تأثير جدار الحماية الآمن لتغييرات EKU وي مايو لمصادقة عميل CA العامة التي تبدأ في 2026 لتأمين الاتصالات

المقدمة

يصف هذا المستند تأثير القيود المفروضة على معايير إصدار الشهادات التي تفرضها السلطات المصدقة التي تمتثل لبرنامج شهادة جذر كروم، وخاصة ما يتعلق منها بمنتجات جدار الحماية الآمن من Cisco.

معلومات أساسية

يتم إصدار شهادات TLS الموثوقة بشكل عام بواسطة CAs التي يجب أن تتوافق مع سياسات الصناعة التي تحكم إصدار الشهادات واستخدامها.

تحدد سياسة برنامج Chrome Root، التي تديرها شركة Google، المتطلبات التي يجب على CAs التقيد بها حتى يتم الوثوق بشهاداتهم من خلال متصفح Google Chrome. تؤثر هذه المتطلبات على كيفية إصدار الشهادات الموثوقة بشكل عام في الصناعة. وكجزء من الممارسات الأمنية المتطورة، يقدم برنامج Chrome Root إرشادات أكثر صرامة بشأن إستخدام الشهادات.

ولهذا فإن العديد من الشهادات المصدقة العامة تنتقل من إصدار الشهادات التي تتضمن EKU لمصادقة العميل وتتحول إلى إصدار الشهادات المخصصة لمصادقة الخادم فقط. ونتيجة لذلك، يتوقع أن تتضمن الشهادات التي تم إصدارها حديثا من العديد من CAs مصادقة الخادم EKU فقط.

إستخدام المفاتح الموسع (EKU)، وهو امتداد شهادة يحدد الوظيفة المقصودة لمفتاح عام داخل شهادة رقمية. وهو يؤسس مجموعة مهيكلة من التطبيقات المسموح بها، مما يضمن إستخدام المفاتح فقط لعمليات تشفير معينة. تتحكم في هذه الوظيفة معرفات الكائنات (OIDs)—معرفات رقمية فريدة تصنف كل إستخدام مسموح به، مثل توقيع الرمز، ومصادقة الخادم، ومصادقة العميل، أو البريد الإلكتروني الآمن.

عندما تكون المصادقة مستندة إلى شهادة، يقوم الكيان الذي يتحقق من الصحة بمراجعة التحقق لتحديد معرف الكائن (OID) داخل EKU. من خلال تضمين ملحق EKU، يقوم مرجع مصدق (CA) بتقييد نطاق الشهادة بالأدوار المحددة مسبقا، مع تعيين كل غرض محدد بشكل صريح إلى OID.

الغرض من سمات EKU

· تحديد الاستخدام: توضح سمات EKU أنواع المصادقة وأ التشفير المسموح بها لتنفيذ الشهادة.

· تحسين الأمان: ومن خلال تقييد الشهادات على إستخدامات معينة، تساعد EKU في منع إساءة إستخدامها أو عدم إستخدامها في التطبيقات غير المقصودة (على سبيل المثال، لا يمكن إستخدام شهادة الخادم لمصادقة العميل).

· التوافق: يضمن إستخدام الشهادات بما يتوافق مع سياسات الأمان والمعايير الصناعية.

الاستخدامات الرئيسية لسمات EKU

1. مصادقة عميل ويب TLS

· يسمح باستخدام الشهادات لتعريف ومصادقة المستخدمين أو الأجهزة على الخادم.

· معرف المستخدم: 1.3.6.1.5.5.7.3.2

· مستخدم في شبكات VPN و TLS المتبادلة وسيناريوهات تسجيل الدخول الآمنة.

2. مصادقة خادم ويب TLS

· يسمح باستخدام الشهادات من قبل الخوادم لإثبات هويتها للعملاء.

· معرف المستخدم: 1.3.6.1.5.5.7.3.1

· مستخدم في خوادم الويب HTTPS و SSL/TLS ونقاط النهاية الآمنة لواجهة برمجة التطبيقات (API).

3 - توقيع الرمز

· يشير إلى أنه يمكن إستخدام الشهادة لتوقيع البرامج أو الملفات التنفيذية.

· معرف المستخدم: 1.3.6.1.5.5.7.3.3

· تستخدم في عمليات التحقق من توزيع البرامج وسلامتها.

4. حماية البريد الإلكتروني

· تمكين الشهادات التي يمكن إستخدامها لتوقيع رسائل البريد الإلكتروني وتشفيرها.

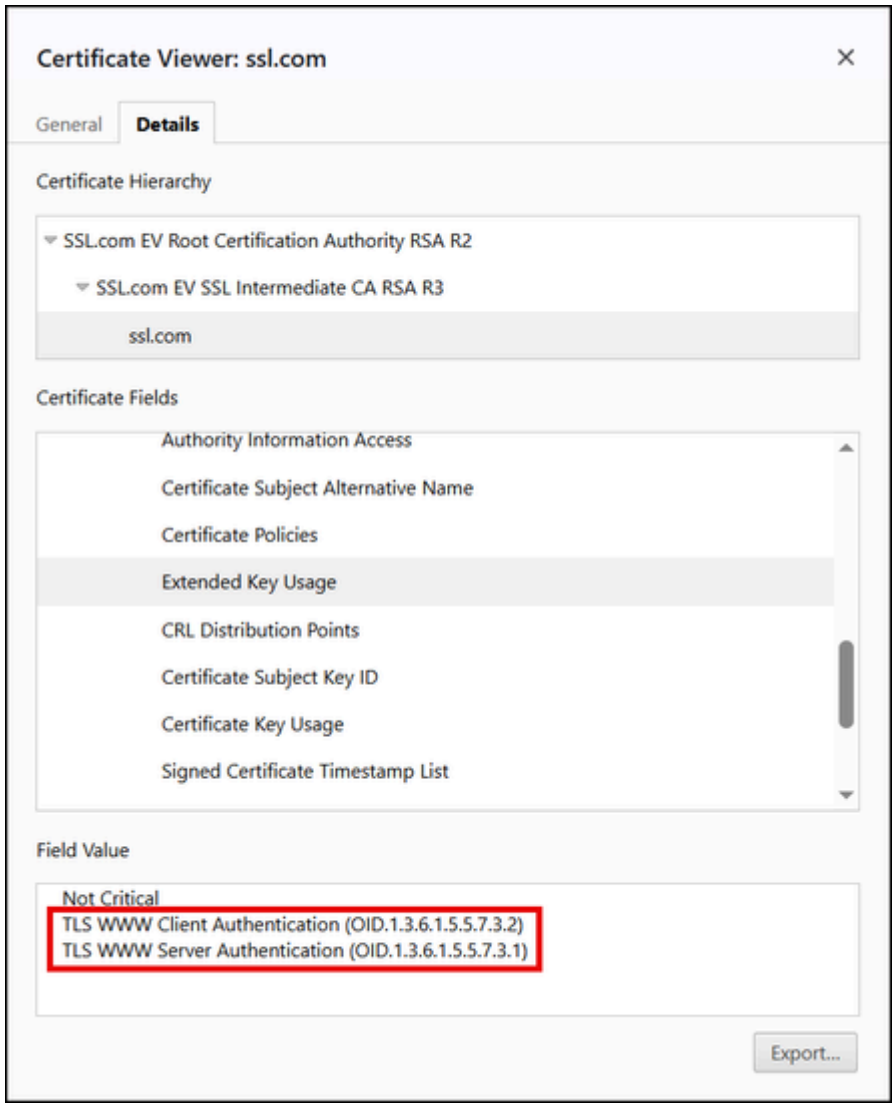
· معرف المستخدم: 1.3.6.1.5.5.7.3.4

· مستخدم في أمان البريد الإلكتروني ل S/MIME.

5 - أغراض أخرى

· توقيع المستند وختم الوقت وتسجيل الدخول إلى البطاقة الذكية وما إلى ذلك، كل منها بمعرف فريد خاص به.

لا تحتاج المستعرضات والخوادم إلى إلى وجود EKU للخادم المصادقة لإنشاء اتصال آمن ل HTTPS ولكن تاريخياً، تضمنت العديد من شهادات خادم TLS كل من serverAuth وclientAuth EKUs، أدناه مثال لهذه الشهادة:



لماذا تتم إزالة EKU لمصادقة العميل من محطات الخادم؟

- الأمان والنطاق:من المفترض أن تصادق شهادات TLS العامة على الخوادم على الويب فقط. توفر عملية الإزالة فصلا واضحا بين ظائف الخادم والعميل. يتم إستخدام EKU ل ClientAuth لمصادقة الأجهزة والمستخدمين مع TLS المتبادل (mTLS) وسيناريوهات المصادقة الأخرى.

- منع التكوين غير الصحيح: قد تثق بعض الأنظمة في أي شهادة من مرجع مصدق عام لمصادقة العميل إذا كانت وحدة الاحتفاظ بالمخزون (EKU) موجودة، مما قد يشكل خطرا على الأمان.

- متطلبات المستعرض: لا تتطلب المستعرضات الرئيسية أو تحقق من EKU الخاص بالعميل في شهادة موقع ويب.

- بنية PKI المبسطة: من خلال فصل الاستخدامات، يمكن ل CAs الاحتفاظ بتدرجات هرمية متميزة للشهادات لمقامات TLS مقابل أغراض أخرى.

وهذا مهم بشكل خاص لمنتجات مثل جهاز الأمان القابل للتكيف لجدار الحماية الآمن (ASA) من Cisco، والدفاع عن تهديد جدار الحماية الآمن (FTD) من Cisco، ومدير جهاز جدار الحماية الآمن (FDM) من Cisco، ومركز إدارة جدار الحماية الآمن (FMC) من Cisco الذي يمكن أن يعمل إما كخادم أو عميل أثناء مصادقة TLS، وفقا لحالة الاستخدام.

التأثير على بيئات الخوادم

بالنسبة للغالبية العظمى لعمليات نشر الخوادم، سيكون هذا التغيير منخفض التأثير أو غير مؤثر. إليك ما يجب توقعه:

- خوادم الويب القياسية (HTTPS):بدون تأثير. ستستمر الشهادات المحدثة في العمل بشكل طبيعي.

- الشهادات الموجودة: ستستمر أي شهادة صادرة قبل القطع في العمل حتى انتهاء صلاحيتها.

- سيناريوهات TLS (mTLS) وسيناريوهات شهادة العميل: إذا كنت تستخدم شهادة خادم TLS لمصادقة العميل، فستحتاج إلى الحصول على شهادة منفصلة باستخدام وحدة EKU ل ClientAuth من مصدر آخر.

- أنظمة المؤسسات التي تحتاج إلى كل من وحدة المعالجة المركزية (EKU): من المتوقع توفر كل من وحدة المعالجة المركزية (EKU) لبعض الأنظمة القديمة أو الخاصة بالمؤسسات. يجب التحقق مما إذا كانت هناك حاجة إلى التحديثات للتوافق مع القواعد الجديدة.

وصف المشكلة

بدءا من مايو 2026، ستتوقف العديد من هيئات الشهادات العامة (CAs) عن إصدار شهادات أمان طبقة النقل (TLS) التي تتضمن إستخدام مفتاح مصادقة العميل (EKU) الموسع. تشتمل الشهادات التي تم إصدارها حديثا عادة

.طقف EKU لمصادقة الخادم على

ونتيجة لذلك، إذا تم تجديد الشهادات التي تم إصدارها من مرجع مصدق عام بموجب سياسات CA المحدثة ثم تم نشرها في منتجات جدار الحماية الآمن من Cisco، فسوف تفشل الخدمات التي تكون فيها مصادقة العميل EKU مطلوبة. وفيما يلي الخدمات المحددة التي تأثرت بها:

- عندما يعمل ASA أو FTD أو FDM أو FMC كعميل - على سبيل المثال، عند التوصيل بموزدي الهوية أو خوادم المصادقة مثل ISE (pxGrid) أو RADIUS أو LDAPs أو المصادقة المستندة إلى الدليل النشط - قد يفشل إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وهي تفتقد EKU لمصادقة العميل. في هذه السيناريوهات، إذا رفض خادم المصادقة الشهادات بدون EKU المطلوب، فقد يحدث فشل في الاتصال.

- يمكن لعميل Cisco الآمن (المعروف سابقا باسم AnyConnect) المصادقة على خوادم ASA أو FTD باستخدام الشهادات. ومع ذلك، إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وكانت تفتقد إلى EKU لمصادقة العميل، فسيفشل اتصال VPN (RAVPN) للوصول عن بعد.

- عندما يقوم FTD أو ASA بإنشاء نفق VPN من موقع إلى موقع — سواء إلى FTD آخر أو ASA أو موجه Cisco أو نظير VPN خارجي باستخدام مصادقة الشهادة (RSA أو ECDSA)، يفشل النفق إذا كانت شهادة الهوية التي تم إنشاؤها بواسطة CA عام تفتقد سمة EKU لمصادقة العميل. يحدث هذا لأن نظير VPN البعيد يتطلب وجود وحدة مصادقة العميل EKU في شهادة الهوية.

تغيير سياسة برنامج جذر الكروم

ويتوقف تنفيذ EKU على توقيع المرجع المصدق على الشهادة. كان إستخدام كل من مصادقة الخادم ومصادقة العميل EKU ممارسة شائعة. ومع ذلك، وكجزء من CAs لتغيير نهج برنامج Chrome الجذر المطابق لمعايير إصدار الشهادة هذه، توقف التوقيع على شهادات TLS التي تتضمن إستخدام المفتاح الموسع لمصادقة العميل (EKU). تتضمن الشهادات الصادرة حديثا مصادقة الخادم EKU فقط.

المتطلبات الرئيسية للسياسات

- يجب أن تؤكد مراجع CA العامة إستخدام المفتاح الموسع (EKU) فقط لمصادقة الخادم (id-KP-serverAuth)

- يجب أن تتضمن الشهادات EKU لمصادقة الخادم فقط.

- يحظر تضمين EKU لمصادقة العميل في هذه الشهادات

- تتم إزالة CAs الجذر التي تستمر في إصدار الشهادات باستخدام EKU لمصادقة العميل في نهاية المطاف بواسطة "غير موثوق بها" من مخزن جذر Chrome مما يتسبب في وضع عالمة على مثل هذه الشهادات على أنها Chrome مستعرض

التسلسل الزمني

- سبتمبر 2025، SSL.com سيصدر شهادات TLS التي تتضمن فقط EKU ServerAuth (وليس ClientAuth) للشهادات الخادم. وبمعنى آخر، سيتم إستخدام الشهادات SSL/TLS الجديدة لموقع على الويب أو الخادم فقط "مصادقة الخادم" بشكل صريح.
- تشرين الأول/أكتوبر 2025: بدأت الجهات المختصة المكيفة التابعة للبرنامج (مثل DigiCert و Sectigo وما إلى ذلك) في إصدار شهادات الخادم فقط بشكل افتراضي.
- مايو 2026: توقف المراجع المصدقة المتوافقة مع البرنامج عن إصدار شهادات EKU لمصادقة العميل
- مارس 2027: سياسة برنامج كروم روت تصبح فعالة تماما

التأثير على منتجات جدار الحماية الآمن من Cisco

بعد أن يبدأ المرجع المصدق العام بتضمين مصادقة الخادم EKU فقط في الشهادات الصادرة. قد يكون لهذا التأثير التالي على سيناريوهات منتجات Cisco Secure Firewall:

- عندما يعمل ASA أو FTD أو FDM أو FMC كعميل - على سبيل المثال، عند التوصيل بموزع الهوية أو خوادم المصادقة مثل ISE (pxGrid) أو RADIUS أو LDAPs أو المصادقة المستندة إلى الدليل النشط - قد يفشل إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وهي تفتقد EKU لمصادقة العميل. في هذه السيناريوهات، إذا رفض خادم المصادقة الشهادات بدون EKU المطلوب، فقد يحدث فشل في الاتصال.
- يمكن لعميل Cisco الآمن (المعروف سابقا باسم AnyConnect) المصادقة على خوادم ASA أو FTD باستخدام شهادات. ومع ذلك، إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وكانت تفتقد إلى EKU لمصادقة العميل، فسيفشل اتصال VPN (RAVPN) للوصول عن بعد.
- عندما يقوم FTD أو ASA بإنشاء نفق VPN من موقع إلى موقع — سواء إلى FTD آخر أو ASA أو موجه Cisco أو ظير VPN خارجي باستخدام مصادقة الشهادة (RSA أو ECDSA)، في حالة إذا كانت شهادة الهوية التي تم إنشاؤها بواسطة CA عام تفتقد سمة EKU لمصادقة العميل. يحدث هذا لأن ظير VPN البعيد يتطلب وجود وحدة مصادقة العميل EKU في شهادة الهوية.

ملاحظة: إذا كنت تقوم بدمج FMC أو FDM مع ISE من خلال PXgrid وتفتقر الشهادات المثبتة على FMC/FDM إلى سمة EKU لمصادقة العميل، فعليك مراجعة الحلول المقترحة في هذا المستند ومرجعيات ISE التالية: FN74392 و[إعداد محرك خدمات الهوية لدعم إستخدام المفاتيح الموسعة في الشهادات التي تصدرها السلطات المصدقة العامة].

ملاحظة: يعد إزالة شهادة خادم ClientAuth EKU من TLS بمثابة تغيير في السياسة على مستوى الصناعة

من شأنه تعزيز الأمان ومنع إساءة الاستخدام. لن يكون هناك تأثير ملحوظ لمعظم المستخدمين. ومع ذلك، إذا كنت تعتمد على وحدة المعالجة المركزية (EKU) الخاصة بالعميل، فيجب عليك إتخاذ خطوات إستباقية للحصول على النوع الصحيح من الشهادات لاحتياجاتك.

المنتجات المتأثرة

منتج جدار الحماية الآمن من Cisco	إصدار البرامج	السيناريوهات المتأثرة	علاجات
نظام Firepower Threat Defense (FTD)	جميع الإصدارات	عند العمل كعميل - على سبيل المثال، عند التوصيل بمزودي الهوية أو خوادم المصادقة مثل ISE (pxGrid) أو RADIUS أو LDAPs أو المصادقة المستندة إلى شهادة Active Directory - قد يفشل إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وكانت تفتقد EKU لمصادقة العميل. في هذا السيناريو، إذا رفض خادم المصادقة الشهادات بدون EKU المطلوب، فقد يحدث فشل في الاتصال.	الخيار 1. إذا كنت تستخدم شهادة خادم TLS لمصادقة العميل، ستحتاج إلى الحصول على شهادة باستخدام EKU الخاص ب ClientAuth من مصدر آخر. أو الخيار 2. قم بالتبديل إلى المرجع المصدق الجذر العام (مراجع الشهادات) التي توفر شهادات EKU (ClientAuth و ServerAuth) المجمعة. ملاحظة: يرجى الرجوع إلى قسم الحلول البديلة في هذا المستند للحصول على خيارات إضافية.
FDM	جميع الإصدارات		
FMC	جميع الإصدارات		
ASA	جميع الإصدارات		
عميل Cisco الآمن (المعروف سابقا باسم AnyConnect)	جميع الإصدارات	يمكن لعميل Cisco الآمن المصادقة على خوادم ASA أو FTD باستخدام الشهادات. ومع ذلك، إذا تم إنشاء شهادة العميل بواسطة مرجع مصدق عام وكانت	

	تفتقد إلى EKU لمصادقة العميل، فسيفشل اتصال VPN للوصول عن بعد (RAVPN).		
	عندما يقوم FTD أو ASA بإنشاء نفق VPN من موقع إلى موقع — سواء إلى FTD آخر أو ASA أو موجه Cisco أو نظير VPN خارجي باستخدام مصادقة الشهادة (RSA أو ECDSA)، يفشل نفق VPN إذا كانت شهادة الهوية التي تم إنشاؤها بواسطة CA عام تفتقد سمة EKU لمصادقة العميل. يحدث هذا لأن النظير VPN البعيد يتطلب وجود وحدة مصادقة العميل EKU في شهادة الهوية.	جميع الإصدارات	FTD أو ASA

ملاحظة: إذا كنت تقوم بدمج FMC أو FDM مع ISE من خلال PXgrid وتفتقر الشهادات المثبتة على FMC/FDM لديك إلى سمة EKU لمصادقة العميل، فعليك مراجعة الحلول المقترحة في هذه المستند ومرجعيات ISE التالية: FN74392 و[إعداد محرك خدمات الهوية لدعم استخدام المفاتيح الموسعة في الشهادات التي تصدرها السلطات المصدقة العامة].

ملاحظة: يعد إزالة شهادة خادم ClientAuth EKU من TLS بمثابة تغيير في السياسة على مستوى الصناعة من شأنه تعزيز الأمان ومنع إساءة الاستخدام. لن يكون هناك تأثير ملحوظ لمعظم المستخدمين. ومع ذلك، إذا كنت تعتمد على وحدة المعالجة المركزية (EKU) الخاصة بالعميل، فيجب عليك اتخاذ خطوات استباقية للحصول على النوع الصحيح من الشهادات لاحتياجاتك.

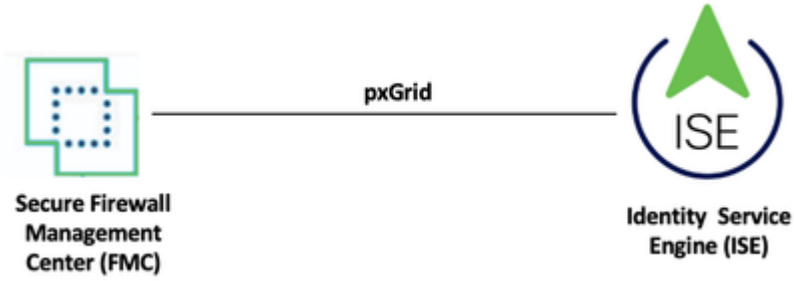
تحذير: وبالنسبة لبيئات الإنتاج، يوصى بشدة بأن يستخدم العملاء الشهادات ذات سمات EKU المناسبة. وتضمن هذه الممارسة الأمن والتوافق والالتزام بالمعايير وأفضل الممارسات في هذا المجال.

⚠ ينبغي إعتبار الشهادات التي لا تتضمن سمات EKU مجرد حل بديل مؤقت، وفقط مع فهم واضح للمخاطر المرتبطة بها.

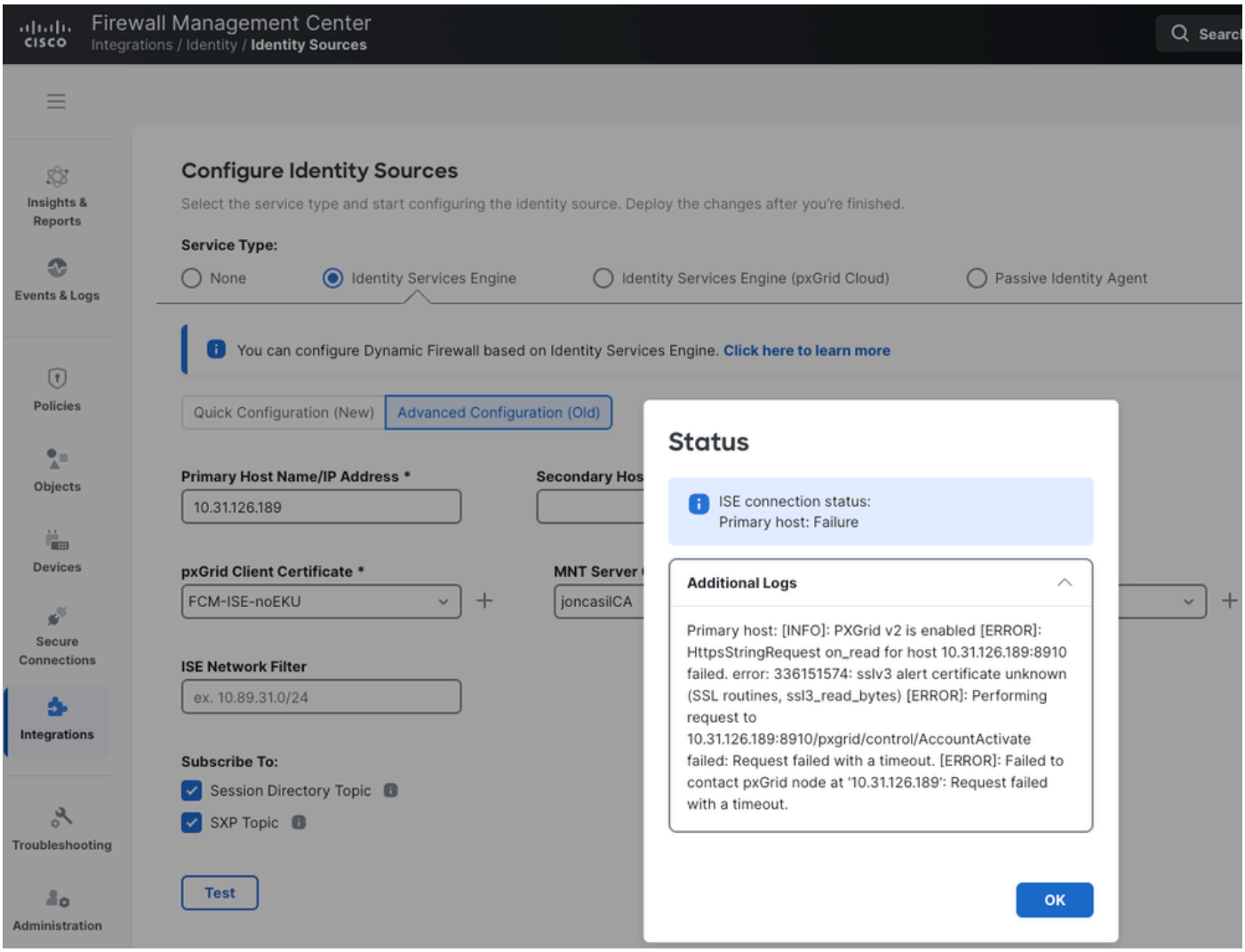
مشكلة 1. مشكلة تكامل PxGrid بين FMC و ISE، عندما تفتقر شهادة FMC إلى سمة EKU لمصادقة العميل

في هذا السيناريو، تفتقد الشهادة التي تستخدمها وحدة التحكم في إدارة اللوحة الأساسية (FMC) لتكامل PxGrid مع ISE إلى سمة EKU لمصادقة العميل. وتتيجة لذلك، يفشل تكامل PxGrid لأن خادم ISE يتوقع أن تكون هذه السمة موجودة في الشهادة المقدمة من قبل FMC.

المخطط



أخطاء واجهة مستخدم FMC: هذه هي رسالة الخطأ المعروضة في FMC، عندما تفتقد الشهادة المستخدمة من قبل FMC إلى سمة EKU لمصادقة العميل لتكامل pxGrid مع ISE.



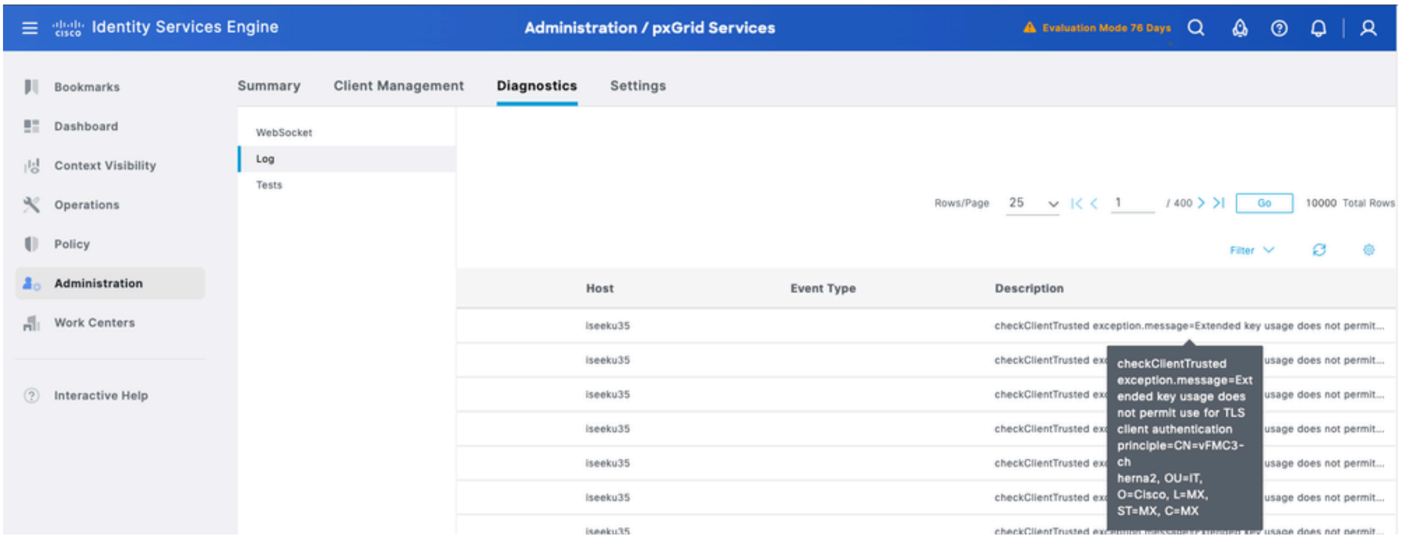
أخطاء واجهة سطر الأوامر (CLI) لوحدة التحكم FMC: تم العثور على نفس رسائل الخطأ في دليل FMC /var/log/messages.

```
<#root>

        HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

                                                sslv3 alert certificate unknown


                                                (SSL routines, ssl3_read_bytes)

                    Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService
```

```
[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.
```

```
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [II
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [II
```

خطأ ISE: هذه هي رسالة الخطأ المعروضة في ISE، CheckClientTrusted exception.message=Extended key لا يسمح بإستخدام مبدأ مصادقة عميل TLS=cn=vFMC3-chherna2، OU=IT، o=Cisco، L=MX، ST=MX، C=MX".



الحل: إذا كنت تقوم بدمج FMC أو FDM مع ISE من خلال PxGrid وتفتقر الشهادة المثبتة في FMC/FDM لديك إلى سمة EKU لمصادقة العميل، فراجع بعد ذلك المقترح في هذا المستند وراجع ISE التالية: [FN74392](#) و[Prepare Identity Services Engine (محرك خدمات الهوية) لقيود إستخدام المفاتيح الموسعة في الشهادات الصادرة من قبل هيئات التصديق العامة](#) لتكامل PXgrid الناجح.

ملاحظة: يجب أن تتضمن شهادة عميل FMC pxGrid سمة EKU ل ClientAuth أو لا تحتوي على سمات EKU للعميل أو الخادم على الإطلاق.

ملاحظة: على الرغم من أن إستخدام الشهادة العامة الموقعة من قبل CA مدعوم من أجل IMS. توصي Cisco باستخدام شهادة ISE الداخلية CA حيث إن هذا الاتصال خاص بالحركات الداخلية فقط.

المشكلة 2. مشكلة تكامل FTD أو ASA مع خادم LDAP، عندما تفتقر الشهادة المقدمة إلى سمة EKU لمصادقة العميل

في هذا السيناريو، يعمل FTD أو ASA كعميل للتكامل مع خادم LDAP باستخدام مصادقة الشهادة. إذا كانت الشهادة المستخدمة من قبل FTD أو ASA تفتقد إلى سمة EKU لمصادقة العميل، يفشل التكامل لأن خادم LDAP

يتطلب أن تكون هذه السمة موجودة في الشهادة.

المخطط

'التحقق من شهادة TLS: خطأ، غرض شهادة غير معتمد و'تتبع TLS: كتابة تنبيه LDAP: أخطاء خادم LDAP: رسالة غير معروفة:شهادة مميت:SSL3'

```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

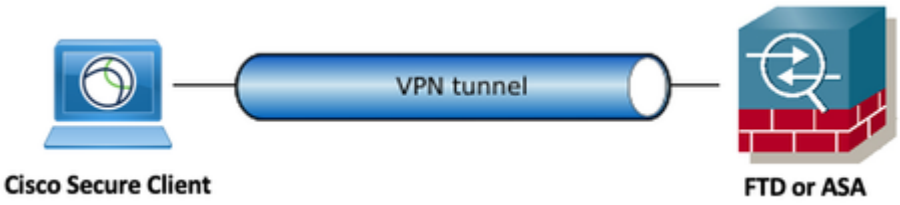
الحل: راجع المقترح في هذا المستند للتأكد من أن FTD أو ASA يستخدم شهادة الهوية الصحيحة مع الشهادة القائمة على الثقة لمصادقة العميل - من أجل مصادقة EKU لمصادقة العميل - بما في ذلك سمة خادم LDAPs.

المشكلة 3. قد يواجه العميل الآمن من Cisco (المعروف سابقا باسم AnyConnect) مشاكل في الاتصال ب FTD أو

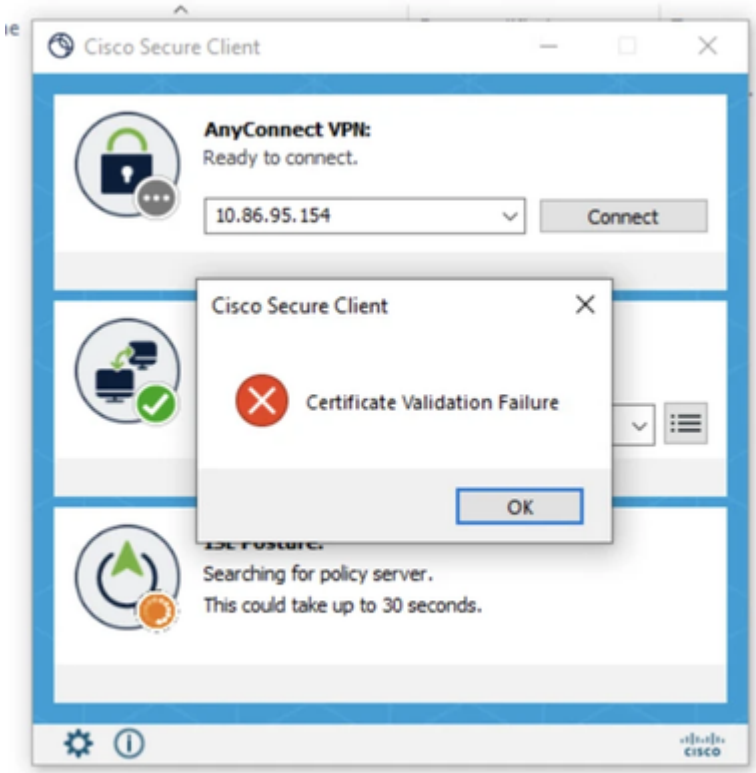
لعميل لمصادقة العميل EKU سمة إلى تفتقر العميل شهادة كانت إذا ASA

في هذا السيناريو، يستخدم عميل Cisco الآمن مصادقة الشهادة لإنشاء نفق WAPN إلى FTD أو ASA. ومع ذلك، إذا كانت شهادة العميل تفتقد إلى سمة EKU لمصادقة العميل، فسيفشل جلسة RAPN لأن ASA أو FTD يتطلب أن تكون هذه السمة موجودة في شهادة العميل.

المخطط



خطأ عميل Cisco الآمن: 'فشل التحقق من صحة الشهادة'



أخطاء DART الخاصة بالعميل الآمن من Cisco:توفر السجلات التالية من ملف AnyConnectVPN.txt في حزمة DART أن عميل Cisco الآمن رفض الشهادة المستخدمة للمصادقة المستندة إلى شهادة العميل (لتحديد موقع ملف AnyConnectVPN.txt في حزمة DART، انتقل إلى عميل Cisco Secure Client > AnyConnect VPN > سجلات > AnyConnect vpn.txt.).

<#root>

```
****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi

Description : Function: CVerifyExtKeyUsage::compareEKUs

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2

****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Information
Source : csc_vpnapi

Description : Function: CCertStore::GetCertificates

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

Certificate details:
Store: [Omitted Output]

****************************************
```

الحل: مراجعة المقترح في هذا المستند لضمان إستخدام العميل الآمن من Cisco للشهادة الصحيحة - بما في ذلك سمة EKU لمصادقة العميل - للحصول على مصادقة ناجحة مستندة إلى شهادة مع FTD أو ASA.

ملاحظة: من ال DART حزمة خطأ 'EKU ال في شهادة: 1.3.6.1.5.5.7.3.2' ، هذا الرقم '1.3.6.1.5.5.7.3.2' يتوافق مع معرف EKU الخاص بمصادقة العميل.

المشكلة 4. تفشل أنفاق شبكة VPN من موقع إلى موقع مع المصادقة المستندة إلى شهادة في حالة فقدان شهادة الهوية لسمة EKU لمصادقة

العميل

في هذا السيناريو، الذي يتضمن مصادقة قائمة على الشهادة لنفق VPN من موقع IKEv2 إلى موقع، تفتقر شهادة الهوية التي يستخدمها FTD/ASA (1) لإنشاء النفق إلى نظير FTD/ASA (2) إلى سمة EKU لمصادقة العميل. ونتيجة لذلك، لا يمكن إنشاء نفق VPN لأن النظير البعيد، FTD/ASA (2)، يتطلب وجود هذه السمة في الشهادة.

المخطط

أخطاء FTD أو ASA CLI: هذه هي الأخطاء التي تم ملاحظتها على FTD/ASA (2) أثناء المصادقة
FTD/ASA (1) التي تفتقر إلى سمة شهادة هوية IKEv2 عندما ترفض شهادة هوية FTD/ASA (1) المستندة إلى شهادة EKU لمصادقة العميل.

```
<#root>

                                                                    Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

                subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
                                                                    Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

    Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

                IKEv2 Certificate authentication failed.  Error: Certificate authentication failed

    Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

                                        IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

ملاحظة: في المثال أعلاه، كان FTD/ASA (2) يستخدم شهادة هوية تتضمن كل من سمات EKU الخاصة بكل

من ClientAuth و ServerAuth.

ملاحظة: في المثال أعلاه، يمكن أيضا إستبدال FTD/ASA (2) بموجه أو مركز VPN مادي أو قائم على شبكة خارجية (VPN). بعد ذلك، سوف تستمر المشكلة نفسها، لأن نظير VPN يتطلب أن تكون سمة EKU للمصادقة العميل موجودة في الشهادة المستخدمة من قبل FTD/ASA (1) للمصادقة الناجحة المستندة إلى الشهادة.

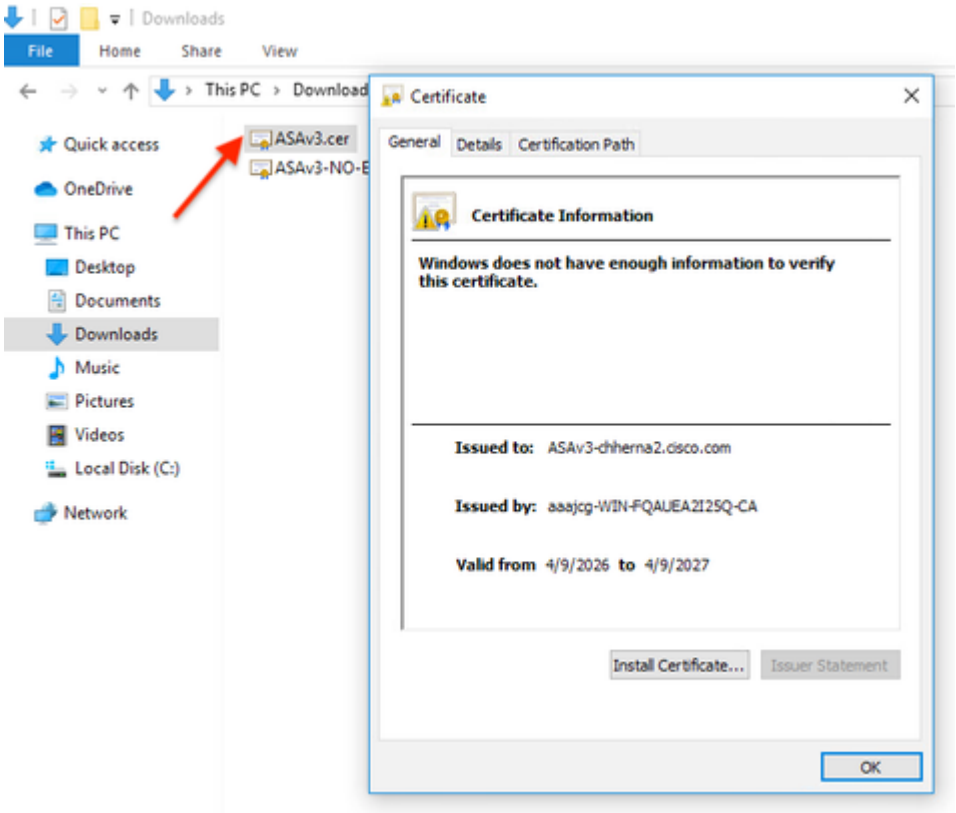
الحل: راجع المقترح في هذا المستند لضمان إستخدام FTD/ASA (1) لشهادة الهوية الصحيحة مع إلى موقع من موقع VPN نافق شبكة VPN لمصادقة العميل - بما في ذلك سمة EKU مصادقة قائمة على الشهادة.

إرشادات لتأكيد ما إذا كانت شهادتك تفتقر إلى سمة EKU لمصادقة العميل

التحقق من سمات EKU من شهادة .cer باستخدام إدارة شهادات Windows

اتبع الخطوات التالية للتحقق من سمات EKU من شهادة .cer باستخدام إدارة شهادات Windows:

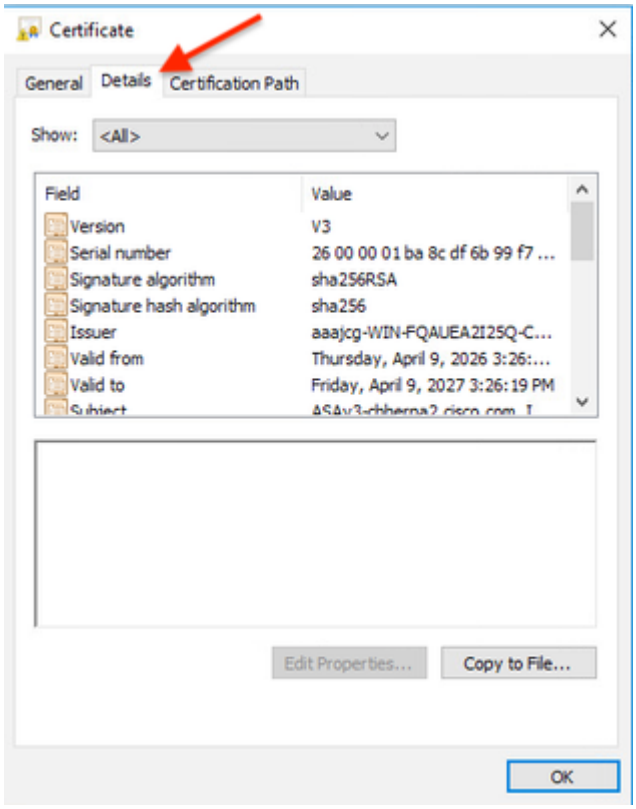
الخطوة 1. انقر نقرا مزدوجا على ملف .cer لفتحه في "إدارة شهادات Windows".



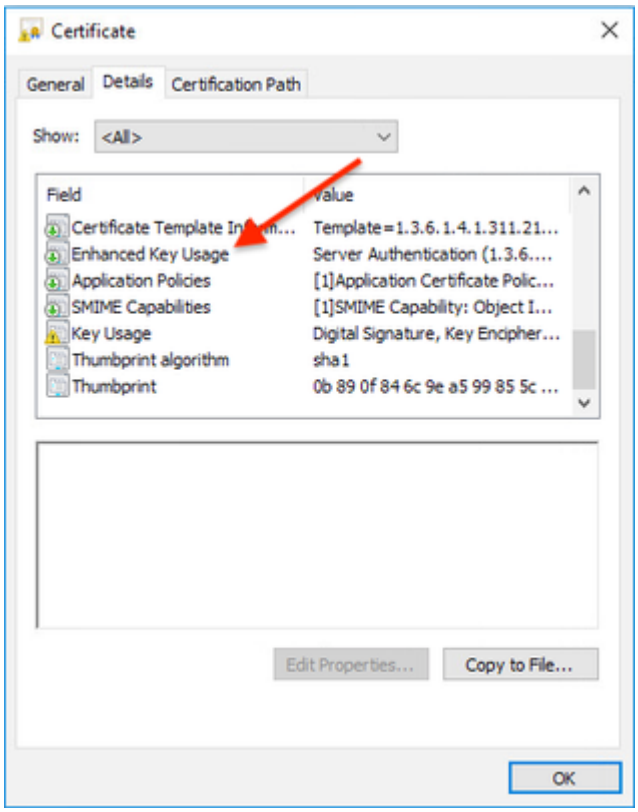
ملاحظة: يتم فتح ملفات وحدات التخفيض المعتمد فقط بهذه الطريقة مباشرة؛ إذا كانت شهادتك تحتوي على ملحق .pem، فأعد تسميته إلى .cer أو .crt أولا.

الخطوة 2. معالجة تحذير الأمان (إن وجد)، إذا ظهرت مطالبة تحذير أمان، انقر فوق فتح للمتابعة.

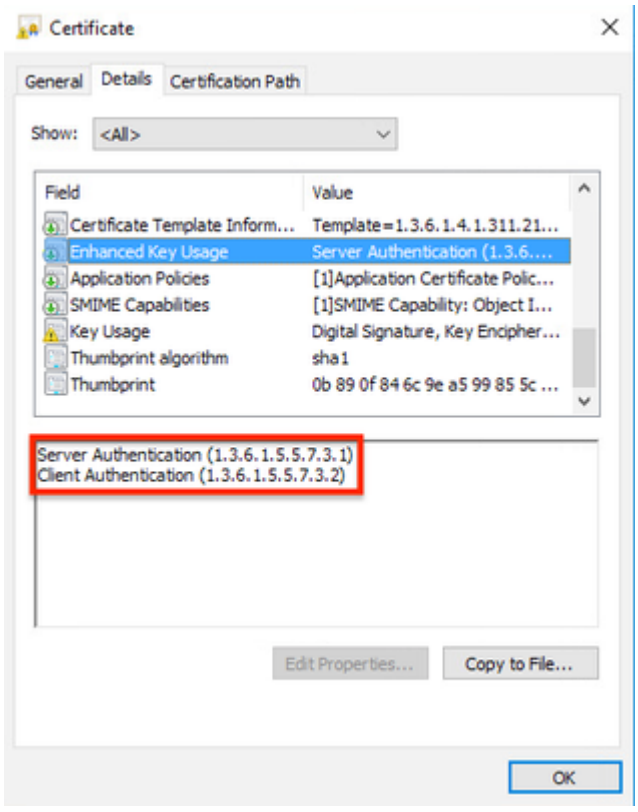
الخطوة 3. في نافذة الترخيص، انقر فوق علامة التبويب تفاصيل.



الخطوة 4. قم بالتمرير عبر قائمة الحقول وحدد "إستخدام المفتاح المحسن" (أو إستخدام المفتاح الموسع).

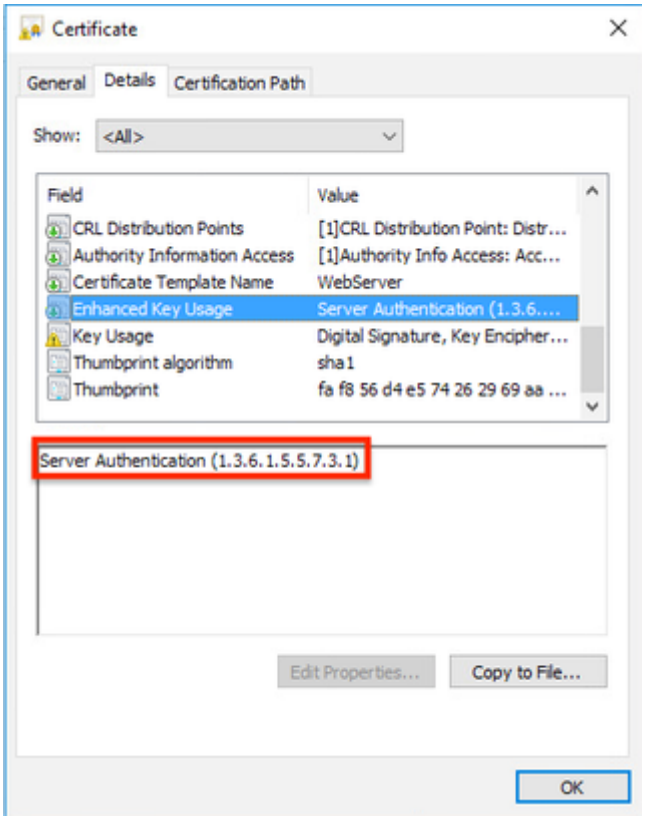


الخطوة 5. تحقق من سمات EKU، قد ترى إدخالات مثل "مصادقة الخادم" و"مصادقة العميل" تشير إلى قيم EKU الموجودة في الشهادة.

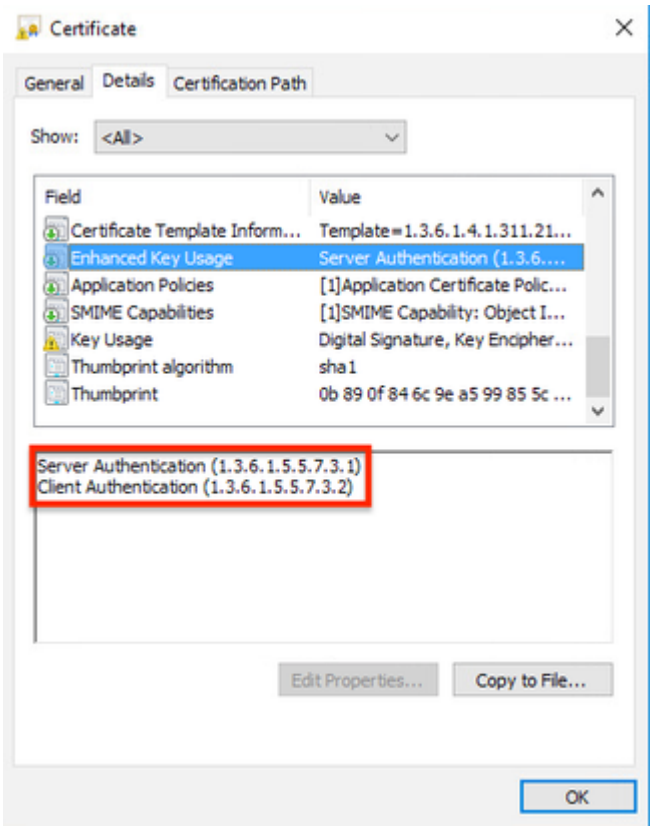


الخطوة 6. بعد التحقق، انقر فوق موافق لإغلاق نافذة الشهادة.

مثال 1: شهادة .cer هذه تفتقد سمة EKU لمصادقة العميل وتتضمن سمة EKU لمصادقة الخادم فقط.



مثال 2: تتضمن شهادة .cer هذه سمات EKU الخاصة بمصادقة الخادم والعميل.



تحقق من سمات EKU من شهادة PKCS#12 و PEM و .cer باستخدام OpenSSL

اتبع الخطوات التالية للتحقق من سمات EKU من شهادة .p12 (PKCS#12) و .pem (PEM) و.cer:

الخطوة 1. حدد مكان الشهادة التي تحتاج إلى فحصها، ثم قم بتصديرها بتنسيق .p12 (PKCS#12)، .pem (PEM) أو .cer.

لشهادات .p12 (PKCS#12)، أستخدم OpenSSL لاستخراج الشهادة من ملف .p12 (PKCS#12)، قد يحتوي ملف .p12 (PKCS#12) على المفتاح الخاص، والشهادة، وشهادات CA.

أستخدم الأمر التالي لاستخراج الشهادة من ملف .p12 (PKCS#12) إلى ملف .pem (بدون المفتاح الخاص أو سلسلة CA):

```
openssl pkcs12 -in yourfile.p12 -nokeys -clcerts -out cert.pem
```

- الملف الخاص بك.p12: إستبدال باسم الملف الفعلي الخاص بك.
- قد تحتاج إلى إدخال كلمة المرور لملف .p12.
- كورت بيم: له الشهادة المستخرجة (بدون المفتاح الخاص أو سلسلة CA) بتنسيق .pem (PEM).

الخطوة 2. أستخدم أوامر OpenSSL التالية لعرض تفاصيل الشهادة وسمات EKU.

أ) لملفات .pem، أستخدم الأمر openssl التالي لعرض تفاصيل الشهادة وخصائص EKU:

```
openssl x509 -in cert.pem -text -noout
```

- كورت بيم: إستبدال باسم الملف الفعلي الخاص بك.

ب) لملفات .cer، أستخدم الأمر openSSL التالي لعرض تفاصيل الشهادة وخصائص EKU:

```
openssl x509 -in yourfile.cer -text -noout
```

- الملف الخاص بك.cer: إستبدال باسم الملف الفعلي الخاص بك.

الخطوة 3. بعد ذلك، ابحث عن قسم إستخدام المفتاح الموسع X509v3 في الإخراج، فقد ترى إدخالات مثل "مصادقة خادم ويب TLS" و"مصادقة عميل ويب TLS" تشير إلى قيم EKU الموجودة في الشهادة.

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

أو OIDs لسمة EKU (معرفات الكائنات):

```
X509v3 Extended Key Usage:
1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2
```

- 1.3.6.1.5.5.7.3.1: معرف EKU الخاص بمصادقة الخادم
- 1.3.6.1.5.5.7.3.2: معرف EKU الخاص بمصادقة العميل

سمة EKU لمصادقة العميل وتتضمن سمة EKU هذه تفتقد .pem (PEM) شهادة :1 لمثال لمصادقة الخادم فقط.

<#root>

```
                                                MyHost$ openssl x509 -in cert.pem -text -noout
                                                                                Certificate:
                                                                                    Data:
                                                                              Version: 3 (0x2)
                                                                                Serial Number:
                                                  26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
                                                                    Signature Algorithm: sha256WithRSAEncryption
                                                  Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
                                                                                    Validity
                                                                          Not Before: Mar 27 00:31:40 2026 GMT
                                                                          Not After : Mar 26 00:31:40 2028 GMT
                                        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
                                                                                Subject Public Key Info:
                                                                      Public Key Algorithm: rsaEncryption
                                                                                RSA Public-Key: (2048 bit)
                                                                                    Modulus:
                                                                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                                                                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                                                                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                                                                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                                                                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                                                                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                                                                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                                                                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                                                                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                                                                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                                                                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                                                                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                                                                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                                                                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                                                                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                                                                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                                                                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                                                                                                        82:f5
                                                                                Exponent: 65537 (0x10001)
                                                                                    X509v3 extensions:
                                                                            X509v3 Subject Key Identifier:
                                                  0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
                                                                            X509v3 Authority Key Identifier:
                                        keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

                                                                            X509v3 CRL Distribution Points:

                                                                                    Full Name:
                    URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

                                                                            Authority Information Access:
                  CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

                                                                                1.3.6.1.4.1.311.20.2:
                                                                                 ...W.e.b.S.e.r.v.e.r
                                                                            X509v3 Key Usage: critical
                                                                    Digital Signature, Key Encipherment


                                                                        X509v3 Extended Key Usage:

                                                                                <-------- "EKU SECTION"
```

```
                                                TLS Web Server Authentication

                                <-------- "Server Authentication EKU Attribute Included"
                                            Signature Algorithm: sha256WithRSAEncryption
                                  2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
                                  0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
                                  46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
                                  d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
                                  55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
                                  dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
                                  41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
                                  d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
                                  7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
                                  4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
                                  61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
                                  70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
                                  86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
                                  2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
                                                                        c5:d3:c5:8f
```

مثال 2: تتضمن شهادة .pem (PEM) هذه سمات EKU الخاصة بمصادقة العميل والخادم.

<#root>

```
                                    MyHost$ openssl x509 -in cert.pem -text -noout
                                                            Certificate:
                                                                    Data:
                                                          Version: 3 (0x2)
                                                            Serial Number:
                                  26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
                                                Signature Algorithm: sha256WithRSAEncryption
                                 Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
                                                                    Validity
                                                      Not Before: Mar 26 23:44:58 2026 GMT
                                                      Not After : Mar 26 23:44:58 2027 GMT
                          Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
                                                                Subject Public Key Info:
                                                  Public Key Algorithm: rsaEncryption
                                                            RSA Public-Key: (2048 bit)
                                                                    Modulus:
                                                00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                                                56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                                                ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                                                62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                                                91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                                                fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                                                74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                                                2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
                                                75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                                                6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                                                86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                                                33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                                                c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                                                48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                                                38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
```

```
                                                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                                                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                                                                                          ba:7d
                                                                Exponent: 65537 (0x10001)
                                                                      X509v3 extensions:
                                                           X509v3 Subject Key Identifier:
                                          D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
                                                           X509v3 Authority Key Identifier:
                                      keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

                                                           X509v3 CRL Distribution Points:

                                                                                Full Name:
                        URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

                                                                 Authority Information Access:
                       CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

                                                                 X509v3 Key Usage: critical
                                                              Digital Signature, Key Encipherment
                                                                      1.3.6.1.4.1.311.21.7:
                                                                    0-.%+.....7.....^..9...
                                                                    ...b.../ ...R...Z..d...


                                                           X509v3 Extended Key Usage:


                                                                 <-------- "EKU SECTION"


                                                    TLS Web Server Authentication, TLS Web Client Authentication


                                                          <----- "Server & Client EKU Attributes Included"
                                                                      1.3.6.1.4.1.311.21.10:
                                                                                          0.0
                                                                                  ..+.......0
                                                                                  ..+.......
                                                                       S/MIME Capabilities:
                                                                ......0...+....0050...*.H..
                                                                                  ..*.H..
                                                           Signature Algorithm: sha256WithRSAEncryption
                                                3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
                                                ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
                                                11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
                                                d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
                                                c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
                                                0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
                                                33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
                                                84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
                                                29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
                                                3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
                                                9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
                                                01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
                                                b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
                                                0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
                                                                                          cc:67:09:8e
```

الحلول

يمكن للمسؤولين الاختيار من أحد خيارات الحل التالية.

الخيار 1. التبديل إلى CAs الجذر العام التي توفر شهادات EKU المجمعة

بعض الشهادات المصدقة الجذر العامة، مثل DigiCert و IdenTrust، تصدر شهادات مع أنواع EKU مجمعة (شهادات الخادم والعميل) من جذر بديل، والتي لا يتم تضمينها في مخزن جذر Chrome. قم بالتنسيق مع موفر المرجع المصدق للتحقق من توفر هذه الشهادات، وقبل الشروع، تأكد من أن كل من الخادم الذي يقدم الشهادة والعملاء الذين يستهلكونها يثقون في المرجع المصدق الجذر المطابق.

يلقي هذا النهج من الحاجة إلى ترقية برامج الخوادم لتقليل الحالات غير المشروبة في EKU المصادقة الخاصة والعملاء والتي يتم فرضها بواسطة نهج برامج Chrome Root.

الجدول التالي، الذي يبين أمثلة لأنواع CA الجذر العام وأنواع EKU، ليس قائمة شاملة وهو لأغراض توضيحية فقط.

مورد CA	نوع EKU	الجذر المصدق المرجع	المصدق المرجع/الإصدار الفرعي
IdenTrust	ClientAuth + ServerAuth	IdenTrust Public Root CA 1	خادم القطاع العام من IdenTrust CA 1
IdenTrust	clientAuth	IdenTrust Public Root CA 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth (المستعرض موثوق به)	IdenTrust Commercial Root CA 1	خادم HydrantID CA O1
ديجي سيرت	ClientAuth + ServerAuth	جذر فرعي G2 المؤكد ل DigiCert	فرعي DigiCert المضمون CA G2
ديجي سيرت	clientAuth	جذر فرعي G2 المؤكد ل DigiCert	DigiCert Secure ID Client CA G2
ديجي سيرت	serverAuth (المستعرض موثوق به)	جذر عام DigiCert g2	DigiCert Global G2 TLS RSA SHA256

الخيار 2. تجديد الشهادات الحالية لتمديد صلاحيتها

ستستمر الشهادات التي تم إصدارها بواسطة CAs الجذر العام قبل مايو 2026 في الوفاء بالشهادات التي تحتوي على EKU المصادقة الخادم والعميل حتى انتهاء مدة صلاحيتها. ومع ذلك، من الأفضل تجديد شهادات EKU المجمعة قبل حدوث إعداد النهج.

- قد تختلف سياسة CA العامة وتواريخ التنفيذ حسب المورد.
- ارجع إلى المرجع المصدق وقم بتجديد الشهادة وفقا لذلك.
- بعد 15 آذار/مارس 2026، تكون الشهادات العامة صالحة فقط ل 200 يوم.
- مع الأخذ بعين الاعتبار أن بعض وكالات تشجيع الاستثمار العامة قد توقفت عن إصدار شهادات EKU مجتمعة.

الخيار 3. الترحيل إلى PKI الخاص لإصدار شهادات EKU (الخادم والعميل) المشتركة

تقييم إمكانية التحول إلى بنية أساسية للمفاتيح العامة الخاصة (PKI)، ثم إعداد مرجع مصدق خاص لإصدار شهادات فردية مع EKU (شهادات الخادم والعميل مع وحدات EKU المطلوبة).

قبل إصدار أو نشر شهادة، تأكد من أن كل من الخادم الذي يقدم الشهادة وكل العملاء الذين يستهلكونها يثقون في المرجع المصدق الجذر المطابق.

الخيار 4. الحصول على شهادة موثوق بها بشكل عام باستخدام EKU لمصادقة العميل فقط

توفر بعض المراجع المصدقة (CA) مثل SSL.com شهادات مصادقة العميل المخصصة. وتكون هذه الشهادات منفصلة عن شهادات TLS وتستخدم عادة لمصادقة المؤسسة.

⚠ تحذير: وبالنسبة لبيئات الإنتاج، يوصى بشدة بأن يستخدم العملاء الشهادات ذات سمات EKU المناسبة. وتضمن هذه الممارسة الأمن والتوافق والالتزام بالمعايير وأفضل الممارسات في هذا المجال. ينبغي إعتبار الشهادات التي لا تتضمن سمات EKU مجرد حل بديل مؤقت، وفقط مع فهم واضح للمخاطر المرتبطة بها.

الأسئلة المتداولة (FAQ)

س 1. هل يجب أن أقلق بشأن هذا إذا أستخدمت PKI خاص؟

ألف: تحدد كل منظمة السياسة التي تنفذها الولايات المتخصصة الخاصة. إذا قام المرجع المصدق الخاص لديك باعتماد نفس معايير الإصدار - مثل إزالة سمة EKU لمصادقة العميل من الشهادات - تكون الإرشادات الواردة في هذا المستند قابلة للتطبيق.

السؤال 2. هل يمكنني الاستمرار في إستخدام الشهادات الموجودة لدي؟

ج: نعم، يمكن إستخدام الشهادات الصالحة ذات EKUs المجمعة حتى وقت انتهاء مدة الصلاحية.

Q3. ما هي الخيارات المتوفرة لدمج FMC أو FDM مع ISE من خلال PXgrid إذا كانت الشهادة المثبتة على FMC/FDM تفتقر إلى سمة EKU لمصادقة العميل؟

ج: بالإضافة إلى الحلول المقترحة في هذا المستند، نوصيك بشدة بالتحقق من مراجع ISE التالية:

- إشعار ميداني: FN74392 - محرك خدمات الهوية من Cisco: التأثير على الاتصالات الآمنة من مصادقة عميل CA العامة تغييرات EKU بدءا من مايو 2026 - الحل البديل متوفر
- إعداد محرك خدمات الهوية لقيود إستخدام المفاتيح الموسعة في الشهادات التي تصدرها السلطات المصدقة العامة

ملاحظة: على الرغم من أن إستخدام الشهادة العامة الموقعة من قبل CA مدعوم من أجل IMS. توصي Cisco باستخدام شهادة ISE الداخلية CA حيث إن هذا الاتصال خاص بالحركات الداخلية فقط.

السؤال 4- ما هي وحدة "مصادقة العميل" ولماذا كانت في شهادتي؟

ألف: تشير وحدة الاحتفاظ بالمخزون (EKU) المسماة "مصادقة العميل" إلى أنه يمكن إستخدام شهادة من قبل العميل للمصادقة على الخادم. بعض CAs تاريخيا أدرجها في شهادات TLS افتراضيا، غير أنها لم تكن مطلوبة لأمان موقع الويب العادي.

Q5. تقول شهادة TLS الحالية "مصادقة العميل" تحت إستخدام المفتاح الموسع. هل هو الآن غير صالح؟

أ: لا، لا يزال صحيحا. لا تحتاج لاستبداله فورا. عند التجديد، لن تشتمل الشهادة الجديدة ببساطة على EKU clientAuth.

Q6. كيف يمكنني التحقق مما إذا كانت الشهادة تحتوي على EKU ل ClientAuth؟

ج: يمكنك فحص تفاصيل الشهادة باستخدام أدوات OpenSSL أو PowerShell أو واجهة المستخدم الرسومية (GUI) للتحقق من ملحق إستخدام المفتاح الموسع.

Q7. هل يمكنني الحصول على شهادة موثوق بها بشكل عام مع وحدة EKU فقط لمصادقة العميل؟

ج: توفر بعض المراجع المصدقة (CA) مثل SSL.com شهادات مصادقة العميل المخصصة.

وتكون هذه الشهادات منفصلة عن شهادات TLS وتستخدم عادة لمصادقة المؤسسة.

Q8. هل يؤثر هذا على وحدات EKU الأخرى أو أنواع الشهادات (توقيع الرموز والبريد الإلكتروني وما إلى ذلك)؟

ج: لا، هذا التغيير خاص بشهادات خادم TLS. تشتمل شهادات توقيع الرموز والبريد الإلكتروني على متطلبات وحدة الاحتفاظ بالمخزون (EKU) الخاصة بها.

السؤال 9: أين يمكنني أن أرى المتطلبات الرسمية لهذا التغيير؟

ج: توفر سياسة برنامج Google Chrome Root إرشادات بشأن حظر إستخدام EKU العميل في شهادات خادم TLS.

Q10. هل من الآمن إستخدام الشهادات بدون سمات EKU الخاصة بالعميل والخادم في بيئة الإنتاج؟

ألف: بالنسبة لبيئات الإنتاج، يوصى بشدة بأن يستخدم العملاء الشهادات ذات سمات EKU المناسبة. وتضمن هذه الممارسة الأمن والتوافق والالتزام بالمعايير وأفضل الممارسات في هذا المجال. ينبغي إعتبار الشهادات التي لا تتضمن سمات EKU مجرد حل بديل مؤقت، وفقط مع فهم واضح للمخاطر المرتبطة بها.

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC) من Cisco. يلزم عقد دعم صالح: جهات إتصال الدعم العالمية من Cisco.
- الدعم والتنزيلات من Cisco: الدعم الفني والتنزيلات من Cisco

الأخطاء ذات الصلة

- CSCwt9492 ENH: يجب أن تتحقق FMC من وجود سمة EKU لمصادقة العميل في شهادة العميل المستخدمة لتكامل pxGrid
- CSCwt94509 ENH: يجب أن تعرض FMC رسالة تشير إلى أن سمة EKU لمصادقة العميل مطلوبة في شهادة العميل المستخدمة لتكامل pxGrid

- نكت مل اذإ ASA نيوكت ريذحت رادصإ - طقف EKU مداخ رييغت 2026 ويام CSCwt61767
EKU ةيفاك

- ISE يف ClientAuth EKU ذافنإل ريثأتلا مييقت :EKU CSCws83036

عجارم Cisco ISE

- ةنمآلا تالاصتالا ىلع ريثأتلا :Cisco نم ةيوهلا تامدخ كرحم - FN74392 :يناديم راعشإ
رفوتم ليدبلا لحلا - 2026 ويام نم اءدب EKU تاريغت ةماعلا CA ليمع ةقداصم نم

- يتلا تاداهشلا يف ةعسوملا حيتافملا مادختسإ دويقل ةيوهلا تامدخ كرحم دادعإ
ةماعلا ةقدصملا تاطلسلا اهردصت

عجارملا ةيجراخلا

- تور موركلا جمانرب ةسايس

- ةباوب IdenTrust

- هتفرعم ىلإ جاتحت ام - TLS مداخ تاداهش نم ليمعلا ةقداصمل EKU ةلازإ - SSL

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).