



## ةيساسأل اتابلطتملا تابلطتملا

ةيلاتل اعيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت:

- اهليغشت وةيضارتفالا ةصاخلا AMP ةكبش يلع لمعلا
- ةيامحل تاديدهت ةكبش ليغشت و لمعلا

ةمدختسمل اتانوكملا

ةيلاتل ةيدامل اتانوكملا و اجماربلا تارادصا اذى دنن سمل اذى ف ةدراولا تامولعمل دنن ست

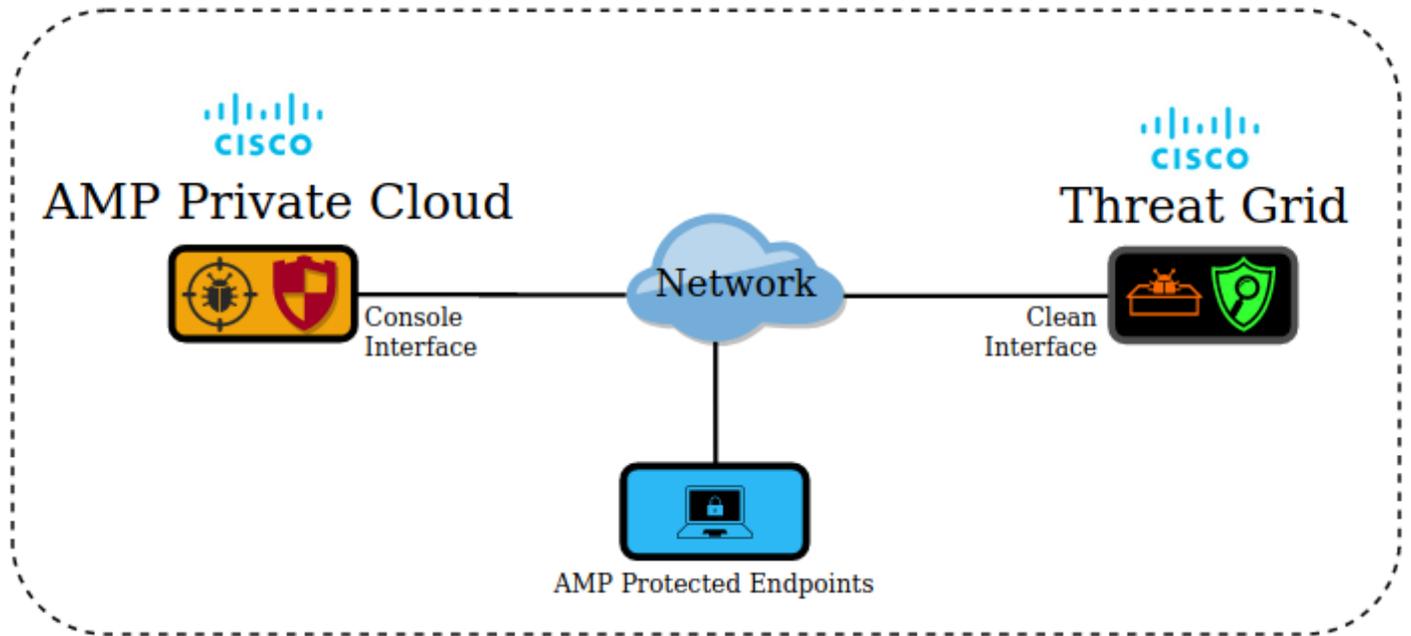
- AMP Private Cloud، رادصا اإلا 3.2.0
- 2.12.0.1 تاديدهتلا ةكبش زاى

ف ةصاخلا AMP ةكبش ةزهجأ و تاديدهتلا ةكبش ةزهجأ ةحلص قئاثولا نوكت: ةظالم  
ي رهاظلا رادصا اإلا و زاى

().

## ةيساسأ تامولعم

لماكل ةينب



## لماكل لوح ةيساسأ تامولعم

- AMP ةباحس زاى ةطساوب اهلاسر امت ي تال اتانيعلا "تاديدهتلا ةكبش" زاى للحي  
صاخلا
- ديدهتلا ةكبش زاى اى ائاقلت و اى ودي جدامنلا لاسر نكمي
- ةصاخلا AMP ةباحس زاى ف يضارفتفالا لكش ب يئاقلتلا ليحلتلا نيكمت متي ال
- ةنيعل ليحلت نم ةجرود اريقت صاخلا AMP ةباحس زاى تاديدهتلا ةكبش زاى رفوي

- وأديزت أني عيأ نع "صاخلا AMP ءكبش" زاه مالعإب (poke) "أيامحلا ءكبش" زاه موقوي ءجرد 95 يواسل
- أني علإل ع مالع عضم مئي، 95 يواسل وأ 95 نم ربكأ ليلحتلا نم ءجيتنلا تناك إذا ءراضلا ءايشأل ي ف فرصللإب AMP تانايب ءءاق ي ف ءءومللا
- تانيل علإل AMP Private Cloud ءكرش لبق نم يءجر رثأب فشكلا تايلمع قي ببط مئي 95 يواسل وأ نم ربكأ مالع علإل يوتحت يلال

## ءارءال

ءوء نم ققحت .(ءعب لمالكل ءءوي ال) هنيوكلو تاءيءهلا ءكبش زاه ءاءعإب مق.1 ءوطخلل رمال مزلا إذا ،لبيبثلو تاءيءهلا

(ءعب لمالكل ءءوي ال) ءياهنلا طاقنل ءصاخلا ءباحسلل AMP نيوكلو تاءعإب مق.2 ءوطخلل

SSL رلءا ونويوكلو بيوبللا ءمالع ءء ،لءيءهلا ءكبش ءراءل مءخلسم ءءاو ي ف .3 ءوطخلل

(PANDEM) ءفيظنلا ءءءاولل ءءيءج SSL ءءاهش ليلمءب مق وأ ئشنأ.4 ءوطخلل

## SSL إءاءة إنشاء شءاءل

(SAN) يملك إنشاء شءاءة موقعة ءايلآ ءءيءة إذا لم يءطابق اسم المصيف للواءة النظيفة مع الاسم البءيل للموضوع في الشءاءة المءبلة ءاليلآ في ءهاز اللواءة النظيفة. يولء ءهاز شءاءة ءءيءة للواءة، مما يشكل اسم مصيف اللواءة لشءاءة اللوقيع الءايل SAN الءاليل في ءقل

الءطوة 4.1. من عمول الإءراءل ءء (..) ومن القائمة المنيبقة ءء إنشاء شءاءة ءءيءة

الءطوة 4.2. في واءة مءءءم شبكة الءهءيء، ءء عمليات، في الشاشة الءاليل ءءء ءلشيط واءلر إءاءة اللوكولن

أيءل ءءقوم ءأشنملا ءءاهشلا هءة: ءظءالم

## SSL تاءاهش ليلمءب

نكمي ،"لءيءهلا ءكبش" زاه فيظنل ءءءاول لعللاب اهؤاشنل مء ءءاهش ءوءو ءلءل ي ف زاهلل إل ءءاهشلا هءة ليلمءب

ءءيءج ءءاهش ليلمءب ءء ءقءب نملا ءمئلل نمو (..) ءءل ءاءارءل ءوءم نم .4.1 ءوطخلل

يئل صنلا ءاعبرم ي ف PEM قيسنل ءب فءارملا صاخلا ءلءملا ءءاهشلا ءسنل .4.2 ءوطخلل ءءاهش ءفاضل ءءوء ءشاشلا علل رهظل

ءء ءيئلل ءشاشلا ي ف ،لءيلمع ءء ،لءيءهلا ءكبش مءخلسم ءءاو ي ف .4.3 ءوطخلل نويوكلو ءءاعل رلءا و طيئشنل

رلءا و لمالكلا تايلمع ءء ،AMP Private Cloud Device Admin مءخلسم ءءاو ي ف .5 ءوطخلل لءيءهلا ءكبش

رلءل ءء ،لءيءهلا ءكبش نيوكلو ليلصافل ي ف .6 ءوطخلل

زاهج ة فيظنلا ةهجاو لاب صاخلا FQDN لخدأ ، تاديدهتلا ةكبشل فيضملا مسا يف 7. ةوطخل تاديدهتلا ةكبش .

ةكبش زاهج ة فيظنلا ةهجاو ةداهش فضا ، تاديدهتلا ةكبشل SSL ةداهش يف 8. ةوطخل (هاندا تاظحالم رظنا) . تاديدهتلا

## الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات موقعة ذاتيا

SSL الخطوة 8.1. في واجهة مستخدم "إدارة شبكة التهديدات" ، حدد التكوين واختر

الخطوة 8.2. من عمود الإجراءات حدد (..) ومن القائمة المنبثقة حدد تنزيل الشهادة

في صفحة تكامل AMP الخطوة 8.3. قم بالمتابعة لإضافة الملف الذي تم تنزيله إلى الجهاز الخاص الظاهري من شبكة التهديدات.

## يتم توقيع الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات من قبل مرجع مصدق (CA) مؤسسي

الكاملة CA الخطوة 8.1. انسخ في ملف نصي شهادة الواجهة النظيفة لجهاز شبكة الحماية وسلسلة شهادات

PEM. قيسنتب يصنلا فلملا يف ةدوجوملا تاداهشلا نوكت نأ بجي :ةظحالم

ةداهش > ROOT\_CA ةداهش :يه ةلماك تاداهشلا ةلسلس تناك اذا  
يف حضورم وه امك ، يصنلا فلملا ءاشنإ مزلي يف :THREAT\_GRID\_CLEAN\_INTERFACE  
ةروصل.

```
-----BEGIN CERTIFICATE-----  
Threat_Grid_Clean_Interface certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
ROOT_CA certificate PEM data  
-----END CERTIFICATE-----
```

ةداهش > Sub\_CA ةداهش > ROOT\_CA ةداهش :يه ةلماك تاداهشلا ةلسلس تناك اذا  
يف حضورم وه امك ، يصنلا فلملا ءاشنإ مزلي يف :THREAT\_GRID\_CLEAN\_INTERFACE  
ةروصل.

```
-----BEGIN CERTIFICATE-----
Threat_Grid_Clean_Interface certificate PEM data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sub_CA certificate PEM data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ROOT_CA certificate PEM data
-----END CERTIFICATE-----
```

9. (API) API .

# API

API Key \*\*\*\*\*  

Disable API Key   True  False  Unset

Can Download Sample Content Via API   True  False  Unset

**Disable** عمل عملنا نأمدختسملل دكؤي، تاديدهتلل ةكبش نم باسحلل تاداعل في: **ةظحالم API Key** ريل إلى ةنيلعمل ريل **True**.

10. ةوطخلل **ظفح** ددح، تارييلل ةفاكل لامتكل دعب.

AMP نم يرهاظلال ةباحسلل زاهج لعل نيوكتل ةداعل ةيلعمل قيبطت. 11. ةوطخلل

ةكبش رتخاو لملكتلل تاي لملعمل ددح، صاخلل AMP ةباحسلل زاهج مدمختسمل ةهجاو نم. 12. ةوطخلل تاديدهتلل.

مدمختسمل و، يئاهنلل ريلصلل شيدحت ةمدخل URL ناوئل ميق خسنا ليلصافتلل نم. 13. ةوطخلل هذه مادختسلا متي. يئاهنلل ريلصلل شيدحت ةمدخل رورم ةملكو، يئاهنلل ريلصلل شيدحت ةمدخل 17. ةوطخلل في تامولعملل

CA تاداهش رتخاو نيوكتل ددح، ديدهتلل ةكبش ةرادا مدمختسمل ةهجاو في. 14. ةوطخلل

ةمدخل ةداهش لعل نعلقو يئلل CA ةداهش PEM قيسننل ب خسنو ةداهش ةفاضل ددح. 15. ةوطخلل



### File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

There are no File Analyses to view

بإحسالى مكحت ةدحو لىلحت نم اىوڊى اهل اسرا م تي يتللا تافلما كاردإ نم دكأت 3. ةوطخلل ةدحاو ةطقنب ريرقت عاجرا نمو، "تاديدتهتلا ةكبش" زاڭ يف تافلما لىلحت > AMP ل ةصاخلا "تاديدتهتلا ةكبش" زاڭ ةطساوب.

File has been uploaded for analysis

### File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

There are no File Analyses to view

### File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

glogg.exe ( e309efdd...0c2c3d25 ) 2021-01-31 06:16:55 UTC Report 24

شيدحت ةمدخ ةداهش لىل ةعقووملا (CAs) ةقدصملا تاداهشلا تيبتت نم دكأت 4. ةوطخلل زاڭ يف تاديدتهتلا ةكبش زاڭ يف AMP ل ةصاخلا ةباحسلا زاڭب ةصاخلا لىل ةصاخلا ريصملا صيخرتلا.

ةمالع عم ديدتهتلا ةكبش زاڭ ةطساوب اهل ةمالع عضو مت ةني عيا نأ نم دكأت 5. ةوطخلل ةعب ةراض راثأ ةيا عم لماعتلا عم ةصاخلا AMP ةباحس تانايب ةدعاق يف اهل جيست متي >=95 ديدتهتلا ةكبش زاڭ ةطساوب طاقن ةنيو ريرقتلا م يدقت.

مكحت ةدحو يف ةني <=95 لىل جيست وحا بنب ي جذومنلا ريرقتلا يقلت ينعى ال: **ةظحالم** ريرغت مت هنا ةرورضلاب فلفلما لىلحت بيوبتلا ةمالع AMP نم ةصاخلا ةباحسلا

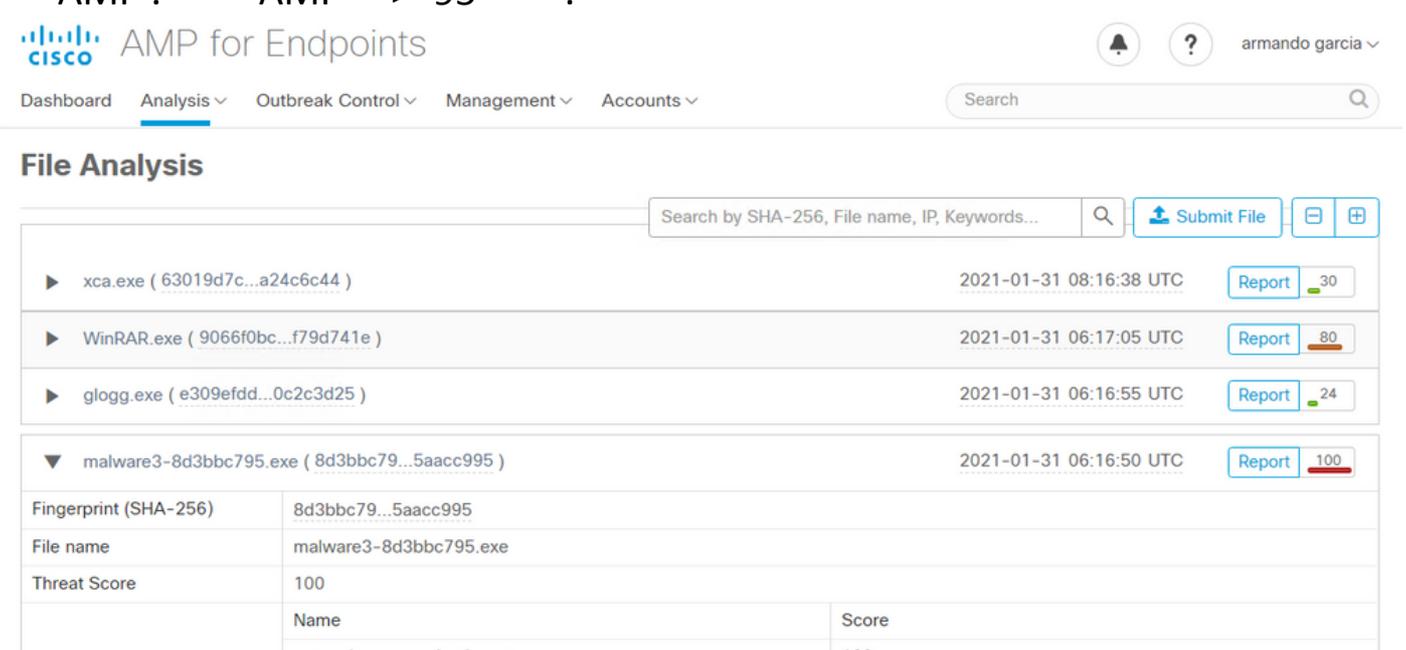
تتعلق ويتلقى CASs تثبيت متي مل اذا AMP. اتاناي بة دعاق في فللمل ليئاهنل ريصملا زاغ في AMP صاخلا بة احسلا زاغ بة صاخلا ليئاهنل ريصملا شي دحت ةمدخ ةداهش لىل زاغ ةطساوب اتانيعلا وريراقتلا يقلت متي ، تاداهشلا تائي ه في تاديدهتلا ةكبش تاديدهتلا ةكبش زاغ نم لئاسرر ي ا يقلت متي ال نكلو ، AMP ل صاخلا بة احسلا

دعاق في ةنيعلل ليئاهنل ريصملا ريغت ليغشتل يلاتلا رابتخاللا لامكإ مت :ري دحت ناك >=95 ةمالع وذل فلم لىل ةمالع عضوب Threat Grid زاغ ماق نا دع ب AMP اتاناي ب AMP بة احس زاغ في ةيلخادلا تايلمعل لوج تامولعم ريفوت رابتخاللا اذه نم ضرغلا ريغت ةيلمعل ليغشتل >=95 نم ةنيع تاديدهتلا ةكبش زاغ رفوي ام دنع صاخلا قي بطت مادختساب ةراضلا جماربللا ةاكاحم رابتخاللا فلم عاشنإ مت ، ليئاهنل ريصملا Cisco McWare.exe يلخادلا :ةنيع 3-419d23483.exeSHA256: 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

جاتنإ ةئي ب في ةراض جماربللا ةاكاحم رابتخاللا فلم ي ا ريغت بة حصني ال :ري دحت

## صاخلا AMP بة احس اتاناي بة دعاق في ةنيعلل ليئاهنل ريصملا شي دحت ديكت

" " AMP. 100 AMP Private Cloud Device Threat Grid. >=95  
AMP . AMP >=95 .



The screenshot shows the Cisco AMP for Endpoints interface. At the top, there's a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. A search bar is on the right. Below the navigation bar, the 'File Analysis' section is active. It displays a table of files with columns for file name, SHA-256 hash, and threat score. The file 'malware3-8d3bbc795.exe' is highlighted, and its details are shown below the table.

File Name	SHA-256 Hash	Threat Score
xca.exe	63019d7c...a24c6c44	30
WinRAR.exe	9066f0bc...f79d741e	80
glogg.exe	e309efdd...0c2c3d25	24
malware3-8d3bbc795.exe	8d3bbc79...5aacc995	100

File Analysis Details for malware3-8d3bbc795.exe:

Fingerprint (SHA-256)	8d3bbc79...5aacc995
File name	malware3-8d3bbc795.exe
Threat Score	100

اذا:

- حاجن ب لمككتلا لامكإ مت
- ايودي تافللملا لاسرا دع ب تافللملا ليحت في تانيعلا وريراقتلا جذا من ضرع متي

ثم:

- فللملا لىل لاخذ ا ةفاض ا مت ، >=95 ةجرد بة احملا ةكبش زاغ اه يل ريشي ةنيع لك ل /data/poked/poked.log في صاخلا AMP ةكبش زاغ في
- ةي احملا بة صاخلا ةكبشلا زاغ في /data/poked/poked.log ةحفصلا عاشنإ متي ةي احملا ةكبش زاغ اهمدقي ةنيع >=95 ةمالع لو ا دع بة مدقتملا
- ليئاهنل ريصملا صاخلا AMP بة احس في ةدوجوملا db\_protect اتاناي بة دعاق لمحت لىل يوتحت ةنيعلل تناك اذا امم دكأتلل تامولعمل ا هذه مادختس ا نكمي . ةنيعلل يلاخلا

ةجيتنل ري فوتب "تاديدهتلا ةكبش" زاغ ماق نأ دعب 3 ىلع يئاهنلا ريصملا ل ةصاخلا ةباحسلا مكحت ةدحو يف فلملا ليحت يف  $\geq 95$  ةجردو جذومنلا ريرقت ضرعت مت اذا ةيئاهنلا تاوطلخا قيبطتت مقف AMP،

صاخلا AMP ةباحس زاغ ىلى SSH ربع لوخدلا لجس 1. ةوطلخا

ةنيعلل /data/poked/poked.log يف لاخدا دوجو نم دكأت 2. ةوطلخا

$\geq 95$  ةمالع ادبأ ملتسي مل يذلا صاخ AMP ةباحس زاغ يف /data/poked/ لىلدلا ةمئاق رهظت ماظنلا يف هؤاشنلا متي مل poked.log فلم نأ تاديدهت ةكبش زاغ نم ةنيعل

روثعل متي نلف ،تاديدهت ةكبش زاغ نم سدكم يأ ةصاخلا AMP ةباحس زاغ ملتسي مل اذا ةروصللا يف حضورم وه امك ،لىلدلا يف /data/poked/poked.log فلم ىلع

```
[root@fireamp ~]# ls /data/poked/
poked_error.log
poked.log
[root@fireamp ~]#
```

هؤاشنلا مت يذلا فلملا ، $\geq 95$  ةمالع لوأ مالتسا دعب /data/poked/ لىلدلا ةمئاق رهظت

$\geq 95$  ةجردب ىلوالا ةنيعل مالتسا دعب

```
[root@fireamp ~]# ls /data/poked/
poked_error.log  poked.log
[root@fireamp ~]#
[root@fireamp ~]# cat /data/poked/poked.log
Jan 30 18:25:18 fireamp poked[9557]: [9557] info @0.004940 127.0.0.1 --
{"disposition": "malicious", "force": 0, "state": "local", "name": "W32.80388C7958-100.SBX.TG", "ok": 1, "time": 1612031118, "hash": "8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995", "engine": "sha256", "user": "-", "mode": "tg", "score": 100}
[root@fireamp ~]#
```

دربم poked.log لا لخاد مهفي نأ نكمي ةكبش ديدهت لا ب دوزي ةأدال نم ةمولعم ةنيعل

يلاجل يئاهنلا ريصملا دادرستال SHA256 جذومن مادختساب رمألا اذه ليغشتت مق 3. ةوطلخا صاخلا AMP ةباحس زاغ تانايب ةدعاق نم

```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

لاثم

ليمحت لبقتنيعل لىلدلا ريصملا ىلع لوصحلل تانايب ةدعاق مالعستسا رفوي ال ةروصللا يف حضورم وه امك چئاتن ةيأ "تاديدهتلا ةكبش زاغ" ىلى ةنيعللا

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
[root@fireamp ~]#
```

ريرقتلا مالتسا دعب ةنيعل لىلدلا ريصملا ىلع لوصحلل تانايب ةدعاق مالعستسا رهظي ةراض ربتعت يتلا او 3 يئاهنلا ريصملا اهل يتلا ةنيعللا ،تاديدهتلا ةكبش زاغ نم ةمالعلاو

