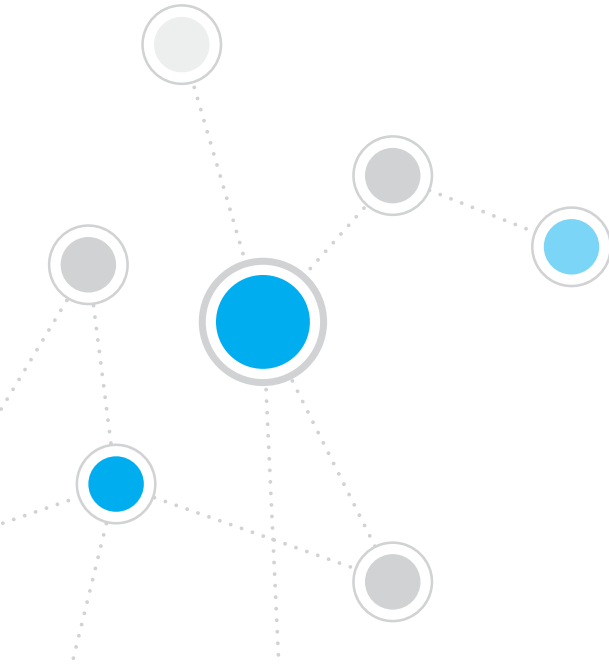




# ForeScout CounterACT® 7

Tek CounterACT Cihazı

**Hızlı Kurulum Kılavuzu**



# İçindekiler

<b>ForeScout CounterACT® Versiyon 7'ye Hoş Geldiniz</b>	<b>3</b>
CounterACT Paketinizin İçeriği	3
<b>Genel Bakış</b>	<b>4</b>
<b>1. Dağıtım Planı Oluşturun</b>	<b>5</b>
Cihazı Nerede Dağıtmak İstedığınıize Karar Verin.	5
Cihaz Arabirim Bağlantıları	5
<b>2. Anahtarınızı Ayarlayın</b>	<b>8</b>
A. Anahtar Bağlantı Seçenekleri	8
B. Anahtar Ayarı Notları	9
<b>3. Ağ Kablolarını Bağlayın ve Cihazı Açın</b>	<b>10</b>
A. Cihazı Ambalajından Çıkarın ve Kabloları Bağlayın.	10
B. Arabirim Atamalarını Kaydedin	11
C. Cihazı Açın.	11
<b>4. Cihazı Yapılandırın</b>	<b>12</b>
Lisans.	14
Ağ Bağlantı Gereksinimleri	14
<b>5. Uzaktan Yönetim</b>	<b>15</b>
iDRAC Kurulumu	15
Modülü Ağa Bağlayın	18
iDRAC'te oturum açın	18
<b>6. Bağlanılabilirliği Doğrulayın</b>	<b>19</b>
Yönetim Arabirim Bağlantısını Doğrulayın.	19
Anahtar/Cihaz Bağlanılabilirliğini Doğrulayın	19
Ping Testi Yapın	20
<b>7. CounterACT Konsolunu Ayarlayın</b>	<b>21</b>
CounterACT Konsolunu Kurun	21
Oturum Aç	22
İlk Kurulumu Yapın	22
<b>İrtibat Bilgileri</b>	<b>24</b>

# ForeScout CounterACT® Versiyon 7'ye Hoş Geldiniz

ForeScout CounterACT, ağ aygıtlarını ve uygulamalarını ağınıza bağlandıkları anda dinamik olarak tanımlayan ve değerlendiren fiziksel veya sanal bir güvenlik cihazıdır. CounterACT, aracı gerektirmediği için yönetilen ve yönetilmeyen, bilinen ve bilinmeyen, PC ve mobil, gömülü ve sanal aygıtlarınızla çalışır. CounterACT, hızlı bir şekilde kullanıcıyı, sahibi, işletim sistemi aygıt yapılandırmasını, yazılımı, servisleri, yama durumunu ve güvenlik araçlarının bulunup bulunmadığını belirler. Daha sonra bu aygıtlar ağda hareket ederken aygıtların onarımını, kontrolünü ve sürekli izlemeyi sağlar. Bunları yaparken de mevcut BT altyapınızla kusursuz bir şekilde entegre olur.



## ***Bu kılavuz tek bir bağımsız CounterACT Cihazının kurulumunu açıklamaktadır.***

Ayrıntılı bilgi almak veya kurum çapında ağ koruması için birden fazla cihazın nasıl kurulup dağıtılacağı hakkında bilgi edinmek için *CounterACT Kurulum Kılavuzu* ve *Konsol Kullanım Kılavuzuna* bakınız. Bu dokümanlar CounterACT CD'sinde /docs dizininde bulunmaktadır.

Ayrıca <https://www.forescout.com/support> adresindeki destek web sitesini ziyaret ederek en güncel dokümanlar, bilgi bankası makaleleri ve Cihazınız için güncellemelere ulaşabilirsiniz.

## **CounterACT Paketinizin İçeriği**

- CounterACT Cihazı
- Hızlı Kurulum Kılavuzu
- Konsol yazılımını içeren CounterACT CD'si, CounterACT Konsolu Kullanım ve Kurulum Kılavuzu
- Garanti belgesi
- Montaj braketleri
- Güç kablosu
- DB9 Konsolu bağlantı kablosu (sadece seri bağlantılar içindir)

# Genel Bakış

CounterACT'i ayarlamak için şu işlemleri yapın:

1. Dağıtım Planı Oluşturun
2. Anahtarınızı Ayarlayın
3. Ağ Kablolarını Bağlayın ve Cihazı Açın
4. Cihazı Yapılandırın
5. Uzaktan Yönetim
6. Bağlanılabilirliği Doğrulayın
7. CounterACT Konsolunu Ayarlayın

# 1. Dağıtım Planı Oluşturun

Kurulum yapmadan önce Cihazı nerede dağıtacağınıza karar vermeli ve Cihaz arabirim bağlantıları hakkında bilgi edinmelisiniz.

## Cihazı Nerede Dağıtmak İstedığınıza Karar Verin

Cihaz için doğru ağ konumunu seçmek, başarılı dağıtım ve CounterACT'in optimum performansı açısından büyük önem taşımaktadır. Doğru konum, istenilen uygulama hedeflerinize ve ağ erişim politikalarınıza bağlıdır. Cihaz, gereken politikayla ilgili trafiği izleyebilmelidir. Örneğin, politikanız uç noktalar ile kurumsal kimlik doğrulama sunucuları arasındaki yetki olaylarının takibine bağlıysa Cihaz kimlik doğrulama sunucusuna/sunucularına akan uç nokta trafiğini görecektir şekilde kurulmalıdır.

Kurulum ve dağıtımla ilgili ayrıntılı bilgi için bu paketin içeriğinde bulunan CounterACT CD'sindeki CounterACT Kurulum Kılavuzuna bakınız.

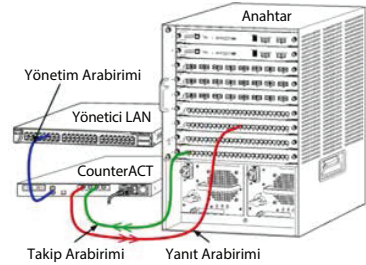
## Cihaz Arabirim Bağlantıları

Cihaz genellikle ağ anahtarına üç bağlantı ile yapılandırılır.

### Yönetim Arabirimi

Bu arabirim CounterACT'i kontrol etmenizi, sorgu gerçekleştirmenizi ve uç noktada ayrıntılı denetim yapmanızı sağlar. Bu arabirim bütün ağ uç noktalarına erişimi olan bir anahtar bağlantı noktasına bağlı olmalıdır.

Her Cihaz tek bir ağ yönetim bağlantısı gerektirir. Bu bağlantı yerel LAN'da IP adresi ve CounterACT Konsol yönetim uygulamasını çalıştıracak makinelerden 13000/TCP bağlantı noktası erişimi gerektirir. Yönetim arabiriminin ağıңызda bulunan şu öğelere erişimi olmalıdır:



Bağlantı noktası	Servis	CounterACT'ten veya CounterACT'e	İşlev
22/TCP	SSH	CounterACT'e	CounterACT komut hattı arabirimine erişim sağlar.
2222/TCP			(Yüksek Kullanılabilirlik) Yüksek Kullanılabilirlik kümesinin parçası olan fiziksel CounterACT aygıtlarına erişim sağlar. Kümenin paylaşılan (sanal) IP adresine erişmek için 22/TCP'yi kullanın.

Bağlantı noktası	Servis	CounterACT'ten veya CounterACT'e	İşlev
25/TCP	SMTP	CounterACT'ten	CounterACT'ten posta göndermek için kullanılır
53/UDP	DNS	CounterACT'ten	CounterACT'in iç IP adreslerini çözümlemesi sağlar.
80/TCP	HTTP	CounterACT'e	HTTP yeniden yönlendirmesi sağlar.
123/UDP	NTP	CounterACT'ten	CounterACT'in NTP zaman sunucusuna erişimini sağlar. CounterACT varsayılan olarak ntp.foreScout.net kullanır.
135	WMI	CounterACT'ten	CounterACT'in WMI kullanarak Windows uç noktalarında ayrıntılı denetim yapmasını ve onları kontrol etmesini sağlar.
139/TCP	SMB, MS-RPP	CounterACT'ten	Windows uç noktalarında uzaktan denetim sağlar (Windows 7 ve daha eski sürümlerini çalıştıran uç noktalar için).
445/TCP			Windows uç noktalarında uzaktan denetim sağlar.
161/UDP	SNMP	CounterACT'ten	CounterACT'in anahtar ve yönlendiriciler gibi ağ altyapı aygıtlarıyla iletişim kurmasını sağlar. SNMP yapılandırmasıyla ilgili bilgi için <i>CounterACT Konsol Kullanım Kılavuzuna</i> bakınız.
162/UDP	SNMP	CounterACT'e	CounterACT'in anahtar ve yönlendiriciler gibi ağ altyapı aygıtlarından SNMP yakalamaları almasını sağlar. SNMP yapılandırmasıyla ilgili bilgi için <i>CounterACT Konsol Kullanım Kılavuzuna</i> bakınız.
443/TCP	HTTPS	CounterACT'e	TLS kullanarak HTTP yeniden yönlendirmesi sağlar.
2200/TCP	Secure Connector	CounterACT'e	SecureConnector'ın Macintosh/ Linux makinelerden Cihaza güvenli (şifreli SSH) bağlantı kurmasını sağlar. SecureConnector, Macintosh ve Linux uç noktalarının bu uç noktalar ağa bağlıyken yönetimini sağlayan komut dosyası bazlı bir araçtır.

10003/TCP	Windows için Secure Connector	CounterACT'e	SecureConnector'ın Windows makinelerden Cihaza güvenli (şifreli TLS) bağlantı kurmasını sağlar. SecureConnector, Windows uç noktalarının bu uç noktalar ağa bağlıyken yönetimini sağlayan bir araçtır. SecureConnector, ile ilgili ayrıntılı bilgi için <i>CounterACT Konsol Kullanım Kılavuzuna</i> bakınız.  SecureConnector, bir Cihaza veya Enterprise Manager'a bağlanırsa ana bilgisayarının atandığı Cihaza yeniden yönlendirilir. Kurum içinde şeffaf mobilite sağlamak için bu bağlantı noktasının tüm Cihazlara ve Enterprise Manager'a açık olduğundan emin olun.
13000/TCP	CounterACT	CounterACT'e	Konsoldan Cihaza bağlantı sağlar.  Birden fazla CounterACT Cihazı olan sistemlerde Konsoldan Enterprise Manager'a ve Enterprise Manager'dan her bir Cihaza bağlantı sağlar.

## Takip Arabirimi

Bu bağlantı, Cihazın ağ trafiğini takip etmesini ve izlemesini sağlar.

Trafik, anahtardaki bir bağlantı noktasına yansıtılır ve Cihaz tarafından takip edilir. Yansıtılan VLAN sayısına bağlı olarak trafik 802.1Q VLAN etiketli olabilir veya olmayabilir.

- **Tek VLAN (etiketlenmemiş):** Takip edilen trafik tek VLAN kaynaklıysa yansıtılan trafiğin VLAN etiketli olması gerekmez.
- **Birden fazla VLAN (etiketli):** Takip edilen trafik birden fazla VLAN kaynaklıysa yansıtılan trafik 802.1Q VLAN etiketli *olmalıdır*.

İki anahtar yedekli çift halinde bağlı olduğunda Cihaz her iki anahtardan gelen trafiği kontrol etmelidir.

Takip arabiriminde IP adresi gerekmez.

## Yanıt Arabirimi

Cihaz bu arabirimi kullanarak trafiğe yanıt verir. Yanıt trafiği, kötü amaçlı aktivitelere karşı koruma sağlamak ve NAC politikası eylemlerini gerçekleştirmek için kullanılır. Bu eylemler arasında Web tarayıcılarını yeniden yönlendirmek veya güvenlik duvarı engellemek sayılabilir. İlgili anahtar bağlantı noktası yapılandırması takip edilen trafiğe bağlıdır.

- **Tek VLAN (etiketlenmemiş):** Takip edilen trafik tek bir VLAN kaynaklı olursa yanıt arabirimi aynı VLAN'ın parçası olacak şekilde yapılandırılmalıdır. Bu durumda Cihaz bu VLAN'da tek IP adresi gerektirir.
- **Birden fazla VLAN (etiketli):** Takip edilen trafik birden fazla VLAN kaynaklıysa aynı VLAN'lar için yanıt arabirimi 802.1Q etiketiyle yapılandırılmalıdır. Cihaz, korumalı her VLAN için IP adresi gerektirir.

## 2. Anahtarınızı Ayarlayın

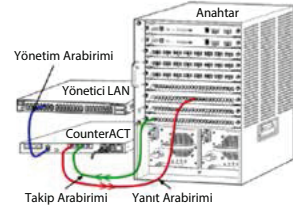
### A. Anahtar Bağlantı Seçenekleri

Cihaz, çeşitli ağ ortamlarına kusursuz bir şekilde entegre edilecek şekilde tasarlanmıştır. Cihazı başarılı bir şekilde ağınıza entegre etmek için anahtarınızın gereken trafiği takip edecek şekilde ayarlandığını doğrulayın.

Cihazı anahtarınıza bağlamak için birkaç seçenek vardır.

#### 1. Standart Dağıtım (Ayrı Yönetim, Takip ve Yanıt Arabirimleri)

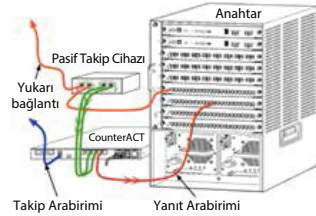
Önerilen dağıtımda üç ayrı bağlantı noktası kullanılmaktadır. Bu bağlantı noktaları *Cihaz Arabirim Bağlantılarında* açıklanmaktadır.



#### 2. Hatta Bağlı Pasif Takip Cihazı

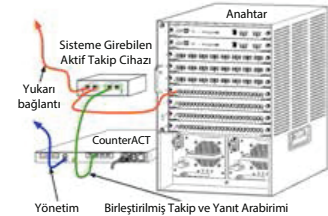
Cihaz, anahtar takip bağlantı noktasına bağlantı yerine hatta bağlı pasif takip cihazı kullanabilir.

Pasif takip cihazı, “yeniden birleşme” takip cihazları haricinde çift yönlü akışı tek bağlantı noktasında birleştiren iki takip bağlantı noktası gerektirir. Takip cihazlı bağlantı noktasındaki trafik ile yanıt arabirimi aynı şekilde yapılandırılmalıdır. Örneğin, takip cihazlı bağlantı noktasındaki trafik VLAN etiketliyse (802.1Q) yanıt arabirimi de VLAN etiketli bağlantı noktası olmalıdır.



#### 3. Hatta Bağlı Aktif (Sisteme Girebilen) Takip Cihazı

Cihaz, *sisteme girebilen* hatta bağlı bir takip cihazı kullanıyorsa takip ve yanıt arabirimleri birleştirilebilir. Anahtarda ayrı bir yanıt bağlantı noktasını yapılandırmaya gerek yoktur. Bu seçenek her türlü upstream veya downstream anahtar yapılandırmasında kullanılabilir.



#### 4. IP Katmanı Yanıtı (Katman-3 Anahtar Kurulumları)

Cihaz, trafiğe yanıt vermek için kendi yönetim arabirimini kullanabilir. Bu seçenek, takip edilen her trafikte kullanılabilmesine rağmen, Cihazın VLAN'ın parçası olmayan bağlantı noktalarını takip ederken kullanılması önerilir, böylece Cihaz takip edilen trafiğe başka bir anahtar bağlantı noktasını kullanarak yanıt veremez. Bu, iki yönlendiriciyi bağlayan bir bağlantıyı takip ederken gerçekleşen tipik bir durumdur.

Bu seçenek Adres Çözümleme Protokolü (ARP) isteklerine yanıt veremez ve Cihazın takip edilen alt ağdaki IP adreslerinde hedeflenen taramaları tespit etme özelliğini sınırlandırır. İki yönlendirici arasındaki trafik takip edilirken bu sınırlama uygulanmaz.

## B. Anahtar Ayarı Notları

### VLAN (802.1Q) Etiketleri

- **Tek VLAN (etiketlenmemiş trafik) Takibi** Takip edilen trafiğin kaynağı tek bir VLAN ise trafiğin 802.1Q ile etiketlenmesine gerek yoktur.
- **Birden fazla VLAN (etiketlenmiş trafik) Takibi** Takip edilen trafiğin kaynağı iki veya daha fazla VLAN ise takip ve yanıt arabirimlerinin *her ikisinde* de 802.1Q etiketi etkin olmalıdır. Yansıtılan bağlantı noktası sayısını minimize ederken en iyi genel kapsamı sunduğu için birden fazla VLAN'ın takip edilmesi önerilir.
- Anahtar, yansıtılan bağlantı noktalarında 802.1Q VLAN etiketi kullanamıyorsa şunlardan birini yapın:
  - Sadece bir VLAN yansıtın
  - Tek bir etiketlenmemiş yukarı bağlantı noktası yansıtın
  - IP Katmanı yanıt seçeneğini kullanın
- Anahtar sadece bir bağlantı noktasını yansıtabiliyorsa tek yukarı bağlantı noktası yansıtın. Bu bağlantı noktası etiketlenmiş olabilir. Genel olarak, anahtar 802.1Q VLAN etiketlerini çıkarırsa IP Katmanı yanıt seçeneğini kullanmanız gerekir.

### Ek Bilgi

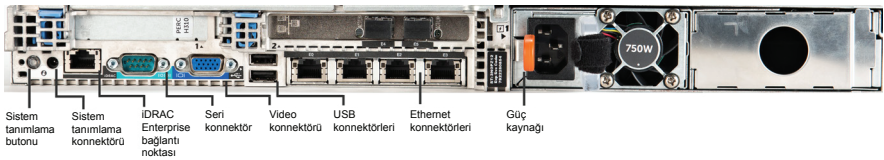
- Anahtar hem gönderilen hem de alınan trafiği yansıtamıyorsa tüm anahtarı ve VLAN'ların tamamını (gönderme/alma işlemi sağlar) veya sadece bir arabirimi (gönderme/alma olanağı sağlar) takip edin. Yansıtma bağlantı noktasını aşırı yüklenmediğinizi doğrulayın.
- Bazı anahtarlar (Cisco 6509 gibi) yeni yapılandırma girmeden önce eski bağlantı noktası yapılandırmasının tamamen temizlenmesini gerektirebilir. Eski bağlantı noktası bilgileri temizlenmediğinde meydana gelen en yaygın sonuç, anahtarın 802.1Q etiketlerini çıkarmasıdır.

### 3. Ağ Kablolarını Bağlayın ve Cihazı Açın

#### A. Cihazı Ambalajından Çıkarın ve Kabloları Bağlayın

1. Cihazı ve güç kablosunu nakliye kutusundan çıkarın.
2. Cihazla birlikte aldığınız ray kitini çıkarın.
3. Ray kitini Cihaza ve Cihazı rafa monte edin.
4. Ağ kablolarını Cihazın arka panelindeki ağ arabirimleri ile anahtar bağlantı noktaları arasına bağlayın.

#### **Arka Panel Örneği — CounterACT Ayrıtı**



## B. Arabirim Atamalarını Kaydedin

Cihazın veri merkezindeki kurulumunu tamamladıktan ve CounterACT Konsolunu kurduktan sonra arabirim atamalarını kaydetmeniz istenir. Bu atamalar *Kanal tanımları* olarak adlandırılır ve Konsola ilk kez giriş yaptığınızda açılan İlk Kurulum Sihirbazına girilir.

Fiziksel arabirim atamalarını aşağıya kaydedin ve Konsolda Kanal kurulumunu tamamlarken kullanın.

Ethernet Arabirimi	Arabirim Ataması (ör. Yönetim, Takip, Yanıt)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

## C. Cihazı Açın

1. Güç kablosunu Cihazın arka panelindeki güç konnektörüne bağlayın.
2. Güç kablosunun diğer ucunu topraklanmış AC prize takın.
3. Klavye ve monitörü Cihaza bağlayın veya Cihazı seri bağlantı için ayarlayın. CounterACT CD'sindeki *CounterACT Kurulum Kılavuzuna* bakınız.
4. Ön panelden Cihazı açın.

**Önemli: Makinenin fişini prizden çekmeden önce makineyi kapatın.**

## 4. Cihazı Yapılandırın

Cihazı yapılandırmadan önce aşağıdaki bilgileri hazır bulundurun.

<input type="checkbox"/> Cihaz ana bilgisayar adı	
<input type="checkbox"/> CounterACT Yönetici parolası	<b>Parolayı güvenli bir yerde muhafaza edin.</b>
<input type="checkbox"/> Yönetim arabirimi	
<input type="checkbox"/> Cihaz IP adresi	
<input type="checkbox"/> Ağ maskesi	
<input type="checkbox"/> Varsayılan Ağ Geçidi IP adresi	
<input type="checkbox"/> DNS Alan Adı	
<input type="checkbox"/> DNS sunucu adresleri	

Cihazı açtıktan sonra aşağıdaki mesaj ekrana gelerek yapılandırmayı başlatmanız istenir:

**CounterACT Cihazı önyükleme işlemi tamamlandı.  
Devam etmek için <Enter>'a basın.**

1. Aşağıdaki menüyü görüntülemek için **Enter'a** basın:

**1) CounterACT'i yapılandır**  
**2) Kayıtlı CounterACT yapılandırmasını geri yükle**  
**3) Ağ arabirimlerini tanımla ve yeniden numaralandır**  
**4) Klavye düzenini yapılandır**  
**5) Makineyi kapat**  
**6) Makineyi yeniden başlat**  
**Seçim (1 - 6) :1**

2. **1 - CounterACT'i yapılandır**'ı seçin. Şu mesaj ekrana geldiğinde:

**Devam: (evet/hayır)?**

Kurulumu başlatmak için **Enter'a** basın.

3. **Yüksek Kullanılabilirlik Modu** menüsü açılır. Standart Kurulumu seçmek için **Enter'a** basın.
4. **CounterACT İlk Kurulumu** mesajı ekrana gelir. Devam etmek için **Enter'a** basın.
5. **Select CounterACT Kurulum Türü** menüsü açılır. Standart CounterACT kurulumu için **1** yazın ve **Enter'a** basın. Kurulum başlar. Bu işlem bir dakika kadar sürebilir.


6. **Makine Tanımı Gir** mesajı belirttiğinde bu cihazı tanımlayan kısa bir yazı yazın ve **Enter**'a basın.  
Aşağıdaki mesaj belirir:

>>>>> Yönetici Parolasını Ayarla <<<<<<

Bu parola, makine İşletim Sistemi 'kök' kullanıcı ve CounterACT Konsolunda 'yönetici' olarak oturum açmak için kullanılır.

Parola 6 - 15 karakter uzunluğunda olmalı ve en az bir alfabetik olmayan karakter içermelidir.

Yönetici parolası:

7. **Yönetici Parolasını Ayarla** mesajı belirttiğinde parola olarak belirlemek istediğiniz bir ifade yazın (yazdığınız ifade ekranda görünmez) ve **Enter**'a basın. Parolayı doğrulamanız istenir. Parola altı - 15 karakter uzunluğunda olmalı ve en az bir alfabetik olmayan karakter içermelidir.
-  Cihazda kök kullanıcı ve Konsolda yönetici olarak oturum açın.
8. **Ana Bilgisayar Adını Ayarla** mesajı belirttiğinde bir ana bilgisayar adı yazın ve **Enter**'a basın. Ana bilgisayar adı Konsola giriş yaparken kullanılabilir ve görüntülediğiniz CounterACT Cihazının kimliği belirlemenize yardımcı olmak için Konsolda görüntülenir.
9. **Ağ Ayarlarını Yapılandır** ekranında bir dizi yapılandırma parametresi girmeniz istenir. Her mesaj belirttiğinde bir değer yazın ve devam etmek için **Enter**'a basın.
- CounterACT bileşenleri yönetim arabirimleri aracılığıyla iletişim kurar. Belirtilen yönetim arabirimlerinin sayısı Cihaz modeline bağlıdır.
  - **Yönetim IP adresi**, CounterACT bileşenlerinin iletişim kurduğu arabirim adresidir. Sadece CounterACT bileşenleri arasında iletişim kurmak için kullanılan arabirim, etiketlenmiş bağlantı noktasına bağlı olduğunda bu arabirim için VLAN kimliği ekleyin.
  - Birden fazla **DNS sunucu adresi** varsa her adresi boşlukla ayırın— İç DNS sunucularının birçoğu dış ve iç adresleri çözümler, fakat dış çözümleyici DNS sunucusu eklemeniz gerekebilir. Cihaz tarafından yapılan DNS sorgularının neredeyse tamamı iç adresler için olacağından, dış DNS sunucusu listenin en sonunda olmalıdır.
10. **Kurulum Özeti** ekranı görüntülenir. Genel bağlanabilirlik testleri yapmanız, ayarları yeniden yapılandırmanız veya kurulumu tamamlamanız istenir. Kurulumu tamamlamak için **D** yazın.

## Lisans

Kurulum tamamlandıktan sonra CounterACT temsilciniz tarafından verilen ilk demo lisansını yüklemelisiniz. Lisans ilk Konsol kurulumu sırasında yüklenir. İlk demo lisansı kısıtlı bir süre boyunca geçerlidir. Bu süre dolmadan kalıcı bir lisans yüklemelisiniz. Son geçerlilik tarihine ilişkin bir e-posta tarafınıza gönderilecektir. Ayrıca lisansın son geçerlilik tarihine ilişkin bilgiler ve lisans durumu Konsolda Cihazlar/Aygıtlar bölümünde gösterilecektir.

Kalıcı lisans aldığınızda, lisans ForeScout Lisans Sunucusu tarafından her gün doğrulanacaktır. Lisans uyarıları ve ihlaller Aygıt Bilgileri bölümünde görüntülenir.

Bir ay boyunca doğrulanamayan lisanslar iptal edilecektir. Lisanslar hakkında ayrıntılı bilgi için CounterACT Kurulum Kılavuzuna bakınız.

## Ağ Bağlantı Gereksinimleri

En az bir CounterACT aygıtında (cihaz veya Enterprise Manager) internet erişimi olmalıdır. Bu bağlantı CounterACT lisanslarını ForeScout Lisans sunucusuyla doğrulamak için kullanılmaktadır.

Bir ay boyunca kimlik doğrulaması yapılmayan lisanslar iptal edilecektir. Sunucuyla iletişim hatası olduğu görüldüğünde CounterACT günde bir uyarı e-postası gönderir.

## 5. Uzaktan Yönetim

### iDRAC Kurulumu

Integrated Dell Remote Access Controller (iDRAC), konumdan/işletim sisteminden bağımsız olarak LAN veya internet üzerinden CounterACT Cihazlarına/Enterprise Manager'lara uzaktan erişmenizi sağlayan entegre sunucu sistemi çözümüdür. KVM erişimi, açma/kapatma/sıfırlama, sorun giderme ve bakım işlemlerini gerçekleştirmek için bu modülü kullanın.

iDRAC modülüyle çalışmak için şunları yapın:

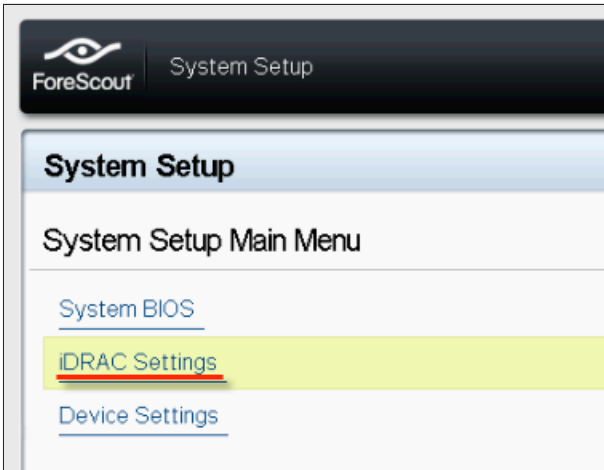
- *iDRAC Modülünü Etkinleştirin ve Yapılandırın*
- *Modülü Ağa Bağlayın*
- *iDRAC'te Oturum Açın*

### iDRAC Modülünü Etkinleştirin ve Yapılandırın

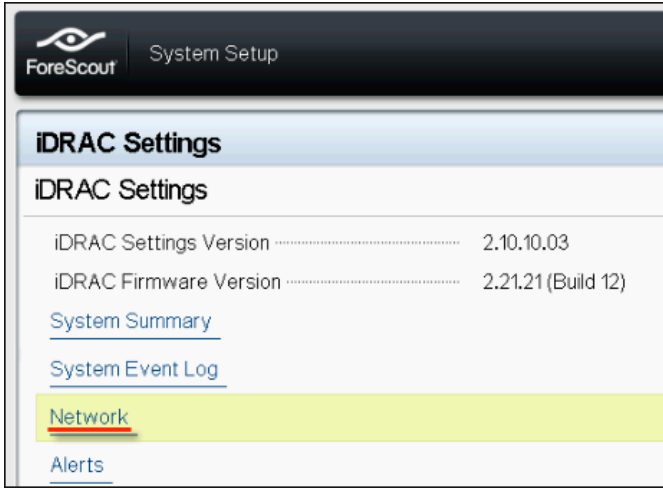
CounterACT aygıtına uzaktan erişimi etkinleştirmek için iDRAC ayarlarını değiştirin. Bu bölümde CounterACT ile çalışmak için gereken temel entegrasyon ayarları açıklanmaktadır.

#### iDRAC'ı yapılandırmak için:

1. Yönetilen sistemi açın.
2. Açılış testi (POST) sırasında F2'ye basın.
3. Sistem Kurulumu Ana Menüsü sayfasında **iDRAC Ayarları**'nı seçin.

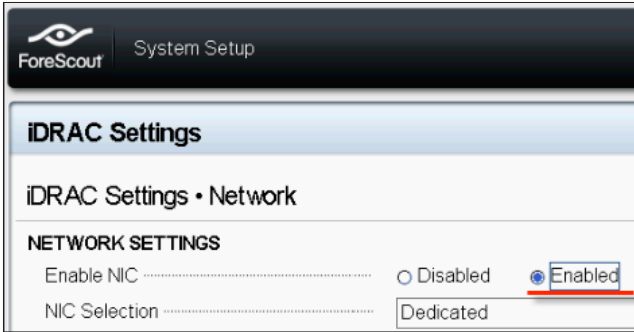


4. iDRAC Ayarları sayfasında **Ağ**'ı seçin.



5. Aşağıdaki Ağ ayarlarını yapılandırın:

- **Ağ Ayarları.** NIC'i etkinleştir alanının **Etkin** olarak ayarlandığını doğrulayın.



- **Genel Ayarlar.** DNS DRAC Adı alanında, dinamik bir DNS'i (opsiyonel) güncelleyebilirsiniz.

- **IPv4 Ayarları.** IPv4'ü etkinleştir alanının **Etkin** olarak ayarlandığını doğrulayın. Dinamik IP Adresleme işlemine başvurmak veya Statik IP Adresleme kullanımını Devre Dışı Bırakmak için **DHCP'yi etkinleştir** alanının **Etkin** olarak ayarlandığını doğrulayın. Etkinse DHCP otomatik olarak IP adresi, ağ geçidi ve alt ağ maskesini iDRAC değerine ayarlar. Devre dışıysa **Statik IP Adresi, Statik Ağ Geçidi** ve **Statik Alt Ağ Maskesi** alanlarına ilgili değerleri girin.

**ForeScout** System Setup

### iDRAC Settings

#### iDRAC Settings • Network

**IPv4 SETTINGS**

Enable IPv4 .....	<input type="radio"/> Disabled	<input checked="" type="radio"/> <b>Enabled</b>
Enable DHCP .....	<input checked="" type="radio"/> <b>Disabled</b>	<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"/> <b>Disabled</b>	<input type="radio"/> Enabled
Static Preferred DNS Server .....	192.168.1.2	
Static Alternate DNS Server .....	0.0.0.0	

6. **Geri'yi** seçin.
7. **Kullanıcı Yapılandırması'nı** seçin.
8. Aşağıdaki Kullanıcı Yapılandırması alanlarını yapılandırın:
  - **Kullanıcıyı Etkinleştir.** Bu alanın Etkin olarak ayarlandığını doğrulayın.
  - **Kullanıcı Adı.** Kullanıcı adı girin.
  - **LAN ve Seri Bağlantı Noktası Kullanıcı Ayrıcalıkları.** Yönetici için ayrıcalık seviyelerini ayarlayın.
  - **Parola Değiştir.** Kullanıcının oturum açma parolasını belirleyin.

**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"/> <b>Enabled</b>
User Name .....	root
LAN User Privilege .....	Administrator
Serial Port User Privilege .....	Administrator
Change Password .....	

9. **Geri** ve ardından **Bitti**'yi seçin. Değiştirilen ayarları onaylayın. Ağ ayarları kaydedilir ve sistem yeniden başlatılır.

## Modülü Ağa Bağlayın

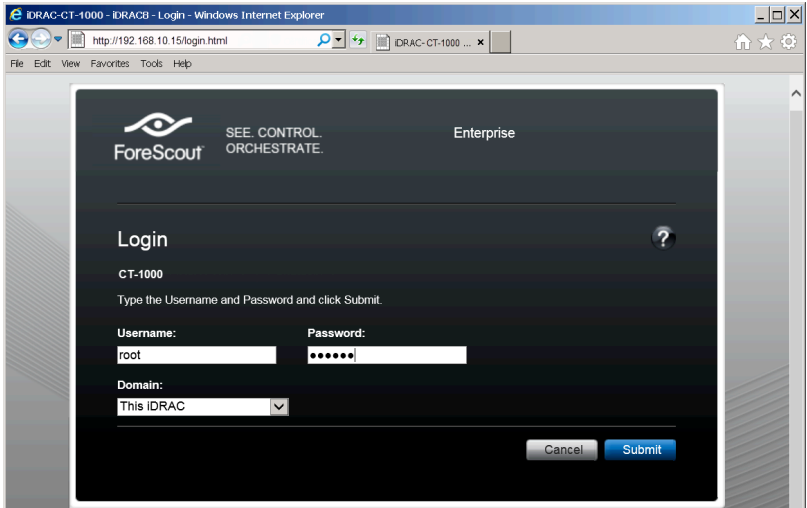
iDRAC, Ethernet ağına bağlanır. Yönetim ağına bağlanması uygundur. Aşağıdaki resim CT-1000 cihazının arka panelindeki iDRAC bağlantı noktası konumunu göstermektedir:



## iDRAC'te oturum açın

**iDRAC'te oturum açmak için:**

1. **iDRAC Ayarları > Ağ** menüsünde yapılandırılan IP Adresine veya alan adına göz atın.



2. iDRAC sistem kurulumunda Kullanıcı Yapılandırması sayfasında yapılandırılan Kullanıcı Adı ve Parolayı girin.
3. **Gönder**'i seçin.

iDRAC hakkında ayrıntılı bilgi için [iDRAC Kullanıcı Kılavuzuna](#) bakınız. Varsayılan kimlik bilgilerini güncellemek çok önemlidir.

## 6. Bağlanılabilirliği Doğrulayın

### Yönetim Arabirim Bağlantısını Doğrulayın

Yönetim arabirim bağlantısını test etmek için Cihazda oturum açın ve aşağıdaki komutu çalıştırın:

```
fstool linktest
```

Aşağıdaki bilgi ekrana gelir:

```
Yönetim Arabirimi durumu  
Varsayılan ağ geçidi bilgileri yoklanıyor  
Ping istatistikleri  
Ad Çözümleme Testi Yapılıyor  
Test özeti
```

### Anahtar/Cihaz Bağlanılabilirliğini Doğrulayın

Veri merkezinden ayrılmadan önce anahtarın Cihaza düzgün bağlandığını doğrulayın. Cihazda, algılanan her arabirim için fstool ifcount komutunu çalıştırarak bundan emin olabilirsiniz.

```
fstool ifcount eth0 eth1 eth2
```

*(Her arabirimi boşlukla ayırın.)*

Bu araç, sürekli olarak belirli arabirimlerdeki ağ trafiğini gösterir. İki farklı modda çalışır: arabirim veya VLAN için. Mod, ekrandan değiştirilebilir. Saniyedeki toplam bit sayısı ve aşağıdaki trafik kategorilerinin yüzdesi gösterilmektedir:

- Takip arabirimi ağırlıklı olarak — %90'ın üzerinde yansıtılan trafiği görmelidir.
- Yanıt arabirimi ağırlıklı olarak yayın trafiğini görmelidir.
- Takip ve yanıt arabirimleri beklenen VLAN'ları görmelidir.

#### Komut seçenekleri:

```
v - VLAN modunda görüntüle  
I - arabirim modunda görüntüle  
P - öncekini göster  
N - sonrakini göster  
q - görüntülemeyi durdur
```

## VLAN Modu:

```
güncelleme=[4] [eth3: 14 vlan]
Arayüz/Vlan      Toplam   Yayın    Yansıtılan  *MAC'ime  *MAC'imden
eth3.etiket-
lenmemiş         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
Göster [v]lanlar [a]rayüzler <-[ö]nceki [s]onraki-> [d]urdur
```

## Arabirim Modu:

```
güncelleme=[31] [eth0: 32 vlan] [eth1: 1 vlan]
Arayüz          Toplam   Yayın    Yansıtılan  *MAC'ime  *MAC'imden
eth0            3 Kbps   %42,3    %0,0         %14,1     %43,7
eth1            475 bps  %0,0     %100,0       %0,0      %0,0
```

\*MAC'ime — Hedef MAC, Cihazın MAC'idir.

\*MAC'imden — Bu cihaz tarafından gönderilen trafik (Kaynak MAC, Cihazın MAC'idir. Hedef, genel yayın veya tek yönlü yayın olabilir).

Hiç trafik görmüyorsanız arabirimin çalıştığını doğrulayın. Cihazda aşağıdaki komutu kullanın:

```
ifconfig [arabirim adı] up
```

## Ping Testi Yapın

Bağlanılabilirliği doğrulamak için Cihazdan bir ağ masaüstüne ping testi yapın.

### Test yapmak için:

1. Cihazda oturum açın.
2. Aşağıdaki komutu çalıştırın: **Ping [ağ masaüstü IP'si]**  
Cihaz varsayılan olarak ping'e karşılık vermez.

## 7. CounterACT Konsolunu Ayarlayın

### CounterACT Konsolunu Kurun

CounterACT Konsolu, Cihaz tarafından tespit edilen etkinliği görüntüleme, takip ve analiz etme için kullanılan merkezî yönetim uygulamasıdır. NAC, Tehdit Koruması, Güvenlik Duvarı ve diğer kurallar Konsoldan belirlenebilir. Ayrıntılı bilgi için *CounterACT Konsolu Kullanım Kılavuzuna* bakınız.

CounterACT Konsol uygulama yazılımını barındırması için bir makine tedarik etmeniz gerekir. Minimum donanım gereksinimleri şunlardır:

- Şunları çalıştıran atanmamış makine:
  - Windows XP, Windows Vista veya Windows 7
  - Windows Server 2003 veya Server 2008
  - Linux
- Pentium 3, 1 GHz
- 2 GB hafıza
- 1 GB disk alanı

Konsol kurulumunu gerçekleştirmek için iki yöntem vardır:

#### Cihazınızdaki kurulum yazılımını kullanın.

1. Konsol bilgisayarında bir tarayıcı penceresi açın.

Aşağıdakileri tarayıcının adres satırına yazın:

**<http://<Appliance ip>/install>**

<Appliance ip>, Cihazın IP adresidir. Tarayıcı, Konsol kurulumu penceresini görüntüler.

2. Ekrana gelen talimatları takip edin.

#### CounterACT CD-ROM'undan kurulum yapın.

1. CounterACT CD ROM'unu DVD sürücüsüne yerleştirin.
2. CD ROM'daki **ManagementSetup.htm** dosyasını tarayıcıda açın.
3. Ekrana gelen talimatları takip edin.

## Oturum Aç

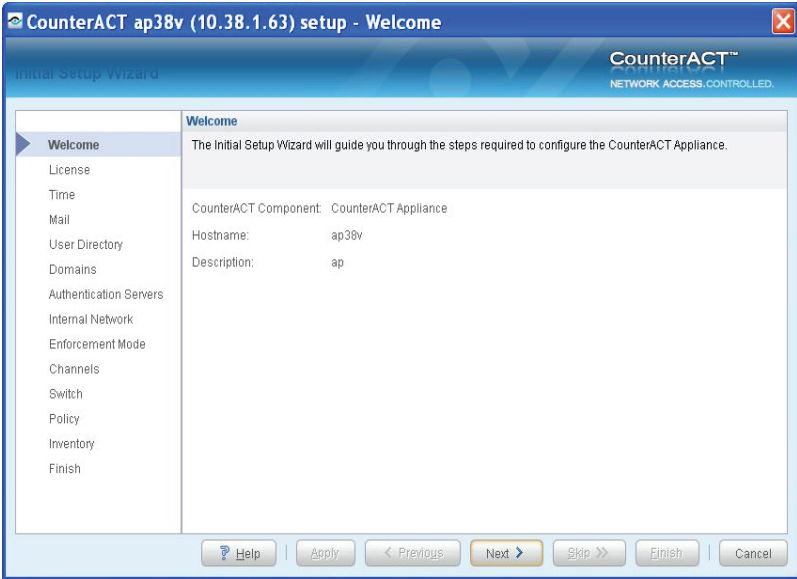
Kurulumu tamamladıktan sonra CounterACT Konsolunda oturum açabilirsiniz.

1. Oluşturduğunuz kısayol konumundan CounterACT simgesini seçin.
2. **IP/Ad** alanına Cihazın IP adresini veya ana bilgisayar adını girin.
3. **Kullanıcı Adı** alanına, **yönetici** yazın.
4. **Parola** alanına Cihaz kurulumu sırasında oluşturduğunuz parolayı girin.
5. Konsolu başlatmak için **Oturum Aç**'ı seçin.



## İlk Kurulumu Yapın

İlk kez oturum açtığınızda, İlk Kurulum Sihirbazı ekrana gelir. CounterACT'in hızlı ve verimli bir şekilde çalışmasını sağlamak için Sihirbaz sizi temel yapılandırma adımlarıyla yönlendirir.



## İlk Kurulumu Başlatmadan Önce

Sihirbazla çalışmaya başlamadan önce aşağıdaki bilgileri hazır bulundurun:

Bilgiler	Değerler
<input type="checkbox"/> Kurumunuzun kullandığı NTP sunucu adresi (opsiyonel).	
<input type="checkbox"/> İç posta geçişi IP adresi. Cihazdan SMTP trafiğine izin verilmezse CounterACT'ten e-posta gönderimi yapılmasını sağlar (opsiyonel).	
<input type="checkbox"/> CounterACT yöneticisi e-posta adresi.	
<input type="checkbox"/> Veri Merkezinde belirlenen takip ve yanıt arabirim atamaları.	
<input type="checkbox"/> DHCP olmayan bölütler veya VLAN'lar için, takip arabiriminin doğrudan bağlı olduğu ağ bölütü veya VLAN'lar ve VLAN gibi her birinde CounterACT tarafından kullanılacak kalıcı bir IP adresi. Enterprise Manager kurulumunda bu bilgiler gerekli değildir.	
<input type="checkbox"/> IP adresi Cihazın koruma aralığını değiştirir (kullanılmayan adresler dâhil tüm iç adresler).	
<input type="checkbox"/> Kullanıcı Dizini hesap bilgileri ve Kullanıcı Dizini sunucusu IP adresi.	
<input type="checkbox"/> Alan adı yöneticisi hesap adı ve parolası dâhil olmak üzere alan adı kimlik bilgileri.	
<input type="checkbox"/> CounterACT'in hangi ağ ana bilgisayarının kimlik doğrulamasının başarılı olduğunu analiz edebilmesi için kimlik doğrulama sunucuları.	
<input type="checkbox"/> Temel anahtar IP adresi, satıcı ve SNMP parametreleri.	

Sihirbazla çalışmayla ilgili olarak *CounterACT Konsolu Kullanım Kılavuzuna* veya Çevrimiçi Yardıma bakınız.

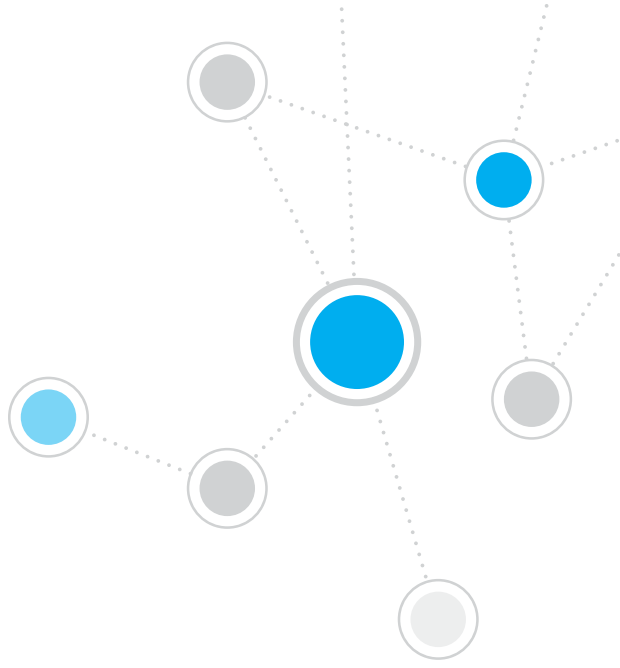
# İrtibat Bilgileri

ForeScout teknik destek ekibine ulaşmak için [support@forescout.com](mailto:support@forescout.com) adresine e-posta gönderin veya aşağıdaki numaralardan birini arayın:

- Ücretsiz Tel. (ABD): 1.866.377.8771
- Uluslararası Telefon: 1.408.213.3191
- Destek: 1.708.237.6591
- Faks: 1.408.371.2284

©2016 ForeScout Technologies, Inc. Ürünleri 6.363.489, 8.254.286, 8.590.004 ve 8.639.800 sayılı ABD patentleri ile korunmaktadır. Tüm hakları saklıdır. ForeScout Technologies ve ForeScout logosu, ForeScout Technologies, Inc.in ticari markalarıdır. Diğer tüm ticari markalar ilgili sahiplerine aittir.

Herhangi bir ForeScout Ürününün kullanımı [www.forescout.com/eula](http://www.forescout.com/eula) adresinde yer alan ForeScout Son Kullanıcı Lisans Sözleşmesi hükümlerine tabidir.



# ForeScout®

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

**Ücretsiz Tel. (ABD)** 1.866.377.8771

**Uluslararası Telefon** 1.408.213.3191

**Destek** 1.708.237.6591

**Faks** 1.408.371.2284

400-00020-01