

حرفش مت Cisco: نم ةنمآلا ةياهنلا ةطقن رم اوآلا رطس تالوحم

تايوتحمل

ةمدقملا

ةيساسأ تامولعم

Cisco نم ةنمآلا ةياهنلا ةطقن رماوآ رطس تالوحم

ةنمآلا ةياهنلا ةطقن تيبثت تالوحم

[amp_installer.exe](#)

ةنمآلا ةياهنلا ةطقن معد صيخش تالوحم

[ipsupportTool.exe](#)

ةنمآلا ةياهنلا ةطقن (UI) مدختسمل ةهجاو تالوحم

[iptraytool.exe](#)

ةياهنلا ةطقن ةنمآلا SFC تالوحم

[sfc.exe](#)

ةلص تاذا تامولعم

ةمدقملا

نم ةنمآلا ةياهن ةطقن عم مادختس لة ةرفوتملا (CLI) رماوآ رطس تالوحم دنتسمل اذه فصي Cisco.

ةيساسأ تامولعم

ةلباقلا تاءارجإ او تازيمل نم ديدعلا لىل Cisco نم ةنمآلا ةياهنلا ةطقن يوتحت رماوآ رطس تالوحم مادختساب ةياهن ةطقن لىل ايلحم اهذيفنت نكمي يتلا صيخش تالوحم. رصانعلا هذه دنتسمل اذه ضرعي.

Cisco نم ةنمآلا ةياهنلا ةطقن رماوآ رطس تالوحم

ةنمآلا ةياهنلا ةطقن تيبثت تالوحم

amp_installer.exe

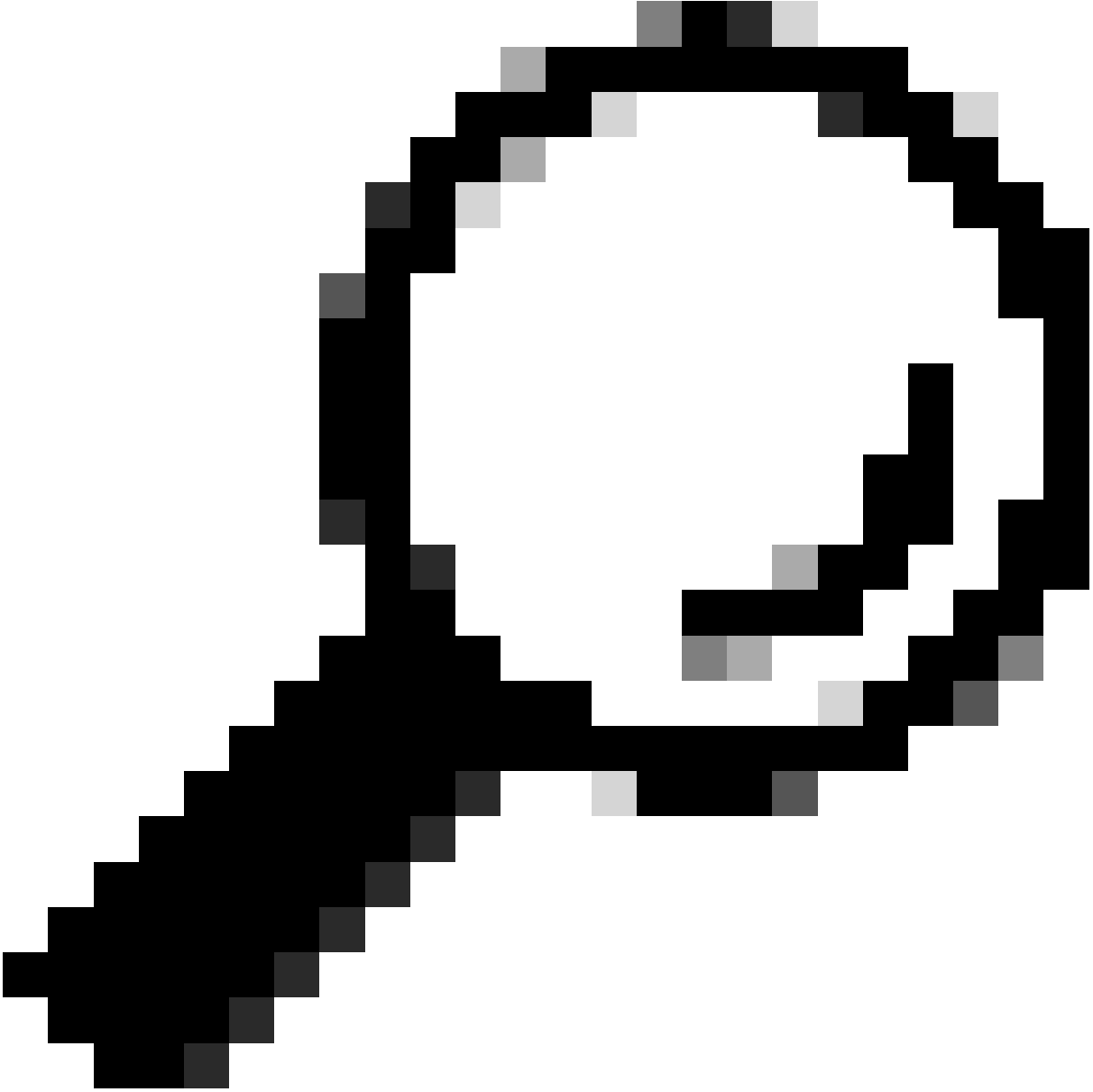
1. Windows لىل رماوآ هجومت فا.

2. تاليزنتلا دلجم) رماوآ هجومي ف كب صاخلا تيبثتملا هب دجوي يذلا دلجملا لىل لقتنا.
(هاندا لاثمك مدختسمل)

cd C:\Users\sysadmin\Downloads

- ةرفوت مل ةرفوت مل تالو ح مل ذيفنت ب مق
amp_protect.exe <switch>

رم اوألا ذيفنت دعب جارخا ي أ عا ج را متي نل : ةظح الم



دحاو تقويف دحاو لو ح م نم رثكأ مادختسا نكمي : حيمك

رطس لي دبت	رمألا فصو	ةصاخ تاظح الم
------------	-----------	---------------

رم اوآل		
/S	مدختسي عضول يفتبتمل عضول تماصل	
/temppath	مدختسي عقوم ديدحتل صصخم تقوم تافلمل تبتتال دارمل اهجارختس اهذيفنتو	/temppath C:\
/desktopTopicon 0	مدختسي مدع ديدحتل قنوقيا عاشن بتكمل حطس	هريفوت مزلي الويضارتفال نيوكتلا وه اذه
/desktopIcon 1	مدختسي عاشن ديدحتل حطس زمر بتكمل	
/startMenu 0	عاشن امتي مل تاراصتخ عدبال عمئاق	
/startMenu 1	عاشن امتي تاراصتخ عدبال عمئاق	هريفوت مزلي الويضارتفال نيوكتلا وه اذه
/contextmenu 0	ليطعت حسمل نال يئوول عمئاق نم يتل قايسل دنع رهظت رزب رقل	

	سواملا نميا	
/contextmenu 1	نيكمت حسمل نآل يئوضلا ةمئاق يف يتلا قايسلا دنع رهظت رزب رقللا سواملا نميا	هريفوت مزلي الو يضارتفال نيوكتلا وه اذه.
/remove 0	تثبت اغلا كرتو لصوللا تافللا ةداعلا تثبتلا اقحالا	مادختسا اءاعاب كل حمست و UUID تاذ XML تافلما يقبت متي. لصوللا تثبت اءاعا دنع يلا لجال رتوي بمكلا نئاك ةيامح رورم ةملك تناك اذا. كذلك لجال تافلما بظافتحالا ةمالعلا مادختساب اهديحت بجيف. مادختساللا ديقلصوللا /uninstallpassword.
/remove 1	تثبت اغلا ةلازا لصوللا تافللا ةفاك ةنرتقلا	بجيف، مادختساللا ديقلصوللا ةيامح رورم ةملك تناك اذا /uninstallpassword. ةمالعلا مادختساب اهديحت
/uninstallpassword	ةملك ديحت ةلازا رورم دنع تثبتلا مادختسا ةمالعلا بجيف. /remove يف ديحتلا نيكمت ةلاح ةيامح "ةزيم لصوللا"	ةمالعلا دعبت تثبتلا ةلازا رورم ةملك دح.
/skipdfc 1	تثبت يطخت جم انرب DFC. ليغشت	ةوومجم يف ةمالعلا هذبة تثبتم تالصولما يا نوكت نا بجي هبة كبشلا كرحم ليطعت مت جهن تاذ.
/skiptetra 1	تثبت يطخت جم انرب	ةوومجم يف ةمالعلا هذبة تثبتم تالصولما يا نوكت نا بجي هل Tetra ةمالع نم ققحتلا متي ال جهن تاذ.

	Tetra. لي غشت	
/d=[راسم]	مدختسي ديحتل يذلا ليلدل ءارج متيس تيتبتل يلع. هيلع لبيس لالم، /d=C:\	ةملم رخأك اذه ديدحت بجي تيتبتل ليلد فلتي، /D= رم أوأل رطس لوحملة بسنلاب تيتبتل ليلد أيل اميف. لي غشتل ماظن نم يضارتفال Service Pack 3 مع Microsoft Windows XP لعل تيدحت رادصا أو: x86 لمع تاصنم C:\Program Files (x86)\Cisco\AMP x64 لمع تاصنم C:\Program Files\Cisco\AMP
/goDenimage 1	لصوم تيتبتل دادعتسالل ةبهدلا روصلل	روصل دادع ي ف ةدعاسم لل ةمالعلا هذه ميمصت مت هذه مادختسا يدوي. ةيضارتفال تائيبلا ي ف ةبهدلا ليجستلاو لي غشتلا ادب نم لوصول عنم ي ل ةمالعلا ي جري، تامولعمل نم ديزم. ةبهدلا ةروصللا ءاشنل ءانثأ يلع عالطال: نم آة ياهن طاقن ب ةبهدلة روص ريضحت ةيفيك https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html
/skiposcheck 1	صحف زواجتي لي غشتل ماظن تيتبتل ءانثأ	"نم آة ياهن ةطقن" تيتبتل ةمالعلا هذه مادختسا نكمي اهم ةقفاوتمل ريغ لي غشتل ةمظنا يلع

نم آل ة ياهن ل ةطقن معد صيخشت ةادأ تالدم


ipsupportTool.exe

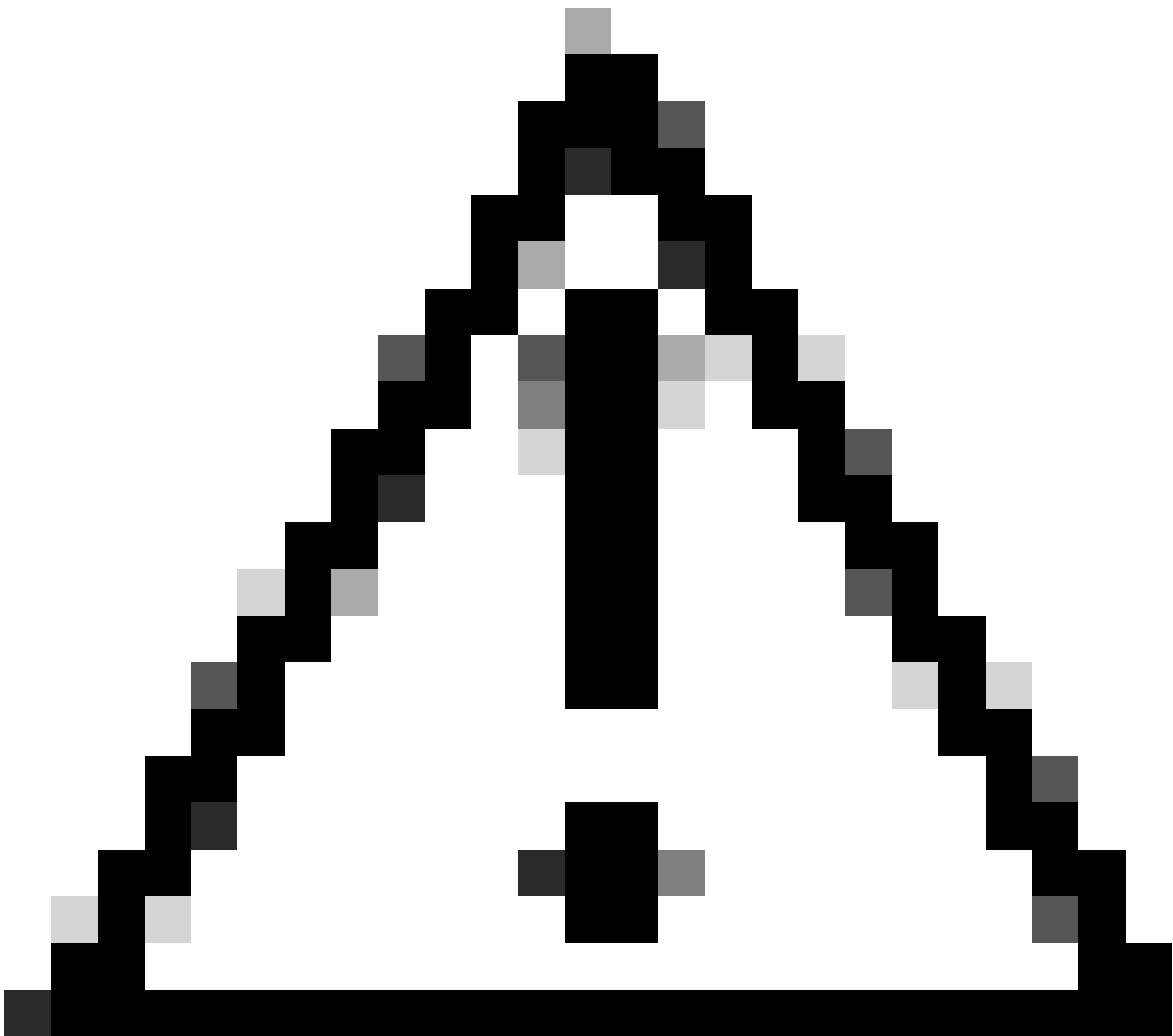
- Windows. لعل رم أوأل هجومت فا
- مقرر ي ل X.X.X ريشي، C:\Program Files\Cisco\AMP\X.X.X\ :يضارتفال راسملا. رم أوأل هجوم ي ف دلجملا ي ل لقتنا

(رادصإلإ).

cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- ةرفوتملا ةرفوتملا تالوحملا ذيفنتب مق
ipsupporttool.exe <switch>

 تاجرخم يآ عاجرا متي نل ،تالوحملا ذيفنت دنع :ةظحالم

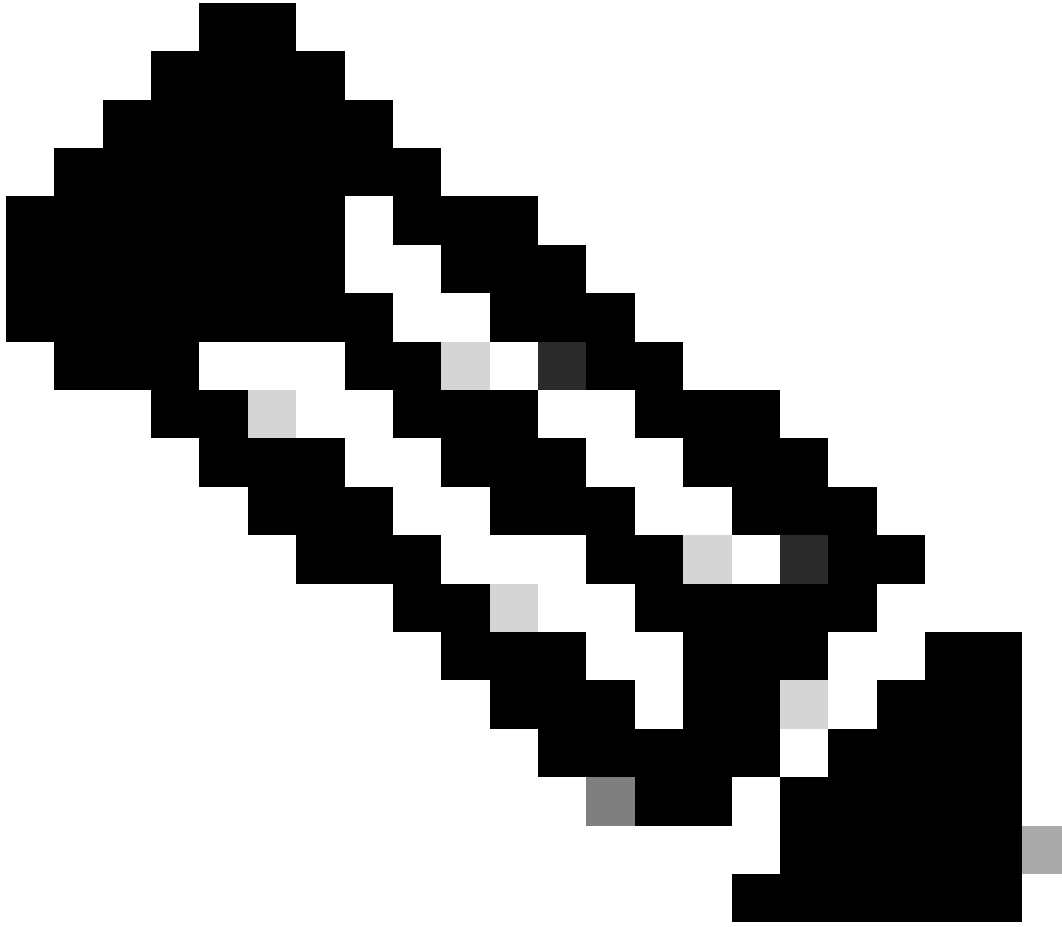


لعللاب ةدوجوم تادلجملا نوكت نأ دلجم رايخا ىلا ريشي لوحم يآ بلطاتي :ريذحت

رطس ليدبت رم أوألا	رمألا فصول	ةصاخ تاظحال
<راسملا> -o	ةأدألا تاخرملا دلجم ددحي معدلا	ةلأحي فبتكملا حطسل ةيضارتفالا تاادعإلا رايخلا اذه ديدحت مدع
-d <install_path>	يذلا دلجملا ديدحت معد ةأدألا نكمي دادرتسإ Windows هنم تاफलلا	تيبثتلا ليلدل ةيضارتفالا تاادعإلا متميل اذإ ةنمألا ةياهنلا ةطقنل يضارتفالا اهديدحت
<ةقيقد> -t	صخش ليدشت حيحصت يوتسم تيقوتلا بسح ءاخالألا "Windows" معد ةأدألا متميل .ددحمل تقولل ةينمزالا ةدملا ديدحت قئاق دلألا	

ةنمألا ةياهنلا ةطقنل (UI) مدختسملا ةهجاو تالوحم

iptraytool.exe



ةنمآلا ةياهنلا ةطقن نم ةميدقلا تارادصإلا ىلع طقف iptraytool.exe فلم رفوتي :ةظالم

-
- Windows ىلع رماوأل هجوم حتفا
 - مقر ىلإ X.X.X ري شي ، C:\Program Files\Cisco\AMP\X.X.x\ :يضارتفالا راسملا .رماوأل هجوم يف دلجملا ىلإ لقتنا (رادصإلا)
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
