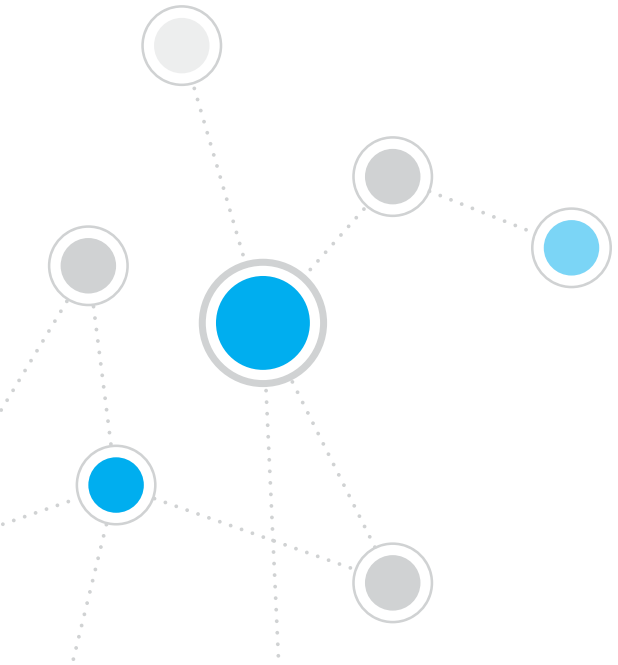
ForeScout

ForeScout CounterACT® 7

Egymagában álló CounterACT készülék

Rövid telepítési útmutató



Tartalomjegyzék

Üdvözli a ForeScout CounterACT® 7 verzió

A ForeScout CounterACT egy fizikai, illetve virtuális adatbiztonsági készülék, amely dinamikusan azonosítja és kiértékeli a hálózati eszközöket és alkalmazásokat, amint azok a hálózatára kapcsolódnak. Mivel a CounterACT nem igényel ügynököket, az az eszközeivel működik együtt, legyen szó akár kezelt vagy nem kezelt, ismert vagy ismeretlen, beágyazott vagy virtuális eszközről, illetve PC-ről vagy mobileszközről. A CounterACT gyorsan meghatározza a felhasználót, a tulajdonost, az operációs rendszert, az eszközkonfigurációt, a szoftvert, a szolgáltatásokat, a javítócsomagok telepítésének állapotát, valamint a biztonsági ügynökök jelenlétét. Ezután javítást, ellenőrzést és folyamatos felügyeletet biztosít ezen eszközökhöz, ahogy azok a hálózatra csatlakoznak, illetve leválnak arról. Mindezt úgy teszi, hogy közben tökéletesen beépül az Ön meglévő informatikai infrastruktúrájába.

Ebben az útmutatóban ismertetjük az önmagában álló CounterACT készülék telepítését.

Ha részletesebben szeretne tájékozódni vállalati méretű hálózatok védelmét biztosító több készülék telepítéséről, olvassa át a *CounterACT telepítési útmutatóját* és a *Console felhasználói kézikönyvét*. Ezeket a dokumentumokat a CounterACT CD /docs könyvtárában találja.

Ezenkívül elnavigálhat a támogató webhelyre is: https://www.forescout.com/support, ahol készülékéhez megtalálhatja a legfrisebb dokumentációt, tudásbázis-cikkeket és frissítéseket.

A CounterACT csomag tartalma

- CounterACT készülék
- Rövid telepítési útmutató
- CounterACT CD a Console szoftverével, a CounterACT Console felhasználói kézikönyve és telepítési útmutató
- Garancialevél
- Szerelőkeretek
- Tápkábel
- DB9 Console csatlakozókábele (csak soros csatlakozásokhoz)

Áttekintés

A CounterACT beállítását a következő módon végezze:

1. Telepítési terv készítése
2. A switch beállítása
3. A hálózati kábelek és a tápkábel csatlakoztatása
4. A készülék konfigurálása
5. Távoli kezelés
6. Kapcsolódás ellenőrzése
7. A CounterACT Console beállítása

1. Telepítési terv készítése

A telepítés előtt el kell döntenie, hová kívánja telepíteni a készüléket, és meg kell ismerkednie a készülék interfészeinek csatlakoztatásaival.

A készülék telepítési helyének meghatározása

A készülék hálózati helyének helyes megválasztása a CounterACT sikeres telepítéséhez és optimális teljesítményéhez létfontosságú. A megfelelő hely függ attól, milyen célokat kíván megvalósítani, illetve függ az Ön hálózati hozzáférési szabályzataitól. A készüléknek képesnek kell lennie a szabályzat szempontjából lényeges forgalom figyelemmel kísérésére. Ha például az Ön szabályzata szerint a végpontokból a vállalati hitelesítő szerverekbe menő hitelesítési eseményeket kell figyelemmel kísérni, a készüléket úgy kell telepíteni, hogy lássa a végpontokból a hitelesítő szerver(ek)be áramló forgalmat.

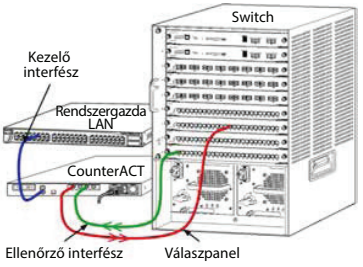
A telepítésről bővebb tájékoztatást a CounterACT telepítési útmutatójában, a csomagban mellékelt CounterACT CD-n talál.

A készülék interfészeinek csatlakoztatása

A készülék általában úgy van konfigurálva, hogy a hálózati switch-hez három csatlakozással rendelkezik.

Kezelő interfész

Ezzel az interfésszel kezelheti a CounterACT készüléket, végezhet lekérdezéseket és mélyrehatóan felügyelheti a végpontokat. Az interfészt a switch olyan portjára kell csatlakoztatni, amelynek a hálózat minden végpontjához van hozzáférése.



EMinden egyes készülék egyetlen kezelő-csatlakozást igényel a hálózathoz. Ehhez a csatlakozáshoz szükséges egy IP cím a helyi LAN hálózaton és 13000/TCP port hozzáférés a gépektől, amelyek a CounterACT Console kezelési alkalmazását fogják futtatni. A kezelő interfésznek hozzáféréssel kell bírnia a hálózaton a következőkhöz:

Port	Szolgáltatás	A CounterACThoz vagy a CounterACT-tól	Funkció
22/TCP	SSH	-hoz	Hozzáférést enged a CounterACT parancssor-interfészhez.
2222/TCP			(Magas rendelkezésre állás) Hozzáférést enged a fizikai CounterACT eszközökhöz, amelyek a magas rendelkezésre állású klaszter részei. 22/TCP használata a klaszter megosztott (virtuális) IP címéhez való hozzáférésre.

Port	Szolgáltatás	A CounterACThoz vagy a CounterACT-tól	Funkció
25/TCP	SMTP	-tól	A CounterACT-ról történő e-mail küldésre használható.
53/UDP	DNS	-tól	Lehetővé teszi belső IP címek feloldását a CounterACT számára.
80/TCP	HTTP	-hoz	HTTP átirányítást tesz lehetővé.
123/UDP	NTP	-tól	A CounterACT számára hozzáférést enged egy NTP időszerverhez. A CounterACT alapértelmezés szerint ezt használja: ntp.foreScout.net.
135/TCP	MS-WMI	-tól	Lehetővé teszi Windows végpontok távoli vizsgálatát.
139/TCP	SMB, MS-RPP	-tól	Lehetővé teszi Windows végpontok távoli vizsgálatát (Windows 7 vagy korábbi rendszert futtató végpontok esetén).
445/TCP			Lehetővé teszi Windows végpontok távoli vizsgálatát.
161/UDP	SNMP	-tól	Lehetővé teszi, hogy a CounterACT kommunikáljon a hálózati infrastruktúra részeivel, például switchekkel és routerekkel. Az SNMP konfigurálásáról tájékozódhat a *CounterACT Console felhasználói kézikönyvében*.
162/UDP	SNMP	-hoz	Lehetővé teszi, hogy a CounterACT SNMP-jelzéseket kapjon a hálózati infrastruktúra részeitől, például switchektől és routerektől. Az SNMP konfigurálásáról tájékozódhat a *CounterACT Console felhasználói kézikönyvében*.
443/TCP	HTTPS	-hoz	TLS-t használó HTTP átirányítást tesz lehetővé.
2200/TCP	Secure Connector	-hoz	Lehetővé teszi, hogy a SecureConnector létrehozzon egy biztonságos (SSH titkosítású) csatlakozást a készülékhez Macintosh/Linux gépektől. A *SecureConnector* egy script alapú ügynök, amely lehetővé teszi Macintosh és Linux végpontok kezelését, miközben azok a hálózatra kapcsolódnak.
10003/TCP	Secure Connector Windowshoz	-hoz	Lehetővé teszi, hogy a SecureConnector létrehozzon egy biztonságos (TLS titkosítású) csatlakozást a készülékhez a Windows gépektől. A *SecureConnector* egy ügynök, amely lehetővé teszi Windows végpontok kezelését, miközben azok a hálózatra kapcsolódnak. A SecureConnectorról bővebb tájékoztatást a CounterACT Console felhasználói kézikönyvében olvashat.

			Ha a SecureConnector egy készülékhez vagy az Enterprise Managerhez kapcsolódik, az átirányításra kerül ahhoz a készülékhez, amelyhez a gazdagépe hozzá van rendelve. Biztosítsa, hogy ez a port nyitva legyen minden készülék és az Enterprise Manager számára, hogy átlátható mobilitást tegyen lehetővé a szervezeten belül.
13000/TCP	CounterACT	-hoz	Csatlakozást tesz lehetővé a Console-tól a készülékhez. Több CounterACT-ből álló rendszereknél csatlakozást tesz lehetővé a Console-tól az Enterprise Managerhez és az Enterprise Managertől minden egyes készülékhez.

Ellenőrző interfész

Ez a csatlakozás biztosítja, hogy a készülék ellenőrizze és nyomon kövesse a hálózati forgalmat.

A forgalom a switch egyik portjára tükröződik, és a készülék nyomon követi. A tükrözött VLAN-ok számától függ, hogy a forgalom 802.1Q VLAN-címkézett-e vagy nem.

- **Egyedüli VLAN (címkézetlen):** Amikor egyedüli VLAN-ról generálódik ellenőrzött forgalom, a tükrözött forgalomnak nem kell VLANcímkézettnek lennie.
- **Több VLAN (címkézett):** Amikor egynél több VLAN-ról generálódik ellenőrzött forgalom, a tükrözött forgalomnak 802.1Q VLAN-címkézettnek kell lennie.

Amikor két switch redundáns párként van csatlakoztatva, a készüléknek figyelnie kell mindkét switchről érkező forgalmat.

Az ellenőrző interfésznek általában nem szükséges IP cím.

Válaszpanel

A készülék válaszol ennek az interfésznek a forgalmára. A válaszforgalom a rosszindulatú tevékenységek elleni védelemre és a NAC szabályzat szerinti intézkedések kivitelezésére használatos. Ilyen intézkedés lehet például webböngészők átirányítása vagy tűzfal blokkolás. Az adott switch port konfigurálása az ellenőrzés alatt lévő forgalomtól függ.

- **Egyedüli VLAN (címkézetlen):** Amikor az ellenőrzött forgalom egyedüli VLAN-ról generálódik, a válaszadaptert úgy kell konfigurálni, hogy ugyanazon VLAN része legyen. Ez esetben a készülék egyetlen IP címet igényel azon a VLAN-on.
- **Több VLAN (címkézett):** IfHa az ellenőrzött forgalom egynél több VLANról generálódik, a válaszadaptert 802.1Q címkézéssel kell konfigurálni ugyanazokra a VLAN-okra. A készülék minden egyes védett VLAN-hoz igényel IP címet.

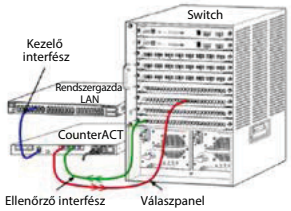
2. A switch beállítása

A. A switch csatlakoztatási lehetőségei

A készülék úgy van tervezve, hogy gond nélkül beépüljön sokféle hálózati környezetbe. Ahhoz, hogy a készülék sikeresen beépüljön az Ön hálózatába, ellenőrizze, hogy a switch be van-e állítva a kívánt forgalom ellenőrzéséhez.

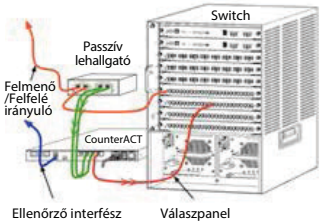
A készülék több módon csatlakoztatható a switch-hez.

1. **Szokványos telepítés (külön kezelő, ellenőrző és válaszadapterek)**
   TAz ajánlott telepítéshez három különálló port szükséges. Ezeknek a portoknak az ismertetése *A készülék interfészeinek csatlakoztatása alatt található.*

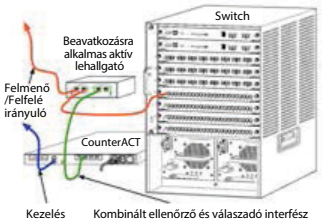


2. **Passzív beépített lehallgató**
   A switch ellenőrző portjára való csatlakoztatás helyett a készülék passzív beépített lehallgatóval is képes működni.

   A passzív beépített lehallgató két ellenőrző portot igényel, kivéve a lehallgatók „újrakombinálásának“ esetét, amikor a két duplex áramlás egyetlen portra van kombinálva. A forgalmat a lehallgatóval ellátott porton és a válaszadapteren ugyanúgy kell konfigurálni. Ha például a lehallgatott porton a forgalom VLAN-címkézett (802.1Q), a válaszadapternek is VLANcímkézett portnak kell lennie.



3. **Aktív (beavatkozásra alkalmas) beépített lehallgató**
   Amikor a készülék *beavatkozásra alkalmas* beépített lehallgatóval működik, az ellenőrző és a válaszadapterek kombinálhatók. Nem szükséges a switchen külön válaszadó portot konfigurálni. Ez a lehetőség bármilyen típusú fel- vagy lefelé irányuló switch-konfigurációhoz használható.



4. **IP réteg válasz (3 rétegű switchekhez)**
   A készülék képes saját kezelő interfészét használni a forgalomra történő válaszadáshoz. Bár ez a lehetőség használható bármilyen ellenőrzött forgalomnál, akkor ajánlatos a használata, amikor a készülék olyan portokat ellenőriz, amelyek nem részei semmilyen VLAN-nak, azaz a készülék nem képes bármilyen más switch portot használó forgalom ellenőrzésére. Két routert összekötő kapcsolat ellenőrzésénél ez tipikus.

   Ez az opció címfeloldó protokoll (ARP) kéréseire nem képes válaszolni, ami korlátozza a készüléknek azt a képességét, hogy felderítse az ellenőrzött alhálózaton lévő IP címekre irányuló kereséseket. Ez a korlátozás nem áll fenn két router közötti forgalom ellenőrzésénél.

B. Megjegyzések a switch beállításához

VLAN (802.1Q) címkék

- **Egyedüli VLAN (címkézetlen forgalom) ellenőrzése** Egyedüli VLANról jövő forgalom ellenőrzéséhez nem szükségesek 802.1Q címkék.
- **Több VLAN (címkézett forgalom) ellenőrzése** Két vagy több VLAN-ról jövő forgalom esetén *mind* az ellenőrző, *mind* a válaszadapterek 802.1Q címkézést igényelnek. Több VLAN ellenőrzésénél ez az opció az ajánlott, mivel a legjobb teljes lefedettséget adja, miközben minimalizálja a tükröző portok számát.
- Ha a switch nem képes 802.1Q VLAN címke használatára a tükröző portokon, a következőt tegye:
  - Csak egyetlen VLAN-t tükrözzön
  - Csak egy, címkézetlen, felmenő portot tükrözzön
  - Használja az IP réteg válaszadási lehetőséget
- Ha a switch csak egy portot képes tükrözni, akkor egy felmenő portot tükrözzön. Ez lehet címkézett. Általában, ha a switch ledobja a 802.1Q VLAN címkéket, az IP réteg válaszadási lehetőséget kell használnia.

További információk

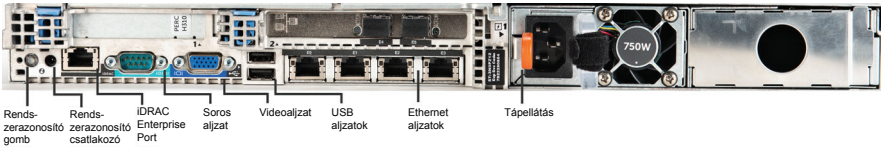
- Ha a switch nem képes mind a küldött, mind a kapott forgalmat ellenőrizni, akkor ellenőrizze az egész switchet, a teljes VLAN-okat (ez küldést/vételt biztosít), vagy csak egy interfészt (amelyik küldést/vételt lehetővé tesz). Ellenőrizze, hogy nem terheli-e túl a tükröző portot.
- Némelyik switchnél (ilyen például a Cisco 6509) szükséges lehet a korábbi portkonfigurációk teljes törlése az új konfigurációk bevitele előtt. Ha a régi port-adatokat nem törlik ki, annak az a leggyakoribb következménye, hogy a switch ledobja a 802.1Q címkéket.

3. Hálózati kábelek csatlakoztatása és bekapcsolás

A. A készülék és a csatlakozó kábelek kicsomagolása

1. Vegye ki a készüléket és a tápkábelt a gyári csomagolásából.
2. Távolítsa el a készülékhez mellékelt sínkészletet.
3. Szerelje a sínkészletet a készülékre, és a készüléket szerelje az állványhoz.
4. Csatlakoztassa a készülék hátlapján lévő hálózati interfészek és a switch portok közötti hálózati kábeleket.

A hátlap képe — CounterACT készülék



B. Az interfész hozzárendelések rögzítése

Miután végzett a készülék telepítésével az adatközpontnál, illetve a CounterACT Console telepítésével, az interfész hozzárendelések regisztrálására felszólító üzenetet fog kapni. Ezek a hozzárendelések, amelyeket csatorna-kijelölésnek nevezünk, bekerülnek a Kezdőbeállítások varázslóba, amely akkor nyílik meg, amikor először bejelentkezik a Console-ba.

Rögzítse az alábbi fizikai interfész hozzárendeléseket, és használja őket, amikor a Console-on a csatorna-beállítást végzi.

Ethernet interfész	Interfész hozzárendelés (pl. kezelő, ellenőrző, válaszadó)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. A készülék bekapcsolása

1. Csatlakoztassa a tápkábelt a készülék hátlapján lévő tápcsatlakozó aljzatra.
2. A tápkábel másik végét dugaszolja egy földelt váltakozó áramú konnektorra.
3. Csatlakoztassa a billentyűzetet és a monitort a készülékhez, vagy állítsa a készüléket soros kapcsolódásra. Lásd a *CounterACT telepítési útmutatóját* a CounterACT CD-n.
4. Kapcsolja be a készüléket az előlapon.

Fontos: Kapcsolja ki a gépet, mielőtt a konnektorból kihúzná!

4. A készülék konfigurálása

A készülék konfigurálása előtt készítse elő a következő adatokat.

□ A készülék neve	
□ A CounterACT rendszergazdai jelszava	**A jelszót biztonságos helyen tartsa**
□ Kezelő interfész	
□ A készülék IP címe	
□ Hálózati maszk	
□ Alapértelmezett átjáró IP címe	
□ DNS tartomány neve	
□ DNS kiszolgáló címei	

Bekapcsolás után a konfigurálás kezdésére felkérő üzenetet kap:

```
A CounterACT készülék betöltése kész.
A folytatáshoz nyomja meg az <Enter> gombot.
```

1. Nyomja meg az **Enter** gombot a következő menü megjelenítéséhez:

```
1) A CounterACT konfigurálása
2) Mentett CounterACT konfiguráció visszaállítása
3) Hálózati interfészek azonosítása és
   újraszámozása
4) Billentyűzet-kiosztás konfigurálása
5) A gép kikapcsolása
6) A gép újraindítása
Kiválasztva (1-6) :1
```

2. Válassza az **1-et** – A CounterACT konfigurálása. A figyelemfelhívó üzenet:

   `Folytatás: (igen/nem)?`

   Nyomja meg az **Enter** gombot a beállítás inicializálásához.

3. A **`Magas rendelkezésre állás mód`** menü megnyílik. Az **Enter** gombbal válassza a Szokványos telepítést.
4. A **`CounterACT kezdőbeállítása`** üzenet jelenik meg. A folytatáshoz nyomja meg az **Enter** gombot.
5. A **`CounterACT telepítési típusa`** menü nyílik meg. Billentyűzzön be **1-et**, majd nyomja meg az **Enter** gombot a CounterACT készülék szokványos telepítéséhez. A telepítés inicializálódik. Ez eltarthat egy ideig.

6. A **`Gép leírásának bevitele`** üzenetnél vigyen be a készüléket azonosító rövid szöveget, majd nyomja meg az **Enter** gombot. A következő jelenik meg:

```
>>>>>> Rendszergazdai jelszó beállítása <<<<<<

Ezzel a jelszóval lehet „root"-ként a gép
operációs rendszerébe és „rendszergazda"-ként
a CounterACT Console-ba bejelentkezni.
A jelszónak 6 és 15 közötti karakterből kell
állnia, és legalább egy nem-alfabetikus
karaktert kell tartalmaznia.

Rendszergazdai jelszó:
```

7. A **`Rendszergazdai jelszó beállítása`** üzenetnél billentyűzze be a jelszónak szánt karakterláncot (a karakterlánc nem látható a képernyőn), majd nyomja meg az **Enter**. gombot. Egy üzenet a jelszó megismétlésére kéri fel. A jelszónak 6 és 15 közötti karakterből kell állnia, és legalább egy nem-alfabetikus karaktert kell tartalmaznia.

   Jelentkezzen be a készülékbe rootként, majd jelentkezzen be a Consoleba rendszergazdaként.

8. **`A készülék nevének beállítása`** üzenetnél billentyűzzön be egy készüléknevet, és nyomja meg az **Enter** gombot. A készülék neve használható a Console-ba történő bejelentkezésnél, és a Consoleon meg is jelenik, segítve ezzel annak a CounterACT készüléknek az azonosítását, amelyiket éppen figyeli.

9. A **`Hálózati beállítások konfigurálása`** képernyőn üzenetek figyelmeztetik egy sor konfigurációs paraméterre. Billentyűzzön be egy számot minden üzenetnél, és nyomja meg az **Enter** gombot a folytatáshoz.
   - A CounterACT komponensei kezelő interfészeken keresztül kommunikálnak. A felsorolt kezelő interfészek száma a készülék típusától függ.
   - **Kezelő IP címe** annak az interfésznek a címe, amelyen keresztül a CounterACT komponensei kommunikálnak. Csak akkor adjon VLAN azonosítót ehhez az interfészhez, ha a CounterACT komponensei közötti kommunikációra használt interfész címkézett portra van csatlakoztatva.
   - Ha egynél több **DNS kiszolgáló cím** van, szóközzel válassza el az egyes címeket—A legtöbb belső DNS kiszolgáló feloldja a külső és belső címeket, de előfordulhat, hogy szükség van egy külső címeket feloldó DNS kiszolgáló beiktatására. Mivel a készülék által végzett majdnem minden DNS lekérdezés belső címeket fog érinteni, a külső DNS kiszolgálónak kell a listában az utolsónak lennie.

10. A **`Beállítások összegzése`** képernyő jelenik meg. Egy üzenet általános kapcsolódási tesztek elvégzésére, beállítások újrakonfigurálására vagy a beállítás befejezésére kéri fel. Billentyűzzön be **D**-t a beállítás befejezéséhez.

Licenc

Telepítés után a CounterACT képviselője által rendelkezésére bocsátott kezdeti demo licencet kell telepítenie. A licenc a Console kezdőbeállítása közben telepítődik. Ez a kezdeti demo licenc bizonyos számú napig érvényes. Ezen időszak lejárta előtt állandó licencet kell telepítenie. A lejárat dátumáról e-mailben fog értesítést kapni. Ezenkívül, a lejárat dátumát és a licenc státuszát tartalmazó információ megjelenik a Console-on, a Készülékek/ Eszközök mezőben.

Amint megkapta az állandó licencet, a ForeScout licenc-szervere azt naponta érvényesíti. Licenccel és kihágásokkal kapcsolatos figyelmeztető jelzések az Eszköz részletei mezőben jelennek meg.

Az egy hónapra nem érvényesíthető licencek visszavonásra kerülnek. A licencekről részletesebb tájékoztatást a CounterACT telepítési útmutatójában talál.

Hálózati kapcsolódás követelményei

Legalább egy CounterACT eszköznek (készülék vagy Enterprise Manager) kell internet kapcsolattal rendelkeznie. Ez a kapcsolat a CounterACT licenceknek a ForeScout licenc szervere általi érvényesítésére használatos.

Az egy hónapra nem hitelesíthető licencek visszavonásra kerülnek. A CounterACT naponta küld e-mailt, jelezve, hogy a szerverrel kommunikációs hiba áll fenn.

5. Távoli kezelés

Az iDRAC beállítása

Az integrált Dell távoli hozzáférés-vezérlő (iDRAC) egy integrált szerverrendszer, amely helytől és operációs rendszertől függetlenül távoli hozzáférést biztosít a LAN-on vagy az interneten keresztül a CounterACT készülékekhez/Enterprise Managerekhez. A modult KVM hozzáféréshez, be- és kikapcsoláshoz, alaphelyzetbe állításhoz, valamint hibaelhárítási és karbantartási munkákhoz használja.

A következőket tegye, hogy dolgozhasson az iDRAC modullal:

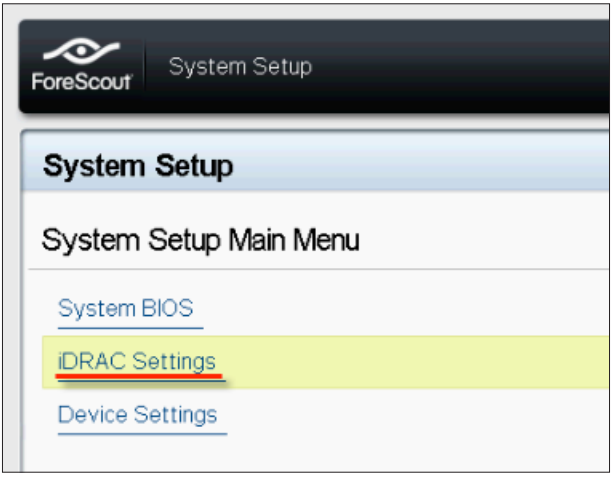
- *Engedélyezze és konfigurálja az iDRAC modult*
- *Csatlakoztassa a modult a hálózatra*
- *Jelentkezzen be az iDRAC modulba*

Engedélyezze és konfigurálja az iDRAC modult

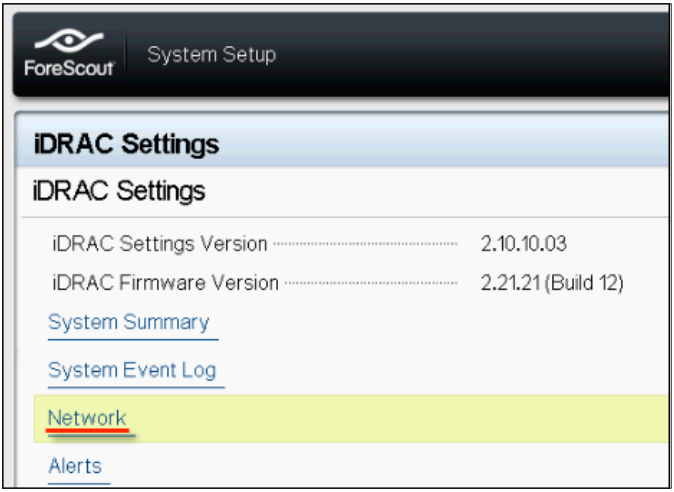
Változtassa meg az iDRAC beállításait, hogy lehetővé tegye a távoli hozzáférést a CounterACT eszközön. Ebben a fejezetben találja a CounterACTtel való munkavégzéshez szükséges alapvető integrációs beállítások leírását.

Az iDRAC konfigurálása:

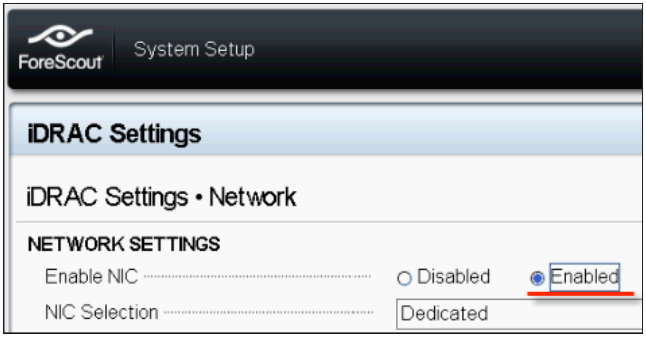
1. Kapcsolja be a kezelt rendszert.
2. A bekapcsolási önellenőrzés (POST) közben válassza az F2-t.
3. A Rendszerbeállító főmenü oldalon válassza ezt: **iDRAC beállítások**.



4. Az iDRAC beállítások oldalon válassza ezt: **Hálózat**.

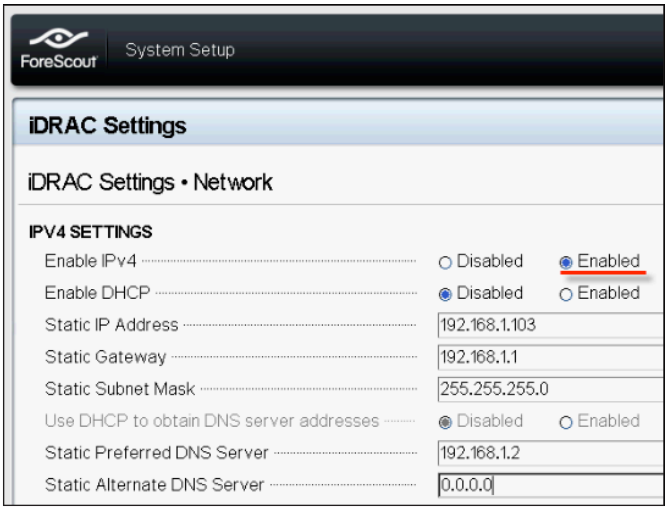


5. Konfigurálja a következő hálózati beállításokat:
   - ***Hálózati beállítások.*** Ellenőrizze, hogy a **NIC engedélyezése** mező **Engedélyezve** opcióra van-e állítva.

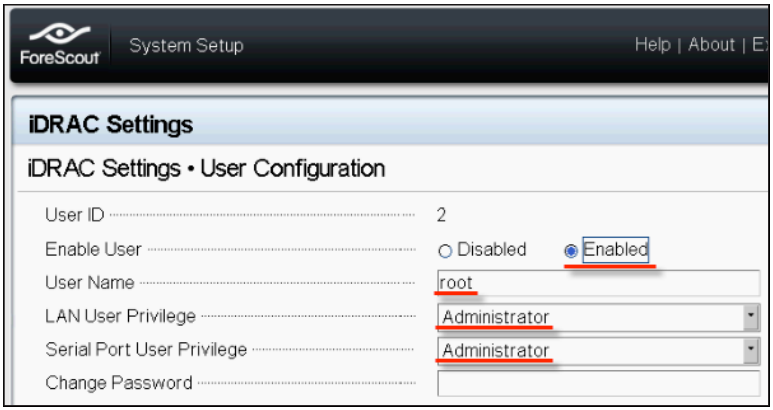


   - ***Általános beállítások.*** A DNS DRAC név mezőben frissíthet egy dinamikus DNS-t (választható).

- ***IPV4 beállítások.*** Ellenőrizze, hogy az **IPv4 engedélyezése** mező **Engedélyezve** opcióra van-e állítva. Állítsa a **DHCP engedélyezése** mezőt **Engedélyezve** opcióra dinamikus IP címhez vagy Letiltva opcióra statikus IP címhez. Ha engedélyezve van, a DHCP automatikusan hozzárendeli az IP címet, átjárót és alhálózati maszkot az iDRAC modulhoz. Ha le van tiltva, vigyen be számokat a **Statikus IP cím, Statikus átjáró** és **Statikus alhálózati maszk** mezőkbe.



6. Válassza a **Vissza** lehetőséget.
7. Válassza a **Felhasználói konfiguráció** lehetőséget.
8. Konfigurálja a következő Felhasználói konfiguráció mezőket:
   - ***Felhasználó engedélyezése.*** Ellenőrizze, hogy ez a mező Engedélyezve opcióra van-e állítva.
   - ***Felhasználói név.*** Vigyen be egy felhasználói nevet.
   - ***LAN és soros port felhasználói jogosultságok.*** Állítsa a jogosultságot Rendszergazda opcióra
   - **Jelszó megváltoztatása.** Állítson be egy jelszót a felhasználó bejelentkezéséhez.



9. Válassza a **Vissza**, majd a **Befejezés** opciót. Erősítse meg a módosított beállításokat. A hálózati beállításokat ezzel elmentette, és a rendszer újraindul.

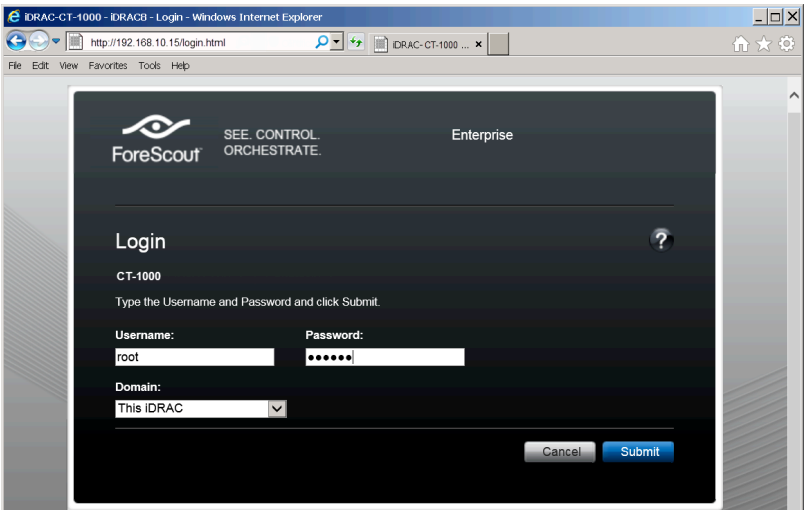
Csatlakoztassa a modult a hálózatra

Az iDRAC az Ethernet hálózatra kapcsolódik. Szokás szerint kezelő hálózatra csatlakoztatják. A következő képen az iDRAC port elhelyezkedése látható a CT-1000 készülék hátlapján:

Jelentkezzen be az iDRAC modulba

Az iDRAC modulba történő bejelentkezéshez:

1. Navigáljon az **iDRAC beállítások > Hálózat** lehetőséghez.



2. Vigye be Az iDRAC rendszer beállítása Felhasználói konfiguráció oldalán megadott felhasználói nevet és jelszót.
3. Válassza a **Küldés** lehetőséget.

Az iDRAC modulról további tájékoztatást az iDRAC felhasználói útmutatójában talál.

Nagyon fontos az alapértelmezett hitelesítő adatok frissítése.

6. Kapcsolódás ellenőrzése

A kezelő interfész kapcsolódásának ellenőrzése

A kezelő interfész kapcsolódásának ellenőrzéséhez jelentkezzen be a készülékbe, és futtassa a következő parancsot:

```
fstool linktest
```

A következő információ jelenik meg:

```
Kezelő interfész státusza
Alapértelmezett átjáró adatainak pingelése
Pingelési statisztika
Névfeloldási teszt végzése
Teszt összegzése
```

A switch/készülék kapcsolódásának ellenőrzése

Mielőtt elhagyja az adatközpontot, ellenőrizze, hogy a switch helyesen van-e csatlakoztatva a készülékhez. Ehhez futtassa az fstool ifcount parancsot a készüléken minden egyes észlelt interfésznél.

```
fstool ifcount eth0 eth1 eth2
```
(Az egyes interfészeket szóközzel válassza el.)

Ez az eszköz folyamatosan megjeleníti a hálózati forgalmat a megadott interfészeken. Két módon működik: interfészenként vagy VLAN-onként. A mód a kijelzőről változtatható. A következő forgalmi kategóriák mindegyikének teljes másodpercenkénti bitszáma és százalékaránya látható:

- Az ellenőrző interfésznek elsősorban a tükrözött forgalmat kell látnia — 90% felett.
- A válaszpanelnek főleg a broadcast forgalmat kell látnia.
- Mind az ellenőrző mind a válaszpanelnek látnia kell az elvárt VLAN-okat.

Parancs opciók:

```
v – kijelző VLAN módban
I – kijelző interfész módban
P – előző mutatása
N – következő mutatása
q – kilépés a megjelenítésből
```

VLAN mód:

```
update=[4]       [eth3: 14 vlans]
Interfész/Vlan   teljes  broadcast  forgalma   *Saját     *Saját
                                    tükrözve   MAC-hoz    MAC-tól
eth3.címkézetlen 4 Mbps  0,2%       99,8%      0,0%       0,0%
eth3.1           9 Mbps  0,0%       100,0%     0,0%       0,0%
eth3.2           3 Mbps  0,1%       99,9%      0,0%       0,0%
eth3.4           542 bps 100,0%     0,0%       0,0%       0,0%
eth3.20          1 Kbps  100,0%     0,0%       0,0%       0,0%
Mutat: [v]lans [i]nterfaces <-[p]rev [n]ext->      [q]uit
```

Interfész mód:

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interfész/Vlan   teljes  broadcast  forgalma   *Saját     *Saját
                                    tükrözve   MAC-hoz    MAC-tól
eth0             3 Kbps  42,3%      0,0%       14,1%      43,7%
eth1             475 bps 0,0%       100,0%     0,0%       0,0%
```

*Saját MAC-hoz — Cél-MAC a készülék MAC címe.

*Saját MAC-tól — A készülék által küldött forgalom (forrás-MAC a készülék MAC címe. A cél lehet broadcast vagy unicast).

Ha semmilyen forgalmat nem észlel, ellenőrizze, működőképes-e az interfész. Használja a készüléknél a következő parancsot:

`ifconfig [interface name] up`

Ping teszt elvégzése

Futtasson ping tesztet a készüléktől a hálózati desktophoz a kapcsolódás ellenőrzése végett.

A teszt futtatása:

1. Jelentkezzen be a készülékbe.
2. Futtassa a következő parancsot: **`Ping [network desktop IP]`**
   Alapértelmezés szerint maga a készülék nem válaszol a pingelésre.

7. A CounterACT Console beállítása

A CounterACT Console telepítése

A CounterACT Console központi kezelő alkalmazás, amellyel figyelhető, nyomon követhető és elemezhető a készülék által érzékelt tevékenység. A Console-lal NAC, fenyegetések elleni védelem, tűzfal és egyéb szabályok állíthatók fel. Bővebb tájékoztatást a *CounterACT Console felhasználói kézikönyvében* talál.

A CounterACT Console alkalmazásszoftver telepítéséhez biztosítani kell egy számítógépet. A minimális hardverkövetelmények:

- Nem-dedikált számítógép a következő operációs rendszerrel:
  - Windows XP, Windows Vista vagy Windows 7
  - Windows Server 2003 vagy Server 2008
  - Linux
- Pentium 3, 1GHz-es processzor
- 2 GB memória
- 1 GB szabad lemezterület

A Console telepítésének két módja van:

Használja a készülékbe épített telepítő szoftvert.

1. Nyisson meg egy böngészőablakot a Console számítógépben.
2. Írja be a következőt a böngésző címsorába:
   http://<Appliance ip>/install
   Ahol <Appliance ip> ennek a készüléknek az IP címe. A böngésző megjeleníti a Console telepítési ablakát.
3. Kövesse a képernyőn megjelenő utasításokat.

Telepítse a CounterACT CD-ROM-ról

1. Illessze a CounterACT CD ROM-ot a DVD meghajtóba.
2. Nyissa meg a **ManagementSetup.htm** fájlt a CD ROM-ról a böngészővel.
3. Kövesse a képernyőn megjelenő utasításokat.

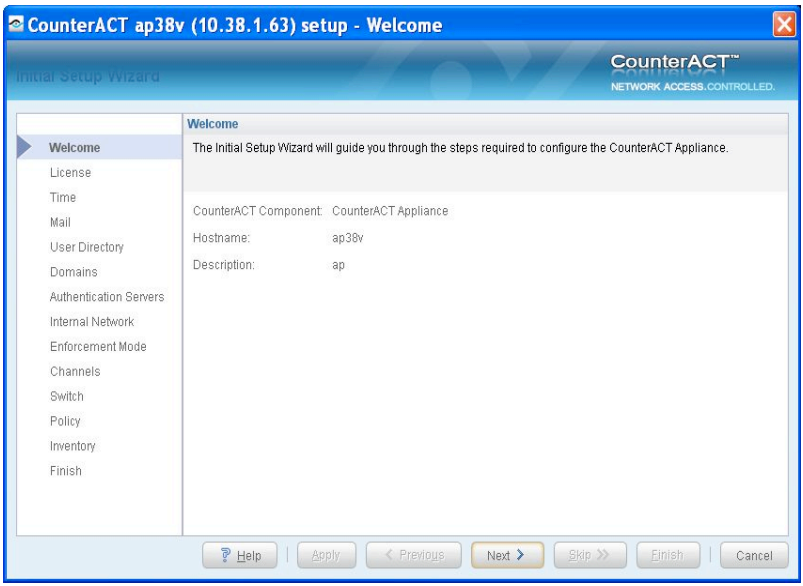
Bejelentkezés

A telepítés befejezése után bejelentkezhet a CounterACT Console-ba.

1. Válassza a CounterACT ikont az Ön által létrehozott parancsikonhelyről.
2. Vigye be a készülék IP címét vagy készüléknevét az **IP/Név** mezőbe.
3. A **Felhasználói név** mezőbe vigye be ezt: **admin**.
4. A **Jelszó** mezőbe vigye be a jelszót, amelyet a készülék telepítése közben létrehozott.
5. Válassza a **Bejelentkezés** opciót a Console indításához.

Kezdőbeállítás elvégzése

Az első bejelentkezés után megjelenik a Kezdőbeállítás varázsló. A varázsló végigvezeti Önt a lényeges konfigurációs lépéseken, hogy a CounterACT működőképes legyen, gyorsan és hatékonyan működjön.



A kezdőbeállítás indítása előtt

A készülék konfigurálása előtt készítse elő a következő adatokat:

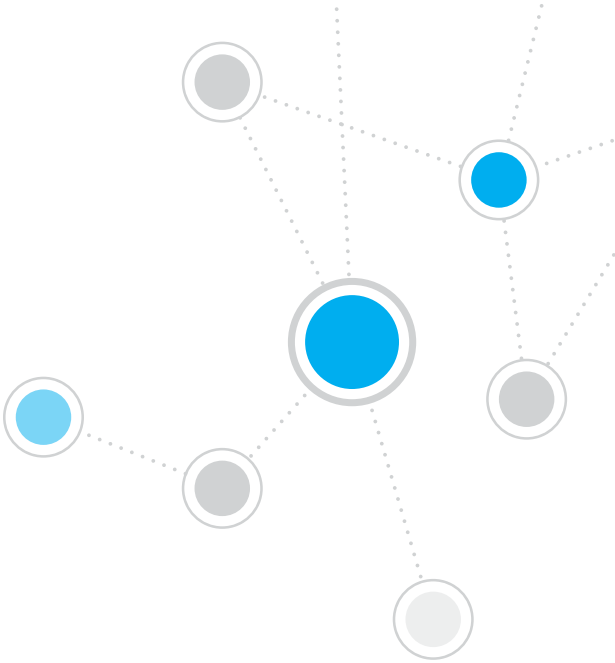
Adatok	Számértékek
☐ Az Ön szervezete által használt NTP szerver címe (választható).	
☐ Belső levélkezelő IP címe. Ez lehetővé teszi e-mail küldését a CounterACT-ről, ha SMTP forgalom nincs engedélyezve a készülékről (választható).	
☐ A CounterACT rendszergazdai e-mail címe.	
☐ Az adatközpontnál meghatározott ellenőrző és válaszpanel hozzárendelések.	
☐ DHCP nélküli szegmensekhez vagy VLAN-okhoz, a hálózati szegmens vagy VLAN-ok, amelyekhez az ellenőrző interfész közvetlenül kapcsolódik, és egy állandó IP cím, amelyet a CounterACT használ minden ilyen VLAN-nál. Ez az adat nem kötelező az Enterprise Manager beállításához.	
☐ IP cím tartományok, amelyeket a Készülék védeni fog (minden belső cím, a használaton kívülieket is beleértve).	
☐ Felhasználói könyvtár fiókjainak adatai és a Felhasználói könyvtár szerver IP címei.	
☐ Tartomány hitelesítő adatai, a tartomány rendszergazdai fiókjának nevét és jelszavát is beleértve.	
☐ Hitelesítő szerverek, hogy a CounterACT képes legyen elemezni, mely hálózatgazdák vannak sikeresen hitelesítve.	
☐ Core switch IP címe, vendor és SNMP paraméterek.	

A varázsló működtetéséről tájékoztatást talál a *CounterACT Console felhasználói kézikönyvében* vagy az internetes súgóban.

Kapcsolatfelvétel

Műszaki támogatásért a ForeScout következő címére küldjön e-mailt: support@forescout.com, vagy hívja a következő telefonszámok egyikét:

- Ingyenesen hívható (US): 1.866.377.8771
- Telefon (nközi): 1.408.213.3191
- Támogatás: 1.708.237.6591
- Fax: 1.408.371.2284



ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Ingyenesen hívható (US): 1.866.377.8771
Telefon (nközi): 1.408.213.3191
Támogatás: 1.708.237.6591
Fax: 1.408.371.2284

400-00020-01