Infoblox
CONTROL YOUR NETWORK

Deployment Guide

ActiveTrust Platform Dossier and Tide

Quick Start Guide

Contents

© 2018 Infoblox Inc. All rights reserved.

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 infrastructures. 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 quicker and with greater confidence.

This document contains a high-level overview of 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.

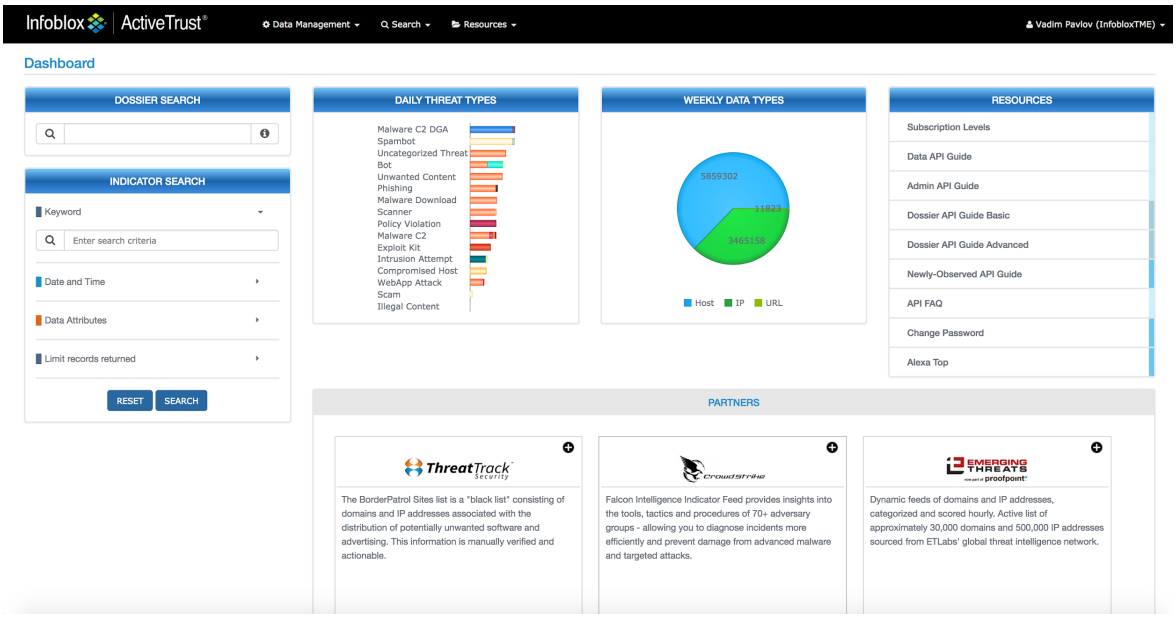
ActiveTrust Dossier and TIDE common Web-interface

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" → "Dossier"**. These sites are respectively referred to as The Portal and CSP (Cloud Service Portal). Additionally, you can use Dossier 2.0 on the CSP portal under **"Analyze" → "Dossier (early release)"**.

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 profile sub-menus.



- **"Data Management"**: provides access to data governance and submission tools as well as links to the dashboard, Alexa Top domains and data report search page.
- **"Search"**: provides an access to Dossier and Indicator searches.

© 2018 Infoblox Inc. All rights reserved.

- **"Resources"**: contains API guides, the Automated indicator sharing (AIS) program, Dossier and TIDE quick start guide, descriptions of the subscription levels, default threat indicator TTLs, and the Threat Classification Guide.
- **"Your username"**: sub-menu with metric reports, user settings and the ability to logout.

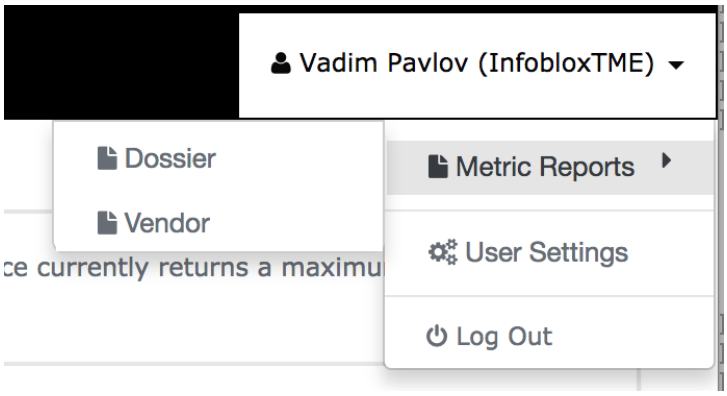
On the home dashboard you can find:

- Dossier keyword 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 - provides 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 - provides 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

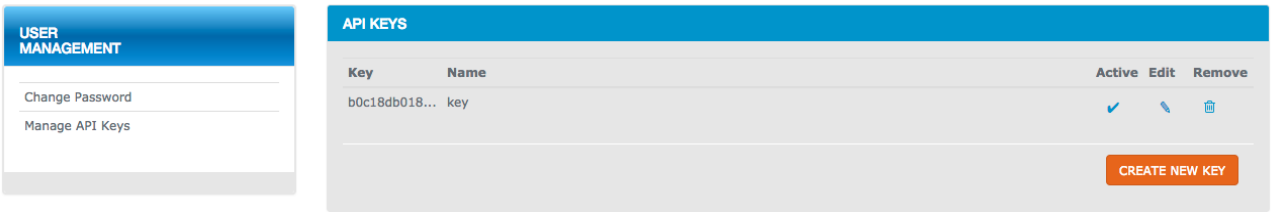
Metric Reports

Subscriptions includes a 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.



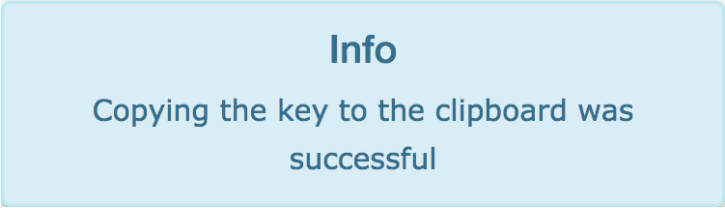
User Settings

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.



API keys are required to access Dossier and TIDE via REST API. A user can create multiple API keys. There are no specific permissions related to a key. Only the key name, description and whether it is active or not 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

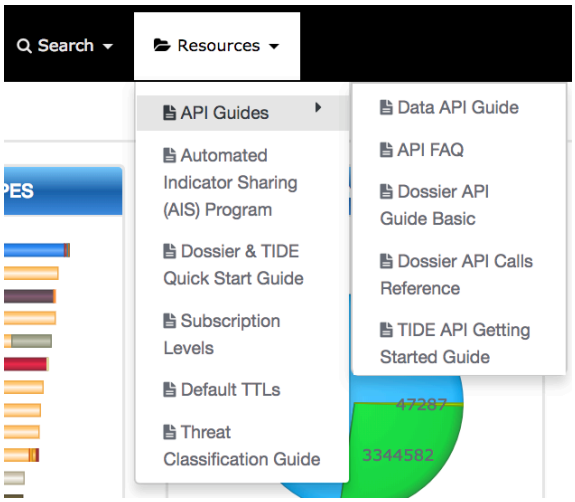


Refer to the next section RESOURCES for examples of API key usage.

Resources

API Guides

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

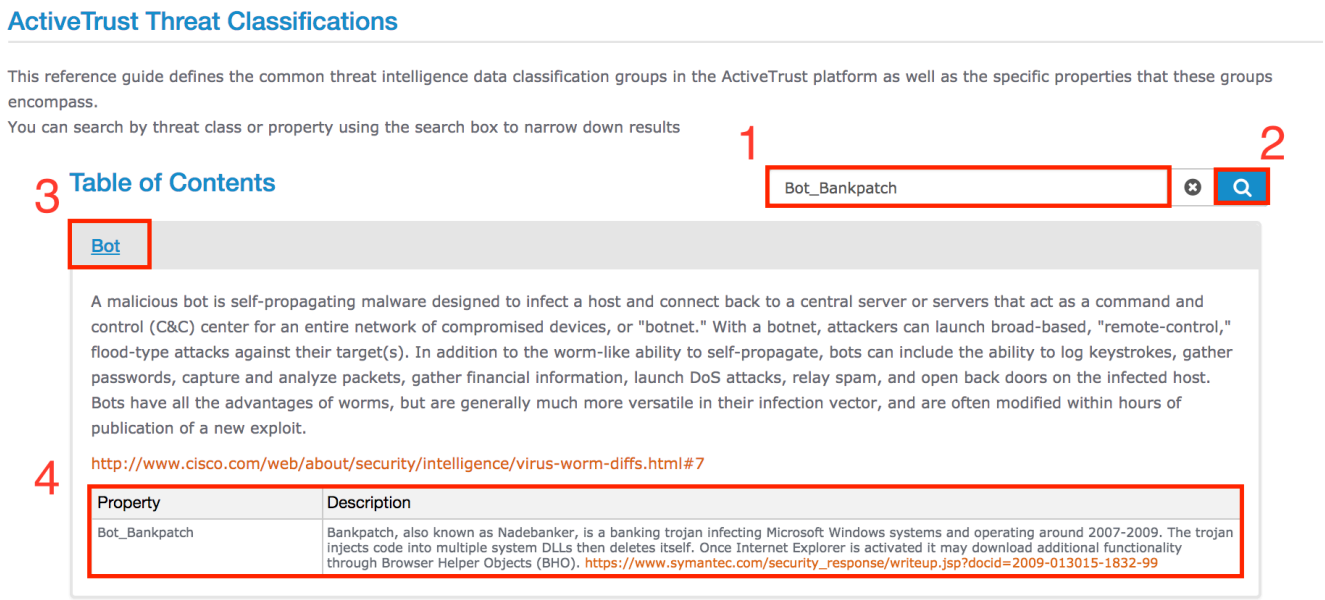


The required API key can be obtained as described in the "User Settings" chapter.

