

نم اهنويوكتو AMP ةيظمنلا ةدحوللا تيبتت AMP و AnyConnect 4.x نيكمت ةادالخالخ

تايوتحمل

[ةمدقملا](#)

[ةيساسالابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ASA نيكمت ةادا AnyConnect AMP Enabler ل رشن](#)

[AnyConnect AMP Enabler ليمع فيرعت فلم نيوكت 1: ةوطخلال](#)

[AnyConnect AMP Enabler ليزنتل ةومجملا ةسايس ريرحت 2: ةوطخلال](#)

[FireAMP جهن ليزنت 3: ةوطخلال](#)

[بيولا نامأ ليمع فيرعت فلم ليزنت 4: ةوطخلال](#)

[ةيظمنلا ةدحوللا تيبتت نم ققحتو AnyConnect ب لصلتا 5: ةوطخلال](#)

[لصوم AMP و Start نم VPN لصلتا تيبتت نيكمت ةادا 6: ةوطخلال](#)

[عيش لك تيبتت نم ققحتو AnyConnect نم ققحت 7: ةوطخلال](#)

[Zombies PDF فلم في ةنمضتملا eicar ةلسلس مادختساب ربتخا 8: ةوطخلال](#)

[رشنلا صلخم 9: ةوطخلال](#)

[طبارتلل تارشوم فاشتك نم ققحتللا 10: ةوطخلال](#)

[ةيفاضا تامولعم](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

(AMP) "ةراضلا جماربللا نم ةمدقتملا ةياملال" لصوم تيبتت تاوطخب دننتملا اذه رمي AnyConnect مادختساب.

الاهنوا امك. ةياهنلا طاقنل AMP رشنل طيسوك AnyConnect AMP نيكمت ةادا مادختسا متي طاقنل AMP جماربل عفدي وهو. تافللملا في فرصتلا ةيلمع ةنادا يلع ةردق يا كملت نم ققحتلل ةباحسلا ةعس مدختسي، AMP تيبتت درجمب ASA. نم ةياهن ةطقن يلا ةياهنلا يمسي يكيما نيدي ليحت يلا تافللملا لاسرا ةيفاضا ل AMP ةمدخل نكمي. تافللملا ريصم تافللك تافللملا هذه يلع مكحل نكمي. فورعم ريغ تافللم كولس ليجستل ThreatGrid، مويلا تامجهل عساو قاطن يلع دي فم اذهو. ةقيقدلا ريغ جئاتنلا ضعيب عافولا مت اذا ةراض رفس.

ةيساسالابلطتملا

تابلطتملا

- AnyConnect Secure Mobility Client، 4.x رادصللا
- FireAMP / AMP طاقنل
- Adaptive Security Device Manager (ASDM)، 7.3.2 رادصللا وأ

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربال تارادصا اذف ةدراولا تامولعمل دنتست

- 9.5.1 جم انربلا رادصا عم 5525 (ASA) فيكتلل لباقلا نامألا زاهج
- AnyConnect Secure Mobility Client 4.2.00096 Microsoft Windows 7 ليغشتلا ماظن اذف
تب 64 رادصا Professional
- ASDM رادصا 7.5.1(112)

ASA نيكمت ةادا) AnyConnect AMP Enabler رشن

يولي اماك نيوكتلا في ةينعمل تاوطخلا نوكت:

- AnyConnect AMP Enabler ليمع فيرعت فلم نيوكت.
- AMP Enabler ةمدخ فيرعت فلم ليزنتو AnyConnect VPN ةومجم جهن ريرحتب مق
- صاخلا URL ليزنت طايترا اذف لوصحلل AMP تامولعمل ةحول اذف لوخدلا ليجستب مق
لصوملاب.
- ممدختسملا زاهج اذف تيبتتلا نم ققحت.

AnyConnect AMP Enabler ليمع فيرعت فلم نيوكت: 1 ةوطخلا

- Remote Access VPN (ذعب نع لوصول) > Network (اليمعلا) Access > AnyConnect Client Profile.
- AMP نيكمت ةمدخ فيرعت فلم ةافاضا.

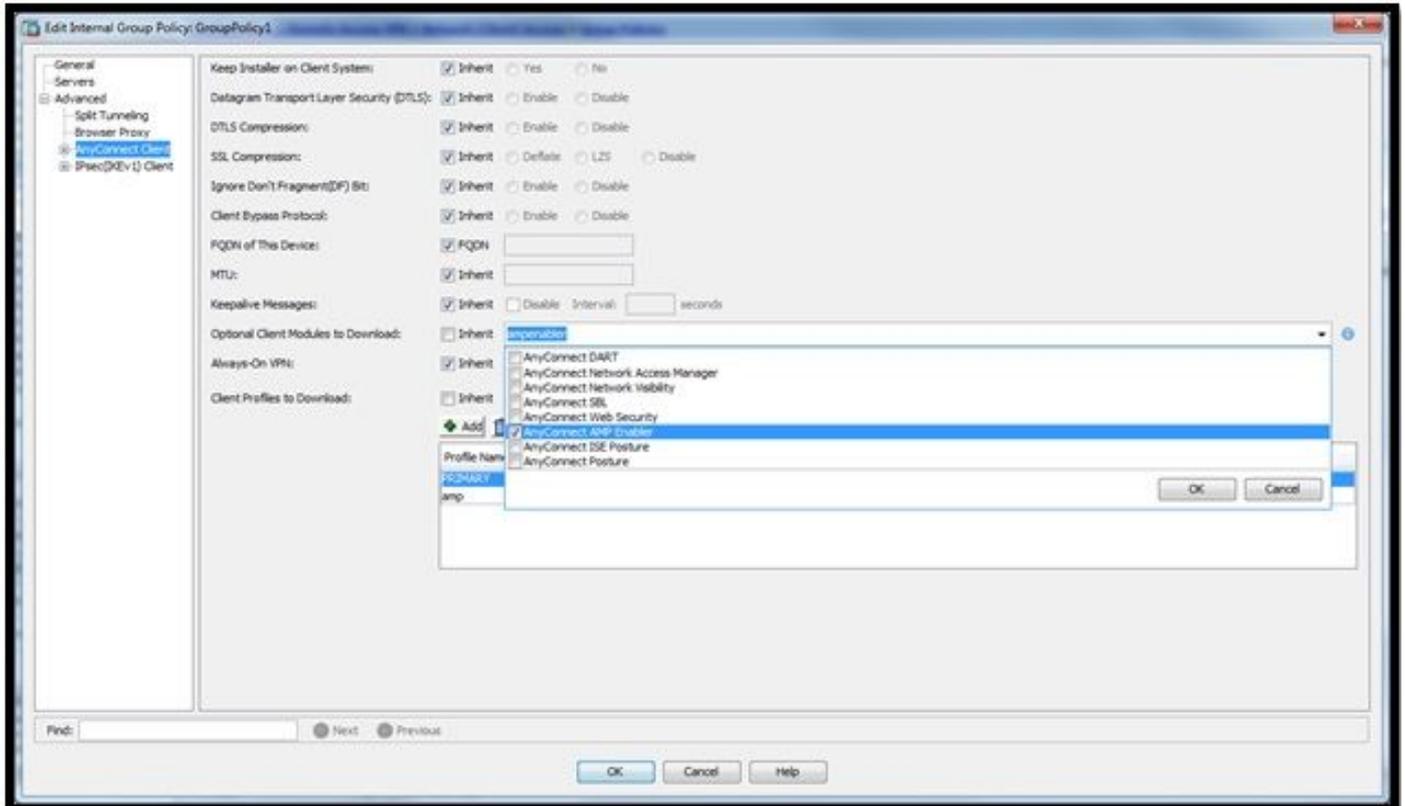
The screenshot shows the 'Add AnyConnect Client Profile' dialog box. The toolbar includes 'Add', 'Edit', 'Change Group Policy', 'Delete', 'Import', 'Export', and 'Validate'. The main area has the following fields and buttons:

- Profile Name:** amp
- Profile Usage:** AMP Enabler Service Profile
- Profile Location:** disk0:/amp.asp. Buttons: Browse Flash..., Upload...
- Group Policy:** <Unassigned>
- Enable 'Always On VPN' for selected group
- Buttons:** OK, Cancel, Help

Profile Name	Profile Usage	Group Policy	Profile Location
PRIMARY	AnyConnect VPN Profile	GroupPolicy1	disk0:/primary.xml
amp	AMP Enabler Service Profile	GroupPolicy1	disk0:/amp.asp

AnyConnect AMP Enabler ليزننتل ةومجمل ةسايس ريرحت : 2 ةوطخلال

- ريرحت > ةومجمل جهن > Access VPN ةلازا > نيوكتلال لال لقتنا
- لهمل ةادحو > (AnyConnect لهمل) AnyConnect Client > ةمدقتم ةارايل لال لقتنا
اهل ليزننتل ةيراي ةخالال
- AnyConnect AMP نيكم ةادار ةخأ.



FireAMP جهن ليزننت : 3 ةوطخلال

ةياهنل طاقنل AMP تابلطتمب يف كماظن ناك اذا امم ققحت ،ةعباتملا لبق :ةظالم ل Windows Connector.

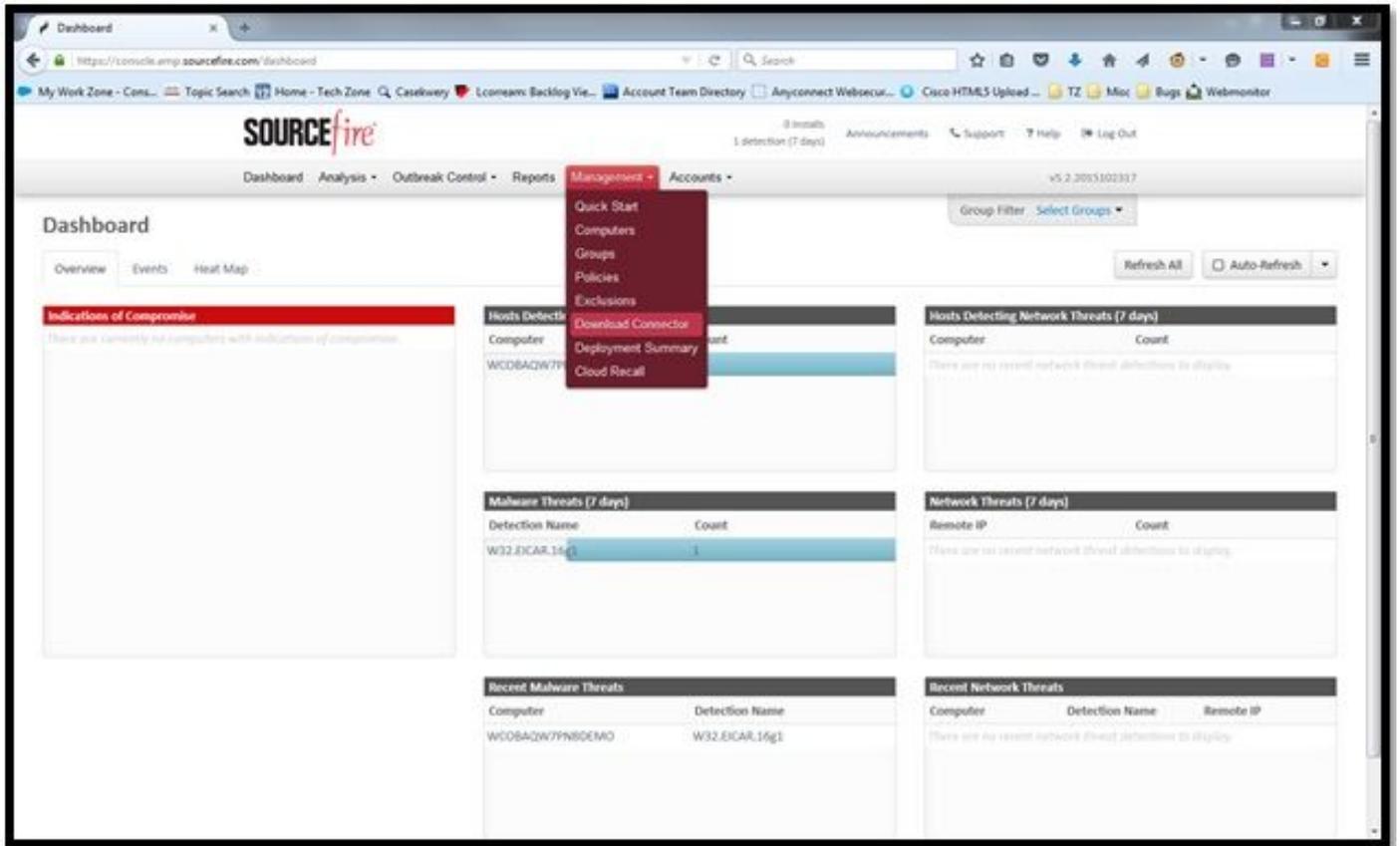
Windows Connector ةياهنل طاقنل AMP ل ماظنل تابلطتم

ليغشتلا ماظن ل اذانتسا FireAMP ل صومل ماظنل تابلطتمل ىندأل دحلل يه هذه نكمي .هذه ليغشتلا ةمظنأل تب 64 و 32 ني رادصال نم الك FireAMP ل صوم معدني .Windows [AMP رشن](#) يف AMP قئاثو ثدحأ يل ع روثعل

