Infoblox®
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

ActiveTrust Platform

Dossier and TIDE

Quick Start Guide
NIOS 8.1

Table of Contents

Overview

Infoblox ActiveTrust uses highly accurate machine-readable threat intelligence data via a flexible Threat Intelligence Data Exchange (TIDE) to aggregate, curate, and enable distribution of data across a broad range of infrastructure. TIDE enables organizations to ease consumption of threat intelligence from various internal and external sources, and to effectively defend against and quickly respond to cyberthreats. TIDE is backed by the Infoblox threat intelligence team that normalizes and refines high-quality threat intelligence data feeds.

Dossier™ is a threat indicator research tool that gives contextual information from a dozen sources (including TIDE) simultaneously, empowering users to make accurate decisions more quickly and with greater confidence.

The document contains a high-level overview how to use ActiveTrust Dossier and TIDE.

Prerequisites

ActiveTrust Dossier and TIDE are subscription-based services provided in Infoblox Cloud. There are no specific requirements for software to access the services except a relevant subscription. Recent versions of Google Chrome are recommended to access ActiveTrust portal.

ActiveTrust Dossier and TIDE common Web-interface

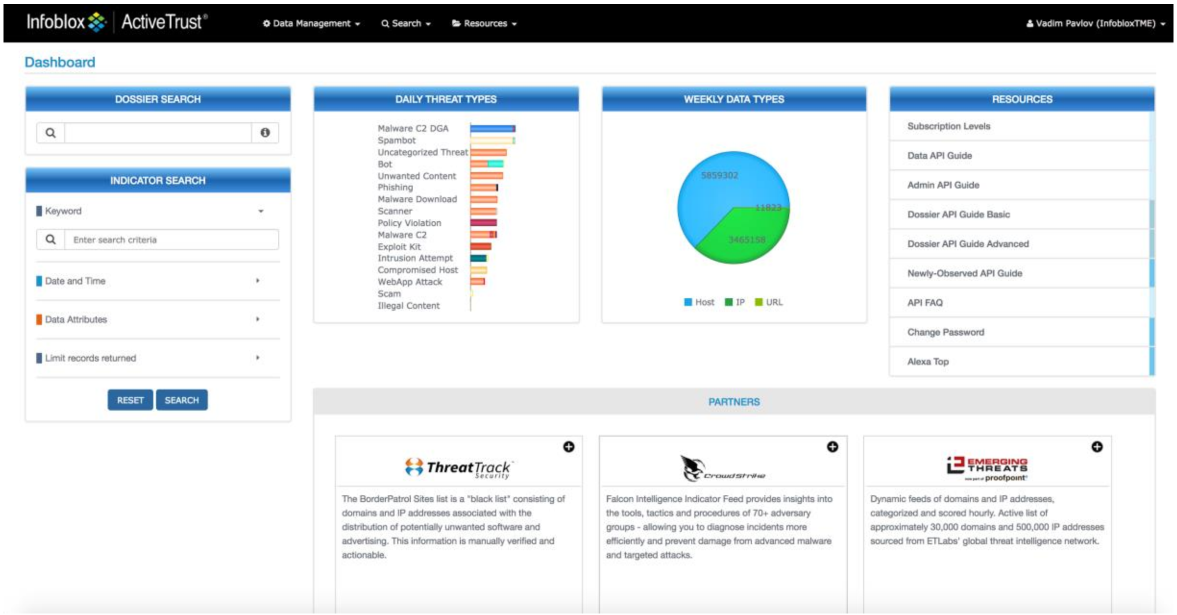
Access to the ActiveTrust portal

ActiveTrust Dossier and TIDE can be accessed on https://platform.activetrust.net You can get to Dossier on https://csp.infoblox.com under the “Analyze” section. These sites are respectively referred to as The Portal and CSP.

The Portal is not integrated with CSP and separate credentials are required. Your credentials are provided in a welcome email when your account is created.

Home dashboard and navigation menu

The navigation menu is located on the top of the screen and provides an access to all functions of the portal. It consists of “Data Management”, “Search”, “Resources” and user’s profile sub-menus.



The BorderPatrol Sites list is a "black list" consisting of domains and IP addresses associated with the distribution of potentially unwanted software and advertising. This information is manually verified and actionable.

Falcon Intelligence Indicator Feed provides insights into the tools, tactics and procedures of 70+ adversary groups - allowing you to diagnose incidents more efficiently and prevent damage from advanced malware and targeted attacks.

Dynamic feeds of domains and IP addresses, categorized and scored hourly. Active list of approximately 30,000 domains and 500,000 IP addresses sourced from ETLabs' global threat intelligence network.

- “Data Management” provides access to data governance and submission tools, link to the dashboard and Alexa Top domains.
- “Search”: provides an access to Dossier and Indicator searches.
- “Resources” contains API guides, Threat Classification Guide, default threat indicators TTLs and description of the subscription levels.
- “Your username”: sub-menu with metric reports and user settings.

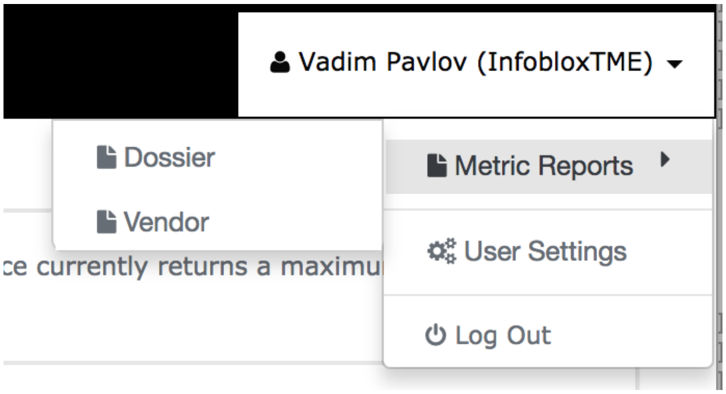
On the home dashboard you can find:

- Dossier search widget - a shortcut to start a Dossier search.
- Indicator search widget - a shortcut to perform an Infoblox Threat Indicator search.
- Daily Threat Types and Weekly Data Types widgets - provide information about daily and weekly Infoblox published IOC’s discovered/added by our Cyber Threat Intelligence team.
- “Resources” widget provides shortcuts to popular resource links.
- Partners widgets provide overview information about premium partner data feeds which are part of the TIDE marketplace and can be purchased “a la carte”.
- By selecting “ActiveTrust” in the upper left corner you can return to the start page/dashboard.

User Settings and Metric Reports

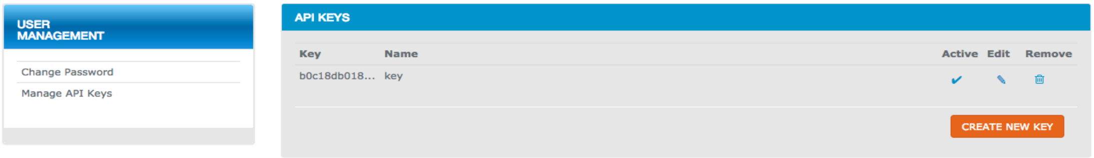
Metric Reports

Subscriptions includes limited number of Dossier and partners’ searches. Statistics per user, organization, partners, and dossier transactions are provided in “Metric Reports”. The menu is available only to organization’s administrators.



User Settings

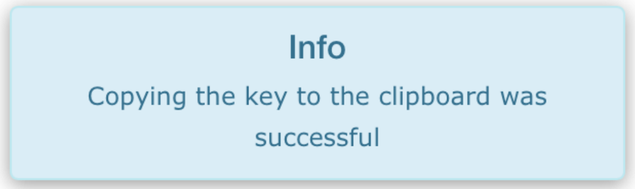
On the User Management page, you can change your password and manage API Keys. The passwords must satisfy the requirements described on the “Change Password” page.



Key	Name	Active	Edit	Remove
b0c18db018...	key	✓	✎	🗑

API keys are required to access Dossier and TIDE via REST API. A user can create multiple API keys. There are no any specific permissions related to a key. Only the key name and description can be changed. A key may be deactivated or deleted. In order to copy the key you can:

- Click on a key. Info window “Copying the key to the clipboard was successful” will be displayed.
- Edit a key



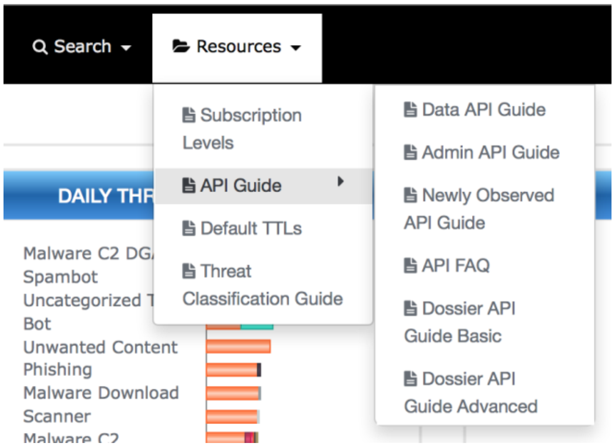
Info

Copying the key to the clipboard was successful

Refer to the next section RESOURCES for examples of API key usage.

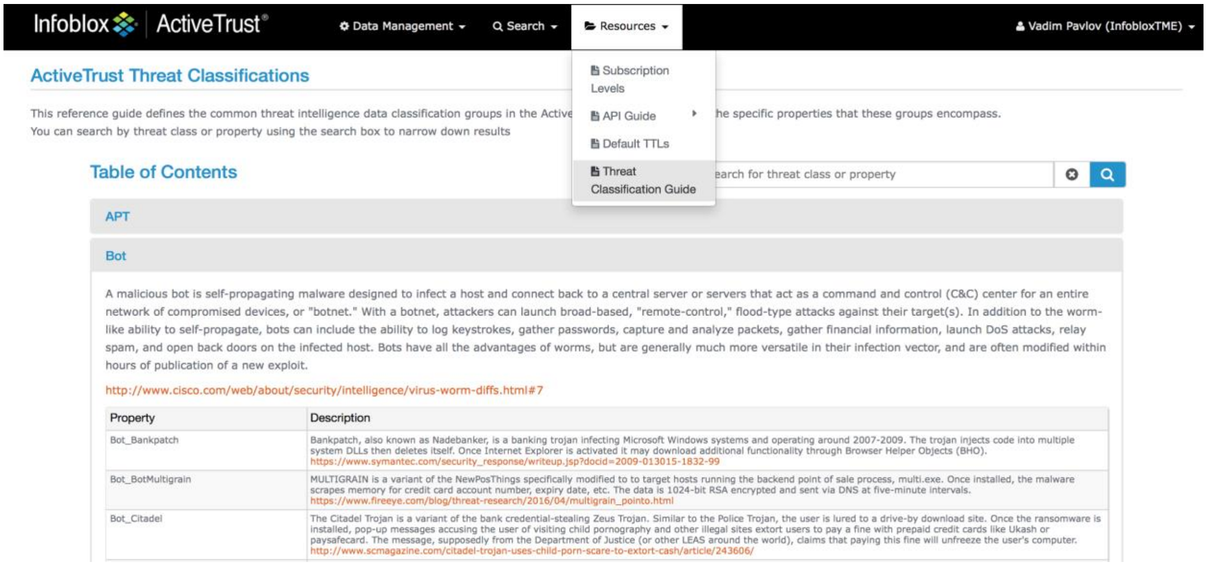
Resources

Under the Resources menu you can find APIs and Threat Classification Guide. API Guides are toolkits which help you build API calls and review retrieved data.



The required API key can be obtained as described in the “User Settings” chapter.

Threat indicators returned by a search contain “Class” and “Property” fields e.g. class “Bot” and property “Bot_Bankpatch”. “Threat Classification Guide” contains descriptions of all classes and properties supported by Dossier and TIDE.



ActiveTrust Threat Classifications

This reference guide defines the common threat intelligence data classification groups in the Active he specific properties that these groups encompass.
You can search by threat class or property using the search box to narrow down results

Table of Contents

APT

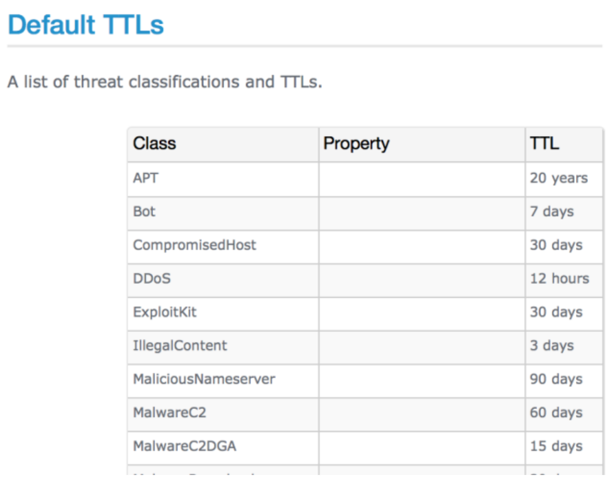
Bot

A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit.

http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#7

Property	Description
Bot_Bankpatch	Bankpatch, also known as Nadebanker, is a banking trojan infecting Microsoft Windows systems and operating around 2007-2009. The trojan injects code into multiple system DLLs then deletes itself. Once Internet Explorer is activated it may download additional functionality through Browser Helper Objects (BHO). https://www.symantec.com/security_response/writeup.jsp?docid=2009-013015-1832-99
Bot_BotMultigrain	MULTIGRAIN is a variant of the NewPosThings specifically modified to to target hosts running the backend point of sale process, multi.exe. Once installed, the malware scrapes memory for credit card account number, expiry date, etc. The data is 1024-bit RSA encrypted and sent via DNS at five-minute intervals. https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
Bot_Citadel	The Citadel Trojan is a variant of the bank credential-stealing Zeus Trojan. Similar to the Police Trojan, the user is lured to a drive-by download site. Once the ransomware is installed, pop-up messages accusing the user of visiting child pornography and other illegal sites extort users to pay a fine with prepaid credit cards like Ukash or paysafecard. The message, supposedly from the Department of Justice (or other LEAS around the world), claims that paying this fine will unfreeze the user's computer. http://www.scmagazine.com/citadel-trojan-uses-child-porn-scare-to-extort-cash/article/243606/

Each threat indicator belongs to a specific class and has a default expiration time (TTL). Expired threat indicators are still available in the database and returned by a search but they are not included in the ActiveTrust/DNS Firewall feeds. The Cyber Threat Intelligence team periodically checks the indicators for validity and accuracy.
Default expiration time for all classes are provided on “Default TTLs” page.



Default TTLs

A list of threat classifications and TTLs.

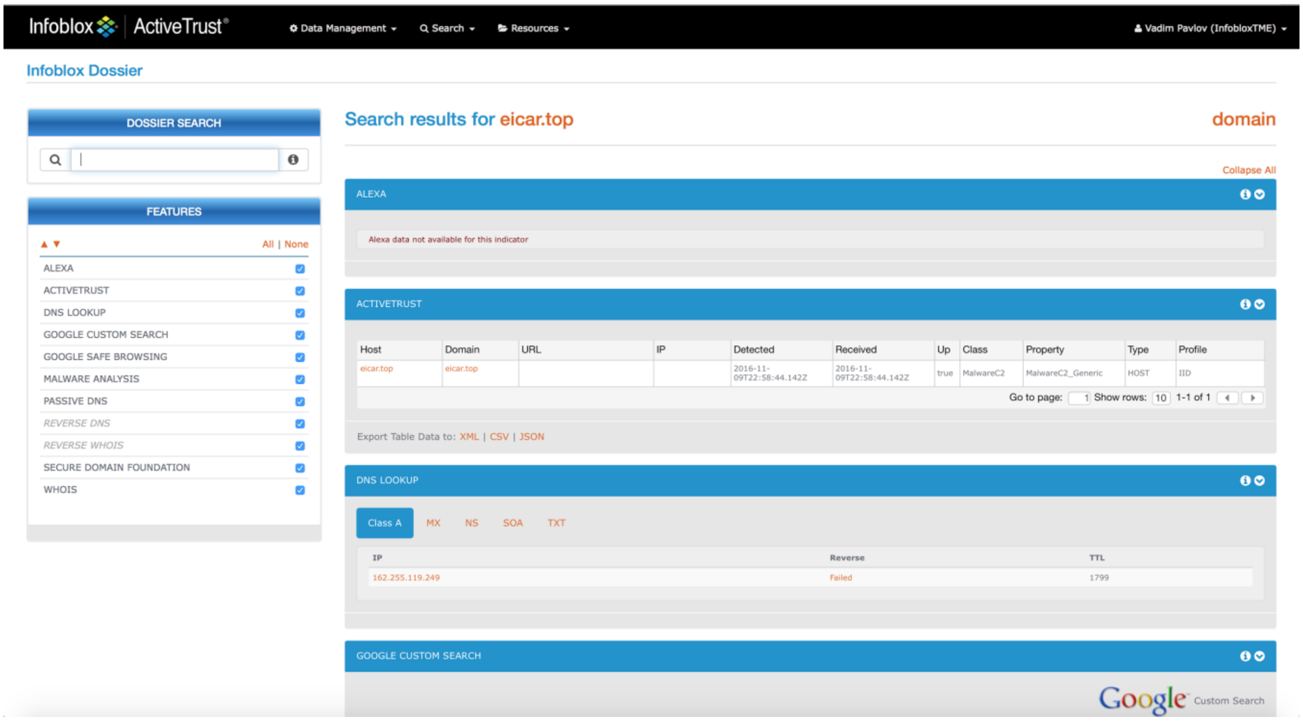
Class	Property	TTL
APT		20 years
Bot		7 days
CompromisedHost		30 days
DDoS		12 hours
ExploitKit		30 days
IllegalContent		3 days
MaliciousNameserver		90 days
MalwareC2		60 days
MalwareC2DGA		15 days

Dossier

Dossier search is available via the web-interface and a REST API. The portal uses the same API so there is no difference in available filters and search results between Web and API searches.

Dossier Search

You can use the following items in the Dossier search field: IPs, URLs, Domains, Hostnames, Email addresses, and MD5, SHA1, and SHA256 hashes. Not all features/data providers support all data types, e.g. Alexa supports only hostnames and domains.



Search results for eicar.top

domain

FEATURES:

- ALEXA ☑
- ACTIVETRUST ☑
- DNS LOOKUP ☑
- GOOGLE CUSTOM SEARCH ☑
- GOOGLE SAFE BROWSING ☑
- MALWARE ANALYSIS ☑
- PASSIVE DNS ☑
- *REVERSE DNS* ☑
- *REVERSE WHOIS* ☑
- SECURE DOMAIN FOUNDATION ☑
- WHOIS ☑

ALEXA

Alexa data not available for this indicator

ACTIVETRUST

Host	Domain	URL	IP	Detected	Received	Up	Class	Property	Type	Profile
eicar.top	eicar.top			2016-11-09T22:58:44.142Z	2016-11-09T22:58:44.142Z	true	MalwareC2	MalwareC2_Generic	HOST	IID

Go to page: 1 Show rows: 10 1-1 of 1

Export Table Data to: XML | CSV | JSON

DNS LOOKUP

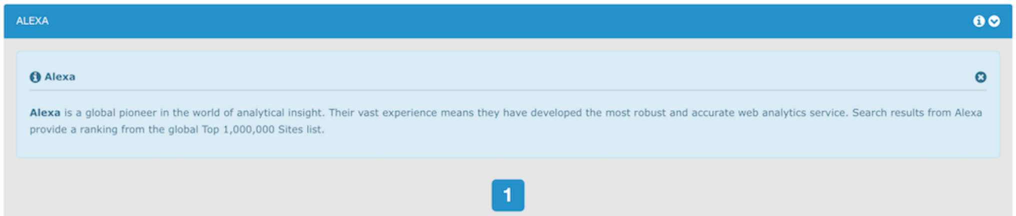
Class A MX NS SOA TXT

IP	Reverse	TTL
162.255.119.249	Failed	1799

Dossier automatically detects type of the data in a search field and performs only relevant searches. It is intelligent enough and it is possible to enter domains in this format "example[.]com".

“Features” sidebar provides an ability to select only required features.

A brief description of a feature is provided if you hover a mouse pointer over ⓘ icon.



Alexa is a global pioneer in the world of analytical insight. Their vast experience means they have developed the most robust and accurate web analytics service. Search results from Alexa provide a ranking from the global Top 1,000,000 Sites list.

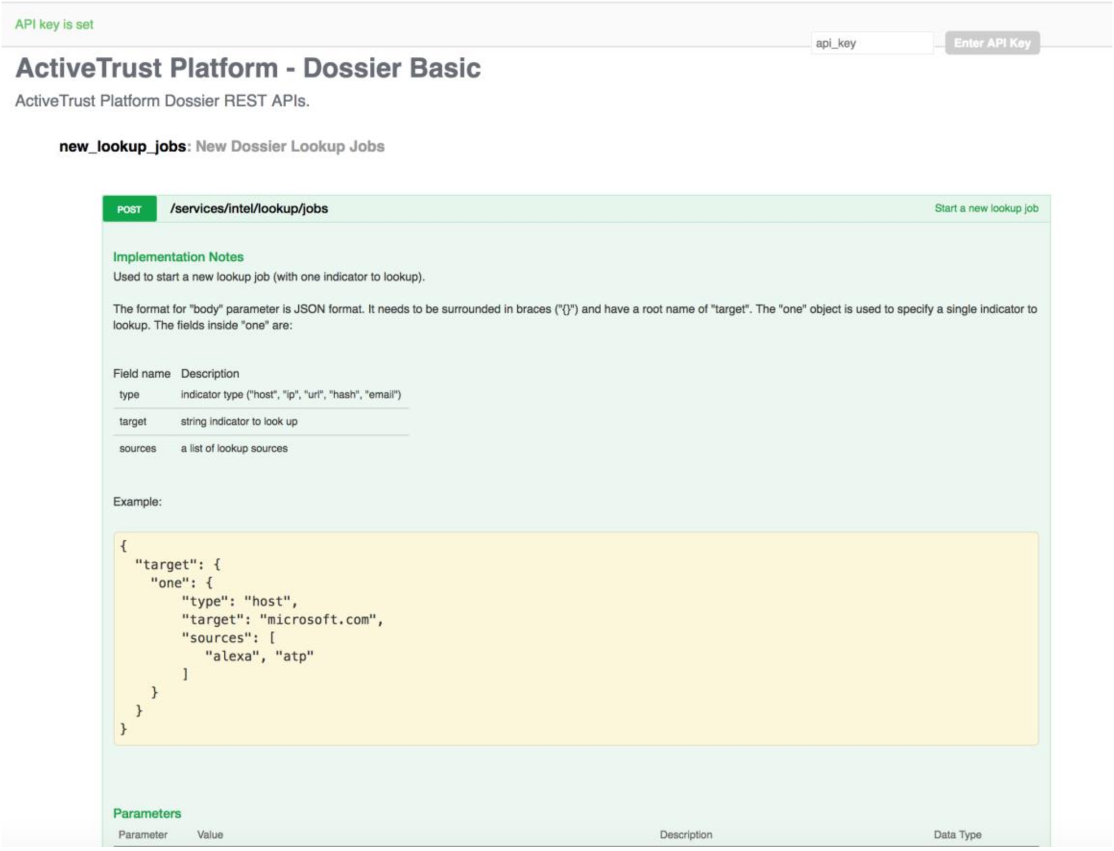
Dossier API

Customers commonly use Dossier API Basic. It provides access to all information available on the portal. Dossier API Basic Guide describes all available filters and options. Before using Dossier API Guide you need to enter an API Key in “api_key” field.

The API keys are configured on “User Settings” → “Manage API Keys” page.

The ActiveTrust platform leverages the Basic Auth method in HTTP/HTTPS to transport the API key.

The API key is passed in the username field. The password field should be set to an empty string.



ActiveTrust Platform - Dossier Basic

ActiveTrust Platform Dossier REST APIs.

new_lookup_jobs: New Dossier Lookup Jobs

/services/intel/lookup/jobs

Implementation Notes

Used to start a new lookup job (with one indicator to lookup).

The format for "body" parameter is JSON format. It needs to be surrounded in braces ("{}") and have a root name of "target". The "one" object is used to specify a single indicator to lookup. The fields inside "one" are:

Field name	Description
type	indicator type ("host", "ip", "url", "hash", "email")
target	string indicator to look up
sources	a list of lookup sources

Example:

```
{
  "target": {
    "one": {
        "type": "host",
        "target": "microsoft.com",
        "sources": [
           "alexa", "atp"
        ]
    }
  }
}
```

Parameters

Parameter	Value	Description	Data Type

When you execute a test query, API Guide returns: a CURL command to request the data, response body and response code. The listing below contains a sample CURL command which retrieves information about “eicar.top” domain in JSON format, which is the only supported export format for API based indicator search

```
curl -H "Content-Type":"application/json" -X POST
"https://platform.activetrust.net:8000/api/services/intel/lookup/jobs?wait=true" -u <User_API_Key>: -d
'{"target":{"one":{"type": "host","target": "eicar.top", "sources":
["alexa","atp","dns","gcs","gsb","malware_analysis","pdns","ptr","rwhois","sdf","whois"]}}}'
```

It takes some time to retrieve data in case if the data is not required immediately a search can be executed with “wait” parameter set to “false” and retrieved later using Dossier API Advanced call. In this case the first search (Basic API call) will return “job_id”. The status of the job and results can be retrieved using Advanced API “lookup_jobs_management” calls. The URL below retrieves results of a job with “job_id” parameter.

https://platform.activetrust.net:8000/api/services/intel/lookup/jobs/**job_id**/results

Dossier Advanced API provides these API calls:

- Lookup Jobs APIs (lookup_jobs_management) API calls - return status and results of the lookup jobs.
- Lookup Job Index (lookup_jobs_index) API calls - return list of the performed searches per user or organization.

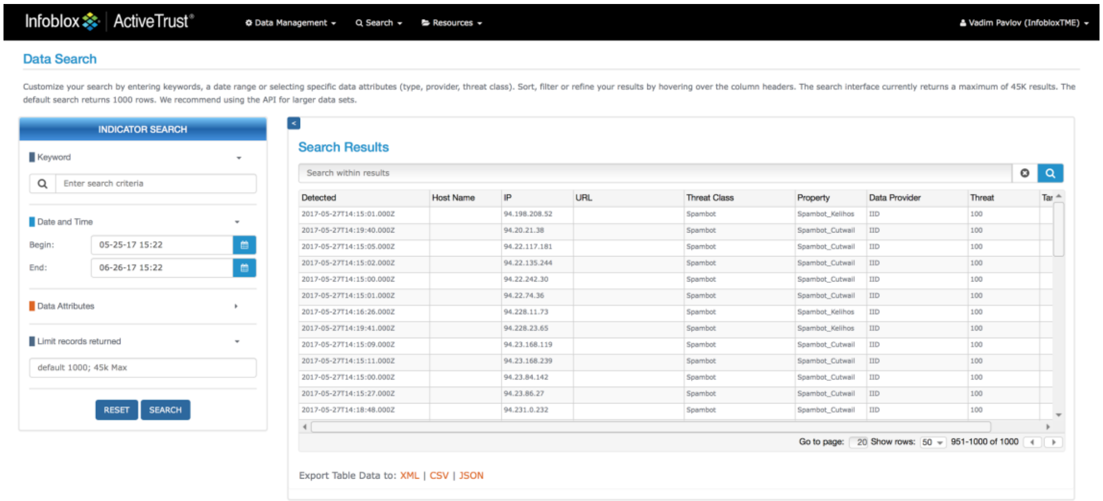
- Worker Status (worker_stats) API calls - provide statistics per source, e.g. alexa, atp, dns etc.
- Service Metadata (service_metadata) API calls - return information about supported sources, targets, supported sources by targets and targets descriptions.

Infoblox Threat Intelligence Data Exchange (TIDE)

Infoblox Threat Intelligence Data Exchange provides an access to highly curated threat indicators and data governance tools to share indicators inside the organization and/or between the organizations.

Indicator Search

Indicator search versus Dossier search returns data only from ActiveTrust database but the search is not limited to a specific indicator (e.g. a hostname). The search interface currently returns a maximum of 45 thousand results. It is recommended to use API for larger data sets.



Data Search

Customize your search by entering keywords, a date range or selecting specific data attributes (type, provider, threat class). Sort, filter or refine your results by hovering over the column headers. The search interface currently returns a maximum of 45K results. The default search returns 1000 rows. We recommend using the API for larger data sets.

Begin: 05-25-17 15:22

End: 06-26-17 15:22

Detected	Host Name	IP	URL	Threat Class	Property	Data Provider	Threat	Tar
2017-05-27T14:15:01.000Z		94.198.208.52		Spambot	Spambot_Kelihos	IID	100	
2017-05-27T14:19:40.000Z		94.20.21.38		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:05.000Z		94.22.117.181		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:02.000Z		94.22.135.244		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:00.000Z		94.22.242.30		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:01.000Z		94.22.74.36		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:16:26.000Z		94.228.11.73		Spambot	Spambot_Kelihos	IID	100	
2017-05-27T14:19:41.000Z		94.228.23.65		Spambot	Spambot_Kelihos	IID	100	
2017-05-27T14:15:09.000Z		94.23.168.119		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:11.000Z		94.23.168.239		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:00.000Z		94.23.84.142		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:15:27.000Z		94.23.86.27		Spambot	Spambot_Cutwail	IID	100	
2017-05-27T14:18:48.000Z		94.231.0.232		Spambot	Spambot_Cutwail	IID	100	

Go to page: 20 Show rows: 50 951-1000 of 1000

Export Table Data to: XML | CSV | JSON

Because of size of the available data, it is recommended to apply filters to limit the resulting dataset.

When a keyword is used to search data other filters are not applied even if they were specified.

The result dataset can be exported in XML, CSV or JSON format.

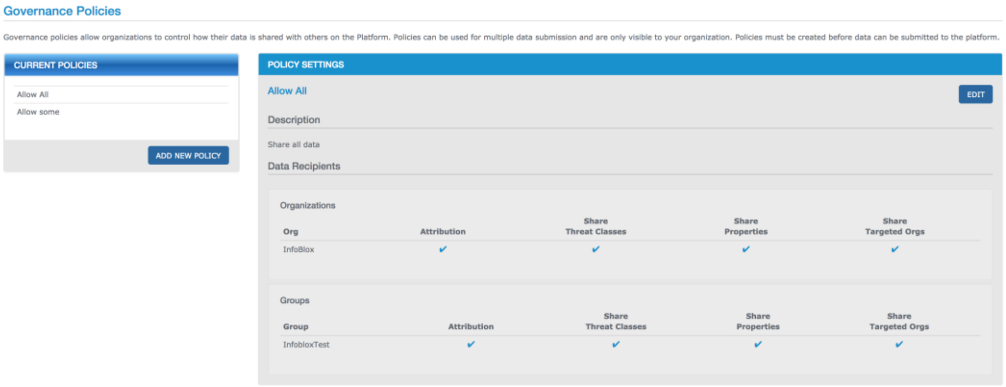
Data Management

Alexa Top

Alexa top is a rank of the most used sites in the Internet. This tool provides an access to Alexa Top 10000 sites.

Governance policies and data submission

Customers can submit/upload own threat indicators and share them with other organizations or groups that they have rights to. Submitted data is available via Dossier and Indicator searches on the portal and Data API. Data Governance Policies allow organizations to control how their submitted data is shared with other organizations or groups on the platform. Infoblox can enable access/data share between organizations by a request. Policies can be used for multiple data submissions and are only visible within your organization.



Governance Policies

Governance policies allow organizations to control how their data is shared with others on the Platform. Policies can be used for multiple data submission and are only visible to your organization. Policies must be created before data can be submitted to the platform.

Allow All

Description

Share all data

Data Recipients

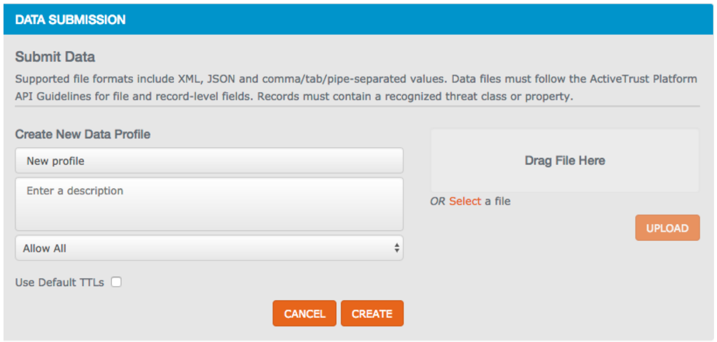
Organizations

Org	Attribution	Share Threat Classes	Share Properties	Share Targeted Orgs
InfoBlox	✓	✓	✓	✓

Groups

Group	Attribution	Share Threat Classes	Share Properties	Share Targeted Orgs
InfobloxTest	✓	✓	✓	✓

Data profiles are used to identify data in the platform from one or many data submissions. A data profile must be specified when data is submitted. Data profiles are associated with governance policies, which control who can access the data. When a data profile is created it must be associated with a governance policy.



Submit Data

Supported file formats include XML, JSON and comma/tab/pipe-separated values. Data files must follow the ActiveTrust Platform API Guidelines for file and record-level fields. Records must contain a recognized threat class or property.

Create New Data Profile

New profile

Enter a description

Allow All

Use Default TTLs □

Users can submit threat indicators on the portal or via Data API.
In order to submit data you should create:

1. A governance policy - defines how data is shared;
2. A data profile - defines if standard TTL should be used and a governance policy.

Users can submit data using the following formats: JSON, CSV, XML, TSV (tab separated values). For all data formats the submitted data must identify the data/record type in addition to the list of data records. For CSV and TSV the record type must be provided as one of the columns. For JSON and XML the record type is defined in a separate top level field. The record type field can be one of the following values: "host", "ip", or "url". It is not possible to upload data using different profiles or different record types in the same file. Threat data consists of file-level fields and record-level fields. The table below contains descriptions of all available fields.

Field name	Description
File-level fields	
profile	data profile id or name
record_type	host, ip, or url
external_id	string indicating an external ID to assign to the batch
record	surrounds the individual record(s) in the XML and JSON formats
Record-level fields	
host	threat hostname
ip	threat IP address
url	threat URL
property	threat type
target	target of threat
detected	date/time threat was detected, in ISO 8601 format
duration	duration of this threat in XyXmXwXdXh format, expiration date will be set to the detected date + this duration

The listing below contains a sample data submission in XML format.

```
<feed>
  <profile>SampleProfile</profile>
  <record_type>ip</record_type>
  <record>
    <ip>127.1.0.1</ip>
    <property>Phishing_Phish</property>
    <detected>20170602T154742Z</detected>
  </record>
  <record>
    <ip>8.8.8.8</ip>
    <property>Scanner_Generic</property>
    <detected>19980927T154242Z</detected>
    <duration>42y0m0w0d42h</duration>
  </record>
</feed>
```

The listing below contains a sample data submission in JSON format.

```
{
   "feed": {
     "profile": "SampleProfile",
     "record_type": "host",
     "record": [
      {"host": "www.google.com", "property": "Scanner_Generic", "detected": "19980927T154242Z",
"duration":"42y0m0w0d42h"},
      {"host": "www.example.com", "property": "Phishing_Phish", "detected": "20170602T154742Z"}
      ]
     }
}
```

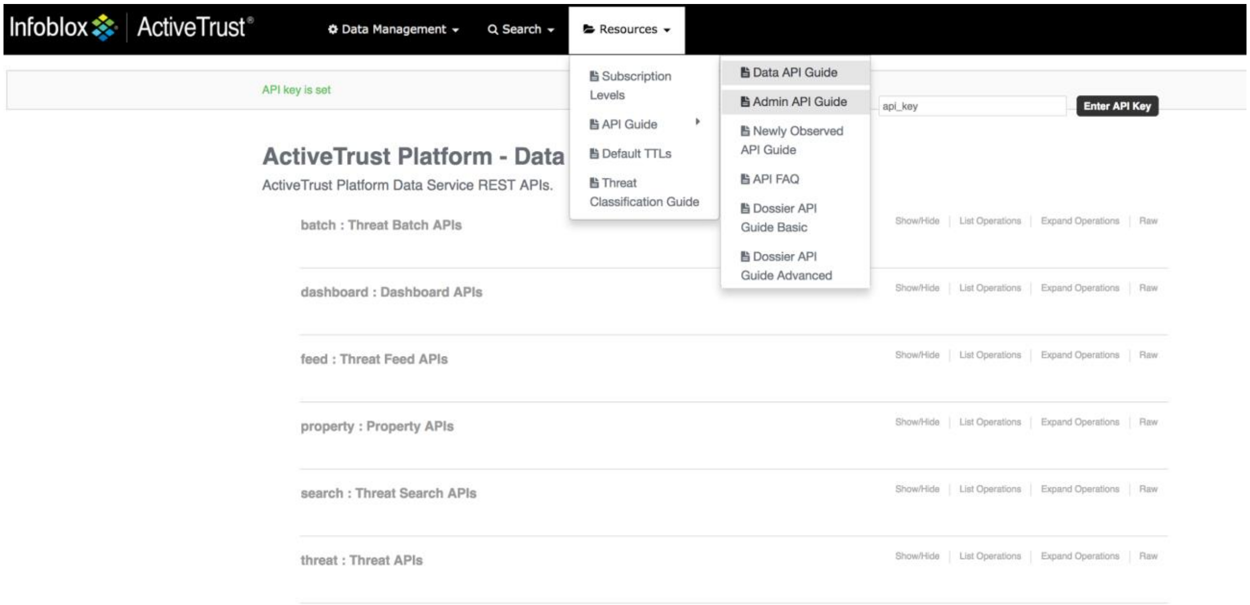
The listing below contains a sample data submission in CSV format.

```
record_type,url,profile,detected,property
url,"https://example.com/page1.html","SampleProfile","20170602T154742Z",
"UnwantedContent_Parasite"
url,"http://example.com/gift.html","SampleProfile","20170602T154742Z", "Scam_FakeGiftCard"
```

The recommended limit for the number of records in a given data submission is 50,000. The maximum number of records should be no more than 60,000 at this point in time.

TIDE API

TIDE API consist of Data API, Admin API. Data API is used to submit and retrieve threat indicators. Admin API provide an access to governance policies, data profiles and information about available sources and targets for data sharing. ActiveTrust platform provides API Guides, which describe all available filters and options of API calls. Before using API Guides you need to enter an API Key in “api_key” field. The API keys are configured on “User Settings” → “Manage API Keys” page.



ActiveTrust Platform - Data

ActiveTrust Platform Data Service REST APIs.

batch : Threat Batch APIs

dashboard : Dashboard APIs

feed : Threat Feed APIs

property : Property APIs

search : Threat Search APIs

threat : Threat APIs

The ActiveTrust platform leverages the Basic Auth method in HTTP/HTTPS to transport the API key. The API key is passed in the username field. The password field should be set to an empty string. All data fields (including filter) represented in ISO 8601 format.

Data API

ActiveTrust Data API consist of:

- Threat Batch APIs (batch) - used to submit own threat indicators and retrieve details about uploaded batches.
- Dashboard APIs (dashboard) - used to retrieve daily, weekly and monthly statistics by threats. This information is available on the dashboard.
- Threat Feed APIs (feed) - used to create feeds and retrieve threat indicators using the feeds.
- Property APIs (property) - used to retrieve threat properties registered on ActiveTrust platform.
- Threat Search APIs (search) - allow to save predefined searches of threat indicators and evoke them later by a name.
- Threat APIs (threat) - search threat indicators on ActiveTrust platform.
- Threat Class APIs (threat_class) - used to retrieve threat classes registered on ActiveTrust platform.
- Whitelist Host APIs (whitelist_host) - used to check if a hostname is whitelisted. If the call was evoked without the parameter, it returns all whitelisted hostnames.
- Whitelist IP APIs (whitelist_ip) - used to check if an IP address is whitelisted. If the call was evoked without the parameter, it returns all whitelisted IP ranges and IP-addresses.

Submitting threat indicators

The listing below contains a sample curl command to submit threat indicators in JSON format to ActiveTrust.

```
curl -X POST -H "Content-Type: application/json" --data-binary @DATA_FILE_NAME.json
```

```
http://api.activetrust.net:8000/api/data/batches -u [YOUR_API_KEY]:
```

The system determines the format of the input data based on the Content-Type HTTP header (application/xml, text/xml, application/json, text/plain, text/csv, text/tab-separated-values, text/tsv, text/psv). If the Content-Type is not match with predefined types, or is not specified, it tries to determine the format dynamically by reading the first part of the data. It's safest to specify the format in the Content-Type. The file format is described in "Governance policies and data submission" chapter.

Search for threat indicators/Export threat indicators for 3rd party solutions

Data Threat API calls are used to search threat indicators. Submitted threat indicators are also available for the search. The resulting dataset can be formatted in JSON, XML, STIX, CSV, TSV, PSV, CEF.

The threat indicators can be used by 3rd party solutions, e.g. with Palo Alto NGFW (please check Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls deployment guide for details) after a simple postprocessing.

It is highly recommended to limit amount of retrieving data by applying filters. The table below contains sample requests using CURL command.

Request	Description
curl "https://platform.activetrust.net:8000/api/data/threats/host?profile=IID&dga=false&from_date=2017-06-04T00:00:00Z&data_format=csv&rlimit=100" -u [YOUR_API_KEY]:	1000 threat indicators in CSV format which were added after 2017-06-04 GMT (Date/Time is in ISO 8601 format) by Infoblox and are not DGA.
curl "https://platform.activetrust.net:8000/api/data/threats/state/host?Profile=IID&data_format=json" -u [YOUR_API_KEY]:	All currently active hostname threats detected by Infoblox (IID)
curl "https://platform.activetrust.net:8000/api/data/threats?type=host&profile=IID&period=30min&data_format=json" -u [YOUR_API_KEY]:	Infoblox-sourced hostnames for the past 30 minutes.
curl "https://platform.activetrust.net:8000/api/data/threats?profile=AIS-FEDGOV,iSIGHTPARTNERS&period=1w&data_format=csv " -u [YOUR_API_KEY]:	iSight Partners and DHS AIS IPs for the past week, in CSV format.

Admin API

ActiveTrust Admin API consist of:

- Sharing Info APIs (sharing) - provide information about organizations and groups which provide thereat indicators or can be shared with.

- Resource Info APIs (resources) - manage data profiles. GET requests retrieve information, POST create a profile. API FAQ contains information how to create a profile.
- Governance Policy APIs (governance) - manage governance policies. GET requests retrieve information, POST create a policy. API FAQ contains information how to create a policy.

References

1. ActiveTrust Data API Guide (https://platform.activetrust.net/#dataapi).
2. ActiveTrust Admin API Guide (https://platform.activetrust.net/#adminapi).
3. ActiveTrust Dossier API Guide Basic (https://platform.activetrust.net/#dossier_api_guide_basic).
4. ActiveTrust Dossier API Guide Advanced (https://platform.activetrust.net/#dossier_api_guide_advance).
5. ActiveTrust API FAQ (https://platform.activetrust.net/#apifaq).
6. Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls. Deployment guide. (https://www.infoblox.com/wp-content/uploads/infoblox-deployment-guide-implementing-infoblox-tide-feeds-into-palo-alto-networks-firewalls.pdf).