

يتم الآن إعداد طقن إاطخاً فاشكتساً دادرتس الابل ساساً مادختساب لزعل في تقلع إحالصلو

تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[لزعل فاقيا](#)

[مكحتل دحو نم لزعل لمع ةسلج فاقيا](#)

[رماوأل رطس نم لزعل ةسلج فاقيا](#)

[إحالصلو دادرتس الابل ساساً فاشكتساً](#)

[رماوأل رطس نم لزعل بولسأ ةداعتسا](#)

[رماوأل رطس نودب لزعل بولسأ ةداعتسا](#)

[ةحصلل نم ققحتل](#)

[ةلص تاذ تامولعم](#)

عمدقمل

نم ةنمأل ةياهنل ةطقن لصوصم تيبتت عم ةياهن ةطقن دادرتسإ ةيلمع دنتسمل اذه فصوي
لزعل عضو.

ةيساسأل تابلطتمل

تابلطتمل

ةيلال عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوصت:

- Secure Endpoint Connector
- ةنمأل ةياهنل ةطقن في مكحتل دحو
- ةياهنل ةطقن لزعة زييم

عمدختسمل تانوكمل

ةيلال ةيدامل تانوكمل او جماربل تارادصل إلى دنتسمل اذه في ةدراول تامولعم دنتست:

- Secure Endpoint Console، رادصلإال v5.4.2021092321
- Secure Endpoint Connector، رادصلإال v7.4.5.20701

ةصاخ ةيلمعم ةئيبي في ةدوومل ةزهجال نم دنتسمل اذه في ةدراول تامولعمل عاشنإ مت
تنالك إذا. (يضاوتفا) حوسمم نيوكتب دنتسمل اذه في عمدختسمل ةزهجال عيجم تادب

رماً يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق كتكبش

ةيساسأ تامولعم

ةطقن زاهج اهيف نوكي يتلا تالاحل يف اديفم دنتسمل اذه يف حضورملا ءارجإل نوكي لزلعل عضو لي طعت نكمي الو ةلاحل هذه يف اقلع ةياهنلا

رتويبمك ىلع (IN و OUT) ةكبشل طاشن رطح كل حيتت ةزيم يه ةياهنلا ةطقن لزلعل رفوتم وهو .ةراضل جماربل رشنو تانايبلا ةيفصت لثم تاديدهتلا عنمل Windows لصلومل نم ثدحال تارادصل او 7.0.5 رادصلال معدت يتل Windows نم تب 64 تارادصل

كانه Cisco ةباحسو Windows لصلوم نيبل لاصلتال ىلع ةياهنلا ةطقن لزلعل تاسلج رثؤت ال لبق ناك امك كب ةصاخل ةياهنلا طاقن ىلع ةيؤرلا ةينامك او ةيامحل ىوتسم سفن رطح لصلومل مايق بنجتل نيوانعل لل IP لزلعل جامسلل مئوق نيوكت كنكمي .ةسلجل ةعجارم كنكمي .ةطشنل ةياهنلا ةطقن لزلعل ةسلج طيشنت ءانثأ ةينعمل IP نيوانع [انه](#) "ةياهنلا ةطقن لزلعل" ةزيم لوح اليفصت رثكأ تامولعم

لزلعل فاقيل

تاوطلخل هذه عابتا كنكمي ،ام رتويبمك ىلع ةياهنلا ةطقن لزلعل فاقيل يف بغرت نأ درجب رماوأل رطس وأ ةنمأل ةياهنلا ةطقن مكحت ةدحو لالخل نم ةعيرسل

مكحتل ةدحو نم لزلعل لمع ةسلج فاقيل

ةياهن ةطقن ىل ةكبشل رورم ةكرح لك ةداعتساو لزلعل ةسلج فاقيل

رتويبمكل ةزهج > ةرادال ىل لقتنا ،مكحتل ةدحو يف 1. ةوطلخل لىصافتل ضرعل رقناو هلزلعل فاقيل ديرت يذل رتويبمكل ل ناكم ددح 2. ةوطلخل ةروصلل يف حضورم وه امك ،لزلعل فاقيل رزرقنا 3. ةوطلخل

DESKTOP-075I5MB in group testing bremarqu		Definitions Up To Date	
Hostname	DESKTOP-075I5MB	Group	testing bremarqu
Operating System	Windows 10 Pro	Policy	Copy of bremarqu_mssp
Connector Version	7.4.5.20701	Internal IP	[Redacted]
Install Date	2021-09-28 20:02:16 CDT	External IP	[Redacted]
Connector GUID	[Redacted]	Last Seen	2021-09-28 23:39:08 CDT
Definition Version	TETRA 64 bit (daily version: 85768)	Definitions Last Updated	2021-09-28 21:28:59 CDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	[Redacted]		

Events Device Trajectory Diagnostics View Changes

Stop Isolation Scan... Diagnose... Move to Group... Delete

ةياهنلا ةطقن ىلع لزلعل ةزيم فاقيل ببس لوح تاقيلعت ةيأ لخدأ 4. ةوطلخل

رماوأل رطس نم لزلعل ةسلج فاقيل

نم لزعل لمع ةسلج فاقيا نع زجعتو Cisco، ةباحسب اهلصتا ةلوزعم ةياهن ةطقن تدقف اذا unlock ل عم طخ رمأل نم ايلحم ةسلجل تفقوا عيطتسي تنأ، تالاحل هذه يف .مكحتلا ةدحو زمز.

رتويبمكلا ةزهج > ةرادال لىل لقتنا، مكحتلا ةدحو يف 1. ةوطخل

ليصافتلا ضرعل رقل او هلزع فاقيا ديرت يذلا رتويبمكلا ناكم دح 2. ةوطخل

ةروصلال يف حضورم وه امك، زمرلا نيئات كف ظحال 3. ةوطخل

DESKTOP-075I5MB in group testing bremarqu Definitions Up To Date

Isolated 2021-09-28 21:33:48 CDT Isolated for less than a minute Unlock Code:fwq8qw

Isolated	2021-09-28 21:33:48 CDT		
Isolating...	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw

لجس > باسحلا لىل لقتنلاب تمق اذا زمرلا لفق كف لىل روثعلا اضيا كنكمي 4. ةوطخل
ةروصلال يف حضورم وه امك، قيقدتلا

Isolation Started DESKTOP-075I5MB bremarqu+...@cisc... 2021-09-28 21:33:48 CDT

Isolation Start Requested DESKTOP-075I5MB 2021-09-28 21:33:46 CDT

Attribute	Old	New
Comment	None	None
ID	None	07200270-0000-4014-0000-240001000000
Unlock Code	None	fwq8qw

لوؤسمل تازايتما ب رم او هجوم حتفا، لوزعملا رتويبمكلا لىل 5. ةوطخل

هيف لصولملا تيبتت مت يذلا ليلدل لىل لقتنا 6. ةوطخل
(C:\Program Files\Cisco\AMP\ [مقو (رادصال مقو) sfc.exe -n [زمرلا نيئات اغل]]
ةروصلال يف حضورم وه امك

```
sfc.exe -n [unlock code]
```

```
C:\Program Files\Cisco\AMP\7.4.5.20701>sfc.exe -n fwq8qw
C:\Program Files\Cisco\AMP\7.4.5.20701>
```

راظنتال يرورصلال نم ف، تارم 5 حيحص ريغ لكشب نيئاتل اغل لىل زمز لاخذ مت اذا: ريذحت
ىرخأ نيئات اغل ةلواحم ارجل لبق ةقيقد 30 ةدمل

اهحالص او دادرتسال اعاطخأ فاشكتسا

نم ةلوزعم ةياهن ةطقن دادرتسا لىل رداق ريغ لازت الو تاراسملا ةفاك دافنتسا ةلاح يف
دادرتسا كنكمي؛ نيئاتل اغل لىل زمز مادختساب ايلحم وا ةنمألا ةياهنلا ةطقن مكحت ةدحو

ئراوطلال دادرتسا بېلاسأ مادختساب ةلوزعملال ةياهنلال ةطقن.

رم اوأال رطس نم لزعلال بولسا ةداعتسا

نكمي الو لزعلال في اقلع كب صاخلا ةياهنلال ةطقن زاه اهيف نوكي يتلالتالاحلا في كنكمي، نيمألالا غلإ زمر مادختساب وأ ةنمألالا ةياهنلال ةطقن مكحت ةدحو ربع لزعلال لي طعت تاوطلخال هذه عابتا.

Windows تامدخ وأ لصومال مادختسم ةهجاو ربع Connector ةمدخ فاقيا ب مق 1. ةوطلخال

ةمدخال فقو وأ ةنمألالا ةياهنلال ةطقن لصوم ةمدخ عقوم ددح 2. ةوطلخال

لوؤسمل تازايتما ب رماو هجوم حتفا، لوزعملال رتوي ب مكال لىلع 3. ةوطلخال

ةوطلخال 4. `reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f` رمالا لي غشت ب مق ةوطلخال ةروصلال في حضورم وه امك.

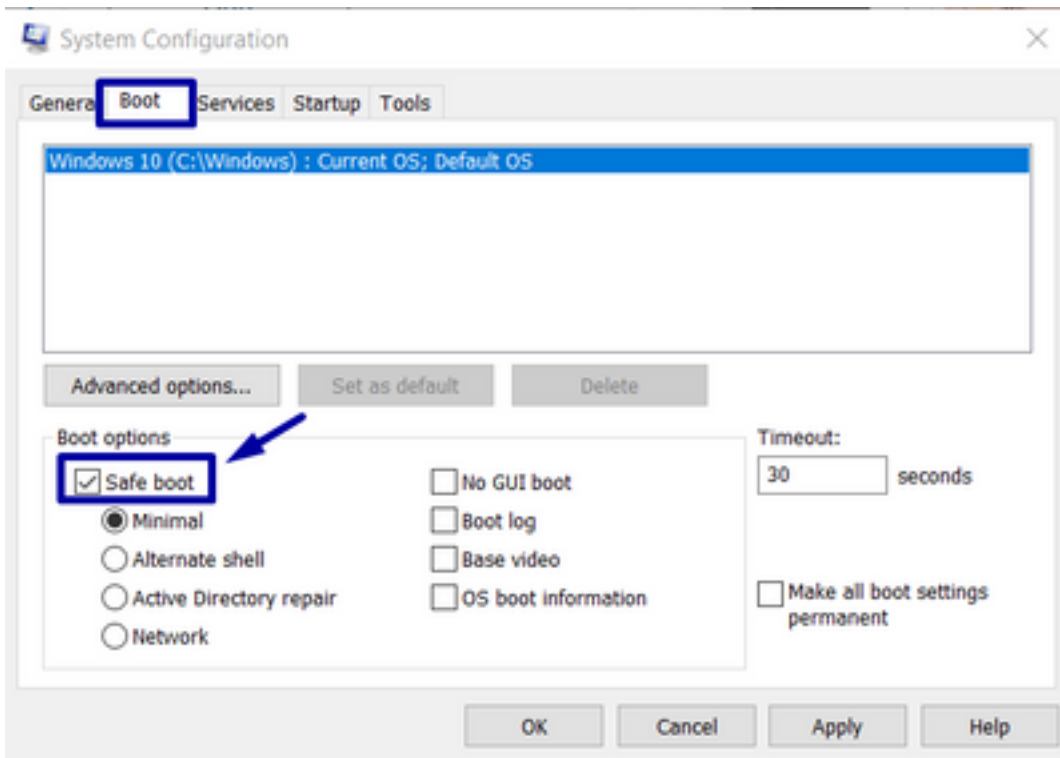
```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
The operation completed successfully.
C:\Windows\system32>
```

ضرع مت اذا). ةي لمعلال لامتكال لىل حاجن ب ةي لمعلال تلمتكال يتلالتالاسرللا ريشت 5. ةوطلخال لبق ةنمألالا ةياهنلال ةطقن لصوم ةمدخ فاقيا ب جي، "لوصولال صفر مت: أطخ" ك، رخأ ةلاسرر (رمالا لي غشت).

ةنمألالا ةياهنلال ةطقن لصوم ةمدخ لي غشت ادب 6. ةوطلخال

مدختسمال ةهجاو نم ةنمألالا ةياهنلال ةطقن لصوم ةمدخ فاقيا ب لي لع رذعت اذا: **حي ملت** نم أ دي همت عارجا كنكمي في Windows تامدخ وأ لصوملل

ددحو دي همتل تاراخي > لي محت > ماظنلالي نوكت لىل لقتنا، ةلوزعملال ةياهنلال ةطقن لىلع ةروصلال في حضورم وه امك، نيمألالا دي همتل

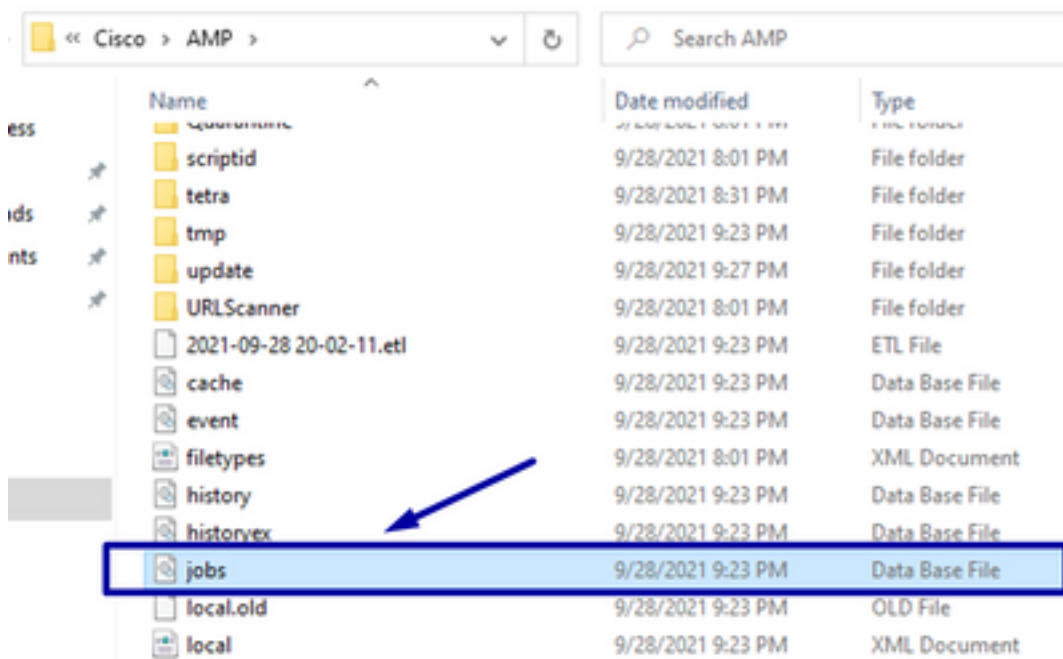


رم اوآل رطس نودب لزعل بولسأ ةداعتسا

ةطقن مكحت ةدحو ربع لزعل ليطعت رذعتي و لزعل ي ةياهنلا ةطقن زاهج فوقت ةلاح ي رم اوآل رطس مادختسا كي لع رذعت اذا يتح و اني ماتلا اغال زمر مادختساب و انمآلا ةياهنلا ةيالات تاوطخل اعابتا كنكمي:

1. ةوطخل Windows تامدخ و لصومال مدختسم ةهجاو ربع Connector ةمدخ فاقيا ب مق 1. ةوطخل

2. ةوطخل (C:\Program Files\Cisco\AMP\) هي ف لصومال تيبتت مت يذلا لي لدلا يلى لقتنا 2. ةوطخل ةروصل ي ف حضوره وه امك ،db. فللمل فئاظو فذخاو



3. رتوي بمكلا ليغشت ةداعيا ب مق 3.

ليصافات يلى لاقتنالا كنكمي ف ،مكحتلا ةدحو ي ف لزعل ثدح تيأ اذا ،كلذ يلى ةفاضلا ب

ةروصلال يف حضورم وه امك ،هفصوو أطخلال زمر ةعجارمل أطخلال

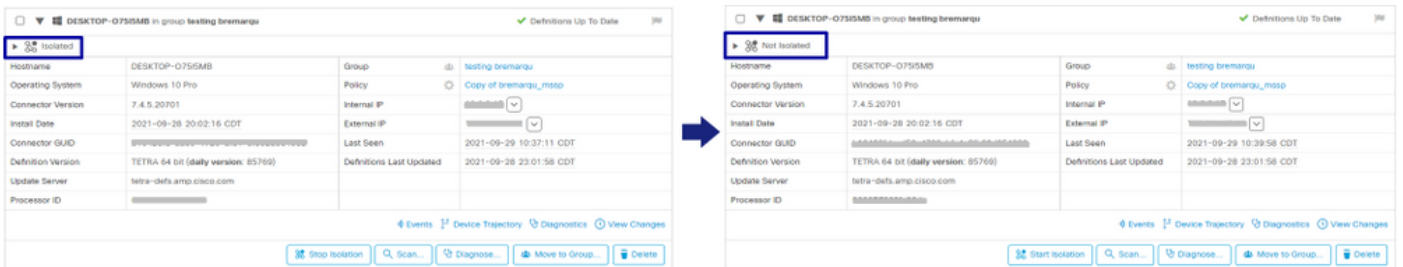


ةحصلال نم ققحتلال

ةهجاو ةيؤر كنكمي ،ةلوزعم دعت مل وا لزعلال نم تداع دق ةياهنلال ةطقن نا نم ققحتلال حضورم وه امك ،ةلوزعم ريغ اهنأ يلعل لزعلال ةلاح ضرعت ةنمآلال ةياهنلال ةطقن لوصولم مدختسم ةروصلال يف



ديحتو ،رتويبمكلل ةزهجا > ةرادلال يف لقننتلاب تمق اذا ،ةنمآلال ةياهنلال ةطقن مكحت ةدحو نم ةلوزعم ريغ لزعلال ةلاح ضرعت .لصافتلال ضرعل رقنلال كنكمي ،ينعملال رتويبمكلل ةقوم ةروصلال يف حضورم وه امك



ةلص تاذا تامولعم

- [ةنمآلال ةياهنلال ةطقن مدختسم ليلد](#)
- [Cisco Systems - تادنتسملالو ينقتلال مغللا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلل دن تسمل