تكوين FMC و FTD باستخدام LDAP للمصادقة الخارجية

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين المصادقة الخارجية لبروتوكول الوصول إلى الدليل (LDAP) في الوضع Microsoft Lightweight باستخدام كل من Cisco FMC و FTD.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- مركز إدارة FireSIGHT (FMC) من Cisco
- مايكروسوفت LDAP

المكونات المستخدمة

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

- FTD 6.5.0-123
- FMC 6.5.0-115
- نظام التشغيل Microsoft Server 2012

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

تتضمن FMC والأجهزة المدارة حساب مسؤول افتراضي للوصول إلى الإدارة. يمكنك إضافة حسابات مستخدمين مخصصة على وحدة التحكم في إدارة للوحة الأساسية (FMC) وعلى الأجهزة المدارة، إما كمستخدمين داخليين أو كمستخدمين خارجيين على خادم LDAP أو RADIUS، إذا كان هذا النموذج مدعوما. يتم دعم مصادقة المستخدم الخارجي ل FMC و FTD.

· مستخدم داخلي - يتحقق جهاز FMC/FTD من قاعدة بيانات محلية لمصادقة المستخدم.

· مستخدم خارجي - إذا لم يكن المستخدم موجودا في قاعدة البيانات المحلية، تقوم معلومات النظام من خادم مصادقة LDAP أو RADIUS خارجي بملء قاعدة بيانات المستخدم الخاصة به.

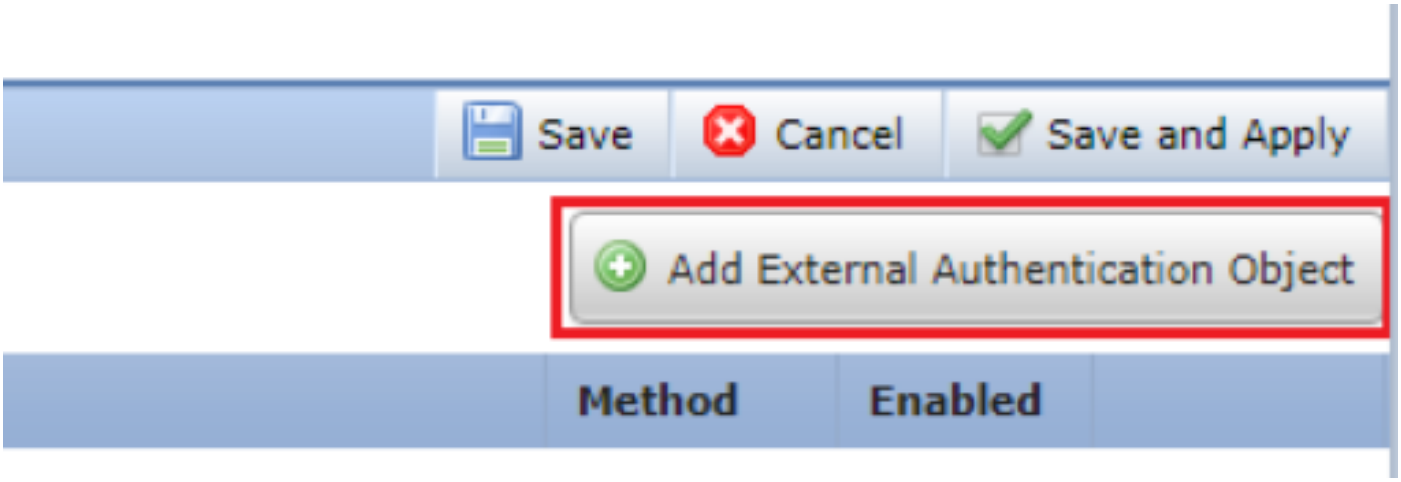
الرسم التخطيطي للشبكة

التكوين

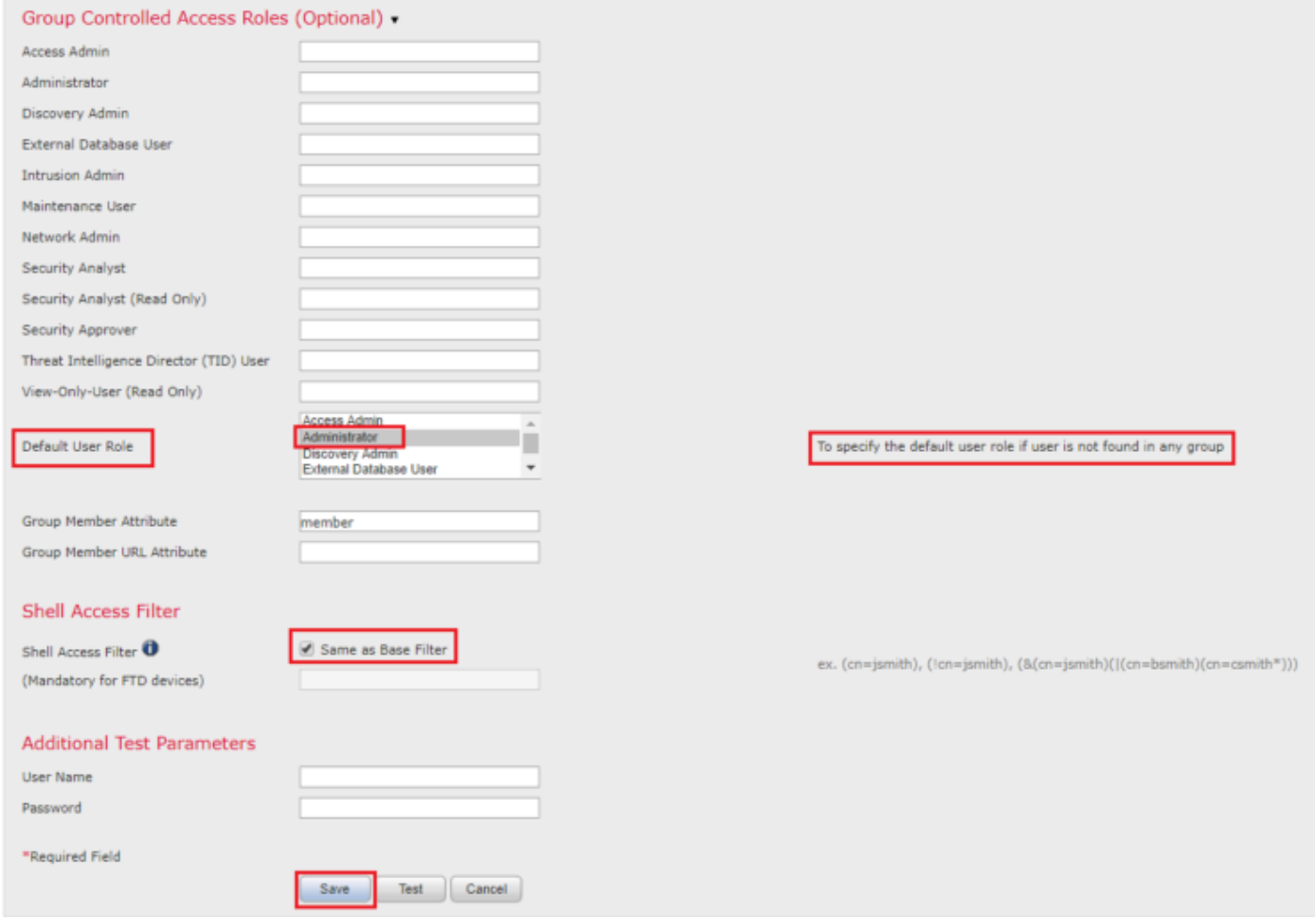
تكوين LDAP الأساسي في واجهة المستخدم الرسومية FMC

الخطوة 1. انتقل إلىSystem > Users > External Authentication:

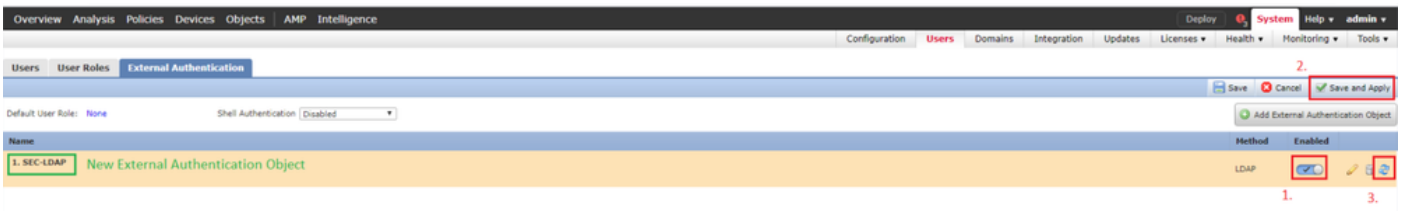
الخطوة 2. أختارAdd External Authentication Object:



الخطوة 3. أكمل الحقول المطلوبة:



الخطوة 4. قم بتمكين External Authenticationالكائن والحفظ:



Shell Access للمستخدمين الخارجيين

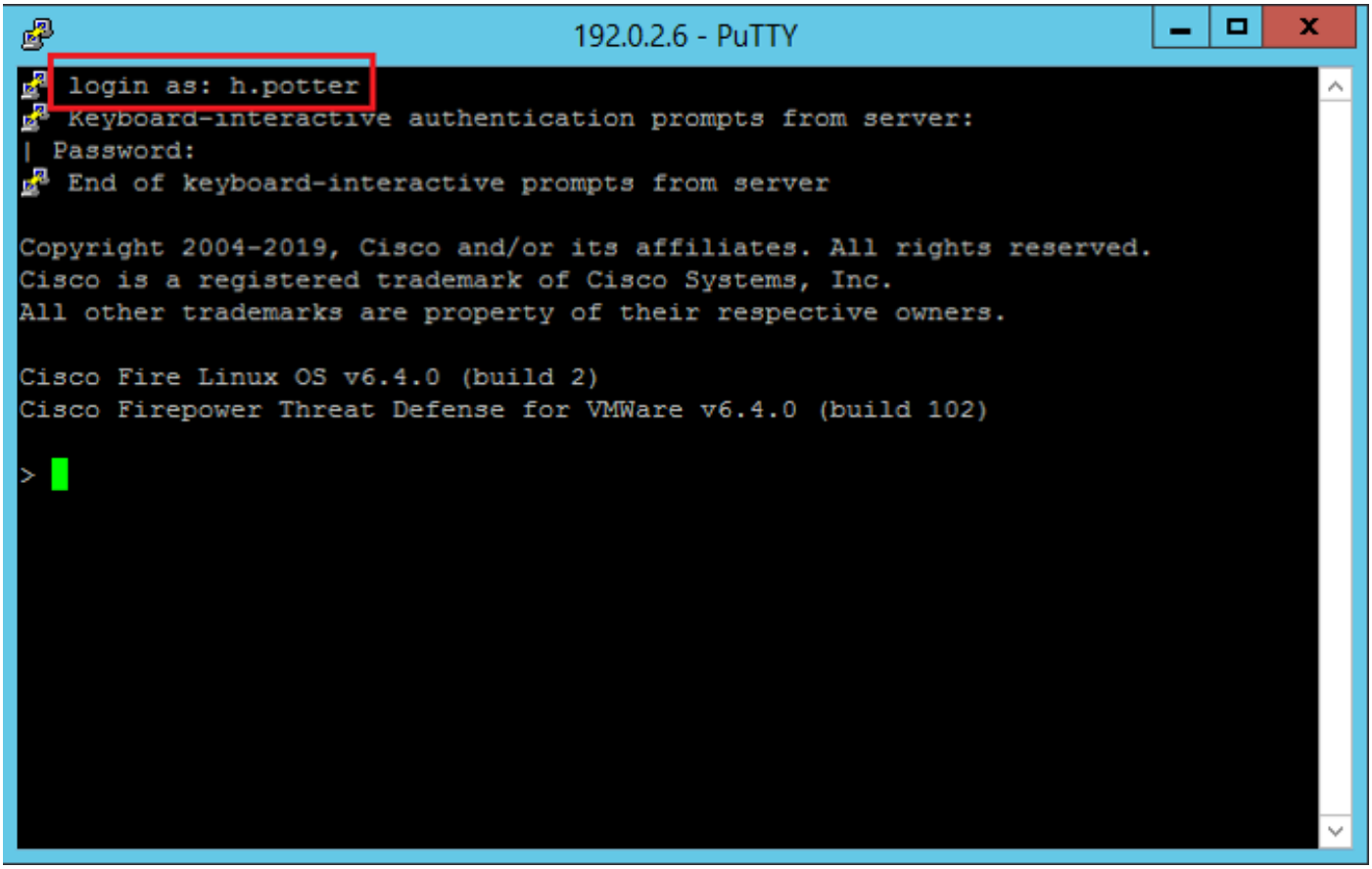
تدعم FMC إثنين من مستخدمي الإدارة الداخلية المختلفة: واحد لواجهة الويب، والآخر وصول واجهة سطر الأوامر. هذا يعني أنه يوجد تمييز واضح بين من يمكنه الوصول إلى واجهة المستخدم الرسومية ومن يمكنه الوصول إلى واجهة سطر الأوامر. في وقت التثبيت، تتم مزامنة كلمة المرور الخاصة بمستخدم المسؤول الافتراضي لكي تكون هي نفسها على كل من واجهة المستخدم الرسومية (GUI) وواجهة سطر الأوامر (CLI)، ومع ذلك، يتم تتبعها بواسطة آليات داخلية مختلفة، ويمكن أن تكون مختلفة في نهاية المطاف.

يجب أيضا منح مستخدمي LDAP الخارجيين حق الوصول إلى shell.

الخطوة 1. انتقل إلىSystem > Users > External AuthenticationالمربعShell Authentication المنسدل وطقطقة كما يظهر في الصورة واحفظ:

الخطوة 2. نشر التغييرات في FMC.

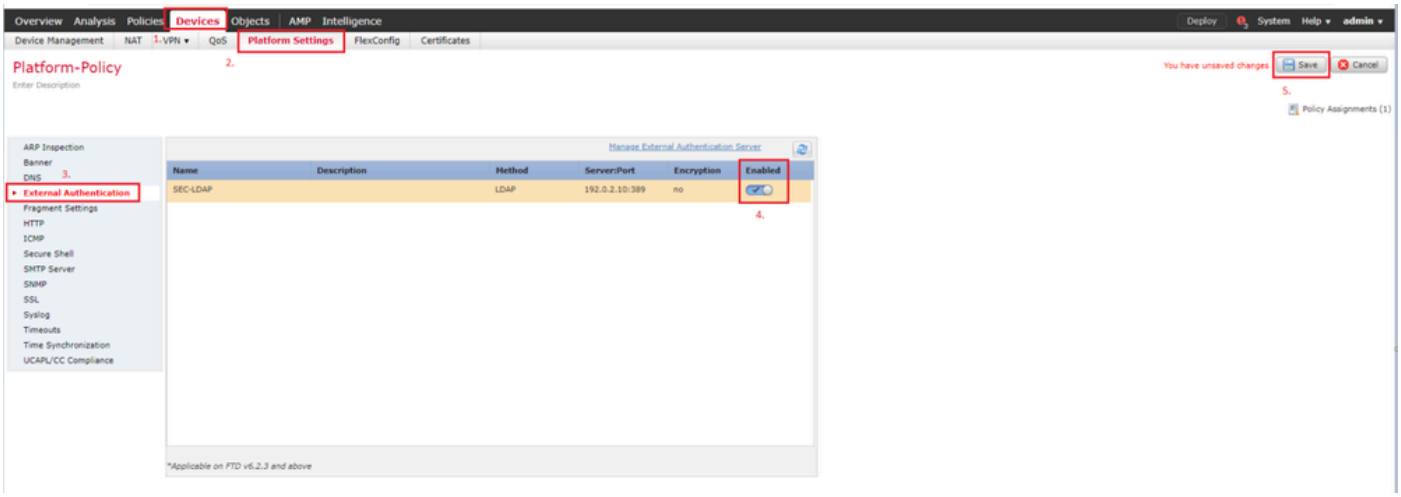
بمجرد تكوين وصول طبقة للمستخدمين الخارجيين، يتم تمكين تسجيل الدخول عبر بروتوكول SSH كما هو موضح في الصورة:



المصادقة الخارجية ل FTD

يمكن تمكين المصادقة الخارجية على FTD.

