" ]
    },
    "policyId" : 10,
    "policySettingType" : "IP/GEO/URL",
    "policyDataExceptions" : [ {
        "data" : [ {

```

```

    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
}, {
  "data" : [ {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }, {
    "exceptionType" : "GEO",
    "values" : [ "values", "values" ]
  }],
  "policySettingsId" : 55,
  "comment" : "exclude all ips for pen tests",
  "id" : 10
} ],
  "id" : 10,
  "settingsAction" : "BLOCK"
},
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [ {
  "accountId" : 10,
  "policyId" : 8,
  "id" : 10,
  "assetType" : "WEBSITE"
}, {
  "accountId" : 10,
  "policyId" : 8,
  "id" : 10,
  "assetType" : "WEBSITE"
}],
"description" : "This is policy blocks all requests from Europe",
"enabled" : true
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success GetPolicyResponse

400

Bad Request [SimpleTextErrorResponse](#)

404

Not Found [SimpleTextErrorResponse](#)

```
put /v2/policies/{policyId}
```

Overwrite an existing policy (full update) (updatePolicy)

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [PolicyDto](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— By default, the policy is saved for the account (A) associated with the API credentials used for authentication. To save the policy for a different account (an account under the account (A)), specify the account ID. format: int64

Return type

[GetPolicyResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : {  
    "accountId" : 10,
```

```

"policySettings" : [ {
  "data" : {
    "geo" : {
      "countries" : [ "AE", "AC" ],
      "continents" : [ "APAC", "US" ]
    },
    "urls" : [ {
      "pattern" : "EQUALS",
      "url" : "/test"
    }, {
      "pattern" : "EQUALS",
      "url" : "/test"
    } ],
    "ips" : [ "ips", "ips" ]
  },
  "policyId" : 10,
  "policySettingType" : "IP/GEO/URL",
  "policyDataExceptions" : [ {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    }, {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
  }, {
    "data" : [ {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    }, {
      "exceptionType" : "GEO",
      "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
  }],
  "id" : 10,
  "settingsAction" : "BLOCK"
}, {
  "data" : {
    "geo" : {
      "countries" : [ "AE", "AC" ],
      "continents" : [ "APAC", "US" ]
    },
    "urls" : [ {
      "pattern" : "EQUALS",
      "url" : "/test"
    }, {
      "pattern" : "EQUALS",
      "url" : "/test"
    } ],
    "ips" : [ "ips", "ips" ]
  },
  "policyId" : 10,
  "policySettingType" : "IP/GEO/URL",

```

```

"policyDataExceptions" : [ {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
}, {
    "data" : [ {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    }, {
        "exceptionType" : "GEO",
        "values" : [ "values", "values" ]
    } ],
    "policySettingsId" : 55,
    "comment" : "exclude all ips for pen tests",
    "id" : 10
} ],
"id" : 10,
"settingsAction" : "BLOCK"
} ],
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [ {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
}, {
    "accountId" : 10,
    "policyId" : 8,
    "id" : 10,
    "assetType" : "WEBSITE"
} ],
"description" : "This is policy blocks all requests from Europe",
"enabled" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Success GetPolicyResponse

400

Bad Request SimpleTextErrorResponse

404

Not Found SimpleTextErrorResponse

```
patch /v2/policies/{policyId}/{assetType}/{assetId}
```

Overwrite applied assets in a policy (updatePolicyToSingleAsset)

Applies a single policy to a single asset and removes the previously applied assets from the policy.

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

assetType (required)

Path Parameter

— The type of asset on which the policy is applied

assetId (required)

Path Parameter

— Asset ID format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the policy is applied for an asset that belongs to the account (A) associated with the API credentials used for authentication. To apply the policy for an asset that belongs to a different account (an account under the account (A)), specify the account ID. format: int64

uiContext (optional)

Query Parameter

Return type

AssetResult

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "policyId" : 6,
    "assetId" : 0,
    "id" : 10,
    "assetType" : "WEBSITE"
  }
]
```

```

} , {
  "policyId" : 6,
  "assetId" : 0,
  "id" : 10,
  "assetType" : "WEBSITE"
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success AssetResult

400

Bad Request SimpleTextErrorResponse

500

Internal error SimpleTextErrorResponse

PolicyManagementAccountApplication

```
post /v2/accounts/{subAccountId}/policies/{policyId}
```

Enables an account to access a policy (addAvailableAccountToPolicy)

Adds an account to the list of accounts that can view and manage a given policy. If the policy is currently defined as available to all sub accounts, running this API overwrites the setting. The policy will be available to the parent account and the specified sub account only.

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

subAccountId (required)

Path Parameter

— Sub Account Id to add to the policy format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PolicyAccountsResult

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ 123456 ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyAccountsResult

400

Bad Request SimpleTextErrorResponse

```
get /v3/accounts/associated-policies
```

Retrieve the list of default and available policies of the account (getAccountPolicyAssociation)
Retrieves the account's default polices, and all the policies that are available to the account.

Query parameters

caid (optional)

Query Parameter

— By default, the policies association is retrieved for the account (A) associated with the API credentials used for authentication. To retrieve the policies associated with a different account (an account under the account (A)),

specify the account ID. format: int64

Return type

[AccountPolicyAssociationV3RequestResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 10,
    "defaultWafPolicyId" : 5,
    "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
    "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
  }, {
    "accountId" : 10,
    "defaultWafPolicyId" : 5,
    "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
    "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Success [AccountPolicyAssociationV3RequestResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
get /v2/accounts/policies/{policyId}
```

Retrieves the list of accounts that can access a policy (`getAllAvailableAccountsOfPolicy`)
 Retrieves the IDs of accounts that can view and manage a policy

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PolicyAccountsResult

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ 123456 ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyAccountsResult

400

Bad Request SimpleTextErrorResponse

```
patch /v3/accounts/associated-policies
```

Update the list of default and available policies of the account (patchAccountPolicyAssociation)
Updates the account's default polices and updates the list of policies that are available to the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AccountPolicyAssociationV3RequestResponse](#) (required)
Body Parameter

Query parameters

caid (optional)

Query Parameter

— By default, the policies association is set for the account (A) associated with the API credentials used for authentication. To retrieve the policies associated with a different account (an account under the account (A)), specify the account ID. format: int64

Return type

[AccountPolicyAssociationV3RequestResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 10,
    "defaultWafPolicyId" : 5,
    "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
    "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
  }, {
    "accountId" : 10,
    "defaultWafPolicyId" : 5,
    "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
    "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [AccountPolicyAssociationV3RequestResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
put /v3/accounts/associated-policies
```

Set the list of default and available policies of the account (full overwrite) (`putAccountPolicyAssociation`).
Sets the account's default policies, and sets the list of policies that are available to the account (full overwrite).

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AccountPolicyAssociationV3RequestResponse](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— By default, the policies association is set for the account (A) associated with the API credentials used for authentication. To retrieve the policies associated with a different account (an account under the account (A)), specify the account ID. format: int64

Return type

[AccountPolicyAssociationV3RequestResponse](#)

Example data

Content-Type: application/json

```
{
```

```

"data" : [ {
  "accountId" : 10,
  "defaultWafPolicyId" : 5,
  "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
  "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
}, {
  "accountId" : 10,
  "defaultWafPolicyId" : 5,
  "defaultNonMandatoryNonDistinctPolicyIds" : [ 3, 4 ],
  "availablePolicyIds" : [ 1, 2, 3, 4, 5 ]
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [AccountPolicyAssociationV3RequestResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
delete /v2/accounts/{subAccountId}/policies/{policyId}
```

Removes access to a policy by an account (removeAvailableAccountFromPolicy)
 Removes an account from the list of accounts that can view and manage a policy

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

subAccountId (required)

Path Parameter

— Sub Account Id to remove from the policy format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PolicyAccountsResult

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ 123456 ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyAccountsResult

400

Bad Request SimpleTextErrorResponse

```
put /v2/accounts/policies/{policyId}
```

Defines the list of accounts that can access a policy (setAvailableAccountToPolicy)

Configures the list of accounts that can view and manage a policy

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body long (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PolicyAccountsResult

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : [ 123456 ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyAccountsResult

400

Bad Request SimpleTextErrorResponse

PolicyManagementAssetApplication

```
post /v2/assets/{assetType}/{assetId}/policies/{policyId}
```

Apply a single policy to a single asset (applyAssetToPolicy)

Applies a policy to an asset. Policies already assigned to the asset are not modified. A website must have exactly one WAF Rules policy applied to it

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

assetType (required)

Path Parameter

— The type of asset on which the policy is applied

assetId (required)

Path Parameter

— Asset ID to add to policy format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the Asset should belong to the account (A) associated with the API credentials used for authentication. To assign an asset of a different account (an account under the account (A)), specify the account ID. format: int64

Return type

GetAssetsResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "policyId" : 6,
    "assetId" : 0,
    "id" : 10,
    "assetType" : "WEBSITE"
  }, {
    "policyId" : 6,
    "assetId" : 0,
    "id" : 10,
    "assetType" : "WEBSITE"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

200

Success [GetAssetsResponse](#)

400

Bad Request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /v2/assets/policies/{policyId}
```

Retrieve assets to which policy is applied (getAllAssetOfPolicy)

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the policy should belong to the account (A) associated with the API credentials used for authentication. To get the assets for a policy of a different account (an account under the account (A)), specify the account ID. format: int64

Return type

[GetAssetsResponse](#)

Example data

Content-Type: application/json

```
{
```

```

    "isError" : false,
    "value" : [ {
        "policyId" : 6,
        "assetId" : 0,
        "id" : 10,
        "assetType" : "WEBSITE"
    } , {
        "policyId" : 6,
        "assetId" : 0,
        "id" : 10,
        "assetType" : "WEBSITE"
    } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success [GetAssetsResponse](#)

400

Bad Request [SimpleTextErrorResponse](#)

404

Not Found [GetAssetsResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /v2/assets/{assetType}/{assetId}/policies
```

Retrieve all policies applied to an asset (getAllPoliciesOfAsset)

Path parameters

assetType (required)

Path Parameter

— The type of asset on which the policy is applied

assetId (required)

Path Parameter

— The Asset ID format: int64

Query parameters

extended (optional)

Query Parameter

— Optional to get full policy data. Default is false. When set to false, the response returns basic policy details such as name, ID, and policy type, according to GetLeanPoliciesResponse. This is the default value. If set to true, the response returns full policy details, including current configuration and settings, according to GetPoliciesResponse.

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetLeanPoliciesResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  }, {
    "lastModifiedBy" : 0,
    "policyType" : "ACL",
    "name" : "Block ip Policy",
    "description" : "description",
    "lastUserModified" : "lastUserModified",
    "id" : 10,
    "isMarkedAsDefault" : true,
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "numberOfAssets" : 6
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Success `GetLeanPoliciesResponse`

404

Not found `GetAssetsResponse`

500

Internal error `SimpleTextErrorResponse`

```
delete /v2/assets/{assetType}/{assetId}/policies/{policyId}
```

Remove policy from asset (unApplyPolicyOnAsset)

If you remove a WAF Rules policy from a website, the account's default policy is automatically re-applied to the website.

Path parameters

`policyId` (required)

Path Parameter

— The Policy ID format: int64

`assetType` (required)

Path Parameter

— Asset type to remove

`assetId` (required)

Path Parameter

— Asset ID to remove format: int64

Query parameters

`caid` (optional)

Query Parameter

— By default, the policy should belong to the account (A) associated with the API credentials used for authentication. To unapply a policy for a different account (an account under the account (A)), specify the account ID. format: int64

Return type

`PolicyAssetMappingResult`

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "policyId" : 6,
    "assetId" : 0,
    "id" : 10,
    "assetType" : "WEBSITE"
  }, {
    "policyId" : 6,
    "assetId" : 0,
    "id" : 10,
    "assetType" : "WEBSITE"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyAssetMappingResult

400

Bad Request SimpleTextErrorResponse

500

Internal error SimpleTextErrorResponse

```
put /v2/assets/{assetType}/{assetId}/policies/{policyId}
```

Overwrite policies assigned to a single asset (updateAssetWithSinglePolicy)

Applies a single policy to a single asset and removes previously assigned policies. If you apply a WAF Rules policy to a website, it replaces the policy that is currently applied. Since this API is removing all other policies but the one provided, it can be only applied to WAF Rules policies

Path parameters

policyId (required)

Path Parameter

— The Policy ID format: int64

assetType (required)

Path Parameter

— The type of asset on which the policy is applied

assetId (required)

Path Parameter

— Asset Id format: int64

Query parameters

caid (optional)

Query Parameter

— By default, the policy should belong to the account (A) associated with the API credentials used for authentication. To update a policy for a different account (an account under the account (A)), specify the account ID. format: int64

Return type

PolicyDtoResult

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "accountId" : 10,
    "policySettings" : [ {
      "data" : {
        "geo" : {
          "countries" : [ "AE", "AC" ],
          "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
          "pattern" : "EQUALS",
          "url" : "/test"
        }, {
          "pattern" : "EQUALS",
          "url" : "/test"
        } ],
        "ips" : [ "ips", "ips" ]
      },
      "policyId" : 10,
      "policySettingType" : "IP/GEO/URL",
      "policyDataExceptions" : [ {
        "data" : [ {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        }, {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        } ],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
      }, {
        "data" : [ {
          "exceptionType" : "GEO",
          "values" : [ "values", "values" ]
        } ]
      }
    }
  }
}
```

```

        },
        {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        },
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
    },
    "id" : 10,
    "settingsAction" : "BLOCK"
},
{
    "data" : {
        "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
        },
        "urls" : [ {
            "pattern" : "EQUALS",
            "url" : "/test"
        }, {
            "pattern" : "EQUALS",
            "url" : "/test"
        }],
        "ips" : [ "ips", "ips" ]
    },
    "policyId" : 10,
    "policySettingType" : "IP/GEO/URL",
    "policyDataExceptions" : [ {
        "data" : [ {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        },
        {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        }],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
    },
    {
        "data" : [ {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        },
        {
            "exceptionType" : "GEO",
            "values" : [ "values", "values" ]
        }],
        "policySettingsId" : 55,
        "comment" : "exclude all ips for pen tests",
        "id" : 10
    },
    "id" : 10,
    "settingsAction" : "BLOCK"
}
],
"policyType" : "ACL",
"name" : "Block ip Policy",
"defaultPolicyConfig" : [
    {
        "accountId" : 10,
        "policyId" : 8,
        "id" : 10,

```

```

    "assetType" : "WEBSITE"
}, {
  "accountId" : 10,
  "policyId" : 8,
  "id" : 10,
  "assetType" : "WEBSITE"
} ],
"description" : "This is policy blocks all requests from Europe",
"enabled" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Success PolicyDtoResult

400

Bad Request SimpleTextErrorResponse

500

Internal error SimpleTextErrorResponse

Models

Methods

Table of Contents

1. APIError
 2. AccountPolicyAssociationDto
 3. AccountPolicyAssociationV3RequestResponse
 4. AssetResult
 5. DefaultPolicyConfigDto
 6. ExceptionsDataDto
 7. GeoDto
 8. GetAssetsResponse
 9. GetLeanPoliciesResponse
-

-
10. GetPolicyResponse
 11. LeanPolicyDto
 12. PaginatedCollectionPolicyDtoWithAssetsAndSubAccountsAssignment
 13. PaginationMetadata
 14. PolicyAccountsResult
 15. PolicyAssetMappingResult
 16. PolicyBaseFailureResponse
 17. PolicyDataExceptionDto
 18. PolicyDto
 19. PolicyDtoResult
 20. PolicyDtoWithAssetsAndSubAccountsAssignment
 21. PolicyResult
 22. PolicySettingsDto
 23. SettingsDataDto
 24. SimpleTextErrorResponse
 25. UpdatePolicyDto
 - 26.UrlsDto
 27. value

APIError

code (optional)
String
 detail (optional)
String
 id (optional)
String
 source (optional)
map[String, Object]
 status (optional)
Integer
 format: int32
 title (optional)
String

AccountPolicyAssociationDto

accountId (optional)
Long
 The Imperva ID of the current account. format: int64
 example: 10
 availablePolicyIds (optional)
array[Long]
 The account's available policies. These policies can be applied to the websites in the account format: int64
 example: [1,2,3,4,5]
 defaultNonMandatoryNonDistinctPolicyIds (optional)
array[Long]
 The Imperva IDs of the account's default, optional and simultaneously applied policies. An account can have multiple policies for each of these policy types. (e.g ACL, WHITELIST) format: int64
 example: [3,4]
 defaultWafPolicyId (optional)

Long

The Imperva ID of the account's default WAF Rules policy. Each Imperva account and sub account includes a default WAF Rules policy. format: int64

example: 5

AccountPolicyAssociationV3RequestResponse

data (optional)

array[AccountPolicyAssociationDto]

AssetResult

isError (optional)

Boolean

States if an error has occurred

example: false

value (optional)

array[value]

DefaultPolicyConfigDto

Sets the specified policy as default for the account, or indicates that the policy is set as default. A default policy is used by any new website added to the account.

accountId (optional)

Long

The account ID format: int64

example: 10

assetType (optional)

String

The type of asset on which the policy is applied

Enum:

WEBSITE

WEBSITE

id (optional)

Long

The ID of this default policy configuration. format: int64

example: 10

policyId (optional)

Long

The ID of this policy format: int64

example: 8

ExceptionsDataDto

The Filter/s of the exception

exceptionType (optional)

String

The element that the exception is based on.

Enum:

GEO

IP

URL

URL_NOT_EQUALS

URL_NOT_CONTAINS

URL_PREFIX

URL_SUFFIX

URL_NOT_PREFIX
 URL_NOT_SUFFIX
 URL_CONTAINS
 CLIENT_ID
 SITE_ID
 HTTP_PARAM
 USER_AGENT
 FILE_HASH
 GEO,IP,URL,URL_NOT_EQUALS,URL_NOT_CONTAINS,URL_PREFIX,URL_SUFFIX,URL_NOT_PREFIX,URL_NOT_SUFFIX
 FILE_HASH
 values (optional)
 array[String]
 Values of the exception vary based on the exceptionType parameter

GeoDto

Country/Continent Codes arrays
 continents (optional)
 array[String]
 Continent Codes array
 example: ["APAC", "US"]
 countries (optional)
 array[String]
 Country Codes array
 example: ["AE", "AC"]

GetAssetsResponse

isError (optional)
 Boolean
 States if an error has occurred
 example: false
 value (optional)
 array[value]

GetLeanPoliciesResponse

isError (optional)
 Boolean
 States if an error has occurred
 example: false
 value (optional)
 array[LeanPolicyDto]

GetPolicyResponse

isError (optional)
 Boolean
 States if an error has occurred
 example: false
 value (optional)
 PolicyDto

LeanPolicyDto

description (optional)
String
 id (optional)
Long
 The Policy ID format: int64
 example: 10
 isMarkedAsDefault (optional)
Boolean
 lastModified (optional)
Date
 format: date-time
 lastModifiedBy (optional)
Long
 format: int64
 lastUserModified (optional)
String
 name (optional)
String
 The Policy name
 example: Block ip Policy
 numberOfAssets (optional)
Integer
 The number of assets to which the policy is applied format: int32
 policyType (optional)
String
 The Policy type
 Enum:
 ACL
 WHITELIST
 WAF_RULES
 FILE_UPLOAD
 example: ACL

PaginatedCollectionPolicyDtoWithAssetsAndSubAccountsAssignment

data
 array[PolicyDtoWithAssetsAndSubAccountsAssignment]
 API paginated response data
 links (optional)
 map[String, String]
 API pagination links
 meta (optional)
 PaginationMetadata

PaginationMetadata

API pagination metadata
 page (optional)
Integer
 format: int32
 size (optional)
Integer
 format: int32
 totalElements (optional)
Long

format: int64
totalPages (optional)
Integer
format: int32

PolicyAccountsResult

isError (optional)
Boolean
States if an error has occurred
example: false
value (optional)
array[Long]
Account Ids format: int64
example: [123456]

PolicyAssetMappingResult

isError (optional)
Boolean
States if an error has occurred
example: false
value (optional)
array[value]
Policy Asset Mapping

PolicyBaseFailureResponse

isError (optional)
Boolean
States if an error has occurred
example: true
value (optional)
Object

PolicyDataExceptionDto

The exception configuration on a given settings
comment (optional)
String
Comment describing the exception and its reason
example: exclude all ips for pen tests
data (optional)
array[ExceptionsDataDto]
The Filter/s of the exception
id (optional)
Long
The PolicyDataExceptions ID format: int64
example: 10
policySettingsId (optional)
Long
The PolicySettings ID format: int64
example: 55

PolicyDto

Policy meta data

accountId (optional)

Long

The Account Id Of the Policy format: int64

example: 10

defaultPolicyConfig (optional)

array[DefaultPolicyConfigDto]

Sets the specified policy as default for the account, or indicates that the policy is set as default. A default policy is used by any new website added to the account.

description (optional)

String

The Policy description

example: This is policy blocks all requests from Europe

enabled

Boolean

Enable or disable the policy. A WAF Rules policy is always created in the enabled state, and cannot be disabled.

name

String

The Policy name

example: Block ip Policy

policySettings (optional)

array[PolicySettingsDto]

policyType

String

The Policy type

Enum:

ACL

WHITELIST

WAF_RULES

FILE_UPLOAD

PolicyDtoResult

isError (optional)

Boolean

States if an error has occurred

example: false

value (optional)

PolicyDto

PolicyDtoWithAssetsAndSubAccountsAssignment

API paginated response data

accountId (optional)

Long

The Account Id Of the Policy format: int64

example: 10

assetsIds (optional)

array[Long]

Set of asset IDs that this policy assigned to. format: int64

defaultPolicyConfig (optional)

array[DefaultPolicyConfigDto]

Sets the specified policy as default for the account, or indicates that the policy is set as default. A default policy is used by any new website added to the account.

description (optional)

String

The Policy description

example: This is policy blocks all requests from Europe

enabled

Boolean

Enable or disable the policy. A WAF Rules policy is always created in the enabled state, and cannot be disabled.

name

String

The Policy name

example: Block ip Policy

policySettings (optional)

array[PolicySettingsDto]

policyType

String

The Policy type

Enum:

ACL

WHITELIST

WAF_RULES

FILE_UPLOAD

subaccountIds (optional)

array[Object]

set of subaccount IDs that allowed to use this policy.

PolicyResult

isError (optional)

Boolean

States if an error has occurred

example: false

value (optional)

Object**PolicySettingsDto**

data (optional)

SettingsDataDto

id (optional)

Long

The Policy Settings ID format: int64

example: 10

policyDataExceptions (optional)

array[PolicyDataExceptionDto]

The exception configuration on a given settings

policyId (optional)

Long

The Policy ID of this setting format: int64

example: 10

policySettingType (optional)

String

The PolicySettings type

Enum:

GEO

URL

IP

HEADER_VALUE

CROSS_SITE_SCRIPTING

ILLEGAL_RESOURCE_ACCESS

REMOTE_FILE_INCLUSION

SQL_INJECTION

RESP_DATA_LEAK

MALICIOUS_FILE_UPLOAD

IP,GEO,URL,CROSS_SITE_SCRIPTING,ILLEGAL_RESOURCE_ACCESS,REMOTE_FILE_INCLUSION,SQL_INJECTION,R

example: IP/GEO/URL

settingsAction (optional)

String

The action taken by Imperva when a policy rule is triggered

Enum:

BLOCK

ALLOW

ALERT

BLOCK_USER

BLOCK_IP

IGNORE

HIDDEN_ALERT

MASK

example: BLOCK

SettingsDataDto

depends on the policy settings type

geo (optional)

GeoDto

ips (optional)

array[String]

urls (optional)

array[UrlsDto]

SimpleTextErrorResponse

isError (optional)

Boolean

States if an error has occurred

example: true

value (optional)

String

UpdatePolicyDto

Policy to save. The supported format JSON

accountId (optional)

Long

The Account Id Of the Policy format: int64

example: 10

defaultPolicyConfig (optional)

array[DefaultPolicyConfigDto]

Sets the specified policy as default for the account, or indicates that the policy is set as default. A default policy is used by any new website added to the account.

description (optional)

String

The Policy description

example: This is policy blocks all requests from Europe

enabled (optional)

Boolean

Enable or disable the policy. A WAF Rules policy is always created in the enabled state, and cannot be disabled.
name (optional)

String

The Policy name

example: Block ip Policy

policySettings (optional)

array[PolicySettingsDto]

The Policy settings configuration

policyType (optional)

String

The Policy type

Enum:

ACL

WHITELIST

WAF_RULES

FILE_UPLOAD

UrlsDto

pattern (optional)

String

URL pattern for rule

Enum:

EQUALS

NOT_EQUALS

NOT_CONTAINS

PREFIX

SUFFIX

NOT_PREFIX

NOT_SUFFIX

CONTAINS

EQUALS,NOT_EQUALS,NOT_CONTAINS,PREFIX,SUFFIX,NOT_PREFIX,NOT_SUFFIX,CONTAINS

url (optional)

String

URL value

example: /test

value

Policy Asset Mapping

assetId (optional)

Long

format: int64

assetType (optional)

String

The type of asset on which the policy is applied

Enum:

WEBSITE

WEBSITE

id (optional)

Long

The PolicySettings ID format: int64

example: 10

policyId (optional)

Long

format: int64

Policies API Extended Information

This document provides specific details on how to use the **Policies APIs** to manage and configure policies in your account. For a detailed description of the Policies feature and the different policy types, see [Create and Manage Policies](#).

Overview

The **Policies API** definition file (Swagger) provides documentation on full, formatted, and interactive version of the Policies APIs that you can use to learn about the APIs, or test them using your API ID and key. To view or download the file, see [Policy Management API Definition](#).

The API documentation is divided into sections based on functional areas:

- Policy Management: Create, modify, and delete policies for use in your account and subaccounts.
- Policy Management account application: Define policy availability for your account and subaccounts.
- Policy Management asset application: Manage policies at the asset level. For example, apply a policy to a website.

There are several examples below of how to create the different types of policies. If you do not find an example that you are looking for, we suggest you create a policy in the GUI and then retrieve it using the GET API and use the response as an example.

Policy availability

A policy must be designated as available for a specific account before it can be applied to assets (such as a website) in the account. By default, a policy created in a parent account is available for all of its subaccounts. Parent account users with the appropriate permissions can subsequently change the settings and make the policy available to any or all of its subaccounts.

By default, a policy is created for the account (A) associated with the API credentials used for authentication. To create the policy for a different account (an account under the account (A)), specify the account ID using the `caid` query parameter.

Policies are always created at the parent account level.

User creating the policy	Specifies this account ID	The policy is available by default for:
Parent account user	Parent account ID or leave empty	Parent account and all subaccounts
Parent account user	Subaccount ID	Parent account and only the specified subaccount
Sub account user	Subaccount ID or leave empty	Parent account and only the specified subaccount

Access Control List (ACL) policy example

The payload below is used to configure the following Access Control List policy:

- Name: Access Control List Example

- Block requests received from subnet 10.10.10.0 with the exceptions of requests arriving from 10.10.10.1 and arriving from Benin.
- Block requests for URL /index with the exception of /index/a.htm.
- Block requests from Africa with the exception of traffic arriving from Algeria.

```
{
    "policySettings": [
        {
            "settingsAction": "BLOCK",
            "policySettingType": "IP",
            "data": {
                "ips": [
                    "10.10.10.0"
                ]
            },
            "policyDataExceptions": [
                {
                    "data": [
                        {
                            "exceptionType": "IP",
                            "values": [
                                "10.10.10.1"
                            ]
                        }
                    ]
                },
                {
                    "data": [
                        {
                            "exceptionType": "GEO",
                            "values": [
                                "BJ"
                            ]
                        }
                    ]
                }
            ]
        },
        {
            "settingsAction": "BLOCK",
            "policySettingType": "GEO",
            "data": {
                "geo": {
                    "countries": [],
                    "continents": [
                        "AF"
                    ]
                }
            },
            "policyDataExceptions": [
                {
                    "data": [
                        {
                            "exceptionType": "GEO",
                            "values": [

```

```
        "DZ"
    ]
}
]
}
]

{
  "settingsAction": "BLOCK",
  "policySettingType": "URL",
  "data": {
    "urls": [
      {
        "pattern": "EQUALS",
        "url": "/index"
      }
    ],
    "policyDataExceptions": [
      {
        "data": [
          {
            "exceptionType": "URL",
            "values": [
              "/index/a.htm"
            ]
          }
        ]
      }
    ],
    "name": "Access Control List Example",
    "description": "Access Control List Example",
    "enabled": false,
    "policyType": "ACL"
  }
}
```

Edit Policy

General Configuration Applied on

Block Countries

Africa X

+ Add Exception

View Exceptions (1)

Q Search

Exception	Comment	Date modified	Modified by
Countries (1)		Dec 04 2022	⋮

Exception on:

Countries:

Algeria

1 - 1 of 1 Rows per page 10 < 1 >

Block URLs

URL is X e.g. /index.php + Add

URL is:

/index X

+ Add Exception

View Exceptions (1)

Q Search

Exception	Comment	Date modified	Modified by
URL is (1)		Dec 04 2022	⋮

Exception on:

URL is:

/index/a.htm

1 - 1 of 1 Rows per page 10 < 1 >

The screenshot shows the 'Block IPs' configuration page. At the top, there's a search bar and a 'Remove' button. Below that is a text input field with placeholder 'e.g. 1.1.1.1' and a '+ Add' button. A dashed box contains a file icon and the text 'Upload IP list in CSV format [Upload file](#)'. The main list area has a header with columns: Exception, Comment, Date modified, and Modified by. There are two entries:

Exception	Comment	Date modified	Modified by
IPs (1)		Dec 04 2022	⋮
Countries (1)		Dec 04 2022	⋮

Below the list, there are sections for 'Exception on:' and 'Countries:' with a single entry each: '10.10.10.1' and 'Benin'. At the bottom, there's a search bar, a 'Rows per page' dropdown set to 10, and navigation buttons.

Allowlist policy example

The payload below is used to configure the following **Allowlist** policy:

- Name: Allowlist Policy Example
- Allow requests arriving from 10.10.10.10 and 20.20.20.20.

```
{
  "policySettings": [
    {
      "settingsAction": "ALLOW",
      "policySettingType": "IP",
      "data": {
        "ip": "10.10.10.10"
      }
    }
  ]
}
```

```

        "ips": [
            "20.20.20.2",
            "10.10.10.10"
        ]
    }
],
"name": "Allowlist Policy Example",
"description": "Allowlist Policy Example",
"enabled": true,
"policyType": "WHITELIST"
}

```

Edit Policy

Allowlist IPs		+ Add
e.g. 1.1.1.1		
<input type="button" value="Upload IP list in CSV format"/> Upload file		
<input type="button" value="Search"/> <input type="button" value="Remove"/>		
<input type="checkbox"/> IP		
<input type="checkbox"/> 10.10.10.10		
<input type="checkbox"/> 20.20.20.2		
1 - 2 of 2 Rows per page <input type="button" value="10"/>		

Save **Cancel**

WAF Rules policy example

The payload below is used to configure the following **WAF Rules** policy:

- Name: WAF Rules Policy Example
- Cross site scripting: The rule is set to **IGNORE** with the exception of the /index URL.
- Illegal resource access: The rule is set to **BLOCK** with the exception of IP 10.10.10.10.
- Remote file exclusion: The rule is set to **ALERT**.
- SQL injection: The rule is set to **BLOCK_IP**.

```

{
  "defaultPolicyConfig": [],
  "policySettings": [
    {
      "settingsAction": "BLOCK_IP",

```

```

    "policySettingType": "SQL_INJECTION",
    "policyDataExceptions": []
},
{
    "settingsAction": "IGNORE",
    "policySettingType": "CROSS_SITE_SCRIPTING",
    "policyDataExceptions": [
    {
        "data": [
        {
            "exceptionType": "URL",
            "values": [
                "/index"
            ]
        }
    ],
    "comment": "",
    "exceptionAssetMapping": []
}
]
},
{
    "settingsAction": "BLOCK",
    "policySettingType": "ILLEGAL_RESOURCE_ACCESS",
    "policyDataExceptions": [
    {
        "data": [
        {
            "exceptionType": "IP",
            "values": [
                "10.10.10.10"
            ]
        }
    ],
    "comment": "",
    "exceptionAssetMapping": []
}
]
},
{
    "settingsAction": "ALERT",
    "policySettingType": "REMOTE_FILE_INCLUSION",
    "policyDataExceptions": []
}
],
"name": "WAF Rules Policy Example",
"description": "",
"enabled": true,
"policyType": "WAF_RULES"

```

WAF rules
Define how Imperva responds to malicious visitors or requests.

Cross Site Scripting (XSS) ⓘ Mitigation level
 Ignore Alert Only Block Request Block User Block IP

[+ Add Exception](#)

[View Exceptions \(1\)](#)

Search

Exception	Comment	Date modified	Modified by
URL is (1)		Nov 29 2022	...

Exception on:
URL is:
[/index](#)

1 - 1 of 1 Rows per page [10](#)

Illegal Resource Access ⓘ Mitigation level
 Ignore Alert Only Block Request Block User Block IP

[+ Add Exception](#)

[View Exceptions \(1\)](#)

Remote File Inclusion ⓘ Mitigation level
 Ignore Alert Only Block Request Block User Block IP

[+ Add Exception](#)

[View Exceptions \(0\)](#)

SQL Injection ⓘ Mitigation level
 Ignore Alert Only Block Request Block User Block IP

[+ Add Exception](#)

[View Exceptions \(0\)](#)

[Save](#) [Cancel](#)

Use case examples

Here are some examples of goals you can achieve using policies:

- Create a default ACL policy at the parent account level.
- Create specific a ACL policy at the parent account level.
- Create a new default WAF_RULES policy at the parent account level
- Define a policy as available to a specific subaccount.
- Set the default ACL and default WAF_RULES policies as default in a subaccount.
- Apply a specific ACL policy to a website.
- Modify (partial update) or overwrite (full update) an existing policy.

Example:

The following examples are schematic (pseudocode) and do not have the full details.

	<p>Request: https://api.imperva.com/policies/v2/policies</p> <p>Body:</p> <pre>{ "policySettings": [{ "settingsAction": "BLOCK", "policySettingType": "SQL_INJECTION" }, { "settingsAction": "ALERT", "policySettingType": "CROSS_SITES" }, { "settingsAction": "BLOCK", "policySettingType": "ILLEGAL_CHARACTERS" }, { "settingsAction": "BLOCK", "policySettingType": "REMOTE_COMMAND" }], "name": "Test WAF RULES", "description": "Test WAF RULES", "enabled": true, "policyType": "WAF_RULES" }</pre> <p>The policy ID is returned: <policy ID></p>
<p>Create a policy in the parent account.</p> <p>The policy is created.</p>	<p>Request: <a href="https://api.imperva.com/policies/v2/accounts/policies/<policy ID>">https://api.imperva.com/policies/v2/accounts/policies/<policy ID></p> <p>Response:</p> <pre>{ "value": "Policy is available for all accounts", "isError": false }</pre>
<p>Get policy account availability.</p> <p>This example shows that the policy is available to the parent and subaccounts.</p>	<p>Request: <a href="https://api.imperva.com/policies/v2/accounts/policies/<policy ID>">https://api.imperva.com/policies/v2/accounts/policies/<policy ID></p> <p>Response:</p>

	<pre>{ "value": [<account ID>], "isError": false }</pre>
Get policy asset application.	<p>Request: <a href="https://api.imperva.com/policies/v2/assets/policies/<policy ID>">https://api.imperva.com/policies/v2/assets/policies/<policy ID></p> <p>Response:</p> <pre>{ "value": "could not find assets for policy wi "isError": true }</pre>
Apply the policy to an asset in an account that does not have access to the policy.	<p>Request: <a href="https://api.imperva.com/policies/v2/assets/WEBSITE/<site id>/policies/<policy ID>">https://api.imperva.com/policies/v2/assets/WEBSITE/<site id>/policies/<policy ID></p> <p>Response:</p> <pre>{ "value": "The selected assets must be part of t "isError": true }</pre>
Apply the policy to an asset in an account that is allowed to access to the policy.	<p>Request: <a href="https://api.imperva.com/policies/v2/assets/WEBSITE/<site ID>/policies/<policy ID>">https://api.imperva.com/policies/v2/assets/WEBSITE/<site ID>/policies/<policy ID></p> <p>Response:</p> <pre>{ "value": [{ "id": <association ID>, "policyId": <policy ID>, "assetId": <site ID>, "assetType": "WEBSITE" }], "isError": false }</pre>

Modify or overwrite an existing policy:

To update an existing policy, you need to first retrieve the ID of the existing settings object and then send it in the request.

To locate the relevant ID, run a GET call on the /v2/policies/{policyId} endpoint to retrieve the policy details. Make sure to send the `extended` parameter and set it to `true` to get full policy data.

You can then run the modify or overwrite operations and supply the ID of the relevant setting.

This example shows a sample request body for updating an existing WAF Rules policy that includes the policy settings IDs.

```
{
  "name": "My Existing Policy",
  "description": "Demonstrates how to modify or overwrite an existing policy",
  "enabled": true,
  "policyType": "WAF_RULES",
  "policySettings": [
    {
      "id": 4540719,
      "settingsAction": "BLOCK",
      "policySettingType": "ILLEGAL_RESOURCE_ACCESS",
      "policyDataExceptions": []
    },
    {
      "id": 4540720,
      "settingsAction": "BLOCK",
      "policySettingType": "REMOTE_FILE_INCLUSION",
      "policyDataExceptions": []
    },
    {
      "id": 4540721,
      "settingsAction": "BLOCK",
      "policySettingType": "SQL_INJECTION",
      "policyDataExceptions": []
    },
    {
      "id": 4540722,
      "settingsAction": "ALERT",
      "policySettingType": "CROSS_SITE_SCRIPTING",
      "policyDataExceptions": []
    }
  ],
  "defaultPolicyConfig": []
}
```

See also:

- [Create and Manage Policies](#)
- [Policy Management API Definition](#)

Looking for the API on other features? You'll find it here in the [Imperva API Documentation](#).

Imperva API2 WAF

To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your Cloud Application Security account and websites. These APIs provide either an alternative to existing APIs, or provide APIs with new functionality. For more details about Imperva APIs, see [Imperva API Documentation](#).

Version: 2.0.0

BasePath:/api/prov/v2

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

[Models](#)

Table of Contents

Rules

- `post /sites/{siteId}/rules`
- `delete /sites/{siteId}/rules/{ruleId}`
- `get /sites/{siteId}/rules/{ruleId}`
- `post /sites/{siteId}/rules/{ruleId}`
- `put /sites/{siteId}/rules/{ruleId}`

Rules

```
post /sites/{siteId}/rules
```

Create rule (`sitesSiteldRulesPost`)

Create a custom rule. For full feature documentation, see [Rules](#).

Path parameters

`siteld` (required)

Path Parameter

— Site id

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `Rule` (required)

Body Parameter

— The rule to create

Return type

[Rule](#)

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
  "action" : "RULE_ACTION_BLOCK_IP",
  "filter" : "ASN == 1",
  "blockDurationDetails" : {
    "blockDurationPeriodType" : "fixed",
    "blockFixedDurationValue" : 10
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The rule is returned. [Rule](#)

401

Unauthorized siteId [ApiResult](#)

404

Resource not found [ApiResult](#)

406

Invalid Input [ApiResult](#)

500

Internal server error [ApiResult](#)

```
delete /sites/{siteId}/rules/{ruleId}
```

Delete rule - must contain valid rule id (sitesSitIdRulesRuleIdDelete)
Delete rule

Path parameters

sitId (required)

Path Parameter

— Numeric identifier of the site to operate on

ruleId (required)

Path Parameter

— Numeric identifier of the rule to operate on

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

OK [ApiResult](#)

401

Unauthorized sitId [ApiResult](#)

404

Resource not found [ApiResult](#)

405

Rule can not be deleted [ApiResult](#)

406

Invalid Input [ApiResult](#)

```
get /sites/{siteId}/rules/{ruleId}
```

Read rule - must contain valid rule id (`sitesSiteldRulesRuleIdGet`)

Read rule

Path parameters

`siteld` (required)

Path Parameter

— Numeric identifier of the site to operate on

`ruleId` (required)

Path Parameter

— Numeric identifier of the rule to operate on

Return type

[Rule](#)

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
  "action" : "RULE_ACTION_BLOCK_IP",
  "filter" : "ASN == 1",
  "blockDurationDetails" : {
    "blockDurationPeriodType" : "fixed",
    "blockFixedDurationValue" : 10
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

OK. The rule is returned. [Rule](#)

401

Unauthorized sitelId [ApiResult](#)

404

Resource not found [ApiResult](#)

406

Invalid Input [ApiResult](#)

```
post /sites/{siteId}/rules/{ruleId}
```

Update rule - must contain valid rule id (sitesSitelIdRulesRuleIdPost)

Update rule

Path parameters

sitelId (required)

Path Parameter

— Numeric identifier of the site to operate on

ruleId (required)

Path Parameter

— Numeric identifier of the rule to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [Rule](#) (required)

Body Parameter

— The rule to update

Return type

[Rule](#)

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
  "action" : "RULE_ACTION_BLOCK_IP",
  "filter" : "ASN == 1",
  "blockDurationDetails" : {
    "blockDurationPeriodType" : "fixed",
    "blockFixedDurationValue" : 10
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The rule is returned. Rule

401

Unauthorized sitelid ApiResult

404

Resource not found ApiResult

406

Invalid input ApiResult

500

Internal server error ApiResult

```
put /sites/{siteId}/rules/{ruleId}
```

Overwrite rule - must contain valid rule id (sitesSitelidRulesRuleidPut)
Overwrite rule

Path parameters

siteld (required)
 Path Parameter
 — Numeric identifier of the site to operate on
 ruleId (required)
 Path Parameter
 — Numeric identifier of the rule to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body Rule (required)
 Body Parameter
 — The rule to overwrite

Return type

Rule

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
  "action" : "RULE_ACTION_BLOCK_IP",
  "filter" : "ASN == 1",
  "blockDurationDetails" : {
    "blockDurationPeriodType" : "fixed",
    "blockFixedDurationValue" : 10
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The rule is returned. Rule

401

Unauthorized siteId [ApiResult](#)

404

Resource not found [ApiResult](#)

406

Invalid Input [ApiResult](#)

500

Internal server error [ApiResult](#)

Models

Methods

Table of Contents

1. [ApiResult](#)
2. [Rule](#)
3. [Rule_blockDurationDetails](#)

ApiResult

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

Rule

rule_id (optional)

Integer

Numeric identifier of the rule to operate on

name

String

Rule name

action

String

<p>Rule action.</p> RULE_ACTION_REDIRECT - Redirect rule. Redirect the client to a different URL, responding with a 30X response. RULE_ACTION_SIMPLIFIED_REDIRECT - Redirect the client to a

different URL using restricted redirect settings. RULE_ACTION_REWRITE_URL - Redirect rule. Modify the path to which a specific request is targeted. RULE_ACTION_REWRITE_HEADER - Redirect rule. Modify or add a request header before passing traffic to the origin server. RULE_ACTION_REWRITE_COOKIE - Redirect rule. Allows the modification and addition of cookies that are sent by the client to the origin server. The cookie name and value should be indicated. RULE_ACTION_DELETE_HEADER - Redirect rule. Remove a specific request header, which means that it won't be sent to the origin server. RULE_ACTION_DELETE_COOKIE - Redirect rule. Allows the removal of a specific cookie set on the client, which means that it won't be sent to the origin server. RULE_ACTION_RESPONSE_REWRITE_HEADER - Redirect rule. Modify or add a response header before passing traffic by the origin server to the client. RULE_ACTION_RESPONSE_DELETE_HEADER - Redirect rule. Remove a specific response header, which means that it won't be sent to the client. RULE_ACTION_RESPONSE_RESPONSE_CODE - Redirect rule. Modify the response status code before passing traffic by the origin server to the client. RULE_ACTION_FORWARD_TO_DC - Redirect rule. Used to define the data center to which a specific request will be sent. RULE_ACTION_FORWARD_TO_PORT - Redirect rule. Used to define the port to which a specific request will be sent. RULE_ACTION_ALERT - Security rule. Generate a non blocking alert for this event. RULE_ACTION_BLOCK - Security rule. Block the current request and generate an alert for this event. RULE_ACTION_BLOCK_USER - Security rule. Block the current session and generate an alert for this event. Any subsequent request from the same Session will be blocked. RULE_ACTION_BLOCK_IP - Security rule. Block the current IP and generate an alert for this event. Any subsequent request from the same IP will be blocked for a period of 10 minutes. RULE_ACTION_RETRY - Security rule. Require any client matching the rule filters to support cookies in order to complete the request. RULE_ACTION_INTRUSIVE_HTML - Security rule. Require any client matching the rule filters to support javascript in order to complete the request. Since the Javascript test is embedded in an HTML page, this action should only be enabled for HTML resources. RULE_ACTION_CAPTCHA - Security rule. Require any client matching the rule filters to pass a CAPTCHA test in order to complete the request. Since the CAPTCHA test is embedded in an HTML page, this action should only be enabled for HTML resources. RULE_ACTION_RATE - Count the number of requests received that match the rule filter. RULE_ACTION_CUSTOM_ERROR_RESPONSE - Replace default error response & error code with custom ones. Once blocked a rule that matches the provided filter & error type will return a custom error & error code. RULE_ACTION_WAF_OVERRIDE - Overrides the global WAF setting for a specific threat type.

Enum:

- RULE_ACTION_REDIRECT
- RULE_ACTION_SIMPLIFIED_REDIRECT
- RULE_ACTION_REWRITE_URL
- RULE_ACTION_REWRITE_HEADER
- RULE_ACTION_REWRITE_COOKIE
- RULE_ACTION_DELETE_HEADER
- RULE_ACTION_DELETE_COOKIE
- RULE_ACTION_RESPONSE_REWRITE_HEADER
- RULE_ACTION_RESPONSE_DELETE_HEADER
- RULE_ACTION_RESPONSE_RESPONSE_CODE
- RULE_ACTION_FORWARD_TO_DC
- RULE_ACTION_FORWARD_TO_PORT
- RULE_ACTION_ALERT
- RULE_ACTION_BLOCK
- RULE_ACTION_BLOCK_USER
- RULE_ACTION_BLOCK_IP
- RULE_ACTION_RETRY
- RULE_ACTION_INTRUSIVE_HTML
- RULE_ACTION_CAPTCHA
- RULE_ACTION_RATE
- RULE_ACTION_CUSTOM_ERROR_RESPONSE
- RULE_ACTION_WAF_OVERRIDE

filter (optional)

String

The filter defines the conditions that trigger the rule action. For action RULE_ACTION_SIMPLIFIED_REDIRECT filter is not relevant. For other actions, if left empty, the rule is always run.

response_code (optional)

Integer

For RULE_ACTION_REDIRECT or RULE_ACTION_SIMPLIFIED_REDIRECT rule's response code, valid values are 302, 301, 303, 307, 308. For RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE rule's response code, valid values are all 3-digits numbers. For RULE_ACTION_CUSTOM_ERROR_RESPONSE, valid values are [200, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 419, 420, 422, 423, 424, 429, 500, 501, 502, 503, 504, 505, 507]

add_missing (optional)

Boolean

Add cookie or header if it doesn't exist (Rewrite cookie rule only)

rewrite_existing (optional)

Boolean

Rewrite cookie or header if it exists

from (optional)

String

Pattern to rewrite. For RULE_ACTION_REWRITE_URL - Url to rewrite. For RULE_ACTION_REWRITE_HEADER/RULE_ACTION_RESPONSE_REWRITE_HEADER - Header value to rewrite. For RULE_ACTION_REWRITE_COOKIE - Cookie value to rewrite to (optional)

String

Pattern to change to. RULE_ACTION_REWRITE_URL - Url to change to. RULE_ACTION_REWRITE_HEADER/RULE_ACTION_RESPONSE_REWRITE_HEADER - Header value to change to.

RULE_ACTION_REWRITE_COOKIE - Cookie value to change to

rewrite_name (optional)

String

Name of cookie or header to rewrite. Applies only for RULE_ACTION_REWRITE_COOKIE, RULE_ACTION_REWRITE_HEADER and RULE_ACTION_RESPONSE_REWRITE_HEADER

dc_id (optional)

Integer

Data center to forward request to. Applies only for RULE_ACTION_FORWARD_TO_DC

port_forwarding_context (optional)

String

Context for port forwarding. "Use Port Value" or "Use Header Name". Applies only for RULE_ACTION_FORWARD_TO_PORT

port_forwarding_value (optional)

String

Port number or header name for port forwarding. Applies only for RULE_ACTION_FORWARD_TO_PORT

rate_context (optional)

String

The context of the rate counter. Possible values IP or Session. Applies only to rules using RULE_ACTION_RATE.

Enum:

IP

Session

rate_interval (optional)

Integer

The interval in seconds of the rate counter. Possible values is a multiple of 10 minimum 10 maximum 300. Applies only to rules using RULE_ACTION_RATE.

error_type (optional)

String

The error that triggers the rule. error.type.all triggers the rule regardless of the error type. Applies only for RULE_ACTION_CUSTOM_ERROR_RESPONSE

Enum:

error.type.all

error.type.connection_timeout

error.type.access_denied

error.type.parse_req_error

error.type.parse_resp_error

error.type.connection_failed

error.type.deny_and_retry

error.type.ssl_failed

error.type.deny_and_captcha
 error.type.2fa_required
 error.type.no_ssl_config
 error.type.no_ipv6_config
 error.type.waiting_room
 error_response_format (optional)
String
 The format of the given error response in the error_response_data field. Applies only for RULE_ACTION_CUSTOM_ERROR_RESPONSE
 Enum:
 json
 xml
 error_response_data (optional)
String
 The response returned when the request matches the filter and is blocked. Applies only for RULE_ACTION_CUSTOM_ERROR_RESPONSE
 multiple_deletions (optional)
Boolean
 Delete multiple header occurrences. Applies only to rules using RULE_ACTION_DELETE_HEADER and RULE_ACTION_RESPONSE_DELETE_HEADER
 overrideWafRule (optional)
String
 The setting to override. Possible values: SQL Injection, Remote File Inclusion, Cross Site Scripting, Illegal Resource Access
 overrideWafAction (optional)
String
 The action for the override rule. Possible values: Alert Only, Block Request, Block User, Block IP, Ignore enabled (optional)
Boolean
 The setting enables or disables the rule.
 blockDurationDetails (optional)
Rule_blockDurationDetails
 sendNotifications (optional)
Boolean
 Send an email notification whenever this rule is triggered. Available for Security rules only.

Rule_blockDurationDetails

Context for block duration. Valid only for rules with action RULE_ACTION_BLOCK_IP or RULE_ACTION_BLOCK_USER
 blockDurationPeriodType (optional)
String
 Block duration types: Fixed, Randomized. Time range: 1-1440 minutes. The Fixed type blocks the IP address or session for the duration specified by the blockFixedDurationValue parameter. The Randomized type generates a random duration for each block between the specified minimum and maximum values.
 Enum:
 fixed
 randomized
 blockFixedDurationValue (optional)
Integer
 Value of the fixed block duration. Valid only for 'fixed' blockDurationPeriodType
 blockRandomizedDurationMinValue (optional)
Integer
 The lower limit for the randomized block duration. Valid only for 'randomized' blockDurationPeriodType
 blockRandomizedDurationMaxValue (optional)
Integer
 The upper limit for the randomized block duration. Valid only for 'randomized' blockDurationPeriodType

Site Onboarding with an Imperva Account Certificate

This document provides additional information for working with the Cloud Application Security Version 1 Site Management APIs, as described in the API Definition file.

To view or download the file, see [Site Management API Definition](#).

For more details on SSL support, see [Web protection - SSL/TLS](#).

Add, remove, and update sites

The process of adding a site to Imperva depends on whether the site requires SSL support. If the site requires SSL support, Imperva needs to generate a proxy SSL certificate on your behalf, which requires your approval and action.

After a site is added, its status is one of the following:

Name	Description
pending-select-approver	A site with SSL support was added. Domain approval email needs to be selected or a new domain validation method should be selected.
pending-certificate	The site owner needs to approve the SSL certificate generation by completing a domain validation action (following a link in the approval email, DNS change, adding an HTML meta tag, adding a new file, etc.)
pending-dns-changes	The site is ready for the user to perform the required DNS changes in order to be fully configured on the service.
fully-configured	Site is active on the Imperva network.

To add a non-SSL site

1. Call the **Add site** (/api/prov/v1/sites/add) operation. A successful response will contain the required DNS changes. The site is in **pending-dns-changes** state.
2. Perform the DNS changes. The system will detect the DNS changes in a few minutes and will set the site to the **fully-configured** state.
3. Call the **Get site status** (/api/prov/v1/sites/status) operation periodically until the site is in the **fully-configured** state.

To add an SSL site:

Prerequisite: Imperva must verify that HTTPS is supported by your site, in order to support SSL for your site.

1. Call the **Add site** (/api/prov/v1/sites/add) operation. The site is in **pending-select-approver** state.
2. To continue with E-mail based domain validation:
 - a. Call the **Modify site configuration** (/api/prov/v1/sites/configure) operation and set the SSL domain validation method to email.

-
- b. Call the **Get domain approver email addresses** (/api/prov/v1/domain/emails) operation and select an email address from the list.
 - c. Call the **Modify site configuration** (/api/prov/v1/sites/configure) operation again and set the selected email address. The system will send the certificate generation approval email and set the site to the **pending-certificate** state.
3. To continue with HTML meta tag domain validation:
- a. Call the **Modify site configuration** (/api/prov/v1/sites/configure) operation and set the SSL domain validation method to html. The operation will return the required HTML snippet to place in the homepage of the site and set the site to the **pending-certificate** state.
 - b. The site owner needs to place the HTML snippet in the homepage of the site.
 - c. Call the **Get site status** (/api/prov/v1/sites/status) operation and use the tests parameter to verify that domain validation was performed successfully.
4. To continue with DNS domain validation:
- a. Call the **Modify site configuration** (/api/prov/v1/sites/configure) operation and set the SSL domain validation method to dns. The operation will return the required DNS records to set on the site's domain and set the site to the **pending-certificate** state.
 - b. The site owner needs to set the DNS records on the site's domain.
 - c. Call the **Get site status** (/api/prov/v1/sites/status) operation and use the tests parameter to verify that domain validation was performed successfully.
5. Call the **Get site status** (/api/prov/v1/sites/status) operation periodically until the site is in the **pending-dns** state. The required DNS changes will be provided in the response.
6. Perform the DNS changes. The system will detect the DNS changes in a few minutes and will set the site to the **fully-configured** state.
7. Call the **Get site status** (/api/prov/v1/sites/status) operation periodically until the site is in the **fully-configured** state.

To add SSL to an existing site

1. Verify that Imperva has detected that HTTPS is supported by your site:
 - a. Call the **Get site status** (/api/prov/v1/sites/status) operation and look for the **detected** field under **origin_server**.
 - b. If the **detected** value is **false**, add the **services** test parameters and call the **Get site status** operation again.
 - c. Keep calling the **Get site status** (/api/prov/v1/sites/status) operation until the **detected** value changes to **true**.
2. Call the **Modify site configuration** (/api/prov/v1/sites/configure) operation and set the SSL domain validation method. Then, continue according to the flow above.

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

SiteManagement

- `post /api/prov/v1/sites/performance/caching-rules/add`
- `post /api/prov/v1/sites/incapRules/add`
- `post /api/prov/v1/sites/dataCenters/servers/add`
- `post /api/prov/v1/sites/dataCenters/add`
- `post /api/prov/v1/sites/add`
- `post /api/prov/v1/caa/check-compliance`
- `post /api/prov/v1/sites/customCertificate/csr`
- `post /api/prov/v1/sites/performance/caching-rules/delete`
- `post /api/prov/v1/sites/incapRules/delete`
- `post /api/prov/v1/sites/dataCenters/servers/delete`
- `post /api/prov/v1/sites/dataCenters/delete`
- `post /api/prov/v1/sites/delete`
- `post /api/prov/v1/domain/emails`
- `post /api/prov/v3/sites/{extSiteId}/settings/botConfiguration`
- `post /api/prov/v1/sites/performance/caching-rules/edit`
- `post /api/prov/v1/sites/incapRules/edit`
- `post /api/prov/v1/sites/dataCenters/servers/edit`
- `post /api/prov/v1/sites/dataCenters/edit`
- `post /api/prov/v1/sites/performance/cache-shield/enable`
- `post /api/prov/v1/sites/performance/caching-rules/enable`
- `post /api/prov/v1/sites/incapRules/enableDisable`
- `post /api/prov/v1/sites/performance/advanced/get`
- `get /api/prov/v3/sites/{extSiteId}/settings/botConfiguration`
- `post /api/prov/v1/sites/performance/cache404`

-
- post /api/prov/v1/sites/performance/cache-mode/get
 - post /api/prov/v1/sites/data-privacy/show
 - post /api/prov/v1/sites/htmlinjections
 - post /api/prov/v1/sites/data-privacy/show-override-by-geo
 - post /api/prov/v1/sites/datacenter/origin-pop/recommend
 - post /api/prov/v1/sites/performance/response-headers/get
 - post /api/prov/v1/sites/performance/rewrite-port
 - post /api/prov/v1/sites/performance/secure-resources/get
 - post /api/prov/v1/sites/performance/error-page
 - post /api/prov/v1/sites/report
 - post /api/prov/v1/sites/performance/stale-content/get
 - get /api/prov/v3/sites/{extSiteId}/settings/TLSConfiguration
 - post /api/prov/v1/sites/performance/tag-response/get
 - post /api/prov/v1/sites/xray/get-link
 - post /api/prov/v1/sites/performance/cache-shield
 - post /api/prov/v1/sites/performance/caching-rules/list
 - post /api/prov/v1/sites/incapRules/list
 - get /api/prov/v3/rules
 - post /api/prov/v1/sites/dataCenters/list
 - get /api/prov/v3/sites/{extSiteId}/data-centers-configuration
 - get /api/prov/v3/sites/{extSiteId}/delivery-rules-configuration
 - post /api/prov/v1/sites/list
 - post /api/prov/v1/sites/performance/advanced
 - post /api/prov/v1/sites/performance/cache404/modify
 - post /api/prov/v1/sites/performance/purge
 - post /api/prov/v1/sites/performance/response-headers
 - post /api/prov/v1/sites/performance/rewrite-port/modify
 - post /api/prov/v1/sites/configure/allowlists
 - post /api/prov/v1/sites/configure
 - post /api/prov/v1/sites/performance/error-page/modify
 - post /api/prov/v1/sites/setlog
 - post /api/prov/v1/sites/configure/security
 - post /api/prov/v1/sites/tls
 - post /api/prov/v1/sites/performance/stale-content
 - post /api/prov/v1/sites/performance/tag-response
 - post /api/prov/v1/sites/moveSite
 - post /api/prov/v1/sites/hostname/purge
 - post /api/prov/v1/sites/cache/purge
 - put /api/prov/v3/sites/{extSiteId}/data-centers-configuration
 - put /api/prov/v3/sites/{extSiteId}/delivery-rules-configuration
 - post /api/prov/v1/sites/customCertificate/remove
 - post /api/prov/v1/sites/dataCenters/resume
 - post /api/prov/v1/sites/performance/cache-mode
-

- post /api/prov/v1/sites/datacenter/origin-pop/modify
- post /api/prov/v1/sites/data-privacy/region-change
- post /api/prov/v1/sites/configure/htmlInjections
- post /api/prov/v1/sites/data-privacy/override-by-geo
- post /api/prov/v1/sites/incapRules/priority/set
- post /api/prov/v1/sites/performance/secure-resources
- post /api/prov/v1/sites/status
- post /api/prov/v3/sites/{extSiteId}/settings/TLSConfiguration
- post /api/prov/v1/sites/customCertificate/upload

SiteManagement

```
post /api/prov/v1/sites/performance/caching-rules/add
```

Add a cache rule (addCacheRule)

Use this operation for adding a cache rule

Query parameters

action (required)

Query Parameter

— Rule action. See Possible action parameter values.
Possible action parameter values:

- HTTP_CACHE_MAKE_STATIC Cache Resource
- HTTP_CACHE_CLIENT_CACHE_CTL Cache Resource on Client
- HTTP_CACHE_FORCE_UNCACHEABLE Don't Cache Resource
- HTTP_CACHE_DIFFERENTIATE_SSL Differentiate Cache Key by HTTP/HTTPS Scheme
- HTTP_CACHE_DIFFERENTIATE_BY_HEADER Differentiate Cache Key by Header
- HTTP_CACHE_DIFFERENTIATE_BY_COOKIE Differentiate Cache Key by Cookie
- HTTP_CACHE_DIFFERENTIATE_BY_GEO Differentiate Cache Key by Geolocation
- HTTP_CACHE_IGNORE_PARAMS Ignore Parameters in Cache Key
- HTTP_CACHE_IGNORE_AUTH_HEADER Cache Authenticated Resources
- HTTP_CACHE_FORCE_VALIDATION Force User Authentication
- HTTP_CACHE_ADD_TAG Create Tag
- HTTP_CACHE_ENRICH_CACHE_KEY Enrich Cache Key

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

name (required)

Query Parameter

— Rule name.

filter (optional)

Query Parameter

— Rule will trigger only a request that matches this filter. For more details on filters, see [Syntax Guide](https://docs.imperva.com/csh?context=rule_syntax).

ttl (optional)

Query Parameter

— Rule TTL. Only relevant when action is **HTTP_CACHE_MAKE_STATIC** or **HTTP_CACHE_CLIENT_CACHE_CTL**

ttl_unit (optional)

Query Parameter

— Rule TTL time unit.
Must be one of SECONDS, MINUTES, HOURS, DAYS or WEEKS. If no time unit is provided, SECONDS is used.
Only relevant when action is **HTTP_CACHE_MAKE_STATIC** or **HTTP_CACHE_CLIENT_CACHE_CTL**

differentiated_by_value (optional)

Query Parameter

— Value to differentiate by. HTTP_CACHE_DIFFERENTIATE_BY_HEADER - header name, HTTP_CACHE_DIFFERENTIATE_BY_COOKIE - cookie name, HTTP_CACHE_DIFFERENTIATE_BY_GEO - geo location
(ISO 3166-1 alpha-2 country codes), otherwise irrelevant.

params (optional)

Query Parameter

— Comma separated list of parameters to ignore. Parameters name must be alphanumeric.

all_params (optional)

Query Parameter

— When set to true: all parameters in cache key will be ignored.
Default: false.
Relevant for HTTP_CACHE_IGNORE_PARAMS action

tag_name (optional)

Query Parameter

— The name of the tag to add.

text (optional)

Query Parameter

— Add text to the cache key as suffix. Relevant for the HTTP_CACHE_ENRICH_CACHE_KEY action

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
2 - Invalid input [inline_response_200](#)

```
post /api/prov/v1/sites/incapRules/add
```

Add rule (addCustomRule)

Use this operation to add a rule (Delivery, Security or Rate).

Query parameters

action (required)

Query Parameter

— Rule action. See the possible values in the table below.
Possible action parameter values for Delivery Rules:

- **RULE_ACTION_REDIRECT** Redirect the client to a different URL, responding with a 30X response.
- **RULE_ACTION_SIMPLIFIED_REDIRECT** Redirect the client to a different URL, responding with a 30X response.
- **RULE_ACTION_REWRITE_URL** Modify the path to which a specific request is targeted.
- **RULE_ACTION_REWRITE_HEADER** Modify or add a request header before passing traffic to the origin server.
- **RULE_ACTION_REWRITE_COOKIE** Modify or add cookies that are sent by the client to the origin server. The cookie name and value should be indicated.
- **RULE_ACTION_DELETE_HEADER** Remove a specific request header, which means that it won't be sent to the origin server.
- **RULE_ACTION_DELETE_COOKIE** Remove a specific cookie set on the client, which means that it won't be sent to the origin server.
- **RULE_ACTION_FORWARD_TO_DC** Define the data center to which a specific request will be sent.
- **RULE_ACTION_FORWARD_TO_PORT** Define the port to which a specific request will be sent.
- **RULE_ACTION_RESPONSE_REWRITE_HEADER** Modify or add a header to the response received from the origin server.
- **RULE_ACTION_RESPONSE_DELETE_HEADER** Remove a specific response header, which means that it won't be returned to the client.
- **RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE** Modify the response code received from the origin server.

Possible action parameter values for security rules:

- **RULE_ACTION_ALERT** Generate a non blocking alert for this event.
- **RULE_ACTION_BLOCK** Block the current request and generate an alert for this event.
- **RULE_ACTION_BLOCK_USER** Block the current session and generate an alert for this event. Any subsequent request from the same Session will be blocked.
- **RULE_ACTION_BLOCK_IP** Block the current session and generate an alert for this event. Any subsequent request from the same Session will be blocked.
- **RULE_ACTION_RETRY** Require any client matching the rule filters to support cookies in order to complete the request.
- **RULE_ACTION_INTRUSIVE_HTML** Require any client matching the rule filters to support javascript in order to complete the request. Since the Javascript test is embedded in an HTML page, this action should only be enabled for HTML resources.
- **RULE_ACTION_CAPTCHA** Require any client matching the rule filters to pass a CAPTCHA test in order to complete the request. Since the CAPTCHA test is embedded in an HTML page, this action should only be enabled for HTML resources.

Possible action parameter values for counter (rate) rules:

- **RULE_ACTION_RATE** Count the number of requests received that match the rule filter.

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

name (required)

Query Parameter

— Rule name.

filter (required)

Query Parameter

— Rule will trigger only a request that matches this filter. For more details on filter guidelines, see [Syntax Guide](https://docs.imperva.com/csh?context=rule_syntax).
The filter may contain up to 400 characters.

response_code (optional)

Query Parameter

— Redirect rule's response code. Valid values are 302, 301, 303, 307, 308. format: int32

protocol (optional)

Query Parameter

—

add_missing (optional)

Query Parameter

— Add cookie or header if it doesn't exist (Rewrite cookie rule only)

from (optional)

Query Parameter

— The pattern to rewrite.
For RULE_ACTION_REWRITE_URL - The URL to rewrite.
For

RULE_ACTION_REWRITE_HEADER - The header value to rewrite.
For

RULE_ACTION_REWRITE_COOKIE - The cookie value to rewrite.
For

RULE_ACTION_SIMPLIFIED_REDIRECT - Redirect the client to a different URL, responding with a 30X response.

to (optional)

Query Parameter

— The pattern to change to.
For RULE_ACTION_REWRITE_URL - The URL to change to.
For RULE_ACTION_REWRITE_HEADER - The header value to change to.
For RULE_ACTION_REWRITE_COOKIE - The cookie value to change to.
For RULE_ACTION_SIMPLIFIED_REDIRECT - Redirect the client to a different URL, responding with a 30X response.

rewrite_name (optional)

Query Parameter

— Name of cookie or header to rewrite. Applies only for RULE_ACTION_REWRITE_COOKIE and RULE_ACTION_REWRITE_HEADER.

dc_id (optional)

Query Parameter

— Data center to forward request to. Applies only for RULE_ACTION_FORWARD_TO_DC. format: int64

allow_caching (optional)

Query Parameter

is_test_mode (optional)

Query Parameter

— Apply the rule only to the IP address the API request was sent from.
This option is not available for Simplified Redirect rules.

rate_context (optional)

Query Parameter

— The context of the rate counter. Possible values: IP / Session. Applies only to rules using RULE_ACTION_RATE.

rate_interval (optional)

Query Parameter

— The interval (in seconds) of the rate counter. Possible values: A multiple of 10 from 10-300. Applies only to rules using RULE_ACTION_RATE. format: int32

port_forwarding_context (optional)

Query Parameter

— Context for port forwarding. "Use Port Value" or "Use Header Name". Applies only for RULE_ACTION_FORWARD_TO_PORT.

port_forwarding_value (optional)

Query Parameter

— Port number or header name for port forwarding. Applies only for RULE_ACTION_FORWARD_TO_PORT. multiple_deletions (optional)

Query Parameter

— Delete multiple header occurrences. Applies only to rules using RULE_ACTION_DELETE_HEADER and RULE_ACTION_RESPONSE_DELETE_HEADER.

rewrite_existing (optional)

Query Parameter

— Rewrite cookie or header if it exists

Return type

CustomRuleResponse

Example data

Content-Type: application/json

```
{
  "rule_id" : 43573,
  "res" : 0,
  "status" : "ok"
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input, 3015 - Granularity invalid [CustomRuleResponse](#)

```
post /api/prov/v1/sites/dataCenters/servers/add
```

Add server (addDCServer)

Use this operation to add a server to a data center.

Query parameters

dc_id (required)

Query Parameter

— The data center's ID. format: int64

server_address (required)

Query Parameter

— Server IP address.

is_disabled (optional)

Query Parameter

— Enables the data center

is_standby (optional)

Query Parameter

— Set the server as Active (P0) or Standby (P1) (Boolean).

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1 -General error</br>2- invalid data center [inline_response_200_2](#)

```
post /api/prov/v1/sites/dataCenters/add
```

Add data center (addDataCenter)

Use this operation for adding data center to site.

You can configure up to 40 data centers per site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

name (required)

Query Parameter

— The new data center's name.

server_address (required)

Query Parameter

— The server's address. Possible values: IP, CNAME

lb_algorithm (optional)

Query Parameter

— Data center load balancing algorithm. Possible values are:
LB_LEAST_PENDING_REQUESTS - Server with least pending requests
LB_LEAST_OPEN_CONNECTIONS - Server with least open connections
LB_SOURCE_IP_HASH - Server by IP hash
RANDOM - Random server
WEIGHTED - Server by weight

is_enabled (optional)

Query Parameter

— Enables the data center.

is_content (optional)

Query Parameter

— The data center will be available for specific resources (Forward Delivery Rules).

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - a data center with that name already exists [inline_response_200_3](#)

```
post /api/prov/v1/sites/add
```

Add a site (addSite)

Add a new site to an account. If the site already exists, its status is returned.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **string** (optional)

Body Parameter

Query parameters

domain (required)

Query Parameter

— The domain name of the site. For example: www.example.com, www.example.com, www.example.com

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

ref_id (optional)

Query Parameter

— Customer specific identifier for this operation

send_site_setup_emails (optional)

Query Parameter

— If this value is false, end users will not get emails about the add site process such as DNS instructions and SSL setup.

site_ip (optional)

Query Parameter

— Manually set the web server IP/CNAME

force_ssl (optional)

Query Parameter

— If this value is true, manually set the site to support SSL.
This option is only available for sites with manually configured IP/CNAME and for specific accounts.

naked_domain_san (optional)

Query Parameter

-
- Use “true” to add the naked domain SAN to a www site’s SSL certificate. Default value: true
wildcard_san (optional)
Query Parameter
- Use “true” to add the wildcard SAN or “false” to add the full domain SAN to the site’s SSL certificate. Default value: true
log_level (optional)
Query Parameter
- Available only for customers that purchased the Logs Integration SKU.
Sets the log reporting level for the site. Options are “full”, “security”, “none” and default
logs_account_id (optional)
Query Parameter
- Available only for customers that purchased the Logs Integration SKU.
Numeric identifier of the account that purchased the logs integration SKU and which collects the logs.
If not specified, operation will be performed on the account identified by the authentication parameters

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3001 - Domain invalid
3002 - Site is on the CloudFlare network
3003 - Site requires SSL
3004 - Domain belongs to a known service
3005 - Site is on a service
3006 - Site requires multiple IPs support
3011 - Site unresolvable
3012 - Site unreachable
3013 - Site already protected by the service
3014 - Number of allowed sites exceeded.
3015 - Internal error [inline_response_200_16](#)

```
post /api/prov/v1/caa/check-compliance
```

Check CAA compliance (checkCAACompliance)

Check site’s associated SANs for CAA compliance. If a given SAN is compliant, its SSL domain validation status is updated accordingly. This operation returns an updated list of the site’s associated SANs that are not compliant. An empty list indicates that all SANs are compliant.

Query parameters

site_id (required)
 Query Parameter
 — Numeric identifier of the site to operate on. format: int64

Return type

CaaComplianceCheckResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "res_message",
  "non_compliant_sans" : [ "*.caa.incaptest.co", "*.caa.incaptest.co" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success CaaComplianceCheckResult

```
post /api/prov/v1/sites/customCertificate/csr
```

Create new CSR (createNewCSR)
 Use this operation to create a certificate signing request (CSR) for your site.

Query parameters

site_id (required)
 Query Parameter
 — Numeric identifier of the site to operate on format: int64

domain (optional)
 Query Parameter
 — common name. For example: example.com

email (optional)
 Query Parameter
 — Email address. For example: joe@example.com

country (optional)

Query Parameter

— The two-letter ISO code for the country where your organization is located
state (optional)

Query Parameter

— The state/region where your organization is located. This should not be abbreviated
city (optional)

Query Parameter

— The city where your organization is located
organization (optional)

Query Parameter

— The legal name of your organization. This should not be abbreviated or include suffixes such as Inc., Corp., or
LLC

organization_unit (optional)

Query Parameter

— The division of your organization handling the certificate. For example, IT Department

Return type

CreateNewCSRResponse

Example data

Content-Type: application/json

```
{
  "res" : "0",
  "csr_content" : "-----BEGIN CERTIFICATE REQUEST-----\\nMIIC5DCCAwCAQAwgZ4xNTAz
BgnVBAMTLGEucmV1c2VjdXN0b21jZXJ0aWZpY2F0\\nZXdpdGhjc3J0ZXN0MzUzOTYuY29tMQqwCgYDVQ
QHEwNKRVixCzAJBgNVBAYTAKlM\\nMQswCQYDVQQIEwJJTDEQMA4GA1UEChMHaW1wZXJ2YTELMakGA1UE
CxMCQ04xHjAc\\nBgkqhkiG9w0BCQEWD2Zvb0BpbXBlcnzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQA
D\\nggEPADCCAQoCggEBAMAHcUrB5rhio8jaAueo6rdpgW1SuscfiK01xZF5utOqrQ2\\nSfD3IBaQcT
6pf9fFT5zUcErXmCpjabay42JmjRvS04aKhI4pKydm17e5CSevSyM\\n0gAYhUdQOgjpCY81/58RKwnd
G3diFbsdrGnDuKWF7kLmx/biK+3IIzxSPF7JsQ1i\\nDHzs9X1Sq3Hwk7GBwOLB1KqG6VXS3SMUReggW6
VJhUCK1Y+FPuut7Qr80fkfVt8x\\nbCF1e7gMF8v390Tc36FFXF7/Jo5m9aSgFLFPRPsBj+UlRxvRXrnL
Nm+ycCcXvL5A\\ngE50PJaCHJz4U45c9zSAKbrvGHKzz6ewkdVCDfsCAwEAAAaAMA0GCSqGSIB3DQE
B\\nCwUAA4IBAQAvRrtUP861G3J+uYrtnvZzDGRue6eIVwfDOKqrPBAX3fm+JnctZKC5\\nQVmLT0MFKR
yL/FsF3K4a9hf8pN5TjT2/LS70vgOHOfQC0eZCcocRmz++MtUaQxsx\\n+WHiUkpgnXnH3KQhj3WzP6HJ
V/qjRzcRBsHUhuE75/J0153REWQssC5y4t3hv1\\nynkT6BUkQDy8XdRA3kgahPd9Jnwx4be9pRuq7h
w1JIA7jfqu4A/ZSoUaoCqgWIFD\\nXSt26/4tt4DITt+G/SLGNPuhuc2z+VmGkDDrRm8SNfykEvHF1Kkd
YcSKgLH2+fgf\\nlCCHPIALjavOirG+cki5Ppc0M/Wmagl+\\n-----END CERTIFICATE REQUEST
-----\\n",
  "status" : "ok"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 2 - Invalid input
 4205 - Site does not have SSL
 9414 - Feature not permitted
 9414 - Feature not permitted
 3015 - Internal error [CreateNewCSRResponse](#)

```
post /api/prov/v1/sites/performance/caching-rules/delete
```

Delete a cache rule (deleteCacheRule)

Use this operation for deleting a cache rule

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

`rule_id` (required)

Query Parameter

— ID of the rule to change. format: int64

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
2 - Invalid input
2002 - Object is not found
1 - Unexpected error [ApiResult](#)

```
post /api/prov/v1/sites/incapRules/delete
```

Delete rule (deleteCustomRule)

Use this operation to delete a rule (Delivery, Security or Rate).

Query parameters

rule_id (required)

Query Parameter

— Rule id format: int64

Return type

[DeleteCustomRuleResponse](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "status" : "ok"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 2 - Timerange invalid, 9413 - Unknown/unauthorized site_id
[DeleteCustomRuleResponse](#)

```
post /api/prov/v1/sites/dataCenters/servers/delete
```

Delete server (deleteDCServer)

Use this operation to delete a data center's server.

Query parameters

server_id (required)

Query Parameter

— Server ID. format: int64

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9415 -invalid.server.state</br>2- invalid data center
1 - Unexpected error [inline_response_200_2](#)

```
post /api/prov/v1/sites/dataCenters/delete
```

Delete data center (deleteDataCenter)

Use this operation to delete a site's data center.

Query parameters

dc_id (required)

Query Parameter

— The data center's ID. format: int64

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
5 -Could not delete data center</br>2- invalid data center</br>9415- invalid.dc.state
3011 - There must be at least one active data center not configured for forward rules in the site [inline_response_200_3](#)

```
post /api/prov/v1/sites/delete
```

Delete site (deleteSite)
Delete the site.

Query parameters

site_id (optional)

Query Parameter

— Numeric identifier of the site to operate on

ignore_grace_period (optional)

Query Parameter

— The process ignores the site's 24 hour grace period and immediately deletes the site. Default value: false

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, { }
```

```

    "key" : { }
}
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1 - Unexpected error ApiResult

```
post /api/prov/v1/domain/emails
```

Get domain approver e-mail addresses (domainEmails)

Use this operation to get the list of email addresses that can be used when adding an SSL site.

Query parameters

domain (required)

Query Parameter

— The domain name of the site. For example: www.example.com, www.example.com, www.example.com

Return type

[inline_response_200_17](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3001 - Domain invalid
3011 - Site unresolvable
[inline_response_200_17](#)

```
post /api/prov/v3/sites/{extSiteId}/settings/botConfiguration
```

Update website bot configuration (editBotsConfiguration)
 Update the Bot Access Control configuration for a given website.
 For the full list of client applications and their associated IDs, see [Client Classification](#).

Path parameters

extSiteId (required)
 Path Parameter
 — format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body BotsConfigurationDTO (required)
 Body Parameter
 — JSON body.
 Note: displayName is relevant for response only.

Return type

BotsConfigurationDTO

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "badBots" : [ null, null ],
    "canceledGoodBots" : [ {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    }, {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    } ]
  }, {
    "badBots" : [ null, null ],
    "canceledGoodBots" : [ {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    }, {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    } ]
  }
}
```

```

"canceledGoodBots" : [ {
    "displayName" : "Googlebot (Search Bot)",
    "id" : 6
}, {
    "displayName" : "Googlebot (Search Bot)",
    "id" : 6
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [BotsConfigurationDTO](#)

401

Unauthorized [ApiErrorResponse](#)

404

Not Found [ApiErrorResponse](#)

406

Not Acceptable [ApiErrorResponse](#)

500

[Server Error ApiErrorResponse](#)

```
post /api/prov/v1/sites/performance/caching-rules/edit
```

Edit a cache rule (editCacheRule)
Use this operation for editing a cache rule

Query parameters

action (required)

Query Parameter

— Rule action. See Possible action parameter values.
Possible action parameter

values:
HTTP_CACHE_MAKE_STATIC Cache ResourceHTTP_CACHE_CLIENT_CACHE_CTL Cache Resource on ClientHTTP_CACHE_FORCE_UNCACHEABLE Don't Cache ResourceHTTP_CACHE_DIFFERENTIATE_SSL Differentiate Cache Key by HTTP/HTTPS SchemeHTTP_CACHE_DIFFERENTIATE_BY_HEADER Differentiate Cache Key by HeaderHTTP_CACHE_DIFFERENTIATE_BY_COOKIE Differentiate Cache Key by CookieHTTP_CACHE_DIFFERENTIATE_BY_GEO Differentiate Cache Key by GeolocationHTTP_CACHE_IGNORE_PARAMS Ignore Parameters in Cache KeyHTTP_CACHE_IGNORE_AUTH_HEADER Cache Authenticated ResourcesHTTP_CACHE_FORCE_VALIDATION Force User AuthenticationHTTP_CACHE_ADD_TAG Create TagHTTP_CACHE_ENRICH_CACHE_KEY Enrich Cache Key

site_id (required)
Query Parameter
— Numeric identifier of the site to operate on. format: int64

rule_id (required)
Query Parameter
— ID of the rule to change. format: int64

name (required)
Query Parameter
— Rule name.

filter (optional)
Query Parameter
— Rule will trigger only a request that matches this filter. For more details on filters, see Syntax Guide.

ttl (optional)
Query Parameter
— Rule TTL. Only relevant when action is HTTP_CACHE_MAKE_STATIC or HTTP_CACHE_CLIENT_CACHE_CTL

ttl_unit (optional)
Query Parameter
— Rule TTL time unit.
Must be one of SECONDS, MINUTES, HOURS, DAYS or WEEKS. If no time unit is provided, SECONDS is used.
Only relevant when action is HTTP_CACHE_MAKE_STATIC or HTTP_CACHE_CLIENT_CACHE_CTL

differentiated_by_value (optional)
Query Parameter
— Value to differentiate by. HTTP_CACHE_DIFFERENTIATE_BY_HEADER - header name, HTTP_CACHE_DIFFERENTIATE_BY_COOKIE - cookie name, HTTP_CACHE_DIFFERENTIATE_BY_GEO - geo location
(ISO 3166-1 alpha-2 country codes), otherwise irrelevant.

params (optional)
Query Parameter
— Comma separated list of parameters to ignore. Parameters name must be alphanumeric.

all_params (optional)
Query Parameter
— When set to true: all parameters in cache key will be ignored.
Default: false.
Relevant for HTTP_CACHE_IGNORE_PARAMS action

tag_name (optional)
Query Parameter
— The name of the tag to add.

text (optional)
Query Parameter
— Add text to the cache key as suffix. Relevant for the HTTP_CACHE_ENRICH_CACHE_KEY action

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
2 - Invalid input
2002 - Object is not found [ApiResult](#)

```
post /api/prov/v1/sites/incapRules/edit
```

Edit rule (editCustomRule)

Use this operation to edit an existing rule (Delivery, Security or Rate).

Query parameters

action (optional)

Query Parameter

— Rule action.

Possible action parameter values for Delivery

Rules:
RULE_ACTION_REDIRECT Redirect the client to a different URL, responding with a 30X response.RULE_ACTION_SIMPLIFIED_REDIRECT Redirect the client to a different URL, responding with a 30X response.RULE_ACTION_REWRITE_URL Modify the path to which a specific request is targeted.RULE_ACTION_REWRITE_HEADER Modify or add a request header before passing traffic to the origin server.RULE_ACTION_REWRITE_COOKIE Modify or add cookies that are sent by the client to the origin server. The cookie name and value should be indicated.RULE_ACTION_DELETE_HEADER Remove a specific request header, which means that it won't be sent to the origin server.RULE_ACTION_DELETE_COOKIE Remove a specific cookie set on the client, which means that it won't be sent to the origin server.RULE_ACTION_FORWARD_TO_DC Define the data center to which a specific request will be sent.RULE_ACTION_FORWARD_TO_PORT Define the port to which a specific request will be sent.RULE_ACTION_RESPONSE_REWRITE_HEADER Modify or add a header to the response received from the origin server.RULE_ACTION_RESPONSE_DELETE_HEADER Remove a specific response header, which means that it won't be returned to the

client.RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE Modify the response code received from the origin server.
Possible action parameter values for security rules:
RULE_ACTION_ALERT Generate a non blocking alert for this event.RULE_ACTION_BLOCK Block the current request and generate an alert for this event.RULE_ACTION_BLOCK_USER Block the current session and generate an alert for this event. Any subsequent request from the same Session will be blocked.RULE_ACTION_BLOCK_IP Block the current session and generate an alert for this event. Any subsequent request from the same Session will be blocked.RULE_ACTION_RETRY Require any client matching the rule filters to support cookies in order to complete the request.RULE_ACTION_INTRUSIVE_HTML Require any client matching the rule filters to support javascript in order to complete the request. Since the Javascript test is embedded in an HTML page, this action should only be enabled for HTML resources.RULE_ACTION_CAPTCHA Require any client matching the rule filters to pass a CAPTCHA test in order to complete the request. Since the CAPTCHA test is embedded in an HTML page, this action should only be enabled for HTML resources.
Possible action parameter values for counter (rate) rules:
RULE_ACTION_RATE Count the number of requests received that match the rule filter.

rule_id (required)

Query Parameter

— Rule ID. format: int64

name (optional)

Query Parameter

— Rule name.

filter (optional)

Query Parameter

— Rule will trigger only a request that matches this filter. For more details on filter guidelines, see Syntax Guide.

response_code (optional)

Query Parameter

— Redirect rule's response code. Valid values are 302, 301, 303, 307, 308. format: int32

protocol (optional)

Query Parameter

—

add_missing (optional)

Query Parameter

— Add cookie or header if it doesn't exist (Rewrite cookie rule only)

from (optional)

Query Parameter

— The pattern to rewrite.
For RULE_ACTION_REWRITE_URL - The URL to rewrite.
For RULE_ACTION_REWRITE_HEADER - The header value to rewrite.
For RULE_ACTION_REWRITE_COOKIE - The cookie value to rewrite.
For RULE_ACTION_SIMPLIFIED_REDIRECT - Redirect the client to a different URL, responding with a 30X response.

to (optional)

Query Parameter

— The pattern to change to.
For RULE_ACTION_REWRITE_URL - The URL to change to.
For RULE_ACTION_REWRITE_HEADER - The header value to change to.
For RULE_ACTION_REWRITE_COOKIE - The cookie value to change to.
For RULE_ACTION_SIMPLIFIED_REDIRECT - Redirect the client to a different URL, responding with a 30X response.

rewrite_name (optional)

Query Parameter

— Name of cookie or header to rewrite. Applies only for RULE_ACTION_REWRITE_COOKIE and RULE_ACTION_REWRITE_HEADER.

dc_id (optional)

Query Parameter

— Data center to forward request to. Applies only for RULE_ACTION_FORWARD_TO_DC. format: int64

allow_caching (optional)

Query Parameter

rate_context (optional)

Query Parameter

— The context of the rate counter. Possible values: IP / Session. Applies only to rules using RULE_ACTION_RATE.

rate_interval (optional)

Query Parameter

— The interval (in seconds) of the rate counter. Possible values: A multiple of 10 from 10-300. Applies only to rules using RULE_ACTION_RATE. format: int32

is_test_mode (optional)

Query Parameter

— Make rule apply only for IP address the API request was sent from.
This option is not available for Simplified Redirect rules.

port_forwarding_context (optional)

Query Parameter

— Context for port forwarding. "Use Port Value" or "Use Header Name". Applies only for RULE_ACTION_FORWARD_TO_PORT.

port_forwarding_value (optional)

Query Parameter

— Port number or header name for port forwarding. Applies only for RULE_ACTION_FORWARD_TO_PORT.

multiple_deletions (optional)

Query Parameter

— Delete multiple header occurrences. Applies only to rules using RULE_ACTION_DELETE_HEADER and RULE_ACTION_RESPONSE_DELETE_HEADER.

rewrite_existing (optional)

Query Parameter

— Rewrite cookie or header if it exists

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 2 - Timerange invalid, 9413 - Unknown/unauthorized site_id
 9415 - Operation not allowed
 3015 - Internal error [ApiResult](#)

```
post /api/prov/v1/sites/dataCenters/servers/edit
```

Edit server (editDCServer)

Use this operation to edit a server in a data center.

Query parameters

server_id (required)

Query Parameter

— Server ID. format: int64

server_address (optional)

Query Parameter

— The IP address of the server to modify.

is_enabled (optional)

Query Parameter

— Enable or disable the server (Boolean).

is_standby (optional)

Query Parameter

— Set the server as Active (P0) or Standby (P1) (Boolean).

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9415 -invalid.server.state
2- invalid data center
1 -Unexpected error
9413 -invalid server
1 -General error [inline_response_200_2](#)

```
post /api/prov/v1/sites/dataCenters/edit
```

Edit data center (editDataCenter)
Use this operation to edit site's data center.

Query parameters

dc_id (required)

Query Parameter

— The data center's ID. format: int64

name (optional)

Query Parameter

— The new data center's name.

is_enabled (optional)

Query Parameter

— Enables the data center.

is_standby (optional)

Query Parameter

— Defines the data center as **standby** for failover.

is_content (optional)

Query Parameter

— The data center will be available for specific resources (**Forward Delivery Rules**).

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 -invalid data center
2- data center with that name already exists
[inline_response_200_3](#)

```
post /api/prov/v1/sites/performance/cache-shield/enable
```

Enable cache shield (enableCacheShield)
Enable Cache Shield for a given site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

enable (required)

Query Parameter

— Use **true** to enable cache shield on the specified site, and **false** to disable it.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
1 - Unexpected error
[405 - Api is disabled](#) [ApiResult](#)

```
post /api/prov/v1/sites/performance/caching-rules/enable
```

Enable or disable cache rule (enableDisableCacheRule)
Use this operation for enabling or disable cache rule

Query parameters

site_id (required)
 Query Parameter
 — Numeric identifier of the site to operate on. format: int64

rule_id (required)
 Query Parameter
 — Numeric identifier of the site to operate on. format: int64

enable (required)
 Query Parameter
 — When true, the rule will be enabled. Set to false to disable.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 9413 - Unknown/unauthorized site_id
 9415 - Operation not allowed
 2 - Invalid input
 2002 - Object is not found [ApiResult](#)

```
post /api/prov/v1/sites/incapRules/enableDisable
```

Enable or disable rule (enableDisableCustomRule)
 Use this operation to enable or disable a rule (Delivery, Security or Rate).

Query parameters

rule_id (required)
 Query Parameter
 — Rule id format: int64
 enable (required)
 Query Parameter
 — When true, the rule will be enabled. Set to false to disable

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

res - contains the specific error code:
 2 - Timerange invalid, 9413 - Unknown/unauthorized site_id
 9415 - Operation not allowed
 3015 - Internal error [ApiResult](#)

```
post /api/prov/v1/sites/performance/advanced/get
```

Get advanced caching settings (getAdvancedCachingSettings)
 Use this operation to get advanced caching settings.

Query parameters

site_id (required)
 Query Parameter
 — Numeric identifier of the site to operate on.

param (required)

Query Parameter

— Name of configuration parameter to set. Possible values for param and value parameters:

- async_validation Sets Async validation. Pass "true" or "false" in the value parameter.
- minify_javascript Sets the Minify JS. Pass "true" or "false" in the value parameter.
- minify_css Sets the Minify CSS. Pass "true" or "false" in the value parameter.
- minify_static_html Sets Minify static HTML. Pass "true" or "false" in the value parameter.
- compress_jpeg Sets the Compress JPEG. Pass "true" or "false" in the value parameter.
- progressive_image_rendering Sets the Progressive Image rendering flag. Pass "true" or "false" in the value parameter.
- aggressive_compression Sets the Aggressive compression rendering flag. Pass "true" or "false" in the value parameter.
- compress_png Sets the Compress PNG flag. Pass "true" or "false" in the value parameter.
- on_the_fly_compression "On the fly" Compression. Pass "true" or "false" in the value parameter.
- tcp_pre_pooling TCP Pre-Pooling. Pass "true" or "false" in the value parameter.
- comply_no_cache Comply with no-cache and max-age directives in client requests. Pass "true" or "false" in the value parameter.
- comply_vary Comply with the Vary header. Pass "true" or "false" in the value parameter.
- use_shortest_caching Use shortest caching duration in case of conflicts. Pass "true" or "false" in the value parameter.
- prefer_last_modified Prefer 'last modified' over eTag. Pass "true" or "false" in the value parameter.
- disable_client_side_caching Disable client side caching. Pass "true" or "false" in the value parameter.
- cache_300x Cache 300X responses. Pass "true" or "false" in the value parameter.
- unite_naked_full_cache Use the same cache for full and naked domains. For example, use the same cached resource for and a.
- cache_empty_responses Cache responses that don't have a message body.
- cache_http_10_responses Cache HTTP 1.0 type responses that don't include the Content-Length header or chunking.
- send_age_header Send Cache-Control: max-age and Age headers. Pass "true" or "false" in the value parameter.
- support_non_sni_clients Enable or disable the support for Non-SNI clients for TLS connections between clients and Imperva. Pass "true" or "false" in the value parameter.
- origin_connection_reuse Requests from multiple client connections may be transmitted through a single TCP connection to the origin, while requests from a single client connection may be distributed across multiple TCP connections to the origin. This option disables that behavior. Pass "true" or "false" in the value parameter.
- redirect_http_to_https Redirect HTTP requests to HTTPS requests by sending an HTTP 301 response.
- redirect_naked_domain_to_full Redirect requests from your website's naked domain to its full domain by sending an HTTP 301 response.
- http_2 Enables supporting browsers to take advantage of the performance enhancements provided by HTTP/2 for your website. Non-supporting browsers can connect via HTTP/1.0 or HTTP/1.1. HTTP/2 support requires that SSL is configured for your website. Pass "true" or "false" in the value parameter

Return type

inline_response_200_6

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id [inline_response_200_6](#)

```
get /api/prov/v3/sites/{extSiteId}/settings/botConfiguration
```

Get website bot configuration (getBotsConfiguration)
Retrieve the Bot Access Control configuration for a given website.

Path parameters

extSiteId (required)

Path Parameter

— format: int64

Return type

BotsConfigurationDTO

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "badBots" : [ null, null ],
    "canceledGoodBots" : [ {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    }, {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    } ]
  }, {
    "badBots" : [ null, null ],
    "canceledGoodBots" : [ {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    }, {
      "displayName" : "Googlebot (Search Bot)",
      "id" : 6
    } ]
  } ]
}
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [BotsConfigurationDTO](#)

401

Unauthorized [ApiErrorResponse](#)

404

Not Found [ApiErrorResponse](#)

500

Server Error [ApiErrorResponse](#)

```
post /api/prov/v1/sites/performance/cache404
```

Get cache 404 settings (getCache404Settings)

Use this operation to get the caching settings of 404 responses for a site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

[inline_response_200_7](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_7](#)

```
post /api/prov/v1/sites/performance/cache-mode/get
```

Get caching mode (getCachingMode)
Use this operation to get a site's caching mode.

Query parameters

site_id (required)
Query Parameter
— Numeric identifier of the site to operate on.

Return type

[inline_response_200_8](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id [inline_response_200_8](#)

```
post /api/prov/v1/sites/data-privacy/show
```

Get site data storage region (getDataRegion)
Use this operation to get the site data region.

Query parameters

site_id (required)
Query Parameter
— Numeric identifier of the site to operate on. format: int64

Return type

[inline_response_200_18](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9415 - Operation not allowed
14002 - No region for account [inline_response_200_18](#)

```
post /api/prov/v1/sites/htmlinjections
```

Get HTML injection rules (getHtmlInjectionRules)
Use this operation to list all the HTML Injection rules

Query parameters

site_id (required)
Query Parameter
— Numeric identifier of the site to operate on

Return type

[inline_response_200_19](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [inline_response_200_19](#)

```
post /api/prov/v1/sites/data-privacy/show-override-by-geo
```

Check Site Regions by Origin Geolocation (getOverrideSiteRegionsByGeo)

Use this operation to check if the data storage region for each new site is based on the geolocation of the origin server.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [
    {
      "key" : {}
    },
    {
      "key" : {}
    }
  ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [ApiResult](#)

```
post /api/prov/v1/sites/datacenter/origin-pop/recommend
```

Get data center recommended origin PoPs (getRecommendedDataCenterOriginPoPs)
Get a list of recommended origin PoPs for a given data center.

Query parameters

dc_id (required)

Query Parameter

— Numeric identifier of the data center to operate on. format: int64

Return type

[inline_response_200_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
405 - Api is disabled</br>2- invalid data center
5 - Cant set Origin PoP for datacenter [inline_response_200_4](#)

```
post /api/prov/v1/sites/performance/response-headers/get
```

Get cached response headers (getResponseHeaderSettings)
Use this operation to get a site's cached response headers.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

[inline_response_200_9](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 9413 - Unknown/unauthorized site_id
 9415 - Operation not allowed
 5 - Operation is unavailable [inline_response_200_9](#)

```
post /api/prov/v1/sites/performance/rewrite-port
```

Get rewrite port (getRewritePorts)

Use this operation to get the rewritten port number used to access the origin server.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

Return type

[inline_response_200_10](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_10](#)

```
post /api/prov/v1/sites/performance/secure-resources/get
```

Get secure resources mode (getSecureResourcesMode)
Use this operation to get the Secure Resources mode for a site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

Return type

[inline_response_200_11](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_11](#)

```
post /api/prov/v1/sites/performance/error-page
```

Get error page (getSiteErrorPageTemplate)

Use this operation to get the custom error page for a given site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
[ApiResult](#)

```
post /api/prov/v1/sites/report
```

Get site report (getSiteReport)

Use this operation to get a report for a site. Reports are sent using Base64 encoding. The time_range parameter is ignored for accounts with the WAF Rules policy feature. For such accounts, the report returns the current status.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

report (required)

Query Parameter

— The report to get. One of: pci-compliance

format (required)

Query Parameter

— The format to get the report in. One of: pdf | html

time_range (required)

Query Parameter

— Time range to fetch data for.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
</i>today Retrieve data from midnight today until the current time.
</i>last_7_days Retrieve data from midnight of 7 days ago until the current time.
</i>last_30_days Retrieve data from midnight of 30 days ago until the current time.
</i>last_90_days Retrieve data from midnight of 90 days ago until the current time.
</i>month_to_date Retrieve data from midnight of the first day of the month until the current time.
</i>custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
****A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
****A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
** **A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

start (optional)

Query Parameter

— Start date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
</i>today Retrieve data from midnight today until the current time.
</i>last_7_days Retrieve data from midnight of 7 days ago until the current time.
</i>last_30_days Retrieve data from midnight of 30 days ago until the current time.
</i>last_90_days Retrieve data from midnight of 90 days ago until the current time.
</i>month_to_date Retrieve data from midnight of the first day of the month until the current time.
</i>custom Specify a custom time range using two additional parameters: start and end.

Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
****A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
****A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
** **A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (optional)

Query Parameter

— End date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

Return type

[inline_response_200_20](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
5001 - Report invalid
5002 - Format invalid
[inline_response_200_20](#)

```
post /api/prov/v1/sites/performance/stale-content/get
```

Get stale content settings (getStaleContent)

When Imperva can't connect to the origin server, serve stale content instead of displaying an error to end users for the specified amount of time. Expired resources are returned from cache, and refreshed asynchronously in the background.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

[inline_response_200_12](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_12](#)

```
get /api/prov/v3/sites/{extSiteId}/settings/TLSConfiguration
```

Get website TLS configuration (getTLSConfiguration)
Retrieve the TLS configuration for a given website.

Path parameters

extSiteId (required)

Path Parameter

— The Imperva ID of the website to operate on. format: int64

Return type

[TLSConfigurationDto](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
```

```

        "subDomainsIncluded" : false,
        "preLoaded" : false
    }
} , {
    "hstsConfiguration" : {
        "maxAge" : 7543,
        "isEnabled" : false,
        "subDomainsIncluded" : false,
        "preLoaded" : false
    }
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK TLSConfigurationDto

401

Unauthorized ApiErrorResponse

404

Not Found ApiErrorResponse

500

Server Error ApiErrorResponse

```
post /api/prov/v1/sites/performance/tag-response/get
```

Get header to tag responses by (getTagResponseHeader)
Get the origin response header containing the cache tags in your resources

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

[inline_response_200_13](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_13](#)

```
post /api/prov/v1/sites/xray/get-link
```

Get XRay access link (getXrayLink)

Use this operation to get a URL that enables debug headers on the specific site. For more details see [XRAY Debug Headers Guide](#)

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

Return type

[inline_response_200_14](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1 - Unexpected error [inline_response_200_14](#)

```
post /api/prov/v1/sites/performance/cache-shield
```

Is cache shield enabled (isCacheShieldEnabled)

Get the enablement state of the Cache Shield feature for a given site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

Return type

[inline_response_200_15](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [inline_response_200_15](#)

```
post /api/prov/v1/sites/performance/caching-rules/list
```

List cache rules for a given site (listCacheRules)
 Use this operation for representing cache rules for a given site

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

page_size (optional)

Query Parameter

— The number of objects to return in the response.
Default is 50.
Maximum: 100

page_num (optional)

Query Parameter

— The page to return starting from 0. Default is 0.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
2 - Invalid input
 [inline_response_200_1](#)

```
post /api/prov/v1/sites/incapRules/list
```

List rules (listCustomRules)
 Use this operation to list security, delivery, and rate rules for a given site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on
include_incap_rules (optional)

Query Parameter

— Whether or not security rules be included. Defaults to "Yes";
include_ad_rules (optional)

Query Parameter

— Whether or not delivery rules should be included. Defaults to Yes

page_size (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 50. Maximum is 100
page_num (optional)

Query Parameter

— The page to return starting from 0. Default to 0

Return type

[ListCustomRulesResponse](#)

Example data

Content-Type: application/json

```
{
  "rate_rules" : {
    "Rates" : [ {
      "id" : "4723",
      "enabled" : "true",
      "interval" : "120",
      "name" : "Test Rate IP",
      "context" : "IP",
      "action" : "RULE_ACTION_RATE",
      "internal_name" : "test-rate-ip",
      "filter" : "ASN == 2"
    } ]
  },
  "delivery_rules" : {
    "Redirect" : [ {
      "to" : "/home.php",
      "id" : "3648",
      "priority" : "1",
      "last_7_days_requests_count" : "0",
      "name" : "Test new",
      "action" : "RULE_ACTION_REWRITE_URL",
      "from" : "*/home.html",
      "filter" : "ASN == 1"
    } ],
    "Forward" : [ {
      "id" : "3628",
      "priority" : "2",
      "last_7_days_requests_count" : "0",
      "name" : "move to rewrite",
      "dc_id" : "54313",
      "action" : "RULE_ACTION_FORWARD_TO_DC",
      "filter" : ""
    } ]
  }
}
```

```

"incap_rules" : {
  "All" : [ {
    "id" : "3660",
    "last_7_days_requests_count" : "0",
    "name" : "Ortal",
    "action" : "RULE_ACTION_ALERT",
    "filter" : ""
  } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input, 9413 - Unknown/unauthorized site_id
[ListCustomRulesResponse](#)

```
get /api/prov/v3/rules
```

List rules ([listCustomRulesByFilter](#))
Use this operation to list security rules by filters.

Query parameters

sitelds (optional)

Query Parameter

— A list of website ids. If this parameter is provided, only rules of websites matching one of these IDs will be returned.

ruleids (optional)

Query Parameter

— A list of rule ids. If this parameter is provided, only rules matching one of these IDs will be returned.

categories (optional)

Query Parameter

— A list of rule categories. If this parameter is provided, only rules matching one of these categories will be returned.

subAccts (optional)

Query Parameter

— A list of sub account IDs. When provided, the API returns rules corresponding to websites that belong to the specified sub account IDs. This parameter is ignored if the API call is authenticated as a sub account.

names (optional)

Query Parameter

— A list of rules names. If this parameter is provided, only rules matching one of these names will be returned.

page_size (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 50. Maximum is 500

page_num (optional)

Query Parameter

— The page to return starting from 0. Default to 0

Return type

CustomRulesDTOSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "account_id" : 1,
    "site_id" : 6,
    "rule" : {
      "rule_id" : 0,
      "name" : "name",
      "action" : "RULE_ACTION_NONE",
      "enabled" : true
    }
  }, {
    "account_id" : 1,
    "site_id" : 6,
    "rule" : {
      "rule_id" : 0,
      "name" : "name",
      "action" : "RULE_ACTION_NONE",
      "enabled" : true
    }
  } ],
  "meta" : {
    "size" : 2,
    "totalPages" : 5,
    "page" : 7,
    "totalElements" : 5
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res CustomRulesDTOSuccessResponse

```
post /api/prov/v1/sites/dataCenters/list
```

List data centers (listDataCenters)

Use this operation to list a site's data centers including the data centers' servers.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

Return type

[inline_response_200_5](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - invalid site</br>2 - invalid data center

[inline_response_200_5](#)

```
get /api/prov/v3/sites/{extSiteId}/data-centers-configuration
```

get site's data centers' configuration (listDataCentersConfiguration)

Use this operation to get configured data centers and all their servers

Path parameters

extSiteId (required)

Path Parameter

— format: int64

Return type

DataCentersConfigurationDTO

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lbAlgorithm" : "GEO_PREFERRED",
    "dataCenterMode" : "MULTIPLE_DC",
    "kickStartPass" : "kickstart-pass",
    "kickStartURL" : "https://www.example.com:443/kickStart",
    "isPersistent" : false,
    "dataCenters" : [ {
      "lbAlgorithm" : "WEIGHTED",
      "isContent" : true,
      "weight" : 40,
      "isRestOfTheWorld" : true,
      "isActive" : false,
      "geoLocations" : [ "AFRICA", "AFRICA" ],
      "ipMode" : "MULTIPLE_IP",
      "servers" : [ {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
      }, {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
      } ],
      "originPop" : "lax",
      "isEnabled" : false,
      "name" : "London DC",
      "id" : 7543,
      "webServersPerServer" : 5
    }, {
      "lbAlgorithm" : "WEIGHTED",
      "isContent" : true,
      "weight" : 40,
      "isRestOfTheWorld" : true,
      "isActive" : false,
      "geoLocations" : [ "AFRICA", "AFRICA" ],
      "ipMode" : "MULTIPLE_IP",
      "servers" : [ {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
      }, {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
      } ]
    }
  }
}
```

```

        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
    } ],
    "originPop" : "lax",
    "isEnabled" : false,
    "name" : "London DC",
    "id" : 7543,
    "webServersPerServer" : 5
} ],
"kickStartUser" : "kickstart-user",
"minAvailableServersForDataCenterUp" : 3,
"failOverRequiredMonitors" : "MANY"
}, {
    "lbAlgorithm" : "GEO_PREFERRED",
    "dataCenterMode" : "MULTIPLE_DC",
    "kickStartPass" : "kickstart-pass",
    "kickStartURL" : "https://www.example.com:443/kickStart",
    "isPersistent" : false,
    "dataCenters" : [ {
        "lbAlgorithm" : "WEIGHTED",
        "isContent" : true,
        "weight" : 40,
        "isRestOfTheWorld" : true,
        "isActive" : false,
        "geoLocations" : [ "AFRICA", "AFRICA" ],
        "ipMode" : "MULTIPLE_IP",
        "servers" : [ {
            "serverMode" : "ACTIVE",
            "address" : "1.2.3.4",
            "isEnabled" : false,
            "weight" : 70,
            "id" : 7543
        }, {
            "serverMode" : "ACTIVE",
            "address" : "1.2.3.4",
            "isEnabled" : false,
            "weight" : 70,
            "id" : 7543
        } ],
        "originPop" : "lax",
        "isEnabled" : false,
        "name" : "London DC",
        "id" : 7543,
        "webServersPerServer" : 5
    }, {
        "lbAlgorithm" : "WEIGHTED",
        "isContent" : true,
        "weight" : 40,
        "isRestOfTheWorld" : true,
        "isActive" : false,
        "geoLocations" : [ "AFRICA", "AFRICA" ],
        "ipMode" : "MULTIPLE_IP",
        "servers" : [ {
            "serverMode" : "ACTIVE",
            "address" : "1.2.3.4",
            "isEnabled" : false,
            "weight" : 70,
        } ]
    }
]
}

```

```

        "id" : 7543
    }, {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
    } ],
    "originPop" : "lax",
    "isEnabled" : false,
    "name" : "London DC",
    "id" : 7543,
    "webServersPerServer" : 5
} ],
"kickStartUser" : "kickstart-user",
"minAvailableServersForDataCenterUp" : 3,
"failOverRequiredMonitors" : "MANY"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DataCentersConfigurationDTO

401

Unauthorized. E.g. Wrong API key, locked user [ApiErrorResponse](#)

403

Forbidden. E.g. Missing abilities [ApiErrorResponse](#)

404

Not Found. E.g. Site doesn't exist or belongs to other tenant [ApiErrorResponse](#)

500

Server Error [ApiErrorResponse](#)

```
get /api/prov/v3/sites/{extSiteId}/delivery-rules-configuration
```

Get site's delivery rule priority order for a specific rule category. (listDeliveryRulesConfiguration)
Use this operation to list all delivery rules of a specific category. The rules are prioritized by order of appearance.

Path parameters

extSiteId (required)

Path Parameter

— Numeric identifier of the site to operate on. format: int64

Query parameters

category (required)

Query Parameter

— Rules category. Possible values:
 REDIRECT - Redirect requests with 30X response.
SIMPLIFIED_REDIRECT - Redirect requests with 30X response. (static redirect, doesn't support condition)
 REWRITE - Modify, add, and remove different request attributes such as URL, headers and cookies.
 REWRITE_RESPONSE - Modify, add, and remove different response attributes such as headers, status code and error responses.
 FORWARD - Forward the request to a specific data-center or port.

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

Example data

Content-Type: Supported actions:

RULE_ACTION_FORWARD_TO_PORT (ForwardToPortRuleDTO),
RULE_ACTION_FORWARD_TO_DC (ForwardToDcRuleDTO)

```
{"data": [{"filter": "ASN == 1", "dc_id": 1234, "rule_name": "New delivery rule", "action": "RULE_ACTION_FORWARD_TO_DC", "enabled": true}, {"filter": "ASN == 1", "port_forwarding_context": "[header/port]", "port_forwarding_value": "1234", "rule_name": "New delivery rule", "action": "RULE_ACTION_FORWARD_TO_PORT", "enabled": true}]} 
```

Example data

Content-Type: Supported actions:

RULE_ACTION_REDIRECT (RedirectRuleDTO)

```
{"data": [{"filter": "ASN == 1", "from": "/1", "to": "/2", "response_code": 302, "rule_name": "New delivery rule"}]} 
```

```
e":"New delivery rule","action":"RULE_ACTION_REDIRECT","enabled":true}]]}
```

Example data

Content-Type: Supported actions:

RULE_ACTION_SIMPLIFIED_REDIRECT (SimplifiedRedirectRuleDTO)

```
{"data": [{"from":"/1","to":"/2","response_code":302,"rule_name":"New delivery rule","action":"RULE_ACTION_REDIRECT","enabled":true}]}]
```

Example data

Content-Type: Supported actions:

RULE_ACTION_REWRITE_COOKIE (RewriteRequestCookieRuleDTO),
RULE_ACTION_REWRITE_HEADER (RewriteRequestHeaderRuleDTO),
RULE_ACTION_REWRITE_URL (RewriteRequestUrlRuleDTO),
RULE_ACTION_DELETE_HEADER (RewriteRequestDeleteHeaderRuleDTO),
RULE_ACTION_DELETE_COOKIE (RewriteRequestDeleteCookieRuleDTO)

```
{"data": [{"filter": "ASN == 1", "from": "cookie1", "to": "cookie2", "cookie_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_COOKIE", "enabled": true}, {"filter": "ASN == 1", "from": "header1", "to": "header2", "header_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_HEADER", "enabled": true}, {"filter": "ASN == 1", "from": "/1", "to": "/2", "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_URL", "enabled": true}, {"filter": "ASN == 1", "header_name": "abc", "multiple_headers_deletion": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_HEADER", "enabled": true}, {"filter": "ASN == 1", "cookie_name": "abc", "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_COOKIE", "enabled": true}]}]
```

Example data

Content-Type: Supported actions:

RULE_ACTION_RESPONSE_REWRITE_HEADER (RewriteResponseHeaderRuleDTO),
RULE_ACTION_RESPONSE_DELETE_HEADER (RewriteResponseDeleteHeaderRuleDTO),
RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE (RewriteResponseCodeRuleDTO),
RULE_ACTION_CUSTOM_ERROR_RESPONSE (RewriteResponseCustomErrorRuleDTO)

```
{"data": [{"filter": "ASN == 1", "header_name": "abc", "multiple_headers_deletion": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_RESPONSE_DELETE_HEADER", "enabled": true}, {"filter": "ASN == 1", "from": "header1", "to": "header2", "header_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_RESPONSE_REWRITE_HEADER", "enabled": true}, {"filter": "ASN == 1", "response_code": 302, "rule_name": "New delivery rule", "action": "RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE", "enabled": true}, {"filter": "ASN == 1", "error_response_format": "[JSON|XML]", "error_response_data": "<?xml version='1.0' encoding='UTF-8'?>", "error_type": "error.type.all", "response_code": 400, "rule_name": "New delivery rule", "action": "RULE_ACTION_CUSTOM_ERROR_RESPONSE", "enabled": true}]}]
```

401

Unauthorized [ApiErrorResponse](#)

404

Not Found [ApiErrorResponse](#)

500

[Server Error ApiErrorResponse](#)

```
post /api/prov/v1/sites/list
```

List sites (listSites)
List sites for an account

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.
If the account has sub accounts, the operation returns results for the sites in the account and in all of its sub accounts.

page_size (optional)

Query Parameter

— The number of objects to return in the response. Default is 50. Maximum: 100

page_num (optional)

Query Parameter

— The page to return starting from 0. Default is 0

Return type

[ApiResultListSites](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ],
  "ApiResultSiteStatus" : [ {
    "login_protect" : {
      "urls" : [ "/userlist", "/userlist" ],
      "allow_all_users" : true,
      "allow_anonymous" : false
    }
  } ]
}
```



```

        "name" : "Illegal Resource Access",
        "action" : "api.threats.action.block_user",
        "action_text" : "Block User"
    }, {
        "id" : "api.threats.ddos",
        "name" : "DDoS",
        "activation_mode" : "api.threats.ddos.activation_mode.off",
        "activation_mode_text" : "Off",
        "ddos_traffic_threshold" : "api.threats.ddos.ddos_trassic_threshold",
        "ddos_traffic_threshold_text" : "750",
        "ddos_adaptive_threshold" : "500",
        "ddos_adaptive_threshold_last_update_time" : "1610396346000"
    }, {
        "id" : "api.threats.backdoor",
        "name" : "Backdoor Protect",
        "action" : "api.threats.action.quarantine_url",
        "action_text" : "Auto-Quarantine"
    }, {
        "action" : "api.threats.action.block_ip",
        "action_text" : "Block IP",
        "id" : "api.threats.remote_file_inclusion",
        "name" : "Remote File Inclusion"
    }
},
"acls" : {
    "rules" : [ {
        "ips" : [ "2.3.4.5" ],
        "exceptions" : [ {
            "values" : [ {
                "id" : "api.rule_exception_type.url",
                "name" : "URL",
                "urls" : [ {
                    "value" : "/home",
                    "pattern" : "EQUALS"
                } ]
            } ],
            "id" : 493271006
        } ],
        "id" : "api.acl.blacklisted_ips",
        "name" : "Visitors from denylisted IPs"
    } ]
},
"acceleration_level" : "advanced",
"requestBodyTimeouts" : {
    "methods" : [ { }, { } ],
    "byteCount" : 1,
    "interval" : 6
},
"res" : 0,
"res_message" : "OK",
"support_all_tls_versions" : true,
"use_wildcard_san_instead_of_full_domain_san" : true,
"additionalErrors" : [ 3005, 3005 ],
"warnings" : [ {
    "type" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
}, {

```

```

    "type" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
  },
  "dns" : [ {
    "dns_record_name" : "loginprotectapi1610396334653.incaptest.info",
    "set_type_to" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
  },
  {
    "dns_record_name" : "loginprotectapi1610396334653.incaptest.info",
    "set_type_to" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
  ],
  "active" : "active",
  "restricted_cname_reuse" : true,
  "performance_configuration" : {
    "compress_png" : true,
    "aggressive_compression" : true,
    "use_shortest_caching" : true,
    "prefer_last_modified" : true,
    "minify_css" : true,
    "comply_no_cache" : true,
    "comply_vary" : true,
    "advanced_caching_rules" : [
      "never_cache_resources" : [ {
        "pattern" : "SUFFIX",
        "url" : "/test.html"
      }],
      "always_cache_resources" : [ {
        "pattern" : "NOT_EQUALS",
        "url" : "/index.html",
        "ttl" : "5",
        "ttlUnits" : "SECONDS"
      },
      {
        "pattern" : "EQUALS",
        "url" : "/home.html",
        "ttl" : "6",
        "ttlUnits" : "DAYS"
      }]
    },
    "prefer_last_modified" : true,
    "cache_headers" : [ { }, { } ],
    "acceleration_level_raw" : "none",
    "async_validation" : true,
    "progressive_image_rendering" : true,
    "compress_jpeg" : true,
    "disable_client_side_caching" : true,
    "minify_javascript" : true,
    "minify_static_html" : true,
    "cache300x" : true,
    "acceleration_level" : "advanced",
    "on_the_fly_compression" : true,
    "tcp_pre_pooling" : true,
    "compress_jpeg" : true
  },
  "display_name" : "loginprotectapi1610396334653.incaptest.info",
  "ips" : [ "1.2.3.4", "1.2.3.4" ],

```

```

"acceleration_level_raw" : "none",
"account_id" : 1,
"add_naked_domain_san" : true,
"domain" :"admin@example.com",
"siteDualFactorSettings" : {
  "customAreas" : [ {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  }, {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  } ],
  "customAreasExceptions" : [ {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  }, {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  } ],
  "application" : true,
  "shouldSendLoginNotifications" : true,
  "specificUsers" : [ "lpuser1_api1610396342408@incaptest.info", "lpuser1_api1610396342408@incaptest.info" ],
  "allowAllUsers" : true,
  "shouldSuggestApplicatons" : true,
  "allowedMedia" : [ "sms", "sms" ],
  "version" : 0,
  "enabled" : false
},
"site_id" : 10,
"extended_ddos" : 5,
"incap_rules" : [ {
  "updated_at" : 1611228121241,
  "name" : "Block Click Worms",
  "updated_by" : "John",
  "action" : "api.rule_action_type.rule_action_block",
  "rule" : "ClientIP == 1.2.3.4",
  "comment" : "rule comment",
  "id" : 123,
  "creation_date" : 5
}, {
  "updated_at" : 1611228121241,
  "name" : "Block Click Worms",
  "updated_by" : "John",
  "action" : "api.rule_action_type.rule_action_block",
  "rule" : "ClientIP == 1.2.3.4",
  "comment" : "rule comment",
  "id" : 123,
  "creation_date" : 5
} ],
"status" : "pending-dns-changes",
"enable_http_between_Imperva_and_origin" : "80"
}, {
  "login_protect" : {
    "urls" : [ "/userlist", "/userlist" ],
    "allow_all_users" : true,
    "authentication_methods" : [ "email", "email" ],
    "send_lp_notifications" : true,
    "enabled" : true,
    "allow_ip_overrides" : true
  }
}

```



```

}, {
    "id" : "api.threats.ddos",
    "name" : "DDoS",
    "activation_mode" : "api.threats.ddos.activation_mode.off",
    "activation_mode_text" : "Off",
    "ddos_traffic_threshold" : "api.threats.ddos.ddos_trassic_threshold",
    "ddos_traffic_threshold_text" : "750",
    "ddos_adaptive_threshold" : "500",
    "ddos_adaptive_threshold_last_update_time" : "1610396346000"
}, {
    "id" : "api.threats.backdoor",
    "name" : "Backdoor Protect",
    "action" : "api.threats.action.quarantine_url",
    "action_text" : "Auto-Quarantine"
}, {
    "action" : "api.threats.action.block_ip",
    "action_text" : "Block IP",
    "id" : "api.threats.remote_file_inclusion",
    "name" : "Remote File Inclusion"
}
},
"acls" : {
    "rules" : [ {
        "ips" : [ "2.3.4.5" ],
        "exceptions" : [ {
            "values" : [ {
                "id" : "api.rule_exception_type.url",
                "name" : "URL",
                "urls" : [ {
                    "value" : "/home",
                    "pattern" : "EQUALS"
                } ]
            } ],
            "id" : 493271006
        } ],
        "id" : "api.acl.blacklisted_ips",
        "name" : "Visitors from denylisted IPs"
    }
]
},
"acceleration_level" : "advanced",
"requestBodyTimeouts" : {
    "methods" : [ { }, { } ],
    "byteCount" : 1,
    "interval" : 6
},
"res" : 0,
"res_message" : "OK",
"support_all_tls_versions" : true,
"use_wildcard_san_instead_of_full_domain_san" : true,
"additionalErrors" : [ 3005, 3005 ],
"warnings" : [ {
    "type" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
}, {
    "type" : "CNAME",
    "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
} ]
}

```

```

} ],
"dns" : [ {
  "dns_record_name" : "loginprotectapi1610396334653.incaptest.info",
  "set_type_to" : "CNAME",
  "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
}, {
  "dns_record_name" : "loginprotectapi1610396334653.incaptest.info",
  "set_type_to" : "CNAME",
  "set_data_to" : [ "67eufzur3g.dev.impervadns.net", "67eufzur3g.dev.impervadns.net" ]
},
"active" : "active",
"restricted_cname_reuse" : true,
"performance_configuration" : {
  "compress_png" : true,
  "aggressive_compression" : true,
  "use_shortest_caching" : true,
  "prefer_last_modified" : true,
  "minify_css" : true,
  "comply_no_cache" : true,
  "comply_vary" : true,
  "advanced_caching_rules" : [
    "never_cache_resources" : [ {
      "pattern" : "SUFFIX",
      "url" : "/test.html"
    }],
    "always_cache_resources" : [ {
      "pattern" : "NOT_EQUALS",
      "url" : "/index.html",
      "ttl" : "5",
      "ttlUnits" : "SECONDS"
    },
    {
      "pattern" : "EQUALS",
      "url" : "/home.html",
      "ttl" : "6",
      "ttlUnits" : "DAYS"
    }]
  },
  "prefer_last_modified" : true,
  "cache_headers" : [ { }, { } ],
  "acceleration_level_raw" : "none",
  "async_validation" : true,
  "progressive_image_rendering" : true,
  "compress_jpeg" : true,
  "disable_client_side_caching" : true,
  "minify_javascript" : true,
  "minify_static_html" : true,
  "cache300x" : true,
  "acceleration_level" : "advanced",
  "on_the_fly_compression" : true,
  "tcp_pre_pooling" : true,
  "compress_jpeg" : true
},
"display_name" : "loginprotectapi1610396334653.incaptest.info",
"ips" : [ "1.2.3.4", "1.2.3.4" ],
"acceleration_level_raw" : "none",
"account_id" : 1,
"add_naked_domain_san" : true,

```

```

"domain" : "admin@example.com",
"siteDualFactorSettings" : {
  "customAreas" : [ {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  }, {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  } ],
  "customAreasExceptions" : [ {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  }, {
    "pattern" : "CONTAINS",
    "url" : "/userlist"
  } ],
  "application" : true,
  "shouldSendLoginNotifications" : true,
  "specificUsers" : [ "lpuser1_api1610396342408@incaptest.info", "lpuser1_api1610396342408@incaptest.info" ],
  "allowAllUsers" : true,
  "shouldSuggestApplicatons" : true,
  "allowedMedia" : [ "sms", "sms" ],
  "version" : 0,
  "enabled" : false
},
"site_id" : 10,
"extended_ddos" : 5,
"incap_rules" : [ {
  "updated_at" : 1611228121241,
  "name" : "Block Click Worms",
  "updated_by" : "John",
  "action" : "api.rule_action_type.rule_action_block",
  "rule" : "ClientIP == 1.2.3.4",
  "comment" : "rule comment",
  "id" : 123,
  "creation_date" : 5
}, {
  "updated_at" : 1611228121241,
  "name" : "Block Click Worms",
  "updated_by" : "John",
  "action" : "api.rule_action_type.rule_action_block",
  "rule" : "ClientIP == 1.2.3.4",
  "comment" : "rule comment",
  "id" : 123,
  "creation_date" : 5
} ],
"status" : "pending-dns-changes",
"enable_http_between_Imperva_and_origin" : "80"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1 - Unexpected error ApiResultListSites

```
post /api/prov/v1/sites/performance/advanced
```

Advanced caching settings (modifyAdvancedCachingSettings)
Use this operation to modify advanced caching settings.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

param (required)

Query Parameter

— Name of configuration parameter to set.
Possible values for param and value parameters:
async_validation Sets Async validation. Pass "true" or "false" in the value parameter.minify_javascript Sets the Minify JS. Pass "true" or "false" in the value parameter.minify_css Sets the Minify CSS. Pass "true" or "false" in the value parameter.minify_static_html Sets Minify static HTML. Pass "true" or "false" in the value parameter.compress_jpeg Sets the Compress JPEG. Pass "true" or "false" in the value parameter.progressive_image_rendering Sets the Progressive Image rendering flag. Pass "true" or "false" in the value parameter.aggressive_compression Sets the Aggressive compression rendering flag. Pass "true" or "false" in the value parameter.compress_png Sets the Compress PNG flag. Pass "true" or "false" in the value parameter.on_the_fly_compression "On the fly" Compression. Pass "true" or "false" in the value parameter.tcp_pre_pooling TCP Pre-Pooling. Pass "true" or "false" in the value parameter.comply_no_cache Comply with no-cache and max-age directives in client requests. Pass "true" or "false" in the value parameter.comply_vary Comply with the "Vary" header. Pass "true" or "false" in the value parameter.use_shortest_caching Use shortest caching duration in case of conflicts. Pass "true" or "false" in the value parameter.prefer_last_modified Prefer 'last modified' over eTag. Pass "true" or "false" in the value parameter.disable_client_side_caching Disable client side caching. Pass "true" or "false" in the value parameter.cache_300x Cache 300X responses. Pass "true" or "false" in the value parameter.unite_naked_full_cache Use the same cache for full and naked domains. For example, use the same cached resource for and a.cache_empty_responses Cache responses that don't have a message body.cache_http_10_responses Cache HTTP 1.0 type responses that don't include the Content-Length header or chunking. Pass "true" or "false" in the value parameter.send_age_header Send "Cache-Control: max-age" and "Age" headers. Pass "true" or "false" in the value parameter.support_non_sni_clients Enable or disable the support for Non-SNI clients for TLS connections between clients and Imperva. Pass "true" or "false" in the value parameter.origin_connection_reuse Requests from multiple client connections may be transmitted through a single TCP connection to the origin, while requests from a single client connection may be distributed across multiple TCP connections to the origin. This option disables that behavior.. Pass "true" or "false" in the value

parameter.redirect_http_to_https Redirect HTTP requests to HTTPS requests by sending an HTTP 301 response.redirect_naked_domain_to_full Redirect requests from your website's naked domain to its full domain by sending an HTTP 301 response.http_2 Enables supporting browsers to take advantage of the performance enhancements provided by HTTP/2 for your website. Non-supporting browsers can connect via HTTP/1.0 or HTTP/1.1. HTTP/2 support requires that SSL is configured for your website. Pass "true" or "false" in the value parameter

value (required)
Query Parameter
— According to the param value.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
5 - Operation unavailable
[ApiResult](#)

```
post /api/prov/v1/sites/performance/cache404/modify
```

Modify cache 404 settings (modifyCache404Settings)
Use this operation to modify the caching settings of 404 responses for a site.

Query parameters

site_id (required)
Query Parameter

— Numeric identifier of the site to operate on.
enable (required)
 Query Parameter
 — Pass 'true' to cache 404 responses, 'false' to disable the option.
time (optional)
 Query Parameter
 — A positive number representing the amount of time to cache 404 responses. Default value: 10
time_unit (optional)
 Query Parameter
 — Unit of time for caching 404 responses. One of MINUTES, HOURS, DAYS, WEEKS. Default value: HOURS

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [ApiResult](#)

```
post /api/prov/v1/sites/performance/purge
```

Purge resources (modifyPurgeSettings)
 Use this operation to purge site resources.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

`resource_url` (required)

Query Parameter

— Comma separated list of URLs where the resource is located.

`resource_pattern` (required)

Query Parameter

— Comma separated list of pattern. One of: contains | equals | prefix | suffix | not_equals | not_contains |

not_prefix | not_suffix

`should_purge_all_site_resources` (optional)

Query Parameter

— Should purge all cached resources on site.
Possible values:
If the parameter does not exist, is null, or an empty string, it is ignored and only specific resources defined by the `resource_pattern` and `resource_url` parameters are purged.
`true` or `TRUE`: All site resources are purged.
`false` or `FALSE`: Nothing is done.
Any other string: An error is returned.

Return type

`ApiResult`

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
3015 - Internal error
[ApiResult](#)

```
post /api/prov/v1/sites/performance/response-headers
```

Modify cached response headers (modifyResponseHeaderSettings)

Use this operation to modify cached response headers.

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on.

`cache_headers` (optional)

Query Parameter

— Comma separated list of header names to be cached

`cache_all_headers` (optional)

Query Parameter

— Cache all response headers. Pass "true" or "false" in the value parameter. Cannot be selected together with `cache_headers`. Default:false

Return type

`ApiResult`

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed `ApiResult`

```
post /api/prov/v1/sites/performance/rewrite-port/modify
```

Modify rewrite port (modifyRewritePorts)

Use this operation to rewrite the port number used to access the origin server.

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on

`rewrite_port_enabled` (required)

Query Parameter

— Boolean value to indicate whether the default non-SSL port should be rewritten or not

`port` (optional)

Query Parameter

— The port number. If empty, rewrite port will be removed

`rewrite_ssl_port_enabled` (required)

Query Parameter

— Boolean value to indicate whether the default SSL port should be rewritten or not

`ssl_port` (optional)

Query Parameter

— The port number to rewrite default SSL port to

Return type

`ApiResult`

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
`ApiResult`

```
post /api/prov/v1/sites/configure/allowlists
```

Modify allowlists configuration (modifySiteAllowListsConfiguration)

Use this operation to set allowlists to security rules or ACLs. To update an existing allowlist, send its ID in the id parameter. If the id parameter does not exist a new allowlist will be created.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body string (optional)

Body Parameter

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

rule_id (required)

Query Parameter

— The id of the rule (either a security or an acl rule), e.g api.threats.bot_access_control. The following WAF rules should be updated via Policy WAF rules, api.threats.sql_injection, api.threats.cross_site_scripting, api.threats.illegal_resource_access and api.threats.remote_file_inclusion

allowlist_id (required)

Query Parameter

— The id (an integer) of the allowlist to be set. This field is optional - in case no id is supplied, a new allowlist will be created.

delete_allowlist (optional)

Query Parameter

— An optional boolean parameter. If it is set to "true" and a allowlist id is sent, the allowlist will be deleted.

urls (optional)

Query Parameter

— A comma separated list of resource paths. For example, /home and /admin/index.html are resource paths, while http://www.example.com/home is not. Each URL should be encoded separately using percent encoding as specified by RFC 3986 (http://tools.ietf.org/html/rfc3986#section-2.1). An empty URL list will remove all URLs.

countries (optional)

Query Parameter

— A comma separated list of country codes.

continents (optional)

Query Parameter

— A comma separated list of continent codes.

ips (optional)

Query Parameter

— A comma separated list of IPs or IP ranges, e.g: 192.168.1.1, 192.168.1.1-192.168.1.100 or 192.168.1.1/24

client_app_types (optional)

Query Parameter

— A comma separated list of client application types

client_apps (optional)

Query Parameter

— A comma separated list of client application IDs.

parameters (optional)

Query Parameter

— A comma separated list of encoded parameters.

user_agents (optional)

Query Parameter

— A comma separated list of encoded user agents.

exception_id_only (optional)

Query Parameter

— Return only the new/edited exception id.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input. [inline_response_200_16](#)

```
post /api/prov/v1/sites/configure
```

Modify site configuration (modifySiteConfiguration)

Use this operation to change one of the basic configuration settings of the site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

param (required)

Query Parameter

— Name of configuration parameter to set.
Parameter values:
active Whether the site is active or bypassed by the Imperva network. One of: active | bypass.site_ip Comma separated list of IPs. For example: 8.8.8.8,1.2.2.2domain_validation Sets the domain validation method that will be used to generate an SSL certificate. One of: email | html | dns | cname
One-step onboarding: After adding a site and configuring your traffic to point to Imperva, use the html option to automatically add SSL support. Certificate creation takes approximately 5 minutes. During this time no traffic will reach the origin

server.
Note: When running domain validation on a site, you may see the following error message in the API response: Internal error - "Add site operation hasn't finished";
After running the add site process, it may take several minutes for the database to finish updating. During this time, attempts to further configure the site are blocked.
In some cases, the database is not updated even after the add site process is complete.
If the issue does not resolve after a few minutes, contact Support.approver Sets the approver e-mail address that will be used to perform SSL domain validation.ignore_ssl Sets the ignore SSL flag (if the site is in pending-select-approver state). Pass "true" in the value parameter.acceleration_level Sets the acceleration level of the site, one of: none | standard | aggressive. It is advised to use the newer Modify caching mode API call instead, as it provides enhanced functionality.seal_location Sets the seal location, e.g. "api.seal_location.bottom_right".domain_redirect_to_full Sets the redirect naked to full flag. Pass "true" in the value parameter.remove_ssl Sets the remove SSL from site flag. Pass "true" in the value parameter.ref_id Sets the Reference ID, a free-text field that enables you to add a unique identifier to correlate an object in our service, such as a protected website, with an object on the customer side.naked_domain_san Use this option to determine if the naked domain SAN will be added to the SSL certificate for www site. Will take effect in the next renewal.wildcard_san Use this option to determine if the wildcard SAN or the full domain SAN is added to the Imperva SSL certificate for site. Will take effect in the next renewal.set_cookies_without_domain Use this option to determine if to set site cookies without domain.restricted_cname_reuse Use this option to determine if legitimate traffic for all verified domains in the table is automatically allowed.request_body_timeouts Use this option to override default mitigation settings for slow HTTP attacks.Note: Send value in the format of {"methods": [method name, method name, ...], "interval": integer, "byteCount": integer}. For example: {"methods": [HTTP_POST, HTTP_GET], "interval": 30, "byteCount": 20}. Each post of the API overwrites the custom configuration. To delete the whole custom configuration, send {} as the value. Possible values for method: HTTP_POST, HTTP_GET, HTTP_PUT, HTTP_RPC_IN_DATA, HTTP_RPC_OUT_DATA

value (required)

Query Parameter

— According to the param value.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
6001 - Invalid configuration parameter name
6002 - Invalid configuration parameter value
1 - Unexpected error
9414 - Feature not

permitted inline_response_200_16

```
post /api/prov/v1/sites/performance/error-page/modify
```

Modify error page (modifySiteErrorPageTemplate)

Use this operation to set a custom error page for a given site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

error_page_template (required)

Query Parameter

— The error page html template. \$TITLE\$ and \$BODY\$ placeholders are required.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
ApiResult

```
post /api/prov/v1/sites/setlog
```

Modify site logs level (modifySiteLogLevel)
Use this operation to change the site log configuration.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

log_level (required)

Query Parameter

— Available only for customers that purchased the Logs Integration SKU. Sets the log reporting level for the site.
Possible values: full, security, none, default

logs_account_id (optional)

Query Parameter

— Available only for customers that purchased the Logs Integration SKU. Numeric identifier of the account that purchased the logs integration SKU and which collects the logs.
If not specified, operation will be performed on the account identified by the authentication parameters

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
6002 - Invalid configuration parameter name
6001 - Invalid configuration parameter name
9415 - Operation not allowed [ApiResult](#)

```
post /api/prov/v1/sites/configure/security
```

Modify site security configuration (modifySiteSecurityConfiguration)

Use this operation to change the security configuration of a site. To modify the configuration for a specific rule, additional parameters may be required, as documented below.

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on

`rule_id` (required)

Query Parameter

— ID of the security rule to change.
Values for the `rule_id`

parameter:
api.threats.bot_access_controlapi.threats.sql_injectionapi.threats.cross_site_scripting

`block_bad_bots` (optional)

Query Parameter

— Whether or not to block bad bots. Possible values: true, false

`challenge_suspected_bots` (optional)

Query Parameter

— Whether or not to send a challenge to clients that are suspected to be bad bots (CAPTCHA for example).

Possible values: true, false

`activation_mode` (optional)

Query Parameter

— Possible values: api.threats.ddos.activation_mode.off, api.threats.ddos.activation_mode.auto, api.threats.ddos.activation_mode.on,

api.threats.ddos.activation_mode.adaptive
api.threats.ddos.activation_mode.off Security measures are disabled even if site is under a DDoS attackapi.threats.ddos.activation_mode.auto Security measures will be activated automatically when the system suspects site is under a DDoS

attackapi.threats.ddos.activation_mode.on Security measures are enabled even if site is not under a DDoS attackapi.threats.ddos.activation_mode.adaptive Security measures are enabled with an adaptive threshold based on the website's trafficThe syntax is as follows:<rule_id>.activation_mode.<value> For example, for 'off', use

'activation_mode=api.threats.ddos.activation_mode.off.
Note: This parameter is relevant and required for a DDoS rule only -- where rule_id=api.threats.ddos.

`security_rule_action` (optional)

Query Parameter

— The action that should be taken when a threat is detected, for example:
api.threats.action.block_ip.

Different actions are allowed per different threats, e.g. backdoors may only be quarantined, ignored, or trigger an alert.
Values for the `security_rule_action` parameter:
api.threats.action.disabled Threat is not blocked, site owner is not notified.api.threats.action.alert Threat is not blocked, site owner is notified.api.threats.action.block_request Threat blocked by stopping the request, site owner is notified.api.threats.action.block_user Threat blocked by stopping the request. Additional requests by the client application will be automatically blocked for a duration of several minutes. Site owner is notified.api.threats.action.block_ip Threat blocked by stopping the request. Additional requests from the same IP addresses will be automatically blocked for a duration of several minutes. Site owner is notified.api.threats.action.quarantine_url Relevant only for Backdoor Protect. When detecting a backdoor, additional requests to the URL of the backdoor will be automatically blocked. Site owner is notified.

`quarantined_urls` (optional)

Query Parameter

— Removes quarantined URLs from the backdoor protection list, as defined in the Cloud Security Console Website Settings > WAF Settings > Backdoor Protect.
To remove a URL from the backdoor protection list, use the following parameters with the specified values:
quarantined_urls: <URL full path>
rule_id: api.threats.backdoor
security_rule_action: api.threats.action.quarantine_url

`ddos_traffic_threshold` (optional)

Query Parameter

— Consider site to be under DDoS if the request rate is above this threshold.
Allowed values: 10-10000 requests per second. format: int64

`unknown_clients_challenge` (optional)

Query Parameter

— Defines a method used for challenging suspicious bots. Possible values: none, cookies, javascript, captcha.
This parameter is relevant for a DDoS rule only.

block_non_essential_bots (optional)

Query Parameter

— If non-essential bots should be blocked or not. Possible values: true, false. This parameter is relevant for a DDoS rule only.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9414 - Feature not permitted
9415 - Operation not allowed
2 - Invalid input [inline_response_200_16](#)

```
post /api/prov/v1/sites/tls
```

Set support for all TLS versions (modifySiteSupportDeprecatedTLS)

Use this operation to support all TLS versions for the site for connectivity between clients (visitors) and the Imperva service. To remain PCI-compliant, do not enable this option.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

support_all_tls_versions (required)

Query Parameter

— Support all TLS versions. Default value: false

Return type

[inline_response_200_21](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 5 - Operation unavailable
 9415 - Operation not allowed
 1 - Unexpected error [inline_response_200_21](#)

```
post /api/prov/v1/sites/performance/stale-content
```

Modify stale content settings (modifyStaleContent)

When Imperva can't connect to the origin server, serve stale content instead of displaying an error to end users for the specified amount of time. Expired resources are returned from cache, and refreshed asynchronously in the background.

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on

`serve_stale_content` (required)

Query Parameter

— Pass **true** to serve stale content, **false** to disable the option.

`stale_content_mode` (required)

Query Parameter

— Pass **ADAPTIVE** to use Imperva's algorithm, or **CUSTOM** to specify an amount of time. When using **CUSTOM**, you must specify the time and `time_unit` parameters.

`time` (optional)

Query Parameter

— A positive number representing the amount of time to serve stale content.

`time_unit` (optional)

Query Parameter

— Stale content time unit. One of SECONDS, MINUTES, HOURS.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed
5 - Operation unavailable [ApiResult](#)

```
post /api/prov/v1/sites/performance/tag-response
```

Tag the response according to the value of a header (modifyTagResponseHeader)
Specify which origin response header contains the cache tags in your resources.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

header (required)

Query Parameter

— Specify which origin response header contains the cache tags in your resources. default: "".

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [ApiResult](#)

```
post /api/prov/v1/sites/moveSite
```

Move site (moveSite)

Use this operation to move a site from its account to another account.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to move format: int64

destination_account_id (required)

Query Parameter

— The numeric identifier of the account which the site will be moved to format: int64

Return type

[inline_response_200_22](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9415 - Operation not allowed [inline_response_200_22](#)

```
post /api/prov/v1/sites/hostname/purge
```

Purge hostname from cache (purgeHostname)

Use this operation to purge the hostname from the cache. This API is for customers who use the same CNAME provided by Imperva for multiple hostnames and would like to change the CNAME for a particular hostname. Purging the hostname is required for the CNAME change to take effect.

Query parameters

host_name (optional)

Query Parameter

— The hostname to purge from the cache

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
3015 - Internal error ApiResult

```
post /api/prov/v1/sites/cache/purge
```

Purge site cache (purgeSiteCache)

Use this operation to purge all cached content on our proxy servers for a specific site.

Our Proxy servers keep cached content of your sites in order to accelerate page load times for your users.

When you want this cached content to be refreshed (for example, after making adjustments in your site) you can use this API call.

In order to purge the entire cached content for this site just use the API call with no parameters.

If you want to purge a specific resource add the resource name as parameter.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

purge_pattern (optional)

Query Parameter

— The pattern of the resource to be purged from the cache. For example:
Resource_name - Resources that contain Resource_name will be purged^Resource_name - Resources that start with Resource_name will be purgedResource_name\$ - Resources that end with Resource_name will be purged.

purge_tag_names (optional)

Query Parameter

— A comma separated list of tag names to purge.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
5010 - Pattern invalid
9413 - Unknown/unauthorized site_id.
9415 - Operation not allowed [ApiResult](#)

```
put /api/prov/v3/sites/{extSiteId}/data-centers-configuration
```

set site's data centers' configuration (putDataCentersConfiguration)
Use this operation to configure site's data centers and all their servers

Path parameters

extSiteId (required)
Path Parameter
— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DataCentersConfigurationDTO (required)
Body Parameter
— JSON body. Schema is identical to the response.

Return type

[DataCentersConfigurationDTO](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lbAlgorithm" : "GEO_PREFERRED",
    "dataCenterMode" : "MULTIPLE_DC",
    "kickStartPass" : "kickstart-pass",
    "kickStartURL" : "https://www.example.com:443/kickStart",
    "isPersistent" : false,
    "dataCenters" : [ {
```

```

"lbAlgorithm" : "WEIGHTED",
"isContent" : true,
"weight" : 40,
"isRestOfTheWorld" : true,
"isActive" : false,
"geoLocations" : [ "AFRICA", "AFRICA" ],
"ipMode" : "MULTIPLE_IP",
"servers" : [ {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
}, {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
} ],
"originPop" : "lax",
"isEnabled" : false,
"name" : "London DC",
"id" : 7543,
"webServersPerServer" : 5
}, {
    "lbAlgorithm" : "WEIGHTED",
    "isContent" : true,
    "weight" : 40,
    "isRestOfTheWorld" : true,
    "isActive" : false,
    "geoLocations" : [ "AFRICA", "AFRICA" ],
    "ipMode" : "MULTIPLE_IP",
    "servers" : [ {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
    }, {
        "serverMode" : "ACTIVE",
        "address" : "1.2.3.4",
        "isEnabled" : false,
        "weight" : 70,
        "id" : 7543
    } ],
    "originPop" : "lax",
    "isEnabled" : false,
    "name" : "London DC",
    "id" : 7543,
    "webServersPerServer" : 5
}, {
    "kickStartUser" : "kickstart-user",
    "minAvailableServersForDataCenterUp" : 3,
    "failOverRequiredMonitors" : "MANY"
}, {
    "lbAlgorithm" : "GEO_PREFERRED",
    "dataCenterMode" : "MULTIPLE_DC",
    "kickStartPass" : "kickstart-pass",
}

```

```

"kickStartURL" : "https://www.example.com:443/kickStart",
"isPersistent" : false,
"dataCenters" : [ {
  "lbAlgorithm" : "WEIGHTED",
  "isContent" : true,
  "weight" : 40,
  "isRestOfTheWorld" : true,
  "isActive" : false,
  "geoLocations" : [ "AFRICA", "AFRICA" ],
  "ipMode" : "MULTIPLE_IP",
  "servers" : [ {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
  }, {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
  } ],
  "originPop" : "lax",
  "isEnabled" : false,
  "name" : "London DC",
  "id" : 7543,
  "webServersPerServer" : 5
}, {
  "lbAlgorithm" : "WEIGHTED",
  "isContent" : true,
  "weight" : 40,
  "isRestOfTheWorld" : true,
  "isActive" : false,
  "geoLocations" : [ "AFRICA", "AFRICA" ],
  "ipMode" : "MULTIPLE_IP",
  "servers" : [ {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
  }, {
    "serverMode" : "ACTIVE",
    "address" : "1.2.3.4",
    "isEnabled" : false,
    "weight" : 70,
    "id" : 7543
  } ],
  "originPop" : "lax",
  "isEnabled" : false,
  "name" : "London DC",
  "id" : 7543,
  "webServersPerServer" : 5
} ],
"kickStartUser" : "kickstart-user",
"minAvailableServersForDataCenterUp" : 3,
"failOverRequiredMonitors" : "MANY"
} ]

```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DataCentersConfigurationDTO

401

Unauthorized. E.g. Wrong API key, locked user [ApiErrorResponse](#)

403

Forbidden. E.g. Missing abilities [ApiErrorResponse](#)

404

Not Found. E.g. Site doesn't exist or belongs to other tenant [ApiErrorResponse](#)

406

Bad client request. Actually, HTTP 400 is more appropriate here [ApiErrorResponse](#)

500

Server Error [ApiErrorResponse](#)

```
put /api/prov/v3/sites/{extSiteId}/delivery-rules-configuration
```

Set site's delivery rules and priorities for a specific rule category. (`putDeliveryRulesConfiguration`)
Use this operation to set all delivery rules for a specific category. The rules are prioritized by order of appearance.

Notes:

- This API replaces all rules within the specified category, so existing rules that are not specified in the request will be deleted.
- When using this resource, the rule names within each category must be unique. When multiple rules have the same name, the update would fail with an error message specifying the index of the offending rules.

Path parameters

extSiteId (required)
 Path Parameter
 — Numeric identifier of the site to operate on. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DeliveryRulesListDTO (required)
 Body Parameter
 — JSON body. Schema is identical to the response.
 example: {

```

    "summary" : "REDIRECT category",
    "description" : "Supported actions:<br/> <b>RULE_ACTION_REDIRECT</b> (RedirectRuleDTO)",
    "value" : [
        "data" : [ {
            "filter" : "ASN == 1",
            "from" : "/1",
            "to" : "/2",
            "response_code" : 302,
            "rule_name" : "New delivery rule",
            "action" : "RULE_ACTION_REDIRECT",
            "enabled" : true
        } ]
    }
}
```

Query parameters

category (required)
 Query Parameter
 — Rules category. Possible values:
 REDIRECT - Redirect requests with 30X response.

 SIMPLIFIED_REDIRECT - Redirect requests with 30X response. (static redirect, doesn't support condition)
 REWRITE - Modify, add, and remove different request attributes such as URL, headers and cookies.
 REWRITE_RESPONSE - Modify, add, and remove different response attributes such as headers, status code and error responses.
 FORWARD - Forward the request to a specific data-center or port.

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

Example data

Content-Type: Supported actions:

RULE_ACTION_FORWARD_TO_PORT (ForwardToPortRuleDTO),
RULE_ACTION_FORWARD_TO_DC (ForwardToDcRuleDTO)

```
{"data": [{"filter": "ASN == 1", "dc_id": 1234, "rule_name": "New delivery rule", "action": "RULE_ACTION_FORWARD_TO_DC", "enabled": true}, {"filter": "ASN == 1", "port_forwarding_context": "[header/port]", "port_forwarding_value": "1234", "rule_name": "New delivery rule", "action": "RULE_ACTION_FORWARD_TO_PORT", "enabled": true}]} 
```

Example data

Content-Type: Supported actions:

RULE_ACTION_REDIRECT (RedirectRuleDTO)

```
{"data": [{"filter": "ASN == 1", "from": "/1", "to": "/2", "response_code": 302, "rule_name": "New delivery rule", "action": "RULE_ACTION_REDIRECT", "enabled": true}]} 
```

Example data

Content-Type: Supported actions:

RULE_ACTION_SIMPLIFIED_REDIRECT (SimplifiedRedirectRuleDTO)

```
{"data": [{"from": "/1", "to": "/2", "response_code": 302, "rule_name": "New delivery rule", "action": "RULE_ACTION_REDIRECT", "enabled": true}]} 
```

Example data

Content-Type: Supported actions:

RULE_ACTION_REWRITE_COOKIE (RewriteRequestCookieRuleDTO),
RULE_ACTION_REWRITE_HEADER (RewriteRequestHeaderRuleDTO),
RULE_ACTION_REWRITE_URL (RewriteRequestUrlRuleDTO),
RULE_ACTION_DELETE_HEADER (RewriteRequestDeleteHeaderRuleDTO),
RULE_ACTION_DELETE_COOKIE (RewriteRequestDeleteCookieRuleDTO)

```
{"data": [{"filter": "ASN == 1", "from": "cookie1", "to": "cookie2", "cookie_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_COOKIE", "enabled": true}, {"filter": "ASN == 1", "from": "header1", "to": "header2", "header_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_HEADER", "enabled": true}, {"filter": "ASN == 1", "from": "/1", "to": "/2", "rule_name": "New delivery rule", "action": "RULE_ACTION_REWRITE_URL", "enabled": true}, {"filter": "ASN == 1", "from": "header1", "to": "header2", "header_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_HEADER", "enabled": true}, {"filter": "ASN == 1", "from": "cookie1", "to": "cookie2", "cookie_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_COOKIE", "enabled": true}]} 
```

```
== 1", "header_name": "abc", "multiple_headers_deletion": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_HEADER", "enabled": true}, {"filter": "ASN == 1", "cookie_name": "abc", "rule_name": "New delivery rule", "action": "RULE_ACTION_DELETE_COOKIE", "enabled": true}]]}
```

Example data

Content-Type: Supported actions:

RULE_ACTION_RESPONSE_REWRITE_HEADER (RewriteResponseHeaderRuleDTO),
RULE_ACTION_RESPONSE_DELETE_HEADER (RewriteResponseDeleteHeaderRuleDTO),
RULE_ACTION_RESPONSE_RESPONSE_CODE (RewriteResponseCodeRuleDTO),
RULE_ACTION_CUSTOM_ERROR_RESPONSE (RewriteResponseCustomErrorRuleDTO)

```
{"data": [{"filter": "ASN == 1", "header_name": "abc", "multiple_headers_deletion": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_RESPONSE_DELETE_HEADER", "enabled": true}, {"filter": "ASN == 1", "from": "header1", "to": "header2", "header_name": "abc", "rewrite_existing": true, "add_if_missing": false, "rule_name": "New delivery rule", "action": "RULE_ACTION_RESPONSE_RESPONSE_CODE", "enabled": true}, {"filter": "ASN == 1", "error_response_format": "[JSON|XML]", "error_response_data": "<?xml version='1.0' encoding='UTF-8'?>", "error_type": "error.type.all", "response_code": 400, "rule_name": "New delivery rule", "action": "RULE_ACTION_CUSTOM_ERROR_RESPONSE", "enabled": true}]]}
```

401

Unauthorized [ApiErrorResponse](#)

404

Not Found [ApiErrorResponse](#)

406

Not Acceptable [ApiErrorResponse](#)

500

Server Error [ApiErrorResponse](#)

```
post /api/prov/v1/sites/customCertificate/remove
```

Remove custom certificate (removeCustomCertificate)
 Use this operation to remove a custom certificate.

Query parameters

site_id (optional)

Query Parameter

— Numeric identifier of the site to operate on format: int64

auth_type (optional)

Query Parameter

— The authentication type of the certificate (RSA or ECC). Optional. If not provided, then RSA will be assumed.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
4205 - Site does not have SSL
9414 - Feature not permitted
9414 - Feature not permitted</br>3015 - Internal error ApiResult

```
post /api/prov/v1/sites/dataCenters/resume
```

Resume traffic to your active data centers (resumeTrafficToActiveDCs)

When at least one active data center is back up, you have to manually reroute your traffic back to the active data center.

Traffic does not revert automatically to your active data centers.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 -Unknown/unauthorized site_id [ApiResult](#)

```
post /api/prov/v1/sites/performance/cache-mode
```

Modify caching mode (setCachingMode)

Use this operation to edit basic site caching settings.

Query parameters

cache_mode (required)

Query Parameter

— Possible

values:
disablecustom_cache_rules_onlystatic_onlystatic_and_dynamicaggressive

value: static_only

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

dynamic_cache_duration (optional)

Query Parameter

— Profile dynamic pages and cache duration. Pass a number followed by '_' and one of: hr | min | sec | days |

weeks.</br>Default: 5_min

aggressive_cache_duration (optional)

Query Parameter

— Cache resource duration. Pass a number followed by '_' and one of: hr | min | sec | days | weeks
Default: 1_hr

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id [ApiResult](#)

```
post /api/prov/v1/sites/datacenter/origin-pop/modify
```

Set data center origin PoP (setDataCenterOriginPoP)

Set an origin PoP for a given data center.

Query parameters

dc_id (required)

Query Parameter

— Numeric identifier of the data center to operate on. format: int64

origin_pop (optional)

Query Parameter

— The ID of the PoP that serves as an access point between Imperva and the customer's origin server. For example: "lax", for Los Angeles.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
405 - Api is disabled</br>2 - invalid data center
5 - Cant set Origin PoP for data center [ApiResult](#)

```
post /api/prov/v1/sites/data-privacy/region-change
```

Set site data storage region (setDataRegion)
Use this operation to set the site data region.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

data_storage_region (required)

Query Parameter

— The data region to use.

Return type

[inline_response_200_18](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9415 - Operation not allowed
[inline_response_200_18](#)

```
post /api/prov/v1/sites/configure/htmlInjections
```

Add, replace or remove a HTML injection rule (setHtmlInjectionRule)

Use this operation to add a new HTML injection rule, or to replace or remove an existing rule.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

url (required)

Query Parameter

— The URL where the content is injected

url_pattern (required)

Query Parameter

— The url pattern. One of: contains | not_contains | equals | not_equals | prefix | suffix | not_prefix | not_suffix

location (required)

Query Parameter

— The location of the injection inside the URL ('head' or 'body_end')

content (optional)

Query Parameter

— The injected HTML snippet, Base64-encoded

delete_content (optional)

Query Parameter

— Whether or not to delete existing HTML content.
Possible values: true/false

Return type

[inline_response_200_19](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input [inline_response_200_19](#)

```
post /api/prov/v1/sites/data-privacy/override-by-geo
```

Set site regions by origin geolocation (setOverrideSiteRegionsByGeo)

Use this operation to set the data storage region for each new site based on the geolocation of the origin server.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

override_site_regions_by_geo (required)

Query Parameter

— A boolean parameter. If it is set to "true", the data storage region for each new site will be based on the geolocation of the origin server.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
```

```

    "key" : { }
}
]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9415 - Operation not allowed ApiResult

```
post /api/prov/v1/sites/incapRules/priority/set
```

Set rule priority (setPriority)

Use this operation to change delivery rule's priority.

Query parameters

rule_id (required)

Query Parameter

— Rule ID format: int64

priority (required)

Query Parameter

— New priority for the selected rule format: int32

Return type

[SetPriorityResponse](#)

Example data

Content-Type: application/json

```
{
  "res" : "0",
  "status" : "ok"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 9413 - Unknown/unauthorized site_id
 2 - Invalid input
SetPriorityResponse

```
post /api/prov/v1/sites/performance/secure-resources
```

Modify secure resources mode (setSecureResourcesMode)
 Use this operation to modify the Secure Resources mode for a site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

secured_resources_mode (required)

Query Parameter

— **do_not_cache** - Do not cache HTTPS resources
defaults - Use default HTTPS caching.

Do not cache HTML pages
defaults_with_html - Use default HTTPS caching. Also cache HTML pages
general - Cache HTTPS according to general caching settings

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9413 - Unknown/unauthorized site_id
9415 - Operation not allowed [ApiResult](#)

```
post /api/prov/v1/sites/status
```

Get site status (siteStatus)

Use this operation to get the status of a site.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on

tests (optional)

Query Parameter

— List of tests to run on site before returning its status.
A comma separated list of one of: domain_validation, services, dns
Values for the stats parameters:
domain_validation Runs the domain validation test on the specified site. This test will check for HTML meta tag or DNS records, according to the selected domain validation method.services Runs the services test on the specified site. This test will check the availability of HTTP and HTTPS connections on the site.dns Runs the DNS test on the specified site. This test will check whether the site owner performed the DNS changes required in order to protect the site.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3001 - Domain invalid
6002 - Invalid configuration parameter value
9415 - Operation not allowed [inline_response_200_16](#)

```
post /api/prov/v3/sites/{extSiteId}/settings/TLSConfiguration
```

Update website TLS configuration (updateTLSConfiguration)
Update the TLS configuration for a given website.

Path parameters

extSiteId (required)
Path Parameter
— The Imperva ID of the website to operate on. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **TLSConfigurationDto** (required)
Body Parameter
— JSON body. Schema is identical or semi identical to the response.

Return type

TLSConfigurationDto

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
      "subDomainsIncluded" : false,
      "preLoaded" : false
    }
  }, {
    "hstsConfiguration" : {
      "maxAge" : 7543,
      "isEnabled" : false,
      "subDomainsIncluded" : false,
      "preLoaded" : false
    }
  }
]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [TLSConfigurationDto](#)

401

Unauthorized [ApiErrorResponse](#)

404

Not Found [ApiErrorResponse](#)

406

Not Acceptable [ApiErrorResponse](#)

500

Server Error [ApiErrorResponse](#)

```
post /api/prov/v1/sites/customCertificate/upload
```

Upload custom certificate (uploadCustomCertificate)

Use this operation to upload a custom certificate for your site. The following SSL certificate file formats are supported: PFX, PEM, CER.

Query parameters

site_id (optional)

Query Parameter

— Numeric identifier of the site to operate on format: int64

certificate (required)

Query Parameter

— The certificate file in base64 format

private_key (optional)

Query Parameter

— The private key of the certificate in base64 format. Optional in case of PFX certificate file format

passphrase (optional)

Query Parameter

— The passphrase used to protect your SSL certificate

auth_type (optional)

Query Parameter

— The authentication type of the certificate (RSA or ECC). Optional. If not provided, then RSA will be assumed.

input_hash (optional)

Query Parameter

— optional parameter. usually a hash representation for the concatenation of all inputs

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

res - contains the specific error code:
2 - Invalid input
4205 - Site does not have SSL
9414 - Feature not permitted
9414 - Feature not permitted
3015 - Internal error [ApiResult](#)

Models

Methods

Table of Contents

1. [APIPaginationMetadata](#)
 2. [ApiError](#)
 3. [ApiErrorResponse](#)
 4. [ApiErrorSource](#)
 5. [ApiResult](#)
-

-
- 6. ApiResultAddCacheRule
 - 7. ApiResultDomainEmails
 - 8. ApiResultGetCacheMode
 - 9. ApiResultGetResponseHeaderSettings
 - 10. ApiResultGetRewritePorts
 - 11. ApiResultGetSecureResources
 - 12. ApiResultGetSiteXrayLink
 - 13. ApiResultGetTagResponseHeader
 - 14. ApiResultHtmlInjections
 - 15. ApiResultListSites
 - 16. ApiResultMoveSite
 - 17. ApiResultReport
 - 18. ApiResultSetDataRegion
 - 19. ApiResultSetSupportDeprecatedTLSForSite
 - 20. ApiResultSiteStatus
 - 21. BaseRuleDTO
 - 22. BaseRuleDtoExtended
 - 23. BotConfiguration
 - 24. BotsConfiguration
 - 25. BotsConfigurationDTO
 - 26. CaaComplianceCheckResult
 - 27. CreateNewCSRResponse
 - 28. CustomRuleResponse
 - 29. CustomRulesDTOSuccessResponse
 - 30. DataCenterConfiguration
 - 31. DataCenterResponse
 - 32. DataCenterServerConfiguration
 - 33. DataCentersConfiguration
 - 34. DataCentersConfigurationDTO
 - 35. DeleteCustomRuleResponse
 - 36. DeliveryRuleDTO
 - 37. DeliveryRulesListDTO
 - 38. DnsInstructionItem
 - 39. GetAdvancedCachingSettingsApiResult
 - 40. GetCache404SettingsApiResult
 - 41. GetStaleContentApiResult
 - 42. HSTSConfiguration
 - 43. HtmlInjectionItem
 - 44. IncapRuleApiResult
 - 45. IsCacheShieldEnabledApiResult
 - 46. ListCustomRulesResponse
 - 47. ListDataCenterResponse
 - 48. LoginProtectApiResult
-

```
49. PerformanceConfigurationApiResult
50. PopRttResponse
51. RecommendedPopsApiResult
52. RequestBodyTimeoutDTO
53. RewritePort
54. ServerOperationResponse
55. SetPriorityResponse
56. SiteCacheRuleResponse
57. SiteConfigurationWarning
58. SiteDualFactorSettings
59. TLSConfiguration
60. TLSConfigurationDto
61. customAreas
62. customAreasExceptions
63. inline_response_200
64. inline_response_200_1
65. inline_response_200_10
66. inline_response_200_11
67. inline_response_200_12
68. inline_response_200_13
69. inline_response_200_14
70. inline_response_200_15
71. inline_response_200_16
72. inline_response_200_17
73. inline_response_200_18
74. inline_response_200_19
75. inline_response_200_2
76. inline_response_200_20
77. inline_response_200_21
78. inline_response_200_22
79. inline_response_200_3
80. inline_response_200_4
81. inline_response_200_5
82. inline_response_200_6
83. inline_response_200_7
84. inline_response_200_8
85. inline_response_200_9
86. specific_users_list
```

API PaginationMetadata

totalPages (optional)

Integer

format: int32

totalElements (optional)

Long

format: int64

size (optional)

Integer

format: int32

page (optional)

Integer

format: int32

ApiError

id (optional)

String

Globally unique error id.

example: 01234567-0123-0123-0123456789ab

status (optional)

String

HTTP status code

example: 404

code (optional)

String

Error code

example: ERROR_2002

message (optional)

String

Detailed error message

example: Site 123456 not found

source (optional)

ApiErrorSource

title (optional)

String

Short error title

example: Domain exists for another site

detail (optional)

String

Detailed error description

example: The domain 'example.com' is already associated with another site.

ApiErrorResponse

errors (optional)

array[**ApiError**]

ApiErrorSource

Pointer to source of error

pointer (optional)

String

a JSON Pointer [RFC6901] to the erroneous JSON element in the request payload

example: \$.data[0].fieldName

parameter (optional)

String

The name of erroneous query/path parameter name

example: extSitId

ApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]

ApiResultAddCacheRule

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
rule_id (optional)
Long
format: int64
example: 10

ApiResultDomainEmails

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
domain_emails (optional)
array[Object]

ApiResultGetCacheMode

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
cache_mode (optional)
String
example: static_and_dynamic

ApiResultGetResponseHeaderSettings

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
enabled (optional)
Boolean
example: true
mode (optional)
String
example: CUSTOM
custom_headers (optional)
array[String]

ApiResultGetRewritePorts

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
port (optional)
RewritePort
ssl_port (optional)
RewritePort

ApiResultGetSecureResources

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
secured_resources_mode (optional)
String
example: do_not_cache (i.e. Do not cache HTTPS resources)

ApiResultGetSiteXrayLink

res (optional)
Integer
res - contains specific error code format: int32

example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
url (optional)
String
example: https://

ApiResultGetTagResponseHeader

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
header (optional)
String
example: h1

ApiResultHtmlInjections

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
html_injections (optional)
array[HtmlInjectionItem]

ApiResultListSites

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
ApiResultSiteStatus (optional)
array[ApiResultSiteStatus]

ApiResultMoveSite

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

status (optional)

String

Enum:

MOVED

PENDING_CA_APPROVAL

FAILED

ApiResultReport

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

format (optional)

String

Enum:

html

xml

amf

pdf

flash

json

mail

csv

statistics

syslog

example: pdf

report (optional)

String

example: JVBERi0xLjUNCiXvv73vv73vv73vv70NCjEgMCBvYmoNCjw8L1R5cGUvQ2F0YWxvZy9QYWdIcyAyIDA
gUi9MYW5nKGVuLVVT ...

ApiResultSetDataRegion

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

region (optional)

String

example: US

ApiResultSetSupportDeprecatedTLSForSite

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

support_all_tls_versions (optional)

Boolean

example: true

new_A_record (optional)

String

example: 1.2.3.4

additional_instructions (optional)

String

example: After the site is moved, update the site's 'A' records according to the information in Websites General Settings.

ApiResultSiteStatus

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

site_id (optional)

Long

format: int64

example: 10

statusEnum (optional)

String

Enum:

pending-txt-validation

pending-dns-changes

fully-configured

pending-select-approver

pending-certificate

unknown

example: pending-dns-changes

status (optional)

String

example: pending-dns-changes

domain (optional)

String

example: admin@example.com

account_id (optional)

```

Long
format: int64
example: 1
acceleration_level (optional)
String
example: advanced
acceleration_level_raw (optional)
String
example: none
site_creation_date (optional)
Long
format: int64
example: 1610396346000
ips (optional)
array[Object]
dns (optional)
array[DnsInstructionItem]
original_dns (optional)
array[DnsInstructionItem]
warnings (optional)
array[SiteConfigurationWarning]
active (optional)
String
Enum:
active
bypass
example: active
support_all_tls_versions (optional)
Boolean
example: true
use_wildcard_san_instead_of_full_domain_san (optional)
Boolean
example: true
add_naked_domain_san (optional)
Boolean
example: true
set_site_cookies_without_domain (optional)
Boolean
example: true
enable_http_between_Imperva_and_origin (optional)
String
example: 80
additionalErrors (optional)
array[Object]
display_name (optional)
String
example: loginprotectapi1610396334653.incaptest.info
security (optional)
array[map[String, Object]]
example: {"waf": {"rules": [{"id": "api.threats.bot_access_control", "name": "Bot Access Control", "block_bad_bots": true, "challenge_suspected_bots": true}, {"id": "api.threats.sql_injection", "name": "SQL Injection", "action": "api.threats.action.block_request", "action_text": "Block Request"}, {"id": "api.threats.cross_site_scripting", "name": "Cross Site Scripting (XSS)", "exceptions": [{"values": [{"urls": [{"value": "/gsddg", "pattern": "EQUALS"}]}, {"id": "api.rule_exception_type.url", "name": "URL"}], "id": 244711494}], "action": "api.threats.action.alert", "action_text": "Alert Only"}, {"id": "api.threats.illegal_resource_access", "name": "Illegal Resource Access", "action": "api.threats.action.block_user", "action_text": "Block User"}, {"id": "api.threats.ddos", "name": "DDoS", "activation_mode": "api.threats.ddos.activation_mode.off", "activation_mode_text": "Off", "ddos_traffic_threshold": "api.threats.ddos.ddos_trassic_threshold", "ddos_traffic_threshold_text": "750", "ddos_adaptive_threshold": "500", "ddos_adaptive_threshold_last_update_time": "1610396346000"}, {"id": "api.threats.backdoor", "name": "Backdoor Protect", "action": "api.threats.action.quarantine_url", "action_text": "Aut

```

o-Quarantine"}, {"action": "api.threats.action.block_ip", "action_text": "Block IP", "id": "api.threats.remote_file_inclusion", "name": "Remote File Inclusion"}], "acls": {"rules": [{"ips": "2.3.4.5"}, {"exceptions": [{"values": [{"id": "api.rule_exception_type.url"}, {"name": "URL"}, {"urls": [{"value": "/home", "pattern": "EQUALS"}]}]}]}], "id": 493271006}, "id": "api.acl.blacklisted_ips", "name": "Visitors from denylisted IPs"}]}
 ssl (optional)
 array[map[String, Object]]
 example: {"origin_server": {"detected": "true", "detectionStatus": "ok"} }
 siteDualFactorSettings (optional)
SiteDualFactorSettings
 requestBodyTimeouts (optional)
RequestBodyTimeoutDTO
 login_protect (optional)
LoginProtectApiResult
 performance_configuration (optional)
PerformanceConfigurationApiResult
 extended_ddos (optional)
Integer
 format: int32
 incap_rules (optional)
 array[IcapRuleApiResult]
 restricted_cname_reuse (optional)
Boolean
 example: true

BaseRuleDTO

rule_id (optional)
Long
 format: int64
 name (optional)
String
 action (optional)
String
 Enum:
 RULE_ACTION_NONE
 RULE_ACTION_EXCLUDE
 RULE_ACTION_NOP
 RULE_ACTION_SESSION_COUNTER_INC
 RULE_ACTION_SET_CAPTCHA_FAILED
 RULE_ACTION_SET_DUAL_FACTOR_AUTHENTICATION_FAILED
 RULE_ACTION_SKIP_TEST_COOKIES
 RULE_ACTION_NULL_ROUTE
 RULE_ACTION_TRANSPARENT_HTML_JS_FORCE
 RULE_ACTION_TRANSPARENT_HTML_JS_RELAXED
 RULE_ACTION_HIDDEN_ALERT
 RULE_ACTION_ALERT
 RULE_ACTION_QUARANTINE_URL
 RULE_ACTION_RETRY
 RULE_ACTION_INTRUSIVE_HTML
 RULE_ACTION_DDOS_ACTION
 RULE_ACTION_CAPTCHA
 RULE_ACTION_DUAL_FACTOR_AUTHENTICATE
 RULE_ACTION_BLOCK
 RULE_ACTION_BLOCK_USER
 RULE_ACTION_BLOCK_IP
 RULE_ACTION_BLOCK_IP.Aggressive
 RULE_ACTION_REDIRECT
 RULE_ACTION_REWRITE

```
RULE_ACTION_BYPASS_CACHE
RULE_ACTION_REWRITE_URL
RULE_ACTION_REWRITE_HEADER
RULE_ACTION_REWRITE_COOKIE
RULE_ACTION_DELETE
RULE_ACTION_DELETE_HEADER
RULE_ACTION_DELETE_COOKIE
RULE_ACTION_FORWARD_TO_DC
RULE_ACTION_RATE
RULE_ACTION_SIMPLIFIED_REDIRECT
RULE_ACTION_RESPONSE_DELETE_HEADER
RULE_ACTION_RESPONSE_REWRITE_HEADER
RULE_ACTION_CUSTOM_ERROR_RESPONSE
RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE
RULE_ACTION_FORWARD_REQUEST
RULE_ACTION_FORWARD_TO_PORT
RULE_ACTION_WAF_OVERRIDE
RULE_ACTION_MASK
enabled (optional)
Boolean
```

BaseRuleDtoExtended

rule (optional)
BaseRuleDTO
 site_id (optional)
Long
 format: int64
 account_id (optional)
Long
 format: int64

BotConfiguration

id
Long
 The ID number assigned to the bot, according to Imperva's client classification database. format: int64
 example: 6
 displayName (optional)
String
 The bot name and type, according to Imperva's client classification database.
 This field is relevant for response only
 example: Googlebot (Search Bot)

BotsConfiguration

canceledGoodBots (optional)
array[BotConfiguration]
 Bots that an account user has removed from the list of bots that Imperva allows to access your website by default.
 badBots (optional)
array[BotConfiguration]
 Bots that an account user has added to the list of bots that Imperva blocks by default.

BotsConfigurationDTO

data (optional)

array[BotsConfiguration]**CaaComplianceCheckResult**

res (optional)
Integer
format: int32
res_message (optional)
String
non_compliant_sans (optional)
array[Object]

CreateNewCSRResponse

csr_content (optional)
String
example: -----BEGIN CERTIFICATE REQUEST-----\nMIIC5DCCAcwCAQAwZ4xNTAzBgNVBAMTLGEucmV1c2VjdXN0b21jZXJ0aWZpY2F0\nZXdpdGhjc3J0ZXN0MzUzOTYuY29tMQwwCgYDVQQHEwNKRVlxCzAJBgNVBAYTAKIM\nMQswCQYDVQQIEwJJTDEQMA4GA1UEChMHaW1wZXJ2YTELMAkGA1UECxMCQ04xHjAclnBqkqhkiG9w0BCQEWd2Zvb0BpbXBlcZhLmNvbTCASlwDQYJKoZIhvcNAQEBBQADnggEPADCCAQoCggEBAMAHcUrB5rhio8jaAueo6rdpgW1SuscflK01xF5utOqrQ2\nSfD3IBaQcT6pf9fFT5zUcErXmCpjdbY42JmjiRvS04aKhI4pKydm17e5CSevSyM\n0gAYhUdQOgjpCY81/58RKwndG3diFbsdrGnDuKWf7kLmx/biK+3IIzSPF7JsQ1\nnDHZS9X1Sq3Hwk7GBwOLBIkqG6VXS3SMUReggW6VJhuCKIY+FPuT7Qr80fkvt8x\nnbCFle7gMF8v390Tc36FFXF7/J05m9aSgFLPRPsJ+UIRxvRXrnLNm+ycCcXvL5A\nngE50PJaCHJz4U45c9zSAKbrvGHKzZ6eWkdVCDfsCAwEAAaAAMA0GCSqGSIb3DQEBlCwUAA4IBAQAvRrtUP86IG3J+uYrtnvZzDGRue6elVwfDOKqrPBAX3fm+JnctZKC5\nnQVmLTofMKRyL/FsF3K4a9hf8pN5TjT2/LS7OvgOHOfQC0eZCcocRmz++MtUaQxsx\nn+WHiUkpgnXnH3KQhj3WzP6HJV/qjRzcRWBsHUhuE75/J0153RWEXQssC5y4t3hv\nlnynkT6BUkQDy8XdRA3kgahPd9Jnwx4be9pRuq7hw1JIA7jFqu4A/ZSoUAoCqgWlfD\nnXSt26/4tt4Dltt+G/SLGNPuhuc2z+VmGkDDrRm8SNfykEvHF1KkdYcSKgLH2+fg\nnICCHPIAljavOirG+cki5Ppc0M/Wmagl+\n-----END CERTIFICATE REQUEST-----\nstatus (optional)
String
example: ok
res (optional)
String
example: 0

CustomRuleResponse

rule_id (optional)
Long
format: int64
example: 43573
status (optional)
String
example: ok
res (optional)
Integer
format: int32
example: 0

CustomRulesDTOSuccessResponse

data (optional)
array[BaseRuleDtoExtended]
meta (optional)
APIPaginationMetadata

DataCenterConfiguration

name

String

Data center name

example: London DC

id (optional)

Long

Data center id format: int64

example: 7543

ipMode (optional)

String

Load-balancing mode.
Possible values:

- SINGLE_IP - Use it only when you need to support multiple ports. Allows a single active server listening on multiple ports, plus the option of a single standby server. Traffic is distributed across the server ports.
-
Note: The server address must be a valid IP address (i.e. not host/domain name).
-
SINGLE_IP is applicable only for datacenters. It may not be used when dataCenterMode = 'SINGLE_SERVER'.
- MULTIPLE_IP – Allows one or more origin servers having a single webserver and listening port per server. Traffic is distributed across servers.

Enum:

SINGLE_IP

MULTIPLE_IP

example: MULTIPLE_IP

webServersPerServer (optional)

Integer

When IP mode = SINGLE_IP, number of webservers per server. Each webserver listens to different port. E.g. when webServersPerServer = 5, HTTP traffic will use ports 80-84 while HTTPS traffic will use ports 443-447

format: int32

example: 5

lbAlgorithm (optional)

String

Specifies how to load balance between the servers of this data center

Enum:

LB_LEAST_PENDING_REQUESTS

LB_LEAST_OPEN_CONNECTIONS

LB_SOURCE_IP_HASH

RANDOM

WEIGHTED

example: WEIGHTED

weight (optional)

Integer

Weight in percentage. Mandatory if lbAlgorithm = WEIGHTED_LB. Then, total weights of all data centers must be equal to 100

format: int32

example: 40

isEnabled (optional)

Boolean

For each site, at least one data center must be enabled

example: false

isActive (optional)

Boolean

Specify false to define a standby datacenter. No more than one data center can be defined as standby. Failover to standby data center is performed only when no other active data center is available

example: false

isContent (optional)

Boolean

When true, this data center will only handle requests that were routed to it using application delivery forward rules.

If true, must be an active data center.

example: true

isRestOfTheWorld (optional)

Boolean

When global lbAlgorithm = GEO_PREFERRED or GEO_REQUIRED, exactly one data center must have isRestOfTheWorld = true. This data center will handle traffic from any region that is not assigned to a specific data center.

example: true

geoLocations (optional)

array[String]

Enum:

originPop (optional)

String

The ID of the PoP that serves as an access point between Imperva and the customer's origin server. For example: "lax", for Los Angeles. When not specified, all Imperva PoPs can send traffic to this data center. The list of available PoPs is documented at: <https://docs.imperva.com/bundle/cloud-application-security/page/more/pops.htm>

example: lax

servers (optional)

array[DataCenterServerConfiguration]

DataCenterResponse

datacenter_id (optional)

Integer

format: int32

example: 484377

status (optional)

String

example: ok

res (optional)

String

example: 0

DataCenterServerConfiguration

address

String

Server address as: host name, ipv4, or ipv6

example: 1.2.3.4

id (optional)

Long

Server id format: int64

example: 7543

isEnabled (optional)

Boolean

For each data center, at least one server must be enabled

example: false

serverMode (optional)

String

Single IP allows single active server plus optionally single standby server. Each server may have multiple web servers (listening to different port). Multiple IPs allow multiple servers having single web server and listening port per server.

Enum:

ACTIVE

STANDBY

weight (optional)

Integer

Weight in percentage. Mandatory when Data center's lbAlgorithm = WEIGHTED format: int32

example: 70

DataCentersConfiguration**IbAlgorithm** (optional)**String**

Specifies how to load balance between multiple data centers

Enum:

BEST_CONNECTION_TIME

GEO_PREFERRED

GEO_REQUIRED

WEIGHTED_LB

example: GEO_PREFERRED

failOverRequiredMonitors (optional)**String**

How many Imperva PoPs should assess Data Center as down before failover is performed. MANY means more than one. MOST means more than 50%.

Enum:

ONE

MANY

MOST

ALL

example: MANY

dataCenterMode (optional)**String**

SINGLE_SERVER does not allow load balancing. SINGLE_DC allows load balancing and/or failover between its servers. MULTIPLE_DC allows load balancing and/or failover between the data centers plus geo aware routing.

Enum:

SINGLE_SERVER

SINGLE_DC

MULTIPLE_DC

example: MULTIPLE_DC

minAvailableServersForDataCenterUp (optional)**Integer**

The minimal number of available data center's servers to consider that data center as UP format: int32

example: 3

kickStartURL (optional)**String**

The URL that will be sent to the standby server when Imperva performs failover based on our monitoring. Port must be specified, if protocol is https.

example: https://www.example.com:443/kickStart

kickStartUser (optional)**String**

The kickstart user, if kickstart URL is protected by user and password

example: kickstart-user

kickStartPass (optional)**String**

The kickstart password, if kickstart URL is protected by user and password

example: kickstart-pass

isPersistent (optional)**Boolean**

When true our proxy servers will maintain session stickiness to origin servers by a cookie

example: false

dataCenters (optional)[array\[DataCenterConfiguration\]](#)

DataCentersConfigurationDTO**data** (optional)[array\[DataCentersConfiguration\]](#)

DeleteCustomRuleResponse

status (optional)

String

example: ok

res (optional)

Integer

format: int32

example: 0

DeliveryRuleDTO

Delivery rule DTO

rule_name

String

The rule name

example: Custom rule 1

action

String

Rule action. Possible values: **RULE_ACTION_REDIRECT** Redirect the client to a different URL, responding with a 30X response.
RULE_ACTION_SIMPLIFIED_REDIRECT Redirect the client to a different URL, responding with a 30X response.
RULE_ACTION_REWRITE_URL Modify the path to which a specific request is targeted.
RULE_ACTION_REWRITE_HEADER Modify or add a request header before passing traffic to the origin

RULE_ACTION_REWRITE_COOKIE Modify or add cookies that are sent by the client to the origin server. The cookie name and value should be indicated.

RULE_ACTION_DELETE_HEADER Remove a specific request header, which means that it won't be sent to the origin server.
RULE_ACTION_DELETE_COOKIE Remove a specific cookie set on the client, which means that it won't be sent to the origin

RULE_ACTION_FORWARD_TO_DC Define the data center to which a specific request will be sent.
RULE_ACTION_FORWARD_TO_PORT Define the port to which a specific request will be sent.
RULE_ACTION_RESPONSE_REWRITE_HEADER Modify or add a header to the response received from the origin server.

RULE_ACTION_RESPONSE_DELETE_HEADER Remove a specific response header, which means that it won't be returned to the client.
RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE Modify the response code received from the origin server.
RULE_ACTION_CUSTOM_ERROR_RESPONSE Control the error response that is returned to the client when a request is blocked.

Enum:

RULE_ACTION_NONE**RULE_ACTION_EXCLUDE****RULE_ACTION_NOP****RULE_ACTION_SESSION_COUNTER_INC****RULE_ACTION_SET_CAPTCHA_FAILED****RULE_ACTION_SET_DUAL_FACTOR_AUTHENTICATION_FAILED****RULE_ACTION_SKIP_TEST_COOKIES****RULE_ACTION_NULL_ROUTE****RULE_ACTION_TRANSPARENT_HTML_JS_FORCE****RULE_ACTION_TRANSPARENT_HTML_JS_RELAXED****RULE_ACTION_HIDDEN_ALERT****RULE_ACTION_ALERT****RULE_ACTION_QUARANTINE_URL****RULE_ACTION_RETRY****RULE_ACTION_INTRUSIVE_HTML****RULE_ACTION_DDOS_ACTION****RULE_ACTION_CAPTCHA****RULE_ACTION_DUAL_FACTOR_AUTHENTICATE****RULE_ACTION_BLOCK****RULE_ACTION_BLOCK_USER**

RULE_ACTION_BLOCK_IP
 RULE_ACTION_BLOCK_IP.Aggressive
 RULE_ACTION_REDIRECT
 RULE_ACTION_REWRITE
 RULE_ACTION_BYPASS_CACHE
 RULE_ACTION_REWRITE_URL
 RULE_ACTION_REWRITE_HEADER
 RULE_ACTION_REWRITE_COOKIE
 RULE_ACTION_DELETE
 RULE_ACTION_DELETE_HEADER
 RULE_ACTION_DELETE_COOKIE
 RULE_ACTION_FORWARD_TO_DC
 RULE_ACTION_RATE
 RULE_ACTION_SIMPLIFIED_REDIRECT
 RULE_ACTION_RESPONSE_DELETE_HEADER
 RULE_ACTION_RESPONSE_REWRITE_HEADER
 RULE_ACTION_CUSTOM_ERROR_RESPONSE
 RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE
 RULE_ACTION_FORWARD_REQUEST
 RULE_ACTION_FORWARD_TO_PORT
 RULE_ACTION_WAF_OVERRIDE
 RULE_ACTION_MASK
 RULE_ACTION_REDIRECT
 RULE_ACTION_SIMPLIFIED_REDIRECT
 RULE_ACTION_REWRITE_URL
 RULE_ACTION_REWRITE_HEADER
 RULE_ACTION_REWRITE_COOKIE
 RULE_ACTION_DELETE_HEADER
 RULE_ACTION_DELETE_COOKIE
 RULE_ACTION_FORWARD_TO_DC
 RULE_ACTION_FORWARD_TO_PORT
 RULE_ACTION_RESPONSE_REWRITE_HEADER
 RULE_ACTION_RESPONSE_DELETE_HEADER
 RULE_ACTION_RESPONSE_REWRITE_RESPONSE_CODE
 RULE_ACTION_CUSTOM_ERROR_RESPONSE
 example: RULE_ACTION_REDIRECT
 enabled (optional)
Boolean
 Boolean that enables the rule. Possible values: true, false.
 example: true

DeliveryRulesListDTO

data (optional)
 array[DeliveryRuleDTO]

DnsInstructionItem

dns_record_name (optional)
String
 example: loginprotectapi1610396334653.incaptest.info
 set_type_to (optional)
String
 Enum:
 CNAME
 A
 AAAA

MX
NS
TXT
Unkown
CAA
example: CNAME
set_data_to (optional)
array[Object]

GetAdvancedCachingSettingsApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
value (optional)
Boolean
example: true

GetCache404SettingsApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
enabled (optional)
Boolean
example: true
time (optional)
Integer
format: int32
example: 10
time_unit (optional)
String
example: HOURS

GetStaleContentApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)

```
array[map[String, Object]]
enabled (optional)
Boolean
example: false
mode (optional)
String
example: ADAPTIVE
time (optional)
Integer
format: int32
example: 10
unit (optional)
String
example: HOURS
```

HSTSConfiguration

HTTP Strict transport security (HSTS) ensures that any attempt by visitors to use the unsecure version (`http://`) of a page will be forwarded automatically to the secure version (`https://`).

isEnabled (optional)

Boolean

Enable/disable HSTS support for this website

maxAge (optional)

Long

(TTL) The amount of time in seconds to apply HSTS in the browser before attempting to load the page using

`http://`. format: int64

example: 7543

subDomainsIncluded (optional)

Boolean

Enforce HSTS on sub-domains. For example, a page listed on `xxx.ddd.com` uses resources from `images.ddd.com`. If HSTS for sub-domains is enabled, the images are also covered. Make sure that the site and all sub-domains support HTTPS so that HSTS does not break an internal resource when rendering the page.

preLoaded (optional)

Boolean

The most secure way to enforce HSTS. Ensures the first request goes out in a secure tunnel, since the browser already has that URL in the pre-load list. The domain needs to be listed at <https://hstspreload.appspot.com/>.

HtmlInjectionItem

url (optional)

String

example: /

url_pattern (optional)

String

Enum:

EQUALS

NOT_EQUALS

NOT_CONTAINS

PREFIX

SUFFIX

NOT_PREFIX

NOT_SUFFIX

CONTAINS

example: prefix

location (optional)

String

example: head

content (optional)

String

example: Some content

IncapRuleApiResult

id (optional)

Long

format: int64

example: 123

name (optional)

String

example: Block Click Worms

action (optional)

String

example: api.rule_action_type.rule_action_block

rule (optional)

String

example: ClientIP == 1.2.3.4

creation_date (optional)

Long

format: int64

updated_by (optional)

String

example: John

updated_at (optional)

Long

format: int64

example: 1611228121241

comment (optional)

String

example: rule comment

IsCacheShieldEnabledApiResult

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

enabled (optional)

Boolean

example: true

ListCustomRulesResponse

incap_rules (optional)

array[map[String, Object]]

example: {"All": [{"id": "3660", "last_7_days_requests_count": "0", "name": "Ortal", "action": "RULE_ACTION_ALERT", "filter": ""}]}
delivery_rules (optional)

array[map[String, Object]]

example: {"Redirect": [{"to": "/home.php", "id": "3648", "priority": "1", "last_7_days_requests_count": "0", "name": "Test new", "action": "RULE_ACTION_REWRITE_URL", "from": "*/home.html", "filter": "ASN == 1"}], "Forward": [{"id": "3628", "priority": "2", "last_7_days_requests_count": "0", "name": "move to rewrite", "dc_id": "54313", "action": "RULE_ACTION_FORWARD_TO_DC", "filter": ""}]}

rate_rules (optional)
array[map[String, Object]]
example: {"Rates": [{"id": "4723", "enabled": "true", "interval": "120", "name": "Test Rate IP", "context": "IP", "action": "RULE_ACTION_RATE", "internal_name": "test-rate-ip", "filter": "ASN == 2"}]}

ListDataCenterResponse**LoginProtectApiResult**

enabled (optional)
Boolean
example: true
specific_users_list (optional)
array[specific_users_list]
send_ip_notifications (optional)
Boolean
example: true
allow_all_users (optional)
Boolean
example: true
authentication_methods (optional)
array[Object]
urls (optional)
array[Object]
url_patterns (optional)
array[Object]

PerformanceConfigurationApiResult

advanced_caching_rules (optional)
array[map[String, Object]]
example: {"never_cache_resources": [{"pattern": "SUFFIX", "url": "/test.html"}], "always_cache_resources": [{"pattern": "NOT_EQUALS", "url": "/index.html", "ttl": "5", "ttlUnits": "SECONDS"}, {"pattern": "EQUALS", "url": "/home.html", "ttl": "6", "ttlUnits": "DAYS"}]}
acceleration_level (optional)
String
example: advanced
acceleration_level_raw (optional)
String
example: none
async_validation (optional)
Boolean
example: true
minify_javascript (optional)
Boolean
example: true
minify_css (optional)
Boolean
example: true
minify_static_html (optional)
Boolean
example: true
compress_jpeg (optional)

Boolean
example: true
compress_jpeg (optional)
Boolean
example: true
progressive_image_rendering (optional)
Boolean
example: true
aggressive_compression (optional)
Boolean
example: true
compress_png (optional)
Boolean
example: true
on_the_fly_compression (optional)
Boolean
example: true
tcp_pre_pooling (optional)
Boolean
example: true
comply_no_cache (optional)
Boolean
example: true
comply_vary (optional)
Boolean
example: true
use_shortest_caching (optional)
Boolean
example: true
prefer_last_modified (optional)
Boolean
example: true
prefer_last_modified (optional)
Boolean
example: true
disable_client_side_caching (optional)
Boolean
example: true
cache300x (optional)
Boolean
example: true
cache_headers (optional)
array[Object]

PopRttResponse

id (optional)
String
example: ord
name (optional)
String
example: Chicago, IL
region (optional)
String
example: US Central
rtt (optional)
Integer
format: int32

example: 8

RecommendedPopsApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
pops (optional)
array[PopRttResponse]
reason (optional)
String
example: N/A

RequestBodyTimeoutDTO

methods (optional)
array[Object]
interval (optional)
Integer
format: int32
byteCount (optional)
Integer
format: int32
requestBodyTimeouts (optional)
RequestBodyTimeoutDTO

RewritePort

from (optional)
String
to (optional)
String

ServerOperationResponse

server_id (optional)
String
example: 2
status (optional)
String
example: ok
res (optional)
String
example: 0

SetPriorityResponse

status (optional)
String

example: ok
res (optional)
String
example: 0

SiteCacheRuleResponse

SiteConfigurationWarning

type (optional)
String
Enum:
CNAME
A
AAAA
MX
NS
TXT
Unkown
CAA
example: CNAME
set_data_to (optional)
array[Object]

SiteDualFactorSettings

specificUsers (optional)
array[String]
enabled (optional)
Boolean
Enable/disable LoginProtect
example: false
customAreas (optional)
array[customAreas]
customAreasExceptions (optional)
array[customAreasExceptions]
allowAllUsers (optional)
Boolean
Authorize all Login Protect users in this account
example: true
shouldSuggestApplicatons (optional)
Boolean
example: true
allowedMedia (optional)
array[String]
Enum:
shouldSendLoginNotifications (optional)
Boolean
Send Notifications on Login to protected URL
example: true
application (optional)
Boolean
version (optional)
Integer
format: int32

TLSConfiguration

hstsConfiguration (optional)
HSTSConfiguration

TLSConfigurationDto

data (optional)
array[TLSConfiguration]

customAreas

Pages or areas on your website requiring extended authentication
pattern (optional)

String

Enum:

EQUALS
NOT_EQUALS
NOT_CONTAINS
PREFIX
SUFFIX

NOT_PREFIX
NOT_SUFFIX

CONTAINS

example: CONTAINS

url (optional)

String

example: /userlist

customAreasExceptions

Pages or areas on your website to exclude from extended authentication
pattern (optional)

String

Enum:

EQUALS
NOT_EQUALS
NOT_CONTAINS
PREFIX
SUFFIX

NOT_PREFIX
NOT_SUFFIX

CONTAINS

example: CONTAINS

url (optional)

String

example: /userlist

inline_response_200**inline_response_200_1****inline_response_200_10**

`inline_response_200_11`

`inline_response_200_12`

`inline_response_200_13`

`inline_response_200_14`

`inline_response_200_15`

`inline_response_200_16`

`inline_response_200_17`

`inline_response_200_18`

`inline_response_200_19`

`inline_response_200_2`

`inline_response_200_20`

`inline_response_200_21`

`inline_response_200_22`

`inline_response_200_3`

`inline_response_200_4`

`inline_response_200_5`

`inline_response_200_6`

`inline_response_200_7`

`inline_response_200_8`

`inline_response_200_9`

`specific_users_list`

email (optional)

String

email

example: John@example.com

name (optional)
String
 name
 example: John Doe
 status (optional)
String
 status
 example: INVITATION_SENT

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

TrafficStatisticsAndLogs

- `post /api/v1/infra/events`
- `post /api/v1/infra/histogram`
- `post /api/v1/infra/top-graph`
- `post /api/v1/infra/top-table`
- `post /api/v1/infra/stats`
- `post /api/stats/v1`
- `post /api/visits/v1`

TrafficStatisticsAndLogs

```
post /api/v1/infra/events
```

Get infrastructure protection events (getInfraEvents)

Use this operation to get Infrastructure Protection event information for an account

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

event_type (optional)

Query Parameter

— A comma separated list of specific event types. Any of: GRE_TUNNEL_UP, GRE_TUNNEL_DOWN, ORIGIN_CONNECTION_GRE_UP, ORIGIN_CONNECTION_GRE_DOWN, ORIGIN_CONNECTION_ECX_UP, ORIGIN_CONNECTION_ECX_DOWN, ORIGIN_CONNECTION_CROSS_CONNECT_UP, ORIGIN_CONNECTION_CROSS_CONNECT_DOWN, DDOS_START_IP_RANGE, DDOS_STOP_IP_RANGE, DDOS QUIET TIME IP RANGE, EXPORTER_NO DATA, EXPORTER_BAD DATA, EXPORTER_GOOD DATA, MONITORING_CRITICAL_ATTACK, PROTECTED_IP_STATUS_UP, PROTECTED_IP_STATUS_DOWN, PER_IP_DDOS_START_IP_RANGE.

ip_prefix (optional)

Query Parameter

— Specific Protected IP or IP range. For example, 1.1.1.0/24.

page_size (optional)

Query Parameter

— The number of objects to return in the response.
Default: 50
Maximum: 100

page_num (optional)

Query Parameter

— The page to return starting from 0. Default: 0

start (optional)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:

- today Retrieve data from midnight today until the current time.
- last_7_days Retrieve data from midnight of 7 days ago until the current time.
- last_30_days Retrieve data from midnight of 30 days ago until the current time.
- last_90_days Retrieve data from midnight of 90 days ago until the current time.
- month_to_date Retrieve data from midnight of the first day of the month until the current time.
- custom Specify a custom time range using two additional parameters: start and end.

 Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
 For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (optional)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:

- today Retrieve data from midnight today until the current time.
- last_7_days Retrieve data from midnight of 7 days ago until the current time.
- last_30_days Retrieve data from midnight of 30 days ago until the current time.
- last_90_days Retrieve data from midnight of 90 days ago until the current time.
- month_to_date Retrieve data from midnight of the first day of the month until the current time.
- custom Specify a custom time range using two additional parameters: start and end.

 Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
 For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

Return type

inline_response_200

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input [inline_response_200](#)

```
post /api/v1/infra/histogram
```

Get infrastructure protection histogram (getInfraProtectHistogram)

Use this operation to view the highest packet size values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the

current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_1](#)

```
post /api/v1/infra/top-graph
```

Get infrastructure protection top items (graph view) (getInfraProtectTopData)

Use this operation to view the highest peak values and highest average values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.
last_7_days Retrieve data from midnight of 7 days ago until the current time.
last_30_days Retrieve data from midnight of 30 days ago until the current time.
last_90_days Retrieve data from midnight of 90 days ago until the current time.
month_to_date Retrieve data from midnight of the first day of the month until the current time.
custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.
last_7_days Retrieve data from midnight of 7 days ago until the current time.
last_30_days Retrieve data from midnight of 30 days ago until the current time.
last_90_days Retrieve data from midnight of 90 days ago until the current time.
month_to_date Retrieve data from midnight of the first day of the month until the current time.
custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

data_type (required)

Query Parameter

— One of the following: SRC_IP, DST_IP, SRC_PORT_PROTOCOL, DST_PORT_PROTOCOL

metric_type (required)

Query Parameter

— One of the following: BW, PPS

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

objects (optional)

Query Parameter

— A comma separated list of items to fetch data for. e.g., 10.10.10.10, 2.2.2.2. If not specified, top items are automatically fetched.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_2](#)

```
post /api/v1/infra/top-table
```

Get infrastructure protection top items (table view) (getInfraProtectTopTable)

Use this operation to view the highest peak values and highest average values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:

-
today Retrieve data from midnight today until the current time.
- last_7_days Retrieve data from midnight of 7 days ago until the current time.
- last_30_days Retrieve data from midnight of 30 days ago until the current time.
- last_90_days Retrieve data from midnight of 90 days ago until the current time.
- month_to_date Retrieve data from midnight of the first day of the month until the current time.
- custom Specify a custom time range using two additional parameters: start and end.

Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

data_type (required)

Query Parameter

— One of the following: SRC_IP, DST_IP, SRC_PORT_PROTOCOL, DST_PORT_PROTOCOL

metric_type (required)

Query Parameter

— One of the following: BW, PPS

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

aggregation_type (required)

Query Parameter

— One of the following: PEAK, AVERAGE

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
"""

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_3](#)

```
post /api/v1/infra/stats
```

Get infrastructure protection statistics (getInfraStats)

Use this operation to get Infrastructure Protection event information for an account.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_prefix (optional)

Query Parameter

— Specific Protected IP or IP range. For example, 1.1.1.0/24.

traffic (optional)

Query Parameter

— Specific traffic. One of: Total, Passed, Blocked.

traffic_type (optional)

Query Parameter

— A comma separated list of specific traffic types. Any of: UDP, TCP, DNS, DNS_RESPONSE, ICMP, SYN, FRAG, LARGE_SYN, NTP, NETFLOW, SSDP, GENERAL. Cannot be used together with the pop parameter.

pop (optional)

Query Parameter

— A comma separated list of specific PoP names. For example: iad, tko. Cannot be used together with the traffic_type parameter. For the list of PoP codes and locations, see Imperva Data Centers (PoPs).

start (optional)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (optional)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

directionTypes (optional)

Query Parameter

- The type of direction(INGRESS/EGRESS) to filter the data

range_type (optional)

Query Parameter

- Can be one of the following: BGP, PROTECTED_IP, NETFLOW

Return type

[inline_response_200_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses**200**

res - contains the specific error code:
2 - Invalid input
3015 - Internal error [inline_response_200_4](#)

```
post /api/stats/v1
```

Get statistics (getStats)

Get site statistics for one or more sites. This operation may return multiple statistics, as specified in the stats parameter.

Query parameters

account_id (optional)

Query Parameter

- Numeric identifier of the account to fetch data for.
Note: You must specify either account_id or site_id.

time_range (required)

Query Parameter

- Time range to fetch data for.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of

yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

start (optional)

Query Parameter

— Start date in milliseconds since January 1, 1970 (midnight UTC/GMT). Used together with the time_range parameter to specify a custom time range.

end (optional)

Query Parameter

— End date in milliseconds since January 1, 1970 (midnight UTC/GMT). Used together with the time_range parameter to specify a custom time range.

site_id (optional)

Query Parameter

— Numeric identifier of the site to fetch data for. Multiple sites can be specified in a comma separated list. For example: 123,124,125.
Note: You must specify either account_id or site_id.

stats (required)

Query Parameter

— Statistics to fetch, as specified in the table below. Multiple statistics can be specified in a comma separated list.
Values for the stats parameters:
visits_timeseries Number of sessions by type (Humans/Bots) over time.hits_timeseries Number of requests by type (Humans/Bots/Blocked) over time and per second.bandwidth_timeseries Amount of bytes (bandwidth) and bits per second (throughput) transferred via the Imperva network from clients to proxy servers and vice-versa over time.requests_geo_dist_summary Total number of requests routed via the Imperva network by data center location.visits_dist_summary Total number of sessions per client application and country.caching Total number of requests and bytes that were cached by the Imperva network.caching_timeseries Number of requests and bytes that were cached by the Imperva network, with one day resolution, with info regarding the caching mode (standard or advanced).threats Total number of threats by type with additional information regarding the security rules configuration.incap_rules List of security rules with total number of reported incidents for each rule.incap_rules_timeseries List of security rules with a series of reported incidents for each rule with the specified granularity.delivery_rules List of delivery rules with total number of hits for each rule.delivery_rules_timeseries List of delivery rules with a series of hits for each rule with the specified granularity.

granularity (optional)

Query Parameter

— Time interval in milliseconds between data points for time series statistics. (See the timeseries values in the table below.)
The default granularity depends on the specified time range, as follows:
Time range of less than 24 hours: Default granularity is 7200000 (2 hours).Time range of between 24 hours and 30 days: Default granularity is 86400000 (1 day).Time range of more than 30 days: Default granularity is 259200000 (3 days).The response includes one result for each interval. For example, if you specify a time range value of last_7_days, the default granularity is 1 day, and the response will return 7 results.
The response timestamps are in milliseconds since January 1, 1970 (midnight UTC/GMT)
Minimum granularity is 5 minutes (300000).
Note: Time series statistics are presented oldest to newest.

Return type

[inline_response_200_5](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 13001 (Timerange invalid), 13002 (Granularity invalid)
[inline_response_200_5](#)

```
post /api/visits/v1
```

Get visits (getVisits)

Use this operation to get a log of recent visits to a website.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

time_range (optional)

Query Parameter

— Time range to fetch data for. Default is last_7_days.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

start (optional)

Query Parameter

— Start date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (optional)

Query Parameter

— End date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

page_size (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 10. Maximum is 100.

page_num (optional)

Query Parameter

— The page to return starting from 0. Default to 0.

security (optional)

Query Parameter

— Filter the sessions that were handled according to the security-related specifications. Multiple values are supported, e.g.: "api.threats.sql_injection, api.acl.blacklisted_ips";

country (optional)

Query Parameter

— Filter the sessions coming from the specified country.

ip (optional)

Query Parameter

— Filter the sessions coming from the specified IP.

visit_id (optional)

Query Parameter

— Comma separated list of visit IDs to load.

list_live_visits (optional)

Query Parameter

— Whether or not to list visits that did not end and that may still be updated.
Possible values: true, false
Default: true

use_previous_region (optional)

Query Parameter

— Whether or not to list visits from old region data. Valid only if a data region was changed in the last 90 days. One of: true | false. Default: false

Return type

[inline_response_200_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

res - contains the specific error code:
1 - Unexpected error [inline_response_200_6](#)

Models

Methods

Table of Contents

1. ADRule
 2. ADRuleSeries
 3. ActionItem
 4. AnalyticsHistogramApiResponse
 5. AnalyticsTopGraphDataResponse
 6. AnalyticsTopTableApiResponse
 7. AnalyticsTopTableData
 8. ApiResult
 9. ApiResultSessions
 10. ApiResultSiteStats
 11. Caching
 12. IncapRule
 13. IncapRuleSeries
 14. InfraEventsApiResponse
 15. InfraProtectEvent
 16. InfraStatsApiResponse
 17. RequestsGeo
 18. SessionItem
 19. Stats
 20. Threat
 21. ThreatItem
 22. TimeSeriesItem
 23. TopGraphPayloads
 24. VisitsItem
 25. VisitsSummary
 26. inline_response_200
 27. inline_response_200_1
 28. inline_response_200_2
 29. inline_response_200_3
 30. inline_response_200_4
-

-
31. inline_response_200_5
 32. inline_response_200_6

ADRule

id (optional)
String
name (optional)
String
action (optional)
String
example: Redirect
createdAt (optional)
Date
format: date-time
updatedBy (optional)
String
example: example@imperva.com
hits (optional)
Long
format: int64
example: 3451

ADRuleSeries

id (optional)
String
name (optional)
String
action (optional)
String
example: Redirect
createdAt (optional)
Date
format: date-time
updatedBy (optional)
String
example: example@imperva.com
hits (optional)
array[Object]
example: [[1478613600000,6],[1478617200000,3]]

ActionItem

queryString (optional)
String
example: ?jobSYapi_password\u003dXXXXXX
postData (optional)
String
requestResult (optional)
String
requestResult
example: api.request_result.req_challenge_javascript
isSecured (optional)
Boolean
example: false

url (optional)
String
example: www.google.com/ddos/ddos-mitigation-services
httpStatus (optional)
Integer
format: int32
example: 200
responseTime (optional)
Long
format: int64
example: 170
thinkTime (optional)
Long
format: int64
example: 169
incidentId (optional)
String
example: 3411008890000033213-29571073433152
threats (optional)
array[ThreatItem]

AnalyticsHistogramApiResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
stats (optional)
array[map[String, Object]]
example: {"PL_100": "366450640", "PL_200": "305475960", "PL_300": "0", "PL_400": "0", "PL_500": "0", "PL_60": "0", "PL_700": "0", "PL_800": "0", "PL_900": "0", "PL_1000": "0", "PL_1100": "0", "PL_1200": "0", "PL_1300": "0", "PL_1400": "0", "PL_1500": "0"}

AnalyticsTopGraphDataResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
stats (optional)
array[Stats]

AnalyticsTopTableApiResponse

res (optional)
Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

stats (optional)

array[AnalyticsTopTableData]

AnalyticsTopTableData

object (optional)

String

example: 10.200.98.3

value (optional)

Double

format: double

example: 334160

ApiResult

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

ApiResultSessions

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

visits (optional)

array[SessionItem]

ApiResultSiteStats

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

```

array[map[String, Object]]
visits_timeseries (optional)
array[VisitsItem]
requests_geo_dist_summary (optional)
RequestsGeo
visits_dist_summary (optional)
array[VisitsSummary]
caching (optional)
Caching
caching_timeseries (optional)
array[TimeSeriesItem]
hits_timeseries (optional)
array[TimeSeriesItem]
bandwidth_timeseries (optional)
array[TimeSeriesItem]
threats (optional)
array[Threat]
incap_rules (optional)
array[IncapRule]
incap_rules_timeseries (optional)
array[IncapRuleSeries]
delivery_rules (optional)
array[ADRule]
delivery_rules_timeseries (optional)
array[ADRuleSeries]
```

Caching

saved_requests (optional)

Long

format: int64

example: 23984923

total_requests (optional)

Long

format: int64

example: 48723648

saved_bytes (optional)

Long

format: int64

example: 762394786

total_bytes (optional)

Long

format: int64

example: 1098349834

IncapRule

id (optional)

String

name (optional)

String

action (optional)

String

example: Require Javascript Support

incidents (optional)

Long

format: int64

example: 3451
 createdAt (optional)
Date
 format: date-time
 updatedBy (optional)
String
 example: example@example.com

IncapRuleSeries

id (optional)
String
 name (optional)
String
 action (optional)
String
 example: Require Javascript Support
 createdAt (optional)
Date
 format: date-time
 updatedBy (optional)
String
 example: example@example.com
 incidents (optional)
array[Object]
 example: [[1478613600000,6],[1478617200000,3]]

InfraEventsApiResponse

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
array[map[String, Object]]
 events (optional)
array[InfraProtectEvent]

InfraProtectEvent

eventTime (optional)
Date
 format: date-time
 eventType (optional)
String
 Enum:
 GRE_TUNNEL_UP
 GRE_TUNNEL_DOWN
 ORIGIN_CONNECTION_GRE_UP
 ORIGIN_CONNECTION_GRE_DOWN
 ORIGIN_CONNECTION_ECX_UP
 ORIGIN_CONNECTION_ECX_DOWN
 ORIGIN_CONNECTION_CROSS_CONNECT_UP

ORIGIN_CONNECTION_CROSS_CONNECT_DOWN
IP_RANGE_ATTACK_START
IP_RANGE_ATTACK_STOP
DDOS_START_IP RANGE
DDOS_STOP_IP RANGE
DDOS QUIET TIME IP RANGE
EXPORTER_NO_DATA
EXPORTER_BAD_DATA
EXPORTER_GOOD_DATA
MONITORING ATTACK
MONITORING_CRITICAL_ATTACK
PROTECTED_IP_STATUS_UP
PROTECTED_IP_STATUS_DOWN
PROTECTED_NETWORK_STATUS_ACTIVE
PROTECTED_NETWORK_STATUS_INACTIVE
PER_IP_DDOS_START_IP RANGE
PER_IP_DDOS_STOP_IP RANGE
IIP_ACCOUNT_SERVICE_SUSPENDED
IIP_ACCOUNT_SERVICE_UNSUSPENDED
INFRAPROTECT_NULL_ROUTE_STARTED
INFRAPROTECT_NULL_ROUTE_ESCALATED
INFRAPROTECT_NULL_ROUTE_ENDED
INFRAPROTECT_RANGE_DIVERT
INFRAPROTECT_RANGE_REVERT
BGP_UP
BGP_DOWN
CONNECTION_PERFORMANCE_DEGRADED
CONNECTION_PERFORMANCE_RESTORED
example: DDOS_STOP_IP RANGE
bwTotal (optional)
Long
format: int64
example: 9000
ppsTotal (optional)
Long
format: int64
example: 90
bwPassed (optional)
Long
format: int64
example: 200
ppsPassed (optional)
Long
format: int64
example: 87
bwBlocked (optional)
Long
format: int64
example: 8800
ppsBlocked (optional)
Long
format: int64
example: 3
eventTarget (optional)
String
Enum:
GRE_TUNNEL
IP RANGE
EXPORTER

PROTECTED_IP

INCAPSULA_IP

NULL_ROUTE

BGP

example: IP_RANGE

reportedByPop (optional)

String

example: zrh

InfraStatsApiResponse

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

RequestsGeo

id (optional)

String

name (optional)

String

data (optional)

array[Object]

example: [['Tokyo, JA',24365435],['Los Angeles, CA',98762738]]

SessionItem

id (optional)

String

example: 133077760038625792

siteld (optional)

Long

format: int64

example: 7

startTime (optional)

Long

format: int64

example: 1361468485000

endTime (optional)

Long

format: int64

example: 1361468486000

clientIPs (optional)

array[Object]

country (optional)

array[Object]

countryCode (optional)

array[Object]

clientType (optional)

String

example: Unclassified
 clientApplication (optional)
String
 example: Bot
 clientApplicationId (optional)
Long
 format: int64
 example: 0
 httpVersion (optional)
String
 example: 2.0
 clientApplicationVersion (optional)
String
 example: 0
 userAgent (optional)
String
 example: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)
 os (optional)
String
 example: Windows
 osVersion (optional)
String
 example: Windows
 supportsCookies (optional)
Boolean
 example: true
 supportsJavaScript (optional)
Boolean
 example: true
 hits (optional)
Long
 format: int64
 example: 1
 pageViews (optional)
Long
 format: int64
 example: 1
 entryReferer (optional)
String
 example: http://lp.usafis.org/_Incapsula_Resource?CWUDNSAI=9_E1521557&incident_id=13307776003810242
 3-139906691365201416&edet=12&cinfo=2ef678e2c753856785000000
 entryPage (optional)
String
 example: www.incapsula.com/ddos/ddos-mitigation-services
 servedVia (optional)
array[Object]
 securitySummary (optional)
array[map[String, Object]]
 example: {"api.threats.sql_injection":"2","api.threats.cross_site_scripting":"1","api.threats.illegal_resource_acces s":"3","api.threats.remote_file_inclusion":"2","api.threats.customRule":"3","api.threats.ddos=DDoS":"4","api.threat s.backdoor":"2","api.threats.bot_access_control":"1","api.acl.blacklisted_countries":"1","api.acl.blacklisted_url s":"1","api.acl.blacklisted_ips":"1"}
 actions (optional)
array[ActionItem]

Stats

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

objectid (optional)

String

example: 200

time (optional)

String

example: 1522761000000

payload (optional)

array[TopGraphPayloads]

Threat

id (optional)

String

name (optional)

String

incidents (optional)

Long

format: int64

example: 12

status (optional)

String

example: ok

status_text_id (optional)

String

example: api.threats.action.block_request

status_text (optional)

String

example: Block Request

followup (optional)

String

example: api.threats.followup.view

followup_text (optional)

String

example: View Incidents

followup_url (optional)

String

example: https://my.incapsula.com/sites/siteVisits?token=1123_103_13234435091_5d55197912387b94&timeFrame=last_7_days&extSiteId=123&threatFilters=badBot

ThreatItem

threats

securityRule (optional)

String

example: api.threats.illegal_resource_access

alertLocation (optional)

String

example: api.alert_location.alert_location_path

attackCodes (optional)

array[Object]
securityRuleAction (optional)
String
example: api.rule_action_type.rule_action_block

TimeSeriesItem

id (optional)
String
name (optional)
String
data (optional)
array[Object]
example: [[1344247200000,5]]

TopGraphPayloads

interval (optional)
String
example: 15000
startTime (optional)
Date
format: date-time
data (optional)
array[Object]
example: [5462,7563]
metric (optional)
String
example: pps
dataType (optional)
String
example: ip
item (optional)
String
example: 10.13.0.1
traffic (optional)
String
example: blocked

VisitsItem

id (optional)
String
name (optional)
String
data (optional)
array[Object]
example: [[1344247200000,50],[1344247500000,40]]

VisitsSummary

id (optional)
String
name (optional)
String
data (optional)

```
array[array[Object]]
example: [['np',15],['no',778]]
```

`inline_response_200`

`inline_response_200_1`

`inline_response_200_2`

`inline_response_200_3`

`inline_response_200_4`

`inline_response_200_5`

`inline_response_200_6`

Login Protect API Overview

Provision Login Protect users and configure protected pages using the Imperva API. For details, see [Login Protect API Definition](#).

What is Login Protect?

Imperva's Login Protect feature lets online businesses implement strong two-factor authentication on any website or application without integration, coding, or software changes.

Single-click activation lets you protect administrative access to any page or URL, secure remote access to corporate web applications, and restrict access to a particular webpage.

Login Protect manages and controls multiple logins across several websites in a centralized manner. Two-factor authentication is supported using either email, SMS, or Google Authenticator.

User Provisioning

Login Protect users are the users that will be allowed to access the protected pages. They are added to the account's Login Protect users list. Access permissions for specific sites can be decided during configuration of the site's protected pages. Login Protect users can be provisioned using the **Add Login Protect User** API call (`/api/prov/v1/sites/lp/configure`).

If user details are available they can be associated with each user using the **name**, **email** and **phone** parameters.

If the details are not available the **should_send_activation_email** parameter should be set to True, in which case users will get an activation email in which they will be able to enter their details.

The "Send SMS" API call can be used in order to validate a user's phone number, in case the **should_send_activation_email** option is not used. In that case, it is advised to generate a random code, and send it to the user's phone using the **Send SMS to user** API call (`/api/prov/v1/sites/lp/send-sms`).

Configuring protected pages for a site

Protected pages are added using the **Modify Site Login Protect Configuration** API call (/api/prov/v1/sites/lp/configure). The URLs of the protected pages can be entered, in comma separated format, using the “urls” parameter. In order to define URL patterns (e.g. “URL starts with” or “URL contains”) use the “url_patterns” parameters in accordance with the entered URLs.

It is also possible to allow access to specific users out of the account’s Login Protect users list using the “specific_users_list” parameter. In order to get notifications on successful user logins to the protected pages use the “send_lp_notifications”. Allowed authentication methods for the site can be decided using the “authentication_methods” parameter.

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

LoginProtect

- `post /api/prov/v1/sites/lp/add-user`
- `post /api/prov/v1/sites/lp/configure-app`
- `post /api/prov/v1/sites/lp/edit-user`
- `post /api/prov/v1/sites/lp/users`
- `post /api/prov/v1/sites/lp/configure`
- `post /api/prov/v1/sites/lp/remove`
- `post /api/prov/v1/sites/lp/send-sms`

LoginProtect

```
post /api/prov/v1/sites/lp/add-user
```

Add login protect user (addLpUser)

Use this operation to add a Login Protect user for a site.

Query parameters

account_id (required)
 Query Parameter
 — Numeric identifier of the account to operate on.

email (required)
 Query Parameter
 — Email address.

name (optional)
 Query Parameter
 — Example: John Smith

phone (optional)
 Query Parameter
 — Phone number. For example: "1-8662507659"

is_phone_verified (optional)
 Query Parameter
 — Whether or not to skip phone verification.

is_email_verified (optional)
 Query Parameter
 — Whether or not to skip email address verification.

should_send_activation_email (optional)
 Query Parameter
 — Whether or not to send activation email to user.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9403 - Unknown/unauthorized account_id
1001 - E-mail invalid
18005 - Login Protect User Exists
18006 - Operation Not Allowed
18009 - Not Supported Action
18004 - Failed to Send E-Mail [ApiResult](#)

```
post /api/prov/v1/sites/lp/configure-app
```

Configure login protect on admin areas (configureProtectedAppByLp)
Use this operation to configure Login Protect on wordpress | joomla | phpBB admin areas.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

protected_app (optional)

Query Parameter

— Protect admin areas of joomla | wordpress | phpBB.

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9413 - Unknown/unauthorized site_id
18001 - Format invalid
18002 - Application invalid
18011 - Invalid SMS Text
9403 - Unknown/unauthorized account_id
1001 - E-mail invalid
18003 - Invalid phone number [inline_response_200](#)

```
post /api/prov/v1/sites/lp/edit-user
```

Edit login protect user (editLpUser)
Edit Login Protect user's settings.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.

email (required)

Query Parameter

— Email address.

name (optional)

Query Parameter

— Example: John Smith

phone (optional)

Query Parameter

— Phone number. For example: "1-8662507659"

is_phone_verified (optional)

Query Parameter

— Whether or not to skip phone verification.

is_email_verified (optional)

Query Parameter

— Whether or not to skip email address verification.

should_send_activation_email (optional)

Query Parameter

— Whether or not to send activation email to user.

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
9403 - Unknown/unauthorized account_id
1001 - E-mail invalid
18005 - Login Protect User Exists
18006 - Operation Not Allowed
18009 - Not Supported Action
18004 - Failed to Send E-Mail [ApiResult](#)

```
post /api/prov/v1/sites/lp/users
```

Get login protect users (getLpUsers)
Use this operation to get the account's login protect user list.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
18003 - Invalid phone number
18004 - Failed to Send E-Mail
9403 - Unknown/unauthorized account_id
1001 - E-mail invalid
18005 - Login Protect User Exists
18006 - Operation Not Allowed [inline_response_200_1](#)

```
post /api/prov/v1/sites/lp/configure
```

Modify Site Login Protect Configuration (modifyLpSiteConfiguration)
Use this operation to change Login Protect settings for a site.

Query parameters

`site_id` (required)

Query Parameter

— Numeric identifier of the site to operate on. format: int64

`enabled` (optional)

Query Parameter

— Pass true to enable login protect on site, and false to disable it.
Default: true

`specific_users_list` (optional)

Query Parameter

— Comma separated email list to set login protect users for the site. If the list is empty all users will be allowed to access the site using Login Protect.

`send_ip_notifications` (optional)

Query Parameter

— Pass true to send notification on successful login using login protect.
Default: false

`allow_all_users` (optional)

Query Parameter

— Pass true to allow all login protect users to access the site. If you want to allow only a specific list of users to access the site using Login Protect set this to false, and add the list to `specific_user_list`.
Default: true

`authentication_methods` (optional)

Query Parameter

— Comma separated list of allowed authentication methods: sms | email | ga

`urls` (optional)

Query Parameter

— A comma separated list of resource paths. For example, /home and /admin/index.html are resource paths, while http://www.example.com/home is not. Each URL should be encoded separately using percent encoding as specified by RFC 3986 (http://tools.ietf.org/html/rfc3986#section-2.1). An empty URL list will remove all URLs.

`url_patterns` (optional)

Query Parameter

— A comma separated list of url patterns. Possible values: contains | equals | prefix | suffix | not_equals | not_contain | not_prefix | not_suffix. The patterns should be in accordance with the matching urls sent by the urls parameter.

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
"""

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 9413 - Unknown/unauthorized site_id
 18001 - Format invalid
 18002 - Application invalid
 18011 - Invalid SMS Text
 9403 - Unknown/unauthorized account_id
 1001 - E-mail invalid
 18003 - Invalid phone number [inline_response_200](#)

```
post /api/prov/v1/sites/lp/remove
```

Remove login protect user (removeLpUser)
 Use this operation to remove a login protect user from an account's user list.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.

email (required)

Query Parameter

— Email address.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
18003 - Invalid phone number
18004 - Failed to Send E-Mail
9403 - Unknown/unauthorized account_id
1001 - E-mail invalid
18005 - Login Protect User Exists
18006 - Operation Not Allowed [ApiResult](#)

```
post /api/prov/v1/sites/lp/send-sms
```

Send SMS to user (sendSms)
Use this operation to send an SMS to a login protect user.

Query parameters

account_id (required)

Query Parameter

— Numeric identifier of the account to operate on.

email (required)

Query Parameter

— Email address.

sms_text (required)

Query Parameter

— Text that will be sent in SMS.

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

res - contains the specific error code:
18003 -Invalid phone number
18011 - Invalid SMS Text
9403 - Unknown/unauthorized account_id
18010 - Invalid User
18007 - Exceeded Allowed SMS
18008 - Failed to Send SMS [ApiResult](#)

Models

Methods

Table of Contents

1. [ApiResult](#)
2. [ApiResultSiteStatus](#)
3. [DnsInstructionItem](#)
4. [IncapRuleApiResult](#)
5. [LoginProtectApiResult](#)
6. [LoginProtectUsersApiResults](#)
7. [LpExtendedUser](#)
8. [PerformanceConfigurationApiResult](#)
9. [RequestBodyTimeoutDTO](#)
10. [SiteConfigurationWarning](#)
11. [SiteDualFactorSettings](#)
12. [customAreas](#)
13. [customAreasExceptions](#)
14. [inline_response_200](#)
15. [inline_response_200_1](#)
16. [specific_users_list](#)

ApiResult

res (optional)

[Integer](#)

res - contains specific error code format: int32

example: 0

res_message (optional)

[String](#)

example: OK

debug_info (optional)

array[map[String, Object]]

ApiResultSiteStatus

res (optional)

[Integer](#)

res - contains specific error code format: int32

example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
site_id (optional)
Long
format: int64
example: 10
statusEnum (optional)
String
Enum:
pending-txt-validation
pending-dns-changes
fully-configured
pending-select approver
pending-certificate
unknown
example: pending-dns-changes
status (optional)
String
example: pending-dns-changes
domain (optional)
String
example: admin@example.com
account_id (optional)
Long
format: int64
example: 1
acceleration_level (optional)
String
example: advanced
acceleration_level_raw (optional)
String
example: none
site_creation_date (optional)
Long
format: int64
example: 1610396346000
ips (optional)
array[Object]
dns (optional)
array[DnsInstructionItem]
original_dns (optional)
array[DnsInstructionItem]
warnings (optional)
array[SiteConfigurationWarning]
active (optional)
String
Enum:
active
bypass
example: active
support_all_tls_versions (optional)
Boolean
example: true
use_wildcard_san_instead_of_full_domain_san (optional)
Boolean

example: true
 add_naked_domain_san (optional)
Boolean
 example: true
 set_site_cookies_without_domain (optional)
Boolean
 example: true
 enable_http_between_Imperva_and_origin (optional)
String
 example: 80
 additionalErrors (optional)
array[Object]
 display_name (optional)
String
 example: loginprotectapi1610396334653.incaptest.info
 security (optional)
array[map[String, Object]]
 example: {"waf":{"rules":[{"id":"api.threats.bot_access_control","name":"Bot Access Control","block_bad_bots":true,"challenge_suspected_bots":true},{"id":"api.threats.sql_injection","name":"SQL Injection","action":"api.threats.action.block_request","action_text":"Block Request"}, {"id":"api.threats.cross_site_scripting","name":"Cross Site Scripting (XSS)","exceptions":[{"values":[{"urls":[{"value":"/gsddg","pattern":"EQUALS"}]}],"id":"api.rule_exception_type.url","name":"URL"}], "id":244711494}],"action":"api.threats.action.alert","action_text":"Alert Only"}, {"id":"api.threats.illegal_resource_access","name":"Illegal Resource Access","action":"api.threats.action.block_user","action_text":"Block User"}, {"id":"api.threats.ddos","name":"DDoS","activation_mode":"api.threats.ddos.activation_mode.off","activation_mode_text":"Off", "ddos_traffic_threshold": "api.threats.ddos.ddos_trassic_threshold", "ddos_traffic_threshold_text": "750", "ddos_adaptive_threshold": "500", "ddos_adaptive_threshold_last_update_time": "1610396346000"}, {"id":"api.threats.backdoor","name":"Backdoor Protect","action":"api.threats.action.quarantine_url","action_text":"Auto-Quarantine"}, {"id":"api.threats.action.block_ip","action_text":"Block IP", "id": "api.threats.remote_file_inclusion", "name": "Remote File Inclusion"}]}, "acls":{"rules":[{"ips":["2.3.4.5"]}], "exceptions":[{"values":[{"id": "api.rule_exception_type.url", "name": "URL"}, {"urls": [{"value": "/home", "pattern": "EQUALS"}]}]}, {"id": 493271006}, {"id": "api.acl.blacklisted_ips", "name": "Visitors from denylisted IPs"}]}}}
 ssl (optional)
array[map[String, Object]]
 example: {"origin_server":{"detected": "true", "detectionStatus": "ok"} }
 siteDualFactorSettings (optional)
SiteDualFactorSettings
 requestBodyTimeouts (optional)
RequestBodyTimeoutDTO
 login_protect (optional)
LoginProtectApiResult
 performance_configuration (optional)
PerformanceConfigurationApiResult
 extended_ddos (optional)
Integer
 format: int32
 incap_rules (optional)
array[IcapRuleApiResult]
 restricted_cname_reuse (optional)
Boolean
 example: true

DnsInstructionItem

dns_record_name (optional)
String
 example: loginprotectapi1610396334653.incaptest.info
 set_type_to (optional)
String

Enum:
CNAME
A
AAAA
MX
NS
TXT
Unknown
CAA
example: CNAME
set_data_to (optional)
array[Object]

IncapRuleApiResult

id (optional)
Long
format: int64
example: 123
name (optional)
String
example: Block Click Worms
action (optional)
String
example: api.rule_action_type.rule_action_block
rule (optional)
String
example: ClientIP == 1.2.3.4
creation_date (optional)
Long
format: int64
updated_by (optional)
String
example: John
updated_at (optional)
Long
format: int64
example: 1611228121241
comment (optional)
String
example: rule comment

LoginProtectApiResult

enabled (optional)
Boolean
example: true
specific_users_list (optional)
array[specific_users_list]
send_ip_notifications (optional)
Boolean
example: true
allow_all_users (optional)
Boolean
example: true
authentication_methods (optional)
array[Object]

urls (optional)
array[Object]
url_patterns (optional)
array[Object]

LoginProtectUsersApiResults

users (optional)
array[LpExtendedUser]

LpExtendedUser

email (optional)
String
email
example: John@example.com
name (optional)
String
name
example: John Doe
status (optional)
String
status
example: INVITATION_SENT
phone (optional)
String
phone
example: 1-8662507658
creation_date (optional)
Date
creation_date format: date-time

PerformanceConfigurationApiResult

advanced_caching_rules (optional)
array[map[String, Object]]
example: {"never_cache_resources":[{"pattern":"SUFFIX","url":"/test.html"}],"always_cache_resources":[{"pattern":"NOT_EQUALS","url":"/index.html","ttl":5,"ttlUnits":"SECONDS"}],"pattern": "EQUALS","url":"/home.html","ttl":6,"ttlUnits": "DAYS"}]}
acceleration_level (optional)
String
example: advanced
acceleration_level_raw (optional)
String
example: none
async_validation (optional)
Boolean
example: true
minify_javascript (optional)
Boolean
example: true
minify_css (optional)
Boolean
example: true
minify_static_html (optional)
Boolean

```
example: true
compress_jpeg (optional)
Boolean
example: true
compress_jpeg (optional)
Boolean
example: true
progressive_image_rendering (optional)
Boolean
example: true
aggressive_compression (optional)
Boolean
example: true
compress_png (optional)
Boolean
example: true
on_the_fly_compression (optional)
Boolean
example: true
tcp_pre_pooling (optional)
Boolean
example: true
comply_no_cache (optional)
Boolean
example: true
comply_vary (optional)
Boolean
example: true
use_shortest_caching (optional)
Boolean
example: true
prefer_last_modified (optional)
Boolean
example: true
prefer_last_modified (optional)
Boolean
example: true
disable_client_side_caching (optional)
Boolean
example: true
cache300x (optional)
Boolean
example: true
cache_headers (optional)
array[Object]
```

RequestBodyTimeoutDTO

```
methods (optional)
array[Object]
interval (optional)
Integer
format: int32
byteCount (optional)
Integer
format: int32
requestBodyTimeouts (optional)
RequestBodyTimeoutDTO
```

SiteConfigurationWarning

type (optional)

String

Enum:

CNAME

A

AAAA

MX

NS

TXT

Unknown

CAA

example: CNAME

set_data_to (optional)

array[Object]

SiteDualFactorSettings

specificUsers (optional)

array[String]

enabled (optional)

Boolean

Enable/disable LoginProtect

example: false

customAreas (optional)

array[customAreas]

customAreasExceptions (optional)

array[customAreasExceptions]

allowAllUsers (optional)

Boolean

Authorize all Login Protect users in this account

example: true

shouldSuggestApplications (optional)

Boolean

example: true

allowedMedia (optional)

array[String]

Enum:

shouldSendLoginNotifications (optional)

Boolean

Send Notifications on Login to protected URL

example: true

application (optional)

Boolean

version (optional)

Integer

format: int32

customAreas

Pages or areas on your website requiring extended authentication

pattern (optional)

String

Enum:

EQUALS

NOT_EQUALS

NOT_CONTAINS
PREFIX
SUFFIX
NOT_PREFIX
NOT_SUFFIX
CONTAINS
example: CONTAINS
url (optional)
String
example: /userlist

customAreasExceptions

Pages or areas on your website to exclude from extended authentication pattern (optional)
String
Enum:
EQUALS
NOT_EQUALS
NOT_CONTAINS
PREFIX
SUFFIX
NOT_PREFIX
NOT_SUFFIX
CONTAINS
example: CONTAINS
url (optional)
String
example: /userlist

inline_response_200**inline_response_200_1****specific_users_list**

email (optional)
String
email
example: John@example.com
name (optional)
String
name
example: John Doe
status (optional)
String
status
example: INVITATION_SENT

Imperva API2 WAF

To better align with REST API standards and best practices, Imperva is gradually rolling out a new version of APIs, available for your use in managing your Cloud Application Security account and websites. These APIs provide either an alternative to existing APIs, or provide APIs with new functionality. For more details about Imperva APIs, see [Imperva API Documentation](#).

Version: 2.0.0
 BasePath:/api/prov/v2
 All rights reserved
<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Settings

- `delete /sites/{extSiteId}/settings/general/additionalTxtRecords`
- `delete /sites/{extSiteId}/settings/general/additionalTxtRecords/delete-all`
- `get /sites/{extSiteId}/settings/general/additionalTxtRecords`
- `post /sites/{extSiteId}/settings/general/additionalTxtRecords`
- `put /sites/{extSiteId}/settings/general/additionalTxtRecords`
- `get /sites/{siteId}/settings/masking`
- `post /sites/{siteId}/settings/masking`

Settings

```
delete /sites/{extSiteId}/settings/general/additionalTxtRecords
```

Delete a specific TXT record that is defined for the site in Cloud WAF
 (sitesExtSiteIdSettingsGeneralAdditionalTxtRecordsDelete)

Delete a specific TXT record that is defined for the site in Cloud WAF

Path parameters

`extSiteId` (required)

Path Parameter

— Site id

Query parameters

`record_number` (optional)

Query Parameter

— Number of txt record to delete

Responses

200

OK

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

```
delete /sites/{extSiteId}/settings/general/additionalTxtRecords/delete-all
```

Delete all TXT records that are defined for the site in Cloud WAF
(sitesExtSiteIdSettingsGeneralAdditionalTxtRecordsDeleteAllDelete)
Delete all TXT records that are defined for the site in Cloud WAF

Path parameters

extSiteId (required)

Path Parameter

— Site id

Responses

200

OK

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

```
get /sites/{extSiteId}/settings/general/additionalTxtRecords
```

Return all TXT records defined for the site in Cloud WAF (sitesExtSiteIdSettingsGeneralAdditionalTxtRecordsGet)
 Return all TXT records defined for the site in Cloud WAF

Path parameters

extSiteId (required)

Path Parameter

— Site id

Responses

200

OK

401

Unauthorized sitelD

404

Resource not found

406

Invalid Input

```
post /sites/{extSiteId}/settings/general/additionalTxtRecords
```

Create or modify one or more of the TXT records defined for the site in Cloud WAF (partial update) (sitesExtSiteIdSettingsGeneralAdditionalTxtRecordsPost)

Create or modify one or more of the TXT records defined for the site in Cloud WAF (partial update)

Path parameters

extSiteId (required)

Path Parameter

— Site id

Query parameters

txt_record_value_one (optional)

Query Parameter

— New value for txt record number one

txt_record_value_two (optional)

Query Parameter

— New value for txt record number two

txt_record_value_three (optional)
Query Parameter
— New value for txt record number three

txt_record_value_four (optional)
Query Parameter
— New value for txt record number four

txt_record_value_five (optional)
Query Parameter
— New value for txt record number five

Responses

200

OK

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

```
put /sites/{extSiteId}/settings/general/additionalTxtRecords
```

Overwrite a specific TXT record that is defined for the site in Cloud WAF (full update)
(sitesExtSitelidSettingsGeneralAdditionalTxtRecordsPut)
Overwrite a specific TXT record that is defined for the site in Cloud WAF (full update)

Path parameters

extSitelid (required)
Path Parameter
— Site id

Query parameters

record_number (optional)
Query Parameter
— Number of txt record to edit

txt_record_value (optional)
Query Parameter
— New value for txt record

Responses

200

OK

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

```
get /sites/{siteId}/settings/masking
```

Returns a masking setting for the given site. (sitesSitelidSettingsMaskingGet)

Read masking settings.

Path parameters

sitelid (required)

Path Parameter

— Site id

Responses

200

OK

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

```
post /sites/{siteId}/settings/masking
```

Update masking settings for site (sitesSitIdSettingsMaskingPost)
Update masking settings.

Path parameters

siteId (required)
Path Parameter
— Site id

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body MaskingSettings (required)
Body Parameter
— The masking setting to configure

Responses

200

OK

401

Unauthorized siteId

404

Resource not found

406

Invalid Input

Models

Methods

Table of Contents

1. MaskingSettings
-

MaskingSettings

hashing_enabled (optional)

Boolean

Use the hashing method for masking fields in your logs and events page.

hash_salt (optional)

String

The hash salt to use for the hashing algorithm.

WAF Settings

View and manage WAF settings in your account.

Version: 1.0.0

BasePath:/waf-settings-v2

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

SessionReleaseAPI

- `post /v3/sites/{siteId}/sessions/{sessionId}/release`

SessionReleaseAPI

```
post /v3/sites/{siteId}/sessions/{sessionId}/release
```

Release blocked session (releaseSession)
 Releases a blocked session by sessionId and siteld

Path parameters

siteld (required)

Path Parameter

— format: int64

sessionId (required)

Path Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

ExternalResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "message" : "message",
    "successful" : true
  }, {
    "message" : "message",
    "successful" : true
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful operation ExternalResponse

400

Bad Request ErrorResponse

Example data

Content-Type: Bad Request

```
{"errors": [{"status":400,"id":"358eebec0102e42c","source":{"pointer":"/v3/sites/123/sessions/1/release"},"title":"Bad Request","detail":"Invalid session id"}]}
```

404

Not found [ErrorResponse](#)

Example data

Content-Type: Not found

```
{"errors": [{"status":404,"id":"358eebec0102e42c","source":{"pointer":"/v3/sites/123/sessions/1/release"},"title":"Not Found","detail":"Site 123 not found"}]}
```

500

Internal Server Error [ErrorResponse](#)

Example data

Content-Type: Internal Server Error

```
{"errors": [{"status":500,"id":"1dce2fbdec3e60e2","source":{"pointer":"/v3/sites/123/sessions/1/release"},"title":"Internal Server Error","detail":"Internal Server Error"}]}
```

Models

Methods

Table of Contents

1. [APIError](#)
2. [ErrorResponse](#)
3. [ExternalResponse](#)
4. [SessionReleaseResponseDto](#)

APIError

status (optional)

Integer

format: int32

example: 400

id (optional)

String

example: afec0aac0e30808f

code (optional)

String

example: 2

source (optional)

map[String, Object]

example: {"pointer":"/v3/sites/16612920/settings/spa"}

title (optional)

String

example: Invalid Input Error

detail (optional)

String

example: state State must not be null!

ErrorResponse

errors (optional)

array[APIError]

ExternalResponse

data (optional)

array[SessionReleaseResponseDto]

SessionReleaseResponseDto

message (optional)

String

successful (optional)

Boolean

Account Takeover Protection API

This is the API documentation for Imperva Account Takeover Protection. ATO detects and mitigates account takeover attempts, protecting your web applications against volumetric and low and slow ATO attacks. For the full feature documentation, see <https://docs.imperva.com/bundle/account-takeover>.

Version: 2.0.0

BasePath:/ato

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true

2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Configuration

- `post /v2/sites/{siteId}/onboard/copy-to/{target-site-id}`
- `delete /v2/sites/{siteId}/endpoint/{endpointId}`

-
- `get /v2/sites/{siteId}/endpoints`
 - `get /v2/sites`

Evidence

- `post /v2/sites/{siteId}/report/evidence/aggregators`
- `post /v2/sites/{siteId}/report/evidence`
- `post /v2/sites/{siteId}/report/evidence/suspicious-successful`
- `post /v2/sites/{siteId}/report/evidence/leaked-creds`
- `post /v2/sites/{siteId}/report/evidence/likely-leaked`
- `post /v2/sites/{siteId}/report/evidence/mitigated-request`

General

- `post /v2/sites/{siteId}/allowlist`
- `get /v2/sites/{siteId}/allowlist`
- `post /v2/sites/{siteId}/report/evidence/leaked`
- `post /v2/sites/{siteId}/report/evidence/mitigated`
- `post /v2/sites/{siteId}/report/evidence/suspicious-successful`
- `delete /v2/sites/{siteId}/allowlist`
- `post /v2/sites/{siteId}/reset-risk`
- `put /v2/sites/{siteId}/allowlist`

Mitigation

- `get /v2/sites/{siteId}/mitigation`
- `post /v2/sites/{siteId}/mitigation`

PiiPassword

- `delete /v2/sites/{siteId}/pii-password`
- `post /v2/sites/{siteId}/pii-password`

Statistics

- `post /v2/sites/{siteId}/stats`

Timeline

- `post /v2/sites/{siteId}/timeline`

TopSources

- `post /v2/sites/{siteId}/stats/top`
-

-
- `post /v2/sites/{siteId}/stats/top/client`
 - `post /v2/sites/{siteId}/stats/top/country`
 - `post /v2/sites/{siteId}/stats/top/ip`
 - `post /v2/sites/{siteId}/stats/top/ip-fingerprint`
 - `post /v2/sites/{siteId}/stats/top/reputation`

Users

- `post /v2/sites/{siteId}/stats/users/aggregators`
- `post /v2/sites/{siteId}/stats/users`
- `post /v2/sites/{siteId}/stats/users/leaked`
- `post /v2/sites/{siteId}/stats/users/likely-leaked`
- `post /v2/sites/{siteId}/stats/users/suspicious-successful`

Configuration

```
post /v2/sites/{siteId}/onboard/copy-to/{target-site-id}
```

Copy a single login endpoint, or all of them, from the "source" website to the "target" website under the same account ID (`copyEndpointConfigurationFromSiteToAnotherSite`)

Both sites must be under the same account ID (no sub-accounts support yet). In addition, mitigation settings are not copied.

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the "source" website (the website we copy from) format: int64

`target-site-id` (required)

Path Parameter

— The Imperva ID of the "target" website (the website we want to copy the endpoint config to) format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

`default: -1` format: int64

`endpointId` (optional)

Query Parameter

— Optional: pass an endpoint ID to copy, if none passed all endpoints will be copied

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
delete /v2/sites/{siteId}/endpoint/{endpointId}
```

Delete an endpoint for this website (deleteEndpoint)

Delete the specified endpoint from the specified website. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

endpointId (required)

Path Parameter

— The endpoint ID to delete

sitId (required)

Path Parameter

— The Imperva ID of the website format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
get /v2/sites/{siteId}/endpoints
```

Retrieve all the onboarded login endpoints for this website (getEndpoints)

Retrieve a list of all onboarded login endpoints for your website. Each endpoint will include its id, url, username and password parameters. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the website format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

array[[Endpoints](#)]

Example data

Content-Type: application/json

```
[ {  
    "passwordParameter" : "passwordParameter",  
    "endpointId" : "endpointId",  
    "usernameParameter" : "usernameParameter",  
    "url" : "url"  
, {  
    "passwordParameter" : "passwordParameter",  
    "endpointId" : "endpointId",  
    "usernameParameter" : "usernameParameter",  
    "url" : "url"
```

```
    } ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of onboarded endpoints, each includes url, id, username and password parameters

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
get /v2/sites
```

Retrieve all onboarded sites with their mitigation status. (getOnboardedSitesWithMitigationStatus)
 Retrieve a list of all onboarded sites for the account ID. Each site will include the Imperva website ID, site name, and mitigation status. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
 default: -1 format: int64

Return type

array[SiteStatus]

Example data

Content-Type: application/json

```
[ {
  "websiteName" : "mysite.com",
  "isMitigationOn" : true,
  "siteId" : 0
}, {
  "websiteName" : "mysite.com",
  "isMitigationOn" : true,
  "siteId" : 0
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of onboarded sites with their mitigation status.

400

Bad Request

401

Not Authorized

500

Internal Server Error

Evidence

```
post /v2/sites/{siteId}/report/evidence/aggregators
```

Retrieve aggregated login report (getAggregatorsEvidence)

Retrieve the list of login events that were classified as coming from known aggregators. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body EvidenceRequest (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

caId (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. default: -1 format: int64

Return type

Evidence

Example data

Content-Type: application/json

```
{
  "evaluation" : {
    "riskFactors" : [ "riskFactors", "riskFactors" ],
    "recordType" : "recordType",
    "reputation" : [ "reputation", "reputation" ]
  },
  "request" : {
    "country" : "country",
    "clients" : [ "clients", "clients" ],
    "declaredClients" : [ "declaredClients", "declaredClients" ],
    "ip" : "ip",
    "declaredClient" : "declaredClient",
    "userAgent" : "userAgent",
    "sessionId" : 6,
    "path" : "path",
    "referrer" : "referrer",
    "requestId" : 0,
    "client" : "client",
    "user" : "user",
  }
}
```

```

    "timestamp" : 1
},
"deviceStats" : {
  "failedLogins" : 5,
  "fingerprint" : "fingerprint",
  "risk" : "LOW",
  "successfulLogins" : 2,
  "leakedCredentials" : 5
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of aggregator login events [Evidence](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

```
post /v2/sites/{siteId}/report/evidence
```

Retrieve report of all user logins (getAllEvidence)

Retrieve the list of successful login events that used publicly available leaked credentials. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `EvidenceRequest` (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

`SuspiciousSuccessfulEvidence`

Example data

Content-Type: application/json

```
{
  "aggregators" : "aggregators",
  "suspiciousSuccessful" : "suspiciousSuccessful",
  "likelyLeaked" : "likelyLeaked",
  "leaked" : "leaked",
  "mitigated" : "mitigated"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

List of login events `SuspiciousSuccessfulEvidence`

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/suspicious-successful
```

Retrieve the compromised users login report (getCompromisedEvidence)

Retrieve the list of successful login events that had a non-zero probability of being an attack. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body EvidenceRequest (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

Evidence

Example data

Content-Type: application/json

```
{
  "evaluation" : {
    "riskFactors" : [ "riskFactors", "riskFactors" ],
    "recordType" : "recordType",
    "reputation" : [ "reputation", "reputation" ]
  },
  "request" : {
    "country" : "country",
    "clients" : [ "clients", "clients" ],
    "declaredClients" : [ "declaredClients", "declaredClients" ],
    "ip" : "ip",
    "declaredClient" : "declaredClient",
    "userAgent" : "userAgent",
    "sessionId" : 6,
    "path" : "path",
    "referrer" : "referrer",
    "requestId" : 0,
    "client" : "client",
    "user" : "user",
    "timestamp" : 1
  },
  "deviceStats" : {
    "failedLogins" : 5,
    "fingerprint" : "fingerprint",
    "risk" : "LOW",
    "successfulLogins" : 2,
    "leakedCredentials" : 5
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of login events, returned type is always COMPROMISED Evidence

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/leaked-creds
```

Retrieve the leaked users login report (getLeakedEvidence)

Retrieve the list of successful login events that used publicly available leaked credentials. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- * / *

Request body

body EvidenceRequest (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. default: -1 format: int64

Return type

Evidence

Example data

Content-Type: application/json

```
{
```

```

"evaluation" : {
  "riskFactors" : [ "riskFactors", "riskFactors" ],
  "recordType" : "recordType",
  "reputation" : [ "reputation", "reputation" ]
},
"request" : {
  "country" : "country",
  "clients" : [ "clients", "clients" ],
  "declaredClients" : [ "declaredClients", "declaredClients" ],
  "ip" : "ip",
  "declaredClient" : "declaredClient",
  "userAgent" : "userAgent",
  "sessionId" : 6,
  "path" : "path",
  "referrer" : "referrer",
  "requestId" : 0,
  "client" : "client",
  "user" : "user",
  "timestamp" : 1
},
"deviceStats" : {
  "failedLogins" : 5,
  "fingerprint" : "fingerprint",
  "risk" : "LOW",
  "successfulLogins" : 2,
  "leakedCredentials" : 5
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of login events, returned type is always LEAKED Evidence

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/likely-leaked
```

Retrieve the likely leaked users login report (getLikelyLeakedEvidence)

Retrieve the list of likely leaked login events that potentially used publicly available leaked credentials. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body EvidenceRequest (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

LikelyLeakedEvidence

Example data

Content-Type: application/json

```
{  
  "ip" : "ip",  
  "user" : "user",  
  "timestamp" : 0  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of likely leaked login events [LikelyLeakedEvidence](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/mitigated-request
```

Retrieve the mitigated (CAPTCHA, BLOCK, TARPIT) users login report (getMitigatedEvidence)
 Retrieve the list of mitigated (CAPTCHA, BLOCK, TARPIT) login events. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body [EvidenceRequest](#) (required)

Body Parameter

— Specify the time selection and/or endpoint ID

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

Evidence

Example data

Content-Type: application/json

```
{
  "evaluation" : {
    "riskFactors" : [ "riskFactors", "riskFactors" ],
    "recordType" : "recordType",
    "reputation" : [ "reputation", "reputation" ]
  },
  "request" : {
    "country" : "country",
    "clients" : [ "clients", "clients" ],
    "declaredClients" : [ "declaredClients", "declaredClients" ],
    "ip" : "ip",
    "declaredClient" : "declaredClient",
    "userAgent" : "userAgent",
    "sessionId" : 6,
    "path" : "path",
    "referrer" : "referrer",
    "requestId" : 0,
    "client" : "client",
    "user" : "user",
    "timestamp" : 1
  },
  "deviceStats" : {
    "failedLogins" : 5,
    "fingerprint" : "fingerprint",
    "risk" : "LOW",
    "successfulLogins" : 2,
    "leakedCredentials" : 5
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

List of login events, returned type is always MITIGATED Evidence

400

Bad Request

401

Not Authorized

500

Internal Server Error

General

```
post /v2/sites/{siteId}/allowlist
```

Update the allowlist for a specific site (addToAllowList)

Update the list of IPs and subnets excluded from traffic mitigation by ATO Protection. All traffic from these IPs will not be mitigated. The input should be a comma separated JSON list containing the IPs to add to the site allowlist. Each allowed IP object can have a mask property to be applied to that IP and allow that whole subnet. For example: [{"ip":"192.20.1.1","desc":"My own IP"}, {"ip":"15.5.0.0","mask":16,"desc":"Office subnet"}, {"ip":"20.1.1.0","mask":24,"desc":"Home subnet"}]

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body [AllowlistIp](#) (required)

Body Parameter

— List of IPs/subnets

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
get /v2/sites/{siteId}/allowlist
```

Retrieve the allowlist for a specific site (getAllowList)

Retrieve the list of IPs and subnets excluded from traffic mitigation by ATO Protection. All traffic from these IPs will not be mitigated.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Return type

AllowlistIp

Example data

Content-Type: application/json

```
{
  "ip" : "192.10.20.0",
  "updated" : 1632530998076,
  "mask" : "24",
  "desc" : "My own IP to always allow"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

List of the IPs and subnets to exclude from mitigation [AllowlistIp](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/leaked
```

Retrieve the leaked users login report (`getLeakedReport`)

Retrieve the list of successful login events that used publicly available leaked credentials. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `ReportRequest` (required)

Body Parameter

— Specify event selection range, PII password and endpoint ID

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used

for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

[LoginEvent](#)

Example data

Content-Type: application/json

```
{  
    "path" : "path",  
    "referrer" : "referrer",  
    "endpointId" : "endpointId",  
    "ip" : "ip",  
    "risk" : "LOW",  
    "time" : 0,  
    "type" : "LEAKED",  
    "user" : "user"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

List of login events, returned type is always LEAKED [LoginEvent](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

```
post /v2/sites/{siteId}/report/evidence/mitigated
```

Retrieve the mitigated (CAPTCHA, BLOCK) users login report (getMitigatedReport)
 Retrieve the list of mitigated (CAPTCHA, BLOCK) login events. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`sitId` (required)
 Path Parameter
 — The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `ReportRequest` (required)
 Body Parameter
 — Specify event selection range, PII password and endpoint ID

Query parameters

`caId` (optional)
 Query Parameter
 — The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
 default: -1 format: int64

Return type

`LoginEvent`

Example data

Content-Type: `application/json`

```
{
  "path" : "path",
  "referrer" : "referrer",
  "endpointId" : "endpointId",
  "ip" : "ip",
  "risk" : "LOW",
  "time" : 0,
  "type" : "LEAKED",
  "user" : "user"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- `*/*`

Responses

200

List of login events, returned type is always MITIGATED LoginEvent

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/report/evidence/suspicious/successful
```

Retrieve the compromised users login report (getSuccessfulAndSuspiciousReport)

Retrieve the list of successful login events that had a non-zero probability of being an attack. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

`body ReportRequest` (required)

Body Parameter

— Specify event selection range, PII password and endpoint ID

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Return type

[LoginEvent](#)

Example data

Content-Type: application/json

```
{
  "path" : "path",
  "referrer" : "referrer",
  "endpointId" : "endpointId",
  "ip" : "ip",
  "risk" : "LOW",
  "time" : 0,
  "type" : "LEAKED",
  "user" : "user"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

List of login events, returned type is always [LoginEvent](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
delete /v2/sites/{siteId}/allowlist
```

Remove IPs from the allowlist for a specific site (removeFromAllowList)

Remove the list of IPs and subnets from the current allowlist configuration of the site. Matching the IPs and subnets will be done by comparing the 'ip' and 'mask' fields of the entries. For example:

[{"ip":"192.20.1.1"}, {"ip":"15.5.0.0", "mask": "16"}]

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `AllowlistIp` (required)

Body Parameter

— List of IPs/subnets to remove

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/reset-risk
```

Reset the risk level of IPs for a specific site (resetRisk)

Resets the risk level assigned to an IP address by Account Takeover Protection. Risk level indicates the severity of risk. If there is continued suspicious activity from an IP, the risk level will escalate again afterwards. For example: ["192.20.1.1", "15.5.0.0"] For sites with ATO fingerprint enabled, not all devices will have their risk reset.

Priority will be given to devices that were most recently active. IPV4 and IPV6 values are accepted but IP ranges will be rejected There is a limit of 10 IPs per request

Path parameters

siteld (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body string (required)

Body Parameter

— List of IPs. The input must be a comma separated list of IP addresses in JSON format. It can take up to one minute to fully process the request after it has been sent.

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Responses

200

OK

400

Bad Request

401

Not Authorized

429

Too many requests

500

Internal Server Error

```
put /v2/sites/{siteId}/allowlist
```

Overwrite the allowlist for a specific site (setAllowList)

Overwrite the list of IPs and subnets excluded from traffic mitigation by ATO Protection. THIS CALL WILL REPLACE THE EXISTING LIST. All traffic from these IPs will not be mitigated. The input should be a comma separated JSON list containing all the IPs in the allowlist for the site. Each allowed IP object can have a mask property to be applied to that IP and allow that whole subnet.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body AllowlistIp (required)

Body Parameter

— Complete list of IPs/subnets

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

Mitigation

```
get /v2/sites/{siteId}/mitigation
```

Get the mitigation configuration for a specific site. (getMitigationConfig)

Pass a comma-separated string of endpoint ids in order to get the mitigation configuration just for those ones. If not passed, this API will retrieve the mitigation configuration for all endpoints

Path parameters

`siteId` (required)

Path Parameter

— The Imperva ID of the website format: int64

Query parameters

`caId` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. default: -1 format: int64

`endpointIds` (optional)

Query Parameter

— Comma-separated list of endpoint ids

Return type

array[MitigationRequest]

Example data

Content-Type: application/json

```
[ {
  "lowAction" : "NONE",
  "highAction" : "NONE",
  "endpointId" : "endpointId",
  "mediumAction" : "NONE"
}, {
  "lowAction" : "NONE",
  "highAction" : "NONE",
  "endpointId" : "endpointId",
  "mediumAction" : "NONE"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve a list of endpoint IDs with their mitigation configuration, e.g. [{ "endpointId": "764337755", "lowAction": "NONE", "mediumAction": "NONE", "highAction": "BLOCK" }, { "endpointId": "1429179364", "lowAction": "NONE", "mediumAction": "CAPTCHA", "highAction": "CAPTCHA" }]

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/mitigation
```

Change the mitigation configuration for a specific site and endpoint. The actions (low, medium, high) should all be in UPPER CASE. (setMitigationConfigForEndpoints)
Possible values for actions are: NONE, CAPTCHA, BLOCK, TARPIT.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **MitigationRequest** (required)

Body Parameter

— Specify endpoint ID and mitigation actions list

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

PiiPassword

```
delete /v2/sites/{siteId}/pii-password
```

Reset the PII password (deletePiiPassword)

Reset the PII password for the current account. This will delete the currently configured PII password and you will have to configure a new one before being able to see plaintext usernames. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The Imperva ID of the website format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

Responses

204

No Content

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/pii-password
```

Update the PII password (setPiiPassword)

Update the PII password for the current account. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body PiiConfigPassword (required)

Body Parameter

— Pii Password to update

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. default: -1 format: int64

Responses

200

OK

400

Bad Request

401

Not Authorized

500

Internal Server Error

Statistics

```
post /v2/sites/{siteId}/stats
```

Get all stats - top stats and unique users stats. (getAllStats)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
 default: -1 format: int64
 endpointId (optional)
 Query Parameter
 — format: int64

Return type

AllStats

Example data

Content-Type: application/json

```
{
  "top" : {
    "client" : {
      "high" : {
        "key" : 2
      },
      "low" : {
        "key" : 5
      },
      "none" : {
        "key" : 1
      },
      "medium" : {
        "key" : 5
      }
    }
  },
  "users" : {
    "leaked" : {
      "prevTotal" : 6,
      "currentTotal" : 0
    }
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve all stats - top stats and unique users stats. [AllStats](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

Timeline

```
post /v2/sites/{siteId}/timeline
```

Get the login timeline for a site. (getLoginsTimeline)

Pass an endpoint id in order to get the timeline just for that one. If you don't pass an endpoint id, all configured ids will be sent as one "TOTAL" (summed together). A login timeline represents ongoing login requests made to your site over a time period. Each data point represents the number of logins attempted for that time bucket (each 5 minutes).

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

endpointId (optional)

Query Parameter

Return type

[LoginsTimeline](#)

Example data

Content-Type: application/json

```
{
  "intervalMs" : 300000,
  "endpointId" : "1616877031",
  "timeline" : {
    "key" : {
      "total" : 7944,
      "data" : "[5, 1, 0, 0, 0, 75, 2, 1, 0, 0]",
      "prevTotal" : 4532
    }
  },
  "startTime" : 1673624384997
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the login requests timeline [LoginsTimeline](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

TopSources

```
post /v2/sites/{siteId}/stats/top
```

Get all the top stats (country, client, reputation, successful user, ip, ip+fingerprint). (getAllTopSourcesStats)
If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

endpointId (optional)

Query Parameter

Return type

TopStats

Example data

Content-Type: application/json

```
{
  "client" : {
    "high" : {
      "key" : 2
    }
  },
}
```

```

    "low" : {
      "key" : 5
    },
    "none" : {
      "key" : 1
    },
    "medium" : {
      "key" : 5
    }
  }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve all the top stats (country, client, reputation, successful user, ip, ip+fingerprint). [TopStats](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

```
post /v2/sites/{siteId}/stats/top/client
```

Get top number of requests by client of unique users for the current time period compared to previous time period (getTopClients)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `StatsRequest` (required)

Body Parameter

— Specify the time selection

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

`endpointId` (optional)

Query Parameter

Return type

TopSource

Example data

Content-Type: application/json

```
{
  "high" : {
    "key" : 2
  },
  "low" : {
    "key" : 5
  },
  "none" : {
    "key" : 1
  },
  "medium" : {
    "key" : 5
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the top clients performing logins to this site and endpoint ID, by risk level [TopSource](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/top/country
```

Get top number of requests by country of unique users for the current time period compared to previous time period ([getTopCountries](#))

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [StatsRequest](#) (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

endpointId (optional)
Query Parameter

Return type

TopSource

Example data

Content-Type: application/json

```
{  
  "high" : {  
    "key" : 2  
  },  
  "low" : {  
    "key" : 5  
  },  
  "none" : {  
    "key" : 1  
  },  
  "medium" : {  
    "key" : 5  
  }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the top countries performing logins to this site and endpoint ID, by risk level [TopSource](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

```
post /v2/sites/{siteId}/stats/top/ip
```

Get top number of requests by IP of unique users for the current time period compared to previous time period (getTopIps)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

endpointId (optional)

Query Parameter

Return type

TopSource

Example data

Content-Type: application/json

```
{
  "high" : {
    "key" : 2
  },
  "low" : {
    "key" : 5
  }
}
```

```

},
"none" : {
    "key" : 1
},
"medium" : {
    "key" : 5
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the top IPs performing logins to this site and endpoint ID, by risk level **TopSource**

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/top/ip-fingerprint
```

Get top number of requests by IP + Fingerprint of unique users for the current time period compared to previous time period (getTopIpsFps)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `StatsRequest` (required)

Body Parameter

— Specify the time selection

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

`endpointId` (optional)

Query Parameter

Return type

TopSource

Example data

Content-Type: application/json

```
{
  "high" : {
    "key" : 2
  },
  "low" : {
    "key" : 5
  },
  "none" : {
    "key" : 1
  },
  "medium" : {
    "key" : 5
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the top IPs + Fingerprints performing logins to this site and endpoint ID, by risk level TopSource

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/top/reputation
```

Get top number of requests by reputation of unique users for the current time period compared to previous time period (getTopReputation)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **StatsRequest** (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

endpointId (optional)
Query Parameter

Return type

TopSource

Example data

Content-Type: application/json

```
{  
  "high" : {  
    "key" : 2  
  },  
  "low" : {  
    "key" : 5  
  },  
  "none" : {  
    "key" : 1  
  },  
  "medium" : {  
    "key" : 5  
  }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the top reputations performing logins to this site and endpoint ID, by risk level [TopSource](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

Users

```
post /v2/sites/{siteId}/stats/users/aggregators
```

Get aggregators successful requests of unique users for the current time period compared to previous time period (getAggregatorsStats)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

endpointId (optional)

Query Parameter

—

Return type

UsersStats

Example data

Content-Type: application/json

```
{  
  "prevTotal" : 6,  
  "currentTotal" : 0
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the aggregators unique users for the requested time span, including the same for the previous time span
[UsersStats](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/users
```

Get all the unique users stats (leaked, aggregator, likely-leaked, suspicious-successful). (`getAllUniqueUsersStats`)
If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`siteld` (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `StatsRequest` (required)

Body Parameter

— Specify the time selection

Query parameters

`caid` (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

`endpointId` (optional)

Query Parameter

Return type

`AllUserStats`

Example data

Content-Type: application/json

```
{
  "leaked" : {
    "prevTotal" : 6,
    "currentTotal" : 0
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Get all the unique users stats (leaked, aggregator, likely-leaked, suspicious-successful). `AllUserStats`

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/users/leaked
```

Get leaked successful requests of unique users for the current time period compared to previous time period (getLeakedStats)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

endpointId (optional)

Query Parameter

—

Return type

UsersStats

Example data

Content-Type: application/json

```
{
  "prevTotal" : 6,
  "currentTotal" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the leaked unique users for the requested time span, including the same for the previous time span
[UsersStats](#)

400

Bad Request

401

Not Authorized

500

[Internal Server Error](#)

```
post /v2/sites/{siteId}/stats/users/likely-leaked
```

Get likely leaked successful requests of unique users for the current time period compared to previous time period
[\(getLikelyLeakedCredentialsStats\)](#)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
-

Request body

body [StatsRequest](#) (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

default: -1 format: int64

endpointId (optional)

Query Parameter

—

Return type

[UsersStats](#)

Example data

Content-Type: application/json

```
{  
    "prevTotal" : 6,  
    "currentTotal" : 0  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the likely leaked unique users for the requested time span, including the same for the previous time span
[UsersStats](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

```
post /v2/sites/{siteId}/stats/users/suspicious-successful
```

Get suspicious successful requests of unique users for the current time period compared to previous time period (getSuspiciousSuccessfulStats)

If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The Imperva ID of the website format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body StatsRequest (required)

Body Parameter

— Specify the time selection

Query parameters

caid (optional)

Query Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
default: -1 format: int64

endpointId (optional)

Query Parameter

—

Return type

UsersStats

Example data

Content-Type: application/json

```
{
  "prevTotal" : 6,
  "currentTotal" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Retrieve the suspicious successful unique users for the requested time span, including the same for the previous time span [UsersStats](#)

400

Bad Request

401

Not Authorized

500

Internal Server Error

Models

Methods

Table of Contents

1. [AllStats](#)
 2. [AllUserStats](#)
 3. [AllowlistIp](#)
 4. [DeviceStats](#)
 5. [Endpoints](#)
 6. [Evaluation](#)
 7. [Evidence](#)
 8. [EvidenceRequest](#)
 9. [LikelyLeakedEvidence](#)
-

-
10. LoginEvent
 11. LoginsTimeline
 12. MitigationRequest
 13. PiConfigPassword
 14. ReportRequest
 15. Request
 16. RequestTimeline
 17. SiteStatus
 18. StatsRequest
 19. StreamingOutput
 20. SuspiciousSuccessfulEvidence
 21. TopSource
 22. TopStats
 23. UsersStats

AllStats

users (optional)
AllUserStats
 top (optional)
TopStats

AllUserStats

leaked (optional)
UsersStats
 aggregator (optional)
UsersStats
 suspiciousSuccessful (optional)
UsersStats
 likelyLeaked (optional)
UsersStats

AllowlistIp

ip
String
 IP address to exclude. This will be either an IPv4 (e.g. 50.3.183.2) or normalized IPv6 representation (e.g. 2001:db8:0:0:1:0:0:1).

example: 192.10.20.0

mask (optional)

String

[Optional] IP subnet mask to use for excluding a range of IPs. This is the number of bits to use from the IP address as a subnet mask to apply on the source IP of incoming traffic.

example: 24

updated (optional)

Long

Timestamp, in UNIX Epoch milliseconds, of the latest update of this entry. format: int64

example: 1632530998076

desc (optional)

String

Description of the IP/subnet.
example: My own IP to always allow

DeviceStats

failedLogins (optional)

Long

Failed logins in last 24 hours. format: int64

fingerprint (optional)

String

Client fingerprint.

leakedCredentials (optional)

Long

Number of leaked credentials used to login in last 24 hours. format: int64

risk (optional)

String

Probability that this event was part of an attack, as computed post-factum.

Enum:

LOW

MEDIUM

HIGH

successfulLogins (optional)

Long

Successful logins in last 24 hours. format: int64

Endpoints

endpointId (optional)

String

The endpoint ID

url (optional)

String

URL configured for this endpoint

usernameParameter (optional)

String

Username parameter configured for this endpoint

passwordParameter (optional)

String

Password parameter configured for this endpoint

Evaluation

riskFactors (optional)

array[String]

Additional risk factors contributing to the total risk score.

recordType (optional)

String

Type of login evidence.

reputation (optional)

array[String]

IP reputation as classified by the proxy.

Evidence

request (optional)

Request

deviceStats (optional)

DeviceStats

evaluation (optional)

Evaluation

EvidenceRequest

piiPassword (optional)

String

Specify the PII password used to encrypt login information. If not specified, the user names will be hashed or encrypted.

example: password

endpointId (optional)

String

Optional: Specify the endpoint ID you would like to fetch information for. If not specified, all endpoints would be used. If no endpoint ID is supplied, the default will be all endpoints.

example: 1234567890

startTime (optional)

Long

Specify the timestamp, in UNIX Epoch milliseconds, from which events are retrieved. format: int64

example: 1644000700000

endTime (optional)

Long

Specify the timestamp, in UNIX Epoch milliseconds, to which events are retrieved. format: int64

example: 1644000702000

rangeHours (optional)

Long

Specify the range, in hours, for which events are retrieved. If specified, range will be used. If not specified,

startTime and endTime will be used instead. format: int64

example: 24

LikelyLeakedEvidence

user (optional)

String

The username of the user sending the login request. If the PII password was specified, the username is returned. If the PII password was not specified or does not match our record, a hashed/encrypted form of the username is returned.

ip (optional)

String

IP address from which the login attempt was made. This will be either an IPv4 (e.g. 50.3.183.2) or normalized IPv6 representation (e.g. 2001:db8:0:0:1:0:0:1).

timestamp (optional)

Long

Timestamp, in UNIX Epoch milliseconds, of the login event. format: int64

LoginEvent

ip (optional)

String

IP address from which the login attempt was made. This will be either an IPv4 (e.g. 50.3.183.2) or normalized IPv6 representation (e.g. 2001:db8:0:0:1:0:0:1).

risk (optional)

String

Probability that this event was part of an attack, as computed post-factum.

Enum:

LOW
MEDIUM
HIGH
time (optional)

Long

Timestamp, in UNIX Epoch milliseconds, of the login event. format: int64

user (optional)

String

The username, if the PII password was specified, or a hashed/encrypted form of the username if the PII password was not specified or does not match.

type (optional)

String

Reason for the presence of the login event in the report.

Enum:

LEAKED

COMPROMISED

path (optional)

String

The login request endpoint path.

referrer (optional)

String

The URL of the referring page.

endpointId (optional)

String

The endpoint ID associated with the login request.

LoginsTimeline

startTime (optional)

Long

Starting timestamp in UNIX Epoch milliseconds from which this timeline data begins. format: int64

example: 1673624384997

intervalMs (optional)

Long

Time interval between data points in milliseconds. format: int64

example: 300000

endpointId (optional)

String

The endpoint ID related to this login timeline.

example: 1616877031

timeline

map[String, RequestTimeline]

MitigationRequest

endpointId (optional)

String

Endpoint ID associated with this request.

lowAction (optional)

String

Mitigation action configured for low risk requests - in UPPER CASE.

Enum:

NONE

CAPTCHA

BLOCK

TARPIT

mediumAction (optional)

String

Mitigation action configured for medium risk requests - in UPPER CASE.

Enum:

NONE

CAPTCHA

BLOCK

TARPIT

highAction (optional)

String

Mitigation action configured for high risk requests - in UPPER CASE.

Enum:

NONE

CAPTCHA

BLOCK

TARPIT

PiiConfigPassword

current (optional)

String

Current password.

proposed (optional)

String

Proposed password.

ReportRequest

startTime (optional)

Long

Specify the timestamp, in UNIX Epoch milliseconds, from which events are retrieved. format: int64

limit (optional)

Integer

Specify the maximum number of events in the report (maximum 10000, default 10000). format: int32

example: 10

piiPassword (optional)

String

Specify the PII password used to encrypt login information. If not specified, the user names will be hashed or encrypted in the response.

endpointId (optional)

String

Optional: Specify the endpoint ID to fetch information for. If no endpoint ID is specified, details of all endpoints defined for the website are returned.

Request

user (optional)

String

The username of the user sending the login request. If the PII password was specified, the username is returned. If the PII password was not specified or does not match our record, a hashed/encrypted form of the username is returned.

client (optional)

String

The client application used to send the request.

declaredClient (optional)

String

The client application used to send the request, according to the declaration in the UserAgent HTTP header.

clients (optional)

array[String]

All client applications used to send requests during the specified timeframe.

declaredClients (optional)

array[String]

All client applications used to send requests during the specified timeframe, according to the declaration in the UserAgent HTTP header.

requestId (optional)

Long

A unique identifier assigned to the request. format: int64

sessionId (optional)

Long

A unique identifier assigned to the session. format: int64

ip (optional)

String

IP address from which the login attempt was made. This will be either an IPv4 (e.g. 50.3.183.2) or normalized IPv6 representation (e.g. 2001:db8:0:0:1:0:0:1).

timestamp (optional)

Long

Timestamp, in UNIX Epoch milliseconds, of the login event. format: int64

path (optional)

String

The login request endpoint path.

country (optional)

String

Country code where the login attempt was made.

referrer (optional)

String

The URL of the referring page.

userAgent (optional)

String

The user agent of the login event.

RequestTimeline

total (optional)

Long

Total requests for the current time span selection. format: int64

example: 7944

prevTotal (optional)

Long

Total requests for the previous time span selection. format: int64

example: 4532

data (optional)

array[Long]

List where every value is the count of login requests for that time interval. format: int64

example: [5, 1, 0, 0, 0, 75, 2, 1, 0, 0]

SiteStatus

siteld (optional)

Long

The Imperva website ID format: int64

websiteName (optional)

String

The site name (URL)

example: mysite.com

isMitigationOn (optional)

Boolean

The site mitigation status (true/false)

example: true

StatsRequest

startTime (optional)

Long

Specify the timestamp, in UNIX Epoch milliseconds, from which events are retrieved. format: int64

example: 1644000700000

endTime (optional)

Long

Specify the timestamp, in UNIX Epoch milliseconds, to which events are retrieved. format: int64

example: 1644000702000

rangeHours (optional)

Long

Specify the range, in hours, for which events are retrieved. If specified, range will be used. If not specified,

startTime and endTime will be used instead. format: int64

example: 24

StreamingOutput

SuspiciousSuccessfulEvidence

likelyLeaked (optional)

String

aggregators (optional)

String

suspiciousSuccessful (optional)

String

mitigated (optional)

String

leaked (optional)

String

TopSource

none (optional)

map[String, Long]

Top source by type mapped to a count of requests with risk level "none". format: int64

low (optional)

map[String, Long]

Top source by type mapped to a count of requests with risk level "low". format: int64

medium (optional)

map[String, Long]

Top source by type mapped to a count of requests with risk level "medium". format: int64

high (optional)

map[String, Long]

Top source by type mapped to a count of requests with risk level "high". format: int64

TopStats

client (optional)

TopSource

country (optional)
TopSource
 ip (optional)
TopSource
 ipFingerprint (optional)
TopSource
 reputation (optional)
TopSource

UsersStats

currentTotal (optional)
Integer
 Total number of unique users for the requested time span, as passed in the API model
 "StatsRequest" format: int32
 prevTotal (optional)
Integer
 Total number of unique users for the previous time span, as passed in the API model "StatsRequest"
 (e.g. if time specified in API is 24 hours, then this will return for the previous 24 hours. format: int32)

Advanced Bot Protection API Overview

Terminology differences

The API term **Domain** corresponds to, and is interchangeable with, a **Website** as used in the UI and web based documentation.

The API term **Site** corresponds to and is interchangeable with a **Website Group** as used in the UI and web based documentation.

The API term **Selector** corresponds to and is interchangeable with a **per-Path Policy** as used in the UI and web based documentation.

Besides the Imperva **account**, there is also an Advanced Bot Protection account. They are connected but have their own identifiers that cannot be mixed. In the API, **account** always refers to an ABP account unless otherwise specified.

Updates

When using PUT to update a resource, the entire resource will be replaced and any omitted fields may be deleted. To prevent data loss when performing an update you must GET the resource, update the returned response, and then send the result as the PUT request body.

API compatibility

Previous versions of the API are deprecated when a new version is released. Previous versions will be supported until further notice.

For a client to stay compatible with non breaking changes they need to take the following into account:

- New optional properties and properties with default values may be added to JSON objects used as API request bodies.
- New properties may be added to JSON objects in API response bodies.

-
- Certain sum types (e.g. `enum` and `oneOf`) are documented as open which means new alternatives can be added. The new values will only be present if configured using the API or UI.

Pagination

Resources may be paginated. This is indicated by the inclusion of the 'next' and/or the 'prev' relations in the '`_links`' property. See the **Links** schema documentation.

See also:

[Advanced Bot Protection API Definition](#)

Advanced Bot Protection API

This is the API for onboarding websites into Advanced Bot Protection. For full feature documentation, see [Advanced Bot Protection](#)

Terminology differences

The API term *Domain* corresponds to, and is interchangeable with, a *Website* as used in the UI and web based documentation.

The API term *Site* corresponds to and is interchangeable with a *Website Group* as used in the UI and web based documentation.

The API term *Selector* corresponds to and is interchangeable with a *per-Path Policy* as used in the UI and web based documentation.

Besides the Imperva *account*, there is also an Advanced Bot Protection *account*. They are connected but have their own identifiers that cannot be mixed. In the API, *account* always refers to an ABP account unless otherwise specified.

Updates

When using PUT to update a resource, the entire resource will be replaced and any omitted fields may be deleted. To prevent data loss when performing an update you must GET the resource, update the returned response, and then send the result as the PUT request body.

API compatibility

Previous versions of the API are deprecated when a new version is released. Previous versions will be supported until further notice.

For a client to stay compatible with non breaking changes they need to take the following into account:

-
- New optional properties and properties with default values may be added to JSON objects used as API request bodies.
 - New properties may be added to JSON objects in API response bodies.
 - Certain sum types (e.g. `enum` and `oneOf`) are documented as *open* which means new alternatives can be added. The new values will only be present if configured using the API or UI.

Authentication

See [API Key Management](#) for instructions on how to authenticate to this API.

Pagination

Resources may be paginated. This is indicated by the inclusion of the 'next' and/or the 'prev' relations in the '`_links`' property. See the [Links schema documentation](#).

Version: 0.1.0

BasePath:/botmanagement

Imperva License Agreement

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-api-id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-api-key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Account

- `get /v1/account/{accountId}/default_encryption_key`
- `get /v1/account/{accountId}`

Campaign

- `get /v1/account/{accountId}/campaign`
- `post /v1/account/{accountId}/campaign`
- `delete /v1/campaign/{campaignId}`
- `get /v1/campaign/{campaignId}`
- `put /v1/campaign/{campaignId}`

Condition

- `delete /v1/account/{accountId}/condition`
- `get /v1/account/{accountId}/condition`
- `post /v1/account/{accountId}/condition`
- `get /v1/account/{accountId}/condition/search`
- `get /v1/condition/{conditionId}/children`
- `delete /v1/condition/{conditionId}`
- `get /v1/condition/{conditionId}`
- `put /v1/condition/{conditionId}`
- `post /v1/condition/validate`

Credential

- `get /v1/account/{accountId}/credential`
- `post /v1/account/{accountId}/credential`
- `delete /v1/credential/{credentialId}`
- `get /v1/credential/{credentialId}`

Domain

- `get /v1/account/{accountId}/domain`
- `post /v1/account/{accountId}/domain`
- `delete /v1/domain/{domainId}`
- `get /v1/domain/{domainId}`
- `put /v1/domain/{domainId}`
- `get /v1/site/{siteId}/domain`
- `get /v1/site/{siteId}/domain_priority`
- `put /v1/site/{siteId}/domain_priority`

Encryptionkey

- `get /v1/domain/{domainId}/encryptionkey`
- `post /v1/domain/{domainId}/encryptionkey`
- `delete /v1/encryptionkey/{encryptionKeyId}`

Policy

- `delete /v1/account/{accountId}/policy`
- `get /v1/account/{accountId}/policy`
- `post /v1/account/{accountId}/policy`
- `delete /v1/policy/{policyId}`
- `get /v1/policy/{policyId}/environmental_parameters`
- `get /v1/policy/{policyId}`

- `put /v1/policy/{policyId}`

Preflight

- `post /v1/account/{accountId}/preflight`
- `get /v1/preflight/{preflightId}`
- `post /v1/preflight/{preflightId}/publish`

Publish

- `get /v1/account/{accountId}/publish/latest_successful`
- `post /v1/preflight/{preflightId}/publish`
- `get /v1/publish/{publishId}`

Root

- `get /v1/`

Site

- `get /v1/account/{accountId}/site`
- `post /v1/account/{accountId}/site`
- `get /v1/account/{accountId}/site_priority`
- `put /v1/account/{accountId}/site_priority`
- `delete /v1/site/{siteId}`
- `get /v1/site/{siteId}/environmental_parameters`
- `get /v1/site/{siteId}`
- `put /v1/site/{siteId}`

Snapshot

- `get /v1/account/{accountId}/snapshot`
- `post /v1/account/{accountId}/snapshot`
- `delete /v1/snapshot/{snapshotId}`
- `get /v1/snapshot/{snapshotId}`
- `post /v1/snapshot/{snapshotId}/restore`

Account

```
get /v1/account/{accountId}/default_encryption_key
```

Retrieve the default encryption key for an Account (v1AccountAccountIdDefaultEncryptionKeyGet)
 Retrieve the default encryption key for an Account

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_2](#)

404

The Account can not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/account/{accountId}
```

Retrieve an Account (v1AccountAccountIdGet)
Retrieve an Account

Path parameters

accountId (required)
Path Parameter
— Identifies an Account to operate on.

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_1](#)

404

The Account can not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Campaign

```
get /v1/account/{accountId}/campaign
```

Retrieve the list of all Campaigns belonging to the Account (v1AccountAccountIdCampaignGet)
Retrieves the list of all Campaigns belonging to the Account.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_17](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_17](#)

404

The Account can not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/campaign
```

Create a new Campaign ([v1AccountAccountIdCampaignPost](#))

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateCampaignV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_8](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created [inline_response_201_8](#)

404

The Account can not be found. [ErrorV1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/campaign/{campaignId}
```

Delete a Campaign ([v1CampaignCampaignIdDelete](#))

Path parameters

campaignId (required)
Path Parameter

— Identifies a Campaign to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_8](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

The Campaign was deleted. [inline_response_201_8](#)

404

The Campaign could not be found. [ErrorV1](#)

400

The Campaign could not be deleted because it has attached Domains. The Domains need to be deleted first.
[ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/campaign/{campaignId}
```

Retrieve a Campaign (v1CampaignCampaignIdGet)
Retrieve a Campaign.

Path parameters

campaignId (required)

Path Parameter

— Identifies a Campaign to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_201_8

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK inline_response_201_8

404

The Campaign could not be found. ErrorV1

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/campaign/{campaignId}
```

Update a Campaign (v1CampaignCampaignIdPut)
Replaces a Campaign resource with the given representation.

Path parameters

campaignId (required)

Path Parameter

— Identifies a Campaign to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdateCampaignV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_8](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_8](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The Campaign could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Condition

```
delete /v1/account/{accountId}/condition
```

Delete multiple conditions (v1AccountAccountIdConditionDelete)

Delete multiple conditions at once. All target condition IDs should be explicitly provided in the query. All condition deletion restrictions stay in place: conditions should not be referenced by policies and other conditions.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-

accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

id (required)

Query Parameter

— Condition IDs to be deleted

Return type

ConditionBatchDeleteResponseV1

Example data

Content-Type: application/json

```
{
  "conditions" : [ {
    "id" : "11b7372c-8183-468f-8d40-5f6ff85ea23d",
    "account_id" : "1c180fbc-b5c1-46b0-bf14-b4c7771a7320",
    "name" : "List name",
    "description" : "List description",
    "created_at" : "2020-05-03T14:31:00Z",
    "modified_at" : "2020-05-03T14:31:00Z",
    "owner" : "account"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

All conditions were successfully deleted ConditionBatchDeleteResponseV1

404

The Account could not be found. ErrorV1

default

An unspecified error occurred.

```
get /v1/account/{accountId}/condition
```

Retrieve the list of all Conditions belonging to the Account (v1AccountAccountIdConditionGet)

Retrieves the list of all Conditions belonging to the Account.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_200_7

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK inline_response_200_7

404

The Account could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/condition
```

Create a new Condition (v1AccountAccountIdConditionPost)
Creates a new Condition.

Path parameters

accountId (required)
Path Parameter
— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body CreateConditionV1 (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_201_4

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

OK [inline_response_201_4](#)

404

The Account could not be found. [ErrorV1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/account/{accountId}/condition/search
```

Search for Conditions (`v1AccountAccountIdConditionSearchGet`)

Searches for Conditions belonging to the Account.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

q (optional)

Query Parameter

— Search string that will be matched infix against name and description.

Return type

[inline_response_200_8](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_8](#)

404

The Account could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/condition/{conditionId}/children
```

Retrieve children of a Condition List (v1ConditionConditionIdChildrenGet)

Retrieves children of a Condition List. The children can only be condition references.

Path parameters

conditionId (required)

Path Parameter

— Identifies a Condition to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_18](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_18](#)

404

The Condition could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/condition/{conditionId}
```

Delete a Condition ([v1ConditionConditionIdDelete](#))
Deletes a Condition.

Path parameters

conditionId (required)

Path Parameter

— Identifies a Condition to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_4](#)

404

The Condition could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/condition/{conditionId}
```

Retrieve a Condition (v1ConditionConditionIdGet)

Retrieves a Condition.

Path parameters

conditionId (required)

Path Parameter

— Identifies a Condition to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_4](#)

404

The Condition could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/condition/{conditionId}
```

Update a Condition (v1ConditionConditionIdPut)

Replaces a Condition resource with the given representation.

Path parameters

conditionId (required)

Path Parameter

— Identifies a Condition to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdateConditionV1](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_4](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The Condition could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/condition/validate
```

Validate a Condition literal (v1ConditionValidatePost)
Validates a Condition literal.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ValidateLiteralV1](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_19](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_19](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

default

An unspecified error occurred.

Credential

```
get /v1/account/{accountId}/credential
```

Retrieve access keys for the analysis host API (`v1AccountAccountIdCredentialGet`)

The response is sorted in ascending order of the time the keys were created. It is recommended to try the last (newest) key first and then proceeding backwards in the array, as the most recent is most likely to be active. The Account configuration needs to be published for the analysis host to accept new keys.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

OK [inline_response_200_3](#)

404

The Account can not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/credential
```

Create new Account credentials (v1AccountAccountIdCredentialPost)
No request body is expected as the new credentials are generated automatically.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

The Account credentials were created [inline_response_201](#)

404

The specified Account could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/credential/{credentialId}
```

Delete credentials (v1CredentialCredentialIdDelete)

After credentials have been deleted and the Account configuration has been published, the analysis host will no longer accept it. In order to perform a key rotation you should

1. Create new credentials
 2. Publish the configuration
 3. Delete the old credentials
 4. Publish the configuration
- This is necessary to prevent gaps where the analysis host and integration do not share common credentials. Do not delete the last credentials and publish, as that will make the Analysis Host unreachable until a new set of credentials is added.

Path parameters

credentialId (required)

Path Parameter

— Identifies a Credential to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default

it to the main account's ID.

Return type

[inline_response_201](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201](#)

404

The credentials could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/credential/{credentialId}
```

Retrieve credentials (v1CredentialCredentialIdGet)

Path parameters

credentialId (required)

Path Parameter

— Identifies a Credential to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201](#)

404

The credentials could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Domain

```
get /v1/account/{accountId}/domain
```

Retrieve the list of Domains belonging to the Account (v1AccountAccountIdDomainGet)
The Domains are returned in order from most to least significant.

Path parameters

accountId (required)
Path Parameter
— Identifies an Account to operate on.

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_200_5

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_5](#)

404

The Account could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/domain
```

Create a new Domain (v1AccountAccountIdDomainPost)
If an encryption key is not specified, a new one will be created.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateDomainV1](#) (required)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

201

OK [inline_response_201_2](#)

404

The Account or Site could not be found. [ErrorV1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/domain/{domainId}
```

Delete a domain ([v1DomainDomainIdDelete](#))

The domain will no longer be usable with the Analysis Host.

Path parameters

domainId (required)

Path Parameter

— Identifies a Domain to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_2](#)

404

The Domain could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/domain/{domainId}
```

Retrieve a Domain ([v1DomainDomainIdGet](#))
Retrieve a Domain

Path parameters

domainId (required)

Path Parameter

— Identifies a Domain to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default

it to the main account's ID.

Return type

[inline_response_201_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_2](#)

404

The Domain could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/domain/{domainId}
```

Update a Domain (v1DomainDomainIdPut)

Replaces a Domain resource with the given representation.

Path parameters

domainId (required)

Path Parameter

— Identifies a Domain to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

-
- application/json

Request body

body [UpdateDomainV1](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_2](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/site/{siteId}/domain
```

Retrieve the list of Domains belonging to the Site (v1SiteSiteIdDomainGet)
The Domains are returned in order from most to least significant.

Path parameters

siteld (required)
Path Parameter
— Identifies a Site to operate on.

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_15](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_15](#)

404

The Site could not be found. ErrorV1

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/site/{siteId}/domain_priority
```

Retrieve the Site's Domain priority order (v1SiteSiteldDomainPriorityGet)

The response contains an array of DomainIDs ordered by their priority. Listing all domains in the site returns results in the same order.

Path parameters

siteld (required)

Path Parameter

— Identifies a Site to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_14](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_14](#)

404

The Site could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/site/{siteId}/domain_priority
```

Update the Site's Domain priority order. (`v1SiteSiteIdDomainPriorityPut`)

Sets the priority order of the domains within this site. All domain IDs belonging to the site must be provided exactly once. The first element has the highest priority.

Path parameters

`siteld` (required)

Path Parameter

— Identifies a Site to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body [DomainPriorityV1](#) (required)

Body Parameter

— The new domain priority order.

Query parameters

`caid` (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_200_14

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK inline_response_200_14

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The Site could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Encryptionkey

```
get /v1/domain/{domainId}/encryptionkey
```

Retrieve the token encryption keys for a Domain ([v1DomainDomainIdEncryptionkeyGet](#))

The response is sorted in ascending order of time of creation. It is recommended to try the last (newest) key first and then proceeding backwards in the array, as the latest key is most likely to be active. The account configuration needs to be published for the analysis host to accept new keys.

Path parameters

domainId (required)

Path Parameter

— Identifies a Domain to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_12](#)

Example data

Content-Type: application/json

```
{
  "items" : [ {
    "id" : "6f53cb6d-c19b-43c7-adf5-b0643c37ef24",
    "domain_id" : "eb1b3ff7-d380-457d-a8e0-fe2760572a72",
    "key" : "/ThnbFkVZgqdeqeKkwe77cSWbU0B2ro60QPNyHEjWYsevDvxVpnAz+cFC7W5bHS1kz/5
S+nSCCwvHCpqbRzJNw==",
    "created_at" : "2020-05-03T14:31:00Z"
  }, {
    "id" : "5f3eed88-08c2-44ea-a427-5e5cb188fdf8",
    "domain_id" : "28dcc280-bd2a-46fc-8dd9-92019ebd67cb",
    "key" : "ayOsEl8LsGygQjRDX989cmXylxNg5Quk/D4Py6MVFR11051mAxkq0qsNH9NDCb9lf1tn
dNNhb0Q2dEtQ3pLgmQ==",
    "created_at" : "2021-06-08T00:00:00Z"
  } ],
  "_links" : { }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_12](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/domain/{domainId}/encryptionkey
```

Create a new encryption key for a Domain ([v1DomainDomainIdEncryptionkeyPost](#))

A new encryption key will be created even if the same encryption key material is used by another Domain.

Path parameters

domainId (required)

Path Parameter

— Identifies a Domain to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateEncryptionKeyV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_7](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created [inline_response_201_7](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/encryptionkey/{encryptionkeyId}
```

Delete an encryption key. (v1EncryptionkeyEncryptionkeyIdDelete)

Delete an encryption key for a Domain. Other domains are unaffected.

Path parameters

encryptionkeyId (required)

Path Parameter

— Identifies the Encryption Key to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_7](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Ok [inline_response_201_7](#)

404

The encryption key or Domain was not found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Policy

```
delete /v1/account/{accountId}/policy
```

Delete multiple policies ([v1AccountAccountIdPolicyDelete](#))

Delete multiple policies at once. All target policy IDs should be explicitly provided in the query. All policy deletion restrictions stay in place, like the policy should not be used in a selector

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

id (required)

Query Parameter

— Policy ID to be deleted

Return type

PolicyBatchDeleteResponseV1

Example data

Content-Type: application/json

```
{
  "policies" : [ {
    "id" : "4d6c00cb-cd2a-46b1-9ad4-716bf5b6d96b",
    "account_id" : "187a671f-e335-48b2-8d87-9fa44b008d08",
    "description" : "A simple example",
    "name" : "Example Policy",
    "directives" : [ {
      "action" : "allow",
      "condition_id" : "6cd38028-a172-4ac4-8c60-7cc7e7a1ebf2"
    } ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

All policies were successfully deleted PolicyBatchDeleteResponseV1

404

The Account could not be found. ErrorV1

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/account/{accountId}/policy
```

Retrieve the list of Policies belonging to the Account (v1AccountAccountIdPolicyGet)
Retrieves the list of Policies belonging to the Account.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_6](#)

404

The Account could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/policy
```

Create a new Policy ([v1AccountAccountIdPolicyPost](#))

Creates a new Policy.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreatePolicyV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Policy has been successfully created. [inline_response_201_3](#)

404

The Account could not be found. [ErrorV1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/policy/{policyId}
```

Delete a Policy (v1PolicyPolicyIdDelete)
Deletes a policy

Path parameters

policyId (required)

Path Parameter

— Identifies a Policy to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_3](#)

404

The Policy could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/policy/{policyId}/environmental_parameters
```

Retrieve all environmental parameters used in a Policy (v1PolicyPolicyIdEnvironmentalParametersGet)
Retrieve all environmental parameters used in a Policy

Path parameters

policyId (required)
Path Parameter
— Identifies a Policy to operate on.

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

inline_response_200_11

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_11](#)

404

The Policy could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/policy/{policyId}
```

Retrieve a Policy (v1PolicyPolicyIdGet)
Retrieve a Policy

Path parameters

policyId (required)
Path Parameter
— Identifies a Policy to operate on.

Query parameters

caid (optional)
Query Parameter
— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_3](#)

404

The Policy could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/policy/{policyId}
```

Update a Policy (v1PolicyPolicyIdPut)

Replaces a Policy resource with the given representation.

Path parameters

policyId (required)

Path Parameter

— Identifies a Policy to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdatePolicyV1](#) (required)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

OK [inline_response_201_3](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Preflight

```
post /v1/account/{accountId}/preflight
```

Create a preflight used to publish the configuration to the analysis host (`v1AccountAccountIdPreflightPost`)
In the future the preflight response will contain indications of the modifications that will be applied.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_5](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created [inline_response_201_5](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/preflight/{preflightId}
```

Retrieve a preflight (v1PreflightPreflightIdGet)

Provides information about the modifications that are done when a preflight is published.

Path parameters

`preflightId` (required)

Path Parameter

— Identifies a Preflight to operate on.

Query parameters

`caid` (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_5](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_5](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/preflight/{preflightId}/publish
```

Publishes a preflight (v1PreflightPreflightIdPublishPost)

Publishes the account configuration snapshot contained in the preflight to the analysis host.

Path parameters

`preflightId` (required)

Path Parameter

— Identifies a Preflight to operate on.

Query parameters

`caid` (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_9](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Preflight published. [inline_response_201_9](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Publish

```
get /v1/account/{accountId}/publish/latest_successful
```

Gets the latest successful Publish for the Account (v1AccountAccountIdPublishLatestSuccessfulGet)
Gets the latest successful Publish for the Account. If the account has never been successfully published this endpoint responds with Not Found.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_9](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_9](#)

404

The Account has never been successfully published [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/preflight/{preflightId}/publish
```

Publishes a preflight (v1PreflightPreflightIdPublishPost)

Publishes the account configuration snapshot contained in the preflight to the analysis host.

Path parameters

preflightId (required)

Path Parameter

— Identifies a Preflight to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_9](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Preflight published. [inline_response_201_9](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/publish/{publishId}
```

Retrieve publish information (v1PublishPublishIdGet)

Provides information about a published preflight.

Path parameters

publishId (required)

Path Parameter

— Identifies a Publish to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_9](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_9](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Root

```
get /v1/
```

Retrieve the authenticated Account's ID (v1Get)

Call this endpoint to retrieve an Account ID. The Account is identified by the API credentials. This endpoint is only meant to give the Account ID. Once you have that there is no need to use this endpoint.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Site

```
get /v1/account/{accountId}/site
```

Retrieve the list of Sites belonging to an Account (v1AccountAccountIdSiteGet)
The Sites are returned in order from most to least significant.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_4](#)

404

The Account can not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/site
```

Create a new Site ([v1AccountAccountIdSitePost](#))

In addition to the provided Selectors, a default Selector that matches any path will automatically be created with the lowest priority. A default Policy will be automatically created and assigned to the default Selector.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateSiteV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created [inline_response_201_1](#)

404

The Account can not be found. [ErrorV1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/account/{accountId}/site_priority
```

Retrieve the Account's Site priority order (`v1AccountAccountIdSitePriorityGet`)

The response contains an array of `SiteIds` ordered by their priority. Listing all sites in the account returns results in the same order.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_16](#)

404

The Account could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/account/{accountId}/site_priority
```

Set site priority in this Account (v1AccountAccountIdSitePriorityPut)

Sets the order of the sites within this Account. All site IDs in the account must be provided exactly once.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [SitePriorityV1](#) (required)

Body Parameter

— The new site priority list.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_16](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_16](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The Account could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/site/{siteId}
```

Delete a Site (v1SiteSiteIdDelete)

You must delete all Domains belonging to the Site before it can be deleted.

Path parameters

sitId (required)

Path Parameter

— Identifies a Site to operate on.

Query parameters

caId (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

The Site was deleted. [inline_response_201_1](#)

404

The Site could not be found. [ErrorV1](#)

400

The Site could not be deleted because it has attached Domains. The Domains need to be deleted first. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/site/{siteId}/environmental_parameters
```

Retrieve all environmental parameters used in a Site (v1SiteSitIdEnvironmentalParametersGet)
Retrieve all environmental parameters used in a Site

Path parameters

sitId (required)

Path Parameter

— Identifies a Site to operate on.

Query parameters

caId (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_13](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_13](#)

404

The Site could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/site/{siteId}
```

Retrieve a Site ([v1SiteSitIdGet](#))

Retrieve a Site.

Path parameters

sitId (required)

Path Parameter

— Identifies a Site to operate on.

Query parameters

caId (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_1](#)

404

The Site could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

```
put /v1/site/{siteId}
```

Update a Site ([v1SiteSiteldPut](#))

Replaces a Site resource with the given representation.

Path parameters

siteld (required)

Path Parameter

— Identifies a Site to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdateSiteV1](#) (required)
Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_1](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The Site could not be found. [ErrorV1](#)

429

Rate limit has been exceeded. [ErrorV1](#)

default

An unspecified error occurred.

Snapshot

```
get /v1/account/{accountId}/snapshot
```

Retrieve the list of snapshots belonging to an Account (v1AccountAccountIdSnapshotGet)
Retrieves the list of snapshots belonging to an Account.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_200_10](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_200_10](#)

404

The account could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/account/{accountId}/snapshot
```

Create a snapshot to allow a configuration rollback ([v1AccountAccountIdSnapshotPost](#))
The snapshot is based on the current configuration. It is recommended to publish the configuration before creating a snapshot to make sure that it only contains live configuration.

Path parameters

accountId (required)

Path Parameter

— Identifies an Account to operate on.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateSnapshotV1](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Created [inline_response_201_6](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The account could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
delete /v1/snapshot/{snapshotId}
```

Delete a snapshot (v1SnapshotSnapshotIdDelete)
Deletes a snapshot.

Path parameters

snapshotId (required)

Path Parameter

— Identifies a Snapshot to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_6](#)

404

The snapshot could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
get /v1/snapshot/{snapshotId}
```

Retrieve a snapshot (v1SnapshotSnapshotIdGet)
Retrieves a snapshot.

Path parameters

snapshotId (required)

Path Parameter

— Identifies a Snapshot to operate on.

Query parameters

caid (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_6](#)

404

The snapshot could not be found. [ErrorV1](#)

default

An unspecified error occurred.

```
post /v1/snapshot/{snapshotId}/restore
```

Restore the account configuration to the state in the provided snapshot. (`v1SnapshotSnapshotIdRestorePost`) Restores the account configuration to the state in the provided snapshot. The restored configuration needs to be published to take effect. A snapshot can not be restored if encryption keys for a currently existing domain have changed since the snapshot was created. It can also not be restored if a domain is connected to a CloudWAF website that has been offboarded or moved to a different account.

Path parameters

`snapshotId` (required)

Path Parameter

— Identifies a Snapshot to operate on.

Query parameters

`caid` (optional)

Query Parameter

— Current Account ID. API keys are valid for an account and all of its sub accounts. When working with sub-accounts, this needs to be set to the corresponding Imperva account ID. Not specifying the parameter will default it to the main account's ID.

Return type

[inline_response_201_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [inline_response_201_6](#)

400

Bad request. See the returned error for detailed validation errors. [ErrorV1](#)

404

The snapshot could not be found. [ErrorV1](#)

default

An unspecified error occurred.

Models

Methods

Table of Contents

1. AccountDefaultEncryptionKeyV1

-
- 2. AccountId
 - 3. AccountV1
 - 4. AnalysisSettingsV1
 - 5. AssociatedItemsV1
 - 6. CampaignId
 - 7. CampaignV1
 - 8. CaptchaSettingsPassword
 - 9. CaptchaSettingsV1
 - 10. CaptchaSettingsV1_geetest
 - 11. CaptchaSettingsV1_managed_geetest
 - 12. CaptchaSettingsV1_managed_hcaptcha
 - 13. CaptchaSettingsV1_recaptcha
 - 14. CaptchaSettingsValue
 - 15. CloudWafId
 - 16. CloudWafWebsiteId
 - 17. ConditionBatchDeleteResponseV1
 - 18. ConditionId
 - 19. ConditionRefV1
 - 20. ConditionStateV1
 - 21. ConditionV1
 - 22. CookieModeV1
 - 23. Cookiescope
 - 24. CreateCampaignV1
 - 25. CreateConditionV1
 - 26. CreateDirectiveV1
 - 27. CreateDomainCriteriaV1
 - 28. CreateDomainV1
 - 29. CreateEncryptionKeyV1
 - 30. CreatePolicyV1
 - 31. CreateSelectorV1
 - 32. CreateSiteV1
 - 33. CreateSnapshotV1
 - 34. CredentialId
 - 35. CredentialV1
 - 36. DateTimeWithOffsetV1
 - 37. DerivedId
 - 38. DirectiveAction
 - 39. DirectiveV1
 - 40. DomainCriteriaV1
 - 41. DomainId
 - 42. DomainNamePart
 - 43. DomainPriorityV1
 - 44. DomainV1
-

45. EncryptionKeyId
46. EncryptionKeyMaterial
47. EncryptionKeyV1
48. EnvironmentalParameterV1
49. ErrorV1
50. GeetestDifficultyV1
51. HcaptchaDifficultyV1
52. HeaderNameV1
53. IpLookupModeV1
54. IpLookupModeV1_lookup
55. LatestSuccessfulPublishV1
56. Link
57. Links
58. LogRegionV1
59. MaxRequestsPerMinute
60. MaxRequestsPerSession
61. MaxSessionLength
62. MoiCode
63. MoiValidationResultV1
64. MxHostnameId
65. Name
66. NoJsInjectionPathV1
67. Path
68. PathPrefix
69. PolicyBatchDeleteResponseV1
70. PolicyEnvironmentalParametersV1
71. PolicyId
72. PolicyV1
73. PreflightId
74. PreflightV1
75. PreflightWarningV1
76. ProxyFlagV1
77. ProxyFlagsV1
78. PublishId
79. PublishProgressPercentV1
80. PublishStatusV1
81. PublishV1
82. RateLimitingCustomScope
83. RateLimitingV1
84. Regex
85. RootV1
86. SelectorCriteriaPostbackV1
87. SelectorCriteriaV1

88. SelectorId
89. SelectorV1
90. SiteEnvironmentalParametersV1
91. SiteId
92. SitePriorityV1
93. SiteV1
94. SnapshotId
95. SnapshotV1
96. TagV1
97. Template
98. UnmaskedHeadersV1
99. UpdateCampaignV1
100. UpdateConditionV1
101. UpdateDirectiveV1
102. UpdateDomainV1
103. UpdatePolicyV1
104. UpdateSelectorV1
105. UpdateSiteV1
106. UtcDateTimeV1
107. ValidateLiteralV1
108. WithLinks
109. inline_response_200
110. inline_response_200_1
111. inline_response_200_10
112. inline_response_200_11
113. inline_response_200_12
114. inline_response_200_13
115. inline_response_200_14
116. inline_response_200_15
117. inline_response_200_16
118. inline_response_200_17
119. inline_response_200_18
120. inline_response_200_19
121. inline_response_200_2
122. inline_response_200_3
123. inline_response_200_4
124. inline_response_200_5
125. inline_response_200_6
126. inline_response_200_7
127. inline_response_200_8
128. inline_response_200_9
129. inline_response_201
130. inline_response_201_1

-
131. inline_response_201_2
 132. inline_response_201_3
 133. inline_response_201_4
 134. inline_response_201_5
 135. inline_response_201_6
 136. inline_response_201_7
 137. inline_response_201_8
 138. inline_response_201_9

AccountDefaultEncryptionKeyV1

The default encryption key for an ABP Account.

account_id
AccountId
 default_encryption_key
EncryptionKeyMaterial

AccountId

Identifies an Account

AccountV1

The ABP Account.

id
AccountId
 my_account_id
Integer
 The corresponding Imperva account. format: int32
 name
String
 The name of the account in ABP. The name is not guaranteed to match the name of the corresponding Imperva account.
 created_at (optional)
 oneOf:
 UtcDateTimeV1
 modified_at (optional)
 oneOf:
 UtcDateTimeV1

AnalysisSettingsV1

Settings that control the traffic on the Analysis Host.

rate_limiting
RateLimitingV1
 max_requests_per_minute (optional)
MaxRequestsPerMinute
 max_requests_per_session (optional)
MaxRequestsPerSession
 max_session_length (optional)
MaxSessionLength
 use_site_rate_limiting_parameters (optional)
Boolean

Apply default values from the website group
example: true

AssociatedItemsV1

Items attached to a Campaign site

array[Siteld]

List of Site ids to be attached to a Campaign

CampaignId

Identifies a Campaign

CampaignV1

id
CampaignId
 account_id
AccountId
 name
Name
 start
DateTimeWithOffsetV1
 end
DateTimeWithOffsetV1
 associated_items
 oneOf:
AssociatedItemsV1
 created_at
UtcDateTimeV1
 modified_at
UtcDateTimeV1

CaptchaSettingsPassword

CaptchaSettingsV1

Configures the type of CAPTCHA to use. The list is considered open and may be expanded in the future. Clients must handle new alternatives gracefully.

CaptchaSettingsV1_geetest

geetest_captcha_id
CaptchaSettingsValue
 geetest_private_key
CaptchaSettingsPassword

CaptchaSettingsV1_managed_geetest

difficulty
GeetestDifficultyV1

CaptchaSettingsV1_managed_hcaptcha

difficulty
HcaptchaDifficultyV1

CaptchaSettingsV1_recaptcha

recaptcha_site_key
CaptchaSettingsValue
recaptcha_secret_key
CaptchaSettingsPassword

CaptchaSettingsValue**CloudWafId**

Customer-facing identification of a CloudWAF website. This ID is preferred over the deprecated CloudWafWebsiteId.

CloudWafWebsiteId

Identifies a CloudWAF website. Deprecated in favor of the customer-facing CloudWafId.

ConditionBatchDeleteResponseV1

conditions
array[ConditionV1]

ConditionId

Identifies a Condition

ConditionRefV1

Reference to a condition literal or list by id

ConditionStateV1

<p>The state for a condition reference affects whether the condition is active or not.</p> inactive: The condition will be skipped monitor: The condition will be evaluated and results will be available in logs, but it will not trigger any action active: The condition will be evaluated and may trigger an action

ConditionV1

<p>A Condition is one of:</p> A Moi expression literal A reference to a literal or a list A list of references <p>For more details see the variants</p>

CookieModeV1

Configures the SameSite policy of the ABP cookies.

Cookiescope

The Domain attribute of the Set-Cookie header that is set by the ABP JavaScript. Additionally you may replace the Domain name TLD with \$suffix to set the appropriate Domain when using a prefix criteria.

CreateCampaignV1

The schema to use when creating a new Campaign. It is a strict subset of `<code>Campaign</code>`, only containing fields that are relevant when creating a new object. See `<code>CampaignV1</code>` for additional details on these fields.

```
name
Name
start
DateTimeWithOffsetV1
end
DateTimeWithOffsetV1
associated_items
oneOf:
AssociatedItemsV1
```

CreateConditionV1

The schema to use when creating a Condition. It is a strict subset of `<code>ConditionV1</code>`, only containing fields that are relevant when creating a new object. See `<code>ConditionV1</code>` for additional details on these fields.

CreateDirectiveV1

The schema to use when creating a Directive. Only the Directive Action is specified. The server will create a unique empty condition list for this directive and return its id.

```
action
DirectiveAction
```

CreateDomainCriteriaV1

The Domain Criteria to specify when creating a new Domain.

CreateDomainV1

The schema to use when creating a new Domain. It is a strict subset of `<code>DomainV1</code>`, only containing fields that are relevant when creating a new object. See `<code>DomainV1</code>` for additional details on these fields. Creating a Domain will also trigger the creation of a new encryption key, if `<code>encryption_key_id</code>` is not supplied.

```
site_id
SiteId
challenge_ip_lookup_mode (optional)
oneOf:
IpLookupModeV1
analysis_ip_lookup_mode (optional)
oneOf:
IpLookupModeV1
criteria
CreateDomainCriteriaV1
cookiescope
```

Cookiescope
captcha_settings (optional)

oneOf:

CaptchaSettingsV1

log_region (optional)

oneOf:

LogRegionV1

no_js_injection_paths (optional)

array[NoJsInjectionPathV1]

obfuscate_path (optional)

String

It is recommended to omit this field or set it to null when creating a Domain, which will cause a new value to be generated by the server.

cookie_mode (optional)

oneOf:

CookieModeV1

encryption_key_id (optional)

Provide an ID to copy an already existing key. If <code>null</code>, a copy of the account default encryption key will be used.

oneOf:

EncryptionKeyId

unmasked_headers (optional)

oneOf:

UnmaskedHeadersV1

proxy_flags (optional)

oneOf:

ProxyFlagsV1

filter_out_static_assets (optional)

Boolean

CWAF Only: Prevents certain static asset paths from being analyzed by ABP. Currently, this filters paths matching the following regular expression: ".(js|gif|jpe?g|ico|png|css|svg?z|woff2?|ttf)\$"

enable_mitigation (optional)

Boolean

If set to false, all Conditions in all related Policies will behave as if they were passive. If set to true, all Conditions will behave according to their state (active or passive).

CreateEncryptionKeyV1

Required fields for creating a new encryption key.

key

EncryptionKeyMaterial

CreatePolicyV1

The schema to use when creating a new Policy. It is a strict subset of <code>PolicyV1</code>, only containing fields that are relevant when creating a new object. See <code>PolicyV1</code> for additional details on these fields.

name

Name

description (optional)

String

directives

array[CreateDirectiveV1]

CreateSelectorV1

The schema to use when creating a new Selector. It is a strict subset of SelectorV1, only containing fields that are relevant when creating a new object. See SelectorV1 for additional details on these fields.

policy_id (optional)

oneOf:

PolicyId

criteria

SelectorCriteriaV1

analysis_settings

AnalysisSettingsV1

CreateSiteV1

The schema to use when creating a new Site. It is a strict subset of <code>SiteV1</code>, only containing fields that are relevant when creating a new object. See SiteV1 for additional details on these fields. Creating a Site will also trigger the creation of a default policy which is used by the Site's default Selector.

mx_hostname_id (optional)

Only relevant when creating an Imperva WAF Gateway Site. This should typically be set to null.

oneOf:

MxHostnameId

name

Name

selectors

array[CreateSelectorV1]

default_max_requests_per_minute (optional)

MaxRequestsPerMinute

default_max_requests_per_session (optional)

MaxRequestsPerSession

default_max_session_length (optional)

MaxSessionLength

CreateSnapshotV1

Create a snapshot. The name does not need to be unique.

name

Name

CredentialId

Identifies credentials

CredentialV1

Credential to authenticate with the Analysis Host.

id

CredentialId

account_id

AccountId

secret

byte[]

The Base64 encoded secret. format: byte

created_at

UtcDateTimeV1

modified_at (optional)

oneOf:
UtcDateTimeV1

DateTimeWithOffsetV1

ISO 8601 Date and time with offset from UTC.

DerivedId

A hash of the contents of a <code>SelectorV1</code>. It is used to count requests that hit the Selector.

DirectiveAction

Action to apply in a directive. Must be snake_case.

DirectiveV1

A Directive is a set of conditions coupled with an action to perform when traffic matches said conditions.
action

DirectiveAction
condition_id
ConditionId

DomainCriteriaV1

Matches one or more domain names.

DomainId

Identifies a Domain

DomainNamePart

Domain name or part of a domain name.

DomainPriorityV1

Domain IDs ordered by their priority within a Site.

domain_ids
array[DomainId]

The domain IDs in order of priority. The first element has the highest priority.

DomainV1

A Domain object maps to one or more domain names. Multiple Domains can be grouped together in a Site.
Additional documentation is available on the Imperva documentation website.

id
DomainId
account_id
AccountId

site_id
SiteId
challenge_ip_lookup_mode
IpLookupModeV1
analysis_ip_lookup_mode
IpLookupModeV1
criteria
DomainCriteriaV1
cookiescope
Cookiescope
captcha_settings
CaptchaSettingsV1
log_region
LogRegionV1
no_js_injection_paths
array[NoJsInjectionPathV1]
Prevents JavaScript injection on the specified paths.
obfuscate_path (optional)
The recommended path to use to load the ABP JavaScript.
oneOf:
Path
mobile_api_obfuscate_path
Path
cookie_mode
CookieModeV1
unmasked_headers
UnmaskedHeadersV1
proxy_flags
ProxyFlagsV1
filter_out_static_assets (optional)
Boolean
CWAF Only: Prevents certain static asset paths from being analyzed by ABP. Currently, this filters paths matching the following regular expression: ".(js|gif|jpe?g|ico|png|css|svg?z|woff2?|ttf)\$"
created_at
UtcDateTimeV1
modified_at
UtcDateTimeV1
enable_mitigation
Boolean
If set to false, all active Conditions in all related Policies will behave as if they were in monitor state. If set to true, all active Conditions will behave according to their state (active or monitor).

EncryptionKeyId

Identifies an encryption key.

EncryptionKeyMaterial

Base64 encoded. At least 24 bytes (32 base64 characters) and at most 64 bytes (88 base64 characters, rounded up). Used to encrypt the ABP cookies.

EncryptionKeyV1

Used to encrypt the ABP cookies.

id
EncryptionKeyId

```
domain_id
DomainId
key
EncryptionKeyMaterial
created_at
UtcDateTimeV1
first_published_at (optional)
oneOf:
UtcDateTimeV1
```

EnvironmentalParameterV1

Environmental parameter that can be used by Conditions

ErrorV1

Generic structure for error responses. The message should not be used for machine parsing. It is meant for display purposes only. Its format and content can change at any time.

message (optional)

String

GetTestDifficultyV1**HcaptchaDifficultyV1****HeaderNameV1**

An HTTP Header name.

IpLookupModeV1

Controls how the Analysis Host determines the IP of the end user.

IpLookupModeV1_lookup

```
header_name
HeaderNameV1
reverse_index
Integer
```

If the header contains multiple comma-separated IP addresses, this controls which IP will be used. format: int32

LatestSuccessfulPublishV1

Describes the most recent account configuration that was successfully published to the Analysis Host.

```
id
PublishId
account_id
AccountId
preflight_id
PreflightId
created_at
UtcDateTimeV1
modified_at
```

UtcDateTimeV1

Link

A relation to another REST resource, following the HAL specification.

href

String

The URI of the resource. If `templated` is `true` the `href` will be a URI Template containing interpolation markers denoted by `{identifier}`, as specified by RFC 6570.

format: uri-template

example: /v1/site/{site_id}

templated (optional)

Boolean

`true` if the `href` is templated. Otherwise the `href` is not templated.

Links

The Links object describes relations. The property is the relation name and the value is the details of the relation.

account (optional)

A related Account resource

oneOf:

Link

analysis_host (optional)

The Analysis Host

oneOf:

Link

condition (optional)

A Condition resource

oneOf:

Link

create_condition (optional)

A relation for creating a new Condition resource. The relation will only be included if the user has permission to create a new Condition.

oneOf:

Link

create_domain (optional)

A relation for creating a new Domain resource. The relation will only be included if the user has permission to create a new Domain.

oneOf:

Link

create_preflight (optional)

A relation for creating a new preflight resource. The relation will only be included if the user has permission to create a new preflight.

oneOf:

Link

create_site (optional)

A relation for creating a new Site resource. The relation will only be included if the user has permission to create a new Site.

oneOf:

Link

create_policy (optional)

A relation for creating a new Policy resource. The relation will only be included if the user has permission to create a new Policy.

oneOf:

Link

create_publish (optional)

A relation for creating a new Publish resource. The relation will only be included if the user has permission to

create a new Policy.

oneOf:

Link

preflight (optional)

A related Preflight resource.

oneOf:

Link

publish (optional)

A related Publish resource.

oneOf:

Link

policy (optional)

A related Policy resource.

oneOf:

Link

delete_policy (optional)

A relation for deleting a Policy resource. The relation will only be included if the user has permission to delete a Policy.

oneOf:

Link

update_policy (optional)

A relation for updating a Policy resource. The relation will only be included if the user has permission to update a Policy.

oneOf:

Link

credential (optional)

A related credential resource.

oneOf:

Link

default_encryption_key (optional)

A relation for retrieving the default encryption key of an Account.

oneOf:

Link

delete_condition (optional)

A relation for deleting a Condition resource. The relation will only be included if the user has permission to delete a Condition.

oneOf:

Link

delete_domain (optional)

A relation for deleting a Domain resource. The relation will only be included if the user has permission to delete a Domain.

oneOf:

Link

delete_encryptionkey (optional)

A relation for deleting an encryption key resource. The relation will only be included if the user has permission to delete an encryption key.

oneOf:

Link

delete_site (optional)

A relation for deleting a Site resource. The relation will only be included if the user has permission to delete a Site.

oneOf:

Link

delete_snapshot (optional)

A relation for deleting a snapshot. The relation will only be included if the user has permissions to delete a snapshot.

oneOf:

Link

domain (optional)

A related Domain resource

oneOf:

Link

domain_priority (optional)

Domain priorities for this site

oneOf:

Link

encryptionkey (optional)

A related encryption key resource

oneOf:

Link

list_conditions (optional)

List all related conditions

oneOf:

Link

list_condition_children (optional)

List all children of a condition

oneOf:

Link

list_credentials (optional)

List all related credentials

oneOf:

Link

list_domains (optional)

List all related Domains

oneOf:

Link

list_policies (optional)

List all related Policies

oneOf:

Link

list_encryptionkeys (optional)

List all related encryption keys

oneOf:

Link

list_sites (optional)

List all related Sites

oneOf:

Link

next (optional)

The resource is paginated, and following the href in the 'next' relation will lead to the next page.

oneOf:

Link

prev (optional)

The resource is paginated, and following the href in the 'prev' relation will lead to the previous page.

oneOf:

Link

search_conditions (optional)

Search for conditions

oneOf:

Link

restore_snapshot (optional)

A relation for restoring a snapshot. The relation will only be included if the user has permissions to change everything in the account.

oneOf:
 Link
 site (optional)
 The related Site resource

oneOf:
 Link
 site_priority (optional)
 Site priorities for this account

oneOf:
 Link
 update_condition (optional)
 A relation for updating a Condition resource. The relation will only be included if the user has permission to update a Condition.

oneOf:
 Link
 snapshot (optional)
 A related snapshot

oneOf:
 Link
 update_domain (optional)
 A relation for updating a Domain resource. The relation will only be included if the user has permission to update a Domain.

oneOf:
 Link
 update_domain_priority (optional)
 A relation for updating Domain priorities for this site. The relation will only be included if the user has permission to update this Site.

oneOf:
 Link
 update_site (optional)
 A relation for updating a Site resource. The relation will only be included if the user has permission to update a Site.

oneOf:
 Link
 update_site_priority (optional)
 A relation for updating Site priorities for this account. The relation will only be included if the user has permission to update this account.

oneOf:
 Link

LogRegionV1

The region where ABP logs are stored.

MaxRequestsPerMinute

Maximum number of requests without a token per minute

MaxRequestsPerSession

Maximum number of requests without a token per session

MaxSessionLength

Maximum length of a session without a token in a moi duration format. Must be positive

MoiCode

An expression in the Moi language

MoiValidationResultV1

Validation result of MOI Code. Either contains the formatted code or a validation error.

MxHostnameId

Only set if the site belongs to the Imperva WAF Gateway. It maps an ABP Site to an MX Hostname.

Name

Free text naming for a resource, used in the user interface and generated reports. The value of this field does not need to be unique and has no effect on ABP functionality.

NoJsInjectionPathV1

Describes a rule for where the ABP JavaScript injection should not occur. The list is considered open and may be expanded in the future. Users of the API must handle new rule types gracefully.

Path

The path portion of a URI. Leading whitespace is stripped and a leading <code>/</code> is added automatically if it's missing.

PathPrefix

Beginning of a path. Must start with /.

PolicyBatchDeleteResponseV1

policies
array[PolicyV1]

PolicyEnvironmentalParametersV1

All environmental parameters used in a Policy
environmental_parameters
array[EnvironmentalParameterV1]

PolicyId

Identifies a Policy

PolicyV1

A Policy is a collection of Directives, containing conditions and actions to apply to matched traffic.
id

```

PolicyId
account_id
AccountId
name
Name
description (optional)
String
An optional user-defined description for this policy.
directives
array[DirectiveV1]
created_at (optional)
oneOf:
UtcDateTimeV1
modified_at (optional)
oneOf:
UtcDateTimeV1

```

PreflightId

Identifies a preflight

PreflightV1

A preflight is a snapshot of the entire Account Configuration. It is required to publish the Account Configuration to the Analysis Host. The preflight may be deleted if the account configuration or external dependent state changes, or if too much time has passed since its creation. Publishing an old preflight can act as a rollback if it is still consistent with any external state.

```

id
PreflightId
account_id
AccountId
created_at
UtcDateTimeV1
modified_at
UtcDateTimeV1
warnings (optional)
oneOf:

```

PreflightWarningV1

A warning about a specific condition in a preflight that may cause some issues or unexpected behaviour. They do not cause errors, but it is recommended to fix these issues if possible. New kinds of warnings may be added in the future.

ProxyFlagV1

A configuration flag for CloudWAF.

ProxyFlagsV1

Configuration flags for CloudWAF.

PublishId

Identifies a published account configuration.

PublishProgressPercentV1

The progress of the publish in percentage.

PublishStatusV1

<p>The status for a publish can be any of the following:</p> in_progress: The publish is in progress completed: The publish has completed successfully failed: The publish failed aborted: The publish was aborted

PublishV1

Indicates that the account configuration was successfully published to the Analysis Host.

`id`

`PublishId`

`account_id`

`AccountId`

`status`

`PublishStatusV1`

`progress_percent`

`PublishProgressPercentV1`

`created_at`

`UtcDateTimeV1`

`preflight_id`

`PreflightId`

`modified_at`

`UtcDateTimeV1`

RateLimitingCustomScope**RateLimitingV1**

Controls the scope for which rate limiting is applied.

Regex

The supported regular expression format is specified here.

RootV1

Contains an authenticated Account's ID

`account_id`

`AccountId`

SelectorCriteriaPostbackV1

SelectorCriteriaV1

A Criteria matches an aspect of an incoming request. If the Criteria matches, then the Selector it belongs to will be selected.

SelectorId

Identifies a Selector

SelectorV1

A Selector contains a Criteria that will be matched against the request. If the Criteria matches, the Policy pointed to by the Selector will be applied.

`id`

`SelectordId`

`policy_id` (optional)

The ID of the Policy to be applied if this Selector is the first Selector in the list of Selectors for a Site that matches a request. If the ID is `<code>null</code>` then no Policy will be applied to matching requests. This is, for example, useful to prevent protection on static assets.

`oneOf:`

`PolicyId`

`criteria`

`SelectorCriteriaV1`

`analysis_settings`

`AnalysisSettingsV1`

`derived_id` (optional)

`oneOf:`

`DerivedId`

`created_at` (optional)

`oneOf:`

`UtcDateTimeV1`

`modified_at` (optional)

`oneOf:`

`UtcDateTimeV1`

SiteEnvironmentalParametersV1

All environmental parameters used in all Policies used by a Site

`environmental_parameters`

`array[EnvironmentalParameterV1]`

SiteId

Identifies a Site

SitePriorityV1

Site IDs ordered by their priority within an Account.

`site_ids`

`array[SiteId]`

The site IDs in order of priority. The first element has the highest priority.

SiteV1

A Site represents a logical website to which a number of domains can be attached. The Site object maps specific paths and path patterns, called Selectors, to Policies.

id

SiteId

account_id

AccountId

mx_hostname_id (optional)

oneOf:

MxHostnameId

name

Name

selectors

array[SelectorV1]

A list of Selectors in priority order, such that the first Selector that matches the incoming request will decide the Policy that will be applied.

created_at (optional)

oneOf:

UtcDateTimeV1

modified_at (optional)

oneOf:

UtcDateTimeV1

default_max_requests_per_minute (optional)

MaxRequestsPerMinute

default_max_requests_per_session (optional)

MaxRequestsPerSession

default_max_session_length (optional)

MaxSessionLength

SnapshotId

Identifies a Snapshot

SnapshotV1

A snapshot of an account that allows restoring the configuration to a previous state.

id

SnapshotId

account_id

AccountId

name

Name

created_at

UtcDateTimeV1

valid_until

UtcDateTimeV1

TagV1

A freetext tag that can only contain valid snake_case. In other words, it always matches <code>^[_a-z][_a-zA-Z0-9]*\$</code>.

Template

The template to be used when creating and editing the condition. This field controls which editor will show up in the configuration UI. This is an open enumeration. Defaults to custom.

UnmaskedHeadersV1

CloudWAF masks certain header values from ABP. To prevent the masking, headers can be specified here. Entries are compared case-insensitively and duplicates will be merged.

UpdateCampaignV1

The schema to use when updating a Campaign. It is a strict subset of `<code>Campaign</code>`, only containing fields that are relevant when updating an object. See `<code>CampaignV1</code>` for additional details on these fields.

```
name
Name
start
DateTimeWithOffsetV1
end
DateTimeWithOffsetV1
associated_items
oneOf:
AssociatedItemsV1
```

UpdateConditionV1

The schema to use when updating a Condition. It is a strict subset of `<code>ConditionV1</code>`, only containing fields that are relevant when creating a new object. See `<code>ConditionV1</code>` for additional details on these fields.

UpdateDirectiveV1

```
action
DirectiveAction
condition_id (optional)
oneOf:
ConditionId
```

UpdateDomainV1

```
site_id
SiteId
challenge_ip_lookup_mode
IpLookupModeV1
analysis_ip_lookup_mode
IpLookupModeV1
cookiescope
Cookiescope
captcha_settings
CaptchaSettingsV1
log_region
LogRegionV1
no_js_injection_paths
```

array[NoJsInjectionPathV1]
obfuscate_path (optional)

String

If <code>obfuscate_path</code> already has a value for this Domain, omitting the field or setting it to <code>null</code> will result in a 400 Bad Request.

cookie_mode

CookieModeV1

unmasked_headers

UnmaskedHeadersV1

proxy_flags

ProxyFlagsV1

filter_out_static_assets (optional)

Boolean

CWAF Only: Prevents certain static asset paths from being analyzed by ABP. Currently, this filters paths matching the following regular expression: ".(js|gif|jpe?g|ico|png|css|svg?z|woff2?|ttf)\$"

enable_mitigation (optional)

Boolean

If set to false, all Conditions in all related Policies will behave as if they were passive. If set to true, all Conditions will behave according to their state (active or passive).

UpdatePolicyV1

name

Name

description (optional)

String

directives

array[UpdateDirectiveV1]

UpdateSelectorV1

The schema to use when updating Selectors in a Site. It is a strict subset of SelectorV1, only containing fields that are relevant when updating a site. See SelectorV1 for additional details on these fields.

id (optional)

oneOf:

SelectorId

policy_id (optional)

oneOf:

PolicyId

criteria

SelectorCriteriaV1

analysis_settings

AnalysisSettingsV1

UpdateSiteV1

name

Name

selectors

array[UpdateSelectorV1]

A list of Selectors in priority order, such that the first Selector that matches the incoming request will decide the Policy that will be applied. In addition to the provided Selectors, a default Selector will be created with the lowest priority. It will match any path and apply the default policy.

default_max_requests_per_minute (optional)

MaxRequestsPerMinute

default_max_requests_per_session (optional)

MaxRequestsPerSession
default_max_session_length (optional)
MaxSessionLength

UtcDateTimeV1

ISO 8601 Date and time in UTC.

ValidateLiteralV1

The schema to use when validating a Condition literal. It is a strict subset of <code>ConditionV1</code>, only containing fields that are relevant when validating a literal.

name
Name
description
String
code
MoiCode

WithLinks

The <code>_links</code> property contains HAL relations.

_links
Links

inline_response_200

_links
Links
account_id
AccountId

inline_response_200_1

_links
Links
id
AccountId
my_account_id
Integer

The corresponding Imperva account. format: int32

name
String

The name of the account in ABP. The name is not guaranteed to match the name of the corresponding Imperva account.

created_at (optional)
modified_at (optional)

inline_response_200_10

_links
Links
items
array[SnapshotV1]

inline_response_200_11

environmental_parameters
array[EnvironmentalParameterV1]
_links
Links

inline_response_200_12

_links
Links

inline_response_200_13

environmental_parameters
array[EnvironmentalParameterV1]
_links
Links

inline_response_200_14

_links
Links
domain_ids
array[DomainId]
The domain IDs in order of priority. The first element has the highest priority.

inline_response_200_15

_links
Links
items
array[DomainV1]

inline_response_200_16

_links
Links
site_ids
array[SiteId]
The site IDs in order of priority. The first element has the highest priority.

inline_response_200_17

An object containing the array of Campaigns.

_links
Links

inline_response_200_18

_links
Links
items

array[ConditionV1]

inline_response_200_19

_links
Links

inline_response_200_2

_links
Links
account_id
AccountId
default_encryption_key
EncryptionKeyMaterial

inline_response_200_3

An object containing the array of credentials.

_links
Links

inline_response_200_4

An object containing the array of Sites.

_links
Links

inline_response_200_5

_links
Links
items
array[DomainV1]

inline_response_200_6

_links
Links
items
array[PolicyV1]

inline_response_200_7

_links
Links
items
array[ConditionV1]

inline_response_200_8

_links

Links
items
array[ConditionV1]

inline_response_200_9

_links
Links
id
PublishId
account_id
AccountId
preflight_id
PreflightId
created_at
UtcDateTimeV1
modified_at
UtcDateTimeV1

inline_response_201

_links
Links
id
CredentialId
account_id
AccountId
secret
byte[]
The Base64 encoded secret. format: byte
created_at
UtcDateTimeV1
modified_at (optional)

inline_response_201_1

_links
Links
id
SitId
account_id
AccountId
mx_hostname_id (optional)
name
Name
selectors
array[SelectorV1]
A list of Selectors in priority order, such that the first Selector that matches the incoming request will decide the Policy that will be applied.
created_at (optional)
modified_at (optional)
default_max_requests_per_minute (optional)
MaxRequestsPerMinute
default_max_requests_per_session (optional)
MaxRequestsPerSession
default_max_session_length (optional)

MaxSessionLength

inline_response_201_2

_links
 Links
 id
 DomainId
 account_id
 AccountId
 site_id
 SiteId
 challenge_ip_lookup_mode
 IpLookupModeV1
 analysis_ip_lookup_mode
 IpLookupModeV1
 criteria

DomainCriteriaV1

cookiescope

Cookiescope

captcha_settings

CaptchaSettingsV1

log_region

LogRegionV1

no_js_injection_paths

array[NoJsInjectionPathV1]

Prevents JavaScript injection on the specified paths.

obfuscate_path (optional)

The recommended path to use to load the ABP JavaScript.

mobile_api_obfuscate_path

Path

cookie_mode

CookieModeV1

unmasked_headers

UnmaskedHeadersV1

proxy_flags

ProxyFlagsV1

filter_out_static_assets (optional)

Boolean

CWAF Only: Prevents certain static asset paths from being analyzed by ABP. Currently, this filters paths matching the following regular expression: ".(js|gif|jpe?g|ico|png|css|svg?z|woff2?)|ttf)\$"

created_at

UtcDateTimeV1

modified_at

UtcDateTimeV1

enable_mitigation

Boolean

If set to false, all active Conditions in all related Policies will behave as if they were in monitor state. If set to true, all active Conditions will behave according to their state (active or monitor).

inline_response_201_3

_links
 Links
 id
 PolicyId
 account_id

```
AccountId
name
Name
description (optional)
String
An optional user-defined description for this policy.
directives
array[DirectiveV1]
created_at (optional)
modified_at (optional)
```

inline_response_201_4

```
_links
Links
```

inline_response_201_5

```
_links
Links
id
PreflightId
account_id
AccountId
created_at
UtcDateTimeV1
modified_at
UtcDateTimeV1
warnings (optional)
```

inline_response_201_6

```
_links
Links
id
SnapshotId
account_id
AccountId
name
Name
created_at
UtcDateTimeV1
valid_until
UtcDateTimeV1
```

inline_response_201_7

```
_links
Links
id
EncryptionKeyId
domain_id
DomainId
key
EncryptionKeyMaterial
created_at
```

UtcDateTimeV1

first_published_at (optional)

inline_response_201_8

```
_links
Links
id
CampaignId
account_id
AccountId
name
Name
start
DateTimeWithOffsetV1
end
DateTimeWithOffsetV1
associated_items
created_at
UtcDateTimeV1
modified_at
UtcDateTimeV1
```

inline_response_201_9

```
_links
Links
id
PublishId
account_id
AccountId
status
PublishStatusV1
progress_percent
PublishProgressPercentV1
created_at
UtcDateTimeV1
preflight_id
PreflightId
modified_at
UtcDateTimeV1
```

Imperva Advanced API Security

This topic describes the API for Imperva Advanced API Security. For full feature documentation, see [Imperva API Security](#).

Version: 1.0.0

BasePath:/api-security

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
-

2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

API

- `post /api/{siteId}`
- `delete /api/{siteId}/{apiId}`
- `get /api`
- `get /api/{siteId}`
- `get /api/{siteId}/all`
- `get /api/{siteId}/{apiId}`
- `get /api/file/{siteId}/{apiId}`
- `post /api/{siteId}/{apiId}`

DiscoveryAccountSettings

- `post /v2/discovery/account/settings/auth-parameter-location`
- `delete /v2/discovery/account/settings`
- `get /v2/discovery/account/settings`
- `post /v2/discovery/account/settings`

DiscoveryHosts

- `get /v2/discovery/hosts`

DiscoveryInventory

- `get /v2/discovery/inventory/endpoints/files`
- `get /v2/discovery/inventory/endpoints`
- `get /v2/discovery/inventory/endpoints/{endpointId}`
- `delete /v2/discovery/inventory/endpoints/risks`

DiscoverySiteSettings

- `get /v2/discovery/sites/{siteId}/settings`
- `get /v2/discovery/sites/settings`
- `post /v2/discovery/sites/{siteId}/settings`
- `post /v2/discovery/sites/settings`

DiscoveryStatistics

- `get /v2/discovery/statistics/classification/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/usage/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/geolocation/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/volume/from/{from-timestamp}/to/{to-timestamp}`

Endpoint

- `get /endpoint/{apiId}`
- `get /endpoint/{apiId}/{endpointId}`
- `post /endpoint/{apiId}/{endpointId}`

SiteConfiguration

- `get /config/site`
- `get /config/site/{siteId}`
- `post /config/site/{siteId}`

Verification

- `delete /v2/shift-left/actions/{actionId}`
- `get /v2/shift-left/actions/{actionId}/actionType/{actionTypeId}`
- `get /v2/shift-left/actions/action-types`
- `get /v2/shift-left/actions`
- `post /v2/shift-left/files/discovery`
- `post /v2/shift-left/files/oas`

API

```
post /api/{siteId}
```

Add an API (addApi)
 Adds an API specification to a site

Path parameters

`siteId` (required)
 Path Parameter
 — The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

apiSpecification (required)

Form Parameter

— format: binary

basePath (required)

Form Parameter

— description (required)

Form Parameter

oasFileName (required)

Form Parameter

specificationViolationAction (required)

Form Parameter

validateHost (required)

Form Parameter

violationActions (required)

Form Parameter

Return type

AddApiResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "duplicateEndpointsList" : [ {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    }, {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    } ],
    "resultMessage" : "API 10 was added successfully",
    "apiId" : 1234
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [AddApiResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

409

API Conflict [SimpleTextErrorResponse](#)

422

Failed to parse the API specification document [ParserErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
delete /api/{siteId}/{apiId}
```

Delete an API (deleteApi)

Deletes an API from a site in the account

Path parameters

apild (required)

Path Parameter

— The API ID format: int64

siteld (required)

Path Parameter

— The site ID format: int64

Return type

[SimpleTextSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [SimpleTextSuccessResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api
```

Retrieve all APIs for the account (getAllApis)

Retrieves details of all protected APIs for all sites in the account

Return type

[GetApisResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : [ {  
    "apiSource" : "USER",  
    "hostName" : "example.com",  
    "siteName" : "example.com",  
    "url" : "https://example.com/api/v1/authn"  
  } ]  
}
```

```

"oasFileName" : "bank.yaml",
"basePath" : "/api",
"creationTime" : 1556735907,
"siteId" : 1234567,
"siteName" : "example.com",
"description" : "This is an example API",
"violationActions" : {
    "otherTrafficViolationAction" : "ALERT_ONLY",
    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"lastModified" : 1556735907,
"specificationViolationAction" : "ALERT_ONLY"
}, {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "creationTime" : 1556735907,
    "siteId" : 1234567,
    "siteName" : "example.com",
    "description" : "This is an example API",
    "violationActions" : {
        "otherTrafficViolationAction" : "ALERT_ONLY",
        "invalidMethodViolationAction" : "ALERT_ONLY",
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY",
        "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907,
    "specificationViolationAction" : "ALERT_ONLY"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisResponse](#)

500

Internal error SimpleTextErrorResponse

```
get /api/{siteId}
```

Retrieve all APIs for a site (getAllSiteApis)

Retrieves details of all protected APIs for a specific site in the account

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

Return type

[GetApisResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "creationTime" : 1556735907,
    "siteId" : 1234567,
    "siteName" : "example.com",
    "description" : "This is an example API",
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907,
    "specificationViolationAction" : "ALERT_ONLY"
  }, {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "creationTime" : 1556735907,
    "siteId" : 1234567,
    "siteName" : "example.com",
    "description" : "This is an example API",
  }
]
```

```

"violationActions" : {
    "otherTrafficViolationAction" : "ALERT_ONLY",
    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"lastModified" : 1556735907,
"specificationViolationAction" : "ALERT_ONLY"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/{siteId}/all
```

Retrieve all APIs and endpoints for a site (getAllSiteApisWithEndpoints)

Retrieves details of all protected APIs and their endpoints for a specific site in the account

Path parameters

`siteld` (required)

Path Parameter

— The site ID format: int64

Return type

[GetApisWithEndpointsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "endpoints" : [ {
      "path" : "/api/{param}",
      "sensitiveDataClassificationList" : [ {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      }, {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      } ],
      "method" : "GET",
      "violationActions" : {
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY"
      },
      "id" : 1234,
      "specificationViolationAction" : "ALERT_ONLY",
      "duplicateOfEndpointId" : 1234
    }, {
      "path" : "/api/{param}",
      "sensitiveDataClassificationList" : [ {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      }, {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      } ],
      "method" : "GET",
      "violationActions" : {
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY"
      },
      "id" : 1234,
      "specificationViolationAction" : "ALERT_ONLY",
      "duplicateOfEndpointId" : 1234
    } ],
    "creationTime" : 1556735907,
    "siteName" : "example.com",
    "description" : "This is an example API",
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "otherTrafficViolationAction" : "ALERT_ONLY"
    }
  } ]
}
```

```

    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
  },
  "id" : 1234,
  "lastModified" : 1556735907
}, {
  "apiSource" : "USER",
  "hostName" : "example.com",
  "endpoints" : [ {
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "specificationViolationAction" : "ALERT_ONLY",
    "duplicateOfEndpointId" : 1234
  }, {
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "specificationViolationAction" : "ALERT_ONLY",
    "duplicateOfEndpointId" : 1234
  } ],
  "creationTime" : 1556735907,
  "siteName" : "example.com",
  "description" : "This is an example API",

```

```

"specificationViolationAction" : "ALERT_ONLY",
"oasFileName" : "bank.yaml",
"basePath" : "/api",
"siteId" : 1234567,
"violationActions" : {
    "otherTrafficViolationAction" : "ALERT_ONLY",
    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"lastModified" : 1556735907
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisWithEndpointsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/{siteId}/{apiId}
```

Retrieve an API (getApi)

Retrieves details of a specific API

Path parameters

apild (required)

Path Parameter

— The API ID format: int64

siteld (required)

Path Parameter

— The site ID format: int64

Return type

[GetApiResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "creationTime" : 1556735907,
    "siteId" : 1234567,
    "siteName" : "example.com",
    "description" : "This is an example API",
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907,
    "specificationViolationAction" : "ALERT_ONLY"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApiResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/file/{siteId}/{apiId}
```

Download the API OAS file (getApiFile)

Download the manually uploaded or automatically discovered OAS file for a specific API. If the API source is mixed, the result is the manually uploaded file.

Path parameters

apild (required)

Path Parameter

— The API ID format: int64

siteld (required)

Path Parameter

— The site ID format: int64

Return type

[DownloadApiSpecificationDtoResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [DownloadApiSpecificationDtoResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error SimpleTextErrorResponse

```
post /api/{siteId}/{apiId}
```

Update an API (updateApi)
Updates any or all of the optional parameters.

Path parameters

apild (required)
Path Parameter
— The API ID format: int64
siteld (required)
Path Parameter
— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

apiSpecification (optional)
Form Parameter
— format: binary
description (optional)
Form Parameter
—
oasFileName (optional)
Form Parameter
—
specificationViolationAction (optional)
Form Parameter
—
validateHost (optional)
Form Parameter
—
violationActions (optional)
Form Parameter
—

Return type

AddApiResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "duplicateEndpointsList" : [ {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    }, {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    } ],
    "resultMessage" : "API 10 was added successfully",
    "apiId" : 1234
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [AddApiResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

409

API Conflict [SimpleTextErrorResponse](#)

422

Failed to parse the API specification document [ParserErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

DiscoveryAccountSettings

```
post /v2/discovery/account/settings/auth-parameter-location
```

Add Authentication Location (addAuthLocation)

Adds the Authentication Location for all websites currently configured or to a specific website

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body AuthParameterLocationDto (optional)

Body Parameter

— Authentication location details

Return type

AuthParameterLocationResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "useForFutureWebSites" : true,
    "siteIds" : "1234567",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http-req-header-x-jwt"
  }, {
    "useForFutureWebSites" : true,
    "siteIds" : "1234567",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http-req-header-x-jwt"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success AuthParameterLocationResponse

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
delete /v2/discovery/account/settings
```

Deletes the Discovery account settings (deleteDiscoveryAccountSettings)

Deletes the specific settings of the Discovery account which includes the site settings.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DiscoveryAccountSettings](#) (optional)

Body Parameter

— Discovery Account Settings

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/account/settings
```

Retrieve the Discovery account settings (getDiscoveryAccountSettings)

Retrieves the configuration details for the Discovery account settings associated with the account.

Return type

GetDiscoveryAccountSettingsResponse

Example data

Content-Type: application/json

```
{
  "data" : {
    "dataLabelSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "visible" : true,
      "dataLabel" : "ssn",
      "lastModifiedUser" : "John Doe",
      "sensitive" : true,
      "lastModified" : 1556735907
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "visible" : true,
      "dataLabel" : "ssn",
      "lastModifiedUser" : "John Doe",
      "sensitive" : true,
      "lastModified" : 1556735907
    } ],
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
    }
  }
}
```

```

        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    }
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveryAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/account/settings
```

Update only the changed Discovery account settings (updateDiscoveryAccountSettings)

Updates the configuration details for the changed Discovery account settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DiscoveryAccountSettings](#) (optional)

Body Parameter

— Discovery Account Settings

Return type

[GetDiscoveryAccountSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [
    {
      "dataLabelSettings" : [ {
        "auditString" : "auditString",
        "accountId" : 12345,
        "visible" : true,
        "dataLabel" : "ssn",
        "lastModifiedUser" : "John Doe",
        "sensitive" : true,
        "lastModified" : 1556735907
      }, {
        "auditString" : "auditString",
        "accountId" : 12345,
        "visible" : true,
        "dataLabel" : "ssn",
        "lastModifiedUser" : "John Doe",
        "sensitive" : true,
        "lastModified" : 1556735907
      } ],
      "authenticationEnabled" : true,
      "deprecatedApiSettings" : {
        "deprecatedApiEnabled" : true,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "inactiveForDays" : 100
      },
      "authParameterSettings" : [ {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
      }, {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
      } ],
      "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
      }
    }
  ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveryAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryHosts

```
get /v2/discovery/hosts
```

Retrieves the account's discovered hosts (getHosts)
Retrieves a list of all hosts discovered within a particular account.

Return type

[GetHostsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetHostsResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryInventory

```
get /v2/discovery/inventory/endpoints/files
```

Download all OAS files of the discovered APIs to a compressed ZIP file (getDiscoveredApiFiles)

Download all OAS files of the discovered APIs, for all hosts or selected hosts in the query, to a compressed ZIP file. The ZIP file format is account-<account_id>-api-files.zip and the ZIP file name format is <host_name>-<base_path>-discovery.json. Underscore is used as the delimiter for the basePath.

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/zip

Responses

200

Success

404

Not Found [ApiFailureResponse](#)

500

Internal Server Error [ApiFailureResponse](#)

```
get /v2/discovery/inventory/endpoints
```

Retrieve all discovered endpoints (getDiscoveredEndpoints)

Retrieve all discovered endpoints for the account or for the specified hosts. If no host id is provided - retrieve all discovered endpoints for all hosts

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

Return type

[GetDiscoveredEndpointsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "summary" : {
      "numberOfLabels" : 9,
      "numberOfEndpointsWithRisks" : "{\"OWASP": 1, "other": 20}",
      "numberOfEndpoints" : 7,
      "numberOfResources" : 2,
      "numberOfApiDiscoveryStatuses" : "{\"IN_PROGRESS": 1, "BASELINED": 20, {"OTHER": 2}},
      "numberOfEndpointsWithDataLabels" : "{\"sensitive": 2, "non-sensitive": 5, "total": 7}",
      "numberOfHosts" : 5
    },
    "endpointsNumberByRisk" : [
      {
        "numberOfEndpoints" : 5,
        "risk" : "unauthenticated"
      },
      {
        "numberOfEndpoints" : 5,
        "risk" : "unauthenticated"
      }
    ],
    "endpoints" : [
      {
        "hostName" : "example.com",
        "authenticationInfo" : {
          "authParameterLocations" : [
            {
              "useForFutureWebSites" : true,
              "siteIds" : "1234567",
              "lastModifiedUser" : "John Doe",
              "lastModified" : 1556735907,
              "authParameterLocation" : "http-req-header-x-jwt"
            }
          ]
        }
      }
    ]
  }
}
```

```

    "useForFutureWebSites" : true,
    "siteIds" : "1234567",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http-req-header-x-jwt"
  ],
  "status" : "status"
},
"method" : "GET",
"resource" : "/api/users",
"hostId" : 12345,
"counter" : 0,
"labels" : [ {
  "name" : "generalinfo:email",
  "sensitive" : false
}, {
  "name" : "generalinfo:email",
  "sensitive" : false
} ],
"discoveryDate" : 1657886850000,
"risks" : [ "risks", "risks" ],
"siteId" : 1234567,
"riskTypes" : [ "OWASP", "OWASP" ],
"id" : 1234567890,
"risksInfo" : [ {
  "owaspTag" : "owaspTag",
  "riskType" : "OWASP",
  "risk" : "risk"
}, {
  "owaspTag" : "owaspTag",
  "riskType" : "OWASP",
  "risk" : "risk"
} ],
"baselinedDate" : 1657886850000,
"dataExposureInfo" : {
  "status" : "status"
},
"status" : "BASELINED"
},
{
  "hostName" : "example.com",
  "authenticationInfo" : {
    "authParameterLocations" : [ {
      "useForFutureWebSites" : true,
      "siteIds" : "1234567",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    },
    {
      "useForFutureWebSites" : true,
      "siteIds" : "1234567",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    }
  ],
  "status" : "status"
},
"method" : "GET",
"resource" : "/api/users",
"hostId" : 12345,

```

```
"counter" : 0,
"labels" : [ {
    "name" : "generalinfo:email",
    "sensitive" : false
}, {
    "name" : "generalinfo:email",
    "sensitive" : false
} ],
"discoveryDate" : 1657886850000,
"risks" : [ "risks", "risks" ],
"siteId" : 1234567,
"riskTypes" : [ "OWASP", "OWASP" ],
"id" : 1234567890,
"risksInfo" : [ {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
}, {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
} ],
"baselinedDate" : 1657886850000,
"dataExposureInfo" : {
    "status" : "status"
},
"status" : "BASELINED"
} ],
"endpointsNumberByHost" : [ {
    "hostName" : "example.com",
    "numberOfEndpoints" : 6,
    "hostId" : 12345
}, {
    "hostName" : "example.com",
    "numberOfEndpoints" : 6,
    "hostId" : 12345
} ],
"endpointsNumberByLabel" : [ {
    "numberOfEndpoints" : 1,
    "label" : "generalinfo:email"
}, {
    "numberOfEndpoints" : 1,
    "label" : "generalinfo:email"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveredEndpointsResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/inventory/endpoints/{endpointId}
```

Retrieve detailed information for the endpoint (getEndpointDrillDown)

Path parameters

endpointId (required)

Path Parameter

— endpoint ID format: int64

Return type

[GetEndpointDrillDownResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "hostName" : "example.com",
    "request" : {
      "queryParamList" : [ {
        "dataTypes" : "[\"type\":\"String\", \"children\": [ { \n          \"name\": \"id\", \n          \"dataTypes\": [\"type\" : \"String\", \n            \"labels\": [ \n              { \n                \"name\": \"generalinfo:email\", \n                \"sensitive\": false, \n                \"visible\": true\n              } \n            ] \n          ]\n        ]\n      }, \n      \"name\" : \"id\", \n      \"required\" : false, \n      \"labels\" : [ { \n        \"name\": \"generalinfo:email\", \n        \"sensitive\" : false\n      }, \n      { \n        \"name\" : \"generalinfo:email\", \n        \"sensitive\" : false\n      } \n    ]\n  ]\n} ]\n  }
}
```

```

    },
    {
      "dataTypes" : "[{"type":"String","children":[]},
                    {"name": "id",
                     "required": true,
                     "labels": [{"name": "generalinfo:email", "visible": true}],
                     "sensitive": false},
                  ]]",
      "name" : "id",
      "required" : false,
      "labels" : [ {
        "name" : "generalinfo:email",
        "sensitive" : false
      }, {
        "name" : "generalinfo:email",
        "sensitive" : false
      } ]
    },
    "contentTypeToRequestBody" : {
      "key" : [ null, null ]
    }
  },
  "authenticationInfo" : {
    "authParameterLocations" : [ {
      "useForFutureWebSites" : true,
      "siteIds" : "1234567",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    }, {
      "useForFutureWebSites" : true,
      "siteIds" : "1234567",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    }],
    "status" : "status"
  },
  "method" : "GET",
  "resource" : "/api/users",
  "responses" : {
    "key" : {
      "contentTypeToResponseBody" : {
        "key" : [ null, null ]
      }
    },
    "endpointStatisticsSummary" : {
      "numberOfParametersWithDataLabels" : "{\"sensitive\": 2, \"non-sensitive\": 5, \"total\": 7}",
      "numberOfParametersByDataLabel" : {
        "key" : 0
      }
    },
    "pathParamSegments" : [ {
      "segmentDetails" : [ {
        "dataType" : "DATE"
      }, {
        "dataType" : "DATE"
      }],
      "index" : 1
    }]
  }
}

```

```
        },
        {
            "segmentDetails" : [ {
                "dataType" : "DATE"
            }, {
                "dataType" : "DATE"
            } ],
            "index" : 1
        }],
        "status" : {
            "designIssueReason" : "designIssueReason",
            "name" : "BASELINED",
            "lastModified" : 1556735907
        }
    }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetEndpointDrillDownResponse

400

Bad input error ApiFailureResponse

500

Internal error ApiFailureResponse

```
delete /v2/discovery/inventory/endpoints/risks
```

Relearn risk data (relearnRisk)
Deletes the current risk data and adds new risk data by relearning.

Query parameters

`endpointIds` (optional)

Query Parameter

Query Parameters
— endpointIds

Return type

[ApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
    "data" : { },  
    "meta" : { }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [ApiSuccessResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoverySiteSettings

```
get /v2/discovery/sites/{siteId}/settings
```

Retrieve discovery settings for a site (getSiteDiscoverySettings)
Retrieve discovery settings for a site

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

Return type

[GetSiteDiscoverySettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "discoveryIncludeOnlyPaths" : "[\"/api", "/service\"]",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "responseParameterLimit" : 100,
      "responseParameterWithDataLabelLimit" : 100
    },
    "relatedHosts" : [ {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }, {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    } ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 12345,
    "isDiscoveryEnabled" : true,
    "endpointSettings" : [ {
      "id" : 1234567890,
      "name" : "Default Endpoint"
    } ]
  }
}
```

```

    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
}, {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
} ],
"siteId" : 1234567,
"discoveryExcludePaths" : ["/test"],
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/sites/settings
```

Retrieve the discovery settings for all sites in the account (getSitesDiscoverySettings)
 Retrieve the discovery settings for all sites in the account

Return type

[GetSiteDiscoverySettingsListResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "discoveryIncludeOnlyPaths" : "[\"/api", "/service\"]",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "responseParameterLimit" : 100,
      "responseParameterWithDataLabelLimit" : 100
    },
    "relatedHosts" : [ {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }, {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    } ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 12345,
    "isDiscoveryEnabled" : true,
    "endpointSettings" : [ {
      "hostname" : "example.com",
      "authenticationEnabled" : true,
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data"
    } ]
  } ]
}
```

```

} ,
  {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
  ],
  "siteId" : 1234567,
  "discoveryExcludePaths" : ["[/test]"],
  "lastModifiedUser" : "John Doe",
  "lastModified" : 1556735907
}, {
  "authenticationEnabled" : true,
  "deprecatedApiSettings" : {
    "deprecatedApiEnabled" : true,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "inactiveForDays" : 100
  },
  "siteName" : "example.com",
  "discoveryIncludeOnlyPaths" : ["/api", "/service"],
  "authParameterSettings" : [
    {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    },
    {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }
  ],
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  },
  "relatedHosts" : [
    {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    },
    {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }
  ],
  "isAutomaticDiscoveryApiIntegrationEnabled" : true,
  "accountId" : 12345,
  "isDiscoveryEnabled" : true,
  "endpointSettings" : [
    {

```

```

    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
}, {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
} ],
"siteId" : 1234567,
"discoveryExcludePaths" : ["/test"],
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsListResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/sites/{siteId}/settings
```

Update the site's discovery settings (updateOneSiteDiscoverySettings)
 Update the site's discovery settings with one of the optional parameters for each site

Path parameters

`siteId` (required)

Path Parameter

— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SiteDiscoverySettings` (optional)

Body Parameter

— Discovery settings

Return type

`GetSiteDiscoverySettingsResponse`

Example data

Content-Type: application/json

```
{
  "data" : {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "discoveryIncludeOnlyPaths" : "[\"/api", "/service\"]",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "responseParameterLimit" : 100,
      "responseParameterWithDataLabelLimit" : 100
    },
    "relatedHosts" : [ {
```

```

    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
}, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
} ],
"isAutomaticDiscoveryApiIntegrationEnabled" : true,
"accountId" : 12345,
"isDiscoveryEnabled" : true,
"endpointSettings" : [ {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
}, {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
} ],
"siteId" : 1234567,
"discoveryExcludePaths" : "[\"/test\"]",
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/sites/settings
```

Update the site's discovery settings (updateSitesDiscoverySettings)
 Update the site's discovery settings with one of the optional parameters for each site

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [SiteDiscoverySettings](#) (optional)

Body Parameter

— Discovery settings

Return type

[GetSiteDiscoverySettingsListResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "discoveryIncludeOnlyPaths" : "[\"/api", "/service\"]",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "excessiveDataExposureThreshold" : 100
    }
  } ]
}
```

```

    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  },
  "relatedHosts" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  } ],
  "isAutomaticDiscoveryApiIntegrationEnabled" : true,
  "accountId" : 12345,
  "isDiscoveryEnabled" : true,
  "endpointSettings" : [ {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
  }, {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
  } ],
  "siteId" : 1234567,
  "discoveryExcludePaths" : ["[/test"]",
  "lastModifiedUser" : "John Doe",
  "lastModified" : 1556735907
}, {
  "authenticationEnabled" : true,
  "deprecatedApiSettings" : {
    "deprecatedApiEnabled" : true,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "inactiveForDays" : 100
  },
  "siteName" : "example.com",
  "discoveryIncludeOnlyPaths" : ["/api", "/service"],
  "authParameterSettings" : [ {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  }, {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "enabled" : true
  } ]
}

```

```

    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  } ],
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  },
  "relatedHosts" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }],
  "isAutomaticDiscoveryApiIntegrationEnabled" : true,
  "accountId" : 12345,
  "isDiscoveryEnabled" : true,
  "endpointSettings" : [ {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
  }, {
    "hostname" : "example.com",
    "authenticationEnabled" : true,
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data"
  }],
  "siteId" : 1234567,
  "discoveryExcludePaths" : ["/test"],
  "lastModifiedUser" : "John Doe",
  "lastModified" : 1556735907
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsListResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryStatistics

```
get /v2/discovery/statistics/classification/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' classification statistics ([getDashboardClassificationStatistics](#))
Retrieve account level baselined endpoints' classification statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

Return type

[GetDashboardClassificationStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "topRisksVolumeStatistics" : [ {
```

```

    "volume" : 2,
    "risk" : "Unauthenticated",
    "percent" : 7
}, {
    "volume" : 2,
    "risk" : "Unauthenticated",
    "percent" : 7
} ],
"resourcesClassificationStatistics" : [ {
    "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
    },
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ null, null ]
}, {
    "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
    },
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ null, null ]
} ],
"endpointsClassificationStatistics" : [ {
    "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
    },
    "risks" : [ "risks", "risks" ],
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "risksInfo" : [ {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    }, {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    } ],
    "labels" : [ null, null ]
}, {
    "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
    },
    "risks" : [ "risks", "risks" ],
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "risksInfo" : [ {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    }, {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    } ]
} ]
}

```

```

    } ],
    "labels" : [ null, null ]
  } ],
  "sensitiveClassificationVolumeStatistics" : [ {
    "volume" : 5,
    "label" : "generalinfo:email",
    "percent" : 5
  }, {
    "volume" : 5,
    "label" : "generalinfo:email",
    "percent" : 5
  } ],
  "nonSensitiveClassificationVolumeStatistics" : [ null, null ],
  "labelsIdentified" : {
    "trendPercent" : 1,
    "currentCount" : 0,
    "trendDirection" : "UP",
    "previousCount" : 6
  },
  "allClassificationVolumeStatistics" : [ null, null ],
  "hostsClassificationStatistics" : [ {
    "hostDetails" : {
      "hostname" : "example.com"
    },
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ {
      "name" : "generalinfo:email",
      "sensitive" : false
    }, {
      "name" : "generalinfo:email",
      "sensitive" : false
    } ]
  }, {
    "hostDetails" : {
      "hostname" : "example.com"
    },
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ {
      "name" : "generalinfo:email",
      "sensitive" : false
    }, {
      "name" : "generalinfo:email",
      "sensitive" : false
    } ]
  } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDashboardClassificationStatisticsSuccessfulResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/statistics/usage/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' usage statistics ([getDashboardGeneralStatistics](#))

Retrieve account level baselined endpoints' usage statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host IDs

Return type

[GetDashboardGeneralStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "clientApps" : 6,
    "clientCountries" : 5,
    "clientUserAgents" : 1,
    "apiCalls" : 0
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDashboardGeneralStatisticsSuccessfulResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/statistics/geolocation/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' geolocation statistics (getDashboardGeolocationStatistics)
Retrieve account level baselined endpoints' geolocation statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

Return type

[GetDashboardGeolocationStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "clientGeolocationCountryStatisticsDto" : [ {
      "code" : "US",
      "currentCallVolume" : 0,
      "name" : "United States",
      "currentCallPercent" : 6
    }, {
      "code" : "US",
      "currentCallVolume" : 0,
      "name" : "United States",
      "currentCallPercent" : 6
    } ],
    "destinationGeolocationCountryStatisticsDto" : [ null, null ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDashboardGeolocationStatisticsSuccessfulResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/statistics/volume/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' volume statistics (`getDashboardVolumeStats`)
Retrieve account level baselined endpoints' volume statistics

Path parameters

`from-timestamp` (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

`to-timestamp` (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

Return type

GetDashboardVolumeStatisticsSuccessfulResponse

Example data

Content-Type: application/json

```
{
  "data" : {
    "resourcesVolumeStatistics" : [ {
      "currentCallVolume" : 1,
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 5
    }, {
      "currentCallVolume" : 1,
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 5
    } ],
    "endpointsVolumeStatistics" : [ {
      "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
      },
      "currentCallVolume" : 5,
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 2
    }, {
      "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
      },
      "currentCallVolume" : 5,
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 2
    } ],
    "hostsResourceStatTrend" : {
      "trendPercent" : 1,
      "trendType" : "Up"
    }
  }
}
```

```
        "currentCount" : 0,
        "trendDirection" : "UP",
        "previousCount" : 6
    },
    "hostsVolumeStatistics" : [ {
        "hostDetails" : {
            "hostname" : "example.com"
        },
        "currentCallVolume" : 0,
        "isFirstTimeSeenInCurrentTimePeriod" : true,
        "currentCallPercent" : 6
    }, {
        "hostDetails" : {
            "hostname" : "example.com"
        },
        "currentCallVolume" : 0,
        "isFirstTimeSeenInCurrentTimePeriod" : true,
        "currentCallPercent" : 6
    } ]
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetDashboardVolumeStatisticsSuccessfulResponse

400

Bad input error ApiFailureResponse

500

Internal error ApiFailureResponse

Endpoint

get /endpoint/{apiId}

Retrieve all endpoints (getAllUserFacingEndpoints)
Retrieve details on all endpoints for an API

Path parameters

apild (required)
 Path Parameter
 — The API ID format: int64

Return type

GetEndpointsResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "specificationViolationAction" : "ALERT_ONLY",
    "duplicateOfEndpointId" : 1234
  }, {
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    }
  }
}
```

```

},
"id" : 1234,
"specificationViolationAction" : "ALERT_ONLY",
"duplicateOfEndpointId" : 1234
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetEndpointsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /endpoint/{apiId}/{endpointId}
```

Retrieve an endpoint (getUserFacingEndpoint)
Retrieve details for an endpoint

Path parameters

apild (required)

Path Parameter

— The API ID format: int64

endpointId (required)

Path Parameter

— The endpoint ID format: int64

Return type

[GetEndpointResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "specificationViolationAction" : "ALERT_ONLY",
    "duplicateOfEndpointId" : 1234
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetEndpointResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
post /endpoint/{apiId}/{endpointId}
```

Update an endpoint (updateEndpoint)
 Update an endpoint API Specification Violation Action

Path parameters

apild (required)
 Path Parameter
 — The API ID format: int64
 endpointId (required)
 Path Parameter
 — The endpoint ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

specificationViolationAction (optional)
 Form Parameter

—
 violationActions (optional)
 Form Parameter

Return type

[UpdateEndpointResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "endpointId" : 1234567890
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateEndpointResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

SiteConfiguration

```
get /config/site
```

Retrieves all site configurations (getSiteConfigurationForAccount)
Retrieves configuration settings for all sites in the account.

Query parameters

`filterActiveOnly` (optional)
Query Parameter

Return type

[GetSiteConfigurationsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludebasePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 6,
    "discoveryEnabled" : true,
    "siteId" : 0,
    "siteName" : "example.com",
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludebasePath" ],
    "lastModified" : 1556735907,
    "accountName" : "Thales Group"
  } ]
}
```

```

    "apiOnlySite" : true
  } , {
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludeB
asePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 6,
    "discoveryEnabled" : true,
    "siteId" : 0,
    "siteName" : "example.com",
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludeB
asePath" ],
    "lastModified" : 1556735907,
    "apiOnlySite" : true
  } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteConfigurationsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /config/site/{siteId}
```

Retrieves a site configuration (getSiteConfigurationForSite)
 Retrieves the configuration settings for a specific site

Path parameters

`sitId` (required)
 Path Parameter
 — The site ID format: int64

Return type

`GetSiteConfigurationResponse`

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludebasePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 6,
    "discoveryEnabled" : true,
    "siteId" : 0,
    "siteName" : "example.com",
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludebasePath" ],
    "lastModified" : 1556735907,
    "apiOnlySite" : true
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

Success `GetSiteConfigurationResponse`

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
post /config/site/{siteId}
```

Updates site configuration (updateSiteConfiguration)

Updates the site configuration with settings such as attack policy and more as the optional parameters

Path parameters

`siteId` (required)

Path Parameter

— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body [SiteConfigurationResponse](#) (optional)

Body Parameter

— Settings for attack policy and more

Return type

[UpdateSiteConfigurationResponse](#)

Example data

Content-Type: `application/json`

```
{
  "isError" : false,
  "value" : {
    "siteId" : 12345
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateSiteConfigurationResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

Verification

```
delete /v2/shift-left/actions/{actionId}
```

Delete an action (deleteAction)

Deletes a specified action from the account.

Path parameters

actionId (required)

Path Parameter

— The ActionId format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

No Content

404

Resource not found [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions/{actionId}/actionType/{actionTypeId}
```

Download reports (downloadResults)

Downloads the requested reports for a specified action

Path parameters

actionId (required)

Path Parameter

— Action Id format: int64

actionTypId (required)

Path Parameter

— Action Type Id format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/zip

Responses

200

Success

400

Bad Request [ApiFailureResponse](#)

404

Resource not found [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions/action-types
```

Retrieve all action types for an account (getActionTypes)

Retrieves details of all action types for the account

Return type

[GetActionTypesResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "actionType" : "SECURITY_TEST_PKG",
    "actionTypeId" : 123,
    "actionTypeDisplayName" : "Generate security test"
  }, {
    "actionType" : "SECURITY_TEST_PKG",
    "actionTypeId" : 123,
    "actionTypeDisplayName" : "Generate security test"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

Success [GetActionTypesResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions
```

Retrieve all actions for an account (getActions)
 Retrieves details of all actions for the account

Return type

[GetActionsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "source" : "Discovery",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }, {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    } ]
  }, {
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "source" : "Discovery",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }, {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    } ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetActionsResponse](#)

500

[Internal error ApiFailureResponse](#)

```
post /v2/shift-left/files/discovery
```

Uploads discovered APIs (uploadDiscoveredHostsSpecFiles)

Uploads the OAS file generated by the Discovery engine which contains discovered APIs for a selected host

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **string** (optional)

Body Parameter

— Selected host ids

Return type

[UploadFileSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "source" : "Discovery",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }, {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UploadFileSuccessResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/shift-left/files/oas
```

Upload an OAS file (uploadFile)
Uploads an OAS file manually.

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

actionTypes (optional)
Form Parameter

—
file (optional)
Form Parameter
— format: binary

Return type

[UploadFileSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "source" : "Discovery",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }
  }
}
```

```

        } , {
            "errMsg" : "Error in processing request",
            "id" : 123,
            "type" : "SECURITY_TEST_PKG",
            "status" : "IN_PROGRESS"
        } ]
    }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UploadFileSuccessResponse](#)

400

Bad Request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

Models

Methods

Table of Contents

1. Action
 2. ActionType
 3. ActionTypeMap
 4. AddApiResponse
 5. AddApiResponseValue
 6. ApiFailureResponse
 7. ApiResponse
 8. ApiSuccessResponse
 9. ApiViolationActions
 10. ApiWithEndpointResponse
 11. AuthParameterLocationDto
-

-
- 12. AuthParameterLocationResponse
 - 13. AuthParameterSettings
 - 14. AuthenticationInfo
 - 15. ClassificationRiskVolumeStatistics
 - 16. ClassificationStatistics
 - 17. ClassificationVolumeStatistics
 - 18. DataExposureInfo
 - 19. DataLabelSettings
 - 20. DataTypeDto
 - 21. DeprecatedApiSettings
 - 22. DiscoveredApisSummary
 - 23. DiscoveredEndpoint
 - 24. DiscoveryAccountSettings
 - 25. DownloadApiSpecificationDtoResponse
 - 26. DuplicateEndpointResponse
 - 27. EndpointClassificationStatistics
 - 28. EndpointDetails
 - 29. EndpointDrillDown
 - 30. EndpointResponse
 - 31. EndpointSettingsDto
 - 32. EndpointStatisticsSummary
 - 33. EndpointStatusDrillDownDto
 - 34. EndpointViolationActions
 - 35. EndpointVolumeStatistics
 - 36. EndpointsPerHost
 - 37. EndpointsPerLabel
 - 38. ExcessiveDataExposureSettings
 - 39. GeolocationCountryStatistics
 - 40. GeolocationStatistics
 - 41. GetActionTypesResponse
 - 42. GetActionsResponse
 - 43. GetApiResponse
 - 44. GetApisResponse
 - 45. GetApisWithEndpointsResponse
 - 46. GetDashboardClassificationStatisticsSuccessfulResponse
 - 47. GetDashboardGeneralStatisticsSuccessfulResponse
 - 48. GetDashboardGeolocationStatisticsSuccessfulResponse
 - 49. GetDashboardVolumeStatisticsSuccessfulResponse
 - 50. GetDiscoveredEndpointsResponse
 - 51. GetDiscoveryAccountSettingsResponse
 - 52. GetEndpointDrillDownResponse
 - 53. GetEndpointResponse
 - 54. GetEndpointsResponse
-

55. GetHostsResponse
56. GetSiteConfigurationResponse
57. GetSiteConfigurationsResponse
58. GetSiteDiscoverySettingsListResponse
59. GetSiteDiscoverySettingsResponse
60. Host
61. HostClassificationStatistics
62. HostDetails
63. HostVolumeStatistics
64. InventoryDiscoveryData
65. Label
66. NumberOfEndpointsByRisks
67. ParameterDrillDown
68. ParserErrorResponse
69. PathParamSegments
70. RequestDrillDown
71. ResourceClassificationStatistics
72. ResourceDetails
73. ResourceStatTrend
74. ResourceVolumeStatistics
75. ResponseDrillDown
76. RiskInfo
77. SegmentDetails
78. SensitiveDataClassification
79. SimpleTextErrorResponse
80. SimpleTextSuccessResponse
81. SiteConfigurationResponse
82. SiteDiscoverySettings
83. UpdateEndpointResponse
84. UpdateEndpointResponseValue
85. UpdateSiteConfigurationResponse
86. UpdateSiteConfigurationResponseValue
87. UploadFileSuccessResponse
88. UsageStatistics
89. VolumeStatistics
90. apiId_endpointId_body
91. api_siteId_body
92. files_oas_body
93. siteId_apiId_body

Action

apiBundleName (optional)
String

API Bundle Name

example: Test.zip

source (optional)

String

Source Name

example: Discovery

lastModifiedUser

String

lastModified

Date

format: date-time

actionId (optional)

Long

Action Id format: int64

example: 123

actionTypes (optional)

array[ActionTypeMap]

Action Types

ActionType

actionTypeId (optional)

Long

ActionTypeId format: int64

example: 123

actionType (optional)

String

Action Type

example: SECURITY_TEST_PKG

actionTypeDisplayName (optional)

String

Action Type Display Name

example: Generate security test

ActionTypeMap

id (optional)

Long

Action Type Map Id format: int64

example: 123

type (optional)

String

Action Type

example: SECURITY_TEST_PKG

status (optional)

String

Action Type Map Status

example: IN_PROGRESS

errMsg (optional)

String

Error Message

example: Error in processing request

AddApiResponse

value (optional)

AddApiResponseValue

isError (optional)

Boolean

States if an error occurred

example: false

AddApiResponseValue

apild (optional)

Long

The API specification ID format: int64

example: 1234

resultMessage (optional)

String

Additional information on the action taken

example: API 10 was added successfully

duplicateEndpointsList (optional)

array[DuplicateEndpointResponse]

A list of objects representing duplicate endpoints which were not added as part of the action taken because they exist in another API

ApiFailureResponse

errors

Object**ApiResponse**

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

violationActions (optional)

ApiViolationActions

id (optional)

Long

The API ID format: int64

example: 1234

siteId (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

hostName (optional)

String

The API's host name

example: example.com
basePath (optional)
String
The API's basePath
example: /api
description (optional)
String
The API's description in the dashboard
example: This is an example API
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
creationTime (optional)
Long
The timestamp when this api was created format: int64
example: 1556735907
apiSource (optional)
String
The source from which the API was created
Enum:
USER
DISCOVERY
MIXED
example: USER
oasFileName (optional)
String
Uploaded oas file name
example: bank.yaml

ApiSuccessResponse

data
Object
meta
Object

ApiViolationActions

missingParamViolationAction (optional)
String
The action taken when a missing parameter Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs
Enum:
ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT
example: ALERT_ONLY
invalidParamValueViolationAction (optional)
String
The action taken when an invalid parameter value Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs
Enum:
ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidParamNameViolationAction (optional)

String

The action taken when an invalid parameter name Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidUrlViolationAction (optional)

String

The action taken when an invalid URL Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidMethodViolationAction (optional)

String

The action taken when an invalid method Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

otherTrafficViolationAction (optional)

String

The action taken when traffic that does not belong to the APIs defined in the OAS files or integrated from API Discovery is identified.

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

ApiWithEndpointResponse

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

violationActions (optional)

ApiViolationActions

id (optional)

Long

The API ID format: int64

example: 1234

siteId (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

hostName (optional)

String

The API's host name

example: example.com

basePath (optional)

String

The API's basePath

example: /api

description (optional)

String

The API's description in the dashboard

example: This is an example API

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

creationTime (optional)

Long

The timestamp when this api was created format: int64

example: 1556735907

apiSource (optional)

String

The source from which the API was created

Enum:

USER

DISCOVERY

MIXED

example: USER

oasFileName (optional)

String

Uploaded oas file name

example: bank.yaml

endpoints

array[EndpointResponse]

AuthParameterLocationDto

authParameterLocation (optional)
String
Authentication location name
example: http-req-header-x-jwt
sitelds (optional)
array[Long]
Sitelds format: int64
example: 1234567
useForFutureWebSites (optional)
Boolean
Enable same configuration for future website on-boarding
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe

AuthParameterLocationResponse

data
array[AuthParameterLocationDto]

AuthParameterSettings

authParameterLocation (optional)
String
Authentication location name
example: http->req->header->jwt
accountid (optional)
Long
The account ID format: int64
example: 12345
enabled (optional)
Boolean
Enable or disable the authentication location
example: true
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe
auditString
String

AuthenticationInfo

status (optional)
String

The status of the authentication locations identified
 authParameterLocations (optional)
 array[AuthParameterLocationDto]
 The authentication locations identified

ClassificationRiskVolumeStatistics

risk (optional)
String
 The type of the risk
 example: Unauthenticated
 volume (optional)
Long
 format: int64
 percent (optional)
Integer
 format: int32

ClassificationStatistics

labelsIdentified (optional)
ResourceStatTrend
 labeledHosts (optional)
ResourceStatTrend
 labeledResources (optional)
ResourceStatTrend
 labeledEndpoints (optional)
ResourceStatTrend
 riskyEndpoints (optional)
ResourceStatTrend
 endpointsOWASPTop10Risks (optional)
ResourceStatTrend
 endpointsOtherRisks (optional)
ResourceStatTrend
 hostsClassificationStatistics (optional)
 array[HostClassificationStatistics]
 The collection of hosts which had any label in the time window
 resourcesClassificationStatistics (optional)
 array[ResourceClassificationStatistics]
 The collection of resources which had any label in the time window
 endpointsClassificationStatistics (optional)
 array[EndpointClassificationStatistics]
 The collection of endpoints which had a label in the time window
 sensitiveClassificationVolumeStatistics (optional)
 array[ClassificationVolumeStatistics]
 The collection of endpoints which had sensitive label in the time window
 nonSensitiveClassificationVolumeStatistics (optional)
 array[ClassificationVolumeStatistics]
 The collection of endpoints which had non sensitive label in the time window
 allClassificationVolumeStatistics (optional)
 array[ClassificationVolumeStatistics]
 The collection of endpoints which had both sensitive and non sensitive label in the time window
 topRisksVolumeStatistics (optional)
 array[ClassificationRiskVolumeStatistics]
 The collection of endpoints that had top risks in the time window
 risksIdentified (optional)
ResourceStatTrend

ClassificationVolumeStatistics

label (optional)

String

The name of the label

example: generalinfo:email

volume (optional)

Long

format: int64

percent (optional)

Integer

format: int32

DataExposureInfo

status (optional)

String

The status of the Data Exposure

DataLabelSettings

dataLabel (optional)

String

The data label

example: ssn

accountId (optional)

Long

The account ID format: int64

example: 12345

sensitive (optional)

Boolean

Is this data label sensitive

example: true

visible (optional)

Boolean

Is this data label visible

example: true

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

auditString

String

DataTypeDto

type (optional)

String

The type of the parameter

example: String

children (optional)

array[ParameterDrillDown]

Other ParameterDrillDown that are children of this current parameter

example: "type": "String", "children": [{
 "name": "id",
 "dataTypes": ["type" : "String",
 "required": true,
 "labels": [
 {
 "name": "generalinfo:email",
 "sensitive": false,
 "visible": true
 }
]
 }]

DeprecatedApiSettings

deprecatedApiEnabled (optional)

Boolean

inactiveForDays (optional)

Integer

number of days for which API is inactive format: int32

example: 100

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

DiscoveredApisSummary

numberOfHosts (optional)

Long

The total number of hosts for all endpoints format: int64

numberOfResources (optional)

Long

The total number of resources for all endpoints format: int64

numberOfEndpoints (optional)

Long

The total number of endpoints for the account format: int64

numberOfLabels (optional)

Long

The total number of labels for all endpoints format: int64

numberOfApiDiscoveryStatuses (optional)

map[String, Long]

The number of endpoints per discovery status format: int64

example: {"IN_PROGRESS": 1,"BASELINED": 20,"OTHERS": 2}

numberOfEndpointsWithRisks (optional)

map[String, Long]

The discovered API risks format: int64

example: {"OWASP": 1,"other": 20}

numberOfEndpointsWithDataLabels (optional)

map[String, Long]

Number of sensitive and non-sensitive data labels format: int64

example: {"sensitive": 2,"non-sensitive": 5,"total": 7}

DiscoveredEndpoint

id (optional)

Long

The endpoint ID format: int64

example: 1234567890

labels

array[Label]

method (optional)

String

The endpoint HTTP method

Enum:

POST

GET

PUT

PATCH

DELETE

HEAD

OPTIONS

example: GET

risks (optional)

array[String]

The discovered API risks

risksInfo (optional)

array[RiskInfo]

The discovered API risks' information

authenticationInfo (optional)

AuthenticationInfo

dataExposureInfo (optional)

DataExposureInfo

hostId (optional)

Long

The ID of the host to which endpoint belongs format: int64

example: 12345

siteld (optional)

Long

The ID of the site to which host belongs format: int64

example: 1234567

hostName (optional)

String

The name of the host to which endpoint belongs

example: example.com

resource (optional)

String

The resource (url) to which endpoint belongs

example: /api/users

status (optional)

String

The discovery status for the endpoint

Enum:

BASELINED

IN_PROGRESS

UNDER_INVESTIGATION

DESIGN_ISSUE

example: BASELINED

discoveryDate (optional)

Long

The time when endpoint discovery started format: int64

example: 1657886850000
riskTypes
array[String]
Enum:
counter (optional)
Integer
Counter for endpoint in case of duplicate/multiple endpoints with same path format: int32
baselinedDate (optional)
Long
The time when endpoint got baselined format: int64
example: 1657886850000

DiscoveryAccountSettings

dataLabelSettings (optional)
array[DataLabelSettings]
Data label settings
authenticationEnabled (optional)
Boolean
authParameterSettings (optional)
array[AuthParameterSettings]
Authentication location settings
excessiveDataExposureSettings (optional)
ExcessiveDataExposureSettings
deprecatedApiSettings (optional)
DeprecatedApiSettings

DownloadApiSpecificationDtoResponse

value (optional)
String
isError (optional)
Boolean
States if an error occurred
example: false

DuplicateEndpointResponse

id (optional)
Long
The endpoint ID format: int64
example: 1234567890
fullPath (optional)
String
The endpoint full path
example: /api/{param}
method (optional)
String
The endpoint HTTP method
Enum:
POST
GET
PUT
PATCH
DELETE
HEAD

OPTIONS

example: GET

EndpointClassificationStatistics

endpointDetails (optional)

EndpointDetails

labels (optional)

array[Label]

hostsResourceStatTrend (optional)

ResourceStatTrend

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

risks (optional)

array[String]

The discovered API risks

risksInfo (optional)

array[RiskInfo]

The discovered API risks info

EndpointDetails

endpointId (optional)

Long

The endpoint ID format: int64

example: 1234567890

endpointUrl (optional)

String

The endpoint url

example: /v1/data

hostname (optional)

String

The host's name

example: example.com

method (optional)

String

example: POST

EndpointDrillDown

hostName (optional)

String

The name of the host to which endpoint belongs

example: example.com

method (optional)

String

The method of the endpoint

example: GET

resource (optional)

String

The resource (url) to which endpoint belongs

example: /api/users

authenticationInfo (optional)

AuthenticationInfo

request (optional)

RequestDrillDown

responses (optional)
map[String, ResponseDrillDown]
 endpointStatisticsSummary (optional)
EndpointStatisticsSummary
 status (optional)
EndpointStatusDrillDownDto
 pathParamSegments (optional)
array[PathParamSegments]
 Description of path param segments

EndpointResponse

specificationViolationAction (optional)
String
 The action taken when an API Specification Violation occurs
 Enum:
 ALERT_ONLY
 BLOCK_REQUEST
 BLOCK_USER
 BLOCK_IP
 IGNORE
 DEFAULT
 example: ALERT_ONLY
 violationActions (optional)
EndpointViolationActions
 id (optional)
Long
 The endpoint ID format: int64
 example: 1234
 path (optional)
String
 The endpoint path
 example: /api/{param}
 method (optional)
String
 The endpoint HTTP method
 Enum:
 POST
 GET
 PUT
 PATCH
 DELETE
 HEAD
 OPTIONS
 example: GET
 duplicateOfEndpointId (optional)
Long
 The ID of the endpoint that this endpoint is the duplicate of format: int64
 example: 1234
 sensitiveDataClassificationList (optional)
array[SensitiveDataClassification]
 Sensitive data classification list for this endpoint

EndpointSettingsDto

endpointId (optional)
Long

The endpoint ID format: int64

example: 1234567890

endpointUrl (optional)

String

The endpoint url

example: /v1/data

hostname (optional)

String

The host's name

example: example.com

method (optional)

String

example: POST

authenticationEnabled (optional)

Boolean

excessiveDataExposureSettings (optional)

ExcessiveDataExposureSettings

deprecatedApiSettings (optional)

DeprecatedApiSettings

EndpointStatisticsSummary

numberOfParametersWithDataLabels (optional)

map[String, Integer]

Number of total, sensitive and non-sensitive data labels for all parameters format: int32

example: {"sensitive": 2, "non-sensitive": 5, "total": 7}

numberOfParametersByDataLabel (optional)

map[String, Integer]

Number of parameters for a specific label format: int32

EndpointStatusDrillDownDto

name (optional)

String

Status of endpoint

Enum:

BASELINED

IN_PROGRESS

DESIGN_ISSUE

example: BASELINED

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

designIssueReason (optional)

String

Reason for the DESIGN_ISSUE

EndpointViolationActions

missingParamViolationAction (optional)

String

The action taken when a missing parameter Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidParamValueViolationAction (optional)

String

The action taken when an invalid parameter value Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidParamNameViolationAction (optional)

String

The action taken when an invalid parameter name Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

EndpointVolumeStatistics

endpointDetails (optional)

EndpointDetails

currentCallVolume (optional)

Long

format: int64

currentCallPercent (optional)

Integer

format: int32

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

EndpointsPerHost

hostId (optional)

Long

The host ID format: int64

example: 12345

hostName (optional)

String

The host name

example: example.com

numberOfEndpoints (optional)

Long

The number of endpoints for the specific host format: int64

EndpointsPerLabel

label (optional)

String

The name of the label

example: generalinfo:email

numberOfEndpoints (optional)

Long

The number of endpoints per specific label format: int64

ExcessiveDataExposureSettings

excessiveDataExposureEnabled (optional)

Boolean

responseParameterLimit (optional)

Integer

Response parameters limit format: int32

example: 100

responseParameterWithDataLabelLimit (optional)

Integer

Response parameters with data label limit format: int32

example: 100

responseParameterWithSensitiveDataLabelLimit (optional)

Integer

Response parameters with sensitive data label limit format: int32

example: 100

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

GeolocationCountryStatistics

name (optional)

String

The country name

example: United States

code (optional)

String

The country code

example: US

currentCallVolume (optional)

Long

format: int64

currentCallPercent (optional)

Integer

format: int32

GeolocationStatistics

clientGeolocationCountryStatisticsDto (optional)

array[GeolocationCountryStatistics]

destinationGeolocationCountryStatisticsDto (optional)
array[GeolocationCountryStatistics]

GetActionTypesResponse

data
array[ActionType]

GetActionsResponse

data
array[Action]

GetApiResponse

value (optional)
ApiResponse
isError (optional)
Boolean
States if an error occurred
example: false

GetApisResponse

value (optional)
array[ApiResponse]
isError (optional)
Boolean
States if an error occurred
example: false

GetApisWithEndpointsResponse

value (optional)
array[ApiWithEndpointResponse]
isError (optional)
Boolean
States if an error occurred
example: false

GetDashboardClassificationStatisticsSuccessfulResponse

data
ClassificationStatistics

GetDashboardGeneralStatisticsSuccessfulResponse

data
UsageStatistics

GetDashboardGeolocationStatisticsSuccessfulResponse

data
GeolocationStatistics

GetDashboardVolumeStatisticsSuccessfulResponse

data
VolumeStatistics

GetDiscoveredEndpointsResponse

data
InventoryDiscoveryData

GetDiscoveryAccountSettingsResponse

data
DiscoveryAccountSettings

GetEndpointDrillDownResponse

data
EndpointDrillDown

GetEndpointResponse

value (optional)
EndpointResponse
isError (optional)
Boolean
States if an error occurred
example: false

GetEndpointsResponse

value (optional)
array[EndpointResponse]
isError (optional)
Boolean
States if an error occurred
example: false

GetHostsResponse

data
array[Host]

GetSiteConfigurationResponse

value (optional)
SiteConfigurationResponse

isError (optional)

Boolean

States if an error occurred

example: false

GetSiteConfigurationsResponse

value (optional)

array[SiteConfigurationResponse]

isError (optional)

Boolean

States if an error occurred

example: false

GetSiteDiscoverySettingsListResponse

data

array[SiteDiscoverySettings]

GetSiteDiscoverySettingsResponse

data

SiteDiscoverySettings

Host

hostId (optional)

Long

The host ID format: int64

example: 12345

hostName (optional)

String

The host's domain name

example: example.com

siteld (optional)

Long

The site external ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

HostClassificationStatistics

hostDetails (optional)

HostDetails

labels (optional)

array[Label]

hostsResourceStatTrend (optional)

ResourceStatTrend

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

HostDetails

hostname (optional)

String

The host's name

example: example.com

HostVolumeStatistics

hostDetails (optional)

HostDetails

currentCallVolume (optional)

Long

format: int64

currentCallPercent (optional)

Integer

format: int32

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

InventoryDiscoveryData

endpoints (optional)

array[DiscoveredEndpoint]

endpointsNumberByHost (optional)

array[EndpointsPerHost]

endpointsNumberByLabel (optional)

array[EndpointsPerLabel]

endpointsNumberByRisk (optional)

array[NumberOfEndpointsByRisks]

summary (optional)

DiscoveredApisSummary

Label

name (optional)

String

The name of the label

example: generalinfo:email

sensitive (optional)

Boolean

An indication whether the label is sensitive

example: false

NumberOfEndpointsByRisks

risk (optional)

String

The type of risk

example: unauthenticated

numberOfEndpoints (optional)

Long

The number of endpoints for a specific risk format: int64

ParameterDrillDown

name (optional)

String

The name of the parameter

example: id

dataTypes (optional)

array[DataTypeDto]

The type of the parameter

example: ["type": "String", "children": [{

 "name": "id",

 "dataTypes": ["type" : "String",

 "required": true,

 "labels": [

 {

 "name": "generalinfo:email",

 "sensitive": false,

 "visible": true

 }

]

}]

required (optional)

Boolean

An indication whether the parameter is required

example: false

labels (optional)

array[Label]

ParserErrorResponse

value (optional)

array[String]

isError (optional)

Boolean

States if an error occurred

example: true

PathParamSegments

index (optional)

Integer

Segment index format: int32

example: 1

segmentDetails (optional)

array[SegmentDetails]

path parameter segment details

RequestDrillDown

queryParamList (optional)

array[ParameterDrillDown]

contentTypeToRequestBody (optional)

map[String, array[ParameterDrillDown]]

ResourceClassificationStatistics

resourceDetails (optional)
ResourceDetails
labels (optional)
array[Label]
resourceStatTrend (optional)
ResourceStatTrend
isFirstTimeSeenInCurrentTimePeriod (optional)
Boolean

ResourceDetails

resourceUrl (optional)
String
example: v1/data
hostname (optional)
String
The host's name
example: example.com

ResourceStatTrend

currentCount (optional)
Long
format: int64
previousCount (optional)
Long
format: int64
trendPercent (optional)
Integer
format: int32
trendDirection (optional)
String
Enum:
UP
DOWN
NEUTRAL

ResourceVolumeStatistics

resourceDetails (optional)
ResourceDetails
currentCallVolume (optional)
Long
format: int64
currentCallPercent (optional)
Integer
format: int32
isFirstTimeSeenInCurrentTimePeriod (optional)
Boolean

ResponseDrillDown

contentTypeToResponseBody (optional)

map[String, array[ParameterDrillDown]]

RiskInfo

risk (optional)

String

The discovered API risk

riskType (optional)

String

The discovered API risk type

Enum:

OWASP

OTHER

owaspTag (optional)

String

The OWASP tag associated with the risk

SegmentDetails

dataType (optional)

String

Data type of path param segment

Enum:

DATE

TIME

EMAIL

IP

NUMBER

MIXED

REGION_LANGUAGE

UUID

WORD

ALPHA_NUMERIC

GENERIC

example: DATE

SensitiveDataClassification

classification (optional)

String

The classification of the sensitive value

example: large_us_city

lastSeen (optional)

Long

The time this sensitive value was seen last format: int64

example: 1556735907

locationPath (optional)

String

The detailed location of the sensitive value in the location (response body) including any parent objects

example: users/user/name/address

location (optional)

String

The location of the sensitive value

example: RESPONSE

SimpleTextErrorResponse

value (optional)
String
isError (optional)
Boolean
States if an error occurred
example: true

SimpleTextSuccessResponse

value (optional)
String
isError (optional)
Boolean
States if an error occurred
example: false

SiteConfigurationResponse

siteld (optional)
Long
The site id format: int64
accountId (optional)
Long
The account Id format: int64
siteName (optional)
String
The site name
example: example.com
apiOnlySite
Boolean
nonApiRequestViolationAction
String
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
violationActions (optional)
ApiViolationActions
discoveryEnabled (optional)
Boolean
discoveryExcludebasePath (optional)
array[String]
discoveryIncludebasePath (optional)
array[String]
isAutomaticDiscoveryApilIntegrationEnabled (optional)
Boolean

SiteDiscoverySettings

siteld (optional)
Long
The site ID format: int64
example: 1234567
accountId (optional)

Long

The account ID format: int64

example: 12345

siteName (optional)

String

The site name

example: example.com

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

relatedHosts (optional)

array[Host]

isDiscoveryEnabled (optional)

Boolean

discoveryExcludePaths (optional)

array[String]

Exclude discovery from these specific base paths

example: ["/test"]

discoveryIncludeOnlyPaths (optional)

array[String]

Set discovery for these specific base paths only

example: ["/api", "/service"]

isAutomaticDiscoveryApilIntegrationEnabled (optional)

Boolean

authenticationEnabled (optional)

Boolean

authParameterSettings (optional)

array[AuthParameterSettings]

Authentication location settings

excessiveDataExposureSettings (optional)

ExcessiveDataExposureSettings

deprecatedApiSettings (optional)

DeprecatedApiSettings

endpointSettings (optional)

array[EndpointSettingsDto]

Enable or disable endpoint exceptions

UpdateEndpointResponse

value (optional)

UpdateEndpointResponseValue

isError (optional)

Boolean

States if an error occurred

example: false

UpdateEndpointResponseValue

endpointId (optional)

Long

The API endpoint ID format: int64

example: 1234567890

UpdateSiteConfigurationResponse

value (optional)

[UpdateSiteConfigurationResponseValue](#)

isError (optional)

[Boolean](#)

States if an error occurred

example: false

UpdateSiteConfigurationResponseValue

siteld (optional)

[Long](#)

The Site ID format: int64

example: 12345

UploadFileSuccessResponse

data

[Action](#)

UsageStatistics

apiCalls (optional)

[Long](#)

format: int64

clientApps (optional)

[Long](#)

format: int64

clientUserAgents (optional)

[Long](#)

format: int64

clientCountries (optional)

[Long](#)

format: int64

VolumeStatistics

hostsVolumeStatistics (optional)

[array\[HostVolumeStatistics\]](#)

resourcesVolumeStatistics (optional)

[array\[ResourceVolumeStatistics\]](#)

endpointsVolumeStatistics (optional)

[array\[EndpointVolumeStatistics\]](#)

hostsResourceStatTrend (optional)

[ResourceStatTrend](#)

resourcesResourceStatTrend (optional)

[ResourceStatTrend](#)

endpointsResourceStatTrend (optional)

[ResourceStatTrend](#)

newHostsResourceStatTrend (optional)

[ResourceStatTrend](#)

newResourcesResourceStatTrend (optional)

[ResourceStatTrend](#)

newEndpointsResourceStatTrend (optional)

ResourceStatTrend
apiId_endpointId_body

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

violationActions (optional)

String

Json payload described by ViolationActions Object. This object defines different actions taken when each violation occurs

api_siteId_body

apiSpecification

byte[]The API specification document. The supported format is OAS2 or OAS3 (JSON or YAML) format: binary
basePath (optional)**String**

Override the spec basePath / server base path with this value

description (optional)

String

A description that will help recognize the API in the dashboard

oasFileName (optional)

String

Uploaded OAS file name

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

validateHost (optional)

Boolean

When set to true, verifies that the host name and site name match. Set to false in cases such as CNAME reuse or API management integrations where the host name and site name do not match.

violationActions (optional)

String

Json payload described by ViolationActions Object. This object defines different actions taken when each violation occurs

files_oas_body

actionTypes (optional)

String

Action types in Json format e.g. [{“actionTypeId”: 1}, {“actionTypeId”: 2}]
file (optional)

byte[]

Upload Swagger file. Swagger2.0, Swagger3.0 formats are supported format: binary

siteId_apiId_body

apiSpecification (optional)

byte[]

The API specification document. The supported format is OAS2 or OAS3 (JSON or YAML) format: binary
description (optional)

String

A description that will help recognize the API in the dashboard

oasFileName (optional)

String

Uploaded OAS file name

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

validateHost (optional)

Boolean

When set to true, verifies that the host name and site name match. Set to false in cases such as CNAME reuse or API management integrations where the host name and site name do not match.

violationActions (optional)

String

Json payload described by ViolationActions Object. This object defines different actions taken when each violation occurs

Imperva Advanced API Security

This topic describes the API for Imperva Advanced API Security. For full feature documentation, see [Imperva API Security](#).

Version: 1.0.0

BasePath:/api-security

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

API

- post /api/{siteId}
- delete /api/{siteId}/{apiId}
- get /api
- get /api/{siteId}
- get /api/{siteId}/all
- get /api/{siteId}/{apiId}
- get /api/file/{siteId}/{apiId}
- post /api/{siteId}/{apiId}

BFLASiteSettings

- get /v2/bfla/future-default/settings
- get /v2/bfla/sites/settings
- post /v2/bfla/future-default/settings
- post /v2/bfla/sites/settings

BOLASiteSettings

- post /v2/bola/add-risk
- get /v2/bola/future-default/settings
- get /v2/bola/sites/settings
- post /v2/bola/future-default/settings
- post /v2/bola/sites/settings

Console

- post /v3/provisioner/consoles
- delete /v3/provisioner/consoles/{console_id}
- get /v3/provisioner/consoles

Controllers

- post /v3/provisioner/controllers
- post /v3/provisioner/controllers/{controller_id}/microsensors
- delete /v3/provisioner/controllers/{controller_id}
- get /v3/provisioner/controllers/{controller_id}
- get /v3/provisioner/controllers/{controller_id}/controller-instances/{controller_instance_id}
- get /v3/provisioner/controllers/{controller_id}/controller-instances/{controller_instance_id}/service/{service}/stats
- get /v3/provisioner/controllers
- get /v3/provisioner/controllers/{controller_id}/microsensors

-
- `put /v3/provisioner/controllers/{controller_id}`

DataClassification

- `post /v2/data-classification/categories`
- `post /v2/data-classification/categories/{categoryId}/data-labels`
- `delete /v2/data-classification/categories/{categoryId}`
- `delete /v2/data-classification/categories/{categoryId}/data-labels/{dataLabelId}`
- `get /v2/data-classification/data-labels`
- `put /v2/data-classification/categories`
- `put /v2/data-classification/categories/{categoryId}/data-labels`
- `put /v2/data-classification/categories/data-labels`
- `post /v2/data-classification/data-labels/validate`

DiscoveryAccountSettings

- `post /v2/discovery/account/settings/auth-parameter-location`
- `delete /v2/discovery/account/settings`
- `get /v2/discovery/account/settings`
- `post /v2/discovery/account/settings`

DiscoveryHosts

- `get /v2/discovery/hosts`

DiscoveryInventory

- `get /v2/discovery/inventory/endpoints/files`
- `get /v2/discovery/inventory/endpoints`
- `get /v2/discovery/inventory/endpoints/{endpointId}`
- `delete /v2/discovery/inventory/endpoints/risks`

DiscoveryInventoryV3

- `delete /v3/discovery/inventory/sites/{siteId}/endpoints`
- `post /v3/discovery/inventory/endpoints/exceptions`
- `get /v3/discovery/inventory/endpoints/exceptions`
- `get /v3/discovery/inventory/endpoints/{endpointId}`
- `get /v3/discovery/inventory/endpoints/{endpointId}/object/{objectId}`
- `patch /v3/discovery/inventory/endpoints/exceptions`
- `patch /v3/discovery/inventory/endpoints`

DiscoverySiteSettings

- `get /v2/discovery/sites/{siteId}/settings`
- `get /v2/discovery/sites/settings`
- `post /v2/discovery/sites/{siteId}/settings`
- `post /v2/discovery/sites/settings`

DiscoveryStatistics

- `get /v2/discovery/statistics/classification/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/usage/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/geolocation/from/{from-timestamp}/to/{to-timestamp}`
- `get /v2/discovery/statistics/volume/from/{from-timestamp}/to/{to-timestamp}`

Endpoint

- `get /endpoint/{apiId}`
- `get /endpoint/{apiId}/{endpointId}`
- `post /endpoint/{apiId}/{endpointId}`

Microsensors

- `delete /v3/provisioner/microsensors/{microsensor_id}`
- `get /v3/provisioner/microsensors/{microsensor_id}`
- `get /v3/provisioner/microsensors/{microsensor_id}/microsensor-instances/{microsensor_instance_id}`
- `get /v3/provisioner/microsensors/{microsensor_id}/microsensor-instances/{microsensor_instance_id}/stats`
- `put /v3/provisioner/microsensors/{microsensor_id}`

Provisioner

- `post /v3/provisioner/download`

Reports

- `post /v3/reports`
- `delete /v3/reports/{reportId}`
- `get /v3/reports`
- `get /v3/reports/{reportId}`
- `get /v3/reports/status`

SITES

- `get /v3/sites`

SiteConfiguration

- `get /config/site`
- `get /config/site/{siteId}`
- `post /config/site/{siteId}`

Verification

- `delete /v2/shift-left/actions/{actionId}`
- `get /v2/shift-left/actions/{actionId}/actionType/{actionTypeId}`
- `get /v2/shift-left/actions/action-types`
- `get /v2/shift-left/actions`
- `get /v2/shift-left/actions/{actionId}/validate`
- `post /v2/shift-left/files/discovery`
- `post /v2/shift-left/files/oas`

API

```
post /api/{siteId}
```

Add an API (`addApi`)

Adds an API specification to a site

Path parameters

`siteld` (required)

Path Parameter

— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `multipart/form-data`

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Form parameters

apiSpecification (required)
 Form Parameter
 — format: binary
 basePath (required)
 Form Parameter

—
 description (required)
 Form Parameter

—
 matchTrailingSlash (required)
 Form Parameter

—
 oasFileName (required)
 Form Parameter

—
 specificationViolationAction (required)
 Form Parameter

—
 validateHost (required)
 Form Parameter

—
 violationActions (required)
 Form Parameter

Return type

AddApiResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "duplicateEndpointsList" : [ {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    }, {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    } ],
    "resultMessage" : "API 10 was added successfully",
    "apiId" : 1234
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

Success [AddApiResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

409

API Conflict [SimpleTextErrorResponse](#)

422

Failed to parse the API specification document [ParserErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
delete /api/{siteId}/{apiId}
```

Delete an API (deleteApi)

Deletes an API from a site in the account

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

apiId (required)

Path Parameter

— The API ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

SimpleTextSuccessResponse

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success SimpleTextSuccessResponse

400

Bad request SimpleTextErrorResponse

500

Internal error SimpleTextErrorResponse

```
get /api
```

Retrieve all APIs for the account (getAllApis)

Retrieves details of all protected APIs for all sites in the account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetApisResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907
  }, {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/{siteId}
```

Retrieve all APIs for a site (getAllSiteApis)

Retrieves details of all protected APIs for a specific site in the account

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetApisResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
```

```

"specificationViolationAction" : "ALERT_ONLY",
"oasFileName" : "bank.yaml",
"basePath" : "/api",
"siteId" : 1234567,
"violationActions" : {
    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"lastModified" : 1556735907
}, {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
        "invalidMethodViolationAction" : "ALERT_ONLY",
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY",
        "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/{siteId}/all
```

Retrieve all APIs and endpoints for a site (getAllSiteApisWithEndpoints)
 Retrieves details of all protected APIs and their endpoints for a specific site in the account

Path parameters

`siteld` (required)
 Path Parameter
 — The site ID format: int64

Query parameters

`caid` (optional)
 Query Parameter
 — The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetApisWithEndpointsResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "endpoints" : [ {
      "fullPath" : "/base/api/{param}",
      "path" : "/api/{param}",
      "sensitiveDataClassificationList" : [ {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      }, {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
      } ],
      "method" : "GET",
      "violationActions" : {
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY"
      },
      "id" : 1234,
      "duplicateOfEndpointId" : 1234,
    } ]
  } ]
```

```

    "internalEndpointId" : 0,
    "specificationViolationAction" : "ALERT_ONLY",
    "defaultEndpointType" : "INVALID_URL"
}, {
    "fullPath" : "/base/api/{param}",
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
}, {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
} ],
    "method" : "GET",
    "violationActions" : {
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY"
},
    "id" : 1234,
    "duplicateOfEndpointId" : 1234,
    "internalEndpointId" : 0,
    "specificationViolationAction" : "ALERT_ONLY",
    "defaultEndpointType" : "INVALID_URL"
} ],
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
        "invalidMethodViolationAction" : "ALERT_ONLY",
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY",
        "invalidUrlViolationAction" : "ALERT_ONLY"
},
    "id" : 1234,
    "lastModified" : 1556735907
}, {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "endpoints" : [ {
        "fullPath" : "/base/api/{param}",
        "path" : "/api/{param}",
        "sensitiveDataClassificationList" : [ {
            "lastSeen" : 1556735907,
            "location" : "RESPONSE",
            "classification" : "large_us_city",
            "locationPath" : "users/user/name/address"
}, {
            "lastSeen" : 1556735907,

```

```

    "location" : "RESPONSE",
    "classification" : "large_us_city",
    "locationPath" : "users/user/name/address"
} ],
"method" : "GET",
"violationActions" : {
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"duplicateOfEndpointId" : 1234,
"internalEndpointId" : 0,
"specificationViolationAction" : "ALERT_ONLY",
"defaultEndpointType" : "INVALID_URL"
}, {
    "fullPath" : "/base/api/{param}",
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
}, {
        "lastSeen" : 1556735907,
        "location" : "RESPONSE",
        "classification" : "large_us_city",
        "locationPath" : "users/user/name/address"
} ],
"method" : "GET",
"violationActions" : {
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"duplicateOfEndpointId" : 1234,
"internalEndpointId" : 0,
"specificationViolationAction" : "ALERT_ONLY",
"defaultEndpointType" : "INVALID_URL"
} ],
"creationTime" : 1556735907,
"description" : "This is an example API",
"siteName" : "example.com",
"matchTrailingSlash" : false,
"specificationViolationAction" : "ALERT_ONLY",
"oasFileName" : "bank.yaml",
"basePath" : "/api",
"siteId" : 1234567,
"violationActions" : {
    "invalidMethodViolationAction" : "ALERT_ONLY",
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY",
    "invalidUrlViolationAction" : "ALERT_ONLY"
},
"id" : 1234,
"lastModified" : 1556735907
} ]

```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApisWithEndpointsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/{siteId}/{apiId}
```

Retrieve an API (getApi)

Retrieves details of a specific API

Path parameters

`siteld` (required)

Path Parameter

— The site ID format: int64

`apild` (required)

Path Parameter

— The API ID format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetApiResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "apiSource" : "USER",
    "hostName" : "example.com",
    "creationTime" : 1556735907,
    "description" : "This is an example API",
    "siteName" : "example.com",
    "matchTrailingSlash" : false,
    "specificationViolationAction" : "ALERT_ONLY",
    "oasFileName" : "bank.yaml",
    "basePath" : "/api",
    "siteId" : 1234567,
    "violationActions" : {
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "lastModified" : 1556735907
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetApiResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /api/file/{siteId}/{apiId}
```

Download the API OAS file (getApiFile)

Download the manually uploaded or automatically discovered OAS file for a specific API. If the API source is mixed, the result is the manually uploaded file.

Path parameters

siteld (required)

Path Parameter

— The site ID format: int64

apild (required)

Path Parameter

— The API ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

DownloadApiSpecificationDtoResponse

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success DownloadApiSpecificationDtoResponse

400

Bad request SimpleTextErrorResponse

500

Internal error SimpleTextErrorResponse

```
post /api/{siteId}/{apiId}
```

Update an API (updateApi)
Updates any or all of the optional parameters.

Path parameters

siteld (required)
Path Parameter
— The site ID format: int64
apild (required)
Path Parameter
— The API ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

caid (optional)
Query Parameter
— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Form parameters

apiSpecification (optional)
Form Parameter
— format: binary
basePath (optional)
Form Parameter
—
description (optional)
Form Parameter
—
matchTrailingSlash (optional)
Form Parameter
—
oasFileName (optional)
Form Parameter
—
specificationViolationAction (optional)
Form Parameter
—
validateHost (optional)

Form Parameter

violationActions (optional)

Form Parameter

Return type

AddApiResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "duplicateEndpointsList" : [ {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    }, {
      "fullPath" : "/api/{param}",
      "method" : "GET",
      "id" : 1234567890
    } ],
    "resultMessage" : "API 10 was added successfully",
    "apiId" : 1234
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success AddApiResponse

400

Bad request SimpleTextErrorResponse

409

API Conflict SimpleTextErrorResponse

422

Failed to parse the API specification document [ParserErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

BFLASiteSettings

```
get /v2/bfla/future-default/settings
```

Retrieves the BFLA account settings ([getBflaAccountSettings](#))

Retrieves the configuration details for the BFLA account settings associated with the account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetBflaAccountSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "bflaEnabled" : true,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetBflaAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/bfla/sites/settings
```

Retrieves BFLA discovery site settings (getBflaDiscoverySiteSettings)

Retrieves the configuration details for the BFLA discovery site settings of all sites associated with the account.

Query parameters

detailed (optional)
Query Parameter

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetBflaSiteSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "bflaEnabled" : true,
    "accountId" : 12345,
    "endpointSettings" : [ {
      "bflaEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "tags" : [ {
        "tag" : "Production"
      }
    }
  }
]
```

```

        "name" : "My Tag",
        "id" : 1234567
    } ,
    {
        "name" : "My Tag",
        "id" : 1234567
    } ]
},
{
    "bflaEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "tags" : [
        {
            "name" : "My Tag",
            "id" : 1234567
        },
        {
            "name" : "My Tag",
            "id" : 1234567
        }
    ],
    "siteId" : 1234567,
    "siteName" : "example.com",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
},
{
    "bflaEnabled" : true,
    "accountId" : 12345,
    "endpointSettings" : [
        {
            "bflaEnabled" : true,
            "hostname" : "example.com",
            "method" : "POST",
            "endpointId" : 1234567890,
            "endpointUrl" : "/v1/data",
            "lastModifiedUser" : "John Doe",
            "lastModified" : 1556735907,
            "tags" : [
                {
                    "name" : "My Tag",
                    "id" : 1234567
                },
                {
                    "name" : "My Tag",
                    "id" : 1234567
                }
            ]
        },
        {
            "bflaEnabled" : true,
            "hostname" : "example.com",
            "method" : "POST",
            "endpointId" : 1234567890,
            "endpointUrl" : "/v1/data",
            "lastModifiedUser" : "John Doe",
            "lastModified" : 1556735907,
            "tags" : [
                {
                    "name" : "My Tag",
                    "id" : 1234567
                },
                {
                    "name" : "My Tag",
                    "id" : 1234567
                }
            ]
        }
    ]
}

```

```

    } ],
    "siteId" : 1234567,
    "siteName" : "example.com",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetBflaSiteSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/bfla/future-default/settings
```

Updates only the changed BFLA account settings (updateBflaAccountSettings)

Updates the configuration details for the changed BFLA account settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [BflaAccountSettingsDto](#) (optional)

Body Parameter

— Bfla Account Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success String

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/bfla/sites/settings
```

Updates only the changed BFLA discovery site settings (updateBflaDiscoverySiteSettings)

Updates the configuration details for the changed BFLA discovery site settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [BflaSiteDiscoverySettings](#) (required)

Body Parameter

— Bfla discovery Site Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success String

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

BOLASiteSettings

```
post /v2/bola/add-risk
```

(addBolaManualRiskToEndpoints)

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body BolaManualSiteSettings (required)

Body Parameter

— Bola Site Manual Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK String

```
get /v2/bola/future-default/settings
```

Retrieves the BOLA account settings (getBolaAccountSettings)

Retrieves the configuration details for the BOLA account settings associated with the account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetBolaAccountSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "bolaEnabled" : true,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

Success [GetBolaAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/bola/sites/settings
```

Retrieves BOLA discovery site settings (getBolaDiscoverySiteSettings)

Retrieves the configuration details for the BOLA discovery site settings of all sites associated with the account.

Query parameters

detailed (optional)
Query Parameter

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetBolaSiteSettingsResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 12345,
    "bolaEnabled" : true,
    "endpointSettings" : [ {
      "bolaEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
      }, {
        "name" : "My Tag",
        "id" : 1234567
      } ]
    }, {
      "bolaEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
      } ]
    } ]
  } ]
```

```

}, {
  "name" : "My Tag",
  "id" : 1234567
} ],
},
"siteId" : 1234567,
"siteName" : "example.com",
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907
}, {
  "accountId" : 12345,
  "bolaEnabled" : true,
  "endpointSettings" : [ {
    "bolaEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "bolaEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "bolaEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "siteId" : 1234567,
    "siteName" : "example.com",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetBolaSiteSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/bola/future-default/settings
```

Updates only the changed BOLA account settings (updateBolaAccountSettings)

Updates the configuration details for the changed BOLA account settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [BolaSettingsDto](#) (optional)

Body Parameter

— Bola Account Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetBolaAccountSettingsResponse](#)

Example data

Content-Type: application/json

```
{
```

```

"data" : {
  "bolaEnabled" : true,
  "lastModifiedUser" : "John Doe",
  "lastModified" : 1556735907
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetBolaAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/bola/sites/settings
```

Updates only the changed BOLA discovery site settings (updateBolaDiscoverySiteSettings)
Updates the configuration details for the changed BOLA discovery site settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [BolaSiteDiscoverySettings](#) (optional)

Body Parameter

— Bola discovery Site Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetBolaSiteSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 12345,
    "bolaEnabled" : true,
    "endpointSettings" : [ {
      "bolaEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
      }, {
        "name" : "My Tag",
        "id" : 1234567
      } ]
    }, {
      "bolaEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
      }, {
        "name" : "My Tag",
        "id" : 1234567
      } ]
    }, {
      "siteId" : 1234567,
      "siteName" : "example.com",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907
    }, {
      "accountId" : 12345,
      "bolaEnabled" : true,
      "endpointSettings" : [ {
        "bolaEnabled" : true,
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data",
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907
      } ]
    }
  }
}
```

```

"method" : "POST",
"endpointId" : 1234567890,
"endpointUrl" : "/v1/data",
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907,
"tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
}, {
    "name" : "My Tag",
    "id" : 1234567
} ]
}, {
    "bolaEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    }
],
    "siteId" : 1234567,
    "siteName" : "example.com",
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907
}
]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetBolaSiteSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

Console

```
post /v3/provisioner/consoles
```

Create a console (createConsole)
Create a console

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body CreateConsole (required)

Body Parameter

— Create Console

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[CreateConsoleResponseV3](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "modifiedAt" : 1556735907,
    "description" : "description",
    "tags" : [ "tag1", "tag2" ],
    "accountId" : 0,
    "createdAt" : 1556735907,
    "apiToken" : "apiToken",
    "valuesFilePath" : "provisioner/accounts/1234/console/519113/values.yaml",
    "createdBy" : "John Doe",
    "deploymentsFilePath" : "templates/console/falcon-console-0.1.0.tgz",
  } ]
}
```

```

    "infrastructureType" : "infrastructureType",
    "name" : "name",
    "modifiedBy" : "John Doe",
    "id" : 1,
    "apiId" : 6
} , {
    "modifiedAt" : 1556735907,
    "description" : "description",
    "tags" : [ "tag1", "tag2" ],
    "accountId" : 0,
    "createdAt" : 1556735907,
    "apiToken" : "apiToken",
    "valuesFilePath" : "provisioner/accounts/1234/console/519113/values.yaml",
    "createdBy" : "John Doe",
    "deploymentsFilePath" : "templates/console/falcon-console-0.1.0.tgz",
    "infrastructureType" : "infrastructureType",
    "name" : "name",
    "modifiedBy" : "John Doe",
    "id" : 1,
    "apiId" : 6
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Success [CreateConsoleResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
delete /v3/provisioner/consoles/{console_id}
```

Delete a specific Console and its instances (deleteConsole)

Delete a specific Console and its instances

Path parameters

console_id (required)

Path Parameter

— The Console ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success

404

No existing console-Package found with given id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/consoles
```

Retrieve the package details for all Consoles (getConsoles)

Retrieve the package details for all Consoles

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetConsolesResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "modifiedAt" : 1556735907,
    "description" : "description",
    "tags" : [ "tag1", "tag2" ],
    "accountId" : 0,
    "createdAt" : 1556735907,
    "apiToken" : "apiToken",
    "valuesFilePath" : "provisioner/accounts/1234/console/519113/values.yaml",
    "createdBy" : "John Doe",
    "deploymentsFilePath" : "templates/console/falcon-console-0.1.0.tgz",
    "infrastructureType" : "infrastructureType",
    "name" : "name",
    "modifiedBy" : "John Doe",
    "id" : 1,
    "apiId" : 6
  }, {
    "modifiedAt" : 1556735907,
    "description" : "description",
    "tags" : [ "tag1", "tag2" ],
    "accountId" : 0,
    "createdAt" : 1556735907,
    "apiToken" : "apiToken",
    "valuesFilePath" : "provisioner/accounts/1234/console/519113/values.yaml",
    "createdBy" : "John Doe",
    "deploymentsFilePath" : "templates/console/falcon-console-0.1.0.tgz",
    "infrastructureType" : "infrastructureType",
    "name" : "name",
    "modifiedBy" : "John Doe",
    "id" : 1,
    "apiId" : 6
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetConsolesResponse

400

Bad input error [ApiFailureResponseV3](#)

404

No Console found with given Id [ApiFailureResponseV3](#)

500

[Internal error ApiFailureResponseV3](#)

Controllers

```
post /v3/provisioner/controllers
```

Create a controller (createControllers)

Create a controller

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body CreateController (required)

Body Parameter

— Create Controller Request

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetControllerResponseV3](#)

Example data

Content-Type: application/json

```
{
```

```

"data" : [ {
  "instances" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    } ],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
      "status" : "SUCCESS"
    }
  }, {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    } ],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
      "status" : "SUCCESS"
    }
  }
], "modifiedAt" : 1556735907,
"microsensors" : [ {
  "microsensorType" : "Universal Log Consumer",
  "controller" : 3421,
  "modifiedAt" : 1556735907,
  "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
  "description" : "Microsensor to sniff data from Security API",
}
]
}

```

```

"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
}, {
  "microsensorType" : "Universal Log Consumer",
  "controller" : 3421,
  "modifiedAt" : 1556735907,
  "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
  "description" : "Microsensor to sniff data from Security API",
  "microsensorId" : 10,
  "tags" : "Security API",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "createdBy" : "John Doe",
  "infrastructureType" : "Kubernetes",
  "name" : "Security API Microsensor",
  "modifiedBy" : "John Doe",
  "apiId" : 123496875
} ],
"description" : "This is a test controller",
"tags" : "List [ "CC Processing", "US West" ]",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
"createdBy" : "John Doe",
"deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
"infrastructureType" : "[ Kubernetes ]",
"name" : "TestController",
"modifiedBy" : "John Doe",
"id" : 0,
"apiId" : 123496875
}, {
  "instances" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    } ],
    "firstSeenAt" : 6,
  }
]

```

```

"version" : "1.1b",
"deployment" : {
    "status" : "SUCCESS"
}
}, {
    "instanceId" : "1234",
    "health" : {
        "status" : "ACTIVE"
    },
    "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    }],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
],
"modifiedAt" : 1556735907,
"microsensors" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
}
]
}

```

```

    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  } ],
  "description" : "This is a test controller",
  "tags" : "List [ "CC Processing", "US West" ]",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
  "createdBy" : "John Doe",
  "deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
  "infrastructureType" : "[ Kubernetes ]",
  "name" : "TestController",
  "modifiedBy" : "John Doe",
  "id" : 0,
  "apiId" : 123496875
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllerResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
post /v3/provisioner/controllers/{controller_id}/microsensors
```

Create a Microsensor for a specific Controller (`createMicrosensorForController`)
Create a Microsensor for a specific Controller

Path parameters

`controller_id` (required)

Path Parameter

— The Controller Id format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateMicrosensor](#) (required)

Body Parameter

— Create Microsensors Request

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetMicrosensorResponseV3](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "instances" : [ {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "healthStatus" : "Active",
      "networkInterface" : "eth0",
      "ipAddress" : "1.1.1.1",
      "services" : [ {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      }, {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      } ],
      "firstSeenAt" : 0,
    }
  ]
}
```

```

    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
  "hostName" : "docker-desktop",
  "instanceId" : "1234",
  "healthStatus" : "Active",
  "networkInterface" : "eth0",
  "ipAddress" : "1.1.1.1",
  "services" : [ {
    "stats" : {
      "lastSeenCpu" : 40.56,
      "lastSeenMemory" : 11956224
    },
    "name" : "data",
    "version" : "1.1b"
  }, {
    "stats" : {
      "lastSeenCpu" : 40.56,
      "lastSeenMemory" : 11956224
    },
    "name" : "data",
    "version" : "1.1b"
  }],
  "firstSeenAt" : 0,
  "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
  "modifiedAt" : 1556735907,
  "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
  "description" : "Microsensor to sniff data from Security API",
  "microsensorId" : 10,
  "tags" : "Security API",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "createdBy" : "John Doe",
  "infrastructureType" : "Kubernetes",
  "name" : "Security API Microsensor",
  "modifiedBy" : "John Doe",
  "apiId" : 123496875
}, {
  "microsensorType" : "Universal Log Consumer",
  "controller" : 3421,
  "instances" : [ {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
      "stats" : {
        "lastSeenCpu" : 40.56,
        "lastSeenMemory" : 11956224
      },
      "name" : "data",
      "version" : "1.1b"
    }, {
      "stats" : {
        "lastSeenCpu" : 40.56,
        "lastSeenMemory" : 11956224
      },
      "name" : "data",
      "version" : "1.1b"
    }]
  }]
}

```

```

        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetMicrosensorResponseV3

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
delete /v3/provisioner/controllers/{controller_id}
```

Delete a specific Controller and its microsensors and their instances (deleteController)
Delete a specific Controller and its microsensors and their instances

Path parameters

controller_id (required)

Path Parameter

— The Controller Id format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success

404

No existing Controller-Package found with given id [ApiFailureResponseV3](#)

500

Internal error ApiFailureResponseV3

```
get /v3/provisioner/controllers/{controller_id}
```

Retrieve the package details for a specific Controller (getController)
 Retrieve the package details for a specific Controller

Path parameters

controller_id (required)

Path Parameter

— The Controller Id format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetControllerResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "instances" : [ {
      "instanceId" : "1234",
      "health" : {
        "status" : "ACTIVE"
      },
      "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      } ]
    }
  ]
}
```

```

    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
}, {
    "instanceId" : "1234",
    "health" : {
        "status" : "ACTIVE"
    },
    "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    } ],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
},
"modifiedAt" : 1556735907,
"microsensors" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
}
]
}

```

```

    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  },
  "description" : "This is a test controller",
  "tags" : "List [ \"CC Processing\", \"US West\" ]",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
  "createdBy" : "John Doe",
  "deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
  "infrastructureType" : "[ Kubernetes ]",
  "name" : "TestController",
  "modifiedBy" : "John Doe",
  "id" : 0,
  "apiId" : 123496875
}, {
  "instances" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
      "status" : "SUCCESS"
    }
  }, {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }]
  }
]

```

```

        "status" : "ACTIVE"
    }
} ],
"firstSeenAt" : 6,
"version" : "1.1b",
"deployment" : {
    "status" : "SUCCESS"
}
} ],
"modifiedAt" : 1556735907,
"microsensors" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
} ],
"description" : "This is a test controller",
"tags" : "List [ \"CC Processing\", \"US West\" ]",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
"createdBy" : "John Doe",
"deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
"infrastructureType" : "[ Kubernetes ]",
"name" : "TestController",
"modifiedBy" : "John Doe",
"id" : 0,
"apiId" : 123496875
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllerResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/controllers/{controller_id}/controller-instances/{controller_instance_id}
```

Retrieve the details of a specific Controller Instance for a specific Controller (getControllerInstance)
Retrieve the details of a specific Controller Instance for a specific Controller

Path parameters

controller_id (required)

Path Parameter

— The Controller Id format: int64

controller_instance_id (required)

Path Parameter

— The Controller Instance Id

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetControllerInstanceResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
      "status" : "SUCCESS"
    }
  }, {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {

```

```

        "status" : "SUCCESS"
    }
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllerInstanceResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No ControllerInstance found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/controllers/{controller_id}/controller-instances/{controller_instance_id}/service/{service}/stats
```

Retrieve the CPU and Memory usage statistics of a specific Controller Instance for a specific Controller (`getControllerInstanceState`)

Retrieve the CPU and Memory usage statistics of a specific Controller Instance for a specific Controller

Path parameters

`controller_id` (required)

Path Parameter

— The Controller Id format: int64

`controller_instance_id` (required)

Path Parameter

— The Controller Instance Id

`service` (required)

Path Parameter

— Service

Query parameters

`start_time` (optional)

Query Parameter

— Start Time format: int64

`end_time` (optional)

Query Parameter

— End Time format: int64

`interval` (optional)

Query Parameter

— Interval

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`GetControllerInstanceServiceResponseV3`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "replica" : 2,
    "stats" : [ {
      "hostname" : "normalizer-9ddb79c5c-lnskc",
      "memory" : [ 11956224, 24365465, 24565767 ],
      "cpu" : [ 23.6, 45.33, 67.21 ]
    }, {
      "hostname" : "normalizer-9ddb79c5c-lnskc",
      "memory" : [ 11956224, 24365465, 24565767 ],
      "cpu" : [ 23.6, 45.33, 67.21 ]
    } ],
    "name" : "abc"
  }, {
    "replica" : 2,
    "stats" : [ {
      "hostname" : "normalizer-9ddb79c5c-lnskc",
      "memory" : [ 11956224, 24365465, 24565767 ],
      "cpu" : [ 23.6, 45.33, 67.21 ]
    }, {
      "hostname" : "normalizer-9ddb79c5c-lnskc",
      "memory" : [ 11956224, 24365465, 24565767 ],
      "cpu" : [ 23.6, 45.33, 67.21 ]
    } ],
    "name" : "abc"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllerInstanceServiceResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No stats found with given controller Instance Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/controllers
```

Retrieve the package details for all Controllers (getControllers)
Retrieve the package details for all Controllers

Query parameters

detailed (optional)
Query Parameter

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetControllersResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "instances" : [ {
      "instanceId" : "1234",
      "health" : {
        "status" : "ACTIVE"
      },
      "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      } ],
      "firstSeenAt" : 6,
      "version" : "1.1b",
      "deployment" : {
        "status" : "SUCCESS"
      }
    }, {
      "instanceId" : "1234",
      "health" : {
        "status" : "ACTIVE"
      },
      "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      } ],
      "firstSeenAt" : 6,
      "version" : "1.1b",
      "deployment" : {
        "status" : "SUCCESS"
      }
    } ],
    "modifiedAt" : 1556735907,
    "microsensors" : [ {
      "microsensorType" : "Universal Log Consumer",
      "controller" : 3421,
      "modifiedAt" : 1556735907,
      "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    }
  ]
}
```

```

    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  } , {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  } ],
  "description" : "This is a test controller",
  "tags" : "List [ "CC Processing", "US West" ]",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
  "createdBy" : "John Doe",
  "deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
  "infrastructureType" : "[ Kubernetes ]",
  "name" : "TestController",
  "modifiedBy" : "John Doe",
  "id" : 0,
  "apiId" : 123496875
}, {
  "instances" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    } ]
  } ,

```

```

    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
}, {
    "instanceId" : "1234",
    "health" : {
        "status" : "ACTIVE"
    },
    "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    } ],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
},
"modifiedAt" : 1556735907,
"microsensors" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
}
]
}

```

```

    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  },
  "description" : "This is a test controller",
  "tags" : "List [ "CC Processing", "US West" ]",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
  "createdBy" : "John Doe",
  "deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
  "infrastructureType" : "[ Kubernetes ]",
  "name" : "TestController",
  "modifiedBy" : "John Doe",
  "id" : 0,
  "apiId" : 123496875
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllersResponse](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/controllers/{controller_id}/microsensors
```

Retrieve the details of all Microsensors for a specific Controller (getMicrosensorsForController)
 Retrieve the details of all Microsensors for a specific Controller

Path parameters

controller_id (required)

Path Parameter

— The Controller Id format: int64

Query parameters

detailed (optional)

Query Parameter

— detailed

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetMicrosensorsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "instances" : [ {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "healthStatus" : "Active",
      "networkInterface" : "eth0",
      "ipAddress" : "1.1.1.1",
      "services" : [ {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      }, {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      } ],
      "firstSeenAt" : 0,
      "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
    }, {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "lastSeenAt" : 0,
      "lastSeenCpu" : 40.56,
      "lastSeenMemory" : 11956224
    } ]
  }
}
```

```

    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "instances" : [ {
        "hostName" : "docker-desktop",
        "instanceId" : "1234",
        "healthStatus" : "Active",
        "networkInterface" : "eth0",
        "ipAddress" : "1.1.1.1",
        "services" : [ {
            "stats" : {
                "lastSeenCpu" : 40.56,
                "lastSeenMemory" : 11956224
            },
            "name" : "data",
            "version" : "1.1b"
        }, {
            "stats" : {
                "lastSeenCpu" : 40.56,
                "lastSeenMemory" : 11956224
            },
            "name" : "data",
            "version" : "1.1b"
        } ],
        "firstSeenAt" : 0,
        "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
    }
]

```

```

}, {
  "hostName" : "docker-desktop",
  "instanceId" : "1234",
  "healthStatus" : "Active",
  "networkInterface" : "eth0",
  "ipAddress" : "1.1.1.1",
  "services" : [ {
    "stats" : {
      "lastSeenCpu" : 40.56,
      "lastSeenMemory" : 11956224
    },
    "name" : "data",
    "version" : "1.1b"
  }, {
    "stats" : {
      "lastSeenCpu" : 40.56,
      "lastSeenMemory" : 11956224
    },
    "name" : "data",
    "version" : "1.1b"
  } ],
  "firstSeenAt" : 0,
  "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetMicrosensorsResponse](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
put /v3/provisioner/controllers/{controller_id}
```

Update details for a specific Controller (updateController)
Update details for a specific Controller

Path parameters

controller_id (required)

Path Parameter

— The Controller Id format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdateControllerRequest](#) (required)

Body Parameter

— Update Controller Request

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetControllerResponseV3](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "instances" : [ {
      "instanceId" : "1234",
      "health" : {
        "status" : "ACTIVE"
      },
      "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      } ],
      "firstSeenAt" : 6,
      "version" : "1.1b",
      "deployment" : {
        "status" : "SUCCESS"
      }
    }, {
      "instanceId" : "1234",
      "health" : {
        "status" : "ACTIVE"
      },
      "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
          "reason" : "reason",
          "status" : "ACTIVE"
        }
      } ],
      "firstSeenAt" : 6,
      "version" : "1.1b",
      "deployment" : {
        "status" : "SUCCESS"
      }
    } ],
    "modifiedAt" : 1556735907,
    "microsensors" : [ {
      "microsensorType" : "Universal Log Consumer",
      "controller" : 3421,
      "modifiedAt" : 1556735907,
      "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    }
  ]
}
```

```

    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  } , {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
  } ],
  "description" : "This is a test controller",
  "tags" : "List [ "CC Processing", "US West" ]",
  "createdAt" : 1556735907,
  "apiToken" : "iakasd-sdfsadas",
  "valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
  "createdBy" : "John Doe",
  "deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
  "infrastructureType" : "[ Kubernetes ]",
  "name" : "TestController",
  "modifiedBy" : "John Doe",
  "id" : 0,
  "apiId" : 123496875
}, {
  "instances" : [ {
    "instanceId" : "1234",
    "health" : {
      "status" : "ACTIVE"
    },
    "services" : [ {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    }, {
      "replica" : 2,
      "name" : "normalizer",
      "health" : {
        "reason" : "reason",
        "status" : "ACTIVE"
      }
    } ]
  } ,

```

```

    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
}, {
    "instanceId" : "1234",
    "health" : {
        "status" : "ACTIVE"
    },
    "services" : [ {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    }, {
        "replica" : 2,
        "name" : "normalizer",
        "health" : {
            "reason" : "reason",
            "status" : "ACTIVE"
        }
    } ],
    "firstSeenAt" : 6,
    "version" : "1.1b",
    "deployment" : {
        "status" : "SUCCESS"
    }
},
"modifiedAt" : 1556735907,
"microsensors" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "modifiedAt" : 1556735907,
    "filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
    "description" : "Microsensor to sniff data from Security API",
    "microsensorId" : 10,
    "tags" : "Security API",
    "createdAt" : 1556735907,
    "apiToken" : "iakasd-sdfsadas",
    "createdBy" : "John Doe",
    "infrastructureType" : "Kubernetes",
}
]
}

```

```

    "name" : "Security API Microsensor",
    "modifiedBy" : "John Doe",
    "apiId" : 123496875
} ],
"description" : "This is a test controller",
"tags" : "List [ "CC Processing", "US West" ]",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"valuesFilePath" : "/accounts/1234/controller/519113/values.yaml",
"createdBy" : "John Doe",
"deploymentsFilePath" : "/controller/falcon-controller-0.1.0.tgz",
"infrastructureType" : "[ Kubernetes ]",
"name" : "TestController",
"modifiedBy" : "John Doe",
"id" : 0,
"apiId" : 123496875
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetControllerResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

DataClassification

```
post /v2/data-classification/categories
```

Add Category (addCategory)

Adds a new category for custom data label classification.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CategoryDto](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[UpdateCategoryResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "name" : "name",
    "lastModifiedUser" : "lastModifiedUser",
    "id" : 0,
    "lastModified" : 6
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateCategoryResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/data-classification/categories/{categoryId}/data-labels
```

Add Data Label (addDataLabel)

Adds a new data label for custom data label classification.

Path parameters

categoryId (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DataLabelDto](#) (required)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[UpdateDataLabelResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
```

```

    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateDataLabelResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
delete /v2/data-classification/categories/{categoryId}
```

Delete Category (deleteCategory)

Deletes an existing category for custom data label classification.

Path parameters

categoryId (required)

Path Parameter

— format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID

format: int64

Return type

[UpdateCategoryResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "name" : "name",
    "lastModifiedUser" : "lastModifiedUser",
    "id" : 0,
    "lastModified" : 6
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

Success [UpdateCategoryResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
delete /v2/data-classification/categories/{categoryId}/data-labels/{dataLabelId}
```

Delete dataLabel (deleteDataLabel)

Deletes an existing data label for custom data label classification.

Path parameters

categoryId (required)
Path Parameter

— format: int64
 dataLabelId (required)
 Path Parameter
 — format: int64

Query parameters

caid (optional)
 Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
 format: int64

Return type

[UpdateDataLabelResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateDataLabelResponse](#)

400Bad request [ApiFailureResponse](#)**500**[Internal error](#) [ApiFailureResponse](#)

```
get /v2/data-classification/data-labels
```

List All Data Labels (getAllDataLabels)

Receive a list of all data label settings linked to the given account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type[GetAllDataLabelsResponse](#)**Example data**

Content-Type: application/json

```
{
  "data" : [ {
    "dataLabels" : [ {
      "isActive" : true,
      "type" : "type",
      "acceleration" : "acceleration",
      "createdAt" : 6,
      "nameRegex" : "nameRegex",
      "isSensitive" : true,
      "pathOrPathRegex" : "pathOrPathRegex",
      "name" : "name",
      "paramLocation" : "paramLocation",
      "lastModifiedUser" : "lastModifiedUser",
      "valueRegex" : "valueRegex",
      "id" : 1,
      "lastModified" : 5,
      "categoryId" : 0
    }, {
      "isActive" : true,
      "type" : "type",
      "acceleration" : "acceleration",
      "createdAt" : 6,
      "nameRegex" : "nameRegex",
      "isSensitive" : true,
    } ]
  }
}
```

```

    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  } ],
  "lastModifiedUser" : "lastModifiedUser",
  "lastModified" : 6,
  "type" : "type",
  "categoryName" : "categoryName",
  "categoryId" : 0
}, {
  "dataLabels" : [ {
    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  }, {
    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  } ],
  "lastModifiedUser" : "lastModifiedUser",
  "lastModified" : 6,
  "type" : "type",
  "categoryName" : "categoryName",
  "categoryId" : 0
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

Success [GetAllDataLabelsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
put /v2/data-classification/categories
```

Update Category (updateCategory)

Updates an existing category for custom data label classification.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CategoryDto](#) (required)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[UpdateCategoryResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "name" : "name",
    "lastModifiedUser" : "lastModifiedUser",
    "id" : 0,
    "lastModified" : 6
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateCategoryResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
put /v2/data-classification/categories/{categoryId}/data-labels
```

Update Data Label (updateDataLabel)

Updates an existing data label for custom data label classification.

Path parameters

categoryId (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `DataLabelDto` (required)
 Body Parameter

Query parameters

`caid` (optional)
 Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`UpdateDataLabelResponse`

Example data

Content-Type: application/json

```
{
  "data" : {
    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

Success [UpdateDataLabelResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
put /v2/data-classification/categories/data-labels
```

Update Data Labels (updateDataLabels)

Updates an existing list of data labels for custom data label classification

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DataLabelDto](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[DataLabelDto](#)

Example data

Content-Type: application/json

```
{
```

```

    "isActive" : true,
    "type" : "type",
    "acceleration" : "acceleration",
    "createdAt" : 6,
    "nameRegex" : "nameRegex",
    "isSensitive" : true,
    "pathOrPathRegex" : "pathOrPathRegex",
    "name" : "name",
    "paramLocation" : "paramLocation",
    "lastModifiedUser" : "lastModifiedUser",
    "valueRegex" : "valueRegex",
    "id" : 1,
    "lastModified" : 5,
    "categoryId" : 0
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [DataLabelDto](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/data-classification/data-labels/validate
```

Validate Regex (validateRegexExpression)

Verify the regex patterns provided for data labels are valid or not.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DataLabelRegexDto](#) (required)
Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{  
  "isError" : true,  
  "value" : { }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [ApiResult](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryAccountSettings

```
post /v2/discovery/account/settings/auth-parameter-location
```

Add Authentication Location (addAuthLocation)

Adds the Authentication Location for all websites currently configured or to a specific website

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AuthParameterLocationDto](#) (optional)

Body Parameter

— Authentication location details

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[AuthParameterLocationResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "useForFutureWebSites" : true,
    "lastModifiedUser" : "John Doe",
    "siteIds" : 1234567,
    "lastModified" : 1556735907,
    "authParameterLocation" : "http-req-header-x-jwt"
  }, {
    "useForFutureWebSites" : true,
    "lastModifiedUser" : "John Doe",
    "siteIds" : 1234567,
    "lastModified" : 1556735907,
    "authParameterLocation" : "http-req-header-x-jwt"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [AuthParameterLocationResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
delete /v2/discovery/account/settings
```

Deletes the Discovery account settings (deleteDiscoveryAccountSettings)

Deletes the specific settings of the Discovery account which includes the site settings.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success

400Bad request [ApiFailureResponse](#)**500**[Internal error](#) [ApiFailureResponse](#)

```
get /v2/discovery/account/settings
```

Retrieve the Discovery account settings (getDiscoveryAccountSettings)

Retrieves the configuration details for the Discovery account settings associated with the account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type[GetDiscoveryAccountSettingsResponse](#)**Example data**

Content-Type: application/json

```
{
  "data" : {
    "dataLabelSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "visible" : true,
      "dataLabelId" : 0,
      "dataLabel" : "ssn",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "sensitive" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "visible" : true,
      "dataLabelId" : 0,
      "dataLabel" : "ssn",
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "sensitive" : true
    } ],
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "deprecatedApiVersion" : "2020-01-01"
    }
  }
}
```

```

    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "inactiveForDays" : 100
  },
  "authParameterSettings" : [ {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  }, {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  } ],
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  }
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveryAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/account/settings
```

Update only the changed Discovery account settings (updateDiscoveryAccountSettings)
Updates the configuration details for the changed Discovery account settings associated with the account.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DiscoveryAccountSettings](#) (optional)

Body Parameter

— Discovery Account Settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetDiscoveryAccountSettingsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [
    {
      "dataLabelSettings" : [ {
        "auditString" : "auditString",
        "accountId" : 12345,
        "visible" : true,
        "dataLabelId" : 0,
        "dataLabel" : "ssn",
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "sensitive" : true
      }, {
        "auditString" : "auditString",
        "accountId" : 12345,
        "visible" : true,
        "dataLabelId" : 0,
        "dataLabel" : "ssn",
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "sensitive" : true
      } ],
      "authenticationEnabled" : true,
      "deprecatedApiSettings" : {
        "deprecate" : true
      }
    }
  ]
}
```

```

    "deprecatedApiEnabled" : true,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "inactiveForDays" : 100
  },
  "authParameterSettings" : [ {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  }, {
    "auditString" : "auditString",
    "accountId" : 12345,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  } ],
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  }
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveryAccountSettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryHosts

```
get /v2/discovery/hosts
```

Retrieves the account's discovered hosts (getHosts)
 Retrieves a list of all hosts discovered within a particular account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetHostsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

Success [GetHostsResponse](#)

500

[Internal error ApiFailureResponse](#)

DiscoveryInventory

```
get /v2/discovery/inventory/endpoints/files
```

Download all OAS files of the discovered APIs to a compressed ZIP file (getDiscoveredApiFiles)

Download all OAS files of the discovered APIs, for all hosts or selected hosts in the query, to a compressed ZIP file. The ZIP file format is account-<account_id>-api-files.zip and the ZIP file name format is <host_name>-<base_path>-discovery.json. Underscore is used as the delimiter for the basePath.

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
{  
  "name" : "name",  
  "comment" : "comment"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/zip](#)
- [application/json](#)

Responses

200

Success [inline_response_200](#)

404

Not Found [ApiFailureResponse](#)

500

Internal Server Error [ApiFailureResponse](#)

```
get /v2/discovery/inventory/endpoints
```

Retrieve all discovered endpoints (getDiscoveredEndpoints)

Retrieve all discovered endpoints for the account or for the specified hosts. If no host id is provided - retrieve all discovered endpoints for all hosts

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetDiscoveredEndpointsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "summary" : {
      "numberOfEndpointsWithRisks" : "{\"OWASP": 1, "other": 20}",
      "numberOfLabels" : 7,
      "numberOfEndpoints" : 5,
      "numberOfResources" : 9,
      "numberOfApiDiscoveryStatuses" : "{\"IN_PROGRESS": 1, "BASELINED": 20, "OTHER": 2}",
      "numberOfEndpointsWithDataLabels" : "{\"sensitive": 2, "non-sensitive": 5, "total": 7}",
      "numberOfHosts" : 2
    }
  }
}
```

```

},
"endpointsNumberByRisk" : [ {
    "numberOfEndpoints" : 5,
    "risk" : "unauthenticated"
}, {
    "numberOfEndpoints" : 5,
    "risk" : "unauthenticated"
} ],
"endpoints" : [ {
    "hostName" : "example.com",
    "authenticationInfo" : {
        "authParameterLocations" : [ {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        }, {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        } ],
        "status" : "status"
    },
    "method" : "GET",
    "resource" : "/api/users",
    "parsers" : [ "parsers", "parsers" ],
    "hostId" : 12345,
    "counter" : 0,
    "accessibilityInfo" : {
        "accessibility" : [ "INTERNAL", "INTERNAL" ]
    },
    "labels" : [ {
        "name" : "generalinfo:email",
        "sensitive" : false
    }, {
        "name" : "generalinfo:email",
        "sensitive" : false
    } ],
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ],
    "endpointSources" : [ {
        "sourceType" : "Security API",
        "name" : "Security API Microsensor",
        "id" : 10,
        "tags" : "[ 'Security API', 'PROD' ]"
    }, {
        "sourceType" : "Security API",
        "name" : "Security API Microsensor",
        "id" : 10,
        "tags" : "[ 'Security API', 'PROD' ]"
    } ],
}
]
}

```

```

"discoveryDate" : 1657886850000,
"risks" : [ "risks", "risks" ],
"siteId" : 1234567,
"riskTypes" : [ "OWASP", "OWASP" ],
"id" : 1234567890,
"baselinedDate" : 1657886850000,
"risksInfo" : [ {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
}, {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
} ],
"dataExposureInfo" : {
    "status" : "status"
},
"status" : "BASELINED"
}, {
    "hostName" : "example.com",
    "authenticationInfo" : {
        "authParameterLocations" : [ {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        }, {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        } ],
        "status" : "status"
    },
    "method" : "GET",
    "resource" : "/api/users",
    "parsers" : [ "parsers", "parsers" ],
    "hostId" : 12345,
    "counter" : 0,
    "accessibilityInfo" : {
        "accessibility" : [ "INTERNAL", "INTERNAL" ]
    },
    "labels" : [ {
        "name" : "generalinfo:email",
        "sensitive" : false
    }, {
        "name" : "generalinfo:email",
        "sensitive" : false
    } ],
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ],
}

```

```
"endpointSources" : [ {
    "sourceType" : "Security API",
    "name" : "Security API Microsensor",
    "id" : 10,
    "tags" : "[ 'Security API', 'PROD' ]"
}, {
    "sourceType" : "Security API",
    "name" : "Security API Microsensor",
    "id" : 10,
    "tags" : "[ 'Security API', 'PROD' ]"
} ],
"discoveryDate" : 1657886850000,
"risks" : [ "risks", "risks" ],
"siteId" : 1234567,
"riskTypes" : [ "OWASP", "OWASP" ],
"id" : 1234567890,
"baselinedDate" : 1657886850000,
"risksInfo" : [ {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
}, {
    "owaspTag" : "owaspTag",
    "riskType" : "OWASP",
    "risk" : "risk"
} ],
"dataExposureInfo" : {
    "status" : "status"
},
"status" : "BASELINED"
} ],
"endpointsNumberByHost" : [ {
    "hostName" : "example.com",
    "numberOfEndpoints" : 6,
    "hostId" : 12345
}, {
    "hostName" : "example.com",
    "numberOfEndpoints" : 6,
    "hostId" : 12345
} ],
"endpointsNumberByLabel" : [ {
    "numberOfEndpoints" : 1,
    "label" : "generalinfo:email"
}, {
    "numberOfEndpoints" : 1,
    "label" : "generalinfo:email"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDiscoveredEndpointsResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/inventory/endpoints/{endpointId}
```

Retrieve detailed information for the endpoint (`getEndpointDrillDown`)

Retrieve detailed information for the endpoint

Path parameters

`endpointId` (required)

Path Parameter

— endpoint ID format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetEndpointDrillDownResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "hostName" : "example.com",
    "request" : {
      "headerList" : [ "", "" ],
      "queryParamList" : [ null, null ],
      "isError" : true,
      "error" : {
        "errorMessage" : "errorMessage"
      }
    }
  }
}
```

```

},
"contentTypeToRequestBody" : {
    "key" : [
        "dataTypes" : "[\"type\":\"String\", \"children\": [ \n            \"name\": \"id\", \n            \"dataTypes\": [\"type\" : \"String\", \n                \"required\": true, \n                \"labels\": [ \n                    \"name\": \"generalinfo:email\", \n                    \"visible\": true\n                ] \n            ], \n            \"name\" : \"id\", \n            \"id\" : 6, \n            \"required\" : false, \n            \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n        ], \n        \"dataTypes\" : [\"type\":\"String\", \"children\": [ \n            \"name\": \"id\", \n            \"dataTypes\": [\"type\" : \"String\", \n                \"required\": true, \n                \"labels\": [ \n                    \"name\": \"generalinfo:email\", \n                    \"visible\": true\n                ] \n            ], \n            \"name\" : \"id\", \n            \"id\" : 6, \n            \"required\" : false, \n            \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n        ] \n    ] \n}, \n    \"authenticationInfo\" : {
        "authParameterLocations" : [ {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        }, {
            "useForFutureWebSites" : true,
            "lastModifiedUser" : "John Doe",
            "siteIds" : 1234567,
            "lastModified" : 1556735907,
            "authParameterLocation" : "http-req-header-x-jwt"
        }],
        "status" : "status"
    },
    "method" : "GET",
    "resource" : "/api/users",
    "responses" : {
        "key" : {
            "headerList" : [ null, null ],
            "isError" : true,
            "contentTypeToResponseBody" : {
                "key" : [ null, null ]
            }
        }
    },
    "endpointStatisticsSummary" : {
        "numberOfParametersWithDataLabels" : "{\"sensitive\": 2, \"non-sensitive\": 5, \"total\": 7}",
        "numberOfParametersByDataLabel" : {
            "key" : 0
        }
    }
}

```

```

"accessibilityInfo" : {
    "accessibility" : [ "INTERNAL", "INTERNAL" ]
},
"pathParamSegments" : [ {
    "segmentDetails" : [ {
        "dataType" : "DATE"
    }, {
        "dataType" : "DATE"
    } ],
    "index" : 1
}, {
    "segmentDetails" : [ {
        "dataType" : "DATE"
    }, {
        "dataType" : "DATE"
    } ],
    "index" : 1
} ],
"status" : {
    "designIssueReason" : "designIssueReason",
    "name" : "BASELINED",
    "lastModified" : 1556735907
},
"tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
}, {
    "name" : "My Tag",
    "id" : 1234567
} ]
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetEndpointDrillDownResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
delete /v2/discovery/inventory/endpoints/risks
```

Relearn risk data (relearnRisk)
Deletes the current risk data and adds new risk data by relearning

Query parameters

endpointIds (optional)

Query Parameter

— endpointIds

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : { },
  "meta" : { }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [ApiSuccessResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryInventoryV3

```
delete /v3/discovery/inventory/sites/{siteId}/endpoints
```

Deleting all the endpoints under this site (deleteAllEndpointsForSite)

Deleting all the endpoints under this site

Path parameters

siteId (required)

Path Parameter

— format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success String

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v3/discovery/inventory/endpoints/exceptions
```

Delete selected endpoints (deleteEndpoints)
Deletes the selected endpoints and adds to exception list

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [EndpointRequest](#) (required)

Body Parameter

— List of endpoints

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[DeleteEndpointResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "id" : 1234567
  }, {
    "id" : 1234567
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [DeleteEndpointResponse](#)

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/discovery/inventory/endpoints/exceptions
```

Get deleted endpoints (getDeleteEndpoints)

Get deleted endpoints for an account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[DeletedEndpointResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "endpointSources" : [ {
      "sourceType" : "Security API",
      "name" : "Security API Microsensor",
      "id" : 10,
      "tags" : "[ 'Security API', 'PROD' ]"
    }, {
      "sourceType" : "Security API",
      "name" : "Security API Microsensor",
      "id" : 10,
      "tags" : "[ 'Security API', 'PROD' ]"
    } ]
  }
}
```

```

"hostName" : "new-host.example.com",
"deletedAt" : 1721000001000,
"method" : "DELETE",
"resource" : "/api/v3/test/new/endpoint/two/88888",
"endpointId" : 2911578398,
"siteId" : 57365335,
"id" : 2,
"userName" : "userName"
}, {
"endpointSources" : [ {
"sourceType" : "Security API",
"name" : "Security API Microsensor",
"id" : 10,
"tags" : "[ 'Security API', 'PROD' ]"
}, {
"sourceType" : "Security API",
"name" : "Security API Microsensor",
"id" : 10,
"tags" : "[ 'Security API', 'PROD' ]"
} ],
"hostName" : "new-host.example.com",
"deletedAt" : 1721000001000,
"method" : "DELETE",
"resource" : "/api/v3/test/new/endpoint/two/88888",
"endpointId" : 2911578398,
"siteId" : 57365335,
"id" : 2,
"userName" : "userName"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success DeletedEndpointResponse

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/discovery/inventory/endpoints/{endpointId}
```

Retrieve detailed information for the endpoint (getEndpointDetails)
 Retrieve detailed information for the endpoint

Path parameters

endpointId (required)

Path Parameter

— format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
 format: int64

Return type

[EndpointDrillDownDtoV2](#)

Example data

Content-Type: application/json

```
{
  "hostName" : "hostName",
  "authenticationInfo" : {
    "authParameterLocations" : [ {
      "useForFutureWebSites" : true,
      "lastModifiedUser" : "John Doe",
      "siteIds" : 1234567,
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    }, {
      "useForFutureWebSites" : true,
      "lastModifiedUser" : "John Doe",
      "siteIds" : 1234567,
      "lastModified" : 1556735907,
      "authParameterLocation" : "http-req-header-x-jwt"
    } ],
    "status" : "status"
  },
  "method" : "method",
  "resource" : "resource",
  "endpointId" : 0,
  "parsers" : [ {
    "request" : {
      "headerList" : [ "", "" ],
      "queryParamList" : [ null, null ],
      "isError" : true,
      "error" : {
        "code" : 404,
        "message" : "Resource not found"
      }
    }
  } ]
}
```



```

"headerList" : [ "", "" ],
"queryParamList" : [ null, null ],
"isError" : true,
"error" : {
  "errorMessage" : "errorMessage"
},
"contentTypeToRequestBody" : {
  "key" : [
    {
      "dataTypes" : "[\"type\":\"String\", \"children\": [ { \n        \"name\": \"id\", \n        \"dataTypes\": [\"type\" : \"String\", \n          \"required\": true, \n          \"labels\": [ \n            { \n              \"name\": \"generalinfo:email\", \n              \"visible\": true\n            } \n          ] \n        ], \n        \"name\" : \"id\", \n        \"id\" : 6, \n        \"required\" : false, \n        \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n      }, { \n        \"dataTypes\" : [\"type\":\"String\", \"children\": [ { \n          \"name\": \"id\", \n          \"dataTypes\": [\"type\" : \"String\", \n            \"required\": true, \n            \"labels\": [ \n              { \n                \"name\": \"generalinfo:email\", \n                \"visible\": true\n              } \n            ] \n          ], \n          \"name\" : \"id\", \n          \"id\" : 6, \n          \"required\" : false, \n          \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n        } ] \n      } \n    }, \n    {
      "queryParamList" : [
        {
          "dataTypes" : "[\"type\":\"String\", \"children\": [ { \n            \"name\": \"id\", \n            \"dataTypes\": [\"type\" : \"String\", \n              \"required\": true, \n              \"labels\": [ \n                { \n                  \"name\": \"generalinfo:email\", \n                  \"visible\": true\n                } \n              ] \n            ], \n            \"name\" : \"id\", \n            \"id\" : 6, \n            \"required\" : false, \n            \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n          }, { \n            \"dataTypes\" : [\"type\":\"String\", \"children\": [ { \n              \"name\": \"id\", \n              \"dataTypes\": [\"type\" : \"String\", \n                \"required\": true, \n                \"labels\": [ \n                  { \n                    \"name\": \"generalinfo:email\", \n                    \"visible\": true\n                  } \n                ] \n              ], \n              \"name\" : \"id\", \n              \"id\" : 6, \n              \"required\" : false, \n              \"labels\" : [ \"generalinfo:email\", \"generalinfo:email\" ] \n            } ] \n          } \n        }, \n        {
          "responses" : {
            "key" : {
              "headerList" : [ null, null ],
              "isError" : true,
              "contentTypeToResponseBody" : {
                "key" : [ null, null ]
              }
            }
          }
        }
      ]
    }
  ]
}

```

```

        }
    },
} ],
"endpointStatisticsSummary" : {
    "numberOfParametersWithDataLabels" : {"sensitive": 2,"non-sensitive": 5,"total": 7}"},
    "numberOfParametersByDataLabel" : {
        "key" : 0
    }
},
"accessibilityInfo" : {
    "accessibility" : [ "INTERNAL", "INTERNAL" ]
},
"pathParamSegments" : [ {
    "segmentDetails" : [ {
        "dataType" : "DATE"
    },
    {
        "dataType" : "DATE"
    }],
    "index" : 1
}, {
    "segmentDetails" : [ {
        "dataType" : "DATE"
    },
    {
        "dataType" : "DATE"
    }],
    "index" : 1
}],
"status" : {
    "designIssueReason" : "designIssueReason",
    "name" : "BASELINED",
    "lastModified" : 1556735907
},
"tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
}, {
    "name" : "My Tag",
    "id" : 1234567
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success EndpointDrillDownDtoV2

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v3/discovery/inventory/endpoints/{endpointId}/object/{objectId}
```

Retrieve detailed information of the GraphQL object (getGraphQLObjectResponse)
Retrieve detailed information of the GraphQL object

Path parameters

endpointId (required)

Path Parameter

— format: int64

objectId (required)

Path Parameter

— format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
format: int64

Return type

[ObjectDto](#)

Example data

Content-Type: application/json

```
{
  "objectPath" : "objectPath",
  "paramList" : [
    {
      "dataTypes" : "[\"type\":\"String\", \"children\": [ { \n        \"name\" : \"id\", \n        \"label\" : \"\", \n        \"required\" : true, \n        \"type\" : \"String\", \n        \"value\" : \"\", \n        \"visible\" : true \n      } ] ]",
      "name" : "id",
      "id" : 6,
      "required" : false,
      "labels" : [ "generalinfo:email", "generalinfo:email" ]
    },
    {
      "dataTypes" : "[\"type\":\"String\", \"children\": [ { \n        \"name\" : \"id\", \n        \"label\" : \"\", \n        \"required\" : true, \n        \"type\" : \"String\", \n        \"value\" : \"\", \n        \"visible\" : true \n      } ] ]",
      "name" : "id",
      "id" : 6,
      "required" : false,
      "labels" : [ "generalinfo:email", "generalinfo:email" ]
    }
  ]
}
```

```

"dataTypes": ["type" : "String",\n              "required": true,\n              "label":\n              "name": "generalinfo:email",\n              "visible": true\n            }]\n          }\n        ]\n      },\n      "name" : "id",\n      "id" : 6,\n      "required" : false,\n      "labels" : [ "generalinfo:email", "generalinfo:email" ]\n    },\n    "objectId" : 0\n  }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success ObjectDto

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
patch /v3/discovery/inventory/endpoints/exceptions
```

Recover deleted endpoints (recoverEndpoints)

Recovers the selected endpoints

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [RecoverEndpointRequest](#) (required)

Body Parameter

— List of exceptionIds

Query parameters

action (required)

Query Parameter

— default: delete

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success String

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
patch /v3/discovery/inventory/endpoints
```

Rediscover endpoints (rediscoverEndpoints)

Deletes the selected endpoints and starts re-discovery

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [EndpointRequest](#) (required)

Body Parameter

— List of endpoints

Query parameters

action (required)

Query Parameter

—

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

Success String

400

Bad input error [ApiFailureResponse](#)

500

Internal error ApiFailureResponse

DiscoverySiteSettings

```
get /v2/discovery/sites/{siteId}/settings
```

Retrieve discovery settings for a site (getSiteDiscoverySettings)
Retrieve discovery settings for a site

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetSiteDiscoverySettingsResponse

Example data

Content-Type: application/json

```
{
  "data" : {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "enabled" : true
    }
  }
}
```

```

"accountId" : 12345,
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907,
"authParameterLocation" : "http->req->header->jwt",
"enabled" : true
} ],
"discoveryIncludeOnlyPaths" : [ "/api", "/service" ],
"relatedHosts" : [ {
  "hostName" : "example.com",
  "hostId" : 12345,
  "siteId" : 1234567,
  "siteName" : "example.com"
}, {
  "hostName" : "example.com",
  "hostId" : 12345,
  "siteId" : 1234567,
  "siteName" : "example.com"
} ],
"isAutomaticDiscoveryApiIntegrationEnabled" : true,
"accountId" : 12345,
"isDiscoveryEnabled" : true,
"endpointSettings" : [ {
  "authenticationEnabled" : true,
  "hostname" : "example.com",
  "method" : "POST",
  "endpointId" : 1234567890,
  "endpointUrl" : "/v1/data",
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  },
  "tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
  }, {
    "name" : "My Tag",
    "id" : 1234567
  } ]
}, {
  "authenticationEnabled" : true,
  "hostname" : "example.com",
  "method" : "POST",
  "endpointId" : 1234567890,
  "endpointUrl" : "/v1/data",
  "excessiveDataExposureSettings" : {
    "excessiveDataExposureEnabled" : true,
    "responseParameterWithSensitiveDataLabelLimit" : 100,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "responseParameterLimit" : 100,
    "responseParameterWithDataLabelLimit" : 100
  },
  "tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
  } ]
}
]

```

```

        },
        {
            "name" : "My Tag",
            "id" : 1234567
        }
    ],
    "discoveryExcludePaths" : [ "/test" ],
    "siteId" : 1234567,
    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "siteType" : "CWAF, ANYWHERE"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/sites/settings
```

Retrieve the discovery settings for all sites in the account (getSitesDiscoverySettings)
 Retrieve the discovery settings for all sites in the account

Query parameters

detailed (optional)
 Query Parameter

caid (optional)
 Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetSiteDiscoverySettingsListResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "discoveryIncludeOnlyPaths" : [ "/api", "/service" ],
    "relatedHosts" : [ {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }, {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    } ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 12345,
    "isDiscoveryEnabled" : true,
    "endpointSettings" : [ {
      "authenticationEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
      }
    } ]
  } ]
}
```

```

        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ]
}, {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ]
},
"discoveryExcludePaths" : [ "/test" ],
"siteId" : 1234567,
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907,
"siteType" : "CWAF, ANYWHERE"
}, {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
        "deprecatedApiEnabled" : true,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
    }, {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
    }
]
}

```

```

    "lastModified" : 1556735907,
    "authParameterLocation" : "http->req->header->jwt",
    "enabled" : true
  ],
  "discoveryIncludeOnlyPaths" : [ "/api", "/service" ],
  "relatedHosts" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  },
  {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
  }],
  "isAutomaticDiscoveryApiIntegrationEnabled" : true,
  "accountId" : 12345,
  "isDiscoveryEnabled" : true,
  "endpointSettings" : [ {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "responseParameterLimit" : 100,
      "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    },
    {
      "name" : "My Tag",
      "id" : 1234567
    }
  ],
  {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
      "excessiveDataExposureEnabled" : true,
      "responseParameterWithSensitiveDataLabelLimit" : 100,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "responseParameterLimit" : 100,
      "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    },
    {
      "name" : "My Tag",
      "id" : 1234567
    }
  ]
}

```

```

        "id" : 1234567
    } ]
}
"discoveryExcludePaths" : [ "/test" ],
"siteId" : 1234567,
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907,
"siteType" : "CWF, ANYWHERE"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsListResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/sites/{siteId}/settings
```

Update the site's discovery settings (updateOneSiteDiscoverySettings)
Update the site's discovery settings with one of the optional parameters for each site

Path parameters

siteId (required)

Path Parameter

— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SiteDiscoverySettings` (optional)

Body Parameter

— Discovery settings

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`GetSiteDiscoverySettingsResponse`

Example data

Content-Type: application/json

```
{
  "data" : {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "discoveryIncludeOnlyPaths" : [ "/api", "/service" ],
    "relatedHosts" : [ {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }, {
      "hostName" : "example.com",
    }
  }
}
```

```

        "hostId" : 12345,
        "siteId" : 1234567,
        "siteName" : "example.com"
    ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 12345,
    "isDiscoveryEnabled" : true,
    "endpointSettings" : [ {
        "authenticationEnabled" : true,
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data",
        "excessiveDataExposureSettings" : {
            "excessiveDataExposureEnabled" : true,
            "responseParameterWithSensitiveDataLabelLimit" : 100,
            "lastModifiedUser" : "John Doe",
            "lastModified" : 1556735907,
            "responseParameterLimit" : 100,
            "responseParameterWithDataLabelLimit" : 100
        },
        "tags" : [ {
            "name" : "My Tag",
            "id" : 1234567
        }, {
            "name" : "My Tag",
            "id" : 1234567
        } ]
    }, {
        "authenticationEnabled" : true,
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data",
        "excessiveDataExposureSettings" : {
            "excessiveDataExposureEnabled" : true,
            "responseParameterWithSensitiveDataLabelLimit" : 100,
            "lastModifiedUser" : "John Doe",
            "lastModified" : 1556735907,
            "responseParameterLimit" : 100,
            "responseParameterWithDataLabelLimit" : 100
        },
        "tags" : [ {
            "name" : "My Tag",
            "id" : 1234567
        }, {
            "name" : "My Tag",
            "id" : 1234567
        } ]
    }, {
        "discoveryExcludePaths" : [ "/test" ],
        "siteId" : 1234567,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "siteType" : "CWF, ANYWHERE"
    }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/discovery/sites/settings
```

Update the site's discovery settings (updateSitesDiscoverySettings)

Update the site's discovery settings with one of the optional parameters for each site

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [SiteDiscoverySettings](#) (optional)

Body Parameter

— Discovery settings

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetSiteDiscoverySettingsListResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
      "deprecatedApiEnabled" : true,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    }, {
      "auditString" : "auditString",
      "accountId" : 12345,
      "lastModifiedUser" : "John Doe",
      "lastModified" : 1556735907,
      "authParameterLocation" : "http->req->header->jwt",
      "enabled" : true
    } ],
    "discoveryIncludeOnlyPaths" : [ "/api", "/service" ],
    "relatedHosts" : [ {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    }, {
      "hostName" : "example.com",
      "hostId" : 12345,
      "siteId" : 1234567,
      "siteName" : "example.com"
    } ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "accountId" : 12345,
    "isDiscoveryEnabled" : true,
    "endpointSettings" : [ {
      "authenticationEnabled" : true,
      "hostname" : "example.com",
      "method" : "POST",
      "endpointId" : 1234567890,
      "endpointUrl" : "/v1/data",
      "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
      }
    } ]
  } ]
}
```

```

"tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
}, {
    "name" : "My Tag",
    "id" : 1234567
} ]
}, {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
}, {
        "name" : "My Tag",
        "id" : 1234567
} ]
},
"discoveryExcludePaths" : [ "/test" ],
"siteId" : 1234567,
"lastModifiedUser" : "John Doe",
"lastModified" : 1556735907,
"siteType" : "CWF, ANYWHERE"
}, {
    "authenticationEnabled" : true,
    "deprecatedApiSettings" : {
        "deprecatedApiEnabled" : true,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "inactiveForDays" : 100
    },
    "siteName" : "example.com",
    "authParameterSettings" : [ {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
}, {
        "auditString" : "auditString",
        "accountId" : 12345,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "authParameterLocation" : "http->req->header->jwt",
        "enabled" : true
} ],
"discoveryIncludeOnlyPaths" : [ "/api", "/service" ],

```

```

"relatedHosts" : [ {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
}, {
    "hostName" : "example.com",
    "hostId" : 12345,
    "siteId" : 1234567,
    "siteName" : "example.com"
} ],
"isAutomaticDiscoveryApiIntegrationEnabled" : true,
"accountId" : 12345,
"isDiscoveryEnabled" : true,
"endpointSettings" : [ {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ]
}, {
    "authenticationEnabled" : true,
    "hostname" : "example.com",
    "method" : "POST",
    "endpointId" : 1234567890,
    "endpointUrl" : "/v1/data",
    "excessiveDataExposureSettings" : {
        "excessiveDataExposureEnabled" : true,
        "responseParameterWithSensitiveDataLabelLimit" : 100,
        "lastModifiedUser" : "John Doe",
        "lastModified" : 1556735907,
        "responseParameterLimit" : 100,
        "responseParameterWithDataLabelLimit" : 100
    },
    "tags" : [ {
        "name" : "My Tag",
        "id" : 1234567
    }, {
        "name" : "My Tag",
        "id" : 1234567
    } ]
}, {
    "discoveryExcludePaths" : [ "/test" ],
    "siteId" : 1234567,

```

```

    "lastModifiedUser" : "John Doe",
    "lastModified" : 1556735907,
    "siteType" : "CWAF, ANYWHERE"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteDiscoverySettingsListResponse](#)

400

Bad request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

DiscoveryStatistics

```
get /v2/discovery/statistics/classification/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' classification statistics ([getDashboardClassificationStatistics](#))
Retrieve account level baselined endpoints' classification statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

detailed (optional)
Query Parameter

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetDashboardClassificationStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "topRisksVolumeStatistics" : [ {
      "volume" : 7,
      "risk" : "Unauthenticated",
      "percent" : 2
    }, {
      "volume" : 7,
      "risk" : "Unauthenticated",
      "percent" : 2
    } ],
    "resourcesClassificationStatistics" : [ {
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "firstTimeSeenInCurrentTimePeriod" : true,
      "labels" : [ null, null ]
    }, {
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "firstTimeSeenInCurrentTimePeriod" : true,
      "labels" : [ null, null ]
    } ],
    "endpointsClassificationStatistics" : [ {
      "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
      },
      "risks" : [ "risks", "risks" ],
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "hostsResourceStatTrend" : {
        "trendPercent" : 5,
        "currentCount" : 1,
      }
    } ]
  }
}
```

```

        "trendDirection" : "UP",
        "previousCount" : 5
    },
    "risksInfo" : [ {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    }, {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    } ],
    "firstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ {
        "name" : "generalinfo:email",
        "sensitive" : false
    }, {
        "name" : "generalinfo:email",
        "sensitive" : false
    } ]
}, {
    "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
    },
    "risks" : [ "risks", "risks" ],
    "isFirstTimeSeenInCurrentTimePeriod" : true,
    "hostsResourceStatTrend" : {
        "trendPercent" : 5,
        "currentCount" : 1,
        "trendDirection" : "UP",
        "previousCount" : 5
    },
    "risksInfo" : [ {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    }, {
        "owaspTag" : "owaspTag",
        "riskType" : "OWASP",
        "risk" : "risk"
    } ],
    "firstTimeSeenInCurrentTimePeriod" : true,
    "labels" : [ {
        "name" : "generalinfo:email",
        "sensitive" : false
    }, {
        "name" : "generalinfo:email",
        "sensitive" : false
    } ]
},
"sensitiveClassificationVolumeStatistics" : [ null, null ],
"nonSensitiveClassificationVolumeStatistics" : [ null, null ],
"allClassificationVolumeStatistics" : [ {
    "volume" : 6,
    "label" : "generalinfo:email",
    "percent" : 0
}
]

```

```
        },
        {
          "volume" : 6,
          "label" : "generalinfo:email",
          "percent" : 0
        }],
      "hostsClassificationStatistics" : [ {
        "hostDetails" : {
          "hostname" : "example.com"
        },
        "isFirstTimeSeenInCurrentTimePeriod" : true,
        "firstTimeSeenInCurrentTimePeriod" : true,
        "labels" : [ null, null ]
      }, {
        "hostDetails" : {
          "hostname" : "example.com"
        },
        "isFirstTimeSeenInCurrentTimePeriod" : true,
        "firstTimeSeenInCurrentTimePeriod" : true,
        "labels" : [ null, null ]
      } ]
    }
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetDashboardClassificationStatisticsSuccessfulResponse

400

Bad input error ApiFailureResponse

500

Internal error ApiFailureResponse

Retrieve account level baselined endpoints' usage statistics (getDashboardGeneralStatistics)
Retrieve account level baselined endpoints' usage statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host IDs

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetDashboardGeneralStatisticsSuccessfulResponse

Example data

Content-Type: application/json

```
{
  "data" : {
    "clientApps" : 6,
    "clientCountries" : 1,
    "clientUserAgents" : 5,
    "apiCalls" : 0
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success GetDashboardGeneralStatisticsSuccessfulResponse

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/statistics/geolocation/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' geolocation statistics (getDashboardGeolocationStatistics)
Retrieve account level baselined endpoints' geolocation statistics

Path parameters

from-timestamp (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

to-timestamp (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

hostIds (optional)

Query Parameter

— Comma separated list of host ids

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetDashboardGeolocationStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "clientGeolocationCountryStatisticsDto" : [ {
      "code" : "US",
      "currentCallVolume" : 6,
      "name" : "United States",
      "currentCallPercent" : 0
    }, {
      "code" : "US",
      "currentCallVolume" : 6,
      "name" : "United States",
      "currentCallPercent" : 0
    } ]
  }
}
```

```

        "currentCallPercent" : 0
    } ],
    "destinationGeolocationCountryStatisticsDto" : [ null, null ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDashboardGeolocationStatisticsSuccessfulResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/discovery/statistics/volume/from/{from-timestamp}/to/{to-timestamp}
```

Retrieve account level baselined endpoints' volume statistics (`getDashboardVolumeStats`)
Retrieve account level baselined endpoints' volume statistics

Path parameters

`from-timestamp` (required)

Path Parameter

— Start Date or Start Time of the statistics in milliseconds (epoch time). format: int64

`to-timestamp` (required)

Path Parameter

— End Date or End Time of the statistics in milliseconds (epoch time). format: int64

Query parameters

`hostIds` (optional)

Query Parameter

— Comma separated list of host ids

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID

format: int64

Return type

[GetDashboardVolumeStatisticsSuccessfulResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "resourcesVolumeStatistics" : [ {
      "currentCallVolume" : 2,
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 5,
      "firstTimeSeenInCurrentTimePeriod" : true
    }, {
      "currentCallVolume" : 2,
      "resourceDetails" : {
        "hostname" : "example.com",
        "resourceUrl" : "v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 5,
      "firstTimeSeenInCurrentTimePeriod" : true
    } ],
    "endpointsVolumeStatistics" : [ {
      "currentCallVolume" : 6,
      "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 0,
      "firstTimeSeenInCurrentTimePeriod" : true
    }, {
      "currentCallVolume" : 6,
      "endpointDetails" : {
        "hostname" : "example.com",
        "method" : "POST",
        "endpointId" : 1234567890,
        "endpointUrl" : "/v1/data"
      },
      "isFirstTimeSeenInCurrentTimePeriod" : true,
      "currentCallPercent" : 0,
      "firstTimeSeenInCurrentTimePeriod" : true
    } ],
    "hostsVolumeStatistics" : [ {
      "hostDetails" : {
        "hostname" : "example.com"
      }
    } ]
  }
}
```

```

},
"currentCallVolume" : 5,
"isFirstTimeSeenInCurrentTimePeriod" : true,
"currentCallPercent" : 1,
"firstTimeSeenInCurrentTimePeriod" : true
}, {
"hostDetails" : {
"hostname" : "example.com"
},
"currentCallVolume" : 5,
"isFirstTimeSeenInCurrentTimePeriod" : true,
"currentCallPercent" : 1,
"firstTimeSeenInCurrentTimePeriod" : true
} ],
"endpointsResourceStatTrend" : {
"trendPercent" : 5,
"currentCount" : 1,
"trendDirection" : "UP",
"previousCount" : 5
}
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetDashboardVolumeStatisticsSuccessfulResponse](#)

400

Bad input error [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

Endpoint

```
get /endpoint/{apiId}
```

Retrieve all endpoints (getAllUserFacingEndpoints)
 Retrieve details on all endpoints for an API

Path parameters

apild (required)
 Path Parameter
 — The API ID format: int64

Query parameters

caid (optional)
 Query Parameter
 — The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetEndpointsResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "fullPath" : "/base/api/{param}",
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "duplicateOfEndpointId" : 1234,
    "internalEndpointId" : 0,
    "specificationViolationAction" : "ALERT_ONLY",
    "defaultEndpointType" : "INVALID_URL"
  }, {
    "fullPath" : "/base/api/{param}",
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    } ]
  }
}
```

```

    "classification" : "large_us_city",
    "locationPath" : "users/user/name/address"
  } , {
    "lastSeen" : 1556735907,
    "location" : "RESPONSE",
    "classification" : "large_us_city",
    "locationPath" : "users/user/name/address"
  } ],
  "method" : "GET",
  "violationActions" : {
    "invalidParamNameViolationAction" : "ALERT_ONLY",
    "invalidParamValueViolationAction" : "ALERT_ONLY",
    "missingParamViolationAction" : "ALERT_ONLY"
  },
  "id" : 1234,
  "duplicateOfEndpointId" : 1234,
  "internalEndpointId" : 0,
  "specificationViolationAction" : "ALERT_ONLY",
  "defaultEndpointType" : "INVALID_URL"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetEndpointsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /endpoint/{apiId}/{endpointId}
```

Retrieve an endpoint (`getUserFacingEndpoint`)
Retrieve details for an endpoint

Path parameters

`apild` (required)

Path Parameter

— The API ID format: int64

endpointId (required)

Path Parameter

— The endpoint ID format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetEndpointResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "fullPath" : "/base/api/{param}",
    "path" : "/api/{param}",
    "sensitiveDataClassificationList" : [ {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }, {
      "lastSeen" : 1556735907,
      "location" : "RESPONSE",
      "classification" : "large_us_city",
      "locationPath" : "users/user/name/address"
    }],
    "method" : "GET",
    "violationActions" : {
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY"
    },
    "id" : 1234,
    "duplicateOfEndpointId" : 1234,
    "internalEndpointId" : 0,
    "specificationViolationAction" : "ALERT_ONLY",
    "defaultEndpointType" : "INVALID_URL"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetEndpointResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
post /endpoint/{apiId}/{endpointId}
```

Update an endpoint (updateEndpoint)

Update an endpoint API Specification Violation Action

Path parameters

apild (required)

Path Parameter

— The API ID format: int64

endpointId (required)

Path Parameter

— The endpoint ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Form parameters

specificationViolationAction (optional)

Form Parameter

violationActions (optional)
Form Parameter

Return type

[UpdateEndpointResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : {  
    "endpointId" : 1234567890  
  }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

Success [UpdateEndpointResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

Microsensors

```
delete /v3/provisioner/microsensors/{microsensor_id}
```

Delete a specific Microsensor and its instances (deleteMicrosensor)
Delete a specific Microsensor and its instances

Path parameters

microsensor_id (required)

Path Parameter

— Microsensor Id format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success

400

Bad input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/microsensors/{microsensor_id}
```

Retrieve the package details for a specific Microsensor (getMicrosensor)

Retrieve the package details for a specific Microsensor

Path parameters

microsensor_id (required)

Path Parameter

— Microsensor Id format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetMicrosensorResponseV3](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "instances" : [ {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "healthStatus" : "Active",
      "networkInterface" : "eth0",
      "ipAddress" : "1.1.1.1",
      "services" : [ {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      }, {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      } ],
      "firstSeenAt" : 0,
      "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
    }, {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "healthStatus" : "Active",
      "networkInterface" : "eth0",
      "ipAddress" : "1.1.1.1",
      "services" : [ {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      }, {
        "stats" : {
          "lastSeenCpu" : 40.56,
          "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
      } ]
    }
  }
}
```

```

        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
}, {
"microsensorType" : "Universal Log Consumer",
"controller" : 3421,
"instances" : [ {
"hostName" : "docker-desktop",
"instanceId" : "1234",
"healthStatus" : "Active",
"networkInterface" : "eth0",
"ipAddress" : "1.1.1.1",
"services" : [ {
"stats" : {
"lastSeenCpu" : 40.56,
"lastSeenMemory" : 11956224
},
"name" : "data",
"version" : "1.1b"
}, {
"stats" : {
"lastSeenCpu" : 40.56,
"lastSeenMemory" : 11956224
},
"name" : "data",
"version" : "1.1b"
} ],
"firstSeenAt" : 0,
"uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
"hostName" : "docker-desktop",
"instanceId" : "1234",
"healthStatus" : "Active",
"networkInterface" : "eth0",
"ipAddress" : "1.1.1.1",
"services" : [ {
"stats" : {
"lastSeenCpu" : 40.56,
"lastSeenMemory" : 11956224
},
"name" : "data",
"version" : "1.1b"
}, {
"stats" : {

```

```

        "lastSeenCpu" : 40.56,
        "lastSeenMemory" : 11956224
    },
    "name" : "data",
    "version" : "1.1b"
} ],
"firstSeenAt" : 0,
"uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetMicrosensorResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/microsensors/{microsensor_id}/microsensor-instances/{microsensor_instance_id}
```

Retrieve the details of a specific Microsensor Instance for a specific Microsensor (getMicrosensorInstance)
 Retrieve the details of a specific Microsensor Instance for a specific Microsensor

Path parameters

microsensor_id (required)

Path Parameter

— Microsensor Id format: int64

microsensor_instance_id (required)

Path Parameter

— Microsensor Instance Id

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetMicrosensorInstanceResponseV3](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
      "stats" : {
        "lastSeenCpu" : 40.56,
        "lastSeenMemory" : 11956224
      },
      "name" : "data",
      "version" : "1.1b"
    }, {
      "stats" : {
        "lastSeenCpu" : 40.56,
        "lastSeenMemory" : 11956224
      },
      "name" : "data",
      "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
  }, {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "ipAddress" : "1.1.1.1",
    "networkInterface" : "eth0",
    "services" : [ {
      "name" : "data",
      "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "lastSeenAt" : 1677721600000
  } ]
}
```

```

"healthStatus" : "Active",
"networkInterface" : "eth0",
"ipAddress" : "1.1.1.1",
"services" : [ {
  "stats" : {
    "lastSeenCpu" : 40.56,
    "lastSeenMemory" : 11956224
  },
  "name" : "data",
  "version" : "1.1b"
}, {
  "stats" : {
    "lastSeenCpu" : 40.56,
    "lastSeenMemory" : 11956224
  },
  "name" : "data",
  "version" : "1.1b"
} ],
"firstSeenAt" : 0,
"uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetMicrosensorInstanceResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No microSensorInstance found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/provisioner/microsensors/{microsensor_id}/microsensor-instances/{microsensor_instance_id}/stats
```

Retrieve the CPU and Memory usage statistics of a specific Microsensor Instance for a specific Microsensor
(getMicrosensorInstanceStats)

Retrieve the CPU and Memory usage statistics of a specific Microsensor Instance for a specific Microsensor

Path parameters

microsensor_id (required)

Path Parameter

— Microsensor Id format: int64

microsensor_instance_id (required)

Path Parameter

— Microsensor Instance Id

Query parameters

start_time (optional)

Query Parameter

— Start Time format: int64

end_time (optional)

Query Parameter

— End Time format: int64

interval (optional)

Query Parameter

— Interval

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetMicrosensorInstanceStatsResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
      "stats" : {
        "memory" : [ 11956224, 24365465, 24565767 ],
        "cpu" : [ 23.6, 45.33, 67.21, 21.56 ]
      },
      "name" : "data",
      "version" : "1.1b"
    }, {
      "stats" : {
        "memory" : [ 11956224, 24365465, 24565767 ],
        "cpu" : [ 23.6, 45.33, 67.21, 21.56 ]
      }
    } ]
  } ]
}
```

```

        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "memory" : [ 11956224, 24365465, 24565767 ],
            "cpu" : [ 23.6, 45.33, 67.21, 21.56 ]
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "memory" : [ 11956224, 24365465, 24565767 ],
            "cpu" : [ 23.6, 45.33, 67.21, 21.56 ]
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetMicrosensorInstanceStatsResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No stats found with given microsensor Instance Id [ApiFailureResponseV3](#)

500

Internal error ApiFailureResponseV3

```
put /v3/provisioner/microsensors/{microsensor_id}
```

Update details for a specific Microsensor (updateMicrosensor)
 Update details for a specific Microsensor

Path parameters

microsensor_id (required)

Path Parameter

— Microsensor Id format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body UpdateMicrosensorRequest (required)

Body Parameter

— Update Microsensor Request

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

UpdateMicrosensorResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,
    "instances" : [ {
      "hostName" : "docker-desktop",
      "instanceId" : "1234",
      "status" : "OK"
    }
  ]
}
```

```

    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875
}, {
    "microsensorType" : "Universal Log Consumer",
    "controller" : 3421,

```

```

"instances" : [ {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
}, {
    "hostName" : "docker-desktop",
    "instanceId" : "1234",
    "healthStatus" : "Active",
    "networkInterface" : "eth0",
    "ipAddress" : "1.1.1.1",
    "services" : [ {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    }, {
        "stats" : {
            "lastSeenCpu" : 40.56,
            "lastSeenMemory" : 11956224
        },
        "name" : "data",
        "version" : "1.1b"
    } ],
    "firstSeenAt" : 0,
    "uuid" : "45fb3fd4-085d-11ee-be56-0242ac120002"
} ],
"modifiedAt" : 1556735907,
"filePath" : "/microsensor/537881/network_packet_sniffer_kubernetes.zip",
"description" : "Microsensor to sniff data from Security API",
"microsensorId" : 10,
"tags" : "Security API",
"createdAt" : 1556735907,
"apiToken" : "iakasd-sdfsadas",
"createdBy" : "John Doe",
"infrastructureType" : "Kubernetes",
"name" : "Security API Microsensor",
"modifiedBy" : "John Doe",
"apiId" : 123496875

```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UpdateMicrosensorResponseV3](#)

400

Bad input error [ApiFailureResponseV3](#)

404

No Controller found with given Id [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

Provisioner

```
post /v3/provisioner/download
```

Download a specific controller package, or microsensor package, or their supporting files
(downloadFilesFromS3Path)

Download a specific controller package, or microsensor package, or their supporting files

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [FileRequest](#) (required)

Body Parameter

— File Request

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success

400

Bad input error [ApiFailureResponseV3](#)

404

Not Found [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

Reports

```
post /v3/reports
```

Create a new report (createReport)

Creates a new report based on the configuration provided.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateReportRequest](#) (required)

Body Parameter

— Create Report Dto

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetReportResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 67890,
    "lastModifiedByUserName" : "jane_doe",
    "createdDate" : "2000-01-23T04:56:07.000+00:00",
    "createdUserId" : 42,
    "reportId" : "12345",
    "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
    "reportConfiguration" : "{\"siteId\":\"123\",\"siteName\":\"site 1\",\"startTime\":1556735907,\"endTime\":1556735907}",
    "name" : "Monthly Report",
    "createUser" : "john_doe",
    "type" : "RISK_REPORT",
    "lastModifiedByUserId" : 43,
    "status" : "Completed"
  }, {
    "accountId" : 67890,
    "lastModifiedByUserName" : "jane_doe",
    "createdDate" : "2000-01-23T04:56:07.000+00:00",
    "createdUserId" : 42,
    "reportId" : "12345",
    "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
    "reportConfiguration" : "{\"siteId\":\"123\",\"siteName\":\"site 1\",\"startTime\":1556735907,\"endTime\":1556735907}",
    "name" : "Monthly Report",
    "createUser" : "john_doe",
    "type" : "RISK_REPORT",
    "lastModifiedByUserId" : 43,
    "status" : "Completed"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Report created successfully [GetReportResponse](#)

400

Bad Input error [ApiFailureResponseV3](#)

500

[Internal error ApiFailureResponseV3](#)

```
delete /v3/reports/{reportId}
```

Delete a report (deleteReport)
Deletes a specific report

Path parameters

reportId (required)
Path Parameter
— format: uuid

Query parameters

caid (optional)
Query Parameter
— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
format: int64

Return type

Object

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`
- `application/json`

Responses

204

Report deleted successfully Object

400

Bad Input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/reports
```

Get all reports (getReport)
Retrieves all reports

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetReportResponse](#)

Example data

Content-Type: `application/json`

```
{
  "data" : [ {
```

```

"accountId" : 67890,
"lastModifiedByUserName" : "jane_doe",
"createdDate" : "2000-01-23T04:56:07.000+00:00",
"createdUserId" : 42,
"reportId" : "12345",
"lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
"reportConfiguration" : "{\"siteId\":\"123\",\"siteName\":\"site 1\",\"startTime\":1556735907,\"endTime\":1556735907}",
"name" : "Monthly Report",
"createUser" : "john_doe",
"type" : "RISK_REPORT",
"lastModifiedByUserId" : 43,
"status" : "Completed"
}, {
"accountId" : 67890,
"lastModifiedByUserName" : "jane_doe",
"createdDate" : "2000-01-23T04:56:07.000+00:00",
"createdUserId" : 42,
"reportId" : "12345",
"lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
"reportConfiguration" : "{\"siteId\":\"123\",\"siteName\":\"site 1\",\"startTime\":1556735907,\"endTime\":1556735907}",
"name" : "Monthly Report",
"createUser" : "john_doe",
"type" : "RISK_REPORT",
"lastModifiedByUserId" : 43,
"status" : "Completed"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Report retrieved successfully [GetReportResponse](#)

400

Bad Input error [ApiFailureResponseV3](#)

500

Internal error [ApiFailureResponseV3](#)

```
get /v3/reports/{reportId}
```

Get report data (getReportData)
Retrieves the data of a specific report

Path parameters

reportId (required)
Path Parameter
— format: uuid

Query parameters

caid (optional)
Query Parameter
— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetReportDataResponse

Example data

Content-Type: application/json

```
{  
    "data" : [ "", "" ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Report data retrieved successfully GetReportDataResponse

400

Bad Input error ApiFailureResponseV3

500

Internal error ApiFailureResponseV3

```
get /v3/reports/status
```

Get all report statuses (getReportStatus)
Retrieves all report statuses

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetReportStatusResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "reportId" : "12345",
    "status" : "Completed"
  }, {
    "reportId" : "12345",
    "status" : "Completed"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Report instance retrieved successfully GetReportStatusResponse

400

Bad Input error ApiFailureResponseV3

500**Internal error ApiFailureResponseV3**

SITES

```
get /v3/sites
```

Retrieves all site details (getSitesForAccount)
 Retrieves all site details for the account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[GetSiteDetailsResponse]

Example data

Content-Type: application/json

```
[ {
  "siteDtoList" : [ {
    "accountId" : 0,
    "internalSiteId" : 6,
    "hosts" : 12345,
    "siteId" : 12345,
    "siteName" : "host.com",
    "siteType" : "CWFANYWHERE"
  }, {
    "accountId" : 0,
    "internalSiteId" : 6,
    "hosts" : 12345,
    "siteId" : 12345,
    "siteName" : "host.com",
    "siteType" : "CWFANYWHERE"
  } ]
}, {
  "siteDtoList" : [ {
    "accountId" : 0,
    "internalSiteId" : 6,
    "hosts" : 12345,
    "siteId" : 12345,
    "siteName" : "host.com",
    "siteType" : "CWFANYWHERE"
  }, {
    "accountId" : 0,
```

```

    "internalSiteId" : 6,
    "hosts" : 12345,
    "siteId" : 12345,
    "siteName" : "host.com",
    "siteType" : "CWAF, ANYWHERE"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success

500

Internal error [ApiFailureResponse](#)

SiteConfiguration

```
get /config/site
```

Retrieves all site configurations (getSiteConfigurationForAccount)
Retrieves configuration settings for all sites in the account.

Query parameters

`filterActiveOnly` (optional)
Query Parameter

`caid` (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetSiteConfigurationsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludeB
asePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "accountId" : 0,
    "discoveryEnabled" : true,
    "siteId" : 6,
    "siteName" : "example.com",
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludeB
asePath" ],
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "lastModified" : 1556735907,
    "apiOnlySite" : true
  }, {
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludeB
asePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "accountId" : 0,
    "discoveryEnabled" : true,
    "siteId" : 6,
    "siteName" : "example.com",
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludeB
asePath" ],
    "violationActions" : {
      "otherTrafficViolationAction" : "ALERT_ONLY",
      "invalidMethodViolationAction" : "ALERT_ONLY",
      "invalidParamNameViolationAction" : "ALERT_ONLY",
      "invalidParamValueViolationAction" : "ALERT_ONLY",
      "missingParamViolationAction" : "ALERT_ONLY",
      "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "lastModified" : 1556735907,
    "apiOnlySite" : true
  } ]
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteConfigurationsResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
get /config/site/{siteId}
```

Retrieves a site configuration (getSiteConfigurationForSite)

Retrieves the configuration settings for a specific site

Path parameters

`siteId` (required)

Path Parameter

— The site ID format: int64

Query parameters

`caId` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetSiteConfigurationResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "discoveryExcludebasePath" : [ "discoveryExcludebasePath", "discoveryExcludebasePath" ],
    "isAutomaticDiscoveryApiIntegrationEnabled" : true,
    "nonApiRequestViolationAction" : "nonApiRequestViolationAction",
    "accountId" : 0,
    "discoveryEnabled" : true,
```

```

    "siteId" : 6,
    "siteName" : "example.com",
    "discoveryIncludebasePath" : [ "discoveryIncludebasePath", "discoveryIncludebasePath" ],
    "violationActions" : {
        "otherTrafficViolationAction" : "ALERT_ONLY",
        "invalidMethodViolationAction" : "ALERT_ONLY",
        "invalidParamNameViolationAction" : "ALERT_ONLY",
        "invalidParamValueViolationAction" : "ALERT_ONLY",
        "missingParamViolationAction" : "ALERT_ONLY",
        "invalidUrlViolationAction" : "ALERT_ONLY"
    },
    "lastModified" : 1556735907,
    "apiOnlySite" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetSiteConfigurationResponse](#)

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

```
post /config/site/{siteId}
```

Updates site configuration (updateSiteConfiguration)

Updates the site configuration with settings such as attack policy and more as the optional parameters

Path parameters

`siteId` (required)

Path Parameter

— The site ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body SiteConfigurationResponse (required)

Body Parameter

— Settings for attack policy and more

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

UpdateSiteConfigurationResponse

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : {  
    "siteId" : 12345  
  }  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success UpdateSiteConfigurationResponse

400

Bad request [SimpleTextErrorResponse](#)

500

Internal error [SimpleTextErrorResponse](#)

Verification

```
delete /v2/shift-left/actions/{actionId}
```

Delete an action (deleteAction)

Deletes a specified action from the account.

Path parameters

actionId (required)

Path Parameter

— The ActionId format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Boolean

Example data

Content-Type: application/json

```
true
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

No Content Boolean

404

Resource not found [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions/{actionId}/actionType/{actionTypeId}
```

Download reports (downloadResults)

Downloads the requested reports for a specified action

Path parameters

actionId (required)

Path Parameter

— Action Id format: int64

actionTypeld (required)

Path Parameter

— Action Type Id format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
{
  "name" : "name",
  "comment" : "comment"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/zip

Responses

200

Success [inline_response_200](#)

400

Bad Request [ApiFailureResponse](#)

404

Resource not found [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions/action-types
```

Retrieve all action types for an account (getActionTypes)
Retrieves details of all action types for the account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetActionTypesResponse](#)

Example data

Content-Type: application/json

```
{  
  "data" : [ {
```

```

    "actionType" : "SECURITY_TEST_PKG",
    "actionTypeId" : 123,
    "actionTypeDisplayName" : "Generate security test"
} , {
    "actionType" : "SECURITY_TEST_PKG",
    "actionTypeId" : 123,
    "actionTypeDisplayName" : "Generate security test"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetActionTypesResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions
```

Retrieve all actions for an account (getActions)

Retrieves details of all actions for the account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetActionsResponse](#)

Example data

Content-Type: application/json

```
{
```

```

"data" : [ {
  "hasValidationErrors" : true,
  "apiBundleName" : "Test.zip",
  "actionId" : 123,
  "lastModifiedUser" : "lastModifiedUser",
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "source" : "Discovery",
  "actionTypes" : [ {
    "errMsg" : "Error in processing request",
    "id" : 123,
    "type" : "SECURITY_TEST_PKG",
    "status" : "IN_PROGRESS"
  }, {
    "errMsg" : "Error in processing request",
    "id" : 123,
    "type" : "SECURITY_TEST_PKG",
    "status" : "IN_PROGRESS"
  } ]
}, {
  "hasValidationErrors" : true,
  "apiBundleName" : "Test.zip",
  "actionId" : 123,
  "lastModifiedUser" : "lastModifiedUser",
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "source" : "Discovery",
  "actionTypes" : [ {
    "errMsg" : "Error in processing request",
    "id" : 123,
    "type" : "SECURITY_TEST_PKG",
    "status" : "IN_PROGRESS"
  }, {
    "errMsg" : "Error in processing request",
    "id" : 123,
    "type" : "SECURITY_TEST_PKG",
    "status" : "IN_PROGRESS"
  } ]
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [GetActionsResponse](#)

500

Internal error [ApiFailureResponse](#)

```
get /v2/shift-left/actions/{actionId}/validate
```

Retrieve all validation errors for an actionId (getValidationErrors)
Retrieves details of all validation errors for an actionId

Path parameters

actionId (required)

Path Parameter

— The ActionId format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Json

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*
- application/json

Responses

200

Success Json

500

Internal error ApiFailureResponse

```
post /v2/shift-left/files/discovery
```

Uploads discovered APIs (uploadDiscoveredHostsSpecFiles)

Uploads the OAS file generated by the Discovery engine which contains discovered APIs for a selected host

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **string** (optional)

Body Parameter

— Selected host ids

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

UploadFileSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : {
    "hasValidationErrors" : true,
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "source" : "Discovery",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }, {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    } ]
  }
}
```

```

    "errMsg" : "Error in processing request",
    "id" : 123,
    "type" : "SECURITY_TEST_PKG",
    "status" : "IN_PROGRESS"
  } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UploadFileSuccessResponse](#)

500

Internal error [ApiFailureResponse](#)

```
post /v2/shift-left/files/oas
```

Upload an OAS file (`uploadFile`)
Uploads an OAS file manually.

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Form parameters

`actionTypes` (optional)

Form Parameter

`file` (optional)

Form Parameter
— format: binary

Return type

[UploadFileSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : {
    "hasValidationErrors" : true,
    "apiBundleName" : "Test.zip",
    "actionId" : 123,
    "lastModifiedUser" : "lastModifiedUser",
    "lastModified" : "2000-01-23T04:56:07.000+00:00",
    "source" : "Discovery",
    "actionTypes" : [ {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    }, {
      "errMsg" : "Error in processing request",
      "id" : 123,
      "type" : "SECURITY_TEST_PKG",
      "status" : "IN_PROGRESS"
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Success [UploadFileSuccessResponse](#)

400

Bad Request [ApiFailureResponse](#)

500

Internal error [ApiFailureResponse](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [AccessibilityInfo](#)
 3. [Action](#)
 4. [ActionType](#)
 5. [ActionTypeMap](#)
 6. [AddApiResponse](#)
 7. [AddApiResponseValue](#)
 8. [ApiFailureResponse](#)
 9. [ApiFailureResponseV3](#)
 10. [ApiResponse](#)
 11. [ApiResult](#)
 12. [ApiSuccessResponse](#)
 13. [ApiViolationActions](#)
 14. [ApiWithEndpointResponse](#)
 15. [AuthParameterLocationDto](#)
 16. [AuthParameterLocationResponse](#)
 17. [AuthParameterSettings](#)
 18. [AuthenticationInfo](#)
 19. [BflaAccountSettingsDto](#)
 20. [BflaEndpointDiscoverySettings](#)
 21. [BflaSiteDiscoverySettings](#)
 22. [BolaEndpointDiscoverySettings](#)
 23. [BolaManualEndpointSetting](#)
 24. [BolaManualSiteSettings](#)
 25. [BolaSettingsDto](#)
 26. [BolaSiteDiscoverySettings](#)
 27. [CategoriesAndDataLabelsDto](#)
 28. [CategoryDto](#)
 29. [ClassificationRiskVolumeStatistics](#)
 30. [ClassificationStatistics](#)
 31. [ClassificationVolumeStatistics](#)
 32. [Console](#)
 33. [ConsoleInstance](#)
 34. [ConsoleInstanceStateStats](#)
-

-
- 35. ConsoleInstanceStats
 - 36. ConsoleService
 - 37. ConsoleServiceHealthStatus
 - 38. ConsoleSummary
 - 39. Controller
 - 40. ControllerInstance
 - 41. ControllerInstanceService
 - 42. ControllerInstanceStats
 - 43. ControllerService
 - 44. ControllerServiceHealthStatus
 - 45. Cookies
 - 46. CreateConsole
 - 47. CreateConsoleResponseV3
 - 48. CreateController
 - 49. CreateMicrosensor
 - 50. CreateReportRequest
 - 51. DataExposureInfo
 - 52. DataLabelDto
 - 53. DataLabelRegexDto
 - 54. DataLabelSettings
 - 55. DataTypeDto
 - 56. DeleteEndpointResponse
 - 57. DeletedEndpointDto
 - 58. DeletedEndpointResponse
 - 59. DeploymentStatus
 - 60. DeprecatedApiSettings
 - 61. DiscoveredApisSummary
 - 62. DiscoveredCookies
 - 63. DiscoveredEndpoint
 - 64. DiscoveredHeaders
 - 65. DiscoveryAccountSettings
 - 66. DiscoveryEndpointDto
 - 67. DownloadApiSpecificationDtoResponse
 - 68. DuplicateEndpointResponse
 - 69. EndpointClassificationStatistics
 - 70. EndpointDetails
 - 71. EndpointDrillDown
 - 72. EndpointDrillDownDtoV2
 - 73. EndpointRequest
 - 74. EndpointResponse
 - 75. EndpointSettingsDto
 - 76. EndpointSources
 - 77. EndpointStatisticsSummary
-

-
- 78. EndpointStatusDrillDownDto
 - 79. EndpointViolationActions
 - 80. EndpointVolumeStatistics
 - 81. EndpointsPerHost
 - 82. EndpointsPerLabel
 - 83. Error
 - 84. ExceptionDto
 - 85. ExcessiveDataExposureSettings
 - 86. FileRequest
 - 87. GeolocationCountryStatistics
 - 88. GeolocationStatistics
 - 89. GetActionTypesResponse
 - 90. GetActionsResponse
 - 91. GetAllDataLabelsResponse
 - 92. GetApiResponse
 - 93. GetApisResponse
 - 94. GetApisWithEndpointsResponse
 - 95. GetBflaAccountSettingsResponse
 - 96. GetBflaSiteSettingsResponse
 - 97. GetBolaAccountSettingsResponse
 - 98. GetBolaSiteSettingsResponse
 - 99. GetConsoleInstanceResponseV3
 - 100. GetConsoleInstanceServiceStatsResponseV3
 - 101. GetConsoleResponseV3
 - 102. GetConsolesResponse
 - 103. GetControllerInstanceResponseV3
 - 104. GetControllerInstanceServiceResponseV3
 - 105. GetControllerResponseV3
 - 106. GetControllersResponse
 - 107. GetDashboardClassificationStatisticsSuccessfulResponse
 - 108. GetDashboardGeneralStatisticsSuccessfulResponse
 - 109. GetDashboardGeolocationStatisticsSuccessfulResponse
 - 110. GetDashboardVolumeStatisticsSuccessfulResponse
 - 111. GetDiscoveredEndpointsResponse
 - 112. GetDiscoveryAccountSettingsResponse
 - 113. GetEndpointDrillDownResponse
 - 114. GetEndpointResponse
 - 115. GetEndpointsResponse
 - 116. GetHostsResponse
 - 117. GetMicrosensorInstanceResponseV3
 - 118. GetMicrosensorInstanceStatsResponseV3
 - 119. GetMicrosensorResponseV3
 - 120. GetMicrosensorsResponse
-

121. GetReportDataResponse
122. GetReportResponse
123. GetReportStatusResponse
124. GetSiteConfigurationResponse
125. GetSiteConfigurationsResponse
126. GetSiteDetailsResponse
127. GetSiteDiscoverySettingsListResponse
128. GetSiteDiscoverySettingsResponse
129. Headers
130. HealthStatus
131. Host
132. HostClassificationStatistics
133. HostDetails
134. HostVolumeStatistics
135. InventoryDiscoveryData
136. Json
137. Label
138. LabelDtoV2
139. Microsensor
140. MicrosensorInstance
141. MicrosensorInstanceStateService
142. MicrosensorInstanceStateServiceGraphStats
143. MicrosensorInstanceStateServiceStats
144. MicrosensorInstanceStateService
145. MicrosensorInstanceWithGraphStats
146. MicrosensorSummary
147. NumberOfEndpointsByRisks
148. ObjectDto
149. ParameterDrillDown
150. ParserErrorResponse
151. ParserInfo
152. PathParamSegments
153. RecoverEndpointRequest
154. Report
155. ReportConfigurationDto
156. ReportData
157. ReportInsights
158. ReportRequest
159. ReportStatus
160. RequestDrillDown
161. ResourceClassificationStatistics
162. ResourceDetails
163. ResourceStatTrend

164. ResourceVolumeStatistics
165. ResponseDrillDown
166. RiskInfo
167. RiskReportAccessibilityData
168. RiskReportAuthData
169. RiskReportData
170. RiskReportDataLabelDto
171. RiskReportEntitiesData
172. RiskReportRequestConfiguration
173. RiskReportSummary
174. RiskReportSummaryAuthData
175. RiskReportSummaryInsights
176. SegmentDetails
177. SensitiveDataClassification
178. SimpleTextErrorResponse
179. SimpleTextSuccessResponse
180. SiteConfigurationResponse
181. SiteDetails
182. SiteDiscoverySettings
183. SiteLevelViolationActions
184. TagDetails
185. UpdateCategoryResponse
186. UpdateConsoleRequest
187. UpdateControllerRequest
188. UpdateDataLabelResponse
189. UpdateEndpointResponse
190. UpdateEndpointResponseValue
191. UpdateMicrosensorRequest
192. UpdateMicrosensorResponseV3
193. UpdateSiteConfigurationResponse
194. UpdateSiteConfigurationResponseValue
195. UploadFileSuccessResponse
196. UsageStatistics
197. VolumeStatistics
198. apiId_endpointId_body
199. api_siteId_body
200. files_oas_body
201. inline_response_200
202. siteId_apiId_body

APIError

code (optional)
String

detail (optional)
String
 id (optional)
String
 source (optional)
map[String, Object]
 status (optional)
Integer
 format: int32
 title (optional)
String

AccessibilityInfo

accessibility (optional)
array[String]
 Accessibility information identified for endpoint
 Enum:

Action

actionId (optional)
Long
 Action Id format: int64
 example: 123
 actionTypes (optional)
array[ActionTypeMap]
 Action Types
 apiBundleName (optional)
String
 API Bundle Name
 example: Test.zip
 hasValidationErrors
Boolean
 lastModified
Date
 format: date-time
 lastModifiedUser
String
 source (optional)
String
 Source Name
 example: Discovery

ActionType

actionType (optional)
String
 Action Type
 example: SECURITY_TEST_PKG
 actionPerformedDisplayName (optional)
String
 Action Type Display Name
 example: Generate security test
 actionPerformedId (optional)
Long

ActionTypeId format: int64
example: 123

ActionTypeMap

errMsg (optional)
String
Error Message
example: Error in processing request
id (optional)
Long
Action Type Map Id format: int64
example: 123
status (optional)
String
Action Type Map Status
example: IN_PROGRESS
type (optional)
String
Action Type
example: SECURITY_TEST_PKG

AddApiResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
[AddApiResponseValue](#)

AddApiResponseValue

apild (optional)
Long
The API specification ID format: int64
example: 1234
duplicateEndpointsList (optional)
[array\[DuplicateEndpointResponse\]](#)
A list of objects representing duplicate endpoints which were not added as part of the action taken because they exist in another API
resultMessage (optional)
String
Additional information on the action taken
example: API 10 was added successfully

ApiFailureResponse

errors
Object

ApiFailureResponseV3

errors (optional)
[array\[APIError\]](#)

ApiResponse

apiSource (optional)

String

The source from which the API was created

Enum:

USER

DISCOVERY

MIXED

example: USER

basePath (optional)

String

The API's basePath

example: /api

creationTime (optional)

Long

The timestamp when this api was created format: int64

example: 1556735907

description (optional)

String

The API's description in the dashboard

example: This is an example API

hostName (optional)

String

The API's host name

example: example.com

id (optional)

Long

The API ID format: int64

example: 1234

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

matchTrailingSlash (optional)

Boolean

When set to <code>true</code>, endpoints with and without a trailing slash are treated as equivalent. For example, <code>/api/v1/resource</code> and <code>/api/v1/resource/</code> will be considered the same.

When set to <code>false</code>, trailing slashes are considered significant, and the endpoints will be treated as different.

example: false

oasFileName (optional)

String

Uploaded oas file name

example: bank.yaml

sitId (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

violationActions (optional)

ApiViolationActions

ApiResult

isError (optional)

Boolean

value (optional)

Object

ApiSuccessResponse

data

Object

meta

Object

ApiViolationActions

invalidMethodViolationAction (optional)

String

The action taken when an invalid method Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidParamNameViolationAction (optional)

String

The action taken when an invalid parameter name Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidParamValueViolationAction (optional)

String

The action taken when an invalid parameter value Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

invalidUrlViolationAction (optional)

String

The action taken when an invalid URL Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

missingParamViolationAction (optional)

String

The action taken when a missing parameter Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

ApiWithEndpointResponse

apiSource (optional)

String

The source from which the API was created

Enum:

USER

DISCOVERY

MIXED

example: USER

basePath (optional)

String

The API's basePath

example: /api

creationTime (optional)

Long

The timestamp when this api was created format: int64

example: 1556735907

description (optional)

String

The API's description in the dashboard

example: This is an example API

endpoints

array[EndpointResponse]

hostName (optional)

String

The API's host name

example: example.com

id (optional)

Long

The API ID format: int64

example: 1234

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

matchTrailingSlash (optional)

Boolean

When set to <code>true</code>, endpoints with and without a trailing slash are treated as equivalent. For example, <code>/api/v1/resource</code> and <code>/api/v1/resource/</code> will be considered the same.

When set to <code>false</code>, trailing slashes are considered significant, and the endpoints will be treated as different.

example: false

oasFileName (optional)

String

Uploaded oas file name

example: bank.yaml

siteld (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

violationActions (optional)

ApiViolationActions

AuthParameterLocationDto

authParameterLocation (optional)

String

Authentication location name

example: http-req-header-x-jwt

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

sitelds (optional)

array[Long]

Sitelds format: int64

example: 1234567
useForFutureWebSites (optional)
Boolean
Enable same configuration for future website on-boarding

AuthParameterLocationResponse

data
array[AuthParameterLocationDto]

AuthParameterSettings

accountId (optional)
Long
The account ID format: int64
example: 12345
auditString (optional)
String
authParameterLocation (optional)
String
Authentication location name
example: http->req->header->jwt
enabled (optional)
Boolean
Enable or disable the authentication location
example: true
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe

AuthenticationInfo

authParameterLocations (optional)
array[AuthParameterLocationDto]
The authentication locations identified
status (optional)
String
The status of the authentication locations identified

BflaAccountSettingsDto

bflaEnabled (optional)
Boolean
Indicates BFLA detection is enabled/disabled for the account
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user

example: John Doe

BflaEndpointDiscoverySettings

bflaEnabled (optional)

Boolean

Indicates BFLA detection is enabled/disabled for the endpoint

endpointId (optional)

Long

The endpoint ID format: int64

example: 1234567890

endpointUrl (optional)

String

The endpoint url

example: /v1/data

hostname (optional)

String

The host's name

example: example.com

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

method (optional)

String

example: POST

tags (optional)

array[TagDetails]

BflaSiteDiscoverySettings

accountId (optional)

Long

The account ID format: int64

example: 12345

bflaEnabled (optional)

Boolean

Indicates BFLA detection is enabled/disabled for the site

endpointSettings (optional)

array[BflaEndpointDiscoverySettings]

Enable or disable endpoint exceptions

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

sitId (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site name

example: example.com

BolaEndpointDiscoverySettings

bolaEnabled (optional)

Boolean

Indicates BOLA detection is enabled/disabled for the endpoint

endpointId (optional)

Long

The endpoint ID format: int64

example: 1234567890

endpointUrl (optional)

String

The endpoint url

example: /v1/data

hostname (optional)

String

The host's name

example: example.com

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

method (optional)

String

example: POST

tags (optional)

array[TagDetails]

BolaManualEndpointSetting

list of bola endpoint manual settings

authLocation (optional)

String

The auth location

example: http-req-header-Authorization

endpointId (optional)

Long

The endpoint id format: int64

example: 123456

paramLocations (optional)

array[String]

list of param locations which are bola susceptible

BolaManualSiteSettings

endpointManualSettings (optional)

array[BolaManualEndpointSetting]

list of bola endpoint manual settings

siteld (optional)

Long

The site id format: int64

example: 123456

BolaSettingsDto

bolaEnabled (optional)

Boolean

Indicates BOLA detection is enabled/disabled for the account

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

BolaSiteDiscoverySettings

accountId (optional)

Long

The account ID format: int64

example: 12345

bolaEnabled (optional)

Boolean

Indicates BOLA detection is enabled/disabled for the site

endpointSettings (optional)

array[BolaEndpointDiscoverySettings]

Enable or disable endpoint exceptions

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

lastModifiedUser (optional)

String

The last modified user

example: John Doe

siteld (optional)

Long

The site ID format: int64

example: 1234567

siteName (optional)

String

The site name

example: example.com

CategoriesAndDataLabelsDto

categoryId (optional)

Long

format: int64

categoryName (optional)

String

dataLabels (optional)

array[DataLabelDto]
 lastModified (optional)
Long
 format: int64
 lastModifiedUser (optional)
String
 type (optional)
String

CategoryDto

id (optional)
Long
 format: int64
 lastModified (optional)
Long
 format: int64
 lastModifiedUser (optional)
String
 name (optional)
String

ClassificationRiskVolumeStatistics

percent (optional)
Integer
 format: int32
 risk (optional)
String
 The type of the risk
 example: Unauthenticated
 volume (optional)
Long
 format: int64

ClassificationStatistics

allClassificationVolumeStatistics (optional)
 array[ClassificationVolumeStatistics]
 The collection of endpoints which had both sensitive and non sensitive label in the time window
 endpointsClassificationStatistics (optional)
 array[EndpointClassificationStatistics]
 The collection of endpoints which had a label in the time window
 endpointsOWASPTop10Risks (optional)
ResourceStatTrend
 endpointsOtherRisks (optional)
ResourceStatTrend
 hostsClassificationStatistics (optional)
 array[HostClassificationStatistics]
 The collection of hosts which had any label in the time window
 labeledEndpoints (optional)
ResourceStatTrend
 labeledHosts (optional)
ResourceStatTrend
 labeledResources (optional)
ResourceStatTrend

labelsIdentified (optional)
ResourceStatTrend
nonSensitiveClassificationVolumeStatistics (optional)
array[ClassificationVolumeStatistics]
The collection of endpoints which had non sensitive label in the time window
resourcesClassificationStatistics (optional)
array[ResourceClassificationStatistics]
The collection of resources which had any label in the time window
risksIdentified (optional)
ResourceStatTrend
riskyEndpoints (optional)
ResourceStatTrend
sensitiveClassificationVolumeStatistics (optional)
array[ClassificationVolumeStatistics]
The collection of endpoints which had sensitive label in the time window
topRisksVolumeStatistics (optional)
array[ClassificationRiskVolumeStatistics]
The collection of endpoints that had top risks in the time window

ClassificationVolumeStatistics

label (optional)
String
The name of the label
example: generalinfo@email
percent (optional)
Integer
format: int32
volume (optional)
Long
format: int64

Console

Contains the response Body
accountId (optional)
Long
Account Id format: int64
apiId (optional)
Long
Api Id format: int64
apiToken (optional)
String
Api Token
createdAt (optional)
Long
Created At format: int64
example: 1556735907
createdBy (optional)
String
Created by
example: John Doe
deploymentsFilePath (optional)
String
deploymentsFilePath
example: templates/console/falcon-console-0.1.0.tgz
description (optional)

String
Description
id (optional)
Long
 Console Id format: int64
infrastructureType (optional)
String
 Infrastructure Type
instances (optional)
array[ConsoleInstance]
 Console Instances
modifiedAt (optional)
Long
 Modified At format: int64
example: 1556735907
modifiedBy (optional)
String
 Modified By
example: John Doe
name (optional)
String
 Console name
tags (optional)
array[String]
Tags
example: ["tag1", "tag2"]
valuesFilePath (optional)
String
valuesFilePath
example: provisioner/accounts/1234/console/519113/values.yaml

ConsoleInstance

Contains the response Body
deployment (optional)
DeploymentStatus
firstSeenAt (optional)
Long
 Timestamp when instance was first identified format: int64
health (optional)
HealthStatus
instanceId (optional)
String
 Id of the instance
example: 1234
services (optional)
array[ConsoleService]
 Service Health Status
version (optional)
String
 version of console
example: 1.1b

ConsoleInstanceStateStats

Contains the response Body
name (optional)

String

Name of the service

example: abc

replica (optional)

Integer

Replica of consoleInstance format: int32

example: 2

stats (optional)

array[ConsoleInstanceState]

Stats data for cpu and memory

ConsoleInstanceState

cpu (optional)

array[Float]

Stats for cpu usages format: float

example: [23.6,45.33,67.21]

hostname (optional)

String

Hostname for the stats

example: normalizer-9ddb79c5c-lnskc

memory (optional)

array[Long]

Stats for memory usages format: int64

example: [11956224,24365465,24565767]

ConsoleService

health (optional)

ConsoleServiceHealthStatus

name (optional)

String

Name of the service running in Console

example: normalizer

replica (optional)

Integer

Number of replica of the services format: int32

example: 2

ConsoleServiceHealthStatus

reason (optional)

String

Reason for failed status

status (optional)

String

Health status of service running in console

Enum:

Active

Issues

Failed

example: ACTIVE

ConsoleSummary

accountId (optional)

Long
Account Id format: int64
apild (optional)

Long
Api Id format: int64
apiToken (optional)

String
Api Token
createdAt (optional)

Long
Created At format: int64
example: 1556735907
createdBy (optional)

String
Created by
example: John Doe
deploymentsFilePath (optional)

String
deploymentsFilePath
example: templates/console/falcon-console-0.1.0.tgz
description (optional)

String
Description
id (optional)

Long
Console Id format: int64
infrastructureType (optional)

String
Infrastructure Type
modifiedAt (optional)

Long
Modified At format: int64
example: 1556735907
modifiedBy (optional)

String
Modified By
example: John Doe
name (optional)

String
Console name
tags (optional)
array[String]
Tags
example: ["tag1", "tag2"]
valuesFilePath (optional)

String
valuesFilePath
example: provisioner/accounts/1234/console/519113/values.yaml

Controller

Contains the response Body

apild (optional)

Long
API ID to create controller format: int64
example: 123496875
apiToken (optional)

String

API token to create controller

example: iakasd-sdfsadas

createdAt (optional)

Long

Created At format: int64

example: 1556735907

createdBy (optional)

String

Created by

example: John Doe

deploymentsFilePath (optional)

String

deploymentsFilePath

example: /controller/falcon-controller-0.1.0.tgz

description (optional)

String

Description of the controller

example: This is a test controller

id (optional)

Long

Controller Id format: int64

infrastructureType (optional)

String

Infrastructure type of client

Enum:

KUBERNETES

example: [Kubernetes]

instances (optional)

array[ControllerInstance]

Controller Instances

microsensors (optional)

array[MicrosensorSummary]

Microsensor Summary

modifiedAt (optional)

Long

Modified At format: int64

example: 1556735907

modifiedBy (optional)

String

Modified By

example: John Doe

name (optional)

String

Name of the controller

example: TestController

tags (optional)

array[String]

unique labels to identify

example: List ["CC Processing", "US West"]

valuesFilePath (optional)

String

valuesFilePath

example: /accounts/1234/controller/519113/values.yaml

ControllerInstance

Contains the response Body

deployment (optional)

DeploymentStatus
firstSeenAt (optional)
Long
Timestamp when instance was first identified format: int64
health (optional)
HealthStatus
instanceId (optional)
String
Id of the instance
example: 1234
services (optional)
array[ControllerService]
Service Health Status
version (optional)
String
version of controller
example: 1.1b

ControllerInstanceService

Contains the response Body
name (optional)
String
Name of the service
example: abc
replica (optional)
Integer
Replica of controllerInstance format: int32
example: 2
stats (optional)
array[ControllerInstanceStats]
Stats data for cpu and memory

ControllerInstanceStats

cpu (optional)
array[Float]
Stats for cpu usages format: float
example: [23.6,45.33,67.21]
hostname (optional)
String
Hostname for the stats
example: normalizer-9ddb79c5c-lnskc
memory (optional)
array[Long]
Stats for memory usages format: int64
example: [11956224,24365465,24565767]

ControllerService

health (optional)
ControllerServiceHealthStatus
name (optional)
String
Name of the service running in controller
example: normalizer

replica (optional)

Integer

Number of replica of the services format: int32

example: 2

ControllerServiceHealthStatus

reason (optional)

String

Reason for failed status

status (optional)

String

Health status of service running in controller

Enum:

Active

Issues

example: ACTIVE

Cookies

Cookies

dataTypes (optional)

array[DataTypeDto]

Header data types

example: {

 "type": "Integer"

},

{

 "type": "String"

},

key

String

Header Key

example: X-Item2-Request-ID

labels (optional)

array[LabelDtoV2]

Labels

example: generalinfo:email

required (optional)

Boolean

required

example: false

CreateConsole

description (optional)

String

Description of the console

example: This is a test console

infrastructureType (optional)

String

Infrastructure type of client

Enum:

KUBERNETES

example: KUBERNETES

name (optional)

String
Name of the Console
example: TestConsole
tags (optional)
array[String]
Tags of the Console
example: ["tag1", "tag2"]

CreateConsoleResponseV3

data (optional)
array[ConsoleSummary]
Contains the response Body

CreateController

description (optional)
String
Description of the controller
example: This is a test controller
infrastructureType (optional)
String
Infrastructure type of client
Enum:
KUBERNETES
example: [Kubernetes]
name (optional)
String
Name of the controller
example: TestController
tags (optional)
array[String]
unique labels to identify
example: List ["CC Processing", "US West"]

CreateMicrosensor

description (optional)
String
Microsensor Description
example: Security API Microsensor
infrastructureType (optional)
String
Microsensor Infrastructure Type
Enum:
KUBERNETES
DEBIAN
RPM
WINDOWS_JAVA
WINDOWS_NET_FRAMEWORK
WINDOWS_NET_CORE
WINDOWS_NODEJS
WINDOWS_PYTHON
LINUX_NET_CORE
LINUX_JAVA
LINUX_NODEJS

LINUX_PYTHON
ALPINE_LINUX_NET_CORE
ALPINE_LINUX_JAVA
ALPINE_LINUX_NODEJS
ALPINE_LINUX_PYTHON
WAF_GW
example: Kubernetes
microsensorType (optional)
String
Microsensor Type
Enum:
NETWORK_PACKET_SNIFFER
LOG_CONSUMER
RUNTIME_SENSOR
WAF_GW
example: Universal Log Consumer
name (optional)
String
Microsensor Name
example: Security API Microsensor
tags (optional)
array[String]
Microsensor Tags
example: Security API

CreateReportRequest

data (optional)
array[ReportRequest]
Contains the request Body

DataExposureInfo

status (optional)
String
The status of the Data Exposure

DataLabelDto

acceleration (optional)
String
categoryId (optional)
Long
format: int64
createdAt (optional)
Long
format: int64
id (optional)
Long
format: int64
isActive (optional)
Boolean
isSensitive (optional)
Boolean
lastModified (optional)
Long

