

ديربال بي وري دمل TLSv1.3 نيوكت نمآل اينورتكلال

تايوتحمل

مدمقمل

لوكوتورب نيوكت دنتسمل اذه فصوي
Cisco Secure Email and Web Manager
(EWM) ل TLS v1.3

سياسال تابلطتم

بولطم هنيوكت و SEWM تاداعاب عماع ةفرعم.

مدمختسمال تانوكمل

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 تارادصلال او
- SSL نيوكت تاداعاب

صاخ ةي لمعم ةئيبي في ةدوجومال ةزهجال نم دنتسمل اذه في ةدراول تامولعمل اعاشن امت
تتاك اذ. (يضا رتفا) حوسمم نيوكت ب دنتسمل اذه في مدمختسمل ةزهجال عيمج تادب
رمأ يال لمتمحمل ري ثاتلل كمهف نم دكأتف، ةرشابم كتكباش

عماع ةرظن

ةهجو او HTTPS ةلصلال تاذ تامدخلل تالاصتال ري فشتل TLS v1.3 لوكوتورب جمدمب SEWM ماق
REST API، و NGUI، ةيكي السالكل مدمختسمل

يسست امنبي عرسا تاضوافم وانام رثكأ لاصتال ةينك ماب TLS v1.3 لوكوتورب زي متيو
راي عمل هلعل ةدهاج ةعانصلال

ضعب عم SSL ب صاخال SEGWebUI or CLI لخاد ةدوجومال SSL نيوكت ةقيرط SEWM مدمختسي
اهزاربال ةزبابال تاداعبال

- اهب حوسمل تالوكوتوربال نيوكت دنع ةئيبي وحوئاصن
- TLS v1.3 تارفش ةجلعم نكمي ال
- طقف HTTPS GUI ل TLS v1.3 نيوكت نكمي
- طمن TLS v1.0 و TLS v1.3 ني ب TLS لوكوتوربال راي تخالال ةناخ ديحت تاراخي مدمختست
ةلاقمل لخاد لي صافاتلل نم ديزمب حضورم

نيوكتال

AsycOS 15.5 نمض HTTPS ل TLS v1.3 لوكوتورب SEWM جمدا

HTTPS لشف عنمل لوكوتوربال تادادع| رايتخ| دنع رذحلاب ىصوي

طبض تايلمع بلطتت تائيبلا ضعب نأ نم مغرلاب عئاش TLS v1.3 ل بيولا ضرعتسم معد SEWM لى لوصولل

وأ هريغت نكمي ال يضارتفا ريفشت 3 TLS v1.3 لوكوتوربل Cisco SEWM ذيفنت معدي SEWM لخد هداعبتس|

TLS 1.3 ريفشت

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUI نم نيوكتال

SSL نيوكت > ماطنلا ةرادا > لى لقتنا

- AsyncOS 15.5 HTTPS لى لى يضارتفال TLS لوكوتورب دي دحت روشنم ةيقرت نمضتت طقف TLS v1.1 و TLS v1.2
- TLS، ثيدحتل تامدخو ةنمأل LDAP تامدخ امهو، ناتجرمدل ناتيفاضال ناتمدخل معدت ال v1.3.

SSL Configuration

| SSL Configuration | |
|--|---|
| Appliance Management Web User Interface: | Enable protocol versions: TLS v1.2 TLS v1.1 |
| Secure LDAP Services: | Enable protocol versions: TLS v1.2 TLS v1.1 |
| Updater Service: | Enable protocol versions: TLS v1.2 TLS v1.1 |
| Peer Certificate FQDN Validation: | Used for Alert Over TLS, Updater and LDAP: Disabled |
| Peer Certificate X509 Validation: | Used for Alert Over TLS, Updater and LDAP: Disabled |

[Edit Settings](#)

ن. نيوكتال تاراخي مي دقتل "تادادع| رايتخ" دح

TLS v1.0 و TLS v1.1 و TLS v1.2، "بيو مدختسم ةهجاو" ل TLS لوكوتورب دي دحت تاراخي نمضتت و TLS v1.3.

- دي دحت متيو، AsyncOS 15.5 تالوكوتورب لى لى رشنلا ةدام ةيقرت دي دحت متيو. يضارتفا لكش ب TLS v1.1 و TLS v1.2 تالوكوتورب

| SSL Configuration | |
|--|--|
| <p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p> <p>For the peer certificate FQDN validation for LDAP, ensure that you enable LDAP server certificate validation in LDAP Global Settings.</p> | |
| Appliance Management Web User Interface: | <p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions:</p> <p><input type="checkbox"/> TLS v1.3 ←</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p> |
| Secure LDAP Services: | <p>Secure LDAP services include Authentication and External Authentication.</p> <p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p> |
| Updater Service: | <p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p> |
| Peer Certificate FQDN Validation: | <p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p> |
| Peer Certificate X509 Validation: | <p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p> |

Cancel Submit

✎ إذا ارفوتم TLS v1.0 لازي ال. يضارتفا لكش ب لطعم يلاتلابو لمهم TLS1.0: عظام الم
هن كمت كلالم راتخ.

- عحاتم ال تالوكوتورب ال ضرعت جالزم تاذ تاعبرم مادختساب رايتخالالا عناخ تاراخي ئضت
ةق اوتم ال ريغ تاراخي لل ةجراخ تامال ع تاذ تاعبرم و
- ببول مادختسم هةجاول رايتخالالا عناخ تاراخي ةروصل ال يف ةنيعل تاراخي حضوت

| | | | |
|--|--|--|-----------------------------------|
| <input type="checkbox"/> TLS v1.3 | <input type="checkbox"/> TLS v1.3 | <input type="checkbox"/> TLS v1.3 | <input type="checkbox"/> TLS v1.3 |
| <input checked="" type="checkbox"/> TLS v1.2 | <input checked="" type="checkbox"/> TLS v1.2 | <input type="checkbox"/> TLS v1.2 | <input type="checkbox"/> TLS v1.2 |
| <input checked="" type="checkbox"/> TLS v1.1 | <input type="checkbox"/> TLS v1.1 | <input checked="" type="checkbox"/> TLS v1.1 | <input type="checkbox"/> TLS v1.1 |
| <input type="checkbox"/> TLS v1.0 | <input type="checkbox"/> TLS v1.0 | <input type="checkbox"/> TLS v1.0 | <input type="checkbox"/> TLS v1.0 |
| <input checked="" type="checkbox"/> TLS v1.3 | <input type="checkbox"/> TLS v1.3 | <input checked="" type="checkbox"/> TLS v1.3 | <input type="checkbox"/> TLS v1.3 |
| <input checked="" type="checkbox"/> TLS v1.2 | <input type="checkbox"/> TLS v1.2 | <input type="checkbox"/> TLS v1.2 | <input type="checkbox"/> TLS v1.2 |
| <input checked="" type="checkbox"/> TLS v1.1 | <input type="checkbox"/> TLS v1.1 | <input type="checkbox"/> TLS v1.1 | <input type="checkbox"/> TLS v1.1 |
| <input type="checkbox"/> TLS v1.0 | <input checked="" type="checkbox"/> TLS v1.0 | <input type="checkbox"/> TLS v1.0 | <input type="checkbox"/> TLS v1.0 |

✎ ليغشت ةداعا يف SSL نيوكت يلع اهوارج متي يتل تاليدعتل ببستت دق: عظام الم
WebUI ةمدخل ةريصق ةعطاقم يف ببستت. ةلصل تاذ تامدخل

SSL Configuration

Attention — ⚠ Your settings have been saved. After you commit your changes, the settings of the SSL Configuration can cause all related services to restart. This leads to interruption in the services.

| SSL Configuration | |
|--|---|
| Appliance Management Web User Interface: | Enable protocol versions: TLS v1.3 ← |
| Secure LDAP Services: | Enable protocol versions: TLS v1.2 TLS v1.1 |
| Updater Service: | Enable protocol versions: TLS v1.2 TLS v1.1 |
| Peer Certificate FQDN Validation: | Used for Alert Over TLS, Updater and LDAP: Disabled |
| Peer Certificate X509 Validation: | Used for Alert Over TLS, Updater and LDAP: Disabled |

[Edit Settings](#)

CLI من نيوكتا

WebUI: ةدخاو ةمدخ ىل ع TLS v1.3 ب EWM حمسي

```
sma1.example.com> sslconfig
```

نيمأت لصفأ ىل ع لوصحلل SSLv3 لىطعت ب ىصوي.

ةيللاتم ةدحمل TLS تارادصا نوكت نأ بلطتت ةديعبلا مداوخل ىل ع SSL/TLS ةمدخ نأ طحال لصتم فلم ديدحتب امئاد مق ،لاصتالا ءاطخأ بنجتل كرت عم ،1.2 و 1.0 TLS نيكمتب مقت ال ،لاثملا لىبس ىل ع .ةمدخ لك تارادصا نىم ةعومحم لاطعم TLS 1.1.

اهذيفنت ديرت يتلا ةيلمعل رتخأ:

- اهلىطعت وأ SSL/TLS تارادصا نيكمت - تارادصا

- peer_cert_fqdn - فوات نم ققحتلا - FQDN عم ريظنلا ةداهش ققحتلا - LDAP.

- PEER_CERT_X509 - فوات نم ققحتلا - X509 ل ريظنلا ةداهش ققحتلا - LDAP.

تارادصا []>

تامدخلل SSL/TLS رادصا لىطعت وأ نيكمت:

ثيدحت ةمدخ - ثدحم

زهجالا ةرادال بىو مدختسم ةهجاو - WebUI

(ةيجراخلا ةقداصملاو ةقداصملا لكذيف امب) ةنمألا LDAP تامدخ - LDAPs

TLSv1.3 عم طقف WebUI نيوكت نكمي ،LDAPs و Updater ل رفوتم ريغ TLSv1.3 نأ طحال

(لطمع : N ،نكمم : Y): ةمدخلال بسح ايلاح ةنكمملا SSL/TLS تارادصا

UpdateUI LDAPs

TLSv1.0 N N
TLSv1.1 Y N Y
TLSv1.2 Y Y
TLSv1.3 ق بطن ي ال a/ال

اهل SSL/TLS تارادصل ل ليطعت/ن ي كمت متيس يتل ا ةمدخلال دح:

1. ثدحم
 2. WebUI
 - 3- اومن نادلبال لقا
 - 4 - تامدخال عيجم
- []> 2

TLSv1.2 يه WebUI ل ايلاح ةنك ممل (تالوكوتوربل) لوكوتوربل

هاندا تارايلخال دح ا دح، ددحم لوكوتوربل دادعال ريغتل

1. TLSv1.0
 2. TLSv1.1
 3. TLSv1.2
 4. TLSv1.3
- []> 4

Y [N]> اهن ي كمت ديرت له. ايلاح لطمم ةزهجال ا ةرادال بيو مدختسم ةهجال اول TLSv1.3 م عد

TLSv1.2 و TLSv1.3 يه WebUI ل ايلاح ةنك ممل تالوكوتوربل

اهذي فننت ديرت يتل ا ةلمعال رتخ ا:

- اهل ي طعت او SSL/TLS تارادصل ن ي كمت - تارادصل ال
 - و ثدحمل او TLS ربع ه ي بننت لل FQDN عم ريظنل ا ةداهش قفاوت نم ققحت ال - peer_cert_fqdn - LDAP.
 - و ثدحمل او TLS ربع ه ي بننت لل X509 ل ريظنل ا ةداهش قفاوت نم ققحت ال - PEER_CERT_X509 - LDAP.
- []>

مازل ال SMA1.example.com>

ي ف SSL نيوكت ي ف تاريغتل ببستت: ريذحت
Commit - gui.euq_webui. دعب تاي لمعال هذه ليغشت ةداعل متتس
SMA. تاي لمعال ةريصق ةعطاقم ال ك لذي دوي

ك تاريغتل فصت يتل ا تاقيلعتلل ضعبل لخال ا اجرل:

[]> TLS v1.3 ني كمت

اهب مازتل الال مت يتل ا تاريغتل: Sun Jan 28 23:55:40 2024 EST

...موسرلا مدختسملا ةهجاو ليغشت ةداع
موسرلا مدختسملا ةهجاو ليغشت ةداع
EUQ_WEBUI... ليغشت ةداع نآل متي
euq_webui ليغشت ةداع تمت

WebUI لوصول ةيناكم نم دكأت واري صق اتقورظتنا

✎ ةمدخ ديدحت مدختسملا نم ام ةمدخل TLS نم ةددعت تارادصا ديدحت بلطتي :ةظحالم
عيمج ليدعت متي يتح رخأ ةرم لوكوتوربو ةمدخ ديدحت راركث مت ،لوكوتورب رادصا و
تادادعإل.

ةحصلال نم ققحتل

مدع ببسب رهظت يتللا ءاطخأل او ةيساسأل رابتخال تاهوي رانيس ضعب مسقلا اذه نمضتي
ةلمجل ءانب ءاطخأ و تارادصإل قباطت.

NGUI و EWM WebUI لىل بيو ضرعتسم ةسلج حتف لالخ نم ضرعتسملا ةفيظو نم ققحت
TLSv1.3 مادختساب هنوكت مت يذلا

TLS v1.3 لوبقل لعفلاب اه رابتخاب انمق يتللا بيول تاضرعتسم عيمج نيوكت مت

- ءاطخأ هن عجتني TLS v1.3 معد لي طعتل Firefox لىل ضرعتسملا دادعإ نييعت جذومن
زاهجلاب صاخأل NGUI و ClassicUI نم لك لىل
- TLS v1.3 داعبتسال هنوكت مت Firefox مادختساب ةيكي سالك (UI) مدختسم ةهجاو
رابتخال
- (يضارتفال) 4431 ذفنملا مقرر وه ديحول ءانثتسال عم هسفن أطخال NGUI لىل قلتتس
URL ناو نع لخاد

Secure Connection Failed

An error occurred during a connection to dh6219-sma1.iphmx.com. Peer reports incompatible or unsupported protocol version.

Error code: SSL_ERROR_PROTOCOL_VERSION_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

[Learn more...](#)

It looks like your network security settings might be causing this. Do you want the default settings to be restored?

- هذه TLSv1.3 نيمضت نم دكأتلل ضرعتسملا تادادع| نم ققحت ،لاصتالا نامضل (Firefox نم ةنيعلال)

| | | |
|-------------------------------------|---|---|
| security.tls.version.fallback-limit | 4 |  |
| security.tls.version.max | 4 |  |
| security.tls.version.min | 1 |  |

- لشف :جارخ| أطخلا اذه يطييس ةرفشم ريغ ريفشت ةميقي مادختساب openssl رمأ جذومن
"-ciphersuites TLS_AES_256_GCM_SHA386" :رمألا عم أطخ :حلأص ريغ ريفشت ببسب ةنيعلال OpenSSL لاصتالا رابتخ|

226823168:Error:1426E089:SSL routines:ciphersuite_cb:no cipher match:ssl/ssl_ciph.c:1299:

- أطخلا اذه TLS v1.3 ليطعت دنع NG-ui لىل جذومن ءاشن| رمأ جتنى

curl: (35) curl_sslversion_max ريغ curl_sslversion عم قفاوتم

ةلص تاذا تاملول عم

- [رادصاللا تاظحال م - Cisco نم يوتحمللا نامأ قرادا زاغ](#)
- [يئاهنللا مدختسملا ةلدا - Cisco نم يوتحمللا نامأ قرادا زاغ](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انء عي مچ ي ف ني مدخت سمل معد و ت م مي دقت لة يرش بل او
امك ة قيق د نوك ت نل ةلأل ةمچرت لصف أن ةظحال م يچري . ةصاغل مة تغل بل
Cisco ي لخت . فرت م مچرت م اهدقي ي تلل ةي فارتحال ةمچرتل عم لاعل او
ىل إلمءاد عوچرلاب ي صؤت و تاملرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل