

TLS: أطلخ؛ "نمآل لوصول اءاطخأ فاشكك تسأ
268435703:SSL

routines:openssl_internal:wrong_version_number";

تايوت حمل ا

[ءمدقم ل ا](#)

[ءلكش ل ا](#)

[ل حل ا](#)

[ءف فاضل ل ل ص ا ف ت](#)

[ءلص ت ا ذ ت ا م و ل ع م](#)

ءمدقم ل ا

TLS: 268435703:SSL أطلخ: "نمآل لوصول اءاطخ ل حل ءق رط دن ت س ل ا اذ ه ف ص ي
routines:openssl_internal:wrong_version_number".

ءلكش ل ا

ل ل دن ت س ل ا Zero Trust Access م ا ذ ت س ا ب ص ا خ دروم ح ت ف م ذ خ ت س ل ا ل و ا ح ي ا م ذ ن ع
https://<app-
name>.ztna.sse.cisco.io) ل ا ث م ل ا ل ل ب س ي ل ع) دروم ل ل م ا ع ل ا URL م ا ذ خ ت س ا ب ، ض ر ع ت س ل ا
أطلخ ل ا ء ط ا ل م م ت ي و ض ر ع ت س ل ا ي ف ق ي ب ط ت ل ل ل م ح ت م ت ي ا ل ،

ق ي ب ط ت ل ل ل ل ل و ص و ل ا ر ذ ع ت ي

ل و و س ل ا ب ل ا ص ت ا ل ا ء ا ج ر ل ا

ن ي ي ع ت ء د ا ع ا ب ب س . س و و ر ل ل ل ب ق ن ي ي ع ت ل ا ء د ا ع ا ل ل ا ص ت ا ل ا ع ط ق و ا م ذ ا خ ل ل ا ص ت ا ي ف ا ط خ
TLS: 268435703:SSL أطلخ: ل ل ق ن ل ل ل ش ف ب ب س ، ل ل ا ص ت ا ل ل ش ف
:openssl_internal:wrong_version_number ت ا ه ج و م ل ا

Cisco Secure Access



Application is unreachable

Please contact your administrator

upstream connect error or disconnect/reset before headers. reset reason: connection failure, transport failure reason: TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER

نم آ ليمع أطخ

لحل

دراوم لا مسق يف ةياهنلا ةطقن لاصتا بولسأ نمض بسانم لوكوتورب نيوكت نم دكأت
ةصاخلا:

- HTTP ديدحت بجيف ، طقف HTTP ربع ارفوتم صاخلا قيبطتلا ناك اذا
- HTTPS ديدحت بجيف ، طقف HTTPS ربع ارفوتم صاخلا قيبطتلا ناك اذا
- اقلطم أطخلا اذه ةيؤر مدع بجيف ، HTTPS وأ HTTP ربع ارفوتم صاخلا قيبطتلا ناك اذا

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

+ FQDN or IP Address

Browser-based connection

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not

Public URL for this resource ⓘ

https://

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

ةصاخلا دراوملا نيوكت

ةيفاضا ليصافت

ددحملا لوكوتوربلا مادختساب صاخلا دروملاب لاصتا عاشنإ نمآلا لوصولا ليكوكرحم لواحي تامولعمل ةحول يف

ئطاخلا نيوكتلا ببسب) صاخلا قيبطتلا عم HTTPS ةانق عاشنإ نم ليكولا نكمتي مل اذا دنع ضرعتسملا يف OpenSSL بةقلعتمل ةاطخالا ةدهاشم كنكم يف، (نبنجال نم يألعل ضرعتسملا يلا دننتملا لاصتال ربع ةصاخلا دراوملا يلا لوصول ةلواحم

ةلص تاذا تامولعم

- [Secure Access مدختسم ليلد](#)
- [Cisco Systems - تادنتسملا وينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا