Table of Contents

SIEM Event Delivery APIs

Last Modified on 06/22/2020 9:32 pm PDT

API endpoints available for use with the SIEM Event Delivery Service. SIEM (Security Information and Event Management) is a recognized standard for collecting, aggregating, and analyzing events within an IT organization.

Endpoint	Methods
/eventdelivery/activate Add an Identity Cloud application to the SIEM Event Delivery service.	• POST
/eventdelivery/deactivate Removes an application from the SIEM Event Delivery service.	• POST
/eventdelivery/readStatus View the activation/deactivation status for an application.	• GET
/eventdelivery/readKeys View the public keys associated with an application.	• GET
/eventdelivery/addKeys Add one or more public keys to an application.	• POST
/eventdelivery/deleteKeys Remove one or more public keys from an application.	• POST
/eventdelivery/readBlacklist View an application's SIEM Event Delivery Service event blacklist.	• GET
/eventdelivery/addBlacklist Add one or more events to an application's blacklist.	• POST

Endpoint	Methods
Endpoint /eventdelivery/deleteBlacklist	**Methods** ● POST

Remove one or more events from an application's blacklist.

/eventdelivery/activate

Last Modified on 06/12/2020 10:13 am PDT

POST

Description

Adds an Identity Cloud application to the SIEM Event Delivery service: you cannot collect SIEM events for an application until that application has been activated for event delivery. (Events will still be generated, of course, but those events will not be collected and made accessible to the organization associated with the application.) In addition to activating the application, you can also use this endpoint to assign a set of public keys (required to download event data). Alternatively, keys can be added later using the /addKeys endpoint.

Note that activation is not instantaneous: there are a series of back-end processes that must be completed before an application is fully activated and event delivery begins. You can use the /eventdelivery/readStatus endpoint to check the progress of the provisioning process for an application.

> **Important**. Before you can activate an application, your Akamai account number must be present in your application's global settings (with the setting name **akamai_account_id**). You can verify that this setting has been added to your application by using the Console or by calling the /{appId}/settings/options API endpoint. If you try to activate an application and the account number cannot be found, your API call will fail. In addition to that, and thanks to server caching, even if you immediately add the account number there will be a 10-minute period in which you cannot activate the application.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL Path Parameters

Parameter	Type	Required	Description

region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc
appID	string	Yes	Unique identifier of the Identity Cloud application being activated. For example: `htb8fuhxnf8e38jrzub3c7pfrr`

Request Parameters

Request parameters must be formatted as JSON objects and included in your API call's **body** parameter. Valid request parameters include the following:

Parameter	Type	Required	Description
keys	array (string)	No	JSON-formatted array of public keys that can be used to access the Amazon Web Services S3 bucket where SIEM data feeds are delivered; these public keys must be supplied by the Identity Cloud customer. Note that public keys are not required in order to activate an application; public keys can be added later by using the /eventdelivery/addKeys endpoint. However, at least one key must be configured before organizations can access their S3 bucket. For example: `["ssh-rsa DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6ty PEFEzV0LX3XGF55RMsQz1x2cEikKDEY0alj4 1qgxMCP/iteneqXSIFZBp5vizPvaoIR3Um9x K7PGoW8giupGn+EPuxlA4cDM4vzOqOkiMPh 5XK0whEjkVzTo4+S0puvDZuwIsdiW9mxhJc7 tgBNL0c2r3SYVkz4G/fsINfRPAABAAM49f4 htxPb5ok4Q2Lg9dPKVHO/Bgeu5woMc7RY0p`

			ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP Gt5Rq9t2ta6F6fmX0agvpFyNfRPFbXeUBr7o sSCJNgvavWbA4cDniWrOvYX2xwWdhXmX3ue6 8ZbabVoha3W1 karim.nafir@mail.com"]

Note that you do not need to include the parameter name (keys) in the body request. The parameter value (the public keys) is all that's needed.

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command activates SIEM Event Delivery for the application with the ID htb8fuhxnf8e38jrzub3c7pfrr. This command also specifies a single public key to be used when accessing the S3 bucket:

```
curl -X GET \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/activate \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqdXdzRhb3E=' \
  -H 'Content-Type: application/json' \
  -d '[
      "ssh-rsa DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6tyPEFEzV0LX3XGF55RMsQz1x2cEikKDEY0aI
j41qgxMCP/iteneqXSIFZBp5vizPvaoIR3Um9xK7PGoW8giupGn+EPuxIA4cDM4vzOqOkiMPhz5XK0whEjkVz
To4+S0puvDZuwIsdiW9mxhJc7tgBNL0c2r3SYVkz4G/fslNfRPAABAAM49f4fhtxPb5ok4Q2Lg9dPKVHO/Bge
u5woMc7RY0p1ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP7xGt5Rq9t2ta6F6fmX0agvpFyNfRPFbXeUBr7os
SCJNgvavWbA4cDniWrOvYX2xwWdhXmX3ue68ZbabVoha3W1 karim.nafir@mail.com"
    ]'
```

Responses

202 Accepted

If your call to this endpoint succeeds, you'll get back a response similar to this:

```
{
    "message": "Your request has been accepted and is being
    processed.",
    "sftp":
```

```
  {
      "uri": "sftp://user_karim.nafir@v1.api.us.janrain.com",

      "user": "user_ htb8fuhxnf8e38jrzub3c7pfrr ",

      "host": " v1.api.us.janrain.com"

  }
}
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
403	**Forbidden**. Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/deactivate

Last Modified on 04/28/2020 10:44 pm PDT

POST

Description

Deletes the SIEM Event Delivery service for the specified application. After you call this endpoint, event messages for the application will no longer be delivered by the SIEM Event Delivery service. In addition to that, the user account associated with the service will be deleted, and any messages stored in the SFTP server will no longer be accessible.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

> https://v1.api.**us**.janrain.com/config/applications/**htb8fuhxnf8e38jrzub3c7pfrr**

If you are in the Australian (AU) region your URL will look like this:

> https://v1.api.**au**.janrain.com/config/applications/**htb8fuhxnf8e38jrzub3c7pfrr**

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

| appID | string | Yes | Unique identifier of the Identity Cloud application being deactivated. For example: |
| | | | htb8fuhxnf8e38jrzub3c7pfrr |

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command deactivates SIEM Event Delivery for the Identity Cloud application with the ID htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X GET \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/deactivate \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqqdzRhb3E='
```

Responses

202 Accepted

If your call to this endpoint succeeds, you'll get back the following response:

```
{
    "message": "Your request has been accepted and is being
    processed."
}
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client

	name and/or an invalid client secret.
403	**Forbidden**. Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.

/eventdelivery/readStatus

Last Modified on 06/12/2020 10:13 am PDT

GET

Description

Returns the SIEM Event Delivery activation/deactivation status for the specified application. You can use this endpoint to determine whether or not an application has completed activation and is now capable of receiving SIEM event deliveries; you can also determine whether or not an application has been deactivated and is no longer capable of receiving SIEM event deliveries.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

appID	string	Yes	Unique identifier of the Identity Cloud application whose status is being checked. For example:
			htb8fuhxnf8e38jrzub3c7pfrr

Authentication

This endpoint requires Basic authentication and an API client with read permissions. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command verifies SIEM Event Delivery activation status for the Identity Cloud application with the ID htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X GET \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/readStatus \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhj12W
szYmZocnl2d2NmY2c3NTdqdzRhb3E='
```

Responses

200 OK

If your call to this endpoint succeeds, and if the activation process is complete, you'll get back status information similar to the following:

```
{
  "status": "creation complete"
}
```

Other possible status values for the activation/deactivation process include:

- creation queued
- creation in progress
- creation failed
- deletion queued
- deletion in progress
- deletion complete
- deletion failed

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'**. Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/readKeys

GET

Description

Returns information about the public keys associated with the specified application. Public keys are required in order to download the event messages delivered by the SIEM Event Delivery service. Each user that accesses the S3 bucket must supply a valid public key; note, however, that no application can be assigned more than 10 public keys.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the **US** region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc
appID	string	Yes	Unique identifier of the Identity Cloud application. For example:

			htb8fuhxnf8e38jrzub3c7pfrr

Authentication

This endpoint requires Basic authentication and an API client with read permissions. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command returns information about the public keys associated with the Identity Cloud application htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X GET \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/readKeys \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqdzRhb3E='
```

Responses

200 OK

If your call to this endpoint succeeds, you'll get back information about the SIEM Event Delivery public keys associated with the application:

```
[
 {
  "key": {
   "$ref": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDWKvQV0MoER+0mv+KGRDxY7b39yrEGo6qiQ0xPM8vhDp5JMjm9
4KFSVrx0qewp2AsCl3qamJcvaStyxBZTfhlFsEWt1BAtixki0WRj8iTDugtXhdu65lGYuxkLiGWUNZu5OTXSA/6usdtv
gS7WleeFWWl0jYwoU4cLGbafldSDfH77Ab1m6PbZGalw7rJLZkkY+yPan/0ONzlEfTJdBUZl4g+MfFvTcsCG5Jo3Ad
V/g08hL8/SFMhbtKFAlslAkmmcEP1Oj27AAj6EtoD8YqjJZtO6uDq7KApq2J/M499NKhHGnrPl23AqgaOBNDdJNgj5
YKyhNudUl1ap+qt gstemp@akamai.com"
  },
  "status": "creation complete",
  "created": "2019-08-05T18:01:30Z"
 }
]
```

16

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/addKeys

POST

Description

Adds one or more public keys to the specified application. Public keys are required in order to download the event messages delivered by the SIEM Event Delivery service. Note, however, that applications can only be assigned a maximum of 10 public keys: your API call will fail if you attempt to add more than 10 keys to an application. If you need to do, say, add 10 different keys to an application, you'll have to remove the 10 existing keys and *then* add the replacement keys.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

18

appID	string	Yes	Unique identifier of the Identity Cloud application where the public keys are being added. For example:
			htb8fuhxnf8e38jrzub3c7pfrr

Request Parameters

Request parameters must be formatted as JSON objects and included in your API call's **body** parameter. Valid request parameters include the following:

Parameter	Type	Required	Description
keys	array (string)	Yes	JSON array of the public keys to be added to the Identity Cloud application. For example:
			["ssh-rsa DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6ty PEFEzV0LX3XGF55RMsQz1x2cEikKDEY0alj4 1qgxMCP/iteneqXSIFZBp5vizPvaoIR3Um9x K7PGoW8giupGn+EPuxIA4cDM4vzOqOkiMPhz 5XK0whEjkVzTo4+S0puvDZuwlsdiW9mxhJc7 tgBNL0c2r3SYVkz4G/fslNfRPAABAAM49f4f htxPb5ok4Q2Lg9dPKVHO/Bgeu5woMc7RY0p1 ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP7x Gt5Rq9t2ta6F6fmX0agvpFyNfRPFbXeUBr7o sSCJNgvavWbA4cDniWrOvYX2xwWdhXmX3ue6 8ZbabVoha3W1 karim.nafir@mail.com"]

Note that you do not need to include the parameter name (**keys**) in the body request. The parameter value (the public keys) is all that's needed.

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command adds a single public key to the application with the ID htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X POST \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/addKeys \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqdzRhb3E=' \
  -H 'Content-Type: application/json' \
  -d '{
  ["ssh-rsa
DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6tyPEFEzV0LX3XGF55RMsQz1x2cEikKDEY0aIj41qgxMCP/itene
qXSIFZBp5vizPvaoIR3Um9x
K7PGoW8giupGn+EPuxIA4cDM4vzOqOkiMPhz5XK0whEjkVzTo4+S0puvDZuwIsdiW9mxhJc7tgBNL0c2r3SYV
kz4G/fslNfRPAABAAM49f4f
htxPb5ok4Q2Lg9dPKVHO/Bgeu5woMc7RY0p1ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP7xGt5Rq9t2ta6F6
fmX0agvpFyNfRPFbXeUBr7o
sSCJNgvavWbA4cDniWrOvYX2xwWdhXmX3ue68ZbabVoha3W1 karim.nafir@mail.com"]
}'
```

Responses

201 Created

If your call to this endpoint succeeds, you'll get back a response similar to this:

"The public key(s) were added successfully."

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
400	**The request payload is not valid JSON.** Your API request did not pass the JSON schema validation. Verify that you are using correctly-formatted JSON in the request parameter and then try again. You will also receive this error if you attempt to add more than 10 keys to your S3 bucket.
401	**Not authorized. Your client credentials may be invalid.** You have specified an invalid client name and/or an invalid client secret.

403	**Forbidden**. Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/deleteKeys

Last Modified on 06/12/2020 10:12 am PDT

POST

Description

Removes one or more of the SIEM Event Delivery public keys associated with an application. Public keys are required in order to download the messages delivered by the SIEM Event Delivery service. However, because an application can only be assigned a maximum of 10 public keys, you might need to delete existing keys in order to make room for new keys (or to remove keys that might have been compromised). The /deleteKeys endpoint provides a way to delete public keys.

Note that, if you include keys in the array that are *not* associated with the application ID, those keys will simply be ignored.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the **US** region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au

			• sg
			• cc
appID	string	Yes	Unique identifier of the Identity Cloud application containing the public keys being removed. For example:
			htb8fuhxnf8e38jrzub3c7pfrr

Request Parameters

Request parameters must be formatted as JSON objects and included in your API call's **body** parameter. Valid request parameters include the following:

Parameter	Type	Required	Description
keys	array (string)	Yes	JSON array of the public keys to be removed from the application. For example:
			["ssh-rsa DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6ty PEFEzV0LX3XGF55RMsQz1x2cEikKDEY0alj4 1qgxMCP/iteneqXSIFZBp5vizPvaoIR3Um9x K7PGoW8giupGn+EPuxIA4cDM4vzOqOkiMPhz 5XK0whEjkVzTo4+S0puvDZuwlsdiW9mxhJc7 tgBNL0c2r3SYVkz4G/fslNfRPAABAAM49f4f htxPb5ok4Q2Lg9dPKVHO/Bgeu5woMc7RY0p1 ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP7x Gt5Rq9t2ta6F6fmX0agvpFyNfRPFbXeUBr7o sSCJNgvavWbA4cDniWrOvYX2xwWdhXmX3ue6 8ZbabVoha3W1 karim.nafir@mail.com"]

Note that you do not need to include the parameter name (keys) in the body request. The parameter value (the public keys) is all that's needed.

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command removes a single public key from the application **htb8fuhxnf8e38jrzub3c7pfrr**:

```
curl -X POST \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/deleteKeys \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqdzRhb3E=' \
  -H 'Content-Type: application/json' \
  -d '{
  ["ssh-rsa
DDDAB3NzaC1yc2EAACCDEQABAAABAPOUh6tyPEFEzV0LX3XGF55RMsQz1x2cEikKDEY0aIj41qgxMCP/itene
qXSIFZBp5vizPvaoIR3Um9xK7
PGoW8giupGn+EPuxIA4cDM4vzOqOkiMPhz5XK0whEjkVzTo4+S0puvDZuwIsdiW9mxhJc7tgBNL0c2r3SYVkz
4G/fslNfRPAABAAM49f4fhtxP
b5ok4Q2Lg9dPKVHO/Bgeu5woMc7RY0p1ej6D4CKFE6lymSDJpW0YHX/wqE9+cfNfRP7xGt5Rq9t2ta6F6fmX0
agvpFyNfRPFbXeUBr7osSCJNg
vavWbA4cDniWrOvYX2xwWdhXmX3ue68ZbabVoha3W1 karim.nafir@mail.com"]
  }'
```

Responses

200 OK

If your call to this endpoint succeeds, you'll get back a response similar to the following:

```
{
  "message": "The public key was successfully removed."
}
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
400	**The request payload is not valid JSON.** Your API request did not pass the JSON schema validation. Verify that you are using correctly-formatted JSON in the request parameter and then try again.

401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
403	**Forbidden**. Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/readBlacklist

Last Modified on 06/12/2020 10:12 am PDT

GET

Description

Returns a list of the SIEM Event Delivery event types that have been blacklisted for the specified application. If an event type has been blacklisted, event messages for that type will not be delivered by the event delivery service; however, all other event types (i.e., all the event types *not* on the blacklist) will be delivered. By default, blacklists are empty, meaning that applications receive event messages for all available event types.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL path parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

appID	string	Yes	Unique identifier of the Identity Cloud application whose blacklist is being returned. For example:
			htb8fuhxnf8e38jrzub3c7pfrr

Authentication

This endpoint requires Basic authentication and an API client with read permissions. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command returns the event type blacklist for the application **htb8fuhxnf8e38jrzub3c7pfrr**:

```
curl -X GET \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/readBlacklist \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqcdzRhb3E='
```

Responses

200 OK

If your call to this endpoint succeeds, you'll get back event blacklist information similar to this:

```
[
  {
    "eventType": "config_change",
    "created": "2019-08-05T23:55:04.622346Z"
  },
  {
    "eventType": "email_verification",
    "created": "2019-08-05T23:55:04.622346Z"
  }
]
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/addBlacklist

Last Modified on 06/12/2020 10:12 am PDT

POST

Description

Adds one or more events to an application's SIEM Event Delivery service blacklist. If an event type has been blacklisted, event messages for that type will not be delivered by the SIEM Event Delivery service; however, all other event types *will* be delivered. By default, blacklists are empty, meaning that applications receive event messages for all available event types.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

```
https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

If you are in the Australian (AU) region your URL will look like this:

```
https://v1.api.au.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr
```

URL path parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

appID	string	Yes	Unique identifier of the Identity Cloud application whose blacklist is being updated. For example:
			htb8fuhxnf8e38jrzub3c7pfrr

Request Parameters

Request parameters must be formatted as JSON objects and included in your API call's **body** parameter. Valid request parameters include the following:

Parameter	Type	Required	Description
blacklist	Array (string)	Yes	JSON array of the event types being added to the blacklist. For example:
			["config_change","email_verification"]

Note that you do not need to include the parameter name (**blacklist**) in the body request. The parameter value (the events to be blacklisted) is all that's needed.

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command adds a pair of event types – **config_change** and **email_verification** to the event type blacklist for the application htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X POST \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/addBlacklist \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjjeW
szYmZocnl2d2NmY2c3NTdqdzRhb3E=' \
  -H 'Content-Type: application/json'
  -d '[
       "config_change",
       "email_verification"
      ]'
```

Responses

201 Created

If your call to this endpoint succeeds, you'll get back the following response:

```
{
    "message": "The event type(s) were successfully added to the
    blacklist."
}
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
400	**The request payload is not valid JSON.** Your API request did not pass the JSON schema validation. Verify that you are using correctly-formatted JSON in the request parameter and then try again.
401	**Not authorized. Your client credentials may be invalid.** You have specified an invalid client name and/or an invalid client secret.
403	**Forbidden.** Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'.** Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.

/eventdelivery/deleteBlacklist

Last Modified on 06/12/2020 10:12 am PDT

POST

Description

Removes one or more events from an application's SIEM Event Delivery service blacklist. If an event type has been blacklisted, event messages for that type will not be delivered by the event delivery service; however, all other event types *will* be delivered. If you remove an event type from the blacklist then the SIEM Event Delivery service will resume delivering event messages for that event type.

Base URL

The base URL for this endpoint is your Identity Cloud Configuration API URL (including the appropriate region) followed by your application ID. For example, if you are in the US region and your application ID is **htb8fuhxnf8e38jrzub3c7pfrr** then your base URL will look like this:

> https://v1.api.**us**.janrain.com/config/applications/**htb8fuhxnf8e38jrzub3c7pfrr**

If you are in the Australian (AU) region your URL will look like this:

> https://v1.api.**au**.janrain.com/config/applications/**htb8fuhxnf8e38jrzub3c7pfrr**

URL Path Parameters

Parameter	Type	Required	Description
region	string	Yes	Identity Cloud geographic region that hosts the application. Allowed values are: • us • eu • au • sg • cc

appID	string	Yes	Unique identifier of the Identity Cloud application whose blacklist is being updated. For example:		
			htb8fuhxnf8e38jrzub3c7pfrr		

Request Parameters

Request parameters must be formatted as JSON objects and included in your API call's **body** parameter. Valid request parameters include the following:

Parameter	Type	Required	Description
blacklist	array (string)	Yes	JSON array of the event types being removed from the blacklist. For example:
			["config_change","email_verification"]

Note that you do not need to include the parameter name (**blacklist**) in the body request. The parameter value (the events being removed from the blacklist) is all that's needed.

Authentication

This endpoint requires Basic authentication and an API client with the **owner** feature. When configuring authentication, use your client ID as the username and your client secret as the password.

Sample Request (curl)

The following command removes a pair of event types – **config_change** and **email_verification** from the event type blacklist for the application htb8fuhxnf8e38jrzub3c7pfrr:

```
curl -X POST \
  https://v1.api.us.janrain.com/config/applications/htb8fuhxnf8e38jrzub3c7pfrr/eventd
elivery/deleteBlacklist \
  -H 'Authorization: Basic M2dmYmdycmE3dzI4MmhndHJ5cGZxeDlwemhxaGpnZDU6Y2dkY3A3bWhjeW
szYmZocnl2d2NmY2c3NTdqdzRhb3E=' \
  -H 'Content-Type: application/json' \
  -d '
        "config_change",
        "email_verification"
      ]'
```

Responses

200 OK

If your call to this endpoint succeeds, you'll get back the following response:

```
{
    "message": "The event type(s) were successfully removed from
    the blacklist."
}
```

Error Response Codes

The following table includes information about some of the other response codes that you might encounter when calling this endpoint.

Response Code	Description
400	**The request payload is not valid JSON**. Your API request did not pass the JSON schema validation. Verify that you are using correctly-formatted JSON in the request parameter and then try again.
401	**Not authorized. Your client credentials may be invalid**. You have specified an invalid client name and/or an invalid client secret.
403	**Forbidden**. Your credentials are valid for the application but not for this endpoint. For example, if you have read-only credentials those credentials can only be used with GET endpoints.
404	**The Akamai account ID was not found. Check your application settings for 'akamai_account_id'**. Your Akamai account ID must be listed in the application settings for the application specified in your API call. You can use the /{appId}/settings/options API endpoint or the Console to verify your application settings.