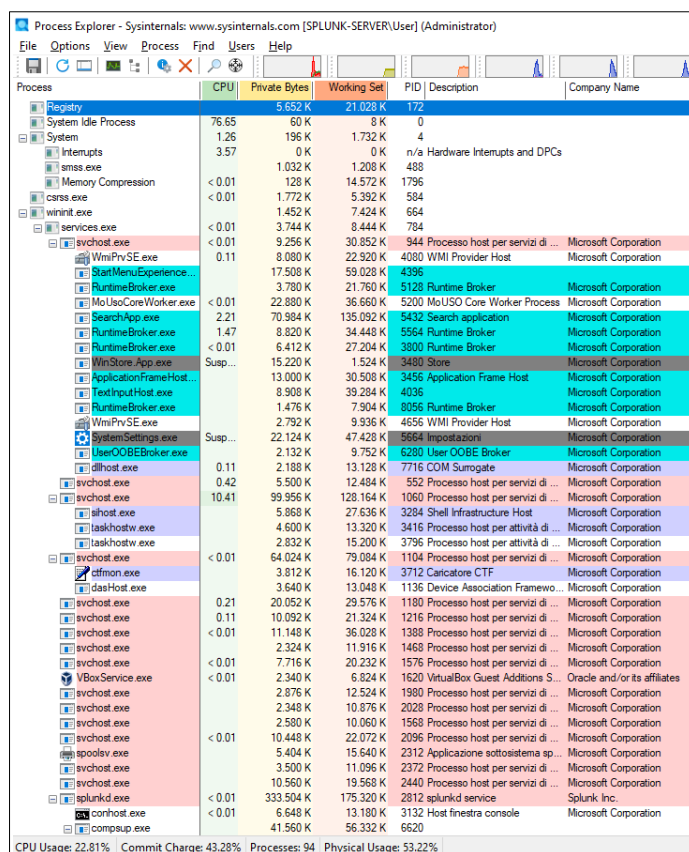
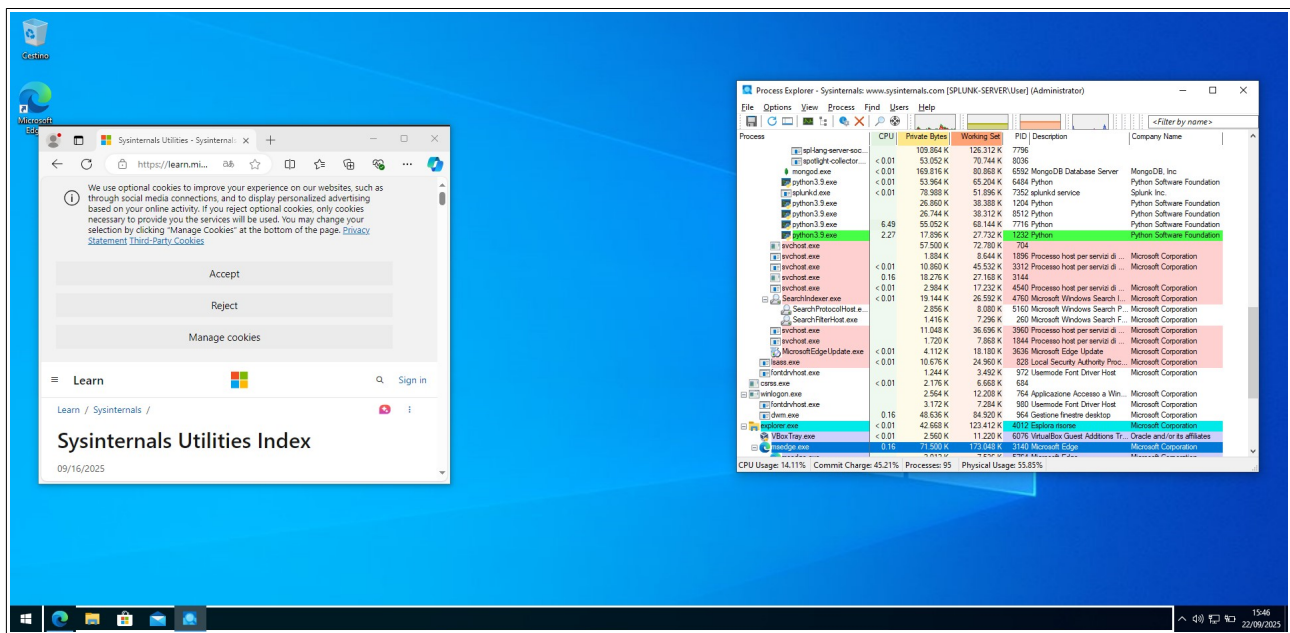


Introduzione

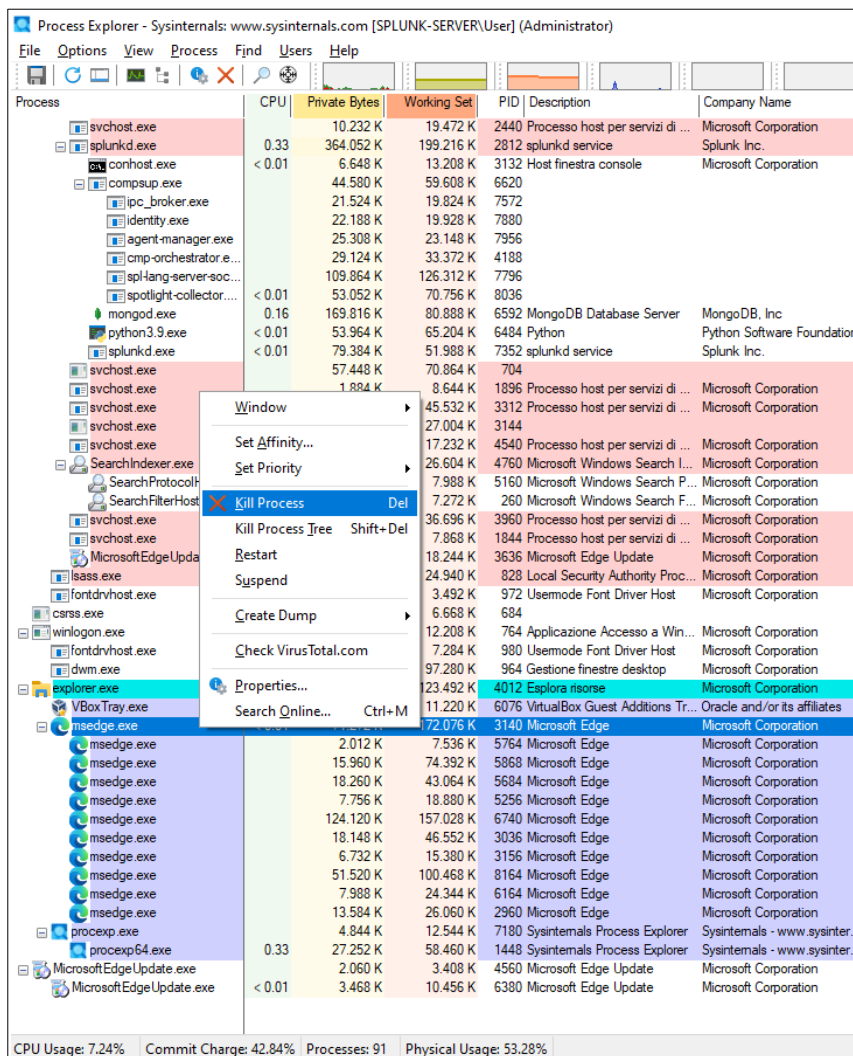
Esplorazione dei processi



Dopo aver scaricato e avviato Process Explorer, abbiamo usato l'icona *“Find Window's Process”* per localizzare il processo associato al browser web (Microsoft Edge).

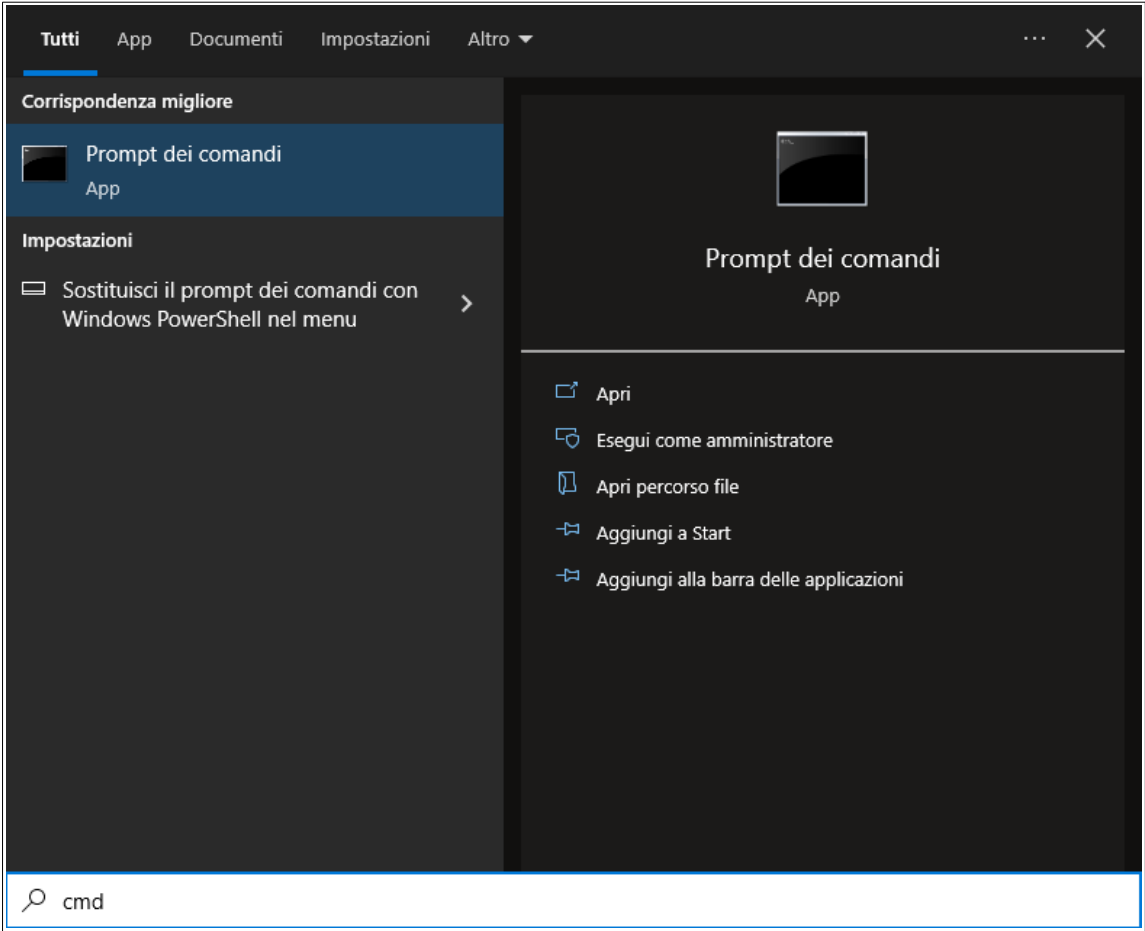


Dopo aver localizzato il processo di *“Microsoft Edge”* cliccando con il tasto destro sopra il processo si apre un menù a dove è possibile terminare il processo tramite *“Kill Process”*.



Cliccando su “Kill Process” la finestra del browser si chiude immediatamente, confermando che la terminazione di un processo corrisponde alla alla chiusura forzata dell’applicazione collegata.

Avvio e analisi del prompt dei comandi



È stato avviato il prompt dei comandi ed è stato individuato in Process Explorer notando la divisione tra “cmd.exe” (processo padre) e “conhost.exe” (processo figlio).

	explorer.exe	< 0.01	43.024 K	124.844 K	4012	Esplora risorse	Microsoft Corporation
	VBoxTray.exe	< 0.01	2.584 K	11.232 K	6076	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
	procexp.exe		4.844 K	12.544 K	7180	Sysinternals Process Explorer	Sysinternals - www.sysinter...
	procexp64.exe	0.46	27.228 K	60.140 K	1448	Sysinternals Process Explorer	Sysinternals - www.sysinter...
	cmd.exe		4.056 K	4.224 K	4168	Processore dei comandi di ...	Microsoft Corporation
	conhost.exe		7.568 K	19.264 K	4608	Host finestra console	Microsoft Corporation
	MicrosoftEdgeUpdate.exe		2.128 K	3.432 K	4560	Microsoft Edge Update	Microsoft Corporation
	MicrosoftEdgeUpdate.exe	0.09	3.468 K	10.156 K	6380	Microsoft Edge Update	Microsoft Corporation

Avviando un ping al prompt si nota la comparsa di un processo temporaneo chiamato PING.EXE (evidenziato in verde) il quale scompare una volta terminato il ping sul terminale.

The screenshot shows two windows. On the left is Process Explorer (Sysinternals) displaying a list of running processes. The 'conhost.exe' process is highlighted in green, indicating it is the active process. On the right is a command prompt window showing the execution of a ping command to 8.8.8.8. The output shows the ping was successful, with a response time of 7ms.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	11.528 K	37.132 K	1388	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	2.272 K	11.912 K	1468	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	7.592 K	20.456 K	1576	Processo host per servizi di ...	Microsoft Corporation
VBoxService.exe	< 0.01	2.336 K	6.996 K	1620	VirtualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe	< 0.01	2.964 K	13.148 K	1980	Processo host per servizi di ...	Microsoft Corporation
audiodg.exe	< 0.01	6.432 K	12.168 K	8932	Isolamento grafico dispositiv...	Microsoft Corporation
svchost.exe	< 0.01	2.348 K	10.896 K	2028	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	2.548 K	10.068 K	1568	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	12.932 K	24.724 K	2096	Processo host per servizi di ...	Microsoft Corporation
spoolsv.exe	< 0.01	5.404 K	15.656 K	2312	Applicazione sottosistema sp...	Microsoft Corporation
svchost.exe	< 0.01	3.296 K	11.000 K	2372	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	10.232 K	19.456 K	2440	Processo host per servizi di ...	Microsoft Corporation
splunkd.exe	0.35	420.096 K	198.460 K	2812	splunkd service	Splunk Inc.
conhost.exe	< 0.01	6.648 K	13.208 K	3132	Host finestra console	Microsoft Corporation
comsup.exe	< 0.01	43.432 K	58.632 K	6620		
pc_broker.exe	< 0.01	22.488 K	20.880 K	7572		
identity.exe	< 0.01	21.716 K	19.636 K	7880		
agent-manager.exe	< 0.01	24.396 K	22.312 K	7956		
cmp-orchestrator.e...	< 0.01	30.796 K	35.028 K	4188		
spl-lang-server-soc...	< 0.01	107.816 K	124.272 K	7796		
spotlight-collector...	< 0.01	53.420 K	71.176 K	8036		
mongod.exe	< 0.01	169.816 K	80.928 K	6592	MongoDB Database Server	MongoDB, Inc
python3.9.exe	< 0.01	53.932 K	65.188 K	6484	Python	Python Software Foundation
splunkd.exe	< 0.01	79.384 K	52.180 K	7352	splunkd service	Splunk Inc.
svchost.exe	< 0.01	57.104 K	77.296 K	704		
svchost.exe	< 0.01	1.968 K	8.656 K	1896	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	10.740 K	44.884 K	3312	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	13.908 K	25.136 K	3144		
svchost.exe	< 0.01	3.384 K	17.740 K	4540	Processo host per servizi di ...	Microsoft Corporation
SearchIndexer.exe	< 0.01	20.260 K	27.304 K	4760	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe	< 0.01	10.888 K	36.620 K	3960	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	1.720 K	7.868 K	1844	Processo host per servizi di ...	Microsoft Corporation
MicrosoftEdgeUpdate.exe	< 0.01	4.276 K	18.348 K	3636	Microsoft Edge Update	Microsoft Corporation
svchost.exe	< 0.01	1.958 K	8.044 K	7076		
svchost.exe	< 0.01	10.872 K	24.960 K	828	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe	< 0.01	1.244 K	3.492 K	972	Usemode Font Driver Host	Microsoft Corporation
csrss.exe	< 0.01	2.204 K	6.648 K	684		
winlogon.exe	< 0.01	2.564 K	12.196 K	764	Applicazione Accesso a Win...	Microsoft Corporation
fontdrvhost.exe	< 0.01	3.244 K	7.428 K	980	Usemode Font Driver Host	Microsoft Corporation
dmw.exe	< 0.01	52.880 K	91.916 K	964	Gestione finestre desktop	Microsoft Corporation
explorer.exe	< 0.01	43.072 K	124.972 K	4012	Esplora risorse	Microsoft Corporation
VBoxTray.exe	< 0.01	2.584 K	11.220 K	6076	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
proccp.exe	< 0.01	4.844 K	12.544 K	7180	Sysinternals Process Explorer	Sysinternals - www.sysinter...
proccp64.exe	< 0.01	58.552 K	58.552 K	1448	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe	< 0.01	2.128 K	4.652 K	4168	Processore dei comandi di ...	Microsoft Corporation
conhost.exe	< 0.01	6.648 K	13.208 K	3132	Host finestra console	Microsoft Corporation
MicrosoftEdgeUpdate.exe	< 0.01	2.056 K	3.532 K	4560	Microsoft Edge Update	Microsoft Corporation
MicrosoftEdgeUpdate.exe	< 0.01	3.536 K	10.320 K	6380	Microsoft Edge Update	Microsoft Corporation

Dopodiché cliccando con il tasto destro su “conhost.exe” e selezionando “Check VirusTotal.com” si può verificare all’istante se un processo è malevolo o meno. Purtroppo nonostante click ripetuti non si è aperto il report di VirusTotal.

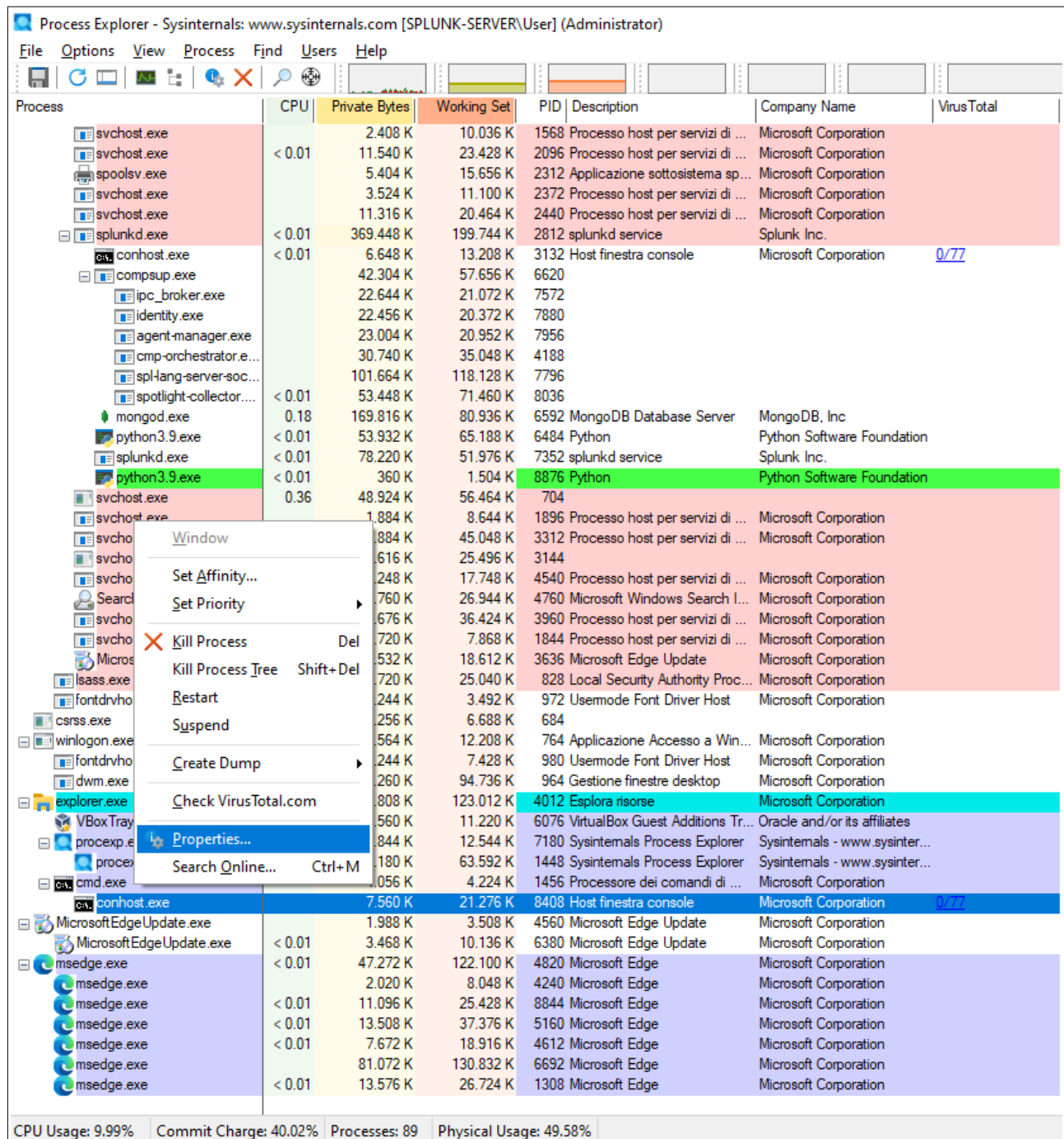
The screenshot shows Process Explorer with a right-click context menu open over the 'conhost.exe' process. The menu includes options like 'Set Affinity...', 'Set Priority', 'Kill Process', 'Restart', 'Suspend', 'Create Dump', 'Check VirusTotal.com', 'Properties...', and 'Search Online...'. The 'Check VirusTotal.com' option is highlighted in blue.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	11.536 K	37.060 K	1388	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	2.272 K	11.912 K	1468	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	7.640 K	20.444 K	1576	Processo host per servizi di ...	Microsoft Corporation
VBoxService.exe	< 0.01	2.036 K	6.840 K	1620	VirtualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe	< 0.01	2.880 K	13.152 K	1980	Processo host per servizi di ...	Microsoft Corporation
audiodg.exe	< 0.01	6.432 K	12.168 K	8932	Isolamento grafico dispositiv...	Microsoft Corporation
svchost.exe	< 0.01	2.348 K	10.896 K	2028	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	2.548 K	10.068 K	1568	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	12.936 K	24.724 K	2096	Processo host per servizi di ...	Microsoft Corporation
spoolsv.exe	< 0.01	5.404 K	15.656 K	2312	Applicazione sottosistema sp...	Microsoft Corporation
svchost.exe	< 0.01	3.296 K	11.000 K	2372	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	10.232 K	19.456 K	2440	Processo host per servizi di ...	Microsoft Corporation
splunkd.exe	0.36	366.004 K	200.392 K	2812	splunkd service	Splunk Inc.
conhost.exe	< 0.01	6.648 K	13.208 K	3132	Host finestra console	Microsoft Corporation
comsup.exe	< 0.01	43.432 K	58.632 K	6620		
pc_broker.exe	< 0.01	22.500 K	20.908 K	7572		
identity.exe	< 0.01	21.740 K	19.652 K	7880		
agent-manager.exe	< 0.01	24.428 K	22.320 K	7956		
cmp-orchestrator.e...	< 0.01	30.804 K	35.072 K	4188		
spl-lang-server-soc...	< 0.01	107.816 K	124.272 K	7796		
spotlight-collector...	< 0.01	53.420 K	71.192 K	8036		
mongod.exe	< 0.01	169.816 K	80.928 K	6592	MongoDB Database Server	MongoDB, Inc
python3.9.exe	< 0.01	53.932 K	65.188 K	6484	Python	Python Software Foundation
splunkd.exe	< 0.01	79.384 K	52.180 K	7352	splunkd service	Splunk Inc.
svchost.exe	< 0.01	57.376 K	79.008 K	704		
svchost.exe	< 0.01	1.968 K	8.656 K	1896	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	10.696 K	44.868 K	3312	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	29.144 K	3144			
svchost.exe	< 0.01	17.748 K	4540	Processo host per servizi di ...	Microsoft Corporation	
SearchIndexer.exe	< 0.01	27.276 K	4760	Microsoft Windows Search I...	Microsoft Corporation	
svchost.exe	< 0.01	36.620 K	3960	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe	< 0.01	7.868 K	1844	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe	< 0.01	18.348 K	3636	Microsoft Edge Update	Microsoft Corporation	
MicrosoftEdgeUpdate.exe	< 0.01	24.944 K	828	Local Security Authority Proc...	Microsoft Corporation	
fontdrvhost.exe	< 0.01	3.492 K	972	Usemode Font Driver Host	Microsoft Corporation	
csrss.exe	< 0.01	6.648 K	684			
winlogon.exe	< 0.01	12.196 K	764	Applicazione Accesso a Win...	Microsoft Corporation	
fontdrvhost.exe	< 0.01	7.428 K	980	Usemode Font Driver Host	Microsoft Corporation	
dmw.exe	< 0.01	94.700 K	964	Gestione finestre desktop	Microsoft Corporation	
explorer.exe	< 0.01	124.620 K	4012	Esplora risorse	Microsoft Corporation	
VBoxTray.exe	< 0.01	11.220 K	6076	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	
proccp.exe	< 0.01	12.544 K	7180	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
proccp64.exe	< 0.01	58.552 K	58.552 K	1448	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe	< 0.01	4.652 K	4168	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe	< 0.01	21.180 K	4608	Host finestra console	Microsoft Corporation	
MicrosoftEdgeUpdate.exe	< 0.01	2.056 K	3.532 K	4560	Microsoft Edge Update	Microsoft Corporation
MicrosoftEdgeUpdate.exe	< 0.01	3.536 K	10.320 K	6380	Microsoft Edge Update	Microsoft Corporation

Infine, il processo padre “cmd.exe” è stato terminato. Insieme ad esso anche il processo figlio “conhost.exe” è stato terminato automaticamente.

Esplorazione di Thread e Handle

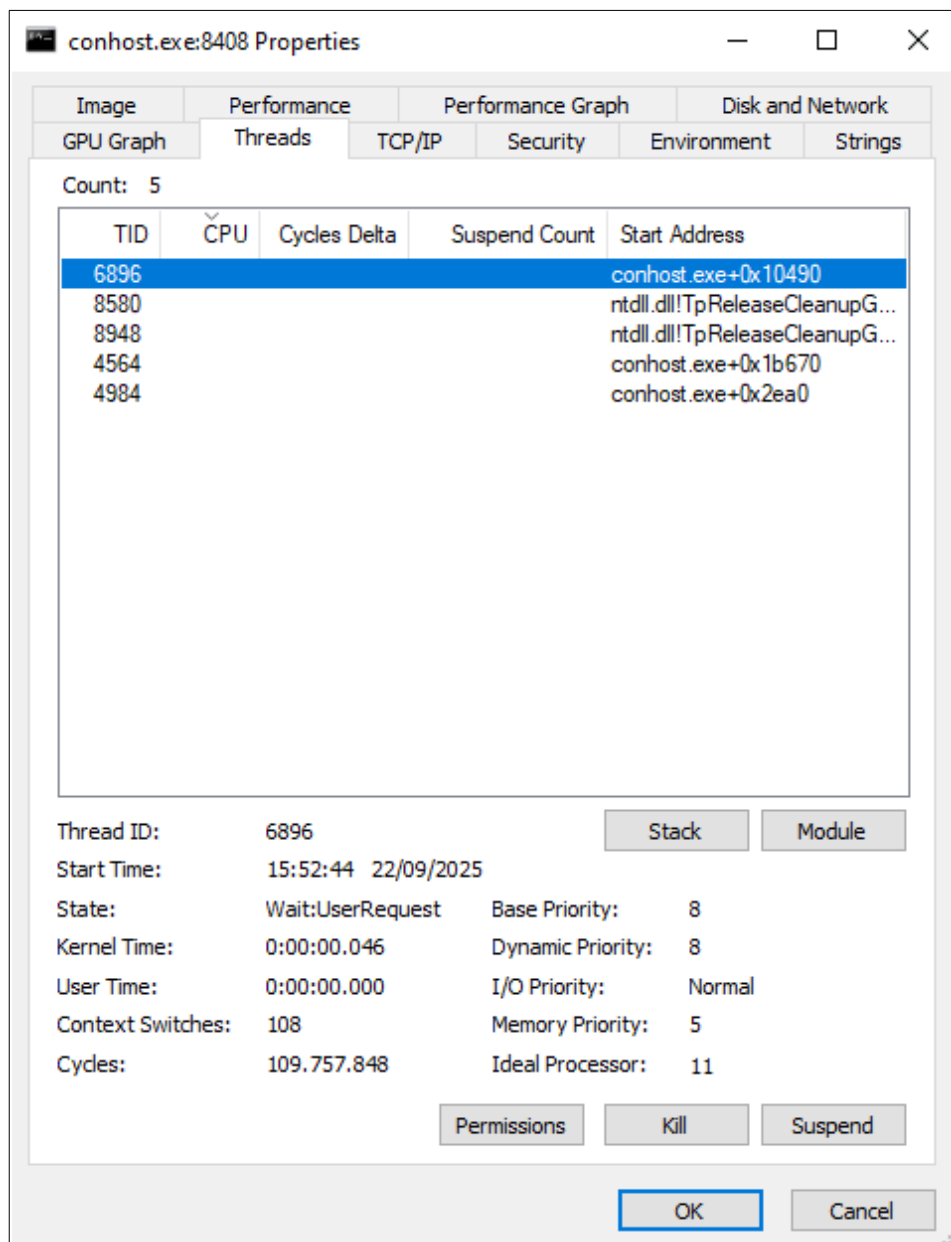
Una volta riaperto il prompt dei comandi, cliccando con il tasto destro su “conhost.exe” si può accedere alle proprietà del processo.+



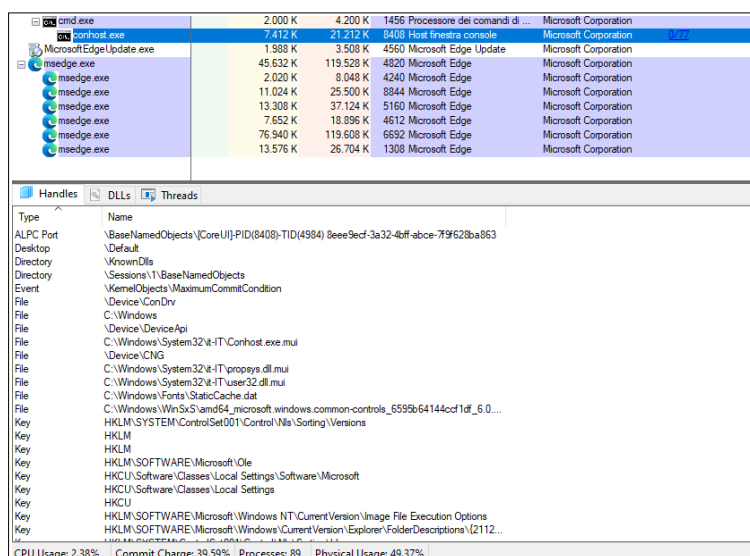
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
svchost.exe		2.408 K	10.036 K	1568	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe	< 0.01	11.540 K	23.428 K	2096	Processo host per servizi di ...	Microsoft Corporation	
spoolsv.exe		5.404 K	15.656 K	2312	Applicazione sottosistema sp...	Microsoft Corporation	
svchost.exe		3.524 K	11.100 K	2372	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		11.316 K	20.464 K	2440	Processo host per servizi di ...	Microsoft Corporation	
splunkd.exe	< 0.01	369.448 K	199.744 K	2812	splunkd service	Splunk Inc.	
conhost.exe	< 0.01	6.648 K	13.208 K	3132	Host finestra console	Microsoft Corporation	0/77
comsup.exe		42.304 K	57.656 K	6620			
ipc_broker.exe		22.644 K	21.072 K	7572			
identity.exe		22.456 K	20.372 K	7880			
agent-manager.exe		23.004 K	20.952 K	7956			
cmp-orchestrator.e...		30.740 K	35.048 K	4188			
spl-hang-server-soc...		101.664 K	118.128 K	7796			
spotlight-collector...	< 0.01	53.448 K	71.460 K	8036			
mongod.exe	0.18	169.816 K	80.936 K	6592	MongoDB Database Server	MongoDB, Inc	
python3.9.exe	< 0.01	53.932 K	65.188 K	6484	Python	Python Software Foundation	
splunkd.exe	< 0.01	78.220 K	51.976 K	7352	splunkd service	Splunk Inc.	
python3.9.exe	< 0.01	360 K	1.504 K	8876	Python	Python Software Foundation	
svchost.exe	0.36	48.924 K	56.464 K	704			
svchost.exe		1.884 K	8.644 K	1896	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		1.884 K	45.048 K	3312	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		616 K	25.496 K	3144			
svchost.exe		248 K	17.748 K	4540	Processo host per servizi di ...	Microsoft Corporation	
SearchIndexer.exe		760 K	26.944 K	4760	Microsoft Windows Search I...	Microsoft Corporation	
svchost.exe		676 K	36.424 K	3960	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		720 K	7.868 K	1844	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		532 K	18.612 K	3636	Microsoft Edge Update	Microsoft Corporation	
svchost.exe		720 K	25.040 K	828	Local Security Authority Proc...	Microsoft Corporation	
svchost.exe		244 K	3.492 K	972	Usermode Font Driver Host	Microsoft Corporation	
csrss.exe		256 K	6.688 K	684			
winlogon.exe		564 K	12.208 K	764	Applicazione Accesso a Win...	Microsoft Corporation	
fontdrvhost.exe		244 K	7.428 K	980	Usermode Font Driver Host	Microsoft Corporation	
fontdrvhost.exe		260 K	94.736 K	964	Gestione finestre desktop	Microsoft Corporation	
explorer.exe		808 K	123.012 K	4012	Esplora risorse	Microsoft Corporation	
VBoxTray.exe		560 K	11.220 K	6076	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	
procexp.exe		844 K	12.544 K	7180	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp.exe		180 K	63.592 K	1448	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		1056 K	4.224 K	1456	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		7.560 K	21.276 K	8408	Host finestra console	Microsoft Corporation	0/77
MicrosoftEdgeUpdate.exe		1.988 K	3.508 K	4560	Microsoft Edge Update	Microsoft Corporation	
MicrosoftEdgeUpdate.exe	< 0.01	3.468 K	10.136 K	6380	Microsoft Edge Update	Microsoft Corporation	
msedge.exe	< 0.01	47.272 K	122.100 K	4820	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	2.020 K	8.048 K	4240	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	11.096 K	25.428 K	8844	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	13.508 K	37.376 K	5160	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	7.672 K	18.916 K	4612	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	81.072 K	130.832 K	6692	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	13.576 K	26.724 K	1308	Microsoft Edge	Microsoft Corporation	

CPU Usage: 9.99% Commit Charge: 40.02% Processes: 89 Physical Usage: 49.58%

Aprendo le proprietà si può accedere alla sezione “Threads” dove sono visibili dli ID dei thread. Queste informazioni sono utili per capire quali componenti sono attivi in un processo.

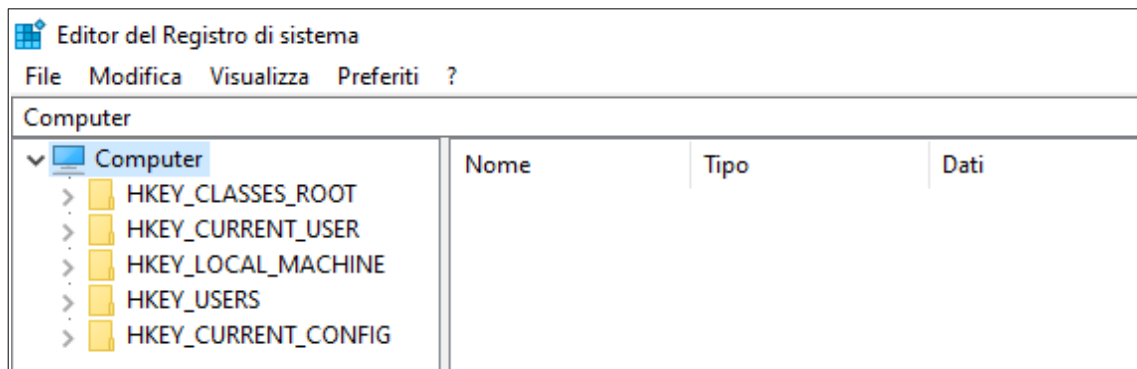


A questo punto dal menù di Process Explorer eseguendo il percorso View > Lower Pane View > Handles si possono vedere gli handles di “conhost.exe”.

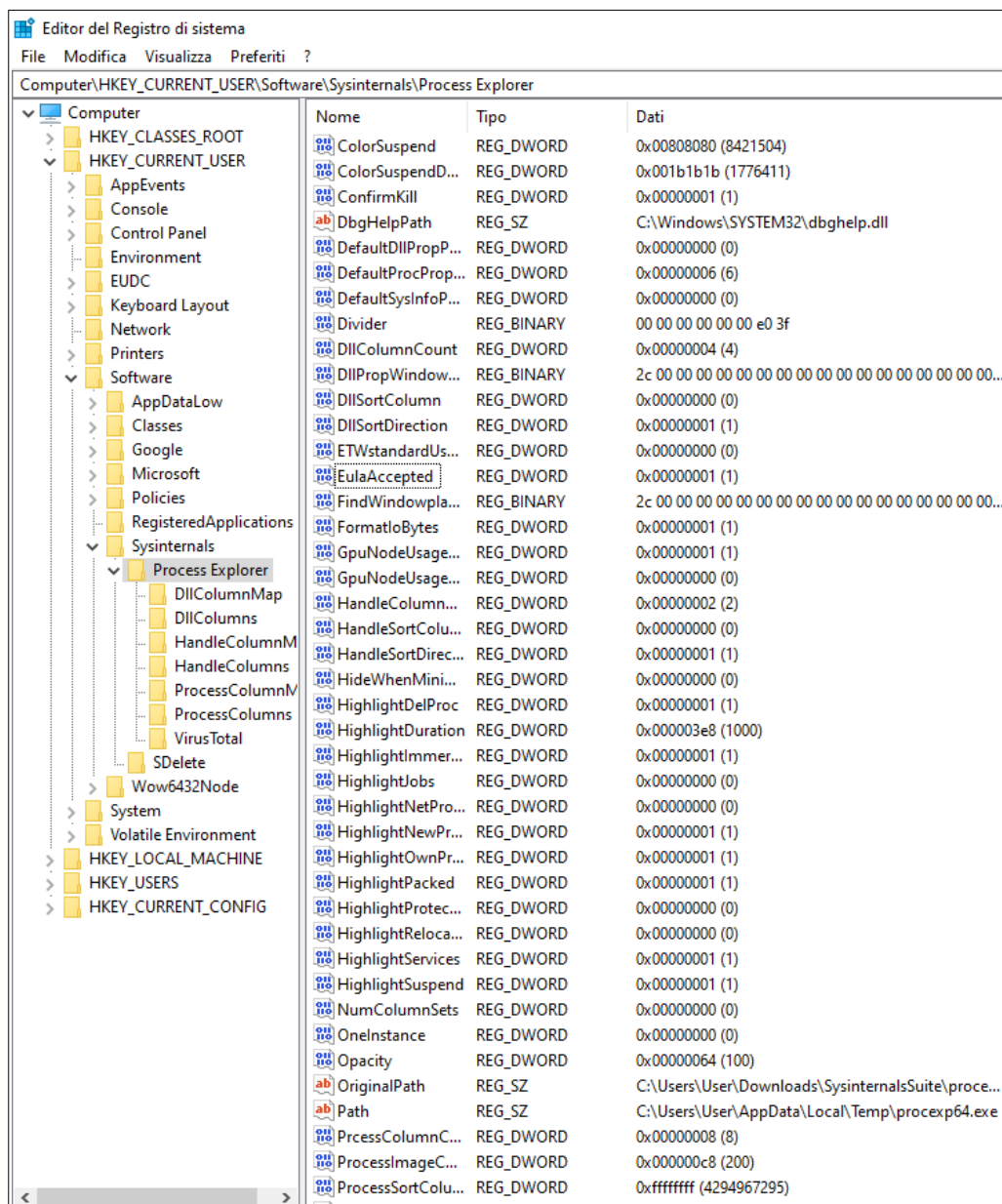


Esplorazione del registro di Windows

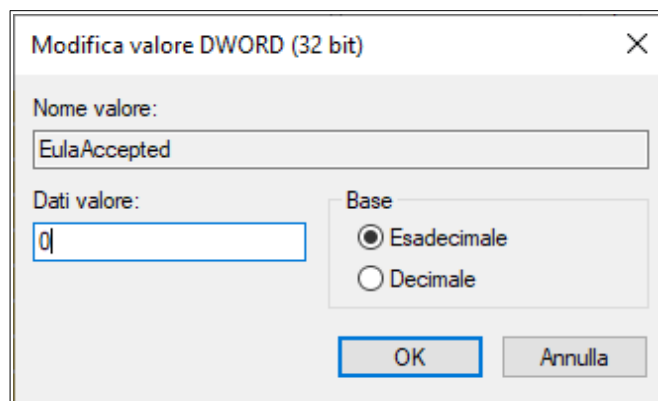
Come ultima cosa è stato aperto l'editor del registro di Windows.



Da qui è stato possibile ricercare la chiave relativa a Process Explorer in modo da poter controllare il valore di EulaAccepted.



Essendo 1 il valore di questa chiave di può evincere che la licenza EULA è stata accettata. Modificando il valore da 1 a 0 saremo obbligati a accettare nuovamente la licenza EULA di Process Explorer.



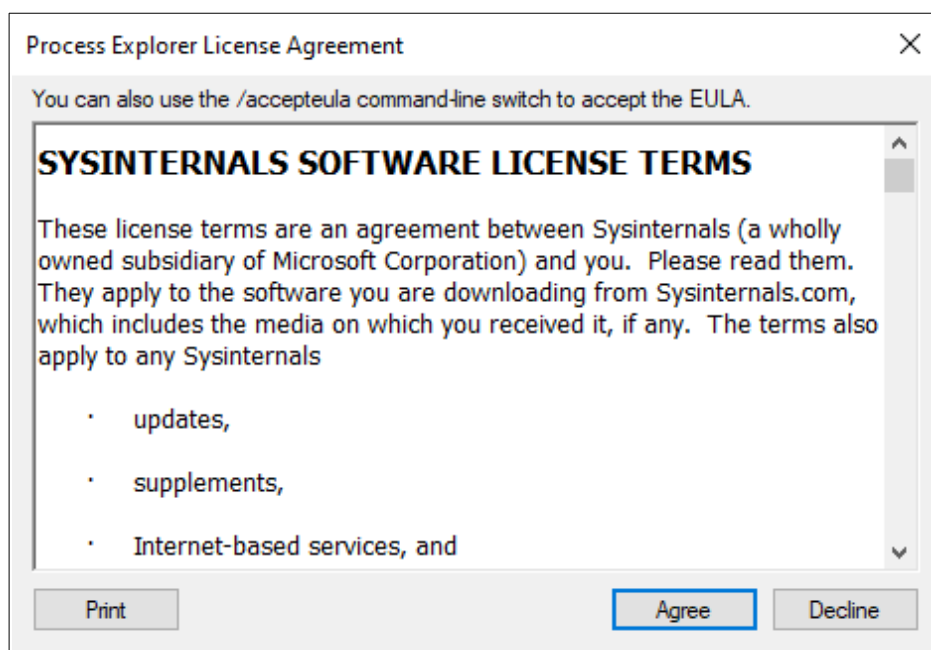
Modifica valore DWORD (32 bit)

Nome valore:
EulaAccepted

Dati valore:
0

Base
☒ Esadecimale
☐ Decimale

OK Annulla



Process Explorer License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Print Agree Decline