ةياەنلا ةطقن ىلع ءاطخالا حيحصت نيكمت ةياەنلا ةطقن مكحت ةدحول AMP نم

تاىوتحملا

<u>قمدق مل ا</u>
<u>قي، س اس أل ا ت ابل طتمل ا</u>
<u>تابا.طتملا</u>
<u>ةمدختسملاً تانوكملاً</u>
<u>قيساساً تامولعم</u>
<u>ەلىكەشمل.ا</u>
<u>نېوكتا.</u>
<u>ءاطخأليا چيچصت عبل امليقين متيس بيتليا قيامنليا قطقين ددج :1 قوطخلا</u>
<u>قدوچومل ا ةس اي سل ا راركت :2 ةوطخل ا</u>
<u>چەنلارا ادە ءاطخا چېچصټل لرچسلا يوټسم نېوكت :3 قوطخلا</u>
<u>قديدچل ا ةس اي س ل ا هذه طب رو قدي دج قعوم جم عاش ن ا:4 قوطخل ا</u>
<u>ةديدجا ا قعومجما ا هذه يال قددحما ا قيامنا ا قطقن ل.ق.ن :5 قوطخا ا</u>
<u>مدختسم ةمجاو يفو رتويټمكلا قحفص يف قيامنلا ةطقين نم قرقحتايا :6 قوطخا،</u> ليصوملا

ةمدقملا

مكحت ةدحو نم ةياهنلا ةطقن ىلع ءاطخألا حيحصت نيكمت ةيفيك دنتسملا اذه حضوي .Cisco نم ةنمآلا ةياەنلا ةطقن

ةىساسألا تابلطتملا

تابلطتملا

كىدل نأ نم دكأت ،ءدبلا لبق:

- . ةياەنلا طاقن مكحت ةدحول Cisco نم ةنمآلا ةياەنلا ةطقن ىلإ يرادإلا لوصولا •
- ةنمآلا ةياهنلا ةطقن يف لعفلاب ةلجسم اهئاطخاً حيحصت ديرت يتلا ةياهنلا ةطقن Cisco نم

ةمدختسملا تانوكملا

:ةغيص ةيجمرب اذه ىلع ةقيثولا يف لمعتسي ةمولعملا تسساً

- Cisco Secure Endpoint Console، رادصإلاا 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 ثدحألا تارادصإلاو
- Microsoft Windows لىغشتارا ماظن

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

ةيساسأ تامولعم

نم (TAC) ةينقتلا تادعاسملا زكرم ىلإ اهؤاشنإ مت يتلا صيخشتلا تانايب ريفوت نكمي Cisco ليلحتلا نم ديزم ىلع لوصحلل.

لثم تامولعم صيخشتلا تانايب نمضتت:

- (ةركاذلاو ةيزكرملا ةجلاعملا قدحوو صرقلا) دراوملا مادختسإ
- لصوملاب ةصاخلا تالجسلا
- لصوملا نيوكت تامولعم •

ةلكشملا

دحأ ءانثأ Cisco Secure Endpoint Console نم ةياهنلا ةطقن ىلع ءاطخألا حيحصت نيكمت مزلي ةيلاتلا تاهويرانيسلا.

ةەجاو نم ءاطخألاا حيحصت عضو نيكمتب مقف ،زاەجلا ليغشت ةداعإب تمق اذإ :1 ويرانيسلا تالجس بلط ةلاح يف .ديەمتلا ةداعإ ةيلمع ذيفنتب مقت مل وأ IP جرد ةەجاو ةەجاو ةەجاو ةدحو يف جەنلا نيوكت نم ءاطخألا حيحصت عضو نيكمت كنكمي ،ديەمتلا ءاطخأ حيحصت ةدحو يف جەنلا قياەنلا قطقن مكحت.

زاهج ىلع Cisco نم ةنمآلا ةياەنلا ةطقن لصوم عم ءادألا يف لكاشم تەجاو اذإ :2 ويرانيسلا ةيليصفتلا تالجسلا عيمجت يف دعاسي نأ نكمي ءاطخألا حيحصت عضو نيكمت نإف ،ام ليلحتلل.

نأ نكمي ،ةنمآلا ةياەنلا ةطقن لصوم عم امحالصإو ةددحم ءاطخأ فاشكتسأ دنع :3 ويرانيسلا ةلكشملل يرذجلا ببسلا لوح ىؤر ةيليصفتلا تالجسلا رفوت.

نيوكتلا

لالخ نم ةددحملا ةياەنلا ةطقن ىلع حاجنب ءاطخألا حيحصت عضو نيكمتل تاوطخلا ەذە لمكأ ةنمآلا ةياەنلا ةطقن مكحت ةدحو.

ءاطخألاا حيحصت ىلإ اەلقن متيس يتلا ةياەنلا ةطقن ددح :1 ةوطخلا

- تامولعملا ةحول نم .Cisco نم ةنمآلا ةياەنلا ةطقن مكحت ةدحو ىلإ لوخدلا لجس .1 ةرادإلا مسق ىلإ لقتنا ،ةيسيىئرلا.
- . رتويبمكلا ةزهجاً < ةرادإلا ىلإ لقتنا.
- .ءاطخألاا حيحصت عضو بلطتت يُتلا ةيامنلا ةطقن ظحالو ددح .3

ةدوجوملا ةسايسلا راركت :2 ةوطخلا

.تاسايسلا < ةرادإلا ىلإ لقتنا .1

Ξ		Management	×
==	Dashboard	Computers	
$ _{\Theta}^{ _{1} }$	Inbox	Groups	
	Overview	Policies	~
_		Exclusions	
3	Events	Device Control	
dil	Analysis >	Host Firewall	
20	Outbreak Control >	Deployment	
5	Management	Download Connector	
		Deploy Clarity for iOS	
20	Administration >	Deployment Summary	
		AV Definition Summary	

. ةددحملا ةياەنلا ةطقن ىلع ايلاح ةقبطملا ةسايسلا عقوم ديدحت.

- .جەنلا ةذفان عيسوتل جەنلا قوف رقنا .3
- 4. دوجوملا جەنلا نم ةخسن ءاشنإلراركت قوف رقنا.

tection and Response	Exclusion Sets	Custom Detections	Groups	-
es Quarantine twork Block dicious Activity Prote Quarantine	Cieco-Maintained Microsoft Windows Default	Simple Not configured Advanced Not configured	TEST	
atem Process Protec. Protect ript Protection Quarantine		Application Control		
ploit Prevention Block ploit Prevention Scrip., Audit		Alow Not configured		
havioral Protection Protect TRA Offine File Scan, Disabled		Block Not configured		
sital Enabled		Network Control		
wice Control		Not configured		
8 Mass Store. Not configured			Proxy.	

جەنلا اذە ءاطخأ حيحصتل لجسلا ىوتسم نيوكت :3 ةوطخلا

- اهعيسوتب مقو ةرركملا ةسايسلا ةذفان ددح .1.
- 2. جەن ،لاثملا ليبس ىلع) جەنلا ةيمست دعأ مث ريرحت قوف رقنا.
- .ةمدقتم تادادعإ ىلع رقنا .3
- 4. يبناجلا طيرشلا نم ةيرادإلا تازيملا ددح.
- .ءاطخألاا حيحصت ىلع جرد لجس ىوتسمو لصوملًا لجس ىوتسم نم لك نييعتب مق .5
- .تارييغتلا ظفحل ظفح قوف رقنا .6

Name	Debug TechZone Policy	
Description	Taking debug on endpoint	
Modes and Engines		Send User Name in Events ()
Exclusions exclusion set	Heartbeat Interval	Send Filename and Path Info ()
Proxy	Connector Log Level	Cebug ~ 0
Host Firewall	Tray Log Level	Ontrag ~ 0
Outlineak Control		Enable Connector Protection ()
Device Control	Connector Protection Password	0
Product Updaties		Automated Crash Dump Uploads ()
Advanced Settings		Command Line Capture ()
Administrative Features		Command Line Logging ()
File and Process Scan		
Cathe		
Endpoint lociation		
Orbital		
Ungenese TETEL		
Network.		
Schuck and Science		

ةديدجلا ةسايسلا هذه طبرو ةديدج ةعومجم ءاشنإ :4 ةوطخلا

.تاعومجملا < ةرادإلا ىلإ لقتنا .1

≡			Management ×	
5	Dashboard		Computers	
1 ¹ ©	Inbox		Groups 🗸	
	Overview		Policies	
•	Events		Device Control	c
нI	Analysis	>	Host Firewall	
20	Outbreak Control	>	Deployment	
5	Management		Download Connector	
#o	Administration	>	Deploy Clarity for iOS Deployment Summary AV Definition Summary	

- .ةشاشلا نم رسيألا يولعلا بناجلا نم برقلاب ةعومجم ءاشنإ قوف رقنا .2
- 3. أعومجم ،لاثملا ليبس ىلع) ةعومجملل امسا لخدأ Debug TechZone.)
- اثيدح ەؤاشنإ مت يذلا ءاطخألا حيحصت جەن ىلإ يضارتڧالا دادعإلا نم جەنلا رييغتب مق .4.
- .ظفح قوف رقنا .5

Name	Debug TechZone Group		Computers
Description	This Group is used to Debug Cisco Sec Endpoint Connector	**	Assign computers from the Computers page after you have saved the new group
Parent Group		~	
Windows Policy	Debug TechZone Policy	~	
Android Policy	Default Policy (Protect)	v	
Mac Policy	Default Policy (Audit)	~	
Linux Policy	Default Policy (Audit)	~	
Network Policy	Default Policy (Default Network)	v	
KIS Policy	Default Policy (Audit)	v	

ةديدجلا ةعومجملا هذه ىلإ ةددحملا ةياەنلا ةطقن لـقن :5 ةوطخلا

.رتويبمكلا ةزهجأ < ةرادإلا ىلإ ىرخأ ةرم لقتنا .1

Secure Endpoint

=			Management	×
5	Dashboard		Computers	~
0	Inbox		Groups	
	Overview		Policies	
•	Events		Exclusions Device Control	
dd	Analysis	>	Deployment	
20	Outbreak Control	>	Download Connector	
	Management		Deploy Clarity for iOS	
20	Administration	>	Deployment Summary AV Definition Summary	

2. ةمئاقلا نم ةددحملا ةياەنلا ةطقن ددح.

.ةعومجملا ىلإ لقن قوف رقنا .3

• ¥ # 00070*	prod TENT		
Rodrane	DESKTOP MIGHUEP	from a	Test
Operating System	 Windows 10 Pro Build 18045.45280 	Pulky 0	151
Connector territori	T 8-40-30001 + Drow download URL	Internal IP	0
Install (Inte	2024 07-25 15:03/0 67	External IP	0
Connector 64/0	201thc7b-040a-4754-aceb-ctxXie8046cH	Lost Seen	2024-07-25 18-42-50 /07
Processor (5	0%w/w/000008/17	BP apprature version	19294
Class Secure Clent ID	N/A	Class Security Rek Score	Pendra_
B Sea Farmer Engenet Vice	Instatut R Investigate in Orbital		a Dearts (P Deales Trajectory, 10 Disposition, (D Mex Changes
		9, Son.	10 Disprose More to Group 5 Universit Connector

. ةعومجم ديدحت ةلدسنملا ةمئاقلا نم اثيدح اهؤاشنا مت يتلا ةعومجملا ددح

.ةديدجلا ةعومجملا ىل قددحملا ةياەنلا ةطقن لقنل لقن قوف رقنا .5

Move Computers to Group	\times
ESKTOP- in group TEST	
Move To Existing Group New Group	
Select Group Cebug TechZone Group	
Cancel	ove

لصوملا مدختسم ةهجاو يفو رتويبمكلا ةحفص يف ةياهنلا ةطقن نم ققحتلا :6 ةوطخلا

- . رتويبمكلا ةزهجأ ةحفص يف ةديدجلا ةعومجملا نمض ةياهنلا قطقن جاردإ نم دكأت .1
- .ةنمآلا ةياەنلا ةطقن لصوم مدختسم ةەجاو حتفا ،ةياەنلا ةطقن ىلع .2
- ةطقن ةنوقيأ نم ققحتلا قيرط نع ديدجلا ءاطخألا حيحصت جەن قيبطت نم ققحت .3 مئاوقلا طيرش يف ةنمآلا ةياەنلا.



Secure Client

Secure Endpoint

tatistics	Update	Advanced					
Agen	t						
Status:			Connected				
Version:			8.4.0.30201				
GUID:			202dac7b-093a-4784-ace8-cb95e8696c96				
Last Sc	an:		Today 03:03:18 PM				
Isolatio	n:		Not Isolated				
Policy	y						
Name:			Debug TechZone Policy				
Serial N	lumber:		229				
Last Up	date:		Today 03:52:38 PM				
() ()	isco Secu	ure Client	×				
(\mathbf{b}	Secure End Connected.	point:				
		Flash Scan	✓ Start				



ينقتلا Cisco معد سدنهم بلط اذإ الإ ءاطخألا حيحصت عضو نيكمت نكمي ال :ةظحالم هنيكمت مت يذلا ءاطخألا حيحصت عضوب ظافتحالا يدؤي نأ نكمي .تانايبلا هذه تانايب عيمجت عنمي نأ نكمي امك ،ةعرسب صرقلا ةحاسم علم ىلإ ةدتمم ةرتفل فلمل ل دئازلا مجحلا ببسب معدلا صيخشت فلم يف "جرد لجس"و "تالصوملا لجس"

.ةدعاسملا نم ديزم ىلع لوصحلل Cisco معدب لصتا

<u>ملاعلا عاجناً عيمج يف Cisco معد لاصتا تامج</u>

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