

ThreatQuotient



IPQS Fraud and Risk Scoring Operation Guide

Version 1.0.0

March 08, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 **Developer Supported**

Support

Email: support@ipqualityscore.com

Web: N/A

Phone: N/A

Contents

Support	4
Versioning.....	5
Introduction	6
Prerequisites	7
Installation.....	8
Configuration	9
Actions	10
ip_address_reputation.....	11
Configuration Options.....	12
Response Attributes	13
fqdn_reputation	16
Configuration Options.....	17
Response Attributes	17
url_reputation.....	20
Configuration Options.....	21
Response Attributes	21
email_address_reputation	23
Configuration Options.....	24
Response Attributes	25
Change Log.....	29

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **Developer Supported**.

Support Email: support@ipqualityscore.com

Support Web: N/A

Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.



Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Supported.

Versioning

- Current operation version: 1.0.0
- Compatible with ThreatQ versions \geq 4.49.0

Introduction

IPQS Fraud and Risk Scoring Operation provides enterprise grade fraud prevention, risk analysis, and threat detection. Analyze IP addresses, Email addresses, URLs and Domains to identify sophisticated bad actors and high risk behavior.

The operation provides the following actions:

- **ip_address_reputation** - performs real-time lookups to instantly determine how risky a user, click, or transaction is based on an IP address and optional device information.
- **fqdn_reputation** - scans links and domains in real-time to detect suspicious URLs using trusted machine learning models.
- **url_reputation** - detects suspicious URLs using trusted machine learning models.
- **email_address_reputation** - provides real-time email address reputation scoring and validation with hundreds of syntax & DNS checks.

See the [Actions](#) chapter for more information on these actions.

The operation is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- URL



Features marked as **Premium Account Feature** in this guide are not available with the free IPQualityScore account. Contact IPQualityScore for more details on upgrading your account. ThreatQuotient does not manage nor assign IPQualityScore accounts.

Prerequisites

The IPQS Fraud and Risk Scoring Operation requires an IPQualityScore API Key. This key can be obtained by registering an account at the following:

<https://www.ipqualityscore.com/create-account/threatQ>

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

6. You will still need to [configure and then enable the operation](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
IPQualityScore API Key	Your IPQualityScore API Key.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The IPQS Fraud and Scoring operation provides the following actions:

ACTION	DESCRIPTION	SYSTEM OBJECTS	SYSTEM SUB-OBJECTS
ip_address_reputation	IP Address reputation data provides context in the form of attributes from the IPQualityScore API.	Indicator	IP Address
fqdn_reputation	FQDN Reputation scans links and domains in real-time to detect suspicious URLs using trusted machine learning models	Indicator	FQDN
url_reputation	URL reputation data provides context in the form of attributes from the IPQualityScore API.	Indicator	URL
email_address_reputation	Email Address reputation data provides context in the form of attributes from the IPQualityScore API.	Indicator	Email Address

ip_address_reputation

The ip_address_reputation action performs real-time lookups to instantly determine how risky a user, click, or transaction is based on an IP address and optional device information.

<https://ipqualityscore.com/api/json/ip?ip=182.76.175.118>

In addition to analyzing if the IP address is a proxy or VPN, the API returns over 20 relevant data points such as:

- Geo Location Data
- ISP
- Connection Type
- Device Details,
- Recent Reputation Activity
- Overall Fraud Score
- Status as a Proxy
- VPN or TOR Connection
- Abuse Velocity
- Other similar Data Points to Classify Reputation and Risk


Sample Response:


```
{
  "success": true,
  "message": "Success",
  "fraud_score": 0,
  "country_code": "IN",
  "region": "Maharashtra",
  "city": "Kolhapur",
  "ISP": "Airtel",
  "ASN": 9498,
  "organization": "Airtel",
  "is_crawler": false,
  "timezone": "Asia/Kolkata",
  "mobile": false,
  "host": "nsg-static-118.175.76.182-airtel.com",
  "proxy": false,
  "vpn": false,
  "tor": false,
  "active_vpn": false,
  "active_tor": false,
  "recent_abuse": false,
  "bot_status": false,
  "connection_type": "Residential",
  "abuse_velocity": "medium",
}
```

```
"zip_code": "N/A",  
"latitude": 16.70000076,  
"longitude": 74.22000122,  
"request_id": "4DtEk1ASjgvEM1I"  
}
```

Configuration Options


The ip_address_reputation action provides the following configuration options:

PARAMETER	DESCRIPTION
Strictness	<p>Set how depth (strict) of the query. Higher values take longer to process and may provide a higher false-positive rate. Options include:</p> <ul style="list-style-type: none">• 0 (default)• 1• 2 <div> It is recommended to start at 0, the lowest strictness setting, and then increase to 1 or 2 depending on your levels of fraud.</div>
User Agent	<p>You can optionally provide the operation with the user agent string (browser). This allows IPQualityScore to run additional checks to see if the user is a bot or running an invalid browser in order to evaluate the risk of the user as judged in the Fraud Score attribute.</p>
User Language	<p>You can optionally provide the user's language header. This allows the operation to evaluate the risk of the user as judged in the Fraud Score attribute.</p>
Fast	<p>When this parameter is enabled, IPQualityScore's API will not perform certain forensic checks that take longer to process. Enabling this feature greatly increases the API speed without much impact on accuracy. This option is intended for services that require decision making in a time sensitive manner and can be used for any strictness level.</p>

PARAMETER	DESCRIPTION
Mobile	<p>You can optionally specify that this lookup should be treated as a mobile device. This option is recommended for mobile lookups that do not have a user agent attached to the request.</p> <div> This can cause unexpected and abnormal results if the device is not a mobile device.</div>
Allow Public Access Points	Bypass certain checks for IP addresses from education and research institutions, schools, and some corporate connections to better accommodate audiences that frequently use public connections.
Lighter Penalties	Enable this setting to lower detection rates and Fraud Scores for mixed quality IP addresses. If you experience any false-positives with your traffic then enabling this feature will provide better results.

Response Attributes

The ip_address_reputation action provides the following response in the form of attributes:

ATTRIBUTE	DESCRIPTION
Fraud Score	<p>This attribute is the overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores ≥ 75 are suspicious, but not necessarily fraudulent.</p> <div> It is recommend to flag or block traffic with Fraud Scores ≥ 85, but you may find it beneficial to use a higher or lower threshold.</div>
Country Code	The two character country code of IP address or "N/A" if unknown.
Region	The Region (state) of IP address if available or "N/A" if unknown.

ATTRIBUTE	DESCRIPTION
City	The City of IP address if available or "N/A" if unknown.
Zip Code	The Postal code of IP address if available or "N/A" if unknown. IP addresses can relate to multiple postal codes in a city, so it is recommend to perform analysis of similar postal codes nearby.
ISP	The ISP if one is known. Otherwise "N/A".
ASN	The Autonomous System Number if one is known. The attribute will display as Null if nonexistent.
Organization	The Organization if one is known. This can be parent company or sub company of the listed ISP. Otherwise "N/A".
Is Crawler	Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification.
Timezone	The Timezone of IP address if available or "N/A" if unknown.
Mobile	Is this user agent a mobile browser? This attribute will always be false if the user agent is not passed in the API request.
Host	The Hostname of the IP address if one is available.
Proxy	Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.)
VPN	Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The "proxy" status will always be true when this value is true.
TOR	Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR

ATTRIBUTE	DESCRIPTION
	exits at any time. The "proxy" status will always be true when this value is true.
Active VPN	Premium Account Feature - This option identifies active VPN connections used by popular VPN services and private VPN servers.
Active TOR	Premium Account Feature - This option identifies active TOR exits on the TOR network.
Recent Abuse	This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days.
Bot Status	Premium Account Feature - Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious.
Connection Type	The Classification of the IP address connection type as Residential, Corporate, Education, Mobile, OR Data Center.
Abuse Velocity	Premium Account Feature - How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be high , medium , low , or none . This option can be used in combination with the Fraud Score to identify bad behavior.
Latitude	The Latitude of IP address if available or "N/A" if unknown.
Longitude	The Longitude of IP address if available or "N/A" if unknown.

fqdn_reputation

Scans links and domains in real-time to detect suspicious URLs using trusted machine learning models. These machine learning models can accurately identify phishing links, malware URLs, viruses, parked domains, and suspicious URLs with real-time risk scores. In addition, the machine learning models can confidently classify poor reputation domains, suspicious links, and phishing URLs with a real-time API integration. Features such as parking domain detection, domain spam scores, reputation checks, and domain age, elevates URL intelligence to a whole new level.


<https://ipqualityscore.com/api/json/url?url=google.com>

Sample Response:

```
{
  "message": "Success.",
  "success": true,
  "unsafe": false,
  "domain": "google.com",
  "ip_address": "142.250.186.142",
  "server": " gws\r\n",
  "content_type": "text/html; charset=UTF-8",
  "status_code": 200,
  "page_size": 60750,
  "domain_rank": 1,
  "dns_valid": true,
  "parking": false,
  "spamming": false,
  "malware": false,
  "phishing": false,
  "suspicious": false,
  "adult": false,
  "risk_score": 0,
  "category": "Search Engines",
  "domain_age": {
    "human": "24 years ago",
    "timestamp": 874296000,
    "iso": "1997-09-15T00:00:00-04:00"
  },
  "request_id": "4DtEk1AT0nyFj41"
}
```


Configuration Options

The fqdn_reputation action provides the following configuration options:

PARAMETER	DESCRIPTION
Strictness	<p>Set how depth (strict) when scanning a URL. Higher values take longer to process and may provide a higher false-positive rate. Options include:</p> <ul style="list-style-type: none">• 0 (default)• 1• 2 <div> It is recommended to start at 0, the lowest strictness setting, and then increase to 1 or 2 depending on your levels of abuse.</div>
User Agent	When enabled, the API will provide quicker response times by using lighter checks and analysis. The default setting is false .

Response Attributes

The fqdn_reputation action provides the following response in the form of attributes:

ATTRIBUTE	DESCRIPTION
Unsafe	Is this domain suspected of being unsafe due to phishing, malware, spamming, or abusive behavior? View the confidence level by analyzing the "risk_score".
Domain	The Domain name of the final destination URL of the scanned link, after following all redirects.
IP Address	The IP address corresponding to the server of the domain name.

ATTRIBUTE	DESCRIPTION
Server	<p>The server banner of the domain's IP address.</p> <p>Example: "nginx/1.16.0". Value will be "N/A" if unavailable.</p>
Domain Rank	<p>The estimated popularity rank of website globally. Value is "0" if the domain is unranked or has low traffic.</p>
DNS Valid	<p>The domain of the URL has valid DNS records.</p>
Parking	<p>Is the domain of this URL currently parked with a for sale notice?</p>
Spamming	<p>Is the domain of this URL associated with email SPAM or abusive email addresses?</p>
Malware	<p>Is this URL associated with malware or viruses?</p>
Phishing	<p>Is this URL associated with malicious phishing behavior?</p>
Suspicious	<p>Is this URL suspected of being malicious or used for phishing or abuse? Use in conjunction with the <code>risk_score</code> as a confidence level.</p>
Adult	<p>Is this URL or domain hosting dating or adult content?</p>
Risk Score	<p>The IPQS risk score which estimates the confidence level for malicious URL detection. Risk Scores 85+ are high risk, while Risk Scores = 100 are confirmed as accurate.</p>
Category	<p>The website classification and category related to the content and industry of the site. Over 70 categories are available including video Streaming, Trackers, Gaming, Privacy, Advertising, Hacking, Malicious, Phishing, etc. The value will be N/A if unknown.</p>

ATTRIBUTE	DESCRIPTION
Domain Age Human	A human description of when this domain was registered. Example: 3 months ago
Domain Age Timestamp	The unix time since epoch when this domain was first registered. Example: 1568061634
Domain Age ISO	The time this domain was registered in ISO8601 format Example: 2019-09-09T16:40:34-04:00

url_reputation

The url_reputation action scans links and domains in real-time to detect suspicious URLs using trusted machine learning models. These machine learning models can accurately identify phishing links, malware URLs, viruses, parked domains, and suspicious URLs with real-time risk scores. In addition, the machine learning models can confidently classify poor reputation domains, suspicious links, and phishing URLs with a real-time API integration. Features such as parking domain detection, domain spam scores, reputation checks, and domain age, elevates URL intelligence to a whole new level.

<https://ipqualityscore.com/api/json/url?url=https%3A%2F%2Fgoogle.com>

Sample Response:

```
{
  "message": "Success.",
  "success": true,
  "unsafe": false,
  "domain": "google.com",
  "ip_address": "142.250.186.142",
  "server": " gws\r\n",
  "content_type": "text/html; charset=UTF-8",
  "status_code": 200,
  "page_size": 60707,
  "domain_rank": 1,
  "dns_valid": true,
  "parking": false,
  "spamming": false,
  "malware": false,
  "phishing": false,
  "suspicious": false,
  "adult": false,
  "risk_score": 0,
  "category": "Search Engines",
  "domain_age": {
    "human": "24 years ago",
    "timestamp": 874296000,
    "iso": "1997-09-15T00:00:00-04:00"
  },
  "request_id": "4DtEk1BYvQ3E4hk"
}
```

Configuration Options

The url_reputation action provides the following Configuration options:

PARAMETER	DESCRIPTION
Strictness	How strict should we scan this URL? Stricter checks may provide a higher false-positive rate. We recommend defaulting to level "0", the lowest strictness setting, and increasing to "1" or "2" depending on your levels of abuse. The default value is to "0".
Fast	When enabled, the API will provide quicker response times using lighter checks and analysis. This setting defaults to false.

Response Attributes

The url_reputation action provides the following response in the form of attributes:

ATTRIBUTE	DESCRIPTION
Unsafe	Is this domain suspected of being unsafe due to phishing, malware, spamming, or abusive behavior? View the confidence level by analyzing the "risk_score".
Domain	Domain name of the final destination URL of the scanned link, after following all redirects.
IP Address	The IP address corresponding to the server of the domain name.
Server	The server banner of the domain's IP address. For example: "nginx/1.16.0". Value will be "N/A" if unavailable.
Domain Rank	Estimated popularity rank of website globally. Value is "0" if the domain is unranked or has low traffic.

ATTRIBUTE	DESCRIPTION
DNS Valid	The domain of the URL has valid DNS records.
Parking	Is the domain of this URL currently parked with a for sale notice?
Spamming	Is the domain of this URL associated with email SPAM or abusive email addresses?
Malware	Is this URL associated with malware or viruses?
Phishing	Is this URL associated with malicious phishing behavior?
Suspicious	Is this URL suspected of being malicious or used for phishing or abuse? Use in conjunction with the "risk_score" as a confidence level.
Adult	Is this URL or domain hosting dating or adult content?
Risk Score	The IPQS risk score which estimates the confidence level for malicious URL detection. Risk Scores 85+ are high risk, while Risk Scores = 100 are confirmed as accurate.
Category	Website classification and category related to the content and industry of the site. Over 70 categories are available including "Video Streaming", "Trackers", "Gaming", "Privacy", "Advertising", "Hacking", "Malicious", "Phishing", etc. The value will be "N/A" if unknown.
Domain Age Human	A human description of when this domain was registered. (Ex: 3 months ago)
Domain Age Timestamp	The unix time since epoch when this domain was first registered. (Ex: 1568061634)
Domain Age ISO	The time this domain was registered in ISO8601 format (Ex: 2019-09-09T16:40:34-04:00)

email_address_reputation

This API provides real-time email address reputation scoring and validation with hundreds of syntax & DNS checks. The API can be leveraged to determine if the email address inbox exists with the mail service provider and is able to accept new messages. In addition, users can determine if the email address has a poor reputation or has recently been associated with abuse or threats. Additional risk scoring can detect disposable and temporary mail services as well as emails with a history of fraudulent behavior online.


<https://ipqualityscore.com/api/json/email?>

Sample Response:

```
{
  "message": "Success.",
  "success": true,
  "valid": true,
  "disposable": false,
  "smtp_score": 2,
  "overall_score": 3,
  "first_name": "Corporate",
  "generic": true,
  "common": false,
  "dns_valid": true,
  "honeypot": true,
  "deliverability": "low",
  "frequent_complainer": false,
  "spam_trap_score": "medium",
  "catch_all": true,
  "timed_out": false,
  "suspect": true,
  "recent_abuse": true,
  "fraud_score": 100,
  "suggested_domain": "N/A",
  "leaked": false,
  "domain_age": {
    "human": "10 years ago",
    "timestamp": 1302837997,
    "iso": "2011-04-14T23:26:37-04:00"
  },
  "first_seen": {
    "human": "2 years ago",
    "timestamp": 1557122946,
    "iso": "2019-05-06T02:09:06-04:00"
  },
  "sanitized_email": "noreply@ipqualityscore.com",
  "request_id": "4DtEk1BYvx3DXCp"
}
```

Configuration Options

The email_address_reputation action provides the following configuration options:


PARAMETER	DESCRIPTION
Abuse Strictness	<p>Set how depth (strict) for machine learning pattern recognition of abusive email addresses with the recent_abuse data point. Options include:</p> <ul style="list-style-type: none">• 0 (default)• 1• 2 <div> If you are filtering account applications and facing advanced fraudsters, it recommend increasing this value to level 1 or 2.</div>
Fast	<p>When this parameter is enabled, the IPQualityScore API will not perform an SMTP check with the mail service provider, which greatly increases the API speed. Syntax and DNS checks are still performed on the email address as well as our disposable email detection service. This option is intended for services that require decision making in a time sensitive manner.</p>
Timeout in Seconds	<p>The Maximum number of seconds to wait for a reply from a mail service provider. If your implementation requirements do not need an immediate response, we recommend bumping this value to 20. Any results which experience a connection timeout will return the "timed_out" variable as true. Default value is 7 seconds.</p>
suggest_domain	<p>This option will force analyze if the email address's domain has a typo and should be corrected to a popular mail service. By default, this test is currently only performed when the email is invalid or if the recent abuse status is true.</p>

Response Attributes

The email_address_reputation action provides the following response in the form of attributes:

ATTRIBUTE	DESCRIPTION
Valid	Does this email address appear valid?
Disposable	Is this email suspected of belonging to a temporary or disposable mail service? Usually associated with fraudsters and scammers.
SMTP Score	Validity score of email server's SMTP setup. Range: -1 to 3. Scores above -1 can be associated with a valid email. <ul style="list-style-type: none">• -1 = invalid email address• 0 = mail server exists, but is rejecting all mail• 1 = mail server exists, but is showing a temporary error• 2 = mail server exists and accepts all email• 3 = mail server exists and has verified the email address
Overall Score	Overall email validity score. Range: 0 to 4. Scores above 1 can be associated with a valid email. <ul style="list-style-type: none">• 0 = invalid email address• 1 = dns valid, unreachable mail server• 2 = dns valid, temporary mail rejection error• 3 = dns valid, accepts all mail• 4 = dns valid, verified email exists
First Name	Suspected first name based on email. The operation will return a value of CORPORATE if the email is suspected of being a generic company email and UNKNOWN if the first name was not determinable.

ATTRIBUTE	DESCRIPTION
Generic	<p>Is this email suspected as being a catch all or shared email for a domain?</p> <p>Example: admin@, webmaster@, newsletter@, sales@, contact@</p>
Common	<p>Is this email from a common email provider?</p> <p>Example: gmail.com, yahoo.com, hotmail.com</p>
DNS Valid	<p>Does the email's hostname have valid DNS entries or partial indication of a valid email?</p>
Honeypot	<p>Is this email believed to be a honeypot or SPAM trap? Bulk mail sent to these emails increases your risk of being blacklisted by large ISPs & ending up in the spam folder.</p>
Deliverability	<p>How likely is this email to be delivered to the user and land in their mailbox. Values can be high, medium, or low.</p>
Frequent Complainer	<p>This attribute indicates if this email frequently unsubscribes from marketing lists or reports email as SPAM.</p>
Spam Trap Score	<p>The confidence level of the email address being an active SPAM trap. Values can be high, medium, low, or none. It is recommended to scrub emails with high or medium statuses. Avoid low emails whenever possible for any promotional mailings.</p>
Catch All	<p>Is this email likely to be a catch all, where the mail server verifies all emails tested against it as valid? It is difficult to determine if the address is truly valid in these scenarios, since the email's server will not confirm the account's status.</p>
Timed Out	N/A

ATTRIBUTE	DESCRIPTION
Suspect	This value indicates if the mail server is currently replying with a temporary error and unable to verify the email address. This status will also be true for catch all email addresses as defined below. If this value is true, then we suspect the valid result may be tainted and there is not a guarantee that the email address is truly valid.
Recent Abuse	This value will indicate if there has been any recently verified abuse across our network for this email address. Abuse could be a confirmed chargeback, fake signup, compromised device, fake app install, or similar malicious behavior within the past few days.
Fraud Score	The overall Fraud Score of the user based on the email's reputation and recent behavior across the IPQS threat network. Fraud Scores ≥ 75 are suspicious, but not necessarily fraudulent.
Suggested Domain	<p>This attribute indicates if this email's domain should in fact be corrected to a popular mail service. This field is useful for catching user typos. The default value is N/A.</p> <p>Example: An email address with gmai.com would display a suggested domain of gmail.com.</p> <div> This feature supports all major mail service providers.</div>
Leaked	Was this email address associated with a recent database leak from a third party? Leaked accounts pose a risk as they may have become compromised during a database breach.
Sanitized Email	A sanitized email address with all aliases and masking removed, such as multiple periods for Gmail.com.
Domain Age Human	A human description of when this domain was registered. (Ex: 3 months ago)

ATTRIBUTE	DESCRIPTION
Domain Age Timestamp	The unix time since epoch when this domain was first registered. (Ex: 1568061634)
Domain Age ISO	The time this domain was registered in ISO8601 format (Ex: 2019-09-09T16:40:34-04:00)
First Seen Human	A human description of the email address age, using an estimation of the email creation date when IPQS first discovered this email address. (Ex: 3 months ago)
First Seen Timestamp	The unix time since epoch when this email was first analyzed by IPQS. (Ex: 1568061634)
First Seen ISO	The time this email was first analyzed by IPQS in ISO8601 format (Ex: 2019-09-09T16:40:34-04:00)

Change Log

- Version 1.0.0
 - Initial Release