الخطوة 1. انتقل إلىDevices > Platform Settings > External Authentication. طقطقةEnabledوحفظ:



أدوار المستخدم

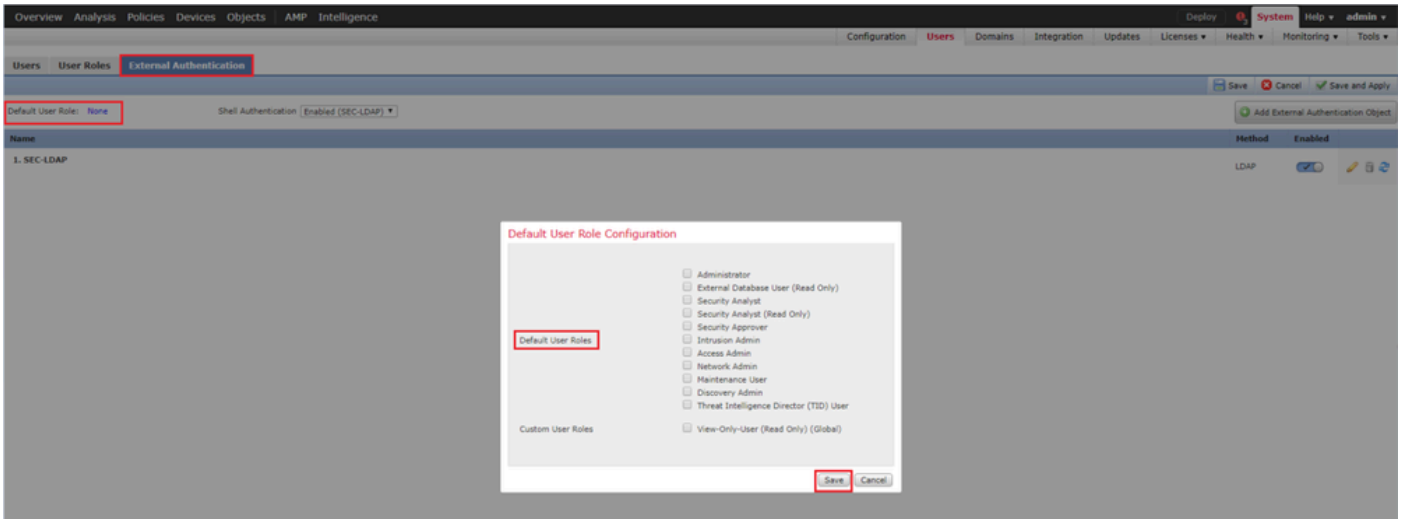
تستند امتيازات المستخدم إلى دور المستخدم المعين. يمكنك أيضا إنشاء أدوار مستخدم مخصصة باستخدام امتيازات الوصول التي تم تخصيصها لتلبية إحتياجات مؤسستك أو يمكنك إستخدام أدوار محددة مسبقا مثل "محلل الأمان" و"مسؤول الاكتشاف".

هناك نوعان من أدوار المستخدم:

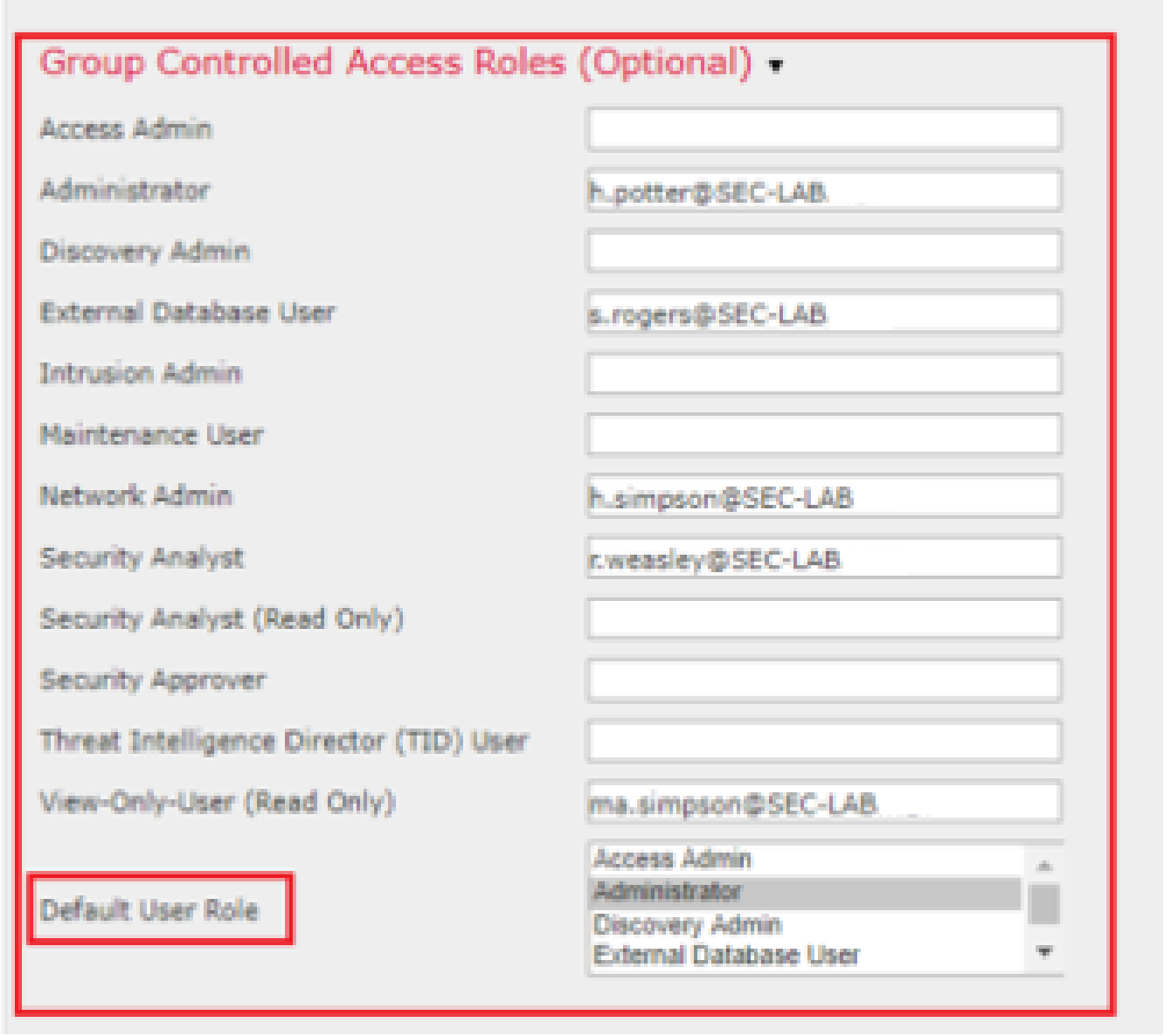
1. أدوار مستخدم واجهة الويب
2. أدوار مستخدمي CLI

للحصول على قائمة كاملة من الأدوار المحددة مسبقا والمزيد من المعلومات، راجع أدوار المستخدم.

لتكوين دور مستخدم افتراضي لجميع كائنات المصادقة الخارجية، انتقل إلىSystem > Users > External Authentication > Default User Role. أختر دور المستخدم الافتراضي الذي ترغب في تعيينه وانقر فوقSave.



لاختيار دور مستخدم افتراضي أو تعيين أدوار معينة لمستخدمين معينين في مجموعة كائنات معينة، يمكنك إختيار الكائن والتصفح إليهGroup Controlled Access Rolesكما هو موضح في الصورة:



SSL وأ TLS

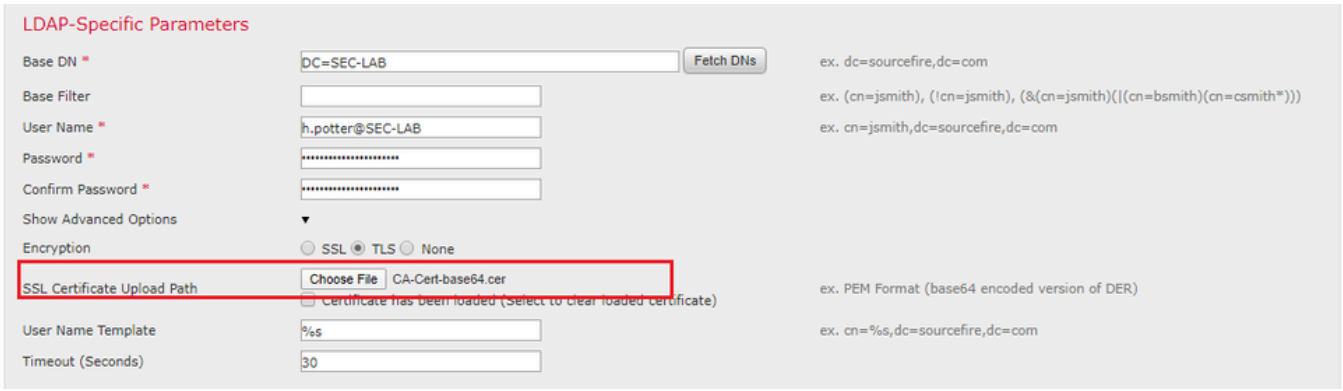
يجب تكوين DNS في FMC. وذلك لأن قيمة الموضوع للشهادة يجب أن تتطابق مع Authentication Object Primary Server Hostname. بمجرد تكوين LDAP الآمن، لم تعد عمليات التقاط الحزم تعرض طلبات ربط نص واضح.

يقوم SSL بتغيير المنفذ الافتراضي إلى 636، ويحتفظ TLS به على هيئة 389.

ملاحظة: يتطلب تشفير TLS شهادة على كل الأنظمة الأساسية. بالنسبة لـ SSL، يتطلب FTD أيضا شهادة. بالنسبة للأنظمة الأساسية الأخرى، لا يتطلب SSL شهادة. ومع ذلك، يوصى بتحميل شهادة لـ SSL دائما لمنع هجمات الدخيل.

الخطوة 1. انتقل إلىDevices > Platform Settings > External Authentication > External Authentication Objectمعلومات الخيارات المتقدمة SSL/TLS وأدخلها:

الخطوة 2. تحميل شهادة المرجع المصدق الذي وقع شهادة الخادم. يجب أن تكون الشهادة بتنسيق PEM.



الخطوة 3. احفظ التكوين.

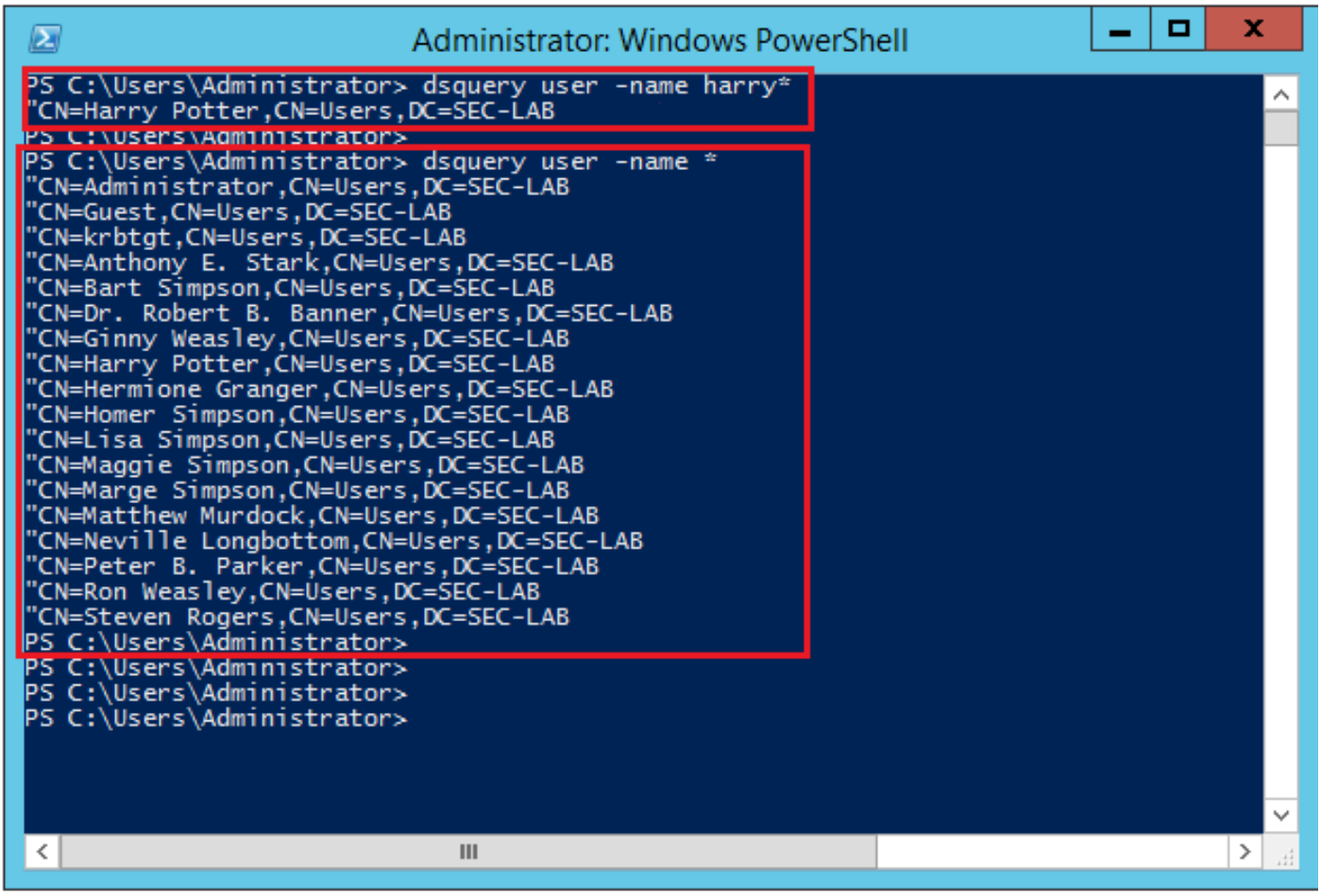
التحقق من الصحة

قاعدة بحث الاختبار

افتح موجه أوامر Windows أو PowerShell حيث تم تكوين LDAP واكتب الأمر:dsquery user -name
.

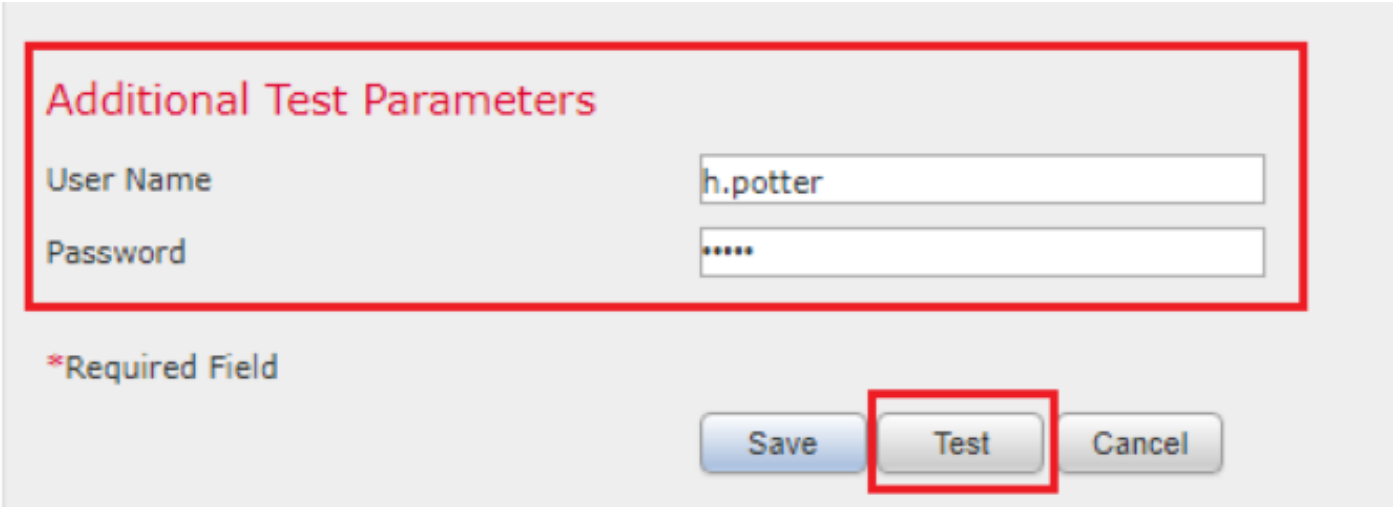
على سبيل المثال:

```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```

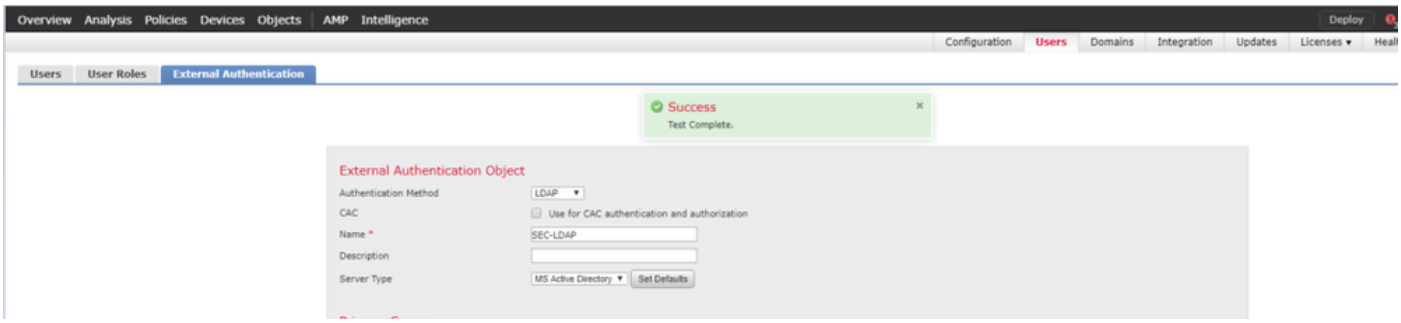


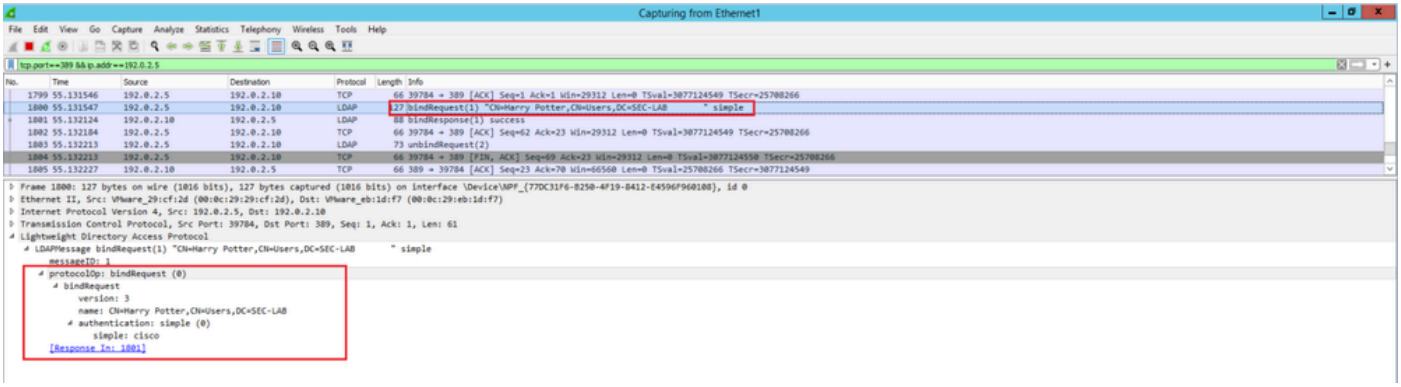
إختبار تكامل LDAP

انتقل إلىSystem > Users > External Authentication > External Authentication Object. في أسفل الصفحة، هناك Additional Test Parameters قسم كما يرى في الصورة:



أخترت إختبار in order to رأيت النتيجة.





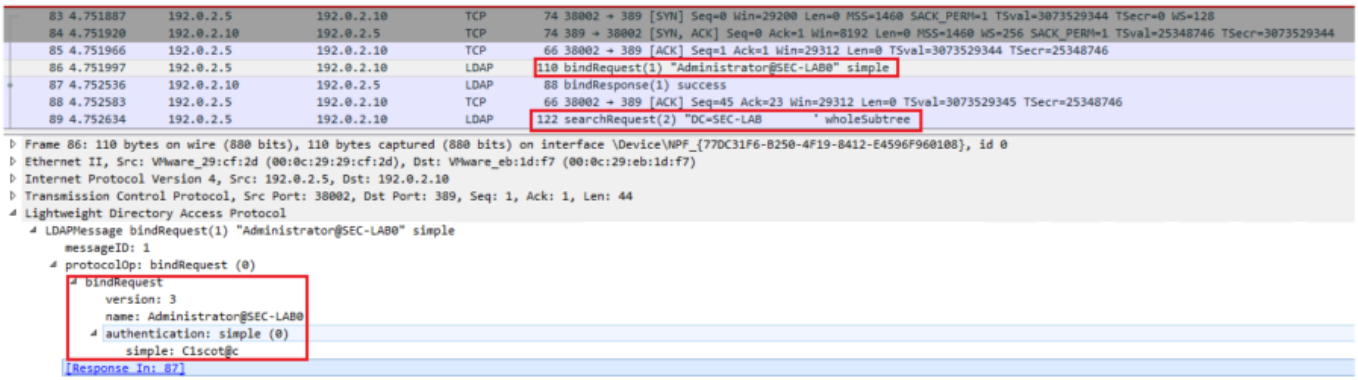
استكشاف الأخطاء وإصلاحها

كيف يتفاعل FMC/FTD و LDAP لتنزيل المستخدمين

لكي تتمكن FMC من سحب المستخدمين من خادم Microsoft LDAP، يجب على FMC إرسال طلب ربط أولا على المنفذ 389 أو 636 (SSL) باستخدام بيانات اعتماد مسؤول LDAP. بمجرد أن يكون خادم LDAP قادرا على مصادقة FMC، فإنه يستجيب برسالة نجاح. أخيرا، تستطيع FMC تقديم طلب مع رسالة طلب البحث كما هو موضح في الرسم التخطيطي:

<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

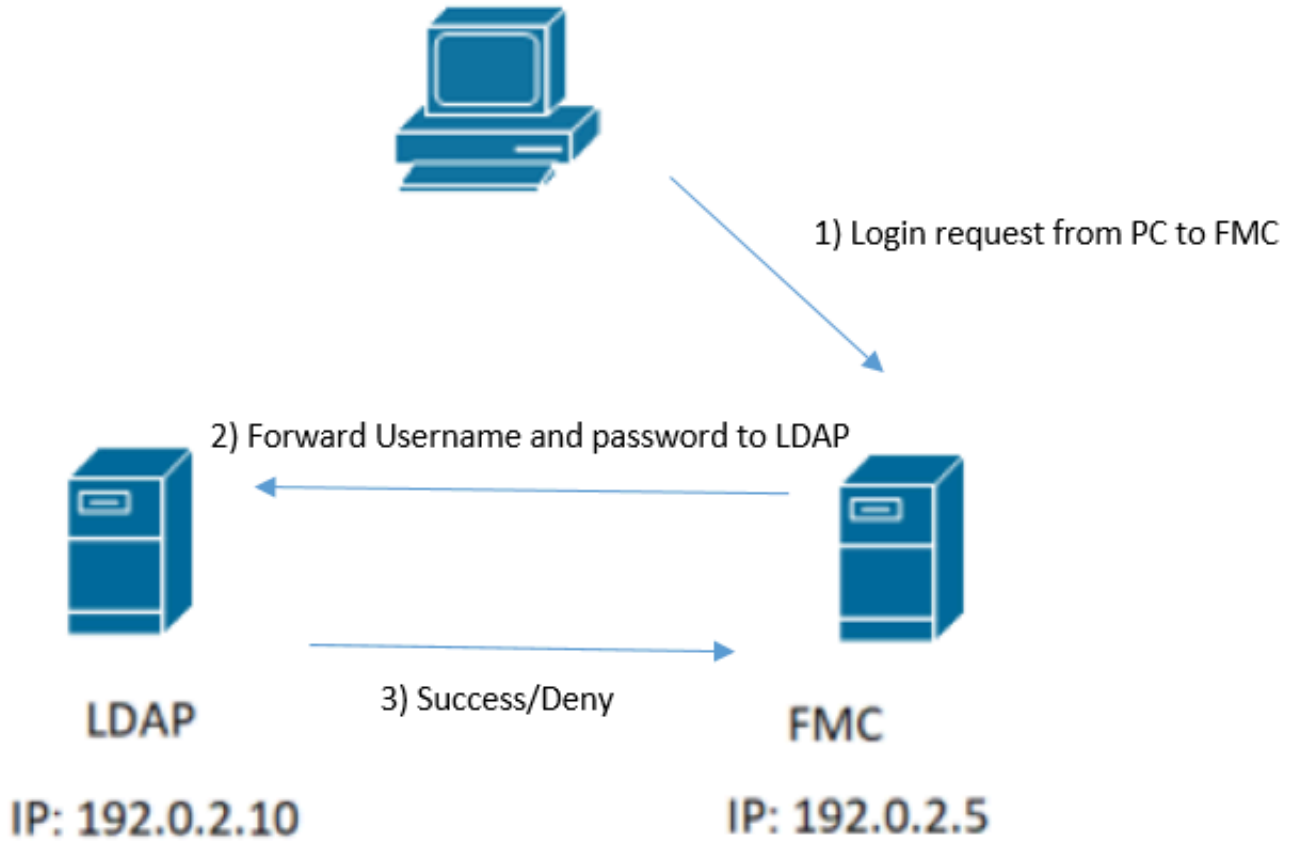
لاحظ أن المصادقة ترسل كلمات مرور في المسح بشكل افتراضي:

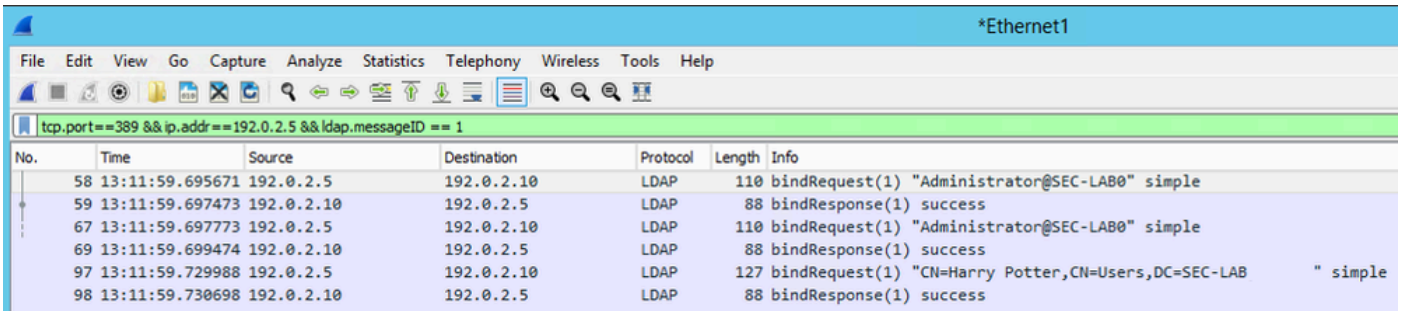


كيف يتفاعل FMC/FTD و LDAP لمصادقة طلب تسجيل دخول المستخدم

لكي يتمكن المستخدم من تسجيل الدخول إلى FMC أو FTD أثناء تمكين مصادقة LDAP،

يتم إرسال طلب تسجيل الدخول الأولي إلى FirePOWER، ومع ذلك، تتم إعادة توجيه اسم المستخدم وكلمة المرور إلى LDAP للحصول على إستجابة نجاح/رفض. وهذا يعني أن FMC و FTD لا يحتفظان بمعلومات كلمة المرور محليا في قاعدة البيانات وبدلا من ذلك ينتظرون تأكيد من LDAP حول كيفية المتابعة.





إذا تم قبول اسم المستخدم وكلمة المرور، تتم إضافة إدخال في واجهة المستخدم الرسومية (GUI) للويب كما هو موضح في الصورة:

قم بتشغيل الأمر show user في واجهة سطر أوامر FMC للتحقق من معلومات المستخدم: >
show user

يعرض الأمر معلومات التكوين التفصيلية للمستخدم (المستخدمين) المحدد. يتم عرض هذه القيم:

تسجيل الدخول — اسم تسجيل الدخول

UID — معرف المستخدم الرقمي
المصادقة (محلي أو بعيد) — كيفية مصادقة المستخدم
الوصول (أساسي أو config) — مستوى الامتياز للمستخدم
ممكن (ممكن أو معطل) — ما إذا كان المستخدم نشطا
إعادة تعيين (نعم أو لا) — ما إذا كان يجب على المستخدم تغيير كلمة المرور في تسجيل الدخول التالي
EXP (أبدا أو رقم) — عدد الأيام حتى يجب تغيير كلمة مرور المستخدم
تحذير (N/A أو رقم) — عدد الأيام التي يتم منح المستخدم فيها لتغيير كلمة المرور قبل انتهاء صلاحيتها
STR (نعم أو لا) — ما إذا كان يجب أن تستوفي كلمة مرور المستخدم المعايير للتحقق من القوة
القفل (نعم أو لا) — ما إذا كان حساب المستخدم قد تم تأمينه بسبب عدد كبير جدا من مرات تسجيل الدخول في حالات الفشل
الحد الأقصى (رقم N/A أو رقم) — الحد الأقصى لعدد عمليات تسجيل الدخول الفاشلة قبل تأمين حساب المستخدم

ال يعمل SSL أو TLS كما هو متوقع

إذا لم تقم بتمكين DNS على FTDs، فيمكنك مشاهدة أخطاء في سجل خيوط البيانات تشير إلى أنه يتعذر الوصول إلى LDAP:

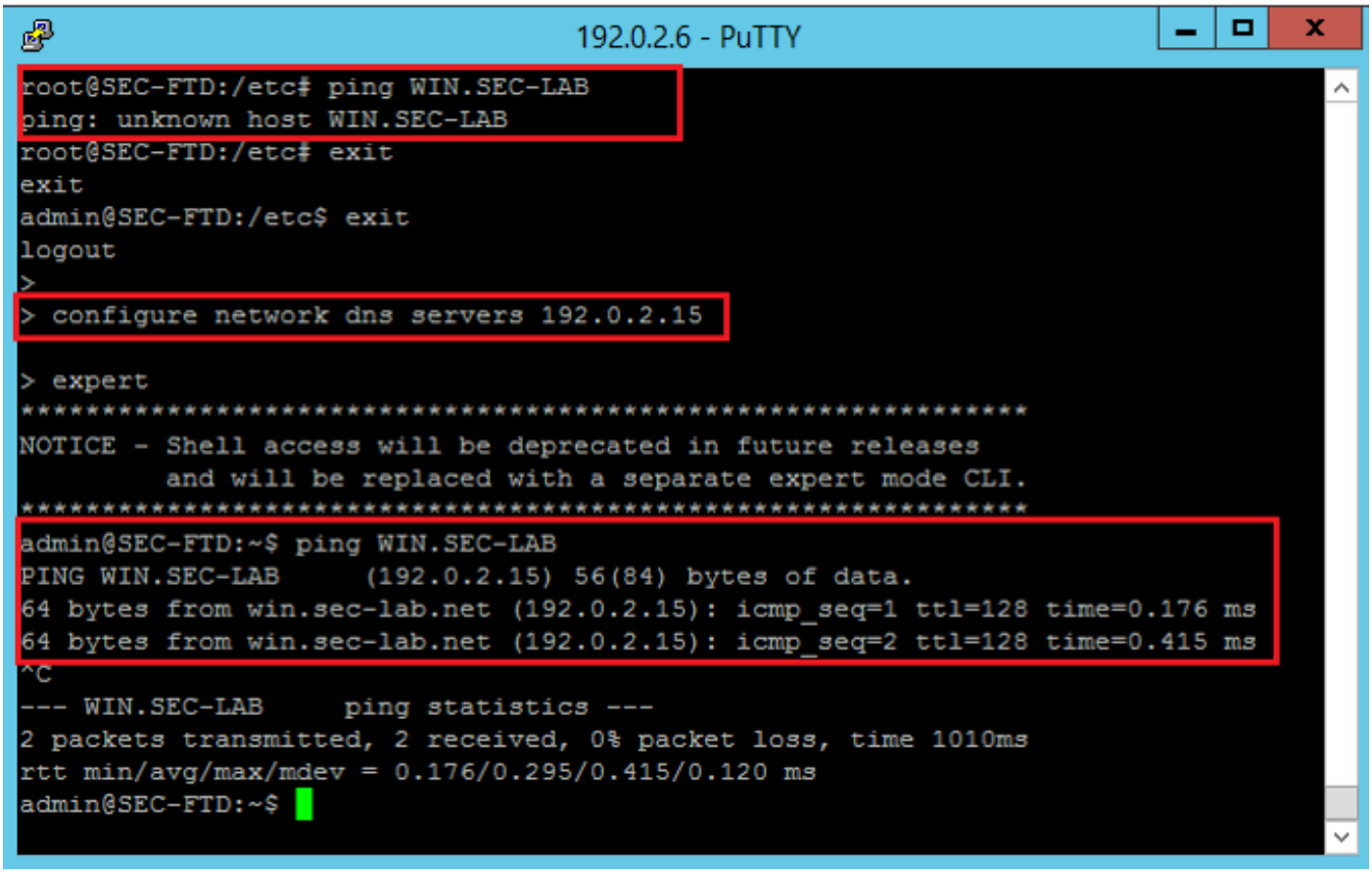
```
root@SEC-FMC:/$ sudo cd /var/common
root@SEC-FMC:/var/common$ sudo pigtail
```

```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61
```

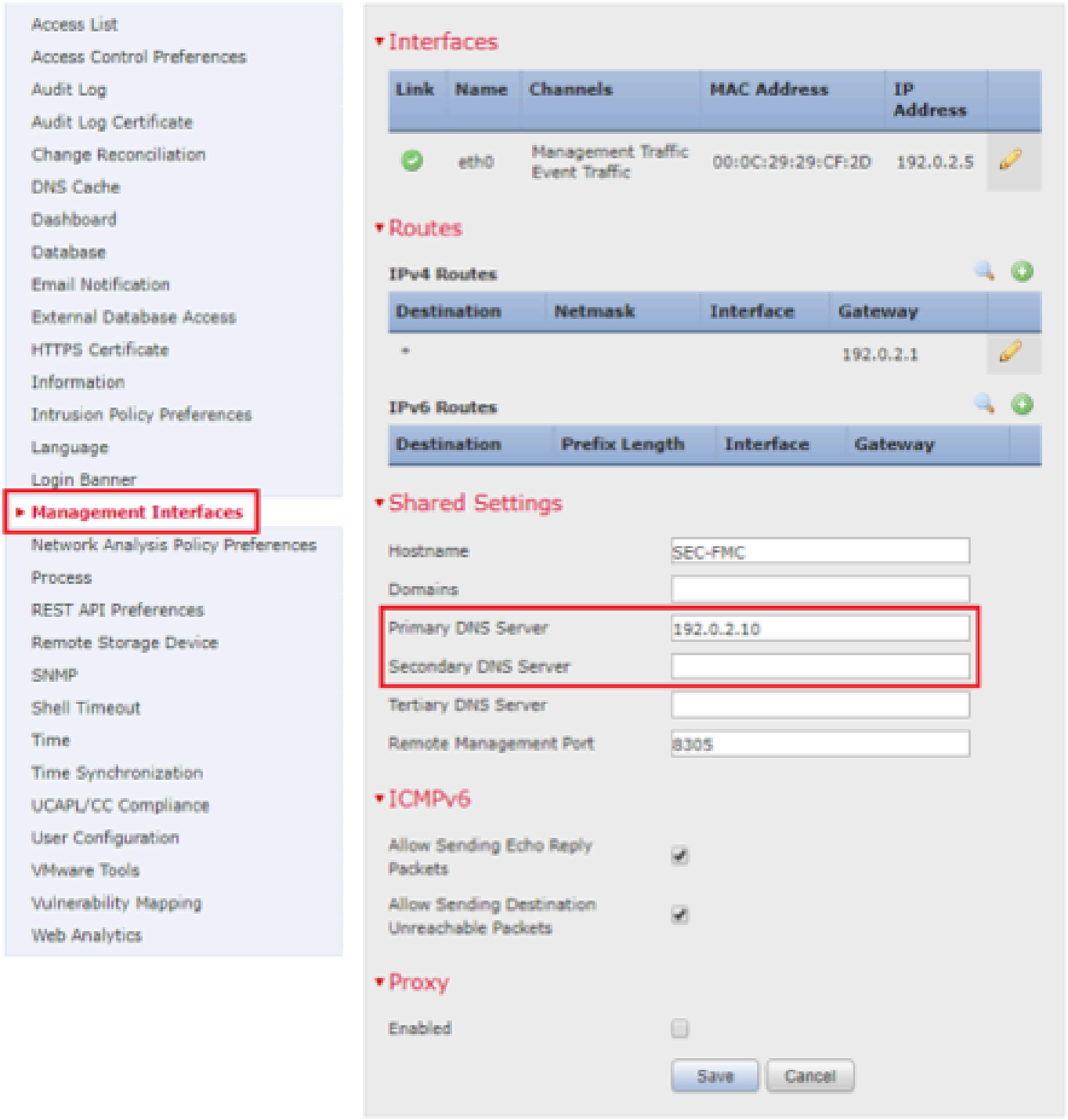
تأكد من قدرة Firepower على حل اسم المجال المؤهل بالكامل (FQDN) الخاص بخادم LDAP. إذا لم تكن هناك حاجة، فقم بإضافة DNS الصحيح كما يظهر في الصورة.

برنامج FTD: الوصول إلى FTD CLISH وتشغيل الأمر: > configure network dns servers

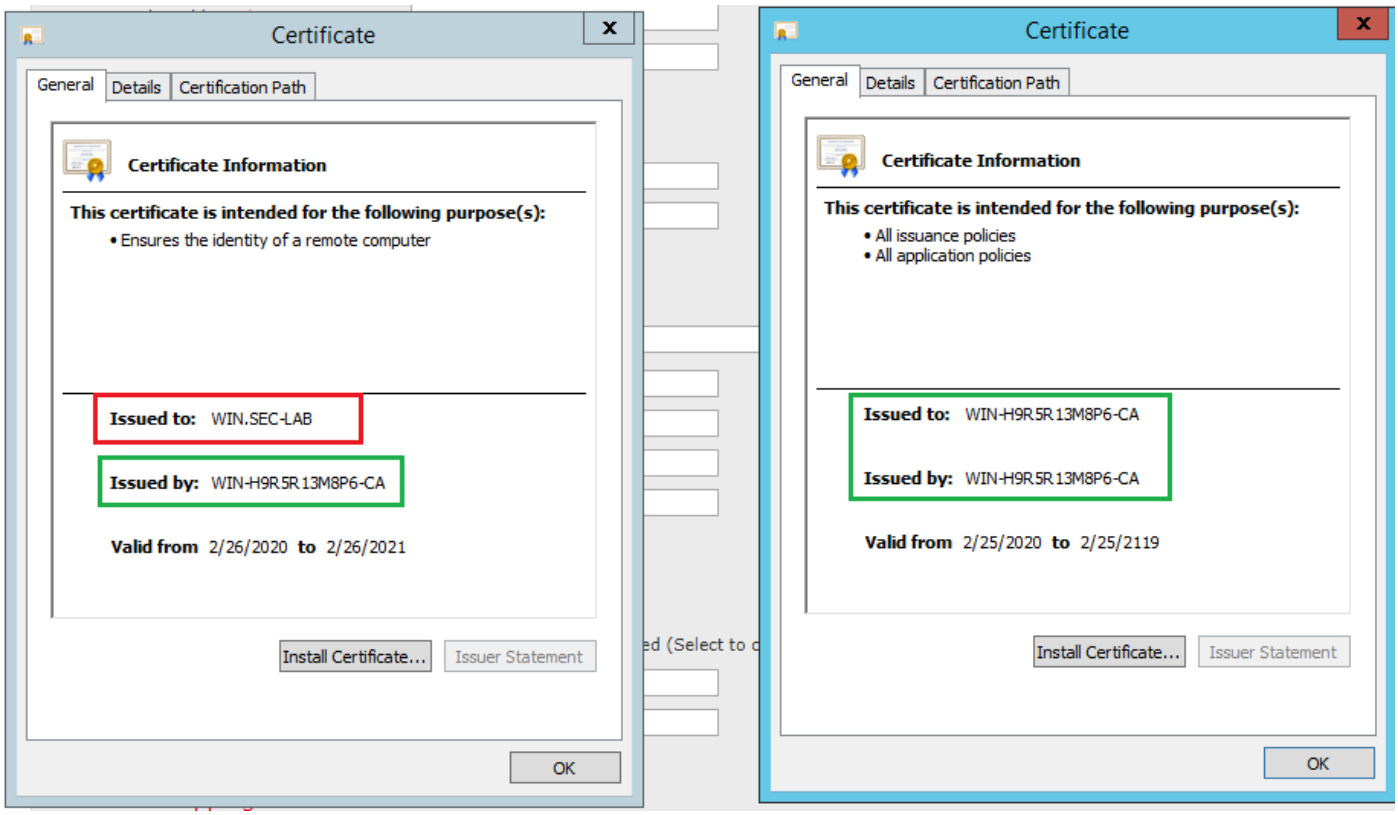
.



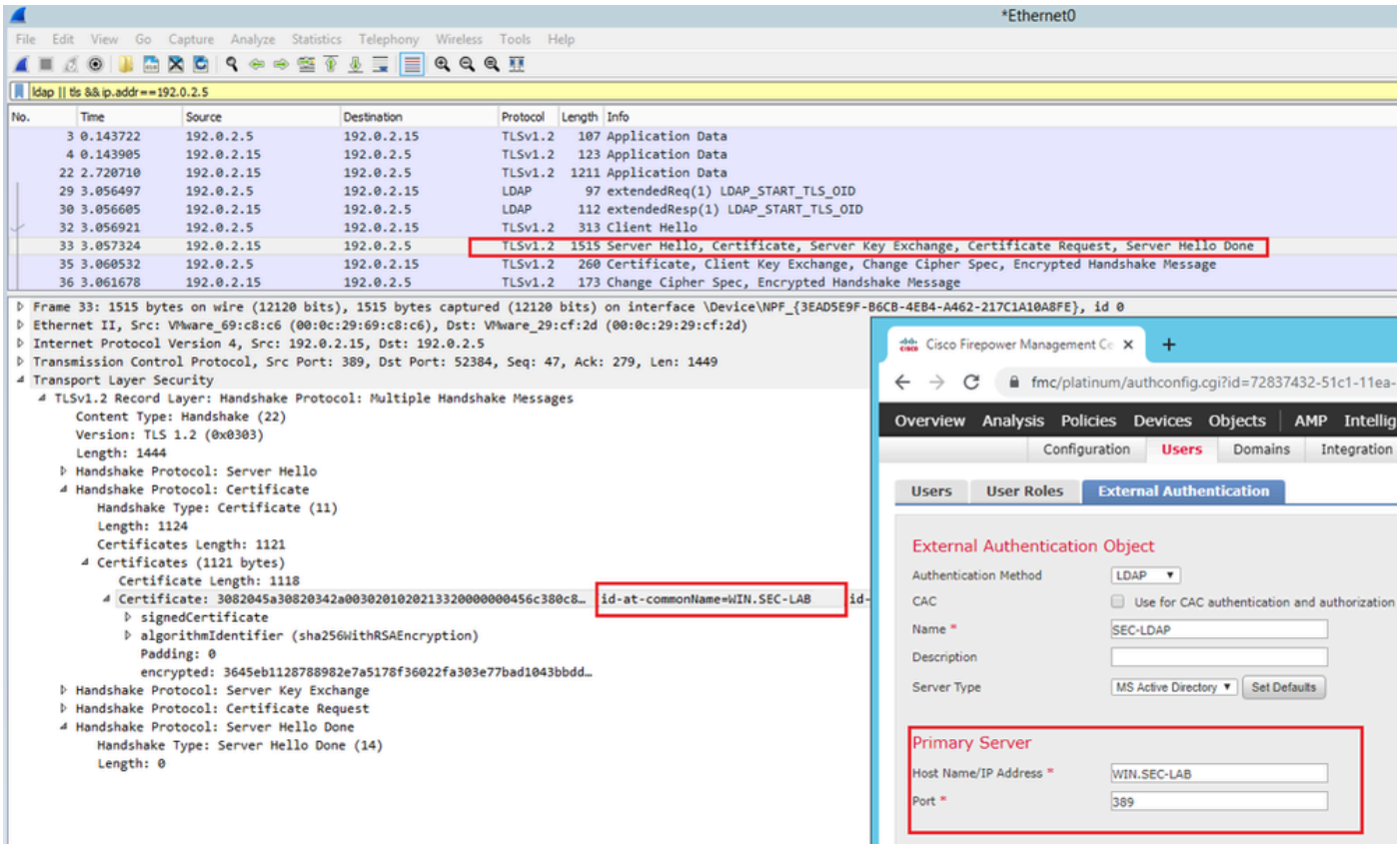
وحدة التحكم FMC: أخترSystem > Configuration، ثم أختر واجهات الإدارة كما هو موضح في الصورة:



تأكد من أن الشهادة التي تم تحميلها إلى FMC هي شهادة المرجع المصدق الذي وقع على شهادة الخادم الخاصة ب LDAP، كما هو موضح في الصورة:



أستخدم التقاط الحزم لتأكيد إرسال خادم LDAP المعلومات الصحيحة:



معلومات ذات صلة

- [حسابات المستخدمين للوصول إلى الإدارة]

- إمكانية تجاوز مصادقة بروتوكول الوصول إلى الدليل الخفيف في Cisco Firepower Management Center
- تكوين كائن مصادقة LDAP على نظام FireSIGHT
- 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).