Threat Classification Guide

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

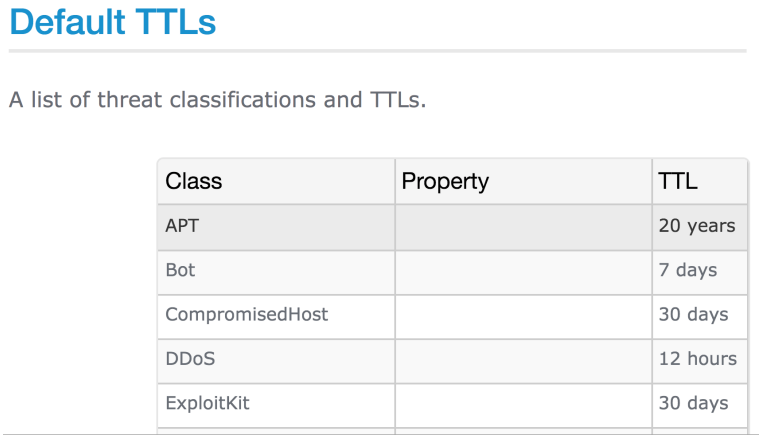
© 2018 Infoblox Inc. All rights reserved.



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 TTLs

Default expiration time for all classes are provided on **"Resources" → "Default TTLs"** page.



Class	Property	TTL
APT		20 years
Bot		7 days
CompromisedHost		30 days
DDoS		12 hours
ExploitKit		30 days

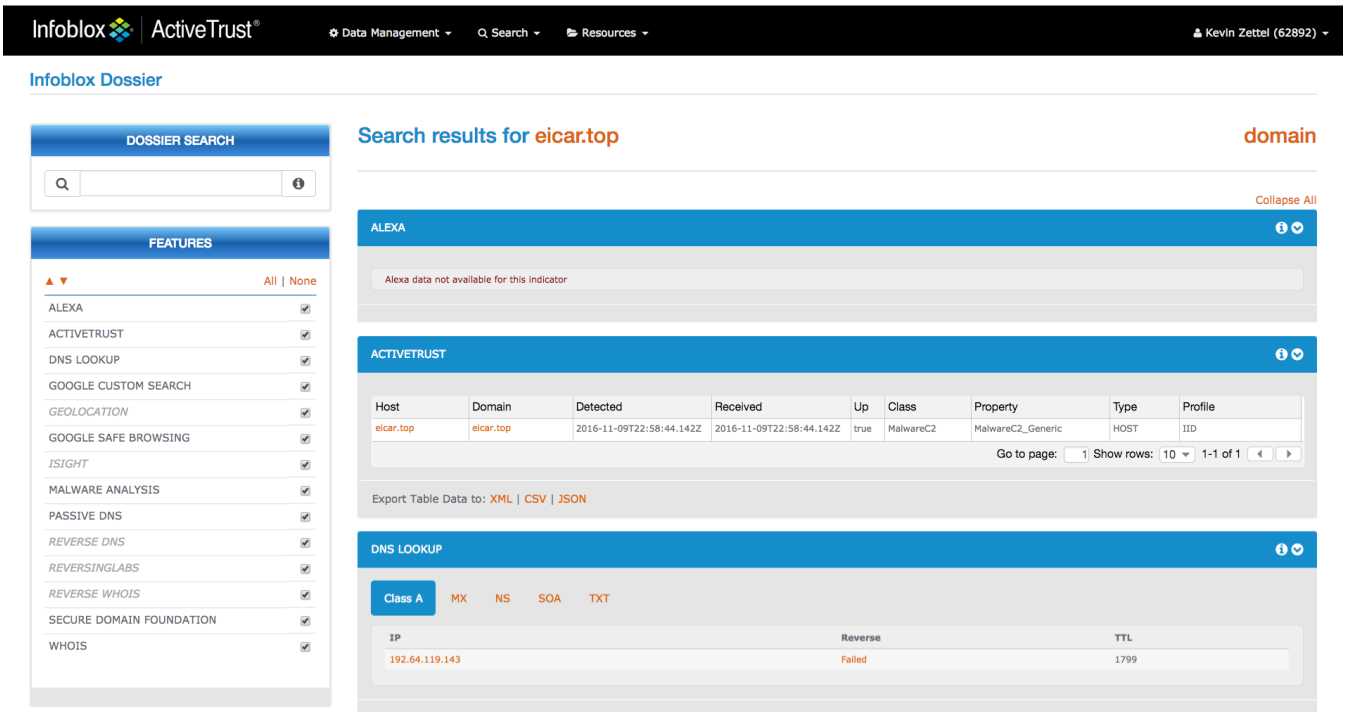
Dossier

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

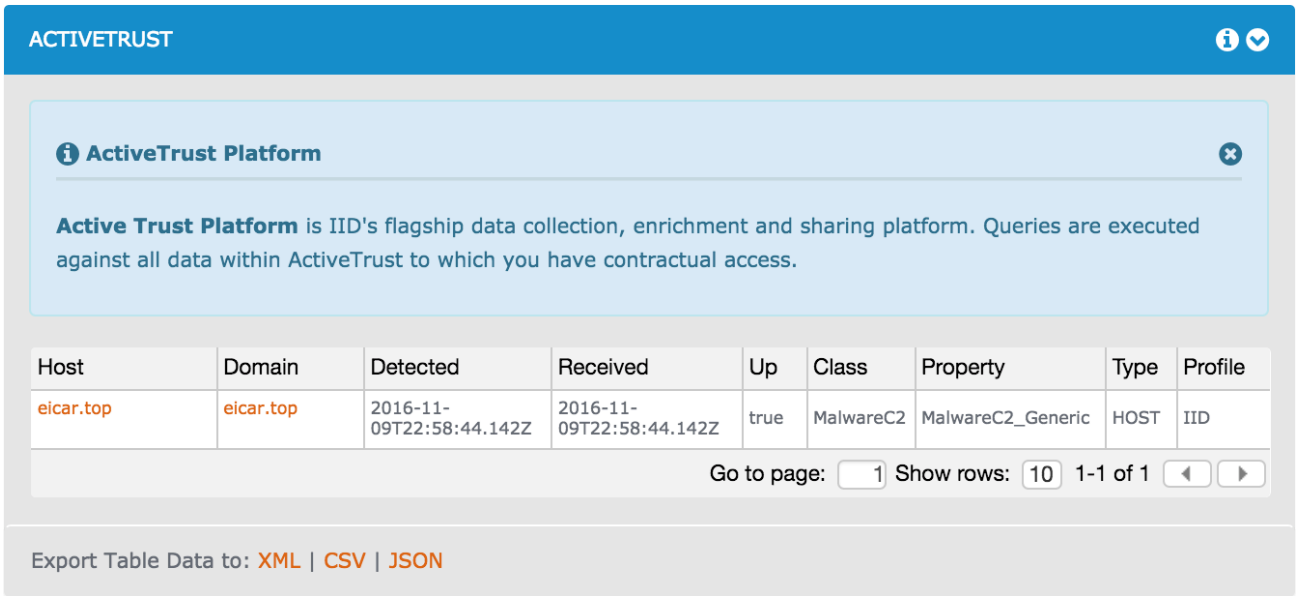
Found under **"Data Management" → "Dashboard" → "Dossier Keyword Search"** or **"Search" → "Dossier"**, you can use the following items in the Dossier keyword search field: IPs, URLs, Domains, Hostnames, Email addresses, MD5, SHA1, and SHA256 hashes. Not all features/data providers support all data types, e.g. Alexa supports only hostnames and domains.

© 2018 Infoblox Inc. All rights reserved.



Dossier automatically detects the type of the data in a search field and performs only relevant searches. It's intelligent and it's possible to enter domains in a format like: "example[.]com". The **"Features"** sidebar provides an ability to select the wanted features.

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

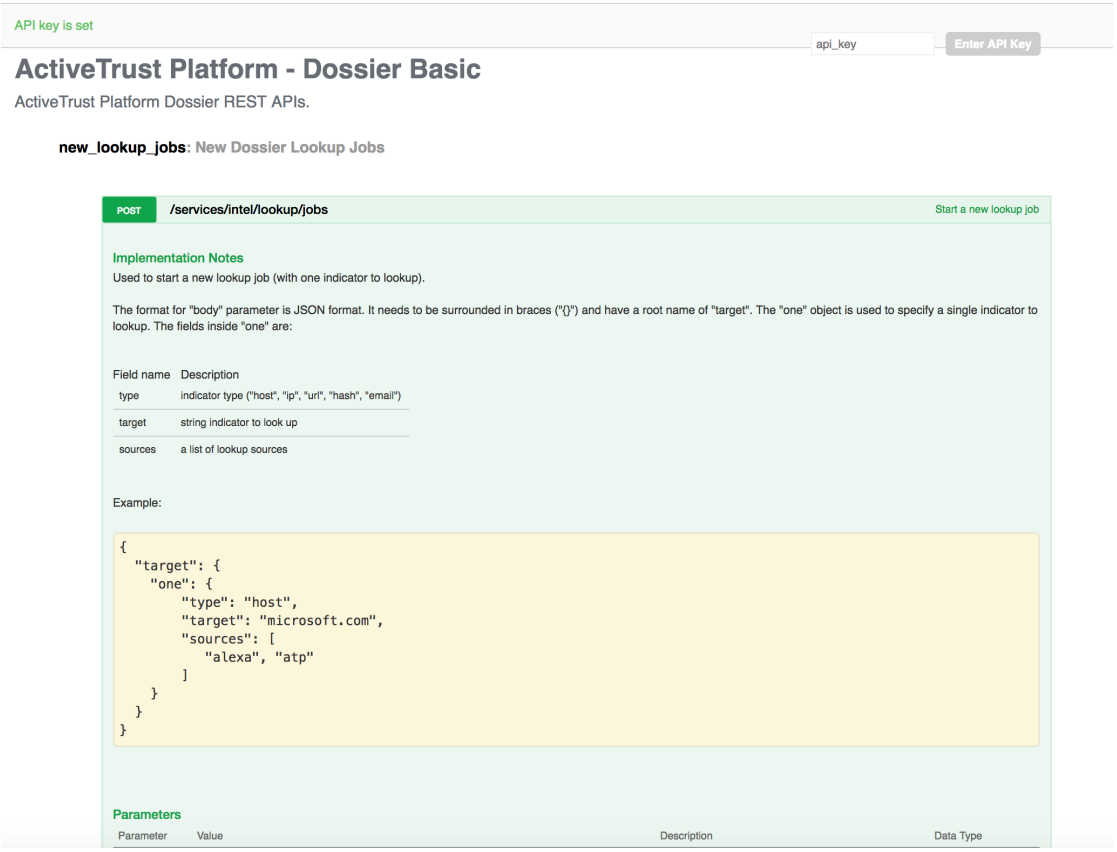


Dossier API

Dossier API Basic is commonly used by customers. It provides access to all information available on the portal. **"Dossier API Guide Basic"**, found in **"Resources" → "API Guides"**, describes all available filters and options. Before using **"Dossier API Guide Basic"** you need to enter an API Key in the **"api_key"** field. The API keys are configured on the **"User Settings" → "Manage API Keys"** page. The ActiveTrust platform leverages the Basic Auth method in HTTP/HTTPS to transport the API key.

© 2018 Infoblox Inc. All rights reserved.

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



When you execute a test query, API Guide Basic 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 the **"eicar.top"** domain in JSON format, which is the only supported export format for API based indicator searches.

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

It takes some time to retrieve data. If the data is not required immediately a search can be executed with **"wait"** parameter set to **"false"** and retrieved later using a 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 the **"job_id"** parameter.

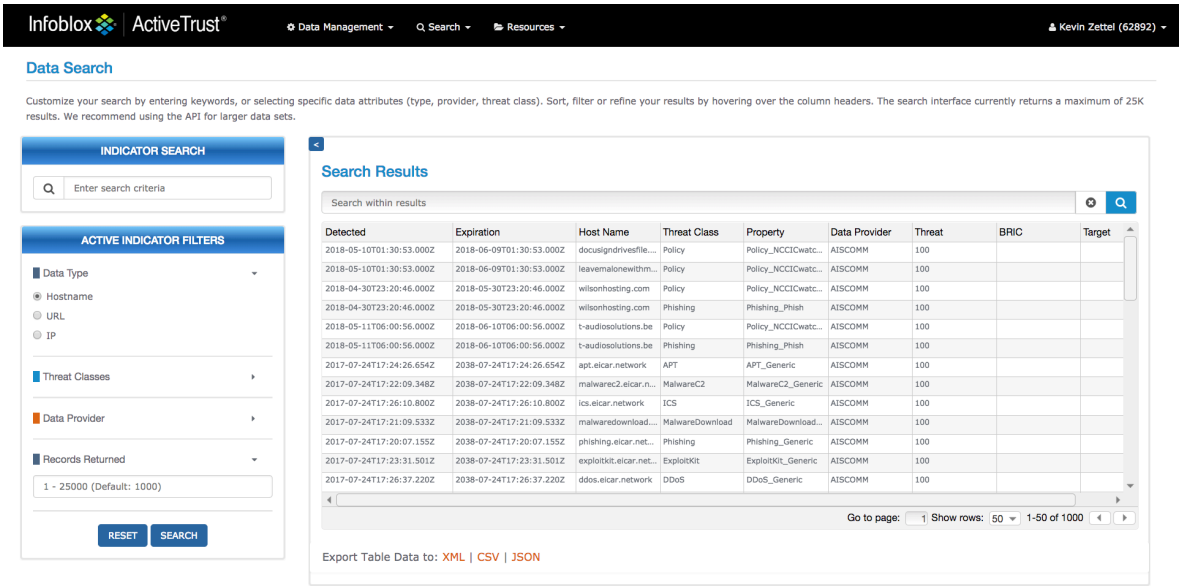
https://platform.activetrust.net:8000/api/services/intel/lookup/jobs/**job_id**/results

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", which can be found at **"Data Management" → "Dashboard" → "Indicator Search"** or **"Search" → "Indicator"**, is different than Dossier search which only returns data from the ActiveTrust database. Indicator search is not limited to a specific indicator (e.g. a hostname). The search interface currently returns a maximum of 25,000 results. It is recommended to use API for larger data sets.



Due to the 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 resulting dataset can be exported in XML, CSV or JSON format.

Data Management

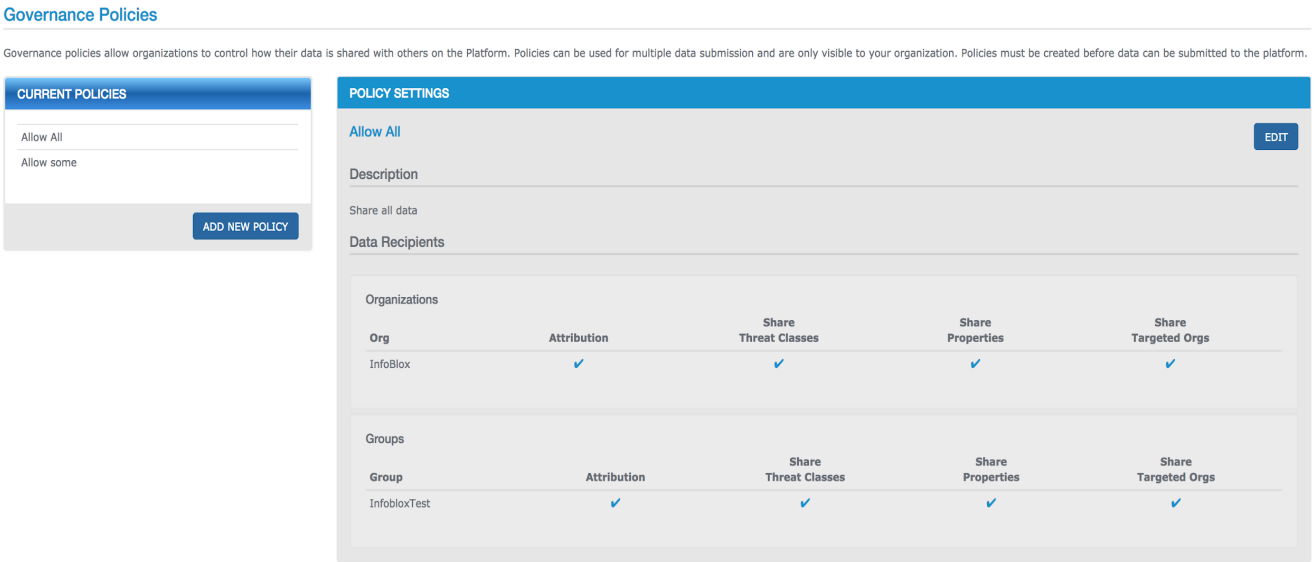
Alexa Top

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

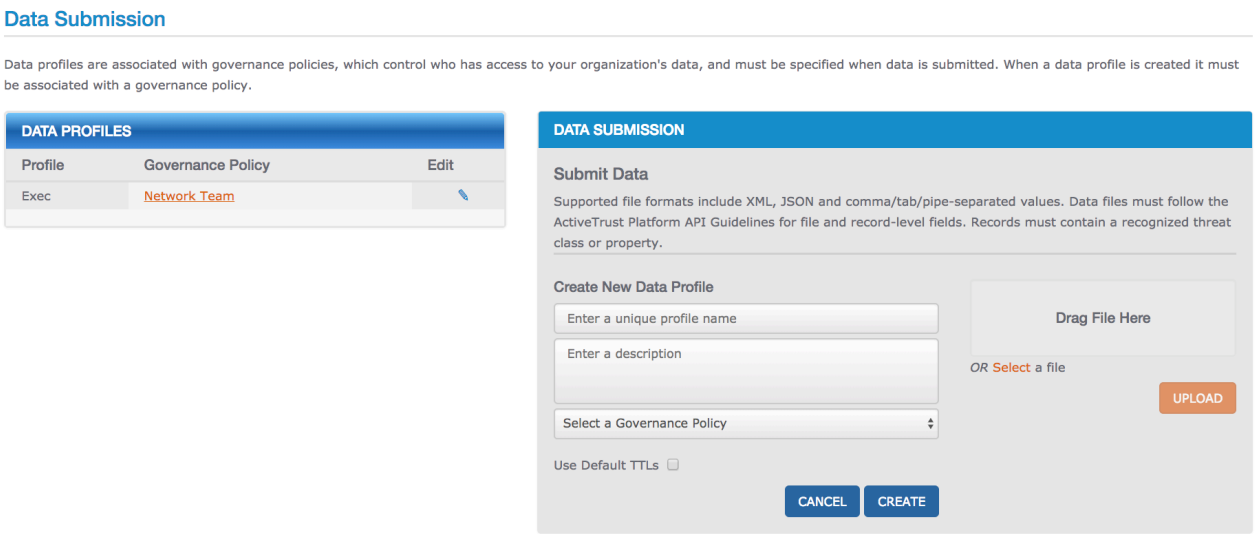
Governance Policies and Data Submission

Customers can submit/upload their 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 and data sharing between organizations via a request. Policies can be used to control multiple data submissions and are only visible within your organization.

© 2018 Infoblox Inc. All rights reserved.



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.



Users can submit threat indicators through 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 a standard TTL should be used
3. A governance policy - defines which data profile is used.

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.

© 2018 Infoblox Inc. All rights reserved.

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

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>
```

© 2018 Infoblox Inc. All rights reserved.

```
  <property>Scanner_Generic</property>
  <detected>19980927T154242Z</detected>
  <duration>42y0m0w0d42h</duration>
 </record>
</feed>
```


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"}
     ]
    }
}
```

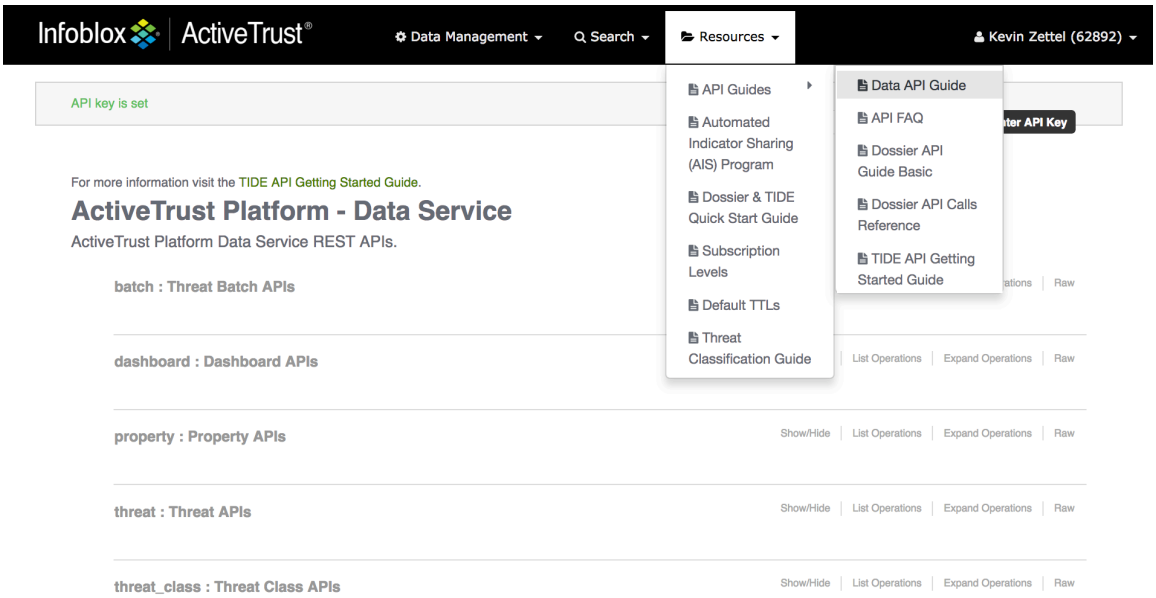

CSV format:


```
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"
```


TIDE API

TIDE API consist of Data API. Data API is used to submit and retrieve threat indicators. 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. API keys are configured on the **"User Settings" → "Manage API Keys"** page.

© 2018 Infoblox Inc. All rights reserved.



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 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.
- Property APIs (property) - used to retrieve threat properties registered on the ActiveTrust platform.
- Threat APIs (threat) - search threat indicators on the ActiveTrust platform.
- Threat Class APIs (threat_class) - used to retrieve threat classes registered on the ActiveTrust platform.

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 doesn't match with predefined types, or isn't specified, it tries to determine the format dynamically by reading the first part of the data. Best practice is to specify the format in the Content-Type. The file format is described in the "Governance policies and data submission" chapter.

© 2018 Infoblox Inc. All rights reserved.

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.

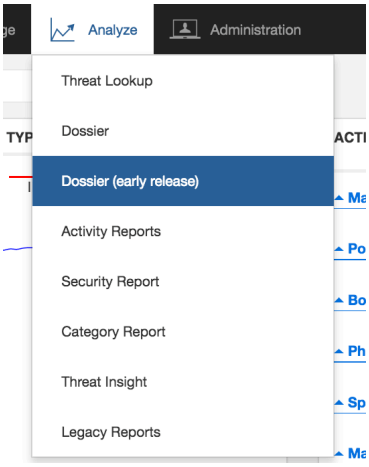
The threat indicators can be used by 3rd party solutions, e.g. with Palo Alto NGFW (check Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls deployment guide for details) after a simple post-processing.

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

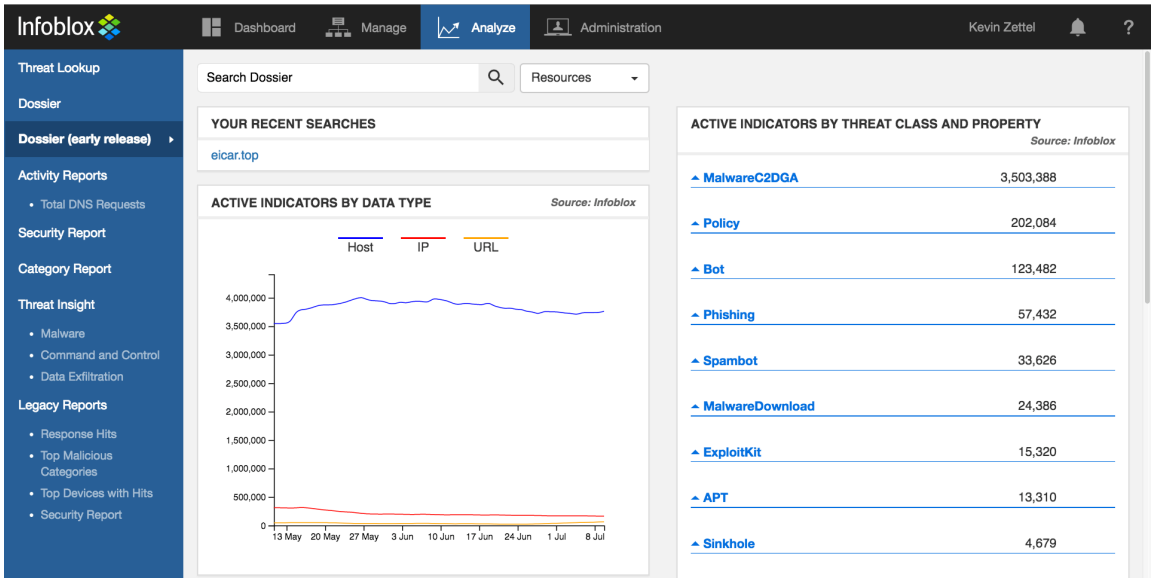
Request	Description
curl "https://platform.activetrust.net:8000/api/data/threats/host?profile=IID&dga=false&from_date=2017-06-04T00:00:00Z&data_format=csv&rlimit=100" -u [YOUR_API_KEY]:	1,000 threat indicators in CSV format which were added after 2017-06-04 GMT (Date/Time is in ISO 8601 format) by Infoblox 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.

Dossier (early release)

Dossier (early release) is a new web interface for Dossier available on the https://csp.infoblox.com under **"Analyze" → "Dossier (early release)"**.



The Dossier (early release) page contains a search bar to search the specific indicators, a chart that shows the number of active indicators by data type, a list of recent indicators searched for and a number of active indicators by threat class and property.



The Dossier (early release) search field accepts the following input types: domains, hostnames, IPs, URLs, MD5, SHA1 and SHA256 hashes, and email addresses.

Not all features/data providers support all data types, e.g. Alexa supports only hostnames and domains, for example.

Dossier automatically detects the type of the data in a search field and performs only relevant searches. With Dossier, it is possible to enter domains, hostnames, URLs in a format where TLD is separated by a dot in square brackets e.g.: “example[.]com”.

Conducting a UI search will return all data a user has access to.

More detailed information about the Dossier (early release) can be found in the Dossier 2.0 User Guide under **“Analyze” → Dossier (early release)** on the Resources drop down.

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).
7. ActiveTrust 2.0 Dossier User Guide (http://help.csp.infoblox.com/wp-content/uploads/2018/05/Dossier-V2-Quickstart-Guide-1.pdf).

© 2018 Infoblox Inc. All rights reserved.