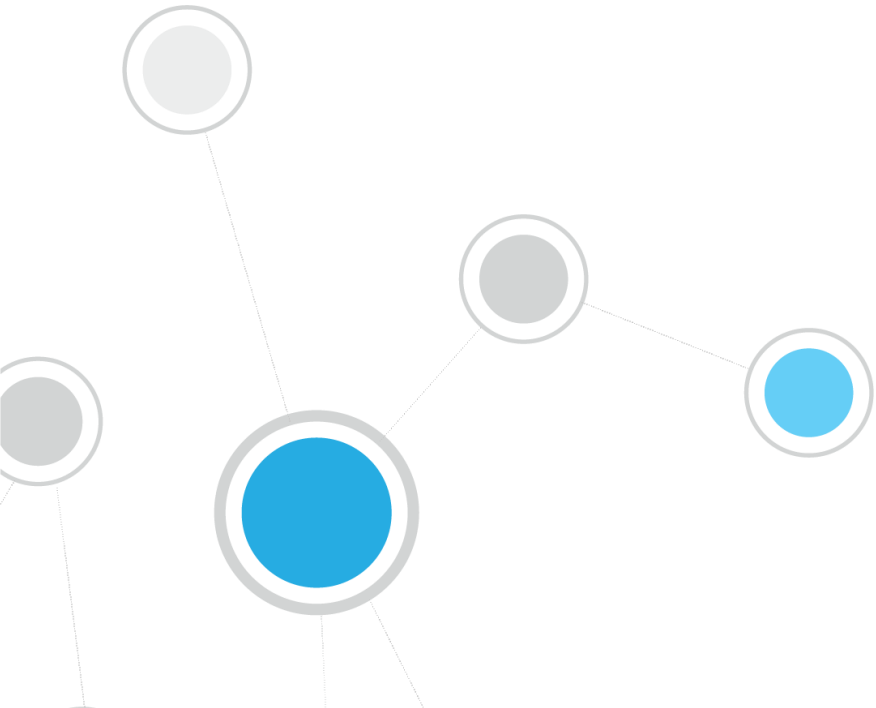
ForeScout CounterACT®

جهاز CounterACT واحد

كتيب تركيب سريع

الإصدار 8.0



جدول المحتويات

مرحبا بك في CounterACT الإصدار 8.0

تتيح منصة CounterACT مراقبة البنية التحتية والأجهزة وإدارة السياسات وخدمات التنسيق وتبسيط إجراءات سير العمل من أجل تعزيز أمن الشبكات. توفر CounterACT للشركات معلومات سياقية لحظية تتعلق بالأجهزة والمستخدمين على الشبكة. يتم تعريف السياسات في CounterACT باستخدام المعلومات السياقية التي تساعد على تحقيق الالتزام والمعالجة والوصول المناسب للشبكات وتبسيط عمليات الخدمة.

يتناول هذا الدليل طريقة تركيب جهاز CounterACT واحد مستقل.

لمزيد من التفاصيل أو المعلومات عن طريقة تركيب أكثر من جهاز من أجل حماية الشبكة على مستوى الشركات، راجع *دليل إدارة CounterACT* و*دليل إدارة CounterACT*. راجع وثائق إضافية لجهاز CounterACT للحصول على معلومات عن طريقة الوصول إلى تلك الأدلة.

كما يمكنك زيارة الموقع الإلكتروني الخاص بالدعم عبر الرابط التالي: http://www.forescout.com/support للحصول على أحدث المستندات ومقالات قاعدة المعارف والتحديثات الخاصة بالجهاز.

محتويات عبوة CounterACT

تحتوي عبوة جهاز CounterACT على العناصر التالية:

- جهاز CounterACT
- الإطار الأمامي
- مجموعات القضبان (كتائف تركيب)
- كبل/كبلات الكهرباء
- كابل توصيل كونسول DB9 (للاتصالات التسلسلية فقط)
- معلومات عن سلامة منتجات الشركات ومعلومات بيئية ونظامية
- مستند بدء الاستخدام (عدد 51xx جهاز فقط)

لمحة عامة

اتبع الخطوات التالية لإعداد جهاز CounterACT للتركيب:

1- وضع خطة للتركيب

2- إعداد المُبدل

3- قم بتوصيل كابلات الشبكة والتشغيل

4- تهيئة الجهاز

5- الإدارة عن بُعد

6- التحقق من الاتصال

7- إعداد كونسول CounterACT

1- وضع خطة للتركيب

قبل البدء في التركيب، يجب تحديد مكان وضع الجهاز ومعرفة وصلات الجهاز البينية.

تحديد مكان وضع الجهاز

يعد اختيار موقع الشبكة الصحيح لتركيب الجهاز أمرًا ضروريًا للتركيب الناجح والتشغيل الأمثل لجهاز CounterACT. سيعتمد اختيار الموقع الصحيح على أهداف التنفيذ المرجوة وسياسة الوصول إلى الشبكة. يجب أن يكون الجهاز قادرًا على مراقبة الحركة ذات الصلة بالسياسة المرغوبة. على سبيل المثال، إذا كانت السياسية الخاصة بك تعتمد على مراقبة أحداث الترخيص من نقاط النهاية وحتى خوادم المصادقة للشركات، فيتعين تركيب الجهاز في موقع يمكّنه من رؤية حركة نقاط النهاية حتى خادم/خوادم المصادقة.

لمزيد من المعلومات عن التركيب والتثبيت، راجع دليل إدارة CounterACT. راجع وثائق إضافية لجهاز CounterACT للحصول على معلومات عن طريقة الوصول إلى هذا الدليل.

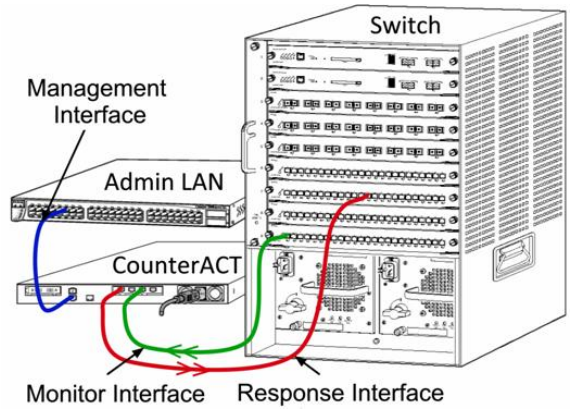
وصلات الجهاز البينية

يتم توصيل الجهاز عمومًا بثلاث وصلات بمبدل الشبكة.

واجهة الإدارة

تمكنك واجهة الإدارة من إدارة CounterACT وتنفيذ الاستعلامات وفحص نقاط النهاية بشكل عميق. يجب أن تتصل الواجهة بمنفذ مبدل مع إمكانية الوصول إلى جميع نقاط نهاية الشبكات.

يتطلب كل جهاز اتصال إدارة مستقل بالشبكة. تتطلب هذه الوصلة عنوان بروتوكول الإنترنت على شبكة الاتصال المحلية ومنفذ وصول TCP/13000 للوصول إلى الأجهزة المسؤولة عن تشغيل تطبيق إدارة كونسول CounterACT. يجب أن يكون لمنفذ الإدارة إمكانية الوصول إلى خدمات الشبكة الإضافية.



متطلبات الوصول إلى الشبكة

منفذ	الخدمة	من أو إلى CounterACT	الوظيفة
TCP/22	SSH	من	يسمح بالفحص عن بعد لنقاط نهاية نظامي التشغيل OS X وLinux. يمكن CounterACT من التواصل مع مبدلات الشبكة وأجهزة التوجيه.
		إلى	يسمح بالوصول إلى واجهة سطر الأوامر الخاصة بـCounterACT.

منفذ	الخدمة	من أو إلى CounterACT	الوظيفة
TCP/2222	SSH	إلى	(التوفر العالي) يتيح الوصول إلى أجهزة CounterACT الفعلية التي تُعد جزءًا من زوج التوفر العالي. استخدام منفذ TCP/22 للوصول إلى عنوان IP المشترك (الظاهري) للزوج.
TCP/25	بروتوكول إرسال البريد البسيط	من	يُمكِّن CounterACT من الوصول إلى رسائل البريد الإلكتروني المُرَحّلة والتي تخص الشركة.
UDP/53	نظام أسماء النطاقات	من	يُمكِّن CounterACT من حل عناوين IP الداخلية.
TCP/80	بروتوكول نقل النص الفائق	إلى	يسمح بإعادة توجيه بروتوكول نقل النص الفائق
UDP/123	بروتوكول وقت الشبكة	من	يُمكِّن CounterACT من الوصول إلى الخادم بالتوقيت الوقت المحلي أو إلى موقع ntp.forescout.net. يقوم CounterACT في الوضع الافتراضي بالوصول إلى موقع ntp.foreScout.net
TCP/135	MS-WMI	من	يسمح بالفحص عن بعد لنقاط نهاية Windows.
TCP/139	SMB, MS-RPC	من	يسمح بالفحص عن بعد لنقاط نهاية Windows (لنقاط النهاية التي تشغل نظام Windows 7 والإصدارات السابقة منه)
TCP/445			يسمح بالفحص عن بعد لنقاط نهاية Windows.
UDP/161	بروتوكول إدارة الشبكات البسيط	من	يُمكِّن CounterACT من التواصل مع مبدلات الشبكة وأجهزة التوجيه. لمزيد من المعلومات عن تكوين SNMP، راجع *دليل إدارة CounterACT*.
UDP/162	بروتوكول إدارة الشبكات البسيط	إلى	يُمكِّن CounterACT من استقبال اتصالات بروتوكول إدارة الشبكات البسيط من مبدلات الشبكة وأجهزة التوجيه. لمزيد من المعلومات عن تكوين SNMP، راجع *دليل إدارة CounterACT*.
TCP/389 (636)	بروتوكول النفاذ إلى الدليل البسيط	من	يُمكِّن CounterACT من التواصل مع الدليل النشط. يسمح بالتواصل مع بوابات ويب CounterACT
TCP/443	بروتوكول نقل النص التشعبي الآمن	إلى	يتيح إعادة توجيه بروتوكول نقل النص الفائق باستخدام TLS.
TCP/2200	SecureConnector لنظام Linux	إلى	يُمكِّن SecureConnector من إنشاء اتصال آمن (SSH مشفر) بجهاز من أجهزة Linux. *SecureConnector* هو برنامج يستند إلى تعليمات نصية برمجية يتيح إدارة نقاط نهاية Linux أثناء اتصالها بالشبكة.
TCP/10003	SecureConnector لنظام Windows	إلى	يُمكِّن SecureConnector من إنشاء اتصال آمن (TLS مشفر) بجهاز من الأجهزة التي تعمل بنظام تشغيل Windows. *SecureConnector* هو برنامج يستند إلى تعليمات نصية برمجية يتيح إدارة نقاط نهاية Windows أثناء اتصالها بالشبكة. لمزيد من المعلومات عن SecureConnector، راجع *دليل إدارة CounterACT* عندما يتصل SecureConnector بأحد الأجهزة أو بـ Enterprise Manager، فإنه يتم إعادة توجيهه إلى الجهاز الذي تم تعيين مضيفه عليه. تأكد من أن هذا المنفذ مفتوح لجميع الأجهزة وكذلك Enterprise Manager للسماح بالحركة الشفافة داخل المؤسسة.

منفذ	الخدمة	من أو إلى CounterACT	الوظيفة
TCP/10005	SecureConnector for OS X	إلى	يمكن SecureConnector من إنشاء اتصال آمن (TLS مشفر) بجهاز من أجهزة OS X. *SecureConnector* هو برنامج يستند إلى تعليمات نصية برمجية يمكّن من إدارة نقاط نهاية نظام التشغيل OS X أثناء اتصالها بالشبكة. لمزيد من المعلومات عن SecureConnector، راجع *دليل إدارة CounterACT* عندما يتصل SecureConnector بأحد الأجهزة أو بـ Enterprise Manager، فإنه يتم إعادة توجيهه إلى الجهاز الذي تم تعيين مضيفه عليه. تأكد من أن هذا المنفذ مفتوح لجميع الأجهزة وكذلك Enterprise Manager للسماح بالحركة الشفافة داخل المؤسسة.
TCP/13000	CounterACT	من/إلى	للأماكن التي تحتوي على جهاز واحد فقط - من وحدة التحكم إلى الجهاز. بالنسبة للأماكن التي بها أكثر من جهاز CounterACT- من وحدة وحدة الكونسل إلى جهاز CounterACT ومن جهاز CounterACTإلى جهاز آخر. تتضمن إمكانيات تواصل جهاز CounterACTالتواصل مع Enterprise Manager وRecovery Enterprise Manager وذلك باستخدام TLS.

واجهة التحكم في الشاشة

تسمح واجهة التحكم في الشاشة للجهاز بالمراقبة وتتبع حركة عمل الشبكة. يمكن استخدام أي واجهة متوفرة لتكون واجهة التحكم في الشاشة.

تنعكس حركة المرور في منفذ على المبدل ومن ثم يراقبها الجهاز. يعتمد استخدام بطاقات ربط 802.1Q VLAN على عدد الشبكات المحلية الافتراضية "VLANs" الجاري محاكاتها.

- ***شبكة محلية افتراضية فردية***: عندما يتم التحكم في الحركة من شبكة محلية افتراضية، لا يلزم ربط الحركة المحاكاة بشبكة VLAN.
- ***شبكات محلية افتراضية متعددة***: إذا كانت حركة الاتصالات التي يتم التحكم فيها من أكثر من شبكة محلية افتراضية، فإنه يجب ربط الحركة المحاكاة بـ 802.1Q VLAN.

في حال توصيل اثنين من المبدلات كزوج متكرر، فإنه يجب أن يراقب الجهاز حركة المرور من كلا المبدلين.

لا يوجد عنوان IP مطلوب على واجهة الشاشة.

واجهة الاستجابة

يستجيب الجهاز لحركة الاتصالات باستخدام واجهة الاستجابة. يتم استخدام حركة مرور الاستجابة للحماية ضد أي نشاط ضار وتنفيذ إجراءات السياسة. قد تضمن هذه الإجراءات على سبيل المثال إعادة توجيه متصفحات الويب أو تنفيذ حظر الجلسة. يعتمد تكوين منفذ التبديل ذي الصلة على مراقبة حركة الاتصالات.

يمكن استخدام أي واجهة متوفرة لتكون واجهة الاستجابة.

- ***شبكة محلية افتراضية فردية***: عند إنشاء حركة اتصالات خاضعة للمراقبة من شبكة محلية افتراضية فردية، فإنه يجب أن يكون منفذ الاستجابة مقترناً بذات الشبكة. وفي هذه الحالة، يتطلب الجهاز عنوان IP واحد على الشبكة المحلية الافتراضية الفردية.
- ***شبكات محلية افتراضية متعددة***: في حالة مراقبة حركة الاتصالات من أكثر من شبكة محلية افتراضية، فإنه يجب توصيل منفذ الاستجابة من خلال ربط 802.1Q VLAN بذات الشبكات المحلية الافتراضية. ويتطلب الجهاز عنوان IP لكل شبكة محلية افتراضية خاضعة للمراقبة.

2- إعداد المُبدل

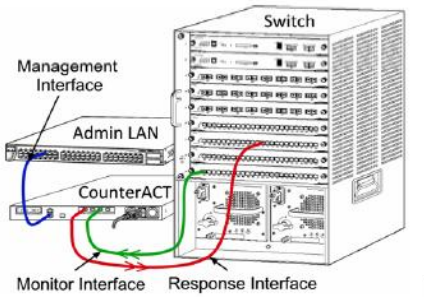
أ- خيارات توصيل المُبدل

صُمّم الجهاز ليتكامل بسلاسة مع مجموعة واسعة من بيئات الشبكات. لتوصيل الجهاز بنجاحٍ بالشبكة، تحقق من إعداد المبدل لمراقبة حركة الاتصالات اللازمة.

تتوفر خيارات عديدة لتوصيل بالمبدل.

1- نظام التشغيل القياسي (واجهات منفصلة للإدارة والتحكم والاستجابة)

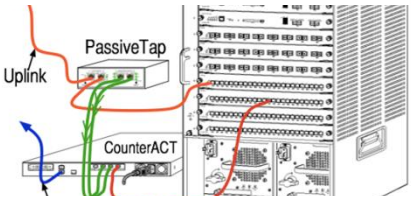
يستخدم نظام التشغيل الموصى به ثلاث منافذ منفصلة. وهذه المنافذ موضحة في وصلات الجهاز البينية.



2- المأخذ السلبي الداخلي

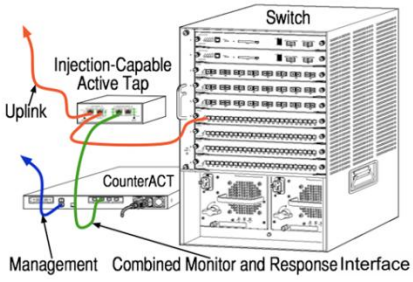
بدلًا من الاتصال بمنفذ التحكم بالمبدل، قد يستخدم الجهاز مأخذاً سلبياً داخليًا.

يتطلب المأخذ السلبي الداخلي وجود منفذي تحكم (منفذ لحركة الاتصالات الصاعدة وآخر لحركة الاتصالات الهابطة)، باستثناء في حالة مأخذ *إعادة التركيب*، الذي يدمج الناقلين المزدوجين في منفذ واحد. يرجى ملاحظة أنه في حالة ربط حركة الاتصالات على منفذ التحكم بـ 802.1Q VLAN، فإنه يجب أيضاً ربط منفذ الاستجابة بـ 802.1Q VLAN.



3- المأخذ الداخلي النشط (قابل للإدخال)

قد يستخدم الجهاز مأخذاً داخلياً نشطاً. في حال كان المأخذ قابلاً للإدخال، فإن الجهاز يجمع الشاشة ومنافذ الاستجابة بحيث لا توجد حاجة لتهيئة منفذ استجابة منفصل على المبدل. وقد يُستخدم هذا الخيار بصرف النظر عن نوع تهيئة المُبدل لحركة الاتصالات الصاعدة أو الهابطة.



4- الاستجابة لطبقات عنوان IP (لتركيبات المُبدل للطبقة 3)

قد يستخدم الجهاز واجهة الإدارة للاستجابة لحركة الاتصالات. وعلى الرغم من إمكانية استخدام هذا الخيار مع أي حركة اتصالات خاضعة للمراقبة، إلا أنه يُوصى بذلك فقط في حالة مراقبة الجهاز للمنافذ التي لا تمثل جزءًا من أي شبكة افتراضية محلية ومن ثم لا يمكن الاستجابة لحركة الاتصالات الخاضعة للمراقبة باستخدام أي منفذ مبدل آخر. وهذا أمرٌ طبيعي عند مراقبة ارتباط يصل بين جهازي توجيه. ولا يستطيع هذا الخيار الاستجابة لطلبات بروتوكول تحليل العناوين، الأمر الذي يحد من قدرة الجهاز على الكشف عن عمليات المسح الموجهة إلى عناوين IP المتضمنة في الشبكة الفرعية الخاضعة للتحكم. ولا ينطبق هذا القيد في حالة التحكم في حركة الاتصالات بين جهازي التوجيه.

ب- ملاحظات حول ضبط المُبدل

بطاقات VLAN (802.1Q)

- ***التحكم في شبكة محلية افتراضية فردية***: في حال كانت حركة الاتصالات الخاضعة للمراقبة من شبكة محلية افتراضية فردية، فإن حركة الاتصالات لا تحتاج إلى بطاقات 802.1Q VLAN.

- ***التحكم في شبكات محلية افتراضية متعددة***: في حالة التحكم في الحركة بواسطة شبكتين محليتين افتراضيتين أو أكثر، فيجب تمكين *كل* من المنفذ المتحكم به ومنفذ الاستجابة وإظهار علامة 802.1Q VLAN. ويُوصى بالتحكم في عدة شبكات محلية افتراضية حيث إن ذلك يوفر أفضل تغطية شاملة ويقلل في نفس الوقت من عدد المنافذ المطابقة.
- في حالة عدم قدرة المُبدل على استخدام بطاقة 802.1Q VLAN على المنفذ المطابق، فقم بأحد الإجراءات التالية:
  - مطابقة شبكة محلية افتراضية فردية فقط
  - مطابقة منفذ ارتباط صاعد فردي بدون بطاقة تعريفية
  - استخدام طبقة عنوان IP لخيار الاستجابة
- إذا كان من الممكن أن يطابق المُبدل منفذًا واحدًا فقط، فيمكن مطابقة منفذ ارتباط صاعد فردي. ومن الممكن وضع بطاقة تعريفية. وبشكل عام، إذا قام المبدل بحذف بطاقات 802.1Q VLAN التعريفية، فيجب استخدام خيار الاستجابة لطبقة عنوان IP.

إرشادات إضافية

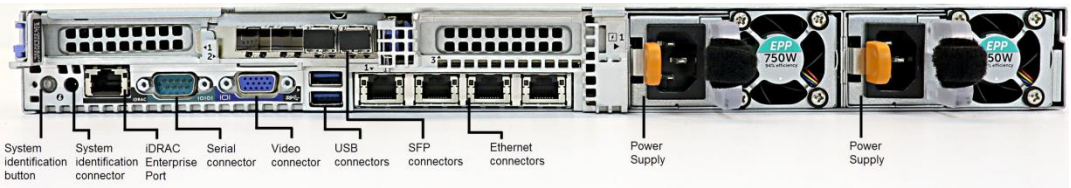
- في الحالات التالية، يجب مطابقة واجهة واحدة فقط (تسمح بالإرسال / الاستلام):
  - إذا لم يطابق المُبدل كلاً من الحركة المرسلة والمستلمة
  - إذ لم يطابق المُبدل كل حركات اتصالات المبدل
  - إذا لم يطابق المُبدل كل حركة الاتصالات عبر الشبكات المحلية الافتراضية
- تحقق من عدم التحميل الزائد على المنفذ المطابق.
- قد تتطلب بعض المبدلات (مثل Cisco 6509) حذف تكوين المنفذ الحالي بالكامل قبل إدخال تكوين جديدة. إن عدم حذف معلومات المنفذ غالبًا ما يؤدي إلى قيام المبدل باستبعاد بطاقات 802.1Q التعريفية.

3- قم بتوصيل كابلات الشبكة والتشغيل

أ. قم بفك الجهاز وتوصيل الكابلات

1. أخرج الجهاز وكابل الطاقة من حاوية الشحن
2. أخرج مجموعة القضبان التي استلمتها مع الجهاز.
3. قم بتجميع مجموعة القضبان الموجودة على الجهاز مع تركيب الجهاز على الحامل.
4. قم بتوصيل كابلات الشبكة بين واجهات الشبكة الموجودة على اللوحة الخلفية للجهاز ومنافذ المبدل.

نموذج اللوحة الخلفية - جهاز CounterACT



يمكنك استبدال أجهزة SFP المزودة من شركة ForeScout بأجهزة FinisarSFPs التي تم اختبارها والموافقة عليها من قبل ForeScout. راجع *دليل تركيب CounterACT* لمزيد من المعلومات.

ب. تسجيل تعيينات الواجهة

بعد الانتهاء من تثبيت الجهاز في مركز البيانات وتثبيت وحدة تحكم CounterACT، ستتم مطالبتك بتسجيل تعيينات الواجهة. يتم إدخال هذه التعيينات، المشار إليها باسم *تعريفات القناة*، في "معالج الإعداد الأولي" الذي يفتح عند تسجيل الدخول لأول مرة إلى وحدة التحكم.

سجل تعيينات الواجهة الفعلية أدناه واستخدمها عند إكمال إعداد القناة في وحدة التحكم.

واجهة Eth	تعيين الواجهة (على سبيل المثال، الإدارة، المراقبة، الاستجابة)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

جـ الطاقة اللازمة لتشغيل الجهاز

1. قم بتوصيل كابل الطاقة بموصل الطاقة الموجود في اللوحة الخلفية للجهاز.
2. قم بتوصيل الطرف الآخر لكابل الطاقة بمأخذ تيار أرضي متردد.
3. قم بتوصيل لوحة المفاتيح والشاشة بالجهاز أو قم بإعداد الجهاز للاتصالات التسلسلية. راجع *دليل إدارة CounterACT* لمزيد من المعلومات عن إعداد جهاز CounterACT.
4. قم بتشغيل الجهاز من خلال اللوحة الأمامية.

4- تهيئة الجهاز

يتعين عليك تحضير المعلومات الآتية قبل تهيئة الجهاز:

اسم مضيف الجهاز	
كلمة مرور مسؤول CounterACT	احتفظ بكلمة المرور في مكان آمن
واجهة الإدارة	
عنوان IP للجهاز	
قناع الشبكة	
عنوان IP للبوابة الافتراضية	
اسم نظام أسماء النطاقات	
عناوين خادم نظام أسماء النطاقات	

عقب التشغيل، سوف تكون مطالبًا ببدء التهيئة من خلال الرسالة التالية:

```
تم الانتهاء من عملية تشغيل جهاز CounterACT
اضغط على <دخول> للمتابعة.
```

1. اضغط على **دخول**. إذا كان لديك جهاز CounterACT 51xx، سوف تظهر القائمة التالية:

```
خيارات <تهيئة>- CounterACT 8.0.0:
```

```
1) تهيئة CounterACT
2) استعادة تهيئة CounterACT التي تم حفظها
3) تحديد وإعادة ترقيم واجهات الشبكة
4) تهيئة تخطيط لوحة المفاتيح
5) إيقاف تشغيل الجهاز
6) إعادة تشغيل الجهاز

الاختيار (1-6): 1
```

إذا كان لديك جهاز كونتراكت CT-xxxx، فستشاهد إما كونتراكت 7.0.0 أو كونتراكت 8.0.0 مدرجًا كإصدار أعلى القائمة.

- بعد مشاهدتك لـ CounterACT 7.0.0، فيمكنك الترقية إلى الإصدار 8.0.0 أو إجراء تثبيت جديد له. راجع *دليل تهيئة CounterACT* للمزيد من المعلومات. عقب إجراء الترقية أو التثبيت للإصدار 8.0.0، سوف تشاهد القائمة الواردة أعلاه.
- عند مشاهدة CounterACT 8.0.0، تعرض القائمة خيارًا لتثبيت CounterACT 7.0.0 أو لتهيئة CounterACT 8.0.0، كما هو موضح أدناه. إذا قمت بتحديد CounterACT 7.0.0، فلن تتمكن من إعادة تثبيت CounterACT 8.0.0 من خلال قائمة Configuration. راجع *دليل تثبيت CounterACT للإصدار 7.0.0* لمعرفة المزيد من التفاصيل عن تهيئة CounterACT 7.0.0.

```
خيارات <تهيئة>- CounterACT 8.0.0:
```

```
1) تثبيت CounterACT 7.0.0 -<تهيئة>
2)تهيئة CounterACT -<تهيئة>
3)استعادة تهيئة CounterACT الذي تم حفظه
4) تحديد وإعادة ترقيم واجهات الشبكة
5) تهيئة تخطيط لوحة المفاتيح
6) إيقاف تشغيل الجهاز
7) إعادة تشغيل الجهاز

الخيار (1-7) :
```

إذا تمت مقاطعة التهيئة أو إذا قمت بتحديد إصدار غير صحيح لجهاز CounterACT، فستحتاج إلى إعادة تعيين الإصدار المناسب من ملف ISO. راجع دليل إدارة CounterACT للمزيد من المعلومات عن إعادة تعيين الجهاز.

2. قم بتحديد **تهيئة جهاز .CounterACT** في الموجه:

استمرار: (نعم/لا)؟

اضغط على **دخول** لبدء عملية الإعداد.

3. يتم فتح موجه وضع التوفر العالي. اضغط على **دخول** لتحديد التثبيت القياسي.

4. يتم عرض موجه الإعداد المبدئي لجهاز CounterACT. اضغط على **دخول** للمتابعة.

5. يتم فتح خيار موجه نوع تثبيت جهاز CounterACT. اكتب **1** ثم اضغط على **دخول** لتثبيت جهاز CounterACT قياسي.

يتم تهيئة الإعداد. قد يستغرق ذلك بضع لحظات.

6. يتم فتح خيار موجه وضع الترخيص. حدد وضع الترخيص الذي يستخدمه النشر الخاص بك. يتم تحديد وضع الترخيص أثناء عملية الشراء. ***لا تقم بكتابة أي من القيم حتى يتم التحقق من وضع الترخيص الذي تستخدمه عملية النشر***. اتصل بممثل شركة فورسكوت للتحقق من وضع الترخيص الخاص بك أو في حال قيامك بإدخال الوضع الخاطئ.

7. في موجه "إدخال وصف جهاز"، قم بإدخال نص قصير يحدد هذا الجهاز، ثم اضغط على **دخول**.

يتم عرض ما يلي:

```
>>>>>> تعيين كلمة مرور المسؤول <<<<<<
سوف يتم استخدام كلمة المرور هذه لتسجيل الدخول كـ "جذر" إلى نظام
تشغيل الجهاز وكـ "إداري" إلى وحدة التحكم في جهاز CounterACT.
يجب أن تحتوي كلمة المرور على ما بين 6 إلى 15 حرف بحد أقصى وأن
تحتوي على الأقل على حرف من الحروف غير الهجائية.
كلمة مرور المسؤول :
```

8. في موجه "تعيين كلمة مرور المسؤول" ، اكتب السلسلة التي تكون كلمة المرور الخاصة بك (السلسلة غير مطابقة للشاشة) ثم اضغط على **دخول**. تتم مطالبتك بتأكيد كلمة المرور. يجب أن تتألف كلمة المرور ما بين 6 إلى 15 حرفًا بحد أقصى، وأن تحتوي على الأقل على حرف من الحروف الغير هجائية.

قم بتسجيل الدخول في الجهاز كجذر، *ثم قم بالتسجيل كمسئول في* جذر وحدة التحكم (كونسول).

9. قم بكتابة اسم المضيف في موجه اسم المضيف المحدد، ثم اضغط على **دخول**. من الممكن استخدام اسم المضيف عند تسجيل الدخول في الكونسول وعرضه في الكونسول، وذلك لمساعدتك في تحديد جهاز CounterACT الذي تعرضه. يجب ألا يتجاوز اسم المضيف 13 حرفًا.

10. تقدم لك إعدادات شبكة الإعدادات الخاصة تكوين الشبكة سلسلة من معلمات التكوين. قم بكتابة قيمة ما في كل موجه، ثم اضغط على **دخول** لعرض الموجه التالية.

– تتواصل عناصر CounterACT من خلال واجهة الإدارة. يعتمد عدد واجهات الإدارة المدرج في القائمة على نموذج الجهاز.

- عنوان **Management IP address** هو عنوان واجهة الاتصال الذي تتواصل من خلاله مع عناصر CounterACT. أضف VLAN ID لواجهة الاتصال في حالة استخدام واجهة الاتصال فقط للتواصل بين مكونات CounterACT المتصلة بمنفذ محدد بعلامة.
- وفي حالة وجود أكثر من عنوان لخادم **نظام أسماء النطاقات**، فعليك وضع مسافة بين كل عنوان والآخر. تقوم معظم خوادم نظام أسماء النطاقات الداخلية بحل العناوين الداخلية والخارجية، إلا أنك قد تحتاج إلى تضمين حل خارجي لخادم نظام أسماء النطاقات. وعلى وجه التقريب، يتم تنفيذ استعلامات نظام نطاق الأسماء من خلال الجهاز الذي سيُخصَّص للعناوين الداخلية. ولذا يجب إدراج خادم نظام نطاق الأسماء الخارجي مؤخرًا.

11. يتم عرض شاشة ملخص الإعداد. يُسمح لك بإجراء اختبارات عامة تتعلق بالاتصال، أو بإعادة تكوين الإعدادات أو بإتمام عملية الإعداد. أُكتب **"D"** لإتمام عملية الإعداد.

الترخيص

بعد إتمام عملية التكوين، تأكد من توافر ترخيص صالح لدى جهاز CounterACT. تعتمد حالة الترخيص الافتراضية لجهاز CounterACT على وضع الترخيص الذي يستخدمه ويعمل عليه الجهاز.

- وفي حالة تشغيل جهاز CounterACT ***وفقًا لوضع ترخيص الجهاز***، يمكنك الآن أن تبدأ العمل باستخدام الرخصة التجريبية التي تكون صالحة لمدة 30 يومًا. وخلال هذه الفترة التجريبية، يتعين عليك استلام ترخيص دائم من شركة فورسكوت، ثم إدخاله في مجلد يُمكن الوصول إليه على حاسوبك أو على الشبكة. قم بإعداد الترخيص من هذا المكان قبل انتهاء الترخيص التجريبي الصالح لـ30 يومًا فقط. (يمكنك طلب مُلحق إلى الترخيص التجريبي إذا لزم الأمر).

  ستظهر لك رسالة تنبيهية بأن الترخيص التجريبي على وشك الانتهاء بعدة طرق. راجع *دليل إدارة CounterACT* لمزيد من المعلومات عن الرسائل التنبيهية الخاصة بالترخيص التجريبي.

  إذا كنت تعمل بنظام CounterACT الظاهري:

  - لن يتم إعداد الترخيص التجريبي بصورة تلقائية في هذه المرحلة. ويتعين عليك إعداد الترخيص التجريبي الذي استلمته من مندوب شركة فورسكوت عن طريق البريد الإلكتروني.
  - ويجب أن يكون جهاز CounterACT قادرًا على الأقل على الوصول إلى الإنترنت. يُستخدم هذا الاتصال من أجل تنشيط تراخيص CounterACT مقابل خادم ترخيص شركة فورسكوت. وسوف تصبح التراخيص، التي لا يُمكن التصديق عليها لمدة شهر واحد، غير سارية. كما سترسل CounterACT رسالة تنبيهية عبر البريد الإلكتروني، بعد يوم واحد، مفادها وجود خطأ في الاتصال بالخادم.

    راجع دليل إدارة CounterACT لمزيد من المعلومات عن إعداد جهاز CounterACT.

- في حالة تشغيل جهاز CounterACT في ***وضع الترخيص المتمركز***، يستلم *مسئول الاستحقاق* بريدًا إلكترونيًا عند إنشاء استحقاق الحصول على الترخيص، وعند توفره في بوابة عميل شركة فورسكوت. وعند توفر الترخيص، *يستطيع* الفرد المسئول عن تشغيل جهاز CounterACT تفعيل الترخيص في كونسول CounterACT. لن تعمل ميزات جهاز CounterACT بصورة صحيحة حتى تفعيل الترخيص. فعلى سبيل المثال، لن يتم تقييم السياسات ولن يتم تنفيذ أية إجراءات. *يتم إعداد ترخيص تجريبي عادي أثناء عملية إعداد النظام.*

راجع دليل إدارة CounterACT لمزيد من المعلومات حول إدارة الترخيص.

5- الإدارة عن بُعد

إعداد خادم *iDRAC*

وحدة التحكم المتكاملة في الوصول عن بُعد المدمجة المقدمة من شركة Dell هي إحدى حلول نظام الخادم المتكامل التي تحدد لك الموقع– وصول مستقل/ غير مستقل للخدمة المفعلة حول الشبكة المحلية أو الإنترنت لأجهزة CounterACT. استخدم الوحدة النمطية لتنفيذ إجراء الوصول إلى الآلة الافتراضية المعتمدة على النواة (KVM) وإعادة ضبط توصيل الجهاز بالطاقة وفصله وتنفيذ مهام استكشاف الأخطاء وإصلاحها.

قم بتنفيذ ما يلي للعمل مع وحدة iDRAC النمطية:

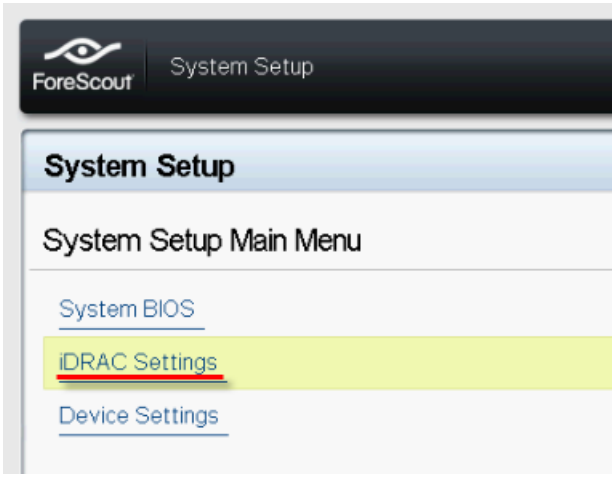
- تمكين وحدة iDRAC النمطية وتكوينها
- اتصال الوحدة النمطية بالشبكة
- تسجيل الدخول إلى iDRAC

تمكين وحدة iDRAC النمطية وتكوينها

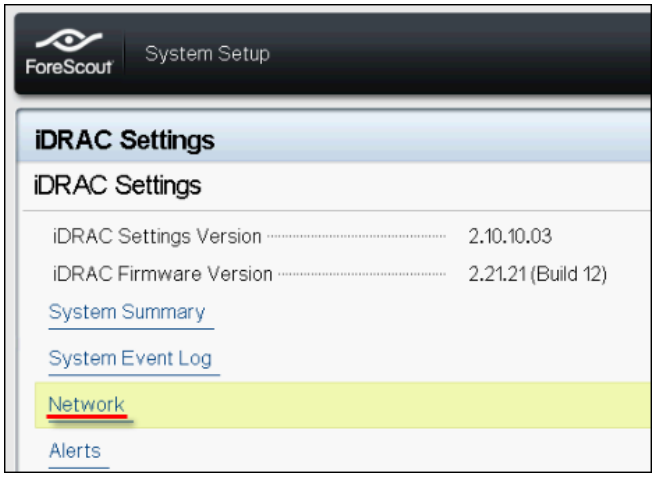
قم بتغيير إعدادات iDRAC لتمكين الوصول عن بُعد إلى جهاز CounterACT. يصف هذا القسم إعدادات التركيب الأساسية اللازمة للعمل مع جهاز CounterACT.

لتهيئة iDRAC ، اتبع ما يلي:

1. شغِّل الجهاز المستخدم.
2. اختر الشكل رقم 2 عند عملية إعادة التشغيل.
3. في الصفحة التي تظهر فيها القائمة الرئيسة لإعداد النظام، حدد **إعدادات** .**iDRAC**

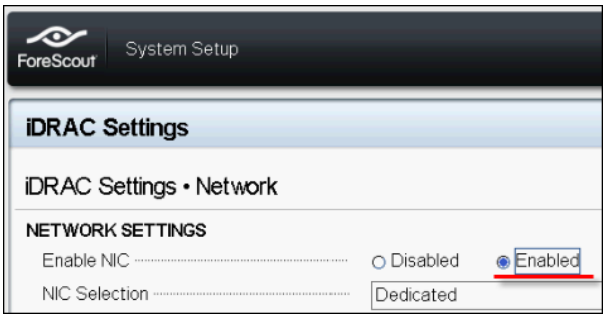


4. في صفحة إعدادات iDRAC، حدد **الشبكة**.



5. لتكوين إعدادات الشبكة، اتبع ما يلي:

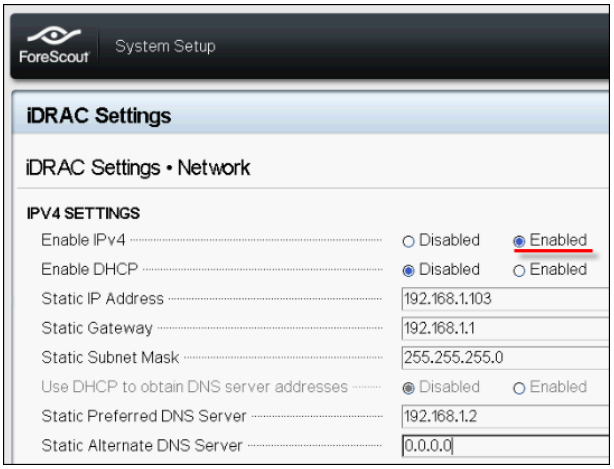
– ***إعدادات الشبكة***. تحقق من **تفعيل وحدة تحكم واجهة الشبكة** يتم تحديد حقل **مُفعَّل**.



– ***إعدادات عامة***. في الحقل الخاص بـ(DNS DARC، يمكنك تحديث (DNS) ديناميكي. (اختياري).

– ***إعدادات النسخة الرابعة من بروتوكول الإنترنت (IPv4)***. تحقق من **تفعيل IPv4** يتم تحديد حقل **مُفعَّل**.

حدد حقل **Enable DHCP** بروتوكول التهيئة الآلية للمضيفين (**DHCP**) على **"مُفعَّل"** لاستخدام عنوان IP ديناميكي أو تحديد **"غير مُفعَّل"** لاستخدام عنوان IP ثابت. في حالة التفعيل، ستخصص DHCP عنوان الـ IP بصورة تلقائية والبوابة ومهمة الشبكة الفرعية لـiDRAC. وفي حالة عدم التفعيل، قم بإدخال قيم **العنوان الثابت** و**البوابة الثابتة** وحقول **مهمة الشبكة الفرعية الثابتة**



6. حدد **"رجوع"**.

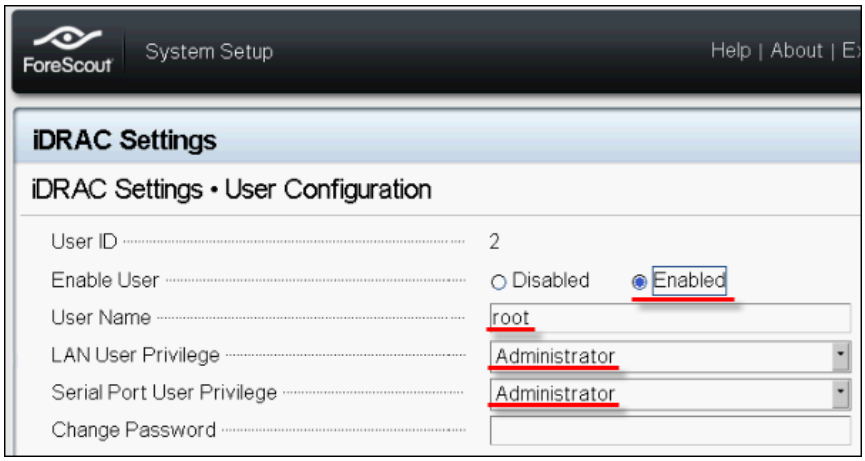
7. حدد **تكوين المستخدم**.

8. لتكوين حقول المستخدم التالية للمستخدم الجذري، اتبع ما يلي:

- ***تفعيل المستخدم***. تحقق من أن هذا الحقل محدد على وضع "مُفعَّل".

  اسم المستخدم المكوَّن هنا غيرمطابق لاسم مستخدم جهاز CounterACT.

- ***امتيازات مستخدم المنفذ التسلسلي والشبكة المحلية***. حدد مستويات الامتيازات إلى المسئول.
- ***تغيير كلمة المرور***. حدد كلمة مرور لتسجيل دخول المستخدم.



9. حدد **رجوع** ثم حدد **إنهاء**. تأكيد الإعدادات التي تم تغييرها.

يتم حفظ الإعدادات التي تم تكوينها، ثم يتم إعادة التشغيل.

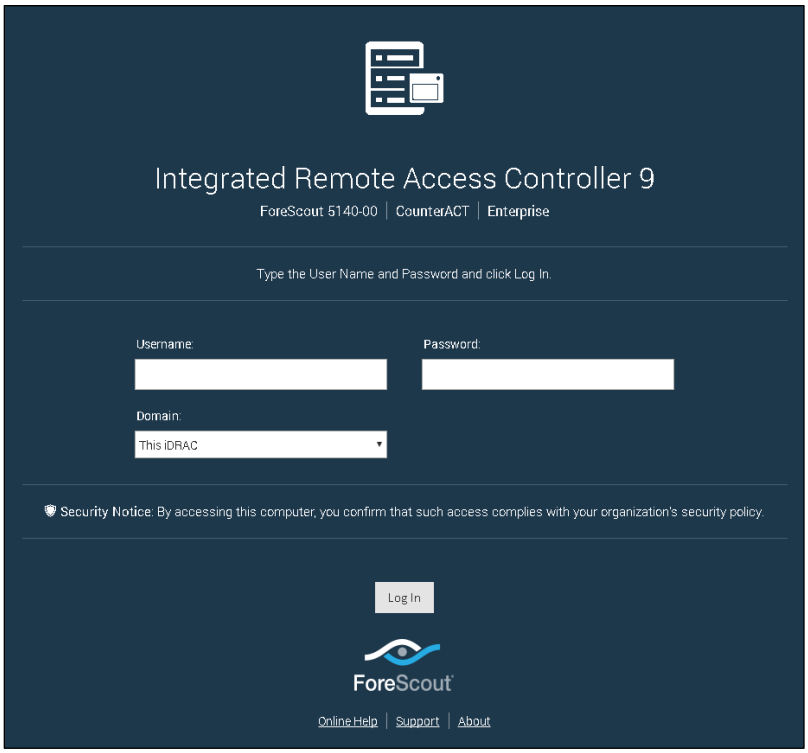
اتصال الوحدة النمطية بالشبكة

تتصل iDRAC بشبكة Ethernet. جرت العادة اتصاله بشبكة الإدارة. الصورة التالية تُظهر موقع منفذ iDRAC على اللوحة الخلفية لجهاز CT-1000:

تسجيل الدخول إلى iDRAC

لتسجيل الدخول إلى iDRAC، اتبع ما يلي:

1. قم باستعراض عنوان الـ IP أو اسم المجال المكوَّن في **إعدادات** > **iDRAC** > **الشبكة**.



2. أدخل اسم المستخدم وكلمة المرور المكونة في صفحة تكوين المستخدم لإعداد نظام iDRAC.
3. حدد **إرسال**.

لمزيد من المعلومات حول iDRAC، راجع *دليل مستخدم iDRAC*. يمكنك تصفح هذا الدليل على إحدى المواقع التالية التي تعتمد على وضع الترخيص الذي يستخدمه نظام تشغيلك:

- وفقًا لوضع ترخيص الجهاز، تجده على هذا الرابط - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- وضع الترخيص المتمركز – بوابة العميل، صفحة الوثائق.

راجع وثائق إضافية لجهاز CounterACT (*تعريف وضع الترخيص في الكونسول*) لإيجاد وضع الترخيص الذي يستخدمه نظام تشغيلك.

يُعَدُّ تحديث كلمة المرور الجذرية الافتراضية أمرًا هامًا في حالة عدم تحديثها.

6- التحقق من الاتصال

التحقق من اتصال واجهة اتصال الإدارة

لاختبار اتصال الواجهة بالإدارة، قم بتسجيل الدخول إلى الجهاز وأدخل الأمر التالي:

fstool linktest

تظهر المعلومات التالية كما يلي:

```
حالة واجهة اتصال الإدارة
التحقق من معلومات البوابة الافتراضية
إحصائيات أداة اختبار الاتصال
تنفيذ اختبار تحليل الاسم
ملخص الاختبار
```

تنفيذ اختبار على أداة الاختبار

أدخل الأمر التالي من الجهاز إلى سطح مكتب الشبكة للتحقق من الاتصال:

Ping <network_desktop_IP_address>

7- إعداد كونسول CounterACT

تثبيت كونسول *CounterACT*

الكونسول هو تطبيق تشغيل جهاز CounterACT الذي يتم استخدامه لعرض معلومات تفصيلية ذات أهمية عن النقاط النهائية والتحكم فيها. ويتم الحصول على هذه المعلومات من خلال أجهزة CounterACT. ولمزيد من المعلومات، *راجع* دليل إدارة جهاز CounterACT.

يتعين عليك تزويد برنامج تطبيق جهاز كونسول CounterACT المضيف بجهاز ما. المتطلبات اللازمة للجهاز، على الأقل، هي:

- جهاز غير مخصص يقوم بتشغيل هذه الأنظمة، وهي:
  - Windows 7/8/8.1/10
  - خادم أنظمة بإصدارات 2008/2008 R2/2012/2012 R2/2016
  - نظامي Linux RHEL/CentOS 7
- ذاكرة وصول عشوائي (RAM) بسعة 2 جيجا بايت
- قرص بمساحة 1 جيجا بايت

الطريقة التالية متاحة لتنفيذ تثبيت الكونسول، وهي ما يلي:

استخدم تثبيت البرنامج المرفق بجهازك.

1. افتح نافذة مستعرض من الحاسوب المرفق به الكونسول.
2. اكتب ما يلي في سطر عنوان المستعرض:

   `http://<Appliance_ip>/install`

   عند مطابقة IP الجهاز لعنوان IP هذا الجهاز، يقوم المستعرض بعرض نافذة تثبيت الكونسول.
3. اتبع التعليمات عن تشغيل الشاشة.

تسجيل الدخول

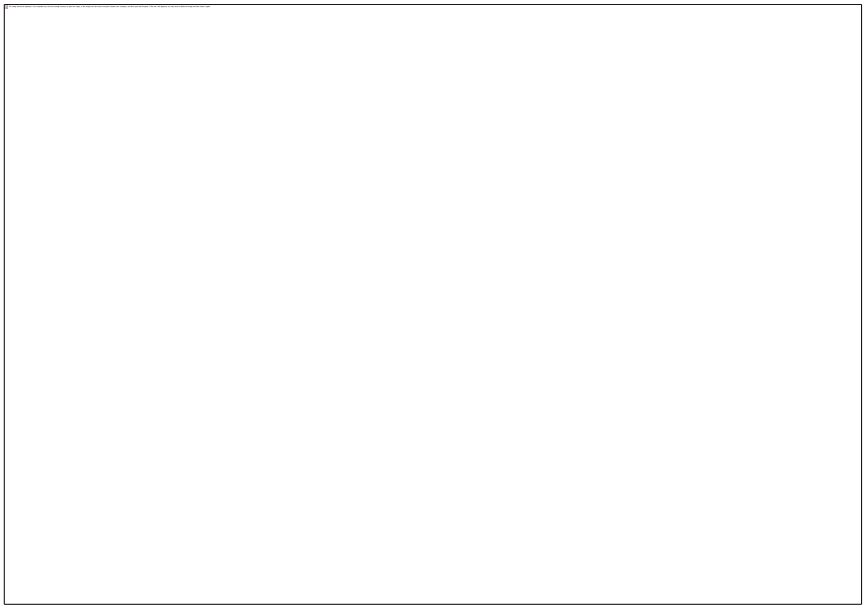
بعد الانتهاء من التثبيت، يمكنك تسجيل الدخول إلى كونسول CounterACT.

1. حدد أيقونة CounterACT من المكان المختصر الذي أنشأته.

2. أدخل عنوان الـ IP أو اسم مضيف الجهاز في حقل **"IP/Name"**
3. في حقل **"اسم المستخدم"** أدخل المسئول.
4. في حقل **كلمة المرور** أدخل كلمة المرور التي أنشأتها أثناء تثبيت الجهاز.
5. اختر **"تسجيل الدخول"** لتشغيل الكونسول.

تنفيذ عملية الإعداد الأوليّ

عند تسجيل دخولك لأول مرة، يتم فتح معالج الإعداد الأوليّ. وبعد ذلك، يُرشدك المعالج إلى خطوات التكوين الأولية لإصلاح جهاز CounterACT وتشغيله بسرعة وبكفاءة.



قبل أن تبدأ في عملية التثبيت الأوليّ، اتبع الآتي:

قدِّم المعلومات الآتية قبل العمل مع المعالج:

معلومات لازمة للمعالج	القيمة
عنوان خادم NTP مستخدَم من جانب مؤسستك.(اختياري)	
عنوان IP ترحيل بريد داخلي يسمح بإخراج الرسائل التنبيهية للبريد الإلكتروني في عدم السماح بمرور SMTP من الجهاز. (اختياري)	
عنوان البريد الإلكتروني لمسئول CounterACT	
شاشة وواجهات استجابة	
مقاطع/ VLANs التي لا تحتوي على DHCP وعلى مقطع الشبكة/ VLANs تتصل بواجهة اتصال الرد بصورة مباشرة، ويتم استخدام عنوان IP دائم من جانب جهاز CounterACT في كل عنوان مثل مدى عنوان.	
عنوان IP الذي يعرضه هذا الجهاز. (كافة العناوين الداخلية، بما في ذلك العناوين الغير مستخدمة)	
معلومات حساب مستخدم الـLDAP وعنوان IP خادم الـLDAP	
بيانات اعتماد النطاق، بما في ذلك اسم وكلمة مرور الحساب الإداري للنطاق	
خوادم المصادقة حتى يتسنى لجهاز CounterACT تحليل مضيفي الشبكة الذين تم التصديق عليهم بنجاح	
عنوان IP المُبدل ومورِّد ومعلمات SNMP	

راجع *دليل إدارة جهاز CounterACT* أو تقديم المساعدة عبر الإنترنت للحصول على معلومات بشأن العمل مع المعالج.

وثائق إضافية لجهاز CounterACT

ولمزيد من المعلومات عن الميزات والوحدات النمطية الأخرى لجهاز CounterACT، راجع المصادر التالية:

- تحميل الوثائق
- بوابة الوثائق
- أدوات مساعدة CounterACT

تحميل الوثائق

يمكن الوصول إلى تحميل الوثائق من إحدى بواباتي شركة فورسكوت، وذلك من خلال الاعتماد على الترخيص الذي يستخدمه نظام تشغيلك.

- ***وفقًا لوضع ترخيص الجهاز*** - بوابة تحديثات المنتج
- ***وضع الترخيص المتمركز*** - بوابة العميل

يُمكن تحميل البرامج من هذه البوابات.

ولمعرفة الترخيص الذي يستخدمه نظام تشغيلك، راجع تعريف وضع الترخيص في الكونسول.

بوابة تحديثات المنتج

تُقدم بوابة تحديثات المنتج ارتباطات بها إصدارات متنوعة لجهاز CounterACT وبقاعدة وبوحدات نمطية ووثائق أخرى ذات صلة. وتقوم البوابة أيضًا بتقديم مجموعة إضافية من الوثائق

وللوصول إلى بوابة تحديثات المنتج، اتبع ما يلي:

1. راجع هذه الروابط: https://updates.forescout.com/support/index.php?url=counteract.
2. حدد إصدار جهاز كونتراكت الذي ترغب في اكتشافه.

بوابة العميل

تقوم صفحة التحميلات الموجودة على بوابة عميل شركة فورسكوت بتزويد الارتباطات إلى إصدارات جهاز CounterACT التي تم شراؤها، وتزويدها كذلك بقاعدة وبوحدات نمطية للمحتوى وبوثائق أخرى ذات صلة. سوف تظهر البرامج والوثائق الأخرى ذات الصلة على صفحة التحميلات، وذلك إذا كان لديك رخصة الانتفاع بالبرنامج. كما تقوم الوثائق الموجودة على البوابة بتقديم مجموعة إضافية من الوثائق.

وللوصول إلى الوثائق المعروضة على بوابة عملاء شركة فورسكوت، اتبع الآتي:

1. طالع الروابط الآتية: https://forescout.force.com/support/.
2. حدد **"التنزيلات"** أو **الوثائق**.

بوابة الوثائق

بوابة وثائق شركة فورسكوت هي مكتبة متاحة على الإنترنت يمكن البحث فيها. كما تحتوي على معلومات تخص أدوات CounterACT وميزاتها ووظيفتها وتركيبها.

إذا كان نظام تشغيلك يستخدم وضع الترخيص المتمركز، فلا يجوز لك الحصول على اعتمادات النطاق للوصول إلى هذه البوابة.

وللوصول إلى الوثائق المعروضة على بوابة عميل شركة فورسكوت، اتبع ما يلي:

1. طالع: www.forescout.com/docportal.
2. استخدم اعتمادات نطاق الدعم الخاصة بعميلك لتسجيل الدخول.
3. حدد إصدار جهاز كونتراكت الذي ترغب في اكتشافه.

أدوات مساعدة CounterACT

تصفَّح المعلومات بصورة مباشرة من كونسول CounterACT.

أزرار مساعدة كونسول

استخدم أزرار تعليمات تتبع السياق *للتصفح* السريع للمعلومات عن المهام والموضوعات التي تعمل عليها.

دليل إدارة جهاز CounterACT

حدد **زر المساعدة** في استخدام جهاز CounterACT **من القائمة التي يظهر عليها** كلمة "مساعدة".

ملفات تعليمات أداة التوصيل

1. بعد تثبيت أداة التوصيل، حدد **"خيارات"** من قائمة **"أدوات"** ثم حدد **"وحدات نمطية"**.
2. حدد أداة التوصيل، ثم حدد **"مساعدة"**.

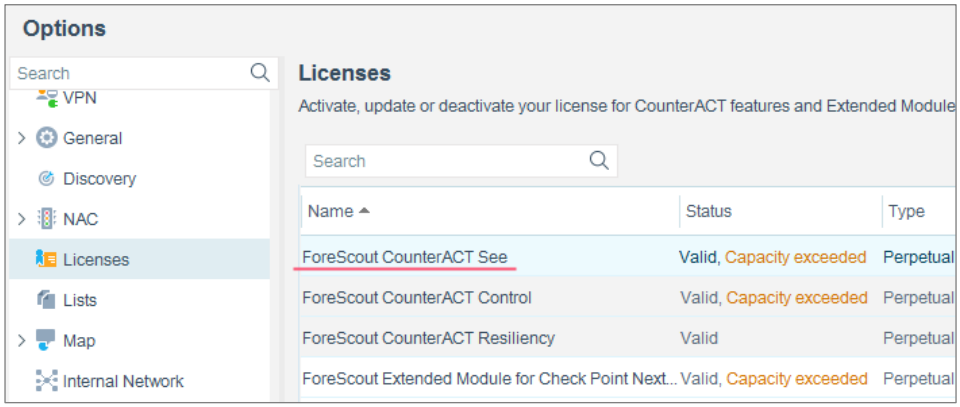
بوابة الوثائق

حدد **بوابة الوثائق** من قائمة **"مساعدة"**

تعريف وضع الترخيص في الكونسول

إذا كان مدير المشروع لديه جهاز CounterACT *راجع* النسخة المدرجة في الكونسول، نظرًا لأن نظام التشغيل الخاص بك يعمل في وضع الترخيص المتمركز . وفي حالة عدم حصوله على الجهاز، فإن نظام التشغيل يعمل وفقًا لوضع ترخيص الجهاز.

حدد **"خيارات" > تراخيص** لمعرفة إذا ما كان *جهاز CounterACT، راجع* الرخصة المدرجة في الجدول.



تواصل مع مندوب شركة فورسكوت إذا كان لديك أية استفسارات تتعلق بتعريف وضع الترخيص الخاص بك.

إخطار قانوني

هذه المنتجات قائمة على البرامج التي تطورها شركة فورسكوت. ويجوز حماية المنتجات الواردة في هذه الوثيقة من خلال واحدة أو أكثر من براءات الاختراع التالية التابعة للولايات المتحدة: #6,363,489, #8,254,286, #8,590.004, #8,639,800 و#9,027,079 ويجوز حمايتها ببراءات الاختراع التابعة للولايات المتحدة والجهات الأجنبية الأخرى.

أرسل تعليقاتك واستفساراتك عن هذه الوثيقة على هذا الرابط: support@forescout.com

2018-03-2715:02