

VPN İstemcisi Kullanım Kılavuzu

9236267

1. Baskı

© 2004 Nokia telif hakkıdır. Tüm hakları mahfuzdur.

Bu belge içindekilerin tamamı veya bir bölümü, Nokia'nın önceden yazılı izni alınmaksızın herhangi bir biçimde yeniden oluşturulamaz, kopyalanamaz, çoğaltılamaz, taklit edilemez, başka bir yere aktarılamaz, dağıtılamaz, saklanamaz veya yedeklenemez.

Nokia, Nokia Corporation'in tescilli ticari markasıdır. Burada adı geçen diğer ürün ve şirket isimleri, kendi sahiplerinin ticari markaları ve ticari adları olabilir.

Symbian and Symbian OS are trademarks of Symbian Ltd.

SecurID is a registered trademark of RSA Security INC.

Nokia, sürekli bir gelişim politikası izlemektedir. Nokia, bu belgede tanımlanan herhangi bir üründe önceden bildirimde bulunmaksızın değişiklik ve yenilik yapma hakkını saklı tutar.

Nokia, hiçbir durumda, meydana gelme nedeni ne olursa olsun oluşabilecek herhangi bir gelir, kar veya veri kaybından veya özel, arızı, bir netice olarak hasıl olan ya da dolaylı hasar veya kayıplardan sorumlu tutulamaz.

İşbu belgenin içeriği 'olduğu gibi' sunulmaktadır. Yürürlükteki kanunların gerektirdiği haller dışında, ticari olarak satılabilirlik, iyi bir evsafa olma ve belirli bir amaca uygunluk ile ilgili zımnî garantiler de dahil olmak üzere ancak bunlarla kısıtlı olmamak şartıyla, işbu belgenin doğruluğu, güvenilirliği veya içeriği ile ilgili olarak, açık veya zımnî herhangi bir garanti verilmemiştir. Nokia, herhangi bir zamanda, önceden bildirimde bulunmaksızın, işbu belgeyi değiştirme veya geçersiz kılma hakkını saklı tutar. Bazı ürünlerin temini, bölgelere göre farklılık gösterebilir. Bu konuda, lütfen size en yakın Nokia bayiine danışınız.

İçindekiler

Sanal Özel Ağ.....	4
--------------------	---

Yükleme	6
---------------	---

Sistem gereksinimleri.....	6
----------------------------	---

VPN poliçeleri.....	7
---------------------	---

VPN poliçelerini VPN poliçe sunucularından yükleme	7
--	---

VPN poliçelerini SIS dosyalarından yükleme.....	8
---	---

VPN poliçelerini görüntüleme	8
------------------------------------	---

Poliçe durumu	9
---------------------	---

Sertifika durumu	9
------------------------	---

Varsayılan değerlerle VPN erişim noktası	
--	--

oluşturma.....	10
----------------	----

VPN poliçelerini güncelleştirme.....	10
--------------------------------------	----

VPN poliçelerini silme.....	11
-----------------------------	----

VPN poliçe sunucuları	12
-----------------------------	----

VPN poliçe sunucularına bağlanma.....	12
---------------------------------------	----

Ayarları SIS dosyalarından yükleme	12
--	----

VPN poliçe sunucularını görüntüleme	13
---	----

VPN poliçe sunucuları ekleme.....	13
-----------------------------------	----

VPN poliçe sunucularını düzenleme	15
---	----

VPN poliçe sunucularını senkronize etme.....	15
--	----

VPN sertifikalarının kaydı	16
----------------------------------	----

VPN poliçe sunucularını silme.....	16
------------------------------------	----

VPN erişim noktaları	17
----------------------------	----

VPN erişim noktalarını görüntüleme.....	17
---	----

VPN erişim noktası oluşturma.....	17
-----------------------------------	----

VPN erişim noktalarını silme.....	18
-----------------------------------	----

VPN işlem kaydı	19
-----------------------	----

VPN işlem kaydını görüntüleme	19
-------------------------------------	----

VPN işlem kaydını silme.....	19
------------------------------	----

Anahtar saklama şifreleri	20
---------------------------------	----

Anahtar saklama şifresi oluşturma veya	
--	--

değiştirme.....	20
-----------------	----

Anahtar saklama şifrelerini girme	20
---	----

VPN ve uygulamalar	22
--------------------------	----

VPN ağ geçitlerinde kimlik doğrulaması	
--	--

gerçekleştirme	22
----------------------	----

Sorun giderme.....	24
--------------------	----

Dizin	29
-------------	----

1. Sanal Özel Ağ

➡ *Menü*'ye gidip
Araçlar→*Ayarlar*→*Bağlantı*
ayarları→*VPN* seçeneğini
belirleyin.

Bir **sanal özel ağ** (VPN) kullanarak, işyerinden uzaktayken gereksinim duyduğunuz bilgilere erişmek için şifreli bağlantılar oluşturabilirsiniz. E-posta, veritabanı uygulamaları ve intranet için kuruluş ağınıza şifreli erişimle bağlantı kurabilir ve bunları denetleyebilirsiniz.

Bir VPN oluşturmak üzere eriştiğiniz bilgilerin gizliliğinin ve bütünlüğünün korunmasına yardımcı olmak amacıyla ağ geçidi ve mobil cihaz birbirinin kimliğini doğrular, şifreleme ve kimlik doğrulama algoritmalarına karar verir.

VPN bağlantıları oluşturmak için önce VPN erişim noktaları oluşturulur sonra da kuruluş ağına bağlanmak üzere uygulamalar kullanıldığı zaman VPN erişim noktaları seçilir. Kuruluş ağıyla VPN bağlantısı başka türde bir İnternet bağlantısı üzerinden oluşturulur. VPN bağlantısı oluşturulur ve veriler VPN erişim noktasına bağlandığınızda yüklenen VPN poliçesine göre şifrelenir.



Not: VPN'i kullanabilmek için, yöneticilerden VPN poliçe sunucusu ayarlarını almanız gerekir. Yöneticiler size bu ayarları **SIS** – Symbian yükleme sistemi (Symbian installation system) dosyası olarak gönderebilir.

Sanal özel ağı kullanabilmek için

1 VPN İstemcisini yükleyin.

Daha fazla bilgi için, bkz:“Yükleme” sayfa 6.

2 Bir VPN poliçe sunucusu bağlantısı belirleyin.

VPN poliçe sunucusunun ayarlarını belirleyebilir veya ayarları bir SIS dosyasından yükleyebilirsiniz.

Daha fazla bilgi için, bkz:“VPN poliçe sunucularına bağlanma” sayfa 12.



Not: VPN poliçelerini SIS dosyalarından yüklerseniz, VPN poliçe sunucularıyla bağlantı oluşturmanız gerekmez.

3 VPN poliçelerini VPN poliçe sunucusundan yükleyin.

Daha fazla bilgi için, bkz:“VPN poliçelerini VPN poliçe sunucularından yükleme” sayfa 7.

4 VPN erişim noktalarını oluşturun.

VPN erişim noktaları bir İnternet erişim noktası ve bir de VPN poliçesi belirler.
Daha fazla bilgi için, bkz:“VPN erişim noktası oluşturma” sayfa 17.



Not: VPN erişim noktaları VPN poliçeleriyle İnternet erişim noktalarını birleştirir. VPN poliçe sunucusunu ilk kez senkronize ettiğinizde, mobil cihaza yüklediğiniz her poliçe için uygun VPN erişim noktaları oluşturulur.

- 5 Kuruluş ağına bağlanan uygulamalar kullandığınızda bir VPN erişim noktası seçin.
Daha fazla bilgi için, bkz:“VPN ve uygulamalar” sayfa 22.
İnternet bağlantısı üzerine bir VPN bağlantısı oluşturulur.

2. Yüklemeye

VPN istemcisi standart **SIS** - Symbian yüklemeye sistemi (Symbian installation system) dosyası olarak alınır.

VPN istemcisi, uyumlu bir mobil cihaza diğer yazılımların yüklendiği gibi yüklenir. Mobil cihaza yazılım yüklemeye konusunda daha fazla bilgi için, mobil cihazın belgelerine bakın.

Yüklemeye tamamlandığında, değişikliklerin etkin olması için mobil cihazı kapatıp açın.

Yüklemeye tamamlandıktan sonra VPN istemcisi SIS dosyasına gereksiniminiz olmaz. Hafızada yer açmak için SIS dosyasını silin.

Sistem gereksinimleri

VPN istemcisini telefon hafızasına veya hafıza kartına yükleyebilirsiniz. VPN istemcisinin yüklenmesi sırasında telefon hafızasında, yüklemeye paketinin iki katı büyüklüğünde yer ayrılır. Her VPN poliçesi genellikle telefon hafızasında 1 K - 16 K yer ayırır.

3. VPN poliçeleri

VPN poliçeleri mobil cihazın ve ağ geçidinin birbirinin kimliğini doğrulamak için kullandığı kimlik doğrulama yöntemini ve verileri şifrelemek için kullandıkları şifreleme algoritmalarını tanımlar. Yöneticiler VPN poliçelerini oluşturur ve bunları VPN poliçe sunucularında depolar veya **SIS** - Symbian yükleme sistemi (Symbian installation system) dosyası biçiminde size iletir. VPN poliçelerini VPN poliçe sunucusundan veya SIS dosyalarından yükleyebilirsiniz.

➡ **Menü**'ye gidip **Araçlar**→ **Ayarlar**→ **Bağlantı ayarları**→ **VPN**→ **VPN yönetimi**→ **VPN poliçeleri** seçeneğini belirleyin.

VPN poliçelerini VPN poliçe sunucularından yükleme

VPN poliçelerini yüklemek için

- 1 Boş bir **VPN poliçeleri** görünümüne gittiğinizde ve VPN poliçelerini yüklemeniz istendiğinde **Evet** tuşuna basın.
- 2 VPN poliçe sunucularını yüklemeniz istendiğinde **Evet** tuşuna basın.
- 3 VPN poliçe sunucusuna bağlanmak için ayarları belirtin.
Daha fazla bilgi için, bkz: "VPN poliçe sunucularına bağlanma" sayfa 12.
- 4 VPN poliçe sunucusunu senkronize etmeniz istendiğinde **Evet** tuşuna basın.
- 5 Bir **anahtar saklama şifresi** oluşturun.
Daha fazla bilgi için, bkz: "Anahtar saklama şifresi oluşturma veya değiştirme" sayfa 20.
VPN poliçe sunucusuna bağlanın.
- 6 Güven ilişkisi oluşturmak için **VPN poliçe sunucusu kimlik kodu**'nu doğrulayın.
VPN poliçe sunucusunun ayarlarını SIS dosyasından yüklediyseniz bu adımı geçebilirsiniz.
Daha fazla bilgi için, bkz: "VPN poliçe sunucuları ekleme" sayfa 13.

▶ **Sözlük:** VPN poliçe sunucuları VPN poliçelerini içeren kuruluş ağı üzerindeki sunuculardır.

▶ **Sözlük:** Anahtar saklama şifresi VPN poliçelerindeki özel anahtarların ve VPN poliçe sunucusu bağlantılarının izinsiz kullanıma karşı korunmasına yardımcı olur.

 **Sözlük:** VPN poliçe sunucusu kimlik kodu, sertifikayı tanımlayan VPN poliçe sunucusu sertifikasının parmak izidir.

 **Sözlük:** Bir anahtar alma şifresi VPN poliçe dosyasındaki özel anahtarların korunmasına yardımcı olur.

- 7 VPN poliçe sunucusuna erişmek için doğrulama bilgilerini girin ve **Tamam** tuşuna basın. Bu bilgileri size VPN poliçe sunucusunun yöneticisi sağlar.

VPN poliçeleri mobil cihaza yüklenir.

 **Not:** **Çıkış** tuşuna basarsanız, VPN poliçeleri yüklenmez. VPN poliçelerini VPN poliçe sunucusundan yüklemek için **Seçenek** tuşuna basıp **Poliçeyi yükle** seçeneğini belirleyin.

VPN poliçelerini SIS dosyalarından yükleme

Yöneticiler VPN poliçelerini size SIS dosyaları olarak iletebilir. VPN poliçelerini SIS dosyalarından yüklerseniz, VPN poliçe sunucularıyla bağlantıları tanımlamanız gerekmez. VPN poliçelerini yükledikten sonra, VPN erişim noktaları oluşturabilir ve bunları uygulamalarla ilişkilendirebilirsiniz.

VPN poliçeleri özel anahtarlar ve ilgili sertifikaları içeriyorsa, özel anahtarların korunmasına yardımcı olmak için yöneticiler **anahtar alma şifreleri** tanımlar. Anahtar alma şifresini size göndermek için yöneticilerin güvenli bir yöntem kullanması gerekir.

VPN poliçelerini SIS dosyalarından yüklemek için

- 1 **Anahtar alma şifresi:** alanına anahtar alma şifresini yazın ve **Tamam** tuşuna basın.
- 2 **Anahtar saklama şifresi:** alanına anahtar saklama şifresini yazın ve **Tamam** tuşuna basın.

VPN poliçelerini görüntüleme

VPN poliçeleri görünümü mobil cihaza yüklediğiniz VPN poliçelerini görüntüler.

(VPN poliçesi yok) görüntüleniyorsa, VPN poliçeleri yüklemeniz gerekir. VPN poliçelerini VPN poliçe sunucusundan yüklemek için **Seçenek** tuşuna basıp **Poliçeyi yükle** seçeneğini belirleyin.

Aşağıdaki bilgileri görüntülemek için bir VPN poliçesi seçin:

- **Açıklama:**—VPN poliçesindeki ek bilgiler. Yöneticiler açıklamayı VPN poliçesini oluştururken tanımlar.

- **Poliçe durumu:**—VPN poliçesinin kullanıma hazır veya zaten kullanımda olduğunu gösterir.
- **Sertifika durumu:**—mobil cihazda geçerli kullanıcı sertifikası olup olmadığını gösterir.
- **Poliçe ismi:**—VPN poliçesini oluştururken yöneticilerin VPN poliçesine verdiği isim.
- **Poliçe sunucusu:**—VPN poliçesini yüklediğiniz VPN poliçe sunucusunun ismi. VPN poliçe sunucularıyla bağlantı tanımlarken VPN poliçe sunucularına isim verilir. VPN poliçesini SIS dosyasından yüklediyseniz bu alan gizli olur.
- **Güncelleme:**—VPN poliçesinin VPN poliçe sunucusundan güncelleştirildiği son tarih. VPN poliçesini SIS dosyasından yüklediyseniz bu alan gizli olur.

Poliçe durumu



Not: VPN poliçesi ayrıntıları görünümü açıkken poliçe durumu değişirse, görünüm yenilenmez.

Poliçe durumu: alanında aşağıdaki değerler yer alabilir:

- **Kullanımda**—VPN poliçesiyle ilişkili bir VPN erişim noktasıyla bağlantı oluşturduunuz. Bağlantı oluşturduğunuzda, VPN poliçesi kullanıma alınır.
- **VPN erişim noktası ile bağlantılı**—VPN poliçesini bir veya birkaç VPN erişim noktasıyla ilişkilendirdiniz. VPN poliçesini kullanıma almak için bu VPN erişim noktalarından herhangi birini seçebilirsiniz.
- **VPN erişim noktası ile bağlantılı değil**—VPN poliçesini kullanıma almak için bir VPN erişim noktasıyla ilişkilendirmeniz gerekir.

Sertifika durumu

Sertifika durumu: alanında aşağıdaki değerler yer alabilir:

- **Tamam**—mobil cihazda en az bir geçerli sertifika var veya VPN ağ geçitlerinde kimlik doğrulama için sertifika kullanmıyorsunuz.
- **Süresi dolmuş**—bir veya daha fazla sertifikanın geçerlilik süresi dolmuş.

VPN bağlantısı oluşturamıyorsanız, yeni sertifika kaydı yapabilmek için VPN poliçesini güncelleştirmeyi deneyin.

- **Sertifika yok**—Gerekli sertifikalardan biri veya daha fazlası mobil cihazda bulunamadı. VPN bağlantısı oluşturamıyorsanız, yeni sertifika kaydı yapabilmek için VPN poliçesini güncelleştirmeyi deneyin.
- **Henüz geçerli değil**—bir veya daha fazla sertifika daha sonra kullanım içindir. Bu değer ayrıca mobil cihazdaki tarih ve saatin geçmişte bir değere ayarlandığı, saat dilimlerinin düzgün ayarlanmadığı veya yaz saati ayarının açık olmadığı anlamına da gelebilir.

Ayrıntıları kapatıp [VPN poliçeleri](#) görünümüne dönmek için seçim tuşuna basın.

Varsayılan değerlerle VPN erişim noktası oluşturma

VPN poliçesini kullanabilmek için, bunu bir VPN erişim noktasıyla ilişkilendirmeniz gerekir. [Seçenek](#) tuşuna basın ve [VPN poliçeleri](#) görünümünde [VPN eriş. nk. tanımla](#) seçeneğini belirleyin.

Mobil VPN İstemcisi, varsayılan ayarlarla bir VPN erişim noktası oluşturur. VPN erişim noktaları görünümünde VPN erişim noktaları oluşturabilir veya bunları düzenleyebilirsiniz.

VPN poliçesini SIS dosyasından yüklediyseniz bu seçenek kullanılamaz.

VPN poliçelerini güncelleştirme

VPN erişim noktasıyla bir bağlantı oluşturduğunuzda, VPN poliçe sunucusundan VPN poliçesinin durumu kontrol edilir. Yöneticiler VPN poliçesinin yeni bir sürümünü oluşturmuşsa, mobil cihaza yeni sürüm yüklenir. Yöneticiler VPN poliçesini VPN poliçe sunucusundan silmişse, bu VPN poliçesi mobil cihazdan kaldırılır.

Değişiklikler, VPN erişim noktasıyla oluşturduğunuz sonraki bağlantıda geçerli hale geldiğinden, o andaki VPN bağlantısını etkilemez.

VPN poliçesini ayrıca, [VPN poliçeleri](#) görünümünden de güncelleştirebilirsiniz. VPN poliçesini güncelleştirmek için, VPN poliçesini seçin, [Seçenek](#) tuşuna basıp [Poliçeyi güncelle](#) seçeneğini belirleyin. VPN poliçesinin durumu VPN poliçe sunucusundan kontrol edilir.

VPN poliçelerini silme

Yöneticiler VPN poliçe sunucusundan VPN poliçelerini sildikten sonra bir VPN poliçe sunucusunu senkronize ettiğinizde ilgili VPN poliçeleri otomatik olarak silinir. VPN poliçe sunucusunda hala bulunan bir VPN poliçesini silerseniz, VPN poliçe sunucusundan VPN poliçelerini senkronize ettiğinizde ilgili VPN poliçesi yeniden yüklenir.

VPN poliçesini silmek için VPN poliçesini seçin ve silme tuşuna basın.

Bir VPN erişim noktasının ilişkili olduğu VPN poliçesini silerseniz, o erişim noktasını kullanamazsınız.

↔ Menü'ye gidip
Araçlar→ Ayarlar→
Bağlantı ayarları→ VPN→
VPN yönetimi→ VPN poliçe
sunucuları seçeneğini
belirleyin.

▶ **İpucu!** Yöneticiler
bir VPN poliçe sunucusu
bağlantısı ayarlarını
içeren bir SIS dosyasını
size gönderebilir veya
VPN poliçe sunucusunun
ayarlarını siz
belirleyebilirsiniz.

4. VPN poliçe sunucuları

VPN poliçelerini VPN poliçe sunucularından yükleyebilirsiniz. VPN erişim noktasıyla bir bağlantı kurduğunuzda, VPN erişim noktasıyla ilişkili VPN poliçesi bir VPN poliçe sunucusundan otomatik olarak güncelleştirilir. Tüm VPN poliçelerini güncelleştirmek için VPN poliçe sunucularını mobil cihazla senkronize edin. Daha fazla bilgi için, bkz: "VPN poliçe sunucularını senkronize etme" sayfa 15.

VPN poliçe sunucularına bağlanma

Bir VPN poliçe sunucusundan VPN poliçeleri yüklediğinizde, mobil cihazla VPN poliçe sunucusu arasında güven ilişkisi oluştursunuz. Güven ilişkisini oluşturmak için, sizin VPN poliçe sunucusunun kimliğini doğrulamanız ve VPN poliçe sunucusunun da sizin kimliğinizi doğrulaması gerekir.

VPN poliçe sunucusu kimliğinizi doğruladıktan sonra bir özel anahtar oluşturulur ve ilgili sertifika kaydı yapılır. Kimliğiniz VPN poliçe sunucusunda bu sertifikayla doğrulanır. Özel anahtar ve sertifika, mobil cihazınızdaki bir anahtar saklama alanında saklanır.

Ayarları SIS dosyalarından yükleme

VPN poliçe sunucusunun VPN poliçe sunucusu ayarlarını bir SIS dosyasından yükleyebilirsiniz. Bu ayarlar, diğer yazılımların bir mobil cihaza yüklendiği gibi yüklenir.

Bu ayarlar VPN poliçe sunucusunun adresi ve sunucu sertifikasından oluşur. Sunucu sertifikası mobil cihazın VPN poliçe sunucusuna güvenmesini sağlar ve böylece, kimliğinizi kanıtlamak için yalnızca kullanıcı adını ve şifresini sunmanız yeterli olur.

SIS dosyası VPN poliçe sunucusuna bağlanmak için kullanılan İnternet erişim noktası ayarlarını içermez. İnternet erişim noktasını belirtmek için, VPN poliçe sunucusu ayarlarını düzenleyin. İnternet erişim noktasını VPN poliçe sunucusuna bağlandığınızda da seçebilirsiniz.

Yöneticiler SIS dosyasını imzalamazsa, SIS dosyasını yüklediğinizde bir güvenlik uyarısı görüntülenir. SIS dosyasını VPN poliçe sunucusu yöneticisinin oluşturduğundan ve SIS dosyasının değiştirilmediğinden eminseniz, bu uyarıyı yok sayabilirsiniz.

SIS dosyasından ayarları yüklemeyen veya yükleme başarısız olmadan **VPN** den çıkın.

VPN poliçe sunucularını görüntüleme

VPN poliçe sunucuları görünümü oluşturduğunuz VPN poliçe sunucularını listeler.

(VPN poliçe sunucusu yok) ifadesi görüntüleniyorsa VPN poliçe sunucuları oluşturmanız gerekir. VPN poliçe sunucusu eklemek için, **Seçenek** tuşuna basın ve **Yeni sunucu** seçeneğini belirleyin.

VPN poliçe sunucuları ekleme

VPN poliçe sunucusunun ayarlarını SIS dosyasından yüklemeyerseniz, VPN poliçe sunucusu ayarlarını belirleyin.

VPN poliçe sunucusu adresine ilk kez bağlandığınızda, VPN poliçe sunucusu kimliğini doğrulamanız gerekir. Yöneticilerden bir VPN poliçe sunucusu kimlik kodu alınır. VPN poliçe sunucusu kimlik kodunu kontrol edin ve tamamlayın.

Başarılı kimlik doğrulamasının ardından, VPN poliçe sunucusuna sonraki kimlik doğrulamaları için bir sertifika kaydedilir.

VPN poliçe sunucusu eklemek için

- 1 **Seçenek** tuşuna basın ve **VPN poliçe sunucuları** görünümünde **Yeni sunucu** seçeneğini belirleyin.



Sözlük:

Senkronizasyon VPN poliçe sunucusunda, yeni, güncelleştirilmiş ve kaldırılmış VPN poliçelerin kontrol edilmesi anlamına gelir.



Sözlük:

Poliçe sunucusu kullanıcı ismi ve şifresi VPN poliçe sunucusunun izinsiz erişime karşı korunmasına yardımcı olur.

- 2 VPN poliçe sunucusuna bir isim girmek için *Poliçe sunucusu ismi* seçeneğini belirleyip *Tamam* tuşuna basın.
VPN poliçe sunucuları görünümünde benzersiz olmak koşuluyla, istediğiniz bir poliçe sunucusu ismi seçebilirsiniz.
Bu alanı boş bırakırsanız, bu alanda *Poliçe sunucu. adresi* görünür.
Poliçe sunucusu ismi VPN poliçe sunucusu listesinde ve VPN poliçe sunucusu ayarları iletişim kutusunun başlık çubuğunda görüntülenir.
- 3 *Poliçe sunucu. adresi* seçeneğini belirleyin, VPN poliçelerinin yükleneceği kaynak VPN poliçe sunucusunun ana makine ismini veya IP adresini girin ve *Tamam* tuşuna basın.
Ayrıca, iki nokta üst üste (:) karakteriyle ayrılmış olarak bağlantı noktası numarasını da belirtebilirsiniz.
Poliçe sunucusu adresi yöneticilerden alınır.
- 4 *Internet erişim nokt.* seçeneğini belirleyin, VPN poliçe sunucusunu bir erişim noktasıyla ilişkilendirin ve *Tamam* tuşuna basın.
Erişim noktası bu VPN poliçe sunucusuna bağlanmak için kullanılır.
Seçilecek erişim noktasını yöneticiler size söyleyecektir.
- 5 VPN poliçe sunucusu ayarlarını kaydetmek için *Geri* tuşuna basın.
- 6 VPN poliçe sunucusunu **senkronize** etmeniz istendiğinde *Evet* tuşuna basın.
VPN poliçe sunucusunun kimliğini doğrulamanız istenir.
Yöneticilerden bir VPN poliçe sunucusu kimlik kodu alınır.
- 7 Görüntülenen VPN poliçe sunucusu kimlik kodunu yöneticilerden aldığınız kodla dikkatlice karşılaştırın, alandaki eksik karakterleri girin ve *Tamam* tuşuna basın.
- 8 VPN poliçe sunucusunda kimlik doğrulaması için *Poliçe sunucusu kullanıcıismi:* alanına **kullanıcı isminizi** ve *Poliçe sunucusu şifresi:* alanına **şifrenizi** girin ve sonra *Tamam* tuşuna basın.
Gireceğiniz kullanıcı ismini ve şifrenizi yöneticiler size söyleyecektir.

VPN poliçe sunucusuna sonraki kimlik doğrulamaları için bir sertifika kaydedilir ve VPN poliçeleri mobil cihaza yüklenir.

Artık, VPN erişim noktaları oluşturabilir ve bunları uygulamalarla ilişkilendirebilirsiniz. Daha fazla bilgi için, bkz:“VPN erişim noktası oluşturma” sayfa 17.

VPN poliçe sunucularını düzenleme

VPN poliçe sunucusunun ayarlarını görüntülemek veya değiştirmek için, [VPN poliçe sunucuları](#) görünümünden bir VPN poliçe sunucusu seçin.

Poliçe sunucusuna yeni bir isim vermek için [Poliçe sunucusu ismi](#) seçeneğini belirleyin. [VPN poliçe sunucuları](#) görünümünde yeni isim görüntülenir.

VPN poliçe sunucusu, poliçe sunucusu adresini ilk bağlantı sırasında gönderdiğinden, VPN poliçelerini VPN poliçe sunucusundan yükledikten sonra [Poliçe sunucu. adresi](#)’ni değiştiremezsiniz.

VPN poliçe sunucusuyla ilişkili erişim noktasını sildiyseniz, [İnternet erişim nokt.](#)’nda (seçili değil) metni görüntülenir. Yeni bir erişim noktası seçmek için İnternet erişim noktası seçeneğini belirleyin. Tüm erişim noktalarını sildiyseniz, ayarları kaydedemezsiniz.

VPN poliçe sunucularını senkronize etme

[VPN poliçe sunucuları](#) görünümünden bir VPN poliçe sunucusu seçin, [Seçenek](#) tuşuna basın ve VPN poliçe sunucusundan poliçeleri yüklemek ve güncelleştirmek için [Sunucuyu senk. et](#) seçeneğini belirleyin. VPN poliçe sunucusunda eklenmiş, güncelleştirilmiş veya silinmiş VPN poliçeleri kontrol edilir.

VPN poliçe sunucusunda yeni VPN poliçeleri veya VPN poliçelerinin yeni sürümleri varsa, bu VPN poliçeleri mobil cihaza yüklenir. Yöneticiler VPN poliçe sunucusundan VPN poliçelerini silmişse, bu VPN poliçeleri mobil cihazdan kaldırılır.

VPN poliçe sunucusunu ilk kez senkronize ettiğinizde, mobil cihaza yüklediğiniz her VPN poliçesi için uygun bir VPN erişim noktası oluşturulur. [VPN erişim noktaları](#) görünümünde VPN erişim noktaları oluşturabilir veya bunları düzenleyebilirsiniz.

VPN poliçelerini yüklemek veya güncelleştirmek için VPN poliçe sunucusuna bağlandığınızda, VPN poliçe sunucusundaki VPN sertifikalarının kaydını yapmanız gerekebilir.

VPN sertifikalarının kaydı

Gerekli her sertifika için bir sertifika isteği oluşturulur ve VPN poliçe sunucusuna gönderilir. VPN poliçe sunucusu her istenen sertifikayı bir **sertifika yetkilisinden** (CA) kaydeder.

Sertifika isteği ve ilgili sertifika kullanıcı kimliğinizi içerir. VPN poliçe sunucusu yapılandırmasına göre, VPN poliçe sunucusu kullanıcı kimliği de VPN sertifikalarında kullanıcı kimliği olarak kullanılabilir. Bu mümkün değilse, belirli bir etki alanı için kullanıcı kimliğiniz istenir.

Sertifika isteği oluşturmak için

- 1 Belirtilen etki alanı için sertifika kullanıcı kimliğinizi *'için kullanıcıkimliği:* alanına girin. Girilecek bilgileri yöneticiler size söyleyecektir.
- 2 *Tamam* tuşuna basın.

VPN poliçe sunucularını silme

VPN poliçe sunucusunu silmek için, *VPN poliçe sunucuları* görünümünde bir VPN poliçe sunucusu seçin ve sil tuşuna basın.

VPN poliçe sunucusundan yüklediğiniz VPN poliçelerinin silinmesini onaylayın.

5. VPN erişim noktaları

VPN erişim noktası bir VPN poliçesi ve bir İnternet erişim noktası içeren sanal erişim noktasıdır. VPN bağlantısı oluşturmak için İnternet erişim noktası listesinden bir VPN erişim noktası seçin.

↩ *Menü*'ye gidip
Araçlar→*Ayarlar*→
Bağlantı ayarları→*VPN*→
VPN erişim noktaları
seçeneğini belirleyin.

VPN erişim noktalarını görüntüleme

VPN erişim noktaları görünümü, mobil cihazda oluşturduğunuz VPN erişim noktalarını listeler. (*VPN erişim noktası yok*) metni, VPN erişim noktası oluşturmadığınız anlamına gelir. Yeni bir VPN erişim noktası oluşturmak için, *Seçenek* tuşuna basın ve *Yeni erişim noktası*'nı seçin.

Aşağıdaki bilgileri görüntülemek ve düzenlemek için, bir VPN erişim noktası seçin ve sonra *Seçenek*→*Düzenle*'yi seçin:

- *Bağlantı ismi*—VPN erişim noktasını erişim noktası listesinde tanımlar.
- *VPN poliçesi* —VPN erişim noktasıyla bağlantılı VPN poliçesinin ismi.
- *İnternet erişim noktası*—üzerinden VPN bağlantısının oluşturulduğu erişim noktasının ismi.
- *Yakın kopya. sun. adr.*—kuruluş ağındaki yakın kopya sunucusunun adresi.
- *Yakın kopya port no.*—yakın kopya sunucusunda bağlanılacak port numarası.

VPN erişim noktası oluşturma

VPN erişim noktaları görünümünü ilk kez açtığınızda, VPN erişim noktaları oluşturmanız istenir. *İstedi* tuşuna basın.

 **İpucu!** VPN erişim noktası ayarlarında yakın kopya sunucusu belirtirseniz, yakın kopya sunucusunu İnternet tarayıcısı ayarlarında belirtmeniz gerekmez.

VPN erişim noktası oluşturmak için

- 1 [Seçenek](#) tuşuna basın ve [Yeni erişim noktası](#)'nı seçin.
- 2 Bağlantının ismini değiştirmek için [Bağlantı ismi](#)'ni seçin. İstedığınız bir bağlantı ismi seçebilirsiniz.
- 3 Bağlantının şifreleme yöntemini tanımlamak için [VPN poliçesi](#)'ni seçin. Liste boşsa, VPN poliçelerini SIS dosyalarından veya VPN poliçe sunucularından yüklemeniz gerekir.
- 4 VPN bağlantısında kullanılacak erişim noktasını seçmek için [İnternet erişim nokt.](#)'nı seçin. Liste boşsa, erişim noktaları oluşturmanız gerekir.
- 5 Kuruluş ağındaki yakın kopya sunucusunun adresini girmek için [Yakın kopya. sun. adr.](#)'ni seçin.
- 6 Varsayılan port numarasını (80) değiştirmek için [Yakın kopya port no.](#)'yu seçin.

VPN erişim noktalarını silme

VPN erişim noktasını silmek için, [VPN erişim noktaları](#) görünümünde bir VPN erişim noktası seçin ve sil tuşuna basın.

6. VPN işlem kaydı

VPN işlem kaydı VPN poliçelerini güncelleştirdiğinizde ve senkronize ettiğinizde ve VPN ağ geçitlerine VPN bağlantıları oluşturduğunuzda kaydedilen işlem kaydı mesajlarını içerir.

VPN işlem kaydını görüntüleme

VPN işlem kaydı görünümü VPN İstemcisinin sürüm numarasını görüntüler.

Mesaj türünü, mesaj saatini ve işlem kaydı mesajının başlangıcını görüntüleyebilirsiniz. İşlem kaydının tümünü görüntülemek için ilgili işlem kaydı mesajını seçin.

VPN işlem kaydı görünümü, en son mesaj ilk görüntülenecek şekilde işlem kaydı mesajlarını saat ve tarihe göre sıralar. Mesajları *VPN işlem kaydı* görünümünü açtığınız ana kadar görüntüleyebilirsiniz. En son mesajları görüntülemek için, *Seçenek* tuşuna basın ve *İşlem kaydını yenile*'yi seçin.

İşlem kaydı mesajları hata, durum ve neden kodlarını içerebilir. Yöneticilere hata bildirirken işlem kaydı mesajlarındaki kodları da bildirin.

VPN işlem kaydını silme

İşlem kaydı mesajları döngüsel arabelleğe kaydedilir. İşlem kaydı boyutu 20 kilobayt olduğunda, yeni işlem kaydı mesajları en eski işlem kaydı mesajlarının üzerine yazılır.

İşlem kaydındaki tüm işlem kaydı mesajlarını silmek ve *VPN işlem kaydı* görünümünü temizlemek için, *Seçenek* tuşuna basın ve *İşlem kaydını sil*'i seçin.

↩ *Menü*'ye gidip *Araçlar*→*Ayarlar*→*Bağlantı ayarları*→*VPN*→*VPN yönetimi*→*VPN işlem kaydı* seçeneğini belirleyin.

Simgeler: hatalar için , uyarı için  ve açıklama için .

7. Anahtar saklama şifreleri

↔ Menü'ye gidip
Araçlar→ Ayarlar→
Bağlantı ayarları→ VPN→
VPN yönetimi→ Anahtar
sakl. şifresi seçeneğini
belirleyin.

▶ **İpucu!** Anahtar saklama şifresi hem harf hem de rakam içerebilir ve en az altı karakter uzunluğunda olması gerekir.

Anahtar saklama şifresi mobil cihazdaki özel anahtarların ve VPN poliçe sunucusu bağlantılarının izinsiz kullanıma karşı korunmasına yardımcı olur.

Anahtar saklama şifresi oluşturma veya değiştirme

Anahtar saklama şifresini ilk VPN poliçesini yüklediğinizde oluşturursunuz. Saldırganlar anahtar saklama şifresini tahmin eder veya kırarsa, VPN'nin korunmasına yardımcı olduğu kuruluş ağına erişmek için mobil cihazı kullanabilirler. Bu nedenle, anahtar saklama şifrelerini kırılması güç olacak kadar uzun oluşturmanız gerekir. Şifrenizi gizli tuttuğunuzdan emin olun. Şifrelerinizi bir kağıda yazmayın.

Anahtar saklama şifresi oluşturmak veya değiştirmek için:

- 1 **Yeni anahtar saklama şifresi:** altından, sizin için anımsanması kolay ancak başkalarının tahmin etmesi güç bir şifre girin.
- 2 **Şifreyi doğrulayın!** ı seçin ve yazım hatalarını önlemek için şifreyi yeniden girin.
- 3 Şifreyi oluşturmak için **Tamam**'a basın.

Anahtar saklama şifrelerini girme

Aşağıdaki durumlarda anahtar saklama şifresini girmeniz istenir:

- VPN poliçe sunucularından yeni veya güncelleştirilmiş VPN poliçeleri yüklediğinizde.

- Sertifika doğrulaması gerektiren VPN erişim noktalarına bağlanan uygulamalar kullandığınızda.



Not: Şifreler girilirken, akıllı metin girişi kapalıdır. Karakterleri birer birer girin. Karakterler varsayılan olarak küçük harf olarak yazılır.

8. VPN ve uygulamalar

VPN bağlantısı oluşturan bir uygulama kullandığınızda, VPN istemcisi aşağıdaki görevleri gerçekleştirir:

- VPN erişim noktasıyla ilişkili İnternet erişim noktasına bağlanır.
- VPN erişim noktasıyla ilişkili VPN poliçesini yükler.
- VPN bağlantısı oluşturmak için VPN ağ geçidine bağlanır.

VPN ağ geçitlerinde kimlik doğrulaması gerçekleştirme

Kuruluş ağına oturum açtığınızda kimliğinizi ispat etmeniz gerekir. VPN poliçesi kullanacağınız kimlik doğrulaması yöntemini belirler:

- Sertifika tabanlı kimlik doğrulaması—Güvenilen sertifika yetkilisinin imzaladığı bir sertifikanızın olması gerekir. Sertifikayı edinmek için çevrimiçi sertifika kaydını kullanabilir veya sertifikaları bir SIS dosyasından VPN poliçesini yüklediğinizde yükleyebilirsiniz.
- Eski kimlik doğrulama—Kimlik doğrulaması için kullanıcı adlarını ve şifreleri veya parolaları kullanırsınız. Kullanıcı adlarını veya şifreleri yöneticiler oluşturur ya da yöneticiler parola oluşturmanız için size SecurID belirteçleri verir.

Kimlik doğrulaması için sertifika kullanıyorsanız, anahtar saklama şifresini girin.

Eski kimlik doğrulama yöntemini kullanıyorsanız, VPN erişim noktalarına bağlanan uygulamaları kullanırken ve mobil cihaz VPN ağ geçidiyle şifreli bağlantılar oluştururken VPN kimlik doğrulama bilgilerini girin.

VPN ağ geçidinde kimlik doğrulaması gerçekleştirmek için

- 1 **VPN kullanıcı ismi:** alanına VPN kullanıcı isminizi girin.
- 2 VPN şifrenizi veya parolanızı girin:
 - Şifrenizi **VPN şifresi:** alanına girin.

- SecurID parolası oluşturun, parolayı *VPN parolası* : alanına girin ve *Tamam* tuşuna basın.
- 3 SecurID belirtecinin ACE/Sunucu saatiyle senkronizasyonu bozulursa, ACE/Sunucu tarafından belirtecin saat temeli için yeni bir referans olarak kullanılan sonraki parolayı girmeniz istenir. Yeni parolayı oluşturun ve *Sonraki parola*: alanına girin. Bu başarısız olursa, yöneticiye başvurun.
 - 4 *Tamam* tuşuna basın.

9. Sorun giderme

Aşağıdaki tabloda hata mesajları alfabetik olarak sıralanmış, hataların olası nedenleri açıklanmış ve bu hataların düzeltilmesi için gerçekleştirilebilecek işlemler önerilmiştir.

Mesaj	Neden	İşlem
<i>Doğrulanamadı. Kullanıcı ismini ve şifreyi kontrol edin.</i>	- VPN poliçe sunucusunda doğrulama yapılırken veya bir VPN'de oturum açarken hatalı kullanıcı adı veya şifre girdiniz. - Sonraki parola istendiğinde hatalı parola girdiniz.	- Kullanıcı adınızı ve şifreyi kontrol edin ve yeniden deneyin. - SecurID belirteç görünümündeki parola değişene kadar bekleyin ve parolayı girin.
<i>Yanlış parola</i>	Yanlış anahtar saklama şifresi veya anahtar alma şifresi girdiniz.	- Şifreyi kontrol edin ve yeniden deneyin. - Anahtar alma şifresini yöneticilerden alın. Anahtar saklama şifresini kendiniz oluşturun.

Mesaj	Neden	İşlem
<i>Yanlış sunucu kimlik kodu</i>	VPN poliçe sunucusu kimlik kodunu girmeniz istendiğinde yanlış bir dize girdiniz.	VPN poliçe sunucusu kimlik kodunu yöneticilerden aldığınız kodla dikkatlice karşılaştırın ve eksik karakterleri yeniden girin.
<i>Poliçe sunucusu şu anda kullanılıyor. Silinemez.</i>	Sunucudan VPN poliçelerini güncellerken, VPN poliçe sunucusunu silemezsiniz. VPN bağlantısı oluşturan bir uygulama kullandığınızda, VPN poliçeleri otomatik olarak güncelleştirilir.	VPN poliçeleri güncelleştirilene kadar bekleyin ve yeniden deneyin.

Mesaj	Neden	İşlem
<i>VPN poliçesi etkinleştirilemiyor. Önce VPN poliçesini güncelleyin.</i>	- Eski doğrulanama başarısız oldu. - VPN ağ geçidinde doğrulama yapmak için kullandığınız sertifika eksik, süresi dolmuş veya geçerlilik süresi henüz başlamamış.	- Kullanıcı adınızı ve şifreyi kontrol edin ve yeniden deneyin. <i>VPN poliçeleri</i> görünümünde bir VPN poliçesi seçin, <i>Seçenek</i> tuşuna basın ve VPN poliçesini güncelleştirmek için <i>Poliçeyi güncelle</i> seçeneğini belirleyin. - Mobil cihazdaki tarih ve saat ayarlarını kontrol edin.

Mesaj	Neden	İşlem
<i>Polİçe sunucusuna giriş yapılamıyor. Sunucuyu silin ve bilgileri yeniden tanımlayın.</i>	VPN poliçe sunucusunun sunucu sertifikasının süresi dolmuş.	<i>VPN poliçe sunucuları</i> görünümünde: - VPN poliçe sunucusunu silmek için <i>Seçenek</i> tuşuna basın ve <i>Sunucuyu sil</i> seçeneğini belirleyin. - VPN poliçe sunucusunu yeniden eklemek için <i>Seçenek</i> tuşuna basın ve <i>Yeni sunucu</i>'yu seçin veya yöneticinizden VPN poliçe sunucusunun yeni ayarlarını içeren SIS dosyasını isteyin.
<i>Polİçe sunucusuna giriş yapılamıyor. Polİçe sunucusu kullanıcı ismini ve şifresini girin.</i>	VPN poliçe sunucusunda kimliğinizi doğrulayan sertifikanın süresi dolmuş veya yönetici sertifikayı iptal etmiş.	- Bu durumu yöneticiye bildirin. Size bir kullanımlık bir şifre vereceklerdir. - VPN poliçe sunucusunda kimlik doğrulaması gerçekleştirmek için kullanıcı adını ve bir kullanımlık şifreyi girin. - Sizin için yeni bir sertifika oluşturulur.

Mesaj	Neden	İşlem
<i>Poliçe sunucusuna giriş yapılamıyor. Bilgiler için VPN işlem kaydına bakın.</i>	VPN poliçe sunucusunda kimliğinizi doğrulayan sertifikanın geçerlilik süresi henüz başlamamış.	Tarih ve saat ayarlarını kontrol edin veya sertifikanın geçerlilik süresi başlayana kadar bekleyin.
<i>Poliçe güncellenemiyor. Bilgiler için VPN işlem kaydına bakın.</i> <i>Senkronize edilemiyor. Bilgiler için VPN işlem kaydına bakın.</i>	VPN poliçe sunucusundan VPN poliçeleri indirilirken veya mobil cihaza yüklenirken bir hata oluştu.	<i>VPN poliçeleri</i> görünümünde bir VPN poliçesi seçin, <i>Seçenek</i> tuşuna basın ve VPN poliçesini güncellemek için <i>Poliçeyi güncelle</i>'yi seçin. <i>VPN poliçe sunucuları</i> görünümünden bir VPN poliçe sunucusu seçin, <i>Seçenek</i> tuşuna basın ve VPN poliçe sunucusundan poliçeleri yüklemek için <i>Sunucuyu senk. et</i>'i seçin.
<i>VPN poliçesi silindi. VPN erişim noktası ayarlarını kontrol edin.</i>	VPN poliçesi eski olduğundan VPN erişim noktasıyla bağlantılı VPN poliçesi silindi.	<i>VPN erişim noktaları</i> görünümünden bir VPN erişim noktası seçin, <i>Seçenek</i> tuşuna basın ve VPN erişim noktasıyla başka bir VPN poliçesini ilişkilendirmek için <i>Düzenle</i> 'yi seçin.

Dizin

A

Açıklama alanı 9

alanlar

Açıklama 9

Bağlantı ismi 17

Güncelleme 9

İnternet erişim nokt. 14, 17

Polİçe durumu 9

Polİçe ismi 9

Polİçe sunucu. adresi 14

Polİçe sunucusu 9

Polİçe sunucusu ismi 14

Polİçe sunucusu kullanıcı ismi 14

Polİçe sunucusu şifresi 14

Sertifika durumu 9, 10

Sonraki parola 23

VPN kullanıcı ismi 22

VPN parolası 23

VPN poliçesi 17

VPN şifresi 22

Yakın kopy. sun. adr. 17

Yakın kopya port no. 17

Yeni anahtar saklama şifresi 20

anahtar saklama şifreleri

hakkında 20

B

Bağlantı ismi alanı 17

D

Doğrulanamadı. Kullanıcı adını ve şifreyi

kontrol edin. 24

Düzenle seçeneği 17

E

eski kimlik doğrulama 22

G

Güncelleme alanı 9

güvenlik uyarıları 13

H

hata mesajları 24

henüz geçerli olmayan sertifikalar 10

I

İnternet erişim nokt. alanı 14, 17

İ

İşlem kaydını sil seçeneği 19

İşlem kaydını yenile seçeneği 19

P

Polİçe durumu alanı 9

Polİçe güncellenemiyor. Bilgiler için

VPN işlem kaydına bakın. 28

Polİçe ismi alanı 9

Polİçe sunucu. adresi alanı 14

Polİçe sunucusu alanı 9

Polİçe sunucusu ismi alanı 14

Polİçe sunucusu kullanıcı ismi alanı 14

Polİçe sunucusu şifresi alanı 14

Polİçe sunucusu şu anda kullanılıyor.

Silinemez. 25

Polİçe sunucusuna giriş yapılamıyor.

Bilgiler için VPN işlem kaydına

bakın. 28

Polİçe sunucusuna giriş yapılamıyor.

Polİçe sunucusu kullanıcı

ismini ve şifresini girin. 27

Polİçe sunucusuna giriş yapılamıyor.

Sunucuyu silin ve bilgileri

yeniden tanımlayın. 27

S

SecurID parolası 23

Senkronize edilemiyor. Bilgiler için VPN

işlem kaydına bakın. 28

Sertifika durumu alanı 9, 10

sertifika tabanlı kimlik doğrulama 22

sertifika yok 10

sertifikalar

kayıt 16

kullanıcı kimliği 16

VPN poliçe sunucularında kimlik

doğrulama 12

sistem gereksinimleri 6

Sonraki parola alanı 23

Sunucuyu senk. et seçeneği 15
süresi dolmuş sertifikalar 10

T

Tamam 10

V

VPN

kimlik doğrulaması
gerçekleştirme 22
kullanma 4
uygulamalarla kullanma 22

VPN erişim noktaları

düzenleme 17
görüntüleme 17
hakkında 17
oluşturma 17
silme 18

VPN erişim noktası yok 17

VPN işlem kaydı

görüntüleme 19
silme 19
yenileme 19

VPN kullanıcı ismi alanı 22

VPN parolası alanı 23

VPN poliçe sunucuları

ayarları SIS dosyalarından
yükleme 12
bağlanma 12
ekleme 13
görüntüleme 13
senkronize etme 15

VPN poliçe sunucusu yok 13

VPN poliçeleri

görüntüleme 9
güncelleştirme 11
silme 11
yükleme 7

VPN poliçelerini silme 11

VPN poliçesi alanı 17

VPN poliçesi etkinleştirilemiyor. Önce
VPN poliçesini güncelleyin. 26

VPN poliçesi silindi. VPN erişim noktası
ayarlarını kontrol edin. 28

VPN poliçesi yok 9

VPN şifresi alanı 22

Y

Yakın kopy. sun. adr. alanı 17

Yakın kopya port no. alanı 17

Yanlış sunucu kimlik kodu. 25

Yanlış şifre. 24

Yeni anahtar saklama şifresi alanı 20

Yeni erişim noktası seçeneği 17, 18

Yeni sunucu seçeneği 13

yükleme

SIS dosyalarından VPN poliçe
sunucusu ayarları 12

VPN istemcisi 6

VPN poliçeleri 7, 15