

ESET Tech Center

Kennisbank > Legacy > Legacy ESET Remote Administrator (6.x / 5.x / 4.x) > 6.x > How do I create or edit firewall rules for client workstations in ESET Remote Administrator? (6.x)

How do I create or edit firewall rules for client workstations in ESET Remote Administrator? (6.x)

Ondersteuning | ESET Nederland - 2017-12-05 - Reacties (0) - 6.x

<https://support.eset.com/kb3718>

Issue

Create, edit, or delete a firewall rule for client workstations running ESET Endpoint Security
Create, edit, or delete firewall rules on individual client workstations

Solution

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

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

Create or edit firewall rules in ESET Remote Administrator

Permissions changes in ESET Remote administrator 6.5 and later

Before proceeding, please note important changes to user access rights and permissions in the latest versions of ESET Remote Administrator.

[View](#)

[Per
mis
sion
s
Cha
nge
s](#)

[Vie
w
per
mis
sion
s](#)
Once
e
the
se
per
mis
sion
s
are
in
plac
e,
foll
ow
the
ste
ps
bel
ow.

1. Open
ESE
I
Re
mot
e
Ad
min
istr
ato
r
We
b
Con
sol
e (E
RA
We
b
Con
sol
e)
in
you
r
we
b
bro
wse
r
and

log
in.


2. Click **Admin**  → **Policies**, select the policy that you want to edit and then click **Policies** → **Edit**.



Figure 1-1
Click the

**image
to
view
w
larger
in
new
window
w**

3. To apply a rule
Expand **Settings** → **Personal Firewall** all → **Advanced** and click **Edit**

next
to
Rules.



Figure 1-2
Click the image to view larger in new window

4. Click **Add** and set the parameters

for
you
r
rule
in
the
the
**Ge
ner
al,
Loc
al,
and
Re
mo
te** t
abs
.

Ed
iti
ng
an
d
re
m
ov
in
g
rul
es
**To
edi
t a
rul
e:**
Sel

ect
the
rule
you
wa
nt
to
mo
dify
and
clic
k **E**
dit.
To
re
mo
ve
a
rul
e:
Sel
ect
the
rule
you
wa
nt
to
re
mo
ve
and

click **Remove**.



Figure 1-3

5. Set any combination of the following parameters in the **General** tab to define your new rule

- :
- Type a name for your rule into the **Name** field.
- Select **Both, In** or **Out** from the **Direction** dropdown menu.
- Select

All
ow
,
D
en
y o
r **A**
sk
fro
m
the
Ac
tio
n d
rop
-
dow
n
me
nu.
• The **P**
rot
oc
ol
an
d **P**
ro
file
se
ttin
gs
are
not
ma
nd
ato
ry,
but
ca
n
be

use
d
to
mo
re
pre
cis
ely
tar
get
a
rul
e.

- Select the check box next to **Log** and/or **Notify user** to have ES ET Remote Ad

ministrator automatically perform the selections when the rule is triggered.



Figure 1-4

6. Set any combination of the following

ng
par
am
ete
rs
in
the
Loc
al t
ab:

- **Port:** specify a port or range of ports this rule will target.
• Multiple entries must be delimi

ted
by
a
co
m
ma
, or
yo
u
ca
n
spe
cify
a
ran
ge
of
por
ts,
for
ex
am
ple
10
00-
20
00.

- **IP:** spe
cify
an
IP
ad
dre
ss
or
ran
ge
thi
s
rul

e
will
tar
get

- **Zo
ne
s:**
clic
k **A
dd**
to
[spe
cify
zon
es
wh
ere
thi
s
rul
e
will
ap
ply](#)

- **Ap
pli
cat
ion**
: to
tar
get
a
spe
cifi
c
ap
plic
ati
on,

type
the
.exe
file
for
the
app
lic
ati
on
int
o
thi
s
fiel
d.

- **Service:** to target a specific service, type the name of the service

int
o
thi
s
fiel
d.



**Fig
ure
1-5**

7. Set any combination of the following parameters in the **Remote** tab:

- **Port:** specify a port or

range of ports this rule will target.
Multiple entries must be delimited by a comma, or you can specify a range of

ports,
for
ex
am
ple
10
00-
20
00.

- **IP:**
spe
cify
an
IP
ad
dre
ss
or
ran
ge
thi
s
rul
e
will
tar
get

- **Zone**
s:
clic
k **A**
dd
to
[spe](#)
[cify](#)
[zon](#)
[es](#)
[wh](#)

ere
thi
s
rul
e
will
ap
ply
.



**Fig
ure
1-6**

8. Wh en you are fini she d ma kin g cha nge s to rule par am ete rs, clic k **O K**. You r new rule will

appear in the **Firewall rules** window. Click **OK** again to close the **Firewall rules** window.



Figure 1-7

9. Click **Finish**. Client wor

kst
atio
ns
will
rec
eiv
e
you
r
new
rule
the
nex
t
tim
e
tha
t
the
y
che
ck
in
to
ESE
T
Re
mot
e
Ad
min
istr
ato
r.

Ed

it
fir
ew
all
rul
es
on
in
div
id
ual
cli
en
t
wo
rks
tat
ion
s

1. Op
en
ESE
T
End
poi
nt
Sec
urit
y.
[Op](#)
[en](#)

my
ESE
I
pro
duc
t.

2. Press the **F5** key to access Advanced setup. Click **Firewall** and then click **Edit** next

to
Rul
es.



Fig
ure
2-1

3. Clic
k **A**
dd
and
set
the
par
am
ete
rs
for
you
r
rule
in
the
the **Ge**
ner
al,
Loc
al,
and **Re**
mo
te t
abs
.



Fig
ure

2-2

Ed
iti
ng
an
d
re
m
ov
in
g
rul
es

**To
edi
t a
rul
e:**

Sel
ect
the
rule
you
wa
nt
to
mo
dify
and
cl
ic
k **E**

dit.
To
re
mo
ve
a
rul
e:
Sel
ect
the
rule
you
wa
nt
to
re
mo
ve
and
clic
k **R**
em
ov
e.

4. Set any combination of the

following parameters in the **General** tab to define your new rule :

- Type a name for your rule into the **Name** field.
- Select

Both, In or Out from the **Direction** dropdown menu.

- Select **Allow, Deny** or **Ask** from the **Action** dropdown menu.

- The **P**

rot
oc
ol
an
d **P**
ro
file
se
ttin
gs
are
not
ma
nd
ato
ry,
but
ca
n
be
use
d
to
mo
re
pre
cis
ely
tar
get
a
rul
e.

- Use the **Lo**
ggi
ng
se
ve

rit
y d
rop
-
dow
n
me
nu
to
set
yo
ur
pre
fer
en
ce
for
the
typ
es
of
ev
ent
s
to
log
. Select
ect **N**
on
e t
o
rec
ord
no
log
s
wh
en
thi

s
rul
e is
trig
ger
ed.
**Di
ag
no
sti
c** w
ill
log
all
ev
ent
s. **I
nf
or
ma
tio
n**
will
log
not
ific
ati
ons
ab
out
up
dat
es.
**Wa
rni
ng**
will
log
wa
rni
ng

not
ific
ati
ons
not
rel
ate
d
to
sys
te
m
err
ors

- Select the check box next to **Notify user** to have ES ET Endpoint Security

ity display a notification when the rule is triggered.



Figure 2-3

5. Set the following parameters in the **Local** tab:
 - **Port:** specify

a
por
t or
ran
ge
of
por
ts
thi
s
rul
e
will
tar
get
. Mul
tipl
e
ent
rie
s
mu
st
be
del
imi
ted
by
a
co
m
ma
, or
yo
u
ca
n
spe
cify
a

range of ports, for example 10.00.20.00.

- **IP:** specify an IP address or range this rule will target.

- **Zones:** click **Add** to [specify](#)

zon
es
wh
ere
thi
s
rul
e
will
ap
ply

- To target a specific application with your rule, click browse (...) under **A pplica**

tion,
navigate to the .exe file for the target application and then click **Open**.

- To target a specific service with your rule

e,
use
the
Se
rvi
ce
dro
p-
do
wn
me
nu
to
sel
ect
the
tar
get
ser
vic
es
fro
m
ser
vic
es
run
nin
g
on
yo
ur
co
mp
ute
r.



Fig
ure

2-4

6. Set the following parameters in the **Remote** tab:

- **Port:** specify a port this rule will target.
• Multiple entries must be

delimited by a comma, or you can specify a range of ports, for example 1000-2000.

- **IP:** specify an IP address or range thi

s
rul
e
will
tar
get
.

- **Zo
ne
s:**
cl
ic
k **A
dd**
to
spe
cify
zon
es
wh
ere
thi
s
rul
e
will
ap
ply



**Fig
ure
2-5**

7. Wh
en
you
are
fini
she
d

making changes to rule parameters, click **OK**. Your new rule will appear in the **Firewall rules** window. Click **OK** again to close the **Fire**

**all
rules**
win
do
w.



**Fig
ure
2-6**

8. Click **O
K** to
save
your
changes
and
exit
Advanced
setup.
Client
worksta-
tions
will
receive
you

r
new
rule
the
next
t
tim
e
the
y
che
ck
in
to
ESE
T
Re
mot
e
Ad
min
istr
ato
r.

Tags
Endpoint
ERA 6.x