Güvenlik Özellikleri Kılavuzu

İçindekiler

Giriş

Not Tanımları

Bu Kullanıcı Kılavuzunda aşağıdaki semboller ve kurallar kullanılmaktadır:

ÖNEMLİ	ÖNEMLİ, kaçınılmadığı takdirde mala zarar verebilecek veya ürün işlevselliğinin kaybolmasıyla sonuçlanabilecek potansiyel olarak tehlikeli bir durumu gösterir.
NOT	NOT, çalışma ortamını, kurulum şartlarını veya özel kullanım şartlarını belirtir.
	İpuçları simgeleri faydalı ipuçları ve destekleyici bilgiler gösterir.
Kalın	Kalın yazı stili, makinenin kontrol panelindeki veya bilgisayar ekranındaki düğmeleri belirtir.
İtalik	Italicized yazı stili, önemli bir noktayı emphasizes veya sizi ilgili başlığa yönlendirir.

İlgili bilgiler

- Giriş

Ticari Markalar

Adobe® ve Reader®, Adobe Systems Incorporated'ın Amerika Birleşik Devletleri ve/veya diğer ülkelerdeki ticari markaları veya tescilli ticari markalarıdır.

Bu kılavuzda yazılımından bahsedilen her şirket kendi mülkü olan programlara özel Yazılım License Anlaşması'na sahiptir.

Brother ürünleri, ilgili dokümanlar ve diğer materyallerde görünen şirketlerin tüm ticaret adları ve ürün adları ilgili şirketlerin ticari markaları veya tescilli ticari markalarıdır.

İlgili bilgiler

- Giriş

Telif Hakkı

İlgili bilgiler

- Giriş

Ağ Güvenlik Özelliklerini Kullanmadan Önce

Makineniz, günümüzde mevcut olan en yeni ağ güvenliği ve şifreleme protokollerini kullanır. Bu ağ özellikleri, verilerinizi korumaya ve makineye unauthorized erişimleri engellemeye yardımcı olmak için genel ağ güvenliği planınıza entegre edilebilir.

FTP ve TFTP protokollerini devre dışı bırakmanızı öneririz. Makinenize bu protokolleri kullanarak erişim sağlamak güvenli değildir.

İlgili bilgiler

- Giriş
  - Gereksiz Protokolleri Devre Dışı Bırakma

Gereksiz Protokolleri Devre Dışı Bırakma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. Devre dışı bırakmak için gereksiz protokol onay kutularını temizleyin.
6. **Submit (Gönder)** öğesine tıklayın.
7. Yapılandırmayı etkinleştirmek için Brother makinenizi yeniden başlatın.

İlgili bilgiler

- Ağ Güvenlik Özelliklerini Kullanmadan Önce

Ağ Güvenliği

Aygıt Güvenliği için Sertifikaları Yapılandırma

Ağa bağlı makinenizi SSL/TLS kullanarak güvenli şekilde yönetmek için bir sertifika yapılandırmalısınız. Bir sertifika yapılandırmak için Web Tabanlı Yönetim'i kullanmanız gerekir.

Güvenlik Sertifikası Özelliklerine Genel Bakış

Makineniz birden fazla güvenlik sertifikasının kullanılmasını destekler, böylece makine ile güvenli bir kimlik doğrulama ve iletişim sağlanır. Makine ile aşağıdaki güvenlik sertifikası özellikleri kullanılabilir:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

- SSL/TLS iletişimi
- IEEE 802.1x kimlik doğrulama
- IPsec

Makineniz aşağıdakileri destekler:

- Önceden yüklenmiş sertifika

  Makineniz önceden yüklenmiş, otomatik olarak imzalanan bir sertifikaya sahiptir. Bu sertifika, farklı bir sertifika oluşturmaya veya yüklemeye gerek kalmadan, SSL/TLS iletişimini kullanmanıza olanak sağlar.

Önceden yüklenmiş otomatik olarak imzalanan sertifika belli bir seviyeye kadar iletişiminizi korur. Daha iyi bir güvenlik için güvenilir bir organization yayınladığı bir sertifika kullanılmasını tavsiye ederiz.

- Otomatik olarak imzalanan sertifika

  Bu yazdırma sunucusu kendi sertifikasını yayınlar. Bu sertifikayı kullanarak, CA'dan farklı bir sertifika oluşturmaya veya yüklemeye gerek olmadan, SSL/TLS iletişimini kolaylıkla kullanabilirsiniz.
- Bir Sertifika Yetkilisinden (CA) Sertifika

  Bir CA'dan gelen sertifikayı yüklemek için iki yöntem vardır. Bir CA'dan bir sertifikanız varsa veya harici güvenilir bir CA'dan sertifika kullanmak isterseniz:
  - Bu yazdırma sunucusundan bir Sertifika İmzalama İsteği (CSR) kullanıldığında.
  - Bir sertifika ve özel anahtar alındığında.
- Sertifika Yetkilisi (CA) Sertifikası

  CA'yı tanımlayan ve kendi özel anahtarına sahip olan bir CA sertifikası kullanmak için Ağ güvenlik özelliklerini yapılandırmadan önce CA'dan o CA sertifikasını almanız gerekir.

- SSL/TLS iletişimini kullanacaksanız, önce sistem yöneticinize başvurmanızı öneririz.
- Yazdırma sunucusunu varsayılan fabrika ayarlarına geri sıfırladığınızda, yüklenen sertifika ve özel anahtar silinir. Yazdırma sunucusu sıfırlandıktan sonra aynı sertifikayı ve özel anahtarı tutmak isterseniz, bunları sıfırlamadan önce dışarıya aktarın ve sonra yeniden yükleyin.

İlgili bilgiler

- Aygıt Güvenliği için Sertifikaları Yapılandırma

İlgili konular:

- Web Tabanlı Yönetim'i (Web Tarayıcı) kullanarak Ağınız için IEEE 802.1x Kimlik Doğrulamayı Yapılandırma

Sertifikanın Oluşturulması ve Yüklenmesi

Bir güvenlik sertifikasını seçerken iki seçenek vardır: kendinden imzalı bir sertifika kullanın veya Sertifika Yetkilisinden (CA) bir sertifika kullanın.

Seçenek 1

Kendinden İmzalı Sertifika

1. Web Tabanlı Yönetim'i kullanarak kendinden imzalı bir sertifika oluşturun.
2. Kendinden imzalı sertifikayı bilgisayarınıza yükleyin.

Seçenek 2

CA'dan bir Sertifika

1. Web Tabanlı Yönetim'i kullanarak Sertifika İmzalama İsteği (CSR) oluşturun.
2. Web Tabanlı Yönetim'i kullanarak CA tarafından verilen sertifikayı Brother makinenize yükleyin.
3. Sertifikayı bilgisayarınıza yükleyin.

İlgili bilgiler

- Aygıt Güvenliği için Sertifikaları Yapılandırma

Kendi Kendine İmzalanan Sertifika Oluştur

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Create Self-Signed Certificate (Kendinden İmzalı Sertifika Oluştur)** öğesine tıklayın.
6. **Common Name (Ortak Ad)** ve **Valid Date (Geçerlilik Tarihi)** girin.
   - **Common Name (Ortak Ad)** uzunluğu 64 bayttan azdır. Bu makineye SSL/TLS iletişimiyle erişirken kullanmak için bir IP adresi, düğüm adı veya etki alanı adı gibi bir tanımlayıcı girin. Düğüm adı varsayılan olarak görüntülenir.
   - IPPS veya HTTPS protokolünü kullanıyorsanız bir uyarı görünecektir ve URL'ye kendinden imzalı sertifika için kullanılan **Common Name (Ortak Ad)** dışında bir ad girin.
7. Ayarınızı **Public Key Algorithm (Ortak Anahtar Algoritması)** açılır listesinden seçin.
8. Ayarınızı **Digest Algorithm (Özet Algoritma)** açılır listesinden seçin.
9. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Aygıt Güvenliği için Sertifikaları Yapılandırma

Sertifika İmzalama İsteği (CSR) Oluşturma ve Sertifika Yetkilisinden (CA) Sertifika Yükleme

Harici güvenilir bir Sertifika Yetkilisi'nden (CA) zaten bir sertifikanız varsa, sertifikayı ve özel anahtarı makinede depolayabilir ve bunları alarak ve vererek yönetebilirsiniz. Harici güvenilir bir CA'dan sertifikanız yoksa bir Sertifika İmzalama İsteği (CSR) oluşturun, kimlik doğrulama için bir CA'ya gönderin ve dönen sertifikayı makinenize yükleyin.

- Sertifika İmzalama İsteği Oluşturma (CSR)
- Makinenize Sertifika Yükleme

Sertifika İmzalama İsteği Oluşturma (CSR)

Bir Sertifika İmzalama İsteği (CSR), sertifika içindeki kimlik bilgilerini doğrulamak için bir Sertifika Yetkilisine (CA) gönderilen bir istektir.

CSR'yi oluşturmadan önce bilgisayarınızda CA'dan bir Kök Sertifika yüklemeniz önerilir.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Create CSR (CSR Oluştur)** öğesine tıklayın.
6. Bir **Common Name (Ortak Ad)** (gerekli) yazın ve **Organization (Organizasyon)** (isteğe bağlı) hakkında diğer bilgileri ekleyin.

   - Bir CA'nın kimliğinizi onaylayabilmesi ve dışarıdan birine doğrulayabilmesi için şirketinizin ayrıntıları gerekir.
   - **Common Name (Ortak Ad)** uzunluğu 64 bayttan az olmalıdır. Bu makineye SSL/TLS iletişimiyle erişirken kullanmak için bir IP adresi, düğüm adı veya etki alanı adı gibi bir tanımlayıcı girin. Düğüm adı varsayılan olarak görüntülenir. **Common Name (Ortak Ad)** gerekir.
   - URL'ye sertifika için kullanılan Ortak Ad'dan farklı bir ad yazarsanız bir uyarı görünecektir.
   - **Organization (Organizasyon)**, **Organization Unit (Organizasyon Birimi)**, **City/Locality (Şehir/Konum)** ve **State/Province (Ülke/Şehir)** uzunluğu 64 bayttan küçük olmalıdır.
   - **Country/Region (Ülke/Bölge)**, iki karakterli ISO 3166 ülke kodu olmalıdır.
   - Bir X.509v3 sertifikası uzantısı yapılandırıyorsanız, **Configure extended partition (Genişletilmiş bölmeyi yapılandır)** onay kutusunu seçin ve sonra **Auto (Register IPv4) (Oto (Kayıt IPv4))** veya **Manual (El İle)** öğesini seçin.
7. Ayarınızı **Public Key Algorithm (Ortak Anahtar Algoritması)** açılır listesinden seçin.
8. Ayarınızı **Digest Algorithm (Özet Algoritma)** açılır listesinden seçin.
9. **Submit (Gönder)** öğesine tıklayın.

   Ekranınızda CSR görünür. CSR'yi bir dosya olarak kaydedin veya kopyalayıp bir Sertifika Yetkilisinin sunduğu çevrimiçi bir CSR formu içine yapıştırın.
10. **Kaydet** öğesine tıklayın.

    - CA'nızın bir CSR'yi CA'nıza gönderme yöntemiyle ilgili ilkesini izleyin.
    - Windows Server'ın Kuruluş Kök CA'sını kullanıyorsanız, İstemci Sertifikasını güvenli bir şekilde oluşturmak üzere sertifika şablonu için Web Sunucusunu kullanmanızı öneririz. EAP-TLS kimlik doğrulamasıyla bir IEEE 802.1x ortamı için bir İstemci Sertifikası oluşturuyorsanız, Sertifika için kullanıcı şablonunu kullanmanızı öneririz.

İlgili bilgiler

- Sertifika İmzalama İsteği (CSR) Oluşturma ve Sertifika Yetkilisinden (CA) Sertifika Yükleme

Makinenize Sertifika Yükleme

Bir Sertifika Yetkilisi'nden (CA) bir sertifika aldığınızda, bunu yazıcı sunucusuna yüklemek için aşağıdaki adımları izleyin:

> Yalnızca makinenizin Sertifika İmzalama İsteği (CSR) ile verilen bir sertifika makinenize yüklenebilir. Başka bir CSR oluşturmak istediğinizde, yeni CSR oluşturmadan önce sertifikanın yüklendiğinden emin olun. Yalnızca makineye sertifika yüklendikten sonra başka bir CSR oluşturun, aksi durumda yeni CSR yüklenmeden önce oluşturulan CSR geçersiz olur.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Install Certificate (Sertifikayı Yükle)** öğesine tıklayın.
6. CA’nın verdiği sertifikayı içeren dosyaya gözatın ve sonra **Submit (Gönder)** öğesini tıklatın.

   Sertifika oluşturulur ve makinenizin belleğine kaydedilir.

SSL/TLS iletişimini kullanmak için, CA’dan Kök Sertifika bilgisayarınıza yüklenmelidir. Ağ yöneticinize başvurun.

İlgili bilgiler

- Sertifika İmzalama İsteği (CSR) Oluşturma ve Sertifika Yetkilisinden (CA) Sertifika Yükleme

Sertifika ve Özel Anahtarı İçe ve Dışa Aktarma

Makinenizde sertifikayı ve özel anahtarı depolayın ve bunları alarak ve vererek yönetin.

- Sertifika ve Özel Anahtar Alma
- Sertifika ve Özel Anahtar Aktarma

Sertifika ve Özel Anahtar Alma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Import Certificate and Private Key (Sertifika ve Özel Anahtarı Al)** öğesine tıklayın.
6. İçe aktarmak istediğiniz dosyaya göz atın ve seçin.
7. Dosya şifreliyse şifreyi yazın ve sonra **Submit (Gönder)** öğesini tıklatın.

Sertifika ve özel anahtar makinenize alınır.

İlgili bilgiler

- Sertifika ve Özel Anahtarı İçe ve Dışa Aktarma

Sertifika ve Özel Anahtar Aktarma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Certificate List (Sertifika Listesi)** ile göstermek için **Export (Gönder)** öğesini tıklatın.
6. Dosyayı şifrelemek isterseniz şifreyi girin.

   Boş şifre kullanılırsa, çıktı şifrelenmez.
7. Doğrulama için şifreyi yeniden girin ve sonra **Submit (Gönder)** öğesini tıklatın.
8. **Kaydet** öğesine tıklayın.

Sertifika ve özel anahtar bilgisayarınıza aktarılır.

Sertifikayı bilgisayarınıza da alabilirsiniz.

İlgili bilgiler

- Sertifika ve Özel Anahtarı İçe ve Dışa Aktarma

Bir CA Sertifikasını İçeriye ve Dışarıya Aktarma

CA sertifikalarını içe ve dışa aktarabilir ve Brother makinenizde saklayabilirsiniz.

- Bir CA Sertifikasını İçeri Aktarma
- Bir CA Sertifikasını Dışarıya Aktarma

Bir CA Sertifikasını İçeri Aktarma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **CA Certificate (CA Sertifikası)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Import CA Certificate (CA Sertifikasını Al)** öğesine tıklayın.
6. Almak istediğiniz dosyaya gözatın.
7. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Bir CA Sertifikasını İçeriye ve Dışarıya Aktarma

Bir CA Sertifikasını Dışarıya Aktarma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **CA Certificate (CA Sertifikası)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. Dışa aktarmak istediğiniz sertifikayı seçin ve **Export (Gönder)** öğesini tıklatın.
6. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Bir CA Sertifikasını İçeriye ve Dışarıya Aktarma

SSL/TLS Kullanımı

- SSL/TLS Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme
- SSL/TLS Kullanarak Belgeleri Güvenli Biçimde Yazdırma
- SSL/TLS Kullanarak Güvenli Şekilde E-posta Gönderme veya Alma

SSL/TLS Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

- SSL/TLS ve Mevcut Protokoller için Bir Sertifika Yapılandırma
- SSL/TLS Kullanarak Web Tabanlı Yönetim'e Erişim
- Yönetici olarak Windows Kullanıcıları İçin Kendinden İmzalı Sertifika Yükleme
- Aygıt Güvenliği için Sertifikaları Yapılandırma

SSL/TLS ve Mevcut Protokoller için Bir Sertifika Yapılandırma

SSL/TLS iletişimini kullanmadan önce Web Tabanlı Yönetim'i kullanarak makinenizde bir sertifika yapılandırın.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **HTTP Server Settings (HTTP Sunucu Ayarları)** öğesine tıklayın.
6. **Select the Certificate (Sertifikayı Seçin)** açılır listesinden yapılandırmak istediğiniz sertifikayı seçin.
7. **Submit (Gönder)** öğesine tıklayın.
8. Yazdırma sunucusunu yeniden başlatmak için **Yes (Evet)** öğesini tıklatın.

İlgili bilgiler

- SSL/TLS Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

İlgili konular:

- SSL/TLS Kullanarak Belgeleri Güvenli Biçimde Yazdırma

SSL/TLS Kullanarak Web Tabanlı Yönetim'e Erişim

Ağ makinenizi güvenle yönetmek için, güvenlik protokolleriyle yönetim yardımcı programlarını kullanmanız gerekir.

- HTTPS protokolünü kullanmak için, makinenizde HTTPS etkinleştirilmelidir. HTTPS protokolü varsayılan olarak etkindir.
- HTTPS protokolü ayarlarını Web Tabanlı Yönetim ekranını kullanarak değiştirebilirsiniz.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Artık makineye HTTPS'yi kullanarak erişebilirsiniz.

İlgili bilgiler

- SSL/TLS Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

Yönetici olarak Windows Kullanıcıları İçin Kendinden İmzalı Sertifika Yükleme

- Aşağıdaki adımlar Microsoft Edge içindir. Başka bir web tarayıcısı kullanıyorsanız, sertifikaların yüklenmesine yönelik talimatlar için web tarayıcınızın belgeleri veya çevrim içi yardımına başvurun.
- Kendinden imzalı sertifikanızı Web Tabanlı Yönetim kullanarak oluşturduğunuzdan emin olun.

1. **Microsoft Edge** simgesine sağ tıklayın ve ardından **Yönetici olarak çalıştır** öğesine tıklayın.

   Kullanıcı Hesabı Denetimi ekranı görünürse **Evet** öğesini tıklatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Bağlantınız özel değilse, **Gelişmiş** düğmesine tıklayın ve ardından web sayfasına devam edin.
4. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
5. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **Certificate (Sertifika)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
6. **Export (Gönder)** öğesine tıklayın.
7. Çıktı dosyasını şifrelemek için **Enter Password (Parola Girin)** alanına bir şifre girin. **Enter Password (Parola Girin)** alanı boşsa, çıkış dosyanız şifrelenmeyecektir.
8. Şifreyi yeniden **Retype Password (Parolayı Tekrar Girin)** alanına yazın ve sonra **Submit (Gönder)** öğesini tıklatın.
9. Açmak için indirilen dosyaya tıklayın.
10. **Sertifika Alma Sihirbazı** göründüğünde **İleri** öğesini tıklatın.
11. **İleri** öğesine tıklayın.
12. Gerekiyorsa bir şifre girin ve ardından **İleri** öğesine tıklayın.
13. **Tüm sertifikaları aşağıdaki depolama alanına yerleştir** öğesini seçin ve ardından **Gözat...** öğesini tıklatın.
14. **Güvenilen Kök Sertifika Yetkilileri** öğesini seçin ve sonra **Tamam** öğesine tıklatın.
15. **İleri** öğesine tıklayın.
16. **Son** öğesine tıklayın.
17. Parmak izi doğruysa **Evet** öğesini tıklatın.
18. **Tamam** öğesine tıklayın.

İlgili bilgiler

- SSL/TLS Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

SSL/TLS Kullanarak Belgeleri Güvenli Biçimde Yazdırma

IPPS Kullanarak Belgeleri Yazdırma

IPP protokolüyle belgeleri güvenle yazdırmak için, IPPS protokolünü kullanın.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **IPP** onay kutusunun seçili olduğundan emin olun.

   IPP onay kutusu seçili değilse, **IPP** onay kutusunu seçin ve sonra **Submit (Gönder)** öğesini tıklatın.

   Yapılandırmayı etkinleştirmek için makinenizi yeniden başlatın.

   Makine yeniden başladıktan sonra, makinenin web sayfasına dönün, şifreyi girin ve ardından, sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.
6. **HTTP Server Settings (HTTP Sunucu Ayarları)** öğesine tıklayın.
7. **IPP** alanında **HTTPS(Port 443)** onay kutusunu seçin ve ardından **Submit (Gönder)** öğesine tıklayın.
8. Yapılandırmayı etkinleştirmek için makinenizi yeniden başlatın.

IPPS'yi kullanarak iletişim yazdırma sunucusuna unauthorized erişimi önleyemez.

İlgili bilgiler

- SSL/TLS Kullanarak Belgeleri Güvenli Biçimde Yazdırma

SNMPv3 Kullanımı

- SNMPv3 Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

SNMPv3 Kullanarak Ağ Makinenizi Güvenli Şekilde Yönetme

Basit Ağ Yönetim Protokolü sürüm 3 (SNMPv3), ağ aygıtlarını güvenli şekilde yönetmek için kullanıcı kimliği doğrulama ve veri şifreleme sağlar.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna “https://Ortak Ad” yazın (burada “Ortak Ad” sertifikaya atadığınız Ortak Addır; bu, IP adresiniz, düğüm adı veya etki alanı adı olabilir).
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **SNMP** ayarının etkin olduğundan emin olun ve sonra **Advanced Settings (Gelişmiş ayarlar)** öğesini tıklatın.
6. SNMPv1/v2c modu ayarlarını yapılandırın.

Seçenek	Açıklama
SNMP v1/v2c read-write access (SNMP v1/v2c okuma-yazma erişimi)	Yazdırma sunucusu, SNMP protokolü sürüm 1 ve sürüm 2c’yi kullanır. Bu modda tüm makine uygulamalarını kullanabilirsiniz. Ancak, kullanıcı kimliğini doğrulamadığından ve veriler şifrelenmediğinden güvenli değildir.
SNMP v1/v2c read-only access (SNMP v1/v2c salt okunur erişim)	Yazdırma sunucusu, SNMP protokolünün sürüm 1 ve sürüm 2c’sinin salt okunur erişimini kullanır.
Disabled (Devredışı)	SNMP protokolünün sürüm 1 ve sürüm 2c’sini devre dışı bırakın. SNMPv1/v2c kullanan tüm uygulamalar kısıtlanacaktır. SNMPv1/v2c uygulamalarını kullanmaya izin vermek için **SNMP v1/v2c read-only access (SNMP v1/v2c salt okunur erişim)** veya **SNMP v1/v2c read-write access (SNMP v1/v2c okuma-yazma erişimi)** modunu kullanın.

7. SNMPv3 modu ayarlarını yapılandırın.

Seçenek	Açıklama
Enabled (Etkinleştirildi)	Yazdırma sunucusu, SNMP protokolü sürüm 3'ü kullanır. Yazdırma sunucusunu güvenli bir şekilde yönetmek için SNMPv3 modunu kullanın.
Disabled (Devredışı)	SNMP protokolünün sürüm 3’ünü devre dışı bırakın. SNMPv3 kullanan tüm uygulamalar kısıtlanacaktır. SNMPv3 uygulamalarını kullanmaya izin vermek için SNMPv3 modunu kullanın.

8. **Submit (Gönder)** öğesine tıklayın.

Makineniz protokol ayarı seçeneklerini gösteriyorsa, istediğiniz seçenekleri seçin.

9. Yapılandırmayı etkinleştirmek için makinenizi yeniden başlatın.

İlgili bilgiler

- SNMPv3 Kullanımı

IPsec Kullanımı

IPsec'e Giriş

IPsec (Internet Protokolü Güvenliği), veri değiştirmeyi önlemek ve IP paketleri olarak iletilen verilerin gizliliğini sağlamak için isteğe bağlı bir Internet Protokolü işlevi kullanan bir güvenlik protokolüdür. IPsec, bilgisayarlardan bir yazıcıya gönderilen yazdırma verileri gibi bir ağ üzerinden taşınan verileri şifreler. Veri ağ katmanında şifrelendiğinden, yüksek düzey protokol kullanan uygulamalar, kullanıcı kullanımının farkında olmasa da IPsec'i kullanır.

IPsec aşağıdaki fonksiyonları destekler:

- IPsec gönderimleri

  IPsec ayar koşullarına göre, ağ bağlantılı bir bilgisayar, IPsec kullanan belirli bir aygıta veri gönderir ve bu aygıttan veri alır. Aygıtlar IPsec kullanarak iletişim kurmaya başladığında, anahtarlar önce İnternet Anahtar Değişimi (IKE) kullanılarak değiştirilir ve ardından anahtarlar kullanılarak şifreli veri gönderilir.

  Ayrıca, IPsec'in iki çalışma modu vardır: Taşıma modu ve Tünel modu. Taşıma modu genellikle aygıtlar arasında iletişim kurmak için kullanılırken, Tünel modu Sanal Özel Ağ (VPN) gibi ortamlarda kullanılır.

  IPsec gönderimleri için aşağıdaki koşullar gereklidir:
  - IPsec kullanarak iletişim kurabilen bir bilgisayar ağa bağlıdır.
  - Makineniz, IPsec iletişimi için yapılandırılır.
  - Makinenize bağlı bilgisayar, IPsec bağlantıları için yapılandırılır.

- IPsec ayarları

  IPsec kullanan bağlantılar için gerekli olan ayarlar. Bu ayarlar, Web Tabanlı Yönetim kullanılarak yapılandırılabilir.

  IPsec ayarlarını yapılandırmak için, ağa bağlı bir bilgisayar üzerinden İnternet tarayıcısını kullanmanız gerekir.

İlgili bilgiler

- IPsec Kullanımı

Web Tabanlı Yönetim'i Kullanarak IPsec'i Yapılandırma

Address (Adresi) ve **IPsec** olmak üzere iki **Template (Şablon)** tip IPsec bağlantı koşulu bulunur. 10 adede kadar bağlantı koşulu yapılandırılabilir.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **IPsec** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. Ayarları yapılandırın.

Seçenek	Açıklama
Status (Durum)	IPsec'i etkinleştirin veya devre dışı bırakın.
Negotiation Mode (Anlaşma Modu)	IKE faz 1 için **Negotiation Mode (Anlaşma Modu)** öğesini seçin. IKE, IPsec ile şifreli iletişim için şifreleme anahtarı değiş tokuşunda kullanılan bir protokolüdür. **Main (Ana)** modunda işlem hızı yavaş ancak güvenlik yüksektir. **Aggressive (Katı)** modunda işlem hızı **Main (Ana)** modundan daha hızlıdır ancak güvenlik düşüktür.
All Non-IPsec Traffic (IPsec Tanımayan Tüm Trafik)	IPsec olmayan paketler için yapılacak işlemi seçin. Web Hizmetleri kullanıldığında **All Non-IPsec Traffic (IPsec Tanımayan Tüm Trafik)** için **Allow (İzin Ver)** öğesi seçilmelidir. **Drop (Bırak)** öğesini seçerseniz Web Hizmetleri kullanılamaz.
Broadcast/Multicast Bypass (Yayın/Çok Noktaya Yayın Atlama)	veya **Disabled (Devredışı)** öğesini seçin.**Enabled (Etkinleştirildi)**
Protocol Bypass (Protokol Atlama)	İstediğiniz seçenek veya seçeneklerin onay kutusunu işaretleyin.
Rules (Kurallar)	Şablonu etkinleştirmek için **Enabled (Etkinleştirildi)** onay kutusunu işaretleyin. Birden fazla onay kutusu işaretlendiğinde, işaretlenen onay kutularına ilişkin ayarların çakışması halinde numarası daha küçük onay kutularının önceliği vardır. IPsec bağlantı koşulları için kullanılan **Address Template (Adres Şablonu)** öğesini seçmek için ilgili açılır listeden tıklayın. **Address Template (Adres Şablonu)** öğesini eklemek için **Add Template (Şablon Ekle)** öğesini tıklatın. IPsec bağlantı koşulları için kullanılan **IPsec Template (IPsec Şablonu)** öğesini seçmek için ilgili açılır listeden tıklayın. **IPsec Template (IPsec Şablonu)** öğesini eklemek için **Add Template (Şablon Ekle)** öğesini tıklatın.

6. **Submit (Gönder)** öğesine tıklayın.

   Yeni ayarları etkinleştirmek için makine yeniden başlatılacaksa yeniden başlatma onay ekranı görünecektir.

   Rules (Kurallar) tablosunda etkinleştirdiğiniz şablonda boş bir öğe varsa bir hata mesajı görünür. Seçimlerinizi onaylayın ve **Submit (Gönder)** öğesini yeniden tıklatın.

İlgili bilgiler

- IPsec Kullanımı

İlgili konular:

- Aygıt Güvenliği için Sertifikaları Yapılandırma

Web Tabanlı Yönetim'i Kullanarak IPsec Adres Şablonu Yapılandırma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **IPsec Address Template (IPsec Adres Şablonu)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **Address Template (Adres Şablonu)** öğesini silmek için **Delete (Sil)** düğmesini tıklatın. **Address Template (Adres Şablonu)** kullanılıyorken silinemez.
6. Oluşturmak istediğiniz **Address Template (Adres Şablonu)** öğesini tıklatın. **IPsec Address Template (IPsec Adres Şablonu)** görüntülenir.
7. Ayarları yapılandırın.

Seçenek	Açıklama
Template Name (Şablon Adı)	Şablon için bir ad girin (en fazla 16 karakter).
Local IP Address (Yerel IP Adresi)	• **IP Address (IP Adresi)** IP adresini belirtin. Açılır listeden **ALL IPv4 Address (TÜM IPv4 Adresleri)**, **ALL IPv6 Address (TÜM IPv6 Adresleri)**, **All Link Local IPv6 (Tüm Bağlantı Yerel IPv6)** veya **Custom (Özel)** öğesini seçin. Açılır listeden **Custom (Özel)** öğesini seçerseniz, metin kutusuna IP adresini (IPv4 veya IPv6) girin. • **IP Address Range (IP Adresi Aralığı)** Metin kutularına IP adresi aralığı için başlangıç ve bitiş IP adreslerini girin. Başlangıç ve bitiş IP adresleri IPv4 veya IPv6'ya standardized veya bitiş IP adresi başlangıç adresinden küçükse bir hata oluşacaktır. • **IP Address / Prefix (IP Adresi / Öneki)** CIDR gösterimini kullanarak IP adresini belirtin. Örneğin: 192.168.1.1/24 Ön ek, 192.168.1.1 için 24-bit alt ağ maskesi (255.255.255.0) şeklinde belirtildiğinden 192.168.1.### şeklindeki adresler geçerlidir.
Remote IP Address (Uzak IP Adresi)	• **Any (Herhangi Biri)** **Any (Herhangi Biri)** öğesini seçerseniz, tüm IP adresleri etkinleştirilir. • **IP Address (IP Adresi)** Metin kutusuna belirtilen IP adresini (IPv4 veya IPv6) girin. • **IP Address Range (IP Adresi Aralığı)** IP adresi aralığı için ilk ve son IP adreslerini girin. İlk ve son IP adresleri IPv4 veya IPv6'ya standardized veya son IP adresi ilk adresten küçükse bir hata oluşacaktır.

Seçenek	Açıklama
	• **IP Address / Prefix (IP Adresi / Öneki)** CIDR gösterimini kullanarak IP adresini belirtin. Örneğin: 192.168.1.1/24 Ön ek, 192.168.1.1 için 24-bit alt ağ maskesi (255.255.255.0) şeklinde belirtildiğinden 192.168.1.### şeklindeki adresler geçerlidir.

8. **Submit (Gönder)** öğesine tıklayın.

Geçerli olarak kullanılan şablon için ayarları değiştirdiğinizde, yapılandırmayı etkinleştirmek için makinenizi yeniden başlatın.

İlgili bilgiler

- IPsec Kullanımı

Web Tabanlı Yönetim'i Kullanarak IPsec Şablonu Yapılandırma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Security (Güvenlik)** > **IPsec Template (IPsec Şablonu)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. **IPsec Template (IPsec Şablonu)** öğesini silmek için **Delete (Sil)** düğmesini tıklatın. **IPsec Template (IPsec Şablonu)** kullanılıyorken silinemez.
6. Oluşturmak istediğiniz **IPsec Template (IPsec Şablonu)** öğesini tıklatın. **IPsec Template (IPsec Şablonu)** ekranı görüntülenir. Yapılandırma alanları seçtiğiniz **Use Prefixed Template (Önekli Şablon Kullan)** ve **Internet Key Exchange (IKE)** ayarlarına bağlı olarak farklılık gösterir.
7. **Template Name (Şablon Adı)** alanında, şablon için bir ad yazın (en fazla 16 karakter).
8. **Use Prefixed Template (Önekli Şablon Kullan)** açılır listesinde **Custom (Özel)** öğesini seçtiyseniz, **Internet Key Exchange (IKE)** seçeneklerini seçin ve sonra ayarları gerektiği gibi değiştirin.
9. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- IPsec Kullanımı
  - IPsec Şablonu için IKEv1 Ayarları
  - IPsec Şablonu için IKEv2 Ayarları
  - IPsec Şablonu için Manuel Ayarlar

IPsec Şablonu için IKEv1 Ayarları

Seçenek	Açıklama
Template Name (Şablon Adı)	Şablon için bir ad girin (en fazla 16 karakter).
Use Prefixed Template (Önekli Şablon Kullan)	**Custom (Özel)**, **IKEv1 High Security (IKEv1 Yüksek Güvenlik)** veya **IKEv1 Medium Security (IKEv1 Orta Güvenlik)** öğesini seçin. Ayar öğeleri seçili şablona bağlı olarak farklıdır.
Internet Key Exchange (IKE)	IKE, şifrelenen iletişimi IPsec kullanarak taşımak için şifreleme anahtarı değiş tokuşu için kullanılan bir iletişim protokolüdür. Şifrelenen iletişimi yalnızca o kez için taşımak için, IPsec için gerekli şifreleme algoritması belirlenir ve şifreleme anahtarları paylaşılır. IKE için, şifreleme anahtarları Diffie-Hellman anahtarı değiş tokuş yöntemi kullanılarak değiştirilir ve IKE ile sınırlı şifrelenen iletişim taşınır. **Use Prefixed Template (Önekli Şablon Kullan)** içinde **Custom (Özel)** öğesini seçtiyseniz, **IKEv1** öğesini seçin.
Authentication Type (Kimlik Doğrulama Türü)	• **Diffie_Hellman_Group** Bu anahtar değişim yöntemi gizli anahtarların korunmasız bir ağ üzerinden güvenli bir şekilde değiştirilmesini sağlar. Diffie-Hellman anahtar değişim yöntemi rastlantı sayısı ve gizli anahtar kullanılarak oluşturulan açık bilgileri göndermek ve almak için gizli anahtar değil ayrık logaritma problemi kullanır. **Group1 (Grup1)**, **Group2 (Grup2)**, **Group5 (Grup5)** veya **Group14 (Grup14)** öğesini seçin. • **Encryption (Şifreleme)** **DES**, **3DES**, **AES-CBC 128** veya **AES-CBC 256** öğesini seçin. • **Hash (Karma)** **MD5**, **SHA1**, **SHA256**, **SHA384** veya **SHA512** öğesini seçin. • **SA Lifetime (SA Ömrü)** IKE SA kullanım ömrünü belirtin. Zamanı (saniye) ve kilobayt (KBayt) sayısını yazın.
Encapsulating Security (Kapsüllenen Güvenlik)	• **Protocol (Protokol)** **ESP**, **AH** veya **AH+ESP** öğesini seçin. - ESP, IPsec kullanarak şifreli iletişim kurmak için kullanılan bir protokoldür. ESP, yükü şifreler (iletilen içerik) ve ek bilgiler ekler. IP paketi, başlıktan ve başlığı takip eden şifrelenmiş yükten oluşur. Şifrelenmiş verilere ek olarak, IP paketi ayrıca şifreleme yöntemi ve şifreleme anahtarı, kimlik doğrulama verileri vb. ile ilgili bilgileri içerir. - AH, gönderenin kimliğini doğrulayan ve verilerin değiştirilmesini önleyen (tamamlılığı sağlar) IPsec protokolünün bir parçasıdır. IP paketinde, veri başlıktan hemen sonra girilir. Ek olarak, gönderenin yanlış olmasını ve verilerin değiştirilmesini önlemek için paketler iletişim kurulan içerik, gizli anahtar vb. denklemi kullanarak hesaplanan karma değerleri içerir. ESP'den farklı olarak, iletişim kurulan içerik şifrelenmez ve veri düz metin olarak gönderilir ve alınır. • **Encryption (Şifreleme) (AH seçeneği için sunulmaz.)** **DES**, **3DES**, **AES-CBC 128** veya **AES-CBC 256** öğesini seçin. • **Hash (Karma)** **None (Hiçbiri)**, **MD5**, **SHA1**, **SHA256**, **SHA384** veya **SHA512** öğesini seçin.

Seçenek	Açıklama
	None (Hiçbiri) sadece **Protocol (Protokol)** için **ESP** seçildiğinde seçilebilir. • **SA Lifetime (SA Ömrü)** IKE SA kullanım ömrünü belirtin. Zamanı (saniye) ve kilobayt (KBayt) sayısını yazın. • **Encapsulation Mode (Kapsülleme Modu)** **Transport (Aktarım)** veya **Tunnel (Tünel)** öğesini seçin. • **Remote Router IP-Address (Uzak Yönlendirici IP Adresi)** Uzak yönlendiricinin IP adresini (IPv4 veya IPv6) yazın. Bu bilgileri yalnızca **Tunnel (Tünel)** modu seçildiğinde girin. SA (Security Association), iletişim başlamadan önce güvenli bir iletişim kanalı oluşturmak amacıyla IPsec veya IPv6 kullanan ve şifreleme yöntemi ve şifreleme anahtarı gibi bilgileri alıp paylaşan şifreli bir iletişim yöntemidir. SA ayrıca kurulu olan sanal bir şifreli iletişim kanalıyla da alakalı olabilir. IPsec için kullanılan SA, şifreleme yöntemini belirler, anahtarları değiştirir ve IKE (Internet Anahtar Değişimi) standart prosedürüne göre karşılıklı kimlik doğrulaması yapar. Ayrıca, SA periyodik olarak güncellenir.
Perfect Forward Secrecy (PFS) (Kusursuz İletme Gizliliği)	PFS, mesajları şifrelemek için kullanılan önceki anahtarlardan anahtarlar türetmez. Ayrıca, bir mesajı şifrelemek için kullanılan bir anahtar bir ana anahtardan türetilmişse, bu ana anahtar diğer anahtarları türetmek için kullanılmaz. Bu nedenle, bir anahtarın güvenliği tehlikeye girse bile, hasar yalnızca bu anahtarı kullanarak şifrelenmiş olan mesajlarla sınırlı olacaktır. **Enabled (Etkinleştirildi)** veya **Disabled (Devredışı)** öğesini seçin.
Authentication Method (Kimlik Doğrulama Yöntemi)	Kimlik doğrulama yöntemini seçin. **Pre-Shared Key (Önceden Paylaşılan Anahtar)** veya **Certificates (Sertifikalar)** öğesini seçin.
Pre-Shared Key (Önceden Paylaşılan Anahtar)	İletişimi şifrelerken, şifreleme anahtarı başka bir kanal kullanılarak önceden değiştirilir ve paylaşılır. **Authentication Method (Kimlik Doğrulama Yöntemi)** için **Pre-Shared Key (Önceden Paylaşılan Anahtar)** seçtiyseniz, **Pre-Shared Key (Önceden Paylaşılan Anahtar)** yazın (en fazla 32 karakter). • **Local/ID Type/ID (Yerel/Kimlik Tipi/Kimlik)** Gönderenin kimlik türünü seçin ve sonra kimliği yazın. Tür için **IPv4 Address (IPv4 Adresi)**, **IPv6 Address (IPv6 Adresi)**, **FQDN**, **E-mail Address (E-posta Adresi)** ya da **Certificate (Sertifika)** seçimini yapın. **Certificate (Sertifika)** seçerseniz, sertifikanın ortak adını **ID (Kimlik)** alanına yazın. • **Remote/ID Type/ID (Uzak/Kimlik Türü/Kimlik)** Alıcının kimlik türünü seçin ve sonra kimliği yazın. Tür için **IPv4 Address (IPv4 Adresi)**, **IPv6 Address (IPv6 Adresi)**, **FQDN**, **E-mail Address (E-posta Adresi)** ya da **Certificate (Sertifika)** seçimini yapın. **Certificate (Sertifika)** seçerseniz, sertifikanın ortak adını **ID (Kimlik)** alanına yazın.
Certificate (Sertifika)	**Authentication Method (Kimlik Doğrulama Yöntemi)** için **Certificates (Sertifikalar)** öğesini seçtiyseniz, sertifikayı seçin. Yalnızca Web Tabanlı Yönetimin Güvenlik yapılandırma ekranındaki **Certificate (Sertifika)**sayfasını kullanarak oluşturulan sertifikaları seçebilirsiniz.

İlgili bilgiler

- Web Tabanlı Yönetim'i Kullanarak IPsec Şablonu Yapılandırma

IPsec Şablonu için IKEv2 Ayarları

Seçenek	Açıklama
Template Name (Şablon Adı)	Şablon için bir ad girin (en fazla 16 karakter).
Use Prefixed Template (Önekli Şablon Kullan)	**Custom (Özel)**, **IKEv2 High Security (IKEv2 Yüksek Güvenlik)** veya **IKEv2 Medium Security (IKEv2 Orta Güvenlik)** öğesini seçin. Ayar öğeleri seçili şablona bağlı olarak farklıdır.
Internet Key Exchange (IKE)	IKE, şifrelenen iletişimi IPsec kullanarak taşımak için şifreleme anahtarı değiş tokuşu için kullanılan bir iletişim protokolüdür. Şifrelenen iletişimi yalnızca o kez için taşımak için, IPsec için gerekli şifreleme algoritması belirlenir ve şifreleme anahtarları paylaşılır. IKE için, şifreleme anahtarları Diffie-Hellman anahtarı değiş tokuş yöntemi kullanılarak değiştirilir ve IKE ile sınırlı şifrelenen iletişim taşınır. **Use Prefixed Template (Önekli Şablon Kullan)** içinde **Custom (Özel)** öğesini seçtiyseniz, **IKEv2** öğesini seçin.
Authentication Type (Kimlik Doğrulama Türü)	• **Diffie_Hellman_Group** Bu anahtar değişim yöntemi gizli anahtarların korunmasız bir ağ üzerinden güvenli bir şekilde değiştirilmesini sağlar. Diffie-Hellman anahtar değişim yöntemi rastlantı sayısı ve gizli anahtar kullanılarak oluşturulan açık bilgileri göndermek ve almak için gizli anahtar değil ayrık logaritma problemi kullanır. **Group1 (Grup1)**, **Group2 (Grup2)**, **Group5 (Grup5)** veya **Group14 (Grup14)** öğesini seçin. • **Encryption (Şifreleme)** **DES**, **3DES**, **AES-CBC 128** veya **AES-CBC 256** öğesini seçin. • **Hash (Karma)** **MD5**, **SHA1**, **SHA256**, **SHA384** veya **SHA512** öğesini seçin. • **SA Lifetime (SA Ömrü)** IKE SA kullanım ömrünü belirtin. Zamanı (saniye) ve kilobayt (KBayt) sayısını yazın.
Encapsulating Security (Kapsüllenen Güvenlik)	• **Protocol (Protokol)** **ESP** öğesini seçin. ESP, IPsec kullanarak şifreli iletişim kurmak için kullanılan bir protokoldür. ESP, yükü şifreler (iletilen içerik) ve ek bilgiler ekler. IP paketi, başlıktan ve başlığı takip eden şifrelenmiş yükten oluşur. Şifrelenmiş verilere ek olarak, IP paketi ayrıca şifreleme yöntemi ve şifreleme anahtarı, kimlik doğrulama verileri vb. ile ilgili bilgileri içerir. • **Encryption (Şifreleme)** **DES**, **3DES**, **AES-CBC 128** veya **AES-CBC 256** öğesini seçin. • **Hash (Karma)** **MD5**, **SHA1**, **SHA256**, **SHA384** veya **SHA512** öğesini seçin. • **SA Lifetime (SA Ömrü)** IKE SA kullanım ömrünü belirtin. Zamanı (saniye) ve kilobayt (KBayt) sayısını yazın. • **Encapsulation Mode (Kapsülleme Modu)** **Transport (Aktarım)** veya **Tunnel (Tünel)** öğesini seçin. • **Remote Router IP-Address (Uzak Yönlendirici IP Adresi)** Uzak yönlendiricinin IP adresini (IPv4 veya IPv6) yazın. Bu bilgileri yalnızca **Tunnel (Tünel)** modu seçildiğinde girin.

Seçenek	Açıklama
	SA (Security Association), iletişim başlamadan önce güvenli bir iletişim kanalı oluşturmak amacıyla IPsec veya IPv6 kullanan ve şifreleme yöntemi ve şifreleme anahtarı gibi bilgileri alıp paylaşan şifreli bir iletişim yöntemidir. SA ayrıca kurulu olan sanal bir şifreli iletişim kanalıyla da alakalı olabilir. IPsec için kullanılan SA, şifreleme yöntemini belirler, anahtarları değiştirir ve IKE (Internet Anahtar Değişimi) standart prosedürüne göre karşılıklı kimlik doğrulaması yapar. Ayrıca, SA periyodik olarak güncellenir.
Perfect Forward Secrecy (PFS) (Kusursuz İletme Gizliliği)	PFS, mesajları şifrelemek için kullanılan önceki anahtarlardan anahtarlar türetmez. Ayrıca, bir mesajı şifrelemek için kullanılan bir anahtar bir ana anahtardan türetilmişse, bu ana anahtar diğer anahtarları türetmek için kullanılmaz. Bu nedenle, bir anahtarın güvenliği tehlikeye girse bile, hasar yalnızca bu anahtarı kullanarak şifrelenmiş olan mesajlarla sınırlı olacaktır. **Enabled (Etkinleştirildi)** veya **Disabled (Devredışı)** öğesini seçin.
Authentication Method (Kimlik Doğrulama Yöntemi)	Kimlik doğrulama yöntemini seçin. **Pre-Shared Key (Önceden Paylaşılan Anahtar)**, **Certificates (Sertifikalar)**, **EAP - MD5** veya **EAP - MS-CHAPv2** öğesini seçin. EAP, PPP'nin uzantısı olan bir kimlik doğrulama protokolüdür. IEEE802.1x ile EAP kullanıldığında, her oturum sırasında kullanıcı kimlik doğrulaması için farklı bir anahtar kullanılır. Aşağıdaki ayarlar sadece **EAP - MD5** veya **EAP - MS-CHAPv2** öğesi **Authentication Method (Kimlik Doğrulama Yöntemi)** içinde seçildiğinde gereklidir: • **Mode (Modu)** veya **Client-Mode (İstemci Modu)** öğesini seçin.**Server-Mode (Sunucu Modu)** • **Certificate (Sertifika)** Sertifikayı seçin. • **User Name (Kullanıcı Adı)** Kullanıcı adını girin (en fazla 32 karakter). • **Password (Şifre)** Şifreyi girin (en fazla 32 karakter). Şifre onay için iki kez girilmelidir.
Pre-Shared Key (Önceden Paylaşılan Anahtar)	İletişimi şifrelerken, şifreleme anahtarı başka bir kanal kullanılarak önceden değiştirilir ve paylaşılır. **Authentication Method (Kimlik Doğrulama Yöntemi)** için **Pre-Shared Key (Önceden Paylaşılan Anahtar)** seçtiyseniz, **Pre-Shared Key (Önceden Paylaşılan Anahtar)** yazın (en fazla 32 karakter). • **Local/ID Type/ID (Yerel/Kimlik Tipi/Kimlik)** Gönderenin kimlik türünü seçin ve sonra kimliği yazın. Tür için **IPv4 Address (IPv4 Adresi)**, **IPv6 Address (IPv6 Adresi)**, **FQDN**, **E-mail Address (E-posta Adresi)** ya da **Certificate (Sertifika)** seçimini yapın. **Certificate (Sertifika)** seçerseniz, sertifikanın ortak adını **ID (Kimlik)** alanına yazın. • **Remote/ID Type/ID (Uzak/Kimlik Türü/Kimlik)** Alıcının kimlik türünü seçin ve sonra kimliği yazın. Tür için **IPv4 Address (IPv4 Adresi)**, **IPv6 Address (IPv6 Adresi)**, **FQDN**, **E-mail Address (E-posta Adresi)** ya da **Certificate (Sertifika)** seçimini yapın. **Certificate (Sertifika)** seçerseniz, sertifikanın ortak adını **ID (Kimlik)** alanına yazın.

Seçenek	Açıklama
Certificate (Sertifika)	**Authentication Method (Kimlik Doğrulama Yöntemi)** için **Certificates (Sertifikalar)** öğesini seçtiyseniz, sertifikayı seçin. Yalnızca Web Tabanlı Yönetimin Güvenlik yapılandırma ekranındaki **Certificate (Sertifika)**sayfasını kullanarak oluşturulan sertifikaları seçebilirsiniz.

İlgili bilgiler

- Web Tabanlı Yönetim'i Kullanarak IPsec Şablonu Yapılandırma

IPsec Şablonu için Manuel Ayarlar

Seçenek	Açıklama
Template Name (Şablon Adı)	Şablon için bir ad girin (en fazla 16 karakter).
Use Prefixed Template (Önekli Şablon Kullan)	**Custom (Özel)** öğesini seçin.
Internet Key Exchange (IKE)	IKE, şifrelenen iletişimi IPsec kullanarak taşımak için şifreleme anahtarı değiş tokuşu için kullanılan bir iletişim protokolüdür. Şifrelenen iletişimi yalnızca o kez için taşımak için, IPsec için gerekli şifreleme algoritması belirlenir ve şifreleme anahtarları paylaşılır. IKE için, şifreleme anahtarları Diffie-Hellman anahtarı değiş tokuş yöntemi kullanılarak değiştirilir ve IKE ile sınırlı şifrelenen iletişim taşınır. **Manual (El İle)** öğesini seçin.
Authentication Key (ESP, AH) (Kimlik Doğrulama Anahtarı (ESP, AH))	**In/Out (Giriş/Çıkış)** değerlerini girin. **Use Prefixed Template (Önekli Şablon Kullan)** öğesi için **Custom (Özel)** değeri seçilirse, **Internet Key Exchange (IKE)** öğesi için **Manual (El İle)** değeri seçilirse ve **Encapsulating Security (Kapsüllenen Güvenlik)** bölümüne ilişkin olarak **Hash (Karma)** öğesi için **None (Hiçbiri)** değerinden başka bir ayar seçilirse bu ayarların kullanılması gerekir. Ayarladığınız karakter sayısı **Encapsulating Security (Kapsüllenen Güvenlik)** bölümüne ilişkin olarak **Hash (Karma)** öğesi için seçtiğiniz ayara bağlı olarak farklılık gösterebilir. Belirtilen kimlik doğrulama anahtarının uzunluğu seçilen karma algoritmadan farklıysa bir hata oluşacaktır. • **MD5**: 128 bit (16 bayt) • **SHA1**: 160 bit (20 bayt) • **SHA256**: 256 bit (32 bayt) • **SHA384**: 384 bit (48 bayt) • **SHA512**: 512 bit (64 bayt) Anahtarı ASCII Kodunda belirttiğinizde karakterleri çift tırnak (“) içine alın.
Code key (ESP) (Kod anahtarı (ESP))	**In/Out (Giriş/Çıkış)** değerlerini girin. **Use Prefixed Template (Önekli Şablon Kullan)** için **Custom (Özel)** ayarı, **Internet Key Exchange (IKE)** için **Manual (El İle)** ayarı ve **Encapsulating Security (Kapsüllenen Güvenlik)** altındaki **Protocol (Protokol)** için **ESP** ayarı seçilirse bu ayarlar kullanılmalıdır. Ayarladığınız karakter sayısı **Encapsulating Security (Kapsüllenen Güvenlik)** bölümüne ilişkin olarak **Encryption (Şifreleme)** öğesi için seçtiğiniz ayara bağlı olarak farklılık gösterebilir. Belirtilen kod anahtarının uzunluğu seçilen şifreleme algoritmasından farklıysa bir hata oluşacaktır. • **DES**: 64 bit (8 bayt) • **3DES**: 192 bit (24 bayt) • **AES-CBC 128**: 128 bit (16 bayt) • **AES-CBC 256**: 256 bit (32 bayt) Anahtarı ASCII Kodunda belirttiğinizde karakterleri çift tırnak (“) içine alın.

Seçenek	Açıklama
SPI	Bu parametreler güvenlik bilgilerini belirlemek için kullanılır. Genelde, ana bilgisayarda çeşitli IPsec iletişim türleri için birden fazla Güvenlik Birliği (SA) bulunur. Bu nedenle bir IPsec paketi alındığında uygun SA'nın belirlenmesi gerekir. SA'yı belirleyen SPI parametresi Kimlik Doğrulama Başlığında (AH) ve Kapsüllenen Güvenlik Yükü (ESP) başlığında yer alır. Bu ayarlar, **Use Prefixed Template (Önekli Şablon Kullan)** öğesi için **Custom (Özel)** değeri, **Internet Key Exchange (IKE)** öğesi için **Manual (El İle)** değeri seçilirse kullanılmalıdır. **In/Out (Giriş/Çıkış)** değerlerini girin. (3-10 karakter)
Encapsulating Security (Kapsüllenen Güvenlik)	• **Protocol (Protokol)** **ESP** veya **AH** öğesini seçin. - ESP, IPsec kullanarak şifreli iletişim kurmak için kullanılan bir protokoldür. ESP, yükü şifreler (iletilen içerik) ve ek bilgiler ekler. IP paketi, başlıktan ve başlığı takip eden şifrelenmiş yükten oluşur. Şifrelenmiş verilere ek olarak, IP paketi ayrıca şifreleme yöntemi ve şifreleme anahtarı, kimlik doğrulama verileri vb. ile ilgili bilgileri içerir. - AH, gönderenin kimliğini doğrulayan ve verilerin değiştirilmesini önleyen (veri bütünlüğünü sağlar) IPsec protokolünün bir parçasıdır. IP paketinde, veri başlıktan hemen sonra girilir. Ek olarak, gönderenin yanlış olmasını ve verilerin değiştirilmesini önlemek için paketler iletişim kurulan içerik, gizli anahtar vb. denklemi kullanarak hesaplanan karma değerleri içerir. ESP'den farklı olarak, iletişim kurulan içerik şifrelenmez ve veri düz metin olarak gönderilir ve alınır. • **Encryption (Şifreleme) (AH seçeneği için sunulmaz.)** **DES**, **3DES**, **AES-CBC 128** veya **AES-CBC 256** öğesini seçin. • **Hash (Karma)** **None (Hiçbiri)**, **MD5**, **SHA1**, **SHA256**, **SHA384** veya **SHA512** öğesini seçin. **None (Hiçbiri)** sadece **Protocol (Protokol)** için **ESP** seçildiğinde seçilebilir. • **SA Lifetime (SA Ömrü)** IKE SA kullanım ömrünü belirtin. Zamanı (saniye) ve kilobayt (KBayt) sayısını yazın. • **Encapsulation Mode (Kapsülleme Modu)** **Transport (Aktarım)** veya **Tunnel (Tünel)** öğesini seçin. • **Remote Router IP-Address (Uzak Yönlendirici IP Adresi)** Uzak yönlendiricinin IP adresini (IPv4 veya IPv6) yazın. Bu bilgileri yalnızca **Tunnel (Tünel)** modu seçildiğinde girin. SA (Security Association), iletişim başlamadan önce güvenli bir iletişim kanalı oluşturmak amacıyla IPsec veya IPv6 kullanan ve şifreleme yöntemi ve şifreleme anahtarı gibi bilgileri alıp paylaşan şifreli bir iletişim yöntemidir. SA ayrıca kurulu olan sanal bir şifreli iletişim kanalıyla da alakalı olabilir. IPsec için kullanılan SA, şifreleme yöntemini belirler, anahtarları değiştirir ve IKE (Internet Anahtar Değişimi) standart prosedürüne göre karşılıklı kimlik doğrulaması yapar. Ayrıca, SA periyodik olarak güncellenir.

İlgili bilgiler

- Web Tabanlı Yönetim'i Kullanarak IPsec Şablonu Yapılandırma

Ağınız için IEEE 802.1x Kimlik Doğrulaması Kullanımı

IEEE 802.1x Kimlik Doğrulaması Nedir?

IEEE 802.1x, unauthorized ağ aygıtlarından erişimi sınırlayan bir IEEE standardıdır. Brother makineniz bir RADIUS sunucusuna (Kimlik doğrulama sunucusu) erişim noktanız veya hub yoluyla bir kimlik doğrulama isteği gönderir. İsteğiniz RADIUS sunucusu tarafından doğrulandıktan sonra, makineniz ağa erişebilir.

İlgili bilgiler

- Ağınız için IEEE 802.1x Kimlik Doğrulaması Kullanımı

Web Tabanlı Yönetim'i (Web Tarayıcı) kullanarak Ağınız için IEEE 802.1x Kimlik Doğrulamayı Yapılandırma

- Makinenizi EAP-TLS kimlik doğrulaması kullanarak yapılandırırsanız, yapılandırmayı başlatmadan önce bir CA tarafından verilen istemci sertifikasını yüklemeniz gerekir. İstemci sertifikası ile ilgili olarak ağ yöneticiniz ile iletişime geçin. Birden fazla sertifika yüklediyseniz, kullanmak istediğiniz sertifika adını yazmanızı tavsiye ederiz.
- Sunucu sertifikasını doğrulamadan önce, sunucu sertifikasını imzalayan CA tarafından yayınlanan CA sertifikasını içe aktarmanız gerekir. CA sertifikası aktarımının gerekli olup olmadığını doğrulamak için ağ yöneticinize veya İnternet Servis Sağlayıcınıza (ISP) başvurun.

Ayrıca kontrol panelinden Kablosuz Kurulum Sihirbazını kullanarak IEEE 802.1x kimlik doğrulamasını yapılandırabilirsiniz (Kablosuz ağ).

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Network (Ağ)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. Aşağıdakilerden birini yapın:
   - Kablolu ağ için

     Wired (Kablolu) > **Wired 802.1x Authentication (Kablolu 802.1x Kimlik Doğrulama)** öğesini tıklatın.
   - Kablosuz ağ için

     Wireless (Kablosuz) > **Wireless (Enterprise) (Kablosuz (Kuruluş))** öğesini tıklatın.
6. IEEE 802.1x kimlik doğrulama ayarlarını yapılandırın.

- Kablolu ağlar için IEEE 802.1x kimlik doğrulamasını etkinleştirmek için, **Wired 802.1x Authentication (Kablolu 802.1x Kimlik Doğrulama)** sayfasında **Wired 802.1x status (Kablolu 802.1x durumu)** için **Enabled (Etkinleştirildi)** öğesini seçin.
- **EAP-TLS** kimlik doğrulamasını kullanıyorsanız, **Client Certificate (İstemci sertifikası)** açılır listesinden doğrulama için yüklenen istemci sertifikasını (sertifika adı ile gösterilir) seçmeniz gerekir.
- **EAP-FAST**, **PEAP**, **EAP-TTLS** veya **EAP-TLS** kimlik doğrulamasını seçerseniz, **Server Certificate Verification (Sunucu Sertifikası Doğrulaması)** açılır listesinden doğrulama yöntemini seçin. Sunucu sertifikasını imzalayan CA tarafından verilen makineye önceden alınan CA sertifikasını kullanarak sunucu sertifikasını doğrulayın.

Server Certificate Verification (Sunucu Sertifikası Doğrulaması) açılır listesinden aşağıdaki doğrulama yöntemlerinden birini seçin:

Seçenek	Açıklama
No Verification (Doğrulama Yok)	Sunucu sertifikasına her zaman güvenilebilir. Doğrulama gerçekleştirilmez.
CA Cert. (SY Sertifika)	Sunucu sertifikasını imzalayan CA tarafından verilen CA sertifikasını kullanarak Sunucu sertifikasının CA güvenilirliğini kontrol etmeye yönelik doğrulama yöntemidir.
CA Cert. + ServerID (SY Sert. + Sunucu Kimliği)	Sunucu sertifikasının CA güvenilirliğinin yanı sıra ortak ad [1] değerini kontrol etmek için doğrulama yöntemi.

7. Yapılandırma işlemi bittiğinde, **Submit (Gönder)** öğesini tıklatın.

   Kablolu ağlar için: Yapılandırdıktan sonra, makinenizi IEEE 802.1x destekli ağa bağlayın. Birkaç dakika sonra, <**Wired IEEE 802.1x**> durumunu kontrol etmek için Ağ Yapılandırma Raporunu yazdırın.

Seçenek	Açıklama
Success	Kablolu IEEE 802.1x işlevi etkindir ve kimlik doğrulama başarılı olmuştur.
Failed	Kablolu IEEE 802.1x işlevi etkindir ancak kimlik doğrulama başarısız olmuştur.
Off	Kablolu IEEE 802.1x işlevi kullanılamaz.

İlgili bilgiler

- Ağınız için IEEE 802.1x Kimlik Doğrulaması Kullanımı

İlgili konular:

- Güvenlik Sertifikası Özelliklerine Genel Bakış
- Aygıt Güvenliği için Sertifikaları Yapılandırma

1 Ortak Ad doğrulaması sunucu sertifikasının ortak adını **Server ID (Sunucu Kimliği)** için yapılandırılan karakter dizesiyle karşılaştırır. Bu yöntemi kullanmadan önce, sunucu sertifikalarının ortak adıyla ilgili olarak sistem yöneticinize başvurun ve sonra **Server ID (Sunucu Kimliği)** öğesini yapılandırın.

IEEE 802.1x Kimlik Doğrulama Yöntemleri

EAP-FAST

Bir tunneled kimlik doğrulama işlemine erişmek için kimlik doğrulama için bir kullanıcı kimliği ve şifre ve simetrik anahtar algoritmalar kullanan Genişletilebilir Kimlik Doğrulama Protokolü-Güvenli Tünelleme Yoluyla Esnek Kimlik Doğrulama (EAP-FAST) Cisco Systems, Inc. tarafından geliştirilmiştir.

Brother makineniz aşağıdaki dahili kimlik doğrulama yöntemlerini destekler:

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (Kablolu ağ)

Genişletilebilir Kimlik Doğrulama Protokolü-Mesaj Özetleme Algoritması 5 (EAP-MD5), kimlik sorma-yanıt verme kimlik doğrulaması için bir kullanıcı kimliği ve şifre kullanır.

PEAP

Korumalı Genişletilebilir Kimlik Doğrulama Protokolü (PEAP) Cisco Systems, Inc., Microsoft Corporation ve RSA Security tarafından geliştirilmiş bir EAP yöntemi sürümüdür. PEAP, bir kullanıcı kimliği ve şifre göndermek için bir istemci ve bir kimlik doğrulama sunucusu arasında şifreli bir Güvenli Yuva Katmanı (SSL)/ Aktarım Katmanı Güvenliği (TLS) tüneli ve kimlik doğrulama sunucusu oluşturur. PEAP, sunucu ve istemci arasında karşılıklı kimlik doğrulaması sağlar.

Brother makineniz aşağıdaki dahili kimlik doğrulama yöntemlerini destekler:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Genişletilebilir Kimlik Doğrulama Protokolü-Tünelli Ulaştırma Katmanı Güvenliği (EAP-TTLS), Funk Software ve Certicom tarafından geliştirilmiştir. EAP-TTLS, bir kullanıcı kimliği ve şifre göndermek için, bir istemci ve kimlik doğrulama sunucusu arasında PEAP'ye benzer bir şifreli SSL tüneli oluşturur. EAP-TTLS, sunucu ve istemci arasında karşılıklı kimlik doğrulaması sağlar.

Brother makineniz aşağıdaki dahili kimlik doğrulama yöntemlerini destekler:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

Genişletilebilir Kimlik Doğrulama Protokolü-İletim Katmanı Güvenliği (EAP-TLS), hem istemcide hem de kimlik doğrulama sunucusunda dijital sertifika kimlik doğrulaması gerektirir.

İlgili bilgiler

- Ağınız için IEEE 802.1x Kimlik Doğrulaması Kullanımı

Kullanıcı Kimliği Doğrulama

- Active Directory Kimlik Doğrulaması Kullanımı
- LDAP Kimlik Doğrulaması Kullanımı
- Secure Function Lock 3.0'ı Kullanma

Active Directory Kimlik Doğrulaması Kullanımı

Active Directory Kimlik Doğrulamasına Giriş

Active Directory Kimlik Doğrulaması makinenizin kullanımını kısıtlar. Active Directory Kimlik Doğrulaması etkinse, makinenin kontrol paneli kilitlenecektir. Bir Kullanıcı Kimliği ve şifre girene kadar makinenin ayarlarını değiştiremezsiniz.

Active Directory Kimlik Doğrulaması aşağıdaki özellikleri sunar:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

- Gelen yazdırma verilerini depolar
- Gelen faks verilerini depolar
- Taranan verileri bir e-posta sunucusuna gönderirken e-posta adresini Kullanıcı Kimliğine göre Active Directory sunucusundan alır.

  Bu özelliği kullanmak amacıyla, **Get Mail Address (Posta Adresi Edin)** ayarı için **On (Açık)** seçeneğini ve **LDAP + kerberos** ya da **LDAP + NTLMv2** kimlik doğrulama yöntemini seçin. Taranan verileri e-posta adresinize göndermek isterseniz makine taranan verileri bir e-posta sunucusuna veya alıcı olarak gönderdiğinde e-posta adresiniz gönderen olarak ayarlanır.

Active Directory Kimlik Doğrulaması etkinken, makineniz gelen tüm faks verilerini depolar. Oturum açtıktan sonra, makine depolanan faks verilerini yazdırır.

Web Tabanlı Yönetimi kullanarak Active Directory Kimlik Doğrulaması ayarlarını değiştirebilirsiniz.

İlgili bilgiler

- Active Directory Kimlik Doğrulaması Kullanımı

Web Tabanlı Yönetim'i Kullanarak Active Directory Kimlik Doğrulamayı Yapılandırma

Active Directory kimlik doğrulaması Kerberos kimlik doğrulamasını ve NTLMv2 kimlik doğrulamasını destekler. SNTP protokolü (ağ zaman sunucusu) ve DNS sunucusu yapılandırmasını kimlik doğrulama için yapılandırmalısınız.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve **"Pwd"** olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **User Restriction Function (Kullanıcı Kısıtlama İşlevi)** veya **Restriction Management (Kısıtlama Yönetimi)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Active Directory Authentication (Active Directory Kimlik Doğrulaması)** öğesini seçin.
6. **Submit (Gönder)** öğesine tıklayın.
7. **Active Directory Authentication (Active Directory Kimlik Doğrulaması)** öğesine tıklayın.
8. Aşağıdaki ayarları yapılandırın:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

Seçenek	Açıklama
Storage Fax RX Data (Faks RX Verilerini Kaydet)	Bu seçeneği gelen faks verilerini depolamak için seçin. Makinede oturum açtıktan sonra tüm gelen faks verilerini yazdırabilirsiniz.
Remember User ID (Kullanıcı Kimliğini Hatırla)	Bu seçeneği Kullanıcı Kimliğinizi kaydetmek için seçin.
Active Directory Server Address (Active Directory Sunucu Adresi)	Active Directory Sunucusunun IP adresini veya sunucu adını (örneğin: ad.example.com) yazın.
Active Directory Domain Name (Active Directory Etki Alanı Adı)	Active Directory etki alanı adını yazın.
Protocol & Authentication Method (Protokol ve Kimlik Doğrulama Yöntemi)	Protokol ve kimlik doğrulama yöntemi seçin.
SSL/TLS	**SSL/TLS** seçeneğini seçin.
LDAP Server Port (LDAP Sunucusu Bağlantı Noktası)	Active Directory sunucusunu LDAP yoluyla bağlamak için bağlantı noktası numarasını yazın (yalnızca **LDAP + kerberos** veya **LDAP + NTLMv2** kimlik doğrulama yöntemi için kullanılabilir).

Seçenek	Açıklama
LDAP Search Root (LDAP Arama Kökü)	LDAP arama kökünü yazın (yalnızca **LDAP + kerberos** veya **LDAP + NTLMv2** kimlik doğrulama yöntemi için kullanılabilir).
Get Mail Address (Posta Adresi Edin)	Bu seçeneği Active Directory sunucusundan oturum açan kullanıcının e-posta adresini almak için seçin. (yalnızca **LDAP + kerberos** veya **LDAP + NTLMv2** kimlik doğrulama yöntemi için kullanılabilir)
Get User's Home Directory (Kullanıcının Giriş Dizinini Edin)	Bu seçeneği ana dizininizi Ağa Tara hedefi olarak almak için seçin. (yalnızca **LDAP + kerberos** veya **LDAP + NTLMv2** kimlik doğrulama yöntemi için kullanılabilir)

9. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Active Directory Kimlik Doğrulaması Kullanımı

Makinenin Kontrol Panelini (Active Directory Kimlik Doğrulaması) Kullanarak Makine Ayarlarını Değiştirmek İçin Oturum Açma

Active Directory Kimlik Doğrulaması etkinken, makinenin kontrol panelinde Kullanıcı Kimliği ve şifresini girene kadar makinenin kontrol paneli kilitlenecektir.

1. Makinenin kontrol panelinde, oturum açmak için Kullanıcı Kimliğinizi ve Şifreyi girin.
2. Kimlik doğrulama başarılı olduğunda, makinenin kontrol panelinin kilidi açılır.

İlgili bilgiler

- Active Directory Kimlik Doğrulaması Kullanımı

LDAP Kimlik Doğrulaması Kullanımı

LDAP Kimlik Doğrulamasına Giriş

LDAP Kimlik Doğrulaması makinenizin kullanımını kısıtlar. LDAP Kimlik Doğrulaması etkinse, makinenin kontrol paneli kilitlenecektir. Bir Kullanıcı Kimliği ve şifre girene kadar makinenin ayarlarını değiştiremezsiniz.

LDAP Kimlik Doğrulaması aşağıdaki özellikleri sunar:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

- Gelen yazdırma verilerini depolar
- Gelen faks verilerini depolar
- Taranan verileri bir e-posta sunucusuna gönderirken e-posta adresini Kullanıcı Kimliğine göre LDAP sunucusundan alır.

  Bu özelliği kullanmak amacıyla, **Get Mail Address (Posta Adresi Edin)** ayarı için **On (Açık)** öğesini seçin. Taranan verileri e-posta adresinize göndermek isterseniz makine taranan verileri bir e-posta sunucusuna veya alıcı olarak gönderdiğinde e-posta adresiniz gönderen olarak ayarlanır.

LDAP Kimlik Doğrulaması etkinken, makineniz gelen tüm faks verilerini depolar. Oturum açtıktan sonra, makine depolanan faks verilerini yazdırır.

Web Tabanlı Yönetimi kullanarak LDAP Kimlik Doğrulaması ayarlarını değiştirebilirsiniz.

İlgili bilgiler

- LDAP Kimlik Doğrulaması Kullanımı

Web Tabanlı Yönetim'i Kullanarak LDAP Kimlik Doğrulamasını Yapılandırma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **User Restriction Function (Kullanıcı Kısıtlama İşlevi)** veya **Restriction Management (Kısıtlama Yönetimi)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **LDAP Authentication (LDAP Kimlik Doğrulaması)** öğesini seçin.
6. **Submit (Gönder)** öğesine tıklayın.
7. **LDAP Authentication (LDAP Kimlik Doğrulaması)** menüsüne tıklayın.
8. Aşağıdaki ayarları yapılandırın:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

Seçenek	Açıklama
Storage Fax RX Data (Faks RX Verilerini Kaydet)	Bu seçeneği gelen faks verilerini depolamak için seçin. Makinede oturum açtıktan sonra tüm gelen faks verilerini yazdırabilirsiniz.
Remember User ID (Kullanıcı Kimliğini Hatırla)	Bu seçeneği Kullanıcı Kimliğinizi kaydetmek için seçin.
LDAP Server Address (LDAP Sunucu Adresi)	LDAP sunucusunun IP adresini veya sunucu adını yazın (örneğin: ldap.example.com).
SSL/TLS	SSL/TLS üzerinden LDAP'ı kullanmak için **SSL/TLS** seçeneğini belirtin.
LDAP Server Port (LDAP Sunucusu Bağlantı Noktası)	LDAP sunucusu bağlantı noktası numarasını yazın.
LDAP Search Root (LDAP Arama Kökü)	LDAP araması kök dizinini yazın.
Attribute of Name (Search Key) (Ad Niteliği (Arama Tuşu))	Arama anahtarı olarak kullanmak istediğiniz özniteliği yazın.
Get Mail Address (Posta Adresi Edin)	Bu seçeneği LDAP sunucusundan oturum açan kullanıcının e-posta adresini almak için seçin.
Get User's Home Directory (Kullanıcının Giriş Dizinini Edin)	Bu seçeneği ana dizininizi Ağa Tara hedefi olarak almak için seçin.

9. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- LDAP Kimlik Doğrulaması Kullanımı

Makinenin Kontrol Panelini (LDAP Kimlik Doğrulaması) Kullanarak Makine Ayarlarını Değiştirmek İçin Oturum Açma

LDAP Kimlik Doğrulaması etkinken, makinenin kontrol panelinde Kullanıcı Kimliği ve şifresini girene kadar makinenin kontrol paneli kilitlenecektir.

1. Makinenin kontrol panelinde, oturum açmak için Kullanıcı Kimliğinizi ve Şifreyi girin.
2. Kimlik doğrulama başarılı olduğunda, makinenin kontrol panelinin kilidi açılır.

İlgili bilgiler

- LDAP Kimlik Doğrulaması Kullanımı

Secure Function Lock 3.0'ı Kullanma

Secure Function Lock 3.0, makinenizdeki kullanılabilir işlevleri kısıtlayarak güvenliği artırır.

Secure Function Lock 3.0 Kullanmadan Önce

Güvenli Fonksiyon Kilidi özelliğini, şifre yapılandırmak, belli kullanıcı sayfa sınırlamaları belirlemek ve burada listelenen işlevlerin bazılarına veya tümüne erişim vermek amacıyla kullanın.

Aşağıdaki Secure Function Lock (Güvenli İşlev Kilidi) 3.0 ayarlarını, Web Tabanlı Yönetim'i kullanarak yapılandırabilir ve değiştirebilirsiniz:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

- **Print (Yazdır)**
- **Copy (Kopyalama)**
- **Scan (Tara)**
- **Fax (Faks)**
- **Media (Ortam)**
- **Web Connect (Web Bağlantısı)**
- **Apps (Uygulamalar)**
- **Page Limits (Sayfa Sınırı)**
- **Page Counters (Sayfa Sayaçları)**
- **Card ID (NFC ID) (Kart Kimliği (NFC Kimliği))**

Dokunmatik ekranlı LCD modeller:

Secure Function Lock (Güvenli İşlev Kilidi) etkinleştirildiğinde, makine otomatik olarak Ortak Moda girer ve makinenin bazı işlevleri yalnızca authorized kullanıcılarla kısıtlanır. Kısıtlanmış makine işlevlerine erişim için öğesine basın, kullanıcı adınızı seçin ve şifrenizi girin.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Secure Function Lock 3.0 Ayarlarını Web Tabanlı Yönetim'i Kullanarak Yapılandırma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **User Restriction Function (Kullanıcı Kısıtlama İşlevi)** veya **Restriction Management (Kısıtlama Yönetimi)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Secure Function Lock (Güvenli İşlev Kilidi)** öğesini seçin.
6. **Submit (Gönder)** öğesine tıklayın.
7. **Restricted Functions (Kısıtlı İşlevler)** menüsüne tıklayın.
8. Kullanıcı veya grup başına kısıtlamaları yönetmek için ayarları yapılandırın.
9. **Submit (Gönder)** öğesine tıklayın.
10. **User List (Kullanıcı Listesi)** menüsüne tıklayın.
11. Kullanıcı Listesini Yapılandırın.
12. **Submit (Gönder)** öğesine tıklayın.

Ayrıca, **Secure Function Lock (Güvenli İşlev Kilidi)** menüsünde kullanıcı listesi kilitleme ayarlarını da değiştirebilirsiniz.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Secure Function Lock 3.0 Kullanarak Tarama

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

Tarama kısıtlamalarının ayarlanması (yöneticiler için)

Secure Function Lock (Güvenli İşlev Kilidi) 3.0 sayesinde yönetici hangi kullanıcıların tarama yapmasına izin verileceğini kısıtlayabilir. Tarama özelliği ortak kullanıcı ayarı için Kapalı olarak ayarlandığında, sadece **Scan (Tara)** onay kutusu seçili olan kullanıcılar tarama yapabilecektir.

Tarama özelliğini kullanma (kısıtlı kullanıcılar için)

- Makinenin kontrol panelini kullanarak taramak için:

  Kısıtlı kullanıcılar, Tarama moduna erişim sağlamak için makinenin kontrol panelinde şifrelerini girmelidir.
- Bilgisayardan tarama yapma:

  Kısıtlı kullanıcılar bilgisayarlarından tarama yapmadan önce makinenin kontrol panelinde şifrelerini girmelidir. Makinenin kontrol paneline şifre girilmezse, kullanıcının bilgisayarında bir hata mesajı görüntülenir.

Makine IC kartı kimlik doğrulama yöntemini destekliyorsa, kısıtlı kullanıcılar da kayıtlı IC kartları ile makinenin kontrol panelindeki NFC sembolüne dokunarak Tarama moduna erişebilir.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Güvenli İşlev Kilidi 3.0 için Ortak Modu Yapılandırma

Secure Function Lock (Güvenli İşlev Kilidi) ekranınndan ortak kullanıcıların kullanabileceği işlevleri kısıtlayan Ortak Mod'u ayarlayın. Ortak kullanıcıların, Ortak Mod'la kullanılabilir hale getirilen özelliklere erişmek için şifre girmelerine gerek yoktur.

Ortak Mod, Brother iPrint&Scan ve Brother Mobile Connect üzerinden gönderilen yazdırma işlerini içerir.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **User Restriction Function (Kullanıcı Kısıtlama İşlevi)** veya **Restriction Management (Kısıtlama Yönetimi)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Secure Function Lock (Güvenli İşlev Kilidi)** öğesini seçin.
6. **Submit (Gönder)** öğesine tıklayın.
7. **Restricted Functions (Kısıtlı İşlevler)** menüsüne tıklayın.
8. **Public Mode (Ortak Modu)** satırında, listelenen işleve izin vermek için bir onay kutusunu işaretleyin, kısıtlamak için onay kutusunun işaretini kaldırın.
9. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Kişisel Ana Ekran Ayarlarını Web Tabanlı Yönetim Kullanarak Yapılandırma

Bir Yönetici olarak, kullanıcıların bireysel ana ekranlarında hangi sekmeleri göreceğini belirtebilirsiniz. Bu sekmeler, kullanıcıların makinenin kontrol panelinden kişisel ana sayfalarına atayabilecekleri favorite kısayollarına hızlıca erişebilmesini sağlar.

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **User Restriction Function (Kullanıcı Kısıtlama İşlevi)** veya **Restriction Management (Kısıtlama Yönetimi)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Secure Function Lock (Güvenli İşlev Kilidi)** öğesini seçin.
6. **Tab Settings (Sekme Ayarları)** alanında, kişisel ana ekranınız olarak kullanmak istediğiniz sekme adları için **Personal (Kişisel)** öğesini seçin.
7. **Submit (Gönder)** öğesine tıklayın.
8. **Restricted Functions (Kısıtlı İşlevler)** menüsüne tıklayın.
9. Kullanıcı veya grup başına kısıtlamaları yönetmek için ayarları yapılandırın.
10. **Submit (Gönder)** öğesine tıklayın.
11. **User List (Kullanıcı Listesi)** menüsüne tıklayın.
12. Kullanıcı Listesini Yapılandırın.
13. Her kullanıcı için açılır listeden **User List / Restricted Functions (Kullanıcı Listesi / Kısıtlı İşlevler)** öğesini seçin.
14. Her kullanıcı için **Home Screen (Başlangıç Ekranı)** açılır listesinden sekme adını seçin.
15. **Submit (Gönder)** öğesine tıklayın.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Diğer Secure Function Lock 3.0 Özellikleri

Güvenli Fonksiyon Kilidi ekranında aşağıdaki özellikleri yapılandırın:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

All Counter Reset (Tüm Sayacı Sıfırla)

Sayfa sayacını sıfırlamak için **Page Counters (Sayfa Sayaçları)** sütunundaki **All Counter Reset (Tüm Sayacı Sıfırla)** öğesini tıklatın.

Export to CSV file (CSV dosyasına gönder)

User List / Restricted Functions (Kullanıcı Listesi / Kısıtlı İşlevler) bilgisi dahil geçerli ve son sayfa sayacını bir CSV dosyası olarak dışa aktarmak için **Export to CSV file (CSV dosyasına gönder)** öğesine tıklayın.

Card ID (NFC ID) (Kart Kimliği (NFC Kimliği))

User List (Kullanıcı Listesi) menüsüne tıklayın ve ardından bir kullanıcının Kart Kimliğini **Card ID (NFC ID) (Kart Kimliği (NFC Kimliği))** alanına yazın. IC kartınızı kimlik doğrulama için kullanabilirsiniz.

Output (Çıkış)

Posta Kutusu ünitesi makinenize takıldığında, açılır listeden her kullanıcı için çıkış çekmecesini seçin.

Last Counter Record (Son Sayaç Kaydı)

Sayaç sıfırlandıktan sonra makinenin sayfa sayısını tutmasını istiyorsanız **Last Counter Record (Son Sayaç Kaydı)** öğesini tıklatın.

Counter Auto Reset (Sayaç Oto Sıfırlama)

Sayfa sayacı sıfırlama işlemleri arasındaki zaman aralığını yapılandırmak için **Counter Auto Reset (Sayaç Oto Sıfırlama)** öğesini tıklatın. Zaman aralığını günlük, haftalık veya aylık olarak seçin.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Makinenin Kontrol Panelini Kullanarak Yeni Bir IC Kartını Kaydetme

Makinenize Entegre Devre Kartları (IC Kartları) kaydedebilirsiniz.

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

1. Kayıtlı bir Entegre Devre Kartı (IC Kartı) ile makinenin kontrol panelindeki Yakın Alan İletişimi (NFC) sembolüne dokunun.
2. LCD'de kullanıcı kimliğinize basın.
3. Kartı Kaydet düğmesine basın.
4. Yeni bir IC Kartını NFC sembolüne dokundurun.

   Ardından yeni IC Kartının numarası makineye kaydedilir.
5. Tamam düğmesine basın.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Harici IC Kart Okuyucuyu Kaydetme

Harici IC (Entegre Devre) kart okuyucusu bağlandığında, kart okuyucuyu kaydetmek için Web Tabanlı Yönetim'i kullanın. Makineniz, harici IC kart okuyucularını destekleyen HID sınıfı sürücüsünü destekler.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **External Card Reader (Harici Kart Okuyucu)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. Gerekli bilgileri girin ve ardından **Submit (Gönder)** öğesine tıklayın.
6. Yapılandırmayı etkinleştirmek için Brother makinenizi yeniden başlatın.
7. Kart okuyucuyu makinenize bağlayın.
8. Kart kimlik doğrulamasını kullanırken kartı kart okuyucuya dokundurun.

İlgili bilgiler

- Secure Function Lock 3.0'ı Kullanma

Güvenli Şekilde E-Posta Gönderme ve Alma

Web Tabanlı Yönetim'i Kullanarak E-posta Göndermeyi veya Almayı Yapılandırma

- E-posta Alma yalnızca belirli modeller için kullanılabilir.
- Kullanıcı kimliği doğrulama ile güvenli e-posta gönderimini veya SSL/TLS kullanarak (yalnızca desteklenen modeller) e-posta gönderimi ve alımını yapılandırmak için Web Tabanlı Yönetim kullanımını öneririz.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

   Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.
4. Sol gezinme çubuğunda **Network (Ağ)** > **Network (Ağ)** > **Protocol (Protokol)** öğesine tıklayın.

   Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.
5. alanında, **Advanced Settings (Gelişmiş ayarlar)** öğesini tıklatın ve **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP İstemcisi)** durumunun **Enabled (Etkinleştirildi)** şeklinde olduğundan emin olun.**POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP İstemcisi)**

   - Kullanılabilir protokoller makinenize bağlı olarak farklılık gösterebilir.
   - **Authentication Method (Kimlik Doğrulama Yöntemi)** seçim ekranı görüntülenirse, kimlik doğrulama yönteminizi seçin ve ardından ekran talimatlarını izleyin.
6. **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP İstemcisi)** ayarlarını yapılandırın.
   - Yapılandırmadan sonra bir deneme e-postası göndererek, e-posta ayarlarının doğru olduğunu onaylayın.
   - POP3/IMAP4/SMTP sunucu ayarlarını bilmiyorsanız, ağ yöneticinize veya Internet Servis Sağlayıcınıza (ISS) başvurun.
7. Bittiğinde, **Submit (Gönder)** öğesini tıklatın.

   Test Send/Receive E-mail Configuration (E-posta Gönderme/Alma Yapılandırmasını Test Et) iletişim kutusu görünür.
8. Geçerli ayarları test etmek için iletişim kutusundaki talimatları izleyin.

İlgili bilgiler

- Güvenli Şekilde E-Posta Gönderme ve Alma

İlgili konular:

- SSL/TLS Kullanarak Güvenli Şekilde E-posta Gönderme veya Alma

Kullanıcı Kimliği Doğrulama ile E-posta Gönderme

Makineniz, kullanıcı kimliği doğrulaması gerektiren bir e-posta sunucusu yoluyla e-posta gönderir. Bu yöntem, unauthorized kullanıcıların e-posta sunucusuna erişimini engeller.

Kullanıcı kimlik doğrulamasını kullanarak e-posta bildirimi, e-posta raporları ve I-Fax (yalnızca belirli modellerde mevcuttur) gönderebilirsiniz.

- Kullanılabilir protokoller makinenize bağlı olarak farklılık gösterebilir.
- SMTP kimlik doğrulamasını yapılandırmak için Web Tabanlı Yönetim'i kullanmanızı öneririz.

E-posta Sunucusu Ayarları

Makinenizin SMTP kimlik doğrulama yöntemini, e-posta sunucunuz tarafından kullanılan yöntemle eşleşecek şekilde yapılandırmanız gerekir. E-posta sunucusu ayarlarınız hakkında ayrıntılar için ağ yöneticinize veya İnternet Servis Sağlayıcınıza (ISP) başvurun.

Web Tabanlı Yönetim'i kullanarak SMTP sunucusu kimlik doğrulamasını etkinleştirmek için **Server Authentication Method (Sunucu Kimlik Doğrulaması Yöntemi)** altında ve **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP İstemcisi)** ekranında kimlik doğrulama yönteminizi seçin.

İlgili bilgiler

- Güvenli Şekilde E-Posta Gönderme ve Alma

SSL/TLS Kullanarak Güvenli Şekilde E-posta Gönderme veya Alma

Makineniz SSL/TLS iletişim yöntemlerini destekler. SSL/TLS iletişimini kullanan bir e-posta sunucusunu kullanmak için aşağıdaki ayarları yapılandırmanız gerekir.

- E-posta Alma yalnızca belirli modeller için kullanılabilir.
- SSL/TLS yapılandırması için Web Tabanlı Yönetim'i kullanmanızı öneririz.

Sunucu Sertifikasını Doğrulama

SSL/TLS altında, **SSL** veya **TLS** öğesini seçerseniz **Verify Server Certificate (Sunucu Sertifikasını Doğrula)** onay kutusu otomatik seçilecektir.

- Sunucu sertifikasını doğrulamadan önce, sunucu sertifikasını imzalayan CA tarafından yayınlanan CA sertifikasını içe aktarmanız gerekir. Bir CA sertifikası alma gerekiyorsa onaylamak için ağ yöneticinize veya Internet Servis Sağlayıcı'nıza (ISS) başvurun.
- Sunucu sertifikasını doğrulamanız gerekmiyorsa **Verify Server Certificate (Sunucu Sertifikasını Doğrula)** onay kutusunun işaretini kaldırın.

Bağlantı Noktası Numarası

SSL veya **TLS** öğesini seçerseniz, **Port (Bağlantı Noktası)** değeri protokolle eşleşecek şekilde değişecektir. Bağlantı noktası numarasını manuel olarak değiştirmek için **SSL/TLS** ayarlarını seçtikten sonra bağlantı noktası numarasını yazın.

Makinenizin iletişim yöntemini, e-posta sunucunuz tarafından kullanılan yöntemle eşleşecek şekilde yapılandırmanız gerekir. E-posta sunucunuzun ayarları hakkında ayrıntılar için ağ yöneticinize veya ISP'nize başvurun.

Pek çok durumda, güvenli web postası hizmetleri aşağıdaki ayarları gerektirir:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

SMTP	**Port (Bağlantı Noktası)**	587
	Server Authentication Method (Sunucu Kimlik Doğrulaması Yöntemi)	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port (Bağlantı Noktası)**	995
	SSL/TLS	**SSL**
IMAP4	**Port (Bağlantı Noktası)**	993
	SSL/TLS	**SSL**

İlgili bilgiler

- Güvenli Şekilde E-Posta Gönderme ve Alma

İlgili konular:

- Web Tabanlı Yönetim'i Kullanarak E-posta Göndermeyi veya Almayı Yapılandırma
- Aygıt Güvenliği için Sertifikaları Yapılandırma

Yazdırma Günlüğünü Ağa Depolama

Yazdırma Günlüğünü Ağa Kaydetmeye Genel Bakış

Yazdırma Günlüğünü Ağa Depolama özelliği, Ortak İnternet Dosya Sistemi (CIFS) protokolü kullanarak yazdırma günlüğü dosyasını makinenizden bir ağ sunucusuna kaydetme imkanı sağlar. Her yazdırma işi için Kimliği, yazdırma işi tipini, iş adını, kullanıcı adını, tarihi, saati ve yazdırılan sayfa sayısını kaydedebilirsiniz. CIFS, bir ağdaki bilgisayarların bir intranet veya İnternet üzerinden dosya paylaşmasına izin vererek TCP/IP üzerinden çalışan bir protokoldür.

Aşağıdaki yazdırma fonksiyonları, yazdırma günlüğüne kaydedilir:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

- Bilgisayarınızdaki yazdırma işleri
- Doğrudan USB'den Yazdırma
- Kopyalama
- Alınan Faks
- Web Connect Yazdırma

- Yazdırma Günlüğünü Ağa Depolama özelliği, Kerberos kimlik doğrulamasını ve NTLMv2 kimlik doğrulamasını destekler. Kimlik doğrulaması için kontrol panelinde SNTP protokolünü (ağ zaman sunucusu) yapılandırmanız veya tarih, saat ve saat dilimini doğru ayarlamanız gerekir.
- Sunucuya bir dosya depolarken dosya tipini TXT veya CSV olarak ayarlayabilirsiniz.

İlgili bilgiler

- Yazdırma Günlüğünü Ağa Depolama

Web Tabanlı Yönetim ile Yazdırma Günlüğünü Ağa Depolama Ayarlarını Yapılandırma

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın ("makinenin IP adresi", makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **Store Print Log to Network (Baskı Kaydını Ağa Depola)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Print Log (Günlük Yazdır)** alanında, **On (Açık)** öğesini tıklatın.
6. Aşağıdaki ayarları yapılandırın:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

Seçenek	Açıklama
Network Folder Path (Ağ Klasörü Yolu)	Yazdırma günlüğünüzün CIFS sunucusunda kaydedileceği hedef klasörü belirtin (örneğin: \\ComputerName\SharedFolder).
File Name (Dosya Adı)	Yazdırma günlüğü için kullanmak istediğiniz dosya adını (32 karaktere kadar) girin.
File Type (Dosya Türü)	Yazdırma günlüğü dosya tipi için **TXT** veya **CSV** öğesini seçin.
Time Source for Log (Günlük için Zaman Kaynağı)	Yazdırma günlüğü için zaman kaynağını seçin.
Auth. Method (Kimlik Doğrulama Yöntemi)	CIFS sunucusuna erişmek için gereken kimlik doğrulama yöntemini seçin: **Auto (Otomatik)**, **Kerberos** veya **NTLMv2**. Kerberos, aygıtların veya kişilerin kimliklerini ağ sunucularına tek bir kayıt işlemiyle güvenli bir şekilde kanıtlamalarını sağlayan bir kimlik doğrulama protokolüdür. NTLMv2, Windows tarafından sunuculara oturum açmak için kullanılan kimlik doğrulama yöntemidir. • **Auto (Otomatik)**: **Auto (Otomatik)** öğesini seçerseniz, NTLMv2, kimlik doğrulama yöntemini kullanacaktır. • **Kerberos**: Yalnızca Kerberos kimlik doğrulamasını kullanmak için **Kerberos** öğesini seçin. • **NTLMv2**: Yalnızca NTLMv2 kimlik doğrulamasını kullanmak için **NTLMv2** öğesini seçin.

Seçenek	Açıklama
	• **Kerberos** ve **NTLMv2** kimlik doğrulaması için, **Date&Time (Tarih ve Saat)** ayarlarını veya SNTP protokolünü (ağ zaman sunucusu) ve DNS sunucusunu da yapılandırmanız gerekir. • Tarih ve Saat ayarlarını makinenin kontrol panelinden de yapılandırabilirsiniz.
Username (Kullanıcı Adı)	Kimlik doğrulaması için kullanıcı adını yazın (en fazla 96 karakter). Kullanıcı adı etki alanının bir parçasıysa, aşağıdaki stillerden birinde kullanıcı adını girin: user@domain veya domain\user.
Password (Şifre)	Kimlik doğrulama için şifreyi girin (en fazla 32 karakter).
Kerberos Server Address (Kerberos Sunucusu Adresi) (gerekirse)	Şifre Dağıtım Merkezi (KDC) ana makine adresini (örneğin: kerberos.example.com; 64 karaktere kadar) veya IP adresini (örneğin: 192.168.56.189) girin.
Error Detection Setting (Hata Algılama Ayarı)	Ağ hatası nedeniyle sunucuda yazdırma günlüğü depolanamadığında hangi işlemin yapılacağını seçin.

7. **Connection Status (Bağlantı Durumu)** alanında, son günlüğe alma durumunu onaylayın.

Makinenizin LCD'sindeki hata durumunu da onaylayabilirsiniz.

8. **Test Print Log to Network (Yazdırma Günlüğünü Ağda Test Etme)** sayfasını görüntülemek için **Submit (Gönder)** öğesine tıklayın.

   Ayarlarınızı test etmek için, **Yes (Evet)** öğesine tıklayın ve ardından sonraki adıma gidin.

   Testi atlamak için **No (Hayır)** öğesine tıklayın. Ayarlarınız otomatik olarak gönderilecektir.
9. Makine ayarlarınızı test edecektir.
10. Ayarlarınız kabul edilirse, ekranda **Test OK (Deneme Tamam)** görünür.

    Test Error (Deneme Hatası) öğesi görünürse, tüm ayarları kontrol edin ve ardından **Submit (Gönder)** öğesine tıklayarak Test sayfasını tekrar görüntüleyin.

İlgili bilgiler

- Yazdırma Günlüğünü Ağa Depolama

Yazdırma Günlüğünü Ağa Depolama Hata Algılama Ayarını Kullanma

Yazdırma günlüğü ağ hatası nedeniyle sunucuya depolanamadığında yapılması gereken eylemi belirlemek için Hata Algılama Ayarlarını kullanın.

1. Web tarayıcınızı başlatın.
2. Tarayıcınızın adres çubuğuna "https://makinenin IP adresi" yazın (“makinenin IP adresi”, makinenizin IP adresidir).

   Örneğin:

   https://192.168.1.2

   Makinenizin IP adresi Ağ Yapılandırma Raporunda bulunabilir.
3. Gerekirse, **Login (Oturum Aç)** alanına şifreyi yazın ve ardından **Login (Oturum Aç)** öğesine tıklayın.

Bu makinenin ayarlarını yönetmeye yönelik varsayılan şifre makinenin arkasında bulunur ve "**Pwd**" olarak işaretlidir. İlk oturum açtığınızda ekran talimatlarını izleyerek varsayılan şifreyi değiştirin.

4. Sol gezinme çubuğunda **Administrator (Yönetici)** > **Store Print Log to Network (Baskı Kaydını Ağa Depola)** öğesine tıklayın.

Sol gezinme çubuğu görülmüyorsa, gezinmeye ☰ öğesinden başlayın.

5. **Error Detection Setting (Hata Algılama Ayarı)** bölümünde, **Cancel Print (Baskıyı İptal et)** veya **Ignore Log & Print (Günlüğe Almayı Yoksay ve Yazdır)** öğesini seçin.

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

Seçenek	Açıklama
Cancel Print (Baskıyı İptal et)	**Cancel Print (Baskıyı İptal et)** seçeneğini seçerseniz, yazdırma günlüğü sunucuda depolanamadığında yazdırma işleri canceled. **Cancel Print (Baskıyı İptal et)** öğesini seçseniz bile makineniz alınan bir faksı yazdıracaktır.

Ignore Log & Print (Günlüğe Almayı Yoksay ve Yazdır)	**Ignore Log & Print (Günlüğe Almayı Yoksay ve Yazdır)** öğesini seçerseniz, yazdırma günlüğü sunucuda depolanamasa dahi makine belgeyi yazdırır.
	Yazdırma Günlüğünü Depola işlevi kurtarıldığında, yazdırma günlüğü şu şekilde kaydedilir:
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), “Document01.doc”, “user01”, 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), “Document02.doc”, “user01”, 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), “Report01.xls”, “user02”, 03/03/20xx, 19:30:40, 4`
	a. Yazdırma günlüğü, yazdırma işleminin sonunda depolanamazsa, yazdırılan sayfaların sayısı kaydedilmez.
	b. Yazdırma günlüğü yazdırma işleminin başında ve sonunda depolanamıyorsa, işin yazdırma günlüğü kaydedilmeyecektir. İşlev kurtarıldığında, hata yazdırma günlüğünde gösterilir.

6. **Test Print Log to Network (Yazdırma Günlüğünü Ağda Test Etme)** sayfasını görüntülemek için **Submit (Gönder)** öğesine tıklayın.

   Ayarlarınızı test etmek için, **Yes (Evet)** öğesine tıklayın ve ardından sonraki adıma gidin.

Testi atlamak için **No (Hayır)** öğesine tıklayın. Ayarlarınız otomatik olarak gönderilecektir.

7. Makine ayarlarınızı test edecektir.
8. Ayarlarınız kabul edilirse, ekranda **Test OK (Deneme Tamam)** görünür.

   Test Error (Deneme Hatası) öğesi görünürse, tüm ayarları kontrol edin ve ardından **Submit (Gönder)** öğesine tıklayarak Test sayfasını tekrar görüntüleyin.

İlgili bilgiler

- Yazdırma Günlüğünü Ağa Depolama

Secure Function Lock 3.0 ile Yazdırma Günlüğünü Ağda Depolama Özelliğini Kullanma

Secure Function Lock (Güvenli İşlev Kilidi) 3.0 etkinken, kopyalama, Faks Alma Gönderme, Web Connect Yazdırma ve USB Doğrudan Yazdırma için kayıtlı kullanıcıların adları Yazdırma Günlüğünü Ağda Depola raporuna kaydedilir. Active Directory Kimlik Doğrulaması etkinken, kullanıcı adı Yazdırma Günlüğünü Ağda Depola raporuna kaydedilir:

Desteklenen özellikler, seçenekler ve ayarlar modelinize bağlı olarak farklılık gösterebilir.

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

İlgili bilgiler

- Yazdırma Günlüğünü Ağa Depolama

brother

Brother Earth

www.brotherearth.com

TUR
Sürüm 0