

Sürüm 1.0  
Ocak, 2011



# Xerox® Phaser™ 3635MFP Extensible Interface Platform



©2011 Xerox Corporation. XEROX® ve XEROX and Design®, Xerox Corporation'ın Amerika Birleşik Devletleri'nde ve/veya diğer ülkelerde ticari markasıdır.

Bu dokümanda düzenli aralıklarla değişiklikler yapılmaktadır. Değişiklikler, teknik hatalar ve dizgi hataları sonraki baskılarda düzeltilecektir.

Doküman Sürümü 1.0: Ocak, 2011

Çeviren:

Xerox  
CTC European Operations  
Bessemer Road  
Welwyn Garden City  
Hertfordshire  
AL7 1BU  
İngiltere

# İçindekiler

Giriş .....	4
EIP Kullanmanın Son Kullanıcıya Sağladığı Avantajlar.....	4
EIP'nin neleri sağlayabileceğine ilişkin örnekler .....	4
Daha Basit İşlemler .....	5
Kişisel Çözümler .....	5
XEIP'yi Yapılandırma .....	6
Bilgi Kontrol Listesi .....	6
Özel Hizmetleri Etkinleştirme .....	6
Makine Dijital Sertifika Yönetimi .....	7
Secure HTTP (SSL) Protokolünü Etkinleştirme .....	8
Proxy Sunucusu .....	9

# Giriş

Xerox Extensible Interface Platform (EIP), Xerox aygıtına pek çok yeni olanak sağlar. EIP ile, artık siz Xerox aygıtınıza değil Xerox aygıtınız sizin çalışma tarzınıza uyum sağlayacak.

- **Son Kullanıcılar** kolayca bilgi paylaşabilir, saklayabilir ve yazdırabilir
- **BT** müşterileri için artı değer ve bilgi güvenliği sağlayabilir
- **Geliştiriciler** çabucak ve kolayca aygıtın kullanıcı arabirimi için özelleştirilebilen uygulamalar geliştirebilir

Satın alınıp aygıtınıza kurulabilecek birkaç isteğe bağlı yazılım çözümü bulunmaktadır. EIP, aygıtınızı kendi iş akışı süreçlerinize göre özelleştirmenizi sağlar. Xerox EIP (Extensible Interface Platform), yazılım satıcılarının ve ortaklarının, doğrudan aygıtın kullanıcı arabiriminden erişilebilecek sunucu tabanlı uygulamalar oluşturmak için standart Web tabanlı araçlar kullanarak özel programlar geliştirmesini sağlar.

## EIP Kullanmanın Son Kullanıcıya Sağladığı Avantajlar

- Karmaşık iş akışlarını **basitleştirerek** aygıtın kullanımını kolaylaştırın.
- Basılı dokümanları dijital bilgi biçimine **dönüştürerek** bilgi düzenlemeyi, saklamayı ve paylaşmayı kolaylaştırın.
- Siz aygıtınıza değil, aygıtınız size ve çalışma alışkanlıklarınıza **uyum sağlasın**.
- Bilgisayar kullanmadan ağdan doküman alma gibi bazı işlerin tamamını aygıtta **tamamlayın**.
- Müşterilerinize daha hızlı **hizmet** sağlayın.
- Çözümleri mevcut BT altyapınızla **bütünleştirin**.
- Merkezi çözümleri dünyanın herhangi bir yerinden **yönetin**.
- Aygıtı işinizle birlikte **genişletin** ve uyarlayın.
- Kolayca özelleştirilmiş çözümler **oluşturun**; EIP HTML, CSS, XML ve JavaScript gibi Web standartlarına dayanır. Ayrıca, HTTPS ve SSL olmak üzere standart güvenli protokoller kullanır.

## EIP'nin neleri sağlayabileceğine ilişkin örnekler

- İşinize ve iş grubunuza özgü menüler ve dil kullanın, örneğin "Müşteri veritabanını ara", "Formu alacak tahsil departmanına gönder" veya "Borç hesabına faksla".
- Tüm kişisel tercihleriniz, kimlik kartınızı geçirdiğinizde aygıt sisteminizin kullanıcı arabiriminde görüntülenir.
- Karmaşık bir iş akışını, yalnızca birkaç düğmenin basılmasını gerektiren basit bir sürece dönüştürün.
- Basılı bilgileri, tek bir tuşa dokunarak bir doküman havuzuna girin.
- Yazdırmak için ağ yazdırma sırasına doküman gönderin ve ağdaki herhangi bir aygıttan kimlik kartınızı geçirerek doküman yazdırın.
- Günün haberlerini veya hisse senedi raporlarını doğrudan Xerox aygıtın kullanıcı arabiriminden yazdırın.

## Daha Basit İşlemler

Karmaşık bir iş akışını basit bir işleme dönüştürün.

Aygıtınızda bir faturayı aynı anda hem ilgili departmana gönderen, hem kolay bulunabilmesi için bilgilerini bir doküman yönetim sisteminde arşivleyen, hem de kendi kayıtlarınız için bir kopyasını yazdıran bir 'fatura' düğmesi hayal edin.

Kullanıcılar kağıt dokümanları çabucak tarayıp kaydedebilir, küçük resimlerinin önizlemesini görebilir ve bunları sık kullanılan doküman saklama yerine ekleyebilir. Örneğin:

Bir öğretmen, öğrencilerin kolayca erişebilmesi bir dersin notlarını tarayarak belirli bir havuzda saklayabilir.

Bir öğrenci, sınav kağıtlarını, öğretmenin not verebilmesi için tarayarak dersin klasörüne koyabilir.

Xerox Extensible Interface Platform, kullanıcıların makinenin kontrol panelinden doküman havuzlarına ulaşmalarını sağlamak için Web tabanlı Xerox Ortağı çözümlerinden yararlanır.

Bunlara ek olarak, hassas kayıtları için daha fazla güvenlik arayan sağlık bakım hizmeti şirketleri, finans hizmeti şirketleri ve eğitim kurumları gibi kuruluşlar için tasarlanmış olan **Xerox Secure Access Unified ID System™** bulunmaktadır. Kart okuyucuları ve kart okuyucu yazılımını birleştiren bu sistemle kullanıcılar, kimlik kartlarını aygıttaki kart okuyucudan geçirerek veya kart okuyucunun önünde sallayarak Xerox aygıtlarına erişebilirler. Daha fazla güvenlik için bir PIN veya parola yazılıma yerleştirilebilir. Secure Access sistemi kuruluşun mevcut çalışan kimlik kartı sistemiyle bütünleştirilebilir.

Çözüme bağlı olarak aygıta ek kaynak gerekebilir.

Daha fazla bilgi için Xerox Satış Temsilcinizle görüşün.

## Kişisel Çözümler

EIP, oturum açma bilgilerinizi girerek veya şirket kimlik kartınızı üzerinden geçirerek aygıtta oturum açmanızı kolaylaştırır.

Bu, aygıtta güvenli erişim sağlamakla kalmaz, artık aygıt kim olduğunuzu bildiği için iş akışınıza özgü seçeneklere de erişebilir ve böylece işinizi daha kolay yaparsınız.

# XEIP'yi Yapılandırma

## Bilgi Kontrol Listesi

Kurulum işlemine başlamadan önce, lütfen aşağıdakilerin mevcut olduğundan veya gerçekleştirildiğinden emin olun.

- **Aygıtın ağda tamamen sorunsuz olarak çalıştığından emin olun.**
- **EIP çözümünüzün kurulu ve çalışır durumda olduğundan emin olun.** Daha fazla bilgi için, Xerox Satış Temsilcinize danışın.
- **Aygıtta Secure HTTP SSL protokolünün etkin olduğundan emin olun.** (Bu, isteğe bağlıdır) Ayrıntılar için, bkz. [Secure HTTP \(SSL\) Protokolünü Etkinleştirme](#), sayfa. 8.

**Not:** Secure HTTP (SSL) protokolünü etkinleştirebilmeniz için önce aygıtta Makine Dijital Sertifikası'nın yüklenmiş olması gerekir. Ayrıntılar için, bkz. [Makine Dijital Sertifika Yönetimi](#), sayfa. 7.

## Özel Hizmetleri Etkinleştirme

### İş istasyonunuzda

1. Web tarayıcınızı açın, makinenin *IP adresini* Adres çubuğuna veya Konum alanına girin.
2. Aygıtın Internet Hizmetleri'ne erişmek için **Enter** (Gir) seçeneğini tıklatın.
3. Aygıtı EIP uygulamalarını kullanmak üzere etkinleştirmek için:
  - a. **Properties** (Özellikler) sekmesini tıklatın.
  - b. **Services** (Hizmetler) seçeneğini ve ardından **Custom Services** (Müşteri Hizmetleri) bağlantısını tıklatın.
  - c. Hizmeti etkinleştirmek için *Custom Services* (Özel Hizmetler) sayfasında, *Enablement*(Etkinleştirme) alanında, *Custom Services* (Özel Hizmetler) için **Enabled** (Etkin) onay kutusunu işaretleyin.
  - d. *Optional Information* (İsteğe Bağlı Bilgiler) alanında, gerekirse aşağıdakiler için **Enabled** (Etkin) onay kutularını işaretleyin:
    - **Export User Password to Custom Service** (Kullanıcı Parolasını Özel Hizmette Aktar) - seçilirse, parolalar Özel Hizmet'e gönderilir.
    - **Automatically validate signed certificates from server** (Sunucudaki imzalı sertifikaları otomatik olarak doğrula) - seçilirse, bu seçeneğin çalışması için hem sunucu, hem aygıt sertifika ister. Bu sertifikaların aygıtın güvendiği bir yetkili tarafından yayınlanmış olması gerekir.
  - e. **Apply** (Uygula) seçeneğini tıklatın.
  - f. İstenirse, Sistem Yönetici Kimliğinizi ve geçiş kodunuzu girin. Varsayılan Sistem Yöneticisi Kimliği ve geçiş kodu, sırasıyla "**admin**" ve "**1111**" değerleridir.
4. Dijital bir sertifika (gerekirse) üretmek için, bkz. [Makine Dijital Sertifika Yönetimi](#), sayfa. 7.
5. SSL protokolünü (gerekirse) etkinleştirme konusunda bilgi için, bkz. [Secure HTTP \(SSL\) Protokolünü Etkinleştirme](#), sayfa. 8.

## Aygıtta

1. **All Services** (Tüm Hizmetler) düğmesine basın.
2. **Custom Services** (Özel Hizmetler) düğmesine dokununuz.
3. Kaydettiğiniz **EIP Application** (EIP Uygulaması) düğmesine dokununuz. XEIP iş akışınıza yeni düğmeden erişilebiliyor olması gerekir.

## Makine Dijital Sertifika Yönetimi

1. Web tarayıcınızı açın, makinenin *IP adresini* Adres çubuğuna veya Konum alanına girin.
2. Aygıtın Internet Hizmetleri'ne erişmek için **Enter** (Gir) seçeneğini tıklattın.
3. **Properties** (Özellikler) sekmesini tıklattın.
4. İstenirse, Sistem Yönetici Kimliğinizi ve geçiş kodunuzu girin. Varsayılan Sistem Yöneticisi Kimliği ve geçiş kodu, sırasıyla "**admin**" ve "**1111**" değerleridir.
5. **Security** (Güvenlik) seçeneğini tıklattın.
6. Dizin ağacında **Machine Digital Certificate** (Makine Dijital Sertifikası) bağlantısını tıklattın.
7. *Machine Digital Certificate* (Makine Dijital Sertifikası) alanında, **Create New Certificate** (Yeni Sertifika Oluştur) düğmesini tıklattın.
8. *Create New Certificate* (Yeni Sertifika Oluştur) alanında, aşağıdakilerden birini seçin:
  - **Self Signed Certificate: Establish a Self Signed Certificate on this machine** (Kendinden İmzalı Sertifika: Bu makineye Kendinden İmzalı Sertifika Kur) - aygıt kendi sertifikasını güvenilir olarak imzalar ve SSL şifrelemede kullanılması için sertifikanın ortak anahtarını oluşturur.
  - **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** (Sertifika İmzalama İsteği: Güvenilir Sertifika Yetkilisi tarafından işleme alınacak bir Sertifika İmzalama İsteği indir) - Güvenilir bir Yetkili'den veya Güvenilir Yetkili görevi gören bir sunucudan alınan bir sertifika makineye yüklenebilir.
9. **Continue** (Devam) seçeneğini tıklattın.
10. Gerekli seçim için ayrıntıları aşağıdaki alanlara girin:

<b>Kendinden İmzalı Sertifika:</b>	<b>Sertifika İmzalama İsteği:</b>
<ul style="list-style-type: none"><li>• 2 Harfli Ülke Kodu</li><li>• Eyalet/İl Adı</li><li>• Semt Adı</li><li>• Kuruluş Adı</li><li>• Kuruluş Birimi</li><li>• E-posta Adresi</li><li>• Gün Olarak Geçerlilik Süresi</li></ul>	<ul style="list-style-type: none"><li>• 2 Harfli Ülke Kodu</li><li>• Eyalet/İl Adı</li><li>• Semt Adı</li><li>• Kuruluş Adı</li><li>• Kuruluş Birimi</li><li>• E-posta Adresi</li></ul>

11. **Apply** (Uygula) seçeneğini tıklattın.

12. Seçiminize bağlı olarak:

- *Self Signed Certificate*: (Kendinden İmzalı Sertifika:) seçeneğini seçerseniz Current Status (Geçerli Durum) ekranında **A Self Signed Certificate is established on this machine** (Bu makineye Kendinden İmzalı bir Sertifika kuruldu) ifadesi görüntülenir.
- *Certificate Signing Request*: (Sertifika İmzalama İsteği:) seçeneğini seçerseniz, **Certificate Signing Request (CSR)** (Sertifika İmzalama İsteği (Sİİ)) formu görüntülenir.
- a. **Certificate Signing Request** (Sertifika İmzalama İsteği) seçeneğini seçtiyseniz, **Save As** (Farklı Kaydet) düğmesini tıklatın
- b. Açılan iletişim kutusundan **X.509 (.pem)** veya **DER** biçimini seçin, **Save** (Kaydet) seçeneğini tıklatın.
- c. *File Download* (Dosya İndir) açılır menüsünden **Save** (Kaydet) seçeneğini tıklatın, iş istasyonunuzdaki kaydedeceğiniz yeri seçin ve dosyayı kaydetmek için **Save** (Kaydet) seçeneğini tıklatın. Sertifika, güvenilir bir sertifika yetkilisi tarafından imzalandıktan sonra makineye kaydedilmeye hazırdır.
- d. **Machine Digital Certificate Management** (Makine Dijital Sertifika Yönetimi) ekranına dönün, *Machine Digital Certificate* (Makine Dijital Sertifikası) alanında **Upload Signed Certificate** (İmzalı Sertifikayı Karşıya Yükle) düğmesini tıklatın.
- e. **Browse** (Gözet) düğmesini tıklatın, dosyayı iş istasyonunuzda bulun ve **Open** (Aç) seçeneğini tıklatın.
- f. **Upload Certificate** (Sertifikayı Karşıya Yükle) seçeneğini tıklatın.

## Secure HTTP (SSL) Protokolünü Etkinleştirme

**Not:** Secure HTTP (SSL) protokolünü etkinleştirebilmeniz için önce aygıtta Makine Dijital Sertifikası'nın yüklenmiş olması gerekir. Ayrıntılar için, bkz. [Makine Dijital Sertifika Yönetimi](#), sayfa. 7.

### İş istasyonunuzda

1. Web tarayıcınızı açın, makinenin *IP adresini* Adres çubuğuna veya Konum alanına girin.
2. Aygıtın Internet Hizmetleri'ne erişmek için **Enter** (Gir) seçeneğini tıklatın.
3. **Properties** (Özellikler) sekmesini tıklatın.
4. İstenirse, Sistem Yönetici Kimliğinizi ve geçiş kodunuzu girin. Varsayılan Sistem Yöneticisi Kimliği ve geçiş kodu, sırasıyla "**admin**" ve "**1111**" değerleridir.
5. **Connectivity** (Bağlantı) ve ardından **Protocols** (Protokoller) seçeneğini tıklatın.
6. Dizin ağacında **HTTP** bağlantısını tıklatın.
7. *Configuration* (Yapılandırma) alanında:
  - a. *Protocol* (Protokol) seçeneği için, aygıtta HTTP iletişimini etkinleştirmek üzere **Enable** (Etkinleştir) onay kutusunu işaretleyin.
  - b. *Port Number* (Bağlantı Noktası Numarası) alanına aygıtın Web sunucusunun istemci HTTP bağlantıları için kullanacağı bağlantı kapısı numarasını girin. Varsayılan bağlantı kapısı numarası 80'dir.



c. *HTTP Security Mode* (HTTP Güvenlik Modu) için aşağıdaki aşağı açılır menülerden birini seçin:

- **Disable SSL (SSL'yi Devre Dışı Bırak)**
- **Enable SSL (SSL'yi Etkinleştir)** - güvenli (HTTPS) iletişimi sağlamak üzere Güvenli Yuva Katmanı'nı (SSL) etkinleştirmek için.
- **Require SSL (SSL İste)** - Güvenli Yuva Katmanı'nı (SSL) zorunlu yapmak için.

**Not:** Secure HTTP etkinleştirilirse, CentreWare Internet Services hizmetine erişmek için tüm sayfaların Web sayfasının URL'sinde **https://** içermesi gerekir.

d. *Keep Alive Timeout* (Canlı Kalma Süresi Bitimi) alanına, Web sunucusunun bir istemcinin oturumu kapatmadan önce istemciden bir HTTP yanıtı almak için bekleyeceği süreyi girin. Varsayılan süre 10 saniyedir.

8. **Apply** (Uygula) seçeneğini tıklatın.

## Proxy Sunucusu

Proxy sunucusu, hizmet almak isteyen istemciler ve bu hizmetleri sağlayan sunucular için bir filtre görevi görür. Proxy sunucusu, istekler proxy sunucusunun filtreleme kurallarını doğruluyorsa istekleri filtreler; isteğe geçiş ve bağlantıya izin verilir.

Proxy sunucusunun iki ana amacı vardır:

- Sunucunun arkasındaki aygıtları, güvenlik amacıyla anonim tutmak.
- İçeriği, örneğin bir sitedeki Web sayfalarını önbelleğe alarak bir kaynağa erişim süresini azaltmak.

### İş istasyonunuzda

1. Web tarayıcınızı açın, makinenin *IP adresini* Adres çubuğuna veya Konum alanına girin.
2. Aygıtın Internet Hizmetleri'ne erişmek için **Enter** (Gir) seçeneğini tıklatın.
3. **Properties** (Özellikler) sekmesini tıklatın.
4. İstenirse, Sistem Yönetici Kimliğinizi ve geçiş kodunuzu girin. Varsayılan Sistem Yöneticisi Kimliği ve geçiş kodu, sırasıyla "**admin**" ve "**1111**" değerleridir.
5. **Connectivity** (Bağlantı) ve ardından **Protocols** (Protokoller) seçeneğini tıklatın.
6. Dizin ağacında **Proxy Server** (Proxy Sunucusu) bağlantısını tıklatın.
7. *HTTP Proxy Server* (HTTP Proxy Sunucusu) alanında:
  - a. Proxy ayarlarını WPAD protokolünü kullanarak otomatik algılamak için **Auto Detect Proxy Settings** (Proxy Ayarlarını Otomatik Algıla) onay kutusunu işaretleyin. Otomatik proxy algılamayı devre dışı bırakmak ve el ile proxy kullanımı ayarlarını kullanmak için bu onay kutusunun işaretini kaldırın.
  - b. *HTTP Proxy Server* (HTTP Proxy Sunucusu) seçeneğinde, proxy ayarlarını el ile yapmak için **Enabled** (Etkin) onay kutusunu işaretleyin.
  - c. **IP Address** (IP Adresi) veya **Hostname** (Ana Makine Adı) seçeneğini seçin.
  - d. Doğru biçimlendirilmiş adresi ve bağlantı noktası numarasını **IP Address and Port** (IP Adresi Ve Bağlantı Noktası) veya **Host Name and Port** (Ana Makine Adı Ve Bağlantı Noktası) alanına girin, varsayılan bağlantı noktası numarası 8080'dir.

8. **Apply** (Uygula) seçeneğini tıklatın.

**Not:** Proxy sunucusu ayarları EIP, Smart eSolutions, HTTP(s) Ağ Tarama ve HTTP(s) Şablon Havuzu İndirme için kullanılır.

**Not:** Proxy ayarlarını otomatik olarak algılama, el ile yapılan ayarları geçersiz kılabilir. El ile yapılan ayarların kullanıldığından emin olmak için, Otomatik Proxy Algıla seçeneğini devre dışı bırakın.