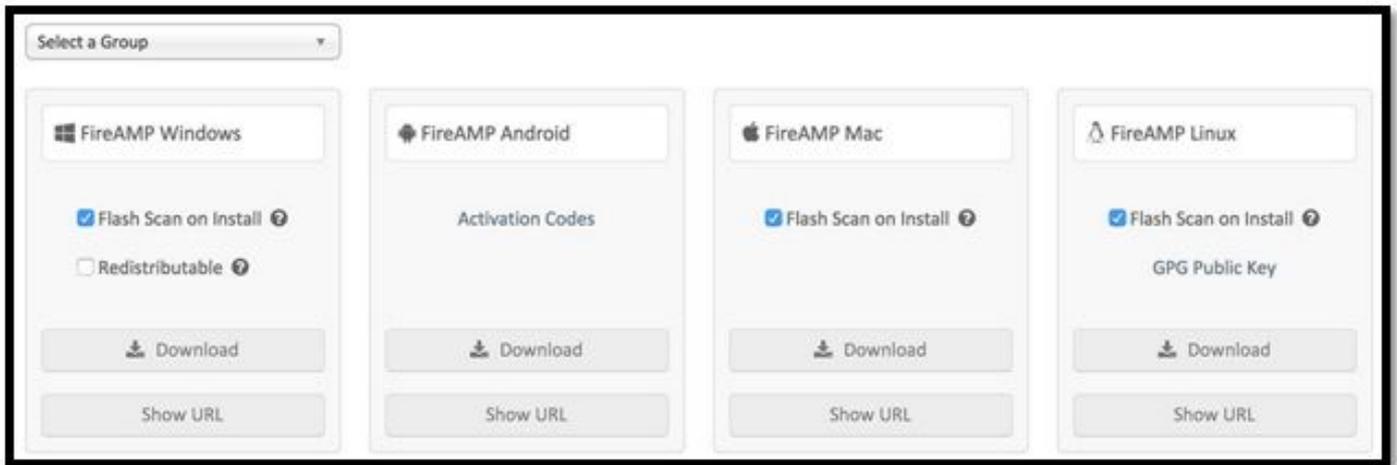
ل يغشت ماظن	جل اعمل	ةركاذ	صرق ل ةحاسم ، ةباحس ل ا عضو طقف	صرق ل ةحاسم
ليغشتلا ماظن Microsoft Windows 7	1 ةعرسب جل اعمل وأ زتره اچيچ عرسأ	ل و ص و ةركاذ (RAM) يئ او ش ع 1 ةع س تي ا با چيچ	صرق ل ةحاسم ةرفو تم تباث 150 ةع س - تي ا با چيچ ةباحس ل ا عضو طقف	صرق ل ةحاسم ةرفو تم تباث 1 ةع سب - تي ا با چيچ Tetra
Microsoft Windows 8 و 8.1 (ل صوم بل طتي) FireAMP 5.1.3 وأ (ثدحأ)	1 ةعرسب جل اعمل وأ زتره اچيچ عرسأ	ل و ص و ةركاذ (RAM) يئ او ش ع 512 ةع س تي ا با چيچ	صرق ل ةحاسم ةرفو تم تباث 150 ةع س - تي ا با چيچ ةباحس ل ا عضو طقف	صرق ل ةحاسم ةرفو تم تباث 1 ةع سب - تي ا با چيچ Tetra
ليغشتلا ماظن Microsoft Windows Server 2003	1 ةعرسب جل اعمل وأ زتره اچيچ عرسأ	ل و ص و ةركاذ (RAM) يئ او ش ع 512 ةع س تي ا با چيچ	صرق ل ةحاسم ةرفو تم تباث 150 ةع س - تي ا با چيچ ةباحس ل ا عضو طقف	صرق ل ةحاسم ةرفو تم تباث 1 ةع سب - تي ا با چيچ Tetra
ليغشتلا ماظن Microsoft Windows Server 2008	2 ةعرسب جل اعمل وأ زتره اچيچ عرسأ	ل و ص و ةركاذ (RAM) يئ او ش ع 2 ةع س تي ا با چيچ	صرق ل ةحاسم ةرفو تم تباث 150 ةع س - تي ا با چيچ ةباحس ل ا عضو طقف	صرق ل ةحاسم ةرفو تم تباث 1 ةع سب - تي ا با چيچ Tetra
Microsoft Windows Server 2012 (بل طتي) FireAMP Connector 5.1.3 (ثدحأ وأ)	2 ةعرسب جل اعمل وأ زتره اچيچ عرسأ	ل و ص و ةركاذ (RAM) يئ او ش ع 2 ةع س تي ا با چيچ	صرق ل ةحاسم ةرفو تم تباث 150 ةع س - تي ا با چيچ ةباحس ل ا عضو طقف	صرق ل ةحاسم 1 ةرفو تم بل ص - تي ا با چيچ Tetra

تاسس ؤملا ب صاخالل بيولا مداخ يل ع AMP تي ب ثت ةادا عضو وه ةيغلل عئاش .

ليزنتب مقو ةباتكل رتخأ مث .ل صومل ليزنت > ةرادلال يل ل لقتنا ،ل صومل ليزنتل (Windows و Android و Mac و Linux) FireAMP .



FireAMP تالصوم نم عون لك لتي بثت ل مزح لي زنت "لصوم ل ليزنت" ؤحفص كل حيتت ةرادل اجم ان رب ربع اه عيزوت وا ؤكبش ؤكراشم يل ؤمزحل هذه عضو نكم ي.



ةوعومج ديدحت

- لم عي ال فلم لك يل ؤسوم ل SHA-256 يل اذانتسا ماظن ل ؤبقارم :طقف ؤعجارم ل هيبنتك اذح لسري هنكلو، ؤراض ل اجم ار بل لزع يل ؤه قي قذت ل عضو.
- اهل قنو تافل ل ؤسن ؤبقارم .لزع ل ؤراض تافل لم ماذختسا ب عضو ل ؤيامح :ةيامح ل.
- لعل فابل باصم/ل لخب هب رت ووي بكم زاخ يل ؤ ماذختسا ل ل اذح :زر فل.
- Tetra كرحم نوب ل لصوم ل تي بثت متي شيح ، Windows مداخل تي بثت ؤوعومج :مداخل اجم كحت ل اذحو مداخل اهمسا ماذختسا ب ؤوعومج ل هذه ميمصت مت DFC لي غشت اجم ان رب و ل اجم ل اب ريغ.
- قي قذت ل عضو يل ؤوعومج ل هذه ل يضارت فال اجهن ل ني عت مت :ل اجم ل اب م كحت ل ؤدحو ؤوعومج ل هذه في Active Directory مداول ؤوعومج في ل اجم ل وه امك Windows ل اجم ل اب م كحت ل ؤدحو يل ؤه لي غشت متي س ل لصوم ل نأ ين عي امم.

رايخالا اذه. لمالكالب تاسوري فلل داضم كرحم يه و ارتيت يعدت ةزي م زاهجال اذه عتمت ي و اذه جهن لك ل يراي تخا

تازي مل

- اناثا يئوضلا حسملا ةي لمع ليغشت متي :تتبتتال دنع يئوضلا حسملا ةزي م . طقف ةدحاو ةرم هليغشتب ي صوي و ذيفنتال ي ف اي بسن عي رس وه . تتبتتال
- تب 64 و تب 32 تاتبتت يلع يوتحت ، ةدحاو ةدحاو ةم زح لي زنت بجي : عيزوتال ةداعل لباق . ددحم ريغ رايخالا اذه كرتتال ةرفوت م نوكت ي تال او ، رتوي بمكلا ليغشت ديهمت ةادأ نم ال دب . اذهذيفنت درجم ب ، تتبتتال ةادأ تافل م لي زنت و

عضو وه ضرغلا . اهب نرتقملا جهنلا نيوكت و ةصاخلا كتعومجم عاشن كنكمي : ةظخال م ي ف جهنلا نوكي شيح ، ةدحاو ةعومجم ي ف لاثملا ل بس يلع Active Directory مداوخ ةفاك قيقدتال عضو

م تي policy.xml فلم يلع redistribution و bootstrapper تتبتت ةادأ نم لك يوتحي امك AMP . ل صومل نيوكت فلمك هم ادختسا

ببول ناما ليمع فيرعت فلم لي زنت : 4 ةوطخال

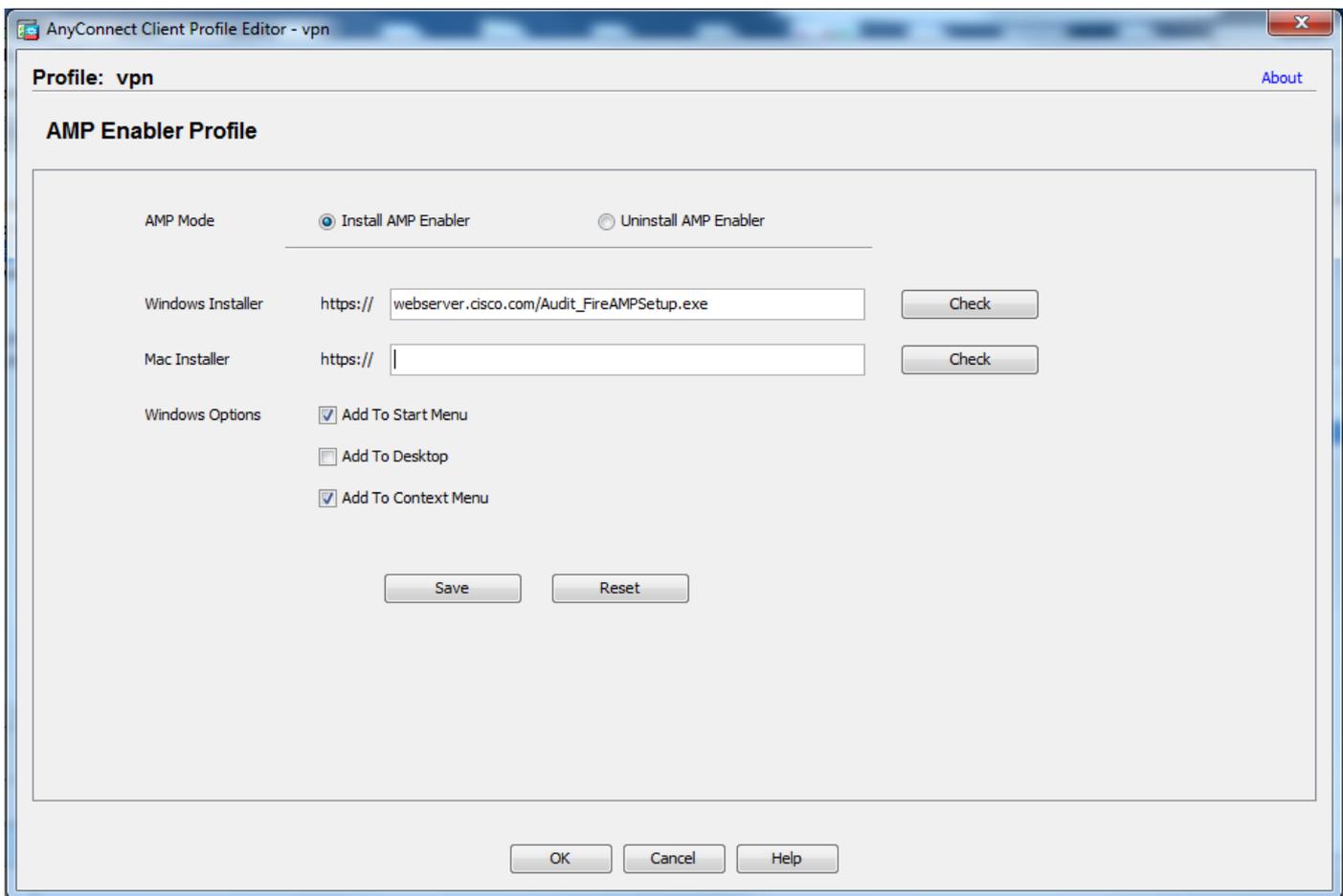
ي ف مادختسالا عئاش وه . AMP تتبتت ةادأ عم ةكبش ةكراشم وأ ةكرشل لب ي و مداخ دي دحت ي زكرم عقوم ي ف ةقوئوملا تاتبتتال عضو و ي ددرتال قاطنلا ريفوتل تاكرشال عي مج

ي ف أطخيأ نودب ةياهنلا طاقن يلع HTTPS طابترال ي ل لوصول كنكمي هنأ نم دكأتل اعجلال . ةزهجال نزخم ي ف ةتبتتال ةساسالا ةداهشلا نأ و ةداهشلا

فلم ريرحتو (1 ةوطخال) ASA يلع لبق نم هؤاشنإ مت يذال AMP فيرعت فلم يلع ةدوعال **AMP** نيكمت ةادأ فيرعت

1. AMP Radio نيكمت ةادأ تتبتت رزلا قوف رقنا ، AMP عضول ةبسنلاب .
2. FireAMP ل فلملا و ببول مداخل IP ةفاضاب مق ، Windows Installer ل قح ي ف .
3. ةيرايتخا Windows ليغشتال ماظن تاراخي .

تاريغيغتلال قبطو ok ةقطق



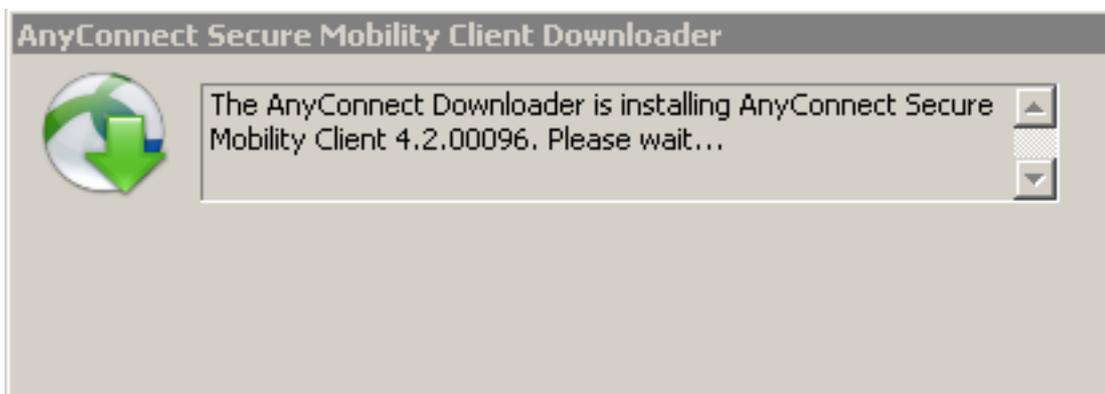
ةيظمنلا ةدحوللا تيبتت نم ققحتو AnyConnect ب لصتا :5 ةوطخل

نم AnyConnect AMP نيكم ت ةدحو عفدب ASA موقبي، AnyConnect VPN يمدختسم لاصتا دن ع مهلوخد ليجست مت نينذل نيمدختسم لل ةبسنلاب (VPN). ةيرهاطلا ةصاخلا ةكبشلا لال خ ةفيظوللا نيكم تل رخأ ةرم لوخدلا ليجست مت جورخلا ليجستب ي صوي، لعفلاب

```

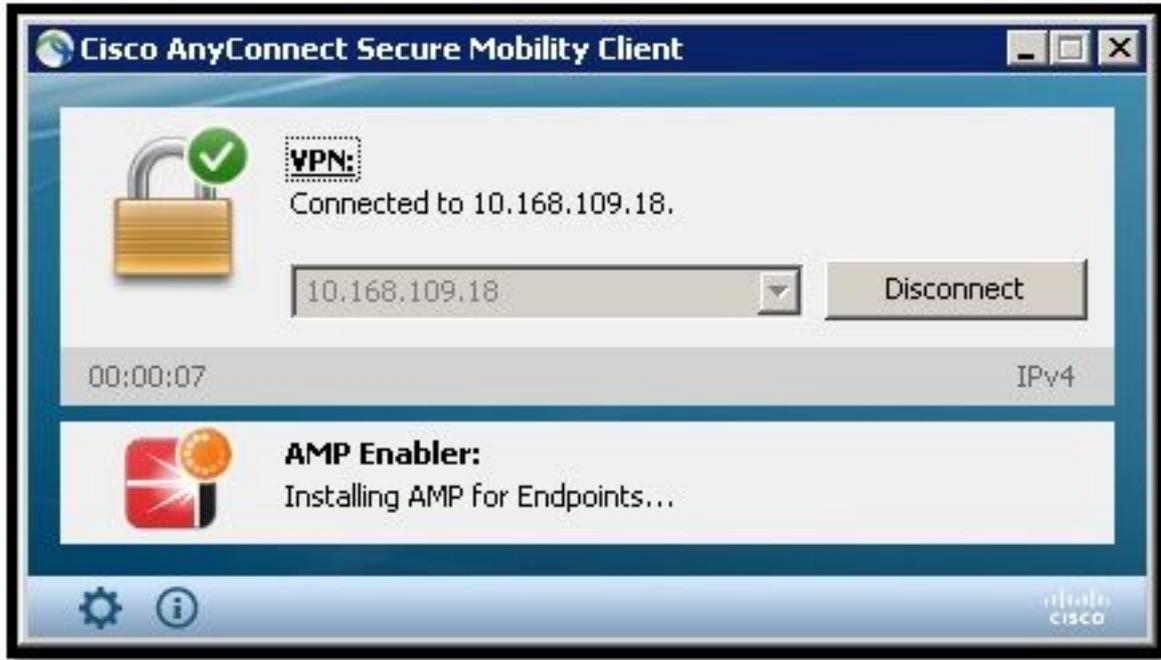
10:08:29 AM Establishing VPN session...
10:08:29 AM The AnyConnect Downloader is performing update checks...
10:08:29 AM Checking for profile updates...
10:08:29 AM Checking for product updates...
10:08:31 AM Downloading AnyConnect AMP Enabler 4.4.01054 - 48%
10:08:32 AM Downloading AnyConnect AMP Enabler 4.4.01054 - 91%
10:08:33 AM Downloading AnyConnect AMP Enabler 4.4.01054 - 100%

```



لصوم AMP و Start نم VPN لاصتا تيبتت نيكم ت ةادأ :6 ةوطخل

نمضتيس. ةيطمن ةدحو ليزنت ديدجلا لزنني وه، VPN لا أدبي نأ طبري رزلا تنأ طغضي نإ ام نيتوطخ لبق هتدح يذلا URL ناونع راسم نم AMP ةمزح ليزنتب موقيو AMP نيكمم ةادأ اذه.



If you look at the event viewer:

AMP enabler install:

Date : 04/24/2017
Time : 10:08:34
Type : Information
Source : acvpndownloader

Description : Cisco AnyConnect Secure Mobility Client Downloader (2) exiting, version 4.4.01054 , return code 0 [0x00000000]

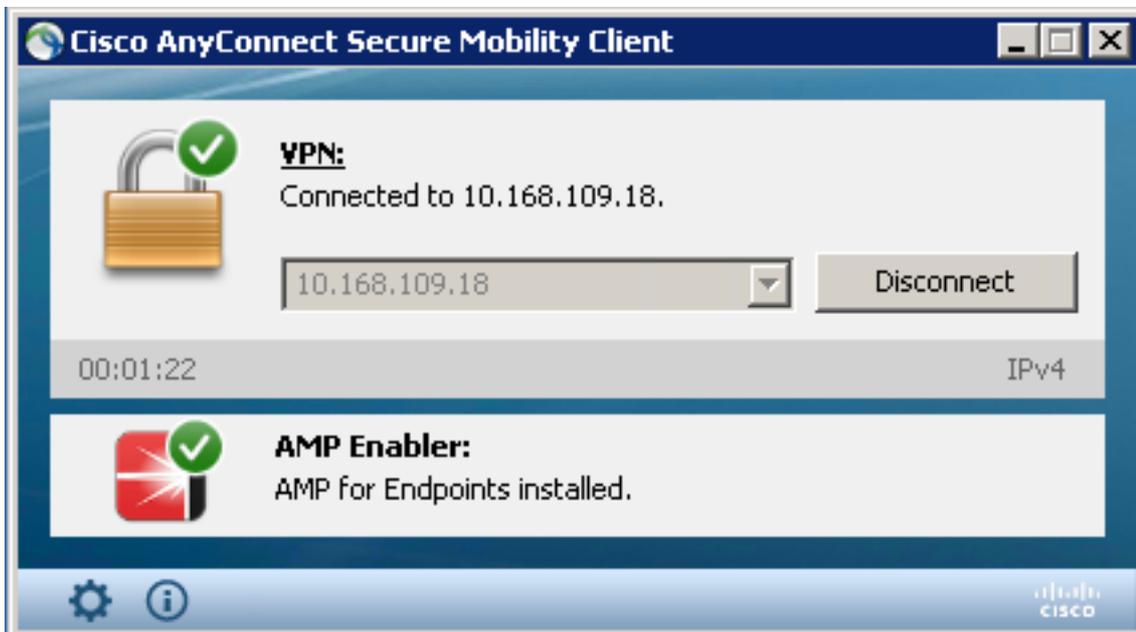
ءيش لك تيبتت نم ققحتو AnyConnect نم ققحت :7 ةوطخلا

نم ققحت، بيولا مداخ نيوكت تيبتتو (VPN) ةيره اظلال ةصاخلا ةكبشلا ليصوت درجمب ححص لكشب ءيش لك تيبتت نم ققحتو AnyConnect.

PowerShell رمأ ي CiscoAMP_5.1.3 مسمت ةديج ةمدخ ىلع روثلعلا كنكمي services.msc في ىرن:

```
PS C:\Users\winUser348> Get-Service -name "*CiscoAMP*"
```

Status	Name	DisplayName
Running	CiscoAMP_5.1.3	Cisco AMP for Endpoints Connector 5...



رمألا مدختست دق Windows لىغشتال ماظن ىلإ ةديج لىغشت جمارب AMP تبثم فيضي تافدارمل درس ل driveQuery.

```
C:\Windows\System32>driverquery /v | findstr immunet
```

```

ImmunetProte ImmunetProtectDriver ImmunetProtectDriver File System System Running
OK TRUE FA
LSE 4,096 69,632 0 3/17/2017 5:04:20 PM
\??\C:\WINDOWS\System32\Drivers\immunetprotect.s 8,192

ImmunetSelfP ImmunetSelfProtectDriv ImmunetSelfProtectDriv File System System Running
OK TRUE FA
LSE 4,096 28,672 0 3/17/2017 5:04:08 PM
\??\C:\WINDOWS\System32\Drivers\immunetselfprote 8,192

```

Zombies PDF فلم في ةنمضتمل eicar ةلسلس مادختساب ربتخا: 8 ةوطخلال

يرابتخا بساح في Zombies PDF فلم في ةدوجوم راكإ ةلسلس مادختساب رابتخالاب مق راضل فلمل لزع نم ققحتلل.

The screenshot shows a web browser window with the URL <https://mysite.science.uottawa.ca/rsmith43/Zombies.pdf>. The document content includes:

In: Infectious Disease Modelling Research Progress ISBN 978-1-60741-34-4
 Editors: J.M. Tchuente and C. Chiyaka, pp. 133-150 2009 Nova Science Publishers,

Chapter 4

WHEN ZOMBIES ATTACK!: MATHEMATICAL MODELLING OF AN OUTBREAK OF ZOMBIE INFECTION

Philip Munz^{1}, Ioan Hudea^{1†}, Joe Imad^{2†}, Robert J. Smith^{2,3§}*

¹School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada
²Department of Mathematics, The University of Ottawa, 585 King Edward Ave, Ottawa ON K1N 6N5, Canada
³Department of Mathematics and Faculty of Medicine, The University of Ottawa, 585 King Edward Ave, Ottawa ON K1N 6N5, Canada

Abstract

Zombies are a popular figure in pop culture/entertainment and they are usually portrayed as being brought about through an outbreak or epidemic. Consequently, we model a zombie attack, using biological assumptions based on popular zombie

Overlaid on the page are two windows:

- Otevíráni Zombies.pdf**: A dialog box asking to open the file 'Zombies.pdf' (302 KB) from the URL. It offers options to 'Otevřít pomocí Adobe Acrobat Reader DC (výchozí)', 'Uložit soubor', or 'Provádět od teď automaticky s podobnými soubory'.
- Cisco AMP Warning!**: A warning message stating 'Threat Quarantined' and '43p1CE_x.pdf part has been detected as W32.Zombies.NoAVirus. Quarantine was successful.'

راكبي ةلسلس ىلع ع Zombies.pdf يوتحي

رشننلا صخلم 9: ةوطخلال

ةلشافلاو ةحجانلا FireAMP تالصوصم تيبتت تايلمعب ةمئاق ةحفصلا هذه كل رهظت رشننلا صخلم > ةرادلال ىل لاق تنالال كنكمي. ايلاح مدقتلا دي ق كلت ىل ةفاضللاب

The screenshot shows the Sourcefire dashboard interface. At the top, it displays '0 installs' and '1 detection (7 days)'. The main section is titled 'Deployment Summary' and includes a 'Group Filter' dropdown set to 'Select Groups'. Below this, there are tabs for 'All', 'Successful', 'Installing', and 'Failed' deployments. A table shows the following deployment record:

✓ Hostname	Version	OS	Timestamp	Last Error
WCOBAQW7PNBDEMO 10.168.109.41 / 00:23:24:54:93:5c 10.10.10.1 / 00:05:9a:3c:7a:00	4.2.1.10103	Windows 7, SP 1.0	2015-11-19 15:14:38 UTC	None.

At the bottom, it indicates 'Showing 1 - 1 of 1 total records' and provides an 'Export to CSV' button.

طبارتلل تارشؤم فاشتكا نم ققحتلا: ةوطخلال

AMP تامول عم ةحول ىل لاسراب مق ،لزع شح لىغش تب Zombies.pdf ماق

The screenshot shows the Cisco AMP for Endpoints dashboard. At the top, there's a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is also present. Below this, a notification banner for 'New AMP for Endpoints Linux Connector' is visible. The main dashboard area has tabs for 'Dashboard', 'Inbox', 'Overview', 'Events', and 'Heat Map'. A filter section allows users to select event types and groups. The main content area displays a file detection event: 'DJANULIK-HYYPD.cisco.com detected 4XpjCE_X.pdf.part as W32.Zombies.NotAVirus'. The event details include: Detection (W32.Zombies.NotAVirus), Fingerprint (SHA-256) (00b32c34...989bb002), Filename (4XpjCE_X.pdf.part), Filepath (C:\Users\djanulik\AppData\Local\Temp\4XpjCE_X.pdf.part), File Size (bytes) (309500), Parent Fingerprint (SHA-256) (0fff6b17...5fd32be), and Parent Filename (firefox.exe). The event is dated 2017-07-27 13:32:08 UTC and has a status of 'Quarantine: Successful'. There are buttons for 'Report', 'Restore File', and 'All Computers' at the bottom of the event details.

لزع ل شح

ةففاضل تامول عم

ةماع ةرطن اذه كحنمى .ATS ةعماج فى لىجستلا كنكمى ،كب صاخلا AMP باسح ىلع لوصحلل Lab فى AMP فئاظو ىلع

ةلص تاذا تامول عم

- [AMP نىكمت ةادا نىوكت](#)
- [تادنتس مل او ىنقتلا مرعدلا - Cisco Systems](#)

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 ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل