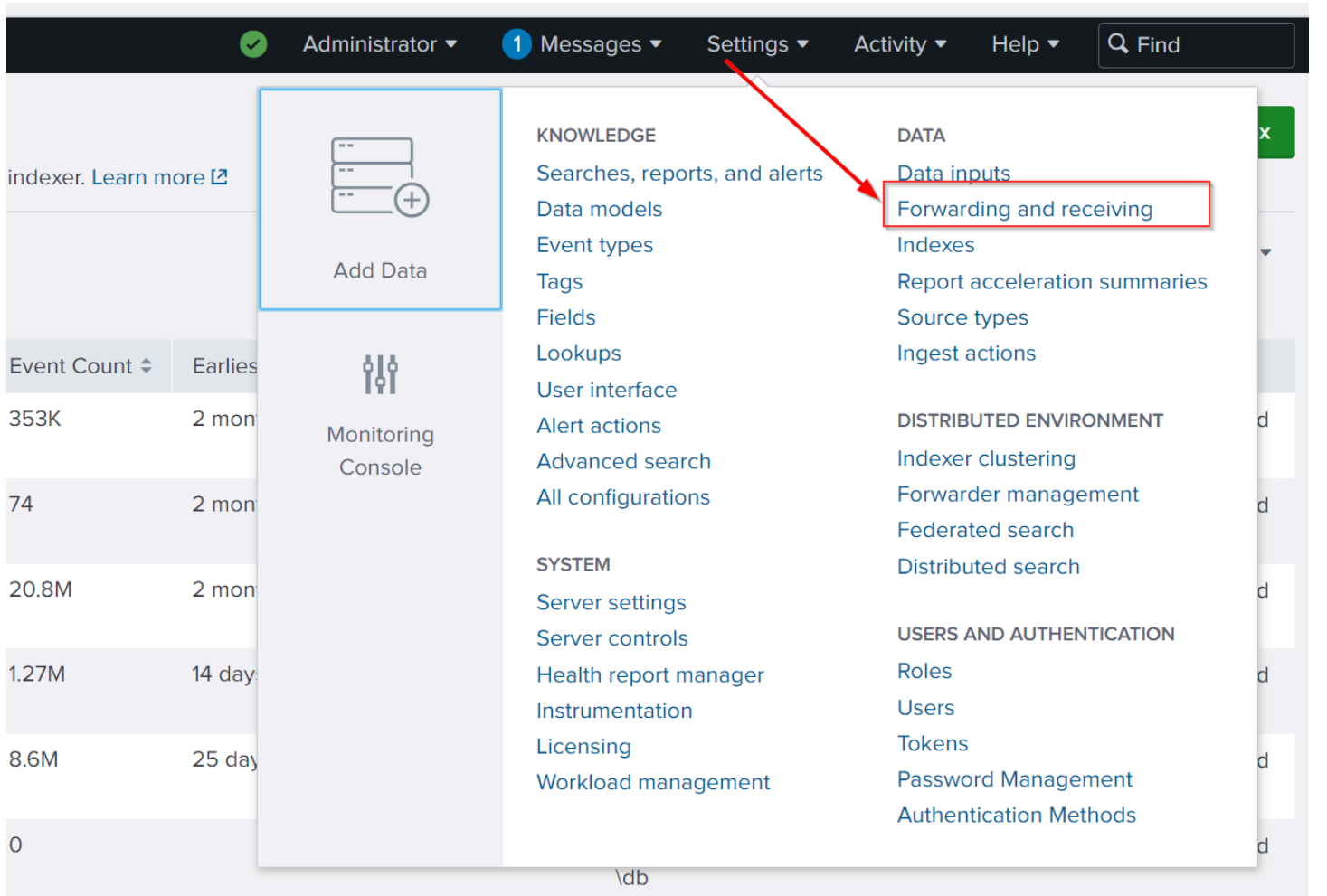


```
d=EST-6&product_id=AV-5B-82" "Opera/9.01 (Windows NT 5.1; U; en)" 1
-01" "Opera/9.01 (Windows NT 5.1; U; en)" 695 130.253.37.97 [05/Mar/
06 195.69.160.22 [05/Mar/2014 18:10:54:192] "GET /cart.do?action=r
ws NT 5.1; SV1)" 163 131.178.233.243 [05/Mar/2014 18:10:54:171] "G
; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 S
on=addtocart&itemId=EST-7&product_id=FI-SW-81" "Mozilla/4.0 (compa
1 "http://buttercup-shopping.com/category.screen?category_id=BOUQUET5" "Mozilla/5.0
1437 "http://buttercup-shopping.com/category.screen?category_id=BOUQUET5" "Mozilla/5.0
FF3ADFF4 HTTP 1.1" 200 363 "http://buttercup-shopping.com/product.i
```

splunk>enterprise

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.

## Forward data

Set up forwarding between two or more Splunk instances.

Forwarding defaults

Configure forwarding

+ Add new

## Receive data

Configure this instance to receive data forwarded from other instances.

Configure receiving

+ Add new

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:

### Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port

9997

For example, 9997 will receive data on TCP port 9997.

Cancel

Save

# Splunk Forwarder'ı Yükleme

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

## Splunk Universal Forwarder 9.0.4

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

### Choose Your Installation Package

Windows

Linux

Mac OS

Free BSD

Solaris

AIX

64-bit

Windows 10 , Windows 11  
Windows Server 2012, 2012 R2, 2016,  
2019, 2022

.msi 77.41 MB

Download Now



32-bit

Windows 10

.msi 64.34 MB

Download Now



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

UniversalForwarder Setup

splunk>universal forwarder

☒ Check this box to accept the License Agreement [View License Agreement](#)

**Default Installation Options**

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

☒ An on-premises Splunk Enterprise instance

☐ A Splunk Cloud instance

Cancel Customize Options Next

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

UniversalForwarder Setup

# splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:  
Analyst

☐ Generate random password

Password:  
●●●●●●●●

Confirm password:  
●●●●●●●●

Cancel Back Next

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.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

### Deployment Server

Hostname or IP

:

*Enter the hostname or IP of your deployment server, e.g. ds.splunk.com* *default is 8089*

Cancel

Back

Next

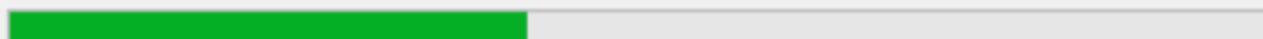
Yönlendiriciyi Windows uç noktasına yüklemek 3–5 dakika sürecektir.



# splunk>universal forwarder

Please wait while the Setup Wizard installs UniversalForwarder.

Status: Copying new files



Back

Next



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