

ةطقن لزعل يئاقللتلا لمعلال ريس نيوكت Cisco XDR. مادختساب ةياهنلا

تايوتحملال

[ةمدقملا](#)

[ةيساسالال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلال](#)

[ةنمآلا Cisco ةياهن ةطقن يفلؤلألا نيوكتلال](#)

[جهنللا يفل لزعلال ةزيم نيوكمت: 1.1 ةوطخلال](#)

[ةنمآلا Cisco ةياهن ةطقن عملماكتالال ةحص نم ققحتلال](#)

[لمماكتالال نم ققحتلال: 2.1 ةوطخلال](#)

[Cisco XDR Exchange نم لمعلال ريس تيبثت](#)

[ةياهنلال طاقن لزعل لمعل ريس تيبثت: 3.1 ةوطخلال](#)

[ةتمتأ ةدعاق عاشنلا](#)

[ةتمتأ ةدعاق نيوكت: 4.1 ةوطخلال](#)

[لمعلال ريس ةفيظو نم ققحتلال](#)

[لمعلال ريس ذيفنت نم ققحتلال: 5.1 ةوطخلال](#)

[ةياهنلال ةطقن لزعل ديكأت: 5.2 ةوطخلال](#)

[ةكرتشم ةيضق](#)

[ةنمآلا Cisco ةياهن ةطقن نم لزعلال ةزيم نيوكمت متيمل](#)

ةمدقملا

ديدج ثداحل ةياهن ةطقن لزعل ةتمتأ لمعل ريس عاشنلا ةيفيك دنتسملا اذه حضوي

ةيساسالال تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوتال

ةمدختسملا تانوكملا

ةنيعم ةيдам تانوكم وجومارب تارادصا ىلع دنتسملا اذه رصتقيال

ةصاخ ةيلمعم ةئيب يفل ةدوجوملا ةزهجالال نم دنتسملا اذه يفل ةدراولا تامولعملال عاشنلا مت
تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يفل ةمدختسملا ةزهجالال عيمج تادب
رما يال لمتمحملال ريثأتلل كمهف نم دكأتف، ليغشتلال ديقلكتك بش

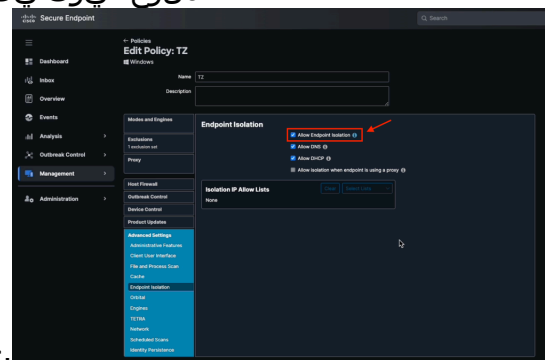
نڨوكتال

اڤئاقلت ةڤاهن ةطقن لزعل هطيشنتو لمع ريس نڨوكتل ةمزالل تاوطخل لڤلدل اذه حضوي لمعل ريس ةتمت اءفطوو Cisco Secure Endpoint عم لماكلل اذفنت متي .ثداح ثودح دنع ڤلالتل وحنل ىلع تاوطخل هذه درتو

ةنمآل Cisco ةڤاهن ةطقن ف ڤلوال نڨوكتال

جهنل ف لزعل ةزيم نڨم ت: 1.1 ةوطخل

1. Cisco نم ةنمآل ةڤاهنل ةطقن ةبواب ىل لوخدل لڤس .
2. تاساڤسل > ةرادل مسق ىل لقتنا .
3. اهلزعل دڤرت ڤتال ةڤاهنل ةطقن ىلع قبطنت ڤتال ةساڤسل ددح .



4. جهنل تادادعا نمض ةزهجال لزعل راڤ نڨم ت نم دكأت .

ةنمآل ةڤاهنل ةطقن جهن نم ةڤاهنل ةطقن لزعل ؤامسل

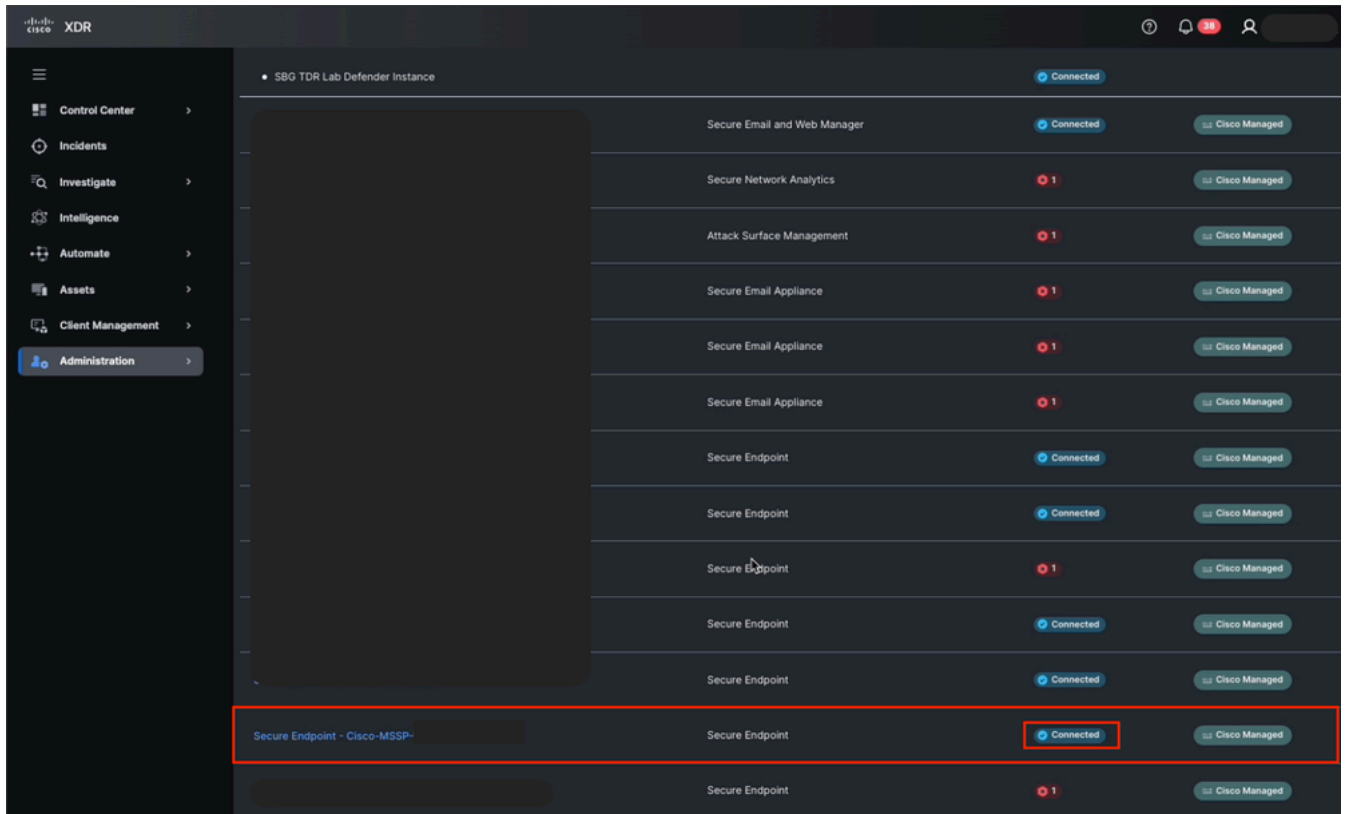
5. رمال مزل اذا جهنل عڤزوتو تارڤڤتال ظفحب مق .

ةنمآل Cisco ةڤاهن ةطقن عم لماكلل ةحص نم ققحتال

لماكلل نم ققحتال: 2.1 ةوطخل

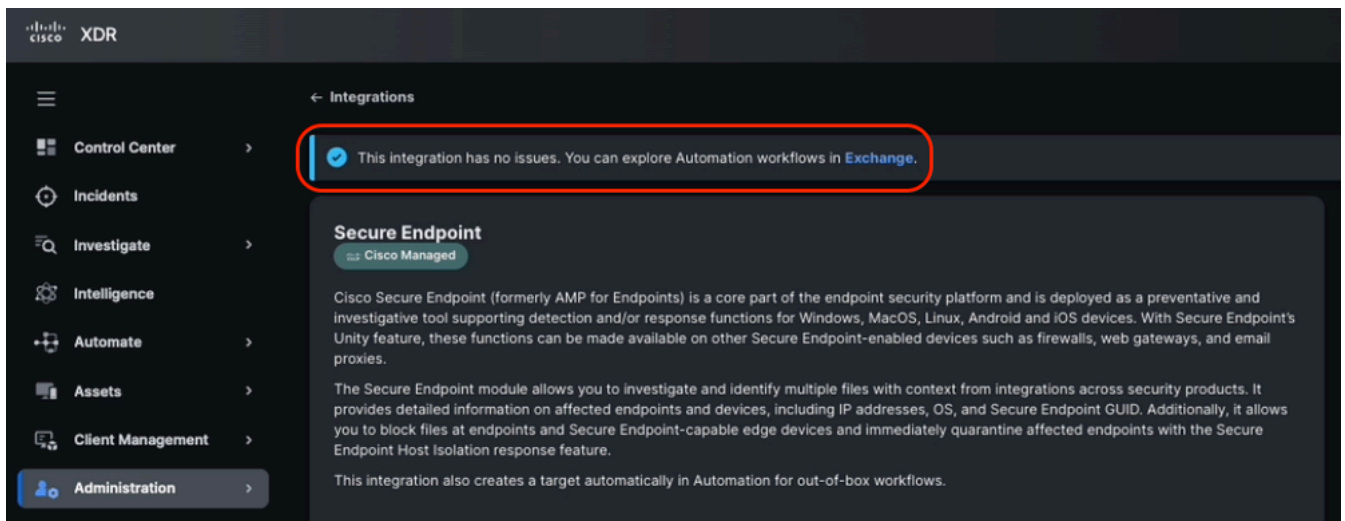
1. Cisco XDR ىل لوخدل لڤس ت .
2. ڤ ةصاا لماكلل تاڤلمع مسق > لماكل تاڤلمع > ةرادل ىل لقتنا .
3. جڤحص لكشب Cisco Secure Endpoint عم لماكلل نڨوكت نم دكأت :

"لصتم" ف لماكلل ةلاح نم ققحت



Cisco XDR. نم ةمآل ةياهنل ةطقن لمكك ةلح

.تاقببطل ةجر رب ةهجاو نيوكك يف ءاطخا دوجو مدع نم دكأت

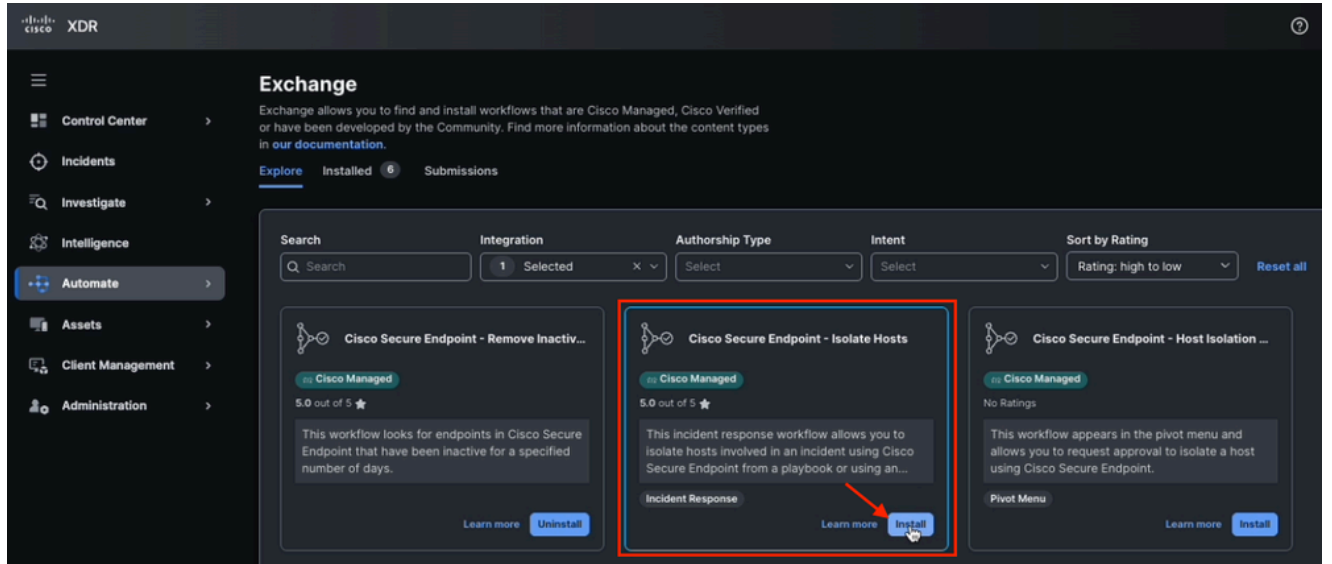


ةمآل ةياهنل ةطقن لمكك ةحص نم ققحتل

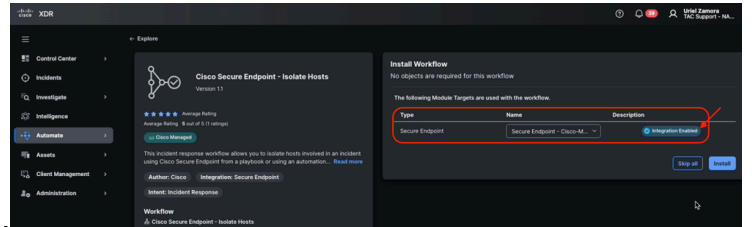
Cisco XDR Exchange نم لمعل ريس تبثت

ةياهنل طاقن لنع لمعل ريس تبثت: 3.1 ةوطخل

1. Exchange > ةتمتأ لى لقتناو Cisco XDR لى لوخدل ليجستب مق.
2. ةقبطو ةفيضم التايبل لنع - Cisco Secure Endpoint مسململ لمعل ريس نع ثحبا لتبثت.



Exchange نم فيضالم لمع ريس لزع



3. تېبثتال لبق فدهال رفوت نم ققحت.

لمعال ريس نم هنيكمت مت يذلا عيطمنال دحوال فده

4. ك صاخال يئاقولتال ليغشتال ماظن في لمعال ريس تېبثت مق.

ةتمت أةدعاق عاشنإ

لمعال ريس ذيفنت هي ف بجي يذلا تقولا ددحي نيوكت يه يئاقولتال ليغشتال دةدعاق اطورش دةواقال هذه نمضتت نا نكمي. اقابس دم دودج وأةني عم ثادحأ إلى ادانتسا نرتقمال (لمعال ريس) لمعال ريس ليغشت متي، طورشل هذه عافيتسا مت اذاو، ةيرايتخا يئاقولت.

ةتمت أةدعاق نيوكت: 4.1 ةوطخلا

1. تالغشمال > ةتمتأل مسق إلى لقتنا.

2. مسان ييغتت مقو ةتمت أةدعاق ةفاضإ قوف رقنا. ةديج ةدعاق عاشنإ.

تالغشمال نم ةتمت أةدعاق ةفاضإ

3. طشن ي ثدح ي نا نمضي اذهو، ةغراف طورشل كرت كنكمي. لغمشمال طورش ييغتت مق. ايرورض ناك اذا طرشل صي صختت مق. ةدعاقال هذه



Edit

General

Type
Incident Rule

Title * 12 / 64

Description 0 / 1024

☒ Automation rule is on

Create as priority or standalone rule

☒ Priority Rule

☒ Stop processing subsequent rules

☐ Standalone Rule

Conditions

☒ ALL of these conditions must be met

☐ ANY of these conditions can be met

☐ Advanced

[+ Add condition](#)

ةتمتألا ةدعاق طورش

ةفيضملا ةزهجألا لمع ريس لزح - Cisco نم ةنمآلا ةيانهنلا ةطقن دح ،ةدعاقلا ءارجإ يف 4.

Description 0 / 1024

☒ Automation rule is on

Create as priority or standalone rule

☒ Priority Rule

☒ Stop processing subsequent rules

☐ Standalone Rule

Conditions

☒ ALL of these conditions must be met

☐ ANY of these conditions can be met

☐ Advanced

[+ Add condition](#)

Apply to selected workflows

☒ On

Select workflow

Cisco Secure Endpoint - Isolate Hosts

Action(s)
contain

Intent
incident_response

Observable Type(s)
hostname amp_computer_guid device

[+ Add workflow](#)

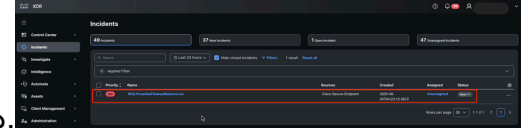
اقابسما هتيتبثتب تمق يتلا

لمعل ريسل يئاقلتلا ليغشتلا ةدعاق نييعت

5. طفح قوف رقنا .

لمعال ريس ةفيظو نم ققحتال

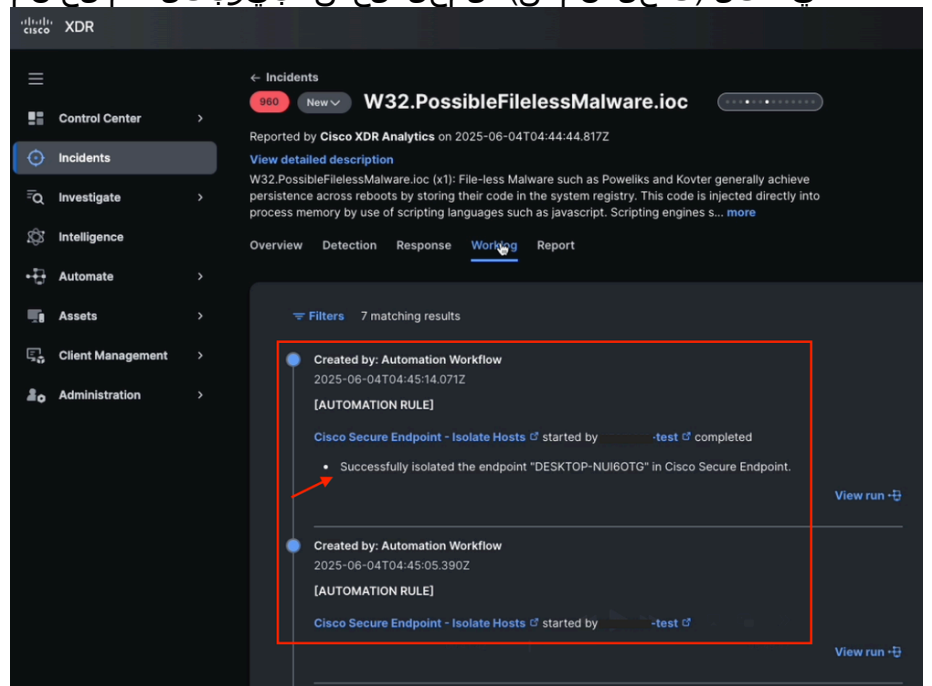
لمعال ريس ذيفنت نم ققحتال :5.1 ةوطخل



1. .رأظتنا وأ ةدعاقال طورش عم قفاوتي ثدح ءاشنإب مق .

Cisco XDR في ديدج ثداح فاشتكأ مت

2. ديكأتل (ثدحل نمض) "لمعال لجس" بيوبتل ةمالع نم ققحت ،ثدحل ءاشنإ درجمب .



حاجنب لمعال ريس ذيفنت

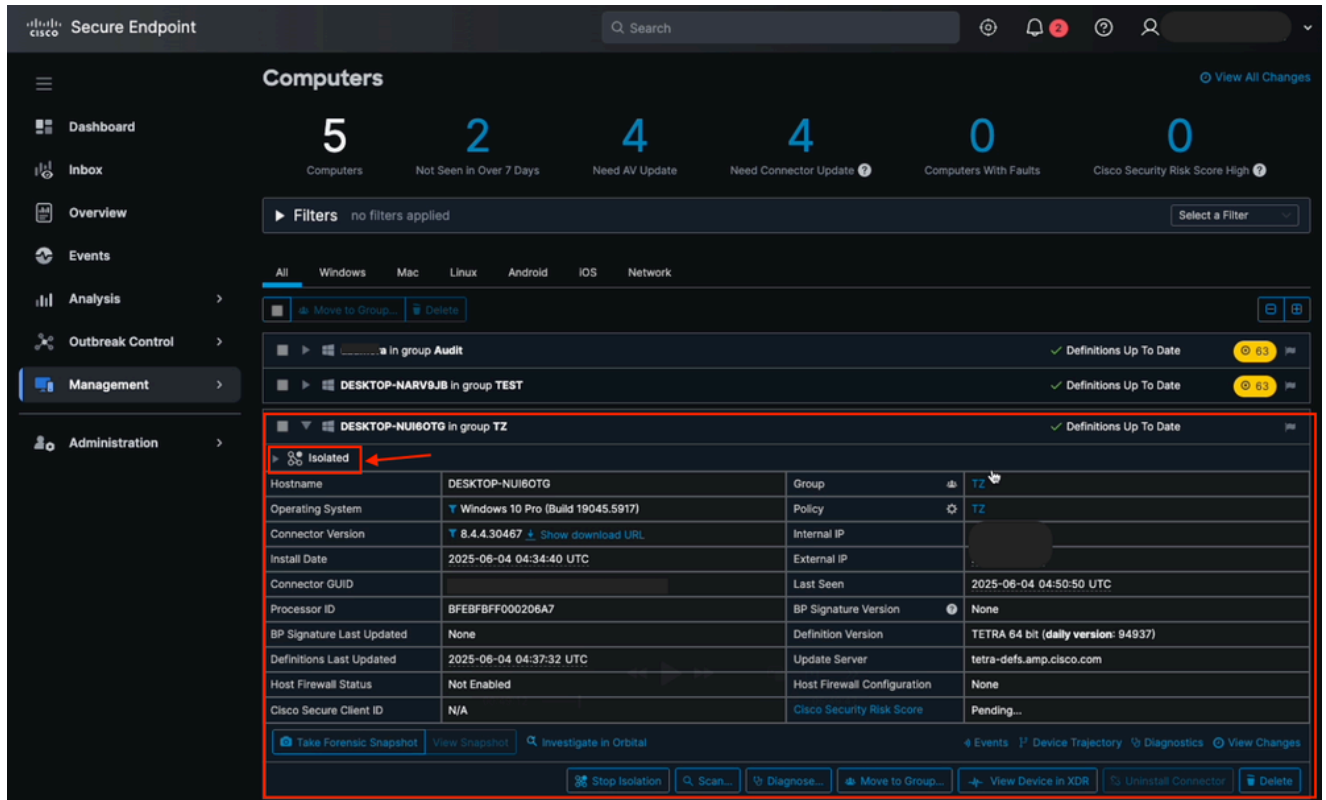
ثداحال لمع لجس بيوبتل ةمالع تامولعم

ةياهنل ةطقن لزع ديكأت :5.2 ةوطخل

1. Cisco نم ةنمآل ةياهنل ةطقن ةبواب ىلإ لوخدل لجس .

2. فدهال ةياهنل ةطقن ددحو رتوي بمكال ةزهجأ > ةرادإل مسق ىلإ لقتنا .

3. زاهجل ةلاح لزع نم دكأت .



ةنمآل ةياهنل ةطقن رتوي بمك ةزهجأ نم لزعل ةلاح

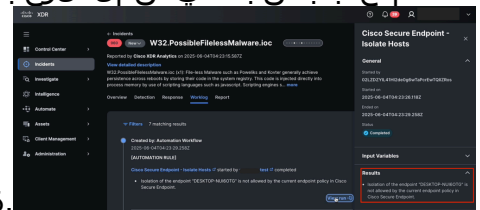
لكاشم ل دي دحتل نيوكتالو لمعل ريس تالجس عجار، ةلوزعم ةياهنل ةطقن نكت مل اذإ 4. ةلمتحملم.

ةكرتشم ةيضق

ةنمآل Cisco ةياهن ةطقن نم لزعل ةزي م نيكمت متي مل

1. لمعل لجس لىل لقتناو، ثداح رخآ دحو، ثداوخل لىل لقتنا Cisco XDR نم.
2. ةتمتأل لمعل ريس ليغشت دعب ةلص يذ أطخ يأ كانه ناك اذإ امم ققحت.

مدع ببسب فيضملم لزعب ةياهنل ةطقن لزعل ةيلمع حمست مل، لاثملم ليلبس لىل



ةنمآل ةياهنل ةطقن جهن لىل ةياهنل ةطقن لزعل نيكمت

ثداوخل لمعل لجس نم ةتمتأل لمعل ريس جئاتن

ةينعمل ةسايسل دح تاسايسل > ةرادإل لىل لقتنا، ةنمآل ةياهنل ةطقن نم 3.

حامس لىل عبرملم دحو EdnPoint لزعل > ةمدقتم تادادع لىل لقتنا، جهنل لخد حبصت نأ درجمب 4. EdnPoint لزعل.

Secure Endpoint

← Policies
Edit Policy: TZ
Windows

Name: TZ
Description:

Management

- Modes and Engines
- Exclusions
1 exclusion set
- Proxy
- Host Firewall
- Outbreak Control
- Device Control
- Product Updates
- Advanced Settings**
 - Administrative Features
 - Client User Interface
 - File and Process Scan
 - Cache
 - Endpoint Isolation**
 - Orbital
 - Engines
 - TETRA
 - Network
 - Scheduled Scans
 - Identity Persistence

Endpoint Isolation

- ☒ Allow Endpoint Isolation ⓘ
- ☒ Allow DNS ⓘ
- ☒ Allow DHCP ⓘ
- ☐ Allow isolation when endpoint is using a proxy ⓘ

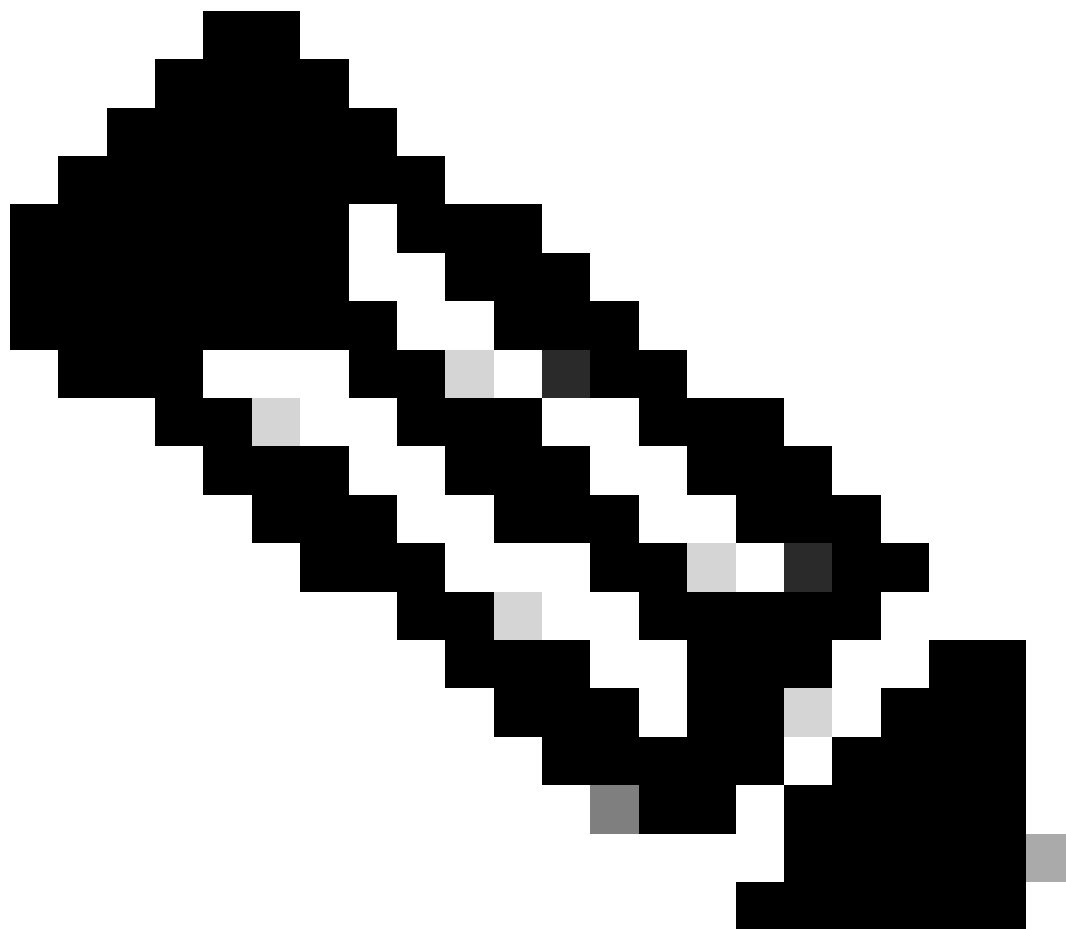
Isolation IP Allow Lists Clear Select Lists

None

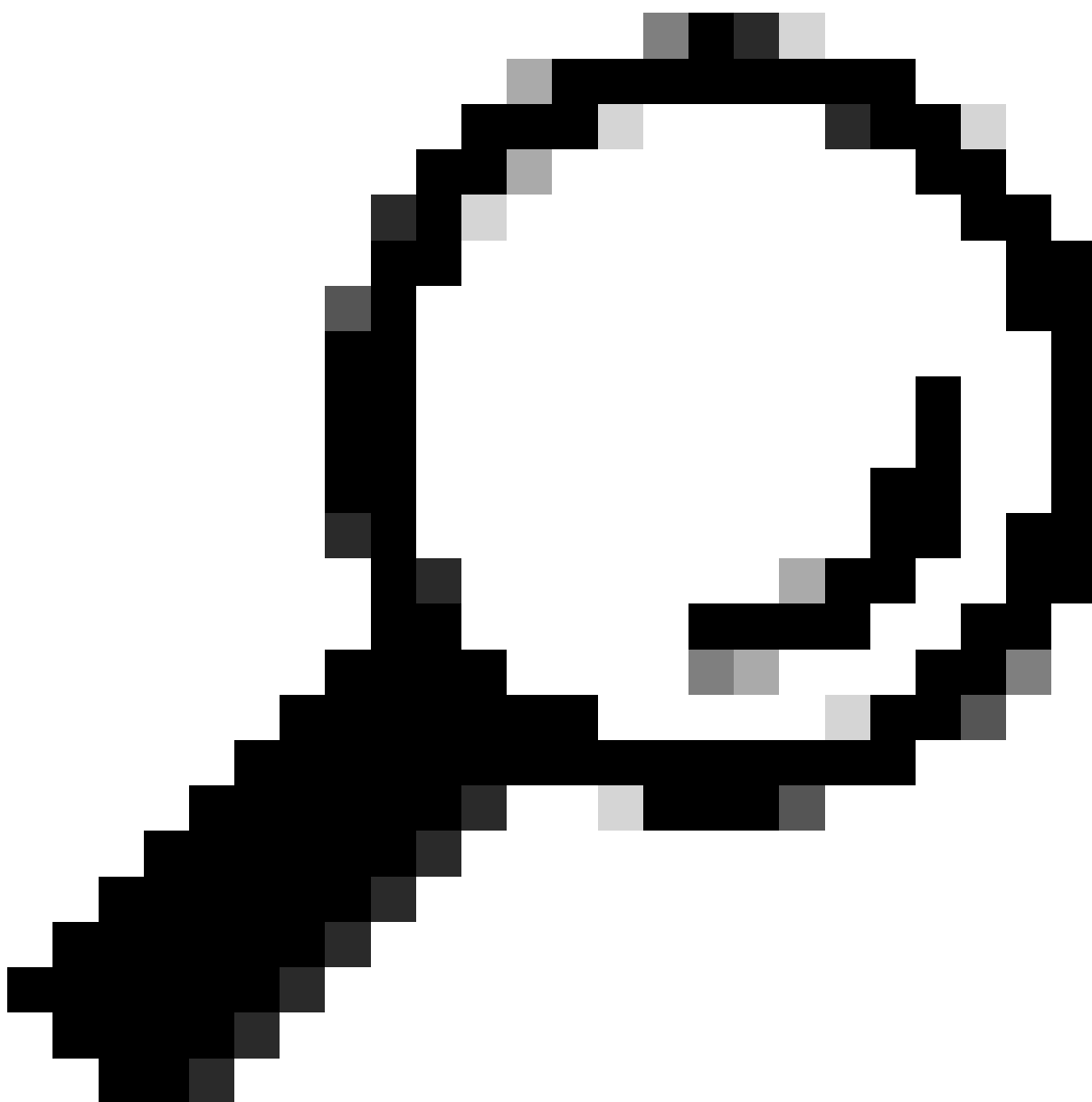
Save **Cancel**

نم آلا ةياهنلا ةطقن جهن يف ةياهنلا ةطقن لزعب حامسلا

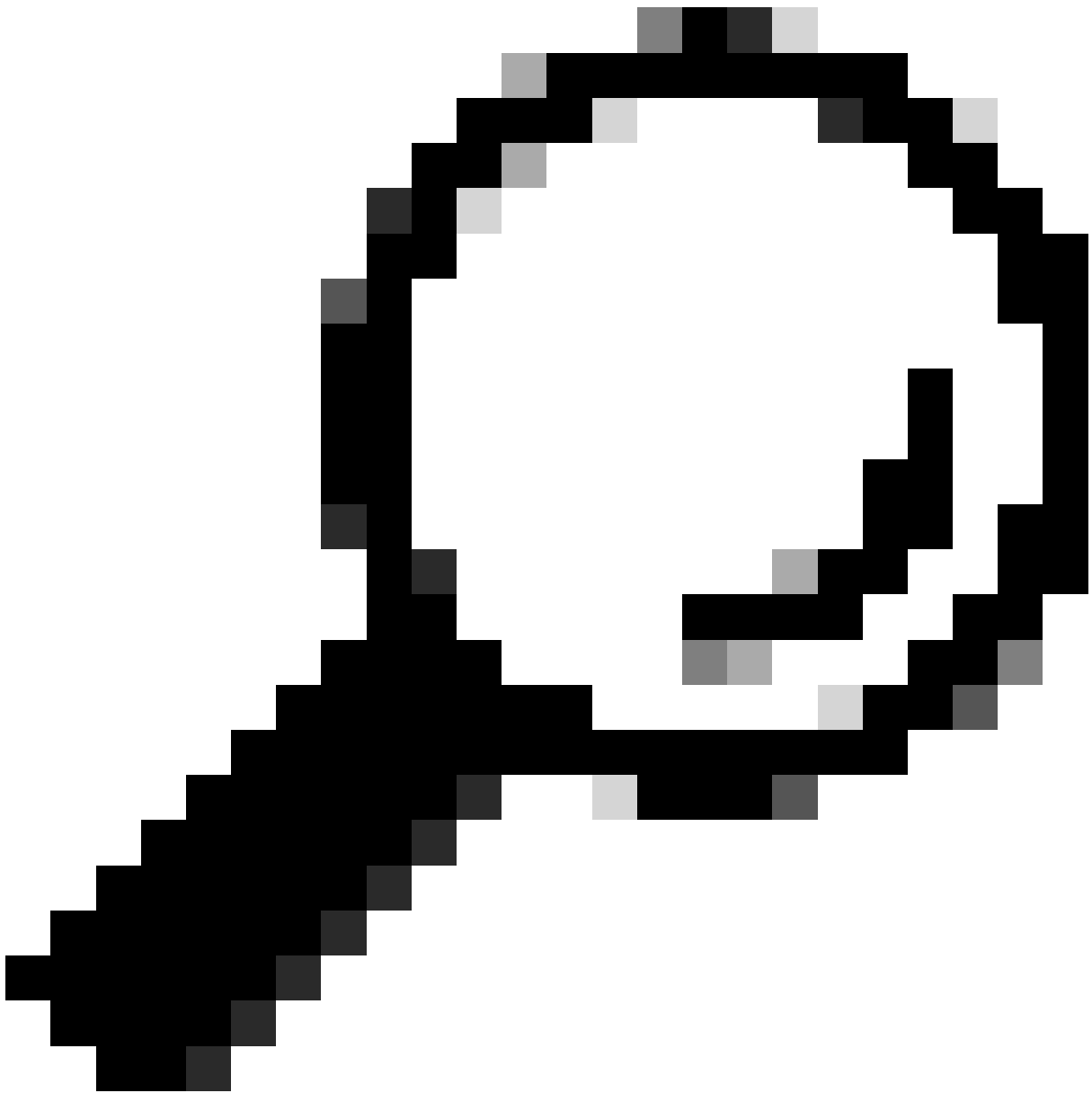
5. ظفح قوف رقنا.



لمعلا ريسو لم اكلتلا نيوكتل ةمزاللا ةيرادلإا تانوذاللا كي دل نأ نم دكأت :ةظحالم



في فة تم أال رشن لبق مكحت لل عضاخ ةئيب في دادع إال رابتخاب مق :حيملت
جاتن إال



ةدعاق وألمعلا ريس ىلع اهؤارجإ مت ةصصخم تاليدعت ةيأ قيثوتب مق :خيملت
ةتمألا

ةطقن لزعب موقبي حاجنب هطيشتولم عريس نيوكت كنكمي ،تاوطخلا هذه ذيفنت درجمب
نامألا تاديدهتل ةلاعفو ةعيرس ةباجتسا نمضي وشح عاشنإ دعب ايئاقلت ةياهن

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