```
format: int64
lastModifiedUser (optional)
String
name (optional)
String
nameRegex (optional)
String
paramLocation (optional)
String
pathOrPathRegex (optional)
String
type (optional)
String
valueRegex (optional)
String
```

DataLabelRegexDto

```
nameRegex (optional)
String
pathRegex (optional)
String
validNameRegex (optional)
Boolean
validPathRegex (optional)
Boolean
validValueRegex (optional)
Boolean
valueRegex (optional)
String
```

DataLabelSettings

```
accountId (optional)
Long
The account ID format: int64
example: 12345
auditString (optional)
String
dataLabel (optional)
String
The data label
example: ssn
dataLabelId (optional)
Long
format: int64
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe
sensitive (optional)
Boolean
Is this data label sensitive
```

example: true
visible (optional)
Boolean
Is this data label visible
example: true

DataTypeDto

Header data types
children (optional)
array[ParameterDrillDown]
Other ParameterDrillDown that are children of this current parameter
example: "type": "String", "children": [{
 "name": "id",
 "dataTypes": ["type" : "String",
] "required": true,
 "labels": [
 {
 "name": "generalinfo:email",
 "sensitive": false,
 "visible": true
 }
]
}]
type (optional)
String
The type of the parameter
example: String

DeleteEndpointResponse

data (optional)
array[ExceptionDto]
Contains the response Body

DeletedEndpointDto

Contains the response Body
deletedAt (optional)
Long
The deleted time format: int64
example: 1721000001000
endpointId (optional)
Long
The endpointId ID format: int64
example: 2911578398
endpointSources (optional)
array[EndpointSources]
The endpoint source info
hostName (optional)
String
The hostName
example: new-host.example.com
id (optional)
Integer
The exception ID format: int32

example: 2
method (optional)

String

The method

example: DELETE
resource (optional)

String

The resource

example: /api/v3/test/new/endpoint/two/88888
siteId (optional)

Long

The site ID format: int64

example: 57365335

userName (optional)

String

The username

DeletedEndpointResponse

data (optional)
array[DeletedEndpointDto]
Contains the response Body

DeploymentStatus

status (optional)
String
Deployment Status
Enum:
Pending
In Progress
Error
Success
example: SUCCESS

DeprecatedApiSettings

deprecatedApiEnabled (optional)
Boolean
inactiveForDays (optional)
Integer
number of days for which API is inactive format: int32
example: 100
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe

DiscoveredApisSummary

numberOfApiDiscoveryStatuses (optional)
map[String, Long]

The number of endpoints per discovery status format: int64
example: {"IN_PROGRESS": 1,"BASELINED": 20, "OTHERS": 2}
numberOfEndpoints (optional)
Long
The total number of endpoints for the account format: int64
numberOfEndpointsWithDataLabels (optional)
map[String, Long]
Number of sensitive and non-sensitive data labels format: int64
example: {"sensitive": 2,"non-sensitive": 5,"total": 7}
numberOfEndpointsWithRisks (optional)
map[String, Long]
The discovered API risks format: int64
example: {"OWASP": 1,"other": 20}
numberOfHosts (optional)
Long
The total number of hosts for all endpoints format: int64
numberOfLabels (optional)
Long
The total number of labels for all endpoints format: int64
numberOfResources (optional)
Long
The total number of resources for all endpoints format: int64

DiscoveredCookies

cookies (optional)
array[Cookies]
Cookies
example: max-age=31536000
dataTypes (optional)
array[DataTypeDto]
Header data types
example: {
 "type": "Integer"
},
{
 "type": "String"
},
headerWithValue (optional)
Boolean
Header With Value
example: false
key
String
Cookie Key
example: user_id
required (optional)
Boolean
required
example: false
type
String
The type of header
Enum:
COOKIE
example: COOKIE

DiscoveredEndpoint

accessibilityInfo (optional)

AccessibilityInfo

authenticationInfo (optional)

AuthenticationInfo

baselinedDate (optional)

Long

The time when endpoint got baselined format: int64

example: 1657886850000

counter (optional)

Integer

Counter for endpoint in case of duplicate/multiple endpoints with same path format: int32

dataExposureInfo (optional)

DataExposureInfo

discoveryDate (optional)

Long

The time when endpoint discovery started format: int64

example: 1657886850000

endpointSources

array[EndpointSources]

hostId (optional)

Long

The ID of the host to which endpoint belongs format: int64

example: 12345

hostName (optional)

String

The name of the host to which endpoint belongs

example: example.com

id (optional)

Long

The endpoint ID format: int64

example: 1234567890

labels

array[Label]

method (optional)

String

The endpoint HTTP method

Enum:

POST

GET

PUT

PATCH

DELETE

HEAD

OPTIONS

DEFAULT

example: GET

parsers

array[String]

resource (optional)

String

The resource (url) to which endpoint belongs

example: /api/users

riskTypes (optional)

array[String]

Enum:

risks (optional)

array[String]
The discovered API risks
risksInfo (optional)
array[RiskInfo]
The discovered API risks' information
sitId (optional)
Long
The ID of the site to which host belongs format: int64
example: 1234567
status (optional)
String
The discovery status for the endpoint
Enum:
IN_PROGRESS
BASELINED
UNDER_INVESTIGATION
DESIGN_ISSUE
DEPRECATED
PROCESS_LIMITATION
example: BASELINED
tags (optional)
array[TagDetails]

DiscoveredHeaders

dataTypes (optional)
array[DataTypeDto]
Header data types
example: {
 "type": "Integer"
},
{
 "type": "String"
},
error (optional)
Error
headerWithValue (optional)
Boolean
Header With Value
example: false
key
String
Header Key
example: X-Item2-Request-ID
labels (optional)
array[LabelDtoV2]
Labels
example: generalinfo:email
required (optional)
Boolean
required
example: false
type
String
The type of header
Enum:
HEADER
example: HEADER

value (optional)
String
Header value

DiscoveryAccountSettings

authParameterSettings (optional)
array[AuthParameterSettings]
Authentication location settings
authenticationEnabled (optional)
Boolean
dataLabelSettings (optional)
array[DataLabelSettings]
Data label settings
deprecatedApiSettings (optional)
DeprecatedApiSettings
excessiveDataExposureSettings (optional)
ExcessiveDataExposureSettings

DiscoveryEndpointDto

Contains the request Body
endpointId (optional)
Long
The endpoint ID format: int64
example: 1234567

DownloadApiSpecificationDtoResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
String

DuplicateEndpointResponse

fullPath (optional)
String
The endpoint full path
example: /api/{param}
id (optional)
Long
The endpoint ID format: int64
example: 1234567890
method (optional)
String
The endpoint HTTP method
Enum:
POST
GET
PUT
PATCH
DELETE
HEAD

OPTIONS

DEFAULT

example: GET

EndpointClassificationStatistics

endpointDetails (optional)

EndpointDetails

firstTimeSeenInCurrentTimePeriod (optional)

Boolean

hostsResourceStatTrend (optional)

ResourceStatTrend

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

labels (optional)

array[Label]

risks (optional)

array[String]

The discovered API risks

risksInfo (optional)

array[RiskInfo]

The discovered API risks info

EndpointDetails

endpointId (optional)

Long

The endpoint ID format: int64

example: 1234567890

endpointUrl (optional)

String

The endpoint url

example: /v1/data

hostname (optional)

String

The host's name

example: example.com

method (optional)

String

example: POST

EndpointDrillDown

accessibilityInfo (optional)

AccessibilityInfo

authenticationInfo (optional)

AuthenticationInfo

endpointStatisticsSummary (optional)

EndpointStatisticsSummary

hostName (optional)

String

The name of the host to which endpoint belongs

example: example.com

method (optional)

String

The method of the endpoint

example: GET
pathParamSegments (optional)
array[PathParamSegments]
Description of path param segments
request (optional)
RequestDrillDown
resource (optional)
String
The resource (url) to which endpoint belongs
example: /api/users
responses (optional)
map[String, ResponseDrillDown]
status (optional)
EndpointStatusDrillDownDto
tags (optional)
array[TagDetails]

EndpointDrillDownDtoV2

accessibilityInfo (optional)
AccessibilityInfo
authenticationInfo (optional)
AuthenticationInfo
endpointId (optional)
Long
format: int64
endpointStatisticsSummary (optional)
EndpointStatisticsSummary
hostName (optional)
String
method (optional)
String
parsers (optional)
array[ParserInfo]
pathParamSegments (optional)
array[PathParamSegments]
resource (optional)
String
status (optional)
EndpointStatusDrillDownDto
tags (optional)
array[TagDetails]

EndpointRequest

data (optional)
array[DiscoveryEndpointDto]
Contains the request Body

EndpointResponse

defaultEndpointType (optional)
String
Type of default endpoint
Enum:
INVALID_URL

INVALID_METHOD

duplicateOfEndpointId (optional)

Long

The ID of the endpoint that this endpoint is the duplicate of format: int64

example: 1234

fullPath (optional)

String

The endpoint full path

example: /base/api/{param}

id (optional)

Long

The endpoint ID format: int64

example: 1234

internalEndpointId (optional)

Long

format: int64

method (optional)

String

The endpoint HTTP method

Enum:

POST

GET

PUT

PATCH

DELETE

HEAD

OPTIONS

DEFAULT

example: GET

path (optional)

String

The endpoint path

example: /api/{param}

sensitiveDataClassificationList (optional)

array[SensitiveDataClassification]

Sensitive data classification list for this endpoint

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

example: ALERT_ONLY

violationActions (optional)

EndpointViolationActions

EndpointSettingsDto

authenticationEnabled (optional)

Boolean

deprecatedApiSettings (optional)

DeprecatedApiSettings

endpointId (optional)

Long

The endpoint ID format: int64
example: 1234567890
endpointUrl (optional)
String
The endpoint url
example: /v1/data
excessiveDataExposureSettings (optional)
ExcessiveDataExposureSettings
hostname (optional)
String
The host's name
example: example.com
method (optional)
String
example: POST
tags (optional)
array[TagDetails]

EndpointSources

id (optional)
Long
Id of the source format: int64
example: 10
name (optional)
String
Source Name
example: Security API Microsensor
sourceType (optional)
String
Type of the source
Enum:
PROXY
NETWORK_PACKET_SNIFFER
LOGCONSUMER
WAF_GATEWAY
RASP_CLIENT
NGNIX_IMPV
ENVOY_IMPV
example: Security API
tags (optional)
array[String]
Microsensor Tags
example: ['Security API','PROD']

EndpointStatisticsSummary

numberOfParametersByDataLabel (optional)
map[String, Integer]
Number of parameters for a specific label format: int32
numberOfParametersWithDataLabels (optional)
map[String, Integer]
Number of total, sensitive and non-sensitive data labels for all parameters format: int32
example: {"sensitive": 2, "non-sensitive": 5, "total": 7}

EndpointStatusDrillDownDto

designIssueReason (optional)
String
 Reason for the DESIGN_ISSUE
 lastModified (optional)
Long
 The last modified timestamp format: int64
 example: 1556735907
 name (optional)
String
 Status of endpoint
 Enum:
 IN_PROGRESS
 BASELINED
 UNDER_INVESTIGATION
 DESIGN_ISSUE
 DEPRECATED
 PROCESS_LIMITATION
 example: BASELINED

EndpointViolationActions

invalidParamNameViolationAction (optional)
String

The action taken when an invalid parameter name Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:
 ALERT_ONLY
 BLOCK_REQUEST
 BLOCK_USER
 BLOCK_IP
 IGNORE
 DEFAULT
 example: ALERT_ONLY

invalidParamValueViolationAction (optional)
String

The action taken when an invalid parameter value Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:
 ALERT_ONLY
 BLOCK_REQUEST
 BLOCK_USER
 BLOCK_IP
 IGNORE
 DEFAULT
 example: ALERT_ONLY

missingParamViolationAction (optional)
String

The action taken when a missing parameter Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:
 ALERT_ONLY
 BLOCK_REQUEST
 BLOCK_USER
 BLOCK_IP
 IGNORE
 DEFAULT

example: ALERT_ONLY

EndpointVolumeStatistics

currentCallPercent (optional)
Integer
format: int32
currentCallVolume (optional)
Long
format: int64
endpointDetails (optional)
EndpointDetails
firstTimeSeenInCurrentTimePeriod (optional)
Boolean
isFirstTimeSeenInCurrentTimePeriod (optional)
Boolean

EndpointsPerHost

hostId (optional)
Long
The host ID format: int64
example: 12345
hostName (optional)
String
The host name
example: example.com
numberOfEndpoints (optional)
Long
The number of endpoints for the specific host format: int64

EndpointsPerLabel

label (optional)
String
The name of the label
example: generalinfo:email
numberOfEndpoints (optional)
Long
The number of endpoints per specific label format: int64

Error

Error
errorMessage (optional)
String
Error message

ExceptionDto

Contains the request Body
id (optional)
Long
The exception ID format: int64
example: 1234567

ExcessiveDataExposureSettings

excessiveDataExposureEnabled (optional)
Boolean
lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907
lastModifiedUser (optional)
String
The last modified user
example: John Doe
responseParameterLimit (optional)
Integer
Response parameters limit format: int32
example: 100
responseParameterWithDataLabelLimit (optional)
Integer
Response parameters with data label limit format: int32
example: 100
responseParameterWithSensitiveDataLabelLimit (optional)
Integer
Response parameters with sensitive data label limit format: int32
example: 100

FileRequest

filePath (optional)
String
S3 File Path
example: templates/controller/falcon-controller-0.1.0.tgz

GeolocationCountryStatistics

code (optional)
String
The country code
example: US
currentCallPercent (optional)
Integer
format: int32
currentCallVolume (optional)
Long
format: int64
name (optional)
String
The country name
example: United States

GeolocationStatistics

clientGeolocationCountryStatisticsDto (optional)
array[GeolocationCountryStatistics]
destinationGeolocationCountryStatisticsDto (optional)
array[GeolocationCountryStatistics]

GetActionTypesResponse

data
array[ActionType]

GetActionsResponse

data
array[Action]

GetAllDataLabelsResponse

data
array[CategoriesAndDataLabelsDto]

GetApiResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
ApiResponse

GetApisResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
array[ApiResponse]

GetApisWithEndpointsResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
array[ApiWithEndpointResponse]

GetBflaAccountSettingsResponse

data
BflaAccountSettingsDto

GetBflaSiteSettingsResponse

data
array[BflaSiteDiscoverySettings]

GetBolaAccountSettingsResponse

data
BolaSettingsDto

GetBolaSiteSettingsResponse

data
array[BolaSiteDiscoverySettings]

GetConsoleInstanceResponseV3

data (optional)
array[ConsoleInstance]
Contains the response Body

GetConsoleInstanceServiceStatsResponseV3

data (optional)
array[ConsoleInstanceServiceStats]
Contains the response Body

GetConsoleResponseV3

data (optional)
array[Console]
Contains the response Body

GetConsolesResponse

data
array[ConsoleSummary]

GetControllerInstanceResponseV3

data (optional)
array[ControllerInstance]
Contains the response Body

GetControllerInstanceServiceResponseV3

data (optional)
array[ControllerInstanceState]
Contains the response Body

GetControllerResponseV3

data (optional)
array[Controller]
Contains the response Body

GetControllersResponse

data
array[Controller]

GetDashboardClassificationStatisticsSuccessfulResponse

data
ClassificationStatistics

GetDashboardGeneralStatisticsSuccessfulResponse

data
UsageStatistics

GetDashboardGeolocationStatisticsSuccessfulResponse

data
GeolocationStatistics

GetDashboardVolumeStatisticsSuccessfulResponse

data
VolumeStatistics

GetDiscoveredEndpointsResponse

data
InventoryDiscoveryData

GetDiscoveryAccountSettingsResponse

data
DiscoveryAccountSettings

GetEndpointDrillDownResponse

data
EndpointDrillDown

GetEndpointResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
EndpointResponse

GetEndpointsResponse

isError (optional)

Boolean

States if an error occurred

example: false

value (optional)

array[EndpointResponse]

GetHostsResponse

data

array[Host]

GetMicrosensorInstanceResponseV3

data (optional)

array[MicrosensorInstance]

Contains the response Body

GetMicrosensorInstanceStatsResponseV3

data (optional)

array[MicrosensorInstanceWithGraphStats]

Contains the response Body

GetMicrosensorResponseV3

data (optional)

array[Microsensor]

Contains the response Body

GetMicrosensorsResponse

data

array[Microsensor]

GetReportDataResponse

data (optional)

array[ReportData]

Contains the response Body

GetReportResponse

data (optional)

array[Report]

Contains the response Body

GetReportStatusResponse

data (optional)

array[ReportStatus]
Contains the response Body

GetSiteConfigurationResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
SiteConfigurationResponse

GetSiteConfigurationsResponse

isError (optional)
Boolean
States if an error occurred
example: false
value (optional)
array[SiteConfigurationResponse]

GetSiteDetailsResponse

siteDtoList
array[SiteDetails]

GetSiteDiscoverySettingsListResponse

data
array[SiteDiscoverySettings]

GetSiteDiscoverySettingsResponse

data
SiteDiscoverySettings

Headers

Headers

HealthStatus

status (optional)
String
Health Status
Enum:
Active
Issues
Failed
Not Available
example: ACTIVE

Host

hostId (optional)

Long

The host ID format: int64

example: 12345

hostName (optional)

String

The host's domain name

example: example.com

siteld (optional)

Long

The site external ID format: int64

example: 1234567

siteName (optional)

String

The site's domain name

example: example.com

HostClassificationStatistics

firstTimeSeenInCurrentTimePeriod (optional)

Boolean

hostDetails (optional)

HostDetails

hostsResourceStatTrend (optional)

ResourceStatTrend

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

labels (optional)

array[Label]

HostDetails

hostname (optional)

String

The host's name

example: example.com

HostVolumeStatistics

currentCallPercent (optional)

Integer

format: int32

currentCallVolume (optional)

Long

format: int64

firstTimeSeenInCurrentTimePeriod (optional)

Boolean

hostDetails (optional)

HostDetails

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

InventoryDiscoveryData

endpoints (optional)
array[DiscoveredEndpoint]
endpointsNumberByHost (optional)
array[EndpointsPerHost]
endpointsNumberByLabel (optional)
array[EndpointsPerLabel]
endpointsNumberByRisk (optional)
array[NumberOfEndpointsByRisks]
summary (optional)
DiscoveredApisSummary

Json**Label**

name (optional)
String
The name of the label
example: generalinfo:email
sensitive (optional)
Boolean
An indication whether the label is sensitive
example: false

LabelDtoV2

Labels
confidence (optional)
Integer
The confidence of the label format: int32
example: 50
labelProgressStatus (optional)
String
The label of the progress
Enum:
UNKNOWN
INITIAL
DEVELOPING
ESTABLISHING
LABEL_DONE
example: LABEL_DONE
name (optional)
String
The name of the label
example: generalinfo:email
sensitive (optional)
Boolean
An indication whether the label is sensitive
example: false
status (optional)
String
The status of the label
Enum:
UNSPECIFIED

IN_PROGRESS

DONE

example: done

Microsensor

apild (optional)

Long

Microsensor apild format: int64

example: 123496875

apiToken (optional)

String

Microsensor apiToken

example: iakasd-sdfsadas

controller (optional)

Long

Controller Id format: int64

example: 3421

createdAt (optional)

Long

Created At format: int64

example: 1556735907

createdBy (optional)

String

Created by

example: John Doe

description (optional)

String

Microsensor Description

example: Microsensor to sniff data from Security API

filePath (optional)

String

Deployment File Path

example: /microsensor/537881/network_packet_sniffer_kubernetes.zip

infrastructureType (optional)

String

Microsensor Infrastructure Type

Enum:

KUBERNETES

DEBIAN

RPM

WINDOWS_JAVA

WINDOWS_NET_FRAMEWORK

WINDOWS_NET_CORE

WINDOWS_NODEJS

WINDOWS_PYTHON

LINUX_NET_CORE

LINUX_JAVA

LINUX_NODEJS

LINUX_PYTHON

ALPINE_LINUX_NET_CORE

ALPINE_LINUX_JAVA

ALPINE_LINUX_NODEJS

ALPINE_LINUX_PYTHON

WAF_GW

example: Kubernetes

instances (optional)

array[MicrosensorInstance]

Microsensor Instance
microsensorId (optional)
Long
Microsensor Id format: int64
example: 10
microsensorType (optional)
String
Microsensor Type
Enum:
NETWORK_PACKET_SNIFFER
LOG_CONSUMER
RUNTIME_SENSOR
WAF_GW
example: Universal Log Consumer
modifiedAt (optional)
Long
Modified At format: int64
example: 1556735907
modifiedBy (optional)
String
Modified By
example: John Doe
name (optional)
String
Microsensor Name
example: Security API Microsensor
tags (optional)
array[String]
Microsensor Tags
example: Security API

MicrosensorInstance

firstSeenAt (optional)
Long
Timestamp when instance was first identified format: int64
healthStatus (optional)
String
Status of health of instance
Enum:
Active
Issues
Inactive
example: Active
hostName (optional)
String
Host name
example: docker-desktop
instanceId (optional)
String
Instance Id
example: 1234
ipAddress (optional)
String
IP Address of sensor
example: 1.1.1.1
networkInterface (optional)
String

Network interface
example: eth0
services (optional)
array[MicrosensorInstanceService]
Microsensor Services
uuid (optional)
String
UUID
example: 45fb3fd4-085d-11ee-be56-0242ac120002

MicrosensorInstanceService

name (optional)
String
Name of the service
example: data
stats (optional)
MicrosensorInstanceServiceStats
version (optional)
String
Version of the service
example: 1.1b

MicrosensorInstanceServiceGraphStats

cpu (optional)
array[Float]
Stats for cpu utilizations format: float
example: [23.6,45.33,67.21,21.56]
memory (optional)
array[Long]
Stats for memory utilizations format: int64
example: [11956224,24365465,24565767]

MicrosensorInstanceServiceStats

lastSeenCpu (optional)
Float
Last seen CPU utilization format: float
example: 40.56
lastSeenMemory (optional)
Long
Last seen Memory utilization format: int64
example: 11956224

MicrosensorInstanceStatsService

name (optional)
String
Name of the service
example: data
stats (optional)
MicrosensorInstanceServiceGraphStats
version (optional)
String
Version of the service

example: 1.1b

MicrosensorInstanceWithGraphStats

Contains the response Body

hostName (optional)

String

Host name

example: docker-desktop

instanceld (optional)

String

Instance Id

example: 1234

ipAddress (optional)

String

IP Address of sensor

example: 1.1.1.1

networkInterface (optional)

String

Network interface

example: eth0

services (optional)

array[MicrosensorInstanceStatsService]

Microsensor Services

uuid (optional)

String

UUID

example: 45fb3fd4-085d-11ee-be56-0242ac120002

MicrosensorSummary

apild (optional)

Long

Microsensor apild format: int64

example: 123496875

apiToken (optional)

String

Microsensor apiToken

example: iakasd-sdfsadas

controller (optional)

Long

Controller Id format: int64

example: 3421

createdAt (optional)

Long

Created At format: int64

example: 1556735907

createdBy (optional)

String

Created by

example: John Doe

description (optional)

String

Microsensor Description

example: Microsensor to sniff data from Security API

filePath (optional)

String

Deployment File Path

example: /microsensor/537881/network_packet_sniffer_kubernetes.zip
 infrastructureType (optional)

String

Microsensor Infrastructure Type

Enum:

KUBERNETES

DEBIAN

RPM

WINDOWS_JAVA

WINDOWS_NET_FRAMEWORK

WINDOWS_NET_CORE

WINDOWS_NODEJS

WINDOWS_PYTHON

LINUX_NET_CORE

LINUX_JAVA

LINUX_NODEJS

LINUX_PYTHON

ALPINE_LINUX_NET_CORE

ALPINE_LINUX_JAVA

ALPINE_LINUX_NODEJS

ALPINE_LINUX_PYTHON

WAF_GW

example: Kubernetes

microsensorId (optional)

Long

Microsensor Id format: int64

example: 10

microsensorType (optional)

String

Microsensor Type

Enum:

NETWORK_PACKET_SNIFFER

LOG_CONSUMER

RUNTIME_SENSOR

WAF_GW

example: Universal Log Consumer

modifiedAt (optional)

Long

Modified At format: int64

example: 1556735907

modifiedBy (optional)

String

Modified By

example: John Doe

name (optional)

String

Microsensor Name

example: Security API Microsensor

tags (optional)

array[String]

Microsensor Tags

example: Security API

NumberOfEndpointsByRisks

numberOfEndpoints (optional)

Long

The number of endpoints for a specific risk format: int64

risk (optional)

String

The type of risk

example: unauthenticated

ObjectDto

objectId (optional)

Long

format: int64

objectPath (optional)

String

paramList (optional)

array[ParameterDrillDown]

ParameterDrillDown

dataTypes (optional)

array[DataTypeDto]

The type of the parameter

example: ["type": "String", "children": [{
 "name": "id",
 "dataTypes": ["type" : "String",
] "required": true,
 "labels": [
 {
 "name": "generalinfo:email",
 "sensitive": false,
 "visible": true
 }
]
}]]

id (optional)

Long

Object id for graphQL object format: int64

labels (optional)

array[LabelDtoV2]

name (optional)

String

The name of the parameter

example: id

required (optional)

Boolean

An indication whether the parameter is required

example: false

ParserErrorResponse

isError (optional)

Boolean

States if an error occurred

example: true

value (optional)

array[String]

ParserInfo

name (optional)
String
queryParamList (optional)
array[ParameterDrillDown]
request (optional)
RequestDrillDown
responses (optional)
map[String, ResponseDrillDown]

PathParamSegments

index (optional)
Integer
Segment index format: int32
example: 1
segmentDetails (optional)
array[SegmentDetails]
path parameter segment details

RecoverEndpointRequest

data (optional)
array[ExceptionDto]
Contains the request Body

Report

Report details
accountId (optional)
Long
Account ID associated with the report format: int64
example: 67890
createUser (optional)
String
Name of the user who created the report
example: john_doe
createdDate (optional)
Date
Report creation date format: date-time
createdUserId (optional)
Long
User ID who created the report format: int64
example: 42
lastModifiedByUserId (optional)
Long
User ID who last modified the report format: int64
example: 43
lastModifiedByUserName (optional)
String
Name of the user who last modified the report
example: jane_doe
lastModifiedDate (optional)
Date
Report last modified date format: date-time

name (optional)
String
Name of the report
example: Monthly Report
reportConfiguration (optional)
String
Configuration for report
example: {"siteId": "123", "siteName": "site 1", "startTime": 1556735907, "endTime": 1556735907}
reportId (optional)
String
Unique identifier of the report
example: 12345
status (optional)
String
Status of the report
Enum:
In Progress
Completed
Failed
example: Completed
type (optional)
String
Type of the report
Enum:
Risk Report
example: RISK_REPORT

ReportConfigurationDto

ReportData

Data for Report

ReportInsights

Report Insights Data
externallyAccessedEndpoints (optional)
RiskReportAccessibilityData
internallyAccessedEndpoints (optional)
RiskReportAccessibilityData
numberOfEndpointRequests (optional)
Long
Total number of endpoint requests format: int64
example: 1000

ReportRequest

Report request details
name (optional)
String
Name of the report
example: Monthly Report
reportConfiguration (optional)
ReportConfigurationDto
type (optional)
String

Type of the report

Enum:

Risk Report

example: RISK_REPORT

ReportStatus

Report status details

reportId (optional)

String

Unique identifier of the report

example: 12345

status (optional)

String

Status of the report

Enum:

In Progress

Completed

Failed

example: Completed

RequestDrillDown

contentTypeToRequestBody (optional)

map[String, array[ParameterDrillDown]]

error (optional)

Error

headerList (optional)

array[Headers]

Header list

isError (optional)

Boolean

is Error

queryParamList (optional)

array[ParameterDrillDown]

ResourceClassificationStatistics

firstTimeSeenInCurrentTimePeriod (optional)

Boolean

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

labels (optional)

array[Label]

resourceDetails (optional)

ResourceDetails

resourceStatTrend (optional)

ResourceStatTrend

ResourceDetails

hostname (optional)

String

The host's name

example: example.com

resourceUrl (optional)

String
example: v1/data

ResourceStatTrend

currentCount (optional)

Long

format: int64

previousCount (optional)

Long

format: int64

trendDirection (optional)

String

Enum:

UP

DOWN

NEUTRAL

trendPercent (optional)

Integer

format: int32

ResourceVolumeStatistics

currentCallPercent (optional)

Integer

format: int32

currentCallVolume (optional)

Long

format: int64

firstTimeSeenInCurrentTimePeriod (optional)

Boolean

isFirstTimeSeenInCurrentTimePeriod (optional)

Boolean

resourceDetails (optional)

ResourceDetails**ResponseDrillDown**

contentTypeToResponseBody (optional)

map[String, array[ParameterDrillDown]]

error (optional)

Error

headerList (optional)

array[Headers]

Header list

isError (optional)

Boolean

is Error

RiskInfo

owaspTag (optional)

String

The OWASP tag associated with the risk

risk (optional)

String

The discovered API risk

riskType (optional)

String

The discovered API risk type

Enum:

OWASP

OTHER

RiskReportAccessibilityData

Data for internally accessed APIs

authenticated (optional)

RiskReportAuthData

numberOfEndpointRequests (optional)

Long

Total number of endpoint requests format: int64

example: 200

unauthenticated (optional)

RiskReportAuthData

RiskReportAuthData

Authentication data for the report

nonSensitive (optional)

RiskReportDataLabelDto

numberOfEndpointRequests (optional)

Long

Total number of endpoint requests format: int64

example: 200

sensitive (optional)

RiskReportDataLabelDto

RiskReportData

apiCallInsights (optional)

ReportInsights

createdTimestamp (optional)

Long

Timestamp when the report was created format: int64

example: 1622547800000

endDate (optional)

Long

End date of the report period format: int64

example: 1625139800000

reportName (optional)

String

Name of the report

example: Monthly Security Report

reportSummary (optional)

RiskReportSummary

sensitiveLabels (optional)

array[LabelDtoV2]

List of sensitive labels

siteName (optional)

String

Site name for which report is created

example: imperva.com
startDate (optional)

Long

Start date of the report period format: int64

example: 1622547800000

userName (optional)

String

Name of the user

example: John Doe

RiskReportDataLabelDto

Summary data for sensitive and non-sensitive API calls

clientApps (optional)

array[RiskReportEntitiesData]

List of client applications making API calls

endpoints (optional)

array[RiskReportEntitiesData]

List of sensitive API calls

hosts (optional)

array[RiskReportEntitiesData]

List of hosts making API calls

numberOfEndpointRequests (optional)

Long

Total number of endpoint requests format: int64

example: 200

RiskReportEntitiesData

Data for entities in the report

count (optional)

Long

Count of the entity format: int64

example: 100

name (optional)

String

Name of the entity

example: EntityName

RiskReportRequestConfiguration

Request Configuration for token risk report

endTime (optional)

Long

End time of the report format: int64

example: 1556735907

siteld (optional)

String

Site ID associated with the report

example: abc-123

startTime (optional)

Long

Start time of the report format: int64

example: 1556735907

RiskReportSummary

Summary of the Risk Report

callInsights (optional)

RiskReportSummaryInsights

nonSensitiveInsights (optional)

RiskReportSummaryInsights

sensitiveInsights (optional)

RiskReportSummaryInsights

RiskReportSummaryAuthData

Summary of the external and internal insights

authenticated (optional)

Long

Summary of the authenticated insights format: int64

example: 100

numberOfEndpointRequests (optional)

Long

Total number of endpoint requests format: int64

example: 150

unAuthenticated (optional)

Long

Summary of the unauthenticated insights format: int64

example: 50

RiskReportSummaryInsights

Summary of the external and internal insights

external (optional)

RiskReportSummaryAuthData

internal (optional)

RiskReportSummaryAuthData

numberOfEndpointRequests (optional)

Long

Total number of endpoint requests format: int64

SegmentDetails

dataType (optional)

String

Data type of path param segment

Enum:

DATE

TIME

EMAIL

IP

NUMBER

MIXED

REGION_LANGUAGE

UUID

WORD

ALPHA_NUMERIC

GENERIC

example: DATE

SensitiveDataClassification

classification (optional)

String

The classification of the sensitive value

example: large_us_city

lastSeen (optional)

Long

The time this sensitive value was seen last format: int64

example: 1556735907

location (optional)

String

The location of the sensitive value

example: RESPONSE

locationPath (optional)

String

The detailed location of the sensitive value in the location (response body) including any parent objects

example: users/user/name/address

SimpleTextErrorResponse

isError (optional)

Boolean

States if an error occurred

example: true

value (optional)

String

SimpleTextSuccessResponse

isError (optional)

Boolean

States if an error occurred

example: false

value (optional)

String

SiteConfigurationResponse

accountId (optional)

Long

The account Id format: int64

apiOnlySite

Boolean

discoveryEnabled (optional)

Boolean

discoveryExcludebasePath (optional)

array[String]

discoveryIncludebasePath (optional)

array[String]

isAutomaticDiscoveryApilIntegrationEnabled (optional)

Boolean

lastModified (optional)

Long

The last modified timestamp format: int64

example: 1556735907

nonApiRequestViolationAction

String

siteId (optional)

Long

The site id format: int64

siteName (optional)

String

The site name

example: example.com

violationActions (optional)

[SiteLevelViolationActions](#)

SiteDetails

accountId

Long

format: int64

hosts (optional)

[array\[Host\]](#)

The host ID

example: 12345

internalSiteId

Long

format: int64

siteId (optional)

Long

The site ID format: int64

example: 12345

siteName (optional)

String

The site name

example: host.com

siteType (optional)

String

Type of site

Enum:

CWAF

ANYWHERE

example: CWAF,ANYWHERE

SiteDiscoverySettings

accountId (optional)

Long

The account ID format: int64

example: 12345

authParameterSettings (optional)

[array\[AuthParameterSettings\]](#)

Authentication location settings

authenticationEnabled (optional)

Boolean

deprecatedApiSettings (optional)

[DeprecatedApiSettings](#)

discoveryExcludePaths (optional)

[array\[String\]](#)

Exclude discovery from these specific base paths

example: ["/test"]

discoveryIncludeOnlyPaths (optional)
array[String]
Set discovery for these specific base paths only
example: `["/api", "/service"]`

endpointSettings (optional)
array[EndpointSettingsDto]
Enable or disable endpoint exceptions

excessiveDataExposureSettings (optional)
ExcessiveDataExposureSettings

isAutomaticDiscoveryApilIntegrationEnabled (optional)
Boolean

isDiscoveryEnabled (optional)
Boolean

lastModified (optional)
Long
The last modified timestamp format: int64
example: 1556735907

lastModifiedUser (optional)
String
The last modified user
example: John Doe

relatedHosts (optional)
array[Host]

sitId (optional)
Long
The site ID format: int64
example: 1234567

siteName (optional)
String
The site name
example: example.com

siteType (optional)
String
Type of Site
Enum:
CWF
ANYWHERE
example: CWF,ANYWHERE

SiteLevelViolationActions

invalidMethodViolationAction (optional)
String
The action taken when an invalid method Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs
Enum:
ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT
example: ALERT_ONLY

invalidParamNameViolationAction (optional)
String
The action taken when an invalid parameter name Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs
Enum:

ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT

example: ALERT_ONLY
invalidParamValueViolationAction (optional)
String

The action taken when an invalid parameter value Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT

example: ALERT_ONLY
invalidUrlViolationAction (optional)
String

The action taken when an invalid URL Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT

example: ALERT_ONLY
missingParamViolationAction (optional)
String

The action taken when a missing parameter Violation occurs. Assigning DEFAULT will inherit the action from parent object, DEFAULT is not applicable for site-level configuration APIs

Enum:

ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT

example: ALERT_ONLY
otherTrafficViolationAction (optional)
String

The action taken when traffic that does not belong to the APIs defined in the OAS files or integrated from API Discovery is identified.

Enum:

ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT

example: ALERT_ONLY

TagDetails

Tags associated with endpoint

id (optional)

Long

The tag ID format: int64

example: 1234567

name (optional)

String

The tag Name

example: My Tag

UpdateCategoryResponse

data

CategoryDto

UpdateConsoleRequest

description (optional)

String

Console Description

example: Security API Microsensor

name (optional)

String

Console Name

example: Security API Microsensor

tags (optional)

array[String]

Tags of the Console

example: ["tag1", "tag2"]

UpdateControllerRequest

description (optional)

String

Description of the controller

example: This is a test controller

name (optional)

String

Name of the controller

example: TestController

tags (optional)

array[String]

unique labels to identify

example: List ["CC Processing", "US West"]

UpdateDataLabelResponse

data

DataLabelDto

UpdateEndpointResponse

isError (optional)

Boolean

States if an error occurred

example: false

value (optional)

UpdateEndpointResponseValue

UpdateEndpointResponseValue

endpointId (optional)

Long

The API endpoint ID format: int64

example: 1234567890

UpdateMicrosensorRequest

description (optional)

String

Microsensor Description

example: Security API Microsensor

name (optional)

String

Microsensor Name

example: Security API Microsensor

tags (optional)

array[String]

Microsensor Tags

example: Security API

UpdateMicrosensorResponseV3

data (optional)

array[Microsensor]

Contains the response Body

UpdateSiteConfigurationResponse

isError (optional)

Boolean

States if an error occurred

example: false

value (optional)

UpdateSiteConfigurationResponseValue

UpdateSiteConfigurationResponseValue

sitelid (optional)

Long

The Site ID format: int64

example: 12345

UploadFileSuccessResponse

data
Action

UsageStatistics

apiCalls (optional)
Long
format: int64
clientApps (optional)
Long
format: int64
clientCountries (optional)
Long
format: int64
clientUserAgents (optional)
Long
format: int64

VolumeStatistics

endpointsResourceStatTrend (optional)
ResourceStatTrend
endpointsVolumeStatistics (optional)
array[EndpointVolumeStatistics]
hostsResourceStatTrend (optional)
ResourceStatTrend
hostsVolumeStatistics (optional)
array[HostVolumeStatistics]
newEndpointsResourceStatTrend (optional)
ResourceStatTrend
newHostsResourceStatTrend (optional)
ResourceStatTrend
newResourcesResourceStatTrend (optional)
ResourceStatTrend
resourcesResourceStatTrend (optional)
ResourceStatTrend
resourcesVolumeStatistics (optional)
array[ResourceVolumeStatistics]

apiId_endpointId_body

specificationViolationAction (optional)
String
The action taken when an API Specification Violation occurs
Enum:
ALERT_ONLY
BLOCK_REQUEST
BLOCK_USER
BLOCK_IP
IGNORE
DEFAULT
violationActions (optional)
String
Json payload described by ViolationActions Object. This object defines different actions taken when each violation

occurs

api_siteId_body

apiSpecification

byte[]

The API specification document. The supported format is OAS2 or OAS3 (JSON or YAML) format: binary
basePath (optional)

String

Override the spec basePath / server base path with this value

description (optional)

String

A description that will help recognize the API in the dashboard

matchTrailingSlash (optional)

Boolean

When set to false, request with and without slash will be treated as different for same URL

oasFileName (optional)

String

Uploaded OAS file name

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

validateHost (optional)

Boolean

When set to true, verifies that the host name and site name match. Set to false in cases such as CNAME reuse or API management integrations where the host name and site name do not match.

violationActions (optional)

String

Json payload described by ViolationActions Object. This object defines different actions taken when each violation occurs

files_oas_body

actionTypes (optional)

String

Action types in Json format e.g. [{"actionTypeId": 1}, {"actionTypeId": 2}]

file (optional)

byte[]

Upload Swagger file. Swagger2.0, Swagger3.0 formats are supported format: binary

inline_response_200

comment (optional)

String

name (optional)

String

siteId_apiId_body

apiSpecification (optional)

byte[]

The API specification document. The supported format is OAS2 or OAS3 (JSON or YAML) format: binary
basePath (optional)

String

Override the spec basePath / server base path with this value

description (optional)

String

A description that will help recognize the API in the dashboard

matchTrailingSlash (optional)

Boolean

When set to false, request with and without trailing slash will be treated as different for same path

oasFileName (optional)

String

Uploaded OAS file name

specificationViolationAction (optional)

String

The action taken when an API Specification Violation occurs

Enum:

ALERT_ONLY

BLOCK_REQUEST

BLOCK_USER

BLOCK_IP

IGNORE

DEFAULT

validateHost (optional)

Boolean

When set to true, verifies that the host name and site name match. Set to false in cases such as CNAME reuse or API management integrations where the host name and site name do not match.

violationActions (optional)

String

Json payload described by ViolationActions Object. This object defines different actions taken when each violation occurs

Imperva Advanced API Security

This Topic Describes Manual Tagging for API Security.

Version: 1.0.0

BasePath:/tag-manager

The terms in the absence of an applicable signed agreement between you and Imperva

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Resources

- `get /v3/resources/{resourceType}`
- `get /v3/resources/{resourceType}/{resourceId}`
- `get /v3/resources/search`
- `post /v3/resources/{resourceType}/tag`
- `put /v3/resources/{resourceType}/{resourceId}`
- `post /v3/resources/{resourceType}/untag`

Tags

- `post /v3/tags`
- `delete /v3/tags/{tagId}`
- `get /v3/tags`
- `get /v3/tags/{tagId}`
- `put /v3/tags/{tagId}`

Resources

```
get /v3/resources/{resourceType}
```

(`getAllResourcesWithTags`)

Get all resources and their associated tags for a specific resource type

Path parameters

`resourceType` (required)

Path Parameter

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`GetTaggedResourcesResponse`

Example data

Content-Type: application/json

```
{
```

```

"data" : [ {
  "resourceId" : 12345,
  "tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
  }, {
    "name" : "My Tag",
    "id" : 1234567
  } ]
}, {
  "resourceId" : 12345,
  "tags" : [ {
    "name" : "My Tag",
    "id" : 1234567
  }, {
    "name" : "My Tag",
    "id" : 1234567
  } ]
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Successful `GetTaggedResourcesResponse`

500

Error while processing request `ApiFailureResponseV3`

```
get /v3/resources/{resourceType}/{resourceId}
```

`(getResourceWithTags)`

Get all tags for a specific resource Id of a specific resource type

Path parameters

`resourceType` (required)

Path Parameter

`resourceId` (required)

Path Parameter

— format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetTaggedResourcesResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful [GetTaggedResourcesResponse](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
get /v3/resources/search
```

(getResourcesBasedOnTags)
Search resources based one or more tags

Query parameters

tagIds (required)

Query Parameter

— Comma separated list of tag Ids

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ResourceSearchByTagsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "resourceType" : "DISCOVERY_ENDPOINT",
    "resourceIds" : [ 12345, 345221 ]
  }, {
    "resourceType" : "DISCOVERY_ENDPOINT",
    "resourceIds" : [ 12345, 345221 ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

[Successful ResourceSearchByTagsResponse](#)

400

Invalid Request [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
post /v3/resources/{resourceType}/tag
```

(mapResourcesToTag)

Associate one or more resources with one or more tags of a specific resource type

Path parameters

resourceType (required)

Path Parameter

— Type of the Resource

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ResourcesDto](#) (required)

Body Parameter

— Map Resource to Tag

Query parameters

tags (required)

Query Parameter

— Comma separated list of tag IDs

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetTaggedResourcesResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

201

Successful GetTaggedResourcesResponse

400

Failed to map resource to tag ApiFailureResponseV3

500

Error while processing request ApiFailureResponseV3

```
put /v3/resources/{resourceType}/{resourceId}
```

(tagUntagResources)

Tag and/or Untag a specific resource Id of a specific resource type

Path parameters

resourceType (required)

Path Parameter
— Resource Type
resourceId (required)
Path Parameter
— Resource ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body UpdateResourceDto (required)
Body Parameter
— Patch Resource

Query parameters

caid (optional)
Query Parameter
— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetTaggedResourcesResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }
]
```

```
    } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Successful [GetTaggedResourcesResponse](#)

400

Invalid Request [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
post /v3/resources/{resourceType}/untag
```

`(unMapResourcesFromTag)`

Clear tags for one or more resources of a specific resource type

Path parameters

`resourceType` (required)

Path Parameter

— Type of the Resource

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `ResourcesDto` (required)

Body Parameter

— Map Resource to Tag

Query parameters

tags (required)

Query Parameter

— Comma separated list of tag IDs

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

GetTaggedResourcesResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }, {
    "resourceId" : 12345,
    "tags" : [ {
      "name" : "My Tag",
      "id" : 1234567
    }, {
      "name" : "My Tag",
      "id" : 1234567
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

201

Successful GetTaggedResourcesResponse

400

Failed to map resource to tag [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

Tags

```
post /v3/tags
```

(createTag)

Create a tag with the given name and the given info

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CreateTagRequest](#) (required)

Body Parameter

— Create Tag

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetTagsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
```

```

    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
} , {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

201

Successful [GetTagsResponse](#)

400

Failed to validate tag [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
delete /v3/tags/{tagId}
```

(deleteTag)

Delete the tag with given tag id

Path parameters

tagId (required)

Path Parameter

— Id of the Tag format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successfully deleted tag String

400

Failed to validate tag ApiFailureResponseV3

500

Error while processing request ApiFailureResponseV3

```
get /v3/tags
```

(getAllTagsForAccount)

Get all tag info for a given account

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetAllTagsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "tags" : [ {
      "createdAt" : 1710478488,
      "modifiedById" : 1234567,
      "modifiedAt" : 1710478488,
      "name" : "My Tag",
      "additionalInfo" : "Tag detailed Information",
      "id" : 1234567,
      "type" : "USER_DEFINED",
      "lastModifiedUserName" : "John Doe",
      "createdById" : 1234567
    }, {
      "createdAt" : 1710478488,
      "modifiedById" : 1234567,
      "modifiedAt" : 1710478488,
      "name" : "My Tag",
      "additionalInfo" : "Tag detailed Information",
      "id" : 1234567,
      "type" : "USER_DEFINED",
      "lastModifiedUserName" : "John Doe",
      "createdById" : 1234567
    } ]
  }, {
    "tags" : [ {
      "createdAt" : 1710478488,
      "modifiedById" : 1234567,
      "modifiedAt" : 1710478488,
      "name" : "My Tag",
      "additionalInfo" : "Tag detailed Information",
      "id" : 1234567,
      "type" : "USER_DEFINED",
      "lastModifiedUserName" : "John Doe",
      "createdById" : 1234567
    }, {
      "createdAt" : 1710478488,
      "modifiedById" : 1234567,
      "modifiedAt" : 1710478488,
      "name" : "My Tag",
      "additionalInfo" : "Tag detailed Information",
      "id" : 1234567,
      "type" : "USER_DEFINED",
      "lastModifiedUserName" : "John Doe",
      "createdById" : 1234567
    } ]
  }
}
```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Successful [GetAllTagsResponse](#)

400

Failed to validate tag [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
get /v3/tags/{tagId}
```

`(getTagById)`

Get tag info for a given tag id

Path parameters

`tagId` (required)

Path Parameter

— Id of the Tag format: int64

Query parameters

`caid` (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[GetTagsResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
  }, {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Successful [GetTagsResponse](#)

400

Failed to validate tag [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

```
put /v3/tags/{tagId}
```

(updateTag)

Update the tag with the given name and the given info for a given tag id

Path parameters

tagId (required)

Path Parameter

— Id of the Tag format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `UpdateTagRequest` (required)

Body Parameter

— Update Tag

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`GetTagsResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
  }, {
    "createdAt" : 1710478488,
    "modifiedById" : 1234567,
    "modifiedAt" : 1710478488,
    "name" : "My Tag",
  }
]
```

```

    "additionalInfo" : "Tag detailed Information",
    "id" : 1234567,
    "type" : "USER_DEFINED",
    "lastModifiedUserName" : "John Doe",
    "createdById" : 1234567
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

Successfully updated Tag [GetTagsResponse](#)

400

Failed to validate tag [ApiFailureResponseV3](#)

500

Error while processing request [ApiFailureResponseV3](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [ApiFailureResponseV3](#)
 3. [CreateTagRequest](#)
 4. [GetAllTagsResponse](#)
 5. [GetTaggedResourcesResponse](#)
 6. [GetTagsForAccount](#)
 7. [GetTagsResponse](#)
 8. [ResourceSearchByTagsResponse](#)
 9. [ResourcesByType](#)
 10. [ResourcesDto](#)
 11. [Tag](#)
-

-
- 12. TagDetails
 - 13. TaggedResource
 - 14. UpdateResourceDto
 - 15. UpdateTagRequest

APIError

status (optional)
Integer
format: int32
id (optional)
String
code (optional)
String
source (optional)
map[String, Object]
title (optional)
String
detail (optional)
String

ApiFailureResponseV3

errors (optional)
array[APIError]

CreateTagRequest

name (optional)
String
The tag Name
example: My Tag
additionalInfo (optional)
String
Additional Info for the Tag
example: Tag detailed Information

GetAllTagsResponse

data (optional)
array[GetTagsForAccount]
Contains the response Body

GetTaggedResourcesResponse

data (optional)
array[TaggedResource]
Contains the response Body

GetTagsForAccount

Contains the response Body
tags (optional)

array[Tag]
Tags available for account

GetTagsResponse

data (optional)
array[Tag]
Contains the response Body

ResourceSearchByTagsResponse

data (optional)
array[ResourcesByType]
Contains the response Body

ResourcesByType

Contains the response Body
resourceType (optional)
String
Enum:
DISCOVERY_ENDPOINT
resourceIds (optional)
array[Long]
format: int64
example: [12345,345221]

ResourcesDto

resourceIds (optional)
array[Long]
format: int64
example: [12345,345221]

Tag

Contains the response Body
id (optional)
Long
The tag ID format: int64
example: 1234567
name (optional)
String
The tag Name
example: My Tag
additionalInfo (optional)
String
Additional Info for the Tag
example: Tag detailed Information
type (optional)
String
The tag type
Enum:
USER_DEFINED
SYSTEM_DEFINED

example: USER_DEFINED

createdAt (optional)

Long

The tag creation timestamp format: int64

example: 1710478488

createdById (optional)

Long

Account Id of the tag's creator format: int64

example: 1234567

modifiedAt (optional)

Long

The tag modification timestamp format: int64

example: 1710478488

modifiedById (optional)

Long

Account Id of the tag's modifier format: int64

example: 1234567

lastModifiedUserName (optional)

String

The last modified user

example: John Doe

TagDetails

id (optional)

Long

The tag ID format: int64

example: 1234567

name (optional)

String

The tag Name

example: My Tag

TaggedResource

Contains the response Body

resourceId (optional)

Long

format: int64

example: 12345

tags (optional)

array[**TagDetails**]

The tags that are associated with that resource id

UpdateResourceDto

action (optional)

String

Enum:

TAG

UNTAG

tags (optional)

array[**Long**]

format: int64

example: [12345,345221]

UpdateTagRequest

name (optional)

String

The tag Name

example: My Tag

additionalInfo (optional)

String

Additional Info for the Tag

example: Tag detailed Information

Attack Analytics API Overview

Imperva enables you to access your Attack Analytics data using an API.

Predominance

Incident details include information on the predominance of the value among other values in the incident. The **dominance** field indicates how many events in an incident shared a specific value.

Possible values include:

- STRONGLY_DOMINANT - the vast majority (more than 99%) of events in the incident shared a specific value
- DOMINANT- more than 50% of the events in the incident shared a specific value.
- DISTRIBUTED - no specific value was present in more than 50% of the events in the incident.

Time series data

The time series response parameters return the number of blocked or alert events at each time stamp. The data is calculated as follows:

Data is provided according to 10 minute buckets throughout the incident, for buckets with values greater than zero. For example, if you request data spanning 30 minutes and there were events on the 5th and 14th minutes, the response shows 2 values, such as:

```
[{timestamp: '1553420378000', value: 5}, {timestamp: '1553420978000', value: 10}]
```

Buckets with zero events are not shown.

Attack Analytics API Definition

For instructions on using the Attack Analytics API, see the [Attack Analytics API Definition](#).

The definition file presents a full, formatted, and interactive version of the Attack Analytics APIs that you can use to learn about the APIs, or test them using your API ID and key.

Attack Analytics API

Access the Attack Analytics data for your account using the API. For full feature documentation, see [Imperva Attack Analytics](#).

Version: v1
BasePath:/analytics
ISC
<https://opensource.org/licenses/ISC>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AttackAnalytics

- `get /v1/incidents/{incidentId}/stats`
- `get /v1/incidents`
- `get /v1/insights`
- `get /v1/incidents/{incidentId}/sample-events`

AttackAnalytics

```
get /v1/incidents/{incidentId}/stats
```

Retrieve incident details (getIncidentStatsByAccount)
Retrieves full details of a specified incident.

Path parameters

incidentId (required)
Path Parameter
— The incident identifier. format: uuid

Query parameters

caid (required)
Query Parameter
— Account ID. Unique identifier of the account to operate on. format: int64

Return type

IncidentStats

Example data

Content-Type: application/json

```
{
  "attack_geolocations" : "[{key: 'Oregon US', count: 5}, {key: 'Poltavskaya Oblast', count: 10}]",
  "alerted_events_timeseries" : "[{timestamp: '1553420378000', value: 2}, {timestamp: '1553420978000', value: 12}]",
  "attack_class_c" : "[{key: '1.0.0', count: 5}, {key: '2.0.0', count: 10}]",
  "violations_blocked" : "[{key: '1553420378000', count: 5}, {key: '1553420978000', count: 10}]",
  "blocked_events_timeseries" : "[{timestamp: '1553420378000', value: 5}, {timestamp: '1553420978000', value: 10}]",
  "attack_tool_types" : "[{key: 'MALICIOUS_TOOL', count: 5}, {key: 'CLAPP_TYPE_UNKOWN', count: 10}]",
  "attack_tools" : "[{key: 'AddSugarSpiderBot', count: 5}, {key: 'Google bot', count: 10}]",
  "attack_ips" : [
    {
      "value" : 0,
      "key" : {
        "countryCode" : "RU",
        "ip" : "192.168.0.1",
        "reputation" : "['comment-spammers','sql-injection']"
      }
    },
    {
      "value" : 0,
      "key" : {
        "countryCode" : "RU",
        "ip" : "192.168.0.1",
        "reputation" : "['comment-spammers','sql-injection']"
      }
    }
  ],
  "attack_urls" : "[{key: '/admin.php', count: 5}, {key: '/', count: 10}]",
  "events_count" : 520,
  "attacked_hosts" : "[{key: 'acme.com', count: 5}, {key: 'm.acme.com', count: 10}]",
  "waf_origins_of_blocks" : "[{site_id: 123, site_name:'acme.com', violation:'Bad Bots', count: 1},{site_id: 124, site_name:'www.acme.com', violation:'DDOS', count: 4}]",
  "waf_origins_entities" : "[{site_id: 123, site_name:'acme.com', violation:'', count: 1},{site_id: 124, site_name:'www.acme.com', violation:'', count: 4}]",
  "associated_cve" : "['CVE-2020-8417', 'CVE-2017-6090']",
  "attack_agents" : "[{key:'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683 Safari/537.36', 5},{key: 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) AddSugarSpiderBot www.idealobserver.com', 10}]",
  "id" : "ad2c8f40-3e82-11e9-354e-b114829e37eb",
  "violations_alerted" : "[{key: '1553420378000', count: 2}, {key: '1553420978000', count: 15}]",
  "rules_list" : "[{key: '12.1.0', count: 5}, {key: '8.2.0', count: 10}]",
  "waf_origins_of_alerts" : "[{site_id: 123, site_name:'acme.com', violation:'Bad Bots', count: 1},{site_id: 124, site_name:'www.acme.com', violation:'DDOS', count: 4}]"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response [IncidentStats](#)

500

Error while fetching incident [ErrorResponseWrapper](#)

```
get /v1/incidents
```

Retrieve a list of incidents (`getIncidentsByAccount`)

Retrieves Attack Analytics details for an account during a specified time period.

Query parameters

`caid` (required)

Query Parameter

— Account ID. Unique identifier of the account to operate on. format: int64

`from_timestamp` (optional)

Query Parameter

— Earliest time boundary, specified as number of milliseconds since midnight 1970 (UNIX time * 1000). format: int64

`to_timestamp` (optional)

Query Parameter

— Latest time boundary, specified as number of milliseconds since midnight 1970 (UNIX time * 1000). format: int64

Return type

[array\[Incident\]](#)

Example data

Content-Type: application/json

```
[ {
  "severity" : "MINOR",
  "dominant_attacked_host" : {
    "dominance" : "STRONGLY_DOMINANT",
    "value" : "acme.com"
  },
}
```

```

"incident_type" : "REGULAR",
"last_event_time" : 1548073343000,
"dominant_attack_ip" : {
    "ip" : "192.168.0.1",
    "reputation" : "[comment-spammer]",
    "dominance" : "STRONGLY_DOMINANT"
},
"severity_explanation" : "Highly targeted",
"first_event_time" : 1548073343000,
"how_common" : "INDUSTRY",
"only_custom_rule_based" : true,
"dominant_attack_country" : {
    "country" : "Russia",
    "countryCode" : "RU",
    "dominance" : "STRONGLY_DOMINANT"
},
"dominant_attack_tool" : {
    "name" : "Google bot",
    "dominance" : "STRONGLY_DOMINANT",
    "type" : "Suspicious"
},
"ddos_data" : {
    "max_BPS_passed" : 0.8008281904610115,
    "network_traffic_data_list" : [ {
        "blocked" : 10.0,
        "name" : "SYN",
        "passed" : 30.0
    }, {
        "blocked" : 10.0,
        "name" : "SYN",
        "passed" : 30.0
    } ],
    "max_BPS_blocked" : 6.027456183070403
},
"events_count" : 520,
"secondary_sentence" : "On host \"acme.com\" targeting an empty URL resource extension",
"false_positive" : true,
"dominant_attackViolation" : "Backdoor",
"main_sentence" : "Bad Bots attack from United States using hacking_tool",
"events_blocked_percent" : 20,
"id" : "ad2c8f40-3e82-11e9-354e-b114829e37eb"
},
{
    "severity" : "MINOR",
    "dominant_attacked_host" : {
        "dominance" : "STRONGLY_DOMINANT",
        "value" : "acme.com"
    },
    "incident_type" : "REGULAR",
    "last_event_time" : 1548073343000,
    "dominant_attack_ip" : {
        "ip" : "192.168.0.1",
        "reputation" : "[comment-spammer]",
        "dominance" : "STRONGLY_DOMINANT"
    },
    "severity_explanation" : "Highly targeted",
    "first_event_time" : 1548073343000,
    "how_common" : "INDUSTRY",
    "only_custom_rule_based" : true,
}

```

```

"dominant_attack_country" : {
    "country" : "Russia",
    "countryCode" : "RU",
    "dominance" : "STRONGLY_DOMINANT"
},
"dominant_attack_tool" : {
    "name" : "Google bot",
    "dominance" : "STRONGLY_DOMINANT",
    "type" : "Suspicious"
},
"ddos_data" : {
    "max_BPS_passed" : 0.8008281904610115,
    "network_traffic_data_list" : [ {
        "blocked" : 10.0,
        "name" : "SYN",
        "passed" : 30.0
    }, {
        "blocked" : 10.0,
        "name" : "SYN",
        "passed" : 30.0
    } ],
    "max_BPS_blocked" : 6.027456183070403
},
"events_count" : 520,
"secondary_sentence" : "On host \"acme.com\" targeting an empty URL resource extension",
    "false_positive" : true,
    "dominant_attackViolation" : "Backdoor",
    "main_sentence" : "Bad Bots attack from United States using hacking_tool",
    "events_blocked_percent" : 20,
    "id" : "ad2c8f40-3e82-11e9-354e-b114829e37eb"
} ]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

```
get /v1/insights
```

Retrieve insights (getInsightsPerAccount)

Retrieves the list of insights for your account (recommended actions to take based on attacks that have targeted your sites and applications).

Query parameters

caid (required)

Query Parameter

— Unique account id format: int64

Return type

array[[InsightsDataApi](#)]

Example data

Content-Type: application/json

```
[ {
  "insights" : [ {
    "secondarySentence" : "secondarySentence",
    "recommendation" : "recommendation",
    "type" : "type",
    "mainSentence" : "mainSentence",
    "additionalDetails" : {
      "key" : { }
    },
    "moreInfo" : "moreInfo",
    "vulnerableSites" : [ {
      "insightDetails" : {
        "snoozedUntil" : 1602968400000,
        "attacked_site_info" : {
          "site_name" : "example.com",
          "site_id" : 12345678
        },
        "status" : "SNOOZE"
      },
      "type" : "type",
      "additionalDetails" : {
        "key" : { }
      }
    },
    {
      "insightDetails" : {
        "snoozedUntil" : 1602968400000,
        "attacked_site_info" : {
          "site_name" : "example.com",
          "site_id" : 12345678
        },
        "status" : "SNOOZE"
      },
      "type" : "type",
      "additionalDetails" : {
        "key" : { }
      }
    }
  ],
  "timestamp" : "timestamp"
}, {
  "secondarySentence" : "secondarySentence",
  "recommendation" : "recommendation",
  "type" : "type",
}
```

```

"mainSentence" : "mainSentence",
"additionalDetails" : {
    "key" : { }
},
"moreInfo" : "moreInfo",
"vulnerableSites" : [ {
    "insightDetails" : {
        "snoozedUntil" : 1602968400000,
        "attacked_site_info" : {
            "site_name" : "example.com",
            "site_id" : 12345678
        },
        "status" : "SNOOZE"
    },
    "type" : "type",
    "additionalDetails" : {
        "key" : { }
    }
}, {
    "insightDetails" : {
        "snoozedUntil" : 1602968400000,
        "attacked_site_info" : {
            "site_name" : "example.com",
            "site_id" : 12345678
        },
        "status" : "SNOOZE"
    },
    "type" : "type",
    "additionalDetails" : {
        "key" : { }
    }
}],
"timestamp" : "timestamp"
} ]
},
{
    "insights" : [ {
        "secondarySentence" : "secondarySentence",
        "recommendation" : "recommendation",
        "type" : "type",
        "mainSentence" : "mainSentence",
        "additionalDetails" : {
            "key" : { }
        },
        "moreInfo" : "moreInfo",
        "vulnerableSites" : [ {
            "insightDetails" : {
                "snoozedUntil" : 1602968400000,
                "attacked_site_info" : {
                    "site_name" : "example.com",
                    "site_id" : 12345678
                },
                "status" : "SNOOZE"
            },
            "type" : "type",
            "additionalDetails" : {
                "key" : { }
            }
        }, {
            "insightDetails" : {

```

```

    "snoozedUntil" : 1602968400000,
    "attacked_site_info" : {
        "site_name" : "example.com",
        "site_id" : 12345678
    },
    "status" : "SNOOZE"
},
"type" : "type",
"additionalDetails" : {
    "key" : { }
}
} ],
"timestamp" : "timestamp"
}, {
    "secondarySentence" : "secondarySentence",
    "recommendation" : "recommendation",
    "type" : "type",
    "mainSentence" : "mainSentence",
    "additionalDetails" : {
        "key" : { }
    },
    "moreInfo" : "moreInfo",
    "vulnerableSites" : [ {
        "insightDetails" : {
            "snoozedUntil" : 1602968400000,
            "attacked_site_info" : {
                "site_name" : "example.com",
                "site_id" : 12345678
            },
            "status" : "SNOOZE"
        },
        "type" : "type",
        "additionalDetails" : {
            "key" : { }
        }
    }, {
        "insightDetails" : {
            "snoozedUntil" : 1602968400000,
            "attacked_site_info" : {
                "site_name" : "example.com",
                "site_id" : 12345678
            },
            "status" : "SNOOZE"
        },
        "type" : "type",
        "additionalDetails" : {
            "key" : { }
        }
    } ],
    "timestamp" : "timestamp"
} ]
}
]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

500

Error while fetching insights [ErrorResponseWrapper](#)

```
get /v1/incidents/{incidentId}/sample-events
```

Retrieve event sample (getSampleEventsByIncident)
Retrieves a sampling of events in a specified incident.

Path parameters

incidentId (required)

Path Parameter

— The incident identifier format: uuid

Query parameters

caid (required)

Query Parameter

— Unique identifier of the account to operate on format: int64

Return type

Event

Example data

Content-Type: application/json

```
{
  "creation_time" : "1561727125000",
  "headers" : "[{key: 'Access-Control-Allow-Origin', value:'*', key: 'cache-control', value: 'no-cache'}]",
  "response_code" : "200",
  "method" : "GET",
  "violations" : "[{'ruleDescription': 'Bad Bots','action': 'RULE_ACTION_BLOCK', 'violationContext': 'Path'}]",
  "client_application" : "BLEXBot Crawler",
  "is_event_blocked" : true,
  "session_id" : "S5jb22Z4z8XE7C84lZe",
  "reporter" : "Cloud WAF",
  "main_client_ip" : "10.0.0.1",
```

```

"cookies" : "[{"name:'acme_auth', value:'1234', domain:'acme.com', expiration:'2019-06-26T11:16:59.000Z', path:'/'},]]",
"country_code" : "US",
"referrer" : "/",
"event_id" : 123,
"destination_ip" : "10.0.0.1",
"declared_client_application" : "Firefox",
"host" : "www.acme.com",
"query_string" : "id=1&base=true",
"url_path" : "/admin/login"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response Event

500

Error while fetching sample events [ErrorResponseWrapper](#)

Models

Methods

Table of Contents

1. AttackedSiteInfo
 2. Cookie
 3. CountryDominance
 4. DdosData
 5. ErrorResponseWrapper
 6. Event
 7. GeneralInsightData
 8. Incident
 9. IncidentStats
 10. Insight
 11. InsightSummaryVOApi
 12. InsightsDataApi
-

-
- 13. IpDominance
 - 14. IpObject
 - 15. KeyValue
 - 16. KeyValueIpObjectLong
 - 17. KeyValueLongInteger
 - 18. KeyValueStringLong
 - 19. KeyValueStringString
 - 20. NetworkTrafficData
 - 21. ShinyObject
 - 22. Site
 - 23. SiteViolation
 - 24. ToolDominance
 - 25. Violation

AttackedSiteInfo

site_id (optional)
Long
site id format: int64
example: 12345678
site_name (optional)
String
site name
example: example.com

Cookie

name (optional)
String
Cookie name
example: auth_cookie
value (optional)
String
Content of the cookie
example: anything stored in the cookie
domain (optional)
String
Cookie source domain
example: acme.com
expiration (optional)
String
When the cookie is going to expire
example: 2019-06-26T11:16:59.000Z
path (optional)
String
Path under which this cookie is valid
example: /subfolder
persistent (optional)
Boolean
True if a cookie is persistent
example: true
secure (optional)
Boolean

True id cookie is secure

example: true

traceability (optional)

String

Tracability of a cookie

example: aa

CountryDominance

dominance (optional)

String

How dominant is the value among other values

Enum:

STRONGLY_DOMINANT

DOMINANT

DISTRIBUTED

BLANK

example: STRONGLY_DOMINANT

country (optional)

String

Country name

example: Russia

countryCode (optional)

String

Country two character code

example: RU

DdosData

max_BPS_passed (optional)

Double

Peak clean traffic values during the DDoS attack format: double

max_BPS_blocked (optional)

Double

Peak blocked traffic values during the DDoS attack- format: double

network_traffic_data_list (optional)

array[NetworkTrafficData]

Peak passed and blocked traffic values by protocol during the DDoS attack (e.g. TCP, UDP, SYN).

ErrorResponseWrapper

Object that describes a non valid response

id (optional)

String

Unique id to identify the error in the logs

example: Xu09cHAb

code (optional)

String

HTTP response code

Enum:

OK

CREATED

ACCEPTED

NO_CONTENT

RESET_CONTENT

PARTIAL_CONTENT

```

MOVED_PERMANENTLY
FOUND
SEE_OTHER
NOT_MODIFIED
USE_PROXY
TEMPORARY_REDIRECT
BAD_REQUEST
UNAUTHORIZED
PAYMENT_REQUIRED
FORBIDDEN
NOT_FOUND
METHOD_NOT_ALLOWED
NOT_ACCEPTABLE
PROXY_AUTHENTICATION_REQUIRED
REQUEST_TIMEOUT
CONFLICT
GONE
LENGTH_REQUIRED
PRECONDITION_FAILED
REQUEST_ENTITY_TOO_LARGE
REQUEST_URI_TOO_LONG
UNSUPPORTED_MEDIA_TYPE
REQUESTED_RANGE_NOT_SATISFIABLE
EXPECTATION_FAILED
PRECONDITION_REQUIRED
TOO_MANY_REQUESTS
REQUEST_HEADER_FIELDS_TOO_LARGE
INTERNAL_SERVER_ERROR
NOT_IMPLEMENTED
BAD_GATEWAY
SERVICE_UNAVAILABLE
GATEWAY_TIMEOUT
HTTP_VERSION_NOT_SUPPORTED
NETWORK_AUTHENTICATION_REQUIRED
example: 500
message (optional)
String
Error description
example: Error fetching incident: ad2c8f40-3e82-11e9-354e-b114829e37eb

```

Event

Single event that participated in the attack

event_id (optional)

Long
Id of the event format: int64
example: 123

method (optional)

String
HTTP method that this request was sent with
example: GET

host (optional)

String
The host that this request was sent to
example: www.acme.com

query_string (optional)

String
Query string arguments that were sent with this request

example: id=1&base=true	
url_path (optional)	
String	Path that this request accessed
example: /admin/login	
response_code (optional)	
String	HTTP response code of this request
example: 200	
session_id (optional)	
String	Id of request session
example: S5jb22Z4z8XE7C84lZe	
main_client_ip (optional)	
String	IP address that was identified as request source
example: 10.0.0.1	
country_code (optional)	
array[String]	Two digit country code that this request was sent from
example: US	
client_application (optional)	
String	Application that was identified by Imperva as the sender
example: BLEXBot Crawler	
declared_client_application (optional)	
String	Application that was declared as the sender
example: Firefox	
destination_ip (optional)	
String	IP address that event was sent to
example: 10.0.0.1	
referrer (optional)	
String	The address of the webpage (i.e. the URI or IRI) that linked to the resource being requested
example: /	
is_event_blocked (optional)	
Boolean	Whether or not this event was blocked by Imperva WAF
example: true	
violations (optional)	
array[Violation]	The violations that this request was associated with
example: [{}ruleDescription': 'Bad Bots','action': 'RULE_ACTION_BLOCK','violationContext': 'Path']	
headers (optional)	
array[KeyValueStringString]	List of http headers in this request
example: [{}key: 'Access-Control-Allow-Origin', value:'*', key: 'cache-control', value: 'no-cache']	
cookies (optional)	
array[Cookie]	Cookies passed in the request
example: [{}name:'acme_auth', value:'1234', domain:'acme.com', expiration:'2019-06-26T11:16:59.000Z', path:']/,}]	
reporter (optional)	
String	Imperva WAF system that reported this request. Can be either 'Cloud WAF' or 'On-Premise WAF'
example: Cloud WAF	
creation_time (optional)	
String	

Time when this event occurred, specified as number of milliseconds since midnight 1970 (UNIX time * 1000)
example: 1561727125000

GeneralInsightData

attacked_site_info (optional)

AttackedSiteInfo

status (optional)

String

insight status

example: SNOOZE

snoozedUntil (optional)

Long

Snooze expiration time, specified as number of milliseconds since midnight 1970 (UNIX time * 1000). 0 means that the insight is active format: int64

example: 1602968400000

Incident

Single attack analytics incident

id (optional)

String

Unique incident identifier

example: ad2c8f40-3e82-11e9-354e-b114829e37eb

main_sentence (optional)

String

Short description of the attack

example: Bad Bots attack from United States using hacking_tool

secondary_sentence (optional)

String

Secondary sentence with more details

example: On host "acme.com" targeting an empty URL resource extension

false_positive (optional)

Boolean

Is incident false positive or not

example: true

events_count (optional)

Long

The number of HTTP events that participated in the attack format: int64

example: 520

events_blocked_percent (optional)

Long

Percentage of http events that were blocked by Imperva format: int64

example: 20

first_event_time (optional)

Long

Timestamp (in milliseconds) of first event in the attack, specified as number of milliseconds since midnight 1970 (UNIX time * 1000) format: int64

example: 1548073343000

last_event_time (optional)

Long

Timestamp (in milliseconds) of last event in the attack, specified as number of milliseconds since midnight 1970 (UNIX time * 1000) format: int64

example: 1548073343000

severity (optional)

String

Attack severity as set by the system. Possible values: CRITICAL, MAJOR, MINOR, CUSTOM

example: MINOR
 severity_explanation (optional)
String
 Explanation on why attack receive its severity
 example: Highly targeted
 dominant_attack_country (optional)
CountryDominance
 dominant_attack_ip (optional)
IpDominance
 dominant_attacked_host (optional)
ShinyObject
 dominant_attack_tool (optional)
ToolDominance
 dominant_attack_violation (optional)
String
 Violation in more than 50% of attacks
 example: Backdoor
 only_custom_rule_based (optional)
Boolean
 True if all events of the incident were created due to user defined rules
 example: true
 how_common (optional)
String
 Describes if this incident was spotted on other Imperva customers
 example: INDUSTRY
 incident_type (optional)
String
 The type of the incident - regular or DDoS
 Enum:
 REGULAR
 DDOS
 ddos_data (optional)
DdosData

IncidentStats

id (optional)
String
 Unique incident identifier
 example: ad2c8f40-3e82-11e9-354e-b114829e37eb
 events_count (optional)
Long
 Number of http events participated in the attack format: int64
 example: 520
 blocked_events_timeseries (optional)
array[KeyValueLongInteger]
 Timeseries of blocked event counts
 example: [{timestamp: '1553420378000', value: 5}, {timestamp: '1553420978000', value: 10}]
 alerted_events_timeseries (optional)
array[KeyValueLongInteger]
 Timeseries of alerted event counts
 example: [{timestamp: '1553420378000', value: 2}, {timestamp: '1553420978000', value: 12}]
 attack_ips (optional)
array[KeyValueObjectLong]
 List of IP addresses that participated in the attack
 attack_agents (optional)
array[KeyValueStringLong]
 List of user-agents that participated in the attack

example: [{key:'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683 Safari/537.36', 5},{key: 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) AddSugarSpiderBot www.idealobserver.com', 10}]
attack_tools (optional)
array[KeyValueStringLong]
List of tools that were used in the attack
example: [{key: 'AddSugarSpiderBot', count: 5}, {key: 'Google bot', count: 10}]
attack_tool_types (optional)
array[KeyValueStringLong]
List of tool types that were used in the attack
example: [{key: 'MALICIOUS_TOOL', count: 5}, {key: 'CLAPP_TYPE_UNKNOWN', count: 10}]
violations_blocked (optional)
array[KeyValueStringLong]
A list of blocked violations that were identified in the incident
example: [{key: '1553420378000', count: 5}, {key: '1553420978000', count: 10}]
violations_alerted (optional)
array[KeyValueStringLong]
A list of alerted violations that were identified in the incident
example: [{key: '1553420378000', count: 2}, {key: '1553420978000', count: 15}]
attack_urls (optional)
array[KeyValueStringLong]
List of URLs that were attacked during this incident
example: [{key: '/admin.php', count: 5}, {key: '/', count: 10}]
attacked_hosts (optional)
array[KeyValueStringLong]
List of hosts that were attacked during this incident
example: [{key: 'acme.com', count: 5}, {key: 'm.acme.com', count: 10}]
attack_class_c (optional)
array[KeyValueStringLong]
List of Class C subnets that participated in the attack
example: [{key: '1.0.0', count: 5}, {key: '2.0.0', count: 10}]
attack_geolocations (optional)
array[KeyValueStringLong]
List of geographical areas that events came from
example: [{key: 'Oregon US', count: 5}, {key: 'Poltavska Oblast', count: 10}]
waf_origins_of_alerts (optional)
array[SiteViolation]
List of WAF servers that alerted events
example: [{site_id: 123, site_name:'acme.com', violation:'Bad Bots', count: 1},{site_id: 124, site_name:'www.acme.com', violation:'DDOS', count: 4}]
waf_origins_of_blocks (optional)
array[SiteViolation]
List of WAF servers that blocked events
example: [{site_id: 123, site_name:'acme.com', violation:'Bad Bots', count: 1},{site_id: 124, site_name:'www.acme.com', violation:'DDOS', count: 4}]
waf_origins_entities (optional)
array[Site]
List of WAF servers that events came through
example: [{site_id: 123, site_name:'acme.com', violation:"", count: 1},{site_id: 124, site_name:'www.acme.com', violation:"", count: 4}]
rules_list (optional)
array[KeyValueStringLong]
List of rules that triggered this incident
example: [{key: '12.1.0', count: 5}, {key: '8.2.0', count: 10}]
associated_cve (optional)
array[String]
List of known CVEs associated with this incident
example: ['CVE-2020-8417', 'CVE-2017-6090']

Insight

type
String
 insightDetails
GeneralInsightData
 additionalDetails
map[String, Object]

InsightSummaryVOApi

type
String
 mainSentence
String
 secondarySentence
String
 moreInfo
String
 recommendation
String
 vulnerableSites
array[Insight]
 timestamp
String
 additionalDetails
map[String, Object]

InsightsDataApi

insights
array[InsightSummaryVOApi]

IpDominance

dominance (optional)
String
 How dominant is the value among other values
 Enum:
 STRONGLY_DOMINANT
 DOMINANT
 DISTRIBUTED
 BLANK
 example: STRONGLY_DOMINANT
 ip (optional)
String
 IP address
 example: 192.168.0.1
 reputation (optional)
array[String]
 IP address
 example: ['comment-spammer']

IpObject

ip (optional)

String

IP address

example: 192.168.0.1

reputation (optional)

array[String]

List of IP address metadata tags that would identify its malicious usage

example: ['comment-spammers', 'sql-injection']

countryCode (optional)

String

2 character code of IPs country

example: RU

KeyValue

key

Object

value

Object

KeyValueIpObjectLong

key

IpObject

value

Long

format: int64

KeyValueLongInteger

key

Long

format: int64

value

Integer

format: int32

KeyValueStringLong

key

String

value

Long

format: int64

KeyValueStringString

key

String

value

String

NetworkTrafficData

name (optional)

String

protocol name

example: SYN

passed (optional)

Double

Peak passed traffic values for protocol during the DDoS attack format: double

example: 30.0

blocked (optional)

Double

Peak blocked traffic values for protocol during the DDoS attack format: double

example: 10.0

ShinyObject

dominance (optional)

String

How dominant is the value among other values

Enum:

STRONGLY_DOMINANT

DOMINANT

DISTRIBUTED

BLANK

example: STRONGLY_DOMINANT

value (optional)

String

Value in key/value pair

example: acme.com

Site

siteld

Long

format: int64

siteName

String

count

Integer

format: int32

SiteViolation

siteld

Long

format: int64

siteName

String

count

Integer

format: int32

violation

String

ToolDominance

dominance (optional)

String

How dominant is the value among other values

Enum:

STRONGLY_DOMINANT

DOMINANT

DISTRIBUTED

BLANK

example: STRONGLY_DOMINANT

name (optional)

String

Tool's name

example: Google bot

type (optional)

String

Tool's type

example: Suspicious

Violation

rule_description (optional)

String

Violation that this rule relates to

example: Bad Bots

action (optional)

String

The result of this rule action

example: RULE_ACTION_BLOCK

violation_context (optional)

String

Context on which the violation was applied

example: Path

Imperva Client-Side Protection API

This is an API for Imperva Client-Side Protection. Gain visibility into the JavaScript services making requests to your application along with their risk factors. Use these APIs to pull data and configure which services should have access to your application. For full feature documentation, see [Client-Side Protection](#)

Version: 1.0.0

BasePath:/csp-api

The terms in the absence of an applicable signed agreement between you and Imperva

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Domains

- `get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/authorization`
- `get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}`
- `get /v1/sites/{siteId}/paths/{pathId}/domains`
- `put /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/authorization`

Email

- `post /v1/sites/{siteId}/settings/emails/add`
- `get /v1/sites/{siteId}/settings/emails`
- `post /v1/sites/{siteId}/settings/emails/delete`

Notes

- `post /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes`
- `delete /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes`
- `get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes`

PreApprovedDomainsAndScripts

- `post /v1/sites/{siteId}/preapprovedlist`
- `post /v1/sites/{siteId}/preapproved-scripts`
- `delete /v1/sites/{siteId}/preapprovedlist/{preApprovedDomainId}`
- `delete /v1/sites/{siteId}/preapproved-scripts/{preApprovedScriptId}`
- `get /v1/sites/{siteId}/preapprovedlist/{preApprovedDomainId}`
- `get /v1/sites/{siteId}/preapprovedlist`
- `get /v1/sites/{siteId}/preapproved-scripts`

Scripts

- `post /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes`
- `post /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes`
- `delete /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes`
- `delete /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes`
- `post /v1/sites/{siteId}/script-ai`
- `get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/authorization`
- `post /v1/script`
- `get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/call-chain`
- `get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}`
- `get /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes`
- `get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes`

- `get /v1/sites/{siteId}/paths/{pathId}/scripts`
- `put /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/authorization`

Websites

- `post /v1/sites/{siteId}/paths`
- `post /v1/sites/{siteId}/change-site-type`
- `delete /v1/sites/{siteId}/paths`
- `get /v1/sites/{siteId}/discovery`
- `get /v1/sites/{siteId}/paths/{pathId}/enforce/status`
- `get /v1/sites/{siteId}/paths/{pathId}/enforce-header`
- `get /v1/sites/{siteId}/paths/{pathId}/mode`
- `get /v1/sites/{siteId}/tracking-ids`
- `get /v1/sites/{siteId}/paths/{pathId}/monitor/status`
- `get /v1/sites/{siteId}`
- `get /v1/sites/{siteId}/paths`
- `get /v1/sites/{siteId}/domain_reputation`
- `get /v1/sites/{siteId}/settings`
- `get /v1/sites`
- `get /v1/sites/{siteId}/paths/{pathId}/unsafe-directives`
- `put /v1/sites/{siteId}/discovery`
- `post /v1/sites/{siteId}/paths/{pathId}/mode`
- `put /v1/sites/{siteId}`
- `post /v1/sites/{siteId}/paths/{pathId}/unsafe-directives`

Domains

```
get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/authorization
```

Retrieve authorization details of a discovered domain for specific path (getDomainAuthorizationForPath)

Retrieves authorization details of the domain including whether the domain is blocked or authorized, and reviewed or unreviewed, and notes.

When the website is in "enforce" mode, all requests from the website to blocked domains are blocked.

By default, all newly discovered domains are authorized if the website is in "monitor" mode, and blocked if the website is in "enforce" mode. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`sitId` (required)

Path Parameter

— The numeric identifier of the site format: int64

`pathId` (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

AuthorizationStatus

Example data

Content-Type: application/json

```
{
  "note" : "note",
  "blocked" : true,
  "author" : "Account APIs (admin@imperva.com)",
  "reviewedAt" : 1629260520080,
  "reviewed" : true,
  "lastNoteAt" : 1629260520080,
  "forceChange" : false
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK AuthorizationStatus](#)

```
get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}
```

Retrieve information about specific domain for a specific path (getDomainForPath)

Get full information about the domain for a specific path and its status. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation

Query parameters

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Domain

Example data

Content-Type: application/json

```
{
  "resourceTypes" : [ "ALL", "ALL" ],
  "partOfProfile" : true,
  "notes" : [ {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  }, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  } ],
  "sources" : 119,
  "domainInfo" : {
    "registrationTime" : {
      "type" : "ABSOLUTE",
      "timestamp" : 1629260520080
    },
    "orgOwner" : "Company, Inc",
    "domainCategory" : "Website analytics",
    "sslCertificateInfo" : {
      "organization" : "Organization, Inc",
      "type" : "DOMAIN_VALIDATION"
    },
    "registrar" : "Company, Inc",
    "baseDomain" : "domain.com",
    "companyName" : "Company Inc."
  }
}
```

```

    "countries" : [ "USA", "Canada" ],
    "domainCategorySemrush" : "domainCategorySemrush",
    "additionalInsights" : [ "NONE", "NONE" ],
    "dynamicDnsBased" : true,
    "domainQuality" : {
        "scoreFromHeuristics" : 1.4658129805029452,
        "scoreOverride" : "SUSPICIOUS",
        "score" : 0.8008281904610115,
        "scoreFromMl" : 6.027456183070403
    }
},
"isDynamicallyInjected" : true,
"frequent" : true,
"domainRisk" : "Low",
"domainReports" : [ {
    "referrer" : "https://malicious.domain.com",
    "documentUri" : "https://domain.com/document",
    "scriptSample" : "gtag('event', 'purchase', \n    {\n        'event': 'purchase',\n        'category': 'ecommerce',\n        'label': 'product',\n        'value': 100,\n        'list': [\n            {name: 'product', value: 'Product A'},\n            {name: 'brand', value: 'Brand X'}\n        ]\n    })",
    "sourceType" : "SCRIPT",
    "clientApplication" : "Chrome",
    "blockedUri" : "https://malicious.domain.com",
    "lineNumber" : 101,
    "sourceFile" : "https://domain.com/example.js",
    "statusCode" : 200
}, {
    "referrer" : "https://malicious.domain.com",
    "documentUri" : "https://domain.com/document",
    "scriptSample" : "gtag('event', 'purchase', \n    {\n        'event': 'purchase',\n        'category': 'ecommerce',\n        'label': 'product',\n        'value': 100,\n        'list': [\n            {name: 'product', value: 'Product A'},\n            {name: 'brand', value: 'Brand X'}\n        ]\n    })",
    "sourceType" : "SCRIPT",
    "clientApplication" : "Chrome",
    "blockedUri" : "https://malicious.domain.com",
    "lineNumber" : 101,
    "sourceFile" : "https://domain.com/example.js",
    "statusCode" : 200
} ],
"countryStats" : { "US": 2 },
"discoveredAt" : 1620864000001,
"obfuscationReport" : {
    "reports" : [ {
        "codehash" : "codehash",
        "failed" : true,
        "uri" : "uri",
        "obfuscated" : true,
        "script" : "script"
    }, {
        "codehash" : "codehash",
        "failed" : true,
        "uri" : "uri",
        "obfuscated" : true,
        "script" : "script"
    } ],
    "domain" : "domain",
    "analyzed" : 7,
    "siteId" : 5,
    "failed" : 9,
    "obfuscated" : 5,
    "totalUrls" : 2
},
"significance" : 1,

```

```

    "instantBlockEnabled" : true,
    "dynamicallyInjected" : true,
    "lastSeenMs" : 1620864000001,
    "domain" : "domain.com",
    "ipssSample" : "1.1.1.1",
    "timeBucket" : 1620864000001,
    "browserStats" : {"Chrome": 120},
    "id" : "d21kZWx5LXVzZWQuZG9tYWluLmNvbQ",
    "domainPopularity" : "Rarely used",
    "status" : {
        "blocked" : true,
        "reviewedAt" : 1629260520080,
        "reviewed" : true,
        "preapproved" : true
    }
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK Domain

```
get /v1/sites/{siteId}/paths/{pathId}/domains
```

Retrieve list of all recently-discovered domains for a path (getDomainsForPath)

Every domain accessed from the site is recorded in this list. Client-Side Protection gathers all available information the domain to help with analysis. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Query parameters

significant (optional)

Query Parameter

— Show only significant domains. If the service is part of the profile and/or frequently requested. The two values are 1 or 0. 1 = significant. 0 = not significant.

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[Domain](#)]

Example data

Content-Type: application/json

```
[ {
  "resourceTypes" : [ "ALL", "ALL" ],
  "partOfProfile" : true,
  "notes" : [ {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  }, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  } ],
  "sources" : 119,
  "domainInfo" : {
    "registrationTime" : {
      "type" : "ABSOLUTE",
      "timestamp" : 1629260520080
    },
    "orgOwner" : "Company, Inc",
    "domainCategory" : "Website analytics",
    "sslCertificateInfo" : {
      "organization" : "Organization, Inc",
      "type" : "DOMAIN_VALIDATION"
    },
    "registrar" : "Company, Inc",
    "baseDomain" : "domain.com",
    "companyName" : "Company Inc.",
    "countries" : [ "USA", "Canada" ],
    "domainCategorySemrush" : "domainCategorySemrush",
    "additionalInsights" : [ "NONE", "NONE" ],
    "dynamicDnsBased" : true,
    "domainQuality" : {
      "scoreFromHeuristics" : 1.4658129805029452,
      "scoreOverride" : "SUSPICIOUS",
      "score" : 0.8008281904610115,
      "scoreFromMl" : 6.027456183070403
    }
  },
  "isDynamicallyInjected" : true,
  "frequent" : true,
  "domainRisk" : "Low",
  "domainReports" : [ {
    "referrer" : "https://malicious.domain.com",
  }
]
```

```

"documentUri" : "https://domain.com/document",
"scriptSample" : "gtag('event', 'purchase',\n    {\n        \"sourceType\" : \"SCRIPT\","
"clientApplication" : "Chrome",
"blockedUri" : "https://malicious.domain.com",
"lineNumber" : 101,
"sourceFile" : "https://domain.com/example.js",
"statusCode" : 200
}, {
"referrer" : "https://malicious.domain.com",
"documentUri" : "https://domain.com/document",
"scriptSample" : "gtag('event', 'purchase',\n    {\n        \"sourceType\" : \"SCRIPT\","
"clientApplication" : "Chrome",
"blockedUri" : "https://malicious.domain.com",
"lineNumber" : 101,
"sourceFile" : "https://domain.com/example.js",
"statusCode" : 200
} ],
"countryStats" : "US": 2,
"discoveredAt" : 1620864000001,
"obfuscationReport" : {
"reports" : [ {
"codehash" : "codehash",
"failed" : true,
"uri" : "uri",
"obfuscated" : true,
"script" : "script"
}, {
"codehash" : "codehash",
"failed" : true,
"uri" : "uri",
"obfuscated" : true,
"script" : "script"
} ],
"domain" : "domain",
"analyzed" : 7,
"siteId" : 5,
"failed" : 9,
"obfuscated" : 5,
"totalUrls" : 2
},
"significance" : 1,
"instantBlockEnabled" : true,
"dynamicallyInjected" : true,
"lastSeenMs" : 1620864000001,
"domain" : "domain.com",
"ipsSample" : "1.1.1.1",
"timeBucket" : 1620864000001,
"browserStats" : {"Chrome": 120},
"id" : "d21kZWx5LXVzzWQuZG9tYWluLmNvbQ",
"domainPopularity" : "Rarely used",
"status" : {
"blocked" : true,
"reviewedAt" : 1629260520080,
"reviewed" : true,
"preapproved" : true
}
}, {

```

```

"resourceTypes" : [ "ALL", "ALL" ],
"partOfProfile" : true,
"notes" : [ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ],
"sources" : 119,
"domainInfo" : {
  "registrationTime" : {
    "type" : "ABSOLUTE",
    "timestamp" : 1629260520080
  },
  "orgOwner" : "Company, Inc",
  "domainCategory" : "Website analytics",
  "sslCertificateInfo" : {
    "organization" : "Organization, Inc",
    "type" : "DOMAIN_VALIDATION"
  },
  "registrar" : "Company, Inc",
  "baseDomain" : "domain.com",
  "companyName" : "Company Inc.",
  "countries" : [ "USA", "Canada" ],
  "domainCategorySemrush" : "domainCategorySemrush",
  "additionalInsights" : [ "NONE", "NONE" ],
  "dynamicDnsBased" : true,
  "domainQuality" : {
    "scoreFromHeuristics" : 1.4658129805029452,
    "scoreOverride" : "SUSPICIOUS",
    "score" : 0.8008281904610115,
    "scoreFromMl" : 6.027456183070403
  }
},
"isDynamicallyInjected" : true,
"frequent" : true,
"domainRisk" : "Low",
"domainReports" : [ {
  "referrer" : "https://malicious.domain.com",
  "documentUri" : "https://domain.com/document",
  "scriptSample" : "gtag('event', 'purchase', \\n  {\\n",
  "sourceType" : "SCRIPT",
  "clientApplication" : "Chrome",
  "blockedUri" : "https://malicious.domain.com",
  "lineNumber" : 101,
  "sourceFile" : "https://domain.com/example.js",
  "statusCode" : 200
}, {
  "referrer" : "https://malicious.domain.com",
  "documentUri" : "https://domain.com/document",
  "scriptSample" : "gtag('event', 'purchase', \\n  {\\n",
  "sourceType" : "SCRIPT",
  "clientApplication" : "Chrome",
  "blockedUri" : "https://malicious.domain.com",
  "lineNumber" : 101,
  "sourceFile" : "https://domain.com/example.js",
}
]

```

```

    "statusCode" : 200
} ],
"countryStats" : " "US": 2",
"discoveredAt" : 1620864000001,
"obfuscationReport" : {
    "reports" : [ {
        "codehash" : "codehash",
        "failed" : true,
        "uri" : "uri",
        "obfuscated" : true,
        "script" : "script"
    }, {
        "codehash" : "codehash",
        "failed" : true,
        "uri" : "uri",
        "obfuscated" : true,
        "script" : "script"
    } ],
    "domain" : "domain",
    "analyzed" : 7,
    "siteId" : 5,
    "failed" : 9,
    "obfuscated" : 5,
    "totalUrls" : 2
},
"significance" : 1,
"instantBlockEnabled" : true,
"dynamicallyInjected" : true,
"lastSeenMs" : 1620864000001,
"domain" : "domain.com",
"ipssSample" : "1.1.1.1",
"timeBucket" : 1620864000001,
"browserStats" : {"Chrome": 120},
"id" : "d21kZWx5LXVzZWQuZG9tYWluLmNvbQ",
"domainPopularity" : "Rarely used",
"status" : {
    "blocked" : true,
    "reviewedAt" : 1629260520080,
    "reviewed" : true,
    "preapproved" : true
}
}
]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
put /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/authorization
```

Overwrite authorization of the a discovered domain for specific path (setDomainAuthorizationForPath)

Sets the domain status to block or allow with notes.

When the website is in "enforce" mode, all requests from the website to blocked domains are blocked.

By default, all newly discovered domains are authorized if the website is in "monitor" mode, and blocked if the website is in "enforce" mode. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholesite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body AuthorizationStatus (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

AuthorizationStatus

Example data

Content-Type: application/json

```
{
  "note" : "note",
  "blocked" : true,
  "author" : "Account APIs (admin@imperva.com)",
  "reviewedAt" : 1629260520080,
  "reviewed" : true,
  "lastNoteAt" : 1629260520080,
  "forceChange" : false
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK AuthorizationStatus](#)

Email

```
post /v1/sites/{siteId}/settings/emails/add
```

Add an email address to the notification list (addEmail)

Adds an email address to the event notification recipient list for a specific website. Notifications are reasonably small and limited in frequency

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

— Email address

example: "test@imperva.com"

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

EmailList

Example data

Content-Type: application/json

```
{
  "email" : "name.surname@mail.com"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Email added successfully EmailList

```
get /v1/sites/{siteId}/settings/emails
```

Retrieve the notification recipient list (getEmails)

Retrieves the list of email addresses that are subscribed to event notifications for a specific website.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[EmailList]

Example data

Content-Type: application/json

```
[ {  
    "email" : "name.surname@mail.com"  
, {  
    "email" : "name.surname@mail.com"  
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

A list of email addresses subscribed to notifications about the events related to this site.

```
post /v1/sites/{siteId}/settings/emails/delete
```

Delete an email address from the notification list (removeEmail)

Removes the email address from the event notification recipient list for a specific website.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

— Email address

example: "test@imperova.com"

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Responses

204

Email removed successfully

Notes

```
post /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes
```

Add notes to a discovered domain for specific path (addDomainNoteForPath)

Add a quick note to a domain to help in future analysis and investigation. You can add as many notes as you like. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholesite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

— Content of the note.

example: "Review domain later."

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[FullNote]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Note added successfully

```
delete /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes
```

Delete notes from a discovered domain for specific path (deleteDomainNoteForPath)

Delete all notes for a domain. All notes attached to a domain will be removed! If the API key used is for a parent

account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholesite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body FullNote (optional)

Body Parameter

— Domain note

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[FullNote]

Example data

Content-Type: application/json

```
[ {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
}, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

204

All notes removed

```
get /v1/sites/{siteId}/paths/{pathId}/domains/{domainId}/notes
```

Retrieve user notes for a discovered domain for specific path (getDomainNotesForPath)

Retrieves the list of user-added notes for a domain aimed to help in future analysis in investigation If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholesite" to get All Paths data.

domainId (required)

Path Parameter

— Domain reference id as received from getDomains operation

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[FullNote](#)]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
```

```

    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
}, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
} ]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

PreApprovedDomainsAndScripts

```
post /v1/sites/{siteId}/preapprovedlist
```

Add a domain to pre-approved list (addPreApprovedDomain)

Adds a known domain to a pre-approved list.

When the domain is discovered by Client-Side Protection, it is automatically approved and marked as Authorized.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ShallowPreApprovedDomain (required)

Body Parameter

— The known domain user wants to pre-approve

example: "www.example.com"

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[PreApprovedDomain](#)

Example data

Content-Type: application/json

```
{
  "subdomains" : true,
  "applyToAllOnboardedPaths" : true,
  "domain" : "domain",
  "referenceId" : "d21kZWx5LXVzzWQuZG9tYWluLmNvbQ"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Domain added successfully. [PreApprovedDomain](#)

```
post /v1/sites/{siteId}/preapproved-scripts
```

Add a script to pre-approved list (addPreApprovedScript)

Adds a known script to a pre-approved list.

When the script is discovered by Client-Side Protection, it is automatically approved and marked as Authorized.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body PreApprovedScript (required)

Body Parameter

— The known script user wants to pre-approve

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PreApprovedScript

Example data

Content-Type: application/json

```
{
  "applyToAllOnboardedPaths" : true,
  "script" : "script",
  "referenceId" : "d21kZWx5LXVzZWQuZG9tYWluLmNvbQ"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Domain added successfully. PreApprovedScript

```
delete /v1/sites/{siteId}/preapprovedlist/{preApprovedDomainId}
```

Delete the pre-approved domain (deletePreApprovedDomain)
Removes the domain from the pre-approved list.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site format: int64

preApprovedDomainId (required)

Path Parameter

— The Imperva domain ID of the pre-approved domain. You can retrieve the domain ID using the GET HTTP method.)

Query parameters

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Responses

204

Domain deleted successfully

```
delete /v1/sites/{siteId}/preapproved-scripts/{preApprovedscriptId}
```

Delete the pre-approved script (deletePreApprovedScript)
Removes the script from the pre-approved list.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site format: int64

preApprovedscriptId (required)

Path Parameter

— The Imperva domain ID of the pre-approved script. You can retrieve the domain ID using the GET HTTP method.)

Query parameters

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Responses

204

Script deleted successfully

```
get /v1/sites/{siteId}/preapprovedlist/{preApprovedDomainId}
```

Retrieve the pre-approved domain (getPreApprovedDomain)
Retrieve the domain from the pre-approved list.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

preApprovedDomainId (required)

Path Parameter

— The Imperva domain ID of the pre-approved domain. You can retrieve the domain ID using the GET HTTP method.)

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

PreApprovedDomain

Example data

Content-Type: application/json

```
{
  "subdomains" : true,
  "applyToAllOnboardedPaths" : true,
  "domain" : "domain",
  "referenceId" : "d2lkZWx5LXVzzWQuZG9tYWluLmNvbQ"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK PreApprovedDomain](#)

```
get /v1/sites/{siteId}/preapprovedlist
```

Retrieve list of pre-approved domains (getPreApprovedDomains)

Retrieves the list of domains approved by user before they were discovered by the system.

When these domains are discovered by Client-Side Protection, they are automatically approved and marked as Authorized.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

Query parameters

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[PreApprovedDomain](#)]

Example data

Content-Type: application/json

```
[ {
  "subdomains" : true,
  "applyToAllOnboardedPaths" : true,
  "domain" : "domain",
  "referenceId" : "d2lkZWx5LXVzZWQuZG9tYWluLmNvbQ"
}, {
  "subdomains" : true,
  "applyToAllOnboardedPaths" : true,
  "domain" : "domain",
  "referenceId" : "d2lkZWx5LXVzZWQuZG9tYWluLmNvbQ"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
get /v1/sites/{siteId}/preapproved-scripts
```

Retrieve list of pre-approved scripts (getPreApprovedScripts)

Retrieves the list of scripts approved by user before they were discovered by the system.

When these scripts are discovered by Client-Side Protection, they are automatically approved and marked as Authorized.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[PreApprovedScript]

Example data

Content-Type: application/json

```
[ {
  "applyToAllOnboardedPaths" : true,
  "script" : "script",
  "referenceId" : "d21kZWx5LXVzZWQuZG9tYWluLmNvbQ"
}, {
  "applyToAllOnboardedPaths" : true,
  "script" : "script",
```

```

    "referenceId" : "d21kZWx5LXVzZWQuZG9tYWluLmNvbQ"
}
]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

Scripts

```
post /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes
```

Add notes to a discovered script group. (addScriptGroupNotesForPath)

Add a quick note to a script group to help in future analysis and investigation. You can add as many notes as you like.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

groupId (required)

Path Parameter

— Script group reference id as received from getScripts operation.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

— Content of the note.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[ScriptNote]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
post /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes
```

Add notes to a discovered script for specific path (addScriptNotesForPath)

Add a quick note to a script to help in future analysis and investigation. You can add as many notes as you like.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

-
- Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.
 - scriptId (required)
 - Path Parameter
 - Script reference id as received from getScripts operation.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

- Content of the note.

Query parameters

caid (optional)

Query Parameter

- The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[ScriptNote]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
delete /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes
```

Delete notes of discovered script group. (deleteScriptGroupNotesForPath)
Delete notes of discovered script group.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

groupId (required)

Path Parameter

— Script group reference id as received from getScripts operation.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ScriptNote](#) (optional)

Body Parameter

— Script group note

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[ScriptNote](#)]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
delete /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes
```

Delete notes of discovered script for specific path (deleteScriptNotesForPath)
Delete notes of script.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **ScriptNote** (optional)

Body Parameter

— Script note

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[ScriptNote]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
post /v1/sites/{siteId}/script-ai
```

Retrieve script AI explanation by script key (getScriptAiExplanationByKey)

AI explanation of what the script is doing. Client-Side Protection gathers all available information of the script to help with analysis.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body **string** (required)

Body Parameter

— S3 bucket script key

Query parameters

inline (optional)

Query Parameter

— If true, gets explanation for an inline script, otherwise gets explanation for non-inline script default: false

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK String

```
get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/authorization
```

Retrieve authorization details of a discovered script for specific path (getScriptAuthorizationForPath)

Retrieves authorization details of the script including whether the script is blocked or authorized, and reviewed or unreviewed, and notes.

When the website is in "enforce" mode, all requests from the website to blocked scripts are blocked.

By default, all newly discovered scripts are authorized if the website is in "monitor" mode, and blocked if the website is in "enforce" mode. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ScriptAuthorizationStatus](#)

Example data

Content-Type: application/json

```
{
  "note" : "note",
  "blocked" : true,
  "author" : "Account APIs (admin@imperva.com)",
  "reviewedAt" : 1629260520080,
  "reviewed" : true,
  "lastNoteAt" : 1629260520080,
  "newVersionSinceAuth" : true
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK ScriptAuthorizationStatus](#)

```
post /v1/script
```

Retrieve script by script key (getScriptByKey)

Every script accessed from the site is recorded in this list. Client-Side Protection gathers all available information of the script to help with analysis.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/plain

Request body

body string (required)

Body Parameter

— S3 bucket script key

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK String

```
get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/call-chain
```

Get calling chain of a discovered script for a given path (getScriptCallChainByKeyForPath)
Retrieves the sequence of calls that occur when the discovered script is executed.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation

Query parameters

graph (optional)

Query Parameter

— If true, show call chain in graph structure, otherwise show it in flat list structure. default: true

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Object

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK Object](#)

```
get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}
```

Retrieve script detail for a given script for a given path (getScriptDetailForPath)

Client-Side Protection tracks the specified script when it is accessed by the site and gathers all available information to help with analysis. This feature supports:

- 3rd party and origin scripts from any path
- Inline scripts that originated from paths onboarded in PCI scope (using the "Payment Page" option)

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— The numeric identifier of the path

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ScriptDetail](#)

Example data

Content-Type: application/json

```
{
  "sampleIPsDetected" : 0,
  "origin" : true,
  "source" : "source",
```

```

"requestFile" : "requestFile",
"discoveredOn" : 6,
"path" : {
  "isPciCompliance" : true,
  "name" : "name"
},
"scriptSample" : "scriptSample",
"lastSeen" : 1,
"scriptType" : "thirdparty",
"popularity" : "popularity",
"currentHashScript" : {
  "lastSeen" : 5,
  "time" : 1,
  "hash" : "hash",
  "script" : "script"
},
"scriptDomainInfo" : {
  "domainLastSeenMs" : 5,
  "domain" : "domain",
  "domainRisk" : "domainRisk",
  "domainId" : "domainId",
  "domainPopularity" : "domainPopularity"
},
"risk" : "risk",
"id" : "id",
"hashScripts" : [ null, null ],
"lineNumber" : 5,
"requestPath" : "requestPath",
"isOrigin" : true,
"resourceType" : "ALL",
"status" : {
  "blocked" : true,
  "reviewedAt" : 1629260520080,
  "reviewed" : true,
  "newVersionSinceAuth" : true,
  "preapproved" : true
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ScriptDetail

```
get /v1/sites/{siteId}/paths/{pathId}/scripts-group/{groupId}/notes
```

Retrieve user notes for a discovered script group (getScriptGroupNotesForPath)
Retrieves the list of user-added notes for a script group aimed to help in future analysis in investigation.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

groupId (required)

Path Parameter

— Script group reference id as received from getScripts operation.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[ScriptNote]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
get /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/notes
```

Retrieve user notes for a discovered script for specific path (getScriptNotesForPath)
 Retrieves the list of user-added notes for a script aimed to help in future analysis in investigation.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[ScriptNote](#)]

Example data

Content-Type: application/json

```
[ {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
}, {
  "date" : 1629260520080,
  "author" : "Mr. Hyde (edward.hyde@gmail.com)",
  "text" : "Review this domain with UI team."
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
get /v1/sites/{siteId}/paths/{pathId}/scripts
```

Retrieve list of all discovered scripts for path (getScriptsForPath)

Every script accessed from the site is recorded in this list. Client-Side Protection gathers all available information of the script to help with analysis.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— The base 64 encoded ID of the path

Query parameters

significant (optional)

Query Parameter

— Show scripts that belong to significant or insignificant domains only. default: true

origin (optional)

Query Parameter

— If true, show only scripts from the origin. Otherwise show 3rd party scripts from external sources. default: false

inline (optional)

Query Parameter

— If true, show only inline scripts from the origin. default: false

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[ScriptPath]

Example data

Content-Type: application/json

```
[ {
  "notes" : [ {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  }, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  } ],
  "origin" : true,
  "domainRisk" : "Low",
  "source" : "source",
  "requestFile" : "requestFile",
  "domainId" : "domainId",
  "path" : {
    "isPciCompliance" : true,
    "name" : "name"
  },
  "scriptSample" : "scriptSample",
  "lastSeenMs" : 6,
  "domain" : "domain",
  "scriptType" : "thirdparty",
  "popularity" : "popularity",
  "currentHashScript" : {
    "lastSeen" : 5,
    "time" : 1,
    "hash" : "hash",
    "script" : "script"
  },
  "id" : "id",
  "hashScripts" : [ null, null ],
  "lineNumber" : 0,
  "requestPath" : "requestPath",
  "isOrigin" : true,
  "lastSuccessfulDownload" : 5,
  "status" : {
    "blocked" : true,
    "reviewedAt" : 1629260520080,
    "reviewed" : true,
    "newVersionSinceAuth" : true,
    "preapproved" : true
  }
}, {
  "notes" : [ {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  }, {
    "date" : 1629260520080,
    "author" : "Mr. Hyde (edward.hyde@gmail.com)",
    "text" : "Review this domain with UI team."
  } ],
  "origin" : true,
  "domainRisk" : "Low",
  "source" : "source",
  "requestFile" : "requestFile",
  "domainId" : "domainId",
  "path" : {
```

```

    "isPciCompliance" : true,
    "name" : "name"
  },
  "scriptSample" : "scriptSample",
  "lastSeenMs" : 6,
  "domain" : "domain",
  "scriptType" : "thirdparty",
  "popularity" : "popularity",
  "currentHashScript" : {
    "lastSeen" : 5,
    "time" : 1,
    "hash" : "hash",
    "script" : "script"
  },
  "id" : "id",
  "hashScripts" : [ null, null ],
  "lineNumber" : 0,
  "requestPath" : "requestPath",
  "isOrigin" : true,
  "lastSuccessfulDownload" : 5,
  "status" : {
    "blocked" : true,
    "reviewedAt" : 1629260520080,
    "reviewed" : true,
    "newVersionSinceAuth" : true,
    "preapproved" : true
  }
}
]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
put /v1/sites/{siteId}/paths/{pathId}/scripts/{scriptId}/authorization
```

Overwrite authorization of the a discovered script for specific path (setScriptAuthorizationForPath)

Sets the script status to block or allow with notes.

When the website is in "enforce" mode, all requests from the website to blocked scripts are blocked.

By default, all newly discovered scripts are authorized if the website is in "monitor" mode, and blocked if the website is in "enforce" mode. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

scriptId (required)

Path Parameter

— Script reference id as received from getScripts operation

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body AuthorizationStatus (required)

Body Parameter

Query parameters

caId (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Object

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK Object

Websites

```
post /v1/sites/{siteId}/paths
```

Add path configuration for a site (addSitePathConfig)

Configure a path for a site. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body OnboardSitePathConfig (required)

Body Parameter

— Site path configuration

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

SitePathConfig

Example data

Content-Type: application/json

```
{
  "paths" : [ {
    "mode" : "monitor",
    "removeUnsafeType" : "all",
    "createdAt" : 6,
    "enforceType" : "all",
    "isMonitoringHeader" : true,
    "isPciCompliance" : true,
    "additionalHeader" : "additionalHeader",
    "name" : "name",
    "type" : "pci",
    "simulationIPs" : [ "simulationIPs", "simulationIPs" ],
    "updatedAt" : 1
  }, {
    "mode" : "monitor",
    "removeUnsafeType" : "all",
    "createdAt" : 6,
    "enforceType" : "all",
    "isMonitoringHeader" : true,
    "isPciCompliance" : true,
    "additionalHeader" : "additionalHeader",
    "name" : "name",
    "type" : "pci",
    "simulationIPs" : [ "simulationIPs", "simulationIPs" ],
    "updatedAt" : 1
  } ],
  "name" : "name",
  "onboardType" : "path",
  "id" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SitePathConfig

```
post /v1/sites/{siteId}/change-site-type
```

Change onboarded site type (changeSiteType)

Change the site type that was set during onboarding, either from multi-page application (MPA) to single-page application (SPA), or from SPA to MPA. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

Query parameters

change-to-spa (optional)

Query Parameter

— When set to true, the site type changes from MPA to SPA. When set to false, the site type changes from SPA to MPA. default: true

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Object

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK Object](#)

```
delete /v1/sites/{siteId}/paths
```

Delete path configuration for a site (deleteSitePathConfig)

Delete a path configuration for a site. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

[siteld \(required\)](#)

Path Parameter

— The numeric identifier of the site. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body OnboardSitePathConfig (required)

Body Parameter

— Site path configuration

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Responses

200

OK

```
get /v1/sites/{siteId}/discovery
```

Retrieve discovery status of a website (getDiscoveryStatus)

Indicates if Client-Side Protection discovery is active or suspended.

When paused, Client-Side Protection stops monitoring for new domains and doesn't inject the Content-Security-Policy header in the website response. You can still review domains and update the website settings. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID

format: int64

Return type

DiscoveryStatus

Example data

Content-Type: application/json

```
{
  "onboardingTime" : 0,
  "status" : "start"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DiscoveryStatus

```
get /v1/sites/{siteId}/paths/{pathId}/enforce/status
```

Get the CSP enforce header health status of a website for a specific path (getEnforceStatusForPath)
Get the CSP enforce header health status of a website for a specific path. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholesite" to get All Paths data.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

HealthStateResponse

Example data

Content-Type: application/json

```
{
  "healthState" : "healthy",
  "lastDiscovered" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK HealthStateResponse

```
get /v1/sites/{siteId}/paths/{pathId}/enforce-header
```

Get enforcement header of a website for a specific path (getEnforcementHeaderForPath)

Get the current enforcement header for a specific path. This is useful to check the enforcement policy of the website. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Query parameters

enforce-type (required)

Query Parameter

— Enforce type. Possible values: all, script, domain.

default-header (required)

Query Parameter

— If true, return default header otherwise return true header. default: false
caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK String](#)

```
get /v1/sites/{siteId}/paths/{pathId}/mode
```

Retrieve protection mode of a website for a specific path (getEnforcementModeForPath)

Retrieves the protection mode of a website for a specific path.

When in Enforce Mode, all resources you set to Block are not available in your application and new resources are automatically blocked. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteId (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

EnforcePathMode

Example data

Content-Type: application/json

```
{
  "mode" : "monitor",
  "enforceType" : "all",
  "additionalHeader" : "additionalHeader",
  "simulationIPs" : [ "simulationIPs", "simulationIPs" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK EnforcePathMode

```
get /v1/sites/{siteId}/tracking-ids
```

Retrieve list of Google tracking IDs detected for this website (getGoogleTrackingIds)

Retrieves the list of Google Analytics tracking IDs that were detected, indicating which account Google Analytics data is being sent to from your website.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

array[[Analytics](#)]

Example data

Content-Type: application/json

```
[ {
  "discoveredMs" : 1629260520080,
  "trackingId" : "UA-000000-2"
}, {
  "discoveredMs" : 1629260520080,
  "trackingId" : "UA-000000-2"
} ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
get /v1/sites/{siteId}/paths/{pathId}/monitor/status
```

Get the CSP monitor header health status of a website for a specific path (getMonitorStatusForPath)

Get the CSP report-only header health status of a website for a specific path. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

HealthStateResponse

Example data

Content-Type: application/json

```
{
  "healthState" : "healthy",
  "lastDiscovered" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK HealthStateResponse

```
get /v1/sites/{siteId}
```

Retrieve website configuration and status details (getSite)

Retrieves Client-Side Protection configuration and status details for a specific website. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[Site](#)

Example data

Content-Type: application/json

```
{
  "mode" : "monitor",
  "settings" : {
    "emails" : [ {
      "email" : "name.surname@mail.com"
    }, {
      "email" : "name.surname@mail.com"
    } ]
  },
  "tracking-ids" : [ {
    "discoveredMs" : 1629260520080,
    "trackingId" : "UA-000000-2"
  },
  {
    "discoveredMs" : 1629260520080,
    "trackingId" : "UA-000000-2"
  } ],
  "instantBlockEnabled" : true,
  "discovery" : "start",
  "name" : "www.site.com"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK Site

```
get /v1/sites/{siteId}/paths
```

Retrieve path configuration for a site (getSitePathConfig)

Retrieve all paths configured for a site. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`sitelid` (required)
 Path Parameter
 — The numeric identifier of the site. format: int64

Query parameters

`caid` (optional)
 Query Parameter
 — The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`SitePathConfig`

Example data

Content-Type: application/json

```
{
  "paths" : [ {
    "mode" : "monitor",
    "removeUnsafeType" : "all",
    "createdAt" : 6,
    "enforceType" : "all",
    "isMonitoringHeader" : true,
    "isPciCompliance" : true,
    "additionalHeader" : "additionalHeader",
    "name" : "name",
    "type" : "pci",
    "simulationIPs" : [ "simulationIPs", "simulationIPs" ],
    "updatedAt" : 1
  }, {
    "mode" : "monitor",
    "removeUnsafeType" : "all",
    "createdAt" : 6,
    "enforceType" : "all",
    "isMonitoringHeader" : true,
    "isPciCompliance" : true,
    "additionalHeader" : "additionalHeader",
    "name" : "name",
    "type" : "pci",
    "simulationIPs" : [ "simulationIPs", "simulationIPs" ],
    "updatedAt" : 1
  } ],
  "name" : "name",
  "onboardType" : "path",
  "id" : 0
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SitePathConfig

```
get /v1/sites/{siteId}/domain_reputation
```

Retrieve Osint scores for this website (getSiteReputation)

Retrieves Osint scores for each domain from Osint Domain Reputation Service for this website, Osint score indicates the risk level of a domain.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

SiteReputation

Example data

Content-Type: application/json

```
{
  "key" : {
    "score" : 0.8008281904610115
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

OK SiteReputation

```
get /v1/sites/{siteId}/settings
```

Retrieve website settings (getSiteSettings)

Retrieves Client-Side Protection settings for a specific website, such as the list of email address in the event notification recipient list. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

SiteSettings

Example data

Content-Type: application/json

```
{
  "emails" : [ {
    "email" : "name.surname@mail.com"
  }, {
    "email" : "name.surname@mail.com"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

OK SiteSettings

```
get /v1/sites
```

Retrieve all websites for current account (getSites)

Retrieves the list of all websites in your account, as well as their Client-Side Protection configuration and status details. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

map[Site]

Example data

Content-Type: application/json

```
{
  "key" : {
    "mode" : "monitor",
    "settings" : {
      "emails" : [ {
        "email" : "name.surname@mail.com"
      }, {
        "email" : "name.surname@mail.com"
      } ]
    },
    "tracking-ids" : [ {
      "discoveredMs" : 1629260520080,
      "trackingId" : "UA-000000-2"
    }, {
      "discoveredMs" : 1629260520080,
      "trackingId" : "UA-000000-2"
    } ],
    "instantBlockEnabled" : true,
    "discovery" : "start",
  }
}
```

```

        "name" : "www.site.com"
    }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

```
get /v1/sites/{siteId}/paths/{pathId}/unsafe-directives
```

Get unsafe directives configuration for paths (getUnsafeDirectivesForPath)

Get unsafe directives configuration for a specific website path. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

UnsafeDirectivesConfig

Example data

Content-Type: application/json

```
{
```

```

    "unsafeInlineStyles" : true,
    "unsafeEval" : true,
    "unsafeHashes" : true,
    "unsafeInlineScripts" : true
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK UnsafeDirectivesConfig

```
put /v1/sites/{siteId}/discovery
```

Change discovery status of a website (setDiscoveryStatus)

Suspend or restart the discovery of new services.

When paused, Client-Side Protection stops monitoring for new domains and doesn't inject the Content-Security-Policy header in the website response. You can still review domains and update the website settings. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body string (required)

Body Parameter

— discovery status

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Discovery

Example data

Content-Type: application/json

```
"start"
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK Discovery](#)

```
post /v1/sites/{siteId}/paths/{pathId}/mode
```

Change protection mode of a website for a specific path (setEnforcementModeForPath)

Enables you to switch between Monitor Mode and Enforce Mode for a specific path.

When in Enforce Mode, all resources you set to Block are not available in your application and new resources are automatically blocked. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

sitId (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [EnforcePathMode](#) (required)

Body Parameter

— Enforce configuration for path

Request headers

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

Object

Example data

Content-Type: application/json

```
{ }
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK Object

```
put /v1/sites/{siteId}
```

Change website configuration and status details (setSite)

Change Client-Side Protection configuration and status details for a specific website. This will change the

discovery status, protection mode and emails list all at once for the site. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

`siteld` (required)
 Path Parameter
 — The numeric identifier of the site. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `SetSite` (required)
 Body Parameter
 —

Query parameters

`caid` (optional)
 Query Parameter
 — The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

`SetSite`

Example data

Content-Type: `application/json`

```
{
  "mode" : "monitor",
  "settings" : {
    "emails" : [ {
      "email" : "name.surname@mail.com"
    }, {
      "email" : "name.surname@mail.com"
    } ]
  },
  "tracking-ids" : [ {
    "discoveredMs" : 1629260520080,
    "trackingId" : "UA-000000-2"
  }, {
    "discoveredMs" : 1629260520080,
    "trackingId" : "UA-000000-2"
  } ],
}
```

```

    "discovery" : "start",
    "name" : "www.site.com"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK SetSite](#)

```
post /v1/sites/{siteId}/paths/{pathId}/unsafe-directives
```

Set unsafe directives configuration for paths (setUnsafeDirectivesForPath)

Set unsafe directives configuration for a specific website path. If the API key used is for a parent account, and the website belongs to a sub account, the caid of the sub account must be specified.

Path parameters

siteld (required)

Path Parameter

— The numeric identifier of the site. format: int64

pathId (required)

Path Parameter

— Path reference id, use Base64 encoded string of "wholeSite" to get All Paths data.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body UnsafeDirectivesConfig (required)

Body Parameter

— Unsafe directives configuration. A value of true indicates that the directive is included in the Content-Security-Policy header when Enforcement mode is activated.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used

for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[HeaderPreview](#)

Example data

Content-Type: application/json

```
{  
    "domainsEnforcement" : "domainsEnforcement",  
    "scriptsEnforcement" : "scriptsEnforcement",  
    "domainsAndScriptsEnforcement" : "domainsAndScriptsEnforcement"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK HeaderPreview](#)

Models

[Methods](#)

Table of Contents

1. [Analytics](#)
 2. [AuthorizationStatus](#)
 3. [Discovery](#)
 4. [DiscoveryStatus](#)
 5. [Domain](#)
 6. [DomainInfo](#)
 7. [DomainObfuscationReport](#)
 8. [DomainQuality](#)
 9. [DomainReport](#)
 10. [DomainReputation](#)
 11. [DomainRisk](#)
-

-
12. DomainStatus
 13. EmailList
 14. EnforcePathMode
 15. FullNote
 16. HashScript
 17. HeaderPreview
 18. HealthStateResponse
 19. Mode
 20. OnboardSitePathConfig
 21. PreApprovedDomain
 22. PreApprovedScript
 23. SSLCertificateInfo
 24. ScriptAuthorizationStatus
 25. ScriptDetail
 26. ScriptDomainInfo
 27. ScriptNote
 28. ScriptPath
 29. ScriptPathDetail
 30. ScriptStatus
 31. SetSite
 32. ShallowPreApprovedDomain
 33. Site
 34. SitePath
 35. SitePathConfig
 36. SiteReputation
 37. SiteSettings
 38. TimeMeasurement
 39. UnsafeDirectivesConfig
 40. UrlObfuscationReport

Analytics

trackingId (optional)

String

Google analytics tracking id

example: UA-000000-2

discoveredMs (optional)

Long

Date the tracking id was discovered in milliseconds. format: int64

example: 1629260520080

AuthorizationStatus

Authorization status. Indicates if the domain is reviewed and if it is authorized or blocked and justification note.

blocked (optional)

Boolean

Indicates if the item is blocked. Default is false if the website is in "monitor" mode, and true if the

website is in "enforce" mode.

reviewed (optional)

Boolean

Indicates if the item is reviewed. A convenient tag to mark item reviewed to clearly see which items are reviewed and which are still left for review.

reviewedAt (optional)

Long

The date the item was reviewed. format: int64

example: 1629260520080

note (optional)

String

Authorization justification note

author (optional)

String

Author of the justification note

example: Account APIs (admin@imperva.com)

lastNoteAt (optional)

Long

Latest timestamp of the note creation format: int64

example: 1629260520080

forceChange (optional)

Boolean

Set to true to force the authorization status change, resolving any detected conflicts automatically. Defaults to false if not provided.

example: false

Discovery

In the 'initial' state, discovery has not started for the website. 'start' indicates that the discovery process is active for the website. When discovery is paused, Client-Side Protection stops monitoring for new domains and doesn't inject the CSP header in the website response. You can still review domains and update the website settings. Possible values: start, pause, initial.

DiscoveryStatus

status (optional)

Discovery

onboardingTime (optional)

Long

format: int64

Domain

id (optional)

String

Domain reference id used in different operations.

example: d2lkZWx5LXVzZWQuZG9tYWluLmNvbQ

domain (optional)

String

Domain name

example: domain.com

status (optional)

DomainStatus

domainRisk (optional)

DomainRisk

notes (optional)

array[FullNote]

List of notes associated with the domain. Added by the API user as a quick note for convenience.

timeBucket (optional)

Long

format: int64

example: 1620864000001

significance (optional)

Integer

If the service is part of the profile and/or frequently requested. The two values are 1 or 0. 1 = significant. 0 = not significant. format: int32

example: 1

resourceTypes (optional)

array[String]

Enum:

browserStats (optional)

map[String, Long]

Statistics of browsers of clients that used the domain. format: int64

example: "Chrome": 120

countryStats (optional)

map[String, Long]

Statistics of countries of clients that used the domain. format: int64

example: "US": 2

ipsSample (optional)

array[String]

A sample of IP sources detected in the CSP reports.

example: 1.1.1.1

sources (optional)

Long

IP sources detected in the sampled CSP reports. format: int64

example: 119

frequent (optional)

Boolean

If the service is frequently requested.

example: true

partOfProfile (optional)

Boolean

Domain is likely a part of the profile. The profile is the list of domains and services that are embedded in the website, directly or through 3rd-party dependency.

discoveredAt (optional)

Long

Date when domain was discovered in milliseconds. format: int64

example: 1620864000001

lastSeenMs (optional)

Long

Date when domain was last seen in milliseconds. format: int64

example: 1620864000001

domainInfo (optional)

DomainInfo

domainReports (optional)

array[DomainReport]

Aggregated domain report data.

obfuscationReport (optional)

DomainObfuscationReport

domainPopularity (optional)

String

Domain popularity.

Enum:

Rarely used

Regularly used

Widely used
instantBlockEnabled (optional)
Boolean
 Indicates whether or not Instant Block is enabled for this domain.
isDynamicallyInjected (optional)
Boolean
dynamicallyInjected (optional)
Boolean

DomainInfo

Additional domain information.

baseDomain (optional)
String
 Base domain.
 example: domain.com

companyName (optional)
String
 Name of the company that owns the domain.
 example: Company Inc.

domainCategory (optional)
String
 Category of domain
 Enum:
 Website analytics
 Social media
 Payments
 Personalization tools
 Advertisements
 CDN
 Media sharing
 Cloud storage
 Forms management
 Live support
 Hosted JS libraries
 Marketing tracker
 Unclassified
 countries (optional)
array[String]
 example: ["USA", "Canada"]

sslCertificateInfo (optional)
SSLCertificateInfo
registrationTime (optional)
TimeMeasurement
registrar (optional)
String
 The company which provides the site registration
 example: Company, Inc

orgOwner (optional)
String
 The owner of domain
 example: Company, Inc

dynamicDnsBased (optional)
Boolean
domainQuality (optional)
DomainQuality
additionalInsights (optional)
array[String]

Enum:
domainCategorySemrush (optional)
String

DomainObfuscationReport

Report about obfuscated resources found on this domain.

sitId (optional)

Long

format: int64

domain (optional)

String

reports (optional)

array[UrlObfuscationReport]

obfuscated (optional)

Long

format: int64

totalUrls (optional)

Long

format: int64

analyzed (optional)

Long

format: int64

failed (optional)

Long

format: int64

DomainQuality

The quality of the domain summarized by numerical scores.

score (optional)

Double

format: double

scoreFromMI (optional)

Double

format: double

scoreFromHeuristics (optional)

Double

format: double

scoreOverride (optional)

String

Enum:

SUSPICIOUS

MALICIOUS

MAGECART

MALWARE

BENIGN

DomainReport

Aggregated domain report data.

documentUri (optional)

String

URI of the page requesting the domain dependency.

example: <https://domain.com/document>

sourceFile (optional)

String

The file requesting the domain dependency.

example: <https://domain.com/example.js>

blockedUri (optional)

String

The requested external resource URL.

example: <https://malicious.domain.com>

lineNumber (optional)

Integer

Line number in the requesting file. format: int32

example: 101

sourceType (optional)

String

The type of content requested, such as script, images, or data transfer.

Enum:

ALL

UNKNOWN

RESOURCE

FRAME

IMAGE

DATA_TRANSFER

STYLE

FONT

SCRIPT

MANIFEST

MEDIA

FORM_ACTION

FRAME_ANCESTORS

example: SCRIPT

referrer (optional)

String

The address from which your resource has been requested on.

example: <https://malicious.domain.com>

scriptSample (optional)

String

The first 40 characters of the requesting inline script.

example: gtag('event', 'purchase',\n {\n

clientApplication (optional)

String

Client application that sent the content security policy report.

example: Chrome

statusCode (optional)

Integer

Report status code format: int32

example: 200

DomainReputation

score (optional)

Double

format: double

DomainRisk

The risk of a domain, is calculated by different quality score factors or set by score-override.

DomainStatus

Domain status. Indicates if the domain is reviewed and if it is authorized or blocked.

blocked (optional)

Boolean

Indicates if the item is blocked. Default is false if the website is in "monitor" mode, and true if the website is in "enforce" mode.

reviewed (optional)

Boolean

Indicates if the item is reviewed. A convenient tag to mark item reviewed to clearly see which items are reviewed and which are still left for review.

preapproved (optional)

Boolean

If domain is preapproved.

example: true

reviewedAt (optional)

Long

The date the item was reviewed. format: int64

example: 1629260520080

Emaillist

email (optional)

String

example: name.surname@mail.com

EnforcePathMode

mode (optional)

String

Enum:

monitor

enforce

simulated

suspended

enforceType (optional)

String

Enum:

all

script

domain

simulationIPs (optional)

array[String]

additionalHeader (optional)

String

FullNote

Note added to a domain to help in future reference.

text (optional)

String

The content of the note.

example: Review this domain with UI team.

author (optional)

String

The author email address of the user that added the note.

example: Mr. Hyde (edward.hyde@gmail.com)
date (optional)

Long

The date the note was added. format: int64

example: 1629260520080

HashScript

hash (optional)

String

script (optional)

String

time (optional)

Long

format: int64

lastSeen (optional)

Long

format: int64

HeaderPreview

Enforce header preview of different enforce types.

domainsEnforcement (optional)

String

scriptsEnforcement (optional)

String

domainsAndScriptsEnforcement (optional)

String

HealthStateResponse

Header health status response.

healthState (optional)

String

Enum:

healthy

degraded

unhealthy

not_enough_information

lastDiscovered (optional)

Long

format: int64

Mode

Website Protection Mode. When in "enforce" mode, blocked resources will not be available in the application and new resources will be automatically blocked. When in "monitor" mode, all resources are available in the application and the system keeps track of all new domains that are discovered.

OnboardSitePathConfig

Onboard site path configuration.

onboardType (optional)

String

Enum:

path
wholesite
spa
notOnboarded
isPciCompliance (optional)
Boolean
isMonitoringHeader (optional)
Boolean
paths (optional)
array[SitePath]

PreApprovedDomain

domain (optional)
String
Domain name. For example, www.domain.com.
subdomains (optional)
Boolean
Whether or not subdomains are pre-approved as well.
applyToAllOnboardedPaths (optional)
Boolean
Whether or not this pre-approved domain applies to all onboarded paths.
referenceld (optional)
String
The Imperva ID of the pre-approved domain.
example: d2lkZWx5LXVzZWQuZG9tYWluLmNvbQ

PreApprovedScript

script (optional)
String
Pre approved script name.
applyToAllOnboardedPaths (optional)
Boolean
Whether or not this pre-approved domain applies to all onboarded paths.
referenceld (optional)
String
The Imperva ID of the pre-approved script.
example: d2lkZWx5LXVzZWQuZG9tYWluLmNvbQ

SSLCertificateInfo

type (optional)
String
Enum:
DOMAIN_VALIDATION
SELF_SIGNED
NO_CERTIFICATE
NO_CONNECTION
organization (optional)
String
The organization field declared in an OV SSL Certificate.
example: Organization, Inc

ScriptAuthorizationStatus

blocked (optional)

Boolean

Indicates if the item is blocked. Default is false if the website is in "monitor" mode, and true if the website is in "enforce" mode.

reviewed (optional)

Boolean

Indicates if the item is reviewed. A convenient tag to mark item reviewed to clearly see which items are reviewed and which are still left for review.

reviewedAt (optional)

Long

The date the item was reviewed. format: int64

example: 1629260520080

note (optional)

String

Authorization justification note

author (optional)

String

Author of the justification note

example: Account APIs (admin@imperva.com)

lastNoteAt (optional)

Long

Latest timestamp of the note creation format: int64

example: 1629260520080

newVersionSinceAuth (optional)

Boolean

Indicate whether a new version has been discovered since the last authorization.

example: true

ScriptDetail

id (optional)

String

source (optional)

String

requestPath (optional)

String

requestFile (optional)

String

path (optional)

ScriptPathDetail

scriptType (optional)

String

Enum:

thirdparty

origin

inline

sampleIPsDetected (optional)

Long

format: int64

discoveredOn (optional)

Long

format: int64

lastSeen (optional)

Long

format: int64

popularity (optional)

String
resourceType (optional)

String

The type of content requested, such as script, images, or data transfer.

Enum:

ALL

UNKNOWN

RESOURCE

FRAME

IMAGE

DATA_TRANSFER

STYLE

FONT

SCRIPT

MANIFEST

MEDIA

FORM_ACTION

FRAME_ANCESTORS

risk (optional)

String

lineNumber (optional)

Integer

format: int32

scriptSample (optional)

String

status (optional)

ScriptStatus

currentHashScript (optional)

HashScript

hashScripts (optional)

array[HashScript]

isOrigin (optional)

Boolean

scriptDomainInfo (optional)

ScriptDomainInfo

origin (optional)

Boolean

ScriptDomainInfo

domainId (optional)

String

domain (optional)

String

domainLastSeenMs (optional)

Long

format: int64

domainPopularity (optional)

String

domainRisk (optional)

String

ScriptNote

Note added to a script to help in future reference.

text (optional)

String

The content of the note.

example: Review this domain with UI team.

author (optional)

String

The author email address of the user that added the note.

example: Mr. Hyde (edward.hyde@gmail.com)

date (optional)

Long

The date the note was added. format: int64

example: 1629260520080

ScriptPath

id (optional)

String

domainId (optional)

String

domain (optional)

String

path (optional)

ScriptPathDetail

scriptType (optional)

String

Enum:

thirdparty

origin

inline

source (optional)

String

requestPath (optional)

String

requestFile (optional)

String

isOrigin (optional)

Boolean

scriptSample (optional)

String

lineNumber (optional)

Integer

format: int32

lastSeenMs (optional)

Long

format: int64

currentHashScript (optional)

HashScript

hashScripts (optional)

array[**HashScript**]

popularity (optional)

String

notes (optional)

array[**ScriptNote**]

domainRisk (optional)

DomainRisk

status (optional)

ScriptStatus

lastSuccessfulDownload (optional)

Long

format: int64

origin (optional)
Boolean

ScriptPathDetail

name (optional)
String
isPciCompliance (optional)
Boolean

ScriptStatus

Script status. Indicates if the script is reviewed and if it is authorized or blocked.

blocked (optional)
Boolean

Indicates if the item is blocked. Default is false if the website is in "monitor" mode, and true if the website is in "enforce" mode.

reviewed (optional)
Boolean

Indicates if the item is reviewed. A convenient tag to mark item reviewed to clearly see which items are reviewed and which are still left for review.

reviewedAt (optional)
Long

The date the item was reviewed. format: int64

example: 1629260520080

newVersionSinceAuth (optional)

Boolean

Indicate whether a new version has been discovered since the last authorization.

example: true

preapproved (optional)

Boolean

If script is preapproved.

example: true

SetSite

The website configuration to update.

name (optional)
String
example: www.site.com

mode (optional)
Mode

discovery (optional)

Discovery

settings (optional)

SiteSettings

tracking-ids (optional)

array[Analytics]

ShallowPreApprovedDomain

domain (optional)
String
Domain name. For example, www.domain.com.
subdomains (optional)
Boolean

Whether or not subdomains are pre-approved as well.

applyToAllOnboardedPaths (optional)

Boolean

Whether or not this pre-approved domain applies to all onboarded paths.

Site

name (optional)

String

example: www.site.com

mode (optional)

Mode

discovery (optional)

Discovery

settings (optional)

SiteSettings

tracking-ids (optional)

array[Analytics]

instantBlockEnabled (optional)

Boolean

Indicates whether or not Instant Block is enabled for this website.

SitePath

name (optional)

String

createdAt (optional)

Long

format: int64

updatedAt (optional)

Long

format: int64

mode (optional)

String

Enum:

monitor

enforce

simulated

suspended

enforceType (optional)

String

Enum:

all

script

domain

isPciCompliance (optional)

Boolean

isMonitoringHeader (optional)

Boolean

type (optional)

String

Enum:

pci

sensitive

nonSensitive

simulationIPs (optional)

array[String]

additionalHeader (optional)
String
removeUnsafeType (optional)
String
Enum:
all
script
none

SitePathConfig

name (optional)
String
id (optional)
Long
format: int64
onboardType (optional)
String
Enum:
path
wholesite
spa
notOnboarded
paths (optional)
array[SitePath]

SiteReputation

SiteSettings

emails (optional)
array[EmailList]

TimeMeasurement

timestamp (optional)
Long
format: int64
example: 1629260520080
type (optional)
String
Enum:
ABSOLUTE
AFTER
BEFORE

UnsafeDirectivesConfig

Unsafe directives configuration. A value of true indicates that the directive is included in the Content-Security-Policy header when Enforcement mode is activated.

unsafeEval (optional)
Boolean
unsafeHashes (optional)
Boolean
unsafeInlineStyles (optional)

Boolean
unsafeInlineScripts (optional)
Boolean

UrlObfuscationReport

uri (optional)
String
codehash (optional)
String
script (optional)
String
obfuscated (optional)
Boolean
failed (optional)
Boolean

Reputation Intelligence API

This is an API for Imperva Reputation Intelligence. Gain visibility into the reputation of the IPs attacking your sites to make more informed, data-driven decisions. Leverage reputation data from across the Imperva customer base to help in incident response. Reputation Intelligence is for informational purposes only and does not perform any actions. Limit: 10 requests per minute. For full feature documentation, see [Reputation Intelligence](#).

Version: v1

BasePath:/ip-reputation

ISC

<https://opensource.org/licenses/ISC>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

V1

- `get /v1/reputation`

V1

```
get /v1/reputation
```

Retrieve reputation intelligence data for a specified IP. (`getIpReputation`)
Use this operation to get Reputation Intelligence details on a specified IP address.

Query parameters

ip (required)

Query Parameter

— Unique IP address. Only IPv4 addresses are supported.

Return type

IPDataApi

Example data

Content-Type: application/json

```
{
  "violations_over_time" : "Automated Attack : { 587081600000: 22,1587168000000: 9,1587254400000: 7},Backdoor/Trojan: {1587081600000: 20,1587168000000: 18,1587254400000: 17}",
  "client_application_details" : "Suspicious: {Bot: 37%,Go HTTP library: 63%},Malicious: {WordPress Bruteforcer: 100%}",
  "risk_score" : {
    "risk_score" : "HIGH",
    "risk_description" : "risk_description",
    "risk_score_number" : "77"
  },
  "attacks_by_industries" : "Travel: 41%,Unclassified: 20%,Business: 20%,Financial Services: 19%",
  "known_to_use" : "tor",
  "ip" : "1.1.1.1",
  "origin" : {
    "country" : "Israel",
    "city" : "Rehovot"
  },
  "known_for" : "ddos, sql injection",
  "violations" : "Backdoor/Trojan: 40%,Protocol Manipulation: 25%,Automated Attack: 35%",
  "client_application" : "Suspicious: 50%, Malicious: 50%",
  "requests" : "1260",
  "ASN" : {
    "organization_name" : "Telefonica De Espana",
    "organization_number" : 3352
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response IPDataApi

500

Error while fetching IP reputation [ErrorResponseWrapper](#)

Models

Methods

Table of Contents

1. AsnData
2. ErrorResponseWrapper
3. IPDataApi
4. IPGeoData
5. RiskData

AsnData

organization_name (optional)

String

The organization name associated with the specific IP address.

example: Telefonica De Espana

organization_number (optional)

Integer

The ASN number associated with the specific IP address. format: int32

example: 3352

ErrorResponseWrapper

Object that describes a non valid response

id (optional)

String

Unique id to identify the error in the logs

example: Xu09cHAb

code (optional)

String

HTTP response code

Enum:

OK

CREATED

ACCEPTED

NO_CONTENT

RESET_CONTENT

PARTIAL_CONTENT

MOVED_PERMANENTLY

```

FOUNDED
SEE_OTHER
NOT_MODIFIED
USE_PROXY
TEMPORARY_REDIRECT
BAD_REQUEST
UNAUTHORIZED
PAYMENT_REQUIRED
FORBIDDEN
NOT_FOUND
METHOD_NOT_ALLOWED
NOT_ACCEPTABLE
PROXY_AUTHENTICATION_REQUIRED
REQUEST_TIMEOUT
CONFLICT
GONE
LENGTH_REQUIRED
PRECONDITION_FAILED
REQUEST_ENTITY_TOO_LARGE
REQUEST_URI_TOO_LONG
UNSUPPORTED_MEDIA_TYPE
REQUESTED_RANGE_NOT_SATISFIABLE
EXPECTATION_FAILED
PRECONDITION_REQUIRED
TOO_MANY_REQUESTS
REQUEST_HEADER_FIELDS_TOO_LARGE
INTERNAL_SERVER_ERROR
NOT_IMPLEMENTED
BAD_GATEWAY
SERVICE_UNAVAILABLE
GATEWAY_TIMEOUT
HTTP_VERSION_NOT_SUPPORTED
NETWORK_AUTHENTICATION_REQUIRED
example: 500
message (optional)
String
Error description
example: Error fetching incident: ad2c8f40-3e82-11e9-354e-b114829e37eb

```

IPDataApi

ip (optional)
String
The IP address for which reputation intelligence data is presented.
example: 1.1.1.1
origin (optional)
IPGeoData
ASN (optional)
AsnData
known_to_use (optional)
String
The tools or mechanisms used to carry out the attacks, such as Tor, automated browser, or anonymous proxy.
example: tor
known_for (optional)
String
The attack type, such as DDoS or account takeover.
example: ddos, sql
risk_score (optional)

RiskData

requests (optional)

String

The number of requests sent from this IP to Imperva customers during the 2 week time frame covered in this report.

example: 1260

violations_over_time (optional)

map[String, map[String, String]]

Hits per attack type at the specified time stamp.

example: Automated Attack : { 587081600000: 22,1587168000000: 9,1587254400000: 7},Backdoor/Troja: {15870 81600000: 20,1587168000000: 18,1587254400000: 17}

violations (optional)

map[String, String]

Attack type distribution.

example: Backdoor/Trojan: 40%,Protocol Manipulation: 25%,Automated Attack: 35%

client_application (optional)

map[String, String]

Client application distribution.

example: Suspicious: 50%, Malicious: 50%

client_application_details (optional)

map[String, map[String, String]]

Details of the client applications used to attack.

example: Suspicious: {Bot: 37%,Go HTTP library: 63%},Malicious: {WordPress Bruteforcer: 100%}

attacks_by_industries (optional)

map[String, String]

Distribution of the industries associated with the attacked sites.

example: Travel: 41%,Unclassified: 20%,Business: 20%,Financial Services: 19%

IPGeoData

country (optional)

String

The country of origin of the attack by this IP address.

example: Israel

city (optional)

String

The city of origin of the attack by this IP address.

example: Rehovot

RiskData

risk_score (optional)

String

An assessment of the risk level posed by this IP, based on activity of this IP across the Imperva customer base over the past week (clean and malicious traffic).The calculation takes into account the number of attacks, the number of Imperva customer accounts that were attacked, and the severity of attacks by this IP. Possible values: CRITICAL, HIGH, MEDIUM, LOW. (CRITICAL: Risk score number of 75 or above. HIGH: Risk score number of 50-74. MEDIUM: Risk score number of 25-49. LOW: Risk score number below 25.)

example: HIGH

risk_description (optional)

String

Additional details on the risk assessment.

risk_score_number (optional)

String

risk score number between 0 and 100

example: 77

Runtime Protection API

This topic describes the API for Imperva Runtime Protection.

Version: 1.0.0

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AgentPackages

- `post /v3/agent-packages`
- `delete /v3/agent-packages/{agentId}`
- `get /v3/agent-packages/download-runtime-agent-installer`
- `get /v3/agent-packages/{agentId}`
- `get /v3/agent-packages`
- `patch /v3/agent-packages/{agentId}`

AgentVersions

- `get /v3/runtime-agent-versions`

AgentPackages

```
post /v3/agent-packages
```

Create a new agent package (addAgentPackage)

Creates and stores a new runtime agent package in the database.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body [AddAgentPackageRequest](#) (required)
Body Parameter

Query parameters

caid (optional)
Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[AgentPackageResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  }, {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

500

Unexpected error during agent package creation [ApiFailureResponseV3](#)

200

Agent package created successfully [AgentPackageResponse](#)

400

Validation error for agent package [ApiFailureResponseV3](#)

```
delete /v3/agent-packages/{agentId}
```

Delete runtime agent package (deleteAgentPackage)

Delete runtime agent package based on package Id

Path parameters

agentId (required)

Path Parameter

— format: uuid

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
format: int64

Return type

String

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

▪ */*

Responses

500

Error while processing request [ApiFailureResponseV3](#)

400

Failed to delete agent package [ApiFailureResponseV3](#)

200

Successfully deleted package [String](#)

```
get /v3/agent-packages/download-runtime-agent-installer
```

Download agent package installer (downloadAgentPackage)

Provides the installer for a specific runtime agent package version.

Query parameters

agentVersion (required)

Query Parameter

—

agentType (required)

Query Parameter

—

isVersionLess (required)

Query Parameter

—

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[String](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

400

Error downloading agent package installer [ApiFailureResponseV3](#)

500

Unexpected error during agent package installer download [ApiFailureResponseV3](#)

200

Agent package installer downloaded successfully [String](#)

```
get /v3/agent-packages/{agentId}
```

Get agent package by ID (getAgentPackageById)

Fetches details of a specific runtime agent package using its unique ID.

Path parameters

agentId (required)

Path Parameter

— format: uuid

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
format: int64

Return type

[AgentPackageResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  }, {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

400

Error fetching agent package by ID [ApiResponseV3](#)

200

Agent package retrieved successfully [AgentPackageResponse](#)

500

Unexpected error during agent package retrieval by ID [ApiResponseV3](#)

```
get /v3/agent-packages
```

List all agent packages (getAllPackages)

Retrieves all runtime agent packages associated with the current account.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

AgentPackageResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  }, {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Agent packages retrieved successfully [AgentPackageResponse](#)

500

Unexpected error during agent package retrieval [ApiFailureResponseV3](#)

400

Error fetching agent packages [ApiFailureResponseV3](#)

```
patch /v3/agent-packages/{agentId}
```

Update agent package (updateAgentPackage)

Updates the details of an existing runtime agent package using its unique ID.

Path parameters

agentId (required)

Path Parameter

— format: uuid

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [UpdateAgentPackageRequest](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID
format: int64

Return type

[AgentPackageResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  }, {
    "createdAt" : 0,
    "agentType" : "JAVA_ALPINE_LINUX",
    "createdBy" : "createdBy",
    "modifiedAt" : 6,
    "name" : "name",
    "description" : "description",
    "agentVersion" : "agentVersion",
    "modifiedBy" : "modifiedBy",
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "tags" : [ "tags", "tags" ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

Agent package updated successfully [AgentPackageResponse](#)

500

Unexpected error during agent package update [ApiFailureResponseV3](#)

400

Validation error during agent package update [ApiFailureResponseV3](#)

AgentVersions

```
get /v3/runtime-agent-versions
```

Retrieve agent versions (getAgentVersions)
Fetches all available agent versions from the database.

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

AgentVersionResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "version" : "version",
    "status" : "ACTIVE"
  }, {
    "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "version" : "version",
    "status" : "ACTIVE"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

500

Unexpected error during agent version retrieval [ApiFailureResponseV3](#)

200

Agent versions retrieved successfully [AgentVersionResponse](#)

Models

Methods

Table of Contents

1. [APIError](#)
2. [AddAgentPackageRequest](#)
3. [AgentPackageDto](#)
4. [AgentPackageResponse](#)
5. [AgentVersion](#)
6. [AgentVersionResponse](#)
7. [ApiFailureResponseV3](#)
8. [UpdateAgentPackageRequest](#)
9. [UpdateResourceDto](#)

APIError

status (optional)
Integer
format: int32
id (optional)
String
code (optional)
String
source (optional)
map[String, Object]
title (optional)
String
detail (optional)
String

AddAgentPackageRequest

name (optional)
String
Name of the agent package
example: Agent Package
description (optional)
String
Description of the agent package
example: Description of agent package
tags (optional)
array[Long]
Tags associated with the agent package format: int64
example: ["tag1", "tag2"]
agentType (optional)

String
Type of the agent
Enum:
JAVA_ALPINE_LINUX
JAVA_LINUX
JAVA_WINDOWS
DOTNET_CORE_ALPINE_LINUX
DOTNET_CORE_LINUX
DOTNET_CORE_WINDOWS
DOTNET_FRAMEWORK_WINDOWS
NODEJS_ALPINE_LINUX
NODEJS_LINUX
NODEJS_WINDOWS
PYTHON_ALPINE_LINUX
PYTHON_LINUX
PYTHON_WINDOWS
example: Linux_Java
agentVersion (optional)
String
Version of the agent
example: 1.0.2

AgentPackageDto

Contains the response Body
name (optional)
String
description (optional)
String
agentType (optional)
String
Enum:
JAVA_ALPINE_LINUX
JAVA_LINUX
JAVA_WINDOWS
DOTNET_CORE_ALPINE_LINUX
DOTNET_CORE_LINUX
DOTNET_CORE_WINDOWS
DOTNET_FRAMEWORK_WINDOWS
NODEJS_ALPINE_LINUX
NODEJS_LINUX
NODEJS_WINDOWS
PYTHON_ALPINE_LINUX
PYTHON_LINUX
PYTHON_WINDOWS
agentVersion (optional)
String
tags (optional)
array[String]
id (optional)
UUID
format: uuid
createdAt (optional)
Long
format: int64
createdBy (optional)
String
modifiedAt (optional)

Long
format: int64
modifiedBy (optional)
String

AgentPackageResponse

data (optional)
array[AgentPackageDto]
Contains the response Body

AgentVersion

Contains the response Body
id (optional)
UUID
format: uuid
version (optional)
String
status (optional)
String
Enum:
ACTIVE
INACTIVE

AgentVersionResponse

Response object containing agent version information
data (optional)
array[AgentVersion]
Contains the response Body

ApiFailureResponseV3

errors (optional)
array[APIError]

UpdateAgentPackageRequest

name (optional)
String
Name of the agent package
example: Agent Package
description (optional)
String
Description of the agent package
example: Description of agent package
tagActions (optional)
array[UpdateResourceDto]
List of tags to be added or removed

UpdateResourceDto

List of tags to be added or removed

action (optional)

String

Enum:

TAG

UNTAG

tags (optional)

array[Long]

format: int64

example: [12345,345221]

Imperva API2 Delivery Settings

Configure delivery options to help you optimize your content delivery and improve performance by providing faster loading of your web pages. For full feature documentation, see [Delivery Settings](#).

Version: 2.2.2

BasePath:/api/prov/v2

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

Delivery

- `delete /sites/{siteId}/settings/delivery`
- `get /sites/{siteId}/settings/delivery`
- `put /sites/{siteId}/settings/delivery`

Delivery

```
delete /sites/{siteId}/settings/delivery
```

Restore default delivery settings (`sitesSitIdSettingsDeliveryDelete`)

Restores default delivery settings for a given website according to site ID.

Path parameters

`sitId` (required)

Path Parameter

— Numeric identifier of the site to operate on

Responses

200

OK. The delivery settings restored to default

401

Unauthorized sitelid

406

Invalid Input

500

Internal server error

```
get /sites/{siteId}/settings/delivery
```

Get delivery settings (sitesSitelidSettingsDeliveryGet)

Retrieves delivery settings for a given website according to site ID.

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

Query parameters

sections (optional)

Query Parameter

— The sections of configurations to get, separated by comma. If not passed, all sections will be returned.

Return type

DeliverySettingsObject

Example data

Content-Type: application/json

```
{
  "compression" : {
    "file_compression" : true,
    "minify_js" : true,
    "minify_css" : false,
    "minify_static_html" : true,
```

```

    "compression_type" : "BROTLI"
},
"image_compression" : {
    "compress_jpeg" : true,
    "progressive_image_rendering" : true,
    "aggressive_compression" : false,
    "compress_png" : true
},
"network" : {
    "tcp_pre_pooling" : true,
    "origin_connection_reuse" : false,
    "support_non_sni_clients" : true,
    "port" : {
        "to" : "8080"
    },
    "ssl_port" : {
        "to" : "9001"
    }
},
"redirection" : {
    "redirect_naked_to_full" : false,
    "redirect_http_to_https" : true
},
"custom_error_page" : {
    "error_page_template" : "

```

\$TITLE\$

\$BODY\$

```
", "custom_error_page_templates" : { "error.type.connection_timeout" : "
```

\$TITLE\$

\$BODY\$

```
, "error.type.access_denied" : "
```

\$TITLE\$

\$BODY\$

```
" } } }
```

Produces

AcceptContent-Type

- application/json

Responses

200

DeliverySettingsObject

401

406

500

```
put /sites/{siteId}/settings/delivery
```

Update delivery settings (partial update) (sitesSitIdSettingsDeliveryPut)

Modifies delivery settings for a given website according to site ID. Only specified fields are modified.

Path parameters

sitId (required)

Path Parameter

— Numeric identifier of the site to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DeliverySettingsObject (required)

Body Parameter

— The delivery settings to use

Return type

DeliverySettingsObject

Example data

Content-Type: application/json

```
{  
  "compression" : {  
    "file_compression" : true,  
    "minify_js" : true,  
    "minify_css" : true  
  },  
  "cache" : {  
    "enable" : true,  
    "max_age" : 3600  
  },  
  "image_compression" : {  
    "enable" : true,  
    "quality" : 80  
  }  
}
```

```

    "minify_css" : false,
    "minify_static_html" : true,
    "compression_type" : "BROTLI"
},
"image_compression" : {
    "compress_jpeg" : true,
    "progressive_image_rendering" : true,
    "aggressive_compression" : false,
    "compress_png" : true
},
"network" : {
    "tcp_pre_pooling" : true,
    "origin_connection_reuse" : false,
    "support_non_sni_clients" : true,
    "port" : {
        "to" : "8080"
    },
    "ssl_port" : {
        "to" : "9001"
    }
},
"redirection" : {
    "redirect_naked_to_full" : false,
    "redirect_http_to_https" : true
},
"custom_error_page" : {
    "error_page_template" : "

```

\$TITLE\$

```

$BODY$
",
    "custom_error_page_templates" : {
        "error.type.connection_timeout" : "

```

\$TITLE\$

```

$BODY$
",
    "error.type.access_denied" : "

```

\$TITLE\$

```

$BODY$
"
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

OK. The updated rule is returned. [DeliverySettingsObject](#)

401

Unauthorized sitelid

406

Invalid Input

500

Internal server error

Models

Methods

Table of Contents

1. [DeliverySettingsObject](#)
2. [DeliverySettingsObject_compression](#)
3. [DeliverySettingsObject_custom_error_page](#)
4. [DeliverySettingsObject_custom_error_page_custom_error_page_templates](#)
5. [DeliverySettingsObject_image_compression](#)
6. [DeliverySettingsObject_network](#)
7. [DeliverySettingsObject_network_port](#)
8. [DeliverySettingsObject_network_ssl_port](#)
9. [DeliverySettingsObject_redirection](#)

[DeliverySettingsObject](#)

The overall delivery policy configuration for your website.

compression (optional)

[DeliverySettingsObject_compression](#)

image_compression (optional)

[DeliverySettingsObject_image_compression](#)

network (optional)

[DeliverySettingsObject_network](#)

redirection (optional)

[DeliverySettingsObject_redirection](#)

custom_error_page (optional)

DeliverySettingsObject_custom_error_page**DeliverySettingsObject_compression**

Compress files to shrink file size and reduce load time.

file_compression (optional)

Boolean

When this option is enabled, any textual resource such as JavaScript, CSS and HTML is compressed as it is transferred. Files are decompressed automatically within the browser. Compression options: Gzip or Brotli

compression_type (optional)

String

Gzip (default). Brotli (recommended for more efficient compression)

minify_js (optional)

Boolean

Minify JavaScript. Minification removes characters that are not necessary for rendering the page, such as whitespace and comments. This makes the files smaller and therefore reduces their access time. Minification has no impact on the functionality of the Javascript, CSS, and HTML files.

minify_css (optional)

Boolean

Content minification can applied only to cached Javascript, CSS and HTML content.

minify_static_html (optional)

Boolean

DeliverySettingsObject_custom_error_page

error_page_template (optional)

String

The default error page HTML template. \$TITLE\$ and \$BODY\$ placeholders are required.

custom_error_page_templates (optional)

DeliverySettingsObject_custom_error_page_custom_error_page_templates

DeliverySettingsObject_custom_error_page_custom_error_page_templates

Custom error pages for a specific error type. Errors with no custom pages will get the default error page template. To remove custom error configuration and return to default, send the appropriate error type with an empty template.

error.type.connection_timeout (optional)

String

The HTML template for 'Connection Timeout' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

error.type.access_denied (optional)

String

The HTML template for 'Access Denied' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

error.type.parse_req_error (optional)

String

The HTML template for 'Unable to parse request' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

error.type.parse_resp_error (optional)

String

The HTML template for 'Unable to parse response' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

error.type.connection_failed (optional)

String

The HTML template for 'Unable to connect to origin server' error. \$TITLE\$ and \$BODY\$ placeholders are

required. Set empty value to return to default.

`error.type.ssl_failed` (optional)

`String`

The HTML template for 'Unable to establish SSL connection' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

`error.type.deny_and_captcha` (optional)

`String`

The HTML template for 'Initial connection denied - CAPTCHA required' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

`error.type.no_ssl_config` (optional)

`String`

The HTML template for 'Site not configured for SSL' error. \$TITLE\$ and \$BODY\$ placeholders are required. Set empty value to return to default.

`error.type.abp_identification_failed` (optional)

`String`

The HTML template for 'ABP identification failed' error. Placeholders are not supported. HTML Template must contain only tags located inside the body. Set empty value to return to default.

DeliverySettingsObject_image_compression

Image compression can be applied only to cached JPEG and PNG images. As such, this option is disabled when caching is disabled.

`compress_jpeg` (optional)

`Boolean`

Compress JPEG images. Compression reduces download time by reducing the file size.

`progressive_image_rendering` (optional)

`Boolean`

The image is rendered with progressively finer resolution, potentially causing a pixelated effect until the final image is rendered with no loss of quality. This option reduces page load times and allows images to gradually load after the page is rendered.

`aggressive_compression` (optional)

`Boolean`

A more aggressive method of compression is applied with the goal of minimizing the image file size, possibly impacting the final quality of the image displayed. Applies to JPEG compression only.

`compress_png` (optional)

`Boolean`

Compress PNG images. Compression reduces download time by reducing the file size. PNG compression removes only image meta-data with no impact on quality.

DeliverySettingsObject_network

`tcp_pre_pooling` (optional)

`Boolean`

Maintain a set of idle TCP connections to the origin server to eliminate the latency associated with opening new connections or new requests (TCP handshake).

`origin_connection_reuse` (optional)

`Boolean`

TCP connections that are opened for a client request remain open for a short time to handle additional requests that may arrive.

`support_non_sni_clients` (optional)

`Boolean`

By default, non-SNI clients are supported. Disable this option to block non-SNI clients.

`enable_http2` (optional)

`Boolean`

Allows supporting browsers to take advantage of the performance enhancements provided by HTTP/2 for your website. Non-supporting browsers can connect via HTTP/1.0 or HTTP/1.1.

`http2_to_origin` (optional)

Boolean

Enables HTTP/2 for the connection between Imperva and your origin server. (HTTP/2 must also be supported by the origin server.)

port (optional)

DeliverySettingsObject_network_port

ssl_port (optional)

DeliverySettingsObject_network_ssl_port**DeliverySettingsObject_network_port**

To redirect incoming requests, rewrite the port number used to access the origin.

to (optional)

String

The port number. If field is set to 80 (the default value), rewrite port will be removed.

from (optional)

String

Read only field. Indicate the source port number for the non-SSL port.

DeliverySettingsObject_network_ssl_port

To redirect incoming requests, rewrite the SSL port number used to access the origin.

to (optional)

String

The port number to rewrite default SSL port to. if field is set to 443 (the default value), rewrite SSL port will be removed.

from (optional)

String

Read only field. Indicate the source port number for the SSL port.

DeliverySettingsObject_redirection

redirect_naked_to_full (optional)

Boolean

Redirect all visitors to your site's full domain (which includes www). This option is displayed only for a naked domain.

redirect_http_to_https (optional)

Boolean

Sites that require an HTTPS connection force all HTTP requests to be redirected to HTTPS. This option is displayed only for an SSL site.

Imperva API2 Cache Settings

Define content caching policies and caching rules for your websites. For full feature documentation, see [Cache Settings](#).

Version: 2.2.2

BasePath:/api/prov/v2

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

CacheRules

- `get /sites/{siteId}/settings/cache/rules`
- `post /sites/{siteId}/settings/cache/rules`
- `delete /sites/{siteId}/settings/cache/rules/{ruleId}`
- `get /sites/{siteId}/settings/cache/rules/{ruleId}`
- `put /sites/{siteId}/settings/cache/rules/{ruleId}`

GeneralCacheSettings

- `delete /sites/{siteId}/cache`
- `get /sites/{siteId}/cache/xray`
- `delete /sites/{siteId}/settings/cache`
- `get /sites/{siteId}/settings/cache`
- `put /sites/{siteId}/settings/cache`

CacheRules

```
get /sites/{siteId}/settings/cache/rules
```

List all cache rules for specific site (`sitesSitelIdSettingsCacheRulesGet`)
 List all cache rules for specific site

Path parameters

`sitelid` (required)
 Path Parameter
 — Numeric identifier of the site to operate on

Return type

`CacheRule`

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
```

```

    "action" : "HTTP_CACHE_FORCE_UNCACHEABLE",
    "enabled" : true,
    "filter" : "isMobile == Yes",
    "ttl" : 3600
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. All site cache rules are returned. [CacheRule](#)

401

Unauthorized sitelid

404

Resource not found

```
post /sites/{siteId}/settings/cache/rules
```

Create cache rules ([sitesSitelidSettingsCacheRulesPost](#))
Create custom cache rules to override general cache settings.

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CacheRule](#) (required)

Body Parameter

— The rule to create.

Responses

200

OK. The created cache rule id is returned.

401

Unauthorized sitelid

404

Resource not found

406

Invalid Input

500

Internal server error

```
delete /sites/{siteId}/settings/cache/rules/{ruleId}
```

Delete cache rule (sitesSitelidSettingsCacheRulesRuleIdDelete)
Deletes a given cache rule according to the rule ID.

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

ruleId (required)

Path Parameter

— Numeric identifier of the rule to operate on

Responses

200

OK.

401

Unauthorized sitelid

400

Resource not found

405

Rule can not be deleted

406

Invalid Input

```
get /sites/{siteId}/settings/cache/rules/{ruleId}
```

Retrieve cache rule details (sitesSiteldSettingsCacheRulesRuleIdGet)
Retrieves details of a given cache rule according to the rule ID.

Path parameters

siteId (required)

Path Parameter

— Numeric identifier of the site to operate on

ruleId (required)

Path Parameter

— Numeric identifier of the rule to operate on

Return type

CacheRule

Example data

Content-Type: application/json

```
{
  "name" : "rule name",
  "action" : "HTTP_CACHE_FORCE_UNCACHEABLE",
  "enabled" : true,
  "filter" : "isMobile == Yes",
  "ttl" : 3600
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The requested rule is returned. CacheRule

401

Unauthorized sitelId

404

Resource not found

406

Invalid Input

```
put /sites/{siteId}/settings/cache/rules/{ruleId}
```

Update cache rule (partial update) (sitesSitelIdSettingsCacheRulesRuleIdPut)

Updates a given cache rule according to the rule ID. Only specified fields are modified.

Path parameters

sitelId (required)

Path Parameter

— Numeric identifier of the site to operate on

ruleId (required)

Path Parameter

— Numeric identifier of the rule to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body CacheRule (required)

Body Parameter

— The rule to update

Responses

200

OK.

401

Unauthorized sitelD

404

Resource not found

406

Invalid input

500

Internal server error

GeneralCacheSettings

```
delete /sites/{siteId}/cache
```

Purge a site's cache (sitesSitelDCacheDelete)

Path parameters

sitelD (required)

Path Parameter

— Numeric identifier of the site to operate on

Query parameters

url_pattern (optional)

Query Parameter

— The url pattern of the resource to be purged from the cache. For example:
(1) Resource_name - resources that contain Resource_name will be purged,
(2) ^Resource_name - resources that start with Resource_name will be purged,
(3) Resource_name\$ - resources that end with Resource_name will be purged

tags (optional)

Query Parameter

— A comma separated list of tag names to be purged

Responses

200

OK

401

Unauthorized sitelid

406

Invalid Input

500

Internal server error

```
get /sites/{siteId}/cache/xray
```

Refresh and get a site's XRAY access URL. (sitesSitelIdCacheXrayGet)

Retrieves the XRAY Access URL which enables you to view specialized response headers for a single browser session.

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

Return type

String

Example data

Content-Type: application/json

```
"http://example.com/_Incapsula_Resource?SW_XRAY="
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The site's XRAY access URL is returned. String

401

Unauthorized sitelD

406

Invalid Input

500

Internal server error

```
delete /sites/{siteId}/settings/cache
```

Restore default cache settings (sitesSitelDSettingsCacheDelete)
Restore default cache settings

Path parameters

sitelD (required)

Path Parameter

— Numeric identifier of the site to operate on

Responses

200

OK. The cache settings restored to default

401

Unauthorized sitelD

406

Invalid Input

500

Internal server error

```
get /sites/{siteId}/settings/cache
```

Get cache settings (sitesSitelDSettingsCacheGet)
Retrieves cache settings for a given website according to site ID.

Path parameters

`siteld` (required)

Path Parameter

— Numeric identifier of the site to operate on

Query parameters

`sections` (optional)

Query Parameter

— The sections of configurations to get, separated by comma. If not passed, all sections will be returned.

Return type

`CacheSettingsObject`

Example data

Content-Type: application/json

```
{
  "mode" : {
    "level" : "standard",
    "https" : "include_html",
    "time" : 360
  },
  "key" : {
    "unite_naked_full_cache" : true,
    "comply_vary" : false
  },
  "response" : {
    "stale_content" : {
      "mode" : "adaptive"
    },
    "cache_shield" : true,
    "cache_response_header" : {
      "mode" : "custom",
      "headers" : [ "Access-Control-Allow-Origin", "Access-Control-Allow-Methods" ]
    },
    "tag_response_header" : "Some-Header-Name",
    "cache_empty_responses" : true,
    "cache_300x" : true,
    "cache_http_10_responses" : false
  },
  "ttl" : {
    "use_shortest_caching" : true,
    "prefer_last_modified" : false
  },
  "client_side" : {
    "enable_client_side_caching" : true,
    "comply_no_cache" : false,
    "send_age_header" : false
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. An array of cache settings is returned. [CacheSettingsObject](#)

401

Unauthorized sitelid

406

Invalid Input

500

Internal server error

```
put /sites/{siteId}/settings/cache
```

Change cache settings (partial update) ([sitesSitelidSettingsCachePut](#))

Modifies cache settings for a given website according to site ID. Only specified fields are modified.

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [CacheSettingsObject](#) (required)

Body Parameter

— The cache settings to use

Request headers

Return type

CacheSettingsObject

Example data

Content-Type: application/json

```
{
  "mode" : {
    "level" : "standard",
    "https" : "include_html",
    "time" : 360
  },
  "key" : {
    "unite_naked_full_cache" : true,
    "comply_vary" : false
  },
  "response" : {
    "stale_content" : {
      "mode" : "adaptive"
    },
    "cache_shield" : true,
    "cache_response_header" : {
      "mode" : "custom",
      "headers" : [ "Access-Control-Allow-Origin", "Access-Control-Allow-Methods"
    ]
  },
  "tag_response_header" : "Some-Header-Name",
  "cache_empty_responses" : true,
  "cache_300x" : true,
  "cache_http_10_responses" : false
},
  "ttl" : {
    "use_shortest_caching" : true,
    "prefer_last_modified" : false
  },
  "client_side" : {
    "enable_client_side_caching" : true,
    "comply_no_cache" : false,
    "send_age_header" : false
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The cache settings that were updated are returned. [CacheSettingsObject](#)

401

Unauthorized siteld

406

Invalid Input

500

Internal server error

Models

Methods

Table of Contents

1. [CacheRule](#)
2. [CacheSettingsObject](#)
3. [CacheSettingsObject_client_side](#)
4. [CacheSettingsObject_key](#)
5. [CacheSettingsObject_mode](#)
6. [CacheSettingsObject_response](#)
7. [CacheSettingsObject_response_cache_404](#)
8. [CacheSettingsObject_response_cache_response_header](#)
9. [CacheSettingsObject_response_stale_content](#)
10. [CacheSettingsObject_ttl](#)

CacheRule

rule_id (optional)

Integer

Rule id

name

String

Rule name

action

String

Define the action you want to take for every request that matches the rule.
 * HTTP_CACHE_MAKE_STATIC - Cache Resource. Always cache the resource.
 * HTTP_CACHE_CLIENT_CACHE_CTL - Cache Resource on Client. Cache the resource on the client.
 * HTTP_CACHE_FORCE_UNCACHEABLE - Don't Cache

Resource. Never cache the resource.
 * HTTP_CACHE_ADD_TAG - Create Tag. Tag the resources that match the rule conditions. This enables you to subsequently purge those resources according to the tag name.
 * HTTP_CACHE_ENABLE_ASYNC_VALIDATION - When Imperva can't connect to the origin server, serve stale content instead of displaying an error to end users. * HTTP_CACHE_DIFFERENTIATE_SSL - Differentiate Cache Key by HTTP/HTTPS Scheme. A resource is cached separately depending on whether it is accessed over HTTP or HTTPS.
 * HTTP_CACHE_DIFFERENTIATE_BY_HEADER - Differentiate Cache Key by Header.
 * HTTP_CACHE_DIFFERENTIATE_BY_COOKIE - Differentiate Cache Key by Cookie.
 * HTTP_CACHE_DIFFERENTIATE_BY_GEO - Differentiate Cache Key by Geolocation. Resources are cached separately based on geolocation of the request.
 * HTTP_CACHE_IGNORE_PARAMS - Ignore Parameters in Cache Key. If the parameters do not affect which resource is returned, you can choose to ignore them.
 * HTTP_CACHE_ENRICH_CACHE_KEY - Enrich Cache Key. Add text to the cache key as a suffix.
 * HTTP_CACHE_FORCE_VALIDATION - Force User Authentication. When this option is selected, credentials must be validated with the origin to confirm that the request comes from an authorized client.
 * HTTP_CACHE_IGNORE_AUTH_HEADER - Cache Authenticated Resources. Selecting this option returns cached content if available without authenticating the client.

Enum:

HTTP_CACHE_MAKE_STATIC
 HTTP_CACHE_CLIENT_CACHE_CTL
 HTTP_CACHE_FORCE_UNCACHEABLE
 HTTP_CACHE_ADD_TAG
 HTTP_CACHE_ENABLE_ASYNC_VALIDATION
 HTTP_CACHE_DIFFERENTIATE_SSL
 HTTP_CACHE_DIFFERENTIATE_BY_HEADER
 HTTP_CACHE_DIFFERENTIATE_BY_COOKIE
 HTTP_CACHE_DIFFERENTIATE_BY_GEO
 HTTP_CACHE_IGNORE_PARAMS
 HTTP_CACHE_ENRICH_CACHE_KEY
 HTTP_CACHE_FORCE_VALIDATION
 HTTP_CACHE_IGNORE_AUTH_HEADER

enabled

Boolean

'true' if the rule is enabled.

filter

String

The filter defines the conditions that trigger the rule action, if left empty, the rule is always run.

ttl (optional)

Integer

TTL in seconds. Relevant for HTTP_CACHE_MAKE_STATIC and HTTP_CACHE_CLIENT_CACHE_CTL actions.

ignored_params (optional)

array[String]

Parameters to ignore. Relevant for HTTP_CACHE_IGNORE_PARAMS action. An array containing '*' means all parameters are ignored.

text (optional)

String

Tag name if action is HTTP_CACHE_ADD_TAG action, text to be added to the cache key as suffix if action is HTTP_CACHE_ENRICH_CACHE_KEY.

disabled_by_cache_mode (optional)

Boolean

true if cache mode is 'No Caching'.

differentiate_by_value (optional)

String

Value to differentiate resources by. Relevant for HTTP_CACHE_DIFFERENTIATE_BY_HEADER, HTTP_CACHE_DIFFERENTIATE_BY_COOKIE and HTTP_CACHE_DIFFERENTIATE_BY_GEO actions

CacheSettingsObject

The overall caching policy configuration for your website.

mode (optional)

CacheSettingsObject_mode
key (optional)
CacheSettingsObject_key
response (optional)
CacheSettingsObject_response
ttl (optional)
CacheSettingsObject_ttl
client_side (optional)
CacheSettingsObject_client_side

CacheSettingsObject_client_side

enable_client_side_caching (optional)
Boolean
Cache content on client browsers or applications. When not enabled, content is cached only on the Imperva proxies.
comply_no_cache (optional)
Boolean
Comply with No-Cache and Max-Age directives in client requests. By default, these cache directives are ignored. Resources are dynamically profiled and re-configured to optimize performance.
send_age_header (optional)
Boolean
Send Cache-Control: max-age and Age headers.

CacheSettingsObject_key

unite_naked_full_cache (optional)
Boolean
Use the Same Cache for Full and Naked Domains. For example, use the same cached resource for www.example.com/a and example.com/a.
comply_vary (optional)
Boolean
Comply with Vary. Cache resources in accordance with the Vary response header.

CacheSettingsObject_mode

level
String
Caching level.
 * disabled - Turn off site caching entirely, including user-defined custom cache rules.
 * custom_cache_rules_only - Disable caching, unless specified otherwise by a custom cache rule.
 * standard - Cache according to standard HTTP headers.
 * smart - Cache according to standard HTTP headers as well as profile dynamic pages to identify and cache static content that was not marked as static.
 In addition to content that was marked by the site's developer / web server as static using standard HTTP headers, Imperva also profiles other resources to identify and cache static content that was not marked as such.
 * all_resources - Cache every resource on the web server for the specified amount of time.
 All site content is cached.
Enum:
disabled
custom_cache_rules_only
standard
smart
all_resources
https (optional)
String
The resources that are cached over HTTPS, the general level applies.
 * disabled - No resources are cached over HTTPS.
 * dont_include_html - Only images, css files, js files, and resources defined with the 'Cache-

Control: public' header may be cached over HTTPS.
 * include_html - Same as dont_include_html, also HTML files may be cached over HTTPS.
 * include_all_resources - All resources may be cached over HTTPS.

Enum:

disabled
dont_include_html
include_html
include_all_resources
time (optional)

Integer

The time, in seconds, that you set for this option determines how often the cache is refreshed. Relevant for the 'include_html' and 'include_all_resources' levels only

CacheSettingsObject_response

stale_content (optional)

CacheSettingsObject_response_stale_content

cache_shield (optional)

Boolean

Adds an intermediate cache between other Imperva PoPs and your origin servers to protect your servers from redundant requests.

cache_response_header (optional)

CacheSettingsObject_response_cache_response_header

tag_response_header (optional)

String

Tag the response according to the value of this header. Specify which origin response header contains the cache tags in your resources.

cache_empty_responses (optional)

Boolean

Cache responses that don't have a message body.

cache_300x (optional)

Boolean

When this option is checked Imperva will cache 301, 302, 303, 307, and 308 redirect response headers containing the target URI.

cache_http_10_responses (optional)

Boolean

Cache HTTP 1.0 type responses that don't include the Content-Length header or chunking.

cache_404 (optional)

CacheSettingsObject_response_cache_404

CacheSettingsObject_response_cache_404

enabled

Boolean

time (optional)

Integer

CacheSettingsObject_response_cache_response_header

mode

String

The working mode for caching response headers.
 * all - Cache all headers in responses.
 * custom - Specify which response headers should be cached along with the resource.

Enum:

disabled

all

custom
headers (optional)
array[String]

An array of strings representing the response headers to be cached when working in 'custom' mode. If empty, no response headers are cached.
 For example: [Access-Control-Allow-Origin, Access-Control-Allow-Methods].

CacheSettingsObject_response_stale_content

Serve stale content. When Imperva can't connect to the origin server, serve stale content instead of displaying an error to end users.

mode

String

The working mode for serving stale content.
 * disabled - Disable serving of stale content.
 * adaptive - Stale content is served for a duration of 2 to 24 hours based on the time passed since the resource was last updated.
 * custom - Serve stale content for the specified amount of time.

Enum:

disabled

adaptive

custom

time (optional)

Integer

The time, in seconds, to serve stale content for when working in 'custom' work mode

CacheSettingsObject_ttl

use_shortest_caching (optional)

Boolean

Use shortest caching duration in case of conflicts. By default, the longest duration is used in case of conflict between caching rules or modes. When this option is checked, Imperva uses the shortest duration in case of conflict.

prefer_last_modified (optional)

Boolean

Prefer 'Last Modified' over eTag. When this option is checked, Imperva prefers using Last Modified values (if available) over eTag values (recommended on multi-server setups).

Imperva API2 Load Balancing Settings

Configure load balancing and failover settings for your websites. For full feature documentation, see [Load Balancing Settings](#).

Version: 2.2.2

BasePath:/api/prov/v2

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

LoadBalancing

- `post /sites/{siteId}/dataCenters/resume`
- `post /sites/{siteId}/settings/origin/datacenters/{dcId}/servers`
- `post /sites/{siteId}/settings/origin/datacenters`

LoadBalancing

```
post /sites/{siteId}/dataCenters/resume
```

Resume Traffic to Active DCs (`sitesSiteldDataCentersResumePost`)

Use this operation to resume traffic to your active data centers. When at least one active data center is back up, you have to manually reroute your traffic back to the active data center. Traffic does not revert automatically to your active data centers.

Path parameters

`siteld` (required)

Path Parameter

— Numeric identifier of the site to operate on

Responses

200

OK. The traffic resumed to active DC's

401

Unauthorized `siteld`

404

Resource not found

```
post /sites/{siteId}/settings/origin/datacenters/{dcId}/servers
```

Edit servers (`sitesSiteldSettingsOriginDatacentersDcIdServersPost`)

Edit servers

Path parameters

`siteld` (required)

Path Parameter

— Numeric identifier of the site to operate on

dcId (required)

Path Parameter

— Numeric identifier of the data center to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body **Servers** (required)

Body Parameter

— Array of servers to edit.

Return type

Servers

Example data

Content-Type: application/json

```
{  
  "servers" : [ {  
    "serverId" : "1035103",  
    "serverAddress" : "90.5.5.6",  
    "isEnabled" : true,  
    "isStandby" : true,  
    "weight" : 60  
  }, {  
    "serverId" : "1035103",  
    "serverAddress" : "90.5.5.6",  
    "isEnabled" : true,  
    "isStandby" : true,  
    "weight" : 60  
  } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The updated server configuration is returned. [Servers](#)

401

Unauthorized sitelid

406

Invalid Input

500

Internal server error

```
post /sites/{siteId}/settings/origin/datacenters
```

Edit data centers (`sitesSitelidSettingsOriginDatacentersPost`)

Edit data centers

Path parameters

sitelid (required)

Path Parameter

— Numeric identifier of the site to operate on

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DCs (required)

Body Parameter

— Array of data centers to edit.

Return type

DCs

Example data

Content-Type: application/json

```
{
  "DCs" : [ {
    "dcId" : "484378",
    "isEnabled" : true,
    "isStandby" : false,
    "isContent" : false,
    "weight" : 25
  }, {
    "dcId" : "484378",
    "isEnabled" : true,
    "isStandby" : false,
    "isContent" : false,
    "weight" : 25
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK. The updated data center configuration is returned. DCs

Models

Methods

Table of Contents

1. DCs
2. DataCenter
3. Server
4. Servers

DCs

DCs (optional)
array[DataCenter]

DataCenter

dcId
Integer
Numeric identifier of the data center to operate on

isEnabled (optional)

Boolean

When set to true, the specified data center is enabled.

isStandby (optional)

Boolean

When set to true, the specified data center is defined as standby.

isContent (optional)

Boolean

When set to true, the data center is used only for requests according to a user-defined forwarding delivery rule.

Note: There must be at least one data center that is not configured for forward rules.

weight (optional)

Integer

Percentage of traffic to be served by the data center. To change a data center from active to standby, or to disable a data center, you must first reset its weight to zero.

Server

serverId

Integer

Numeric identifier of the server to operate on

serverAddress (optional)

String

Server address. Either IP or CNAME.

isEnabled (optional)

Boolean

When set to true, the specified server is enabled.

isStandby (optional)

Boolean

When set to true, the specified server is defined as standby.

weight (optional)

Integer

Percentage of traffic to be served by the server. To disable a server, you must first reset its weight to zero.

Servers

servers (optional)

array[Server]

Load Balancing Monitoring Settings API Definition

Configure settings to determine when origin servers should be considered “up” or “down” (active or inactive) by the Imperva Load Balancer. Select which failure scenarios you want to produce alarm messages, and how to send them. For full feature documentation, see [Load Balancing Monitoring Settings](#)

Version: 1.0.0

BasePath:/appdlv-site-settings

Imperva License Agreement.

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true
3. APIKey KeyParamName:caid KeyInQuery:true KeyInHeader:false

Methods

Models

Table of Contents

SiteMonitoringSettings

- `put /v2/site/{siteId}/monitoring`
- `post /v2/site/{siteId}/monitoring`
- `get /v2/site/{siteId}/monitoring`

SiteMonitoringSettings

```
put /v2/site/{siteId}/monitoring
```

Overwrite website monitoring settings (full update) (`editSiteMonitoringFullUpdate`)
Fully update site monitoring settings, if one of the fields are null will be updated to its default

Path parameters

`siteld` (required)

Path Parameter

— The unique ID for the website, assigned by Imperva format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/json`

Request body

body `SiteMonitoringModel` (required)

Body Parameter

—

Query parameters

Return type

`SiteMonitoringSuccessResponse`

Example data

Content-Type: `application/json`

```
{
  "data" : [ {
    "monitoringParameters" : {
      "failedRequestsDuration" : 30,
      "failedRequestsDurationUnits" : "SECONDS",
      "failedRequestsMinNumber" : 30,
      "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
      "upChecksInterval" : 6,
      "upChecksIntervalUnits" : "SECONDS",
      "upCheckRetries" : 30,
      "useVerificationForDown" : false,
      "monitoringUrl" : "/health",
      "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
      "requiredMonitors" : "MANY",
      "alarmOnServerFailover" : true,
      "alarmOnStandsByFailover" : false,
      "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
      "httpRequestTimeoutUnits" : "SECONDS",
      "httpRequestTimeout" : 0,
      "httpResponseError" : "501-510,530"
    }
  }, {
    "monitoringParameters" : {
      "failedRequestsDuration" : 30,
      "failedRequestsDurationUnits" : "SECONDS",
      "failedRequestsMinNumber" : 30,
      "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
      "upChecksInterval" : 6,
      "upChecksIntervalUnits" : "SECONDS",
      "upCheckRetries" : 30,
      "useVerificationForDown" : false,
      "monitoringUrl" : "/health",
      "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
      "requiredMonitors" : "MANY",
      "alarmOnServerFailover" : true,
      "alarmOnStandsByFailover" : false,
      "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
      "httpRequestTimeoutUnits" : "SECONDS",
      "httpRequestTimeout" : 0,
      "httpResponseError" : "501-510,530"
    }
  } ]
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully updated site monitoring settings [SiteMonitoringSuccessResponse](#)

400

Bad Request

500

Internal Server Error

```
post /v2/site/{siteId}/monitoring
```

Modify website monitoring settings (partial update) ([editSiteMonitoringPartiallyUpdate](#))
Updates only provided fields

Path parameters

siteId (required)

Path Parameter

— The unique ID for the website, assigned by Imperva format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [SiteMonitoringModel](#) (required)

Body Parameter

Query parameters

Return type

[SiteMonitoringSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "monitoringParameters" : {
      "failedRequestsDuration" : 30,
      "failedRequestsDurationUnits" : "SECONDS",
      "failedRequestsMinNumber" : 30,
      "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
      "upChecksInterval" : 6,
      "upChecksIntervalUnits" : "SECONDS",
      "upCheckRetries" : 30,
      "useVerificationForDown" : false,
      "monitoringUrl" : "/health",
      "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
      "requiredMonitors" : "MANY",
      "alarmOnServerFailover" : true,
      "alarmOnStandsByFailover" : false,
      "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
      "httpRequestTimeoutUnits" : "SECONDS",
      "httpRequestTimeout" : 0,
      "httpResponseError" : "501-510,530"
    }
  }, {
    "monitoringParameters" : {
      "failedRequestsDuration" : 30,
      "failedRequestsDurationUnits" : "SECONDS",
      "failedRequestsMinNumber" : 30,
      "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
      "upChecksInterval" : 6,
      "upChecksIntervalUnits" : "SECONDS",
      "upCheckRetries" : 30,
      "useVerificationForDown" : false,
      "monitoringUrl" : "/health",
      "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
      "requiredMonitors" : "MANY",
      "alarmOnServerFailover" : true,
      "alarmOnStandsByFailover" : false,
      "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
      "httpRequestTimeoutUnits" : "SECONDS",
      "httpRequestTimeout" : 0,
      "httpResponseError" : "501-510,530"
    }
  } ]
}
```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully updated site monitoring settings [SiteMonitoringSuccessResponse](#)

400

Bad Request

500

Internal Server Error

```
get /v2/site/{siteId}/monitoring
```

Retrieve website monitoring settings for a given website ([getSiteMonitoring](#))

Path parameters

`siteId` (required)

Path Parameter

— The unique ID for the website, assigned by Imperva format: int64

Query parameters

Return type

[SiteMonitoringSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "monitoringParameters" : {
      "failedRequestsDuration" : 30,
```

```

        "failedRequestsDurationUnits" : "SECONDS",
        "failedRequestsMinNumber" : 30,
        "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
        "upChecksInterval" : 6,
        "upChecksIntervalUnits" : "SECONDS",
        "upCheckRetries" : 30,
        "useVerificationForDown" : false,
        "monitoringUrl" : "/health",
        "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
        "requiredMonitors" : "MANY",
        "alarmOnServerFailover" : true,
        "alarmOnStandsByFailover" : false,
        "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
        "httpRequestTimeoutUnits" : "SECONDS",
        "httpRequestTimeout" : 0,
        "httpResponseError" : "501-510,530"
    }
},
{
    "monitoringParameters" : {
        "failedRequestsDuration" : 30,
        "failedRequestsDurationUnits" : "SECONDS",
        "failedRequestsMinNumber" : 30,
        "failedRequestsPercentage" : 30
    },
    "upDownVerification" : {
        "upChecksInterval" : 6,
        "upChecksIntervalUnits" : "SECONDS",
        "upCheckRetries" : 30,
        "useVerificationForDown" : false,
        "monitoringUrl" : "/health",
        "expectedReceivedString" : "Am Alive"
    },
    "notifications" : {
        "requiredMonitors" : "MANY",
        "alarmOnServerFailover" : true,
        "alarmOnStandsByFailover" : false,
        "alarmOnDcFailover" : false
    },
    "failedRequestCriteria" : {
        "httpRequestTimeoutUnits" : "SECONDS",
        "httpRequestTimeout" : 0,
        "httpResponseError" : "501-510,530"
    }
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

Successfully updated site monitoring settings [SiteMonitoringSuccessResponse](#)

400

Bad Request

500

Internal Server Error

Models

Methods

Table of Contents

1. FailedRequestCriteria
2. MonitoringParameters
3. Notifications
4. SiteMonitoringModel
5. SiteMonitoringSuccessResponse
6. UpDownVerification

FailedRequestCriteria

httpRequestTimeout (optional)

Integer

The maximum time to wait for an HTTP response. 1-200 SECONDS or 1-3 MINUTES format: int32

httpRequestTimeoutUnits (optional)

String

Time unit

Enum:

SECONDS

MINUTES

httpResponseError (optional)

String

The HTTP response error codes or patterns that will be counted as request failures

example: 501-510,530

MonitoringParameters

failedRequestsPercentage (optional)

Integer

The percentage of failed requests to the origin server format: int32

example: 30

failedRequestsMinNumber (optional)

Integer

The minimum number of failed requests to be considered as failure format: int32

example: 30

failedRequestsDuration (optional)

Integer

The minimum duration of failures above the threshold to consider server as down. 20-180 SECONDS or 1-2

MINUTES format: int32

example: 30

failedRequestsDurationUnits (optional)

String

Time unit

Enum:

SECONDS

MINUTES

Notifications

alarmOnStandsByFailover (optional)

Boolean

Indicates whether or not an email will be sent upon failover. This parameter is relevant only for a multiple data center configuration that includes a standby data center.

example: false

alarmOnDcFailover (optional)

Boolean

Indicates whether or not an email will be sent upon data center failover. This parameter is relevant only for a multiple data center configuration.

example: false

alarmOnServerFailover (optional)

Boolean

Indicates whether or not an email will be sent upon server failover.

example: true

requiredMonitors (optional)

String

Monitors required to report server / data center as down

Enum:

ONE

MANY

MOST

ALL

example: MANY

SiteMonitoringModel

monitoringParameters (optional)

MonitoringParameters

failedRequestCriteria (optional)

FailedRequestCriteria

upDownVerification (optional)

UpDownVerification

notifications (optional)

Notifications

SiteMonitoringSuccessResponse

data (optional)
array[SiteMonitoringModel]

UpDownVerification

useVerificationForDown (optional)

Boolean

If Imperva determines that an origin server is down according to failed request criteria, it will initiate another request to verify that the origin server is down

example: false

monitoringUrl (optional)

String

The URL to use for monitoring your website.

example: /health

expectedReceivedString (optional)

String

The expected string. If left empty, any response, except for the codes defined in the HTTP response error codes to be treated as Down parameter, will be considered successful. If the value is non-empty, then the defined value must appear within the response string for the response to be considered successful.

example: Am Alive

upChecksInterval (optional)

Integer

After an origin server was identified as down, Imperva will periodically test it to see whether it has recovered, according to the frequency defined in this parameter. 10-120 SECONDS or 1-2 MINUTES format: int32

upChecksIntervalUnits (optional)

String

Time unit

Enum:

SECONDS

MINUTES

upCheckRetries (optional)

Integer

Every time an origin server is tested to see whether it's back up, the test will be retried this number of times.

format: int32

example: 30

Website Performance Statistics API Overview

Retrieve website performance statistics using the Imperva API and integrate them with your preferred SIEM or observability tools.

Overview

Using the API, you can retrieve performance statistics for all websites in your account or filter them by specific metrics for individual websites or for all websites. You can then display these statistics in your SIEM or observability tool. This integration enables proactive monitoring and deeper insights into the performance of your websites.

For details on the performance statistics API, see [Website Performance Statistics API Definition](#).

Update cadence: Statistics refresh every minute. The API retrieves data for the last reliable minute, defined as the minute that ended five minutes ago.

Retry mechanism: We recommend implementing a retry mechanism to handle temporary failures or missing data. Excessive retries may trigger rate limits imposed to maintain system stability.

Empty responses: Empty API responses indicate that no activity occurred in a given minute, so no metrics are reported. Errors will be included in the response as actual error messages.

Available statistics

The API provides these performance statistics for monitoring trends and detecting issues:

Section	Description
PoP latency	The total time (in milliseconds) for a request to be processed from the moment the Imperva proxy selects an origin server (before opening a connection to the origin) until the full response is sent back to the proxy. Redirect requests are excluded from average latency time statistics since there is no origin server response.
Origin server response time	The time (in milliseconds) measured from when the Imperva proxy server in the PoP sends a request to an origin server until the response headers are received by the proxy. Redirect requests are excluded from average response time statistics since there is no origin server response.
Error response count for each error type	The number of requests that resulted in a specific error type.

Sample integration - Splunk

The API integrates seamlessly with observability tools like Splunk to enhance your monitoring and analytics capabilities. You can use the API independently for custom monitoring and data analysis based on your requirements. The Splunk integration is one example of how this can be accomplished. By configuring Splunk to ingest performance statistics data, you can enable real-time visualization and alerting for key metrics, improving your visibility of website performance trends and potential issues.

A sample Python script demonstrating how to retrieve, process, and forward API data to Splunk, along with installation and configuration instructions, is available in [GitHub](#) and managed by the open source community.

Application Performance Statistics API

Retrieve application performance data per account or site.

For full feature documentation, see [Web Performance Dashboard](#).

Version: 1.0

BasePath:/appdlv-dashboards-ui

Imperva License Agreement

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

ApplicationPerformanceStatisticsV3

- `get /v3/performance/statistics`

ApplicationPerformanceStatisticsV3

```
get /v3/performance/statistics
```

Retrieve selected application performance statistics for account (getStats)

This API retrieves application performance statistics for the last reliable minute, defined as the minute that ended 5 minutes ago.

Supported metric types are: popLatency, originResponseTime, errorResponseTypes.

popLatency: The total time (in milliseconds) for a request to be processed from the moment the Imperva proxy selects an origin server (before opening a connection to the origin) until the full response is sent back to the proxy. Redirect requests are excluded from average latency time statistics since there is no origin server response.

originResponseTime: The time (in milliseconds) measured from when the Imperva proxy server in the PoP sends a request to an origin server until the response headers are received by the proxy. Redirect requests are excluded from average response time statistics since there is no origin server response.

errorResponseTypes: The number of requests that resulted in a specific error type.

Specify website IDs to retrieve statistics for specific sites in the account. If omitted, statistics are generated for all sites in the account.

Specify metric types to retrieve specific metrics. If omitted, statistics are generated for all currently supported types.

Query parameters

`caid` (optional)

Query Parameter

— The Imperva ID of the account or subaccount. By default, the account ID is the ID associated with the API credentials used for authentication. To run an API on a sub account, specify the sub account ID. format: int64

`sitelds` (optional)

Query Parameter

— Comma separated list of unique Imperva website IDs for up to 10 sites. If omitted, statistics for all sites in the account are returned.

`metrics` (optional)

Query Parameter

— Comma separated list of metric types. If omitted, all supported metrics are returned. Supported metric types are: popLatency, originResponseTime, errorResponseTypes.

Return type

StatisticsApiSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {"timestamp": 1730122740000, "accountId": 11111, "sitesStatistics": [{"siteId": 22, "siteName": "example.website.com", "statistics": {"popLatency": [{"region": "us-east", "valuePerRegion": 123, "pops": [{"pop": "atl", "valuePerPop": 123}]}], {"region": "apac", "valuePerRegion": 345, "pops": [{"pop": "mel", "valuePerPop": 345}]}}}, {"originResponseTime": [{"origin": "1.1.1.1", "valuePerOrigin": 123}, {"origin": "my.url-address.com", "valuePerOrigin": 345}], "errorResponseTypes": {"REQ_BAD_TIMEOUT": 3, "REQ_SSL_NOT_SUPPORTED": 1, "REQ_IPV6_NOT_SUPPORTED": 4, "REQ_BAD_PARSE_ERROR": 2}], {"timestamp": 1730122740000, "accountId": 11111, "sitesStatistics": [{"siteId": 22, "siteName": "example.website.com", "statistics": {"popLatency": [{"region": "us-east", "valuePerRegion": 123, "pops": [{"pop": "atl", "valuePerPop": 123}]}], {"region": "apac", "valuePerRegion": 345, "pops": [{"pop": "mel", "valuePerPop": 345}]}}}, {"originResponseTime": [{"origin": "1.1.1.1", "valuePerOrigin": 123}, {"origin": "my.url-address.com", "valuePerOrigin": 345}], "errorResponseTypes": {"REQ_BAD_TIMEOUT": 3, "REQ_SSL_NOT_SUPPORTED": 1, "REQ_IPV6_NOT_SUPPORTED": 4, "REQ_BAD_PARSE_ERROR": 2}}] }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved performance statistics in the last reliable minute for requested sites and metrics
StatisticsApiSuccessResponse

400

Bad Request StatisticsApiErrorResponse

Example data

Content-Type: application/json

```
{"errors": [{"status": 400, "source": {"pointer": "/v3/performance/statistics?metrics=1&caid=11111"}, "title": "Invalid input parameters"}]}
```

429

Rate limit exceeded `StatisticsApiErrorResponse`

Example data

Content-Type: application/json

```
{"errors": [{"status":429,"source":{"pointer":"/v3/performance/statistics?metric=s=1&caid=11111"},"title":"Rate limit exceeded"}]}
```

500

Internal Server Error `StatisticsApiErrorResponse`

Example data

Content-Type: application/json

```
{"errors": [{"status":500,"source":{"pointer":"/v3/performance/statistics?metric=s=1&caid=11111"},"title":"Error generating statistics"}]}
```

Models

Methods

Table of Contents

1. `ErrorResponseTypesModel`
2. `LatencyTimeMetricModel`
3. `OriginResponseTimeMetricModel`
4. `OriginResponseTimeModel`
5. `PerformanceStatisticsModel`
6. `PopLatencyModel`
7. `RegionLatencyModel`
8. `SiteStatisticsModel`
9. `StatisticsApiErrorResponseModel`
10. `StatisticsApiErrorResponse`
11. `StatisticsApiSuccessResponse`

`ErrorResponseTypesModel`

A mapping between error response types and their counts.
 For the full list of Cloud WAF Error Codes and their description see <a href="<https://docs.imperva.com/bundle/cloud-application-security/page/error-codes.htm>">Cloud WAF Error Pages and Codes

LatencyTimeMetricModel

A list of average latency time (in milliseconds) of the Imperva proxy servers in the PoP that handled requests for the website. For the full list of Imperva Data Centers (PoPs) see Imperva Data Centers (PoPs)

OriginResponseTimeMetricModel

A list of response times (in milliseconds) for each origin server.

OriginResponseTimeModel

The amount of time taken (in milliseconds) for a request to go from the Imperva proxy server in the PoP to the origin server and back. Calculated as the time the Imperva proxy has decided to send a request to the origin (before opening a connection to the origin), until the origin finishes sending the response to the proxy. Note: Redirect requests are excluded from average response time statistics since there is no origin server response. server (optional)

String

The IP address or URL of the origin server

example: 1.1.1.1 or my.url-address.com

dataCenterName (optional)

String

The name of your data center as defined in Imperva

example: My data center name

originPop (optional)

String

The Imperva PoP used to route traffic through Imperva to the origin server, if the Origin PoP setting was defined.

example: ash

avgResponseTime (optional)

Double

Average response time in milliseconds for all reporting proxies. format: double

example: 234

PerformanceStatisticsModel

timestamp (optional)

Long

Timestamp of the retrieved statistics in unix epoch time, truncated to the nearest full minute. format: int64

example: 1730122740000

accountId (optional)

Long

The unique account ID assigned by Imperva format: int64

example: 11111

sitesStatistics (optional)

array[SiteStatisticsModel]

A list of site statistics

PopLatencyModel

A list of PoPs in the region and their average latency time (in milliseconds)

pop (optional)

String

The 3-digit code for the PoP

example: asr

valuePerPop (optional)

Double

Latency time (in milliseconds) of the Imperva proxy servers in the PoP that handled requests for the website.
Averaged over all servers in the PoP. format: double
example: 234

RegionLatencyModel

The regional average latency (in milliseconds) of Imperva proxy servers in the PoP that processed requests for the website.

region (optional)

String

Region name

example: us-east-1

valuePerRegion (optional)

Double

The regional latency time (in milliseconds) averaged over all PoPs in the region format: double

example: 123

pops (optional)

array[PopLatencyModel]

A list of PoPs in the region and their average latency time (in milliseconds)

SiteStatisticsModel

A list of site statistics

siteld (optional)

Long

The unique website ID assigned by Imperva format: int64

example: 222

siteName (optional)

String

Website name

example: example.website.com

statistics (optional)

map[String, Object]

The metric model that is returned in the response.

StatisticsApiErrorModel

The error response model for the statistics API

status (optional)

Integer

format: int32

source (optional)

map[String, String]

title (optional)

String**StatisticsApiResponse**

The error response model for the statistics API

errors (optional)

array[StatisticsApiErrorModel]

StatisticsApiSuccessResponse

The success response model for the statistics API
data (optional)
array[PerformanceStatisticsModel]

Imperva Waiting Room API

Route your website visitors to a virtual waiting room when their requests can't be handled immediately.
For full feature documentation, see [Set Up a Waiting Room](#).

Retirement note: The v3 APIs supersede the v2 APIs which are going to be decommissioned soon. Therefore it is recommended to move to the new v3 APIs when possible.

Version: 1.0.0

BasePath:/waiting-room-settings

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

WaitingRoomSettingsV2

- post /v2/waiting-room
- delete /v2/waiting-room/{waiting-room-id}
- put /v2/waiting-room/{waiting-room-id}
- post /v2/waiting-room/{waiting-room-id}
- get /v2/waiting-room/{waiting-room-id}
- get /v2/waiting-room

WaitingRoomSettingsV3

- post /v3/sites/{site-id}/waiting-rooms
- delete /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
- get /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
- get /v3/sites/{site-id}/waiting-rooms
- put /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
- post /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}

WaitingRoomStatistics

- get /v2/waiting-room/statistics

WaitingRoomSettingsV2

```
post /v2/waiting-room
```

Create a new waiting room (createWaitingRoom3)

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body WaitingRoomAddRequestModel (required)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

WaitingRoomApiSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example'''",
    "mode" : "QUEUING or NOT_QUEUING",
    "accountId" : 11111,
```

```

    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    }
}, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    }
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully added new waiting room WaitingRoomApiSuccessResponse

400

Bad Request

500

Internal Server Error

```
delete /v2/waiting-room/{waiting-room-id}
```

Delete a waiting room (deleteWaitingRoom3)

Path parameters

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v2/waiting-room format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

ApiSimpleTextSuccessResponse

Example data

Content-Type: application/json

```
{  
  "data" : [ "data", "data" ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Waiting Room was deleted successfully [ApiSimpleTextSuccessResponse](#)

400

Bad Request

500

Internal Server Error

```
put /v2/waiting-room/{waiting-room-id}
```

Overwrite the configuration of an existing waiting room (full update) ([editWaitingRoomFullUpdate1](#))

Path parameters

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v2/waiting-room format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [WaitingRoomEditRequestModel](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHrtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHrtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully modified waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request

500

Internal Server Error

```
post /v2/waiting-room/{waiting-room-id}
```

Overwrite specified waiting room properties (partial update) ([editWaitingRoomPartialUpdate1](#))

Path parameters

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v2/waiting-room format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [WaitingRoomEditRequestModel](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used

for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
    }
  } ]
}
```

```

        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    }
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully modified waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request

500

[Internal Server Error](#)

```
get /v2/waiting-room/{waiting-room-id}
```

Retrieve waiting room details for a given waiting room ID (getWaitingRoom3)

Path parameters

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v2/waiting-room format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request

500

Internal Server Error

```
get /v2/waiting-room
```

Retrieve waiting rooms details (getWaitingRooms3)

Retrieves waiting room details for all waiting rooms in the account. Use the sitelid parameter to retrieve waiting rooms for a specific website

Query parameters

arg0 (optional)

Query Parameter

— Unique website ID (as assigned by Imperva) format: int64

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
```

```

    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example""",
    "mode" : "QUEUING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHrtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    }
}, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example""",
    "mode" : "QUEUING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpb
mc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHrtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    }
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved all waiting rooms for a given website [WaitingRoomApiSuccessResponse](#)

400

Bad Request

500

Internal Server Error

WaitingRoomSettingsV3

```
post /v3/sites/{site-id}/waiting-rooms
```

Create a new waiting room (createWaitingRoom)

Path parameters

site-id (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [WaitingRoomRequestDTO](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example'",
    "mode" : "QUEUING or NOT_QUEUING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == '/example'",
    "mode" : "QUEUING or NOT_QUEUING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  } ]
}
```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

Successfully created new waiting room [WaitingRoomApiSuccessResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
delete /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
```

Delete a waiting room (deleteWaitingRoom1)

Path parameters

site-id (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v3/sites/{site-id}/waiting-rooms format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[ApiSimpleTextSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
    "data" : [ "data", "data" ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Waiting Room was deleted successfully [ApiSimpleTextSuccessResponse](#)

400

Bad Request [APIError](#)

404

Not Found [APIError](#)

500

Internal Server Error [APIError](#)

```
get /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
```

Retrieve waiting room details for a given waiting room ID (getWaitingRoom1)

Path parameters

site-id (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v3/sites/{site-id}/waiting-rooms format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
  } ]
}
```

```

"siteId" : 11111,
"id" : 11111,
"thresholdSettings" : {
    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
}
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request [APIError](#)

404

Not Found [APIError](#)

500

[Internal Server Error APIError](#)

```
get /v3/sites/{site-id}/waiting-rooms
```

Retrieve waiting rooms details (getWaitingRooms)

Retrieves waiting room details for all waiting rooms in the specified site.

Path parameters

site-id (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
    "name" : "test waiting room",
  } ]
}
```

```

"siteId" : 11111,
"id" : 11111,
"thresholdSettings" : {
    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
}
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved all waiting rooms for a given website [WaitingRoomApiSuccessResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
put /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
```

Overwrite the configuration of an existing waiting room (full update) (`replaceWaitingRoom1`)

Path parameters

`site-id` (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

`waiting-room-id` (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET `/v3/sites/{site-id}/waiting-rooms` format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body WaitingRoomRequestDTO (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

WaitingRoomApiSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHrtbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "isEntranceRateEnabled" : true,
      "inactivityTimeout" : 30,
      "concurrentSessionsThreshold" : 600,
      "entranceRateThreshold" : 600,
      "isConcurrentSessionsEnabled" : true
    }
  }, {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
  }
]
```

```

"description" : "this waiting room used for test only",
"botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
"enabled" : true,
"filter" : "URL == '/example""",
"mode" : "QUEUING or NOT_QUEUING",
"accountId" : 11111,
"createdAt" : 1629981261000,
"htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=",
"name" : "test waiting room",
"siteId" : 11111,
"id" : 11111,
"thresholdSettings" : {
    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
}
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully modified waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

```
post /v3/sites/{site-id}/waiting-rooms/{waiting-room-id}
```

Overwrite specified waiting room properties (partial update) ([updateWaitingRoom1](#))

Path parameters

site-id (required)

Path Parameter

— Unique website ID (as assigned by Imperva) format: int64

waiting-room-id (required)

Path Parameter

— The unique ID for the waiting room, assigned by Imperva. To find the waiting room ID, run GET /v3/sites/{site-id}/waiting-rooms format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [WaitingRoomRequestDTO](#) (required)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

[WaitingRoomApiSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "lastModifiedAt" : 1629981261000,
    "hidePositionInLine" : false,
    "queueInactivityTimeout" : 10,
    "lastModifiedBy" : "test user",
    "description" : "this waiting room used for test only",
    "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
    "enabled" : true,
    "filter" : "URL == \"/example\"",
    "mode" : "QUEUEING or NOT_QUEUEING",
    "accountId" : 11111,
    "createdAt" : 1629981261000,
    "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHRTbD4=",
    "name" : "test waiting room",
    "siteId" : 11111,
    "id" : 11111,
    "thresholdSettings" : {
      "thresholds" : [
        {
          "thresholdType" : "PERCENTAGE_OF_WAITING_ROOM_SIZE",
          "percentage" : 50
        }
      ],
      "actions" : [
        {
          "actionType" : "BLOCK"
        }
      ]
    }
  } ]
}
```

```

    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
  }
}, {
  "lastModifiedAt" : 1629981261000,
  "hidePositionInLine" : false,
  "queueInactivityTimeout" : 10,
  "lastModifiedBy" : "test user",
  "description" : "this waiting room used for test only",
  "botsActionInQueuingMode" : "WAIT_IN_LINE, BYPASS or BLOCK",
  "enabled" : true,
  "filter" : "URL == '/example"",
  "mode" : "QUEUEING or NOT_QUEUEING",
  "accountId" : 11111,
  "createdAt" : 1629981261000,
  "htmlTemplateBase64" : "PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEh1YWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZhk+CjwvaHRtbD4=",
  "name" : "test waiting room",
  "siteId" : 11111,
  "id" : 11111,
  "thresholdSettings" : {
    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
  }
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully modified waiting room for a given waiting room id [WaitingRoomApiSuccessResponse](#)

400

Bad Request [APIError](#)

500

Internal Server Error [APIError](#)

WaitingRoomStatistics

```
get /v2/waiting-room/statistics
```

Retrieve waiting room statistics for given asset IDs (getWaitingRoomStatistics1)

Query parameters

arg0 (optional)

Query Parameter

— The asset type to retrieve waiting room statistics for. Possible values: WAITING_ROOM or SITE. Use together with the ids parameter.

arg1 (required)

Query Parameter

— Start date time of the statistics (epoch time) in milliseconds. format: int64

arg2 (required)

Query Parameter

— End date time of the statistics (epoch time) in milliseconds. format: int64

arg3 (optional)

Query Parameter

— The asset's Imperva ID. Use together with the assetType parameter.

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

StatisticsApiResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 1778899,
    "from" : 1637049600000,
    "sites" : [ {
      "siteId" : 98802543,
      "waitingRooms" : [ {
        "usersEnteredQueue" : 342,
        "usersPassedQueue" : 348,
        "totalUsers" : 21,
        "usersLeftQueue" : 17,
        "series" : {
          "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.962133916683182 ],
          "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749251911 ],
          "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.027123023002322 ]
        }
      }
    } ]
  } ]
}
```

```

        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.06140124150
3109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576
],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,
    "waitingRoomId" : 12,
    "avgWaitTimeInQueue" : 0.8008281904610115,
    "enabled" : true
}, {
    "usersEnteredQueue" : 342,
    "usersPassedQueue" : 348,
    "totalUsers" : 21,
    "usersLeftQueue" : 17,
    "series" : {
        "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.9621339166831
82 ],
        "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749
251911 ],
        "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.0271230
23002322 ],
        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.06140124150
3109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576
],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,

```

```

        "waitingRoomId" : 12,
        "avgWaitTimeInQueue" : 0.8008281904610115,
        "enabled" : true
    } ]
}, {
    "siteId" : 98802543,
    "waitingRooms" : [ {
        "usersEnteredQueue" : 342,
        "usersPassedQueue" : 348,
        "totalUsers" : 21,
        "usersLeftQueue" : 17,
        "series" : {
            "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.962133916683182 ],
            "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749251911 ],
            "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.027123023002322 ],
            "intervalMiliSeconds" : 6,
            "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.061401241503109 ],
            "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576 ],
            "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.637376656633329 ],
            "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029452 ],
            "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.3021358869347655 ]
        },
        "name" : "test waiting room",
        "numActiveUsers" : 500,
        "thresholdSettings" : {
            "isEntranceRateEnabled" : true,
            "inactivityTimeout" : 30,
            "concurrentSessionsThreshold" : 600,
            "entranceRateThreshold" : 600,
            "isConcurrentSessionsEnabled" : true
        },
        "usersInQueue" : 342,
        "waitingRoomId" : 12,
        "avgWaitTimeInQueue" : 0.8008281904610115,
        "enabled" : true
    }, {
        "usersEnteredQueue" : 342,
        "usersPassedQueue" : 348,
        "totalUsers" : 21,
        "usersLeftQueue" : 17,
        "series" : {
            "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.962133916683182 ],
            "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749251911 ],
            "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.027123023002322 ],
            "intervalMiliSeconds" : 6,
            "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.061401241503109 ],
            "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576 ]
        }
    }
]
}

```

```
[
    "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
    "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
    "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
},
"name" : "test waiting room",
"numActiveUsers" : 500,
"thresholdSettings" : {
    "isEntranceRateEnabled" : true,
    "inactivityTimeout" : 30,
    "concurrentSessionsThreshold" : 600,
    "entranceRateThreshold" : 600,
    "isConcurrentSessionsEnabled" : true
},
"usersInQueue" : 342,
"waitingRoomId" : 12,
"avgWaitTimeInQueue" : 0.8008281904610115,
"enabled" : true
} ]
} ],
"to" : 1637060400000
}, {
"accountId" : 1778899,
"from" : 1637049600000,
"sites" : [ {
"siteId" : 98802543,
"waitingRooms" : [ {
    "usersEnteredQueue" : 342,
    "usersPassedQueue" : 348,
    "totalUsers" : 21,
    "usersLeftQueue" : 17,
    "series" : {
        "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.9621339166831
82 ],
        "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749
251911 ],
        "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.0271230
23002322 ],
        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.06140124150
3109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576
],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
    }
}
]
```

```

        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,
    "waitingRoomId" : 12,
    "avgWaitTimeInQueue" : 0.8008281904610115,
    "enabled" : true
}, {
    "usersEnteredQueue" : 342,
    "usersPassedQueue" : 348,
    "totalUsers" : 21,
    "usersLeftQueue" : 17,
    "series" : {
        "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.962133916683182 ],
        "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749251911 ],
        "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.027123023002322 ],
        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.061401241503109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576 ],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.637376656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.3021358869347655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,
    "waitingRoomId" : 12,
    "avgWaitTimeInQueue" : 0.8008281904610115,
    "enabled" : true
} ]
}, {
    "siteId" : 98802543,
    "waitingRooms" : [ {
        "usersEnteredQueue" : 342,
        "usersPassedQueue" : 348,
        "totalUsers" : 21,
        "usersLeftQueue" : 17,
        "series" : {
            "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.962133916683182 ],
            "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749251911 ],
            "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.027123023002322 ]
        }
    }]
}

```

```

        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.06140124150
3109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576
],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,
    "waitingRoomId" : 12,
    "avgWaitTimeInQueue" : 0.8008281904610115,
    "enabled" : true
}, {
    "usersEnteredQueue" : 342,
    "usersPassedQueue" : 348,
    "totalUsers" : 21,
    "usersLeftQueue" : 17,
    "series" : {
        "totalUsersInQueuePerMinuteList" : [ 5.962133916683182, 5.9621339166831
82 ],
        "visitorsLeftWaitingRoomAvgTimeList" : [ 3.616076749251911, 3.616076749
251911 ],
        "visitorsPassedWaitingRoomAvgTimeList" : [ 2.027123023002322, 2.0271230
23002322 ],
        "intervalMiliSeconds" : 6,
        "totalVisitorsPassedPerMinuteList" : [ 7.061401241503109, 7.06140124150
3109 ],
        "totalVisitorsPerMinuteList" : [ 9.301444243932576, 9.301444243932576
],
        "totalVisitorsEnteredQueuePerMinuteList" : [ 5.637376656633329, 5.63737
6656633329 ],
        "totalActiveUsersPerMinuteList" : [ 1.4658129805029452, 1.4658129805029
452 ],
        "totalVisitorsLeftPerMinuteList" : [ 2.3021358869347655, 2.302135886934
7655 ]
    },
    "name" : "test waiting room",
    "numActiveUsers" : 500,
    "thresholdSettings" : {
        "isEntranceRateEnabled" : true,
        "inactivityTimeout" : 30,
        "concurrentSessionsThreshold" : 600,
        "entranceRateThreshold" : 600,
        "isConcurrentSessionsEnabled" : true
    },
    "usersInQueue" : 342,

```

```

        "waitingRoomId" : 12,
        "avgWaitTimeInQueue" : 0.8008281904610115,
        "enabled" : true
    } ]
}
} ],
"to" : 1637060400000
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successfully retrieved waiting room statistics for given asset IDs StatisticsApiResponse

400

Bad Request

500

Internal Server Error

Models

Methods

Table of Contents

1. APIError
 2. ApiSimpleTextSuccessResponse
 3. SeriesStatisticsModel
 4. SingleStatisticsWaitingRoomModel
 5. StatisticModel
 6. StatisticsApiResponse
 7. StatisticsSiteModel
 8. WaitingRoomAddRequestModel
 9. WaitingRoomApiSuccessResponse
 10. WaitingRoomEditRequestModel
 11. WaitingRoomModel
-

-
- 12. WaitingRoomRequestDTO
 - 13. WaitingRoomThresholdSettingsModel

APIError

code (optional)
String
detail (optional)
String
id (optional)
String
source (optional)
map[String, Object]
status (optional)
Integer
format: int32
title (optional)
String

ApiSimpleTextSuccessResponse

data (optional)
array[String]

SeriesStatisticsModel

The series statistics for the relevant waiting room id.

intervalMiliSeconds (optional)
Integer
format: int32
totalActiveUsersPerMinuteList (optional)
array[Double]
format: double
totalUsersInQueuePerMinuteList (optional)
array[Double]
format: double
totalVisitorsEnteredQueuePerMinuteList (optional)
array[Double]
format: double
totalVisitorsLeftPerMinuteList (optional)
array[Double]
format: double
totalVisitorsPassedPerMinuteList (optional)
array[Double]
format: double
totalVisitorsPerMinuteList (optional)
array[Double]
format: double
visitorsLeftWaitingRoomAvgTimeList (optional)
array[Double]
format: double
visitorsPassedWaitingRoomAvgTimeList (optional)
array[Double]
format: double

SingleStatisticsWaitingRoomModel

Statistics list for requested waiting rooms

avgWaitTimeInQueue (optional)

Double

The average time that users waited in the queue, in seconds. format: double

enabled (optional)

Boolean

The waiting room status.

example: true

name (optional)

String

The waiting room name.

example: test waiting room

numActiveUsers (optional)

Long

Number of active users currently in the site. format: int64

example: 500

series (optional)

SeriesStatisticsModel

thresholdSettings (optional)

WaitingRoomThresholdSettingsModel

totalUsers (optional)

Long

Total number of users who tried to enter the website. format: int64

example: 21

usersEnteredQueue (optional)

Long

Total number of users that entered waiting room format: int64

example: 342

usersInQueue (optional)

Long

Number of current users in waiting room. format: int64

example: 342

usersLeftQueue (optional)

Long

The number of users that left the waiting room before entering the site. format: int64

example: 17

usersPassedQueue (optional)

Long

The number of users that passed the waiting room and entered the site. format: int64

example: 348

waitingRoomId (optional)

Long

The unique ID for the waiting room, assigned by Imperva. format: int64

example: 12

StatisticModel

accountId (optional)

Long

The unique ID for the account, assigned by Imperva. format: int64

example: 1778899

from (optional)

Long

Start date time of the statistics (epoch time) in milliseconds format: int64

example: 1637049600000

sites (optional)

array[StatisticsSiteModel]

Statistics list for requested sites

to (optional)

Long

End date time of the statistics (epoch time) in milliseconds format: int64

example: 1637060400000

StatisticsApiResponse

data (optional)

array[StatisticModel]**StatisticsSiteModel**

Statistics list for requested sites

siteId (optional)

Long

The unique ID for the site, assigned by Imperva. format: int64

example: 98802543

waitingRooms (optional)

array[SingleStatisticsWaitingRoomModel]

Statistics list for requested waiting rooms

WaitingRoomAddRequestModel

botsActionInQueuingMode (optional)

String

The waiting room bot handling action. Determines the waiting room behavior for legitimate bots trying to access your website during peak time. Applies only when the activation threshold has been passed and visitors are being sent to the queue.

example: WAIT_IN_LINE, BYPASS or BLOCK

description (optional)

String

The waiting room description.

example: this waiting room used for test only

enabled (optional)

Boolean

Indicates whether the waiting room is enabled or not.

example: true

filter (optional)

String

The condition that determines which sessions are routed to the waiting room. If the number of sessions per second matching the condition exceeds the threshold, the sessions are forwarded to the waiting room.

example: URL == "/example"

hidePositionInLine (optional)

Boolean

Hides the user's position in the waiting room line

example: true

htmlTemplateBase64 (optional)

String

The HTML template of the waiting room page, in base64 format.

example: PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEhlYWWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=

name (optional)

String

The waiting room name (must be unique within the same site).

example: unique test waiting room name
queueInactivityTimeout (optional)

Long

Queue inactivity timeout, from 1 to 10 minutes. Default value = 1 minute. A user in the waiting room who is inactive for a longer period of time is considered as having left the queue. On returning to the site, the user moves to the end of the queue and needs to wait in line again if the waiting room is active. format: int64

example: 10

siteId (optional)

Long

The site ID. format: int64

example: 11111

thresholdSettings (optional)

[WaitingRoomThresholdSettingsModel](#)

WaitingRoomApiSuccessResponse

data (optional)

[array\[WaitingRoomModel\]](#)

WaitingRoomEditRequestModel

botsActionInQueuingMode (optional)

String

The waiting room bot handling action. Determines the waiting room behavior for legitimate bots trying to access your website during peak time. Applies only when the activation threshold has been passed and visitors are being sent to the queue.

example: WAIT_IN_LINE, BYPASS or BLOCK

description (optional)

String

The waiting room description.

example: this waiting room used for test only

enabled (optional)

Boolean

Indicates whether the waiting room is enabled or not.

example: true

filter (optional)

String

The condition that determines which sessions are routed to the waiting room. If the number of sessions per second matching the condition exceeds the threshold, the sessions are forwarded to the waiting room.

example: URL == "/example"

hidePositionInLine (optional)

Boolean

Hides the user's position in the waiting room line

example: true

htmlTemplateBase64 (optional)

String

The HTML template of the waiting room page, in base64 format.

example: PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEhlYWWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=

name (optional)

String

The waiting room name (must be unique within the same site).

example: unique test waiting room name

queueInactivityTimeout (optional)

Long

Queue inactivity timeout, from 1 to 10 minutes. Default value = 1 minute. A user in the waiting room who is inactive for a longer period of time is considered as having left the queue. On returning to the site, the user moves

to the end of the queue and needs to wait in line again if the waiting room is active. format: int64

example: 10

thresholdSettings (optional)

[WaitingRoomThresholdSettingsModel](#)

WaitingRoomModel

accountId (optional)

Long

The account ID format: int64

example: 11111

botsActionInQueuingMode (optional)

String

The waiting room bot handling action. Determines the waiting room behavior for legitimate bots trying to access your website during peak time. Applies only when the activation threshold has been passed and visitors are being sent to the queue.

example: WAIT_IN_LINE, BYPASS or BLOCK

createdAt (optional)

Long

The waiting room creation date in milliseconds. format: int64

example: 1629981261000

description (optional)

String

The waiting room description

example: this waiting room used for test only

enabled (optional)

Boolean

Indicates whether the waiting room is enabled or not

example: true

filter (optional)

String

The condition that determines which sessions are routed to the waiting room. If the number of sessions per second matching the condition exceeds the threshold, the sessions are forwarded to the waiting room.

example: URL == "/example"

hidePositionInLine (optional)

Boolean

Hides the user's position in the waiting room line

example: false

htmlTemplateBase64 (optional)

String

The HTML template of the waiting room page, in base64 format.

example: PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEhIYWRpbmc8L2gxPgo8cD5NeSBmaXJzd

CBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=

id (optional)

Long

The waiting room ID format: int64

example: 11111

lastModifiedAt (optional)

Long

The last configuration change date in milliseconds. format: int64

example: 1629981261000

lastModifiedBy (optional)

String

The user who last modified the waiting room configuration

example: test user

mode (optional)

String

The waiting room mode. Indicates whether the waiting room is currently queuing or not.

example: QUEUING or NOT_QUEUEING

name (optional)

String

The waiting room name

example: test waiting room

queueInactivityTimeout (optional)

Long

Queue inactivity timeout, from 1 to 10 minutes. Default value = 1 minute. A user in the waiting room who is inactive for a longer period of time is considered as having left the queue. On returning to the site, the user moves to the end of the queue and needs to wait in line again if the waiting room is active. format: int64

example: 10

sitId (optional)

Long

The site ID format: int64

example: 11111

thresholdSettings (optional)

[WaitingRoomThresholdSettingsModel](#)

WaitingRoomRequestDTO

botsActionInQueuingMode (optional)

String

The waiting room bot handling action. Determines the waiting room behavior for legitimate bots trying to access your website during peak time. Applies only when the activation threshold has been passed and visitors are being sent to the queue.

Enum:

WAIT_IN_LINE

BYPASS

BLOCK

example: WAIT_IN_LINE, BYPASS or BLOCK

description (optional)

String

The waiting room description.

example: this waiting room used for test only

enabled (optional)

Boolean

Indicates whether the waiting room is enabled or not.

example: true

filter (optional)

String

The condition that determines which sessions are routed to the waiting room. If the number of sessions per second matching the condition exceeds the threshold, the sessions are forwarded to the waiting room.

example: URL == "/example"

hidePositionInLine (optional)

Boolean

Hides the user's position in the waiting room line

example: true

htmlTemplateBase64 (optional)

String

The HTML template of the waiting room page, in base64 format.

example: PGh0bWw+Cjxib2R5PgokQk9EWSQKPGgxPk15IEZpcnN0IEhlYWWRpbmc8L2gxPgo8cD5NeSBmaXJzdCBwYXJhZ3JhcGguPC9wPgo8L2JvZHk+CjwvaHRtbD4=

name

String

The waiting room name (must be unique within the same site).

example: unique test waiting room name

queueInactivityTimeout (optional)

Long

Queue inactivity timeout, from 1 to 10 minutes. A user in the waiting room who is inactive for a longer period of time is considered as having left the queue. On returning to the site, the user moves to the end of the queue and needs to wait in line again if the waiting room is active. format: int64

example: 10

thresholdSettings (optional)

[WaitingRoomThresholdSettingsModel](#)

WaitingRoomThresholdSettingsModel

The waiting room activation threshold settings

concurrentSessionsThreshold (optional)

Long

The active users activation threshold of the waiting room. The waiting room is activated when number of active users reached specified value. format: int64

example: 600

entranceRateThreshold (optional)

Long

The entrance rate activation threshold of the waiting room. The waiting room is activated when sessions per minute exceed the specified value. Minimum of 60 users per minute. format: int64

example: 600

inactivityTimeout (optional)

Long

Inactivity timeout, between 1 and 30 minutes. If waiting room conditions that limit the scope of the waiting room to a subset of the website have been defined, the user is considered active only when navigating the pages in scope of the conditions. A user who is inactive for a longer period of time is considered as having left the site. On returning to the site, the user needs to wait in line again if the waiting room is active. format: int64

example: 30

isConcurrentSessionsEnabled (optional)

Boolean

Indicates if the concurrent sessions threshold setting is enabled. Note: at least one of the threshold strategies (entranceRateThreshold / concurrentSessionsThreshold) must be configured

example: true

isEntranceRateEnabled (optional)

Boolean

Indicates if the entrance rate threshold setting is enabled. Note: at least one of the threshold strategies (entranceRateThreshold / concurrentSessionsThreshold) must be configured

example: true

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

DDoSForNetworksTestAlerts

- post /api/v1/infra-protect/test-alerts/bgp/down
- post /api/v1/infra-protect/test-alerts/bgp/up
- post /api/v1/infra-protect/test-alerts/ddos/start
- post /api/v1/infra-protect/test-alerts/ddos/stop
- post /api/v1/infra-protect/test-alerts/monitoring/attack-start
- post /api/v1/infra-protect/test-alerts/monitoring/bad-data
- post /api/v1/infra-protect/test-alerts/monitoring/start
- post /api/v1/infra-protect/test-alerts/monitoring/stop
- post /api/v1/infra-protect/test-alerts/connection/down
- post /api/v1/infra-protect/test-alerts/connection/up
- post /api/v1/infra-protect/test-alerts/ip-protection-status/down
- post /api/v1/infra-protect/test-alerts/ip-protection-status/up

DDoSForNetworksTestAlerts

```
post /api/v1/infra-protect/test-alerts/bgp/down
```

bgp down (postInfraProtectBgpDown)

Use this operation to send a test notification informing you that the Infrastructure Protection bgp is down.

Query parameters

`bgp_id` (optional)

Query Parameter

— The bgp to send a notification for. format: int64

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted [inline_response_200](#)

```
post /api/v1/infra-protect/test-alerts/bgp/up
```

Bgp up (postInfraProtectBgpUp)

Use this operation to send a test notification informing you that the Infrastructure Protection bgp is up.

Query parameters

bgp_id (optional)

Query Parameter

— The bgp to send a notification for. format: int64

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted [inline_response_200](#)

```
post /api/v1/infra-protect/test-alerts/ddos/start
```

DDoS start (postInfraProtectDdosStart)

Use this operation to send a test notification informing you that an Infrastructure Protection DDoS attack has started.

You can optionally provide additional parameters to determine the magnitude of the attack.

Query parameters

ip_prefix (optional)

Query Parameter

— The IP prefix to send a notification for. For example, 10.10.10.10

bps (optional)

Query Parameter

— Number of bits per second format: int32

pps (optional)

Query Parameter

— Number of packets per second format: int64

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_1](#)

```
post /api/v1/infra-protect/test-alerts/ddos/stop
```

DDoS stop (postInfraProtectDdosStop)

Use this operation to send a test notification informing you that an Infrastructure Protection DDoS attack has ended.

You can optionally provide additional parameters to determine the magnitude of the attack.

Query parameters

ip_prefix (optional)

Query Parameter

— The IP prefix to send a notification for. For example, 10.10.10.10

bps (optional)

Query Parameter

— Number of bits per second format: int32
pps (optional)
Query Parameter
— Number of packets per second format: int64

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted
[inline_response_200_1](#)

```
post /api/v1/infra-protect/test-alerts/monitoring/attack-start
```

Monitoring attack start (postInfraProtectMonitoringAttackStartCriticalAlert)

Use this operation to send a test notification informing you that the monitoring service has detected a DDoS attack.

You can optionally provide additional parameters to determine the magnitude of the attack.

Query parameters

ip_prefix (optional)

Query Parameter

— The IP range to send a notification for. For example, 1.1.1.0/24

bps (optional)

Query Parameter

— Number of bits per second format: int32

pps (optional)

Query Parameter

— Number of packets per second format: int64

packet_type (optional)

Query Parameter

— Packet type. (UDP, TCP, DNS, DNS_RESPONSE, ICMP, SYN, FRAG, LARGE_SYN, NTP, NETFLOW, SSDP, GENERAL)

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_1](#)

```
post /api/v1/infra-protect/test-alerts/monitoring/bad-data
```

Monitoring bad data (postInfraProtectNetFlowBadData)

Use this operation to send a test notification informing you that the monitoring service is receiving messages that do not conform to the accepted format.

You can optionally provide the exporter IP found in the Management Console's Monitoring Settings page.

Query parameters

exporter_ip (optional)

Query Parameter

— The exporter IP to send a notification for. For example, 10.10.10.10.
The exporter IP can be found in the Cloud Security Console's Monitoring Settings page.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted
[inline_response_200_2](#)

```
post /api/v1/infra-protect/test-alerts/monitoring/start
```

Monitoring start (postInfraProtectNetFlowStart)

Use this operation to send a test notification informing you that flow monitoring has started.

You can optionally provide the exporter IP found in the Management Console's Monitoring Settings page.

Query parameters

exporter_ip (optional)

Query Parameter

— The exporter IP to send a notification for. For example, 10.10.10.10.
The exporter IP can be found in the Cloud Security Console's Monitoring Settings page.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_2](#)

```
post /api/v1/infra-protect/test-alerts/monitoring/stop
```

Monitoring stop (postInfraProtectNetFlowStop)

Use this operation to send a test notification informing you that NetFlow monitoring has stopped.

Query parameters

exporter_ip (optional)

Query Parameter

— The exporter IP to send a notification for. For example, 10.10.10.10. The exporter IP can be found in the Cloud Security Console's Monitoring Settings page.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_2](#)

```
post /api/v1/infra-protect/test-alerts/connection/down
```

Connection down (postInfraProtectTunnelDown)

Use this operation to send a test notification informing you that the Infrastructure Protection connection is down. You can optionally provide the name of the connection as it appears in the Management Console's Protection

Settings page.

Query parameters

connection_name (optional)

Query Parameter

— The connection to send a notification for.
Enter the connection name as it appears in the Cloud Security Console's Protection Settings page. For example, Test_GRE_Tunnel.

Return type

inline_response_200

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted [inline_response_200](#)

```
post /api/v1/infra-protect/test-alerts/connection/up
```

Connection up (postInfraProtectTunnelUp)

Use this operation to send a test notification informing you that the Infrastructure Protection connection is up. You can optionally provide the name of the connection as it appears in the Management Console's Protection Settings page.

Query parameters

connection_name (optional)

Query Parameter

— The connection to send a notification for.
Enter the connection name as it appears in the Cloud Security Console's Protection Settings page. For example, Test_GRE_Tunnel.

Return type

inline_response_200

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted [inline_response_200](#)

```
post /api/v1/infra-protect/test-alerts/ip-protection-status/down
```

IP protection status down (postProtectedIPStatusDown)

Use this operation to send a test notification informing you that the IP Protection status is down.

Query parameters

ip_protection (optional)

Query Parameter

— The IP to send a notification for. For example, 10.10.10.10

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_3](#)

IP protection status up (postProtectedIPStatusUp)

Use this operation to send a test notification informing you that the IP Protection status is up.

Query parameters

ip_protection (optional)

Query Parameter

— The IP to send a notification for. For example, 10.10.10.10

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

""

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
9414 - Feature not permitted

[inline_response_200_1](#)

Models

Methods

Table of Contents

1. `ApiResult`
2. `ApiResultTestAlert`
3. `ApiResultTestAlertConnectionStatus`
4. `ApiResultTestAlertExporterStatus`
5. `ApiResultTestAlertProtectedIPStatus`
6. `inline_response_200`
7. `inline_response_200_1`
8. `inline_response_200_2`
9. `inline_response_200_3`

ApiResult

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
 array[map[String, Object]]

ApiResultTestAlert

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
 array[map[String, Object]]
 ip_prefix (optional)
String
 example: 100.1.2.0/24
 status (optional)
String
 example: DDoS start notification sent successfully

ApiResultTestAlertConnectionStatus

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
 array[map[String, Object]]

ip_prefix (optional)
String
example: 100.1.2.0/24
status (optional)
String
example: DDoS start notification sent successfully
connection_name (optional)
String
example: CONNECTION_NAME

ApiResultTestAlertExporterStatus

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
ip_prefix (optional)
String
example: 100.1.2.0/24
status (optional)
String
example: DDoS start notification sent successfully

ApiResultTestAlertProtectedIPStatus

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
ip_prefix (optional)
String
example: 100.1.2.0/24
status (optional)
String
example: DDoS start notification sent successfully
ip (optional)
String
example: 1.2.3.4

inline_response_200

inline_response_200_1

inline_response_200_2

inline_response_200_3

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

DDoSProtectionPolicyVisibility

- `get /api/prov/v3/ddos-protection/monitor-policy`
- `get /api/prov/v3/ddos-protection/monitor-policy/revisions`
- `get /api/prov/v3/ddos-protection/security-policy`
- `get /api/prov/v3/ddos-protection/security-policy/revisions`

DDoSProtectionPolicyVisibility

```
get /api/prov/v3/ddos-protection/monitor-policy
```

Get monitoring policy (getMonitorPolicy)

Use this operation to view the monitoring policy of a Protected Range

Query parameters

ipRange (required)

Query Parameter

— IP Range

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
7101 - Policy not found
[inline_response_200](#)

```
get /api/prov/v3/ddos-protection/monitor-policy/revisions
```

Get monitoring policy revisions (getMonitorPolicyRevisions)

Use this operation to view the last 2 revisions of threshold changes in the monitoring policy for a Protected Range

Query parameters

ipRange (required)

Query Parameter

— IP Range

Return type

array[MonitoringPolicyRevisionResponse]

Example data

Content-Type: application/json

```
[ {
  "policyRevisions" : [ {
    "data" : {
      "TCP" : [ {
        "amount" : "100.0K PPS",
        "time" : "Over 15 sec"
      }, {
        "amount" : "70.0K PPS",
        "time" : "Over 30 sec"
      }, {
        "amount" : "200.0 Mbps",
        "time" : "Over 1 min"
      }
    }
  }
}
```

```

        "time" : "Over 30 sec"
    } ],
"UDP" : [ {
    "amount" : "80.0K PPS",
    "time" : "Over 45 sec"
}, {
    "amount" : "200.0 Mbps",
    "time" : "Over 30 sec"
}, {
    "amount" : "90.0 Mbps",
    "time" : "Over 60 sec"
} ],
"OTHER" : [ {
    "amount" : "30.0K PPS",
    "time" : "Over 15 sec"
}, {
    "amount" : "10.0K PPS",
    "time" : "Over 45 sec"
}, {
    "amount" : "150.0 Mbps",
    "time" : "Over 30 sec"
} ],
"FRAG" : [ {
    "amount" : "10.0K PPS",
    "time" : "Over 30 sec"
}, {
    "amount" : "40.0 Mbps",
    "time" : "Over 15 sec"
}, {
    "amount" : "25.0 Mbps",
    "time" : "Over 30 sec"
} ],
"DNS" : [ {
    "amount" : "25.0K PPS",
    "time" : "Over 15 sec"
}, {
    "amount" : "10.0K PPS",
    "time" : "Over 30 sec"
} ],
"SYN" : [ {
    "amount" : "20.0K PPS",
    "time" : "Over 30 sec"
}, {
    "amount" : "17.0K PPS",
    "time" : "Over 75 sec"
} ],
"LARGE_SYN" : [ {
    "amount" : "10.0K PPS",
    "time" : "Over 30 sec"
}, {
    "amount" : "40.0 Mbps",
    "time" : "Over 15 sec"
}, {
    "amount" : "25.0 Mbps",
    "time" : "Over 30 sec"
} ],
"SSDP" : [ {
    "amount" : "10.0K PPS",
    "time" : "Over 30 sec"
}
]

```

```

}, {
    "amount" : "40.0 Mbps",
    "time" : "Over 15 sec"
}, {
    "amount" : "25.0 Mbps",
    "time" : "Over 30 sec"
} ],
"NTP" : [ {
    "amount" : "10.0K PPS",
    "time" : "Over 30 sec"
}, {
    "amount" : "40.0 Mbps",
    "time" : "Over 15 sec"
}, {
    "amount" : "25.0 Mbps",
    "time" : "Over 45 sec"
} ],
"ICMP" : [ {
    "amount" : "20.0K PPS",
    "time" : "Over 30 sec"
}, {
    "amount" : "40.0 Mbps",
    "time" : "Over 15 sec"
}, {
    "amount" : "25.0 Mbps",
    "time" : "Over 30 sec"
} ],
},
"lastUpdate" : "2023-05-02T06:18:51Z"
} ]
},
"policyRevisions" : [
    "data" : {
        "TCP" : [ {
            "amount" : "100.0K PPS",
            "time" : "Over 15 sec"
        }, {
            "amount" : "70.0K PPS",
            "time" : "Over 30 sec"
        }, {
            "amount" : "200.0 Mbps",
            "time" : "Over 30 sec"
        } ],
        "UDP" : [ {
            "amount" : "80.0K PPS",
            "time" : "Over 45 sec"
        }, {
            "amount" : "200.0 Mbps",
            "time" : "Over 30 sec"
        }, {
            "amount" : "90.0 Mbps",
            "time" : "Over 60 sec"
        } ],
        "OTHER" : [ {
            "amount" : "30.0K PPS",
            "time" : "Over 15 sec"
        }, {
            "amount" : "10.0K PPS",
            "time" : "Over 45 sec"
        }
    }
]
}

```

```

}, {
  "amount" : "150.0 Mbps",
  "time" : "Over 30 sec"
} ],
"FRAG" : [ {
  "amount" : "10.0K PPS",
  "time" : "Over 30 sec"
}, {
  "amount" : "40.0 Mbps",
  "time" : "Over 15 sec"
}, {
  "amount" : "25.0 Mbps",
  "time" : "Over 30 sec"
} ],
"DNS" : [ {
  "amount" : "25.0K PPS",
  "time" : "Over 15 sec"
}, {
  "amount" : "10.0K PPS",
  "time" : "Over 30 sec"
} ],
"SYN" : [ {
  "amount" : "20.0K PPS",
  "time" : "Over 30 sec"
}, {
  "amount" : "17.0K PPS",
  "time" : "Over 75 sec"
} ],
"LARGE_SYN" : [ {
  "amount" : "10.0K PPS",
  "time" : "Over 30 sec"
}, {
  "amount" : "40.0 Mbps",
  "time" : "Over 15 sec"
}, {
  "amount" : "25.0 Mbps",
  "time" : "Over 30 sec"
} ],
"SSDP" : [ {
  "amount" : "10.0K PPS",
  "time" : "Over 30 sec"
}, {
  "amount" : "40.0 Mbps",
  "time" : "Over 15 sec"
}, {
  "amount" : "25.0 Mbps",
  "time" : "Over 30 sec"
} ],
"NTP" : [ {
  "amount" : "10.0K PPS",
  "time" : "Over 30 sec"
}, {
  "amount" : "40.0 Mbps",
  "time" : "Over 15 sec"
}, {
  "amount" : "25.0 Mbps",
  "time" : "Over 45 sec"
} ],
"ICMP" : [ {

```

```

        "amount" : "20.0K PPS",
        "time" : "Over 30 sec"
    } ,
    {
        "amount" : "40.0 Mbps",
        "time" : "Over 15 sec"
    } ,
    {
        "amount" : "25.0 Mbps",
        "time" : "Over 30 sec"
    } ]
},
"lastUpdate" : "2023-05-02T06:18:51Z"
} ]
}
]
}
]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
7101 - Policy not found


```
get /api/prov/v3/ddos-protection/security-policy
```

Get security policy (getSecurityPolicy)

Use this operation to view the security policy of a Protected IP or Protected Range. The thresholds determine at what point the range/IP is considered to be under DDoS attack. Mitigation is then started and the traffic is blocked.

Query parameters

assetId (required)

Query Parameter

— Protected Range or Protected IP

isProtectedIp (required)

Query Parameter

— Indicates if the asset is a Protected IP or a Protected Range. Default is false, indicating that the asset is a Protected Range.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
7101 - Policy not found
[inline_response_200_1](#)

```
get /api/prov/v3/ddos-protection/security-policy/revisions
```

Get security policy revisions (getSecurityPolicyRevisions)

Use this operation to view the last 2 revisions of threshold changes in the security policy for a Protected IP or Protected Range. The thresholds determine at what point the range/IP is considered to be under DDoS attack. Mitigation is then started and the traffic is blocked.

Query parameters

assetId (required)

Query Parameter

— Protected Range or Protected IP

isProtectedIp (required)

Query Parameter

— Indicates if the asset is a Protected IP or a Protected Range. Default is false, indicating that the asset is a Protected Range.

Return type

array[[SecurityPolicyRevisionResponse](#)]

Example data

Content-Type: application/json

```
[ {
  "policyRevisions" : [ {
    "singleIpThresholds" : {
      "ppsThresholds" : {
        "UDP" : "10.0K PPS",
        "TCP" : "50.0K PPS",
        "TOTAL" : "50.0K PPS",
        "DNS_RESPONSE" : "0.3K PPS",
        "DNS" : "0.3K PPS",
        "SYN" : "0.5K PPS",
        "ICMP" : "0.5K PPS"
      }
    }
  }
}
```

```

    "SSDP" : "0.3K PPS",
    "NTP" : "0.3K PPS",
    "OTHER" : "3.0K PPS",
    "FRAG" : "0.3K PPS",
    "CUSTOM" : "0.3K PPS",
    "LARGE_SYN" : "0.3K PPS",
    "ICMP" : "0.3K PPS"
  },
  "bandwidthThresholds" : {
    "UDP" : "10.0 Mbps",
    "TCP" : "50.0 Mbps",
    "TOTAL" : "50.0 Mbps",
    "DNS_RESPONSE" : "0.2 Mbps",
    "DNS" : "0.1 Mbps",
    "SYN" : "0.4 Mbps",
    "SSDP" : "0.1 Mbps",
    "NTP" : "0.1 Mbps",
    "OTHER" : "8.0 Mbps",
    "FRAG" : "0.1 Mbps",
    "CUSTOM" : "0.1 Mbps",
    "LARGE_SYN" : "0.1 Mbps",
    "ICMP" : "0.1 Mbps"
  }
},
"ipRangeThresholds" : {
  "ppsThresholds" : {
    "UDP" : "10.0K PPS",
    "TCP" : "50.0K PPS",
    "TOTAL" : "50.0K PPS",
    "DNS_RESPONSE" : "0.3K PPS",
    "DNS" : "0.3K PPS",
    "SYN" : "0.5K PPS",
    "SSDP" : "0.3K PPS",
    "NTP" : "0.3K PPS",
    "OTHER" : "3.0K PPS",
    "FRAG" : "0.3K PPS",
    "CUSTOM" : "0.3K PPS",
    "LARGE_SYN" : "0.3K PPS",
    "ICMP" : "0.3K PPS"
  },
  "bandwidthThresholds" : {
    "UDP" : "10.0 Mbps",
    "TCP" : "50.0 Mbps",
    "TOTAL" : "50.0 Mbps",
    "DNS_RESPONSE" : "0.2 Mbps",
    "DNS" : "0.1 Mbps",
    "SYN" : "0.4 Mbps",
    "SSDP" : "0.1 Mbps",
    "NTP" : "0.1 Mbps",
    "OTHER" : "8.0 Mbps",
    "FRAG" : "0.1 Mbps",
    "CUSTOM" : "0.1 Mbps",
    "LARGE_SYN" : "0.1 Mbps",
    "ICMP" : "0.1 Mbps"
  }
},
"lastUpdate" : "2023-10-09T07:06:36Z"
}, {
  "singleIpThresholds" : {

```

```

"ppsThresholds" : {
    "UDP" : "10.0K PPS",
    "TCP" : "50.0K PPS",
    "TOTAL" : "50.0K PPS",
    "DNS_RESPONSE" : "0.3K PPS",
    "DNS" : "0.3K PPS",
    "SYN" : "0.5K PPS",
    "SSDP" : "0.3K PPS",
    "NTP" : "0.3K PPS",
    "OTHER" : "3.0K PPS",
    "FRAG" : "0.3K PPS",
    "CUSTOM" : "0.3K PPS",
    "LARGE_SYN" : "0.3K PPS",
    "ICMP" : "0.3K PPS"
},
"bandwidthThresholds" : {
    "UDP" : "10.0 Mbps",
    "TCP" : "50.0 Mbps",
    "TOTAL" : "50.0 Mbps",
    "DNS_RESPONSE" : "0.2 Mbps",
    "DNS" : "0.1 Mbps",
    "SYN" : "0.4 Mbps",
    "SSDP" : "0.1 Mbps",
    "NTP" : "0.1 Mbps",
    "OTHER" : "8.0 Mbps",
    "FRAG" : "0.1 Mbps",
    "CUSTOM" : "0.1 Mbps",
    "LARGE_SYN" : "0.1 Mbps",
    "ICMP" : "0.1 Mbps"
},
"ipRangeThresholds" : {
    "ppsThresholds" : {
        "UDP" : "10.0K PPS",
        "TCP" : "50.0K PPS",
        "TOTAL" : "50.0K PPS",
        "DNS_RESPONSE" : "0.3K PPS",
        "DNS" : "0.3K PPS",
        "SYN" : "0.5K PPS",
        "SSDP" : "0.3K PPS",
        "NTP" : "0.3K PPS",
        "OTHER" : "3.0K PPS",
        "FRAG" : "0.3K PPS",
        "CUSTOM" : "0.3K PPS",
        "LARGE_SYN" : "0.3K PPS",
        "ICMP" : "0.3K PPS"
},
    "bandwidthThresholds" : {
        "UDP" : "10.0 Mbps",
        "TCP" : "50.0 Mbps",
        "TOTAL" : "50.0 Mbps",
        "DNS_RESPONSE" : "0.2 Mbps",
        "DNS" : "0.1 Mbps",
        "SYN" : "0.4 Mbps",
        "SSDP" : "0.1 Mbps",
        "NTP" : "0.1 Mbps",
        "OTHER" : "8.0 Mbps",
        "FRAG" : "0.1 Mbps",
        "CUSTOM" : "0.1 Mbps",
    }
}

```

```

        "LARGE_SYN" : "0.1 Mbps",
        "ICMP" : "0.1 Mbps"
    }
},
"lastUpdate" : "2022-09-01T08:30:14Z"
} ]
}, {
"policyRevisions" : [ {
"singleIpThresholds" : {
"ppsThresholds" : {
"UDP" : "10.0K PPS",
"TCP" : "50.0K PPS",
"TOTAL" : "50.0K PPS",
"DNS_RESPONSE" : "0.3K PPS",
"DNS" : "0.3K PPS",
"SYN" : "0.5K PPS",
"SSDP" : "0.3K PPS",
"NTP" : "0.3K PPS",
"OTHER" : "3.0K PPS",
"FRAG" : "0.3K PPS",
"CUSTOM" : "0.3K PPS",
"LARGE_SYN" : "0.3K PPS",
"ICMP" : "0.3K PPS"
},
"bandwidthThresholds" : {
"UDP" : "10.0 Mbps",
"TCP" : "50.0 Mbps",
"TOTAL" : "50.0 Mbps",
"DNS_RESPONSE" : "0.2 Mbps",
"DNS" : "0.1 Mbps",
"SYN" : "0.4 Mbps",
"SSDP" : "0.1 Mbps",
"NTP" : "0.1 Mbps",
"OTHER" : "8.0 Mbps",
"FRAG" : "0.1 Mbps",
"CUSTOM" : "0.1 Mbps",
"LARGE_SYN" : "0.1 Mbps",
"ICMP" : "0.1 Mbps"
}
},
"ipRangeThresholds" : {
"ppsThresholds" : {
"UDP" : "10.0K PPS",
"TCP" : "50.0K PPS",
"TOTAL" : "50.0K PPS",
"DNS_RESPONSE" : "0.3K PPS",
"DNS" : "0.3K PPS",
"SYN" : "0.5K PPS",
"SSDP" : "0.3K PPS",
"NTP" : "0.3K PPS",
"OTHER" : "3.0K PPS",
"FRAG" : "0.3K PPS",
"CUSTOM" : "0.3K PPS",
"LARGE_SYN" : "0.3K PPS",
"ICMP" : "0.3K PPS"
},
"bandwidthThresholds" : {
"UDP" : "10.0 Mbps",
"TCP" : "50.0 Mbps",

```

```

        "TOTAL" : "50.0 Mbps",
        "DNS_RESPONSE" : "0.2 Mbps",
        "DNS" : "0.1 Mbps",
        "SYN" : "0.4 Mbps",
        "SSDP" : "0.1 Mbps",
        "NTP" : "0.1 Mbps",
        "OTHER" : "8.0 Mbps",
        "FRAG" : "0.1 Mbps",
        "CUSTOM" : "0.1 Mbps",
        "LARGE_SYN" : "0.1 Mbps",
        "ICMP" : "0.1 Mbps"
    }
},
"lastUpdate" : "2023-10-09T07:06:36Z"
}, {
    "singleIpThresholds" : {
        "ppsThresholds" : {
            "UDP" : "10.0K PPS",
            "TCP" : "50.0K PPS",
            "TOTAL" : "50.0K PPS",
            "DNS_RESPONSE" : "0.3K PPS",
            "DNS" : "0.3K PPS",
            "SYN" : "0.5K PPS",
            "SSDP" : "0.3K PPS",
            "NTP" : "0.3K PPS",
            "OTHER" : "3.0K PPS",
            "FRAG" : "0.3K PPS",
            "CUSTOM" : "0.3K PPS",
            "LARGE_SYN" : "0.3K PPS",
            "ICMP" : "0.3K PPS"
        },
        "bandwidthThresholds" : {
            "UDP" : "10.0 Mbps",
            "TCP" : "50.0 Mbps",
            "TOTAL" : "50.0 Mbps",
            "DNS_RESPONSE" : "0.2 Mbps",
            "DNS" : "0.1 Mbps",
            "SYN" : "0.4 Mbps",
            "SSDP" : "0.1 Mbps",
            "NTP" : "0.1 Mbps",
            "OTHER" : "8.0 Mbps",
            "FRAG" : "0.1 Mbps",
            "CUSTOM" : "0.1 Mbps",
            "LARGE_SYN" : "0.1 Mbps",
            "ICMP" : "0.1 Mbps"
        }
},
"ipRangeThresholds" : {
    "ppsThresholds" : {
        "UDP" : "10.0K PPS",
        "TCP" : "50.0K PPS",
        "TOTAL" : "50.0K PPS",
        "DNS_RESPONSE" : "0.3K PPS",
        "DNS" : "0.3K PPS",
        "SYN" : "0.5K PPS",
        "SSDP" : "0.3K PPS",
        "NTP" : "0.3K PPS",
        "OTHER" : "3.0K PPS",
        "FRAG" : "0.3K PPS",
        "CUSTOM" : "0.3K PPS",
        "LARGE_SYN" : "0.3K PPS",
        "ICMP" : "0.3K PPS"
    }
}
}

```

```

    "CUSTOM" : "0.3K PPS",
    "LARGE_SYN" : "0.3K PPS",
    "ICMP" : "0.3K PPS"
  },
  "bandwidthThresholds" : {
    "UDP" : "10.0 Mbps",
    "TCP" : "50.0 Mbps",
    "TOTAL" : "50.0 Mbps",
    "DNS_RESPONSE" : "0.2 Mbps",
    "DNS" : "0.1 Mbps",
    "SYN" : "0.4 Mbps",
    "SSDP" : "0.1 Mbps",
    "NTP" : "0.1 Mbps",
    "OTHER" : "8.0 Mbps",
    "FRAG" : "0.1 Mbps",
    "CUSTOM" : "0.1 Mbps",
    "LARGE_SYN" : "0.1 Mbps",
    "ICMP" : "0.1 Mbps"
  }
},
"lastUpdate" : "2022-09-01T08:30:14Z"
} ]
}
]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
7101 - Policy not found

Models

Methods

Table of Contents

1. [ApiError](#)
 2. [ApiErrorResponse](#)
 3. [ApiErrorSource](#)
 4. [DetectionPolicyResponse](#)
 5. [MonitoringPolicyRevisionDto](#)
 6. [MonitoringPolicyRevisionResponse](#)
 7. [SecurityPolicyResponse](#)
-

-
8. SecurityPolicyResponse_singleIpThresholds
 9. SecurityPolicyRevisionResponse
 10. inline_response_200
 11. inline_response_200_1

ApiError

id (optional)
String
 Globally unique error id.
 example: 01234567-0123-0123-0123456789ab
 status (optional)
String
 HTTP status code
 example: 404
 code (optional)
String
 Error code
 example: ERROR_2002
 message (optional)
String
 Detailed error message
 example: Site 123456 not found
 source (optional)
ApiErrorSource

ApiErrorResponse

errors (optional)
array[**ApiError**]

ApiErrorSource

Pointer to source of error
pointer (optional)
String
a JSON Pointer [RFC6901] to the erroneous JSON element in the request payload
example: \$.data[0].fieldName
parameter (optional)
String
The name of erroneous query/path parameter name
example: extSiteId

DetectionPolicyResponse

data (optional)
map[String, array[map[String, String]]]
example: {"TOTAL":[], "OTHER":[{"amount":"150.0 Mbps", "time":"Over 30 sec"}, {"amount":"10.0K PPS", "time":"Over 45 sec"}, {"amount":"30.0K PPS", "time":"Over 15 sec"}, {"TCP": [{"amount":"200.0 Mbps", "time":"Over 30 sec"}, {"amount":"70.0K PPS", "time":"Over 30 sec"}, {"amount":"100.0K PPS", "time":"Over 15 sec"}], "UDP": [{"amount":"200.0 Mbps", "time":"Over 30 sec"}, {"amount":"90.0 Mbps", "time":"Over 60 sec"}, {"amount":"80.0K PPS", "time":"Over 45 sec"}], "FRAG": [{"amount":"25.0 Mbps", "time":"Over 30 sec"}, {"amount":"40.0 Mbps", "time":"Over 15 sec"}, {"amount":"10.0K PPS", "time":"Over 30 sec"}], "DNS": [{"amount":"10.0K PPS", "time":"Over 30 sec"}, {"amount":"20.0K PPS", "time":"Over 30 sec"}, {"amount":"25.0K PPS", "time":"Over 15 sec"}], "SYN": [{"amount":"20.0K PPS", "time":"Over 30 sec"}, {"amount":"17.0K PPS", "time":"Over 15 sec"}]}]

```
S","time":"Over 75 sec"}],"LARGE_SYN": [{"amount": "25.0 Mbps", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "10.0K PPS", "time": "Over 30 sec"}], "SSDP": [{"amount": "25.0 Mbps", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "10.0K PPS", "time": "Over 30 sec"}], "NTP": [{"amount": "25.0 Mbps", "time": "Over 45 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "10.0K PPS", "time": "Over 30 sec"}], "ICMP": [{"amount": "25.0 Mbps", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "20.0K PPS", "time": "Over 30 sec"}]}
```

MonitoringPolicyRevisionDto

data (optional)
`map[String, array[map[String, String]]]`

Data

lastUpdate (optional)

`String`

LastUpdated time

MonitoringPolicyRevisionResponse

policyRevisions (optional)

`array[MonitoringPolicyRevisionDto]`

example: [{"data": {"TCP": [{"amount": "100.0K PPS", "time": "Over 15 sec"}, {"amount": "70.0K PPS", "time": "Over 30 sec"}, {"amount": "200.0 Mbps", "time": "Over 30 sec"}], "UDP": [{"amount": "80.0K PPS", "time": "Over 45 sec"}, {"amount": "200.0 Mbps", "time": "Over 30 sec"}, {"amount": "90.0 Mbps", "time": "Over 60 sec"}], "OTHER": [{"amount": "30.0K PPS", "time": "Over 15 sec"}, {"amount": "10.0K PPS", "time": "Over 45 sec"}, {"amount": "150.0 Mbps", "time": "Over 30 sec"}], "FRAG": [{"amount": "10.0K PPS", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "25.0 Mbps", "time": "Over 30 sec"}], "DNS": [{"amount": "25.0K PPS", "time": "Over 15 sec"}, {"amount": "10.0K PPS", "time": "Over 30 sec"}], "SYN": [{"amount": "20.0K PPS", "time": "Over 30 sec"}, {"amount": "17.0K PPS", "time": "Over 75 sec"}], "LARGE_SYN": [{"amount": "10.0K PPS", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "25.0 Mbps", "time": "Over 30 sec"}], "SSDP": [{"amount": "10.0K PPS", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "25.0 Mbps", "time": "Over 30 sec"}], "NTP": [{"amount": "10.0K PPS", "time": "Over 30 sec"}, {"amount": "40.0 Mbps", "time": "Over 15 sec"}, {"amount": "25.0 Mbps", "time": "Over 30 sec"}]}, "lastUpdate": "2023-05-02T06:18:51Z"]}

SecurityPolicyResponse

singleIpThresholds (optional)

`array[SecurityPolicyResponse_singleIpThresholds]`

thresholds for IP

ipRangeThresholds (optional)

`array[SecurityPolicyResponse_singleIpThresholds]`

thresholds for Subnet

lastUpdate (optional)

`String`

LastUpdated time

SecurityPolicyResponse_singleIpThresholds

ppsThresholds (optional)

`map[String, String]`

bandwidthThresholds (optional)

`map[String, String]`

SecurityPolicyRevisionResponse

policyRevisions (optional)

array[SecurityPolicyResponse]

example: [{"singleIpThresholds": {"ppsThresholds": {"UDP": "10.0K PPS", "TCP": "50.0K PPS", "TOTAL": "50.0K PPS", "DNS_RESPONSE": "0.3K PPS", "DNS": "0.3K PPS", "SYN": "0.5K PPS", "SSDP": "0.3K PPS", "NTP": "0.3K PPS", "OTHER": "3.0K PPS", "FRAG": "0.3K PPS", "CUSTOM": "0.3K PPS", "LARGE_SYN": "0.3K PPS", "ICMP": "0.3K PPS"}, "bandwidthThresholds": {"UDP": "10.0 Mbps", "TCP": "50.0 Mbps", "TOTAL": "50.0 Mbps", "DNS_RESPONSE": "0.2 Mbps", "DNS": "0.1 Mbps", "SYN": "0.4 Mbps", "SSDP": "0.1 Mbps", "NTP": "0.1 Mbps", "OTHER": "8.0 Mbps", "FRAG": "0.1 Mbps", "CUSTOM": "0.1 Mbps", "LARGE_SYN": "0.1 Mbps", "ICMP": "0.1 Mbps"}, "ipRangeThresholds": {"ppsThresholds": {"UDP": "10.0K PPS", "TCP": "50.0K PPS", "TOTAL": "50.0K PPS", "DNS_RESPONSE": "0.3K PPS", "DNS": "0.3K PPS", "SYN": "0.5K PPS", "SSDP": "0.3K PPS", "NTP": "0.3K PPS", "OTHER": "3.0K PPS", "FRAG": "0.3K PPS", "CUSTOM": "0.3K PPS", "LARGE_SYN": "0.3K PPS", "ICMP": "0.3K PPS"}, "bandwidthThresholds": {"UDP": "10.0 Mbps", "TCP": "50.0 Mbps", "TOTAL": "50.0 Mbps", "DNS_RESPONSE": "0.2 Mbps", "DNS": "0.1 Mbps", "SYN": "0.4 Mbps", "SSDP": "0.1 Mbps", "NTP": "0.1 Mbps", "OTHER": "8.0 Mbps", "FRAG": "0.1 Mbps", "CUSTOM": "0.1 Mbps", "LARGE_SYN": "0.1 Mbps", "ICMP": "0.1 Mbps"}}, "lastUpdate": "2023-10-09T07:06:36Z"}, {"singleIpThresholds": {"ppsThresholds": {"UDP": "10.0K PPS", "TCP": "50.0K PPS", "TOTAL": "50.0K PPS", "DNS_RESPONSE": "0.3K PPS", "DNS": "0.3K PPS", "SYN": "0.5K PPS", "SSDP": "0.3K PPS", "NTP": "0.3K PPS", "OTHER": "3.0K PPS", "FRAG": "0.3K PPS", "CUSTOM": "0.3K PPS", "LARGE_SYN": "0.3K PPS", "ICMP": "0.3K PPS"}, "bandwidthThresholds": {"UDP": "10.0 Mbps", "TCP": "50.0 Mbps", "TOTAL": "50.0 Mbps", "DNS_RESPONSE": "0.2 Mbps", "DNS": "0.1 Mbps", "SYN": "0.4 Mbps", "SSDP": "0.1 Mbps", "NTP": "0.1 Mbps", "OTHER": "8.0 Mbps", "FRAG": "0.1 Mbps", "CUSTOM": "0.1 Mbps", "LARGE_SYN": "0.1 Mbps", "ICMP": "0.1 Mbps"}, "ipRangeThresholds": {"ppsThresholds": {"UDP": "10.0K PPS", "TCP": "50.0K PPS", "TOTAL": "50.0K PPS", "DNS_RESPONSE": "0.3K PPS", "DNS": "0.3K PPS", "SYN": "0.5K PPS", "SSDP": "0.3K PPS", "NTP": "0.3K PPS", "OTHER": "3.0K PPS", "FRAG": "0.3K PPS", "CUSTOM": "0.3K PPS", "LARGE_SYN": "0.3K PPS", "ICMP": "0.3K PPS"}, "bandwidthThresholds": {"UDP": "10.0 Mbps", "TCP": "50.0 Mbps", "TOTAL": "50.0 Mbps", "DNS_RESPONSE": "0.2 Mbps", "DNS": "0.1 Mbps", "SYN": "0.4 Mbps", "SSDP": "0.1 Mbps", "NTP": "0.1 Mbps", "OTHER": "8.0 Mbps", "FRAG": "0.1 Mbps", "CUSTOM": "0.1 Mbps", "LARGE_SYN": "0.1 Mbps", "ICMP": "0.1 Mbps"}}, "lastUpdate": "2022-09-01T08:30:14Z"}]

inline_response_200

inline_response_200_1

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

DDoSProtectionForIndividualIPs

- post /api/prov/v1/ddos-protection/edge-ip/add/cname
- post /api/prov/v1/ddos-protection/edge-ip/add/dns-with-cname
- post /api/prov/v1/ddos-protection/edge-ip/add/dns-with-ip
- post /api/prov/v1/ddos-protection/edge-ip/add/ip
- post /api/prov/v1/ddos-protection/edge-ip/edit/cname
- post /api/prov/v1/ddos-protection/edge-ip/edit/dns-with-cname
- post /api/prov/v1/ddos-protection/edge-ip/edit/dns-with-ip
- post /api/prov/v1/ddos-protection/edge-ip/edit/ip
- post /api/prov/v1/ddos-protection/edge-ip/edit/ha-protocol
- post /api/prov/v1/ddos-protection/edge-ip/edit/monitoring-settings
- post /api/prov/v1/ddos-protection/edge-ip/remove

DDoSProtectionForIndividualIPs

```
post /api/prov/v1/ddos-protection/edge-ip/add/cname
```

Protected IP over TCP - add by CNAME (addSipByCname)

Use this operation to onboard a CNAME record to the 'IP Protection over TCP' service. If successful, the operation will return the generated Edge IP.

Query parameters

cname (required)

Query Parameter

— CNAME record to onboard to service

enable_ha_protocol (optional)

Query Parameter

— Provide 'true' to enable the Proxy Protocol setting (disabled by default)

description (optional)

Query Parameter

— Optional description for the generated Edge IP

monitoring_type (optional)

Query Parameter

— Monitoring type for the Edge IP. Possible values: 'ICMP' (default), 'TCP' or 'NONE'

tcp_monitoring_port (optional)

Query Parameter

— Port to use for TCP monitoring of the Edge IP. Required only when TCP monitoring is used. format: int32

Return type

inline_response_200

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7002 - IP Protection quota exceeded
7007 - This entity is already protected</br>7008 - CNAME cannot be used [inline_response_200](#)

```
post /api/prov/v1/ddos-protection/edge-ip/add/dns-with-cname
```

Protected IP over TCP - add by DNS and CNAME (addSipByDnsAndCname)

Use this operation to onboard a CNAME record with an associated DNS name to the 'IP Protection over TCP' service. If DNS check is enabled, the response will include the list of resolved CNAME records for the provided domain name, and the operation will only succeed if the provided CNAME will be included in that list. If successful, the operation will return the generated Edge IP.

Query parameters

`dns_name` (required)

Query Parameter

— Domain name to onboard to service

`cname` (required)

Query Parameter

— CNAME record to onboard to service

`disable_dns_check` (optional)

Query Parameter

— Provide 'true' to disable DNS resolution check (enabled by default)

`enable_ha_protocol` (optional)

Query Parameter

— Provide 'true' to enable the Proxy Protocol setting (disabled by default)

`description` (optional)

Query Parameter

— description for the generated Edge IP

`monitoring_type` (optional)

Query Parameter

— Monitoring type for the Edge IP. Possible values: 'ICMP' (default), 'TCP' or 'NONE'

`tcp_monitoring_port` (optional)

Query Parameter

— Port to use for TCP monitoring of the Edge IP. Required only when TCP monitoring is used. format: int32

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 3015 - Internal error
 7002 - IP Protection quota exceeded
 7004 - Domain name cannot be used
 7005 - No DNS records found
 7007 - This entity is already protected
 7008 - CNAME cannot be used
 7009 - CNAME not among DNS resolved records

inline_response_200_1

```
post /api/prov/v1/ddos-protection/edge-ip/add/dns-with-ip
```

Protected IP over TCP - add by DNS and origin IP (addSipByDnsAndIp)

Use this operation to onboard a public origin IP with an associated DNS name to the 'IP Protection over TCP' service. If DNS check is enabled, the response will include the list of resolved IPs for the provided domain name, and the operation will only succeed if the provided origin IP will be included in that list. If successful, the operation will return the generated Edge IP.

Query parameters

dns_name (required)

Query Parameter

— Domain name to onboard to service

origin_ip (required)

Query Parameter

— Public origin IP to onboard to service

disable_dns_check (optional)

Query Parameter

— Provide 'true' to disable DNS resolution check (enabled by default)

enable_ha_protocol (optional)

Query Parameter

— Provide 'true' to enable the Proxy Protocol setting (disabled by default)

description (optional)

Query Parameter

— description for the generated Edge IP

monitoring_type (optional)

Query Parameter

— Monitoring type for the Edge IP. Possible values: 'ICMP' (default), 'TCP' or 'NONE'

tcp_monitoring_port (optional)

Query Parameter

— Port to use for TCP monitoring of the Edge IP. Required only when TCP monitoring is used. format: int32

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7001 - IP not among DNS resolved records
7002 - IP Protection quota exceeded
7003 - IP cannot be used
7004 - Domain name cannot be used
7005 - No DNS records found
7007 - This entity is already protected [inline_response_200_2](#)

```
post /api/prov/v1/ddos-protection/edge-ip/add/ip
```

Protected IP over TCP - add by origin IP (addSipByIp)

Use this operation to onboard a public origin IP to the 'IP Protection over TCP' service. If successful, the operation will return the generated Edge IP.

Query parameters

origin_ip (required)

Query Parameter

— Public origin IP to onboard to service

enable_ha_protocol (optional)

Query Parameter

— Provide 'true' to enable the Proxy Protocol setting (disabled by default)

description (optional)

Query Parameter

— description for the generated Edge IP

monitoring_type (optional)

Query Parameter

— Monitoring type for the Edge IP. Possible values: 'ICMP' (default), 'TCP' or 'NONE'

tcp_monitoring_port (optional)

Query Parameter

— Port to use for TCP monitoring of the Edge IP. Required only when TCP monitoring is used. format: int32

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7002 - IP Protection quota exceeded
7003 - IP cannot be used
7007 - This entity is already protected [inline_response_200_3](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/cname
```

Protected IP over TCP - edit by CNAME (editSipByCname)

Use this operation to assign a new CNAME record to the provided Edge IP under the 'IP Protection over TCP' service. This operation is also able to change the type of the entity protected by the provided Edge IP (Any existing combination of Origin IP/CNAME and DNS will be overwritten). If successful, the operation will return the Edge IP. WARNING: Any entity already protected by this Edge IP prior to the change will no longer be protected once modification is successful, unless duplicate protection is used.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

cname (required)

Query Parameter

— CNAME to onboard to service

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 3015 - Internal error
 7003 - IP cannot be used
 7006 - Edge IP not found
 7007 - This entity is already protected
 7008 - CNAME cannot be used [inline_response_200](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/dns-with cname
```

Protected IP over TCP - edit by DNS and CNAME (editSipByDnsAndCname)

Use this operation to assign a new CNAME record with an associated DNS name to the provided Edge IP under the 'IP Protection over TCP' service.

This operation is also able to change the type of the entity protected by the provided Edge IP (Any existing combination of Origin IP/CNAME and DNS name will be overwritten).

If DNS check is enabled, the response will include the list of resolved CNAME records for the provided domain name, and the operation will only succeed if the provided CNAME is included in that list.

If successful, the operation will return the Edge IP.

WARNING: Any entity already protected by this Edge IP prior to the change will no longer be protected once modification is successful, unless duplicate protection is used.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

dns_name (required)

Query Parameter

— Domain name to onboard to service

cname (required)

Query Parameter

— CNAME to onboard to service

disable_dns_check (optional)

Query Parameter

— Provide 'true' to disable DNS resolution check (enabled by default)

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 3015 - Internal error
 7003 - IP cannot be used
 7004 - Domain name cannot be used
 7005 - No DNS records found
 7006 - Edge IP not found
 7007 - This entity is already protected
 7008 - CNAME cannot be used
 7009 - CNAME not among DNS resolved records

[inline_response_200_1](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/dns-with-ip
```

Protected IP over TCP - edit by DNS and origin IP (editSipByDnsAndIp)

Use this operation to assign a new origin IP with an associated DNS name to the provided Edge IP under the 'IP Protection over TCP' service. This operation is also able to change the type of the entity protected by the provided Edge IP (Any existing combination of Origin IP/CNAME and DNS name will be overwritten). If DNS check is enabled, the response will include the list of resolved IPs for the provided domain name, and the operation will only succeed if the provided origin IP is included in that list. If successful, the operation will return the Edge IP. WARNING: Any entity already protected by this Edge IP prior to the change will no longer be protected once modification is successful, unless duplicate protection is used.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

dns_name (required)

Query Parameter

— Domain name to onboard to service

origin_ip (required)

Query Parameter

— Public origin IP to onboard to service

disable_dns_check (optional)

Query Parameter

— Provide 'true' to disable DNS resolution check (enabled by default)

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7001 - IP not among DNS resolved records
7003 - IP cannot be used
7004 - Domain name cannot be used
7005 - No DNS records found
7006 - Edge IP not found
7007 - This entity is already protected [inline_response_200_2](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/ip
```

Protected IP over TCP - edit by origin IP (editSipByIp)

Use this operation to assign a new origin IP to the provided Edge IP under the 'IP Protection over TCP' service. This operation is also able to change the type of the entity protected by the provided Edge IP (Any existing combination of Origin IP/CNAME and DNS name will be overwritten). If successful, the operation will return the Edge IP. WARNING: Any entity already protected by this Edge IP prior to the change will no longer be protected once modification is successful, unless duplicate protection is used.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

origin_ip (required)

Query Parameter

— Public origin IP to onboard to service

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7003 - IP cannot be used
7006 - Edge IP not found
7007 - This entity is already protected [inline_response_200_3](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/ha-protocol
```

Protected IP over TCP - edit HA protocol setting (editSipHaProtocol)

Use this operation on the provided Edge IP to toggle its HA Protocol setting on or off. By default, this setting is disabled during onboarding unless explicitly set to 'true'. WARNING: Do not modify this setting unless you are familiar with the proxy protocol and understand the implications of enabling or disabling it for your account.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

enable_ha_protocol (required)

Query Parameter

— Provide 'true' to enable the Proxy Protocol setting, 'false' to disable

Return type

ApiResult

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7003 - IP cannot be used
7006 - Edge IP not found [ApiResult](#)

```
post /api/prov/v1/ddos-protection/edge-ip/edit/monitoring-settings
```

Protected IP over TCP - edit monitoring settings (editSipMonitoringSettings)
Use this operation on the specified Edge IP to modify its monitoring settings.

Query parameters

`edge_ip` (required)

Query Parameter

— Imperva generated Edge IP

`monitoring_type` (required)

Query Parameter

— Monitoring type for the Edge IP. Possible values: 'ICMP' (default), 'TCP' or 'NONE'

`tcp_monitoring_port` (optional)

Query Parameter

— Port to use for TCP monitoring of the Edge IP. Required only when TCP monitoring is used. format: int32

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

res - contains the specific error code:
3015 - Internal error
7003 - IP cannot be used
7006 - Edge IP not found [ApiResult](#)

```
post /api/prov/v1/ddos-protection/edge-ip/remove
```

Protected IP over TCP - remove (removeSip)

Use this operation on the provided Edge IP to remove it from the 'IP Protection over TCP' service.

WARNING: Any entity already protected by this Edge IP will no longer be protected once the operation is successful, unless duplicate protection was enabled and used.

Query parameters

edge_ip (required)

Query Parameter

— Imperva generated Edge IP

Return type

[ApiResult](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : [ {
    "key" : { }
  }, {
    "key" : { }
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
3015 - Internal error
7003 - IP cannot be used
7006 - Edge IP

not found [ApiResult](#)

Models

Methods

Table of Contents

1. [ApiResult](#)
2. [ApiResultInfraProtectSipCname](#)
3. [ApiResultInfraProtectSipDnsWithCname](#)
4. [ApiResultInfraProtectSipDnsWithIp](#)
5. [ApiResultInfraProtectSipIp](#)
6. [inline_response_200](#)
7. [inline_response_200_1](#)
8. [inline_response_200_2](#)
9. [inline_response_200_3](#)

ApiResult

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
[array\[map\[String, Object\]\]](#)

ApiResultInfraProtectSipCname

res (optional)
Integer
 res - contains specific error code format: int32
 example: 0
 res_message (optional)
String
 example: OK
 debug_info (optional)
[array\[map\[String, Object\]\]](#)
 edge_ip (optional)
String
 example: 172.17.14.1
 cname (optional)
String
 example: imperva.test.com

ApiResultInfraProtectSipDnsWithCname

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

edge_ip (optional)

String

example: 172.17.14.1

resolved_cnames (optional)

array[String]

cname (optional)

String

example: imperva.test.com

ApiResultInfraProtectSipDnsWithIp

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

edge_ip (optional)

String

example: 172.17.14.1

resolved_ips (optional)

array[String]

origin_ip (optional)

String

example: 157.166.249.10

ApiResultInfraProtectSipIp

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

edge_ip (optional)

String

example: 172.17.14.1

origin_ip (optional)

String

example: 1.2.3.4

inline_response_200

```
inline_response_200_1
```

```
inline_response_200_2
```

```
inline_response_200_3
```

Imperva Protected IP API

Manage your protected IPs. Imperva's IP Protection service enables you to protect specific IPs from network layer 3 and 4 DDoS attacks. For full feature documentation, see [Settings: DDoS Protection for Individual IPs](#).

Version: 1.0.0

BasePath:/api/v2/ddos-protection

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

ProtectedIPOverGREIPinIP

- post /edge-ip
- delete /edge-ip/{edgeIp}
- put /edge-ip/{edgeIp}
- get /edge-ip

ProtectedIPOverTCPIP

- post /edge-ip/tcp-ip
- delete /edge-ip/tcp-ip/{protectedIp}
- put /edge-ip/tcp-ip/{protectedIp}
- get /edge-ip/tcp-ip

ProtectedIPOverGREIPinIP

```
post /edge-ip
```

Add protected IP over GRE/IPinIP (addProtectedIp)

Onboard an IP to the DDoS Protection for Individual IP service.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

edgelp (required)
Form Parameter

—
description (required)
Form Parameter

—
ipProtectionType (required)
Form Parameter

—
monitoringType (required)
Form Parameter

—
emailNotifications (required)
Form Parameter

—
totalTrafficBandwidth (required)
Form Parameter

—
customTrafficBandwidth (required)
Form Parameter

— format: int32

tcpDistribution (required)
Form Parameter

— format: int32

udpDistribution (required)
Form Parameter

— format: int32

otherDistribution (required)
Form Parameter

— format: int32

ipsecProtocol (required)
Form Parameter

—

Return type

AddOrEditResponse

Example data

Content-Type: application/json

```
{  
  "res" : 0,
```

```

    "res_message" : "OK",
    "debug_info" : {
        "id-info" : "999999"
    },
    "edge_ip" : "172.17.14.2",
    "origin_ip" : "182.10.20.30"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation AddOrEditResponse

```
delete /edge-ip/{edgeIp}
```

Remove protected IP over GRE/IPinIP (deleteProtectedIp)

Remove a protected IP from the DDoS Protection for Individual IP service.

Path parameters

edgelp (required)

Path Parameter

— The Imperva global anycast protected IP. This is the IP to use for any internet-facing access to your service

Return type

DeleteResponse

Example data

Content-Type: application/json

```
{
    "res" : 0,
    "res_message" : "OK",
    "debug_info" : {
        "id-info" : "999999"
    }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [DeleteResponse](#)

```
put /edge-ip/{edgeIp}
```

Edit protected IP over GRE/IPinIP (editProtectedIp)
Edit the protected IP over GRE/IPinIP.

Path parameters

edgelp (required)

Path Parameter

— The Imperva global anycast protected IP. This is the IP to use for any internet-facing access to your service

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

description (required)

Form Parameter

ipProtectionType (required)

Form Parameter

monitoringType (required)

Form Parameter

emailNotifications (required)

Form Parameter

totalTrafficBandwidth (required)

Form Parameter

customTrafficBandwidth (required)

Form Parameter

— format: int32

tcpDistribution (required)

Form Parameter

```

— format: int32
  udpDistribution (required)
  Form Parameter
— format: int32
  otherDistribution (required)
  Form Parameter
— format: int32
  ipsecProtocol (required)
  Form Parameter
—

```

Return type

AddOrEditResponse

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : {
    "id-info" : "999999"
  },
  "edge_ip" : "172.17.14.2",
  "origin_ip" : "182.10.20.30"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation AddOrEditResponse

```
get /edge-ip
```

Retrieve protected IP (getProtectedIp)
Retrieve details of the protected IP.

Consumes

This API call consumes the following media types via the Content-Type request header:

-
- application/x-www-form-urlencoded

Form parameters

impervaAnycastIp (required)

Form Parameter

Return type

ProtectedIpDetails

Example data

Content-Type: application/json

```
{  
    "accountId" : 50055,  
    "originPublicIp" : "192.10.50.98",  
    "description" : "Main server.",  
    "impervaAnycastIp" : "3.3.3.4",  
    "id" : 4  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation ProtectedIpDetails

ProtectedIPOverTCPIP

```
post /edge-ip/tcp-ip
```

Add protected IP over TCP Proxy (addSIP)
Onboard an IP to the DDoS Protection for Individual IP service.

Consumes

This API call consumes the following media types via the Content-Type request header:

-
- application/x-www-form-urlencoded

Form parameters

dns_name (required)

Form Parameter

—

ipOrCname (required)

Form Parameter

enable_ha_protocol (required)

Form Parameter

—

description (required)

Form Parameter

—

monitoringType (required)

Form Parameter

—

tcpMonitoringPort (required)

Form Parameter

— format: int32

disable_dns_check (required)

Form Parameter

—

Return type

AddOrEditResponse

Example data

Content-Type: application/json

```
{  
    "res" : 0,  
    "res_message" : "OK",  
    "debug_info" : {  
        "id-info" : "999999"  
    },  
    "edge_ip" : "172.17.14.2",  
    "origin_ip" : "182.10.20.30"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AddOrEditResponse](#)

```
delete /edge-ip/tcp-ip/{protectedIp}
```

Delete protected IP over TCP Proxy (deleteSIP)

Remove a protected IP (over TCP proxy) from the DDoS Protection for Individual IP service.

Path parameters

protectedIp (required)

Path Parameter

— The Imperva global anycast protected IP. This is the IP to use for any internet-facing access to your service

Return type

[DeleteResponse](#)

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : {
    "id-info" : "999999"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [DeleteResponse](#)

```
put /edge-ip/tcp-ip/{protectedIp}
```

Edit protected IP over TCP Proxy (editSIP)
Edit the protected IP.

Path parameters

protectedIp (required)

Path Parameter

— The Imperva global anycast protected IP. This is the IP to use for any internet-facing access to your service

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

dns_name (optional)

Form Parameter

ipOrCname (optional)

Form Parameter

disable_dns_check (optional)

Form Parameter

enable_ha_protocol (optional)

Form Parameter

monitoringType (optional)

Form Parameter

tcpMonitoringPort (optional)

Form Parameter

— format: int32

Return type

AddOrEditResponse

Example data

Content-Type: application/json

```
{
  "res" : 0,
  "res_message" : "OK",
  "debug_info" : {
    "id-info" : "999999"
  },
  "edge_ip" : "172.17.14.2",
  "origin_ip" : "182.10.20.30"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [AddOrEditResponse](#)

```
get /edge-ip/tcp-ip
```

Retrieve protected IP (getSIP)
Retrieve details of the protected IP.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

impervaAnycastIp (required)
Form Parameter

Return type

[ProtectedIpDetails](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 50055,
  "originPublicIp" : "192.10.50.98",
  "description" : "Main server.",
  "impervaAnycastIp" : "3.3.3.4",
  "id" : 4
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be

conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ProtectedIpDetails](#)

Models

Methods

Table of Contents

1. AddOrEditResponse
2. AddOrEditResponse_debug_info
3. DeleteResponse
4. ProtectedIpDetails
5. edgeip_body
6. edgeip_body_1
7. edgeip_edgeIp_body
8. edgeip_tcpip_body
9. edgeip_tcpip_body_1
10. tcpip_protectedIp_body

AddOrEditResponse

origin_ip
String

The origin server IP or CNAME that is protected.

example: 182.10.20.30

edge_ip

String

Imperva anycast IP address

example: 172.17.14.2

res

Integer

The operation's numeric result format: int32

example: 0

res_message

String

The result's message

example: OK

debug_info

[AddOrEditResponse_debug_info](#)

AddOrEditResponse_debug_info

id-info (optional)

String

example: 999999

DeleteResponse

res

Integer

The operation's numeric result format: int32

example: 0

res_message

String

The result's message

example: OK

debug_info

AddOrEditResponse_debug_info

ProtectedIpDetails

id

Long

Unique identifier of your service. format: int64

example: 4

originPublicIp

String

The origin server IP or CNAME that is protected.

example: 192.10.50.98

impervaAnycastIp

String

The Imperva global anycast protected IP, used for any internet-facing access to your service.

example: 3.3.3.4

accountId

Long

The account ID. format: int64

example: 50055

description

String

The name you assign to the service you want to protect. If you do not assign a name, your origin IP address or domain name is used.

example: Main server.

edgeip_body

impervaAnycastIp

String

The Imperva global anycast protected IP, used for any internet-facing access to your service.

edgeip_body_1

edgelp

String

The Imperva global anycast protected IP. This is the IP to use for any internet-facing access to your service
description (optional)

String

The name you assign to the service you want to protect. If you do not assign a name, your origin IP address or domain name is used.

ipProtectionType**String**

The connection method. Available values: GRE - for IP protection over GRE tunneling IPINIP - for IP protection over IP-in-IP

monitoringType (optional)**String**

The method for monitoring the connection to your origin server. Available values:

tunnelMonitoring,originMonitoring.

emailNotifications (optional)**Boolean**

Send email notifications when the connectivity status of your origin IP changes. Email notifications are sent to the addresses defined in your account settings. Available values: true, false.

totalTrafficBandwidth (optional)**String**

The estimated traffic bandwidth that you expect for your origin service. Available values: upTo50 - for up to 50 Mbps. upTo100 - for up to 100 Mbps. For other values, use the customTrafficBandwidth parameter.

customTrafficBandwidth (optional)**Integer**

The estimated traffic bandwidth that you expect for your origin service (in Mbps). format: int32

tcpDistribution (optional)**Integer**

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

udpDistribution (optional)**Integer**

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

otherDistribution (optional)**Integer**

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

ipsecProtocol (optional)**Boolean**

Enables support for the IP Security protocol. Available values: true, false

edgeip_edgeIp_body**description (optional)****String**

The name you assign to the service you want to protect. If you do not assign a name, your origin IP address or domain name is used.

ipProtectionType**String**

The connection method. Available values: GRE - for IP protection over GRE tunneling IPINIP - for IP protection over IP-in-IP

monitoringType (optional)**String**

The method for monitoring the connection to your origin server. Available values: tunnelMonitoring, originMonitoring.

emailNotifications (optional)**Boolean**

Send email notifications when the connectivity status of your origin IP changes. Email notifications are sent to the addresses defined in your account settings. Available values: true, false.

totalTrafficBandwidth (optional)**String**

The estimated traffic bandwidth that you expect for your origin service. Available values: upTo50 - for up to 50 Mbps. upTo100 - for up to 100 Mbps. For other values, use the customTrafficBandwidth parameter.

customTrafficBandwidth (optional)

Integer

The estimated traffic bandwidth that you expect for your origin service (in Mbps). format: int32

tcpDistribution (optional)

Integer

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

udpDistribution (optional)

Integer

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

otherDistribution (optional)

Integer

The estimated distribution percentage per protocol type that you expect for your origin service. The values for TCP, UDP, and other should total 100%. format: int32

ipsecProtocol (optional)

Boolean

Enables support for the IP Security protocol. Available values: true, false

edgeip_tcpip_body

impervaAnycastIp

String

The Imperva global anycast protected IP, used for any internet-facing access to your service.

edgeip_tcpip_body_1

dns_name (optional)

String

The name of the protected domain.

ipOrCname

String

The IP address or CNAME of the protected IP.

enable_ha_protocol

Boolean

Enables the Proxy Protocol for this IP, allowing Imperva to pass IP addresses of visiting clients on to your destination application or service by adding the Proxy Protocol header to the request. Requires support of the Proxy Protocol on the origin side. Do not activate this option if your server does not support it. Available values: true, false

description

String

The name you assign to the service you want to protect. If you do not assign a name, your origin IP address or domain name is used.

monitoringType

String

The method for monitoring the connection to your origin server. Available values: NONE, TCP, ICMP.

tcpMonitoringPort

Integer

The port on the origin server to use for monitoring. format: int32

disable_dns_check (optional)

Boolean

When set to false and both a DNS name and IP address are provided, Imperva checks that the DNS name resolves to the provided IP. When set to true, this validation is not performed.

tcpip_protectedIp_body

dns_name (optional)

String

The name of the protected domain.

ipOrCname (optional)

String

The IP address or CNAME of the protected IP.

disable_dns_check (optional)

Boolean

When set to false and both a DNS name and IP address are provided, Imperva checks that the DNS name resolves to the provided IP. When set to true, this validation is not performed.

enable_ha_protocol (optional)

Boolean

Enables the Proxy Protocol for this IP, allowing Imperva to pass IP addresses of visiting clients on to your destination application or service by adding the Proxy Protocol header to the request. Requires support of the Proxy Protocol on the origin side. Do not activate this option if your server does not support it. Available values:

true, false

monitoringType (optional)

String

The method for monitoring the connection to your origin server. Available values: NONE, TCP, ICMP.

tcpMonitoringPort (optional)

Integer

The port on the origin server to use for monitoring. format: int32

Connectivity Settings API Definition

This is the API for DDoS Protection for Networks connections. View and manage connections between Imperva's network and your origin network. For full feature documentation, see [Connectivity Settings](#).

Version: 1.0.0

BasePath:/api/v2/ddos-protection

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true

2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

ASNManagement

- post /asn
- delete /asn/{asnId}
- get /asn

AccountConnectionsManagement

- `get /account/{accountId}/connections`

OriginConnectivityManagement

- `post /origin-connectivity`
- `delete /origin-connectivity/{connectionId}`
- `put /origin-connectivity/{connectionId}`
- `get /origin-connectivity`

RoutingPolicyManagement

- `post /routing-policy`
- `delete /routing-policy/{routingPolicyId}`
- `put /routing-policy/{routingPolicyId}`
- `get /routing-policy`

ASNManagement

```
post /asn
```

Add ASN (addASN)
Adds an ASN.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/x-www-form-urlencoded`

Form parameters

asn (required)
Form Parameter
— format: int64
accountid (required)
Form Parameter
— format: int64

Return type

ASNDATA

Example data

Content-Type: application/json

```
{
  "asnNumber" : 123,
  "asnId" : 664
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ASNDATA](#)

```
delete /asn/{asnId}
```

Delete ASN (deleteASN)
Removes an ASN.

Path parameters

asnId (required)

Path Parameter

— The ASN's Imperva ID. The ASN ID is provided as part of the response when an ASN is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

[ASNDATA](#)

Example data

Content-Type: application/json

```
{
  "asnNumber" : 123,
  "asnId" : 664
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [ASNDATA](#)

```
get /asn
```

Retrieve ASN (getASN)

Retrieves details of the ASN.

Query parameters

asn (required)

Query Parameter

— The ASN number. format: int64

accountId (required)

Query Parameter

— The account ID. format: int64

Return type

[ASNDATA](#)

Example data

Content-Type: application/json

```
{
  "asnNumber" : 123,
  "asnId" : 664
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

Successful operation [ASNData](#)

AccountConnectionsManagement

```
get /account/{accountId}/connections
```

Retrieve account connections (getAccountConnections)
Retrieves the details of all connections defined in your account.

Path parameters

accountId (required)

Path Parameter

— The account ID. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

type (optional)

Form Parameter

—

Return type

[OriginConnectivityData](#)

Example data

Content-Type: application/json

```
{  
    "customerPublicIp" : "203.192.160.199",  
    "name" : "Main server",  
    "tunnelEndpoint" : "PRIMARY",  
    "id" : 170,  
    "type" : "BGP",  
    "popName" : "ogn",  
    "mtu" : 1476,
```

```

    "status" : "UP"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation OriginConnectivityData

OriginConnectivityManagement

```
post /origin-connectivity
```

Add connection (GRE tunnel) (addConnection)
Adds a connection between Imperva and your origin network.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

body (required)
Form Parameter

—
accountId (required)
Form Parameter
— format: int64

Return type

OriginConnectivityData

Example data

Content-Type: application/json

```
{
}
```

```

"customerPublicIp" : "203.192.160.199",
"name" : "Main server",
"tunnelEndpoint" : "PRIMARY",
"id" : 170,
"type" : "BGP",
"popName" : "ogn",
"mtu" : 1476,
"status" : "UP"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[Successful operation OriginConnectivityData](#)

```
delete /origin-connectivity/{connectionId}
```

Delete connection (GRE tunnel) (deleteConnection)
Removes the connection.

Path parameters

connectionId (required)

Path Parameter

— The connection's Imperva ID. The connection ID is provided as part of the response when a connection is first added. You can also retrieve it using the GET HTTP method. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

[OriginConnectivityData](#)

Example data

Content-Type: application/json

```
{
  "customerPublicIp" : "203.192.160.199",
  "name" : "Main server",
  "tunnelEndpoint" : "PRIMARY",
  "id" : 170,
  "type" : "BGP",
  "popName" : "ogn",
  "mtu" : 1476,
  "status" : "UP"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [OriginConnectivityData](#)

```
put /origin-connectivity/{connectionId}
```

Edit connection (GRE tunnel) (editConnection)
Edits the connection details.

Path parameters

connectionId (required)

Path Parameter

— The connection's Imperva ID. The connection ID is provided as part of the response when a connection is first added. You can also retrieve it using the GET HTTP method. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

body (required)

Form Parameter

Return type

OriginConnectivityData

Example data

Content-Type: application/json

```
{  
    "customerPublicIp" : "203.192.160.199",  
    "name" : "Main server",  
    "tunnelEndpoint" : "PRIMARY",  
    "id" : 170,  
    "type" : "BGP",  
    "popName" : "ogn",  
    "mtu" : 1476,  
    "status" : "UP"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation OriginConnectivityData

```
get /origin-connectivity
```

Retrieve connection (getConnection)

Retrieves details of the connection.

Query parameters

impervaAnycastIp (required)

Query Parameter

— The Imperva global anycast protected IP, used for any internet-facing access to your service.

accountId (required)

Query Parameter

— The account ID. format: int64

Return type

OriginConnectivityData

Example data

Content-Type: application/json

```
{
  "customerPublicIp" : "203.192.160.199",
  "name" : "Main server",
  "tunnelEndpoint" : "PRIMARY",
  "id" : 170,
  "type" : "BGP",
  "popName" : "ogn",
  "mtu" : 1476,
  "status" : "UP"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation OriginConnectivityData

RoutingPolicyManagement

```
post /routing-policy
```

Add routing policy (addPolicy)
Adds a routing policy.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

body (required)

Form Parameter

—
accountId (required)
Form Parameter
— format: int64

Return type

RoutingPolicyData

Example data

Content-Type: application/json

```
{
  "connectionId" : 139,
  "id" : 5,
  "asnId" : 660,
  "type" : "BGP"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [RoutingPolicyData](#)

```
delete /routing-policy/{routingPolicyId}
```

Delete routing policy (deletePolicy)
Removes a routing policy.

Path parameters

routingPolicyId (required)

Path Parameter

— The policy's Imperva ID. The policy ID is provided as part of the response when a routing policy is first added. You can also retrieve it using GET HTTP method. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

OriginConnectivityData

Example data

Content-Type: application/json

```
{
  "customerPublicIp" : "203.192.160.199",
  "name" : "Main server",
  "tunnelEndpoint" : "PRIMARY",
  "id" : 170,
  "type" : "BGP",
  "popName" : "ogn",
  "mtu" : 1476,
  "status" : "UP"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation OriginConnectivityData

```
put /routing-policy/{routingPolicyId}
```

Edit routing policy (editPolicy)

Edits the routing policy.

Path parameters

routingPolicyId (required)

Path Parameter

— The policy's Imperva ID. The routing policy ID is provided as part of the response when a policy is first added. You can also retrieve it using GET HTTP method. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

body (required)

Form Parameter

— accountId (required)

Form Parameter

— format: int64

Return type

[RoutingPolicyData](#)

Example data

Content-Type: application/json

```
{
  "connectionId" : 139,
  "id" : 5,
  "asnId" : 660,
  "type" : "BGP"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [RoutingPolicyData](#)

```
get /routing-policy
```

Retrieve routing policy (getPolicy)

Retrieves a routing policy.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

connectionId (required)

Form Parameter

— format: int64

accountId (required)

Form Parameter

— format: int64

Return type

RoutingPolicyData

Example data

Content-Type: application/json

```
{  
    "connectionId" : 139,  
    "id" : 5,  
    "asnId" : 660,  
    "type" : "BGP"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [RoutingPolicyData](#)

Models

Methods

Table of Contents

1. ASNData
2. OriginConnectivityData
3. RoutingPolicyData
4. accountId_connections_body
5. asn_asnId_body
6. asn_body
7. originconnectivity_body
8. originconnectivity_connectionId_body
9. originconnectivity_connectionId_body_1
10. routingpolicy_body
11. routingpolicy_body_1
12. routingpolicy_routingPolicyId_body
13. routingpolicy_routingPolicyId_body_1

ASNData

asnNumber

Long

The ASN number. format: int64

example: 123

asnId

Long

Unique identifier of your ASN. format: int64

example: 664

OriginConnectivityData

id (optional)

Long

Unique identifier of your connection. format: int64

example: 170

name (optional)

String

The connection name.

example: Main server

customerPublicIp (optional)

String

The IP address of your service.

example: 203.192.160.199

popName

String

The name of the Imperva data center (PoP).

example: ogn

mtu (optional)

Integer

The MTU (Maximum Transmission Unit) value. format: int32

example: 1476

type (optional)

String

The connection type. Possible values: BGP, PIP, ECX, CROSS_CONNECT, IPIP

example: BGP

status

String

The connection status. Possible values: UP, DOWN, MONITORING_DISABLED

example: UP

tunnelEndpoint (optional)

String

Each Imperva data center contains two tunnel endpoints (external routers) for optimal resilience and failover. In some cases, a second connection to a second router in the same Imperva PoP may be useful. It can be configured for your account by Imperva Support. Possible values: PRIMARY, SECONDARY

example: PRIMARY

RoutingPolicyData

id (optional)

Long

Unique identifier of the routing policy. format: int64

example: 5

connectionId

Long

Unique identifier of your connection. format: int64

example: 139

asnId

Long

Unique identifier of your ASN. format: int64

example: 660

type

String

The connection type. Possible values: BGP, STATIC

example: BGP

accountId_connections_body

type (optional)

String

The connection type. Available values: BGP, ECX, CROSS_CONNECT.

asn_asnId_body

accountId

Long

The account ID. format: int64

asn_body

asn

Long

The ASN number. format: int64

accountId

Long

The account ID. format: int64

originconnectivity_body

body

String

JsonString containing all the connection's data. Mandatory fields: name(string), popName(string), customerPublicIp(string). For example: {name:connectionName, popName:ogn, customerPublicIp:203.192.160.222}

accountId**Long**

The account ID. format: int64

originconnectivity_connectionId_body**body****String**

JsonString containing all the connection's data. Mandatory fields: name(string), popName(string), customerPublicIp(string). For example : {name:connectionName, popName:ogn, customerPublicIp:203.192.160.222}

originconnectivity_connectionId_body_1**accountId****Long**

The account ID. format: int64

routingpolicy_body**connectionId****Long**

The connection's Imperva ID. The connection ID is provided as part of the response when a connection is first added. You can also retrieve it using GET HTTP method. format: int64

accountId**Long**

The account ID. format: int64

routingpolicy_body_1**body****String**

JsonString containing all the policy's data. Mandatory fields: asnId(long), connectionId(string). For example: {asnId: 664, connectionId: 139 }

accountId**Long**

The account ID. format: int64

routingpolicy_routingPolicyId_body**body****String**

JsonString containing all the connection's data. Mandatory fields: asn(long), connectionId(string). For example: {asnId: 664, connectionId: 139 }

accountId**Long**

The account ID. format: int64

routingpolicy_routingPolicyId_body_1

accountId

Long

The account ID. format: int64

Flow Exporter Settings API Documentation

This is the API for Imperva Flow Monitoring. Configure exporter settings and define recipients for notifications. These settings apply to the DDoS Protection for Networks service when used in on-demand mode. Using flows that you provide, Imperva monitors your origin network to detect and notify you about DDoS attacks. For full feature documentation, see [Flow Monitoring Settings](#).

Version: 1.0.0

BasePath:/api/v2/ddos-protection

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

[Models](#)

Table of Contents

FlowExporterManagement

- `post /exporter`
- `delete /exporter/{exporterId}`
- `put /exporter/{exporterId}`
- `get /exporter`

FlowExporterManagement

```
post /exporter
```

Add flow exporter (addExporter)
Adds an exporter.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/x-www-form-urlencoded`

Form parameters

`data` (required)
Form Parameter

—
`accountId` (required)
Form Parameter
— format: int64

Return type

FlowExporterData

Example data

Content-Type: application/json

```
{
  "exporterId" : 170,
  "getNotifications" : true,
  "incorrectTimeUnit" : "MINUTES",
  "description" : "Main router",
  "startThreshold" : 5,
  "stopTimeUnit" : "MINUTES",
  "type" : "PRIMARY",
  "samplingRatio" : 1000,
  "stopThreshold" : 5,
  "startTimeUnit" : "MINUTES",
  "collectorIp" : "203.192.160.10",
  "exporterIp" : "203.192.160.199",
  "incorrectThreshold" : 5,
  "region" : "EU"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation FlowExporterData

```
delete /exporter/{exporterId}
```

Delete flow exporter (deleteExporter)
Removes the flow exporter.

Path parameters

exporterId (required)

Path Parameter

— The exporter's Imperva ID. The exporter ID is provided as part of the response when an exporter is first added.
format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

FlowExporterData

Example data

Content-Type: application/json

```
{
  "exporterId" : 170,
  "getNotifications" : true,
  "incorrectTimeUnit" : "MINUTES",
  "description" : "Main router",
  "startThreshold" : 5,
  "stopTimeUnit" : "MINUTES",
  "type" : "PRIMARY",
  "samplingRatio" : 1000,
  "stopThreshold" : 5,
  "startTimeUnit" : "MINUTES",
  "collectorIp" : "203.192.160.10",
  "exporterIp" : "203.192.160.199",
  "incorrectThreshold" : 5,
  "region" : "EU"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [FlowExporterData](#)

```
put /exporter/{exporterId}
```

Edit flow exporter (editExporter)
Edits the flow exporter.

Path parameters

exporterId (required)

Path Parameter

— The flow exporter's Imperva ID. The exporter ID is provided as part of the response when an exporter is first added. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

data (required)

Form Parameter

—

accountId (required)

Form Parameter

— format: int64

Return type

[FlowExporterData](#)

Example data

Content-Type: application/json

```
{
  "exporterId" : 170,
  "getNotifications" : true,
  "incorrectTimeUnit" : "MINUTES",
  "description" : "Main router",
  "startThreshold" : 5,
  "stopTimeUnit" : "MINUTES",
  "type" : "PRIMARY",
  "samplingRatio" : 1000,
  "stopThreshold" : 5,
```

```

    "startTimeUnit" : "MINUTES",
    "collectorIp" : "203.192.160.10",
    "exporterIp" : "203.192.160.199",
    "incorrectThreshold" : 5,
    "region" : "EU"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [FlowExporterData](#)

```
get /exporter
```

Retrieve flow exporter (getExporter)
Retrieves details of the flow exporter.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

exporterId (required)
Form Parameter

exporterIp (required)
Form Parameter

accountId (required)
Form Parameter
— format: int64

Return type

[FlowExporterData](#)

Example data

Content-Type: application/json

```
{
  "exporterId" : 170,
  "getNotifications" : true,
  "incorrectTimeUnit" : "MINUTES",
  "description" : "Main router",
  "startThreshold" : 5,
  "stopTimeUnit" : "MINUTES",
  "type" : "PRIMARY",
  "samplingRatio" : 1000,
  "stopThreshold" : 5,
  "startTimeUnit" : "MINUTES",
  "collectorIp" : "203.192.160.10",
  "exporterIp" : "203.192.160.199",
  "incorrectThreshold" : 5,
  "region" : "EU"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation [FlowExporterData](#)

Models

Methods

Table of Contents

1. [FlowExporterData](#)
2. [exporter_body](#)
3. [exporter_body_1](#)
4. [exporter_exporterId_body](#)
5. [exporter_exporterId_body_1](#)

FlowExporterData

exporterId

[Long](#)

Unique identifier of your exporter. format: int64

example: 170

exporterIp

[String](#)

The IP address of the network device sending flow data to Imperva.

example: 203.192.160.199

description

String

Meaningful description to help you identify the exporter.

example: Main router

collectorIp (optional)

String

The IP address of the Imperva device that receives your flow data.

example: 203.192.160.10

region

String

The region name. Possible values : EU, APAC , US.

example: EU

samplingRatio

Integer

The number of packets of actual traffic represented by each sample packet sent to Imperva, in a ratio of 1:X.

Enter a value for X. format: int32

example: 1000

startThreshold (optional)

Integer

The amount of time after Imperva starts receiving a flow from this exporter that a notification is sent. format: int32

example: 5

startTimeUnit (optional)

String

The time unit. Available options: MINUTES, HOURS, DAYS.

example: MINUTES

incorrectThreshold (optional)

Integer

The amount of time after Imperva receives an incompatible flow from this exporter that a notification is sent.

format: int32

example: 5

incorrectTimeUnit (optional)

String

The time unit. Available options: MINUTES, HOURS, DAYS.

example: MINUTES

stopThreshold (optional)

Integer

The amount of time after Imperva stops receiving a flow from this exporter that a notification is sent. format: int32

example: 5

stopTimeUnit (optional)

String

The time unit. Available options: MINUTES, HOURS, DAYS.

example: MINUTES

getNotifications (optional)

Boolean

Get notification by Email.

example: true

type

String

The intended use of your exporter. Available options: PRIMARY or SECONDARY.

example: PRIMARY

exporter_body

exporterId (optional)

String

The ID of the flow exporter. If a valid value is provided for this field, the exporter's details are returned. Otherwise,

the details of all the exporters of this account are returned.

exporterIp (optional)

String

The IP address of the network device sending flow data to Imperva. If a valid value is provided for this field, the exporter's details are returned. Otherwise, the details of all the exporters of this account are returned.

accountId

Long

The account ID. format: int64

exporter_body_1

data

String

JsonString containing all the flow exporter's data. Mandatory fields: exporterIp(string), description(string), samplingRatio(integer), type(string), region(string). For example: {exporterIp:203.192.160.222, description:router1, samplingRatio:1000, type:PRIMARY, region:EU}

accountId

Long

The account ID. format: int64

exporter_exporterId_body

data

String

JsonString containing all the flow exporter's data. Mandatory fields: exporterIp(string), description(string), samplingRatio(integer), type(string), region(string). For example: {exporterIp:203.192.160.222, description:router1, samplingRatio:1000, type:PRIMARY, region:EU}

accountId

Long

The account ID. format: int64

exporter_exporterId_body_1

accountId

Long

The account ID. format: int64

Network Range Diversion API

Divert your protected network ranges to Imperva's DDoS Protection for Network service on demand. For full feature documentation, see [Control Network Range Diversions](#).

Version: 1.0.0

BasePath:/api/v3

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountRangeManagement

- `get /infra-protect/account/ranges/diversion-status`

IPRangeManagement

- `post /infraProtect/range/divert`
- `post /infraProtect/range/revert`

AccountRangeManagement

```
get /infra-protect/account/ranges/diversion-status
```

Get the diversion status of all IP ranges in an account (getAccountRangesDiversionStatus)
 Returns the diversion status of the account's IP ranges.

Consumes

This API call consumes the following media types via the Content-Type request header:

- `application/x-www-form-urlencoded`

Form parameters

`accountId` (required)

Form Parameter

— format: int64

Return type

`RangesDiversionStatus`

Example data

Content-Type: `application/json`

```
{
  "diversionStatus" : "DIVERTED",
  "range" : "1.2.3.4/24"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Successful operation RangesDiversionStatus

401

Unauthorized

500

Unexpected error.

IPRangeManagement

```
post /infraProtect/range/divert
```

Diverts a list of IP ranges (divertIPRanges)

Diverts a list of IP ranges and returns an action status for each range.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Query parameters

rangelds (required)

Query Parameter

— To send multiple range IDs in a single request, use the same parameter as many times as needed. For example, rangelds=123&rangelds=456&rangelds=789.

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

ActionStatusResults

Example data

Content-Type: application/json

```
{
  "66816" : {
    "isSuccess" : false,
    "error" : {
      "httpReturnCode" : 500,
      "errorMessage" : "failed to invoke divert request,"
    }
  },
  "11894" : {
    "isSuccess" : false,
    "error" : {
      "httpReturnCode" : 400,
      "errorMessage" : "the range is not related to the given account,"
    }
  },
  "11190" : {
    "isSuccess" : true
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

400

One or more of the request parameters are invalid

401

Unauthorized

403

The given account does not have the required permissions for invoke this API

500

Unexpected error.

200

Successfull operation.(a status action is given for each range in the response) [ActionStatusResults](#)

```
post /infraProtect/range/revert
```

Reverts a list of IP ranges (revertIPRanges)

Reverts a list of IP ranges and returns an action status for each range.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Query parameters

rangelds (required)

Query Parameter

— To send multiple range IDs in a single request, use the same parameter as many times as needed. For example, rangelds=123&rangelds=456&rangelds=789.

Form parameters

accountId (required)

Form Parameter

— format: int64

Return type

[ActionStatusResults](#)

Example data

Content-Type: application/json

```
{
  "66816" : {
    "isSuccess" : false,
    "error" : {
      "httpReturnCode" : 500,
      "errorMessage" : "failed to invoke divert request,"
    }
  },
  "11894" : {
    "isSuccess" : false,
```

```

    "error" : {
        "httpReturnCode" : 400,
        "errorMessage" : "the range is not related to the given account,"
    }
},
"11190" : {
    "isSuccess" : true
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

400

One or more of the request parameters are invalid

401

Unauthorized

403

The given account does not have the required permissions for invoke this API

500

Unexpected error.

200

Successfull operation.(a status action is given for each range in the response) [ActionStatusResults](#)

Models

Methods

Table of Contents

1. [ActionStatusResult](#)
 2. [ActionStatusResults](#)
 3. [FailureReason](#)
-

-
- 4. RangesDiversionStatus
 - 5. range_divert_body
 - 6. range_revert_body
 - 7. ranges_diversionstatus_body

ActionStatusResult

isSuccess (optional)

Boolean

example: true

error (optional)

FailureReason

ActionStatusResults

FailureReason

httpReturnCode (optional)

Integer

the http return code for the specific ip range action

example: 400

errorMessage (optional)

String

the error informative text

example: the range is not related to the given account

RangesDiversionStatus

range

String

The IP range.

example: 1.2.3.4/24

diversionStatus

String

The diversion status of the IP range.

example: DIVERTED

range_divert_body

accountId

Long

The account ID. format: int64

range_revert_body

accountId

Long

The account ID. format: int64

ranges_divisionstatus_body

accountId

Long

The account ID. format: int64

Performance Monitoring API

Gain visibility into the performance of the connections between Imperva data centers and your origin network.

For full feature documentation, see [DDoS Protection for Networks and IPs: Connectivity Monitoring](#)

Version: 1.0.0

BasePath:/netsec-dashboards

The terms in the absence of an applicable signed agreement between you and Imperva

<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

PerformanceMetrics

- `get /netsec/stats/series`
- `get /netsec/stats/single`

PerformanceMetrics

```
get /netsec/stats/series
```

Get a series of performance metrics for a specified time range (`getSeriesStats`)

Gets metrics for one or more connections during the specified time range. Returns multiple values for each metric requested at a specified interval. For example, get the metrics for every hour during the last 24 hours.

Query parameters

`caid` (required)

Query Parameter

— The Imperva account ID. By default, the API operates on the account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. format: int64

`objectIds` (required)

Query Parameter

— The unique Imperva IDs of the requested connections. Use the GET /account/{accountId}/connections API to retrieve the connection IDs for an account. format: int64

`fromDate` (required)

Query Parameter

— Start of time range. Epoch timestamp in milliseconds. Can not be older than 90 days format: int64
toDate (required)
Query Parameter

— End of time range. Epoch timestamp in milliseconds format: int64
resolution (optional)
Query Parameter

— <p>The interval at which to return the statistics during the specified time range. Used together with the timeUnit parameter.</p> <p>For example, resolution of 1, timeUnit of hours.</p> <p>If not specified, the resolution is calculated dynamically according to the time range.</p> format: int32
timeUnit (optional)
Query Parameter

— The time unit of the resolution. Used together with the resolution parameter. default: SECONDS
aggregationFunction (required)
Query Parameter

— The aggregation function to apply on data point
metrics (required)
Query Parameter

— The requested metrics. Supports multiple selection.

Return type

SeriesStatsDTO

Example data

Content-Type: application/json

```
{
  "aggregation" : "AVG",
  "startTime" : 5,
  "id" : 0,
  "metricItems" : [ {
    "metricName" : "LATENCY",
    "values" : [ 6, 6 ]
  }, {
    "metricName" : "LATENCY",
    "values" : [ 6, 6 ]
  } ],
  "resolution" : 1
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SeriesStatsDTO

400

Client Error

500Server Error

```
get /netsec/stats/single
```

Get performance metrics for a specified time range (getSingleStats)

Gets metrics for one or more connections during the specified time range. Returns a single value for each metric requested.

Query parameters

caid (required)

Query Parameter

— The Imperva account ID. By default, the API operates on the account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. format: int64

objectIds (required)

Query Parameter

— List of connection ids format: int64

fromDate (required)

Query Parameter

— Start of time range. Epoch timestamp in milliseconds format: int64

toDate (required)

Query Parameter

— End of time range. Epoch timestamp in milliseconds format: int64

aggregationFunction (required)

Query Parameter

— The aggregation function to apply on data point

metrics (required)

Query Parameter

— The requested metrics

Return type

SingleStatsDTO

Example data

Content-Type: application/json

```
{
  "aggregation" : "AVG",
  "id" : 0,
  "metricItems" : [ {
    "metricName" : "LATENCY",
    "value" : 6
  }, {
```

```

    "metricName" : "LATENCY",
    "value" : 6
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SingleStatsDTO

400

Client Error

500

Server Error

Models

Methods

Table of Contents

1. SeriesStatsDTO
2. SeriesStatsMetricDTO
3. SingleStatsDTO
4. SingleStatsMetricDTO

SeriesStatsDTO

aggregation (optional)

String

Enum:

AVG

MAX

MIN

id (optional)

Long

format: int64

metricItems (optional)
array[SeriesStatsMetricDTO]
resolution (optional)
Long
format: int64
startTime (optional)
Long
format: int64

SeriesStatsMetricDTO

metricName (optional)
String
Enum:
LATENCY
JITTER
PACKET_LOSS
values (optional)
array[Long]
format: int64

SingleStatsDTO

aggregation (optional)
String
Enum:
AVG
MAX
MIN
id (optional)
Long
format: int64
metricItems (optional)
array[SingleStatsMetricDTO]

SingleStatsMetricDTO

metricName (optional)
String
Enum:
LATENCY
JITTER
PACKET_LOSS
value (optional)
Long
format: int64

DDoS Network and IP Protection: Asset Migration API

Move your protected network/IP assets between a parent account and its sub accounts, or between the sub accounts. For full feature documentation, see [Sub Account Support](#).

Version: 1.0.0

BasePath:/api/v2/ddos-protection

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

MoveConnection

- post /origin-connectivity/move

MoveExporter

- post /exporter/move

MoveProtectedIP

- post /protected-ip/move

MoveProtectedNetwork

- post /protected-network/move

MoveConnection

```
post /origin-connectivity/move
```

Move a connection (moveOriginConnectivity)

Moves a connection and its associated resources (routing options, ASN) between a parent account and its sub accounts, or between the sub accounts.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

connectionId (required)

Form Parameter

— format: int64

destAccount (required)

Form Parameter

— format: int64

Responses

200

Successful operation

MoveExporter

```
post /exporter/move
```

Move an exporter (moveExporter)

Move a flow exporter between a parent account and its sub accounts, or between the sub accounts.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

exporterId (required)

Form Parameter

— format: int64

destAccount (required)

Form Parameter

— format: int64

Responses

200

Successful operation

MoveProtectedIP

```
post /protected-ip/move
```

Move a protected IP (moveProtectedIp)

Move a protected IP address between a parent account and its sub accounts, or between the sub accounts.

Consumes

This API call consumes the following media types via the Content-Type request header:

-
- application/x-www-form-urlencoded

Form parameters

ip (required)
Form Parameter

destAccount (required)
Form Parameter
— format: int64

Responses

200

Successful operation

MoveProtectedNetwork

```
post /protected-network/move
```

Move a protected network (moveProtectedNetwork)
Move a protected network between a parent account and its sub accounts, or between the sub accounts.

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/x-www-form-urlencoded

Form parameters

network (required)
Form Parameter

destAccount (required)
Form Parameter
— format: int64

Responses

200

Successful operation

Models

Methods

Table of Contents

1. `exporter_move_body`
2. `originconnectivity_move_body`
3. `protectedip_move_body`
4. `protectednetwork_move_body`

`exporter_move_body`

exporterId

Long

The Imperva ID for your flow exporter. You can locate this ID using the Flow Exporter API. format: int64

destAccount

Long

The Imperva account ID of the destination account. format: int64

`originconnectivity_move_body`

connectionId

Long

The connection ID for your connection. You can locate this ID using the Connections API. format: int64

destAccount

Long

The Imperva account ID of the destination account. format: int64

`protectedip_move_body`

ip

String

The Imperva global anycast Protected IP. This is the IP address used for any internet-facing access to your service.

destAccount

Long

The Imperva account ID of the destination account. format: int64

`protectednetwork_move_body`

network

String

The Protected Network (IP range).

destAccount

Long

The Imperva account ID of the destination account. format: int64

Access List Policies

This is an API for managing access list (ACL) policies for the DDoS Protection for Networks service. Create access lists to centrally configure access restrictions for protected networks in your account. For full feature documentation, see [DDoS Protection for Networks: Access Lists](#)

Version: 1.0.0

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccessListACLPolicyManagement

- post /netsec/v2/accounts/{caid}/policies
- put /netsec/v2/accounts/{caid}/policies/{policyId}
- get /netsec/v2/policies/{policyId}/assets
- get /netsec/v2/accounts/{caid}/policies
- get /netsec/v2/accounts/{caid}/policies/{policyId}
- get /netsec/v2/policies/{policyId}/assets/{assetType}/{assetId}
- delete /netsec/v2/accounts/{caid}/policies/{policyId}
- put /netsec/v2/policies/{policyId}/assets

AccessListACLPolicyManagement

```
post /netsec/v2/accounts/{caid}/policies
```

Add or duplicate an ACL policy (addOrDuplicateACLPolicy)
 Adds a new policy or copies an existing policy.

Path parameters

caid (required)
 Path Parameter
 — Account ID format: int64

Query parameters

body (optional)
 Query Parameter
 — ACL policy settings. for example: {"id": 17}
 sourcePolicyId (optional)
 Query Parameter
 — The source policy ID which you want to clone format: int64

Return type

LeanPolicyDto

Example data

Content-Type: application/json

```
{
  "policyType" : "IP",
  "lastModifiedBy" : 230851,
  "name" : "ACL policy to block a specific range",
  "description" : "Range 1.2.3.4/24 is blocked",
  "lastUserModified" : "Demo account",
  "id" : 123,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "numberOfAssets" : 5
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

500

Internal Server Error

200

OK [LeanPolicyDto](#)

```
put /netsec/v2/accounts/{caid}/policies/{policyId}
```

Edit ACL policy settings (full update) (`editACLPolicy`)
Updates policy settings. Overwrites current settings.

Path parameters

caid (required)
 Path Parameter
 — Account ID format: int64
 policyId (required)
 Path Parameter
 — Policy ID format: int64

Query parameters

body (required)
 Query Parameter

— ACL policy settings. for example: {"id": 16}

Return type

PolicyDto

Example data

Content-Type: application/json

```
{
  "accountId" : 230851,
  "policySettings" : [ {
    "policyId" : 16,
    "policySettingType" : "IP",
    "data" : {
      "geo" : {
        "countries" : [ "AE", "AC" ],
        "continents" : [ "APAC", "US" ]
      },
      "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
    },
    "policyDataExceptions" : [ {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      } ],
      "lastModifiedBy" : 345,
      "comment" : "Exclude all ips for pen tests",
      "id" : 45,
      "lastModified" : "2000-01-23T04:56:07.000+00:00"
    }, {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      } ],
      "lastModifiedBy" : 345,
      "comment" : "Exclude all ips for pen tests",
      "id" : 45,
      "lastModified" : "2000-01-23T04:56:07.000+00:00"
    } ],
    "id" : 12
  }, {
    "summary" : "Summary of the exception details",
    "policySettingsId" : 72,
    "data" : [ {
      "exceptionType" : "IP",
      "validateExceptionData" : true,
      "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
    }, {
      "exceptionType" : "IP",
      "validateExceptionData" : true,
      "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
    } ],
    "lastModifiedBy" : 345,
    "comment" : "Exclude all ips for pen tests",
    "id" : 45,
    "lastModified" : "2000-01-23T04:56:07.000+00:00"
  } ],
  "id" : 12
}, {
```

```

"policyId" : 16,
"policySettingType" : "IP",
"data" : {
  "geo" : {
    "countries" : [ "AE", "AC" ],
    "continents" : [ "APAC", "US" ]
  },
  "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
},
"policyDataExceptions" : [ {
  "summary" : "Summary of the exception details",
  "policySettingsId" : 72,
  "data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  }, {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  } ],
  "lastModifiedBy" : 345,
  "comment" : "Exclude all ips for pen tests",
  "id" : 45,
  "lastModified" : "2000-01-23T04:56:07.000+00:00"
}, {
  "summary" : "Summary of the exception details",
  "policySettingsId" : 72,
  "data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  }, {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  } ],
  "lastModifiedBy" : 345,
  "comment" : "Exclude all ips for pen tests",
  "id" : 45,
  "lastModified" : "2000-01-23T04:56:07.000+00:00"
} ],
"id" : 12
} ],
"policyType" : "IP",
"lastModifiedBy" : 123,
"name" : "ACL policy to block a specific range",
"description" : "Range 1.2.3.4/24 is blocked",
"id" : 12,
"lastModified" : "2000-01-23T04:56:07.000+00:00"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

OK PolicyDto

500

Internal Server Error

```
get /netsec/v2/policies/{policyId}/assets
```

Get the assets on which the policy is applied (getACLPolicyAssets)

Retrieves the list of protected IPs or protected networks on which the policy is applied.

Path parameters

policyId (required)

Path Parameter

— Policy ID format: int64

Return type

ACLPolicyAssetsAddresses

Example data

Content-Type: application/json

```
{
  "ipRanges" : [ "", "" ],
  "protectedIps" : [ "", "" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

OK ACLPolicyAssetsAddresses

500

Internal Server Error

```
get /netsec/v2/accounts/{caid}/policies
```

Get all the ACL policies of the account (getAccountACLPolicies)
 Retrieves all policies in the account.

Path parameters

caid (required)
 Path Parameter
 — Account ID format: int64

Return type

[LeanPolicyDto](#)

Example data

Content-Type: application/json

```
{
  "policyType" : "IP",
  "lastModifiedBy" : 230851,
  "name" : "ACL policy to block a specific range",
  "description" : "Range 1.2.3.4/24 is blocked",
  "lastUserModified" : "Demo account",
  "id" : 123,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "numberOfAssets" : 5
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

500

Internal Server Error

200

OK [LeanPolicyDto](#)

```
get /netsec/v2/accounts/{caid}/policies/{policyId}
```

Get details of an ACL policy (getPolicyDetails1)
Retrieves details of a policy.

Path parameters

caid (required)

Path Parameter

— Account ID format: int64

policyId (required)

Path Parameter

— Policy ID format: int64

Return type

PolicyDto

Example data

Content-Type: application/json

```
{
  "accountId" : 230851,
  "policySettings" : [ {
    "policyId" : 16,
    "policySettingType" : "IP",
    "data" : {
      "geo" : {
        "countries" : [ "AE", "AC" ],
        "continents" : [ "APAC", "US" ]
      },
      "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
    },
    "policyDataExceptions" : [ {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }],
      "lastModifiedBy" : 345,
      "comment" : "Exclude all ips for pen tests",
      "id" : 45,
      "lastModified" : "2000-01-23T04:56:07.000+00:00"
    },
    {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }]
    }
  }
}
```

```

"data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
}, {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
} ],
"lastModifiedBy" : 345,
"comment" : "Exclude all ips for pen tests",
"id" : 45,
"lastModified" : "2000-01-23T04:56:07.000+00:00"
} ],
"id" : 12
}, {
    "policyId" : 16,
    "policySettingType" : "IP",
    "data" : {
        "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
        },
        "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
    },
    "policyDataExceptions" : [ {
        "summary" : "Summary of the exception details",
        "policySettingsId" : 72,
        "data" : [ {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        }, {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        } ],
        "lastModifiedBy" : 345,
        "comment" : "Exclude all ips for pen tests",
        "id" : 45,
        "lastModified" : "2000-01-23T04:56:07.000+00:00"
    }, {
        "summary" : "Summary of the exception details",
        "policySettingsId" : 72,
        "data" : [ {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        }, {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        } ],
        "lastModifiedBy" : 345,
        "comment" : "Exclude all ips for pen tests",
        "id" : 45,
        "lastModified" : "2000-01-23T04:56:07.000+00:00"
    } ],
    "id" : 12
}

```

```

} ],
"policyType" : "IP",
"lastModifiedBy" : 123,
"name" : "ACL policy to block a specific range",
"description" : "Range 1.2.3.4/24 is blocked",
"id" : 12,
"lastModified" : "2000-01-23T04:56:07.000+00:00"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

[OK PolicyDto](#)

500

[Internal Server Error](#)

```
get /netsec/v2/policies/{policyId}/assets/{assetType}/{assetId}
```

Returns true if the policy is applied on the asset, otherwise false (isPolicyAppliedOnTheAsset)

Gets the policy ID, asset ID and asset type. Returns true if the policy is applied on the asset, otherwise returns false.

Path parameters

`policyId` (required)

Path Parameter

— Policy ID format: int64

`assetType` (required)

Path Parameter

— Asset Type

`assetId` (required)

Path Parameter

— Asset ID format: int64

Return type

Boolean

Example data

Content-Type: application/json

```
true
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK Boolean

500

Internal Server Error

```
delete /netsec/v2/accounts/{caid}/policies/{policyId}
```

Delete an ACL policy (removeACLPolicy)

Deletes an existing policy.

Path parameters

caid (required)

Path Parameter

— Account ID format: int64

policyId (required)

Path Parameter

— Policy ID format: int64

Responses

500

Internal Server Error

200

OK

```
put /netsec/v2/policies/{policyId}/assets
```

Set the ACL policy assets (full update) (setACLPolicyAssets)

Applies the policy to protected IPs or protected networks in your account. Overwrites current assets.

Path parameters

policyId (required)

Path Parameter

— Policy ID format: int64

Query parameters

body (required)

Query Parameter

— Policy assets. For example: {"protectedIps": [1,2,3], "ipRanges": [4,5,6]}

Responses

500

Internal Server Error

200

OK

Models

Methods

Table of Contents

1. [ACLPolicyAssetsAddresses](#)
2. [ExceptionsDataDto](#)
3. [GeoDto](#)
4. [LeanPolicyDto](#)
5. [Policy](#)
6. [PolicyDataExceptionDto](#)
7. [PolicyDataExceptions](#)
8. [PolicyDto](#)
9. [PolicySettings](#)
10. [PolicySettingsDto](#)
11. [SettingsDataDto](#)

ACLPolicyAssetsAddresses

protectedIps (optional)

array[String]

Array of all the policy's protected IPs

ipRanges (optional)

array[String]

Array of all the policy's protected networks

ExceptionsDataDto

validateExceptionData (optional)

Boolean

Is exception data valid

example: true

exceptionType (optional)

String

The ExceptionType type

Enum:

GEO

IP

example: IP

values (optional)

array[String]

Values of the exception depends on the exceptionType

example: ["1.2.3.4/24","5.6.7.8/24"]

GeoDto

countries (optional)

array[String]

Country Codes array

example: ["AE","AC"]

continents (optional)

array[String]

Continent Codes array

example: ["APAC","US"]

LeanPolicyDto

id (optional)

Long

The Policy ID format: int64

example: 123

policyType (optional)

String

The Policy type

Enum:

IP

RANGE

example: IP

name (optional)

String

The Policy name

example: ACL policy to block a specific range

description (optional)

String

Policy description

example: Range 1.2.3.4/24 is blocked

lastModified (optional)

Date

Date of the last modification format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 230851

lastUserModified (optional)

String

The user name of the last user to modify the policy.

example: Demo account

numberOfAssets (optional)

Integer

The number of assets that the policy is applied to. format: int32

example: 5

Policy

id (optional)

Long

The policy ID format: int64

example: 123

policyType (optional)

String

The policy type

Enum:

IP

RANGE

example: IP

name (optional)

String

The policy name

example: ACL policy to block a specific range

description (optional)

String

Policy description

example: Range 1.2.3.4/24 is blocked

accountId (optional)

Long

The account ID format: int64

example: 230851

lastModified (optional)

Date

User ID of the last user format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 123

policySettings (optional)

array[PolicySettings]

Array of the policy settings

PolicyDataExceptionDto

id (optional)

Long

The PolicyDataExceptions ID format: int64

example: 45

policySettingsId (optional)

Long

The PolicySettings ID format: int64

example: 72

data (optional)

array[ExceptionsDataDto]

The Filter/s of the exception

comment (optional)

String

Comment describing the exception and its reason

example: Exclude all ips for pen tests

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 345

lastModified (optional)

Date

Date of the last modification format: date-time

summary (optional)

String

Summary of the policy data exception

example: Summary of the exception details

PolicyDataExceptions

id (optional)

Long

The PolicyDataExceptions ID format: int64

example: 10

policySettings (optional)

PolicySettings

data (optional)

String

The exception configuration on a given settings

comment (optional)

String

Comment describing the exception and its reason

lastModified (optional)

Date

User ID of the last user format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 1425

PolicyDto

id (optional)

Long

The PolicyDto ID format: int64

example: 12

name (optional)

String

The policy name

example: ACL policy to block a specific range

description (optional)

String

Policy description

example: Range 1.2.3.4/24 is blocked

accountId (optional)

Long

The account ID format: int64

example: 230851

policyType (optional)

String

The policy type

Enum:

IP

RANGE

lastModified (optional)

Date

Date of the last modification format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 123

policySettings (optional)

array[PolicySettingsDto]

Array of all the policy settings

PolicySettings

id (optional)

Long

The Policy Settings ID format: int64

example: 15

policy (optional)

Policy

settingsType (optional)

String

The PolicySettings type

Enum:

GEO

IP

example: IP

data (optional)

String

Depends on the policy settings type

policyDataExceptions (optional)

array[PolicyDataExceptions]

Array of the policy data exceptions

PolicySettingsDto

id (optional)

Long

The PolicySettingsDto ID format: int64

example: 12

policyId (optional)

Long

The policy ID format: int64

example: 16

policySettingType (optional)

String

The policy settings type

Enum:

GEO

IP

example: IP

data (optional)

SettingsDataDto

policyDataExceptions (optional)

array[PolicyDataExceptionDto]

Array of all the policy data exceptions

SettingsDataDto

geo (optional)

GeoDto

ips (optional)

array[String]

Array of all the IP addresses in the policy settings

example: ["1.2.3.4/24", "4.5.6.7/24"]

Access List Policies

This is an API for managing access list (ACL) policies for the DDoS Protection for Individual IPs service. Create access lists to centrally configure access restrictions for protected IPs in your account. For full feature documentation, see [DDoS Protection for Individual IPs: Access Lists](#)

Version: 1.0.0

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccessListACLPolicyManagement

- `post /netsec/v2/accounts/{caid}/policies`
- `put /netsec/v2/accounts/{caid}/policies/{policyId}`
- `get /netsec/v2/policies/{policyId}/assets`

- get /netsec/v2/accounts/{caid}/policies
- get /netsec/v2/accounts/{caid}/policies/{policyId}
- get /netsec/v2/policies/{policyId}/assets/{assetType}/{assetId}
- delete /netsec/v2/accounts/{caid}/policies/{policyId}
- put /netsec/v2/policies/{policyId}/assets

AccessListACLPolicyManagement

```
post /netsec/v2/accounts/{caid}/policies
```

Add or duplicate an ACL policy (addOrDuplicateACLPolicy)

Adds a new policy or copies an existing policy.

Path parameters

caid (required)

Path Parameter

— Account ID format: int64

Query parameters

body (optional)

Query Parameter

— ACL policy settings. for example: {“id”: 17}

sourcePolicyId (optional)

Query Parameter

— The source policy ID which you want to clone format: int64

Return type

LeanPolicyDto

Example data

Content-Type: application/json

```
{
  "policyType" : "IP",
  "lastModifiedBy" : 230851,
  "name" : "ACL policy to block a specific range",
  "description" : "Range 1.2.3.4/24 is blocked",
  "lastUserModified" : "Demo account",
  "id" : 123,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "numberOfAssets" : 5
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

500

Internal Server Error

200

OK [LeanPolicyDto](#)

```
put /netsec/v2/accounts/{caid}/policies/{policyId}
```

Edit ACL policy settings (full update) (`editACLPolicy`)
Updates policy settings. Overwrites current settings.

Path parameters

caid (required)

Path Parameter

— Account ID format: int64

policyId (required)

Path Parameter

— Policy ID format: int64

Query parameters

body (required)

Query Parameter

— ACL policy settings. for example: {"id": 16}

Return type

[PolicyDto](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 230851,
  "policySettings" : [ {
    "policyId" : 16,
```

```

"policySettingType" : "IP",
"data" : {
  "geo" : {
    "countries" : [ "AE", "AC" ],
    "continents" : [ "APAC", "US" ]
  },
  "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
},
"policyDataExceptions" : [ {
  "summary" : "Summary of the exception details",
  "policySettingsId" : 72,
  "data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  }, {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  } ],
  "lastModifiedBy" : 345,
  "comment" : "Exclude all ips for pen tests",
  "id" : 45,
  "lastModified" : "2000-01-23T04:56:07.000+00:00"
}, {
  "summary" : "Summary of the exception details",
  "policySettingsId" : 72,
  "data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  }, {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  } ],
  "lastModifiedBy" : 345,
  "comment" : "Exclude all ips for pen tests",
  "id" : 45,
  "lastModified" : "2000-01-23T04:56:07.000+00:00"
} ],
"id" : 12
}, {
  "policyId" : 16,
  "policySettingType" : "IP",
  "data" : {
    "geo" : {
      "countries" : [ "AE", "AC" ],
      "continents" : [ "APAC", "US" ]
    },
    "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
  },
  "policyDataExceptions" : [ {
    "summary" : "Summary of the exception details",
    "policySettingsId" : 72,
    "data" : [ {
      "exceptionType" : "IP",
      "validateExceptionData" : true,
      "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
    } ]
  } ]
}

```

```

}, {
  "exceptionType" : "IP",
  "validateExceptionData" : true,
  "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
} ],
"lastModifiedBy" : 345,
"comment" : "Exclude all ips for pen tests",
"id" : 45,
"lastModified" : "2000-01-23T04:56:07.000+00:00"
}, {
  "summary" : "Summary of the exception details",
  "policySettingsId" : 72,
  "data" : [ {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  },
  {
    "exceptionType" : "IP",
    "validateExceptionData" : true,
    "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
  }],
  "lastModifiedBy" : 345,
  "comment" : "Exclude all ips for pen tests",
  "id" : 45,
  "lastModified" : "2000-01-23T04:56:07.000+00:00"
},
"id" : 12
} ],
"policyType" : "IP",
"lastModifiedBy" : 123,
"name" : "ACL policy to block a specific range",
"description" : "Range 1.2.3.4/24 is blocked",
"id" : 12,
"lastModified" : "2000-01-23T04:56:07.000+00:00"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK PolicyDto

500

Internal Server Error

```
get /netsec/v2/policies/{policyId}/assets
```

Get the assets on which the policy is applied (getACLPolicyAssets)

Retrieves the list of protected IPs or protected networks on which the policy is applied.

Path parameters

policyId (required)

Path Parameter

— Policy ID format: int64

Return type

ACLPolicyAssetsAddresses

Example data

Content-Type: application/json

```
{
  "ipRanges" : [ "", "" ],
  "protectedIps" : [ "", "" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

200

OK ACLPolicyAssetsAddresses

500

Internal Server Error

```
get /netsec/v2/accounts/{caid}/policies
```

Get all the ACL policies of the account (getAccountACLPolicies)

Retrieves all policies in the account.

Path parameters

caid (required)
 Path Parameter
 — Account ID format: int64

Return type

[LeanPolicyDto](#)

Example data

Content-Type: application/json

```
{
  "policyType" : "IP",
  "lastModifiedBy" : 230851,
  "name" : "ACL policy to block a specific range",
  "description" : "Range 1.2.3.4/24 is blocked",
  "lastUserModified" : "Demo account",
  "id" : 123,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "numberOfAssets" : 5
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- */*

Responses

500

Internal Server Error

200

OK [LeanPolicyDto](#)

```
get /netsec/v2/accounts/{caid}/policies/{policyId}
```

Get details of an ACL policy (getPolicyDetails1)
 Retrieves details of a policy.

Path parameters

[caid \(required\)](#)

Path Parameter

— Account ID format: int64

policyId (required)

Path Parameter

— Policy ID format: int64

Return type

PolicyDto

Example data

Content-Type: application/json

```
{
  "accountId" : 230851,
  "policySettings" : [ {
    "policyId" : 16,
    "policySettingType" : "IP",
    "data" : {
      "geo" : {
        "countries" : [ "AE", "AC" ],
        "continents" : [ "APAC", "US" ]
      },
      "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
    },
    "policyDataExceptions" : [ {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      } ],
      "lastModifiedBy" : 345,
      "comment" : "Exclude all ips for pen tests",
      "id" : 45,
      "lastModified" : "2000-01-23T04:56:07.000+00:00"
    }, {
      "summary" : "Summary of the exception details",
      "policySettingsId" : 72,
      "data" : [ {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      }, {
        "exceptionType" : "IP",
        "validateExceptionData" : true,
        "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
      } ],
      "lastModifiedBy" : 345,
      "comment" : "Exclude all ips for pen tests",
      "id" : 45,
    }
  }
}
```

```

        "lastModified" : "2000-01-23T04:56:07.000+00:00"
    } ],
    "id" : 12
}, {
    "policyId" : 16,
    "policySettingType" : "IP",
    "data" : {
        "geo" : {
            "countries" : [ "AE", "AC" ],
            "continents" : [ "APAC", "US" ]
        },
        "ips" : [ "1.2.3.4/24", "4.5.6.7/24" ]
    },
    "policyDataExceptions" : [ {
        "summary" : "Summary of the exception details",
        "policySettingsId" : 72,
        "data" : [ {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        }, {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        } ],
        "lastModifiedBy" : 345,
        "comment" : "Exclude all ips for pen tests",
        "id" : 45,
        "lastModified" : "2000-01-23T04:56:07.000+00:00"
    }, {
        "summary" : "Summary of the exception details",
        "policySettingsId" : 72,
        "data" : [ {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        }, {
            "exceptionType" : "IP",
            "validateExceptionData" : true,
            "values" : [ "1.2.3.4/24", "5.6.7.8/24" ]
        } ],
        "lastModifiedBy" : 345,
        "comment" : "Exclude all ips for pen tests",
        "id" : 45,
        "lastModified" : "2000-01-23T04:56:07.000+00:00"
    } ],
    "id" : 12
}, {
    "policyType" : "IP",
    "lastModifiedBy" : 123,
    "name" : "ACL policy to block a specific range",
    "description" : "Range 1.2.3.4/24 is blocked",
    "id" : 12,
    "lastModified" : "2000-01-23T04:56:07.000+00:00"
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- * / *

Responses

200

OK PolicyDto

500

Internal Server Error

```
get /netsec/v2/policies/{policyId}/assets/{assetType}/{assetId}
```

Returns true if the policy is applied on the asset, otherwise false (isPolicyAppliedOnTheAsset)
Gets the policy ID, asset ID and asset type. Returns true if the policy is applied on the asset, otherwise returns false.

Path parameters

policyId (required)

Path Parameter

— Policy ID format: int64

assetType (required)

Path Parameter

— Asset Type

assetId (required)

Path Parameter

— Asset ID format: int64

Return type

Boolean

Example data

Content-Type: application/json

```
true
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `*/*`

Responses

200

OK Boolean

500

Internal Server Error

```
delete /netsec/v2/accounts/{caid}/policies/{policyId}
```

Delete an ACL policy (removeACLPolicy)

Deletes an existing policy.

Path parameters

caid (required)

Path Parameter

— Account ID format: int64

policyId (required)

Path Parameter

— Policy ID format: int64

Responses

500

Internal Server Error

200

OK

```
put /netsec/v2/policies/{policyId}/assets
```

Set the ACL policy assets (full update) (setACLPolicyAssets)

Applies the policy to protected IPs or protected networks in your account. Overwrites current assets.

Path parameters

policyId (required)

Path Parameter

— Policy ID format: int64

Query parameters

body (required)

Query Parameter

— Policy assets. For example: `{“protectedIps”: [1,2,3], “ipRanges”: [4,5,6]}`

Responses

500

Internal Server Error

200

OK

Models

Methods

Table of Contents

1. **ACLPolicyAssetsAddresses**
2. **ExceptionsDataDto**
3. **GeoDto**
4. **LeanPolicyDto**
5. **Policy**
6. **PolicyDataExceptionDto**
7. **PolicyDataExceptions**
8. **PolicyDto**
9. **PolicySettings**
10. **PolicySettingsDto**
11. **SettingsDataDto**

ACLPolicyAssetsAddresses

protectedIps (optional)

array[String]

Array of all the policy's protected IPs

ipRanges (optional)

array[String]

Array of all the policy's protected networks

ExceptionsDataDto

validateExceptionData (optional)

Boolean

Is exception data valid

example: true
exceptionType (optional)
String
The ExceptionType type
Enum:
GEO
IP
example: IP
values (optional)
array[String]
Values of the exception depends on the exceptionType
example: ["1.2.3.4/24","5.6.7.8/24"]

GeoDto

countries (optional)
array[String]
Country Codes array
example: ["AE","AC"]
continents (optional)
array[String]
Continent Codes array
example: ["APAC","US"]

LeanPolicyDto

id (optional)
Long
The Policy ID format: int64
example: 123
policyType (optional)
String
The Policy type
Enum:
IP
RANGE
example: IP
name (optional)
String
The Policy name
example: ACL policy to block a specific range
description (optional)
String
Policy description
example: Range 1.2.3.4/24 is blocked
lastModified (optional)
Date
Date of the last modification format: date-time
lastModifiedBy (optional)
Long
The user ID of the last user to modify the policy. format: int64
example: 230851
lastUserModified (optional)
String
The user name of the last user to modify the policy.
example: Demo account
numberOfAssets (optional)

Integer

The number of assets that the policy is applied to. format: int32
example: 5

Policy

id (optional)

Long

The policy ID format: int64

example: 123

policyType (optional)

String

The policy type

Enum:

IP**RANGE**

example: IP

name (optional)

String

The policy name

example: ACL policy to block a specific range

description (optional)

String

Policy description

example: Range 1.2.3.4/24 is blocked

accountId (optional)

Long

The account ID format: int64

example: 230851

lastModified (optional)

Date

User ID of the last user format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 123

policySettings (optional)

array[PolicySettings]

Array of the policy settings

PolicyDataExceptionDto

id (optional)

Long

The PolicyDataExceptions ID format: int64

example: 45

policySettingsId (optional)

Long

The PolicySettings ID format: int64

example: 72

data (optional)

array[ExceptionsDataDto]

The Filter/s of the exception

comment (optional)

String

Comment describing the exception and its reason

example: Exclude all ips for pen tests

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 345

lastModified (optional)

Date

Date of the last modification format: date-time

summary (optional)

String

Summary of the policy data exception

example: Summary of the exception details

PolicyDataExceptions

id (optional)

Long

The PolicyDataExceptions ID format: int64

example: 10

policySettings (optional)

PolicySettings

data (optional)

String

The exception configuration on a given settings

comment (optional)

String

Comment describing the exception and its reason

lastModified (optional)

Date

User ID of the last user format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 1425

PolicyDto

id (optional)

Long

The PolicyDto ID format: int64

example: 12

name (optional)

String

The policy name

example: ACL policy to block a specific range

description (optional)

String

Policy description

example: Range 1.2.3.4/24 is blocked

accountId (optional)

Long

The account ID format: int64

example: 230851

policyType (optional)

String

The policy type

Enum:

IP

RANGE

lastModified (optional)

Date

Date of the last modification format: date-time

lastModifiedBy (optional)

Long

The user ID of the last user to modify the policy. format: int64

example: 123

policySettings (optional)

array[PolicySettingsDto]

Array of all the policy settings

PolicySettings

id (optional)

Long

The Policy Settings ID format: int64

example: 15

policy (optional)

Policy

settingsType (optional)

String

The PolicySettings type

Enum:

GEO

IP

example: IP

data (optional)

String

Depends on the policy settings type

policyDataExceptions (optional)

array[PolicyDataExceptions]

Array of the policy data exceptions

PolicySettingsDto

id (optional)

Long

The PolicySettingsDto ID format: int64

example: 12

policyId (optional)

Long

The policy ID format: int64

example: 16

policySettingType (optional)

String

The policy settings type

Enum:

GEO

IP

example: IP

data (optional)

SettingsDataDto

policyDataExceptions (optional)

array[PolicyDataExceptionDto]

Array of all the policy data exceptions

SettingsDataDto

geo (optional)
GeoDto
 ips (optional)
array[String]
 Array of all the IP addresses in the policy settings
 example: ["1.2.3.4/24","4.5.6.7/24"]

Imperva Netsec Settings API

View allowlist policies for the DDoS Network and IP Protection services that are defined in your account. For full feature documentation, see [DDoS Protection - Allowlist Policies](#).

Version: 1.0.0

BasePath:/netsec-settings

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AddNetwork

- `post /netsec/v2/add/network`

AllowlistPolicyManagement

- `post /netsec/v2/accounts/{caid}/allowlists/add`
- `post /netsec/v2/accounts/{caid}/allowlists/{allowListId}`
- `delete /netsec/v2/accounts/{caid}/allowlists/{allowListId}`
- `put /netsec/v2/accounts/{caid}/allowlists/edit/{allowListId}`
- `get /netsec/v2/accounts/{caid}/allowlists/{allowListId}`
- `get /netsec/v2/accounts/{caid}/allowlists`
- `get /netsec/v2/policies/{caid}/allowlists/{policyType}`
- `post /netsec/v2/accounts/{caid}/allowlists/associations/{allowlistId}`
- `post /netsec/v2/accounts/{caid}/od-allowlists/associations/{allowlistId}`

AddNetwork

```
post /netsec/v2/add/network
```

Add network range (addNetwork)

After you are onboarded to the DDoS Protection for Networks service, you can add additional network ranges.

Prerequisite: There must be at least one ASN already configured for your account and associated with a routing policy. For details, see <https://docs.imperva.com/bundle/cloud-application-security/page/network-connections-api-definition.htm>

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body NetworkRequestDTO (required)
Body Parameter

Query parameters

caid (optional)

Query Parameter

— The Imperva Account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID format: int64

Return type

NetworkResponseDTO

Example data

Content-Type: application/json

```
{
  "message" : "Protected network is successfully added",
  "status" : "OK"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

403

Forbidden

200

OK NetworkResponseDTO

500

Internal server error

401

Unauthorized user

AllowlistPolicyManagement

```
post /netsec/v2/accounts/{caid}/allowlists/add
```

Add allowlist (addAllowlist)

Create an allowlist by sending the following structure in the body of the request:
[{"name": "[name]", "description": "[description]", "rules": "[rules]", "type": "[type (IP, RANGE)]"}].

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body InitialAllowListDto (required)

Body Parameter

Return type

AllowListDto

Example data

Content-Type: application/json

```
{
  "accountId" : 6,
  "assets" : "[1,2] - list of security policy ids that the allowlist is applied on",
  "lastModifiedBy" : 1,
  "name" : "Allowlist name",
  "description" : "Allowlist description",
  "rules" : "6001,CUSTOM_VECTOR,ip.proto==7 && ip.src==1.1.1.1",
  "subType" : "MONITORING or SECURITY",
  "id" : 0,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "type" : "IP or RANGE"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AllowListDto

500

Internal Server Error

```
post /netsec/v2/accounts/{caid}/allowlists/{allowListId}
```

Clone allowlist (cloneAllowList)

Copy an existing allowlist according to its ID.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

format: int64
 allowListId (required)
 Path Parameter
 — Source allowlist ID format: int64

Return type

[AllowListDto](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 6,
  "assets" : "[1,2] - list of security policy ids that the allowlist is applied on",
  "lastModifiedBy" : 1,
  "name" : "Allowlist name",
  "description" : "Allowlist description",
  "rules" : "6001,CUSTOM_VECTOR,ip.proto==7 && ip.src==1.1.1.1",
  "subType" : "MONITORING or SECURITY",
  "id" : 0,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "type" : "IP or RANGE"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

OK [AllowListDto](#)

500

Internal Server Error

```
delete /netsec/v2/accounts/{caid}/allowlists/{allowListId}
```

Remove allowlist (deleteAllowlist)
 Remove an allowlist according to its ID.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

format: int64

allowListId (required)

Path Parameter

— Allowlist ID to delete format: int64

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK

500

Internal Server Error

```
put /netsec/v2/accounts/{caid}/allowlists/edit/{allowListId}
```

Edit allowlist (editAllowlist)

Overwrite an existing allowlist by sending the following structure in the body of the request:

[{"id": "[id]", "name": "[name]", "description": "[description]", "rules": "[rules]", "type": "[type]", "assets": "[assets]"}].

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

format: int64

allowListId (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [AllowListUIDto](#) (required)
Body Parameter

Return type

[AllowListDto](#)

Example data

Content-Type: application/json

```
{
  "accountId" : 6,
  "assets" : "[1,2] - list of security policy ids that the allowlist is applied on",
  "lastModifiedBy" : 1,
  "name" : "Allowlist name",
  "description" : "Allowlist description",
  "rules" : "6001,CUSTOM VECTOR,ip.proto==7 && ip.src==1.1.1.1",
  "subType" : "MONITORING or SECURITY",
  "id" : 0,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "type" : "IP or RANGE"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AllowListDto](#)

500

Internal Server Error

```
get /netsec/v2/accounts/{caid}/allowlists/{allowListId}
```

Get allowlist (getAllowlist)
Retrieves details of the specified allowlist policy according its ID.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

format: int64

allowListId (required)

Path Parameter

— Allowlist ID format: int64

Return type

AllowListUIDto

Example data

Content-Type: application/json

```
{
  "accountId" : 6,
  "assets" : "[1,2] - list of security policy ids that the allowlist is applied on",
  "name" : "Allowlist name",
  "description" : "Allowlist description",
  "rules" : "6001,CUSTOM_VECTOR,ip.proto==7\n6002,CUSTOM_VECTOR,ip.src==1.1.1.1",
  "id" : 0,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "type" : "SECURITY or MONITORING"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AllowListUIDto

500

Internal Server Error

```
get /netsec/v2/accounts/{caid}/allowlists
```

Get all allowlists (getAllowlistsList)
Retrieves a list of all allowlists.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
format: int64

Return type

AllowListDto

Example data

Content-Type: application/json

```
{
  "accountId" : 6,
  "assets" : "[1,2] - list of security policy ids that the allowlist is applied on",
  "lastModifiedBy" : 1,
  "name" : "Allowlist name",
  "description" : "Allowlist description",
  "rules" : "6001,CUSTOM_VECTOR,ip.proto==7 && ip.src==1.1.1.1",
  "subType" : "MONITORING or SECURITY",
  "id" : 0,
  "lastModified" : "2000-01-23T04:56:07.000+00:00",
  "type" : "IP or RANGE"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AllowListDto

500

Internal Server Error

```
get /netsec/v2/policies/{caid}/allowlists/{policyType}
```

Get list of policies by allowlist type (getSecurityPoliciesForAllowListType)
 Retrieves the list of policies by allowlist type (IP, RANGE).

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.
 format: int64

policyType (required)

Path Parameter

— Policy Type. Can be either IP or RANGE

Query parameters

page (required)

Query Parameter

sizePerPage (required)

Query Parameter

searchTerm (optional)

Query Parameter

allowListName (optional)

Query Parameter

Return type

SecurityPolicyDto

Example data

Content-Type: application/json

```
{
  "name" : "Security Policy Name",
  "id" : 0,
  "rangeIPAddress" : "1.1.1.1/24"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SecurityPolicyDto

500

Internal Server Error

```
post /netsec/v2/accounts/{caid}/allowlists/associations/{allowlistId}
```

Apply security allowlist to assets (setAssociatedPolicies)

Apply the security allowlist policy to any or all security policies in your account. Send the relevant security policy IDs in the request body.

To locate the ID of a security policy, use the /netsec/v2/policies/{caid}/allowlists/{policyType} API.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID.

format: int64

allowlistId (required)

Path Parameter

— Allowlist ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body long (required)

Body Parameter

Responses

200

OK

500

Internal Server Error

```
post /netsec/v2/accounts/{caid}/od-allowlists/associations/{allowlistId}
```

Apply monitoring allowlist to assets (setAssociatedRanges)

Apply the monitoring allowlist policy to any or all network prefixes in your account. Send the relevant network prefix IDs in the request body.

To locate the IDs of the account's protected networks, use the /api/v2/ddos-protection/account/{accountId}/protected-networks-ids API.

Path parameters

caid (required)

Path Parameter

— The Imperva account ID. By default, the API operates on account (A) associated with the API credentials used for authentication. To operate on a different account (an account under the account (A)), specify the account ID. format: int64

allowlistId (required)

Path Parameter

— Allowlist ID format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body long (required)

Body Parameter

Responses

200

OK

500

Internal Server Error

Models

Methods

Table of Contents

1. AllowListDto
2. AllowListUIDto
3. InitialAllowListDto
4. NetworkRequestDTO
5. NetworkResponseDTO
6. SecurityPolicyDto

AllowListDto

id (optional)
Long
format: int64
name (optional)
String
example: Allowlist name
description (optional)
String
example: Allowlist description
accountId (optional)
Long
format: int64
type (optional)
String
Enum:
IP
RANGE
example: IP or RANGE
lastModified (optional)
Date
format: date-time
lastModifiedBy (optional)
Long
format: int64
assets (optional)
array[**Long**]
format: int64
example: [1,2] - list of security policy ids that the allowlist is applied on
rules (optional)
String
example: 6001,CUSTOM_VECTOR,ip.proto==7 && ip.src==1.1.1.1
subType (optional)
String
Enum:
MONITORING
SECURITY
example: MONITORING or SECURITY

AllowListUIDto

id (optional)
Long
The unique identifier assigned to the allowlist by Imperva format: int64
name (optional)

String

The user-defined name for the allowlist.

example: Allowlist name

description (optional)

String

A description of the allowlist.

example: Allowlist description

accountId (optional)

Long

The Imperva account ID. format: int64

lastModified (optional)

Date

The time stamp of the last change to the policy. format: date-time

type (optional)

String

The allow list sub type. Indicates if it is a security (default) or monitoring allow list.

Enum:

MONITORING

SECURITY

example: SECURITY or MONITORING

rules (optional)

String

The conditions under which legitimate traffic is permitted. Rules must be formatted as follows: rule id (any number between 6001 and 7999; must be unique within a policy), CUSTOM_VECTOR, attribute operator value

example: 6001,CUSTOM_VECTOR,ip.proto==7

6002,CUSTOM_VECTOR,ip.src==1.1.1.1

assets (optional)

array[Long]

The assets in the account to which the policy is applied. format: int64

example: [1,2] - list of security policy ids that the allowlist is applied on

InitialAllowListDto

Allowlist to add in the structure of

```
[{"name": "allowlist_name", "description": "allowlist_description", "rules": [{"rule_id": 6001, "operator": "CUSTOM_VECTOR", "value": "ip.proto==7"}, {"rule_id": 6002, "operator": "CUSTOM_VECTOR", "value": "ip.src==1.1.1.1"}], "subType": "SECURITY"}
```

name (optional)

String

example: Allowlist name

description (optional)

String

example: Allowlist description

accountId (optional)

Long

format: int64

type (optional)

String

Enum:

IP

RANGE

example: IP or RANGE

lastModifiedBy (optional)

Long

format: int64

lastModified (optional)

Date

format: date-time

rules (optional)

String
example: 6001,CUSTOM_VECTOR,ip.proto==7 && ip.src==1.1.1.1
assets (optional)
array[Long]
format: int64
example: [1,2] - list of security policy ids that the allowlist is applied on
subType (optional)
String
Enum:
MONITORING
SECURITY
example: SECURITY or MONITORING

NetworkRequestDTO

accountId (optional)
String
example: Account Id
asn (optional)
String
Enter the ASN which is associated with a Routing Policy. The ASN from which you peer with Imperva and through which the prefix will be advertised to Imperva.
example: ASN Number
range (optional)
String
example: Prefix/Range
description (optional)
String
example: Describe the Prefix/Range (Optional field)
protectionType (optional)
String
AlwaysOn: Your network traffic is constantly routed through Imperva. OnDemand: Your network traffic is routed through Imperva only during a DDoS attack(specifying a diversion method and monitoring method is required).
example: OnDemand
diversionMethod (optional)
String
Automatic: When using remote monitoring your traffic can be diverted automatically. Requires Confirmation: only after your confirmation (Supported only for IPv4 networks). Self-Managed: you are controlling the divert and revert operations.
example: Automatic
monitoringMethod (optional)
String
Adaptive: System control, Imperva will monitor your network and used AI to set the right thresholds for your monitoring policy. Non-Adaptive: User control, you are controlling the threshold from which you want to receive a notification for DDoS. Non-Monitored: No monitoring sent to Imperva, you are responsible to monitor and manually divert your traffic to Imperva when needed.
example: Adaptive
bandwidth (optional)
String
The traffic profile is used for setting initial security and detection policies. These policies will be regularly adjusted based on your actual monitored traffic. Bandwidth options: 100 or 500 or 1000 or 2000
example: 100
trafficMix (optional)
String
Traffic mix options: TCP or UDP or OTHER or TCP_UDP or TCP_OTHER or UDP_OTHER or TCP_UDP_OTHER
example: TCP

NetworkResponseDTO

message (optional)

String

example: Protected network is successfully added

status (optional)

String

example: OK

SecurityPolicyDto

id (optional)

Long

format: int64

name (optional)

String

example: Security Policy Name

rangelIPAddress (optional)

array[String]

example: 1.1.1.1/24

DDoS Protection for Networks/IPs: Asset Management

Version: 1.0.0

BasePath:/api/v2/ddos-protection

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountProtectedIPs

- `get /account/{accountId}/protected-ips-ids`

AccountProtectedNetworks

- `get /account/{accountId}/protected-networks-ids`

AccountProtectedIPs

```
get /account/{accountId}/protected-ips-ids
```

Retrieve the account's protected IPs and their IDs (getAccountProtectedIpsAndIds)
Retrieve the account's protected IPs and their IDs.

Path parameters

accountId (required)

Path Parameter

— The account ID. format: int64

Return type

[IdProtectedIpMap](#)

Example data

Content-Type: application/json

```
[ "123=1.2.3.4,133=5.6.7.8", "123=1.2.3.4,133=5.6.7.8" ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

500

Internal server error

200

Successful operation. [IdProtectedIpMap](#)

AccountProtectedNetworks

```
get /account/{accountId}/protected-networks-ids
```

Retrieve the account's protected networks and their IDs (getAccountRangesAndIds)
Retrieve the account's protected networks and their IDs.

Path parameters

accountId (required)

Path Parameter

— The account ID. format: int64

Return type

[IdProtectedNetworkMap](#)

Example data

Content-Type: application/json

```
[ "123=1.2.3.4/24,133=5.6.7.8/24", "123=1.2.3.4/24,133=5.6.7.8/24" ]
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

500

Internal server error

200

Successful operation. [IdProtectedNetworkMap](#)

Models

Methods

Table of Contents

- [IdProtectedIpMap](#)
- [IdProtectedNetworkMap](#)

IdProtectedIpMap

A list containing all the account protected IPs and their IDs.

IdProtectedNetworkMap

A list containing all the account protected networks and their IDs.

Cloud Application Security API

Imperva provides customers and partners with the ability to manage accounts and sites via an API. For more information, see [Cloud Application Security API Reference](#).

Version: 1.0

Imperva License Agreement.

http://www.imperva.com/other/license_agreement.asp

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

TrafficStatisticsAndLogs

- post /api/v1/infra/events
- post /api/v1/infra/histogram
- post /api/v1/infra/top-graph
- post /api/v1/infra/top-table
- post /api/v1/infra/stats
- post /api/stats/v1
- post /api/visits/v1

TrafficStatisticsAndLogs

```
post /api/v1/infra/events
```

Get infrastructure protection events (getInfraEvents)

Use this operation to get Infrastructure Protection event information for an account

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters.

event_type (optional)

Query Parameter

— A comma separated list of specific event types. Any of: GRE_TUNNEL_UP, GRE_TUNNEL_DOWN, ORIGIN_CONNECTION_GRE_UP, ORIGIN_CONNECTION_GRE_DOWN, ORIGIN_CONNECTION_ECX_UP, ORIGIN_CONNECTION_ECX_DOWN, ORIGIN_CONNECTION_CROSS_CONNECT_UP, ORIGIN_CONNECTION_CROSS_CONNECT_DOWN, DDOS_START_IP_RANGE, DDOS_STOP_IP_RANGE, DDOS QUIET TIME IP RANGE, EXPORTER_NO_DATA, EXPORTER_BAD_DATA, EXPORTER_GOOD_DATA, MONITORING_CRITICAL_ATTACK, PROTECTED_IP_STATUS_UP, PROTECTED_IP_STATUS_DOWN, PER_IP_DDOS_START_IP_RANGE.

ip_prefix (optional)

Query Parameter

— Specific Protected IP or IP range. For example, 1.1.1.0/24.

page_size (optional)

Query Parameter

— The number of objects to return in the response.
Default: 50
Maximum: 100

page_num (optional)

Query Parameter

— The page to return starting from 0. Default: 0

start (optional)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (optional)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

Return type

[inline_response_200](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input [inline_response_200](#)

```
post /api/v1/infra/histogram
```

Get infrastructure protection histogram (getInfraProtectHistogram)

Use this operation to view the highest packet size values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and

end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

Return type

[inline_response_200_1](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_1](#)

```
post /api/v1/infra/top-graph
```

Get infrastructure protection top items (graph view) (getInfraProtectTopData)

Use this operation to view the highest peak values and highest average values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.
last_7_days Retrieve data from midnight of 7 days ago until the current time.
last_30_days Retrieve data from midnight of 30 days ago until the current time.
last_90_days Retrieve data from midnight of 90 days ago until the current time.
month_to_date Retrieve data from midnight of the first day of the month until the current time.
custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.
last_7_days Retrieve data from midnight of 7 days ago until the current time.
last_30_days Retrieve data from midnight of 30 days ago until the current time.
last_90_days Retrieve data from midnight of 90 days ago until the current time.
month_to_date Retrieve data from midnight of the first day of the month until the current time.
custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:
A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

data_type (required)

Query Parameter

— One of the following: SRC_IP, DST_IP, SRC_PORT_PROTOCOL, DST_PORT_PROTOCOL

metric_type (required)

Query Parameter

— One of the following: BW, PPS

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

objects (optional)

Query Parameter

— A comma separated list of items to fetch data for. e.g., 10.10.10.10, 2.2.2.2. If not specified, top items are automatically fetched.

Return type

[inline_response_200_2](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_2](#)

```
post /api/v1/infra/top-table
```

Get infrastructure protection top items (table view) (getInfraProtectTopTable)

Use this operation to view the highest peak values and highest average values for a protected IP range during a selected time period.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_range (required)

Query Parameter

— The customer's IP range.

range_type (required)

Query Parameter

— One of the following: BGP, PROTECTED_IP, NETFLOW

start (required)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (required)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days

ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

data_type (required)

Query Parameter

— One of the following: SRC_IP, DST_IP, SRC_PORT_PROTOCOL, DST_PORT_PROTOCOL

metric_type (required)

Query Parameter

— One of the following: BW, PPS

mitigation_type (required)

Query Parameter

— One of the following: BLOCK, PASS

aggregation_type (required)

Query Parameter

— One of the following: PEAK, AVERAGE

data_storage_region (optional)

Query Parameter

— The data region to use. If not specified, account's default data region will be used.

Return type

[inline_response_200_3](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
1 - Unexpected error [inline_response_200_3](#)

```
post /api/v1/infra/stats
```

Get infrastructure protection statistics (getInfraStats)

Use this operation to get Infrastructure Protection event information for an account.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to operate on.
If not specified, operation will be performed on the account identified by the authentication parameters. format: int64

ip_prefix (optional)

Query Parameter

— Specific Protected IP or IP range. For example, 1.1.1.0/24.

traffic (optional)

Query Parameter

— Specific traffic. One of: Total, Passed, Blocked.

traffic_type (optional)

Query Parameter

— A comma separated list of specific traffic types. Any of: UDP, TCP, DNS, DNS_RESPONSE, ICMP, SYN, FRAG, LARGE_SYN, NTP, NETFLOW, SSDP, GENERAL. Cannot be used together with the pop parameter.

pop (optional)

Query Parameter

— A comma separated list of specific PoP names. For example: iad, tko. Cannot be used together with the traffic_type parameter. For the list of PoP codes and locations, see Imperva Data Centers (PoPs).

start (optional)

Query Parameter

— The start date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

end (optional)

Query Parameter

— The end date in milliseconds, since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

format: int64

directionTypes (optional)

Query Parameter

— The type of direction(INGRESS/EGRESS) to filter the data

range_type (optional)

Query Parameter

— Can be one of the following: BGP, PROTECTED_IP, NETFLOW

Return type

[inline_response_200_4](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
2 - Invalid input
3015 - Internal error [inline_response_200_4](#)

```
post /api/stats/v1
```

Get statistics (getStats)

Get site statistics for one or more sites. This operation may return multiple statistics, as specified in the stats parameter.

Query parameters

account_id (optional)

Query Parameter

— Numeric identifier of the account to fetch data for.
Note: You must specify either account_id or site_id.

time_range (required)

Query Parameter

— Time range to fetch data for.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.
last_7_days Retrieve data from midnight of 7 days ago until the current time.
last_30_days Retrieve data from midnight of 30 days ago until the current time.
last_90_days Retrieve data from midnight of 90 days ago until the current time.
month_to_date Retrieve data from midnight of the first day of the month until the current time.
custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:

- A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.
- A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days.
- A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

Query Parameter

— Start date in milliseconds since January 1, 1970 (midnight UTC/GMT). Used together with the time_range parameter to specify a custom time range.

end (optional)

Query Parameter

— End date in milliseconds since January 1, 1970 (midnight UTC/GMT). Used together with the time_range parameter to specify a custom time range.

site_id (optional)

Query Parameter

— Numeric identifier of the site to fetch data for. Multiple sites can be specified in a comma separated list. For example: 123,124,125.
Note: You must specify either account_id or site_id.

stats (required)

Query Parameter

— Statistics to fetch, as specified in the table below. Multiple statistics can be specified in a comma separated list.
Values for the stats parameters:
visits_timeseries Number of sessions by type (Humans/Bots) over time.hits_timeseries Number of requests by type (Humans/Bots/Blocked) over time and per second.bandwidth_timeseries Amount of bytes (bandwidth) and bits per second (throughput) transferred via the Imperva network from clients to proxy servers and vice-versa over time.requests_geo_dist_summary Total number of requests routed via the Imperva network by data center location.visits_dist_summary Total number of sessions per client application and country.caching Total number of requests and bytes that were cached by the Imperva network.caching_timeseries Number of requests and bytes that were cached by the Imperva network, with one day resolution, with info regarding the caching mode (standard or advanced).threats Total number of threats by type with additional information regarding the security rules configuration.incap_rules List of security rules with total number of reported incidents for each rule.incap_rules_timeseries List of security rules with a series of reported incidents for each rule with the specified granularity.delivery_rules List of delivery rules with total number of hits for each rule.delivery_rules_timeseries List of delivery rules with a series of hits for each rule with the specified granularity.

granularity (optional)

Query Parameter

— Time interval in milliseconds between data points for time series statistics. (See the timeseries values in the table below.)
The default granularity depends on the specified time range, as follows:
Time range of less than 24 hours: Default granularity is 7200000 (2 hours).Time range of between 24 hours and 30 days: Default granularity is 86400000 (1 day).Time range of more than 30 days: Default granularity is 259200000 (3 days).The response includes one result for each interval. For example, if you specify a time range value of last_7_days, the default granularity is 1 day, and the response will return 7 results.
The response timestamps are in milliseconds since January 1, 1970 (midnight UTC/GMT)
Minimum granularity is 5 minutes (300000).
Note: Time series statistics are presented oldest to newest.

Return type

[inline_response_200_5](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
 13001 (Timerange invalid), 13002 (Granularity invalid)
[inline_response_200_5](#)

```
post /api/visits/v1
```

Get visits (getVisits)

Use this operation to get a log of recent visits to a website.

Query parameters

site_id (required)

Query Parameter

— Numeric identifier of the site to operate on.

time_range (optional)

Query Parameter

— Time range to fetch data for. Default is last_7_days.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

start (optional)

Query Parameter

— Start date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

end (optional)

Query Parameter

— End date in milliseconds since 1970.
Some operations require the user to specify a time range. This is done via the time_range parameter, which accepts the following values:
today Retrieve data from midnight today until the current time.last_7_days Retrieve data from midnight of 7 days ago until the current time.last_30_days Retrieve data from midnight of 30 days ago until the current time.last_90_days Retrieve data from midnight of 90 days ago until the current time.month_to_date Retrieve data from midnight of the first day of the month until the current

time.custom Specify a custom time range using two additional parameters: start and end.
Results are provided for full days only, starting from midnight. A time range of less than 24 hours gives results for the full day.
For example:A time range of 14:00 - 20:00 yesterday gives results for all of yesterday (midnight to midnight) - a full day.A time range of 14:00 last Tuesday to 14:00 last Wednesday gives results for all of Tuesday and Wednesday - two full days. A time range of 14:00 yesterday to 14:00 today gives results for all of yesterday starting from midnight until the current time today.

page_size (optional)

Query Parameter

— The number of objects to return in the response. Defaults to 10. Maximum is 100.

page_num (optional)

Query Parameter

— The page to return starting from 0. Default to 0.

security (optional)

Query Parameter

— Filter the sessions that were handled according to the security-related specifications. Multiple values are supported, e.g.: "api.threats.sql_injection, api.acl.blacklisted_ips".

country (optional)

Query Parameter

— Filter the sessions coming from the specified country.

ip (optional)

Query Parameter

— Filter the sessions coming from the specified IP.

visit_id (optional)

Query Parameter

— Comma separated list of visit IDs to load.

list_live_visits (optional)

Query Parameter

— Whether or not to list visits that did not end and that may still be updated.
Possible values: true, false
Default: true

use_previous_region (optional)

Query Parameter

— Whether or not to list visits from old region data. Valid only if a data region was changed in the last 90 days. One of: true | false. Default: false

Return type

[inline_response_200_6](#)

Example data

Content-Type: application/json

```
""
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

res - contains the specific error code:
1 - Unexpected error [inline_response_200_6](#)

Models

Methods

Table of Contents

1. [ADRule](#)
 2. [ADRuleSeries](#)
 3. [ActionItem](#)
 4. [AnalyticsHistogramApiResponse](#)
 5. [AnalyticsTopGraphDataResponse](#)
 6. [AnalyticsTopTableApiResponse](#)
 7. [AnalyticsTopTableData](#)
 8. [ApiResult](#)
 9. [ApiResultSessions](#)
 10. [ApiResultSiteStats](#)
 11. [Caching](#)
 12. [IncapRule](#)
 13. [IncapRuleSeries](#)
 14. [InfraEventsApiResponse](#)
 15. [InfraProtectEvent](#)
 16. [InfraStatsApiResponse](#)
 17. [RequestsGeo](#)
 18. [SessionItem](#)
 19. [Stats](#)
 20. [Threat](#)
 21. [ThreatItem](#)
 22. [TimeSeriesItem](#)
 23. [TopGraphPayloads](#)
 24. [VisitsItem](#)
 25. [VisitsSummary](#)
 26. [inline_response_200](#)
 27. [inline_response_200_1](#)
 28. [inline_response_200_2](#)
 29. [inline_response_200_3](#)
 30. [inline_response_200_4](#)
 31. [inline_response_200_5](#)
 32. [inline_response_200_6](#)
-

ADRule

id (optional)
String
 name (optional)
String
 action (optional)
String
 example: Redirect
 createdAt (optional)
Date
 format: date-time
 updatedBy (optional)
String
 example: example@imperva.com
 hits (optional)
Long
 format: int64
 example: 3451

ADRuleSeries

id (optional)
String
 name (optional)
String
 action (optional)
String
 example: Redirect
 createdAt (optional)
Date
 format: date-time
 updatedBy (optional)
String
 example: example@imperva.com
 hits (optional)
array[Object]
 example: [[1478613600000,6],[1478617200000,3]]

ActionItem

queryString (optional)
String
 example: ?jobSYapi_password\u003dXXXXX
 postData (optional)
String
 requestResult (optional)
String
 requestResult
 example: api.request_result.req_challenge_javascript
 isSecured (optional)
Boolean
 example: false
 url (optional)
String
 example: www.google.com/ddos/ddos-mitigation-services
 httpStatus (optional)

Integer
format: int32
example: 200
responseTime (optional)

Long
format: int64
example: 170
thinkTime (optional)

Long
format: int64
example: 169
incidentId (optional)

String
example: 3411008890000033213-29571073433152
threats (optional)
array[ThreatItem]

AnalyticsHistogramApiResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
stats (optional)
array[map[String, Object]]
example: {"PL_100": "366450640", "PL_200": "305475960", "PL_300": "0", "PL_400": "0", "PL_500": "0", "PL_600": "0", "PL_700": "0", "PL_800": "0", "PL_900": "0", "PL_1000": "0", "PL_1100": "0", "PL_1200": "0", "PL_1300": "0", "PL_1400": "0", "PL_1500": "0"}

AnalyticsTopGraphDataResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
stats (optional)
array[Stats]

AnalyticsTopTableApiResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String

example: OK
debug_info (optional)
array[map[String, Object]]
stats (optional)
array[AnalyticsTopTableData]

AnalyticsTopTableData

object (optional)
String
example: 10.200.98.3
value (optional)
Double
format: double
example: 334160

ApiResult

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]

ApiResultSessions

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
visits (optional)
array[SessionItem]

ApiResultSiteStats

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]
visits_timeseries (optional)
array[VisitsItem]
requests_geo_dist_summary (optional)

RequestsGeo
 visits_dist_summary (optional)
 array[VisitsSummary]
 caching (optional)
Caching
 caching_timeseries (optional)
 array[TimeSeriesItem]
 hits_timeseries (optional)
 array[TimeSeriesItem]
 bandwidth_timeseries (optional)
 array[TimeSeriesItem]
 threats (optional)
 array[Threat]
 incap_rules (optional)
 array[IncapRule]
 incap_rules_timeseries (optional)
 array[IcapRuleSeries]
 delivery_rules (optional)
 array[ADRule]
 delivery_rules_timeseries (optional)
 array[ADRuleSeries]

Caching

saved_requests (optional)

Long

format: int64

example: 23984923

total_requests (optional)

Long

format: int64

example: 48723648

saved_bytes (optional)

Long

format: int64

example: 762394786

total_bytes (optional)

Long

format: int64

example: 1098349834

IncapRule

id (optional)
String
 name (optional)
String
 action (optional)
String
 example: Require Javascript Support
 incidents (optional)
Long
 format: int64
 example: 3451
 createdAt (optional)
Date
 format: date-time

updatedBy (optional)

String

example: example@imperva.com

IncapRuleSeries

id (optional)

String

name (optional)

String

action (optional)

String

example: Require Javascript Support

createdAt (optional)

Date

format: date-time

updatedBy (optional)

String

example: example@imperva.com

incidents (optional)

array[Object]

example: [[1478613600000,6],[1478617200000,3]]

InfraEventsApiResponse

res (optional)

Integer

res - contains specific error code format: int32

example: 0

res_message (optional)

String

example: OK

debug_info (optional)

array[map[String, Object]]

events (optional)

array[InfraProtectEvent]

InfraProtectEvent

eventTime (optional)

Date

format: date-time

eventType (optional)

String

Enum:

GRE_TUNNEL_UP

GRE_TUNNEL_DOWN

ORIGIN_CONNECTION_GRE_UP

ORIGIN_CONNECTION_GRE_DOWN

ORIGIN_CONNECTION_ECX_UP

ORIGIN_CONNECTION_ECX_DOWN

ORIGIN_CONNECTION_CROSS_CONNECT_UP

ORIGIN_CONNECTION_CROSS_CONNECT_DOWN

IP_RANGE_ATTACK_START

IP_RANGE_ATTACK_STOP

DDOS_START_IP_RANGE

DDOS_STOP_IP_RANGE
DDOS QUIET TIME IP RANGE
EXPORTER_NO_DATA
EXPORTER_BAD_DATA
EXPORTER_GOOD_DATA
MONITORING_ATTACK
MONITORING_CRITICAL_ATTACK
PROTECTED_IP_STATUS_UP
PROTECTED_IP_STATUS_DOWN
PROTECTED_NETWORK_STATUS_ACTIVE
PROTECTED_NETWORK_STATUS_INACTIVE
PER_IP_DDOS_START_IP_RANGE
PER_IP_DDOS_STOP_IP_RANGE
IIP_ACCOUNT_SERVICE_SUSPENDED
IIP_ACCOUNT_SERVICE_UNSUSPENDED
INFRAPROTECT_NULL_ROUTE_STARTED
INFRAPROTECT_NULL_ROUTE_ESCALATED
INFRAPROTECT_NULL_ROUTE_ENDED
INFRAPROTECT_RANGE_DIVERT
INFRAPROTECT_RANGE_REVERT
BGP_UP
BGP_DOWN
CONNECTION_PERFORMANCE_DEGRADED
CONNECTION_PERFORMANCE_RESTORED
example: DDOS_STOP_IP_RANGE
bwTotal (optional)
Long
format: int64
example: 9000
ppsTotal (optional)
Long
format: int64
example: 90
bwPassed (optional)
Long
format: int64
example: 200
ppsPassed (optional)
Long
format: int64
example: 87
bwBlocked (optional)
Long
format: int64
example: 8800
ppsBlocked (optional)
Long
format: int64
example: 3
eventTarget (optional)
String
Enum:
GRE_TUNNEL
IP_RANGE
EXPORTER
PROTECTED_IP
INCAPSULA_IP
NULL_ROUTE
BGP

example: IP_RANGE
reportedByPop (optional)
String
example: zrh

InfraStatsApiResponse

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)
String
example: OK
debug_info (optional)
array[map[String, Object]]

RequestsGeo

id (optional)
String
name (optional)
String
data (optional)
array[Object]
example: [['Tokyo, JA',24365435],['Los Angeles, CA',98762738]]

SessionItem

id (optional)
String
example: 133077760038625792
sitelId (optional)
Long
format: int64
example: 7
startTime (optional)
Long
format: int64
example: 1361468485000
endTime (optional)
Long
format: int64
example: 1361468486000
clientIPs (optional)
array[Object]
country (optional)
array[Object]
countryCode (optional)
array[Object]
clientType (optional)
String
example: Unclassified
clientApplication (optional)
String
example: Bot

clientApplicationId (optional)
Long
format: int64
example: 0
httpVersion (optional)
String
example: 2.0
clientApplicationVersion (optional)
String
example: 0
userAgent (optional)
String
example: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)
os (optional)
String
example: Windows
osVersion (optional)
String
example: Windows
supportsCookies (optional)
Boolean
example: true
supportsJavaScript (optional)
Boolean
example: true
hits (optional)
Long
format: int64
example: 1
pageViews (optional)
Long
format: int64
example: 1
entryReferer (optional)
String
example: http://lp.usafis.org/_Incapsula_Resource?CWUDNSAI=9_E1521557&incident_id=13307776003810242
3-139906691365201416&edet=12&cinfo=2ef678e2c753856785000000
entryPage (optional)
String
example: www.incapsula.com/ddos/ddos-mitigation-services
servedVia (optional)
array[Object]
securitySummary (optional)
array[map[String, Object]]
example: {"api.threats.sql_injection":"2","api.threats.cross_site_scripting":"1","api.threats.illegal_resource_acces s":"3","api.threats.remote_file_inclusion":"2","api.threats.customRule":"3","api.threats.ddos-DDoS":"4","api.threat s.backdoor":"2","api.threats.bot_access_control":"1","api.acl.blacklisted_countries":"1","api.acl.blacklisted_url s":"1","api.acl.blacklisted_ips":"1"}
actions (optional)
array[ActionItem]

Stats

res (optional)
Integer
res - contains specific error code format: int32
example: 0
res_message (optional)

String
example: OK
debug_info (optional)
array[map[String, Object]]
objectid (optional)
String
example: 200
time (optional)
String
example: 1522761000000
payload (optional)
array[TopGraphPayloads]

Threat

id (optional)
String
name (optional)
String
incidents (optional)
Long
format: int64
example: 12
status (optional)
String
example: ok
status_text_id (optional)
String
example: api.threats.action.block_request
status_text (optional)
String
example: Block Request
followup (optional)
String
example: api.threats.followup.view
followup_text (optional)
String
example: View Incidents
followup_url (optional)
String
example: https://my.incapsula.com/sites/siteVisits?token=1123_103_13234435091_5d55197912387b94&timeFrame=last_7_days&extSiteId=123&threatFilters=badBot

ThreatItem

threats
securityRule (optional)
String
example: api.threats.illegal_resource_access
alertLocation (optional)
String
example: api.alert_location.alert_location_path
attackCodes (optional)
array[Object]
securityRuleAction (optional)
String
example: api.rule_action_type.rule_action_block

TimeSeriesItem

id (optional)
String
name (optional)
String
data (optional)
array[Object]
example: [[1344247200000,5]]

TopGraphPayloads

interval (optional)
String
example: 15000
startTime (optional)
Date
format: date-time
data (optional)
array[Object]
example: [5462,7563]
metric (optional)
String
example: pps
dataType (optional)
String
example: ip
item (optional)
String
example: 10.13.0.1
traffic (optional)
String
example: blocked

VisitsItem

id (optional)
String
name (optional)
String
data (optional)
array[Object]
example: [[1344247200000,50],[1344247500000,40]]

VisitsSummary

id (optional)
String
name (optional)
String
data (optional)
array[array[Object]]
example: [['np',15],['no',778]]

inline_response_200

```
inline_response_200_1
```

```
inline_response_200_2
```

```
inline_response_200_3
```

```
inline_response_200_4
```

```
inline_response_200_5
```

```
inline_response_200_6
```

Imperva DNS

Manage your configuration for the Imperva DNS Protection service. For full feature documentation, see [DNS Protection](#).

Version: 1.0.0

BasePath:/dns

The terms in the absence of an applicable signed agreement between you and Imperva
<https://www.imperva.com/legal/license-agreement/>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountConfigurationV3

- `post /v3/account-configuration/automatic-safe-record`
- `put /v3/account-configuration/automatic-safe-record/{config-id}/apply-on-assets`
- `delete /v3/account-configuration/automatic-safe-record/{config-id}`
- `put /v3/account-configuration/automatic-safe-record/{config-id}/status`
- `get /v3/account-configuration/automatic-safe-record`
- `get /v3/account-configuration/automatic-safe-record/domain-sync-details/{domain-id}`
- `put /v3/account-configuration/automatic-safe-record/{config-id}`

Attacks

- `get /attack/{attackId}`
- `get /attack`

AttacksV3

- `get /v3/domains/attacks/{attack-id}`
- `get /v3/domains/attacks`

DNSSIEMLogConfigurationV3

- `get /v3/account-configuration/siem-logs`
- `patch /v3/account-configuration/siem-logs`

Domains

- `post /domain`
- `post /domain/file`
- `post /domain/{domainId}`
- `post /domain/{domainId}/file`
- `put /domain/{domainId}`
- `get /domain`
- `get /domain/{domainId}`
- `delete /domain/{domainId}`
- `post /domain/{domainId}/validate`

DomainsV3

- `get /v3/domains`

PrimaryManagedDomainDNSRecords

- `post /domain/{domainId}/records`
- `delete /domain/{domainId}/records`
- `put /domain/{domainId}/records`
- `get /domain/{domainId}/records`

PrimaryManagedDomainDNSSEC

- `put /domain/{domainId}/dnssec/abort-cancellation`
- `post /domain/{domainId}/dnssec/check`
- `delete /domain/{domainId}/dnssec`
- `post /domain/{domainId}/dnssec`

-
- `get /domain/{domainId}/dnssec`

PrimaryManagedDomainV3

- `post /v3/domains/primary`
- `post /v3/domains/primary/file`
- `delete /v3/domains/primary/{domain-id}`
- `put /v3/domains/primary/{domain-id}/file`
- `get /v3/domains/primary/file/export-all-zones`
- `put /v3/domains/primary/{domain-id}`
- `get /v3/domains/primary`
- `get /v3/domains/primary/{domain-id}`
- `patch /v3/domains/primary/{domain-id}`

ProtectedDomainV3

- `post /v3/domains/protected`
- `delete /v3/domains/protected/{domain-id}`
- `put /v3/domains/protected/{domain-id}`
- `get /v3/domains/protected`
- `get /v3/domains/protected/{domain-id}`
- `get /v3/domains/protected/{domain-id}/safe-records`
- `get /v3/domains/protected/{domain-id}/safe-records/type`
- `patch /v3/domains/protected/{domain-id}`
- `put /v3/domains/protected/{domain-id}/safe-records`
- `put /v3/domains/protected/{domain-id}/safe-records/file`
- `put /v3/domains/protected/{domain-id}/safe-records/type`

PurgeCache

- `post /domain/{domainId}/purge/all`
- `post /domain/{domainId}/purge`

PurgeCacheV3

- `post /v3/domains/protected/{domain-id}/purge-cache`

SecondaryDomain

- `get /secondary-domain/allowed-ips`
- `post /secondary-domain/{domainId}/sync`

SecondaryDomainPrimaryIPs

- post /secondary-domain/{domainId}/primary-ips
- put /secondary-domain/{domainId}/primary-ips
- get /secondary-domain/{domainId}/primary-ips
- delete /secondary-domain/{domainId}/primary-ips

SecondaryDomainTSIGKeys

- post /domain/{domainId}/tsig
- put /domain/{domainId}/tsig
- get /domain/{domainId}/tsig
- delete /domain/{domainId}/tsig

SecondaryDomainV3

- post /v3/domains/secondary
- delete /v3/domains/secondary/{domain-id}
- put /v3/domains/secondary/{domain-id}
- get /v3/domains/secondary
- get /v3/domains/secondary/{domain-id}
- patch /v3/domains/secondary/{domain-id}

Statistics

- get /stats

StatisticsV3

- get /v3/domains/statistics/account-domains
- get /v3/domains/statistics
- get /v3/domains/statistics/origin-server

AccountConfigurationV3

```
post /v3/account-configuration/automatic-safe-record
```

Add new automatic safe record configuration (addAutomaticSafeRecord)
 Add new automatic safe record configuration

Consumes

This API call consumes the following media types via the Content-Type request header:

▪ `*/*`

Request body

body [AutomaticSafeRecordRequestDto](#) (optional)
Body Parameter

Return type

[AutomaticSafeRecordSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    }, {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    }
  }
}
```

```

    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
    "assetDtoList" : [ {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    }, {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
        "appliedOnEntity" : {
            "assetIds" : [ 2, 2 ]
        },
        "accountId" : 5,
        "assetDtoList" : [ null, null ],
        "subConfigurations" : [ null, null ],
        "isDeleted" : true,
        "isEnabled" : true,
        "configurationName" : "configurationName",
        "description" : "description",
        "configurationId" : 5,
        "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
        "isActive" : true,
    } ]
}

```

```

    "configurationValue" : "configurationValue"
}, {
  "appliedOnEntity" : {
    "assetIds" : [ 2, 2 ]
  },
  "accountId" : 5,
  "assetDtoList" : [ null, null ],
  "subConfigurations" : [ null, null ],
  "isDeleted" : true,
  "isEnabled" : true,
  "configurationName" : "configurationName",
  "description" : "description",
  "configurationId" : 5,
  "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
  "isActive" : true,
  "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
  "tsigKeys" : [ {
    "name" : "name",
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "type" : "MD5",
    "value" : "value"
  } ],
  "port" : 7,
  "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
  "type" : "AXFR",
  "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AutomaticSafeRecordSuccessResponse

500

Internal server error [ApiErrorResponse](#)

```
put /v3/account-configuration/automatic-safe-record/{config-id}/apply-on-assets
```

Apply automatic safe record configuration to the provided list of domains (applyAutomaticSafeRecordToDomains)
Apply automatic safe record configuration to the provided list of domains

Path parameters

config-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body [AppliedOnAsset](#) (optional)

Body Parameter

Return type

[AutomaticSafeRecordSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
```

```

    "appliedOnEntity" : {
      "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
  }, {
    "appliedOnEntity" : {
      "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
  }],
  "syncDetailsDto" : {
    "tsigKeys" : [ {
      "name" : "name",
      "type" : "MD5",
      "value" : "value"
    }, {
      "name" : "name",
      "type" : "MD5",
      "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
  },
  "configurationName" : "configurationName",
  "description" : "description",
  "isActive" : true,
  "accountId" : 0,
  "isDeleted" : true,
  "isEnabled" : true,
  "configurationId" : 6,
  "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
  "configurationValue" : "configurationValue"
}, {
  "assetDtoList" : [ {
    "name" : "name",
    "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
    "id" : 1,
  }
]
}

```

```

    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
}, {
    "name" : "name",
    "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
    "id" : 1,
    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
} ],
"subConfigurations" : [ {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,

```

```

    "isDeleted" : true,
    "isEnabled" : true,
    "configurationId" : 6,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "configurationValue" : "configurationValue"
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AutomaticSafeRecordSuccessResponse

500

Internal server error ApiErrorResponse

```
delete /v3/account-configuration/automatic-safe-record/{config-id}
```

Delete automatic safe record configuration (deleteAutomaticSafeRecord)
Delete automatic safe record configuration

Path parameters

config-id (required)

Path Parameter

— format: int64

Return type

AutomaticSafeRecordSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1
    }
  ]
}
}
```

```

    "id" : 1,
    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
}, {
    "name" : "name",
    "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
    "id" : 1,
    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
} ],
"subConfigurations" : [ {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,

```

```

"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
"assetDtoList" : [ {
"name" : "name",
"lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
"id" : 1,
"syncStatus" : "SUCCESS",
"statusMessage" : "statusMessage"
}, {
"name" : "name",
"lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
"id" : 1,
"syncStatus" : "SUCCESS",
"statusMessage" : "statusMessage"
} ],
"subConfigurations" : [ {
"appliedOnEntity" : {
"assetIds" : [ 2, 2 ]
},
"accountId" : 5,
"assetDtoList" : [ null, null ],
"subConfigurations" : [ null, null ],
"isDeleted" : true,
"isEnabled" : true,
"configurationName" : "configurationName",
"description" : "description",
"configurationId" : 5,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"isActive" : true,
"configurationValue" : "configurationValue"
}, {
"appliedOnEntity" : {
"assetIds" : [ 2, 2 ]
},
"accountId" : 5,
"assetDtoList" : [ null, null ],
"subConfigurations" : [ null, null ],
"isDeleted" : true,
"isEnabled" : true,
"configurationName" : "configurationName",
"description" : "description",
"configurationId" : 5,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"isActive" : true,
"configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
"tsigKeys" : [ {
"name" : "name",
"type" : "MD5",
"value" : "value"
}, {
"name" : "name",
"type" : "MD5",

```

```

        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AutomaticSafeRecordSuccessResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
put /v3/account-configuration/automatic-safe-record/{config-id}/status
```

Enable/Disable automatic safe record configuration (enableDisableAutomaticSafeRecord)
Enable/Disable automatic safe record configuration

Path parameters

config-id (required)
Path Parameter
— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `UpdateStatusRequestDto` (optional)
Body Parameter

Return type

`AutomaticSafeRecordSuccessResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    }, {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
    } ]
  }
}
```

```

    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
    "assetDtoList" : [ {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    }, {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
        "appliedOnEntity" : {
            "assetIds" : [ 2, 2 ]
        },
        "accountId" : 5,
        "assetDtoList" : [ null, null ],
        "subConfigurations" : [ null, null ],
        "isDeleted" : true,
        "isEnabled" : true,
        "configurationName" : "configurationName",
        "description" : "description",
        "configurationId" : 5,
        "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
        "isActive" : true,
    } ]
}

```

```

    "configurationValue" : "configurationValue"
}, {
  "appliedOnEntity" : {
    "assetIds" : [ 2, 2 ]
  },
  "accountId" : 5,
  "assetDtoList" : [ null, null ],
  "subConfigurations" : [ null, null ],
  "isDeleted" : true,
  "isEnabled" : true,
  "configurationName" : "configurationName",
  "description" : "description",
  "configurationId" : 5,
  "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
  "isActive" : true,
  "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
  "tsigKeys" : [ {
    "name" : "name",
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "type" : "MD5",
    "value" : "value"
  } ],
  "port" : 7,
  "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
  "type" : "AXFR",
  "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AutomaticSafeRecordSuccessResponse

500Internal server error [ApiErrorResponse](#)

```
get /v3/account-configuration/automatic-safe-record
```

Retrieve all automatic safe record configuration for the account (getAutomaticSafeRecord)
 Retrieve details ok all account automatic safe record configuration

Return type[AutomaticSafeRecordSuccessResponse](#)**Example data**

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    }, {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
    }
  ]
}
```

```

    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
    "assetDtoList" : [ {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    }, {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
        "appliedOnEntity" : {
            "assetIds" : [ 2, 2 ]
        },
        "accountId" : 5,
        "assetDtoList" : [ null, null ],
        "subConfigurations" : [ null, null ],
        "isDeleted" : true,
        "isEnabled" : true,
        "configurationName" : "configurationName",
        "description" : "description",
        "configurationId" : 5,
        "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    } ]
}

```

```

    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AutomaticSafeRecordSuccessResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
get /v3/account-configuration/automatic-safe-record/domain-sync-details/{domain-id}
```

Retrieve all automatic safe record configuration for the domain (getAutomaticSafeRecordByDomain)
Retrieve details ok all account automatic safe record configuration

Path parameters

domain-id (required)
Path Parameter
— format: int64

Return type

[AutomaticSafeRecordSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "syncStatus" : "PENDING"
    } ]
  } ]
```

```

    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
    "assetDtoList" : [ {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "SUCCESS",
        "statusMessage" : "statusMessage"
    }, {
        "name" : "name",
        "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
        "id" : 1,
        "syncStatus" : "PENDING"
    } ]
}

```

```

    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
} ],
"subConfigurations" : [ {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
} ],
"syncDetailsDto" : {
    "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
} ]

```

```
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AutomaticSafeRecordSuccessResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
put /v3/account-configuration/automatic-safe-record/{config-id}
```

Update automatic safe record configuration (updateAutomaticSafeRecord)
Update automatic safe record configuration

Path parameters

config-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body [AutomaticSafeRecordRequestDto](#) (optional)

Body Parameter

Return type

[AutomaticSafeRecordSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "assetDtoList" : [ {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    }, {
      "name" : "name",
      "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
      "id" : 1,
      "syncStatus" : "SUCCESS",
      "statusMessage" : "statusMessage"
    } ],
    "subConfigurations" : [ {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    }, {
      "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
      },
      "accountId" : 5,
      "assetDtoList" : [ null, null ],
      "subConfigurations" : [ null, null ],
      "isDeleted" : true,
      "isEnabled" : true,
      "configurationName" : "configurationName",
      "description" : "description",
      "configurationId" : 5,
      "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
      "isActive" : true,
      "configurationValue" : "configurationValue"
    } ],
    "syncDetailsDto" : {
      "tsigKeys" : [ {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
      }, {
        "name" : "name",
        "type" : "MD5",
        "value" : "value"
      } ]
    }
  }
}
```

```

        "value" : "value"
    } ],
    "port" : 7,
    "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
    "type" : "AXFR",
    "isTsigEnabled" : true
},
"configurationName" : "configurationName",
"description" : "description",
"isActive" : true,
"accountId" : 0,
"isDeleted" : true,
"isEnabled" : true,
"configurationId" : 6,
"configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
"configurationValue" : "configurationValue"
}, {
"assetDtoList" : [ {
    "name" : "name",
    "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
    "id" : 1,
    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
}, {
    "name" : "name",
    "lastSyncDate" : "2000-01-23T04:56:07.000+00:00",
    "id" : 1,
    "syncStatus" : "SUCCESS",
    "statusMessage" : "statusMessage"
} ],
"subConfigurations" : [ {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}, {
    "appliedOnEntity" : {
        "assetIds" : [ 2, 2 ]
    },
    "accountId" : 5,
    "assetDtoList" : [ null, null ],
    "subConfigurations" : [ null, null ],
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationName" : "configurationName",
    "description" : "description",
    "configurationId" : 5,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "isActive" : true,
    "configurationValue" : "configurationValue"
}
]
}

```

```

        "configurationValue" : "configurationValue"
    } ],
    "syncDetailsDto" : {
        "tsigKeys" : [ {
            "name" : "name",
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "type" : "MD5",
            "value" : "value"
        } ],
        "port" : 7,
        "originServerIpList" : [ "originServerIpList", "originServerIpList" ],
        "type" : "AXFR",
        "isTsigEnabled" : true
    },
    "configurationName" : "configurationName",
    "description" : "description",
    "isActive" : true,
    "accountId" : 0,
    "isDeleted" : true,
    "isEnabled" : true,
    "configurationId" : 6,
    "configurationType" : "SIEM_DNS_PROTECTION_EVENTS",
    "configurationValue" : "configurationValue"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK AutomaticSafeRecordSuccessResponse

500

Internal server error ApiErrorResponse

Attacks

```
get /attack/{attackId}
```

Retrieve domain attack (getAttack)
Retrieves details of a specific domain attack

Path parameters

attackId (required)
 Path Parameter
 — The attack ID format: int64

Return type

SimpleDomainAttacksResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SimpleDomainAttacksResponse

400

Failed to find attack with ID {attackId}

500

Internal server error

```
get /attack
```

Retrieve the list of domain attacks (getDomainAttacks)
 Retrieves the list of domain attacks

Query parameters

domainIds (optional)

Query Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
 You can also retrieve it using the GET HTTP method

from (optional)

Query Parameter

— Start date time of the attacks (epoch time) in milliseconds format: int64

limit (optional)

Query Parameter

— Attacks rows number on each page format: int64

page (optional)

Query Parameter

— Page number format: int64

to (optional)

Query Parameter

— End date time of the attacks (epoch time) in milliseconds format: int64

types (optional)

Query Parameter

— Attack types

Return type

GetDomainAttacksResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  }, {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
  }
}
```

```

    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [GetDomainAttacksResponse](#)

400

Failed to get domain attacks.Domain {domainId} not found!

500

Internal server error

AttacksV3

```
get /v3/domains/attacks/{attack-id}
```

Retrieve specific domain attack (getAttackById)
Retrieves details of a specific domain attack

Path parameters

attack-id (required)

Path Parameter

— The attack ID format: int64

Return type

[DomainAttackResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  }, {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DomainAttackResponse](#)

400

Failed to find attack with ID {attackId} [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
get /v3/domains/attacks
```

Retrieve the list of domain attacks (getDomainAttacksByParams)
 Retrieves the list of domain attacks

Query parameters

domainIds (optional)

Query Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
 You can also retrieve it using the GET HTTP method

from (optional)

Query Parameter

— Start date time of the attacks (epoch time) in milliseconds format: int64

limit (optional)

Query Parameter

— Number of attack rows per page format: int64

page (optional)

Query Parameter

— Page number format: int64

to (optional)

Query Parameter

— End date time of the attacks (epoch time) in milliseconds format: int64

types (optional)

Query Parameter

— Attack types

Return type

DomainAttackResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  }, {
    "queriesPerSecondPeak" : 100.0,
    "endedAt" : 1608581355000,
    "detectedBy" : 1000,
    "domainName" : "www.example.com",
    "startedAt" : 1608566594000,
    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  } ]
}
```

```

    "queriesPerSecondAvg" : 100.0,
    "ddosThreshold" : 100,
    "initialRps" : 100,
    "id" : 100,
    "type" : "DDOS",
    "domainId" : 100
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DomainAttackResponse](#)

400

Failed to get domain attacks.Domain {domainId} not found! [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

DNSSIEMLogConfigurationV3

```
get /v3/account-configuration/siem-logs
```

Retrieve SIEM info (getSiemInfo)
Retrieve SIEM info for the given account

Return type

[AccountSiemInfoSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 6,
```

```

    "appliedOnAllAssets" : true,
    "isEnabled" : true,
    "assetIds" : [ 0, 0 ],
    "configurationId" : 1,
    "region" : "US",
    "datasetType" : "DNS_Protection_Events"
} , {
    "accountId" : 6,
    "appliedOnAllAssets" : true,
    "isEnabled" : true,
    "assetIds" : [ 0, 0 ],
    "configurationId" : 1,
    "region" : "US",
    "datasetType" : "DNS_Protection_Events"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AccountSiemInfoSuccessResponse](#)

400

Failed to get siem info for account not found! [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
patch /v3/account-configuration/siem-logs
```

Update SIEM info (updateSiemInfo)
Update SIEM info for the given account

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body `SiemConfigurationRequest` (optional)
 Body Parameter

Return type

`AccountSiemInfoSuccessResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 6,
    "appliedOnAllAssets" : true,
    "isEnabled" : true,
    "assetIds" : [ 0, 0 ],
    "configurationId" : 1,
    "region" : "US",
    "datasetType" : "DNS_Protection_Events"
  }, {
    "accountId" : 6,
    "appliedOnAllAssets" : true,
    "isEnabled" : true,
    "assetIds" : [ 0, 0 ],
    "configurationId" : 1,
    "region" : "US",
    "datasetType" : "DNS_Protection_Events"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

OK `AccountSiemInfoSuccessResponse`

400

Failed to update siem info for account not found! `ApiErrorResponse`

500

Internal server error [ApiErrorResponse](#)

Domains

```
post /domain
```

Add new domain (manual configuration) (addDomain)
Add a new domain to Imperva DNS Protection

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DomainAddRequest (optional)
Body Parameter

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
  "blockDomain" : false,
  "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
  "accountId" : 200,
  "configurationStatus" : "DONE",
  "proxyDomain" : {
    "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
    "bypassDomain" : false,
    "outgoingRequestRateLow" : 10,
    "safeSubDomains" : "[a.example.com, b.example.com]",
    "blockRecordTypes" : [
      {
        "type" : "AAAA",
        "value" : "2001:483:3::1"
      }
    ]
  }
}
```

```

        "enabled" : true
    } ,
    {
        "type" : "AAAA",
        "enabled" : true
    } ],
    "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
    "minTtl" : 1,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "defaultTtl" : 3600,
    "ownerEmail" : "admin@example.com",
    "secondaryDomain" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "customSync" : true,
        "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
        "port" : 53,
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "id" : 0,
        "type" : "AXFR"
    },
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DomainResponse

400

Domain {name} already exists

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
post /domain/file
```

Add new managed domain from DNS zone file (BIND format) (addDomainWithFile)

Add a new domain to Imperva DNS Protection. Import data from a DNS zone file in BIND format.

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

domainDetails (required)

Form Parameter

—

zoneFile (required)

Form Parameter

— format: binary

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
```

```

"blockDomain" : false,
"impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
"accountId" : 200,
"configurationStatus" : "DONE",
"proxyDomain" : {
  "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
  "bypassDomain" : false,
  "outgoingRequestRateLow" : 10,
  "safeSubDomains" : "[a.example.com, b.example.com]",
  "blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
  }, {
    "type" : "AAAA",
    "enabled" : true
  } ],
  "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
  "minTtl" : 1,
  "registrarDetails" : {
    "registrarUrl" : "http://www.godaddy.com",
    "registrar" : "GoDaddy.com, LLC"
  },
  "defaultTtl" : 3600,
  "ownerEmail" : "admin@example.com",
  "secondaryDomain" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "customSync" : true,
    "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
    "port" : 53,
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "id" : 0,
    "type" : "AXFR"
  },
  "tsigDetails" : {
    "tsigKeys" : [ {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    }, {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    } ],
    "isEnabled" : true
  }
},
"id" : 100,

```

```

    "statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DomainResponse

400

Failed to parse DNS zone file! File is missing or empty. Please make sure file is specified under 'zoneFile' form parameters

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
post /domain/{domainId}
```

Edit domain - full update (manual configuration) (editDomainFullUpdate)
Overwrite details of an existing domain (full update)

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body DomainEditRequest (optional)

Body Parameter

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
  "blockDomain" : false,
  "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
  "accountId" : 200,
  "configurationStatus" : "DONE",
  "proxyDomain" : {
    "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
    "bypassDomain" : false,
    "outgoingRequestRateLow" : 10,
    "safeSubDomains" : "[a.example.com, b.example.com]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    } ],
    "outgoingRequestRateHigh" : 50
  },
  "name" : "www.example.com",
  "managedDomain" : {
    "minTtl" : 1,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "defaultTtl" : 3600,
    "ownerEmail" : "admin@example.com",
    "secondaryDomain" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "customSync" : true,
      "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
      "port" : 53,
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "id" : 0,
      "type" : "AXFR"
    }
  }
}
```

```

},
"tsigDetails" : {
  "tsigKeys" : [ {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  } ],
  "isEnabled" : true
}
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DomainResponse

400

Domain {domainId} not found!

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
post /domain/{domainId}/file
```

Edit managed domain - full update from DNS zone file (BIND format) (editDomainFullUpdateWithFile)
Overwrite details of an existing domain (full update)

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.

You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

domainDetails (required)

Form Parameter

— zoneFile (required)

Form Parameter

— format: binary

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
    "lastStatusDate" : 1608754155000,
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "type" : "MANAGED",
    "creationDate" : 1608581355000,
    "blockDomain" : false,
    "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
    "accountId" : 200,
    "configurationStatus" : "DONE",
    "proxyDomain" : {
        "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
        "bypassDomain" : false,
        "outgoingRequestRateLow" : 10,
        "safeSubDomains" : "[a.example.com, b.example.com]",
        "blockRecordTypes" : [ {
            "type" : "AAAA",
            "enabled" : true
        }, {
            "type" : "AAAA",
            "enabled" : true
        } ],
        "outgoingRequestRateHigh" : 50
    },
    "name" : "www.example.com",
    "managedDomain" : {

```

```

    "minTtl" : 1,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "defaultTtl" : 3600,
    "ownerEmail" : "admin@example.com",
    "secondaryDomain" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "customSync" : true,
        "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
        "port" : 53,
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "id" : 0,
        "type" : "AXFR"
    },
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

[OK DomainResponse](#)

400

Domain {domainId} not found!

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
put /domain/{domainId}
```

Edit domain - partial update (editDomainPartialUpdate)
Overwrite specified domain properties (partial update)

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [DomainEditRequest](#) (optional)

Body Parameter

Return type

[DomainResponse](#)

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
  "blockDomain" : false,
  "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]"
}
```

```

"accountId" : 200,
"configurationStatus" : "DONE",
"proxyDomain" : {
  "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
  "bypassDomain" : false,
  "outgoingRequestRateLow" : 10,
  "safeSubDomains" : "[a.example.com, b.example.com]",
  "blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
  }, {
    "type" : "AAAA",
    "enabled" : true
  } ],
  "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
  "minTtl" : 1,
  "registrarDetails" : {
    "registrarUrl" : "http://www.godaddy.com",
    "registrar" : "GoDaddy.com, LLC"
  },
  "defaultTtl" : 3600,
  "ownerEmail" : "admin@example.com",
  "secondaryDomain" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "customSync" : true,
    "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
    "port" : 53,
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "id" : 0,
    "type" : "AXFR"
  },
  "tsigDetails" : {
    "tsigKeys" : [ {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    }, {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    } ],
    "isEnabled" : true
  }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DomainResponse](#)

400

Error -> Domain {domainId} not found!

500

Error -> An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
get /domain
```

Retrieve details of all domains (getAllDomains)

Retrieve details of all protected domains for a given account

Return type

[GetDomainsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "lastStatusDate" : 1608754155000,
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "type" : "MANAGED",
    "creationDate" : 1608581355000,
    "blockDomain" : false,
    "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
    "accountId" : 200,
    "configurationStatus" : "DONE",
    "proxyDomain" : {
      "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudn"
    }
  }
]
```

```
s.net.]",
  "bypassDomain" : false,
  "outgoingRequestRateLow" : 10,
  "safeSubDomains" : "[a.example.com, b.example.com]",
  "blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
  }, {
    "type" : "AAAA",
    "enabled" : true
  } ],
  "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
  "minTtl" : 1,
  "registrarDetails" : {
    "registrarUrl" : "http://www.godaddy.com",
    "registrar" : "GoDaddy.com, LLC"
  },
  "defaultTtl" : 3600,
  "ownerEmail" : "admin@example.com",
  "secondaryDomain" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "customSync" : true,
    "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
    "port" : 53,
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "id" : 0,
    "type" : "AXFR"
  },
  "tsigDetails" : {
    "tsigKeys" : [ {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    }, {
      "name" : "name",
      "id" : 6,
      "type" : "MD5",
      "value" : "value"
    } ],
    "isEnabled" : true
  }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}, {
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
}
```

```

    "creationDate" : 1608581355000,
    "blockDomain" : false,
    "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
    "accountId" : 200,
    "configurationStatus" : "DONE",
    "proxyDomain" : {
      "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
      "bypassDomain" : false,
      "outgoingRequestRateLow" : 10,
      "safeSubDomains" : "[a.example.com, b.example.com]",
      "blockRecordTypes" : [ {
        "type" : "AAAA",
        "enabled" : true
      }, {
        "type" : "AAAA",
        "enabled" : true
      } ],
      "outgoingRequestRateHigh" : 50
    },
    "name" : "www.example.com",
    "managedDomain" : {
      "minTtl" : 1,
      "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
      },
      "defaultTtl" : 3600,
      "ownerEmail" : "admin@example.com",
      "secondaryDomain" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "customSync" : true,
        "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
        "port" : 53,
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "id" : 0,
        "type" : "AXFR"
      },
      "tsigDetails" : {
        "tsigKeys" : [ {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        }, {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        } ],
        "isEnabled" : true
      }
    }
  },
}

```

```

    "id" : 100,
    "statusCheckedAt" : 1608754184000
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK GetDomainsResponse

400

Get all domains failed; {accountId}, errorMessage: {}

500

Internal server error

```
get /domain/{domainId}
```

Retrieve domain details (getDomain)
Retrieves details of a specific domain

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

SimpleDomainResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
```

```

"value" : {
    "lastStatusDate" : 1608754155000,
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "type" : "MANAGED",
    "creationDate" : 1608581355000,
    "blockDomain" : false,
    "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
    "accountId" : 200,
    "configurationStatus" : "DONE",
    "proxyDomain" : {
        "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
        "bypassDomain" : false,
        "outgoingRequestRateLow" : 10,
        "safeSubDomains" : "[a.example.com, b.example.com]",
        "blockRecordTypes" : [ {
            "type" : "AAAA",
            "enabled" : true
        }, {
            "type" : "AAAA",
            "enabled" : true
        } ],
        "outgoingRequestRateHigh" : 50
    },
    "name" : "www.example.com",
    "managedDomain" : {
        "minTtl" : 1,
        "registrarDetails" : {
            "registrarUrl" : "http://www.godaddy.com",
            "registrar" : "GoDaddy.com, LLC"
        },
        "defaultTtl" : 3600,
        "ownerEmail" : "admin@example.com",
        "secondaryDomain" : {
            "customSyncIntervalMillis" : 30000,
            "retryIntervalMillis" : 2400,
            "syncInstructions" : "syncInstructions",
            "customSync" : true,
            "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
            "port" : 53,
            "isCustomSync" : false,
            "defaultSyncIntervalMillis" : 120000,
            "lastSyncedAt" : 1608754155000,
            "lastSyncResult" : "SUCCESS",
            "id" : 0,
            "type" : "AXFR"
        },
        "tsigDetails" : {
            "tsigKeys" : [ {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            }, {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            } ]
        }
    }
}

```

```

        "type" : "MD5",
        "value" : "value"
    } ],
    "isEnabled" : true
}
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SimpleDomainResponse

400

Domain {domainId} not found!

500

Internal server error

```
delete /domain/{domainId}
```

Remove domain (removeDomain)

Remove a domain from the DNS Protection service

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

SimpleTextSuccessResponse

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK -> Domain {domainId} has deleted successfully SimpleTextSuccessResponse

400

Domain {domainId} not found!

500

Internal server error

```
post /domain/{domainId}/validate
```

Check domain records (validateDomainRecords)

Check the domain record configuration for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Query parameters

type (required)

Query Parameter

— Type of the record to validate

Return type

RecordValidationResponse

Example data

Content-Type: application/json

```
{
  "recordValidationMap" : {
    "key" : true
  },
  "hasFound" : true,
  "message" : "TXT record was found!"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK RecordValidationResponse

400

Domain: {domainId} in account: {accountId} does not contain relevant records

500

Internal server error

DomainsV3

```
get /v3/domains
```

Retrieve details of all domains (getAllAccountDomains)
Retrieve details of all domains for the given account

Return type

AccountDomainsSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "name" : "www.example.com",
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000
  }, {
    "accountId" : 200,
    "name" : "www.example.com",
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AccountDomainsSuccessResponse](#)

500

Internal server error [ApiErrorResponse](#)

PrimaryManagedDomainDNSRecords

```
post /domain/{domainId}/records
```

Add domain records (addRecords)
Add records for a given domain ID

Path parameters

domainId (required)
Path Parameter
— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ManagedDomainRecordRequest](#) (optional)
Body Parameter

Return type

[ManagedDomainRecordResponse](#)

Example data

Content-Type: application/json

```
{
  "unsupportedDnsRecords" : [ null, null ],
  "dnsRecords" : [ {
    "data" : "[\"1.2.3.4\"]",
    "name" : "www.example.com",
    "comment" : "Example comment",
    "id" : 1000,
    "type" : "A",
    "ttl" : 1,
    "classType" : "IN"
  }, {
    "data" : "[\"1.2.3.4\"]",
    "name" : "www.example.com",
    "comment" : "Example comment",
    "id" : 1000,
    "type" : "A",
    "ttl" : 1,
    "classType" : "IN"
  } ]
}
```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ManagedDomainRecordResponse

400

Duplicated record: {name}, Record must be unique within the domain.

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
delete /domain/{domainId}/records
```

Delete domain records (deleteRecords)
Delete records for a given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Query parameters

record-ids (optional)

Query Parameter

— format: int64

Return type

ManagedDomainRecordResponse

Example data

Content-Type: application/json

```
{
  "unsupportedDnsRecords" : [ null, null ],
  "dnsRecords" : [ {
    "data" : "[\"1.2.3.4\"]",
    "name" : "www.example.com",
    "comment" : "Example comment",
    "id" : 1000,
    "type" : "A",
    "ttl" : 1,
    "classType" : "IN"
  }, {
    "data" : "[\"1.2.3.4\"]",
    "name" : "www.example.com",
    "comment" : "Example comment",
    "id" : 1000,
    "type" : "A",
    "ttl" : 1,
    "classType" : "IN"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ManagedDomainRecordResponse

400

Record: {id} does not exists under domain: {id} .

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
put /domain/{domainId}/records
```

Edit domain records (editRecords)
Edit records for a given domain ID

Path parameters

domainId (required)
Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ManagedDomainRecordRequest (optional)
Body Parameter

Return type

ManagedDomainRecordResponse

Example data

Content-Type: application/json

```
{  
    "unsupportedDnsRecords" : [ null, null ],  
    "dnsRecords" : [ {  
        "data" : "[\"1.2.3.4\"]",  
        "name" : "www.example.com",  
        "comment" : "Example comment",  
        "id" : 1000,  
        "type" : "A",  
        "ttl" : 1,  
        "classType" : "IN"  
    }, {  
        "data" : "[\"1.2.3.4\"]",  
        "name" : "www.example.com",  
        "comment" : "Example comment",  
        "id" : 1000,  
        "type" : "A",  
        "ttl" : 1,  
        "classType" : "IN"  
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [ManagedDomainRecordResponse](#)

400

Duplicated record: {name}, Record must be unique within the domain.

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
get /domain/{domainId}/records
```

Get domain records (getRecords)

Get records for a given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Return type

[ManagedDomainRecordResponse](#)

Example data

Content-Type: application/json

```
{
  "unsupportedDnsRecords" : [ null, null ],
  "dnsRecords" : [
    {
      "data" : "[\"1.2.3.4\"]",
      "name" : "www.example.com",
      "comment" : "Example comment",
      "id" : 1000,
      "type" : "A",
      "ttl" : 1,
      "classType" : "IN"
    },
    {
      "data" : "[\"1.2.3.4\"]",
      "name" : "www.example.com",
      "comment" : "Example comment",
      "id" : 1000,
      "type" : "A",
      "ttl" : 1,
      "classType" : "IN"
    }
  ]
}
```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ManagedDomainRecordResponse

400

Domain: {id} does not exists under account: {id} .

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

PrimaryManagedDomainDNSSEC

```
put /domain/{domainId}/dnssec/abort-cancellation
```

Stop DNSSEC cancellation process (abortCancellation)
Stop the DNSSEC cancellation process for a given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Responses

200

Abort cancellation performed successfully.

400

Abort cancellation was not performed, domain dnssec is not marked for cancellation.

500

Internal server error

```
post /domain/{domainId}/dnssec/check
```

Check DNSSEC status (checkStatus)

Check if the DS record is updated at the registrar.

Path parameters

domainId (required)

Path Parameter

— format: int64

Return type

DnssecResponseApi

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "statusChangedAt" : 1608754155000,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "domainName" : "example.com",
    "lastSyncedAt" : 1608754155000,
    "dsRecord" : {
      "createdAt" : 0,
      "keyTag" : "IN",
      "digestType" : "www.example.com",
      "digest" : "1",
      "flags" : "267",
      "publicKey" : "A",
      "algorithm" : "1"
    },
    "domainId" : 100,
    "isRegistrarSynced" : false,
    "status" : "ENABLED"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DnssecResponseApi](#)

400

Domain is not allowed

500

Internal server error

```
delete /domain/{domainId}/dnssec
```

Disable DNSSEC (disableDnssec)

Disable DNSSEC for given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Return type

[DnssecResponseApi](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "statusChangedAt" : 1608754155000,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "domainName" : "example.com",
    "lastSyncedAt" : 1608754155000,
    "dsRecord" : {
      "createdAt" : 0,
      "keyTag" : "IN",
      "digestType" : "www.example.com",
      "digest" : "1",
      "signature" : "-----BEGIN PGP SIGNED MESSAGE-----\n\n-----END PGP SIGNED MESSAGE-----"
    }
  }
}
```

```

    "flags" : "267",
    "publicKey" : "A",
    "algorithm" : "1"
  },
  "domainId" : 100,
  "isRegistrarSynced" : false,
  "status" : "ENABLED"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DnssecResponseApi](#)

400

Domain is not allowed

500

Internal server error

```
post /domain/{domainId}/dnssec
```

Enable DNSSEC (enabledDnssec)
Enable DNSSEC for a given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Return type

[DnssecResponseApi](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "statusChangedAt" : 1608754155000,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "domainName" : "example.com",
    "lastSyncedAt" : 1608754155000,
    "dsRecord" : {
      "createdAt" : 0,
      "keyTag" : "IN",
      "digestType" : "www.example.com",
      "digest" : "1",
      "flags" : "267",
      "publicKey" : "A",
      "algorithm" : "1"
    },
    "domainId" : 100,
    "isRegistrarSynced" : false,
    "status" : "ENABLED"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DnssecResponseApi](#)

400

Domain is not allowed

500

Internal server error

```
get /domain/{domainId}/dnssec
```

Get DNSSEC details (getDnssecDetails)
Get DNSSEC details for a given domain ID

Path parameters

domainId (required)

Path Parameter

— format: int64

Return type

[DnssecResponseApi](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "statusChangedAt" : 1608754155000,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "domainName" : "example.com",
    "lastSyncedAt" : 1608754155000,
    "dsRecord" : {
      "createdAt" : 0,
      "keyTag" : "IN",
      "digestType" : "www.example.com",
      "digest" : "1",
      "flags" : "267",
      "publicKey" : "A",
      "algorithm" : "1"
    },
    "domainId" : 100,
    "isRegistrarSynced" : false,
    "status" : "ENABLED"
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- [application/json](#)

Responses

200

[OK DnssecResponseApi](#)

PrimaryManagedDomainV3

```
post /v3/domains/primary
```

Add new primary domain (addPrimaryDomain)
Add a new primary domain to Imperva DNS Protection

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body PrimaryDomainRequest (optional)
Body Parameter

Return type

PrimaryDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : [
      {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a1.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
      }
    ],
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
  }, {
```

```

    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

OK PrimaryDomainSuccessResponse

400

Domain {name} already exists ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. ApiErrorResponse

```
post /v3/domains/primary/file
```

Add new managed domain from DNS zone file (BIND format) (addPrimaryDomainWithFile)
Add a new domain to Imperva DNS Protection. Import data from a DNS zone file in BIND format.

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

domainDetails (required)

Form Parameter

— zoneFile (required)

Form Parameter

— format: binary

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
  "blockDomain" : false,
  "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
  "accountId" : 200,
  "configurationStatus" : "DONE",
  "proxyDomain" : {
    "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
    "bypassDomain" : false,
    "outgoingRequestRateLow" : 10,
    "safeSubDomains" : "[a.example.com, b.example.com]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    } ],
    "outgoingRequestRateHigh" : 50
  },
  "name" : "www.example.com",
  "managedDomain" : {
    "minTtl" : 1,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrarName" : "GoDaddy"
    }
  }
}
```

```

    "registrar" : "GoDaddy.com, LLC"
},
"defaultTtl" : 3600,
"ownerEmail" : "admin@example.com",
"secondaryDomain" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "customSync" : true,
    "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
    "port" : 53,
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "id" : 0,
    "type" : "AXFR"
},
"tsigDetails" : {
    "tsigKeys" : [ {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
    }, {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
    } ],
    "isEnabled" : true
}
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

OK DomainResponse

400

Failed to parse DNS zone file! File is missing or empty. Please make sure file is specified under 'zoneFile' form parameters **ApiErrorResponse**

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
delete /v3/domains/primary/{domain-id}
```

Delete primary domain (deletePrimaryDomain)
Delete primary domain by given {domain-id}

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[PrimaryDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
  }, {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    }
  }
]
```

```
        },
        "name" : "www.example.com",
        "defaultTtl" : 3600,
        "ddosThreshold" : 40,
        "id" : 100,
        "lastSavedAt" : 1608754155000,
        "configurationStatusDetails" : {
            "lastStatusDate" : 1608754155000,
            "configurationStatus" : "DONE",
            "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
            "statusCheckedAt" : 1608754184000,
            "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
        },
        "type" : "Primary",
        "creationDate" : 1608581355000,
        "ownerEmail" : "admin@example.com"
    } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK PrimaryDomainSuccessResponse

400

Invalid input `ApiErrorResponse`

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
put /v3/domains/primary/{domain-id}/file
```

Edit managed domain - full update from DNS zone file (BIND format) (editPrimaryDomainFullUpdateWithFile) Overwrite details of an existing domain (full update)

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Form parameters

domainDetails (required)

Form Parameter

— zoneFile (required)

Form Parameter

— format: binary

Return type

DomainResponse

Example data

Content-Type: application/json

```
{
  "lastStatusDate" : 1608754155000,
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "type" : "MANAGED",
  "creationDate" : 1608581355000,
  "blockDomain" : false,
  "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
  "accountId" : 200,
  "configurationStatus" : "DONE",
  "proxyDomain" : {
    "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
    "bypassDomain" : false,
    "outgoingRequestRateLow" : 10,
    "safeSubDomains" : "[a.example.com, b.example.com]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    }
  }
}
```

```

    } ],
    "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
    "minTtl" : 1,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "defaultTtl" : 3600,
    "ownerEmail" : "admin@example.com",
    "secondaryDomain" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "customSync" : true,
        "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
        "port" : 53,
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "id" : 0,
        "type" : "AXFR"
    },
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [DomainResponse](#)

400

Domain {domain-id} not found! [ApiErrorResponse](#)

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
get /v3/domains/primary/file/export-all-zones
```

Export list of primary DNS zones (exportAllZoneFileInZipFormat)

Exports a zip file containing a zone file for each DNS zone, and subfolders for each subaccount containing their respective zone files.

Query parameters

includeSubAccounts (optional)

Query Parameter

— Include Sub Accounts Zones or not

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/zip

Responses

200

OK

400

Zero managed domains found [ApiErrorResponse](#)

500

An internal error occurred. Please contact support specifying your account ID. [ApiErrorResponse](#)

```
put /v3/domains/primary/{domain-id}
```

Fully update primary domain (fullEditPrimaryDomain)
 Fully update primary domain, Overwrite details of an existing domain

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body PrimaryDomainRequest (optional)

Body Parameter

Return type

PrimaryDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    }
  }
}
```

```

    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
} , {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK PrimaryDomainSuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
get /v3/domains/primary
```

Retrieve all primary domain details (getAllPrimaryDomains)
Retrieve details of all primary domains for a given account

Return type

[PrimaryDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
  }, {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    }
  }
]
```

```

    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Primary",
  "creationDate" : 1608581355000,
  "ownerEmail" : "admin@example.com"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [PrimaryDomainSuccessResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
get /v3/domains/primary/{domain-id}
```

Retrieve primary domain details (getPrimaryDomain)
Retrieves details of a specific primary domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[PrimaryDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
  }, {
    "minTtl" : 1,
    "accountId" : 200,
    "registrarDetails" : {
      "registrarUrl" : "http://www.godaddy.com",
      "registrar" : "GoDaddy.com, LLC"
    },
    "name" : "www.example.com",
    "defaultTtl" : 3600,
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Primary",
    "creationDate" : 1608581355000,
    "ownerEmail" : "admin@example.com"
  } ]
}
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [PrimaryDomainSuccessResponse](#)

404

Domain {domain-id} not found! [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
patch /v3/domains/primary/{domain-id}
```

Partially update primary domain (partialEditPrimaryDomain)

Overwrites specific details of an existing domain. Fields that are not specified will remain the same.

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [PrimaryDomainRequest](#) (optional)

Body Parameter

Return type

[PrimaryDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "minTtl" : 1,
```

```

"accountId" : 200,
"registrarDetails" : {
  "registrarUrl" : "http://www.godaddy.com",
  "registrar" : "GoDaddy.com, LLC"
},
"name" : "www.example.com",
"defaultTtl" : 3600,
"ddosThreshold" : 40,
"id" : 100,
"lastSavedAt" : 1608754155000,
"configurationStatusDetails" : {
  "lastStatusDate" : 1608754155000,
  "configurationStatus" : "DONE",
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "statusCheckedAt" : 1608754184000,
  "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Primary",
"creationDate" : 1608581355000,
"ownerEmail" : "admin@example.com"
}, {
  "minTtl" : 1,
  "accountId" : 200,
  "registrarDetails" : {
    "registrarUrl" : "http://www.godaddy.com",
    "registrar" : "GoDaddy.com, LLC"
  },
  "name" : "www.example.com",
  "defaultTtl" : 3600,
  "ddosThreshold" : 40,
  "id" : 100,
  "lastSavedAt" : 1608754155000,
  "configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Primary",
  "creationDate" : 1608581355000,
  "ownerEmail" : "admin@example.com"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [PrimaryDomainSuccessResponse](#)

400

Invalid input [ApiErrorResponse](#)

404

Domain id not found [ApiErrorResponse](#)

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

ProtectedDomainV3

```
post /v3/domains/protected
```

Add new protected domain (addProtectedDomain)
Add a new protected domain to Imperva DNS Protection

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ProtectedDomainRequest](#) (optional)
Body Parameter

Return type

[ProtectedDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
  "data" : [ {
```

```

"adaptiveThreshold" : { },
"originalNSRecords" : "["ns101.cloudns.net.", "ns102.cloudns.net.", "ns103.cloudns.net."]",
"ddosThreshold" : 40,
"lastSavedAt" : 1608754155000,
"configurationStatusDetails" : {
  "lastStatusDate" : 1608754155000,
  "configurationStatus" : "DONE",
  "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
  "statusCheckedAt" : 1608754184000,
  "impervaNsRecords" : "["ns1.a0.impervasecuredns.net", "ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]"
},
"type" : "Protected",
"creationDate" : 1608581355000,
"safeSubDomains" : "[\"www\", \"http\", \"static\"]",
"blockRecordTypes" : [ {
  "type" : "AAAA",
  "enabled" : true
}, {
  "type" : "AAAA",
  "enabled" : true
} ],
"protectedSafeSubDomainList" : [ {
  "recordName" : "www",
  "recordTypes" : "A, TXT, CNAME"
}, {
  "recordName" : "www",
  "recordTypes" : "A, TXT, CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
}, {
  "adaptiveThreshold" : { },
  "originalNSRecords" : "["ns101.cloudns.net.", "ns102.cloudns.net.", "ns103.cloudns.net."]",
  "ddosThreshold" : 40,
  "lastSavedAt" : 1608754155000,
  "configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "["ns1.a0.impervasecuredns.net", "ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]"
},
  "type" : "Protected",
  "creationDate" : 1608581355000,
  "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
  "blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
  }, {
    "type" : "AAAA",
    "enabled" : true
  } ]
}

```

```

} ],
"protectedSafeSubDomainList" : [ {
  "recordName" : "www",
  "recordTypes" : "A,TXT,CNAME"
}, {
  "recordName" : "www",
  "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

OK ProtectedDomainSuccessResponse

400

Domain {name} already exists ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
delete /v3/domains/protected/{domain-id}
```

Delete protected domain (deleteProtectedDomain)

Delete protected domain by given {domain-id}

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

ProtectedDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    } ],
    "protectedSafeSubDomainList" : [ {
      "recordName" : "www",
      "recordTypes" : "A, TXT, CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A, TXT, CNAME"
    } ],
    "accountId" : 200,
    "name" : "www.example.com",
    "outgoingRequestRateLow" : 10,
    "id" : 100,
    "isAdaptiveThresholdEnabled" : true,
    "outgoingRequestRateHigh" : 50
  }, {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    }
  }
]
```

```

    "impervaNsRecords" : ["ns1.a0.impervasecuredns.net", "ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]
  },
  "type" : "Protected",
  "creationDate" : 1608581355000,
  "safeSubDomains" : ["www", "http", "static"],
  "blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
  }, {
    "type" : "AAAA",
    "enabled" : true
  } ],
  "protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  }, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  } ],
  "accountId" : 200,
  "name" : "www.example.com",
  "outgoingRequestRateLow" : 10,
  "id" : 100,
  "isAdaptiveThresholdEnabled" : true,
  "outgoingRequestRateHigh" : 50
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
put /v3/domains/protected/{domain-id}
```

Fully update protected domain (fullEditProtectedDomain)

Fully update protected domain, Overwrite details of an existing domain

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body ProtectedDomainRequest (optional)

Body Parameter

Return type

ProtectedDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
  }]
```

```

"creationDate" : 1608581355000,
"safeSubDomains" : ["www", "http", "static"]),
"blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
}, {
    "type" : "AAAA",
    "enabled" : true
} ],
"protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
}, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
}, {
    "adaptiveThreshold" : { },
    "originalNSRecords" : ["ns101.cloudns.net.", "ns102.cloudns.net.", "ns103.cloudns.net."],
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : ["ns1.a0.impervasecuredns.net", "ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : ["www", "http", "static"]),
    "blockRecordTypes" : [ {
        "type" : "AAAA",
        "enabled" : true
}, {
        "type" : "AAAA",
        "enabled" : true
} ],
"protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
}, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
}

```

```
    } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. ApiErrorResponse

```
get /v3/domains/protected
```

Retrieve all protected domain details (getAllProtectedDomains)
Retrieve details of all protected domains for a given account

Return type

ProtectedDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
```

```

"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Protected",
"creationDate" : 1608581355000,
"safeSubDomains" : "[\"www\", \"http\", \"static\"]",
"blockRecordTypes" : [ {
    "type" : "AAAA",
    "enabled" : true
}, {
    "type" : "AAAA",
    "enabled" : true
} ],
"protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
}, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
}, {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\",\"ns102.cloudns.net.\",\"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
        "type" : "AAAA",
        "enabled" : true
    }, {
        "type" : "AAAA",
        "enabled" : true
    } ],
    "protectedSafeSubDomainList" : [ {
        "recordName" : "www",
        "recordTypes" : "A,TXT,CNAME"
    }, {

```

```

    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  } ],
  "accountId" : 200,
  "name" : "www.example.com",
  "outgoingRequestRateLow" : 10,
  "id" : 100,
  "isAdaptiveThresholdEnabled" : true,
  "outgoingRequestRateHigh" : 50
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSuccessResponse

500

Internal server error ApiErrorResponse

```
get /v3/domains/protected/{domain-id}
```

Retrieve protected domain details (getProtectedDomain)
Retrieves details of a specific protected domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

ProtectedDomainSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    } ],
    "protectedSafeSubDomainList" : [ {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    } ],
    "accountId" : 200,
    "name" : "www.example.com",
    "outgoingRequestRateLow" : 10,
    "id" : 100,
    "isAdaptiveThresholdEnabled" : true,
    "outgoingRequestRateHigh" : 50
  }, {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    } ]
  }
}
```

```

    "type" : "AAAA",
    "enabled" : true
} ],
"protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
}, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [ProtectedDomainSuccessResponse](#)

404

Domain {domain-id} not found! [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
get /v3/domains/protected/{domain-id}/safe-records
```

Retrieve protected domain safe record details (getProtectedDomainSafeRecords)
Retrieves safe records details of a specific protected domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

ProtectedDomainSafeRecordsSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]"
  }, {
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSafeRecordsSuccessResponse

404

Domain {domain-id} not found! ApiErrorResponse

500

Internal server error ApiErrorResponse

```
get /v3/domains/protected/{domain-id}/safe-records/type
```

Retrieve protected domain safe record details (getProtectedDomainSafeRecordsType)
Retrieves safe records details of a specific protected domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

ProtectedDomainSafeRecordsTypeSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "safeSubDomains" : [ {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    } ]
  }, {
    "safeSubDomains" : [ {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    } ]
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSafeRecordsTypeSuccessResponse

404

Domain {domain-id} not found! ApiErrorResponse

500

Internal server error ApiErrorResponse

```
patch /v3/domains/protected/{domain-id}
```

Partially update protected domain (partialEditProtectedDomain)

Overwrites specific details of an existing domain. Fields that are not specified will remain the same.

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body [ProtectedDomainRequest](#) (optional)

Body Parameter

Return type

[ProtectedDomainSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\", \"ns102.cloudns.net.\", \"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
      "lastStatusDate" : 1608754155000,
      "configurationStatus" : "DONE",
      "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
      "statusCheckedAt" : 1608754184000,
      "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
      "type" : "AAAA",
      "enabled" : true
    }, {
      "type" : "AAAA",
      "enabled" : true
    } ],
  }
}
```

```

"protectedSafeSubDomainList" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
}, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
} ],
"accountId" : 200,
"name" : "www.example.com",
"outgoingRequestRateLow" : 10,
"id" : 100,
"isAdaptiveThresholdEnabled" : true,
"outgoingRequestRateHigh" : 50
}, {
    "adaptiveThreshold" : { },
    "originalNSRecords" : "[\"ns101.cloudns.net.\",\"ns102.cloudns.net.\",\"ns103.cloudns.net.\"]",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Protected",
    "creationDate" : 1608581355000,
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]",
    "blockRecordTypes" : [ {
        "type" : "AAAA",
        "enabled" : true
    }, {
        "type" : "AAAA",
        "enabled" : true
    } ],
    "protectedSafeSubDomainList" : [ {
        "recordName" : "www",
        "recordTypes" : "A,TXT,CNAME"
    }, {
        "recordName" : "www",
        "recordTypes" : "A,TXT,CNAME"
    } ],
    "accountId" : 200,
    "name" : "www.example.com",
    "outgoingRequestRateLow" : 10,
    "id" : 100,
    "isAdaptiveThresholdEnabled" : true,
    "outgoingRequestRateHigh" : 50
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

-
- application/json

Responses

200

OK ProtectedDomainSuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. ApiErrorResponse

```
put /v3/domains/protected/{domain-id}/safe-records
```

Overwrites the protected domain safe record list (full update) (updateProtectedDomainSafeRecords)
This API will overwrite the currently configured list of safe records for a protected domain. **Important:** By default, this operation will add safe records with the 'ALL_TYPES' option for their type, which is not recommended. It is advisable to use the alternative APIs [PUT /{domain-id}/safe-records/type OR /{domain-id}/safe-records/file] that allows specifying safe record names with their respective types for better control and security.

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body ProtectedDomainSafeRecordsRequest (optional)

Body Parameter

Return type

ProtectedDomainSafeRecordsSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]"
  }, {
    "safeSubDomains" : "[\"www\", \"http\", \"static\"]"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSafeRecordsSuccessResponse

404

Domain {domain-id} not found! ApiErrorResponse

500

Internal server error ApiErrorResponse

```
put /v3/domains/protected/{domain-id}/safe-records/file
```

Overwrites the protected domain safe record list (full update) (updateProtectedDomainSafeRecordsByZoneFile)
Upload your zone file to overwrite the currently configured list of safe records for a protected domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- multipart/form-data

Query parameters

fileType (optional)

Query Parameter

— The type of the provided file. It can be either CSV or BIND. If not specified, the default is BIND.

Form parameters

zoneFile (optional)

Form Parameter

— format: binary

Return type

ProtectedDomainSafeRecordsTypeSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "safeSubDomains" : [ {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    } ]
  }, {
    "safeSubDomains" : [ {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    }, {
      "recordName" : "www",
      "recordTypes" : "A,TXT,CNAME"
    } ]
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK `ProtectedDomainSafeRecordsTypeSuccessResponse`

404

Domain `{domain-id}` not found! `ApiErrorResponse`

500

Internal server error `ApiErrorResponse`

```
put /v3/domains/protected/{domain-id}/safe-records/type
```

Overwrites the protected domain safe record list (full update) (`updateProtectedDomainSafeRecordsType`)
Send your safe record list along with record type to overwrite the currently configured list of safe records for a protected domain

Path parameters

`domain-id` (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `ProtectedDomainSafeRecordsTypeRequest` (optional)

Body Parameter

Return type

`ProtectedDomainSafeRecordsTypeSuccessResponse`

Example data

Content-Type: application/json

```
{
```

```

"data" : [ {
  "safeSubDomains" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  }, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  } ]
}, {
  "safeSubDomains" : [ {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  }, {
    "recordName" : "www",
    "recordTypes" : "A,TXT,CNAME"
  } ]
}
]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK ProtectedDomainSafeRecordsTypeSuccessResponse

404

Domain {domain-id} not found! ApiErrorResponse

500

Internal server error ApiErrorResponse

PurgeCache

```
post /domain/{domainId}/purge/all
```

Purge all cached resources (purgeAllDomainResources)
Purge all cached resources for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[SimpleTextSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : "value"
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK -> All resources of domain {domainId} were purged successfully! [SimpleTextSuccessResponse](#)

400

Could not purge domain resource. Domain is not fully configured.

500

Internal server error

```
post /domain/{domainId}/purge
```

Purge specific cached resources (purgeSpecificDomainResource)
Purge a subset of the cached resources for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `PurgeCacheRequest` (optional)

Body Parameter

— purge domain specific resource

Return type

`SimpleTextSuccessResponse`

Example data

Content-Type: application/json

```
{  
    "isError" : false,  
    "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK -> Resource was purged successfully from domain {domainId} `SimpleTextSuccessResponse`

400

Could not purge domain resource. Domain is not fully configured.

500

[Internal server error](#)

PurgeCacheV3

```
post /v3/domains/protected/{domain-id}/purge-cache
```

Purge cached resources (purgeProtectedDomainCache)
 Purge cached resources for a given domain ID

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
 You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body PurgeCacheRequestV3 (optional)

Body Parameter

— purge domain specific resource

Return type

SimpleTextSuccessResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ "data", "data" ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK -> resources of domain {domain-id} were purged successfully! [SimpleTextSuccessResponseV3](#)

400

Could not purge domain resource. Domain is not fully configured. [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

SecondaryDomain

```
get /secondary-domain/allowed-ips
```

Retrieve Imperva IP addresses (getSecondaryServerIp)

To enable Imperva to act as secondary DNS provider and complete the zone transfer process, configure your primary DNS provider to allow access to these Imperva IP addresses.

Return type

[SimpleTextSuccessResponse](#)

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : "value"  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [SimpleTextSuccessResponse](#)

400

Failed to get Secondary server ip

500

Internal server error

```
post /secondary-domain/{domainId}/sync
```

Retrieve the DNS records from the primary provider (sync)

Retrieves and update the secondary domain's DNS record details from your primary DNS provider.

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[SimpleDomainResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "lastStatusDate" : 1608754155000,
    "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
    "ddosThreshold" : 40,
    "lastSavedAt" : 1608754155000,
    "type" : "MANAGED",
    "creationDate" : 1608581355000,
    "blockDomain" : false,
    "impervaNsRecords" : "[ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]",
    "accountId" : 200,
    "configurationStatus" : "DONE",
    "proxyDomain" : {
      "originalNsRecords" : "[ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]",
      "bypassDomain" : false,
      "outgoingRequestRateLow" : 10,
      "safeSubDomains" : "[a.example.com, b.example.com]",
      "blockRecordTypes" : [ {
        "type" : "AAAA",
        "enabled" : true
      }, {
        "type" : "AAAA",
```

```
        "enabled" : true
    } ],
    "outgoingRequestRateHigh" : 50
},
"name" : "www.example.com",
"managedDomain" : {
    "minTtl" : 1,
    "registrarDetails" : {
        "registrarUrl" : "http://www.godaddy.com",
        "registrar" : "GoDaddy.com, LLC"
    },
    "defaultTtl" : 3600,
    "ownerEmail" : "admin@example.com",
    "secondaryDomain" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "customSync" : true,
        "primaryIpAddresses" : "[1.1.1.1,2.2.2.2]",
        "port" : 53,
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "id" : 0,
        "type" : "AXFR"
    },
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"id" : 100,
"statusCheckedAt" : 1608754184000
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SimpleDomainResponse

400

Failed to sync domain {domainId} from primary

500

Internal server error

SecondaryDomainPrimaryIPs

```
post /secondary-domain/{domainId}/primary-ips
```

Add primary IPs (addPrimaryIps)

Add IP addresses of your primary DNS provider to a secondary domain. This enables Imperva to pull your DNS records via zone transfer. You can enter multiple IP addresses or IP ranges in a comma-separated list. A maximum of 256 IP addresses are allowed.

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body PrimaryIpAddressDto (optional)

Body Parameter

—

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

[PrimaryIpsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "id" : 0,
    "value" : "value"
  }, {
    "id" : 0,
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [PrimaryIpsResponse](#)

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
put /secondary-domain/{domainId}/primary-ips
```

Edit primary IPs (`editPrimaryIps`)

Edit an IP address of your primary DNS provider for a secondary domain. You can retrieve the ID of the IP address you want to edit using the GET method.

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- * / *

Request body

body PrimaryIpaddressResponse (optional)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

PrimaryIpsResponse

Example data

Content-Type: application/json

```
{  
  "isError" : false,  
  "value" : [ {  
    "id" : 0,  
    "value" : "value"  
  }, {  
    "id" : 0,  
    "value" : "value"  
  } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [PrimaryIpsResponse](#)

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
get /secondary-domain/{domainId}/primary-ips
```

Get all primary IPs (getAllPrimaryIps)

Retrieves the IP addresses of your primary DNS provider for a given domain ID.

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
You can also retrieve it using the GET HTTP method format: int64

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

[PrimaryIpsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "id" : 0,
    "value" : "value"
  }, {
    "id" : 0,
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK PrimaryIpsResponse

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
delete /secondary-domain/{domainId}/primary-ips
```

Remove primary IPs (removePrimaryIps)

Removes specified primary IPs for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.

You can also retrieve it using the GET HTTP method format: int64

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

ip-ids (optional)

Query Parameter

— format: int64

Return type

PrimaryIpsResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "id" : 0,
    "value" : "value"
  }, {
    "id" : 0,
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK PrimaryIpsResponse

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

SecondaryDomainTSIGKeys

```
post /domain/{domainId}/tsig
```

Add TSIG keys (addTsigKey)

Add TSIG keys for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- `*/*`

Request body

body `TsigKeyDto` (optional)

Body Parameter

Query parameters

`caid` (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

`TsigResponse`

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- `application/json`

Responses

200

OK `TsigResponse`

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
put /domain/{domainId}/tsig
```

Edit TSIG keys (editTsigKey)
Edit TSIG keys for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
You can also retrieve it using the GET HTTP method format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- * / *

Request body

body [TsigKeyDtoResponse](#) (optional)

Body Parameter

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

[TsigResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
```

```

    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
} , {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [TsigResponse](#)

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
get /domain/{domainId}/tsig
```

Get all TSIG keys (getAllTsigKeys)

Get all TSIG keys for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

Return type

TsigResponse

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK TsigResponse

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

```
delete /domain/{domainId}/tsig
```

Remove TSIG keys (removeTsigKeys)
Remove TSIG keys for a given domain ID

Path parameters

domainId (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Query parameters

caid (optional)

Query Parameter

— Your Imperva account id format: int64

key-ids (optional)

Query Parameter

— format: int64

Return type

[TsigResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : [ {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [TsigResponse](#)

400

No domain with given id

500

An internal error occurred. Please contact support specifying your account ID and Domain ID.

SecondaryDomainV3

```
post /v3/domains/secondary
```

Add new secondary domain (addSecondaryDomain)

Add a new secondary domain to Imperva DNS Protection

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body SecondaryDomainRequestV3 (optional)

Body Parameter

Return type

SecondarySuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
  }
]
```

```

    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
        "primaryIpAddresses" : [ {
            "id" : 0,
            "value" : "value"
        }, {
            "id" : 0,
            "value" : "value"
        } ],
        "port" : 53,
        "tsigDetails" : {
            "tsigKeys" : [ {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            }, {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            } ],
            "isEnabled" : true
        }
    },
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
    },
    "type" : "Secondary",
    "creationDate" : 1608581355000
}, {
    "accountId" : 200,
    "secondaryTransferDetails" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
        "primaryIpAddresses" : [ {
            "id" : 0,
            "value" : "value"
        }, {
            "id" : 0,
            "value" : "value"
        } ]
    }
}

```

```

} ],
"port" : 53,
"tsigDetails" : {
  "tsigKeys" : [ {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  }, {
    "name" : "name",
    "id" : 6,
    "type" : "MD5",
    "value" : "value"
  } ],
  "isEnabled" : true
},
"configurationStatusDetails" : {
  "lastStatusDate" : 1608754155000,
  "configurationStatus" : "DONE",
  "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
  "statusCheckedAt" : 1608754184000,
  "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Secondary",
"creationDate" : 1608581355000
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

201

OK SecondarySuccessResponse

400

Domain {name} already exists ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. ApiErrorResponse

```
delete /v3/domains/secondary/{domain-id}
```

Delete secondary domain (deleteSecondaryDomain)
Delete secondary domain by given {domain-id}

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[SecondarySuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
      "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
      }, {
        "id" : 0,
        "value" : "value"
      } ],
      "port" : 53,
      "tsigDetails" : {
        "tsigKeys" : [ {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        }, {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        } ],
        "tsigAlgorithms" : [
          {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
          }
        ]
      }
    }
  } ]
}
```

```

        "isEnabled" : true
    },
},
"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "["ns1.a0.impervasecuredns.net","ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]"
},
{
    "type" : "Secondary",
    "creationDate" : 1608581355000
}, {
    "accountId" : 200,
    "secondaryTransferDetails" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
        "primaryIpAddresses" : [ {
            "id" : 0,
            "value" : "value"
        }, {
            "id" : 0,
            "value" : "value"
        } ],
        "port" : 53,
        "tsigDetails" : {
            "tsigKeys" : [ {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            }, {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            } ],
            "isEnabled" : true
        }
    },
    "configurationStatusDetails" : {
        "lastStatusDate" : 1608754155000,
        "configurationStatus" : "DONE",
        "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
        "statusCheckedAt" : 1608754184000,
        "impervaNsRecords" : "["ns1.a0.impervasecuredns.net","ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]"
    }
}

```

```

    ns.net", "ns1.a2.impervasecuredns.net"]"
    },
    "type" : "Secondary",
    "creationDate" : 1608581355000
  } ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SecondarySuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. ApiErrorResponse

```
put /v3/domains/secondary/{domain-id}
```

Fully update secondary domain (fullEditSecondaryDomain)

Fully update secondary domain, Overwrite details of an existing domain

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SecondaryDomainRequestV3` (optional)
 Body Parameter

Return type

`SecondarySuccessResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
      "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
      }, {
        "id" : 0,
        "value" : "value"
      } ],
      "port" : 53,
      "tsigDetails" : {
        "tsigKeys" : [ {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        }, {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        } ],
        "isEnabled" : true
      }
    },
    "configurationStatusDetails" : {
  
```

```

    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Secondary",
  "creationDate" : 1608581355000
}, {
  "accountId" : 200,
  "secondaryTransferDetails" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "type" : "AXFR"
  },
  "name" : "www.example.com",
  "ddosThreshold" : 40,
  "id" : 100,
  "lastSavedAt" : 1608754155000,
  "primaryDetails" : {
    "primaryIpAddresses" : [ {
      "id" : 0,
      "value" : "value"
    }, {
      "id" : 0,
      "value" : "value"
    } ],
    "port" : 53,
    "tsigDetails" : {
      "tsigKeys" : [ {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
      }, {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
      } ],
      "isEnabled" : true
    }
  },
  "configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Secondary",
  "creationDate" : 1608581355000
}

```

```
    } ]
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [SecondarySuccessResponse](#)

400

Invalid input [ApiErrorResponse](#)

404

Domain id not found [ApiErrorResponse](#)

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

```
get /v3/domains/secondary
```

Retrieve all secondary domain details (getAllSecondaryDomains)
Retrieve details of all secondary domains for a given account

Return type

[SecondarySuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
    }
  }
]
```

```

    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "type" : "AXFR"
},
"name" : "www.example.com",
"ddosThreshold" : 40,
"id" : 100,
"lastSavedAt" : 1608754155000,
"primaryDetails" : {
    "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
    }, {
        "id" : 0,
        "value" : "value"
    } ],
    "port" : 53,
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Secondary",
"creationDate" : 1608581355000
}, {
    "accountId" : 200,
    "secondaryTransferDetails" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "type" : "AXFR"
},
"name" : "www.example.com",
"ddosThreshold" : 40,
"id" : 100,

```

```

"lastSavedAt" : 1608754155000,
"primaryDetails" : {
    "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
    }, {
        "id" : 0,
        "value" : "value"
    } ],
    "port" : 53,
    "tsigDetails" : {
        "tsigKeys" : [ {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        }, {
            "name" : "name",
            "id" : 6,
            "type" : "MD5",
            "value" : "value"
        } ],
        "isEnabled" : true
    }
},
"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Secondary",
"creationDate" : 1608581355000
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SecondarySuccessResponse

500

Internal server error ApiErrorResponse

```
get /v3/domains/secondary/{domain-id}
```

Retrieve secondary domain details (getSecondaryDomain)
Retrieves details of a specific secondary domain

Path parameters

domain-id (required)

Path Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added. You can also retrieve it using the GET HTTP method format: int64

Return type

[SecondarySuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
      "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
      }, {
        "id" : 0,
        "value" : "value"
      } ],
      "port" : 53,
      "tsigDetails" : {
        "tsigKeys" : [ {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        }, {
          "name" : "name",
          "id" : 7,
          "type" : "SHA256"
        } ]
      }
    }
  }
]
```

```

        "id" : 6,
        "type" : "MD5",
        "value" : "value"
    } ],
    "isEnabled" : true
}
},
"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a1.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
},
"type" : "Secondary",
"creationDate" : 1608581355000
}, {
    "accountId" : 200,
    "secondaryTransferDetails" : {
        "customSyncIntervalMillis" : 30000,
        "retryIntervalMillis" : 2400,
        "syncInstructions" : "syncInstructions",
        "isCustomSync" : false,
        "defaultSyncIntervalMillis" : 120000,
        "lastSyncedAt" : 1608754155000,
        "lastSyncResult" : "SUCCESS",
        "type" : "AXFR"
},
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
        "primaryIpAddresses" : [ {
            "id" : 0,
            "value" : "value"
        }, {
            "id" : 0,
            "value" : "value"
        } ],
        "port" : 53,
        "tsigDetails" : {
            "tsigKeys" : [ {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            }, {
                "name" : "name",
                "id" : 6,
                "type" : "MD5",
                "value" : "value"
            } ],
            "isEnabled" : true
        }
},
"configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,

```

```

    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfbd35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\",\"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Secondary",
  "creationDate" : 1608581355000
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [SecondarySuccessResponse](#)

404

Domain {domain-id} not found! [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
patch /v3/domains/secondary/{domain-id}
```

Partially update secondary domain (partialEditSecondaryDomain)

Overwrites specific details of an existing domain. Fields that are not specified will remain the same.

Path parameters

domain-id (required)

Path Parameter

— format: int64

Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json

Request body

body `SecondaryDomainRequestV3` (optional)
 Body Parameter

Return type

`SecondarySuccessResponse`

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 200,
    "secondaryTransferDetails" : {
      "customSyncIntervalMillis" : 30000,
      "retryIntervalMillis" : 2400,
      "syncInstructions" : "syncInstructions",
      "isCustomSync" : false,
      "defaultSyncIntervalMillis" : 120000,
      "lastSyncedAt" : 1608754155000,
      "lastSyncResult" : "SUCCESS",
      "type" : "AXFR"
    },
    "name" : "www.example.com",
    "ddosThreshold" : 40,
    "id" : 100,
    "lastSavedAt" : 1608754155000,
    "primaryDetails" : {
      "primaryIpAddresses" : [ {
        "id" : 0,
        "value" : "value"
      }, {
        "id" : 0,
        "value" : "value"
      } ],
      "port" : 53,
      "tsigDetails" : {
        "tsigKeys" : [ {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        }, {
          "name" : "name",
          "id" : 6,
          "type" : "MD5",
          "value" : "value"
        } ],
        "isEnabled" : true
      }
    },
    "configurationStatusDetails" : {
  
```

```

    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Secondary",
  "creationDate" : 1608581355000
}, {
  "accountId" : 200,
  "secondaryTransferDetails" : {
    "customSyncIntervalMillis" : 30000,
    "retryIntervalMillis" : 2400,
    "syncInstructions" : "syncInstructions",
    "isCustomSync" : false,
    "defaultSyncIntervalMillis" : 120000,
    "lastSyncedAt" : 1608754155000,
    "lastSyncResult" : "SUCCESS",
    "type" : "AXFR"
  },
  "name" : "www.example.com",
  "ddosThreshold" : 40,
  "id" : 100,
  "lastSavedAt" : 1608754155000,
  "primaryDetails" : {
    "primaryIpAddresses" : [ {
      "id" : 0,
      "value" : "value"
    }, {
      "id" : 0,
      "value" : "value"
    } ],
    "port" : 53,
    "tsigDetails" : {
      "tsigKeys" : [ {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
      }, {
        "name" : "name",
        "id" : 6,
        "type" : "MD5",
        "value" : "value"
      } ],
      "isEnabled" : true
    }
  },
  "configurationStatusDetails" : {
    "lastStatusDate" : 1608754155000,
    "configurationStatus" : "DONE",
    "validationRecord" : "7e2a55815405314e079b9568c912ccfb35c83d8",
    "statusCheckedAt" : 1608754184000,
    "impervaNsRecords" : "[\"ns1.a0.impervasecuredns.net\", \"ns1.a1.impervasecuredns.net\", \"ns1.a2.impervasecuredns.net\"]"
  },
  "type" : "Secondary",
  "creationDate" : 1608581355000
}

```

```
    } ]  
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK SecondarySuccessResponse

400

Invalid input ApiErrorResponse

404

Domain id not found ApiErrorResponse

500

An internal error occurred. Please contact support specifying your account ID and Domain ID. [ApiErrorResponse](#)

Statistics

```
get /stats
```

Retrieve a list of domain statistics (getStats)

Retrieves a list of domain statistics

Query parameters

domainIds (optional)

Query Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.

You can also retrieve it using the GET HTTP method

domainType (optional)

Query Parameter

— domain type to be used to query all domains

from (optional)

Query Parameter

— Start date time of the statistics (epoch time) in milliseconds format: int64

selectAllDomains (optional)

Query Parameter

- Select all domains(for specific domain type - PROTECTED or PRIMARY) in the account, if set to true domainType should also be sent to (optional)
- Query Parameter
- End date time of the statistics (epoch time) in milliseconds format: int64

Return type

[GetDomainStatisticsResponse](#)

Example data

Content-Type: application/json

```
{
  "isError" : false,
  "value" : {
    "numOfRequestsTotalAverage" : 3.21,
    "numOfRequestsPassedAverage" : 2.54,
    "numberOfTotalBlockRequests" : 700.0,
    "numOfRequestsBlockedPeak" : 2.0,
    "numOfRequestsPassedPeak" : 3.0,
    "numberOfTotalRequests" : 1000.0,
    "numOfRequestsTotalPeak" : 5.0,
    "domainIds" : "100",
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "from" : 1608566594000,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "to" : 1608566594000,
    "numberOfRequestsCachedAverage" : 0.67
  }
}
```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [GetDomainStatisticsResponse](#)

400

Failed to get domain statistics. There are no domains under account

500

Internal server error

StatisticsV3

```
get /v3/domains/statistics/account-domains
```

Retrieve a list of domain statistics under the account (getAccountDomainStatistics)
Retrieves a list of domain statistics

Query parameters

from (optional)

Query Parameter

— Start date time of the statistics (epoch time) in milliseconds format: int64

to (optional)

Query Parameter

— End date time of the statistics (epoch time) in milliseconds format: int64

Return type

AccountDomainStatisticsSuccessResponse

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "accountId" : 100,
    "domainStatisticsList" : [ {
      "numOfRequestsTotalAverage" : 3.21,
      "numOfRequestsPassedAverage" : 2.54,
      "numberOfTotalBlockRequests" : 700.0,
      "numOfRequestsBlockedPeak" : 2.0,
      "numOfRequestsPassedPeak" : 3.0,
      "numberOfTotalRequests" : 1000.0,
      "domainId" : 100,
      "numOfRequestsTotalPeak" : 5.0,
      "numOfRequestsBlockedAverage" : 0.67,
      "numberOfRequestsCachedPeak" : 0.67,
      "numberOfRequestsCached" : 280.0,
      "numberOfRequestsPassedToOrigin" : 20.0,
      "numberOfRequestsCachedAverage" : 0.67
    }, {
      "numOfRequestsTotalAverage" : 3.21,
      "numOfRequestsPassedAverage" : 2.54,
      "numberOfTotalBlockRequests" : 700.0,
      "numOfRequestsBlockedPeak" : 2.0,
      "numOfRequestsPassedPeak" : 3.0,
      "numberOfTotalRequests" : 1000.0,
      "domainId" : 100
    } ]
  }
}
```

```

    "domainId" : 100,
    "numOfRequestsTotalPeak" : 5.0,
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "numberOfRequestsCachedAverage" : 0.67
  } ],
  "from" : 1608566594000,
  "to" : 1608566594000
}, {
  "accountId" : 100,
  "domainStatisticsList" : [ {
    "numOfRequestsTotalAverage" : 3.21,
    "numOfRequestsPassedAverage" : 2.54,
    "numberOfTotalBlockRequests" : 700.0,
    "numOfRequestsBlockedPeak" : 2.0,
    "numOfRequestsPassedPeak" : 3.0,
    "numberOfTotalRequests" : 1000.0,
    "domainId" : 100,
    "numOfRequestsTotalPeak" : 5.0,
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "numberOfRequestsCachedAverage" : 0.67
  }, {
    "numOfRequestsTotalAverage" : 3.21,
    "numOfRequestsPassedAverage" : 2.54,
    "numberOfTotalBlockRequests" : 700.0,
    "numOfRequestsBlockedPeak" : 2.0,
    "numOfRequestsPassedPeak" : 3.0,
    "numberOfTotalRequests" : 1000.0,
    "domainId" : 100,
    "numOfRequestsTotalPeak" : 5.0,
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "numberOfRequestsCachedAverage" : 0.67
  } ],
  "from" : 1608566594000,
  "to" : 1608566594000
} ]
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK [AccountDomainStatisticsSuccessResponse](#)

400

Failed to get domain statistics. There are no domains under account [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

```
get /v3/domains/statistics
```

Retrieve a list of domain statistics (getDomainStatistics)

Retrieves a list of domain statistics

Query parameters

domainIds (optional)

Query Parameter

— The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.

You can also retrieve it using the GET HTTP method

domainType (optional)

Query Parameter

— domain type to be used to query all domains

from (optional)

Query Parameter

— Start date time of the statistics (epoch time) in milliseconds format: int64

selectAllDomains (optional)

Query Parameter

— Select all domains(for specific domain type - PROTECTED or PRIMARY) in the account, if set to true

domainType should also be sent

to (optional)

Query Parameter

— End date time of the statistics (epoch time) in milliseconds format: int64

Return type

[DomainStatisticsSuccessResponse](#)

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "numOfRequestsTotalAverage" : 3.21,
```

```

    "numOfRequestsPassedAverage" : 2.54,
    "numberOfTotalBlockRequests" : 700.0,
    "numOfRequestsBlockedPeak" : 2.0,
    "numOfRequestsPassedPeak" : 3.0,
    "numberOfTotalRequests" : 1000.0,
    "numOfRequestsTotalPeak" : 5.0,
    "domainIds" : "100",
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "from" : 1608566594000,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "to" : 1608566594000,
    "numberOfRequestsCachedAverage" : 0.67
}, {
    "numOfRequestsTotalAverage" : 3.21,
    "numOfRequestsPassedAverage" : 2.54,
    "numberOfTotalBlockRequests" : 700.0,
    "numOfRequestsBlockedPeak" : 2.0,
    "numOfRequestsPassedPeak" : 3.0,
    "numberOfTotalRequests" : 1000.0,
    "numOfRequestsTotalPeak" : 5.0,
    "domainIds" : "100",
    "numOfRequestsBlockedAverage" : 0.67,
    "numberOfRequestsCachedPeak" : 0.67,
    "numberOfRequestsCached" : 280.0,
    "from" : 1608566594000,
    "numberOfRequestsPassedToOrigin" : 20.0,
    "to" : 1608566594000,
    "numberOfRequestsCachedAverage" : 0.67
} ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK DomainStatisticsSuccessResponse

400

Failed to get domain statistics. There are no domains under account ApiErrorResponse

500

Internal server error ApiErrorResponse

```
get /v3/domains/statistics/origin-server
```

Retrieve a list of origin server statistics (getOriginServerStatistics)
 Retrieves a list of origin server statistics

Consumes

This API call consumes the following media types via the Content-Type request header:

- */*

Request body

body long (optional)
 Body Parameter
 — End date time of the statistics (epoch time) in milliseconds

Query parameters

domainId (optional)
 Query Parameter
 — The domain's Imperva ID. The domain ID is provided as part of the response when a domain is first added.
 You can also retrieve it using the GET HTTP method
 from (optional)
 Query Parameter
 — Start date time of the statistics (epoch time) in milliseconds format: int64

Return type

OriginStatisticsSuccessResponseV3

Example data

Content-Type: application/json

```
{
  "data" : [ {
    "singleStatisticDtoList" : [ {
      "metric" : "NUM_OF_REQUESTS_TOTAL_PEAK",
      "value" : "5.6",
      "domainId" : 100
    }, {
      "metric" : "NUM_OF_REQUESTS_TOTAL_PEAK",
      "value" : "5.6",
      "domainId" : 100
    } ],
    "serverName" : "ns1.example.com",
    "multiStatisticDtoList" : [ {
      "metric" : "NUM_OF_REQUESTS_TOTAL",
      "values" : "[4.67,5.6]",
      "interval" : 15000
    }, {
```

```

    "metric" : "NUM_OF_REQUESTS_TOTAL",
    "values" : "[4.67,5.6]",
    "interval" : 15000
  },
  "requestDistributionDto" : [ {
    "category" : "ns1.example.com",
    "value" : "5000"
  }, {
    "category" : "ns1.example.com",
    "value" : "5000"
  } ]
}, {
  "singleStatisticDtoList" : [ {
    "metric" : "NUM_OF_REQUESTS_TOTAL_PEAK",
    "value" : "5.6",
    "domainId" : 100
  }, {
    "metric" : "NUM_OF_REQUESTS_TOTAL_PEAK",
    "value" : "5.6",
    "domainId" : 100
  } ],
  "serverName" : "ns1.example.com",
  "multiStatisticDtoList" : [ {
    "metric" : "NUM_OF_REQUESTS_TOTAL",
    "values" : "[4.67,5.6]",
    "interval" : 15000
  }, {
    "metric" : "NUM_OF_REQUESTS_TOTAL",
    "values" : "[4.67,5.6]",
    "interval" : 15000
  },
  "requestDistributionDto" : [ {
    "category" : "ns1.example.com",
    "value" : "5000"
  }, {
    "category" : "ns1.example.com",
    "value" : "5000"
  } ]
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

OK OriginStatisticsSuccessResponseV3

400

Failed to get origin server statistics. There are no domains under account [ApiErrorResponse](#)

500

Internal server error [ApiErrorResponse](#)

Models

Methods

Table of Contents

1. [APIError](#)
 2. [AccountConfigPojo](#)
 3. [AccountDomainStatisticsSuccessResponse](#)
 4. [AccountDomainsStatisticsResponse](#)
 5. [AccountDomainsSuccessResponse](#)
 6. [AccountSiemInfoSuccessResponse](#)
 7. [AdaptiveThresholdRequestDto](#)
 8. [ApiErrorResponse](#)
 9. [AppliedOnAsset](#)
 10. [AssetDto](#)
 11. [AutomaticSafeRecordLearningDto](#)
 12. [AutomaticSafeRecordRequestDto](#)
 13. [AutomaticSafeRecordSuccessResponse](#)
 14. [BlockRecordType](#)
 15. [DnssecKeysResponseDto](#)
 16. [DnssecResponse](#)
 17. [DnssecResponseApi](#)
 18. [DomainAddRequest](#)
 19. [DomainAttackResponse](#)
 20. [DomainAttacksResponse](#)
 21. [DomainConfigurationInfo](#)
 22. [DomainEditRequest](#)
 23. [DomainResponse](#)
 24. [DomainResponseV3](#)
 25. [DomainStatisticsDto](#)
 26. [DomainStatisticsSuccessResponse](#)
 27. [GetDomainAttacksResponse](#)
 28. [GetDomainStatisticsResponse](#)
 29. [GetDomainsResponse](#)
 30. [ManagedDomainRecordRequest](#)
-

-
- 31. ManagedDomainRecordResponse
 - 32. ManagedDomainRequest
 - 33. ManagedDomainResponse
 - 34. MultiStatistic
 - 35. OriginServerRequestDistributionDto
 - 36. OriginServerStatsResponseDto
 - 37. OriginStatisticsSuccessResponseV3
 - 38. PrimaryDomainRequest
 - 39. PrimaryDomainResponse
 - 40. PrimaryDomainSuccessResponse
 - 41. PrimaryIpAddressDto
 - 42. PrimaryIpAddressResponse
 - 43. PrimaryIpsResponse
 - 44. ProtectedDomainRequest
 - 45. ProtectedDomainResponse
 - 46. ProtectedDomainSafeRecordsRequest
 - 47. ProtectedDomainSafeRecordsResponse
 - 48. ProtectedDomainSafeRecordsSuccessResponse
 - 49. ProtectedDomainSafeRecordsTypeRequest
 - 50. ProtectedDomainSafeRecordsTypeResponse
 - 51. ProtectedDomainSafeRecordsTypeSuccessResponse
 - 52. ProtectedDomainSuccessResponse
 - 53. ProtectedSafeRecord
 - 54. ProxyDomainRequest
 - 55. ProxyDomainResponse
 - 56. PurgeCacheRequest
 - 57. PurgeCacheRequestV3
 - 58. RecordValidationResponse
 - 59. RegistrarDetails
 - 60. SecondaryDomainRequest
 - 61. SecondaryDomainRequestV3
 - 62. SecondaryDomainResponse
 - 63. SecondaryDomainResponseV3
 - 64. SecondaryPrimaryDetails
 - 65. SecondarySuccessResponse
 - 66. SecondaryTransferDetails
 - 67. SecondaryTsigDetailsResponse
 - 68. SiemConfigResponseDto
 - 69. SiemConfigurationRequest
 - 70. SimpleDomainAttacksResponse
 - 71. SimpleDomainResponse
 - 72. SimpleTextSuccessResponse
 - 73. SimpleTextSuccessResponseV3
-

74. SingleStatistic
 75. StatisticsResponse
 76. SyncDetailsDto
 77. TsigKeyDto
 78. TsigKeyDtoResponse
 79. TsigResponse
 80. UpdateStatusRequestDto
 81. domainId_file_body
 82. domain_file_body
 83. domainid_file_body
 84. primary_file_body
 85. saferecords_file_body

APIError

status
Integer
 format: int32
 id
String
 code
String
 source
 map[String, Object]
 title
String
 detail
String

AccountConfigPojo

accountId
Long
 format: int64
 configurationId
Long
 format: int64
 configurationName
String
 isEnabled
Boolean
 description
String
 assetDtoList
 array[AssetDto]
 configurationType
String
 Enum:
 SIEM_DNS_PROTECTION_EVENTS
 SIEM_DNS_TRAFFIC_LOGS
 SIEM_DNS_SECURITY_LOGS
 AUTOMATIC_SAFE_RECORDS
 AUTOMATIC_SAFE_RECORDS_TSIG_KEYS

```
subConfigurations
array[AccountConfigPojo]
appliedOnEntity
AppliedOnAsset
configurationValue
String
isActive
Boolean
isDeleted
Boolean
```

AccountDomainStatisticsSuccessResponse

```
data
array[AccountDomainsStatisticsResponse]
```

AccountDomainsStatisticsResponse

```
from (optional)
Long
The Statistics time frame Start Date in milliseconds format: int64
example: 1608566594000
to (optional)
Long
The Statistics time frame End Date in milliseconds format: int64
example: 1608566594000
accountId (optional)
Long
The Account ID format: int64
example: 100
domainStatisticsList (optional)
array[DomainStatisticsDto]
The domain statistics list
```

AccountDomainsSuccessResponse

```
data
array[DomainResponseV3]
```

AccountSiemInfoSuccessResponse

```
data
array[SiemConfigResponseDto]
```

AdaptiveThresholdRequestDto

ApiErrorResponse

```
errors
array[APIError]
```

AppliedOnAsset

assetIds
array[Long]
format: int64

AssetDto

id
Long
format: int64
name
String
syncStatus
String
Enum:
SUCCESS
ERROR_PRIMARY_IP
INVALID_DNS_RESPONSE
ERROR_CONNECTION
ERROR_AUTHENTICATION
ERROR_TSIG
ERROR_TOO_MANY_RECORDS
ERROR_DNSSEC_EXISTS
ERROR_GENERAL
ALREADY_SYNCED
INVALID_RECORDS
MISSING_SOA_RECORD
SYNC_DENIED
statusMessage
String
lastSyncDate
Date
format: date-time

AutomaticSafeRecordLearningDto

accountId
Long
format: int64
configurationId
Long
format: int64
configurationName
String
isEnabled
Boolean
description
String
assetDtoList
array[AssetDto]
configurationType
String
Enum:
SIEM_DNS_PROTECTION_EVENTS
SIEM_DNS_TRAFFIC_LOGS
SIEM_DNS_SECURITY_LOGS

AUTOMATIC_SAFE_RECORDS
 AUTOMATIC_SAFE_RECORDS_TSIG_KEYS
 subConfigurations
 array[AccountConfigPojo]
 appliedOnEntity
AppliedOnAsset
 configurationValue
String
 isActive
Boolean
 isDeleted
Boolean
 syncDetailsDto
SyncDetailsDto

AutomaticSafeRecordRequestDto

configName
String
 description
String
 isEnabled
Boolean
 syncDetailsDto
SyncDetailsDto

AutomaticSafeRecordSuccessResponse

data
 array[AutomaticSafeRecordLearningDto]

BlockRecordType

type (optional)
String
 A DNS record type designated as block, which will consistently be blocked.
 example: AAAA
 enabled (optional)
Boolean
 Enable/disable the block record type.
 example: true

DnssecKeysResponseDto

digest (optional)
String
 The digest
 example: 1
 digestType (optional)
String
 The digest type
 example: www.example.com
 algorithm (optional)
String
 The algorithm number
 example: 1

publicKey (optional)
String
The public key
example: A
keyTag (optional)
String
The key tag
example: IN
flags (optional)
String
The key flag
example: 267
createdAt (optional)
Long
The key creation date format: int64

DnssecResponse

domainId (optional)
Long
The Domain ID format: int64
example: 100
domainName (optional)
String
The Domain name
example: example.com
status (optional)
String
The DNSSEC status of the domain.
Enum:
ENABLED
DISABLED
DELETION_PROGRESS
example: ENABLED
isRegistrarSynced (optional)
Boolean
Indicates if the DS record is updated at the registrar.
example: false
lastSyncedAt (optional)
Long
The last time the DNSSEC status of the domain was checked. (Unix epoch time, in milliseconds). format: int64
example: 1608754155000
statusChangedAt (optional)
Long
The last time the DNSSEC status changed. (Unix epoch time, in milliseconds). format: int64
example: 1608754155000
dsRecord (optional)
DnssecKeysResponseDto
registrarDetails (optional)
RegistrarDetails
dsRecords
DnssecKeysResponseDto

DnssecResponseApi

value (optional)
DnssecResponse

isError (optional)

Boolean

States if an error has occurred

example: false

DomainAddRequest

ddosThreshold

Integer

The maximum incoming query rate for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

blockDomain

Boolean

Indicates whether the domain is blocked or not

example: false

managedDomain (optional)

ManagedDomainRequest

proxyDomain (optional)

ProxyDomainRequest

name

String

The Domain name

example: www.example.com

type

String

The Domain type

Enum:

PROXY

MANAGED

SECONDARY

MANAGED_BANK

example: MANAGED

DomainAttackResponse

data

array[**DomainAttacksResponse**]

DomainAttacksResponse

id (optional)

Long

The Attack ID format: int64

example: 100

domainId (optional)

Long

The Domain ID format: int64

example: 100

domainName (optional)

String

The domain name

example: www.example.com

startedAt (optional)

Long

The Attack Start Date in milliseconds format: int64

example: 1608566594000

endedAt (optional)

Long

The Attack End Date in milliseconds format: int64

example: 1608581355000

detectedBy (optional)

Integer

The Machine ID format: int32

example: 1000

type (optional)

String

The Attack Type

Enum:

DDOS

example: DDOS

queriesPerSecondPeak (optional)

Float

Peak queries per second during the attack format: float

example: 100.0

queriesPerSecondAvg (optional)

Float

Average queries per second during the attack format: float

example: 100.0

ddosThreshold (optional)

Long

The DDoS threshold value that were configured during the attack format: int64

example: 100

initialRps (optional)

Long

The initial RPS that was identified and triggered the DDoS attack format: int64

example: 100

DomainConfigurationInfo

configurationStatus (optional)

String

The Domain configuration status

Enum:

DS_VALIDATION_REQUIRED

DNSSEC_VALIDATION_REQUIRED

VALIDATION_REQUIRED

NS_VALIDATION_REQUIRED

DONE

example: DONE

lastStatusDate (optional)

Long

The last configuration status change date in milliseconds format: int64

example: 1608754155000

statusCheckedAt (optional)

Long

The Domain last status check date in milliseconds format: int64

example: 1608754184000

impervaNsRecords (optional)

array[String]

A list of NS records provided by Imperva

example: ["ns1.a0.impervasecuredns.net", "ns1.a1.impervasecuredns.net", "ns1.a2.impervasecuredns.net"]

validationRecord (optional)

String

The TXT record for domain validation
example: 7e2a55815405314e079b9568c912ccfb35c83d8

DomainEditRequest

ddosThreshold

Integer

The maximum incoming query rate for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

blockDomain

Boolean

Indicates whether the domain is blocked or not

example: false

managedDomain (optional)

ManagedDomainRequest

proxyDomain (optional)

ProxyDomainRequest

DomainResponse

id (optional)

Long

The Domain ID format: int64

example: 100

name (optional)

String

The Domain name

example: www.example.com

accountId (optional)

Long

The Account ID format: int64

example: 200

type (optional)

String

The Domain type

Enum:

PROXY

MANAGED

SECONDARY

MANAGED_BANK

example: MANAGED

configurationStatus (optional)

String

The Domain configuration status

Enum:

DS_VALIDATION_REQUIRED

DNSSEC_VALIDATION_REQUIRED

VALIDATION_REQUIRED

NS_VALIDATION_REQUIRED

DONE

example: DONE

lastStatusDate (optional)

Long

The last configuration status change date in milliseconds format: int64

example: 1608754155000

validationRecord (optional)

String

The TXT record for domain validation

example: 7e2a55815405314e079b9568c912ccfb35c83d8

ddosThreshold (optional)

Integer

The maximum incoming query rate for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

blockDomain (optional)

Boolean

Indicates whether the domain is blocked or not

example: false

creationDate (optional)

Long

The Domain creation date in milliseconds format: int64

example: 1608581355000

lastSavedAt (optional)

Long

The Domain last save date in milliseconds format: int64

example: 1608754155000

statusCheckedAt (optional)

Long

The Domain last status check date in milliseconds format: int64

example: 1608754184000

impervaNsRecords (optional)

array[String]

A list of NS records provided by Imperva

example: [ns241.a0.impervasecuredns.net,ns79.a1.impervasecuredns.net,ns158.a2.impervasecuredns.net]

managedDomain (optional)

ManagedDomainResponse

proxyDomain (optional)

ProxyDomainResponse**DomainResponseV3**

id (optional)

Long

The Domain ID format: int64

example: 100

name

String

The Domain name

example: www.example.com

accountId (optional)

Long

The Account ID format: int64

example: 200

type (optional)

String

The Domain type

Enum:

Protected

Primary

Secondary

example: Protected

creationDate (optional)

Long

The Domain creation date in milliseconds format: int64

example: 1608581355000

lastSavedAt (optional)

Long

The Domain last save date in milliseconds format: int64

example: 1608754155000

configurationStatusDetails (optional)

DomainConfigurationInfo

DomainStatisticsDto

domainId (optional)

Long

The Domain ID format: int64

example: 100

numOfRequestsTotalPeak (optional)

Float

Peak number of requests (RPS) in the time frame format: float

example: 5.0

numOfRequestsTotalAverage (optional)

Float

Average number of requests (RPS) in the time frame format: float

example: 3.21

numOfRequestsPassedPeak (optional)

Float

Peak number of passed requests (RPS) in the time frame format: float

example: 3.0

numOfRequestsPassedAverage (optional)

Float

Average number of passed requests (RPS) in the time frame format: float

example: 2.54

numOfRequestsBlockedPeak (optional)

Float

Peak number of blocked requests (RPS) in the time frame format: float

example: 2.0

numOfRequestsBlockedAverage (optional)

Float

Average number of blocked requests (RPS) in the time frame format: float

example: 0.67

numberOfRequestsCachedPeak (optional)

Float

Peak number of cached requests (RPS) in the time frame format: float

example: 0.67

numberOfRequestsCachedAverage (optional)

Float

Average number of cached requests (RPS) in the time frame format: float

example: 0.67

numberOfTotalRequests (optional)

Float

Total requests in the time frame format: float

example: 1000.0

numberOfTotalBlockRequests (optional)

Float

Total blocked requests in the time frame format: float

example: 700.0

numberOfRequestsCached (optional)

Float

Total cached requests in the time frame format: float

example: 280.0

numberOfRequestsPassedToOrigin (optional)

Float

Total passed to origin requests in the time frame format: float

example: 20.0

DomainStatisticsSuccessResponse

data

array[StatisticsResponse]

GetDomainAttacksResponse

value (optional)

array[DomainAttacksResponse]

isError (optional)

Boolean

States if an error has occurred

example: false

GetDomainStatisticsResponse

value (optional)

StatisticsResponse

isError (optional)

Boolean

States if an error has occurred

example: false

GetDomainsResponse

value (optional)

array[DomainResponse]

isError (optional)

Boolean

States if an error has occurred

example: false

ManagedDomainRecordRequest

id

Long

The Record id format: int64

example: 1000

name

String

The Record name

example: www.example.com

ttl (optional)

Integer

The Record TTL format: int32

example: 1

type

String

The Record type

Enum:

A
AAAA
NS
MX
TXT
CNAME
SRV
PTR
example: A
classType (optional)
String
The Record class
Enum:
IN
CH
HS
example: IN
data
array[String]
The Record data
example: ["1.2.3.4"]
comment (optional)
String
The Record comment
example: Example comment

ManagedDomainRecordResponse

dnsRecords (optional)
array[ManagedDomainRecordRequest]
A List of domain records
unsupportedDnsRecords (optional)
array[ManagedDomainRecordRequest]
A List of unsupported domain records

ManagedDomainRequest

ownerEmail (optional)
String
The Domain owner email
example: admin@example.com
defaultTtl (optional)
Integer
The length of time for the DNS resolver to cache a DNS response. format: int32
example: 3600
minTtl (optional)
Integer
The length of time for the DNS resolver to cache a negative DNS response - where the information on the requested domain is unknown or does not exist. format: int32
example: 1
secondaryDomain (optional)
SecondaryDomainRequest
tsigDetails (optional)
SecondaryTsigDetailsResponse

ManagedDomainResponse

ownerEmail (optional)

String

The Domain owner email

example: admin@example.com

defaultTtl (optional)

Integer

The length of time for the DNS resolver to cache a DNS response. format: int32

example: 3600

minTtl (optional)

Integer

The length of time for the DNS resolver to cache a negative DNS response - where the information on the requested domain is unknown or does not exist. format: int32

example: 1

secondaryDomain (optional)

SecondaryDomainResponse

registrarDetails (optional)

RegistrarDetails

tsigDetails (optional)

SecondaryTsigDetailsResponse**Multistatistic**

metric (optional)

String

Name of metric

example: NUM_OF_REQUESTS_TOTAL

values (optional)

array[Object]

Values of the metric

example: [4.67,5.6]

interval (optional)

Long

Metric interval in seconds format: int64

example: 15000

OriginServerRequestDistributionDto

category (optional)

String

Distribution of requests by category like IP, name server, or service. Helps identify traffic load.

example: ns1.example.com

value (optional)

String

requests distribution value(number)

example: 5000

OriginServerStatsResponseDto

serverName (optional)

String

The origin server name

example: ns1.example.com

multiStatisticDtoList

array[MultiStatistic]

```
singleStatisticDtoList
array[SingleStatistic]
requestDistributionDto
array[OriginServerRequestDistributionDto]
```

OriginStatisticsSuccessResponseV3

data
array[OriginServerStatsResponseDto]

PrimaryDomainRequest

name
String
The Domain name
example: www.example.com
ddosThreshold
Integer
The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32
example: 40
ownerEmail (optional)
String
The Domain owner email
example: admin@example.com
defaultTtl (optional)
Integer
The length of time for the DNS resolver to cache a DNS response. format: int32
example: 3600
minTtl (optional)
Integer
The length of time for the DNS resolver to cache a negative DNS response - where the information on the requested domain is unknown or does not exist. format: int32
example: 1

PrimaryDomainResponse

name
String
The Domain name
example: www.example.com
ddosThreshold
Integer
The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32
example: 40
ownerEmail (optional)
String
The Domain owner email
example: admin@example.com
defaultTtl (optional)
Integer
The length of time for the DNS resolver to cache a DNS response. format: int32
example: 3600
minTtl (optional)
Integer

The length of time for the DNS resolver to cache a negative DNS response - where the information on the requested domain is unknown or does not exist. format: int32

example: 1

id (optional)

Long

The Domain ID format: int64

example: 100

accountId (optional)

Long

The Account ID format: int64

example: 200

type (optional)

String

The Domain type

Enum:

Protected

Primary

Secondary

example: Primary

creationDate (optional)

Long

The Domain creation date in milliseconds format: int64

example: 1608581355000

lastSavedAt (optional)

Long

The Domain last save date in milliseconds format: int64

example: 1608754155000

configurationStatusDetails (optional)

DomainConfigurationInfo

registrarDetails (optional)

RegistrarDetails

PrimaryDomainSuccessResponse

data

array[**PrimaryDomainResponse**]

PrimaryIpAddressDto

value (optional)

String

The primary ip value

PrimaryIpAddressResponse

value (optional)

String

The primary ip value

id (optional)

Long

The primary ip id format: int64

PrimaryIpsResponse

value (optional)

array[**PrimaryIpAddressResponse**]

isError (optional)

Boolean

States if an error has occurred

example: false

ProtectedDomainRequest

name

String

The Domain name

example: www.example.com

ddosThreshold

Integer

The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

outgoingRequestRateLow (optional)

Integer

The outgoing request rate low threshold format: int32

example: 10

outgoingRequestRateHigh (optional)

Integer

The outgoing request rate high threshold format: int32

example: 50

safeSubDomains (optional)

array[String]

A list of safe sub domains, **Important:** By default, this operation will add safe records with the 'ALL_TYPES' option for their type, which is not recommended. It is advisable to use the alternative field

[protectedSafeRecordList]

example: ["www", "http", "static"]

protectedSafeSubDomainList (optional)

array[ProtectedSafeRecord]

A list of protected safe domains

originalINSRecords (optional)

array[String]

A list of the original NS records of the domain

example: ["ns101.cloudns.net.", "ns102.cloudns.net.", "ns103.cloudns.net."]

blockRecordTypes (optional)

array[BlockRecordType]

A list of block record types which will consistently be blocked.

ProtectedDomainResponse

name

String

The Domain name

example: www.example.com

ddosThreshold

Integer

The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

outgoingRequestRateLow (optional)

Integer

The outgoing request rate low threshold format: int32

example: 10

outgoingRequestRateHigh (optional)

Integer

The outgoing request rate high threshold format: int32

example: 50

safeSubDomains (optional)

array[String]

A list of safe sub domains, **Important:** By default, this operation will add safe records with the 'ALL_TYPES' option for their type, which is not recommended. It is advisable to use the alternative field [protectedSafeRecordList]

example: ["www", "http", "static"]

protectedSafeSubDomainList (optional)

array[ProtectedSafeRecord]

A list of protected safe domains

originalNSRecords (optional)

array[String]

A list of the original NS records of the domain

example: ["ns101.cloudns.net.", "ns102.cloudns.net.", "ns103.cloudns.net."]

blockRecordTypes (optional)

array[BlockRecordType]

A list of block record types which will consistently be blocked.

id (optional)

Long

The Domain ID format: int64

example: 100

accountId (optional)

Long

The Account ID format: int64

example: 200

type (optional)

String

The Domain type

Enum:

Protected

Primary

Secondary

example: Protected

creationDate (optional)

Long

The Domain creation date in milliseconds format: int64

example: 1608581355000

lastSavedAt (optional)

Long

The Domain last save date in milliseconds format: int64

example: 1608754155000

configurationStatusDetails (optional)

DomainConfigurationInfo

isAdaptiveThresholdEnabled (optional)

Boolean

The domain configuration details

example: true

adaptiveThreshold

AdaptiveThresholdRequestDto

ProtectedDomainSafeRecordsRequest

safeSubDomains (optional)

array[String]

DNS requests for these sub zones are answered until the request rate passes the rate limit threshold.

example: ["www", "http", "static"]

ProtectedDomainSafeRecordsResponse

safeSubDomains (optional)

array[String]

DNS requests for these sub zones are answered until the request rate passes the rate limit threshold.

example: ["www", "http", "static"]

ProtectedDomainSafeRecordsSuccessResponse

data

array[ProtectedDomainSafeRecordsResponse]

ProtectedDomainSafeRecordsTypeRequest

safeSubDomains (optional)

array[ProtectedSafeRecord]

DNS requests for these sub zones are answered until the request rate passes the rate limit threshold.

example: ["www", "http", "static"]

ProtectedDomainSafeRecordsTypeResponse

safeSubDomains (optional)

array[ProtectedSafeRecord]

DNS requests for these sub zones are answered until the request rate passes the rate limit threshold.

ProtectedDomainSafeRecordsTypeSuccessResponse

data

array[ProtectedDomainSafeRecordsTypeResponse]

ProtectedDomainSuccessResponse

data

array[ProtectedDomainResponse]

ProtectedSafeRecord

recordName (optional)

String

The prefix for the domain name. For example, if the full domain is example.com, the prefix would be 'www'.

example: www

recordTypes (optional)

String

The types of the record, A, CNAME, TXT, etc. The value ALL_TYPES allows all record types

example: A,TXT,CNAME

ProxyDomainRequest

outgoingRequestRateLow (optional)

Integer

The outgoing request rate low threshold format: int32

example: 10

outgoingRequestRateHigh (optional)

Integer

The outgoing request rate high threshold format: int32

example: 50

safeSubDomains (optional)

array[String]

A list of safe sub domains

example: [a.example.com, b.example.com]

bypassDomain (optional)

Boolean

When bypass mode = true, queries for this domain bypass Imperva and are served directly by your origin.

example: false

originalNSRecords (optional)

array[String]

A list of the original NS records of the domain

example: [ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]

blockRecordTypes (optional)

array[BlockRecordType]

A list of block record types which will consistently be blocked.

ProxyDomainResponse

originalNsRecords (optional)

array[String]

A list of the original NS records of the domain

example: [ns101.cloudns.net.,ns102.cloudns.net.,ns103.cloudns.net.]

safeSubDomains (optional)

array[String]

A list of safe sub domains

example: [a.example.com, b.example.com]

blockRecordTypes (optional)

array[BlockRecordType]

A list of block record types which will consistently be blocked.

outgoingRequestRateLow (optional)

Integer

The outgoing request rate low threshold format: int32

example: 10

outgoingRequestRateHigh (optional)

Integer

The outgoing request rate high threshold format: int32

example: 50

bypassDomain (optional)

Boolean

When bypass mode = true, queries for this domain bypass Imperva and are served directly by your origin.

example: false

PurgeCacheRequest

resourceType

String

The type of the requested resource to purge

example: A

resourceValue

String

The value of the requested resource to purge

example: 1.2.3.4

PurgeCacheRequestV3

purgeType

StringThe type of the purge, ALL - will purge all resources under domain, SINGLE will purge the given resource
Enum:

ALL

SINGLE

example: SINGLE

resourceType (optional)

String

The type of the requested resource to purge

example: A

resourceValue (optional)

String

The value of the requested resource to purge

example: 1.2.3.4

RecordValidationResponse

hasFound (optional)

Boolean

Indicates whether the record for validation was found in the DNS Protection service

example: true

message (optional)

String

Informative message about the validation record

example: TXT record was found!

recordValidationMap (optional)

map[String, Boolean]

Record name to is found indication map

RegistrarDetails

registrar (optional)

String

Domain registrar name

example: GoDaddy.com, LLC

registrarUrl (optional)

String

Domain registrar URL

example: http://www.godaddy.com

SecondaryDomainRequest

primaryIpAddresses

array[PrimaryIpAddressResponse]

The IP address of the primary DNS server

port (optional)

Integer

The port number format: int32

example: 53

type (optional)

String

The transfer type

Enum:

AXFR

example: AXFR

isCustomSync (optional)

Boolean

Indicates whether the zone should be synchronized according to the custom interval

example: false

customSyncIntervalMillis (optional)

Integer

The custom synchronization interval, in milliseconds format: int32

example: 60000

SecondaryDomainRequestV3

name

String

The Domain name

example: www.example.com

ddosThreshold

Integer

The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32

example: 40

primaryDetails (optional)

SecondaryPrimaryDetails

type (optional)

String

The transfer type

Enum:

AXFR

example: AXFR

isCustomSync (optional)

Boolean

Indicates whether the zone should be synchronized according to the custom interval

example: false

customSyncIntervalMillis (optional)

Integer

The custom synchronization interval, in milliseconds format: int32

example: 60000

SecondaryDomainResponse

id

Long

format: int64

primaryIpAddresses (optional)

array[PrimaryIpAddressDto]

The IP addresses of the primary DNS server

example: [1.1.1.1,2.2.2.2]

port (optional)

Integer

The port number format: int32

example: 53

type (optional)

String

The transfer type

Enum:

AXFR

example: AXFR
 isCustomSync (optional)
Boolean
 Indicates whether the zone should be synchronized according to the custom interval
 example: false
 customSyncIntervalMillis (optional)
Integer
 The custom synchronization interval, in milliseconds format: int32
 example: 30000
 defaultSyncIntervalMillis (optional)
Integer
 The default synchronization interval, in milliseconds format: int32
 example: 120000
 retryIntervalMillis (optional)
Integer
 The retry interval in case previous synchronization failed, in milliseconds format: int32
 example: 2400
 lastSyncedAt (optional)
Long
 The last synchronization date in milliseconds format: int64
 example: 1608754155000
 lastSyncResult (optional)
String
 The last synchronization result
 Enum:
 SUCCESS
 ERROR_AUTHENTICATION
 ERROR_TSIG
 ERROR_GENERAL
 example: SUCCESS
 syncInstructions (optional)
String
 The instructions in case last synchronization failed
 customSync
Boolean

SecondaryDomainResponseV3

name
String
 The Domain name
 example: www.example.com
 ddosThreshold
Integer
 The maximum incoming query rate (QPS) for the domain. The threshold above which Imperva DDoS mitigation is triggered. format: int32
 example: 40
 id (optional)
Long
 The Domain ID format: int64
 example: 100
 accountId (optional)
Long
 The Account ID format: int64
 example: 200
 type (optional)
String
 The Domain type

Enum:
 Protected
 Primary
 Secondary
 example: Secondary
 creationDate (optional)

Long
 The Domain creation date in milliseconds format: int64

example: 1608581355000
 lastSavedAt (optional)

Long
 The Domain last save date in milliseconds format: int64

example: 1608754155000
 primaryDetails (optional)

SecondaryPrimaryDetails
 secondaryTransferDetails (optional)
SecondaryTransferDetails
 configurationStatusDetails (optional)

DomainConfigurationInfo

SecondaryPrimaryDetails

primaryIpAddresses
 array[PrimaryIpAddressResponse]

The IP address of the primary DNS server
 tsigDetails (optional)

SecondaryTsigDetailsResponse
 port (optional)

Integer
 The port number format: int32
 example: 53

SecondarySuccessResponse

data
 array[SecondaryDomainResponseV3]

SecondaryTransferDetails

type (optional)

String
 The transfer type
 Enum:

AXFR

example: AXFR

isCustomSync (optional)

Boolean

Indicates whether the zone should be synchronized according to the custom interval

example: false

customSyncIntervalMillis (optional)

Integer

The custom synchronization interval, in milliseconds format: int32

example: 30000

defaultSyncIntervalMillis (optional)

Integer

The default synchronization interval, in milliseconds format: int32

example: 120000
retryIntervalMillis (optional)

Integer

The retry interval in case previous synchronization failed, in milliseconds format: int32

example: 2400

lastSyncedAt (optional)

Long

The last synchronization date in milliseconds format: int64

example: 1608754155000

lastSyncResult (optional)

String

The last synchronization result

Enum:

SUCCESS

ERROR_AUTHENTICATION

ERROR_TSIG

ERROR_GENERAL

example: SUCCESS

syncInstructions (optional)

String

The instructions in case last synchronization failed

SecondaryTsigDetailsResponse

isEnabled (optional)

Boolean

When true - TSIG is enabled

tsigKeys (optional)

array[TsigKeyDtoResponse]

When true - TSIG is enabled

SiemConfigResponseDto

assetIds

array[Long]

format: int64

region

String

Enum:

US

EU

APAC

AU

accountId

Long

format: int64

configurationId

Long

format: int64

isEnabled

Boolean

appliedOnAllAssets

Boolean

datasetType

String

Enum:

DNS_Protection_Events

DNS_Traffic_Logs
DNS_Security_Logs

SiemConfigurationRequest

region (optional)

String

The Region

Enum:

US

EU

APAC

AU

example: US

assetIds (optional)

array[Long]

Asset Ids List format: int64

example: [123,456]

siemLogType

String

Siem log type

Enum:

DNS_Protection_Events

DNS_Traffic_Logs

DNS_Security_Logs

example: DNS_Protection_Events

appliedOnAllAssets

Boolean

appliedOnAllAssets

example: true

SimpleDomainAttacksResponse

value (optional)

DomainAttacksResponse

isError (optional)

Boolean

States if an error has occurred

example: false

SimpleDomainResponse

value (optional)

DomainResponse

isError (optional)

Boolean

States if an error has occurred

example: false

SimpleTextSuccessResponse

value (optional)

String

isError (optional)

Boolean

States if an error has occurred

example: false

SimpleTextSuccessResponseV3

data

array[String]

SingleStatistic

value (optional)

Object

Value of metric

example: 5.6

metric (optional)

String

Name of metric

example: NUM_OF_REQUESTS_TOTAL_PEAK

domainId (optional)

Long

The Domain ID format: int64

example: 100

StatisticsResponse

from (optional)

Long

The Statistics time frame Start Date in milliseconds format: int64

example: 1608566594000

to (optional)

Long

The Statistics time frame End Date in milliseconds format: int64

example: 1608566594000

domainIds (optional)

array[Long]

The Domain ID format: int64

example: 100

numOfRequestsTotalPeak (optional)

Float

Peak number of requests (RPS) in the time frame format: float

example: 5.0

numOfRequestsTotalAverage (optional)

Float

Average number of requests (RPS) in the time frame format: float

example: 3.21

numOfRequestsPassedPeak (optional)

Float

Peak number of passed requests (RPS) in the time frame format: float

example: 3.0

numOfRequestsPassedAverage (optional)

Float

Average number of passed requests (RPS) in the time frame format: float

example: 2.54

numOfRequestsBlockedPeak (optional)

Float

Peak number of blocked requests (RPS) in the time frame format: float

example: 2.0

numOfRequestsBlockedAverage (optional)

Float

Average number of blocked requests (RPS) in the time frame format: float

example: 0.67

numberOfRequestsCachedPeak (optional)

Float

Peak number of cached requests (RPS) in the time frame format: float

example: 0.67

numberOfRequestsCachedAverage (optional)

Float

Average number of cached requests (RPS) in the time frame format: float

example: 0.67

numberOfTotalRequests (optional)

Float

Total requests in the time frame format: float

example: 1000.0

numberOfTotalBlockRequests (optional)

Float

Total blocked requests in the time frame format: float

example: 700.0

numberOfRequestsCached (optional)

Float

Total cached requests in the time frame format: float

example: 280.0

numberOfRequestsPassedToOrigin (optional)

Float

Total passed to origin requests in the time frame format: float

example: 20.0

SyncDetailsDto

originServerIpList

array[String]

type

String

Enum:

AXFR

IXFR

port

Integer

format: int32

tsigKeys

array[TsigKeyDto]

isTsigEnabled (optional)

Boolean

TsigKeyDto

type (optional)

String

The TSIG Signature Algorithm type

Enum:

MD5

SHA1

SHA224

SHA256

SHA384

SHA512
name (optional)
String
The TSIG name
value (optional)
String
The TSIG value

TsigKeyDtoResponse

type (optional)
String
The TSIG Signature Algorithm type
Enum:
MD5
SHA1
SHA224
SHA256
SHA384
SHA512
name (optional)
String
The TSIG name
value (optional)
String
The TSIG value
id (optional)
Long
The TSIG key id format: int64

TsigResponse

value (optional)
array[TsigKeyDtoResponse]
isError (optional)
Boolean
States if an error has occurred
example: false

UpdateStatusRequestDto

isEnabled
Boolean

domainId_file_body

domainDetails
String
the domain details
example: {
 "ddosThreshold" : "40",
 "blockDomain" : "true"
}
zoneFile (optional)
byte[]
DNS Zone File format: binary

domain_file_body

domainDetails
String
The domain details
example: {
 "ddosThreshold" : "40",
 "blockDomain" : "true",
 "name" : "www.example.com"
}

zoneFile
byte[]
DNS Zone File (BIND) format: binary

domainid_file_body

domainDetails
String
the domain details
example: {
 "ddosThreshold" : "40",
}

zoneFile (optional)
byte[]
DNS Zone File format: binary

primary_file_body

domainDetails
String
The domain details
example: {
 "ddosThreshold" : "40",
 "name" : "www.example.com"
}

zoneFile
byte[]
DNS Zone File (BIND) format: binary

saferecords_file_body

zoneFile (optional)
byte[]
DNS Zone File format: binary

Usage Report API

Retrieve bandwidth usage history for your account. For the full feature documentation, see [View Account Usage](#).

Version: v1

BasePath:/usage-report

All rights reserved

<http://apache.org/licenses/LICENSE-2.0.html>

Access

1. APIKey KeyParamName:x-API-Id KeyInQuery:false KeyInHeader:true
2. APIKey KeyParamName:x-API-Key KeyInQuery:false KeyInHeader:true

Methods

Models

Table of Contents

AccountUsage

- get /api/v1/actual-usage/bandwidth
- get /api/v1/billing-summary

AccountUsage

```
get /api/v1/actual-usage/bandwidth
```

Retrieve account usage data (getActualUsageApi)
 Retrieves usage data for each bucket in the specified time range.

Query parameters

caid (required)
 Query Parameter
 — The account id format: int64

end (required)
 Query Parameter
 — The end date of the usage data to retrieve format: date-time

start (required)
 Query Parameter
 — The start date of the usage data to retrieve format: date-time

usage-type (required)
 Query Parameter
 — The account package

Return type

ActualUsageDtoSwagger

Example data

Content-Type: application/json

```
{
  "INFRASTRUCTURE_ON_DEMAND" : {
```

```

"dataIntervalInMilliseconds" : 6,
"bucketList" : [ {
  "endDate" : "2000-01-23T04:56:07.000+00:00",
  "bucketValue" : 0.8008281904610115,
  "startDate" : "2000-01-23T04:56:07.000+00:00"
}, {
  "endDate" : "2000-01-23T04:56:07.000+00:00",
  "bucketValue" : 0.8008281904610115,
  "startDate" : "2000-01-23T04:56:07.000+00:00"
} ],
"dataUnit" : "dataUnit",
"usageType" : "INFRASTRUCTURE_ON_DEMAND"
}
}

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

The actual usage [ActualUsageDtoSwagger](#)

```
get /api/v1/billing-summary
```

Retrieve details per billing period (getBillingRecordsApi)

Retrieves usage details (purchased/used/overage) for each billing period in the specified time range. Note that for a sub account, the overages and purchasedQuantity fields return -1.

Query parameters

caid (required)

Query Parameter

— The account id format: int64

end (optional)

Query Parameter

— The end date of the required list. format: date-time

start (optional)

Query Parameter

— The start date of the required list. format: date-time

Return type

[array\[BillingDto\]](#)

Example data

Content-Type: application/json

```
[ {
  "billingRecords" : [ {
    "billingIssueDate" : "2000-01-23T04:56:07.000+00:00",
    "endDate" : "2000-01-23T04:56:07.000+00:00",
    "overages" : 5.962133916683182,
    "planName" : "planName",
    "purchasedQuantity" : 0.8008281904610115,
    "services" : [ {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    }, {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    } ],
    "planUsage" : 1.4658129805029452,
    "plan" : "ALWAYS_ON_BANDWIDTH",
    "dataUnit" : "dataUnit",
    "startDate" : "2000-01-23T04:56:07.000+00:00",
    "billingStatus" : "OPEN"
  }, {
    "billingIssueDate" : "2000-01-23T04:56:07.000+00:00",
    "endDate" : "2000-01-23T04:56:07.000+00:00",
    "overages" : 5.962133916683182,
    "planName" : "planName",
    "purchasedQuantity" : 0.8008281904610115,
    "services" : [ {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    }, {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    } ],
    "planUsage" : 1.4658129805029452,
    "plan" : "ALWAYS_ON_BANDWIDTH",
    "dataUnit" : "dataUnit",
    "startDate" : "2000-01-23T04:56:07.000+00:00",
    "billingStatus" : "OPEN"
  } ]
}
```

```

}, {
  "billingRecords" : [ {
    "billingIssueDate" : "2000-01-23T04:56:07.000+00:00",
    "endDate" : "2000-01-23T04:56:07.000+00:00",
    "overages" : 5.962133916683182,
    "planName" : "planName",
    "purchasedQuantity" : 0.8008281904610115,
    "services" : [ {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    }, {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    } ],
    "planUsage" : 1.4658129805029452,
    "plan" : "ALWAYS_ON_BANDWIDTH",
    "dataUnit" : "dataUnit",
    "startDate" : "2000-01-23T04:56:07.000+00:00",
    "billingStatus" : "OPEN"
  }, {
    "billingIssueDate" : "2000-01-23T04:56:07.000+00:00",
    "endDate" : "2000-01-23T04:56:07.000+00:00",
    "overages" : 5.962133916683182,
    "planName" : "planName",
    "purchasedQuantity" : 0.8008281904610115,
    "services" : [ {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    }, {
      "serviceUsage" : 6.027456183070403,
      "service" : "WEBSITE_PROTECTION",
      "serviceName" : "serviceName",
      "usageType" : {
        "dataUnit" : "dataUnit"
      }
    } ],
    "planUsage" : 1.4658129805029452,
    "plan" : "ALWAYS_ON_BANDWIDTH",
    "dataUnit" : "dataUnit",
    "startDate" : "2000-01-23T04:56:07.000+00:00",
    "billingStatus" : "OPEN"
  } ]
}
]

```

Produces

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- application/json

Responses

200

Legal response

Models

Methods

Table of Contents

- ActualUsageDto
- ActualUsageDtoSwagger
- BillingDto
- BillingRecordDto
- BucketDto
- MeasuredProduct
- ServiceUsageDetailsDto

ActualUsageDto

bucketList (optional)

array[BucketDto]

List of bandwidth usage in each bucket during the requested time frame.

dataIntervalMilliseconds (optional)

Long

The time length of the bucket. format: int64

usageType (optional)

String

Account bandwidth type.

Enum:

INFRASTRUCTURE_ON_DEMAND

INFRASTRUCTURE_ALWAYS_ON

WAF_ALWAYS_ON

dataUnit (optional)

String

The measurement unit of the data. For example, bps.

ActualUsageDtoSwagger

INFRASTRUCTURE_ON_DEMAND

ActualUsageDto

BillingDto

billingRecords (optional)

array[BillingRecordDto]

The billing records.

BillingRecordDto

billingIssueDate (optional)

Date

The date that the billing record was created. format: date-time

startDate (optional)

Date

The start date of the billing period. format: date-time

endDate (optional)

Date

The end date of the billing period. format: date-time

purchasedQuantity (optional)

Double

The quantity included with your plan. Returns -1 for a sub account. format: double

plan (optional)

String

The plan category.

Enum:

ALWAYS_ON_BANDWIDTH

INFRA_PROTECT_ALWAYS_ON_BANDWIDTH

INFRA_PROTECT_ON_DEMAND_BANDWIDTH

CONSUMPTION_BANDWIDTH

CONSUMPTION_SITES

ATO

planName (optional)

String

The product name.

services (optional)

array[ServiceUsageDetailsDto]

Information about the services.

planUsage (optional)

Double

The quantity of bandwidth that was used. format: double

overages (optional)

Double

The quantity that was used beyond the quantity allowed by your plan (purchasedQuantity). Returns -1 for a sub account. format: double

billingStatus (optional)

String

The status of the billing period. The value for the current billing period is OPEN and the value for previous billing periods is CLOSED.

Enum:

OPEN

VIEW_ONLY

CLOSED

dataUnit (optional)

String

The measurement unit of the data. For example, Mbps.

BucketDto

startDate (optional)

Date

The start date of the bucket. format: date-time

endDate (optional)

Date

The end date of the bucket. format: date-time

bucketValue (optional)

Double

Bandwidth usage for the bucket. format: double

MeasuredProduct

dataUnit

String

ServiceUsageDetailsDto

serviceUsage (optional)

Double

The quantity that was used for the service. format: double

service (optional)

String

The product service.

Enum:

WEBSITE_PROTECTION

INFRASTRUCTURE_PROTECTION

EDGE_IP

usageType (optional)

MeasuredProduct

serviceName (optional)

String

The service name.

On-Premises Security API

The following APIs are available for managing your Imperva configuration.

Web Application Firewall (WAF) API

This section links to the API Reference Guide for WAF-only releases.

- [v15.4 WAF API Reference Guide](#)
- [v15.3 WAF API Reference Guide](#)
- [v15.2 WAF API Reference Guide](#)
- [v15.1 WAF API Reference Guide](#)
- [v15.0 WAF API Reference Guide](#)
- [v14.7 WAF API Reference Guide](#)

Database Activity Monitoring (DAM) API

This section links to the API Reference Guide for DAM-only releases.

- [v14.19 DAM API Reference Guide](#)
- [v14.18 DAM API Reference Guide](#)
- [v14.17 DAM API Reference Guide](#)
- [v14.16 DAM API Reference Guide](#)
- [v14.15 DAM API Reference Guide](#)
- [v14.14 DAM API Reference Guide](#)
- [v14.13 DAM API Reference Guide](#)
- [v14.12 DAM API Reference Guide](#)
- [v14.11 DAM API Reference Guide](#)
- [v14.10 DAM API Reference Guide](#)
- [v14.9 DAM API Reference Guide](#)
- [v14.8 DAM API Reference Guide](#)
- [v14.7 DAM API Reference Guide](#)

Data Risk Analytics (DRA) API

- [Data Risk Analytics API v4.19](#)
- [Data Risk Analytics API v4.18](#)
- [Data Risk Analytics API v4.17](#)
- [Data Risk Analytics API v4.16](#)
- [Data Risk Analytics API v4.15](#)
- [Data Risk Analytics API v4.14](#)
- [Data Risk Analytics API v4.13](#)
- [Data Risk Analytics API v4.12](#)
- [Data Risk Analytics API v4.11](#)
- [Data Risk Analytics API v4.10](#)
- [Data Risk Analytics API v4.9](#)
- [Data Risk Analytics API v4.8](#)
- [Data Risk Analytics API v4.3](#)
- [Data Risk Analytics API v4.2](#)
- [Data Risk Analytics API v4.0](#)

Data Security Fabric (DSF) Hub API

- [Data Security Fabric API v15.2](#)
 - [Data Security Fabric API v15.1](#)
 - [Data Security Fabric API v15.0](#)
 - [Data Security Fabric API v4.19](#)
 - [Data Security Fabric API v4.18](#)
 - [Data Security Fabric API v4.17](#)
 - [Data Security Fabric API v4.16](#)
-

-
- Data Security Fabric API v4.15
 - Data Security Fabric API v4.14
 - Data Security Fabric API v4.13