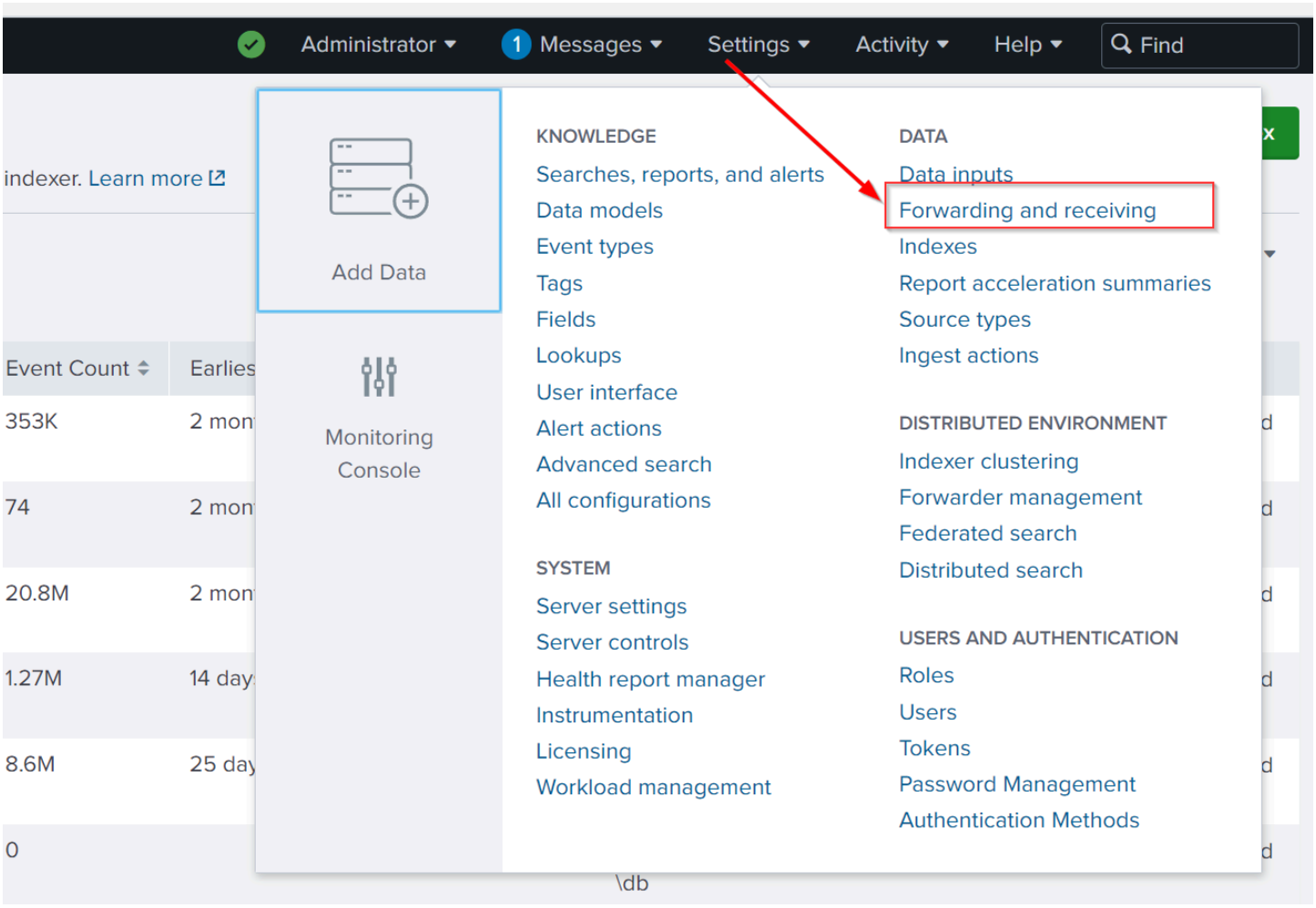
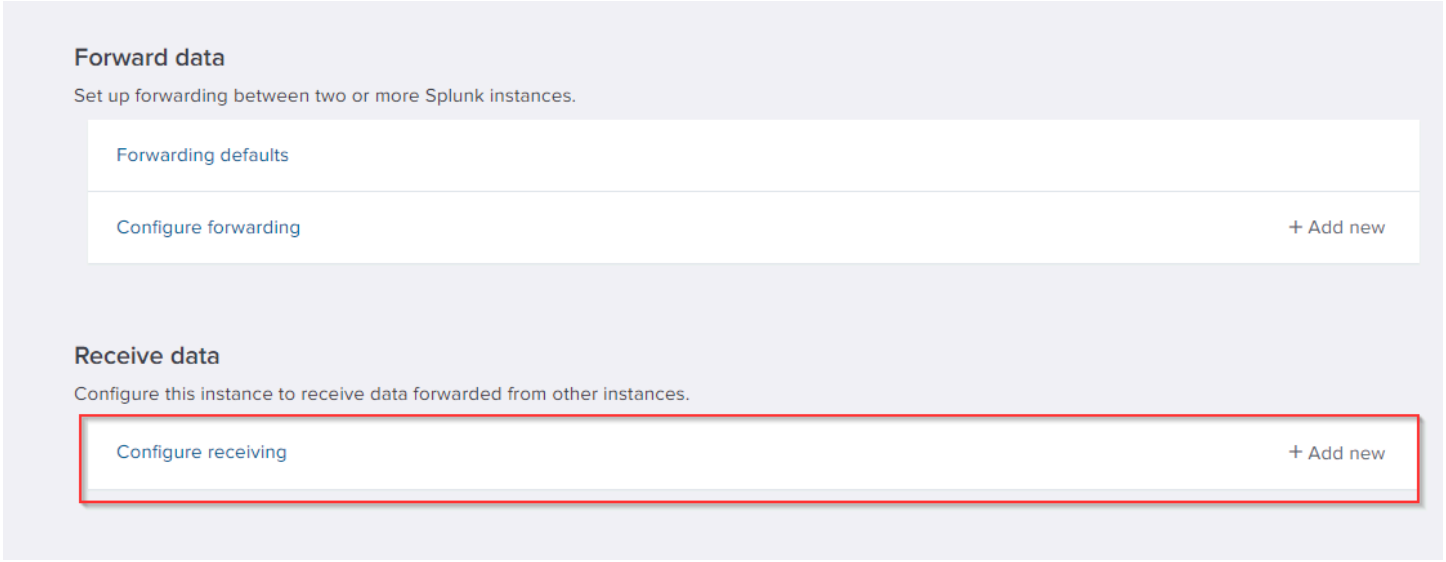
Öncelikle Splunk üzerinde alıcıyı yapılandıracağız, böylece forwarder veriyi nereye göndereceğini bilecek.

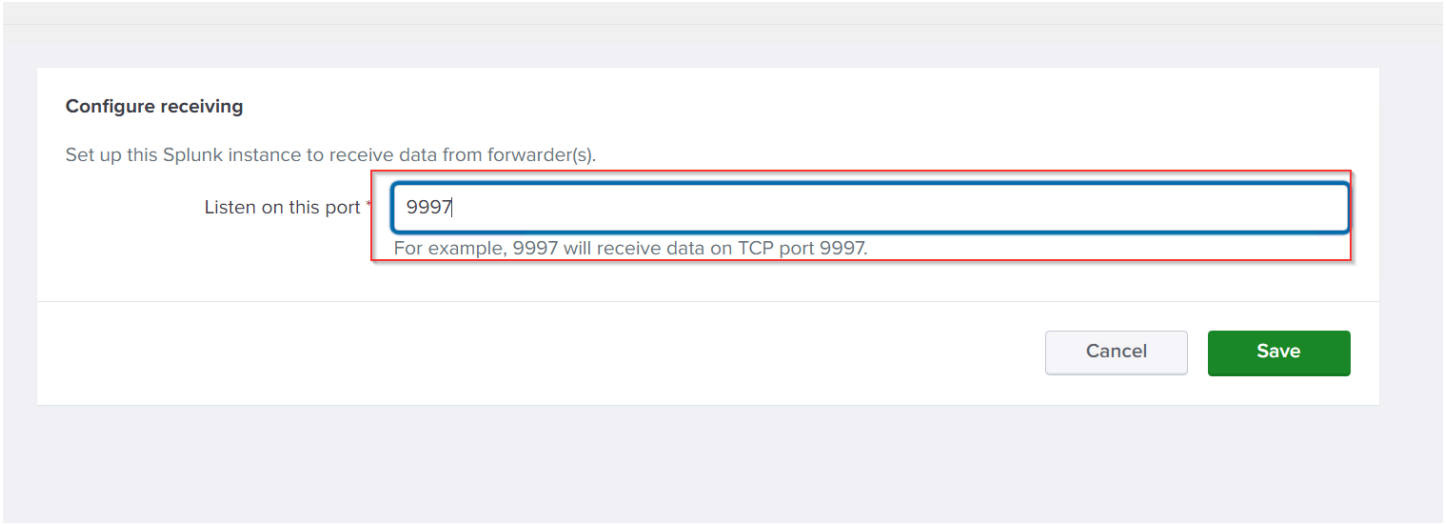
Splunk'a giriş yapın ve aşağıda gösterildiği gibi Ayarlar –> İletme ve alma sekmesine gidin:



Hem yönlendirmeyi hem de almayı yapılandırmak için birden fazla seçenek gösterecektir. Windows Endpoint'ten veri almak istediğimiz için Almayı yapılandır'a tıklayıp ardından yeni bir alma portu yapılandırarak devam edeceğiz.

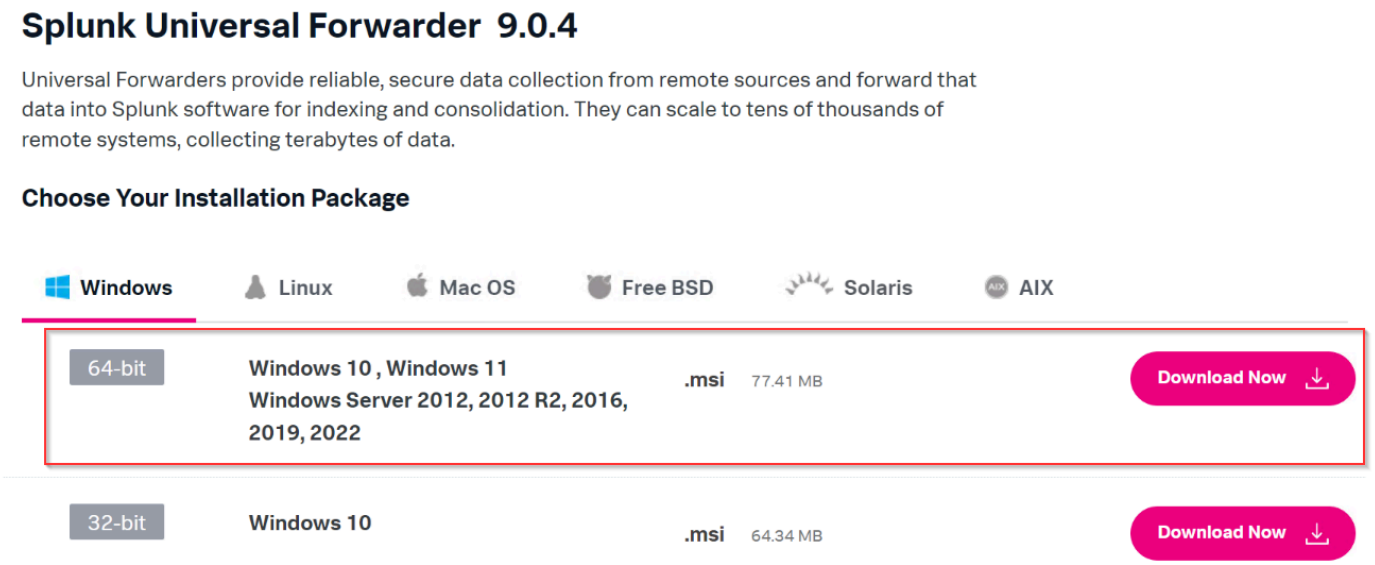


Varsayılan olarak, Splunk örneği verileri 9997 numaralı porttaki yönlendiriciden alır. Bu portu kullanmak veya değiştirmek bize kalmış. Şimdilik, Splunk'ımızı aşağıda gösterildiği gibi 9997 numaralı portta dinlemeye başlayacak şekilde yapılandıracağız ve Kaydedeceğiz:

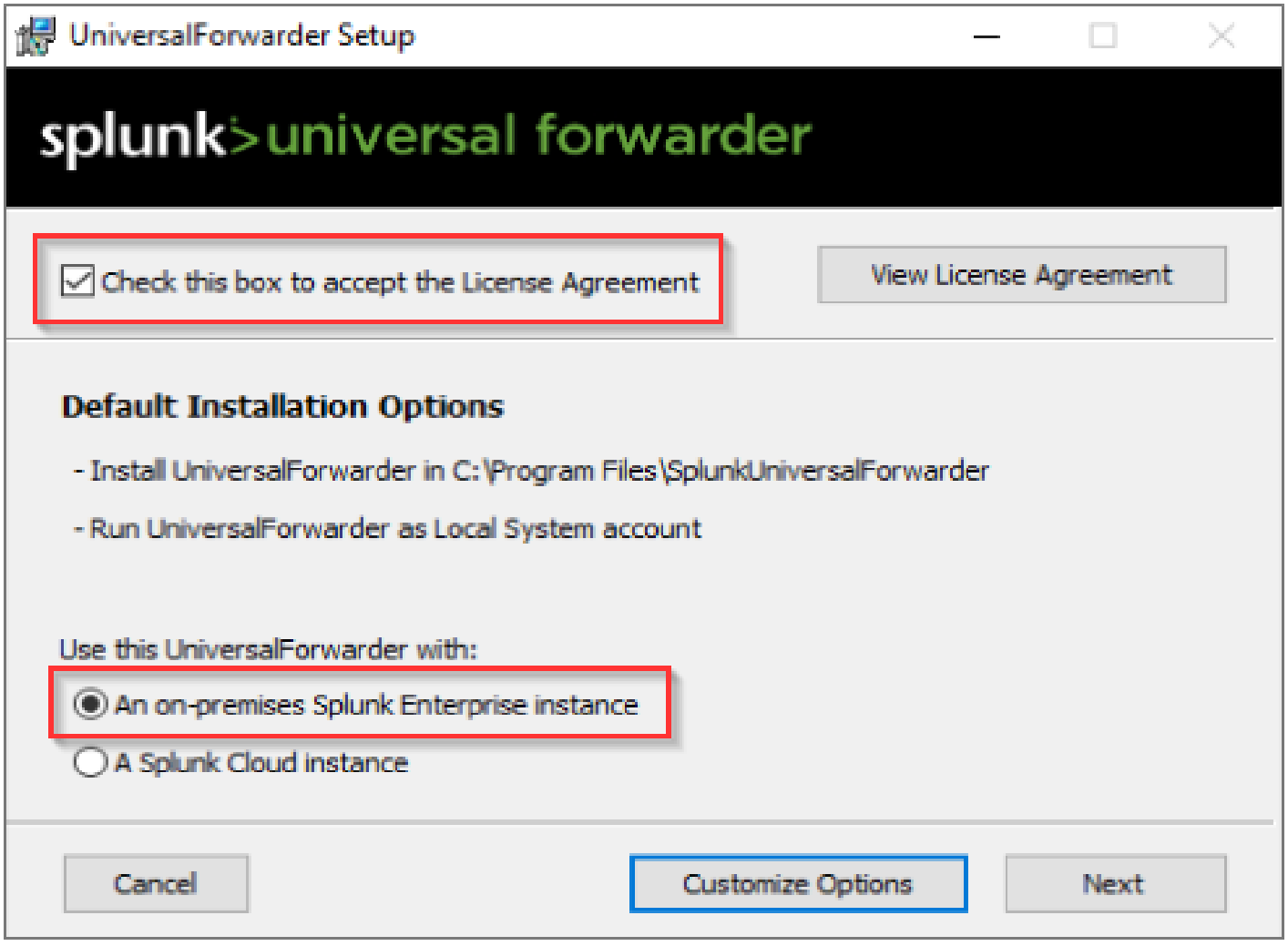


Splunk Forwarder'ı Yükleme

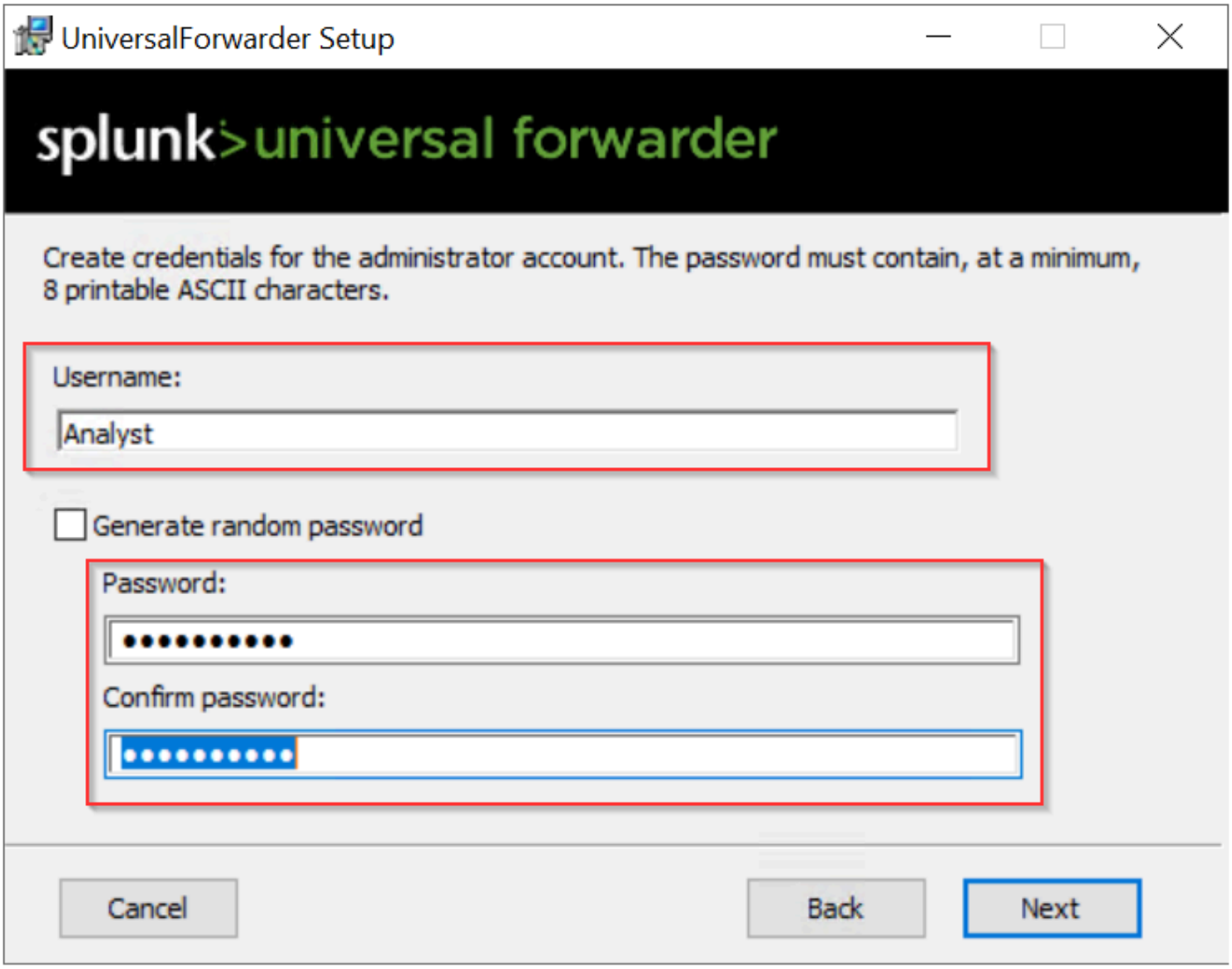
Splunk Forwarder'ı kurmak çok basittir. İlk olarak, resmi web sitesinden en son yönlendiriciyi indireceğiz.



Yükleyiciye tıklayın ve aşağıda gösterildiği gibi Splunk Forwarder'ı yüklemeye başlayın. Lisans Sözleşmesini kabul etmek için Bu kutuyu işaretleyin'i tıklamayı unutmayın.