ةرفوتملا ةرفوتملا تالوجملا ذي فننتب مق
iptray.exe <switch>

رم أو أال رطس ليدبت	رم أو أال فصول	ةصاخ تاظحالم
-و	مدختسم ةهجاول حامسلا نوكت نأب ليمعلا. رم أو أال رطس نم ةطاشن	ةهجاو ليغشت فاقيا مت اذا اإا ايوررض اذه نوكي ال ربع ةياهنلا ةطقنل (GUI) ةيموسرلا مدختسملا. عدبلا ليمع مدختسم ةهجاو ديدحت مدع عم جهنلا.

ةياهنلا ةطقنل ةنم آل SFC تالدم

sfc.exe

- Windows لىع رم أو أال هجوم حتفا
- مقرر لى X.X.X ريشي، C:\Program Files\Cisco\AMP\X.X.x\ :يضارتفالا راسملا. رم أو أال هجوم يف دلجملا لىا لقتنا (رادصلا).
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- ةرفوتملا ةرفوتملا تالوحملا ذيفنت
sfc.exe <switch>

رم أو أال رطس ليدبت	رم أو أال فصول	ةصاخ تاظحالم
-s	زاهجلا ةيامح" ةمدخ عدب (Windows لصوم) "يعانملا مت دق ةمدخل نوكت نأ بجي SCM عم لعفلاب اهليجست اهليغشت عدبل.	
-k	زاهجلا ةيامح" ةمدخ فاقيا (Windows لصوم) "يعانملا	رورملا ةملك لخدأف، لصوملا ةيامح نيكم مت اذا حاجنب ةمدخل فاقيا ل -k دعب.
-u	ةيامح" ةمدخ تيبتت ةلازا (Windows لصوم) "يعانملا زاهجلا (Windows) ءاغل ةمدخ. ةرادا مادختساب ليجستلا Windows ل ةمدخل يف مكحتلا اذه مادختسا متي (SCM). ءاغل ةادأ لبق نم راخلا ةمدخ تيبتت ةلازال تيبتتلا Windows لصوم.	

-ر	<p>زاهجلا ةيامح ةمدخ طبض ةداعإ (Windows Connector) يغانملا ال نأ ريغ راخي i- ادج لثامم اذه نأ ديفم اذه. ةمدخلل بكري داسف xml.ي لحم تبتثي</p>	
-ا ةيادب	<p>ءاطخألا ليحست لي دبت يكييمانيد لكشب ةاونلاو (ريغص L فرح وه لغشملا)</p>	<p>ةداعإ وأ ليغشتلا فاقبي متي يتح ةلجال هذه لظت ريغتل ةديج ةسايس نيوكت وأ ةمدخلل ليغشت ليحستلا يوتسم</p>
-ا فاقبي ا	<p>ليحست ليغشت فاقبي اب مق لكشب kernel و Debug L وه لغشملا) يكييمانيد (ضفخنم)</p>	
-ا SHA_of_file رطح ءاغلا	<p>ءاغلل اب راخلا اذه موقبي نم ةيلمع رطح ليغشت دعب. ذيفنتلا نكمي، اذه رماوالا لوجم ةركاذ نم قبيبطتلا ةلازا تقوملا نيزختلا ةمئاقل kernel ل ةيحلحلا تاقبيبطتلا رطح</p>	<p>ببسب قبيبطت رطح دنع رمألا اذه مادختسا نكمي رطح ءاغلل ديرتو، ةئطاخ ةباجي ةجيتن وأ أطخ وأ ةقيد 30 ةدمل راطتال نود ةعرسب قبيبطتلا زاهجلا ليغشت ةداعإ</p>
-ا ليحستلا ةداعإ	<p>راخلا اذه موقبي نأ نكمي مدختسملا فرعم حسمب local.xml نم ةعباتلاو ءانثأ ليحستلاو موقبي و، ةمدخلل ليغشت ةداعإ ليغشتب شيحت مت. ليحستلا يحلحلا xml و لجلسلا ،كلذ عم و. ةديج ميقيب مت اذا اذه رطح متي ،فرعملا ةنمازم نيكمت ةداعإ لوصوملا موقبي و دوجوملا UUID مادختسا يلا اذه يدؤي نأ نكمي يف لوصوملا عضو جهنلا / ةعومجملا ةداعإ دعبي ضارثالا لي دعت مت اذا ليحستلا تبتثتلا ةمزح تبتثتلا لمدختسملا يلاوالا</p>	<p>ام لاخدا كمزلي، لوصوملا ةيامح نيكمت ةلاح ي يلي: sfc.exe -reregister _password_</p>
-ا شحبلا خيرات	<p>يلع راخلا اذه ضرفي</p>	

	ثي دحت ل صوم ل TETRA ت افيرت	
-Forceapdeupdate	يلع راي خ ل اذه ضر في ثي دحت ل صوم ل ةي امحل ت افيرت ةي كولس ل	ةي كولس ل اةي امحل ت افيرت نم ققحت ل كنكمي راسم ي ف اةي ان ل اةطقن يلع ةت ب ث م ل اةيل ل ةن م آ ل اةي ان ل اةطقن تامول عم ةحول ي ف زاه ل

ةلص تاذ تامول عم

- [Cisco Systems - تادن ت س م ل ا و ين ق ت ل ا م عد ل ا](#)
- [Cisco - TechNotes نم ةن م آ ل اةي ان ل اةطقن](#)
- [مدخت س م ل ا ل ل د - Cisco نم ةن م آ ل اةي ان ل اةطقن](#)
- [Mac/Linux ةن م آ ل اةي ان ل اةطقن ب ةص ا خ ل ا \(CLI\) ر م ا و ا ل ا ر ط س ةه ج ا و م اد خ ت س ا](#)

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 معد 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 ة مچرت ل ض ف ا ن ا 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 (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا