

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](#)

[تاقببطل ةجمرب تاهج او ماخذتساب لصوملا تيبثت ةلازا](#)

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

[ةلص تاذا تامولعم](#)

ةمدقملا

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

ةيساسألا تابلطتملا

تابلطتملا

ةيلال عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

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

ةمدختسملا تانوكملا

ةيلال ةيداملا تانوكملا او جماربل تارادصلإل دنتسملا اذه يف ةدراول تامولعملا دنتست:

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

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسملا اذه يف ةدراول تامولعملا عاشنإ مت
تناك اذإ. (يضا رتف). حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجألا عيمج تأدب
رمايال لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك كتبش.

ةيساساً تامولعم

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

ةديجل تاتيبتتلل ااوس ،لمكلااب لصوم ل نم صلختلل ارايخ لصوم ل تيبتت ةلازا دعت
نآل دعب Windows زاهج ىلع لصوم ل دوجوم دعب ةطاسبب وأ

تيبتتل ةلازا قرط

ماظن ب لمعي رتويبمك ىلع ةنمآل اةياهنل اةطقن لصوم ل تيبتت ةلازا يف بغيرت نأ درجم ب
لصفأ لكشب كتاجايحتح بسانت يتل اةقيرطال عبتا Windows ليغشتل

ايودي تيبتتل ةلازا

اي لحم لصوم تيبتت ةلازال

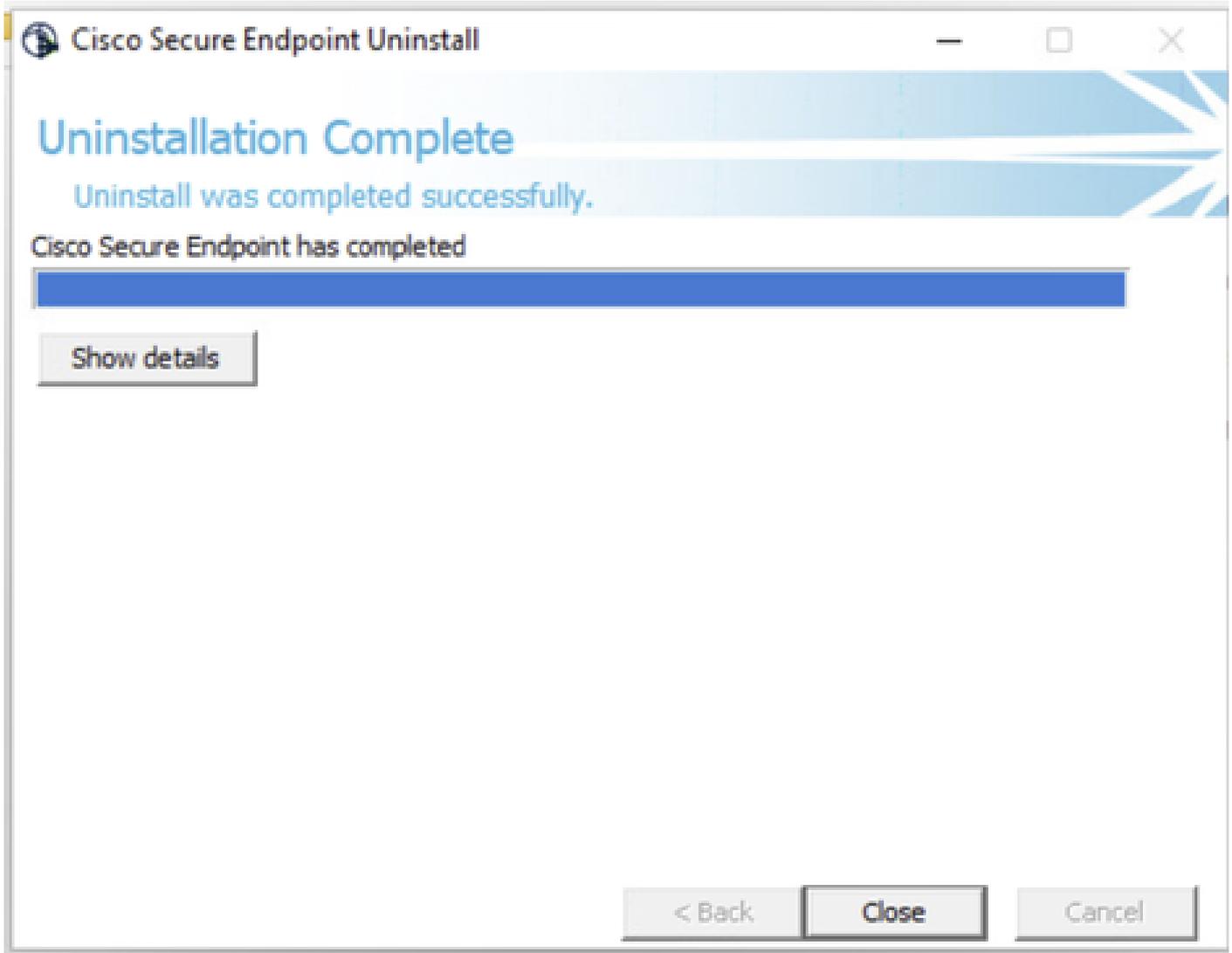
لصوم رادصا وه X ثيخ) Cisco > AMP > X > جماربل تافل م ىلإ لقتنا ،زاهج ل يف 1. ةوطخل
(CSE).

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

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

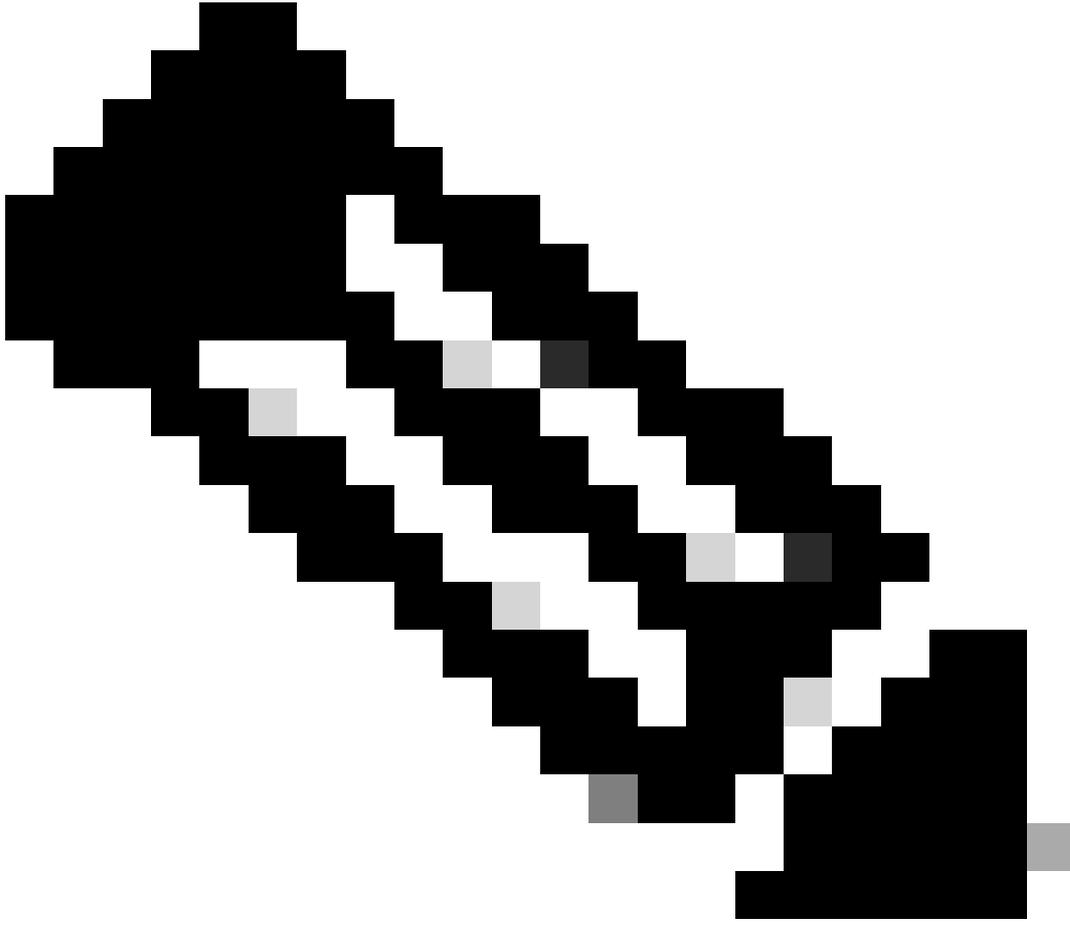
Name	Date modified	Type	Size
hs.dll	2/20/2024 2:54 PM	Application exten...	3,837 KB
ipsupporttool.exe	2/20/2024 2:54 PM	Application	693 KB
libcrypto-1_1-x64.dll	2/20/2024 2:54 PM	Application exten...	3,357 KB
libssl-1_1-x64.dll	2/20/2024 2:54 PM	Application exten...	678 KB
mfc140u.dll	2/20/2024 2:54 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 ةداعت مزلي، "تېبثتلا ةلازا" راوحتل عېرم يف ال ديحت ةلاح يف: ةطحاتم
ةيقبتم ال CSE تادلجم يا نم امامت صلختلل زاهلل ةلمك

ةنمآلا ةياهنلا ةطقن مكحت ةدحو نم لصوملا تېبثت ةلازا

مادختساب كلذب مايقلا كنكم يف، مكحتلا ةدحو نم دعب نع تېبثتلا ةلازا الى ةجاحب تنك اذا
لصوملا تېبثت ةلازا رزلا

