

# لصوم تيبثت ةلازا قرطءاطخأ فاشكتسأ اهحالصإو ةنمآلا ةياهنلا ةطقن

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[تیبثتلا ةلازا قرط](#)

[ايودي تيبثتلا ةلازا](#)

[ةنمآلا ةياهنلا ةطقن مكحت ةدحو نم لصوملا تيبثت ةلازا](#)

[تاقیبتلا ةجمرب تاهج او ماڤتساب لصوملا تيبثت ةلازا](#)

[رماوالا رطس تالوجم ماڤتساب لصوملا تيبثت ةلازا](#)

[ةلص تاڤتامولعم](#)

## ةمدقملا

يلع تبثملا Cisco Secure Endpoint (CSE) لصوم تيبثت ةلازا ةيلمع دننتمسما اذه فصی ةةفلتخم قرطب Windows ةزهجأ.

## ةيساسألا تابلطتملا

### تابلطتملا

ةیلالاتل عیضاوملاب ةفرعم كیل دل نوكت نأ Cisco یصوت:

- Secure Endpoint Connector
- ةنمآلا ةياهنلا ةطقن یف مكحتلا ةدحو
- ةنمآلا ةياهنلا ةطقنل (API) تاقیبتلا ةجمرب تاهج او

### ةمدختسملا تانوكملا

ةیلالاتل ةیدامل تانوكملا وجماربل تارادصل ىل دننتمسما اذه یف ةدراول تامولعملا دننست:

- Secure Endpoint Console، رادصل 5.4.2024042415
- Secure Endpoint Windows Connector رادصل v8.2.3.30119
- Secure Endpoint API v3

ةصاخ ةيلمعم ةئیب یف ةدوجوملا ةزهجألا نم دننتمسما اذه یف ةدراول تامولعملا عاشنإ مت تناك اذإ. (یضارتفا) حوسمم نیوكتب دننتمسما اذه یف ةمدختسملا ةزهجألا عیمج تأدب رمأ یال لمتمحمل ریثاتلل كمهف نم دكأتف، لیغشتلا دیق كتكبش.

## ةيساساً تامولعم

ةلازا ىلإ اهيف عطلتت يتل تالاحل ايف اديفم دننسم ل اذه يف حضوم ل اارجإل نوكي  
ةنمآل اةياهنل ةطقن لصوم تيبثت

ةديجل تاتيبتلل ءاوس ،لمكلا ب لصوم ل نم صلختلل ارايخ لصوم ل تيبثت ةلازا دع  
نآل دع ب Windows زاهج ىلع لصوم ل دوجوم دع ةطاسبب وأ

## تيتبتل ةلازا قرط

ماظن ب لمعي رتويبمك ىلع ةنمآل اةياهنل ةطقن لصوم تيبثت ةلازا يف بغرت نأ درجم ب  
لصفأ لكشب كتاجايحتح بسانت يتل ةقيرطال عبتا Windows ليغشتل

## ايودي تيبثت ةلازا

اي لحم لصوم تيبثت ةلازال

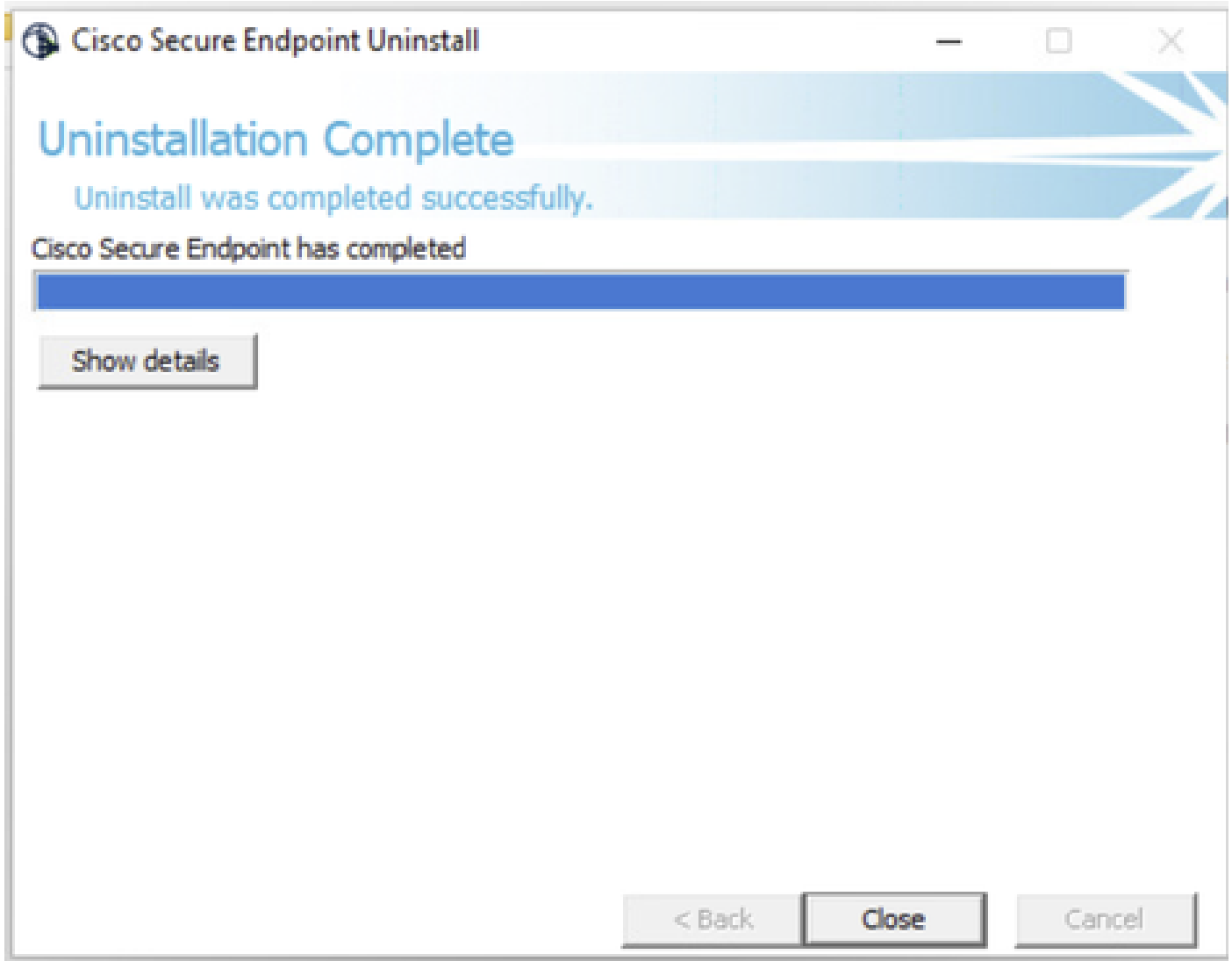
لصوم رادصا وه X ثيخ) Cisco > AMP > X > جماربل تافل م ىلإ لقتنا ،زاهج ل يف 1. ةوطخل  
CSE).

ةروصل ايف حضوم وه امك .uninstall.exe فلم عقوم ددح 2. ةوطخل

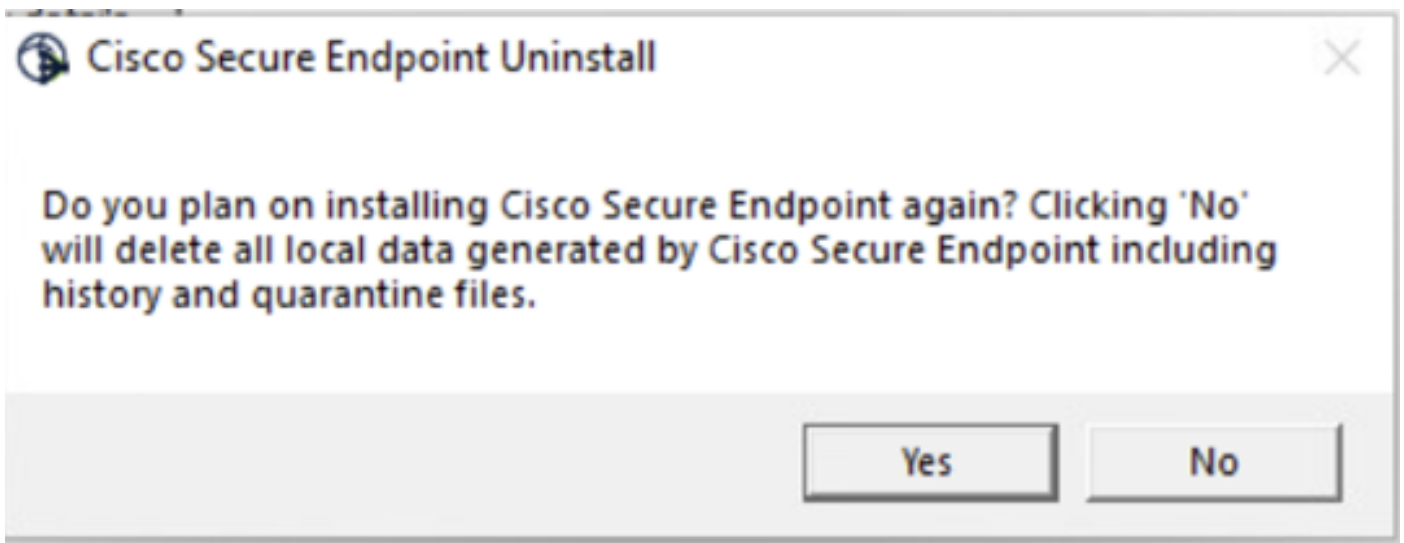
This PC > Windows (C:) > Program Files > Cisco > AMP > 8.2.3.30119

Name	Date modified	Type	Size
hs.dll	2/20/2024 2:54 PM	Application exten...	3,837 KB
ipsupporttool.exe	2/20/2024 2:54 PM	Application	693 KB
libcrypto-1_1-x64.dll	2/20/2024 2:54 PM	Application exten...	3,357 KB
libssl-1_1-x64.dll	2/20/2024 2:54 PM	Application exten...	678 KB
mfc140u.dll	2/20/2024 2:54 PM	Application exten...	5,527 KB
msvcp140.dll	2/20/2024 2:54 PM	Application exten...	567 KB
msvcp140_1.dll	2/20/2024 2:54 PM	Application exten...	35 KB
msvcp140_2.dll	2/20/2024 2:54 PM	Application exten...	193 KB
pthreadVC2.dll	2/20/2024 2:54 PM	Application exten...	115 KB
SecureClientUI.msi	2/20/2024 2:53 PM	Windows Installer ...	4,836 KB
SecurityProductInformation.ini	2/20/2024 2:54 PM	Configuration sett...	1 KB
sfc.exe	2/20/2024 2:54 PM	Application	9,297 KB
sfc.exe.log	4/27/2024 2:28 PM	Text Document	5,533 KB
sfc.exe_1.log	4/24/2024 3:05 PM	Text Document	51,200 KB
sfc.exe_2.log	4/21/2024 11:50 PM	Text Document	51,200 KB
sfc.exe_3.log	4/17/2024 6:12 PM	Text Document	51,200 KB
sfc.exe_4.log	4/6/2024 8:28 PM	Text Document	51,200 KB
sfc.exe_5.log	3/26/2024 1:20 PM	Text Document	51,200 KB
sfc.exe_6.log	3/7/2024 11:03 AM	Text Document	51,200 KB
spd.dat	2/20/2024 2:54 PM	DAT File	9 KB
ucrtbase.dll	2/20/2024 2:54 PM	Application exten...	1,098 KB
uninstall.exe	2/20/2024 2:54 PM	Application	34,624 KB
updater.exe	2/20/2024 2:54 PM	Application	1,708 KB
vcruntime140.dll	2/20/2024 2:54 PM	Application exten...	107 KB
vcruntime140_1.dll	2/20/2024 2:54 PM	Application exten...	49 KB
windows.phsd	2/20/2024 2:55 PM	PHSD File	8,161 KB
zlib.dll	2/20/2024 2:54 PM	Application exten...	98 KB

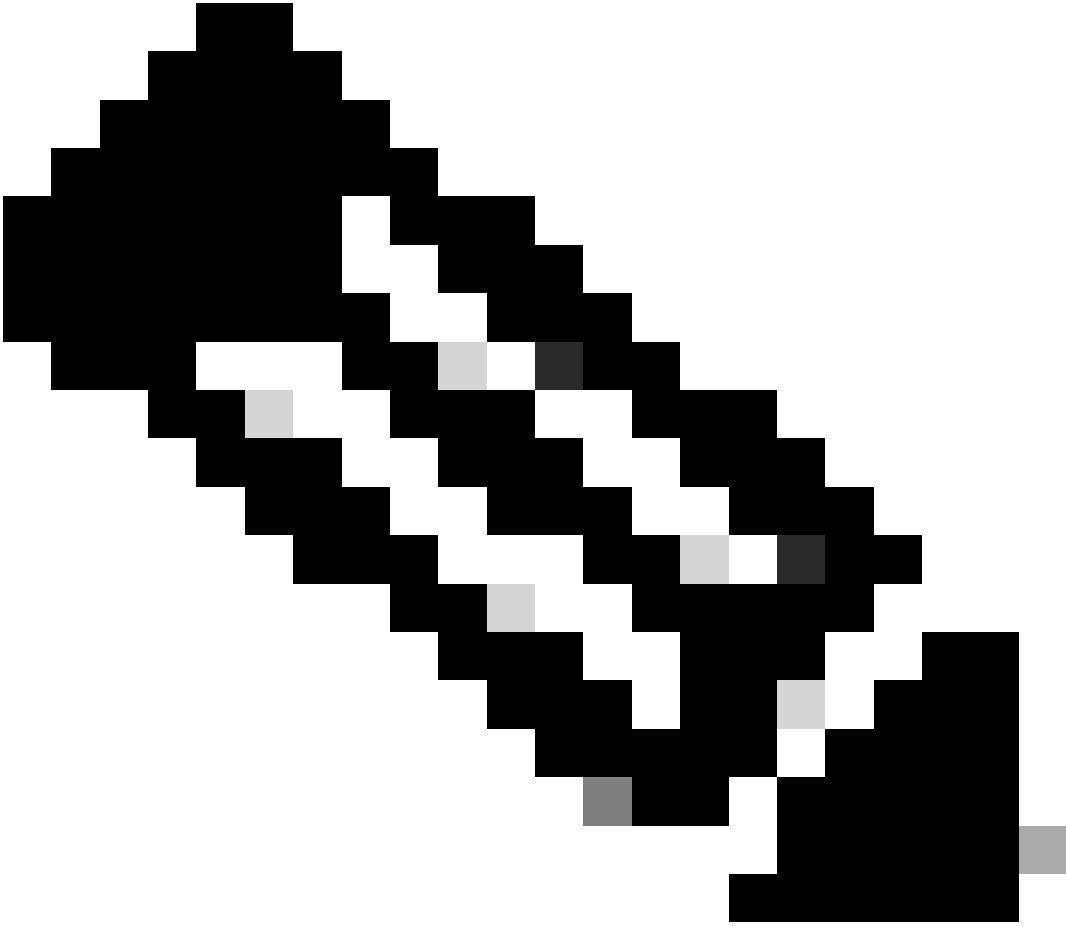
ةلازا لامتك" ةشاش ىلا لصت ىتح جلاعمرل عبتاو فلملا ذىفنتب مق 3 ةوطخلا ةروصلال ىف حضوم وه امك . "تتبتلل



يلا تال راوخل ع برم ىل ع لصحتس ، تي بثت الة لازا ة يلم ع نم ءاهت الال دعب 4. ة وطلال  
ي ف حضوم وه امك .؟ ىرخ أ ةرم Cisco نم ة نم آل الة طقن تي بثت ل ططخت له " الئاس تم  
ة. ة روص ال



---



ليغشت ةداع| مزلي، "تېبثتلا ةلازا" راوحلا ع برم ي ف ال ديحت ةلاح ي ف: ةطحال م  
ةيقبتم ال CSE تادلجم ي ا نم امامت صلختلل زاهجلل ةلمك

---

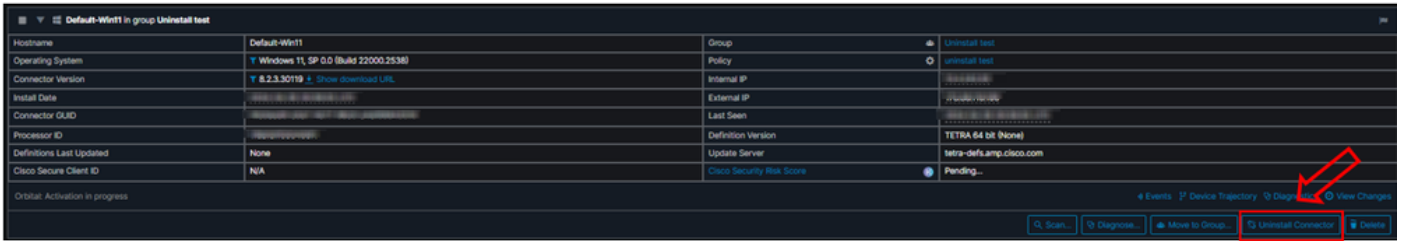
ةنم آلا ةياهنلا ةطقن مكحت ةدحو نم ل صوملا تېبثت ةلازا

مادختساب كلذب م ايقل كنكم ي ف، مكحتلا ةدحو نم دع بنع تېبثتلا ةلازا يلى ةجاحب تنك اذا  
ل صوملا تېبثت ةلازا رزلا

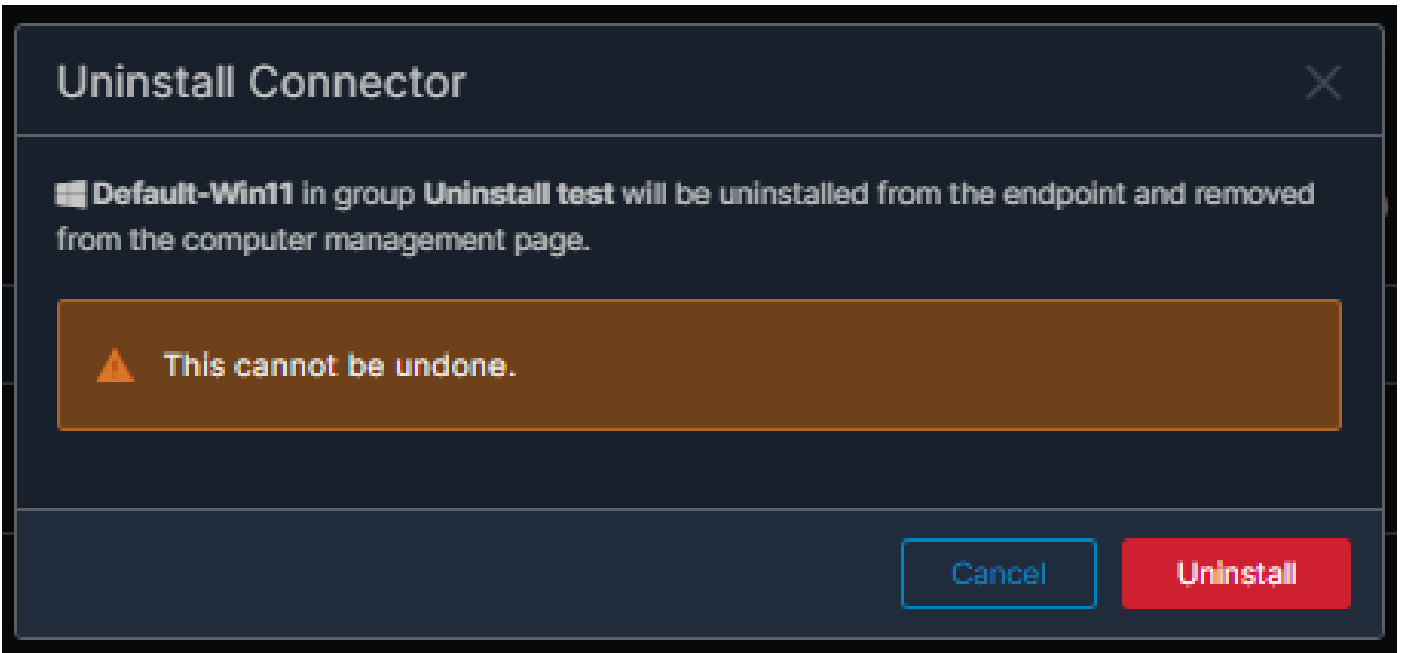
رتويبمكلا ةزهجأ > ةرادإلا يلى لقتنا، مكحتلا ةدحو ي ف 1. ةوطخلا

ليصافتلا ضرعل رقنا م ث، ةتېبثت ةلازا ديرت يذلا رتويبمكلا ع قوم دح 2. ةوطخلا

ةروصلال ي ف حضورم وه امك. ل صوملا تېبثت ةلازا رزىل ع رقنا 3. ةوطخلا



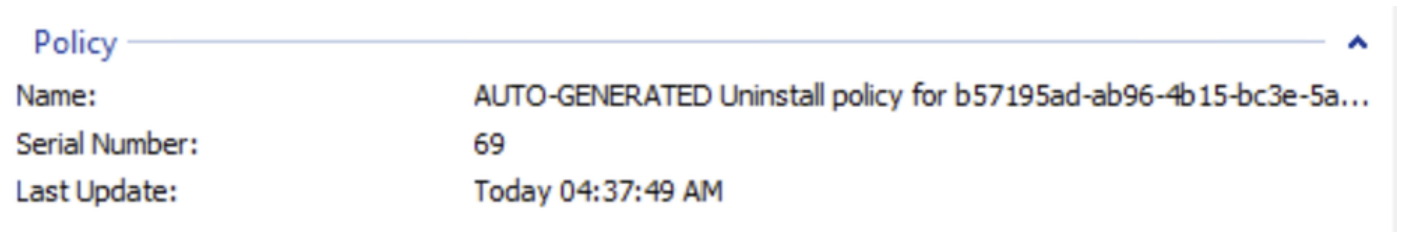
في حضوره وه امك .عارج ال تي ب ث ت كنم بل طي ام دنع تي ب ث الت الازا قوف رونا 4. ة و ط خ ال ل ة روص ال .

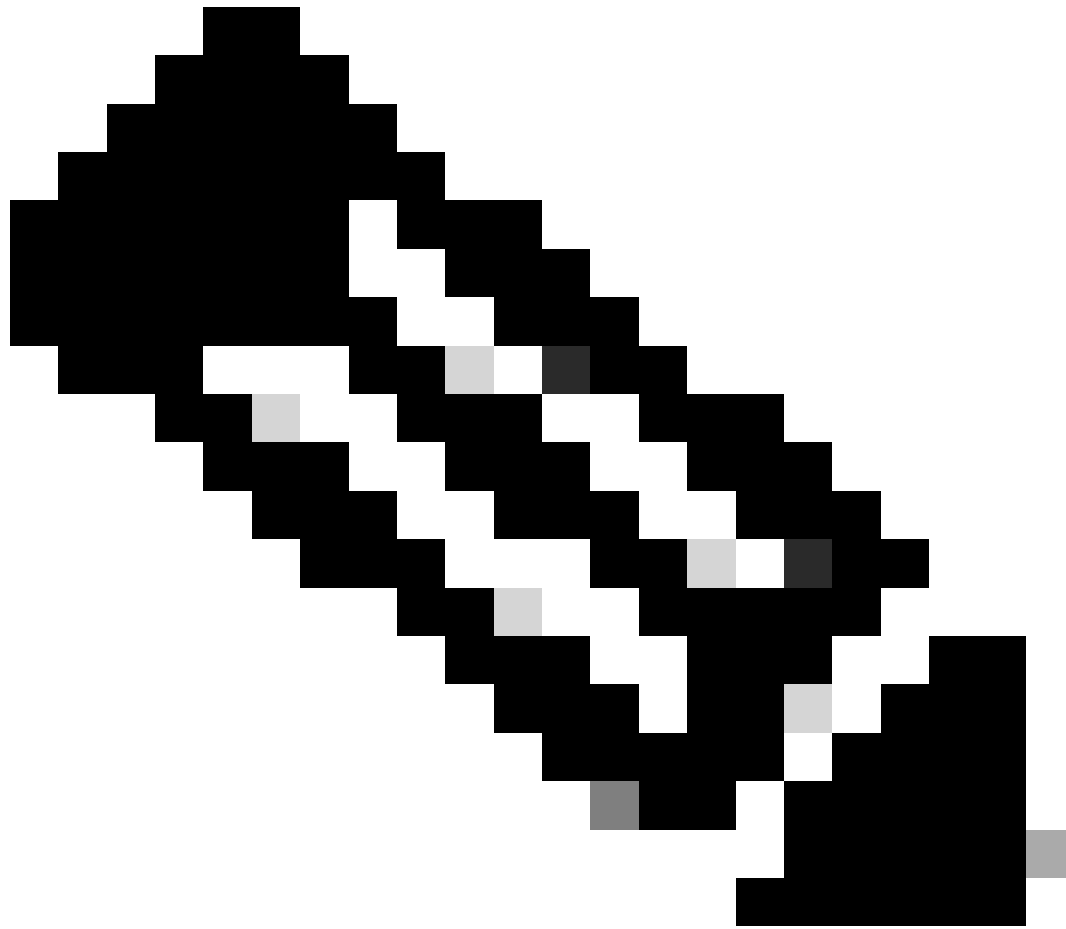


ة ياهن ال ة طقن مكحت ة د ح ونم ي ولع ال ع ز ج ال ي ف دي ك أ ت ة ل اسر ر ي ق ل ت ت فوس 5. ة و ط خ ال ل ة روص ال ي ف حضوره وه امك . ة ن م أ ال .



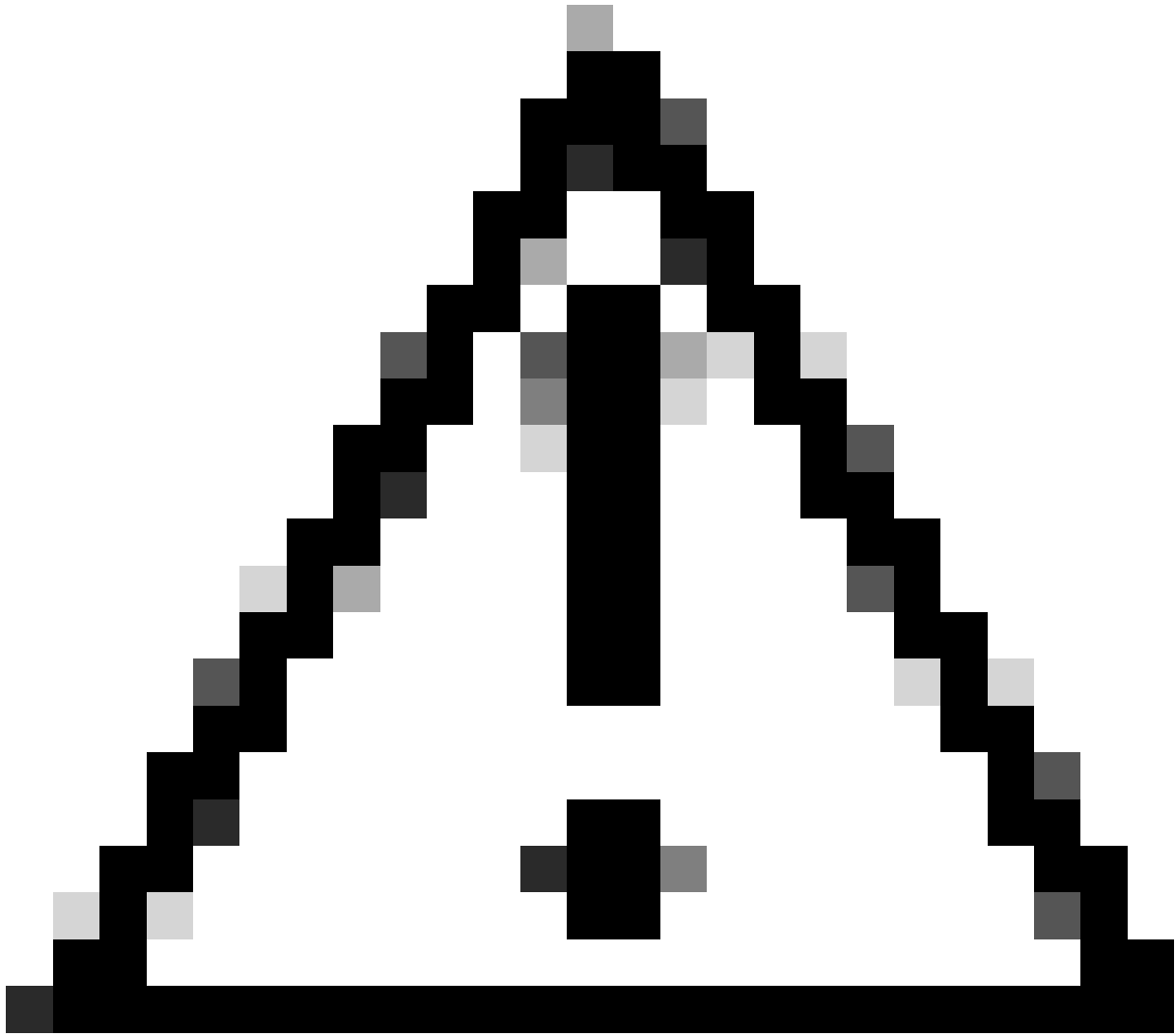
اي ل حم ت ام ولع ال ع ع ج ارم دع ب . روف ال ال ع مكحت ال ة د ح و ي ف ل صوم ال ل ي ف ت خ ي س ، امك ال اب ه ت ل ا ز ا م ت ت س ، ق ئ ا ق د ع ض ب دع ب و تي ب ث الت الازا ح ه ن ال ا ق و م ل صوم ال ل ق ت ن ي س . ة روص ال ي ف حضوره وه امك . زاه ج ل نم





دق ةمهمل هذه ذي فنن تل لصوملا اهم دختسي يتلا ةي نم زلا ةرت فل نأ ركذت :ةظحالم  
كب ةصاخلا ةئيبل بسح فل تخت

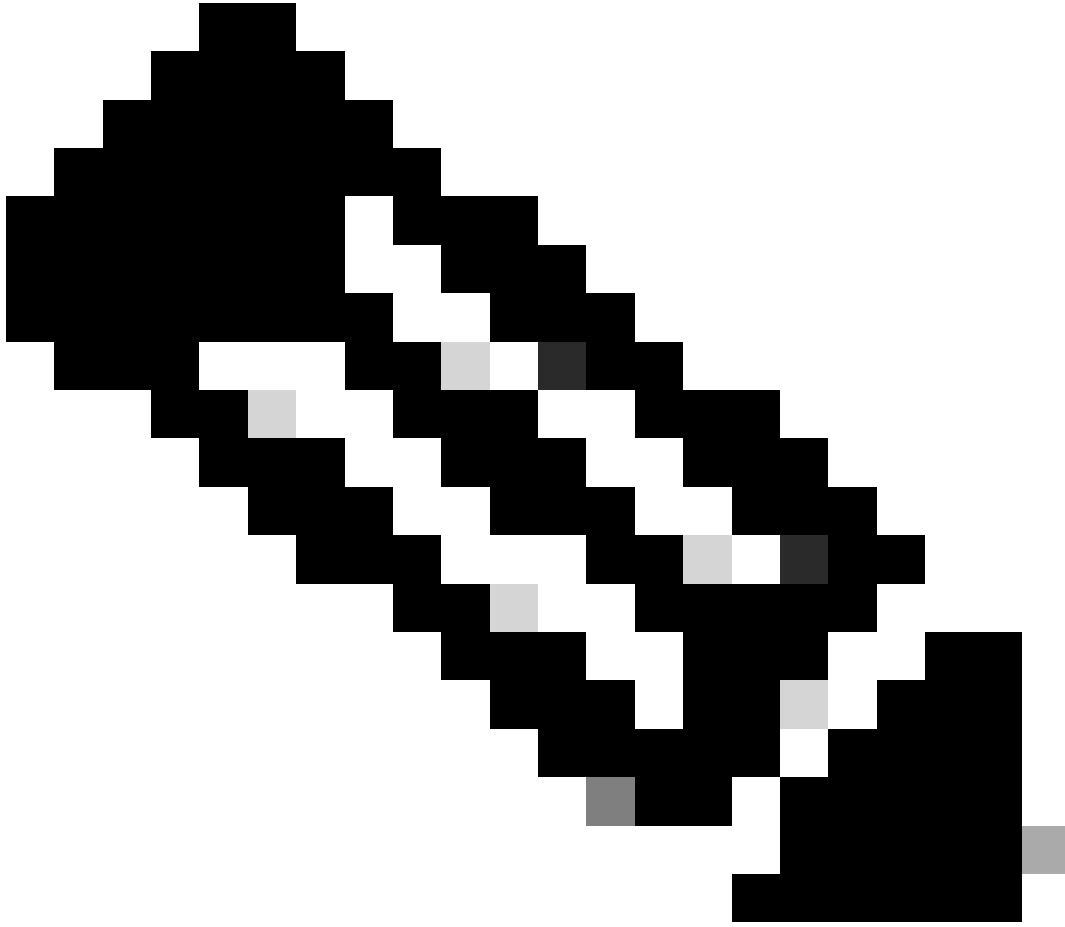
---



ةيلمعلا لاوطالصتم لظي تيبتثتلا ةلازا لبقتسي يذلا زاهجلا نا نم دكأت :ريذحت

---



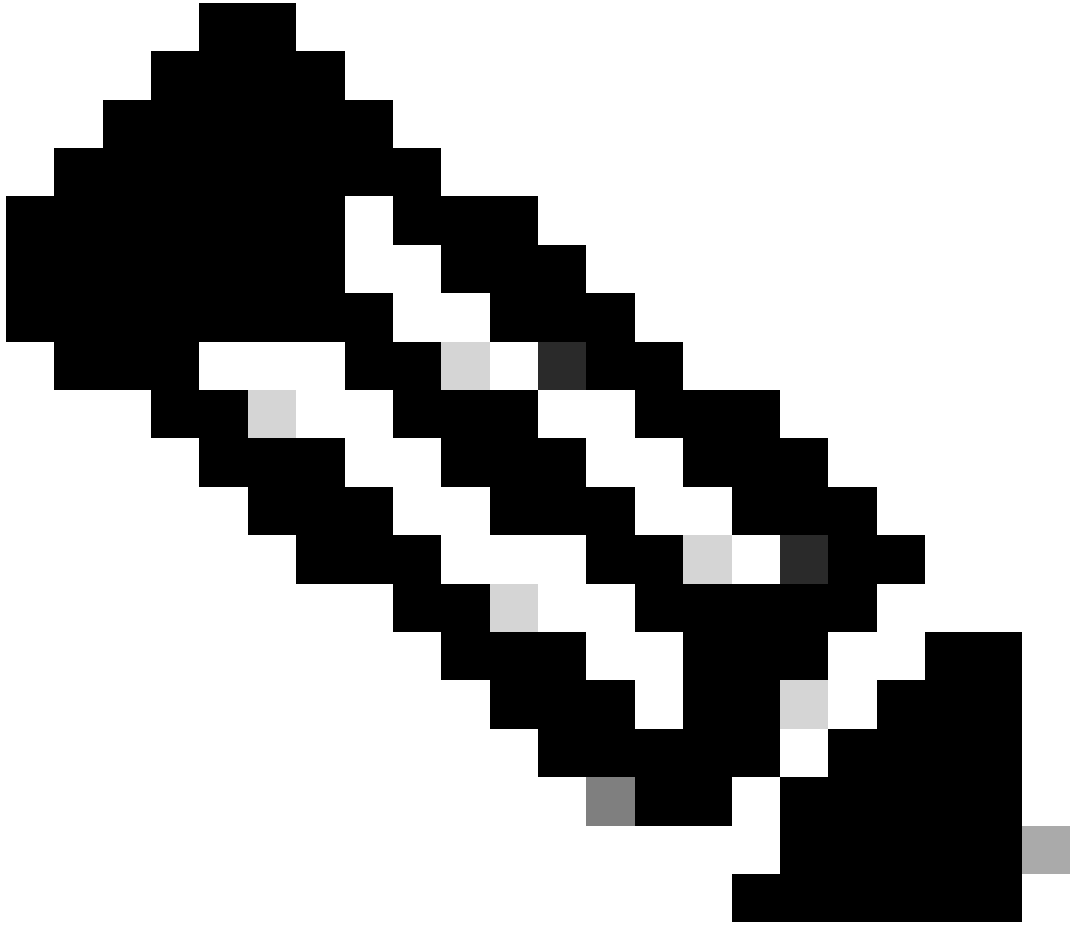


ةلازاب حمست ال اهنأ ي؛ يدرف لكشب ال ةفيظولا هذه ذيفنت نكمي ال: ةظحالم ةزيمل لوصافتل نم ديزمل. اهتثبت ةلازا وأ يعامج لكشب ةزهجال نم ةوعومج دعب نع تيثبتل ةلازا مسق [مدختسم ليلد](#) يف مدختسم ليلد لىل ةوجرلا يجرى [Secure Endpoint](#).

## تاقببطل ةجمرب تاهجاو مادختساب لوصوملا تيثبت ةلازا

رايخل نإف، ةنمآل ةياهنلا ةطقن مكحت ةدحو ربع لوصوملا تيثبت ةلازا لشف ةلاح يف (API) تاقببطل ةجمرب تاهجاو مادختسا وه قيببطل لل لباقل.

ال. هل صخرمو قدصم باسح ربع لوصول [Secure Endpoint](#) تاقببطل ةجمرب ةهجاو بلطت طقف ةدمتعمل تاباسحلل ال تاقببطل ةجمرب ةهجاو تايلمع لىل تابلل لاسرا نكمي. نم آ HTTPS لاصتا ربع تايلمع لىل صتت نأ بجي.



API، لة نم آلا ةياهن لة طقن ةقداصم لوح تامولعمل نم ديزم ىلع لوصحلل :ةظحالم  
[.ةنم آلا ةياهن لة طقن ل API ةقداصم](#): ةيلات لة لاقم لىل اءرا

---

ةروصل اىف حضوم وه امك SecureX عم ةنم آلا ةياهن لة طقن جم د 1. ةوطخلا

# SecureX

SecureX integration: Enabled

Disable

Name: Auto-created for Cisco - MSSP - Monsanc

GUID: 3186786e-ad75-4192-9af0-7974075808dc3

Enable incident promotion

Yes

No

Minimum severity for incident promotion ?

Low



Low, medium, high, and critical incidents will be promoted to SecureX.

ةروصللا يف حضوم وه امك SecureX تاقببطلال ةجمر بة هجاو ليمع ليحست 2. ةوطخلا

Integration Modules    Orchestration    Insights    Administration

Client Name\*  
Remote Uninstall Test

Client Preset  
[Empty] X v

API Clients    OAuth Code Clients

**Scopes\*** [Select None](#)

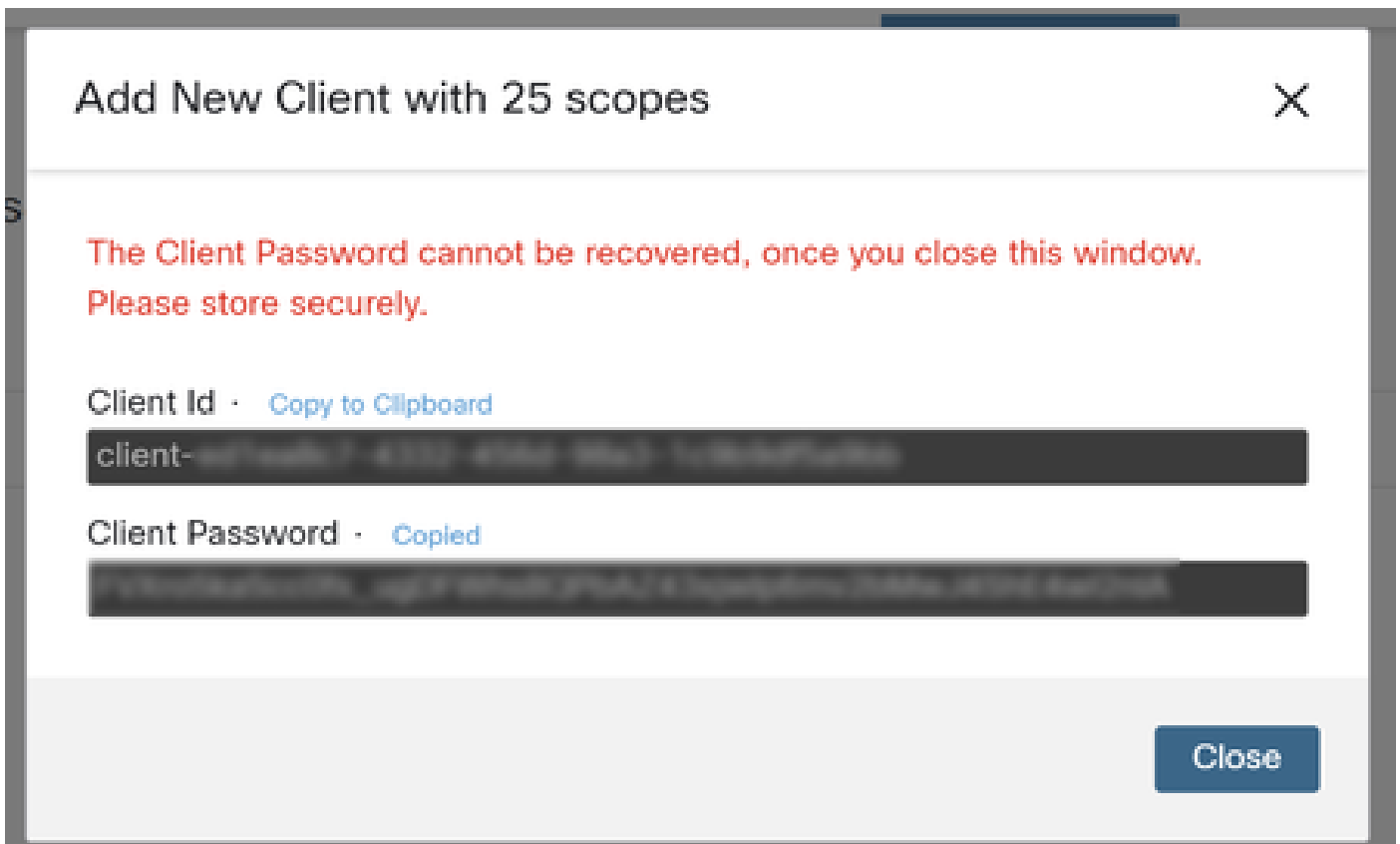
Search [Empty] 🔍

<input checked="" type="checkbox"/>	Admin	Provide admin privileges
<input checked="" type="checkbox"/>	AO	Manage and execute Automation workflows and related objects
<input checked="" type="checkbox"/>	Asset	Access and modify your assets
<input checked="" type="checkbox"/>	Casebook	Access and modify your casebooks
<input checked="" type="checkbox"/>	...	Query your configured modules for threat

Description  
Test for remote uninstall using API

[Add New Client](#)    [Close](#)

ةروصلال ي ف حضوم وه امك .نمآ لكشب دامتعالا تانايب نيزخت .3 ةوطخال



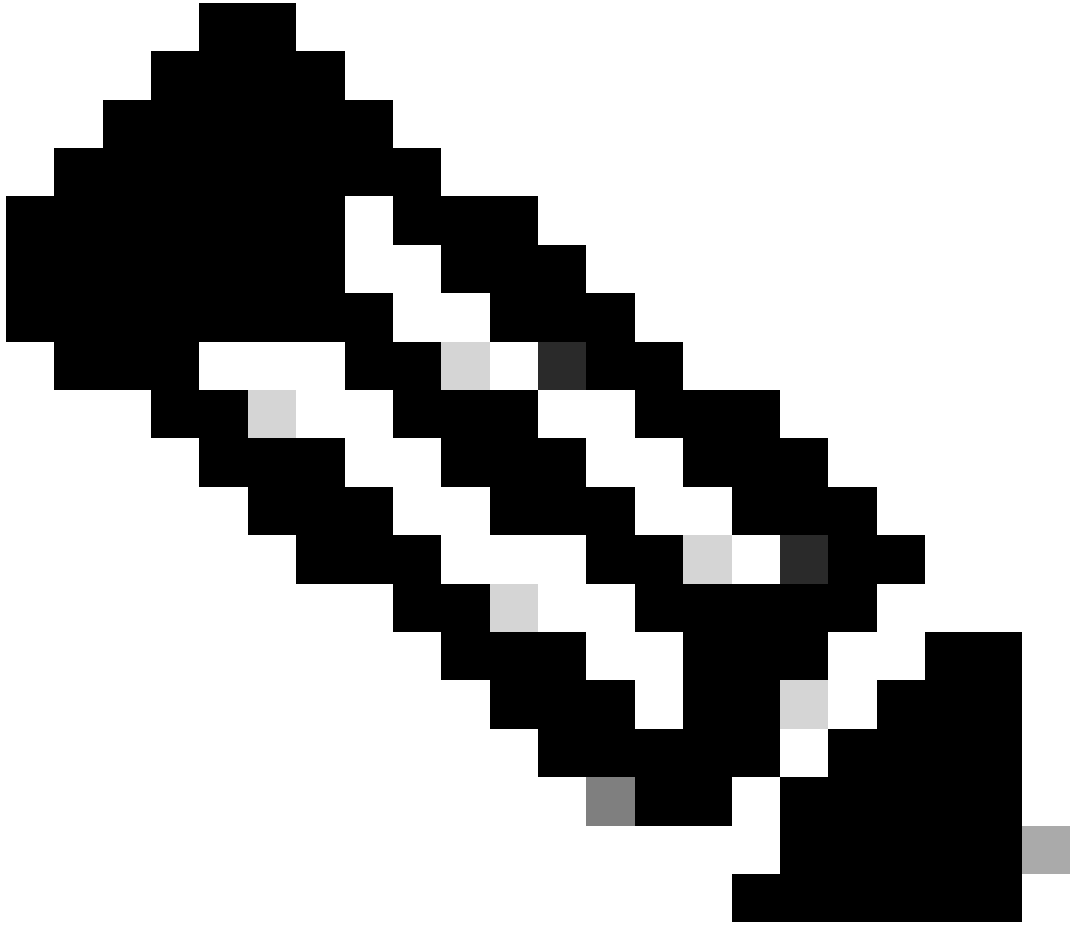
يأ م ادخ تساب فلم ال ( [example.sh](#) نم ه دادر تسإ مت ي ذل) example.sh لي غ ش تب مق 4. ة و ط خ ال  
ك را ي تخ إ نم ي صن جم ان رب فلم جم ان رب

ة ر و ص ل ال ي ف ح ض و م وه امك . ك ب ة ص ا خ ل ال د ا م ت ع ال ا ت ا ن ا ي ب ل خ د ا و فلم ال لي غ ش تب مق 5. ة و ط خ ال

```
Mex-Amp@Default-Win11 MINGW64 ~/Documents
$ bash uninstall.bash
client_id:
client_secret:
```

ل ال ة م ي ق ل ال ه ذه خ س ن ا . " ز ي م م ل ل و ص و ل ا ز م ر " ل ع ر ث ع ت ي ت ح ر ي ر م ت ل ا ب مق 6. ة و ط خ ال  
ة ر و ص ل ال ي ف ح ض و م وه امك . ت ا ق ي ب ط ت ال ة ج م ر ب ت ا ه ج ا و م ا د خ ت س ا ي ف ا ق ح ال ة ق د ا ص م ل

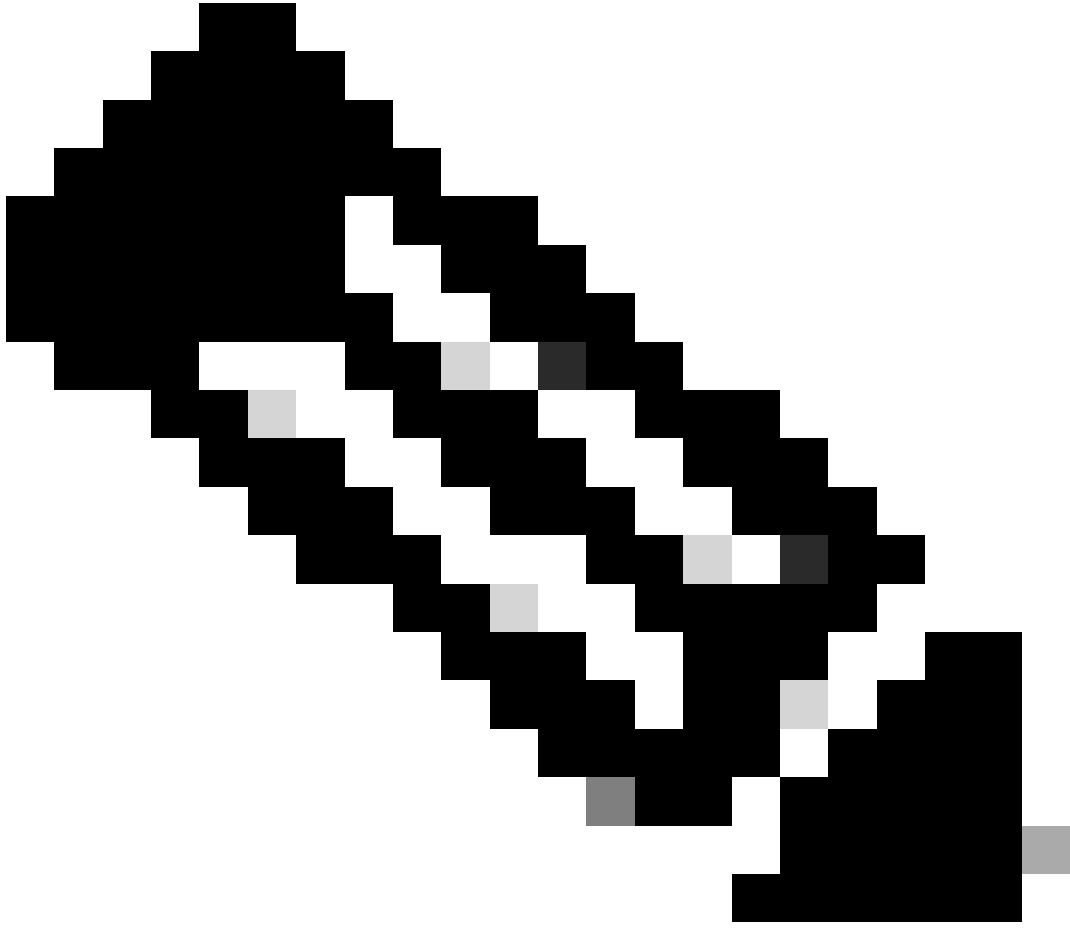
```
{
  "access_token": "
}
```



نم ةم و عدم ريغ ةادأل هذه .git.bash انم دختسإ ، دنن سمل اذه عاش نإل ةبسن لابل : ةظحال م  
ةادأل هذه م عدب لاصتالابل صوي ، اهب قلعت م لاؤس وأ كش ي ، Cisco لبق

---

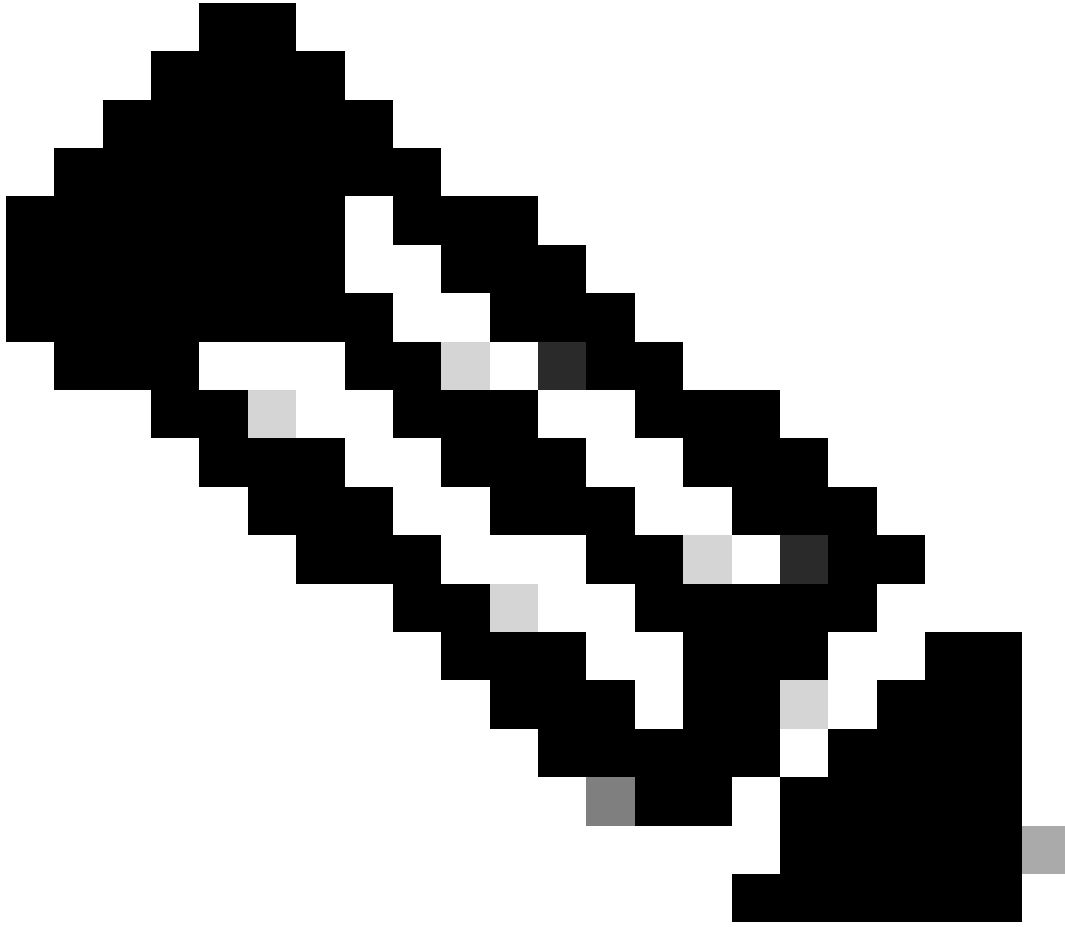
مادختسإ حيتت ةادأ مادختسإ كنكمي ، زي ممل ةقدا صملا زمر لعل لوصحلا درجم ب . 7 ةوطخال  
تاقب بطتلا ةجرم رب تاهجاو



نم ةم و عدم ريغ ةادال هذه Postman م ادختساب انمق ،دنتسم لا اذه عاشنل :ةظحال م ةادال هذه م عدب لاصتالاب ي صوي ،اهب قلعتم لاؤس وأ كش ي، Cisco لبق

---

([لصوم تيبتت ةلازا بلط](#)) تاقيبتتال ةجمر ب ةهجاو عجرم ةغايص ل ا ادانتسا 8 ةوطخال هتبتت ةلازا دارم لا زا جلاب صاخال GUID م ادختساب ل صوم ل تيبتت ةلازا بلط ارجا



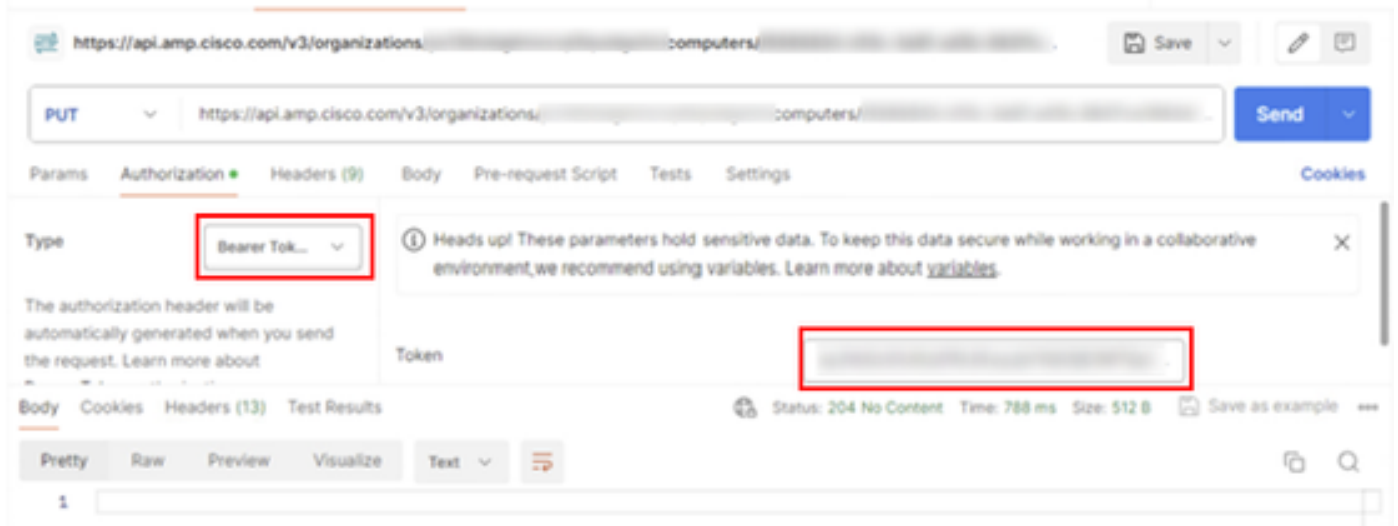
نيتطي سب نيتتقيرطب لصوص لابس صاخ ال GUID لى لوصح ل كنكمي :ةظحالم

- لى لوصح ل كومپيوترس (ةرادال) Management لى لقتنا ةنمآلا ةياهنلا ةطقن ةباب لى ل > لى لوصح ل ضرع > بولطم ل رتوي بكم لى ل لقتنا > (رتوي بكم ل ةزهج) (يمومع ل ديرف ل فرع ل) GUID لى ل لوصح ل
- لوصح ل > "تايئاصح" بيوبت ل ةم لى ل لقتنا > قرولا ةبلع ةنوقيأ حتفا لى ل GUID.

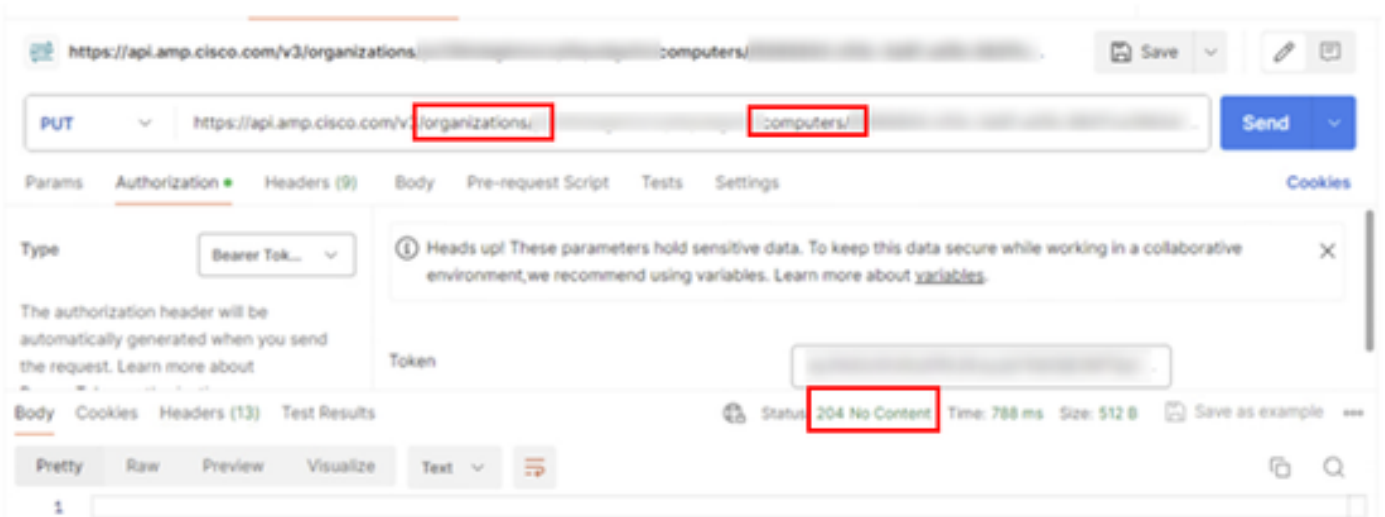
---

لوصح ل م ت يذلا زي م ل لوصول زمر لخدأو ةقداصم ةقيرطك زي م ل لوصح ل زمر دح. 9 ةوطخ ل ةروصل لى ل لوصح ل وه امك. 6 ةوطخ لى ل لوصح ل لوصح ل





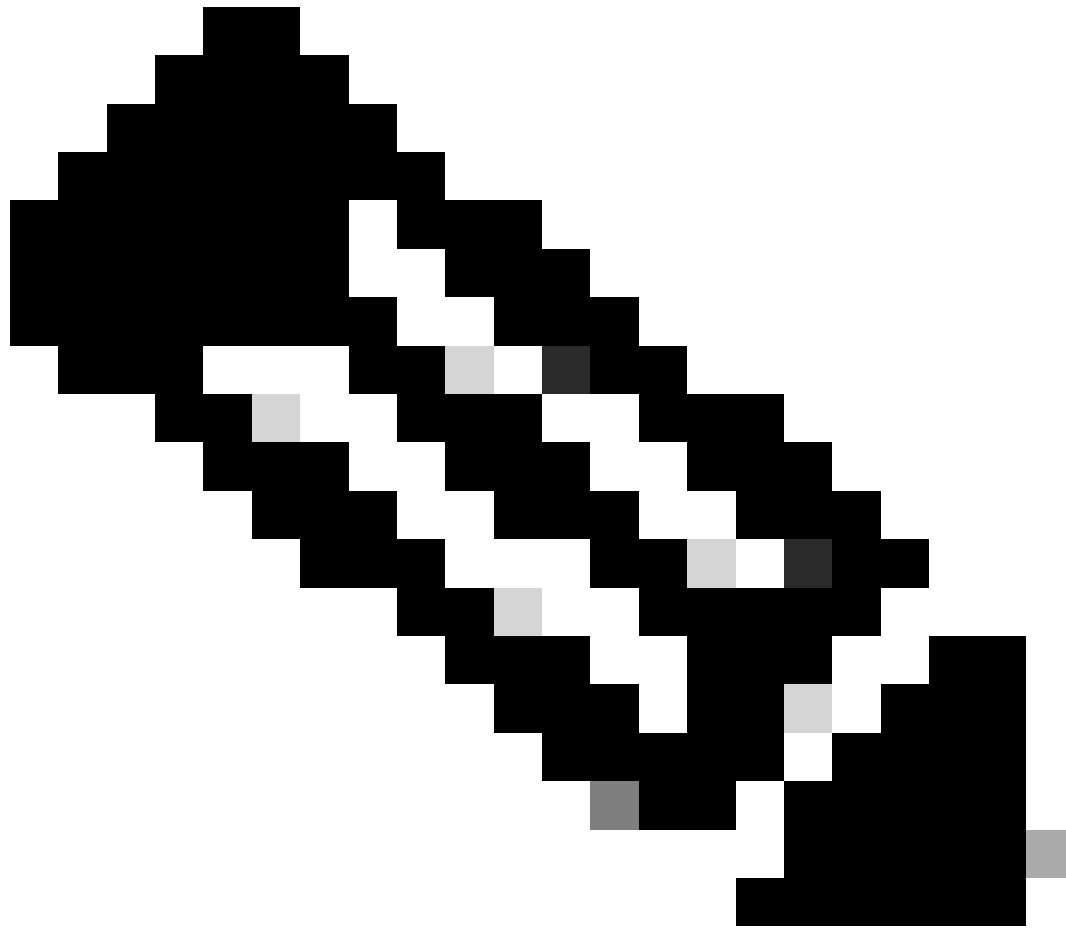
يحتفظ بنا. لاسرنا رزقوف رقن او API اعادتسا نم ةبولطم ل لوقح ل ةئبعتب مق 10 ةوطخل ةروصل اي فحضم وه امك .يوتحمل ل ةباجتسا دجوي ال :204



،اي لحم تام ول عمل ةعجارم دع . روف ال ال عكحت ل ةدحو في ل صوم ل ليجست في تخيس ، امك ل اب هت ل ازم تتس ، قئاق د عضب دعبو وتيبت ل ةلازا حن ال اتقوم ل صوم ل لقتنيس ةروصل اي فحضم وه امك . زاهج ل نم

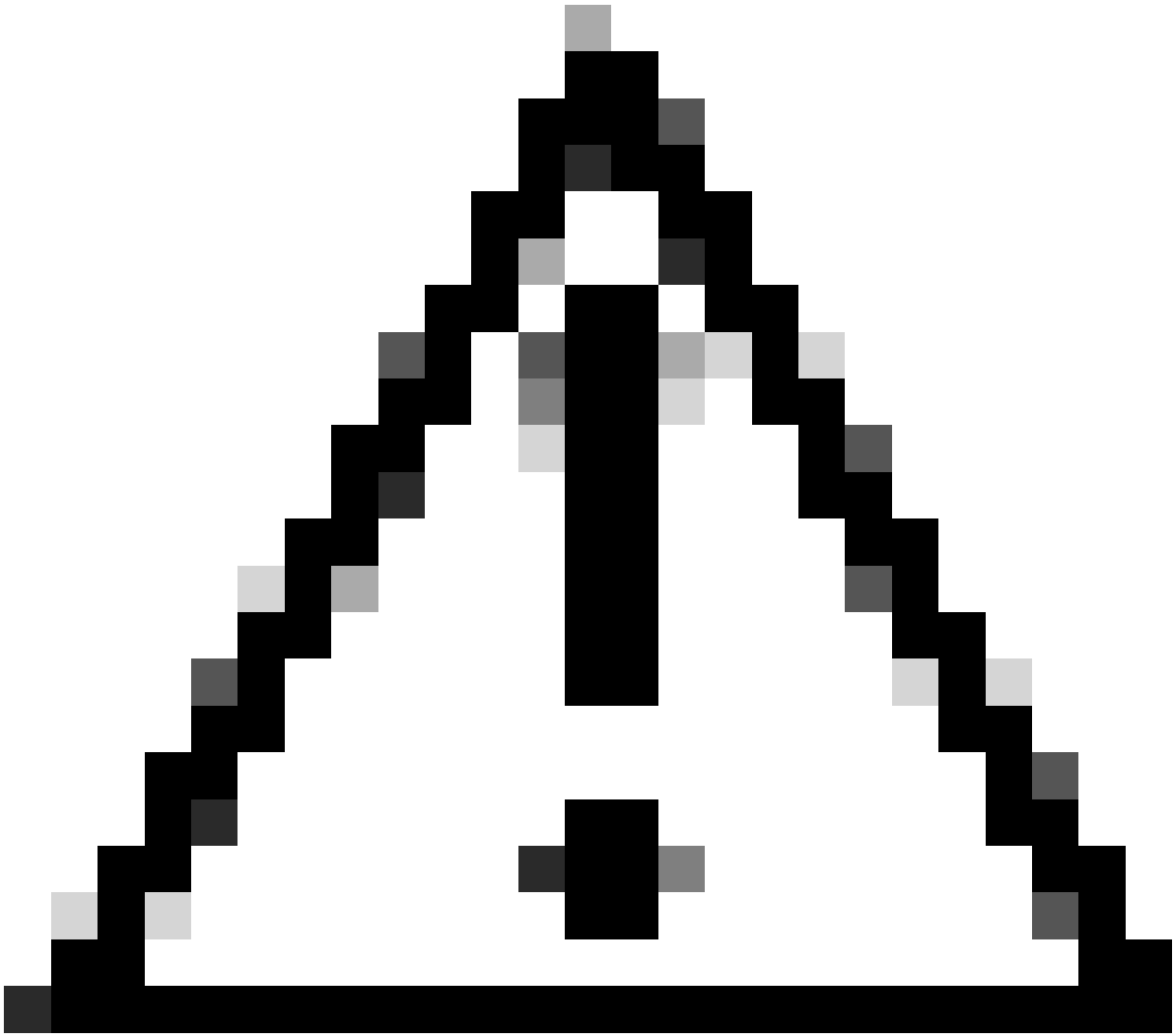
## Policy

Name: AUTO-GENERATED Uninstall policy for b57195ad-ab96-4b15-bc3e-5a...  
 Serial Number: 69  
 Last Update: Today 04:37:49 AM



دق ةمهمل هذه ذي فنن تل لصوملا اهم دخست سي يتلا ةي نم زلا ةرت فلأ نأ ركذت :ةظحالم  
كب ةصاخلا ةئيبل بسح فل تخت

---



ةيلمعلا لاوطالصتم لظي تيبتثتلا ةلازا لبقتسي يذلا زاوجلنا نأ نم دكأت: ريذحت

يتح كنكمت مدعو (تيبتثتلا ةلازا قرط) هالعأ ةروكذملا تاليثملا ةفاك دافنتسا ةلاح يف  
يف جردملا ريخألا ذالملا راخي راخيخا كنكمي، بولطملا لصوملا تيبتثتلا ةلازا نم نألا  
ةيلاتلا ةقيرطلا.

## رمأالا رطس تالوحم مادختساب لصوملا تيبتثتلا ةلازا

تاءارجلنا نم ديدعلا ذيفنت كل حيتت يتلا ةجمدملا رمأالا رطس تالوحم يلعتبثملا يوتحي  
[ةياهنلا ةطقنل رمأالا رطس تالوحم](#): ةيلاتلا ةلاقملا يف روكذم وه امك ةياهنلا ةطقن يف  
[ةنمأالا](#).

ةيلاتلا تاداشرالا مدختست رمأالا رطس تالوحم مادختساب CSE لصوملا تيبتثتلا ةلازال

ةيرادا تازايتما ب رمأاو هجوم حتف. 1. ةوطخلا

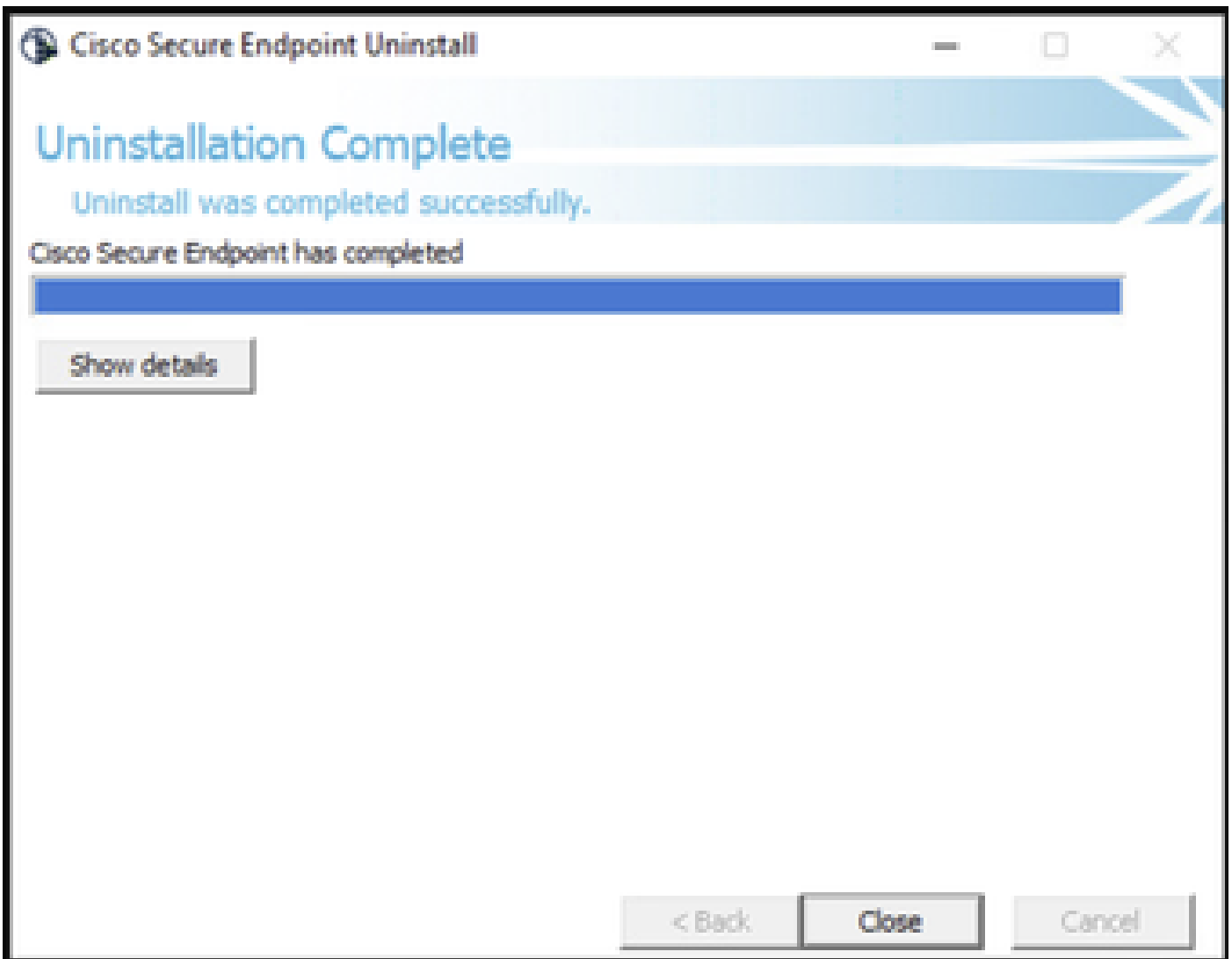
ةروصللا يف حضوم وه امك. تيبتثتلا ةمزح هي ف دجوت يذلا عقوملا للاقنا. 2. ةوطخلا

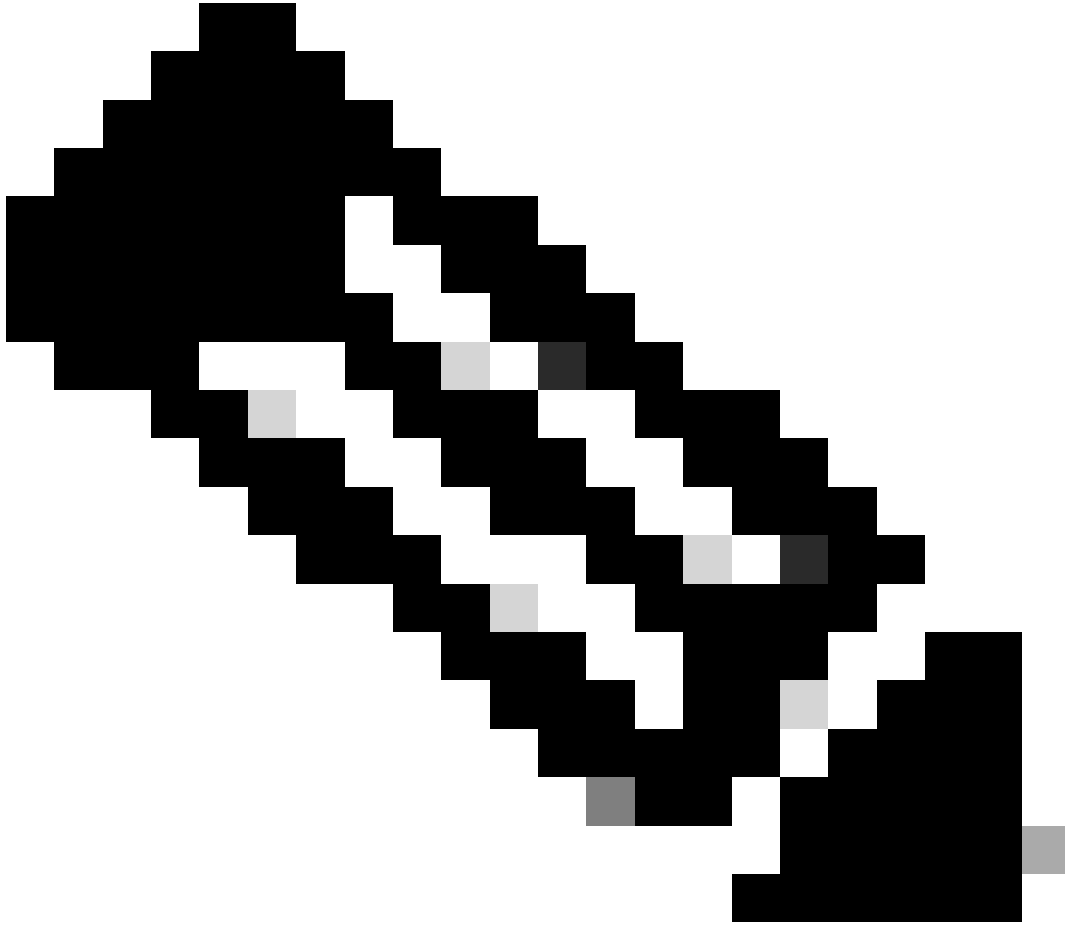
```
C:\Users\Mex-Amp>cd Downloads
```

وه امك . اهذي فنت متيس يتي لرم او ال رطس تال و ح م ب اع و ب ت م ة م ز ح ل ا م س ا ب ت ك ا 3. ة و ط خ ل ا ة ر و ص ل ا ي ف ح ص و م .

```
C:\Users\Mex-Amp\Downloads>FireAMPSetup.exe /R /remove 1
```

وه امك . " ل م ا ك ل ا ت ي ب ث ل ا ا غ ل ا " ة ش ا ش ي ل ع ل و ص ح ل ا م ت ي ي ت ح ج ل ا ع م ل ا ع ب ت ا 4. ة و ط خ ل ا ة ر و ص ل ا ي ف ح ص و م .



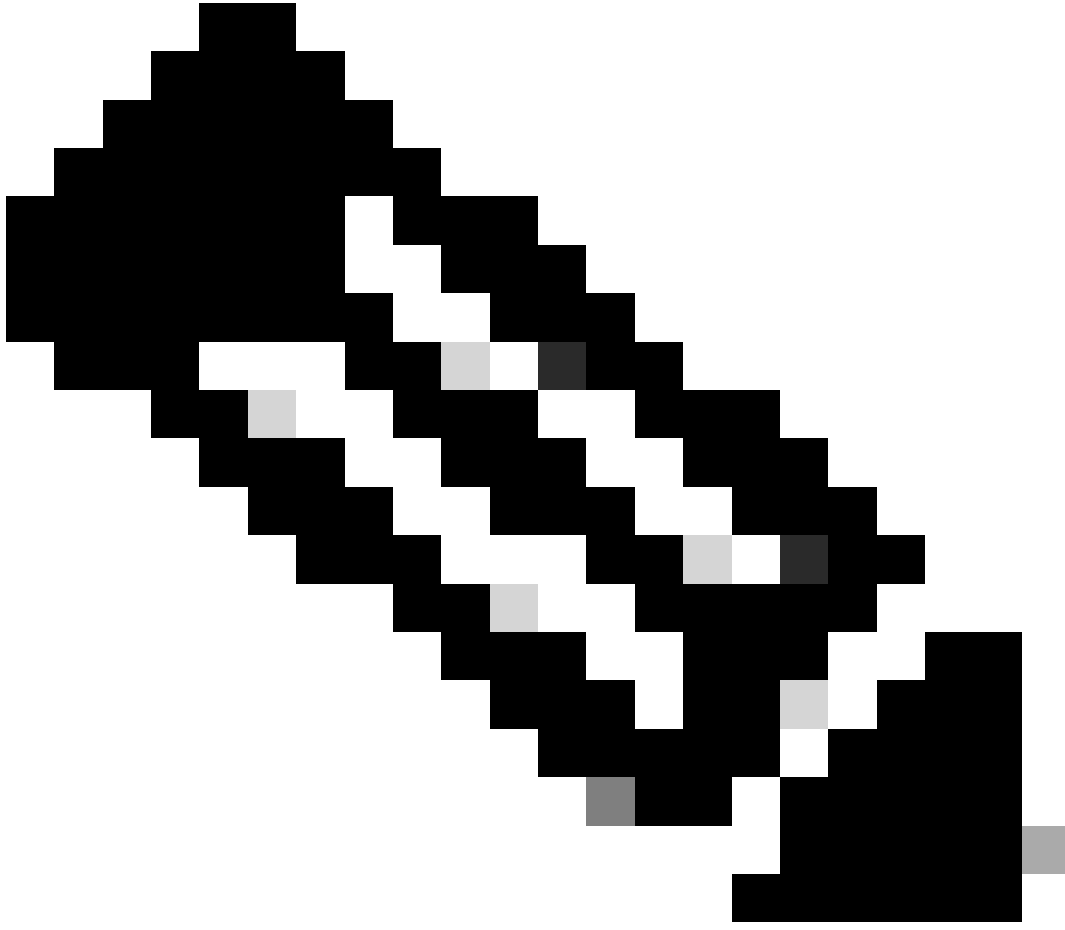


مدعو تي بثلتال ةم زح لباقم تي بثلتال ةلازاب صاخلا لوحملا ليغشت بجي :ةظحالم  
exe.تي بثلتال ةلازا

---

لوحملا نوكي ،لصوملل ةلمكو ةتامص تي بثلتال ةلازا ءارجإل

FireAMPSetup.exe /R /S /remove 1



/s. لوجملا ةلازاب ةتاماصلل ريغ عاضوألل يف كلذ ذيفنت اضيأ كنكمي :ةظحالم

---

لوجملا نوئي ،رورملا ةملك ةيماحب عتمتي لوصول ةلماك تيبتت اعلا ةيلمع اعرجال

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

لوصول تيبتت ةلازاب جي يذلا زاهجال لعل تيبتتال اعلا ةادأ ليغشت نإف ،ريخأ لحو  
ةلكشملا لحيس هيلع

ةيرادإ تازايتماب رماوأ هجوم حتف 1. ةوطخلال

رادصا وه x شيح .ةنمآلا ةياهنلال ةطقن لوصول هيف بجوي يذلا عقوملال للاقنتنا 2. ةوطخلال  
ةروصلال يف حضورم وه امك .CSE لوصول

C:\Program Files\Cisco\AMP\>

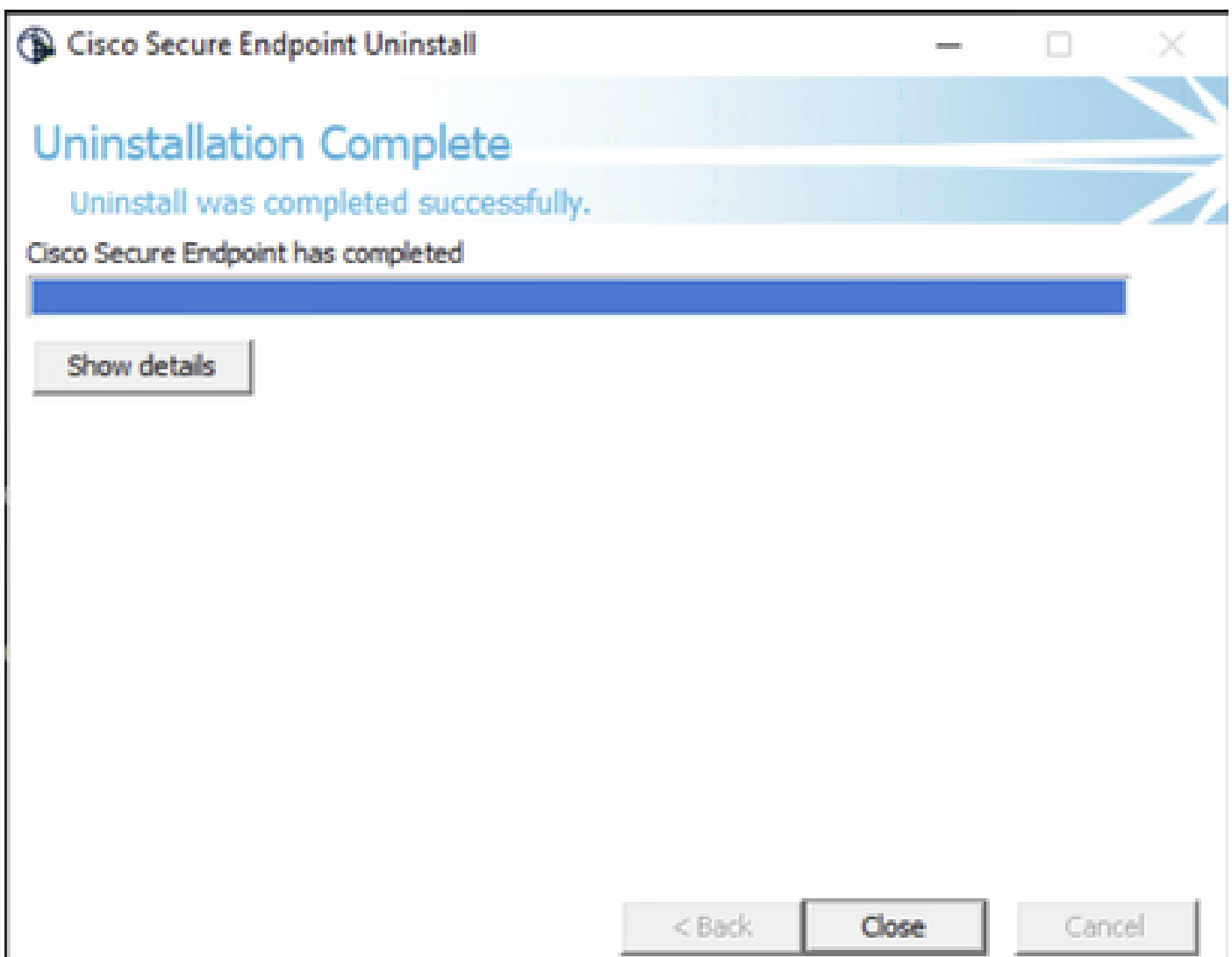
```
C:\Program Files\Cisco\AMP>cd 8.2.3.30119
```

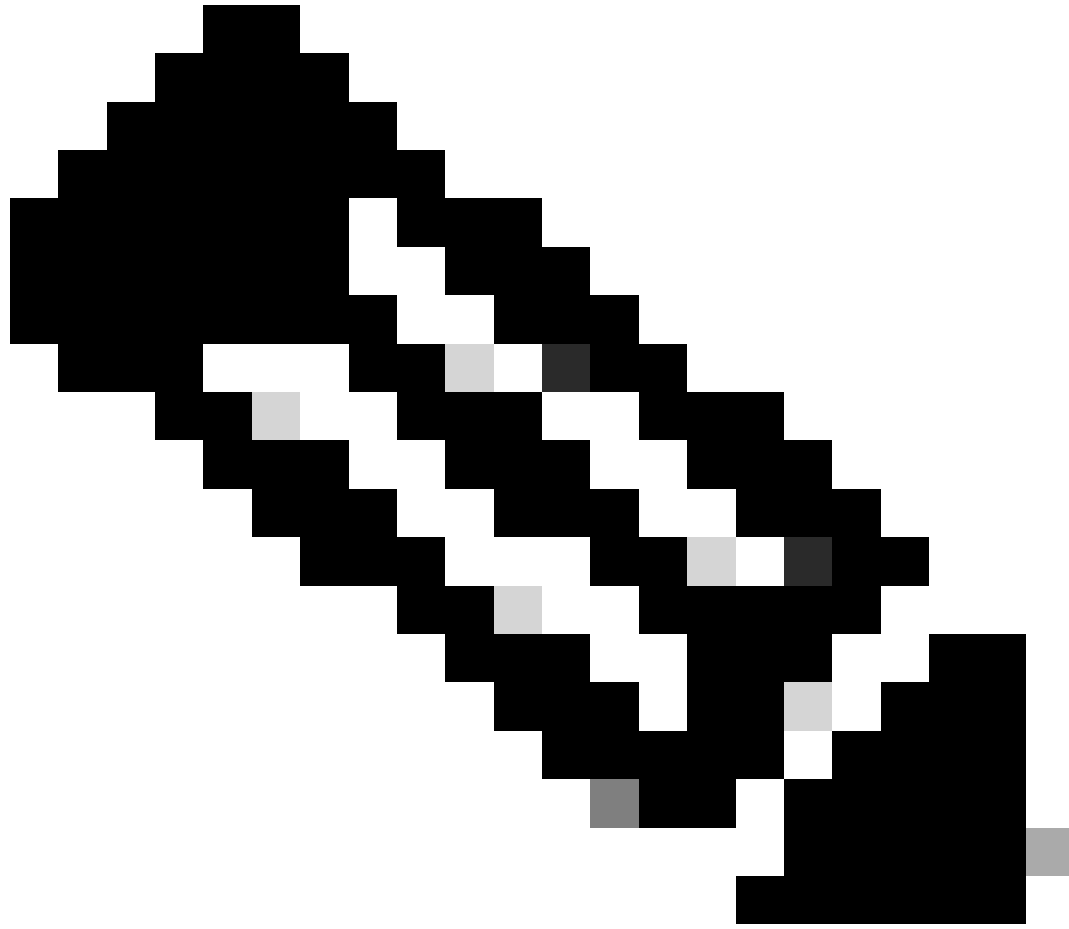
ةروصلال يف حضورم وه امك .ةللاتل تااطيسولل مادختساب فللمل ذيفنتب مق 3. ةوطخلال

```
uninstall.exe/full 1
```

```
C:\Program Files\Cisco\AMP\8.2.3.30119>uninstall.exe/full 1
```

وه امك ".لماكلل تيبتللا ءاغلإ" ةشاش لعل لوصحلل متي يتحل لعمال عبتا 4. ةوطخلال ةروصلال يف حضورم.

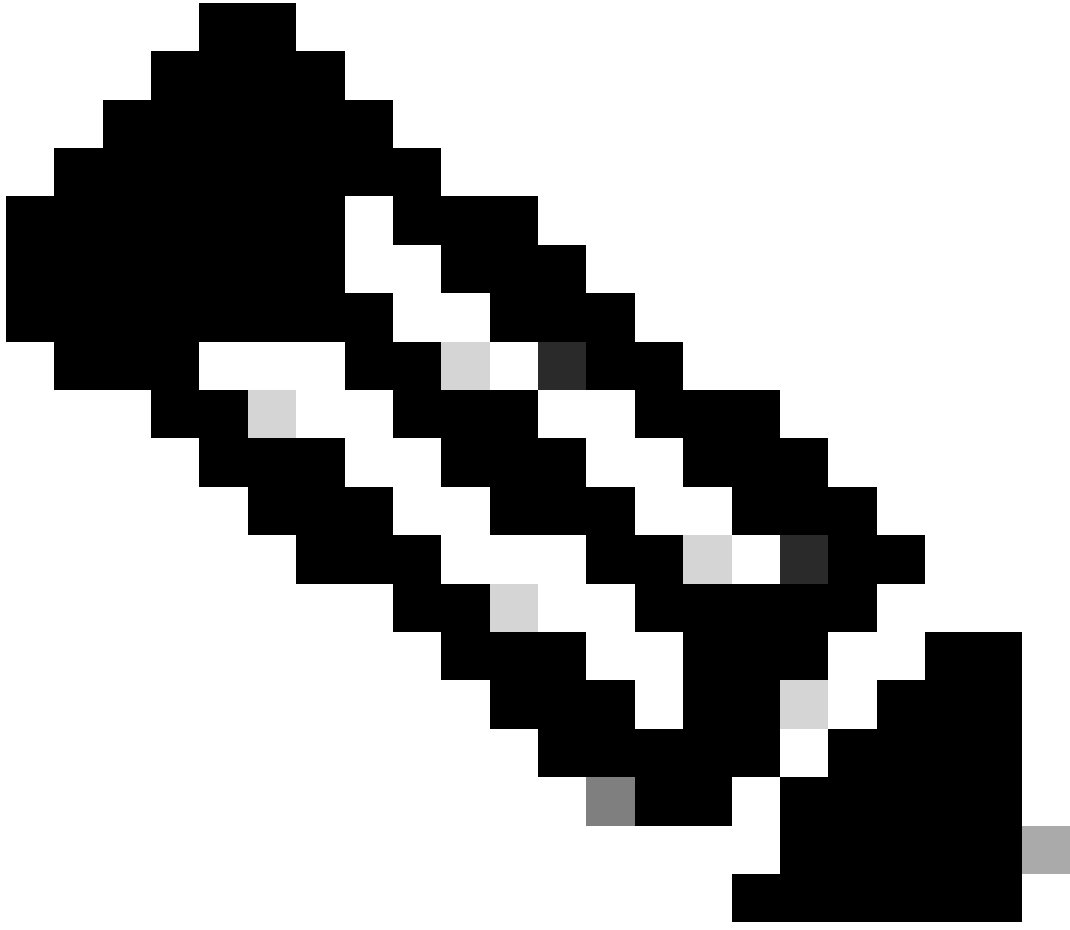




ىلا ةراشإلا نودب رمألا لىغشت كىل ع بىجى ، AMP راسم دوجو مدع ةلا ح ىف :ةظحال م  
اهىلإ راشملا تااطىسولا مادختساب رمألا لىغشتب طقف مق ، راسملا

---





ةلازال رخآ لصومب صاخلا uninstaller.exe ليغشت نكمملا نم، رمألا مزل اذا: ةظحالم  
بولطملا لصوملا تيبتت.

---

## ةلص تاذا تامولعم

- [ةنمألا ةياهنلا ةطقن مدختسم ليلد](#)
- [تادنتسم لاوينقتلا معدلا - Cisco Systems](#)
- [Secure Endpoint API v3](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا