

تامال عال يئاقلا لملعلا ريس نيوكت XDR مادختساب ينورتكلال ديربل

تايوتحمل

[عمدقمل](#)

[سيساسال تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[نيوكتل](#)

[Cisco XDR Exchange](#) نم لمعللا ريس تيبت

[قياهنلا طاقن لزعل لمعل ريس تيبت 1. ةوطخل](#)

[تمتأ دعاق عاشن](#)

[تمتأ دعاق نيوكت 2. ةوطخل](#)

[لمعللا ريس ةفيظونم ققحتل](#)

[لمعللا ريس ذيفنت نم ققحتل 3. ةوطخل](#)

[ينورتكلال ديربل مالعال ديكأت 4. ةوطخل](#)

عمدقمل

ينورتكلال ديربل ربع مالعال لاسرال تمتؤم لمعل ريس عاشن ايفيكن دنتسمل اذه حضوي
ديج ثداح لوح.

سيساسال تابلطتمل

تابلطتمل

دنتسمل اذهل عصاخ تابلطتم دجوت ال

عمدختسمل تانوكمل

ةنيعم ةيدام تانوكموجمارب تارادصا ىلع دنتسمل اذه رصتقي ال

عصاخ ةيلمعم ةئيبي ف ةدوجومل ةزهجال نم دنتسمل اذه في ةدراول تامولعمل عاشن مت
تناك اذ. (يضارتفا) حوسمم نيوكتب دنتسمل اذه في عمدختسمل ةزهجال عيمج تادب
رما يال لمحتحمل ريثاتلل كمهف نم دكأت ف، ليغشتال دي قكتكبش

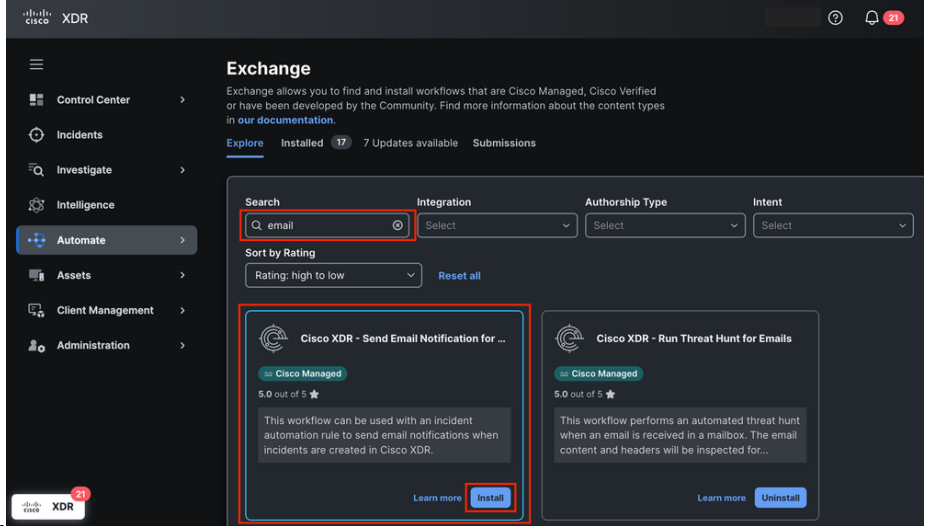
نيوكتل

مالعال لاسرال هطيشتو لمعل ريس نيوكتل ةمزالال تاوطخل ليصف تلاب ليلدل اذه حضوي
وحنلا ىلع تاوطخل هذه ليصافت درتو. ثداح عوقو دنع ايئاقلا ينورتكلال ديربل
يلاتل.

Cisco XDR Exchange نم لمعالجيس تيبثت

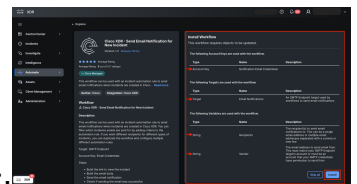
ةياهنلا طاقن لزع لمع ريس تيبتت 1. ةوطخلا

1. Exchange > تمتأى إلى لقتناو Cisco XDR إلى لوخذل ليجستب مق.
2. ثداوخل ينورتكل إلى ديربل ربع مالع لاسرا - Cisco XDR - ىمسمل لمعل ريس نع ثحبا.



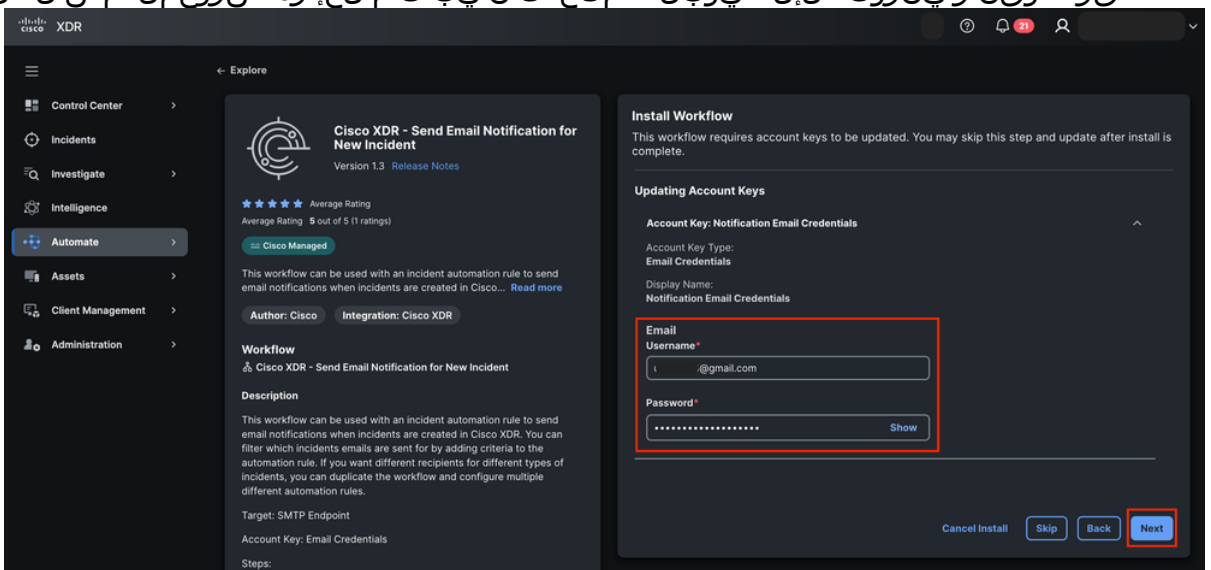
٢٠٠٠

Exchange نم ڀڻو رٽ ڪل لال ڊي ربل راڻا لمع ريس لاس را



3. احي حص لكشب لمعال ريس نيوكتل ةمزالال تامولعمل نم ققحت .
ينورتكللال دبرل ربع لاسرال راطخا لمع ريس لعل ةماع ةرطن

4. نبي عتلى نورتكلىل دىربال دامتعا تانايب مادختساباس حالحي تافم ةئبت قوف رقناو ينورتكلىل دىربال دامتعا تانايب تامالعا وه ضرور عمل مسالا. لىسرمل



ی.ل.ا

لمعلم الريسل باس حل حیاتیات فم

5. مداخلت سباب فدهلا تامول عملانىوكت:

- ينورت كلال دي ربال مالعال دامتعا تانايب :باسحلل حيتافم
- ينورت كلال دي ربال
 - مداخل SMTP: smtp.gmail.com
 - ذفنم SMTP: 587

Cisco XDR - Send Email Notification for New Incident
Version 1.3 [Release Notes](#)

★★★★★ Average Rating
Average Rating: 5 out of 5 (1 ratings)

Cisco Managed

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR.

Author: Cisco Integration: Cisco XDR

Workflow
Cisco XDR - Send Email Notification for New Incident

Description

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR. You can filter which incidents emails are sent for by adding criteria to the automation rule. If you want different recipients for different types of incidents, you can duplicate the workflow and configure multiple different automation rules.

Target: SMTP Endpoint
Account Key: Email Credentials

Steps:

- Build the link to view the incident
- Build the email body
- Send the email notification
- Check if sending the email was successful:
 - If it was, set the workflow result
 - If not, output an error

External Links

[Content Licensing](#) [Developer Community](#)

Contact & Support Information

Install Workflow
This workflow requires targets to be updated. You may skip this step and update after install is complete.

Updating Targets

Target: Email Notifications
Target Type: SMTP Endpoint
Display Name: Email Notifications
Description: An SMTP Endpoint target used by workflows to send email notifications

Account Keys
Use an account key if the target requires authentication.

No Account Keys [?](#)
False

Default Account Keys*

Notification Email Credentials

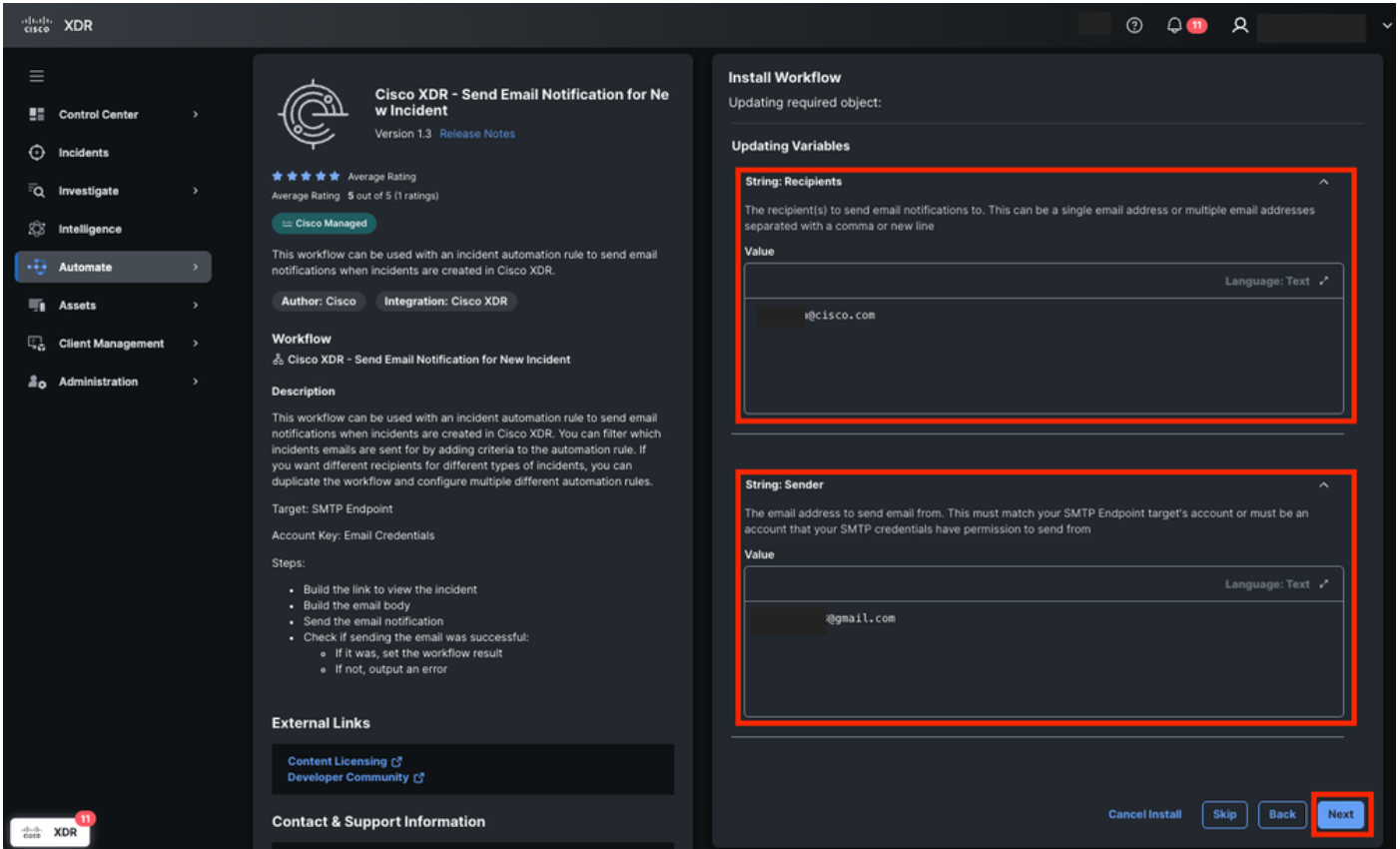
Email
SMTP Server*
smtp.gmail.com
SMTP Port*
587

Protocol
SMTP

Cancel Install Skip Back **Next**

لمعمل ري سل فدهل نيوكتل

1. (اللاتال) Next قوف رونا
2. ل ري غتمل ثي دحت:
 - يي قلم
 - ل س رمل



لمعمل ريسل تاريختم نبيعت

8. يلاتل قوف رقنا .

9. ءءصلا نم ققءءلا ءلاح نم ققءءلل لمعمل ريس ءاي لمع > ءءمءا ءلا لقتنا .

لمعمل ريس ءءص نم ققءءلا ءلاح

ءءمءا ءءءاق ءاشنإ

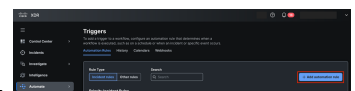
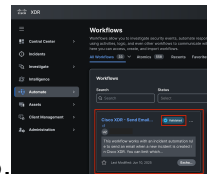
ءءمءا ءءءاق نيوكء 2. ءوطءلا

1. ءالءشملا > ءءمءال مسق ءلا لقتنا .

2. مسا نبيعتو ءءمءا ءءءاق ءافاضا قوف رقنا . ءءءء ءءءاق ءاشنإ .

ءالءشملا نم ءءمءا ءءءاق ءافاضا

3. ءلاح ءافاضا ءلا ءءءال نوء ءءءاملا كنكمي . لءشملا ءورء ءءءو ءءءال ءءءاق ءون ءء . رمال مزلا اءا ءورءال صيصءءب مق . ءءءاقلا هءه ءشني ءءءي أا نمضءي ءالو ، ءءءاق



اه طورشو ةتمتأل ةدعاق عون

ي نورث كل إل دي رب ال ربع مالع إ لاسرا - Cisco XDR يلع يئاق ل لتال لي غشت ال ةدعاق قي بطت 4. ل سرمل او ني مل لت سمل ال تاري غتم ني عت . اق بس م هتي ب ثب تمق دي دج ثداح لمع ريس ل

تاري غتم ني عت و لمع ال ريس يلع ةتمتأل ةدعاق قي بطت

5. ةدعاق ال ظفحب مق .

لمع ال ريس ةفيظو نم ققحت ال

لمع ال ريس ذي فنت نم ققحت ال 3. ةوطخ ال

1. هثودح رظتنا وأ ةدعاق ال طورش عم قفاوتي ثداح عاشناب مق .

Cisco XDR يي دي دج ثداح فاشتك ا مت

Priority	Name	Source	Created	Assigned	Status
4	Malware observed on mobile endpoint	Cisco Secure Endpoint	2020-08-12T11:30:00Z	Assigned	Open

ثدحلا ليصافت ضرعا م ث ثدحلا قوف رقنا 2.

Malware detections on single endpoint



Priority **830** Status **New**

Reported by
Cisco XDR Analytics

on 2025-06-10T20:36:11.917Z

Unassigned

MITRE

Priority score breakdown



830

83

Detection
Risk

10

Asset
Value at Risk

Sources



Cisco Secure Endpoint



[View Incident Detail](#)

اذا ريغت نأ نكمي، كلذ عمو؛ لوألا فشكلا ىلع انب يلوألا شداحل مسا عاشنا متي
شداحل اارثا ىلا ةديدل تامولعمل تدا وأ ةففاض تافاشتك تشدح.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا