

لهاجت مت اذا AMP لصوصم تيبتت ةلازال اارجا رورملا ةم لك

تايوت حمل

[ةمدقملا](#)

[لصتم لصوصملا](#)

[لصوصملا لاصت اعطق مت](#)

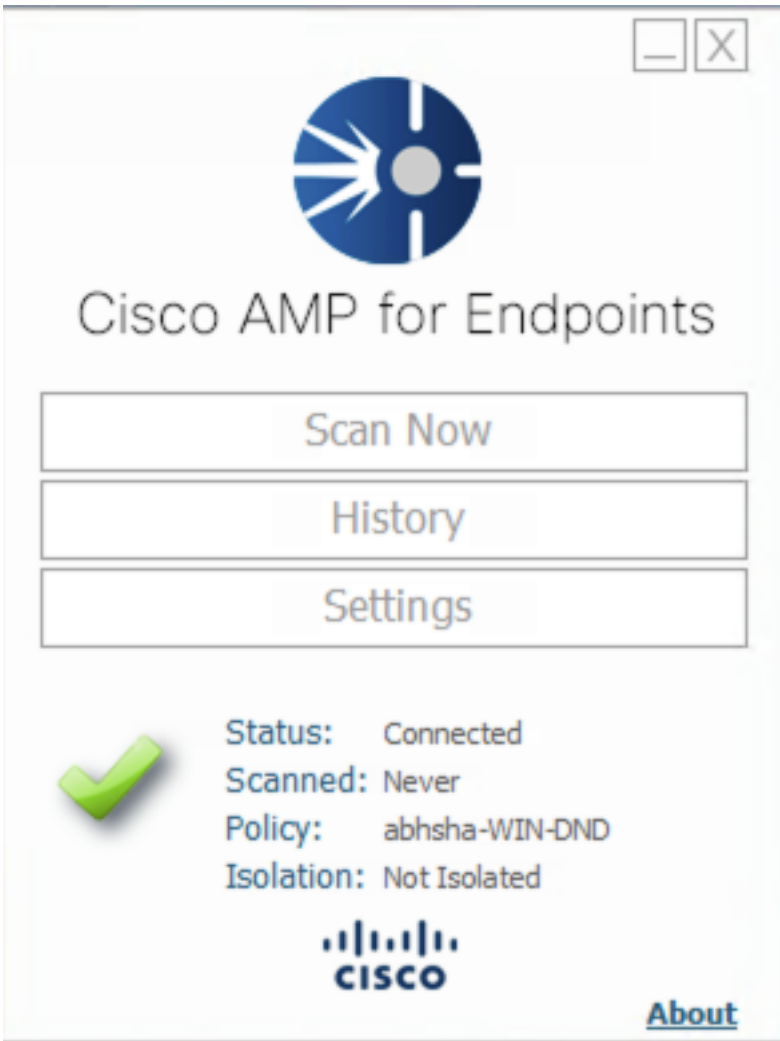
ةمدقملا

(AMP) ةراضال جماربلا نم ةمدقمتلا ةيامحل لصوصم تيبتت ةلازال اارجال دنتمسمل اذف فصي ريفوت بلطت يتلا "لصوصملا ةيامح" ةزيم ةطساوب تيبتتلا اءاغل رطح ةلاح يف Cisco نم ام ىلع كلذ فقوتيو، ةلاحلا هذه يف ناهوي رانيس كانه. هذه رورملا ةم لك نايسنو، رورم ةم لك Windows ليغشتلا ماظن ىلع هقبيبت متي. AMP ةباحسب "لصتم" رهظي لصوصملا ناك اذا طقف Windows ليغشتلا ماظن ىلع ةرفوتم ةزيم يه لصوصملا ةيامح نال ارظن، طقف

لصتم لصوصملا

ةياهنلا طاقن لصوصم Cisco AMP حتفاو ةينيصللا ةنوقيا قوف رقنا. 1. ةوطخل

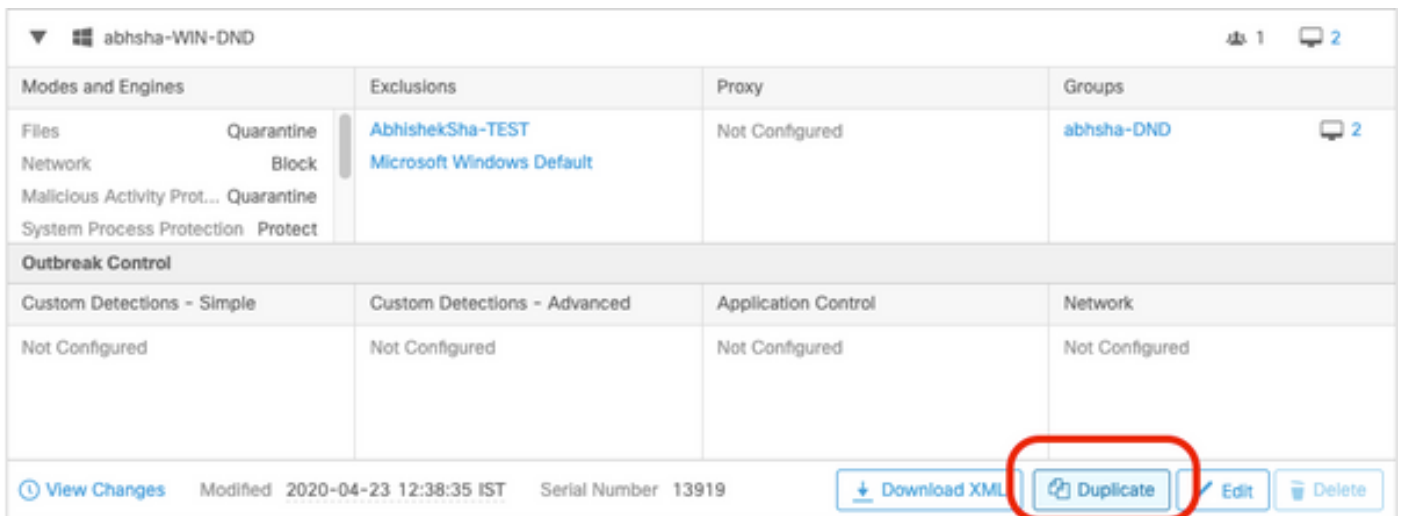
لصتم هنا ىلع لصوصملا راهظا نم دكأت. 2. ةوطخل



لوصول اذهل جهنل نييعت مت هنأ طحال 3. ةوطخل

تمت يذلا جهنل نع ثحبا م ث ةياهنل طاقن مكحت ةدحول كب صاخل AMP لى لقتنا 4. ةوطخل اقباس هت طحال م

ةروصل ي ف حضورم وه امك ةفاعضم رقن او جهنل عيسوت ب مق 5. ةوطخل



اذه ريرحتل ريرحت لى لع رقنا ".نم ةخسن" يمست ةديج ةسايس عاشنإ متيس 6. ةوطخل ةروصل ي ف حضورم وه امك جهنل

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

ة.يرادا تازيم > ةمدقم تادادع| لى لقتنا :ةسايسلا ريرحت ةحفص في 7. ةوطخل

نكمي ةديج رورم ةملك ب رورملا ةملك لدبتسا ،لصوملا رورم ةملك ةيماح ل قح في 8. ةوطخل
ةروصلال في حضورم وه امك اهؤاعدتسا

Modes and Engines

Exclusions
2 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation

Send User Name in Events i

Send Filename and Path Info i

Heartbeat Interval: 15 minutes i

Connector Log Level: Debug i

Tray Log Level: Default i

Enable Connector Protection i

Connector Protection Password:

Automated Crash Dump Uploads i

Command Line Capture i

Command Line Logging i

جهنلا اذه ظفحل ظفح زللا قوف رقنا. 9. ةوطخل

ةديج ةعومجم عاشناب مقوتاعومجم > ةرادا لى لقتنا. 10. ةوطخل

Groups

[View All Changes](#)

Search

[Create Group](#)

وه امك ظفح رز رقنا. اقبسم هريرحت مت جهنك Windows جهن دحو ةعومجم مسا لخدا. 11. ةوطخل
ةروصلال في حضورم

< New Group

Name	<input type="text" value="TZ-TEST-GROUP"/>
Description	<input type="text"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Copy of abhsha-WIN-DND - #1"/>
Android Policy	<input type="text" value="Default Policy (Vanilla Android)"/>
Mac Policy	<input type="text" value="Default Policy (Vanilla OSX)"/>
Linux Policy	<input type="text" value="Default Policy (Vanilla Linux)"/>
Network Policy	<input type="text" value="Default Policy (network_policy)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

ةلازا لواح ت يذلا رتوي بمك لال نع شح باور توي بمك لال ةزهجأ > ةرادإلا لىل ل لقتنا 12. ةوطخلال
تهل ع AMP ل صوم ت ي تبت

رهظت ي تلال ةشاشلال نم . ةعومجملال لىل ل ل قن قوف رقن باور توي بمك لال ع يسوتب مق 13. ةوطخلال
اقبسم اهئاشنإ مت ي تلال ةعومجملال دح

DESKTOP-RESMRDG in group abhsha-DND		Definitions Outdated	
Hostname	DESKTOP-RESMRDG	Group	abhsha-DND
Operating System	Windows 10 Pro	Policy	abhsha-WIN-DND
Connector Version	7.2.7.11687	Internal IP	10.197.225.213
Install Date	2020-04-23 12:35:56 IST	External IP	72.163.220.18
Connector GUID	48838c52-f04f-454a-8c3a-5e55f7366775	Last Seen	2020-04-23 12:49:01 IST
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000006f2		

[Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

30 نم رمالا قرغتسي ام ءءاع. ءءاهنلا ءطقن ىلع ءهنلا شءءء مءى ىءء رءءنا. 14 ءوطفلا اهنىوكء مء ىءءل ءرفلا ىلع ءمءءىو ءءءاو ءءاس ىلا ءقءقء.

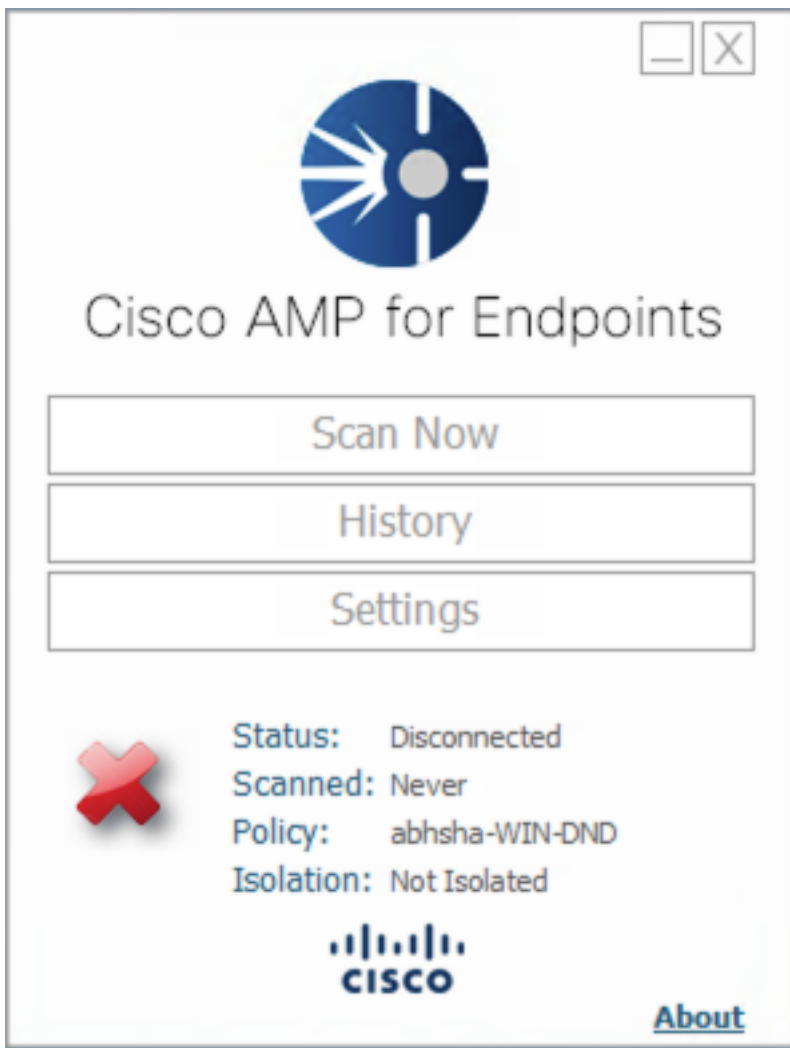
لصوملا ءىءءء ءلازا نم نءمءءس، ءءاهنلا ءطقن ىلع ءهنلا شءءء ءرءمء. 15 ءوطفلا اءءء اهنىوكءء ءمءق ىءءل رورملا ءمءك ماءءءساب.

لصوملا لاصءا ءطق مء

ءىءمء ىلع ارءاق نوكء نا ءءنءىء مءمءل نم ف، AMP ءءءءل لاصءا ءطق مء اءءنا. نم ءل ءءول ءى رءوئءمءل.

ءءاهنلا ءاقن لاصومل Cisco AMP ءءءاو ءءنءىءل ءنوءىءا قوف رءنا. 1 ءوطفلا.

لصمء رىء هنأ ىلع لاصوملا راءءل نم ءءاء. 2 ءوطفلا.



لصوملا اءءل هنءىءء مء ىءءل ءهنلا ءءءل. 3 ءوطفلا.

ءمء ىءءل ءهنلا نع شءءا مء ءءاهنلا ءاقن مءءء ءءءول ءء صءءل AMP ىلا لءءنا. 4 ءوطفلا اءءءل.

ءروصلل ءى ءءوم وه امء ءءءءءم رءنا وهءنلا ءىءوءء مء. 5 ءوطفلا.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsa-DND
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

اذه ريرحتل ريرحت قوف رقنا ".نم ةخسن" يمست ةديج ةسايس عاشنإ متيس 6. ةوطخال جهنلا

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

ةيرادا تازيم > ةمدقم تادادع| ىلإ لقتنا ،ةسايسلا ريرحت ةحفص في 7. ةوطخال

نكمي ةديج رورم ةملكب رورملا ةملك لدبتسا ،لصوملا رورم ةملك ةيامح لقي في 8. ةوطخال اهؤاعتسا

Modes and Engines	<input checked="" type="checkbox"/> Send User Name in Events <i>i</i>
Exclusions 2 exclusion sets	<input checked="" type="checkbox"/> Send Filename and Path Info <i>i</i>
Proxy	Heartbeat Interval: 15 minutes <i>i</i>
Outbreak Control	Connector Log Level: Debug <i>i</i>
Product Updates	Tray Log Level: Default <i>i</i>
Advanced Settings	<input checked="" type="checkbox"/> Enable Connector Protection <i>i</i>
Administrative Features	Connector Protection Password:
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads <i>i</i>
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture <i>i</i>
Cache	<input type="checkbox"/> Command Line Logging <i>i</i>
Endpoint Isolation	

جەنەل اذە ظفحل ظفح رزلا قوف رقنا. 9. ەوطخل

ا.ثيدح اهراركت مت يتي الة سايسال ن ع ثحباو تاسايسال > ەرادال ال ل لقتنا. 10. ەوطخل

ال policy.xml م ساب فلم ظفح متيس XML. ل لزنن قوف رقنا و جەنل عيسوتب مق. 11. ەوطخل
ل كزاه ال

abshsha-WIN-DND			
Modes and Engines	Exclusions	Proxy	Groups
Files Network Malicious Activity Prot... System Process Protection	Quarantine Block Quarantine Protect	Not Configured	abshsha-DND <i>2</i>
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured
View Changes Modified 2020-04-23 12:38:35 IST Serial Number 13919		Download XML	Duplicate Edit Delete

ە.رثأتمل الة ەطقن ال policy.xml اذە خسنا. 12. ەوطخل

ن.م آل ا عضول ال ي ە.رثأتمل الة ەطقن الة ەطقن ديەم دة. 13. ەوطخل

ال C:\Program Files\Cisco\AMP. ال ل لقتنا، ن.م آل ا عضول ال ي ە.رثأتمل الة ەطقن نوكت ن ا درجمب. 14. ەوطخل

ال ال فلم ال اذە ەيمست دة او policy.xml م ساب فلم ن ع ثحبا، دلجم ال اذە ي. 15. ەوطخل
policy_old.xml.

Name	Date modified	Type	Size
update	4/23/2020 11:59 AM	File folder	
URLScanner	4/23/2020 11:59 AM	File folder	
2020-04-23 11-59-18	4/23/2020 11:59 AM	Windows Perform...	0 KB
cache	4/23/2020 12:33 PM	Data Base File	252 KB
cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	4,036 KB
filetypes	4/23/2020 11:59 AM	XML Document	3 KB
history	4/23/2020 12:34 PM	Data Base File	68 KB
historyex	4/23/2020 11:59 AM	Data Base File	4 KB
historyex.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
historyex.db-wal	4/23/2020 12:27 PM	DB-WAL File	137 KB
jobs	4/23/2020 11:59 AM	Data Base File	4 KB
jobs.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
jobs.db-wal	4/23/2020 11:59 AM	DB-WAL File	13 KB
local.old	4/23/2020 12:32 PM	OLD File	4 KB
local	4/23/2020 12:32 PM	XML Document	4 KB
nfm_cache	4/23/2020 11:59 AM	Data Base File	4 KB
nfm_cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
nfm_cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	61 KB
nfm_url_file_map	4/23/2020 11:59 AM	Data Base File	4 KB
nfm_url_file_map.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
nfm_url_file_map.db-wal	4/23/2020 12:08 PM	DB-WAL File	45 KB
policy	4/23/2020 12:30 PM	XML Document	20 KB

دلجمل اذه يف اق بسم هخسن مت يذال **policy.xml** قصلال، نآلا 16 ةوطخلال

ةملك ةبلاطم يف و ي ع ي ب ط لك شب تي بثلال ةلازا عارجا نكمي، فللمل خسن دع ب 17 ةوطخلال
اثيرح اهنويوكت مت يتل رورمل ةملك لاخدا بجي، رورمل

يقببيس، زاهال لاصتا عطق دنع لوصومل تي بثلال ةلازال ارطن. ةيرايتخا ةوطخ هذو 18 ةوطخلال
رتوي بملك ةزهجا > ةرادال ال لاقنتال كنكمي، كلذل. مكلحتال ةدحو يل ع رتوي بملك لاخدا
ةياهال ةطقن فذل فذل قوف رقنا. ةراثملال ةياهال ةطقن عيسوتو

ةمچرتل هذه لوج

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