## ەئاطخأ فاشكتساو Cisco XDR نيوكت رادصإلا نمآلا ةيامحلا رادج مادختساب اەحالصإو 7.2

### تايوتحملا

<u>قمدقملاا</u> <u>قمدقملاا</u> <u>تابلطتملاا</u> <u>قمدختسملاا تانوكملاا</u> <u>قيفلخلاا</u> <u>نيوكتلاا</u>

### ةمدقملا

ةيامحلا رادج جمد عم اهحالصإو هئاطخاً فاشكتساو Cisco XDR جمد ةيفيك دنتسملا اذه فصي نم نمآلا قيامحلا رادج يلع Cisco نم آلا

#### ةيساسألا تابلطتملا

#### تابلطتملا

:ةيلاتانا تاعوضوملا ةفرعمب Cisco يصوت

- Firepower (FMC) ةرادإ زكرم
- Cisco نم نمآلا ةيامحلا رادج •
- روصلل ةيرايتخالا ةيضارتفالا ةاكاحملا
- FMC و نمآلا ةيامحلا رادج صيخرت بجي •

#### ةمدختسملا تانوكملا

- Cisco Secure Firewall 7.2
- Firepower (FMC) 7.2 ةرادإ زكرم
- SSE) نامألا تامدخ لدابت
- Cisco نم XDR
- Smart صيخرتلا ةباوب •
- انم تاديدەتلل ةباجتسالا Cisco (CTR)

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمەف نم دكأتف ،ليغشتلا ديق كتكبش.

### ةيڧلخلا

تادحو عم نمآلا ةيامحلا رادج اهب لماكتي يتلا ةقيرطلا ىلع تارييغت 7.2 رادصإلا نمضتي XDR نم XDR تادحو ةيقيسنتو Cisco نم XDR تادحو تيقيسنتو

ةزيملا	فصولا
نمازت ،نسحملا Cisco XDR لماكت XDR.	We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new Integration > SecureX page, click Enable SecureX, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the systems's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on System > Integration > Cloud Services. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The management center also now supports SecureX orchestration—a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration.

رادصإلا اذه يف ةنمضملا تازيملا عيمج نم ققحتلل ةلماكلا <mark>رادصإل تاظحالم</mark> 7.2 ىلإ عجرا.

#### نيوكتلا

:كتىيب ىلع اەب حومسم ەذە URL نيوانع نأ نم دكأت ،لماكتلا ءدب لبق

ةيكيرمالا ةقطنملا

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

يبوروألا داحتالا ةقطنم

• api.eu.sse.itd.cisco.com

• eventing-ingest.eu.sse.itd.cisco.com

نابايلاو ئداەلاو ايسآ ةقطنم

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

يت لم اكتال لجس عدبل .1 ةوطخلا BMC. يت التقطنما الماكتال الجس عدبان .1 قوطخلا Gisco XDR، يتال التقطن التقيي ال وأ EU وأ US المجال المتالي التقيي التقام التقيي التقام التقيي التقوي التقوي التقوي التقوي التقوي التقوي التقوي XDR، تي كمت ددح مث التقام التقوي ا

þ	Firew Integration	vall Management Cen	ter <sub>Overview</sub>	Analysis	Policies	Devices	Objects	Integration		Deploy	Q 🚱	٥	🛿 admin 🕶	esco SECURE
	Secu This fea ribbon.	IreX Setup ature allows Secure Firewall M Learn more [3 Cloud Region	Aanagement Center to int This setting determiner to the cloud, as well as and Cisco Support Diay Current Region us	tegrate with ot s where event: a data generati gnostics tools -east-1 (US R	ther SecureX : s are sent to, ed by the Cise egion)	Cisco Cloud Support The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. The Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the Management Center from participating in these additional cloud service offerings.  Content of the Cisco Success Network Content of the Cisco Support Diagnostics						and ipating in		
	2	SecureX Enablement	After completing this c the bottom of each pag SecureX is enable configuration for t Enable SecureX [3]	eonfiguration, t ge. Learn more ed for US Regi this change to	he SecureX ri e 🖸 ion. You will n take effect.	bbon will show	v up at ur							
	3	Event Configuration	<ul> <li>Send events to the</li> <li>Intrusion events</li> <li>File and malwar</li> <li>Connection Evention</li> <li>Security</li> <li>All</li> <li>View your Ciscon</li> <li>View your Event</li> </ul>	cloud s re events ents o Cloud config is in SecureX	uration									
	4	Orchestration	Enable SecureX orches workflows that interact Management Center. L	stration to allow with various r earn more E	w SecureX us resources in th	ers to build au ne Secure Firev	tomated wall	w To						Save

. save ديدحتب موقت ىتح ،اەقيبطت متي ال تارييغتلا نأ ظحال

Cisco XDR باسح يف دمتعملا FMC ىلإ كەيجوت ةداعإ متت ،"ظفح" ديدحت درجمب .2 ةوطخلا خيوفت ددح ،(ةوطخلا هذه لبق Cisco XDR باسح ىلإ لوخدلا ليجست بجي) FMC:

# Grant Application Access

Please verify the code provided by the device.

# 21D41262

The application **FMC** would like access to your SecureX account. Specifically, **FMC** is requesting the following:

- casebook: Access and modify your casebooks
- enrich: Query your configured modules for threat intelligence (enrich:read)
- global-intel: Access AMP Global Intelligence
- inspect: Extract Observables and data from text (inspect:read)
- integration: Manage your modules (integration:read)
- notification: Receive notifications from integrations
- orbital: Orbital Integration.
- private-intel: Access Private Intelligence
- profile: Get your profile information
- registry: Manage registry entries (registry/user/ribbon)
- response: List and execute response actions using configured modules
- sse: SSE Integration. Manage your Devices.
- telemetry: collect application data for analytics (telemetry:write)
- users: Manage users of your organisation (users:read)

Authorize FMC

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما