Automating system administration tasks – Part5

michaelfirsov.wordpress.com/automating-system-administration-tasks-part-5

April 9, 2019

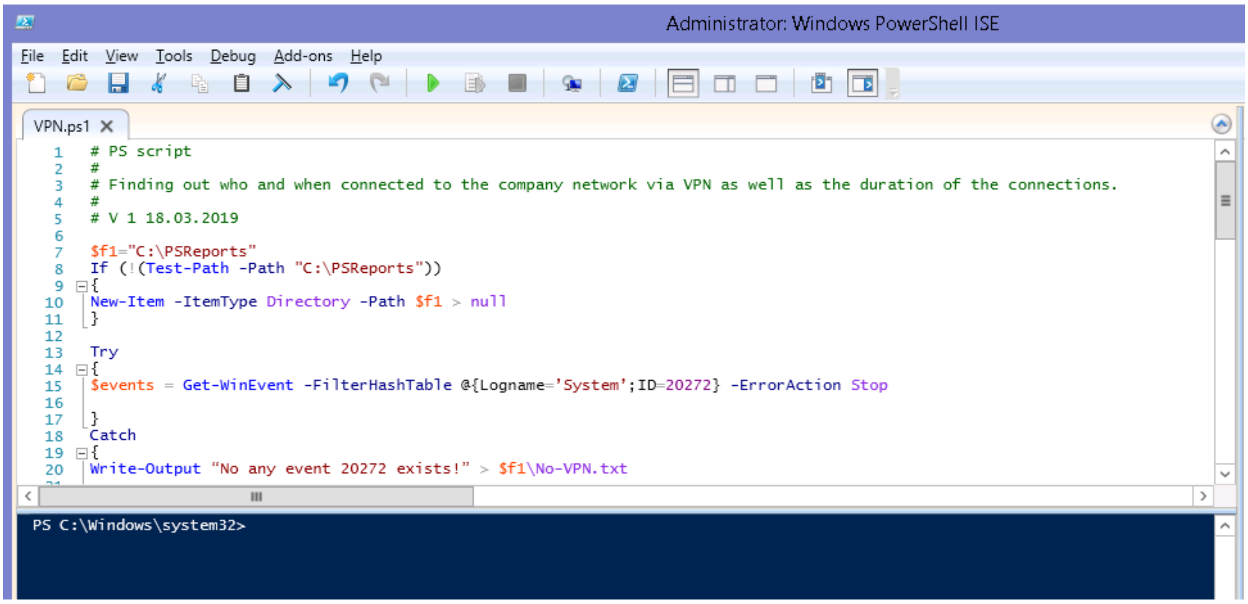
Part4

V VPN Server

What I want to know about remote connections to my network:

1) Which users connected to our company network over past few days?
2) What was the duration of each remote user session?
3) Which ip address has been assisgned to a remote user? (optional)

1-2)
The script: VPN
(please rename the script from *.docx* into *.ps1* and create any needed changes before use)

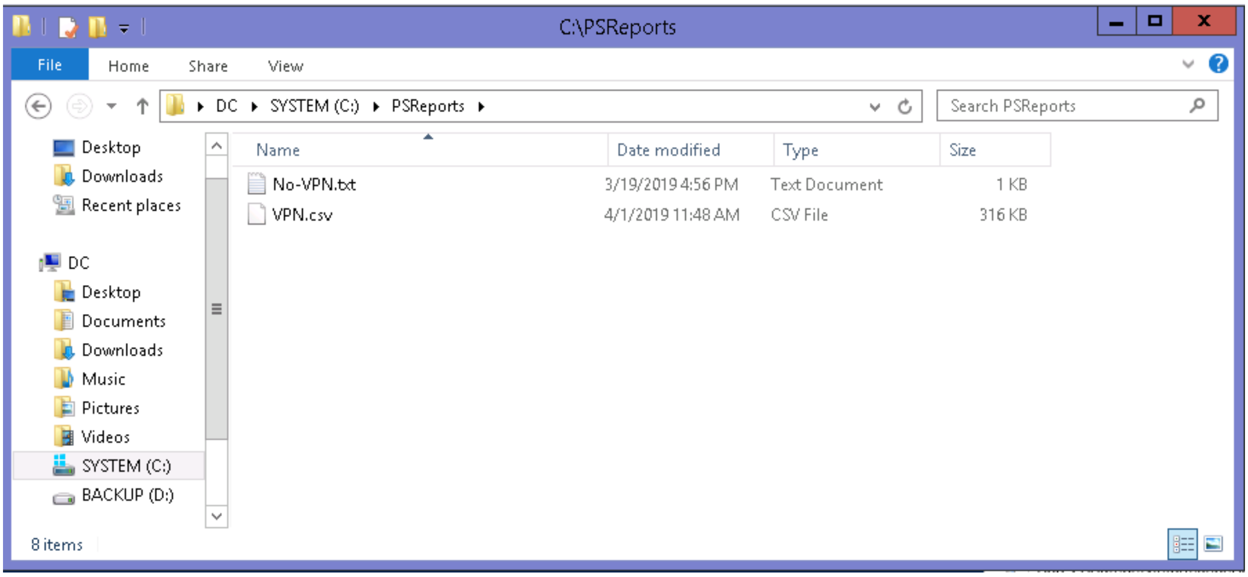


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
VPN.ps1

```
# PS script
#
# Finding out who and when connected to the company network via VPN as well as the duration of the connections.
#
# V 1 18.03.2019

$f1="C:\PSReports"
If (!(Test-Path -Path "C:\PSReports"))
{
New-Item -ItemType Directory -Path $f1 > null
}

Try
{
$events = Get-WinEvent -FilterHashTable @{Logname='System';ID=20272} -ErrorAction Stop

}
Catch
{
Write-Output “No any event 20272 exists!” > $f1\No-VPN.txt
```

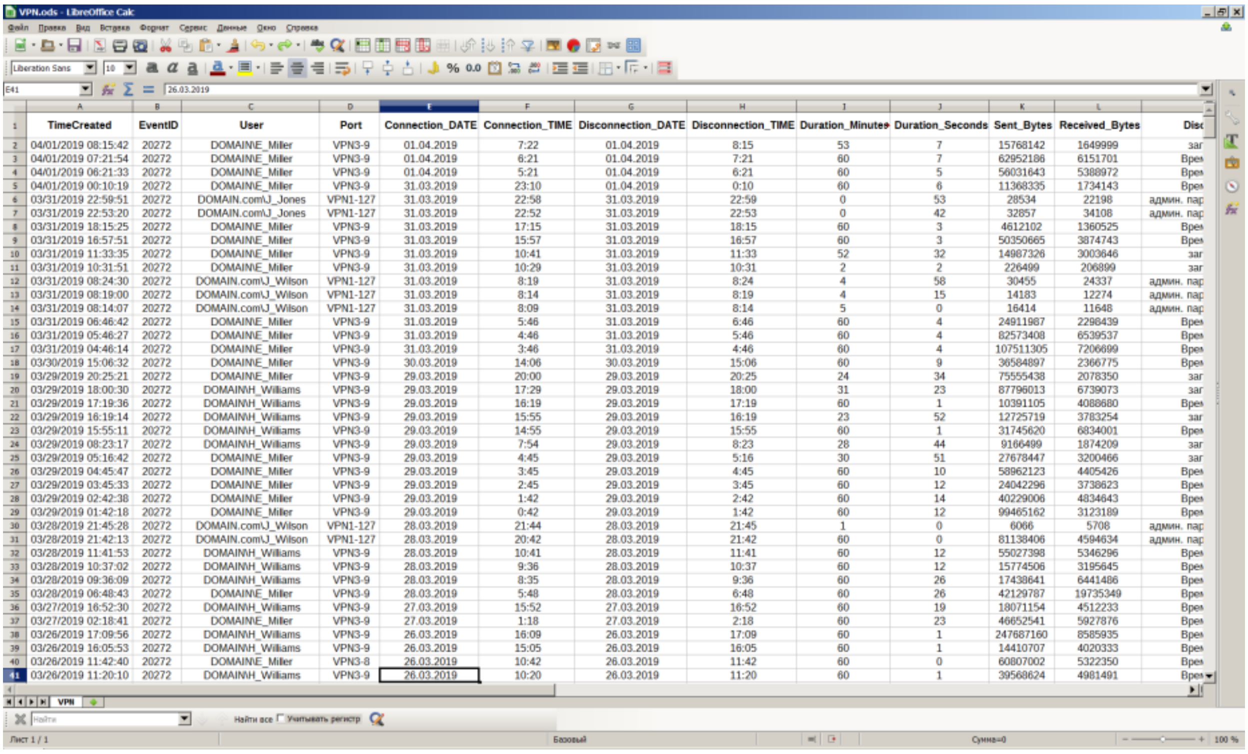
```
PS C:\Windows\system32>
```

This script creates either *vpn.csv* or *no-vpn.txt* file (in case there were no vpn connections) in the **C:\PSReports\** folder and sends it to *michael_firsov@testenterprise.com*:



Name	Date modified	Type	Size
No-VPN.txt	3/19/2019 4:56 PM	Text Document	1 KB
VPN.csv	4/1/2019 11:48 AM	CSV File	316 KB

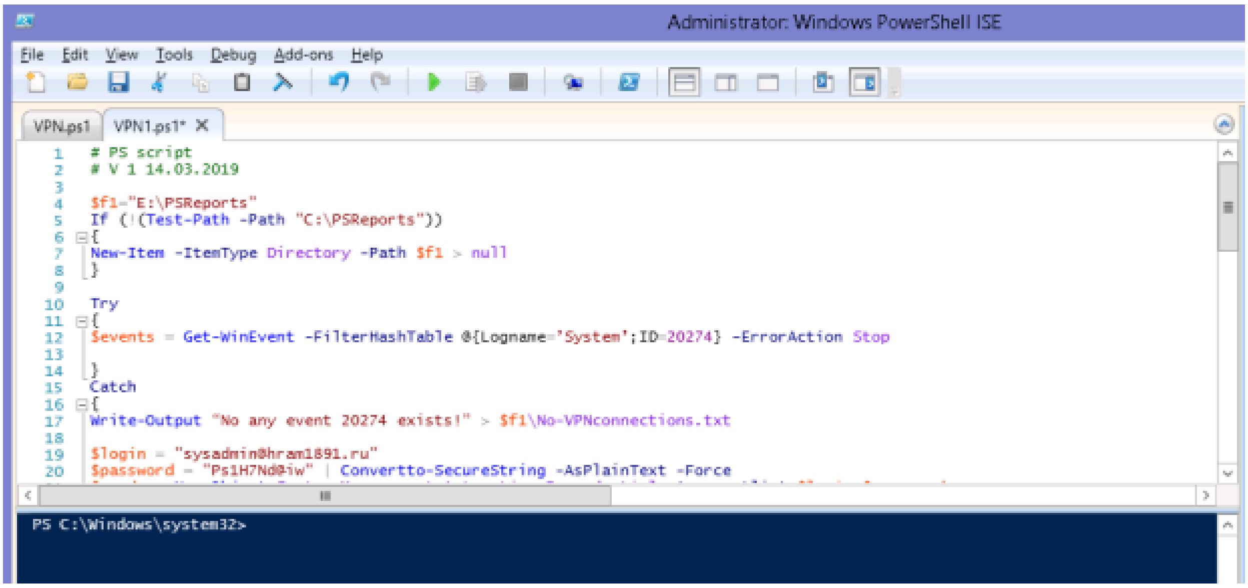
The *VPN.csv* file looks as follows:



	A	B	C	D	E	F	G	H	I	J	K	L	
1	TimeCreated	EventID	User	Port	Connection_DATE	Connection_TIME	Disconnection_DATE	Disconnection_TIME	Duration_Minutes	Duration_Seconds	Sent_Bytes	Received_Bytes	Disc
2	04/01/2019 08:15:42	20272	DOMAIN\E_Miller	VPN3-9	01.04.2019	7:22	01.04.2019	8:15	53	7	15768142	1649999	заг
3	04/01/2019 07:21:54	20272	DOMAIN\E_Miller	VPN3-9	01.04.2019	6:21	01.04.2019	7:21	60	7	62952186	6151701	Врем
4	04/01/2019 06:21:33	20272	DOMAIN\E_Miller	VPN3-9	01.04.2019	5:21	01.04.2019	6:21	60	5	56031643	5388972	Врем
5	04/01/2019 00:10:19	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	23:10	01.04.2019	0:10	60	6	11368335	1734143	Врем
6	03/31/2019 22:59:51	20272	DOMAIN.com\J_Jones	VPN1-127	31.03.2019	22:58	31.03.2019	22:59	0	53	28534	22198	админ. пар
7	03/31/2019 22:53:20	20272	DOMAIN.com\J_Jones	VPN1-127	31.03.2019	22:52	31.03.2019	22:53	0	42	32857	34108	админ. пар
8	03/31/2019 18:15:25	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	17:15	31.03.2019	18:15	60	3	4612102	1360525	Врем
9	03/31/2019 16:57:51	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	15:57	31.03.2019	16:57	60	3	50350665	3874743	Врем
10	03/31/2019 11:33:35	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	10:41	31.03.2019	11:33	52	32	14987326	3003646	заг
11	03/31/2019 10:31:51	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	10:29	31.03.2019	10:31	2	2	226499	206899	заг
12	03/31/2019 08:24:30	20272	DOMAIN.com\J_Wilson	VPN1-127	31.03.2019	8:19	31.03.2019	8:24	4	58	30455	24337	админ. пар
13	03/31/2019 08:19:00	20272	DOMAIN.com\J_Wilson	VPN1-127	31.03.2019	8:14	31.03.2019	8:19	4	15	14183	12274	админ. пар
14	03/31/2019 08:14:07	20272	DOMAIN.com\J_Wilson	VPN1-127	31.03.2019	8:09	31.03.2019	8:14	5	0	16414	11648	админ. пар
15	03/31/2019 06:46:42	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	5:46	31.03.2019	6:46	60	4	24911987	2298439	Врем
16	03/31/2019 05:46:27	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	4:46	31.03.2019	5:46	60	4	82573408	6539537	Врем
17	03/31/2019 04:46:14	20272	DOMAIN\E_Miller	VPN3-9	31.03.2019	3:46	31.03.2019	4:46	60	4	107511305	7206699	Врем
18	03/30/2019 15:06:32	20272	DOMAIN\E_Miller	VPN3-9	30.03.2019	14:06	30.03.2019	15:06	60	9	36584897	2366775	Врем
19	03/29/2019 20:25:21	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	20:00	29.03.2019	20:25	24	34	75555438	2078350	заг
20	03/29/2019 18:00:30	20272	DOMAIN\H_Williams	VPN3-9	29.03.2019	17:29	29.03.2019	18:00	31	23	87796013	6739073	заг
21	03/29/2019 17:19:36	20272	DOMAIN\H_Williams	VPN3-9	29.03.2019	16:19	29.03.2019	17:19	60	1	10391105	4088680	Врем
22	03/29/2019 16:19:14	20272	DOMAIN\H_Williams	VPN3-9	29.03.2019	15:55	29.03.2019	16:19	23	52	12725719	3783254	заг
23	03/29/2019 15:55:11	20272	DOMAIN\H_Williams	VPN3-9	29.03.2019	14:55	29.03.2019	15:55	60	1	31745620	6834001	Врем
24	03/29/2019 08:23:17	20272	DOMAIN\H_Williams	VPN3-9	29.03.2019	7:54	29.03.2019	8:23	28	44	9166499	1874209	заг
25	03/29/2019 05:16:42	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	4:45	29.03.2019	5:16	30	51	27678447	3200466	заг
26	03/29/2019 04:45:47	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	3:45	29.03.2019	4:45	60	10	58962123	4405426	Врем
27	03/29/2019 03:45:33	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	2:45	29.03.2019	3:45	60	12	24042296	3738623	Врем
28	03/29/2019 02:42:38	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	1:42	29.03.2019	2:42	60	14	40229006	4834643	Врем
29	03/29/2019 01:42:18	20272	DOMAIN\E_Miller	VPN3-9	29.03.2019	0:42	29.03.2019	1:42	60	12	99465162	3123189	Врем
30	03/28/2019 21:45:28	20272	DOMAIN.com\J_Wilson	VPN1-127	28.03.2019	21:44	28.03.2019	21:45	1	0	6066	5708	админ. пар
31	03/28/2019 21:42:13	20272	DOMAIN.com\J_Wilson	VPN1-127	28.03.2019	20:42	28.03.2019	21:42	60	0	81138406	4594634	админ. пар
32	03/28/2019 11:41:53	20272	DOMAIN\H_Williams	VPN3-9	28.03.2019	10:41	28.03.2019	11:41	60	12	55027398	5346296	Врем
33	03/28/2019 10:37:02	20272	DOMAIN\H_Williams	VPN3-9	28.03.2019	9:36	28.03.2019	10:37	60	12	15774506	3195645	Врем
34	03/28/2019 09:36:09	20272	DOMAIN\H_Williams	VPN3-9	28.03.2019	8:35	28.03.2019	9:36	60	26	17438641	6441486	Врем
35	03/28/2019 06:48:43	20272	DOMAIN\E_Miller	VPN3-9	28.03.2019	5:48	28.03.2019	6:48	60	26	42129787	19735349	Врем
36	03/27/2019 16:52:30	20272	DOMAIN\H_Williams	VPN3-9	27.03.2019	15:52	27.03.2019	16:52	60	19	18071154	4512233	Врем
37	03/27/2019 02:18:41	20272	DOMAIN\E_Miller	VPN3-9	27.03.2019	1:18	27.03.2019	2:18	60	23	46652541	5927876	Врем
38	03/26/2019 17:09:56	20272	DOMAIN\H_Williams	VPN3-9	26.03.2019	16:09	26.03.2019	17:09	60	1	247687160	8585935	Врем
39	03/26/2019 16:05:53	20272	DOMAIN\H_Williams	VPN3-9	26.03.2019	15:05	26.03.2019	16:05	60	1	14410707	4020333	Врем
40	03/26/2019 11:42:40	20272	DOMAIN\E_Miller	VPN3-8	26.03.2019	10:42	26.03.2019	11:42	60	0	60807002	5322350	Врем
41	03/26/2019 11:20:10	20272	DOMAIN\H_Williams	VPN3-9	26.03.2019	10:20	26.03.2019	11:20	60	1	39568624	4981491	Врем

It also contains the Sent/Received bytes, Disconnection_Reason (why the session has ened) and the Tunnel_TYPE (IKEv2, PPTP and etc) columns.

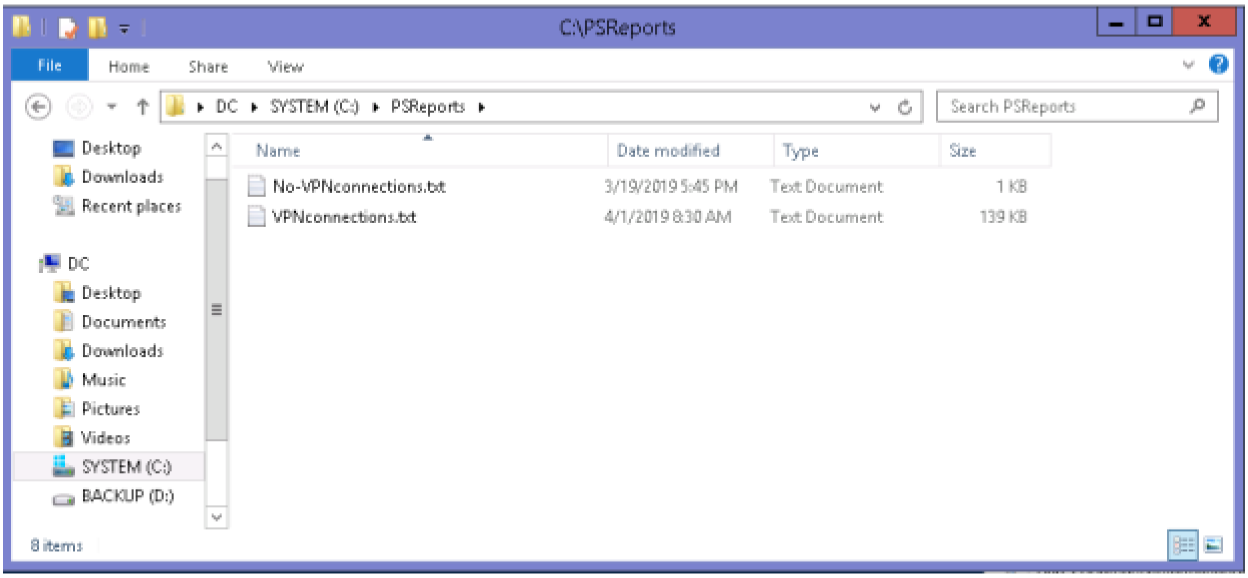
3) To find out which ip address was assigned to a particular user the following script – VPN1 – can be used:


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
VPN.ps1
VPN1.ps1*

```
# PS script
# V 1 14.03.2019

$f1="E:\PSReports"
If (!(Test-Path -Path "C:\PSReports"))
{
New-Item -ItemType Directory -Path $f1 > null
}

Try
{
$events = Get-WinEvent -FilterHashTable @{Logname='System';ID=20274} -ErrorAction Stop

}
Catch
{
Write-Output "No any event 20274 exists!" > $f1\No-VPNconnections.txt

$login = "sysadmin@hram1891.ru"
$password = "Ps1H7Nd@iw" | Convertto-SecureString -AsPlainText -Force
```

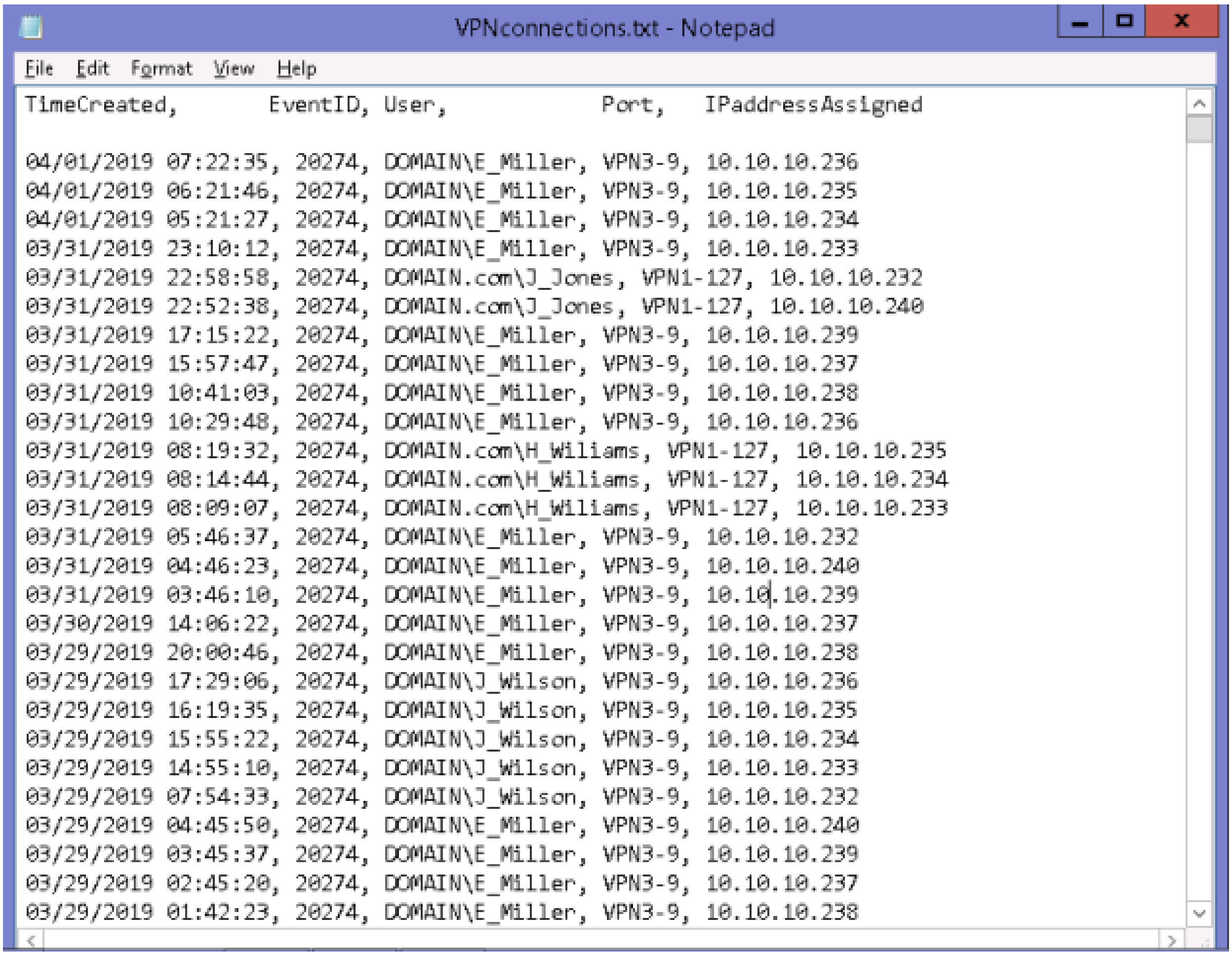
```
PS C:\Windows\system32>
```

The script creates either *VPNconnections.txt* or No-*VPNconnections.txt* file (in case there were no vpn connections) in the **C:\PSReports\** folder and sends it to *michael_firsov@testenterprise.com*:



```
Name                        Date modified        Type            Size
No-VPNconnections.txt       3/19/2019 5:45 PM    Text Document     1 KB
VPNconnections.txt          4/1/2019 8:30 AM     Text Document   139 KB
```

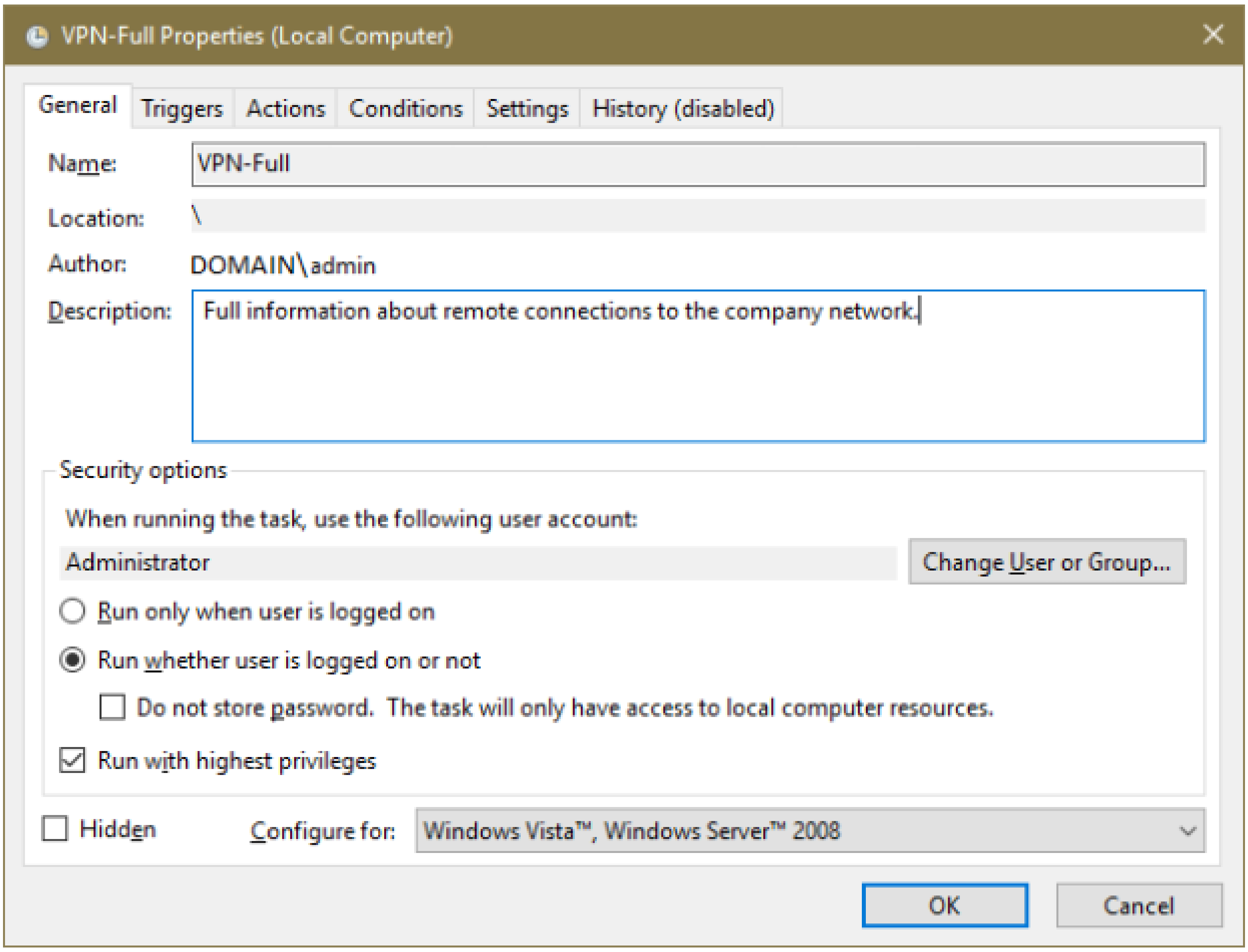
The report (a bit formated):



```
TimeCreated,       EventID, User,            Port,    IPaddressAssigned

04/01/2019 07:22:35, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.236
04/01/2019 06:21:46, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.235
04/01/2019 05:21:27, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.234
03/31/2019 23:10:12, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.233
03/31/2019 22:58:58, 20274, DOMAIN.com\J_Jones, VPN1-127, 10.10.10.232
03/31/2019 22:52:38, 20274, DOMAIN.com\J_Jones, VPN1-127, 10.10.10.240
03/31/2019 17:15:22, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.239
03/31/2019 15:57:47, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.237
03/31/2019 10:41:03, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.238
03/31/2019 10:29:48, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.236
03/31/2019 08:19:32, 20274, DOMAIN.com\H_Wiliams, VPN1-127, 10.10.10.235
03/31/2019 08:14:44, 20274, DOMAIN.com\H_Wiliams, VPN1-127, 10.10.10.234
03/31/2019 08:09:07, 20274, DOMAIN.com\H_Wiliams, VPN1-127, 10.10.10.233
03/31/2019 05:46:37, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.232
03/31/2019 04:46:23, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.240
03/31/2019 03:46:10, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.239
03/30/2019 14:06:22, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.237
03/29/2019 20:00:46, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.238
03/29/2019 17:29:06, 20274, DOMAIN\J_Wilson, VPN3-9, 10.10.10.236
03/29/2019 16:19:35, 20274, DOMAIN\J_Wilson, VPN3-9, 10.10.10.235
03/29/2019 15:55:22, 20274, DOMAIN\J_Wilson, VPN3-9, 10.10.10.234
03/29/2019 14:55:10, 20274, DOMAIN\J_Wilson, VPN3-9, 10.10.10.233
03/29/2019 07:54:33, 20274, DOMAIN\J_Wilson, VPN3-9, 10.10.10.232
03/29/2019 04:45:50, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.240
03/29/2019 03:45:37, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.239
03/29/2019 02:45:20, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.237
03/29/2019 01:42:23, 20274, DOMAIN\E_Miller, VPN3-9, 10.10.10.238
```

To have these reports at hand each morning the following scheduled tasks can be created:

VPN-Full



Name: VPN-Full

Location: \

Author: DOMAIN\admin

Description: Full information about remote connections to the company network.

Security options

When running the task, use the following user account:

Administrator

○ Run only when user is logged on

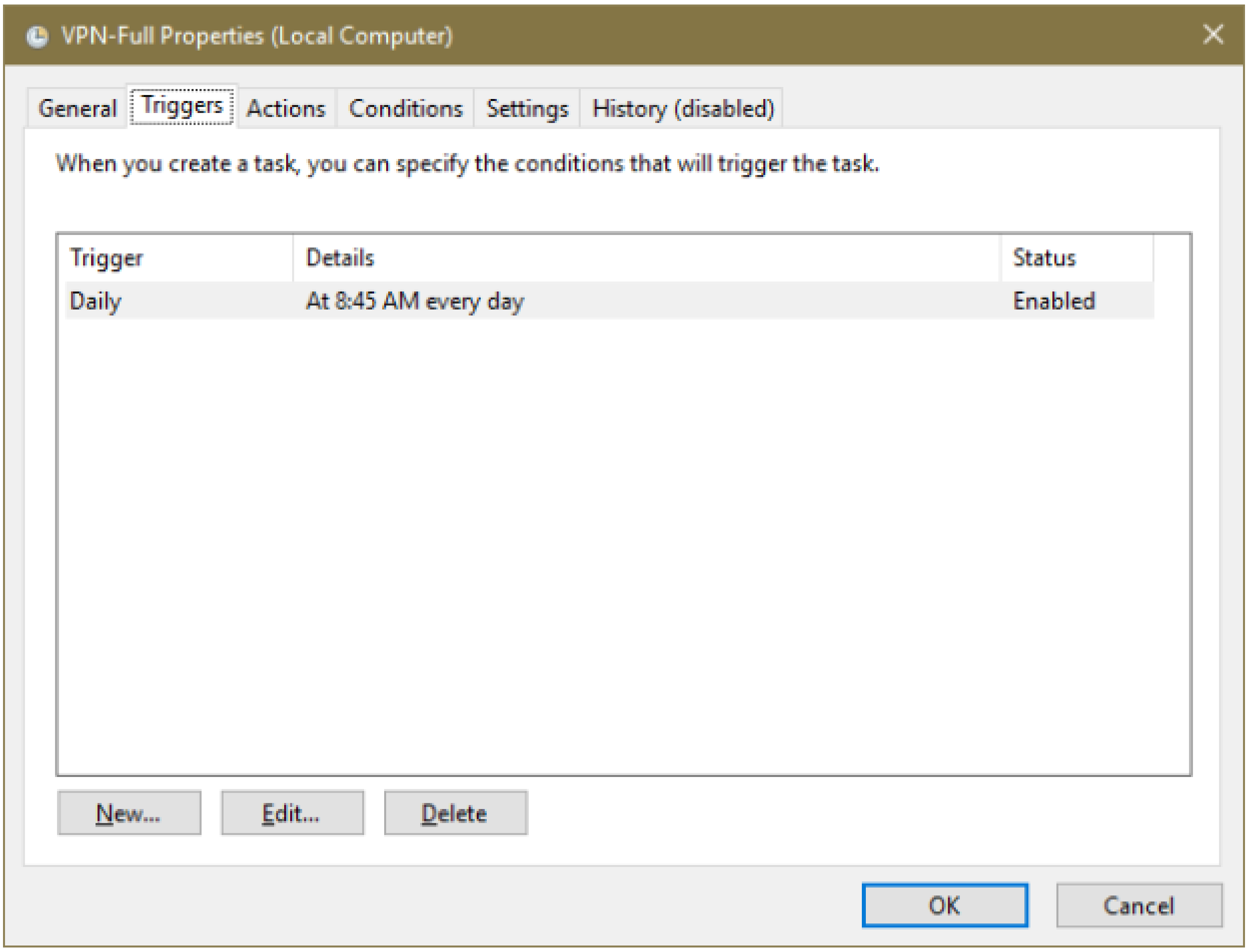
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

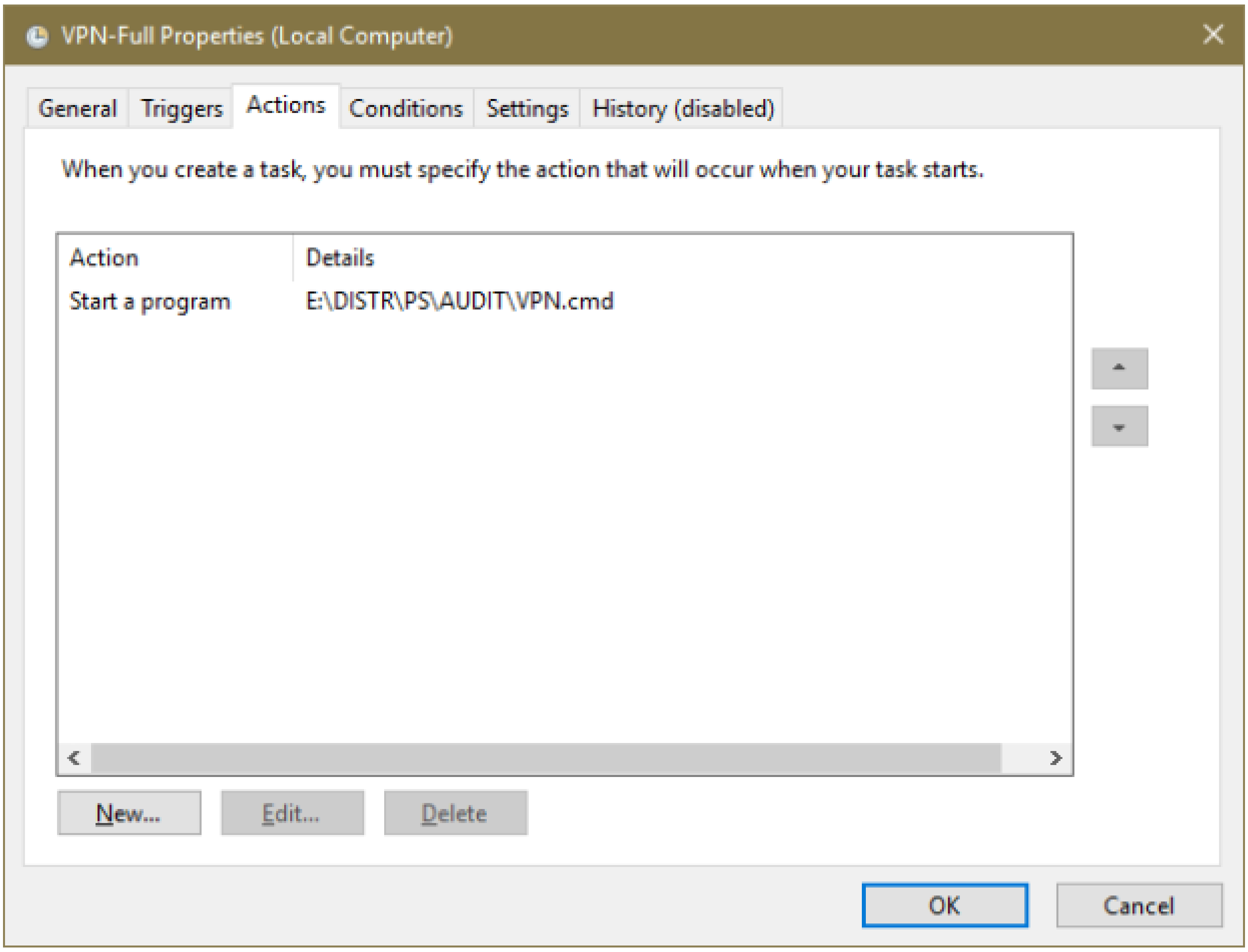
□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008



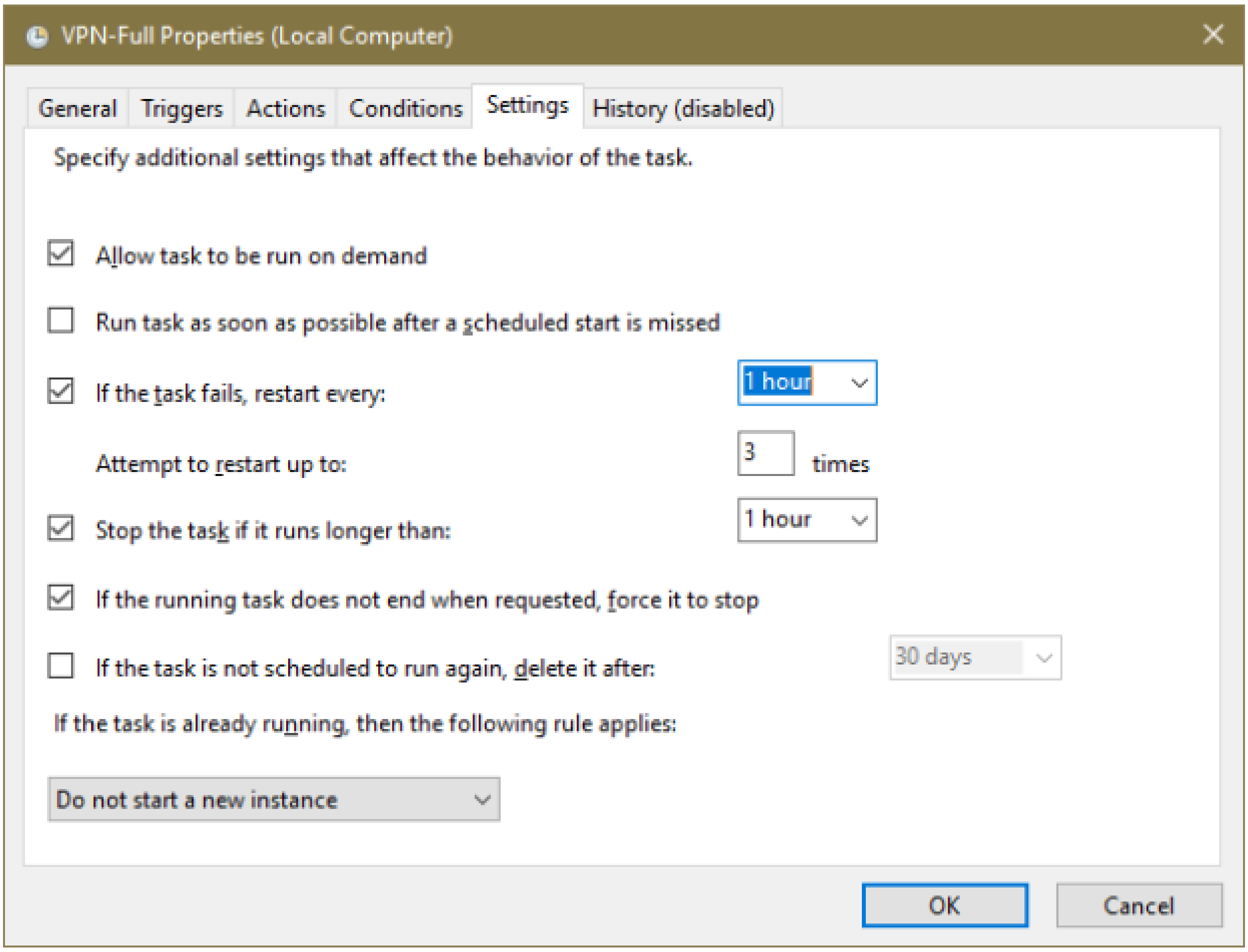
When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 8:45 AM every day	Enabled


VPN-Full Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	E:\DISTR\PS\AUDIT\VPN.cmd


VPN-Full Properties (Local Computer)

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 1 hour

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 1 hour

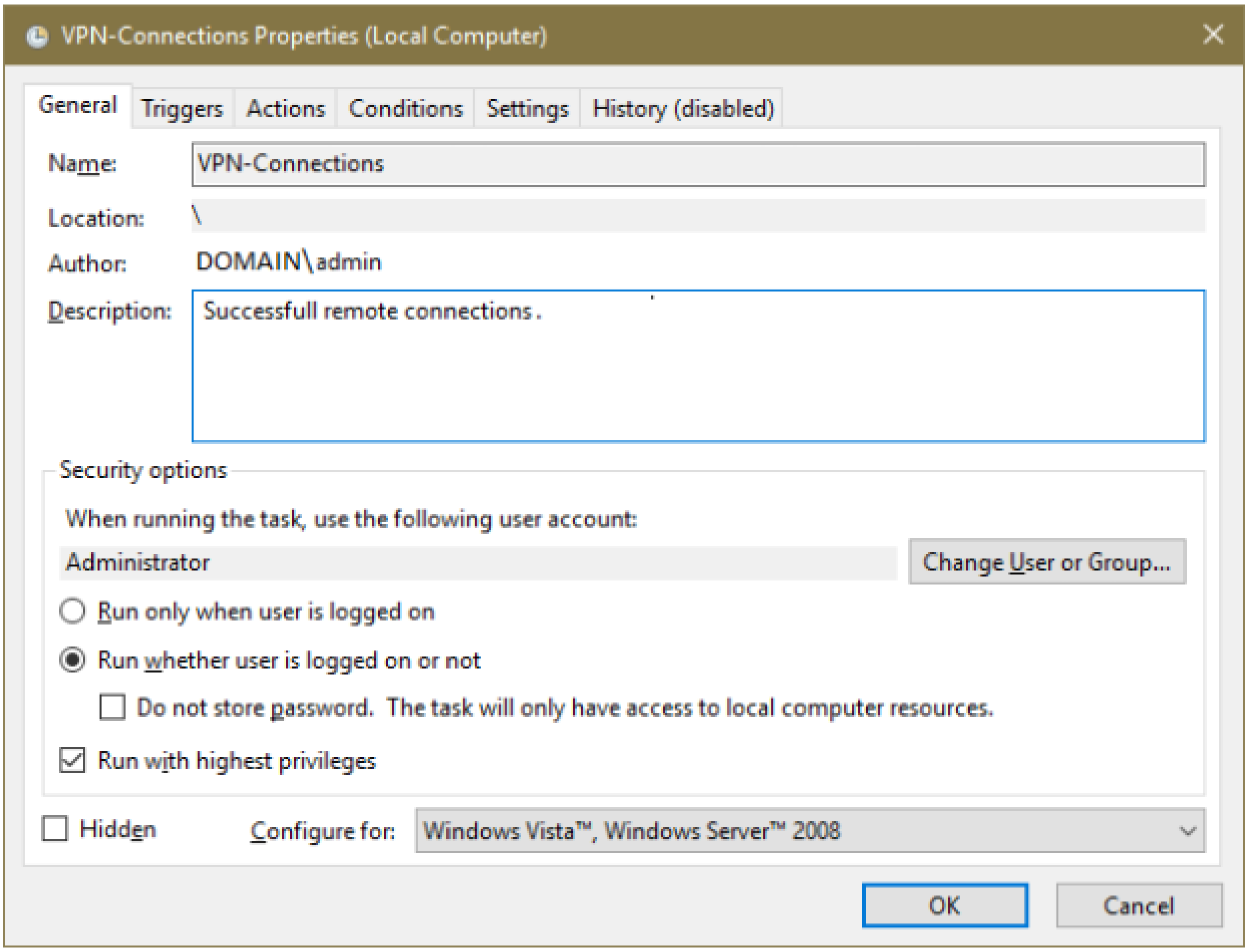
☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

VPN-Connections



Name: VPN-Connections

Location: \

Author: DOMAIN\admin

Description: Successfull remote connections.

Security options

When running the task, use the following user account:

Administrator

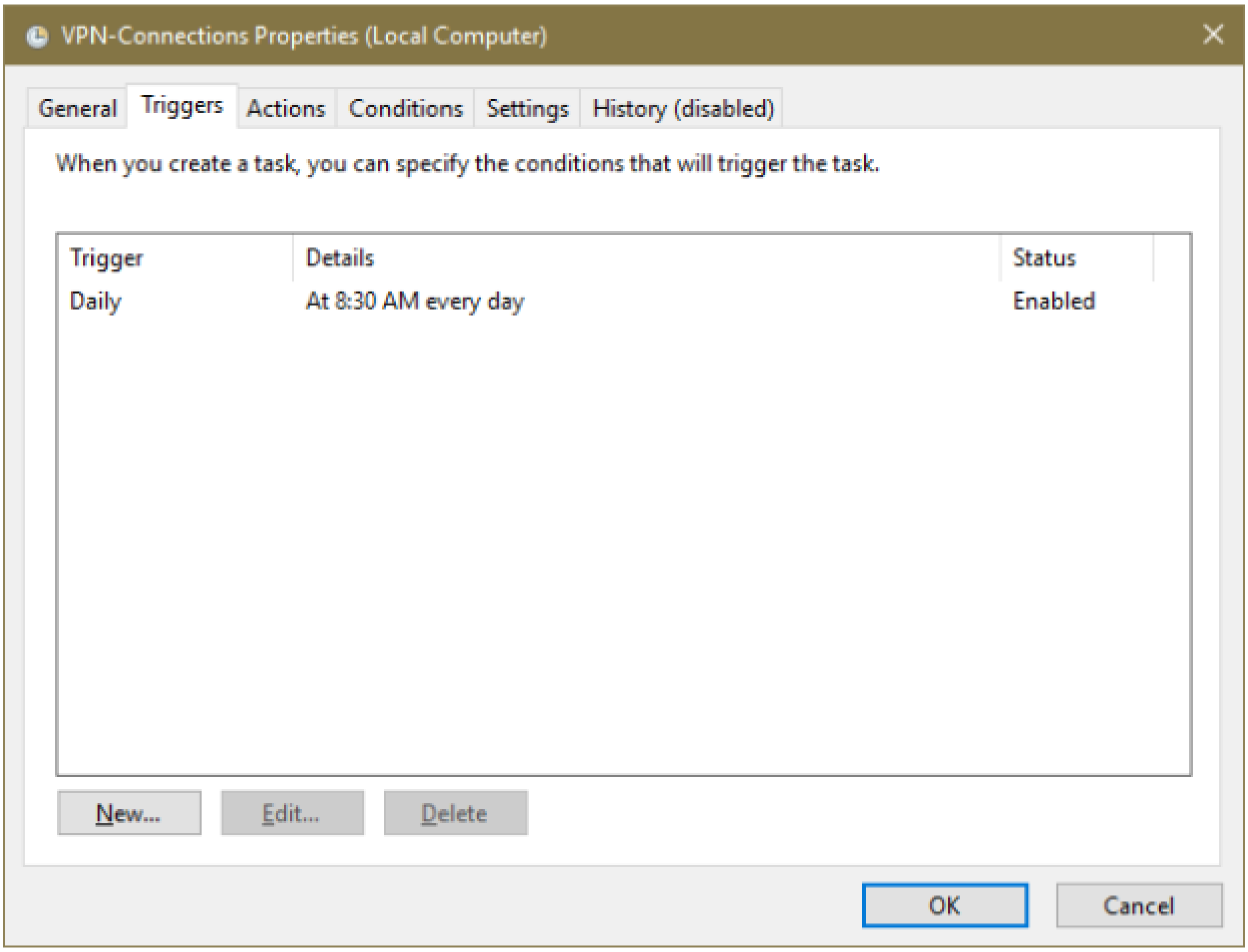
○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

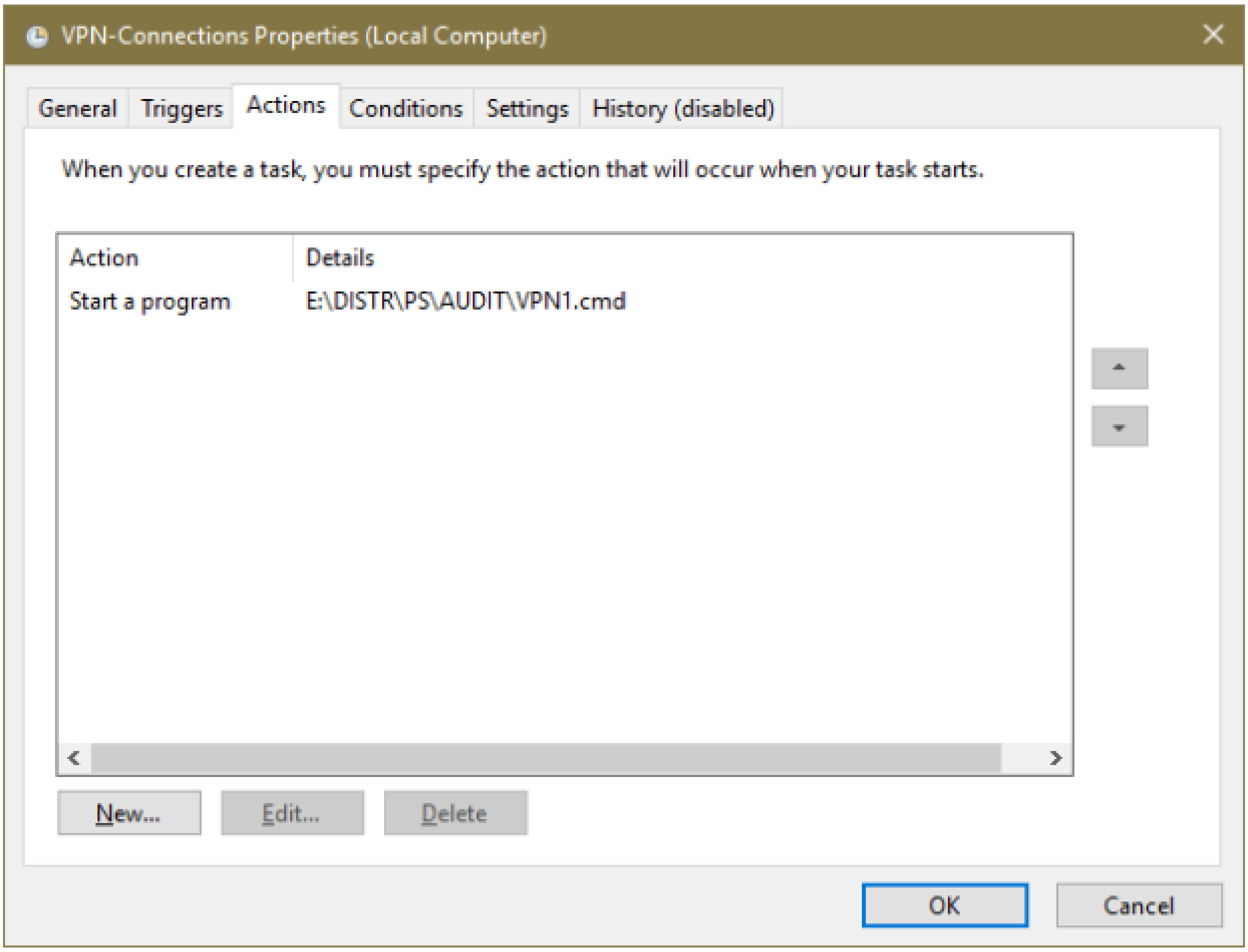
☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008



When you create a task, you can specify the conditions that will trigger the task.

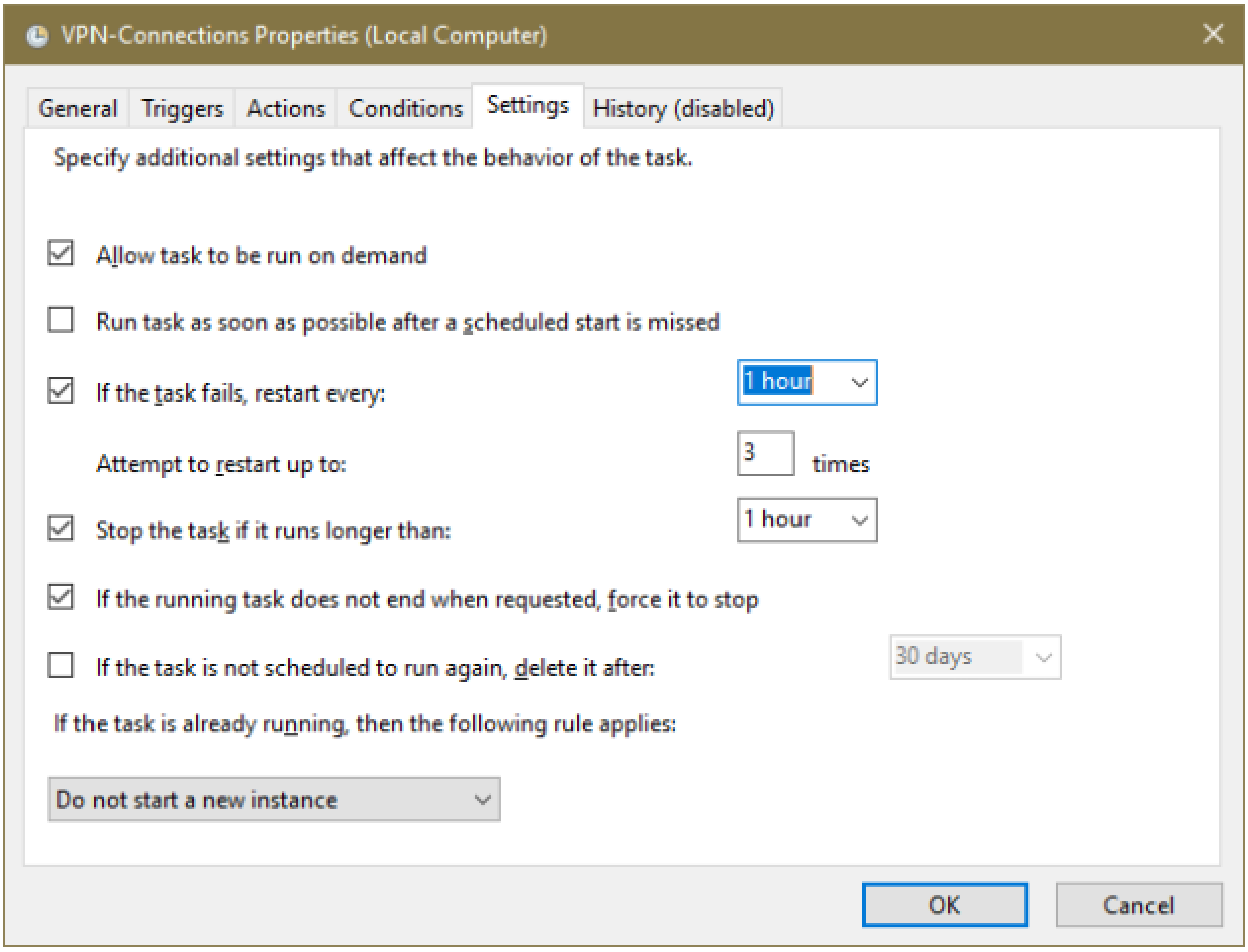
Trigger	Details	Status
Daily	At 8:30 AM every day	Enabled



VPN-Connections Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	E:\DISTR\PS\AUDIT\VPN1.cmd



VPN-Connections Properties (Local Computer)

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 1 hour

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 1 hour

☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

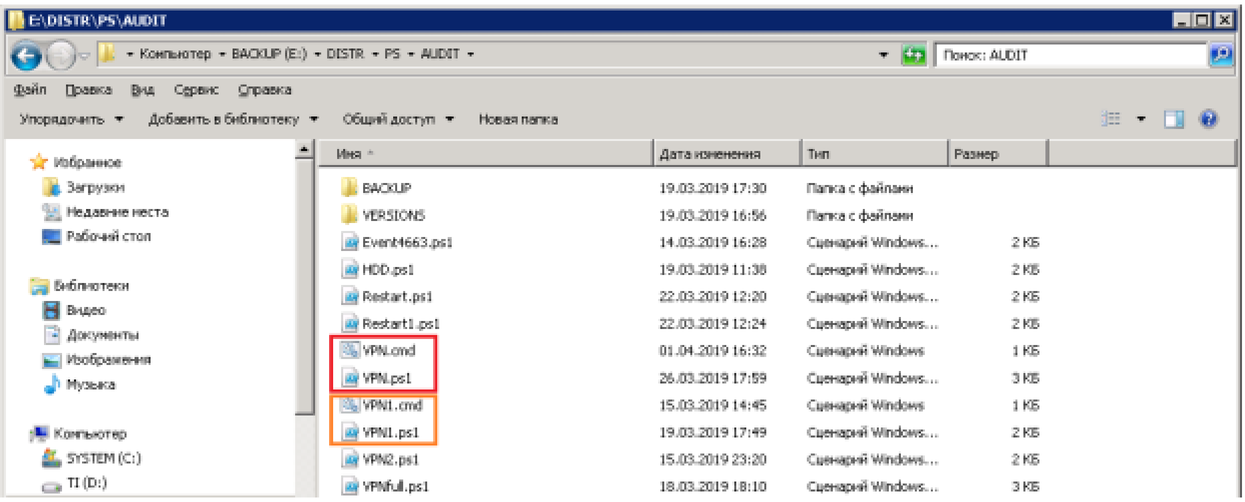
If the task is already running, then the following rule applies:

Do not start a new instance

In both scheduled tasks the role of .cmd files is just to start a corresponding .ps1 file:

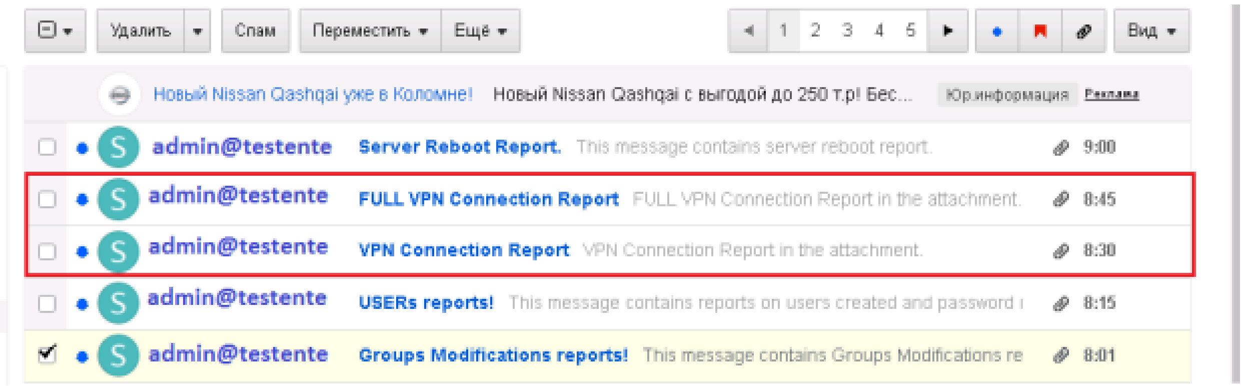
vpn.cmd
powershell -command .\VPN.ps1

vpn1.cmd
powershell -command .\VPN1.ps1



Имя	Дата изменения	Тип	Размер
BACKUP	19.03.2019 17:30	Папка с файлами	
VERSIONS	19.03.2019 16:56	Папка с файлами	
Event4663.ps1	14.03.2019 16:28	Сценарий Windows...	2 КБ
HDD.ps1	19.03.2019 11:38	Сценарий Windows...	2 КБ
Restart.ps1	22.03.2019 12:20	Сценарий Windows...	2 КБ
Restart1.ps1	22.03.2019 12:24	Сценарий Windows...	2 КБ
VPN.cmd	01.04.2019 16:32	Сценарий Windows	1 КБ
VPN.ps1	26.03.2019 17:59	Сценарий Windows...	3 КБ
VPN1.cmd	15.03.2019 14:45	Сценарий Windows	1 КБ
VPN1.ps1	19.03.2019 17:49	Сценарий Windows...	2 КБ
VPN2.ps1	15.03.2019 23:20	Сценарий Windows...	2 КБ
VPNfull.ps1	18.03.2019 18:10	Сценарий Windows...	3 КБ

The result:


Удалить
Спам
Переместить
Ещё
1 2 3 4 5
Вид
Новый Nissan Qashqai уже в Коломне! Новый Nissan Qashqai с выгодой до 250 т.р! Бес...
Юр.информация
Реклама

□	admin@testente	Server Reboot Report.	This message contains server reboot report.	9:00
□	admin@testente	FULL VPN Connection Report	FULL VPN Connection Report in the attachment.	8:45
□	admin@testente	VPN Connection Report	VPN Connection Report in the attachment.	8:30
□	admin@testente	USERs reports!	This message contains reports on users created and password ı	8:15
☑	admin@testente	Groups Modifications reports!	This message contains Groups Modifications re	8:01

This part concludes the series on automating system administration tasks. I hope the information in these articles may help administrators collect the nesessary information about their server infrastructures a bit more easily.