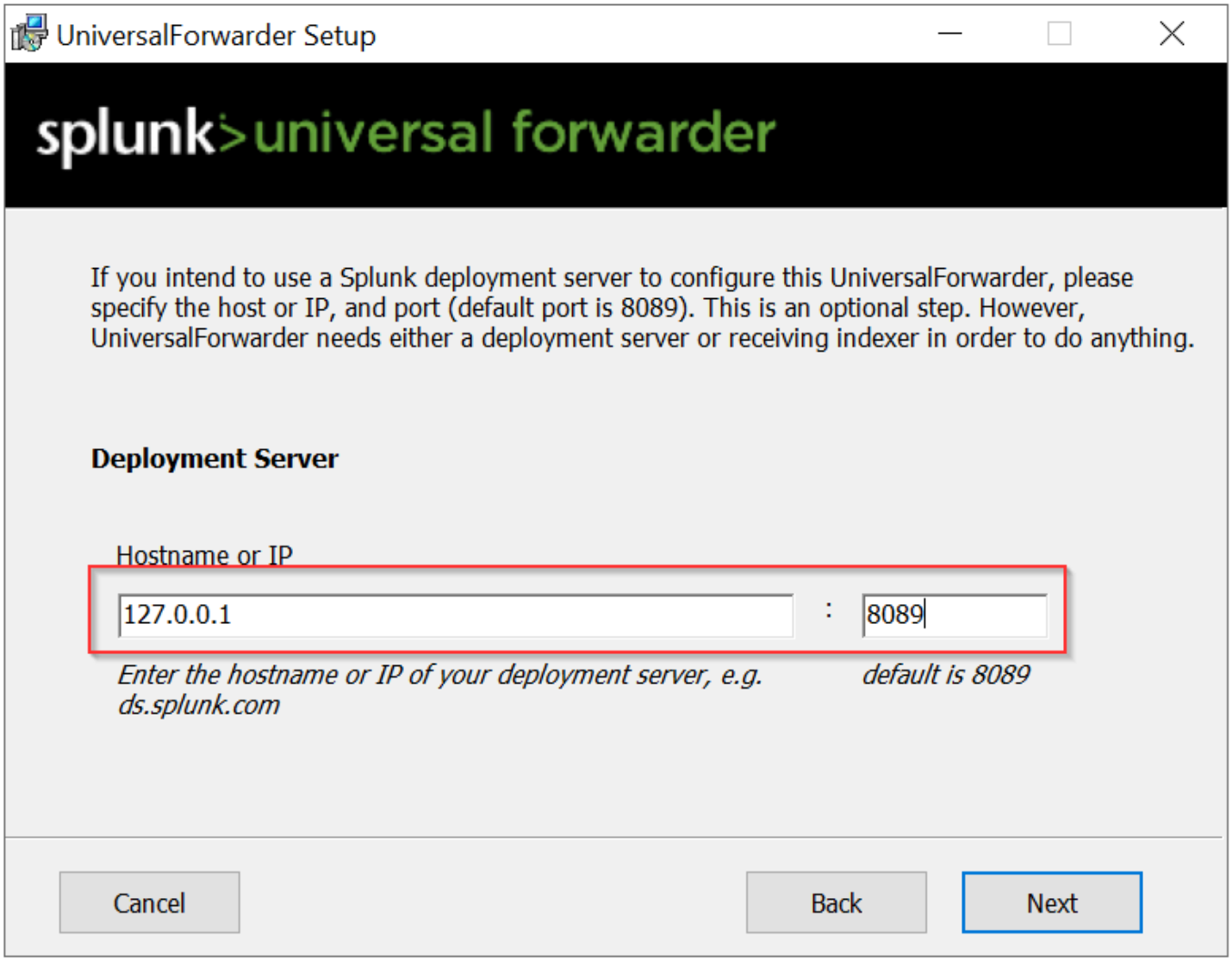


Splunk Forwarder için bir hesap oluşturun. Bu, Splunk forwarder'ı Splunk Indexer'a bağlarken kullanılacaktır.

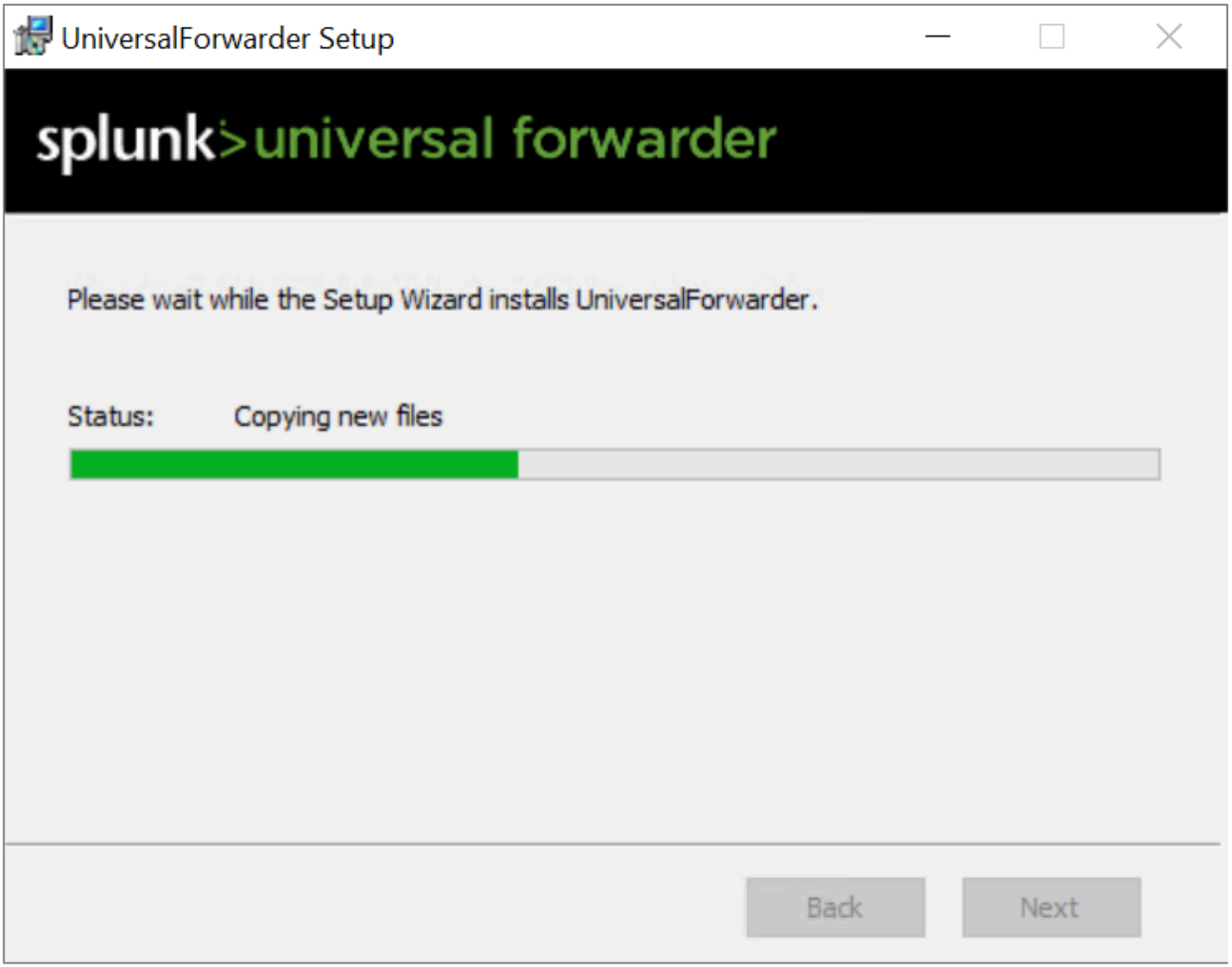


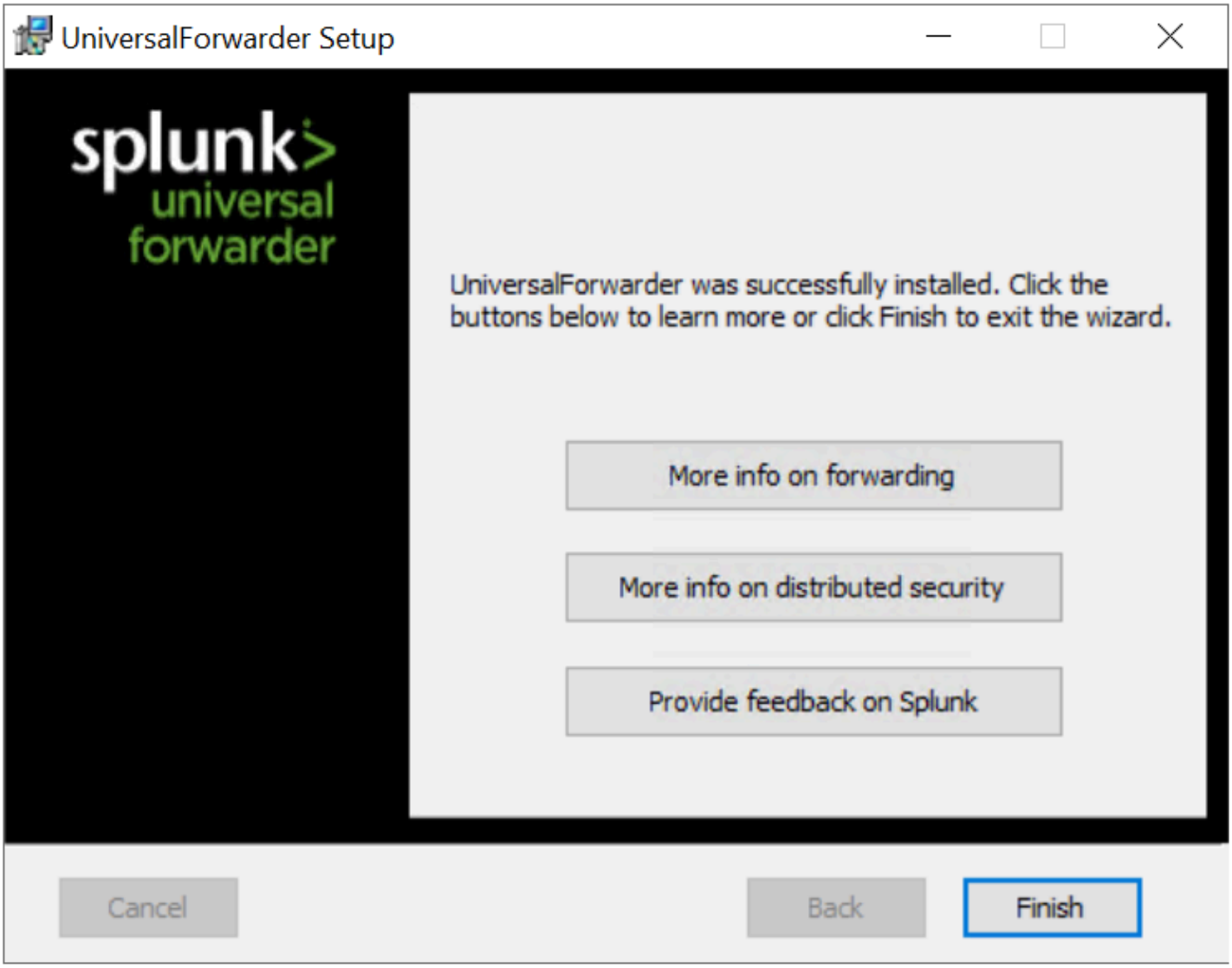
Bu yapılandırma, birden fazla ana bilgisayara Splunk yönlendiricisi kurarsak önemlidir. Bu adım isteğe bağlı olduğundan bu adımı atlayabiliriz.

Varsayılan olarak, Splunk gelen trafik için 9997 portunu dinler.



Yönlendiriciyi Windows uç noktasına yüklemek 3–5 dakika sürecektir.


UniversalForwarder Setup
splunk>universal forwarder
Please wait while the Setup Wizard installs UniversalForwarder.
Status: Copying new files
Back
Next


UniversalForwarder Setup
splunk> universal forwarder
UniversalForwarder was successfully installed. Click the buttons below to learn more or click Finish to exit the wizard.
More info on forwarding
More info on distributed security
Provide feedback on Splunk
Cancel
Back
Finish