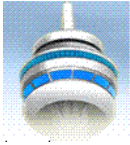




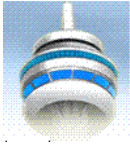
You are accessing confidential information belonging to Panda Security. This information is for the exclusive use of companies belonging to Panda Security. It may not be distributed, copied, divulged or transferred in any way without prior written permission from Panda Security.

© **Panda Security 2008**

Any total or partial reproduction of this document is strictly forbidden without prior written permission from Panda Security. Other product names that are mentioned in this guide may be registered trademarks of their respective owners.



Blocking of P2P applications in Panda for Desktops and Panda for FileServers



Contents

INTRODUCTION.....	4
P2P APPLICATION BLOCKING.....	5
1. PREVENT P2P APPLICATIONS FROM RUNNING.....	5
2. DENY P2P APPLICATION COMMUNICATIONS.....	24
3. SYSTEM RULES	36



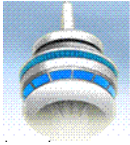
Introduction

This document describes the steps to block P2P applications from the AdminSecure console.

Since applications are blocked by defining TruPrevent security policies, the computers on which you want to apply the policies must have TruPrevent.

This document describes several ways of blocking applications so administrators can choose the one that best suits their needs.

Although the current document is based on P2P applications, the information applies to other applications.



P2P application blocking

1. Prevent P2P applications from running

This procedure allows administrators to define a list of applications that cannot be run on selected computers.

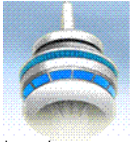
To do so, in the AdminSecure console select the computer or group of computers you want to prevent applications from running on.

The screenshot shows the AdminSecure Console 2007 interface. The main window displays the 'Windows Workstations status' table, which lists the installed Panda Security for Desktops on the WXP_DESKTOP machine. The 'Control panel' on the left shows the 'Windows Workstations' folder selected. Below the table, the 'Protection settings' section is visible, showing a list of protection modules and their status.

Module	Product installed	Threat signature	Enabled	Last connection
wXP_DESKTOP	Panda Security for Desktops [4.02.32]	5/11/2008 1:10 PM	✓	5/12/2008 5:19:04 PM

Protection	Installed	Enabled	Updated
Protection : Antivirus			
HTTP antivirus protection	✓	✓	✓
Email and messaging protection	✓	✓	✓
File protection	✓	✓	✓
Protection : TruPrevent			
TruPrevent	✓	✓	✓
Protection : Content Filter			

Once you have selected the computers, modify the protection settings.



AdminSecure Console 2007 (Server: W2KS_ADMIN) (User: W2KS_ADMIN\ADMINISTRADOR)

File Edit View Protection Tools Help

Install protection Uninstall protection Update Distribute communications agent Include content of subgroups Automatic exclusions and removals...

Control panel

Information monitors

- Dashboard
- Activity
- Jobs and Scans
- Events log

Show data for...

- My organization
- Lost and found
- Windows Servers
- Windows Workstations
 - WXP_DESKTOP

Switch to view of computers by

Control panel

- Installation and update
- Protection settings
- Quarantine
- Audit
- Reports
- Services

Windows Workstations status Switch to category view

Module	Product installed	Threat signature	Enabled	Last connection
WXP_DESKTOP	Panda Security for Desktops (4.02.32)	5/11/2008 1:10 PM	✓	5/12/2008 5:25:28 PM

Context menu for WXP_DESKTOP:

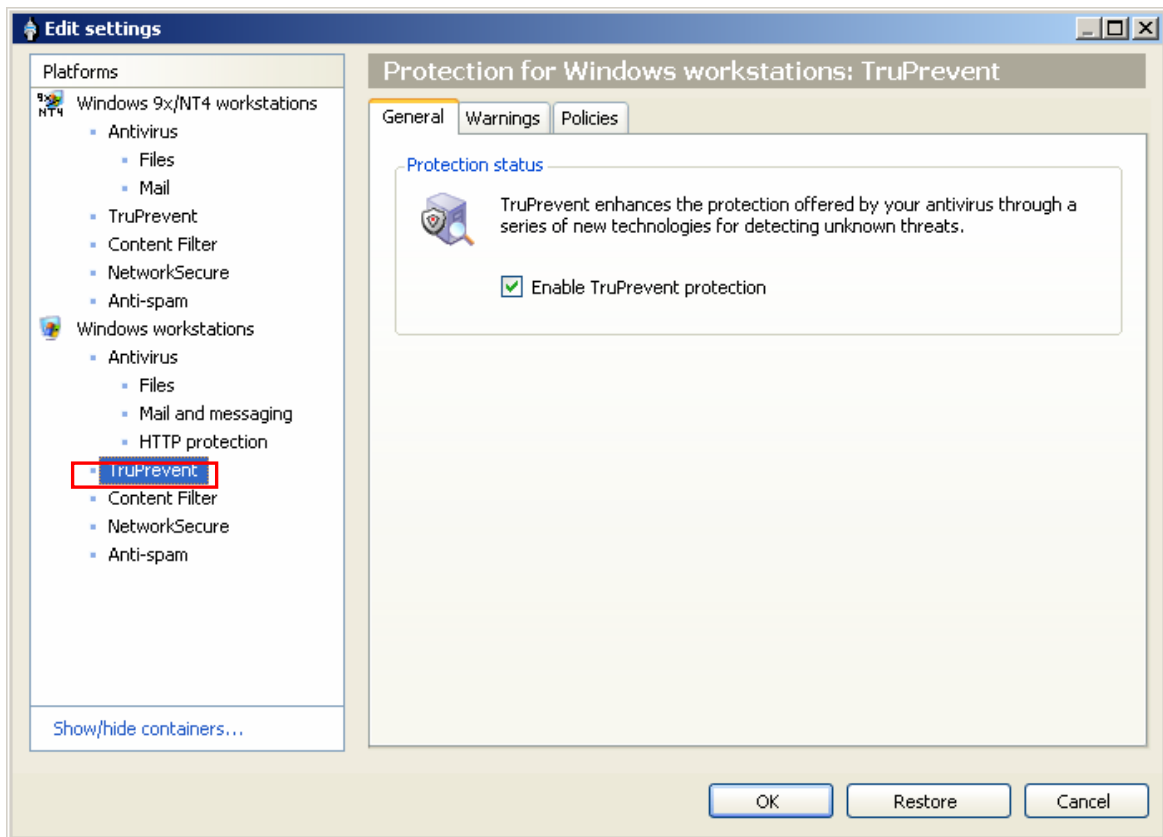
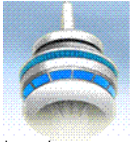
- Install protection...
- Uninstall protection...
- Update protection...
- Modify settings...**
- Add scan...
- Scan Windows servers...
- Scan Windows workstations...
- Add subgroup Ins
- Undo group
- Change name
- Modify rules...
- Uninstall the communications agent
- Delete
- Refresh computer information
- Move modules to group
- Refresh tree FS

	Installed	Enabled	Updated
	✓	✓	✓
	✓	✓	✓
	✓	✓	✓

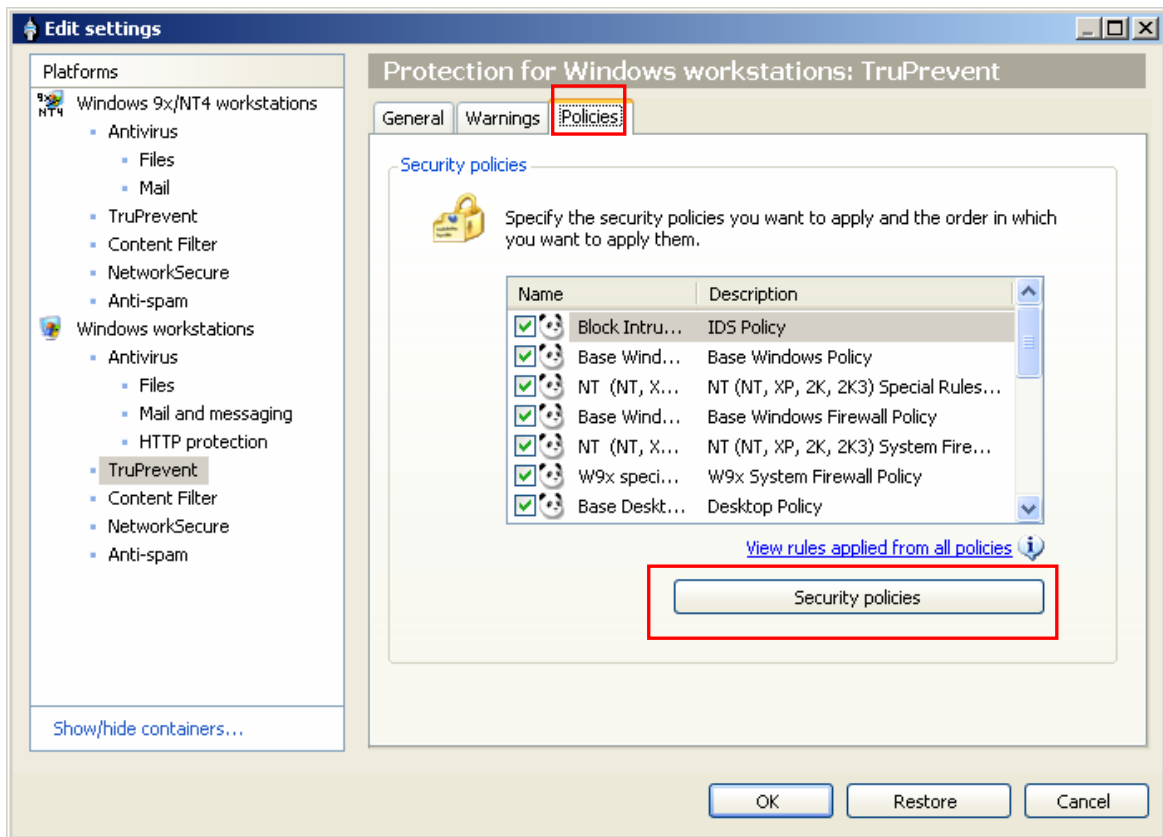
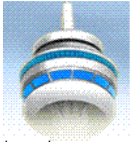
1 of 1 item(s) selected

✓ Yes ✗ No ⚠ Partially

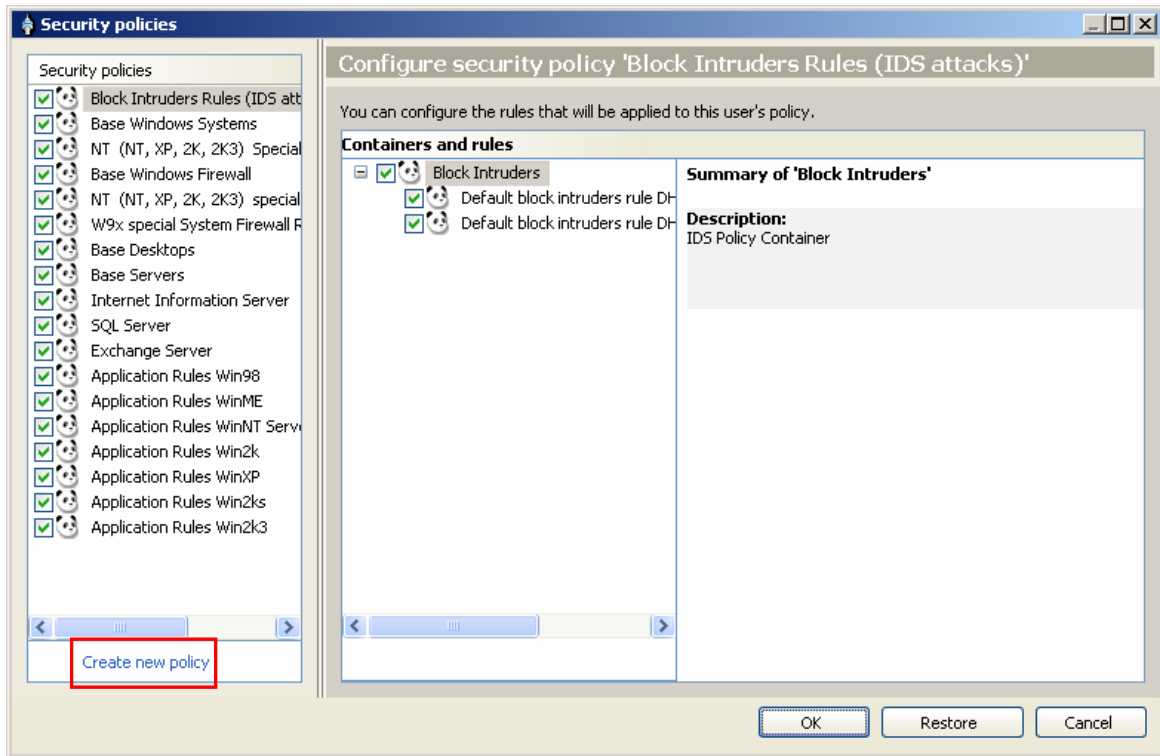
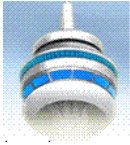
Go to TruPrevent **Settings**, since TruPrevent allows you to configure the blocking of applications, etc.



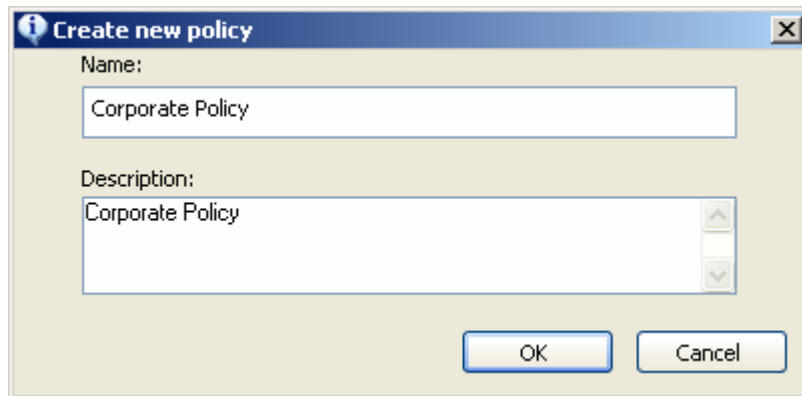
In the TruPrevent settings, select the **Policies** tab and click **Security policies**.



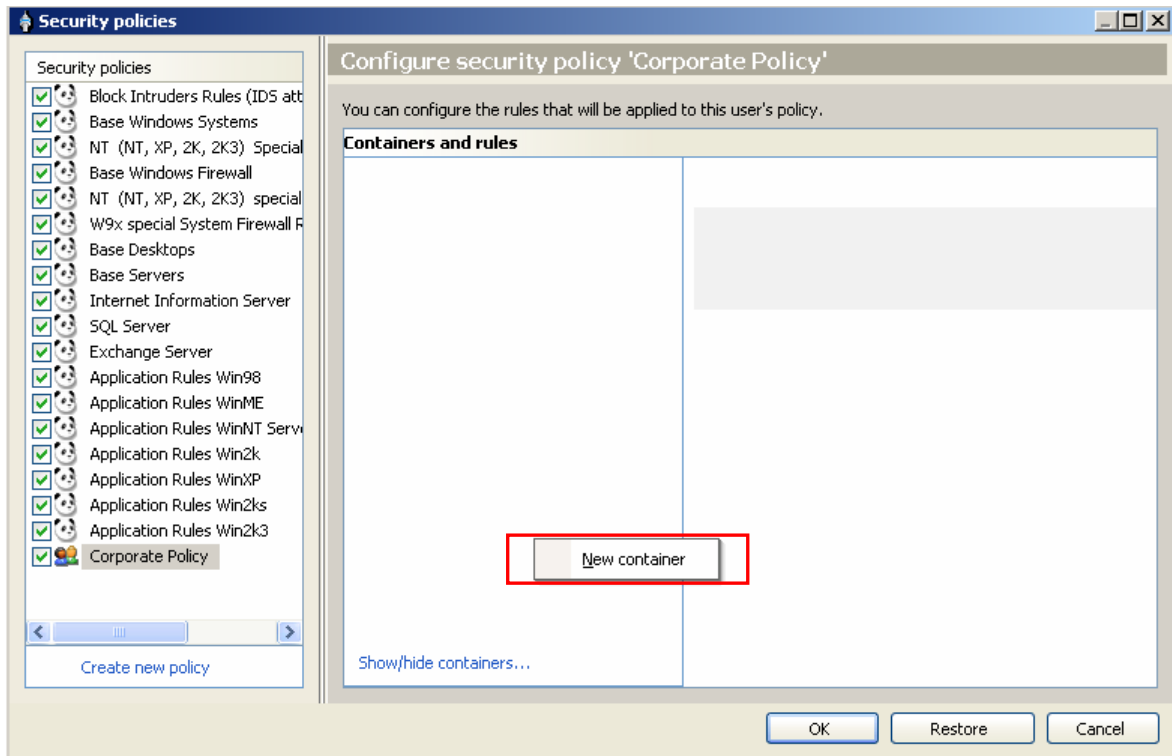
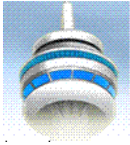
The list of security policies predefined by Panda and those defined by the user are displayed. To define a new security policy, click **Create new policy**.



Enter the name of the policy and a description (optional).



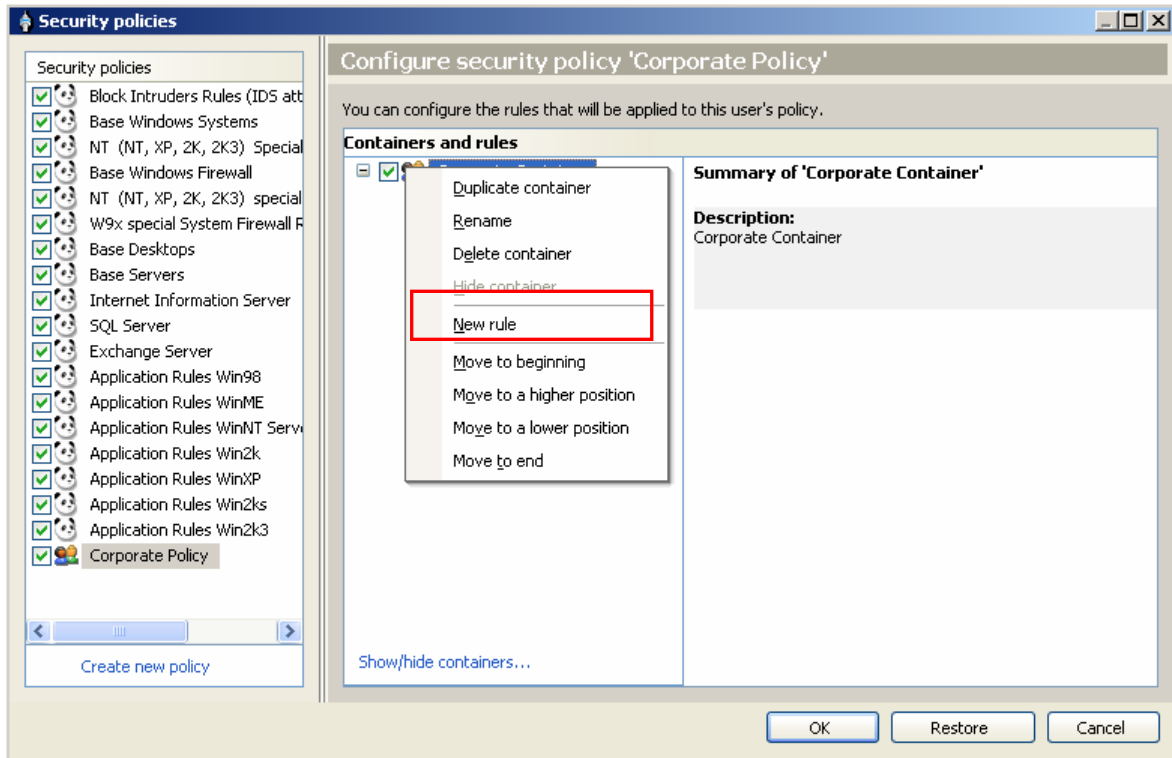
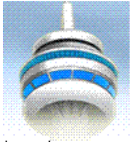
Once the policy is created, you have to create a container that groups the set of rules to be defined, in this case, to block P2P applications. To do so, click **New container**.



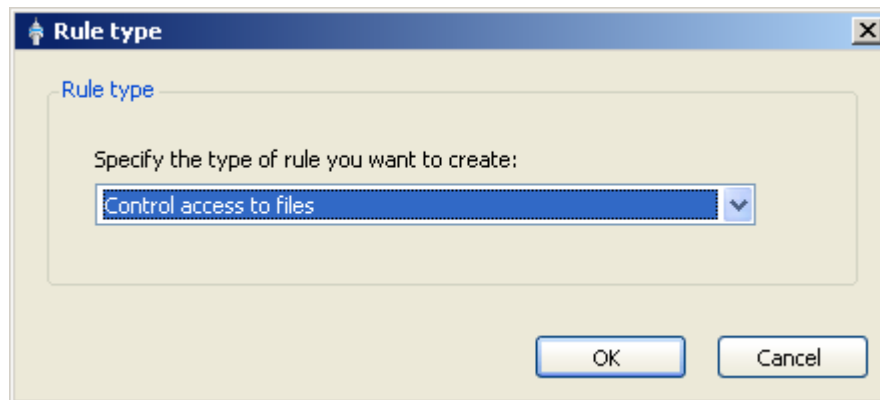
Enter the name of the container and a description (optional).



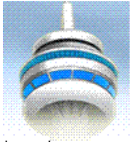
Once the container is created, you have to create a rule which will allow you to configure the applications to be blocked. To do so, click **New rule**.



Then, select the type of rule to be created. In this case, control access to files.



The aim of this rule is to prevent the P2P applications in the list from running when they are launched by other applications (Windows Explorer, etc.). To do so, once you have selected a description of the rule, configure the action to take if the rule is met. In this case, select **Deny**.



Create new control access to files rule

Rule description: P2P: Deny Run

Severity level: Nil

Rule description

Take the following action:

Deny

when the following applications:

...

in the security context of the following user profiles:

*

...

are trying to carry out one of the following operations:

Run Create Load Inject code
 Read Modify Finish

on the following files:

...

Create an entry in the report whenever a rule is met.

OK Cancel

Selection of applications

Selected applications

Enter the values directly in the list or use the selection buttons.

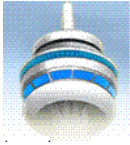
*

Find files... Add group... Manage groups...

NOTE: The wildcards *, ? and & can be used in the list.

OK Cancel

Select the operation of the P2P application that must be denied, in this case, **Run**.



Create new control access to files rule

Rule description: P2P: Deny Run

Severity level: Nil

Rule description

Take the following action:

Deny

when the following applications:

*

in the security context of the following user profiles:

*

are trying to carry out one of the following operations:

Run Create Load Inject code
 Read Modify Finish

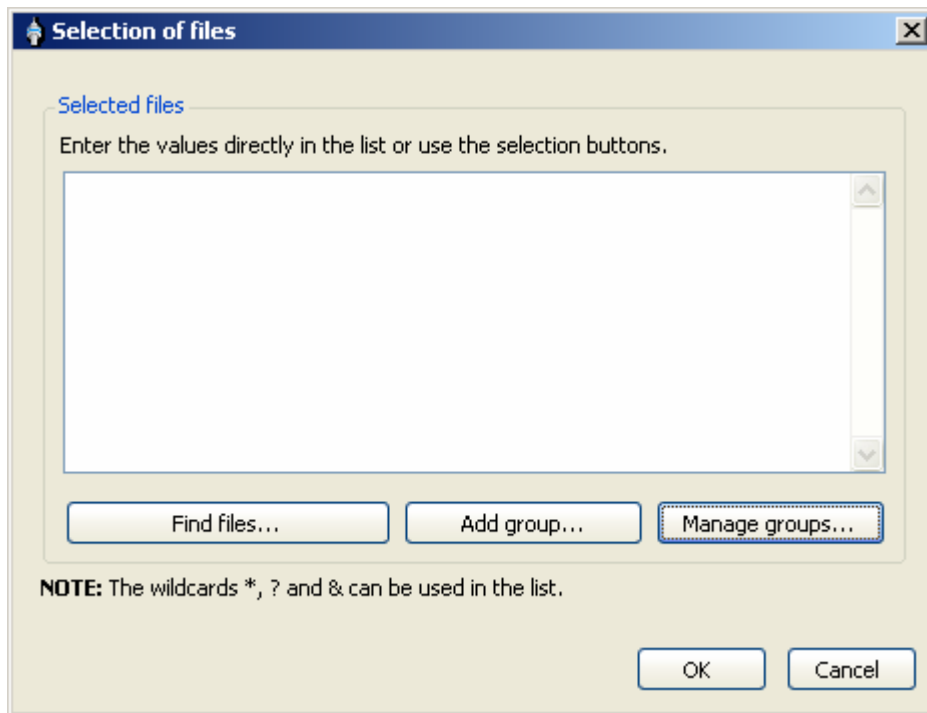
on the following files:

...

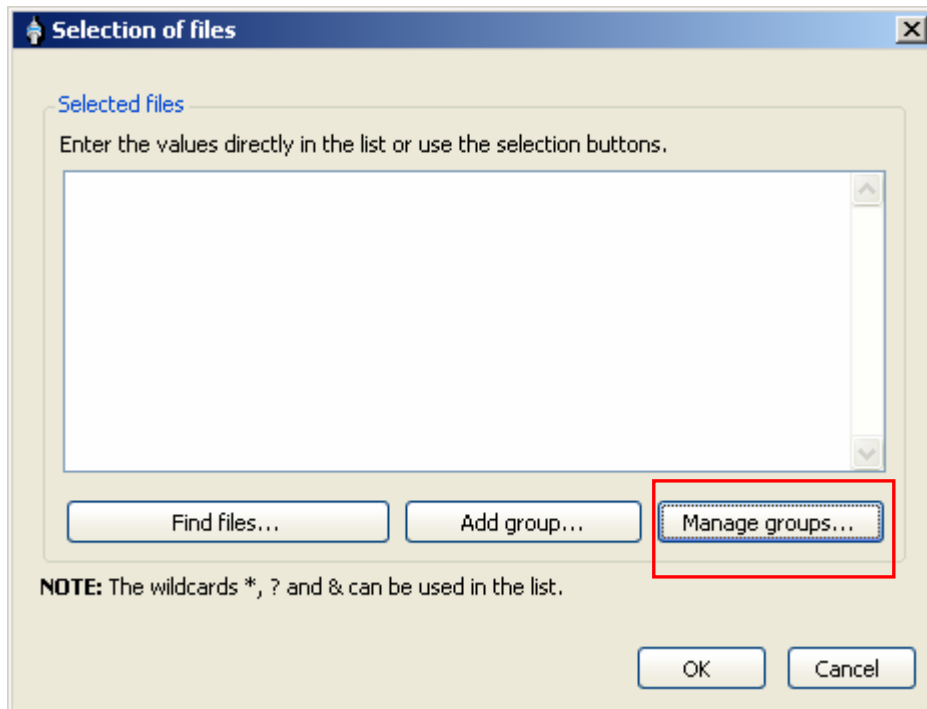
Create an entry in the report whenever a rule is met.

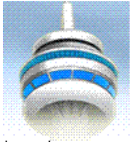
OK Cancel

Finally, configure the list of applications you want to prevent from running. To do so, click “...” to access the file selection window.

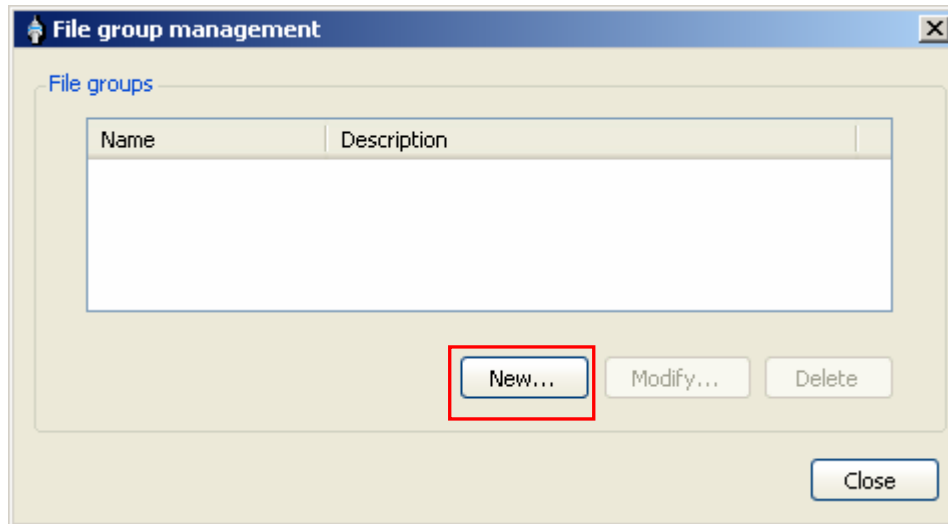


The list of applications to be denied can be entered directly in the top part of the window. However, you are recommended to create a new group which can be reused when defining this type of rule. To do so, click **Manage groups...**

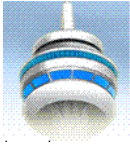




The groups of available files will be displayed. Since there are none in this example, click **New...** to create one.



Enter the group name, a description and the files included in the group.



New file group

Name: P2P Applications

Description: List of P2P Applications

Files included in the group

Enter the values directly in the list.

- emule.exe
- utorrent.exe
- azureus.exe
- pando.exe

Find files...

Files excluded from the group

Enter the values directly in the list.

Find files...

NOTE: The wildcards *, ? and & can be used in the lists.

Help OK Cancel

Click **OK** to finish creating the file group and return to the **File group management** screen.

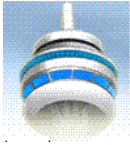
File group management

File groups

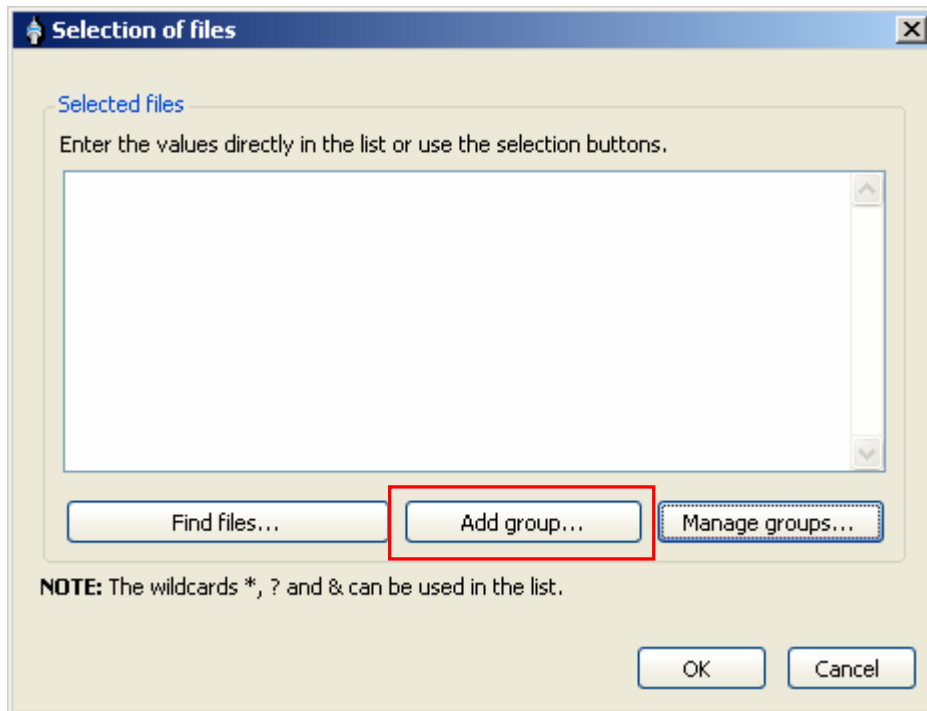
Name	Description
P2P Applications	List of P2P Applications

New... Modify... Delete

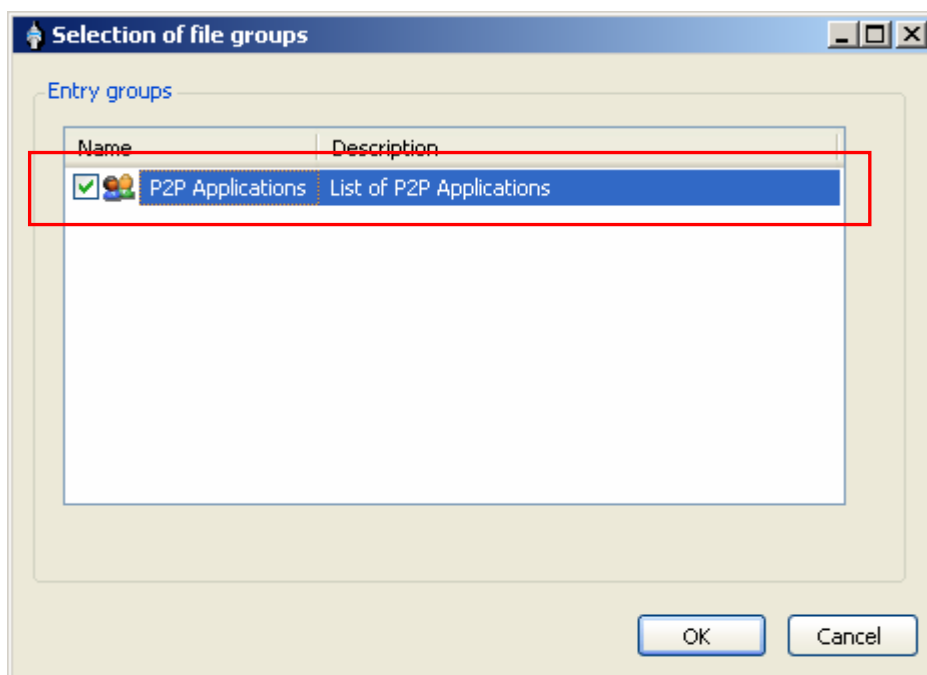
Close

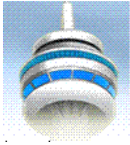


Since no more groups will be created, click **Close**. In the next screen, click **Add group...**

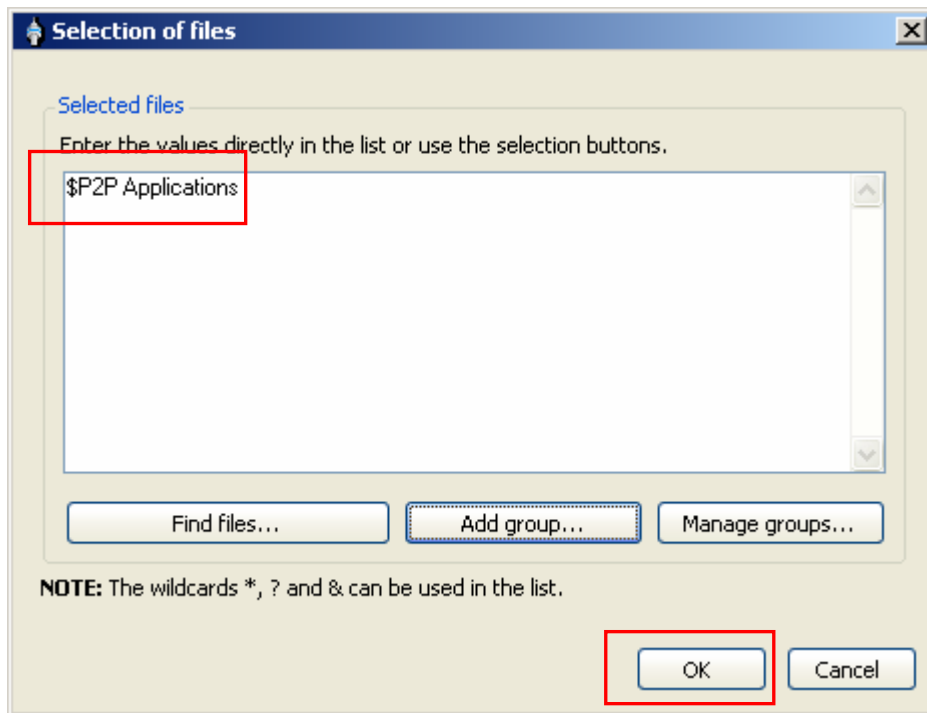


To select the group created, select the checkbox and click **OK**.

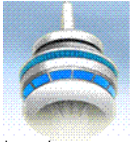




Go to the **Selection of files** window (this window allows you to create new file groups).



Click **OK** to assign a group of applications to the rule. This is the last step for configuring the rule:

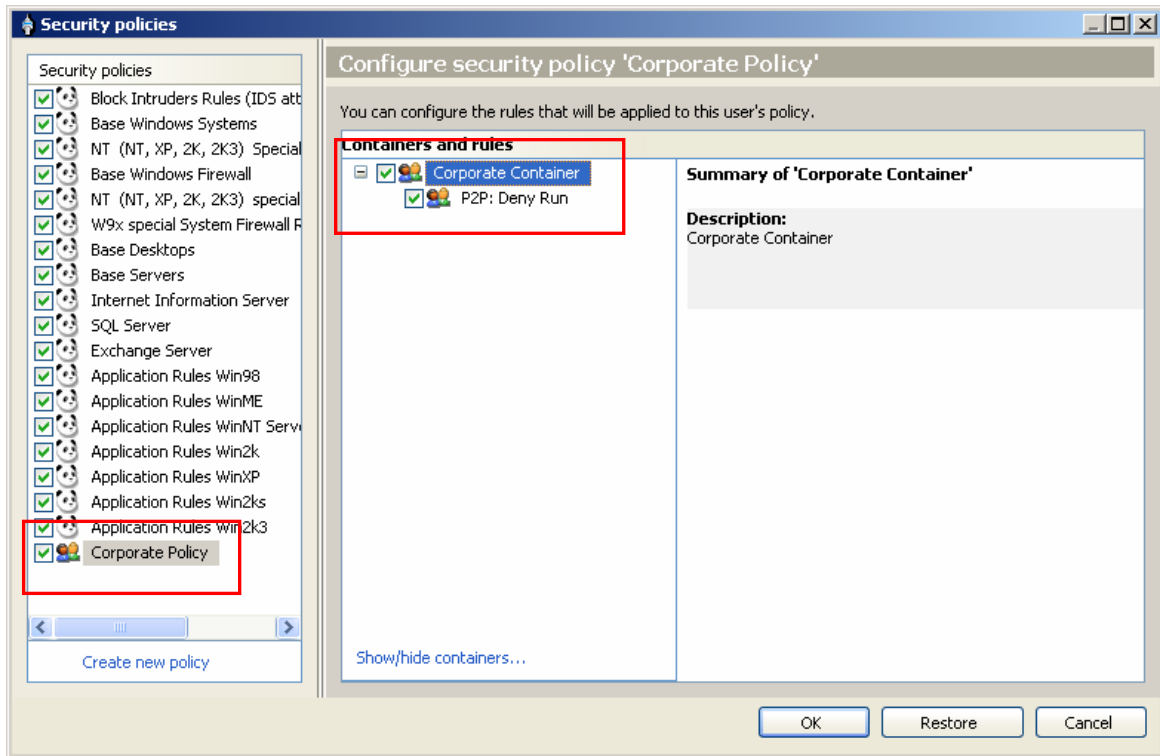
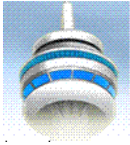


The screenshot shows a dialog box titled "Create new control access to files rule". It contains the following fields and options:

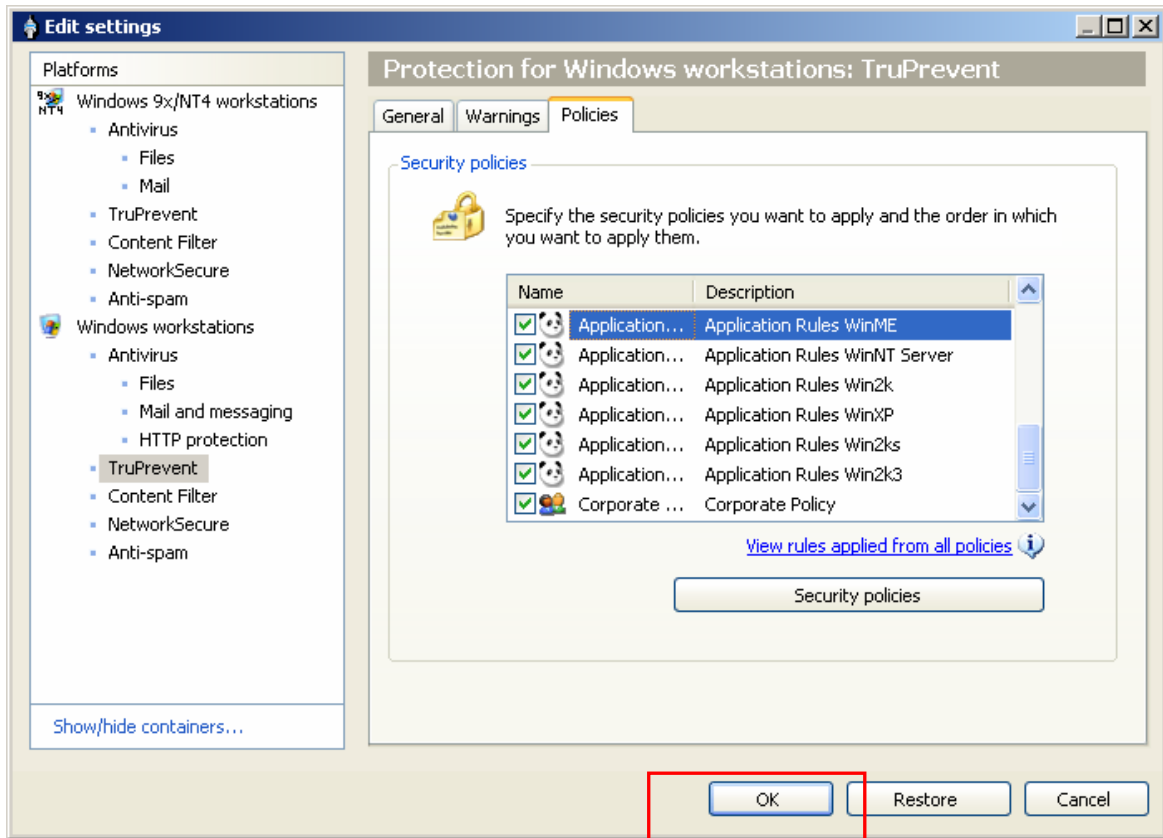
- Rule description:** P2P: Deny Run
- Severity level:** Nil
- Rule description:** (Section header)
- Take the following action:** Deny
- when the following applications:** *
- in the security context of the following user profiles:** *
- are trying to carry out one of the following operations:**
 - Run
 - Create
 - Load
 - Inject code
 - Read
 - Modify
 - Finish
- on the following files:** "\$P2P Applications"
- Create an entry in the report whenever a rule is met.

Buttons: OK, Cancel

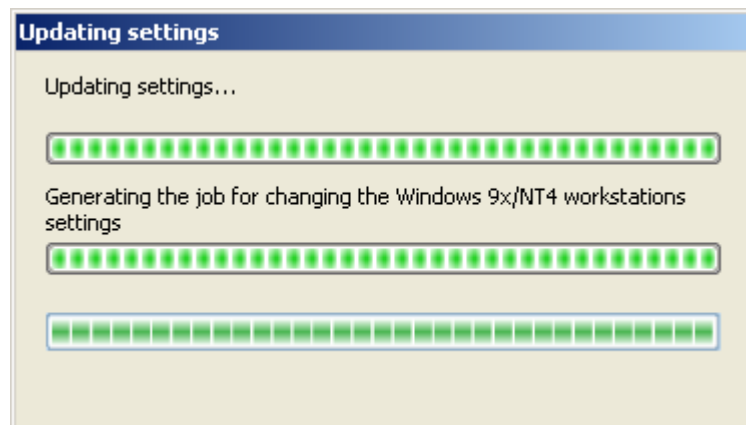
Click **OK** to finish creating the rule. Make sure the policy, the container and the rule are enabled (the checkboxes are selected) and click **OK**.



Click **OK** to finish the configuration.

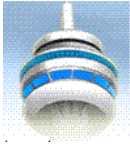


The settings update progress will be displayed in the next window.



Once the settings have been modified, they will be applied to the group of computers selected. You can check whether the rule is correctly applied by launching some of the denied applications on computers to which the policy has been applied.

When trying to run a denied application, the following local warning will be displayed, informing that the application has been blocked.



05/13/2008, 16:33



Suspicious operation blocked!

Panda Security for Desktops has detected an action that could compromise the security of your PC and has blocked it.

Program:

C:\WINDOWS\EXPLORER.EXE

Action:

Access to the file: C:\PROGRAM FILES\EMULE\EMULE.EXE

If this situation is a problem for you, consult your network administrator.

 I want to...

 Close

Panda Security for Desktops

05/13/2008, 16:56



Suspicious operation blocked!

Panda Security for Desktops has detected an action that could compromise the security of your PC and has blocked it.

Program:

C:\WINDOWS\EXPLORER.EXE

Action:

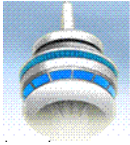
Access to the file: C:\PROGRAM FILES\UTORRENT\UTORRENT.EXE

If this situation is a problem for you, consult your network administrator.

 I want to...

 Close

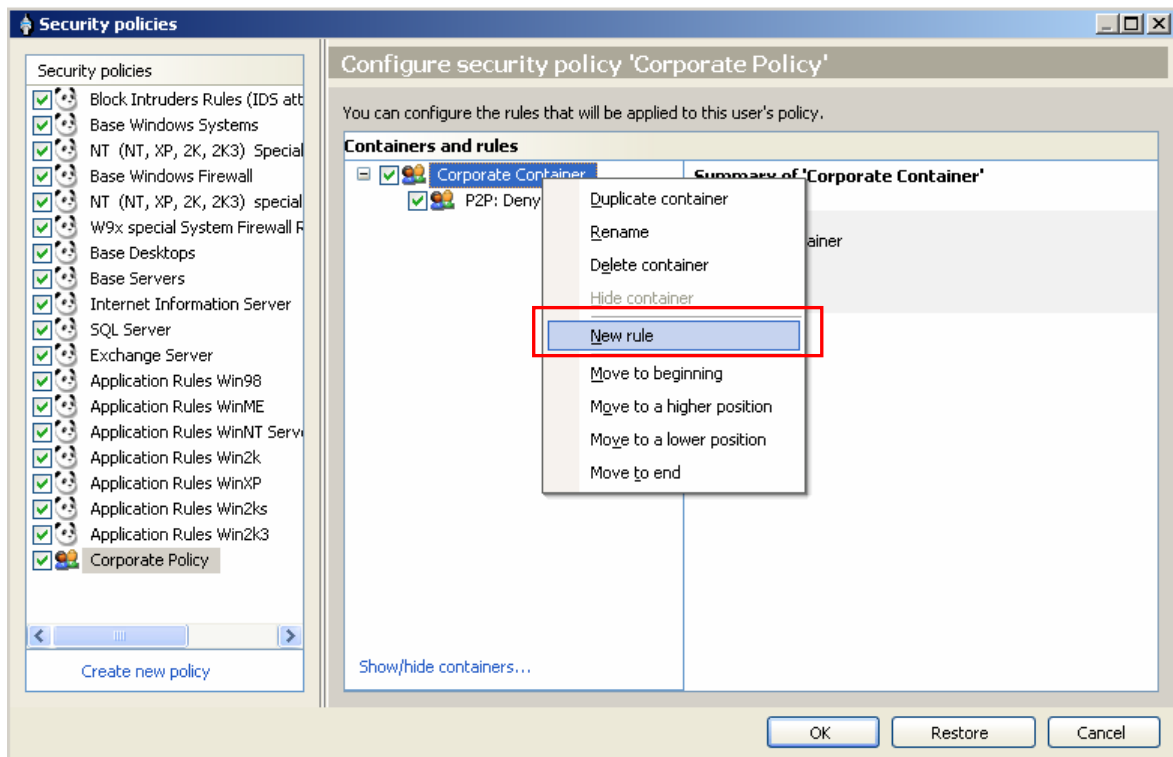
Panda Security for Desktops



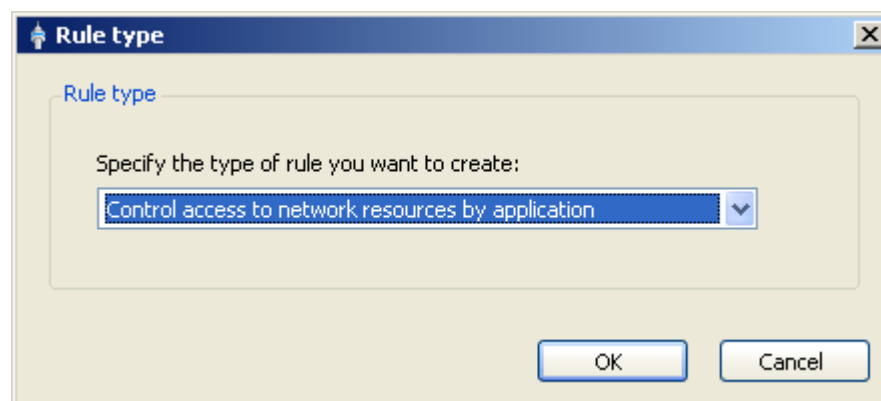
2. Deny P2P application communications

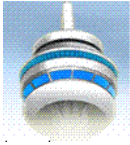
This rule allows administrators to define a list of applications that will be denied communication on computers in which the configuration has been applied.

To do so, click **New rule**.



Then select the type of rule to be created. In this case, Control access to network resources by application.





The aim of this rule is to deny the communications of the listed P2P applications for any protocol and in any direction. To do so, once you have selected a rule description, configure the action to take if the rule is met. In this case, select **Deny the connection**.

Create new control access to network resources by application rule

Rule description: P2P: Deny Connection

Severity level: Nil

Rule description

Take the following action:

Include the application in the group

Include the application in the group

Allow the connection

Deny the connection

try to establish a connection with the following characteristics:

Protocol: TCP

Communication direction: Inbound

Source port: *

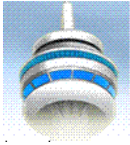
Target port: *

Source address: *

Target address: *

OK Cancel

Configure the list of applications you want to deny communications to. To do so, click “...” and go to the **Selection of applications** window.



Create new control access to network resources by application rule

Rule description: P2P: Deny Connection

Severity level: Nil

Rule description

Take the following action:
Deny the connection

when the following applications:

...

try to establish a connection with the following characteristics:

Protocol: TCP

Communication direction: Inbound

Source port: * ...

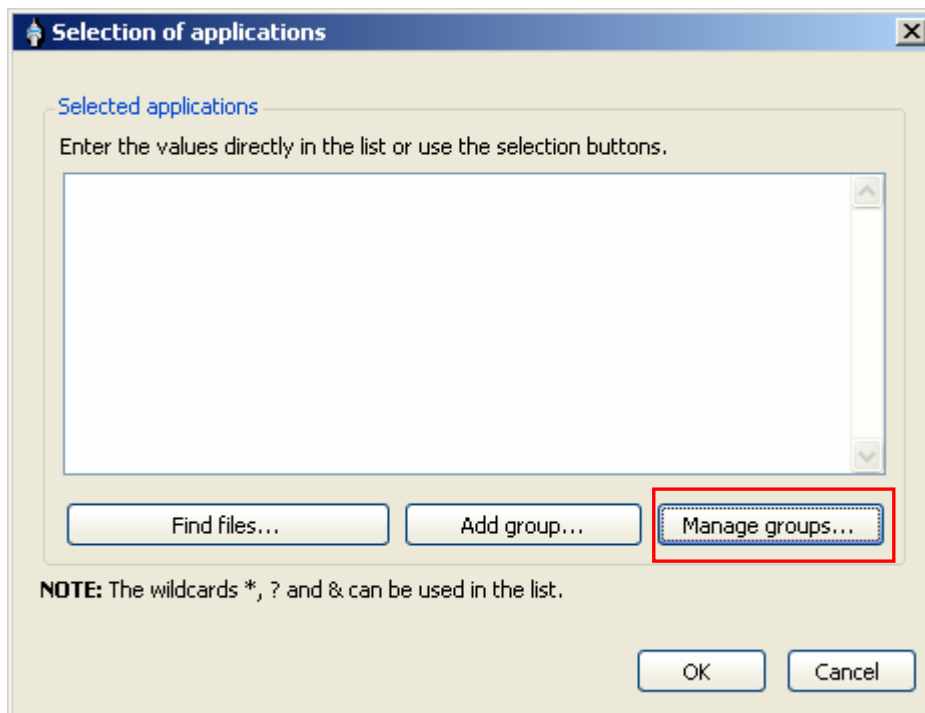
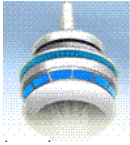
Target port: * ...

Source address: * ...

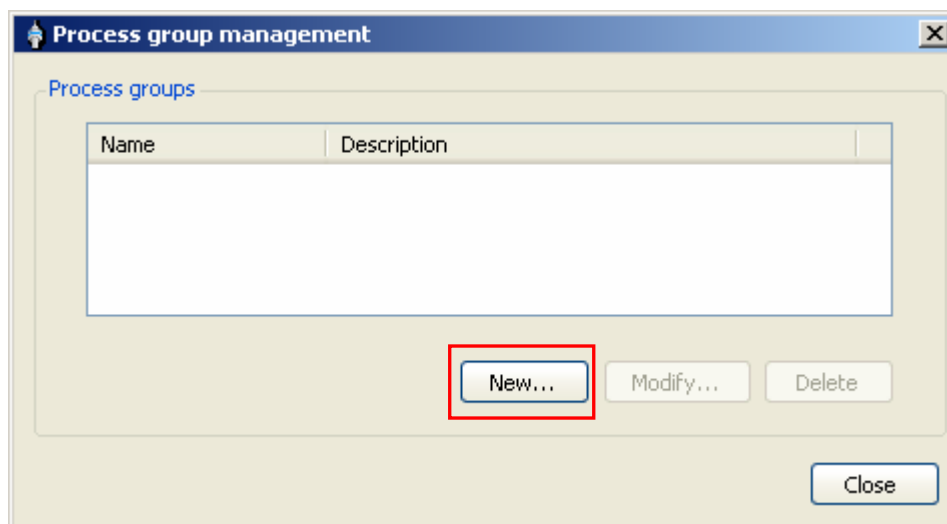
Target address: * ...

OK Cancel

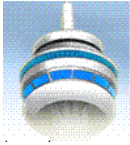
The list of applications can be entered directly in the top part of the window. However, you are recommended to create a new group, which can be reused when defining this type of rule. To do so, click **Manage groups...**



The groups of available processes will be displayed. Since there are none in this example, click **New...** to create one.



Enter the group name, a description and a list of executable files to be included in the group.



Modify process group

Name: P2P

Description: List of P2P Applications

Only include the specified processes

Include the specified processes and their subprocesses

Only include the subprocesses of the specified processes

Processes included in the group

Enter the values directly in the list.

emule.exe
utorrent.exe
azureus.exe
pando.exe

Find files...

Processes excluded from the group

Enter the values directly in the list.

Find files...

NOTE: The wildcards *, ? and & can be used in the lists.

Help OK Cancel

Click **OK** to finish creating the process group and return to the **Process group management** screen.

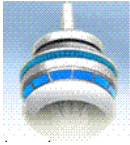
Process group management

Process groups

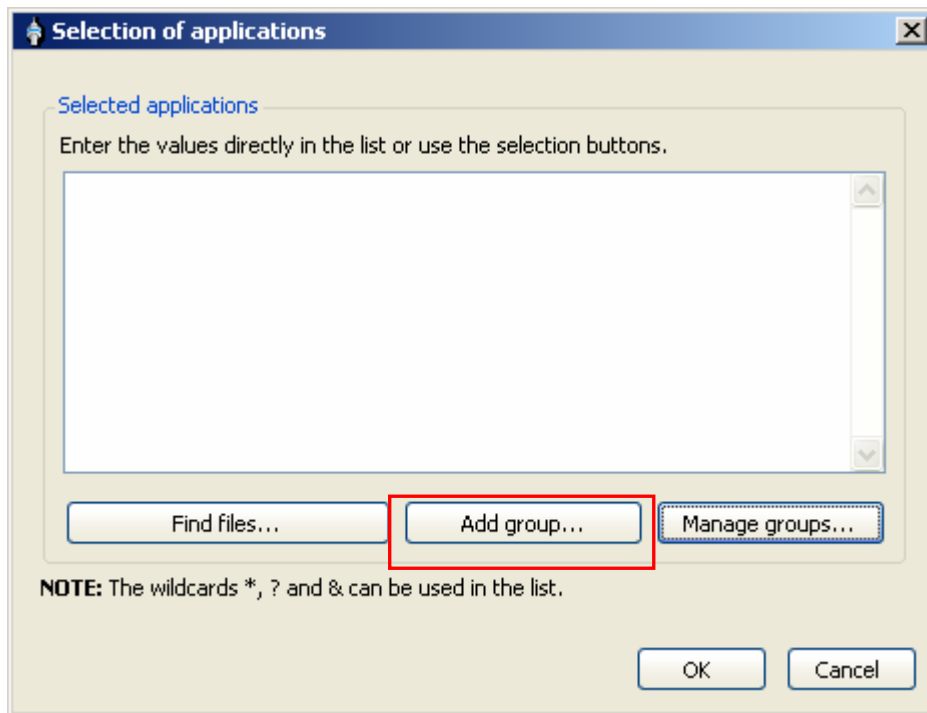
Name	Description
P2P	List of P2P Applications

New... Modify... Delete

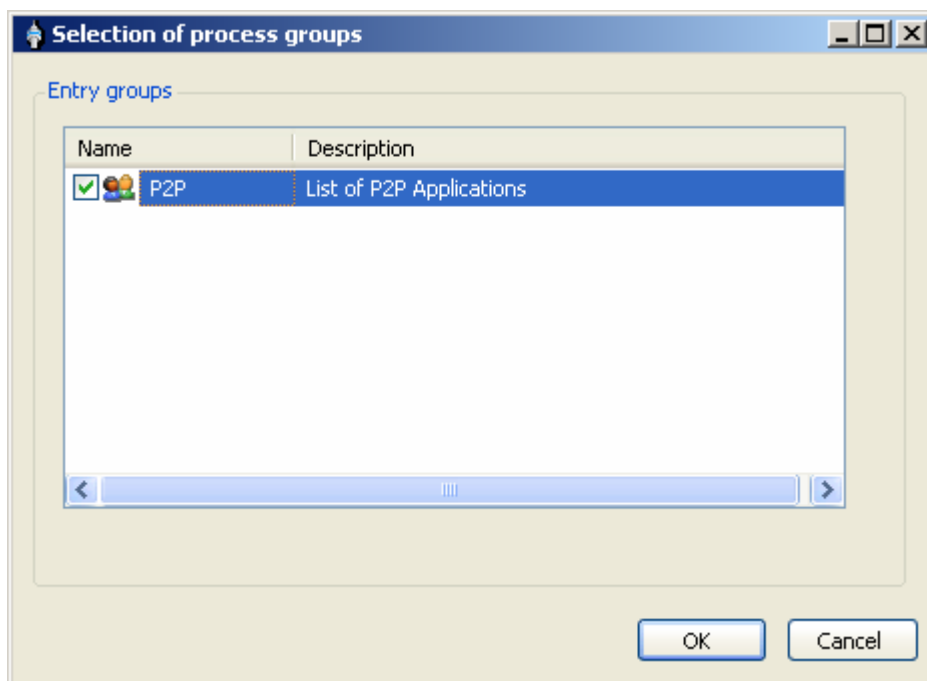
Close

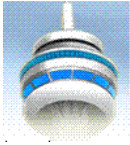


Since no more groups need to be created, click **Close**. In the next screen, click **Add group...**

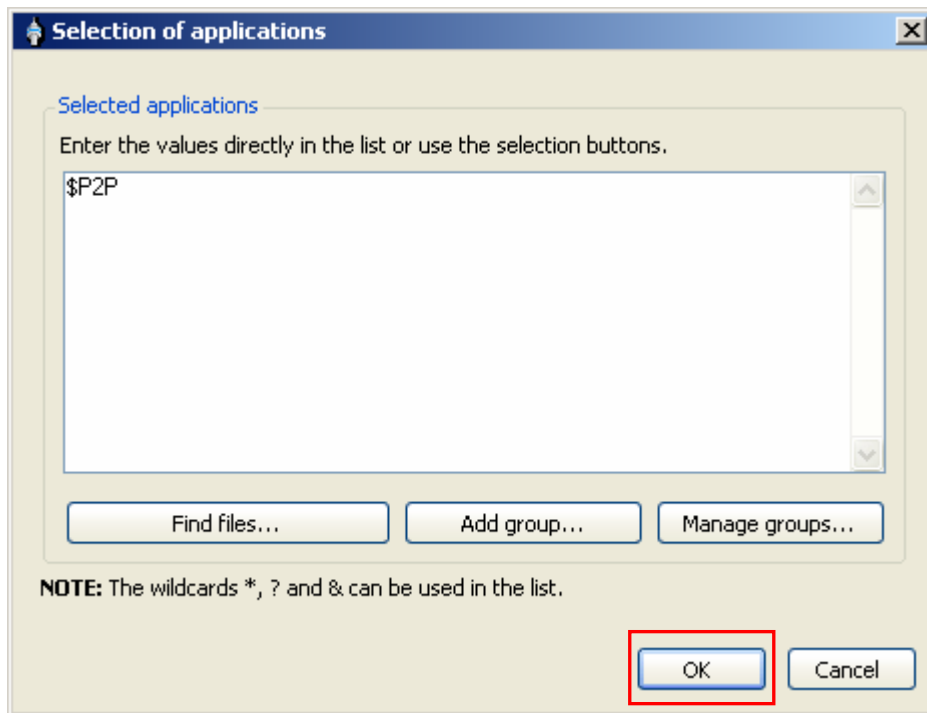


To select the group created, select the checkbox and click **OK**.

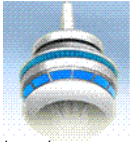




Go to the **Selection of applications** window which allows you to create new application groups.



Click **OK** to assign a group of applications to the rule.



Create new control access to network resources by application rule

Rule description: P2P: Deny Connection

Severity level: Nil

Rule description

Take the following action:

Deny the connection

when the following applications:

\$P2P

try to establish a connection with the following characteristics:

Protocol: TCP and UDP

Communication direction: Inbound

Source port: *

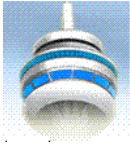
Target port: *

Source address: *

Target address: *

OK Cancel

Finally, select the protocols, communication direction, ports and addresses you want deny in these applications. In this case, TCP and UDP protocols for inbound and outbound connections to any port and direction.



Create new control access to network resources by application rule

Rule description: P2P: Deny Connection

Severity level: Nil

Rule description

Take the following action:

Deny the connection

when the following applications:

\$P2P

try to establish a connection with the following characteristics:

Protocol: TCP and UDP

Communication direction: Inbound and outbound

Source port: *

Target port: *

Source address: *

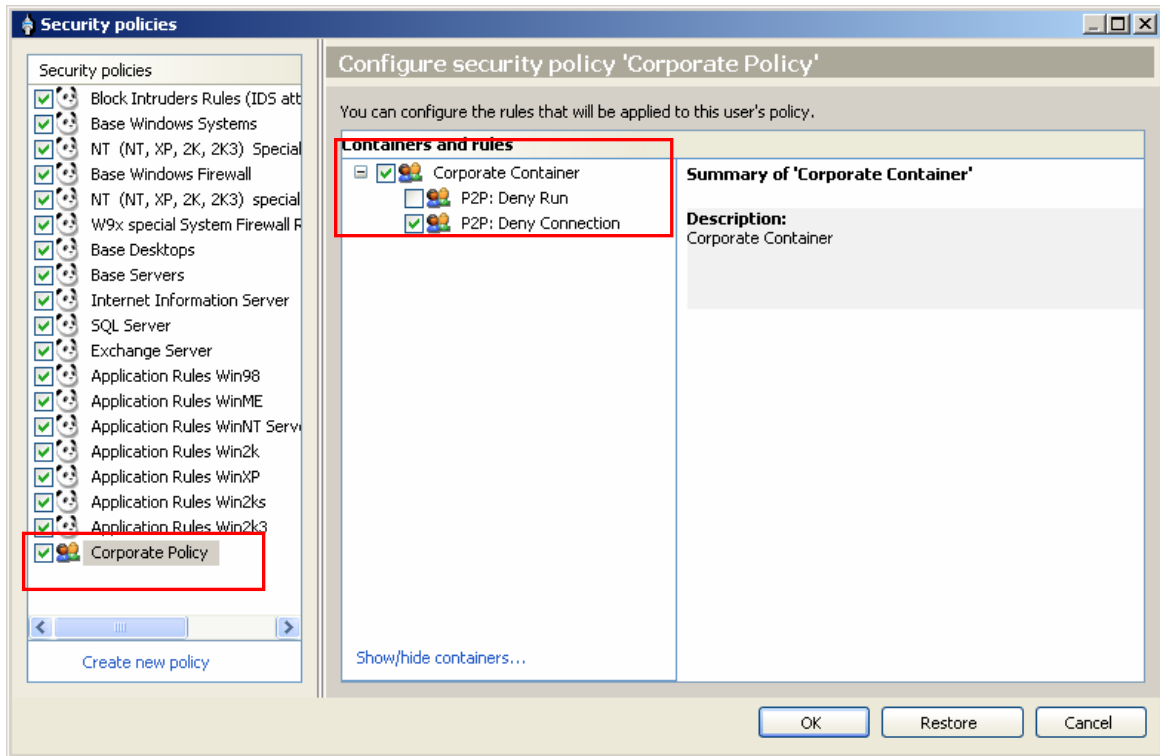
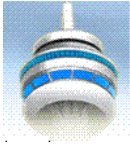
Target address: *

OK Cancel

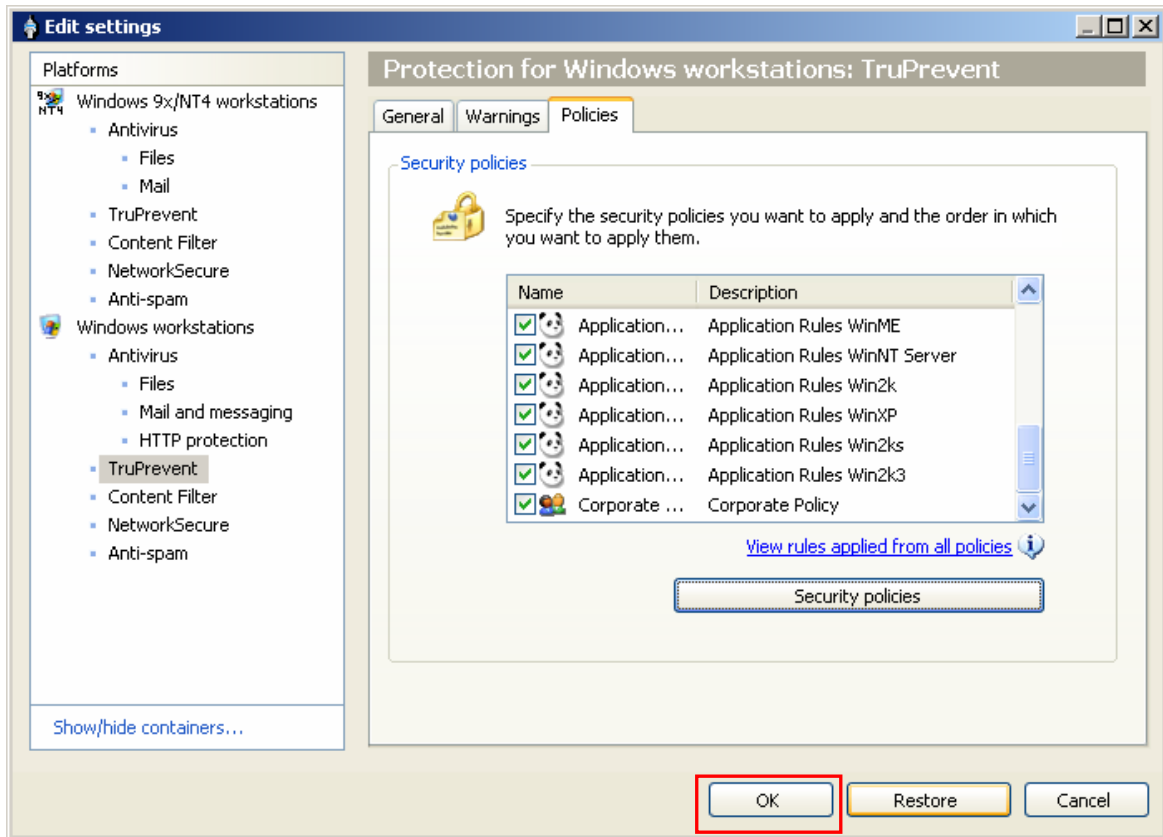
Click **OK** to end the creation of the rule.

Make sure the policy, the container and the rule are enabled (the checkboxes are selected) and click **OK**.

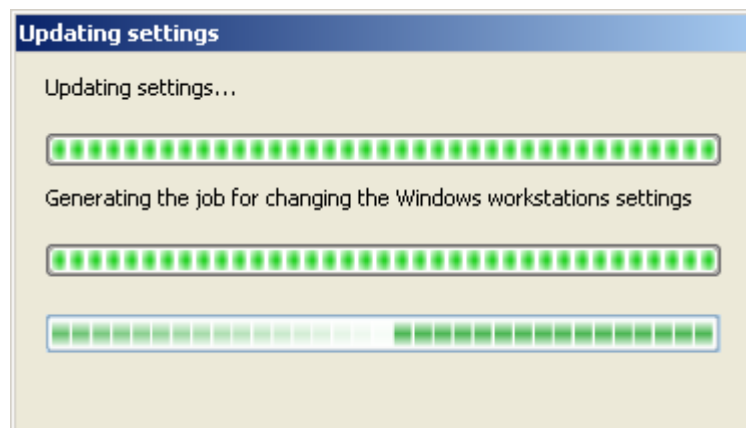
In the example, the rule created in the previous point is disabled since it would not allow the applications to run.



Click **OK** to finish the configuration.



The settings update progress will be displayed in the next window.



Once the settings have been modified, they will be applied to the selected group of computers. You can check whether the rule is correctly applied by launching some of the denied applications on computers to which the policy has been applied.

The application will run, but all its communications will be denied.



eMule v0.49a

Connect Kad Servers Transfers Search Shared Files Messages IRC Statistics Options Tools Help

Server Name	IP	Description	Ping	Users	Max ...	Files	Prefer...
!! Saugstube !!	193.138.221.214 : 4242	www.usenet.1a.to					Normal
# eMule Serverlist Nr...	193.138.221.210 : 4242	www.serverlist.to					Normal
...: France Mule #1 :...	193.42.213.30 : 9510	France eDonkey/EMule/Sh...					Normal
BooTVirus	213.219.239.192 : 4661	Super fast Cart-Blansh se...					Normal
ed2kpower	207.171.62.208 : 4661	Free of Freedom					Normal
eDonkeyServer No1	77.247.178.244 : 4242	www.eDonkey.to					Normal
eDonkeyServer No2	77.247.178.245 : 4242	www.eDonkey.to					Normal
Global Server 1	222.77.179.242 : 4500	www.StormSex.net Dual ...					Normal
Global Server 2	222.77.179.246 : 4500	www.StormSex.net Dual ...					Normal
Global Server 3	218.83.155.86 : 4500	www.StormSex.net Dual ...					Normal
Global Server 4	61.129.115.51 : 4500	www.StormSex.net Dual ...					Normal
PEERATES.NET	88.191.81.111 : 1111	http://edk.peerates.net					Normal
Razorback 3.0	85.17.52.92 : 5000	www.razorback3.com - w...					Normal
Razorback 3.1	193.138.205.25 : 5000	www.razorback3.com - w...					Normal
Razorback 3.2	85.17.52.124 : 5000	www.razorback3.com - w...					Normal
Razorback 3.3	92.48.193.14 : 5000	www.razorback3.com - w...					Normal
Sharing Kingdom 1	61.129.45.177 : 4500	www.StormSex.net Dual ...					Normal

Connect

New Server
IP or Address Port
Name
Add to list

Update server.met from URL
Update

My Info
eD2K Network Status: Disconnected
Kad Network Status: Disconnected
Web Interface Status: Disabled

Reset

Server Info Log

```
13/05/2008 18:00:49: Found U known shared files
13/05/2008 18:00:49: Credit file loaded, 0 clients are known
13/05/2008 18:00:51: 21 servers in server.met found
13/05/2008 18:00:52: No part files found
13/05/2008 18:00:52: Fatal Error: Unable to create socket on port 24569
13/05/2008 18:00:52: eMule Version 0,49a ready
13/05/2008 18:01:46: UploadSpeedSense: Trace routing failed too many times. Disabling Upload SpeedSense
13/05/2008 18:01:47: Connecting
13/05/2008 18:01:47: Connecting to Tower II (85.128.56.84:4567)...
13/05/2008 18:01:48: Connecting to Razorback 3.1 (193.138.205.25:5000)...
13/05/2008 18:02:08: Tower II (85.128.56.84:4567) appears to be dead.
13/05/2008 18:02:08: Connecting to Sharing Kingdom 1 (61.129.45.177:4500)...
13/05/2008 18:02:09: Razorback 3.1 (193.138.205.25:5000) appears to be dead.
13/05/2008 18:02:09: Connecting to # eMule Serverlist Nr.2 # (193.138.221.210:4242)...
13/05/2008 18:02:30: Fatal Error while trying to connect. Internet connection might be down
13/05/2008 18:02:30: Automatic connection to server will retry in 30 seconds
```

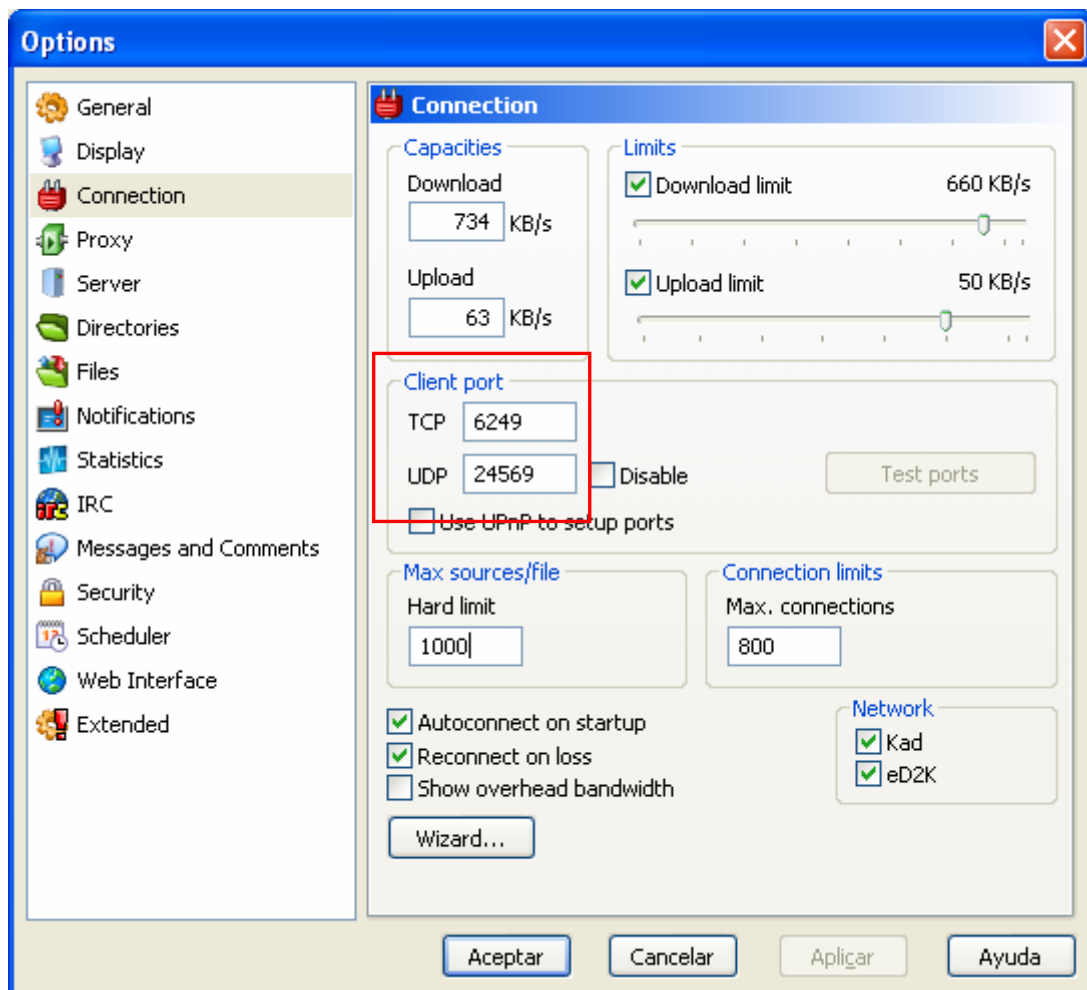
Fatal Error while trying to connect. Internet connection might be down
Users:0(0)|Files:0(0) Up: 0.0 | Down: 0.0 eD2K:Not Connected|Kad:Not Connected 65535.0 | 0ms



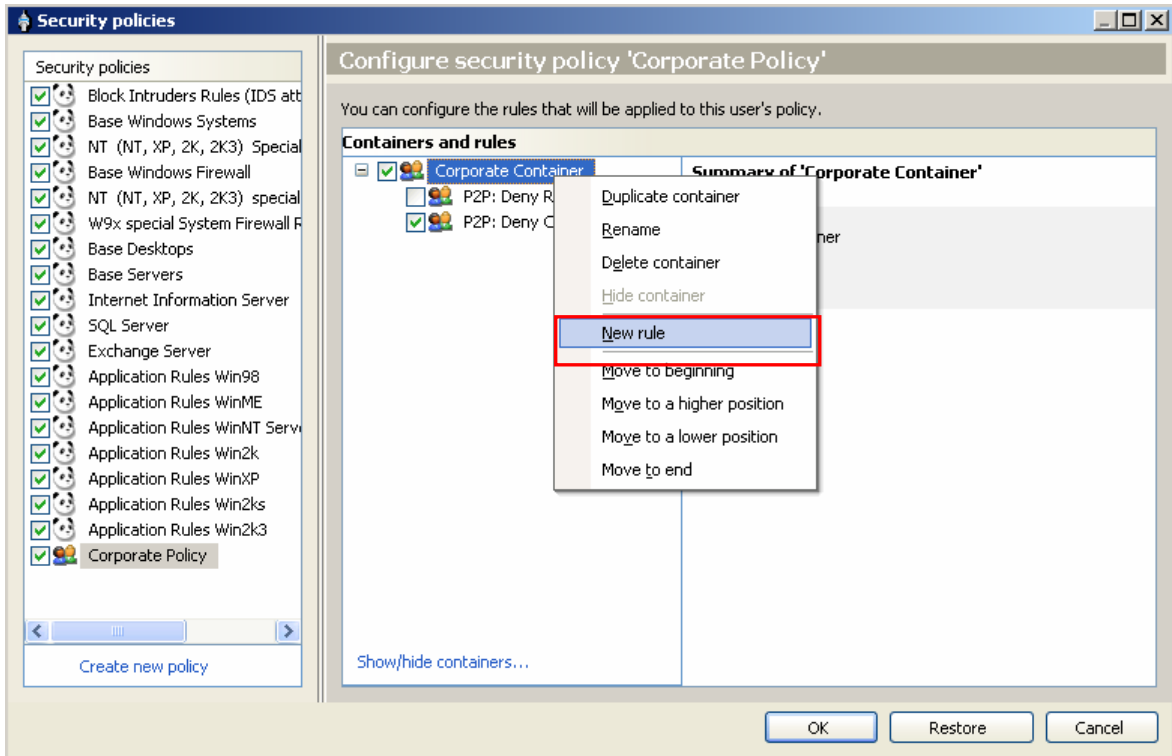
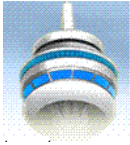
3. System rules

These types of rules allow administrators to deny communications to a set of ports, commonly used by P2P applications to establish communications. Since system rules affect all applications that use these ports, make sure the ports are not used by other corporate applications.

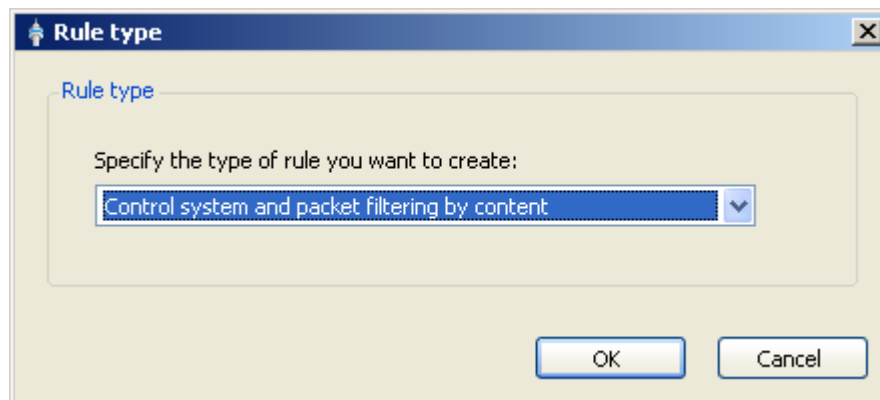
To define the rule, you need to know the ports used by P2P applications.



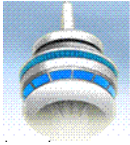
In the example, a rule is created to deny inbound connection through ports 6249 TCP and 24569 UDP. To do so, click **New rule**.



Then, select the type of rule to be created. In this case, Control system and packet filtering by content.



Enter the rule description and configure the **Deny** action for the TCP protocol in inbound connection to port 6249.



Create new control system and packet filtering by content rule

Rule description: P2P: System Rule eMule TCP|

Severity level: Nil

Rule description

Take the following action:

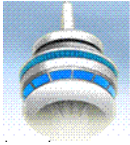
Deny

Whenever a package is detected that matches the following description:

Protocol:	TCP	...
Communication direction:	Inbound	...
Local port:	6249	...
Remote port:	*	...
Remote address:	*	...
Local address:	*	...

OK Cancel

Another rule must be created to deny UDP protocol in inbound connections to port 24569.



Modify Control system and packet filtering by content rule

Rule description: P2P: System Rule eMule UDP

Severity level: Nil

Rule description

Take the following action:

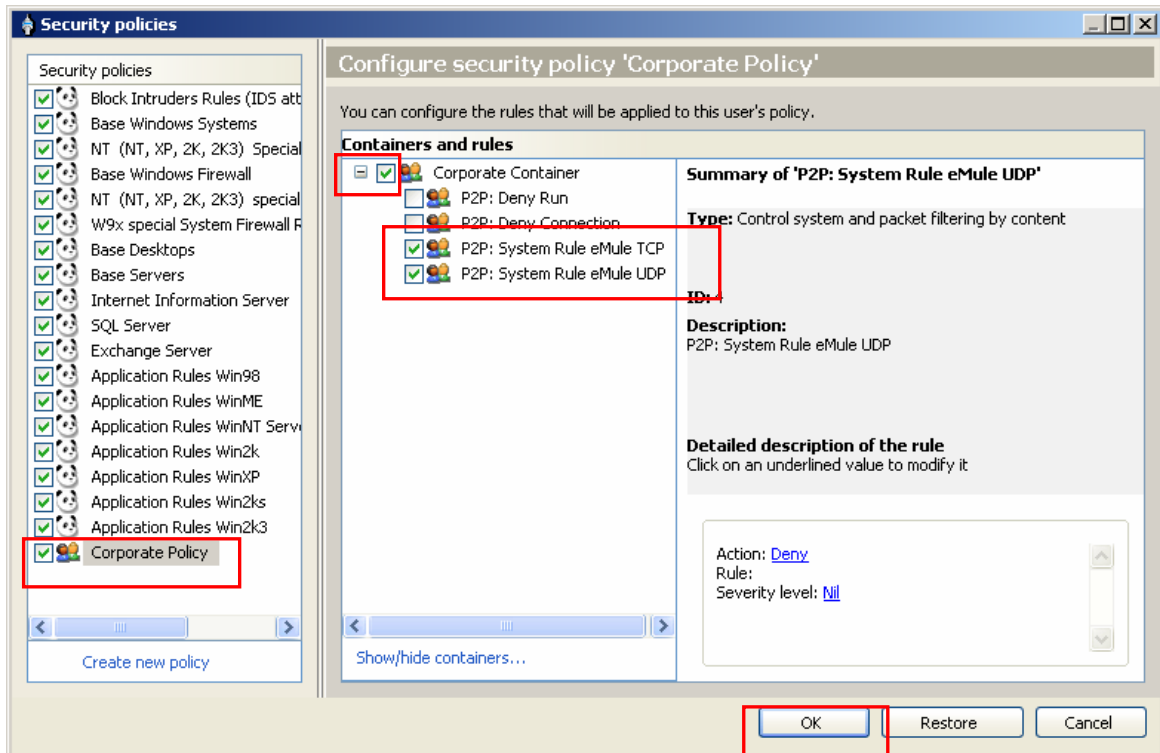
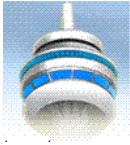
Deny

Whenever a package is detected that matches the following description:

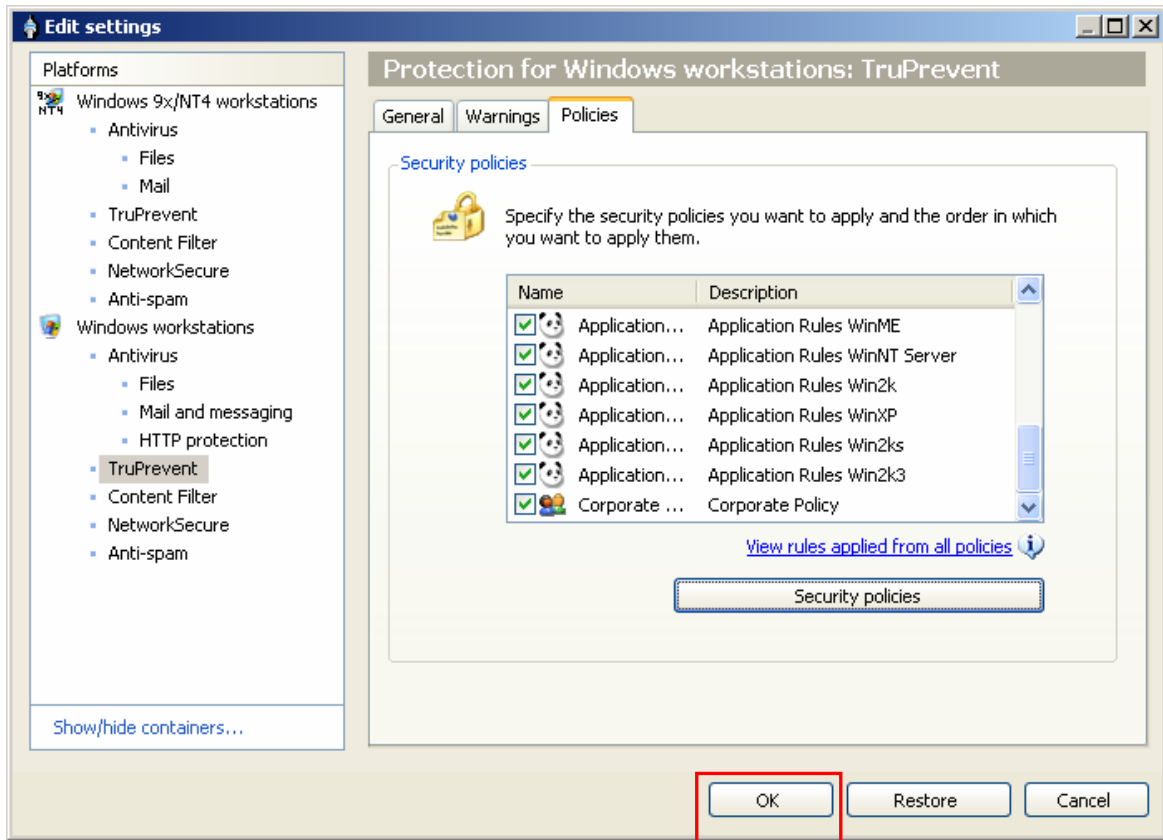
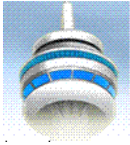
Protocol:	UDP	...
Communication direction:	Inbound	...
Local port:	24569	...
Remote port:	*	...
Remote address:	*	...
Local address:	*	...

OK Cancel

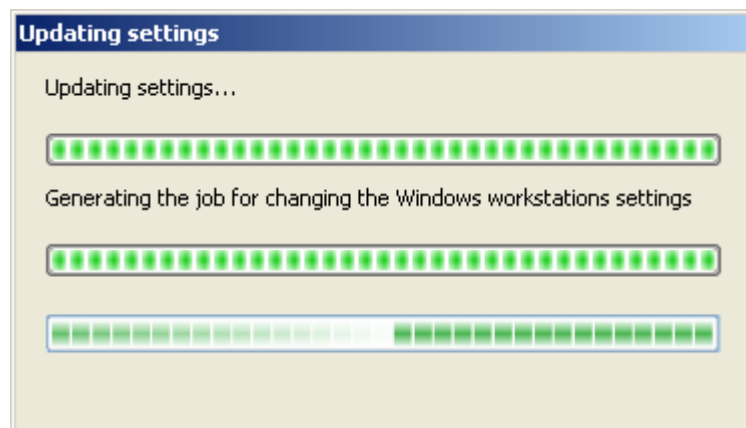
Click **OK** to end the creation of the rule. Make sure the policy, the container and the rule are enabled (the checkboxes are selected) and click **OK**. In this case, the rules created in previous points are disabled.



Click **OK** to finish the configuration.

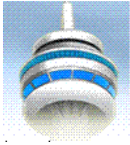


The settings update progress will be displayed in the next window.



Once the settings have been modified, they will be applied to the selected group of computers. You can check whether the rule is correctly applied by launching some of the applications that use the denied communication ports on some of the computers to which the policy has been applied.

The application will run, but all its communications will be denied.



The screenshot shows the eMule v0.49a application window. At the top, there is a menu bar with icons for Cancel, Kad, Servers, Transfers, Search, Shared Files, Messages, IRC, Statistics, and Options. Below the menu bar is a 'Servers (21)' list with columns for Server Name, IP, and Description. The list includes servers like '!! Saugstube !!', '# eMule Serverlist Nr...', and 'France eDonkey/EMule/Sh...'. To the right of the list is a 'New Server' dialog box with fields for IP or Address, Port (set to 4661), and Name, along with 'Add to list' and 'Update' buttons. Below the server list is a 'Server Info' tab and a 'Log' window showing system messages and error reports, such as 'Fatal Error: Unable to create socket on port 24569'. At the bottom of the window, there is a status bar showing 'Razorback 3.1 (193)', 'Users:0(10)|Files:0(1.1 k)', 'Up: 0.0 | Down: 0.0', and 'eD2K:Connecting|Kad:Connecting'.

Server Name	IP	Description
!! Saugstube !!	193.138.221.214 : 4242	www.usenet.1a.to
# eMule Serverlist Nr...	193.138.221.210 : 4242	www.serverlist.to
...: France Mule #1 ...	193.42.213.30 : 9510	France eDonkey/EMule/Sh...
BooTvirus	213.219.239.192 : 4661	Super Fast Cart-Blansh se...
ed2kpower	207.171.62.208 : 4661	Free of Freedom
eDonkeyServer No1	77.247.178.244 : 4242	www.eDonkey.to
eDonkeyServer No2	77.247.178.245 : 4242	www.eDonkey.to
Global Server 1	222.77.179.242 : 4500	www.StormSex.net Dual ...
Global Server 2	222.77.179.246 : 4500	www.StormSex.net Dual ...
Global Server 3	218.83.155.86 : 4500	www.StormSex.net Dual ...
Global Server 4	61.129.115.51 : 4500	www.StormSex.net Dual ...
DFPDATES.NET	88.191.81.111 : 1111	http://edk.persnet.net

Log:

```
14/05/2008 13:20:54: 21 servers in server.met round
14/05/2008 13:20:54: No part files found
14/05/2008 13:20:54: Fatal Error: Unable to create socket on port 24569
14/05/2008 13:20:54: eMule Version 0.49a ready
14/05/2008 13:20:54: Connecting
14/05/2008 13:20:54: Connecting to Razorback 3.0 (85.17.52.92:5000)...
14/05/2008 13:20:54: Connecting to Razorback 3.1 (193.138.205.25:5000)...
14/05/2008 13:21:15: Razorback 3.0 (85.17.52.92:5000) appears to be dead.
14/05/2008 13:21:15: Connecting to Tower II (85.128.56.84:4567)...
14/05/2008 13:21:15: Razorback 3.1 (193.138.205.25:5000) appears to be dead.
14/05/2008 13:21:15: Connecting to Sharing Kingdom 1 (61.129.45.177:4500)...
```