DEPLOYMENT GUIDE

Infoblox BloxOne™ Dossier and TIDE

Table of Contents

Overview **2**
Prerequisites **2**
Access to the Cloud Services Portal **2**
Threat Classification Guide **3**
Default TTLs **3**
Excluded Bogons **4**
Viewing Excluded Bogons 4
Infoblox Dossier **5**
The Dossier Threat Indicator Report **5**
Dossier API **7**
Infoblox Threat Intelligence Data Exchange (TIDE) **8**
Active Indicator Search **9**
Extracting Datasets 9
Data Management **10**
InfoRanks 10
Data Submission 11
Data Profiles 11
TIDE Data API **13**
Submitting Threat indicators **13**
Search for Threat Indicators/Export Threat Indicators for 3rd-Party Solutions **14**
References **15**

Overview

Infoblox BloxOne™ 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.

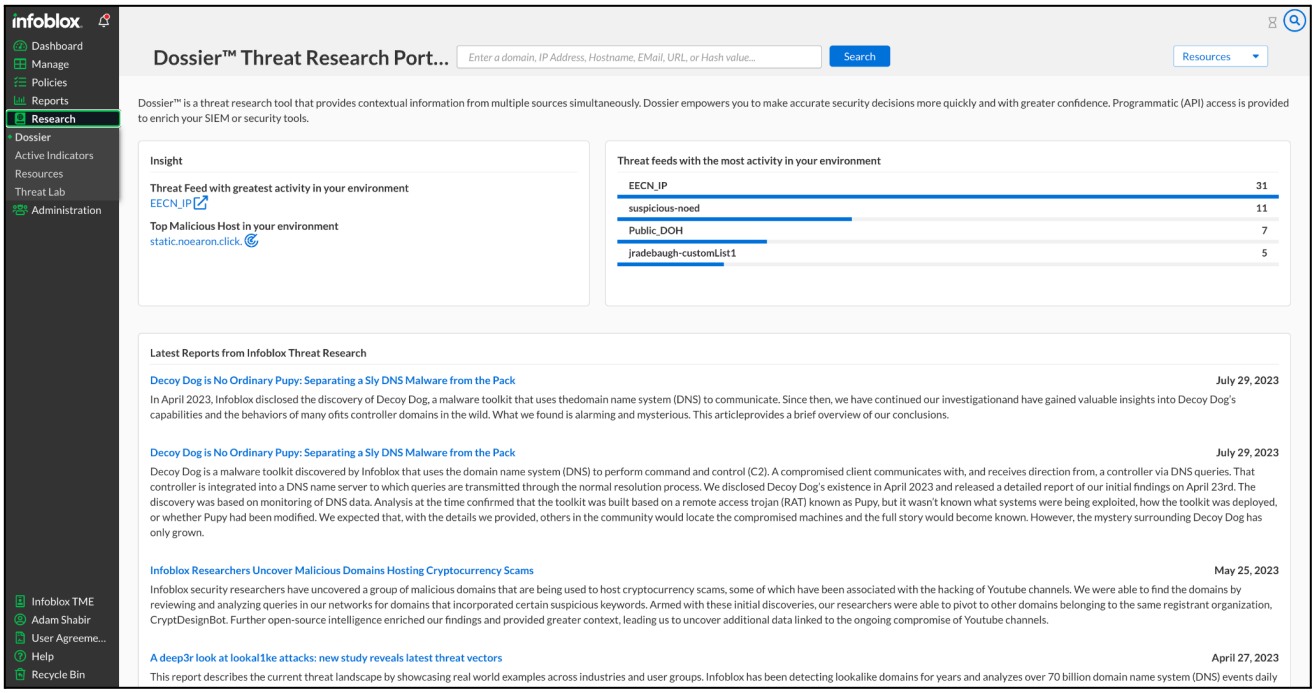
Dossier™ is a threat indicator research tool that gives contextual information from dozens of sources (including TIDE) simultaneously, empowering users to make accurate decisions quicker and with greater confidence.This document contains a high-level overview of how to use BloxOne Dossier and TIDE.

Prerequisites

BloxOne Dossier and TIDE are subscription-based services provided in the 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 BloxOne Portal.

Access to the Cloud Services Portal

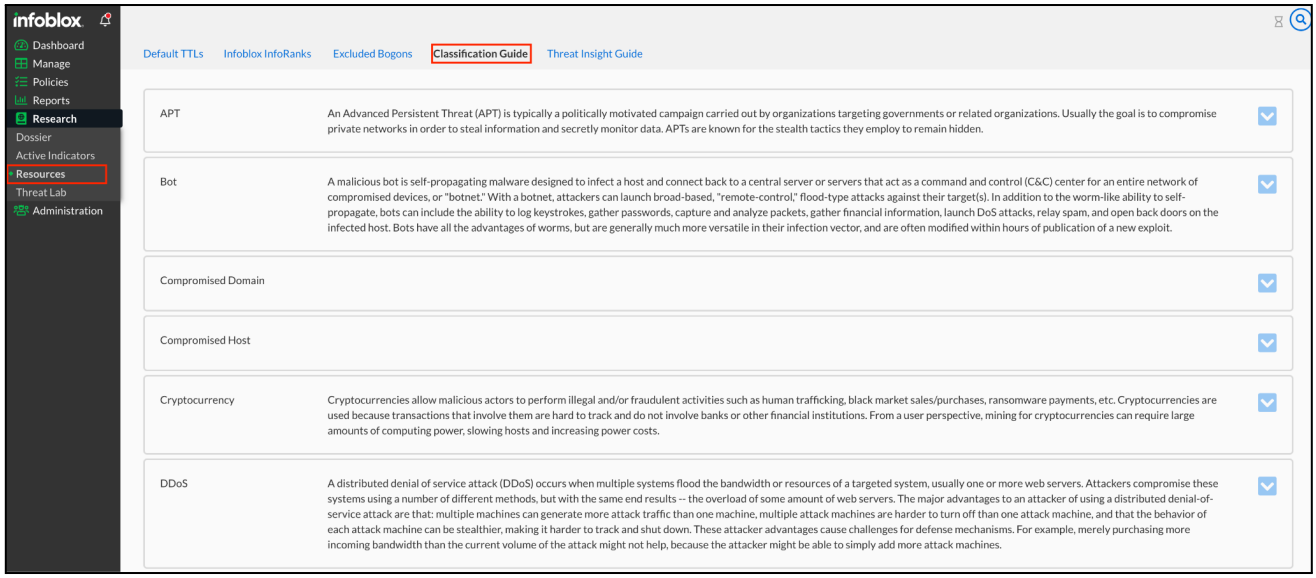
Infoblox Dossier and TIDE can be accessed by navigating to the Dossier™ Threat Research Portal page by clicking Research -> Dossier in the Cloud Services Portal



Threat Classification Guide

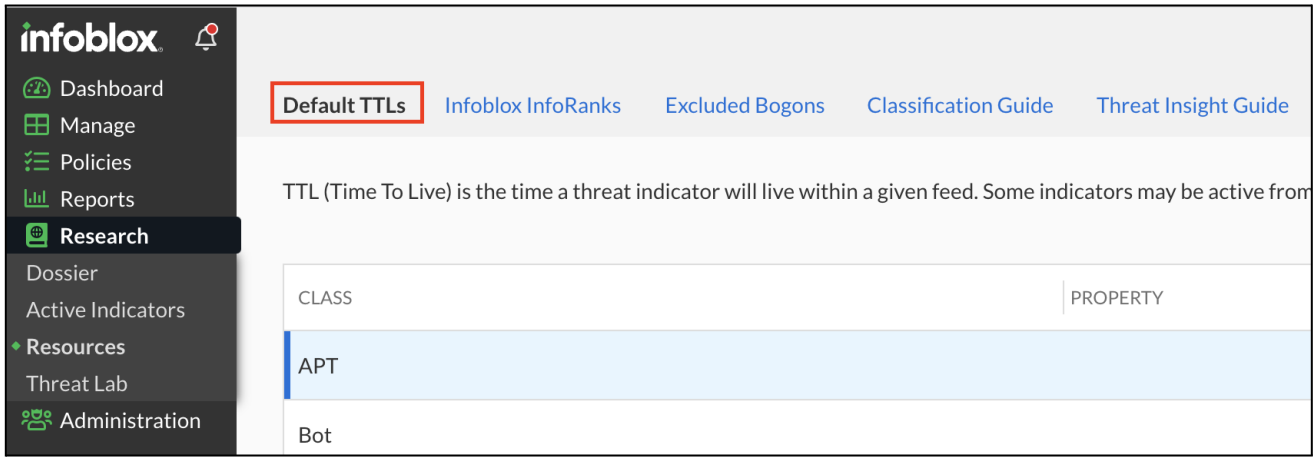
Each threat indicator belongs to a specific class and has a default expiration time (TTL). Expired threat indicators are still available in the database and returned by a search, but they are not included in the Infoblox/DNS Firewall feeds. The Cyber Threat Intelligence team periodically checks the indicators for validity and accuracy. The Threat Classification guide can be located through the Cloud Services Portal at **Research → Resources → Classification Guide**.

For more information about a specific threat classification field, click on the down arrow on the right.

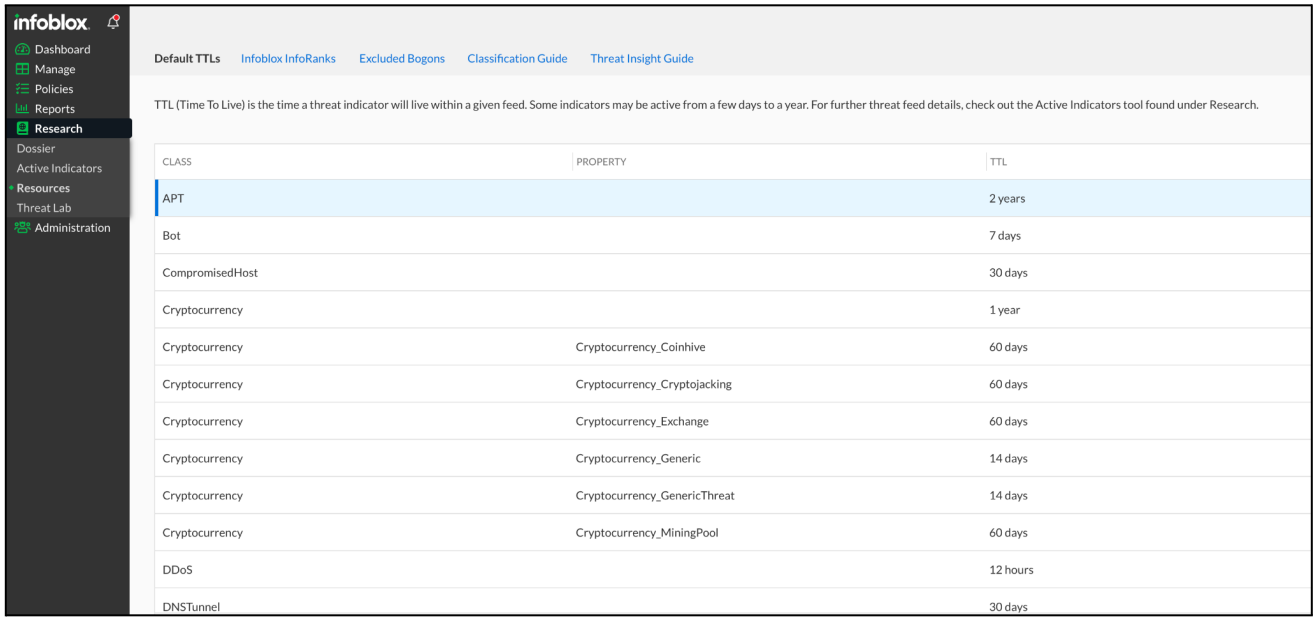


Default TTLs

The default expiration time for all classes can be viewed on the Default TTLs (time-to-live) page at **Research → Resources → Default TTLs**.



TTL field here displays the Time To Live for the Threat Indicator.



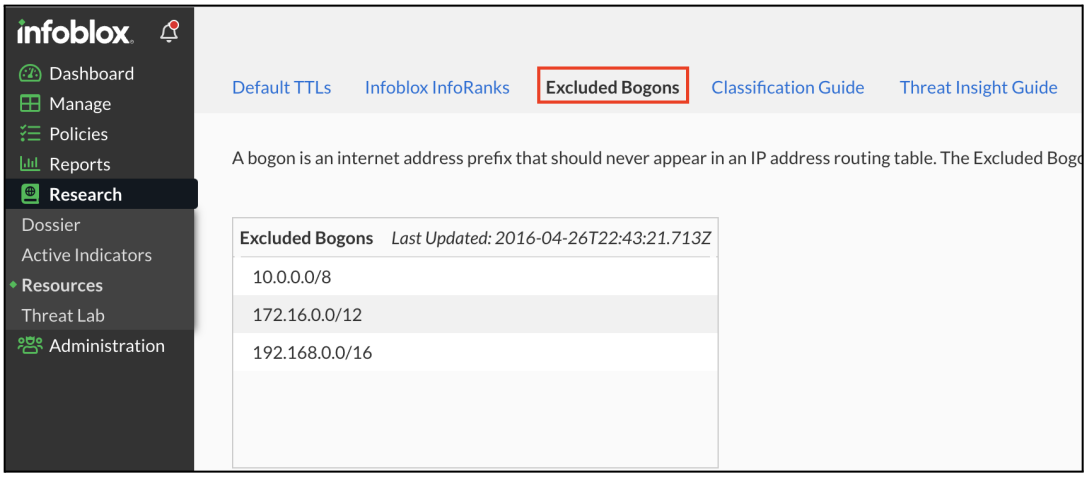
Excluded Bogons

A bogon is an internet address prefix that should never appear in an IP address routing table. The Excluded Bogon page allows administrators to view invalid IP ranges that can be used by malicious entities.

Viewing Excluded Bogons

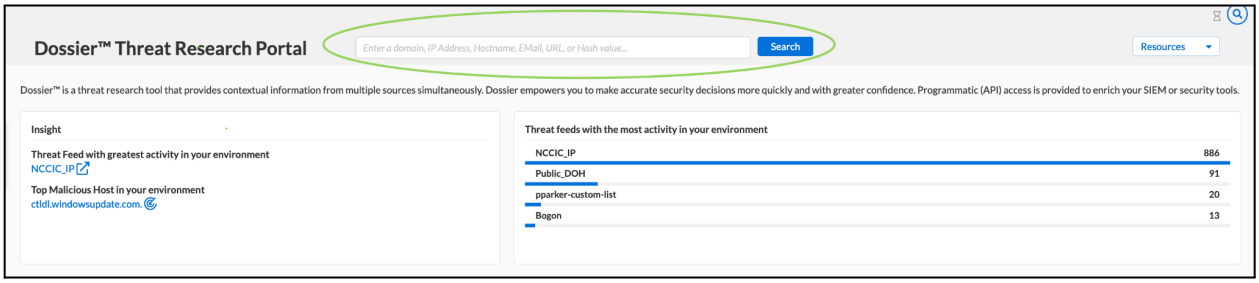
To view Excluded Bogons, perform the following:

1. From the Cloud Services Portal, click **Research** → **Resources**.
2. On the Resources page, click **Excluded Bogons** in the top menu.
3. On the Excluded Bogons page, a list of excluded bogons is displayed.



Infoblox Dossier

Dossier Search is located under **Research** → **Dossier**. You can use the following items in the Dossier keyword search field: IPs, URLs, domains, Host names, Email addresses, MD5, SHA1, and SHA256 hashes. Not all features/data providers support all data types.

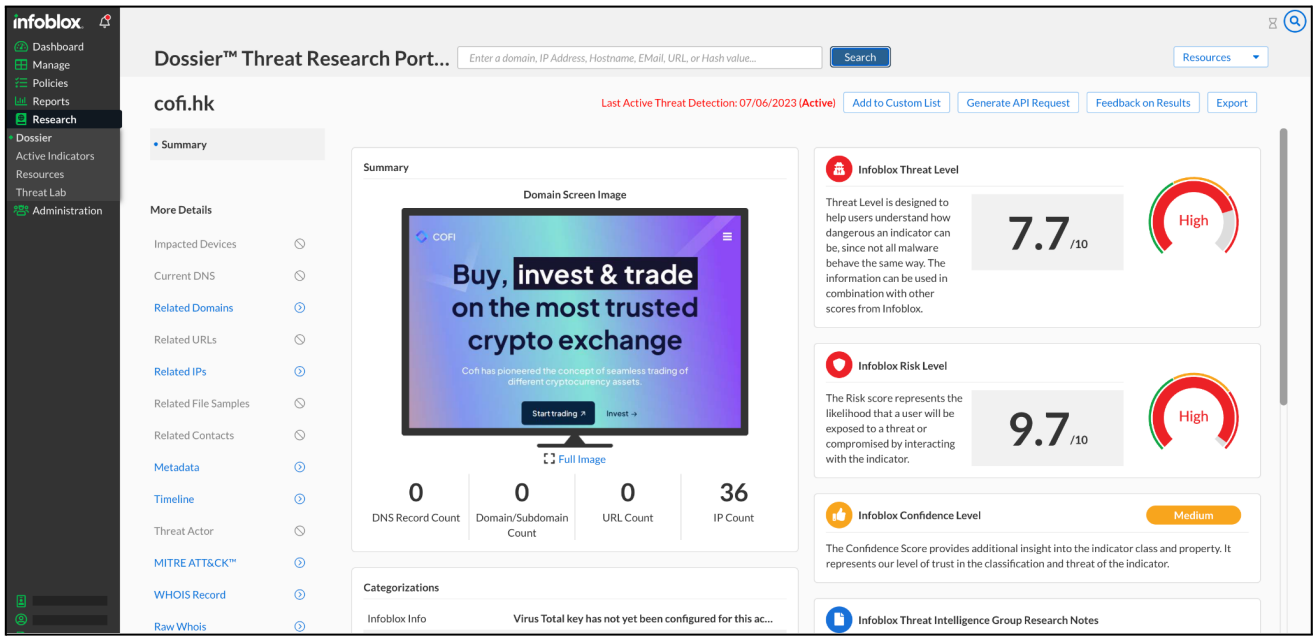


Dossier automatically detects the type of the data in a search field and performs only relevant searches. It's intelligent and it's possible to enter domains in a format like: "example[.]com". When a search has been completed, a set of reports are generated.

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

The Dossier Threat Indicator Report

The Dossier Threat Indicator Report is composed of a dozen smaller, self-contained reports, each focusing on a specific type of information reported in the main threat indicator report.



All available report types are listed in the left-hand column of the report page. The reports generated include the following:
Note: The available report types may change based on the IOC being researched.

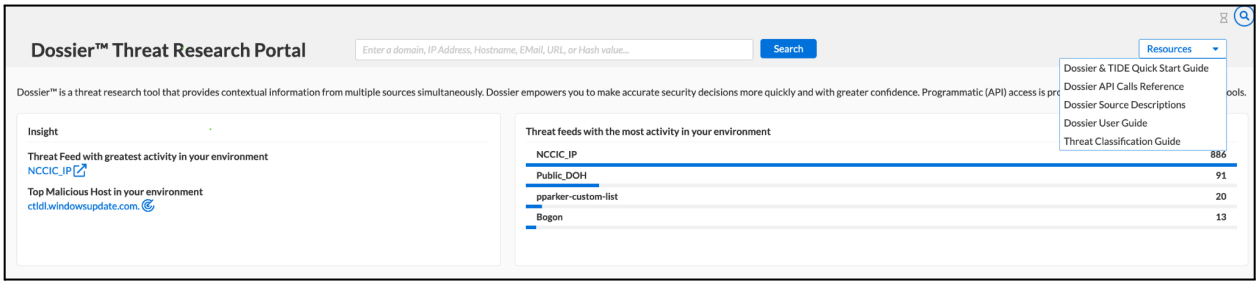
- **Summary**: The Dossier Summary report provides a comprehensive, one-page report summarizing the information obtained when conducting a threat indicator search on a threat indicator.
- **Impacted Devices**: The Dossier Impacted Devices report provides a comprehensive, one-page report detailing impacted devices' information obtained when conducting a threat indicator search on a threat indicator.
- **Current DNS**: The Dossier Current DNS report provides a comprehensive, one-page report detailing current DNS information obtained when conducting a threat indicator search on a threat indicator.
- **Related Domains**: The Dossier Related Domains report provides a comprehensive, one-page report detailing current related domains and sub-domains information obtained when conducting a threat indicator search on a threat indicator.
- **Related URLs**: The Dossier Related URLs report provides a comprehensive, one-page report detailing current related URLs information obtained when conducting a threat indicator search on a threat indicator.
- **Related IPs**: The Dossier Related IPs report provides a comprehensive, one-page report detailing current related IPs information obtained when conducting a threat indicator search on a threat indicator.
- **Related File Samples**: The Dossier Related File Samples report provides a comprehensive, one-page report detailing related file samples information obtained when conducting a threat indicator search.
- **Related Contacts**: The Dossier Related Contacts report provides a comprehensive, one-page report detailing related contact information obtained from Whois data reported by DomainTools.
- **Metadata:** Metadata displays web content related to the indicator from around the web. These may be malicious, as they are unfiltered and listed to give an overall perspective on the nature of this indicator.
- **Timeline**: The Dossier Timeline report provides a comprehensive, one-page report detailing timeline information obtained from domain registration records.

- **Threat Actor**: The Dossier Threat Actor report provides a comprehensive, one-page, score card detailing threat actor information obtained when conducting a threat indicator search on a threat indicator.
- **MITRE ATT&CK**: MITRE ATT&CK is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observation.
- **WHOIS Record**: The WHOIS Record displays location data for a registrant and for the host of a domain or IP address, including domain registration, hosting information, and the domain's creation, updated, and expiry date
- **Raw Whois**: The Dossier Raw WHOIS report provides a comprehensive, one-page report detailing raw WHOIS information that is obtained from the Whois record.

For more information on the Dossier Threat indicator Report, refer to the online documentation available here.

Dossier API

Dossier API Basic is commonly used by customers. It provides access to all information available on the portal. The **Dossier API Calls Reference** located under the **Resources** options tab on the **Dossier™ Threat Research Portal** page describes all available filters and options. When using the API, the same authentication method as used by other features in the Cloud Services Portal applies when using the Dossier API.



When you execute a test query, the API returns a CURL command to request the data, response body and a response code. The following example 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 --location
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs?wait=true' \
--header 'Authorization: Token <API_Key_from_CSP>' \
--header 'Content-Type: application/json' \
--data '{
    "target": {
        "one": {
```

```
            "type": "host",
            "target": "1.1.1.1",
            "sources": [
                "acs",
                "activity",
                "atp",
                "ccb",
                "custom_lists",
                "dns",
                "gcs",
                "geo",
                "gsb",
                "infoblox_web_cat",
                "inforank",
                "isight",
                "malware_analysis",
                "malware_analysis_v3",
                "pdns",
                "ptr",
                "rlabs",
                "rpz_feeds",
                "rwhois",
                "whitelist",
                "whois",
                "ssl_cert",
                "urlhaus",
                "nameserver",
                "threatfox"
            ]
        }
    }
}'
```

It may take some time to retrieve data depending on the quantity of data being requested. If the data is not required immediately, then a search can be executed with a "**wait**" parameter set to "false" and retrieved later. Here, the first search will return "**job_id**". The status of the job and results can be retrieved using a "**lookup_jobs_management**" call. The URL below retrieves results of a job with the "**job_id**" parameter.

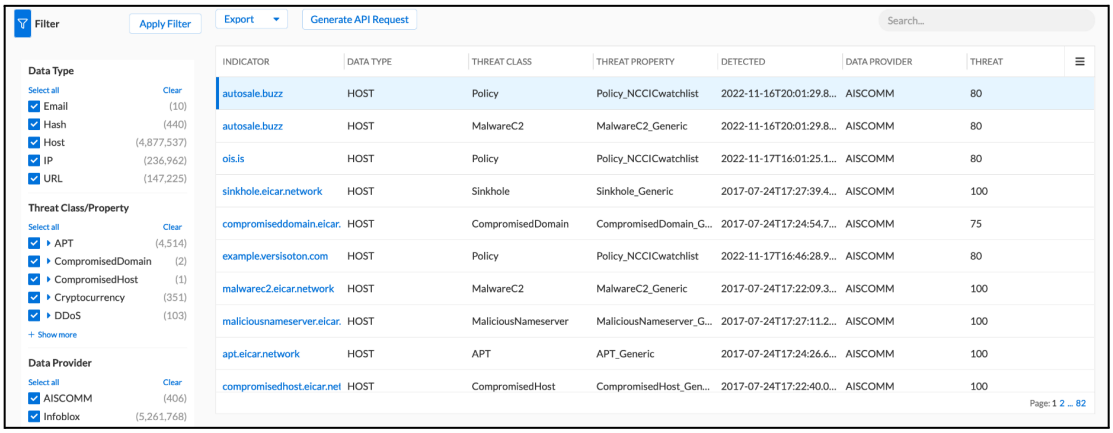
Infoblox Threat Intelligence Data Exchange (TIDE)

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

Infoblox TIDE uses a powerful REST API allowing access to indicators of compromise in the TIDE database in formats like JSON, XML, STIX, CEF, CVS, etc. This allows easy integrations with other solutions without additional transformation/mediation layers. SIEM, NGFW, SWG are good examples where the indicators can be applied to improve overall security in an organization.

Active Indicator Search

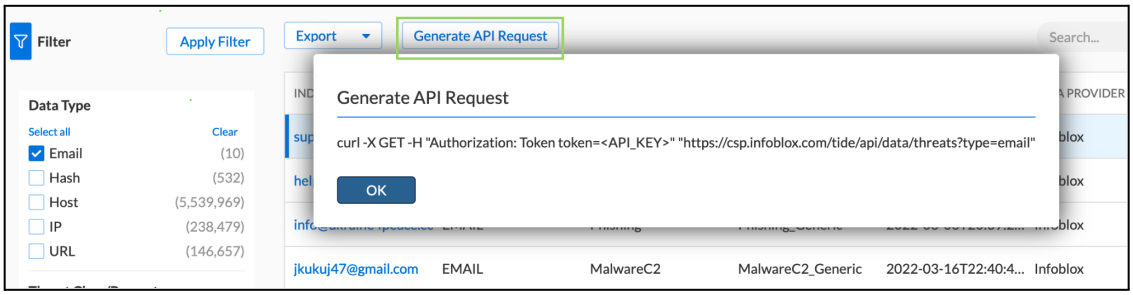
Active Indicator Search is located at **Research** → **Active Indicators** and is different from Dossier search, which only returns data from the database. Indicator search is not limited to a specific indicator (e.g., a hostname). The search interface currently returns limited results. There is no limit to the number of records that can be returned via API. Therefore, it is recommended to use the API for larger data sets.



Due to the size of the available data, it is recommended to apply filters to limit the resulting dataset.
Note: When a keyword is used to search data, other filters are not applied even if they were specified.

You can use the API/CURL Command to Retrieve All Active Indicators Data. To pull all Active Threats indicator data, perform the following:

1. From the Cloud Services Portal, click **Research** → **Active Indicators**.
2. Click **Generate API Request** to generate the CURL command for downloading all records.
3. From the Generate API Request pop-up window, copy the CURL command to run the PULL request.

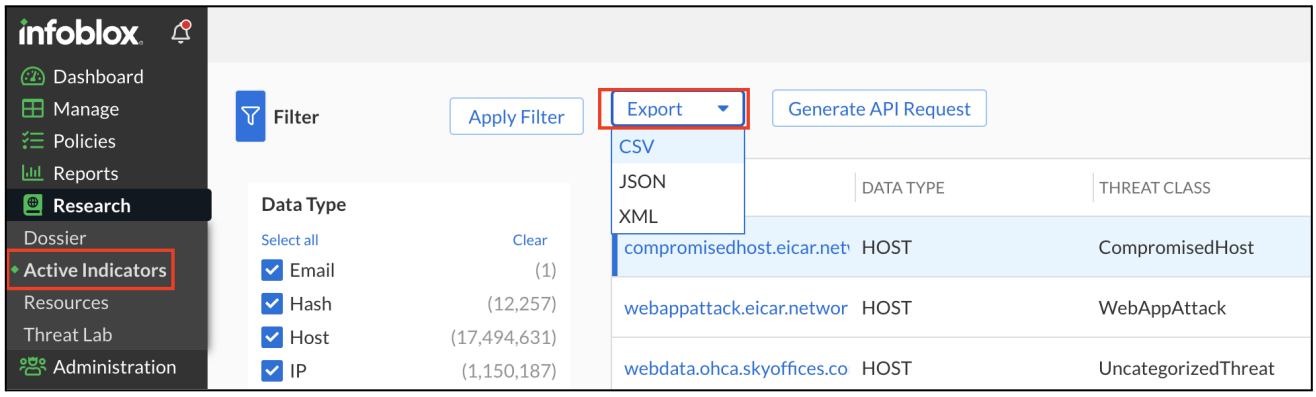


The resulting dataset can be exported in XML, CSV or JSON format.

Extracting Datasets

The datasets can be exported in XML, CSV or JSON format. To extract in any format, do the following:

1. Click on **Research → Active Indicators.**



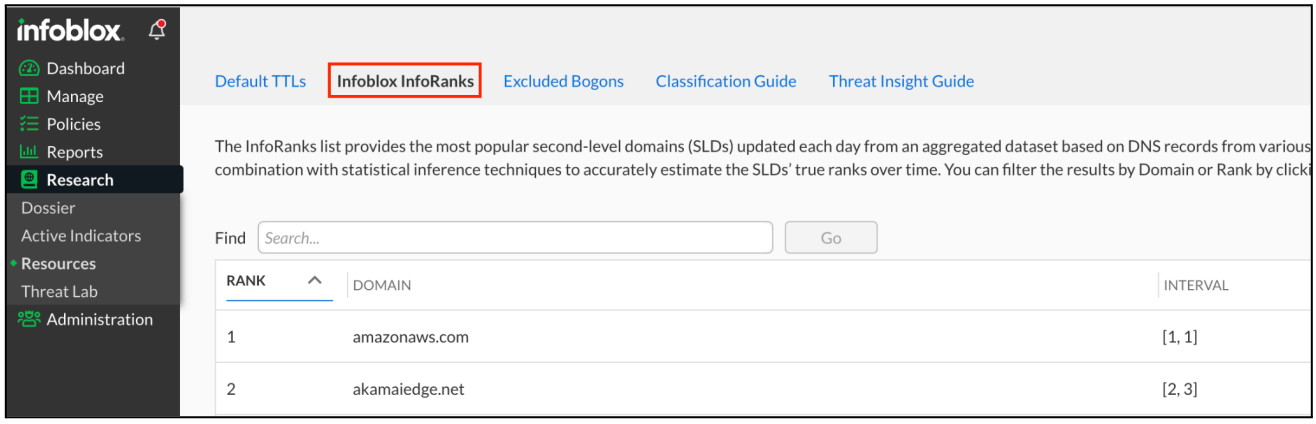
2. Click on **Export** and click on the required format in the dropdown menu. This will download the dataset in the selected format.

Data Management

Dossier and TIDE allow the organization's data administrator to effectively and efficiently manage data with many useful tools including Infoblox InfoRanks, data submission, and the associated data profiles. It also includes the ability to run robust API calls within the Dossier-TIDE ecosystem.

InfoRanks

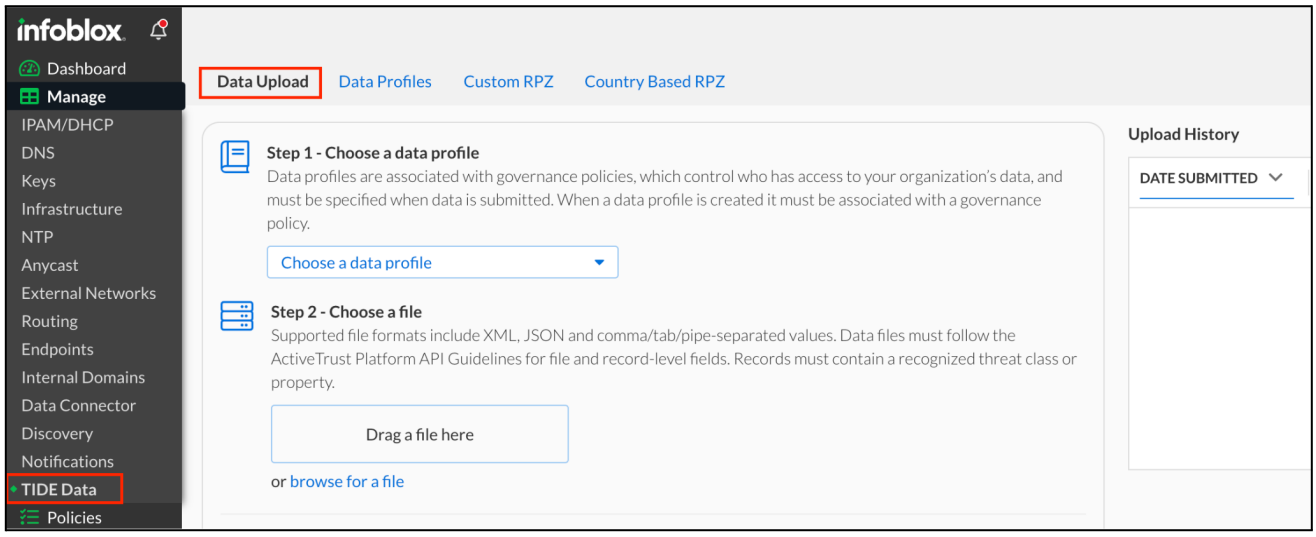
Infoblox InfoRanks provides rankings for the most used sites on the Internet. This tool provides access to the Infoblox InfoRanks Top 10,000 sites and provides ranking based on popularity within the last 7 days. Navigate to **Research → Resources → Infoblox InfoRanks**



InfoRanks returns the ranking of host indicators curated on the Infoblox InfoRank list. The InfoRank list provides the most popular second-level domains (SLDs) updated each day from an aggregated dataset based on DNS records from various data sources. The process to determine the rank for each domain uses count information in combination with statistical inference techniques to accurately estimate the SLDs' true ranks over time.

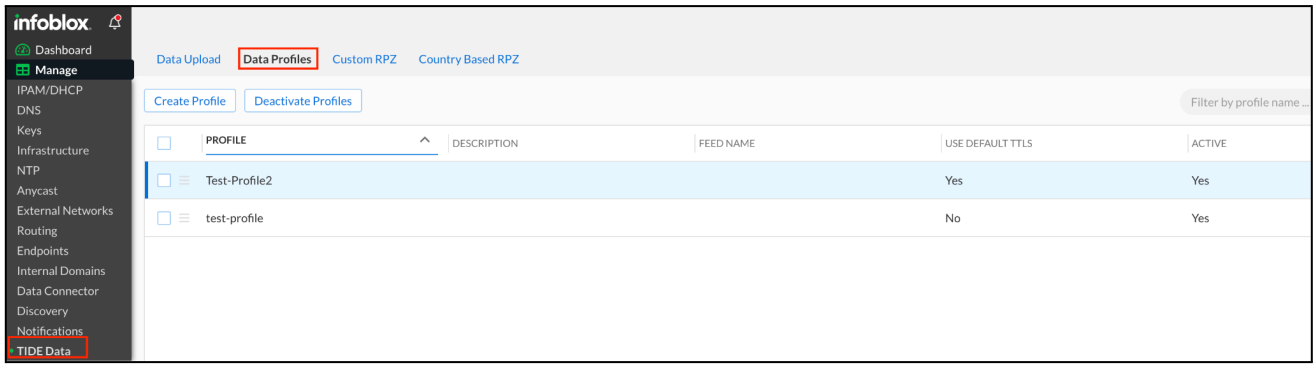
Data Submission

Customers can submit/upload their own threat indicator data via the API or via the Cloud Services portal under **Manage → TIDE Data → Data Upload**.



Data Profiles

Manage → TIDE Data → 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.



Users can submit threat indicators through the portal or via Data API. In order to submit data, a data profile must be created. 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 comprises file level fields and record-level fields. The table below contains descriptions of all available fields.

Data Profiles	
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>
 <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 Data API

The Data API is used to submit and retrieve threat indicators. The Cloud Services Platform provides API Guides, which describes all available filters and options when running API calls. Before using any of the API guides, you need to verify your account using the Cloud Services Platform's token authentication service.

The TIDE API 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.
To create a user API key please refer to the Infoblox documentation. You can learn more about the Tide Data APIs here.

Submitting Threat indicators

The following example contains a sample curl command used to submit threat indicators in JSON format to the Cloud Services Portal. 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.

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.

Searching and Exporting 3rd-Party Indicators	
REQUEST	**DESCRIPTION**
`curl --location 'https://csp.infoblox.com/tide/api/data/threats/host?profile=IID&dga=false&from_date=2017-06-04T00%3A00%3A00Z&data_format=csv&rlimit=100' \ --header 'Authorization: Token <API_Key_from_CSP>'`	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 --location 'https://csp.infoblox.com/tide/api/data/threats/state/host?Profile=IID&data_format=json' \ --header 'Authorization: Token <API_Key_from_CSP>'`	All currently active hostname threats detected by Infoblox (IID).
`curl --location 'https://csp.infoblox.com/tide/api/data/threats?type=host&profile=IID&period=30min&data_format=json' \ --header 'Authorization: Token <API_Key_from_CSP>'`	Infoblox-sourced hostnames for the past 30 minutes.

curl --location 'https://csp.infoblox.com/tide/api/data/threats?profile=IID&period=1w&data_format=csv%20' \ --header 'Authorization: Token <API_Key_from_CSP>'	iSight Partners and DHS AIS IPs for the past week in CSV format.

References

1. Infoblox TIDE API FAQs Guide.
2. Infoblox API Getting Started Guide
3. Infoblox Dossier™ Call Reference
4. Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls (PDF)

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com