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+-----+-----+
| hex(fingerprint) | disposition_id |
+-----+-----+
| 8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995 | 3 |
+-----+-----+
[root@fireamp ~]#
```

## اهحالصوا ءاطخالا فاشكتسا

يُرجى، ةقېثولا نم ءزجلا اذه يفو. ةلمتحملا اياضقلا لىل رظنلا نكمي، لمكتلا ةيلمع يفو اعويش لىاسملا رثكأ ضعب لوانت

## رابتخا متي مل، حلص ريغ فيضملا لوح AMP ل صاخلا ةباحسلا زاهج يف ريذحت API حاتفم رابتخا متي مل، ةداهشلا

ضرع

ةكبش ل SSL ةداهش رابتخا رذعت، حلص ريغ تاديدهتلا ةكبش فيضم: ريذحتلا ةلاسر AMP ةكبش زاهج يف همالتسا مت، تاديدهتلا ةكبش ل API حاتفم رابتخا رذعت، تاديدهتلا تاديدهتلا ةكبش > لمكتلا تايلمع يف لاصتالا رابتخا رز ديذحت دعب ةصاخلا

Connect Threat Grid Appliance to AMP for Endpoints Appliance

### Threat Grid Connection test failed.

- Threat Grid host is invalid.
- Threat Grid SSL Certificate could not be tested.
- Threat Grid API key could not be tested.

لمكتلا يف ةكبشلا يوتسم لىل ةلكشم كانه.

اهب لىصوملا تاوطلخا

- ةفيظنلا ةهجاو لىل AMP ل صاخلا ةباحسلا زاهج مكحت ةدحو ةهجاو لوصو ةينكأ ديكات تاديدهتلا ةكبش زاهج
- ةكبش زاهج فيظنت ةهجاوب صاخلا FQDN لىل هنكمي صاخلا AMP ةباحس زاهج نأ ديكات تاديدهتلا
- ةكبش زاهج و صاخلا AMP ةباحس زاهج ةكبشلا راسم يف ةيفصت زاهج دوجو مدع نم دكات تاديدهتلا

AMP API

ضرع

ريغ تاديدهتلا ةكبش ل صاخلا API، تاديدهتلا ةكبش لاصتالا رابتخا لىل شف: ريذحتلا ةلاسر تايلمع يف لاصتالا رابتخا رز ديذحت دعب صاخلا AMP ةباحس زاهج يف همالتسا متي، حلص تاديدهتلا ةكبش > لمكتلا

Connect Threat Grid Appliance to AMP for Endpoints Appliance

### Threat Grid Connection test failed.

- Threat Grid API key is invalid.

AMP . API

اهب لىصوملا تاوطلخا

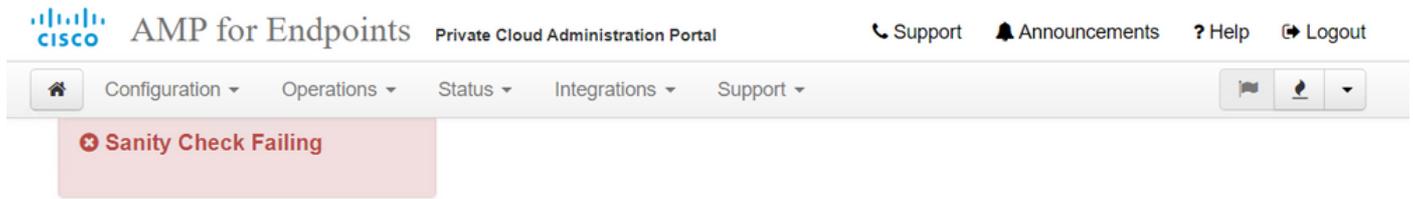
- نييغت متي مل، تاديدهتلا ةكبش زاهج مدختسمب ةصاخلا باسحلا تادادع يف ديكات





ديدهتلا ةكبش زاغ يف CA تاداهش يف Sub\_CA و RootCA تيبتت بجي ، يلاتلابو

ةصاخلا AMP ةباحس ةرادا لخدم يف تاداهشلا تاطلس



Certificate Authorities are used by your Private Cloud device to verify SSL certificates and connections.

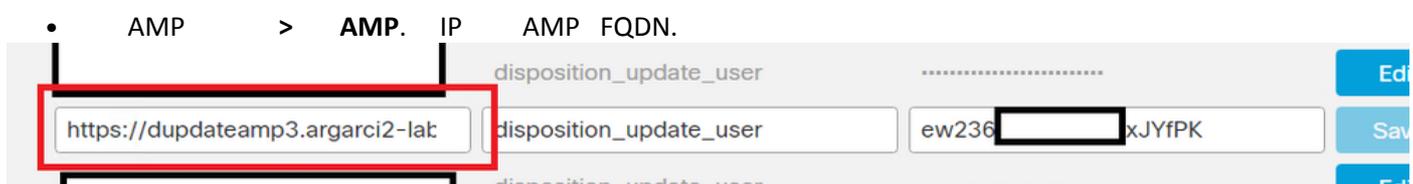
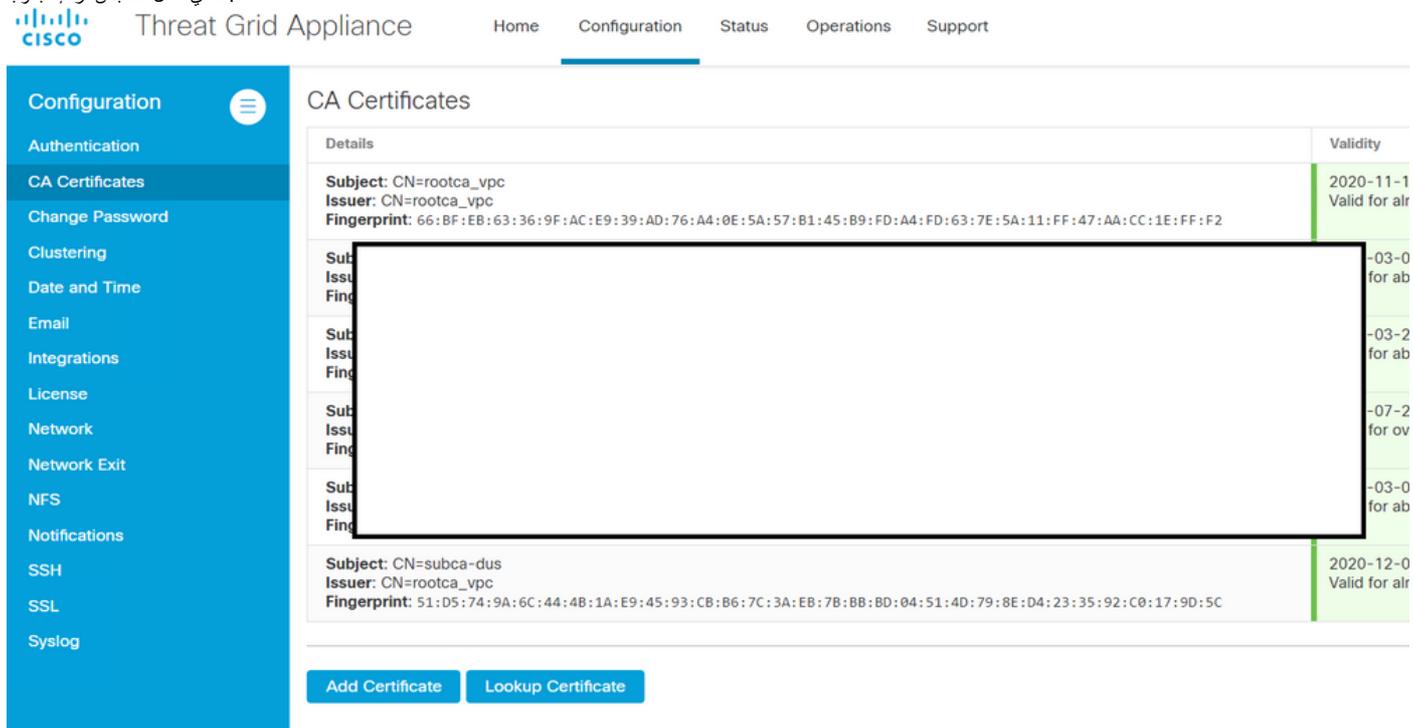
[Add Certificate Authority](#)

Certificate		<a href="#">(click to collapse)</a>
Issuer	rootca_vpc	<a href="#">Download</a> <a href="#">Delete</a>
Subject	rootca_vpc	
Validity	2020-11-15 00:00:00 UTC - 2025-11-14 23:59:59 UTC	

Certificate		<a href="#">(click to collapse)</a>
Issuer	rootca_vpc	<a href="#">Download</a> <a href="#">Delete</a>
Subject	subca-dus	
Validity	2020-12-05 12:01:00 UTC - 2023-12-05 12:01:00 UTC	

تاديدهتلا ةكبش ةرادا قباوب



# ريغ تاديدهت ةكبشل SSL ةداهش لوح AMP ل صاخلا ةباحسلا زاهج في ريذحت ةحلص

ضرع

ةباحسلا زاهج في ،"ةحلص ريغ تاديدهتلا ةكبشل SSL ةداهش": ريذحتلا ةلاسر ريقلت متي تاديدهتلا ةكبش > لمكتلا تاي لمع في لاصتالا رابتخا رز ديذحت دعب AMP ل صاخلا

## Threat Grid Connection test failed.

- Threat Grid SSL Certificate is invalid.
- Threat Grid API key could not be tested.

اهب يصوملا تاوطلال

- لبق نم اهعيقوت متي تال Threat Grid ةهجاو في ةتبثملا ةداهشلا تناك اذا ام ديكت

ي.سسؤم قدصم عجرم

تاي لمع يلى فلم لخاد ةلمكتلا تاداهشلا ةلسلس ةفاضلا بجي في ،CA ةطساوب اهعيقوت متي اذا ةكبشل SSL ةداهش في تاديدهتلا ةكبش > ةصاخلا AMP ةباحس ةزهجا ةرادا ةباوب لمكت تاديدهتلا.

Threat Grid Configuration Details		Edit
Hostname	<input type="text" value="cisco.com"/>	
API Key	<input type="password" value="....."/>	
<b>Threat Grid SSL Certificate</b>		<a href="#">Test Connection</a>
Issuer	subca_tga_clean	
Subject	<input type="text" value="cisco.com"/>	
Validity	2020-11-24 00:00:00 UTC	- 2021-11-23 23:59:59 UTC

ايلاحتبثملا ةيامحلا ةكبش زاهج تاداهش يلع روثل نكمي ،AMP Private Cloud زاهج في في : /opt/fire/etc/ssl/threat\_grid.crt .

## تاداهشلاب ةقلعتملا ديدهتلا ةكبش زاهج في ةدوجوملا تاريذحتلا

قباطم ريغ صاخحاتفم نم دمتسم الماعل حاتفملا - ريذحت ةلاسر

ضرع

زاهج في همالتس متي ،قباطم ريغ صاخحاتفم نم دمتسم الماعل حاتفملا : ريذحتلا ةلاسر ةهجاو يلى ةداهش ةفاضلا ةلواحم دعب ديدهتلا ةكبش



زاهج يف همالتسإ متي و، PEM ريغ يوتحم ىلع صاخلاجاتفملا يوتحي: ريذحتلا ةلاس رة. ةهجاو ىلإ ةداهش ةفاضا ةلواحم دع ب ديدتلا ةكبش



Configuration

Authentication

CA Certificates

Change Password

Clustering

Date and Time

Email

Integrations

License

Network

Network Exit

NFS

Notifications

SSH

SSL

Syslog

### Upload SSL certificate for PANDEM

Certificate (PEM)

```
-----BEGIN CERTIFICATE-----
MIIDTjCCAjagAwIBAgIIcR1youIOY/MwDQYJKoZIhvcNAQELBQAwGjEYMBYGA1UE
AwwPc3ViY2FfdGdhX2NsZWZuMjEwMTEyNDAwMDAwMDFoXDTIxMTEyMzZlZjE2
k1
OVowSTEBMBkGA1UEChMSQ2l2Y28gU3lzdGVtY291MjEwMTEyNDAwMDAwMDFoXDTIxMTEyMzZlZjE2
NlgQT03qqfX7Zh5wKY4BrTWxOpNBodUcl0KxzODPWYZqUUjpeKcgyUkj2L6fY0OV
```

Private Key (PEM)

```
wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
lJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+HONxldl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO
/8E/D+jdT8zhA3aWNXADf8b9xjlRE324TFAfJf73a59q27y7d96tCa1PFaMOiXGc
nY2D9lwNsnl5uk1IHL2SojLtVx8BYqw98w0uuBOMqZZVNprSparsyw==
-----END RSA PRIVATE KEY-----
```

*private key contains non-PEM content*

ةفلات صاخلاجاتفملا فلم لخاد PEM تانايب

اهب ىصوملا تاوطخلا

صاخلاجاتفملا ةمالس نم ققحتلل OpenSSL ةادأ مدختسأ 1. ةوطخلا

```
openssl rsa -check -noout -in
. PEM PEM.
```

```
$ openssl rsa -check -noout -in wrong-private-key.key
unable to load Private Key
140333463315776:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -check -noout -in correct-private-key.key
RSA key ok
```

عم لكاشم ىلع روثعلال مت هنا ىنعى اذهف، RSA OK حاتفم وه OpenSSL رمأل جارخا نك ي مل اذا حاتفملا لخاد PEM تانايب

ذئدنعف، OpenSSL رمأل يف لكاشم ىلع روثعلال مت اذا

- ال مة دوقفم صاخلاجاتفملا لخاد PEM تانايب تناك اذا ام ديكأت نأ نكمي. افرح 64 نم ةنوكملا رطسأل يف صاخلاجاتفملا فلم لخاد PEM تانايب ضرع متي. ةدوقفم تانايب تناك اذا ام فلملا لخاد PEM تانايب لىع رطسأل صخالف رهظي فلملا يف ىرخأل رطسأل عم هتاذاحم متت ال ةدوقفملا تانايب و ذ رطسأل.

```

$ cat wrong-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfiYtwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNIHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTIcI2q/vH/i0WeIgAv10aGuBCOeg <-----
NwOgPyY3XI8g7l 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAGMBA tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfi s7k0sCwmhKUaMacTYAnrg
fINIJto/x0azh 47ttvLvX3zweLCEXsDXK6
mdhzCQSTBFybM 24M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3. 1gd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb! 3gQDePpxacxGRZLXfja3s
SU+TvjNWQGcUs: a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HFVnsq9+xbCU1fRlPxeCS
CbclDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGFhN/ZziDtrkSzJSM6fVGPPhJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBzy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTY1GD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdfQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UByx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----

```

• صاخال حااملك لا أءبءو، ةلصاوا 5 ب أءبى صاخال حااملك لا يف لوالا رطسلا نأ ءىكأء، ةلصاوا 5 ب بهءننى و لاءم.

—صاخال حااملك لا ءءب—

• صاخال حااملك لا ءاهن|ءاملك، ةلصاوا 5 ب أءبى صاخال حااملك لا يف رىءال رطسلا ءىكأء، ةلصاوا 5 ب بهءننى و لاءم.

—صاخال ةىاهنلا حااملك—

• صاخال حااملك لا ءاء ءءوءوملا ءاناىبلا و PEM قىسنىء ءىءصء لاءم.

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwKf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/Pw4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBC0egVDU
NwOgPyY3XI8g7H 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBAAtU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfBs7k0sCwmhKUaMAcTYAnrg
fINIJto/x0azhe47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4R4M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3ahgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9BgQDePpxacxGRZLXfja3s
SU+TvjNWQGcUsXa8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfdPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFp0AFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS
Cbcf1DYBwaMn8Ywp9PfZKpGu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHfn/ZziDtrkSzJSN6fVgPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1S09eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

صاخال حاتفملا نم ماع حاتفم عاشن| نكمي ال - ريذحت ةلاسر

ضرع

ةكبش زاهج ي ف اهيقلت مت ،صاخال حاتفملا نم ماع حاتفم عاشن| نكمي ال :ريذحتلا ةلاسر  
ةهجاو ىلإ ةداهش ةفاضل ةلواحم دعب ديهتلا

Configuration

- Authentication
- CA Certificates
- Change Password
- Clustering
- Date and Time
- Email
- Integrations
- License
- Network
- Network Exit
- NFS
- Notifications
- SSH
- SSL**
- Syslog

### Upload SSL certificate for PANDEM

Certificate (PEM)

```
AN
BgkqhkiG9w0BAQsFAAOCQAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9Kle
epjqQobaJadl3WTh7LMHuxHZP02YZJIO/OjUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF
[Redacted]
wbTboJukREZOyiBoQDPcSWHqe8j3FEtJlf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL
7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1glIYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVVHJdCsczgz1mGalFI6Xinl8JI9i+n2NDIcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5DIb17RLy7Y+wxhMiyRCHH3aZ3I0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

cannot generate public key from private key

Add Certificate Cancel

صاخال حاتفملا فلم لخاد للاحال PEM تانايب نم ماعلا حاتفملا عاشن نكمي ال

اهب ي صوملا تاوطلال:

- .
- 1. OpenSSL .

```
openssl rsa -check -noout -in
```

عم لكاشم يلع روثلال مت هنا ينعې اذهف، RSA OK حاتفم وه OpenSSL رمألا جارخ نكي مل اذا حاتفملا لخاد PEM تانايب

حاتفملا نم ماعلا حاتفملا ريصدت ةينكام نم ققحتلل OpenSSL ةادأ مدختسأ 2. ةوطلال صاخال

```
openssl rsa -in
```

حجان ماع حاتفم ريصدت و ماعلا حاتفملا ريصدت لشف .لاثم

```

$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -in correct-private-key.key -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArc3yMrcJH/VCH0Q5bivT0
2yrw60oYJ/Pwnp/cFxFayATWoZRYmb8GW/+RS/iNa8vz9FiiTII0YS0dmNKKIEL
Lg080/TKGusV2CyqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjijNHNwBICv6wWA02gr/xj+qxpB3
P1YjNTU711SFnSHC4E1Fzg3hy40yHCNqv7x/4j1niIAL9dGhrgQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg61+J4uIjytkVceBw0v1bDNDdDRyk+BIB0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----

```

## PEM تانايب زيمرت ك ف رذعت :لجحتللا ف أطخ - ريذحت ةلاسر

ضرع

زاهج ف اهيقولت مت ، PEM تانايب زيمرت ك ف رذعت :لجحتللا ف أطخ :ريذحتللا ةلاسر  
 ةهجاو لى ةداهش ةفاضل ةلواجم دعب "ذيدهتلا ةكبش"

The screenshot shows the 'Upload SSL certificate for PANDEM' configuration page. The 'Certificate (PEM)' field contains a long string of base64-encoded data. Below the field, a red error message states: 'parse error: PEM data could not be decoded'. The 'Private Key (PEM)' field also contains a long string of base64-encoded data. At the bottom of the page, there are two buttons: 'Add Certificate' and 'Cancel'. The left sidebar shows the navigation menu with 'SSL' selected.

PEM تانايب .ةداهشللا فلم ف ةدوجوملا ةيلاجلا PEM تانايب نم ةداهشللا زيمرت ك ف رذعتي  
 ة.ةلات ةداهشللا فلم لآخاد

- ةداهشللا فلم لآخاد PEM تانايب نم ةداهشللا تامولعم دادرئس نك ام ديكأت .

PEM تانايب فلم نم صيخرتللا تامولعم ضرع ل OpenSSL ةادا مدختسا 1. ةوطخللا

openssl x509 -in

تامولول عم لي مفتح OpenSSL ةادأ لواح ت ام دنع أطخ رهظي سف ، ةفلات PEM تانايب تناك اذا ةداهشل.

ةداهشل فلم في PEM تانايب فلت ببسب ةداهشل تامولول عم لي مفتح ةلواح ت لشف . لاثم

```
$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

## مداخل/اليمع ل ق دصم عجرم ةداهش تسيل - ريذحت ةلاسر

ضرع

في اهمال تسلي م تي ، مداخل/اليمع ق يدصت عجرم ةداهش تسيل : ليلحتل في أطخ : ريذحتل ةلاسر عجرم ل تاداهش > نيوكتل الى ق دصم عجرم ةداهش ةفاضل ةلواح دع ب "ديدهتلا ةكبش" زاهج ق دصم ل.



Threat Grid Appliance

Home

Configuration

Status

Operations

Support

Configuration

Authentication

CA Certificates

Change Password

Clustering

Date and Time

Email

Integrations

License

Network

Network Exit

NFS

Notifications

SSH

SSL

Syslog

### CA Certificates

Certificate (PEM)

```
-----BEGIN CERTIFICATE-----
Ir2MrtEmB8vuU3CzLqSnC3iFRYF9bbwiQTw/AgMBAAGjDzANMAsGA1UdDwQEAwIC
jDANBgkqhkiG9w0BAQsFAAOCAQEAY3b0+QmLE0Ri7q3iHUSK3cGcWhCrWIF5z3OR
w6yBX1YrWKICWS0mT8K/3mScEbUvyjALFRvoGccYLlI3wboaB8ZLxysEL6Nw7r+5
AtTgHWYUedrgnnAUjQbiOIs+NUY826gpRwuH7PBYT9k33OK8XSzo8xmsQQG+oHOo
L2wj6R2hS8e7dzJzHbsp+1icL/w7MAuFRWkTA0j7gEbKmYj+0Q==
-----END CERTIFICATE-----
```

*not a client/server CA cert*

Add Certificate

Cancel

حيحص : CA ك CA ةداهش في "ةيساس ال دويقل" قحل مل ةمي ق في رعت م تي مل .

CA : لىل ةيساس ال دويقل قحل مل ةمي ق نييعت م اذا OpenSSL ةادأ مادخت ساب دي كأتل CA ةداهش في حيحص .

PEM تانايب فلم نم صيخرتل تامولول عم ضرع OpenSSL ةادأ مدختسأ 1. ةوطخل

openssl x509 -in

ةساسةال دوقلا قحللمة لةلحلالمة قلال نع ةداهشلال تامولعم يف شحبا 2. ةوطخلال

تاددهتلال ةكبش زاهج ةطساوب لوبقم CA ل ةساسةال دوقلا ةمق. لاثم

```
Ca.01
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:TRUE
  X509v3 Key Usage:
    Digital Signature, Key Agreement, Certificate
```

## ةلص تاذا تامولعم

- [نوكتلال ةلدأ - ةمامحلال ةكبش زاهج](#)
- [Cisco - نم ةراضلال جماربالا نم ةمدقتملا ةمامحلاب ةصاخلال ةراضارثفالا ةبباسلال ةادألا](#)
- [ةننفلال تاظحالمل او نوكتلال ةلثمأ](#)
- [Cisco Systems - تادنتسمل او نقتلال معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ن أ 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 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 ئ 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 إ ل ا دن تسمل ا