

جماربل نم ةمدقتملا ةيامحل عم SecureX ةياهنلا طاقنل جم دل ليلدل (AMP) ةراضل

تايوت حمل

[ةمدقمل](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[AMP مكحت ةدحو يف API دامتعا تانايب عاشنلا](#)

[AMP مكحت ةدحو يف SecureX طيرش نيكتم](#)

[SecureX يف ةياهنلا طاقنل AMP ةيطمنلا ةدحو لا جم](#)

[ةحصللا نم ققحتلا](#)

[اهحاصل او ءاطخأل افاشكتسا](#)

[\[403\] ةباتكلل لوصول قح هيدل سيل API ليمع](#)

[\[401\] ليمعلا فرعم وأ فرعم ريغ API حاتفم: أاطخ](#)

[ويديفلل ليلد](#)

ةمدقمل

Cisco Advanced Ware عم هنم ققحتلا او Cisco SecureX جمدل ةبولطملا ةيلمعلا دنتمسلا اذه فصوي ةياهنلا طاقنل (AMP) Protection.

ةدعاسملا زكرم وسدنه م ، تيرافان يخرؤخ ريرحت ، سيروت ليريروأو زيشناس نيديلاري هب مهاسم ةكشرلل ةباتلا ةينفلا Cisco.

ةيساسأل تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب فرعم لكيدل نوكت نأب Cisco يصوصت:

- Cisco نم ةراضلا جماربل نم ةياهنلا طاقنل ةمدقتملا ةيامحلا
- SecureX مكحت ةدحو يف يساسأل لقننتلا
- روصول ةيبرايختخال ةيضرارتفالا ءكاحملا

ةمدختسملا تانوكملا

- AMP رادصلإا ، ةياهنلا طاقنل مكحت ةدحو AMP 5.4.20200804
- ةياهنلا طاقنل لوؤسم باسحل AMP
- SecureX Console ، رادصلإا 1.54
- SecureX لوؤسم باسح

- Microsoft Edge رادصلإا 84.0.522.52

ةزهجال اعيجم تادب .ةصاخ ةيلمعم ةئييب يف ةدوجوملا ةزهجالا نم دنتسملما اذه يف ةدراولما تامولعملما ءاشنإ مت كمهف نم دكأتف ،لليغششلال ديق كتكبش تناك اذا .(يضا رتفا) حوسمم نيوكتبب دنتسملما اذه يف ةمدختسملما رما يأل لمحتحملما ريثأتلل

ةيساسأ تامولعملما

نم يساسأ عزج يه ةياهنللا طاقنل Cisco نم (AMP) ةراضللا جماربللا نم ةمدقتملا ةيامحللا وأو فشكلا فئاظو معدت ةيقيقتو ةيئاقو ةادأك اهرشن متيو ةياهنللا طاقن نامأ ةصنم طاقنل AMP ةدحو رفوتو ، iOS و Android و Linux و MacOS و Windows ةزهجال ةباجتساللا .تابناجت 5 ةياهنللا

- تالزاننلا صخلت سييياقملا نم ةعومجم AMP: ةطساوب اهفاشكتا مت يتلا تالزاننلا AMP ةطساوب اهفاشكتا مت يتلا
- AMP رتويبمكلا ةزهجال صخلت سييياقملا نم ةعومجم AMP: رتويبمكلا ةزهجال صخلم
- هل ةباجتساللا او AMP فايشكتا صخلت سييياقملا نم ةعومجم AMP: صخلم
- تقولا بسح AMP Quarantines صخلت يتلا تاسايقلا نم ةعومجم AMP Quarantines:
- صخلت سييياقملا نم ةعومجم AMP: ةطساوب اهفشك مت يتلا Miter ATT&CK تاكيكتا AMP ةطساوب اهفشك مت يتلا Miter ATT&CK تاكيكتا

نيوكتلا

AMP مكحت ةدحو يف API دامتعا تانايب ءاشنإ

ةديج API دامتعا تانايب ءاشنإ متي ، AMP مكحت ةدحو يف

- لوؤسمللا تازايتما ب AMP مكحت ةدحو يلى لوخدلا ليجست
- تاقيببطللا ةجمرب ةهجاو دامتعا تانايب > تاباسحللا يلى لقتنا ، AMP مكحت ةدحو يف (API)
- ةديج تاقيببطللا ةجمرب ةهجاو دامتعا تانايب قوف رقنا

+ New API Credential

- قيببطللا ةيمستب مق
- ةباتكو ةعارق ددح
- عدوتسم ليزنت قيقدت تالجتس يلى API لوصولو حامسللا ورمأوالا رطس نيكمت قيقدت تافللملا
- ءاشنإ قوف رقنا

New API Credential

Application name

Scope Read-only Read & Write

Enable Command line

Allow API access to File Repository download audit logs

- API دامتعال تانايب ءاشنإ متي

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

< API Key Details

3rd Party API Client ID

API Key

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

كب ةصاخلا دامتعال تانايب ظفحا، راطإلا اذه يف طقف ةرفوتم تامولعملل هذه: ةظحالم يطايتحإ خسن فلم يف.

AMP مكحت ةدحو يف SecureX طيرش نيكمتم

ديحوت ىلع لمعت يتلا تاردقلا نم ةعزوم ةومجمو ةيزكرم مكحت ةدحو SecureX جم انرب ربت عي ةصاخلا لمعل ريس تايلمع عيرستو يئاقلا لئغشلا نيكمتمو ةيؤرلا ةينام تاناكإلا هذه ميديقت متي. تاديدهتلا نع شحبللا ةيلمع نيسحتو شواحلل ةباجتسالاب طيرش نيكمتم نكميو، SecureX طيرش يف تاوداو (تاقببطت) تاقببطت لكش يف ةعزوملا AMP مكحت ةدحو يف SecureX.

- SecureX ىلا لوخدلا ليچست
- AMP مكحتلا ةدحو ىلع
- مدختسملا قوف رقنا > نومدختسملا > تاباسحلا ىلا لقتنا
- SecureX طيرش ليوخت قوف رقنا تاداعإلا يف

Settings

Two-Factor Authentication [Manage](#)

Remote File Fetch **Enabled**

Command Line **Enabled**

Endpoint Isolation **Enabled**

Time Zone **UTC**

Appearance **Auto** Light Dark

SecureX Ribbon [Authorize](#)

Google Analytics [Opt Out](#) ?

- SecureX ديدته ةباجتسإىلإ كهيجوت ةداعإ متت
- ةياهنلا طاقنل AMP ليوخت قوف رقنا

Grant Application Access

The application **AMP for Endpoints** (console.amp.cisco.com) would like access to your Cisco Threat Response account.

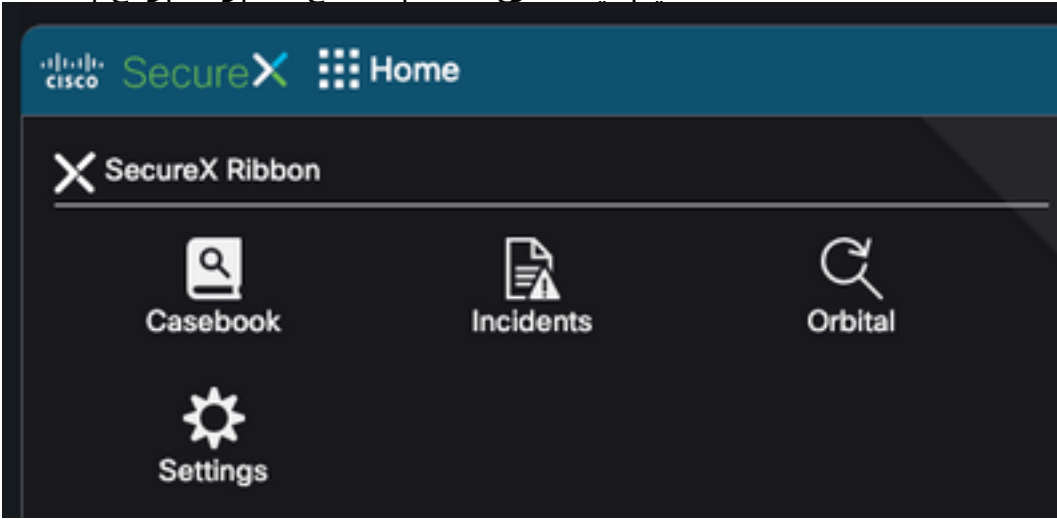
Specifically, **AMP for Endpoints** is requesting the following:

- **casebook**: access and modify your casebooks
- **enrich**: query your configured modules for threat intelligence (*enrich:read*)
- **global-intel**: query AMP Global Intelligence
- **inspect**: extract observables and data from text (*inspect:read*)
- **integration**: manage your integration modules configuration (*integration/module-instance:read, integration/module-type:read*)
- **orbital**
- **private-intel**: access Private Intelligence
- **profile**
- **registry** (*registry/user/ribbon*)
- **response**: list and execute response actions using configured modules
- **telemetry** (*telemetry:write*)
- **users**

[Authorize AMP for Endpoints](#)

[Deny](#)

- ةحول نيب لقننلا ءانثأ ادوجوم لازي الو ةحفصل نم يلفسلل عزجلا يف طيرشلا دجوي



SecureX في ةياهنل طاقنل AMP ةيظمنل ةدحولل جمد

قايسلل تاذه ةدعتملل تافللمل نع يرحتلل اب AMP for Endpoints ةيظمنل ةدحولل كل حمست طاقن لوح ةيلصفت تامولعم رفوي. نامال تاجتنم ربع لمكثلل تايلمع نم اهديدحتو AMP GUID فرعمو ليغشثلل ماظنو IP نيوانع كلذ في امب، ةرثأتمل ةزهجالو ةياهنل

- ةيظمن ةدحو ةفاضل قوف رقنل لملكثلل تايلمع لىل لقتنا، SecureX م كحت ةدحو في ةديج
- ةديج ةيظمن ةدحو فيضي ةقطقو ةيظمن ةدحو ةطقن ةياهنل AMP تيقتنا
- ةيظمنل ةدحولل ةيمست
- AMP ةباحس ديحت
- تحت اقبسم اهعيمجت متي ال (API) تاقيبطلل ةجمررب ةهجاو دامتعا تانايب ل اخدا متي ةجمررب ةهجاو حاتفمو ثلثل فرطلل نم (API) تاقيبطلل ةجمررب ةهجاو لي مع فرعم (API) تاقيبطلل

Add New AMP for Endpoints Module

Module Name*

URL*

https://api.amp.cisco.com

3rd Party API Client ID*

API Key*

Act in the name of Active User ?

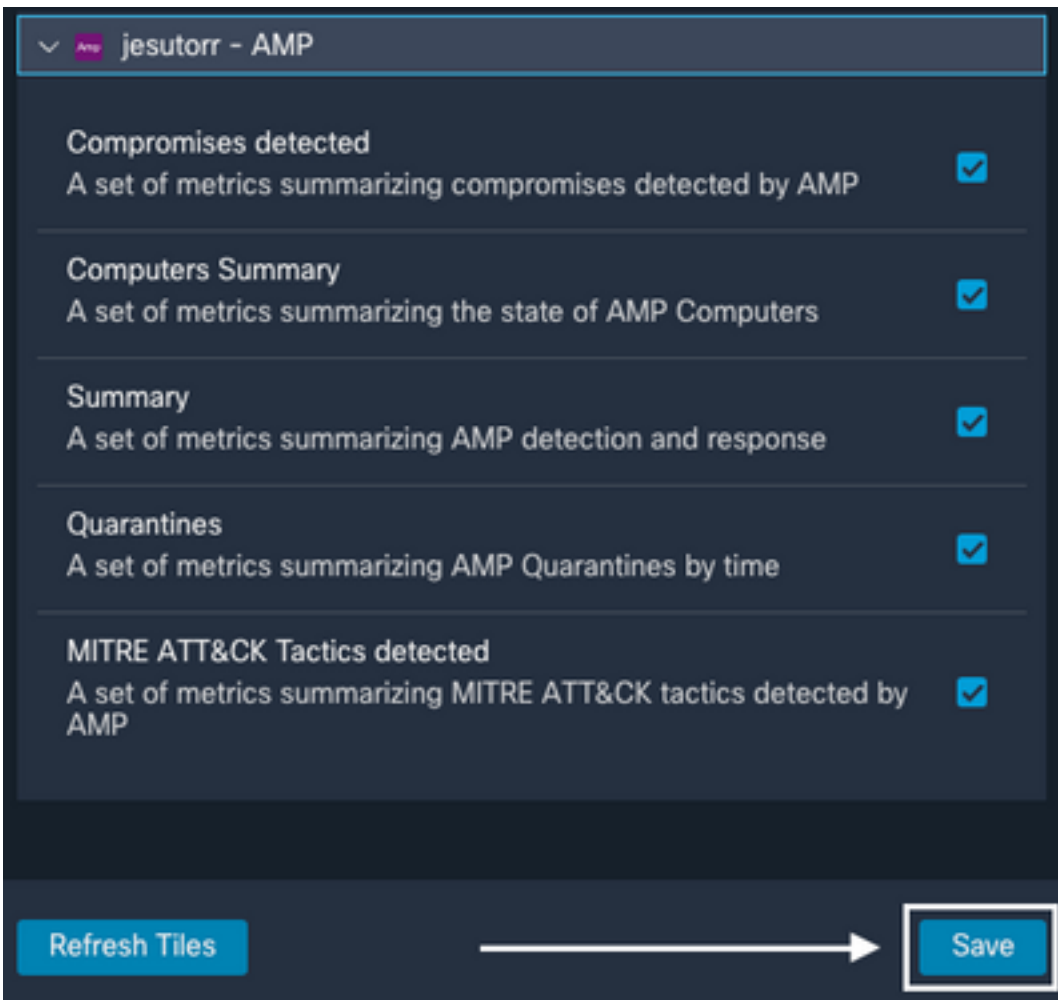
Save

Cancel

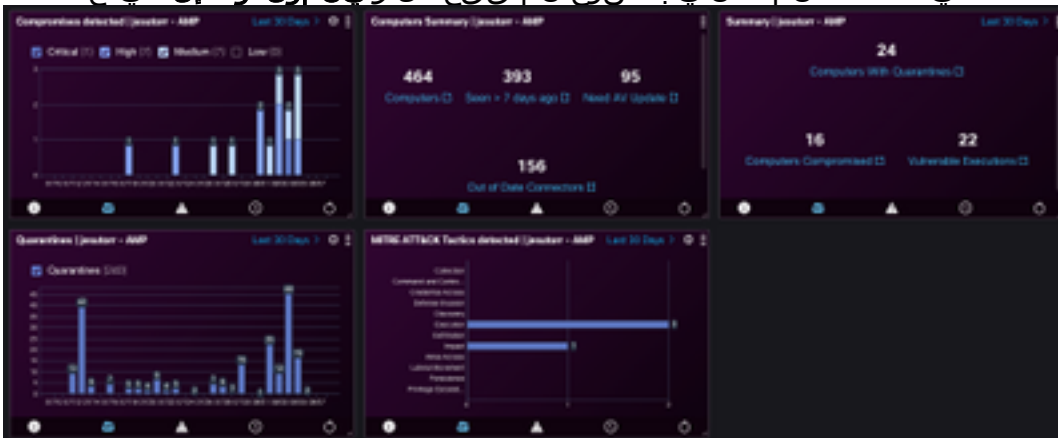
ةحصللا نم ققحتلا

SecureX تامولعم ةحول في AMP مكحت ةدحو نم تامولعملال ضرع نم ققحت

- تامولعملال ةحول لىل SecureX لىل لقتنا
- اهمساو ةديج تامولعم ةحول قوف رقنا
- اقپسم اهؤاشنإ مت يتل AMP ةيطم نلا ةدحولال ديحت
- ليلدلا اذهل تاعبرملا لك ةفاضإ متي شح، تاعبرملا دح
- ظفح ةقطق



- SecureX في AMP نم تانايب ضرع نم ققحت لاولي نم زلا راطال دي دحت



اهحالص او عا طخال فاشكتسا

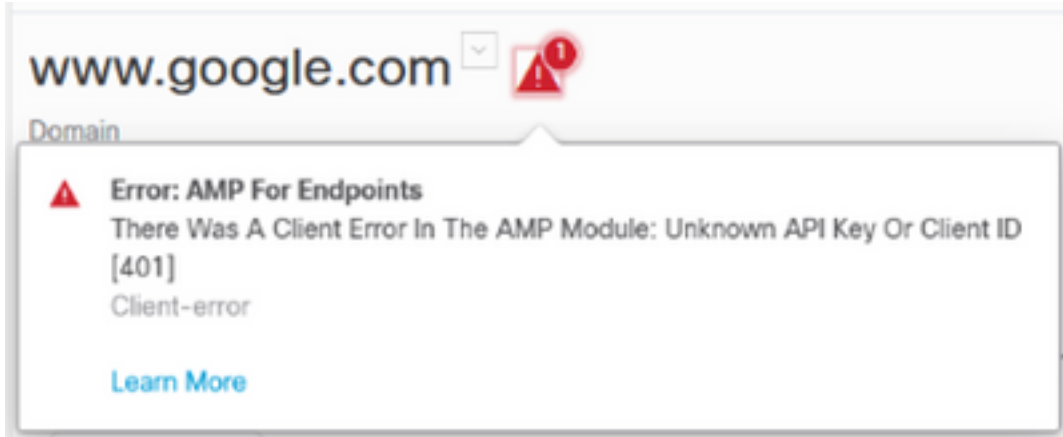
[403] ةباتك لل لوصول قح هيدل سي ل API ليمع

ةجمر ب تاهج اول ةباتك لاول ةعارق لل AMP ةياهن ل طاقن لم اك تل SecureX - AMP ب ل طتي في حضورم وه امك اطح ةلاسر ضرع م تي ،كلذك نكي مل ن ،ةياهن ل طاقن ل (API) تاقبي بط لال ةروصل ل.



[401] لي ماعلا فرعم وأ فرعم ريغ API حات فم: أطخ

ديدهت ةباجتسا" يف قي قحت عارجا مت اذا ةحل اص ريغ تاقي ب طتلا ةجمر رب تاهاو تناك اذا ةروصل يف حضوم وه امك "SecureX".



لواحف، ةح يحيص نكت مل اذا، AMP م كحت ةدحو يف اهدوجو وأ API دامتعا تانايب ةحص نم ققحت ةديج دامتعا تانايب عم.

قي رقب لاصتالا عا جراف، هالعأ ةدراولا تامولعمل ةعجارم دعب تالكشم هجاوت لازت ال تنك اذا م عدلا.

ويدي فال ليلد

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 أ عي مچ ي ف ن ي م دخت سمل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د 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
ى 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