إصدار شهادة Unified Mobility Feature Server مع ASA

المحتويات

المقدمة

يوضح هذا المستند كيفية تبادل الشهادات الموقعة ذاتيا بين جهاز الأمان القابل للتكيف (ASA) وخادم ميزة التنقل الموحد (CUMA) من Cisco والعكس بالعكس. كما يشرح كيفية أستكشاف المشكلات الشائعة التي تحدث أثناء إستيراد الشهادات وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- سلسلة ASA 5500 من Cisco
- Cisco Unified Mobility Advantage Server 7

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

أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

سيناريوهات النشر

هناك سيناريوهان لنشر **وكيل TLS** يستخدم بواسطة حل **ميزة التنقل من Cisco**.

ملاحظة: في كلا السيناريوهين، يتصل العملاء من الإنترنت.

1. يعمل جهاز الأمان القابل للتكيف كوكيل لكل من جدار الحماية و TLS.
2. يعمل جهاز الأمان القابل للتكيف كوكيل TLS فقط.

في كلا السيناريوهين، يلزمك تصدير **شهادة خادم Cisco UMA** و**زوج المفاتيح** بتنسيق **PKCS-12** واستيرادها إلى جهاز الأمان القابل للتكيف. يتم إستخدام الشهادة أثناء المصافحة مع عملاء Cisco UMA.

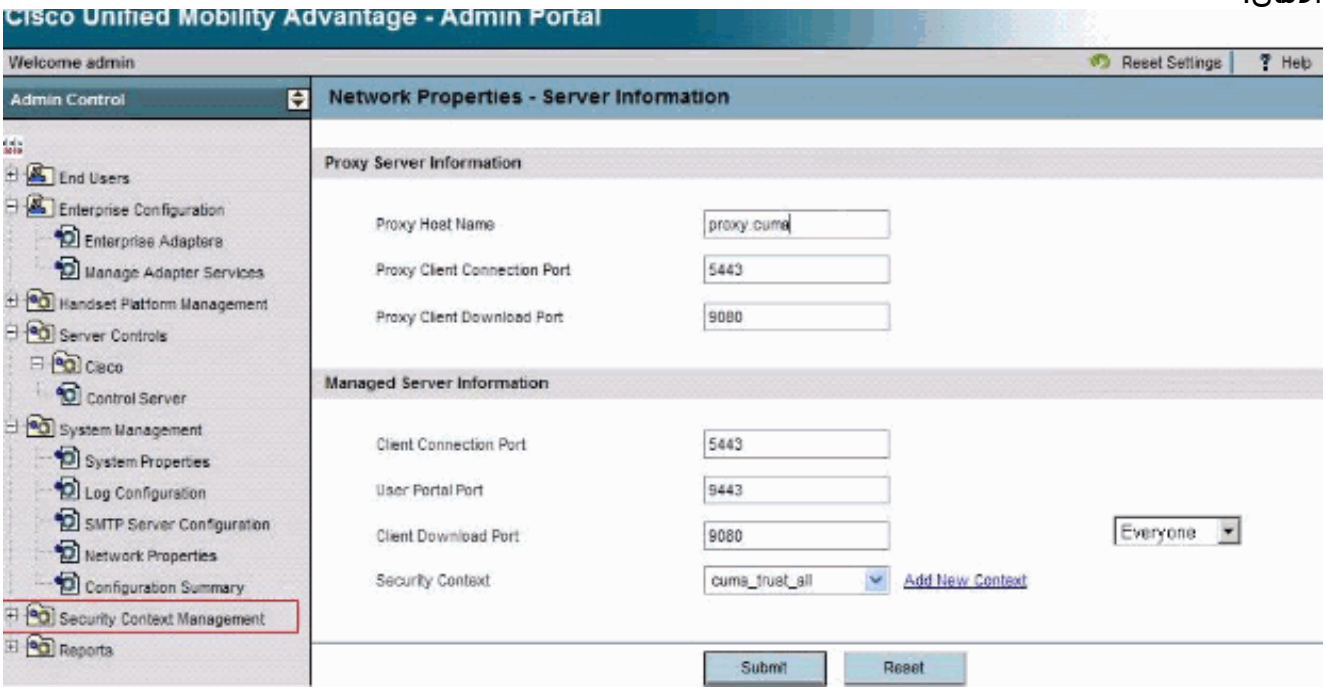
يعد تثبيت الشهادة الموقعة ذاتيا الخاصة بخادم Cisco UMA في متجر TrustedStore الخاص بجهاز الأمان القابل للتكيف أمرا ضروريا لأجهزة الأمان القابلة للتكيف لمصادقة خادم Cisco UMA أثناء المصافحة بين وكيل جهاز الأمان القابل للتكيف وخادم Cisco UMA.

تثبيت شهادة التوقيع الذاتي لخادم Cisco UMA

المهام التي يجب القيام بها على خادم CUMA

يجب تنفيذ هذه الخطوات على خادم CUMA. مع هذه الخطوات، يمكنك إنشاء شهادة موقعة ذاتيا على CUMA للتبادل مع ASA مع CN=portal.aipc.com. يجب تثبيت هذا على مخزن ASA للثقة. أكمل الخطوات التالية:

1. قم بإنشاء فريق موقع ذاتيا على خادم CUMA.قم بتسجيل الدخول إلى مدخل مسؤول ميزة التنقل الموحد من Cisco.أختر **[+]** بجانب إدارة سياق الأمان.



أختر **سياقات التأمين**.أختر **إضافة سياق**.أدخل هذه المعلومات:

```
Do you want to create/upload a new certificate? create
"Context Name "cuma
"Description "cuma
"Trust Policy "Trusted Certificates
"Client Authentication Policy "none
"Client Password "changeme
Server Name cuma.ciscodom.com
"Department Name "vsec
"Company Name "cisco
"City "san jose
"State "ca
"Country "US
```

2. تنزيل الشهادات الموقعة ذاتيا من ميزة التنقل الموحد من Cisco. أتمت هذا steps in order to أنجزت المهمة:أختر **[+]** بجانب إدارة سياق الأمان.أختر **سياقات التأمين**.أختر **إدارة السياق** بجانب سياق الأمان الذي يحمل الشهادة للتنزيل.أختر **تنزيل الشهادة**.**ملاحظة:** إذا كانت الشهادة سلسلة، وكانت لها شهادات جذر أو متوسط مرتبطة بها، فإن الشهادة الأولى فقط هي التي يتم تنزيلها. هذا كاف للشهادات الموقعة ذاتيا.ثم احفظ الملف.
3. تتمثل الخطوة التالية في إضافة الشهادة الموقعة ذاتيا من ميزة التنقل الموحد من Cisco إلى ASA. أتمت هذا steps على ال ASA:افتح الشهادة الموقعة ذاتيا من ميزة التنقل الموحد من Cisco في محرر نصي.قم باستيراد الشهادة إلى مخزن ثقة أجهزة الأمان المعدلة من Cisco:

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
.Enter the base 64 encoded CA certificate
End with the word "quit" on a line by itself

----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. تصدير شهادة ASA موقعة ذاتيا على خادم CUMA. تحتاج إلى تكوين ميزة التنقل الموحد من Cisco لطلب شهادة من جهاز الأمان القابل للتكيف من Cisco. أتمت هذا steps in order to زودت المطلوب توقيع شهادة ذاتيا. يجب تنفيذ هذه الخطوات على ASA.إنشاء زوج مفاتيح جديد:

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024

INFO: The name for the keys will be: asa-id-key

...Keypair generation process begin. Please wait
```

إضافة نقطة ثقة جديدة:

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert

cuma-asa(config-ca-trustpoint)# keypair asa-id-key

cuma-asa(config-ca-trustpoint)# enrollment self
```

تسجيل نقطة الثقة:

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
:The fully-qualified domain name in the certificate will be %
cuma-asa.cisco.com
Include the device serial number in the subject name? [yes/no]: n %
Generate Self-Signed Certificate? [yes/no]: y
```

تصدير الشهادة إلى ملف نصي.

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
:The PEM encoded identity certificate follows

-----BEGIN CERTIFICATE-----

Certificate data omitted
```

```
-----END CERTIFICATE-----
```

5. انسخ المخرجات السابقة إلى ملف نصي وأضفه إلى مخزن ثقة خادم CUMA واستخدم هذا الإجراء:أختر **[+]** بجانب إدارة سياق الأمان.أختر **سياقات التأمين**.أختر **إدارة السياق** بجانب سياق الأمان الذي تقوم باستيراد الشهادة الموقعة إليه.أختر **إدراج** في شريط الشهادات الموثوق بها.لصق نص الشهادة.قم بتسمية الشهادة.أختر **إستيراد**.**ملاحظة:** بالنسبة لتكوين الوجهة البعيدة، اتصل بهاتف المكتب لتحديد ما إذا كان الهاتف الخلوي يرن يرن في نفس الوقت. وهذا من شأنه أن يؤكد أن اتصال الأجهزة المحمولة يعمل وأنه لا توجد مشكلة في تكوين الوجهة البعيدة.

توجد مشكلة في إضافة طلب شهادة CUMA إلى جهات أخرى للشهادات

المشكلة 1

يتم توقيع العديد من عمليات تثبيت النماذج/العروض التوضيحية حيث يساعد إذا كان حل CUC/CUMA يعمل باستخدام شهادات موثوق بها ذاتيا أو يتم الحصول عليها من *هيئات ترخيص أخرى*. شهادات الرصد باهظة الثمن وتحتاج هذه الشهادات لوقت طويل. من الجيد إذا كان الحل يدعم شهادات موقعة ذاتيا وشهادات من مراجع مصدقة أخرى.

الشهادات الحالية المدعومة هي GeoTrust و Verisign. وثقت هذا في cisco بق CSCta62971 id (يسجل زبون فقط)

خطأ: تعذر الاتصال

عندما تحاول الوصول إلى صفحة مدخل المستخدم، على سبيل المثال، `https://<host>:8443`، تظهر رسالة الخطأ .

الحل

وثقت هذا إصدار في cisco بق CSCsm26730 id (يسجل زبون فقط). للوصول إلى صفحة مدخل المستخدم، أكمل هذا الحل البديل:

سبب هذه المشكلة هو حرف الدولار، لذلك افلت من حرف الدولار مع حرف دولار آخر في **ملف server.xml** للخادم المدار. على سبيل المثال، قم بتحرير /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

في السطر: maxSpareThreads="15" **"KeyStorePass="pa$word**

استبدلت `$` حرف ب `$$`. يبدو وكأنه maxSpareThreads="15" **"keyStorePass="pa$$word**.

لا يمكن الوصول إلى بعض الصفحات الموجودة في مدخل إدارة CUMA

يتعذر عرض هذه الصفحات في **مدخل مسؤول CUMA**:

- تنشيط/إلغاء تنشيط المستخدم
- البحث/الصيانة

إذا قام المستخدم بالنقر فوق إحدى الصفحتين المذكورتين أعلاه في القائمة الموجودة على اليسار، فيبدو أن المستعرض يشير إلى أنه يقوم بتحميل صفحة، ولكن لا يحدث شيء (الصفحة السابقة فقط التي كانت في المستعرض مرئية).

الحل

لحل هذه المشكلة المتعلقة بصفحة المستخدم، قم بتغيير المنفذ المستخدم ل Active Directory إلى **3268** وأعد تشغيل CUMA.

معلومات ذات صلة

- تكوين وكيل ASA-CUMA خطوة بخطوة
- المقدمة ASR5000 v1
- ترقية ميزة التنقل الموحد من Cisco
- دعم تقنية الصوت
- دعم منتجات الاتصالات الصوتية والاتصالات الموحّدة
- 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).