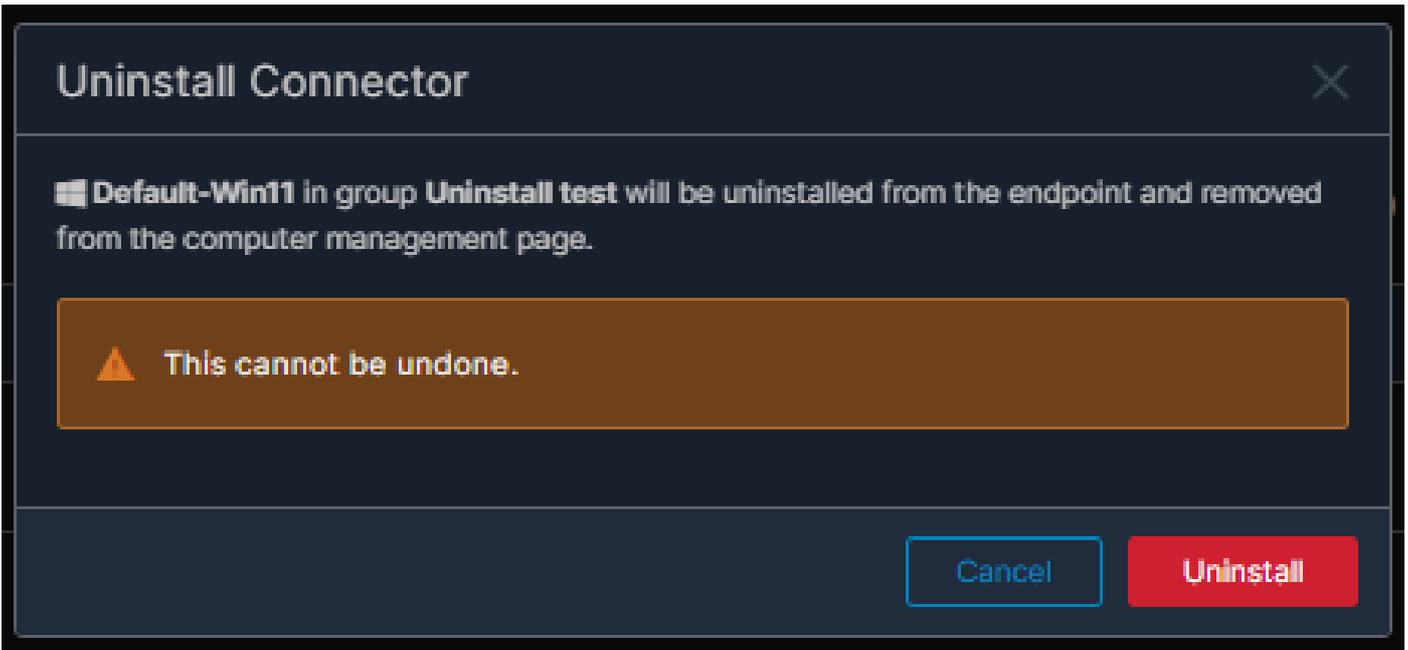
رتويبمكلا ةزهجأ > ةرادإلا الى لقتنا، مكحتلا ةدحو يف 1. ةوطخلا

ليصافتلا ضرعل رقنا م، ةتېبثت ةلازا ديرت يذلا رتويبمكلا عقوم دح 2. ةوطخلا

ةروصلال يف حضورم وه امك. لصوملا تېبثت ةلازا رزىل عل رقنا 3. ةوطخلا



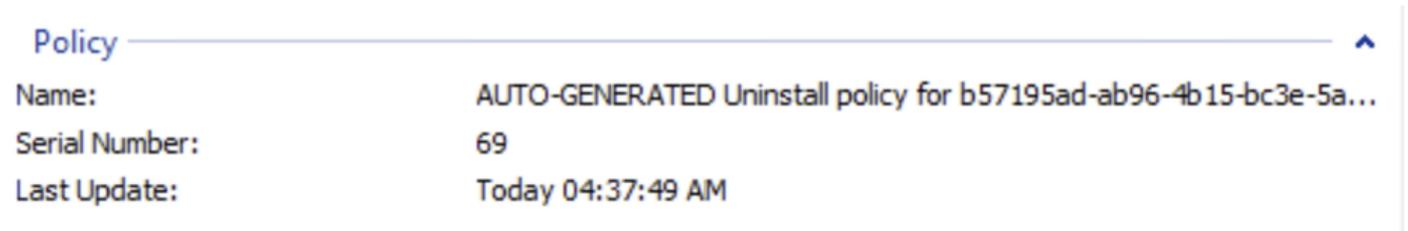
في حضوره وه امك .عارج ال تي بثت ك نم بلطي ام دنع تي بثت ال الازا قوف رقنا 4. ةوطخل ال
الروصل.

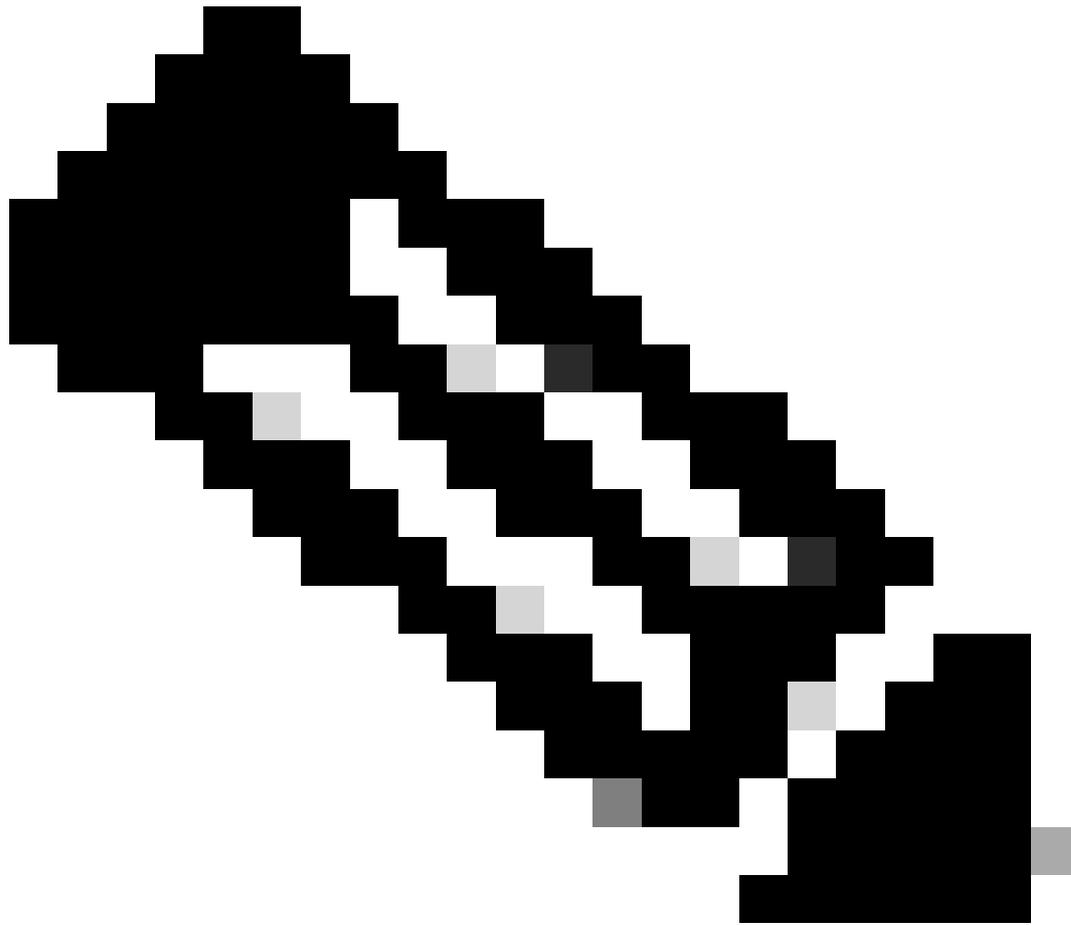


ةياهن ال ةطقن مكحت ةدحو نم يولعل اعزل ال في ديكأت ةلاسر ي قلتت فوس 5. ةوطخل ال
الروصل في حضوره وه امك .ةنمأل

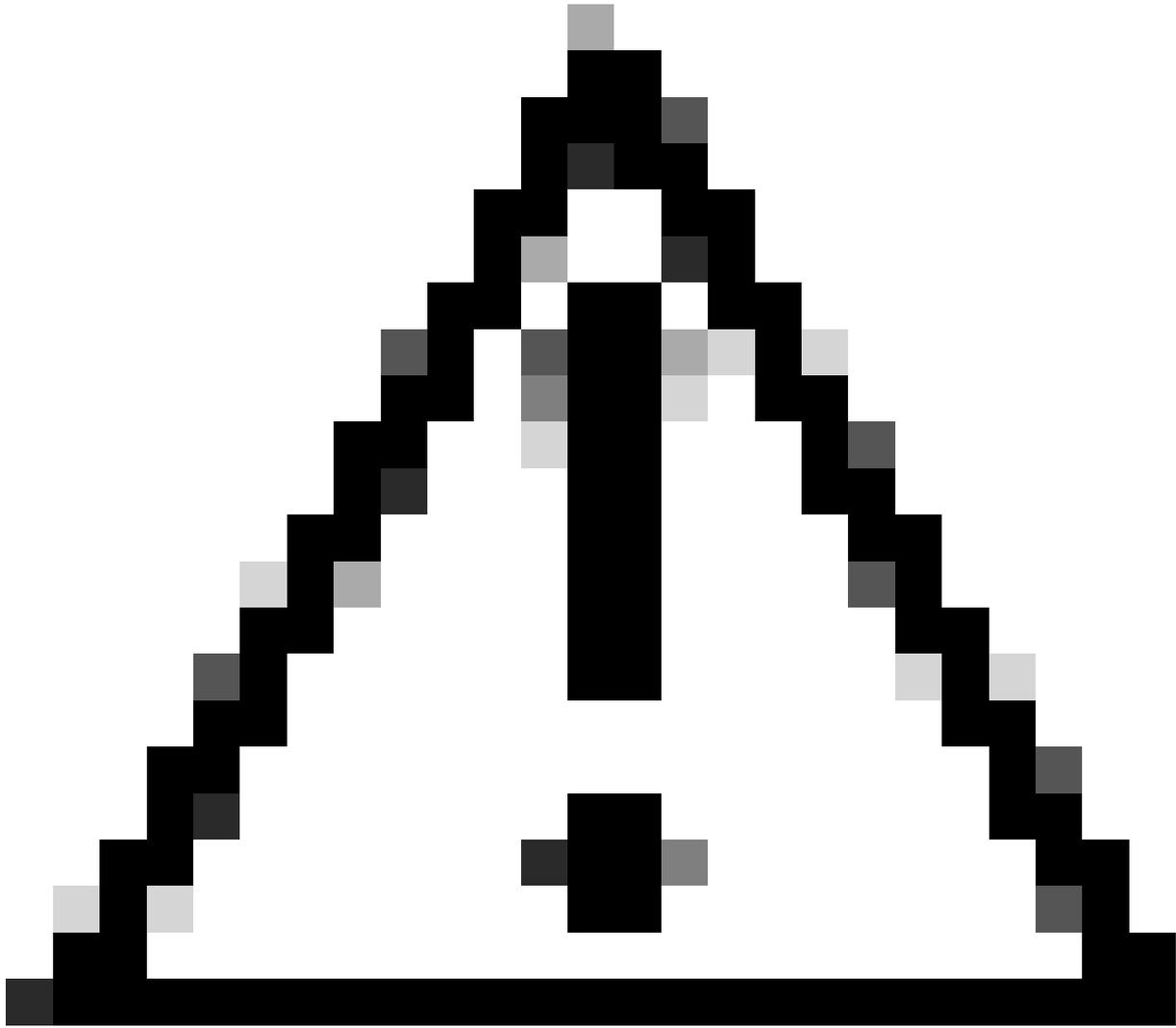


اي لحم تامولعمل اعجارم دع ب .روف ال ال على مكحت ال ةدحو في لصولم ال لي جس تي فتي خي س
لمالك ال اب هت الازا م ت تس ،قئ اقد ع ض ب دع بو تي بثت ال الازا هن ال ات قوم لصولم ال لقت نيس
الروصل في حضوره وه امك .زاهج ال نم

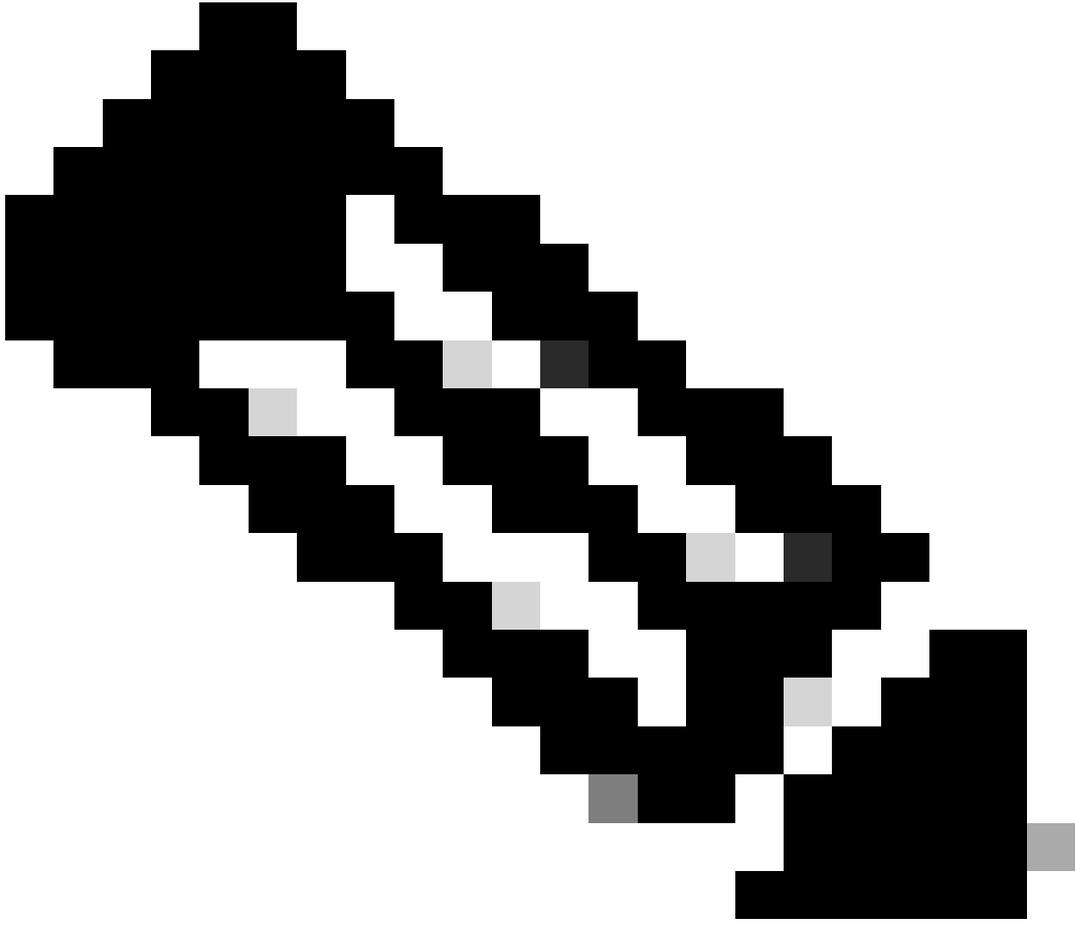




دق ةمهمل هذه ذي فنن تل لصوملا اهم دختسي يتلا ةي نم زلا ةرت فل نا ركذت :ةظحالم
كب ةصاخلا ةئيبل بسح فل تخت



ةيلمعلا لاوطالصتم لظي تيبتثالالازا لبقتسي يذلا زاهجلا نا نم دكات :ريذحت



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
X v

API Clients OAuth Code Clients

Scopes* [Select None](#)

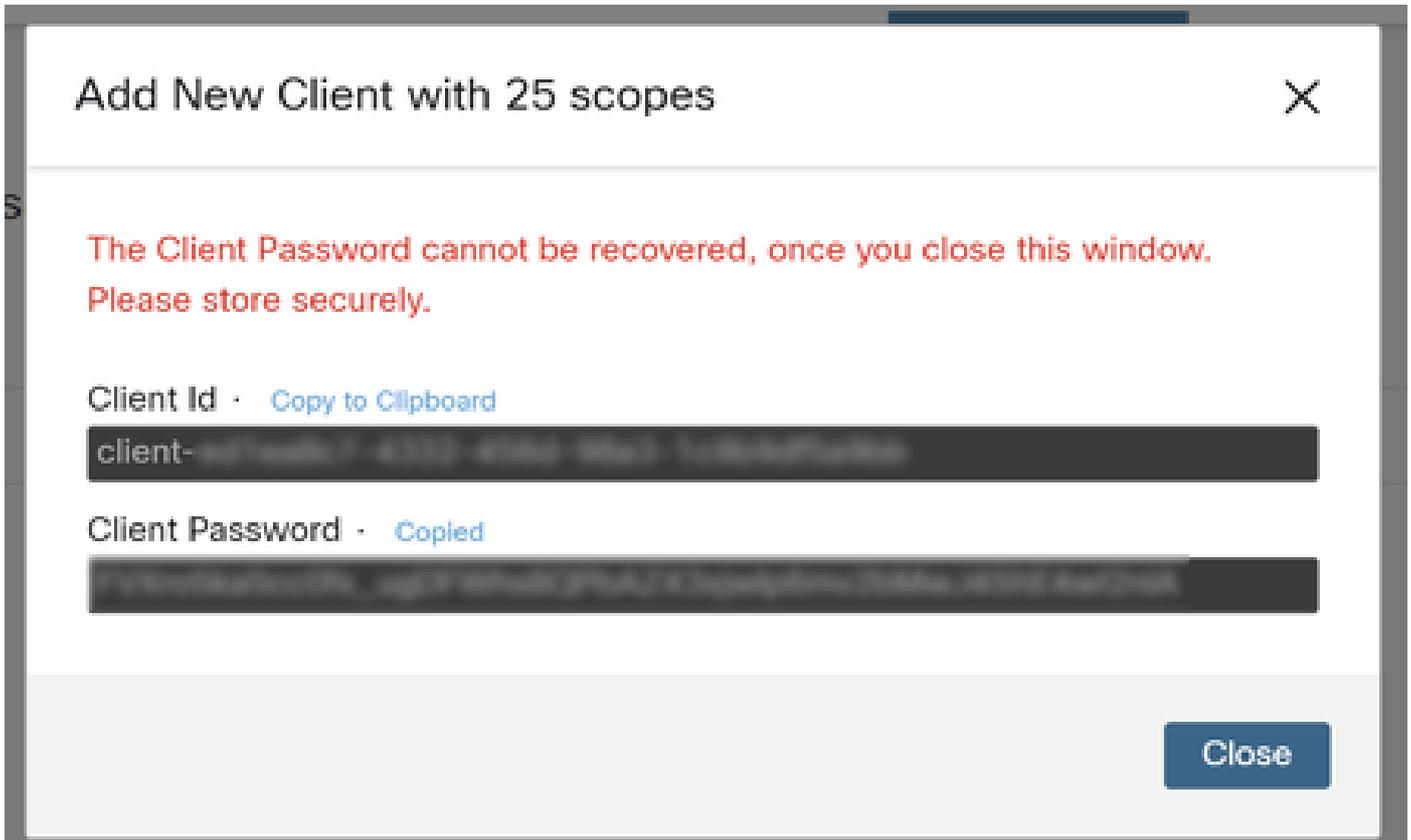
Search

<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 حضورم وه امك .نمآ لكش ب دامتعالا تانايب نيزخت .3 ةوطخال



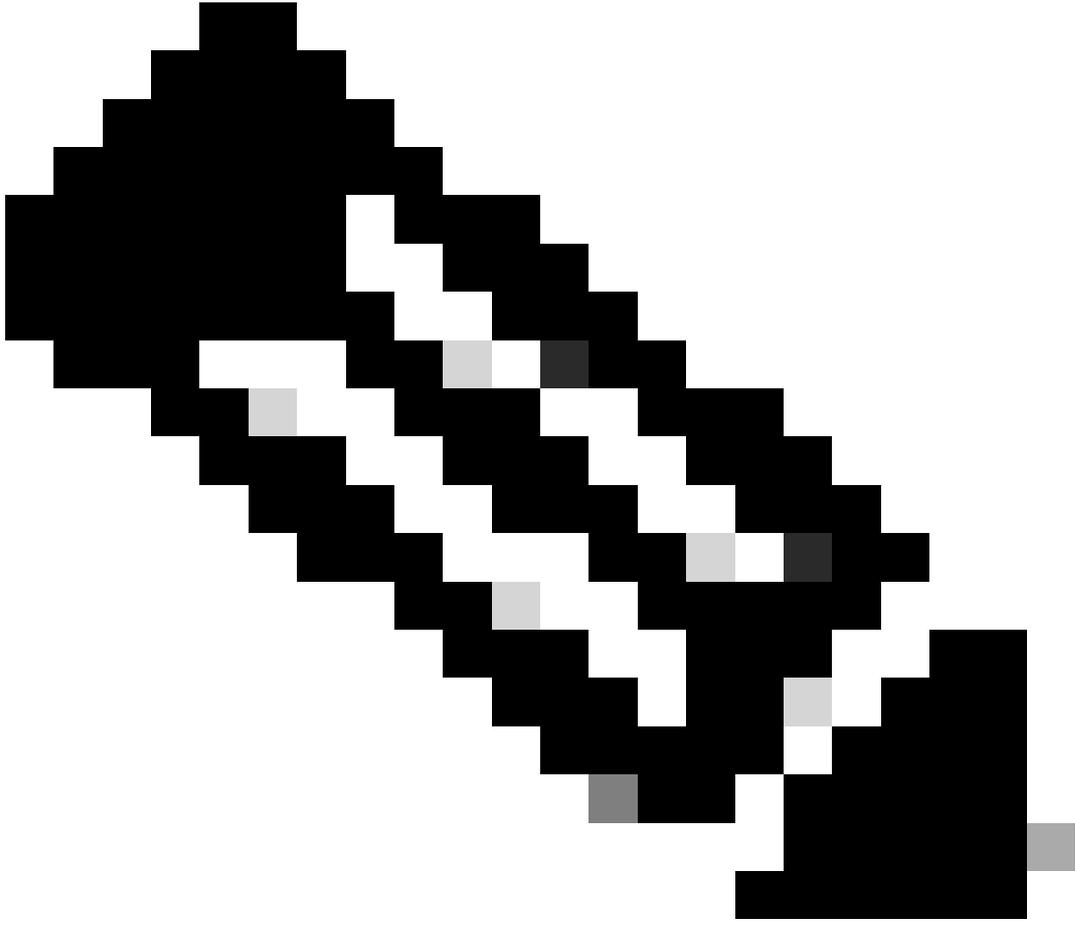
يأ م ادخ تساب فلم ال ([example.sh](#) نم ه دادر تسإ مت ي ذل) example.sh لي غ ش تب مق 4. ة و ط خ ال
ك را ي تخ إ نم ي صن جم ان رب فلم جم ان رب

ة ر و ص ل ال ي ف ح ص 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:
```

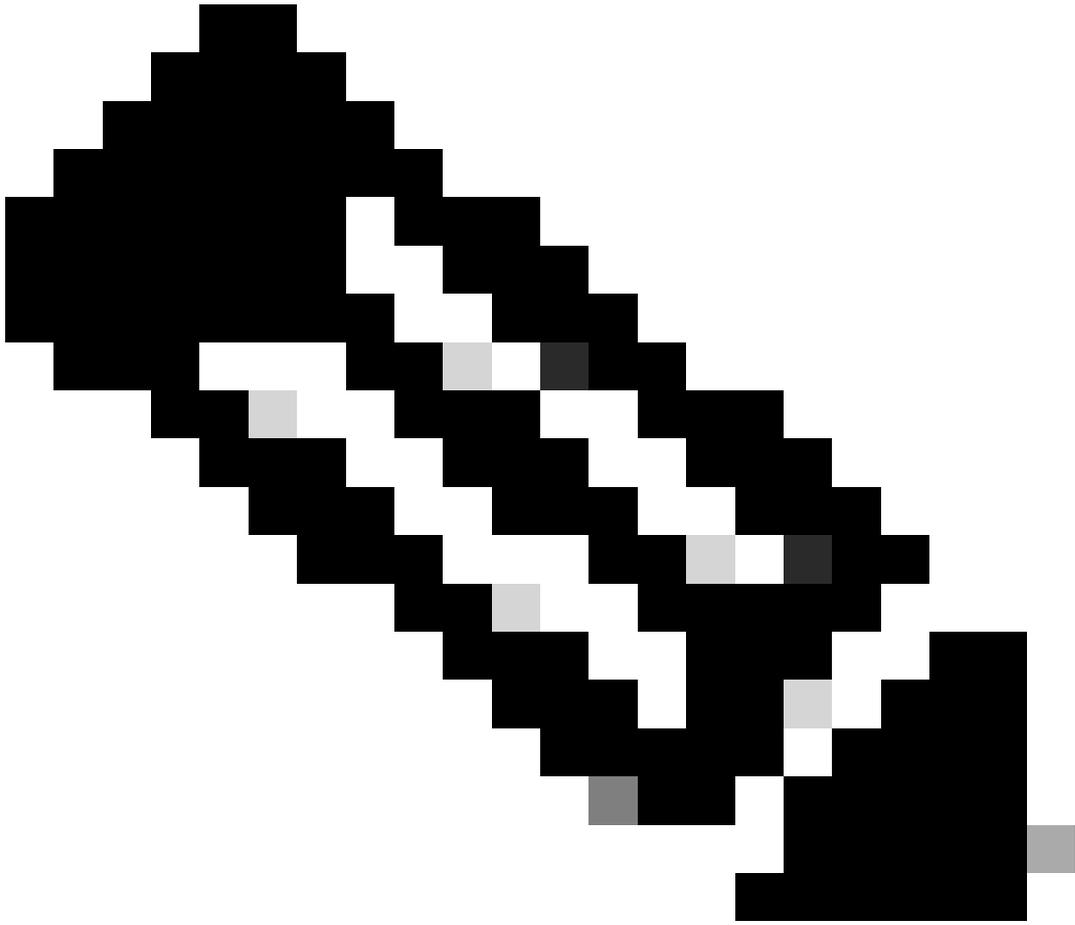
ل ال ة م ي ق ل ال ه ذه خ س ن ا . " ز ي م م ل ل و ص و ل ا ز م ر " ل ع ر ث ع ت ي ت ح ر ي ر م ت ل ا ب مق 6. ة و ط خ ال
ة ر و ص ل ال ي ف ح ص و م وه امك . ت ا ق ي ب ط ت ال ة ج م ر ب ت ا ه ج ا و م ا د خ ت س ا ي ف ا ق ح ال ة ق د ا ص م ل

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



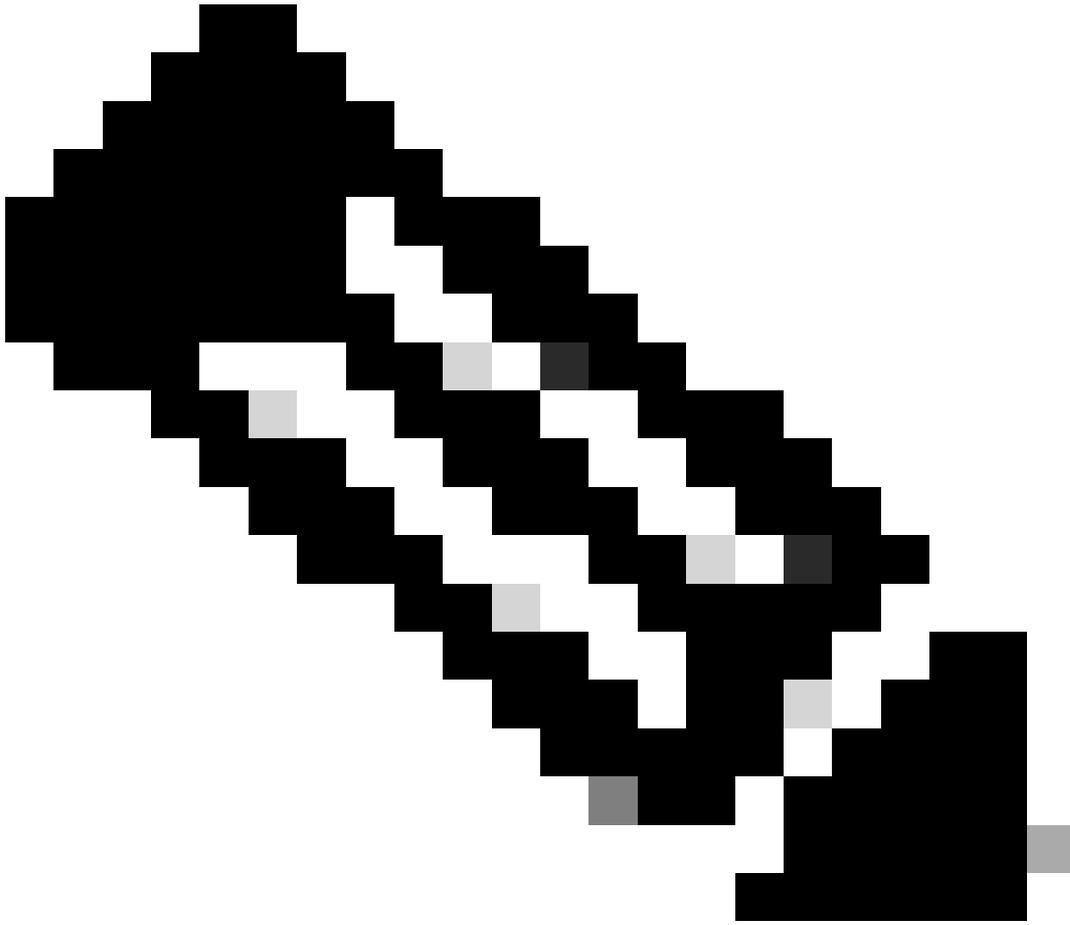
نم ةم و عدم ريغ ةادال هذه .git.bash ان مدخت سا ، دن تس م لا اذه عاش نإ ة بس ن لاب : ة ط ح الم
ةادال هذه م عدب لاصت ال اب ي صوي ، اه ب قل ع تم لاؤس وأ ك ش ي ، Cisco ل بق

م ادخت سا حيتت ةادأ م ادخت سا كن كم ي ، زي م الم ة ق د اص م لا زم ر ي ل ع ل و ص ح ل ا در ج م ب . 7 ة و ط خ ل ا
ت ا ق ي ب ط ت ل ا ة ج م ر ب ت ا ه ج ا و



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

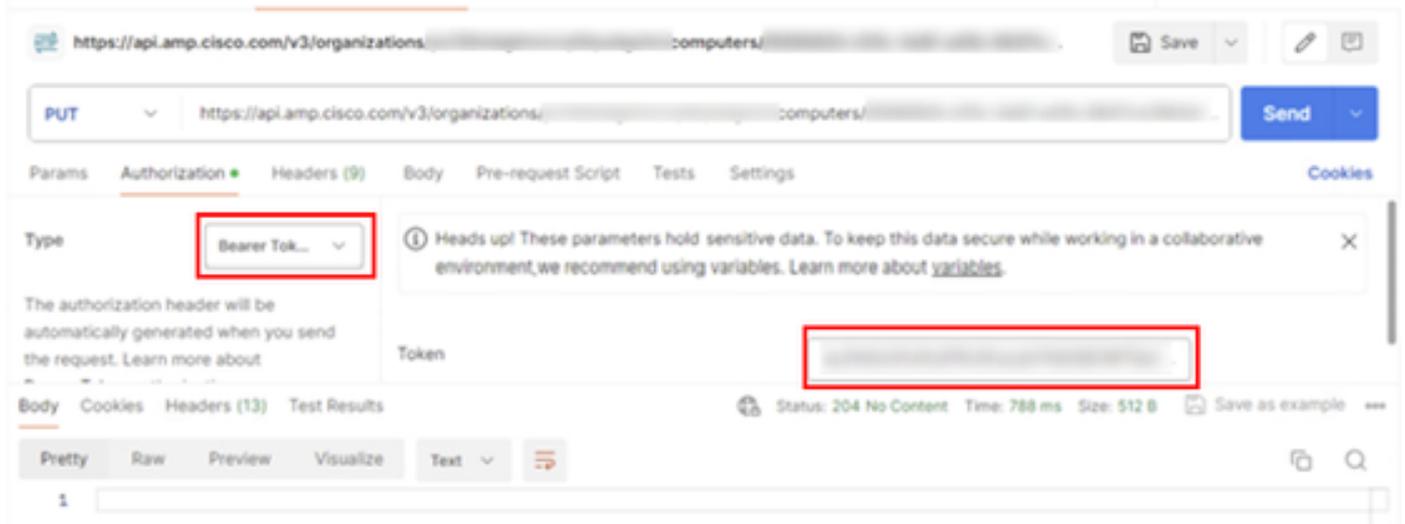
([لصوم تيبتت ةلازا بلط](#)) تاقيبتتال ةجمر ب ةهجاو عجرم ةغايص ل ا ادانتسا 8 ةوطخال هتبتت ةلازا دارم لا زا جلاب صاخال GUID م ادختساب لصوم ل تيبتت ةلازا بلط ارجا



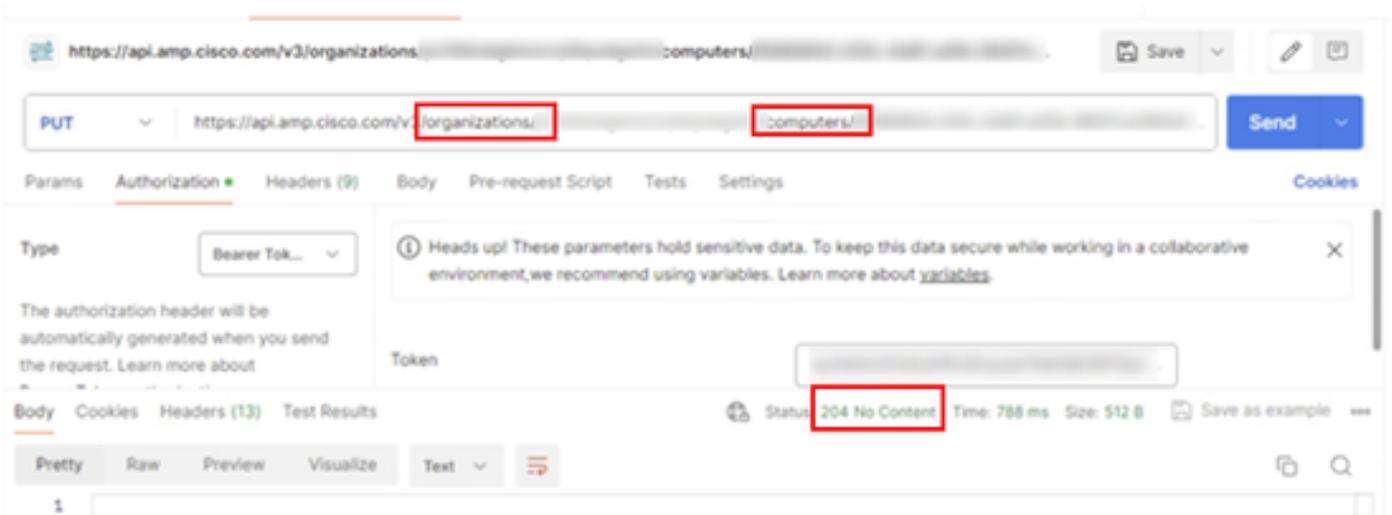
نيتطي سب نيتتقيرطب لوصوم لابس صاخ ال GUID لى لوصح ل كنكمي :ةظحالم

- لى لوصح ل (ةراد ل) Management لى لقتنا ةنمآ لة ياهن لة طقن ة باوب لى ل > لى صافات ل ضرع > بولطم ل رتوي بكم ل لى لقتنا > (رتوي بكم ل ةزهج) (يموم ل ديرف ل فرم ل) GUID لى لوصح ل
- لوصح ل > "تايئاصح ل" بيوبت لة مال لى لقتنا > قرولا ة بل لة نوق ي أحتفا لى ل GUID.

لوصح ل م ت يذ ل زي م ل لوصول زمر لخدأ وة قداصم ة قيرطك زي م ل لوصح ل زمر ددح . 9 ةوطخ ل ةرول ل ي ف حصوم وه امك . 6 ةوطخ ل ي ف اق بس م ه لى ل



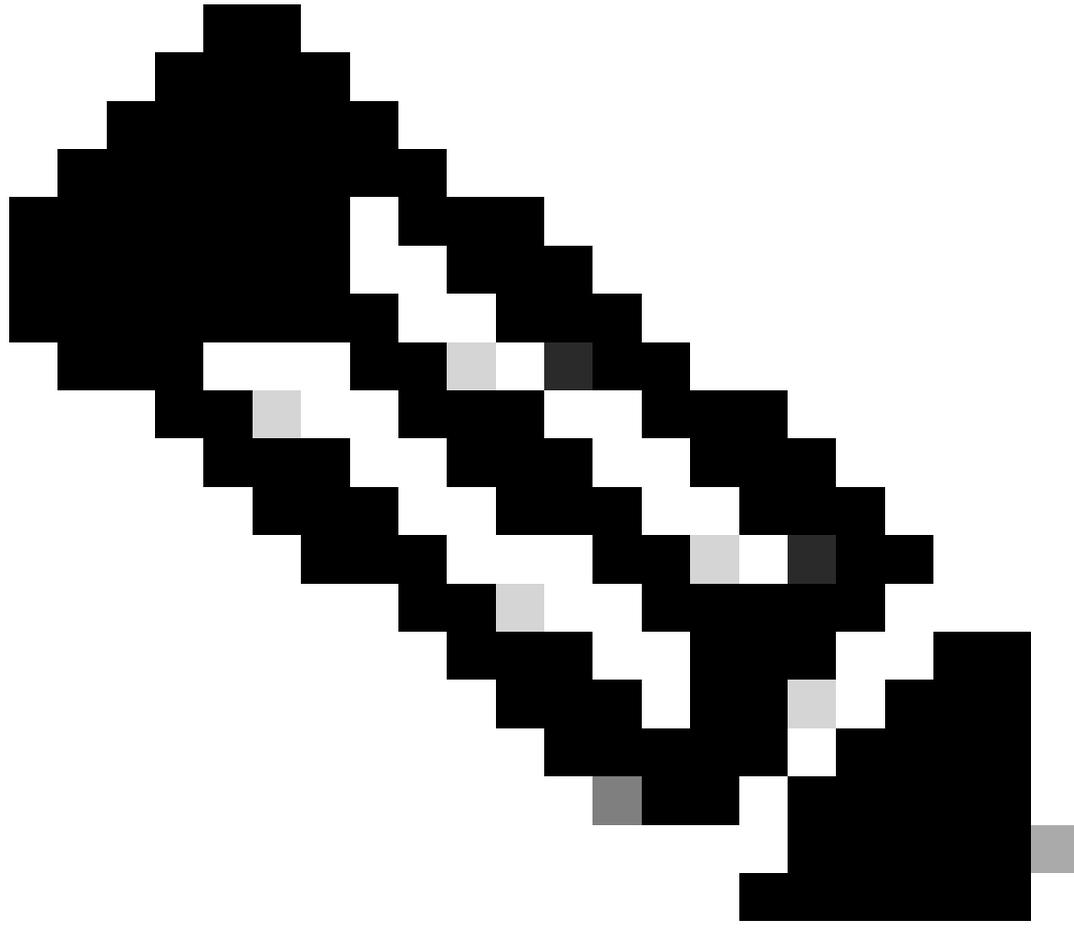
يحتفظ بنا. لاسرنا رز قوف رقن او API اعادتسا نم ةبولطم ل لوقح ل ةئبعتب مق 10 ةوطخل ةروصل يف حضورم وه امك .يوتحمل ل ةباجتسا دجوي ال :204



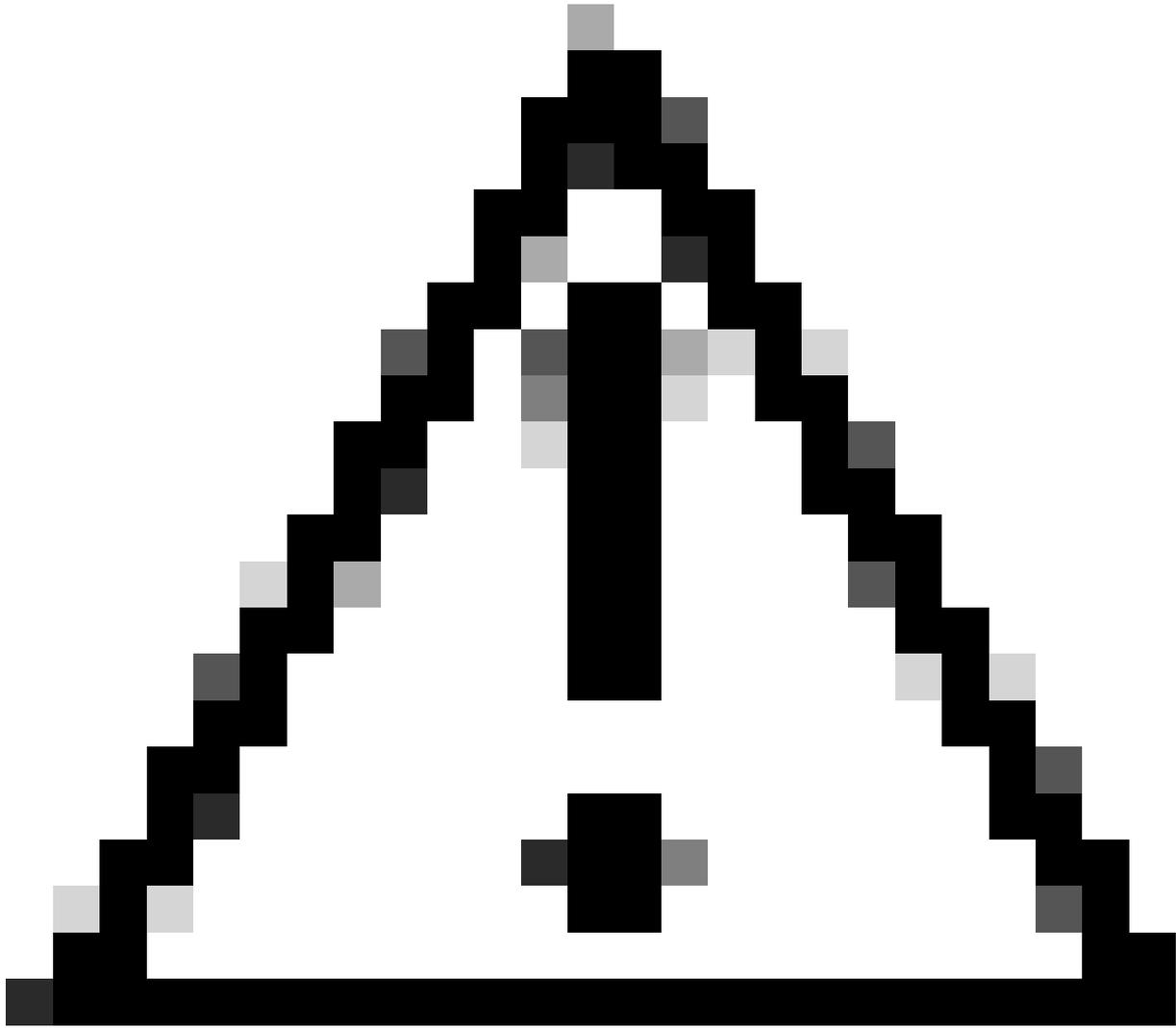
،اي لحم تام ول عمل ةعجارم دع . روف ال على مكحتل ةدحو يف لصوم ل ليحست يف تخيس ، لم اك لاب هتلازا ممتس ، قئاق دعضب دعبو وتيبتل ةلازا حهن الى اتقوم لصوم ل لقتنيس ةروصل يف حضورم وه امك . زاهج نم

