

DS-790WN

Yönetici Kılavuzu

Amacınıza Uygun Gerekli Ayarlar

Ağ Ayarları

Tarama İçin Gerekli Ayarlar

Temel Güvenlik Ayarları

Gelişmiş Güvenlik Ayarları

Kimlik Doğrulama Ayarları

Telif Hakkı

Bu belgenin herhangi bir kısmı, Seiko Epson Corporation'ın yazılı izni olmadan kısmen veya bütün olarak çoğaltılamaz, bilgi erişim sistemlerinde saklanamaz veya elektronik, mekanik yöntemlerle, fotokopi, kayıt yöntemleriyle veya diğer yöntemlerle başka ortamlara aktarılamaz. Burada bulunan bilgilerin kullanımı konusunda herhangi bir patent yükümlülüğü olduğu varsayılmamıştır. Buradaki bilgilerin kullanılması sonucu oluşan zararlar için de herhangi bir sorumluluk kabul edilmez. Burada bulunan bilgiler yalnızca bu Epson ürünü ile kullanılmak üzere tasarlanmıştır. Epson, bu bilgilerin diğer ürünlerle ilgili olarak herhangi bir şekilde kullanılmasından sorumlu değildir.

Seiko Epson Corporation ve bağlı kuruluşları ürünü satın alanın veya üçüncü kişilerin kaza, ürünün yanlış veya kötü amaçla kullanılması, ürün üzerinde yetkisiz kişilerce yapılan değişiklikler, onarımlar veya tadilatlar veya (ABD hariç olmak üzere) Seiko Epson Corporation'ın çalıştırma ve bakım talimatlarına aykırı hareketler nedeniyle uğradıkları zarar, kayıp, maliyet veya gider konusunda ürünü satın alana ve üçüncü kişilere karşı kesinlikle yükümlü olmayacaktır.

Seiko Epson Corporation tarafından Orijinal Epson Ürünü veya Epson Tarafından Onaylanmış Ürün olarak tanımlananlar dışında herhangi bir opsiyonun veya sarf malzemesi ürünün kullanılmasından kaynaklanan herhangi bir zarar veya sorun için Seiko Epson Corporation ve yan kuruluşları sorumlu tutulamaz.

Seiko Epson Corporation tarafından Epson Tarafından Onaylanmış Ürün olarak tanımlananlar dışında herhangi bir arayüz kablosu kullanıldığında oluşan elektromanyetik parazitlerden kaynaklanan herhangi bir hasar için Seiko Epson Corporation sorumlu tutulamaz.

© 2021 Seiko Epson Corporation

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

Ticari Markalar

- ❑ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION ve logoları Seiko Epson'ın tescilli ticari markaları veya ticari markalarıdır.
- ❑ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❑ Chrome is a trademark of Google LLC.
- ❑ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❑ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❑ FeliCa ve PaSoRi Sony Corporation'ın tescilli ticari markalarıdır.
- ❑ MIFARE NXP Semiconductor Corporation'ın tescilli ticari markasıdır.
- ❑ Genel Bildirim: bu belgede kullanılan 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.

İçindekiler

Telif Hakkı

Ticari Markalar

Giriş

Bu Belgenin İçeriği.	7
Bu Kılavuzu Kullanma.	7
Marka ve Semboller.	7
Bu Kılavuzda Kullanılan Açıklamalar.	7
İşletim Sistemi Referansları.	8

Amacınıza Uygun Gerekli Ayarlar

Amacınıza Uygun Gerekli Ayarlar.	10
--	----

Ağ Ayarları

Tarayıcıyı Ağa Bağlama.	13
Ağ Bağlantısını Yapmadan Önce.	13
Kontrol Panelinden Ağa Bağlanma.	15
Bilgisayar veya Cihaz Ekleme veya Değiştirme.	19
Ağa Bağlı Bir Tarayıcıya Bağlanma.	19
Akıllı Bir Cihazı ve Tarayıcıyı Doğrudan Bağlama (Wi-Fi Direct).	21
Ağ Bağlantısını Yeniden Ayarlama.	23
Ağ Bağlantı Durumunu Kontrol Etme.	25
Kontrol Panelinden Ağ Bağlantısı Durumunu Kontrol Etme.	25
Ağ Özellikleri.	26
Wi-Fi Teknik Özellikleri.	26
Ethernet Özellikleri.	28
Ağ İşlevleri ve IPv4/IPv6.	28
Güvenlik Protokolü.	28
Tarayıcı İçin Bağlantı Noktasını Kullanma.	29
Sorunları Çözme.	30
Bir Ağa bağlanılamıyor.	30

Tarayıcıyı Ayarlamak için Yazılım

Web Config.	35
Web Tarayıcıda Web Yapılandırmayı Çalıştırma.	35
Web Config üzerinde Windows ögesini çalıştırma.	35
Epson Device Admin.	36
Yapılandırma Şablonu.	36

Tarama İçin Gerekli Ayarlar

Posta Sunucusu Yapılandırma.	41
Posta Sunucusu Ayarlama Öğeleri.	41
Posta Sunucusu Bağlantı Kontrolü.	42
Paylaşılan Bir Klasörünü Ayarlama.	44
Paylaşılan Klasör Oluşturma.	44
Kişileri Uygun Hale Getirme.	61
Kişiler Yapılandırma Karşılaştırması.	62
Web Config Kullanarak Kişileri Hedefe Kaydetme.	62
Web Config'i Kullanarak Bir Grup Olarak Hedefleri Kaydetme.	64
Kişileri Yedekleme ve Alma.	65
Aracı Kullanarak Kişileri Verme Ve Toplu Kaydetme.	66
LDAP Sunucusu ve Kullanıcılar Arasındaki Ortaklık.	67
Document Capture Pro Server'yi Kullanma.	70
Sunucu Modunu Ayarlama.	71
AirPrint Ayarlama.	71
Ağ Taramaya Hazırlanırken Sorunlar.	71
Sorunları Çözme İpuçları.	71
Web Config'e Erişilemiyor.	72

Kontrol Paneli Ekranını Özelleştirme

Ön ayarlar Öğelerinin Kaydedilmesi.	75
Ön ayarlar Menü Seçenekleri.	76
Kontrol Paneli Ana Ekranını Düzenleme.	77
Ana ekranda Düzen ögesini değiştirme.	77
Simge Ekle.	78
Simge Kaldır.	79
Simge Taşı.	80

Temel Güvenlik Ayarları

Ürün Güvenliği Özelliklerine Giriş.	83
Yönetici Ayarları.	83
Yönetici Şifresi Yapılandırma.	83
Kontrol Paneli için Kilit Ayarları Kullanma.	85
Kontrol Panelinden Yönetici olarak Giriş Yapma.	88
Harici Arayüzü Devre Dışı Bırakma.	89
Uzak Tarayıcıyı İzleme.	90
Uzak Tarayıcı İçin Bilgileri Kontrol Etme.	90
Olaylar Meydana Geldiğinde E-posta Bildirimi Alma.	90

Sorunları Çözme.	91
Şifrenizi mı Unuttunuz.	91

Gelişmiş Güvenlik Ayarları

Güvenlik Ayarları ve Tehlikeyi Önleme.	93
Güvenlik Özelliği Ayarları.	94
İletişim Kurallarını Denetleme ve Kullanma.	94
İletişim kurallarını denetleme.	94
Etkinleştirebileceğiniz veya Devre Dışı Bırakabileceğiniz İletişim Kuralları.	94
İletişim Kuralı Ayarlama Öğeleri.	95
Dijital Sertifika Kullanımı.	97
Dijital Sertifikasyon Hakkında.	97
CA İmzalı Sertifika Yapılandırma.	97
Kendinden İmzalı Sertifika Güncelleme.	101
CA Sertifikası Yapılandırma.	101
Tarayıcıyla SSL/TLS İletişimi.	102
Temel SSL/TLS Ayarlarını Yapılandırma.	102
Tarayıcı için Sunucu Sertifikası Yapılandırma.	103
IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim.	104
IPsec/IP Filtreleme Hakkında.	104
Varsayılan İlkeyi Yapılandırma.	104
Grup İlkesini Yapılandırma.	107
IPsec/IP Filtreleme Yapılandırma Örnekleri.	113
IPsec/IP Filtresi İçin Bir Sertifikayı Yapılandırma.	114
Tarayıcıyı Bir IEEE802.1X Ağına Bağlama.	114
IEEE 802.1X Ağı Yapılandırma.	114
IEEE 802.1X İçin Bir Sertifikayı Yapılandırma.	116
Gelişmiş Güvenlik İçin Sorunları Çözme.	116
Güvenlik Ayarlarını Geri Yükleme.	116
Ağ Güvenlik Özellikleri Kullanımı Sorunları.	117
Dijital Sertifika Kullanımı Sorunları.	119

Kimlik Doğrulama Ayarları

Kimlik Doğrulama Ayarları Hakkında.	124
Kimlik Doğrulama Ayarları İçin Kullanılabilir İşlevler.	124
Doğrulama Yöntemi Hakkında.	125
Ayar İçin Yazılım.	127
Tarayıcının Bellenim Sürümünü Güncelleme.	127
Kimlik Doğrulama Aygıtını Bağlama ve Yapılandırma.	127
Kart Okuyucu Uyumluluk Listesi.	127
Kimlik Doğrulama Aygıtını Bağlama.	130
Kimlik Doğrulama Aygıtı Ayarları.	131

Bilgileri Kaydetme ve Ayarlama.	132
Ayarlama.	132
Kimlik Doğrulamanın Etkinleştirilmesi.	133
Kimlik Doğrulama Ayarları.	133
Kullnc Ayrları Öğelerinin Kaydedilmesi.	135
LDAP Sunucusu ile Senkronize Etme.	141
E-posta Sunucusunu Ayarlama.	145
Klasörüne Tara Ayarlama.	146
Tek Dokunma İşlevlerini Özelleştirin.	147
Epson Device Admin Kullanarak Job History Raporları.	148
Rapora Eklenebilecek Öğeler.	148
Kontrol Panelinden Yönetici olarak Giriş Yapma.	148
Kimlik Doğrulama Ayarları öğesini devre dışı bırakma.	148
Kimlik Doğrulama Ayarları Bilgilerinin Silinmesi (Varsayılan Ayarları Geri Yükle).	149
Sorunları Çözme.	149
Kimlik Doğrulama Kartı Okunamıyor.	149

Bakım

Tarayıcının Dışını Temizleme.	151
Tarayıcının İçini Temizleme.	151
Makara Takma Kitini Değiştirme.	156
Makara Takma Kiti Kodları.	161
Tarama Sayısını Sıfırlama.	161
Enerji Tasarrufu.	161
Tarayıcıyı Nakletme.	162
Ayarları Yedekleme.	163
Ayarları dışa aktarın.	163
Ayarları alma.	164
Varsayılan Ayarları Geri Yükle.	164
Uygulamaları ve Bellenimi Güncelleme.	165
Kontrol Panelini Kullanarak Tarayıcının Bellenimini Güncelleme.	165
Web Config Kullanarak Bellenimi Güncelleme.	166
İnternet'e Bağlanmadan Bellenimi Güncelleme.	166

Giriş

Bu Belgenin İçeriği.	7
Bu Kılavuzu Kullanma.	7

Bu Belgenin İçeriği

Bu belge, tarayıcı yöneticileri için aşağıdaki bilgileri sunar.

- ☐ Ağ ayarları
- ☐ Tarama işlevini hazırlama
- ☐ Güvenlik ayarlarını etkinleştirin ve yönetin
- ☐ Kimlik Doğrulama Ayarları ögesini etkinleştirin ve yönetin
- ☐ Günlük bakım yapın

Tarayıcıyı kullanmanın standart yöntemleri için *Kullanım Kılavuzu* ögesine bakın.

Not:

Bu belge, bir kimlik doğrulama sunucusu kullanmak zorunda kalmadan bağımsız kimlik doğrulama sağlayan Kimlik Doğrulama Ayarları ögesini açıklar. Bu kılavuzda tanıtılan Kimlik Doğrulama Ayarları ögesine ek olarak, kimlik doğrulama sunucusunu kullanarak kimlik doğrulama sistemi de oluşturabilirsiniz. Bir sistem oluşturmak için Document Capture Pro Server Authentication Edition (kısa ad Document Capture Pro Server AE) ögesini kullanın.

Daha fazla bilgi için yerel Epson satıcınıza başvurun.

Bu Kılavuzu Kullanma

Marka ve Semboller



Dikkat:

Yaralanmayı önlemek için dikkatle takip edilmesi gereken talimatlardır.



Önemli:

Ekipmanınızın zarar görmesini önlemek için uyulması gereken talimatlardır.

Not:

Tamamlayıcı ve referans bilgiler sağlar.

İlgili Bilgi

➔ İlgili bölümlere bağlanır.

Bu Kılavuzda Kullanılan Açıklamalar

- ☐ Uygulamalara yönelik ekran görüntüleri Windows 10 ya da macOS High Sierra işletim sistemindendir. Ekranda görüntülenen içerik modele ve duruma bağlı olarak değişir.
- ☐ Bu kılavuzda kullanılan resimler yalnızca başvuru içindir. Asıl üründen biraz farklılık gösterebilir de, çalıştırma yöntemleri aynıdır.

İşletim Sistemi Referansları

Windows

Bu kılavuzda yer alan “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Server 2019”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012” ve “Windows Server 2008 R2” ifadeleri ile aşağıdaki işletim sistemleri kastedilmektedir. Ek olarak “Windows” tüm sürümler için kullanılır ve “Windows Server” “Windows Server 2019”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012” ve “Windows Server 2008 R2” için kullanılır.

- ☐ Microsoft® Windows® 10 işletim sistemi
- ☐ Microsoft® Windows® 8.1 işletim sistemi
- ☐ Microsoft® Windows® 8 işletim sistemi
- ☐ Microsoft® Windows® 7 işletim sistemi
- ☐ Microsoft® Windows Server® 2019 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

Mac OS

Bu kılavuzda, “Mac OS”; macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan ve OS X Yosemite ifade etmek için kullanılır.

Amacınıza Uygun Gerekli Ayarlar

Amacınıza Uygun Gerekli Ayarlar. 10

Amacınıza Uygun Gerekli Ayarlar

Amacınıza uygun gerekli ayarları yapmak için aşağıdakilere bakın.

Tarayıcıyı Ağa Bağlama

Amaç	Gerekli Ayarlar
Tarayıcıyı ağa bağlamak istiyorum.	Tarayıcınızı ağ taraması için ayarlayın. “Tarayıcıyı Ağa Bağlama” sayfa 13
Tarayıcıyı yeni bir bilgisayara bağlamak istiyorum.	Tarayıcınızın ağ ayarlarını yeni bilgisayarda yapın. “Bilgisayar veya Cihaz Ekleme veya Değiştirme” sayfa 19

Tarama İçin Ayarlar

Amaç	Gerekli Ayarlar
Taranan görüntüleri e-postayla göndermek istiyorum. (E-postaya Tara)	1. Bağlamak istediğiniz e-posta sunucusunu ayarlayın. “Posta Sunucusu Yapılandırma” sayfa 41 2. Alıcının e-posta adresini Kişiler içine kaydedin (isteğe bağlı). E-posta adresini kaydederek, bir şey göndermek istediğinizde bunu girmek zorunda kalmazsınız, bunu sadece Kişilerinizden seçebilirsiniz. “Kişileri Uygun Hale Getirme” sayfa 61
Taranan görüntüleri ağda bir klasöre kaydetmek istiyorum. (Ağ Klasörüne/FTP Sunucusuna Tara)	1. Görüntüleri kaydetmek istediğiniz ağ üzerinde bir klasör oluşturun. “Paylaşılan Bir Klasörünü Ayarlama” sayfa 44 2. Yolu Kişiler içindeki klasöre kaydedin (isteğe bağlı). Klasör yolunu kaydederek, bir şey göndermek istediğinizde bunu girmek zorunda kalmazsınız, bunu sadece Kişilerinizden seçebilirsiniz. “Kişileri Uygun Hale Getirme” sayfa 61
Taranan görüntüleri bulut hizmetine kaydetmek istiyorum. (Buluta Tara)	Epson Connect öğesini ayarlayın. Ayarlama ile ilgili ayrıntılar için Epson Connect portal web sitesine bakın. Ayarlanırken bağlamak istediğiniz çevrimiçi depolama hizmeti için bir kullanıcı hesabına gerek duyarsınız. https://www.epsonconnect.com/ http://www.epsonconnect.eu (yalnızca Avrupa)

Kontrol Paneli Ekranını Özelleştirme

Amaç	Gerekli Ayarlar
Tarayıcının kontrol panelinde görüntülenen öğeleri değiştirmek istiyorum.	Ön ayarlar veya Ana Ekranı Düzenle öğesini ayarlayın. Sık kullanılan tarama ayarlarınızı, kontrol paneline kaydedebilir ve görüntülenen öğeleri düzenleyebilirsiniz. “Kontrol Paneli Ekranını Özelleştirme” sayfa 74

Temel Güvenlik İşlevlerini Ayarlama

Amaç	Gerekli Ayarlar
Yönetici dışında herhangi birinin tarayıcı ayarlarını değiştirmesini önlemek istiyorum.	Tarayıcı için bir yönetici parolası ayarlayın. “Yönetici Ayarları” sayfa 83
USB bağlantılara sahip tarayıcıların kullanımını devre dışı bırakmak istiyorum.	Harici arayüzü devre dışı bırakın. “Harici Arayüzü Devre Dışı Bırakma” sayfa 89

Gelişmiş Güvenlik İşlevlerini Ayarlama

Amaç	Gerekli Ayarlar
Hangi protokolün kullanılacağını kontrol etmek istiyorum.	Protokolleri etkinleştirin veya devre dışı bırakın. “İletişim Kurallarını Denetleme ve Kullanma” sayfa 94
İletişim yolunu şifrelemek istiyorum.	1. Dijital sertifikanızı ayarlayın. “Dijital Sertifika Kullanımı” sayfa 97 2. SSL/TLS iletişimini ayarlayın. “Tarayıcıyla SSL/TLS İletişimi” sayfa 102
Şifreli iletişim kullanmak istiyorum (IPsec). Yazılımı sadece belirli bir bilgisayardan kullanabilmek istiyorum (IP filtreleme).	Trafiği filtrelemek için ilkeleri ayarlayın. “IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim” sayfa 104
Bir IEEE802.1X ağı içindeki bir tarayıcıyı kullanmak istiyorum.	Tarayıcı için IEEE802.1X ayarlayın. “Tarayıcıyı Bir IEEE802.1X Ağına Bağlama” sayfa 114

Tarayıcıyı tarafından Kimliği Doğrulanacak İşlevleri Ayarlama

Amaç	Gerekli Ayarlar
Kimlik Doğrulama Ayarları ögesini etkinleştirmek istiyorum.	Kullanılabilir Kimlik Doğrulama Ayarları ve Doğrulama Yöntemi hakkında daha fazla bilgi için aşağıdakine bakın. “Kimlik Doğrulama Ayarları Hakkında” sayfa 124 “Doğrulama Yöntemi Hakkında” sayfa 125

Bir Sunucunun Kimlik Doğrulama Sistemini Kullanma

Document Capture Pro Server Authentication Edition ile (kısa adı Document Capture Pro Server AE) kimlik doğrulama için bir sunucu kullanan bir kimlik doğrulama sistemi oluşturabilirsiniz.

Daha fazla bilgi için yerel Epson satıcınıza başvurun.

Ağ Ayarları

Tarayıcıyı Ağa Bağlama.	13
Bilgisayar veya Cihaz Ekleme veya Değıştirme.	19
Ağ Bağlantı Durumunu Kontrol Etme.	25
Ağ Özellikleri.	26
Sorunları Çözme.	30

Tarayıcıyı Ağa Bağlama

Bu kısımda, tarayıcının kontrol paneli kullanılarak tarayıcıyı ağa bağlama açıklanmaktadır.

Not:

Tarayıcınız ve bilgisayarınız aynı segmentin içindeyse, yükleyiciyi kullanarak da bağlayabilirsiniz.

☐ Web sitesinden ayarlama

Aşağıdaki web sitesine erişin ve ardından ürün adını girin. **Kurulum** ögesine gidin ve ardından, ayarlamayı başlatın.
<http://epson.sn>

☐ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücüler olan Windows bilgisayarlarına sahip kullanıcılar içindir)

Yazılım diskini bilgisayara takın ve ardından, ekrandaki talimatları izleyin.

Ağ Bağlantısını Yapmadan Önce

Ağa bağlamak için bağlantı için bağlantı yöntemini ve ayar bilgilerini önceden kontrol edin.

Bağlantı Ayarlarında Bilgi Toplama

Bağlanmak için gerekli ayar bilgilerini hazırlayın. Aşağıdaki bilgileri önceden kontrol edin.

Bölümler	Öğeler	Not
Cihaz bağlantı yöntemi	☐ Ethernet ☐ Wi-Fi	Tarayıcıyı ağa nasıl bağlayacağınıza karar verin. Kablolu LAN için LAN anahtarına bağlanın. Wi-Fi için erişim noktasının ağına bağlanın (SSID).
LAN bağlantısı bilgileri	☐ IP adresi ☐ Alt ağ maskesi ☐ Varsayılan ağ geçidi	Tarayıcıya atanacak IP adresine karar verin. IP adresini statik olarak atadığınızda, tüm değerler gerekir. DHCP işlevini kullanarak IP adresini dinamik olarak atadığınızda otomatik ayarlandığından bu bilgi gerekmez.
Wi-Fi bağlantısı bilgileri	☐ SSID ☐ Parola	Bunlar tarayıcının bağlandığı erişim noktasının SSID'si (ağ adı) ve parolasıdır. MAC adresi filtreleme ayarlanırsa tarayıcıyı kaydetmek için tarayıcının MAC adresini önceden kaydedin. Desteklenen standartlar için aşağıya bakın. "Ağ Özellikleri" sayfa 26
DNS sunucusu bilgileri	☐ Birincil DNS için IP adresi ☐ İkincil DNS için IP adresi	Bunlar DNS sunucuları belirtilirken gerekir. Sistemde gereksiz yapılandırma olduğunda ve ikincil bir DNS sunucusu olduğunda ikincil DNS ayarlanır. Küçük bir kuruluştaysanız ve DNS sunucusunu ayarlamadıysanız, yönlendiricinin IP adresini ayarlayın.

Bölümler	Öğeler	Not
Proxy sunucusu bilgileri	☐ Proxy sunucusu adı	İnternet'e intranetten erişmek için ağ ortamınız proxy sunucusunu kullanıyorsa ve tarayıcının doğrudan İnternet'e erişmesi işlevini kullanıyorsanız bunu ayarlayın. Aşağıdaki işlevler için tarayıcı doğrudan İnternet'e bağlanır. ☐ Epson Connect Hizmetleri ☐ Diğer şirketlerin bulut hizmetleri ☐ Bellenim güncellemesi ☐ Taranan görüntüleri SharePoint(WebDAV)'e gönderme
Bağlantı noktası numarası bilgileri	☐ Bırakılacak bağlantı noktası	Tarayıcının ve bilgisayarın kullandığı bağlantı noktası numarasını işaretleyin, sonra gerekirse güvenlik duvarı ile engellenen bağlantı noktasını serbest bırakın. Tarayıcı tarafından kullanılan bağlantı noktası numarası için aşağıya bakın. "Tarayıcı İçin Bağlantı Noktasını Kullanma" sayfa 29

IP Adresi Ataması

Bunlar aşağıdaki IP adresi ataması türleridir.

Statik IP adresi:

Önceden belirlenen IP adresini tarayıcıya (ana makine) manüel atayın.

Ağa bağlanma bilgilerinin (alt ağ maskesi, varsayılan ağ geçidi, DNS sunucusu vb.) manuel ayarlanması gerekir.

IP adresi aygıt kapatılsa bile değişmez, bu yüzden IP adresini değiştiremediğiniz bir ortam olmadan aygıtları yönetmek istediğinizde veya aygıtları IP adresini kullanarak yönetmek istediğinizde bu kullanışlıdır. Birçok bilgisayarın erişebildiği tarayıcı, sunucu vb. ayarlarını öneririz. Ayrıca, IPsec/IP filtreleme gibi güvenlik özellikleri kullanılırken sabit bir IP adresi atayın, böylece IP adresi değişmez.

DHCP işlevini (dinamik IP adresi) kullanarak otomatik atama:

IP adresini tarayıcıya (ana makine) DHCP sunucusunun veya yönlendiricinin DHCP işlevini kullanarak otomatik atayın.

Ağa bağlanma bilgileri (alt ağ maskesi, varsayılan ağ geçidi, DNS sunucusu vb.) otomatik ayarlanır, bu yüzden aygıtı ağa kolayca bağlayabilirsiniz.

Aygıt veya yönlendirici kapatılırsa veya DHCP sunucusu ayarlarına bağlı olarak yeniden bağlanırken IP adresi değişebilir.

IP adresi ve IP adresini izleyebilen protokollerle iletişim kurma dışında aygıtları yönetmenizi öneririz.

Not:

DHCP'nin IP adresi ayırma işlevini kullandığınızda, aynı IP adresini aygıtlara istediğiniz zaman atayabilirsiniz.

DNS Sunucusu ve Proxy Sunucusu

DNS sunucusunun IP adresi bilgileriyle ilişkilendirilmiş bir ana bilgisayar adı, e-posta adresinin etki alanı adı vb. vardır.

Bilgisayar veya tarayıcı IP iletişimi gerçekleştirirken diğer taraf ana bilgisayar adı, etki alanı adı vb. ile tanımlanıyorsa iletişim mümkün değildir.

O bilgi için DNS sunucusunu sorgular ve diğer tarafın IP adresini alır. Bu işlem ad çözümlemesi olarak adlandırılır.

Bu yüzden, bilgisayar ve tarayıcı gibi cihazlar IP adresi kullanılarak iletişim kurabilir.

E-posta işlevi veya İnternet bağlantısı işlevini kullanarak iletişim kurmak için tarayıcı için ad çözümlemesi gerekir.

Bu işlevleri kullanırken, DNS sunucusu ayarlarını yapın.

DHCP sunucusu veya yönlendiricinin DHCP işlevini kullanarak tarayıcının IP adresini atarken otomatik ayarlanır.

Proxy sunucusu ağ ve İnternet arasındaki ağ geçidine yerleştirilir ve bunlardan her biri yerine bilgisayar, tarayıcı ve İnternet (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.

İnternete proxy sunucusu yoluyla bağlandığınızda, tarayıcıdaki proxy sunucusunu yapılandırın.

Kontrol Panelinden Ağa Bağlanma

Tarayıcının kontrol panelini kullanarak tarayıcıyı ağa bağlayın.

IP Adresi Atama

Ana Bilgisayar Adresi, Alt Ağ Maskesi, Varsayılan Ağ Geçidi gibi temel öğeleri ayarlayın.

Bu bölümde statik bir IP adresi ayarlamak için prosedür açıklanmaktadır.

1. Tarayıcıyı açın.
2. Tarayıcı kontrol panelinin ana ekranında **Ayarlar** öğesini seçin.
3. **Ağ Ayarları** > **Gelişmiş** > **TCP/IP** öğesini seçin.
4. **IP Adresi Alın** için **Manuel** seçimini yapın.

Yönlendiricinin DHCP işlevini kullanarak IP adresini otomatik ayarladığınızda, **Otomatik** öğesini seçin. Bu durumda, adım 5 ile 6'deki **IP Adresi**, **Alt Ağ Maskesi** ve **Varsayılan Ağ Geçidi** öğesi de otomatik ayarlanır, bu yüzden adım 7'e gidin.

5. IP adresini girin.

◀ ve ▶ öğelerini seçerseniz odak nokta ile ayarlanan sonraki segmente veya önceki segmente taşınır.

Önceki ekranda yansıtılan değeri onaylayın.

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

Önceki ekranda yansıtılan değeri onaylayın.



Önemli:

IP Adresi, Alt Ağ Maskesi ve Varsayılan Ağ Geçidi birleşimi yanlışsa **Ayarı Başlat** devre dışıdır ve ardından,ki ayarlara geçilemez. Girişte bir hata olmadığını onaylayın.

7. Birincil DNS sunucusu için IP adresini girin.

Önceki ekranda yansıtılan değeri onaylayın.

Not:

IP adresi atama ayarları için **Otomatik** ögesini seçtiğinizde, **Manuel** veya **Otomatik** içinden DNS sunucusu ayarlarını seçebilirsiniz. DNS sunucusu adresini otomatik alamıyorsanız, **Manuel** ögesini seçin ve DNS sunucusu adresini girin. Sonra, ikincil DNS sunucusu adresini doğrudan girin. **Otomatik** ögesini seçerseniz adım 9'a gidin.

8. İkincil DNS sunucusu için IP adresini girin.

Önceki ekranda yansıtılan değeri onaylayın.

9. **Ayarı Başlat** ögesine dokununuz.

Proxy Sunucusunu Ayarlama

Aşağıdakilerin ikisi de doğruysa proxy sunucusunu ayarlayın.

☐ Proxy sunucusu İnternet bağlantısı için yapılmış.

☐ Tarayıcının Epson Connect hizmeti veya başka bir şirketin bulut hizmetleri gibi doğrudan İnternete bağlı olduğu bir işlevi kullanırken.

1. Giriş ekranında **Ayarlar** ögesini seçin.

IP adresi ayarından sonra ayarlar yaparken, **Gelişmiş** ekranı görüntülenir. Adım 3'e gidin.

2. **Ağ Ayarları** > **Gelişmiş** seçeneklerini seçin.

3. **Proxy Sunucu** ögesini seçin.

4. **Proxy Sunucu Ayarları** için **Kullan** seçimini yapın.

5. IPv4 veya FQDN biçimiyle proxy sunucusu için adresi girin.

Önceki ekranda yansıtılan değeri onaylayın.

6. Proxy sunucusu için bağlantı noktası numarasını girin.

Önceki ekranda yansıtılan değeri onaylayın.

7. **Ayarı Başlat** ögesine dokununuz.

Ethernet'e Bağlama

Tarayıcı LAN kablосunu kullanarak ağa bağlayın ve ardından bağlantıyı kontrol edin.

1. Tarayıcıyı ve hub'ı (LAN anahtarı) LAN kablосuyla bağlayın.

2. Ana ekranda  ögesini seçin.

3. **Yönlendirici** ögesini seçin.

4. Bağlantı ve IP Adresi ayarlarının doğru olduğundan emin olun.
5. **Kapat** ögesine dokununuz.

Kablosuz LAN'a Bağlanma (Wi-Fi)

Tarayıcıyı kablosuz LAN'a (Wi-Fi) birçok yolla bağlayabilirsiniz. Kullandığınız ortamla ve koşullarla eşleşen bağlantı yöntemini seçin.

SSID ve parola gibi kablosuz yönlendiriciye ait bilgileri biliyorsanız ayarları manuel yapabilirsiniz.

Kablosuz yönlendirici WPS'yi destekliyorsa düğme ayarı ile ayarları yapabilirsiniz.

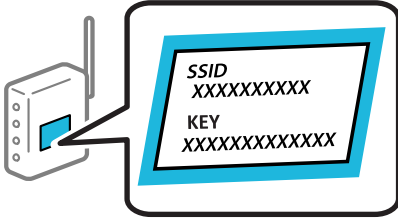
Tarayıcıyı ağa bağladıktan sonra, kullanmak istediğiniz cihazdan (bilgisayar, akıllı cihaz, tablet vb.) tarayıcıya bağlanın

SSID ve Parolayı Girerek Wi-Fi Ayarlarını Yapma

Tarayıcının kontrol panelinden kablosuz bir yönlendiriciye bağlanmak için gerekli bilgileri girerek bir Wi-Fi ağını ayarlayabilirsiniz. Bu yöntemi kullanarak ayarlamak için kablosuz bir yönlendirici için SSID ve parolaya ihtiyacınız vardır.

Not:

Varsayılan ayarlarıyla bir kablosuz yönlendirici kullanıyorsanız, SSID ve parola etiket üzerindedir. SSID ve parolayı bilmiyorsanız, kablosuz yönlendiriciyi ayarlayan kişiye başvurun veya kablosuz yönlendiriciyle sağlanan belgelere bakın.



1. Ana ekranda  ögesine dokununuz.

2. **Yönlendirici** ögesini seçin.

3. **Ayarı Başlat** ögesine dokununuz.

Ağ bağlantısı zaten ayarlandıysa bağlantı ayrıntıları görüntülenir. Ayarları değiştirmek için **Wi-Fi bağlantısına değiştirin.** veya **Ayarları Değiştir** ögesine dokununuz.

4. **Wi-Fi Kurulum Sihirbazı** ögesini seçin.

5. SSID'yi seçmek için ekrandaki talimatları izleyin, kablosuz yönlendirici için parolayı girin ve ayarları başlatın.

Kurulum tamamlandıktan sonra tarayıcı için ağ bağlantısı durumunu kontrol etmek istiyorsanız, ayrıntılar için aşağıdaki ilgili bilgiler bağlantısına bakın.

Not:

- ☐ SSID'yi bilmiyorsanız, kablosuz yönlendiricinin etiketinde yazıp yazmadığını kontrol edin. Varsayılan ayarlarıyla kablosuz yönlendiriciyi kullanıyorsanız, etikette yazılı SSID'yi kullanın. Bir bilgiyi bulamıyorsanız kablosuz yönlendiriciyle sağlanan belgelere bakın.
- ☐ Parola küçük/büyük harf duyarlıdır.
- ☐ Parolayı bilmiyorsanız, bilgilerin kablosuz yönlendiricinin etiketinde yazıp yazmadığını kontrol edin. Etiket, parola "Network Key", "Wireless Password" vb. yazılabilir. Varsayılan ayarlarıyla kablosuz yönlendiriciyi kullanıyorsanız, etikette yazılı parolayı kullanın.

İlgili Bilgi

➔ ["Ağ Bağlantı Durumunu Kontrol Etme" sayfa 25](#)

Düğme Kurulumu (WPS) ile Wi-Fi Ayarlarını Yapma

Kablosuz yönlendiricide bir düğmeye basarak bir Wi-Fi ağını otomatik ayarlayabilirsiniz. Aşağıdaki koşullar karşılandığında, bu yöntemi kullanarak ayarlayabilirsiniz.

- ☐ Kablosuz yönlendirici WPS (Wi-Fi Protected Setup) ile uyumludur.
- ☐ Kablosuz yönlendiricide bir düğmeye basarak geçerli Wi-Fi bağlantısı kurulmuştur.

Not:

Düğmeyi bulamıyorsanız veya yazılımı kullanarak ayarlarsanız, kablosuz yönlendiriciyle sağlanan belgelere bakın.

1. Ana ekranda  ögesine dokunun.

2. **Yönlendirici** ögesini seçin.

3. **Ayarı Başlat** ögesine dokunun.

Ağ bağlantısı zaten ayarlandıysa bağlantı ayrıntıları görüntülenir. Ayarları değiştirmek için **Wi-Fi bağlantısına değiştirin.** veya **Ayarları Değiştir** ögesine dokunun.

4. **Düğme Kurulumu (WPS)** ögesini seçin.

5. Ekrandaki talimatları izleyin.

Kurulum tamamlandıktan sonra tarayıcı için ağ bağlantısı durumunu kontrol etmek istiyorsanız, ayrıntılar için aşağıdaki ilgili bilgiler bağlantısına bakın.

Not:

Bağlantı başarısız olursa kablosuz yönlendiriciyi yeniden başlatın, tarayıcıya yaklaştırın ve yeniden deneyin.

İlgili Bilgi

➔ ["Ağ Bağlantı Durumunu Kontrol Etme" sayfa 25](#)

PIN Kodu Kurulumu (WPS) ile Wi-Fi Ayarlarını Yapma

Bir kablosuz yönlendiriciye bir PIN kodu kullanarak otomatik bağlanabilirsiniz. Bir kablosuz yönlendirici WPS (Wi-Fi Korunmalı Kurulumu) özellikliyse ayarlamak için bu yöntemi kullanabilirsiniz. Kablosuz yönlendiriciye bir PIN kodu girmek için bir bilgisayar kullanın.

1. Ana ekranda  ögesine dokunun.

2. **Yönlendirici** ögesini seçin.

3. **Ayarı Başlat** ögesine dokunun.

Ağ bağlantısı zaten ayarlandıysa bağlantı ayrıntıları görüntülenir. Ayarları değiştirmek için **Wi-Fi bağlantısına değiştirin.** veya **Ayarları Değiştir** ögesine dokunun.

4. **Diğerleri > PIN Kodu Kurulumu (WPS)** ögesini seçin

5. Ekrandaki talimatları izleyin.

Kurulum tamamlandıktan sonra tarayıcı için ağ bağlantısı durumunu kontrol etmek istiyorsanız, ayrıntılar için aşağıdaki ilgili bilgiler bağlantısına bakın.

Not:

Bir PIN kodu girme hakkında ayrıntılar için kablosuz yönlendiricinizle sağlanan belgelere bakın.

İlgili Bilgi

➔ “Ağ Bağlantı Durumunu Kontrol Etme” sayfa 25

Bilgisayar veya Cihaz Ekleme veya Değiştirme

Ağa Bağlı Bir Tarayıcıya Bağlanma

Tarayıcı ağa bağlandığında, bir bilgisayarı veya akıllı bir cihazı tarayıcıya ağ üzerinden bağlayabilirsiniz.

Ağ Tarayıcısını İkinci Bir Bilgisayardan Kullanma

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

☐ Web sitesinden ayarlama

Aşağıdaki web sitesine erişin ve ardından, ürün adını girin. **Kurulum** ögesine gidin ve ardından, ayarlamayı başlatın.

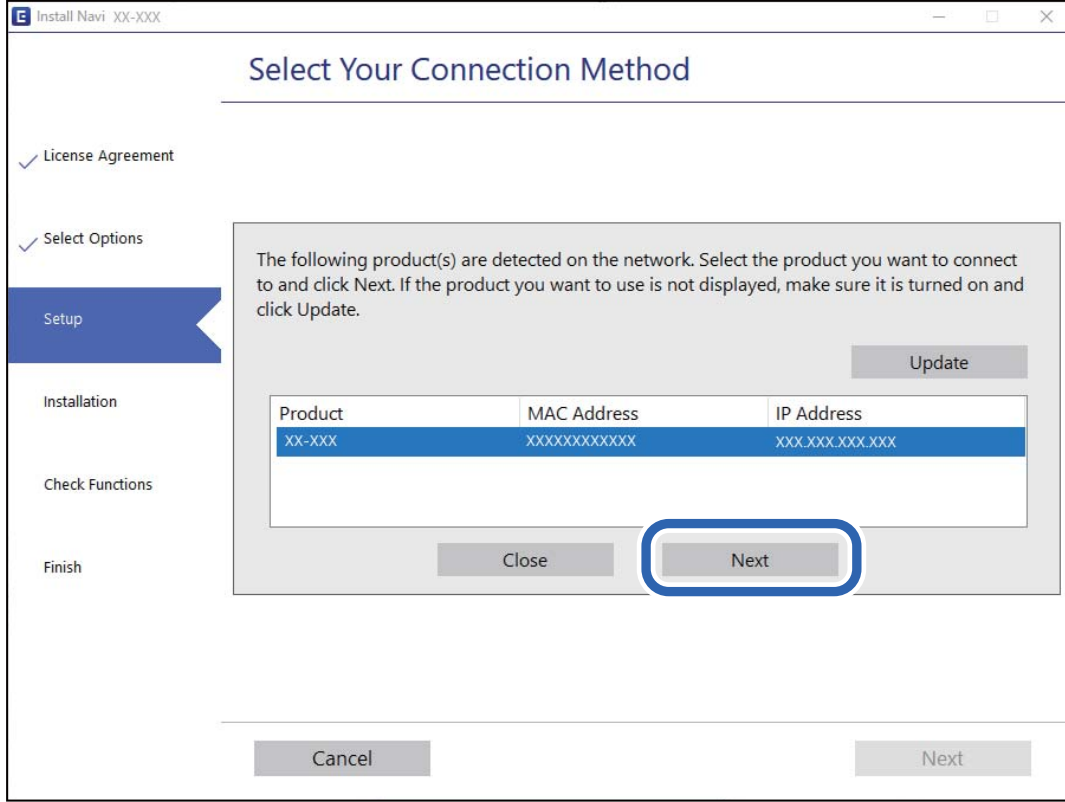
<http://epson.sn>

☐ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücülerini olan Windows bilgisayarlarına sahip kullanıcılar içindir).

Yazılım diskini bilgisayara takın ve ardından, ekrandaki talimatları izleyin.

Tarayıcıyı Seçme

Aşağıdaki ekran görüntülenene kadar ekrandaki talimatları izleyin, bağlanmak istediğiniz tarayıcı adını seçin ve ardından, **İleri** ögesine tıklayın.



Ekrandaki talimatları izleyin.

Ağ Tarayıcısını Akıllı Cihazdan Kullanma

Aşağıdaki yöntemlerden birini kullanarak bir akıllı cihazı tarayıcıyı bağlayabilirsiniz.

Kablosuz bir yönlendirici üzerinden bağlanma

Akıllı cihazı tarayıcıyla aynı Wi-Fi ağına (SSID) bağlayın.

Daha fazla ayrıntı için aşağıdaki kısma bakın.

[“Akıllı Cihaza Bağlanmak İçin Ayarlar Yapma” sayfa 24](#)

Wi-Fi Direct ile Bağlanma

Kablosuz bir yönlendirici olmadan akıllı cihazı tarayıcıya doğrudan bağlayın.

Daha fazla ayrıntı için aşağıdaki kısma bakın.

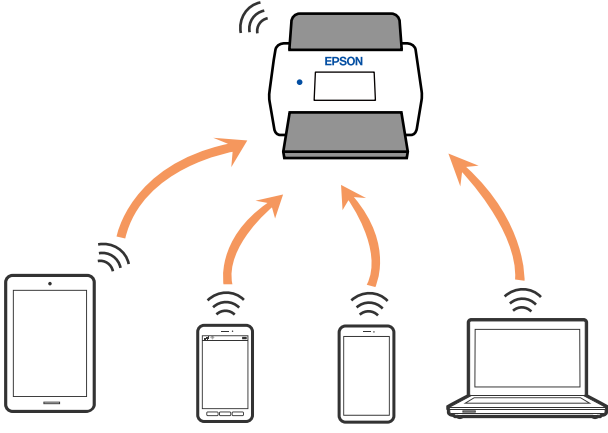
[“Akıllı Bir Cihazı ve Tarayıcıyı Doğrudan Bağlama \(Wi-Fi Direct\)” sayfa 21](#)

Akıllı Bir Cihazı ve Tarayıcıyı Doğrudan Bağlama (Wi-Fi Direct)

Wi-Fi Direct (Basit Erişim Noktası) akıllı bir cihazı kablosuz yönlendirici olmadan doğrudan tarayıcıya bağlamanızı ve akıllı cihazdan taramanızı sağlar.

Wi-Fi Direct Hakkında

Bu bağlantı yöntemini, evde ya da ofiste Wi-Fi kullanmadığınızda veya tarayıcıyı ve bilgisayarı ya da akıllı cihazı doğrudan bağlamak istediğinizde kullanın. Bu modda, tarayıcı bir kablosuz yönlendirici görevi görür ve standart bir kablosuz yönlendirici kullanmaya gerek kalmadan cihazları tarayıcıya bağlayabilirsiniz. Ancak, doğrudan tarayıcıya bağlı cihazlar tarayıcı yoluyla birbirleriyle iletişim kuramaz.



Tarayıcı Wi-Fi veya Ethernet ve Wi-Fi Direct (Basit Erişim Noktası) bağlantısıyla eşzamanlı olarak bağlanabilir. Ancak, tarayıcı Wi-Fi aracılığıyla bağlıyken Wi-Fi Direct (Basit Erişim Noktası) bağlantısıyla bir ağ bağlantısı başlatırsanız Wi-Fi bağlantısı geçici olarak kesilir.

Wi-Fi Direct'i Kullanarak Bir Akıllı Cihaza Bağlanma

Bu yöntem, bir kablosuz yönlendirici olmadan tarayıcıyı doğrudan akıllı cihazlara bağlamanızı sağlar.

1. Giriş ekranında  ögesini seçin.
2. **Wi-Fi Direct** ögesini seçin.
3. **Ayarı Başlat** ögesini seçin.
4. Akıllı cihazınızda Epson Smart Panel'i başlatın.
5. Tarayıcınıza bağlanmak için Epson Smart Panel'de görüntülenen talimatları izleyin.
Akıllı cihazınız tarayıcıya bağlandığında sonraki adıma geçin.
6. Tarayıcının kontrol panelinde **Tamam** ögesini seçin.

Wi-Fi Direct (Basit Erişim Noktası) Bağlantısını Kesme

Bir Wi-Fi Direct (Basit Erişim Noktası) bağlantısını devre dışı bırakmak için iki yöntem vardır; tarayıcının kontrol panelini kullanarak tüm bağlantıları devre dışı bırakabilirsiniz veya bilgisayardan veya akıllı cihazdan her bağlantıyı devre dışı bırakın.

Tüm bağlantıları devre dışı bırakmak istediğinizde,  > **Wi-Fi Direct** > **Ayarı Başlat** > **Değiştir** > **Wi-Fi Direct işlevini devre dışı bırak** öğesini seçin.



Önemli:

Wi-Fi Direct (Basit Erişim Noktası) bağlantısı devre dışı bırakıldığında, tüm bilgisayarlar ve Wi-Fi Direct (Basit Erişim Noktası) bağlantısında tarayıcıya bağlı akıllı cihazların bağlantısı kesilir.

Not:

Belirli bir cihazın bağlantısını kesmek istiyorsanız, bağlantıyı tarayıcıdan kesmek yerine cihazdan kesin. Wi-Fi Direct (Basit Erişim Noktası) bağlantısını cihazdan kesmek için aşağıdaki yöntemlerden birini kullanın.

- ☐ Tarayıcının ağ adına (SSID) olan Wi-Fi bağlantısını kesin.
- ☐ Başka bir ağ adına (SSID) bağlanın.

SSID Gibi Wi-Fi Direct (Basit Erişim Noktası) Ayarlarını Değiştirme

Wi-Fi Direct (Basit Erişim Noktası) bağlantısı etkinleştirildiğinde, ayarları  > **Wi-Fi Direct** > **Ayarı Başlat** > **Değiştir** içinden değiştirebilirsiniz, sonra aşağıdaki menü öğeleri görüntülenir.

Ağ Adını Değiştir

Tarayıcıya isteğe bağlı adınıza bağlamak için kullanılan Wi-Fi Direct (Basit Erişim Noktası) ağ adını (SSID) değiştirin. Kontrol panelinin yazılım klavyesinde görüntülenen ağ adını (SSID) ASCII karakterler olarak ayarlayabilirsiniz. En fazla 22 karakter girebilirsiniz.

Ağ adını (SSID) değiştirdiğinizde, bağlı tüm cihazların bağlantısı kesilir. Cihazı yeniden bağlamak istiyorsanız yeni ağ adını (SSID) kullanın.

Şifreyi Değiştir

Tarayıcıya bağlanmak için Wi-Fi Direct (Basit Erişim Noktası) parolasını istediğiniz değere değiştirin. Parolayı kontrol panelindeki yazılım klavyesinde görüntülenen ASCII karakterine ayarlayabilirsiniz. 8 ila 22 arasında karakter girebilirsiniz.

Parolayı değiştirdiğinizde, bağlı tüm cihazların bağlantısı kesilir. Cihazı yeniden bağlamak istiyorsanız yeni parolayı kullanın.

Frekans Aralığını Değiştir

Wi-Fi Direct'in tarayıcıya bağlanmak için kullanılan frekans aralığını değiştirin. 2,4 GHz veya 5 GHz'yi seçebilirsiniz.

Frekans aralığını değiştirirken, bağlı tüm cihazların bağlantısı kesilir. Cihazı yeniden bağlayın.

5 GHz'ye değiştirirken 5 GHz frekans aralığını desteklemeyen cihazlardan yeniden bağlanamayacağınızı unutmayın.

Bölgeye bağlı olarak bu ayar görüntülenmeyebilir.

Wi-Fi Direct işlevini devre dışı bırak

Tarayıcının Wi-Fi Direct (Basit Erişim Noktası) ayarlarını devre dışı bırakın. Devre dışı bırakırken Wi-Fi Direct (Basit Erişim Noktası) bağlantısındaki tarayıcıya bağlı tüm cihazların bağlantıları kesilir.

Varsayılan Ayarları Geri Yükle

Tüm Wi-Fi Direct (Basit Erişim Noktası) ayarlarını varsayılanlarına geri yükleyin.

Tarayıcıya bağlanan akıllı cihazın Wi-Fi Direct (Basit Erişim Noktası) bağlantısı bilgileri silinir.

Not:

Aşağıdaki ayarları Web Config'de Ağ sekmesi > **Wi-Fi Direct** ögesinden de ayarlayabilirsiniz.

- ☐ Wi-Fi Direct'i (Basit Erişim Noktası) etkinleştirme veya devre dışı bırakma
- ☐ Ağ adını değiştirme (SSID)
- ☐ Parolayı değiştirme
- ☐ Frekans aralığını değiştirme
Bölgeye bağlı olarak bu ayar görüntülenmeyebilir.
- ☐ Wi-Fi Direct (Basit Erişim Noktası) ayarlarını geri yükleme

Ağ Bağlantısını Yeniden Ayarlama

Bu kısımda ağ bağlantısı ayarlarının nasıl yapılacağı ve kablosuz yönlendirici veya bilgisayar değiştirilirken bağlantı yöntemini değiştirme açıklanmaktadır.

Kablosuz Yönlendiriciyi Değiştirirken

Kablosuz yönlendiriciyi değiştirdiğinizde, bilgisayar veya akıllı cihaz ve tarayıcı arasında bağlantı için ayarları yapın.

İnternet servis sağlayıcınızı vb. değiştirirseniz bu ayarları yapmanız gerekir.

Bilgisayara Bağlanmak İçin Ayarlar Yapma

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

- ☐ Web sitesinden ayarlama
Aşağıdaki web sitesine erişin ve ardından, ürün adını girin. **Kurulum** ögesine gidin ve ardından, ayarlamayı başlatın.
<http://epson.sn>
- ☐ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücüler olan Windows bilgisayarlarına sahip kullanıcılar içindir).
Yazılım diskini bilgisayara takın ve ardından, ekrandaki talimatları izleyin.

Bağlantı Yöntemlerini Seçme

Ekrandaki talimatları izleyin. **Operasyonunuzu Seçin** ekranında **Yazıcı bağlantısını tekrar kurun (yeni ağ yönlendirici veya USB'yi ağa değiştirme gibi durumlar için)** ögesini seçin ve ardından, **İleri** ögesine tıklayın.

Kurulumu bitirmek için ekrandaki talimatları izleyin.

Bağlanamazsınız sorunu çözmek için aşağıdakileri deneyin.

[“Bir Ağa bağlanılamıyor” sayfa 30](#)

Akıllı Cihaza Bağlanmak İçin Ayarlar Yapma

Tarayıcıyı akıllı cihazla aynı Wi-Fi ağına (SSID) bağladığınızda tarayıcıyı bir akıllı cihazdan kullanabilirsiniz. Tarayıcıyı bir akıllı cihazdan kullanmak için aşağıdaki web sitesine erişin ve ürün adını girin. **Kurulum** öğesine gidin ve ardından, ayarlamayı başlatın.

<http://epson.sn>

Tarayıcıyı bağlamak istediğiniz akıllı cihazdan web sitesine erişin.

Bilgisayarı Değiştirirken

Bilgisayarı değiştirirken, bilgisayar ve tarayıcı arasında bağlantı ayarlarını yapın.

Bilgisayara Bağlanmak İçin Ayarlar Yapma

Tarayıcıyı bir bilgisayara bağlamak için yükleyici kullanmanızı öneririz. Aşağıdaki yöntemi kullanarak yükleyiciyi çalıştırabilirsiniz.

☐ Web sitesinden ayarlama

Aşağıdaki web sitesine erişin ve sonra ürün adını girin. **Kurulum** öğesine gidin ve ardından, ayarlamayı başlatın.

<http://epson.sn>

☐ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücüler olan Windows bilgisayarlarına sahip kullanıcılar içindir).

Yazılım diskini bilgisayara takın ve ardından, ekrandaki talimatları izleyin.

Ekrandaki talimatları izleyin.

Bağlantı Yöntemini Bilgisayara Değiştirme

Bu kısımda bilgisayar ve tarayıcı bağlandığında bağlantı yöntemini değiştirme açıklanmaktadır.

Ağ Bağlantısını Ethernet’ren Wi-Fi’ye Değiştirme

Tarayıcının kontrol panelinden Ethernet bağlantısını Wi-Fi bağlantısına değiştirin. Bağlantı değiştirme yöntemi temel olarak Wi-Fi bağlantı ayarlarıyla aynıdır.

İlgili Bilgi

➔ [“Kablosuz LAN’a Bağlanma \(Wi-Fi\)” sayfa 17](#)

Ağ Bağlantısını Wi-Fi’den Ethernet’e Değiştirme

Bir Wi-Fi bağlantısından bir Ethernet bağlantısına değiştirmek için aşağıdaki adımları izleyin.

1. Giriş ekranında **Ayarlar** öğesini seçin.

2. **Ağ Ayarları** > **Kablolu LAN Ayarı** seçeneklerini seçin.
3. Ekrandaki talimatları izleyin.

USB'den Ağ Bağlantısına Değiştirme

Yükleyiciyi kullanın ve farklı bir bağlantı yöntemiyle yeniden ayarlayın.

☐ Web sitesinden ayarlama

Aşağıdaki web sitesine erişin ve ardından, ürün adını girin. **Kurulum** ögesine gidin ve ardından, ayarlamayı başlatın.

<http://epson.sn>

☐ Yazılım diskini kullanarak ayarlama (yalnızca bir yazılım diskiyle gelen modeller ve disk sürücülerine sahip kullanıcılar içindir).

Yazılım diskini bilgisayara takın ve ardından, ekrandaki talimatları izleyin.

Bağlantı Yöntemlerini Değiştirme Seçme

Ekrandaki talimatları izleyin. **Operasyonunuzu Seçin** ekranında **Yazıcı bağlantısını tekrar kurun (yeni ağ yönlendirici veya USB'yi ağa değiştirme gibi durumlar için)** ögesini seçin ve ardından, **İleri** ögesine tıklayın.

Kullanmak istediğiniz ağ bağlantısını, **Kablosuz ağ (Wi-Fi) aracılığıyla bağlan** veya **Kablolu LAN (Ethernet) aracılığıyla bağlan** ögesini seçin ve ardından, **İleri** ögesine tıklayın.

Kurulumu bitirmek için ekrandaki talimatları izleyin.

Ağ Bağlantı Durumunu Kontrol Etme

Aşağıdaki yolla ağ bağlantı durumunu kontrol edebilirsiniz.

Kontrol Panelinden Ağ Bağlantısı Durumunu Kontrol Etme

Tarayıcının kontrol panelindeki ağ simgesini veya ağ bilgilerini kullanarak ağ bağlantı durumunu kontrol edebilirsiniz.

Ağ Simgesini Kullanarak Ağ Bağlantısı Durumunu Kontrol Etme

Tarayıcının ana ekranındaki ağ simgesini kullanarak ağ bağlantı durumunu ve radyo dalgası gücünü kontrol edebilirsiniz.



	Ağ bağlantı durumunu görüntüler. Geçerli ayarları kontrol etmek ve değiştirmek için simgeyi seçin. Bu, aşağıdaki menünün kısayoldur. Ayarlar > Ağ Ayarları > Wi-Fi Ayarı	
		Tarayıcı bir kablosuz (Wi-Fi) ağa bağlı değil.
		Tarayıcı SSID arıyor, IP adresi ayarlanmamış veya kablosuz (Wi-Fi) ağda sorun var.
		Tarayıcı bir kablosuz (Wi-Fi) ağa bağlı. Çubuk sayısı, bağlantının sinyal gücünü belirtir. Ne kadar fazla çubuk varsa bağlantı o kadar güçlüdür.
		Tarayıcı Wi-Fi Direct (Basit Erişim Noktası) modunda bir kablosuz (Wi-Fi) ağa bağlı değil.
		Tarayıcı Wi-Fi Direct (Basit Erişim Noktası) modunda bir kablosuz (Wi-Fi) ağa bağlı.
		Tarayıcı kablolu (Ethernet) ağa bağlı değil veya ayarı kaldırılmış.
		Tarayıcı bir kablolu (Ethernet) ağa bağlı.

Kontrol Panelinde Ayrıntılı Ağ Bilgilerini Görüntüleme

Tarayıcınız ağa bağlandığında kontrol etmek istediğiniz ağ menülerini seçerek ağ ile ilgili diğer bilgileri de görüntüleyebilirsiniz.

1. Giriş ekranında **Ayarlar** ögesini seçin.
2. **Ağ Ayarları > Ağ Durumu** seçeneklerini seçin.
3. Bilgiyi kontrol etmek için kontrol etmek istediğiniz menüleri seçin.
 - ☐ Kablolu LAN/Wi-Fi Durumu
Ethernet veya Wi-Fi bağlantıları için ağ bilgilerini (cihaz adı, bağlantı, sinyal gücü vb.) görüntüler.
 - ☐ Wi-Fi Direct Durumu
Wi-Fi Direct'in ve SSID, parolasının vb. etkinleştirilip etkinleştirilmediğini görüntüler (Wi-Fi Direct bağlantıları için).
 - ☐ E-posta Sncu Drmu
E-posta sunucusu için ağ bilgilerini görüntüler.

Ağ Özellikleri

Wi-Fi Teknik Özellikleri

Wi-Fi özellikleri için aşağıdaki tabloya bakın.

Aşağıda listelenenler hariç ülkeler veya bölgeler	Tablo A
Avustralya Yeni Zelanda Tayvan Güney Kore	Tablo B

Tablo A

Standartlar	IEEE 802.11b/g/n ^{*1}
Frekans Aralığı	2.4 GHz
İletilen maksimum radyo frekansı gücü	2.400–2.483,5 MHz: 20 dBm (EIRP)
Kanallar	1/2/3/4/5/6/7/8/9/10/11/12/13
Bağlantı Modları	Altyapı, Wi-Fi Direct (Basit Erişim Noktası) ^{*2*}
Güvenlik Protokolleri ^{*4}	WEP (64/128bit), WPA2-PSK (AES) ^{*5} , WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Yalnızca HT20 için kullanılabilir

*2 IEEE 802.11b için desteklenmez

*3 Altyapı ve Wi-Fi Direct modları veya bir Ethernet bağlantısı eşzamanlı olarak kullanılabilir.

*4 Wi-Fi Direct, yalnızca WPA2-PSK (AES)'yi destekler.

*5 WPA/WPA2 Personal desteğine sahip WPA2 standartlarıyla uyumludur.

Tablo B

Standartlar	IEEE 802.11a/b/g/n ^{*1} /ac		
Frekans Aralıkları	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanallar	Wi-Fi	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 ^{*2} /13 ^{*2}
		5 GHz ^{*3}	W52 (36/40/44/48) W58 (149/153/157/161/165)
Bağlantı Modları	Altyapı, Wi-Fi Direct (Basit Erişim Noktası) ^{*4, *5}		
Güvenlik Protokolleri ^{*6}	WEP (64/128bit), WPA2-PSK (AES) ^{*7} , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Yalnızca HT20 için kullanılabilir

*2 Tayvan'da kullanılamaz

- *3 Bu kanalların kullanılabilirliği ve ürünün bu kanallar üzerinden dış mekanda kullanımı konuma göre değişir. Daha fazla bilgi için bkz. <http://support.epson.net/wifi5ghz/>
- *4 IEEE 802.11b için desteklenmez
- *5 Altyapı ve Wi-Fi Direct modları veya bir Ethernet bağlantısı eşzamanlı olarak kullanılabilir.
- *6 Wi-Fi Direct yalnızca WPA2-PSK (AES) destekler.
- *7 WPA/WPA2 Personal desteğine sahip WPA2 standartlarıyla uyumludur.

Ethernet Özellikleri

Standartlar	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (Enerji Verimli Ethernet)* ²
İletişim Modu	Otomatik, 10 Mb/sn Tam duplex, 10 Mb/sn Yarı duplex, 100 Mb/sn Tam duplex, 100 Mb/sn Yarı duplex
Konnektör	RJ-45

*1 Radyo etkileşimi riskini önlemek için bir kategori 5e veya üstü STP (Korumalı bükümlü çift) kablosu kullanın.

*2 Bağlı cihaz IEEE802.3az standartlarına uymalıdır.

Ağ İşlevleri ve IPv4/IPv6

İşlevler	Desteklenen
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Güvenlik Protokolü

IEEE802.1X*	
IPsec/IP Filtreleme	
SSL/TLS	HTTPS Sunucusu/İstemcisi
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* IEEE802.1X ile uyumlu bir bağlantı cihazı kullanmanız gerekir.

Tarayıcı İçin Bağlantı Noktasını Kullanma

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

Gönderen (İstemci) Tarayıcı Olduğunda

Kullan	Hedef (Sunucu)	Protokol	Bağlantı Noktası Numarası
Dosya gönderme (Ağ klasörüne tarama tarayıcıdan kullanıldığında)	FTP/FTPS sunucusu	FTP/FTPS (TCP)	20
			21
	Dosya sunucusu	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV sunucusu	Protokol HTTP (TCP)	80
		Protokol HTTPS(TCP)	443
E-posta gönderme (Postaya tarama tarayıcıdan kullanıldığında)	SMTP sunucusu	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
SMTP öncesinde POP bağlantısı (Tarayıcıdan postaya tara kullanılırken)	POP sunucusu	POP3 (TCP)	110
Epson Connect kullanıldığında	Epson Connect Sunucusu	HTTPS	443
		XMPP	5222
Kullanıcı bilgileri toplama (Tarayıcıdan kişileri kullanın)	LDAP sunucusu	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Kullanıcı bilgileri toplanırken kullanıcı kimlik doğrulaması (Tarayıcıdan kişileri kullanılırken)	KDC sunucusu	Kerberos	88
Tarayıcıdan ağ klasörüne tara (SMB) kullanıldığında kullanıcı kimlik doğrulaması			
Kontrol WSD	İstemci bilgisayarı	WSD (TCP)	5357
Bir uygulamadan itmeli taranırken bilgisayarı arayın	İstemci bilgisayarı	Ağdan İtmeli Tarama Bulma	2968

Gönderen (İstemci) İstemci Bilgisayar Olduğunda

Kullan	Hedef (Sunucu)	Protokol	Bağlantı Noktası Numarası
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
Bir uygulamadan tarama verilerini iletme	Tarayıcı	Ağdan Tarama (TCP)	1865
Bir uygulamadan itmeli tararken iş bilgilerini toplama	Tarayıcı	Ağdan İtmeli Tarama	2968
Web Config	Tarayıcı	HTTP (TCP)	80
		HTTPS (TCP)	443

Sorunları Çözme

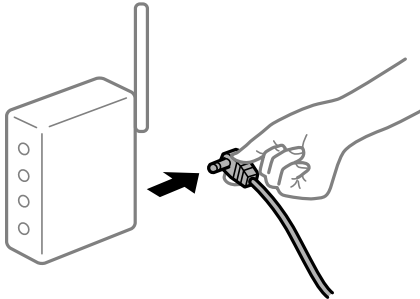
Bir Ağa bağlanılamıyor

Sorun aşağıdaki sorunlardan biri olabilir.

■ Wi-Fi bağlantısı için ağ cihazlarıyla ilgili bir şeyler yanlış.

Çözümler

Ağa bağlamak istediğiniz cihazları kapatın. Yaklaşık 10 saniye bekleyin ve ardından, cihazları şu sırayla açın; kablosuz yönlendirici, bilgisayar veya akıllı cihaz ve ardından, tarayıcı. Tarayıcı ve bilgisayarı veya akıllı cihazı radyo dalgası iletişimine yardımcı olmak için kablosuz yönlendiricinin yakınına taşıyın ve ardından, ağ ayarlarını yeniden yapmayı deneyin.



■ Araları çok açık olduğundan cihazlar kablosuz yönlendiriciden sinyalleri alamıyor.

Çözümler

Bilgisayarı veya akıllı cihazı ve tarayıcıyı kablosuz yönlendiricinin yakınına taşıdıktan sonra kablosuz yönlendiriciyi kapatın ve ardından, yeniden açın.

Kablosuz yönlendiriciyi değiştirirken, ayarlar yeni yönlendiriciyle eşleşmiyor.

Çözümler

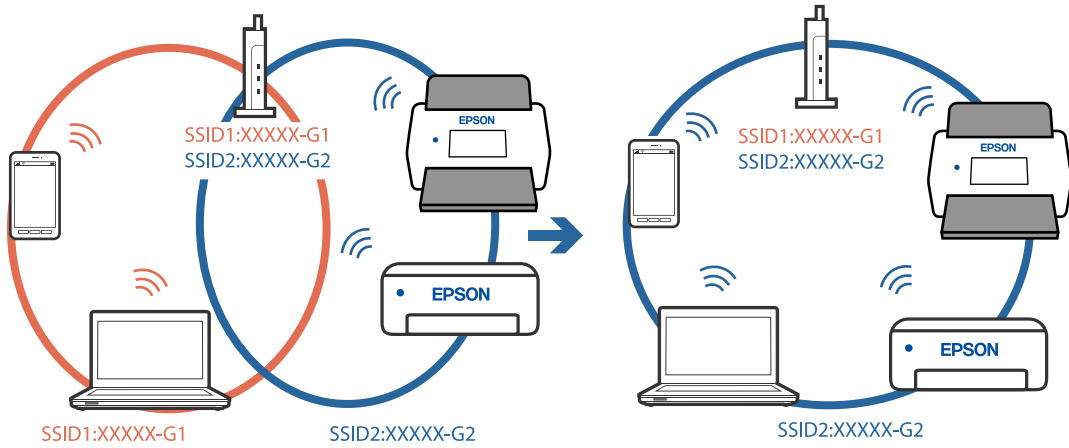
Bağlantı ayarlarını yeni kablosuz yönlendiriciyle eşleştirecek şekilde yeniden yapın.

Bilgisayardan veya akıllı cihazdan ve bilgisayardan bağlanan SSID'ler farklı.

Çözümler

Birden fazla kablosuz yönlendiriciyi aynı zamanda kullanırken veya kablosuz yönlendiricinin birden fazla SSID'si ve cihazı farklı SSID'lere bağlandığında, kablosuz yönlendiriciye bağlanamazsınız.

Bilgisayarı veya akıllı cihazı tarayıcıyla aynı SSID'ye bağlayın.



Kablosuz yönlendiricide özel bir ayraç bulunur.

Çözümler

Çoğu kablosuz yönlendiricide bağlı cihazlar arasındaki iletişimi engelleyen bir gizlilik ayırıcı özelliği bulunur. Aynı ağa bağlı olsalar bile tarayıcı ile bilgisayar veya akıllı cihaz arasında iletişim kuramıyorsanız, kablosuz yönlendiricideki gizlilik ayırıcısını devre dışı bırakın. Ayrıntılar için kablosuz yönlendiriciyle verilen kılavuza bakın.

IP adresi yanlış atanmış.

Çözümler

Tarayıcıya atanan IP adresi 169.254.XXX.XXX ve alt ağ maskesi 255.255.0.0 ise IP adresi doğru atanmamış olabilir.

Tarayıcının kontrol panelinde **Ayarlar > Ağ Ayarları > Gelişmiş > TCP/IP Ayarı** öğesini seçin ve ardından, IP adresinin ve alt ağ maskesinin tarayıcıya atandığını kontrol edin.

Kablosuz yönlendiriciyi yeniden başlatın veya tarayıcının ağ ayarlarını sıfırlayın.

Bilgisayardaki ağ ayarlarında bir sorun var.

Çözümler

Bilgisayarınızın ağ ayarlarının doğru olduğundan emin olmak için bilgisayarınızdan herhangi bir web sitesine erişmeye çalışın. Herhangi bir web sitesine erişemiyorsanız, bilgisayarda bir sorun olabilir.

Bilgisayarın ağ bağlantısını kontrol edin. Ayrıntılar için bilgisayarla sağlanan belgelere bakın.

Tarayıcı IEEE 802.3az (Enerji Tasarruflu Ethernet) destekleyen cihazlar kullanılarak Ethernet ile bağlandı.**Çözümler**

IEEE 802.3az (Enerji Tasarruflu Ethernet)'i destekleyen cihazlar kullanarak tarayıcıyı Ethernet ile bağlarken, kullandığınız hub veya yönlendiriciye bağlı olarak aşağıdaki sorunlar oluşabilir.

- ☐ Bağlantı tutarsız duruma gelir, art arda tarayıcı bağlanır ve bağlantısı kesilir.
- ☐ Tarayıcıya bağlanılamıyor.
- ☐ İletişim hızı yavaşlar.

Tarayıcı için IEEE 802.3az'yi devre dışı bırakmak için aşağıdaki adımları izleyin ve ardından, bağlanın.

1. Bilgisayara ve tarayıcıya bağlı Ethernet kablosunu çıkarın.
2. Bilgisayar için IEEE 802.3az etkinleştirildiğinde devre dışı bırakın.
Ayrıntılar için bilgisayarla sağlanan belgelere bakın.
3. Bilgisayarı ve tarayıcıyı bir Ethernet kablosuyla doğrudan bağlayın.
4. Tarayıcıda ağ ayarlarını kontrol edin.
Ayarlar > Ağ Ayarları > Ağ Durumu > Kablolu LAN/Wi-Fi Durumu ögesini seçin.
5. Tarayıcının IP adresini kontrol edin.
6. Bilgisayarda, Web Config'e erişin.
Bir Web tarayıcısını başlatın ve ardından, tarayıcının IP adresini girin.
["Web Tarayıcıda Web Yapılandırma Çalıştırma" sayfa 35](#)
7. **Ağ** sekmesi > **Kablolu LAN** ögesini seçin.
8. **IEEE 802.3az** için **Kapalı** seçimini yapın.
9. **İleri** ögesine tıklayın.
10. **Tamam** ögesine tıklayın.
11. Bilgisayara ve tarayıcıya bağlı Ethernet kablosunu çıkarın.
12. Adım 2'de bilgisayar için IEEE 802.3az'yi devre dışı bırakırsanız etkinleştirin.
13. Adım 1'de çıkardığınız Ethernet kablolarını bilgisayara ve tarayıcıya bağlayın.
Sorun hala devam ediyorsa tarayıcı dışındaki cihazlar soruna neden oluyor olabilir.

Tarayıcı kapalı.**Çözümler**

Tarayıcının açık olduğundan emin olun.

Ayrıca, tarayıcının tarama için hazır olduğunu gösteren durum ışığının yanıp sönmesi duruncaya kadar bekleyin.

Tarayıcıyı Ayarlamak için Yazılım

Web Config.	35
Epson Device Admin.	36

Web Config

Web Config, bilgisayar veya akıllı cihaz üzerindeki Internet Explorer ve Safari gibi web tarayıcılarda çalışan bir uygulamadır. Tarayıcı durumunu onaylayabilir ya da ağ servisini ve tarayıcı ayarlarını değiştirebilirsiniz. Tarayıcılar doğrudan ağ üzerinden erişildiğinden ve çalıştırıldığından, bir seferde bir tarayıcı kurmak için uygundur. Web Config kullanmak için bilgisayarınızı tarayıcının olduğu aynı ağa bağlayın.

Aşağıdaki tarayıcılar desteklenmektedir.

Microsoft Edge, Windows Internet Explorer 8 veya üstü, Firefox*, Chrome*, Safari*

* En yeni sürümü kullanın.

Web Tarayıcıda Web Yapılandırmayı Çalıştırma

1. Tarayıcının IP adresini kontrol edin.

Tarayıcının kontrol panelinde **Ayarlar > Ağ Ayarları > Ağ Durumu** ögesini seçin. Sonra tarayıcının IP adresini onaylamak için etkin bağlantı yöntemi durumunu (**Kablolu LAN/Wi-Fi Durumu** veya **Wi-Fi Direct Durumu**) seçin.

2. Bir bilgisayardan veya akıllı cihazdan bir Web tarayıcısı başlatın ve ardından, tarayıcının IP adresini girin.

Biçim:

IPv4: http://tarayıcının IP adresi/

IPv6: http://[tarayıcının IP adresi]/

Örnekler:

IPv4: http://192.168.100.201/

IPv6: http://[2001:db8::1000:1]/

Not:

Tarayıcı HTTPS'ye erişirken kendinden imzalı sertifika kullandığından, Web Config'i başlattığınızda tarayıcıda bir uyarı görüntülenir; bu, bir sorun olduğunu göstermez ve güvenle yoksayılabilir.

3. Tarayıcı ayarlarını değiştirmek için yönetici olarak oturum açın.

Ekranın sağ üstündeki **Yönetici Oturumu** ögesini tıklatın. **Kullanıcı Adı** ve **Mevcut parola** ögesini girin ve ardından, **Tamam** ögesini tıklatın.

Not:

☐ Aşağıda, Web Config yönetici bilgileri için başlangıç değerleri sağlanmaktadır.

· Kullanıcı adı: yok (boş)

· Şifre: tarayıcının seri numarası

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin.

☐ Ekranın sağ üstünde **Yönetici Oturum Kpt** görüntüleniyorsa zaten yönetici olarak oturum açmışsınız demektir.

Web Config üzerinde Windows ögesini çalıştırma

Bilgisayarı WSD ile tarayıcıya bağlarken Web Config ögesini çalıştırmak için aşağıdaki adımları uygulayın.

1. Bilgisayarda tarayıcı listesini açın.

☐ Windows 10

Başlat düğmesini tıklatın ve sonra **Windows Sistemi > Denetim Masası > Donanım ve Ses içinde Cihazları ve yazıcıları görüntüle** ögesini seçin.

☐ Windows 8.1/Windows 8

Masaüstü > Ayarlar > Denetim Masası > Donanım ve Ses (veya Donanım) kısmında yer alan **Cihazları ve yazıcıları görüntüle** ögesini seçin.

☐ Windows 7

Başlat düğmesine tıklayın ve **Denetim Masası > Cihazları ve yazıcıları görüntüle** seçeneklerini **Donanım ve Ses** bölümünden seçin.

2. Tarayıcınızı sağ tıklayın ve **Özellikler** ögesini seçin.

3. **Web Hizmeti** sekmesini seçin ve URL'ye tıklayın.

Tarayıcı HTTPS'ye erişirken kendinden imzalı sertifika kullandığından, Web Config'i başlattığınızda tarayıcıda bir uyarı görüntülenir; bu, bir sorun olduğunu göstermez ve güvenle yoksayılabilir.

Not:

- ☐ Aşağıda, Web Config yönetici bilgileri için başlangıç değerleri sağlanmaktadır.

· Kullanıcı adı: yok (boş)

· Şifre: tarayıcının seri numarası

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin.

- ☐ Ekranın sağ üstünde **Yönetici Oturum Kpt** görüntüleniyorsa zaten yönetici olarak oturum açmışsınız demektir.

Epson Device Admin

Epson Device Admin, ağdaki cihazları yönetmenizi sağlayan çok işlevli bir uygulamadır.

Bir ağdaki birden fazla tarayıcıya birleşik ayarlar uygulamak için yapılandırma şablonlarını kullanabilirsiniz ve böylece birden fazla tarayıcıyı kurmak ve yönetmek için uygun hale getirebilirsiniz.

Epson Device Admin ögesini Epson destek birimi web sitesinden indirebilirsiniz. Bu uygulamanın nasıl kullanılacağı ile ilgili ayrıntılar için Epson Device Admin belgelerine veya yardıma bakın.

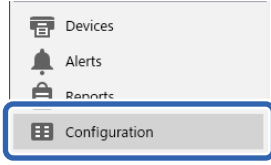
Yapılandırma Şablonu

Yapılandırma Şablonu Oluşturma

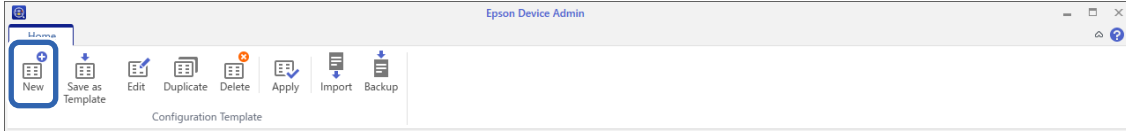
Yeni yapılandırma şablonu oluşturun.

1. Epson Device Admin programını başlatın.

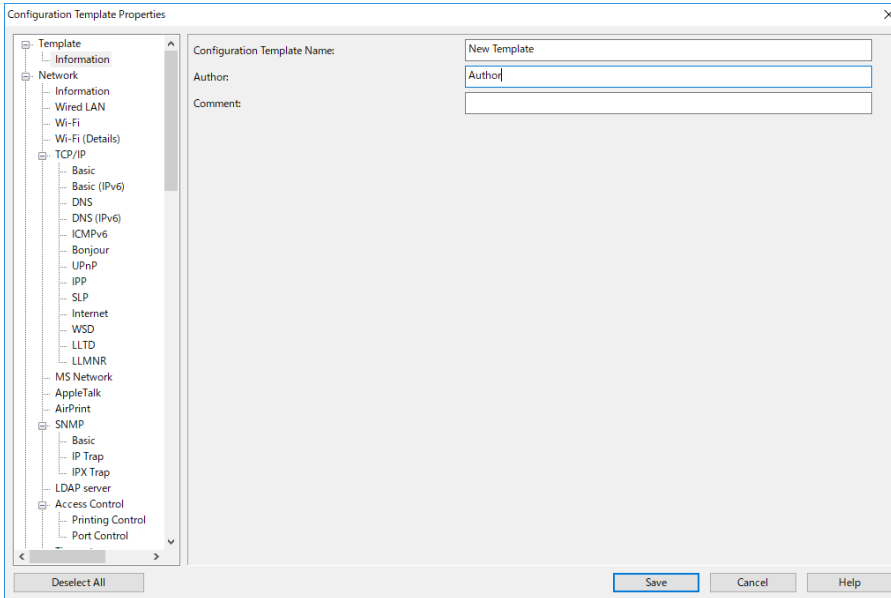
2. Yan çubuk görev menüsünde **Configuration** öğesini seçin.



3. Şerit menüsünde **New** öğesini seçin.



4. Her bir öğeyi ayarlayın.



Öge	Açıklama
Configuration Template Name	Yapılandırma şablonunu adı. Unicode (UTF-8) kısmına en fazla 1024 karakter girilebilir.
Author	Şablonun oluşturucusu hakkında bilgi. Unicode (UTF-8) kısmına en fazla 1024 karakter girilebilir.
Comment	İsteğe bağlı bilgileri girin. Unicode (UTF-8) kısmına en fazla 1024 karakter girilebilir.

5. Solda ayarlamak istediğiniz öğeleri seçin.

Not:

Her bir ekrana geçmek için soldaki menü öğelerine tıklayın. Ekranı değiştirirseniz, ancak ekranı iptal etmezseniz ayarlanan değer korunur. Tüm ayarları yapmayı tamamladığınızda, **Save** öğesine tıklayın.

Yapılandırma Şablonunu Uygulama

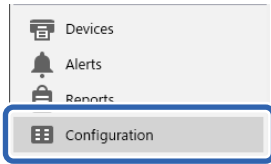
Kayıtlı yapılandırma şablonunu tarayıcıya uygulayın. Şablonda seçili öğeler uygulanır. Hedef tarayıcıda uygun bir işlev yoksa uygulanmaz.

Not:

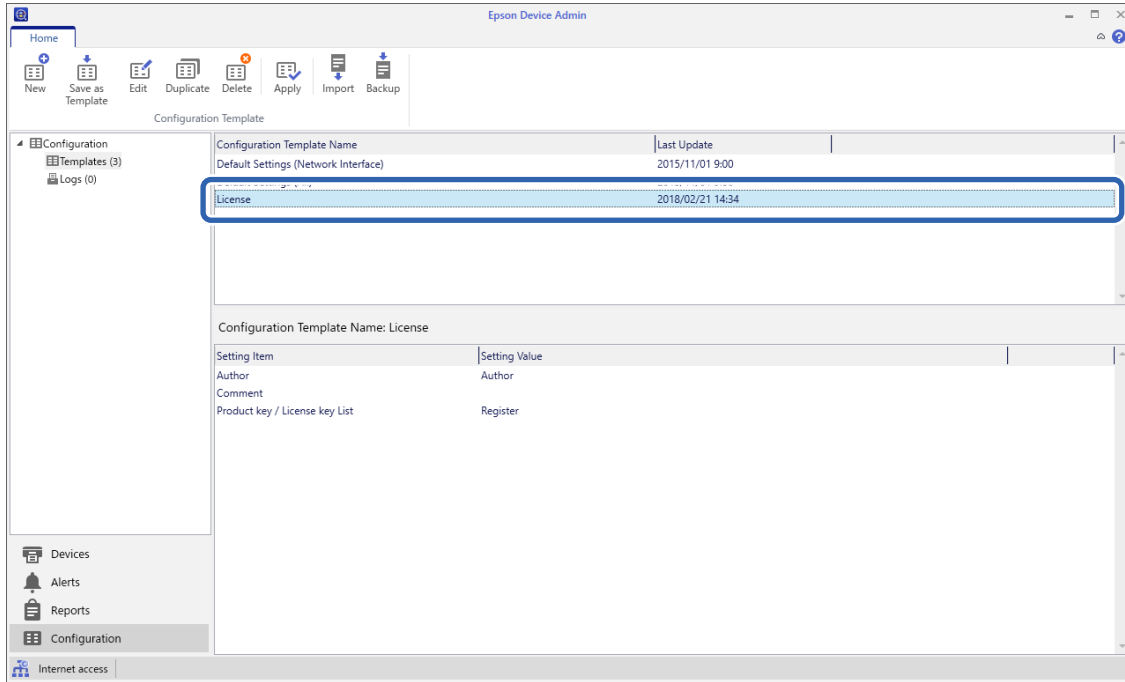
Yönetici parolası tarayıcıya ayarlandığında, parolayı önceden yapılandırın.

1. Aygıt Listesi ekranındaki şerit menüsünde **Options** > **Password manager** öğesini seçin.
2. **Enable automatic password management** öğesini seçin ve ardından **Password manager** öğesine tıklayın.
3. Uygun tarayıcıyı seçin ve ardından **Edit** öğesine tıklayın.
4. Parolayı ayarlayın ve sonra **OK** öğesine tıklayın.

1. Yan çubuk görev menüsünde **Configuration** öğesini seçin.

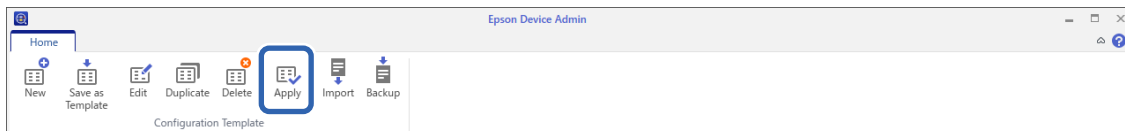


2. **Configuration Template Name** öğesinden uygulamak istediğiniz yapılandırma şablonunu seçin.



3. Şerit menüsünde **Apply** öğesine tıklayın.

Aygıt seçim ekranı görüntülenir.

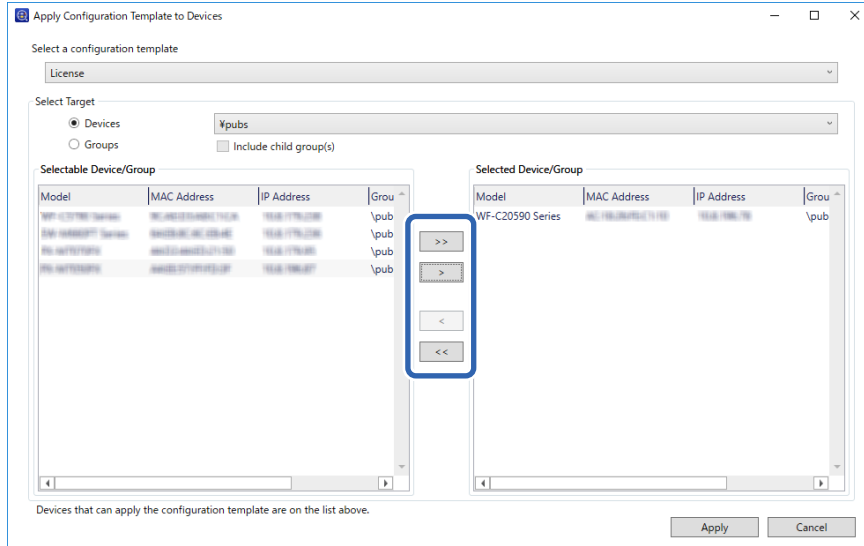


4. Uygulamak istediğiniz yapılandırma şablonunu seçin.

Not:

- ☐ Açılır menüden **Devices** öğesini ve aygıtları içeren grupları seçtiğinizde her aygıt görüntülenir.
- ☐ **Groups** öğesini seçtiğinizde gruplar görüntülenir. Seçili grup içinde alt grupları otomatik seçmek için **Include child group(s)** öğesini seçin.

5. Şablonu uygulamak istediğiniz aygıtları veya grupları **Selected Device/Group** öğesine taşıyın.



6. **Apply** öğesine tıklayın.

Uygulanacak yapılandırma şablonu için bir onay ekranı görüntülenir.

7. Yapılandırma şablonunu uygulamak için **OK** öğesine tıklayın.

8. İşlemin tamamlandığını bildiren bir mesaj görüntülendiğinde, **OK** öğesine tıklayın.

9. **Details** öğesine tıklayın ve bilgileri kontrol edin.

Uyguladığınız öğelerde ☒ görüntülendiğinde, uygulama başarıyla tamamlanmıştır.

10. **Close** öğesine tıklayın.

Tarama İçin Gerekli Ayarlar

Posta Sunucusu Yapılandırma.	41
Paylaşılan Bir Klasörünü Ayarlama.	44
Kişileri Uygun Hale Getirme.	61
Document Capture Pro Server'yi Kullanma.	70
AirPrint Ayarlama.	71
Ağ Taramaya Hazırlanırken Sorunlar.	71

Posta Sunucusu Yapılandırma

Web Config'den posta sunucusunu ayarlayın.

Tarayıcı posta sunucusunu ayarlayarak e-postayı gönderebildiğinde aşağıdaki mümkündür.

- ☐ E-posta kullanarak tarama sonuçlarını aktarır
- ☐ Tarayıcıdan e-posta bildirimini alır

Ayarlamadan önce kontrol edin.

- ☐ Tarayıcı posta sunucusuna erişebileceği ağa bağlı.
- ☐ Tarayıcıyla aynı posta sunucusunu kullanan bilgisayarın e-posta ayarı bilgileri.

Not:

- ☐ *Internet'te posta sunucusunu kullanırken, ayar bilgilerini sağlayıcıdan veya web sitesinden onaylayın.*
- ☐ *Posta sunucusunu tarayıcının kontrol panelinden de ayarlayabilirsiniz. Aşağıdaki gibi erişin.*
Ayarlar > Ağ Ayarları > Gelişmiş > E-posta Sncsu > Sncu Ayarları

1. Web Config'e erişin ve **Ağ** sekmesi > **E-posta Sncsu** > **Temel** ögesini seçin.
2. Her öge için bir değer girin.
3. **Tamam** ögesini seçin.
Seçtiğiniz ayarlar görüntülenir.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Posta Sunucusu Ayarlama Öğeleri

Öğeler	Ayarlar ve Açıklama	
Doğrulama Yöntemi	Tarayıcının posta sunucusuna erişimi için kimlik doğrulama yöntemini belirtin.	
	Kapalı	Bir posta sunucusuyla iletişim kurarken kimlik doğrulama devre dışı bırakılır.
	SMTP Doğrulaması	Bir posta sunucusunun SMTP Kimlik Doğrulamasını desteklemesini gerektirir.
	SMTP öncesinde POP	Yöntemi seçerken POP3 sunucusunu yapılandırın.
Doğrulama Hesabı	SMTP Doğrulaması olarak SMTP öncesinde POP veya Doğrulama Yöntemi seçimini yaparsanız, ASCII (0x20–0x7E) biçimli 0 ila 255 karakterden oluşan kimlik doğrulaması yapılmış hesap adını girin.	
Doğrulan Parola	Doğrulama Yöntemi olarak SMTP Doğrulaması veya SMTP öncesinde POP ögesini seçerseniz, ASCII (0x20–0x7E) biçimli 0 ila 20 karakterden oluşan kimlik doğrulaması yapılmış parolayı girin.	
Gönderenin Eposta Adresi	Göndericinin e-posta adresini girin. ASCII (0x20–0x7E) olarak şunlar hariç 0 ve 255 karakter arası girin : () < > [] ; ¥. Başlangıç karakteri olarak "." kullanılamaz.	

Öğeler	Ayarlar ve Açıklama
SMTP Sunucusu Adresi	Şunları kullanarak 0 ila 255 arası karakter girin A–Z a–z 0–9 . - . IPv4 ya da FQDN formatını kullanabilirsiniz.
SMTP Sunucusu Port Numarası	1 ile 65535 arasında bir sayı girebilirsiniz.
Güvenli Bağlantı	E-posta sunucusu için güvenli bağlantı yöntemini belirleyin.
	Hiçbiri SMTP öncesinde POP kısmında Doğrulama Yöntemi seçimini yaparsanız bağlantı yöntemi Hiçbiri olarak ayarlanır.
	SSL/TLS Bu, Doğrulama Yöntemi özelliği Kapalı veya SMTP Doğrulaması olarak ayarlandığında kullanılabilir.
	STARTTLS Bu, Doğrulama Yöntemi özelliği Kapalı veya SMTP Doğrulaması olarak ayarlandığında kullanılabilir.
Sertifika Doğrulama	Bu etkinleştirildiğinde sertifika doğrulanır. Bunun Etkinleştir olarak ayarlanmasını öneririz.
POP3 Sunucusu Adresi	SMTP öncesinde POP öğesini Doğrulama Yöntemi 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 Sunucusu Port Numarası	SMTP öncesinde POP öğesini Doğrulama Yöntemi olarak seçerseniz 1 ve 65535 arasında bir sayı girin.

Posta Sunucusu Bağlantı Kontrolü

Bağlantı kontrolünü gerçekleştirerek posta sunucusuna olan bağlantıyı kontrol edebilirsiniz.

1. Web Config'e erişin ve **Ağ** sekmesi > **E-posta Sncsu** > **Bağlantı Testi** öğesini seçin.
2. **Başlat** öğesini seçin.

Posta sunucusuna bağlantı testi başlatılır. Testten sonra kontrol raporu görüntülenir.

Not:

Kontrol panelinden posta sunucusuna olan bağlantıyı da kontrol edebilirsiniz. Aşağıdaki gibi erişin.

Ayarlar > Ağ Ayarları > Gelişmiş > E-posta Sncsu > Bağlantı Kontrolü

Posta Sunucusu Bağlantı Kontrolü Referansları

Mesajlar	Neden
Bağlantı testi başarılı oldu.	Bu mesaj sunucu ile bağlantı başarılı olduğunda görünür.
SMTP sunucusu iletişim hatası. Aşağıdakini kontrol edin. - Ağ Ayarları	Bu mesaj şu durumlarda görünür ☐ Tarayıcınız ağa bağlı olmadığında ☐ SMTP sunucusu kapalıyken ☐ Ağ bağlantısı iletişim kurulurken devre dışı bırakıldı ☐ Tamamlanmamış veriler alındı

Mesajlar	Neden
POP3 sunucusu iletişim hatası. Aşağıdakileri kontrol edin. - Ağ Ayarları	Bu mesaj şu durumlarda görünür ☐ Tarayıcınız ağa bağlı olmadığına ☐ POP3 sunucusu kapalıyken ☐ Ağ bağlantısı iletişim kurulurken devre dışı bırakıldı ☐ Tamamlanmamış veriler alındı
SMTP sunucusuna bağlanırken bir hata oluştu. Aşağıdakileri kontrol edin. - SMTP Sunucusu Adresi - DNS Sunucusu	Bu mesaj şu durumlarda görünür ☐ Bir DNS sunucusuna bağlanılamadı ☐ Bir SMTP sunucusu için ad çözülmedi
POP3 sunucusuna bağlanırken bir hata oluştu. Aşağıdakileri kontrol edin. - POP3 Sunucusu Adresi - DNS Sunucusu	Bu mesaj şu durumlarda görünür ☐ Bir DNS sunucusuna bağlanılamadı ☐ Bir POP3 sunucusu için ad çözülmedi
SMTP sunucusu kimlik doğrulama hatası. Aşağıdakileri kontrol edin. - Kimlik Doğrulama Yöntemi - Kimliği Doğrulanmış Hesap - Kimliği Doğrulanmış Şifre	Bu mesaj SMTP sunucusu kimlik doğrulaması başarısız olduğunda görünür.
POP3 sunucusu kimlik doğrulama hatası. Aşağıdakileri kontrol edin. - Kimlik Doğrulama Yöntemi - Kimliği Doğrulanmış Hesap - Kimliği Doğrulanmış Şifre	Bu mesaj POP3 sunucusu kimlik doğrulaması başarısız olduğunda görünür.
Desteklenmeyen iletişim yöntemi. Aşağıdakileri kontrol edin. - SMTP Sunucusu Adresi - SMTP Sunucusu Bağlantı Noktası Numarası	Bu mesaj desteklenmeyen protokollerle iletişim kurulmaya çalışıldığında görünür.
SMTP sunucusuna bağlanılamadı. Güvenli Bağlantı ayarını Hiçbiri olarak değiştirin.	Bu mesaj bir sunucu ve bir istemci arasında bir SMTP eşleşmemesi oluştuğunda veya sunucu SMTP güvenli bağlantısını (SSL bağlantısı) desteklemediğinde görünür.
SMTP sunucusuna bağlanılamadı. Güvenli Bağlantı ayarını SSL/TLS olarak değiştirin.	Bu mesaj bir sunucu ve bir istemci arasında bir SMTP eşleşmemesi oluştuğunda veya SMTP güvenli bağlantısı için sunucu bir SSL/TLS bağlantısı istediğinde görünür.
SMTP sunucusuna bağlanılamadı. Güvenli Bağlantı ayarını STARTTLS olarak değiştirin.	Bu mesaj bir sunucu ve bir istemci arasında bir SMTP eşleşmemesi oluştuğunda veya SMTP güvenli bağlantısı için sunucu bir STARTTLS bağlantısı istediğinde görünür.
Bağlantı güvenli değil. Aşağıdakileri kontrol edin. - Tarih ve Saat	Bu mesaj tarayıcının tarih ve saat ayarı yanlış olduğunda veya sertifika sona erdiğinde görünür.
Bağlantı güvenli değil. Aşağıdakileri kontrol edin. - CA Sertifikası	Bu mesaj tarayıcıda sunucuyla ilgili bir kök sertifikası olmadığında veya bir CA Sertifikası alınmadığında görünür.
Bağlantı güvenli değil.	Bu mesaj alınan sertifika hasar gördüğünde görünür.
SMTP sunucusu kimlik doğrulaması başarısız oldu. Kimlik Doğrulama Yöntemini SMTP-AUTH olarak değiştirin.	Bu mesaj bir sunucu ve bir istemci arasında bir kimlik doğrulama yöntemi eşleşmemesi oluştuğunda görünür. Sunucu SMTP Doğrulaması'ı destekler.

Mesajlar	Neden
SMTP sunucusu kimlik doğrulaması başarısız oldu. Kimlik Doğrulama Yöntemini SMTP ayarından önce POP olarak değiştirin.	Bu mesaj bir sunucu ve bir istemci arasında bir kimlik doğrulama yöntemi eşleşmemesi oluştuğunda görünür. Sunucu SMTP Doğrulaması'ı desteklemez.
Gönderenin E-posta Adresi yanlış. E-posta hizmetinize yönelik e-posta adresine değiştirin.	Bu mesaj belirtilen gönderenin E-posta adresi yanlış olduğunda görünür.
İşlem tamamlanana kadar ürüne erişilemez.	Tarayıcı meşgulken bu mesaj görünür.

Paylaşılan Bir Klasörünü Ayarlama

Taranan bir görüntüyü kaydetmek için paylaşılan bir ağ klasörü ayarlayın.

Bir dosyayı klasöre kaydederken, tarayıcı, klasörün oluşturulduğu bilgisayarın kullanıcısı olarak oturum açar.

Paylaşılan Klasör Oluşturma

İlgili Bilgi

- ➔ “Paylaşılan Klasör Oluşturmadan Önce” sayfa 44
- ➔ “Ağ Profilini Kontrol Etme” sayfa 44
- ➔ “Paylaşılan Klasörün Oluşturulduğu Konum ve Güvenlik Örneği” sayfa 45
- ➔ “Erişime İzin Verilen Grup veya Kullanıcı Ekleme” sayfa 58

Paylaşılan Klasör Oluşturmadan Önce

Paylaşılan klasör oluşturmadan önce aşağıdakileri kontrol edin.

- ☐ Tarayıcı, paylaşılan klasörün oluşturulacağı bilgisayara erişebileceğiniz bir ağa bağlı.
- ☐ Bir çok baytlı karakter paylaşılan klasörün oluşturulacağı bilgisayarın adına eklenir.



Önemli:

Birden fazla baytlı karakter bilgisayar adına eklendiğinde, dosyayı paylaşılan klasöre kaydetme başarısız olabilir.

Bu durumda, Çok baytlı karakter ada eklenmeyecek veya bilgisayar adı değiştirilmeyecek şekilde bilgisayarı değiştirin.

Bilgisayar adını değiştirirken, bilgisayar yönetimi, kaynak erişimi vb. gibi bazı ayarları etkileyebileceğinden yöneticiyle önceden onayladığınızdan emin olun.

Ağ Profilini Kontrol Etme

Paylaşılan klasörün oluşturulacağı bilgisayarda, klasör paylaşımının mümkün olup olmadığını kontrol edin.

1. Yönetici yetkisi kullanıcı hesabı ile paylaşılan klasörün oluşturulacağı bilgisayarda oturum açın.
2. **Denetim Masası > Ağ ve İnternet > Ağ ve Paylaşım Merkezi** ögesini seçin.
3. **Gelişmiş paylaşım ayarlarını değiştir** ögesine tıklayın ve ardından, görüntülenen ağ profillerinde (**geçerli profil**), içeren profil için  ögesine tıklayın.
4. **Dosya ve yazıcı paylaşımını aç** ögesinin **Dosya ve Yazıcı Paylaşımı** ögesinde seçili olup olmadığını kontrol edin.
Zaten seçilmediyse **İptal** ögesine tıklayın ve pencereyi kapatın.
Ayarları değiştirdiğinizde, **Değişiklikleri Kaydet** ögesine tıklayın ve pencereyi kapatın.

Paylaşılan Klasörün Oluşturulduğu Konum ve Güvenlik Örneği

Paylaşılan klasörün oluşturulduğu konuma bağlı olarak, güvenlik ve uygunluk değişir.

tarayıcılardan veya başka bilgisayarlardan paylaşılan klasörü çalıştırmak için klasör için aşağıdaki okuma ve izinleri değiştirme gerekir.

☐ **Paylaşım** sekmesi > **Gelişmiş Paylaşım > İzinler**

Paylaşılan klasörün ağ erişim iznini kontrol eder.

☐ **Güvenlik** sekmesinin erişim izni

Paylaşılan klasörün ağ erişiminin ve yerel erişiminin iznini kontrol eder.

Masaüstünde oluşturulan **Herkes** ögesini paylaşılan klasöre ayarladığınızda, paylaşılan bir klasör oluşturma örneği olarak bilgisayara erişebilen tüm kullanıcıların erişimine izin verilecektir.

Ancak, masaüstü (klasör) kullanıcı klasörünün kontrolü altında olduğundan yetkisi olmayan kullanıcı bunlara erişemez ve ardından, kullanıcı klasörünün güvenlik ayarları ona geçirilir. **Güvenlik** sekmesine erişim izni olan kullanıcı (oturum açan kullanıcı ve bu durumda yönetici) klasörü çalıştırabilir.

Uygun konum oluşturmak için aşağıya bakın.

Bu örnek “scan_folder” oluşturmayı gösterir.

İlgili Bilgi

➔ “Dosya Sunucuları İçin Yapılandırma Örneği” sayfa 45

➔ “Kişisel Bilgisayar İçin Yapılandırma Örneği” sayfa 52

Dosya Sunucuları İçin Yapılandırma Örneği

Bu açıklama, aşağıdaki koşul altında dosya sunucusu gibi paylaşılan bilgisayarda sürücünün klasöründe paylaşılan klasör oluşturma örneğidir.

Paylaşılan bir klasör oluşturmak için bilgisayarın aynı etki alanına sahip kişi gibi erişimi kontrol edilebilir kullanıcılar paylaşılan klasöre erişebilir.

Herhangi bir kullanıcının dosya sunucusu ve paylaşılan bilgisayar gibi bilgisayardaki paylaşılan klasörü okumasına ve yazmasına izin verdiğinizde bu yapılandırmayı ayarlayın.

☐ Paylaşılan klasör oluşturma yeri: Sürücünün kökü

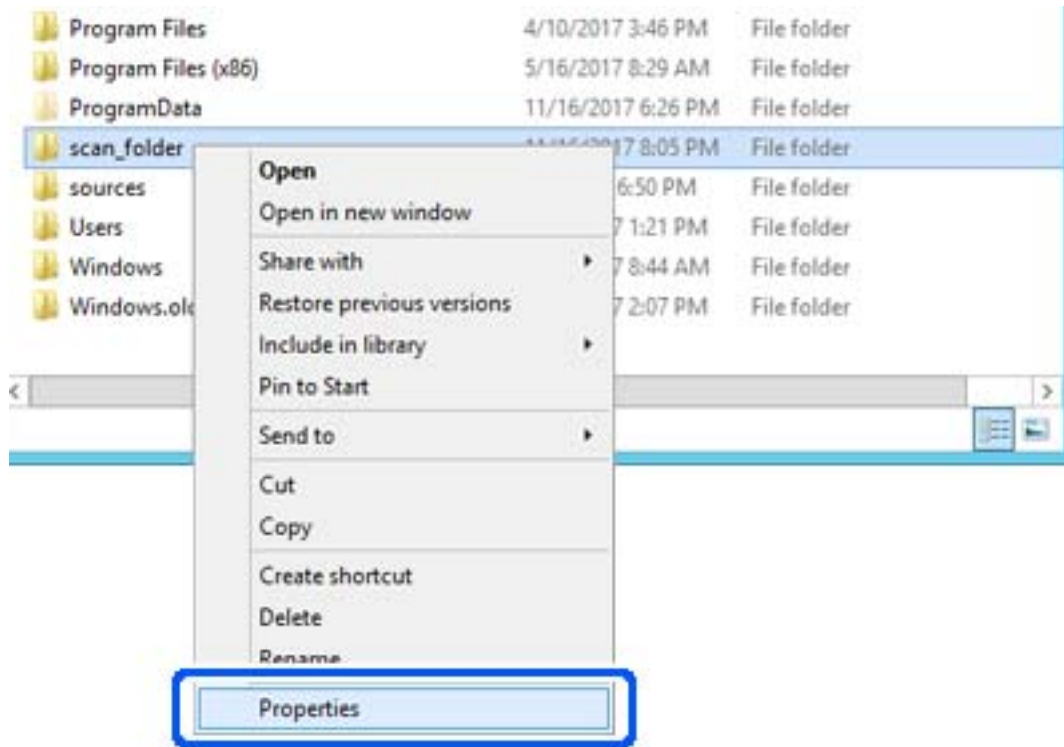
☐ Klasör yolu: C:\scan_folder

- ☐ Ağ yoluyla erişim izni (Paylaşım İzinleri): Herkes
- ☐ Dosya sistemindeki erişim izni (Güvenlik): Kimliği Doğrulanmış Kullanıcılar

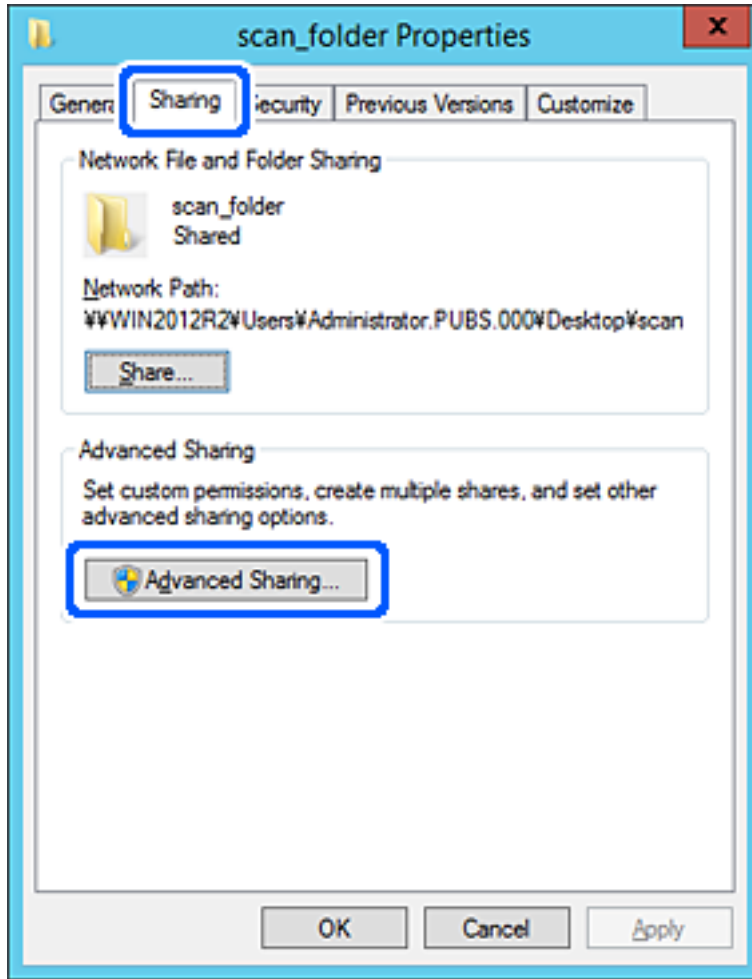
1. Yönetici yetkisi kullanıcı hesabı ile paylaşılan klasörün oluşturulacağı bilgisayarda oturum açın.
2. Gezgini başlatın.
3. Sürücünün kökünde klasör oluşturun ve ardından, “scan_folder” olarak adlandırın.

Klasör adı için 1 ve 12 alfasayısal karakter arasında bir değer girin. Klasör adının karakter sınırı aşılsa değişen ortamda ona normal olarak erişemezsiniz.

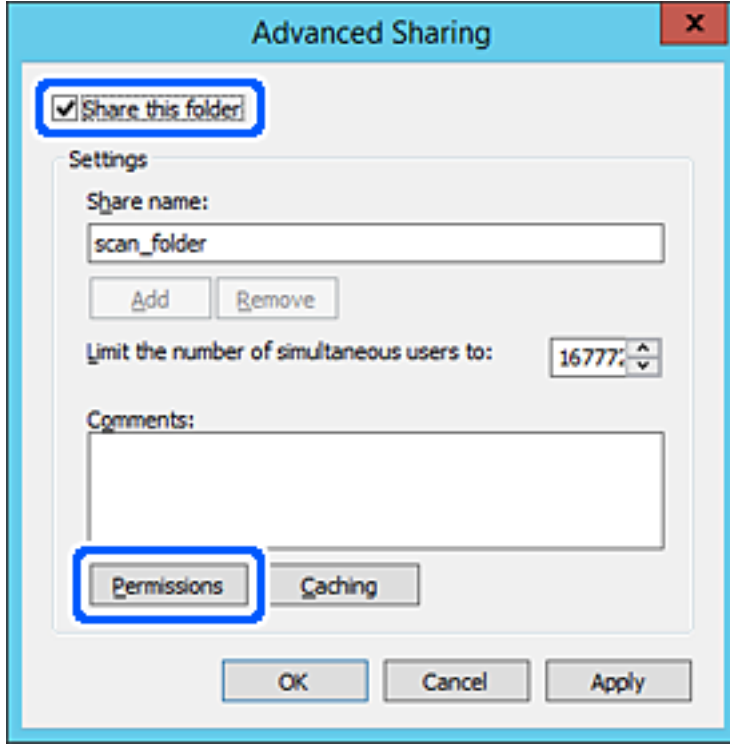
4. Klasörü sağ tıklayın ve ardından, **Özellikler** öğesini seçin.



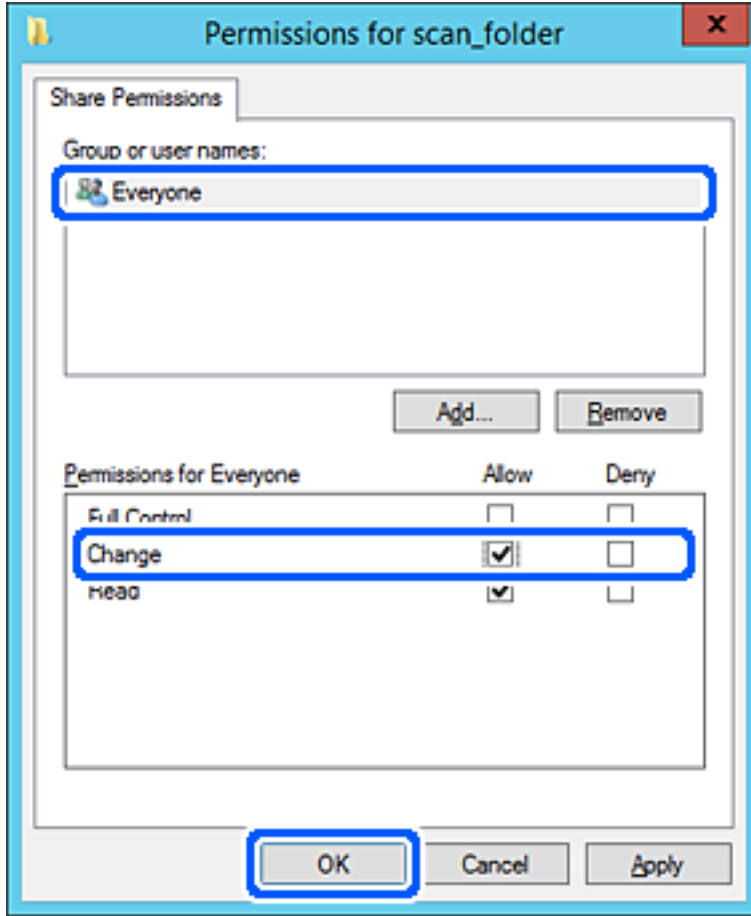
5. **Paylaşım** sekmesinde **Gelişmiş Paylaşım** ögesine tıklayın.



6. Bu klasörü paylaş öğesini seçin ve ardından, **İzinler** öğesine tıklayın.

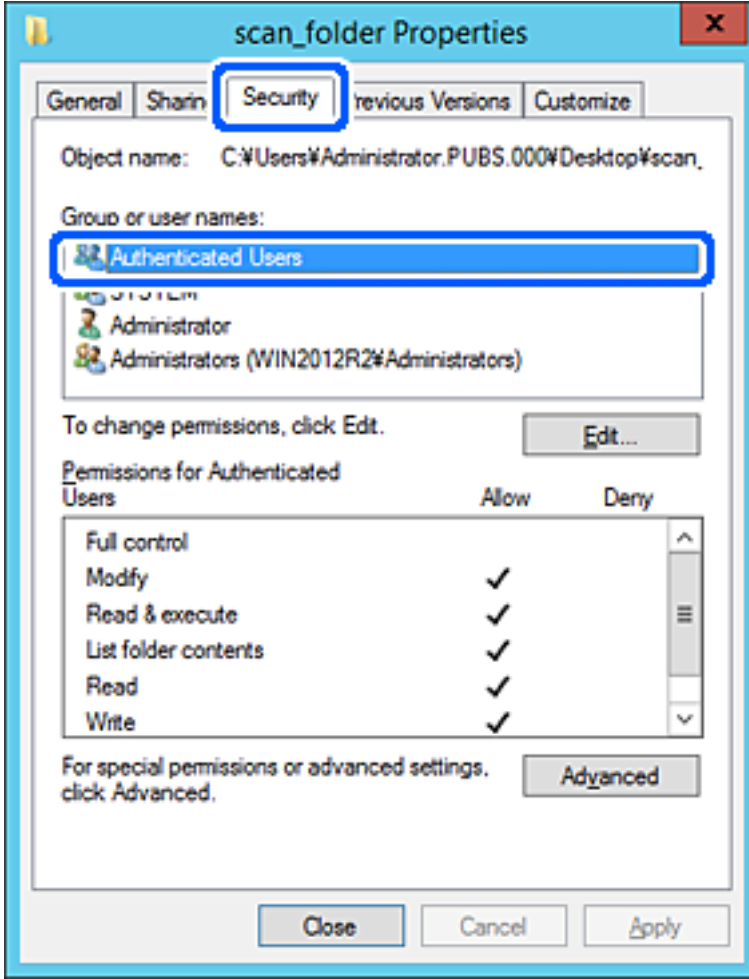


7. **Grup veya kullanıcı adları** ögesinin **Herkes** grubunu seçin, **Değiştir** ögesinde **İzin Ver** ögesini seçin ve ardından, **OK** ögesine tıklayın.



8. **OK** düğmesine tıklayın.

9. Güvenlik sekmesini seçin ve ardından, **Grup veya kullanıcı adları** ögesinde **Kimliği Doğrulanmış Kullanıcılar** ögesini seçin.

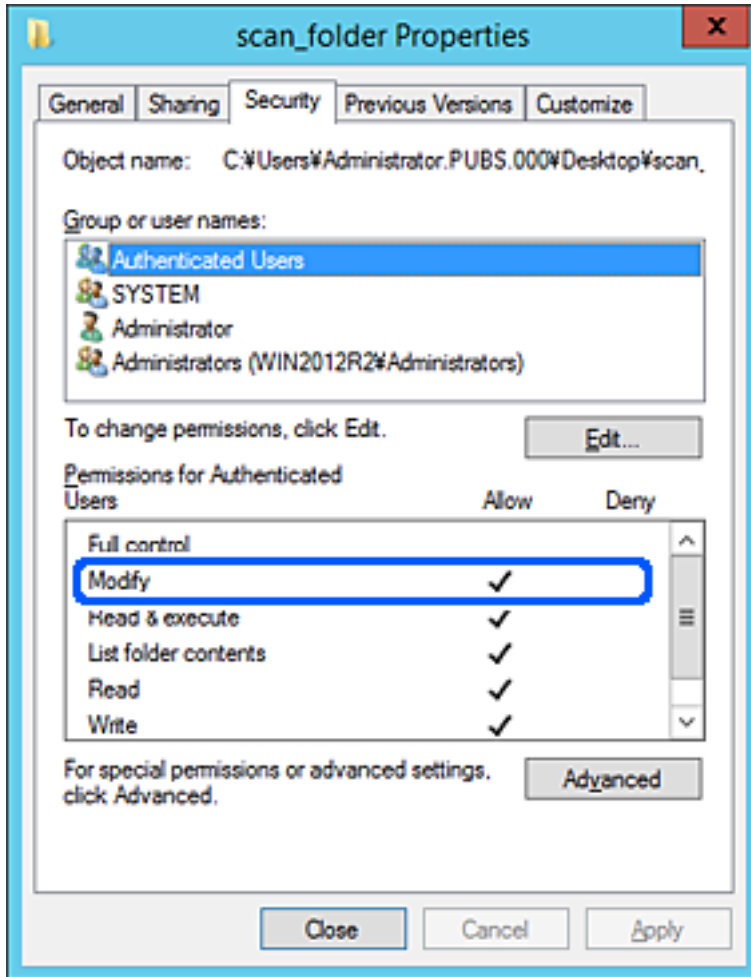


“Kimliği Doğrulanmış Kullanıcılar” tüm kullanıcıları içeren etki alanında veya bilgisayarda oturum açabilen özel gruptur. Bu grup yalnızca klasör kök klasörün hemen altında oluşturulduğunda görüntülenir.

Görüntülenmezse **Düzenle** ögesine tıklayarak ekleyebilirsiniz. Daha fazla ayrıntı için **İlgili Bilgiler’e** bakın.

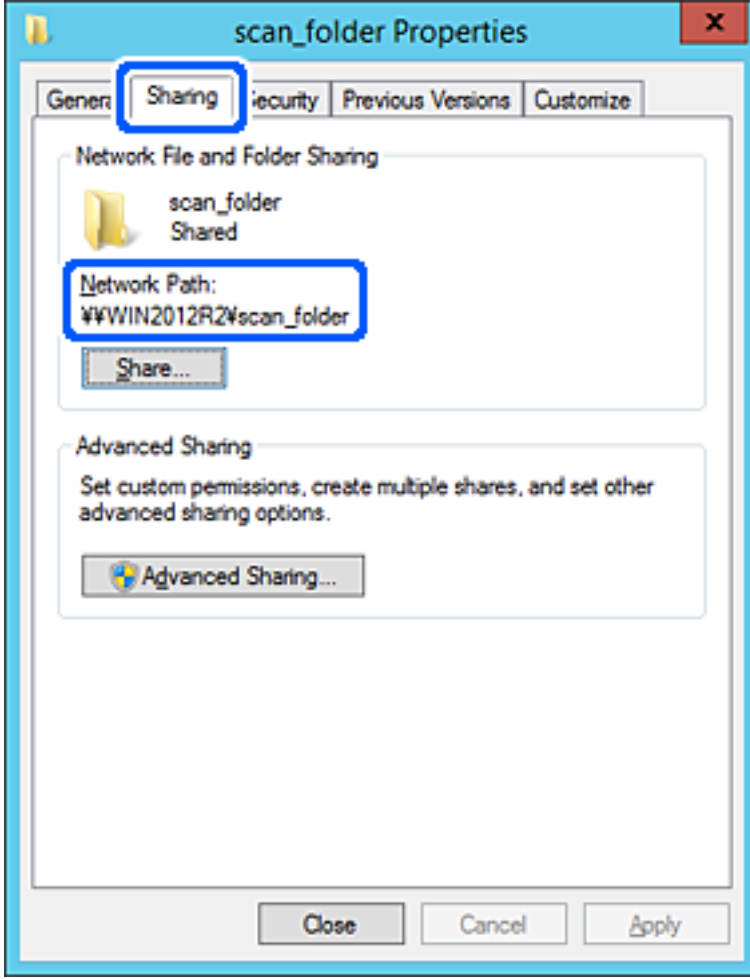
10. **Kimliği Doğrulanmış Kullanıcılar İçin İzinler** içinde **Değiştir** öğesinde **İzin Ver** öğesinin seçili olduğunu kontrol edin.

Seçilmezse **Kimliği Doğrulanmış Kullanıcılar** öğesini seçin, **Düzenle** öğesine tıklayın, **Kimliği doğrulanmış Kullanıcılar İçin İzinler** içindeki **Değiştir** öğesinde **İzin Ver** öğesini seçin ve ardından, **OK** öğesine tıklayın.



11. **Paylaşım** sekmesini seçin.

Paylaşılan klasörün ağ yolu görüntülenir. Bu, tarayıcının kişilerini kaydederken kullanılır. Lütfen yazın.



12. Ekranı kapatmak için **OK** veya **Kapat** ögesine tıklayın.

Dosyanın, bazı etki alanlarının bilgisayarından paylaşılan klasöre yazılabildiğini veya okunabildiğini kontrol edin.

İlgili Bilgi

- ➔ “Erişime İzin Verilen Grup veya Kullanıcı Ekleme” sayfa 58
- ➔ “Web Config Kullanarak Kişileri Hedefe Kaydetme” sayfa 62

Kişisel Bilgisayar İçin Yapılandırma Örneği

Bu açıklama bilgisayarda geçerli olarak oturum açan kullanıcının masaüstünde paylaşılan klasör oluşturma örneğidir.

Bilgisayarda oturum açan ve yönetici yetkisine sahip kullanıcı Kullanıcı klasörü altındaki belge klasörüne ve masaüstü klasörüne erişebilir.

Başka bir kullanıcının kişisel bilgisayardaki paylaşılan klasöre okuma ve yazma yetkisi VERMEDİĞİNİZDE bu yapılandırmayı ayarlayın.

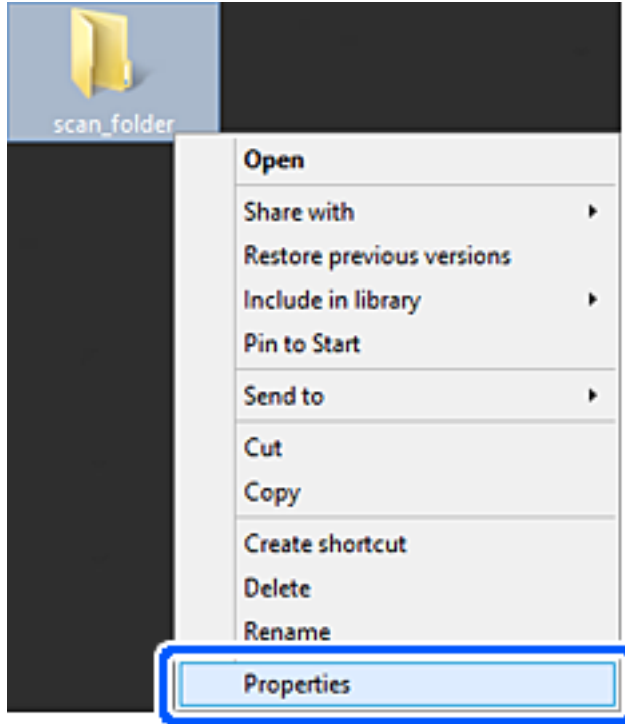
- ☐ Paylaşılan klasör oluşturma yeri: Masaüstü

- ☐ Klasör yolu: C:\Users\xxxx\Desktop\scan_folder
- ☐ Ağ yoluyla erişim izni (Paylaşım İzinleri): Herkes
- ☐ Dosya sisteminde erişim izni (Güvenlik): Erişime izin vermek için Kullanıcı/Grup adları ekleyin veya eklemeyin

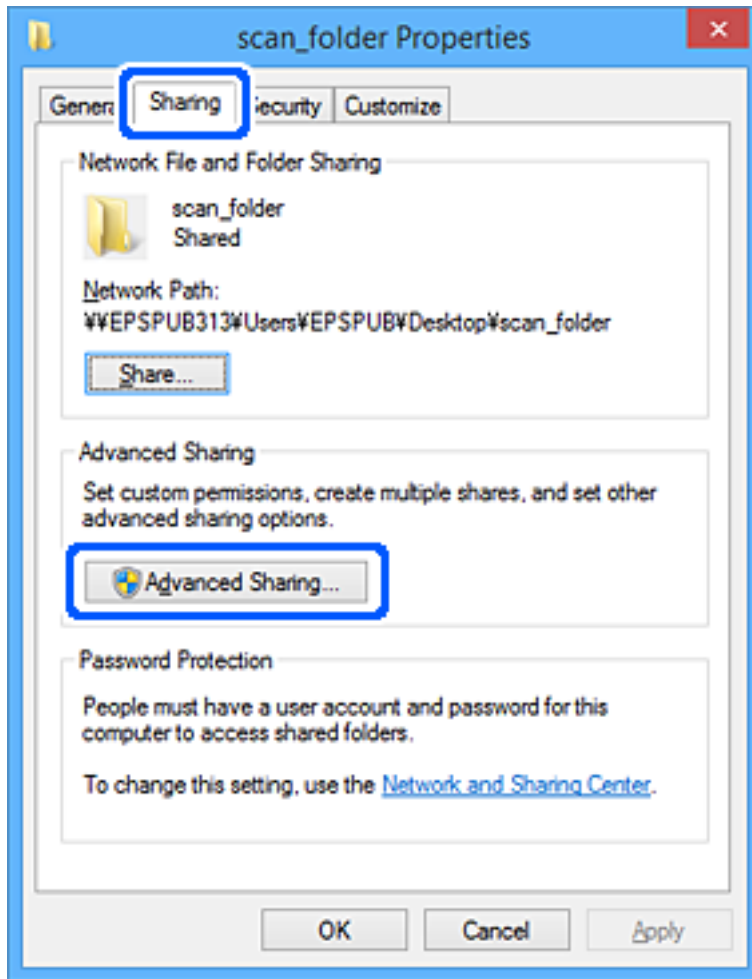
1. Yönetici yetkisi kullanıcı hesabı ile paylaşılan klasörün oluşturulacağı bilgisayarda oturum açın.
2. Gezgini başlatın.
3. Masaüstünde klasör oluşturun ve ardından, “scan_folder” olarak adlandırın.

Klasör adı için 1 ve 12 alfasayısal karakter arasında bir değer girin. Klasör adının karakter sınırı aşılsa değişen ortamda ona normal olarak erişemezsiniz.

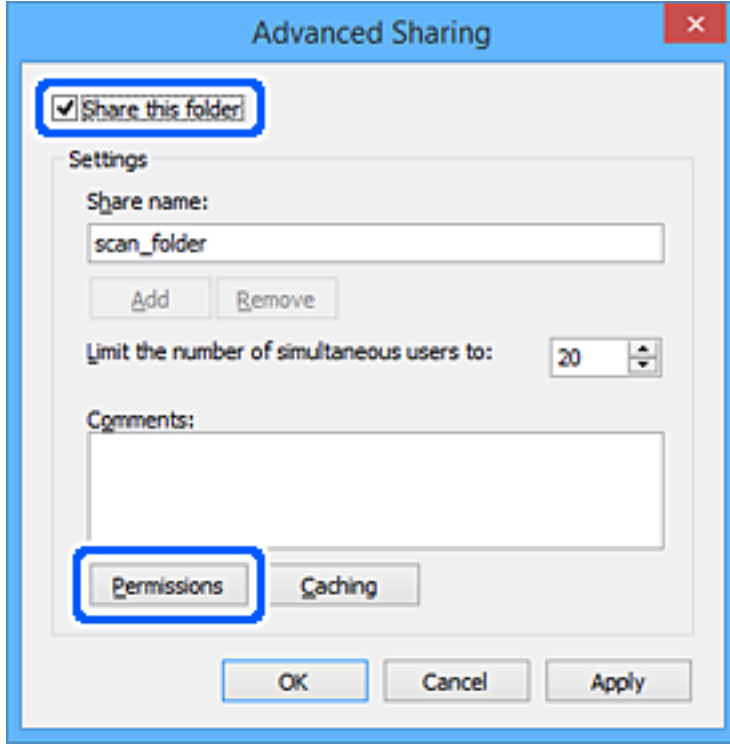
4. Klasörü sağ tıklayın ve ardından, **Özellikler** öğesini seçin.



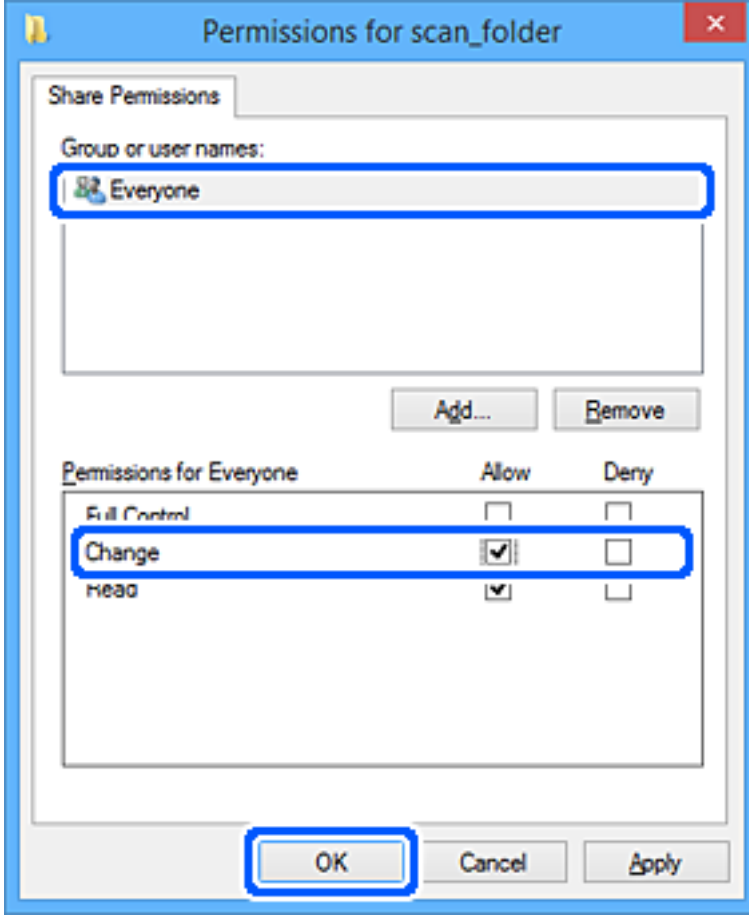
5. **Paylaşım** sekmesinde **Gelişmiş Paylaşım** ögesine tıklayın.



6. Bu klasörü paylaş öğesini seçin ve ardından, **İzinler** öğesine tıklayın.

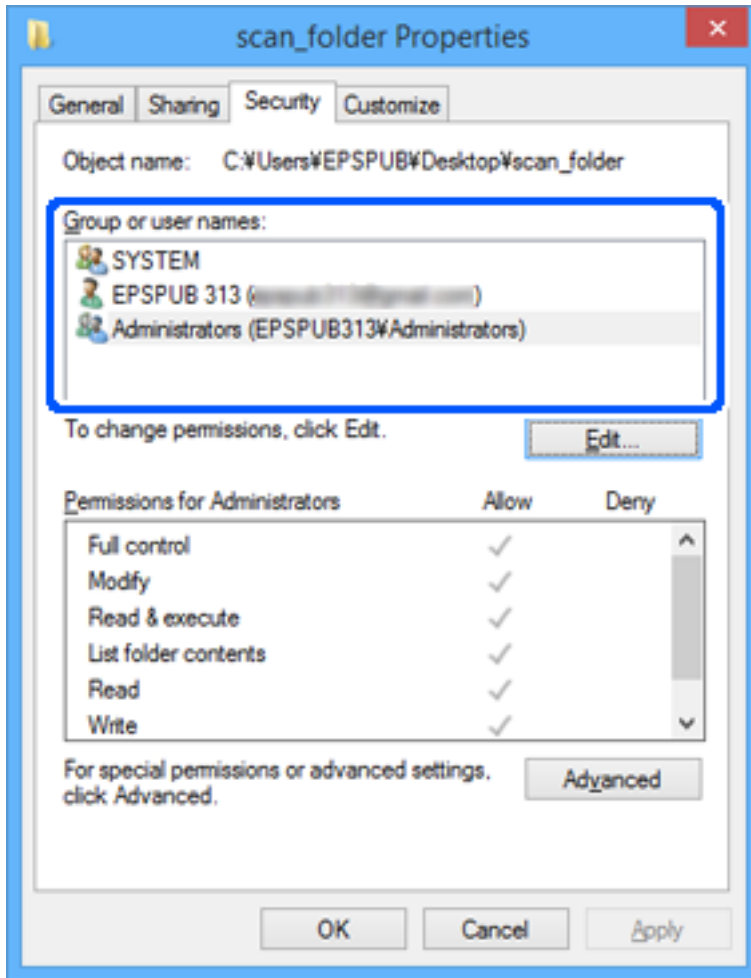


7. **Grup veya kullanıcı adları** ögesinin **Herkes** grubunu seçin, **Değiştir** ögesinde **İzin Ver** ögesini seçin ve ardından, **OK** ögesine tıklayın.



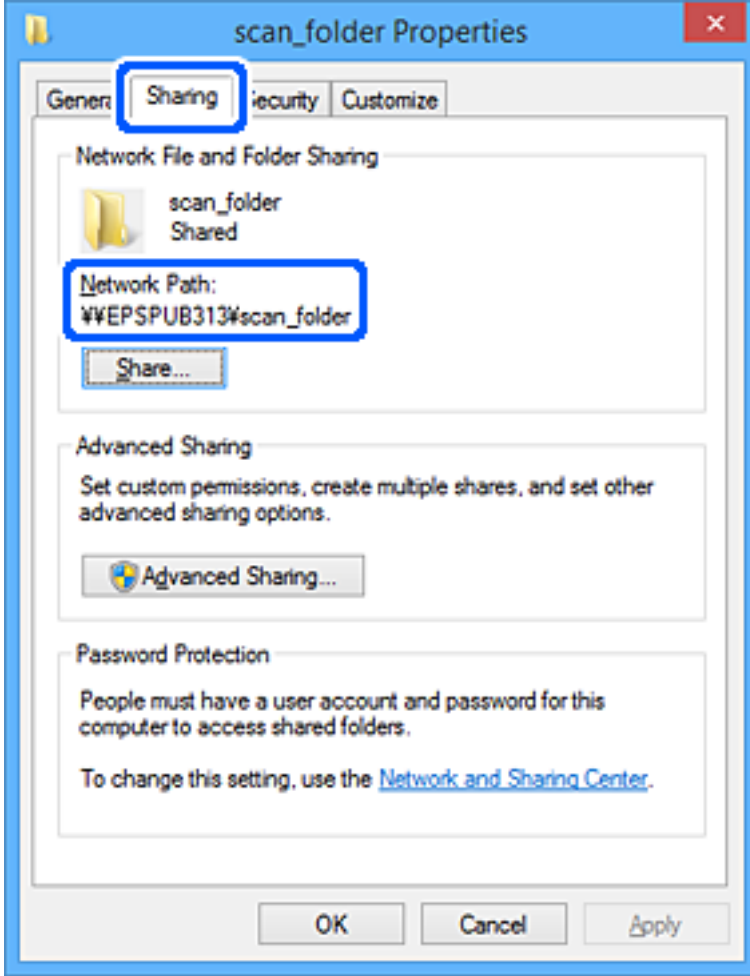
8. **OK** düğmesine tıklayın.
9. **Güvenlik** sekmesini seçin.
10. **Grup veya kullanıcı adları** içinde grup veya kullanıcıyı işaretleyin.
Burada görüntülenen grup veya kullanıcı paylaşılan klasöre erişebilir.
Bu durumda, bu bilgisayarda oturum açan kullanıcı ve Yönetici paylaşılan klasöre erişebilir.

Gerekirse erişim izni ekleyin. **Düzenle** ögesine tıklayarak ekleyebilirsiniz. Daha fazla ayrıntı için İlgili Bilgiler'e bakın.



11. **Paylaşım** sekmesini seçin.

Paylaşılan klasörün ağ yolu görüntülenir. Bu, tarayıcının kişilerini kaydederken kullanılır. Lütfen yazın.



12. Ekranı kapatmak için **OK** veya **Kapat** ögesine tıklayın.

Erişim izni olan kullanıcı veya grup bilgisayarlarından paylaşılan klasörde dosyanın yazılabilir veya okunabilir olduğunu kontrol edin.

İlgili Bilgi

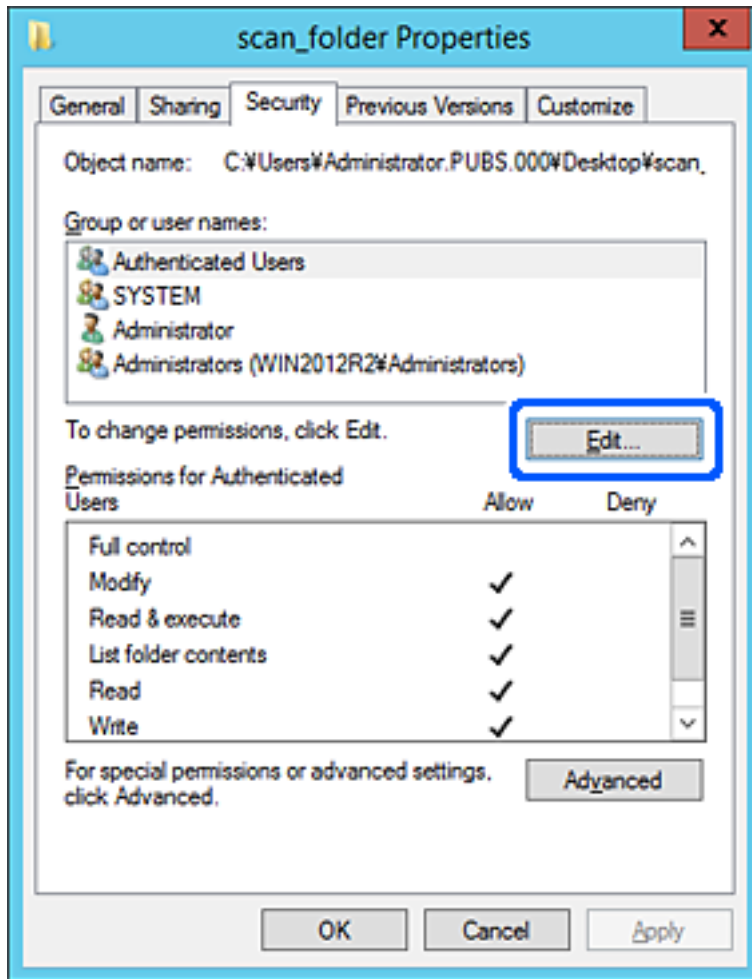
- ➔ “Erişime İzin Verilen Grup veya Kullanıcı Ekleme” sayfa 58
- ➔ “Web Config Kullanarak Kişileri Hedefe Kaydetme” sayfa 62

Erişime İzin Verilen Grup veya Kullanıcı Ekleme

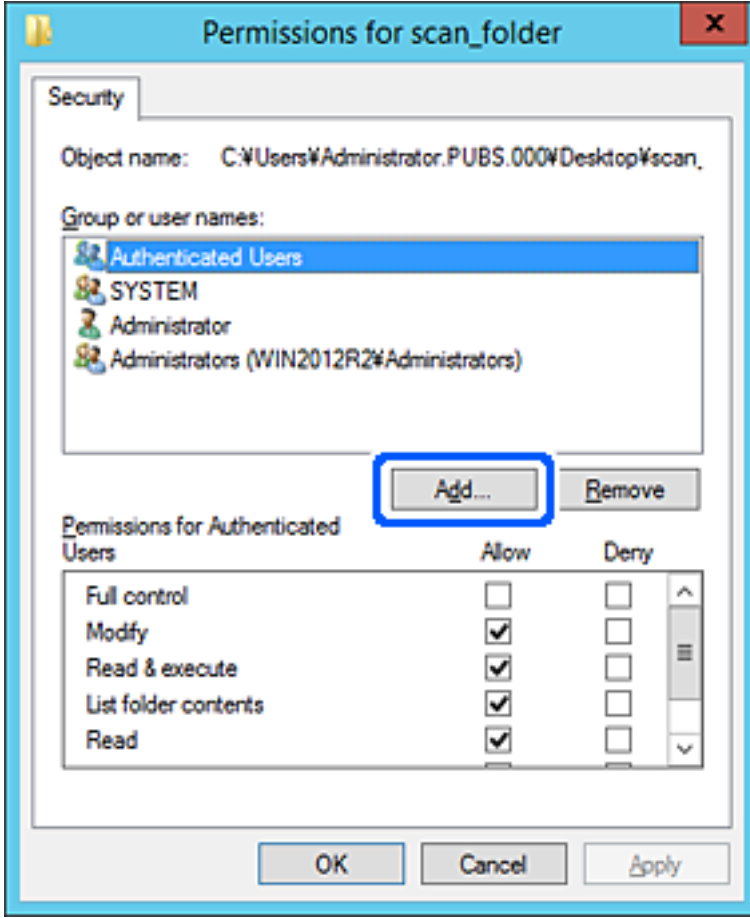
Erişime izin veren grup veya kullanıcı ekleyebilirsiniz.

1. Klasörü sağ tıklayın ve **Özellikler** ögesini seçin.
2. **Güvenlik** sekmesini seçin.

3. **Düzenle**'yi tıklatın.



4. Grup veya kullanıcı adları altındaki Ekle'yi tıklatın.



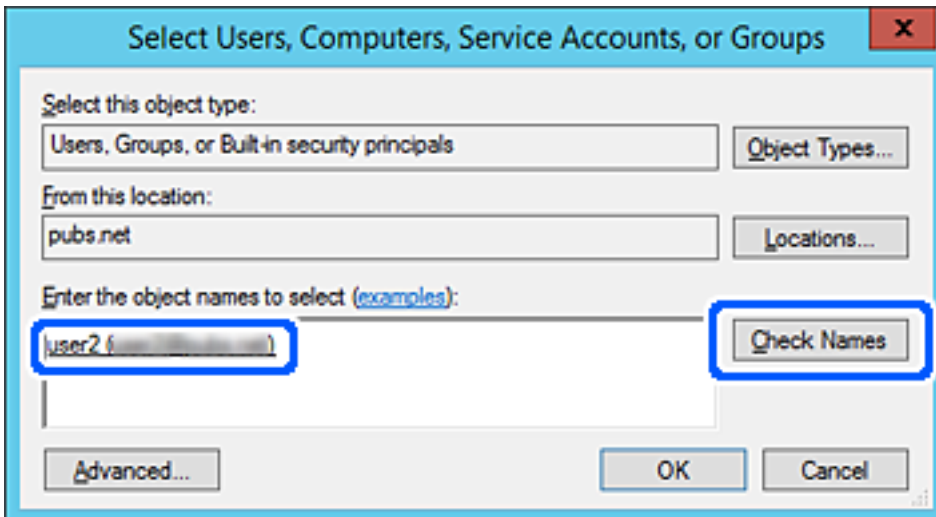
5. Erişime izin vermek istediğiniz grup veya kullanıcı adını girin ve sonra **Adları Kontrol Et** ögesini tıklatın.

Bir alt çizgi ada eklenir.

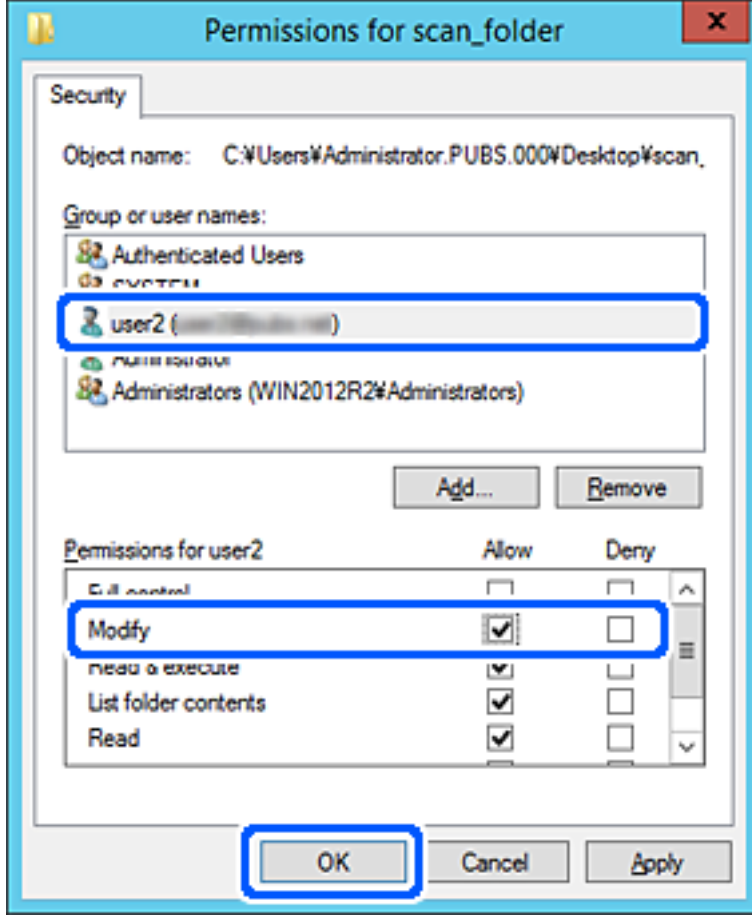
Not:

Grup veya kullanıcının tam adını bilmiyorsanız, adın bir kısmını girin ve sonra **Adları Kontrol Et** ögesini tıklatın. Adın bir bölümüyle eşleşen grup adları ve kullanıcı adları listelenir ve sonra listeden tam adı seçebilirsiniz.

Yalnızca bir ad eşleşirse altı çizili tam ad **Seçmek için nesne adını girin** içinde görüntülenir.



6. **Tamam**'ı tıklatın.
7. İzin ekranında, **Grup veya kullanıcı adları** içinde girilen kullanıcı adını seçin, **Değiştir** öğesinde erişim iznini seçin ve sonra **Tamam** öğesini tıklatın.



8. Ekranı kapatmak için **Tamam** veya **Kapat** öğesini tıklatın.
Erişim izni olan kullanıcı veya grup bilgisayarlarından paylaşılan klasörde dosyanın yazılabilir veya okunabilir olduğunu kontrol edin.

Kişileri Uygun Hale Getirme

Tarayıcının kişiler listesinde hedefleri kaydetme faksları tararken kolayca hedefi girmenizi sağlar.

Kişi listesinde aşağıdaki hedef türlerini kaydedebilirsiniz. Toplamda en fazla 300 giriş kaydedebilirsiniz.

Not:

Hedefi girmek için LDAP sunucusunu (LDAP arama) da kullanabilirsiniz.

E-posta	E-posta için hedef. E-posta sunucusu ayarlarını önceden yapılandırmanız gerekir.
Ağ Klasörü	Tarama verisi için hedef. Ağı önceden hazırlamalısınız.

İlgili Bilgi

➔ “LDAP Sunucusu ve Kullanıcılar Arasındaki Ortaklık” sayfa 67

Kişiler Yapılandırma Karşılaştırması

Tarayıcının kişilerini yapılandırmak için üç araç mevcuttur: Web Config, Epson Device Admin ve tarayıcının kontrol paneli. Bu üç araç arasındaki farklar aşağıdaki tabloda listelenmiştir.

Özellikler	Web Config*	Epson Device Admin	Tarayıcı'nın kontrol paneli
Bir hedef atama	✓	✓	✓
Bir hedef düzenleme	✓	✓	✓
Bir grup ekleme	✓	✓	✓
Bir grup düzenleme	✓	✓	✓
Bir hedef ya da grup silme	✓	✓	✓
Tüm hedefleri silme	✓	✓	–
Bir dosyayı içe aktarma	✓	✓	–
Bir dosyayı dışa aktarma	✓	✓	–

* Ayarları yapmak için yönetici olarak oturum açın.

Web Config Kullanarak Kişileri Hedefe Kaydetme**Not:**

Tarayıcının kontrol panelinde de kişileri kaydedebilirsiniz.

1. Web Config'e erişin ve **Tara** sekmesi > **Kişiler** ögesini seçin.
2. Kaydetmek istediğiniz numarayı seçin ve ardından, **Dğışt** ögesine tıklayın.
3. **Adı** ve **Dizin Sözcüğü** öğelerini girin.
4. Hedef türünü **Tür** seçeneği olarak seçin.

Not:

Tür seçeneğini kayıt tamamlandıktan sonra seçemezsiniz. Türü değiştirmek istiyorsanız, hedefi silin ve ardından, yeniden kaydedin.

5. Her öge için bir değer girin ve ardından, **Uygula** ögesine tıklayın.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35

Hedef Ayar Öğeleri

Öğeler	Ayarlar ve Açıklama
Ortak Ayarlar	
Adı	30 karakter veya daha kısa Unicode (UTF-8) kişilerde görüntülenen bir ad girin. Bunu belirtmezseniz boş bırakın.
Dizin Sözcüğü	Tarayıcının kontrol panelindeki kişileri aramak için Unicode'da (UTF-8) 30 veya daha az karakter kullanarak bir ad girin. Bunu belirtmezseniz boş bırakın.
Tür	Kaydetmek istediğiniz adresin türünü seçin.
Sık Kullanılana Ata	Kayıtlı adresi sık kullanılan adres olarak ayarlamayı seçin. Sık kullanılan adres olarak ayarlarken, tarama ekranını en üstünde görüntülenir ve hedefi kişileri görüntülemekten belirtebilirsiniz.
E-posta	
Eposta Adresi	Şunları kullanarak 1 ila 255 arası karakter girin A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Ağ Klasörü (SMB)	
Kaydet	\\“Klasör yolu” 1 ve 253 karakter arasında Unicode (UTF-8) hedef klasörün bulunduğu konumu girin, “\\” kullanmayın. Klasörün özellik ekranında görüntülenen ağ yolunu girin. Ağ yolunun ayarlanmasıyla ilgili ayrıntılar için aşağıya bakın. “Kişisel Bilgisayar İçin Yapılandırma Örneği” sayfa 52
Kullanıcı Adı	Ağ klasörüne erişmek için 30 karakter veya daha kısa Unicode (UTF-8) bir kullanıcı adı girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının.
Parola	Ağ klasörüne erişmek için 20 karakter veya daha kısa Unicode (UTF-8) bir şifre girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının.
FTP	
Güvenli Bağlantı	FTP sunucusunun desteklediği dosya aktarım protokolüne göre FTP veya FTPS seçin. Tarayıcının güvenlik önlemleriyle iletişim kurmasına izin vermek için FTPS öğesini seçin.
Kaydet	1 ve 253 karakter arası, ASCII (0x20–0x7E) biçiminde, “ftp://” veya “ftps://” yazmadan sunucu adını girin.
Kullanıcı Adı	Bir FTP sunucusuna erişmek için 30 karakter veya daha kısa Unicode (UTF-8) bir kullanıcı adı girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının. Sunucu adsız bağlantılara izin veriyorsa Anonymous ve FTP gibi bir kullanıcı adı girin. Bunu belirtmezseniz boş bırakın.
Parola	Bir FTP sunucusuna erişmek için 20 karakter veya daha kısa Unicode (UTF-8) bir şifre girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının. Bunu belirtmezseniz boş bırakın.
Bağlantı Modu	Menüden bağlantı modunu seçin. Tarayıcı ile FTP sunucusu arasında bir güvenlik duvarı kurulmuşsa Pasif Mod seçin.
Port Numarası	1 ve 65535 arasında FTP sunucusu bağlantı noktası numarası girin.

Öğeler	Ayarlar ve Açıklama
Sertifika Doğrulama	Bu etkinleştirildiğinde FTP sunucusunun sertifikası doğrulanır. Bu, FTPS ögesi Güvenli Bağlantı için seçildiğinde kullanılabilir. Ayarlamak için CA Sertifikası ögesini tarayıcıya almanız gerekir.
SharePoint(WebDAV)	
Güvenli Bağlantı	Sunucunun desteklediği dosya aktarım protokolüne göre HTTP veya HTTPS seçin. Tarayıcının güvenlik önlemleriyle iletişim kurmasına izin vermek için HTTPS ögesini seçin.
Kaydet	1 ve 253 karakter arası, ASCII (0x20–0x7E) biçiminde, "http://" veya "https://" yazmadan sunucu adını girin.
Kullanıcı Adı	Bir sunucuya erişmek için 30 karakter veya daha kısa Unicode (UTF-8) kullanıcı adı girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının. Bunu belirtmezseniz boş bırakın.
Parola	Bir sunucuya erişmek için 20 karakter veya daha kısa Unicode (UTF-8) şifre girin. Ancak kontrol karakterlerini (0x00 ila 0x1F, 0x7F) kullanmaktan kaçının. Bunu belirtmezseniz boş bırakın.
Sertifika Doğrulama	Bu etkinleştirildiğinde sunucunun sertifikası doğrulanır. Bu, HTTPS ögesi Güvenli Bağlantı için seçildiğinde kullanılabilir. Ayarlamak için CA Sertifikası ögesini tarayıcıya almanız gerekir.
Proxy Sunucu	Proxy sunucusu kullanıp kullanmamayı seçin.

Web Config'i Kullanarak Bir Grup Olarak Hedefleri Kaydetme

Hedef türü **E-posta** olarak ayarlanırsa hedefleri bir grup olarak kaydedebilirsiniz.

1. Web Config'e erişin ve **Tara** sekmesi > **Kişiler** ögesini seçin.
2. Kaydetmek istediğiniz numarayı seçin ve ardından, **Dğışt** ögesine tıklayın.
3. **Tür** içinden bir grup seçin.
4. **Grup için kişiler** için **Seç** ögesine tıklayın.
Kullanılabilir hedefler görüntülenir.
5. Gruba kaydetmek istediğiniz hedefi seçin ve ardından, **Seç** ögesine tıklayın.
6. Bir **Adı** ve **Dizin Sözcüğü** girin.
7. Kayıtlı grubu sık kullanılan gruba atayıp atamayacağınızı seçin.
Not:
Hedefler birden fazla gruba kaydedilebilir.
8. **Uygula** ögesine tıklayın.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırma Çalıştırma” sayfa 35

Kişileri Yedekleme ve Alma

Web Config veya başka aletleri kullanarak kişileri yedekleyebilir ve alabilirsiniz.

Web Config için kişileri içeren tarayıcı ayarlarını vererek kişileri yedekleyebilirsiniz. İkili dosya olarak verildiğinden verilen dosya düzenlenemez.

Tarayıcı ayarlarını tarayıcıya alırken kişilerin üzerine yazılır.

Epson Device Admin için cihazın özellik ekranından yalnızca kişiler verilebilir. Ayrıca, güvenlikle ilgili öğeleri vermezseniz, SYLK dosyası veya CSV dosyası olarak kullanabileceğinizden verilen kişileri düzenleyebilir ve alabilirsiniz.

Web Config’i Kullanarak Kişileri Alma

Kişileri yedeklemenize izin veren bir tarayıcıya sahipseniz ve tarayıcıyla uyumluysa yedek dosyasını alarak kişileri kolayca kaydedebilirsiniz.

Not:

Tarayıcı kişilerini yedekleme hakkında talimatlar için tarayıcıyla sağlanan kılavuza bakın.

Kişileri bu tarayıcıya almak için aşağıdaki adımları izleyin.

1. Web Config öğesine erişin, **Aygıt Yönetimi** sekmesi > **Ayar Değerini Dışa ve İçe Aktar** > **İçe Aktar** menüsünü seçin.
2. **Dosya** içinde oluşturduğunuz yedek dosyasını seçin, parolayı girin ve ardından, **İleri** öğesine tıklayın.
3. **Kişiler** onay kutusunu seçin ve ardından, **İleri** öğesine tıklayın.

Web Config Kullanılarak Kişilerin Yedeklenmesi

Tarayıcı arızasından dolayı kişi verileri kaybedilebilir. Verileri güncellediğiniz her seferde verileri yedeklemenizi tavsiye ederiz. Epson, garanti süresi içinde bile herhangi bir veri kaybından, verilerin ve/veya ayarların yedeklenmesinden veya geri yüklenmesinden sorumlu tutulamaz.

Web Config öğesini kullanarak tarayıcıda kayıtlı kişi verilerini bilgisayara yedekleyebilirsiniz.

1. Web Config’e erişin ve ardından, **Aygıt Yönetimi** sekmesi > **Ayar Değerini Dışa ve İçe Aktar** > **Dışa Aktar** öğesini seçin.
2. **Tara** kategorisi altından **Kişiler** onay kutusunu seçin.
3. Verilen dosyayı şifrelemek için bir parola girin.
Dosyayı almak için şifre gerekir. Dosyayı şifrelemek istemiyorsanız bunu boş bırakın.
4. **Dışa Aktar** öğesine tıklayın.

Aracı Kullanarak Kişileri Verme Ve Toplu Kaydetme

Epson Device Admin ögesini kullanıyorsanız, yalnızca kişileri yedekleyebilir ve verilen dosyaları düzenleyebilirsiniz, sonra hepsini bir kerede kaydedin.

Yalnızca kişileri yedeklemek istediğinizde veya tarayıcıyı değiştirdiğinizde ve kişileri eskisinden yenisine aktarmak istediğinizde kullanışlıdır.

Kişileri Verme

Kişi bilgilerini dosyaya kaydedin.

Elektronik tablo uygulaması veya metin düzenleyici kullanarak dosyaları SYLK biçiminde veya csv biçiminde düzenleyebilirsiniz. Bilgileri sildikten veya ekledikten sonra hepsini bir kerede kaydedebilirsiniz.

Parola ve kişisel bilgi gibi güvenlik öğelerini içeren bilgi bir parolayla ikili biçimde kaydedilebilir. Dosyayı kaydedemezsiniz. Bu, güvenlik öğeleri dahil bilgilerin yedek dosyası olarak kullanılabilir.

1. Epson Device Admin ögesini başlatın.
2. Yan çubuk görev menüsünde **Devices** ögesini seçin.
3. Cihaz listesinden yapılandırmak istediğiniz cihazı seçin.
4. Şerit menüsündeki **Home** sekmesinde **Device Configuration** ögesine tıklayın.
Yönetici parolası ayarlandığında, parolayı girin ve **OK** ögesine tıklayın.
5. **Common > Contacts** ögesine tıklayın.
6. **Export > Export items** ögesinden verme biçimini seçin.
 - ☐ All Items
Şifreli ikili dosyayı verin. Parola ve kişisel bilgiler gibi güvenlik öğelerini eklemek istediğinizde seçin.
Dosyayı kaydedemezsiniz. Seçerseniz, parolayı ayarlamanız gerekir. **Configuration** ögesine tıklayın ve 8 ve 63 karakter arası uzunlukta ASCII biçiminde bir parola ayarlayın. İkili dosyayı alırken bu parola gerekir.
 - ☐ Items except Security Information
SYLK biçimi veya csv biçimi dosyalarını verin. Verilen dosyanın bilgilerini düzenlemek istediğiniz seçin.
7. **Export** ögesine tıklayın.
8. Dosyayı kaydedeceğiniz yeri belirtin, dosya türünü seçin ve ardından, **Save** ögesine tıklayın.
Tamamlanma mesajı görüntülenir.
9. **OK** ögesine tıklayın.
Dosyanın belirtilen yere kaydedilmediğini kontrol edin.

Kişileri Alma

Dosyadan kişi bilgilerini alın.

SYLK biçiminde veya csv biçiminde kaydedilecek dosyaları veya güvenlik öğelerini içeren yedeklenen ikili dosyayı alabilirsiniz.

1. Epson Device Admin öğesini başlatın.
2. Yan çubuk görev menüsünde **Devices** öğesini seçin.
3. Cihaz listesinden yapılandırmak istediğiniz cihazı seçin.
4. Şerit menüsündeki **Home** sekmesinde **Device Configuration** öğesine tıklayın.
Yönetici parolası ayarlandığında, parolayı girin ve **OK** öğesine tıklayın.
5. **Common** > **Contacts** öğesine tıklayın.
6. **Import** öğesinde **Browse** öğesine tıklayın.
7. Almak istediğiniz dosyayı seçin ve ardından, **Open** öğesine tıklayın.
İkili dosyayı seçtiğinizde, dosyayı verirken **Password** içinde ayarladığınız parolayı girin.
8. **Import** öğesine tıklayın.
Onay ekranı görüntülenir.
9. **OK** öğesine tıklayın.
Doğrulama sonucu görüntülenir.
 - ☐ Edit the information read
Bilgileri tek tek düzenlemek istediğinizde tıklayın.
 - ☐ Read more file
Birden fazla dosyayı almak istediğinizde tıklayın.
10. **Import** öğesine tıklayın ve ardından, alma tamamlama ekranında **OK** öğesine tıklayın.
Cihazın özellik ekranına dönün.
11. **Transmit** öğesine tıklayın.
12. Onay mesajında **OK** öğesine tıklayın.
Ayarlar tarayıcıya gönderilir.
13. Gönderme tamamlama ekranında, **OK** öğesine tıklayın.
Tarayıcının bilgileri güncelleştirilmiştir.
Web Config veya tarayıcının kontrol panelinden kişileri açın ve ardından, kişinin güncellendiğini kontrol edin.

LDAP Sunucusu ve Kullanıcılar Arasındaki Ortaklık

LDAP sunucusuyla birlikte çalışırken, LDAP sunucusuna kayıtlı adres bilgilerini e-posta hedefi olarak kullanabilirsiniz.

LDAP Sunucusunun Yapılandırılması

LDAP sunucusu bilgilerini kullanmak için tarayıcıda kaydedin.

1. Web Config'e erişin ve **Ağ** sekmesi > **LDAP Sunucusu** > **Temel** ögesini seçin.
2. Her öge için bir değer girin.
3. **Tamam** ögesini seçin.
Seçtiğiniz ayarlar görüntülenir.

LDAP Sunucusu Ayarlama Öğeleri

Öğeler	Ayarlar ve Açıklama
LDAP Sunucusu Kullan	Kullan veya Kullanmayın ögesini seçin.
LDAP Sunucusu Adresi	LDAP sunucusunun adresini girin. IPv4, IPv6 ya da FQDN formatında 1 ila 255 karakter girin. FQDN formatında, ASCII (0x20–0x7E) kısmında alfasayısal karakterler ve adresin başlangıcı ve sonu hariç “-” karakterini de kullanabilirsiniz.
LDAP Sunucusu Bağlantı Noktası Numarası	1 ve 65535 arasında LDAP sunucusu bağlantı noktası numarası girin.
Güvenli Bağlantı	Tarayıcı LDAP sunucusuna eriştiğinde kimlik doğrulama yöntemini belirtin.
Sertifika Doğrulama	Bu etkinleştirildiğinde, LDAP sunucusu sertifikası doğrulanır. Bunun Etkinleştir olarak ayarlanmasını öneririz. Ayarlamak için CA Sertifikası ögesinin tarayıcıya alınması gerekir.
Arama Zaman Aşımı (sn.)	5 ve 300 arasında zaman aşımı oluşmadan önce arama için süre uzunluğunu ayarlayın.
Doğrulama Yöntemi	Yöntemlerden birini seçin. Kerberos Kimlik Doğrulama ögesini seçerseniz, Kerberos ayarlarını yapmak için Kerberos Ayarları ögesini seçin. Kerberos Kimlik Doğrulama işlemini gerçekleştirmek için aşağıdaki ortam gerekir. ☐ Tarayıcı ve DNS sunucusu iletişim kurabilir. ☐ Tarayıcı saati, KDC sunucusu ve kimlik doğrulama için gereken sunucu (LDAP sunucusu, SMTP sunucusu, File sunucusu) senkronize edilir. ☐ Hizmet sunucusu IP adresi olarak atandığında, hizmet sunucusunun FQDN'si DNS sunucusu ters arama bölgesinde kaydedilir.
Kullanılacak Kerberos Erişim Alanı	Kerberos Kimlik Doğrulama ögesini Doğrulama Yöntemi için seçtiyseniz, kullanmak istediğiniz Kerberos bölgesini seçin.
Yönetici Etki Alanı Adı / Kullanıcı Adı	LDAP sunucusu için kullanıcı adını 128 karakter veya daha kısa Unicode (UTF-8) biçiminde girin. 0x00–0x1F ve 0x7F gibi kontrol karakterlerini kullanamazsınız. Adsız Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçildiğinde bu ayar kullanılmaz. Bunu belirtmezseniz boş bırakın.
Parola	LDAP sunucusu kimlik doğrulaması için şifreyi 128 karakter veya daha kısa Unicode (UTF-8) biçiminde girin. 0x00–0x1F ve 0x7F gibi kontrol karakterlerini kullanamazsınız. Adsız Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçildiğinde bu ayar kullanılmaz. Bunu belirtmezseniz boş bırakın.

Kerberos Ayarları

LDAP Sunucusu > Temel öğesinin **Doğrulama Yöntemi** için **Kerberos Kimlik Doğrulama** öğesini seçerseniz, **Ağ** sekmesi > **Kerberos Ayarları** öğesinden aşağıdaki Kerberos ayarlarını yapabilirsiniz. Kerberos ayarları için en fazla 10 ayar kaydedebilirsiniz.

Öğeler	Ayarlar ve Açıklama
Erişim Alanı (Etki Alanı)	255 karakter veya daha kısa ASCII (0x20–0x7E) Kerberos kimlik doğrulama alanını girin. Bunu kaydetmezseniz boş bırakın.
KDC Adresi	Kerberos kimlik doğrulama sunucusunun adresini girin. IPv4, IPv6 veya FQDN biçiminde 255 karakter veya daha az girin. Bunu kaydetmezseniz boş bırakın.
Bağlantı Noktası Numarası (Kerberos)	1 ve 65535 arasında Kerberos sunucusu bağlantı noktası numarasını girin.

LDAP Sunucusu Arama Ayarlarının Yapılandırılması

Arama ayarlarını ayarlarken LDAP sunucusuna kayıtlı e-posta adresini kullanabilirsiniz.

1. Web Config'e erişin ve **Ağ** sekmesi > **LDAP Sunucusu** > **Arama Ayarları** öğesini seçin.
2. Her öğe için bir değer girin.
3. Ayar sonucunu görüntülemek için **Tamam** öğesine tıklayın.
Seçtiğiniz ayarlar görüntülenir.

LDAP Sunucusu Arama Ayarı Öğeleri

Öğeler	Ayarlar ve Açıklama
Arama Temeli (Belirgin Ad)	İsteğe bağlı bir tanım kümesi aramak istiyorsanız, LDAP sunucusu tanım kümesi ismi belirleyebilirsiniz. 0 ve 128 karakter arası (UTF-8) girin. İsteğe bağlı öznitelik aramazsanız bunu boş bırakın. Yerel sunucu dizini örneği: dc=sunucu,dc=yerel
Arama girdileri sayısı	5 ve 500 arasında arama girişi sayısını belirtin. Belirtilen arama girişi sayısı kaydedilir ve geçici olarak görüntülenir. Arama girişi sayısı belirtilen sayıdan fazla olsa ve bir hata mesajı görünse de arama tamamlanamayabilir.
Kullanıcı Adı Özniteliği	Kullanıcı adlarını ararken belirtilecek öznitelik adını belirtin. 1 ve 255 karakter arası (UTF-8) girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: cn, uid
Kullanıcı Adı Görüntüleme Özniteliği	Kullanıcı adı olarak görüntülenecek öznitelik adını belirtin. 0 ve 255 karakter arası (UTF-8) girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: cn, sn
E-posta Adresi Özniteliği	E-posta adreslerini ararken belirtilecek öznitelik adını belirtin. A–Z, a–z, 0–9 ve - karakterlerini kombine ederek 1 ila 255 karakter girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: posta

Öğeler	Ayarlar ve Açıklama
İsteğe Bağlı Öznitelik 1 - İsteğe Bağlı Öznitelik 4	Aranacak diğer isteğe bağlı öznitelikleri belirtebilirsiniz. 0 ve 255 karakter arası (UTF-8) girin. Başlangıç karakteri a-z ya da A-Z karakterlerinden olmalıdır. İsteğe bağlı öznitelik araması yapmak istemiyorsanız burayı boş bırakın. Örnek: o, ou

LDAP Sunucusu Bağlantı Kontrolü

LDAP Sunucusu > Arama Ayarları ögesinde ayarlanan parametreyi kullanarak LDAP sunucusuna bağlantı testini gerçekleştirir.

1. Web Config'e erişin ve **Ağ** sekmesi > **LDAP Sunucusu > Bağlantı Testi** ögesini seçin.
2. **Başlat** ögesini seçin.
Bağlantı testi başlar. Testten sonra kontrol raporu görüntülenir.

LDAP Sunucusu Bağlantı Kontrolü Referansları

Mesajlar	Açıklama
Bağlantı testi başarılı oldu.	Bu mesaj sunucu ile bağlantı başarılı olduğunda görünür.
Bağlantı testi başarısız oldu. Ayarları kontrol edin.	Bu mesaj aşağıdaki nedenlerle görünür: ☐ LDAP sunucu adresi ya da bağlantı noktası sayısı doğru değil. ☐ Bir zaman aşımı oluştuysa. ☐ Kullanmayın ögesi LDAP Sunucusu Kullan olarak seçildiyse. ☐ Kerberos Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçilirse Erişim Alanı (Etki Alanı) , KDC Adresi ve Bağlantı Noktası Numarası (Kerberos) gibi ayarlar yanlışır.
Bağlantı testi başarısız oldu. Ürününüz veya sunucu üzerindeki tarih ve saati işaretleyin.	Bu mesaj, tarayıcı ve LDAP sunucusu için yapılan zaman ayarlarının eşleşmemesi sebebiyle bağlantı başarısız olduğunda belirir.
Kimlik doğrulama başarısız oldu. Ayarları kontrol edin.	Bu mesaj aşağıdaki nedenlerle görünür: ☐ Kullanıcı Adı ve/veya Parola yanlış. ☐ Kerberos Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçilirse zaman/tarih yapılandırılmayabilir.
İşlem tamamlanana kadar ürüne erişilemez.	Tarayıcı meşgulken bu mesaj görünür.

Document Capture Pro Server'yi Kullanma

Document Capture Pro Server kullanarak tarayıcının kontrol panelinden yürütülen bir tarama sonucunun sıralama yöntemini, kaydetme biçimini ve iletim hedefini yönetebilirsiniz. Tarayıcının kontrol panelinden önceden sunucuya kaydedilmiş bir işi çağırabilir ve yönetebilirsiniz.

Sunucu bilgisayarına yükleyin.

Document Capture Pro Server hakkında daha fazla bilgi için yerel Epson ofisinize başvurun.

Sunucu Modunu Ayarlama

Document Capture Pro Server ögesini şu şekilde ayarlayın.

1. Web Config'e erişin ve **Tara** sekmesi > **Document Capture Pro** ögesini seçin.
2. **Mod** için **Sunucu Modu** seçimini yapın.
3. **Sunucu Adresi** için yüklenen Document Capture Pro Server ile sunucunun adresini girin.
IPv4, IPv6, ana bilgisayar adı ya da FQDN formatında 2 ila 255 karakter girin. FQDN formatında, ASCII (0x20–0x7E) kısmında alfasayısal karakterler ve adresin başlangıcı ve sonu hariç “-” karakterini de kullanabilirsiniz.
4. **Tamam** ögesine tıklayın.
Ağ yeniden bağlanır ve ardından, ayarlar etkinleştirilir.

AirPrint Ayarlama

Web Config ögesine erişin, **Ağ** sekmesini seçin ve sonra **AirPrint Kurulumu** ögesini seçin.

Öğeler	Açıklama
Bonjour Hizmet Adı	ASCII metin (0x20–0x7E) ve en fazla 41 karakter kullanarak bir Bonjour servis adı girin.
Bonjour Konumu	Unicode (UTF-8) metin ve en fazla 127 bayt kullanarak tarayıcının konum açıklamasını girin.
Wide-Area Bonjour	Geniş Alanlı Bonjour'u kullanıp kullanmamayı ayarlayın. Kullanırsanız, segment üzerinden tarayıcıyı aramak için tarayıcı DNS sunucusunda kaydedilmelidir.
AirPrint'i Etkinleştir	Bonjour ve AirPrint (Tarama hizmeti) etkinleştirilir.

Ağ Taramaya Hazırlanırken Sorunlar

Sorunları Çözme İpuçları

- ☐ Hata mesajını kontrol etme

Sorun oluştuğunda, önce tarayıcının kontrol panelinde veya sürücü ekranında herhangi bir mesaj olup olmadığını kontrol edin. Olaylar oluştuğunda bildirim e-postasına ayarlandıysa durumu hemen öğrenebilirsiniz.

☐ İletişim durumunu kontrol etme

Ping ve ipconfig gibi komutları kullanarak sunucu bilgisayarının veya istemci bilgisayarın iletişim durumunu kontrol edin.

☐ Bağlantı testi

Tarayıcıdan posta sunucusuna olan bağlantıyı kontrol etmek için tarayıcıdan bağlantı testini gerçekleştirin. Ayrıca, iletişim durumunu kontrol etmek için istemci bilgisayarından sunucuya olan bağlantıyı kontrol edin.

☐ Ayarları ilkleme

Ayarlar ve iletişim durumu hiç sorun göstermiyorsa sorunlar tarayıcının ağ ayarları devre dışı bırakılarak veya ilklenerek ve ardından, yeniden ayarlanarak çözülebilir.

Web Config'e Erişilemiyor

■ IP adresi tarayıcıya atanmamış.

Çözümler

Geçerli bir IP adresi tarayıcıya atanmamış olabilir. Tarayıcının kontrol panelini kullanarak IP adresini yapılandırın. Tarayıcının kontrol panelinden mevcut ayar bilgilerini onaylayabilirsiniz.

■ Web tarayıcısı SSL/TLS için Şifreleme Güvenlik Düzeyini desteklemiyor.

Çözümler

SSL/TLS'de Şifreleme Gücü var. Aşağıda gösterildiği gibi toplu şifrelemeleri kullanarak bir web tarayıcısı kullanarak Web Config'i açabilirsiniz. Desteklenen bir tarayıcı kullandığınızı kontrol edin.

- ☐ 80 bit: AES256/AES128/3DES
- ☐ 112 bit: AES256/AES128/3DES
- ☐ 128 bit: AES256/AES128
- ☐ 192 bit: AES256
- ☐ 256 bit: AES256

■ CA İmzalı Sertifika sona erdi.

Çözümler

SSL/TLS iletişimiyle (https) Web Config'e bağlanırken sertifikanın sona erme tarihiyle ilgili bir sorun varsa "Sertifika süresi doldu" görüntülenir. Mesaj sona erme tarihinden önce görünürse tarayıcının tarihi düzgün yapılandırıldığından emin olun.

■ Sertifika ve tarayıcının ortak adı eşleşmiyor.

Çözümler

Sertifika ve tarayıcının ortak adı eşleşmiyorsa SSL/TLS iletişimi (https) kullanılarak Web Config'e erişirken "Güvenlik sertifikası adı eşleşmiyor..." mesajı görüntülenir. Bu, aşağıdaki IP adresleri eşleşmediğinde oluşur.

- ☐ Kendinden İmzalı Sertifika veya CSR oluşturmak için tarayıcının IP adresi ortak ada girilir
- ☐ Web Config çalıştırılırken web tarayıcısına girilen IP adresi

Kendinden İmzalı Sertifika için sertifikayı güncelleyin.

CA İmzalı Sertifika için tarayıcı için sertifikayı yeniden alın.

Yerel adresin proxy sunucusu ayarı web tarayıcısına ayarlanmamış.

Çözümler

Tarayıcı bir proxy sunucusu kullanmaya ayarlandığında, proxy sunucusu yoluyla web tarayıcısını yerel adrese bağlanmamaya yapılandırın.

❑ Windows:

Denetim Masası > Ağ ve Internet > Internet Seçenekleri > Bağlantılar > LAN ayarları > Proxy sunucusu öğesini seçin ve sonra LAN (yerel adresler) için proxy sunucusunu kullanmamayı yapılandırın.

❑ Mac OS:

Sistem Tercihleri > Ağ > Gelişmiş > Proxy'ler öğesini seçin ve sonra **Bu Ana Bilgisayarlar ve Etki Alanları için proxy ayarlarını atlayın** 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

DHCP, bilgisayarın ayarlarında devre dışı bırakılmıştır.

Çözümler

Bilgisayarda otomatik olarak bir IP adresi almak için DHCP devre dışı bırakılırsa Web Config'e erişemezsiniz. DHCP'yi etkinleştirin.

Windows 10 için örnek:

Kontrol Panelini açın ve sonra **Ağ ve Internet > Ağ ve Paylaşım Merkezi > Adaptör ayarlarını değiştir** öğesini tıklayın. Kullandığınız bağlantının Özellikler ekranını açın ve sonra **Internet Protokolü Sürüm 4 (TCP/IPv4)** veya **Internet Protokolü Sürüm 6 (TCP/IPv6)** için özellikler ekranını açın. Görüntülenen ekranda **Bir IP adresini otomatik al** öğesinin seçili olduğunu kontrol edin.

Kontrol Paneli Ekranını Özelleřtirme

Ön aylar Öğelerinin Kaydedilmesi.	75
Kontrol Paneli Ana Ekranını Düzenleme.	77

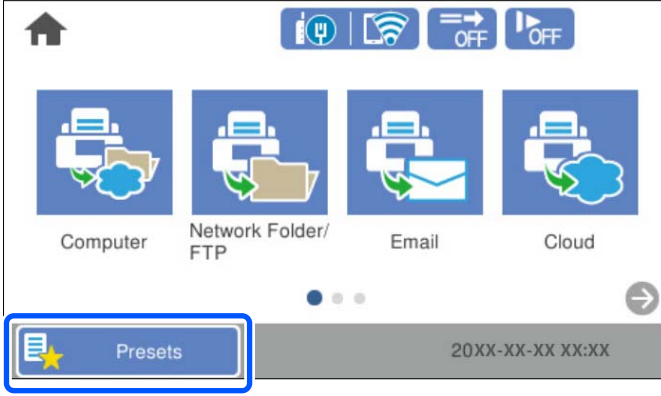
Ön ayrlar Öğelerinin Kaydedilmesi

Sık kullanılan tarama ayarlarını **Ön ayrlar** olarak kaydedebilirsiniz. En fazla 48 ön ayar kaydedebilirsiniz.

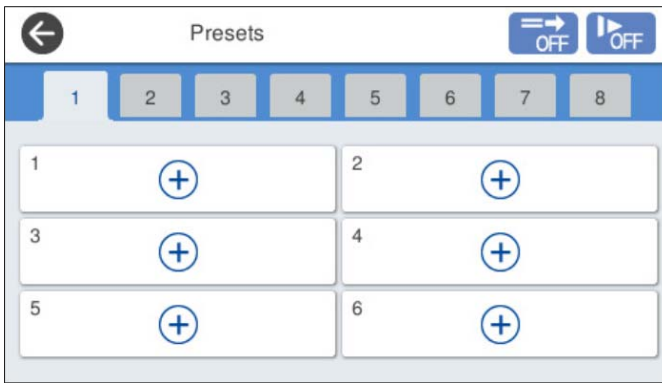
Not:

- ☐ Taramayı başlat ekranında ☆ öğesini seçerek geçerli ayarları kaydedebilirsiniz.
- ☐ **Ön ayrlar** öğelerini Web Config kısmında da kaydedebilirsiniz.
Tara sekmesi > Ön ayrlar öğesini seçin.
- ☐ Kaydederken **Bilgisayara Tara** öğesini seçerseniz, Document Capture Pro içinde oluşturulan işi **Ön ayrlar** olarak kaydedebilirsiniz. Bu, yalnızca bir ağ üzerinden bağlı bilgisayarlar için kullanılabilir. Document Capture Pro'da işi önceden kaydedin.
- ☐ Kimlik doğrulama işlevi etkinleştirilirse yalnızca yönetici **Ön ayrlar** kaydedebilir.

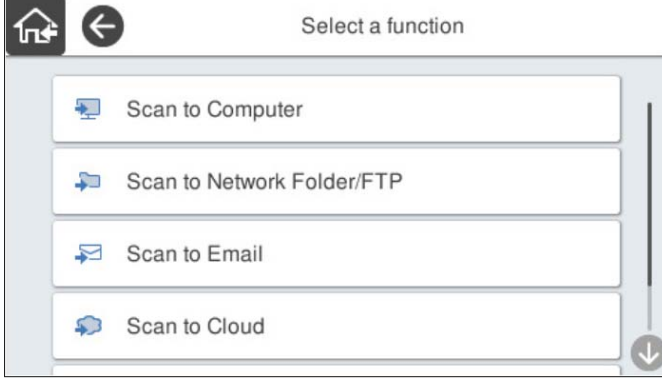
1. Tarayıcı kontrol panelinin ana ekranında **Ön ayrlar** öğesini seçin.



2. (+) öğesini seçin.



3. Bir ön ayarı kaydetmek amacıyla kullanmak istediğiniz menüyü seçin.



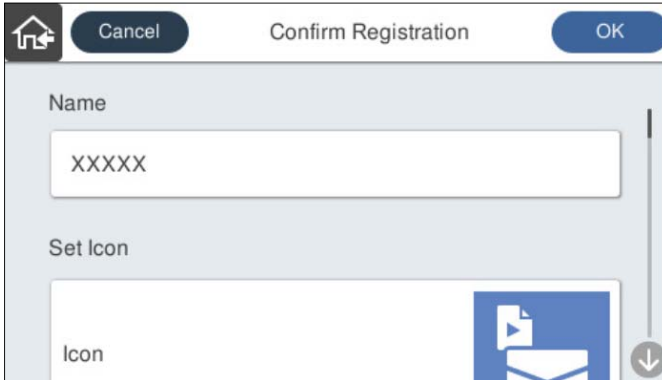
4. Her öğeyi ayarlayın ve ardından, ☆ öğesini seçin.

Not:

Bilgisayara Tara öğesini seçtiğinizde, Document Capture Pro'nun yüklendiği bilgisayarı seçin ve sonra kayıtlı işi seçin. Bu, yalnızca bir ağ üzerinden bağlı bilgisayarlar için kullanılabilir.

5. Ön ayar ayarlarını yapın.

- ☐ **Ad:** Adı ayarlar.
- ☐ **Simge ayarla:** Görüntülenecek görüntüyü ve simgenin rengini ayarlayın.
- ☐ **Hızlı Gönder Ayarı:** Ön ayar seçildiğinde onay olmadan hemen taramaya başlar.
Document Capture Pro Server kullanırken, taramadan önce bir işin içeriğini onaylamak için yazılımı ayarlasanız bile tarayıcının ön ayarındaki **Hızlı Gönder Ayarı** yazılıma göre öncelik kazanır.
- ☐ **İçindekiler:** Tarama ayarlarını kontrol edin.



6. **OK** öğesini seçin.

Ön ayrlar Menü Seçenekleri

Bir ön ayarın ayarlarını her bir ön ayarda > öğesini seçerek görüntüleyebilirsiniz.

İsmi Değiştir:

Ön ayar adını değiştirir.

Simgeyi değiştir:

Ön ayarın simge görüntüsünü ve rengini değiştirir.

Hızlı Gönder Ayarı:

Ön ayar seçildiğinde onay olmadan hemen taramaya başlar.

Konum Değiştir:

Ön ayarların görüntülenme sırasını değiştirir.

Sil:

Ön ayarı siler.

Başlangıç'ta Simge Ekleyin veya Kaldırın.:

Ön ayar simgesini ana ekrandan ekler ya da siler.

Ayrıntıları Onayla:

Bir ön ayarın ayarlarını görüntüleyin. Ön ayarı **Bu Ayarı Kullan** ögesini seçerek yükleyebilirsiniz.

Kontrol Paneli Ana Ekranını Düzenleme

Ana ekranı, tarayıcının kontrol panelinde **Ayarlar > Ana Ekranı Düzenle** ögesini seçerek özelleştirebilirsiniz.

☐ Düzen: Menü simgelerinin görüntülenme yöntemini değiştirir.

[“Ana ekranda Düzen ögesini değiştirme” sayfa 77](#)

☐ Simge Ekle: Simgeleri yaptığınız **Ön ayarlar** ayarlarına ekler ya da ekrandan kaldırılmış simgeleri geri yükler.

[“Simge Ekle” sayfa 78](#)

☐ Simge Kaldır: Simgeleri ana ekrandan kaldırır.

[“Simge Kaldır” sayfa 79](#)

☐ Simge Taşı: Simgelerin görüntülenme sırasını değiştirir.

[“Simge Taşı” sayfa 80](#)

☐ Varsayılan Simge Gösterimine Geri Al: Ana ekran varsayılan ekran ayarlarını geri yükler.

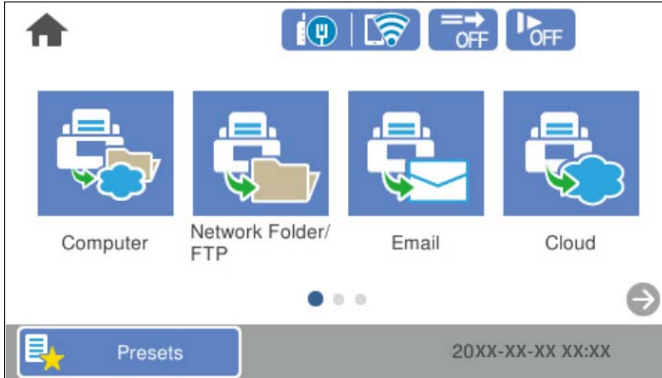
☐ Duvar Kâğıdı: ana ekranın duvar kağıdı rengini değiştirin.

Ana ekranda Düzen ögesini değiştirme

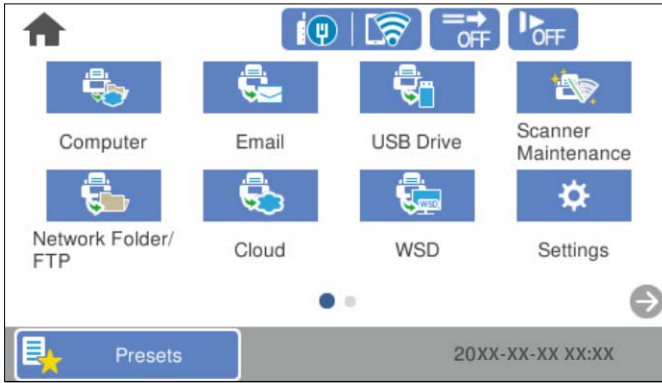
1. Tarayıcının kontrol panelinde **Ayarlar > Ana Ekranı Düzenle > Düzen** ögesini seçin.

2. **Hat** veya **Matris** ögesini seçin.

Hat:



Matris:

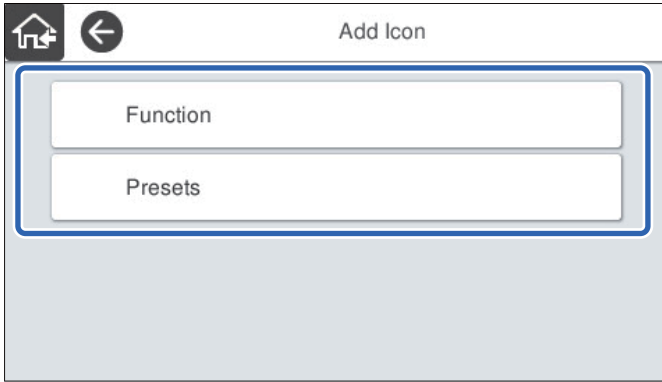


3. Dönmek için  ögesini seçin ve ana ekranı kontrol edin.

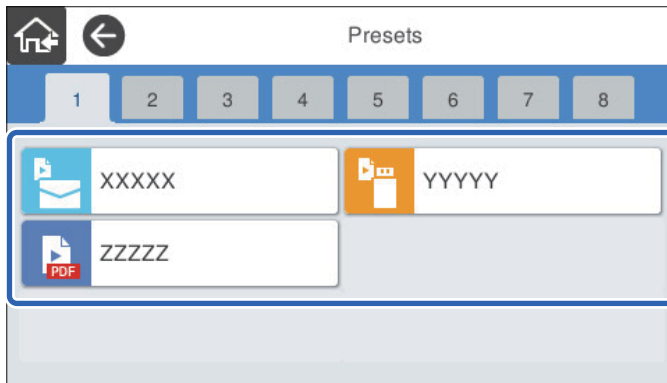
Simge Ekle

1. Tarayıcının kontrol panelinde **Ayarlar** > **Ana Ekranı Düzenle** > **Simge Ekle** ögesini seçin.
2. **Fonksiyon** veya **Ön ayrlar** ögesini seçin.
 - ☐ Fonksiyon: Ana ekranda gösterilen varsayılan işlevleri görüntüler.

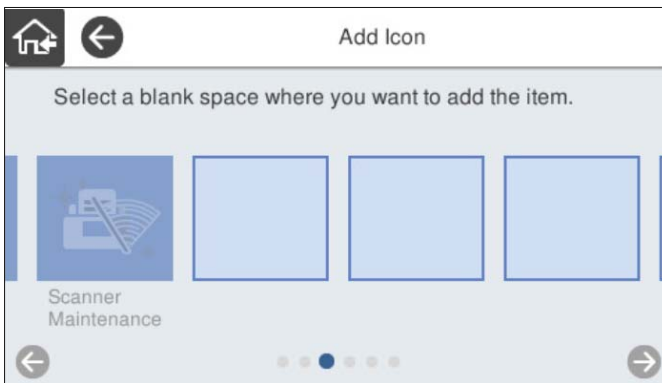
- ❑ Ön ayrlar: Kaydedilmiş ön ayarları görüntüler.



3. Ana ekrana eklemek istediğiniz öğeyi seçin.



4. Öğeyi eklemek istediğini boş alanı seçin.
Birden fazla simge eklemek istiyorsanız 3. ve 4. adımları yineleyin.

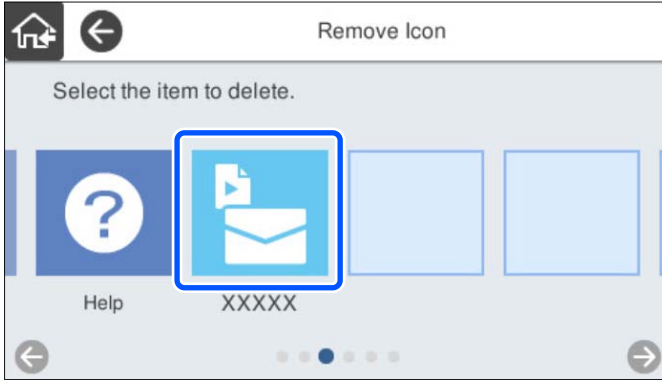


5. Dönmek için  ögesini seçin ve ana ekranı kontrol edin.

Simge Kaldır

1. Tarayıcının kontrol panelinde **Ayarlar** > **Ana Ekranı Düzenle** > **Simge Kaldır** öğesini seçin.

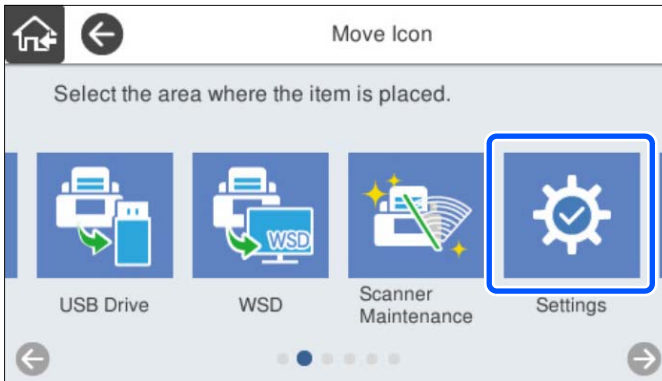
2. Kaldırmak istediğiniz simgeyi seçin.



3. Bitirmek için **Evet** ögesini seçin.
Birden fazla simge kaldırmak istiyorsanız 2. ve 3. prosedürleri yineleyin.
4. Dönmek için  ögesini seçin ve ana ekranı kontrol edin.

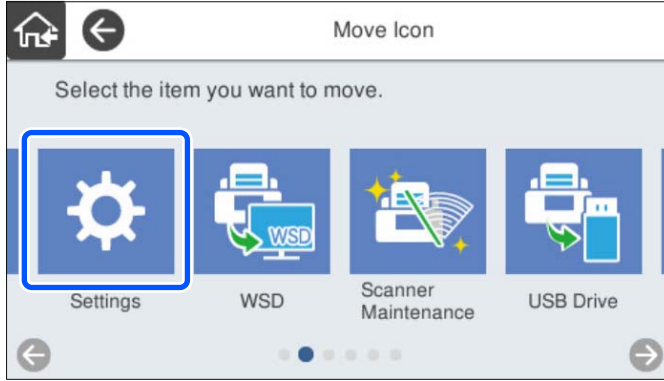
Simge Taşı

1. Tarayıcının kontrol panelinde **Ayarlar** > **Ana Ekranı Düzenle** > **Simge Taşı** ögesini seçin.
2. Taşımak istediğiniz simgeyi seçin.



3. Hedef çerçeveyi seçin.

Hedef çerçevesinde başka bir simge zaten ayarlanmışsa simgeler değiştirilir.



4. Dönmek için  ögesini seçin ve ana ekranı kontrol edin.

Temel Güvenlik Ayarları

Ürün Güvenliği Özelliklerine Giriş.	83
Yönetici Ayarları.	83
Harici Arayüzü Devre Dışı Bırakma.	89
Uzak Tarayıcıyı İzleme.	90
Sorunları Çözme.	91

Ürün Güvenliği Özelliklerine Giriş

Bu kısımda Epson Cihazlarının güvenlik işlevi açıklanmaktadır.

Özellik adı	Özellik türü	Ayarlanacak öğe	Neyi önler
Yönetici parolası için ayar	Ağ veya USB için bağlantı ayarı gibi sistem ayarlarını kilitler.	Bir yönetici cihaza bir parola ayarlar. Hem Web Config ögesinden hem de tarayıcının kontrol panelinden ayarlayabilir veya değiştirebilirsiniz.	Kimlik, parola, ağ ayarları vb. gibi cihazda depolanan bilgilerin yasal olmayan bir şekilde okunmasını ve değiştirilmesini önler. Ayrıca, ağ ortamı veya güvenlik ilkesi için bilgi sızıntısı gibi geniş aralıklı güvenlik risklerini azaltır.
Harici arayüz için ayar	Cihaza bağlanan arayüzü kontrol eder.	Bilgisayarla USB bağlantısını etkinleştirin veya devre dışı bırakın.	Bilgisayarın USB bağlantısı: Ağda dolaşmadan taramayı yasaklayarak cihazın yetkisiz kullanımını önler.

İlgili Bilgi

- ➔ “Yönetici Şifresi Yapılandırma” sayfa 83
- ➔ “Harici Arayüzü Devre Dışı Bırakma” sayfa 89

Yönetici Ayarları

Yönetici Şifresi Yapılandırma

Yönetici parolasını ayarladığınızda, kullanıcıların sistem yönetim ayarlarını değiştirmesini önleyebilirsiniz. Varsayılan değerler, satın alma zamanında ayarlanır. Gerekli olduğu gibi değiştirin.

Not:

Aşağıda, yönetici bilgileri için varsayılan değerler sağlanmaktadır.

- ☐ Kullanıcı adı (sadece Web Config için kullanılır): yok (boş)
- ☐ Parola: tarayıcının seri numarası

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin.

Web Config ögesini, tarayıcının kontrol panelini veya Epson Device Admin ögesini kullanarak yönetici parolasını değiştirebilirsiniz. Epson Device Admin kullanırken, Epson Device Admin kılavuzuna veya yardıma bakın.

Web Config’i Kullanarak Yönetici Parolasını Değiştirme

Yönetici parolasını Web Config içinde değiştirin.

1. Web Config’e erişin ve **Ürün Güvenliği** sekmesi > **Yönetici Şifresini Değiştir** ögesini seçin.

2. Gerekli bilgileri **Mevcut parola**, **Kullanıcı Adı**, **Yeni parola** ve **Yeni Parolayı Doğrula** içine girin.
Yeni parola için en az bir karakter girin.

Not:

Aşağıda, yönetici bilgileri için varsayılan değerler sağlanmaktadır.

- ☐ Kullanıcı adı: yok (boş)
- ☐ Parola: tarayıcının seri numarası

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin.



Önemli:

Ayarladığınız yönetici parolasını hatırladığınızdan emin olun. Parolanızı unutursanız, sıfırlayamayacaksınız ve servis personelinizden yardım istemeniz gerekecek.

3. **Tamam** ögesini seçin.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Kontrol Panelinden Yönetici Parolasını Değiştirme

Yönetici parolasını tarayıcının kontrol panelinden değiştirebilirsiniz.

1. Tarayıcının kontrol panelinde **Ayarlar** ögesini seçin.
2. **Sistem Yöneticisi** > **Yntci Ayarları** seçeneklerini seçin.
3. **Yönetici Parolası** > **Değiştir** seçeneklerini seçin.
4. Geçerli parolanızı girin.

Not:

Yönetici parolası için satın alma zamanındaki ayar (varsayılan değer), tarayıcının seri numarasıdır.

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin.

5. Yeni parolanızı girin.
En az bir karakter girin.



Önemli:

Ayarladığınız yönetici parolasını hatırladığınızdan emin olun. Parolanızı unutursanız, sıfırlayamayacaksınız ve servis personelinizden yardım istemeniz gerekecek.

6. Yeni parolayı onay için tekrar girin.

Bir tamamlanma mesajı görüntülenir.

Kontrol Paneli için Kilit Ayarları Kullanma

Kullanıcıların sistem ayarlarıyla ilgili öğeleri değiştirmesini önlemek üzere kontrol panelini kilitlemek için Kilit Ayarları öğesini kullanabilirsiniz.

Not:

Tarayıcıdaki Kimlik Doğrulama Ayarları öğesini etkinleştirirseniz, kontrol paneli için Kilit Ayarları öğesi de etkinleştirilir. Kontrol panelinin kilidi, Kimlik Doğrulama Ayarları etkinleştirildiğinde açılmaz.

Kimlik Doğrulama Ayarları öğesini devre dışı bırakırsanız, Kilit Ayarları öğesi etkin kalır. Devre dışı bırakmak isterseniz, ayarları kontrol panelinden ya da Web Config öğesinden yapabilirsiniz.

Kontrol Panelinden Kilit Ayarları Öğesini Ayarlama

1. Etkinleştirildikten sonra **Kilit Ayarları** öğesini iptal etmek isterseniz, yönetici olarak giriş yapmak için Ana ekranın sağ üst köşesindeki  öğesine dokununuz.

Kilit Ayarları devre dışı bırakıldığında  görüntülenmez. Bu ayarı etkinleştirmek isterseniz, sonraki adıma gidin.

2. **Ayarlar** öğesini seçin.
3. **Sistem Yöneticisi > Yntci Ayarları** seçeneklerini seçin.
4. **Kilit Ayarları** olarak **Açık** veya **Kplı** öğesini seçin.

Kilit Ayarları Öğesini Web Config Öğesinden Ayarlama

1. **Aygıt Yönetimi** sekmesi > **Kontrol Paneli** öğesini seçin.
2. **Panel Kilidi** için **Açık** veya **Kapalı** öğesini seçin.
3. **Tamam** öğesine tıklayın.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırma Çalıştırma” sayfa 35](#)

Ayarlar Menüsündeki Kilit Ayarları Öğeleri

Bu, Kilit Ayarları tarafından kontrol panelindeki **Ayarlar** menüsünde kilitlenen öğelerin listesidir.

✓: kilitlenecek.

- : kilitlenmeyecek.

Ayarlar menüsü	Kilit Ayarları
Temel Ayarlar	-

Ayarlar menüsü		Kilit Ayarları
	LCD Parlaklığı	-
	Sesler	-
	Uyku Zmnlaycsı	✓
	Kapanma Zamanı	✓
	Tarih/Saat Ayarları	✓
	Dil/Language	✓/-*
	Klavye (Bölgenize bağlı olarak bu özellik kullanılamayabilir.)	-
	Çalışma Zaman Aşımı	✓
	PC Bğlntısı USB üzerinden	✓
	Direkt güç açma	✓
Tarayıcı Ayarları		-
	Yavaş	-
	Çift Besleme Durdurma Zamanlaması	✓
	DFDS İşlevi	-
	Kâğıt Koruması	✓
	Cam Kiri Algılama	✓
	Yüksek Frekanslı Çift Besleme Algıml	✓
	Otomatik Besleme Modu Zaman Aşımı	✓
	Alıcıyı Onayla	✓
Ana Ekranı Düzenle		✓
	Düzen	✓
	Simge Ekle	✓
	Simge Kaldır	✓
	Simge Taşı	✓
	Varsayılan Simge Gösterimine Geri Al	✓
	Duvar Kâğıdı	✓
Kullanıcı Ayarları		✓
	Ağ Klasörü/FTP	✓
	E-posta	✓
	Bulut	✓
	USB Sürücü	✓

Ayarlar menüsü		Kilit Ayarları
Ağ Ayarları		✓
	Wi-Fi Ayarı	✓
	Kablolu LAN Ayarı	✓
	Ağ Durumu	✓
	Gelişmiş	✓
Web Hizmeti Ayarları		✓
	Epson Connect Servisleri	✓
Document Capture Pro		-
	Ayarları Değiştir	✓
İrtibatlar Yöneticisi		-
	Kayıt ol/Sil	✓/-*
	Sık	-
	Seçenekleri Görüntüle	-
	Arama Seçenekleri	-
Sistem Yöneticisi		✓
	İrtibatlar Yöneticisi	✓
	Yntci Ayarları	✓
	Kısıtlamalar	✓
	Parola ile Şifreleme	✓
	Müşteri Araştırması	✓
	WSD Ayarları	✓
	Varsayılan Ayarları Geri Yükle	✓
	Aygıt Yazılımı Güncelleme	✓
Aygıt Bilgileri		-

Ayarlar menüsü			Kilit Ayarları
	Seri Numarası		-
	Geçerli Sürüm		-
	Toplam Tarama Sayısı		-
	1 Taraflı Tarama Sayısı		-
	2 Taraflı Tarama Sayısı		-
	Taşıyıcı Kağıt Tarama Sayısı		-
	Silindirin Değiştirilmesinden Sonra Tarama Sayısı		-
	Düzenli Temizlik Sonrasındaki Tarama Sayısı		-
	Tarama Sayısını Sıfırla		✓
Tarayıcı Bakımı			-
	Silindir Temizliği		-
	Silindir Değişimi		-
		Tarama Sayısını Sıfırla	✓
		Değiştirme Yöntemi	-
	Düzenli Temizlik		-
		Tarama Sayısını Sıfırla	✓
		Temizleme Yöntemi	-
	Cam Temizleme		-
Silindir Değiştirme Uyarısı Ayarı			✓
	Uyarı Ayarı Sayımı		✓
Düzenli Temizlik Uyarı Ayarları			✓
	Uyarı İkaz Ayarı		✓
	Uyarı Ayarı Sayımı		✓

* Değişikliklere **Sistem Yöneticisi** > **Kısıtlamalar** içinde izin verilip verilmeyeceğini ayarlayabilirsiniz.

Kontrol Panelinden Yönetici olarak Giriş Yapma

Tarayıcının kontrol panelinden yönetici olarak giriş yapmak için aşağıdaki yöntemlerden birini kullanabilirsiniz.

- Ekranın sağ üstündeki  ögesine dokununuz.
 - ☐ Kimlik Doğrulama Ayarları ögesi etkinleştirildiğinde, simge **Hoş Geldiniz** ekranında görüntülenir (kimlik doğrulama bekleme ekranı).
 - ☐ Kimlik Doğrulama Ayarları devre dışı bırakıldığında, simge Ana ekranda görüntülenir.

2. Onay ekranı görüntülendiğinde **Evet** ögesine dokununuz.
3. Yönetici parolasını giriniz.
Giriş yapma tamamlandı mesajı görüntülenir ve ardından kontrol panelindeki Ana ekran görüntülenir.

Çıkış yapmak için Ana ekranın sağ üstündeki  ögesine dokununuz.

Harici Arayüzü Devre Dışı Bırakma

Cihazı tarayıcıya bağlamak için kullanılan arayüzü devre dışı bırakabilirsiniz. Taramayı ağ yolu dışında bir yola kısıtlamak için kısıtlama ayarlarını yapınız.

Not:

Tarayıcının kontrol panelinde kısıtlama ayarlarını yaptığınızdan da emin olabilirsiniz.

PC Bağlı USB üzerinden: **Ayarlar > Temel Ayarlar > PC Bağlı USB üzerinden**

1. Web Config'e erişin ve **Ürün Güvenliği** sekmesi > **Harici Arabirim** ögesini seçin.
2. Ayarlamak istediğiniz işlevlerde **Devre dışı bırak** ögesini seçin.
Kontrol etmeyi iptal etmek istediğinizde **Etkinleştir** ögesini seçin.
PC Bağlı USB üzerinden
USB bağlantısının kullanımını bilgisayardan kısıtlayabilirsiniz. Kısıtlamak istiyorsanız, **Devre dışı bırak** ögesini seçin.
3. **Tamam** ögesine tıklayın.
4. Devre dışı bırakılan bağlantı noktasının kullanılmadığını kontrol edin.
PC Bağlı USB üzerinden
Sürücü bilgisayara yüklendiyse
Tarayıcıyı bilgisayara bir USB kablosu kullanarak bağlayın ve ardından, tarayıcının taramadığını onaylayın.
Sürücü bilgisayara yüklenmediyse
Windows:
Cihaz yöneticisini açın ve açık tutun, tarayıcıyı bilgisayara bir USB kablosu kullanarak bağlayın ve ardından, cihaz yöneticisi ekranı içeriğinin değişmeden kaldığını onaylayın.
Mac OS:
Tarayıcıyı bilgisayara bir USB kablosu kullanarak bağlayın ve ardından, tarayıcıyı **Yazıcılar ve Tarayıcılar** ögesinden ekleyemediğinizi onaylayın.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırma Çalıştırma” sayfa 35](#)

Uzak Tarayıcıyı İzleme

Uzak Tarayıcı İçin Bilgileri Kontrol Etme

Durum ögesinden çalışan tarayıcının aşağıdaki bilgilerini Web Config'i kullanarak kontrol edebilirsiniz.

☐ Ürün Durumu

Durumu, bulut hizmetini, ürün numarasını, MAC adresini vb. kontrol edin.

☐ Ağ Durumu

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

☐ Kullanım Durumu

İlk tarama gününü, tarama sayısını vb. kontrol edin.

☐ Donanım Durumu

Tarayıcının her işlevinin durumunu kontrol edin.

☐ Panel Anlık Görüntüsü

Tarayıcının kontrol panelinde görüntülenen bir ekran anlık görüntüsünü görüntüler.

Olaylar Meydana Geldiğinde E-posta Bildirimi Alma

E-posta Bildirimleri Hakkında

Bu, taramanın durdurulması ve tarayıcı hatası oluşması, e-postanın belirtilen adrese gönderilmesi gibi olaylar olduğunda bildirim işlevidir.

Beş kadar hederi kaydedebilir ve her hedef için bildirim ayarlarını yapabilirsiniz.

Bu işlevi kullanmak için bildirimleri ayarlamadan önce posta sunucusunu ayarlamanız gerekir.

İlgili Bilgi

➔ [“Posta Sunucusu Yapılandırma” sayfa 41](#)

E-posta Bildirimini Yapılandırma

Web Config'i kullanarak e-posta bildirimini yapılandırın.

1. Web Config'e erişin ve **Aygıt Yönetimi** sekmesi > **E-posta Bildirimi** ögesini seçin.
2. E-posta bildiriminin konusunu ayarlayın.
İki aşağı açılır menüden konuda görüntülenen içeriği seçin.
 - ☐ Seçili içerik **Konu** yanında görüntülenir.
 - ☐ Aynı içerik sol ve sağda ayarlanamaz.
 - ☐ **Konum** içindeki karakter sayısı 32 baytı aştığında, 32 baytı aşan karakterler atlanır.

3. Bildirim e-postasını göndermek için e-posta adresini girin.

Şunları kullanın: A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @ ve 1 ve 255 arası karakter girin.

4. E-posta bildirimleri için dili seçin.

5. Bir bildirim almak istediğiniz olayın onay kutusunu seçin.

Bildirim Ayarları sayısını **E-posta Adresi Ayarları** hedef numarasına bağlayın.

Örnek:

Yönetici parolası değiştiğinde **E-posta Adresi Ayarları** içinde numara 1 için ayarlanan e-posta adresine bir bildirim göndermek istiyorsanız **Yönetici şifresi değiştirildi** satırında sütun 1 onay kutusunu seçin.

6. **Tamam** ögesine tıklayın.

Bir olaya neden olan bir e-posta bildiriminin gönderileceğini onaylayın.

Örnek: Yönetici parolası değişmiştir.

İlgili Bilgi

➡ “Web Tarayıcıda Web Yapılandırma Çalıştırma” sayfa 35

E-posta Bildirimi İçin Öğeler

Öğeler	Ayarlar ve Açıklama
Yönetici şifresi değiştirildi	Yönetici parolası değiştiğinde bildirim.
Tarayıcı hatası	Tarayıcı hatası oluştuğunda bildirim.
Wi-Fi hatası	Kablosuz LAN arayüzü hatası oluştuğundaki bildirim.

Sorunları Çözme

Şifrenizi mı Unuttunuz

Hizmet personelinden yardım almanız gerekiyor. Yerel satıcınızla iletişim kurun.

Not:

Aşağıda, Web Config yöneticisi bilgileri için başlangıç değerleri sağlanmaktadır.

☐ Kullanıcı adı: yok (boş)

☐ Şifre: tarayıcının seri numarası

Seri numarasını bulmak için tarayıcının arkasına yapıştırılmış etiketi kontrol edin. Yönetici şifresi için varsayılan ayarları geri yüklerseniz, başlangıç değerlerine sıfırlanır.

Gelişmiş Güvenlik Ayarları

Güvenlik Ayarları ve Tehlikeyi Önleme.	93
İletişim Kurallarını Denetleme ve Kullanma.	94
Dijital Sertifika Kullanımı.	97
Tarayıcıyla SSL/TLS İletişimi.	102
IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim.	104
Tarayıcıyı Bir IEEE802.1X Ağına Bağlama.	114
Gelişmiş Güvenlik İçin Sorunları Çözme.	116

Güvenlik Ayarları ve Tehlikeyi Önleme

Bit tarayıcı bir ağa bağlandığında cihaza uzak bir konumdan erişebilirsiniz. Ek olarak, çoğu insan çalışma etkinliğini ve rahatlığını iyileştirmeye yardımcı olacak şekilde tarayıcıyı paylaşabilir. Ancak, yasal olmayan erişim, yasal olmayan kullanım ve verilerde değiştirme gibi riskler artar. Tarayıcıyı İnternet'e erişebileceğiniz bir ortamda kullanırsanız riskler daha da büyür.

Dışarıdan erişim koruması olmayan tarayıcılar için İnternet'ten tarayıcıda depolanan kişileri okumak mümkün olacaktır.

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

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

Ad	Özellik türü	Ayarlanacak öğe	Neyi öner
Protokollerin kontrolü	Tarayıcılar ve bilgisayarlar arasında iletişim için kullanılacak protokoller ve hizmetleri kontrol eder ve özellikleri etkinleştirir ve 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.
SSL/TLS iletişimleri	Epson Connect kullanılarak ve belenim güncellenerek web tarayıcısından bilgisayarla iletişim kurma gibi İnternet'te tarayıcıdan Epson sunucusuna erişirken iletişim içeriği SSL/TLS iletişimleriyle şifrelenir.	Bir CA imzalı sertifika edinin ve ardından, onu tarayıcıya alın.	CA imzalı sertifika ile bir tarayıcı kimliğini temizleme kişiselleştirme ve yetkisi erişimi önler. Ek olarak, SSL/TLS'nin iletişim içeriği korunur ve verileri tarama ve kurulum bilgileri için içeriğin sızmasını önler.
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 protokolle güvenli bir şekilde iletişim kurabilirsiniz.	Tarayıcıya erişebilen istemciyi veya veri türünü ayarlamak için temel bir ilke ve özel ilke oluşturun.	Yetkisiz erişime ve değiştirmeye ve tarayıcıya ulaşan iletişim verilerinin kuralanmasına ve kesilmesine karşı koruyun.
IEEE 802.1X	Yalnızca kimliği doğrulanan kullanıcıların ağa bağlanmasına izin verir. Yalnızca izin verilen bir kullanıcının tarayıcıyı kullanmasına izin verir.	RADIUS sunucusuna kimlik doğrulama ayarı (kimlik doğrulama sunucusu).	Kimliği doğrulanmamış erişime ve tarayıcının kullanılmasına karşı koruyun.

İlgili Bilgi

- ➔ [“İletişim Kurallarını Denetleme ve Kullanma” sayfa 94](#)
- ➔ [“Tarayıcıyla SSL/TLS İletişimi” sayfa 102](#)
- ➔ [“IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim” sayfa 104](#)
- ➔ [“Tarayıcıyı Bir IEEE802.1X Ağına Bağlama” sayfa 114](#)

Güvenlik Özelliği Ayarları

IPsec/IP filtresi veya IEEE 802.1X'i ayarlarken, ayarlar bilgileriyle iletişim kurmak için değiştirme veya durdurma gibi güvenlik risklerini azaltmak için Web Config'e SSL/TLS'yi kullanarak erişmeniz önerilir.

IPsec/IP filtresi veya IEEE 802.1X'i ayarlamadan önce yönetici parolasını yapılandırdığınızdan emin olun.

İletişim Kurallarını Denetleme ve Kullanma

Çeşitli yolları ve iletişim kurallarını kullanarak tarayabilirsiniz. Belirtilmeyen sayıda ağ bilgisayarından ağ taramasını da kullanabilirsiniz.

Belirli yollardan taramayı kısıtlayarak veya kullanılabilir işlevleri denetleyerek istenmeyen güvenlik risklerini azaltabilirsiniz.

İletişim kurallarını denetleme

Tarayıcı tarafından desteklenen protokol ayarlarını yapılandırın.

1. Web Config'e erişin ve ardından, **Ağ Güvenliği** tab > **İletişim Kuralı** ögesini seçin.
2. Her bir ögeyi yapılandırın.
3. **İleri** ögesine tıklayın.
4. **Tamam** ögesine tıklayın.
Ayarlar tarayıcıya uygulanır.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Etkinleştirebileceğiniz veya Devre Dışı Bırakabileceğiniz İletişim Kuralları

Protokol	Açıklama
Bonjour Ayarları	Bonjour kullanılıp kullanılmayacağını belirleyebilirsiniz. Bonjour cihazları aramak, taramak ve benzeri işlemler için kullanılır.
SLP Ayarları	SLP işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. SLP, EpsonNet Config yazılımında itmeli tarama ve ağ arama için kullanılır.
WSD Ayarları	WSD işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde WSD cihazları ekleyebilir ve WSD bağlantı noktasından tarayabilirsiniz.
LLTD Ayarları	LLTD işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde, Windows ağ haritasında görüntülenir.

Protokol	Açıklama
LLMNR Ayarları	LLMNR işlevini etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu etkinleştirildiğinde, NetBIOS kullanamasanız bile DNS. olmadan ad çözümlemesini kullanabilirsiniz.
SNMPv1/v2c Ayarları	SNMPv1/v2c özelliğinin etkinleştirilip etkinleştirilmeyeceğini belirleyebilirsiniz. Bu, cihazları ayarlama, izleme ve benzeri işlemler için kullanılır.
SNMPv3 Ayarları	SNMPv3 özelliğinin etkinleştirilip etkinleştirilmeyeceğini belirleyebilirsiniz. Bu, şifreli cihazları ayarlama, izleme vb. için kullanılır.

İletişim Kuralı Ayarlama Öğeleri

Bonjour Ayarları

Öğeler	Ayar değeri ve Açıklama
Bonjour Kullan	Bonjour aracılığıyla cihazları aramak veya kullanmak için bu- nu seçin.
Bonjour Adı	Bonjour adını görüntüler.
Bonjour Hizmet Adı	Bonjour hizmet adını görüntüler.
Konum	Bonjour konum adını görüntüler.
Wide-Area Bonjour	Wide-Area Bonjour'u kullanıp kullanmamayı ayarlayın.

SLP Ayarları

Öğeler	Ayar değeri ve Açıklama
SLP Etkinleştir	SLP işlevini etkinleştirmek için bunu seçin. Bu, EpsonNet Config içinde ağ arama gibi kullanılır.

WSD Ayarları

Öğeler	Ayar değeri ve Açıklama
WSD Etkinleştir	WSD kullanarak cihazlar eklemeyi etkinleştirmek için bunu seçin ve WSD bağlantı noktasından tarayın.
Tarama Zaman Aşımı (sn.)	WSD taramaya yönelik iletişim zaman aşımı değerini 3 ila 3.600 saniye arasında girin.
Aygıt Adı	WSD cihaz adını görüntüler.
Konum	WSD konum adını görüntüler.

LLTD Ayarları

Öğeler	Ayar değeri ve Açıklama
LLTD Etkinleştir	LLTD etkinleştirmek için bunu seçin. Tarayıcı Windows ağ ha- ritasında görüntülenir.

Öğeler	Ayar değeri ve Açıklama
Aygıt Adı	LLTD cihaz adını görüntüler.

LLMNR Ayarları

Öğeler	Ayar değeri ve Açıklama
LLMNR Etkinleştir	LLMNR etkinleştirmek için bunu seçin. NetBIOS kullanamasa-nız bile DNS olmadan ad çözümlemesini kullanabilirsiniz.

SNMPv1/v2c Ayarları

Öğeler	Ayar değeri ve Açıklama
SNMPv1/v2c Etkinleştir	SNMPv1/v2c etkinleştirmek için seçin.
Erişim Yetkisi	SNMPv1/v2c etkinleştirildiğinde erişim yetkilisini ayarlayın. Salt Okunur veya Okuma/Yazma ögesini seçin.
Topluluk Adı (Yalnızca Okuma)	0 ila 32 ASCII (0x20 ila 0x7E) karakter girin.
Topluluk Adı (Okuma/Yazma)	0 ila 32 ASCII (0x20 ila 0x7E) karakter girin.

SNMPv3 Ayarları

Öğeler		Ayar değeri ve Açıklama
SNMPv3 Etkinleştir		Kutu işaretlendiğinde SNMPv3 etkindir.
Kullanıcı Adı		1 bayt karakterleri kullanarak 1 ve 32 karakter arası girin.
Kimlik Doğrulama Ayarları		
	Algoritma	SNMPv3 için kimlik doğrulama için bir algoritma seçin.
	Parola	SNMPv3 için kimlik doğrulama için parolayı girin. 8 ve 32 karakter arası ASCII (0x20–0x7E) girin. Bunu belirtmezseniz boş bırakın.
	Şifreyi Onayla	Yapılandırduğınız parolayı onay için girin.
Şifreleme Ayarları		
	Algoritma	SNMPv3 için şifreleme için bir algoritma seçin.
	Parola	SNMPv3 için şifreleme için parolayı girin. 8 ve 32 karakter arası ASCII (0x20–0x7E) girin. Bunu belirtmezseniz boş bırakın.
	Şifreyi Onayla	Yapılandırduğınız parolayı onay için girin.
İçerik Adı		32 karakter veya daha kısa Unicode (UTF-8) girin. Bunu belirtmezseniz boş bırakın. Girilebilen karakter sayısı dile bağlı olarak değişir.

Dijital Sertifika Kullanımı

Dijital Sertifikasyon Hakkında

❑ CA İmzalı Sertifika

Bu, CA (Sertifika Yetkilisi) tarafından imzalanan bir sertifikadır. Sertifika Yetkilisi'ne uygulamak için bunu alabilirsiniz. Bu sertifika tarayıcının bulunduğu belgeler ve SSL/TLS iletişimi için kullanılır, bu yüzden veri iletişimi güvenliğini sağlayabilirsiniz.

SSL/TLS iletişimi için kullanıldığında, bir sunucu sertifikası olarak kullanılır.

IPsec/IP Filtreleme veya IEEE 802.1X iletişimi olarak ayarlandığında, bir istemci sertifikası olarak kullanılır.

❑ CA Sertifikası

Bu, CA İmzalı Sertifika zincirinde bir sertifikadır, ayrıca orta CA sertifikası olarak adlandırılır. Diğer tarafın veya Web Config'in sunucusuna erişirken web tarayıcısı tarafından tarayıcı sertifikası yolunu doğrulamak için kullanılır.

CA Sertifikası için tarayıcıdan erişilen sunucu sertifikası yolunu doğrularken ayarlayın. Tarayıcı için SSL/TLS bağlantısı için CA İmzalı Sertifika yolunu onaylamak için ayarlayın.

tarayıcının CA sertifikasını CA sertifikasının verdiği Sertifika Yetkilisi'nden alabilirsiniz.

Ayrıca, diğer sunucunun CA İmzalı Sertifika ögesini veren Sertifika Yetkilisi'nden diğer tarafın sunucusunu doğrulamak için kullanılan CA sertifikasını alabilirsiniz.

❑ Kendinden İmzalı Sertifika

Bu, tarayıcının imzaladığı ve kendisi verdiği bir sertifikadır. Kök sertifika olarak da adlandırılır. Verici kendisini belgelediğinden güvenilir değildir ve kişiselleştirmeyi önleyemez.

Güvenlik ayarı yaparken ve CA İmzalı Sertifika olmadan basit SSL/TLS iletişimi gerçekleştirirken kullanın.

Bir SSL/TLS iletişimi için bu sertifikayı kullanıyorsanız, sertifika bir web tarayıcısında kaydedilmediğinden web tarayıcısında bir güvenlik uyarısı görüntülenebilir. Kendinden İmzalı Sertifika ögesini yalnızca bir SSL/TLS iletişimi için kullanabilirsiniz.

İlgili Bilgi

- ➔ [“CA İmzalı Sertifika Yapılandırma” sayfa 97](#)
- ➔ [“Kendinden İmzalı Sertifika Güncelleme” sayfa 101](#)
- ➔ [“CA Sertifikası Yapılandırma” sayfa 101](#)

CA İmzalı Sertifika Yapılandırma

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 bilgisayar 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 **Ağ Güvenliği** sekmesini seçin. Sonra, **SSL/TLS > Sertifika** veya **IPsec/IP Filtreleme > İstemci Sertifikası** veya **IEEE802.1X > İstemci Sertifikası** ögesini seçin.

Neyi seçerseniz seçin, aynı sertifikayı alabilir ve ortak olarak kullanabilirsiniz.

2. **Oluştur CSR** ögesine tıklayın.

CSR oluşturma sayfası açılır.

3. Her öge için bir değer girin.

Not:

İzin verilen anahtar uzunluğu ve kısaltmalar sertifika yetkilisine bağlı olarak değişir. Her sertifika yetkilisinin kurallarına uygun talep hazırlayın.

4. **Tamam** ögesine tıklayın.

Bir tamamlanma mesajı görüntülenir.

5. **Ağ Güvenliği** sekmesini seçin. Sonra, **SSL/TLS > Sertifika** veya **IPsec/IP Filtreleme > İstemci Sertifikası** veya **IEEE802.1X > İstemci Sertifikası** ögesini 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 İmzalı Sertifika içe aktarılamayabilir.

7. Bir sertifika yetkilisine CSR'yi gönderin ve bir CA İmzalı Sertifika alın.

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

8. Verilen CA İmzalı Sertifika ögesini tarayıcıya bağlı bir bilgisayara kaydedin.

Sertifikayı bir hedefe kaydettiğinizde CA İmzalı Sertifika alma işlemi tamamlanmış olur.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

CSR Ayarlama Öğeleri

Öğeler	Ayarlar ve Açıklama
Anahtar Uzunluğu	CSR için anahtar uzunluğu seçin.

Öğeler	Ayarlar ve Açıklama
Ortak Ad	1 ve 128 karakter arası girebilirsiniz. Bu bir IP adresi ise, sabit bir IP adresi olmalıdır. 1 ila 5 arası IPv4 adresi, IPv6 adresi, ana bilgisayar adı, FQDN virgüllerle ayırarak girebilirsiniz. İlk öğe ortak adda depolanır ve diğer öğeler sertifika konusunun takma ad alanında depolanır. Örnek: Tarayıcının IP adresi: 192.0.2.123, Tarayıcı adı: EPSONA1B2C3 Ortak Ad: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Kuruluş/ Kuruluş Birimi/ Bölge/ Eyalet/İl	0 ve 64 karakter arası ASCII (0x20–0x7E) girebilirsiniz. Belirleyici isimleri virgüllerle ayırabilirsiniz.
Ülke	ISO-3166 tarafınca belirlenmiş iki haneli bir şehir kodu girin.
Gönderenin Eposta Adresi	Posta sunucusu ayarı için gönderenin e-posta adresini girebilirsiniz. Ağ sekmesi > E-posta Sncsu > Temel için Gönderenin Eposta Adresi olarak aynı e-posta adresini girin.

CA İmzalı bir Sertifikanın İçe Aktarımı

Alınan CA İmzalı Sertifika öğesini tarayıcıya aktarın.



Önemli:

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

1. Web Config'e erişin ve ardından, **Ağ Güvenliği** sekmesini seçin. Sonra, **SSL/TLS** > **Sertifika** veya **IPsec/IP Filtreleme** > **İstemci Sertifikası** veya **IEEE802.1X** > **İstemci Sertifikası** öğesini seçin.

2. **İçe Aktar** öğesine tıklayın

Sertifika içe aktarım sayfası açılır.

3. Her öğe için bir değer girin. Tarayıcıya erişen web tarayıcısında sertifikanın yolunu doğrularken **CA Sertifikası 1** ve **CA Sertifikası 2** öğesini ayarlayın.

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
 - ☐ **Özel Anahtar:** Tarayıcının özel bir anahtarı olduğu için yapılandırmayın.
 - ☐ **Parola:** Yapılandırmayın.
 - ☐ **CA Sertifikası 1/CA Sertifikası 2:** İsteğe bağlı
- ☐ Bilgisayardan alınmış, PEM/DER formatında bir sertifika
 - ☐ **Özel Anahtar:** Ayarlamamız gerekir.
 - ☐ **Parola:** Yapılandırmayın.
 - ☐ **CA Sertifikası 1/CA Sertifikası 2:** İsteğe bağlı

- ☐ Bilgisayardan alınmış, PKCS#12 formatında bir sertifika
- ☐ **Özel Anahtar:** Yapılandırmayın.
- ☐ **Parola:** İsteğe bağlı
- ☐ **CA Sertifikası 1/CA Sertifikası 2:** Yapılandırmayın.

4. **Tamam** ögesine tıklayın.

Bir tamamlanma mesajı görüntülenir.

Not:

Sertifika bilgisini doğrulamak için **Onayla** ögesine tıklayın.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

CA-imzalı Sertifika Alma Ayar Öğeleri

Öğeler	Ayarlar ve Açıklama
Sunucu Sertifikası veya İstemci Sertifikası	Bir sertifikanın biçimini seçin. SSL/TLS bağlantısı için Sunucu Sertifikası görüntülenir. IPsec/IP Filtreleme veya IEEE 802.1X için İstemci Sertifikası görüntülenir.
Özel Anahtar	Bilgisayardan oluşturulmuş bir CSR kullanarak PEM/DER biçiminin bir sertifikasını alırsanız bir sertifikayla eşleşen bir özel anahtar dosyası belirtin.
Parola	Dosya biçimi Özel Anahtarlı Sertifika (PKCS#12) ise sertifika aldığınızda ayarlanmış özel anahtarı şifrelemek için parolayı girin.
CA Sertifikası 1	Sertifikanın biçimi Sertifika (PEM/DER) ise sunucu sertifikası olarak kullanılan bir CA İmzalı Sertifika veren sertifika yetkilisinin bir sertifikasını alın. Gerekirse bir dosya belirtin.
CA Sertifikası 2	Sertifikanızın biçimi Sertifika (PEM/DER) ise CA Sertifikası 1 veren sertifika yetkilisinin bir sertifikasını alın. Gerekirse bir dosya belirtin.

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.

- Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesini seçin. Sonra, **SSL/TLS > Sertifika veya IPsec/IP Filtreleme > İstemci Sertifikası veya IEEE802.1X > İstemci Sertifikası** ögesini seçin.
- Sil** ögesine tıklayın.

3. Görüntülenen mesajda, sertifikayı silmek istediğinizi onaylayın.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Kendinden İmzalı Sertifika Güncelleme

Kendinden İmzalı Sertifika tarayıcı tarafından verildiğinden, süresi dolduğunda veya açıklanan içerik değiştiğinde güncelleyebilirsiniz.

1. Web Config’e erişin ve **Ağ Güvenliği** tab > **SSL/TLS** > **Sertifika** ögesini seçin.
2. **Güncelle** ögesine tıklayın.
3. **Ortak Ad** girin.

5 kadar IPv4 adresi, IPv6 adresi, ana bilgisayar adı, 1 ila 128 karakter arası FQDN girebilir ve bunları virgüllerle ayırabilirsiniz. İlk parametre ortak adda depolanır ve diğerleri sertifikanın konusu için takma ad alanında depolanır.

Örnek:

Tarayıcının IP adresi: 192.0.2.123, Tarayıcı adı: EPSONA1B2C3

Ortak isim: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Sertifika için bir geçerlilik süresi belirleyin.
5. **İleri** ögesine tıklayın.
Bir doğrulama mesajı görüntülenir.
6. **Tamam** ögesine tıklayın.
Tarayıcı güncelleştirilmiştir.

Not:

Ağ Güvenliği sekmesi > **SSL/TLS** > **Sertifika** > **Kendinden İmzalı Sertifika** ögesinden sertifika bilgilerini kontrol edebilir ve **Onayla** ögesini tıklatabilirsiniz.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

CA Sertifikası Yapılandırma

CA Sertifikası ögesini ayarladığınızda tarayıcının eriştiği sunucunun CA sertifikasına olan yolu doğrulayabilirsiniz. Bu, kişiselleştirmeyi önleyebilir.

CA Sertifikası ögesini CA İmzalı Sertifika verildiği Sertifika Yetkilisi’nden alabilirsiniz.

Bir CA Sertifikası içe aktarma

CA Sertifikası ögesini tarayıcıya aktarın.

1. Web Config'e erişin ve ardından, **Ağ Güvenliği** sekmesi > **CA Sertifikası** ögesini seçin.
2. **İçe Aktar** ögesine tıklayın.
3. İçe aktarmak istediğiniz CA Sertifikası ögesini belirleyin.
4. **Tamam** ögesine tıklayın.

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

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

CA Sertifikası Silme

Alınan CA Sertifikası ögesini silebilirsiniz.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **CA Sertifikası** ögesini seçin.
2. Silmek istediğiniz CA Sertifikası yanındaki **Sil** ögesine tıklayın.
3. Görüntülenen mesajda sertifikayı silmek istediğinizi onaylayın.
4. **Ağı Yeniden Başlat** ögesine tıklayın ve sonra silinen CA Sertifikasının güncellenen ekranda listelenmediğini kontrol edin.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Tarayıcıyla SSL/TLS İletişimi

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

Temel SSL/TLS Ayarlarını Yapılandırma

Tarayıcı HTTPS sunucu özelliğini destekliorsa iletişimlerini şifrelemek için bir SSL/TLS iletişimi kullanabilirsiniz. Güvenliği sağlayarak tarayıcıyı Web Config kullanarak yapılandırabilir ve yönetebilirsiniz.

Şifreleme gücünü yapılandırın ve özelliği yönlendirin.

1. Web Config'e erişin ve **Ağ Güvenliği** sekmesi > **SSL/TLS** > **Temel** ögesini seçin.
2. Her öge için bir değer seçin.
 - ☐ Şifreleme Gücü
Şifreleme gücü düzeyini seçin.
 - ☐ HTTP iletişimini HTTPS iletişimine yönlendir
HTTP'ye erişildiğinde HTTPS'ye yönlendirin.
3. **İleri** ögesine tıklayın.
Bir onay mesajı görüntülenir.
4. **Tamam** ögesine tıklayın.
Tarayıcı güncellenir.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Tarayıcı için Sunucu Sertifikası Yapılandırma

1. Web Config'e erişin ve **Ağ Güvenliği** sekmesi > **SSL/TLS** > **Sertifika** ögesini seçin.
2. **Sunucu Sertifikası** ile kullanmak için bir sertifika belirleyin.
 - ☐ Kendinden İmzalı Sertifika
Tarayıcı tarafından kendinden imzalı bir sertifika oluşturuldu. CA imzalı bir sertifika almadıysanız bunu seçin.
 - ☐ CA İmzalı Sertifika
Önceden CA imzalı sertifika almış ve içe aktarımı gerçekleştirmişseniz, bunu yapabilirsiniz.
3. **İleri** ögesine tıklayın.
Bir doğrulama mesajı görüntülenir.
4. **Tamam** ögesine tıklayın.
Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

- ➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)
➔ [“CA İmzalı Sertifika Yapılandırma” sayfa 97](#)
➔ [“CA Sertifikası Yapılandırma” sayfa 101](#)

IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim

IPsec/IP Filtreleme Hakkında

IPsec/IP Filtreleme işlevini kullanarak 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.

Not:

Windows Vista veya üstünü ya da Windows Server 2008 veya üstünü çalıştıran bilgisayarlar IPsec'i destekler.

Varsayılan İlkeyi Yapılandırma

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.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** ögesini seçin.
2. Her öge için bir değer girin.
3. **İleri** ögesine tıklayın.
Bir doğrulama mesajı görüntülenir.
4. **Tamam** ögesine tıklayın.
Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Varsayılan İlke Ayarlama Öğeleri

Varsayılan İlke

Öğeler	Ayarlar ve Açıklama
IPsec/IP Filtreleme	IPsec/IP Filtre özelliğini etkinleştirebilir ya da devre dışı bırakabilirsiniz.

☐ Erişim Denetimi

IP paketlerinin trafiği için bir kontrol yöntemi yapılandırın.

Öğeler	Ayarlar ve Açıklama
Erişime İzin Ver	Yapılandırılmış IP paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
Erişimi Reddet	Yapılandırılmış IP paketlerinin düz geçişlerini reddetmek için bu öğeyi seçin.
IPsec	Yapılandırılmış IPsec paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.

☐ IKE Sürümü

IKE Sürümü için **IKEv1** veya **IKEv2** ögesini seçin. Tarayıcının bağlı olduğu cihaza göre bunlardan birini seçin.

☐ IKEv1

IKE Sürümü için **IKEv1** ögesini seçtiğinizde aşağıdaki ögeler görüntülenir.

Öğeler	Ayarlar ve Açıklama
Doğrulama Yöntemi	Sertifika ögesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
Önceden Paylaşılmış Anahtar	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
Önceden Paylaşılmış Anahtarı Onayla	Yapılandırığınız anahtarı onay için girin.

☐ IKEv2

IKE Sürümü için **IKEv2** ögesini seçtiğinizde aşağıdaki ögeler görüntülenir.

Öğeler	Ayarlar ve Açıklama
Lokal	Doğrulama Yöntemi
	Sertifika ögesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
	Kimlik Türü
	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz tarayıcının kimlik türünü seçin.
	Kimlik
	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@" , "#" ve "=" ögelerini kullanamazsınız. Ayrıcalıklı Ad: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" ögesini eklemeniz gerekir. IP Adresi: IPv4 veya IPv6 biçimini girin. FQDN: A–Z, a–z, 0–9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. Eposta Adresi: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" ögesini eklemeniz gerekir. Anahtar Kimliği: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Önceden Paylaşılmış Anahtar
	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Önceden Paylaşılmış Anahtarı Onayla
	Yapılandırığınız anahtarı onay için girin.

Öğeler		Ayarlar ve Açıklama
Uzak	Doğrulama Yöntemi	Sertifika öğesini seçmek için önceden CA imzalı sertifika almış ve iç aktarımını gerçekleştirmiş olmalısınız.
	Kimlik Türü	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar öğesini seçerseniz, kimlik doğrulamasını yapmak istediğiniz cihazın kimlik türünü seçin.
	Kimlik	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@", "#" ve "=" öğelerini kullanamazsınız. Ayrıcalıklı Ad: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" öğesini eklemeniz gerekir. IP Adresi: IPv4 veya IPv6 biçimini girin. FQDN: A-Z, a-z, 0-9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. Eposta Adresi: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" öğesini eklemeniz gerekir. Anahtar Kimliği: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Önceden Paylaşılmış Anahtar	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar öğesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Önceden Paylaşılmış Anahtarı Onayla	Yapılandırduğunuz anahtarı onay için girin.

☐ Kuşatma

IPsec için **Erişim Denetimi** öğesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.

Öğeler	Ayarlar ve Açıklama
Taşıma Modu	Aynı LAN üzerinde sadece tarayıcıyı kullanırsanız bu öğeyi seçin. Katman 4 ya da sonraki IP paketleri şifrelenmiştir.
Tünel Modu	Tarayıcıyı IPsec-VPN gibi İnternet özellikli bir ağda kullanıyorsanız bu seçeneği seçin. IP paketlerinin başlıkları ve verileri şifrelenmiştir. Uzak Ağ Geçidi (Tünel Modu): Kuşatma için Tünel Modu öğesini seçerseniz, 1 ve 39 karakter arası bir ağ geçidi adresi girin.

☐ Güvenlik İletişim Kuralı

Erişim Denetimi için **IPsec** öğesini seçerseniz bir seçenek seçin.

Öğeler	Ayarlar ve Açıklama
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.

❑ Algoritma Ayarları

Tüm ayarlar için **Herhangi** ögesini seçmeniz veya her ayar için **Herhangi** dışında bir öge seçmeniz önerilir. Ayarların bazıları için **Herhangi** ögesini seçerseniz ve diğer ayarlar için **Herhangi** dışında bir öge seçerseniz, cihaz kimliğini doğrulamak istediğiniz diğer cihazlara bağlı olarak iletişim kuramayabilir.

Öğeler		Ayarlar ve Açıklama
IKE	Şifreleme	IKE için şifreleme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
	Yetkilendirme	IKE için kimlik doğrulama algoritmasını seçin.
	Anahtar Değişimi	IKE için anahtar değiştirme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
ESP	Şifreleme	ESP için şifreleme algoritmasını seçin. Bu, ESP ögesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.
	Yetkilendirme	ESP için kimlik doğrulama algoritmasını seçin. Bu, ESP ögesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.
AH	Yetkilendirme	AH için şifreleme algoritmasını seçin. Bu, AH ögesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.

Grup İlkesini Yapılandırma

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.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** ögesini seçin.
2. Yapılandırmak istediğiniz numaralandırılmış bir sekmeyi tıklatın.
3. Her öge için bir değer girin.
4. **İleri** ögesine tıklayın.
Bir doğrulama mesajı görüntülenir.
5. **Tamam** ögesine tıklayın.
Tarayıcı güncelleştirilmiştir.

Grup İlkesi Ayarlama Öğeleri

Öğeler	Ayarlar ve Açıklama
Bu Grup İlkesini etkinleştir	Bir grup ilkesi etkinleştirebilir ya da devre dışı bırakabilirsiniz.

Erişim Denetimi

IP paketlerinin trafiği için bir kontrol yöntemi yapılandırın.

Öğeler	Ayarlar ve Açıklama
Erişime İzin Ver	Yapılandırılmış IP paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.
Erişimi Reddet	Yapılandırılmış IP paketlerinin düz geçişlerini reddetmek için bu öğeyi seçin.
IPsec	Yapılandırılmış IPsec paketlerinin düz geçişlerine izin vermek için bu öğeyi seçin.

Yerel Adres (Tarayıcı)

Ağ ortamınızla eşleşen bir IPv4 adresi veya IPv6 adresi seçin. Bir IP adresi otomatik atanırsa, **Otomatik olarak alınan IPv4 adresini kullan** öğesini seçebilirsiniz.

Not:

Bir IPv6 adresi otomatik atandıysa bağlantı kullanılamaz olabilir. Statik bir IPv6 adresi yapılandırın.

Uzak Adres (Ana Bilgisayar)

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.

Bağlantı Noktası Seçme Yöntemi

Bağlantı noktalarını belirtmek için bir yöntem seçin.

☐ Hizmet Adı

Bağlantı Noktası Seçme Yöntemi için **Hizmet Adı** öğesini seçerseniz bir seçenek seçin.

☐ Taşıma İletişim Kuralı

Port Numarası için **Bağlantı Noktası Seçme Yöntemi** öğesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.

Öğeler	Ayarlar ve Açıklama
Herhangi Bir İletişim Kuralı	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.

☐ Yerel Bağlantı Noktası

Bağlantı Noktası Seçme Yöntemi için **Port Numarası** öğesini seçerseniz ve **Taşıma İletişim Kuralı** 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.

☐ Uzak Bağlantı Noktası

Bağlantı Noktası Seçme Yöntemi için **Port Numarası** ögesini seçerseniz ve **Taşıma İletişim Kuralı** için **TCP** veya **UDP** ögesini 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 Sürümü

IKE Sürümü için **IKEv1** veya **IKEv2** ögesini seçin. Tarayıcının bağlı olduğu cihaza göre bunlardan birini seçin.

☐ IKEv1

IKE Sürümü için **IKEv1** ögesini seçtiğinizde aşağıdaki öğeler görüntülenir.

Öğeler	Ayarlar ve Açıklama
Doğrulama Yöntemi	Erişim Denetimi için IPsec ögesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
Önceden Paylaşılmış Anahtar	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
Önceden Paylaşılmış Anahtarı Onayla	Yapılandığınız anahtarı onay için girin.

❑ IKEv2

IKE Sürümü için **IKEv2** ögesini seçtiğinizde aşağıdaki ögeler görüntülenir.

Öğeler		Ayarlar ve Açıklama
Lokal	Doğrulama Yöntemi	Erişim Denetimi için IPsec ögesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
	Kimlik Türü	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz tarayıcının kimlik türünü seçin.
	Kimlik	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@" , "#" ve "=" ögelerini kullanamazsınız. Ayrıcalıklı Ad: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" ögesini eklemeniz gerekir. IP Adresi: IPv4 veya IPv6 biçimini girin. FQDN: A-Z, a-z, 0-9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. Eposta Adresi: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" ögesini eklemeniz gerekir. Anahtar Kimliği: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Önceden Paylaşılmış Anahtar	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Önceden Paylaşılmış Anahtarı Onayla	Yapılandırıdığınız anahtarı onay için girin.
Uzak	Doğrulama Yöntemi	Erişim Denetimi için IPsec ögesini seçerseniz bir seçenek seçin. Kullanılmış sertifika, varsayılan ilke ile ortaktır.
	Kimlik Türü	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, kimlik doğrulamasını yapmak istediğiniz cihazın kimlik türünü seçin.
	Kimlik	Kimliğin türüyle eşleşen tarayıcının kimliğini girin. İlk karakter için "@" , "#" ve "=" ögelerini kullanamazsınız. Ayrıcalıklı Ad: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "=" ögesini eklemeniz gerekir. IP Adresi: IPv4 veya IPv6 biçimini girin. FQDN: A-Z, a-z, 0-9, "-" ve nokta (.) karakterlerini kullanarak 1 ila 255 karakter arası bir kombinasyon girin. Eposta Adresi: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin. "@" ögesini eklemeniz gerekir. Anahtar Kimliği: 1 ila 255 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.
	Önceden Paylaşılmış Anahtar	Doğrulama Yöntemi için Önceden Paylaşılmış Anahtar ögesini seçerseniz, 1 ve 127 karakter arasında önceden paylaşılan bir anahtar girin.
	Önceden Paylaşılmış Anahtarı Onayla	Yapılandırıdığınız anahtarı onay için girin.

Kuşatma

IPsec için **Erişim Denetimi** ögesini seçerseniz, bir kapsülleme modu yapılandırmanız gerekir.

Öğeler	Ayarlar ve Açıklama
Taşıma Modu	Aynı LAN üzerinde sadece tarayıcıyı kullanırsanız bu öğeyi seçin. Katman 4 ya da sonraki IP paketleri şifrelenmiştir.
Tünel Modu	Tarayıcıyı IPsec-VPN gibi İnternet özellikli bir ağda kullanıyorsanız bu seçeneği seçin. IP paketlerinin başlıkları ve verileri şifrelenmiştir. Uzak Ağ Geçidi (Tünel Modu): Kuşatma için Tünel Modu öğesini seçerseniz, 1 ve 39 karakter arası bir ağ geçidi adresi girin.

Güvenlik İletişim Kuralı

Erişim Denetimi için IPsec öğesini seçerseniz bir seçenek seçin.

Öğeler	Ayarlar ve Açıklama
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.

Algoritma Ayarları

Tüm ayarlar için **Herhangi** öğesini seçmeniz veya her ayar için **Herhangi** dışında bir öğe seçmeniz önerilir. Ayarların bazıları için **Herhangi** öğesini seçerseniz ve diğer ayarlar için **Herhangi** dışında bir öğe seçerseniz, cihaz kimliğini doğrulamak istediğiniz diğer cihazlara bağlı olarak iletişim kuramayabilir.

Öğeler	Ayarlar ve Açıklama
IKE	Şifreleme IKE için şifreleme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
	Yetkilendirme IKE için kimlik doğrulama algoritmasını seçin.
	Anahtar Değişimi IKE için anahtar değiştirme algoritmasını seçin. Öğeler IKE sürümüne bağlı olarak değişir.
ESP	Şifreleme ESP için şifreleme algoritmasını seçin. Bu, ESP öğesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.
	Yetkilendirme ESP için kimlik doğrulama algoritmasını seçin. Bu, ESP öğesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.
AH	Yetkilendirme AH için şifreleme algoritmasını seçin. Bu, AH öğesi Güvenlik İletişim Kuralı için seçildiğinde kullanılabilir.

Grup İlkesi üzerinde Yerel Adres (Tarayıcı) ve Uzak Adres (Ana Bilgisayar) birleşimi

	Yerel Adres (Tarayıcı) Öğesini Ayarlama		
	IPv4	IPv6*2	Herhangi bir adres*3

Uzak Adres (Ana Bilgisayar) Ögesini Ayarlama	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Boş	✓	✓	✓

*1 Erişim Denetimi için IPsec seçilirse, örnek uzunluğunu belirtebilirsiniz.

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

*3 IPv6 bağlantı yerel adresleri hariç.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35

Grup İlkesinde Hizmet Adı Referansları

Not:

Kullanılmayan hizmetler görüntülenir ancak seçilemez.

Hizmet adı	Protokol türü	Yerel bağlantı noktası numarası	Uzak bağlantı noktası numarası	Kontrol edilen özellikler
Herhangi	–	–	–	Tüm hizmetler
ENPC	UDP	3289	Herhangi bir bağlantı noktası	Epson Device Admin ve tarayıcı sürücüsü gibi uygulamalardan bir tarayıcı arama
SNMP	UDP	161	Herhangi bir bağlantı noktası	Epson Device Admin 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 tarayıcıları için arama
Network Scan	TCP	1865	Herhangi bir bağlantı noktası	Document Capture Pro ögesinden taranmış verileri iletme
Network Push Scan	TCP	Herhangi bir bağlantı noktası	2968	Document Capture Pro ögesinden itmeli tarama için iş bilgilerini alma
Network Push Scan Discovery	UDP	2968	Herhangi bir bağlantı noktası	Tarayıcıdan bir bilgisayarı arama
FTP Verisi (Uzak)	TCP	Herhangi bir bağlantı noktası	20	FTP istemcisi (taranmış verileri iletme) Ancak, bu yalnızca uzak bağlantı noktası numarası 20 olan bir FTP sunucusunu kontrol edebilir.
FTP Kontrolü (Uzak)	TCP	Herhangi bir bağlantı noktası	21	FTP istemcisi (iletilmiş taranmış verileri kontrol etme)

Hizmet adı	Protokol türü	Yerel bağlantı noktası numarası	Uzak bağlantı noktası numarası	Kontrol edilen özellikler
CIFS (Uzak)	TCP	Herhangi bir bağlantı noktası	445	CIFS istemcisi (taranmış verileri bir klasöre iletme)
NetBIOS Name Service (Uzak)	UDP	Herhangi bir bağlantı noktası	137	CIFS istemcisi (taranmış verileri bir klasöre iletme)
NetBIOS Datagram Service (Uzak)	UDP	Herhangi bir bağlantı noktası	138	
NetBIOS Session Service (Uzak)	TCP	Herhangi bir bağlantı noktası	139	
HTTP (Yerel)	TCP	80	Herhangi bir bağlantı noktası	HTTP(S) sunucusu (Web Config ve WSD verilerini iletme)
HTTPS (Yerel)	TCP	443	Herhangi bir bağlantı noktası	
HTTP (Uzak)	TCP	Herhangi bir bağlantı noktası	80	HTTP(S) istemcisi (bellenim sürümünü ve kök sertifikayı güncelleme)
HTTPS (Uzak)	TCP	Herhangi bir bağlantı noktası	443	

IPsec/IP Filtreleme Yapılandırma Örnekleri

Sadece IPsec paketlerinin alımı

Bu örnek sadece varsayılan ilke yapılandırması içindir.

Varsayılan İlke:

- ☐ IPsec/IP Filtreleme: Etkinleştir
- ☐ Erişim Denetimi: IPsec
- ☐ Doğrulama Yöntemi: Önceden Paylaşılmış Anahtar
- ☐ Önceden Paylaşılmış Anahtar: En fazla 127 karakter girin.

Grup İlkesi: Yapılandırmayın.

Tarama verileri ve tarayıcı ayarlarını alma

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

Varsayılan İlke:

- ☐ IPsec/IP Filtreleme: Etkinleştir
- ☐ Erişim Denetimi: Erişimi Reddet

Grup İlkesi:

- ☐ Bu Grup İlkesini etkinleştir: Kutuyu kontrol edin.
- ☐ Erişim Denetimi: Erişime İzin Ver

- ☐ **Uzak Adres (Ana Bilgisayar):** Bir istemcinin IP adresi
- ☐ **Bağlantı Noktası Seçme Yöntemi: Hizmet Adı**
- ☐ **Hizmet Adı:** ENPC, SNMP, HTTP (Yerel), HTTPS (Yerel) ve Network Scan kutularını işaretleyin.

Sadece belirlenen bir IP adresinden erişim sağlama

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

Varsayılan İlke:

- ☐ **IPsec/IP Filtreleme: Etkinleştir**
- ☐ **Erişim Denetimi: Erişimi Reddet**

Grup İlkesi:

- ☐ **Bu Grup İlkesini etkinleştir:** Kutuyu kontrol edin.
- ☐ **Erişim Denetimi: Erişime İzin Ver**
- ☐ **Uzak Adres (Ana Bilgisayar):** Bir yönetici istemcisinin IP adresi

Not:

İlke yapılandırmasından bağımsız olarak, istemci tarayıcıya erişebilecek ve yapılandırabilecek.

IPsec/IP Filtresi İçin Bir Sertifikayı Yapılandırma

IPsec/IP Filtresi İçin İstemci Sertifikasını yapılandırın. Ayarladığınızda sertifikayı IPsec/IP Filtresi için bir kimlik doğrulama yöntemi olarak kullanabilirsiniz. Sertifika yetkilisini yapılandırmak istiyorsanız **CA Sertifikası** ögesine gidin.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **İstemci Sertifikası** ögesini seçin.
2. **İstemci Sertifikası** içinde sertifikayı alın.

Zaten Sertifika Yetkilisi tarafından yayınlanmış bir sertifika aldıysanız, sertifikayı kopyalayabilir ve IPsec/IP Filtresi içinde kullanabilirsiniz. Kopyalamak için sertifikayı **Kopyalama Kaynağı** içinden seçin ve sonra **Kopyala** ögesine tıklayın.

İlgili Bilgi

- ➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)
- ➔ [“CA İmzalı Sertifika Yapılandırma” sayfa 97](#)
- ➔ [“CA Sertifikası Yapılandırma” sayfa 101](#)

Tarayıcıyı Bir IEEE802.1X Ağına Bağlama

IEEE 802.1X Ağı Yapılandırma

IEEE 802.1X'i tarayıcıya ayarladığınızda, RADIUS sunucusuna bağlı bir ağda, kimlik doğrulama işlevi olan bir LAN anahtarında veya bir erişim noktasında kullanabilirsiniz.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **IEEE802.1X** > **Temel** ögesini seçin.
2. Her öge için bir değer girin.
Bir Wi-Fi ağındaki tarayıcıyı kullanmak istiyorsanız, **Wi-Fi Kurulumu** ögesini tıklatın ve bir SSID seçin veya girin.
Not:
Ethernet ve Wi-Fi arasında ayarları paylaşabilirsiniz.
3. **İleri** ögesine tıklayın.
Bir doğrulama mesajı görüntülenir.
4. **Tamam** ögesine tıklayın.
Tarayıcı güncelleştirilmiştir.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35

IEEE 802.1X Ağı Ayarlama Öğeleri

Öğeler	Ayarlar ve Açıklama	
IEEE802.1X (Kablolu LAN)	IEEE802.1X için sayfanın ayarlarını etkinleştirebilir veya devre dışı bırakabilirsiniz (IEEE802.1X > Temel) (Kablolu LAN).	
IEEE802.1X (Wi-Fi)	IEEE802.1X (Wi-Fi) bağlantı durumu görüntülenir.	
Bağlantı Yöntemi	Geçerli ağın bağlantı yöntemi görüntülenir.	
EAP Türü	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.
	EAP-TTLS	
Kullanıcı Kimliği	Bir RADIUS sunucusunun kimlik doğrulaması için kullanmak üzere bir kimlik yapılandırın. 1 ila 128 arasında 1 baytlık ASCII (0x20 ila 0x7E) karakterler girin.	
Parola	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.	
Şifreyi Onayla	Yapılandığınız parolayı onay için girin.	
Sunucu Kimliği	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.	

Öğeler	Ayarlar ve Açıklama
Sertifika Doğrulama	Sertifika doğrulamasını kimlik doğrulama yöntemini dikkate almadan ayarlayabilirsiniz. Sertifikayı CA Sertifikası kısmında içe aktarın.
Adsız	PEAP-TLS veya PEAP/MSCHAPv2 (EAP Türü) 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.
Şifreleme Gücü	Aşağıdakilerden bir tanesini seçebilirsiniz.
	Yüksek AES256/3DES
	Orta AES256/3DES/AES128/RC4

IEEE 802.1X İçin Bir Sertifikayı Yapılandırma

IEEE802.1X için İstemci Sertifikasını yapılandırın. Ayarladığınızda, **EAP-TLS** ve **PEAP-TLS** öğelerini IEEE 802.1X'in bir kimlik doğrulama yöntemi olarak kullanabilirsiniz. Sertifika yetkilisi sertifikasını yapılandırmak istiyorsanız **CA Sertifikası** öğesine gidin.

1. Web Config'e erişin ve sonra **Ağ Güvenliği** sekmesi > **IEEE802.1X** > **İstemci Sertifikası** öğesini seçin.
2. **İstemci Sertifikası** içinde bir sertifika girin.
Zaten Sertifika Yetkilisi tarafından yayınlanmış bir sertifika aldıysanız, sertifikayı kopyalayabilir ve IEEE802.1X içinde kullanabilirsiniz. Kopyalamak için sertifikayı **Kopyalama Kaynağı** içinden seçin ve sonra **Kopyala** öğesine tıklayın.

İlgili Bilgi

➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)

Gelişmiş Güvenlik İçin Sorunları Çözme

Güvenlik Ayarlarını Geri Yükleme

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

Web Config Kullanılarak Güvenlik İşlevinin Devre Dışı Bırakılması

IPsec/IP Filtreleme öğesini Web Config öğesini kullanarak devre dışı bırakabilirsiniz.

1. Web Config'e erişin ve **Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** öğesini seçin.
2. **IPsec/IP Filtreleme** işlevini devre dışı bırakın.

Ağ Güvenlik Özellikleri Kullanımı Sorunları

Önceden Paylaşılmış Bir Anahtar Unutuldu

Önceden paylaşılan bir anahtarı yeniden yapılandırın.

Anahtarı değiştirmek için Web Config öğesine erişin ve **Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** > **Varsayılan İlke** veya **Grup İlkesi** öğesini seçin.

Önceden paylaşılan anahtarı değiştirirken bilgisayarlar için önceden paylaşılan anahtarı yapılandırın.

İlgili Bilgi

- ➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)
- ➔ [“IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim” sayfa 104](#)

IPsec İletişimi ile İletişim Kurulamıyor

Tarayıcının veya bilgisayarın desteklemediği algoritmayı belirtin.

Tarayıcı aşağıdaki algoritmaları destekler. Bilgisayarın ayarlarını kontrol edin.

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 Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
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 104](#)

İletişim Aniden Kesiliyor

Tarayıcının IP adresi değişti veya kullanılamıyor.

Grup İlkesi öğesinde yerel adrese kayıtlı IP adresi değiştiğinde veya kullanılamadığında, IPsec iletişimi gerçekleştirilemez. Tarayıcının kontrol panelini kullanarak IPsec'i devre dışı bırakın.

DHCP süresi dolduysa yeniden başlatın veya IPv6 adresi süresi geçmişse veya alınmamışsa tarayıcının Web Config (**Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** > **Grup İlkesi** > **Yerel Adres (Tarayıcı)**) ögesi için kayıtlı IP adresi bulunamayabilir.

Sabit bir IP adresi kullanın.

Bilgisayarın IP adresi değişti veya kullanılamıyor.

Grup İlkesi ögesinde uzak adrese kayıtlı IP adresi değiştiğinde veya kullanılamadığında, IPsec iletişimi gerçekleştirilemez.

Tarayıcının kontrol panelini kullanarak IPsec'i devre dışı bırakın.

DHCP süresi dolduysa yeniden başlatın veya IPv6 adresi süresi geçmişse veya alınmamışsa tarayıcının Web Config (**Ağ Güvenliği** sekmesi > **IPsec/IP Filtreleme** > **Temel** > **Grup İlkesi** > **Uzak Adres (Ana Bilgisayar)**) ögesi için kayıtlı IP adresi bulunamayabilir.

Sabit bir IP adresi kullanın.

İlgili Bilgi

- ➔ [“Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35](#)
- ➔ [“IPsec/IP Filtrelemeyi Kullanan Şifrelenmiş İletişim” sayfa 104](#)

IPsec/IP Filtreleme Yapılandırıldıktan Sonra Bağlanılamıyor

IPsec/IP Filtreleme ayarları yanlış.

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 104](#)

IEEE 802.1X Yapılandırmasından Sonra Tarayıcıya Erişilemiyor

IEEE 802.1X ayarları yanlış.

IEEE 802.1X ve Wi-Fi'yi tarayıcının kontrol panelinden devre dışı bırakın. Tarayıcı ve bilgisayarı bağlayın ve ardından, IEEE 802.1X ögesini yeniden yapılandırın.

Tarayıcı ve bilgisayarı bağlayın ve ardından, IEEE 802.1X ögesini yeniden yapılandırın.

İlgili Bilgi

- ➔ [“IEEE 802.1X Ağı Yapılandırma” sayfa 114](#)

Dijital Sertifika Kullanımı Sorunları

CA İmzalı Sertifika Alınamıyor

CSR'deki CA İmzalı Sertifika ve bilgisi eşleşmiyor.

CA İmzalı Sertifika ve CSR aynı bilgilere sahip değilse CSR alınamaz. 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 İmzalı Sertifika 5 KB'den fazla.

5 KB'den fazla bir CA İmzalı Sertifika ögesini alamazsınız.

Sertifikayı alma parolası yanlış.

Doğru parolayı girin. Şifreyi unuttuysanız sertifikayı içe aktaramazsınız. CA İmzalı Sertifika ögesini yeniden alın.

İlgili Bilgi

➔ [“CA İmzalı bir Sertifikanın İçe Aktarımı” sayfa 99](#)

Kendinden İmzalı bir Sertifika Güncellenmiyor

Ortak Ad girilmedi.

Ortak Ad girilmelidir.

Desteklenmeyen karakterler Ortak Ad içine girildi.

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

Ortak ad içinde bir virgöl veya boşluk var.

Ortak Ad virgöl içeriyorsa, o noktada ayrılır. Virgölün önünde ya da ardında sadece bir boşluk girilmişse hata oluşur.

İlgili Bilgi

➔ [“Kendinden İmzalı Sertifika Güncelleme” sayfa 101](#)

CSR Oluşturulamıyor

Ortak Ad girilmedi.

Ortak Ad girilmelidir.

Desteklenmeyen karakterler Ortak Ad, Kuruluş, Kuruluş Birimi, Bölge ve Eyalet/İl öğelerine girildi.

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

Ortak Ad virgül ya da boşluk içeriyor.

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

İlgili Bilgi

➔ [“CA İmzalı bir Sertifika Alınması” sayfa 97](#)

Görüntülenen bir Dijital Sertifikaya İlişkin Uyarı

Mesajlar	Neden/Çözüm
Bir Sunucu Sertifikası girin.	Neden: İçe aktarmak için bir dosya seçmediniz. Çözüm: Bir dosya seçin ve İçe Aktar ögesine tıklayın.
CA Sertifikası 1 girilmedi.	Neden: CA sertifikası 1 girilmedi ve sadece CA sertifikası 2 girildi. Çözüm: Önce CA sertifikası 1'i içe aktarın.
Aşağıdaki değer geçersiz.	Neden: Dosya yolu ve/veya şifrede desteklenmeyen karakterler mevcut. Çözüm: Öge için girilen karakterlerin doğru olduğundan emin olun.
Geçersiz tarih ve saat.	Neden: Tarayıcının tarih ve saat ayarları yapılmamış. Çözüm: Web Config ya da EpsonNet Config'i kullanarak tarih ve saati ayarlayın.
Geçersiz şifre.	Neden: CA sertifikası için ayarlanan şifre ile girilen şifre eşleşmiyor. Çözüm: Doğru şifreyi girin.

Mesajlar	Neden/Çözüm
Geçersiz dosya.	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.
Üçten fazla CA sertifikası içeren Sunucu Sertifikaları kullanılamaz.	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.
Sertifika süresi dolmuş. Sertifikanın geçerli olup olmadığını veya ürünündeki tarih ve saat ayarını kontrol edin.	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.
Özel anahtar gereklidir.	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.

Mesajlar	Neden/Çözüm
Kurulum başarısız oldu.	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 97](#)

Yanlışlıkla CA İmzalı bir Sertifikanın Silinmesi

CA imzalı sertifika için hiç yedek dosya yok.

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

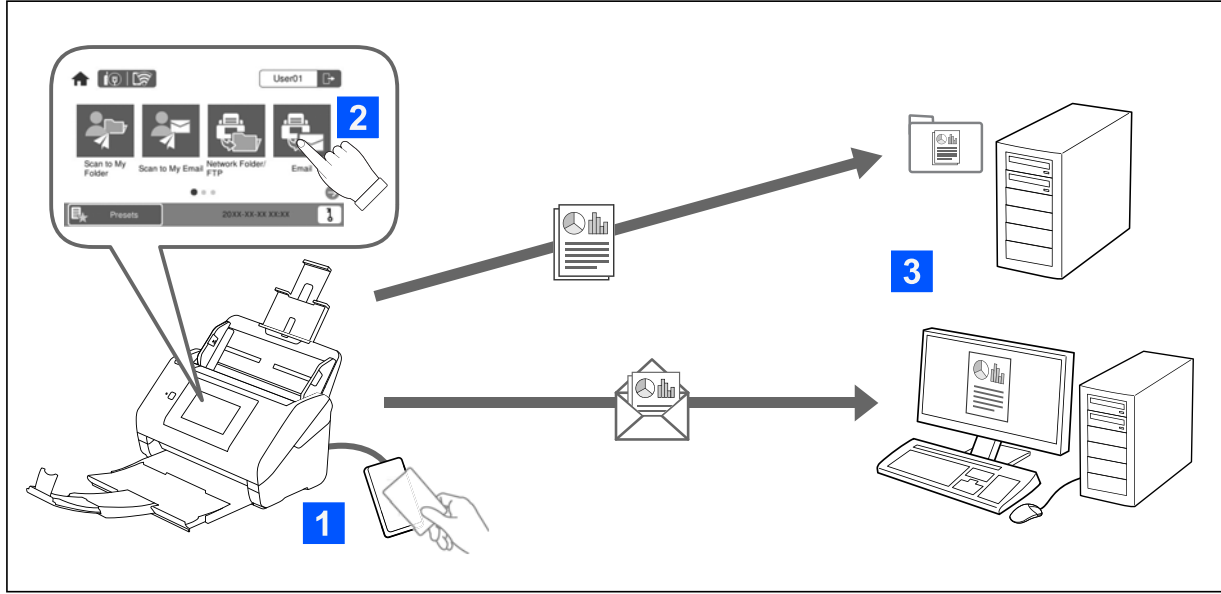
➔ [“CA İmzalı bir Sertifikanın İçe Aktarımı” sayfa 99](#)

➔ [“CA İmzalı bir Sertifika Silme” sayfa 100](#)

Kimlik Doğrulama Ayarları

Kimlik Doğrulama Ayarları Hakkında.	124
Doğrulama Yöntemi Hakkında.	125
Ayar İçin Yazılım.	127
Tarayıcının Bellenim Sürümünü Güncelleme.	127
Kimlik Doğrulama Aygıtını Bağlama ve Yapılandırma.	127
Bilgileri Kaydetme ve Ayarlama.	132
Epson Device Admin Kullanarak Job History Raporları.	148
Kontrol Panelinden Yönetici olarak Giriş Yapma.	148
Kimlik Doğrulama Ayarları ögesini devre dışı bırakma.	148
Kimlik Doğrulama Ayarları Bilgilerinin Silinmesi (Varsayılan Ayarları Geri Yükle).	149
Sorunları Çözme.	149

Kimlik Doğrulama Ayarları Hakkında



Kimlik Doğrulama Ayarları etkinleştirildiğinde, taramaya başlamak için kullanıcı kimlik doğrulaması gereklidir. Her kullanıcı tarafından kullanılabilen tarama yöntemlerini ayarlayabilirsiniz ve kazara çalışmaları önleyebilirsiniz.

Kimliği doğrulanmış kullanıcının e-posta adresini tarama hedefi olarak belirleyebilirsiniz (E-postama Tara) ya da her kullanıcının verilerini kişisel klasöre kaydedebilirsiniz (Klasörüne Tara). Ayrıca diğer tarama yöntemlerini de belirleyebilirsiniz.

Not:

- ❑ Kimlik Doğrulama Ayarları etkinleştirildiğinde, bir bilgisayardan veya akıllı cihazdan tarama yapamazsınız.
- ❑ Bu kılavuzda tanıtılan Kimlik Doğrulama Ayarları ögesine ek olarak, kimlik doğrulama sunucusunu kullanarak kimlik doğrulama sistemi de oluşturabilirsiniz. Bir sistem oluşturmak için Document Capture Pro Server Authentication Edition (kısa ad Document Capture Pro Server AE) ögesini kullanın. Daha fazla bilgi için yerel Epson satıcınıza başvurun.

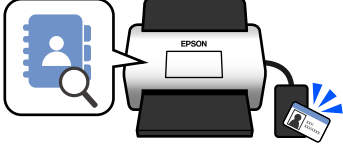
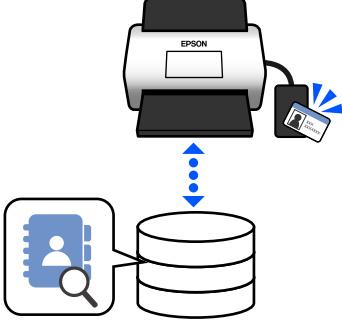
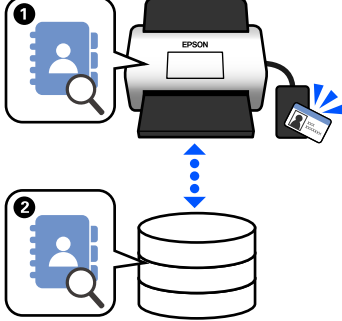
Kimlik Doğrulama Ayarları İçin Kullanılabilir İşlevler

Kontrol Panelindeki Tarama İşlevi	Kimlik Doğrulama Ayarları	
	Etkinleştirildiği nde	Devre dışı bırakıldığında
Klasörüne Tara Görüntüleri kimliği doğrulanmış kullanıcıya atanan klasöre kaydeder.	✓	-
E-postama Tara Görüntüleri kimliği doğrulanmış kullanıcının e-posta adresine gönderir.	✓	-
Ağ Klasörüne/FTP'ye Tara Görüntüleri ağda bir klasöre kaydeder.	✓	✓

Kontrol Panelindeki Tarama İşlevi	Kimlik Doğrulama Ayarları	
	Etkinleştirildiğinde	Devre dışı bırakıldığında
Bilgisayara Tara Document Capture Pro (Windows)/Document Capture (Mac OS) içinde oluşturulan işleri kullanarak görüntüleri bağlı bilgisayara kaydeder. * Kimlik Doğrulama Ayarları etkinleştirildiğinde, sadece Ön ayrlar içinde kayıtlı işleri kullanabilirsiniz.	✓*	✓
E-postya Tara Görüntüleri ayarladığınız e-posta adresine gönderir.	✓	✓
Buluta Tara Görüntüleri ayarladığınız bulut hizmetine gönderir.	✓	✓
USB Sürücü içine tara Görüntüleri tarayıcıya bağlı USB sürücüye kaydeder. Bu, yalnızca tarayıcıya hiçbir kimlik doğrulama aygıtı bağlı olmadığında kullanılabilir.	✓	✓
WSD kısmına tara Görüntüleri WSD özelliğini kullanarak bağlı bilgisayara kaydeder.	-	✓
Ön ayrlar En fazla 48 ön ayarlı tarayıcı işlevi kaydedebilirsiniz. En fazla beş Ön ayrlar ögesini Yerel DB içinde kayıtlı kullanıcılara tahsis edebilirsiniz. Tahsis edilen Ön ayrlar sadece o kullanıcı için mevcut olur. Herhangi bir kullanıcıya tahsis edilmemiş Ön ayrlar, tüm kullanıcılar tarafından kullanılabilir.	✓	✓

Doğrulama Yöntemi Hakkında

Bu tarayıcı, bir kimlik doğrulama sunucusu oluşturmaya gerek kalmadan, aşağıdaki yöntemleri kullanarak kimlik doğrulama sağlayabilir.

	Yerel DB	LDAP	Yerel DB ve LDAP
Kullanıcı bilgisi konumu	Tarayıcının belleği Bu kimlik doğrulama yöntemi, tarayıcıya kayıtlı kullanıcı bilgilerini kontrol eder ve bunları tarama işlevini kullanan kullanıcıyla karşılaştırır.	LDAP sunucusu* Bu kimlik doğrulama yöntemi, tarayıcıyla senkronize edilmiş LDAP sunucusunun kullanıcı bilgilerini kontrol eder. LDAP sunucusundan gelen en fazla 300 adet kullanıcı bilgisi tarayıcıda geçici olarak bir önbellek olarak saklanabileceğinden, LDAP sunucusu kapatılırsa kimlik doğrulama önbellek kullanılarak gerçekleştirilebilir. * LDAP ile iletişim kurabilen bir dizin servisi sağlayan bir sunucu.	Tarayıcının belleği ve LDAP sunucusu Önce tarayıcıda kayıtlı kullanıcı bilgilerini kontrol edin (1) ve bir eşleşme yoksa, kullanıcı bilgilerini LDAP sunucusundan kontrol edin (2).
			
Kayıtlı kullanıcı sayısı	50 (tarayıcının belleği)	Sınırsız (LDAP sunucusu)	50 (tarayıcının belleği) Sınırsız (LDAP sunucusu)
Tarayıcının bellek önbelleği	-	300	Maksimum 300 (Önbellek yuvalarının 50'si Yerel DB içindeki Kullanıcı Ayarları ile paylaşılır)
Giriş yapma yöntemleri	Aşağıdaki yöntemlerden birini kullanabilirsiniz. ☐ Kimlik doğrulama kartını tutun veya bir Kullanıcı Kimliği ve Parola girin ☐ Kimlik doğrulama kartını tutun veya bir Kimlik Numarası girin ☐ Bir Kullanıcı Kimliği ve Parola girin ☐ Bir Kullanıcı Kimliği girin ☐ Bir Kimlik Numarası girin		
"Şuraya tara:" özelliğinin sınırları	Her kullanıcı için tek tek ayarlayın	Tüm LDAP kullanıcıları için aynı ayarlar	Yerel DB kullanıcıları: tek tek ayarlayın LDAP kullanıcıları: tüm kullanıcılar için aynı ayarlar
Ön ayarlar öğelerinin kullanıcılar a tahsis edilmesi	Her kullanıcı için en fazla 5	- (Tek tek ayarlanamaz)	Yerel DB kullanıcıları: her kullanıcı için en fazla 5 LDAP kullanıcıları: -

Ayar İçin Yazılım

Web Config veya Epson Device Admin kullanarak Ayar.

- ❑ Web Config ögesini kullanırken, tarayıcıyı yalnızca bir web tarayıcı kullanarak ayarlayabilirsiniz.
“Web Config” sayfa 35
- ❑ Epson Device Admin ögesini kullanırken, tek seferde birden fazla tarayıcıyı yalnızca yapılandırma şablonu kullanarak ayarlayabilirsiniz.
“Epson Device Admin” sayfa 36

Tarayıcının Bellenim Sürümünü Güncelleme

Kimlik Doğrulama Ayarları ögesini etkinleştirmeden önce, tarayıcının bellenim sürümünü en yeni sürüme güncelleyin. Tarayıcıyı önceden İnternete bağlayın.



Önemli:

Güncelleme yapılırken bilgisayarı ya da tarayıcıyı kapatmayın.

Web Config ögesinden ayarlarken:

Aygıt Yönetimi sekmesi > **Firmware Güncellemesi** ögesini seçin ve sonra bellenim sürümünü güncellemek için ekrandaki talimatları uygulayın.

Epson Device Admin ögesinden ayarlarken:

Aygıt listesi ekranından **Home** > **Firmware** > **Update** ögesini seçin ve sonra bellenim sürümünü güncellemek için ekrandaki talimatları uygulayın.

Not:

En yeni bellenim sürümü zaten yüklenmişse, güncellemeniz gerekmez.

Kimlik Doğrulama Aygıtını Bağlama ve Yapılandırma

IC kart okuyucu gibi bir kimlik doğrulama aygıtı bağlamak ve kullanmak isterseniz, önce aygıtı yapılandırmanız gerekir. Bir kimlik doğrulama aygıtı kullanmıyorsanız, bu gerekli değildir.

İlgili Bilgi

- ➔ “Kimlik Doğrulama Aygıtını Bağlama” sayfa 130
- ➔ “Kimlik Doğrulama Aygıtı Ayarları” sayfa 131

Kart Okuyucu Uyumluluk Listesi

Bu liste, listedeki kart okuyucuların çalışmasını garanti etmez.

Evet: desteklenir (Kimlik bilgileri, standart kart okuyucu ayarları ile okunabilir.)

Hayır: uyumlu değil

Üretici	Model	Model Nu- mara- sı	Kimlik doğrulama kartı							Mod
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14 443 (Type B) Comp- liance	
			iClass	EM40 02	Clas- sic	Ultra- light	Stan- dard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80 081AK U	Evet	Evet*1	Evet*1	Evet*1	Hayır	Hayır	Hayır	Klavye
RF IDEAS	pcProx	RDR-70 81BKU	Evet*1	Hayır	Evet	Evet	Hayır	Hayır	Hayır	Klavye
RF IDEAS	pcProx	RDR-75 81AKU	Evet	Hayır	Evet*1	Evet*1	Hayır	Hayır	Hayır	Klavye
ELATEC	TWN3 MIFARE	T3DT-MB2BE L	Hayır	Hayır	Evet	Evet	Hayır	Hayır	Hayır	Klavye
		T3DT-MB2WE L								
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WE L	Evet	Hayır	Evet	Evet	Evet	Evet	Evet	Klavye
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WE L-PI	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
ELATEC	TWN4 Slim	T4QC-FC3B7	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
HID Global	OMNI-KEY 5427	OMNI-KEY542 7CK OMNI-KEY542 7CK gen2	Evet	Evet	Evet	Evet	Evet	Hayır	Evet	Klav- ye*1
ACS	ACR122 U	ACR122 U	Hayır	Hayır	Evet*2	Evet*2	Evet	Hayır	Evet*2	PC/SC

Üretici	Model	Model Nu- mara- sı	Kimlik doğrulama kartı							Mod
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14 443 (Type B) Comp- liance	
			iClass	EM40 02	Clas- sic	Ultra- light	Stan- dard	Lite/ Lite-S		
ACS	ACR125 2	ACR125 2	Hayır	Hayır	Evet*2	Evet*2	Evet	Evet	Evet*2	PC/SC
Sony	PaSoRi	RC- S330/S	Hayır	Hayır	Evet*2	Evet*2	Evet*2	Evet*2	Evet*2	PaSoRi
Sony	PaSoRi	RC- S380/P RC- S380/S	Hayır	Hayır	Evet*2	Evet*2	Evet*2	Evet*2	Evet*2	PaSoRi
DMZ	Leitor RFID Univer- sal	DMZ00 8	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
DMZ	Leitor RFID Mul- ti-125	DMZ08 7	Hayır	Evet	Hayır	Hayır	Hayır	Hayır	Hayır	Klavye
DMZ	Leitor RFID Mifare	DMZ08 8	Hayır	Hayır	Evet	Evet	Hayır	Hayır	Hayır	Klavye
DMZ	Biome- tric & RFID Reader	DMZ07 3	Hayır	Evet	Hayır	Hayır	Hayır	Hayır	Hayır	Klavye
inepro	SCR708	SCR708	Evet*1	Evet*1	Evet*1	Evet*1	Evet*1	Evet*1	Evet*1	Klavye
Y Soft	YU0308 8 001	MU038 8	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
Carta- dis	TCM3 Carta- dis MiFare Card Reader	ZTCM3- MIFARE	Hayır	Hayır	Evet	Evet	Hayır	Hayır	Evet	Klavye
MICI Net- work Co., Ltd.	EM & Mifare Card Reader	mCR-6 00	Hayır	Hayır	Evet	Evet	Hayır	Hayır	Evet	Klavye

Üretici	Model	Model Nu- mara- sı	Kimlik doğrulama kartı							Mod
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14 443 (Type B) Comp- liance	
			iClass	EM40 02	Clas- sic	Ultra- light	Stan- dard	Lite/ Lite-S		
NT-wa- re	MiCard Multi- Tech4- PI	T4DT- FB4WU F-PI	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Klavye
NT-wa- re	MiCard Plus-2- V2	RDR-80 081AG U- NT2-20	Evet*1	Evet*1	Evet*1	Evet*1	Hayır	Hayır	Hayır	Klavye
NT-wa- re	MiCard V3 Mul- ti	MiCard V3 Mul- ti	Evet	Evet	Evet	Evet	Evet	Evet	Hayır	Klavye

*1 Kart okuyucu üreticisi tarafından tedarik edilen özel yazılımı kullanarak, kart okuyucunun ayarlarını değiştirmeniz gerekir.

*2 Ürün ayarlarını yapılandırarak kimlik doğrulama kimliği olarak kartın standart kimliğinden farklı olarak kartın belirli bir alanındaki verileri kullanmanız gerekiyorsa, ürünü ayarlamanın bir yolu hakkında daha fazla bilgi için lütfen Epson ortağınızla veya yerel temsilcinizle iletişim kurun.

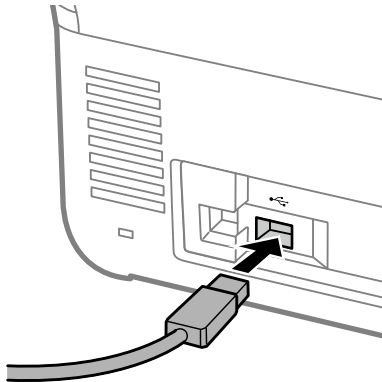
Kimlik Doğrulama Aygıtını Bağlama



Önemli:

Kimlik doğrulama aygıtını birden fazla tarayıcıya bağladığınızda, aynı model numarasına sahip bir ürün kullanın.

Kart okuyucunun USB kablосunu, tarayıcı üzerindeki harici arayüz USB bağlantı noktasına bağlayın.



Kimlik Doğrulama Aygıtı İçin Çalıştırma Kontrolü

Kimlik doğrulama aygıtının bağlantı durumunu ve kimlik doğrulama kartının tanınmasını, tarayıcının kontrol panelinden kontrol edebilirsiniz.

Ayarlar > Aygıt Bilgileri > Kimlik Doğrulama Aygıtı Durumu ögesini seçerseniz bilgi görüntülenir.

Kimlik Doğrulama Aygıtı Ayarları

Bir kimlik doğrulama kartından alınan kimlik doğrulama bilgileri için okuma biçimini ayarlayın.

Kimlik doğrulama aygıtı için aşağıdaki okuma yöntemini ayarlayabilirsiniz.

- ☐ Kimlik doğrulama kartının çalışan numarası veya kişisel kimlik gibi belirli alanlarını okuyun.
- ☐ UID hariç kimlik doğrulama kartı bilgilerini kullanın (seri numarası gibi kimlik doğrulama kartı bilgileri.)
Operasyonel parametreleri oluşturmak için bir araç kullanabilirsiniz. Ayrıntılar için bayinize başvurun.

Not:

Farklı üreticilerin kimlik doğrulama kartlarını kullanma:

UID kart bilgisi kullanırken (seri numarası gibi kart kimliği bilgileri), farklı türde kimlik doğrulama kartlarının karışımını kullanabilirsiniz. Diğer kart bilgileri kullanılırken bu karıştırılamaz.

Web Config ögesinden ayarlarken:

Aygıt Yönetimi sekmesi > **Kart Okuyucu** ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonundan **Administrator Settings > Authentication Settings > Card Reader** ögesini seçin.

Öge	Açıklama
Vendor ID	4 alfasayısal karakter kullanarak kimlik doğrulama aygıtının 0000 ile FFFF arası kullanıma sınırlanan satıcı kimliğini ayarlayın. Sınırlamak istemiyorsanız 0000 olarak ayarlayın.
Product ID	4 alfasayısal karakter kullanarak kimlik doğrulama aygıtının 0000 ile FFFF arası kullanıma sınırlanan ürün kimliğini ayarlayın. Sınırlamak istemiyorsanız 0000 olarak ayarlayın.
Çalışma parametresi	Kimlik doğrulama aygıtının çalışma parametresini 0 ile 8192 arası karaktere ayarlayın. A-Z, a-z, 0-9, +, /, =, boşluk ve satır besleme kullanılabilir.
Kart Okuyucu	Kimlik doğrulama aygıtının dönüştürme biçimini seçin. Biçim ayrıntılarını kontrol edebilirsiniz. Öge açıklamasında verilen bağlantıya bakın.
Kimlik Doğrulama Kartı Kimliği kayıt biçimi	Kimlik kartının kimlik doğrulama bilgileri için dönüştürme biçimini seçin. Biçim ayrıntılarını kontrol edebilirsiniz. Öge açıklamasında verilen bağlantıya bakın.
Kart Kimliği aralığını ayarla	Okuma konumunun özelliklerini etkinleştirin.
Metin Başlangıç Konumu	Kimlik bilgilerini okumak için metin başlangıç konumunu belirtin. 1 ve 4096 arası belirtebilirsiniz.
Karakter Sayısı	Kimlik bilgilerinin başlangıç konumundan okunacak karakter sayısını belirtin. 1 ve 4096 arası belirtebilirsiniz.

Bilgileri Kaydetme ve Ayarlama

Ayarlama

Kullandığınız Doğrulama Yöntemi ve tarama yöntemine bağlı olarak gerekli ayarları yapın.



Önemli:

Kurulumu başlatmadan önce, tarayıcının zaman ayarının doğru olduğunu kontrol edin.

Zaman ayarı yanlışsa, tarayıcı ayarlama arızasına neden olabilen “Lisans süresi doldu” hata mesajı görüntülenir. Ayrıca, SSL/TLS iletişimi veya IPsec gibi güvenlik işlevini kullanabilmek için doğru zaman ayarlanmalıdır. Aşağıdaki gibi zamanı ayarlayabilirsiniz.

- ☐ Web Config: **Aygıt Yönetimi** sekmesi > **Tarih ve Saat** > **Tarih ve Saat**.
- ☐ Tarayıcının kontrol paneli: **Ayarlar** > **Temel Ayarlar** > **Tarih/Saat Ayarları**.

Ayarlar	Yerel DB	LDAP	Yerel DB ve LDAP
Kimlik doğrulamanın etkinleştirilmesi Kimlik doğrulama ayarları yapmadan önce, kimlik doğrulamayı etkinleştirmeniz gerekir. “Kimlik Doğrulamanın Etkinleştirilmesi” sayfa 133	✓	✓	✓
Kimlik Doğrulama Ayarları Doğrulama Yöntemi ögesinin ayarlanması ve kullanıcı kimliğinin doğrulanması. “Kimlik Doğrulama Ayarları” sayfa 133	✓	✓	✓
Kullnc Ayrları Ögelerinin Kaydedilmesi Her kullanıcı için ayarları kaydedin. Kullanıcıları bir CSV dosyası kullanarak toplu olarak kaydedebilirsiniz. “Kullnc Ayrları Ögelerinin Kaydedilmesi” sayfa 135	✓	–	✓
LDAP Sunucusu ile senkronize etme LDAP sunucusu senkronize ayarlarını yapın. “LDAP Sunucusu ile Senkronize Etme” sayfa 141	–	✓	✓
E-posta Snscu Ögesini Ayarlama E-posta sunucusu ayarlarını yapın. Bu ayarı, E-postama Tara gibi e-posta sunucusu ayarları gerektiren işlevleri kullandığınızda yapın. “E-posta Sunucusunu Ayarlama” sayfa 145	✓	✓	✓
Klasörüne Tara Ayarlama Hedef klasörleri ayarlayın. Bu ayarı, Klasörüne Tara işlevini kullandığınızda yapın. “Klasörüne Tara Ayarlama” sayfa 146	✓	✓	✓

Ayarlar	Yerel DB	LDAP	Yerel DB ve LDAP
Tek Dokunma İşlevlerini Özelleştirin Bu ayarı, tarayıcının kontrol panelinde görüntülenen öğeleri değiştirdiğinizde yapın. Kontrol panelinde sadece size gereken simgeleri görüntüleyebilirsiniz veya simgelerin sırasını değiştirebilirsiniz. “Tek Dokunma İşlevlerini Özelleştirin” sayfa 147	✓	✓	✓

Kimlik Doğrulamanın Etkinleştirilmesi

Kimlik doğrulama ayarları yapmadan önce, kimlik doğrulamayı etkinleştirmeniz gerekir.

Web Config ögesinden ayarlarken:

Ürün Güvenliği sekmesi > **Temel** > **Kimlik Doğrulama** ögesinden **Açık (Cihaz/LDAP sunucusu)** ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonunda **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication** ögesinden **Açık (Cihaz/LDAP sunucusu)** ögesini seçin.

Not:

Tarayıcıdaki Kimlik Doğrulama Ayarları ögesini etkinleştirirseniz, kontrol paneli için Kilit Ayarları ögesi de etkinleştirilir. Kontrol panelinin kilidi, Kimlik Doğrulama Ayarları etkinleştirildiğinde açılmaz.

Kimlik Doğrulama Ayarları ögesini devre dışı bırakırsanız, Kilit Ayarları ögesi etkin kalır. Devre dışı bırakmak isterseniz, ayarları kontrol panelinden ya da Web Config ögesinden yapabilirsiniz.

İlgili Bilgi

- ➔ [“Kontrol Panelinden Kilit Ayarları Ögesini Ayarlama” sayfa 85](#)
- ➔ [“Kilit Ayarları Ögesini Web Config Ögesinden Ayarlama” sayfa 85](#)

Kimlik Doğrulama Ayarları

Doğrulama Yöntemi ögesinin ayarlanması ve kullanıcı kimliğinin doğrulanması.

Web Config ögesinden ayarlarken:

Ürün Güvenliği sekmesi > **Kimlik Doğrulama Ayarları** ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonundan **Administrator Settings** > **Authentication Settings** > **Authentication Settings** ögesini seçin.

Öge	Açıklama
Doğrulama Yöntemi	Doğrulama Yöntemi ögesini seçin. ☐ Yerel DB Tarayıcıda kayıtlı Kullnc Ayrıları kullanarak kimlik doğrulayın. Kullanıcıyı tarayıcıya kaydetmek gerekir. ☐ LDAP Tarayıcıyla senkronize edilmiş LDAP sunucusundaki kullanıcı bilgilerini kullanarak kimliği doğrulayın. LDAP sunucusu ayarlarını önceden yapılandırmanız gerekir. ☐ Yerel DB ve LDAP Tarayıcıya veya tarayıcıyla senkronize edilmiş LDAP sunucusuna kayıtlı kullanıcı bilgilerini kullanarak kimliği doğrulayın. Kullanıcıyı tarayıcıya kaydetmeniz ve LDAP sunucusunu ayarlamanız gerekir.
Kullanıcının Kimliğini Doğrulama Yöntemi	Kullanıcının kimliğinin nasıl doğrulanacağını seçin. ☐ Kart veya Kullanıcı kimliği ve parola Kullanıcıların kimliğini doğrulamak için bir kimlik doğrulama kartı kullanın. Kimlik doğrulamak için bir kullanıcı kimliği ve parola da kullanabilirsiniz. ☐ Kullanıcı kimliği ve parola Kullanıcıların kimliklerini doğrulamak için bir kullanıcı kimliği ve parola kullanın. Bu işlevi seçerken kimlik doğrulamak için bir kimlik doğrulama kartı kullanamazsınız. ☐ Kullanıcı Kimliği Kullanıcıların kimliklerini doğrulamak için yalnızca bir kullanıcı kimliği kullanın. Bir parola ayarlamanız gerekmez. ☐ Kart veya Kimlik Numarası Kullanıcıların kimliğini doğrulamak için bir kimlik doğrulama kartı kullanın. Bir Kimlik Numarası da kullanabilirsiniz. ☐ Kimlik Numarası Kullanıcıların kimliklerini doğrulamak için yalnızca bir Kimlik Numarası kullanın.
Kullanıcıların, kimlik doğrulama kartlarının kaydını yapmasına izin ver	Kullanıcıların kimlik doğrulama kartını sisteme kaydetmesine izin veriyorsanız bunu etkinleştirin. Doğrulama Yöntemi için LDAP ögesini seçerseniz bunu ayarlayamazsınız. Kullanıcıların kendi kimlik doğrulama kartlarıyla nasıl kimlik doğrulayacağı hakkında daha fazla bilgi için <i>Kullanım Kılavuzu</i> içindeki “Kimlik Doğrulama Kartının Kaydedilmesi” bölümüne bakın.
Kimlik Numarasının En Az Basamak Sayısı	Kimlik numarası için minimum basamak sayısını seçin.
LDAP kimliği doğrulanmış kullanıcılar için önbellekleme	LDAP sunucusu kimlik doğrulamasını kullanırken, kullanıcı bilgilerini önbelleğe almayı kullanıp kullanmayacağınızı ayarlayabilirsiniz.
SMTP kimlik doğrulamasındaki kullanıcı bilgilerini kullanın	Kimlik doğrulaması için bir kullanıcı kimliği ve parola kullanırken, SMTP kimlik doğrulaması için kullanıcı bilgilerinin kullanılıp kullanılmayacağını ayarlayabilirsiniz. Sistem, giriş yapmış olan son kullanıcı kimliğini ve parolayı kullanır.
LDAP kimliği doğrulanmış kullanıcılar için kısıtlamalar	LDAP kullanıyorsanız, kullanıcı için mevcut olan işlevleri ayarlayabilirsiniz.

Kullnc Ayrları Öğelerinin Kaydedilmesi

Kullanıcı kimlik doğrulaması için kullanılan Kullnc Ayrları öğesini kaydedin. Aşağıdaki yöntemlerden birini kullanarak kaydedebilirsiniz.

- ☐ Kullnc Ayrları Öğesini Birer Birer Kaydetme (Web Config)
- ☐ Bir CSV dosyası kullanarak Toplu İş olarak Birden Fazla Kullnc Ayrları Kaydetme (Web Config)
- ☐ Bir Yapılandırma Şablonu kullanarak Toplu İş olarak User Settings Öğesini Birden Fazla Tarayıcıya Kaydetme (Epson Device Admin)

İlgili Bilgi

- ➔ [“Kullnc Ayrları Seçeneğini Tek Tek Kaydetme \(Web Config\)” sayfa 135](#)
- ➔ [“Bir CSV dosyası kullanarak Birden Fazla Kullnc Ayrları Kaydetme \(Web Config\)” sayfa 136](#)
- ➔ [“User Settings öğesini Toplu İş Olarak Birden Fazla Tarayıcıya Kaydetme \(Epson Device Admin\)” sayfa 139](#)

Kullnc Ayrları Seçeneğini Tek Tek Kaydetme (Web Config)

Web Config öğesine erişin ve **Ürün Güvenliği** sekmesi > **Kullnc Ayrları** > **Ekle** öğesini seçin ve sonra Kullnc Ayrları öğesini girin.

Öge	Açıklama
Kullanıcı Kimliği	Kimlik doğrulama için kullanmak istediğiniz kullanıcı kimliğini Unicode (UTF-8) olarak ifade edilebilen 1 ila 83 bayt aralığında girin. Kullanıcı kimliği büyük/küçük harf duyarlı olmadığından, büyük veya küçük harf kullanarak giriş yapabilirsiniz.
Kullanıcı Adı Görüntüleme	En fazla 32 karakter Unicode (UTF-16) olarak ifade edilebilen tarayıcının kontrol panelinde görüntülenen kullanıcı adını girin. Bunu boş bırakabilirsiniz.
Parola	En fazla ASCII 32 karakter olarak kimlik doğrulama için kullanmak istediğiniz parolayı girin. Parola küçük/büyük harf duyarlıdır. Kullanıcının Kimliğini Doğrulama Yöntemi için Kullanıcı Kimliği öğesini seçerseniz bunu boş bırakın.
Kimlik Doğrulama Kartı Kimliği	En fazla ASCII 116 karakter olarak kimlik doğrulama kartı kimliğini girin. Bunu boş bırakabilirsiniz. Kimlik Doğrulama Ayarları için Kullanıcıların, kimlik doğrulama kartlarının kaydını yapmasına izin ver öğesine izin verdiğinizde kullanıcının yansıttığı sonuç yansıtılır.
Kimlik Numarası	Bu öğe Kart veya Kimlik Numarası veya Kimlik Numarası Kimlik Doğrulama Ayarları > Kullanıcının Kimliğini Doğrulama Yöntemi içinde seçildiğinde görüntülenir. Kimlik Doğrulama Ayarları > Kimlik Numarasının En Az Basamak Sayısı öğesinde ayarlanan sayı arasında bir yerde olan ve en fazla 8 basamaklı olan bir sayı girin.
Otomatik Oluştur	Bu öğe Kart veya Kimlik Numarası veya Kimlik Numarası Kimlik Doğrulama Ayarları > Kullanıcının Kimliğini Doğrulama Yöntemi içinde seçildiğinde görüntülenir. Kimlik Numarasının En Az Basamak Sayısı öğesinde seçtiğiniz aynı sayıda basamağa sahip bir kimlik numarasını otomatik olarak oluşturmak için tıklayın.

Öge	Açıklama
Bölüm	En fazla 40 karakter Unicode (UTF-16) olarak ifade edilebilen kullanıcıyı tanımlayan departman adını vb girin. Bunu boş bırakabilirsiniz.
Eposta Adresi	En fazla ASCII 200 karakter olarak kullanıcı e-posta adresini girin. Bu, E-postama Tara için hedef olarak kullanılır. Bunu boş bırakabilirsiniz.
Klasörüne Tara	Klasörüne Tara > Ayar Türü içinde Bireysel ögesini seçtiğinizde, kaydetme hedeflerini tek tek ayarlayın. Ayar öğeleri konusunda daha fazla bilgi için aşağıdaki kısma bakın. "Klasörüne Tara Ayarlama" sayfa 146
Kısıtlamalar	Her bir kullanıcı için işlevleri kısıtlayabilirsiniz. Kullanmak istediğiniz işlevi seçin.
Ön ayrlar	Tarayıcıda kayıtlı Ön ayrlar ögesinden yalnızca seçili kullanıcı için mevcut olan en fazla beş ön ayar oluşturabilirsiniz. ☐ Bir kullanıcıya tahsis edilmiş Ön ayrlar, sadece o kullanıcı tarafından kullanılabilir. Herhangi bir kullanıcıya tahsis edilmemiş Ön ayrlar, tüm kullanıcılar tarafından kullanılabilir. ☐ Bir kullanıcı sadece bir kullanılabilir Ön ayrlar ögesine sahipse, bu ön ayar kimlik doğrulama sonrasında otomatik olarak yüklenir. Birden fazla Ön ayrlar kullanılabilir durumdaysa, Ön ayrlar ögesinin bir listesi kimlik doğrulama sonrasında görüntülenir. ☐ Kısıtlamalar içinde kısıtlanmış işlevleri kullanan Ön ayrlar öğelerini oluşturamaz veya görüntüleyemezsiniz.

Bir CSV dosyası kullanarak Birden Fazla Kullnc Ayrarı Kaydetme (Web Config)

Her kullanıcı için ayarları bir CSV dosyasına girin ve bunları toplu iş olarak kaydedin.

Bir CSV Dosyası Oluşturma

Kullnc Ayrarı ögesini almak için bir CSV dosyası oluşturun.

Not:

Bir veya daha fazla Kullnc Ayrarı ögesini önceden kaydederseniz ve ardından biçimlendirilmiş bir dosyayı (CSV dosyası) vererseniz, ayar öğelerini girmek için kayıtlı ayarı referans olarak kullanabilirsiniz.

1. Web Config'e erişin ve **Ürün Güvenliği** sekmesi > **Kullnc Ayrarı** ögesini seçin.
2. **Dışa Aktar** ögesine tıklayın.
3. **Dosya Biçimi** için dosya biçimini seçin.
Aşağıya bakarak seçin.

Öge	Açıklama
CSV UTF-16 (Sekmeyle ayrılmış)	Microsoft Excel kullanarak dosyayı ne zaman düzenleyeceğinizi seçin. Her parametre “[]” (köşeli parantez) içinde yer alır. Parametreleri “[]” içinde girin. Dosyayı güncellediğinizde dosyanın üzerine yazmanızı öneririz. Dosyayı yeni kaydettiyseniz, dosya biçimi için Unicode metin (*.txt) ögesini seçin.
CSV UTF-8 (Virgülle ayrılmış)	Microsoft Excel olmadan bir metin düzenleyici veya makro kullanarak dosyayı ne zaman düzenleyeceğinizi seçin.
CSV UTF-8 (Noktalı virgülle ayrılmış)	

4. **Dışa Aktar** ögesine tıklayın.
5. Microsoft Excel gibi elektronik tablo uygulamasında veya bir metin düzenleyicide bu CSV dosyasını düzenleyin ve kaydedin.

**Önemli:**

Dosyayı düzenlerken, kodlama ve başlık bilgilerini değiştirmeyin.

CSV Dosyası Ayar Öğeleri

Öge	Ayarlar ve Açıklama
UserID	Unicode 1 ve 83 bayt arası kimlik doğrulama için kullanılacak kullanıcı kimliğini girin.
UserName	En fazla Unicode 32 karakter olarak tarayıcının kontrol panelinde görüntülenen kullanıcı adını girin. Bunu boş bırakabilirsiniz.
Password	En fazla ASCII 32 karakter olarak kimlik doğrulama için kullanılacak parolayı girin. İçerik aktarırken, bu EncPassword yerine parola olarak ayarlanır. Kullanıcının Kimliğini Doğrulama Yöntemi için Kullanıcı Kimliği ögesini seçerseniz bunu boş bırakın. Dışa aktarılırken, bu her zaman boştur.
AuthenticationCardID	Kimlik doğrulama kartının okuma sonucunu ayarlayın. Kimlik Doğrulama Ayarları içinde Kullanıcıların, kimlik doğrulama kartlarının kaydını yapmasına izin ver ögesine izin verdiğinizde kullanıcının yansıttığı sonuç yansıtılır. En fazla ASCII 116 karakter girin. Bunu boş bırakabilirsiniz.
IDNumber	Bu öge Kart veya Kimlik Numarası veya Kimlik Numarası Kimlik Doğrulama Ayarları > Kullanıcının Kimliğini Doğrulama Yöntemi içinde seçildiğinde görüntülenir. Kimlik Doğrulama Ayarları > Kimlik Numarasının En Az Basamak Sayısı ögesinde ayarlanan sayı arasında bir yerde olan ve en fazla 8 basamaklı olan bir sayı girin. Bir Kimlik Numarası yinelenemez. Yinelenirse dosya alırken hata olduğunda uyarılacaksınız. Boş bırakıldığında, otomatik olarak bir numara atanır.
Department	Kullanıcıları ayırt etmek için isterseniz bölüm adını girin. En fazla Unicode 40 karakter girin. Bunu boş bırakabilirsiniz.

Öge	Ayarlar ve Açıklama
MailAddress	Kullanıcılar için e-posta adresini ayarlayın. Bu, E-postama Tara için hedef olarak kullanılır. A-Z, a-z, 0-9, !#%&'+-./=:?^_{ }~@ kullanabilirsiniz. 200 karakter veya daha az girin. İlk karakter için "," (virgül) kullanamazsınız. Bunu boş bırakabilirsiniz.
FolderProtocol	Klasörüne Tara işlevi türünü belirleyin. Ağ Klasörü/FTP (SMB): 0, FTP: 1
FolderPath	Klasörüne Tara işlevi için kayıt hedefini seçin.
FolderUserName	Klasörüne Tara için kullanıcı adını seçin.
FolderPassword	Klasörüne Tara işlevi için hedef klasörün kimliğini doğrulamak üzere 32 ASCII karakter içeren bir şifre belirleyin. İçe aktarırken, bu EncPassword yerine parola olarak ayarlanır. Dışa aktarılırken, bu her zaman boştur.
FtpPassive	Klasörüne Tara işlevi için Tür olarak FTP seçildiğinde, FTP sunucusu bağlantı modunu seçin. Aktif mod: 0, Pasif mod: 1
FtpPort	Klasörüne Tara işlevi için Tür olarak FTP seçildiğinde, taranan verileri FTP sunucusuna gönderirken kullanılan bağlantı noktası numarasını 0 ile 65535 arasında ayarlayın.
ScanToMemory	USB Sürücü içine tara için kısıtlamaları ayarlayın. İzin Verilmez: 0, İzin Verilir: 1
ScanToMail	E-postaya Tara için kısıtlamaları ayarlayın. E-postama Tara ögesini, sadece E-postaya Tara ögesi etkinleştirildiğinde ayarlayabilirsiniz. İzin Verilmez: 0, İzin Verilir: 1
ScanToFolder	Ağ Klasörüne/FTP Sunucusuna Tara için kısıtlamaları ayarlayın. Klasörüne Tara ögesini, sadece Ağ Klasörüne/FTP Sunucusuna Tara ögesi etkinleştirildiğinde ayarlayabilirsiniz. İzin Verilmez: 0, İzin Verilir: 1
ScanToCloud	Buluta Tara için kısıtlamaları ayarlayın. İzin Verilmez: 0, İzin Verilir: 1
ScanToComputer	Bilgisayara Tara için kısıtlamaları ayarlayın. İzin Verilmez: 0, İzin Verilir: 1
PresetIndex	Kullanıcı ile ilişkilendirmek istediğiniz Ön ayrlar ayarlayın. Virgülle ayrılmış en fazla beş Ön ayrlar kayıt numarası belirleyebilirsiniz.
EncPassword	Kullanıcı ayarlarını verirken, Password için parametre seti şifrelenir, sonra değer BASE64 ve çıkış ile kodlanır. Password için yeni parolayla alırken bu değer yok sayılır. Password ögesi boş ise bu değer kullanılır ve parola vermeden önce olduğu gibi kalır.

Öge	Ayarlar ve Açıklama
EncFolderPassword	Verirken, FolderPassword parametre seti şifrelenir, sonra değer BASE64 ve çıkış ile kodlanır. FolderPassword için yeni parolayla alırken bu değer yok sayılır. FolderPassword ögesi boş ise bu değer kullanılır ve parola vermeden önce olduğu gibi kalır.

Bir CSV Dosyasını Alma

1. Web Config'e erişin ve **Ürün Güvenliği** sekmesi > **Kullnc Ayrıları** ögesini seçin.
2. **İçe Aktar** ögesine tıklayın.
3. Almak istediğiniz dosyayı seçin.
4. **İçe Aktar** ögesine tıklayın.
5. Görüntülenen bilgileri kontrol ettikten sonra, **Tamam** ögesine tıklayın.

User Settings ögesini Toplu İş Olarak Birden Fazla Tarayıcıya Kaydetme (Epson Device Admin)

Yerel DB içinde kullanılan User Settings ögesini, LDAP sunucusu veya CSV/ENE dosyası kullanarak kaydedebilirsiniz.

Not:

ENE dosyası, Epson tarafından sağlanan kişisel bilgiler ve Kullnc Ayrıları gibi **Contacts** için kullanıcı bilgilerini şifreleyen ve kaydeden ikili dosyadır. Epson Device Admin içinden verilebilir ve bir parola ayarlayabilirsiniz. Kullnc Ayrıları ögesini yedek dosyadan almak istediğinizde kullanışlıdır.

CSV/ENE Dosyasından Alma

1. Yapılandırma şablonundan **Administrator Settings** > **Authentication Settings** > **User Settings** ögesini seçin.
2. **Import** ögesine tıklayın.
3. **CSV or ENE File** ögesini **Import Source** içinden seçin.
4. **Browse** ögesine tıklayın.
Dosya seçim ekranı görüntülenir.
5. Açmak için almak istediğiniz dosyayı seçin.
6. Bir alma yöntemi seçin.
 - ☐ Overwrite and Add: aynı kullanıcı kimliği mevcutsa üzerine yazar; mevcut değilse yeni kimlik ekler.
 - ☐ Replace All: almak istediğiniz kullanıcı ayarlarıyla her şeyi değiştirir.

7. **Import** öğesine tıklayın.
Ayar onayı ekranı görüntülenir.

8. **OK** öğesine tıklayın.
Doğrulama sonucu görüntülenir.

Not:

- ☐ Alınan kullanıcı ayarlarının sayısı alınabilecek sayıyı aşarsa, bir mesaj sizden bazı kullanıcı ayarlarını silmenizi isteyecektir. Almadan önce fazla kullanıcı ayarlarını silin.
- ☐ Almadan önce silmek istediğiniz kullanıcı ayarlarını seçin ve sonra **Delete** öğesine tıklayın.

9. **Import** öğesine tıklayın.
Kullanıcı ayarları yapılandırma şablonuna alınır.

LDAP Sunucusundan Alma

1. Yapılandırma şablonundan **Administrator Settings > Authentication Settings > User Settings** öğesini seçin.

2. **Import** öğesine tıklayın.

3. **LDAP** öğesini **Import Source** içinden seçin.

4. **Settings** öğesine tıklayın.

LDAP Server ayarları görüntülenir.

Not:

Bu LDAP sunucusu ayarı, kullanıcı bilgilerini LDAP sunucusundan almak içindir. Alınan (kopyalanan) kullanıcı ayarları, tarayıcının kendisini kullanarak kullanıcıların kimliklerini doğrulamak için kullanılır.

Diğer yandan, kimlik doğrulama yöntemi olarak **LDAP** veya **Local DB and LDAP** seçtiğinizde, kullanıcıların kimliği LDAP sunucusu ile iletişim kurularak doğrulanır.

5. Her öğeyi ayarlayın.

Bir LDAP sunucusundan kullanıcı ayarlarını alırken, LDAP ayarlarına ek olarak aşağıdaki ayarları da yapılandırabilirsiniz.

Diğer öğeler için İlgili Bilgiler kısmına bakın.

Öge		Açıklama
LDAP Server Settings	LDAP Server Type	LDAP sunucusunun türünü seçmenizi sağlar.
Search Settings	Search Filter	LDAP arama filtresi için kullanılan metni ayarlayabilirsiniz. Arama metnini düzenlemek için Custom öğesini seçin.
	Options	Type
	Options	Connection Mode
	Options	Port Number
		Scan To My Folder için kaydetme hedefi türünü ayarlayabilirsiniz.
		Type FTP olarak ayarlandığında, FTP bağlantı modunu ayarlayabilirsiniz.
		Type FTP olarak ayarlandığında, kullanmak istediğiniz bağlantı noktası numarasını ayarlayabilirsiniz.

6. **Connection Test** ögesini tıklayarak bağlantı testini gerektiği gibi gerçekleştirin.
LDAP sunucusundan 10 kullanıcı ayarını alır ve görüntüler.
7. **OK** ögesine tıklayın.
8. Bir alma yöntemi seçin.
 - ☐ Overwrite and Add: aynı kullanıcı kimliği mevcutsa üzerine yazar; mevcut değilse yeni kimlik ekler.
 - ☐ Replace All: almak istediğiniz kullanıcı ayarlarıyla her şeyi değiştirir.
9. **Import** ögesine tıklayın.
Ayar onayı ekranı görüntülenir.
10. **OK** ögesine tıklayın.
Doğrulama sonucu görüntülenir.
11. **Import** ögesine tıklayın.
Kullanıcı ayarları yapılandırma şablonuna alınır.

İlgili Bilgi

- ➔ [“Bir LDAP Sunucusu Yapılandırma” sayfa 141](#)
- ➔ [“LDAP Sunucusu Arama Ayarlarının Yapılandırılması” sayfa 143](#)

LDAP Sunucusu ile Senkronize Etme

Tarayıcı için LDAP Sunucusu ayarlarını yapın.

Ayarları, gerektiği şekilde hem birincil sunucu hem de ikincil sunucu için yapın.

Not:

LDAP Sunucusu ayarları **Kişiler** ile paylaşılır.

Kullanılabilir hizmetler

Aşağıdaki dizin servisleri desteklenir.

Hizmet Adı	Sürüm
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Bir LDAP Sunucusu Yapılandırma

Bir LDAP Sunucusu kullanmak için önce LDAP sunucusunu yapılandırmanız gerekir.

Web Config ögesinden ayarlarken:

Ağ sekmesi > LDAP Sunucusu > Temel (Birincil Sunucu) ya da Temel (İkincil Sunucu) ögesini seçin.

Doğrulama Yöntemi olarak Kerberos Kimlik Doğrulama ögesini seçerseniz, Kerberos ayarlarını yapmak için Ağ > Kerberos Ayarları ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonundan Network > LDAP server > Server Settings (Primary Server) ya da Server Settings (Secondary Server) ögesini seçin.

Doğrulama Yöntemi olarak Kerberos Kimlik Doğrulama ögesini seçerseniz, Kerberos ayarlarını yapmak için Network — Security > Kerberos Ayarları ögesini seçin.

Öge	Ayarlar ve Açıklama
LDAP Sunucusu Kullan	Kullan veya Kullanmayın ögesini seçin.
LDAP Sunucusu Adresi	LDAP sunucusu adresini girin. IPv4, IPv6 ya da FQDN biçiminde 1 ve 255 arası karakteri girin. FQDN biçimi için adresin başında ve sonunda hariç ASCII (0x20–0x7E) alfasayısal karakterleri ve tireleri kullanabilirsiniz.
LDAP Sunucusu Bağlantı Noktası Numarası (Port number)	1 ve 65535 arasında LDAP sunucusu bağlantı noktası numarası girin.
Güvenli Bağlantı	Tarayıcının LDAP sunucusuna erişimi için kimlik doğrulama yöntemini belirtin.
Sertifika Doğrulama	Bu etkinleştirildiğinde LDAP sunucusunun sertifikası doğrulanır. Bunu Etkinleştir olarak ayarlamanızı öneririz. Ayarlamak için CA Sertifikası ögesinin tarayıcıya alınması gerekir.
Arama Zaman Aşımı (sn.)	5 ve 300 saniye arasında zaman aşımı oluşmadan önce, arama için süre uzunluğunu ayarlayın.
Doğrulama Yöntemi	Kimlik doğrulama yöntemini seçin. Kerberos Kimlik Doğrulama ögesini seçerseniz, Kerberos ayarlarını önceden yapın. Kerberos Kimlik Doğrulama işlemini gerçekleştirmek için aşağıdaki ortam gerekir. ☐ Tarayıcı ve DNS sunucusu iletişim kurabilir. ☐ Tarayıcının saati, KDC sunucusu ve kimlik doğrulama için gereken sunucu (LDAP sunucusu, SMTP sunucusu, File sunucusu) senkronize edilir. ☐ Hizmet sunucusu IP adresi olarak atandığında, hizmet sunucusu için FQDN DNS sunucusu ters arama bölgesine kaydedilir.
Kullanılacak Kerberos Erişim Alanı	Kerberos Kimlik Doğrulama ögesini Doğrulama Yöntemi için seçtiyseniz, kullanmak istediğiniz Kerberos bölgesini seçin.
Yönetici Etki Alanı Adı / Kullanıcı Adı	LDAP sunucusu için kullanıcı adını 128 karakter veya daha kısa Unicode (UTF-8) biçiminde girin. 0x00 ila 0x1F ve 0x7F gibi kontrol karakterlerini kullanamazsınız. Adsız Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçildiğinde bu ayar kullanılmaz. Bunu belirtmek istemezseniz boş bırakın.
Parola	LDAP sunucusu kimlik doğrulaması için şifreyi 128 karakter veya daha kısa Unicode (UTF-8) biçiminde girin. 0x00 ila 0x1F ve 0x7F gibi kontrol karakterlerini kullanamazsınız. Adsız Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçildiğinde bu ayar kullanılmaz. Bunu belirtmek istemezseniz boş bırakın.

Kerberos Ayarları

Doğrulama Yöntemi olarak **Kerberos Kimlik Doğrulama** öğesini seçerseniz, Kerberos ayarları yapmanız gerekir. En fazla 10 Kerberos ayarı kaydedebilirsiniz.

Web Config öğesinden ayarlarken:

Ağ sekmesi > **Kerberos Ayarları** öğesini seçin.

Epson Device Admin öğesinden ayarlarken:

Yapılandırma şablonundan **Network > Security > Kerberos Ayarları** öğesini seçin.

Öge	Ayarlar ve Açıklama
Erişim Alanı (Etki Alanı)	255 karakter veya daha kısa ASCII (0x20–0x7E) Kerberos kimlik doğrulama alanını girin. Bunu kaydetmek istemezseniz boş bırakın.
KDC Adresi	Kerberos kimlik doğrulama sunucusunun adresini girin. IPv4, IPv6 veya FQDN biçiminde 255 karakter veya daha az girin. Bunu kaydetmek istemezseniz boş bırakın.
Bağlantı Noktası Numarası (Kerberos)	1 ve 65535 arasında Kerberos sunucusu bağlantı noktası numarasını girin.

LDAP Sunucusu Arama Ayarlarının Yapılandırılması

Kullanıcı ayarları için arama özniteliklerini ayarlar.

Web Config öğesinden ayarlarken:

Ağ sekmesi > **LDAP Sunucusu > Arama Ayarları (Kimlik Doğrulama)** öğesini seçin.

Epson Device Admin öğesinden ayarlarken:

Yapılandırma şablonundan **Administrator Settings > Authentication Settings > LDAP server > Search Settings (Authentication)** öğesini seçin.

Öge	Ayarlar ve Açıklama
Search Base (Distinguished Name)	LDAP sunucusundan kullanıcı bilgilerini aradığınızda başlangıç konumunu belirtin. 0 ve 128 arası karakteri (UTF-8) girin. İsteğe bağlı öznitelik aramazsanız bunu boş bırakın. Yerel sunucu dizini örneği: dc=server,dc=local
User ID Attribute	Kimlik numarasını ararken görüntülenecek öznitelik adını belirtin. 1 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: cn, uid
User name Display Attribute	Kullanıcı adı olarak görüntülenecek öznitelik adını belirtin. 0 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Bunu boş bırakabilirsiniz. Örnek: cn, name
Authentication Card ID Attribute	Kimlik doğrulama kartı kimliği olarak görüntülemek için öznitelik adını belirtin. 0 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Bunu boş bırakabilirsiniz. Örnek: cn, sn
ID Number Attribute	Kimlik numarasını ararken görüntülenecek öznitelik adını belirtin. 1 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: cn, id

Öge	Ayarlar ve Açıklama
Department Attribute	Bölüm adı olarak görüntülenecek öznitelik adını belirtin. 0 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Bunu boş bırakabilirsiniz. Örnek: ou, ou-cl
Email Address Attribute	E-posta adreslerini ararken belirtilecek öznitelik adını belirtin. 1 ve 255 arası karakteri ASCII biçiminde girin. İlk karakter a–z veya A–Z olmalıdır. Örnek: mail
Save To Attribute	Scan To My Folder için hedefi işaret eden öznitelik adını belirtin. 0 ve 255 arası karakteri ASCII biçiminde girin. Örnek: homeDirectory

LDAP Sunucusu Bağlantı Kontrolü

LDAP Sunucusu > Arama Ayarları ögesinde ayarlanan parametreyi kullanarak LDAP sunucusuna bağlantı testini gerçekleştirir.

1. Web Config'e erişin ve **Ağ** sekmesi > **LDAP Sunucusu > Bağlantı Testi** ögesini seçin.
2. **Başlat** ögesini seçin.
Bağlantı testi başlar. Testten sonra kontrol raporu görüntülenir.

LDAP Sunucusu Bağlantı Kontrolü Referansları

Mesajlar	Açıklama
Bağlantı testi başarılı oldu.	Bu mesaj sunucu ile bağlantı başarılı olduğunda görünür.
Bağlantı testi başarısız oldu. Ayarları kontrol edin.	Bu mesaj aşağıdaki nedenlerle görünür: ☐ LDAP sunucu adresi ya da bağlantı noktası sayısı doğru değil. ☐ Bir zaman aşımı oluştuysa. ☐ Kullanmayın ögesi LDAP Sunucusu Kullan olarak seçildiyse. ☐ Kerberos Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçilirse Erişim Alanı (Etki Alanı) , KDC Adresi ve Bağlantı Noktası Numarası (Kerberos) gibi ayarlar yanlıştır.
Bağlantı testi başarısız oldu. Ürününüz veya sunucu üzerindeki tarih ve saati işaretleyin.	Bu mesaj, tarayıcı ve LDAP sunucusu için yapılan zaman ayarlarının eşleşmemesi sebebiyle bağlantı başarısız olduğunda belirir.
Kimlik doğrulama başarısız oldu. Ayarları kontrol edin.	Bu mesaj aşağıdaki nedenlerle görünür: ☐ Kullanıcı Adı ve/veya Parola yanlış. ☐ Kerberos Kimlik Doğrulama ögesi Doğrulama Yöntemi olarak seçilirse zaman/tarih yapılandırılmayabilir.
İşlem tamamlanana kadar ürüne erişilemez.	Tarayıcı meşgulken bu mesaj görünür.

E-posta Sunucusunu Ayarlama

E-postama Tara ögesini kullandığınızda, E-posta Sunucusunu ayarlayın.

Not:

E-postama Tara ögesini, sadece E-postaya Tara ögesi etkinleştirildiğinde ayarlayabilirsiniz.

Web Config ögesinden ayarlarken:

Ağ sekmesi > E-posta Snosu > Temel ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonundan **Common > Email Server > Mail Server Settings** ögesini seçin.

Öge	Ayarlar ve Açıklama	
Doğrulama Yöntemi	Tarayıcının posta sunucusuna erişimi için kimlik doğrulama yöntemini belirtin.	
	Kapalı	Bir posta sunucusuyla iletişim kurarken kimlik doğrulama devre dışı bırakılır.
	SMTP Doğrulaması	E-posta sunucusunun SMTP kimlik doğrulamasını desteklemesi gerekir.
	SMTP öncesinde POP	Bu ögeyi seçtiğinizde, bir POP3 sunucusu ayarlayın.
Doğrulama Hesabı	Doğrulama Yöntemi olarak SMTP Doğrulaması ya da SMTP öncesinde POP seçerseniz, kimliği doğrulanmış hesap adını girin. 0 ve 255 arası karakteri ASCII (0x20–0x7E) girin.	
Doğrulanın Parola	Doğrulama Yöntemi olarak SMTP Doğrulaması ya da SMTP öncesinde POP seçerseniz, kimliği doğrulanmış parolayı girin. 0 ve 20 arası karakteri ASCII (0x20–0x7E) girin.	
Gönderenin Eposta Adresi	Göndericinin e-posta adresini girin. ASCII (0x20–0x7E) olarak şunlar hariç 0 ve 255 arası karakteri girin : () < > [] ; ¥. Başlangıç karakteri olarak “” kullanılamaz.	
SMTP Sunucusu Adresi	A–Z a–z 0–9 kullanarak 0 ila 255 arası karakter girin . -. IPv4 ya da FQDN formatını kullanabilirsiniz.	
SMTP Sunucusu Port Numarası	1 ile 65535 arasında bir sayı girebilirsiniz.	
Güvenli Bağlantı	E-posta sunucusu için güvenli bağlantı yöntemini belirleyin.	
	Hiçbiri	SMTP öncesinde POP kısmında Doğrulama Yöntemi seçimini yaparsanız bağlantı yöntemi Hiçbiri olarak ayarlanır.
	SSL/TLS	Bu, Doğrulama Yöntemi özelliği Kapalı veya SMTP Doğrulaması olarak ayarlandığında kullanılabilir.
	STARTTLS	Bu, Doğrulama Yöntemi özelliği Kapalı veya SMTP Doğrulaması olarak ayarlandığında kullanılabilir.
Sertifika Doğrulama	Bu etkinleştirildiğinde sertifika doğrulanır. Bunu Etkinleştir olarak ayarlamayı öneririz.	
POP3 Sunucusu Adresi	Doğrulama Yöntemi olarak SMTP öncesinde POP seçerseniz, POP3 sunucu adresini girin. A–Z a–z 0–9 kullanarak 0 ila 255 arası karakter girebilirsiniz. IPv4 ya da FQDN formatını kullanabilirsiniz.	
POP3 Sunucusu Port Numarası	Doğrulama Yöntemi olarak SMTP öncesinde POP seçerseniz, bağlantı noktası numarasını belirtin. 1 ile 65535 arasında bir sayı girebilirsiniz.	

Klasörüne Tara Ayarlama

Taranan görüntüleri her kullanıcıya atanan klasöre kaydeder. Aşağıdakileri özel bir klasör olarak ayarlayabilirsiniz.

Not:

Scan To My Folder öğesini, sadece **Ağ Klasörüne/FTP Sunucusuna Tara** öğesi etkinleştirildiğinde ayarlayabilirsiniz.

Ayara Kaydet	Doğrulama Yöntemi	Klasör Yolu Ayar Konumu
Kullanıcı kimliğinin adını kullanarak belirtilen klasörün altında otomatik olarak kişisel bir klasör oluşturmak için tüm Kimlik Doğrulama Ayarları için bir ağ klasörü belirtin.	☐ Yerel DB ☐ LDAP ☐ Yerel DB ve LDAP	Tarayıcı (Klasörüne Tara ayarı)
Her kullanıcıya tek tek farklı ağ klasörleri atayın.	Yerel DB	Tarayıcı (Kullnc Ayrıları)
	LDAP	LDAP Öznitelikleri
	Yerel DB ve LDAP	Tarayıcı (Kullnc Ayrıları) veya LDAP Öznitelikleri

Web Config öğesinden ayarlarken:

Ürün Güvenliği sekmesi > **Ağ Klasörüne/FTP Sunucusuna Tara** öğesini seçin.

Epson Device Admin öğesinden ayarlarken:

Yapılandırma şablonundan **Administrator Settings > Authentication Settings > Ağ Klasörüne/FTP Sunucusuna Tara > Scan to My Folder** öğesini seçin.

Öge	Açıklama
Ayara Kaydet	Ayar Türü ☐ Paylaşılan: Otomatik olarak, Kaydet kısmında belirtilen klasör yolu veya URL altında kullanıcı kimliğiyle adlandırılan bir klasör oluşturur ve taranan görüntüleri bu klasöre kaydeder. ☐ Bireysel: Her kullanıcı için tarama sonuçları kaydetme hedefini ayarlar. Yerel DB kullanıcıları, kullanıcı ayarlarında belirlenebilir. LDAP kullanıcıları, LDAP sunucusunun arama özniteliklerinden alınan depolama konumunu kullanır.
	Tür Aktarım protokolünü tarama çıktı hedefine göre seçin. Bir ağ klasörü için: Ağ Klasörü (SMB) Bir FTP sunucusu için: FTP
	Kaydet Çıktı yolu için yolu veya URL'yi belirtin. En fazla Unicode 160 karakter girin (UTF-16).
	Bağlantı Modu Tür içinde FTP öğesini seçtiğinizde ayarlayın. FTP sunucusuna bir bağlantı modu seçin.
	Port Numarası Tür içinde FTP öğesini seçtiğinizde ayarlayın. Taranan verileri bir FTP sunucusuna göndermek için 0 ve 65535 arasında bağlantı noktası numarasını girin.

Öge	Açıklama
Kimlik Doğrulama Ayarları	Ayar Türü Ayara Kaydet içinde Ayar Türü olarak Bireysel seçtiğinizde ayarlayın. Klasöre erişmek için “Kullanıcı Adı” ve “Parola” ayarlayın. ☐ Paylaşılan: Tüm kullanıcılar için ortak Kullanıcı Adı ve Parola kullanın. ☐ Bireysel: Yerel DB kullanıcıları için Kullanıcı Ayarları içinde tek tek Kullanıcı Adı ve Parola ayarlayın. LDAP kullanıcıları tek tek yapılandırılmaz. Bu öge ile ayarlanan Kullanıcı Adı ve Parola toplu iş olarak kullanılır.
Kullanıcı Adı	Tarama çıkış hedefi klasörüne erişmek için kullanıcı adını girin. En fazla Unicode 30 karakter girin (UTF-16). Bu ayarı, Paylaşılan veya LDAP sunucusu kullandığınızda yapın.
Parola	Kullanıcı Adı ögesine karşılık gelen parolayı girin. En fazla Unicode 20 karakter girin (UTF-16). Bu ayarı, Paylaşılan veya LDAP sunucusu kullandığınızda yapın.

Ağ Klasörüne/FTP Sunucusuna Tara İçin Hedefi Değiştirmeyi Yasaklama

Öge	Açıklama
Hedefin elle girilmesini engelle	Etkinleştirildiğinde, kullanıcı varsayılan hedefi değiştiremez.

Tek Dokunma İşlevlerini Özelleştirin

Kontrol paneli için ana ekranda görüntülenen simge düzenini düzenleyerek sadece gerekli simgeleri görüntüleyebilirsiniz.

Web Config ögesinden ayarlarken:

Ürün Güvenliği sekmesi > **Tek Dokunma İşlevlerini Özelleştirin** ögesini seçin.

Epson Device Admin ögesinden ayarlarken:

Yapılandırma şablonundan **Administrator Settings > Authentication Settings > Customize One-touch Functions** ögesini seçin.

Not:

Aşağıdaki durumlarda, ana ekranda belirtilen işlevlerin simgeleri görüntülenmez.

- ☐ **Kısıtlamalar** nedeniyle izin verilmeyen işlevleri seçtiğinizde.
- ☐ Oturum açmış bir kullanıcının e-posta adresi kayıtlı değilken. (E-postama Tara)
- ☐ Hedef klasör ayarlanmadığında. (Klasörüne Tara)

Öge	Açıklama
Ekran başına maksimum işlev	Kontrol panelinde görüntülenen simgelerin düzenini seçin. Görüntü seçilen düzende göre değişir.
Ekran(lar)	Sayfa sayısını seçin.

Öge	Açıklama
Numara	Her numaralı konum için görüntülemek istediğiniz işlevleri seçin.

Epson Device Admin Kullanarak Job History Raporları

Epson Device Admin ögesini kullanarak her grup ve her kullanıcı için bir Job History raporu oluşturabilirsiniz. Tarayıcıya en fazla 3000 kullanım geçmişi örneği kaydedebilirsiniz. Bir dönem belirterek veya düzenli bir plan ayarlayarak raporu oluşturabilirsiniz.

Job History ögesini bir rapor olarak çıktı almak için Aygıt Listesi ekranındaki şerit menüsünden **Options > Epson Print Admin Serverless/Authentication Settings > Manage the Epson Print Admin Serverless/Authentication compatible devices** ögesini seçin.

Kullanıcı raporunun nasıl oluşturulacağı ile ilgili ayrıntılar için Epson Device Admin belgelerine bakın.

Rapora Eklenebilecek Öğeler

Kullanıcı raporunda aşağıdaki öğelerin çıktısını alabilirsiniz.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Kontrol Panelinden Yönetici olarak Giriş Yapma

Tarayıcının kontrol panelinden yönetici olarak giriş yapmak için aşağıdaki yöntemlerden birini kullanabilirsiniz.

- Ekranın sağ üstündeki  ögesine dokunun.
 - ☐ Kimlik Doğrulama Ayarları ögesi etkinleştirildiğinde, simge **Hoş Geldiniz** ekranında görüntülenir (kimlik doğrulama bekleme ekranı).
 - ☐ Kimlik Doğrulama Ayarları devre dışı bırakıldığında, simge Ana ekranda görüntülenir.
- Onay ekranı görüntülendiğinde **Evet** ögesine dokunun.
- Yönetici parolasını girin.

Giriş yapma tamamlandı mesajı görüntülenir ve ardından kontrol panelindeki Ana ekran görüntülenir.

Çıkış yapmak için Ana ekranın sağ üstündeki  ögesine dokunun.

Kimlik Doğrulama Ayarları ögesini devre dışı bırakma

Kimlik Doğrulama Ayarları ögesini Web Config ögesini kullanarak devre dışı bırakabilirsiniz.

Not:

Tarayıcıya kaydedilen Kullnc Ayrları, Kimlik Doğrulama Ayarları devre dışı bırakılsa bile kaydedilecektir. Tarayıcıyı varsayılan değerlerine geri yükleyerek bunları kaldırabilirsiniz.

1. Web Config ögesine erişin.
2. **Ürün Güvenliği** sekmesi > **Temel** > **Kimlik Doğrulama** ögesini seçin.
3. **Kapalı** ögesini seçin.
4. **İleri** ögesine tıklayın.
5. **Tamam** ögesine tıklayın.

Not:

Kimlik Doğrulama Ayarları ögesini devre dışı bırakırsanız, Kilit Ayarları ögesi etkin kalır. Devre dışı bırakmak isterseniz, ayarları kontrol panelinden ya da Web Config ögesinden yapabilirsiniz.

İlgili Bilgi

- ➔ “Kontrol Panelinden Kilit Ayarları Ögesini Ayarlama” sayfa 85
- ➔ “Kilit Ayarları Ögesini Web Config Ögesinden Ayarlama” sayfa 85

Kimlik Doğrulama Ayarları Bilgilerinin Silinmesi (Varsayılan Ayarları Geri Yükle)

Tüm Kimlik Doğrulama Ayarları bilgilerini (Kart Okuyucu, Doğrulama Yöntemi, Kullnc Ayrları vb.) silmek için tüm tarayıcı ayarlarını satın alma zamanındaki varsayılan ayarlarına geri yükleyin.

Kontrol panelinde **Ayarlar** > **Sistem Yöneticisi** > **Varsayılan Ayarları Geri Yükle** > **Tüm Ayarlar** ögesini seçin.



Önemli:

Tüm kişiler ve diğer ağ ayarları da silinecektir. Silinen ayarlar geri yüklenemez.

Sorunları Çözme

Kimlik Doğrulama Kartı Okunamıyor

Aşağıdakileri kontrol edin.

- ☐ Kimlik doğrulama aygıtının tarayıcıya düzgün bağlanıp bağlanmadığını kontrol edin.
Kimlik doğrulama aygıtını, tarayıcının arkasındaki harici arayüz USB bağlantı noktasına bağlayın.
- ☐ Kimlik doğrulama aygıtının ve kimlik doğrulama kartının desteklendiğini kontrol edin.

Bakım

Tarayıcının Dışını Temizleme.	151
Tarayıcının İçini Temizleme.	151
Makara Takma Kitini Değişirme.	156
Tarama Sayısını Sıfırlama.	161
Enerji Tasarrufu.	161
Tarayıcıyı Nakletme.	162
Ayarları Yedekleme.	163
Varsayılan Ayarları Geri Yükle.	164
Uygulamaları ve Bellenimi Güncelleme.	165

Tarayıcının Dışını Temizleme

Temiz bir bezle veya yumuşak deterjan ve suyla nemlendirilmiş bir bezle dış kasadaki izleri silin.



Önemli:

- ☐ Tarayıcıyı temizlemek için asla alkol, tiner veya aşındırıcı çözücü madde kullanmayın. Deformasyon veya renk solması olabilir.
- ☐ Ürünün içine su girmesine izin vermeyin. Bu, bir arızanın oluşmasına neden olabilir.
- ☐ Tarayıcının kasasını hiçbir zaman açmayın.

1. Tarayıcıyı kapatmak için düğmesine basın.
2. AC adaptörünü tarayıcıdan çıkarın.
3. Hafif deterjan ve suyla ıslatılmış bir bezle dış gövdeyi temizleyin.

Not:

Dokunmatik ekranı yumuşak, kuru bir bez kullanarak silin.

Tarayıcının İçini Temizleme

Tarayıcıyı bir süre kullandıktan sonra, silindir üzerindeki kağıt ve oda tozu veya tarayıcı içindeki cam bölüm kağıt besleme veya taranan görüntü kalitesi sorunlarına neden olabilir. Her 5,000 taramada bir tarayıcının içini temizleyin.

Kontrol panelinde veya Epson Scan 2 Utility içinde en son tarama sayısını kontrol edebilirsiniz.

Bir yüzeye çıkması zor bir madde bulaştıysa izleri çıkarmak için orijinal bir Epson temizleme kiti kullanın. İzleri kaldırmak için temizleme bezi üzerinde az miktarda bir temizleyici kullanın.

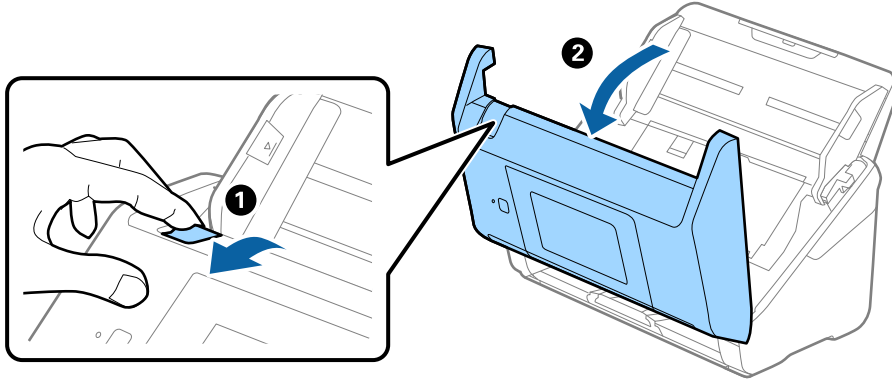


Önemli:

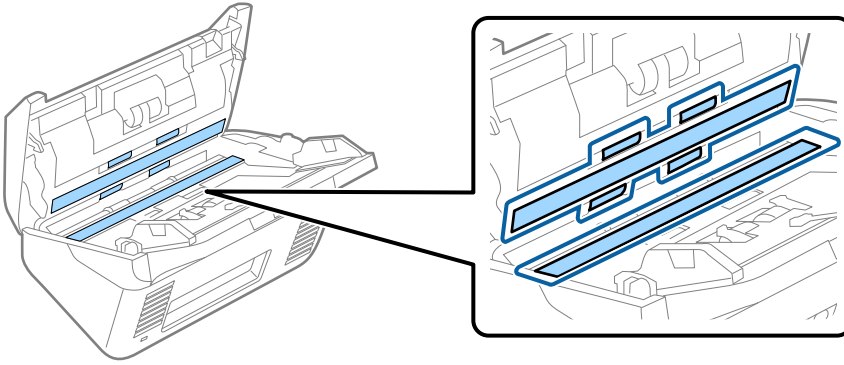
- ☐ Tarayıcıyı temizlemek için asla alkol, tiner veya aşındırıcı çözücü madde kullanmayın. Deformasyon veya renk solması olabilir.
- ☐ Tarayıcı üzerine kesinlikle sıvı veya yağ püskürtmeyin. Ekipmana veya devrelere hasar verme anormal çalışmaya neden olabilir.
- ☐ Tarayıcının kasasını hiçbir zaman açmayın.

1. Tarayıcıyı kapatmak için düğmesine basın.
2. AC adaptörünü tarayıcıdan çıkarın.

3. Kolu çekin ve tarayıcı kapağını açın.



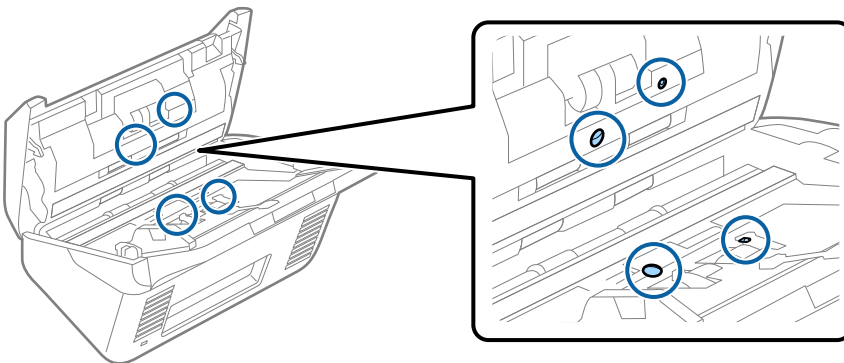
4. Yumuşak bir bez veya orijinal bir Epson temizleme kiti kullanarak tarayıcı kapağının alt iç tarafındaki plastik silindir ve cam yüzey üzerindeki izleri silin.



Önemli:

- ☐ Cam yüzey üzerine aşırı yük koymayın.
- ☐ Bir fırça veya sert bir araç kullanmayın. Cam üzerindeki çizikler tarama kalitesini etkileyebilir.
- ☐ Temizleyiciyi doğrudan cam yüzey üzerine püskürtmeyin.

5. Pamuk bir bez ile sensörler üzerindeki izleri silin.

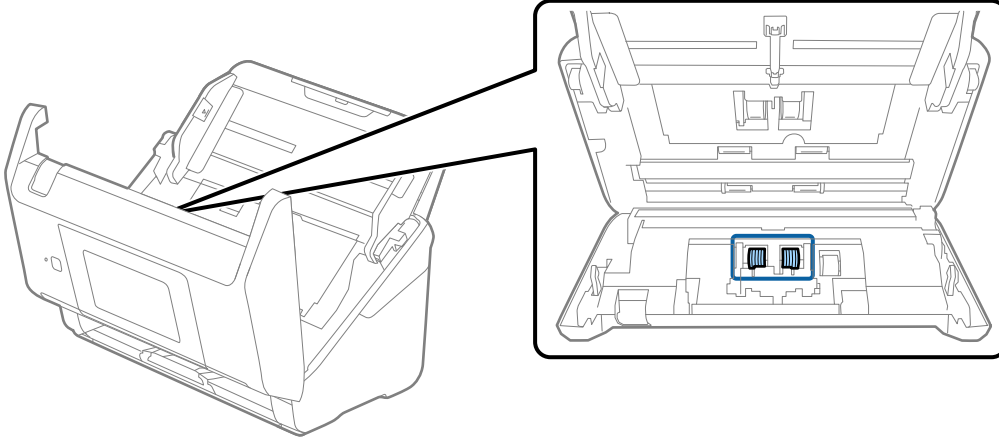




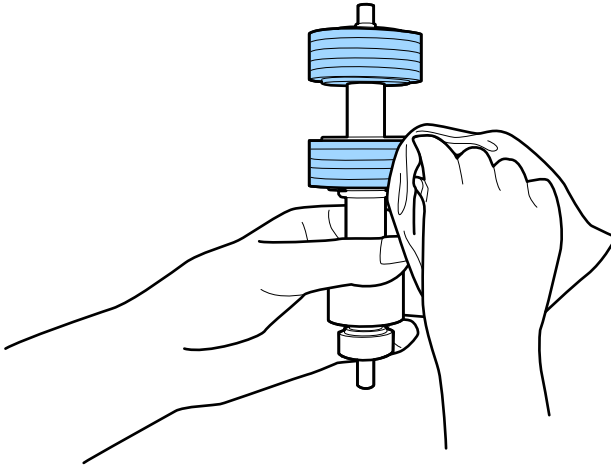
Önemli:

Pamuk bez üzerinde bir temizleyici olarak sıvı kullanmayın.

6. Kapağı açın ve ardından, ayırma makarasını çıkarın.
Daha fazla ayrıntı için bkz. “Silindir Takma Kitini Değiştirme”.



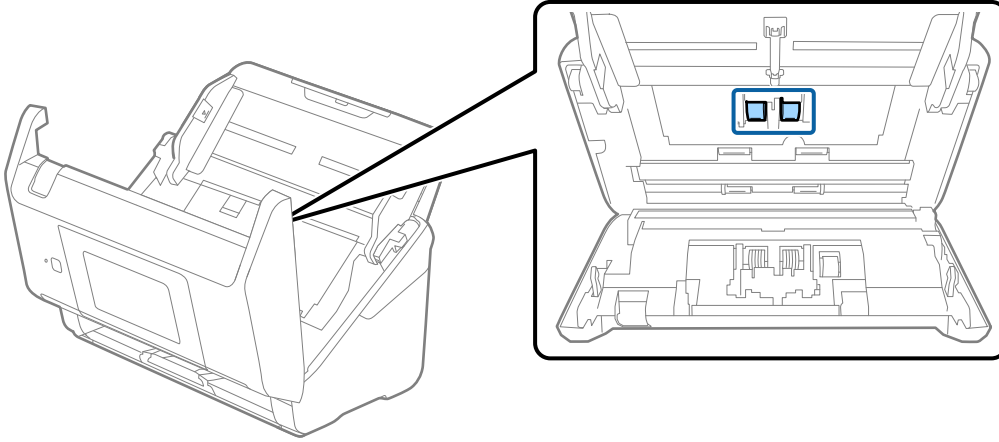
7. Orijinal bir Epson temizleme kiti veya yumuşak, nemli bir bez kullanarak ayırma makarası üzerindeki toz veya kiri silin.



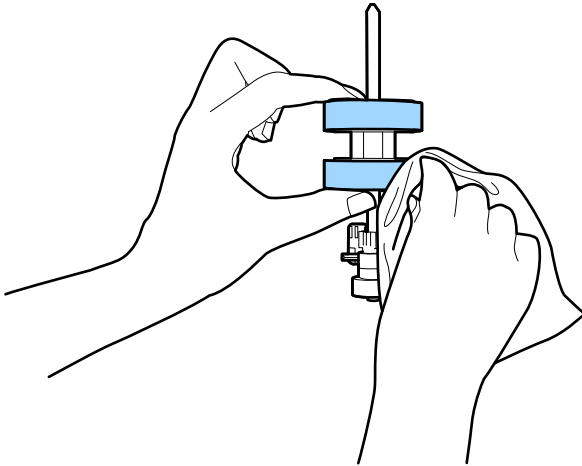
Önemli:

Silindiri silmek için yalnızca orijinal Epson temizleme kiti veya yumuşak, nemli bir bez kullanın. Kuru bir bez kullanma silindirin yüzeyine zarar verebilir.

8. Kapağı açın ve ardından, alma makarasını çıkarın.
Daha fazla ayrıntı için bkz. “Silindir Takma Kitini Değiştirme”.



9. Orijinal bir Epson temizleme kiti veya yumuşak, nemli bir bez kullanarak alma makarası üzerindeki toz veya kırı silin.

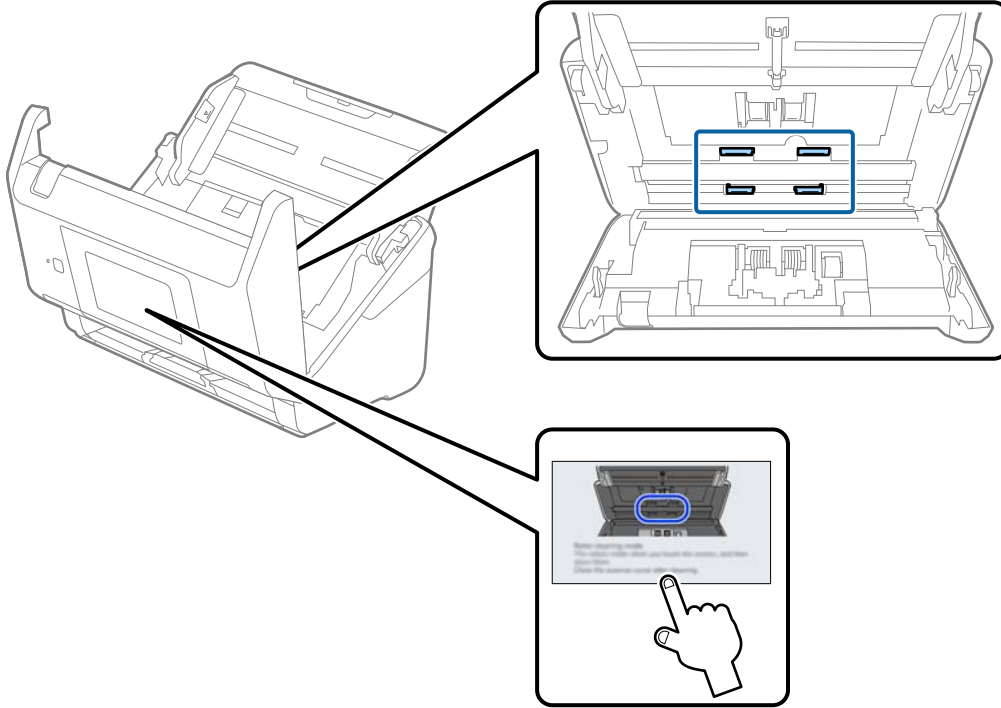


Önemli:

Silindiri silmek için yalnızca orijinal Epson temizleme kiti veya yumuşak, nemli bir bez kullanın. Kuru bir bez kullanma silindirin yüzeyine zarar verebilir.

10. Tarayıcı kapağını kapatın.
11. AC adaptörünü takın ve ardından, tarayıcıyı açın.
12. Giriş ekranından **Tarayıcı Bakımı** ögesini seçin.
13. **Tarayıcı Bakımı** ekranında, **Silindir Temizliği** ögesini seçin.
14. Tarayıcı kapağını açmak için kolu çekin.
Tarayıcı silindir temizleme moduna girer.

15. LCD ekranın herhangi bir yerine dokunarak en alttaki silindirleri yavaşa dndrn. Orijinal bir Epson temizleme kiti veya suyla nemlendirilmiř yumuřak bir bez kullanarak silindirlerin yzeyini silin. Silindirler temizlenene kadar bunu tekrarlayın.



Dikkat:

Silindiri alıřtırırken ellerinizi veya saınızı mekanizmaya kaptırmamaya dikkat edin. Bu, yaralanmaya neden olabilir.

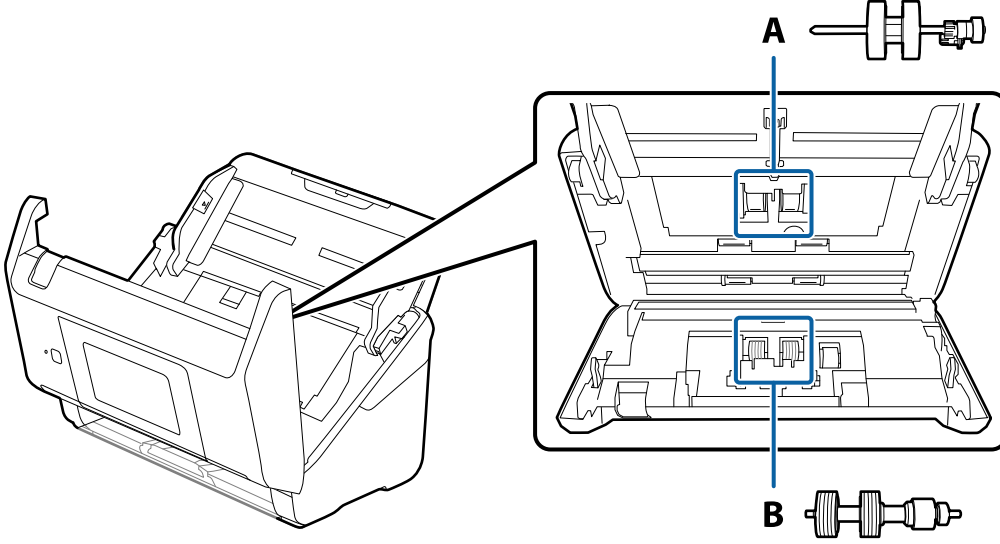
16. Tarayıcı kapağını kapatın.
Tarayıcı silindir temizleme modundan ıkar.

İlgili Bilgi

➔ “Makara Takma Kitini Deėiřtirme” sayfa 156

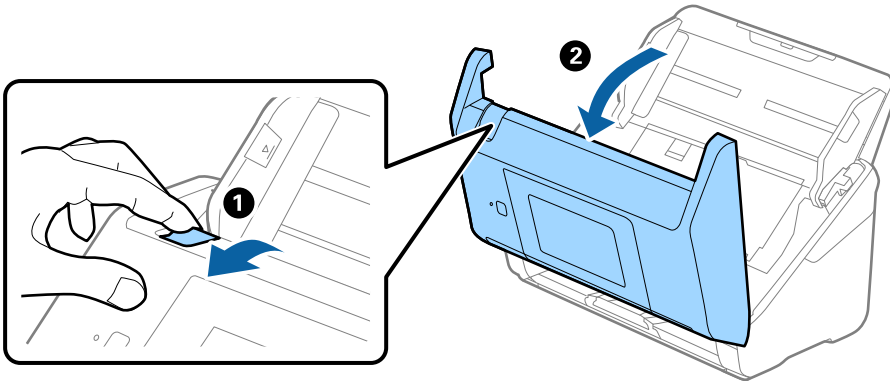
Makara Takma Kitini Deęiřtirme

Tarama sayısı makaralarının ömür döngüsünü ařtıęında makara takma kitinin (alma makarası ve ayırma makarası) deęiřtirilmesi gerekir. Kontrol panelinde veya bilgisayarınızın ekranında bir deęiřtirme mesajı görüntülendięinde, ařaęıdaki adımları takip edin ve deęiřtirin.

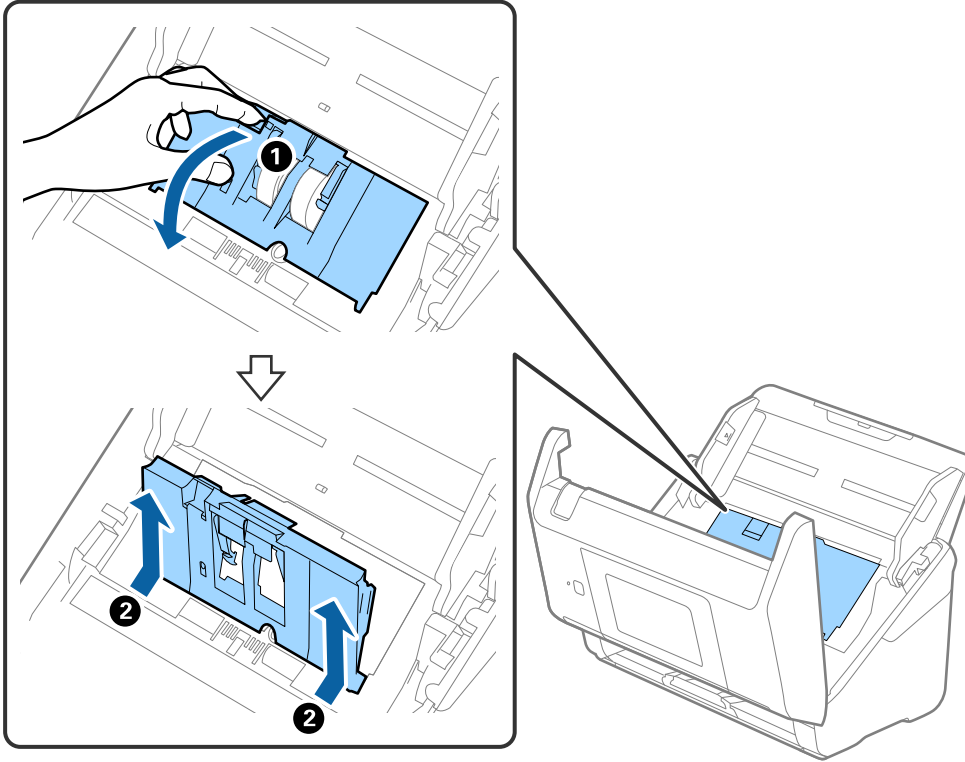


A: alma makarası, B: ayırma makarası

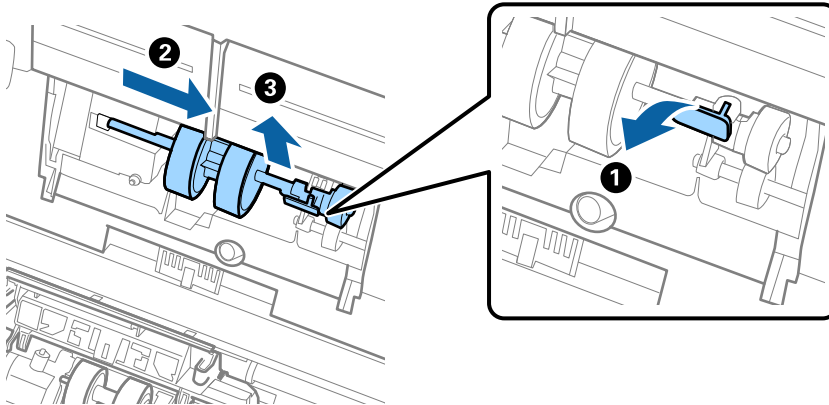
1. Tarayıcıyı kapatmak için  düęmesine basın.
2. AC adaptörünü tarayıcıdan çıkarın.
3. Kolu çekin ve tarayıcı kapaęını açın.



4. Alma makarasının kapaęını aın ve ardından, kaydırıp ıkarın.



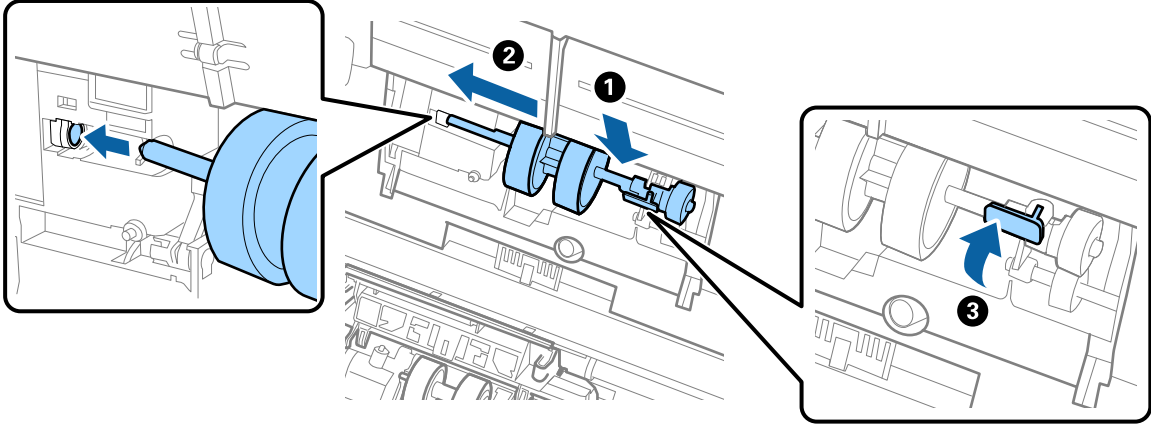
5. Silindir ekseninin fiđstürünü ařaęı ekin ve ardından, takılı alma silindirlerini kaydırın ve ıkarın.



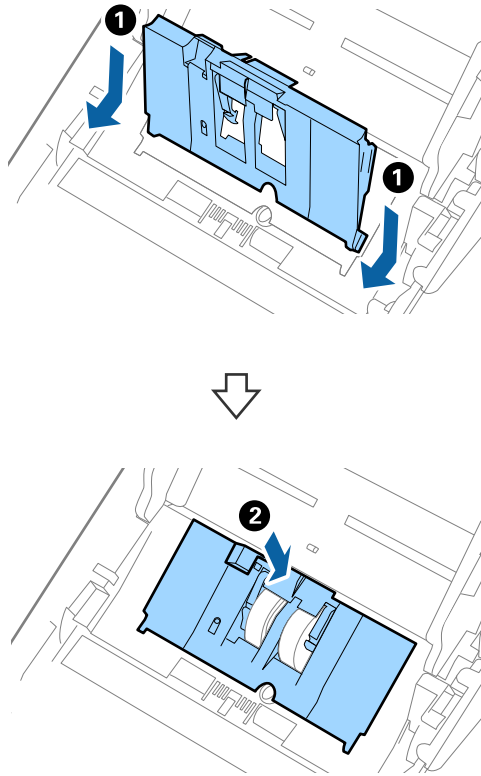
Önemli:

Alma silindirini zorla dıřarı ekmeyin. Bu, tarayıcının iine zarar verebilir.

6. Fikřtörü basılı tutarken, yeni alma silindirini sola kaydırın ve tarayıcıdaki delik içine takın. Sabitlemek için fikřtüre basın.



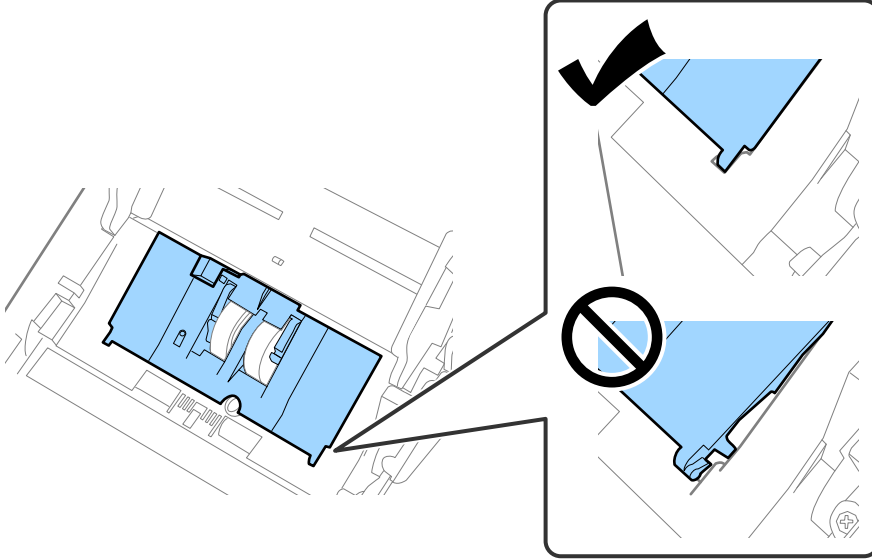
7. Alma silindiri kapaęının kenarını oyuęun içine koyun ve kaydırın. Kapaęı sıkıca kapatın.



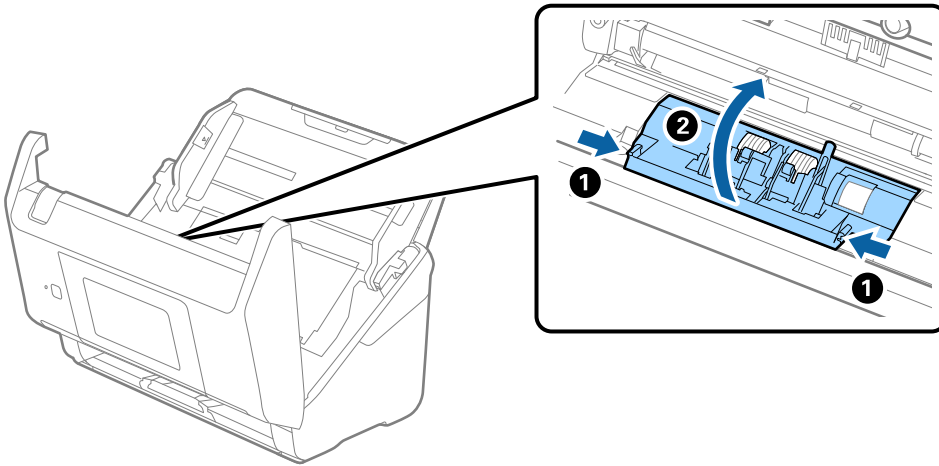


Önemli:

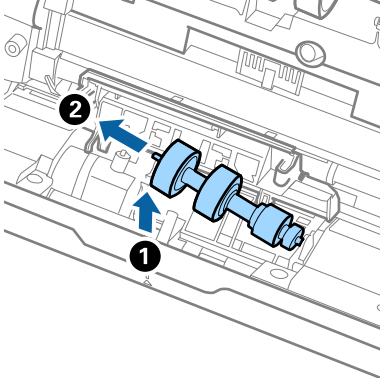
- ❑ Alma kapaęının düzgün kapatıldığından emin olun.
- ❑ Kapak çok sert kapatıldıysa alma silindirlerinin düzgün takıldığından emin olun.
- ❑ Kaldırıldığında kapaęı takmayın.



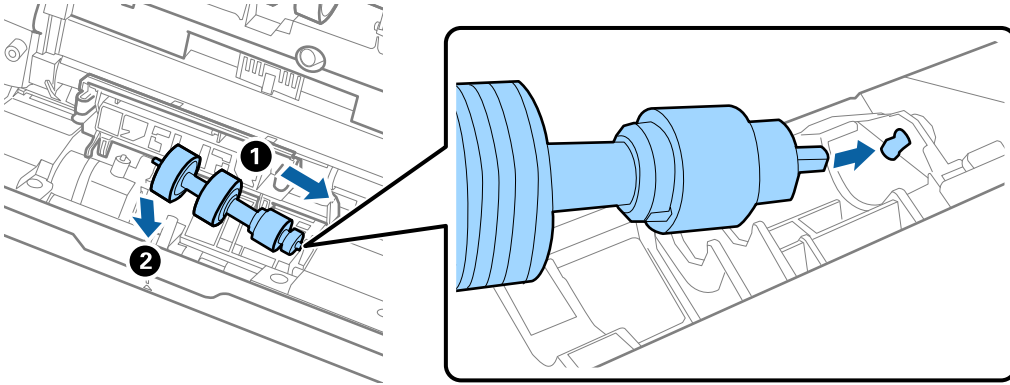
8. Kapaęı açmak için ayırma rulosu kapaęının her iki ucundaki kancaları itin.



9. Ayırma makarasının sol tarafını kaldırın ve ardından, takılı ayırma makaralarını kaydırın ve çıkarın.



10. Yeni ayırma rulosu eksenini saę taraftaki delięin iine takın ve ardından, silindiri alaltın.



11. Ayırma rulosu kapaęını kapatın.



Önemli:

Kapaęı kapatmak zorsa ayırma rulolarının düzgün takıldığından emin olun.

12. Tarayıcı kapaęını kapatın.
13. AC adaptörünü takın ve ardından, tarayıcıyı açın.
14. Kontrol panelindeki tarama sayısını sıfırlayın.

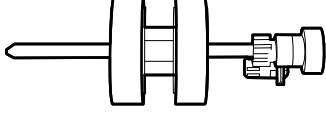
Not:

Alma silindirini ve ayırma rulosunu yerel mercilerin kural ve düzenlemelerini izleyerek elden çıkarın. Bunları paralarına ayırmayın.

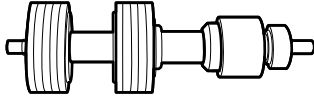
Makara Takma Kiti Kodları

Tarama sayısı servis sayısını aştığında parçalar (alma makarası ve ayırma makarası) değiştirilmelidir. Kontrol panelinde veya Epson Scan 2 Yardımcı Programı içinde en son tarama sayısını kontrol edebilirsiniz.

A



B



A: alma makarası , B: ayırma makarası

Parça adı	Kodlar	Yaşam döngüsü
Makara Takma Kiti	B12B819671 B12B819681 (yalnızca Hindistan)	200,000*

* Epson test orijinal kağıtları kullanılarak art arda taramayla bu sayıya erişilir ve bu sayı değiştirme döngüsünün bir kılavuzudur. Değiştirme döngüsü, birçok kağıt tozu üreten kağıt veya kaba yüzeye sahip kağıt gibi farklı kağıt türlerine bağlı olarak değişebilir, bu durum yaşam döngüsünü kısaltabilir.

Tarama Sayısını Sıfırlama

Silindir takma kitini değiştirdikten sonra tarama sayısını sıfırların.

1. Ana ekrandan **Ayarlar > Aygıt Bilgileri > Tarama Sayısını Sıfırla > Silindirin Değiştirilmesinden Sonra Tarama Sayısı** menüsünü seçin.
2. **Evet** ögesine dokununuz.

İlgili Bilgi

➔ [“Makara Takma Kitini Değiştirme” sayfa 156](#)

Enerji Tasarrufu

Tarayıcı tarafından hiç işlem gerçekleştirilmediğinde uyku modunu veya otomatik güç kapatma modunu kullanarak enerjiden tasarruf edebilirsiniz. Tarayıcı uyku moduna girip otomatik kapanmadan önceki süreyi ayarlayabilirsiniz. Her türlü artış ürünün enerji verimliliğini etkileyecektir. Herhangi bir değişiklik yapmadan önce çevreyi düşünün.

1. Giriş ekranında **Ayarlar** ögesini seçin.
2. **Temel Ayarlar** ögesini seçin.

3. **Kapatma Ayarları** düğmesine basın ve ardından ayarları yapın.

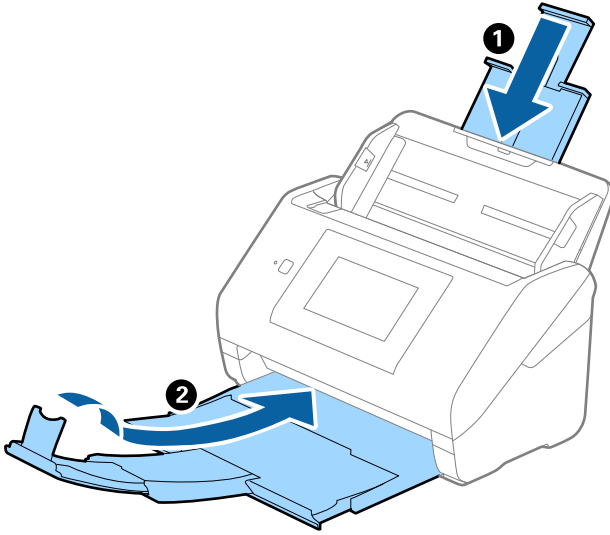
Not:

Kullanılabilir özellikler satın alma konumuna göre değişebilir.

Tarayıcıyı Nakletme

Tarayıcıyı taşımak veya onarım için nakletmeniz gerekirse, tarayıcıyı paketlemek için aşağıdaki adımları izleyin.

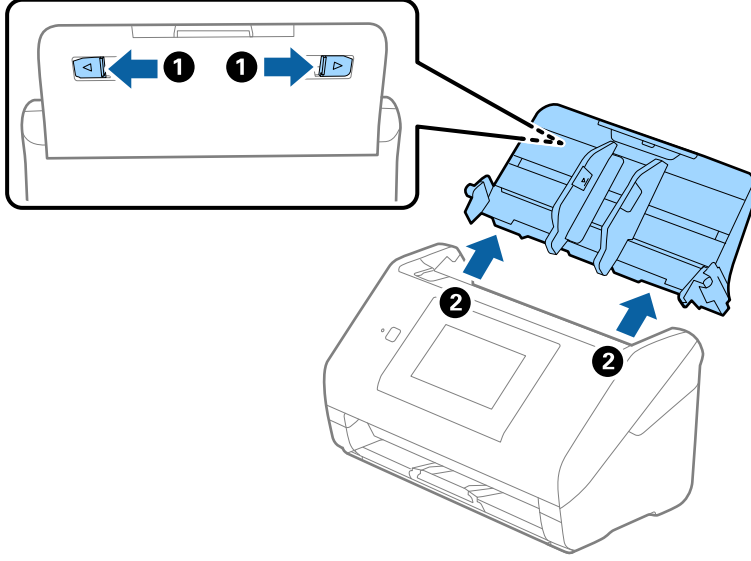
1. Tarayıcıyı kapatmak için  düğmesine basın.
2. AC adaptörünün fişini çıkarın.
3. Kabloları ve cihazları çıkarın.
4. Giriş tepsiyi uzantısını ve çıkış tepsisini kapatın.



Önemli:

Çıkış tepsisini iyice kapattığınızdan emin olun; aksi halde nakliye sırasında hasar görebilir.

5. Giriş tepsisini çıkarın.



6. Tarayıcıyla birlikte gelen ambalaj malzemelerini yerleştirin ve sonra tarayıcıyı orijinal kutusuna veya sağlam bir kutuya yerleştirin.

Ayarları Yedekleme

Web Config'den dosyaya ayarlanan değeri verebilirsiniz. Kişi, ayar değerlerini yedeklemek, tarayıcıyı değiştirmek vb. için kullanabilirsiniz.

İkili dosya olarak verildiğinden verilen dosya düzenlenemez.

Ayarları dışa aktarın

Tarayıcı için ayarı verin.

1. Web Config'e erişin ve sonra **Aygıt Yönetimi** sekmesi > **Ayar Değerini Dışa ve İçe Aktar** > **Dışa Aktar** 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. Verilen dosyayı şifrelemek için bir parola girin.
Dosyayı almak için şifre gerekir. Dosyayı şifrelemek istemiyorsanız bunu boş bırakın.

4. **Dışa Aktar** ögesine tıklayın.



Önemli:

Tarayıcının aygıt adı ve IPv6 adresi gibi ağ ayarlarını vermek istiyorsanız, **Aygıtın ayarlarını birbirinden bağımsız olarak seçmek için etkinleştirin** ögesini seçin ve daha fazla öge seçin. Yedek tarayıcı için yalnızca seçilen değerleri kullanın.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35

Ayarları alma

Verilen Web Config dosyasını tarayıcıya alın.



Önemli:

Tarayıcı adı veya IP adresi gibi tek tek bilgileri içeren değerleri alırken aynı IP adresinin aynı ağda olmadığından emin olun.

1. Web Config'e erişin ve sonra **Aygıt Yönetimi** sekmesi > **Ayar Değerini Dışa ve İçe Aktar** > **İçe Aktar** ögesini seçin.
2. Verilen dosyayı seçin ve sonra kodlanmış şifreyi girin.
3. **İleri** ögesine tıklayın.
4. Almak istediğiniz ayarları seçin ve sonra **İleri** ögesine tıklayın.
5. **Tamam** ögesine tıklayın.

Ayarlar tarayıcıya uygulanır.

İlgili Bilgi

➔ “Web Tarayıcıda Web Yapılandırmayı Çalıştırma” sayfa 35

Varsayılan Ayarları Geri Yükle

Kontrol panelinde **Ayarlar** > **Sistem Yöneticisi** > **Varsayılan Ayarları Geri Yükle** ögesini seçin ve ardından varsayılan ayarlarına geri yüklemek istediğiniz öğeleri seçin.

- ☐ Ağ Ayarları: ağla ilgili ayarları ilk durumlarına geri yükleyin.
- ☐ Ağ Ayarları Dışında Tümü: ağla ilgili ayarlar hariç diğer ayarları ilk durumlarına geri yükleyin.
- ☐ Tüm Ayarlar: tüm ayarları satın alındıkları ilk durumlarına geri yükleyin.



Önemli:

Tüm Ayarlar ögesini seçerseniz ve çalıştırırsanız, kişiler dahil tarayıcıda kayıtlı tüm ayar verileri ve kimlik doğrulama kullanıcı ayarları silinecektir. Silinen ayarlar geri yüklenemez.

Uygulamaları ve Bellenimi Güncelleme

Uygulamaları ve bellenim sürümünü güncelleyerek bazı sorunları giderebilir ve işlevleri iyileştirebilir veya ekleyebilirsiniz. Uygulamaların ve bellenim sürümünün en son sürümüne sahip olduğunuzdan emin olun.



Önemli:

☐ Güncelleme yapılırken bilgisayarı ya da tarayıcıyı kapatmayın.

Not:

Tarayıcı İnternet'e bağlanabildiğinde bellenimi Web Config'den güncelleyebilirsiniz. **Aygıt Yönetimi** sekmesi > **Firmware Güncellemesi** ögesini seçin, görüntülenen mesajı kontrol edin ve ardından, **Başlat** ögesine tıklayın.

1. Tarayıcı ve bilgisayarın birbirine, bilgisayarın da İnternet'e bağlı olduğundan emin olun.
2. EPSON Software Updater uygulamasını başlatıp, uygulamaları ya da bellenim sürümünü güncelleyin.

Not:

Windows Server işletim sistemleri desteklenmez.

☐ Windows 10

Başlat düğmesine tıklayın ve ardından **Epson Software** > **EPSON Software Updater** ögesini seçin.

☐ Windows 8.1/Windows 8

Arama kutusuna uygulama adını girin ve ardından, görüntülenen simgeyi seçin.

☐ Windows 7

Başlangıç düğmesine tıklayın ve ardından, **Tüm Programlar** veya **Programlar** > **Epson Software** > **EPSON Software Updater**'i seçin.

☐ Mac OS

Bulucu > **Git** > **Uygulamalar** > **Epson Software** > **EPSON Software Updater** öğelerini seçin.

Not:

Güncellemek istediğiniz uygulamayı listede bulamıyorsanız, EPSON Software Updater'ı kullanarak güncelleyemezsiniz. Uygulamaların en son sürümlerini yerel Epson web sitesinden kontrol edin.

<http://www.epson.com>

Kontrol Panelini Kullanarak Tarayıcının Bellenimini Güncelleme

Tarayıcı İnternet'e bağlanabilirse kontrol panelini kullanarak tarayıcının bellenimini güncelleyebilirsiniz. Bellenim güncellemelerini düzenli kontrol etmek için de tarayıcıyı ayarlayabilirsiniz, varsa size bildirilir.

1. Giriş ekranında **Ayarlar** ögesini seçin.

2. **Sistem Yöneticisi > Aygıt Yazılımı Güncelleme > Güncelle** öğesini seçin.

Not:

*Tarayıcıyı kullanılabilir bellenim güncellemelerini düzenli kontrol etmeye ayarlamak için **Bildirim > Açık** öğesini seçin.*

3. Ekranda görüntülenen mesajı inceleyin ve uygun güncellemeleri aramaya başlayın.
4. bir bellenim güncellemesinin kullanılabilir olduğu bilgisini veren bir mesaj LCD ekranda görüntülenirse güncellemeyi başlatmak için ekran talimatlarını izleyin.



Önemli:

- ❑ Güncelleme tamamlanana kadar tarayıcıyı kapatmayın veya fişini çıkarın; aksi halde tarayıcı arızalanabilir.
- ❑ Bellenim güncellemesi tamamlanmadıysa veya başarısız olursa tarayıcı normal başlamaz ve tarayıcı bir sonraki kez açıldığında LCD ekranda "Recovery Mode" görüntülenir. Bu durumda, bir bilgisayar kullanarak bellenimi yeniden güncellemeniz gerekir. Tarayıcıyı bir USB kablosu ile bilgisayara bağlayın. Tarayıcıda "Recovery Mode" görüntülenirken, bir ağ bağlantısı üzerinden bellenimi güncelleyemezsiniz. Bilgisayarda, yerel Epson web sitesine erişin ve sonra en son tarayıcı bellenimini indirin. Sonraki adımlar için web sitesindeki talimatlara bakın.

Web Config Kullanarak Bellenimi Güncelleme

Tarayıcı İnternet'e bağlanabildiğinde bellenimi Web Config'den güncelleyebilirsiniz.

1. Web Config'e erişin ve **Aygıt Yönetimi** sekmesi > **Firmware Güncellemesi** öğesini seçin.
2. **Başlat** öğesine tıklayın ve sonra ekrandaki talimatları izleyin.

Bellenim onayı başlar ve güncellenen bellenim varsa bellenim bilgileri görüntülenir.

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 Tarayıcıda Web Yapılandırmayı Çalıştırma" sayfa 35](#)

İnternet'e Bağlanmadan 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.

Not:

Güncellemeden önce Epson Scan 2 tarayıcı sürücüsünün bilgisayarınıza yüklü olduğundan emin olun. Epson Scan 2 yüklü değilse yeniden yükleyin.

1. En yeni bellenim güncellemesi sürümleri için Epson web sitesine göz atın.

<http://www.epson.com>

- ❑ Tarayıcınız için bellenim varsa, bu bellenimi indirin ve sonraki adıma geçin.

❑ Web sitesinde bellenim yoksa, bu zaten en yeni bellenimi kullandığınızı gösterir.

2. USB kablosuyla indirilen bellenimi içeren bilgisayarı tarayıcıya bağlayın.
3. İndirilen .exe dosyasına çift tıklayın.
Epson Firmware Updater başlar.
4. Ekrandaki talimatları uygulayın.