

Kurulum

- Kurulum
- Konfigürasyon

Kurulum

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon> adresinden sysmon indirilir.

Cmd ile indirilen dosya konumuna gidilir ardından Sysmon'u default ayarlarda çalıştırmak için "Sysmon.exe -i -accepteula" komutu girilir.

```
Directory of C:\Users\...Downloads\Sysmon
02.10.2023  10:21    <DIR>          .
02.10.2023  10:21    <DIR>          ..
27.06.2023  16:54             7.490 Eula.txt
27.06.2023  16:55        8.443.704 Sysmon.exe
27.06.2023  16:55        4.548.864 Sysmon64.exe
27.06.2023  16:55        4.989.200 Sysmon64a.exe
            4 File(s)      17.989.258 bytes
            2 Dir(s)  340.618.387.456 bytes free

C:\Users\...Downloads\Sysmon>Sysmon.exe -i -accepteula

System Monitor v15.0 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Sysmon kullanımına ait detayları görmek için Sysmon -h komutu kullanılır.

```
\Downloads\Sysmon>sysmon -h
```

System Monitor v15.0 - System activity monitor

By Mark Russinovich and Thomas Garnier

Copyright (C) 2014-2023 Microsoft Corporation

Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Sysinternals - www.sysinternals.com

Usage:

Install: Sysmon.exe -i [<configfile>]

Update configuration: Sysmon.exe -c [<configfile>]

Install event manifest: Sysmon.exe -m

Print schema: Sysmon.exe -s

Uninstall: Sysmon.exe -u [force]

- c Update configuration of an installed Sysmon driver or dump the current configuration if no other argument is provided. Optionally take a configuration file.
- i Install service and driver. Optionally take a configuration file.
- m Install the event manifest (done on service install as well)).
- s Print configuration schema definition of the specified version. Specify 'all' to dump all schema versions (default is latest)).
- u Uninstall service and driver. Adding force causes uninstall to proceed even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services

Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to accept it.

Neither install nor uninstall requires a reboot.

Konfigürasyon

Sysmon, kurulduğunda kendi konfigürasyon ayarlarına göre kurulum yapar fakat kullanıcılar bu konfigürasyon ayarlarını kendilerine göre düzenleyebilir. Sysmon, konfigürasyon dosyalarını xml biçiminde depolar.

```
<Sysmon schemaversion="3.30">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>

  </EventFiltering>
</Sysmon>
```

Konfigürasyon dosyası için 2 ana bölüm bulunmaktadır.

HashAlgorithms, bölümünde oluşturulan processlerin hangi hash algoritmalarını kullanılacağını belirtmek için kullanılır.

EventFiltering, özellikle izlenilen veya hariç tutulan olayları belirtmek için kullanılır.

Include, olayları dahil etmek için kullanılır. Exclude, olayları hariç tutmak için kullanılır.

```
<tag onmatch="include">
  ...
  ...
</tag>

<tag onmatch="exclude">
  ...
  ...
</tag>
```

Filtrelemede kullanılan tagların listesi aşağıdaki gibi sıralanmıştır.

ProcessCreate	Süreç Oluşturur
ProcessTerminate	İşlem sonlandırır
FileCreateTime	Dosya oluşturma zamanı
NetworkConnect	Ağ bağlantısı kontrolü

DriverLoad	Sürücü yükleme kontrolü
ImageLoad	Resim yükleme kontrolü
CreateRemoteThread	Uzak Konu Oluştur
RawAccessRead	Ham Erişim Okuması

Condition tipleri ve özellikleri:

is	Varsayılan, değerler eşittir
is not	Farklı değerler
contains	Alan bu değeri içeriyor
excludes	Alan bu değeri içermiyor
begin with	Alan bu değerle başlar
end with	Alan bu değerle biter
less than	Sözlükbilimsel karşılaştırma sıfırdan küçüktür
more than	Sözlükbilimsel karşılaştırma sıfırdan büyüktür
image	Bir resim yolunu eşleştirin (tam yol veya yalnızca resim adı)