

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوم ل ةزهجال نم دنتس م ل اذ ه ي ف ةدراول ا تامولعمل اءاشن ا م ت ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) حوس م م ن ي و ك ت ب د ن ت س م ل ا اذ ه ي ف ةم د خ ت س م ل ةزهجال ا ع ي م ج ت ا د ب ر م ا ي ا ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش .

ةي س ا س ا تامولعم

ن م (TAC) ةي ن ق ت ل ا ت ا د ع ا س م ل ا ز ك ر م ل ا ا ه و ا ش ن ا م ت ي ت ل ا ص ي خ ش ت ل ا ت ا ن ا ي ب ر ي ف و ت ن ك م ي ل ي ل ح ت ل ا ن م د ي ز م ل ع ل و ص ح ل ل Cisco .

ل ث م ت ا م و ل ع م ص ي خ ش ت ل ا ت ا ن ا ي ب ن م ض ت ت :

- (ةر ك ا ذ ل ا و ة ي ز ك ر م ل ا ة ج ل ا ع م ل ا ة د ح و و ص ر ق ل ا) د ر ا و م ل ا م ا د خ ت س ا |
- ل ص و م ل ا ب ة ص ا خ ل ا ت ا ل ج س ل ل
- ل ص و م ل ا ن ي و ك ت ت ا م و ل ع م

ةل ك ش م ل ا

د ح ا ن ا ث ا Cisco Secure Endpoint Console ن م ة ي ا ه ن ل ا ة ط ق ن ل ع ا ط خ ا ل ا ح ي ح ص ت ن ي ك م ت م ز ل ي ة ل ا ت ل ا ت ا ه و ي ر ا ن ي س ل ل .

ة ه ج ا و ن م ا ط خ ا ل ا ح ي ح ص ت ع ض و ن ي ك م ت ب م ق ف ، ز ا ه ج ل ا ل ي غ ش ت ة د ا ع ا ب ت م ق ا ذ ا : 1 و ي ر ا ن ي س ل ل ت ا ل ج س ب ل ط ة ل ا ح ي ف . د ي ه م ت ل ا ة د ا ع ا ة ي ل م ع ذ ي ف ن ت ب م ق ت م ل و ا IP ج ر د ة ه ج ا و ة ه ج ا و ة ه ج ا و ة د ح و ي ف ج ه ن ل ل ن ي و ك ت ن م ا ط خ ا ل ا ح ي ح ص ت ع ض و ن ي ك م ت ك ن ك م ي ، د ي ه م ت ل ا ا ط خ ا ل ا ح ي ح ص ت ة ن م ا ل ا ة ي ا ه ن ل ا ة ط ق ن م ك ح ت .

ز ا ه ج ل ع Cisco ن م ة ن م a ل ا ة ي ا ه ن ل ا ة ط ق ن ل ص و م ع م ا د a ل ا ي ف ل ك ا ش م ت ه ج ا و ا ذ ا : 2 و ي ر ا ن ي س ل ل ة ي ل ي ص ف ت ل ا ت ا ل ج س ل ا ع ي م ج ت ي ف د ع ا س ي ن ا ن ك م ي ا ط خ a ل ا ح ي ح ص ت ع ض و ن ي ك م ت ن ا ف ، ا م ل ي ل ح ت ل ل .

ن ا ن ك م ي ، ة ن م a ل ا ة ي ا ه ن ل ا ة ط ق ن ل ص و م ع م ا ه ا ل ص ا و ة د د ح م ا ط خ a ف ا ش ك ت س a د ن ع : 3 و ي ر ا ن ي س ل ل ة ل ك ش م ل ل ر ذ ج ل ل ب ب س ل ل ل و ح ي و ر ة ة ي ل ي ص ف ت ل ا ت ا ل ج س ل ل ر ف و ت .

ن ي و ك ت ل ا

ل ا ل خ ن م ة د د ح م ل ا ة ي ا ه ن ل ا ة ط ق ن ل ع ح ا ج ن ب ا ط خ a ل ا ح ي ح ص ت ع ض و ن ي ك م ت ل ا و ط خ a ل ه ذ ه ل م ك a ة ن م a ل ا ة ي ا ه ن ل ا ة ط ق ن م ك ح ت ة د ح و .

ا ط خ a ل ا ح ي ح ص ت ل ا ا ه ل ق ن م ت ي س ي ت ل ا ة ي ا ه ن ل ا ة ط ق ن د د ح : 1 ة و ط خ a

1. تامولعمل ا ة ح و ل ن م Cisco . ن م ة ن م a ل ا ة ي ا ه ن ل ا ة ط ق ن م ك ح ت ة د ح و ل ا ل و خ د ل ا ل ج س .
• ة ر ا د ا ل م س ق ل ا ل ل ق ت ن ا ، ة ي س ي ئ ر ل ا .
2. ر ت و ي ب م ك ل ا ة ز ه ج a > ة ر ا د ا ل ا ل ا ل ل ق ت ن ا .
3. ا ط خ a ل ا ح ي ح ص ت ع ض و ب ل ط ت ت ي ت ل ا ة ي ا ه ن ل ا ة ط ق ن ظ ح ا ل و د د ح .

ةدوجوملا ةسايسلا راركت :2 ةوطخل

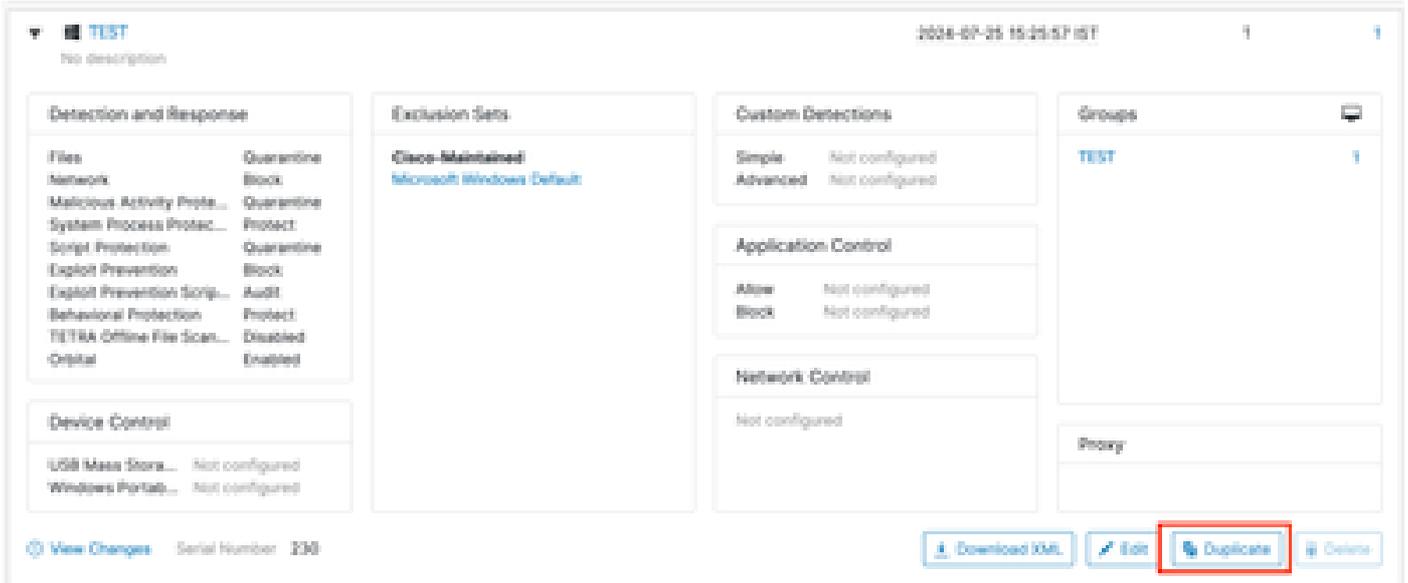
1. تاسايسلا > ةرادإلا ىلإ لقتنا .

The screenshot shows a software interface with a sidebar menu on the left and a main content area on the right. The sidebar menu includes items like Dashboard, Inbox, Overview, Events, Analysis, Outbreak Control, Management, and Administration. The 'Management' item is highlighted with a blue bar. The main content area is titled 'Management' and contains a list of sub-items: Computers, Groups, Policies (highlighted with a blue bar and a checkmark), Exclusions, Device Control, Host Firewall, Deployment, Download Connector, Deploy Clarity for iOS, Deployment Summary, and AV Definition Summary.

2. ةدوملا ةياهنلا ةطقن ىلع ايلاح ةقبطملا ةسايسلا عقوم ديدحت .

3. جهنلا ةذفان عيسوتل جهنلا قوف رقنا .

4. دوجوملا جهنلا نم ةخسن عاشنإل راركت قوف رقنا .



جهنلا اذه ءاطخأ حئصت ل لجسلا يوتسم نيوكت :3 ةوطخل

1. اه عيسوتب مقو ةرركملا ةسايسلا ةذفان ددح.
2. (TechZone جهن ، لاثملا لئبس ىلع) جهنلا ةيمست دعأ مئ ريرحت قوف رقنا .
3. ةمدقتم تادادعإ ىلع رقنا .
4. يبناجال طيرشللا نم ةيرادلإا تازيملا ددح .
5. ءاطخألا حئصت ىلع جرد لجس يوتسمو لصوملا لجس يوتسم نم لك نئيعتبت مق .
6. تاريغتلا ظفحل ظفح قوف رقنا .

← Policies

Edit Policy

Windows

Name: Debug TechZone Policy

Description: Taking debug on endpoint

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

Orbita

Engines

TETRA

Network

Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval: 15 minutes ⓘ

Connector Log Level: Debug ⓘ

Tray Log Level: Debug ⓘ

Enable Connector Protection ⓘ

Connector Protection Password: ⓘ

Automated Crash Dump Uploads ⓘ

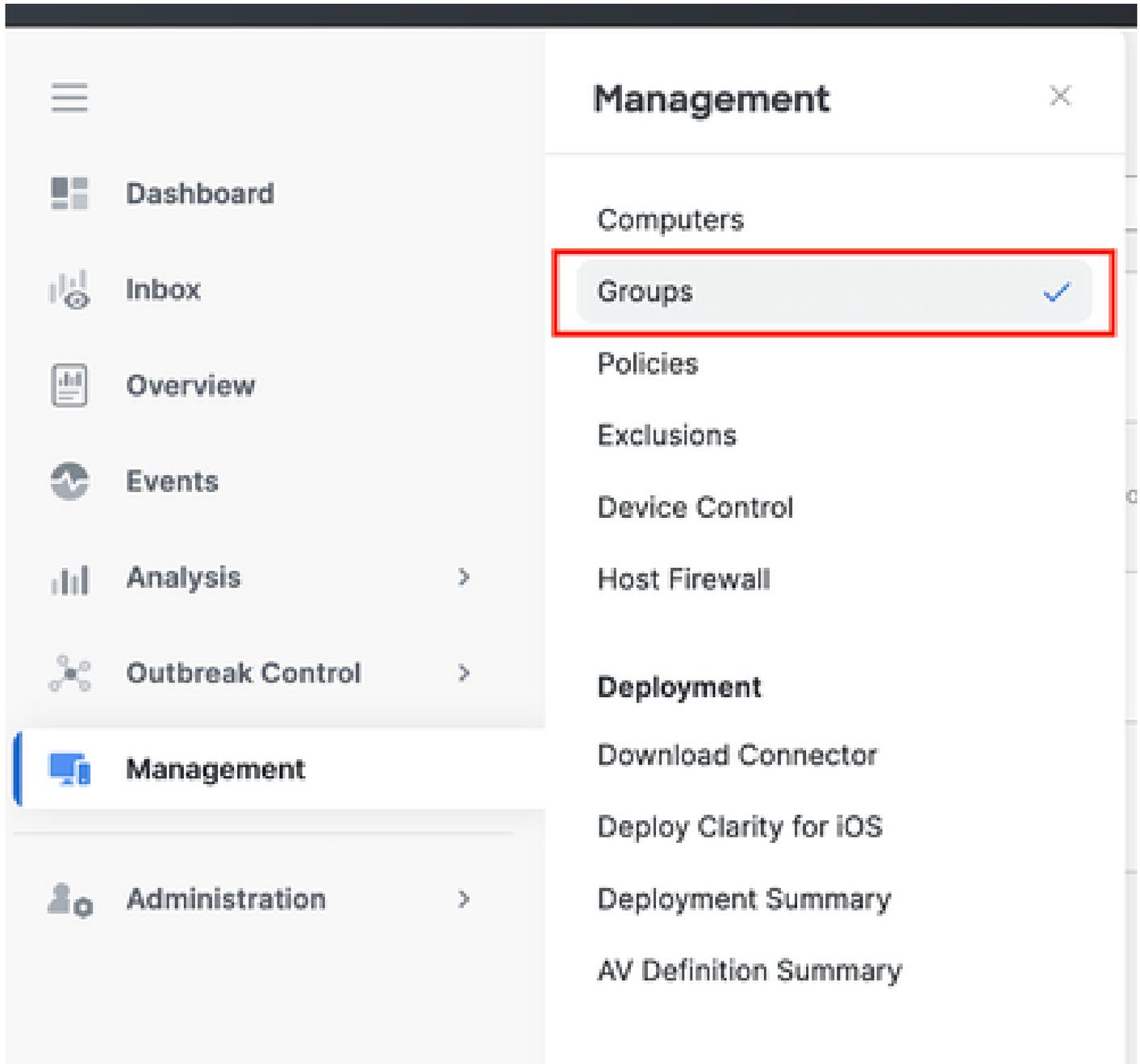
Command Line Capture ⓘ

Command Line Logging ⓘ

Cancel Save

ةديجل ةسايسلا هذه طبرو ةديج ةومجم ءاشنإ: 4 ةوطخلا

1. تاعومجملا > ةرادإلا ىلإ لقتنا.



2. ءشاشلا نم رسيألا يولعل بانجال نم برقلاب ءومجم ءاشنإ قوف رقنا.
3. ءومجم ءومجم، لاثملا لابس ىلع) ءومجم لئامسا لخدأ (Debug TechZone ءومجم.)
4. ائيدح هؤاشنإ مت يذلا ءاطخألا حيصت جهن ىلى يضارتفالا دادعإلا نم جهنلا ريغتت مق.
5. ظفح قوف رقنا.

← Groups

New Group

Name	<input type="text" value="Debug TechZone Group"/>
Description	<input type="text" value="This Group is used to Debug Cisco Secure Endpoint Connector"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Debug TechZone Policy"/>
Android Policy	<input type="text" value="Default Policy (Protect)"/>
Mac Policy	<input type="text" value="Default Policy (Audit)"/>
Linux Policy	<input type="text" value="Default Policy (Audit)"/>
Network Policy	<input type="text" value="Default Policy (Default Network)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

Computers

Assign computers from the Computers page after you have saved the new group

ةديجال ةومجم ال هذه ال ةدحم ال ةياهن ال ةطقن لقن : 5 ةوطخال

رتوي بمك ال ةزهج > ةرادال ال ال رخ أرم لقننا 1.

-
- Dashboard
- Inbox
- Overview
- Events
- Analysis >
- Outbreak Control >
- Management**
- Administration >

Management ✕

- Computers ✓
- Groups
- Policies
- Exclusions
- Device Control
- Deployment**
- Download Connector
- Deploy Clarity for iOS
- Deployment Summary
- AV Definition Summary

2. عمىاق اللى نم ءءءءم ال ءىاهن ال ءطقن ءءء.

3. ءءءءم ال ءىل لىقن قوف رىقنا.

DESCRIPTION		in group TEST	
Username	000010@orange.com	Group	TEST
Operating System	Windows 10 Pro (Build 19045.4526)	Policy	TEST
Connector Version	8.4.0.20201 Show download URL	Internal IP	
Install Date	2024-07-25 15:00:13 IST	External IP	
Connector GUID	000007e-000e-4784-ec0d-cd00e0000000	Last Seen	2024-07-25 15:42:00 IST
Processor ID	00000000000000000000000000000000	BP signature version	10004
Cisco Secure Client ID	NSA	Close Security Risk Score	Pending...

Take Forensic Snapshot View Snapshot Investigate in Orbital

Events Service Traybars Diagnosis Show Changes

Scan... Diagnose... Move to Group... Uninstall Connector Details



Secure Client

Secure Endpoint

Statistics Update Advanced

Agent

Status: Connected
Version: 8.4.0.30201
GUID: 202dac7b-093a-4784-ace8-cb95e8696c96
Last Scan: Today 03:03:18 PM
Isolation: Not Isolated

Policy

Name: Debug TechZone Policy
Serial Number: 229
Last Update: Today 03:52:38 PM

Cisco Secure Client

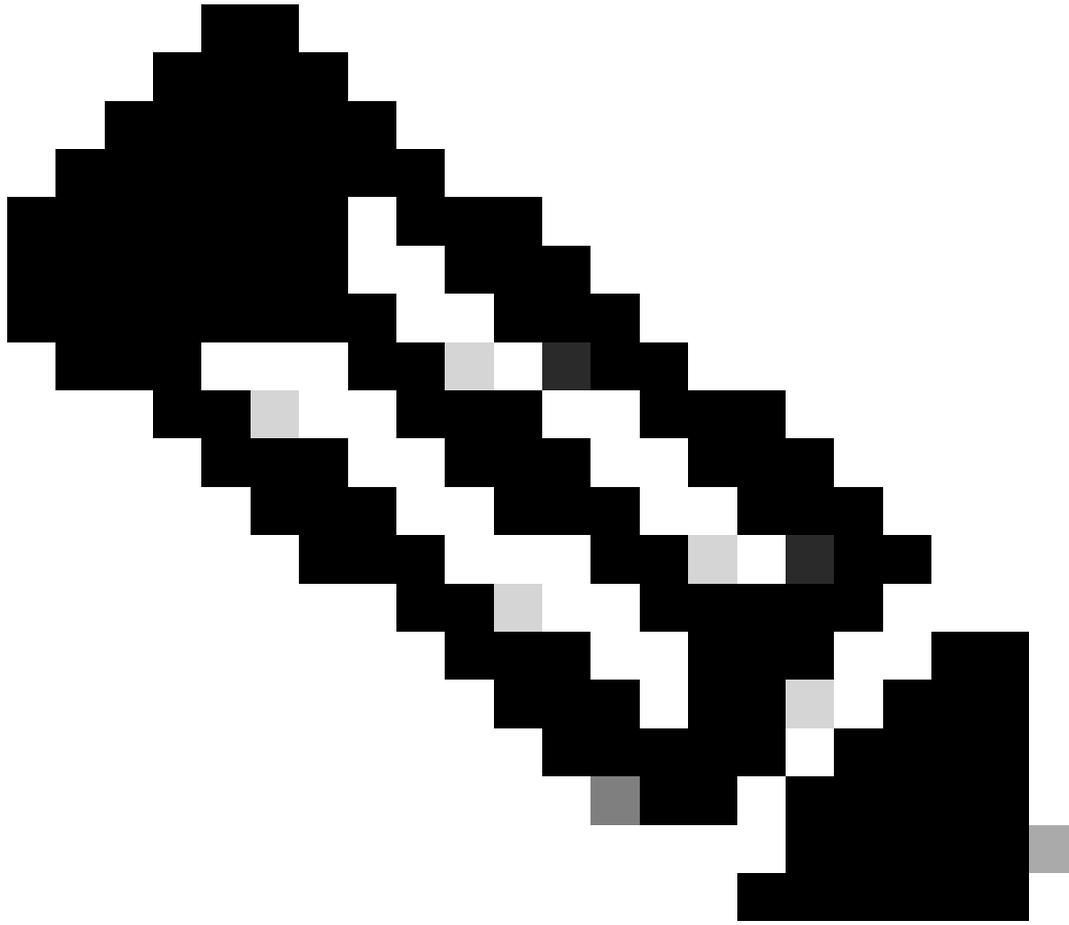


Secure Endpoint:

Connected.

Flash Scan

Start



ينقل Cisco معدس دنهم بلط اذا ال ااطخ ال احيصت عضو نيكم مت نكمي ال: ةظحال منيكم مت يذلا ااطخ ال احيصت عضو ب طاقت حال ايدوي نأ نكمي. تانا يبالا هذه تانا ي ب عي مت عنمي نأ نكمي امك، ة عرس ب صرق ال ةحاسم علم ال ةدتمم ةرت فل فل ملل دئال مجال ببسب معدل صيخش ت فلم ي "ج رد ل ج س" و "تال صوم ل ج س"

ة دعاسم ل ن م ديزم ال ع لوص حال Cisco معدب ل صتا

[ملاعل اءل نأ عي مج ي Cisco معد لاصتا تاهج](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دق ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىلچنل اءل دن تسمل