

# ىلع اهحالصإو ثدحلا قفد ءاطخأ فاشكتسأ ةصاخلا ةباحسلا

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملل تانوكملا](#)

[نيوكتلا](#)

[تاقببط ةجمرب ةهجاو حاتفم عاشنلا](#)

[ثدح قفدت عاشنلا](#)

[MacOS/Linux ليغش تلاماظن](#)

[زودنيو](#)

[ةباحتسا](#)

[ثادحألا تاقفدت ةمئاق](#)

[MacOS/Linux ليغش تلاماظن](#)

[زودنيو](#)

[ةباحتسا](#)

[ثادحألا تاقفدت فذح](#)

[MacOS/Linux ليغش تلاماظن](#)

[زودنيو](#)

[ةباحتسا](#)

[ةحصللا نم ققحتلا](#)

[اهحالصإو ءاطخألا فاشكتسا](#)

[AMQP ةمدخ صحف](#)

[ثدحلا قفدت يقلت مبل لاصتالا نم ققحتلا](#)

[راطت نالا ةمئاق ي ف ثادحألا نم ققحتلا](#)

[ةكبشلا رورم ةكرح فلم عيمجت](#)

[قلص تاذا تامولعم](#)

## ةمدقملا

ةباحسلا يف اهحالصإو ثادحألا تاقفدت ءاطخأ فاشكتسأ ةيفيك دنتسملل اذه فصري  
ةراضلا جماربللا نم ةمدقتملا ةيامحلل ةنمألا ةياهنلا ةطقنل ةصاخلا

## ةيساسألا تابلطتملا

تابلطتملا

عوضوملا نم ةفرعم تنأ يقلتني نأ ي صوي cisco:

- نة مآلة ة ياهن لة طقنب ة صاخلة ة باحس لة
- م الة سة API

## ة مدختس ملة تانوك ملة

ة للة ة ية دامل تانوك ملة او جم ار بلة تارادصل لة دن تسم لة اذ ه ف ة دراولة تامول عم لة دن تست

- Secure Endpoint Private Cloud رادصل لة 3.9.0
- cURL v7.87.0
- cURL رادصل لة 8.0.1

ة صاخ ة ية لم عم ة ئب ب ف ة دوجوم لة ة زه جأ لة ن م دن تست ملة اذ ه ف ة دراولة تامول عم لة ءاشن لة م ت ناك اذ (يضا رة فة). حوس م ن يوك ت ب دن تست ملة اذ ه ف ة مدختس ملة ة زه جأ لة ع ي م ج ت أد ب رمأ ية ل م ت ح م لة ر ية ثأ ل لة م ه ف ن م دكأ ف ، ل ي غ ش ت لة د ي ق ك ت ك ب ش

## ن يوك ت لة

تاق ي ب ط تة ج م ر ب ة ه ج او ح ا ت ف م ءاشن لة

ة صاخ لة ة باحس لة م ك ح تة د ح و ل لة لو خ د لة ل ي ج س ت 1. ة و ط خ ل لة

ل لة ل لة ق ت ن ا 2. ة و ط خ ل لة Accounts > API Credentials.

ل لة ق ن ا 3. ة و ط خ ل لة New API Credential.

ل لة ق ا ط ن ل لة Read & Write ق و ف ر ق ن ا و Application name ة ف ا ض ا 4. ة و ط خ ل لة

### New API Credential

Application name

Scope



Read-only



Read & Write



An API credential with read and write scope can make changes to your Secure Endpoint configuration that may cause significant problems with your endpoints.

Some of the input protections built into the console do not apply to the API.

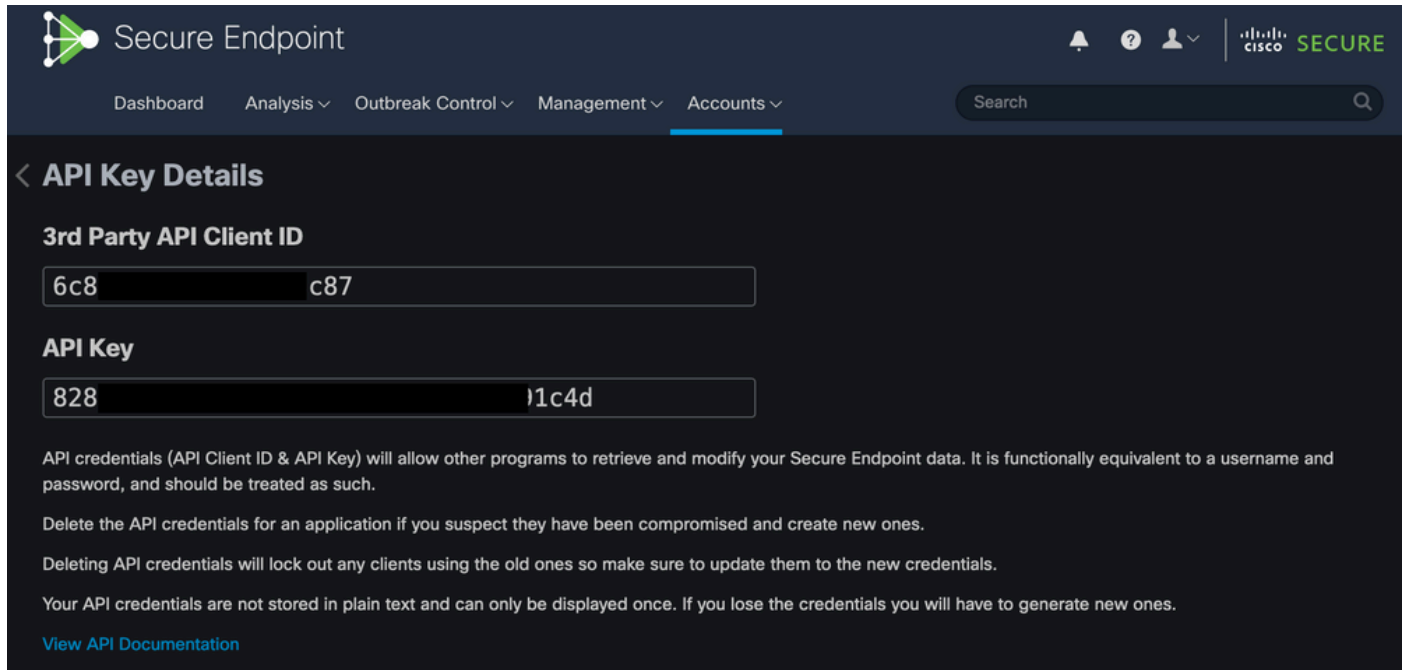
Cancel

Create

تأقېب طت ةج مر ب ةه ج ا و ح ا ت ف م ء ا ش ن ا

رقنا 5. ة و ط خ ل ا Create.

تأقېب طت ل ا ةج مر ب ةه ج ا و د ا م ت ع ا ت ا ن ا ي ب ظ ف ح 6. ة و ط خ ل ا



Secure Endpoint

Dashboard Analysis Outbreak Control Management Accounts

Search

### < API Key Details

**3rd Party API Client ID**

6c8c87

**API Key**

8281c4d

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Secure Endpoint data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

ح ا ت ف م API

ة ح ف ص ل ا ه ذ ه ك ر ت ب ت م ق ا ذ ا API ح ا ت ف م د ا د ر ت س ا ن ك م ي ال : ر ي ذ ح ت

ث د ح ق ف د ت ء ا ش ن ا

" ر ا ط ت ن ا ة م ئ ا ق ي ف ل ئ ا س ر ل ا ع ض و " ة م د خ ل و ك و ت و ر ب ل د ي د ج ل ئ ا س ر ق ف د ء ا ش ن ا ل ا ا ذ ه ي د و ي (AMQP) ث د ح ل ا ت ا م و ل ع م ل م د ق ت م ل ا

ة د د ح م ل ا ت ا ع و م ج م ل ا و ث ا د ح ا ل ا ع ا و ن ا ل " ث د ح ق ف د " ء ا ش ن ا ك ن ك م ي

```
--data '{"name":"EVENT_STREAM_NAME","event_type":["EVENT_TYPE_1", "EVENT_TYPE_2"],"group_guid":["GROUP_1"]}'
```

ة ط س ا و ب ت ا ع و م ج م ل ا ة ف ا ك و ث ا د ح ا ل ا ع ا و ن ا ة ف ا ك ل ث د ح ق ف د ء ا ش ن ا ك ن ك م ي

```
--data '{"name":"EVENT_STREAM_NAME","event_type":[],"group_guid":[]}'
```

ل ي غ ش ت ل ا م ا ط ن MacOS/Linux

مادختساب MacOS/Linux ىل ع ثادحأ قفدت عاشنإ كنكمي:

```
curl -X POST -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_KEY'
```

زودنيو

مادختساب Windows ىل ع ثدح قفد عاشنإ كنكمي:

```
curl -X POST -k -H "Accept: application/json" -H "Content-Type: application/json" -u "CLIENT_ID:API_KEY"
```

قباجتسا

```
HTTP/1.1 201 Created
```

```
(...)
```

```
"data": {  
  "id": 17,  
  "name": "EVENT_STREAM_NAME",  
  "amqp_credentials": {  
    "user_name": "17-1bfXXXXXXXXXX",  
    "queue_name": "event_stream_17",  
    "password": "3961XXXXXXXXXXXXXXXXXXXX814a77",  
    "host": "FMC_SERVICE_URL",  
    "port": 443,  
    "proto": "https"  
  }  
}
```

ثادحألا تاقفدت عمئاق

Private Cloud ىل ع اهؤاشنإ مت يتللا ثادحألا تاقفدتب عمئاق اذه ضرعي

MacOS/Linux ليغشتلا ماظن

مادختساب MacOS/Linux ليغشتلا ماظن ىل ع ثادحألا تاقفدت درس كنكمي:

```
curl -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_KEY' -i 'ht'
```

زودنيو

مادختساب Windows ىلع شادحأل تاقفدت كنكمي:

```
curl -k -H "Accept:application/json" -H "Content-Type:application/json" -u "CLIENT_ID:API_KEY" -i "http
```

ةباجتسا

```
HTTP/1.1 200 OK
```

```
(...)
```

```
"data": {  
  "id": 17,  
  "name": "EVENT_STREAM_NAME",  
  "amqp_credentials": {  
    "user_name": "17-1bfXXXXXXXXXX",  
    "queue_name": "event_stream_17",  
    "host": "FMC_SERVICE_URL",  
    "port": 443,  
    "proto": "https"  
  }  
}
```

شادحأل تاقفدت فذح

طشن شذح قفد فذح.

MacOS/Linux لىغشتلا ماطن

مادختساب MacOS/Linux ىلع شادحأل تاقفدت فذح كنكمي:

```
curl -X DELETE -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_K
```

زودنيو

مادختساب Windows ىلع شادحأل تاقفدت فذح كنكمي:

```
curl -X DELETE -k -H "Accept:application/json" -H "Content-Type:application/json" -u "CLIENT_ID:API_KEY
```

ةباجتسا

```
HTTP/1.1 200 OK
(...)
"data": {}
```

## ةحصلال نم ققحتلال

مساب هظفحاو كزاهج لى لى صننلا Python جم انرب خسنا 1. ةوطخلال EventStream.py.

```
import pika
import ssl

user_name = "USERNAME"
queue_name = "QUEUE_NAME"
password = "PASSWORD"
host = "FMC_SERVICE_URL"
port = 443
proto = "https"

def callback(channel, method, properties, body):
    print(body)

amqp_url = f"amqps://{user_name}:{password}@{host}:{port}"

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
amqp_ssl = pika.SSLOptions(context)

params = pika.URLParameters(amqp_url)
params.ssl_options = amqp_ssl

connection = pika.BlockingConnection(params)
channel = connection.channel()

channel.basic_consume(
    queue_name,
    callback,
    auto_ack = False
)

channel.start_consuming()
```

ةئيه لى عة فرفرطلال ةطحملال يف هذيفنتب مق 2. ةوطخلال python3 EventStream.py.

ثادخال قفدت راطتنا ةمئاق لى لى هتفاضل متت شذح ياً لىغشتب مق 3. ةوطخلال

ةفرفرطلال ةطحملال يف رهظت ثادخال تناك اذا امم ققحت 4. ةوطخلال

## اهحالصاوا ءاطخالال فاشكتسا

ةصخالال ةباحسلا لى لى SSH ربع لوخدلا لىجست كىل ع بچي، رم اوألال هذو ذيفنتل

## AMQP عمده صحت

عمده صحت نيكمت مت اذا ام قحت:

```
[root@fireamp rabbitmq]# ampctl service status rabbitmq
running enabled rabbitmq
```

عمده صحت ليعشت نم قحت:

```
[root@fireamp ~]# svstat /service/rabbitmq
/service/rabbitmq: up (pid 25504) 7402137 seconds
```

ثحت قفت يقلت بم لاصتال نم قحت:

رمال ذيفنت:

```
tail /data/log/rabbitmq/rabbit@fireamp.log
```

لاصتال سيسات مت:

```
=INFO REPORT===== 19-Apr-2023::08:40:12 ===
accepting AMQP connection <0.17588.27> (127.0.0.1:32946 -> 127.0.0.1:5672)
```

لاصتال قالغ مت:

```
=WARNING REPORT===== 19-Apr-2023::08:41:52 ===
closing AMQP connection <0.17588.27> (127.0.0.1:32946 -> 127.0.0.1:5672):
connection_closed_abruptly
```

راظتنال عمئاق ي ف ثا حأل نم قحت:

ملتسمال الى اذه ثحت قفت لاسرالل عهه راظتنال عمئاق ي ف ءوومال ثا حأل نوك  
23. ثحت قفت فرعمل اءح 14 كانه، لائل اذه ي ف. لاصتال سيسات ءب

<#root>

```
[root@fireamp rabbitmq]# rabbitmqctl list_queues
Listing queues ...
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_60b15rn8mpftaico6or6l8zxav11usm 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_61984nlu8p11eeopmgmtcjr1v8gf5p 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_iesRAGVo0h287m0_Det0x9PdDu8MxkS6kL4oSTeBm9s 26
event_decoration 0
event_log_store 0

event_stream_23 14

event_streams_api 0
events_delayed 0
events_retry 0
mongo_event_consumer 0
out_events_q1 0
tevent_listener 0
```

## ةك بشل رورم ة كرح فلم عي مجت

طاقت لال عي مجت كنكمي، ةصاخلا ةباحسلا نم ثادحألا قفدت رورم ة كرح نم ققحتل لب  
ةادألا tcpdump مادختساب:

ةصاخلا ةباحسلا ل SSH 1. ةوطخلا.

رمألا ذيفنت 2. ةوطخلا:

```
tcpdump -vvv -i eth1 host <Event_Stream_Receiver_IP> -w file.pcap
```

ةوطخلا 3. مادختساب طاقتل لال فاق ي 3. ةوطخلا Command-C (MAC) وأ Ctrl+C (Windows ي).

ةصاخلا ةباحسلا نم فلم pcap جارختسا 4. ةوطخلا.

## ةلص تاذا ممول عم

- [في اهنلا طاقن ثدح قفدت ةزيملا AMP نيوكت](#)
- [تادنت سمل او ينقتل ل مع دلا - Cisco Systems](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه  
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل