Query IP Address Risk

HTTP Verb	URI	What is it?	Auth Required?	Available As
GET	`/addresses/{ip}`	Allows the caller to view the risk for a given IP address	Yes	application/json

URI Parameters

Name	Notes	ABNF *(What is 'ABNF'?)*

`ip`	The IP address that the caller is querying the risk of	`ip= 1*3(DIGIT) "."`
		`    1*3(DIGIT) "."`
		`    1*3(DIGIT) "."`
		`    1*3(DIGIT)`

Query String Parameters

Name	Notes	ABNF
`risk-threshold`	**Optional:** Used to filter the results to a risk factor that equals or exceeds a given threshold. The higher the number, the more risky the IP address is considered.	`risk-threshold= 1*2(DIGIT)` Allowed range: [0, 10] Default: 0

Response Codes

Condition	HTTP Code	Comments
No errors, the IP address is not considered a risk	204 (No Content)	Golden path
No errors, the IP address is a risk, but is below the requested "risk-threshold"	204 (No Content)	Golden path
No errors, the IP address is considered a risk and no "risk-threshold" was specified	200 (Ok)	Golden path
No errors, the IP address is considered a risk and the risk level is equal or above the "risk-threshold" was specified	200 (Ok)	Golden path
Specified {ip} is malformed	400 (Bad Request)	In this context, "malformed" indicates that there are unpermitted characters or length violations
The "risk-threshold" parameter is not an integer	400 (Bad Request)	
The "risk-threshold" parameter is out of the allowed range	400 (Bad Request)	
Missing or expired client certificate	401 (Unauthorized)	
Client certificate trust chain cannot be validated or is untrusted	403 (Forbidden)	
Client certificate is not authorized for this endpoint	403 (Forbidden)	
Internal server error	500 (Internal Server Error)	

Authentication & Authorization

A client certificate is required.

Client Certificate Scenarios:
- The client certificate must be valid and chain to a trusted root.
- The client certificates are authorized for this endpoint.

Response Caching

Caching should be configurable for this API.

When disabled (or set to zero), the API should respond with: "Cache-Control: no-store, no-cache".
When enabled, the API should respond with: "Cache-Control: max-age=XXXX, private" where XXX is the cache period in seconds.

Request Headers

	Notes	ABNF
`AD-CorrelationId`	**Optional -** If a value is provided with the request, it will be used as a key intended to tie together related activities for this request; it will be sent for any calls to external services and resources that were triggered by this request as well. If not provided, a unique value will be generated for the request.	`AD-CorrelationId = 1*50(ALPHA / DIGIT / "-" / "." / "_")`

Request Body

None

Response Headers

Name	Notes	ABNF
AD-CorrelationId	The identifier for the request intended to tie together related activities for this request; it will be sent for any calls to external services and resources that were triggered by this request as well.	AD-CorrelationId = 1*50(ALPHA / DIGIT / "-" / "." / "_")

Response Body

For a 204 response, no body is returned.

For a 200 response code, the response body contains the details of the IP:

Type	Field Name	Description	Default
HashSet<string, URI Reference>	Links	A set of related resource links.	One "self" link, that identifies this resource (including the query string, if necessary).
Risk Metadata	Metadata	The set of metadata that offers context around the risk identified for the IP address	null

Risk Metadata

Type	Field Name	Description	Default
byte	RiskLevel	The level of risk associated with the IP address. The higher the value, the more risky the IP address is considered. In the case where multiple sources identify the IP address, the highest associated risk will be reflected here. Valid range: [0, 10]	0
Vector<string>	Sources	The set of sources for the risk information	null

URI Reference

Type	Field Name	Description	Default
string	Uri	The fully qualified URI to be used for addressing the resource	""
enum	Method	The HTTP method to use for interacting with the resource. Valid members: • GET • POST • PATCH • PUT • DELETE	GET
List<enum>	Authentication	The type of authentication supported by the resource. Valid members: • Anonymous • ClientCertificate	Anonymous

Example (JSON)

```
{
    "links" :
    [
        "self" :
        {
            "uri"            : "https://www.root.com/addresses/192.168.0.1?risk-threshold=6",
            "method"         : "GET",
            "authentication" : [ "ClientCertificate" ]
        }
    ],
    "metadata" :
    {
        "riskLevel" : 8,
        "sources"   : [ "The Farmer's Almanac", "My cousin, Vinnie" ]
    }
}
```

For a 400 series response code, other than 401, 403, and 404, the response body contains context around
the failure to allow callers to present the proper messaging:

Type	Field Name	Description	Default
Vector<Error Information>	Errors	The error scenarios that the caller encountered	An empty set

Error Information

Type	Field Name	Description	Default
enum	Code	A code that describes the error scenario Valid members: • Unknown, • RiskThresholdMalformed • RiskOutOfRange	Unknown
string	Description	A short, non-localized, human readable string intended to clarify the problem. This text is intended to help debug calls and should not be considered user-facing.	""

Example (JSON)

```
{
    "errors" :
    [
        {
            "code"        : "RiskThresholdMalformed",
            "description" : "The risk threshold was not an integer"
        }
    ]
}
```