

# اهحال صإو DUO جم دو XDR ءاطخأ فاشك تسأ

## تايوت حمل

[قم دق مل](#)

[ةيساس أال تابلط مل](#)

[تابلط مل](#)

[قم دختس مل تانوك مل](#)

[ةيساس أ تامول عم](#)

## قم دق مل

لم اكتو XDR Device Insights ءاطخأ فاشك تساو لم اكتل نيوك ت تاوطخ دن تس مل اذه فص ي  
اهحال صإو Cisco DUO.

## ةيساس أال تابلط مل

### تابلط مل

ةيلال عيضاوم لابل ءفر عم كي دل نوكت نأب Cisco ي صوت.

- XDR
- DUO
- APIs ب ءيساس أ ءفر عم
- Postman تاق يبط ءجم رب ءه جاو ءادأ

### قم دختس مل تانوك مل

ةيلال ءي دام ل تانوك مل او جم اربل تاراد صإل دن تس مل اذه ي ءراول تامول عم مل دن تس ت

- XDR

ءصاخ ءي لم عم ءئي ب ي ءدو و مل ءزه أال نم دن تس مل اذه ي ءراول تامول عم مل ءاش نإ م ت  
ت ناك اذإ. (يضا رتفا) حوس مم نيوك ت ب دن تس مل اذه ي ءم دختس مل ءزه أال عي مج ت اد ب  
رم أ ي آل لم ت حمل ري ثأ تلل كم هف نم دكأت ف، لي غش تل دي ق كتك ب ش

## ةيساس أ تامول عم

ي ءدو و مل ءزه أال ءدو و م ضرع ءق ي رط ري فوت ي ل ع XDR Device Insights ءزي م لم ع ت  
ءجم دمل تاناي ب ل رداص م نم درجل تاي لم ع جم د ن ع ال صف، كتس سؤ م

ل كي ف كتاناي ب ءي ام حل ءكرشل ءكبش طي حم لوصول نام أ زواج تي و كي ف ظوم نم و ي Duo  
تقو ي ف كتاي وه دي كأت كن كم ي، Duo م ادختس اب. ناكم ي أ ي فو، زاهج ي أ نم، ءق داصم ءل و ام

صصخم ةمئالم نامأ تاسايس عضو ةرادملا ريغو ةرادملا ةزهجالا ةمالس ةبقارم و قجال لهسو نمأ يداحأ لوخد ليحست ريفوت و زاهج ليكو و نودب دعب نع لوصولا نيماؤو كتكرشل ةلوهسو ةعرسب مادختسالا.

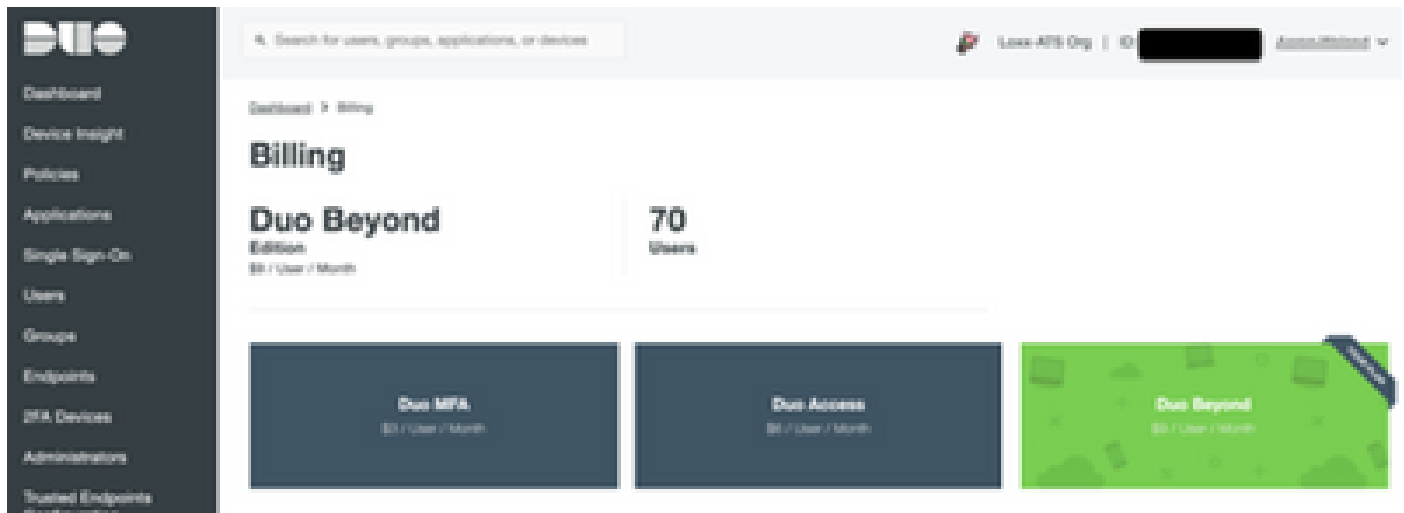
لماكثلا ةدحو لىصافت ةعجارم يجرىف ،نيوكتلا لوح ديزملا ةفرعم يف بغيرت تنك اذا ةيظمنلا.

## اهحال صإو اءاطخال فاشكتسا

تققد عيظتسي تنأ ،لماكث duo و XDR لى عم ةكرتشملا لكاشم تيړت in order to لى API لى اءاؤ ةي لوصولا.

### صيخرتلا يوتسم ةعجارم

- Duo ةرادا ةحول يف صيخرتلا نم ققحتلا
- MFA ، يوتسملا يلاع ثدحأ صيخرت يأ وأ) Duo Beyond و Duo Licensed for Duo Access ةروصلال يف حضوم وه امك (هقبيبطت متي ال Free وأ طقف



### Duo نم تانايب دجوت ال

- يف حضوم وه امك ، ةقداصملا جهن يف Duo Health Agent تانايب مادختسا نم ققحت ةروصلال

**Policy name**  
NPI Policy

**Users**  
New User policy  
Authentication policy  
User location

**Devices**  
Trusted Endpoints  
Device Health application  
Remembered devices  
Operating systems  
Browsers  
Plugins

This section only affects applications protected by Duo's Device Health application.  
[Learn More](#)

**macOS** **Enforcing**

Don't require users to have the app

**Require users to have the app**

Block access if firewall is off.

Block access if FileVault is off.

Block access if system password is not set.

Block access if an endpoint security agent is not running.

**Windows** **Reporting**

- في حضوره وه امك ،ةقداصلما جهن في اب قووثوملا ةياهنلا ةطقن مادختسا نم ققحت ةروصل

**Policy name**  
NPI Policy

**Users**

**Devices**  
Trusted Endpoints  
Device Health application  
Remembered devices  
Operating systems  
Browsers  
Plugins

**Networks**  
Authorized networks  
Anonymous networks

**Authenticators**  
Authentication methods  
Duo Mobile app

**Trusted Endpoints**

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

Allow all endpoints  
Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

**Require endpoints to be trusted**  
Only Trusted Endpoints will be able to access browser-based applications.

Allow AMP for Endpoints to block compromised endpoints  
Endpoints that AMP deems to be compromised will be blocked from accessing browser-based applications.  
**Note:** This option only applies to trusted endpoints.

**Advanced options for mobile endpoints**

**Enable advanced options for mobile endpoints.**  
These options override the policy above only for mobile endpoints.

Allow all mobile endpoints

**Require mobile endpoints to be trusted**

## DUO و Device Insights مادختساب لاصتال رابتخا

لاصتال رابتخا ءانثا رثكأ ةيئرم تاجرخم ىلع لوصحلل PostMan ةادأ مادختسا كنكمي

ةادأ ةفيظونع لاؤس كيذل ناك اذا Cisco لبق نم ةروطم ةادأ سېل Postman :ةظحالم Postman معذب لاصتال ايجري ،

- امك، حيحصل صيخرتلا يوتسم كلتمت ال كنأ ينعي "لوصولا عونمم 40301 أطخلال زمر ةوصولا يف حضورم وه

```
"code": 40301,  
"message": "Access forbidden",  
"stat": "FAIL"
```

- لېوخت ةقيرطك ةقداصم ال دېدحت كنكمي
- ةزهألاب ةمئاق ىلع لوصولل اذه تاقىببطلال ةجرمب ةهجاو اعادتسا مادختسا كنكمي (ةحفصلا يف ةمومعدملا تالاخلال ددعل ىصقألا دحلل تاقىببطلال ةجرمب ةهجاو عجرت)، ةيئانثلا تاقىببطلال ةجرمب ةهجاو تاحفص ميقرت لوح [قئائو](#) ىلع روئعلا كنكمي و (API)

https://

/admin/v1/endpoints

- تاملعم مادختسا كنكمي) تانئاكلل يلماجالا ددعلا عاجرا متي، لوألا اعادتسالل ةباجتسا ةوصولا يف حضورم وه امك، (ةيئانثلا تاحفصلا ىلع لوصولل دحلل ةهجاو ةحزالا

https://

/admin/v1/endpoints?limit=5&offset=5

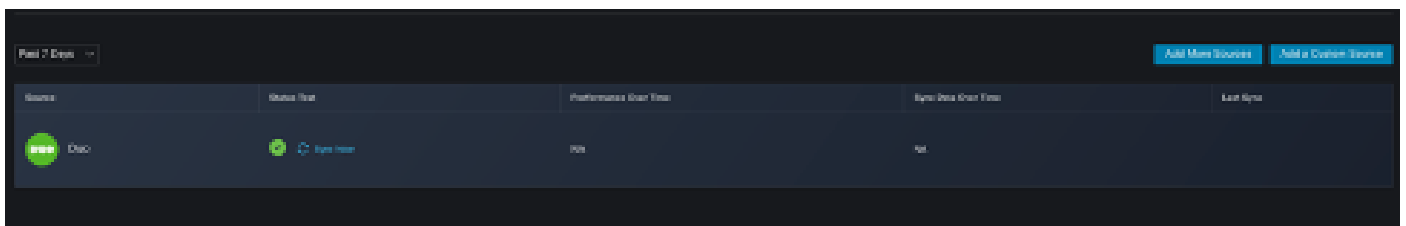
```
"metadata": {  
  "total_objects": 64  
},
```

```
"metadata": {  
  "next_offset": 5,  
  "total_objects": 64  
},
```

## تحصيل نم ققحتلا

تحجان REST API لاصتا ةلاح ةيؤر كنكمي، XDR زاغ يؤر يلا ردصمك DUO ةفاضل درجمب

- ةئيبل ةقيدص ةلاحلاب REST API لاصتا ةدهاشم كنكمي
- ةروصل ي ف حضورم وه امك، ةيلوالا ةلمكلا ةنمازمل ليغشتل نألا ةنمازمل يلع طغضا



نم HAR تالچس عمج يچري، DUO جم دو XDR زاغ يؤر عم ةلكشملا رارمتسلا ةلاح ي ف  
اقم ع رثكأ لي لحت ءارجلا TAC مع دب لاصتالا وضرعتسمل

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء 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 ةللخت. فرتمة مچرت مء مء دقء ةللأل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل