paloalto TECHDOCS

AutoFocus® API Reference

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2017-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

August 30, 2023

Table of Contents

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

About the AutoFocus API

The AutoFocus™ API extends the ability to query the threat intelligence cloud through a programmatic, RESTful API. You can integrate this API into a third-party service, application, or script that accesses AutoFocus outside of the web portal. API responses are in JSON or XML-based STIX format.

AutoFocus API Overview

The AutoFocus API provides several AutoFocus API Resources to aid in the retrieval of threat intelligence.

Depending on the resource, your requests are either indirect (asynchronous) or direct (synchronous). When you Perform AutoFocus Searches for samples, sessions, or aggregate data, you first initiate a search and then make further requests to get the results of your search. For other resources, such as when you request session details and analysis reports, you Perform Direct Searches and immediately get corresponding data. The AutoFocus API uses either JSON, which returns JSON, or XML, which returns data in XML-based STIX format. Learn more about AutoFocus API STIX Support. Using the POST method for requests, you can do the following:

- Search for threat intelligence samples and sessions.
- View aggregate data, such as popular malware, applications, and source countries.
- View file analysis data related to a specified sample.
- Get tag lists, popular tags, and tag details.
- Export lists based on previously saved threat artifacts.

Potential uses of the AutoFocus API include:

- Automated feed extraction of threat analysis—Leverage the AutoFocus API to integrate key data into a third-party dashboard or service such as Splunk.
- Automated hash extraction for blocking attacks—Use the AutoFocus API to provide a layered approach to threat prevention. For example, your organization can use the AutoFocus API in conjunction with a firewall to look up sample hashes and block identified threats.
- Automated import of threat intelligence on your firewall—Use the AutoFocus API to look up hashes and corresponding tags to create custom block lists on your firewall.

To make requests, you must Get Your API Key, which you use to authenticate API calls. Each license uses one API key, regardless of the number of users.

To control the number of requests you can make, you need to observe AutoFocus API Rate Limits, which is a point system to track and rate limit API calls.

 ©2023 Palo Alto Networks, Inc.

AutoFocus API Prerequisites

The following prerequisites will help you fully leverage AutoFocus:

- Register your license.
- Get Your API Key.
- (Recommended) Familiarize yourself with the AutoFocus web portal. Read AutoFocus™ Administrator's Guide to get a better understanding of the AutoFocus web portal.
- (Recommended) Have a working knowledge of web service APIs, HTTP, JSON, and XML.
- (Recommended) If using the STIX API, familiarize yourself with STIX, MAEC, and CybOX.

 ©2023 Palo Alto Networks, Inc.

AutoFocus API Rate Limits

The AutoFocus API uses a point system to track and rate limit API calls. Rate limits are enforced based on the number of users attached to your license. Each request to the AutoFocus API expends a predetermined number of points depending on whether you are initiating a call, checking the results of that call, or calling an API that directly provides results. Refer to AutoFocus API Resources to see the point cost associated with each request. The AutoFocus API returns an error when you exceed the rate limit so you should learn How to Track Points. Refer to AutoFocus API Error Codes for more information.

- Rate Limits and Points Allotment
- How to Track Points
- Points Usage

Rate Limits and Points Allotment

The following table provides rate limits and point allotment.

Rate Limit Type	Description
Limit per Second	Each license can make 60 concurrent calls per second. After 60 concurrent calls, the AutoFocus API queues up to 200 additional calls. The API then processes 60 calls from the queue every second.
Limit per Minute	Each regular or unlimited license can use up to 200 points per minute.
Limit per Day	Each license can use up to 5,000 points per day. The daily points you are alloted depend on how many users are on your license. For example, if you have two users on your license, multiply the 5,000 point limit by two (5,000 x 2 = 10,000 point daily limit). Accounts with an **unlimited license** can use up to 100,000 points per day.

Users on the same license collectively share rate limits applicable to that license.

How to Track Points

The AutoFocus API features built-in tracking of point allotments. Each API response includes information within the `bucket_info` object or element, such as total points, points remaining, and point allotment start times:

```
{
  "minute_points":200,
  "daily_points":30000,
```

 ©2023 Palo Alto Networks, Inc.

```
  "minute_points_remaining":184,
  "daily_points_remaining":4578,
  "minute_bucket_start":"2015-09-02 10:55:33",
  "daily_bucket_start":"2015-09-01 17:08:40"
}
```

Parameter	Description
minute_points	Total number of points alloted per minute
daily_points	Total number of points alloted per day
minute_points_remaining	Remaining number of points per minute
daily_points_remaining	Remaining number of points per day
minute_bucket_start	Timestamp for when the current minute allotment started
daily_bucket_start	Timestamp for when the current daily allotment started

Points Usage

As mentioned in AutoFocus API Resources, most API calls have a point cost that applies to your daily point limit. For example, if you initiate a search query for malware samples, the point cost is 10 points. If you then view the results of this search, you expend 1 points each time you check for the latest set of results. Viewing the details of a particular sample costs 2 points. You can retrieve threat intelligence cards related to particular samples as part of your threat investigation and analysis without incurring a points charge.

If you have an AutoFocus license that allows 5,000 points per day, the following table illustrates how points can accumulate toward your daily point limit:

Request	Cost	Total Remaining Points
Initiate samples search	10 points	4,990
View results of samples search	1 point	4,989
View details of 500 samples	1,000 points (500 samples x 2 points)	3,989
View threat intelligence cards for 20 indicators	0 points	3,989

 ©2023 Palo Alto Networks, Inc.

AutoFocus API Resources

The AutoFocus API provides access to most of the same information that is available through the AutoFocus web portal.

Learn how to Get Started with the AutoFocus API and make your first AutoFocus API calls.

The base URI for all resources is the following, except when explicitly defined:

```
https://autofocus.paloaltonetworks.com/api/v1.0
```

Use the base URI when utilizing AutoFocus API resources:

- Resources for Initiating Searches
- Resources for Viewing Search Results
- Resources for Direct Searches

Resources for Initiating Searches

The following table describes resources available for initiating searches.

Resources for Initiating Searches	Format	Description	Point Cost
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search	JSON	Search signatures in which the signature / threat name meets the match condition you defined in the search query.	2
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search			
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/panav/search			
/samples/search/	JSON	Search samples in which samples meet the match condition you defined.	10
/stix/samples/search/	STIX		
/sessions/search/	JSON	Search for sessions in which samples meet the match conditions you defined.	10
/stix/sessions/search/	STIX		

 ©2023 Palo Alto Networks, Inc.

Resources for Initiating Searches	Format	Description	Point Cost
/sessions/histogram/search/	JSON	Search sessions for histogramdata. The results of this search correspond to the **Malware Download Sessions** data when you view search statistics.	10
/sessions/aggregate/search/	JSON	Initiate a session search for aggregatedata. The results of this search correspond to the aggregate data shown when you view search statistics such as **Top Firewalls, Top Malware**, **Source Countries**, and **Destination Countries**.	10
/top-tags/search/	JSON	Initiate a search for the most popular tags, also known as top tags. The results of this search correspond to the **Top Tags** data available when you view search statistics.	10

Resources for Viewing Search Results

The following table describes resources available for viewing search results.

Resources for Viewing Search Results	Format	Description	Point Cost
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search/result/{search_id}	JSON	View the current search results of the given `(search_id)`. This resource returns the latest results of: • `https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search` • `https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search` • `https://autofocus.paloaltonetworks.com/`	1
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search/result/{search_id}			
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/			

 ©2023 Palo Alto Networks, Inc.

Resources for Viewing Search Results	Format	Description	Point Cost
panav/search/result/{search_id}		`api/intel/v1/threatvault/panav/search`	
/samples/results/{af_cookie}	JSON	View the current search results of the given ID (`af_cookie`). This resource returns the latest results of `/samples/search/` or `/stix/samples/search/`.	1
/stix/samples/results/{af_cookie}	STIX		
/sessions/results/{af_cookie}	JSON	View the current session results of the given ID (`af_cookie`). This resource returns latest results of `/sessions/search/` or `/stix/sessions/search/`.	1
/stix/sessions/results/{af_cookie}	STIX		
/sessions/histogram/results/{af_cookie}	JSON	View the current histogram results of the given ID (`af_cookie`). This resource returns the latest results of `/sessions/histogram/search/`.	1
/sessions/aggregate/results/{af_cookie}	JSON	View the current aggregate session results of the given ID (`af_cookie`). This resource returns the latest results of `/sessions/aggregate/search/`.	1
/top-tags/results/{af_cookie}	JSON	View the current top tags results of the given ID (`af_cookie`). This resource returns the latest results of `/top-tags/search/`.	1

Resources for Direct Searches

The following table describes resources available for direct searches.

Resources for Direct Searches	Format	Description	Point Cost
https://autofocus.paloaltonetworks.com/api/intel/v1/ip/{ip_address}/geolocation	JSON	View geolocation details of a specified IP address	2

 ©2023 Palo Alto Networks, Inc.

Resources for Direct Searches	Format	Description	Point Cost
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/release/{release_id}	JSON	View anti-spyware, vulnerability, and file-format release info for a given release ID.	2
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/signature/{DNS_RTDNS_signature_id}	JSON	View DNS/RTDNS signature details for a given signature ID.	2
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/signature/{signature_id}	JSON	View anti-spyware, vulnerability, and file-format signature details for a given signature ID.	2
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/panav/signature/{antivirus_signature_id}	JSON	View antivirus signature details based on a specified signature ID or SHA256 hash.	2
https://autofocus.paloaltonetworks.com/api/intel/v1/file/{sha256}/signature			2
/session/{_id}	JSON	View details of a specified session.	2
/sample/{sample_id}/analysis/	JSON	View file analysis data related to a specified sample. The results correspond to the **File Analysis**tab shown when you click a sample hash on the search editor.	2
/stix/sample/{sample_id}/analysis/	STIX		
/tags/	JSON	View a list of all tags.	2
/stix/tags/	STIX		
/tag/{public_tag_name}	JSON	View tag details for the given public tag name.	2
/stix/tag/{public_tag_name}	STIX		
/export/	JSON	Export a list based on previously saved artifacts.	2

 ©2023 Palo Alto Networks, Inc.

Resources for Direct Searches	Format	Description	Point Cost
/output/threatFeedResult	JSON	View threat indicators added to the feed list in the past 24 hours.	0
/IOCFeed/{outputFeedId}/{outputFeedName}	JSON	View custom threat indicator feed details based on the feed type (URL or EDL custom feed) and authentication details associated with the feed.	0
EDL/IOCFeed/{outputFeedId}/{outputFeedName}			
/tic?indicatorType={indicator_type}&indicatorValue={value_of_indicator}&includeTags={true_or_false}'	JSON	View Threat Intelligence Card summary based on the indicator type and value (domains, URLs, file hash, or IP address).	0

 ©2023 Palo Alto Networks, Inc.

AutoFocus API STIX Support

In addition to API support for JSON, AutoFocus also provides responses in the form of STIX (Structured Threat Indicator eXpression). STIX is an easily consumable and standardized data model for cyber threat information expressed through structured XML.

STIX support through AutoFocus currently conforms to STIX 1.1.1. To effectively provide the volume of data available through AutoFocus, responses contain embedded MAEC (Malware Attribute Enumeration and Characterization) and CybOX (Cyber Observable eXpression) content. MAEC is especially suited for structured, detailed malware information, such as behaviors, static analysis, and dynamic analysis of malware. CybOX content captures observable events and properties of malware such as platforms where the malware is found and actions taken by the malware.

For example, when you Get Sample Analysis reports using the STIX API, the response shows a combination of STIX, MAEC, and CybOX content:

```
<!-- TRUNCATED RESPONSE -->
<stix>
  <stix:STIX_Package xmlns:DNSQueryObj="http://cybox.mitre.org/
objects#DNSQueryObject-2" xmlns:DNSRecordObj="http://cybox.mitre.org/
objects#DNSRecordObject-2" xmlns:FileObj="http://cybox.mitre.org/
objects#FileObject-2" xmlns:HTTPSessionObj="http://cybox.mitre.org/
objects#HTTPSessionObject-2" xmlns:ProcessObj="http://
cybox.mitre.org/objects#ProcessObject-2" xmlns:SystemObj="http://
cybox.mitre.org/objects#SystemObject-2" xmlns:URIObj="http://
cybox.mitre.org/objects#URIObject-2" xmlns:autofocus="https://
autofocus.paloaltonetworks.com" xmlns:cybox="http://cybox.mitre.org/
cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
 xmlns:maecBundle="http://maec.mitre.org/XMLSchema/
maec-bundle-4" xmlns:maecPackage="http://maec.mitre.org/
XMLSchema/maec-package-2" xmlns:stix="http://stix.mitre.org/
stix-1" xmlns:stix-maec="http://stix.mitre.org/extensions/
Malware#MAEC4.1-1" xmlns:stixCommon="http://stix.mitre.org/common-1"
 xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
 xmlns:ttp="http://stix.mitre.org/TTP-1" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" id="autofocus:Package-
eb6a086e-6dc4-4436-98ad-91faa7914e15" version="1.1.1"
 timestamp="2016-03-07T22:52:45.311237+00:00">
    <stix:TTPs>
    <stix:TTP id="autofocus:ttp-9c427415-4493-4a78-8c1f-172fb46ef0db"
 timestamp="2016-03-07T22:52:45.312313+00:00"
 xsi:type="ttp:TTPType">

 <ttp:Title>3d0d8c0e8b80ea89b6c360d0077ae2e6d08f654ad28d7c5da57adaf4593a333f</
ttp:Title>
      <ttp:Description>dynamic analysis for
 3d0d8c0e8b80ea89b6c360d0077ae2e6d08f654ad28d7c5da57adaf4593a333f</
ttp:Description>
      <ttp:Behavior>
      <ttp:Malware>
        <ttp:Malware_Instance xsi:type="stix-
maec:MAEC4.1InstanceType">
```

 ©2023 Palo Alto Networks, Inc.

```
        <stix-maec:MAEC id="autofocus:package-9c280586-46a1-4b9e-
bc31-cb2e4635fe3c" schema_version="2.1">
          <maecPackage:Malware_Subjects>
          <maecPackage:Malware_Subject id="autofocus:malware_subject-
fdd89da7-6202-45a7-9ccb-569e667088a7">
            <maecPackage:Malware_Instance_Object_Attributes
 id="autofocus:Object-227c3900-4976-414f-8587-1a8dc95c7a8e">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:Hashes>
              <cyboxCommon:Hash>
                <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
<cyboxCommon:Simple_Hash_Value>3d0d8c0e8b80ea89b6c360d0077ae2e6d08f654ad28d7c5d
cyboxCommon:Simple_Hash_Value>
              </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
<!-- TRUNCATED RESPONSE -->
```

STIX Elements and Fields

The following table lists STIX-enabled resources along with the corresponding STIX, MAEC, and CybOX elements visible in the response:

Resource	Element	Fields
Get Samples (Search Samples and Sessions)	cybox:Observables Observables are events or stateful properties such as the value of a registry key, deletion of a file, or the receipt of an HTTP GET.	cybox:Observable • cybox:Description • cybox:Object • cybox:Properties
Get Sessions (Search Samples and Sessions)	stix:Incident Incidents are discrete instances of observable patterns affecting an organization; it includes information discovered during an incident response investigation.	incident:Description incident:Victim incident:Related_Observables

 ©2023 Palo Alto Networks, Inc.

Resource	Element	Fields

Get Sample Analysis	ttp:MalwareType
	TTPs (Tactics, Techniques, and Procedures) represent adversarial behavior, such as potentially targeted victims, attack patterns and malware, leveraged resources (infrastructure, tools, personas).
		ttp:Title
		ttp:Description
		ttp:Behavior
		• ttp:Malware
		  • ttp:Malware_Instance
		  • maecPackage:MAEC_Package
		  • maecPackage:Malware_Subjects
		  - maecPackage:Malware_Subject

Get Tags	stix:Indicator Indicators convey specific observable patterns combined with contextual information. They represent artifacts and behaviors of interest.	indicator:Title indicator:Description indicator:Short_Description indicator:Sightings indicator:Producer • stixCommon:Description • stixCommon:Identity • stixCommon:Name
Get Tag Details	stix:Indicator	indicator:Title indicator:Description indicator:Short_Description indicator:Composite_Indicator_Expression • indicator:Indicator indicator:Sightings indicator:Producer

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Get Started with the AutoFocus API

To use the AutoFocus API™, first get your API key through the Palo Alto Networks Customer Service Portal. You can then use your API key to test a simple API call.

To use the AutoFocus API with Python, refer to the pan-python page on GitHub, which provides a Python and command line interface for AutoFocus. View the corresponding Python syntax for initiating searches for samples, sessions, and aggregate data. You can also use the AutoFocus Python library, which provides an object-oriented interface into AutoFocus.

- Get Your API Key
- Make Your First AutoFocus API Calls

Get Your API Key

Use the following procedure to get your API key.

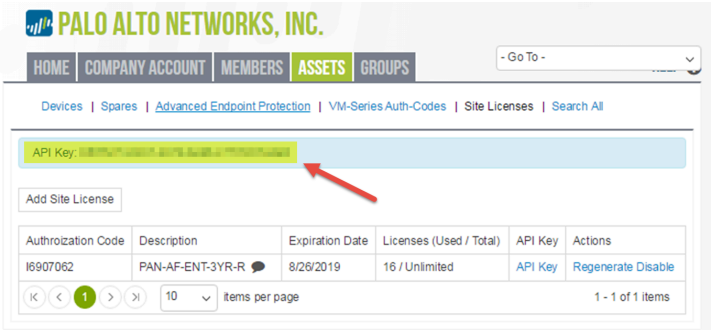
STEP 1 | Log in to the Customer Support Portal and add your authorization code.

1. Visit https://support.paloaltonetworks.com.
2. Select the **Assets** > **Site Licenses** tab.
3. Select **Add Site License**.
4. Enter the authorization code.

STEP 2 | Activate the API.

1. Select the **Enable** action in **Site Licenses**.
2. Select the **API Key** link.

   The API key appears onscreen as shown below. Use this API key for all AutoFocus API requests.



*After you activate your API key on the Customer Support Portal, you can also view related information **Settings** within the AutoFocus web portal, including API key, API key status, the number of license users, points usage, and total available points.*

 ©2023 Palo Alto Networks, Inc.

Make Your First AutoFocus API Calls

After you Get Your API Key, use that API key to make your first calls to the AutoFocus API. Many of the resources in the AutoFocus API require API calls to two resources. The first call is to initiate a search and the next call is to check for the results of that search.

View the corresponding cURLrequest or Python syntax *for initiating searches for samples, sessions, and aggregate data from the AutoFocus web portal.*

Start a Search

In this call, we will start a search for the first 50 samples that WildFire™ has determined are malware.

In your cURL request, specify a POST request using JSON as your content type:

```
curl -X POST https://autofocus.paloaltonetworks.com/api/v1.0/samples/
search/ \
-H "Content-Type: application/json" \
-d '{
  "apiKey": "apikey",
  "query": {
    "operator": "all",
    "children": [
      {
        "field": "sample.malware",
        "operator": "is",
        "value": 1
      }
    ]
  },
  "size": 50,
  "from": 0,
  "sort": {
    "create_date": {
      "order": "desc"
    }
  },
  "scope": "public"
}'
```

In response to your initial request, the API returns the following JSON, which contains a search ID (also known as an `af_cookie`):

```
{
  "in_progress":true,
  "af_cookie":"870218db-27cd-4614-ac36-1d87f3f0016e+0",
  "bucket_info":{
    "minute_points":200,
    "daily_points":25000,
    "minute_points_remaining":190,
    "daily_points_remaining":24114,
```

 ©2023 Palo Alto Networks, Inc.

```
    "minute_bucket_start":"2015-09-04 18:51:39",
    "daily_bucket_start":"2015-09-04 13:58:42"
  }
}
```

View Results

To view the results of your search, include the search ID (`af_cookie`) at the end of the resource URI and include the API key in the JSON body of the request:

```
curl -X POST https://autofocus.paloaltonetworks.com/api/v1.0/samples/
results/870218db-27cd-4614-ac36-1d87f3f0016e+0 \
-H "Content-Type: application/json" \
-d '{
   "apiKey": "apikey"
}'
```

The response to the above request includes 50 samples from the total number flagged as malware. In this example (truncated to the first two results), the total number of results possible is shown as `"total": 32811214`:

```
{
  "total": 32811214,
  "hits": [
{
      "_id":
 "c8fac378e1af77b7e0b7025ceaa1edcdd402bee53a7200a38f0c3878b5bc9309",
      "_source": {
        "app_packagename": "com.ooedsqz.ihma.fwfl",
        "ssdeep": "12288:/wxZYgTlF0oikgCTp58auFJMV2XzoZWnuV/YBH:/
wxS8FvilK3YFJKAupO",
        "create_date": "2016-10-14T10:21:25",
        "sha256":
 "c8fac378e1af77b7e0b7025ceaa1edcdd402bee53a7200a38f0c3878b5bc9309",
        "md5": "1400058f42f283e9c25e15d6bf28266c",
        "filetype": "Android APK",
        "sha1": "6961b6eadc2b577d10597cd45ce9a83d84f39a8e",
        "app_name": "com.system.ojjnippitr",
        "malware": 1,
        "finish_date": "2016-10-14T10:26:18",
        "size": 437266,
        "region": [
          "us"
        ]
      },
      "visible": true
    },
    {
      "_id":
 "b183f65d3372f4f15c5ee56f38f0f782f7003dfb932b0166b765621519930cae",
      "_source": {
        "app_packagename": "iucCaZa.YfaW.dStoaET",
        "create_date": "2016-10-14T10:21:18",
        "sha256":
 "b183f65d3372f4f15c5ee56f38f0f782f7003dfb932b0166b765621519930cae",
```

 ©2023 Palo Alto Networks, Inc.

```
        "ssdeep":
 "98304:QJXWrEEhBYPdandOUFJlHczs5DSamn89jRYVb:QJGgEXR3lKqDe8fYB",
        "md5": "75c2faffadd22485c8b7e98c9cd2f963",
        "filetype": "Android APK",
        "sha1": "a3d280dcb3b2e743acb70bfe8c59fe86c7793da6",
        "app_name": "KYO",
        "finish_date": "2016-10-14T10:26:12",
        "malware": 1,
        "size": 3523310,
        "tag": [],
        "region": [
          "us"
        ]
// TRUNCATED
],
  "took": 4744,
  "af_message": "complete",
  "af_in_progress": false,
  "af_complete_percentage": 100,
  "af_cookie": "53185127-3668-4d7d-85aa-61ef17e8158f+0",
  "bucket_info": {
    "minute_points": 200,
    "daily_points": 25000,
    "minute_points_remaining": 189,
    "daily_points_remaining": 24941,
    "minute_bucket_start": "2015-09-12 23:42:42",
    "daily_bucket_start": "2015-09-12 14:47:43"
  }
}
```


The `af_cookie` expires 120 seconds after search results are complete (when `af_complete_percentage` is 100 and `af_in_progress` is `false`). Until then, you can continually make requests to view results. After you view a complete list of results, the `af_cookie` expires.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Perform AutoFocus Searches

With some core AutoFocus™ API searches, you must retrieve information using the two-step process used to Make Your First AutoFocus API Calls. First send the initial search request, and then view the results of that search through a second API call. This asynchronous process allows you to view partial results while waiting for the complete results of the search.

With the asynchronous searches discussed in this chapter, you may need to make multiple calls to view the completed search or to see the latest search results while the search is in progress.

- Search Samples and Sessions
- Search Field Names
- Search Parameter Types and Operators
- Search Countries and Country Codes
- Search Top Tags, Session Histogram, and Session Aggregate Data
- Search for Signatures
- View Search Results

Search Samples and Sessions

Use the `/samples/search` and `/sessions/search` resources to search through samples and sessions, respectively. The sample search mimics the search functionality available through the AutoFocus web portal and provides corresponding data, such as WildFire™ verdict, SHA1 hash, file size, and file type. The session search also corresponds to information available through the **Sessions** tab when you perform a search in the AutoFocus web portal.

- Resources
- Request Parameters
- Search Top Tags, Session Histogram, and Session Aggregate Data
- STIX Sample

Resources

```
/samples/search/
/sessions/search/
/stix/samples/search/
/stix/sessions/search/
```

Request Parameters

Request parameters are case-sensitive.

- Request Body Parameters
- Search Field Names
- Search Parameter Types and Operators
- Search Countries and Country Codes

JSON Sample

- Request
- Response

View the corresponding cURLrequestor Python syntax *for initiating searches for samples, sessions, and aggregate data from the AutoFocus web portal.*

Request

The following request body searches for malware that originates from Algeria. It restricts the results to 50 private samples (samples within an organization) and sorts them in descending order based on when the sample was last updated.

```
curl -X POST https://autofocus.paloaltonetworks.com/api/v1.0/samples/
search/
-H "Content-Type: application/json"
-d '{
```

 ©2023 Palo Alto Networks, Inc.

```
  "apiKey":"apikey",
  "query":{
    "operator":"all",
    "children":[
      {
        "field":"session.src_country",
        "operator":"is",
        "value":"Algeria"
      }
    ]
  },
  "size":50,
  "from":0,
  "sort":{
    "update_date":{
      "order":"desc"
    }
  },
  "scope":"private"
}'
```

Response

Use the `af_cookie` parameter to view the results of your search.

```
{
  "af_in_progress": true,
  "af_first_result_af_took": 0,
  "in_progress": true,
  "af_cookie": "0-39173c38-b7bd-4c4b-93ec-6e403a35d0ac+0",
  "af_complete_percentage": 0,
  "bucket_info": {
    "minute_points": 200,
    "daily_points": 25000,
    "minute_points_remaining": 190,
    "daily_points_remaining": 24936,
    "minute_bucket_start": "2015-10-21 15:48:14",
    "daily_bucket_start": "2015-10-21 14:41:07"
  }
}
```

STIX Sample

- Request
- Response

 ©2023 Palo Alto Networks, Inc.

Request

The following request body searches for malware that originates from Algeria. It restricts the results to 50 private samples (samples within an organization) and sorts them in descending order based on when the sample was last updated.

```
curl -X POST https://autofocus.paloaltonetworks.com/api/v1.0/stix/
samples/search
-H "Content-Type: application/xml"
-d '
<req>
   <apiKey>apikey</apiKey>
   <query>
      <operator>all</operator>
      <children>
         <item>
            <field>session.src_country</field>
            <operator>is</operator>
            <value>Algeria</value>
         </item>
      </children>
   </query>
   <size>50</size>
   <from>0</from>
   <sort>
      <update_date>
         <order>desc</order>
      </update_date>
   </sort>
   <scope>private</scope>
</req>'
```

Response

Use the `af_cookie` parameter to view the results of your search.

```
<res>
    <af_in_progress>true</af_in_progress>
    <af_first_result_af_took>0</af_first_result_af_took>
    <af_cookie>0-3b0a6076-47fa-4e6f-9b83-6fe3aa8f7079+2</af_cookie>
    <af_complete_percentage>0</af_complete_percentage>
    <bucket_info>
        <minute_points>200</minute_points>
        <daily_points>25000</daily_points>
        <minute_points_remaining>190</minute_points_remaining>
        <daily_points_remaining>24980</daily_points_remaining>
        <minute_bucket_start>2016-02-24 16:17:54</
minute_bucket_start>
        <daily_bucket_start>2016-02-24 16:11:28</daily_bucket_start>
    </bucket_info>
</res>
```

Request Body Parameters

Use the following request body parameters when searching samples or sessions:

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
scope	(**Required**) Scope of the search. Only available and required for: `/samples/search/`.	string enumeration	Possible values: **private, public, global**
size	Number of results to provide.	number	Possible values: Range is 1-4000; however, `size` and `from` parameter values combined cannot exceed 4,000 total. Default value: 50
from	Sample number from which to start.	number	The number when adding the `size` and **from** parameters cannot exceed 4000. Default value: 0
sort	Sort based on the provided artifact. You can display sort results in ascending or descending order.	object	Possible values for sorting: `app_name, app_packagename, filetype, size, finish_date, create_date, update_date, md5, sha1, sha256, ssdeep`Possible values for `/sessions/search`:`app, device_country, device_countrycode, device_hostname, device_serial, vsys, dst_country, dst_countrycode, dst_ip, dst_port, emailsbjcharset, device_industry, src_country,`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			`src_countrycode, src_ip, src_port, sha256, tstamp, upload_src`Possible values for order:**`asc, desc`** Example: `"sort": { "filetype": { "order": "desc" }`
`type`	By default, when you perform a search, AutoFocus displays all search results, up to 4,000, as they accumulate until the search is complete. If you set `type` to `scan`, you can get up to 200,000 search results through pagination. Each time you view results, AutoFocus responds with the next page of results until the search is complete. By default, a page displays 50 results, and you can use the `size` parameter to set the number of results on each page. The **`scan`** value is currently the only possible value. For `type=scan`, the `from` and `sort` parameters are not available. Only available for these JSON resources: `/samples/search/` and `/sessions/search/`.	object	Possible values: **`scan`** Example: `{ "apiKey":"apikey", "query": { "operator":"all", "children": [ { "field":"sample.malware", "operator":"is", "value":1 } ] }, "size":10, "type": "scan", "scope":"public" }`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
`query`	Query based on conditions specified within this object.	object	See Search Field Names and Search Parameter Types and Operators for a list of available fields, operators, and acceptable values. *To easily determine your `query`, first run the equivalent search in the AutoFocus web portal and then use the **API Search** button to view the corresponding JSON.* 
`field`	Child parameter of `query`	string enumeration	See Search Field Names for a list of available fields.
`operator`	Child parameter of `query`	string enumeration	Possible values depend on the specified field. See Search Parameter Types and Operators for a list of available operators. When you have more than one search or child search condition, you must specify an additional operator parameter to specify whether to match `all` or `any` of the search conditions. Possible values are: **`all, any`** For example, the following JSON searches for malware that is either an Adobe Flash file or and Android API: `{ "operator":"all", "children": [ { "field":"sample.malware", "operator":"is", "value":1 }, { "operator":"any",`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			`"children": [ { "field":"sample.filetype", "operator":"is", "value":"Adobe Flash File" }, { "field":"sample.filetype", "operator":"is", "value":"Android APK" } ] } ] }`
`value`	Child parameter of `query`	Type varies depending on the selected `field` and `operator`.	Possible values depending on the selected `field` and `operator` values. Use the **Export Search** button in the AutoFocus web portal to get the corresponding `value` for any search.

 ©2023 Palo Alto Networks, Inc.

Search Field Names

When you Search Samples and Sessions, the following `field` names for artifacts are available to use within the `query` object. They correspond to the Artifact Types available in the AutoFocus web portal.

- General Artifacts
- Sample Artifacts
- Session Artifacts
- Analysis Artifacts
- Linux Artifacts
- Windows Artifacts
- Mac Artifacts
- Android Artifacts
- Macro Artifacts

Read Artifact Types in the AutoFocus Administrator's Guide for detailed descriptions of each artifact type.

General Artifacts

The following table provides field names and related information for general artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`alias.domain`	Domain	domain	Domain seen within DNS Activity, HTTP Activity, or File URL.
`alias.email`	Email Address	alias	Email address seen within email recipient address or email sender address.
`alias.filename`	Filename	alias	Valid filename as detected within a session or File Activity field.
`alias.hash`	Hash	alias	Valid SHA256, SHA1, or MD5 hash Example:

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			eb4559d2debb5de11b3a9053
alias.ip_address	IP Address	alias	A IP address as it appears in connection activity, DNS activity, or HTTP activity.
sample.tag	Tag	tagList	Valid AutoFocus tag. Example: **Parite**
sample.tag_alias	Tag Alias	typeAheadSelect	Valid AutoFocus tag alias. Example: **CryptoHost**
sample.tag_class	Tag Class	simpleSelect	Actor: **actor** Campaign: **campaign** Malware Family: **family** Exploit: **exploit** Malicious Behavior: **malicious_behavior**
sample.tag_group	Tag Group	simpleSelect	Valid AutoFocus tag group. Example: **Ransomware**
sample.tag_scope	Tag Scope	simpleSelect	Private: **private** Public: **public** Information: **commodity** Unit 42: **unit42**
sample.tag_source	Tag Source	simpleSelect	Valid tag source. Example: **Unit 42**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.threat_name`	Threat Name	typeAheadSelect	Valid threat name. Example: **`TDSS/Win32.fey.a`**
`alias.url`	URL	url	Valid File URL or URL as detected in HTTP activity.
`alias.user_agent`	User Agent	alias	Valid browser user agent as detected in HTTP Activity or User Agent Fragments.

Sample Artifacts

The following table provides field names and related information for sample artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.digital_signer`	Digital Signer	string	Valid digital signature.
`sample.filetype`	File Type	select	• **`7zip Archive`** • **`Adobe Flash File`** • **`Android APK`** • **`Android DEX`** • **`DLL`** • **`DLL64`** • **`ELF`** • **`JAVA Class`** • **`JAVA JAR`** • **`JScript`** • **`Link`** • **`Mac OS X app bundle in ZIP archive`**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			• **Mac OS X app installer** • **MacOSX DMG** • **Mach-O** • **Macro** • **Microsoft Excel 97 - 2003 Document** • **Microsoft Excel Document** • **Microsoft PowerPoint 97 - 2003 Document** • **Microsoft PowerPoint Document** • **Microsoft Word 97 - 2003 Document** • **Microsoft Word Document** • **PDF** • **PE** • **PE64** • **PowerShell** • **RAR Archive** • **RTF** • **Shell Script** • **VBScript**
`sample.size`	File Size	number	Sample size in bytes.
`sample.finish_date`	Finish Date	date	Timestamp of initial WildFire verdict. Example: **2015-09-21T11:33:20**
`sample.create_date`	First Seen	date	Timestamp when sample was first uploaded to WildFire.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.imphash`	Import Table Hash	exactStringList	Import hash Example: **`099c0646ea7282d232219f8807883be0`**
`sample.update_date`	Last Updated	date	Sample update date timestamp.
`sample.md5`	MD5	exactStringList	MD5 hash. Example: **`d0b811f1fa5a3f63f337513c41cdf368`**
`sample.sha1`	SHA1	exactStringList	SHA1 hash. Example: **`91ee460785ba550cf24adf06265efb7f24`**
`sample.sha256`	SHA256	exactStringList	SHA256 hash. Example: **`54cf20480c0fbefc9c35b3413c2930a5e1`**
`sample.ssdeep`	Ssdeep Fuzzy Hash	string	ssdeep hash value. Example: **`768:/1cVhpQI2EQK0iPDh84nScF15GYbWj`** **`Ajrq0Hgrik5`**
`sample.malware`	WildFire Verdict	select	Possible values: Benign: **`0`** Malware: **`1`** Grayware: **`2`**
`sample.tasks.metadata_compilation_ts`	Compilation Timestamp	date	Timestamp when a PE sample was created. Example: **`2018-09-21T10:21:12`**

Session Artifacts

The following table provides field names and related information for session artifacts.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`session.app`	Application	select	Refer to Application Research Center for application names.
`session.device_country`	Device Country	select	Refer to Search Countries and Country Codes for valid values.
`session.device_countrycode`	Device Country Code	select	Refer to Search Countries and Country Codes for valid values.
`session.device_hostname`	Device Hostname	exactString	Valid device hostname.
`session.device_serial`	Observed In	exactStringList	Valid device identifier.
`session.vsys`	Device vsys	exactString	Example: **`1`**
`session.dst_country`	Destination Country	select	Refer to Search Countries and Country Codes for valid values.
`session.dst_countrycode`	Destination Country Code	select	Refer to Search Countries and Country Codes for valid values.
`session.dst_ip`	Destination IP	exactStringList	Valid IP address..
`session.dst_port`	Destination Port	number	Valid port number.
`session.emailrecipient`	Email Recipient Address	string	Valid email address.
`session.emailsbjcharset`	Email Charset	exactString	Example: **`koi8-r`**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`session.emailsender`	Email Sender Address	string	Valid email address.
`session.emailsubject`	Email Subject	string	Valid email subject.
`session.filename`	File Name	string	Valid file name.
`session.fileurl`	File URL	url	Valid URL.
`session.imei`	IMEI	exactStringList	IMEI (International Mobile Equipment Identity) of the mobile device
`session.device_industry`	Industry	select	• **`Aerospace and Defense`** • **`Agriculture`** • **`Automotive`** • **`Construction`** • **`Consulting`** • **`Education`** • **`Education - K thru 12`** • **`Energy`** • **`Finance`** • **`Government`** • **`Healthcare`** • **`High Tech`** • **`Higher Education`** • **`Hospitality`** • **`Insurance`** • **`Lower Education`**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			• **Manufacturing** • **Media and Entertainment** • **Non-Profit** • **Other** • **Pharma and Life Sciences** • **Professional and Legal Services** • **Real Estate** • **Service Provider** • **Telecommunications** • **Transportation and Logistics** • **Utilities** • **Waste Management** • **Wholesale and Retail**
`session.user_id`	Recipient User ID	string	Valid user ID.
`session.region`	Region	singleSelect	Possible values: Wildfire global cloud: **us** Wildfire EU cloud: **eu** Wildfire Japan cloud: **jp** Wildfire Singapore cloud: **sg** Wildfire UK cloud: **uk**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			Wildfire Canada cloud: **ca**
session.src_country	Source Country	select	Refer to Search Countries and Country Codes for valid values.
session.src_countrycode	Source Country Code	select	Refer to Search Countries and Country Codes for valid values.
session.src_ip	Source IP	exactStringList	Valid IP address
session.src_port	Source Port	number	Valid port number
session.sha256	SHA256	exactStringList	Valid SHA256 hash
session.status	Status	singleSelect	Possible value: **Blocked**
session.tstamp	Time	date	Valid timestamp Example: **2015-09-21T11:33:20**
session.upload_src	Upload Source	exactStringList	Possible values: • **Firewall** • **Proofpoint** • **Traps** • **Magnifier** • **Manual API** • **Traps Android** • **WF Appliance** • **Prisma SaaS** • **Prisma Access** • **Cortex XDR**

 ©2023 Palo Alto Networks, Inc.

Analysis Artifacts

The following table provides field names and related information for analysis artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.tasks.connection`	Connection Activity	StringProx	Network activity including connections, IP addresses, and country codes. Example: **`tcp-connection, 46.254.18.90:80 , , RU`**
`sample.tasks.dns`	DNS Activity	StringProx	DNS activity including query, response, and type. Example: **`a0ce.akamaiedge.net`**
`sample.tasks.file`	File Activity	StringProx	Parent process, action, and file path. Example: **`Program Files\Zona \utils.jar,`**
`sample.tasks.http`	HTTP Activity	StringProx	HTTP request including host, method, URL, and user agent string. Example: **`/T/a93E_X.jpeg`**
`sample.tasks.metadata_sections`	PE Metadata	StringProx	Metadata from PE files, including the name, virtual

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			address, virtual size, and raw size. Example: **.text , 15872 , 4096 , 15866**
sample.tasks.japi	Java API Activity	StringProx	Java runtime activity. Example: **load, class barcode.Get2D not found.**
sample.tasks.behavior_type	Observed Behavior	StringProx	Behaviors seen when a sample is analyzed by WildFire. Example: **pe_sa_abnl_sect_name**
sample.tasks.misc	Other API Behavior	StringProx	Non-Java API activity seen when a sample is analyzed by WildFire. Example: **sample.exe , ZwProtectVirtualMemoryFa 0xc0000045 , 0xffffffff , pid=1516 , 0x0012fed8 , 0x0012fedc , 0x00000000**
sample.tasks.process	Process Activity	StringProx	Processes that showed activity when the sample

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			was analyzed by WildFire. Example: **cmd.exe , terminated , , Users\ \Administratorexplorer.exe"**
sample.tasks.service	Service Activity	StringProx	Services that showed activity when the sample was analyzed by WildFire. Example: **WINWORD.EXE , StartService , ,**
sample.tasks.user_agent	User Agent Fragments	StringProx	The user agent header for HTTP requests sent when the sample was analyzed by Wildfire. Example: **Microsoft-CryptoAPI/6.1**

Linux Artifacts

The following table provides field names and related information for Linux artifacts.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.tasks.elf_suspicious_behavior`	Linux Suspicious Behavior	StringProx	Suspicious behavior from an Linux file based on static analysis. Example: **`sample contains hard-coded malicious IP address`**
`sample.tasks.elf_functions`	Linux Functions	StringProx	Function contained in the Linux file. Example: **`__libc_sigaction`**
`sample.tasks.elf_commands`	Linux Commands	StringProx	Command contained in the Linux file. Example: **`rm -rf /var/log/wtmp`**
`sample.tasks.elf_file_paths`	Linux File Paths	StringProx	File path contained in an Linux file. Example: **`/var/run`**
`sample.tasks.elf_ip_address`	Linux IP Address	StringProx	An IP address detected during Linux sample analysis.
`sample.tasks.elf_domains`	Linux Domains	StringProx	Domain detected during Linux sample analysis. Example: **`run.work.`**
`sample.tasks.elf_url`	Linux URLs	StringProx	URL detected during Linux sample analysis. Example:

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			http://208.67.1.59/bins.sh.
sample.tasks.elf_command_action	Linux Command Action	StringProx	Command actions embedded into Linux sample file. Example: **/usr/bin/pusjcgkdgq gnome-terminal 739**
sample.tasks.elf_file_activity	Linux File Activity	StringProx	Files that showed activity as a result of the sample being executed in the WildFire analysis environment. Artifacts listed for each file activity include the parent process that showed activity, the action the parent process performed, and the file that was altered (created, modified, duplicated, or deleted). Example: **unlink , /usr/bin/pusjcgkdgq**
sample.tasks.elf_suspicious_action	Linux Suspicious Action	StringProx	An action that the Linux file performed with it was executed in the WildFire analysis environment. Example: **Sample accesses network information or**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			configuration , /proc/net/tcp

Windows Artifacts

The following table provides field names and related information for Windows-specific artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
sample.tasks.mutex	Mutex Activity	StringProx	Mutual exclusion object. Example: **CreateMutexW , WininetConnectionMutex**
sample.tasks.registry	Registry Activity	StringProx	Windows Registry activity. Example: **SetValueKey**

Mac Artifacts

The following table provides field names and related information for Mac-specific artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
sample.tasks.mac_embedded_url	Mac Embedded URL	StringProx	Internal files in a Mac app installer or a Mac app bundle. Example: **http://www.jamfsoftware.com/JAMFMessage**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.tasks.mac_embedded_file`	Mac Embedded File	StringProx	Files and files path to files found within a Mac-compatible file. Example: **parent_sha256=533ae13e2c9bc56b parent_path=Installer.app , sha1=bcf1a268c44b4028f4f00e119 name=ffExtFolder.zip , format=zip , path=Contents/ Resources/ ffExtFolder.zip , sha256=eca8f24eb58d30235a693d1 parent_sha1=38c7005b84b0cb1a37 size=14636**

Android Artifacts

The following table provides field names and related information for Android-specific artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.tasks.apk_app_icon`	APK App Icon	StringProx	Android application icon file path. Example: **res/drawable-hdpi/logo.png**
`sample.tasks.apk_app_name`	APK App Name	StringProx	Android application name. Example: **ElfBrowser**
`sample.tasks.apk_certificate_id`	APK Certificate	StringProx	Valid APK certificate ID.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			Example: **D3E9E50DB0AB284EA7F667B6**
`sample.tasks.apk_cert_file`	APK Certificate File	StringProx	File path to the certificate file, which contains owner and issuer information along with hashes used to sign the certificate. Example: **certificate , META-INF/ PDGVPCK.RSA , owner=CN=pktool, OU=maizi, O=maizi, L=sc, ST=sc,C=CN , issuer=CN=pktool, OU=maizi, O=maizi, L=sc, ST=sc, C=CN , md5=D3E9E50DB0AB284EA7F6 sha1=F483B0AF7786123B549 sha256=6AE89219FC5F8E739**
`sample.tasks.apk_defined_activity`	APK Defined Activity	StringProx	The class name of activities defined in the APK file. Example: **com.google.android.apps.**
`sample.tasks.apk_defined_intent_filter`	APK Defined Intent Filter	StringProx	Expression in an app's manifest file that specifies the type of intents that the component would like to receive. Example:

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			com.google.android.apps.
sample.tasks.apk_defined_receiver	APK Defined Receiver	StringProx	Example: **com.android.kvis.MyRecei**
sample.tasks.apk_defined_sensor	APK Defined Sensor	StringProx	Required sensor readings within an app. Example: **Receivesensor readings from gps**
sample.tasks.apk_defined_service	APK Defined Service	StringProx	Background services used within an APK. Example: **com.canvasmpedometer.Ped**
sample.tasks.apk_embedded_library	APK Embedded Libraries	StringProx	Third-party libraries that are included in the APK file. Example: **"AndroidInternal (Generic Library)"**
sample.tasks.apk_embeded_url	APK Embedded URL	StringProx	URL and originating file path within an APK. Example: **https:// akick.com , classes.dex/ com/koncept/ akick/ MainAdditionals $1.smali**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
`sample.tasks.apk_internal_file`	APK Internal File	StringProx	Path to a file within an Android APK. Example: **`res/menu/sms_activity.xml`**
`sample.tasks.apk_packagename`	APK Package Name	StringProx	Unique app name used by APK on device. Example: **`com.yojorico.photogallery`**
`sample.tasks.apk_isrepackaged`	APK Repackaged	StringProx	Possible values: **`False True`**
`sample.tasks.apk_requested_permission`	APK Requested Permission	StringProx	Example: **`android.permission.WRITE_`** Refer to the Android API Reference for permission values.
`sample.tasks.apk_sensitive_api_call`	APK Sensitive API Call	StringProx	API calls embedded in the APK file that access restricted services or resources. Example: **`java/lang/Runtime;->exec`**
`sample.tasks.apk_digital_signer`	APK Signer	StringProx	Personal information used by owner to sign a certificate. Example:

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			"CN=Android Debug,O=Android, C=US"
sample.tasks.apk_suspicious_api_call	APK Suspicious API Call	StringProx	API calls embedded in the APK file that access restricted services or resources. Example: **java/lang/Runtime;->exec, /smali/smali/com/android/kvis/b/L.smali**
sample.tasks.apk_suspicious_action	APK Monitored Suspicious Action	StringProx	Suspicious action from an APK file based on dynamic analysis. Example: **Attempted to create a file**
sample.tasks.apk_suspicious_file	APK Suspicious File	StringProx	A malicious file and filetype. Example: **/smali/lib/armeabi/libjackpal-androidterm4.so , ELF**
sample.tasks.apk_suspicious_string	APK Suspicious String	StringProx	A string in code that indicates suspicious behavior. Example: **pminstall , /smali/smali/**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			com/qq/RTUtils.smali
sample.tasks.apk_version_num	APK Version	StringProx	Application version number. Example: **1.0**
sample.tasks.apk_suspicious_behavior	APK Suspicious Behavior	StringProx	Suspicious behavior from an APK file based on static analysis. Example: **APK file can send an SMS message**
sample.tasks.apk_suspicious_pattern	APK Suspicious Pattern	StringProx	Suspicious pattern from an APK file based on static analysis. Example: **APK file listens to the phone state**

Macro Artifacts

The following table provides field names and related information for Macro artifacts.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
sample.tasks.macro	Macros	StringProx	The SHA256 and WildFire verdict of macros contained within a sample.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			Example: `b138e74f3db2bad973af2a4d1dbc97aff9599d748800e66799b2b61bc499bc07 , 1 , Malware`

 ©2023 Palo Alto Networks, Inc.

Search Parameter Types and Operators

The following table lists the parameter types and corresponding operators for Search Field Names:

Parameter Type	Available Operators
alias	**contains, does not contain**
bool	**is true, is false, has no value, has any value**
date	**is in the range, is after, is before, is, has no value, has any value**
exactString	**is, is not, has no value, has any value**
exactStringList	**is, is not, is in the list, is not in the list, has no value, has any value**
ipAddress	**is, is not, is in the range, has no value, has any value**
number	**is, is not, is in the range, greater than, greater than or equal, less than, less than or equal, has no value, has any value**
select	**is, is not, is in the list, is not in the list, has no value, has any value**
simpleStringList	**is, is not, is in the list, is not in the list**
singleSelect	**is, is not**
string	**contains, does not contain, has no value, has any value**
stringList	**contains, does not contain, is in the list, is not in the list, has no value, has any value**
stringProx	**contains, does not contain, has no value, has any value, proximity**
tagList	**is in the list, is not in the list, has no value, has any value**
typeAheadSelect	**is, is not, is in the list, is not in the list**

 ©2023 Palo Alto Networks, Inc.

Search Countries and Country Codes

The AutoFocus API allows you to search through samples and sessions using countries and country codes. The following tables lists the available countries and country codes that you can use for search queries:

Country Name	Country Code
Afghanistan	**AF**
Albania	**AL**
Algeria	**DZ**
American Samoa	**AS**
Andorra	**AD**
Angola	**AO**
Anguilla	**AI**
Antarctica	**AQ**
Antigua And Barbuda	**AG**
Argentina	**AR**
Armenia	**AM**
Aruba	**AW**
Asia Pacific Region	**AP**
Australia	**AU**
Austria	**AT**
Azerbaijan	**AZ**
Bahamas	**BS**
Bahrain	**BH**
Bangladesh	**BD**
Barbados	**BB**

©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Belarus	**BY**
Belgium	**BE**
Belize	**BZ**
Benin	**BJ**
Bermuda	**BM**
Bhutan	**BT**
Bolivia Plurinational State Of	**BO**
Bonaire Saint Eustatius And Saba	**BQ**
Bosnia And Herzegovina	**BA**
Botswana	**BW**
Bouvet Island	**BV**
Brazil	**BR**
British Indian Ocean Territory	**IO**
Brunei Darussalam	**BN**
Bulgaria	**BG**
Burkina Faso	**BF**
Burundi	**BI**
Cambodia	**KH**
Cameroon	**CM**
Canada	**CA**
Cape Verde	**CV**
Cayman Islands	**KY**
Central African Republic	**CF**
Chad	**TD**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Chile	**CL**
China	**CN**
Christmas Island	**CX**
Cocos Islands	**CC**
Colombia	**CO**
Comoros	**KM**
Congo	**CG**
Congo The Democratic Republic Of The	**CD**
Cook Islands	**CK**
Costa Rica	**CR**
Crimea	**CE**
Croatia	**HR**
CTe D Ivoire	**CI**
Cuba	**CU**
CuraAo	**CW**
Cyprus	**CY**
Czech Republic	**CZ**
Denmark	**DK**
Djibouti	**DJ**
Dominica	**DM**
Dominican Republic	**DO**
Donetsk	**DN**
Ecuador	**EC**
Egypt	**EG**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
El Salvador	**SV**
Equatorial Guinea	**GQ**
Eritrea	**ER**
Estonia	**EE**
Ethiopia	**ET**
European Union	**EU**
Falkland Islands (Malvinas)	**FK**
Faroe Islands	**FO**
Fiji	**FJ**
Finland	**FI**
France	**FR**
French Guiana	**GF**
French Polynesia	**PF**
French Southern Territories	**TF**
Gabon	**GA**
Gambia	**GM**
Georgia	**GE**
Germany	**DE**
Ghana	**GH**
Gibraltar	**GI**
Greece	**GR**
Greenland	**GL**
Grenada	**GD**
Guadeloupe	**GP**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Guam	**GU**
Guatemala	**GT**
Guernsey	**GG**
Guinea	**GN**
Guinea-Bissau	**GW**
Guyana	**GY**
Haiti	**HT**
Heard Island And Mcdonald Islands	**HM**
Holy See (Vatican City State)	**VA**
Honduras	**HN**
Hong Kong	**HK**
Hungary	**HU**
Iceland	**IS**
India	**IN**
Indonesia	**ID**
Iran Islamic Republic Of	**IR**
Iraq	**IQ**
Ireland	**IE**
Isle Of Man	**IM**
Israel	**IL**
Italy	**IT**
Jamaica	**JM**
Japan	**JP**
Jersey	**JE**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Jordan	**JO**
Kazakhstan	**KZ**
Kenya	**KE**
Kiribati	**KI**
Korea Democratic Peoples Republic Of	**KP**
Korea Republic Of	**KR**
Kuwait	**KW**
Kyrgyzstan	**KG**
Land Islands	**AX**
Lao Peoples Democratic Republic	**LA**
Latvia	**LV**
Lebanon	**LB**
Lesotho	**LS**
Liberia	**LR**
Libyan Arab Jamahiriya	**LY**
Liechtenstein	**LI**
Lithuania	**LT**
Luhansk	**LN**
Luxembourg	**LU**
Macao	**MO**
Macedonia The Former Yugoslav Republic Of	**MK**
Madagascar	**MG**
Malawi	**MW**
Malaysia	**MY**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Maldives	**MV**
Mali	**ML**
Malta	**MT**
Marshall Islands	**MH**
Martinique	**MQ**
Mauritania	**MR**
Mauritius	**MU**
Mayotte	**YT**
Mexico	**MX**
Micronesia Federated States Of	**FM**
Moldova Republic Of	**MD**
Monaco	**MC**
Mongolia	**MN**
Montenegro	**ME**
Montserrat	**MS**
Morocco	**MA**
Mozambique	**MZ**
Myanmar	**MM**
Namibia	**NA**
Nauru	**NR**
Nepal	**NP**
Netherlands	**NL**
Netherlands Antilles	**AN**
New Caledonia	**NC**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
New Zealand	**NZ**
Nicaragua	**NI**
Niger	**NE**
Nigeria	**NG**
Niue	**NU**
Norfolk Island	**NF**
Northern Mariana Islands	**MP**
Norway	**NO**
Oman	**OM**
Pakistan	**PK**
Palau	**PW**
Palestinian Territory Occupied	**PS**
Panama	**PA**
Papua New Guinea	**PG**
Paraguay	**PY**
Peru	**PE**
Philippines	**PH**
Pitcairn	**PN**
Poland	**PL**
Portugal	**PT**
Puerto Rico	**PR**
Qatar	**QA**
Romania	**RO**
RUnion	**RE**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Russian Federation	**RU**
Rwanda	**RW**
Saint BarthLemy	**BL**
Saint Helena Ascension And Tristan Da Cunha	**SH**
Saint Kitts And Nevis	**KN**
Saint Lucia	**LC**
Saint Martin (French Part)	**MF**
Saint Pierre And Miquelon	**PM**
Saint Vincent And The Grenadines	**VC**
Samoa	**WS**
San Marino	**SM**
Sao Tome And Principe	**ST**
Saudi Arabia	**SA**
Senegal	**SN**
Serbia	**RS**
Seychelles	**SC**
Sierra Leone	**SL**
Singapore	**SG**
Sint Maarten (Dutch Part)	**SX**
Slovakia	**SK**
Slovenia	**SI**
Solomon Islands	**SB**
Somalia	**SO**
South Africa	**ZA**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
South Georgia And The South Sandwich Islands	**GS**
South Sudan	**SS**
Spain	**ES**
Sri Lanka	**LK**
Sudan	**SD**
Suriname	**SR**
Svalbard And Jan Mayen	**SJ**
Swaziland	**SZ**
Sweden	**SE**
Switzerland	**CH**
Syrian Arab Republic	**SY**
Taiwan ROC	**TW**
Tajikistan	**TJ**
Tanzania United Republic Of	**TZ**
Thailand	**TH**
Timor-Leste	**TL**
Togo	**TG**
Tokelau	**TK**
Tonga	**TO**
Trinidad And Tobago	**TT**
Tunisia	**TN**
Turkey	**TR**
Turkmenistan	**TM**
Turks And Caicos Islands	**TC**

 ©2023 Palo Alto Networks, Inc.

Country Name	Country Code
Tuvalu	**TV**
Uganda	**UG**
Ukraine	**UA**
United Arab Emirates	**AE**
United Kingdom	**GB**
United States	**US**
United States Minor Outlying Islands	**UM**
Uruguay	**UY**
Uzbekistan	**UZ**
Vanuatu	**VU**
Venezuela Bolivarian Republic Of	**VE**
Viet Nam	**VN**
Virgin Islands British	**VG**
Virgin Islands U.S.	**VI**
Wallis And Futuna	**WF**
Western Sahara	**EH**
Yemen	**YE**
Zambia	**ZM**
Zimbabwe	**ZW**

 ©2023 Palo Alto Networks, Inc.

Search Top Tags, Session Histogram, and Session Aggregate Data

Use the session histogram search to get data that corresponds to the **Malware Download Sessions** histogram data when you view search statistics. Use the sample aggregate search to view top file types. Use the session aggregate data search to view aggregate data such as **Top Firewalls, Top Malware**, **Source Countries**, and **Destination Countries**. Use the top-tags search to identify the most popular tags for any given period of time. The top-tags search corresponds to the **Top Tags** data available when you view search statistics.

Aggregate search data is limited to the top 10 results in each category while top-tags data is limited to the top 20 tags.

Resources

```
/sessions/histogram/search/
/sessions/aggregate/search/
/top-tags/search/
```

Request Parameters

The following request parameters are available when searching top tags, session histogram, and session aggregate data.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
scope	(**Required**) Scope of the search. Case-sensitive.	string enumeration	Possible values: **industry, organization,all, global** Additional possible values for `/sessions/histogram/search/and /`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			`sessions/aggregate/search/:public, private`
`query`	(**Required**) Query based on conditions specified within this object. Condition match those found in the AutoFocus web portal.	object array	See Search Field Names and Search Parameter Types and Operators for a list of available fields, operators, and acceptable values. *To easily determine your `query`, first run the equivalent search in the AutoFocus web portal and then use the API button to view the corresponding JSON:* >_ API Example (nested within the `children` object array): `[ { "field":"session.src_country", "operator":"is", "value":"Algeria" }, { "field":"session.device_country", "operator":"is", "value":"United States" }, { "field":"session.app", "operator":"is", "value":"facebook-base" }`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			]
field	Field for which to provide aggregate data. **Only available and required for**: `/sessions/aggregate/search/`	string enumeration	Possible values for `/sessions/aggregate/search/`: **sha256** **app** **device_serial** **device_industry** **src_countrycode** **dst_countrycode** **upload_src**

size	Number of results to return. **Only available for**:
	`/sessions/aggregate/search/`
	`/top-tags/search/`
		number	Possible values:
			Any number above 0 up to 1000.
			Default value:
			50

tagScopes	Filter based on the type of malware. **Only available for**: `/top-tags/search/`	string enumeration (must be provided as a JSON list)	Possible values: **private,public, commodity, unit42** Default value: **Private** Example: `"tagScopes": [ "private", "unit42" ]`

Sample Request

```
curl -X POST -H "Content-Type: application/json"
-d '{
  "apiKey": "apikey",
  "query": {
    "operator": "all",
    "children": [
      {
```

 ©2023 Palo Alto Networks, Inc.

```
        "field": "sample.malware",
        "operator": "is",
        "value": 1
      },
      {
        "field": "session.tstamp",
        "operator": "is in the range",
        "value": [
          "2015-08-26T00:00:00",
          "2015-09-02T23:59:59"
        ]
      }
    ]
  },"scope":"public"
}' 'https://autofocus.paloaltonetworks.com/api/v1.0/sessions/
histogram/search'
```

View the corresponding cURLrequestor Python syntax *for initiating searches for samples, sessions, and aggregate data from the AutoFocus web portal.*

Sample Response

The response to session histogram and aggregate searches is similar to sample and sessions searches. Use the `af_cookie` parameter to view the results of your search:

```
{
  "af_in_progress": true,
  "af_first_result_af_took": 0,
  "in_progress": true,
  "af_cookie": "0-041ff071-ba35-480a-bcb2-94403ba66c41+0",
  "af_complete_percentage": 0,
  "bucket_info": {
    "minute_points": 200,
    "daily_points": 25000,
    "minute_points_remaining": 190,
    "daily_points_remaining": 24946,
    "minute_bucket_start": "2015-10-21 15:37:34",
    "daily_bucket_start": "2015-10-21 14:41:07"
  }
}
```

Use the `af_cookie` parameter when you check on the results of your search using the `/sessions/histogram/results/or /sessions/aggregate/results/` resource.

 ©2023 Palo Alto Networks, Inc.

Search for Signatures

Use these endpoints to search for signatures that match the specified parameters.

Resource

- Anti-spyware, vulnerability, and file-format signatures

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search
```

- Antivirus Signatures

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/panav/search
```

- DNS | RTDNS Signatures

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search
```

Request Parameters

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
{signatureName}	Palo Alto Networks textual identifier for the threat.	string	A valid signature name. Example: `TDSS/Win32.fey.a`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			For `/ips/search` queries, the signature is an approximate string (fuzzy) search.
`{vendor}`	The identification number for a security vendor. **Only available for**: `/ips/search`	exactString	A valid vendor reference number. Example: `25461`
`{cve}`	The reference number for a vulnerability as defined by Common Vulnerabilities and Exposures (CVE). **Only available for**: `/ips/search`	exactString	A CVE reference number for a vulnerability. Example: `cve-2015-8650`
`{domainName}`	The name of the domain. **Only available for**: `/dns/search`	string	A valid Internet domain. Example: `google.com`

Sample Request

```
curl -X POST -H "Content-Type: application/json" -d
 '{"from": 0, "size":10, "field": "signatureName", "value":
 "ExpertAntivirus_4_1" }' 'https://autofocus.paloaltonetworks.com/
api/intel/v1/threatvault/ips/search?api_key=apikey'
```

Sample Response

The response to signature searches is similar to sample and sessions searches. Use the `af_cookie` parameter from the initial response to view the results of your search:

```
    {
    {
    "total_count": 1,
    "page_count": 1,
    "signatures": [{
    "metadata": {
```

 ©2023 Palo Alto Networks, Inc.

```
    "severity": "low",
    "reference": "http://www.spywareguide.com/
spydet_3531_expertantivirus.html,http://www.ca.com/securityadvisor/
pest/pest.aspx?id=45311130",
    "panOsMaximumVersion": "",
    "description": "This signature detects the runtime behavior of
 ExpertAntivirus 4.1ExpertAntivirus is a rogue anti-spyware program
 that reports false positive infections.",
    "panOsMinimumVersion": "6.1.0",
    "action": "alert",
    "category": "adware",
    "changeData": ""
    },
    "cve": "",
    "signatureName": "ExpertAntivirus_4_1",
    "vendor": "",
    "signatureType": "spyware",
    "firstReleaseTime": "2015-06-26 UTC",
    "signatureId": 11785,
    "latestReleaseTime": "2020-06-09 UTC",
    "latestReleaseVersion": 8281,
    "status": "released",
    "firstReleaseVersion": 509
    }]
    }
```


Use the `af_cookie` parameter when you check on the results of your search using the `/ips/search/result/`, `/panav/search/result`, or `dns/search/result/` resource.

 ©2023 Palo Alto Networks, Inc.

View Search Results

For the following resources, first initiate searches and then use the `af_cookie` or `search_id` string provided in the response to view search results.

Resources for Initiating Searches	Corresponding Resources for Viewing Results
`/samples/search/`	`/samples/results/{af_cookie}`
`/stix/samples/search/`	`/stix/samples/results/{af_cookie}`
`/sessions/search/`	`/sessions/results/{af_cookie}`
`/stix/sessions/search/`	`/stix/sessions/results/{af_cookie}`
`/sessions/histogram/search/`	`/sessions/histogram/results/{af_cookie}`
`/sessions/aggregate/search/`	`/sessions/aggregate/results/{af_cookie}`
`/top-tags/search/`	`/top-tags/results/{af_cookie}`
`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search`	`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/search/result/{search_id}`
`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/panav/search`	`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/panav/search/result/{search_id}`
`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search`	`https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/search/result/{search_id}`

JSON Sample

- Request
- Response

 ©2023 Palo Alto Networks, Inc.

Request

Include the `af_cookie` to the resource URL and include the API key in the body of the request.

```
curl -X POST -H "Content-Type: application/json" -d
 '"apiKey":"apikey"' "https://autofocus.paloaltonetworks.com/api/
v1.0/samples/results/0-31b8b9a7-82d2-4d2c-a414-717cba470f03+0"
```

Response

The sample response contains key parameters such as `af_message` and `af_in_progress` to indicate whether the previously initiated search is complete. When the request is complete, the response `af_message` becomes `complete`.

```
{
  "total": 11143,
  "hits": [
    {
      "_id":
 "d5d252b2a7b145f0777b1e6020ecc2457f14cbb661b384fc7d8a80f3e1004a7a",
      "_source": {
        "create_date": "2016-10-06T02:03:38",
        "sha256":
 "d5d252b2a7b145f0777b1e6020ecc2457f14cbb661b384fc7d8a80f3e1004a7a",
        "ssdeep": "768:+4Ylr/tYrSD810d6xfhhbhBZawROX2kgzIcNaFi48o:
+lr1cSgPxp/mXksooiro",
        "md5": "0611cdbf57b2a7c9840cbff969e6b3f2",
        "filetype": "Microsoft Excel Document",
        "sha1": "dd75186f97b13f9092f3e8dae2f82bb33a20eba4",
        "finish_date": "2016-10-06T02:11:31",
        "malware": 1,
        "size": 37284,
        "tag": [],
        "region": [
          "us"
        ]
      },
      "visible": true
    },

/* TRUNCATED */

  ],
  "took": 19247,
  "af_in_progress": true,
  "af_first_result_af_took": 437,
  "af_complete_percentage": 72,
  "af_cookie": "2-91595279-f7d5-449e-b478-b231b2a9f266+0",
  "bucket_info": {
    "minute_points": 200,
    "daily_points": 100000,
    "minute_points_remaining": 179,
    "daily_points_remaining": 99178,
    "minute_bucket_start": "2016-10-10 17:43:55",
    "daily_bucket_start": "2016-10-10 03:27:03"
  },
```

 ©2023 Palo Alto Networks, Inc.

```
  "original_query": {
    "body": {
      "scope": "public",
      "sort": {
        "create_date": {
          "order": "desc"
        }
      },
      "query": {
        "children": [
          {
            "field": "session.src_country",
            "value": "Algeria",
            "operator": "is"
          }
        ],
        "operator": "all"
      },
      "from": 0,
      "size": 50
    },
    "url": "/api/v1.0/samples/search"
  }
}
```

STIX Sample

- Request
- Response

Request

Include the `af_cookie` to the resource URL and include the API key in the body of the request.

```
curl -X POST -H "Content-Type: application/xml" -
d '<req><apiKey>apikey</apiKey></req>' "https://
autofocus.paloaltonetworks.com/api/v1.0/stix/samples/
results/0-0d0bb06b-6252-48ff-9d3a-4e43af844338+0"
```

Response

The sample response contains key parameters such as `af_message` and `af_in_progress` to indicate whether the previously initiated search is complete. When the request is complete, the response `af_message` becomes `complete`.

```
<res>
    <total>1223</total>
    <took>13559</took>
    <aggregations></aggregations>
    <af_message>complete</af_message>
    <af_in_progress>false</af_in_progress>
    <af_first_result_af_took>123</af_first_result_af_took>
    <af_complete_percentage>100</af_complete_percentage>
    <af_cookie>0-726c560a-fa11-41c7-b900-b267c80c15b3+0</af_cookie>
```

 ©2023 Palo Alto Networks, Inc.

```
    <bucket_info>
        <minute_points>200</minute_points>
        <daily_points>10000</daily_points>
        <minute_points_remaining>189</minute_points_remaining>
        <daily_points_remaining>9268</daily_points_remaining>
        <minute_bucket_start>2016-05-09 14:08:33</
minute_bucket_start>
        <daily_bucket_start>2016-05-09 03:42:10</daily_bucket_start>

    </bucket_info>
    <original_query>
        <body>
            <scope>private</scope>
            <sort>
                <update_date>
                    <order>desc</order>

                </update_date>

            </sort>
            <query>
                <children>
                    <item>
                        <field>session.src_country</field>
                        <value>Algeria</value>
                        <operator>is</operator>

                    </item>

                </children>
                <operator>all</operator>

            </query>
            <from>0</from>
            <size>50</size>

        </body>
        <url>/api/v1.0/stix/samples/search</url>

    </original_query>
    <stix>
        <stix:STIX_Package xmlns:FileObj="http://
cybox.mitre.org/objects#FileObject-2" xmlns:autofocus="https://
autofocus.paloaltonetworks.com" xmlns:cybox="http://cybox.mitre.org/
cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
 xmlns:stix="http://stix.mitre.org/stix-1" xmlns:stixCommon="http://
stix.mitre.org/common-1" xmlns:stixVocabs="http://stix.mitre.org/
default_vocabularies-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" id="autofocus:Package-e2f6487f-37c8-44a7-89e0-2cc7437549f7"
 version="1.1.1" timestamp="2016-05-09T21:09:31.626761+00:00">
            <stix:Observables cybox_major_version="2"
 cybox_minor_version="1" cybox_update_version="0">
                <cybox:Observable
 id="autofocus:Observable-75e24ed4-7201-458f-82b5-b1b529778f50">
```

 ©2023 Palo Alto Networks, Inc.

```
                    <cybox:Description>Wildfire Verdict: 1, First
 Seen: 2016-04-07T04:51:26, Finish Date: 2016-04-07T04:59:16,
 Tags: [Unit42.zNOT-PE-1026,5672.Satish-Cushman-Meta-Word97-2003]</
cybox:Description>
                    <cybox:Object id="autofocus:File-
f6c615ee-98f9-4a92-af21-d29c7c0262f0">
                        <cybox:Properties
 xsi:type="FileObj:FileObjectType">
                            <FileObj:Size_In_Bytes>110080</
FileObj:Size_In_Bytes>
                            <FileObj:File_Format>Microsoft Word 97 -
 2003 Document</FileObj:File_Format>
                            <FileObj:Hashes>
                                <cyboxCommon:Hash>
                                    <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>

 <cyboxCommon:Simple_Hash_Value>393e21b3540a2d2fb56f37e216ef4627d37fe4c407127be
cyboxCommon:Simple_Hash_Value>

                                </cyboxCommon:Hash>
                                <cyboxCommon:Hash>
                                    <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA1</cyboxCommon:Type>

 <cyboxCommon:Simple_Hash_Value>771b59b461da9487253ff40138de627c7ad96e7b</
cyboxCommonSimple_Hash_Value>

                                </cyboxCommon:Hash>
                                <cyboxCommon:Hash>
                                    <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5</cyboxCommon:Type>

 <cyboxCommon:Simple_Hash_Value>ec5753a10ed77f0226c7490ced718c20</
cyboxCommon:Simple_Hash_Value>

                                </cyboxCommon:Hash>
                                <cyboxCommon:Hash>
                                    <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SSDEEP</cyboxCommon:Type>

 <cyboxCommon:Fuzzy_Hash_Value>3072:SnfYFhXQIYH2c4tzeA/
Kn334EEzUFYJ8Bei3DPOgyvqfYdth1lk6TVnAnZ0PmDz:Qm2ONBWpy</
cyboxCommon:Fuzzy_Hash_Value>

                                </cyboxCommon:Hash>

                            </FileObj:Hashes>
                            <FileObj:Digital_Signatures>
                                <cyboxCommon:Digital_Signature></
cyboxCommon:Digital_Signature>

                            </FileObj:Digital_Signatures>

                        </cybox:Properties>
```

 ©2023 Palo Alto Networks, Inc.

```
                    </cybox:Object>

                </cybox:Observable>
<!-- TRUNCATED -->
      </stix:Observables>
    </stix:STIX_Package>
  </stix>
</res>
```

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Perform Direct Searches

While some AutoFocus™ API calls, such as searches for samples or sessions, are asynchronous and require API calls to two resources, other searches don't require queuing and provide responses immediately.

- Get Session Details
- Get Sample Analysis
- Get Tags
- Get Tag Details
- Get Threat Indicator Feed
- Get Custom Threat Indicator Feed
- Get Threat Intelligence Card Summary
- Export List
- Get Anti-spyware, Vulnerability, and File-Format Signature
- Get Antivirus Signature
- Get DNS Signature
- Get Geolocation
- Get Anti-spyware, Vulnerability, and File-Format Release Info

Get Session Details

Use this resource to get details about a specific session, such as application, filename, source country, and device model. Include a session ID parameter (**_id**) in the URL to indicate the session you want to look at. The session ID is shown when you Search Samples and Sessions.

- Resource
- Request Parameters
- Sample Request
- Sample Response

Resource

```
/session/{session_id}
```

Request Parameters

The following table describes request parameters for Get Session requests.

Parameters	Description	Type	Example or Possible Values
_id	(Required) Session ID of the session.	string	Example: **11935370063**

Sample Request

Provide the session ID in the request URL:

```
curl -X POST -H "Content-Type: application/json"
-d '{ "apiKey": "apikey"}' 'https://autofocus.paloaltonetworks.com/
api/v1.0/session/11935370063'
```

Sample Response

The response includes details about the corresponding session:

```
{
  "af_message": "complete",
  "af_in_progress": false,
  "af_responses": 2,
  "took": 76,
  "af_first_result_af_took": 80,
  "af_cookie": "0-5a7b19b4-6854-4af3-9cd5-f33ac7ffca6d",
  "hits": [
    {
      "_id": "11935370063",
      "_source": {
        "app": "smtp",
        "emailsender": "Vhg1lzi@yfmcioVeGVOzyJcblirexNMAjbSb.net",
```

 ©2023 Palo Alto Networks, Inc.

```
        "device_country": "United States",
        "sha256":
 "ae433a1049d4647f6ea6e4ce6ae36717247ebb03edb07869af95c47805250480",
        "dst_port": "25",
        "device_serial": "007200002578",
        "dst_ip": "10.154.10.47",
        "fileurl": "unknown",
        "device_industry": "High Tech",
        "tstamp": "2015-09-08T12:04:47",
        "src_port": "44859",
        "device_hostname": "jp4demo.example.com",
        "emailsubject":
 "7ijZR3aHLzkZPgN6qIpunZkCbRiuj4WjSmBmnPlHU4P4z26uvQContent-
Type: multipart/mixed; boundary=\"_74289530830040887l816834\"--
_74289530830040887l816834Content-Type: text/plainContent-Disposition:
 7bitruo5Umuazuyj4KhfnjJPe44nP2--_74289530830040887l816834Conte",
        "filename": "VRzOAZufmnnuEkd.Exe",
        "src_country": "United States",
        "src_ip": "66.1.1.10",
        "user_id": "unknown",
        "emailrecipient": "sBgeGaIFSp1WksQV2P@yIZGAEwV.edu",
        "device_countrycode": "US",
        "src_countrycode": "US",
        "vsys": 1,
        "region": "us"
      }
    }
  ],
  "af_first_result_es_took": 76,
  "af_first_result_es_hits": 1,
  "af_indices": 2,
  "af_complete_percentage": 100,
  "bucket_info": {
    "minute_points": 200,
    "daily_points": 100000,
    "minute_points_remaining": 198,
    "daily_points_remaining": 99176,
    "minute_bucket_start": "2016-10-10 17:58:36",
    "daily_bucket_start": "2016-10-10 03:27:03"
  }
}
```


 ©2023 Palo Alto Networks, Inc.

Get Sample Analysis

Use this resource to get properties, behaviors, and activities observed for a sample during WildFire™ analysis. To look at this information from the WildFire sample analysis report, include the SHA256 hash of the sample as a URL parameter.

Resource

```
/sample/{sample_id}/analysis/
stix/sample/{sample_id}/analysis
```

Request Parameters

Request URL Parameters

The following table describes URL parameters for Get Sample Analysis requests.

Parameters	Description	Type	Example or Possible Values
{sample_id}	(**Required**) SHA256 hash of the sample. The hash is provided in responses to sample searches.	string	Example: **d87edc101466ec130ce42183c79a5d503a972530b**

Request Body Parameters

The following table describes body parameters for Get Sample Analysis requests.

Parameters	Description	Type	Example or Possible Values
coverage	Boolean to indicate whether to include applicable signature coverage data. This option allows you to see the WildFire signatures available to cover a given sample.	boolean	Possible values: **true, false** Example: `{ "apiKey":"apikey", "coverage":”true”,`

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
	Sample coverage allows you to determine the current level of protection for malware.		<pre> "sections":["coverage"] }</pre>

sections	Include specific WildFire analysis sections, which describe the observed behavior.	string enumeration	**apk_app_icon** :**apk_app_name** :**apk_cert_file** :**apk_certificate_id** :**apk_defined_activity** :**apk_defined_intent_filter** **apk_defined_receiver** **apk_defined_sensor** **apk_defined_service** **apk_digital_signer** **apk_embedded_library** **apk_embeded_url** **apk_internal_file** **apk_isrepackaged** **apk_packagename** **apk_requested_permission** **apk_sensitive_api_call** **apk_suspicious_behavior** **apk_suspicious_file** **apk_suspicious_pattern** **apk_suspicious_action_monitored** **apk_suspicious_file** **apk_suspicious_string** **apk_version_num** **behavior_type** **connection** **coverage** **dns** **file** **http** **japi** **mac_embedded_url** **misc** **mutex** **process** **registry** **service** **user_agent**
			
			*To include coverage as a section, you must also request coverage as part of your response (**"coverage":"true"**).*
			
			Example:
			<pre>{
			"apiKey":"*apikey*",
			  "coverage":"true",
			  "sections":["coverage"]</pre>

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			} }

platforms	Analysis environments to include in the response.	string enumeration	Possible values:
			win7, winxp, android, static_analyzer, mac, bare_metal
			Example:
			{
			"apiKey": "apikey",
			"sections": ["file"],
			"platforms": ["win7",
			"winxp"]
			}

JSON Sample

- Request
- Response

Request

Include the SHA256 hash in the resource URL, and the API key in the request body.

```
curl -X POST -H "Content-Type: application/json"
-d '{
  "apiKey":"apikey",
  "coverage":true,
  "sections":["coverage"]
}' 'https://autofocus.paloaltonetworks.com/api/v1.0/
sample/3d0d8c0e8b80ea89b6c360d0077ae2e6d08f654ad28d7c5da57adaf4593a333f/
analysis'
```

Response

The response, which is specific to the hash that you specify in your request, includes numerous details categorized for both Windows XP and Windows 7: observed behavior; file activity; HTTP requests, process activity; registry activity; DNS activity, connection activity; user agent string fragments; mutex activity, API activity.

```
{
  "sections": [],
  "platforms": [
    "static_analyzer",
    "win7",
    "winxp"
  ],
  "coverage": {
    "wf_av_sig": [
```

 ©2023 Palo Alto Networks, Inc.

```
      {
        "name": "Virus/Win32.WGeneric.hosfp",
        "create_date": "2016-03-05T06:03:40.000Z",
        "first_added_daily": 1805,
        "last_added_daily": 1805,
        "first_added_15min": 90419,
        "last_added_15min": 90419,
        "first_added_5min": 16375,
        "last_added_5min": 16375,
        "currently_present_daily": false,
        "currently_present_15min": false,
        "currently_present_5min": false
      }
    ],
    "dns_sig": [
      {
        "name": "generic:www.stsunsetwest.com",
        "create_date": "2014-01-29T13:30:52.000Z",
        "first_added_daily": 1202,
        "last_added_daily": 1202,
        "first_added_15min": null,
        "last_added_15min": null,
        "first_added_5min": null,
        "last_added_5min": null,
        "currently_present_daily": false,
        "currently_present_15min": false,
        "currently_present_5min": false,
        "domain": "www.stsunsetwest.com"
      },
<!-- TRUNCATED -->
```


STIX Sample

- Request
- Response

Request

Include the SHA256 hash in the resource URL, and the API key in the request body.

```
curl -X POST -H "Content-Type: application/xml" -d '
<req>
    <apiKey>apikey</apiKey>
    <sections><item>file</item></sections>
    <platforms><item>win7</item><item>winxp</item></platforms>
</req>' "https://autofocus.paloaltonetworks.com/api/v1.0/stix/
sample/3d0d8c0e8b80ea89b6c360d0077ae2e6d08f654ad28d7c5da57adaf4593a333f/
analysis"
```

Response

The response, which is specific to the hash that you specify in your request, includes numerous details categorized for both Windows XP and Windows 7: observed behavior; file activity; HTTP

 ©2023 Palo Alto Networks, Inc.

requests, process activity; registry activity; DNS activity, connection activity; user agent string fragments; mutex activity, API activity.

```
<maecBundle:Action id="autofocus:action-
caa0b4e9-18e1-41d6-80ae-5c981196aa08">
     <cybox:Description>Line counts: Malware: 29962552, Benign:
 15163791, Grayware: 3153170</cybox:Description>
     <cybox:Action_Arguments>
       <cybox:Action_Argument>
          <cybox:Argument_Value>Write</cybox:Argument_Value>
       </cybox:Action_Argument>
       <cybox:Action_Argument>
          <cybox:Argument_Value>Windows\AppCompat\Programs
\RecentFileCache.bcf</cybox:Argument_Value>
       </cybox:Action_Argument>
     </cybox:Action_Arguments>
     <cybox:Associated_Objects>
       <cybox:Associated_Object id="autofocus:Process-70224e7f-
a126-48a7-9111-933e8e0f8c40">
          <cybox:Properties xsi:type="ProcessObj:ProcessObjectType">
            <ProcessObj:Name>svchost.exe</ProcessObj:Name>
          </cybox:Properties>
       </cybox:Associated_Object>
       <cybox:Associated_Object id="autofocus:System-319a6a30-
face-49a4-9e41-262558602a0c">
          <cybox:Properties xsi:type="SystemObj:SystemObjectType">
            <SystemObj:OS>
               <SystemObj:Platform>
                 <cyboxCommon:Identifier system="win7">None</
cyboxCommon:Identifier>
               </SystemObj:Platform>
            </SystemObj:OS>
          </cybox:Properties>
       </cybox:Associated_Object>
     </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="autofocus:action-06c9fc06-000b-4759-a555-
ed22c35a5d6d">
     <cybox:Description>Line counts: Malware: 1, Benign: 0, Grayware:
 0</cybox:Description>
     <cybox:Action_Arguments>
       <cybox:Action_Argument>
          <cybox:Argument_Value>Write</cybox:Argument_Value>
       </cybox:Action_Argument>
       <cybox:Action_Argument>
          <cybox:Argument_Value>Users\Administrator\AppData\Local
\Temp\is-RUD9I.tmp\sample.tmp</cybox:Argument_Value>
       </cybox:Action_Argument>
     </cybox:Action_Arguments>
     <cybox:Associated_Objects>
       <cybox:Associated_Object id="autofocus:Process-4e3fe414-
af23-47bd-9338-c5a2665a3903">
          <cybox:Properties xsi:type="ProcessObj:ProcessObjectType">
            <ProcessObj:Name>sample.exe</ProcessObj:Name>
          </cybox:Properties>
       </cybox:Associated_Object>
```

 ©2023 Palo Alto Networks, Inc.

```
        <cybox:Associated_Object
 id="autofocus:System-02eb108b-9d06-4e23-ba87-36a9d84ac95d">
          <cybox:Properties xsi:type="SystemObj:SystemObjectType">
            <SystemObj:OS>
               <SystemObj:Platform>
                 <cyboxCommon:Identifier system="win7">None</
cyboxCommon:Identifier>
               </SystemObj:Platform>
            </SystemObj:OS>
          </cybox:Properties>
        </cybox:Associated_Object>
      </cybox:Associated_Objects>
  </maecBundle:Action>
```

 ©2023 Palo Alto Networks, Inc.

Get Tags

Use this resource to get a list of tags. You can specify optional parameters such as **scope** to further filter results.

- Resource
- Request Parameters
- Tag Identifiers
- STIX Sample

Resource

```
/tags/
/stix/tags/
```

Request Parameters

- Request Body Parameters
- Tag Identifiers
- Parameter Types and Operators

Request Body Parameters

The following table describes body parameters for Get Tags requests.

Parameters	Description	Type	Example or Possible Values
scope	Scope of the search.	string enumeration	Possible values: **visible**: tags visible to you **private**: private tags owned by you **mine**: tags owned by you **public**: public tags **unit42**: Unit 42 tags **commodity**: Unit 42 commodity tags Default value: **visible**
pageSize	The number of results to provide per response.	Number	Possible values: Range is **1-200**; default is **50**.
pageNum	The page number from which to start	Number	Possible values:

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
	displaying tag. When **pageNum** is specified, results are shown starting from that particular page number. A value of 0 indicates page 1.		Range is 0-1,000,000,000; default is 0.
sortBy	Sort by the specified label.	String enumeration	Possible values: **name, status, count, lasthit, upVotes** Default value: **name**
order	Sort either in ascending or descending order. Ascending order is alphabetical or numbers sorted from lowest to highest, descending order is the opposite.	String enumeration	Possible values: **asc, desc** Default value: **asc**
query	Filter the results based on the specified tag conditions and values.	String enumeration	Possible values: **field**: the name of a tag identifier **operator**: specifies the condition whereby the `value` is evaluated. **value**: the parameter that is being tested. See Tag Identifiers and Parameter Types and Operators for a complete list of available fields, operators, and acceptable values.

Tag Identifiers

The following table describes tag identifiers for Get Tags requests.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
alias	Alias	typeAheadSelect	Valid AutoFocus tag.

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
			Example: **`Cekar`**
`customer`	Author Company	String	Valid organization that created the tag. Example: **`Palo Alto Networks`**
`author`	Author Email	exactString	Valid email address of the tag creator. Example: **`john.doe@company.com`**
`tag_class`	Class	Select	Valid tag class ID number. **1**: Actor **2**: Campaign. **3**: Malware Family. **4**: Exploit. **5**: Malicious Behavior. Example: **1**
`created`	Created	Date	The creation date of a tag. Example: **`2015-09-21T11:33:20`**
`description`	Description	String	The description contained in a tag. Example: **`advertising banners`**
`comments`	# Comments	Number	The number of comments associated with a tag. Example: **2**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
lastComment	Last Comment	Date	The date of the last comment added to a tag. Example: **2010-09-21T11:34:15**
lastHit	Last Hit	Date	The time at which the most recent sample matched to the tag was detected. Example: **2016-19-21T11:31:10**
matchCriteria	Match Criteria	String	The conditions listed in the definition column contained within an AutoFocus tag. Example: **sample.exe**
tag_name	Name	String	The name of an AutoFocus tag. Example: **Sconato**
tag_group	Tag Group	typeAheadSelect	The name of an AutoFocus tag group. Example: **AdWare**
reference	References	String	External references providing more information or context for the given threat. Example: **Symantec**
numSamples	# Samples	Number	The total number of private and public samples matched to the tag. Example: **4**

 ©2023 Palo Alto Networks, Inc.

Field Name	Artifact Type as it Appears on AutoFocus Web Portal	Field Type	Acceptable Values and Examples
tagType	Scope	Select	A valid tag type. Example: **private**
source	Source	String	Organization or individual that discovered the threat defined in the tag. Example: **Secureworks**
status	Status	Select	The current operational status of a tag. Example: **Removing**
upVotes	# Up Votes	Number	The number of up-votes the tag has received from the AutoFocus community. Example: **2**
updated	Updated	Date	The date and time that the tag was most recently modified. Example: **2016-19-21T11:31:10**

Parameter Types and Operators

The following table lists the parameter types and corresponding operators for Tag Identifiers.

Parameter Type	Available Operators
alias	**contains, does not contain, proximity**
bool	**is true, is false, has no value, has any value**
date	**is in the range, is after, is before, is, has no value, has any value**

 ©2023 Palo Alto Networks, Inc.

Parameter Type	Available Operators
exactString	**is, is not, has no value, has any value**
exactStringList	**is, is not, is in the list, is not in the list, has no value, has any value**
exactStringListRegexp	**is, is not, is in the list, is not in the list, has no value, has any value, regexp**
ipAddress	**is, is not, is in the range, has no value, has any value**
number	**is, is not, is in the range, greater than, greater than or equal, less than, less than or equal, has no value, has any value**
numberString	**is, is not**
select	**is, is not, is in the list, is not in the list, has no value, has any value**
simpleSelect	**is, is not, is in the list, is not in the list**
simpleStringList	**is, is not, is in the list, is not in the list**
singleSelect	**is, is not**
singleSelectVal	**is, is not, has no value, has any value**
string	**contains, does not contain, has no value, has any value**
stringList	**contains, does not contain, is in the list, is not in the list, has no value, has any value**
stringProx	**contains, does not contain, has no value, has any value, proximity, regexp**
tagList	**is in the list, is not in the list, has no value, has any value**
typeAheadSelect	**is, is not, is in the list, is not in the list**

JSON Sample

- Request
- Response

 ©2023 Palo Alto Networks, Inc.

Request

Include optional request body parameters along with your API key to further filter results.

```
curl -X POST -H "Content-Type: application/json" -d
'{
"apiKey": "apiKey",
"scope": "unit42",
"pageNum": 0,
"pageSize": 3,
"sortBy": "name",
"order": "asc",
"query":{"field":"tag_name","operator":"contains","value":"4h"}
}' 'https://autofocus.paloaltonetworks.com/api/v1.0/tags'
```

Response

The response contains a list of tags that match filters sent in the optional request body parameters.


```
{
    "tags": [
        {
            "tag_name": "1580",
            "public_tag_name": "Commodity.1580",
            "count": 1,
            "lasthit": "2015-10-15 05:42:40",
            "description": null,
            "tag_definition_status_id": 1,
            "tag_definition_scope_id": 3,
            "tag_class_id": null,
            "source": null,
            "customer_name": "Palo Alto Networks Unit42",
            "up_votes": null,
            "down_votes": null,
            "comments": null,
            "aliases": null,
            "tag_definition_status": "enabled",
            "tag_definition_scope": "commodity"
        },
        {
            "tag_name": "4H",
            "public_tag_name": "Unit42.4H",
            "count": 39,
            "lasthit": "2015-12-01 09:43:46",
            "description": null,
            "tag_definition_status_id": 1,
            "tag_definition_scope_id": 4,
            "tag_class_id": null,
            "source": null,
            "customer_name": "Palo Alto Networks Unit42",
            "up_votes": null,
            "down_votes": null,
            "comments": null,
            "aliases": null,
            "tag_definition_status": "enabled",
```


 ©2023 Palo Alto Networks, Inc.

```
            "tag_definition_scope": "unit42"
        },
        {
            "tag_name": "6547",
            "public_tag_name": "Unit42.6547",
            "count": 0,
            "lasthit": null,
            "description": null,
            "tag_definition_status_id": 1,
            "tag_definition_scope_id": 4,
            "tag_class_id": null,
            "source": null,
            "customer_name": "Palo Alto Networks Unit42",
            "up_votes": null,
            "down_votes": null,
            "comments": null,
            "aliases": null,
            "tag_definition_status": "enabled",
            "tag_definition_scope": "unit42"
        }
    ],
    "total_count": 116,
    "bucket_info": {
        "minute_points": 200,
        "daily_points": 25000,
        "minute_points_remaining": 198,
        "daily_points_remaining": 24133,
        "minute_bucket_start": "2015-12-14 16:04:18",
        "daily_bucket_start": "2015-12-14 13:06:01"
    }
```


STIX Sample

- Request
- Response

Request

Include optional request body parameters along with your API key to further filter results.

```
curl -X POST -H "Content-Type: application/xml" -d '<req>
    <apiKey>apikey</apiKey>
    <scope>unit42</scope>
    <pageNum>0</pageNum>
    <pageSize>3</pageSize>
    <sortBy>name</sortBy>
    <order>asc</order>
</req>' "https://autofocus.paloaltonetworks.com/api/v1.0/stix/tags"
```

Response

The response contains a list of tags that match filters sent in the optional request body parameters.


```
<res>
```


 ©2023 Palo Alto Networks, Inc.

```
  <total_count>116</total_count>
  <bucket_info>
    <minute_points>200</minute_points>
    <daily_points>25000</daily_points>
    <minute_points_remaining>198</minute_points_remaining>
    <daily_points_remaining>24994</daily_points_remaining>
    <minute_bucket_start>2016-03-08 13:38:07</minute_bucket_start>
    <daily_bucket_start>2016-03-08 13:29:46</daily_bucket_start>
  </bucket_info>
  <stix>
    <stix:STIX_Package xmlns:stix="http://stix.mitre.org/stix-1"
 xmlns:autofocus="https://autofocus.paloaltonetworks.com"
 xmlns:cybox="http://cybox.mitre.org/cybox-2"
 xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
 xmlns:indicator="http://stix.mitre.org/Indicator-2"
 xmlns:stixCommon="http://stix.mitre.org/common-1"
 xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 id="autofocus:Package-3a86b27f-be11-44ec-b508-58ae583f99b2"
 version="1.1.1" timestamp="2016-03-08T21:38:08.055197+00:00">
      <stix:Indicators>
        <stix:Indicator id="autofocus:indicator-5cb3a95d-40a0-4563-
acb9-12e57aeb6a35" timestamp="2015-10-15T05:42:40"
 xsi:type="indicator:IndicatorType">
          <indicator:Title>Commodity.1580</indicator:Title>
          <indicator:Short_Description>Tag Name: 1580, Down Votes:
 0, Up Votes: 0, Scope: commodity, Status: enabled, Comments: 0</
indicator:Short_Description>
          <indicator:Sightings sightings_count="1" />
          <indicator:Producer>
            <stixCommon:Description />
            <stixCommon:Identity>
              <stixCommon:Name>Palo Alto Networks Unit42</
stixCommon:Name>
            </stixCommon:Identity>
          </indicator:Producer>
        </stix:Indicator>
        <stix:Indicator
 id="autofocus:indicator-4d54e146-110f-45e9-8560-cc77c7d1b172"
 timestamp="2015-12-01T09:43:46" xsi:type="indicator:IndicatorType">
          <indicator:Title>Unit42.4H</indicator:Title>
          <indicator:Short_Description>Tag Name: 4H, Down Votes:
 1, Up Votes: 0, Scope: unit42, Status: enabled, Comments: 0</
indicator:Short_Description>
          <indicator:Sightings sightings_count="38" />
          <indicator:Producer>
            <stixCommon:Description />
            <stixCommon:Identity>
              <stixCommon:Name>Palo Alto Networks Unit42</
stixCommon:Name>
            </stixCommon:Identity>
          </indicator:Producer>
        </stix:Indicator>
        <stix:Indicator
 id="autofocus:indicator-8e996377-96bc-4e12-9ea6-
```

 ©2023 Palo Alto Networks, Inc.

```
dafc2abba436" timestamp="2016-03-08T21:38:08.056075+00:00"
 xsi:type="indicator:IndicatorType">
          <indicator:Title>Unit42.6547</indicator:Title>
          <indicator:Short_Description>Tag Name: 6547, Down Votes:
 0, Up Votes: 0, Scope: unit42, Status: enabled, Comments: 0</
indicator:Short_Description>
          <indicator:Producer>
            <stixCommon:Description />
            <stixCommon:Identity>
              <stixCommon:Name>Palo Alto Networks Unit42</
stixCommon:Name>
            </stixCommon:Identity>
          </indicator:Producer>
        </stix:Indicator>
      </stix:Indicators>
    </stix:STIX_Package>
  </stix>
</res>
```

Get Tag Details

Use this resource to get details on a specific public tag listed on the AutoFocus web portal.

Resource

```
/tag/{public_tag_name}
/stix/tag/{public_tag_name}
```

Request Parameters

The following table describes parameters for Get Tag Details requests.

The public tag name request parameter is not case-sensitive.

Parameters	Description	Type	Example or Possible Values
public_tag_name	(**Required**) Public tag name as listed in the AutoFocus web portal. The public tag name is visible in the response when you Get Tags.	string	Example: **Unit42.CryptoWall**

JSON Sample

Request

Include the public tag name to the request URL and include the API key within the request body.

```
curl -X POST -H "Content-Type: application/json" \
-d '{"apiKey": "apikey"}' 'https://autofocus.paloaltonetworks.com/
api/v1.0/tag/Unit42.CryptoWall'
```

Response

The response contains details about the specified tag.

```
{
```

 ©2023 Palo Alto Networks, Inc.

```
  "tag":{
    "support_id":1,
    "tag_name":"CryptoWall",
    "public_tag_name":"Unit42.CryptoWall",
    "tag_definition_scope_id":4,
    "tag_definition_scope":"unit42",
    "tag_definition_status_id":1,
    "tag_definition_status":"enabled",
    "count":9279,
    "lasthit":"2015-12-11 15:06:33",
    "description":"CryptoWall is a ransomware family which
 encrypts files on the system and then demands a ransom from the
 victim before releasing the encryption key. \n\nMore information
 about CryptoWall is available at the following URLs:\n\nhttp://
researchcenter.paloaltonetworks.com/2014/10/tracking-new-ransomware-
cryptowall-2-0/\nhttp://malware.dontneedcoffee.com/2015/01/guess-
whos-back-again-cryptowall-30.html",
    "customer_name":"Palo Alto Networks Unit42",
    "refs":null,
    "tag_class_id":null,
    "report_actions":null,
    "source":null,
    "comments":[

    ]
  },
  "tag_searches":[
    {
      "count":9279,
      "lasthit":"2015-12-11 15:06:33",
      "search_name":"1e3f1a50ae9547166d",
      "tag_definition_search_status_id":1,
      "tag_definition_search_status":"enabled",
      "ui_search_definition":"{\"operator\":\"Any\",\"children\":
[{\"field\":\"sample.tasks.file\",\"operator\":\"contains\",\"value
\":\"3353616\\3353616.exe\"},{\"field\":\"sample.tasks.file\",
\"operator\":\"contains\",\"value\":\"Users\\Administrator\\AppData
\\Local\\Microsoft\\Internet Explorer\\DECRYPT_INSTRUCTION.TXT
\"},{\"field\":\"sample.tasks.file\",\"operator\":\"contains\",
\"value\":\"HELP_DECRYPT.PNG\"},{\"field\":\"sample.tasks.file\",
\"operator\":\"contains\",\"value\":\"HELP_DECRYPT.URL\"},{\"field
\":\"sample.tasks.file\",\"operator\":\"contains\",\"value\":
\"HELP_DECRYPT.TXT\"},{\"field\":\"sample.tasks.file\",\"operator
\":\"contains\",\"value\":\"HELP_DECRYPT.HTML\"}],\"field\":
\"sample.sha256\"}"
    }
  ],
  "aliases":[

  ],
  "related_tags":[

  ],
  "bucket_info":{
    "minute_points":200,
    "daily_points":25000,
```


 ©2023 Palo Alto Networks, Inc.

```
    "minute_points_remaining":196,
    "daily_points_remaining":24139,
    "minute_bucket_start":"2015-12-14 15:46:06",
    "daily_bucket_start":"2015-12-14 13:06:01"
  }
}
```

STIX Sample

- Request
- Response

Request

Include the public tag name to the request URL and include the API key within the request body.

```
curl -X POST -H "Content-Type: application/xml"
-d '<req><apiKey>apikey</apiKey></req>' "https://
autofocus.paloaltonetworks.com/api/v1.0/stix/tag/Unit42.CryptoWall"
```

Response

The response contains details about the specified tag.

```
<res>
  <bucket_info>
    <minute_points>200</minute_points>
    <daily_points>25000</daily_points>
    <minute_points_remaining>198</minute_points_remaining>
    <daily_points_remaining>24998</daily_points_remaining>
    <minute_bucket_start>2016-03-09 16:44:45</minute_bucket_start>
    <daily_bucket_start>2016-03-09 16:44:45</daily_bucket_start>
  </bucket_info>
  <stix>
    <stix:STIX_Package xmlns:stix="http://stix.mitre.org/stix-1"
 xmlns:autofocus="https://autofocus.paloaltonetworks.com"
 xmlns:cybox="http://cybox.mitre.org/cybox-2"
 xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
 xmlns:indicator="http://stix.mitre.org/Indicator-2"
 xmlns:stixCommon="http://stix.mitre.org/common-1"
 xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 id="autofocus:Package-77c5b3d7-867d-466f-9816-2141f59cd809"
 version="1.1.1" timestamp="2016-03-10T00:44:46.003067+00:00">
      <stix:Indicators>
        <stix:Indicator id="autofocus:indicator-73a63fc4-
dea5-4a81-8e44-ca8934ba1c3c" timestamp="2016-03-06T01:24:06"
 xsi:type="indicator:IndicatorType">
          <indicator:Title>Unit42.CryptoWall</indicator:Title>
          <indicator:Description>CryptoWall is a ransomware family
 which encrypts files on the system and then demands a ransom from
 the victim before releasing the encryption key.
```

 ©2023 Palo Alto Networks, Inc.

```
More information about CryptoWall is available at the following
 URLs:

http://researchcenter.paloaltonetworks.com/2014/10/tracking-new-
ransomware-cryptowall-2-0/
http://malware.dontneedcoffee.com/2015/01/guess-whos-back-again-
cryptowall-30.html</indicator:Description>
          <indicator:Short_Description>Tag Name: CryptoWall, Scope:
 unit42, Status: enabled, Aliases:</indicator:Short_Description>
          <indicator:Composite_Indicator_Expression operator="OR">
            <indicator:Indicator id="autofocus:indicator-d87a50e5-
ef31-454a-95bc-c5efcdde276b" timestamp="2016-03-06T01:24:06"
 xsi:type="indicator:IndicatorType">
              <indicator:Description>&lt;?xml version="1.0"
 encoding="UTF-8"?&gt;&lt;query&gt;&lt;operator&gt;Any&lt;/
operator&gt;&lt;children&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/
operator&gt;&lt;value&gt;3353616\3353616.exe&lt;/value&gt;&lt;/
item&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/operator&gt;&lt;value&gt;Users
\Administrator\AppData\Local\Microsoft\Internet
 Explorer\DECRYPT_INSTRUCTION.TXT&lt;/value&gt;&lt;/
item&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/
operator&gt;&lt;value&gt;HELP_DECRYPT.PNG&lt;/value&gt;&lt;/
item&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/
operator&gt;&lt;value&gt;HELP_DECRYPT.URL&lt;/value&gt;&lt;/
item&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/
operator&gt;&lt;value&gt;HELP_DECRYPT.TXT&lt;/value&gt;&lt;/
item&gt;&lt;item&gt;&lt;field&gt;sample.tasks.file&lt;/
field&gt;&lt;operator&gt;contains&lt;/
operator&gt;&lt;value&gt;HELP_DECRYPT.HTML&lt;/value&gt;&lt;/
item&gt;&lt;/children&gt;&lt;field&gt;sample.sha256&lt;/
field&gt;&lt;/query&gt;</indicator:Description>
              <indicator:Short_Description>Status: enabled</
indicator:Short_Description>
              <indicator:Sightings sightings_count="9676" />
            </indicator:Indicator>
          </indicator:Composite_Indicator_Expression>
          <indicator:Sightings sightings_count="9676" />
          <indicator:Producer>
            <stixCommon:Description />
            <stixCommon:Identity>
              <stixCommon:Name>Palo Alto Networks Unit42</
stixCommon:Name>
            </stixCommon:Identity>
          </indicator:Producer>
        </stix:Indicator>
      </stix:Indicators>
    </stix:STIX_Package>
  </stix>
</res>
```


 ©2023 Palo Alto Networks, Inc.

Get Threat Indicator Feed

Use this resource to retrieve a complete, unsorted list of threat indicators that have been added in the past 24 hours.

- Resource
- JSON Sample

Resource

```
/output/threatFeedResult
```

Request Body Parameters

The following entries describe the body parameters for Get Threat Indicator Feed requests.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**

JSON Sample

- Request
- Response

Request

Include the API key in the request body.

```
curl -XGET -H "apiKey:apikey" -H "Content-Type: application/text"
   https://autofocus.paloaltonetworks.com/api/v1.0/output/
threatFeedResult
```

Response

The response shows a list of threat indicators added in the past 24 hours.

```
{
    c1ecd2eb6353a1b45ca62e575c850fb0d9fcfaf4202adb363ac331e59aeee4eb
ff749295568bf69bb399c8dc5df06bcff2de94d64ab0bf9f30452864560bdfba
186.15.83.52
www.supernetforme.com/search.php?q=2075.2075.300.0.0.a198bb66eec
 6689e36b3ebe6d2fc983415e79e49dd3ad74d697f5bab793cb9e3.1.302754412
www.bb6xndmc6p.com
www.superwebbysearch.com/search.php?q=2070.2070.300.0.0.af98ea42
```


©2023 Palo Alto Networks, Inc.

```
 f248a27d7387a6b344928d442a273bb2ebcec811f7c17d3876014ea2.1.2
 83229881
www.supernetforme.com/search.php?q=2075.2075.300.0.0.2b78ee53771
 e2431d305c279e39249b1c93629a31d13c3f8a0ce51dcc3d33ea5.1.1783
 53990
dqqfuwf.info
5251460f60bbb511769fff86eb5d4b0906131caada00580f7eb6bf21f973aef6
ccvutgpojyr.info
99a0e142e8689a2b24bdc742d284d288ef2437d284c4e628b77cbb5953a75e06
tjsoft.wencyy.top/dot.php?data=oti2odkynjc2njy1njkzmjyyntk1mzm2n
 ji1otq4mju2njm0ndgymzyyntk0mde1njqzndcxmtu2njuymtayody0nti2n
 diznjqzndcxmtk0mdy1njezmjy0nju0mjcxntgynzq4nde0mdy1ndcymzu4m
 juymzqxnda1mzixnze0njm4ndc2mdu4mzgzota2njg0odm5njk1mdyzmzgzo
 tq2mzgymzyznja1mtiymti0ndu0mzywnzuwmzi0ode5ndiznjm4mtq=
www2.megawebdeals.com/search.php?q=1234.2003.280.0.0.b109f20f96a
 cba4c7a7edb880564c2efd3668a955d83c05709b55c32658ba17a.1.6699
 6335
7b1be3641909ece5ed56f6aba38804677f78c77acac5cedf0eb4d7b3942545b5
9fad5cc0a7df8704eddf7b5fe1254a7f9981d12457701a57d011d6804d34f557
a76f5d2d9baa5eb5dcf79884d08d163268c8b9d374ae7e6683a5238422214c0a
36b858d2984cd071818544213cb83a6d1f6c8e2587ad922567834e4782b9ce95
lxmgbnd.info
backupsupport.comxa.com/z/dwn13.dmp
a2dab5947608051dcf4167d5378f2b5ffe0663c7eaa3000d97fd84e43d4377d2
a6cb2ea9e659be63f4c3503719fed2e846b9eb5c848c669b0559227fb6bd08fb
```


©2023 Palo Alto Networks, Inc.

Get Custom Threat Indicator Feed

Use this resource to retrieve the results for a specified custom threat indicator feed. To view this information, you must be in possession of the custom feed URL, as it contains the output feed ID and output feed name; additionally, for custom EDL feeds, you must also have the authentication details associated with the feed.

You can retrieve up to 100,000 IPv4 indicators or 5,000 indicators of all other types, per request. This limitation is based on the maximum number of threat indicators that each feed is capable of processing. For more information about creating custom feeds, refer to: Create Custom Feeds

Resource

- URL Custom Feed—

```
/IOCFeed/{outputFeedId}/{outputFeedName}?limit={max_entries}
```

- EDL Custom Feed—

```
EDL/IOCFeed/{outputFeedId}/{outputFeedName}?limit={max_entries}
```

Request URL Parameters

The following table describes the parameters for Get Custom Threat Intelligence Feed requests.

Parameters	Description	Type	Example or Possible Values
{outputFeedId}	(**Required**) The custom threat feed ID number.	string	Example: **2c9483446d93e094016de0a37f500398**
{outputFeedName}	(**Required**) Name of the custom feed.	string	Example: **urlindicators**
?limit={max_entries}	(**Optional**) Limit the number of indicator entries displayed in the output.	string	Example: **?limit=250**

 ©2023 Palo Alto Networks, Inc.

Request Body Parameters

The following table describes the parameters for Get Custom Threat Intelligence Feed requests.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**

JSON Sample 1

- Request
- Response

Request

Include the output feed ID and the output feed name in the request URL, as well as the API key in the request body.

```
curl -X GET https://autofocus.paloaltonetworks.com/api/v1.0/
IOCFeed/2c9483446d93e094016de0a37f500398/Graywareverdict -H
 "apiKey:apikey"
```

Response

The response displays the indicator IDs for the custom URL feed named Graywareverdict.

```
0048d66d3f4e6cfb2c190087674d76742663668e430094847d6d92b1dc70859d
00ccab21b3357ff53e2dd04cf0cbbabeea72571443b29de40f1d4f688a466388
00f3c157834bf67dcbed2bc4152835c561a61cc760dcc5bf0091a2400c27f852
011e1e93cbe66eae3fc6fcd1d13ae8a3bd862bbb96c13aecfe8d10a90e36c60f
012f2fda4b8efcca162c0d9b140d267f165ea78905cf7c7c24529e7025fcd2dd
0141c6cf2ecd35c1413ceb72fb5b974e601002400e229ae194aea32ebeb2297c
0144d607c470056cbe81ef59255ced1cc4112f69eff4336575e171ed1b93838a
01704ee5950a0cc5a31f97f8e9197214de15665a53e067ebada23045ce0475c6
017daf7bdf367a4a27df0584b232f8e5cac68dcd871fc60bb5ac7ad0fc57700f
0199b38ce4bf6e6a375a16944759bcd0910133d490700a6301842502f2c59445
01a9a8674dbdddf8a960a16d736eabc3c4c676dd29578b623f24be58245b409b
01d5441f50d27154a13da39449d1e59cfac822e99a361ca998e850e029061be9
01e22e1cb7536dd5f77b5a11f939bd541cb5232965d05bb133fca369f6757546
027639a1f0b07a906acdc9012fc2ebd438765c8a367fe7abc4d654e97df934e8
02a0a31135e3a370d8e3af80fbe54a9c1a964481a1e7ddabfcbacda74049ee4e
02df717593c363789e83eafeef2c2de5558bbe01c0d983d6aa900e35ae59439e
030a59ab44b9aab9adbf5223a57bf33600d7472fbdb7d074cee697cb752d759e
0316ba7640df86164788ea20aa696ec50a5e9a07516033ed28dd6ed41062ed82
033d9d38388b1bbbe413c03a3c4b41be8370f4ab366822984f4beda531e0e745
03404b8476d7e9745443554041866dc9265e48264f367c6f12a84d6911263532
```

 ©2023 Palo Alto Networks, Inc.

JSON Sample 2

- Request
- Response

Request

Include the output feed ID and the output feed name in the request URL, as well as the API key in the request body. Additionally, you must also generate and add an authorization header based on the custom EDL feed authentication details to the URL.

To generate an authorization header—In a web browser, open a debugger tool; and then in the console tab, use the following:

```
btoa('username' + ":" + 'password')
```

```
curl -X GET -H "Authorization: Basic TgRCh4ds543hgfD45EDR5rdDF4"
 https://autofocus.paloaltonetworks.com/api/v1.0/EDL/
IOCFeed/2c9483446d93e094016de0a37f500398/Malwareverdict -H
 "apiKey:apikey"
```

Alternatively, you can add the user credentials as a separate parameter:

- *Credentials as a command body parameter:*

```
curl --user {username}:{password} https://
autofocus.paloaltonetworks.com/api/v1.0/EDL/
IOCFeed/2c9483446d93e094016de0a37f500398/Malwareverdict -H
 "apiKey:apikey"
```

Response

The response displays the indicator IDs for the custom URL feed named Malwareverdict.

```
0048d66d3f4e6cfb2c190087674d76742663668e430094847d6d92b1dc70859d
00ccab21b3357ff53e2dd04cf0cbbabeea72571443b29de40f1d4f688a466388
00f3c157834bf67dcbed2bc4152835c561a61cc760dcc5bf0091a2400c27f852
011e1e93cbe66eae3fc6fcd1d13ae8a3bd862bbb96c13aecfe8d10a90e36c60f
012f2fda4b8efcca162c0d9b140d267f165ea78905cf7c7c24529e7025fcd2dd
0141c6cf2ecd35c1413ceb72fb5b974e601002400e229ae194aea32ebeb2297c
0144d607c470056cbe81ef59255ced1cc4112f69eff4336575e171ed1b93838a
01704ee5950a0cc5a31f97f8e9197214de15665a53e067ebada23045ce0475c6
017daf7bdf367a4a27df0584b232f8e5cac68dcd871fc60bb5ac7ad0fc57700f
0199b38ce4bf6e6a375a16944759bcd0910133d490700a6301842502f2c59445
01a9a8674dbdddf8a960a16d736eabc3c4c676dd29578b623f24be58245b409b
01d5441f50d27154a13da39449d1e59cfac822e99a361ca998e850e029061be9
01e22e1cb7536dd5f77b5a11f939bd541cb5232965d05bb133fca369f6757546
027639a1f0b07a906acdc9012fc2ebd438765c8a367fe7abc4d654e97df934e8
02a0a31135e3a370d8e3af80fbe54a9c1a964481a1e7ddabfcbacda74049ee4e
02df717593c363789e83eafeef2c2de5558bbe01c0d983d6aa900e35ae59439e
030a59ab44b9aab9adbf5223a57bf33600d7472fbdb7d074cee697cb752d759e
0316ba7640df86164788ea20aa696ec50a5e9a07516033ed28dd6ed41062ed82
033d9d38388b1bbbe413c03a3c4b41be8370f4ab366822984f4beda531e0e745
```

 ©2023 Palo Alto Networks, Inc.

```
03404b8476d7e9745443554041866dc9265e48264f367c6f12a84d6911263532
```

 ©2023 Palo Alto Networks, Inc.

Get Threat Intelligence Card Summary

Use this resource to retrieve a summary contained in an AutoFocus Threat Intelligence Card. To view this information, you must specify the threat indicator type and value (domains, URLs, file hash, or IP address) and whether you want to include AutoFocus tags in the response.

Resource

```
/tic?
indicatorType={indicator_type}&indicatorValue={value_of_indicator}
    &includeTags={true_or_false}'
```

Request URL Parameters

The following entries describe the URL parameters for Get Threat Intelligence Card Summary requests.

Parameters	Description	Type	Example or Possible Values
{indicatorType}	(**Required**) Type of threat indicator.	string	Possible values: **domain, url, filehash, ipv4_address, ipv6_address**
{indicatorValue}	(**Required**) Value of the threat indicator.	string	Example: **google.com** *The threat indicator value must correspond with the defined indicatorType.*
{includeTags}	(**Required**) Option to include or exclude AutoFocus tags.	string	Possible values: **true, false**

Request Header Parameters

The following entries describe the header parameters for Get Threat Intelligence Card Summary requests.

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**

JSON Sample

- Request
- Response

Request

Include the threat indicator type and value, as well as the option to include tags in the resource URL, and the API key in the request.

```
curl -X GET -H "apiKey: apiKey" "https://
autofocus.paloaltonetworks.com/api/v1.0/tic?
indicatorType=DOMAIN&indicatorValue=exampledomain.com&includeTags=true"
```

Response

The response, which is specific to the threat indicator that you specify in your request, provides a summarization report about the threat, including (as appropriate) the WildFire verdict, sample source, associated tags, domain creation date, the file type, and the first seen date.


```
   {
   "bucketInfo" : {
      "dailyBucketStart" : "2019-11-16 12:03:55",
      "dailyPoints" : 25000,
      "dailyPointsRemaining" : 24990,
      "minuteBucketStart" : "2019-11-16 12:03:55",
      "minutePoints" : 200,
      "minutePointsRemaining" : 190,
      "waitInSeconds" : 0
   },
   "indicator" : {
      "firstSeenTsGlobal" : 1571672361000,
      "indicatorType" : "DOMAIN",
      "indicatorValue" : "exampledomain.com",
      "lastSeenTsGlobal" : 1573856504000,
      "latestPanVerdicts" : {
         "WF_SAMPLE" : "MALWARE"
      },
      "seenByDataSourceIds" : [
         "WF_SAMPLE"
      ],
      "summaryGenerationTs" : 1574114155914,
      "whoisAdminCountry" : null,
      "whoisAdminEmail" : null,
      "whoisAdminName" : null,
      "whoisDomainCreationDate" : null,
```


 ©2023 Palo Alto Networks, Inc.

```
      "whoisDomainExpireDate" : null,
      "whoisDomainUpdateDate" : null,
      "whoisRegistrant" : null,
      "whoisRegistrar" : null,
      "whoisRegistrarUrl" : null,
      "wildfireRelatedSampleVerdictCounts" : {
         "MALWARE" : 99
      }
   },
   "tags": [
{
count: 12081983,
customer_name: "Palo Alto Networks Unit42",
description: "This windows command and/or registry setting adds
an allowed program to bypass the Windows firewall, often used by
malware to ensure c2 traffic
is not blocked by the local firewall.",
doc_count: 1,
lasthit: "2019-01-15 04:38:01",
public_tag_name: "Unit42.ModifyWindowsFirewall",
source: "Unit 42",
tag_class_id: 5,
tag_definition_id: 37576,
tag_definition_scope: "unit42",
tag_definition_scope_id: 4,
tag_definition_status: "enabled",
tag_definition_status_id: 1,
tag_name: "ModifyWindowsFirewall”
},
{
count: 8843812,
customer_name: "Palo Alto Networks Unit42",
description: "Virut is a file-infecting virus that has been in the
wild since 2006. It communicates over IRC to retrieve commands from
it's owner. Virut
variants often infect other malware executables which can lead to
inaccurate signature results. ",
doc_count: 1,
lasthit: "2019-05-14 04:37:53",
public_tag_name: "Commodity.Virut",
source: "Unit 42",
tag_class_id: 3,
tag_definition_id: 27326,
tag_definition_scope: "commodity",
tag_definition_scope_id: 3,
tag_definition_status: "enabled",
tag_definition_status_id: 1,
tag_name: "Virut”
},
{
count: 4928903,
customer_name: "Palo Alto Networks Unit42",
description: "The sample alters the hosts file on a system and
affects the resolution of domain names to IP addresses. This is
often used to prevent a system
```


 ©2023 Palo Alto Networks, Inc.

```
 from reaching a security company's domain for updates. It can also
 be used for phishing attacks.",
 doc_count: 1,
 lasthit: "2019-01-15 04:30:43",
 public_tag_name: "Unit42.ModifyHostsFile",
 source: "Unit 42",
 tag_class_id: 5,
 tag_definition_id: 43791,
 tag_definition_scope: "unit42",
 tag_definition_scope_id: 4,
 tag_definition_status: "enabled",
 tag_definition_status_id: 1,
 tag_name: "ModifyHostsFile",
 }
 ]
 }
}
```


 ©2023 Palo Alto Networks, Inc.

Export List

Use this resource to export threat artifacts that you have already saved in the AutoFocus web portal.

Resource

```
/export/
```

Request Parameters

The following table describes parameters for Export List requests.

Parameters	Description	Type	Example or Possible Values
label	Name of the export list.	string	Valid export list name.
startDate	Specify the start date and time in which to query for saved artifacts. Specify time in Pacific Time.	string	Example: **2015-09-01T00:00:00**
endDate	Specify an end date Pacific Time for saved artifacts.	string	Example: **2015-09-30T00:00:00**
panosFormatted	Format list as a PAN-OS block list.	boolean	Possible values: **true, false** Default value: **false**
exportMetadata	Export metadata.	boolean	Possible values: **true, false** Default value: **false**

 ©2023 Palo Alto Networks, Inc.

Sample Request

Include optional request body parameters, such as **label**, along with your API key to further filter results.

```
curl -X POST -H "Content-Type: application/json" \
-d '{
  "apiKey":"apikey",
  "startDate":"2015-01-01T00:00:00",
  "endDate":"2015-09-30T00:00:00",
  "panosFormatted":true,
  "label":"badurls"
}' 'https://autofocus.paloaltonetworks.com/api/v1.0/export'
```

Sample Response

The PAN-OS formatted response contains a single line for each single IP address, URL, and domain artifact:


```
{
    "export_list": [
        "alabousco.com/en/images/logof.gif?11563=426066",
        "alabousco.com/en/images/logof.gif?1c679=1163450",
        "alabousco.com/en/images/logof.gif?29ecd=1545525",
        "alabousco.com/en/images/logof.gif?37251=1806984",
        "alabousco.com/en/images/logof.gif?45adb=570806",
        "alabousco.com/en/images/logof.gif?52fb6=1019682",
        "aniketkulkarni.in/images/logo.gif?1116d=209991",
        "aniketkulkarni.in/images/logo.gif?1c071=688806",
        "aniketkulkarni.in/images/logo.gif?298d5=1701970",
        "aniketkulkarni.in/images/logo.gif?36bdc=1793760",
        "aniketkulkarni.in/images/logo.gif?45292=2266256",
        "aniketkulkarni.in/images/logo.gif?52ad6=1015938",
        "chonkanya.ac.th/images/logo.gif?1abd8=985752",
        "chonkanya.ac.th/images/logo.gif?25cbf=1548150",
        "chonkanya.ac.th/images/logo.gif?350ec=1955916",
        "chonkanya.ac.th/images/logo.gif?43ffc=1671144",
        "chonkanya.ac.th/images/logo.gif?4f852=1628570",
        "chonkanya.ac.th/images/logo.gif?d815=497853",
        "cmyj.co.th/images/logo.gif?33ea4=1913796",
        "cmyj.co.th/images/logo.gif?4313c=1098992",
        "cmyj.co.th/images/logo.gif?c0af=394616",
        "comsindia.com/images/logo.gif?11821=215139",
        "comsindia.com/images/logo.gif?1c8f9=935880",
        "comsindia.com/images/logo.gif?2a591=1214199",
        "comsindia.com/images/logo.gif?37b27=912540",
        "comsindia.com/images/logo.gif?45e74=2004268",
        "comsindia.com/images/logo.gif?532c2=1022022",
        "dinamikdekor.com/images/logof.gif?10b46=68422",
        "dinamikdekor.com/images/logof.gif?1b144=776412",
        "dinamikdekor.com/images/logof.gif?28bf9=1001430",
        "dinamikdekor.com/images/logof.gif?36048=221256",
        "dinamikdekor.com/images/logof.gif?44d35=1127636",
        "dinamikdekor.com/images/logof.gif?52220=672832",
        "doasoil.gov.np/images/logo.gif?12174=666900",
        "doasoil.gov.np/images/logo.gif?1d825=1087821",
```


 ©2023 Palo Alto Networks, Inc.

```
            "doasoil.gov.np/images/logo.gif?2b3e3=885615",
            "doasoil.gov.np/images/logo.gif?39e9f=1423290",
            "doasoil.gov.np/images/logo.gif?46660=288352",
            "doasoil.gov.np/images/logo.gif?53be6=2058084",
            "doasoil.gov.np/images/logo.gif?a41b=210055",
            "earnestbiz.com/img/logof.gif?12644=301328",
            "earnestbiz.com/img/logof.gif?3a7a3=239523",
            "earnestbiz.com/img/logof.gif?ae67=267882",
            "fotozenistanbul.com/images/logo.gif?12c6c=384540",
            "fotozenistanbul.com/images/logo.gif?1e021=491652",
            "fotozenistanbul.com/images/logo.gif?2c763=1456920",
            "fotozenistanbul.com/images/logo.gif?3b20f=484382",
            "fotozenistanbul.com/images/logo.gif?47770=2927200",
            "fotozenistanbul.com/images/logo.gif?54bce=2776688",
            "fotozenistanbul.com/images/logo.gif?b25d=136983",
            "muaythaiphuketschool.com/logos.gif?11d01=437766",
            "muaythaiphuketschool.com/logos.gif?1d335=717630",
            "muaythaiphuketschool.com/logos.gif?2ac16=700504",
            "muaythaiphuketschool.com/logos.gif?384a9=691707",
            "muaythaiphuketschool.com/logos.gif?46132=861078",
            "muaythaiphuketschool.com/logos.gif?53716=1367128"
        ],
        "bucket_info": {
            "minute_points": 200,
            "daily_points": 25000,
            "minute_points_remaining": 198,
            "daily_points_remaining": 24366,
            "minute_bucket_start": "2015-09-08 19:43:19",
            "daily_bucket_start": "2015-09-08 10:45:00"
        }
}
```


 ©2023 Palo Alto Networks, Inc.

Get Anti-spyware, Vulnerability, and File-Format Signature

Use this resource to get anti-spyware, vulnerability, and file-format signature info based on the specified signature ID.

Resource

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/signature/{signature_id}
```

Request Parameters

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**

{signature_id}	(Required) The identification number of an anti-spyware, vulnerability, or file-format signature.	string	The threat ID range for anti-spyware, vulnerability, and file-format signatures.
			• **Anti-spyware Signatures**
			  • Threat ID Range: 80001-89999
			  • Custom threat ID Range: 15000-18000
			  • Additional threat ID range used for custom signatures; added in PAN-OS 10.0: 6900001-7000000
			• **Vulnerability Signatures**
			  • Threat ID Range: 90000-99999
			  • Custom threat ID Range: 41000-45000
			  • Additional threat ID range used for custom signatures; added

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			in PAN-OS 10.0: 6800001 -6900000 • **File-Format Signatures** • Threat ID Range: 52000-52800 *Refer to the following Knowledge Base article for a complete reference list:* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEtCAK Example: `56285`

JSON Sample

- Request
- Response

Request

Include the API key and vulnerability signature ID number in the resource URL.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/
v1/threatvault/ips/signature/56285?api_key=apiKey" -H "accept:
 application/json"
```

Response

The response contains details about the vulnerability signature.

```
{
  "signatureName": "Microsoft Graphics Component Information
 Disclosure Vulnerability",
  "signatureId": 56285,
  "signatureType": "vulnerability",
  "cve": "CVE 2019-1153",
  "vendor": "",
  "firstReleaseVersion": 8183,
  "firstReleaseTime": "2019-08-17 UTC",
  "latestReleaseVersion": 8183,
  "latestReleaseTime": "2019-08-17 UTC",
  "status": "released",
```

 ©2023 Palo Alto Networks, Inc.

```
  "metadata": "\"severity\":\"medium\",\"reference\":\"avd\""
}
```

 ©2023 Palo Alto Networks, Inc.

Get Antivirus Signature

Use this resource to get antivirus signature info based on the specified signature ID or SHA256 value.

Resource

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/
panav/signature/{antivirus_signature_id}
```

```
https://autofocus.paloaltonetworks.com/api/intel/v1/file/{sha256}/
signature
```

Request Parameters

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
{antivirus_signature_id}	(Required for /panav/signature/) The identification number of an antivirus signature.	string	The ID range for antivirus signatures are based on the file type. • PE: 2000000-2900000 • PDF: 1100000-1102000 • APK: 1000000-1015000 • DNS: 4000000-4100000 • Office/RTF: 1110000-1140000 • JAVA Class: 1250000-1253000 • Flash: 1270000-1273000 • OpenOffice: 1210000-1225000 • SWFZWS: 6000000-60000500 • PKG: 1050000-1055000 • MACH-O: 1060000-106200

 ©2023 Palo Alto Networks, Inc.

Parameters	Description	Type	Example or Possible Values
			• APP: 1070000-1071000 • DMG: 60100000-6015000 Example: `93544016` *Antivirus signatures that are not associated with the file types shown above can have an ID number that exceeds the range defined in this table.*
{sha256}	(Required for /file/{sha256}/signature) The SHA256 hash value of a sample.	string	Valid SHA256 hash. Example: `eb4559d2debb5de11b3a90536ef36709de394`

JSON Sample 1

- Request
- Response

Request

Include the API key and antivirus signature ID number in the resource URL.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/v1/
threatvault/panav/signature/1065689?api_key=apiKey" -H "accept:
 application/json"
```

Response

The response contains details about the antivirus signature.

```
[
  {
    "signatureName": "Worm/Win32.autorun.crck",
    "signatureId": "93534285",
    "createTime": "2010-10-01 10:28:57(UTC)",
    "active": false,
    "sha256": [

 "7a520be9db919a09d8ccd9b78c11885a6e97bc9cc87414558254cef3081dccf8"
    ],
```

 ©2023 Palo Alto Networks, Inc.

```
    "release": {
      "wildfire": {
        "latestReleaseVersion": n/a,
        "latestReleaseTime": n/a,
        "firstReleaseVersion": 316,
        "firstReleaseTime": "2011-04-05 UTC"
      },
      "antivirus": {
        "latestReleaseVersion": n/a,
        "latestReleaseTime": n/a,
        "firstReleaseVersion": 316,
        "firstReleaseTime": "2011-04-05 UTC"
      }
    }
  }
]
```

JSON Sample 2

- Request
- Response

Request

Include the API key and SHA256 hash in the resource URL.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/v1/
file/050aef130c079f10a2549b3f948c5d6548bfd33e0dee4fa264300de57ba619da/
signature?api_key=apiKey" -H "accept: application/json"
```

Response

The response contains details about the antivirus signature.

```
[
  {
    "signatureName": "Adware/Win32.zango.crck",
    "signatureId": "94674345",
    "createTime": "2011-02-16 19:37:56(UTC)",
    "active": false,
    "sha256": [

 "050aef130c079f10a2549b3f948c5d6548bfd33e0dee4fa264300de57ba619da"
    ],
    "release": {
      "wildfire": {
        "latestReleaseVersion": n/a,
        "latestReleaseTime": n/a,
        "firstReleaseVersion": 418,
        "firstReleaseTime": "2011-04-21 UTC"
      },
      "antivirus": {
        "latestReleaseVersion": n/a,
```

 ©2023 Palo Alto Networks, Inc.

```
        "latestReleaseTime": n/a,
        "firstReleaseVersion": 418,
        "firstReleaseTime": "2011-04-21 UTC"
      }
    }
  }
]
```


 ©2023 Palo Alto Networks, Inc.

Get DNS Signature

Use this resource to get DNS and RTDNS signature info based on the specified signature ID.

Resource

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/dns/
signature/{DNS_RTDNS_signature_id}
```

Request Parameters

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
{DNS_signature_id}	(**Required**) The identification number of a DNS/RTDNS signature.	string	The threat ID for DNS/RTDNS signature. Example: `325235352`

JSON Sample

Request

Include the API key and DNS signature ID number in the resource URL.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/v1/
threatvault/dns/signature/109000001?api_key=apiKey" -H "accept:
 application/json"
```

 ©2023 Palo Alto Networks, Inc.

Response

The response contains details about the DNS signature.


```
{
  "domainName": "wwiyudruofdsu439.com",
  "signatureId": 109000001,
  "signatureName": "Real-Time DNS Detection: DGA",
  "category": "rtdns",
  "createTime": "2018-07-23 23:58:42(UTC)",
  "active": true,
  "release": {
    "wildfire": {
      "latestReleaseVersion": n/a,
      "latestReleaseTime": n/a,
      "firstReleaseVersion": n/a,
      "firstReleaseTime": n/a
    },
    "antivirus": {
      "latestReleaseVersion": n/a,
      "latestReleaseTime": n/a,
      "firstReleaseVersion": n/a,
      "firstReleaseTime": n/a
    }
  }
}
```


 ©2023 Palo Alto Networks, Inc.

Get Geolocation

Use this resource to get geolocation information based on the specified IP address.

- Resource
- Request Parameters
- JSON Sample

Resource

```
https://autofocus.paloaltonetworks.com/api/intel/v1/ip/{ip_address}/
geolocation
```

Request Parameters

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
{ip_address}	(Required) The IP address from which you want to retrieve the geolocation information.	string	A valid IP address. Example: `1.1.1.1`

JSON Sample

- Request
- Response

Request

Include the API key and IP address in the resource URL.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/v1/
ip/1.1.1.2/geolocation?api_key=apiKey" -H "accept: application/json"
```

 ©2023 Palo Alto Networks, Inc.

Response

The response contains the geolocation information related to an IP address.


```
{
  "Ip_address": "1.1.1.2",
  "Geolocation": "AU (Australia)",
  "Autonomous_system": "13335 (CLOUDFLARENET - Cloudflare, Inc.,
 US)",
  "Status": "N/A",
  "Feed_Name": "",
  "First_release": ""
}
```


 ©2023 Palo Alto Networks, Inc.

Get Anti-spyware, Vulnerability, and File-Format Release Info

Use this resource to get the release information associated with anti-spyware, vulnerability, and file-format signatures. This includes new signature additions, modifications, deletions, as well a list of unchanged entries.

Resource

Request Parameters

```
https://autofocus.paloaltonetworks.com/api/intel/v1/threatvault/ips/release/{release_id}
```

The following table describes the parameters used with this endpoint.

Parameters	Description	Type	Example or Possible Values
apiKey	(**Required**) API key tied to your license. All users attached to a license share a single API key.	string	Example (obfuscated): **d32108a5-XXX-XXXX-XXXX-c04bda5b8450**
{release_id}	(Required) The identification number of the release containing the anti-spyware, vulnerability, and file-format signatures.	string	The release identification number. Example: `107`

JSON Sample

 ©2023 Palo Alto Networks, Inc.

Request

Include the API key and release ID number in the resource URL to view the anti-spyware, vulnerability, and file-format signature update contents.

```
curl -X GET "https://autofocus.paloaltonetworks.com/api/intel/v1/
threatvault/ips/release/8250?api_key=apiKey" -H "accept: application/
json"
```

Response

The response contains the signature update details for the specified release ID.

```
{
  "releaseVersion": 8250,
  "releaseNotes": "Reminders: (3/10/2020) Palo Alto Networks
 announced new App-IDs that we will release with the content update
 later today. Customers running a PAN-OS 8.1 or later release are
 encouraged to leverage an Application Filter to adopt new App-IDs.",
  "releaseSignatures": {
    "vulnerabilitySignatures": {
      "newSignatures": [
    "fileformatSignatures": {
      "newSignatures": [
        1,
        2,
        3
      ],
      "modifiedSignatures": [
        1,
        2,
        3
      ]
    }
  }
}
```

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

AutoFocus API Error Codes

AutoFocus™ API operations return standard HTTP status codes as defined by the HTTP/1.1 standard. Where applicable, error codes also include messages to help you diagnose the nature of the issue.

AutoFocus API Error Codes

The following table provides a list of standard HTTP status codes that AutoFocus uses when returning errors. An accompanying error messages includes additional details for clarification.

HTTP Status Code	Meaning
200	No errors. Successful call
404	Invalid URL. Example: `{"code": 404, "error": "Error 404 Not Found", "error_description":"The requested URL was not found on this server." }`

409	Invalid message or missing parameters. For example, if the scope is invalid, the corresponding error looks like this:
	`{ "message": "invalid scope" }`
	If parameters are missing, the corresponding error looks like this:
	`{"message": "Missing Body Parameters: [\"scope \"]" }`
	If the license has expired or is otherwise invalid, the corresponding error looks like this:
	`{ mwStatus: 409, mwMessage: 'Invalid license' }`

500	Internal error.
503	Rate limit exceeded. Example: `{"message": "Minute Bucket Exceeded", "bucket_info": { "minute_points":200, "daily_points": 25000, "minute_bucket_start": "2015-09-13 01:23:23","daily_bucket_start": "2015-09-12 14:47:43", "minute_points_remaining":0, "daily_points_remaining": 24715, "wait_in_seconds": 53.086 }}`

 ©2023 Palo Alto Networks, Inc.