



ForeScout CounterACT[®] 7

Enkel CounterACT-enhet

Snabbinstallationsguide

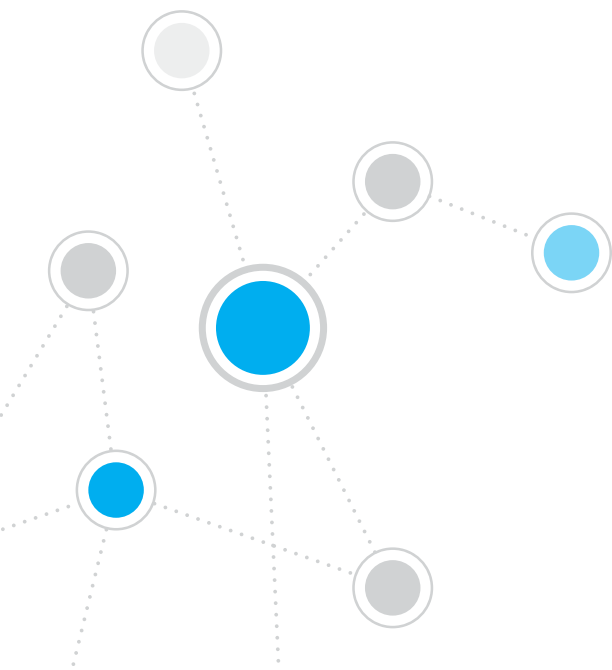


Table of Contents

Välkommen till ForeScout CounterACT® version 7	3
Ditt CounterACT-paket innehåller	3
Översikt	4
1. Skapa en driftsättningsplan	5
Besluta var enheten ska driftsättas	5
Enhetens gränssnittsanslutningar	5
2. Installation av switchen	8
A. Alternativa switchanslutningar	8
B. Inställning av switch – anmärkningar	9
3. Anslut nätverkskablar och slå på strömmen	10
A. Packa upp enheten och anslut kablar	10
B. Registrera gränssnittstilldelningarna	11
C. Slå på strömmen till enheten	11
4. Konfigurera enheten	12
5. Fjärrhantering	15
Installation av iDRAC	15
6. Verifiera anslutningen	19
Verifiera hanteringsgränssnittets anslutning	19
Verifiera switchens/enhetens anslutning	19
Utför pingtest	20
7. Installera CounterACT-konsolen	21
Installera CounterACT-konsolen	21
Logga in	22
Gör första installationen	22
Kontaktuppgifter	24

Välkommen till ForeScout CounterACT® version 7

ForeScout CounterACT är en fysiskt eller virtuell säkerhetsenhet som på ett dynamiskt sätt identifierar och utvärderar nätverksenheter och -program så snart de ansluter till ditt nätverk. Eftersom CounterACT inte kräver agenter fungerar den med dina enheter – hanterade och ohanterade, kända och okända, stationära och mobila, inbäddade och virtuella. CounterACT avgör snabbt ägare, användare, operativsystem, enhetskonfiguration, programvara, tjänster, uppdateringsstatus och om det finns några säkerhetsagenter. Därefter förser den dig med reparation, kontroll och löpande övervakning av dessa enheter varje gång de lämnar och ansluter till nätverket. Den gör allt detta samtidigt som den sömlöst integrerar med all befintlig IT-infrastruktur.



Denna guide beskriver installationen av en enskild fristående CounterACT-enhet.

Om du vill ha mer utförlig information eller information om att driftsätta flera enheter för skydd av företagsomfattande nätverk hänvisar vi till *Installationsguide till CounterACT och Användarmanual till konsolen*. Dessa dokument finns i CounterACT-CD-skivan i /docs-katalogen.

Du kan också gå till webbplatsen för support som finns på: <https://www.forescout.com/support> för senaste dokumentation, kunskapsbasartiklar och uppdateringar till din enhet.

Ditt CounterACT-paket innehåller

- CounterACT-enhet
- Snabbinstallationsguide
- CounterACT-CD-skiva med Console-programvara, Användarmanual och Installationsguide till CounterACT-konsolen
- Garantisedel
- Monteringsfästen
- Strömkabel
- DB9-kabel för anslutning till konsolen (endast för seriella anslutningar)

Översikt

Du installerar CounterACT på följande sätt:

1. Skapa en driftsättningsplan
2. Installera switchen
3. Anslut nätverkskablar och ström
4. Konfigurera enheten
5. Fjärrhantering
6. Verifiera anslutningen
7. Installera CounterACT-konsolen

1. Skapa en driftsättningsplan

Innan du påbörjar installationen måste du besluta var du vill driftsätta enheten och lära dig om enhetens gränssnittsanslutningar.

Besluta var enheten ska driftsättas

Val av korrekt nätverksplats för apparaten är avgörande för lyckad driftsättning och optimal prestanda i CounterACT. Korrekt plats beror på dina önskade implementeringsmål och nätverksåtkomstpolicyer. Enheten ska kunna övervaka den trafik som är relevant för den önskade policyn. Till exempel, om din policy är avhängig av övervakning av autentiseringshändelser från slutpunkter till företagets autentiseringsservrar måste enheten installeras på ett sådant sätt att den ser slutpunktstrafik strömma in i autentiseringsservrarna.

Om du vill ha mer information om installation och driftsättning går du till Installationsguiden för CounterACT som finns i CounterACT-CD-skivan som medföljer detta paket.

Enhetens gränssnittsanslutningar

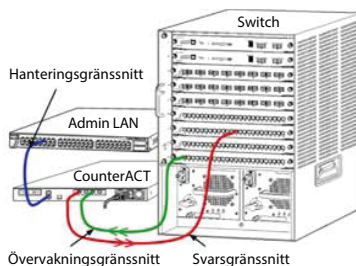
Enheten konfigureras i allmänhet med tre anslutningar till nätverksswitchen.

Hanteringsgränssnitt

I detta gränssnitt kan du hantera CounterACT och göra förfrågningar och djupinspektioner av slutpunkter. Gränssnittet måste vara anslutet till en switchport som har åtkomst till alla nätverksslutpunkter.

Varje enhet kräver en enskild hanteringsanslutning till nätverket.

Denna anslutning kräver en IP-adress i det lokala nätverket (LAN) och åtkomst med port 13000/TCP från datorer som ska köra CounterACT-konsolens hanteringsprogram. Hanteringsgränssnittet måste ha åtkomst till följande i ditt nätverk:



Port	Service	Till eller från CounterACT	Funktion
22/TCP	SSH	Till	Tillåter åtkomst till CounterACTs kommandogränssnitt.
2222/TCP			(Hög tillgänglighet) Tillåter åtkomst till de fysiska CounterACT-enheter som är del av klustret för hög tillgänglighet. Använd 22/TCP för att få åtkomst till klustrets delade (virtuella) IP-adress.

Port	Service	Till eller från CounterACT	Funktion
25/TCP	SMTP	Från	Används för att skicka e-post från CounterACT.
53/UDP	DNS	Från	Tillåter CounterACT att matcha interna IP-adresser.
80/TCP	HTTP	Till	Tillåter HTTP-omdirigering.
123/UDP	NTP	Från	Ger CounterACT åtkomst till en NTP-tidserver. Med standardinställningen använder CounterACT ntp.foreScout.net.
135/TCP	MS-WMI	Från	Tillåter fjärrinspektion av Windows-slutpunkter.
139/TCP	SMB, MS-RPP	Från	Tillåter fjärrinspektion av Windows-slutpunkter (för slutpunkter som kör Windows 7 och tidigare).
445/TCP			Tillåter fjärrinspektion av Windows-slutpunkter.
161/UDP	SNMP	Från	Tillåter CounterACT att kommunicera med infrastrukturutrustning i nätverket, t.ex. switchar och routrar. För information om att konfigurera SNMP hänvisar vi till <i>Användarmanualen till CounterACT-konsolen</i> .
162/UDP	SNMP	Till	Tillåter CounterACT att ta emot SNMPtraps från infrastrukturutrustning i nätverket, t.ex. switchar och routrar. För information om att konfigurera SNMP hänvisar vi till <i>Användarmanualen till CounterACT-konsolen</i> .
443/TCP	HTTPS	Till	Tillåter HTTP-omdirigering med hjälp av TLS.
2200/TCP	Secure Connector	Till	Tillåter SecureConnector att skapa en säker (krypterad SSH) anslutning från Macintosh-/Linux-datorer. <i>SecureConnector</i> är en skriptbaserad agent som möjliggör hantering av slutpunkter i Macintosh och Linux när de är anslutna till nätverket.
10003/TCP	Secure Connector för Windows	Till	Tillåter SecureConnector att skapa en säker (krypterad TLS) anslutning till enheten från Windows-datorer. <i>SecureConnector</i> är en skriptbaserad agent som möjliggör hantering av slutpunkter i Macintosh och Linux när de är anslutna till nätverket. Läs mer om SecureConnector i <i>Användarmanual till CounterACT-konsolen</i> .

			När SecureConnector ansluter till en enhet eller till Enterprise Manager omdirigeras den till den enhet som dess värd har tilldelats. Kontrollera att porten är öppen för alla program och Enterprise Manager för att tillåta genomskinlig mobilitet inom organisationen.
13000/TCP	CounterACT	Till	Tillåter anslutning från konsolen till enheten. I system med flera CounterACT-enheter tillåter den anslutning från konsolen till Enterprise Manager och från Enterprise Manager till respektive enhet.

Övervakningsgränssnitt

Denna anslutning tillåter enheten att övervaka och spåra nätverkstrafik.

Trafik speglas till en port på switchen och övervakas av enheten. Beroende på antalet virtuella lokala nätverks (VLAN) som speglas kan trafiken eventuellt vara 802.1Q VLAN-taggad.

- **Enkelt VLAN (otaggat):** När övervakad trafik genereras från ett enkelt virtuellt lokalt nätverk behöver den speglade trafiken inte vara VLAN-taggad.
- **Flera virtuella lokala nätverk (VLAN) (taggade):** När övervakad trafik kommer från mer än ett VLAN *måste* den speglade trafiken vara 802.1Q VLAN-taggad.

När två switchar är anslutna som ett redundanta par måste enheten övervaka trafik från båda switcharna.

Övervakningsgränssnittet kräver ingen IP-adress.

Svarsgränssnitt

Enheten svarar på trafik med hjälp av den här gränssnittet. Svarstrafik används för att skydda mot skadlig aktivitet och för att utföra NAC-policyåtgärder. Sådana åtgärder kan till exempel vara omdirigering av webbläsare eller blockering med brandvägg. Den relaterade konfigurationen av switchporten beror på trafiken som övervakas.

- **Enkelt VLAN (otaggat):** När övervakad trafik genereras från ett enkelt VLAN måste svarsgränssnittet vara konfigurerat till att vara en del av samma VLAN. I det här fallet kräver enheten en enkel IP-adress i det virtuella lokala nätverket.
- **Flera virtuella lokala nätverk (taggade):** Om övervakad trafik kommer från mer än ett VLAN måste svarsgränssnittet också vara konfigurerat med 802.1Q-tagging för samma VLAN:er. Enheten kräver en IP-adress för vart och ett av de skyddade virtuella lokala nätverken.

2. Installation av switchen

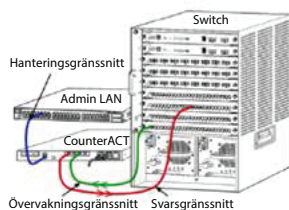
A. Alternativa switchanslutningar

Enheten är utformad för att kunna integreras sömlöst i en rad olika nätverksmiljöer. För att kunna integrera enheten med ditt nätverk ska du kontrollera att switchen är inställd för att övervaka relevant trafik.

Det finns flera olika alternativ för anslutning av enheten till switchen.

1. Standarddriftsättning (separata gränssnitt för hantering, övervakning och svar)

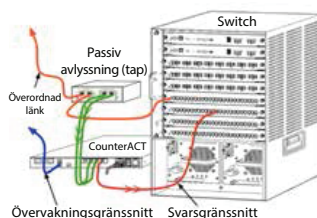
Den rekommenderade driftsättningen använder tre separata portar. Dessa portar beskrivs i *Enhetens gränssnittsanslutningar*.



2. Passiv nätverksavlyssning (inline tap)

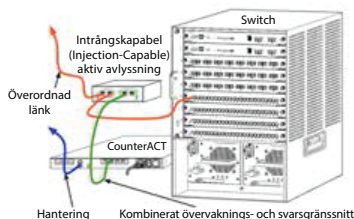
I stället för att anslutas till en övervakningsport på switchen kan enheten använda passiv nätverksavlyssning.

Passiv avlyssning kräver två övervakningsportar, utom då det gäller "recombination" -avlyssning, vilket kombinerar de dubbla strömmarna till en enkel port. Trafiken i den avlyssnade porten och i svarsgränssnittet måste vara konfigurerad på samma sätt. Om till exempel trafiken i den avlyssnade porten är VLAN-taggad (802.1Q) måste också svarsgränssnittet vara en VLAN-taggad port.



3. Aktiv (Injection-Capable) nätverksavlyssning

När enheten använder en nätverksavlyssning som är *intrångskapabel* (injection capable) kan övervaknings- och svarsgränssnitten kombineras. Det finns inget behov av att konfigurera en separat svarsport på switchen. Detta alternativ kan användas till alla typer av uppströmsoch nedströmskonfigurationer för switchen.



4. IP-skiktsvar (för switchinstallation i skikt 3)

Enheten kan använda sitt eget hanteringsgränssnitt till att svara på trafik. Även om detta alternativ kan användas med all övervakad trafik rekommenderas det när enheten övervakar portar som inte är en del av något VLAN, och då kan enheten inte svara på övervakad trafik med hjälp av någon annan switchport. Det gäller i normalfallet när enheten övervakar en länk som ansluter två routrar.

Detta alternativ kan inte svara på begäranden från Address Resolution Protocol (ARP), vilket begränsar enhetens förmåga att upptäcka skannar riktade mot de IP-adresser som ingår i det övervakade undernätet. Denna begränsning gäller inte när trafik mellan två routrar övervakas.

B. Inställning av switch – anmärkningar

VLAN-taggar (802.1Q)

- **Övervakning av enkelt VLAN (otaggad trafik)** Om den övervakade trafiken kommer från ett enkelt VLAN behöver trafiken inte 802.1Q-taggar.
- **Övervakning av flera VLAN:er (taggad trafik)** Om den övervakade trafiken kommer från två eller flera VLAN:er måste *både* övervakningsoch svarsgränssnittet ha 802.1Q-taggningsaktiverad. Övervakning av flera VLAN:er är det rekommenderade alternativet eftersom det ger den bästa totala täckningen samtidigt som det minimerar antalet speglade portar.
- Om switchen inte kan använda en 802.1Q VLAN-tagga till de speglade portarna gör du ett av följande:
 - Spegla endast ett enkelt VLAN
 - Spegla en enkel, otaggad överordnad länkport
 - Använd alternativet IP-skiktsvar
- Om switchen bara kan spegla en port speglar du en enkel överordnad länkport. Denna kan taggas. Om switchen tar bort 802.1Q VLAN-taggar måste du vanligtvis använda IP-skiktsvarsalternativet.

Ytterligare

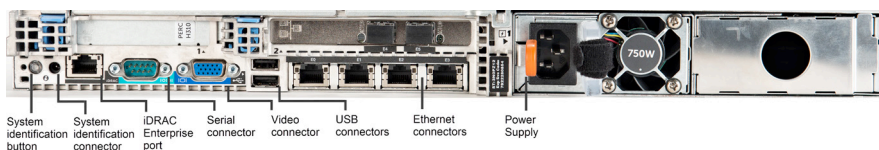
- Om switchen inte kan spegla både utgående och ingående trafik ska du övervaka hela switchen, hela VLAN:er (detta ger utgående/ingående/) eller bara ett gränssnitt (vilket tillåter utgående/ingående). Verifiera att du inte överbelastar speglingsporten.
- Vissa switchar (som Cisco 6509) kan kräva att du fullkomligt rensar tidigare portkonfigurationer innan du anger nya konfigurationer. Det vanligaste resultatet om man inte rensar bort gammal portinformation är att switchen tar bort 802.1Q-taggar.

3. Anslut nätverkskablar och slå på strömmen

A. Packa upp enheten och anslut kablar

1. Ta ut enheten och strömkabeln ur fraktbehållaren.
2. Ta bort paketet med räcken som medföljer enheten.
3. Montera räcken på enheten och fäst enheten på racket.
4. Anslut nätverkskablar mellan nätverksgränssnitten på enhetens bakre panel och switchportarna.

Bild på bakre panel – CounterACT-enhet



B. Registrera gränssnittstilldelningarna

När du har slutfört installationen av enheten i datacentret och har installerat CounterACT-konsolen blir du ombedd att registrera gränssnittstilldelningar. Dessa tilldelningar, som kallas kanaldefinitioner, ska anges i guiden till första inställning som öppnas när du loggar in på konsolen för första gången.

Registrera de fysiska gränssnittstilldelningarna nedan och använd dem när du slutför kanalinstallationen i konsolen.

Ethernet-gränssnitt	Gränssnittstilldelning (t.ex. hantering, övervakning, svar)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Slå på strömmen till enheten

1. Anslut strömkabeln till strömkontakten på enhetens bakre panel.
2. Anslut strömkabelns andra ände till ett jordat växelströmsuttag.
3. Anslut tangentbordet och övervakningen till enheten eller ställ in enheten för serieanslutning. Se *Installationsguiden till CounterACT* i CounterACT-CD-skivan.
4. Slå på strömmen på enhetens främre panel.

Viktigt: Slå av strömmen innan du drar ut kablar.

4. Konfigurera enheten

Förbered följande information innan du konfigurerar enheten.

<input type="checkbox"/> Enhetens värddamn	
<input type="checkbox"/> Admin-lösenord till CounterACT	Förvara lösenordet på ett säkert ställe
<input type="checkbox"/> Hanteringsgränssnitt	
<input type="checkbox"/> Enhetens IP-adress	
<input type="checkbox"/> Nätverksmask	
<input type="checkbox"/> Standard-IP adress till gatewayen	
<input type="checkbox"/> DNS-domännamn	
<input type="checkbox"/> DNS-serveradresser	

När du har slagit till strömmen blir du ombedd att starta konfigurationen med följande meddelande:

**CounterACT-enheten har startat.
Tryck <Retur> för att fortsätta.**

1. Tryck **Retur** för att visa följande meny:

**1) Konfigurera CounterACT
2) Återställ sparad CounterACT-konfiguration
3) Identifiera och omnumrera nätverksgränssnitten
4) Konfigurera tangentbordslayouten
5) Slå av enheten
6) Starta om enheten
Alternativ (1-6) :1**

2. Välj **1** - Konfigurera CounterACT. Vid frågan:

Fortsätta: (ja/nej)?

Tryck **Retur** för att initiera installationen.

3. Menyn **Läget hög tillgänglighet** öppnas. Tryck **Retur** för att välja Standardinstallation.
4. Dialogrutan **Första installation av CounterACT** visas. Tryck **Retur** för att fortsätta.
5. Menyn **Välj installationstyp för CounterACT** öppnas. Skriv in **1** och tryck **Retur** för att installera en CounterACT standardenhet. Installationen initieras. Detta kan ta en stund.


6. När **dialogrutan Ange enhetsbeskrivning** skriver du in en kort beskrivning av denna enhet och trycker **Retur**.
Följande visas:

>>>>> Ange administratörslösenord <<<<<

Dessa lösenord används för att logga in som "rot" i enhetens operativsystem och som "admin" i CounterACT-konsolen.

Lösenordet måste bestå av mellan 6 och 15 tecken och innehålla minst ett tecken som inte är alfabetiskt.

Administratörslösenord:

7. När du blir ombedd att **skriva in administratörslösenordet** skriver du in den sträng som ska vara ditt lösenord (strängen visas inte på skärmen) och trycker **Retur**. Du ombeds därefter bekräfta lösenordet. Lösenordet måste bestå av mellan sex och 15 tecken och innehålla minst ett icke-alfabetiskt tecken.
-  *Logga in på enheten som rot och logga in på konsolen som admin.*
8. När du blir ombedd att **ange värddatornamn** skriver du in ett värddatornamn och trycker **Retur**. Värddatornamnet kan användas när du loggar in på konsolen och visas på konsolen för att hjälpa dig att identifiera den CounterACT-enhet som visas.
9. Fönstret **Konfigurera nätverksinställningar** ber dig ange en serie konfigurationsparametrar. Skriv in ett värde för varje fråga och tryck **Retur** för att fortsätta.
- CounterACT-komponenterna kommunicerar med hjälp av hanteringsgränssnitt. Antalet listade hanteringsgränssnitt beror på enhetens modell.
 - IP-adressen **för hantering** är den adress i gränssnittet genom vilken CounterACT-komponenterna kommunicerar. Lägg till ett VLAN-ID till detta gränssnitt endast om gränssnittet som används för att kommunicera mellan CounterACT-komponenterna är anslutet till en taggad port.
 - Om det finns mer än en **DNS-serveradress** ska du separera varje adress med ett mellanslag—De flesta interna DNS-servrar matchar externa och interna adresser men du kan behöva inkludera en DNS-server som matchar externa adresser. Eftersom nästan alla DNS-förfrågningar som görs av enheten gäller interna adresser ska den externa DNS-servern listas sist.
10. Fönstret **Installationssammanfattning** visas. Du blir ombedd att utföra allmänna anslutningstester, att omkonfigurera inställningar eller att slutföra installationen. Skriv in **D** för att slutföra installationen.

Licens

Efter installationen måste du installera den ursprungliga demolicensen som du har fått av din CounterACT-återförsäljare. Licensen installeras under den första konsolinstallationen. Denna initiala demolicens är giltig under ett visst antal dagar. Du måste installera en permanent licens innan den här tidsperioden har löpt ut. Du kontaktas via e-post angående utgångsdatum. Dessutom visas information om utgångsdatum och statuslicensen i Konsol- Enhetsfönstret.

När du har fått en permanent licens valideras den dagligen av ForeScouts licensserver. Licensviseringar och överträdelser visas i fönstret Information om enheten.

Licenser som inte kan valideras under en månad återkallas. Se Installationsguide till CounterACT för mer information om licenser.

Krav för nätverksanslutningar

Minst en CounterACT-enhet (Appliance eller Enterprise Manager) måste ha åtkomst till internet. Denna anslutning används till att validera CounterACTlicenser mot ForeScouts licensserver.

Licenser som inte kan valideras under en månad återkallas. CounterACT skickar då ett varningsmejl en gång om dagen för att meddela att ett kommunikationsfel har uppstått med servern.

5. Fjärrhantering

Installation av iDRAC

Integrated Dell Remote Access Controller (iDRAC) är en integrerad serversystemlösning som ger dig platsoberoende/OS-oberoende fjärråtkomst över LAN:et eller internet till CounterACT-enheter/Enterprise Managers. Använd denna modul för att få åtkomst till KVM, slå av/på ström och utföra felsökningar och underhåll.

Gör följande för att jobba med iDRAC-modulen:

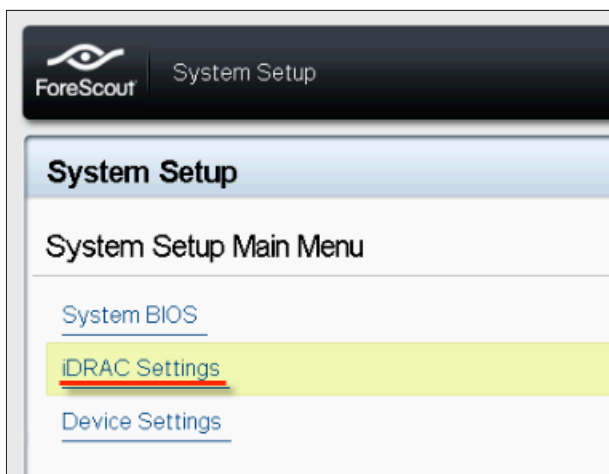
- *Aktivera och konfigurera iDRAC-modulen*
- *Anslut modulen till nätverket*
- *Logga in på iDRAC*

Aktivera och konfigurera iDRAC-modulen

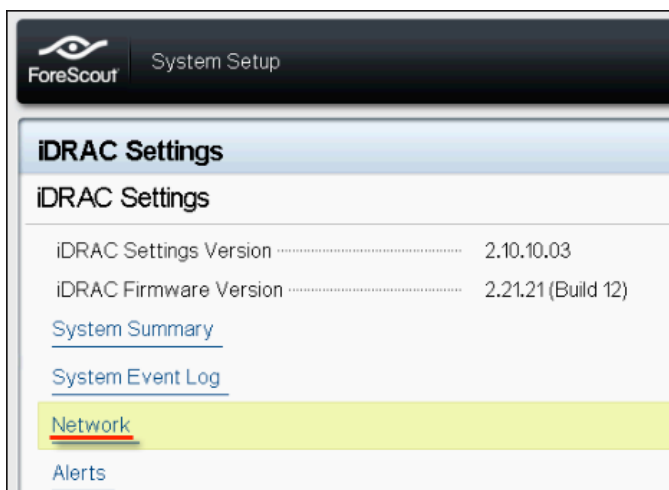
Ändra iDRAC-inställningarna för att möjliggöra fjärråtkomst på CounterACT-enheten. Detta avsnitt beskriver de grundläggande inställningar för integration som krävs för att använda CounterACT.

För att konfigurera iDRAC:

1. Slå på det hanterade systemet.
2. Välj F2 under "Ström-på-själv-testet" (Power-on Self-test (POST)).
3. På sidan Huvudmeny för systeminstallation väljer du **iDRAC-inställningar**.

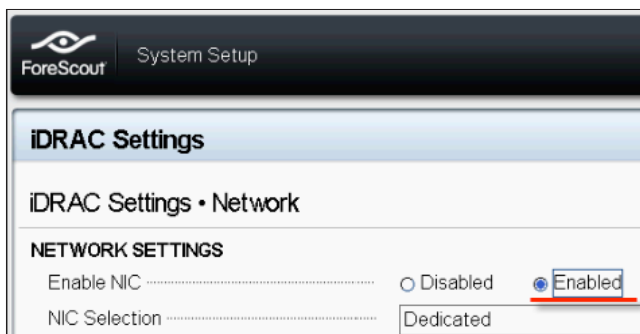


4. På sidan iDRAC-inställningar väljer du **Nätverk**.



5. Konfigurera följande nätverksinställningar:

- **Nätverksinställningar.** Verifiera att fältet **Aktivera NIC** är inställt på **Aktiverat**.



- **Allmänna inställningar.** I fältet DNS DRAC-namn kan du uppdatera en dynamisk DNS (som tillval).

- **IPv4-inställningar.** Verifiera att fältet **Aktivera IPv4** är inställt på **Aktiverat**. Ställ in fältet **Aktivera DHCP** på **Aktiverat** för att använda dynamiska IP-adresser eller på **Inaktiverat** för att använda statiska IP-adresser. Om den är aktiverad tilldelar DHCP automatiskt IP-adressen, gatewayen och undernätmasken till iDRAC7. Om den är inaktiverad anger du värden i fälten för **statisk IP-adress, statisk gateway** och **statisk subnätmask**.

ForeScout System Setup

iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> <u>Enabled</u>
Enable DHCP	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static IP Address	192.168.1.103	
Static Gateway	192.168.1.1	
Static Subnet Mask	255.255.255.0	
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static Preferred DNS Server	192.168.1.2	
Static Alternate DNS Server	0.0.0.0	

6. Välj **Tillbaka**.

7. Välj **Användarkonfigurering**.

8. Konfigurera följande fält i Användarkonfigurering:

- **Aktivera användare.** Verifiera att detta fält är inställt på Aktiverat.
- **Användarnamn.** Ange ett användarnamn.
- **Användarbehörigheter till LAN och seriell port.** Ställ in behörighetsnivåerna på Administratör.
- **Ändra lösenord.** Skriv in ett lösenord för användarinloggning.

ForeScout System Setup Help | About | E

iDRAC Settings

iDRAC Settings • User Configuration

User ID	2
Enable User	<input type="radio"/> Disabled <input checked="" type="radio"/> <u>Enabled</u>
User Name	<u>root</u>
LAN User Privilege	<u>Administrator</u>
Serial Port User Privilege	<u>Administrator</u>
Change Password	

9. Välj **Tillbaka** och välj sedan **Avsluta**. Bekräfta de ändrade inställningarna. Nätverksinställningarna har sparats och systemet startar om.

Anslut modulen till nätverket

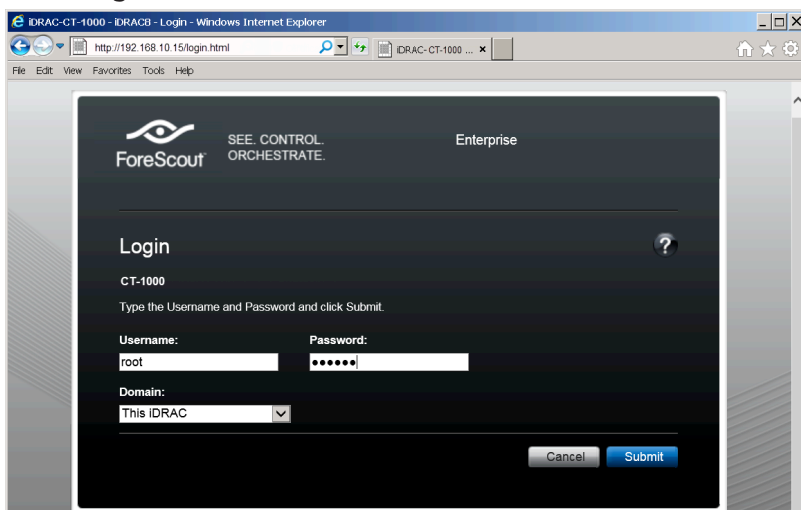
iDRAC ansluter till ett Ethernet-nätverk. Det är brukligt att ansluta det till ett hanteringsnätverk. Följande bild visar iDRAC-portens plats på den bakre panelen på CT-1000-enheten:



Logga in på iDRAC

För att logga in på iDRAC:

1. Gå till IP-adressen eller domännamnet som har konfigurerats i **Inställningar för iDRAC > Nätverk**.



2. Ange det användarnamn och lösenord som har konfigurerats på sidan Användarkonfigurerings i systeminstallation för iDRAC.
3. Välj **Skicka**.

För mer information om iDRAC hänvisar vi till [Användarguide till iDRAC](#).

Det är mycket viktigt att uppdatera de förinställda autentiseringsuppgifterna.

6. Verifiera anslutningen

Verifiera hanteringsgränssnittets anslutning

Testa hanteringsgränssnittets anslutning genom att logga in på enheten och köra följande kommando:

```
fstool linktest
```

Följande information visas:

```
Status för hanteringsgränssnitt  
Pingar standardgatewayinformation  
Pingstatistik  
Utför test för namnmatchning  
Testsammanfattning
```

Verifiera switchens/enhetens anslutning

Verifiera att switchen är ordentligt ansluten till enheten innan du lämnar datacentret. Gör detta genom att köra kommandot `fstool ifcount` i enheten för varje gränssnitt som hittas.

```
fstool ifcount eth0 eth1 eth2  
(Separera varje gränssnitt med ett mellanslag.)
```

Detta verktyg visar kontinuerligt nätverkstrafik på de angivna gränssnitten. Det jobbar i två lägen: genom interface eller genom VLAN. Läget kan ändras på skärmen. Totalt antal bitar per sekund och procentandel för var och en av följande trafik kategorier visas:

- Övervakningsgränssnittet bör primärt se speglad trafik — över 90 %.
- Svarsgränssnittet bör primärt se multisändningstrafik.
- Både övervakningsgränssnittet och svarsgränssnittet bör se de förväntade VLAN:erna.

Kommandoalternativ:

```
v - visa i VLAN-läge  
I - visa i gränssnittsläge  
P - visa föregående  
N - visa nästa  
q - sluta visa
```

VLAN-läge:

update=[4]		[eth3: 14 vlans]			
gränssnitt/VLAN	Total	multi-sändning	speglad	*Till min MAC-adress	*Från min MAC-adress
eth3.otaggad	4Mbps	0,2%	99,8%	0,0%	0,0%
eth3.1	9Mbps	0,0%	100,0%	0,0%	0,0%
eth3.2	3Mbps	0,1%	99,9%	0,0%	0,0%
eth3.4	542bps	100,0%	0,0%	0,0%	0,0%
eth3.20	1Kbps	100,0%	0,0%	0,0%	0,0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext-> [q]uit					

Gränssnittsläge:

update=[31]		[eth0: 32 vlans]		[eth1: 1 vlans]	
gränssnitt/VLAN	Total	multi-sändning	speglad	*Till min MAC-adress	*Från min MAC-adress
eth0	3Kbps	42,3%	0,0%	14,1%	43,7%
eth1	475bps	0,0%	100,0%	0,0%	0,0%

*Till min MAC-adress — Mål-MAC-adressen är enhetens MAC-adress.

*Från min MAC-adress — Trafik som skickas av denna enhet (Källans MACadress är enhetens MAC-adress. Destination kan vara multisändning eller enkelsändning).

Om du inte ser någon trafik ska du verifiera att gränssnittet fungerar. Använd följande kommando i enheten:

ifconfig [interface name] up

Utför pingtest

Kör ett pingtest från enheten till en dator i nätverket för att verifiera anslutningen.

Kör testet genom att:

1. Logga in på enheten.
2. Kör följande kommando: **Ping [network desktop IP]**
Som standard svarar enheten själv inte på pinget.

7. Installera CounterACT-konsolen

Installera CounterACT-konsolen

CounterACT-konsolen är ett centralt hanteringsprogram som används för att visa, spåra och analysera aktiviteter som hittas av enheten. NAC, Threat Protection, Firewall och andra policyer kan anges från konsolen. Se *Användarmanual till CounterACT-konsolen* för mer information.

Du måste ha en PC som kan vara värd för CounterACT-konsolens programvara. Lägsta krav för maskinvara är:

- Ej dedikerad PC som kör:
 - Windows XP, Windows Vista eller Windows 7
 - Windows Server 2003 eller Server 2008
 - Linux
- Pentium 3, 1 GHz
- 2 GB minne
- 1 GB diskutrymme

Det finns två metoder för att installera konsolen:

Använd installationsprogramvaran som är inbyggd i enheten.

1. Öppna ett webbläsarfönster från konsolens dator.
2. Ange följande i webbläsarens adressfält
http://<Appliance_ip>/install
Där <Appliance_ip> är enhetens IP-adress. Webbläsaren visar konsolens installationsfönster.
3. Följ anvisningarna på skärmen.

Installera från CounterACTs CD-ROM

1. Sätt i CounterACT-CD ROM i DVD-enheten.
2. Öppna filen **ManagementSetup.htm** i CD ROM-skivan med en webbläsare.
3. Följ anvisningarna på skärmen.

Logga in

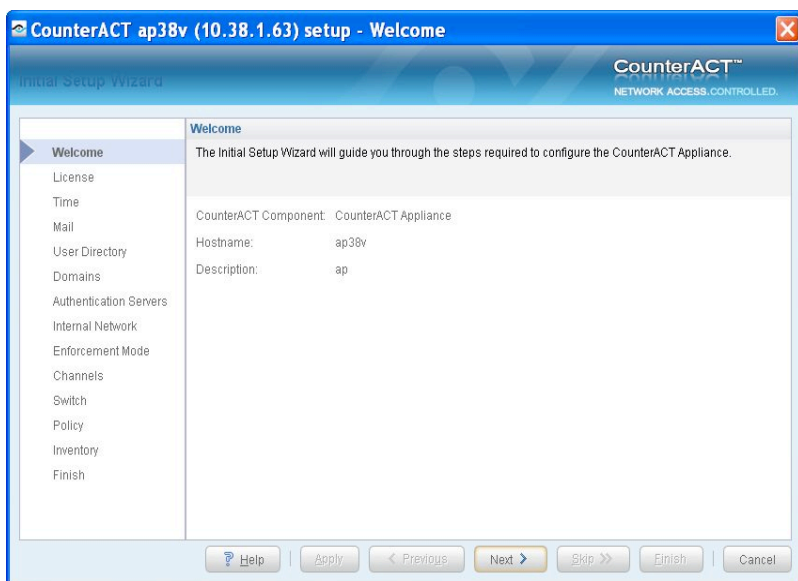
När installationen är slutförd kan du logga in på CounterACT-konsolen.

1. Välj CounterACT-ikonen på genvägsplatsen du har skapat.
2. Ange enhetens IP-adress eller värddatornamn i **IP/namn**-fältet.
3. I **fältet** Användarnamn anger du **admin**.
4. I fältet **Lösenord** anger du det lösenord du skapade under installationen av enheten.
5. Välj **Logga in** för att starta konsolen.



Gör första installationen

När du har loggat in första gången visas guiden för den första installationen. Guiden vägleder dig genom viktiga konfigureringssteg för att säkerställa att CounterACT kommer igång snabbt och effektivt.



Innan du startar den första installationen

Förbered följande information innan du jobbar med guiden:

Information	Värden
<input type="checkbox"/> NTP-serveradress som används av din organisation (valfritt).	
<input type="checkbox"/> Intern IP-adress för e-postvidarebefordran. Detta gör det möjligt att skicka e-post från CounterACT om SMTP-trafik inte är tillåten från enheten (valfritt).	
<input type="checkbox"/> CounterACT-administratörens e-postadress.	
<input type="checkbox"/> Tilldelning av övervaknings- och svarsgränssnitt angivna i datacentret.	
<input type="checkbox"/> För segment eller VLAN:er utan DHCP, nätverkssegmentet eller de VLAN:er till vilka övervakningsgränssnittet är direkt anslutet och en permanent IP-adress som ska användas av CounterACT i respektive sådant VLAN. Denna information är inte nödvändig för installation av Enterprise Manager.	
<input type="checkbox"/> IP-adressintervall som enheten skyddar (alla de interna adresserna, inklusive oanvända adresser).	
<input type="checkbox"/> Information om användarkatalogkonto och användarkatalogservrens IP-adress.	
<input type="checkbox"/> Domänautentiseringssuppgifter, inklusive kontonamn till domänadministration och lösenord.	
<input type="checkbox"/> Autentiseringsservrar så att CounterACT kan analysera vilka nätverksvärdar som har autentiserats.	
<input type="checkbox"/> Huvudswitchens IP-adress, leverantör och SNMP-parametrar.	

Se *användarmanualen till CounterACT-konsolen* eller online-hjälp för information om att arbeta med guiden.

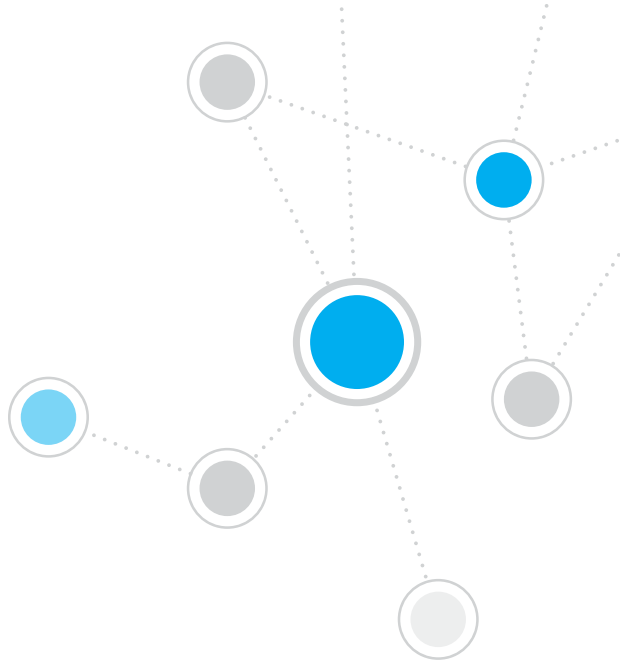
Kontaktuppgifter

För teknisk support från ForeScout ber vi dig skicka mejl till support@forescout.com. Du kan också ringa:

- Avgiftsfritt nummer (i USA): 1.866.377.8771
- Telefon (internationellt): 1.408.213.3191
- Support: 1.708.237.6591
- Fax: 1.408.371.2284

©2016 Produkter från ForeScout Technologies, Inc. skyddas i USA av patent med nummer 6,363,489, nr 8,254,286, nr 8,590,004 och nr 8,639,800. Med ensamrätt. ForeScout Technologies och ForeScouts logotyp är varumärken som tillhör ForeScout Technologies, Inc. Alla övriga varumärken tillhör respektive innehavare.

All användning av ForeScouts produkter regleras av villkoren i ForeScouts licensavtal för slutanvändare som finns tillgängligt på www.forescout.com/eula.



ForeScout®

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

Avgiftsfritt nummer (i USA): 1.866.377.8771

Telefon (internationellt): 1.408.213.3191

Support: 1.708.237.6591

Fax: 1.408.371.2284

400-00020-01