Logging API

This document describes the Logging **API** available for the Menlo Security Isolation Platform (MSIP). This API allows customers to leverage the Menlo Security Cloud Isolation Platform (SaaS) to extract their tenant logs locally.

Note

The **API** is updated as new parameters are added. Please contact Menlo Security Support at https://csportal.menlosecurity.com/hc/en-us for any questions or requests for updates to the documentation.

Logging API Details

Root URL: `https://logs.menlosecurity.com/ api`

Title: **Fetch Logs**

URL: **/rep/v1/fetch/client_select**

Method: **POST**

Authentication and Security

Authenticate all requests with HTTPS, Auth Token, and IP Whitelisting

Resource Information

Data Parameters: The data parameter is in the format: **{token: [alphanumeric], log_type: [web|audit|email|attachment|smtp|isoc], pagingIdentifiers: { [pagingIdentifiers1], [pagingIdentifiers2],...[pagingIdentifiersN]}}**.

Example:

```
{token: "[alphanumeric]", log_type: "web", pagingIdentifiers:
  {
    "next_time": "2020-08-26T11:38:25.894Z",
    "last_iteration": true,
    "hashes": {
       "65653099c7e214052fd8530b6fbdb5d8": 0
    }
 }
```

The **token** parameter is a 32 byte hash that acts as a shared secret to work with the **API** .

The **log_type** parameter defines which type of MSIP log is being exported:

- **web**: Web access logs. This is the default log type returned if `log_type` is not specified.
- **audit**: Admin portal administrator audit logs.
- **email**: Email URL rewriter logs.
- **attachment**: Email attachment logs.
- **smtp**: Logs of SMTP messages processed by the SMTP transform and restore nodes.
- **isoc**: Alerts generated by the Menlo Threat Intelligence platform to help SoC analysts.

The **pagingIdentifiers** parameter is an internal parameter used for log pagination as needed if the request returns more than the maximum number of records (up to 10,000). It should **not** be used for interpretation and the value and format of the parameter may change between releases without any prior communication.

Note

There is a rate limit of 2000 **API** requests per 120 seconds.

Response Details:

Each request returns a maximum of 10,000 records (default limit is 1000). Each response includes a paging dictionary (specified by the `pagingIdentifiers` key).

Note that the `pagingIdentifiers` key is empty on the first page, but if the query generates more results than the set limit, the client must update their local paging directory with the `pagingIdentifiers` key from the response and post it as a parameter with the next request. Continue requesting pages until you receive no data for the time period specified.

Operational logs are output in KVF, CEF and LEEF formats (for details, see Syslog Events).

For Menlo Security Cloud Isolation Platform (SaaS) users, the following URL parameters are provided (Private Cloud users redirect logs to their log server and do not use the **API**).

Note

The logging **API** may occasionally return an empty 200 response when a JSON object is expected. This can occur if there is no log data for the log request (e.g., an audit log for offpeak hours like 22:00 to 22:30). The query will return `Content-Length: 0`.

Please see the **API** Python Script CS Portal page for the latest Python scripts and examples.

URL Parameters

URL Parameter	Description	Example
start	UTC start time in seconds since epoch (1 January 1970). This is set to 5 minutes prior to the current time by default.	1454964247
format	The format used for log output (JSON, KVF, CEF or LEEF). Note that CEF and KVP are wrapped in JSON and you must put single quotes around your URL to avoid bash interpretation of question marks or ampersands if these formats are used.	format=CEF
end	UTC end time in seconds since epoch (1 January 1970). This is set to the current time by default	end=1455569047
limit	Results limit as an integer. The default is 1000 (maximum allowed value).	limit=100

Testing the API

To test the **API**, use curl and a token.

1. Obtain your token to work with the **API**.
2. Enter a command using curl to fetch data. The following example fetches the last 5 minutes of data and outputs it in the JSON format (default):

```
curl --header 'Content-Type: application/json' --data '{"token": "[alphanumeric]"}'
https://logs.menlosecurity.com/ api /rep/v1/fetch/client_select
```

3. If there is an error in your key, an Unauthorized response is sent:

```
<html><title>401: Unauthorized</title><body>401:Unauthorized</body></html>
```

4. If there is no data, the following blank output is returned:

```
{
  "timestamp": "2020-08-04T02:57:46.902Z",
  "result": {
    "pagingIdentifiers": {},
    "events": []
  }
}
```

5. The parameters and examples are provided in the sections below.

Web Logs

Sample Response Details (JSON)

```
{
    "timestamp": "2019-04-10T21:00:02.599Z",
    "result": {
       "metrics": [
          "last_access",
          "rows"
       ],
       "events": [
          {
             "event": {
                "top_url": "http://example.com",
                "egress_country": "US",
                "domain": "example.com",
                "protocol": "http",
                "risk_tally": "-1",
                "origin_ip": "130.65.255.101",
                "has_password": "NA",
                "file_size": "NA",
                "origin_country": "FR",
                "x-client-country": "US",
                "browser_and_version": "Chrome_72",
                "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/72.0.3325.181 Safari/537.36",
                "egress_ip": "54.111.221.123",
                "threats": "cats_Phishing & Fraud",
                "severity": "5",
                "event_time": "2019-04-10T21:00:40.548000",
                "dst": "130.65.255.101",
                "filename": "NA",
                "risk_score": "low",
                "version": "2.0",
                "sha256": "fd1aee671d92aba0f9f0a8a6d5c6b843e09c8295ced9bb85e16d97360b4d7b3a",
                "soph_dlp_ref": "NA"
                "tab_id": "1",
                "xff_ip": "NA",
                "product": "MSIP",
                "vendor": "Menlo Security",
                "request_type": "GET",
                "pe_reason": "6c6ea27d-5350",
                "categories": "Education",
                "x-client-ip": "12.206.221.226",
                "name": "page_request",
                "url": "http://example.com",
                "response_code": "200",
                "userid": "admin@menlosecurity.com",
                "full_session_id": "KbJQIDPS-1"
                "pe_action": "isolate",
                "threat_types": "Phishing",
                "ua_type": "supported_browser",
                "content-type": "text/html; charset=iso-8859-1",
                "is_iframe": "true",
                "region": "us-west-1b"
             }
          }
       ],
       "pagingIdentifiers": {

"pnr_page_request_2019-04-10T21:00:00.000Z_2019-04-10T21:01:03.456Z_2019-04-10T21:00:00.000Z": 1
       }
    }
}
```

Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2019-04-10T21:00:02.599Z
top_url	Top level URL (in case of iframe)	https://example.com
egress_country	Egress IP country (isolation instance)	US
domain	Domain part of the URL	example.com
protocol	The protocol used for the session (http or https)	http
risk_tally	Count of risks encountered	4
origin_ip	Actual IP address of the destination server	130.65.255.101
has_password	Presence of password in form POST request	false
file_size	The size (in bytes) of a file in a file upload/download event	NA
origin_country	Country of actual IP address of the destination server (origin_ip)	FR
x-client-country	Country for IP request from user	US
browser_and_version	The client browser and its version. Non-browser returns a response of undefined_undefined.	Chrome_65
user-agent	The software (software agent) acting on behalf of a user (commonly a web browser).	Mozilla/5.0 (Macintosh; Intel Mac Chrome/65.0.3325.181 Safari/53
egress_ip	IP address for outbound flow (typically from a private network to the Internet)	54.111.221.123
threats	Threat type identified by Menlo Security internal data (what the Risks field is set to)	cats_Phishing & Fraud

Response Parameter	Description	Example
severity	The severity level for the session. This is currently fixed at 5.	5
event_time	The access initiate date and time	2018-04-10T21:00:40.548000
dst	Destination IP that proxy DNS lookup resolved to (may sometimes be a list of IP addresses)	130.65.255.101
filename	The filename of the file being uploaded or downloaded.	NA
risk_score	Risk calculated for URL	low
version	The Menlo Security product version (currently fixed at 2.0)	2.0
tab_id	Tab creation number within a surrogate (used to track how an individual tab is navigated by a user)	1
xff_ip	X-Forwarded-For HTP header field originating client IP address	NA
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
vendor	The product vendor name (Menlo Security)	Menlo Security
request_type	The method type for the request (GET, PUT, POST, etc.)	GET
pe_reason	Web policy rule ID responsible for Menlo Security action. This can be empty for some cases.	6c6ea27d-5350
categories	Category Rules Category type classification (e.g., General, Education, Download Sites, etc.)	Education
x-client-ip	Source IP	12.206.221.226

Response Parameter	Description	Example
name	Request type	page_request
url	The Destination URL	https://example.com
response_code	HTTP response status code	200
userid	The User ID for the log (in Anonymous mode, this is *anon-xxx*).	admin@menlosecurity.com
full_session_id	Unique ID for a page load (used as a correlation ID for other events: uploads/downloads/etc.)	KbJQIDPS-1
pe_action	The Menlo Security action taken for the session (*Isolate*, *Allow*, *Block*, or *Direct*). Direct actions are external application links that a user may click to launch through their web browser (e.g., anchor links, javascript navigations and mailto links)	isolate
threat_types	Top level risk	Phishing
ua_type	The type of user agent (supported/unsupported/non browser)	supported_browser
content-type	Page type	text/html; charset=iso-8859-1
is_iframe	Is inline frame (iframe) element (true/false)	true
cached	Indicates whether the resource was obtained from the isolated browser's cache (True) or by downloading from the origin server (False)	True
sha256	SHA256 hash of this file or document or text. This provides a cryptographically unique identifier.	fd1aee67...
soph_dlp_ref	DLP log link	NA
referer	Page request referer address	https://www.adobe.com

Response Parameter	Description	Example
region	AWS region and availability zone	us-west-1b
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	pnr_page_request_2019-04-10T2
casb_app_name	Cloud application name (for CASB events)	DropBox
casb_org_name	Application organization name	Dropbox Inc.
casb_cat_name	Application category ID	Cloud File Sharing
casb_fun_name	Application function name	upload
casb_risk_score	Menlo risk score for application (0-10)	3
casb_profile_name	Menlo CASB profile name attached to application or exception rule	upload block
casb_profile_type	Menlo CASB profile type (sanctioned/unsanctioned /unclassified)	unclassified
casb_profile_id	Menlo CASB profile ID	e47cecae-721f...

DLP Logs

Sample Response Details (JSON)

```
{
    "timestamp": "2020-03-09T17:16:22.227Z",
    "result": {
        "metrics": [
            "last_access",
            "rows"
        ],
        "events": [
            {
                "event": {
                    "dst_url": "http://tinyupload.com/",
                    "user_input": "false",
                    "protocol": "http",
                    "file_type": "CSV",
                    "domain": "tinyupload.com",
                    "alerted": "false",
                    "ccl_ids": "CreditordebitcardnumbersGlobal",
                    "severity": "5",
                    "event_time": "2020-03-09T17:16:22.227000",
                    "event_id":
"a4c2161b3f81a287ec46d3c993a33f3b97ded5fd854fa184e7f50679303111ce",
                    "filename": "credit_cards.csv",
                    "version": "2.0",
                    "sha256": "fd1aee671d92aba0f9f0a8a6d5c6b843e09c8295ced9bb85e16d97360b4d7b3a",
                    "status": "dirty",
                    "product": "MSIP",
                    "ccl_match_counts": "1",
                    "vendor": "Menlo Security",
                    "ccl_scores": "1",
                    "rule_name": "Credit card block rule",
                    "request_type": "GET",
                    "src_url": "http://tinyupload.com/",
                    "categories": "Download Sites",
                    "stream_name": "/safefile-input/working_file",
                    "name": "file_upload",
                    "userid": "admin@menlosecurity.com",
                    "action": "block",
                    "rule_id": "1f3ef32c-ec62-42fb-8cad-e1fee3375099"
                }
            }
        ],
        "pagingIdentifiers": {
            "dlp_31_2020-03-09T17:11:48.987Z_2020-03-09T17:16:48.987Z_2020-03-09T17:00:00.000Z": 0
        }
    }
}
```


Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2020-03-09T17:16:22.227Z

Response Parameter	Description	Example
dst_url	Destination URL	http://tinyupload.com
user_input	Whether or not this event was generated as a result of user form input	false
protocol	The protocol used for the session (http or https)	http
file_type	Type of file that triggered the DLP violation	CSV
domain	Domain part of the URL	tinyupload.com
alerted	Whether or not an email alert was sent to a DLP Auditor profile	false
ccl_ids	Name of DLP dictionary that was violated. If there are multiple violations, this will be an array of strings	CreditordebitcardnumbersGlobal
severity	The severity level for the session. This is currently fixed at 5.	5
event_time	The access initiate date and time	2020-03-09T17:16:22.227000
event_id	Unique identifier for the DLP request (corresponds to the file_id in web log if this is a file upload)	a4c216...

Response Parameter	Description	Example
filename	The name of the file that triggered the DLP violation (for file uploads)	credit_cards.csv
version	The Menlo Security product version (currently fixed at 2.0)	2.0
sha256	SHA256 hash of this file or document or text. This provides a cryptographically unique identifier.	fd1aee67...
status	Result from the DLP engine (currently fixed at *dirty*)	dirty
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
ccl_match_counts	Number of matches of the string that caused the violation. If there are multiple violations, this will be an array of match counts in the same order as the list of dictionaries from `ccl_ids` field.	1
vendor	The product vendor name (Menlo Security)	Menlo Security

Response Parameter	Description	Example
ccl_scores	DLP score from the dictionary that caused the violation. If there are multiple violations, this will be an array of DLP scores in the same order as the list of dictionaries from `ccl_ids` field.	1
rule_name	Name of the DLP policy rule that was violated	Credit card block rule
request_type	The method type for the request (GET, PUT, POST, etc.)	POST
src_url	Source URL	http://tinyupload.com/
categories	Category Rules Category type classification (e.g., General, Education, Download Sites, etc.)	Download Sites
stream_name	Internal name used for the file (usually *working_file*) or text stream (uid)	1a856c756fea
name	Request type	file_upload
userid	User ID for the log (in Anonymous mode, this is *anon-xxx*)	admin@menlosecurity.com
action	Menlo Security action taken for session (block or log)	block

Response Parameter	Description	Example
rule_id	DLP policy rule identifier responsible for the action taken	1f3ef32...
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	pnr_page_request_2019-04-10T21:00:00.000Z

Audit Logs

Sample Response Details (JSON)


```
{
    "timestamp": "2019-04-10T20:51:10.488Z",
    "result": {
       "metrics": [
          "last_access",
          "rows"
       ],
       "events": [
          {
             "event": {
                "product": "MSIP",
                "sub_event_type": "logout",
                "uid": "admin@menlosecurity.com",
                "event_time": "2019-04-10T20:55:26.347000",
                "name": "authentication",
                "version": "2.0",
                "audit_actions": "logout",
                "vendor": "Menlo Security",
                "rev_id": "NA",
                "severity": "5"
             }
          }
       ],
       "pagingIdentifiers": {

"admin_audit_log_2019-04-10T20:50:29.465Z_2019-04-10T20:55:29.465Z_2019-04-10T20:00:00.000Z": 0
       }
    }
}
```


Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2019-04-10T20:51:10.488Z
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
sub_event_type	Sub request type	logout

Response Parameter	Description	Example
uid	The User ID for the log (in Anonymous mode, this is *anon-xxx*).	admin@menlosecurity.com
event_time	The access initiate date and time	2019-04-10T20:55.26347000
name	Request type	authentication
version	The Menlo Security product version (currently fixed at 2.0)	2.0
audit_actions	Type of action taken	logout
vendor	The product vendor name (Menlo Security)	Menlo Security
rev_id	Revision ID of the policy saved/published.	NA
severity	The severity level for the session. This is currently fixed at 5.	5
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	admin_audit_log_2019-04-10T20:50:29.465Z_

Email URL Rewriter Logs

Sample Response Details (JSON)


```
{
    "timestamp": "2019-04-10T21:16:09.060Z",
    "result": {
       "metrics": [
          "last_access",
          "rows"
       ],
       "events": [
          {
             "event": {
                "delivered_to": "bsmith@company.com",
                "domain": "cnn.com",
                "vendor": "Menlo Security",
                "rewritten": "transform",
                "event_time": "2019-04-10T21:19:47",
                "from": "jdoe@company.com",
                "message_tid": "e52a2c70-3d04-11e8-8a0b-918c2380e1d4",
                "charset": "UTF-8",
                "product": "MSIP",
                "name": "url-rewrite",
                "url": "cnn.com",
                "reason": "default",
                "version": "2.0",
                "email_date": "2019-04-10T14:19:41-07:00",
                "message_id": "CACiMZ7P4LGPwwqbp+dKQ@mail.gmail.com",
                "subject": "Check This Out",
                "to": "bsmith@gmail.com"
                "severity": "5"
             }
          }
       ],
       "pagingIdentifiers": {
          "safemail_2019-04-10T21:16:09.060Z_2019-04-10T21:21:09.060Z_2019-04-10T21:00:00.000Z": 2
       }
    }
}
```


Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2019-04-10T21:16:09.060Z
domain	Domain part of the URL	cnn.com

Response Parameter	Description	Example
vendor	The product vendor name (Menlo Security)	Menlo Security
rewritten	Action performed on the URL present in the email	transform
event_time	The access initiate date and time	2019-04-10T21:19:47
message_tid	Message transaction ID provided within all log messages pertaining to a given message	e52a2c70-3d04-11e8-8a0b-918c2380e1d4
charset	Charset used to encode text containing identified URL	UTF-8
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
name	Request type	url-rewrite
url	Destination URL	cnn.com

Response Parameter	Description	Example
reason	Rationale behind action performed	default
version	The Menlo Security product version (currently fixed at 2.0)	2.0
email_date	Email date	2019-04-10T14:19:41-07:00
message_id	Email identifier	CACiMZ7P4LGPwwqbp+dKQ@mail.gmail.com
severity	The severity level for the session. This is currently fixed at 5.	5
delivered_to	Recipient email address	bsmith@gmail.com
from	Email address in email From: line	jdoe@company.com
subject	Text in email Subject: line	Check This Out
to	Email address in email To: line	bsmith@gmail.com

Response Parameter	Description	Example
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	safemail_2019-04-10T21:16:09.060Z_2019-04-10T

Email Attachment Logs

Sample Response Details (JSON)

```
{
    "timestamp": "2019-04-10T21:16:09.060Z",
    "result": {
       "metrics": [
          "last_access",
          "rows"
       ],
       "events": [
          {
             "event": {
                "product": "MSIP",
                "rvlabs_factor": "0",
                "vendor": "Menlo Security",
                "rewritten": "replaced",
                "event_time": "2019-04-18T11:52:33.459Z",
                "file_type": "PDF",
                "filename": "invite.ics",
                "from": "jdoe@company.com",
                "reply_to": "jdoe@company.com",
                "sender": "Google <calendar notification@google.com>",
                "bytes": "17036",
                "delivered_to": "bsmith@company.com",
                "to": "bsmith@company.com",
                "name": "attachment-rewrite",
                "message_tid": "30d7a0b0-a2dd-11e8-b2b5-916b58752559",
                "reason": "test",
                "version": "2.0",
                "email_date": "2019-04-18T11:38:02+00:00",
                "sha256": "6f5aacaf01daecd95c04d0d43f20649bb7212ecbf304a71cdd6c32cdbd4bfb73",
                "subject": "Meeting Invite",
                "message_id": "4MB00601840C057.namprd94.prod.outlook.com",
                "mime_type": "application/pdf",
                "severity": "5"
             }
          }
       ],
       "pagingIdentifiers": {
          "safemail_2019-04-18T00:00:00.000Z_2019-04-19T21:21:09.060Z_2019-04-10T21:00:00.000Z": 2
       }
    }
}
```


Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2019-04-10T21:16:09.060Z
product	Product (Menlo Security Isolation Platform (MSIP))	MSIP

Response Parameter	Description	Example
rvlabs_factor	Malware risk factor	0
vendor	The product vendor name (Menlo Security)	Menlo Security
rewritten	Action performed on the URL present in the email	replaced
event_time	The access initiate date and time	2019-04-18T11:52:33.459Z
file_type	Attachment file type	PDF
bytes	Size of identified attachment (in bytes)	17036
name	Request type	attachment-rewrite
message_tid	Message transaction ID provided within all log messages pertaining to a given message	30d7a0b0-a2dd-11e8-b2b5-916b58752559
reason	Rationale behind the action performed	test
version	The Menlo Security product version (currently fixed at 2.0)	2.0
email_date	Email date	2019-04-18T11:38:02+00:00
sha256	The SHA256 hash of this file or document. This provides a cryptographically unique identifier.	c2a995de626356f701b6c7f549a3f4
message_id	Email identifier	4MB00601840C057.namprd94.prod.outlook.c

Response Parameter	Description	Example
mime_type	Attachment MIME type	application/pdf
severity	The severity level for the session. This is currently fixed at 5.	5
delivered_to	Recipient email address	bsmith@gmail.com
filename	Attachment filename	invite.ics
from	Email address in email From: line	jdoe@company.com
reply_to	Sender email address	jdoe@company.com
sender	Email sender address information	Google <calendar notification@google.com>
subject	Text in email Subject: line	Meeting Invite
to	Email address in email To: line	bsmith@gmail.com
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	safemail_2019-04-18T00:00:00.000Z_2019-0

SMTP Logs

Sample Response Details (JSON)

```
{
    "timestamp": "2018-04-10T21:16:09.060Z",
    "result": {
       "metrics": [
          "last_access",
          "total_links",
          "time_handoff_up",
          "original_bytes",
          "time_handoff_down",
          "rewritten_links",
          "rewrite_time_taken",
          "rows",
          "time_taken"
       ],
       "events": [
          {
             "event": {
                "severity": "5"
                "smtp_reply": "250",
                "time_handoff_down": 1.5959999561309814,
                "total_links": 3,
                "rows": 1,
                "from": "NA",
                "next_hop_reason": "250 2.6.0
<CACiMZ7P4LGPwwqbpYUiit9VW=HT30vhJorgmq_4g1Uw5b3+dKQ@mail.gmail.com> [InternalId=115680649151408,
Hostname=BY1PR10MB0358.namprd10.prod.outlook.com] 22156 bytes in 0.309, 69.903 KB/sec Queued mail
for delivery",
                "event_time": "2018-04-10T21:19:49",
                "src_tls": "true",
                "hostname": "safemail.menlosecurity.com",
                "src_ip": "216.32.181.23",
                "to": "NA",
                "version": "2.0",
                "message_id": "CACiMZ7P4LGPwwqbp+dKQ@mail.gmail.com",
                "product": "MSIP",
                "vendor": "Menlo Security",
                "timestamp": "2018-04-10T21:19:49.000Z",
                "src_port": "16928",
                "reason": "NA",
                "dst_tls": "true",
                "rewritten_links": 3,
                "time_taken": 2.6410000324249268,
                "rewrite_success": "true",
                "time_handoff_up": 0.2930000126361847,
                "name": "upstream-accept",
                "message_tid": "e52a2c70-3d04-11e8-8a0b-918c2380e1d4",
                "region": "us-east-1a",
                "unix_time": "1523395189",
                "unix_time_iso": "2018-04-10T21:19:49",
                "mode": "transform",
                "dst_ip": "207.46.163.10",
                "dst_from_port": "58145"
             }
          }
       ],
       "pagingIdentifiers": {

"smtp_request_2018-04-10T21:14:51.630Z_2018-04-10T21:19:51.630Z_2018-04-10T21:00:00.000Z": 0
       }
    }
}
```

Response Parameters

Response Parameter	Description	Example
timestamp	Start time of the requesting log. This is internal to the log database.	2018-04-10T21:16:09.060Z
severity	The severity level for the session. This is currently fixed at 5.	5
smtp_reply	The SMTP reply code propagated to upstream; downstream code	250
time_handoff_down	Time spent writing to downstream in seconds	1.5959999561309814
total_links	Number of links in the email	3
rows	Number of rows with the same values	1
from	Envelope sender (MAIL FROM)	NA
next_hop_reason	Downstream response reason (e.g., *550 foo bar** or *NA* if it never got to downstream)	250 2.6.0 <CACiMZ7P4LGPwwqbpYUiit9VW=HT3 [InternalId=115680649151408, Hostname=BY1PR 22156 bytes in 0.309, 69.903 KB/sec Queued mail

Response Parameter	Description	Example
event_time	The access initiate date and time	2018-04-10T21:19:49
src_tls	Whether transport layer security was used talking to the source MTA	true
hostname	Email processor hostname	safemail.menlosecurity.com
src_ip	Source IP address	216.32.181.23
to	Envelope recipients	NA
version	The Menlo Security product version (currently fixed at 2.0)	2.0
message_id	Unique ID for this email	CACiMZ7P4LGPwwqbp+dKQ@mail.gmail.com
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
vendor	The product vendor name (Menlo Security)	Menlo Security
timestamp	Start time of the event	2018-04-10T21:19:49.000Z
src_port	Source port	16928

Response Parameter	Description	Example
reason	Internal error reason; *NA* used if the reason is downstream	NA
dst_tls	Whether transport layer security was used talking to the destination MTA	true
rewritten_links	Number of links rewritten	3
time_taken	Total time spent in seconds processing email	2.6410000324249268
rewrite_success	Whether rewriting was successful or not, or blank if not applicable	true
time_handoff_up	Time spent reading from upstream in seconds, e.g. 1.234, or null if not applicable	0.2930000126361847
name	Result of processing	upstream-accept

Response Parameter	Description	Example
message_tid	A unique transaction id for this attempt to process the email, the same message id may occur with multiple transaction ids if it is retried	e52a2c70-3d04-11e8-8a0b-918c2380e1d4
region	AWS region and availability zone	us-east-1a
unix_time	Unix time epoch	1523395189
unix_time_iso	Unix time stamp	2018-04-10T21:19:49
mode	Whether the processing was to transform or restore the email	transform
dst_ip	Destination IP address	207.46.163.10

Response Parameter	Description	Example
dst_from_port	When connection is established with downstream MTA, MTA's port is fixed, but local port requires indicating - useful for diagnosing issues based on connection, which is identified by tuple (local IP, local port, remote IP, remote port).	58145
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	safemail_2018-04-10T21:16:09.060Z_2018-04-1C

iSOC Logs

Sample Response Details (JSON)

```
{
                    "event": {
                        "alert_type": "isoc",
                        "browser_and_version": "Chrome_83",
                        "policy_applied": "allow",
                        "recommended_action": "investigate",
                        "click_time_verdict": "Malware Sites",
                        "target_domain": "ianfette.org",
                        "click_time_timestamp": "2020-06-02T01:20:56.446Z",
                        "origin_ip": "173.201.140.128",
                        "file_size": "NA",
                        "browser_type": "supported_browser",
                        "severity": "high",
                        "event_time": "2020-06-02T01:21:09.097762",
                        "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36",
                        "version": "2.0",
                        "product": "MSIP",
                        "vendor": "Menlo Security",
                        "alert_sub_type": "isoc_access_malicious_site",
                        "dest_ips": "173.201.140.128",
                        "url": "http://ianfette.org/",
                        "alert_name": "Malicious Site Access",
                        "document_download_type": "false",
                        "http_method": "GET",
                        "resource_category": "page_request",
                        "alert_source": "web",
                        "browser": "Chrome"
                    }
}
```


Response Parameters

Response Parameter	Description	Example
alert_type	Type of alert (iSOC)	isoc
browser_and_version	Browser and major version	IE_11
policy_applied	Policy applied to the request	block

Response Parameter	Description	Example
recommended_action	Recommended action that the customer needs to take for this alert (*none*: alert was either blocked or isolated and no action is required by SoC admin; *investigate*: alert requires SoC to investigate to ensure no improper actions taken by user; *immediate*: alert requires immediate attention by SoC admin)	none
click_time_verdict	Click time categorization	Phishing and Other Frauds
target_domain	Domain as logged	dangeroussite.com
click_time_timestamp	Timestamp recorded at time of click	2020-01-03T13:16:50.214Z
origin_ip	Actual IP address of the destination server	130.65.255.101
file_size	Size of the file in bytes when a malicious file is downloaded	1024
browser_type	Whether the browser request was made from a supported browser	supported_browser
severity	Defines how critical the alert is	high
event_time	The access initiate date and time	2020-06-02T01:21:09.097762

Response Parameter	Description	Example
user-agent	User agent string from the http header	Mozilla/5.0 (Windows NT 10.0; WOW6 Gecko) Chrome/79.0.3945.88 Safari/53
version	The Menlo Security product version (currently fixed at 2.0)	2.0
product	The Menlo Security Product (MSIP or Menlo Security Isolation Platform)	MSIP
vendor	The product vendor name (Menlo Security)	Menlo Security
alert_sub_type	Specific subtype of the alert	isoc_submission_phishing_content
dest_ips	Destination IPs of the malicious request	4.4.4.4
url	Request URL	https://dangeroussite.com
alert_name	Name of the alert	Phishing Site Content Submission
document_download_type	Defines the kind of document that was downloaded (safe/original)	original
http_method	HTTP method	POST
resource_category	Indicates the type of request (i.e. page request/download /etc.)	form_post
alert_source	Email/Web	web
browser	Browser making the web request	Chrome
file_type	Libmagic result of the file type that was downloaded	PDF

Response Parameter	Description	Example
filename	Filename of the downloaded file	LmsCertificate.pdf
password_input	If a web request had a password submitted	false
file_hash	SHA256 of the file download	3c4e2ea86477064daf1c4d3d66bf1289
email_risk_score	Email risk score	low
http_response	HTTP response status	200
malware_family_name	Malware family name from the hash lookup result or manual labelling	Win32.Trojan.Browsefox
isoc_verdict	Menlo Security's verdict of the web request	Phising and Other Frauds
av_scan	Hash lookup/av scan result	Infected

Example Logging Script

Log into the Menlo Security Support Portal and access the following article:

- **API** Python Script

Note

The **API** Perl script is no longer supported or maintained.