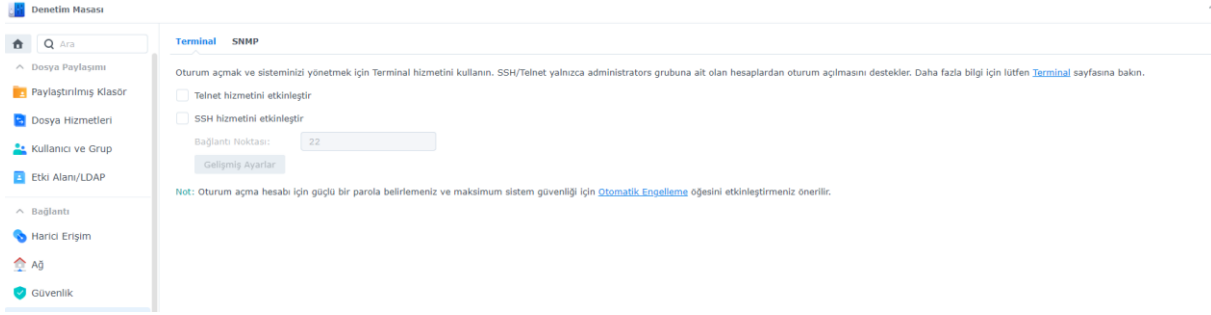


## Synology Terminal Ayarları

**Denetim Masası > Terminal ve SNMP > Terminal'deki** seçeneklerin etkinleştirilmesi , Synology cihazlarınızın Telnet ve SSH komut satırı arabirim hizmetlerini desteklemesini sağlar. SSH şifreleme algoritmasının güvenlik seviyesini de değiştirebilirsiniz.

### Telnet/SSH hizmetini etkinleştirmek için:



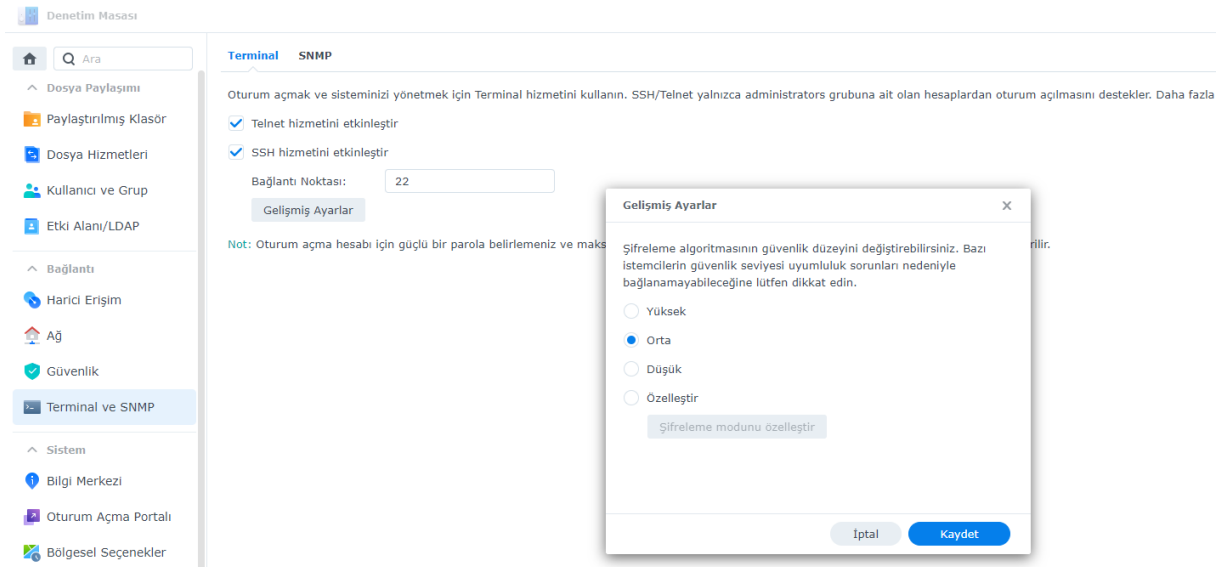
1. İstenen protokolün (SSH veya Telnet) yanındaki kutuyu işaretleyin.
2. **Uygula'yı** tıklayın .

### SSH servis portunu değiştirmek için:

1. **Bağlantı Noktası** alanına yeni bir bağlantı noktası numarası girin .
2. **Uygula'yı** tıklayın .

SSH bağlantılarının güvenliğini sağlamak için farklı güvenlik seviyelerine sahip çeşitli şifreleme algoritmaları kullanılmaktadır. İhtiyaçlarınızı en iyi şekilde karşılamak için hangi algoritmaların kullanılacağına karar verebilirsiniz.

### SSH şifreleme algoritması güvenlik seviyesini değiştirmek için:



- **Gelişmiş Ayarlar** 'ı tıklayın .

Şifreleme algoritmaları için bir güvenlik seviyesi seçin. Tam olarak hangi algoritmaların kullanılabileceğini belirtmek istiyorsanız, üç grup arasından seçim yapmak için **Özelleştir**'i seçin: Şifre, KEX (Anahtar Değişimi) ve MAC (Mesaj Kimlik Doğrulama Kodu).

- **Uygula**'yı tıklayın .

**Not:**

- SSH kullanarak DSM 'de oturum açmak için **Denetim Masası > Terminal ve SNMP > Terminal'de** SSH hizmetini etkinleştirmelisiniz .
- **SSH/Telnet, yalnızca yöneticiler** grubuna ait hesaplarla sisteme giriş yapmayı destekler . Bir **root hesabına geçmek için, lütfen adminler** grubuna ait bir kullanıcı olarak SSH/Telnet ile sisteme giriş yapın, **sudo -i** komutunu çalıştırın ve ardından giriş yapmak için kullanılan hesabın şifresini girin.
- SSH/Telnet ile sisteme giriş yapılırken şifre boş bırakılamaz.
- SSH hizmeti devre dışı bırakıldığında tüm SSH bağlantıları sonlandırılır.
- Synology 'nin ayarlarını uygun olmayan şekilde değiştirilmesi, arızalara veya veri kaybına neden olabilir.

