

ESET Tech Center

Kennisbank > Legacy > Enable advanced logging in ESET Endpoint Security (6.x)

Enable advanced logging in ESET Endpoint Security (6.x)

Anish | ESET Nederland - 2018-03-07 - Reacties (0) - Legacy

Issue

Create a log of all connections blocked by the ESET firewall
Enable advanced logging of the firewall

Solution

If you do not use ESET Remote Administrator to manage your network

[Perform these steps on individual client workstations.](#)

I. Activate logging of blocked connection in ESET Remote Administrator

ERA 6.5 User Permissions

This article assumes that your ERA user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):


[Create a second administrator user in ESET Remote Administrator 6.5](#)

View
w
per
mis
sion
s
nee
ded
for
leas
t
priv
ileg
e
use
r
acc
ess

1. Op
en
ES
ET
Re
mo
te
Ad
mi
nis
tra
tor
We
b
Co

[ns](#)
[ole](#)
(E
RA
We
b
Co
ns
ole
) in
yo
ur
we
b
bro
ws
er
an
d
log
in.

2. Click **Admi**
n 
→ **Pol**
ici
es
→ **Ne**
w
Pol
icy

.
To
edi
t
an
exi
sti
ng
pol
icy,
sel
ect
the
en
dp
oin
t
pol
icy
tha
t
yo
u
wa
nt
to
mo
dif
y
an
d
clie
k
the
ge
ar
ico
n

→
Edi

t.



Figure 1-1
Click the image to view larger in new window

3. Type a name for the new policy in the

Na
me
fiel
d.



Fig
ure
1-2
Clic
k
the
ima
ge
to
vie
w
lar
ger
in
ne
w
win
do
w

4. Exp
and
the
Set
tin
gs
sec
tion
and
sel
ect

Endpoint for Windows.

5. Click **Tools** → **Diagnostics**.

6. Click the slider bar next to **Enable Firewall advanced logging**.



Figure 1-3
Click the image to view larger in new window

7. Expand the **Assignment** section, click **Add Computers**,

select the client for the policy and then click **OK**.



Figure 1-4
Click the image to view larger in new window

8. Click **Finish**. The policy will be applied on the client computer. With logging enabled, repeat the action that is blocked by the firewall

and
the
n
con
tinu
e to
Par
t II.

II.
Do
wn
loa
d
an
d
ru
n
th
e
ES
ET
Lo
g
Co
lle
ct
or
to
ol

The
ESE
T
Log

Collect or will create the firewall log along with other logs to help ESE Technical support resolve your

issue
quickly
.

9. [Download and run the ESE IT Log Collector tool](#)
.

10. Include the log file that the tool produces in your email response

se
to
ESE
T
tec
hni
cal
sup
por
t. If
you
hav
e
not
alre
ady
ope
ned
a
cas
e
wit
h
ESE
T
tec
hni
cal
sup
por
t, [c
om
plet
e a
tec
hni
cal
sup
por
t re
que](#)

[st](#) and submit the file you just saved to ESET Technical support for analysis.

11. To stop recording logs of all blocked connections, rep

eat
the
steps
in
the
[Activate logging of the firewall](#)
section
and
click
the
slider
bar
next
to
Enable firewall advanced logging
to

dis
abl
e it
in
ste
p 6.
Clic
k **Fi
nis
h.**

If
adv
anc
ed
log
gin
g is
not
dis
abl
ed,
it
will
gen
era
te
a la
rge
log
file.



**Fig
ure
1-5
Clic
k
the
ima**

ge
to
vie
w
lar
ger
in
ne
w
win
do
w

Usi
ng
Ov
err
ide
m
od
e
in
ES
ET
Re
m
ot
e
Ad
mi

nis
tra
tor

ESE

T

end

poi

nt

ver

sion

6.5

pro

duc

ts

incl

ude

s an

Ove

rrid

e

mo

de

opti

on.

Wh

en

Ove

rrid

e

mo

de

is

enabled from mERA Web Console, a user on a client machine can change the settings in the installed ESET

end
point
product,
even if
the
settings
were
e
locked
ed
by
ano
ther
poli
cy.
Afte
r
the
cha
nge
s
hav
e
bee
n
con
figu

red
on
the
the
client
machine,
the
configuration
can
be
requested
and
saved
as a
new
policy
that
can
be
then
applied

on
oth
er
co
mp
uter
s.

[Clic
k
for
mor
e
info
rma
tion
abo
ut
Ove
rrid
e
mo
de.](#)

[Ac
tiv
at
e
log
gi
ng](#)

of
blo
ck
ed
co
nn
ec
tio
ns
in
ES
ET
En
dp
oin
t
Se
cu
rit
y

1. Op
en
the
mai
n
pro
gra
m
win
do
w

of
you
r
Win
do
ws
ESE
I
pro
duc
t.

2. Press the **F5** key to access Advanced setup.
3. Click **Tools** → **Diagnos**
tics.
4. Click the

slider bar next to **Enable Firewall advanced logging** and then click **OK**.



Figure 2-1

5. With logging enabled, repeat

the
acti
on
tha
t is
blo
cke
d
by
the
fire
wall
and
the
n
con
tinu
e to
Par
t II.

II.
Do
wn
loa
d
an
d
ru
n
th
e
ES
ET

Lo g Co lle ct or to ol

The
ESE
T
Log
Coll
ect
or
will
cre
ate
the
fire
wall
log
alo
ng
wit
h
oth
er
logs
to
hel
p

ESE
T
tec
hni
cal
sup
port
res
olv
e
you
r
issu
e
qui
ckly
.

6. [Do
wnl
oad
and
run
the
ESE
T
Log
Coll
ect
or
tool](#)
.

7. Incl
ude
the
log

file
tha
t
the
tool
pro
duc
es
in
you
r
em
ail
res
pon
se
to
ESE
T
tec
hni
cal
sup
por
t. If
you
hav
e
not
alre
ady
ope
ned
a
cas
e
wit
h
ESE
T
tec

hni
cal
sup
por
t, c
om
plet
e a
tec
hni
cal
sup
por
t
req
ues
t an
d
sub
mit
the
file
you
just
sav
ed
to
ESE
T
tec
hni
cal
sup
por
t
for
ana
lysi
s.

8. To

stop recording logs of all blocked connections, repeat the steps in the [Activate logging of the firewall](#) section and click the slider bar

next
to
**Enable
firewall
advanced
logging**
to
disable
it
in
step 6.
Click **Finish**.

Disable advanced logging when you have finished collecting logs

Make sure you disable advanced logging after you collect the logs you need. It will generate a large log file if you forget to disable it.

