EPSON
EXCEED YOUR VISION

Yönetici Kılavuzu

NPD5668-00 TR

İçindekiler

Ek

Kuruluş için Gelişmiş Güvenlik Ayarları

Telif Hakkı

Bu kılavuzun içeriği ve bu ürünün teknik özellikleri önceden haber verilmeksizin değiştirilebilir.

Ticari Markalar

- ❏ EPSON®, Seiko Epson Corporation'ın tescilli ticari markası, EPSON EXCEED YOUR VISION veya EXCEED YOUR VISION ise Seiko Epson Corporation'ın ticari markalarıdır.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Genel Bildirim: Bu belgede geçen diğer ürün adları sadece tanımlama amaçlıdır ve bu ürünlerle ilgili ticari marka hakları ilgili sahiplerine aittir. Epson bu markalarla ilgili olarak hiçbir hak talep etmemektedir.

Bu Kılavuz Hakkında

Işaretler ve Semboller

> ***Dikkat:***
> *Fiziksel yaralanmalardan kaçınmak için dikkatle uyulması gereken talimatlar.*

> ***Önemli:***
> *Donanımınıza zarar gelmesinden kaçınmak için göz önünde bulundurulması gereken talimatlar.*

Not:
Tarayıcıya yönelik faydalı ipuçları ve yönlendirmeler içeren talimatlar.

İlgili Bilgi

➡ Bu simgeye tıklayarak ilgili bilgilere ulaşabilirsiniz.

Bu Kılavuzda Kullanılan Açıklamalar

❏ Tarayıcı sürücüsü ekran görüntüleri ve Epson Scan 2 (tarayıcı sürücüsü) ekranları, Windows 10 veya OS X El Capitan'den alınmıştır. Ekranlarda görüntülenen içerik, model ve duruma göre değişir.

❏ Bu kılavuzda kullanılan çizimler sadece örnek teşkil etmektedir. Kullanılan modele bağlı olarak küçük farklılıklar gözlemlenmesine rağmen çalışma yöntemi aynıdır.

❏ LCD ekranında görüntülenen bazı menü öğeleri modele ve ayarlara göre farklılık gösterir.

İşletim Sistemi Referansları

Windows

Bu kılavuzda, “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Vista”, “Windows XP”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012”, “Windows Server 2008 R2”, “Windows Server 2008”, “Windows Server 2003 R2” ve “Windows Server 2003” gibi terimler ile aşağıdaki işletim sistemleri kastedilmektedir. Ayrıca “Windows” ile tüm sürümler ifade edilmektedir.

❏ Microsoft® Windows® 10 işletim sistemi

❏ Microsoft® Windows® 8.1 işletim sistemi

❏ Microsoft® Windows® 8 işletim sistemi

❏ Microsoft® Windows® 7 işletim sistemi

❏ Microsoft® Windows Vista® işletim sistemi

❏ Microsoft® Windows® XP işletim sistemi

❏ Microsoft® Windows® XP Professional x64 Edition işletim sistemi

- ❏ Microsoft® Windows Server® 2016 işletim sistemi
- ❏ Microsoft® Windows Server® 2012 R2 işletim sistemi
- ❏ Microsoft® Windows Server® 2012 işletim sistemi
- ❏ Microsoft® Windows Server® 2008 R2 işletim sistemi
- ❏ Microsoft® Windows Server® 2008 işletim sistemi
- ❏ Microsoft® Windows Server® 2003 R2 işletim sistemi
- ❏ Microsoft® Windows Server® 2003 işletim sistemi

Mac OS

Bu kılavuzda, "Mac OS" ile macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x ve Mac OS X v10.6.8 ifade edilmektedir.

Giriş

Kılavuz Bileşeni

Bu kılavuz yazıcıyı veya tarayıcıyı ağa bağlamakla görevli aygıt yöneticisi içindir ve işlevleri kullanmak için ayarların nasıl yapılacağını gösteren bilgileri içerir.

İşlev kullanım bilgileri için bkz. *Kullanım Kılavuzu*.

Hazırlık

Yöneticinin görevlerini, aygıtların nasıl ayarlanacağını ve yönetim için yazılımı açıklar.

Bağlantı

Bir aygıtın ağa veya telefon hattına nasıl bağlanacağını açıklar. Ayrıca, aygıt için bağlantı noktası kullanma, DNS ve proxy sunucusu bilgileri gibi ağ ortamını da açıklar.

İşlev Ayarları

Aygıtın her işlevi için ayarları açıklar.

Temel Güvenlik Ayarları

Yazdırma, tarama ve faks gibi her işlevin ayarların açıklar.

Çalıştırma ve Yönetim Ayarları

Aygıtların kullanımına başladıktan sonraki bilgi kontrolü ve bakım gibi işlemleri açıklar.

Sorunları Çözme

Ayarları ilkleme ve ağ sorununu gidermeyi açıklar.

Kuruluş için Gelişmiş Güvenlik Ayarları

CA sertifikası, SSL/TLS iletişimi ve IPsec/IP Filtreleme gibi aygıtın güvenliğini iyileştirmek için ayarlar yöntemini açıklar.

Modele bağlı olarak bu bölümdeki bazı işlevler desteklenmez.

Bu Kılavuzda Kullanılan Terimlerin Açıklamaları

Aşağıdaki terimler bu kılavuzda kullanılmaktadır.

Yönetici

Bir ofis veya kuruluşta aygıtı kurma ve ayarlamayla görevli kişi. Küçük kuruluşlar için bu kişi hem aygıt hem de ağ yöneticisi görevini görür. Büyük kuruluşlar için yöneticilerin bir departman veya bölümün grup biriminde ağ veya aygıtlar üzerinde yetkileri vardır ve ağ yöneticileri kuruluşun ötesinde de iletişim ayarlarından (örneğin Internet) sorumludur.

Ağ yöneticisi

Ağ iletişimini kontrolde görevli kişi. Internet veya ağ üzerinden iletişimi kontrol etmek için yönlendirici, proxy sunucusu, DNS sunucusu ve posta sunucusunu ayarlayan kişi.

Kullanıcı

Yazıcılar veya tarayıcılar gibi aygıtları kullanan kişi.

Web Config (aygıtın web sayfası)

Aygıtta yerleşik web sunucusu. Web Config olarak adlandırılır. Tarayıcıyı kullanarak aygıtın durumunu kontrol edebilir ve değiştirebilirsiniz.

Araç

Epson Device Admin, EpsonNet Config, EpsonNet SetupManager vb. gibi bir aygıtı kurmak veya yönetmek için yazılım için genel bir terim.

İtme tarama

Aygıtın kontrol panelinden tarama için genel bir terim.

ASCII (Bilgi Değiş Tokuşu İçin Amerikan Standart Kodu)

Standart karakter kodlarından biri. Alfabe (a–z, A–Z), Arap numaraları (0–9), semboller, boş karakterler ve kontrol karakterleri dahil 128 karakter tanımlanır. Bu kılavuzda "ASCII" tanımlandığında, aşağıda listelenen 0x20–0x7E'yi (onaltılı sayı) gösterir ve kontrol karakterlerini içermez.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Boşluk karakteri.

Unicode (UTF-8)

Büyük genel dilleri kapsayan uluslararası bir standart kod. Bu kılavuzda "UTF-8" açıklandığında, UTF-8 biçiminde kodlama karakterlerini gösterir.

Hazırlık

Bu bölümde yönetici rolünü ve ayarları yapmadan önce hazırlamayı açıklar.

Tarayıcı Ayarları ve Yönetimi Akışı

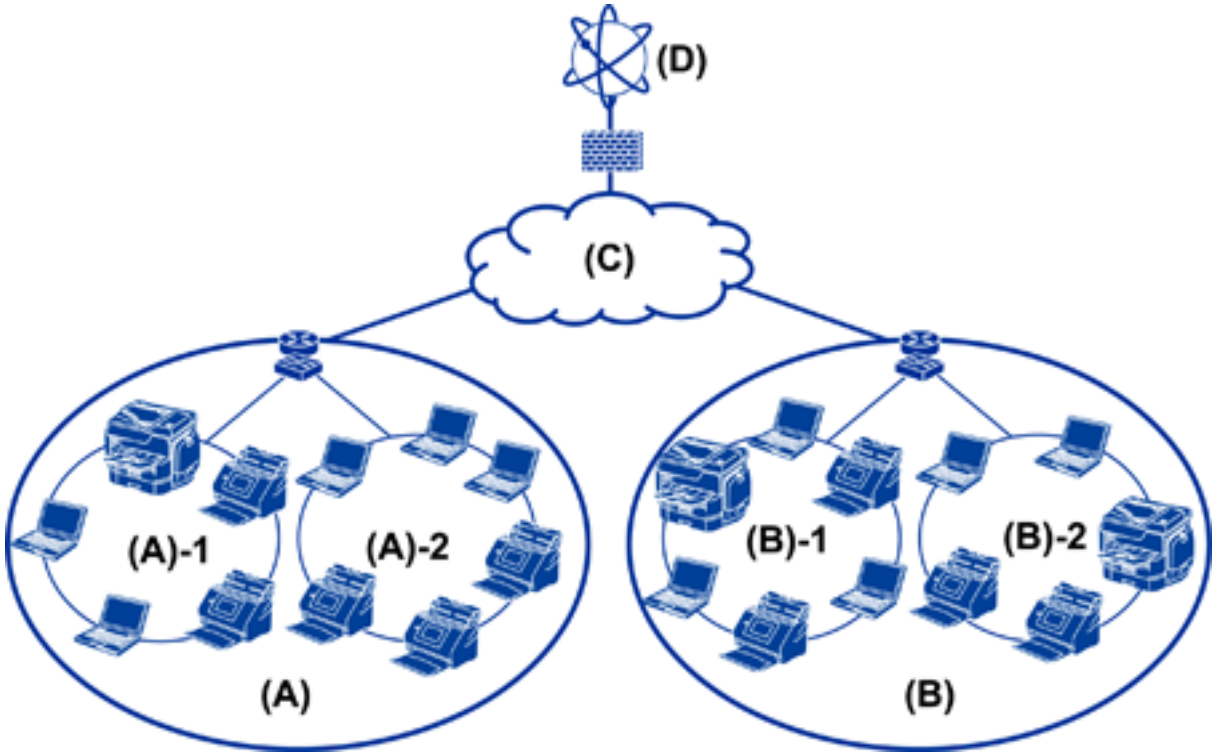
Yönetici tarayıcının ağ bağlantısı ayarlarını, ilk kurulumu ve bakımını yapar, böylece bunlar kullanıcılar tarafından kullanılabilir.

1. Hazırlama
   - ❏ Bağlantı ayarı bilgilerini toplama
   - ❏ Bağlantı yönteminde karar verme
2. Bağlanma
   - ❏ Tarayıcının kontrol panelinden ağ bağlantısı
3. İşlevleri ayarlama
   - ❏ Tarayıcı sürücüsü ayarları
   - ❏ Diğer gelişmiş ayarlar
4. Güvenlik ayarları
   - ❏ Yönetici ayarları
   - ❏ SSL/TLS
   - ❏ Protokol kontrolü
   - ❏ Gelişmiş güvenlik ayarları (Seçenek)
5. Çalıştırma ve yönetme
   - ❏ Aygıt durumunu kontrol etme
   - ❏ Olayların oluşmasını işleme
   - ❏ Aygıt ayarlarını yedekleme

İlgili Bilgi

➡ “Hazırlık” sayfa 10
➡ “Bağlantı” sayfa 15
➡ “İşlev Ayarları” sayfa 22
➡ “Temel Güvenlik Ayarları” sayfa 32
➡ “Çalıştırma ve Yönetim Ayarları” sayfa 40

Ağ Ortamı Örneği



(A): Ofis 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Ofis 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Tarayıcı bağlantısı ayarına giriş örneği

Tarayıcıyı nasıl kullandığınıza bağlı olarak temel olarak iki bağlantı türü bulunur. Her ikisi de hub yoluyla tarayıcıyı bilgisayarla ağa bağlar.

❏ Sunucu / istemci bağlantısı (Windows sunucusunu, iş yönetimini kullanan tarayıcı)

❏ Uçtan uca bağlantı (istemci bilgisayarla doğrudan bağlantı)

İlgili Bilgi

➡ “Sunucu / İstemci Bağlantısı” sayfa 12

➡ “Uçtan Uca Bağlantı” sayfa 12

Sunucu / İstemci Bağlantısı

Sunucunuzda Document Capture Pro Server yüklü olarak tarayıcı ve iş yönetimini merkezileştirin. Belirli bir biçimde çok sayıda belgeyi taramak için birden fazla tarayıcı kullanan en fazla iş için uygundur.

İlgili Bilgi

➡ "Bu Kılavuzda Kullanılan Terimlerin Açıklamaları" sayfa 8

Uçtan Uca Bağlantı

İstemci bilgisayarında yüklü Epson Scan 2 gibi bir tarayıcı sürücüsüyle tek bir tarayıcı kullanın. İstemci bilgisayara Document Capture Pro (Document Capture) yükleme, tarayıcının tek tek istemci bilgisayarlarda işleri çalıştırmanıza izin verir.

İlgili Bilgi

➡ "Bu Kılavuzda Kullanılan Terimlerin Açıklamaları" sayfa 8

Ağa Bağlantıyı Hazırlama

Bağlantı Ayarlarında Bilgi Toplama

Ağ bağlantısı için bir IP adresi, ağ geçidi adresi vb.'niz olması gerekir. Aşağıdakileri önceden kontrol edin.

Bölümler	Öğeler	Not
Aygıt bağlantı yöntemi	❏ Ethernet	Ethernet bağlantısı için bir kategori 5e veya üstü STP (Korumalı Çift Bükümlü) kablo kullanın.
LAN bağlantısı bilgileri	❏ IP adresi ❏ Alt ağ maskesi ❏ Varsayılan ağ geçidi	Yönlendiricinin DHCP işlevini kullanarak otomatik olarak IP adresini ayarlarsanız bu gerekmez.
DNS sunucusu bilgileri	❏ Birincil DNS için IP adresi ❏ İkincil DNS için IP adresi	Statik bir IP adresini IP adresi olarak kullanıyorsanız, DNS sunucusunu yapılandırın. DHCP işlevini kullanarak otomatik olarak atarken ve DNS sunucusu otomatik atanamadığında yapılandırın.
Proxy sunucusu bilgileri	❏ Proxy sunucusu adı ❏ Bağlantı noktası numarası	Internet bağlantısı için bir proxy sunucusu kullanırken ve Epson Connect hizmetini veya bellenimin otomatik güncelleme işlevini kullanırken yapılandırın.

Tarayıcı Özellikleri

Tarayıcının desteklediği standart veya bağlantı modu özelliği, bkz. *Kullanım Kılavuzu*.

Bağlantı Noktasını Kullanma

Tarayıcının kullandığı bağlantı noktası numarası için “Ek”e bakın.

İlgili Bilgi

➡ “Tarayıcı İçin Bağlantı Noktasını Kullanma” sayfa 60

IP Adresi Ataması Türü

Bir IP adresini tarayıcıya atamanın iki türü vardır.

Statik IP adresi:

Önceden belirlenen benzersiz IP adresini tarayıcıya atayın.

Tarayıcıyı veya yönlendiriciyi kapatsanız bile IP adresi değişmez, bu yüzden aygıtı IP adresi ile yönetebilirsiniz.

Bu tür, büyük ofis veya okul gibi birçok tarayıcının yönetildiği bir ağ için uygundur.

DHCP işleviyle otomatik atama:

DHCP işlevini destekleyen tarayıcı ve yönlendirici arasındaki iletişim başarılı olduğunda doğru IP adresi otomatik atanır.

Belirli bir aygıtın IP adresini değiştirmeniz uygun değilse IP adresini önceden koruyun ve sonra ona atayın.

DNS Sunucusu ve Proxy Sunucusu

Bir Internet bağlantısı hizmeti kullanıyorsanız, DNS sunucusunu yapılandırın. Yapılandırmazsanız, ad çözünürlüğünde başarısız olabileceğinizden erişmek için IP adresini belirtmeniz gerekir.

Proxy sunucusu ağ ve Internet arasındaki ağ geçidine yerleştirilir ve bunlardan her biri yerine bilgisayar, tarayıcı ve Internet (karşı sunucu) ile iletişim kurar. Karşı sunucu yalnızca proxy sunucusuyla iletişim kurar. Bu yüzden, IP adresi ve bağlantı noktası numarası gibi tarayıcı bilgileri okunamaz ve güvenliğin artması beklenir.

Proxy sunucusu iletişimin içeriğini kontrol edebildiğinden filtreleme işlevini kullanarak belirli URL'ye erişimi engelleyebilirsiniz.

Ağ Bağlantısını Ayarlama Yöntemi

Şu şekilde ilerleyen tarayıcının IP adresi, alt ağ maskesi ve varsayılan ağ geçidi için bağlantı ayarları içindir.

Kontrol Panelini Kullanma:

Her tarayıcı için tarayıcının kontrol panelini kullanarak ayarları yapılandırın. Tarayıcının bağlantı ayarlarını yapılandırdıktan sonra ağa bağlayın.

Yükleyiciyi kullanma:

Yükleyici kullanılırsa tarayıcının ağı ve istemci bilgisayar otomatik ayarlanır. Ağ hakkında derin bilginiz olmasa bile ayar aşağıdaki yükleyici talimatlarıyla kullanılabilir.

Araç kullanma:

Yöneticinin bilgisayarından bir araç kullanın. Bir tarayıcıyı bulabilir ve sonra tarayıcı ayarlayabilirsiniz veya tarayıcıda toplu ayarlar yapmak için bir SYLK dosyası oluşturabilirsiniz. Birçok tarayıcı ayarlayabilirsiniz, ancak ayarlamadan önce Ethernet kablosuyla fiziki olarak bağlanmaları gerekir. Bu yüzden, ayar için bir Ethernet oluşturabilmek için bu önerilir.

İlgili Bilgi

➡ “Kontrol Panelinden Ağa Bağlanma” sayfa 15

➡ “Yükleyiciyi Kullanarak Ağa Bağlanma” sayfa 19

➡ “EpsonNet Config'i Kullanarak Bir IP Adresi Atama” sayfa 56

Bağlantı

Bu bölümde tarayıcıyı ağa bağlamak için ortam veya prosedür açıklanmaktadır.

Ağa Bağlama

Kontrol Panelinden Ağa Bağlanma

Tarayıcının kontrol panelini kullanarak tarayıcıyı ağa bağlayın.

Tarayıcının kontrol paneli için daha fazla ayrıntı için *Kullanım Kılavuzu* belgesine bakın.

IP Adresi Atama

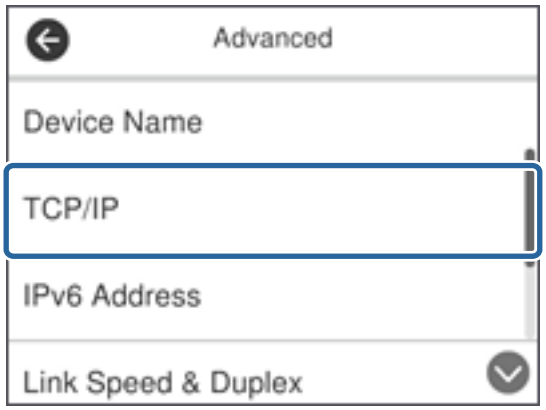
IP Adresi,Alt Ağ Maskesi ve Varsayılan Ağ Geçidi gibi temel öğeleri ayarlayın.

1. Tarayıcıyı açın.
2. Tarayıcının kontrol panelinde ekranda sola hızlı kaydırın ve sonra **Ayarlar** öğesine dokunun.

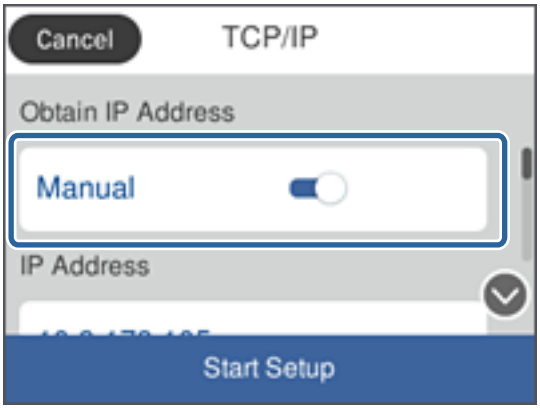
3. **Ağ Ayarları** > **Ayarları Değiştir** öğesine dokunun.

   Öğe görüntülenmezse görüntülemek için ekranı yukarı doğru hızlıca kaydırın.

4. **TCP/IP** öğesine dokunun.

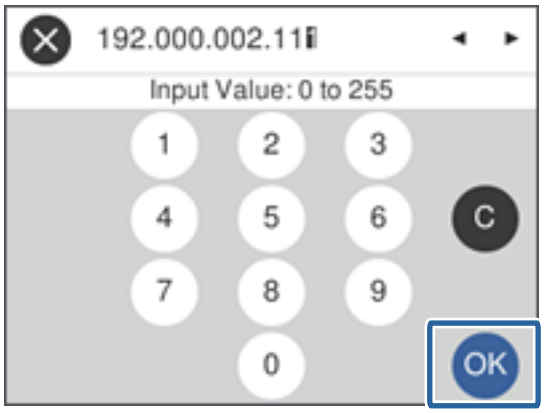


5. **Manuel** için **IP Adresi Alın** seçimini yapın.



Not:
yönlendiricinin DHCP işlevini kullanarak IP adresini otomatik ayarladığınızda, ***Otomatik*** *öğesini seçin. Bu durumda, adım 6 ile 7'daki* ***IP Adresi****,* ***Alt Ağ Maskesi*** *ve* ***Varsayılan Ağ Geçidi*** *öğesi de otomatik ayarlanır, bu yüzden adım 8'a gidin.*

6. **IP Adresi** alanına dokunun, ekranda görüntülenen klavyeyi kullanarak IP adresini girin ve sonra **Tamam** öğesine dokunun.



Önceki ekranda yansıtılan değeri onaylayın.

7. **Alt Ağ Maskesi** ve **Varsayılan Ağ Geçidi** ayarlarını yapın.

   Önceki ekranda yansıtılan değeri onaylayın.

   Not:
   *IP Adresi, Alt Ağ Maskesi ve Varsayılan Ağ Geçidi birleşimi yanlışsa **Ayarı Başlat** devre dışıdır ve sonraki ayarlara geçilemez. Girişte bir hata olmadığını onaylayın.*

8. **DNS Sunucusu** için **Birincil DNS** alanına dokunun, ekranda görüntülenen klavyeyi kullanarak birincil DNS sunucusu için IP adresini girin ve sonra **Tamam** öğesine dokunun.

   Önceki ekranda yansıtılan değeri onaylayın.

   Not:
   *IP adresi ataması ayarları için **Otomatik** öğesini seçtiğinizde, **Manuel** veya **Otomatik** arasından DNS sunucusu ayarlarını seçebilirsiniz. DNS sunucusu adresini otomatik alamıyorsanız, **Manuel** öğesini seçin ve DNS sunucusu adresini girin. Sonra, ikincil DNS sunucusu adresini doğrudan girin. **Otomatik** öğesini seçerseniz adım 10'a gidin.*

9. **İkincil DNS** alanına dokunun, ekranda görüntülenen klavyeyi kullanarak ikincil DNS sunucusu için IP adresini girin ve sonra **Tamam** öğesine dokunun.

   Önceki ekranda yansıtılan değeri onaylayın.

10. **Ayarı Başlat** öğesine dokunun.

11. Onay ekranında **Kapat** öğesine dokunun.

    Kapat düğmesine dokunmazsanız belirli bir süreden sonra ekran otomatik kapanır.

Ethernet'e Bağlama

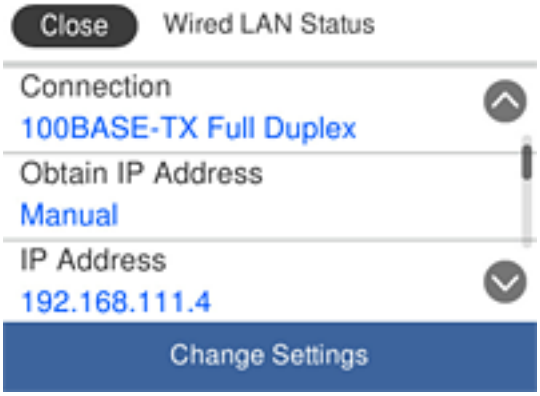
Tarayıcı ağa Ethernet kablosunu kullanarak bağlayın ve bağlantıyı kontrol edin.

1. Tarayıcı ve hub'ı (L2 anahtarı) Ethernet kablosuyla bağlayın.

   Ana ekrandaki simge olarak değişir.

2. Ana ekranda öğesine dokunun.

3. Ekrana yukarı doğru hızlı kaydırın ve sonra bağlantı durumunun ve IP adresinin doğru olduğundan emin olun.



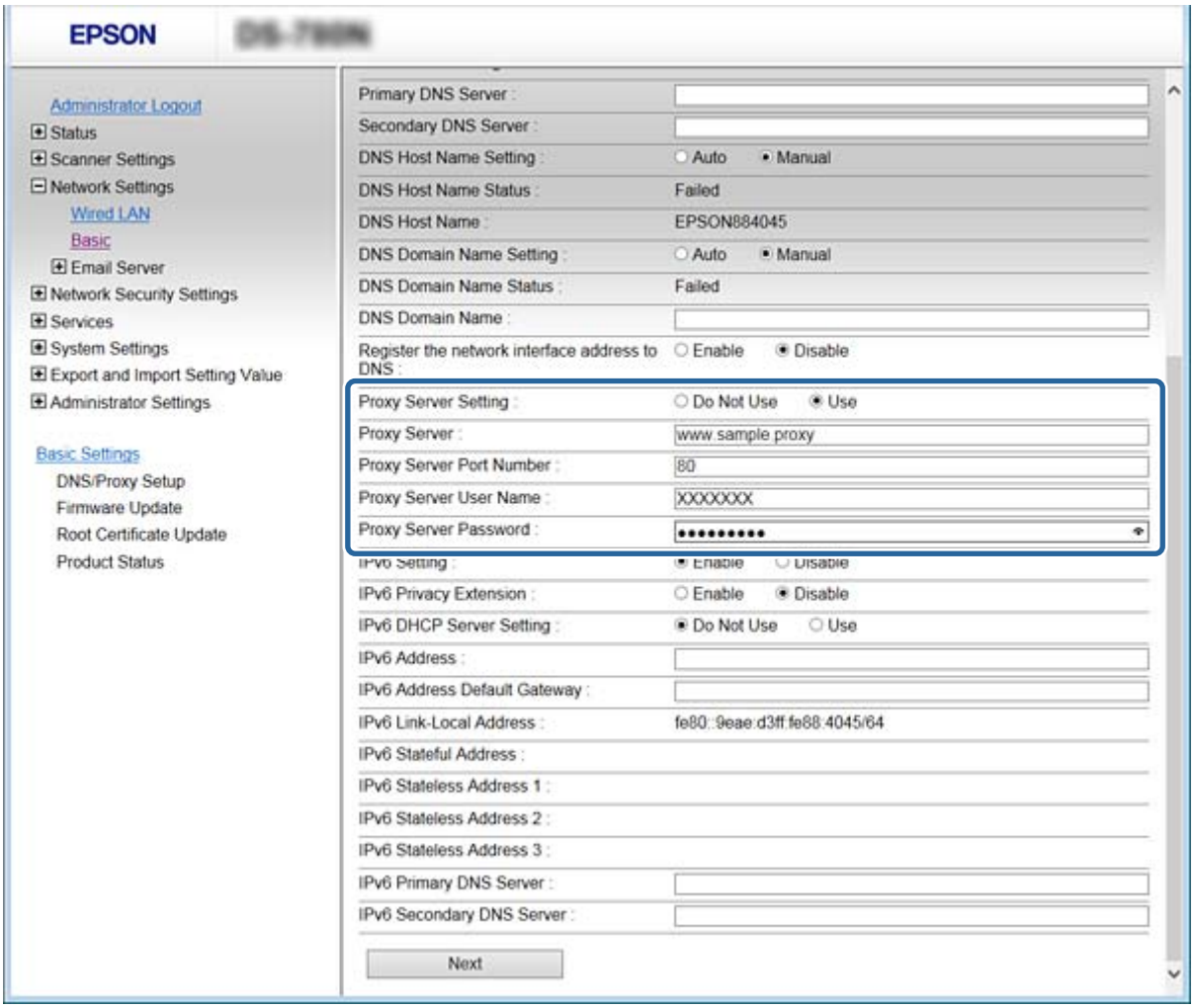
Proxy Sunucusunu Ayarlama

Proxy sunucusu panelde ayarlanamaz. Web Config'i kullanarak yapılandırın.

1. Web Config'e erişin ve **Network Settings** > **Basic** öğesini seçin.
2. **Proxy Server Setting** içinde **Use** öğesini seçin.
3. **Proxy Sunucu** içinde IPv4 adresinde veya FQDN biçiminde proxy sunucusunu belirtin ve sonra **Proxy Server Port Number** içinde bağlantı noktası numarasını girin.

   Kimlik doğrulaması gerektiren proxy sunucuları için Proxy sunucusu kimlik doğrulama kullanıcı adını ve Proxy sunucusu kimlik doğrulama parolasını girin.

4. **Next** düğmesini tıklatın.



5. Ayarları onaylayın ve sonra **Ayarlar** öğesine tıklayın.

İlgili Bilgi

➡ “Web Config Erişimi” sayfa 23

Yükleyiciyi Kullanarak Ağa Bağlanma

Tarayıcıyı bir bilgisayara bağlamak için yükleyiciyi kullanmanızı öneririz. Aşağıdaki yöntemlerden birini kullanarak yükleyiciyi çalıştırabilirsiniz.

❏ Web sitesini ayarlama

Aşağıdaki web sitesine erişin ve sonra ürünün adını girin. **Kurulum** öğesine gidin ve sonra ayarlamayı başlatın.

http://epson.sn

❏ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücüleri olan bilgisayarları olan kullanıcılar içindir.)

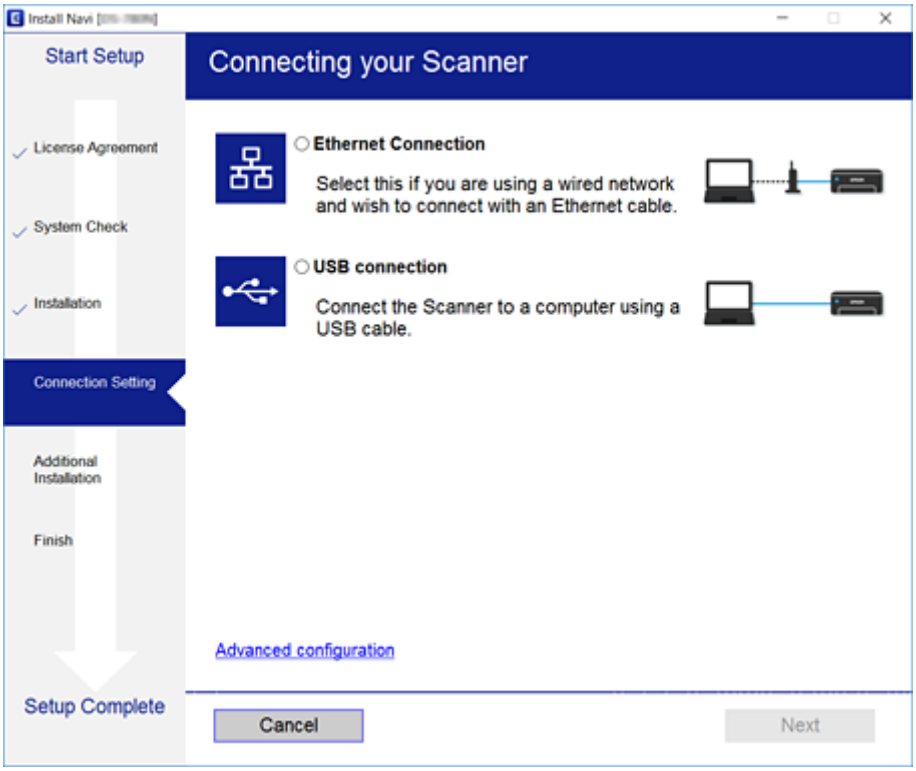
Yazılım diskini bilgisayara takın ve sonra ekrandaki talimatları izleyin.

Bağlantı Yöntemlerini Seçme

Aşağıdaki ekran görüntülenene kadar ekrandaki talimatları izleyin ve sonra tarayıcının bilgisayara bağlantı yöntemini seçin.

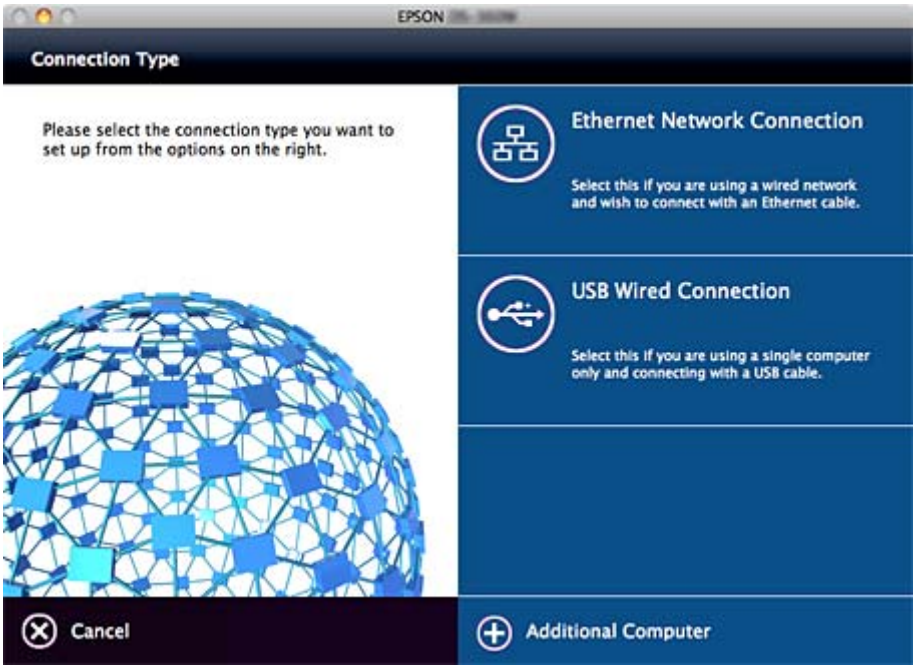
❏ Windows

Bağlantı türünü seçin ve sonra **İleri** öğesine tıklayın.



❏ Mac OS

Bağlantı türünü seçin.



Bağlantı

Ekrandaki talimatları izleyin. Gerekli yazılım yüklenir.

İşlev Ayarları

Bu bölümde her işlevi kullanabilmek için yapılacak ilk ayarlar açıklanmaktadır.

Ayar İçin Yazılım

Bu konuda, Web Config kullanılarak yöneticinin bilgisayarından ayarları yapma prosedürü açıklanmaktadır.

Web Config (Aygıt İçin Web Sayfası)

Web Config Hakkında

Web Config, web tarayıcısı tabanlı, tarayıcının ayarlarını yapılandırmaya yarayan bir uygulamadır.

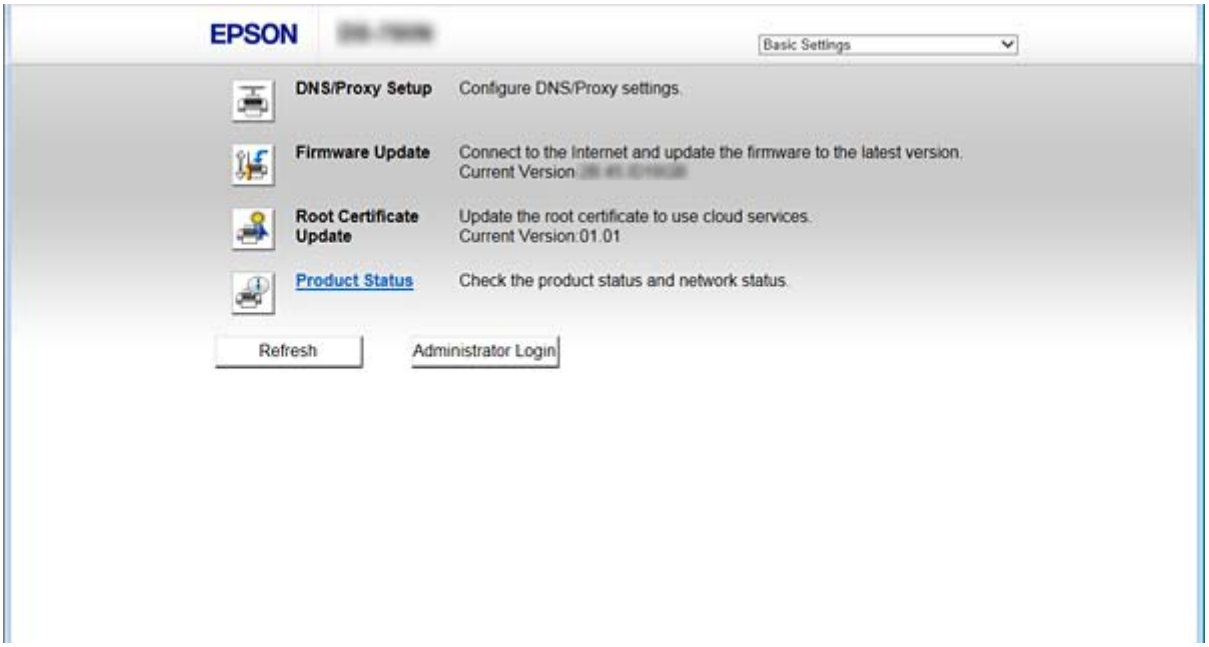
Web Config'e erişebilmek için öncelikle tarayıcıya bir IP adresi atamalısınız.

Not:
Tarayıcının yönetici şifresini yapılandırarak ayarları kilitleyebilirsiniz.

Aşağıdaki gibi iki ayar sayfası mevcuttur.

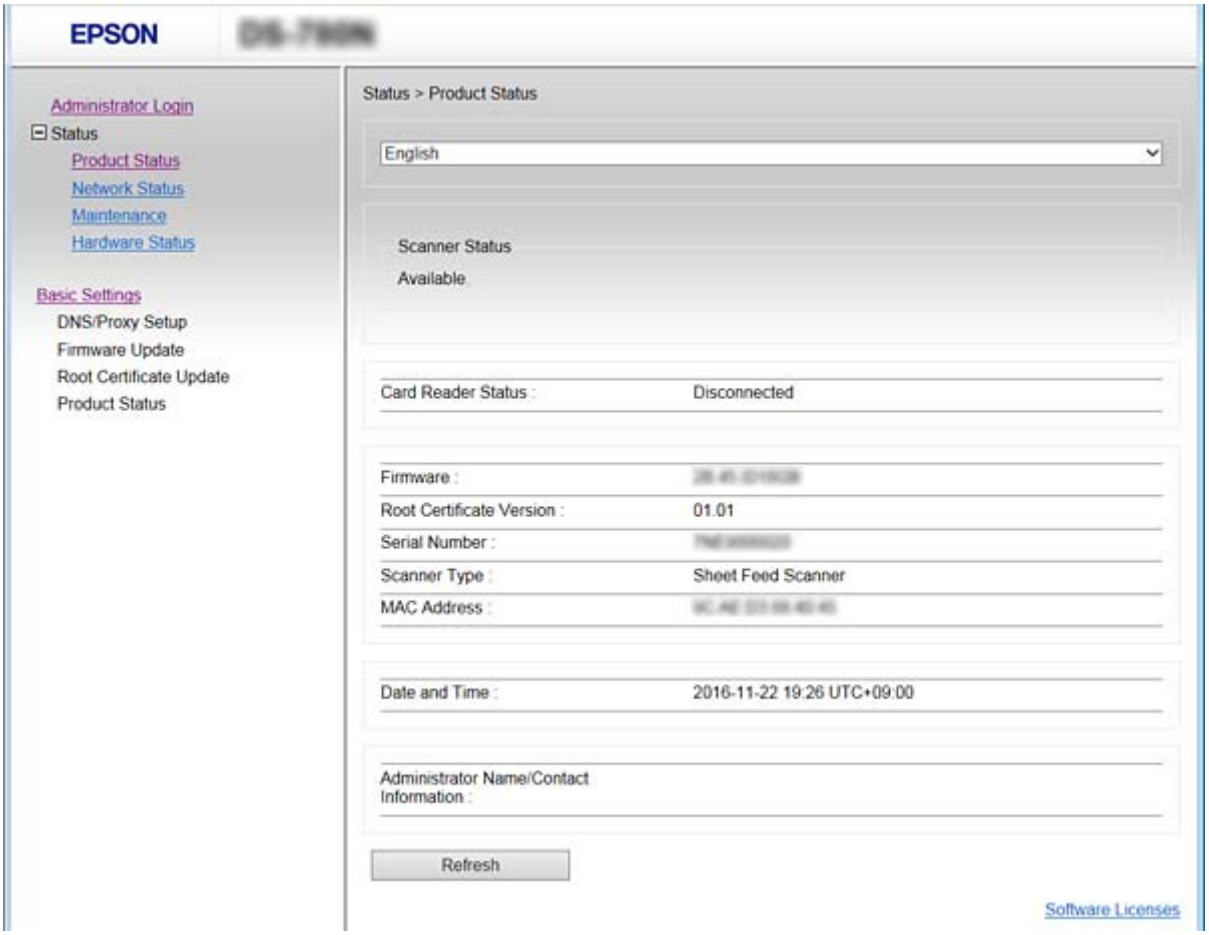
❏ **Basic Settings**

Tarayıcının temel ayarlarını yapılandırabilirsiniz.



❏ **Advanced Settings**

Tarayıcının gelişmiş ayarlarını yapılandırabilirsiniz. Bu sayfa asıl olarak yönetici içindir.



Web Config Erişimi

Tarayıcının IP adresini bir web tarayıcısına girin. JavaScript etkinleştirilmiş olmalıdır. HTTPS yoluyla Web Config'e erişirken tarayıcıda depolanan kendinden imzalı sertifika kullanıldığından web tarayıcısında bir uyarı mesajı görünür.

❏ HTTPS üzerinden erişim

IPv4: https://<tarayıcı IP adresi> (< > işaretleri olmadan)

IPv6: https://[tarayıcı IP adresi]/ ([ ] işaretleri ile birlikte)

❏ HTTP üzerinden erişim

IPv4: http://<tarayıcı IP adresi> (< > işaretleri olmadan)

IPv6: http://[tarayıcı IP adresi]/ ([ ] işaretleri ile birlikte)

Not:

❏ *Örnekler*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

https://[2001:db8::1000:1]/

http://[2001:db8::1000:1]/

❏ *Tarayıcı ismi DNS sunucusu ile kayıtlıysa, tarayıcının IP adresi yerine tarayıcı ismini kullanabilirsiniz.*

İlgili Bilgi

➡ "Tarayıcıyla SSL/TLS İletişimi" sayfa 62

➡ "Dijital Sertifikasyon Hakkında" sayfa 62

Tarama İşlevlerini Kullanma

Tarayıcıyı nasıl kullandığınıza bağlı olarak, aşağıdaki yazılımı yükleyin ve kullandığınızdan emin olun.

❏ **Bilgisayardan tara**

❏ Web Config (fabrika nakliyesinde geçerli) ile ağ tarama hizmetinin doğruluğunu onaylayın.

❏ Epson Scan 2'yi bilgisayarınıza yükleyin ve IP adresini ayarlayın

❏ İşleri kullanarak tararken, Document Capture Pro (Document Capture) öğesini yükleyin ve iş ayarlarını yapın.

❏ **Çalışma panelinden tarama**

❏ Document Capture Pro veya Document Capture Pro Server'ı kullanırken:

Document Capture Pro veya Document Capture Pro Server'ı yükleyin

DCP ayarı (sunucu modu, istemci modu).

❏ WSD protokolünü kullanırken:

Web Config veya çalışma panelinde (fabrika nakliyesinde geçerli) WSD'nin doğruluğunu onaylayın

Ek aygıt ayarları (Windows bilgisayar).

Bilgisayardan Tarama

Yazılımı yükleyin ve bilgisayardan bir ağ yoluyla taramak için ağ tarama hizmetinin etkinleştirildiğini kontrol edin.

İlgili Bilgi

➡ "Yüklenecek yazılım" sayfa 25

➡ "Ağdan Taramayı Etkinleştirme" sayfa 25

Yüklenecek yazılım

❏ Epson Scan 2

Bu bir tarayıcı sürücüsüdür. Cihazı bilgisayardan kullanıyorsanız, her istemci bilgisayarına sürücüyü yükleyin. Document Capture Pro/Document Capture yüklüyse cihazın düğmelerine atanan işlemleri gerçekleştirebilirsiniz.

EpsonNet SetupManager ile yazıcı sürücüleri de paketlerde dağıtılabilir.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

İstemci bilgisayarına yükleyin. Bilgisayar ve tarayıcının çalışma panelinden ağda yüklü Document Capture Pro/Document Capture ile bir bilgisayarda kayıtlı işleri çağırabilir ve yürütebilirsiniz.

Ağ yoluyla bilgisayardan da tarayabilirsiniz. Taramak için Epson Scan 2 gerekir.

İlgili Bilgi

➡ "EpsonNet SetupManager" sayfa 56

Tarayıcının IP adresini Epson Scan 2 olarak ayarlama

Tarayıcının IP adresini belirtin, böylece tarayıcı ağda kullanılabilir.

1. **Başlangıç** > **Tüm Programlar** > **EPSON** > **Epson Scan 2** içinden **Epson Scan 2 Utility**'yi başlatın.

   Başka bir tarayıcı zaten kayıtlıysa adım 2'ye gidin.

   Kaydedilmediyse adım 4'e gidin.

2. **Tarayıcı** üzerindeki ▼ öğesine tıklatın.

3. **Ayarlar** öğesine tıklayın.

4. **Düzenlemeyi Etkinleştir** seçeneğine ve ardından **Ekle** seçeneğine tıklayın.

5. Tarayıcı modeli adını **Model** içinden seçin.

6. **Ağ Ara** içinde **Adres** içinden kullanılacak tarayıcının IP adresini seçin.

   Listeyi güncellemek için  öğesine tıklayın ve  öğesine tıklatın. Tarayıcının IP adresini bulamazsanız, **Adresi girin** öğesini seçin ve IP adresini girin.

7. **Ekle** öğesine tıklayın.

8. **Tamam** öğesine tıklayın.

Ağdan Taramayı Etkinleştirme

Ağ üzerinden bir istemci bilgisayarından taradığınızda ağ tarama hizmetini ayarlayabilirsiniz. Varsayılan ayar etkinleştirilir.

1. Web Config'e erişin ve **Services** > **Network Scan** öğesini seçin.

2. **EPSON Scan**, **Enable scanning** öğesinin seçildiğinden emin olun.

   Seçiliyse bu görev tamamlanır. Web Config'i kapatın.

   İşareti silinmişse seçin ve sonraki adıma gidin.

3. **Next** öğesine tıklayın.

4. **OK** öğesine tıklayın.

   Ağ yeniden bağlanır ve sonra ayarlar etkinleştirilir.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Kontrol panelini kullanarak tarama

Tarayıcının kontrol panelini kullanarak klasöre tarama işlevi ve postaya tarama işlevi ve tarama sonuçlarını postaya, klasörlere vb. aktarma, bilgisayardan bir iş yürütülerek gerçekleştirilir.

Tarama sonuçlarını aktarırken, Document Capture Pro Server veya Document Capture Pro ile işi ayarlayın.

Ayarlar ve işi ayarlama hakkında ayrıntılar için Document Capture Pro Server veya Document Capture Pro belgesine veya yardımına bakın.

İlgili Bilgi

➡ "Document Capture Pro Server/Document Capture Pro ayarları" sayfa 26

➡ "Sunucu ve Klasörleri Ayarlama" sayfa 27

Bilgisayara yüklenecek yazılım

❏ **Document Capture Pro Server**

Bu, Document Capture Pro'nun sunucu sürümüdür. Bir Windows sunucusuna yükleyin. Birden fazla aygıt ve iş sunucu tarafından merkezi olarak yönetilebilir. İşler eşzamanlı olarak birden fazla tarayıcıdan yönetilebilir.

Document Capture Pro Server'ın sertifikalı sürümünü kullanarak, kullanıcılara ve gruplara bağlı işleri ve tarama geçmişini yönetebilirsiniz.

Document Capture Pro Server ayrıntıları için yerel Epson ofisinize başvurun.

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

Bilgisayardan taramaya benzer olarak bilgisayarda kayıtlı işleri kontrol panelinden çağırabilirsiniz ve bunları yürütebilirsiniz. Birden fazla tarayıcıdan bilgisayar işlerini eşzamanlı olarak çalıştırmanız mümkün değildir.

Document Capture Pro Server/Document Capture Pro ayarları

Tarayıcının çalışma panelinden tarama işlevini kullanmak için ayarları yapın.

1. Web Config'e erişin ve **Services** > **Document Capture Pro** öğesini seçin.

2. **Çalışma Modu** öğesini seçin.

   ❏ Server Mode:

   Yalnızca belirli bir bilgisayar için ayarlanmış işler için Document Capture Pro Server öğesini kullanırken veya Document Capture Pro öğesini kullanırken bunu seçin.

   ❏ Client Mode:

   Bilgisayarı belirtmeden ağda her istemci bilgisayarda yüklü Document Capture Pro (Document Capture) iş ayarını seçerken bunu ayarlayın.

3. Seçili moda göre aşağıdakini ayarlayın.

   ❏ Server Mode:

   Server Address içinde, Document Capture Pro Server öğesinin yüklendiği sunucuyu belirtin. IPv4, IPv6, ana bilgisayar adı, FQDN biçiminde 2 ila 252 karakter arası olabilir. FQDN biçiminde, US-ASCII harfler, sayılar, alfabeler ve tireler (başta ve sonda hariç) kullanılabilir.

   ❏ Client Mode:

   Document Capture Pro (Document Capture) içinden belirtilen bir tarayıcı grubunu kullanmak için **Group Settings** öğesini belirtin.

4. **Ayarlar** öğesine tıklayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Sunucu ve Klasörleri Ayarlama

Document Capture Pro ve Document Capture Pro Server taranan verileri sunucu veya istemci bilgisayarına bir kez kaydeder ve klasöre tarama işlevini ve postaya tarama işlevini yürütmek için aktarım işlevini kullanır.

Document Capture Pro, Document Capture Pro Server'ın yüklü olduğu bilgisayardan bilgisayara veya bulut hizmetine aktarmak için yetki ve bilgi gerekir.

Aşağıdakine bakarak kullanacağınız işlev hakkında bilgi hazırlayın.

Document Capture Pro veya Document Capture Pro Server'ı kullanarak bu işlevler için ayarları yapabilirsiniz. Ayarlar hakkındaki ayrıntılar için Document Capture Pro Server veya Document Capture Pro için olan belgelere veya yardıma bakın.

Ad	Ayarlar	Gereksinim
Ağ Klasörüne Tarama (SMB)	Kaydetme klasörünün paylaşımını oluşturun ve ayarlayın	Kaydetme klasörlerini oluşturan bilgisayara yönetici kullanıcı hesabı.
	Ağ Klasörüne Tarama (SMB) İçin Hedef	Kaydetme klasörünü içeren bilgisayarda oturum açmak için kullanıcı adı ve parola ve kaydetme klasörünü güncelleme ayrıcalığı.
Ağ Klasörüne Tarama (FTP)	FTP sunucusu oturumu açma için kurulum	FTP sunucusu için oturum açma bilgileri ve kaydetme klasörünü güncelleme ayrıcalığı.
E-postaya Tarama	E-posta sunucusu için kurulum	E-posta sunucusu için kurulum bilgileri

Ad	Ayarlar	Gereksinim
Document Capture Pro'ya Tarama (Document Capture Pro Server kullanırken)	Bulut hizmetlerinde oturum açmak için kurulum	Internet bağlantısı ortamı Bulut hizmetleri için hesap kaydı

WSD taramayı kullanma (yalnızca Windows)

Bilgisayar Windows Vista veya üstünü kullanıyorsa WSD taramayı kullanabilirsiniz.

WSD protokolü kullanılabilirken, **Bilgisayar (WSD)** menüsü tarayıcının kontrol panelinde görüntülenecektir.

1. Web Config'e erişin ve **Services** > **Protocol** öğesini seçin.
2. **Enable WSD** öğesinin **WSD Settings** içinde işaretlendiğinden emin olun.
   İşaretlenmişse göreviniz tamamdır ve Web Config'i kapatabilirsiniz.
   İşaretlenmemişse işaretleyin ve sonraki adıma ilerleyin.
3. **Next** düğmesini tıklatın.
4. Ayarları onaylayın ve **Ayarlar** öğesine tıklayın.

Sistem Ayarlarını Yapma

Kontrol Panelinde Sistem Ayarlarını Yapma

Ekran parlaklığını ayarlama

LCD ekran parlaklığını ayarlayın.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Genel Ayarlar** > **LCD Parlaklığı** öğesine dokunun.
3. Parlaklığı ayarlamak için  veya  öğesine dokunun.
   1 ila 9 arasından ayarlayabilirsiniz.
4. **Tamam** öğesine dokunun.

Sesi ayarlama

Panel çalışma sesini ve hata sesini ayarlayın.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Genel Ayarlar** > **Ses** öğesine dokunun.

3. Aşağıda öğeleri gerektiği gibi ayarlayın.
   - ❏ Çalışma sesi
     Çalışma panelinin çalışma sesinin ses seviyesini ayarlayın.
   - ❏ Hata sesi
     Hata sesinin düzeyini ayarlayın.
4. **Tamam** öğesine dokunun.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Orijinalin ikili beslemesini algılama

Taranacak belgenin ikili beslemesini algılamak için işlevi belirleyin ve birden fazla besleme oluştuğunda taramayı durdurun.

Zarflar veya etiketli kağıt gibi çoklu besleneceği düşünülen orijinalleri taramak için bunları kapalı olarak ayarlayın.

Not:
Ayrıca Web Config veya Epson Scan 2 öğesinden de ayarlanabilir.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Harici Tarama Ayarları** > **Yüksek Frekanslı Çift Besleme Alglm** öğesine dokunun.
3. Açmak veya kapatmak için **Yüksek Frekanslı Çift Besleme Alglm** öğesine dokunun.
4. **Kapat** öğesine dokunun.

Düşük hız moduna ayarlama

Düşük hızda taramaya ayarlayın, böylece makbuzlar gibi ince belgeleri tararken kağıt sıkışmaları oluşmaz.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Harici Tarama Ayarları** > **Yavaş** öğesine dokunun.
3. Açmak veya kapatmak için **Yavaş** öğesine dokunun.
4. **Kapat** öğesine dokunun.

Web Config'i Kullanarak Sistem Ayarlarını Yapma

İşlem Yapılmadığında Güç Tasarrufu Ayarları

Tarayıcının işlem yapılmadığında güç tasarrufu ayarını yapın. Kullanım ortamınıza göre zamanı ayarlayın.

Not:
Tarayıcının kontrol panelinde güç tasarrufu ayarlarını yaptığınızdan da emin olabilirsiniz.

1. Web Config'e erişin ve **System Settings** > **Power Saving** öğesini seçin.
2. İşlem yapılmadığında güç tasarrufu moduna geçmek için **Sleep Timer** için zamanı girin.

   Dakika olarak en fazla 240 dakikaya ayarlayabilirsiniz.
3. **Power Off Timer** için kapanma süresini seçin.
4. **OK** öğesine tıklayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Kontrol Panelini Ayarlama

Tarayıcının kontrol panelini ayarlayın. Aşağıdaki gibi ayarlayabilirsiniz.

1. Web Config'e erişin ve **System Settings** > **Control Panel** öğesini seçin.
2. Aşağıda öğeleri gerektiği gibi ayarlayın.
   - ❏ Language

     Kontrol panelinde görüntülenen dili seçin.
   - ❏ Panel Lock

     ON öğesini seçerseniz, yöneticinin yetkisini gerektiren bir işlem gerçekleştirirken yönetici parolası gerekir. Yönetici parolası ayarlanmazsa panel kilidi devre dışı bırakılır.
   - ❏ Operation Timeout

     ON öğesini seçerseniz yönetici olarak oturum açtığınızda, oturumunuz otomatik kapanır ve belirli bir süre bir işlem yapmazsanız başlangıç ekranına gidersiniz.

     10 saniye ve 240 dakika arasında saniye cinsinden ayarlayabilirsiniz.
3. **OK** öğesine tıklayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Harici Arayüz İçin Kısıtlamayı Ayarlama

Bilgisayardan USB bağlantısını kısıtlayabilirsiniz. Ağ dışında bir yolla taramayı sınırlamaya ayarlayın.

1. Web Config'e erişin ve **System Settings** > **External Interface** öğesini seçin.
2. **Enable** ya da **Disable** öğesini seçin.

   Kısıtlamak için **Disable** öğesini seçin.
3. **OK** öğesine dokunun.

Zaman Sunucusuyla Tarih ve Saati Eşitleme

Bir CA sertifikası kullanıyorsanız, zamanda yaşanacak sorunları önleyebilirsiniz.

1. Web Config'e erişin ve **System Settings** > **Date and Time** > **Time Server** öğesini seçin.
2. **Use** için **Use Time Server** seçimini yapın.
3. **Time Server Address** için zaman sunucusu adresini girin.

   IPv4, IPv6 ya da FQDN formatını kullanabilirsiniz. 252 karakter veya daha az girin. Bunu belirtmezseniz boş bırakın.
4. **Update Interval (min)** girin.

   Dakika olarak en fazla 10.800 dakikaya ayarlayabilirsiniz.
5. **OK** öğesine tıklayın.

   Not:
   Time Server Status *üzerinde zaman sunucusuyla bağlantı durumunu onaylayabilirsiniz.*

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Temel Güvenlik Ayarları

Bu bölümde özel bir ortam gerektirmeyen temel güvenlik ayarları açıklanmaktadır.

Temel Güvenlik Özelliklerine Giriş

Epson Aygıtların temel güvenlik özelliklerine giriş yapacağız.

Özellik adı	Özellik türü	Ayarlanacaklar	Korunacaklar
Yönetici parolasını ayarlayın	Ağ ve USB bağlantısı ayarları gibi sistemle ilgili ayarları kilitleyin, böylece yönetici haricinde kimse değiştirilemez.	Bir yönetici aygıta bir parola ayarlar. Web Config, kontrol paneli, Epson Device Admin ve EpsonNet Config'den herhangi bir yerden yapılandırma veya güncelleme kullanılabilir.	Kimlik, parola, ağ ayarları ve kişiler gibi aygıtta depolanan bilgilerin yasal olmayan bir şekilde okunmasını ve değiştirilmesini önler. Ayrıca, ağ ortamı veya güvenlik ilkesi gibi bilgi sızıntısı gibi çok çeşitli güvenlik riski ayarlarını azaltır.
SSL/TLS iletişimleri	Bir aygıttan Internet'te bir Epson sunucusuna erişirken, bir tarayıcı veya bellenim güncellemesi yoluyla bir bilgisayarla iletişim gibi SSL/TLS iletişimiyle iletişim içerikleri şifrelenir.	Bir CA imzalı sertifika edinin ve sonra onu tarayıcıya alın.	CA imzalı sertifika ile bir aygıt kimliğini temizleme kişiselleştirme ve yetkisi erişimi önler. Ek olarak, SSL/TLS'nin iletişim içeriği korunur ve verileri yazdırma ve kurulum bilgileri için içeriğin sızmasını önler.
Protokolleri kontrol eder	Aygıtlar ve bilgisayarlar arasında iletişim için kullanılan protokolleri kontrol eder ve işlevleri etkinleştirir / devre dışı bırakır.	Özelliklere uygulanan bir protokol veya hizmete ayrı ayrı izin verilir veya engellenir.	Kullanıcıların gereksiz işlevlerini kullanmalarını önleyerek beklenmedik kullanım yoluyla oluşabilecek güvenlik risklerini azaltma.

İlgili Bilgi

➡ “Web Config Hakkında” sayfa 22
➡ “EpsonNet Config” sayfa 55
➡ “Epson Device Admin” sayfa 55
➡ “Yönetici Şifresi Yapılandırma” sayfa 32
➡ “İletişim kurallarını denetleme” sayfa 35

Yönetici Şifresi Yapılandırma

Yönetici parolasını ayarladığınızda, yöneticiler dışındaki kullanıcılar sistem yöneticisinin ayarlarını değiştiremez. Web Config, tarayıcının kontrol paneli veya yazılımı (Epson Device Admin veyaEpsonNet Config) kullanarak yönetici parolasını ayarlayabilir ve değiştirebilirsiniz. Yazılımı kullanırken, her yazılım için belgelere bakın.

İlgili Bilgi

➡ “Kontrol Panelinden Yönetici Parolasını Yapılandırma” sayfa 33
➡ “Web Config'i Kullanarak Yönetici Parolasını Yapılandırma” sayfa 33
➡ “EpsonNet Config” sayfa 55
➡ “Epson Device Admin” sayfa 55

Kontrol Panelinden Yönetici Parolasını Yapılandırma

Yönetici parolasını tarayıcının kontrol panelinden ayarlayabilirsiniz.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Sistem Yöneticisi** > **Yntci Ayarları** öğesine dokunun.

   Öğe görüntülenmezse öğeyi görüntülemek için ekranı yukarı doğru hızlıca kaydırın.
3. **Yönetici Parolası** > **Kayıt ol** öğesine dokunun.
4. Yeni parolayı girin ve sonra **Tamam** öğesine dokunun.
5. Parolayı yeniden girin ve sonra **Tamam** öğesine dokunun.
6. Onay ekranında **Tamam** öğesine dokunun.

   Yönetici ayarları ekranı görüntülenir.
7. **Kilit Ayarları** öğesine dokunun ve sonra onay ekranında **Tamam** öğesine dokunun.

   Kilit Ayarları öğesi **Açık** olarak ayarlandığında ve kilitli menü öğesini çalıştırırken yönetici parolası gerekecektir.

Not:

- ***Ayarlar*** > ***Genel Ayarlar*** > ***Çalışma Zaman Aşımı*** *öğesini* ***Açık*** *olarak ayarlarsanız, kontrol panelinde bir süre bir işlem yapılmadığında tarayıcı oturumunuzu kapatacaktır.*
- ***Yönetici Parolası*** *ekranında* ***Değiştir*** *veya* ***Sıfırla*** *öğesini seçtiğinizde ve yönetici parolasını girdiğinizde yönetici parolasını değiştirebilir veya silebilirsiniz.*

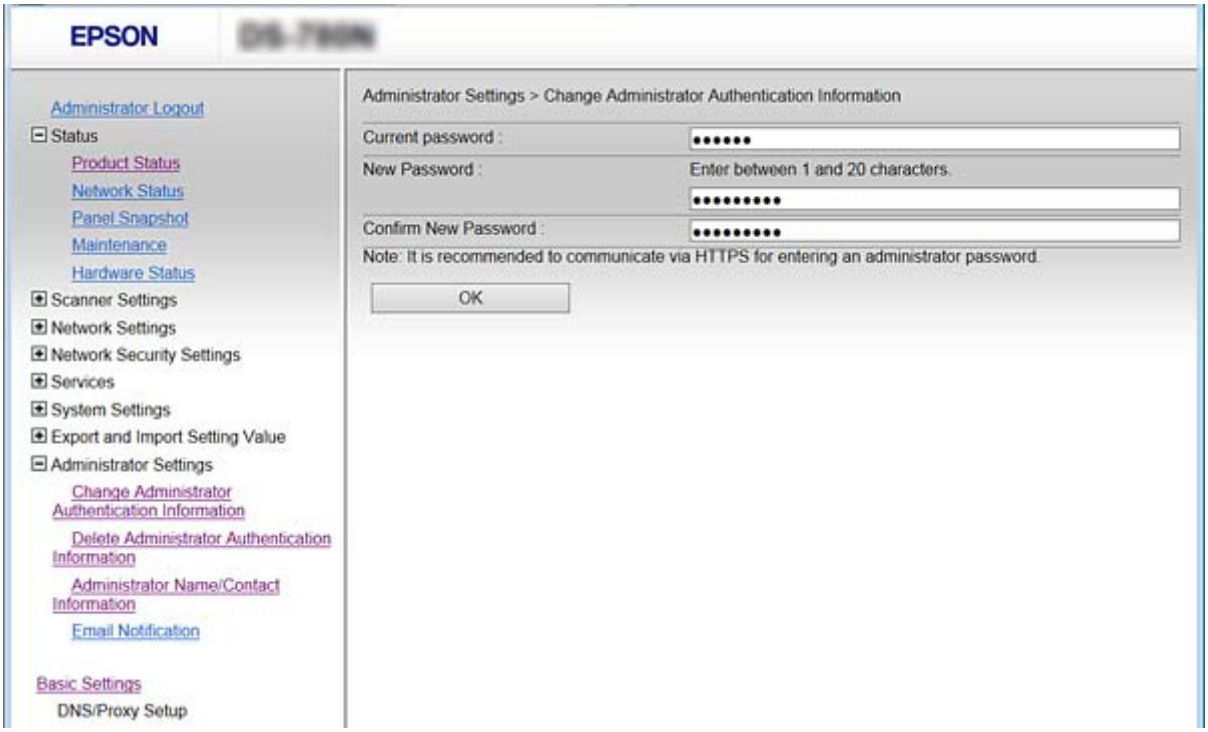
Web Config'i Kullanarak Yönetici Parolasını Yapılandırma

Web Config'i kullanarak yönetici parolasını ayarlayabilirsiniz.

1. Web Config'e erişin ve **Administrator Settings** > **Change Administrator Authentication Information** öğesini seçin.

2. **New Password** ve **Confirm New Password** kısmına bir şifre girin. Gerekirse kullanıcı adını girin.

   Şifreyi yenisiyle değiştirmek istiyorsanız, geçerli bir şifre yazın.



3. **OK** öğesini seçin.

   Not:

   ❏ *Kilitli menü öğelerini ayarlamak ve değiştirmek için **Administrator Login** öğesine tıklayın ve sonra yönetici parolasını girin.*

   ❏ *Yönetici parolasını silmek için **Administrator Settings** > **Delete Administrator Authentication Information** öğesine tıklayın ve sonra yönetici parolasını girin.*

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Yönetici Parolasıyla Kilitlenecek Öğeler

Yöneticilerin aygıtlardaki tüm özellikler için ayar ve değiştirme ayrıcalıkları vardır.

Ayrıca, cihazda yönetici parolasını ayarlarsanız, kilitleyebilirsiniz, böylece aygıt yönetimiyle ilgili öğeleri değiştiremezsiniz.

Aşağıdakiler bir yöneticinin kontrol edebildiği öğelerdir.

Öğe	Açıklama
Tarayıcı ayarları	İkili besleme yönünü ve düşük hız modunu ayarlama.
Ethernet bağlantısı ayarları	Aygıtların adını ve IP adresini değiştirin, DNS sunucusu veya proxy sunucusu ayarlarını ve ağ bağlantılarıyla ilgili ayar değişikliklerini yapın.

Öğe	Açıklama
Kullanıcı hizmetleri ayarı	İletişim protokolleri kontrolü, Ağ taraması ve Document Capture Pro hizmetleri için ayar.
E-posta sunucusu ayarı	Aygıtların doğrudan iletişim kurduğu bir e-posta sunucusu ayarı.
Güvenlik ayarı	Ağ güvenliği için SSL/TLS iletişimi, IPsec/IP filtreleme ve IEEE802.1X gibi ayarlar.
Kök Sertifikası Güncellemesi	Document Capture Pro Server kimlik doğrulaması ve Web Config'den bellenim güncellemesi için kök sertifikalarını güncelleme gerekir.
Bellenim güncellemesi	Aygıtların bellenimini kontrol edin ve güncelleyin.
Zaman, Zamanlayıcı ayarı	Uyku geçiş süresi, otomatik güç kapatma, tarih/saat, çalışmama zamanlayıcısı, zamanlayıcıyla ilgili diğer ayarlar.
Varsayılan ayarları geri yükleme	Tarayıcıyı fabrika ayarlarına sıfırlama ayarı.
Yönetici ayarı	Yönetici kilidi veya yönetici parolası ayarı.
Onaylı aygıt ayarı	Kimlik doğrulama aygıtının kimlik ayarı. Kimlik doğrulama aygıtlarını destekleyen bir kimlik doğrulama sisteminde tarayıcıyı kullanırken ayarlayın.

İletişim kurallarını denetleme

Çeşitli yolları ve iletişim kurallarını kullanarak tarayabilirsiniz. Belirtilmeyen sayıda ağ bilgisayarından ağ taramasını da kullanabilirsiniz. Örneğin, yalnızca belirtilen yol ve protokolleri kullanarak taramaya izin verilir. Belirli yollardan taramayı kısıtlayarak veya kullanılabilir işlevleri denetleyerek istenmeyen güvenlik risklerini azaltabilirsiniz.

İletişim kuralı ayarlarını yapılandırın.

1. Web Config'e erişin ve **Services** > **Protocol** öğesini seçin.
2. Her bir öğeyi yapılandırın.
3. **Next** öğesine tıklayın.
4. **OK** öğesine tıklayın.

   Ayarlar tarayıcıya uygulanır.

İlgili Bilgi

➡ “Web Config Erişimi” sayfa 23
➡ “Etkinleştirebileceğiniz veya Devre Dışı Bırakabileceğiniz İletişim Kuralları” sayfa 36
➡ “İletişim Kuralı Ayarlama Öğeleri” sayfa 37

Etkinleştirebileceğiniz veya Devre Dışı Bırakabileceğiniz İletişim Kuralları

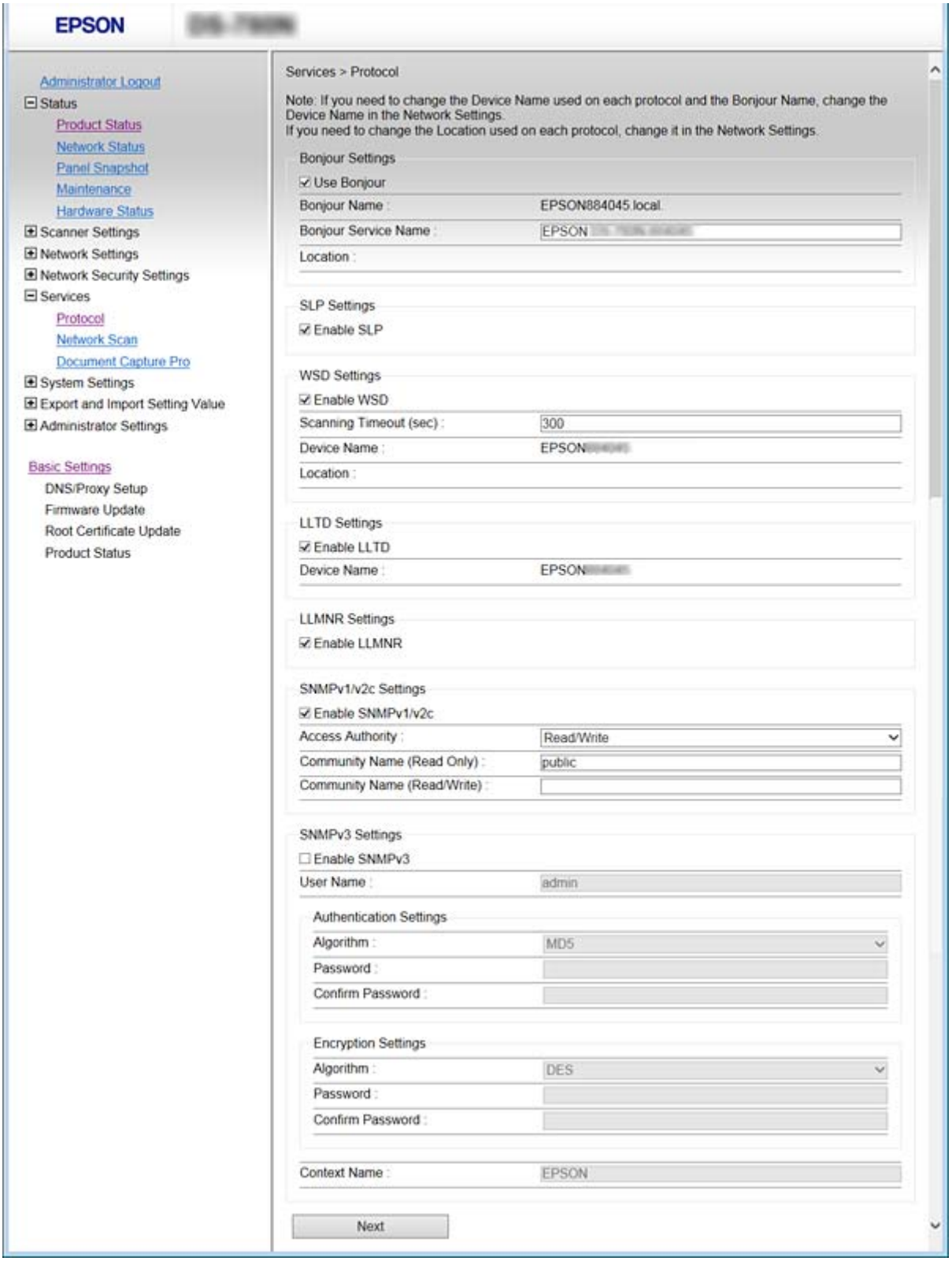
İletişim Kuralı	Açıklama
Bonjour Settings	Bonjour kullanılıp kullanılmayacağını belirleyebilirsiniz. Bonjour aygıtları aramak, taramak ve benzeri işlemler için kullanılır.
SLP Settings	SLP işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. SLP, EpsonNet Config. yazılımında Epson Scan 2 ve ağ arama için kullanılır.
WSD Settings	WSD işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde, WSD aygıtları ekleyebilir veya WSD bağlantı noktasından tarayabilirsiniz.
LLTD Settings	LLTD işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde, Windows ağ haritasında görüntülenir.
LLMNR Settings	LLMNR işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde, NetBIOS kullanamasanız bile DNS olmadan ad çözümlemesini kullanabilirsiniz.
SNMPv1/v2c Settings	SNMPv1/v2c özelliğinin etkinleştirilip etkinleştirilmeyeceğini belirleyebilirsiniz. Bu, aygıtları ayarlama, izleme ve benzeri işlemler için kullanılır.
SNMPv3 Settings	SNMPv3 özelliğinin etkinleştirilip etkinleştirilmeyeceğini belirleyebilirsiniz. Bu, şifreli aygıtları ayarlama, izleme vb. için kullanılır.

İlgili Bilgi

➡ “İletişim kurallarını denetleme” sayfa 35

➡ “İletişim Kuralı Ayarlama Öğeleri” sayfa 37

İletişim Kuralı Ayarlama Öğeleri



Öğeler	Ayar değeri ve Açıklama
Bonjour Settings	

Temel Güvenlik Ayarları

Öğeler	Ayar değeri ve Açıklama
Use Bonjour	Bonjour aracılığıyla aygıtları aramak veya kullanmak için bunu seçin.
Bonjour Name	Bonjour adını görüntüler.
Bonjour Service Name	Bonjour hizmeti adını görüntüleyebilir ve ayarlayabilirsiniz.
Location	Bonjour konum adını görüntüler.
SLP Settings	
Enable SLP	SLP işlevini etkinleştirmek için bunu seçin. Epson Scan 2 ve EpsonNet Config içinde ağ bulmak için kullanılır.
WSD Settings	
Enable WSD	Aygıtların WSD kullanılarak eklenmesini etkinleştirmek ve WSD bağlantı noktasından yazdırmak ve taramak için bunu seçin.
Scanning Timeout (sec)	WSD taramaya yönelik iletişim zaman aşımı değerini 3 ila 3.600 saniye arasında girin.
Device Name	WSD aygıt adını görüntüler.
Location	WSD konum adını görüntüler.
LLTD Settings	
Enable LLTD	LLTD etkinleştirmek için bunu seçin. Tarayıcı Windows ağ haritasında görüntülenir.
Device Name	LLTD aygıt adını görüntüler.
LLMNR Settings	
Enable LLMNR	LLMNR etkinleştirmek için bunu seçin. NetBIOS kullanamasanız bile DNS olmadan ad çözümlemesini kullanabilirsiniz.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	SNMPv1/v2c etkinleştirmek için seçin. Yalnızca SNMPv3 destekleyen tarayıcılar görüntülenir.
Access Authority	SNMPv1/v2c etkinleştirildiğinde erişim yetkilisini ayarlayın. **Read Only** ya da **Read/Write** öğesini seçin.
Community Name (Read Only)	0 ila 32 ASCII (0x20 ila 0x7E) karakter girin.
Community Name (Read/Write)	0 ila 32 ASCII (0x20 ila 0x7E) karakter girin.
SNMPv3 Settings	
Enable SNMPv3	Kutu işaretlendiğinde SNMPv3 etkinleştirilir.
User Name	1 bayt karakterleri kullanarak 1 ve 32 karakter arası girin.
Authentication Settings	
Algorithm	SNMPv3 için kimlik doğrulama için bir algoritma seçin.

Temel Güvenlik Ayarları

Öğeler	Ayar değeri ve Açıklama
Password	SNMPv3 için kimlik doğrulama için parolayı girin. 8 ve 32 karakter arası ASCII (0x20–0x7E) girin. Bunu belirtmezseniz boş bırakın.
Confirm Password	Yapılandırdığınız parolayı onay için girin.
Encryption Settings	
Algorithm	SNMPv3. için şifreleme için bir algoritma seçin.
Password	SNMPv3 için şifreleme için parolayı girin. 8 ve 32 karakter arası ASCII (0x20–0x7E) girin. Bunu belirtmezseniz boş bırakın.
Confirm Password	Yapılandırdığınız parolayı onay için girin.
Context Name	32 karakter veya daha kısa Unicode (UTF-8) girin. Bunu belirtmezseniz boş bırakın. Girilebilen karakter sayısı dile bağlı olarak değişir.

İlgili Bilgi

➡ “İletişim kurallarını denetleme” sayfa 35
➡ “Etkinleştirebileceğiniz veya Devre Dışı Bırakabileceğiniz İletişim Kuralları” sayfa 36

Çalıştırma ve Yönetim Ayarları

Bu bölümde günlük işlemler ve aygıtın yönetimiyle ilgili öğeler açıklanmaktadır.

Aygıtın Bilgilerini Onaylama

Web Config öğesini kullanarak **Status** öğesinden çalıştırma aygıtının aşağıdaki bilgilerini kontrol edebilirsiniz.

❏ Product Status

Dil, durum, ürün numarası, MAC adresi vb.'yi kontrol edin.

❏ Network Status

Ağ bağlantısı durumu, IP adresi, DNS sunucusu vb. bilgilerini kontrol edin.

❏ Panel Snapshot

Aygıtın kontrol panelinde görüntülenen bir ekran görüntüsü görüntüleyin.

❏ Maintenance

Başlangıç Tarihi, Tarama Bilgileri vb.'yi kontrol edin.

❏ Hardware Status

Tarayıcının durumunu kontrol edin.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Aygıtları Yönetme (Epson Device Admin)

Epson Device Admin'i kullanarak birçok aygıtı yönetebilir ve çalıştırabilirsiniz. Epson Device Admin, farklı bir ağda bulunan aygıtları yönetmenizi sağlar. Aşağıda ana yönetim özellikleri özetlenmektedir.

İşlevler ve yazılımı kullanma hakkında daha fazla bilgi için belgelere veya Epson Device Admin yardımına bakın.

❏ Aygıtları bulma

Ağdaki aygıtları bulabilir ve sonra onları bir listeye kaydedebilirsiniz. Yazıcılar ve tarayıcılar gibi Epson aygıtlar yöneticinin bilgisayarıyla aynı ağ segmentine bağlanırsa henüz bir IP adresi atanmamış olsalar bile bunları bulabilirsiniz.

USB kablolarla ağda bilgisayarlara bağlı aygıtları da bulabilirsiniz. Epson Device USB Agent öğesini bilgisayara yüklemeniz gerekir.

❏ Aygıtları ayarlama

Ağ arayüzü ve kağıt kaynağı gibi ayar öğelerini içeren bir şablon yapabilirsiniz ve paylaşılan ayarlar olarak diğer aygıtlara uygulayabilirsiniz. Ağa bağlandığında, IP adresi atanmamış bir aygıtta bir IP adresi atayabilirsiniz.

❏ Aygıtları izleme

Ağdaki aygıtlar için düzenli olarak durum ve ayrıntılı bilgileri alabilirsiniz. Ayrıca USB kablolarıyla ağdaki bilgisayarlara bağlı aygıtları ve aygıt listesine kaydedilmiş diğer şirketlerin aygıtlarını da izleyebilirsiniz. USB kablolarla bağlı aygıtları izlemek için Epson Device USB Agent öğesini yüklemeniz gerekir.

❏ Uyarıları yönetme

Aygıtların ve sarf malzemelerinin durumu hakkında uyarıları yönetebilirsiniz. Sistem ayarlanan koşullara göre otomatik olarak yöneticiye bildirim e-postaları gönderir.

❏ Raporları yönetme

Sistem aygıt kullanımı ve sarf malzemeleriyle ilgili verileri topladıkça düzenli raporlar oluşturabilirsiniz. Sonra bu oluşturulan raporları kaydedebilir ve e-posta ile gönderebilirsiniz.

İlgili Bilgi

➡ "Epson Device Admin" sayfa 55

Olaylar Meydana Geldiğinde E-posta Bildirimi Alma

E-posta Bildirimleri Hakkında

Bu özelliği olaylar oluştuğunda e-postayla uyarılar almak için kullanabilirsiniz. En fazla 5 e-posta adresi kaydedebilirsiniz ve hangi olaylar için bildirimler almak istediğinizi seçebilirsiniz.

Bu işlevi kullanmak için posta sunucusu yapılandırılmalıdır.

İlgili Bilgi

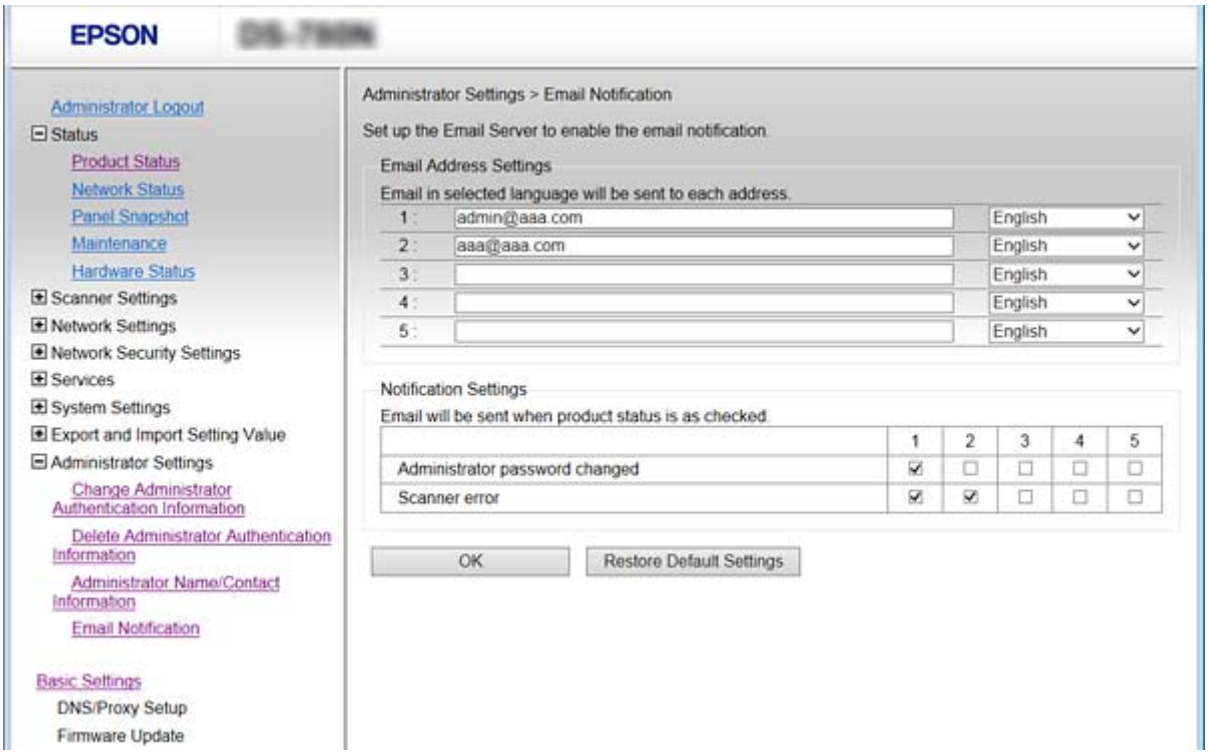
➡ "Posta Sunucusu Yapılandırma" sayfa 42

E-posta Bildirimini Yapılandırma

Özelliği kullanmak için bir posta sunucusu yapılandırmalısınız.

1. Web Config'e erişin ve **Administrator Settings** > **Email Notification** öğesini seçin.
2. E-posta bildirimlerini almak istediğiniz bir e-posta adresi girin.
3. E-posta bildirimleri için dili seçin.

4. Almak istediğiniz bildirimlerin kutularını işaretleyin.



5. **OK** öğesine tıklayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "Posta Sunucusu Yapılandırma" sayfa 42

Posta Sunucusu Yapılandırma

Yapılandırmadan önce aşağıdakileri kontrol edin.

❏ Tarayıcı bir ağa bağlı.

❏ Bilgisayarın e-posta sunucusu bilgileri.

1. Web Config'e erişin ve **Network Settings** > **Email Server** > **Basic** öğesini seçin.

2. Her öğe için bir değer girin.

3. **OK** öğesini seçin.

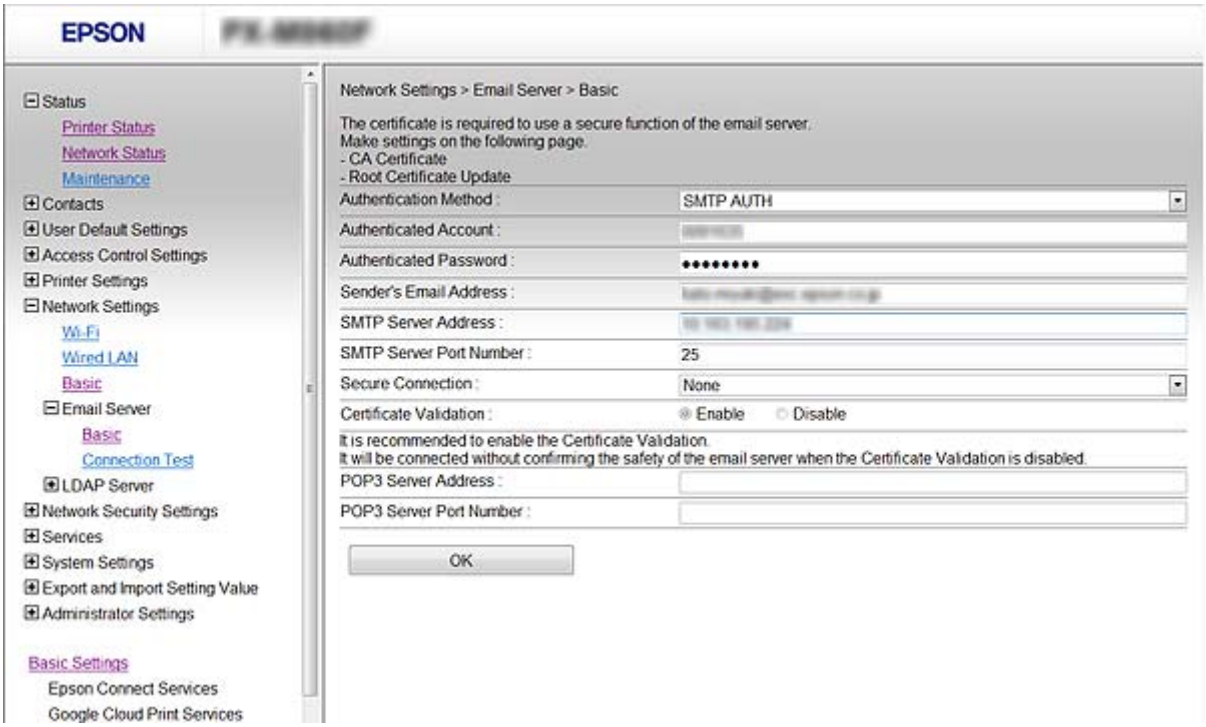
   Seçtiğiniz ayarlar görüntülenir.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "Posta Sunucusu Ayarlama Öğeleri" sayfa 43

Posta Sunucusu Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklamalar	
Authentication Method	Tarayıcının posta sunucusuna erişimi için kimlik doğrulama yöntemini belirtin.	
	Off	Bir posta sunucuyla iletişim kurarken kimlik doğrulama devre dışı bırakılır.
	SMTP AUTH	Bir posta sunucusunun SMTP Kimlik Doğrulamasını desteklemesini gerektirir.
	POP before SMTP	Yöntemi seçerken POP3 sunucusunu yapılandırın.
Authenticated Account	**SMTP AUTH** olarak **POP before SMTP** veya **Authentication Method** seçimini yaparsanız, ASCII (0x20–0x7E) biçimli 0 ila 255 karakterden oluşan kimlik doğrulaması yapılmış hesap adını girin.	
Authenticated Password	**Authentication Method** olarak **SMTP AUTH** veya **POP before SMTP** öğesini seçerseniz, 0 ve 20 karakter arasında şunları kullanarak kimlik doğrulama şifresini girin A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Göndericinin e-posta adresini girin. ASCII (0x20–0x7E) olarak şunlar hariç 0 ve 255 karakter arası girin : ( ) < > [ ] ; ¥. Başlangıç karakteri olarak "." kullanılamaz.	
SMTP Server Address	Şunları kullanarak 0 ila 255 arası karakter girin A–Z a–z 0–9 . - . IPv4 ya da FQDN formatını kullanabilirsiniz.	
SMTP Server Port Number	1 ile 65535 arasında bir sayı girebilirsiniz.	

Öğeler	Ayarlar ve Açıklamalar	
Secure Connection	E-posta sunucusu için güvenli bağlantı yöntemini belirleyin.	
	None	**POP before SMTP** kısmında **Authentication Method** seçimini yaparsanız bağlantı yöntemi **None** olarak ayarlanır.
	SSL/TLS	Bu, **Authentication Method** özelliği **Off** veya **SMTP AUTH** olarak ayarlandığında kullanılabilir.
	STARTTLS	Bu, **Authentication Method** özelliği **Off** veya **SMTP AUTH** olarak ayarlandığında kullanılabilir.
Certificate Validation	Bu etkinleştirildiğinde sertifika doğrulanır. Bunun **Enable** olarak ayarlanmasını öneririz.	
POP3 Server Address	**POP before SMTP** öğesini **Authentication Method** olarak seçerseniz, 0 ve 255 karakter arası şunları kullanarak POP3 sunucu adresini girin A–Z a–z 0–9 . - . IPv4 ya da FQDN formatını kullanabilirsiniz.	
POP3 Server Port Number	**POP before SMTP** öğesini **Authentication Method** olarak seçerseniz 1 ve 65535 arasında bir sayı girin.	

İlgili Bilgi

➡ "Posta Sunucusu Yapılandırma" sayfa 42

Posta Sunucusu Bağlantı Kontrolü

1. Web Config'e erişin ve **Network Settings** > **Email Server** > **Connection Test** öğesini seçin.
2. **Start** öğesini seçin.

   Posta sunucusuna bağlantı testi başlatılır. Kontrolün ardından kontrol raporu görüntülenir.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23
➡ "Posta Sunucusu Bağlantı Kontrolü Referansları" sayfa 44

Posta Sunucusu Bağlantı Kontrolü Referansları

Mesajlar	Açıklama
Connection test was successful.	Bu mesaj, sunucu bağlantısı başarılı olduğunda belirir.
SMTP server communication error. Check the following. - Network Settings	Bu mesaj aşağıdaki durumlarda görünür ❏ Tarayıcı bir ağa bağlı değil ❏ SMTP sunucusu çalışmıyor ❏ İletişim sırasında ağ bağlantısı kesildi ❏ Eksik veri alındı

Mesajlar	Açıklama
POP3 server communication error. Check the following. - Network Settings	Bu mesaj aşağıdaki durumlarda görünür ❏ Tarayıcı bir ağa bağlı değil ❏ POP3 sunucusu çalışmıyor ❏ İletişim sırasında ağ bağlantısı kesildi ❏ Eksik veri alındı
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Bu mesaj aşağıdaki durumlarda görünür ❏ Bir DNS sunucusuna bağlantı başarısız oldu ❏ Bir SMTP sunucusu için ad çözümlemesi başarısız oldu
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Bu mesaj aşağıdaki durumlarda görünür ❏ Bir DNS sunucusuna bağlantı başarısız oldu ❏ Bir POP3 sunucusu için ad çözümlemesi başarısız oldu
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Bu mesaj, SMTP sunucusu kimlik doğrulama başarısız olduğunda görünür.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Bu mesaj, POP3 sunucusu kimlik doğrulama başarısız olduğunda görünür.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Bu mesaj, desteklenmeyen iletişim kurallarıyla haberleşmeyi denediğinizde görünür.
Connection to SMTP server failed. Change Secure Connection to None.	Bu mesaj, sunucuyla istemci arasında SMTP uyuşmazlığı oluştuğunda veya sunucu SMTP güvenli bağlantısını (SSL bağlantısı) desteklemediğinde görünür.
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Bu mesaj, sunucuyla istemci arasında SMTP uyuşmazlığı oluştuğunda veya sunucu bir SSL/TLS bağlantısı (SMTP güvenli bağlantısı için) kullanmak istediğinde görünür.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Bu mesaj, sunucuyla istemci arasında SMTP uyuşmazlığı oluştuğunda veya sunucu bir STARTTLS bağlantısı (SMTP güvenli bağlantısı için) kullanmak istediğinde görünür.
The connection is untrusted. Check the following. - Date and Time	Bu mesaj, tarayıcının tarih ve saat ayarı yanlış olduğunda veya sertifikanın süresi bittiğinde görünür.
The connection is untrusted. Check the following. - CA Certificate	Bu mesaj, tarayıcı sunucuya karşılık gelen bir kök sertifikaya sahip olmadığında veya bir CA Certificate içe aktarılmamış olduğunda görünür.
The connection is not secured.	Bu mesaj, alınan sertifika bozuk olduğunda görünür.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Bu mesaj, sunucu ve bir istemci arasında kimlik doğrulama yöntemi uyuşmazlığı oluştuğunda görünür. Sunucu SMTP AUTH öğesini destekler.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Bu mesaj, sunucu ve bir istemci arasında kimlik doğrulama yöntemi uyuşmazlığı oluştuğunda görünür. Sunucuda SMTP AUTH desteklenmez.

Mesajlar	Açıklama
Sender's Email Address is incorrect. Change to the email address for your email service.	Bu mesaj, belirtilen gönderenin e-posta adresi yanlış olduğunda görünür.
Cannot access the product until processing is complete.	Bu mesaj tarayıcı meşgul olduğunda görünür.

İlgili Bilgi

➡ "Posta Sunucusu Bağlantı Kontrolü" sayfa 44

Bellenimi Güncelleme

Web Config Kullanarak Bellenimi Güncelleme

Web Config kullanarak bellenimi günceller. Aygıt Internet'e bağlanmalıdır.

1. Web Config'e erişin ve **Basic Settings** > **Firmware Update** öğesini seçin.
2. **Start** öğesine tıklayın.

   Bellenim onayı başlar ve güncellenen bellenim varsa bellenim bilgileri görüntülenir.
3. **Start** öğesine tıklayın ve ekrandaki talimatları izleyin.

Not:
Bellenimi ayrıca Epson Device Admin kullanarak da güncelleyebilirsiniz. Aygıt listesinde bellenim bilgilerini görsel olarak onaylayın. Birden fazla aygıtın bellenimini güncellemek istiyorken bu kullanışlıdır. Daha fazla ayrıntı için Epson Device Admin kılavuzu veya yardıma bakın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23
➡ "Epson Device Admin" sayfa 55

Epson Firmware Updater Kullanarak Bellenimi Güncelleme

Aygıtın bellenimini bilgisayardaki Epson web sitesinden indirebilirsiniz ve sonra bellenimi güncellemek için USB kablosu ile aygıtı ve bilgisayarı bağlayın. Ağ üzerinden güncelleyemiyorsanız bu yöntemi deneyin.

1. Epson web sitesine erişin ve bellenimi indirin.
2. USB kablosuyla indirilen bellenimi içeren bilgisayarı aygıta bağlayın.
3. İndirilen .exe dosyasına çift tıklayın.

   Epson Firmware Updater başlar.
4. Ekrandaki talimatları izleyin.

Ayarları Yedekleme

Web Config'de ayar öğelerini vererek ve ayarlayarak öğeleri diğer tarayıcılara kopyalayabilirsiniz.

Ayarları dışa aktarın

Tarayıcı için her bir ayarı dışa aktarın.

1. Web Config'e erişin ve sonra **Export and Import Setting Value** > **Export** öğesini seçin.
2. Dışa aktarmak istediğiniz ayarları seçin.

   Dışa aktarmak istediğiniz ayarları seçin. Ana kategoriyi seçerseniz alt kategoriler de seçilir. Ancak, aynı ağ içinde yinelemeden dolayı (IP adresleri gibi) hatalara neden olan alt kategoriler seçilemez.
3. Dışa aktarılan dosyayı şifrelemek için bir şifre girin.

   Dosyayı içe aktarmak için şifreye gereksiniminiz vardır. Dosyayı şifrelemek istemezseniz bunu boş bırakın.
4. **Export** öğesine tıklayın.

> ***Önemli:***
>
> *Tarayıcının, tarayıcı adı ve IP adresi gibi ağ ayarlarını dışa aktarmak isterseniz,* ***Enable to select the individual settings of device*** *ayarını ve daha fazla öğeyi seçin. Yedek tarayıcı için yalnızca seçilen değerleri kullanın.*

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Ayarları içe aktarın

Dışa aktarılan Web Config dosyasını tarayıcıya içe aktarın.

> ***Önemli:***
>
> *Tarayıcı adı veya IP adresi gibi bağımsız bilgiler içeren değerleri içe aktarırken, aynı ağda aynı IP adresinin olmadığından emin olun. IP adresi çakışırsa, tarayıcı değeri yansıtmaz.*

1. Web Config'e erişin ve sonra **Export and Import Setting Value** > **Import** öğesini seçin.
2. Dışa aktarılan dosyayı seçip şifreleme şifresini girin.
3. **Next** öğesine tıklayın.
4. Almak istediğiniz ayarları seçin ve sonra **Next** öğesine tıklayın.
5. **OK** öğesine tıklayın.

Ayarlar tarayıcıya uygulanır.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Sorunların Çözümleri

Sorunları Çözmek için İpuçları

Aşağıdaki kılavuzda daha fazla bilgi bulabilirsiniz.

❏ Kullanım Kılavuzu

Tarayıcının kullanımı, bakımı ve sorunların çözümü hakkında talimatlar sağlar.

Sunucu ve Ağ Aygıtı İçin Günlüğü Kontrol Etme

Ağ bağlantısında sorun olduğunda, posta sunucusu, LDAP sunucusu vb.'nin günlüğünü onaylayarak, ağ günlüğünü kullanarak, yönlendiriciler gibi sistem ekipmanı günlük ve komutlarının durumunu kontrol ederek nedeni belirlemeniz mümkündür.

Ağ Ayarlarını İlkleme

Kontrol Panelinden Ağ Ayarlarını Geri Yükleme

Tüm ağ ayarlarını varsayılanlarına geri yükleyebilirsiniz.

1. Ana ekranda **Ayarlar** öğesine dokunun.
2. **Sistem Yöneticisi** > **Varsayılan Ayarları Geri Yükle** > **Ağ Ayarları** öğesine dokunun.
3. Mesajı kontrol edin ve sonra **Evet** öğesine dokunun.
4. Bir tamamlama mesajı görüntülendiğinde, **Kapat** öğesine dokunun.

   Kapat düğmesine dokunmazsanız belirli bir süreden sonra ekran otomatik kapanır.

Aygıtlar ve Bilgisayarlar Arasında İletişimi Kontrol Etme

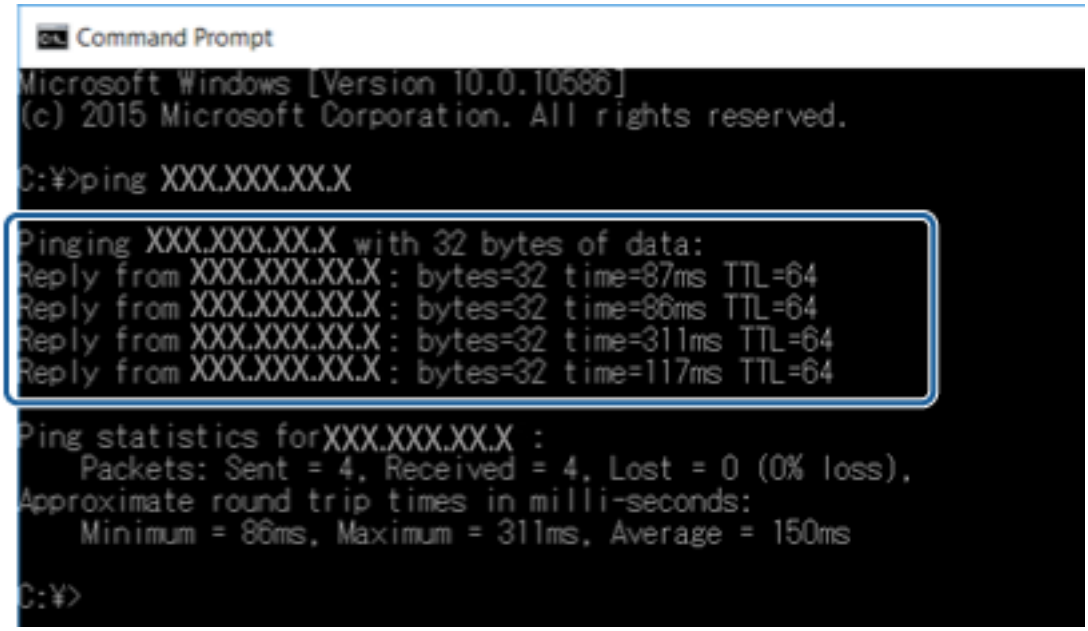
Ping Komutu Kullanarak Bağlantıyı Kontrol Etme — Windows

Bilgisayarın tarayıcıya bağlı olduğundan emin olmak için bir Ping komutu kullanabilirsiniz. Bir Ping komutu kullanarak bağlantıyı kontrol etmek için aşağıdaki adımları izleyin.

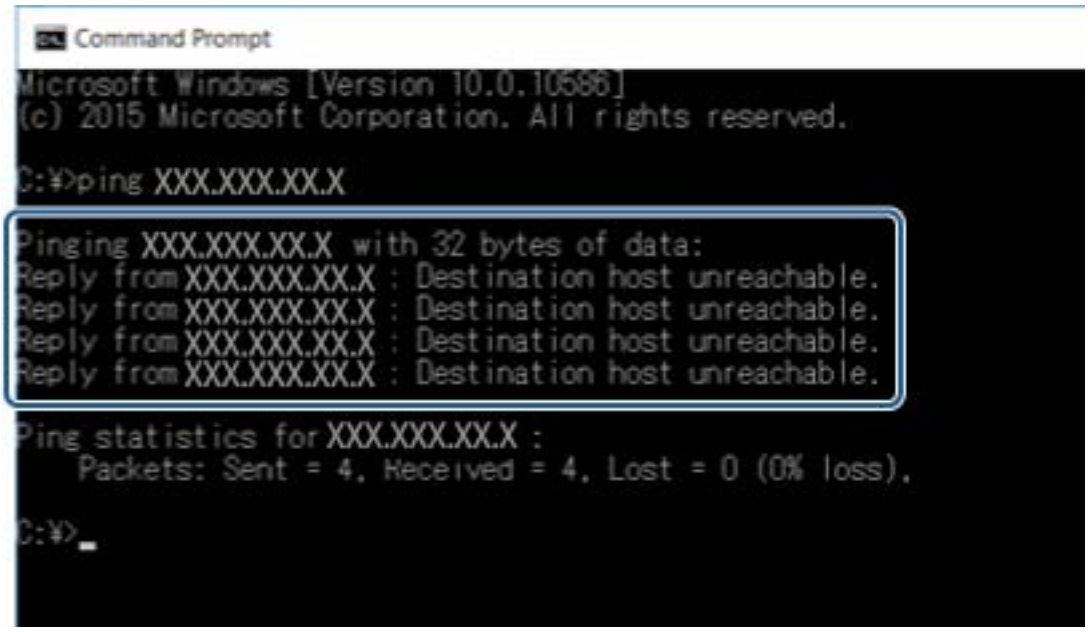
1. Kontrol etmek istediğiniz bağlantı için tarayıcının IP adresini işaretleyin.

   Bunu Epson Scan 2'yi kullanarak kontrol edebilirsiniz.

2. Bilgisayarın komut istemi ekranını görüntüleyin.
   - ❏ Windows 10
     Başlangıç düğmesini sağ tıklatın veya basılı tutun ve sonra **Komut İstemi**'ni seçin.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Uygulama ekranını görüntüleyin ve sonra **Komut İstemi** öğesini seçin.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 veya öncesi
     Başlat düğmesini tıklatın, **Tüm Programlar** veya **Programlar** > **Aksesuarlar** > **Komut İstemi**'ni seçin.
3. "ping xxx.xxx.xxx.xxx" yazın ve sonra Enter tuşuna basın.
   xxx.xxx.xxx.xxx için tarayıcının IP adresini girin.
4. İletişim durumunu kontrol edin.
   Tarayıcı ve bilgisayar iletişim halindeyse, aşağıdaki mesaj görüntülenir.



Tarayıcı ve bilgisayar iletişim halinde değilse, aşağıdaki mesaj görüntülenir.



Ping Komutu Kullanarak Bağlantıyı Kontrol Etme — Mac OS

Bilgisayarın tarayıcıya bağlı olduğundan emin olmak için bir Ping komutu kullanabilirsiniz. Bir Ping komutu kullanarak bağlantıyı kontrol etmek için aşağıdaki adımları izleyin.

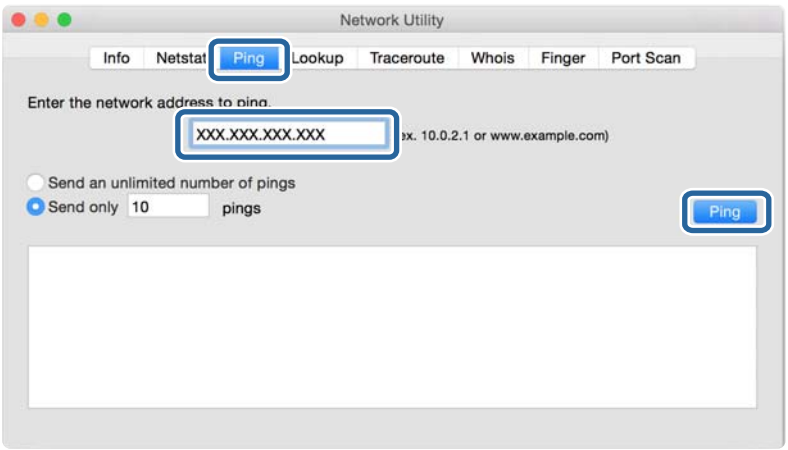
1. Kontrol etmek istediğiniz bağlantı için tarayıcının IP adresini işaretleyin.

   Bunu Epson Scan 2'yi kullanarak kontrol edebilirsiniz.

2. Ağ Yardımcı Programını çalıştırın.

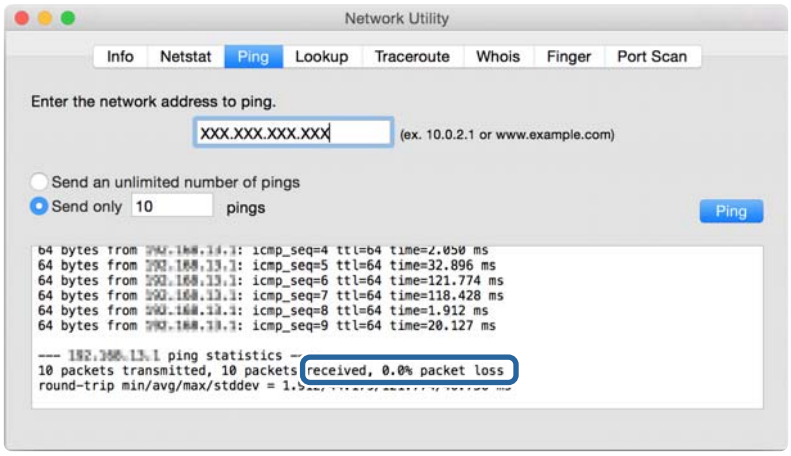
   Spotlight'nda "Ağ Yardımcı Programı" girin.

3. **Ping** sekmesini tıklatın, adım 1'de işaretlediğiniz IP adresini girin ve sonra **Ping**'i tıklatın.

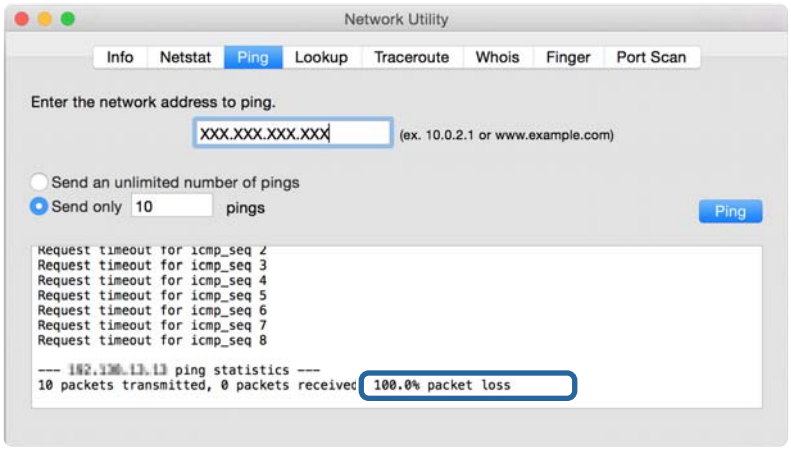


4. İletişim durumunu kontrol edin.

   Tarayıcı ve bilgisayar iletişim halindeyse, aşağıdaki mesaj görüntülenir.



   Tarayıcı ve bilgisayar iletişim halinde değilse, aşağıdaki mesaj görüntülenir.



Ağ Yazılımı Kullanımı Sorunları

Web Config'e Erişemiyorum

Tarayıcının IP adresi doğru yapılandırıldı mı?

Epson Device Admin veya EpsonNet Config'yi kullanarak IP adresini yapılandırın.

Web tarayıcınız SSL/TLS için Encryption Strength için toplu şifrelemeleri destekliyor mu?

SSL/TLS için Encryption Strength için toplu şifrelemeler şu şekildedir. Web Config'e yalnızca aşağıdaki toplu şifrelemeleri destekleyen bir web tarayıcısında erişilebilir. Tarayıcınızın şifreleme desteğini kontrol edin.

❏ 80 bit: AES256/AES128/3DES

❏ 112 bit: AES256/AES128/3DES

❏ 128 bit: AES256/AES128

❏ 192 bit: AES256

❏ 256 bit: AES256

SSL iletişimi (https) kullanan Web Config'e erişim sırasında "Süre doldu" mesajı beliriyor.

Sertifika süre aşımına uğradıysa tekrar sertifika alın. Süre aşımı tarihinden önce bu mesaj beliriyorsa tarayıcının tarih ayarının doğru yapılandırıldığından emin olun.

SSL iletişimi (https) kullanan Web Config'e erişim sırasında "Güvenlik sertifikası ismi ... ile eşleşmiyor" mesajı beliriyor.

Kendinden imzalı sertifika oluşturmak amacıyla **Common Name** için girilen tarayıcı IP adresi ya da CSR web tarayıcısına girilen adres ile eşleşmiyor. Tekrar bir sertifika alın ve içe aktarın ya da tarayıcı ismini değiştirin.

Bir proxy sunucu üzerinden tarayıcıya erişim gerçekleşiyor.

Tarayıcınızda bir proxy sunucu kullanıyorsanız, web tarayıcınızın proxy ayarlarını yapılandırmanız gerekir.

❏ Windows:

Kontrol Paneli > **Ağ ve Internet** > **Internet Seçenekleri** > **Bağlantılar** > **LAN ayarları** > **Proxy sunucusu** öğesini seçin ve ardından yerel adresler için proxy sunucusu kullanmamak üzere yapılandırın.

❏ Mac OS:

Sistem Tercihleri > **Ağ** > **İleri Düzey** > **Proxy** öğesini seçin ve ardından **Şu Ana Bilgisayarlar ve Etki Alanları için proxy ayarlarını atla** için yerel adresi kaydedin.

Örnek:

192.168.1.*: Yerel adres 192.168.1.XXX, alt ağ maskesi 255.255.255.0

192.168.*.*: Yerel adres 192.168.XXX.XXX, alt ağ maskesi 255.255.0.0

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "IP Adresi Atama" sayfa 15

➡ "EpsonNet Config'i Kullanarak Bir IP Adresi Atama" sayfa 56

Model adı ve/veya IP adresi EpsonNet Config üzerinde görüntülenmiyor

Windows güvenlik ekranı ya da güvenlik duvarı görüntülendiğinde, Engelle, İptal et, veya Kapat öğelerini mi seçtiniz?

Engelle, **İptal et** veya **Kapat** seçeneklerinden birini seçtiyseniz, IP adresi ve model ismi EpsonNet Config ya da EpsonNet Setup üzerinde görüntülenmez.

Bunu düzeltmek için Windows güvenlik duvarını ve ticari güvenlik yazılımını kullanarak EpsonNet Config yazılımını bir istisna olarak kaydedin. Bir anti-virüs ya da güvenlik programı kullanıyorsanız, kapatın ve ardından EpsonNet Config yazılımını kullanmayı deneyin.

İletişim hatası süre aşımı ayarı çok mu kısa?

EpsonNet Config yazılımını çalıştırın ve **Tools** > **Options** > **Timeout** öğesini seçin ve ardından **Communication Error** ayarı için süre uzunluğunu arttırın. Bu işlem yüzünden EpsonNet Config yazılımının daha yavaş çalışabileceğini dikkate alın.

İlgili Bilgi

➡ "EpsonNet Config — Windows Çalıştırma" sayfa 56

➡ "EpsonNet Config — Mac OS Çalıştırma" sayfa 56

Ek

Ağ Yazılımına Giriş

Aşağıda aygıtları yapılandıran ve yöneten yazılım açıklanmaktadır.

Epson Device Admin

Epson Device Admin ağda aygıtları yüklemenizi ve sonra aygıtları yapılandırmanızı ve yönetmenizi sağlayan bir uygulamadır. Aygıtlar için durum ve sarf malzemeleri gibi ayrıntılı bilgileri alabilir, uyarı bildirimleri gönderebilir ve aygıt kullanımı için raporlar oluşturabilirsiniz. Ayar öğelerini içeren bir şablon da yapabilir ve onu paylaşılan ayarlar olarak diğer aygıtlara uygulayabilirsiniz. Epson Device Admin uygulamasını Epson destek web sitesinden indirebilirsiniz. Daha fazla bilgi için Epson Device Admin belgesine ya da yardıma başvurun.

Epson Device Admin'i Çalıştırma (yalnızca Windows)

Tüm Programlar > **EPSON** > **Epson Device Admin** > **Epson Device Admin** öğesini seçin.

Not:
Güvenlik duvarı uyarısı görünürse Epson Device Admin erişimine izin verin.

EpsonNet Config

EpsonNet Config sayesinde yönetici tarayıcının ağ ayarlarını yapılandırabilir; örneğin, IP adresi atayabilir ve bağlantı modunu değiştirebilir. Toplu ayar özelliği Windows'da desteklenir. Daha fazla bilgi için EpsonNet Config belgesine ya da yardıma başvurun.

EpsonNet Config — Windows Çalıştırma

Tüm Programlar > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config** öğesini seçin.

Not:
Güvenlik duvarı uyarısı görünürse EpsonNet Config erişimine izin verin.

EpsonNet Config — Mac OS Çalıştırma

Git > **Uygulamalar** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config** öğesini seçin.

EpsonNet SetupManager

EpsonNet SetupManager, tarayıcı sürücüsünü kurma ve yapılandırma ve Document Capture Pro'yu kurma gibi basit tarayıcı kurulumu için bir paket oluşturmak için bir yazılımdır. Bu yazılım sayesinde yönetici benzersiz yazılım paketleri oluşturabilir ve gruplar arasında dağıtabilir.

Daha fazla bilgi için, bölgeniz için olan Epson web sitesini ziyaret edin.

EpsonNet Config'i Kullanarak Bir IP Adresi Atama

Bir IP adresini tarayıcıya EpsonNet Config'i kullanarak atayabilirsiniz. EpsonNet Config, Ethernet kablosu kullanarak bağlandıktan sonra tarayıcıya bir IP adresi atamanızı sağlar.

Toplu Ayarları Kullanarak IP Adresini Atama

Toplu Ayarlar İçin Dosya Oluşturma

Anahtarlarınız olarak MAC adresini ve model adını kullanarak IP adresini ayarlamak için yeni bir SYLK dosyası oluşturabilirsiniz.

1. Bir çalışma sayfası uygulaması (Microsoft Excel gibi) veya bir metin düzenleyiciyi açın.
2. Ayar öğesi adları olarak ilk satıra “Info_MACAddress”, “Info_ModelName” ve “TCPIP_IPAddress” girin.

   Aşağıdaki metin dizeleri için öğe adlarını girin. Büyük harf/küçük harf ve çift baytlı/tek baytlı karakterler arasında ayrım yapmak için yalnızca bir karakter farklıysa öğe tanınacaktır.

   Aşağıda açıklanan ayar öğesi adını girin; aksi halde, EpsonNet Config ayar öğelerini hatırlayamaz.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Her ağ arayüzü için MAC adresi, model adı ve IP adresini girin.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102

0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Bir ad girin ve SYLK dosyası (*.slk) olarak kaydedin.

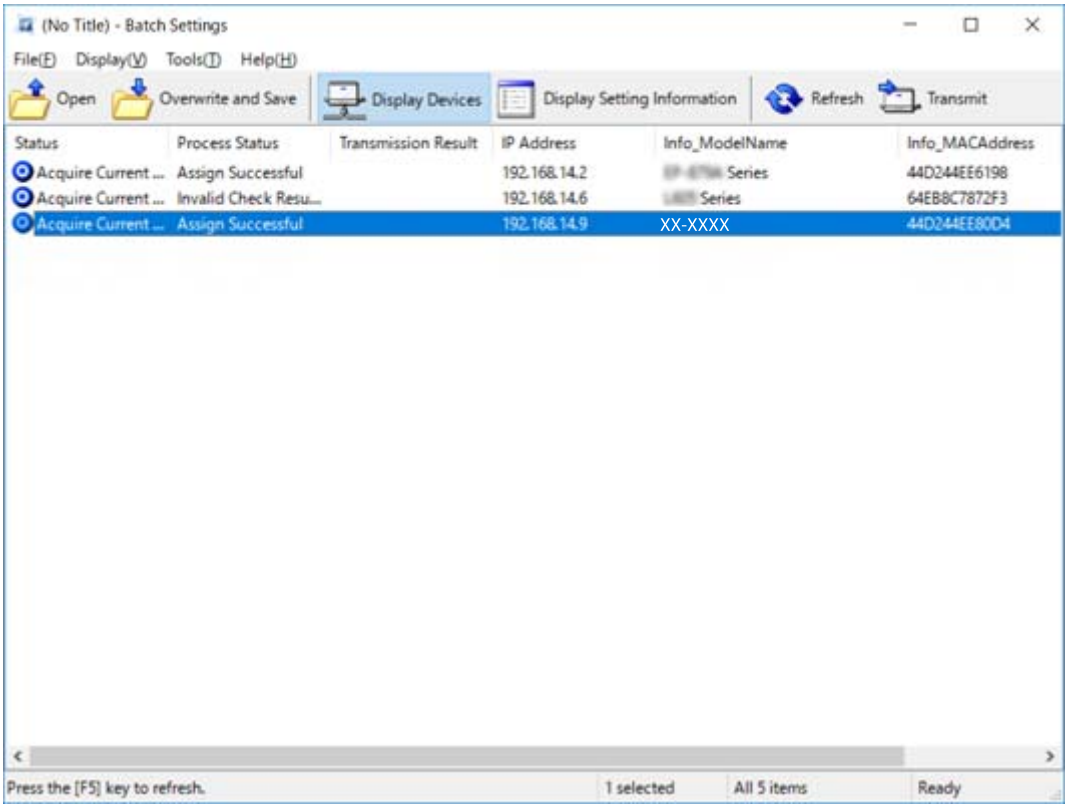
Yapılandırma Dosyasını Kullanarak Toplu Ayarlar Yapma

Yapılandırma dosyasında (SYLK dosyası) bir kez IP adreslerini atayın. Atamadan önce yapılandırma dosyasını oluşturmanız gerekir.

1. Ethernet kabloları kullanarak tüm aygıtları ağa bağlayın.
2. Tarayıcıyı açın.
3. EpsonNet Config öğesini başlatın.

   Ağdaki tarayıcıların listesi görüntülenir. Görüntülenmeleri biraz zaman alabilir.
4. **Tools** > **Batch Settings** öğesine tıklayın.
5. **Open** öğesine tıklayın.
6. Dosya seçim ekranında, ayarları içeren SYLK dosyasını (*.slk) seçin ve sonra **Open** öğesine tıklayın.
7. **Status** sütununu **Unassigned** olarak ayarlayarak ve **Process Status** öğesini **Assign Successful** olarak ayarlayarak toplu ayarlar gerçekleştirmek istediğiniz aygıtları seçin.

   Birden fazla seçim yaparken Ctrl veya Shift tuşlarına basın ve farenize tıklayın veya sürükleyin.



8. **Transmit** öğesine tıklayın.

9. Parola giriş ekranı görüntülendiğinde, parolayı girin ve sonra **OK** öğesine tıklayın.

   Ayarları iletin.

   Not:
   Bilgi, ilerleme göstergesi bitene kadar ağ arayüzüne iletilir. Aygıtı veya kablosuz adaptörü kapatmayın ve aygıta veri göndermeyin.

10. **Transmitting Settings** ekranında, **OK** öğesine tıklayın.

11. Ayarladığınız aygıtın durumunu kontrol edin.

    veya gösteren aygıtlar için ayarlar dosyasının içeriğini veya aygıtın normal yeniden başlatılıp başlatılmadığını kontrol edin.

Simge	Status	Process Status	Açıklama
	Setup Complete	Setup Successful	Kurulum normal tamamlandı.
	Setup Complete	Rebooting	Bilgi iletildiğinde, ayarları etkinleştirmek için her aygıtın yeniden başlatılması gerekir. Yeniden başlattıktan sonra aygıtın bağlanabilip bağlanamadığını belirlemek için bir kontrol gerçekleştirilir.
	Setup Complete	Reboot Failed	İletim ayarlarından sonra aygıt onaylanamıyor. Aygıtın açık olup olmadığını veya normal olarak yeniden başlatılıp başlatılmadığını kontrol edin.
	Setup Complete	Searching	Ayarlar dosyasında gösterilen aygıt aranıyor.*
	Setup Complete	Search Failed	Önceden kurulu olmayan aygıtlar kontrol edilemiyor. Aygıtın açık olup olmadığını veya normal olarak yeniden başlatılıp başlatılmadığını kontrol edin.*

* Yalnızca ayar bilgileri görüntülendiğinde.

İlgili Bilgi

➡ “EpsonNet Config — Windows Çalıştırma” sayfa 56
➡ “EpsonNet Config — Mac OS Çalıştırma” sayfa 56

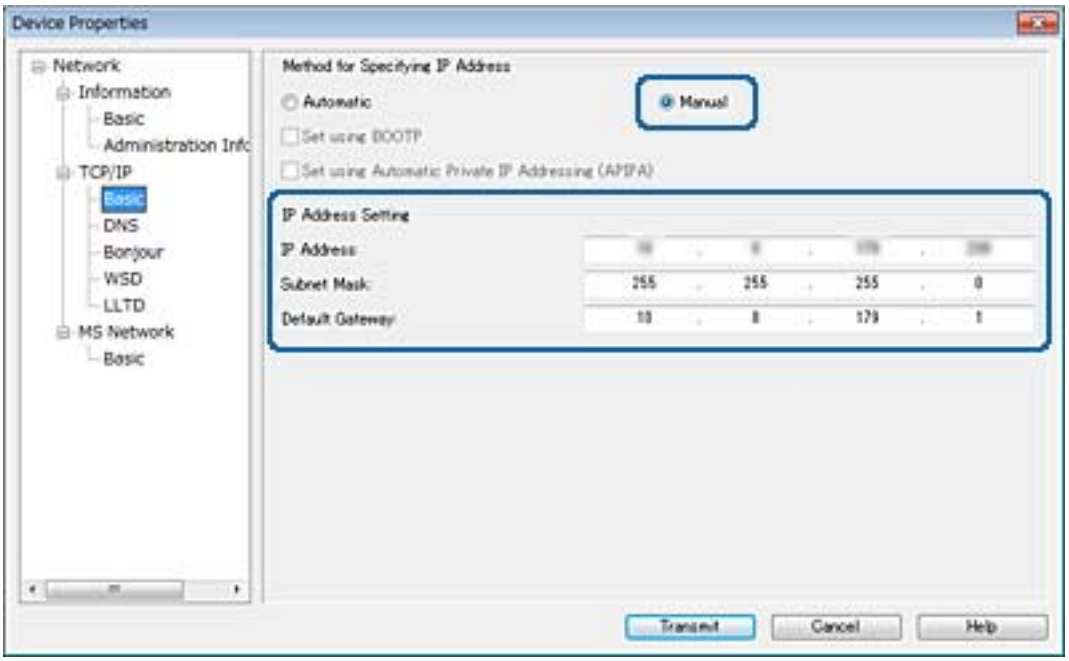
Her Cihaza IP Adresi Atama

Tarayıcıya EpsonNet Config'i kullanarak bir IP adresi atayın.

1. Tarayıcıyı açın.
2. Bir Ethernet kablosu kullanarak tarayıcıyı ağa bağlayın.
3. EpsonNet Config öğesini başlatın.

   Ağdaki tarayıcıların listesi görüntülenir. Görüntülenmeleri biraz zaman alabilir.
4. Atamak istediğiniz tarayıcıya çift tıklayın.

   Not:
   Aynı modelde birden fazla tarayıcıyı bağlarsanız, MAC adresini kullanarak tarayıcıyı tanımlayabilirsiniz.
5. **Network** > **TCP/IP** > **Basic** öğesini seçin.
6. **IP Address**, **Subnet Mask** ve **Default Gateway** için adresleri girin.



   Not:
   Tarayıcıyı güvenli bir ağa bağlarken statik bir adres girin.
7. **Transmit** öğesine tıklayın.

   Bilgilerin iletildiğini onaylayan ekran görüntülenir.
8. **OK** öğesine tıklayın.

   İletim tamamlandı ekranı görüntülenir.

   Not:
   Bilgi aygıta iletilir ve sonra "Yapılandırma başarıyla tamamlandı." mesajı görüntülenir. Aygıtı kapatmayın ve hizmete veri göndermeyin.
9. **OK** öğesine tıklayın.

İlgili Bilgi

➡ "EpsonNet Config — Windows Çalıştırma" sayfa 56

➡ "EpsonNet Config — Mac OS Çalıştırma" sayfa 56

Tarayıcı İçin Bağlantı Noktasını Kullanma

Tarayıcı aşağıdaki bağlantı noktasını kullanır. Bu bağlantı noktalarının gerektiğinde ağ yöneticisi tarafından kullanılabilir olmasına izin verilmelidir.

Gönderen (İstemci)	Kullanın	Hedef (Sunucu)	İletişim Kuralı	Bağlantı Noktası Numarası
Tarayıcı	E-posta gönderme (E-posta bildirimi)	SMTP sunucusu	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	SMTP'den önce POP bağlantısı (E-posta bildirimi)	POP sunucusu	POP3 (TCP)	110
	Kontrol WSD	İstemci bilgisayarı	WSD (TCP)	5357
	Document Capture Pro'dan itmeli tarama yaparken bilgisayarı arayın	İstemci bilgisayarı	Ağdan İtmeli Tarama Bulma	2968
	Document Capture Pro'dan itme tarama yaparken iş bilgilerini toplama	İstemci bilgisayarı	Ağdan İtmeli Tarama	2968
İstemci Bilgisayarı	Tarayıcı EpsonNet Config ve tarayıcı sürücüsü gibi bir uygulamadan bulun.	Tarayıcı	ENPC (UDP)	3289
	MIB bilgilerini EpsonNet Config ve tarayıcı sürücüsü gibi bir uygulamadan toplayın ve ayarlayın.	Tarayıcı	SNMP (UDP)	161
	WSD tarayıcısını arama	Tarayıcı	WS-Bulma (UDP)	3702
	Document Capture Pro'dan tarama verilerini iletme	Tarayıcı	Ağdan Tarama (TCP)	1865

Kuruluş için Gelişmiş Güvenlik Ayarları

Bu bölümde gelişmiş güvenlik özelliklerini açıklıyoruz.

Güvenlik Ayarları ve Tehlikeyi Önleme

Aygıt bir ağa bağlandığında, aygıta uzak bir konumdan erişebilirsiniz. Ek olarak, çoğu insan çalışma etkinliğini ve rahatlığını iyileştirmeye yardımcı olan aygıtı paylaşabilir. Ancak, yasal olmayan erişim, yasal olmayan kullanım ve verilerde değiştirme gibi riskler artar. Aygıtı Internet'e erişebileceğiniz bir ortamda kullanırsanız, riskler daha da büyür.

Bu riskten kaçınmak için Epson aygıtlarının çok çeşitli güvenlik teknolojileri vardır.

Müşterinin ortam bilgileriyle oluşturulmuş ortam koşullarına göre aygıtı gerektiği gibi ayarlayın.

Ad	Özellik türü	Ayarlanacaklar	Korunacaklar
SSL/TLS iletişimi	Bilgisayarın ve aygıtın iletişim yolu SSL/TLS iletişimi kullanılarak korunur. Bir tarayıcı yoluyla iletişimin içeriği korunur.	Sunucu için bir CA (Sertifika Yetkilisi) tarafından aygıta imzalanan sertifika olan bir CA sertifikası ayarlayın.	Bilgi ayarlarının ve bilgisayardan tarayıcıya aktarılan verilerin içeriğinin sızıntısını önleyin. Aygıttan Internet'te Epson sunucusuna erişme de bellenim güncellemesini vb. kullanarak korunabilir.
IPsec/IP filtreleme	Belirli bir istemciden veya belirli bir türden verilerin bölünmesine ve kesilmesine izin vermeye ayarlayabilirsiniz. IPsec verileri IP paket birimleriyle (şifreleme ve kimlik doğrulama) koruduğundan, güvenli olmayan tarama protokolüyle güvenli bir şekilde iletişim kurabilirsiniz.	Aygıta erişebilen istemciyi veya veri türünü ayarlamak için temel bir ilke ve özel ilke oluşturun.	Yetkisiz erişime ve değiştirmeye ve iletişim verilerinin aygıtı kesmesine karşı koruyun.
SNMPv3	Ağda bağlı aygıtları izleme, kontrol etmek için verilerin SNMP protokolüne entegrasyonu, şifreleme, kullanıcı kimliği doğrulama vb. gibi özellikler eklenmiştir.	SNMPv3'ü etkinleştirin, sonra kimlik doğrulama ve şifreleme yöntemini ayarlayın.	Durum izlemede gizli bir şekilde ayarları ağ yoluyla değiştirdiğinizden emin olun.
IEEE802.1X	Ethernet'te kimliği doğrulanmış yalnızca bir kullanıcının bağlanmasına izin verir. Yalnızca izin verilen bir kullanıcının aygıtı kullanmasına izin verir.	RADIUS sunucusuna kimlik doğrulama ayarı (kimlik doğrulama sunucusu).	Kimliği doğrulanmamış erişime ve aygıtın kullanılmasına karşı koruyun.

Ad	Özellik türü	Ayarlanacaklar	Korunacaklar
Kimlik kartını okuyun	Aygıtı bir kimlik kartını kimliği doğrulanmış bağlı aygıta tutarak kullanabilirsiniz. Her kullanıcı ve aygıt için günlük alımını ve aygıtların mevcut kullanımını ve her kullanıcının ve grubun kullanılabilir özelliklerini sınırlayabilir.	Bir kimlik doğrulama aygıtını aygıta bağlayın ve sonra kimlik doğrulama sisteminde bir kullanıcının bilgilerini ayarlayın.	Yetkisiz kullanımı ve aygıtın kötüye kullanımını önleyin.

İlgili Bilgi

➡ “Tarayıcıyla SSL/TLS İletişimi” sayfa 62
➡ “IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim” sayfa 70
➡ “SNMPv3 protokolünü kullanma” sayfa 82
➡ “Tarayıcıyı Bir IEEE802.1X Ağına Bağlama” sayfa 84

Güvenlik Özelliği Ayarları

IPsec/IP filtrelemeyi veya IEEE802.1X'i ayarlarken, değiştirme veya kesinti gibi güvenlik risklerini azaltmak için ayar bilgileri iletişimi kurmak için SSL/TLS'yi kullanarak Web Config'e erişmeniz önerilir.

Tarayıcıyla SSL/TLS İletişimi

Tarayıcıya SSL/TLS (Secure Sockets Layer (Güvenli Giriş Katmanı)/Transport Layer Security (Aktarım Katmanı Güvenliği)) iletişimi kullanılarak sunucu sertifikası ayarlandığında bilgisayarlar arasında iletişim yolunu şifreleyebilirsiniz. Bunu uzak ve yetkisiz erişimi önlemek istediğinizde yapın.

Dijital Sertifikasyon Hakkında

❏ CA tarafından imzalı sertifika

CA (Certificate Authority; Sertifika Yetkilisi) tarafından imzalı bir sertifika, sertifika yetkilisinden alınmalıdır. CA imzalı sertifika sayesinde iletişimlerin güvenliğinden emin olabilirsiniz. CA imzalı bir sertifikayı tüm güvenlik özelliklerine yönelik kullanabilirsiniz.

❏ CA sertifikası

Bir CA sertifikası, üçüncü bir tarafın sunucu kimliğini doğruladığını belirtir. Bu, güven ağı tarzı bir güvenlikte kilit bileşendir. Sunucu kimlik doğrulaması için CA sertifikası hazırlayan bir CA'dan bir CA sertifikası almalısınız.

❏ Kendinden imzalı sertifika

Kendinden imzalı sertifika, tarayıcının hazırladığı bir sertifikadır ve tarayıcı tarafından imzalanır. Bu sertifika güvenilir değildir ve sahte kimlik tehdidini önleyemez. Bu sertifikayı SSL/TLS sertifikası yerine kullanırsanız, web tarayıcısı bir güvenlik alarmı görüntüleyebilir. Bu sertifikayı sadece SSL/TLS iletişimi için kullanabilirsiniz.

İlgili Bilgi

➡ “CA İmzalı bir Sertifika Alma ve İçe Aktarma” sayfa 63

➡ “CA İmzalı bir Sertifika Silme” sayfa 66
➡ “Kendinden İmzalı Sertifika Güncelleme” sayfa 67

CA İmzalı bir Sertifika Alma ve İçe Aktarma

CA İmzalı bir Sertifika Alınması

CA imzalı bir sertifika almak için bir CSR (Sertifika İmzalama Talebi) oluşturun ve bununla sertifika yetkilisine başvurun. Web Config'i ve bir bilgisayarı kullanarak CSR oluşturabilirsiniz.

Web Config'i kullanarak bir CSR oluşturmak ve CA imzalı bir sertifika almak için aşağıdaki adımları izleyin. Web Config'i kullanarak CSR oluştururken, sertifika PEM/DER formatındadır.

1. Web Config'e erişin ve sonra **Network Security Settings** öğesini seçin. Sonra, **SSL/TLS** > **Certificate** veya **IPsec/IP Filtering** > **Client Certificate** veya **IEEE802.1X** > **Client Certificate** öğesini seçin.

2. **Generate CSR** öğesine tıklayın.

   CSR oluşturma sayfası açılır.

3. Her öğe için bir değer girin.

   Not:
   İzin verilen anahtar uzunluğu ve kısaltmalar sertifika yetkilisine bağlı olarak değişir. Her sertifika yetkilisinin kurallarına uygun talep hazırlayın.

4. **OK** öğesine tıklayın.

   Bir tamamlanma mesajı görüntülenir.

5. **Network Security Settings** öğesini seçin. Sonra, **SSL/TLS** > **Certificate** veya **IPsec/IP Filtering** > **Client Certificate** veya **IEEE802.1X** > **Client Certificate** öğesini seçin.

6. Her sertifika yetkilisinin belirlemiş olduğu formata uygun CSR'ı bilgisayarınıza indirmek için **CSR** indirme düğmelerinden birine tıklayın.

   > ***Önemli:***
   > *Tekrar bir CSR oluşturmayın. Bunu yaparsanız, verilen bir CA-signed Certificate içe aktarılamayabilir.*

7. Bir sertifika yetkilisine CSR'yi gönderin ve bir CA-signed Certificate alın.

   Her sertifika yetkilisinin gönderi yöntemi ve biçimi ile ilgili kurallarına uyun.

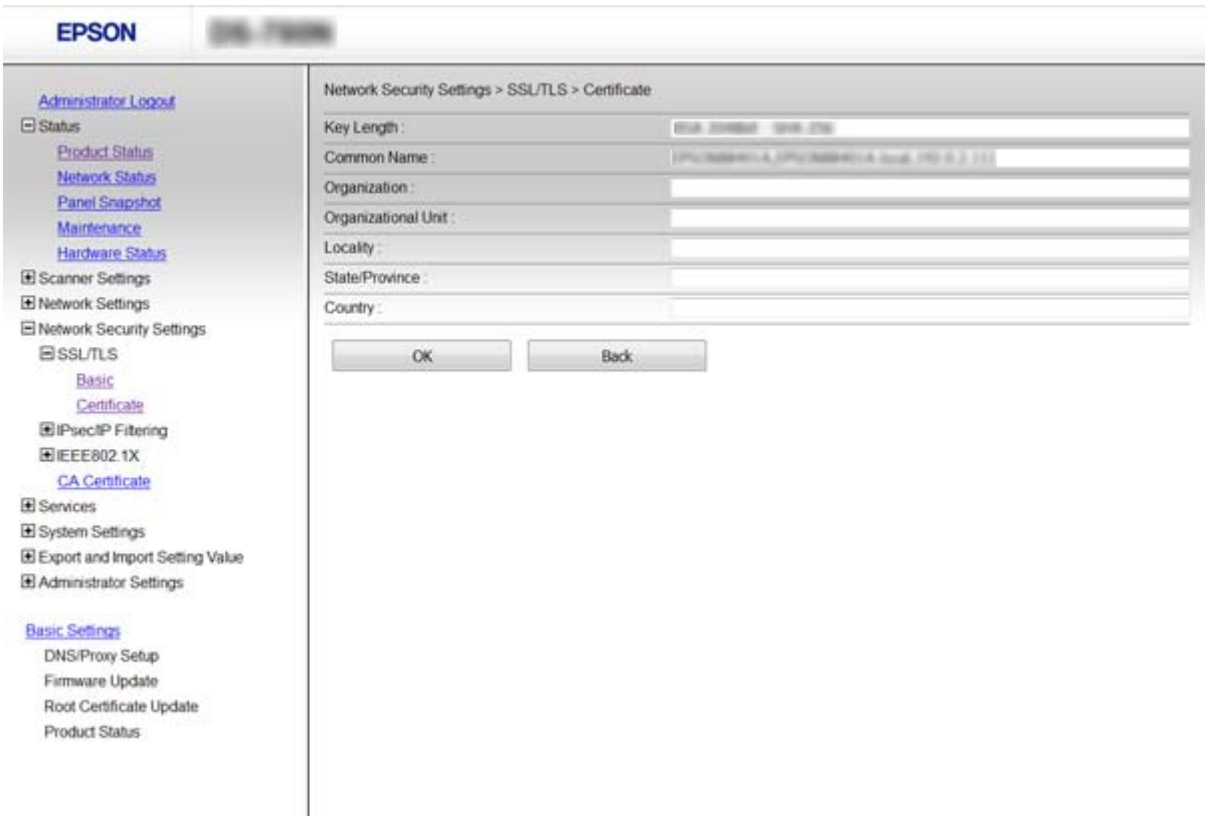
8. Verilen CA-signed Certificate öğesini tarayıcıya bağlı bir bilgisayara kaydedin.

   Sertifikayı bir hedefe kaydettiğinizde CA-signed Certificate alma işlemi tamamlanmış olur.

İlgili Bilgi

➡ “Web Config Erişimi” sayfa 23
➡ “CSR Ayarlama Öğeleri” sayfa 64
➡ “CA İmzalı bir Sertifikanın İçe Aktarımı” sayfa 64

CSR Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklamalar
Key Length	CSR için anahtar uzunluğu seçin.
Common Name	1 ve 128 karakter arası girebilirsiniz. Eğer bu bir IP adresi ise, sabit bir IP adresi olmalıdır. Örnek: Web Config erişimi için URL: https://10.152.12.225 Ortak isim: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	0 ve 64 karakter arası ASCII (0x20–0x7E) girebilirsiniz. Belirleyici isimleri virgüllerle ayırabilirsiniz.
Country	ISO-3166 tarafınca belirlenmiş iki haneli bir şehir kodu girin.

İlgili Bilgi

➡ “CA İmzalı bir Sertifika Alınması” sayfa 63

CA İmzalı bir Sertifikanın İçe Aktarımı

Önemli:

- ❏ *Tarayıcının saat ve tarih ayarının doğru olduğundan emin olun.*
- ❏ *Web Config tarafından hazırlanmış bir CSR kullanıyorsanız, her seferde bir adet sertifika içe aktarabilirsiniz.*

1. Web Config'e erişin ve sonra **Network Security Settings** öğesini seçin. Sonra, **SSL/TLS** > **Certificate** veya **IPsec/IP Filtering** > **Client Certificate** veya **IEEE802.1X** > **Client Certificate** öğesini seçin.
2. **Import** öğesine tıklayın.

   Sertifika içe aktarım sayfası açılır.
3. Her öğe için bir değer girin.

   Nerede CSR oluşturduğunuza ve sertifikanın dosya formatına bağlı olarak gerekli ayarlar değişebilir. Aşağıdakilere göre, değerleri gerekli öğelere girin.

   - ❏ Web Config'den alınmış PEM/DER formatında bir sertifika
     - ❏ **Private Key**: Tarayıcının özel bir anahtarı olduğu için yapılandırmayın.
     - ❏ **Password**: Yapılandırmayın.
     - ❏ **CA Certificate 1/CA Certificate 2**: İsteğe bağlı
   - ❏ Bilgisayardan alınmış, PEM/DER formatında bir sertifika
     - ❏ **Private Key**: Ayarlamanız gerekir.
     - ❏ **Password**: Yapılandırmayın.
     - ❏ **CA Certificate 1/CA Certificate 2**: İsteğe bağlı
   - ❏ Bilgisayardan alınmış, PKCS#12 formatında bir sertifika
     - ❏ **Private Key**: Yapılandırmayın.
     - ❏ **Password**: İsteğe bağlı
     - ❏ **CA Certificate 1/CA Certificate 2**: Yapılandırmayın.
4. **OK** öğesine tıklayın.

   Bir tamamlanma mesajı görüntülenir.

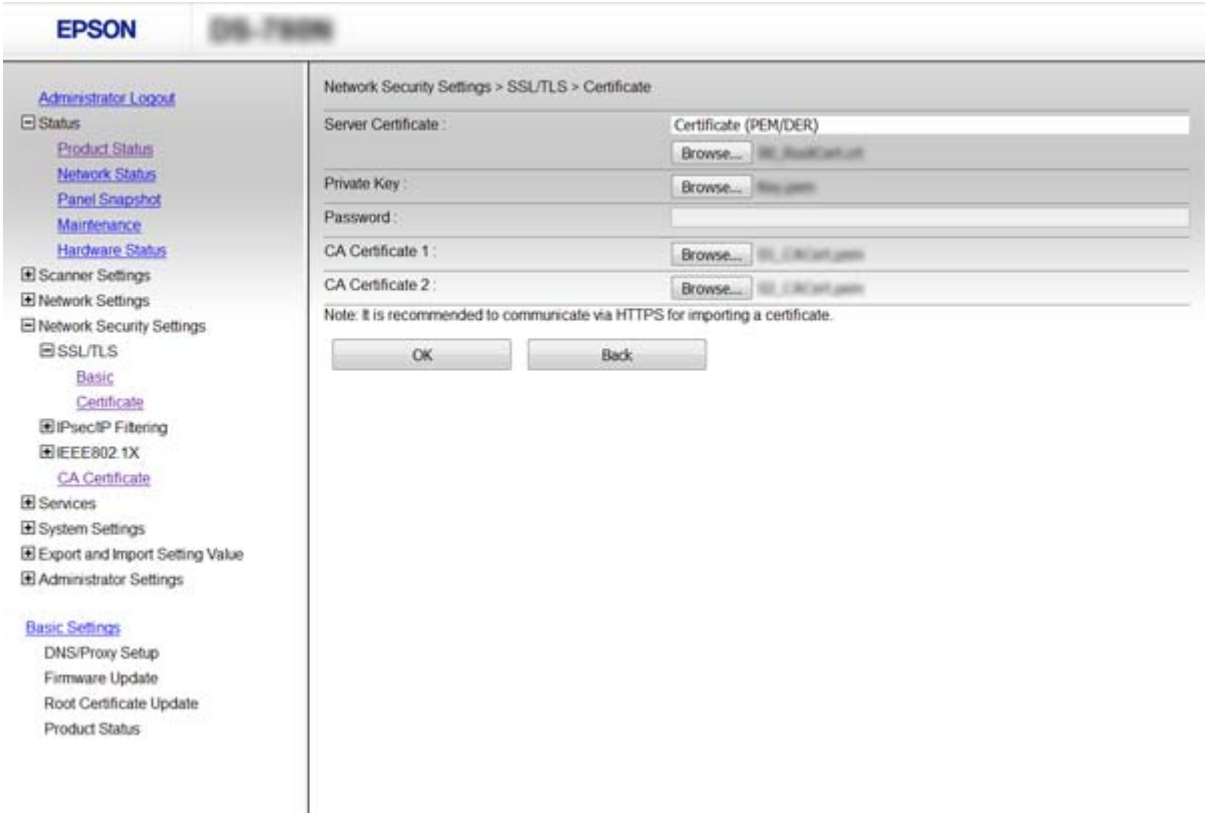
Not:
*Sertifika bilgisini doğrulamak için **Confirm** öğesine tıklayın.*

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "CA İmzalı Sertifika İçe Aktarım Ayarlama Öğeleri" sayfa 66

CA İmzalı Sertifika İçe Aktarım Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklama
Server Certificate veya Client Certificate	Bir sertifikanın formatını seçin.
Private Key	Bilgisayarda oluşturulmuş bir CSR kullanarak PEM/DER formatında bir sertifika alırsanız, sertifika ile eşleşen özel bir anahtar dosya belirleyin.
Password	Özel anahtarı korumak için bir şifre girin.
CA Certificate 1	Sertifikanız **Certificate (PEM/DER)** formatındaysa, sunucu sertifikası hazırlayan bir sertifika yetkilisinin sertifikasını içe aktarın. İsterseniz bir dosya belirleyin.
CA Certificate 2	Sertifikanız **Certificate (PEM/DER)** formatındaysa, **CA Certificate 1** hazırlayan bir sertifika yetkilisinin sertifikasını içe aktarın. İsterseniz bir dosya belirleyin.

İlgili Bilgi

➡ "CA İmzalı bir Sertifikanın İçe Aktarımı" sayfa 64

CA İmzalı bir Sertifika Silme

Sertifika zaman aşımına uğradığında ya da şifreli bir bağlantıya gerek kalmadığında önemli bir sertifikayı silebilirsiniz.

> ***Önemli:***
> *Web Config tarafından hazırlanmış bir CSR kullanıyorsanız, silinmiş bir sertifikayı tekrar içe aktaramazsınız. Bu durumda CSR oluşturun ve tekrar bir sertifika alın.*

1. Web Config'e erişin ve sonra **Network Security Settings** öğesini seçin. Sonra, **SSL/TLS** > **Certificate** veya **IPsec/IP Filtering** > **Client Certificate** veya **IEEE802.1X** > **Client Certificate** öğesini seçin.
2. **Delete** öğesine tıklayın.
3. Görüntülenen mesajda, sertifikayı silmek istediğinizi onaylayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Kendinden İmzalı Sertifika Güncelleme

Tarayıcı HTTPS sunucu özelliğini destekliyorsa, kendinden imzalı bir sertifika güncelleyebilirsiniz. Kendinden imzalı sertifika kullanan Web Config yazılımına erişim sağlarken bir uyarı mesajı belirir.

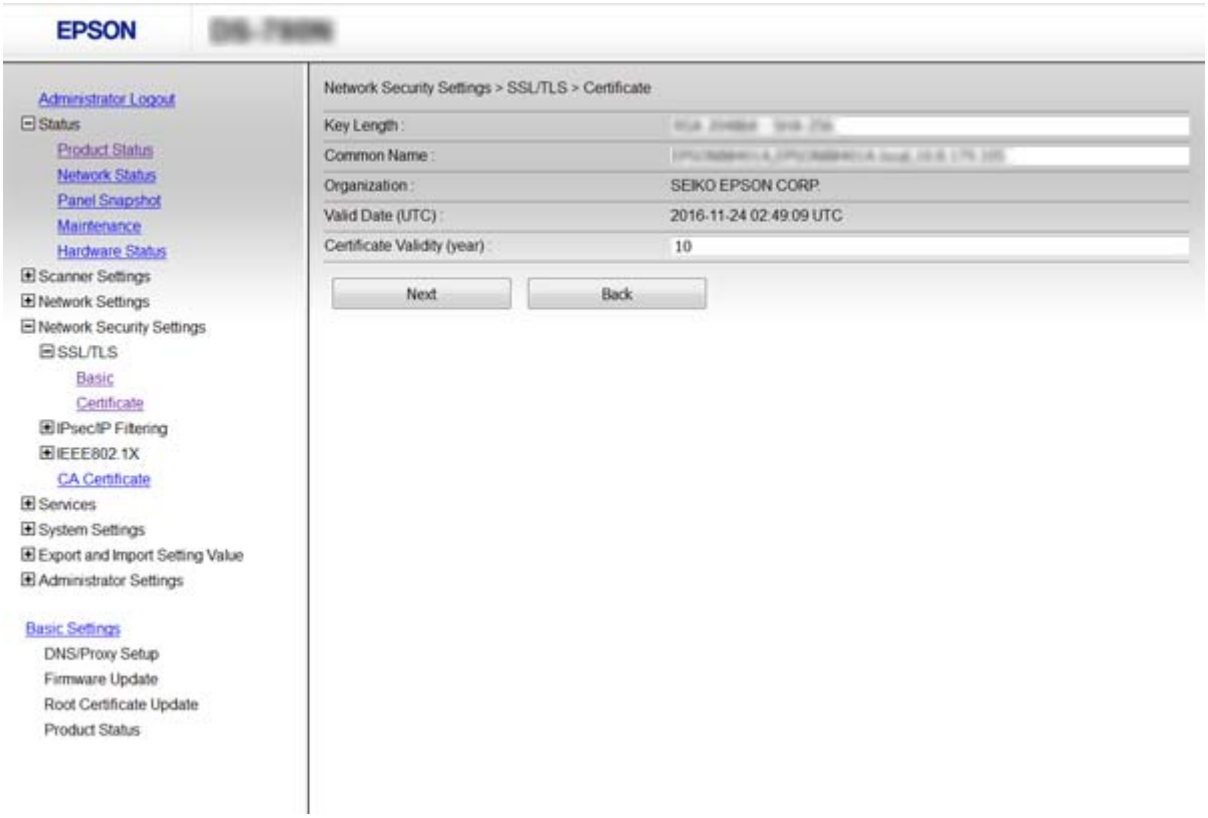
CA imzalı bir sertifika alana kadar geçici olarak kendinden imzalı bir sertifika kullanın.

1. Web Config'e erişin ve **Network Security Settings** > **SSL/TLS** > **Certificate** öğesini seçin.
2. **Update** öğesine tıklayın.
3. **Common Name** girin.

   Bir IP adresi ya da tarayıcı için FQDN ismi gibi kimlik ayırt etmeyi sağlayacak bir belirteç girin. 1 ve 128 karakter arası girebilirsiniz.

   Not:
   Belirleyici ismi (CN) virgülle ayırabilirsiniz.

4. Sertifika için bir geçerlilik süresi belirleyin.



5. **Next** öğesine tıklayın.

   Bir doğrulama mesajı görüntülenir.

6. **OK** öğesine tıklayın.

   Tarayıcı güncelleştirilmiştir.

Not:
*Sertifika bilgisini doğrulamak için **Confirm** öğesine tıklayın.*

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

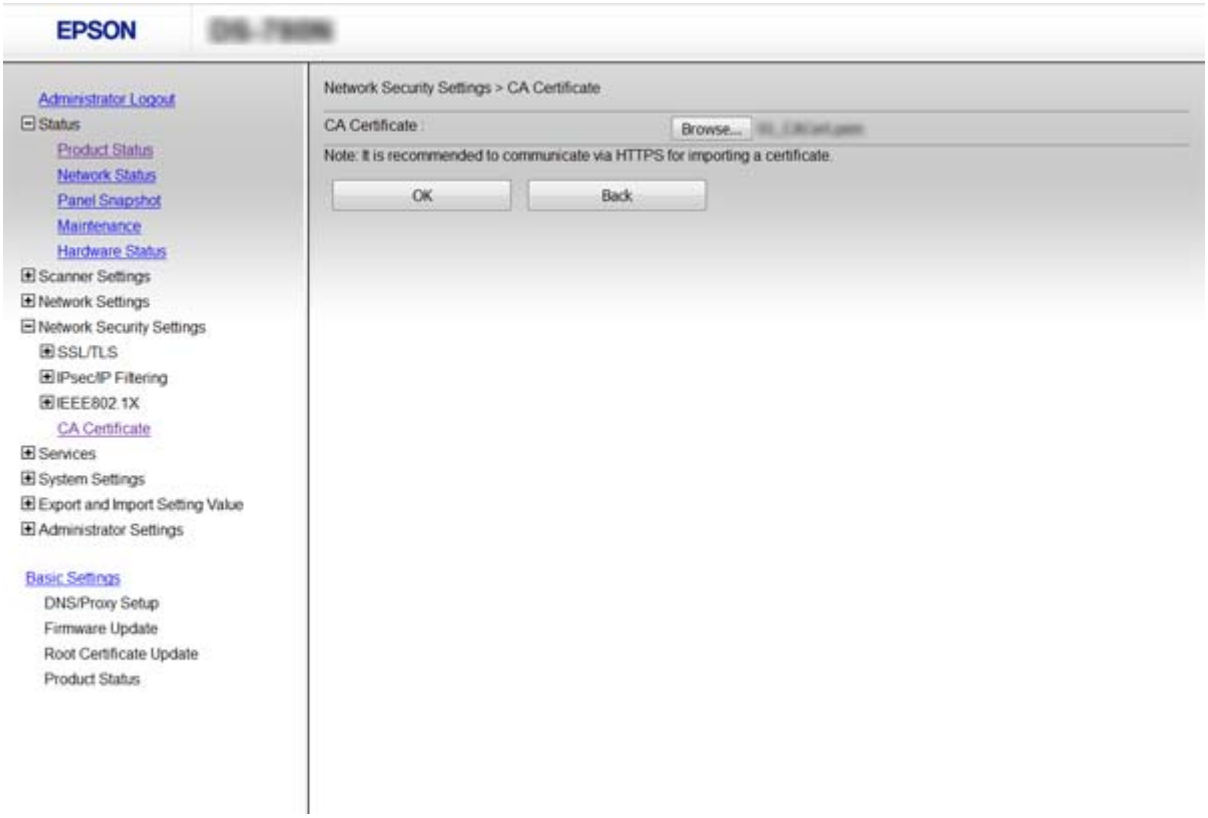
CA Certificate Yapılandırın

Bir CA Certificate öğesini içe aktarabilir, görüntüleyebilir ve silebilirsiniz.

Bir CA Certificate içe aktarma

1. Web Config'e erişin ve sonra **Network Security Settings** > **CA Certificate** öğesini seçin.
2. **Import** öğesine tıklayın.

3. İçe aktarmak istediğiniz CA Certificate öğesini belirleyin.



4. **OK** öğesine tıklayın.

İçe aktarma tamamlandığında **CA Certificate** ekranına döndürülürsünüz ve içe aktarılan CA Certificate görüntülenir.

İlgili Bilgi

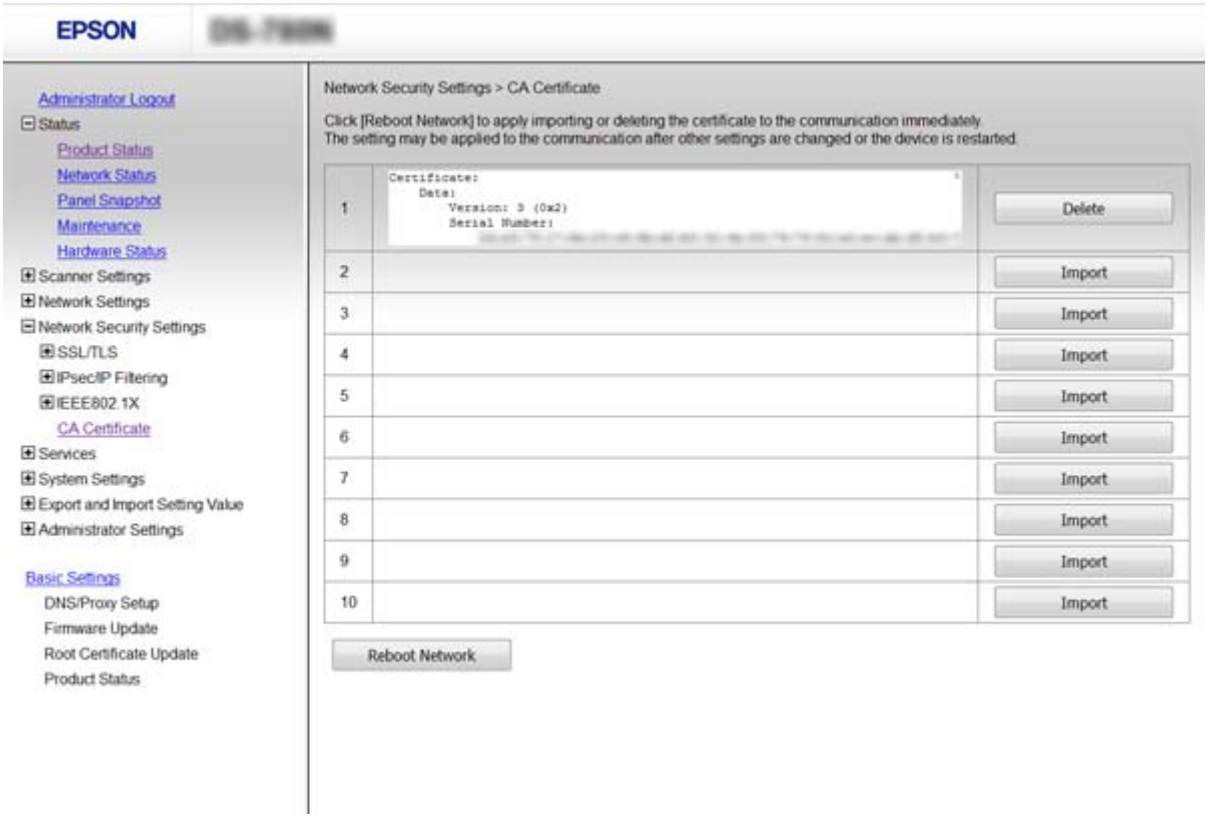
➡ "Web Config Erişimi" sayfa 23

Bir CA Certificate silme

İçe aktarılan CA Certificate öğesini silebilirsiniz.

1. Web Config'e erişin ve sonra **Network Security Settings** > **CA Certificate** öğesini seçin.

2. Silmek istediğiniz CA Certificate öğesinin yanındaki **Delete** düğmesine tıklayın.



3. Görüntülenen mesajda, sertifikayı silmek istediğinizi onaylayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim

IPsec/IP Filtering Hakkında

Tarayıcı IPsec/IP Filtrelemeyi destekliyorsa, IP adresleri, hizmetler ve bağlantı noktasına göre trafiği filtreleyebilirsiniz. Filtreleme özelliğini dahil ederek tarayıcıyı belirli müşterileri ve belirli verileri kabul edecek ya da engelleyecek şekilde yapılandırabilirsiniz. Ayrıca, IPsec kullanarak güvenlik seviyesini arttırabilirsiniz.

Trafiği filtrelemek için varsayılan ilkeyi yapılandırın. Varsayılan ilke, tarayıcıya bağlanan her kullanıcı veya grup için geçerlidir. Kullanıcılar ve kullanıcı gruplarına yönelik daha ayrıntılı kontrol için grup ilkeleri yapılandırın. Grup ilkesi, bir kullanıcı ya da kullanıcı grubu üzerinde geçerli olan, bir ya da daha fazla kuraldır. Tarayıcı, yapılandırılmış ilkelerle eşleşen IP paketlerini kontrol eder. IP paketleri 1 ila 10 adet grup ilkesi ve ardından bir varsayılan ilke seviyesinde kimlik denetiminden geçmiştir.

Not:
Windows Vista veya üstünü ya da Windows Server 2008 veya üstünü çalıştıran bilgisayarlar IPsec'i destekler.

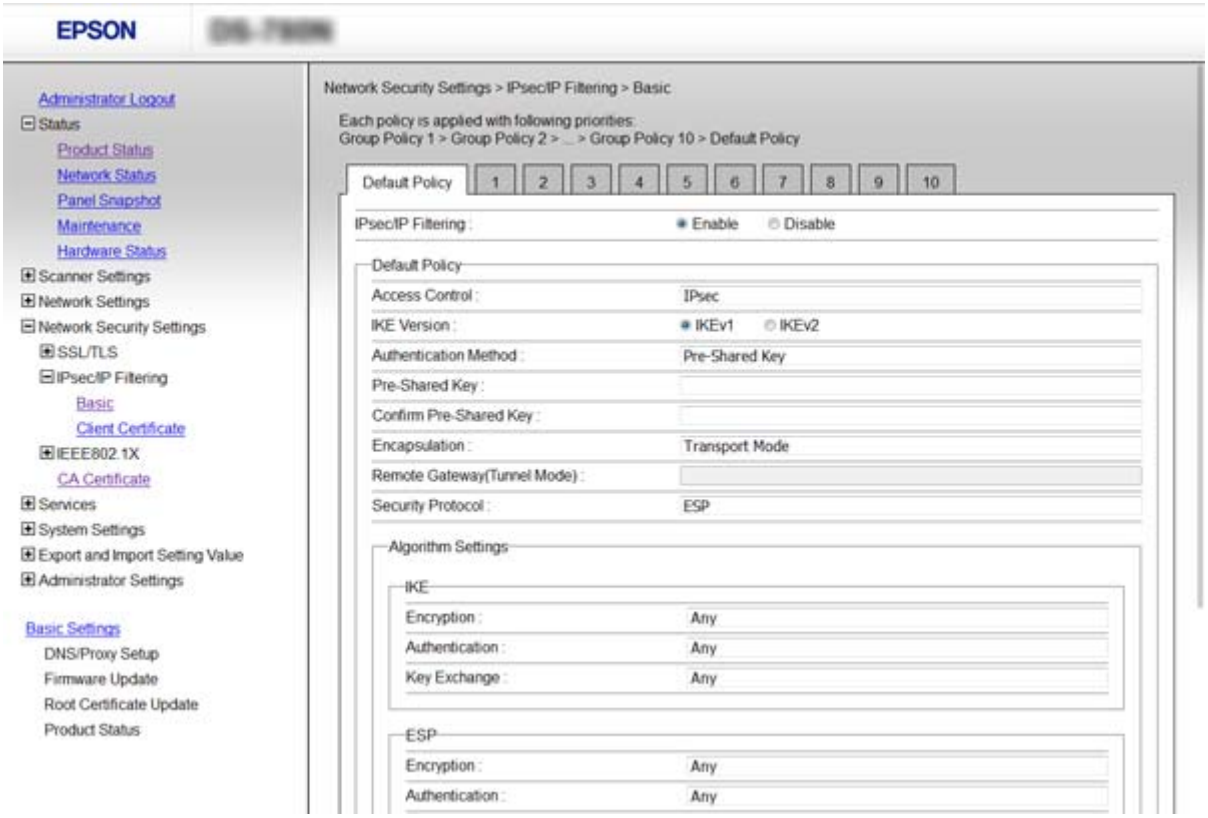
Default Policy Yapılandırma

1. Web Config'e erişin ve **Network Security Settings** > **IPsec/IP Filtering** > **Basic** öğesini seçin.
2. Her öğe için bir değer girin.
3. **Next** öğesine tıklayın.
   Bir doğrulama mesajı görüntülenir.
4. **OK** öğesine tıklayın.
   Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23
➡ "Default Policy Ayarlama Öğeleri" sayfa 71

Default Policy Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklamalar
IPsec/IP Filtering	IPsec/IP Filtre özelliğini etkinleştirebilir ya da devre dışı bırakabilirsiniz.

Kuruluş için Gelişmiş Güvenlik Ayarları

Öğeler	Ayarlar ve Açıklamalar	
Access Control	IP paketlerinin trafiği için bir kontrol yöntemi yapılandırın.	
	Permit Access	Yapılandırılmış IP paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
	Refuse Access	Yapılandırılmış IP paketlerinin düz geçişlerini reddetmek için bu öğeyi seçin.
	IPsec	Yapılandırılmış IPsec paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
IKE Version	IKE sürümü için IKEv1 veya IKEv2 öğesini seçin. Tarayıcının bağlı olduğu aygıta göre bunlardan birini seçin.	
IKEv1	**IKE Version** için **IKEv1** öğesini seçtiğinizde aşağıdaki öğeler görüntülenir.	
	Authentication Method	**Certificate** öğesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.
IKEv2	**IKE Version** için **IKEv2** öğesini seçtiğinizde aşağıdaki öğeler görüntülenir.	
Local	Authentication Method	**Certificate** öğesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
	ID Type	Tarayıcı için kimliğin türünü seçin.
	ID	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@", "#" ve "=" öğelerini kullanamazsınız. **Distinguished Name**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" öğesini eklemeniz gerekir. **IP Address**: IPv4 veya IPv6 biçimini girin. **FQDN**: A–Z, a–z, 0–9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. **Email Address**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" öğesini eklemeniz gerekir. **Key ID**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.

Kuruluş için Gelişmiş Güvenlik Ayarları

Öğeler	Ayarlar ve Açıklamalar	
Remote	Authentication Method	**Certificate** öğesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
	ID Type	Kimliğini doğrulamak istediğiniz aygıtın kimlik türünü seçin.
	ID	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@", "#" ve "=" öğelerini kullanamazsınız. **Distinguished Name**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" öğesini eklemeniz gerekir. **IP Address**: IPv4 veya IPv6 biçimini girin. **FQDN**: A–Z, a–z, 0–9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. **Email Address**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" öğesini eklemeniz gerekir. **Key ID**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.
Encapsulation	**IPsec** için **Access Control** öğesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.	
	Transport Mode	Aynı LAN üzerinde sadece tarayıcıyı kullanırsanız bu öğeyi seçin. Katman 4 ya da sonraki IP paketleri şifrelenmiştir.
	Tunnel Mode	Tarayıcıyı IPsec-VPN gibi Internet özellikli bir ağda kullanıyorsanız bu seçeneği seçin. IP paketlerinin başlıkları ve verileri şifrelenmiştir.
Remote Gateway(Tunnel Mode)	**Encapsulation** için **Tunnel Mode** öğesini seçerseniz, 1 ve 39 karakter arası bir ağ geçidi adresi girin.	
Security Protocol	**Access Control** için **IPsec**, bir seçenek seçin.	
	ESP	Kimlik doğrulama ve veri bütünlüğünü sağlamak ve veri şifrelemesi için bu öğeyi seçin.
	AH	Kimlik doğrulama ve veri bütünlüğünü sağlamak için bu öğeyi seçin. Veri şifrelemesi yasaklandığında bile IPsec kullanabilirsiniz.
Algorithm Settings		
IKE	Encryption	IKE için şifreleme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
	Authentication	IKE için kimlik doğrulama algoritmasını seçin.
	Key Exchange	IKE için anahtar değiştirme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.

Öğeler	Ayarlar ve Açıklamalar	
ESP	Encryption	ESP için şifreleme algoritmasını seçin. Bu, **ESP** öğesi **Security Protocol** için seçildiğinde kullanılabilir.
	Authentication	ESP için kimlik doğrulama algoritmasını seçin. Bu, **ESP** öğesi **Security Protocol** için seçildiğinde kullanılabilir.
AH	Authentication	AH için şifreleme algoritmasını seçin. Bu, **AH** öğesi **Security Protocol** için seçildiğinde kullanılabilir.

İlgili Bilgi

➡ "Default Policy Yapılandırma" sayfa 71

Group Policy Yapılandırma

1. Web Config'e erişin ve **Network Security Settings** > **IPsec/IP Filtering** > **Basic** öğesini seçin.
2. Yapılandırmak istediğiniz numaralandırılmış bir sekmeyi tıklatın.
3. Her öğe için bir değer girin.
4. **Next** öğesine tıklayın.

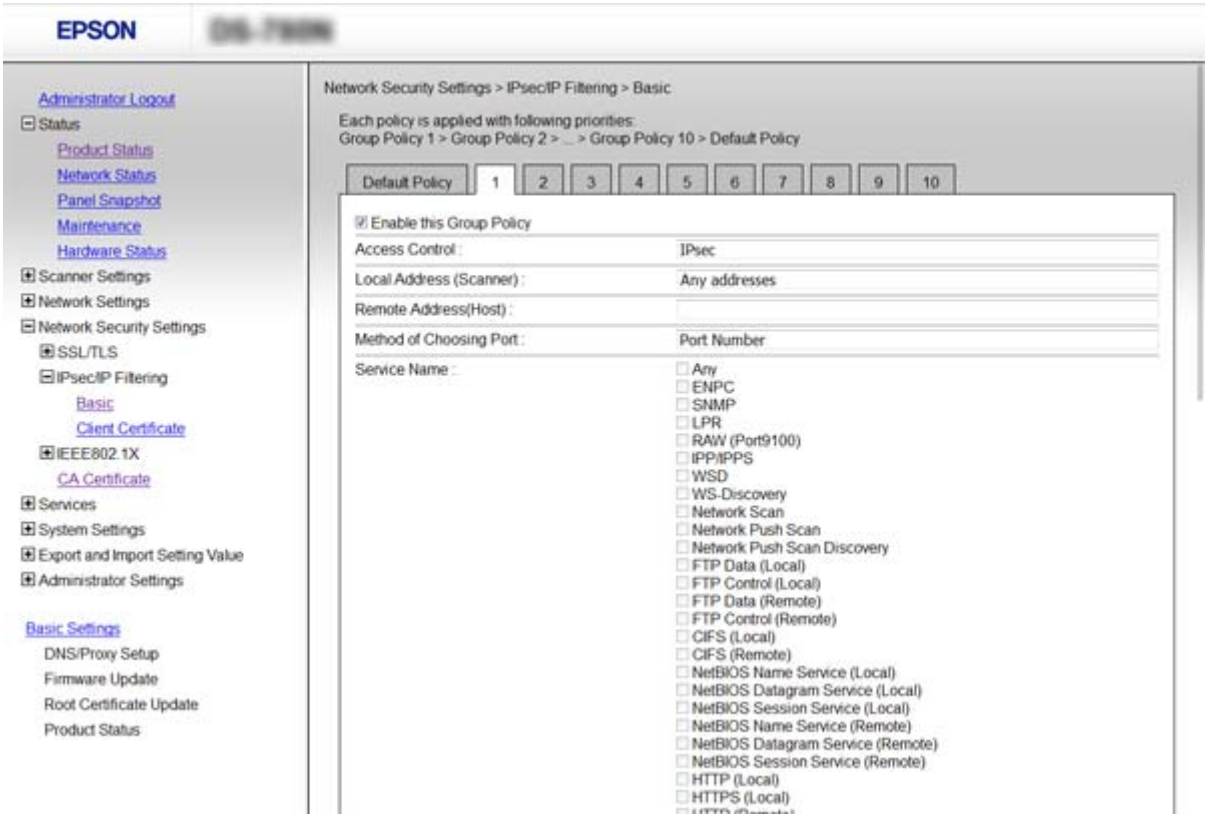
   Bir doğrulama mesajı görüntülenir.
5. **OK** öğesine tıklayın.

   Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23
➡ "Group Policy Ayarlama Öğeleri" sayfa 75

Group Policy Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklamalar	
Enable this Group Policy	Bir grup ilkesi etkinleştirebilir ya da devre dışı bırakabilirsiniz.	
Access Control	IP paketlerinin trafiği için bir kontrol yöntemi yapılandırın.	
	Permit Access	Yapılandırılmış IP paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
	Refuse Access	Yapılandırılmış IP paketlerinin düz geçişlerini reddetmek için bu öğeyi seçin.
	IPsec	Yapılandırılmış IPsec paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
Local Address (Scanner)	Ağ ortamınızla eşleşen bir IPv4 adresi veya IPv6 adresi seçin. Bir IP adresi otomatik atanırsa, **Use auto-obtained IPv4 address** öğesini seçebilirsiniz.	
Remote Address(Host)	Erişimi kontrol etmek için bir cihazın IP adresini girin. IP adresi 43 karakter veya daha kısa olmalıdır. Bir IP adresi girmezseniz, tüm adresler kontrol edilir. ***Not:*** *Bir IP adresi otomatik olarak atanmışsa (örneğin DHCP tarafından atanmışsa), bağlantı kurulamayabilir. Sabit bir IP adresi yapılandırın.*	
Method of Choosing Port	Bağlantı noktalarını belirtmek için bir yöntem seçin.	
Service Name	**Method of Choosing Port** için **Service Name** öğesini seçerseniz bir seçenek seçin.	

Kuruluş için Gelişmiş Güvenlik Ayarları

Öğeler	Ayarlar ve Açıklamalar	
Transport Protocol	**Port Number** için **Method of Choosing Port** öğesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.	
	Any Protocol	Tüm protokol türlerini kontrol etmek için bunu seçin.
	TCP	Tekli gönderim amacıyla veri kontrolü için bu öğeyi seçin.
	UDP	Çoklu gönderim ve yayın amacıyla veri kontrolü için bu öğeyi seçin.
	ICMPv4	Ping komutu kontrolü için bu öğeyi seçin.
Local Port	**Method of Choosing Port** için **Port Number** öğesini seçerseniz ve **Transport Protocol** için **TCP** veya **UDP** öğesini seçerseniz, paketleri almayı kontrol etmek için bağlantı noktası numaralarını virgüllerle ayırarak girin. En fazla 10 bağlantı noktası sayısı girebilirsiniz. Örnek: 20,80,119,5220 Bir bağlantı noktası sayısı girmezseniz, tüm bağlantı noktaları kontrol edilir.	
Remote Port	**Method of Choosing Port** için **Port Number** öğesini seçerseniz ve **Transport Protocol** için **TCP** veya **UDP** öğesini seçerseniz, paketleri göndermeyi kontrol etmek için bağlantı noktası numaralarını virgüllerle ayırarak girin. En fazla 10 bağlantı noktası sayısı girebilirsiniz. Örnek: 25,80,143,5220 Bir bağlantı noktası sayısı girmezseniz, tüm bağlantı noktaları kontrol edilir.	
IKE Version	IKE sürümü için IKEv1 veya IKEv2 öğesini seçin. Tarayıcının bağlı olduğu aygıta göre bunlardan birini seçin.	
IKEv1	**IKE Version** için **IKEv1** öğesini seçtiğinizde aşağıdaki öğeler görüntülenir.	
	Authentication Method	**Access Control** için **IPsec** öğesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.
IKEv2	**IKE Version** için **IKEv2** öğesini seçtiğinizde aşağıdaki öğeler görüntülenir.	

Kuruluş için Gelişmiş Güvenlik Ayarları

Öğeler	Ayarlar ve Açıklamalar	
Local	Authentication Method	**Access Control** için **IPsec** öğesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
	ID Type	Tarayıcı için kimliğin türünü seçin.
	ID	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@", "#" ve "=" öğelerini kullanamazsınız. **Distinguished Name**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" öğesini eklemeniz gerekir. **IP Address**: IPv4 veya IPv6 biçimini girin. **FQDN**: A–Z, a–z, 0–9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. **Email Address**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" öğesini eklemeniz gerekir. **Key ID**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.
Remote	Authentication Method	**Access Control** için **IPsec** öğesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
	ID Type	Kimliğini doğrulamak istediğiniz aygıtın kimlik türünü seçin.
	ID	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@", "#" ve "=" öğelerini kullanamazsınız. **Distinguished Name**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" öğesini eklemeniz gerekir. **IP Address**: IPv4 veya IPv6 biçimini girin. **FQDN**: A–Z, a–z, 0–9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. **Email Address**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" öğesini eklemeniz gerekir. **Key ID**: 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Pre-Shared Key	**Authentication Method** için **Pre-Shared Key** öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Confirm Pre-Shared Key	Yapılandırdığınız anahtarı onay için girin.

Kuruluş için Gelişmiş Güvenlik Ayarları

Öğeler	Ayarlar ve Açıklamalar	
Encapsulation	**IPsec** için **Access Control** öğesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.	
	Transport Mode	Aynı LAN üzerinde sadece tarayıcıyı kullanırsanız bu öğeyi seçin. Katman 4 ya da sonraki IP paketleri şifrelenmiştir.
	Tunnel Mode	Tarayıcıyı IPsec-VPN gibi Internet özellikli bir ağda kullanıyorsanız bu seçeneği seçin. IP paketlerinin başlıkları ve verileri şifrelenmiştir.
Remote Gateway(Tunnel Mode)	**Encapsulation** için **Tunnel Mode** öğesini seçerseniz, 1 ve 39 karakter arası bir ağ geçidi adresi girin.	
Security Protocol	**Access Control** için **IPsec** öğesini seçerseniz bir seçenek seçin.	
	ESP	Kimlik doğrulama ve veri bütünlüğünü sağlamak ve veri şifrelemesi için bu öğeyi seçin.
	AH	Kimlik doğrulama ve veri bütünlüğünü sağlamak için bu öğeyi seçin. Veri şifrelemesi yasaklandığında bile IPsec kullanabilirsiniz.
Algorithm Settings		
IKE	Encryption	IKE için şifreleme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
	Authentication	IKE için kimlik doğrulama algoritmasını seçin.
	Key Exchange	IKE için anahtar değiştirme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
ESP	Encryption	ESP için şifreleme algoritmasını seçin. Bu, **ESP** öğesi **Security Protocol** için seçildiğinde kullanılabilir.
	Authentication	ESP için kimlik doğrulama algoritmasını seçin. Bu, **ESP** öğesi **Security Protocol** için seçildiğinde kullanılabilir.
AH	Authentication	AH için kimlik doğrulama algoritmasını seçin. Bu, **AH** öğesi **Security Protocol** için seçildiğinde kullanılabilir.

İlgili Bilgi

➡ “Group Policy Yapılandırma” sayfa 74

➡ “Group Policy üzerinde Local Address (Scanner) ve Remote Address(Host) birleşimi” sayfa 79

➡ “Grup İlkesinde Hizmet Adı Referansları” sayfa 79

Group Policy üzerinde Local Address (Scanner) ve Remote Address(Host) birleşimi

		Local Address (Scanner) Öğesini Ayarlama		
		IPv4	IPv6*2	Any addresses*3
Remote Address(Host) Öğesini Ayarlama	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Boş	✓	✓	✓

*1 **Access Control** için **IPsec** seçilirse, önek uzunluğunu belirtemezsiniz.

*2 **Access Control** için **IPsec** seçilirse, bir bağlantı yerel adresi (fe80::) seçebilirsiniz ancak grup ilkesi devre dışı bırakılır.

*3 IPv6 bağlantı yerel adresleri hariç.

Grup İlkesinde Hizmet Adı Referansları

Not:
Kullanılamayan hizmetler görüntülenir ancak seçilemez.

Hizmet Adı	Protokol türü	Yerel bağlantı noktası numarası	Uzak bağlantı noktası numarası	Kontrol edilen özellikler
Any	–	–	–	Tüm hizmetler
ENPC	UDP	3289	Herhangi bir bağlantı noktası	EpsonNet Config ve tarayıcı sürücüsü gibi uygulamalardan bir tarayıcı arama
SNMP	UDP	161	Herhangi bir bağlantı noktası	EpsonNet Config ve Epson tarayıcı sürücüsü gibi uygulamalardan MIB alma ve yapılandırma
WSD	TCP	Herhangi bir bağlantı noktası	5357	WSD kontrol etme
WS-Discovery	UDP	3702	Herhangi bir bağlantı noktası	WSD'den bir tarayıcı arama
Network Scan	TCP	1865	Herhangi bir bağlantı noktası	Document Capture Pro'dan tarama verilerini iletme
Network Push Scan Discovery	UDP	2968	Herhangi bir bağlantı noktası	Tarayıcıdan bir bilgisayarı arama.
Network Push Scan	TCP	Herhangi bir bağlantı noktası	2968	Document Capture Pro veya Document Capture öğesinden itmeli tarama iş bilgilerini alma
HTTP (Local)	TCP	80	Herhangi bir bağlantı noktası	HTTP(S) sunucusu (Web Config ve WSD verilerini iletme)
HTTPS (Local)	TCP	443	Herhangi bir bağlantı noktası	

Hizmet Adı	Protokol türü	Yerel bağlantı noktası numarası	Uzak bağlantı noktası numarası	Kontrol edilen özellikler
HTTP (Remote)	TCP	Herhangi bir bağlantı noktası	80	HTTP(S) istemcisi (bellenim güncelleme ve kök sertifikası güncelleme arasında iletişim)
HTTPS (Remote)	TCP	Herhangi bir bağlantı noktası	443	

IPsec/IP Filtering Yapılandırma Örnekleri

Sadece IPsec paketlerinin alımı

Bu örnek sadece varsayılan ilke yapılandırması içindir.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: En fazla 127 karakter girin.

Group Policy:

Yapılandırmayın.

Epson Scan 2 ve tarayıcı ayarlarını kullanarak taramayı kabul etme

Bu örnek belirtilen hizmetlerden tarama verileri iletişimlerine ve tarayıcı yapılandırmasına izin verir.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Kutuyu kontrol edin.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: Bir istemcinin IP adresi

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** ve **HTTPS (Local)** kutularını işaretleyin.

Sadece belirlenen bir IP adresinden erişim sağlama

Bu örnek, belirlenen bir IP adresinin tarayıcıya erişimine izin verir.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Kutuyu kontrol edin.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: Bir yönetici istemcisinin IP adresi

Not:
İlke yapılandırmasından bağımsız olarak, istemci tarayıcıya erişebilecek ve yapılandırabilecek.

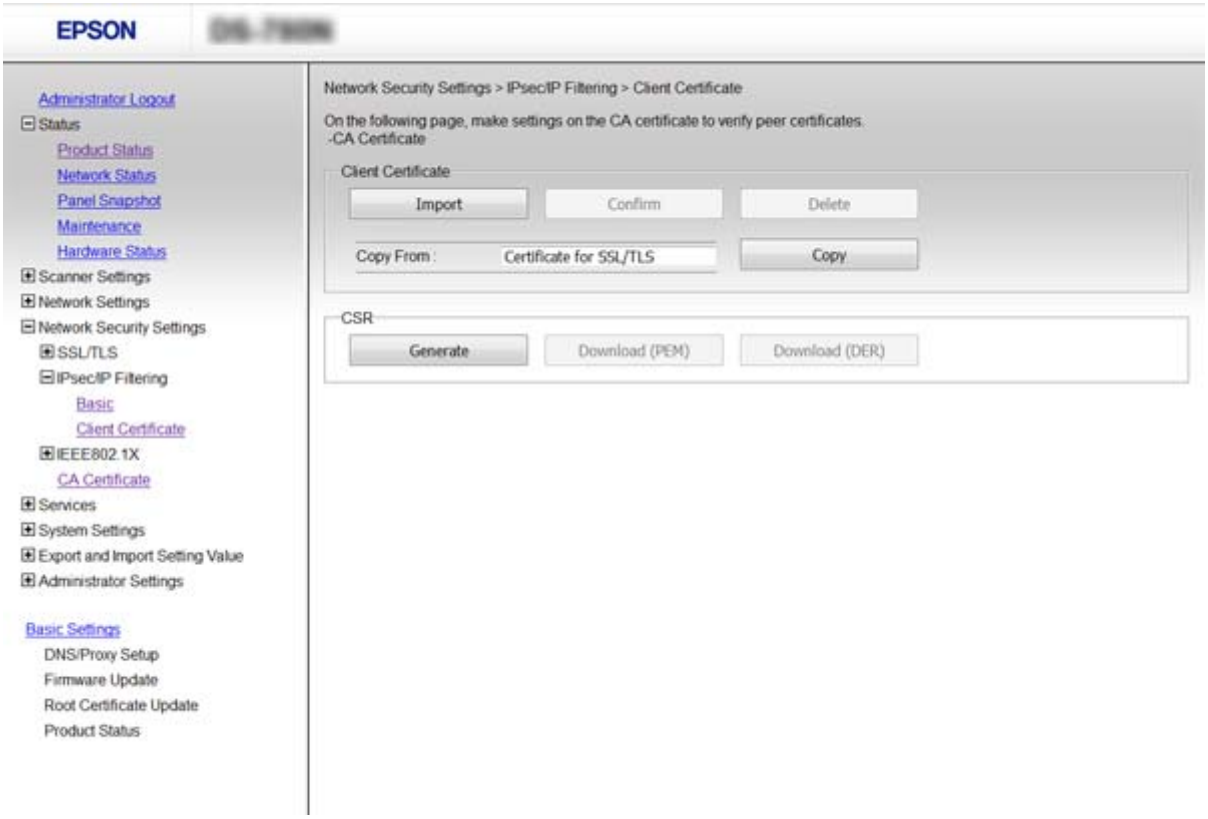
IPsec/IP Filtering için Sertifika Yapılandırma

IPsec/IP Filtreleme için İstemci Sertifikasını yapılandırın. Sertifika yetkilisini yapılandırmak isterseniz **CA Certificate** kısmına gidin.

1. Web Config'e erişin ve **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate** öğesini seçin.

2. Sertifikayı **Client Certificate** kısmında içe aktarın.

   Bir Sertifika Yetkilisi tarafından IEEE802.1X veya SSL/TLS biçiminde yayınlanmış bir sertifikayı zaten içe aktarmışsanız, sertifikayı kopyalayıp IPsec/IP Filtrelemede kullanabilirsiniz. Kopyalamak için, **Copy From** kısmından sertifikayı seçip **Copy** öğesine tıklayın.



İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "CA İmzalı bir Sertifika Alma ve İçe Aktarma" sayfa 63

SNMPv3 protokolünü kullanma

SNMPv3 Hakkında

SNMP, ağa bağlı cihazların bilgilerini toplamak için izleme ve kontrolü taşıyan bir protokoldür. SNMPv3, geliştirilmiş yönetim güvenlik özelliği sürümüdür.

SNMPv3'ü kullanırken, SNMP iletişimini (paket) dinleme, kişileştirme ve değiştirme gibi ağ risklerinden korumak için SNMP iletişiminin (paket) durum izleme ve ayar değişikliklerinin kimliği doğrulanabilir ve şifrelenebilir.

SNMPv3 Yapılandırma

Tarayıcı SNMPv3 protokolünü destekliyorsa, tarayıcıya erişimi izleyebilir ve denetleyebilirsiniz.

1. Web Config'e erişin ve **Services** > **Protocol** öğesini seçin.
2. Her **SNMPv3 Settings** öğesi için bir değer girin.
3. **Next** öğesine tıklayın.

   Bir doğrulama mesajı görüntülenir.
4. **OK** öğesine tıklayın.

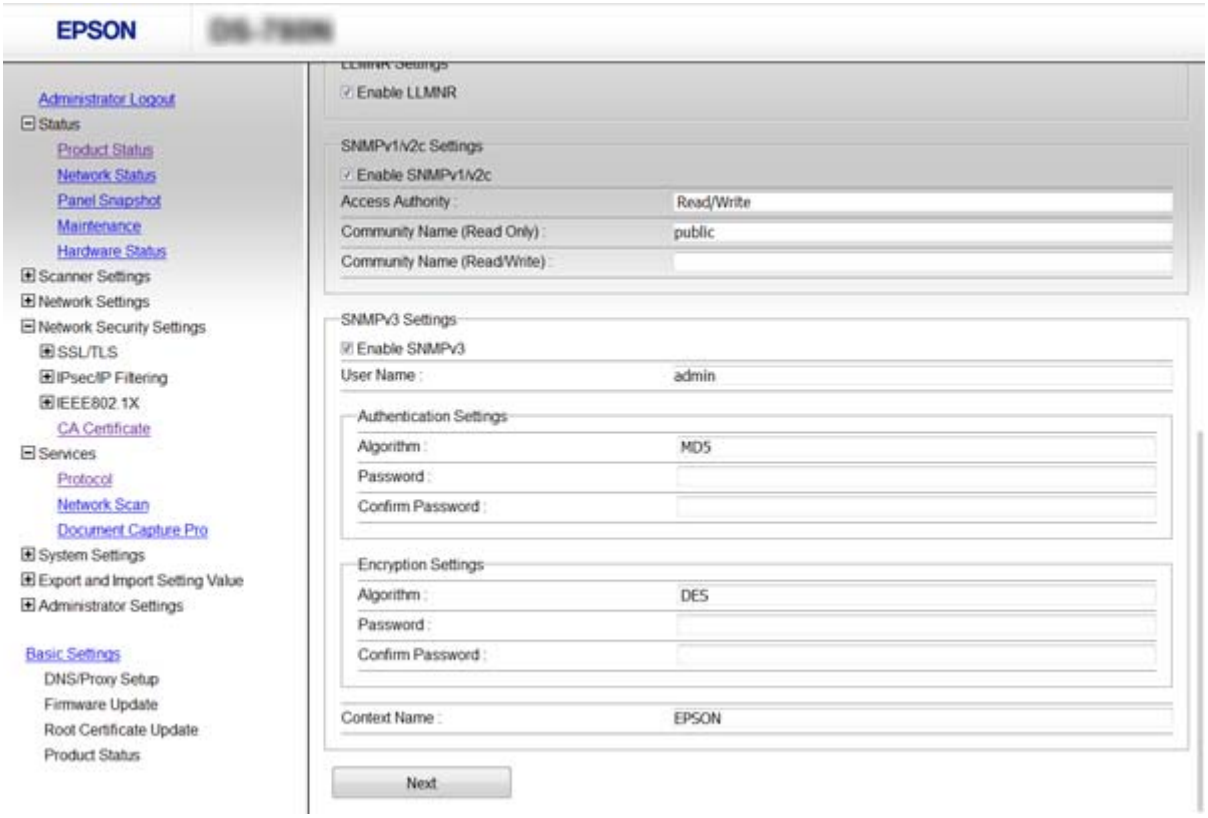
   Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

➡ “Web Config Erişimi” sayfa 23

➡ “SNMPv3 Ayarlama Öğeleri” sayfa 83

SNMPv3 Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklama
Enable SNMPv3	SNMPv3, kutu işaretlendiğinde etkinleştirilir.
User Name	1 bit karakter kullanarak 1 ila 32 karakter girin.
Authentication Settings	
Algorithm	Kimlik denetim için bir algoritma seçin.
Password	ASCII (0x20-0x7E) formatında 8 ila 32 karakter girin.
Confirm Password	Onay için, yapılandırdığınız şifreyi girin.
Encryption Settings	
Algorithm	Şifreleme için bir algoritma seçin.
Password	ASCII (0x20-0x7E) formatında 8 ila 32 karakter girin.
Confirm Password	Onay için, yapılandırdığınız şifreyi girin.
Context Name	1 bit karakter kullanarak 1 ila 32 karakter girin.

İlgili Bilgi

➡ “SNMPv3 Yapılandırma” sayfa 82

Tarayıcıyı Bir IEEE802.1X Ağına Bağlama

IEEE802.1X Ağı Yapılandırma

Tarayıcı, IEEE802.1X ağını destekliyorsa, tarayıcıyı RADIUS sunucusuna ve kimlik doğrulayıcı görevi gören bir huba bağlı kimlik doğrulamalı bir ağ üzerinde kullanabilir.

1. Web Config'e erişin ve **Network Security Settings** > **IEEE802.1X** > **Basic** öğesini seçin.
2. Her öğe için bir değer girin.
3. **Next** öğesine tıklayın.

   Bir doğrulama mesajı görüntülenir.
4. **OK** öğesine tıklayın.

   Tarayıcı güncelleştirilmiştir.

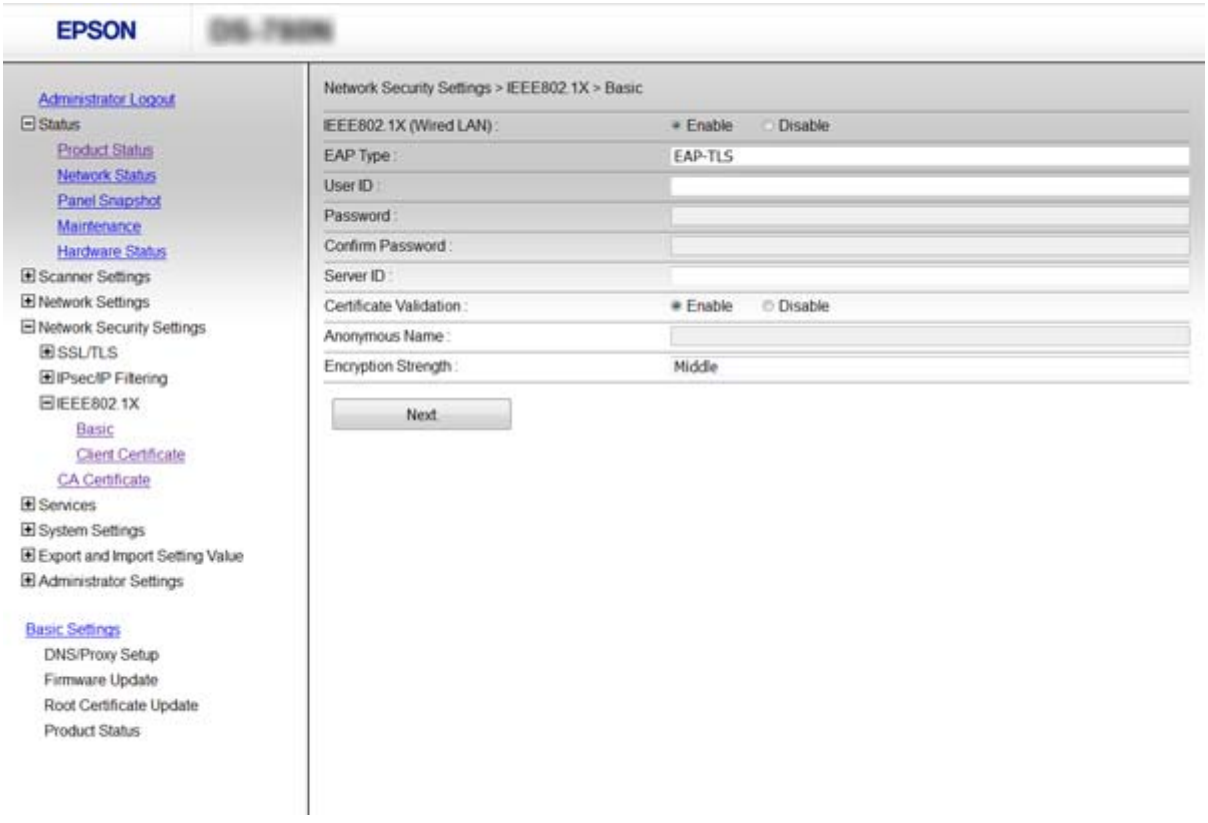
İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "IEEE802.1X Ağı Ayarlama Öğeleri" sayfa 84

➡ "IEEE802.1X Yapılandırmasından Sonra Yazıcıya veya Tarayıcıya Erişilemiyor" sayfa 89

IEEE802.1X Ağı Ayarlama Öğeleri



Öğeler	Ayarlar ve Açıklamalar	
IEEE802.1X (Wired LAN)	**IEEE802.1X** > **Basic** için sayfanın ayarlarını etkinleştirebilir veya devre dışı bırakabilirsiniz (IEEE802.1X) (Kablolu LAN).	
EAP Type	Tarayıcı ile bir RADIUS sunucusu arasında kimlik doğrulama yöntemi için bir seçenek belirleyin.	
	EAP-TLS	CA imzalı bir sertifika almalı ve içe aktarmalısınız.
	PEAP-TLS	
	PEAP/MSCHAPv2	Parola yapılandırmalısınız.
User ID	Bir RADIUS sunucusunun kimlik doğrulaması için kullanmak üzere bir kimlik yapılandırın. 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.	
Password	Tarayıcı kimlik doğrulaması için bir şifre yapılandırın. 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. Windows sunucusu olarak bir RADIUS sunucusu kullanıyorsanız 127 karaktere kadar girebilirsiniz.	
Confirm Password	Yapılandırdığınız parolayı onay için girin.	
Server ID	Belirli bir RADIUS sunucusuyla kimlik doğrulaması için bir sunucu kimliği yapılandırabilirsiniz. Kimlik doğrulayıcı, RADIUS sunucusundan gönderilen bir sunucu sertifikasının subject/subjectAltName alanında bir sunucu kimliği olup olmadığını doğrular. 0 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.	
Certificate Validation	Sertifika doğrulamasını kimlik doğrulama yöntemini dikkate almadan ayarlayabilirsiniz. Sertifikayı **CA Certificate** kısmında içe aktarın.	
Anonymous Name	**PEAP-TLS** veya **PEAP/MSCHAPv2** (**Authentication Method** olarak) seçerseniz, PEAP kimlik doğrulamasının 1. aşamasında kullanıcı kimliği yerine anonim bir ad yapılandırabilirsiniz. 0 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.	
Encryption Strength	Aşağıdakilerden bir tanesini seçebilirsiniz.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

İlgili Bilgi

➡ "IEEE802.1X Ağı Yapılandırma" sayfa 84

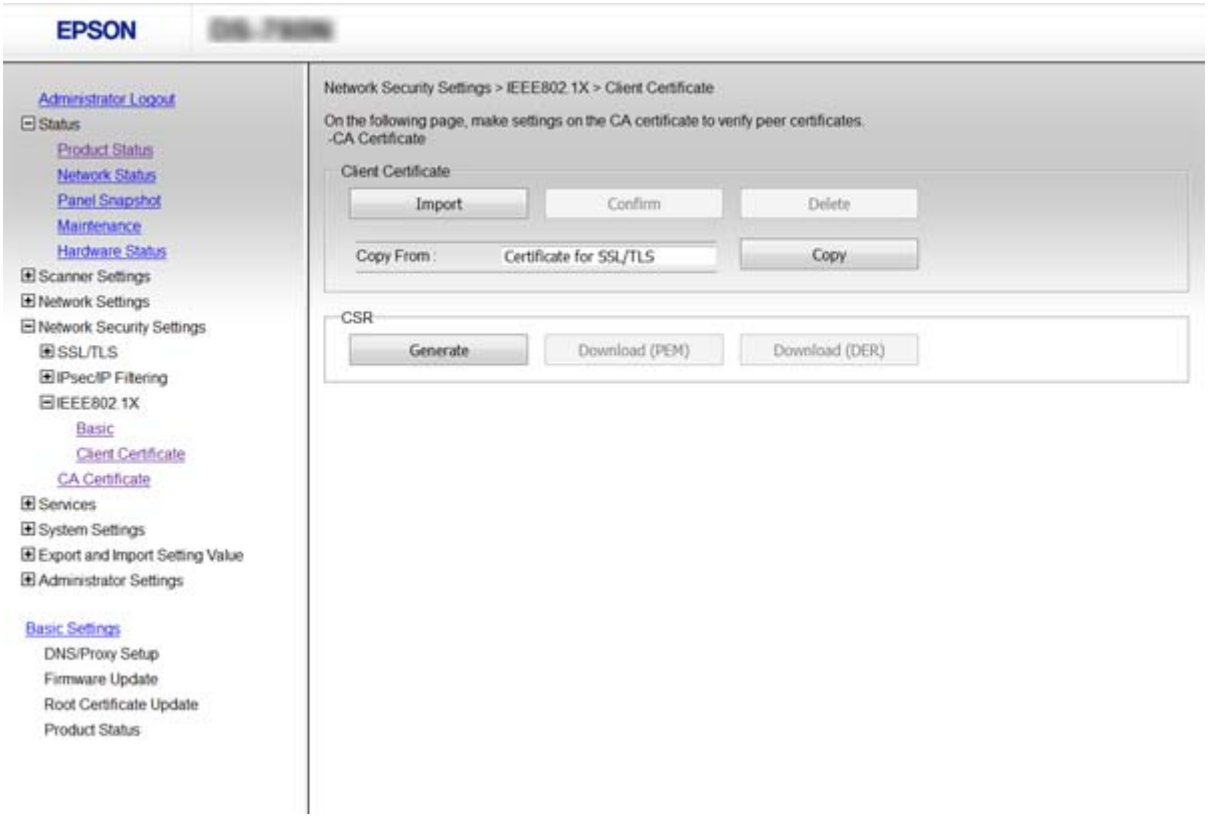
IEEE802.1X için Sertifika Yapılandırma

IEEE802.1X için İstemci Sertifikasını yapılandırın. Sertifika yetkilisi sertifikasını yapılandırmak isterseniz **CA Certificate** kısmına gidin.

1. Web Config'e erişin ve **Network Security Settings** > **IEEE802.1X** > **Client Certificate** öğesini seçin.

2. **Client Certificate** kısmına bir sertifika girin.

   Bir Sertifika Yetkilisi tarafından yayımlanmışsa sertifikayı kopyalayabilirsiniz. Kopyalamak için, **Copy From** kısmından sertifikayı seçip **Copy** öğesine tıklayın.



İlgili Bilgi

➡ “Web Config Erişimi” sayfa 23

➡ “CA İmzalı bir Sertifika Alma ve İçe Aktarma” sayfa 63

Gelişmiş Güvenlik İçin Sorunları Çözme

Güvenlik Ayarlarını Geri Yükleme

IPsec/IP Filtreleme veya IEEE802.1X gibi yüksek güvenli bir ortam kurarken, yanlış ayarlar veya aygıt veya sunucuyla sorun nedeniyle aygıtlarla iletişim kuramayabilirsiniz. Bu durumda, aygıt ayarlarını yeniden yapmak için veya gecikmeli kullanıma izin vermek için güvenlik ayarlarını geri yükleyin.

Kontrol Panelini Kullanarak Güvenlik İşlevini Devre Dışı Bırakma

Tarayıcının kontrol panelini kullanarak IPsec/IP Filtrelemeyi veya IEEE802.1X'i devre dışı bırakabilirsiniz.

1. **Ayarlar** > **Ağ Ayarları** öğesine dokunun.

2. **Ayarları Değiştir** öğesine dokunun.

3. Devre dışı bırakmak istediğiniz öğelere dokunun.
   - ❏ **IPsec/IP Filtreleme**
   - ❏ **IEEE802.1X**
4. Bir tamamlama mesajı görüntülendiğinde, **İlerle** öğesine dokunun.

Web Config'i Kullanarak Güvenlik İşlevini Geri Yükleme

IEEE802.1X için ağda aygıtlar tanınmayabilir. Bu durumda, tarayıcının kontrol panelini kullanarak işlevi devre dışı bırakın.

IPsec/IP Filtreleme için bilgisayardan aygıta erişebilmeniz için işlevi devre dışı bırakabilirsiniz.

Web Config Kullanarak IPsec/IP Filtrelemesini Devre Dışı Bırakma

1. Web Config'e erişin ve **Network Security Settings** > **IPsec/IP Filtering** > **Basic** öğesini seçin.
2. **Disable** öğesini **Default Policy** içindeki **IPsec/IP Filtering** için seçin.
3. **Next** öğesine tıklayın ve sonra tüm grup ilkeleri için **Enable this Group Policy** öğesinin işaretini kaldırın.
4. **OK** öğesine tıklayın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

Ağ Güvenlik Özellikleri Kullanımı Sorunları

Önceden Paylaşılmış Bir Anahtar Unutuldu

Web Config kullanarak anahtarı tekrar yapılandırın.

Anahtarı yapılandırmak için, Web Config'e erişin ve **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** veya **Group Policy** öğesini seçin.

Önceden paylaşılan anahtarı değiştirirken bilgisayarlar için önceden paylaşılan anahtarı yapılandırın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

IPsec İletişimi ile İletişim Kurulamıyor

Bilgisayar ayarları için desteklenmeyen bir algoritma mı kullanıyorsunuz?

Tarayıcı aşağıdaki algoritmaları destekler.

Güvenlik Yöntemleri	Algoritmalar
IKE şifreleme algoritması	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE kimlik doğrulama algoritması	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE anahtar değiştirme algoritması	DH Grubu 1, DH Grubu 2, DH Grubu 5, DH Grubu 14, DH Grubu 15, DH Grubu 16, DH Grubu 17, DH Grubu 18, DH Grubu 19, DH Grubu 20, DH Grubu 21, DH Grubu 22, DH Grubu 23, DH Grubu 24, DH Grubu 25, DH Grubu 26, DH Grubu 27*, DH Grubu 28*, DH Grubu 29*, DH Grubu 30*
ESP şifreleme algoritması	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP kimlik doğrulama algoritması	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH kimlik doğrulama algoritması	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* yalnızca IKEv2 için kullanılabilir

İlgili Bilgi

➡ "IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim" sayfa 70

İletişim Aniden Kesiliyor

Tarayıcının IP adresi geçersiz ya da değiştirildi mi?

Tarayıcının kontrol panelini kullanarak IPsec'i devre dışı bırakın.

DHCP süresi dolduysa yeniden başlatın veya IPv6 adresi süresi geçmişse veya alınmamışsa tarayıcının Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) öğesi için kayıtlı IP adresi bulunamayabilir.

Sabit bir IP adresi kullanın.

Bilgisayarın IP adresi geçersiz mi ya da değiştirildi mi?

Tarayıcının kontrol panelini kullanarak IPsec'i devre dışı bırakın.

DHCP süresi dolduysa yeniden başlatın veya IPv6 adresi süresi geçmişse veya alınmamışsa tarayıcının Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) öğesi için kayıtlı IP adresi bulunamayabilir.

Sabit bir IP adresi kullanın.

İlgili Bilgi

➡ "Web Config Erişimi" sayfa 23

➡ "IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim" sayfa 70

IPsec/IP Filtreleme Yapılandırıldıktan Sonra Bağlanılamıyor

Ayarlı değer yanlış olabilir.

Tarayıcının kontrol panelinden IPsec/IP filtrelemeyi devre dışı bırakın. Tarayıcı ve bilgisayarı bağlayıp, IPsec/IP Filtreleme ayarlarını tekrar yapın.

İlgili Bilgi

➡ "IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim" sayfa 70

IEEE802.1X Yapılandırmasından Sonra Yazıcıya veya Tarayıcıya Erişilemiyor

Ayarlar yanlış olabilir.

IEEE802.1X'i tarayıcının kontrol panelinden devre dışı bırakın. Tarayıcı ve bilgisayarı bağlayın ve sonra IEEE802.1X öğesini yeniden yapılandırın.

İlgili Bilgi

➡ "IEEE802.1X Ağı Yapılandırma" sayfa 84

Dijital Sertifika Kullanımı Sorunları

CA İmzalı bir Sertifika İçe Aktarılamıyor

CA İmzalı ve CSR üzerinde yer alan bilgiler eşleşiyor mu?

CA imzalı sertifika ile CSR bilgileri aynı değilse, CSR içe aktarılamayabilir. Aşağıdakileri kontrol yapın:

❏ Sertifikayı, aynı bilgilere sahip olmayan bir cihaza mı içe aktarmaya çalışıyorsunuz?
CSR bilgilerini kontrol edin ve ardından sertifikayı aynı bilgilere sahip olan bir cihaza içe aktarın.

❏ CSR'ı bir sertifika yetkilisine gönderdikten sonra tarayıcıya kayıtlı CSR'ın üzerine mi yazdınız?
CSR ile CA imzalı sertifikayı tekrar alın.

CA imzalı sertifika 5 KB'den daha mı büyük?

5 KB'den daha büyük bir CA imzalı sertifikayı içe aktaramazsınız.

Sertifikayı içe aktarım şifresi doğru mu?

Şifreyi unuttuysanız sertifikayı içe aktaramazsınız.

İlgili Bilgi

➡ "CA İmzalı bir Sertifikanın İçe Aktarımı" sayfa 64

Kendinden İmzalı bir Sertifika Güncellenmiyor

Common Name girildi mi?

Common Name girilmelidir.

Common Name desteklenen karakterlerle mi girildi? Örneğin Japonca karakterler desteklenmez.

ASCII (0x20-0x7E) kısmına IPv4, IPv6, ana makine ya da FQDN formatında 1 ila 128 karakter girin.

Common Name virgül ya da boşluk içeriyor mu?

Common Name virgül içeriyorsa, o noktada ayrılır. Virgülün önünde ya da ardında sadece bir boşluk girilmişse hata oluşur.

İlgili Bilgi

➡ "Kendinden İmzalı Sertifika Güncelleme" sayfa 67

CSR Oluşturulamıyor

Common Name girildi mi?

Common Name girilmelidir.

Common Name, Organization, Organizational Unit, Locality, State/Province'a desteklenmeyen karakterler girildi mi? Örneğin Japonca karakterler desteklenmez.

ASCII (0x20-0x7E) kısmına IPv4, IPv6, ana makine ya da FQDN formatında karakterler girin.

Common Name virgül ya da boşluk içeriyor mu?

Common Name virgül içeriyorsa, o noktada ayrılır. Virgülün önünde ya da ardında sadece bir boşluk girilmişse hata oluşur.

İlgili Bilgi

➡ "CA İmzalı bir Sertifika Alınması" sayfa 63

Görüntülenen bir Dijital Sertifikaya İlişkin Uyarı

Mesajlar	Neden/Çözüm
Enter a Server Certificate.	**Neden:** İçe aktarmak için bir dosya seçmediniz. **Çözüm:** Bir dosya seçin ve **Import** öğesine tıklayın.

Kuruluş için Gelişmiş Güvenlik Ayarları

Mesajlar	Neden/Çözüm
CA Certificate 1 is not entered.	**Neden:** CA sertifikası 1 girilmedi ve sadece CA sertifikası 2 girildi. **Çözüm:** Önce CA sertifikası 1'i içe aktarın.
Invalid value below.	**Neden:** Dosya yolu ve/veya şifrede desteklenmeyen karakterler mevcut. **Çözüm:** Öğe için girilen karakterlerin doğru olduğundan emin olun.
Invalid date and time.	**Neden:** Tarayıcının tarih ve saat ayarları yapılmamış. **Çözüm:** Web Config ya da EpsonNet Config'i kullanarak tarih ve saati ayarlayın.
Invalid password.	**Neden:** CA sertifikası için ayarlanan şifre ile girilen şifre eşleşmiyor. **Çözüm:** Doğru şifreyi girin.
Invalid file.	**Neden:** X509 formatındaki sertifika dosyasını içe aktarmıyorsunuz. **Çözüm:** Güvenilir sertifika yetkilisi tarafından gönderilen doğru sertifikayı seçtiğinizden emin olun.
	Neden: İçe aktardığınız dosya çok büyük. Maksimum dosya boyutu 5 KB. **Çözüm:** Doğru dosyayı seçerseniz, sertifika bozulabilir ya da sahte bir tane oluşabilir.
	Neden: Sertifikadaki zincir geçersiz. **Çözüm:** Sertifika hakkında daha fazla bilgi için sertifika yetkilisinin web sitesini ziyaret edin.
Cannot use the Server Certificates that include more than three CA certificates.	**Neden:** PKCS#12 formatındaki sertifika dosyası 3'ten daha fazla CA sertifikası içeriyor. **Çözüm:** Her bir sertifikayı PKCS#12 formatından PEM formatına dönüştürerek içe aktarın ya da en fazla 2 CA sertifikası içeren PKCS#12 formatındaki sertifika dosyasını içe aktarın.

Mesajlar	Neden/Çözüm
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Neden:** Sertifika süre aşımına uğradı. **Çözüm:** ❏ Sertifika süresi dolduysa yeni bir sertifika alın ya da içe aktarın. ❏ Sertifika süresi dolmadıysa, tarayıcının tarih ve saat ayarının doğru ayarlandığından emin olun.
Private key is required.	**Neden:** Sertifika ile eşleşen özel anahtar yok. **Çözüm:** ❏ Sertifika PEM/DER formatındaysa ve bilgisayar kullanılarak bir CSR'dan alındıysa, özel anahtar dosyasını belirleyin. ❏ Sertifika PKCS#12 formatındaysa ve bilgisayar kullanılarak bir CSR'dan alındıysa, özel anahtar içeren bir dosya oluşturun.
	Neden: Web Config'i kullanılarak bir CSR'dan alınan PEM/DER sertifikasını yeniden içe aktardınız. **Çözüm:** Sertifika PEM/DER formatındaysa ve Web Config kullanılarak bir CSR'dan alındıysa, sadece bir kez içe aktarabilirsiniz.
Setup failed.	**Neden:** Tarayıcı ve bilgisayar arasındaki iletişim başarısız olduğu için yapılandırma bitirilemiyor ya da bazı hatalar sebebiyle dosya okunamıyor. **Çözüm:** Belirlenen dosya ve iletişim seçildikten sonra, dosyayı tekrar içe aktarın.

İlgili Bilgi

➡ “Dijital Sertifikasyon Hakkında” sayfa 62

Yanlışlıkla CA İmzalı bir Sertifikanın Silinmesi

Sertifikanın yedek dosyası mevcut mu?

Yedek dosyanız varsa, sertifikayı tekrar içe aktarın.

Web Config tarafından hazırlanmış bir CSR kullanıyorsanız, silinmiş bir sertifikayı tekrar içe aktaramazsınız. Bir CSR oluşturun ve yeni bir sertifika alın.

İlgili Bilgi

➡ “CA İmzalı bir Sertifika Silme” sayfa 66

➡ “CA İmzalı bir Sertifikanın İçe Aktarımı” sayfa 64