ءاغلإو Sourcefire مدختسم ليكو تيبثت ەتيبثت

تايوتحملا

قمدق مليا قمدق مليا مي سياس أليا تياب لطتم تي بثنايا تياب لطتم مدختس م ليماع تي بثت قليانا الم الم او تي بثنايا قليانا عاطخاً فاش كتس أ ضيعليا

ةمدقملا

ليغشتلا ماظن ىلع ەتيبثت ةلازا وأ "مدختسم ليمع" تيبثت ةيفيك دنتسملا اذه حضوي Microsoft Active Directory مدختسم ليمع" موقي Microsoft Windows. لوكوتوربلا ربع اەتقداصم تمت يتلا بحسلاو لوخدلا ليجست تايلمع نع غالبإلاو Lightweight Directory Access Protocol (LDAP) ماظن موقي .(FireSIGHT ماخنم موقي عرم تالجسلا ا قزهجألا ةطساوب قرشابملا ةكبشلا رورم ةكرح قبقارم لالخ نم اهعمجي يتلا تامولعملا .

ةيساسألا تابلطتملا

يصوت Cisco و Sourcefire User ب ةفرعم كيدل نوكت نأب Sourcefire User يموت Agent، و Active Directory.

تيبثتلا تابلطتم

- Active Directory مداوخ یل TCP/IP لوصو
- MET Framework، تايعبت ةفاك نمضتي) 4.0 رادصإلا ،NET Framework

Sourcefire مدختسم لماع تيبثت

- . معدلا عقوم نم تيبثتلا ةادأ فلم ليزنتب مق.
- .مدختسملا لماع تيبثت ديرت ثيح Windows ماظن ىلإ setup،exe فلم خسنا .2
- .دادعإلا جلاعم رەظي .Sourcefire مدختسم ليكو تيبثت ةادأ فلم ىلع اجودزم ارقن رقنا .3

فيضم ىلع قديدج تاقىبطت تىبثتل تانوذأ كىدل نكى مل اذإ :قظحالم ءدبل قبسانملا تانوذألا مادختساب يرادإ مدختسم ىلإ دىعصتلا كنكمى دادعإ فلم قوف نميألا سواملا رزب رقنا ،ديعصتلا رايخ ىلإ لوصولل .تيبثتلا مقو ايرادإ امدختسم رتخأ .مساب ليغشت رتخاو 2.0 Sourcefire مدختسملا ليكو .قبسانملا رورملا قملك ريفوتب

جلاعم موقي نأ لبق ةلاسرلا هذه ىقلتتسف ،تيبثتلا تابلطتمب ءافولا متي مل اذا معن قوف رقنا .هتيبثتو 4.0 رادصإلا Microsoft .NET Framework ليزنتب دادعإلا معن قام معن قرف رقنا .متيبثتل تاميلعتلا العبتا .ليزنتلا ةحفص ىل القتنالل Microsoft .NET Framework، تيبثتل تاميلعتلا عبتا .ليزنتلا ةحفص ىل القتنالل 4.0. رادصإلا

🔂 User Agent	×
This setup requires the .NET Framework version 4.0. Please install the .NET Framework and run this setup again. The .NET Framework can be obtained from the web. Would you like to do this now?	ork. d
Yes No	

قوف اجودزم ارقن رقنا ،4.0 رادصإلا Microsoft .NET Framework تيبثت لامتكا درجمب .4 دادعإلا جلاعم رەظي .ىرخأ ةرم "Sourcefire مدختسم ليكو تبثم" فلم.

باسح يف مكحتلا" نيكمت عم Microsoft Windows نم رادصإ ليغشتب تمق اذإ قوف جودزملا رقنلا دعب راوحلا عبرم نم عبرملا اذه ميدقت متيسف ،"(UAC) مدختسملا مدختسم ليكو تبثمل حامسلل معن قوف رقنا ."Sourcefire مدختسم ليكو تبثم" فلم مدختسم ليكو" تيبثت ةادأ ءاغلإل ال قوف رقنا .ماظنلا ىلع تارييغت ءارجإب Sourcefire Sourcefire اهنم جورخلاو "

15	User Ag	ent		
I	nstalli	ing User Ag	gent coupor(•
	🌍 Usei	r Account Contro	ol X	1 re
ι	Do you want to allow the following program from an unknown publisher to make changes to this computer?			
		Program name: Publisher: File origin:	C:\Users\ \De\Sourcefire_User_Agent_2.0.0-34_Setup.msi Unknown Hard drive on this computer	
	•	Show details	Yes No Change when these notifications appear	
			Cancel < Back Next >	

رمألا ءاغلإ قوف رقنا. Sourcefire مدختسم لماع دادعإ جلاعم ةعباتمل يلاتلا قوف رقنا. مدختسم لماع دادعإ جلاعم نم جورخلل

🙀 User Agent			_ 🗆 🗙
Welcome to the User Ag	jent Setup W	izard SOURC	fire
The installer will guide you through the steps required to install User Agent on your computer.			
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.			
	Cancel	< Back N	ext >

هيف Sourcefire مدختسملا لماع تيبثت ديرت يذلا دلجملا ديدحتل ضارعتسا قوف رقنا .6 مدختسم لماع دادعا جلاعم نم جورخلل رمألا ءاغلإ قوف رقنا .يلاتلا قوف رقنا مث Sourcefire.

🖶 User Agent		
Select Installation Folde)r	sourcefire [*]
The installer will install User Agent to the To install in this folder, click "Next". To ir Folder:	following folder. nstall to a different folder, enter it t	below or click "Browse".
C:\Program Files (x86)\Sourcefire\Us	er Agent'\	Browse Disk Cost
	Cancel < Bac	k Next>

لماع دادعإ جلاعم نم جورخلل رمألا ءاغلإ قوف رقنا .تيبثتلا ءدبل يلاتلا ىلع رقنا .7 مدختسم Sourcefire.

🙀 User Agent			
Confirm Installation		SOU	RCE fire
The installer is ready to install User Agent Click "Next" to start the installation.	on your computer.		
	Cancel	< Back	Next >

لماع" تيبثت مت ."Sourcefire مدختسم ليكو" دادعإ جلاعم لامتكا دعب "قالغإ قوف رقنا .8 Windows. ماظن ىلع ةمدخك "Sourcefire مدختسم لماع" أدبي .نآلا "Sourcefire مدختسم

🖶 User Agent			
Installation Complete		SOL	JRCE fire
User Agent has been successfully installe	ed.		
Click "Close" to exit.			
Please use Windows Update to check for any critical updates to the .NET Framework.			
	Cancel	< Back	Close

.Windows ماظن بتكم حطس ىلإ عيرس ليغشت زمر "Sourcefire مدختسم لماع" فيضي .9



Sourcefire مدختسم لماع تيبثت ةلازإ

:ةيلاتان اتاوطخلا يدحإ مدختسأ ،"Sourcefire 2.x مدختسم لماع" تيبثت ةلازإل

- رتخاو ،تازيملاو جماربلا < جماربلا < مكحتلا ةحول ىل لقتنا. تيبثتلا ةلازا قوف رقناو ،ةمئاقلا نم (مدختسملا ليكو).
- رزب رقناو ،"Sourcefire مدختسم لماع" دادعإ فلم هيف دجوي يذلا عقوملا ىل لقتنا تيبثتلا ةلازإ ددحو ،نميألا سواملا.



Sourcefire_U	
er_Agent_2.0	
0-34_Setup	

Iı	nst	tall

Repair

Uninstall

Troubleshoot compatibility

Open with...

Share with

Sourcefire

Restore previous versions

Send to

Cut

Copy

Create shortcut

Delete

Rename

Properties

ىلإ جاتحت دق) رماوأ هجوم حتفا ،(CLI) رماوألا رطس ةهجاو لالخ نم تيبثتلا ةلازإل • اذه لخدأو ،msi. فلم دجوي ثيح عقوملا ىلإ لئالدلا رييغتب مقو ،(لوؤسمك هليغشت

:رمألا

msiexec /x Sourcefire_User_Agent_2.0.0-34_Setup.msi

ثيدحت دنع اذه ءانبلا مقر ريغتي .34 وه ءانبلا مقر ،قباسلا لاثملا يف :ةظحالم رمألا لاخدإ لبق ءانبلا مقر نم ققحت ."Sourcefire مدختسم لماع"

اهحالصإو تيبثتلا ةلازإ ءاطخأ فاشكتسأ

ضرعلا

- مدختسمل لماع تيبثت ءاغل لشف
- اهتيبثت ةلاز دعب ليغشتلا ديق رهظت تامدخلا لازت ال.

الحل

كنكمي ،"مكحتلا ةحول" يف "تازيملاو جماربلا" نمض "مدختسملا لماع" ضرع متي مل اذإ رمألا اذه لخدأو لوؤسمك رماوأ هجوم حتفا ،ةمدخلا ةلازإل ."مدختسملا ليكو ةمدخ" فذح ةطاسبب:

C:\Users\Administrator>sc query type= service | findstr /spinl "Sourcefire RUA AgentService"

.يعبطم أطخ سيل اذه . ' = ' دعب ةحاسم مدختساً :ريذحت

an Administrator: Command Prompt

C:\Users\Administrator>sc query type= service ! findstr /spinl "Sourcefire RUA A gentService" 12:SERVICE_NAME: AgentService 13:DISPLAY_NAME: Sourcefire RUA Agent 622:SERVICE_NAME: Sourcefire RUA Agent 623:DISPLAY_NAME: Sourcefire RUA Agent C:\Users\Administrator>_______

- 🗆 ×

مكحتلا ةدحو حتفل .تامدخلا ةرادإ مكحت ةدحو يف تاوطخلا هذه لامكإ اضيأ كنكمي:

- أدبا ةمئاقلا ىلإ لقتنا .1.
- . services.msc ليغشتب مق
- 3. مدختسم لماع صئاصخ ضرع Sourcefire.

ةمدخلا فذحل رماوألا هذه لخدأ ،تامدخلا ءامسأ ضرع درجمب:

<#root>

C:\Users\Administrator>

sc delete "Sourcefire RUA Agent"

C:\Users\Administrator>

sc delete "AgentService"



ىلٍا جاتحتو زاەجلا ىلع ةدوجوم FireSIGHT ماظنب ةقلعتم تافلم يأ لظت دق :ةظحالم اەتلازا.

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