

- Cisco نم نامأل تامدخ لدابت
- ESA C100V رادصلال جم انرب ىلع 13.0.0-392

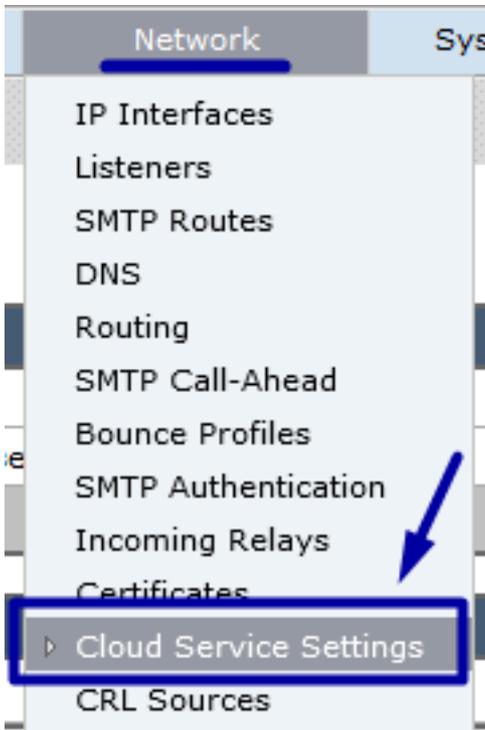
ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسملا اذ ف ةدراولال تامولعمل ءاشنإ م تناك اذإ. (يضا رتفأ) حوسمم نيوكتب دنتسملا اذ ف ةمدختسملا ةزهجالل ءيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

نيوكتلا

ديربلا نامأل يره اظلا زاهجال ىل لوخدلا ليحستب مق، ESA و لمكتلاب صاخال CTR نيوكتل ةيلالاتل ةعيرسلا تاوطخلل عبتا و نيورتكلال:

ةباحسلا ةمدخ تاداعل > ةكبش ىل لقتنا 1. ةوطخل

تيرأر in order to، ةباحسلا ةمدخ تاداعل > ةكبش قاي سلا ةمئاق ىل لقتنا، ESA ل ي ف نإ ام ةروصلال ي ف حضوم وه امك (نكمم / لطمع) ةباجتسالال ةلاح ديدهت يلاحل



تاداعلال ريرحت ىلع رقتنا 2. ةوطخل

ىلع تقطوط، ةمسلا تنكم ESA، ي ف تاديدهتلل ةباجتسالال ةزيم تزجع نأل ىتح ةروصلال ي ف حضوم وه امك تاداعلال ريرحت:

Cisco C100V
Email Security Virtual Appliance

Email Security Appliance is getting a n

Monitor Mail Policies Security Services Network System Administration

Cloud Service Settings

Cloud Services	
Threat Response:	Disabled
Threat Response Server:	No Server is set.

Edit Settings

Cloud Services Settings	
Status:	Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.

تاديدهت لل ةباجتسالال م داخو ني كمت راي تخالال ةناخ ددح 3. ةوطخالال

هاندأ ةروصلال ةعجارم ءاچرلا ، "تاديدهت لل ةباجتسالال م داخ" رتخأ م ث ، "ني كمت" راي تخالال ةناخ ددح

Cloud Service Settings

Edit Cloud Services

Threat Response:	<input checked="" type="checkbox"/> Enable
Threat Response Server:	AMERICAS (api-sse.cisco.com) AMERICAS (api-sse.cisco.com) EUROPE (api.eu.sse.itd.cisco.com)

Cancel Submit

وه تاديدهت لل ةباجتسالال م داخ ب صاخال URL ناو نعل ي ضار تالال دي دحتال نو كي : ةظحالام ةمئاقال قوف رقنا ، ةب وروالال تاك رشل لل ةب سنللاب (api-sse.cisco.com). اب وروا رتخاو ةلد سنملا (api.eu.sse.itd.cisco.com)

اهذي فننتو تاريغي تالال لاسرلا 4. ةوطخالال

ةهجاو شي دحت مت اذنا لال . هقبي بطتو ريغي غت ي اظ فح لجا نم ، اهذي فننتو تاريغي تالال لاسرلا مزلي ةروصلال ي ف حضوم وه امك ، لمكتالال لي جستل لي جستل زيمم لي جستل زمر بل ط متي ف ، ESA هاندأ .

اهتيرجال ي تالال تاريغي تالال ذي فننت مت : حاجن ةلاسر ةدهاشم كنكمي : ةظحالام

Uncommitted Changes

Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Comment (optional): Enabling CTR

Cancel Abandon Changes Commit Changes

Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

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

Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

في بولطم لا ليحست لا زمر عاشن و CTR ةباوب يلى لوخدلا ليحست 5. ةوطخلا ESA

1.- ةدهاشم عاجرلا ، ةزهجالا ةرادا > ةزهجا > تادحو يلى لوقتنا ، CTR ةباوب يلى لخدت نا درجم ب- ةةلاتلا ةروصللا

The screenshot shows the Cisco Visibility AMP web interface. The browser address bar displays <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation menu, the breadcrumb 'Settings > Devices' is visible. The 'Devices' page content includes a 'Settings' sidebar with 'Your Account', 'Devices' (highlighted with a blue box and arrow), 'API Clients', and '> Modules'. The main content area shows 'Devices' with a 'Manage Devices' button (highlighted with a blue box and arrow) and a 'Reload Devices' button. Below the buttons is a table with columns 'Name' and 'Type'.

2.- يلى هلوصلو درجم ب (SSE) نامألا تامدخ لدابت يلى كهيجوت ةداعإ ةزهجالا طابترأ ةرادا موقت - ةروصللا في حضورم وه امك ةزيمملا تامالعال عاشن و ةزهجا ةفاضل زمرلا قوف رقنا ، كانه

Devices for Sourcefire Support

Device Name / ID

0 Rows Selected

Add Devices and Generate Tokens



	1/4	#	Name ^	Type	Versio...	Status	Description	Actions
--	-----	---	--------	------	-----------	--------	-------------	---------

3- إلى خسن" قوف رقنا ،زيمملا زمرلا عاشنإ درجمب ،زيمملا زمرلا عاشنإل "ةعباتم" قوف رقنا 3- .ةروصلال يف حضوم وه امك ،"ةظفال

ديدتو (100 إلى لصي امو 1 نم) اهتفاضإ ديرت يتلا ةزهجالأ ددع ديدحت كنكمي :حيملت و تاعاس 8 و تاعاس 6 و تاعاس 4 و تاعاس 2 و ةعاس 1) زيمملا زمرلا ةيحالص اهتنا تقو (مايأ 05 و مايأ 04 و مايأ 03 و موي 02 و موي 01 و ةعاس 12

Add Devices and Generate Tokens

Number of devices: 1 (Up to 100)

Token expiration time: 1 hour

Buttons: Cancel, Continue

Add Devices and Generate Tokens

The following tokens have been generated and will be valid for 1 hour(s):

8e789d60b6ced63875353d177f25ab0e

Buttons: Close, Copy to Clipboard, Save To File

ESA يف (CTR لخدم نم هؤاشنإ مت يذلا) ليجستلا زمر قصلال 6 ةوطخال

ESA يف "ةباحسلا تامدخ تادادعإ" مسق يف هوقصلا ،ليجستلل زيمملا زمرلا عاشنإ درجمب هاندأ ةروصلال.

يف كب صاخلال زاهجال ليجستل بلط ادب مت :حاجن ةلاسر ةدهاشم كنكمي :ةظحالم ضعب رورم دعب ةحفصلا هذه إلى ىرخأ ةرم لقتنا .Cisco تاديدهتل ةباجتسالال ةباب زاهجال ةلاح نم ققحتلل تقولا

Cloud Service Settings

Cloud Services

Threat Response: Enabled

Threat Response Server: AMERICAS (api-sse.cisco.com)

Edit Settings

Cloud Services Settings

Registration Token: 8e789d60b6ced63875353d177f25ab0e

Register

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

Amp AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#) [Learn More](#) - [Free Trial](#)

Esa Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#) [Learn More](#)

رابطہ اور (اقباس لچسمل زاہل دح) لچسمل زاہل، ڈیٹمنل ڈحو ل مسا: لوقح لخدأ - 3. ةروصلل ىف حضوم وه امك، ظفحل او، (ماي، اب) بل لطلل ىنمزل.

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

Add New Email Security Appliance Module

Module Name*

Registered Device*

esa03.mex-amp.inlab
Type ESA
ID 874141f7-903f-4be9-b14e-45a7f34a2032
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

Quick Start

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

Prerequisite: ESA running minimum AsyncOS 13.0 0-314 (LD) release.

Note: Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

1. In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
2. Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
3. Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
4. Specify the token expiration time (the default is 1 hour), and click **Continue**.
5. Copy the generated token and confirm the device has been created.
6. Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
7. Complete the **Add New Email Security Appliance Module** form:
 - **Module Name** - Leave the default name or enter a name that is meaningful to you.
 - **Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - **Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
8. Click **Save** to complete the ESA module configuration.

ةحصلل نم ققحتل

كنا نكمي يذلاو، رابتخالل ينورتكلل دبر لاسرا كنكمي، ESA و CTR لم اكن نم ققحتلا لجا نم دبر نع ثحبلاو، لئاسرلا بقعت > ةشاشلا لىل حفصتلاو، كب صاخلا ESA نم هتيؤر اضيا ينورتكلل دبرلا عوضوم مادختساب حيشرتلاب تمق، ةلاجال هذه يف. ينورتكلل رابتخالل هاندأ ةروصك

Cisco C100V Email Security Virtual Appliance

Monitor | Mail Policies | Security Services | Network | System Administration

Message Tracking

Search

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With []

Envelope Recipient: ? Begins With []

Subject: Begins With [test test]

Message Received: Last Day Last Week Custom Range

Start Date: [05/13/2020] Time: [13:00] and End Date: [05/14/2020] Time: [13:42] (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

Results

Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com
 RECIPIENT: testingBren@cisco.com
 SUBJECT: test test
 LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

تاطحال مضعب مادختساو، ققحتلل حفصتلاو، ققحتل اراجا كنكمي، CTR ةابوب نم، نالا ةروصلا يف حضوم وه امك، ينورتكلل دبرلا

Threat Response Investigate Snapshots Incidents **Alerts** Intelligence Modules

1 Target 1 Observable 0 Indicators 0 Domains 0 File Hashes 0 IP Addresses 0 URLs 1 Module

Investigation 1 of 1 enrichments complete

email_subject:"test test"

Investigate Clear Reset What can I search for?

Relations Graph Filters: Show All, Expanded Showing 6 nodes

IP Target Email Email Subject test test Cisco Message ID 8 Domain cisco.com Email Address mgmt01@cisco.c...

Sightings

My Environment Global 1 Sighting in My Environment First Seen: May 14, 2020 13:23:57 UTC Last Seen: May 14, 2020 13:23:57 UTC

Module enriched this investigation esa03 ----- Email Security Appliance 1 Sighting, 0 Judgements

Observables

test test

Email Subject My Environment Global 1 Sighting in My Environment First Seen: May 14, 2020 13:23:57 UTC Last Seen: May 14, 2020 13:23:57 UTC

Sightings (1)

Module	Observed	Description	Confidence	Severity	Details
esa03 ----- Email Security Appliance	9 hours ago	Incoming m essage (Del ivered)	High	Low	

امك ىرأل ينورتكلإل دىربلأ ةظحال م طاقنل ةغىصلال سفن مادختسا كنكمى :حيملت ةروصلال فى لىل

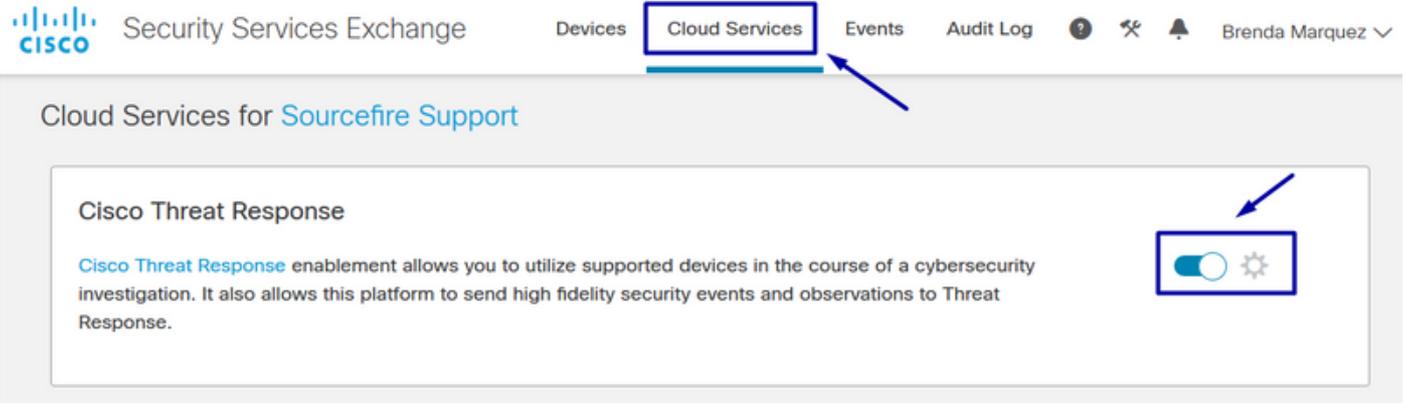
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

اهحالصلو ءاطأل فاشكتسا

لاصلتالا كنكمى فى SMA ربع كب ةصاأل ESA ةزهأ ةرادب تمق اذا وأ CES ءالمع دأ تنك اذا ل كب صاأل SMA لىغشت نم دكأتلا ءاأل SMA ربع طقف تاىدهتلل ةباجتسالاب ESA جم دب تمق و SMA مادختساب كب صاأل ESA ةرادب مقتمل اذا لىل ءا وأ AsyncOS 12.5 لىل ءا رادصلال فى هنا نم دكأت فى ةرشابم

CTR ةبواب فى رهاظ رىغ ESA زاآ

ةدحول ةافاضا ءانثا لدسنم لاجسمل زاوجل ايف كب صاخلا ESA زاغ ضرع م تي مل اذا
CTR لاقتنا يفو SSE يف CTR نيكم ت نم دكأتلا يجرى ف CTR ةبواب يف ESA ةيظمنلا
ةباحسل تامدخ للاقنا SSE ةبواب يف م ث ،ةزهجالا ةرادا > ةزهجالا > ةيظمنلا تادحولا ل
:هاندا حضوم وه امك CTR نيكم ت و



ةيوروبوالا ءاضفلا ةلاك و نم تانايب قيقتل ةنجل قيقت رهظي ال

يلي امم دكأتلا يجرى:

- الءا اهتظالم تم تي تال ي نوركتلالا ديربلا تانايب رهظت ،حيحص قيقتل ةلمج ءانب
قيقتل مسق يف
- نيب) ةبسانملا "تاديدهتلل ةباحتسالالا ةكبش وا مداخ" رايخاب تمق دول
(ابوروا/نيكتيرمألا).

ليجستل زيمملا زملا ESA بلطي ال

نلف ال او ،"تاديدهتلل ةباحتسالالا" نيكم ت م تي امدنع ،تاريغتلا ذيفنت نم دكأتلا يجرى
ESA يف "تاديدهتلل ةباحتسالالا" مسق لعل تاريغتلا قيقت م تي

ةيصالصلا يهتنم واصل ريغ زيمم زمر ببسب ليجستلا لشف

:ةحيصل ةباحسل نم زيمملا زملا ءاشنا نم دكأتلا ءارلا

نم زيمملا زملا ءاشناب مقف ،ESA ل (EU) ابوروا ةباحس مدختست تنك اذا

<https://admin.eu.sse.itd.cisco.com/>

نم زيمملا زملا ءاشناب مقف ،ESA ب ءصاخلا (NAM) ةباحس مدختست تنك اذا

<https://admin.sse.itd.cisco.com/>

ةمءالم رثكالل تقولا دح) ةيصالص ءاهتنا تقو هيدل ليجستل زيمملا زملا نا اضيأ ركذت
(بسانملا تقولا يف لمكأتل لامكأل

ةلص تاذا تامولعم

- [تاديدهتلل ةباحتسالالا](#) ويدي في لاقملا اذه يف ةدراولا تامولعمل لعل روثعلا كنكمي
[ESA لملك و Cisco](#).
- [Cisco Systems - تادنتسمل او يبقنقتل معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م دخت س م ل 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 ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا 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 ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء 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 ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا