

# ESETLogCollector - ESET Log Collector - ELC

## Tema

Slanje dnevnika (logova) na analizu radi rješavanja problema.

---

## Uvod

Za potrebe rješavanja problema koji ne spadaju u kategoriju uobičajenih (za koje rješenje možete pronaći u ovoj Bazi znanja) i zahtijevaju dodatnu analizu, potrebne su nam dodatne informacije o stanju naših programa i operacijskog sustava.

---

## Postupak - Kratko (tl;dr)

- preuzmite ili pokrenite odgovarajuće datoteke iz opisa ili članaka u nastavku
  - pošaljite nam kreirane datoteke s logovima ili (ako su veće od 5MB) ih spremite na Microsoft OneDrive ili DropBox ili sl. i pošaljite nam link za preuzimanje
  - ako nemate online-disk, zatražite podatke za upload na naš FTP
- 

## Postupak - Detaljno

Uvijek preuzmite najnoviju verziju alata za prikupljanje logova.

### [1] Windows

Upute se odnose na Windows 7 i novije, uključujući servere.

- Za Windows, preuzmite

[https://download.eset.com/com/eset/tools/diagnosis/log\\_collector/latest/esetlogcollector.exe](https://download.eset.com/com/eset/tools/diagnosis/log_collector/latest/esetlogcollector.exe)

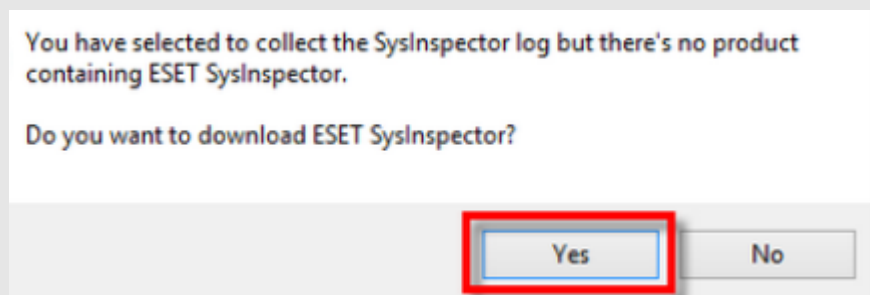
- Pokrenite ga obavezno kao Administrator

(desni klik na datoteku -> "Run as Administrator" / "Pokreni kao Administrator")

○ Ako Windows zatraži lozinku administratora operacijskog sustava, a ne znate ju, zatražite svog

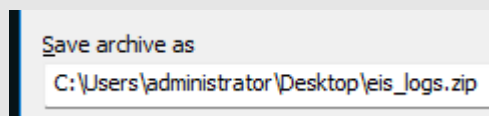
administratora za pomoć

- Ako se pojavi upozorenje UAC-a kliknite na Yes / Da
- Prihvatite Ugovor
- U polju "Collection profile" umjesto standardnog "Default" odaberite "All"
  - Isključite sve stavke koje sadrže "..dumps" osim ako smo se dogovorili da i te logove pošaljete
- U polju "ESET log collection mode" odaberite "Original binary from disk"
- Kliknite na gumb [Collect] i ELC će početi s radom
- U slučaju da je ESET-ov sigurnosni program nekako oštećen ili nije uopće instaliran, ELC će ponuditi da *preuzme i ESET SysInspector, što svakako prihvatite*



1.A. Kreirat će datoteku naziva "ees\_log.zip" ili slično, pa ju stavite na neki svoj online disk (OneDrive, DropBox, ...).

Naziv datoteke će stajati u dijalogu programa, npr.:



Ako ćete logove stavljati na naš FTP – obavezno je zaštitite duljom lozinkom jer je FTP server dostupan svima.

---

## [2] macOS

Pratite ESET-ove upute: <https://support.eset.com/en/kb3404>

---

## [3] Linux

[3.A] Sigurnosni program

Ako je na Linuxu instaliran:

- ESET Endpoint Antivirus for Linux ili
- ESET Server Security for Linux

..pokrenite: [https://help.eset.com/essl/latest/en-US/collect\\_logs.html](https://help.eset.com/essl/latest/en-US/collect_logs.html)

### [3.B] ESET Protect on-prem server (EPX)

Ako se radi o Linuxu

- ESET Protect Virtual Appliance ili
- ESET Protect instaliranom na Linux server

..postavite se u folder “/root” i pokrenite `info_get.command`:

<https://support.eset.com/en/kb6159-run-the-info-getcommand-on-a-linux-virtual-machine-and-send-the-logs-to-eset-technical-support>

Kreirat će datoteku:

3.B.1. `/root/customer_info.tgz`

Na žalost, skripta ne prikuplja sve potrebno, pa dodajte i sljedeće(\*1):

3.B.2. `/var/log/eset/RemoteAdministrator/Era*.log`

3.B.3. `/var/log/tomcat/*`

3.B.4. `/var/opt/eset/RemoteAdministrator/Agent/lastPolicy.dat`

3.B.5. `/etc/opt/eset/*`

3.B.6. `/etc/tomcat/*`

[3.C] Pokrenite i skriptu za Bridge logove:

```
sudo bash /opt/eset/bridge/lib/scripts/collect_logs.sh
```

Kreirat će datoteku:

3.C.1. `/root/bridge_logs.tar.gz`

koju pošaljite zajedno sa 6 paketa iz točke 3.B.

(\*1) Možete si pomoći tako da instalirate ZIP i kreirate ovakvu skriptu (ako pravila firme dopuštaju instalaciju softvera)..

```
yum install zip -y
```

```
zip -vr9 ./customer_info_nort.zip
```

```
/var/log/eset/RemoteAdministrator/Era*.log
```

```
zip -vr9 ./customer_info_nort.zip /var/log/tomcat/*
```

```
zip -vr9 ./customer_info_nort.zip
```

```
/var/opt/eset/RemoteAdministrator/Agent/lastPolicy.dat
```

```
zip -vr9 ./customer_info_nort.zip /etc/opt/eset/*
```

```
zip -vr9 ./customer_info_nort.zip /etc/tomcat/*
```

..koja će sve iz 3.B spremiti u datoteku `"customer_info_nort.zip"`

Za prijenos datoteka Linux <-> Windows možete koristiti WinSCP.

---

## [4] Android

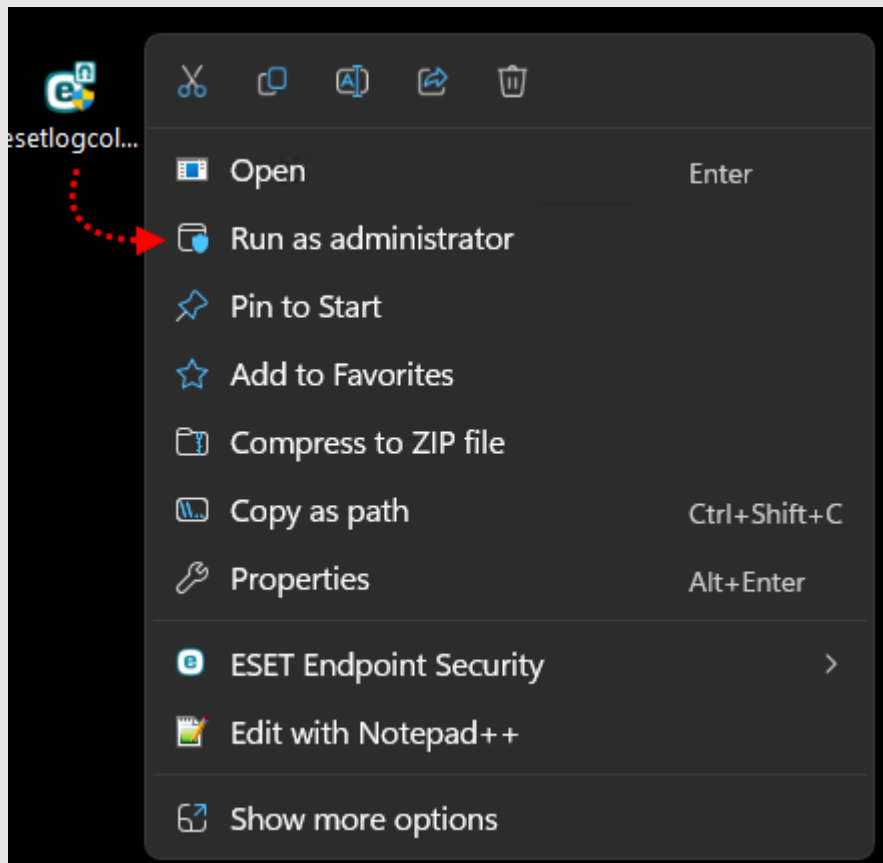
Pratite ESET-ove upute: [https://help.eset.com/ems/5/hr-HR/customer\\_care.html](https://help.eset.com/ems/5/hr-HR/customer_care.html) ili <https://support.eset.com/en/kb6472>

---

## Razno

- ESET - detaljne upute za program ELC: [https://help.eset.com/log\\_collector/latest/en-US/](https://help.eset.com/log_collector/latest/en-US/)
  - Budući da je XP odavno napušten i da su ESET-ovi stari programi u fazi "EOL" (End of Life), za njih više nema podrške i ne možemo preuzeti obvezu analize dnevnika tog okruženja. Radi eventualnih vaših internih potreba, prilažemo vezu na ELC koji valja koristiti samo na Windows XP: [Preuzmite ESET Log Collector za Windows XP](#)
- 

## Slike



**ESET Internet Security 18.0.12.0**

Collection profile

All ▾

**Collect** ?

Artifacts to collect

## Windows Processes

 Running processes (open handles and loaded DLLs)

## System Configuration

- Drives info
- Devices info
- Services Registry key content
- Windows Updates
- PowerShell history
- .NET Framework info
- ESET SysInspector log
- Network configuration
- Winsock LSP catalog
- WFP filters

Logs age limit [days]

30 ▾

ESET logs collection mode

Original binary from disk ▾

 Enable file size limit (4 GB)

Save archive as

C:\Users\administrator\Desktop\eis\_logs.zip

...

 Protect archive by password ⓘ

Operation log

```
[14:01] ESET Log Collector v4.12.0.0 (2024-12-18) - 64 bit
[14:01] Copyright (c) 1992-2024 ESET, spol. s r.o. All rights reserved.
[14:01]
[14:01] Detected product type: eis
```



### ESET Server Security 10.0.12014.0

Collection profile

All

- Default
- Threat detection
- All
- None
- Custom



- Agent database
- Configuration
- Process information and dumps

#### ESET Bridge

- ESET Bridge configuration
- ESET Bridge logs
- ESET Bridge dumps
- Nginx logs

#### ESET Inspect

- EI Connector logs
- EI Connector configuration

Logs age limit [days]

30

ESET logs collection mode

Original binary from disk

Save archive as

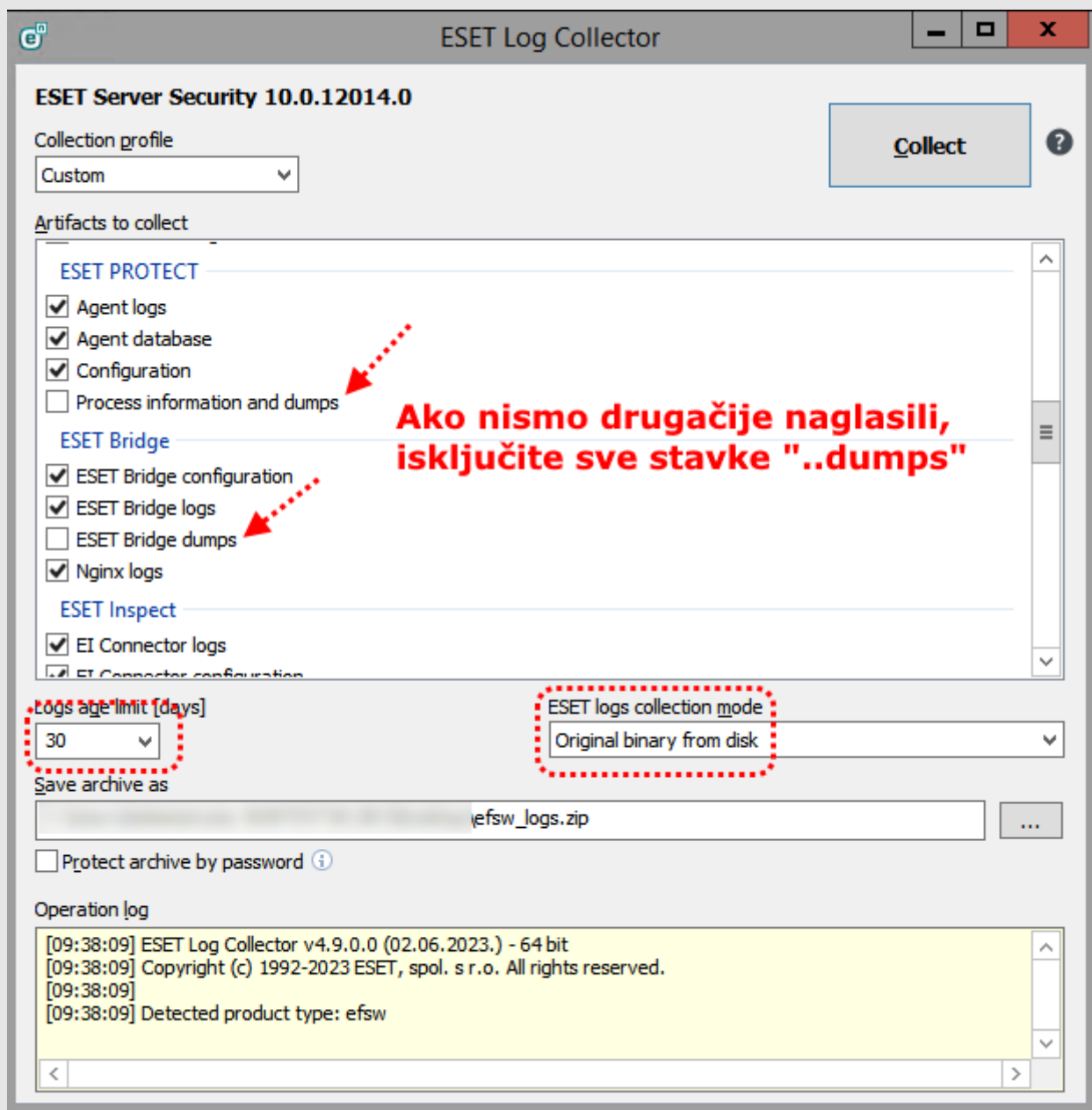
\\fsw\_logs.zip



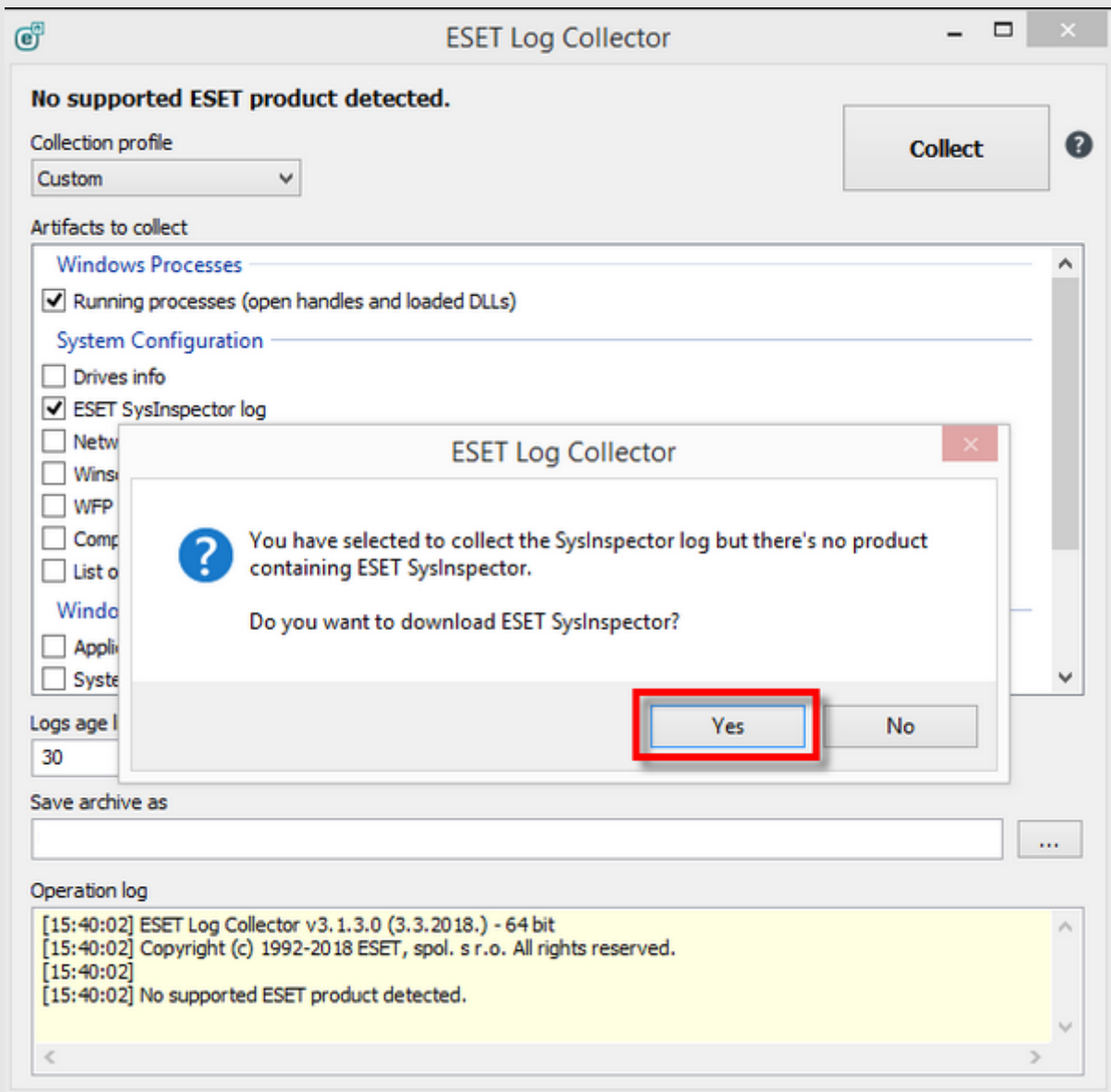
Protect archive by password

Operation log

```
[09:38:09] ESET Log Collector v4.9.0.0 (02.06.2023.) - 64 bit  
[09:38:09] Copyright (c) 1992-2023 ESET, spol. s r.o. All rights reserved.  
[09:38:09]  
[09:38:09] Detected product type: fsw
```

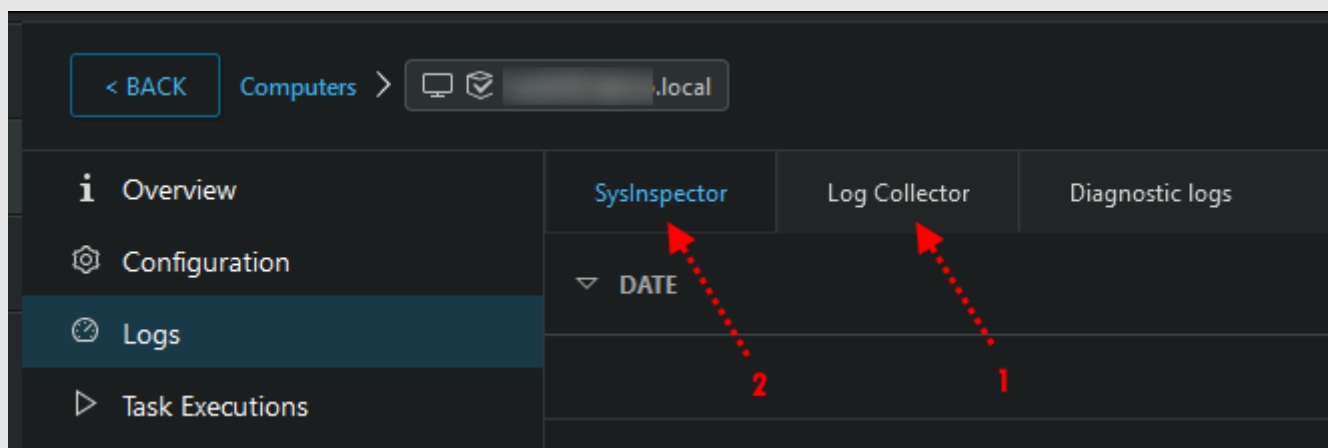


Svakako preuzmite SysInspector ako program predloži:



## ESET Protect

Ako logove skupljate putem ESET Protect konzole, obavezno nakon "Log Collector" otvorite i "SysInspector" karticu i preuzmite i taj paket logova.



---

## Detalji

Detaljna pojašnjenja što koja opcija ELC-a prikuplja:

[https://help.eset.com/log\\_collector/latest/en-US/elc\\_gui.html](https://help.eset.com/log_collector/latest/en-US/elc_gui.html)

ELC logovi će biti u navednom primjeru biti u datoteci "C:\Users\podrska\Desktop\ees\_logs.zip"

Samostalni SysInspector (ESI): <https://www.eset.com/us/download/tools-and-utilities/sysinspector>

---

## Video

v.15+

<https://www.nod32.com.hr/podrska/wp-content/uploads/ELC-All-20211117-opt-2x-b.mp4>

---

elc xelcx xlogcollectorx xdiagx xdebugx xdbgx xinfogetx diagnostics dijagnostika xdiagnostics xdijagnostika  
troubleshooting trblsht xtroubleshooting xtrblsht