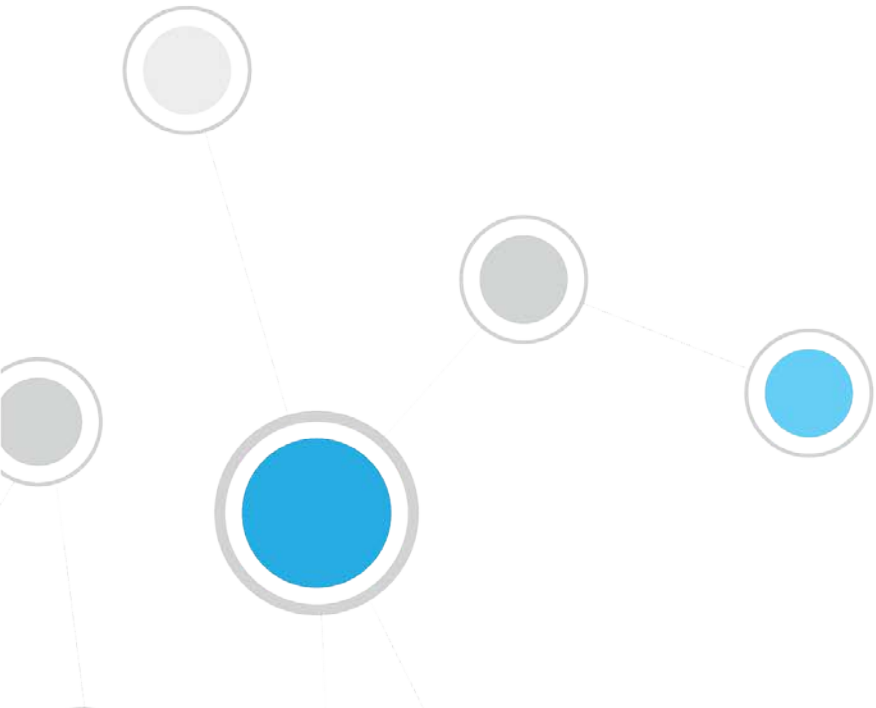
ForeScout CounterACT®

Tek CounterACT Cihazı

Hızlı Kurulum Kılavuzu

Sürüm 8.0



İçindekiler

CounterACT Sürüm 8.0'a Hoş Geldiniz

CounterACT platformu, ağ güvenliğinin geliştirilmesi için altyapı ve aygıt görünürlüğü, politika yönetimi, orkestrasyon ve iş akışı düzenlemesi sağlar. CounterACT kurumlara, ağdaki aygıtlar ve kullanıcılar hakkında gerçek zamanlı bağlamsal bilgi sunar. CounterACT'te politikalar uyuma, onarıma, uygun ağ erişimine ve hizmet operasyonlarının daha verimli hale getirilmesine yardımcı olan bu bağlamsal bilgiler kullanılarak tanımlanır.

Bu kılavuz tek bir bağımsız CounterACT Cihazının kurulumunu açıklamaktadır.

Ayrıntılı bilgi almak veya kurum çapında ağ koruması için birden fazla Cihazın nasıl dağıtılacağı hakkında daha fazla bilgi edinmek için *CounterACT Kurulum Kılavuzu* ve *CounterACT İdare Kılavuzu*'na bakın. Bu kılavuzlara nasıl erişim sağlayacağınız konusunda bilgi için bkz. Ek CounterACT Dokümantasyonu.

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

CounterACT Paket İçerikleri

CounterACT paketi aşağıdaki parçaları içerir:

- CounterACT Cihazı
- Ön Koruyucu Çerçeve
- Ray Kitleri (Montaj braketleri)
- Güç kablosu/kabloları
- DB9 Konsolu bağlantı kablosu (sadece seri bağlantılar içindir)
- Kurum Ürünleri Güvenliği, Çevre ve Düzenlemelerle İlgili Bilgiler
- Başlangıç dokümanı (sadece 51xx aygıtlar içindir)

Genel Bakış

CounterACT'i ayarlamak için şu işlemleri yapın:

1. Dağıtım Planı Oluşturun

Kurulum yapmadan önce Cihazı nereye yerleştireceğinize karar vermeli ve Cihaz arabirim bağlantıları hakkında bilgi edinmelisiniz.

Cihazı Nereye Yerleştirmek İstediğinize Karar Verin

Cihazın kurulacağı doğru ağ konumunu seçmek, başarılı dağıtım ve CounterACT'in optimum performansı açısından büyük önem taşımaktadır. Doğru konum, istenilen uygulama hedeflerinize ve ağ erişim politikanıza 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 görecek şekilde kurulmalıdır.

Kurulum ve dağıtım hakkında daha fazla bilgi için bkz. *CounterACT Kurulum Kılavuzu*. Bu kılavuza nasıl erişim sağlayacağınız konusunda bilgi için bkz. Ek CounterACT Dokümantasyonu.

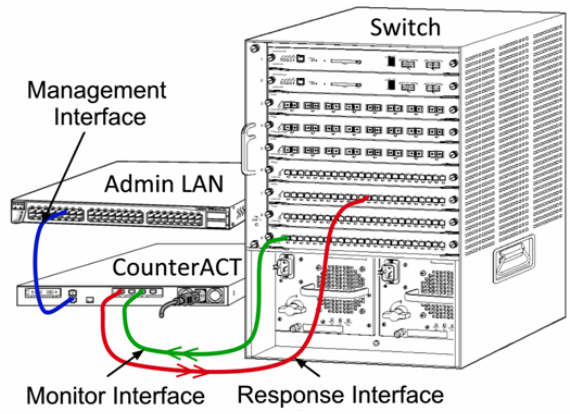
Cihaz Arabirim Bağlantıları

Cihaz genellikle ağ anahtarına üç bağlantı ile yapılandırılır.

Yönetim Arabirimi

Yönetim arabirimi CounterACT'i yönetmenizi, 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 bağlantı noktasının, ek ağ servislerine erişimi olmalıdır.



Ağ Erişimi Gereklilikleri

Bağlantı noktası	Servis	CounterACT'ten veya CounterACT'e	Fonksiyon
22/TCP	SSH	CounterACT'ten	OS X ve Linux uç noktalarının uzaktan denetimini sağlar. CounterACT'in ağ anahtarları ve yönlendiriciler ile iletişim kurmasını sağlar.
		CountertACT'e	CounterACT komut hattı arabirimine erişim sağlar.
2222/TCP	SSH	CountertACT'e	(Yüksek Kullanılabilirlik) Yüksek Kullanılabilirlik çiftinin parçası olan fiziksel CounterACT aygıtlarına erişim sağlar. Çiftin paylaşılan (sanal) IP adresine erişmek için 22/TCP'yi kullanın.
25/TCP	SMTP	CounterACT'ten	CounterACT'in kurumsal posta geçişine erişim sağlamasına olanak tanır.
53/UDP	DNS	CounterACT'ten	CounterACT'in iç IP adreslerini çözümlemesini sağlar.
80/TCP	HTTP	CountertACT'e	HTTP yeniden yönlendirmesi sağlar.
123/UDP	NTP	CounterACT'ten	CounterACT'in yerel zaman sunucusuna veya ntp.forescout.net'e erişimini sağlar. CounterACT varsayılan olarak ntp.foreScout.net'e erişim sağlar.
135/TCP	MS-WMI	CounterACT'ten	Windows uç noktalarında uzaktan denetim sağlar.
139/TCP	SMB, MS-RPC	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 ağ anahtarları ve yönlendiriciler ile iletişim kurmasını sağlar. SNMP yapılandırmasıyla ilgili bilgi için *CounterACT İdare Kılavuzu*'na bakın.

Bağlantı noktası	Servis	CounterACT'ten veya CounterACT'e	Fonksiyon
162/UDP	SNMP	CountertACT'e	CounterACT'in ağ anahtarları ve yönlendiricilerinden SNMP yakalamaları almasını sağlar. SNMP yapılandırmasıyla ilgili bilgi için *CounterACT İdare Kılavuzu*'na bakın.
389/TCP (636)	LDAP	CounterACT'ten	CounterACT'in Active Directory (Aktif Dizin) ile iletişim kurmasını sağlar. CounterACT web-tabanlı portallarla iletişim sağlar.
443/TCP	HTTPS	CountertACT'e	TLS kullanarak HTTP yeniden yönlendirmesi sağlar.
2200/TCP	Linux için SecureConnector	CountertACT'e	SecureConnector'ın Linux makinelerden Cihaza güvenli (şifreli SSH) bağlantı kurmasını sağlar. *SecureConnector* Linux uç noktalarının, bu uç noktalar ağa bağlıyken yönetimini sağlayan komut dizisi bazlı bir aracıdır.
10003/TCP	Windows için SecureConnector	CountertACT'e	SecureConnector'ın Windows makinelerden Cihaza güvenli (şifreli TLS) bağlantı kurmasını sağlar. *SecureConnector* Windows uç noktalarının, bu uç noktalar ağa bağlıyken, yönetimini sağlayan bir aracıdır. SecureConnector ile ilgili ayrıntılı bilgi için *CounterACT İdare Kılavuzuna* bakın. 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.

Bağlantı noktası	Servis	CounterACT'ten veya CounterACT'e	Fonksiyon
10005/TCP	OS X için SecureConnector	CountertACT'e	SecureConnector'ın OS X makinelerden Cihaza güvenli (şifreli TLS) bağlantı kurmasını sağlar. *SecureConnector* OS X uç noktalarının, bu uç noktalar ağa bağlıyken, yönetimini sağlayan bir aracıdır. SecureConnector ile ilgili ayrıntılı bilgi için *CounterACT İdare Kılavuzuna* bakın. 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'ten/CounterACT'e	Tek Cihazlı ortamlar için Konsoldan Cihaza. Birden fazla CounterACT Aygıtı bulunan ortamlar için Konsoldan CounterACT Aygıtına ve CounterACT Aygıtından bir başkasına. CounterACT Aygıtı iletişimi, TLS kullanarak Enterprise Manager ve Recovery Enterprise Manager ile iletişimi içerir.

Takip Arabirimi

Takip arabirimi, Cihazın ağ trafiğini takip etmesini ve izlemesini sağlar. Mevcut herhangi bir arabirim, takip arabirimi olarak kullanılabilir.

Trafik, anahtardaki bir bağlantı noktasına yansıtılır ve cihaz tarafından takip edilir. 802.1Q VLAN etiketlemesi kullanımı, yansıtılan VLAN'ların sayısına bağlıdır.

- ***Tek VLAN***: Takip edilen trafik tek VLAN kaynaklıysa yansıtılan trafiğin VLAN etiketli olması gerekmez.
- ***Çoklu VLAN'lar***: 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.

Arabirimi takip etmek için IP adresi gerekmez.

Yanıt Arabirimi

Cihaz bu yanıt arabirimini kullanarak trafiğe yanıt verir. Yanıt trafiği, kötü amaçlı aktivitelere karşı koruma sağlamak ve politika eylemlerini gerçekleştirmek için kullanılır. Bu eylemler arasında web tarayıcılarını yeniden yönlendirmek veya oturum engellemek sayılabilir. İlgili anahtar bağlantı noktası yapılandırması takip edilen trafiğe bağlıdır.

Mevcut herhangi bir arabirim, yanıt arabirimi olarak kullanılabilir.

- ***Tek VLAN***: Takip edilen trafik tek bir VLAN kaynaklı olursa yanıt bağlantı noktası aynı VLAN'a ait olmalıdır. Bu durumda Cihaz bu VLAN'da tek IP adresi gerektirir.
- ***Çoklu VLAN'lar***: Takip edilen trafik birden fazla VLAN kaynaklıysa aynı VLAN'lar için yanıt bağlantı noktası da 802.1Q VLAN etiketiyle yapılandırılmalıdır. Cihaz, takip edilen her VLAN için bir IP adresi gerektirir.

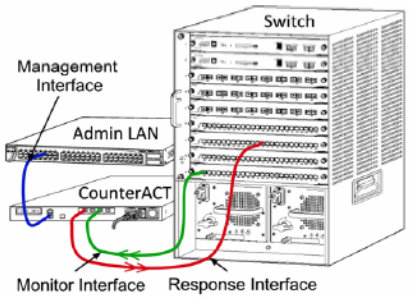
2. Anahtarınızı Ayarlayın

A. Anahtar Bağlantı Seçenekleri

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

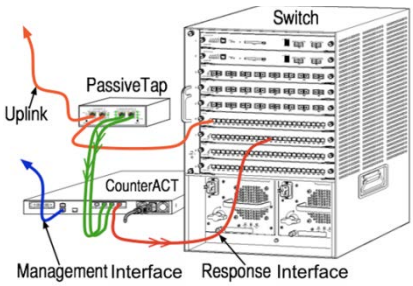
Cihazı anahtarınıza bağlamak için birkaç seçenek vardır.

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



Önerilen dağıtımda üç ayrı bağlantı noktası kullanılır. Bu bağlantı noktaları Cihaz Arabirim Bağlantıları bölümlerinde açıklanmıştır.

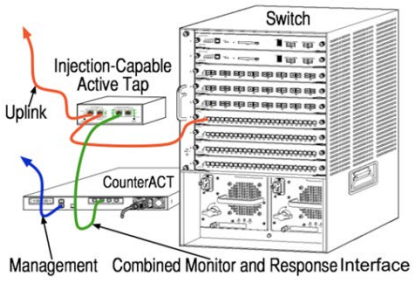
2 Hatta Bağlı Pasif Takip Cihazı



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

Hatta bağlı pasif takip cihazı, iki çift yönlü akışı tek bağlantı noktasında birleştiren *yeniden birleşme* takip cihazları haricinde, iki takip bağlantı noktası (biri yukarı yönlü trafik, biri aşağı yönlü trafik için) gerektirir. Takip cihazlı bağlantı noktasındaki trafik 802.1Q VLAN etiketliyse yanıt bağlantı noktası da 802.1Q VLAN etiketli olmalıdır.

3 Hatta Bağlı Aktif (Enjeksiyon Kabiliyetli) Takip Cihazı



Cihaz, hatta bağlı aktif bir takip cihazı kullanabilir. Takip cihazının enjeksiyon kabiliyeti varsa, Cihaz anahtarda ayrı bir yanıt bağlantı noktası yapılandırmaya gerek duyulmayacak şekilde takip ve yanıt bağlantı noktalarını birleştirir. Bu seçenek her türlü yukarı yönlü veya aşağı yönlü anahtar yapılandırmasında kullanılabilir.

4 IP Katmanı Yanıtı (Katman-3 Anahtar Kurulumları için)

Cihaz, trafiğe yanıt vermek için kendi yönetim arabirimini kullanabilir. Bu seçenek, takip edilen her trafikte kullanılabilmesine rağmen, sadece Cihazın VLAN'ın parçası olmayan bağlantı noktalarını takip ettiği durumlarda 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 Ayar Notları

VLAN (802.1Q) Etiketleri

- ***Tek VLAN Takibi***: Takip edilen trafik tek VLAN kaynaklıysa, trafik için 802.1Q VLAN etiketleri gerekli değildir.
- ***Çoklu VLAN'ların Takibi***: Takip edilen trafik iki veya daha fazla VLAN kaynaklıysa, takip edilen ve yanıt bağlantı noktalarının *her ikisi* için de 802.1Q VLAN etiketlemesi etkin olmalıdır. Yansıtılan bağlantı noktası sayısını minimize ederken en iyi genel kapsamı sunduğu için birden fazla VLAN'ın takip edilmesi önerilir.
- Anahtar, yansıtılan bağlantı noktasında 802.1Q VLAN etiketi kullanamıyorsa şunlardan birini yapın:
  - Sadece bir VLAN yansıtın
  - Tek bir etiketlenmemiş yukarı bağlantı noktasını yansıtın
  - IP katmanı yanıt seçeneğini kullanın
- Anahtar sadece bir bağlantı noktasını yansıtabiliyorsa tek yukarı bağlantı noktasını yansıtın. Bu bağlantı noktası etiketlenmiş olabilir. Genel olarak, anahtar 802.1Q VLAN etiketlerini çıkarırsa IP katmanı yanıt seçeneğini kullanmanız gerekir.

Ek Kurallar

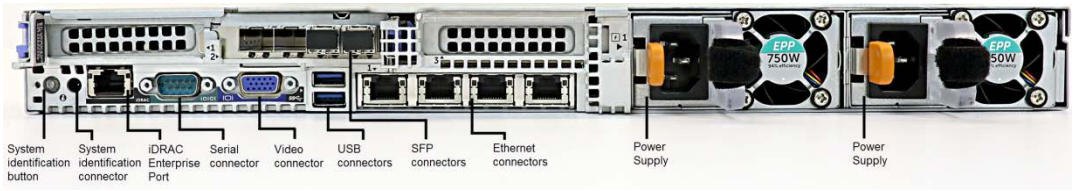
- Aşağıdaki durumlarda sadece bir arabirimi yansıtmalısınız (aktarma/alma özelliğine izin vermeyen):
  - Anahtar hem aktarılan hem alınan trafiği yansıtamıyorsa
  - Anahtar tüm anahtar trafiğini yansıtamıyorsa
  - Anahtar VLAN üzerinden tüm trafiği yansıtamıyorsa
- Yansıtma bağlantı noktasını aşırı yüklemediğinizi doğrulayın.
- Bazı anahtarlar (ör. Cisco 6509), yeni bir yapılandırma girmeden önce mevcut bağlantı noktası yapılandırmasının tamamen silinmesini gerektirebilir. Eski bağlantı noktası bilgilerinin silinmemesi genelde anahtarın 802.1Q etiketlerini çıkarmasını sağlar.

3. Ağ Kablolarını Bağlayın ve Cihazı Çalıştırın

A. Cihazı Ambalajından Çıkarın ve Kabloları Bağlayın

1. Cihazı ve güç kablosunu gönderim kabından çıkarın.
2. Cihazla birlikte gönderilen ray kitini çıkarın.
3. Ray kitini Cihaza takın ve Cihazı kabine monte edin.
4. Cihazın arka paneli ve anahtar bağlantı noktaları üzerindeki ağ arabirimleri arasında yer alan ağ kablolarını bağlayın.

Arka Panel Örneği – CounterACT Aygıtı



ForeScout tarafından temin edilen SFP'leri, ForeScout tarafından test edilen ve onaylanan Finisar SFP'leriyle değiştirebilirsiniz. Daha fazla ayrıntı için *CounterACT Kurulum Kılavuzu*'na bakın.

B. Arabirim Atamalarını Kaydedin

Veri merkezinde Cihaz kurulumunu tamamladıktan ve CounterACT Konsolunu kurduktan sonra, arabirim atamalarını kaydetmeniz istenecektir. *Kanal tanımları* olarak bilinen bu atamalar, Konsolda ilk oturum açtığınızda karşınıza çıkan İlk Kurulum Sihirbazına girilir.

Aşağıdaki fiziksel arabirim atamalarını kaydedin ve Konsolda Kanal kurulumunu tamamlarken kullanın.

Eth Arabirimi	Arabirim Ataması (ör. Yönetim, Takip, Yanıt)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	

Eth5	
Eth6	
Eth7	

C. Cihazı Çalıştırın

1. Güç kablosunu Cihaz arka panelindeki güç kablosuna bağlayın.
2. Güç kablosunun diğer ucunu topraklanmış bir AC çıkışına bağlayın.
3. Klavyeyi ve monitörü Cihaza bağlayın veya seri bağlantı için Cihazı kurun. Daha fazla bilgi için *CounterACT Kurulum Kılavuzu*'na bakın.
4. Cihaza ön panelden güç verin.

4. Cihazı Yapılandırın

Cihazı yapılandırmadan önce aşağıdaki bilgileri hazırlayın.

Cihaz ana bilgisayar adı	
CounterACT Yönetici şifresi	Şifreyi güvenli bir yerde saklayın
Yönetim arabirimi	
Cihaz IP adresi	
Ağ maskesi	
Varsayılan Ağ Geçidi IP adresi	
DNS Alan Adı	
DNS sunucu adresleri	

Güç verdikten sonra aşağıdaki mesajla yapılandırmaya başlamanız istenecektir:

```
CounterACT Cihaz başlatma tamamlandı.
Devam etmek için <Enter>'a basın.
```

1. **Enter** tuşuna basın. 51xx CounterACT aygıtınız varsa, aşağıdaki menü belirir:

```
CounterACT 8.0.0-<build> seçenekleri:


1) CounterACT'i yapılandırın
2) Kaydedilen CounterACT yapılandırmasını geri yükleyin
3) Ağ arabirimlerini belirleyin ve yeniden numaralandırın
4) Klavye düzenini yapılandırın
5) Makineyi kapatın
6) Makineyi yeniden başlatın

Seçenek (1-6) :1
```

CT-xxxx CounterACT aygıtınız varsa, menünün üstünde sürüm olarak CounterACT 7.0.0 veya CounterACT 8.0.0 listelenir.

- CounterACT 7.0.0 görürseniz, 8.0.0 sürümüne yükseltebilir veya en baştan kurabilirsiniz. Ayrıntılar için *CounterACT Kurulum Kılavuzu*'na bakın. 8.0.0 sürümüne yükselttikten sonra veya yeniden kurduktan sonra yukarıda listelenen menüyü görürsünüz.
- CounterACT 8.0.0 görürseniz, menüde aşağıda gösterildiği gibi CounterACT 7.0.0 kurulumu veya CounterACT 8.0.0 yapılandırması seçeneği sunulur. ICounterACT 7.0.0'ı seçerseniz, Yapılandırma menüsü yoluyla CounterACT 8.0.0'ı yeniden kuramazsınız. CounterACT 7.0.0 yapılandırmasıyla ilgili ayrıntılar için bkz. *CounterACT Kurulum Kılavuzu sürüm 7.0.0*.

```
CounterACT 8.0.0-<build> seçenekleri:

1) CounterACT 7.0.0-<build>'ı kurun
2) CounterACT 8.0.0-<build>'ı yapılandırın
3) Kaydedilen CounterACT yapılandırmasını geri yükleyin
4) Ağ arabirimlerini belirleyin ve yeniden numaralandırın
5) Klavye düzenini yapılandırın
6) Makineyi kapatın
7) Makineyi yeniden başlatın

Seçenek (1-7) :
```

Yapılandırma yarıda kesilirse veya yanlış CounterACT sürümünü seçtiyseniz, Cihazın ilgili ISO dosyası sürümüyle yeniden görüntüsünü oluşturmalısınız. Yeniden Cihaz görüntüsü oluşturma hakkında daha fazla bilgi almak için CounterACT Kurulum Kılavuzu'na bakın.

2. **Configure CounterACT (CounterACT'ı Yapılandır)**'ı seçin. İstemde:

   Devam Et: (evet/hayır)?

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

3. Yüksek Kullanılabilirlik Modu istemi açılır. Standart Kurulumu seçmek için **Enter**'a basın.

4. CounterACT İlk Kurulum istemi görüntülenir. Devam etmek için **Enter** 'a basın.

5. CounterACT Kurulum Türünü Seç istemi açılır. Standart bir CounterACT Cihazı kurmak için **1** yazın ve **Enter**'a basın.

   Kurulum başlatılır. Bu, birkaç dakika sürebilir.

6. Lisanslama Modunu Seç istemi açılır. Dağıtımınızda kullanılan lisanslama modunu seçin. Lisanslama modu satın alma esnasında belirlenir. ***Dağıtımınızda kullanılan lisanslama modunu doğrulamadan önce bir değer girmeyin***. Lisanslama modunuzu doğrulamak için veya yanlış mod girdiyseniz ForeScout temsilcinizle irtibata geçin.

7. Makine Açıklamasını Gir isteminde, bu aygıtı tanımlayan kısa metni girin ve **Enter**'a basın.

   Aşağıdaki istem görüntülenir:

```
>>>>>> Yönetici Şifresini Ayarla <<<<<<
Bu şifre, makine İşletim Sisteminde "kök" olarak ve CounterACT
Konsolunda "yönetici" olarak oturum açmak için kullanılır.
Şifre 6 ile 15 karakter arasında olmalı ve en az bir alfabetik
olmayan karakter içermelidir.
Yönetici şifresi:
```

8. Yönetici Şifresini ayarla isteminde, şifreniz olacak diziyi girin (dizi ekrana yansıtılmaz) ve **Enter**'a basın. Şifreyi doğrulamanız istenir. Şifre 6 ile 15 karakter arasında olmalı ve en az bir alfabetik olmayan karakter içermelidir.

Cihazda kök *olarak ve Konsolda* yönetici *olarak oturum açın.*

9. Ana Bilgisayar Adını Ayarla isteminde, ana bilgisayar adını girin ve **Enter**'a basın. Ana bilgisayar adı Konsolda oturum açarken kullanılabilir ve görüntülediğiniz CounterACT Cihazını belirlemenize yardımcı olması için Konsolda görüntülenir. Ana bilgisayar adı uzunluğu 13 karakteri geçmemelidir.
10. Ağ Ayarlarını Yapılandır ekranı, sizden bir dizi yapılandırma parametresi ister. Her istemde bir değer girin ve bir sonraki istemi görüntülemek için **Enter**'a basın.
    - CounterACT bileşenleri yönetim arabirimleri yoluyla iletişim kurar. Listelenen yönetim arabirimi sayısı Cihaz modeline bağlıdır.
    - **Management IP address (Yönetim IP adresi)** CounterACT bileşenlerinin iletişim kurduğu arabirimin adresidir. Bu arabirim için, sadece CounterACT bileşenleri arasında iletişim için kullanılan arabirim etiketli bağlantı noktasına bağlı ise bir VLAN Kimliği ekleyin.
    - Birden fazla **DNS server address (DNS sunucu adresi)** varsa, her adresi boşluk ile ayırın. İç DNS sunucularının çoğu dış ve iç adresleri çözebilir, ancak dışarıdan çözen bir DNS sunucusu dâhil etmeniz gerekebilir. Cihaz tarafından gerçekleştirilen DNS sorgularının neredeyse tümü iç adresler için olacağından, dış DNS sunucusu en sonda listelenmelidir.
11. Kurulum Özeti ekranı görüntülenir. Genel bağlantı testleri yapmanız istenirse, ayarları yeniden yapılandırın veya kurulumu tamamlayın. Kurulumu tamamlamak için **D** yazın.

Lisans

Yapılandırmanın ardından, CounterACT aygıtınızın geçerli bir lisansa sahip olduğundan emin olun. CounterACT aygıtınızın varsayılan lisanslama durumu, dağıtımınızda hangi lisanslama modunun kullanıldığına bağlıdır.

- CounterACT dağıtımınız, ***Cihaz Başına Lisanslama Modu***'nda çalışıyorsa, 30 gün geçerli olan deneme lisansını kullanarak çalışmaya başlayabilirsiniz. Bu dönemde, ForeScout'tan kalıcı bir lisans almalısınız ve diskinizde veya ağınızda erişilebilir bir klasöre yerleştirmelisiniz. 30 günlük deneme lisansının süresi dolmadan buradan lisansı kurun (Gerekliyse, deneme lisansını uzatmayı talep edebilirsiniz).

  Deneme lisansı süresinin dolmak üzere olduğu size birkaç yolla bildirilir. Deneme lisansı uyarıları hakkında daha fazla bilgi için *CounterACT İdare Kılavuzu*'na bakın.

  Bir CounterACT sanal sistemiyle çalışıyorsanız:

  - Deneme lisansı bu aşamada otomatik olarak kurulmaz. ForeScout temsilcinizden e-posta ile aldığınız deneme lisansını kurmalısınız.
  - En az bir CounterACT aygıtının İnternete erişimi olmalıdır. Bu bağlantı, CounterACT lisanslarını ForeScout Lisans sunucusunda doğrulamak için kullanılır. Bir ay boyunca doğrulanmayan lisanslar iptal edilir. CounterACT, her gün sunucuyla iletişim hatası olduğunu bildiren bir uyarı e-postası gönderir.

    Daha fazla bilgi için *CounterACT Kurulum Kılavuzu*'na bakın.

- CounterACT dağıtımınız, ***Merkezi Lisanslama Modu***'nda çalışıyorsa, *Yetkilendirme yöneticisi*, lisans yetkilendirmesi ForeScout Müşteri Portalı'nda oluşturulduğunda ve kullanılabilir olduğunda bir e-posta almalıdır. Kullanılabilir olduktan sonra, dağıtımın *CounterACT yöneticisi* CounterACT Konsolunda lisansı etkinleştirebilir. Lisans etkinleştirilene kadar, CounterACT işlevleri doğru şekilde çalışmaz. Örneğin politikalar değerlendirilmez ve eylemler gerçekleştirilmez. *Sistem kurulumu sırasında deneme lisansı otomatik olarak kurulmaz.*

Lisans yönetimi hakkında daha fazla bilgi için *CounterACT İdare Kılavuzu*'na bakın.

5. Uzaktan Yönetim

iDRAC Kurulumu

Entegre Dell Uzaktan Erişim Kontrolörü (iDRAC), LAN veya İnternet üzerinden CounterACT Cihazlarına lokasyondan bağımsız/OS'tan bağımsız uzaktan erişim sağlayan entegre bir sunucu sistemi çözümüdür. KVM erişimi, güç açma/kapama/sıfırlama ve onarım ve bakım görevlerini gerçekleştirmek için modülü kullanın.

iDRAC modülüyle çalışmak için aşağıdakileri yapın:

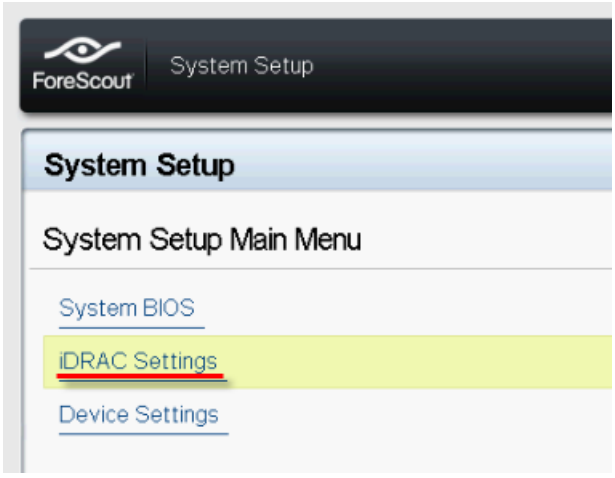
- iDRAC Modülünü Etkinleştirin ve Yapılandırın
- Modülü Ağa Bağlayın
- iDRAC'ta oturum açın

iDRAC Modülünü Etkinleştirin ve Yapılandırın

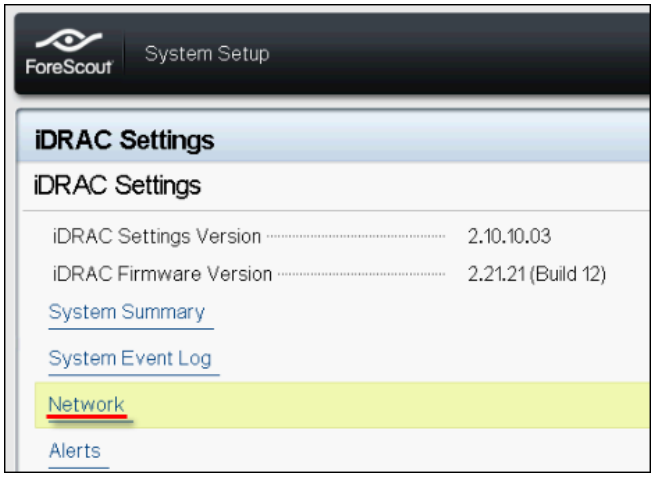
CounterACT aygıtında uzaktan erişimi etkinleştirmek için iDRAC ayarlarını değiştirin. Bu bölümde, CounterACT ile çalışmak için gerekli temel entegrasyon ayarları açıklanmaktadır.

iDRAC'ı yapılandırmak için:

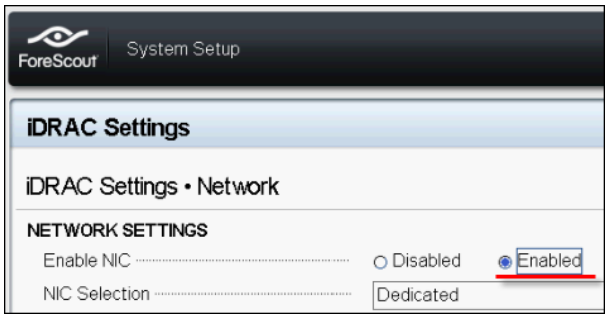
1. Yönetilen Cihazı açın.
2. Başlatma süreci sırasında F2'yi seçin.
3. Sistem Kurulumu Ana Menü sayfasında, **iDRAC Settings (iDRAC Ayarları)**'nı seçin.



4. iDRAC Ayarları sayfasında **Network (Ağ)**'ı seçin.

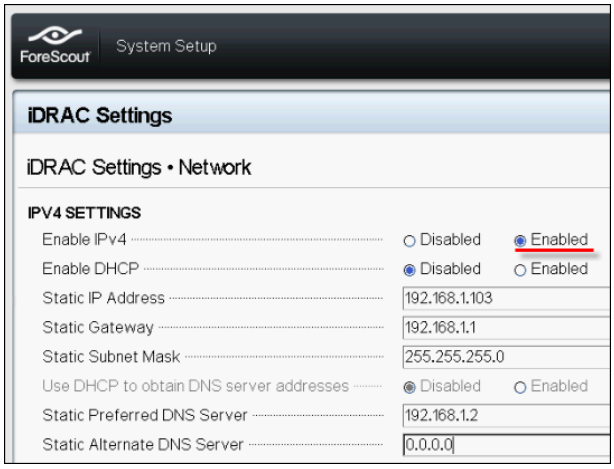


5. Aşağıdaki Ağ ayarlarını yapılandırın:
   - ***Network Settings (Ağ Ayarları)***. **Enable NIC (NIC'i Etkinleştir)** alanının **Enabled (Etkin)** olarak ayarlandığını doğrulayın.



   - ***Genel Ayarlar***. DNS DRAC Adı alanında, dinamik bir DNS'i güncelleyebilirsiniz (İsteğe bağlı).
   - ***IPV4 Settings (IPV4 Ayarları)***. **Enable IPv4 (IPv4'ü Etkinleştir)** alanının **Enabled (Etkin)** olarak ayarlandığını doğrulayın.

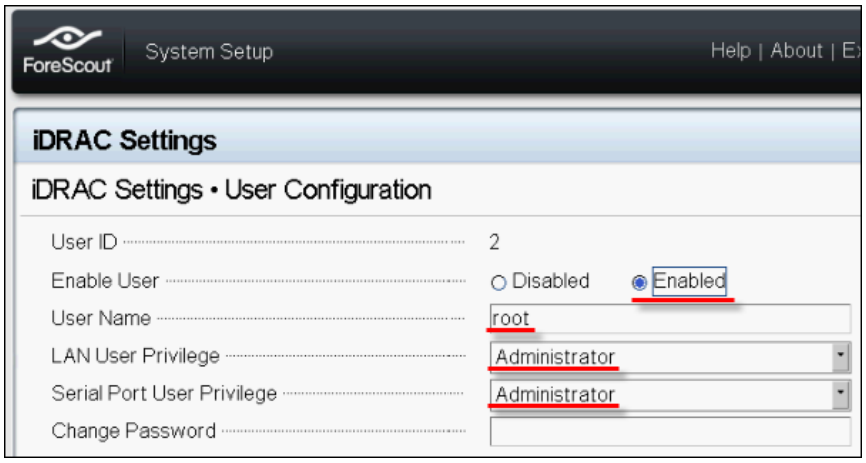
     Enable DHCP (DHCP'yi Etkinleştir) alanını, Dinamik IP Adresi kullanmak için **Enabled (Etkin)** olarak veya Sabit IP Adresi kullanmak için **Disabled (Devre Dışı)** olarak ayarlayın. Etkinleştirilmişse, DHCP IP adresini, ağ geçidini ve alt ağ maskesini iDRAC'a otomatik olarak atar. Devre dışı ise, **Static IP Address (Sabit IP Adresi)**, **Static Gateway (Sabit Ağ Geçidi)** ve **Static Subnet Mask (Sabit Ağ Maskesi)** alanlarına değer girin.



6. **Back (Geri)**'yi seçin.
7. **User Configuration (Kullanıcı Yapılandırması)**'nı seçin.
8. Kök kullanıcı için aşağıdaki Kullanıcı Yapılandırması alanlarını yapılandırın:
   - ***Enable User (Kullanıcıyı Etkinleştir)***. Bu alanın Etkin olarak ayarlandığını doğrulayın.

     Burada yapılandırılan kullanıcı adı, CounterACT kullanıcı adıyla aynı değildir.

   - ***LAN and Serial Port User Privileges (LAN ve Seri Bağlantı Noktası Kullanıcı Ayrıcalıkları)***. Ayrıcalık düzeylerini Administrator (Yönetici)'ye ayarlayın.
   - ***Change Password (Şifreyi Değiştir)***. Kullanıcının oturum açması için bir şifre belirleyin.

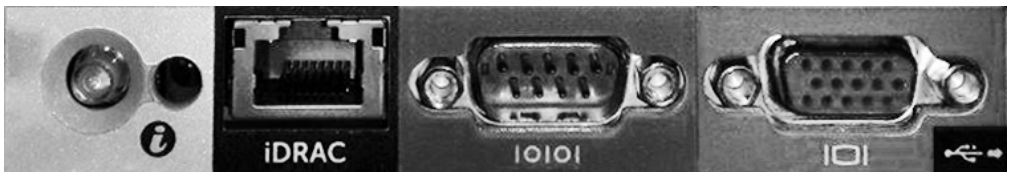


9. **Back (Geri)**'yi ve ardından **Finish (Bitir)**'i seçin. Değiştirilen ayarları doğrulayın.

   Yapılandırılan ayarlar kaydedilir ve sistem yeniden başlatılır.

Modülü Ağa Bağlayın

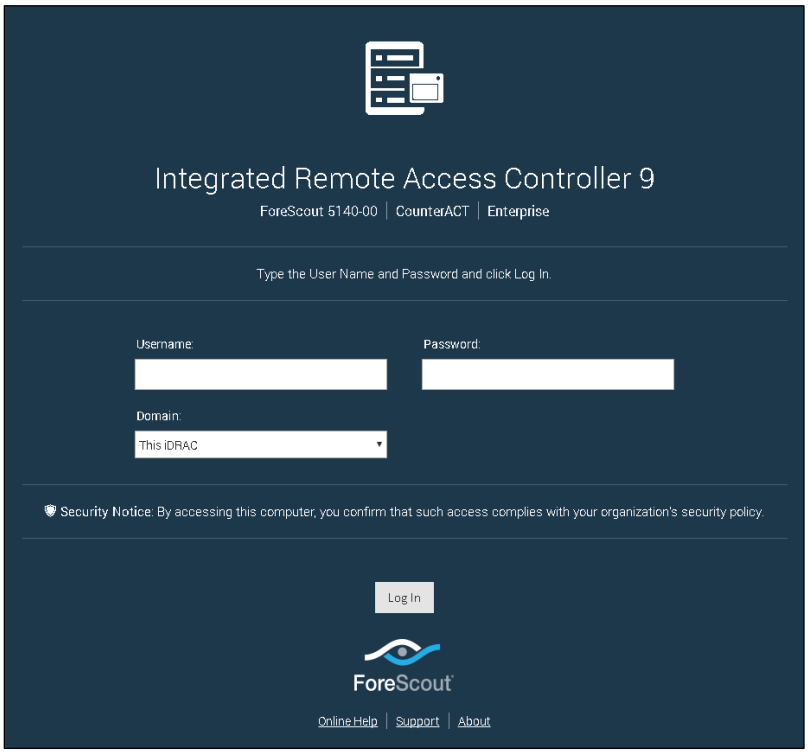
iDRAC bir Ethernet ağına bağlanır. Genelde bir yönetim ağına bağlanır. Aşağıdaki görselde CT-1000 Cihazının arka panelinde iDRAC bağlantı noktasının yeri gösterilmektedir:



iDRAC'ta oturum açın

iDRAC'ta oturum açmak için:

1. **iDRAC Settings (iDRAC Ayarları)** > **Network (Ağ)**'da yapılandırılan IP Adresi veya alan adına göz atın.



2. iDRAC sistem kurulumunun Kullanıcı Yapılandırması sayfasında yapılandırılan Kullanıcı Adını ve Şifreyi girin.
3. **Submit (Gönder)**'i seçin.

iDRAC hakkında daha fazla bilgi için *iDRAC Kullanım Kılavuzu*'na bakın. Dağıtımınızda kullanılan lisanslama moduna bağlı olarak bu kılavuza erişim sağlamak için aşağıdakilerden birini kullanabilirsiniz:

- Cihaz Başına Lisanslama Modu - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf

- Merkezi Lisanslama Modu – Müşteri Portalı, Dokümantasyon sayfası.

Dağıtımınızda hangi lisanslama modunun kullanıldığını öğrenmek için bkz. Ek CounterACT Dokümantasyonu (*Konsolda Lisanslama Modunuzu Belirleme*).

Henüz yapmadıysanız, varsayılan kök şifresini güncellemeniz çok önemlidir.

6. Bağlanabilirliği Doğrulayın

Yönetim Arabirim Bağlantısını Doğrulayın

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

`fstool linktest`

Aşağıdaki bilgiler görüntülenir:

```
Yönetim Arabirimi durumu
Ping yapılan varsayılan ağ geçidi bilgileri
Ping istatistikleri
Ad Çözümleme Testi Yapma
Test özeti
```

Ping Testi Yapın

Bağlantıyı doğrulamak için Cihazdan ağ masaüstüne aşağıdaki komutu çalıştırın:

`Ping <network_desktop_IP_address>`

7. CounterACT Konsolunu Ayarlayın

CounterACT Konsolunu Kurun

Konsol, uç noktalar hakkında önemli bilgilerin ayrıntılarını görüntülemek ve uç noktaları kontrol etmek için kullanılan CounterACT yönetim uygulamasıdır. Söz konusu bilgiler CounterACT aygıtları tarafından toplanır. Daha fazla bilgi için *CounterACT İdare Kılavuzu*'na bakın.

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

- Şunları çalıştıran atanmamış makine:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- 2 GB RAM
- 1 GB disk alanı

Konsol kurulumu için aşağıdaki yöntem kullanılır:

Cihazınızdaki kurulum yazılımını kullanın.

1. Konsol bilgisayarından bir tarayıcı penceresi açın.
2. Tarayıcı adres satırına aşağıdakileri girin:

   `http://<Appliance_ip>/install`

   Appliance_ip bu Cihazın IP adresidir. Tarayıcı, Konsol kurulum penceresini gösterir.
3. Ekrandaki talimatları izleyin.

Oturum Açın

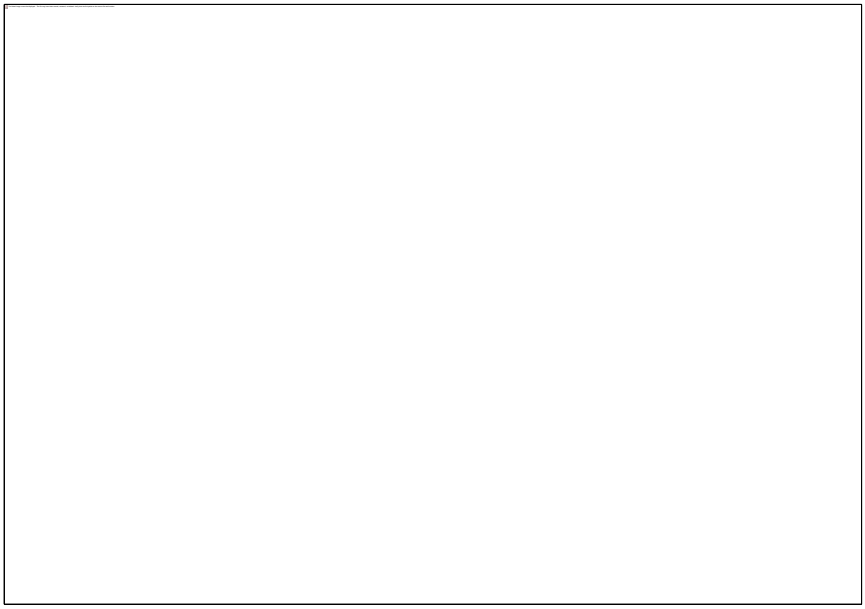
Kurulumu tamamladıktan sonra, CounterACT Konsolunda oturum açabilirsiniz.

1. Oluşturduğunuz kısayol konumundan CounterACT simgesini seçin.

2. **IP/Name (IP/Ad)** alanına Cihazın IP adresini veya ana bilgisayar adını girin.
3. **User Name (Kullanıcı Adı)** alanına yöneticiyi girin.
4. **Password (Şifre)** alanına Cihaz kurulumu esnasında oluşturduğunuz şifreyi girin.
5. Konsolu başlatmak için **Login (Oturum Aç)**'ı seçin.

İlk Kurulumu Yapın

İlk kez oturum açtığınızda, İlk Kurulum Sihirbazı açılır. Sihirbaz, CounterACT'ı hızlı ve verimli bir şekilde kurmanız ve çalıştırmanız için sizi gerekli yapılandırma adımlarına yönlendirir.



İlk Kurulumu Başlatmadan Önce

Sihirbazla çalışmaya başlamadan önce aşağıdaki bilgileri hazırlayın:

Sihirbaz için Gerekli Bilgiler	**Değer**
Kuruluşunuz tarafından kullanılan NTP sunucu adresi (isteğe bağlı)	
Cihazdan SMTP trafiğine izin verilmiyorsa, e-posta uyarılarının gönderilmesini sağlayan iç posta geçişi IP adresi (isteğe bağlı)	
CounterACT yönetici e-posta adresi	
Takip ve yanıt arabirimleri	
DHCP'si olmayan segmentler/VLAN'lar için, yanıt arabiriminin doğrudan bağlı olduğu ağ segmenti/VLAN'ları ve bu VLAN'ların her birinde CounterACT tarafından kullanılacak daimi IP adresi	
Bu Cihazın takip edeceği IP adresi aralığı (kullanılmayan adresler dâhil, tüm iç adresler)	
LDAP kullanıcı hesap bilgileri ve LDAP sunucusu IP adresi	
▪ Alan idari hesap adı ve şifresi dâhil alan kullanıcı bilgileri	
CounterACT'ın hangi ağ ana bilgisayarlarının başarılı bir şekilde doğrulandığını analiz edebilmesi için doğrulama sunucuları	
Anahtar IP Adresi, Sağlayıcı ve SNMP Parametreleri	

Sihirbazla çalışmak konusunda daha fazla bilgi için *CounterACT İdare Kılavuzu*'na veya Online Yardım'a bakın.

Ek CounterACT Dokümantasyonu

CounterACT özellikleri ve modülleri hakkında bilgi için aşağıdaki kaynaklara bakın:

- İndirilecek Dokümantasyon
- Dokümantasyon Portalı
- CounterACT Yardım Araçları

İndirilecek Dokümantasyon

Dağıtımınızda hangi lisanslama modunun kullanıldığına bağlı olarak indirilecek dokümantasyona iki ForeScout portalından erişim sağlanabilir.

- ***Cihaz Başına Lisanslama Modu*** - Ürün Güncellemeleri Portalı
- ***Merkezi Lisanslama Modu*** - Müşteri Portalı

Bu portallardan yazılım da indirebilirsiniz.

Dağıtımınızda hangi lisanslama modunun kullanıldığını öğrenmek için, bkz. Konsolda Lisanslama Modunuzu Belirleme.

Ürün Güncellemeleri Portalı

Ürün Güncellemeleri Portalında, çıkan CounterACT sürümleri, Temel ve İçerik Modülleri ve Genişletilmiş Modüller ve ilgili dokümantasyona bağlantılar bulunur. Portal aynı zamanda çeşitli ek dokümantasyon da sunar.

Ürün Güncellemeleri Portalına erişim sağlamak için:

1. Https://updates.forescout.com/support/index.php?url=counteract adresine gidin.
2. Keşfetmek istediğiniz CounterACT sürümünü seçin.

Müşteri Portalı

ForeScout Müşteri Portalının Downloads (İndirmeler) sayfasında satın alınan CounterACT sürümleri, Temel ve İçerik Modülleri ve Genişletilmiş Modüller ve ilgili dokümantasyona bağlantılar bulunur. İndirmeler sayfasında yazılım ve ilgili dokümantasyon sadece yazılım için lisans yetkisine sahipseniz görüntülenir. Portaldaki Dokümantasyon sayfası aynı zamanda çeşitli ek dokümantasyon da sunar.

ForeScout Müşteri Portalındaki dokümantasyona erişim sağlamak için:

1. Https://forescout.force.com/support/ adresine gidin.
2. **Downloads (İndirmeler)** veya **Documentation (Dokümantasyon)**'u seçin.

Dokümantasyon Portalı

ForeScout Dokümantasyon Portalı, CounterACT araçları, özellikleri, işlevleri ve entegrasyonları hakkında bilgi içeren arama yapılabilen, web-tabanlı bir kütüphanedir.

Dağıtımınızda Merkezi Lisanslama Modu kullanılıyorsa, bu portala erişim sağlamak için gerekli kullanıcı bilgilerine sahip olmayabilirsiniz.

Dokümantasyon Portalına erişim sağlamak için:

1. Www.forescout.com/docportal adresine gidin.
2. Oturum açmak için müşteri desteği kullanıcı bilgilerinizi kullanın.
3. Keşfetmek istediğiniz CounterACT sürümünü seçin.

CounterACT Yardım Araçları

Bilgilere doğrudan CounterACT Konsolundan erişim sağlayın.

Konsol Yardım Düğmeleri

Çalıştığınız görevler ve konular hakkındaki bilgilere hızlıca erişim sağlamak için bağlama duyarlı *Help (Yardım)* düğmelerini kullanın.

CounterACT İdare Kılavuzu

Help (Yardım) menüsünden **CounterACT Help (CounterACT Yardım)**'ı seçin.

Eklenti Yardım Dosyaları

1. Eklenti kurulduktan sonra, **Tools (Araçlar)** menüsünden **Options (Seçenekler)**'i ve ardından **Modules (Modüller)**'i seçin.
2. Eklentiyi ve ardından **Help (Yardım)**'ı seçin.

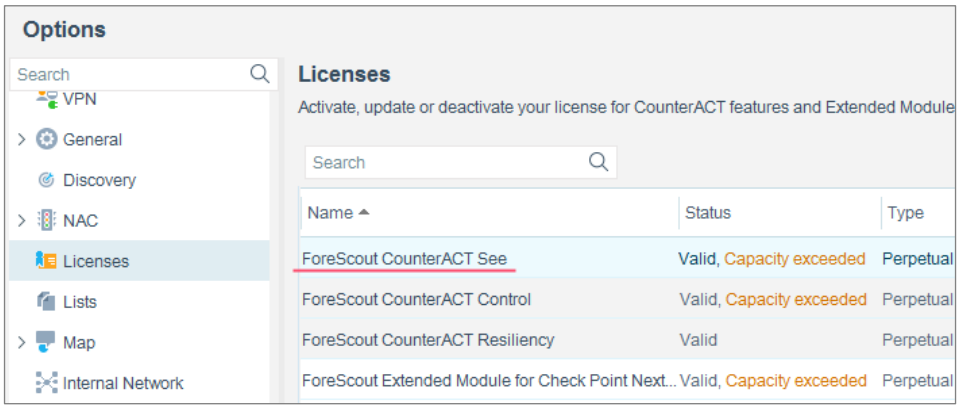
Dokümantasyon Portalı

Help (Yardım) menüsünden **Documentation Portal (Dokümantasyon Portalı)**'nı seçin.

Konsolda Lisanslama Modunuzu Belirleme

Enterprise Manager'ınız Konsolda listelenmiş bir *ForeScout CounterACT Görme* lisansına sahipse, dağıtımınız Merkezi Lisanslama Modunda çalışıyordur. Değilse, dağıtımınız Cihaz Başına Lisanslama Modunda çalışıyordur.

Tabloda listelenmiş *ForeScout CounterACT Görme* lisansınız olup olmadığını görmek için **Options > Licenses (Seçenekler > Lisanları)** seçin.



Lisanslama modunuzu belirleme hakkında herhangi bir sorunuz varsa, ForeScout temsilcinizle irtibata geçin.

Yasal Uyarı

Bu ürünler, ForeScout tarafından geliştirilen yazılımlara dayalıdır. Bu belgede açıklanan ürünler aşağıdaki ABD patentlerinden biri veya birkaçı tarafından korunuyor olabilir: #6,363,489, #8,254,286, #8,590,004, #8,639,800 ve #9,027,079 ve diğer ABD veya yabancı patentler tarafından da korunuyor olabilir.

Bu belgeyle ilgili yorumlarınızı ve sorularınızı aşağıdaki adrese gönderin: support@forescout.com

2018-03-27 15:04