

# ديربل زاہج لم اکتو XDR ءاطخأ فاشكتسأ اهحالصإو (اقباس ESA) نمآلآ ينورتكلإلآ

## تايوتحملآ

[عمدقملآ](#)

[ةيساسألآ تابلطتملآ](#)

[تابلطتملآ](#)

[عمدختسملآ تانوكملآ](#)

[ةيساسأ تامولعم](#)

## عمدقملآ

و XDR ءاطخأ فاشكتسأ ةيفيكيو يساسأ ليلحت ءارجإل ةمزاللآ تاوطخلآ دننتمسملآ اذه فصبي  
اهحالصإو نمآلآ ينورتكلإلآ ديربلآ زاہج لم اکت ةدحوو Insights.

## ةيساسألآ تابلطتملآ

### تابلطتملآ

ةيلالآ عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت:

- XDR
- نامألآ تامدخ لدابت
- نمآلآ ينورتكلإلآ ديربلآ

### عمدختسملآ تانوكملآ

ةيلالآ ةيداملآ تانوكملآ و اجماربلآ تارادصلآ لآ دننتمسملآ اذه يف ةدراولآ تامولعمملآ دننتمس:

- نامألآ تامدخ لدابت
- XDR
- جم انربلآ رادصلآ لىل ع C100V نمآلآ ينورتكلإلآ ديربلآ 13.0.0-392

ةصاخ ةيلمعم ةئيبي يف ةدووملآ ءزهجالآ نم دننتمسملآ اذه يف ةدراولآ تامولعمملآ ءاشنإ مت  
تناك اذإ. (يضارتفا) حوسمم نيوكتب دننتمسملآ اذه يف عمدختسملآ ءزهجالآ عيمج تآدب  
رمأ يأل لم تحملآ ريثأتلل كمهف نم دكأتف، ليغشتلآ ديقتك تكبش.

## ةيساسأ تامولعم

ديربلآ نامأ زاہج مساب اقباس فورعملآ) Cisco نم نمآلآ ينورتكلإلآ ديربلآ نامأ زاہج رفوي  
اهحالصإو اهرطحو تاديدهتلآ فاشكتكال تاديدهتلآ ةيامل عمدقتم تاناکم (ينورتكلإلآ)

مادختساب لقنل اءانثأ ةمهمل تامولعمل نيمأتو تانايبلا نادقف عنمو عرسأ لكش ب "نمآلا ينورتكلال دبرل زاغ" ةيظمنلا ءحول رفوت، اهنوك ت درجم بو. لم اش ريفشت كنكمي. ةبقارملا تاوآب ةنرتقم ليرصافت

- يف ةددعتم ةزهجأ نم تانايبلا لئاسرلا عبتتو ينورتكلال دبرل ريراقت ضرع كتسسؤم
- لئاسرلا تاراسمو ينورتكلال دبرل ريراقت يف تظحول يتلا تاديدهتلا ديحت اهحيصتو اهيف قيقتحلالو
- تاديدهتلا ةهجاومل اهب يصوملا تاءارجلال ريفوتو ةعرسب ةددحمل تاديدهتلا لحب مق ةددحمل
- رخألا ةزهجالا نيب تامولعمل نواعت نيكمتو، قيقتحلال ظفحل تاديدهتلا قيثوت

حمسي (SSE). نامآلا تامدخ لدابت مادختسا نمآلا ينورتكلال دبرل زاغ ءحول لم اءت بلطتي لوصولل اءيرص انذا رفوتو Exchange عم ليجستلاب نمآلا ينورتكلال دبرل زاغ SSE ةلجسمل ةزهجالا ل.

ءحول ليرصافت [انه](#) ةلاقملا هذه ءعجارم يءريف، نيوكتلا لوح ديزملا ءفرعم يف بءرت تنك اذا لءاكتلا.

## اهحالص او ءاطخألا فاشكتسا

كنكمي، نمآلا ينورتكلال دبرل زاغ لءاكتو اءحالص او ءعئاشلا XDR ءاطخأ فاشكتسال تاوطلخا هذه نم ققحتلا.

تامدخ لدابت ءباوب و XDR لءدم يف نمآلا ينورتكلال دبرل زاغ ضرع مءي ال نامآلا

ءباجتسال تامدخ نيكمت نم ءكألا يءريف، SSE ءباوب يف اضورعم كزاهج نكي مل اذا امك، تامدخال نيكمتو، ءباحسلا تامدخ للاقنالو، SSE ءباوب يف ءاءالو XDR تاديدهتل هاندأ ءضوم وه

Cloud Services for  

Cisco SecureX threat response

Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.



Eventing

Eventing allows you to collect and view events in the cloud.



## ليجستل زيمملا زمرلا نمآلا ينورتكلإلا ديربلا بلطي ال

وأ Cisco XDR / Threat Response ةمدخ نيكم تدرجم ،تاريغتلا ذيفنت نم دكأتلا يجرى ينورتكلإلا ديربلا" في "ةباحسلا ةمدخ" مسق يلع تاريغتلا قيبطت متي نل ،كلذ فالخ هاندأ ةروصلارظنا ،"نمآلا

### Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Cisco SecureX / Threat Response:	Enabled
Cisco SecureX / Threat Response Server:	RAM (api-see.cisco.com)
Connectivity:	Proxy Not In Use
<a href="#">Edit Settings</a>	

Cloud Services Settings	
Status:	The Cisco SecureX / Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

## ةيحلصللا يهت نم وأ حل اص ريغ زيمم زمر ببسب ليجستلا لشف

ةيحلصللا يهت نم وأ حيحص ريغ زيمم زمر ببسب ليجستلا لشف :أطخلا ةلاسر ترهظ اذا نم XDR تاديدهت لل ةباحستلا ةباوب مادختساب زاهلل حل اص زيمم زمر مادختسا نم دكأت في حضورم وه امك ،نمآلا ينورتكلإلا ديربلا (GUI) ةيموسرلا مدختسملا ةهجاو في "Cisco هاندأ ةروصللا

## Cloud Service Settings

**Error** — The registration failed because of an invalid or expired token. Make sure that you use a valid token when registering your appliance with the Cisco Threat Response portal.

Cloud Services	
Threat Response:	Enabled
<a href="#">Edit Settings</a>	

Cloud Services Settings	
Registration Token: ⓘ	<input type="text"/>
<a href="#">Register</a>	

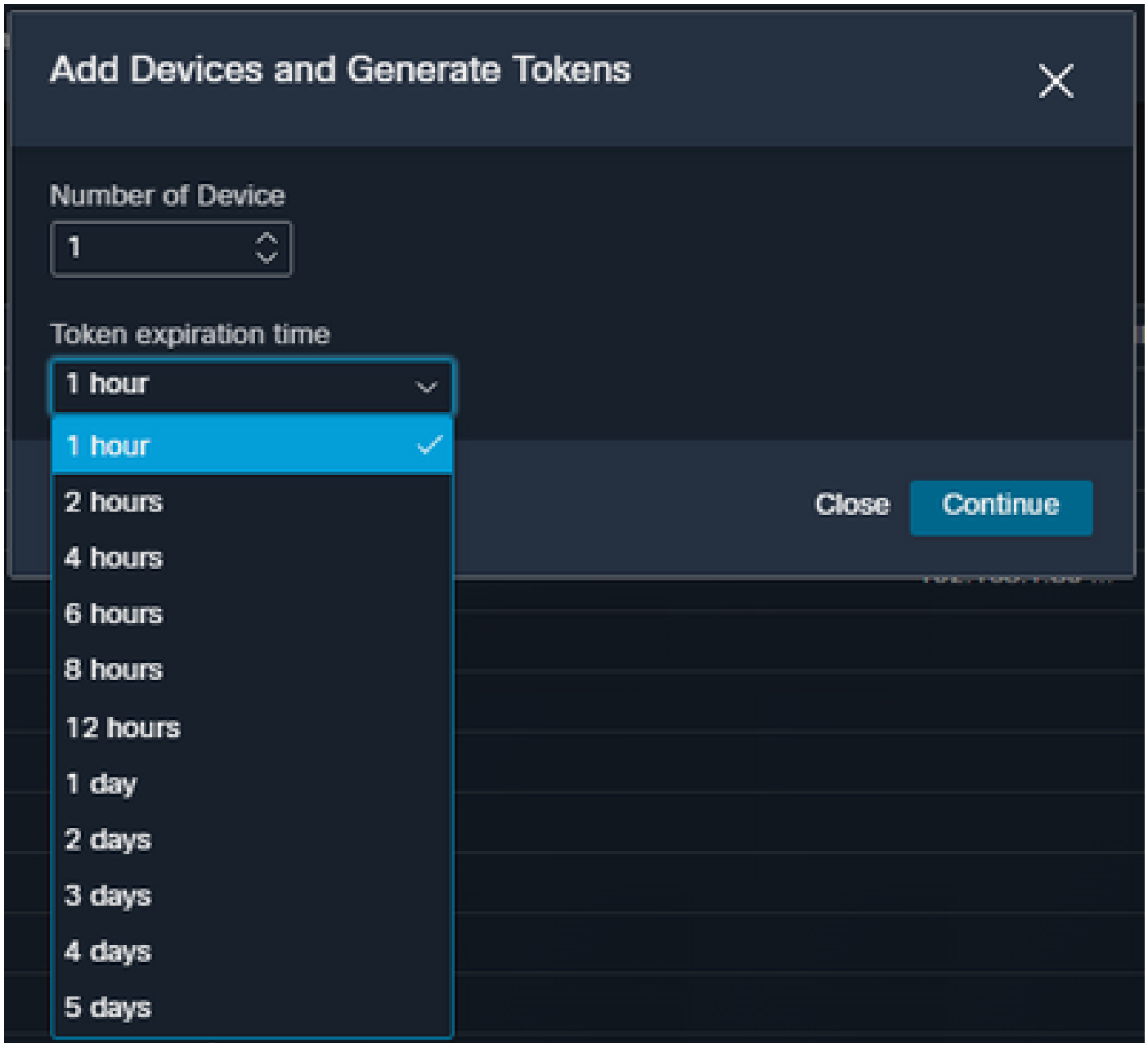
ةح حصل الة با حسل ال نم زيمم ال زم رل اشن ا نم دكأ ال اءرل:

زيمم ال زم رل اشن ا ك ل ع ف ، نم آل ا ينورت كل ال ا ل ا ل ا ل ا ل ا ل (EU) ا ب و ر أ ة با ح س م د خ ت س ت ت ن ك ا ذ ا  
نم <https://admin.eu.sse.itd.cisco.com/>

ا شن ا ك ل ع ف ، ينورت كل ال ا ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل (NAM) ن ي ت ك ي ر م أ ل ا ة با ح س م د خ ت س ت ت ن ك ا ذ ا  
نم زيمم ال زم رل ا <https://admin.sse.itd.cisco.com/>

ابواب SSE) نام ال ا تام د خ ل د اب ت ة با و ب:	NAM: <a href="https://admin.sse.itd.cisco.com/">https://admin.sse.itd.cisco.com/</a> ا ب و ر أ ل ا دا ح ت ال ا ل ا <a href="https://admin.eu.sse.itd.cisco.com/">https://admin.eu.sse.itd.cisco.com/</a>
ابواب Cisco نم XDR ة با و ب	NAM: <a href="https://XDR.us.security.cisco.com/">https://XDR.us.security.cisco.com/</a> ا ب و ر أ ل ا دا ح ت ال ا ل ا <a href="https://XDR.eu.security.cisco.com/">https://XDR.eu.security.cisco.com/</a>
ا ب و ر ا ل ر ب ع XDR / ا ت ا د ي د ه ت ل ل ة با ح ت س ال ا م دا خ Cisco نم نم آل ا ينورت كل ال ا ل ا ل	NAM: api-sse.cisco.com ا ب و ر أ ل ا دا ح ت ال ا ل ا api.eu.sse.itd.cisco.com

ة م ئ ال م ر ث ك ال ا ت ق و ل ا د د ح) ة ح ال ص ا ه ت ن ا ت ق و ه ل ل ي ج س ت ل ل زيمم ال زم رل ا ن ا اض ي ا ر ك ذ ت  
ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ، (ت ق و ل ا ي ف ل م ا ك ت ل ا ل ا م ك ا ل



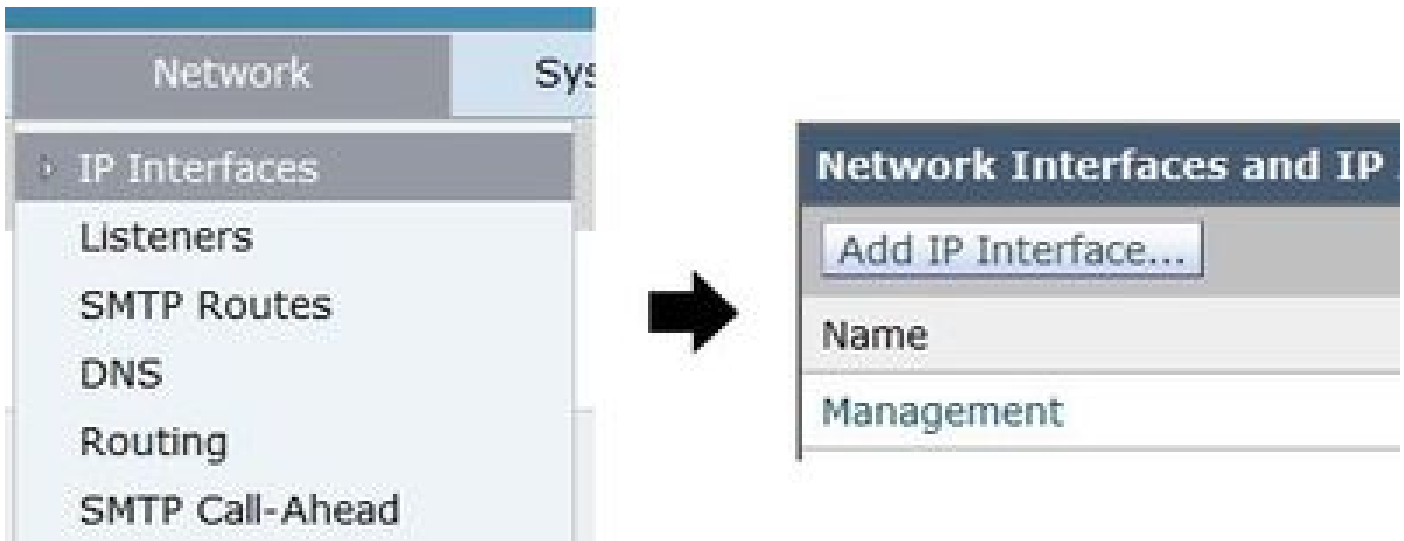
نمآلای نورتكلإلای دیربلا ةدحو لوح تامولعم XDR تامولعم ةحول ضرعت ال

اموي 90 رخآ ىلإ ةريخألأ ةعاسلا نم ،ةحاتملا تاعبرملا يف عسوأ ينمز قاطن ديدحت كنكمي هاندأ ةروصلا يف امك .

Last Hour ^

- Last Hour
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last 60 Days
- Last 90 Days

نم ةزيملا هذه نيوكتب مق ،دادعتسالال عضويف ةنمآينورتكلال ديرب ةلاسرىلع لوصحلل > ةكبشلالىللقننا ،ةنمآلالينورتكلالال ديربالا ةباوبل (GUI) ةيموسرلالمدختسملال ةهجاو امك ، HTTPS و HTTP نيكمتب مقو ، AsyncOS تاقيبطت ةجرمب ةهجاو > ةرادالال ةهجاو > IP تاهجاو ةروصلاليف حضوموه .



AsyncOS API	
The Next Generation portal of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerconfig command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.	
<input checked="" type="checkbox"/> AsyncOS API HTTP	6080
<input checked="" type="checkbox"/> AsyncOS API HTTPS	6443

نيوكتلا اذه ءارجا مزلي ،(ةباحسلاىل دننتمالالينورتكلالال ديربالا) CES ل ةبسنلاب لوصولابلطتيوهو ،نمآلالينورتكلالال ديربالل TAC سدنهم ةطساوبيفلخال فرطالانم ةرثأتمال CES ب صخال معدلا قفنلىل .

## ةحصلالانم ققحتلا

لاصتا ةلاحي ةيؤر كنكمي ،زاهجالىؤرىل رصمك نمآلالينورتكلالال ديربالا ةفاضل درجمب ةحجان REST API .

- ةئيبلا ةقيدص ةلاجال REST API لاصتا ةدهاشم كنكمي
- ةروصلاليف حضوموه امك ،ةيلوالال ةلماكلال ةنمازمال ليغشتل نآالال ةنمازمالىلع طغضا



## Secure Email Appliance

The Cisco Secure Email Appliance (formerly Email Security Appliance) provides advanced threat protection capabilities to detect, block, and remediate threats fast...

Free Trial

Get Started

هذه ةعج ارم ىچري ،نم آلا ينورتك لال ال ديرب ل زاهج لم اكتو XDR عم ةلكشم لارارمت سا ةلا ح يف اق م ع رثك أ ليلحت ءارج ال TAC م ع دب لاصتال او ضرعت سمل ال نم HAR تال جس عم جل [ةلاقم ليا](#)

### ةلص تا ذ تامول عم

- [ديرب ليا لم اكتو XDR ويديف](#) يف ةلاقم ل هذه يف ة دراو ل تامول عم لىل ع روثع ل كنكم ي [نم آلا ينورتك لال ال](#).
- [لنه](#) تاجت نم ل لم اكت تاي لم ع ني وكت ةيفي ك لوح ويديف ع طاقم لىل ع روثع ل كنكم ي
- [Cisco Systems - تادنت سمل او ينقت ل مع دل](#)



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 ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوءو تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل