فاشكتسال TETRA تافيرعت ثيدحت لشف 3000 أطخ عم امحالصإو ءاطخألا

تايوتحملا

مدومل
<u>قيساسأل اتابلطتمل ا</u>
<u>تابلطتملا</u>
<u>ةمدختسملا تانوكملا</u>
<u>ةلكشملاا</u>
الباجيا
ةل.ص. تاذ تامول.عم

ەمدقملا

.3000 أطخب امحالصإو TETRA تافيرعت ءاطخأ فاشكتسأ تاوطخ دنتسملا اذه فصي

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

Cisco نم ةنمآ ةياەن ةطقن •

ةمدختسملا تانوكملا

ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Cisco نم (رادصإ يأ) ةنمآلا ةياەنلا ةطقن لصوم •
- Wireshark (رادصإ يأ)

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

ةلكشملا

تافيرعت ثيدحت لشف ،ةياهنلا ةطقن يف .1 تيبثت رذعت" أطخلا ةلاسر عم TETRA تافيرعت ثيدحت لشف ،ةياهنلا ةطقن يف .1 القحال يرخأ ةرم ةلواحملا يجري.تاثيدحتلاا.

Settings

General Settings			~
Protection			
Monitor Program Install	C On	?	
Monitor Program Start	(C) 01	?	
Monitor Network Connections	C On	?	
Cloud Detection Engines			
ETHOS	(💷 On	?	
SPERO	Con Con	?	
TETRA Detection Engine			
Enable TETRA Engine	(🚍 On	?	
Allow Definition Updates	0n	?	
Scan Settings			v
Unable to install updates. Please try again later.	Update TETRA Sync Policy	Close	

لشفلا أطخ ةظحالم متي ،Cisco نم ةنمآلا ةيفرطلا ةطقنلا مكحت ةدحو يف .2 روكذملا:

رادج وأ ةكبشلا تادادعإ نم ققحت .ةكبشلا ةلەم ءاەتنا ببسب ثيدحتلا لشف" لصتا .ثيدحتلا مداخو ةياەنلا طاقن نيب لاصتالا نم ققحتلل ليكولا وأ ةيامحلا معدب .

	2022-08-24 18:11:15 IST
Definitions Last Updated	Update failed because of a network timeout.
	Check your network, firewall or proxy settings to
	verify connectivity between endpoints and the
	update server. Contact Cisco support if the issue
	persists.

3. فالع ثودح عم اهثيدحت مت يتلا تافيرعتلا تلشف debug sfc.exe.log يف 3. قثوم وه امك Unknown_Error لثمي يذلاو. #root>

(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdateInterface::update updateDir: C:\Progr (978223515, +0 ms) Aug 04 07:30:23 [11944]: ERROR: TETRAUpdateInterface::update

Update failed with error -3000

(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26, (978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle (978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit bUpdate: 0, bReload: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: FASharedPtr<class TETRAUpdateInterface>::Release
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: bUpdated = FALSE, state: 20,
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: sig count: 0, version: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: Config::IsUploadEventEnabled: returns 1, 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
```

لحلا

< AMP جەن يف TETRA تافيرعت رايخ ثيدحتب مدختسملل حامسلا نيكمت ءاجرلا .1 ليغشت كنكمي ،ةملعملا ەذە مادختساب .مكحتلا ةدحو ىلع ليمعلا مدختسم ةەجاو .اەحالصإو ءاطخألا فاشكتسأ ءانثأ بولطم وە امك TETRA ثيدحت

Modes and Engines	Z Start Client User Interface 0
Restantes :	Cloud Notifications ()
8 exclusion sets	Engine Notifications
Praxy	Hide Exclusions O
	Allow user to update TETRA definitions 0
Outbreak Control	
Device Control	
Product Updates	
Advanced Settings	
Administrative Features	
Client User Interface	
File and Process Scan	

- تيكمتب اضيأ مق .2 Debug Connector نيكمتب اضيأ مق .2 مقاهنال المقان على عام المتع عرد عوتسم على المعني المتعاوي المتعافي أمت المتعافي المت متحافي المتعافي المتعافي المتعافي المتعافي المتحافي المتحافي المتحافي المتحافي المتحافي المتحافي المتحافي المتعافي المتحافي المتحافي المتحافي المتحافي المتحافي المتحافي المتحافي المت
- ةحجانلا TETRA ثيدحت ةياهن ةطقن نم لك ىلع مزح طاقتلا طاقتلا ىجري .3 ةطقن ىلع TETRA ثيدحت قوف رقنلا ءانثأ TETRA تافيرعتل ةلشافلاو .ةياهنلا
- 4. مزحلا طاقتلاا ةيفصت يف ،TETRA ثيدحتل ةحجانلاا ةياهنلاا ةطقن ىلع .4 ةمزح لكل "tcp.stream عبتا" مث "ttetra-defs.amp.cisco.com:443 هادختساب .قلصلا تاذ رورملا ةكرح ليلحتل.
- 5. ةمزحلا يف Server Hello، ةرفش لبقي مداخلا ىرت نأ كنكمي Server Hello، قمزحلا يف Server Hello. قمزح يف "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"



- 6. الفشلال الما الما الما الما الما Cisco Secure Endpoint Tetra مداخ لبقي ال
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_AES_128_GCM_SHA256
- يف حداف أطخ رهظي ،مزحلا طاقتلاا يف ،TET<u>RA</u> ثيدحت لشف ةياهن ةطقن يف .7



.Client Hello ةمزح دعب SSL ةحفاصم

- .ةياەنلا ةطقن نم ةضورعملا تارفشلا ةيؤر كنكمي ،Client Hello ةمزح يف .8
- 9. قياەنلا قطقن ىلع ريفشتلا قحص نم ققحتلا كنكمي ،كلذ ىلإ قفاضإلاب مادختساب Get-TlsCipherSuite إمأ | Get-TlsCipherSuite مادختساب

PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

Name

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS ECDHE RSA WITH AES 256 GCM SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS DHE RSA WITH AES 128 GCM SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_NULL_SHA256 TLS_RSA_WITH_NULL_SHA TLS_PSK_WITH_AES_256_GCM_SHA384 TLS_PSK_WITH_AES_128_GCM_SHA256 TLS_PSK_WITH_AES_256_CBC_SHA384 TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_NULL_SHA384 TLS_PSK_WITH_NULL_SHA256

- لشف ببس وه اذهف ،انه 6 ةوطخلا يف ةروكذملا تارفشملا جاردا مدع ةلاح يف .10 ةحفاصم SSL.
- :ةعومجملا جەن يف SSL ريفشت ةعومجم بيترت نم ققحتلا ءاجرلا ،كلذ حالصإل

Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templ



،نكمم ىلع ەنييعت مت اذإو ،ەليطعت وأ ريفشتلا ةعومجم رمأ نيوكت متي الأ بجي .12 ةمئاقلا يف 6 ةوطخلا يف قروكذملا ةرفشلا ةفاضإب مقف.

💭 SSL Cipher Suite C	Order		– o ×
🛃 SSL Cipher Suite C	Order		Previous Setting Next Setting
 Not Configured Enabled Disabled 	Comment: Supported on:	At least Window	ws Vista
Options:			Help:
SSL Cipher Suites TLS_AES_256_GCM_SH	HA384,TLS_AES_1;	8	This policy setting determines the cipher suites used by the Secure Socket Layer (SSL). If you enable this policy setting, SSL cipher suites are prioritized in the order specified. If you disable or do not configure this policy setting, default cipher suite order is used. Link for all the cipherSuites: http://go.microsoft.com/fwlink/? LinkId= 517265
			OK Cancel Apply

- تارييغتلا ەذە بلچل ةياەنلا ةطقن ليغشت دعأو تارييغتلا ەذە قيبطتب مق .13 تاقيبطتلل ةرفوتملا.
- .ليغشتلا ةداعإ ةيلمع لامتكا درجمب TETRA ثيدحت ةلواحم ةداعإ ءاجرلا.

تاريطقتلاو تالجسلا ليلحت ىجري ،TETRA تافيرعت ةلكشم رارمتسإ ةلاح يف .15 ىرخأ ةرم.

ةلص تاذ تامولعم

• <u>Cisco نم تاليزنتلاو ينفلا معدلا</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