# تكوين VCS باستخدام CAC وقارئ البطاقات الذكية

## المحتويات


المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
ما هي البطاقة الذكية؟
التكوين
التحقق من الصحة
استكشاف الأخطاء وإصلاحها


## المقدمة

يصف هذا المستند إرشادات خطوة بخطوة لتثبيت قارئ البطاقة الذكية وتسجيل الدخول لبطاقة الوصول المشتركة واستخدامها مع خادم إتصالات الفيديو (VCS) من Cisco وأ VCS مثل البنوك للمؤسسات التي تتطلب مصادقة ثنائية العوامل لبيئة المستشفيات أو الحكومات ذات المنشآت الآمنة.

## المتطلبات الأساسية

### المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مسؤول Cisco Expressway (X14.0.2).

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## معلومات أساسية

وتوفر إتفاقية التحكم في الوصول إلى البنية الأساسية المصادقة المطلوبة، ومن ثم تعرف "الأنظمة" من الذي تمكن من الوصول إلى بيئتها وأي جزء من البنية الأساسية سواء كان مادي أو إلكتروني. وتضمن البيئات المصنفة حكومي، وغيرها من الشبكات الآمنة، تسود قواعد "الوصول الأقل امتيازا" أو "الحاجة إلى المعرفة". يمكن لأي شخص إستخدام سجل الدخول، وتطلب المصادقة شيئا حصل عليه المستخدم، مثل إخراج CAC، المعروفة أيضا ببطاقة الوصول المشترك، في عام 2006 حتى الآن تحتاج الفرد إلى أجهزة متعددة، سواء كانت مواصلات بينية أو بطاقات هوية أو ملحقات للوصول إلى مكان عمله أو أنظمته.

# ما هي البطاقة الذكية؟

تعد البطاقات الذكية مكونا أساسيا للبنية الأساسية للمفاتيح العام (PKI) التي تستخدمها Microsoft للدمج في نظام Windows الأساسي لأن البطاقات الذكية تحسن الحلول الخاصة بالبرامج فقط، مثل مصادقة العميل وتسجيل الدخول والبريد الإلكتروني الآمن. البطاقات الذكية هي نقطة تقارب لشهادات المفاتيح العامة والمفاتيح المرتبطة لأنها:

- توفير وحدات تخزين مقاومة للعبث لحماية المفاتيح الخاصة وغيرها من أشكال المعلومات الشخصية.
- عزل العمليات الحسابية الحيوية للأمان، والتي تتضمن المصادقة والتوقيعات الرقمية وتبادل المفاتيح عن الأجزاء الأخرى من النظام التي لا تحتاج إلى معرفة.
- تمكين إمكانية نقل بيانات الاعتماد والمعلومات الخاصة الأخرى بين أجهزة الكمبيوتر في العمل أو المنزل أو أثناء التنقل.

أصبحت البطاقة الذكية جزءا لا يتجزأ من النظام الأساسي لنظام التشغيل Windows لأن البطاقات الذكية توفر ميزات جديدة ومرغوبة كما هو الحال بالنسبة لصناعة الكمبيوتر عند تقديم المواس أو القرص المدمج. إذا لم تكن لديك بنية أساسية PKI داخلية في الوقت الحالي، فيلزمك التأكد من القيام بذلك أولا. لا يغطي هذا المستند تثبيت هذا الدور في هذه المقالة المحددة ولكن يمكن العثور على معلومات حول كيفية تنفيذ هذا الإجراء هنا: http://technet.microsoft.com/en-us/library/hh831740.aspx.

# التكوين

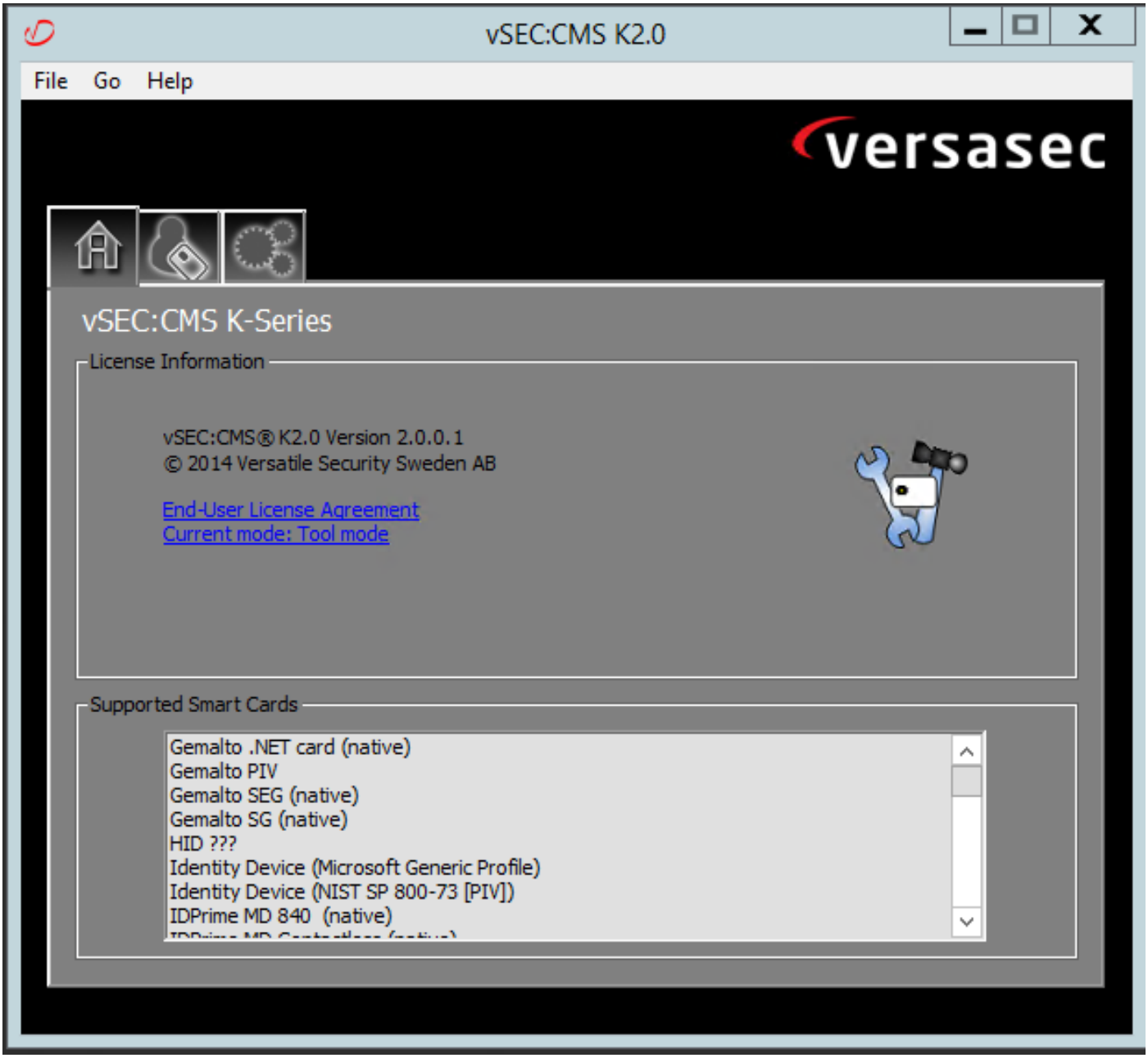
يفترض هذا المختبر أنك قمت بدمج LDAP مع VCS وأن لديك مستخدمين يمكنهم تسجيل الدخول باستخدام بيانات اعتماد LDAP.

1. مهام المختبر
2. تثبيت البطاقة الذكية
3. تكوين قوالب المرجع المصدق
4. تسجيل شهادة وكيل التسجيل
5. التسجيل نيابة عن...
6. تكوين VCS لبطاقة الوصول المشترك

المهام المطلوبة:

خادم مجال Windows 2012R2 الذي يحتوي على هذه الأدوار/البرامج المثبتة:

- جهة منح الشهادة
- خدمة Active Directory
- DNS
- كمبيوتر Windows مرفق بطاقة ذكية
- vSEC: برنامج الإدارة CMS K-Series لإدارة البطاقة الذكية:




برامج قارئ بطاقات فيرسا

**تثبيت البطاقة الذكية**

عادة ما تأتي أجهزة قراءة البطاقات الذكية مزودة بتعليمات حول كيفية توصيل أي كابلات ضرورية. فيما يلي مثال على تثبيت هذا التكوين.

**كيفية تثبيت برنامج تشغيل جهاز لقارئ البطاقة الذكية**

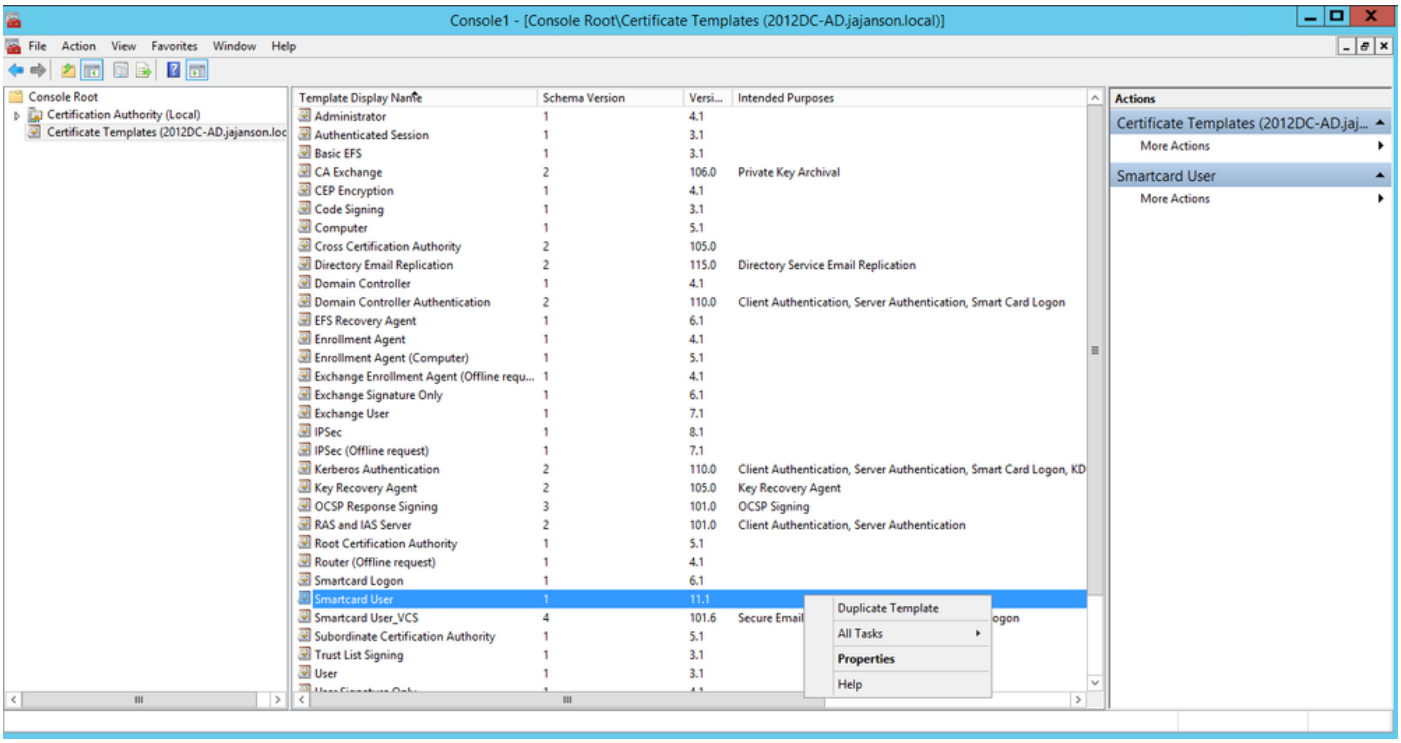
إذا تم اكتشاف قارئ البطاقة الذكية وتثبيته، فإن شاشة تسجيل الدخول إلى Windows التي تعترف بذلك. إذا لم تكن:

1. قم بتوصيل البطاقة الذكية بمنفذ USB الموجود على كمبيوتر Windows
2. اتبع التوجيهات التي تظهر على الشاشة لتثبيت برنامج تشغيل الجهاز. يتطلب ذلك وسائط برنامج التشغيل التي تم اكتشاف الجهة المصنعة للبطاقة الذكية أو برنامج التشغيل في Windows. انا في حالتي استعملت برنامج السواقة المصنعة من موقع التنزيل تبعهم. **ال ثق في نظام التشغيل Windows**.
3. انقر بزر الماوس الأيمن فوق رمز **جهاز الكمبيوتر** على سطح المكتب وانقر فوق **إدارة** في القائمة الفرعية.

4. قم بتوسيع عقدة **الخدمات والتطبيقات**، وانقر فوق **الخدمات**.
5. في الجزء الأيمن، انقر بزر الماوس الأيمن على **البطاقة الذكية**. انقر فوق **خصائص** في القائمة الفرعية.
6. على علامة التبويب **عام**، حدد **تلقائي** في القائمة المنسدلة **نوع بدء التشغيل**. وانقر فوق **OK**.
7. أعد تشغيل الجهاز إذا كان معالج الأجهزة يرشدك للقيام بذلك.

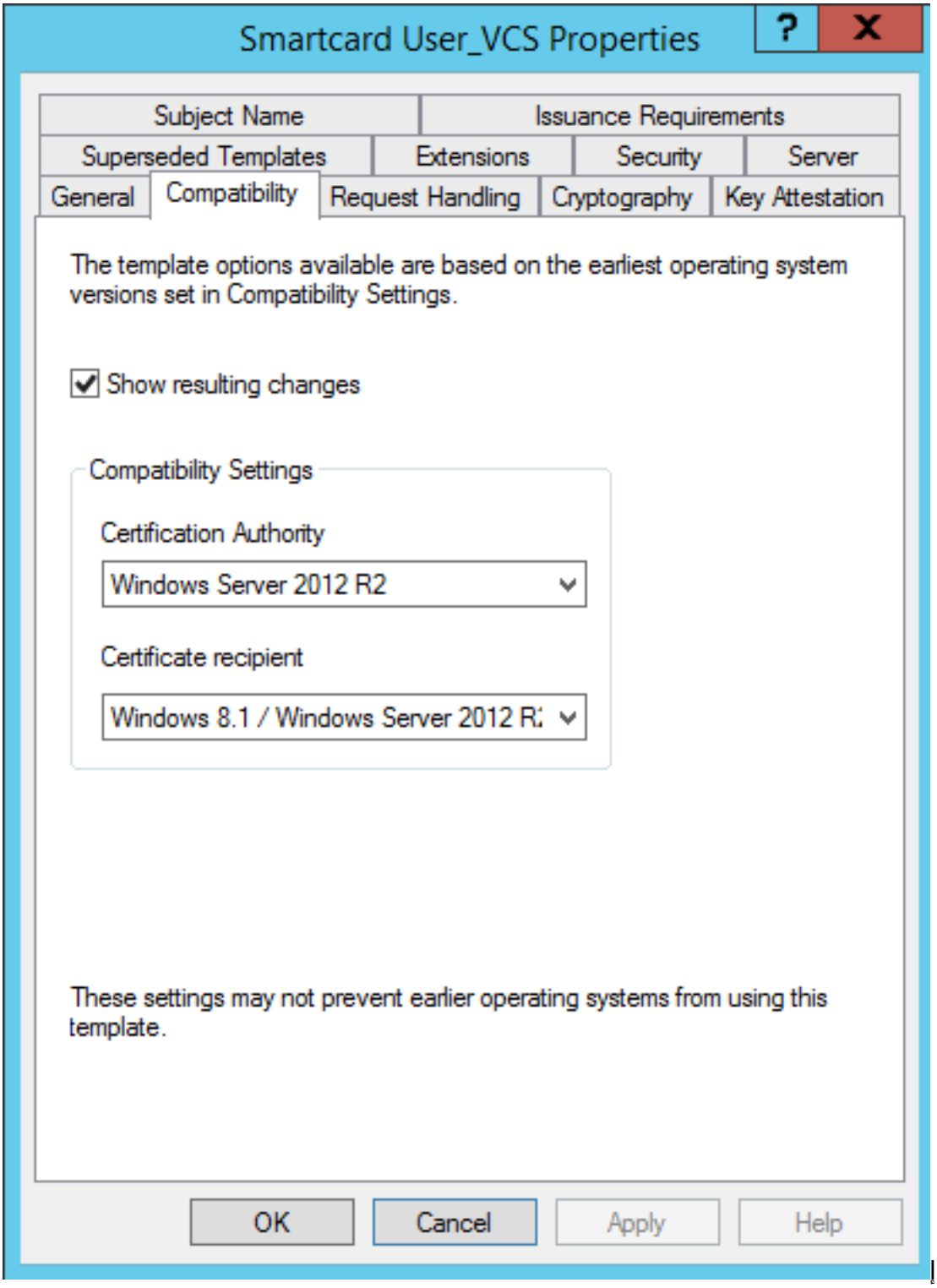
**تكوين قوالب المرجع المصدق**

1. تشغيل MMC المصدق من الأدوات الإدارية.
2. انقر أو حدد عقدة **قوالب الشهادات** وحدد **إدارة**.
3. انقر بزر الماوس الأيمن أو حدد قالب شهادة **مستخدم البطاقة الذكية** ثم حدد **مضاعفة** كما هو موضح في الصورة.



قوالب شهادات وحدة التحكم بالمجال

4. في علامة التبويب **توافق**، تحت **مرجع مصدق**، راجع التحديد وقم بتغييره إذا لزم الأمر.

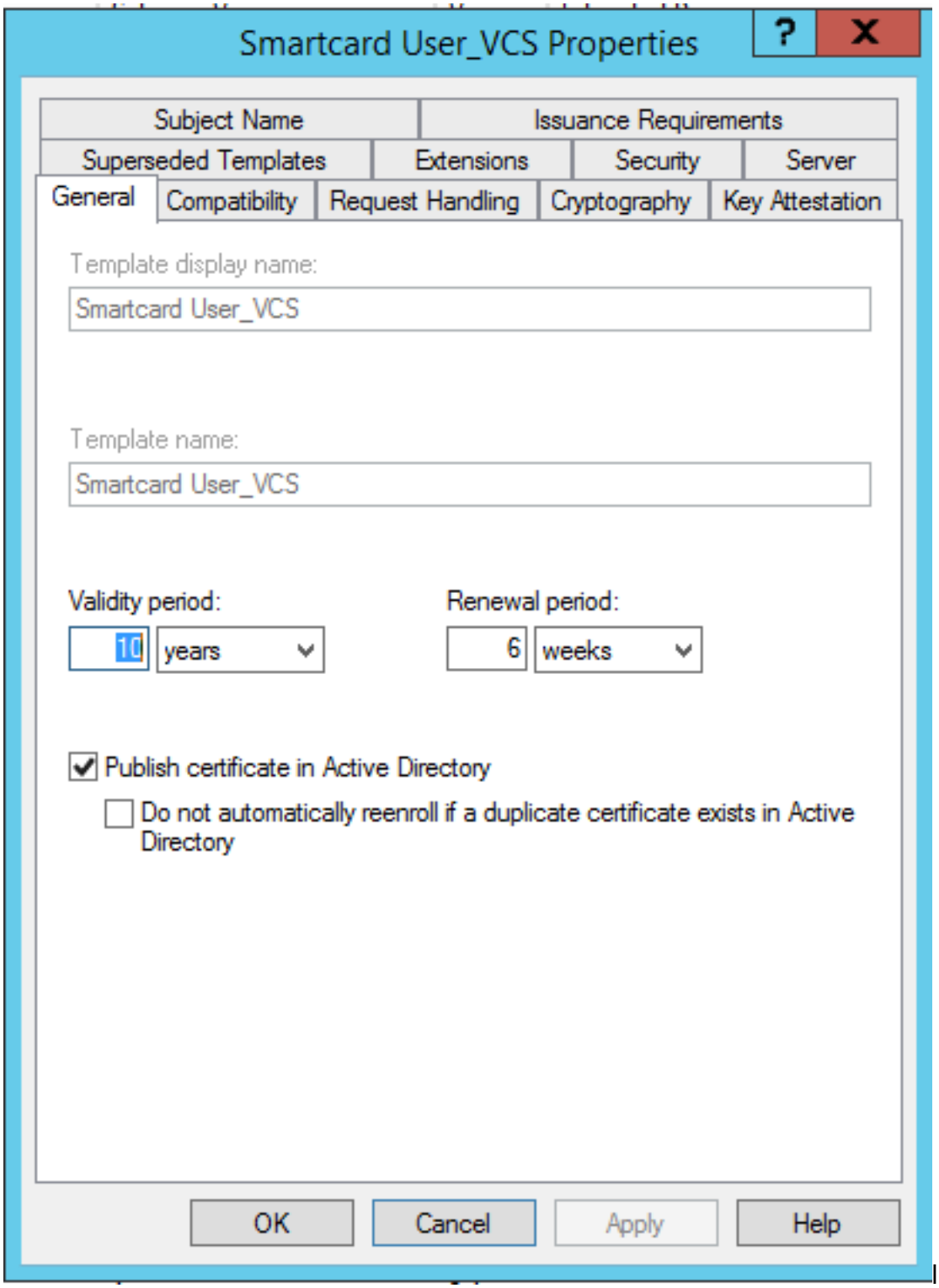


إعدادات توافق البطاقة الذكية

5. على علامة التبويب **عام**:

أ. حدد اسما، مثل **SmartCard User_VCS**.

ب. قم بتعيين فترة الصلاحية على القيمة المرغوبة. طقطقة **يطبق**.

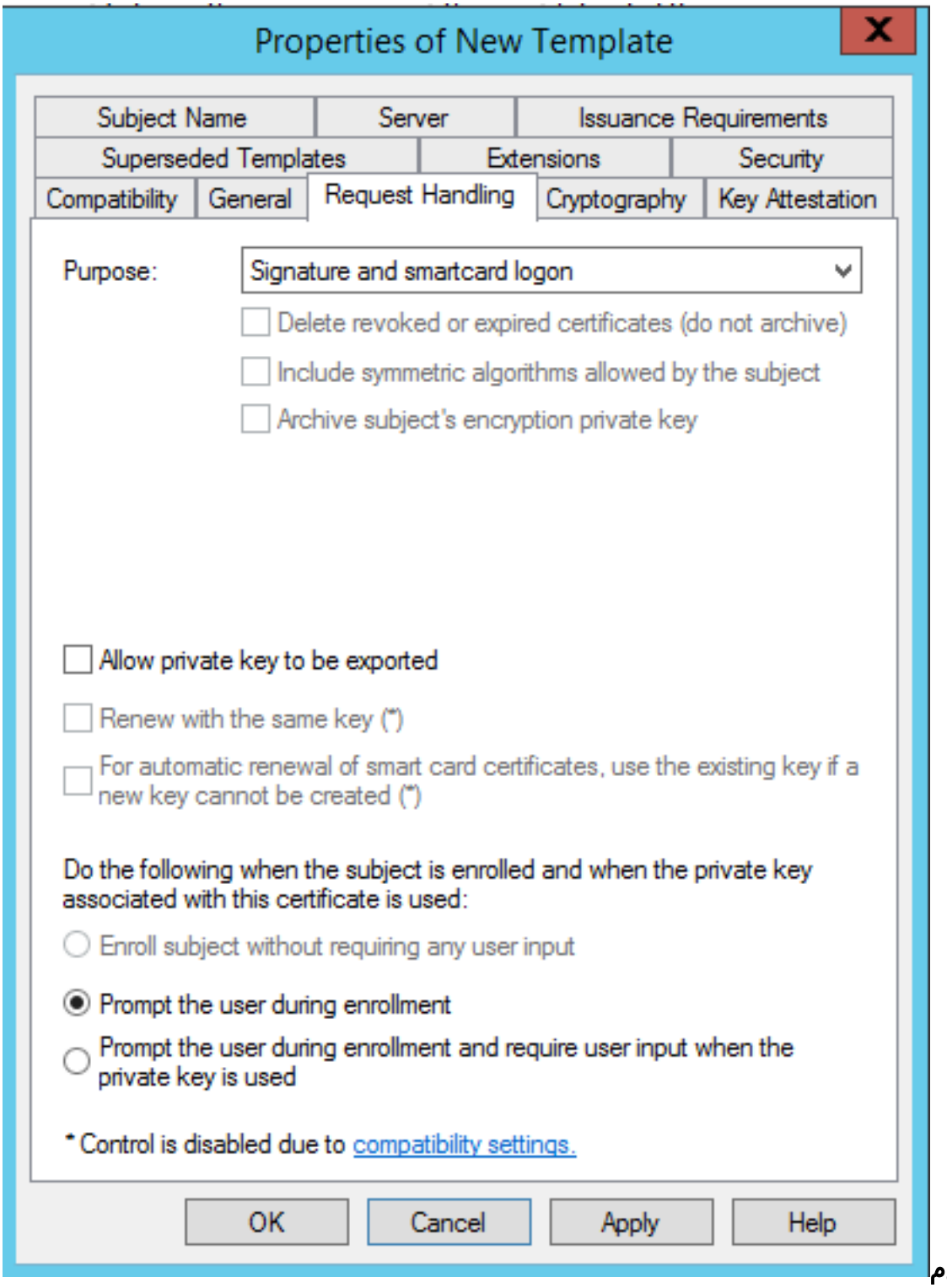



انتهاء صلاحية الوقت العام للبطاقة الذكية

6. في علامة التبويب **معالجة الطلب**:

أ. تعيين **الغرض** على **التوقيع وتسجيل الدخول إلى البطاقة الذكية**.

ب. انقر فوق **مطالبة المستخدم أثناء التسجيل. طقطقة يطبق**.

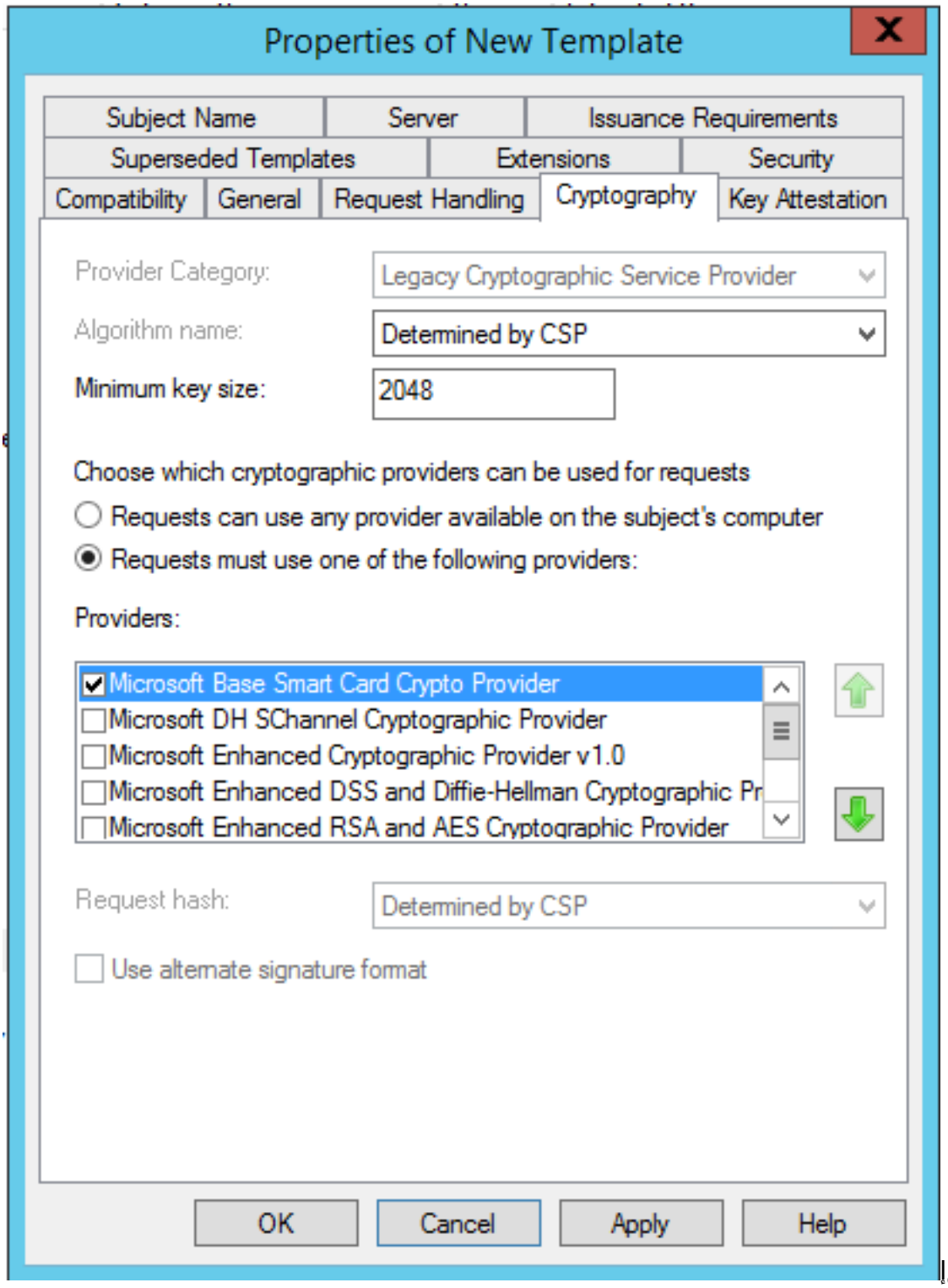



**معالجة طلب البطاقة الذكية**

7. في علامة التبويب **التشفير**، قم بتعيين الحد الأدنى لحجم المفتاح إلى 2048.

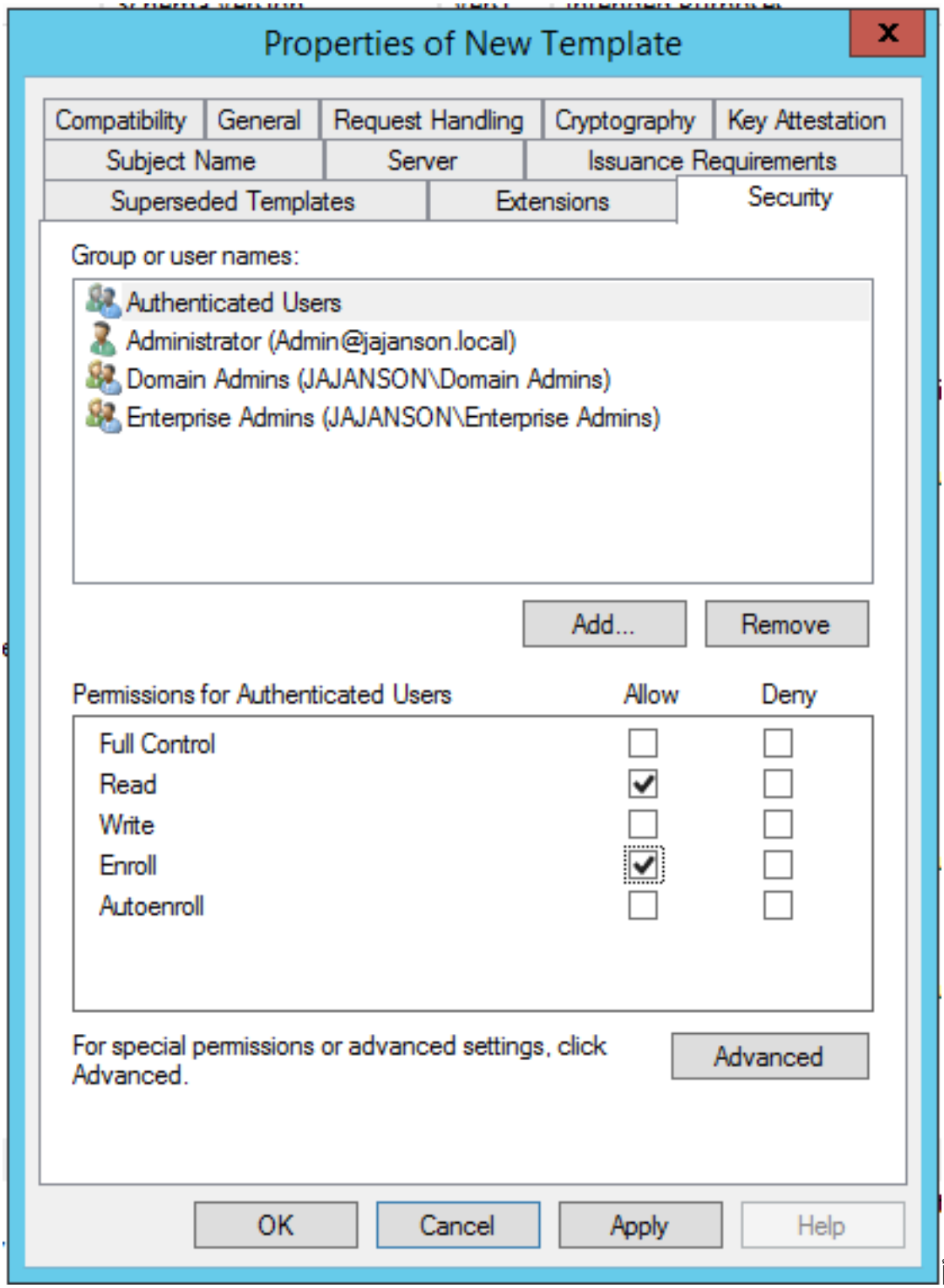
أ. انقر فوق **التطلبات يجب أن تستخدم أحد الموفرين التاليين**، ثم حدد **موفر تشفير البطاقة الذكية لقاعدة Microsoft**.

ب. طقطقة **يطبق**.



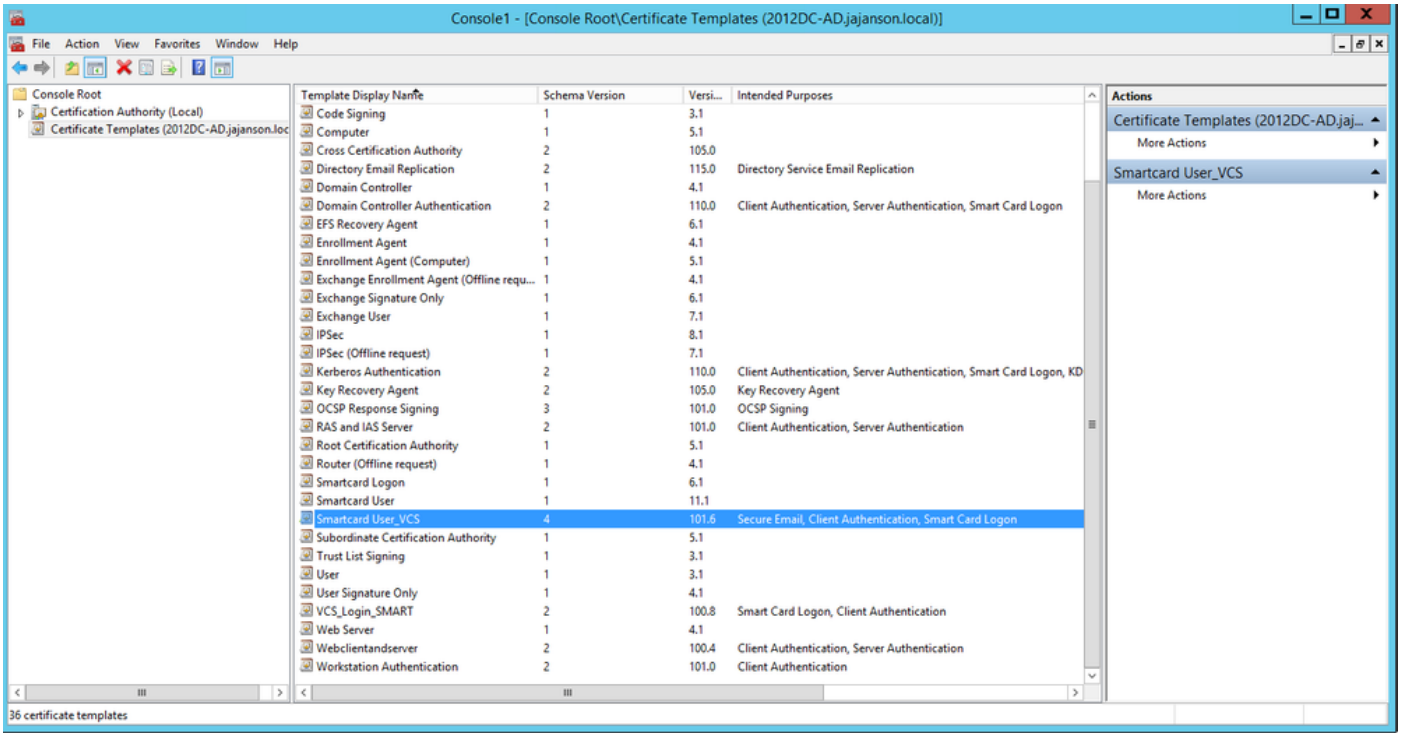
إعدادات تشفير الشهادة

8. في علامة التبويب "أمان"، أضف مجموعة الأمان التي تريد منح حق الوصول إلى التسجيل لها. على سبيل المثال، إذا كنت ترغب في منح حق الوصول إلى جميع المستخدمين، فحدد مجموعة المستخدمين المصدق عليهم، ثم حدد أذونات **التسجيل** لهم.



أمان القالب

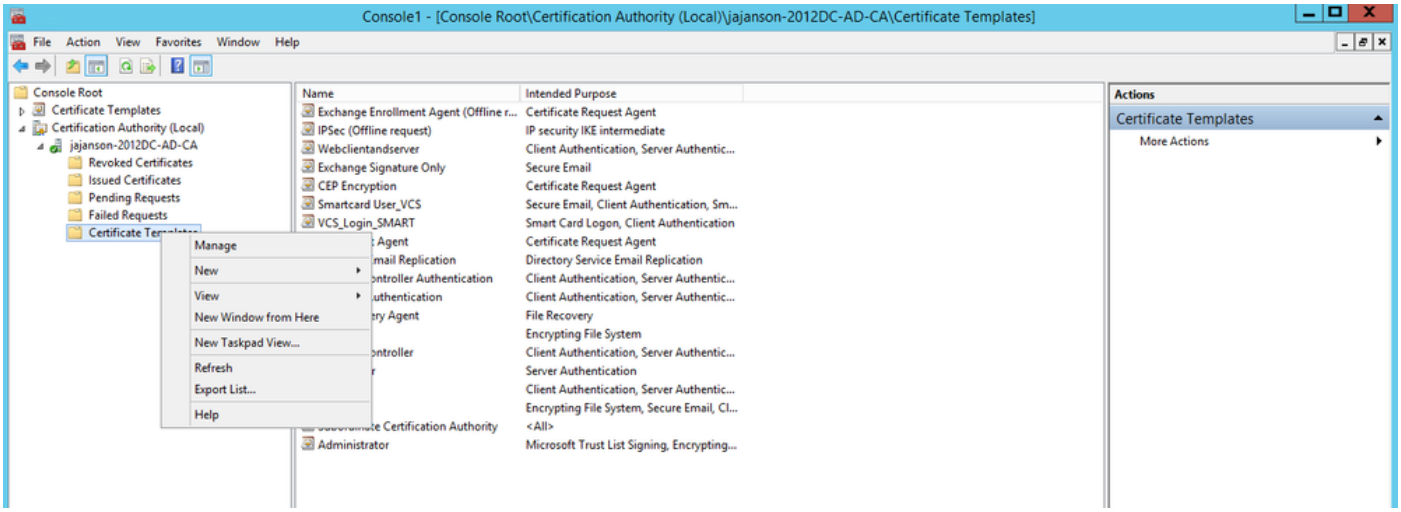
9. انقر فوق **موافق** لإنهاء تغييراتك وإنشاء القالب الجديد. يجب أن يظهر القالب الجديد الآن في قائمة "قوالب الشهادات".




القالب الذي تمت مشاهدته في التحكم بالمجال

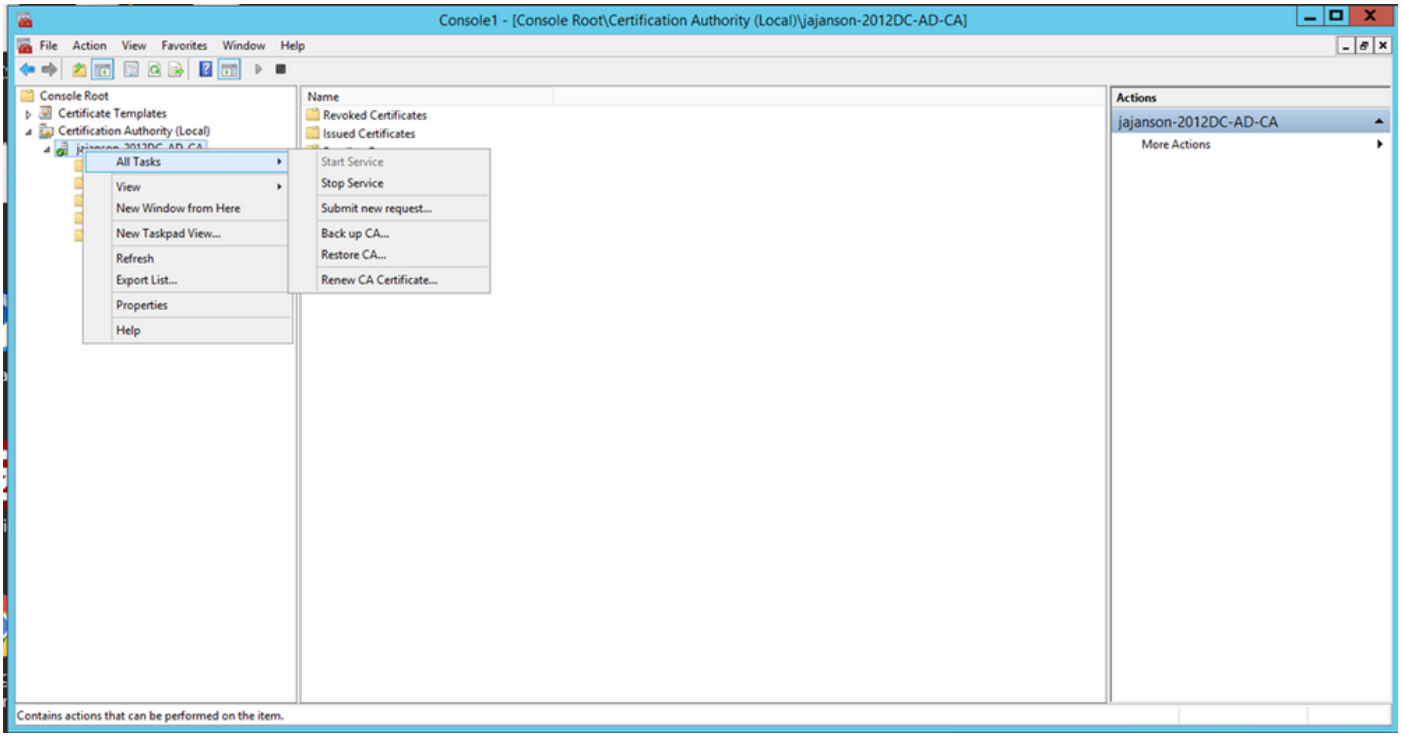
10. في الجزء الأيسر من MMC، قم بتوسيع المرجع المصدق (المحلي)، ثم قم بتوسيع المرجع المصدق الخاص بك ضمن قائمة المرجع المصدق.

انقر بزر الماوس الأيمن فوق "قوالب الشهادات"، ثم انقر فوق **"جديد"** ثم انقر فوق **قالب الشهادة** لإصداره. ثم أختر قالب البطاقة الذكية الذي تم إنشاؤه حديثا.




إصدار قالب جديد

11. بعد النسخ المتماثل للقالب، في MMC، انقر بزر الماوس الأيمن أو حدد قائمة المرجع المصدق، وانقر فوق **جميع المهام**، ثم انقر فوق **إيقاف الخدمة**. ثم انقر بزر الماوس الأيمن فوق اسم المرجع المصدق مرة أخرى، وانقر فوق **جميع المهام**، ثم انقر فوق **بدء الخدمة**.

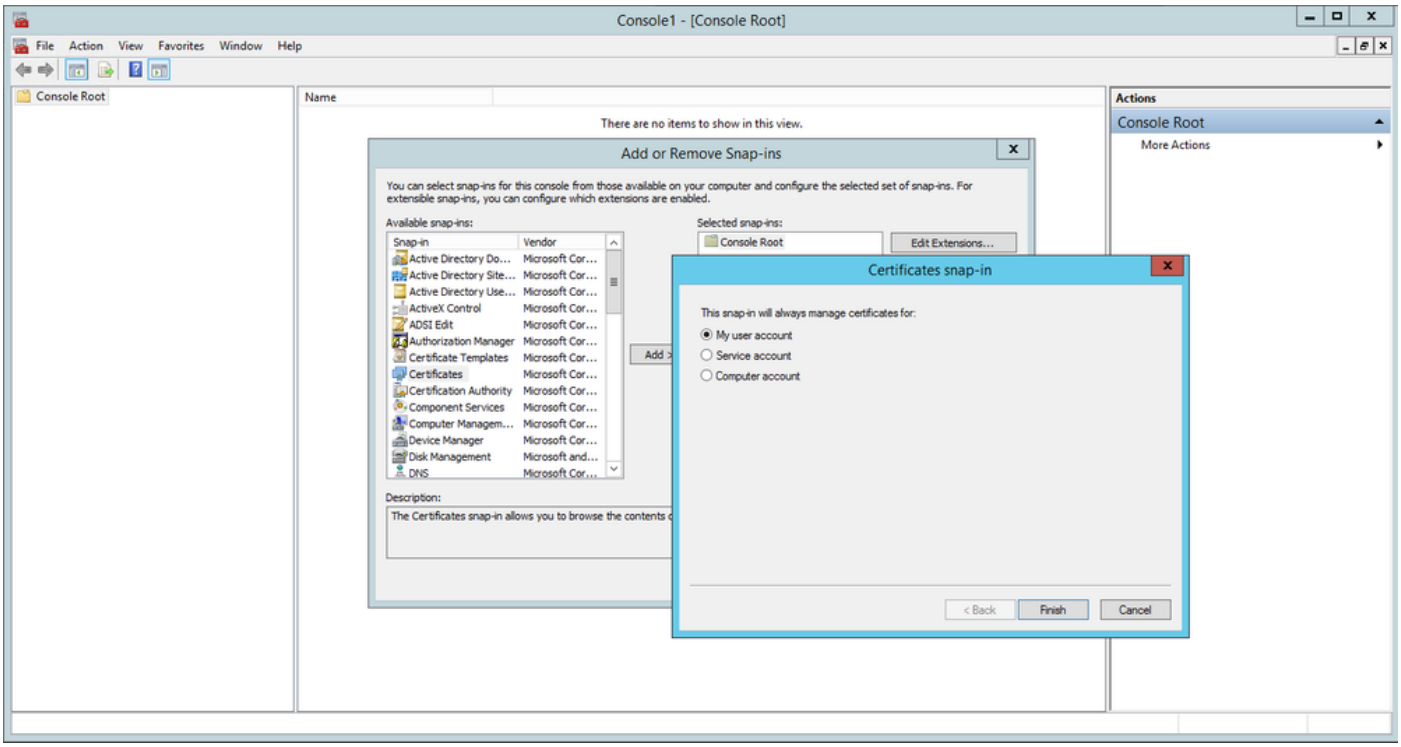



التوقف ثم بدء تشغيل خدمات الشهادات

### التسجيل في شهادة وكيل التسجيل

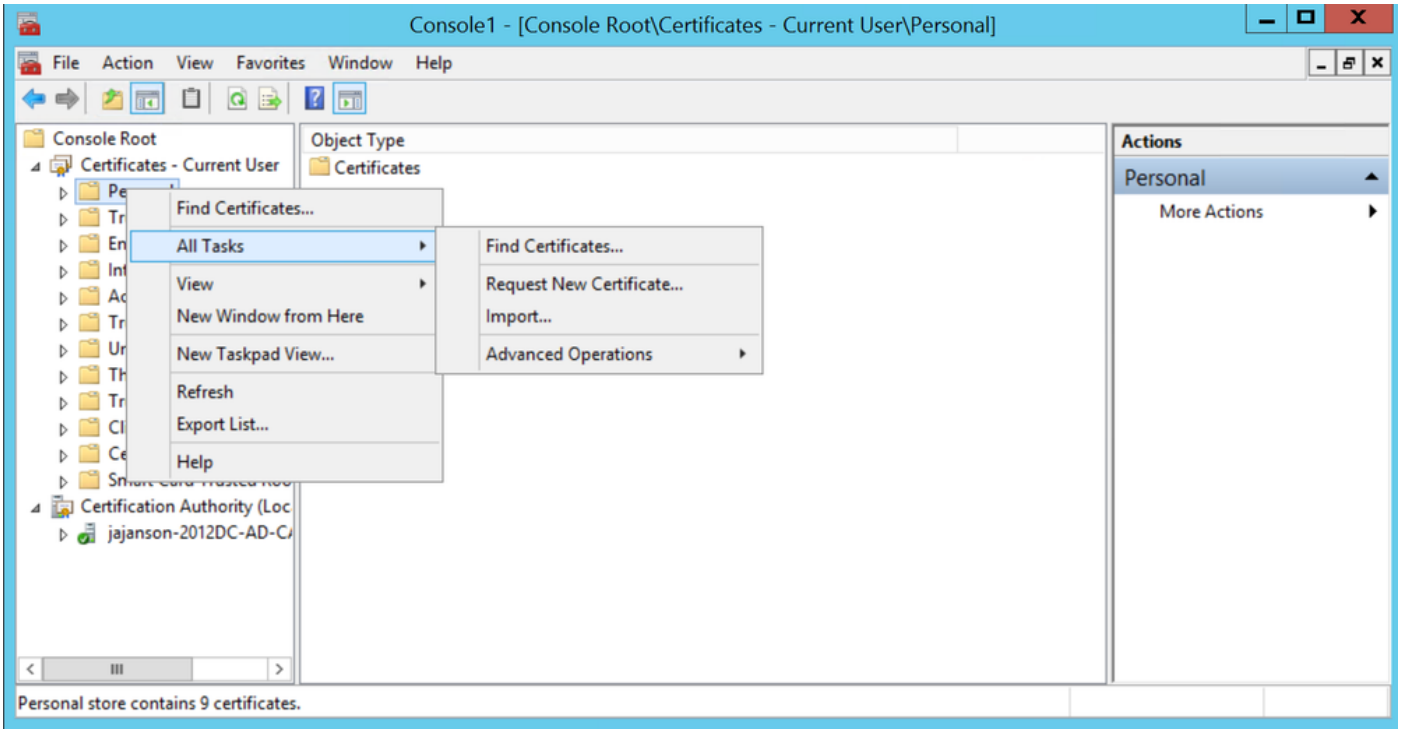
ومن المستحسن القيام بذلك على جهاز عميل (سطح مكتب مسئولي تقنية المعلومات).

1. تشغيل MMC أختر **شهادات**، انقر فوق **إضافة** ثم شهادات **لحساب المستخدم الخاص بي**.



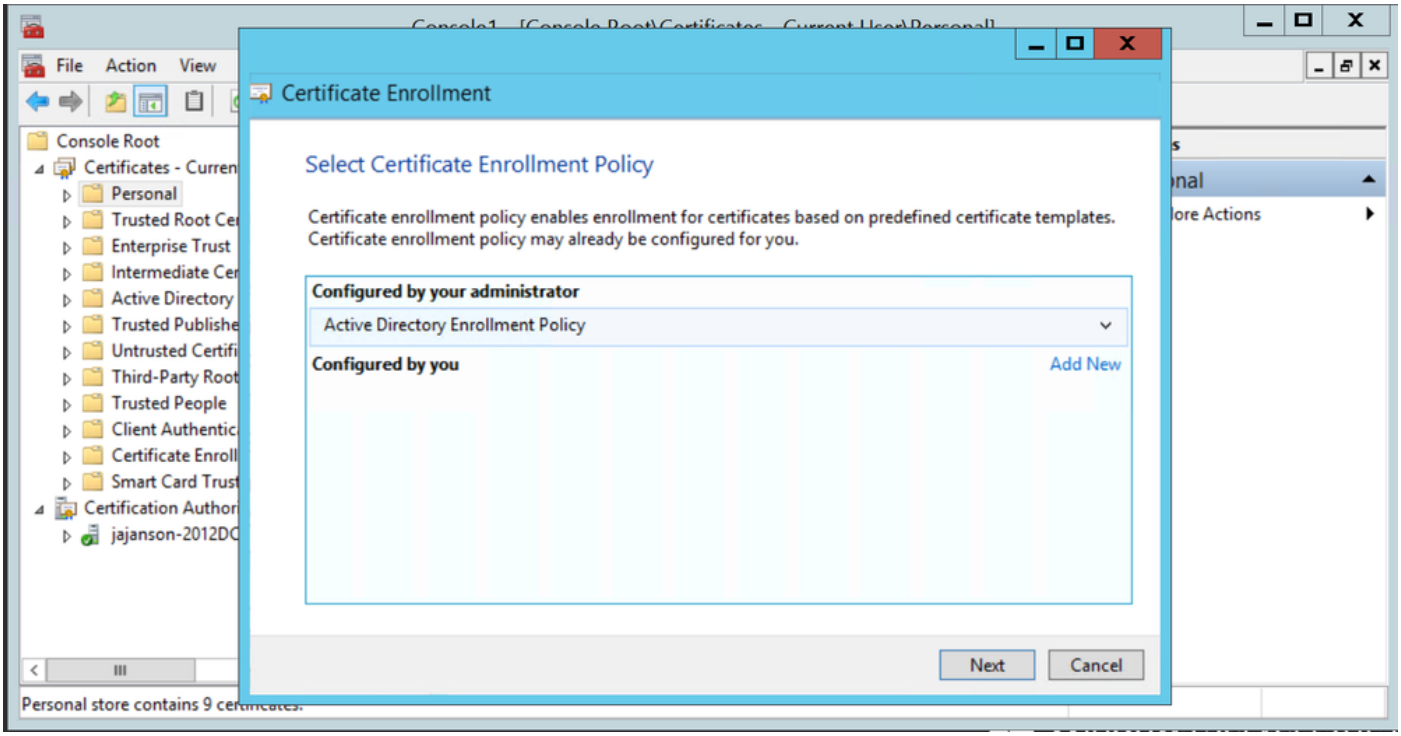

إضافة شهادات

2. انقر بزر الماوس الأيمن أو حدد **العقدة الشخصية**، وحدد **كافة المهام** ثم حدد **طلب شهادة جديدة**.



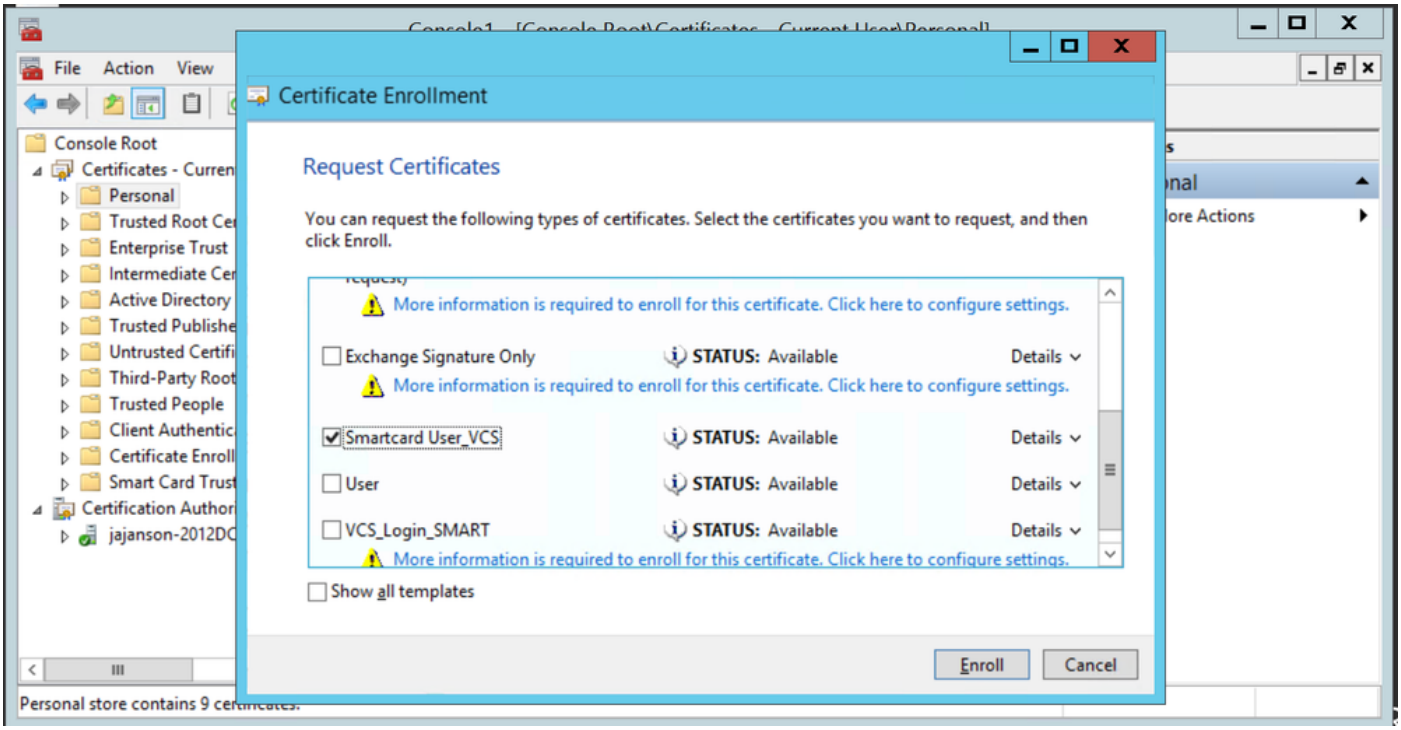

طلب شهادات جديدة

3. انقر فوق **التالي** في المعالج، ثم حدد **نهج تسجيل Active Directory**. ثم انقر فوق **التالي** مرة أخرى.




تسجيل Active Directory

4. حدد **شهادة وكيل التسجيل**، في هذه الحالة، **SmartCard User_VCS** ثم انقر فوق **تسجيل**.

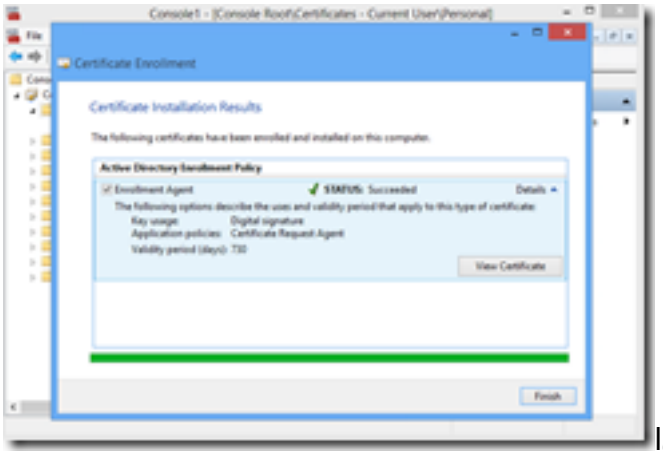



وكيل شهادة التسجيل

تم إعداد سطح المكتب لمسؤولي تقنية المعلومات لديك الآن كمحطة تسجيل، وهذا يتيح لك تسجيل بطاقات ذكية جديدة نيابة عن المستخدمين الآخرين.

## التسجيل نيابة عن...

لكي تتمكن الآن من تزويد الموظفين ببطاقات ذكية للمصادقة، يجب تسجيلهم وإنشاء الشهادة التي يتم إستيرادها بعد ذلك إلى البطاقة الذكية.

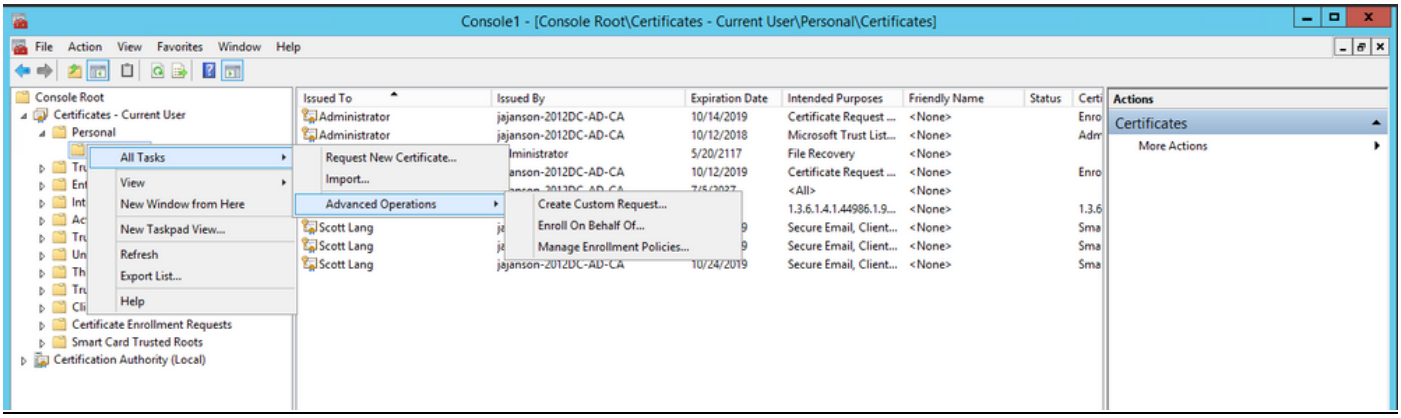


التسجيل نيابة عن

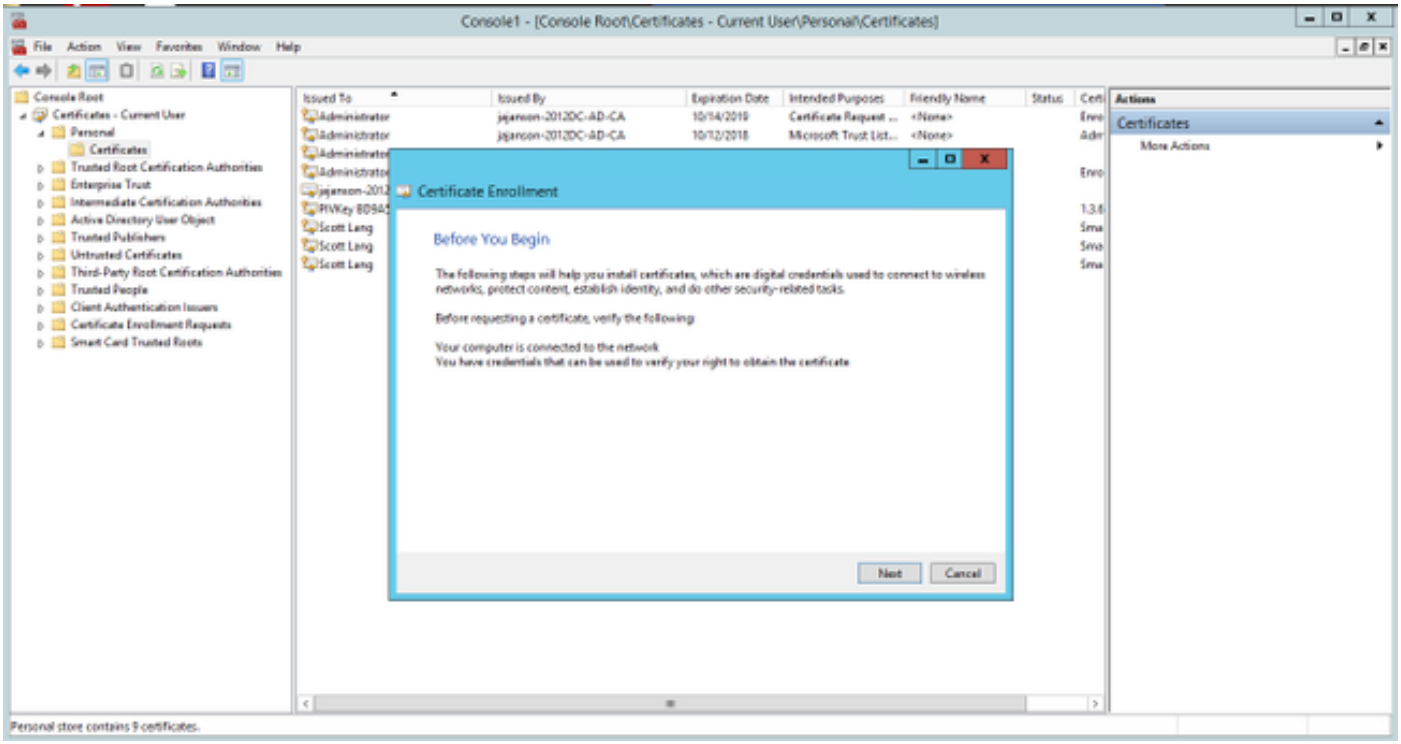
1. قم بتشغيل MMC واستيراد **Certificates Module & Manger** Certificates for My User Account.

2. انقر بزر الماوس الأيمن فوق أو حدد **شخصي > شهادات** وحدد **كافة المهام > العمليات المتقدمة** وانقر فوق **التسجيل بالنيابة عن...**

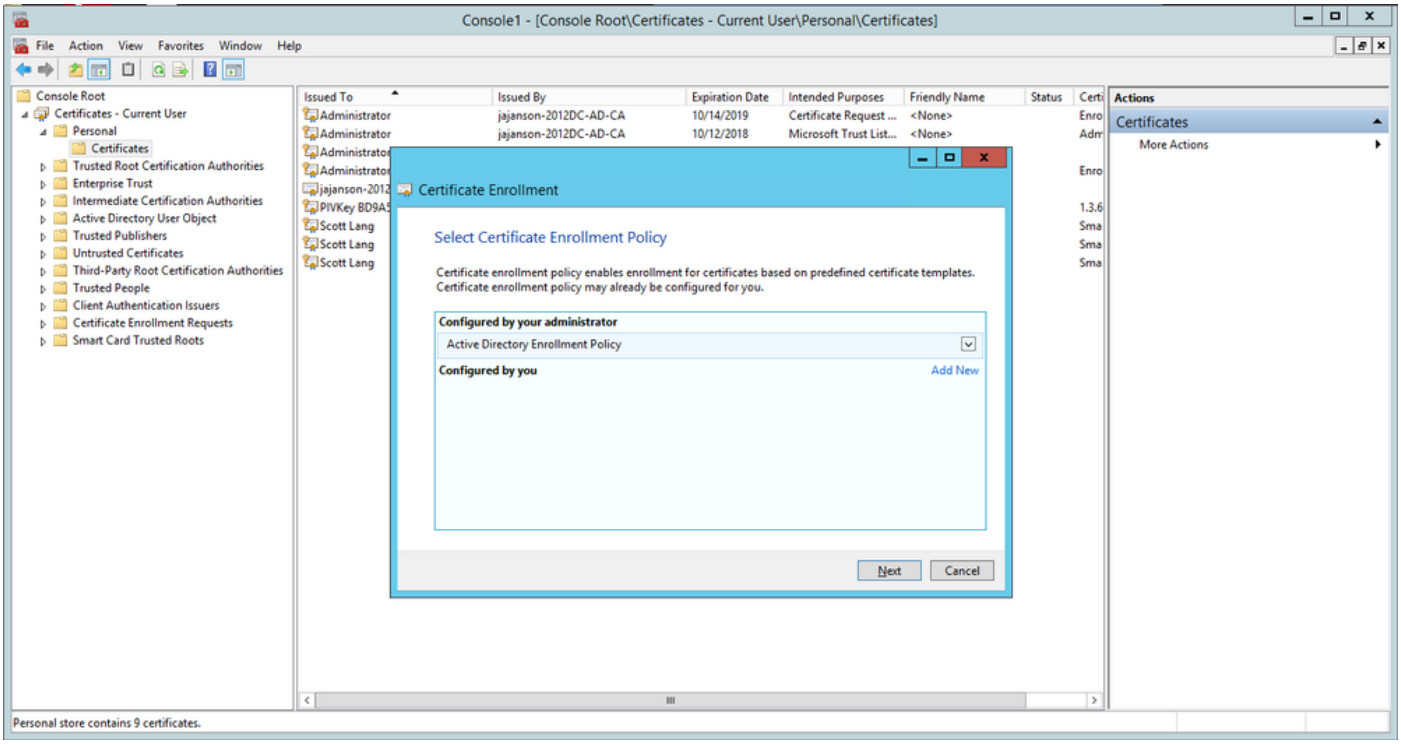
3. في المعالج، واختر نهج تسجيل Active Directory ثم انقر فوق **التالي**.




التسجيل بالنيابة متقدم

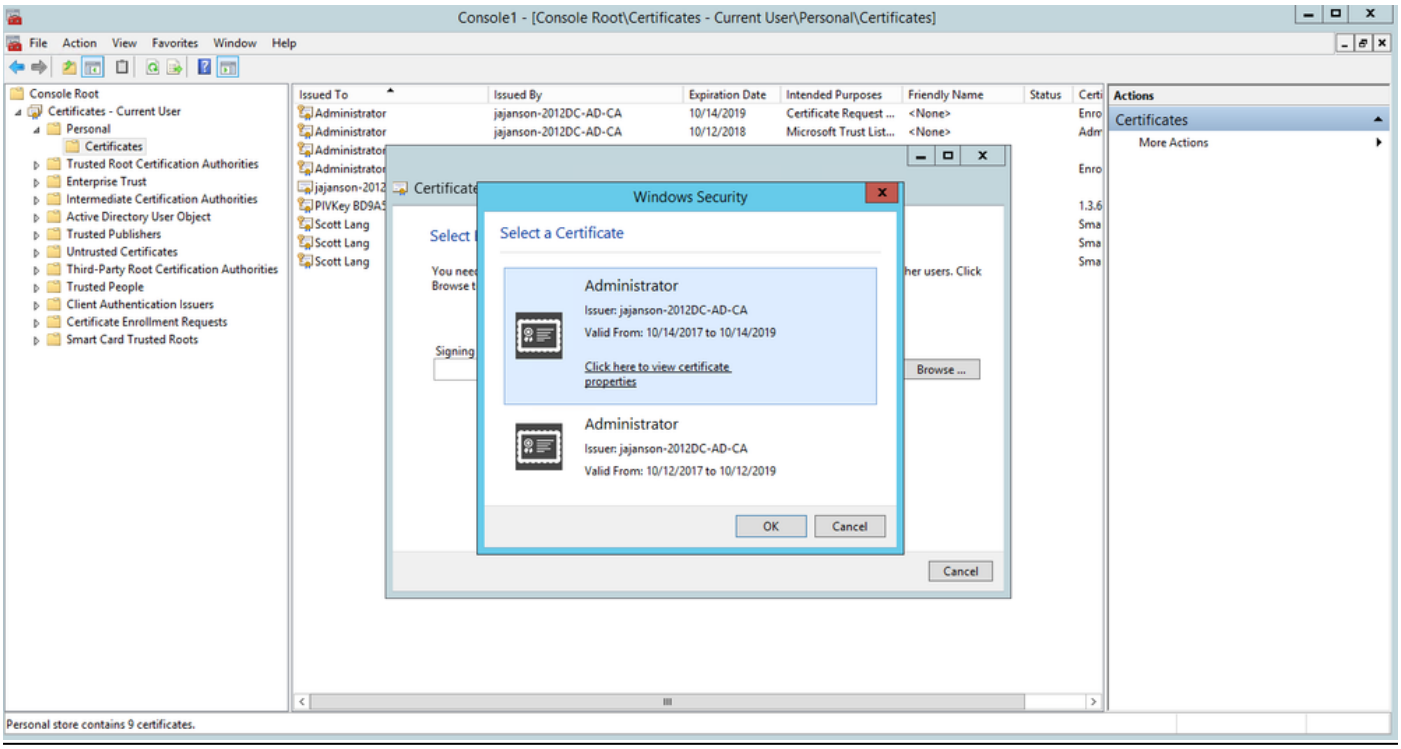



4. حدد نهج تسجيل الشهادة ثم انقر فوق **التالي**.



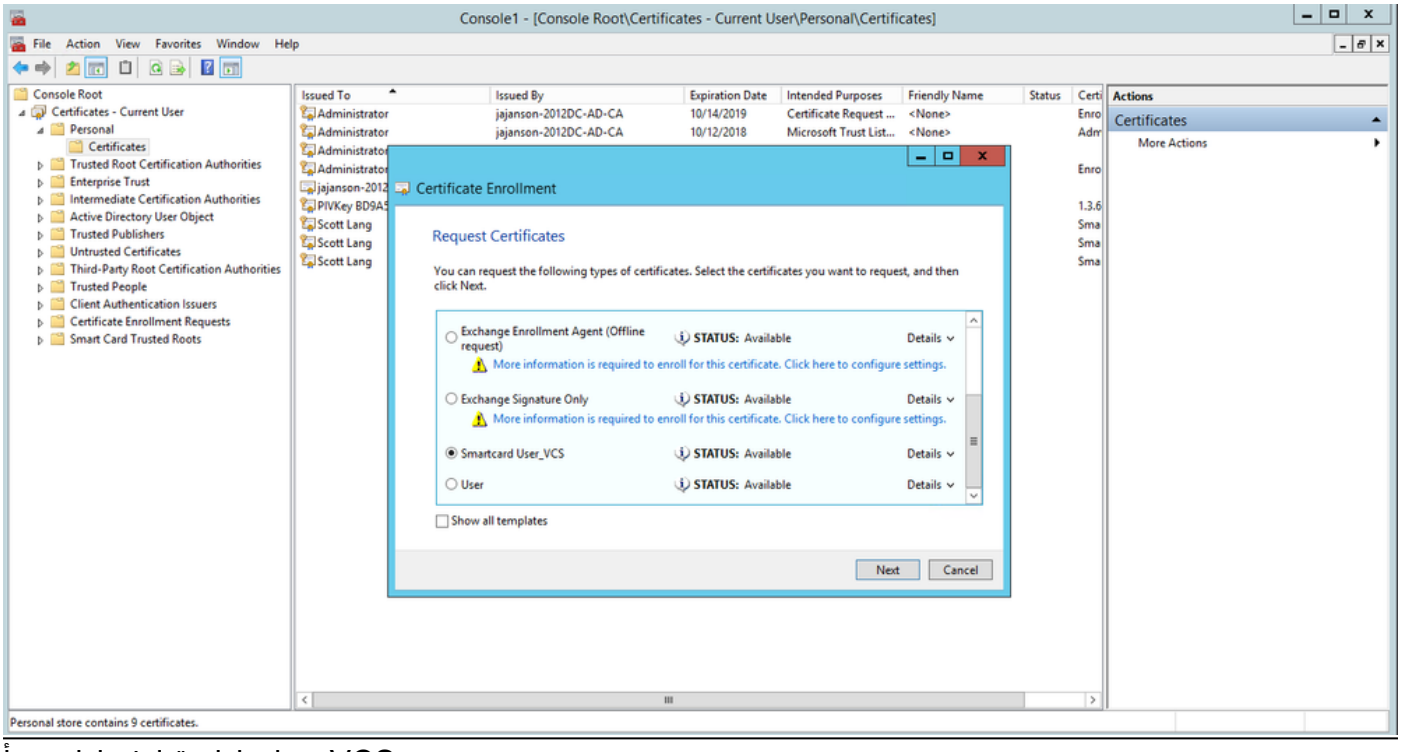

سياسة التسجيل

5. يطلب منك الآن تحديد **شهادة التوقيع**. هذه هي شهادة التسجيل التي طلبتها مسبقا.



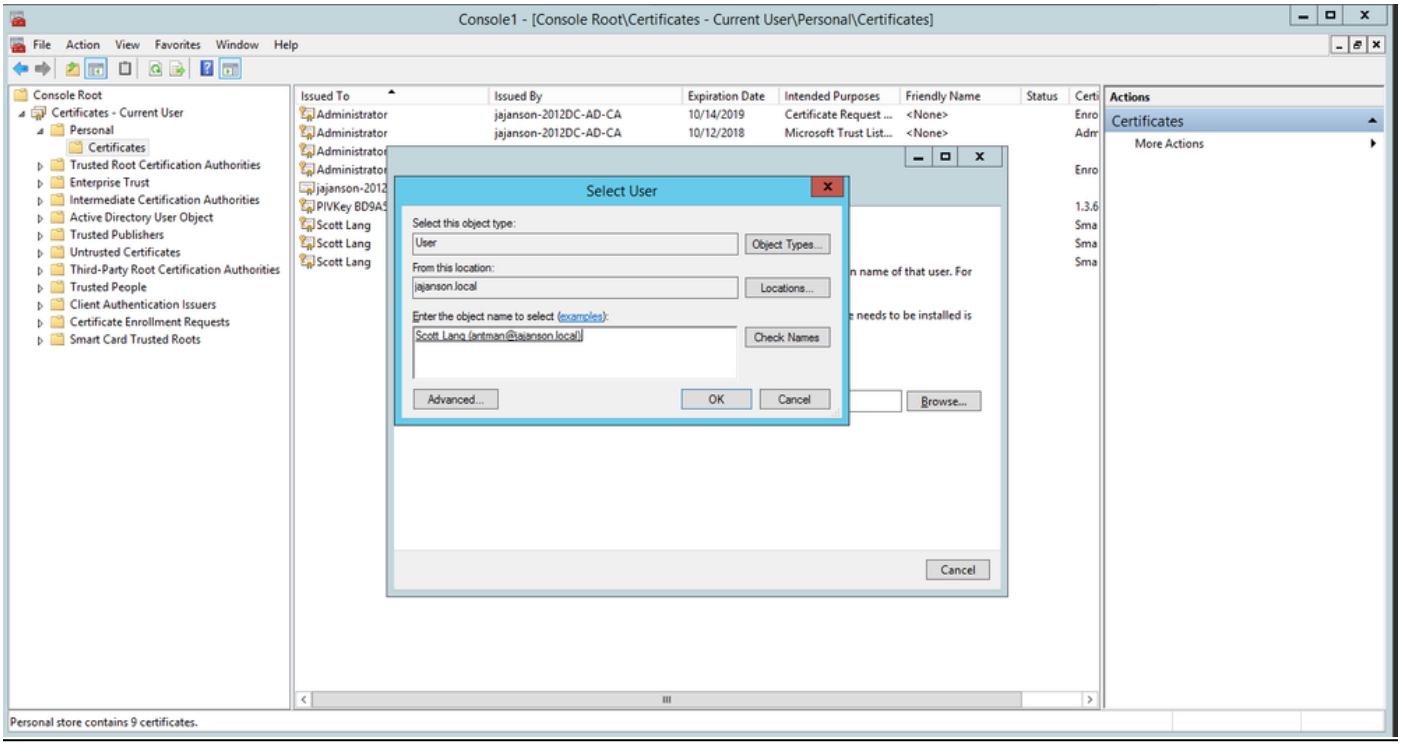

تحديد شهادة التوقيع

6. في الشاشة التالية، تحتاج إلى الاستعراض للوصول إلى الشهادة التي ترغب في طلبها، وفي هذه الحالة، فإن **SmartCard User_VCS** هو القالب الذي أنشأته مسبقا.



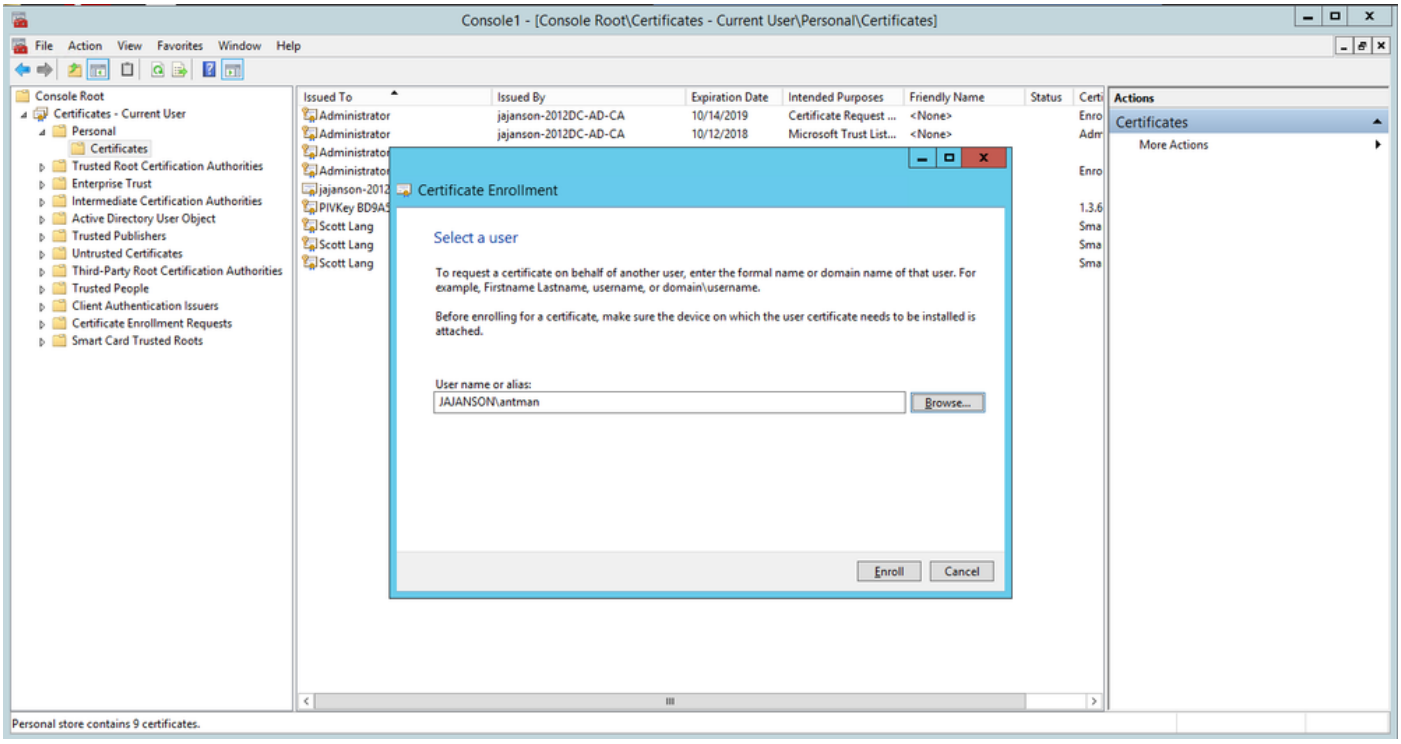

أختر البطاقة الذكية VCS

7. بعد ذلك، تحتاج إلى تحديد المستخدم الذي ترغب في التسجيل نيابة عنه. انقر فوق **استعراض** واكتب اسم المستخدم الخاص بالموظف الذي ترغب في التسجيل. في هذه الحالة، سكوت لانغ يستخدم 'antman@jajanson.local account'.



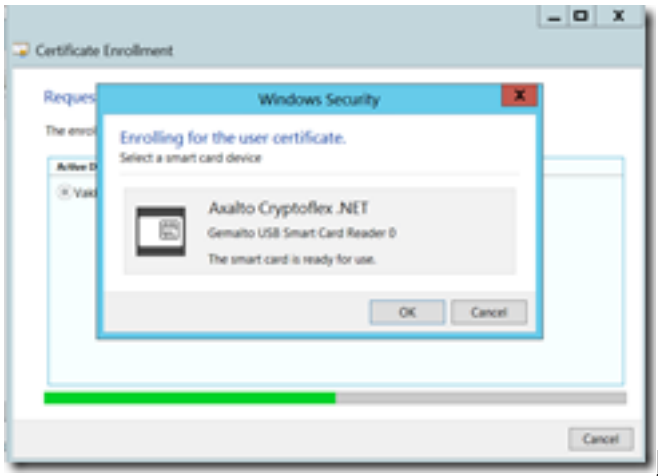

إختيار المستخدم

8. في الشاشة التالية، استمر في التسجيل بالنقر فوق **تسجيل الدخول**. الآن، قم بإدراج بطاقة ذكية في القارئ الخاص بك.



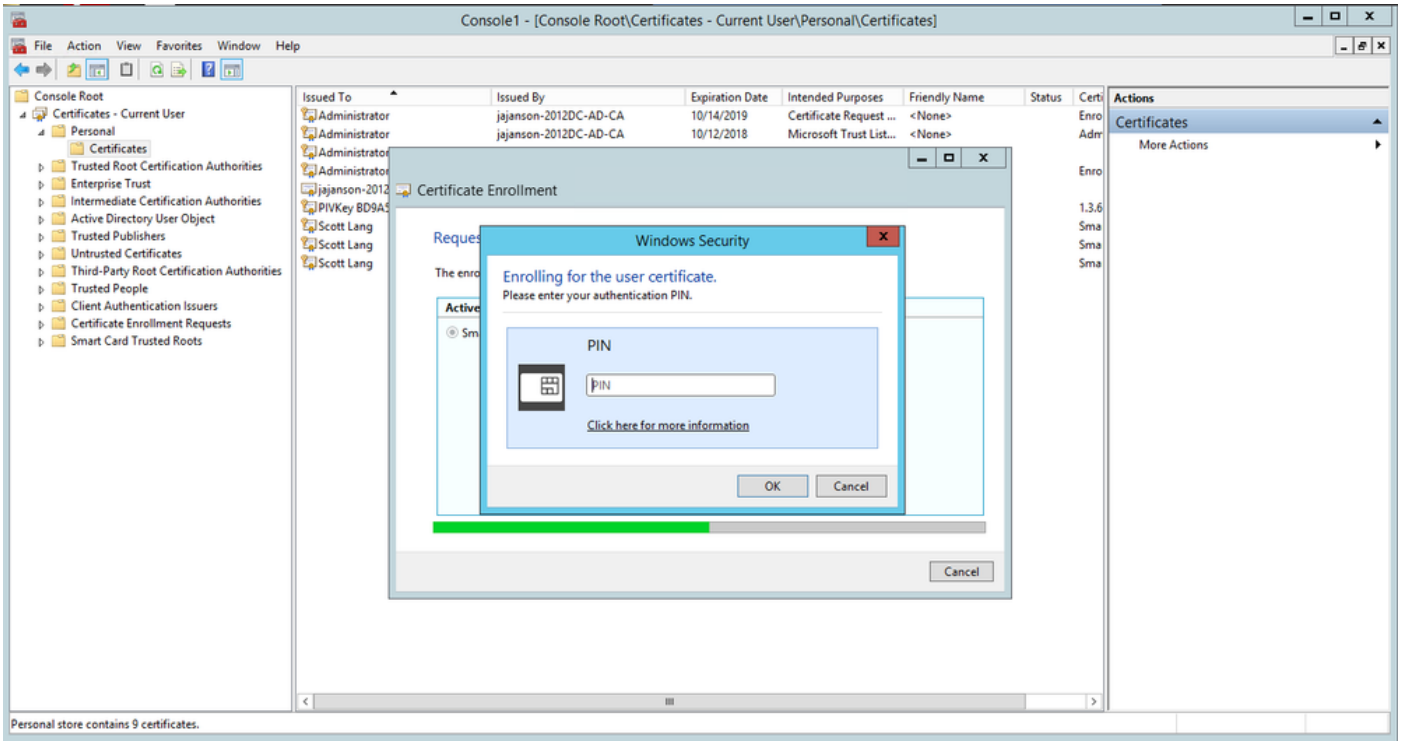

تدويان

9. بمجرد إدخال البطاقة الذكية، يتم الكشف عنها كما يلي:



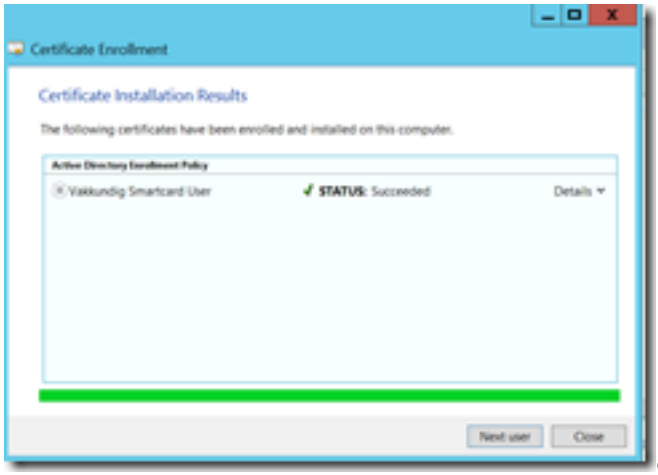

إدراج البطاقة الذكية

10. يطلب منك بعد ذلك كتابة رقم PIN الخاص بالبطاقة الذكية (رقم التعريف الشخصي الافتراضي: 0000).




أدخل رمز PIN

11. أخيرا، بمجرد أن ترى شاشة **نجاح التسجيل**، يمكنك بعد ذلك إستخدام هذه البطاقة الذكية لتسجيل الدخول إلى خادم متصل بالمجال، مثل VCS مع البطاقة فقط ورقم تعريف شخصي معروف. ومع ذلك، لم يتم ذلك نعم، مازلت بحاجة إلى إعداد VCS لإعادة توجيه طلبات المصادقة إلى البطاقة الذكية واستخدام بطاقة الوصول المشترك لإصدار شهادة البطاقة الذكية المخزنة على البطاقة الذكية للمصادقة.



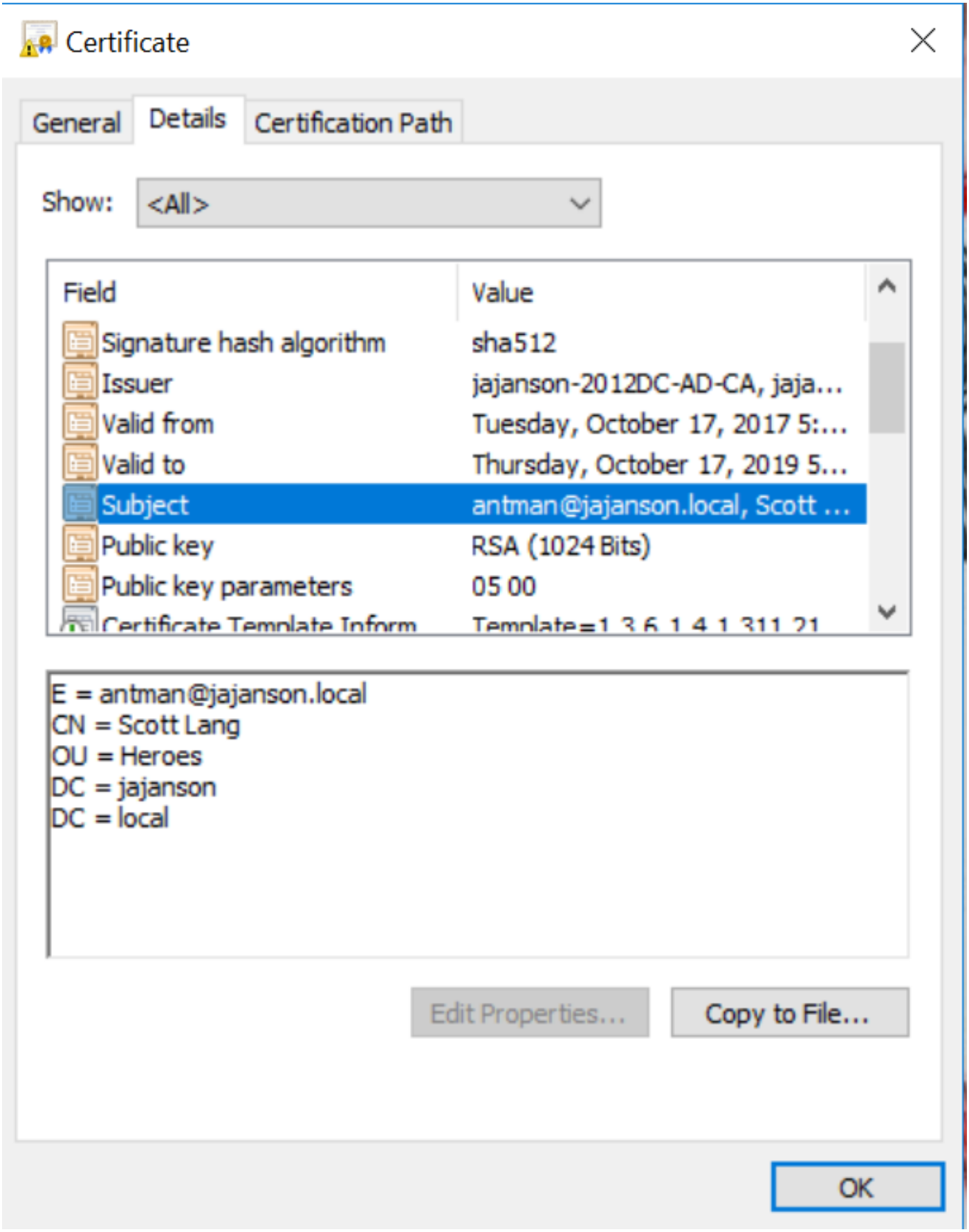

تم التسجيل بنجاح

## تكوين VCS لبطاقة الوصول المشترك

قم بتحميل المرجع المصدق الجذر إلى قائمة شهادات المرجع المصدق ثقة في VCS بالانتقال إلى **الصيانة > التأمين > شهادة المرجع المصدق الثقة.**

2. تحميل قائمة إلغاء الشهادة الموقعة من قبل المرجع المصدق الرئيسي إلى VCS. انتقل إلى **الصيانة > الأمان > إدارة CRL.**

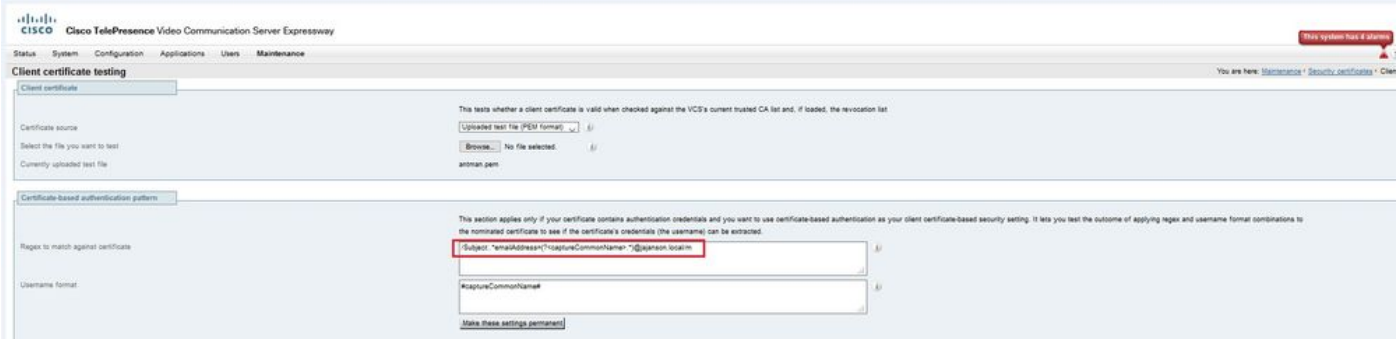
3. قم باختبار شهادة العميل الخاصة بك مقابل السجل الخاص بك الذي يسحب اسم المستخدم من الشهادة لاستخدامها للمصادقة مقابل LDAP أو المستخدم المحلي. سيتم مطابقة regex مع **موضوع** الشهادة. يمكن أن تكون هذه الشبكة الخاصة بك أو بريدك الإلكتروني أو ما إلى ذلك. في هذا المعمل، تم إستخدام البريد الإلكتروني المطلوب مطابقته مقابل شهادة العميل لشهادة العميل.



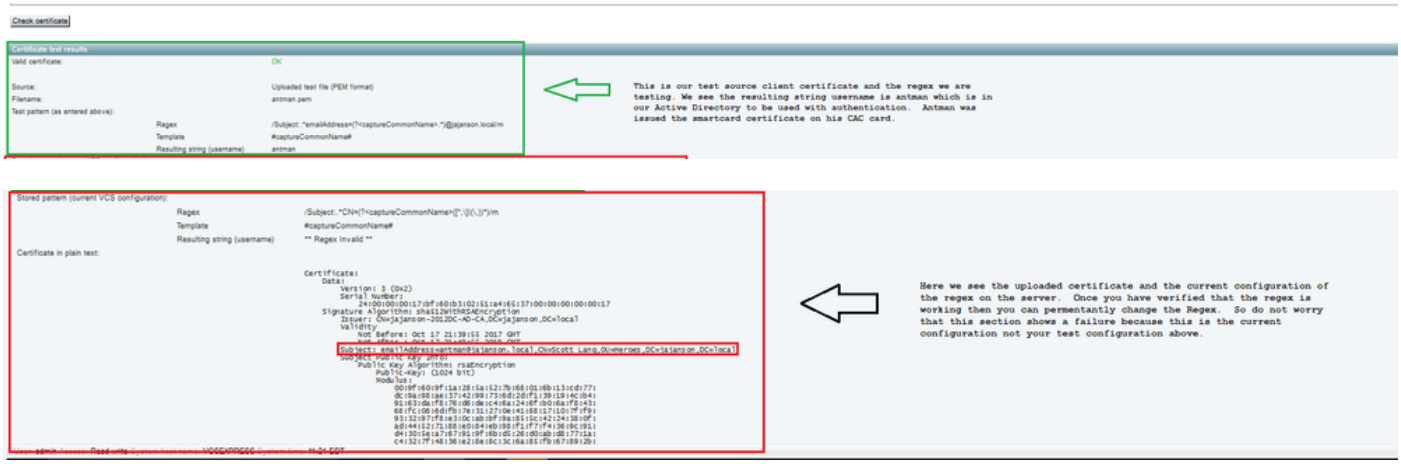

موضوع شهادة العميل

4. انتقل إلى **الصيانة > التأمين > إختبار شهادة العميل**. حدد شهادة العميل المطلوب إختبارها، كانت في مختبري antman.pem، قم بتحميلها إلى منطقة الاختبار. في قسم **نماذج المصادقة المستندة إلى الشهادة** تحت **Regex لمطابقة الترخيص** الصق regex الخاص بك ليتم إختباره. لا تقم بتغيير حقل **تنسيق اسم المستخدم**.

```
My Regex:  /Subject:.*emailAddress=(?.*)@jajanson.local/m
```



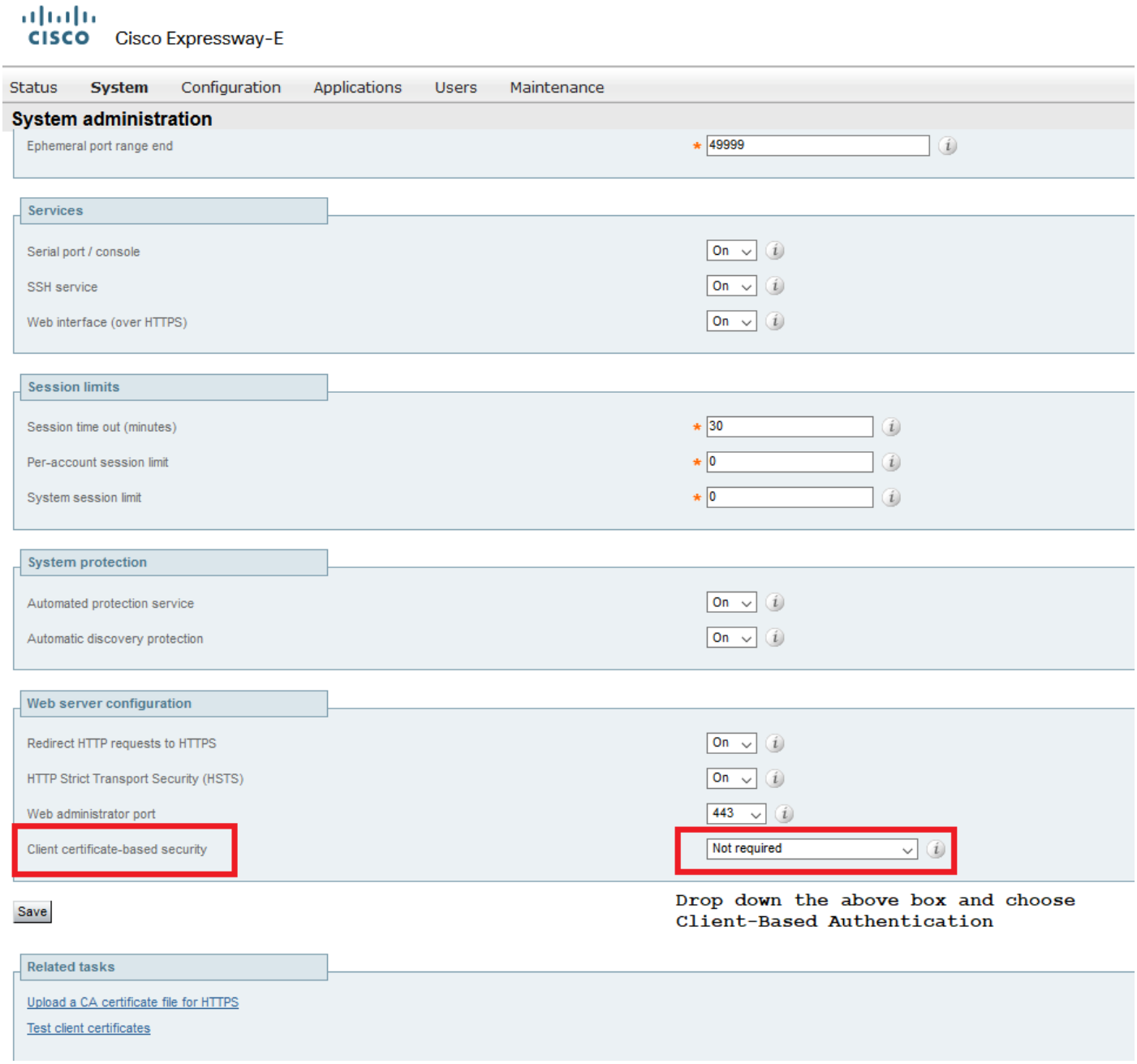

اختبر رقبتك في VCS




نتائج الاختبار

5. إذا كان الاختبار يوفر لك النتائج المطلوبة، ثم يمكنك النقر فوق الزر **أجعل هذه التغييرات دائمة**. يؤدي هذا إلى تغيير regex الخاص بك **لتكوين المصادقة المستندة إلى الشهادة** للخادم. للتحقق من التغيير، انتقل إلى هذا التكوين، **صيانة > تأمين > تكوين مصادقة مستند إلى شهادة.**

6. قم بتمكين المصادقة المستندة إلى العميل من خلال الانتقال إلى **النظام > المؤول** ثم انقر على المربع المنسدل أو حدده لاختيار **الأمان المستند إلى شهادة العميل = المصادقة المستندة إلى العميل.** باستخدام هذا الإعداد، يقوم المستخدم بكتابة FQDN الخاص بخادم VCS في المستعرض الخاص به ويتم مطالبته باختيار حساب العميل الخاص به وإدخال رقم التعريف الشخصي (PIN) المعين لبطاقة الوصول المشتركة الخاصة به. بعد ذلك يتم إصدار الشهادة ويعاد إلى واجهة المستخدم الرسومية (GUI) الخاصة بالويب الخاصة بخادم VCS وكل ما عليه القيام به هو النقر فوق الزر "مؤول" أو تحديده. ثم يتم إدخاله إلى الخادم. في حالة تحديد خيارات **الأمان المستند إلى شهادة العميل = التحقق من الصحة المستند إلى العميل**، تكون العملية هي نفسها مع الاستثناء عند نقر المستخدم فوق زر "المؤول"، يكون قد قام بالمطالبة مرة أخرى بكلمة مرور المؤول. وعادة، لا يكون هذا الأخير ما تحاول المنظمة تحقيقه من خلال اتفاقية مكافحة الفساد.




تمكين المصادقة المستندة إلى العميل

النجدة! أنا محبوس!!!

إذا قمت بتمكين المصادقة المستندة إلى العميل ورفض VCS الشهادة لأي سبب كان، فلن تتمكن من تسجيل الدخول باستخدام واجهة المستخدم الرسومية (GUI) للويب بالطريقة التقليدية بعد الآن. ولكن، لا تقلق من وجود طريقة للعودة إلى نظامك. يمكن العثور على المستند المرفق على موقع Cisco على الويب ويقدم معلومات حول كيفية تعطيل المصادقة المستندة إلى العميل من الوصول الجذري.

# التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

# استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).