Kart Kimlik Doğrulaması

Yönetici Kılavuzu

Aralık 2020

www.lexmark.com

İçerikler

Genel Bakış

Kart okuyucu kullanarak yazıcıya erişimi güvence altına almak için uygulamayı kullanın. Kullanıcılar bilgileri girdiğinde kimlik bilgileri aşağıdakilerden birini kullanılarak doğrulanır:

- Bir ana yazıcı. Ana yazıcı çevrimdışıysa ana yazıcı çevrimiçi olana kadar yedek yazıcı ana yazıcının görevini üstlenir.

  Not: Yazıcı ayarları yapılırken yazıcıların aynı ağ üzerinde bulunduğundan emin olun.
- Kuruluş tarafından belirlenen kimlik doğrulamasına bağlı olarak Lightweight Directory Access Protocol (LDAP), Lexmark™ Belge Dağıtıcı (LDD) sunucuları veya Güvenlik Hizmeti Sağlayıcıları.

Bu belgede uygulamanın yapılandırılması, kullanılması ve sorun gidermesiyle ilgili bilgi verilmektedir.

Ön şartların ayarlanması

Uygulamayı yapılandırmak için yönetici haklarınızın olması gerekebilir.

Yerleşik Web Sunucusu'na erişme

1. Yazıcının IP adresini alın. Aşağıdakilerden birini yapın:
   - IP adresini yazıcı ana ekranında bulun.
   - Ağlar/Bağlantı Noktaları menüsünün TCP/IP bölümünde bulunan IP adresine bakın.
2. Bir web tarayıcısı açın ve yazıcının IP adresini yazın.

İç kullanıcı hesabı ekleme

Yazıcı tabanlı kimlik doğrulama kullanılırken iç kullanıcı hesabı gerekir.

1. Yerleşik Web Sunucusu'ndan sırayla **Ayarlar** veya **Yapılandırma** öğesini tıklatın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Güvenlik** > **Güvenlik Kurulumu** > **İç Hesaplar** > **İç Hesap Ekle** öğesini tıklayın.
   - **Güvenlik** > **Güvenlik Ayarlarını Düzenle** > **İç Hesaplar** > **İç Hesap Ekle** öğesini tıklatın.
3. Hesap bilgilerini girip **Gönder** öğesini tıklatın.
4. Gerekirse İç Hesapları Yönet bölümünden özel bir blok yapı adı girin ve gerekli kullanıcı kimlik bilgilerini belirtin.
5. **İlet** düğmesini tıklatın.

İç kullanıcı hesapları için grup oluşturma

1. Embedded Web Server'dan **Ayarlar** veya **Yapılandırma** öğesine tıklayın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Güvenlik** > **Güvenlik Kurulumu** > **İç Hesaplar** > **İç hesaplarla kullanılacak grupları ayarla** seçeneğine tıklayın.
   - **Güvenlik** > **Güvenlik Ayarlarını Düzenle** > **İç Hesaplar** > **İç hesaplarla kullanılacak grupları ayarla** seçeneğine tıklayın.
3. Bir grup adı girin ve ardından **Ekle** seçeneğine tıklayın.
4. Gruba iç hesaplar ekleyin.
5. **Gönder** öğesine tıklayın.

Güvenlik şablonu oluşturma

Güvenlik şablonu; İç Hesaplar, Kerberos, LDAP, LDAP+GSSAPI ve Active Directory gibi güvenlik blok yapılarından oluşur. Yazıcı işlevlerini ve uygulamalarını güvence altına almak için bu şablonlar erişim denetimine uygulanır.

1. Embedded Web Server'dan **Ayarlar** veya **Yapılandırma** öğesine tıklayın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Güvenlik** > **Güvenlik Kurulumu** > **Güvenlik Şablonu** > **Güvenli Şablonu Ekle** öğesine tıklayın.
   - **Güvenlik** > **Güvenlik Ayarlarını Düzenle** > **Güvenlik Şablonları** > **Güvenli Şablonu Ekle** öğesine tıklayın.
3. Bir güvenlik şablonu adı girin ve aşağıdaki kimlik doğrulama ayarlarından birini seçin:
   - Bağımız bir ayarda yazıcı tabanlı kimlik doğrulaması için iç hesap blok yapısını seçin.
   - Bir Active Directory kurulumunda Lexmark Yazdırma Yönetimi (LPM) Sunucusuz Baskı Sürümü ile yazıcı tabanlı kimlik doğrulaması için LDAP+GSSAPI blok yapısını seçin.
   - LDAP kimlik doğrulaması için bir LDAP blok yapısını belirleyin.
4. **Şablonu Kaydet** öğesine tıklayın.

Not: Mevcut bir güvenlik şablonunu değiştirmek için güvenlik şablonuna tıklayın ve ardından şablon için yetkilendirmeyi ekleyin veya değiştirin.

Erişim denetimlerinin yapılandırılması

Not: Yönetici Oturum Açma özelliğini kullanırken iç hesaplar için güvenlik şablonunu yapılandırdığınızdan emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Güvenlik şablonu oluşturma".

1. Embedded Web Server'dan **Ayarlar** veya **Yapılandırma** öğesine tıklayın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Güvenlik** > **Güvenlik Kurulumu** > **Erişim Denetimleri** öğesine tıklayın.
   - **Güvenlik** > **Güvenlik Ayarlarını Düzenle** > **Erişim Denetimleri** öğesine tıklayın.
3. **Aygıt Uygulamaları** veya **Aygıt Çözümleri** öğesine tıklayın ve aşağıdakileri uygulayın:
   - Uygulama 1 veya Çözüm 1'i bir iç hesaba veya LDAP+GSSAPI ya da Active Directory güvenlik şablonuna ayarlayın.
   - Uygulama 2 veya Çözüm 2'yi uygulama güvenlik şablonuna ayarlayın.

     Not: Uygulama güvenlik şablonunda kimlik doğrulama ayarı olarak CardAuth belirlenmiştir. Daha fazla bilgi için bkz. 6. sayfadaki "Güvenlik şablonu oluşturma".
   - Uygulama 3 veya Çözüm 3'ü bir LDAP güvenlik şablonuna ayarlayın.

   Notlar:

   - LPM Baskı Sürümü yüklüyse Baskı Sürümü erişim denetimini uygulama güvenlik şablonuna ayarlayın.
   - Yerleşik Çözümler Çerçevesi (eSF) sürüm 2.x yazıcılarda erişim denetiminin yapılandırılması için eSF Güvenlik Yöneticisi uygulaması gereklidir. Bu yazıcıların listesi için *Benioku* dosyasına bakın.
4. **Gönder** öğesine tıklayın.

Uygulamayı yapılandırma

Başlamadan önce aşağıdakileri yapın:

- Arka Plan ve Boşta Ekranı ve mevcut tüm kimlik doğrulama uygulamalarını devre dışı bırakın.
- Aşağıdakileri yükleyin:
  - Kart Kimlik Doğrulaması yükleyicisi
  - Kartı okuyucu sürücüsü
  - Kart okuyucu
  - eSF Güvenlik Yöneticisi

    Not: eSF sürüm 2.x yazıcılarda erişim denetiminin yapılandırılması için eSF Güvenlik Yöneticisi uygulaması gereklidir. Bu yazıcıların listesi için *Benioku* dosyasına bakın.

Uygulamanın yapılandırma sayfasına erişme

1. Yerleşik Web Sunucusu'ndan sırayla **Ayarlar** veya **Yapılandırma** öğesini tıklatın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Uygulamalar** > **Uygulama Yönetimi** öğesini tıklatın.
   - **Aygıt Çözümleri** > **Çözümler (eSF)** öğesini tıklatın.
   - **Yerleşik Çözümler** öğesini tıklatın.
3. **Kart Kimlik Doğrulaması** > **Yapılandır** öğesini tıklatın.

Yönetici kimlik doğrulamasını yapılandırma

Not: Yönetici Oturum Açma özelliğini kullanırken İç hesaplar, PIN ve Parola için güvenlik şablonunu yapılandırdığınızdan emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Güvenlik şablonu oluşturma".

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Kullanıcı Kimlik Doğrulaması bölümünden **Yönetici Oturum Açma Erişim Denetimi** seçeneğini tercih ettiğiniz oturum açma yöntemine ayarlayın.

   Notlar:

   - Seçilen erişim denetiminin güvenlik şablonuyla yapılandırıldığından emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Güvenlik şablonu oluşturma".
   - **Devre Dışı** öğesinin seçilmesi, **Yönetici Oturum Açma** seçeneğini yazıcı panelinden gizler.
3. **Uygula** öğesine tıklayın.

Oturum açma ekranını yapılandırma

Oturum açma ekranı aşağıdakileri gerçekleştirmek için yapılandırılabilir:

- Kullanıcıların oturum açmadan kopyalama ve faks işlevlerini kullanmasına izin vermek.
- Kullanıcıların kullanılacak oturum açma yöntemini belirlemesine izin vermek.

- Bir oturum açma ekranı arka planı eklemek ve oturum açma mesajını özelleştirmek.
- Kart okuyucu takılı olmadığında uyarma işlevini devre dışı bırakın.

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Oturum Açma Ekranı bölümünden ayarları yapılandırın.

   Not: Her bir ayar hakkında daha fazla bilgi edinmek için fareyi yardım öğesinin üzerine getirin.
3. **Uygula** öğesine tıklayın.

Oturum açmadan kopyalama veya faks işlevlerini etkinleştirme

"Oturum Açmadan Kopyalamaya İzin Ver" veya "Oturum Açmadan Fakslamaya İzin Ver" seçenekleri etkinleştirilmişse aşağıdakileri uygulayın:

1. Embedded Web Server'dan **Ayarlar** veya **Yapılandırma** öğesine tıklayın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Güvenlik** > **Güvenlik Kurulumu** > **Erişim Denetimleri** > **İşlev Erişimi** öğesini tıklatın.
   - **Güvenlik** > **Güvenlik Ayarlarını Düzenle** > **Erişim Denetimleri** öğesine tıklayın.
3. Kopyalama veya faks işlevini **Güvenlik Yok** olarak ayarlayın.
4. **Gönder** öğesine tıklayın.

Yazıcı tabanlı kimlik doğrulaması

Ana yazıcı üzerinden kullanıcıları doğrularken yazıcı tabanlı kimlik doğrulamasını kullanın.

Yazıcı tabanlı kullanıcı kimlik doğrulamasının yapılandırılması

Başlamadan önce, şunlardan emin olun:

- Uygulama 1 veya Çözüm 1 erişim denetimi bir iç hesaba veya LDAP+GSSAPI ya da Active Directory güvenlik şablonuna ayarlanması.
- Uygulama 2 veya Çözüm 2 erişim denetiminin uygulama güvenlik şablonuna ayarlanması.

  Not: Daha fazla bilgi için bkz. 6. sayfadaki "Erişim denetimlerinin yapılandırılması".

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi'ni **Kartla veya Manuel Oturum Açma** olarak ayarlayın.
3. Kullanıcı Kimlik Doğrulaması bölümünden aşağıdakileri uygulayın:
   - Kart Doğrulaması'nı **Yazıcı Tabanlı** olarak ayarlayın.
   - Kart Kaydı Erişim Denetimi'ni **Uygulama 1** veya **Çözüm 1** olarak ayarlayın.
   - Manuel Oturum Açma Erişim Denetimi'ni **Uygulama 1** veya **Çözüm 1** olarak ayarlayın.
   - Oturum Erişim Denetimi'ni **Uygulama 2** veya **Çözüm 2** olarak ayarlayın.

   Notlar:

   - Kart Kaydı Erişim Denetimi **Yok** olarak ayarlanmışsa kartınızı yazıcıya kaydedemezsiniz.

- Manuel Oturum Açma Erişim Denetimi'nin **Yok** olarak ayarlanması, Oturum Açma Yöntemi **Kartla veya Manuel Oturum Açma** olarak ayarlanmışsa bile yalnızca bir kartın oturum açmasını gerektirir.
- Her ayar hakkında daha fazla bilgi için, fareyi ayarın yanındaki yardım içeriğinin üzerine getirin.

4 **Uygula** öğesini tıklatın.

Yazıcı rolünü ayarlama

Not: İstemci yazıcı için ana yazıcı ve yedek yazıcı gerekir.

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 Yazıcı Tabanlı Kart Doğrulaması bölümünden, yazıcı rolünü seçin.

- **Ana Yazıcı**: Bu yazıcı, kayıtlı kullanıcıların listesini tutar.
- **Yedek Yazıcı**: Ana yazıcı çevrimdışı olduğunda ana yazıcı çevrimiçi olana kadar yedek yazıcı, ana yazıcının rolünü üstlenir.
- **İstemci Yazıcı**: Bu yazıcıda kullanıcı bilgileri depolanmaz. Kullanıcı kimlik bilgilerinin doğrulanması için bir ana veya yedek yazıcı gerekir.

Notlar:

- Tek bir yazıcınız varsa bu yazıcıyı ana yazıcı olarak ayarlayın.
- İki yazıcınız varsa birini ana yazıcı; diğerini ise yedek yazıcı olarak ayarlayın.
- Üç veya daha fazla yazıcınız varsa birini ana yazıcı, birini yedek yazıcı ve geri kalanları ise istemci yazıcılar olarak ayarlayın.

3 Ana yazıcı ve yedek yazıcının ana bilgisayar adını veya IP adresini girin.

Notlar:

- Yedek yazıcı kurulumu sırasında ana yazıcı ana bilgisayar adı veya IP adresi gerekir.
- İstemci yazıcıların kurulumu sırasında ana ve yedek yazıcıların ana bilgisayar adları veya IP adresleri gerekir.
- Yeni bir ana yazıcıya istemci bir yazıcı atamadan önce istemci yazıcıyı eski ana yazıcıdan silin.

4 **Uygula** öğesini tıklatın.

Web hizmeti kimlik doğrulaması

LDD sunucusu üzerinden kullanıcıları doğrularken web hizmeti kimlik doğrulamasını kullanın.

Web hizmeti kullanıcı kimlik doğrulamasının yapılandırılması

Başlamadan önce Uygulama 2 veya Çözüm 2 erişim denetiminin uygulama güvenlik şablonuna ayarlandığından emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Erişim denetimlerinin yapılandırılması".

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi öğesini **Kartla veya Manuel Oturum Açma** olarak ayarlayın.

3 Kullanıcı Kimlik Doğrulaması bölümünden aşağıdakileri yapın:
   - Kart Doğrulaması öğesini **Web Hizmeti** olarak ayarlayın.
   - Kart Kaydı Erişim Denetimi ve Manuel Oturum Açma Erişim Denetimi öğesini tercih ettiğiniz erişim denetimine ayarlayın.
   - Oturum Erişim Denetimi öğesini **Uygulama 2** veya **Çözüm 2** olarak ayarlayın.

   Notlar:

   - Kart Kaydı Erişim Denetimi **Yok** olarak ayarlanmışsa kartınızı yazıcıya kaydedemezsiniz.
   - Manuel Oturum Açma Erişim Denetimi öğesinin **Yok** olarak ayarlanması, Oturum Açma Yöntemi **Kartla veya Manuel Oturum Açma** olarak ayarlanmışsa bile yalnızca bir kartın oturum açmasını gerektirir.
   - Her bir ayar hakkında daha fazla bilgi edinmek için fareyi yardım öğesinin üzerine getirin.

4 Sunucuya yapılan tüm bağlantıları doğrulamak için **Sertifikayı Doğrula** öğesini seçin. Sertifikayı Doğrula öğesi seçilmezse CA doğrulanmaz.

   Not: Sertifikayı Doğrula ayarı yalnızca Kimlik Hizmeti ve Web Hizmeti doğrulaması için geçerlidir.

5 Doğrulama Modu menüsünde **zincir** veya **eşler arası** öğesini seçin.

   Not: Varsayılan değer zincir'dir.

6 Sunucuya güvenli bir şekilde bağlanmak için sunucu SSL sertifikası öğesini yükleyin.

7 KontrolAnaBilgisayarları alanında, sertifikadaki girişleri doğrulamak için ek ana bilgisayar adlarını (varsayılan sunucu URL'si dışında) yazın. Birden fazla ana bilgisayar adını ayırmak için virgül kullanın.

   Not: İlgili beyaz liste varsayılan olarak sadece sunucu URL'sini içerir. Beyaz listeye eklemek üzere KontrolAnaBilgisayarları alanına ek ana bilgisayar adlarını yazın.

8 **Uygula** öğesine tıklayın.

Web hizmeti ayarlarının yapılandırılması

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 Web Hizmeti Ayarları bölümünden ayarları yapılandırın.

   Not: Her bir ayar hakkında daha fazla bilgi edinmek için fareyi yardım öğesinin üzerine getirin.

3 **Uygula** öğesini tıklatın.

Kimlik Hizmeti kimlik doğrulaması

Hizmet Olarak LPM Yazılımı (SaaS) sunucusu gibi bir Kimlik Hizmeti sunucusu üzerinden kullanıcıları doğrularken Kimlik Hizmeti kimlik doğrulamasını kullanın.

Kimlik Hizmeti kullanıcı kimlik doğrulamasının yapılandırılması

Başlamadan önce Uygulama 2 veya Çözüm 2 erişim denetiminin uygulama güvenlik şablonuna ayarlandığından emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Erişim denetimlerinin yapılandırılması".

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi öğesini **Kartla veya Manuel Oturum Açma** olarak ayarlayın.
3. Kullanıcı Kimlik Doğrulaması bölümünden aşağıdakileri yapın:
   - Kart Doğrulaması öğesini **Kimlik Hizmeti** olarak ayarlayın.
   - Kart Kaydı Erişim Denetimi öğesini **Kimlik Hizmeti** olarak ayarlayın.
   - Manuel Oturum Açma Erişim Denetimi öğesini **Kimlik Hizmeti** olarak ayarlayın.
   - Oturum Erişim Denetimi öğesini **Uygulama 2** veya **Çözüm 2** olarak ayarlayın.

   Notlar:

   - Kart Kaydı Erişim Denetimi **Yok** olarak ayarlanmışsa kartınızı yazıcıya kaydedemezsiniz.
   - Manuel Oturum Açma Erişim Denetimi öğesinin **Yok** olarak ayarlanması, Oturum Açma Yöntemi **Kartla veya Manuel Oturum Açma** olarak ayarlanmışsa bile yalnızca bir kartın oturum açmasını gerektirir.
   - Her bir ayar hakkında daha fazla bilgi edinmek için fareyi yardım öğesinin üzerine getirin.
4. Sunucuya yapılan tüm bağlantıları doğrulamak için **Sertifikayı Doğrula** öğesini seçin. Sertifikayı Doğrula öğesi seçilmezse CA doğrulanmaz.

   Not: Sertifikayı Doğrula ayarı yalnızca Kimlik Hizmeti ve Web Hizmeti doğrulaması için geçerlidir.
5. Doğrulama Modu menüsünde **zincir** veya **eşler arası** öğesini seçin.

   Not: Varsayılan değer zincir'dir.
6. Sunucuya güvenli bir şekilde bağlanmak için sunucu SSL sertifikası öğesini yükleyin.
7. KontrolAnaBilgisayarları alanında, sertifikadaki girişleri doğrulamak için ek ana bilgisayar adlarını (varsayılan sunucu URL'si dışında) yazın. Birden fazla ana bilgisayar adını ayırmak için virgül kullanın.

   Not: İlgili beyaz liste varsayılan olarak sadece sunucu URL'sini içerir. Beyaz listeye eklemek üzere KontrolAnaBilgisayarları alanına ek ana bilgisayar adlarını yazın.
8. **Uygula** öğesine tıklayın.

Kimlik Hizmeti ayarlarının yapılandırılması

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Gerekirse Kimlik Hizmeti Ayarları bölümünden **Boşta Ekranı Etkinleştir** seçeneğini belirleyin.

   Not: Boşta Ekranı Etkinleştir seçeneği devre dışı bırakıldığında eSF sürüm 2.x yazıcılar için eSF Güvenlik Yöneticisi gerekir. Bu yazıcıların listesi için *Benioku* dosyasına bakın.

3 Kimlik Hizmeti Sağlayıcısı'nın ana bilgisayar adını veya IP adresini yazın.

4 Gerekirse Rozet Servis Sağlayıcısı'nın ana bilgisayar adını veya IP adresini yazın.

5 Sunucuya güvenli bir şekilde bağlanmak için sunucu SSL sertifikasını yükleyin.

6 Kimlik Hizmeti Sağlayıcısı'ndan aldığınız bir İstemci Kimliği ve İstemci Sırrı varsa ilgili alanlara bilgileri girin.

7 Uygulama erişim ilkesini belirleyin.
- **Devam**: Kimlik Hizmeti sunucusuna bağlanma işlemi başarısız olsa bile yazıcıyı kullanmaya devam eder.
- **Başarısız**: Kimlik Hizmeti sunucusuna bağlanma işlemi başarısız olursa oturum açma ekranına geri döner.

8 Kullanıcıların farklı bir hizmet hesabı kullanarak yazıcıda oturum açmalarına izin vermek için **Hizmet Hesabını Kullan** öğesini seçin ve hizmet hesabı kimlik bilgilerini girin.

9 **Uygula** öğesini tıklatın.

PIN kimlik doğrulaması

PIN kullanıcı kimlik doğrulamasının yapılandırılması

Başlamadan önce Uygulama 2 veya Çözüm 2 erişim denetiminin uygulama güvenlik şablonuna ayarlandığından emin olun. Daha fazla bilgi için bkz. 6. sayfadaki "Erişim denetimlerinin yapılandırılması".

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi'ni PIN'le kimlik doğrulamayı destekleyen bir seçeneğe ayarlayın.

3 Kullanıcı Kimlik Doğrulaması bölümünden aşağıdakileri uygulayın:
- Kart Doğrulaması'nı tercih ettiğiniz kimlik doğrulama yöntemine ayarlayın.
- Kart Kaydı Erişim Denetimi'ni tercih ettiğiniz erişim denetimine ayarlayın.
- PIN Erişim Denetimi'ni **Uygulama 1** veya **Çözüm 1** olarak ayarlayın.
- Manuel Oturum Açma Erişim Denetimi'ni tercih ettiğiniz erişim denetimine ayarlayın.
- Oturum Erişim Denetimi'ni **Uygulama 2** veya **Çözüm 2** olarak ayarlayın.

Notlar:

- PIN Erişim Denetimi **Yok** olarak ayarlanmışsa PIN'inizi yazıcıya kaydedemezsiniz.
- Her ayar hakkında daha fazla bilgi için, fareyi ayarın yanındaki yardım içeriğinin üzerine getirin.

4 **Uygula** öğesini tıklatın.

PIN ayarlarının yapılandırılması

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 PIN Ayarları bölümünde Gerekli Kimlik Bilgileri menüsünden bir oturum açma yöntemi seçin.
- Kullanıcı Kimliği ve PIN: Kimlik doğrulama için bir kullanıcı adı ve PIN gerektirir.
- Yalnızca PIN: Kimlik doğrulama için bir PIN gerektirir.

3 Web sunucusu adresini girin ve minimum PIN uzunluğunu belirleyin.

4 Geçersiz PIN hata mesajlarını girin.

5 **Uygula** öğesine tıklayın.

LDAP kimlik doğrulaması

LDAP sunucusu üzerinden kullanıcıları doğrularken LDAP kimlik doğrulamasını kullanın.

LDAP kullanıcı kimlik doğrulamasının yapılandırılması

Başlamadan önce, şunlardan emin olun:

- Uygulama 2 veya Çözüm 2 erişim denetiminin uygulama güvenlik şablonuna ayarlanması.
- Uygulama 3 veya Çözüm 3 erişim denetiminin LDAP güvenlik şablonuna ayarlanması.

  Not: Daha fazla bilgi için bkz. 6. sayfadaki "Erişim denetimlerinin yapılandırılması".

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi'ni **Kartla veya Manuel Oturum Açma** olarak ayarlayın.

3 Kullanıcı Kimlik Doğrulaması bölümünden aşağıdakileri uygulayın:
   - Kart Doğrulaması'nı **LDAP** olarak ayarlayın.
   - Kart Kaydı Erişim Denetimi'ni **Uygulama 3** veya **Çözüm 3** olarak ayarlayın.
   - Manuel Oturum Açma Erişim Denetimi'ni **Uygulama 3** veya **Çözüm 3** olarak ayarlayın.
   - Oturum Erişim Denetimi'ni **Uygulama 2** veya **Çözüm 2** olarak ayarlayın.

   Notlar:

   - Kart Kaydı Erişim Denetimi **Yok** olarak ayarlanmışsa kartınızı yazıcıya kaydedemezsiniz.
   - Manuel Oturum Açma Erişim Denetimi'nin **Yok** olarak ayarlanması, Oturum Açma Yöntemi **Kartla veya Manuel Oturum Açma** olarak ayarlanmışsa bile yalnızca bir kartın oturum açmasını gerektirir.
   - Her ayar hakkında daha fazla bilgi için, fareyi ayarın yanındaki yardım içeriğinin üzerine getirin.

4 **Uygula** öğesini tıklatın.

LDAP ayarlarının yapılandırılması

1 Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.

2 LDAP Ayarları bölümünden ayarları yapılandırın.

   Notlar:

   - **Adres Defterini Kullan** seçeneği belirlendiyse uygulama, yazıcı ağ hesaplarında daha önceden yapılandırılmış olan LDAP ayarlarını kullanır.
   - Her ayar hakkında daha fazla bilgi için, fareyi ayarın yanındaki yardım içeriğinin üzerine getirin.

3 **Uygula** öğesini tıklatın.

Uygulama tercihlerini ayarlama

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Aşağıdakilerden birini veya daha fazlasını uygulayın:
   - Yazıcı ana ekranını özelleştirmek için ana ekran ayarlarını yapılandırın.
   - Kayıt mesajlarını görüntülemek için Gelişmiş Ayarlar bölümünden **Kayıt Giriş Mesajını Göster** ve **Kayıt Bitirme Mesajını Göster** öğelerini seçin.
   - Başarılı bir şekilde oturum açtıktan sonra bir *uyarı sesi* duymak için Gelişmiş Ayarlar bölümünden **Başarılı Oturum Açma Uyarı Sesini Etkinleştir** öğesini seçin ve uyarı sesi sıklığını ayarlayın.
   - Başarılı bir şekilde oturum açtıktan sonra bir profil kullanmak için Gelişmiş Ayarlar bölümünden Oturum Açma Profili alanına bir profil adı girin.

   Not: Her ayar hakkında daha fazla bilgi için, fareyi ayarın yanındaki yardım içeriğinin üzerine getirin.
3. **Uygula** öğesini tıklatın.

Mevcut profilleri görüntüleme

1. Yerleşik Web Sunucusu'ndan sırayla **Ayarlar** veya **Yapılandırma** öğesini tıklatın.
2. **Kısayolları Yönet** > **Profil Kısayollarını Yönet** öğesini tıklatın.

Kullanıcı hesapları için alanları görüntüleme

Seçili Alanı Kullan özelliği sadece kart kaydı ve manuel oturum açma için oturum açma yöntemi olarak Kerberos, Active Directory veya LDAP+GSSAPI kullanıldığında geçerlidir. Kart doğrulaması, Web Hizmeti veya Yazıcı Tabanlı olarak ayarlandığında da bu özellik kullanılabilir.

Bu özellik etkinleştirilmişse kart kaydı için kaydedilen işaret kodu username@realm şeklindedir.

Bu özellik etkinleştirilmişse manuel oturum açma için yazıcı kontrol panelinde görüntülenen kullanıcı adı username@realm şeklindedir.

Bu ayarla, PIN'le oturum açma ve PIN'le kayıt için geçerli değildir.

Bu özelliği etkinleştirmek için aşağıdakileri uygulayın:

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Gelişmiş Ayarlar bölümünden **Seçili Alanı Kullan** seçeneğini belirleyin.
3. **Uygula** öğesini tıklatın.

Yapılandırma dosyasını içe veya dışa aktarma

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Yapılandırma dosyasını içe veya dışa aktarın.

Notlar:

- **JVM Bellek Dolu** hatası oluşursa, yapılandırma dosyası kaydedilene kadar gönderme işlemini tekrar edin.

- Zaman aşımı oluşursa ve boş bir ekran belirirse web tarayıcısını yenileyin ve ardından **Uygula** öğesini tıklatın.

Uygulamayı yönetme

Not: Uygulamanın durum sayfası yalnızca yazıcı tabanlı kimlik doğrulamasından yararlanılırken kullanılabilir.

Uygulamanın durum sayfasına erişme

Yazıcı etkinliklerini izlemek için durum sayfasını kullanın.

1. Embedded Web Server'dan **Uygulamalar** > **Kart Kimlik Doğrulaması** öğesini tıklatın.
2. Aşağıdaki bilgileri not edin:
   - **Durum**: Yazıcının etkinlik durumunu görüntüler.
     - **Yapılandırılmadı**: Yazıcı yapılandırılmamıştır.
     - **Çevrimdışı**: Hiçbir yazıcı etkinliği veya iletişimi gerçekleştirilmemiştir.
     - **Çevrimiçi**: Yazıcı etkindir.
   - **Çalışma Süresi**: Uygulamanın çalışma süresini gösterir.
   - **(bu yazıcı)**: Geçerli yazıcıdır.
   - **Son Etkinlik**: Ana yazıcının son etkinliğidir.
   - **Kullanıcı Sayısı**: Kayıtlı toplam kullanıcı sayısıdır.
   - **Kayıt Durumu**: Yazıcının çevrimdışı veya çevrimiçi olduğunu belirtir.
   - **Ana Yazıcı ile Son Senkronizasyon**: Yedek yazıcının ana yazıcı ile en son güncellendiği saattir.
   - **Ana Yazıcı ile Son İletişim**: Yedek yazıcının ana yazıcı ile en son iletişime geçtiği saattir.
   - **Ana Yazıcı ile Son Senkronizasyon**: Yedek yazıcının en son ana yazıcı olarak kullanıldığı saattir.
   - **Ana Yazıcı olarak Son Etkinlik**: Yedek yazıcının en son ana yazıcı olarak kullanıldığı etkinliktir.
   - **Ana Yazıcı olarak Süre**: Yedek yazıcının ana yazıcı olarak kullanıldığı süreyi gösterir.
   - **Geçerli Olarak Servis Veren**: Ana veya yedek yazıcı ile yakın zamanda iletişim kuran istemci yazıcıdır.
   - **Yedek Yazıcı ile Son Etkinlik**: İstemci yazıcının yedek yazıcı ile en son iletişime geçtiği saattir.

Kullanıcı hesaplarını ve istemci yazıcıları yönetme

Not: Bu özellik yalnızca yazıcı, ana yazıcı olarak işlev gördüğünde görüntülenir.

1. Embedded Web Server'dan uygulamanın durum sayfasına erişin.
2. Aşağıdakilerden herhangi birini yapın:

Kullanıcı hesaplarını silme

a. Ana Yazıcı bölümünden **Kullanıcıları Sil** öğesini tıklatın.

b. Bir veya daha fazla kullanıcı kimliği yazın ve bunları silin.

İstemci yazıcı ekleme

a. İstemciler bölümünden **İstemci Ekle** öğesini tıklatın.

b. Bir veya daha fazla yazıcı IP adresi yazın ve bunları ekleyin.

İstemci yazıcıları silme

Not: Ana bilgisayar çevrimdışı ise veya uygulama kaldırılmışsa istemci yazıcıları silemezsiniz.

a İstemciler bölümünden bir veya daha fazla istemci yazıcı seçin.

b **İstemcileri Sil** öğesini tıklatın.

Yazıcı rollerini yeniden atama

1 Yeni bir ana yazıcı yapılandırın.

a Yeni ana yazıcının Embedded Web Server'ından uygulamanın yapılandırma sayfasına erişin.

b Yazıcı Tabanlı Kart Doğrulaması bölümünden Rolü **Ana Yazıcı** olarak ayarlayın.

c Yedek yazıcının ana bilgisayar adını veya IP adresini yazın.

d **Uygula** öğesini tıklatın.

2 Yedek yazıcıyı yeni ana yazıcıya atayın.

a Yedek yazıcının Embedded Web Server'ından uygulamanın yapılandırma sayfasına erişin.

b Yazıcı Tabanlı Kart Doğrulaması bölümüne, yeni ana yazıcının ana bilgisayar adını veya IP adresini girin.

c **Uygula** öğesini tıklatın.

3 Geçerli ana yazıcıdan istemci yazıcıyı silin.

a Geçerli ana yazıcının Embedded Web Server'ından uygulamanın durum sayfasına erişin.

b İstemciler bölümünden istemci yazıcıyı silin.

4 İstemci yazıcıyı yeni ana yazıcıya yeniden atayın. Aşağıdakilerden birini yapın:

Uygulamanın yapılandırma sayfasını kullanma

a İstemci yazıcının Embedded Web Server'ından uygulamanın yapılandırma sayfasına erişin.

b Yazıcı Tabanlı Kart Doğrulaması bölümünden Rolü **İstemci** olarak ayarlayın.

c Yeni ana yazıcının ana bilgisayar adını veya IP adresini yazın.

Not: Yedek yazıcının ana bilgisayar adının veya IP adresinin doğru olduğundan emin olun.

d **Uygula** öğesini tıklatın.

Ana yazıcı durum sayfasını kullanma

a Yeni ana yazıcının Embedded Web Server'ından uygulamanın durum sayfasına erişin.

b İstemciler bölümünden **İstemci Ekle** öğesini tıklatın.

c İstemci yazıcının IP adresini yazıp yazıcıyı ekleyin.

Uygulamayı kullanma

Kullanıcıları kaydetme

1. Kartınızı kart okuyucuya dokundurun.
2. Yazıcı kontrol paneline kimlik bilgilerinizi girin.

   Not: Kart kaydı için Kerberos, Active Directory veya LDAP+GSSAPI kullanıyorsanız bir alan belirleyin.
3. Ekrandaki yönergeleri izleyin.

PIN kaydetme

Başlamadan önce oturum açma yönteminin, PIN kimlik doğrulamasını destekleyecek şekilde ayarlandığından emin olun.

1. Yazıcı kontrol panelinden **PIN'le Oturum Açma** öğesine dokunun.
2. Ekrandaki yönergeleri izleyin.

Yazıcıda manuel olarak oturum açma

1. Yazıcı kontrol panelinden aşağıdakilerden birine dokunun:
   - **PIN'le Oturum Açma**
   - **Manuel Oturum Açma**
   - **Yönetici Oturum Açma**

   Not: Yönetici Oturum Açma öğesini seçerken LDAP sunucusundan diğer kullanıcı bilgilerinin alınması mümkün olmaz.
2. Oturum açma bilgilerinizi girin.

   Not: Manuel oturum açma için Kerberos, Active Directory®veya LDAP+GSSAPI kullanıyorsanız bir alan belirleyin.
3. Ekrandaki talimatları izleyin.

Sorun Giderme

Uygulama hatası

Aşağıdakilerden birini veya daha fazlasını deneyin:

Sistem günlüğünü denetleyin

1. Yerleşik Web Sunucusu'ndan sırayla **Ayarlar** veya **Yapılandırma** öğesini tıklatın.
2. Yazıcı modelinize bağlı olarak aşağıdakilerden birini yapın:
   - **Uygulamalar** > **Uygulama Yönetimi** öğesini tıklatın.
   - **Aygıt Çözümleri** > **Çözümler (eSF)** öğesini tıklatın.
   - **Yerleşik Çözümler** öğesini tıklatın.
3. **Sistem** > **Günlük** öğesini tıklatın.
4. Uygun filtreleri seçin ve gönderin.
5. Günlüğü analiz edin ve sorunu çözün.

Lexmark temsilcinizle iletişime geçin

Uygulama, SaaS Baskı Sürümü'nün güncel sürümüyle çalışmıyor

Aşağıdakilerden birini veya daha fazlasını deneyin:

Baskı Sürümü'nün düzgün yapılandırıldığından emin olun

Yazdırma Yönetimi SaaS uygulamanızı Baskı Sürümü v2.0'a veya daha sonraki bir sürüme yükselttiyseniz Arka Plan ve Boşta Ekranı'nın devre dışı bırakıldığından emin olun. Baskı Sürümü'ne Kart Kimlik Doğrulaması erişimini atayın ve Baskı Sürümü'nün düzgün bir şekilde yapılandırıldığından emin olun. Daha fazla bilgi için *Baskı Sürümü Yönetici Kılavuzu*'na bakın.

Lexmark temsilcinizle iletişime geçin

Kimlik doğrulaması hatası

Aşağıdakilerden birini veya daha fazlasını deneyin:

Yazıcı zaman aşım süresini artırın

Kart doğrulama yöntemi olarak Kimlik Hizmeti kullanıyorsanız yazıcının Kimlik Hizmeti Sağlayıcısı'yla iletişime geçmesi için daha fazla zaman gerekebilir.

1. Yerleşik Web Sunucusu'ndan sırayla **Ayarlar** veya **Yapılandırma** öğesini tıklatın.
2. **Genel Ayarlar** > **Zaman Aşımları** öğesini tıklatın.
3. Ekran zaman aşımını ve uyku modunu artırın.
4. **İlet** düğmesini tıklatın.

Yazıcının ağa bağlı olduğundan emin olun

Daha fazla bilgi için yazıcının *Kullanıcı Kılavuzu*'na bakın.

Güvenlik sunucusunun çevrimiçi olduğundan ve meşgul olmadığından emin olun

Daha fazla bilgi için sistem yöneticinize başvurun.

Kullanıcının bağlantısı kilitli

Kullanıcı izin verilen oturum açma hatası sayısına erişmiş olabilir.

Kilitlenme süresini ve izin verilen oturum açma hatası sayısını artırın

1. Yazıcı modelinize bağlı olarak Embedded Web Server'dan aşağıdakilerden birini gerçekleştirin:
   - **Ayarlar** > **Güvenlik** > **Muhtelif Güvenlik Ayarları** > **Oturum Açma Sınırlamaları** öğelerini tıklatın.
   - **Yapılandırma** > **Güvenlik** öğesini tıklatın.
2. Kilitlenme süresini ve izin verilen oturum açma hatası sayısını veya otomatik olarak oturumu kapatma gecikme süresini artırın.
3. **İlet** düğmesini tıklatın.

İstemci yazıcı kaydedilemiyor

Aşağıdakilerden birini veya daha fazlasını deneyin:

Ana yazıcı veya yedek yazıcının çevrimiçi olduğundan emin olun

Daha fazla bilgi için bkz. 16. sayfadaki "Uygulamanın durum sayfasına erişme".

Ana yazıcı ve yedek yazıcının düzgün bir şekilde yapılandırıldığından emin olun

Daha fazla bilgi için bkz. 8. sayfadaki "Yazıcı tabanlı kullanıcı kimlik doğrulamasının yapılandırılması".

Kayıtlı 23 istemci yazıcı sayısını aşmadığınızdan emin olun

Daha fazla bilgi için bkz. 16. sayfadaki "Kullanıcı hesaplarını ve istemci yazıcıları yönetme".

Lexmark temsilcinizle iletişime geçin

Kart doğrulanamıyor

Aşağıdakilerden birini veya daha fazlasını deneyin:

Oturum Açma Yöntemi'ni Kartla veya Manuel Oturum Açma olarak ayarlayın

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Oturum Açma Ekranı bölümünden Oturum Açma Yöntemi'ni **Kartla veya Manuel Oturum Açma** olarak ayarlayın.
3. **Uygula** öğesini tıklatın.

Lexmark temsilcinizle iletişime geçin

Alan bilgisi bulunamıyor

Aşağıdakilerden birini veya daha fazlasını deneyin:

Manuel oturum açma veya kart kaydı için yerel hesaplar ya da LDAP gibi bazı oturum açma yöntemleri alan seçimi gerektirmez. Kerberos, Active Directory ve LDAP+GSSAPI, alan seçimi gerektiren oturum açma yöntemleridir.

Alan seçimini devre dışı bırakma

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Gelişmiş Ayarlar bölümünden **Seçili Alanı Kullan** seçeneğinin işaretini kaldırın.
3. **Uygula** öğesini tıklatın.

Oturum açma yöntemini değiştirme

1. Embedded Web Server'dan uygulamanın yapılandırma sayfasına erişin.
2. Kullanıcı Kimliği Doğrulama bölümünden Kart Kaydı Erişim Denetimi'ni ve Manuel Oturum Açma Erişim Denetimi'ni **Uygulama 1** veya **Çözüm 1** olarak ayarlayın.
3. **Uygula** öğesini tıklatın.

Lexmark temsilcinizle iletişime geçin

LDAP sunucusuna bağlanılamıyor

Aşağıdakilerden birini veya daha fazlasını deneyin:

LDAP ayarlarının düzgün yapılandırıldığından emin olun

Daha fazla bilgi için bkz. 13. sayfadaki "LDAP ayarlarının yapılandırılması".

Lexmark temsilcinizle iletişime geçin

Sık sorulan sorular

Neden yedek yazıcı ana yazıcı olarak işlev görürken bir istemci yazıcı ekleyemiyor veya silemiyorum?

Yalnızca ana yazıcı çevrimiçi iken istemci yazıcıyı silebilir veya ekleyebilirsiniz.

Geçerli ana yazıcı çevrimdışı olsa bile bir istemci yazıcıyı kaldırıp yeni ana yazıcıya yeniden atayabilir miyim?

Evet, aşağıdakileri uygulayın:

1. İstemci yazıcının Embedded Web Server'ından uygulamayı yükleyin.
2. Rolü, istemci yazıcı olarak ayarlayıp yeni ana ve yedek yazıcılar için yapılandırın. Daha fazla bilgi için bkz. 9. sayfadaki "Yazıcı rolünü ayarlama".

Uygulamayı yanlışlıkla yazıcıdan kaldırırsam ne yapmam gerekir?

1. Embedded Web Server'dan uygulamayı yükleyin.
2. Yazıcının rolünü ayarlayın. Daha fazla bilgi için bkz. 9. sayfadaki "Yazıcı rolünü ayarlama".

   Not: Sırasıyla ana yazıcının, ardından yedek yazıcının ve daha sonra istemci yazıcıların kurulduğundan emin olun.
3. Role bağlı olarak yazıcıyı yapılandırın.

   Notlar:

   - Uygulama bir ana yazıcıya yeniden yüklendiyse uygulamayı yedek yazıcıya atayın.
   - Uygulama bir yedek yazıcıya yeniden yüklendiyse uygulamayı ana yazıcıya atayın.
   - Uygulama bir istemci yazıcıya yeniden yüklendiyse uygulamayı kendi ana yazıcısına ve yedek yazıcısına atayın.
   - Daha fazla bilgi için bkz. 17. sayfadaki "Yazıcı rollerini yeniden atama".

Oturum açmadan etkinleştirmeme rağmen neden kilit ekranında kopyalama veya faks düğmesini göremiyorum?

Kopyalama veya faks işlev erişim denetimini **Güvenlik Yok** olarak ayarlayın. Daha fazla bilgi için bkz. 7. sayfadaki "Oturum açma ekranını yapılandırma".

Manuel Oturum Açma Erişim Denetimi ve Oturum Erişim Denetimi için erişim denetimlerim aynıysa ne olur?

Ana ekrandan yazıcı işlevlerine erişmek için manuel olarak oturum açtığınızda kimlik bilgilerinizi girmeniz gerekir.

Manuel Oturum Açma Erişim Denetimi ve Kart Doğrulaması için erişim denetimlerim farklı olabilir mi?

Kimlik Hizmeti kimlik doğrulamasını kullanmıyorsanız evet. Kullanıyorsanız Manuel Oturum Açma Erişim Denetimi ve Kart Doğrulaması'nı **Kimlik Hizmeti** olarak ayarlayın.

Yönetici Oturum Açma özelliği, neden ağ hesaplarında çalışmaz?

Yönetici Oturum Açma özelliği yalnızca İç Hesaplar, PIN ve Parola güvenlik şablonlarıyla kullanılabilir.

Bildirimler

Sürüm bildirimi

Aralık 2020

Aşağıdaki paragraf bu tür şartların yasalara aykırı olduğu ülkeler için geçersizdir. LEXMARK INTERNATIONAL, INC. BU YAYINI, “OLDUĞU GİBİ”, TİCARİ YA DA BELİRLİ BİR AMACA UYGUNLUK GİBİ HERHANGİ BİR KONUDA DOLAYLI VEYA DOĞRUDAN GARANTİ VERMEKSİZİN SAĞLAMAKTADIR. Bazı ülkelerde, belirli konularda dolaylı ya da doğrudan garantilerin reddedilmesine izin verilmez; bu nedenle, bu bildirim sizin için geçerli olmayabilir.

Bu yayın, teknik yanlışlıklar ya da yazım hataları içerebilir. Bu yayında açıklanan bilgilerde düzenli olarak değişiklik yapılmaktadır; bu değişiklikler sonraki basımlara yansıtılacaktır. Hakkında bilgi verilen ürünler ya da programlar üzerinde herhangi bir zamanda geliştirme çalışmaları ya da değişiklikler yapılabilir.

Bu yayında belirli ürünlerden, programlardan ya da hizmetlerden söz edilmesi, bu ürünlerin, programların ya da hizmetlerin sizin ülkenizde de kullanıma sunulacağı anlamına gelmez. Herhangi bir ürün, program ya da hizmetten söz edilmesi, yalnızca o ürünün, programın ya da hizmetin kullanılabileceği anlamına gelmez. Geçerli fikri mülkiyet haklarına aykırı olmayan ve işlevsel olarak eşit herhangi bir ürün, program ya da hizmet kullanılabilir. Üretici tarafından açıkça belirtilenler dışında, diğer ürünlerle, programlarla ya da hizmetlerle birlikte kullanım olanaklarının değerlendirilmesi ve doğrulanması kullanıcının sorumluluğundadır.

Lexmark teknik desteği için şu adrese gidin: **http://support.lexmark.com**.

Lexmark'ın bu ürünün kullanımına ilişkin gizlilik ilkesi hakkında bilgi almak için **www.lexmark.com/privacy** adresine gidin.

Sarf malzemeleri ve indirmeler hakkında bilgi almak için **www.lexmark.com** adresine gidin.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Ticari Markalar

Lexmark ve Lexmark logosu, Lexmark International, Inc.ın ABD ve/veya diğer ülkelerde ticari markaları veya tescilli ticari markalardır.

Diğer tüm ticari markalar kendi sahiplerine aittir.

Dizin

U

W

Y