تشفير الجيل التالي CUCM 11.0 - تشفير المنحنى البيضاوي

المحتويات

المقدمة

يصف هذا المستند تكوين تشفير الجيل التالي (NGE) من Cisco Unified Communications Manager (CUCM) 11.0 وما بعده لتلبية متطلبات الأمان والأداء المحسنة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أساسيات أمان Cisco CallManager
- إدارة شهادات Cisco CallManager

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco CUCM 11.0، حيث تكون شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA) مدعومة فقط لـ CallManager (CallManager-ECDSA).

ملاحظة: يدعم CUCM 11.5 والإصدارات اللاحقة شهادات TOMCAT-ECDSA أيضا.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

يمكن أيضا إستخدام هذا المستند مع منتجات البرامج والإصدارات التي تدعم شهادات ECDSA:

- Cisco Unified CM IM and Presence 11.5
- Cisco Unity Connection 11.5

معلومات أساسية

تشفير المنحنى الاهليلجي (ECC) هو طريقة للتشفير بالمفتاح العام بناء على البنية الجبرية للمنحنيات البيضاوية عبر الحقول المحدودة. يعتبر مستوى الأمان نفسه الذي توفره المفاتيح ذات الحجم الأصغر أحد الفوائد الرئيسية مقارنة بتشفير غير ECC.

توفر المعايير الشائعة (CC) ضمانا بأن ميزات الأمان تعمل بشكل صحيح داخل الحل الذي يتم تقييمه. ويتحقق ذلك من خلال إختبار وتلبية الاحتياجات الواسعة من الوثائق.

وهو مقبول ومدعوم من قبل 26 بلدا في جميع أنحاء العالم عن طريق ترتيب الاعتراف بالمعايير المشتركة.

يدعم Cisco Unified Communications Manager، الإصدار 11.0 شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA).

هذه الشهادات أقوى من الشهادات المستندة إلى RSA وهي مطلوبة للمنتجات التي تحتوي على شهادات CC. يتطلب برنامج الحلول التجارية للأنظمة المصنفة (CSfC) التابع لحكومة الولايات المتحدة اعتماد cc، وبالتالي، يتم تضمينه في الإصدار 11.0 من Cisco Unified Communications Manager والإصدارات الأحدث.

تتوفر شهادات ECDSA مع شهادات RSA الموجودة في هذه المناطق:

- إدارة الشهادات
- وظيفة وكيل جهة منح الشهادة (CAPF)
- تعقب أمان طبقة النقل (TLS)
- إتصالات بروتوكول بدء جلسة عمل الأمان (SIP)
- مدير دمج الاتصال الهاتفي بجهاز الكمبيوتر (CTI)
- HTTP
- إنترنت

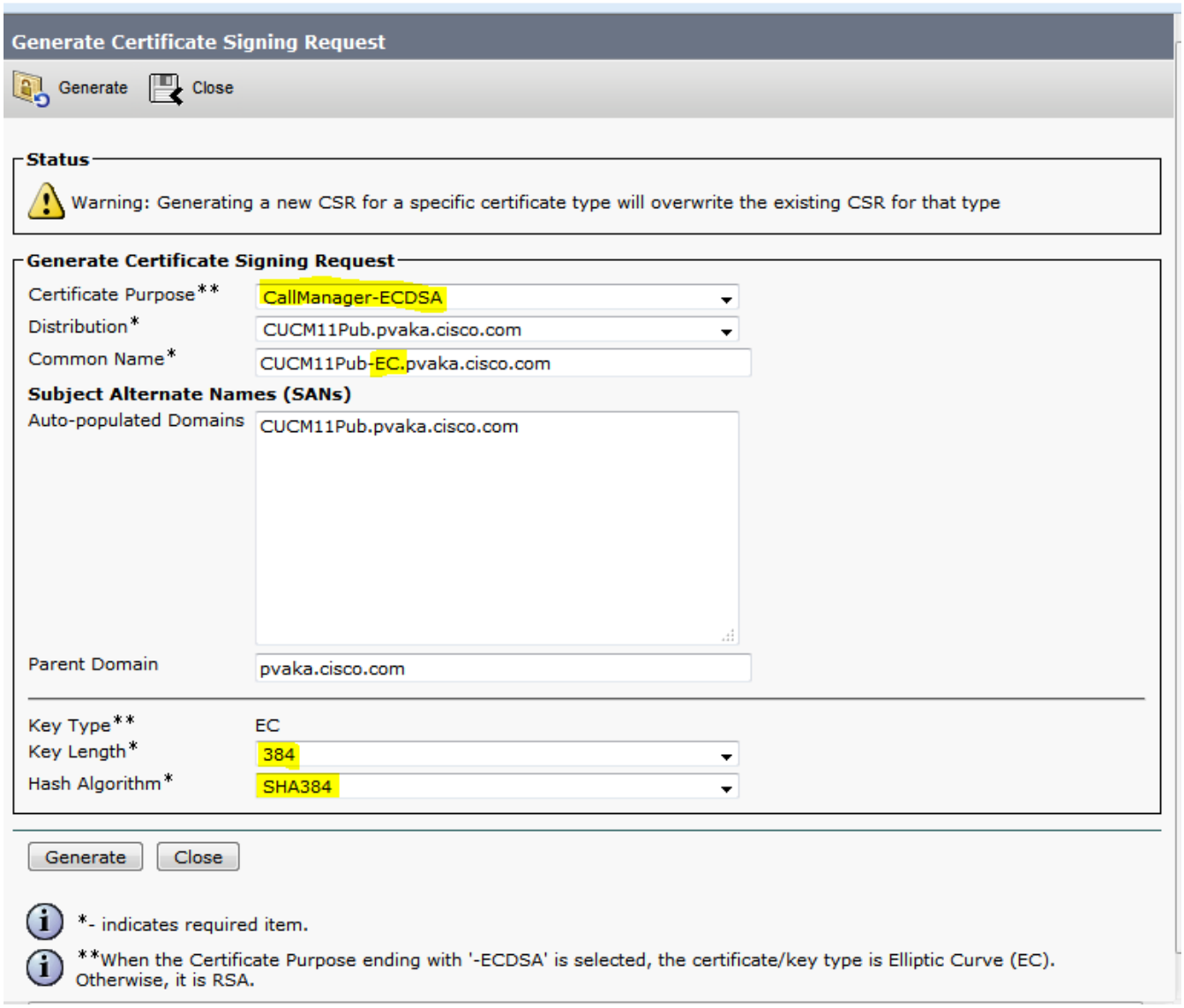
وتوفر الأقسام التالية معلومات أكثر تفصيلا عن كل من هذه المجالات السبعة.

إدارة الشهادات

إنشاء شهادات باستخدام تشفير المنحنى البيضاوي

دعم نظام تصحيح الأخطاء (ECC) من CUCM 11. 0 والإصدارات الأحدث لإنشاء شهادة CallManager بتشفير المنحنى البيضاوي (EC):

- يتوفر الخيار الجديد **CallManager-ECDSA** كما هو موضح في الصورة.
- يتطلب أن ينتهي جزء المضيف من الاسم الشائع في **-EC**. وهذا يمنع أن يكون له نفس الاسم الشائع مثل شهادة **CallManager**.
- في حالة ترخيص شبكة منطقة التخزين (SAN) متعددة الخوادم، يجب أن ينتهي ذلك ب **-EC-ms**.



- يحدد كل من طلب الشهادة الموقع ذاتيا وطلب CSR خيارات خوارزمية التجزئة استنادا إلى حجم مفتاح EC.
- بالنسبة لحجم مفتاح EC 256، يمكن أن تكون خوارزمية التجزئة SHA256 أو SHA384 أو SHA512. بالنسبة لحجم مفتاح EC 384، يمكن أن تكون خوارزمية التجزئة SHA384 أو SHA512. بالنسبة لحجم مفتاح EC 521، يكون الخيار الوحيد هو SHA512.
- الحجم الافتراضي للمفتاح هو 384 وخوارزمية التجزئة الافتراضية هي SHA384، والتي يمكن تغييرها. تستند الخيارات المتاحة إلى حجم المفتاح المختار.

تكوين واجهة سطر الأوامر (CLI)

تمت إضافة وحدة شهادة جديدة باسم **CallManager-ECDSA** لأوامر CLI

- set cert regen [unit] - إعادة إنشاء شهادة موقعة ذاتيا

```
admin:set cert regen ?
Syntax:
set cert regen [name]
name mandatory unit name

admin:set cert regen CallManager-ECDSA

WARNING: This operation will overwrite any CA signed certificate previously imported for  CallManager-
ECDSA
Proceed with regeneration (yes|no)?
```

- set cert import own|trust [unit] - إستيراد الشهادة الموقعة من المرجع المصدق

```
admin:set cert import trust CallManager-ECDSA
Paste the Certificate and Hit Enter
```

- set csr gen [unit] - إنشاء طلب توقيع الشهادة (CSR) **للوحدة** المحددة

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - عندما يكون TFTP وه اسم الوحدة، يتم تضمين شهادات CallManager RSA في العمليات المجمعة. تلقائيا مع شهادات CallManager-ECDSA

ملفات CTL و ITL

- يوجد **CallManager-ECDSA** في كل من ملفات قائمة الشهادات الموثوق بها (CTL) وملفات Identify Trust List (ITL).
- تشتمل شهادة CallManager-ECDSA على وظيفة CCM+TFTP في كل من ملف ITL وملف CTL.
- يمكنك إستخدام **show ctl** أو **show itl** أمر لعرض هذه المعلومات كما هو موضح في هذه الصورة:

```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      61:E4:7E:DA:01:65:E4:68:22:9E:2E:CC:EB:35:18:DD
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     951     3B D9 E1 B0 68 56 5F ED 73 FF 75 B7 36 3B D1 29 9E 93 36 FD (SHA1 Hash HEX)

        ITL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1071
2       DNSNAME         26      CUCM11Pub.pvaka.cisco.com
3       SUBJECTNAME     68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      60:28:0E:23:2C:DC:72:7D:16:B2:16:B1:40:90:20:7E
7       PUBLICKEY       97
8       SIGNATURE       104
9       CERTIFICATE     661     21 C4 B8 E9 71 B0 4C 90 C2 F9 93 30 E0 53 3D 1D DE 86 32 07 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

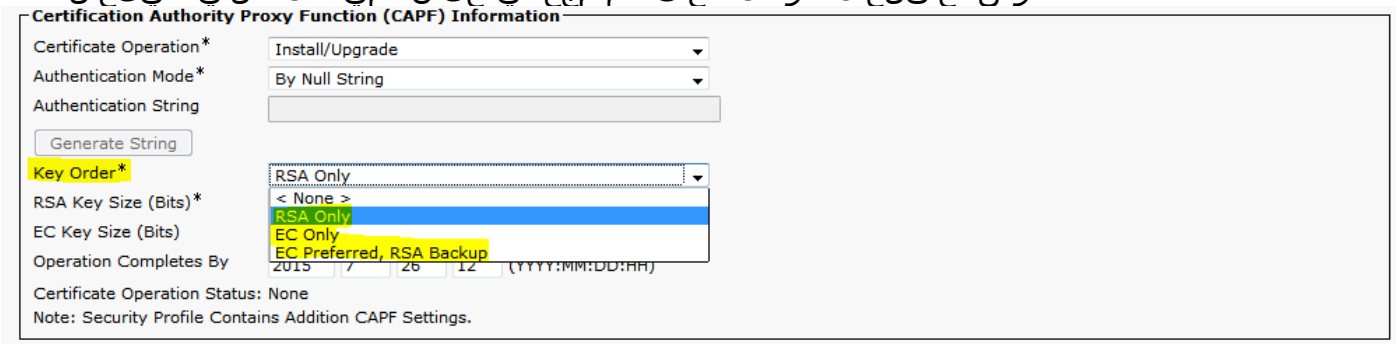
- يمكنك إستخدام الأمر **utils ctl update** لإنشاء ملف CTL.

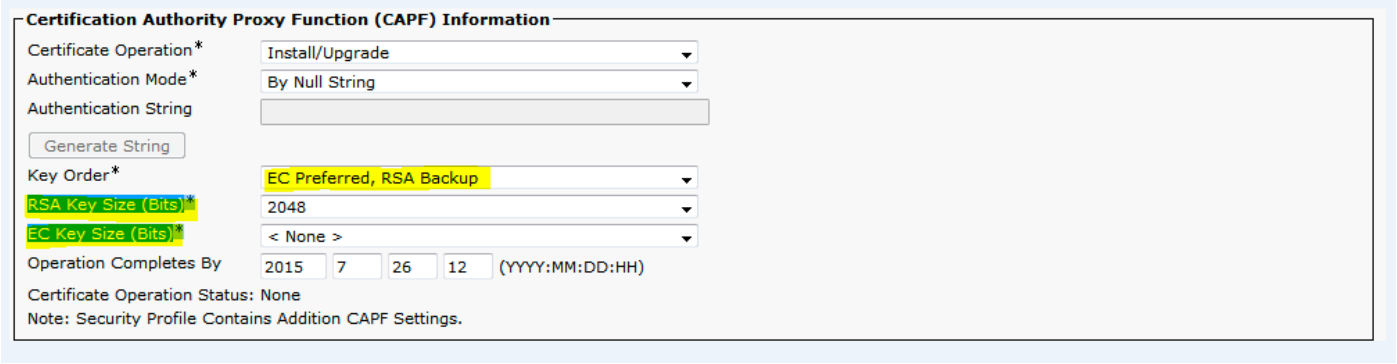
وظيفة وكيل جهة التخليص

- يوفر الإصدار 3.0 من وظيفة وكيل المرجع المصدق (CAPF) في CUCM 11 الدعم لأجهزة

مفاتيح EC مع RSA.

- تعتبر خيارات CAPF الإضافية المقدمة بالإضافة إلى حقول CAPF الموجودة هي ترتيب المفاتح وحجم مفتاح EC (وحدات بت).
- تم تغيير خيار حجم المفتاح (BITS) الحالي إلى حجم مفتاح RSA (BITS).
- يوفر أمر المفاتيح الدعم لخيارات النسخ الاحتياطي ل RSA فقط و EC فقط والمفضل ل EC، و RSA.
- يوفر حجم مفتاح EC الدعم لأحجام المفاتيح التي تبلغ 256 و 384 و 521 بت.
- يوفر حجم مفتاح RSA الدعم ل 512 و 1024 و 2048 بت.
- عند تحديد ترتيب المفاتح RSA فقط، يمكن تحديد حجم مفتاح RSA فقط. عندما يكون EC محدد فقط، يمكن تحديد حجم مفتاح EC فقط. عند تفضيل EC، يتم تحديد النسخ الاحتياطي ل RSA، يمكن تحديد حجم مفتاح RSA و EC على حد سواء.

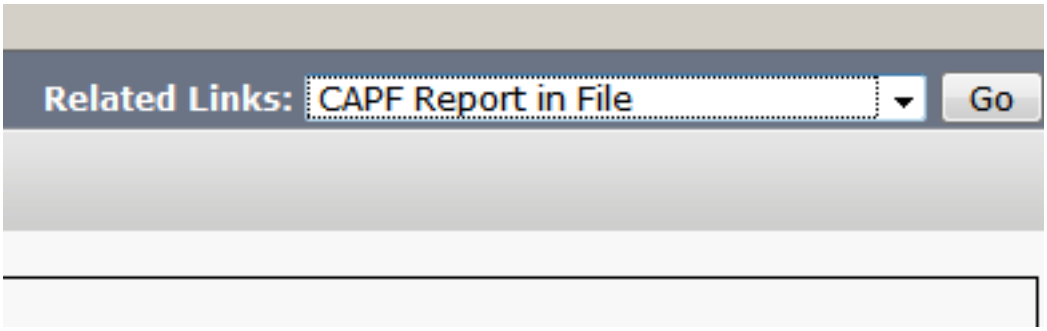




ملاحظة: لا تدعم نقطة نهاية Cisco الإصدار 3 من CAPF حاليا، لذلك لا تحدد خيار EC فقط. ومع ذلك، يمكن للمسؤولين الذين يرغبون في دعم الشهادات الهامة محليا (LSCs) ل ECDSA لاحقا تكوين أجهزتهم باستخدام خيار النسخ الاحتياطي ل RSA المفضل ل EC. عندما تبدأ نقاط النهاية في دعم CAPF الإصدار 3 لوقوائم التحكم في الوصول (LSCs) إلى ECDSA، يحتاج المسؤولون إلى إعادة تثبيت قائمة التحكم في الوصول (LSC) الخاصة بهم.

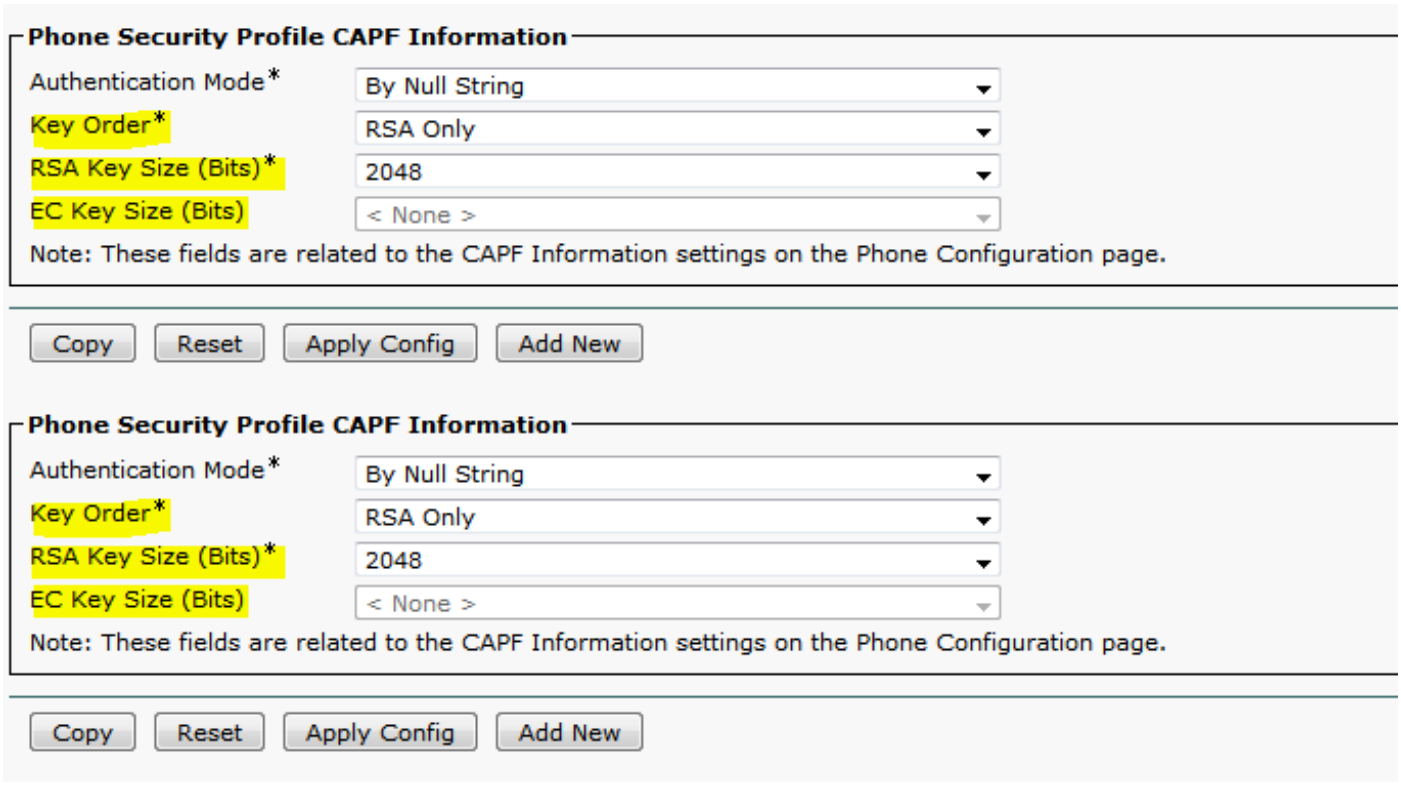
تظهر خيارات CAPF الإضافية الخاصة بالهاتف وملف تعريف أمان الهاتف والمستخدم النهائي وصفحات مستخدم التطبيق هنا:

جهاز > هاتف > روابط ذات صلة

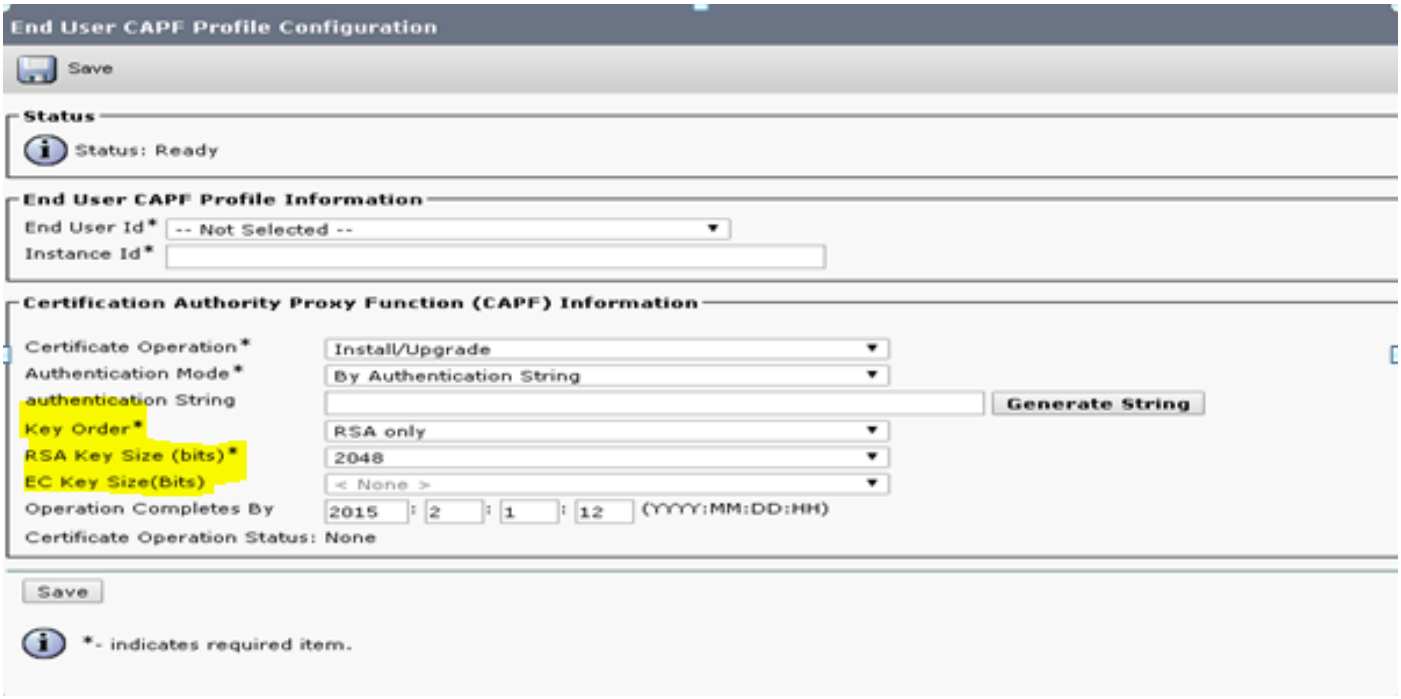


انتقل إلى النظام > التأمين > ملف تعريف تأمين الهاتف

إدارة المستخدم > إعدادات المستخدم > توصيف مستخدم التطبيق CAPF

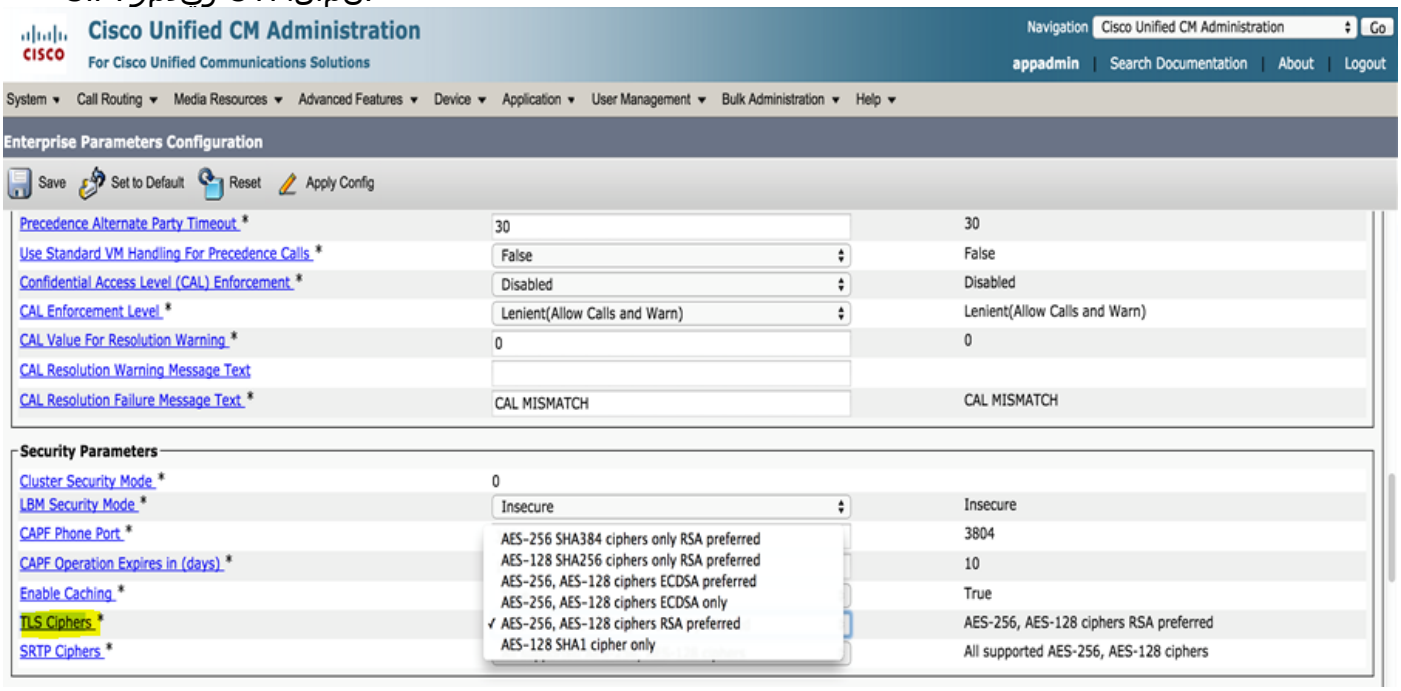


انتقل إلى إدارة المستخدم > إعدادات المستخدم > ملف تعريف CAPF للمستخدم النهائي.



معلمات TLS Ciphers Enterprise

- تم تحديث شفرات TLS لمعلمات المؤسسة لدعم شفرات ECDSA.
- تقوم شفرات TLS لمعلمات المؤسسة الآن بتعيين شفرة TLS لخط SIP، وخطوط اتصال SIP، ومدير CTI الآمن.



دعم SIP ECDSA

- يتضمن Cisco Unified Communications Manager، الإصدار 11.0 دعم ECDSA لخطوط SIP ووواجهات خط اتصال SIP.
- يعد الاتصال بين Cisco Unified Communications Manager وجهاز نقطة نهاية الهاتف أو الفيديو اتصال خط SIP بينما يكون الاتصال بين إثنين من مديري الاتصالات الموحدة من Cisco اتصال خط اتصال SIP.

- تدعم جميع إتصالات SIP تشفير ECDSA وتستخدم شهادات ECDSA.

تم تحديث واجهة SIP الآمنة لدعم الشفرين التاليين:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

هذه هي السيناريوهات التي يقوم فيها بروتوكول SIP بإجراء إتصالات TLS:

- عند عمل SIP كخادم TLS عندما تعمل واجهة خط اتصال SIP لإدارة الاتصالات الموحدة من Cisco كخادم TLS لاتصال SIP الآمن الوارد، تحدد واجهة خط اتصال SIP ما إذا كانت شهادة CallManager-ECDSA موجودة على القرص. إذا كانت الشهادة موجودة على القرص، فإن واجهة خط اتصال SIP تستخدم شهادة CallManager-ECDSA إذا كانت مجموعة التشفير المحددةTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 وأ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- عندما يعمل SIP كعميل TLS عندما تعمل واجهة خط اتصال SIP كعميل TLS، تقوم واجهة خط اتصال SIP بإرسال قائمة من مجموعات التشفير المطلوبة إلى الخادم استنادا إلى حقل شفرات TLS (والذي يتضمن أيضا خيار شفرات ECDSA) في معلمات **CUCM** للمؤسسة و**مجموعات التشفير** عميل TLS و**شفرة TLS**. يحدد هذا التكوين قائمة مجموعة تشفير المدعومة حسب الأفضلية.

ملاحظات:
- يجب أن تحتوي الأجهزة التي تستخدم تشفير ECDSA لإجراء اتصال ب CUCM على شهادة CallManager-ECDSA في ملف قائمة تأمين الهوية (ITL) الخاص بها.
- تدعم واجهة خط اتصال SIP مجموعات تشفير RSA TLS للاتصالات من العملاء الذين لا يدعمون مجموعات تشفير ECDSA وأ عندما يتم إنشاء اتصال TLS باستخدام إصدار أقدم من CUCM، والتي لا تدعم ECDSA.

دعم CTI Manager ECDSA الآمن

تم تحديث واجهة CTI Manager الآمنة لدعم هذه الشفرات الأربعة:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

تقوم واجهة CTI Manager الآمنة بتحميل كل من شهادة CallManager وشهادة CallManager-ECDSA. وهذا يسمح لواجهة CTI Manager الآمنة بدعم التشفير الجديد مع تشفير RSA الحالي.

في Cisco Unified Communications Manager، يتم إستخدام خيار شفرة TLS لمعلمات المؤسسة لتكوين شفرة TLS التي يتم دعمها على الواجهة الآمنة لمدير CTI. وهو الحال مع واجهة SIP.

دعم HTTPS لتنزيل التكوين

- 11.0 الإصدار من بدءا، يتم تحسين تنزيل التكوين الآمن (على سبيل المثال، عملاء Jabber) لدعم HTTPS بالإضافة إلى واجهات HTTP و TFTP التي تم إستخدامها في الإصدارات السابقة.
- يستخدم كل من العميل والخادم المصادقة المتبادلة إذا لزم الأمر. ومع ذلك، يلزم على

العملاء المسجلين في قوائم التحكم في الوصول للمنفذ (LSCs) لبروتوكول ECDSA وتكوينات TFTP المشفرة لتقديم قوائم التحكم في الوصول للمنفذ (LSC) الخاصة بهم.
- تستخدم واجهة HTTPS كل من شهادات CallManager و CallManager-ECDSA كشهادات الخادم.

ملاحظات:
- عند تحديث شهادات CallManager أو CallManager ECDSA أو Tomcat، يجب إلغاء تنشيط خدمة TFTP وإعادة تنشيطها.
- يتم إستخدام المنفذ 6971 لمصادقة شهادات CallManager و CallManager-ECDSA، المستخدمة بواسطة الهواتف.
- يتم إستخدام المنفذ 6972 لمصادقة شهادات Tomcat، المستخدمة من قبل Jabber.

إنتروبي

الانتروبي هي قياس لعشوائية البيانات وتساعد في تحديد الحد الأدنى لمتطلبات المعايير المشتركة. للحصول على تشفير قوي، يلزم وجود مصدر قوي للأنتروبي. إذا كانت خوارزمية التشفير القوية، مثل ECDSA، تستخدم مصدرا ضعيفا للانتروبي، يمكن كسر التشفير بسهولة.

في Cisco Unified Communications Manager، الإصدار 11.0، يتم تحسين مصدر الانتروبي ل Cisco Unified Communications Manager.

برنامج Entropy Monitoring Daemon هو ميزة مدمجة لا تتطلب التهيئة. ومع ذلك، يمكنك إيقاف تشغيله من خلال واجهة سطر الأوامر (CLI) الخاصة بمدير الاتصالات الموحدة من Cisco.

استعملت هذا CLI أمر in order to ضبط الإنتروبي monitore برنامج خفي خدمة:

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the Entropy Monitoring Daemon service.
utils service stop Entropy Monitoring Daemon	Stops the Entropy Monitoring Daemon service.
utils service active Entropy Monitoring Daemon	Activates the Entropy Monitoring Daemon service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the Entropy Monitoring Daemon service, which further unloads the kernel module.

معلومات ذات صلة

- دليل الأمان ل Cisco Unified Communications Manager، الإصدار 11.5(1)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).