

BitSight API Guide: Insurance

Basics

Token Management

Use the BitSight API to integrate BitSight Security Ratings data with your organization's risk underwriting, portfolio modeling/management, claims, or loss control systems. Authentication is token-based; your login credentials to the BitSight Security Ratings Platform will not work.

- Your API token should be treated as a password.
- Anyone with a token will have information about all companies in your portfolio. If you think your token may have been compromised, you can always generate a new one from the same page, which will invalidate the previous one.
- **Authentication occurs via HTTP basic authentication. Use your API token as the basic authentication username, with no password.**
- All API requests must be made over HTTPS. Calls made over HTTP will fail.
- You must authenticate for all requests.

Token Types

User API Tokens

API Token

Current API Token: `api_token`

You can [test the API with your browser](#) (enter your token as the username with no password), or paste the following curl command into your terminal:

```
$ curl https://api.bitsighttech.com/ -u api_token :
```

Your API token is used to authenticate to the BitSight API. To create a new token, click Generate New Token. If you already have an API token, this will destroy your existing token and generate a new one. To delete your token without generating a new one, click Revoke Token.
Note: A user can only have one token at a time. For more information about the BitSight API, see the [API documentation](#).

Each user can set up a “per-user API token.” One token can be generated for each user.

Company API Tokens

Company API Token
A history of previously generated Company Tokens is available to all Admins.

New Token



Write a description before generating token

0 / 255

All Companies ▾

Generate

Previously Generated Tokens

Date	Generated by	Token ending in	Access Control Group	Description	
02-02-2020	Arnold Brown	0000	All Companies	Partner integration	
02-02-2020	Diane Jones	1111	All Companies	Alerts	

←
1
of 1
→

Company API tokens are not user-specific. They can be used without breaking existing integrations if certain user accounts are deleted. For example, one Admin (Customer Admin) might generate a token for their Archer integration. If that Admin leaves the company, the token can either continue to be used or it can be revoked by another Admin.

If using a company API token for the [/alerts](#) API endpoint, the default alert settings are used instead of your own user-specific alert settings, which may return varying query results.

Best Practices

Concurrent Requests

- In general, submitting more requests at the same time will not help overall throughput as the system will take longer to execute each request, and, in the worst case, may return an error. We recommend no more than 3 concurrent API requests as any more may potentially reduce performance. See [Rate Limiting](#).

Peak vs Off Peak Traffic

- Peak traffic hours are from 3 AM to 8 PM EST on weekdays - off hours on weekdays and weekends may offer the most bandwidth for best performance

Rate Limiting

- Our endpoints implement rate limiting to ensure a smooth performance of the BitSight platform. The number of simultaneous requests for certain resources may be reduced.
- Limits:
 - In general, rates are limited to 5000 requests within 5 minutes.
 - In times of heavy processing, rates might be limited to 100 requests within 5 minutes. See [Peak vs Off Peak Traffic](#).
- When your requests are being rate limited a 429 response code will be returned as well as a Retry-After header.
 - It is recommended to account for the 429 response code and when encountered, wait the number of seconds specified in the Retry-After header.

Pagination

- The BitSight API might return a large number of results for a given query and will be paginated. Paginated results include the `next` (or `next_url`), `previous`, and `count` fields.

Filtering

In many cases, filtering relative to your specific use can decrease the amount of data returned, thus increasing operational efficiency.

Example: filtering and response times for Saperix Inc. (a940bb61-33c4-42c9-9231-c8194c305db3), a demo company with a large number of findings, and the companies/findings endpoint (an endpoint that returns a large amount of data):

- With no filtering (all findings for Saperix Inc.):
 - response takes 2 minutes 50 seconds
- Suppose we want only SSL Configuration findings (`risk_vector=ssl_configurations` filter):
 - response takes 16.917 seconds

- Suppose we want only SSL Configuration findings that currently impact the company's rating (affects_rating=true&risk_vector=ssl_configurations filters):
 - response takes 11.618 seconds
- Suppose we want only SSL Configuration findings that currently impact the company's rating and have some level of misconfiguration (affects_rating=true&risk_vector=ssl_configurations&details.grade_lt=GOOD&details.grade_gt=NEUTRAL filters):
 - response takes 4.207 seconds

Especially for finding level detail, filtering can yield great efficiency gains for jobs across a large portfolio.

Organization and Identification:

Identification (GUIDs)

- All resources (company, tier, folder, etc.) have a guid
 - For individual companies, you may assign a custom ID to make matching easier to internal records, should you choose to do so
- Guids are used to reference particular resources when querying information about them or manipulating them (e.g. subscribing, unsubscribing, etc.).

Endpoint Organization Logic

- Endpoints are grouped by resource (Company, Folder, Tier, Portfolio, etc.) or specific operation (fast-ratings, company-requests, subscriptions)
- Options and operations are contextual to that resource (i.e. findings are at the Company level and not the Portfolio level)

Broad Endpoints of Note

Name	URL	Description
Alerts	api.bitsighttech.com/ratings/v2/alerts	Retrieve alerts for your Portfolio: <ul style="list-style-type: none"> ● all (last year) ● latest
Companies	api.bitsighttech.com/ratings/v1/companies	Retrieve information for a Company: <ul style="list-style-type: none"> ● Findings

		<ul style="list-style-type: none"> • Search (retrieve Company guid based on domain) • Ratings trend and risk vector grades
Company Requests	api.bitsighttech.com/ratings/v2/company-requests	<p>Perform the following operations related to a Company Request:</p> <ul style="list-style-type: none"> • Request a Company to be mapped • Check status of a request • Cancel a Company mapping request
Enable Access Program	api.bitsighttech.com/ratings/v1/access-requests	<p>Manage your collaboration efforts via the Enable Access Program.</p>
Folders	api.bitsighttech.com/ratings/v1/folders	<p>Perform the following operations related to one of your Folders:</p> <ul style="list-style-type: none"> • Create a Folder • Edit a Folder • Delete a Folder • Add or remove companies in a Folder
Portfolio	api.bitsighttech.com/v2/portfolio	<p>Returns Companies in your Portfolio and can be filtered on criteria such as:</p> <ul style="list-style-type: none"> • Infections • Open Ports • Vulnerabilities • Products • Providers <p>When filtering logic is:</p> <ul style="list-style-type: none"> • Multiple fields = AND • Multiple items for the same field = OR

Rapid Underwriting Assessments	api.bitsighttech.com/v1/fast-ratings	Quickly get rating details for any mapped or unmapped company within 1 minute.
Subscriptions	api.bitsighttech.com/v1/subscriptions	<p>Perform the following operations related to one of your Subscriptions:</p> <ul style="list-style-type: none"> • Subscribe to a Company • Modify (switch license type) a Subscription • Get expired Subscriptions • Remove/delete a Subscription

Specific Endpoints of Note

Name	URL	Description
Search API	api.bitsighttech.com/ratings/v1/companies/search?{query_parameter}	Search for a company in the BitSight inventory using domain or other query parameters.
Company Details	api.bitsighttech.com/ratings/v1/companies/{company_guid}	Get specific details about a company including rating details, rating history, and risk vector grades.
Finding Details	api.bitsighttech.com/ratings/v1/companies/{company_guid}/findings	Get an organization's finding (events and records) details.
Latest Alerts	api.bitsighttech.com/ratings/v2/alerts/latest	Get alerts generated on the most recent date.

Unsubscribe	<pre>api.bitsighttech.com/ratings/v1/subscriptions/{company_guid}</pre>	Unsubscribe from a particular organization.
-----------------------------	---	---

Response Codes

Code	Status	Description
200	Okay	Everything worked as expected.
201	Success	The request was successfully submitted.
400	Bad Request	This can often be due to missing a required parameter.
401	No Authentication	No valid API token was provided.
402	Request Failed	Parameters were valid but the request failed.
403	Unauthorized	You do not have permission to access this resource.
404	Not Found	The specified resource does not exist.
405	Method Not Allowed	An unsupported request type was attempted.
409	Conflict	There's a discrepancy between the request and the target resource. Check the resource, resolve any conflicting information, and then try again. Refer to Cloudflare Troubleshooting for more information.

429	Rate Limit Reached	<p>To maintain performance and ensure a smooth performance of the BitSight platform, the number of simultaneous requests for certain resources may be reduced. While the majority of the BitSight API allows for 20 simultaneous requests, some are limited to a lower amount.</p> <p>We recommend no more than 3 concurrent requests, as any more may potentially reduce performance. Submitting more requests at the same time will not help overall throughput, as the system will take longer to execute each request. In the worst case, it may return an error.</p> <p>Please wait 1 minute, and then try again. We recommend employing an exponential backoff strategy when retrying your calls.</p> <ul style="list-style-type: none"> ● In general, rates are limited to 5000 requests within 5 minutes. ● In times of heavy processing, rates might be limited to 100 requests within 5 minutes.
500 502 503 504	Server Errors	Something went wrong on the BitSight end.
524	Time Out	The connection to the web server was successful, but the connection timed out. Refer to Cloudflare Troubleshooting for more information.

BitSight Rating Types

- **Rapid Underwriting Assessment (RUA)/Fast Ratings**
 - Rapid Underwriting Assessments (RUA) is a “pay-per-use” service that allows you to quickly get rating details for any client within 1 minute.
 - Rapid Underwriting Assessments does not provide findings details for risk vector grades.
- **Provisional**
 - Unlike a fully mapped BitSight-curated Rating, Provisional Ratings are of companies that have not yet been fully mapped. They’re created by mapping assets through an entirely automated discovery process, which is the first step of the full network mapping process.
 - While a Provisional Rating report is accurate, it may be missing some information when compared to a fully mapped, BitSight-curated Rating report.

- **Curated**
 - A BitSight curated rating is made up of the resulting network footprint and has undergone the full mapping process.
 - Covers all domains and IP addresses associated with a company and any self-published companies.

Job-Related Tasks

Underwriting:

- [Subscribe to a new company](#)
- [Get data for a new insured](#)
- [Get rating history and risk vector grades for an existing company in your portfolio](#)
- [Get detailed findings for a company in your portfolio](#)

Loss Control:

- [Enable Client Access to request remediation activity](#)
- [Get latest alerts generated by your portfolio](#)
- [Get all alerts generated for your portfolio](#)
- [Get companies with a host vulnerable to a particular vulnerability, infected with a specific infection, with a specific port/service exposed, etc](#)
- [Get rating history and risk vector grades for all companies in your portfolio](#)

Portfolio Management:

- [Get companies in your portfolio](#)
- [Subscribe to a new company](#)
- [Remove a Subscription](#)
- [Get companies using a particular provider or providers](#)
- [Get companies using a particular product or products](#)

Task-Related Flows

Get companies in your portfolio:

- A GET [request to the portfolio endpoint](#) will return certain data for every company in your portfolio.
- A key data point in the return is the company's GUID, which is a unique identifier for a company and can be used to query additional information related to the particular company

Get data for a new insured:

- Call [companies/search](#) with the domain of the company
- The response will return a list of possible results for the domain
 - If no company is returned:
 - send POST request to the [company-requests](#) endpoint with the domain as the domain in the body of the request
 - A [provisional](#) rating will be created that will be available within 48 hours
 - This will queue the company for curation and a [BitSight Curated](#) rating report will be available in 3-5 business days in most cases
 - If a rating is needed immediately for underwriting or quoting, send a POST request to the [fast-ratings](#) endpoint (with the domain as the url parameter in the body) and a rating history and risk vector grades will be returned within a minute
 - once the company is mapped, findings data will be available
- Using the GUID of the first element in the list as the GUID in the request body, send a POST request to the [Subscriptions](#) endpoint

- The first (0th) element is recommended, since this endpoint implements an algorithm with many factors to ensure that the most desired result will be returned first (most importantly the primary rating if one exists)
- Now that you are subscribed, use the GUID to send a GET request to the [companies/{guid}](#) endpoint to retrieve ratings history and risk vector grades for the company
- If detailed findings are necessary, send a GET request to [companies/{guid}/findings](#) to retrieve detailed findings for the company (*please see Best Practices: Filtering for info around getting efficient responses from this endpoint*)

Get rating history and risk vector grades for an existing company in your portfolio:

- Use the GUID for the company to send a GET request to the [companies/{guid}](#) endpoint to retrieve ratings history and risk vector grades for the company
- If detailed findings are necessary, send a GET request to [companies/{guid}/findings](#) to retrieve detailed findings for the company (*please see Best Practices: Filtering for info around getting efficient responses from this endpoint*)

Get detailed findings for a company in your portfolio:

- Send a GET request to [companies/{guid}/findings](#) to retrieve detailed findings for the company
- Please see [Best Practices: Filtering](#) for info around getting efficient responses from this endpoint.

Get rating history and risk vector grades for all companies in your portfolio:

- Send a GET request to the [Portfolio](#) endpoint. This will return several data points, but most importantly the GUID for each company.
- For each GUID returned, send a GET request to the [companies/{guid}](#) endpoint to retrieve rating history and risk vector grades.

Get companies with a host vulnerable to a particular vulnerability, infected with a specific infection, with a specific port/service exposed, etc:

- Send a GET request to the [Portfolio](#) endpoint with the relevant filter specified:
 - Note that for an individual filter you can supply multiple vulnerabilities, infections, ports, services, etc. as a list
 - As noted above, filter logic works as follows:
 - When filtering logic is:
 - Multiple fields = AND
 - Multiple items for the same field = OR
 - This will return the companies impacted by the infection, vulnerability, etc.
 - If additional details are needed (such as impacted hosts, duration, etc.), send a GET request to the [companies/{guid}/findings](#) endpoint filtering by the applicable risk vector and vulnerability/infection/port/service/etc.

Subscribe to a new company:

- Call [companies/search](#) with the domain of the company
 - If a large number of subscriptions need to be applied, this operation can also be performed in [bulk](#)
- The response will return a list of possible results for the domain

- If no company is returned:
 - send POST request to the [company-requests](#) endpoint with the domain as the domain in the body of the request
 - A [provisional](#) rating will be created that will be available within 48 hours. This will queue the company for curation; in most cases, a [BitSight Curated](#) rating report will be available in 3-5 business days.
 - If a rating is needed immediately for underwriting or quoting, send a POST request to the [fast-ratings](#) endpoint (with the domain as the url parameter in the body) and a rating history and risk vector grades will be returned within a minute
 - once the company is mapped, findings data will be available
- Using the GUID of the first element in the list as the GUID in the request body, send a POST request to the [Subscriptions](#) endpoint
 - The first (0th) element is recommended, since this endpoint implements an algorithm with many factors to ensure that the most desired result will be returned first (most importantly the primary rating if one exists)

Remove a Subscription:

- Unsubscribe a single company by sending a DELETE request to the [subscriptions](#) endpoint specifying the guid in the body
- If a large number of subscriptions need to be removed, this operation can also be performed in [bulk](#)

Get companies using a particular provider or providers:

- Send a GET request to the [Portfolio](#) endpoint with the providers= filter
 - Note that this may be specified as a list of providers

Get companies using a particular product or products:

- Send a GET request to the [Portfolio](#) endpoint with the products= filter
 - Note that this may be specified as a list of products

Get all alerts generated for your portfolio:

- Send a GET request to the [alerts](#) endpoint
 - This will return all alerts generated by your portfolio for the last year. It is highly recommended that you filter using the alert_date_gt/alert_date_gte filter or use the alerts/latest endpoint

Get latest alerts generated by your portfolio:

- Send a GET request to the [alerts/latest](#) endpoint
 - This will return all alerts from the latest alerts generation date
 - Use if you intend to pull alerts daily

Enable Client Access to request remediation activity:

- When interacting with an organization based upon their BitSight rating, findings, etc. it is always recommended that you provide them access. This is to ensure that they have access to the details necessary to remediate the issue at hand.
- To enable client access, send a POST request to the [access-requests](#) endpoint with the following information in the body of the request:
 - requestee_company_guid (required)
 - requestee_friendly_name
 - [string, body] The preferred name of the recipient.
 - Default: If empty, the user that's pre-attached with the recipient company is used.
 - requestee_formal_name
 - [string, body] The full name of the recipient.
 - Default: If empty, the user that's pre-attached with the recipient company is used.
 - requestee_email
 - [string, body] The email address of the recipient of the access request. The email domain must match a domain that belongs to the requested company.
 - Default: If empty, the user that's pre-attached with the recipient company is used.
 - requestee_phone
 - [string, body] The phone number of the recipient.
 - message
 - [string, body] Introduce yourself and the purpose of your collaboration request.
 - notes
 - [string, body] Document private notes for other users in your organization.
 - ccs
 - [array, body] Send a carbon copy (CC) of the invitation email, but not the activation email. Comma-separated email addresses.

API Calls

Alerts

Get all alerts for your portfolio:

- [Alerts](#)
 - Endpoint: GET
`https://api.bitsighttech.com/ratings/v2/alerts`
 - This will return all alerts generated by your portfolio for the last year. It is highly recommended that you filter using the `alert_date_gt/alert_date_gte` filter or use the `alerts/latest` endpoint

Get latest alerts for your portfolio:

- [Alerts](#)
 - Endpoint: GET
`https://api.bitsighttech.com/ratings/v2/alerts/latest`

Companies

Search for a company in BitSight:

- [Search API](#)
 - Endpoint: GET
`https://api.bitsighttech.com/v1/companies/search?domain=google.com`
- The response will return a list of possible results for the domain

Get rating and risk vector data for an existing company in your portfolio:

- [Company Details](#)
 - Endpoint: GET
`https://api.bitsighttech.com/ratings/v1/companies/{company_guid}`

Get detailed findings for a company:

- [Findings API](#)
 - Endpoint: GET
`https://api.bitsighttech.com/customer-api/v1/companies/{company_guid}/findings`
 - Example:
 - Filter on vulnerabilities:
`https://api.bitsighttech.com/customer-api/v1/companies/fb2d3117-9dfe-4b56-9712-26b4a45c79bd/findings?affects_rating=true&expand=remediation_history%2Cattributed_companies%2Cremediation_validation&limit=40&offset=0&q=&sort=-last_seen&vulnerabilities=CVE-2010-529`
 - Filter on infection:
`https://api.bitsighttech.com/customer-api/v1/companies/41ee2c99-b108-4d34-9225-13de585d3294/findings?affects_rating=true`

&details.infection.family=Trickbot&expand=remediation_history%2Cattributed_companies%2Cremediation_validation&limit=40&offset=0&q=&sort=-last_seen

- Get vulnerabilities currently impacting the company's rating (Patching Cadence Risk Vector):
https://api.bitsighttech.com/v1/companies/1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9/findings?format=json&affects_rating=true&risk_vector=patching_cadence
- Get all vulnerabilities within the last year (Patching Cadence Risk Vector):
https://api.bitsighttech.com/v1/companies/1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9/findings?format=json&risk_vector=patching_cadence
- Get all vulnerabilities within the last 60 days (Patching Cadence Risk Vector):
https://api.bitsighttech.com/v1/companies/1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9/findings?format=json&affects_rating=true&risk_vector=patching_cadence&last_seen_gte=2022-01-28
- For the previous two examples, you may narrow down the data to just unremediated vulnerabilities by searching for the "is_remediated" key. Cases where is_remediated=false mean that when we last checked the asset, the vulnerability was present
- Get desktop software, mobile software, and server software findings currently impacting the company's rating:
https://api.bitsighttech.com/v1/companies/a5e23bf0-38d4-4cea-aa50-19ee75da481d/findings?format=json&affects_rating=true&risk_vector=desktop_software,mobile_software,server_software
 - this data could be further prefiltered to reduce the size of the data returned by also specifying details.grade_lt=GOOD and optionally details.grade_gt=NEUTRAL:
https://api.bitsighttech.com/v1/companies/a5e23bf0-38d4-4cea-aa50-19ee75da481d/findings?format=json&affects_rating=true&risk_vector=desktop_software,mobile_software,server_software&details.grade_lt=GOOD&details.grade_gt=NEUTRAL

Company Requests

Request a new company in the BitSight inventory:

- Submit company request one at a time
 - [Company requests API](#)
 - Endpoint: POST
https://api.bitsighttech.com/customer-api/v2/company-requests/
 - Payload:
{

```
"domain": "bluseas.com"
}
```

- A 201 status code indicates that the response was successfully submitted
- A [provisional](#) rating will be created that will be available within 48 hours
- This will queue the company for curation and a [BitSight Curated](#) rating report will be available in 3-5 business days in most cases
- Once a company (Provisional or curated) is created, you will be able to search for it using the [Search](#) endpoint. We recommend calling the Search endpoint to see if a [provisional](#) or [curated](#) company is already available prior to requesting the company.

[Enable Access Program](#)

Enable Client Access:

- [Access Request API](#)
 - Endpoint: POST
https://api.bitsighttech.com/rating s/v1/access-requests
 - Payload: Enable Access Program

```
{ "requestee_company_guid": "dc24dc48-268a-4e44-8510-c2ae7185668e",
  "requestee_friendly_name": "Bob",
  "requestee_formal_name": "Bob Bobson",
  "requestee_email": "bob@bobson.com",
  "requestee_phone": "555-555-5555",
  "message": "This is a message to the recipient.",
  "notes": "This is a note to anyone in my organization." }
```

[Portfolio](#)

Get all companies in your portfolio:

- [Portfolio V2 API](#)
 - Endpoint: GET
https://api.bitsighttech.com/customer-api/v2/portfolio
- This will return certain information for every company in your portfolio (guid, custom_id, name, etc.)

Get companies impacted in your portfolio:

- Send a GET request to the Portfolio endpoint with the relevant filter specified:
 - [Portfolio V2 API](#)
 - Endpoint: GET
https://api.bitsighttech.com/customer-api/v2/portfolio
 - **Portfolio level filtering examples:**
 - Get all companies impacted by a specific infection (ex. Zloader & Conficker)
https://api.bitsighttech.com/v2/portfolio?format=json&infections=Zloader%2CConficker
 - Get all companies impacted by a specific open port (ex. Port 3389 & Port 137)

`https://api.bitsighttech.com/v2/portfolio?format=json&open_ports=Port%203389%2CPort%20137`

- Get all companies impacted by a specific vulnerability (ex. BlueKeep & POODLE)

`https://api.bitsighttech.com/v2/portfolio?format=json&vulnerabilities=BlueKeep%2CPOODLE`

- Note that the queries above return the impacted companies for the entire portfolio; for the details around the finding itself, you will need to make the appropriate query to the findings endpoint

- When filtering logic is:
 - Multiple fields = AND
 - Multiple items for the same field = OR

- Filter by folder(s) and infection(s)

`https://api.bitsighttech.com/v2/portfolio?format=json&folder=d87cf106-126e-4bbc-99f7-12ee0e069ff4%2C9c883df2-08b6-4df1-a2c4-46c609418565&infections=Zloader%2CConficker`

- The examples above will return the companies impacted by the infection, vulnerability, etc.

Get companies using a particular provider:

- [Portfolio V2 API](#)
 - Endpoint: GET
`https://api.bitsighttech.com/v2/portfolio?format=json&providers=Google%20Corporation`

Get companies using a particular product:

- [Portfolio V2 API](#)
 - Endpoint: GET
`https://api.bitsighttech.com/v2/portfolio?format=json&products=Google%20Cloud`

Rapid Underwriting Assessments

Request a Rapid Underwriting Assessment:

- [Rapid Underwriting Assessments API](#)
 - Endpoint: POST
`https://api.bitsighttech.com/ratings/v1/fast-ratings`
 - Payload:


```
{
    "url": "www.example.com",
    "generate_report": "boolean",
    "industry": "industry_name"
}
```
- The response will return risk vector grades and rating history after a short delay - see [Rapid Underwriting Assessment rating type](#)

Subscriptions

Subscribe to companies:

- For a single company
 - [Subscription API](#)
 - Endpoint: POST
https://api.bitsighttech.com/customer-api/subscriptions
 - Payload:

```
{ "continuous_monitoring": { "companies": [ { "guid": "a5e23bf0-38d4-4cea-aa50-19ee75da481d" } ] } }
```
- For bulk changes(for companies already in the portfolio)
 - [Subscription API \(Bulk\)](#)
 - Endpoint: POST
https://service.bitsighttech.com/customer-api/subscriptions
 - Payload:

```
{ "add": [ { "guid": "a5e23bf0-38d4-4cea-aa50-19ee75da481d", "folder": [ "my_folder", "my_other_folder" ], "tier": "tier_1", "type": "continuous_monitoring" } ] }
```

Unsubscribe:

- Unsubscribe a single company
 - [Company subscription API](#)
 - Endpoint: DELETE
https://api.bitsighttech.com/customer-api/subscriptions/{company_guid}
- Bulk unsubscribe multiple companies
 - [Company subscription API \(Bulk\)](#)
 - Endpoint: POST
https://api.bitsighttech.com/ratings/v1/subscriptions/bulk
 - Payload:

```
{ "delete": [ { "guid": "a5e23bf0-38d4-4cea-aa50-19ee75da481d", } ] }
```

Other Resources

- BitSight Knowledge Base API Documentation
- Swagger UI - [v1](#) & [v2](#)
 - Will provide useful information on the structure of API endpoints, that developers can use to structure queries.
 - Can also run test queries to become familiar with the endpoints

FAQ

[Q]: What do the errors I'm receiving from BitSight's Insurance API mean?

[A]: There are a few classes of API errors that you may encounter

- 202 - your request was processed successfully, you may have not seen an error, but you are not seeing data. This may happen as you try to pull RUAs for domains with too many assets. We recommend trying this again after 5 minutes as the cached results will improve the likelihood that your request will succeed
- 404 - generic response code indicating no resources found. This may suggest that there is not enough data for BitSight to process a rating in the RUA case
- 429 - indicates that too many requests are being made and can be alleviated by lowering the number of concurrent requests and attempting the request again (after 5 minutes)
- 502/503/504 - indicates high traffic, we recommend retrying the request. If the problem is persistent, please contact [BitSight Support](#) as this may indicate a platform issue

[Q]: I'm getting throttled by the BitSight Insurance API, what actions can I take to make sure my requests are getting through?

[A]: Throttling can potentially occur either during peak traffic hours or when too many concurrent requests are made to a single endpoint (see above for [peak vs off-peak hours](#)). We recommend submitting no more than 3 concurrent requests; if you continue to see problems, trying fewer may yield some benefit - see [Best Practices: Rate Limiting](#)

[Q]: I've noticed that the GUID for a company I was monitoring has changed and no longer points to the correct company, what should I do?

[A]: GUID attrition is uncommon, though may result due to duplicate companies getting cleaned up in our system or may be a direct result of the changing in company trees. CustomID fields are handled only by a customer, so collecting data based on that should always return a correct match.