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 دختسي يتلا ةي نم زلا ةرت فل نا 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

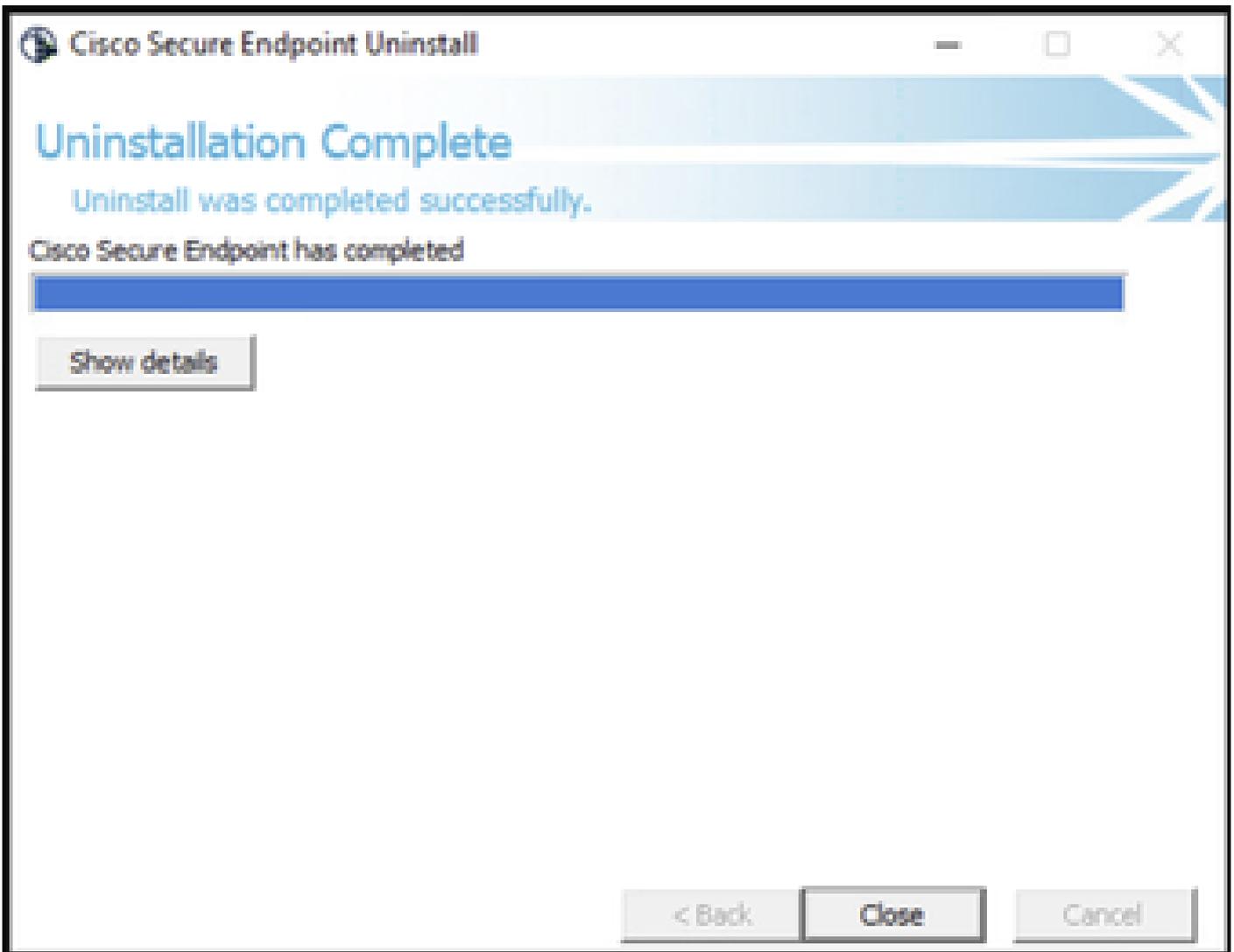
ةروصللا يف حضورم وه امك. تيبتثتلا ةمزح هي ف دجوت يذلا عقوملا يلا لقتنا 2. ةوطخلا

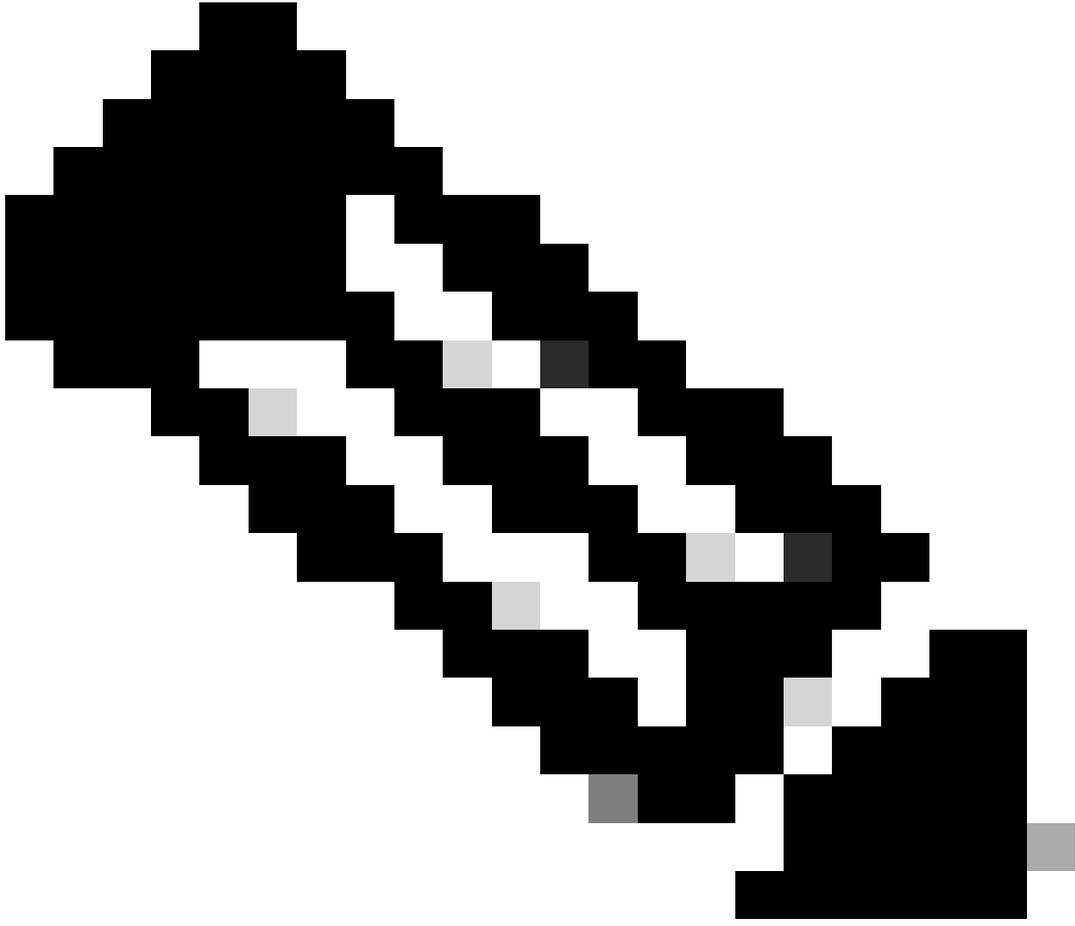
```
C:\Users\Mex-Amp>cd Downloads
```

وه امك . اهذي فننت 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 .

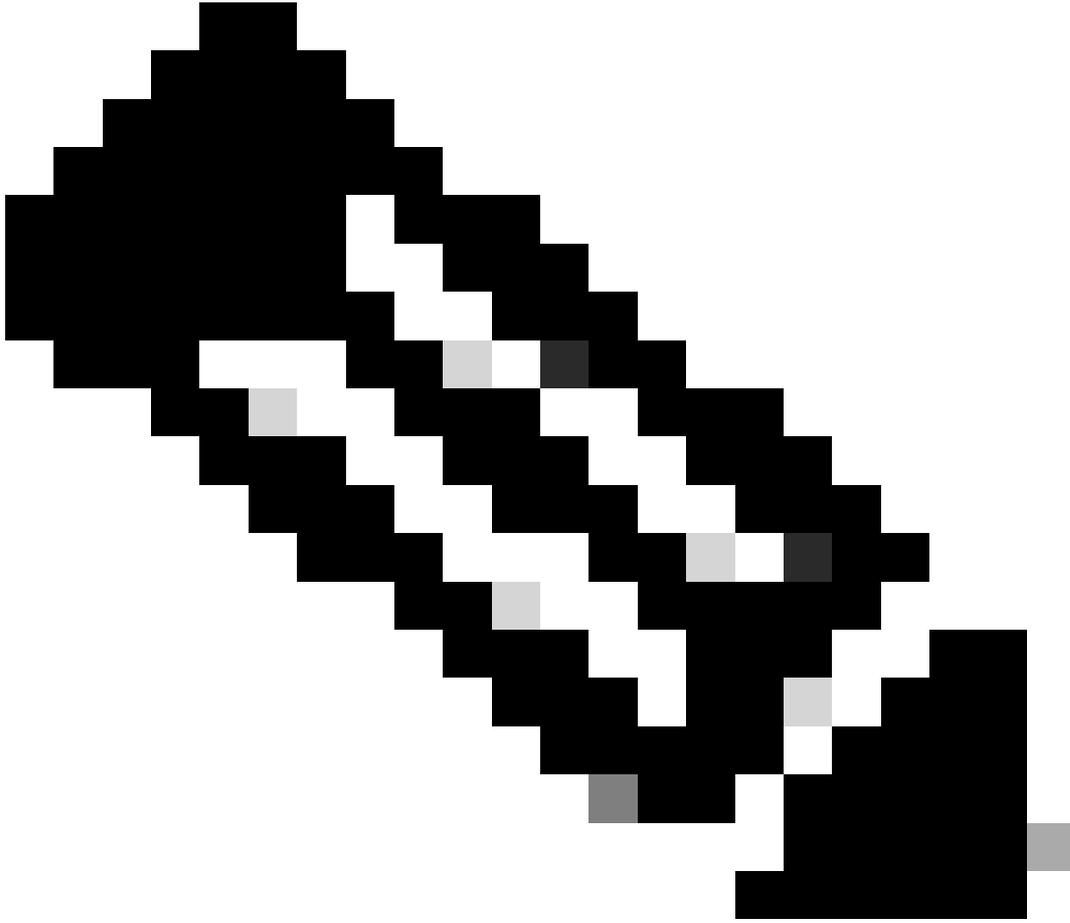




مدعو تي بثلتال ةم زح لباقم تي بثلتال ةلازاب صاخلا لوحملا لي غشت بجي :ةظحالم
exe.تي بثلتال ةلازا

لوحملا نوكي ،لصوملل ةلماك و ةتامص تي بثلتال ةلازا ءارجإل

FireAMPSetup.exe /R /S /remove 1



/s. ل و ح م ل ا ة ل ا ز ا ب ة ت م ا ص ل ا ر ي غ ع ا ض و أ ل ا ي ف ك ل ذ ذ ي ف ن ت ا ض ي أ ك ن ك م ي : ة ط ح ا ل م

ل و ح م ل ا ن و ك ي ، ر و ر م ل ا ة م ل ك ة ي ا م ح ب ع ت م ت ي ل ص و م ل ة ل م ا ك ت ي ب ث ت ا غ ل ا ة ي ل م ع ا ر ج ا ل

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

ل ص و م ل ا ت ي ب ث ت ة ل ا ز ا ب ج ي ي ذ ل ا ز ا ه ج ل ا ي ل ع ت ي ب ث ت ل ا ا غ ل ا ة ا د ا ل ي غ ش ت ن ا ف ، ر ي خ ا ل ح ك و
ة ل ك ش م ل ا ل ح ي س ه ي ل ع

ة ي ر ا د ا ت ا ز ا ي ت م ا ب ر م ا و ا ه ج و م ح ت ف . 1 ة و ط خ ل ا

ر ا د ص ا و ه x ش ي ح . ة ن م أ ل ا ة ي ا ه ن ل ا ة ط ق ن ل ص و م ه ي ف د ج و ي ي ذ ل ا ع ق و م ل ا ي ل ا ل ق ت ن ا . 2 ة و ط خ ل ا
ة ر و و ص ل ا ي ف ح ض و م و ه ا م ك . CSE ل ص و م

C:\Program Files\Cisco\AMP\>

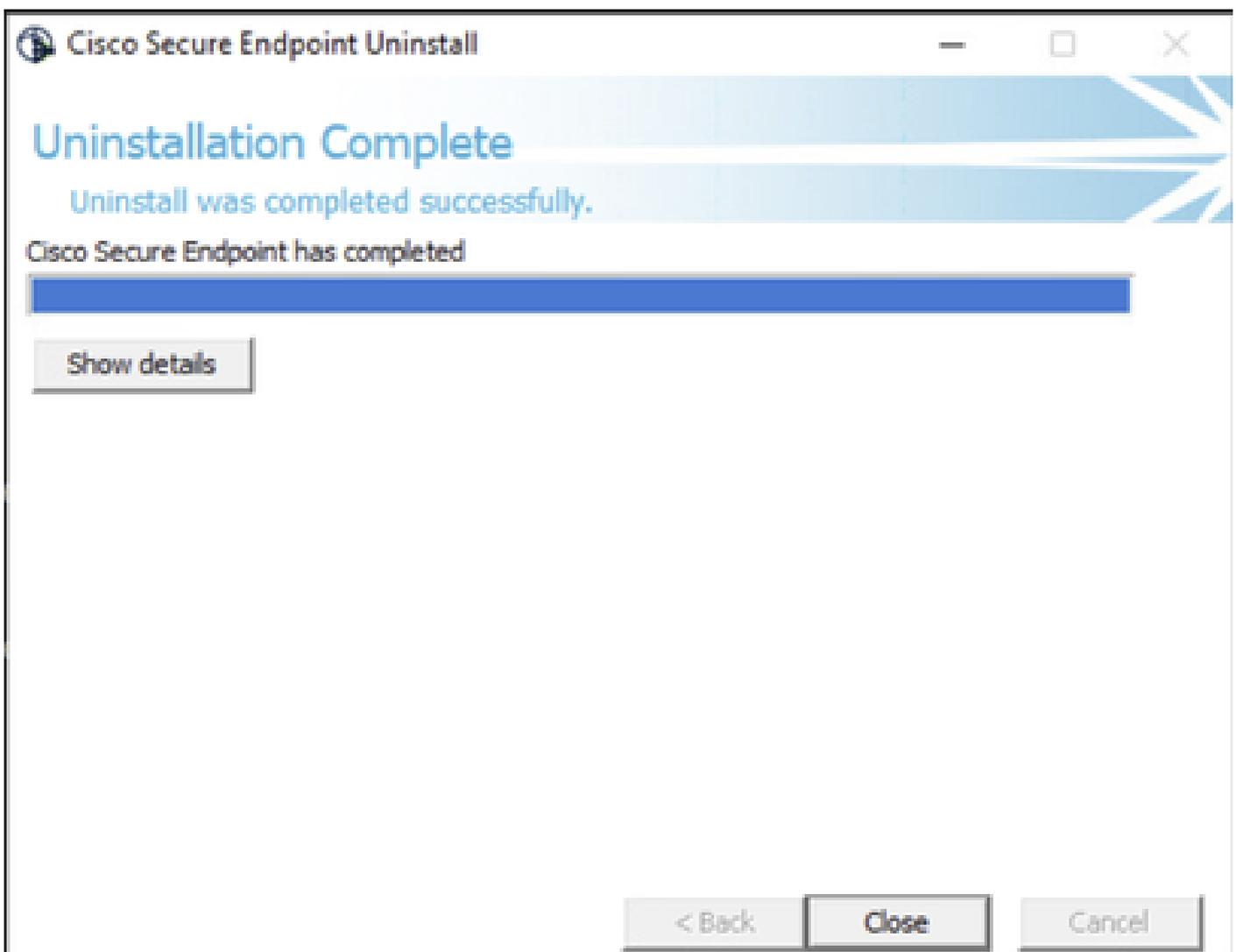
```
C:\Program Files\Cisco\AMP>cd 8.2.3.30119
```

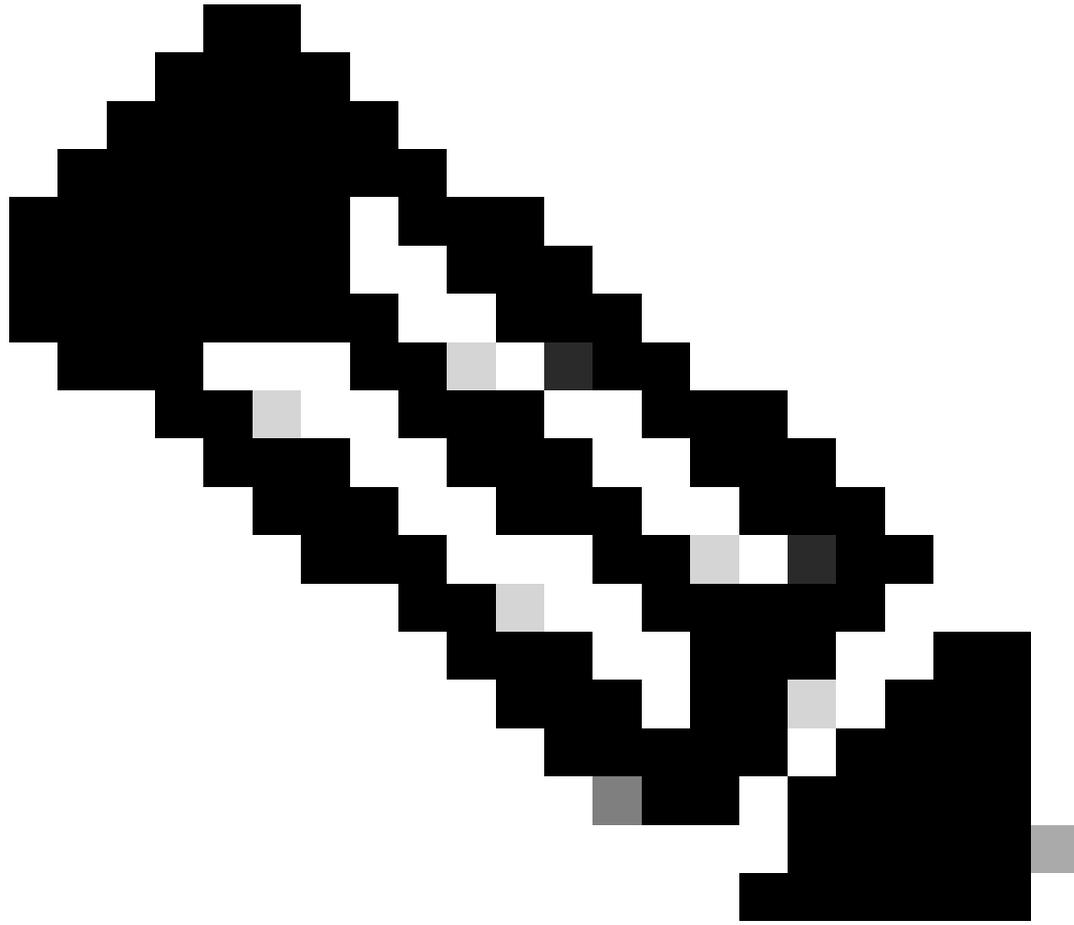
ةروصلال يف حضورم وه امك .ةللاتل تااطيسولل مادختساب فللمل ذيفنتب مق 3. ةوطخلل

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

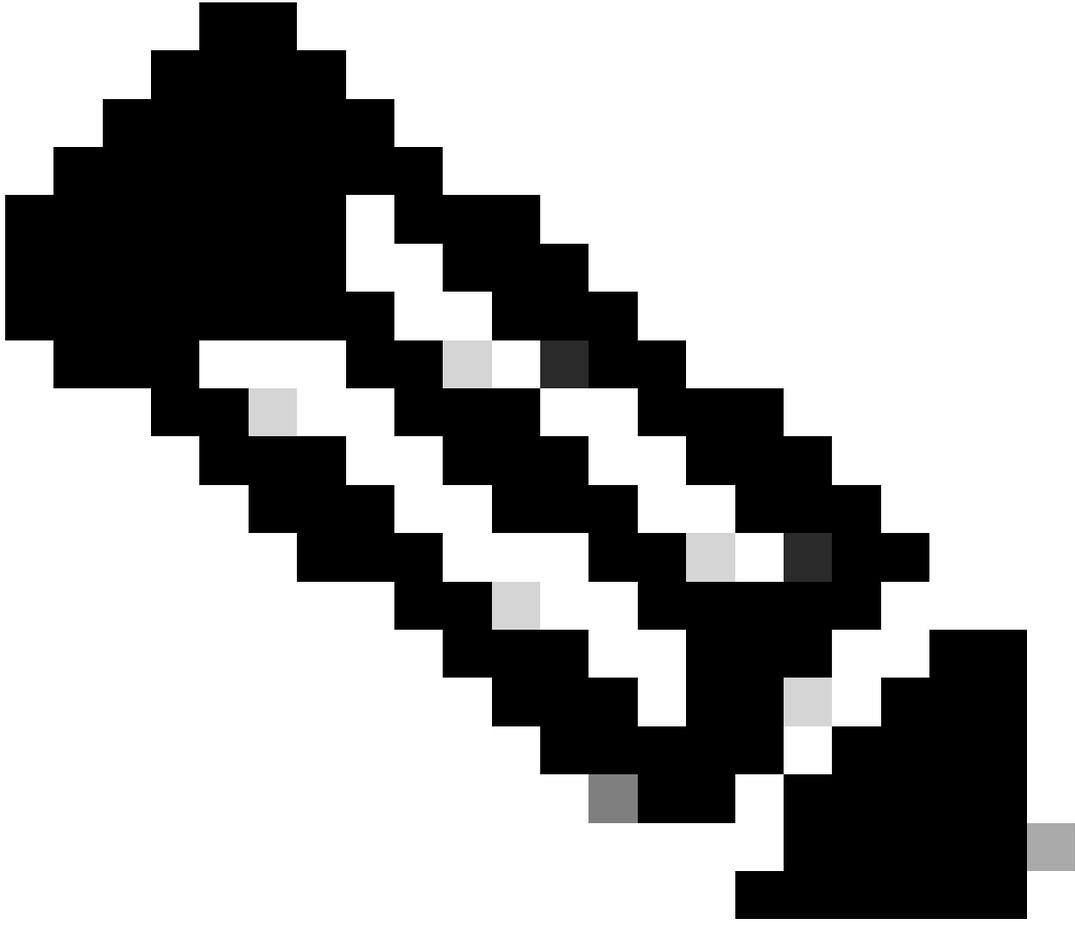
```
C:\Program Files\Cisco\AMP\8.2.3.30119>uninstall.exe/full 1
```

وه امك ".لماكلل تيبتللا ءاغلإ" ةشاش لعل لوصحلل متي يتحل لعمال عبتا 4. ةوطخلل 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 تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا 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 ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا