privacyware

Privatefirewall

Version 7 – User Guide

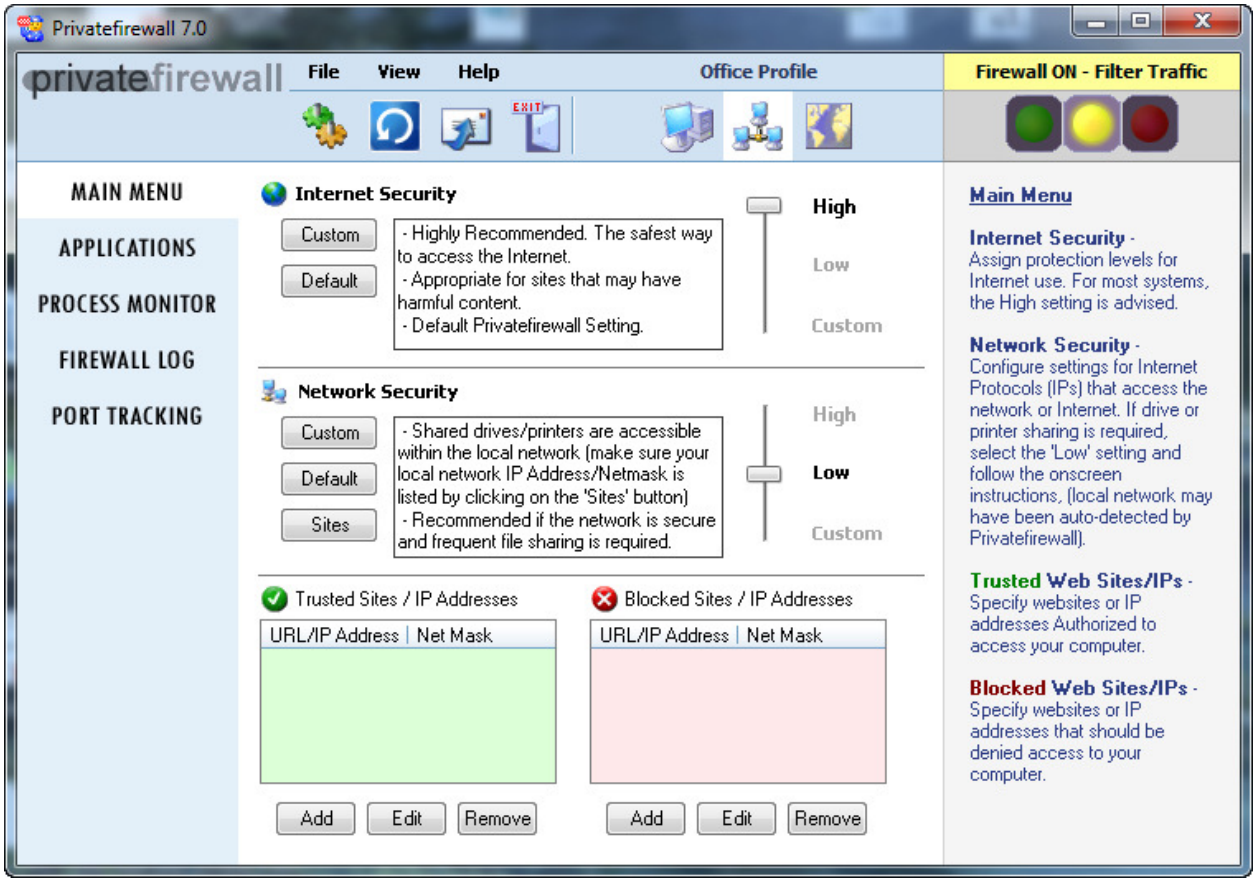
Table of Contents

Using Privatefirewall

Main Menu

(Accessed from the Windows Desktop by clicking on Start/Programs/Privatefirewall 7.0/Privatefirewall 7.0)

Main Menu controls include Internet and Network Security settings, Trusted Sites/IP Addresses and Blocked Sites/IP Addresses. In addition, three different sets of rules and settings can be maintained based on the current Firewall Profile, which can be either "Home", "Network", or "Remote". Each Profile can be viewed by selecting the appropriate Profile Icon from the top Menu Bar.



Internet Traffic (packet) Filtering

Privatefirewall monitors incoming and outgoing Internet traffic. This traffic consists of blocks of information called "packets" that can travel between any 2 computers on the Internet or local network. Packets can be allowed, filtered, or denied based on the level of filtering desired.

Allow Internet Traffic – This allows all incoming and outgoing Internet Traffic and provides the least amount of protection.

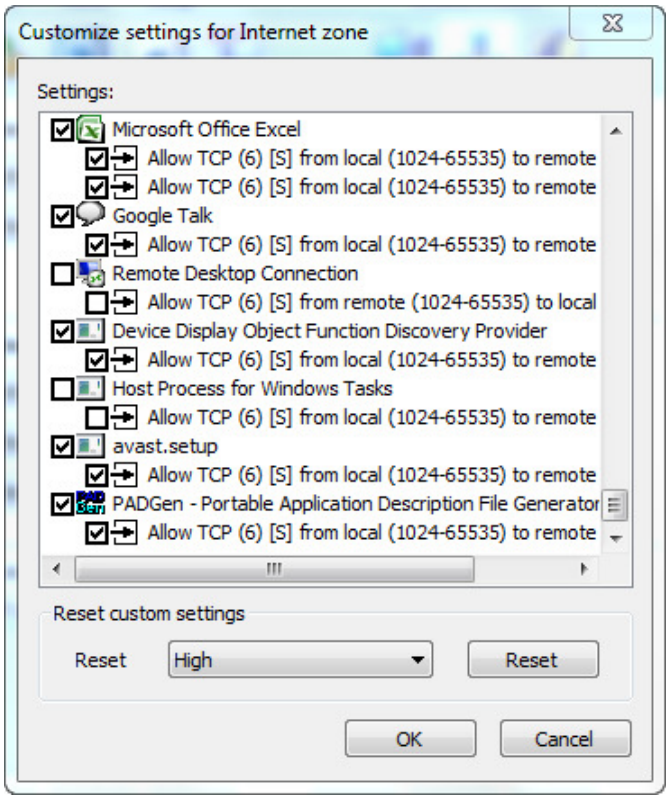
Filter Internet Traffic (RECOMMENDED) – This allows Internet access while maintaining maximum protection from incoming intrusion attempts. NOTE: All rules under Internet Security, Network Security, and Application Settings will be enforced only if this setting is selected.

Deny Internet Traffic – This blocks all incoming and outgoing Internet traffic and effectively locks down your computer. This is useful for computers with broadband connections that are left unattended.

System Security (for Internet and Internal Networks)

Internet Security **-** Various levels of protection can be specified for accessing the Internet. For most users, the 'High' setting is appropriate as it allows basic Internet access while providing the highest level of firewall protection. The 'Low' Setting is only appropriate for the most trusted environments where full system access is needed.

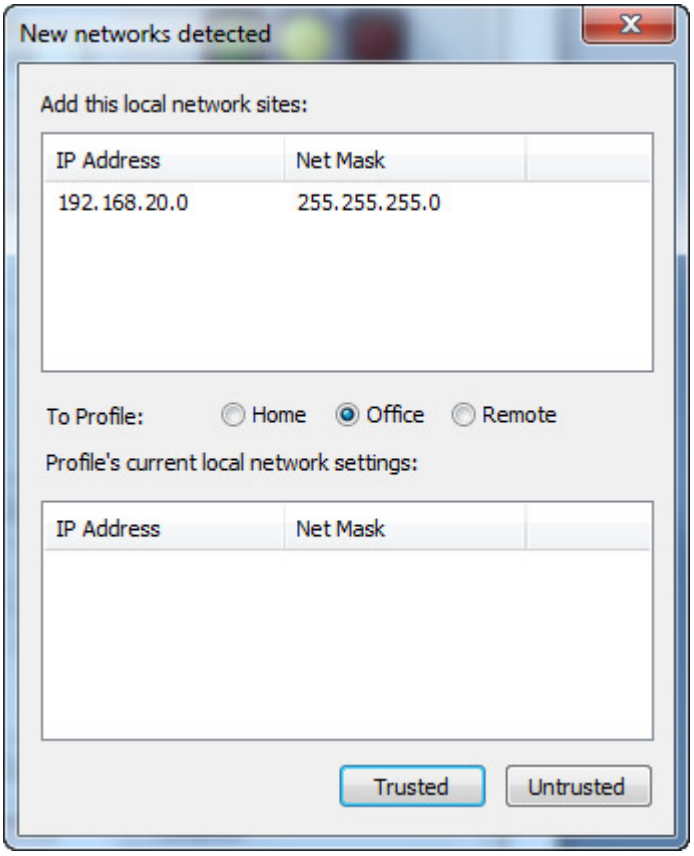
Network Security **-** Various levels of network protection can be specified. The appropriate level should be based on the type of network where the computer is located. For most users, the 'Low' level is appropriate as it allows file and printer sharing within the network. The 'High' Setting will block all shared system drives, printers, and files. This may be appropriate when using third-party or remote networks.

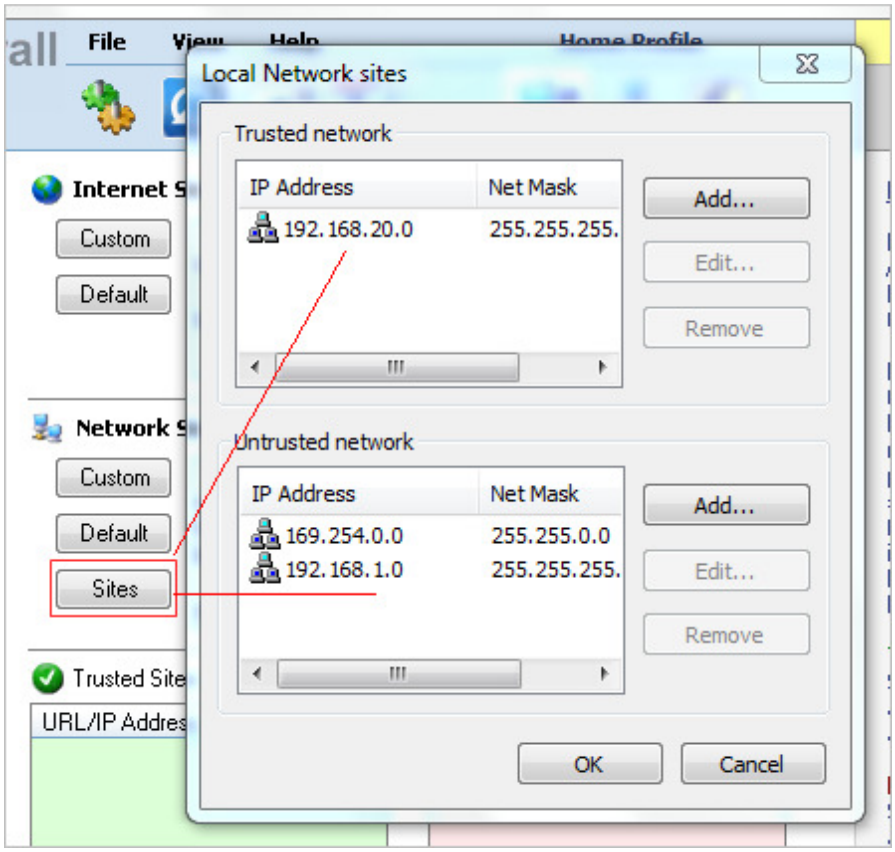


Custom Security Levels – Selecting the **Custom** button from the Internet or Network Security section displays a dialog that allows one to establish a customized set of rules for Internet security by checking/unchecking the available rules that have been configured automatically or manually by the user.

Network IP Addresses

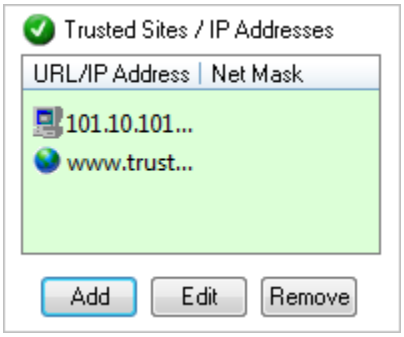
New local area networks are detected automatically. The local area network IP Address and Net Mask can be set as Trusted or Untrusted within the Home, Office, or Remote profile (see screenshot).





All trusted and untrusted network sites can be viewed at any time by selecting the **Sites** button from the Network Security section (see screenshot left).

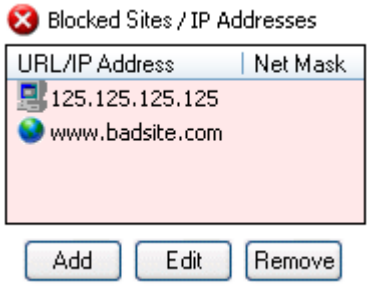
Internet Websites / IP Addresses



Any Internet website or IP Address can be allowed access to your computer. Adding a trusted site that is frequently accessed will reduce the number of pop-up alerts for that specific IP. Similarly, if 'www.trust….com' is a trusted website, the user can add this site to the Trusted Sites section. These additions will prevent any future related pop-up alerts**.**

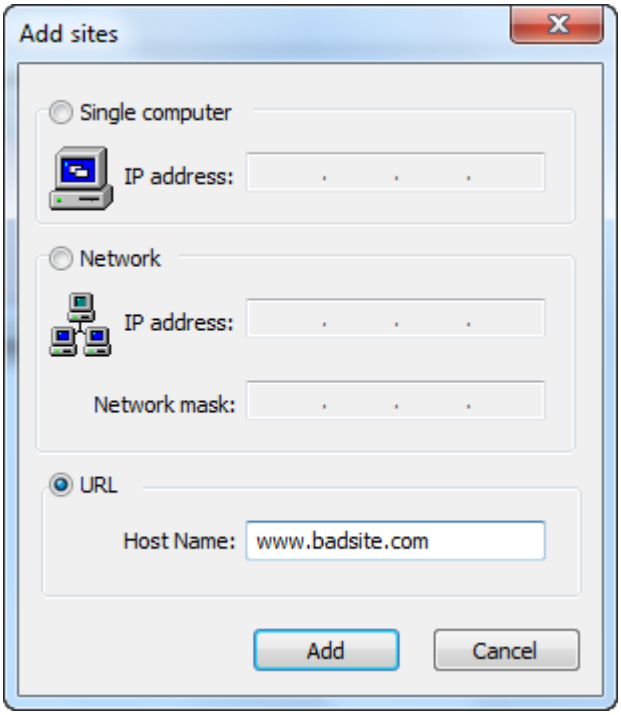
When operating Privatefirewall in Manual Control mode with the **Display Alerts for blocked incoming/ outgoing packets** option selected, whenever an unknown (or un-trusted) IP address attempts to gain access to the user's system, a pop-up alert will appear that includes the date, time, type of packet, and IP address. These pop-ups can be turned off (the information will continue to be logged/stored in the firewall log), and/or the **More Information**... link can be selected to view additional details about the packet.

Similarly, any Internet website or IP Address can be blocked from your computer by clicking on the **Add** button from the Blocked Sites / IP Addresses section and entering the appropriate site / IP Address.



Adding Websites / IP addresses

Trusted or blocked websites / IP addresses can be added by clicking on the **Add** button from the Trusted or Blocked Sites / IP Addresses section in the Main Menu and entering the appropriate information. Entire Local Area Networks can be added by entering the root IP address and the Network Mask. Internet websites can be entered by selecting the "URL" section and entering the site in the "Host Name" field.



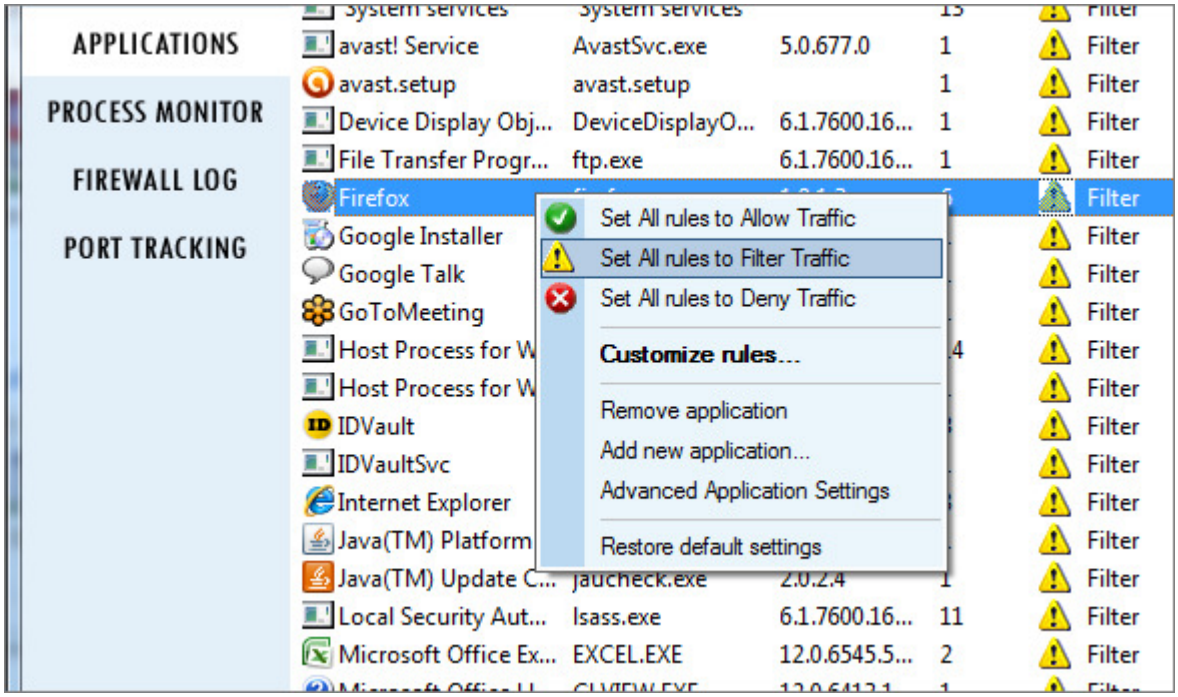
XMAS and NULL Scans

While Privatefirewall does not display any special type of firewall alerts for XMAS and NULL scans/traffic, it detects, blocks and logs these events as "XMAS scan detected" or "NULL scan detected" to the firewall log.

Firewall alerts are enabled when Privatefirewall is operating in Manual Control mode. Regular Packet Filter alerts are displayed indicating the specific port number, but does not reference XMAS or NULL scan.

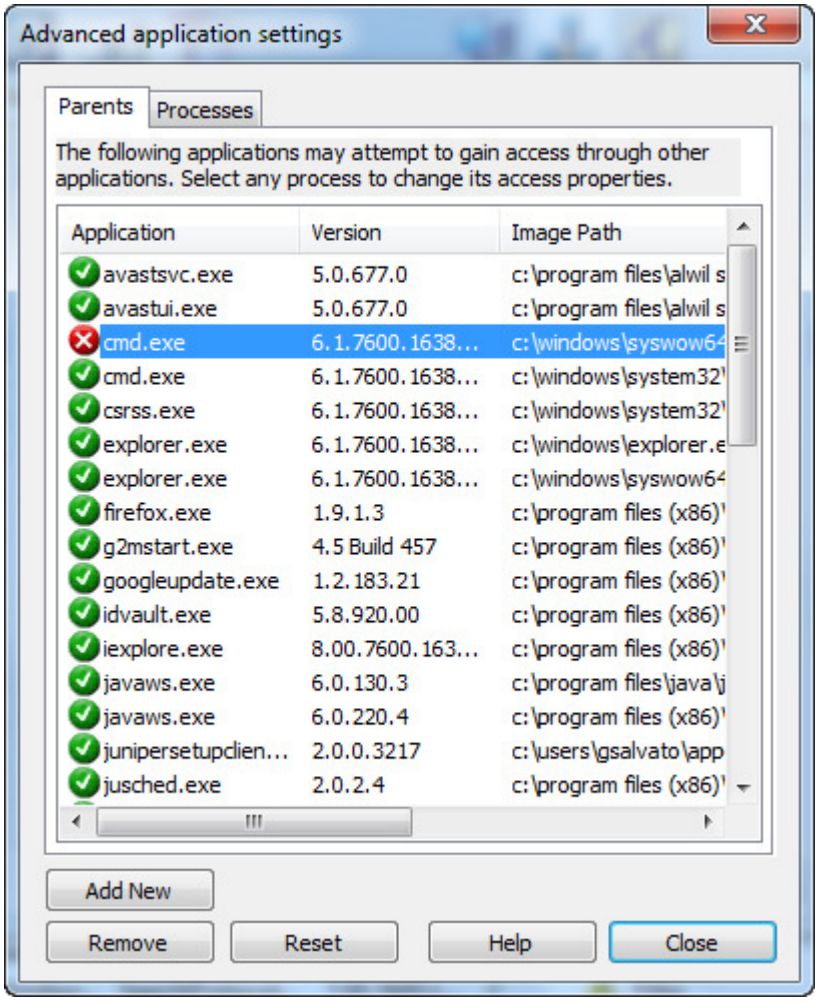
Applications

The Applications Setting screen consists of all the firewall rules that Privatefirewall is enforcing for the Applications listed. The screen includes the Application and file executable name, version number, number of rules being enforced, and the classification of the rules. Privatefirewall can either allow or deny incoming or outgoing traffic for each access attempt, or ask for a decision upon every access attempt.



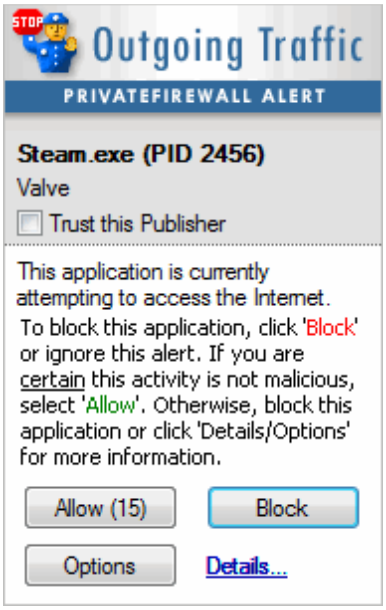
Advanced Application Settings (accessed from File/Settings/Advanced application settings)

Some applications allow other applications to control their actions, which means that the 'primary' application may be protected, but the 'secondary' Parent application may be permitted to access the Internet *through* the primary application. The Advanced Applications settings screen lists these 'secondary' Parent applications that have attempted to access the Internet or network through a 'primary' trusted application. Each application in the list can be set to Allow or Block Access.

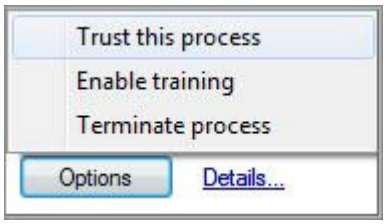


Application Detection (Firewall) Alerts

When an application first attempts to access the Internet, Privatefirewall will display an Application Detection alert and ask to either allow or block access (see Privatefirewall Settings -> Security Alert and Threat Management Options section of this guide for more information about event filtering and alerting).



Selecting the Options button will display additional options that will allow you to Trust this process, Enable Training or Terminate the Process.



NOTE: Privatefirewall will display the Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

Options – Trust This Process

Trust this process on the tray alerts allows you to Allow all activity related to a particular program or process (rather than selecting simply allowing only the activity specific to the alert (i.e. Open Processes, Interprocess Communication, etc.).

Options - Enable Training

Enabling Training via tray or full alert:
The Enable Training option can be selected by clicking on the Options button on the Privatefirewall firewall, process detection or process monitor tray and full alert (full alerts are displayed in Manual Control mode or invoked by clicking ”Details…” from the tray alerts). Selecting this option activates a training period of 180 seconds and allows all actions (just as in the initial/normal training mode), except those that were blocked previously. The training period is extended automatically (restarts the 180 second clock) for every new driver event that occurs within the initial or subsequent related 180 second period. This “temporary” or “on-demand” training is disabled if and at the moment when the user changes any setting via File | Settings or once the 180 second period has expired.

Enabling Training via the Tray menu:
Training is also available via the Privatefirewall tray menu (to accommodate scenarios where, for example, one is installing/using something new and would like to initiate training in this temporary or activity-specific manner). A check mark next to the “Train” tray menu

item will appear if the "Train" option is activated manually or via an alert and remain checked/active based on the same logic as Enabling Training via tray or full alert.

Enabling Training via File | Settings | Advanced Tab (for Firewall and Process Monitor settings): In contrast to enabling training via Privatefirewall alerts or the Tray menu, enabling training via File | Settings | Advanced Tab (for Firewall and Process Monitor settings) will activate Training for as long as the check box is checked.

In all training scenarios, Privatefirewall will block only the activity that was previously blocked (or configured to block). All new activity will be allowed and assimilated ("learned") as legitimate. The Training options should only be selected when you are absolutely sure that the application/process is legitimate.

Options – Terminate process

Clicking the **Terminate Process** option will stop the relevant process.

Click 'Details...' in the Tray Alert to display an expanded alert which provides more detailed information about the suspicious activity and additional threat management options (see right). The expanded alert lists the program name, version number, file path, and other details. If the 'Web Search' link is selected, a search containing the process executable filename will be performed in your default browser. For processes with valid digital signatures, additional options enable you to Trust the software publisher and View the Publisher's digital certificate.

NOTE: In Manual Control mode, the expanded alert will appear automatically and no Tray Alerts will be displayed.

Detailed Alert Management Options

Web Search – clicking the Web Search link provides a convenient way to learn more about the subject application. The feature will start a web search using the system's default browser and search engine.

View certificate - It may be helpful and informative to view the details of the software publisher's certificate before making the determination that the publisher should be added to the Trusted Publisher list. Simply click the **View certificate** link on the Expanded Alert to

invoke the dialog that contains the Certificate's details.

Trust This Publisher – Check this box to add the software publisher to the Trusted Publisher List.

Remember this setting – by default, the rule associated with that particular type of activity is only remembered for the current session (after reboot, the rule will no longer be valid/present). To remember the rule for subsequent same activity, check the Remember this setting box. Related rules will apply to both the High and Low security levels.

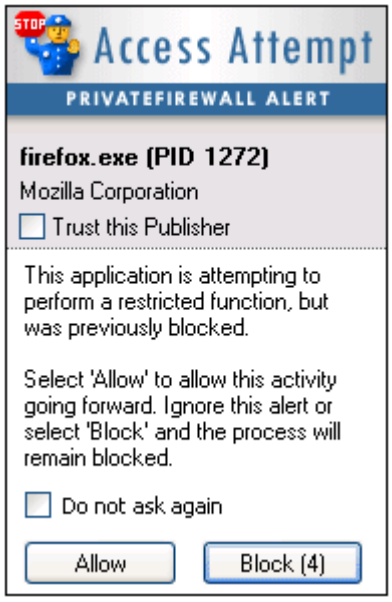
Apply to all alerts - will eliminate the display of additional alerts for this process or application by treating subsequent activity based on the same response to the initial alert. Note: If the alert is firewall derived, the "Apply to all alerts" response will apply to all future firewall alerts. If the alert is Process Monitor derived, the "Apply to all alerts" will apply to all future Process Monitor alerts. In either case, related rules will apply to both the High and Low security levels.

Allow – Clicking the **Allow** button will allow the specific action being attempted by the program. Selecting Allow (with Remember this setting un-checked), will allow the activity, but only for the current session (after reboot, the rule will no longer be valid/present). Related rules will apply to both the High and Low security levels.

Train – Clicking the Train button will invoke Training mode.

Terminate - Clicking the Terminate button will stop the relevant process.

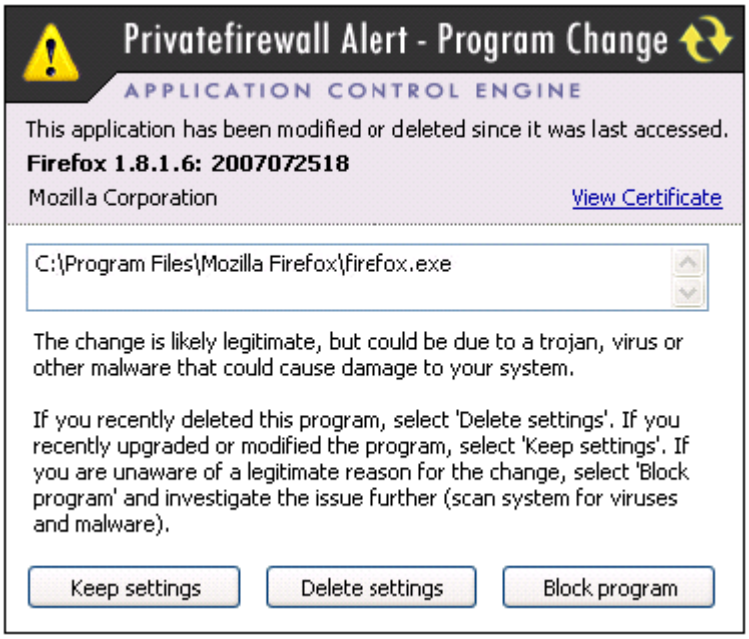
Block – Clicking the **Block** button will stop the specific action being attempted by the program. Selecting Block (with Remember this setting un-checked), will block the activity, but only for the current session (after reboot, the rule will no longer be valid/present). Related rules will apply to both the High and Low security levels.



If an application attempts to load that was previously ignored or blocked, Privatefirewall will generate an alert with the choice of allowing or blocking the previously blocked activity.

Program Changes

After an application has been installed and added to the Program List, Privatefirewall will display an alert if the program version or version number has changed.



There are usually one of 3 scenarios when this alert is displayed:

1) The application has been updated or upgraded:

This is normal for many applications that have frequent update/upgrades. If this is the case, select the 'Keep settings' button.

2) The application has been deleted:

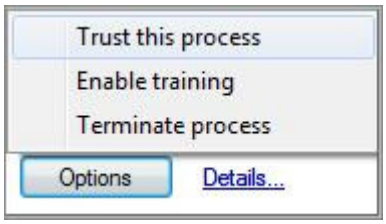
This is normal activity as many applications are frequently added and deleted. If this is the case, select the 'Delete settings' button.

3) The application is being substituted by a hacker/intruder by using the name of the trusted application in order to gain unauthorized access.

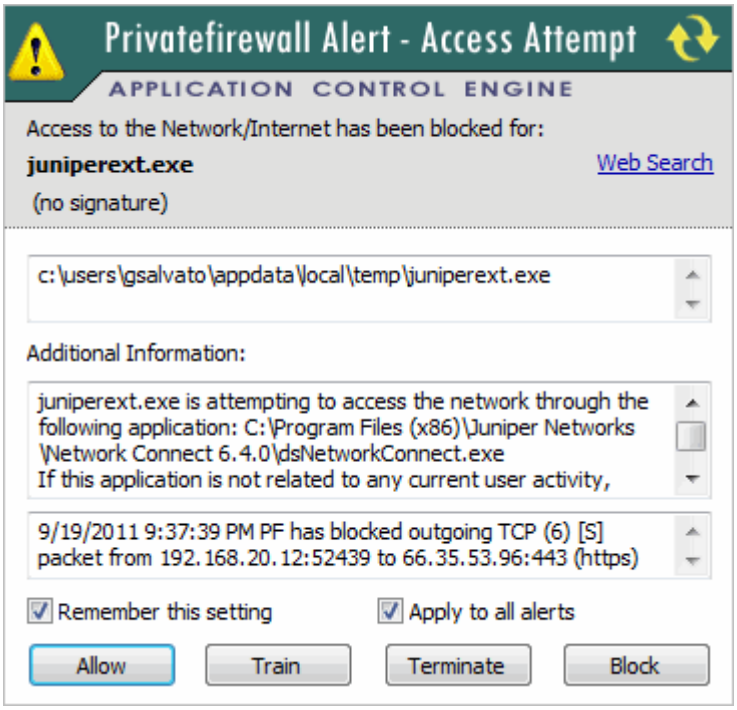
This is commonly referred to as a Trojan Horse. The hacker creates a malicious program that is designed to either cause damage or extract valuable information and assigns a common name to the program (ex: Internet Explorer is usually named iexplore.exe). The hacker then attempts to place this program into the directory where the common application is usually placed (ex: c:\program files\microsoft office). If the hacker is successful, the malicious application will be launched the next time Internet Explorer, or iexplore.exe, is attempted to be accessed. If Privatefirewall is installed, the Program Change alert will be displayed and the 'Deny Access' button should be selected so the issue can be investigated and resolved.

Program Access Alert

A method commonly used by hackers to gain unauthorized access is to launch a trusted application and gain access through it via another 'secondary' or Parent application. However, this activity is also a function of many trusted applications operating normally when accessing the Internet. If you are in the process of accessing the Internet with a trusted application, the Parent application name may not be common or recognizable, so it may be difficult to determine if the activity is normal or malicious. If you receive an alert (see right) and the application listed is related to any form of current activity, it is most likely not malicious activity. However, if the activity may be unrelated (ex: if the application is not even open, etc.), it may be an attack attempt and can be addressed using Allow, Block and other Options investigated further by selecting the 'Details…' link.

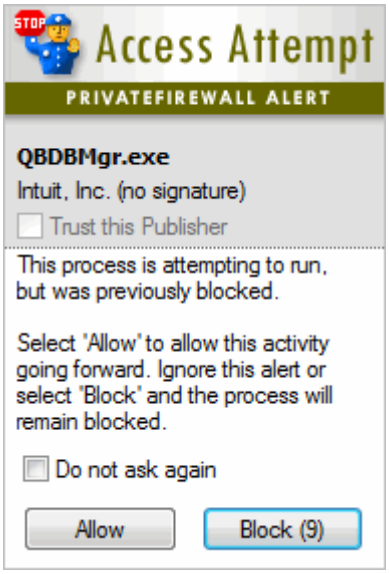


NOTE: Privatefirewall will display the Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

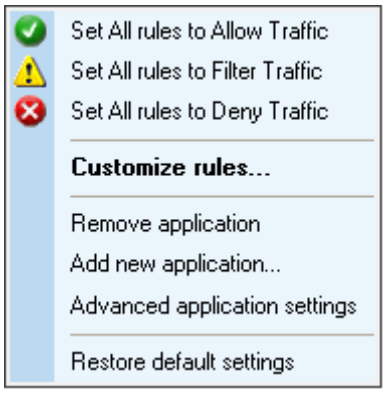


Click 'Details/Options' in the Tray Alert to display an expanded Alert, which contains more detailed information about the suspicious activity and additional threat management options. This alert lists the program name, version number, date, time, and incoming/ outgoing IP address, and the 'parent application' which was attempting to be used. It will also specify whether the Traffic is inbound or outbound and provide several response options. If the 'Web Search' link is selected, a search containing the executable filename will be performed in your default browser.

If an application attempts to load or perform any other action but was previously ignored or blocked, Privatefirewall will generate a special Access Attempt alert. To view a list of all these types of applications detected by Privatefirewall, click on 'File/Settings/Advanced applications' from the Main Menu.



Application Rule Setting



Privatefirewall provides the capability to manually add, remove, or modify rules for any installed application. Hackers can disguise a program as a known application resource to gain unauthorized access. Privatefirewall detects the resources within each application that hackers may specifically use and enables those resources to block any disguised resources or hack attempts. Right-click on any application within the Applications Page and the 'application pop-up' menu will appear (see left).

Allow/Filter/Deny Traffic

Internet Traffic related to any application can be adjusted by selecting 'Set all rules to Allow/Filter/Deny Traffic' from the application pop-up menu. The default setting for any set of rules related to an application is 'Filter Traffic'. However, these rules can be disabled by selecting either 'Allow' or 'Deny' Traffic. This may be appropriate when temporary access or restriction is desired. Additionally, the rules that were created for that application will remain in memory and will still be applied if 'Filter Traffic' is re-selected.

Remove application

The application can be removed from the Application List by selecting 'Remove Application' from the application pop-up menu. This option will remove any protection that was applied to the selected application.

Add new application

A new application can be manually added by selecting 'Add New Application' from the application pop-up menu. Once this is selected, the executable file that corresponds to the desired application must be selected. In addition, rules must be set manually for the application in order for Privatefirewall to apply any filtering or protection.

Advanced Applications settings

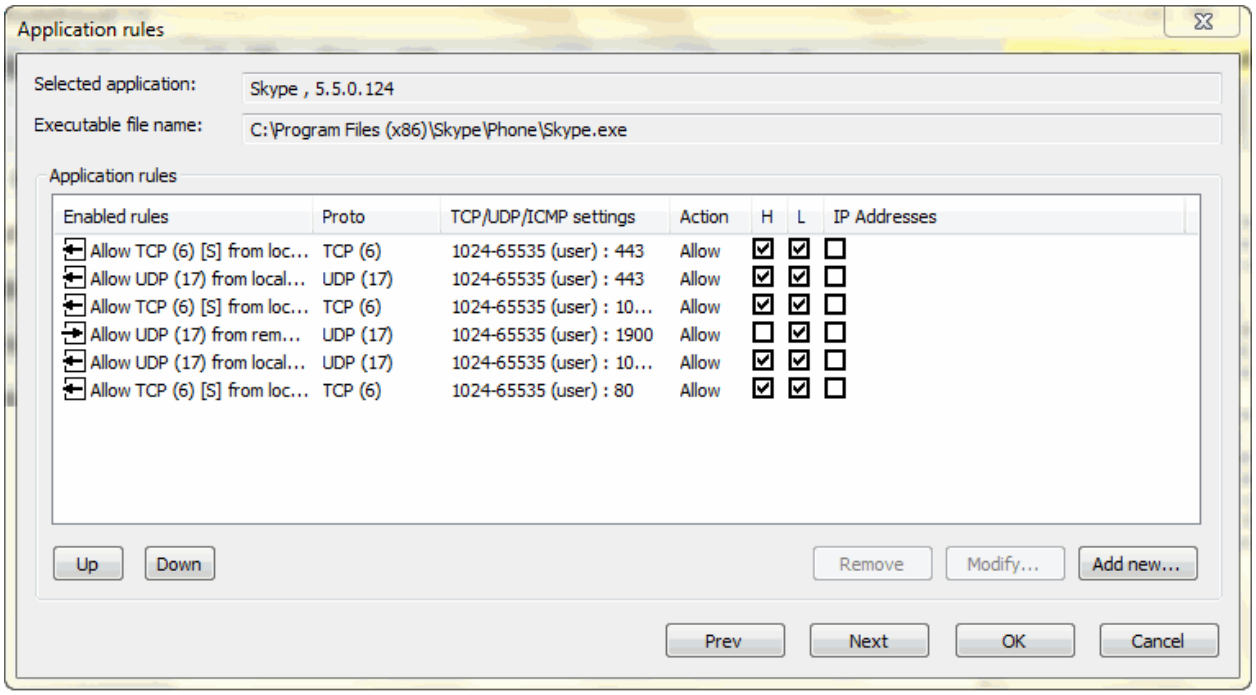
The Advanced Applications settings screen lists applications that have attempted to access the Internet or network through another trusted application. This is a method commonly used by hackers to attempt to gain unauthorized access.

Restore default settings

Restore Default Settings will restore all default applications to the Application List. The option only pertains to applications that are pre-loaded by Privatefirewall. The option will be grayed-out for all other applications.

Customize Rules

Application rules can be customized by selecting 'Customize Rules...' from the application pop-up menu. When selected, Privatefirewall lists the Program name, program executable file name, program version number, and a listing of rules for that application (see below). Rules can be added, removed, or modified by right-clicking on any rule.



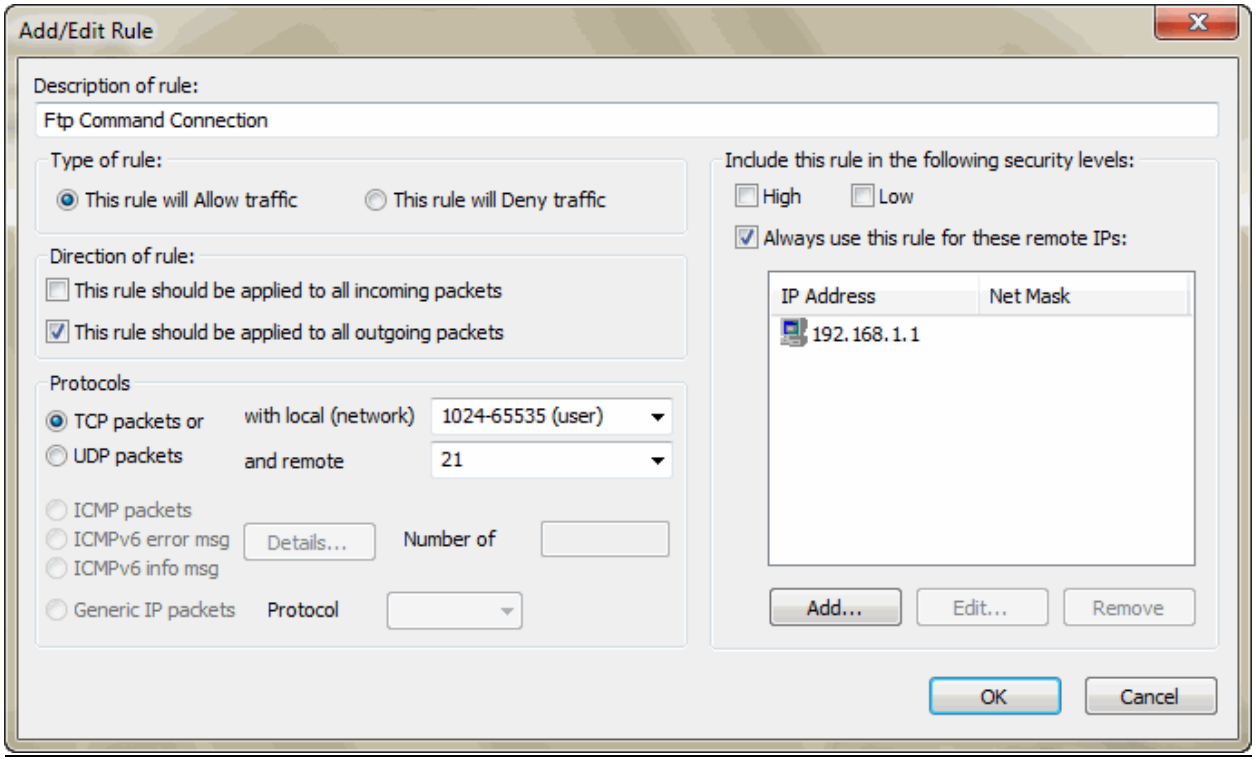
Move Order of Rule

Using the Up and Down buttons will allow the order of the application rule to be prioritized and processed as desired.

Navigating through listed Applications
Navigation to the other listed Applications is possible by selecting the Prev (ious) or Next buttons.

Remove application rule
An application rule can be removed from the Application List by highlighting an application rule and selecting the Remove button.

Add New or Modify Existing Application Rules



The Add/Edit Application rule dialog provides various configuration options that enable even IP Address specific application level communication control. Using this feature, it is possible to permit application access to/from only certain IP addresses.

Examples:

1) Restricting ftp.exe: Remove both L and H zones. Check "Always use this rule for these remote IPs". Add 192.168.1.1 IP address. In this way, ftp.exe will only be able to access the 192.168.1.1 IP address. All others will be blocked.

2) Restricting RDP: From System services, select the Enabled rules for RDP. Remove the L and H zones. Check "Always use this rule for these remote IPs". Add the IP Addresses for which connection to/from your computer should be allowed. For all other IPs, the RDP port will be completely stealth.

In most cases where a custom rule is created for a particular type of activity/application/IP address, the H and L security levels would likely be unchecked, but there are scenarios where one might use a combination - for example, you might check the L security level to manage LAN communication one way while FTP access via specific IP address only - so here

both the L security level and the Always use this rule for these remote IPs would be checked.

Privatefirewall provides flexibility in how a rule might be applied:

Use specified rule for -
1) Any hosts in H zone if checked
2) Any hosts in L zone if checked
3) Listed IPs if checked

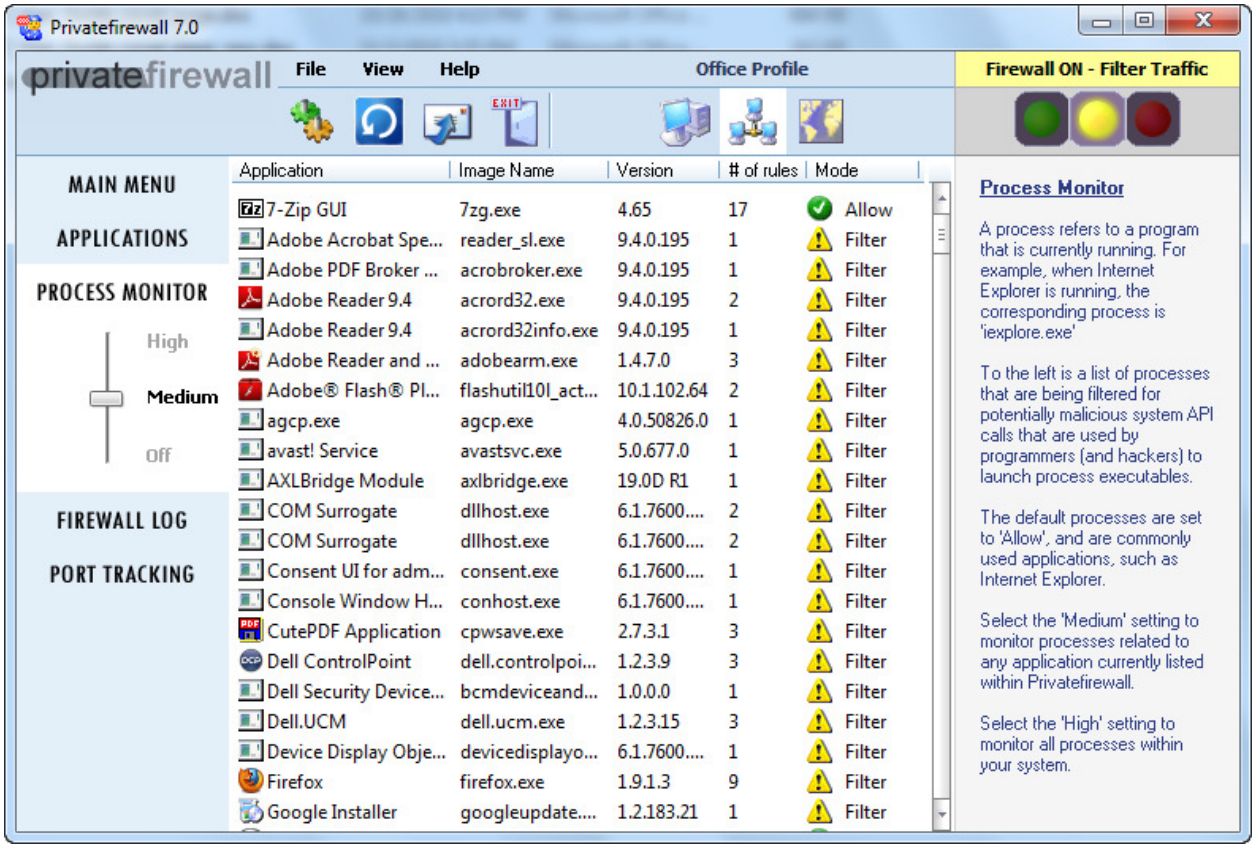
Port-specific Application Control
Port-specific rules can be defined for any Application by using the available port ranges and ports listed in the drop down fields or by manually typing single or multiple ports numbers (i.e. either single port, like 101 or or single range like 101-204).

Unconditional Port Control
- Create port-specific (or range) Deny Rule for System services (Applications, System services, Add new,…).

- Remove any conflicting Allow rules for specific applications (they will override the System services port block). Current default Application rule logic works as follows: 1) check application rules; if such rule exists (to deny or allow traffic) no further processing is performed; 2) check System services application rules and exercise where application-specific rules do not conflict/take precedence.

Process Monitor

A process refers to a program that is currently running. For example, when Privatefirewall is running, the corresponding processes, 'PFNet' and 'PFGUI.exe' will run (visible in Task Manager). Privatefirewall maintains a list of processes that are being filtered for potentially malicious system API calls used by programmers and hackers to launch process executables. Privatefirewall maintains a set of default processes that are related to commonly used applications, such as Internet Explorer, and are set to 'Allow'. Non-default processes that are detected by Privatefirewall will be set to 'Filter' if allowed or 'Deny' if not allowed.

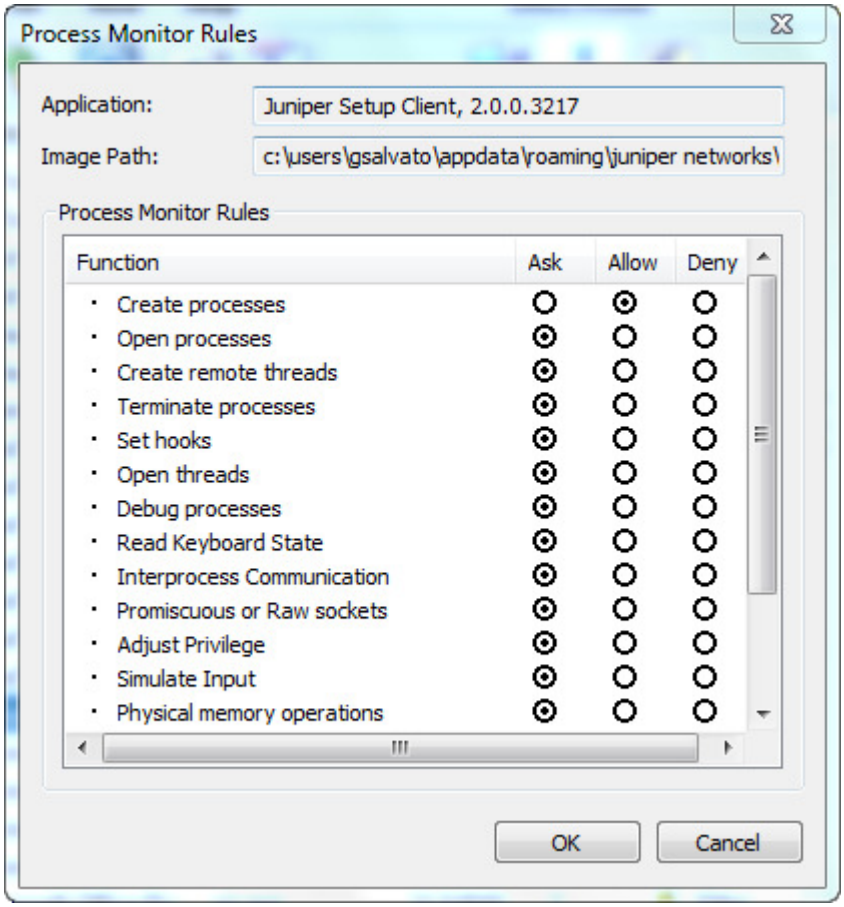


The Process Monitor can be set to either 'High', 'Medium', or 'Off'.

- The 'High' setting will monitor all processes running on your computer and will only allow LOCAL/NETWORK services.
- The 'Medium' setting (default) will monitor processes related to any applications currently listed within Privatefirewall and allow services running under system account.
- The 'Off' setting will disable the Process Monitor, but not any other Privatefirewall functionality.

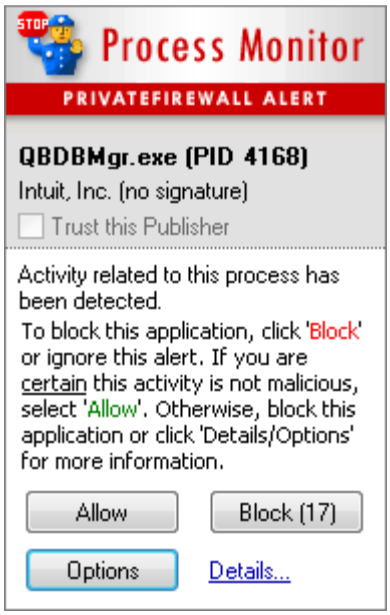
Process Inspection Rules

Double-Click on any process within the Process Monitor menu for detailed information. For each listed process, Privatefirewall monitors the WinAPI functions listed under the 'Function' column within the Process Monitor Rules dialog. Each WinAPI function has the option for Privatefirewall to 'Ask', 'Allow', or 'Deny'. If 'Ask' is selected, Privatefirewall will prompt the user as to whether the specific process function should be executed. If 'Allow' is selected, Privatefirewall will allow the specific process function to operate without any user intervention. If 'Deny' is selected, Privatefirewall will not allow the specific process function to execute. Default applications will set all functions to 'Allow'.

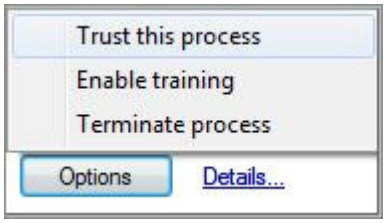


Process Monitor Alerts

If any potentially malicious process-related activity is detected, Privatefirewall will display a Process Monitor alert and ask to either allow or block access (see right). See Privatefirewall Settings -> Security Alert and Threat Management Options section of this guide for more information about event filtering and alerting.

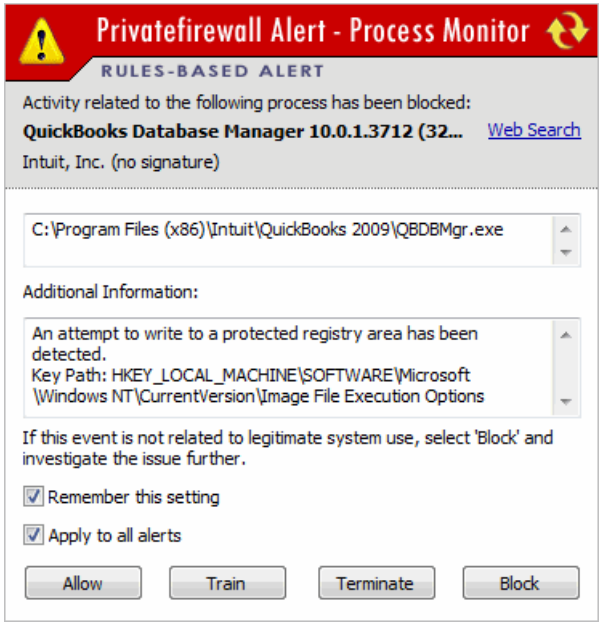


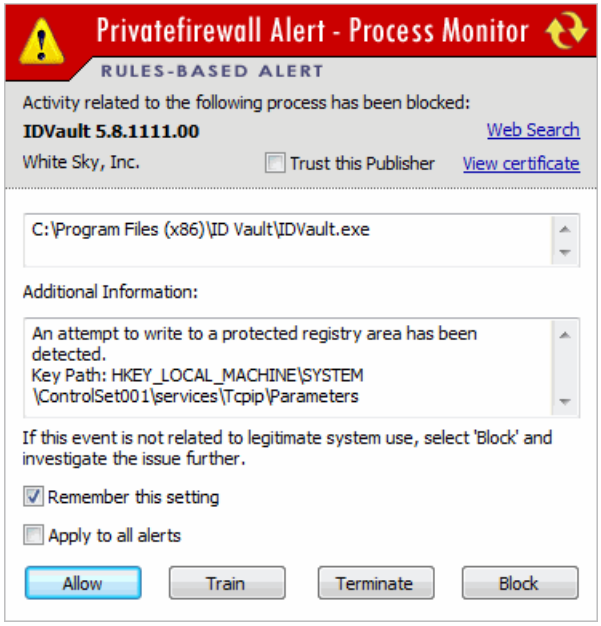
Selecting the Options button will display additional options that will allow you to Enable Training or Terminate the Process.



NOTE: Privatefirewall will display the Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

Clicking the 'Details…' link from the Tray Alert will display an expanded alert, which contains more detailed information about the suspicious activity and additional threat management options (see below). In Manual Control mode, the expanded alert will appear automatically and no Tray Alerts will be displayed. The expanded alert lists the program name, version number, file path, and additional details. If the 'Web Search' link is selected, a search containing the process executable filename will be performed in your default browser. Processes with valid digital signatures include additional options that enable you to Trust the software publisher and View the Publisher's digital certificate.





There are several types of potentially malicious process-related activity that will generate an alert. For example, the Process Monitor will detect attempts to create or change restricted objects. Below are examples of Alerts that are displayed in these cases. For all alerts, if the application or process listed is related to any legitimate activity, it is most likely not malicious activity. However, if it is unrelated (ex: the application or process referenced is not even running, etc.), it may be malicious activity and the "Block" button should be selected so the issue can be investigated.

Detailed Alert Management Options

Web Search – clicking the Web Search link provides a convenient way to learn more about the subject application. The feature will start a web search using the system's default browser and search engine.

View certificate - It may be helpful and informative to view the details of the software publisher's certificate before making the determination that the publisher should be added to the Trusted Publisher list. Simply click the **View certificate** link on the Expanded Alert to invoke the dialog that contains the Certificate's details.

Trust This Publisher – Check this box to add the software publisher to the Trusted Publisher List.

Remember this setting – by default, the rule associated with that particular type of activity is only remembered for the current session (after reboot, the rule will no longer be valid/present). To remember the rule for subsequent same activity, check the Remember this setting box. Related rules will apply to both the High and Low security levels.

Apply to all alerts - will eliminate the display of additional alerts for this process or application by treating subsequent activity based on the same response to the initial alert. Note: If the alert is firewall derived, the "Apply to all alerts" response will apply to all future firewall alerts. If the alert is Process Monitor derived, the "Apply to all alerts" will apply to all future Process Monitor alerts. In either case, related rules will apply to both the High and

Low security levels.

Allow – Clicking the **Allow** button will allow the specific action being attempted by the program. Selecting Allow (with Remember this setting un-checked), will allow the activity, but only for the current session (after reboot, the rule will no longer be valid/present). Related rules will apply to both the High and Low security levels.

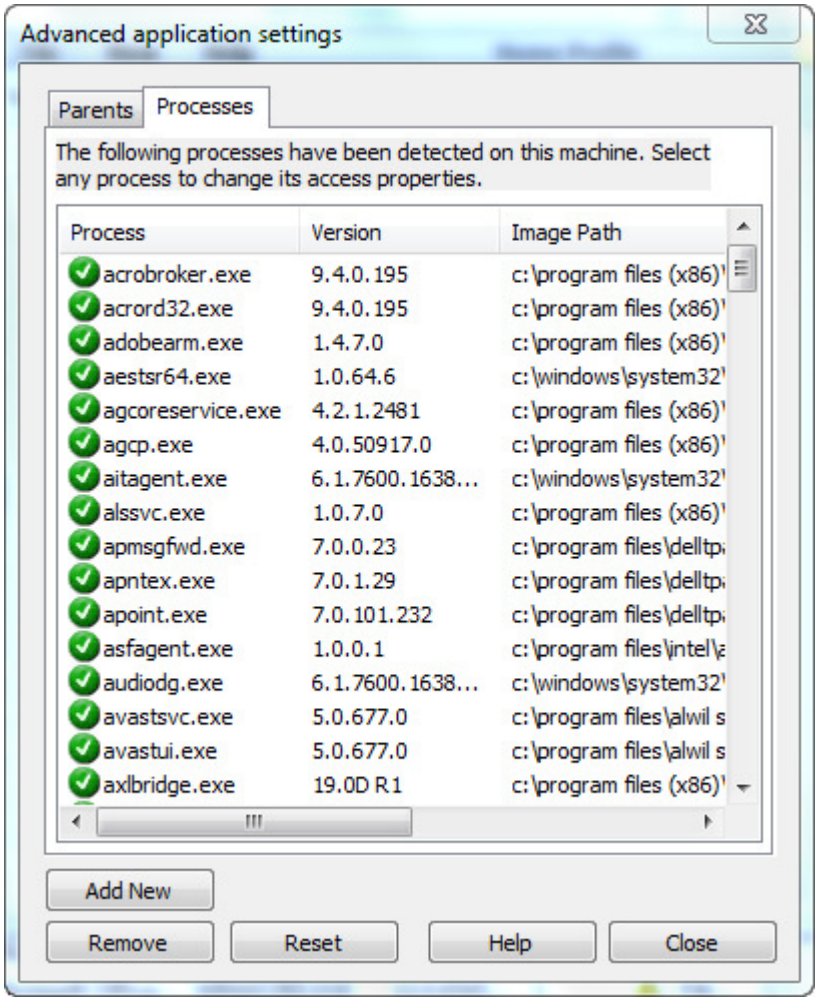
Train – Clicking the Train button will invoke Training mode.

Terminate - Clicking the Terminate button will stop the relevant process.

Block – Clicking the **Block** button will stop the specific action being attempted by the program. Selecting Block (with Remember this setting un-checked), will block the activity, but only for the current session (after reboot, the rule will no longer be valid/present). Related rules will apply to both the High and Low security levels.

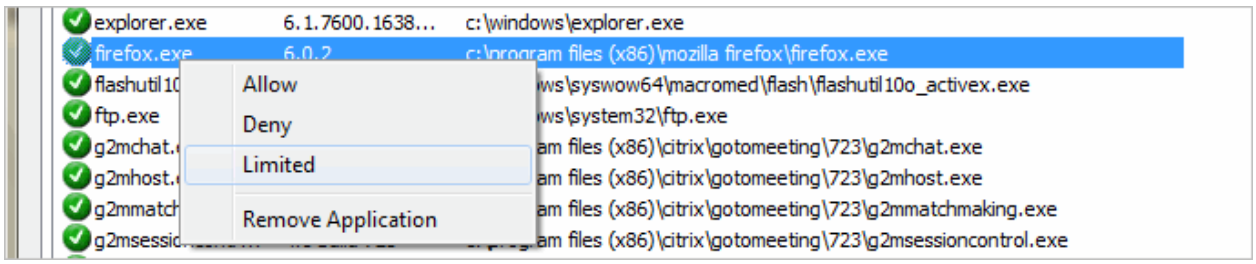
Process Detection

In addition to processes being filtered for system API calls, Privatefirewall also maintains a list of commonly used processes and provides an alert when an unknown process attempts to launch.



Managing Process Rights

Processes can be run with Reduced rights directly via a relevant tray or full alert, but can also be managed via the Processes tab of the Advanced Applications Settings. Simply highlight a Process and apply the right mouse click to Allow, Deny, Remove or run with Limited Rights.



Additional Information

The Process Monitor also checks for any modification to the following:

File Extensions
exe
dll
msi
ocx
com
vxd
sys
bat
cmd
pif
scr
hta
js
jse
lnk
reg
vbe
vbs
wsf
wsh

System Files
win.ini, system.ini, hosts

Paths
start menu\programs\startup

Registry Keys
shell\xxx\open (where xxx is any application)
software\microsoft\active setup\installed components
software\microsoft\windows\currentversion\explorer\sharedtaskscheduler
software\microsoft\windows\currentversion\shellserviceobjectdelayload
software\microsoft\windows\currentversion\explorer\shellexecutehooks
software\microsoft\windows\currentversion\shell extensions\approved
software\classes\folder\shellex\columnhandlers
software\microsoft\windows\currentversion\shellserviceobjectdelayload
software\microsoft\windows\currentversion\app paths
software\microsoft\windows\currentversion\run
software\microsoft\windows nt\currentversion\winlogon\shell
software\microsoft\windows nt\currentversion\winlogon\userinit
software\policies\microsoft\windows\system\scripts\startup
software\policies\microsoft\windows\system\scripts\logon
software\microsoft\windows\currentversion\policies\system\shell
software\microsoft\windows nt\currentversion\windows\load
software\microsoft\windows nt\currentversion\windows\run
software\microsoft\windows\currentversion\policies\explorer\run
system\currentcontrolset\control\session manager\bootexecute
system\currentcontrolset\services
software\microsoft\windows\currentversion\explorer\browser helper objects
software\microsoft\internet explorer\urlsearchhooks
software\microsoft\internet explorer\toolbar
software\microsoft\internet explorer\extensions
software\microsoft\windows nt\currentversion\image file execution options
software\microsoft\command processor\autorun
software\microsoft\windows nt\currentversion\windows\appinit_dlls
system\currentcontrolset\control\session manager\knowndlls
software\microsoft\windows nt\currentversion\winlogon\system
software\microsoft\windows nt\currentversion\winlogon\notify

software\microsoft\windows nt\currentversion\winlogon\ginadll
software\microsoft\windows nt\currentversion\winlogon\taskman
control panel\desktop
system\currentcontrolset\control\bootverificationprogram\imagename
system\currentcontrolset\control\print\monitors
software\pwi, inc.\privatefirewall

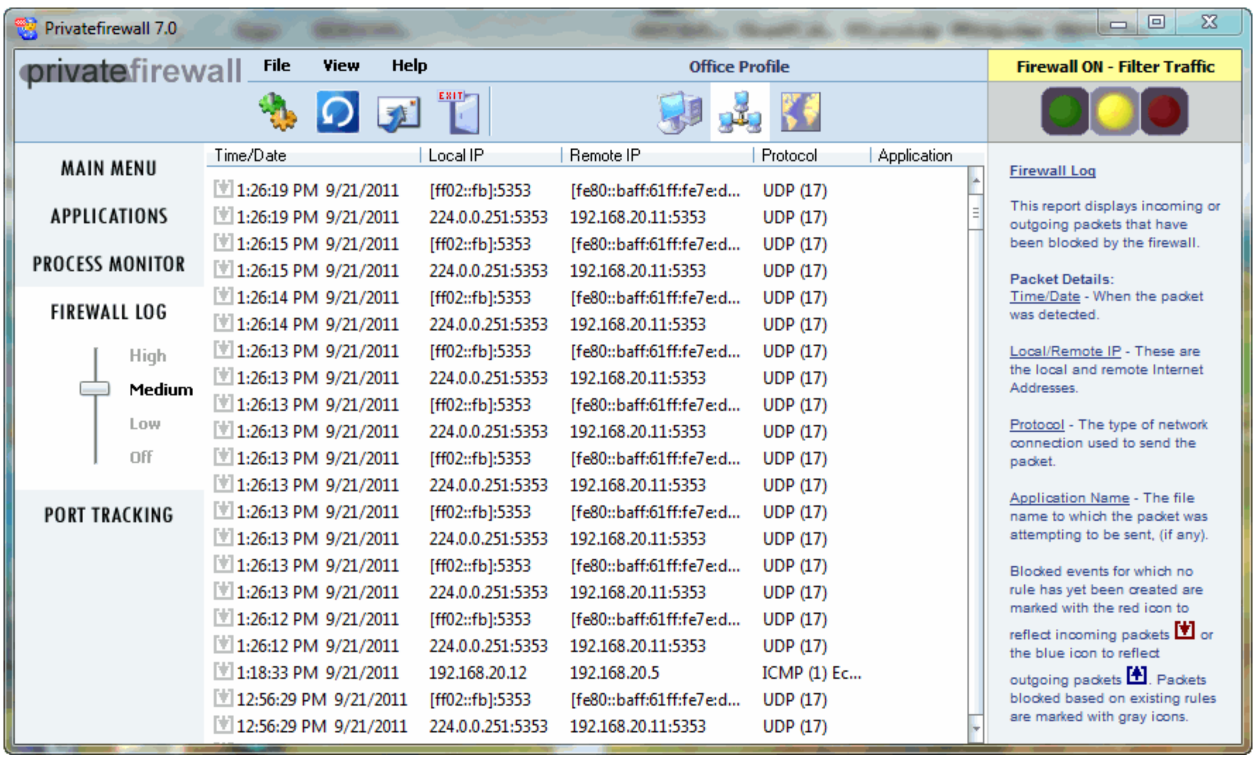
Firewall Log

The Firewall Log records incoming and outgoing packets, which are chunks of information routed between an origin and a destination on the Internet or any other network; one of which is your computer. As illustrated in the screen shot below, the 'home' IP Address is 192.168.0.2. **NOTE: Your IP address may be the same address during every Internet connection (called a "Static IP", used in most T1/DSL connections). Or, your IP may change for each Internet connection (called a "Dynamic IP" used in most Cable/Dial-Up connections).**

Privatefirewall reports the following:

Time/Date - When the packet was detected.
Local IP - The Internet address to which the packet is traveling.
Remote IP - The Internet address from which the packing is coming from.
Protocol - The Network Protocol, or type of network connection used to send the packet.
Application - The name of the application to/from which the packet is attempting to be sent (if any).

Right mouse-clicking any entry within the Firewall Log will provide the following options: Trust Remote (IP), Block Remote (IP), Copy Remote IP(s) to Clipboard, Copy Selection to Clipboard, Clear Report, Save Report As, or invoke Advanced Reports.



Log level control can be managed via the slide bar: Off, Low, Med, High. Low (only events with red/blue icons are logged, i.e. which are not related to any existing rules), Medium (all events except restricted IPs), and High (All firewall events are logged). Duplicate entries are not logged.

Log entries that do not indicate an Application (Application field is empty), mean that no

application was registered for this port or it is handled by the OS itself (i.e. port 137-139, 443), but is not allowed by current ruleset.

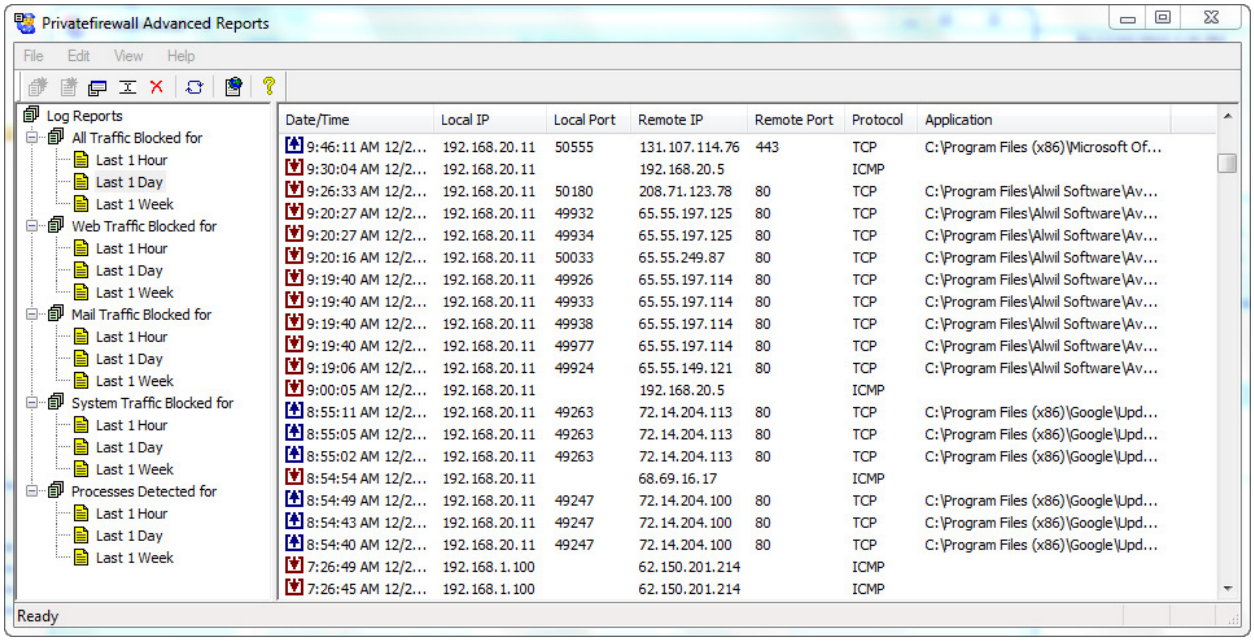
Advanced Reports

Firewall log records can be sorted by type and time of occurrence within Privatefirewall Advanced Reports. This report can be accessed from 'View/Advanced Reports'. Reports can be sorted by Web, Mail, or System access attempts. Each of these reports can also be sorted going back 1 Hour, 1 Day, or 1 Week.

Note: Last 1 hour means last 3600 seconds, last 1 day - last 86400 seconds, (so reports could display data spanning more than one calendar day, last 1 week - last 7*86400 seconds

Privatefirewall Advanced Reports lists the following:

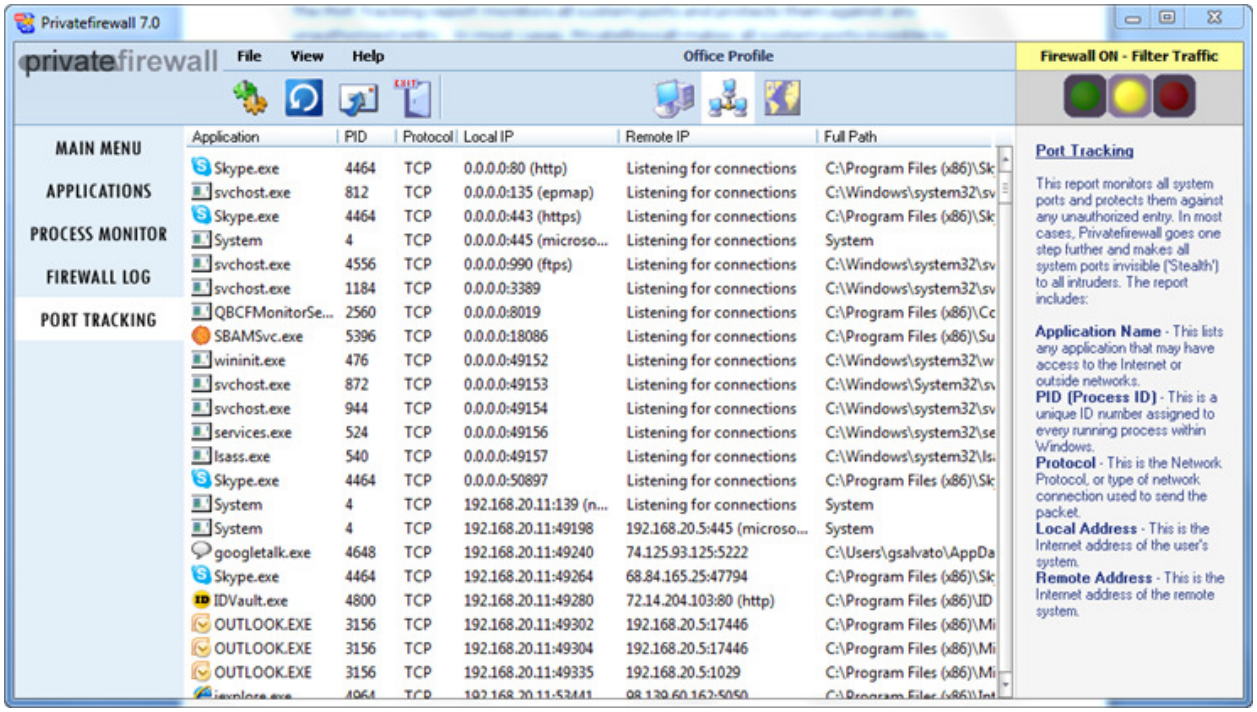
Date/Time - When the packet was detected.
Local IP (Internet address) - The Internet address from which the packing is coming from.
Local Port - The port from the local computer involved in the access attempt.
Remote IP - The Internet address to which the packet is traveling.
Remote Port - The port from the remote computer involved in the access attempt.
Protocol - The Network Protocol, or type of network connection used to send the packet.
Application (if applicable) **-** The name of the application to which the packet is attempting to be sent (if any).



Port Tracking

The Port Tracking report monitors all system ports and protects them against any unauthorized entry. The Privatefirewall Port Tracking report includes the following attributes:

Application Name - Any application that may have access to the Internet or outside networks.
Process ID - The unique number assigned to every running process within the Windows environment.
Protocol - The Network Protocol, or type of network connection used to send the packet.
Local Address - Your system's IP address.
Remote Address - This is the Internet address from where incoming packets are originating. This will display either a specific IP, or if one is not currently detected, a status (such as "Listening for packets/connections").



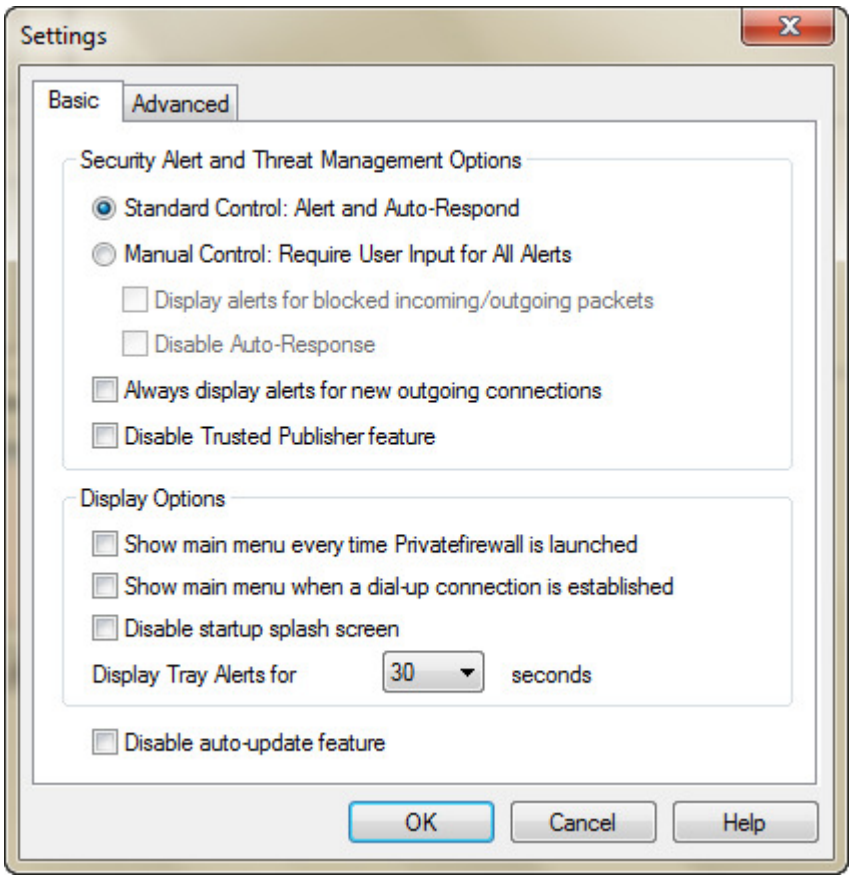
Privatefirewall Settings

(This menu can be accessed by selecting 'File/Settings' from the Main Menu)

Basic Settings

Display Main Menu/alerts

The Basic Tab provides user control over the preferred Security Alert and Threat Management mode and Display options



Standard Control mode

Privatefirewall provides two Security Alert and Threat Management options. Standard Control mode is enabled by default and is designed to reduce alert frequency by automatically managing much of the security-related configuration.

In Standard Control mode, Applications/Processes with **validated digital signatures**, regardless of PID, will be allowed, not generate alerts and be added to the Trusted Publisher/White List.

- ***Exception 1:*** *An alert (fw) will be generated for any App/Proc where inbound traffic is detected that was not recorded during training period. PF will automatically block the event if the user does not elect to Allow via the Tray or Full alert.*

All Applications/Processes that **fail signature validation** will generate an alert, and be blocked by default if not Allowed by the user prior to the alert time-out (30 seconds), or by selecting the Allow button in the Full alert.

In Standard Control mode, clicking the Allow button should prevent, where possible (***see Exceptions***), all other alerts related to the same application. This logic applies to both the Tray or Full alerts.

- ***Exception 2:*** *An alert will be generated if a program change (size, name, version number, etc.) is detected in a process or application file.*

Manual Control mode

Manual Control mode is geared for those desiring complete control over the configuration of Privatefirewall. Most of the automated response functionality provided in Standard Control mode is disabled requiring the user to respond to a greater number of alerts and make configuration determinations regarding the related applications and processes.

- Events generated by processes listed on the Trusted Publisher List will be allowed and will not generate alerts. Essentially, CAPICOM validation does not preclude an alert from being generated in Manual Mode. Only events generated by publishers actually on the TP list will be allowed (and not generate alerts).

- Processes with validated signatures that send/receive packets via the Internet, regardless of PID, will generate an alert and will be allowed by default (user will have option to block event manually via the on-screen alert).

- Processes that fail signature validation will generate an alert and be blocked by default (after alert time-out).

- Manual Control mode provides an option to enable/disable packet-specific tray alerts via "Display alerts for blocked incoming/outgoing packets". In PF7, File -> Settings -> Basic tab (Manual Control), when the "Display Alerts for Blocked incoming/outgoing packets" checkbox is un-checked, firewall tray alerts (incoming/outgoing packets for which firewall blocking rules apply) are not displayed

(for signed or unsigned applications). If the option is enabled, firewall tray alerts reflecting incoming/outgoing packets (for which firewall blocking rules apply) will be displayed (for both signed and unsigned applications).

The checkbox enables the tray alerts which notify the user about any blocked traffic. This option does not change the behavior of the larger/full alerts. The tray alerts are designed to provide visibility to all firewall activity.

The difference between the tray alerts and large is that large alerts are only used when the corresponding packet is associated with a particular application on the pc (vs external scans) and were not previously blocked.

- Manual Control mode provides an option to disable Auto-Response altogether (Disable Auto-Response), thereby requiring that the user authorize any activity that would generate an alert.

- Disabling Auto-Response in Manual Control mode also disables the Auto-Response related to the Trusted Publisher component enabling the user to control what apps should be added to the TP List.

Always display alerts for new outgoing connections
By default, in both Standard and Manual Control modes, Privatefirewall auto-allows outgoing connections for applications for which digital signatures have been validated or for Trusted Publishers.

The **Always display alerts for new outgoing connections** option overrides Trusted Publisher (and the underlying CAPICOM-based digital certificate verification process). This feature allows the user to authorize all new outgoing connections, (but does not apply to outgoing connection rules set manually or by virtue of alert response).

There is a functional difference of this feature between **Standard** and **Manual** modes. Standard mode assumes that if you've allowed one outgoing connection from an app, all others should be allowed.

Manual mode enables the user to influence the rule associated with each type of connection. In some cases, you may want to simply manually Allow a particular application as some establish several/regular outbound connections (often similar, but nonetheless distinct) and thus generate lots of alerts. Privatefirewall's various automated or user-controlled

configuration management provide a different levels of control depending on personal preference for security posture and ease-of-use.

If Manual Control mode is being used, and the "Always display alerts for new outgoing connections" option is enabled, and one does not tick "Remember this setting", the rule associated with that particular type of connection is only remembered for the current session (after reboot, the rule will no longer be valid/present).

Regardless of what Security Alert and Threat Management mode is enabled, blocked processes will continue to be listed under File -> Settings -> Advanced -> View/Edit Application List), and the user can change any blocked process to Allow, if appropriate.

An on-screen alert will be displayed immediately as potential threats are detected. The alert provides event details and threat management options. Tray Alerts will not be displayed when this option is selected. See Privatefirewall Settings -> Security Alert and Threat Management Options section of this guide for more information about event filtering and alerting).

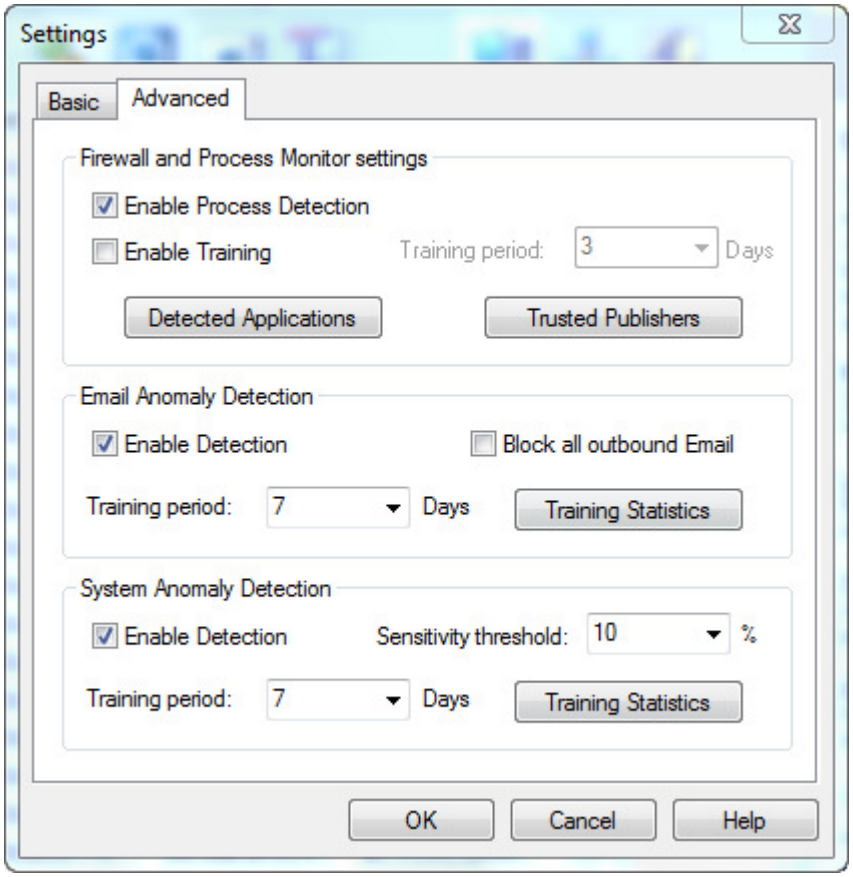
Firewall and Process Monitor settings

After installing Privatefirewall, you may initially observe numerous Application and Process Monitor alerts as Privatefirewall will set rules for all Internet applications and WinAPI Processes as they happen. If you prefer, you can set a 'training' period for these types of alerts so all the rules will be set with no alerts during the training period. When training is completed, the frequency of alerts will be reduced as many rules for commonly used applications and processes will have been set. An on-screen alert will be displayed immediately as potential threats are detected. The alert provides event details and threat management options. Tray Alerts will not be displayed when this option is selected.

Note: Training mode is never required, but can be enabled to reduce the number of alerts generated, when, for example, you are installing a new software program. During Training, only Applications/Processes that fail signature validation ***and attempt to send/receive packets via the Internet*** will generate an alert, and be blocked by default if not Allowed by user prior to the alert time-out (30 seconds), or by selecting the Allow button in the Full alert.

Advanced Settings

The Advanced Tab of the Settings dialog enables you to enable or disable Process detection, System and Email Anomaly Detection and/or training, specify training duration and sensitivity thresholds and review and manage Detected Applications and Trusted Publishers.



Email Anomaly Detection

This feature tracks outbound Email delivery behavior and provides alerts if there is unusual activity. The Email Anomaly Detection Engine is based on the specific behavior of each computer's email activity over a period of time called the 'Training Period'. This can be set to 7 (default), 14, or 28 days within the Settings Menu. In order to initiate training, the 'Enable Detection' checkbox must be selected. The Anomaly Detection Engine will start immediately after the end of the training period. You can also view the training statistics during or after the training period.

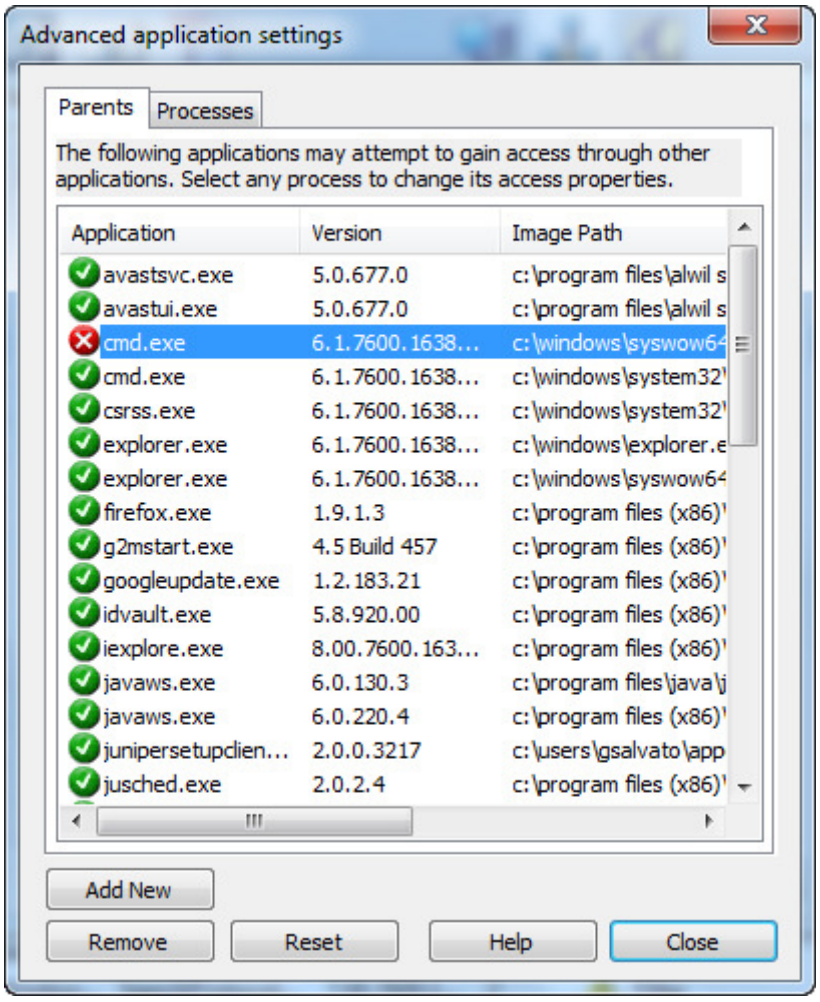
Note: Privatefirewall profiles outgoing email via the default SMTP ports - 25 or 465. If your SMTP server is configured to use a port other than 25 or 465, the email anomaly detection feature will not function.

System Anomaly Detection

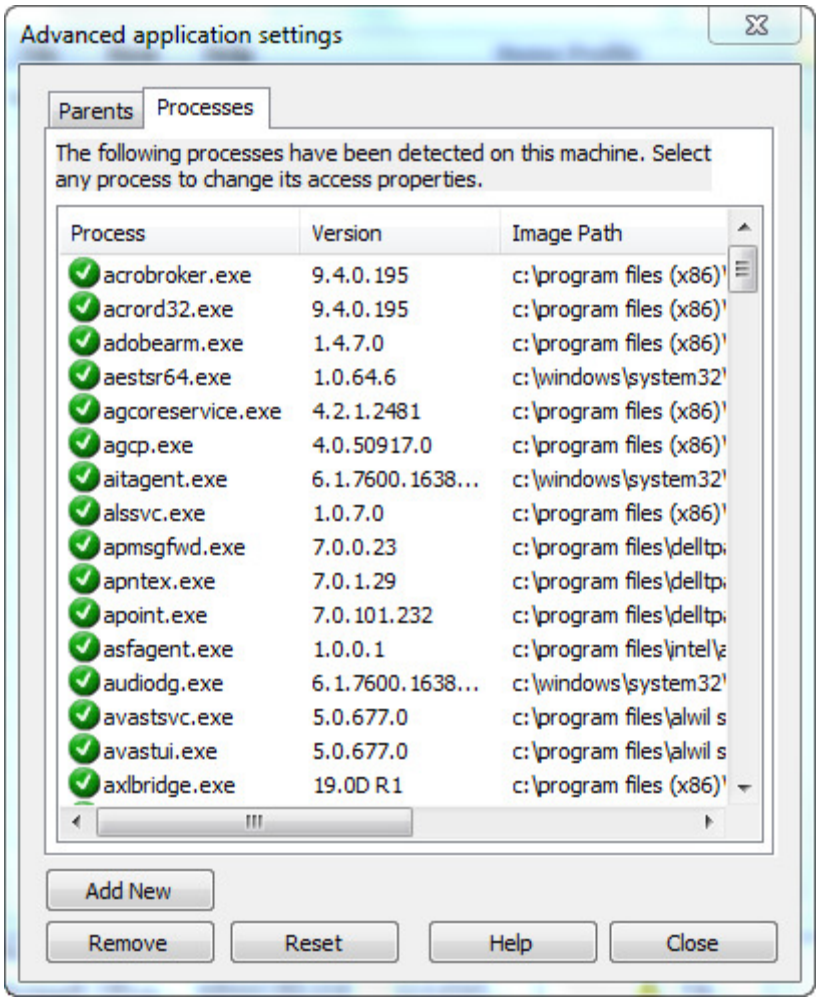
This feature analyzes the normal use patterns of running applications and generates alerts as it detects unusual activity. The System Anomaly Detection Engine applies a sophisticated algorithm to establish a baseline of normal use based on several system variables such as CPU utilization, thread count, and others. These variables are monitored over a specific period of time, called the 'Training Period', which can be set to 7 (default), 14, or 28 days within the Main Menu. The 'Enable Detection' checkbox must be selected for Training to be active. Upon installation, Training is enabled by default and commences immediately upon installation.

Detected Applications

Click the Detected Applications button to invoke the **Parents** screen. All applications that have attempted to access the Internet or network through another trusted application are listed here. The Application Name, Version Number, and Image path are listed, and each application in the list can be set to Allow or Deny access.

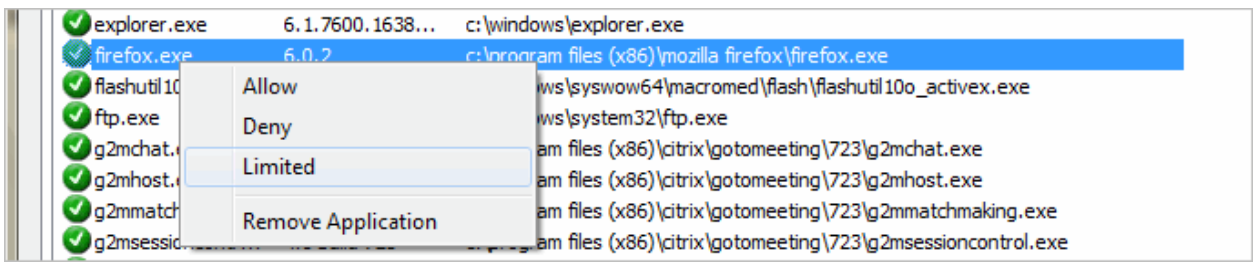


The **Processes** screen lists commonly used processes and provides an alert when an unknown process attempts to launch. The Process Name, Version Name, and Image path are listed, and each application in the list can be set to Allow or Deny access.



Managing Process Rights

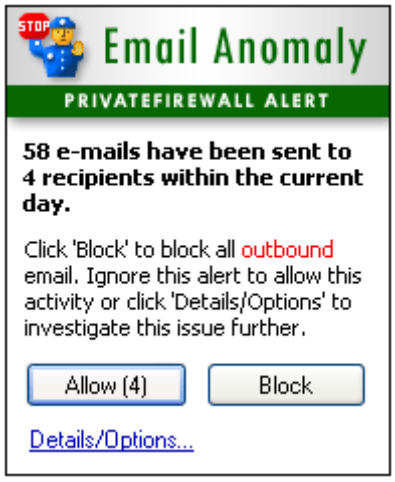
Processes can be run with Reduced rights directly via a relevant tray or full alert, but can also be managed via the Processes tab of the Advanced Applications Settings. Simply highlight a Process and apply the right mouse click to Allow, Deny, Remove or run with Limited Rights.



Email Anomaly Detection

Email Anomaly Detection Alerts

There are several different alerts that may be displayed based on the type and amount of emails delivered within a certain period of time. If there is an alert and the nature of the unusual email activity is unknown, it may be prudent to select the 'Block delivery' checkbox within the alerts to make sure there are no worms or viruses causing the activity. Once the nature of the activity has been determined to be safe, the 'Block all outbound Email' option should be deselected from the settings menu or from the Menu Toolbar.

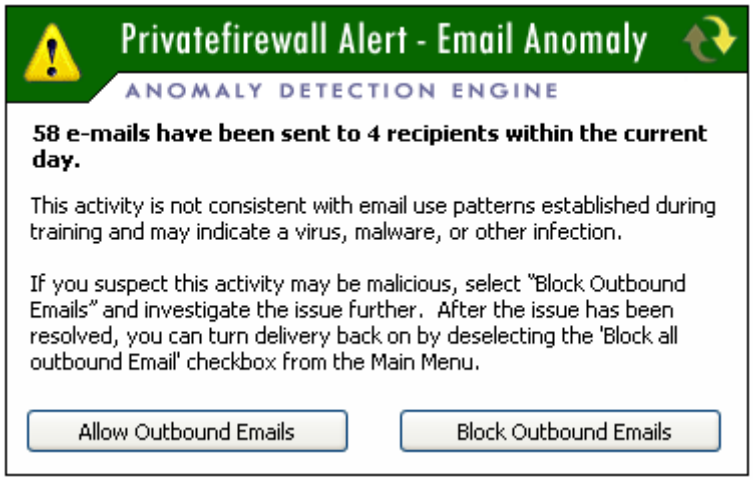


Allow Delivery 

Block Delivery 

NOTE: Privatefirewall will display the Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Allowed.

Click 'Details/Options' in the Tray Alert to display an expanded alert, which contains more detailed information.

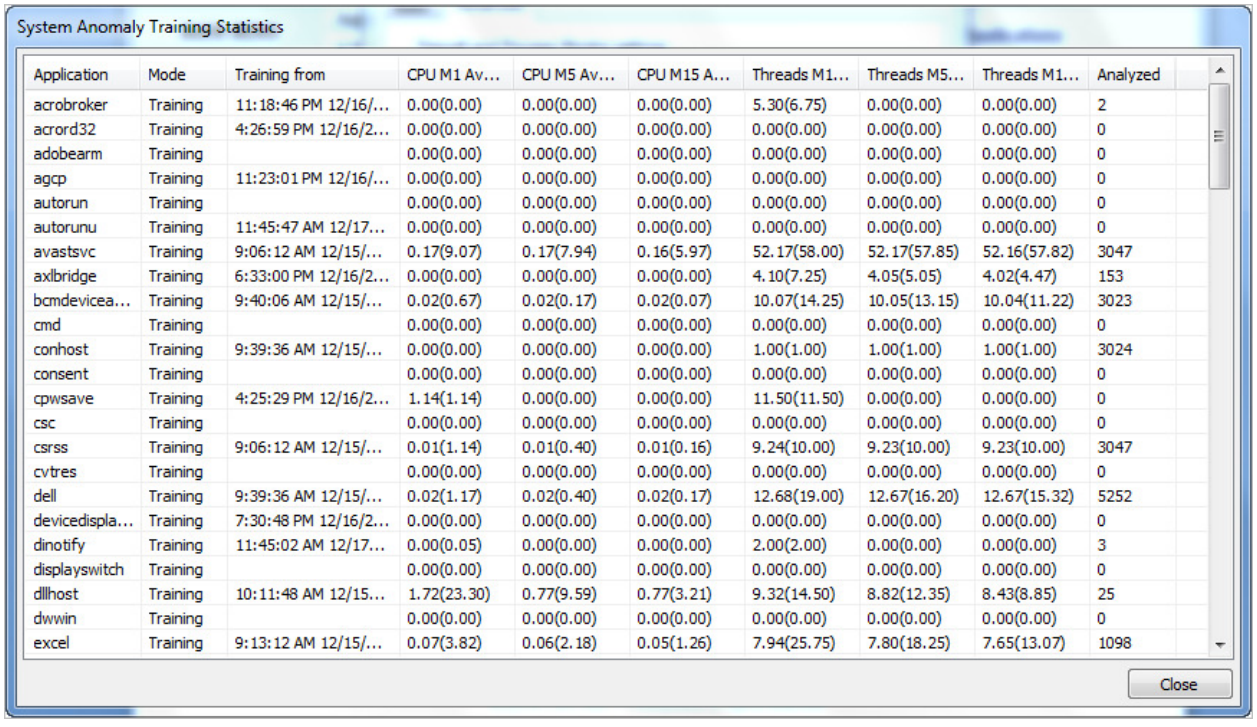


Note: Privatefirewall tracks outgoing, unencrypted email via default SMTP ports - 25 or 465 only. The email anomaly detection feature requires use of one of these ports and that email is not transmitted unencrypted.

System Anomaly Detection

The System Anomaly Detection layer analyzes the normal use patterns of running applications and generates alerts as it detects unusual activity. The System Anomaly Detection Engine applies a sophisticated algorithm to establish a baseline of normal use based on several system variables such as CPU utilization, thread count, and others. These variables are monitored over a specific period of time, called the 'Training Period', which can be set to 7 (default), 14, or 28 days within the Main Menu. The 'Enable Detection' checkbox must be selected for Training to be active. Upon installation, Training is enabled by default and commences immediately upon installation.

Sensitivity Threshold: The Privatefirewall System Anomaly Detection layer generates alerts as it detects system activity that deviates from normal. The sensitivity with which Privatefirewall applies to system anomaly detection can be tuned by adjusting the Sensitivity Threshold. Decreasing the threshold increases the sensitivity, meaning that smaller deviations will generate alerts. Increasing the threshold will allow greater variance from normal activity. The default System Anomaly Detection Sensitivity Threshold is set to 60%, meaning any activity deviating more than 60% from normal will generate an alert.

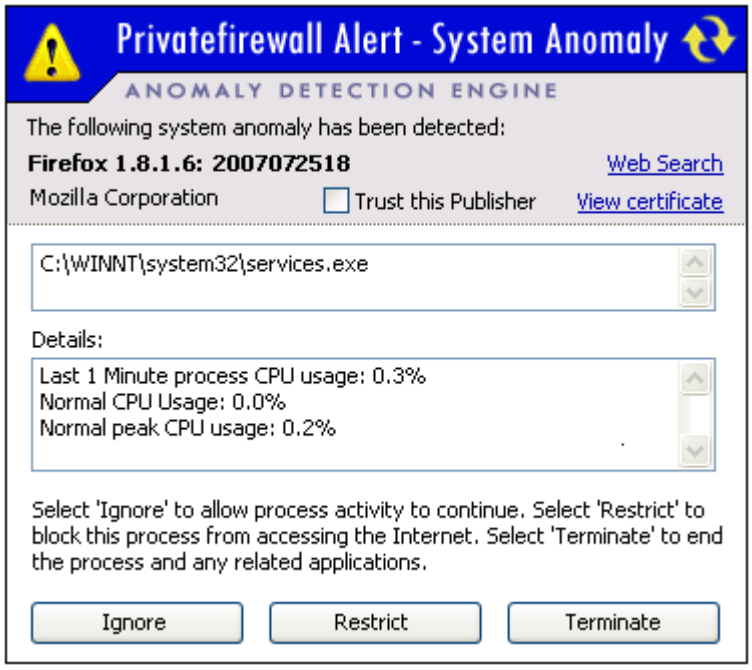


Application	Mode	Training from	CPU M1 Av...	CPU M5 Av...	CPU M15 A...	Threads M1...	Threads M5...	Threads M1...	Analyzed
acrobroker	Training	11:18:46 PM 12/16/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	5.30(6.75)	0.00(0.00)	0.00(0.00)	2
acrord32	Training	4:26:59 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
adobearm	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
agcp	Training	11:23:01 PM 12/16/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
autorun	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
autorunu	Training	11:45:47 AM 12/17...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
avastsvc	Training	9:06:12 AM 12/15/...	0.17(9.07)	0.17(7.94)	0.16(5.97)	52.17(58.00)	52.17(57.85)	52.16(57.82)	3047
axlbridge	Training	6:33:00 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	4.10(7.25)	4.05(5.05)	4.02(4.47)	153
bcmdevicea...	Training	9:40:06 AM 12/15/...	0.02(0.67)	0.02(0.17)	0.02(0.07)	10.07(14.25)	10.05(13.15)	10.04(11.22)	3023
cmd	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
conhost	Training	9:39:36 AM 12/15/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	1.00(1.00)	1.00(1.00)	1.00(1.00)	3024
consent	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
cpwsave	Training	4:25:29 PM 12/16/2...	1.14(1.14)	0.00(0.00)	0.00(0.00)	11.50(11.50)	0.00(0.00)	0.00(0.00)	0
csc	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
csrss	Training	9:06:12 AM 12/15/...	0.01(1.14)	0.01(0.40)	0.01(0.16)	9.24(10.00)	9.23(10.00)	9.23(10.00)	3047
cvtres	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dell	Training	9:39:36 AM 12/15/...	0.02(1.17)	0.02(0.40)	0.02(0.17)	12.68(19.00)	12.67(16.20)	12.67(15.32)	5252
devicedispla...	Training	7:30:48 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dinotify	Training	11:45:02 AM 12/17...	0.00(0.05)	0.00(0.00)	0.00(0.00)	2.00(2.00)	0.00(0.00)	0.00(0.00)	3
displayswitch	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dllhost	Training	10:11:48 AM 12/15...	1.72(23.30)	0.77(9.59)	0.77(3.21)	9.32(14.50)	8.82(12.35)	8.43(8.85)	25
dwwin	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
excel	Training	9:13:12 AM 12/15/...	0.07(3.82)	0.06(2.18)	0.05(1.26)	7.94(25.75)	7.80(18.25)	7.65(13.07)	1098

Selecting the Training Statistics button will display the System behavior data collected during training. These may be viewed during or after the Training period.

The Anomaly Detection Engine will start immediately after the end of the training period, and will generate a Tray Alert (see right) whenever there is any activity that is not consistent with system use patterns established during the training period. If there is an alert and the nature of the activity is unknown, it may be prudent to select 'Details/Options' on the Tray Alert to open an expanded alert (see below) and obtain more detailed information about the suspicious activity and additional threat management options.

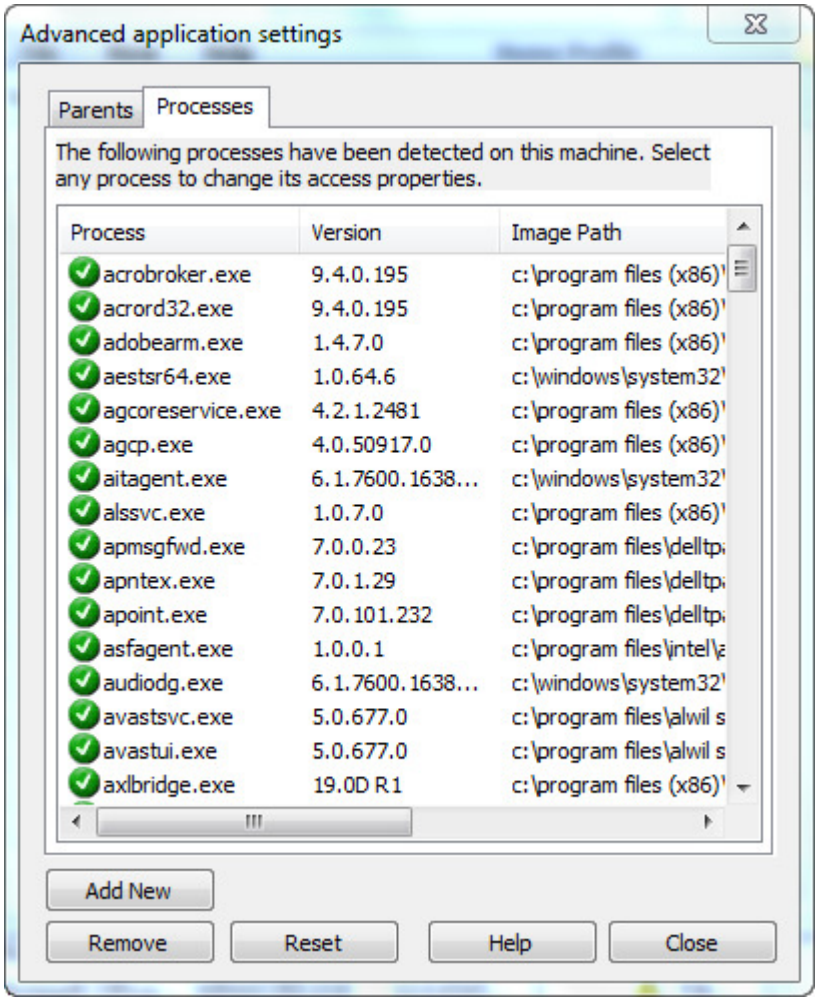
NOTE: Privatefirewall will display a Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Allowed.



If the 'Web Search' link is selected, a search containing the executable filename ('services.exe' in the alert below) will be performed in your default browser.

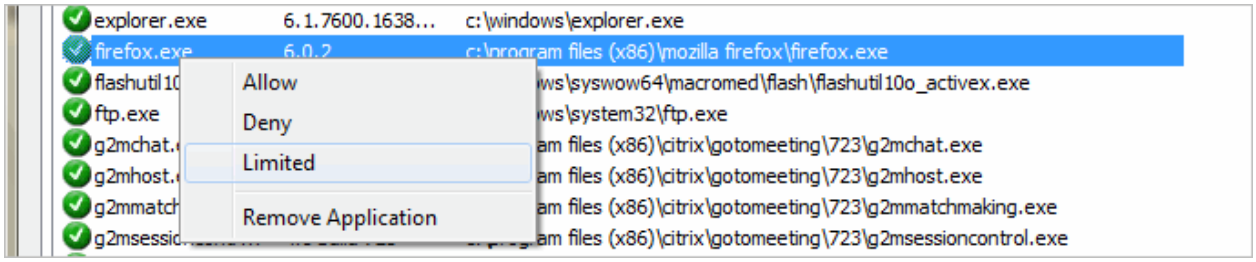
Process Detection

This feature records all processes that are launched during the 'Training Period', which can be set to 1, 3, or 7 days (please refer to Advanced Settings section). Training is enabled by default and commences for a ten minute period immediately upon installation. Extended training periods of 1, 3, 7 or 14 days can be specified as needed. Listed processes can be viewed at any time by selecting the 'Processes' Tab within the Advanced Applications Settings window.

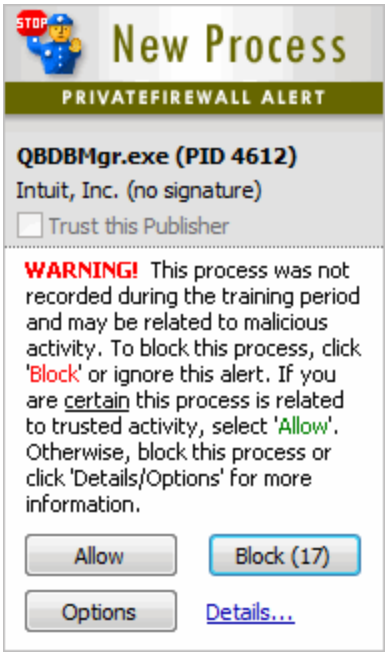


Managing Process Rights

Processes can be run with Reduced rights directly via a relevant tray or full alert, but can also be managed via the Processes tab of the Advanced Applications Settings. Simply highlight a Process and apply the right mouse click to Allow, Deny, Remove or run with Limited Rights.

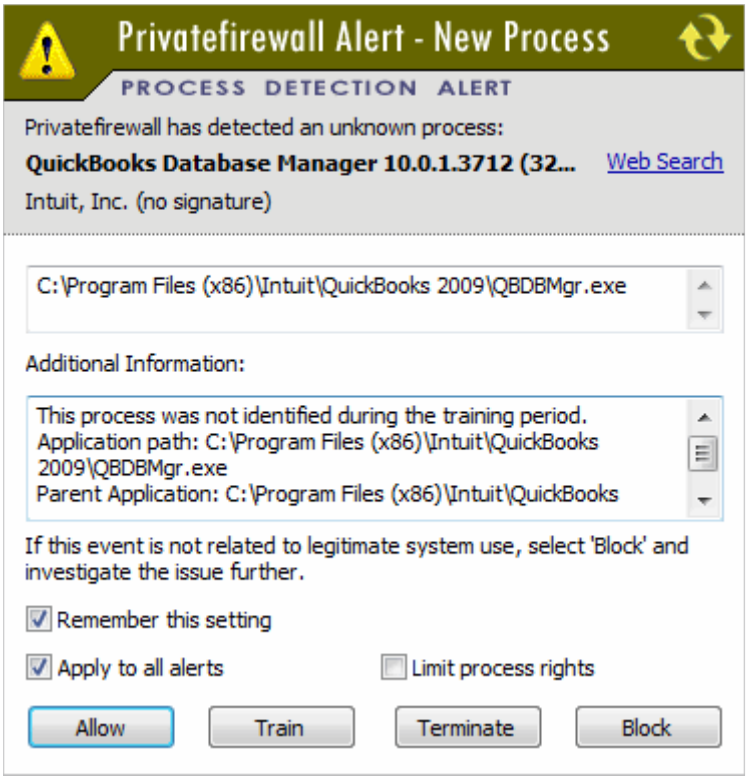


After the training period, Privatefirewall will generate a Tray Alert (see right) when any process attempts to run that was not recorded during the training period. If the process is related to known/trusted activity, the process should be allowed and will then be added to the trusted process list.



Click 'Details…' in the Tray Alert to display an expanded alert (see below), which contains more detailed information about the suspicious activity and additional threat management options. If the 'Require user approval for each alert' box is checked in the Basic Tab of the Settings Menu, an expanded alert will appear automatically and no Tray Alerts will be displayed. If the 'Web Search' link is selected, a search containing the executable filename will be invoked in your default browser.

NOTE: Privatefirewall will display a Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.



In Manual Control mode, with "Always display alerts for outgoing connections" enabled, and **Remember this setting** un-checked, the rule associated with that particular type of connection is only remembered for the current session (after reboot, the rule will no longer be valid/present).

Checking **Apply to all alerts** will eliminate the display of additional Process Monitor alerts for this application by treating subsequent activity based on the same response to the initial alert.

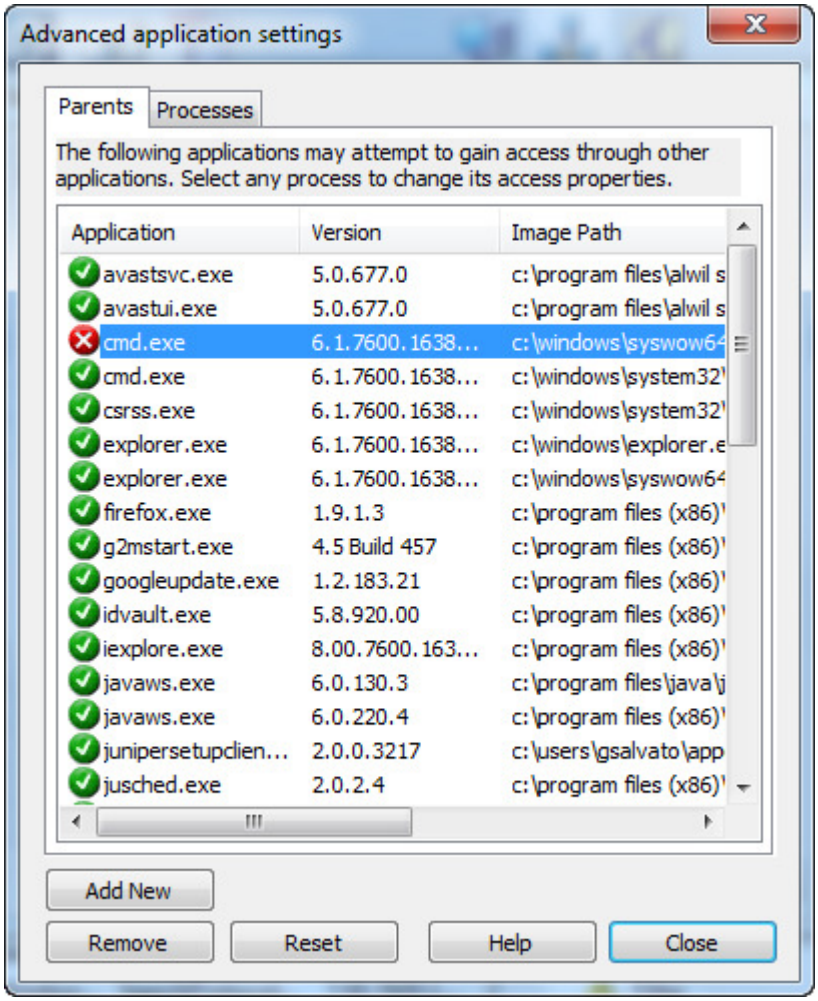
Checking **Limit process rights** enables the process to run with reduced rights (setting can be modified via right-mouse function on Processes tab of Advanced Application settings).

If a process attempts to load that was previously ignored or blocked, Privatefirewall will generate an alert with the choice of allowing or blocking the previously blocked activity.

Advanced Application Settings

(Accessed from File/Settings/Advanced application settings)

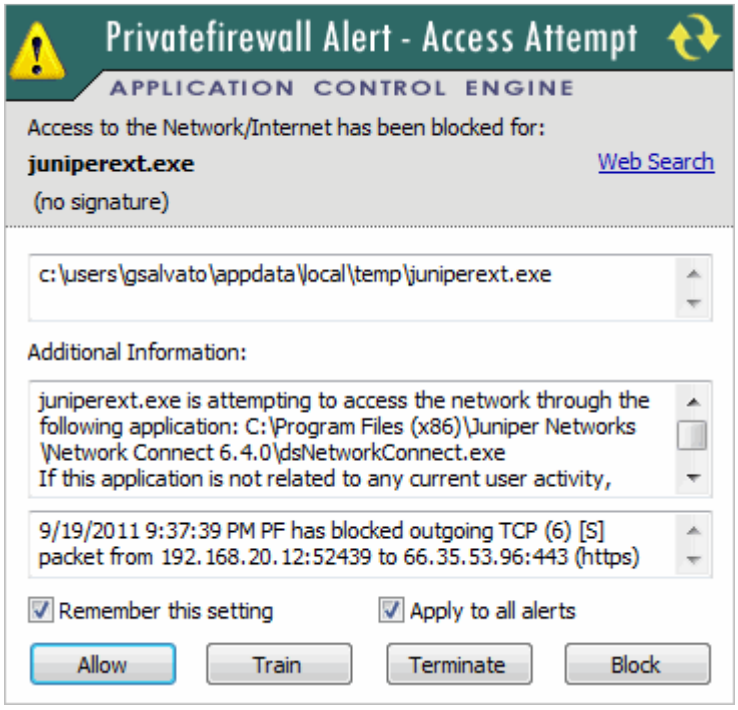
Some applications allow other applications to control their actions, which means that the 'primary' application may be protected, but the 'secondary' or Parent application may be permitted to access the Internet *through* the primary application. The Advanced Applications settings screen lists these 'secondary' Parent applications that have attempted to access the Internet or network through a 'primary' trusted application. Each application in the list can be set to Allow or Block Access.



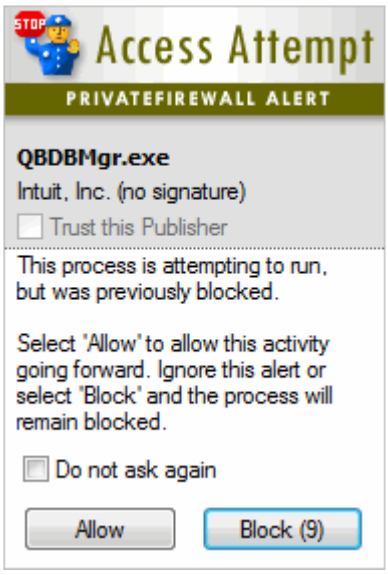
While this is a method commonly used by hackers to attempt to gain unauthorized access, it is also a function of many 'trusted' applications operating normally when accessing the Internet. If you are in the process of accessing the Internet with an application, the 'secondary' or Parent application names may not be common or recognizable, so it may be difficult to determine if the activity is normal or malicious. If you receive an alert and the application listed is related to any form of current activity, it is most likely not malicious activity. However, if it is unrelated (ex: is the application referenced is not even open, etc.), it may be an unauthorized intrusion attempt and the 'Block' button should be selected so the issue can be investigated.

NOTE: Privatefirewall will display the Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

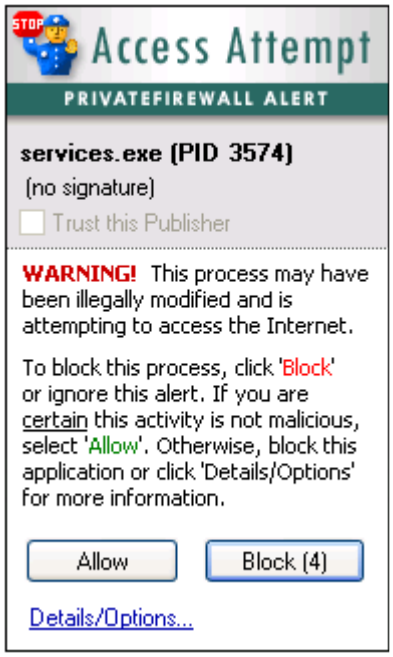
Click 'Details/Options' in the Tray Alert to display an expanded alert, which contains more detailed information about the suspicious activity and additional threat management options This alert lists the program name, version number, date, time, and incoming/outgoing IP address, and the Parent application which was attempting to be used. It will also specify whether the Traffic is inbound or outbound. If the 'Web Search' link is selected, a search containing the executable filename will be performed in your default browser.



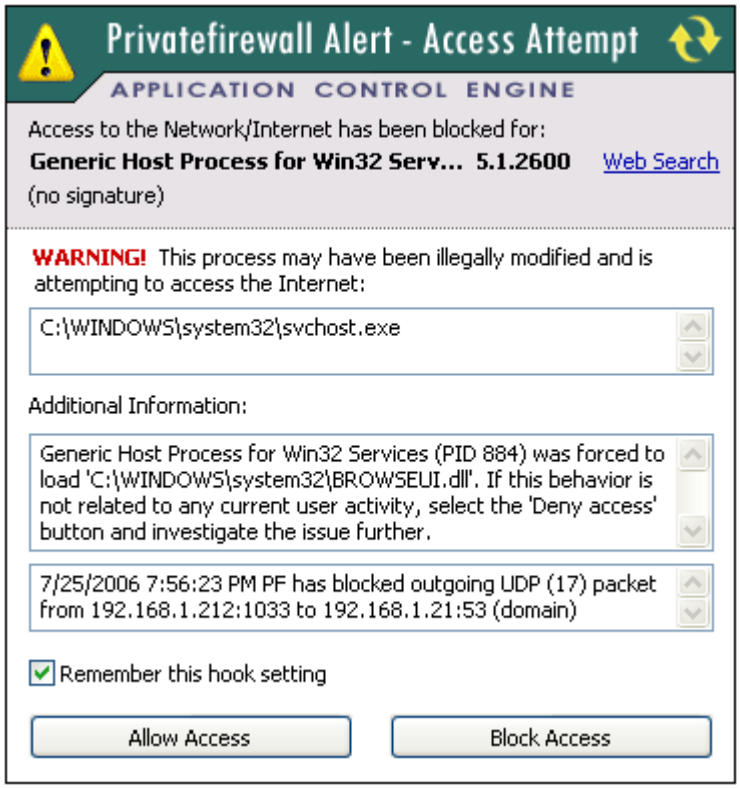
If an application attempts to load that was previously ignored or blocked, Privatefirewall will generate the following alert.



Another type of potential attack is when a process is illegally modified or launched and attempts to access the Internet using that process. This will generate a different alert (see right). If you receive this alert, proceed with caution and carefully investigate the issue to ensure there is no malicious activity.



Click 'Details/Options' in the Tray Alert to display an expanded alert (see below), which contains more detailed information about the suspicious activity and additional threat management options.



Trusted Publisher

(Accessed from File/Settings/Trusted Publisher)

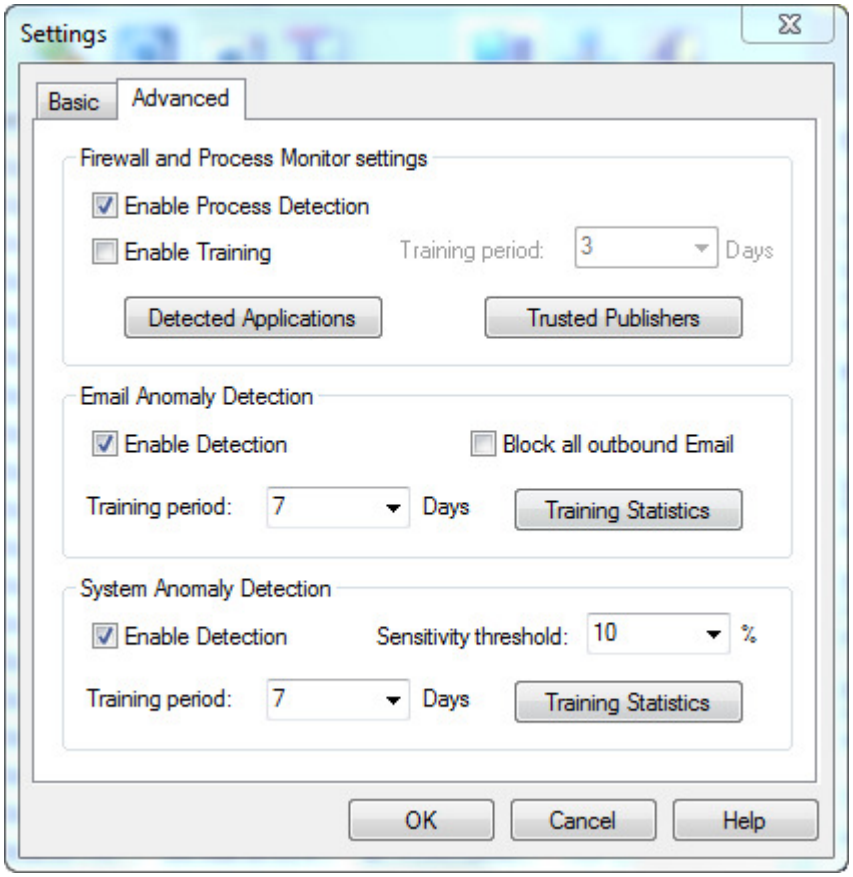
Feature Summary

Privatefirewall employs a combination of conventional and progressive technologies (firewall, process monitor, system and application behavioral profiling and anomaly detection, etc.) to deliver the highest possible levels of security for individual and corporate PCs. To enhance security and ease-of-use, Privatefirewall provides an ability to designate (white list) software from trusted publishers – those that have been pre-approved and/or where the digital signature of the software has been automatically verified by Privatefirewall.

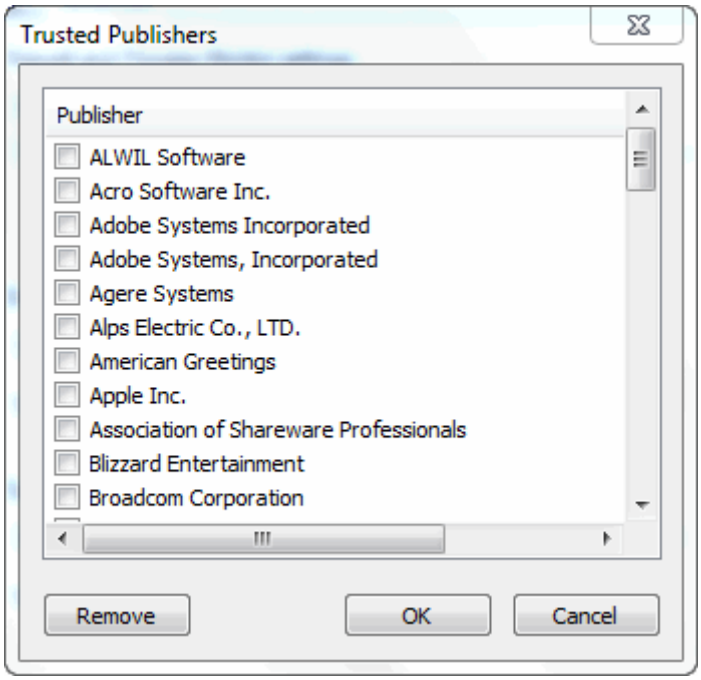
Privatefirewall Trusted Publisher includes a list of pre-approved vendors of popular security, productivity and other general desktop applications, but primarily performs its white-listing function using dynamic verification as new applications are run for the first time. Once a software publisher (vendor) has been added to the list, Privatefirewall will allow (not alert or block) any program associated with the software publisher's verified Certificate.

Accessing Trusted Publisher

To access the Trusted Publisher feature, click **File** > **Settings** and select the **Advanced Tab**. Click the **Trusted Publishers** button on the bottom the screen.



The Trusted Publishers dialog displays the list of software publishers (default of added after installation) for which Certificates have been pre-verified. One or multiple Publishers may be removed from the list by selecting the appropriate checkbox and clicking the **Remove** button.



Disabling Trusted Publisher

The Trusted Publisher feature can be disabled. To do so, click **File** > **Settings** and uncheck the button labeled **Disable Trusted Publisher feature** on the **Basic Tab.**

How Trusted Publisher Works

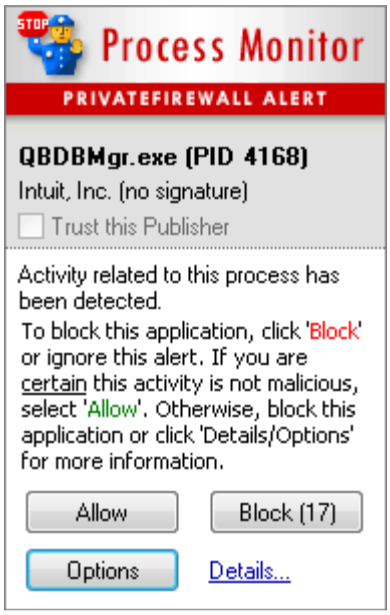
With the exception of email anomaly activity, Privatefirewall will suppress alerts of any type for software publishers that have been added (by default or during use) to the list of Trusted Publishers. This section will describe how Privatefirewall delivers this functionality via its Trusted Publisher feature.

Tray Alerts

When Privatefirewall detects activity (application Internet access, new process detected, etc.), one or more types of alerts are generated. If Privatefirewall is able to verify the software publisher's Certificate and Signature related to the application that has caused the Privatefirewall alert, the Trust this Publisher feature will be "active", meaning that the checkbox to the left of **Trust this Publisher** text will be enabled (as shown in the examples below).

Via the tray alert, the end-user can review basic information regarding the event that triggered the alert, and check the Trust this Publisher checkbox if they are certain that the activity is legitimate and that the software publisher should be trusted thereafter. With the exception of email anomaly detection alerts, Privatefirewall will suppress alerts of any type for software vendors included on the list of Trusted Publishers.

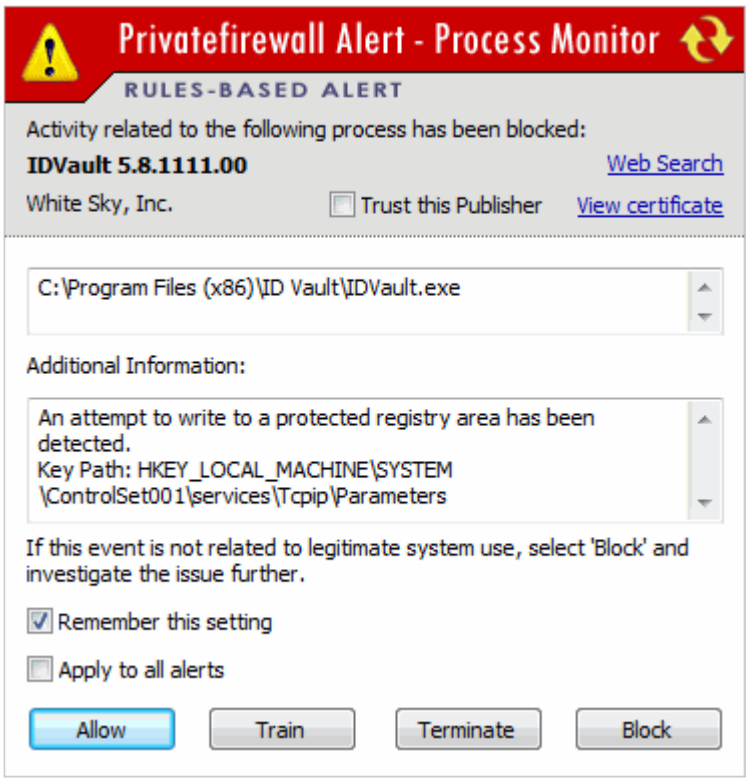
More information about the event can be viewed by clicking the **Details/Options** link on the bottom left corner of the tray alert which invokes the Expanded Alert. Refer to the **Expanded Alerts** of this guide for more information.

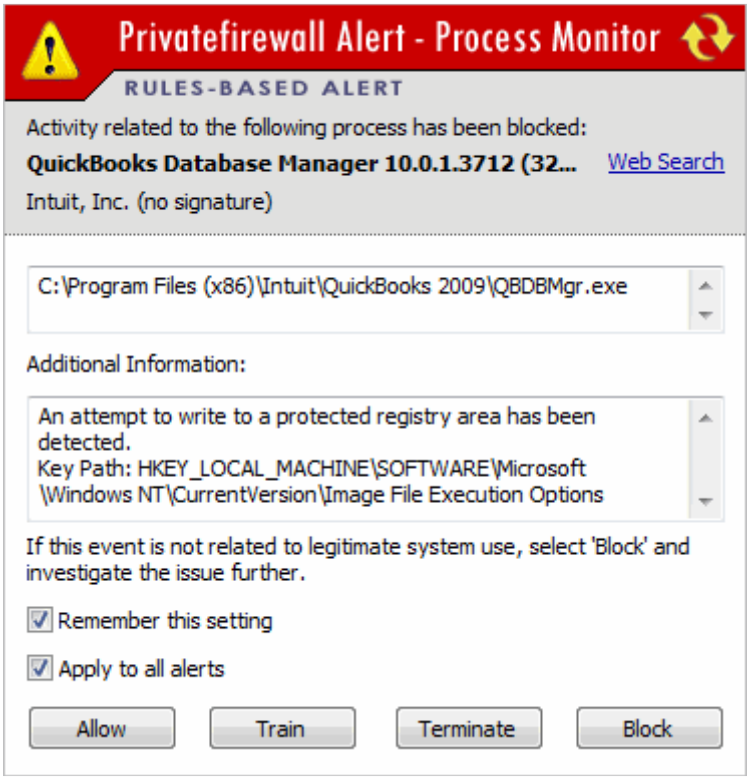


If Privatefirewall is unable to verify the Publisher's Certificate or able to detect a Publisher's Certificate, but unable to verify that the application has been signed, the Trust this Publisher checkbox is disabled (grayed out).

Expanded Alerts

Clicking the Details/Options link on the bottom left corner of the tray alert, will invoke an expanded alert, as shown in this example (right). The Expanded Alert offers more information regarding the suspicious activity and the ability to conduct a **Web Search** to learn more about the process or application and view the software publisher's certificate (**View certificate**).





If Privatefirewall is unable to verify the software publisher's certificate, the Expanded Alert will provide additional information and details regarding the alert, as well as the ability to perform a Web Search, but will not include a link to view the software publisher's certificate.

Web Search

As the name implies, clicking on the Web Search link in the Expanded Alert will invoke a search of the Internet via the computer's default browser for the process, application or other event subject related to the alert. This capability makes it easy to acquire a clear understanding of events that may be unfamiliar to you. Performing a quick Web search will often reveal whether the process or application is malicious and should be blocked or related to a legitimate aspect of your computing environment and use.

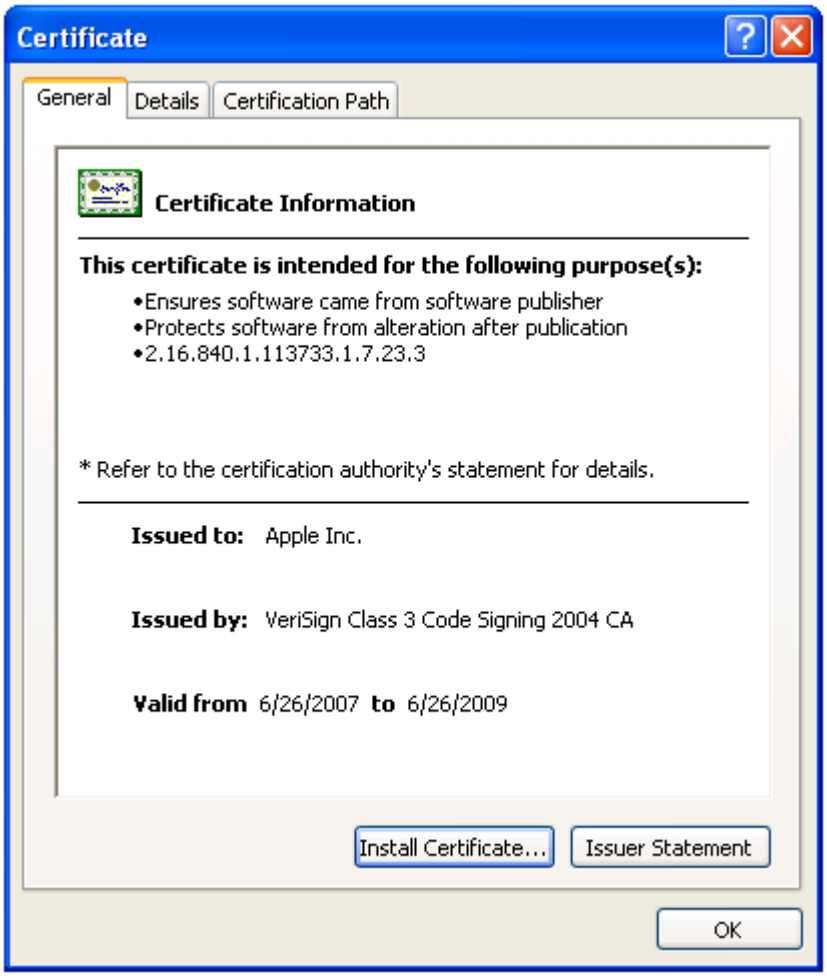
View Certificate

It may be helpful and informative to view the details of the software publisher's certificate before making the determination that the publisher should be added to the Trusted Publisher list. Simply click the **View certificate** link on the Expanded Alert to invoke the dialog that contains the Certificate's details.

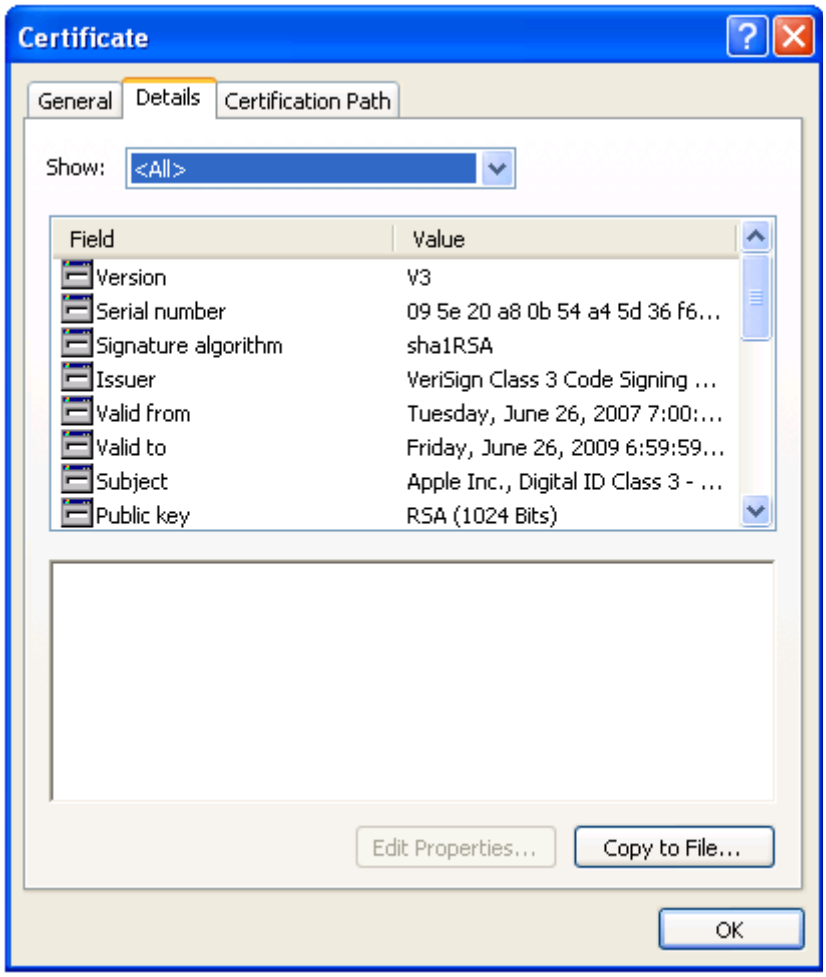
The **General** tab displays a variety of information pertaining to the Certificate including the certificate purpose, Issuer, and the date range for which the certificate is valid.

The Certificate may be imported by selecting the **Install Certificate** button which will launch the Certificate Import Wizard.

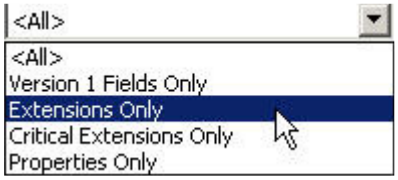
The Certificate Issuer Statement may be viewed by clicking the **Issuer Statement** button.



The **Details** Tab provides the specifics regarding the Certificate such as Public Key, Signature Algorithm, Serial Number and other certificate attributes.

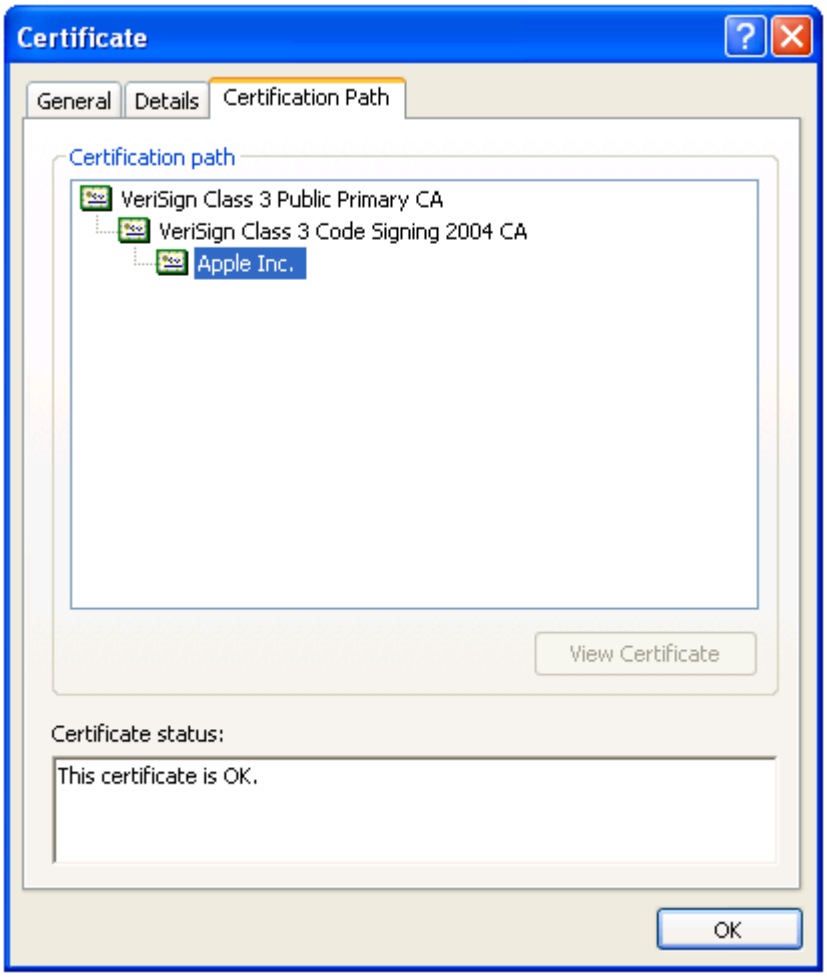


The Details view can be filtered by clicking the drop-down arrow and specifying the certificate details that you would like to display.



The certificate detail information may be copied to a file for future reference by selecting the **Copy to File** button. The **Edit Properties** button is not enabled.

The **Certificate Path** Tab displays the certificate path. A path starts with the Subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted Certification Authority (CA).



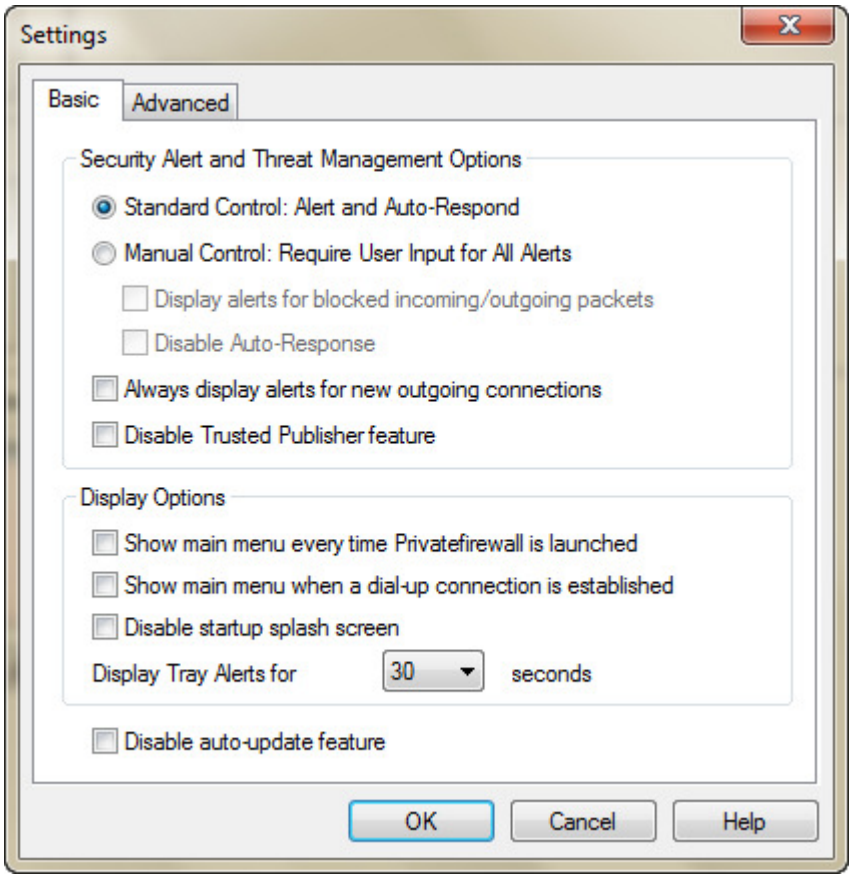
Menus and Toolbars

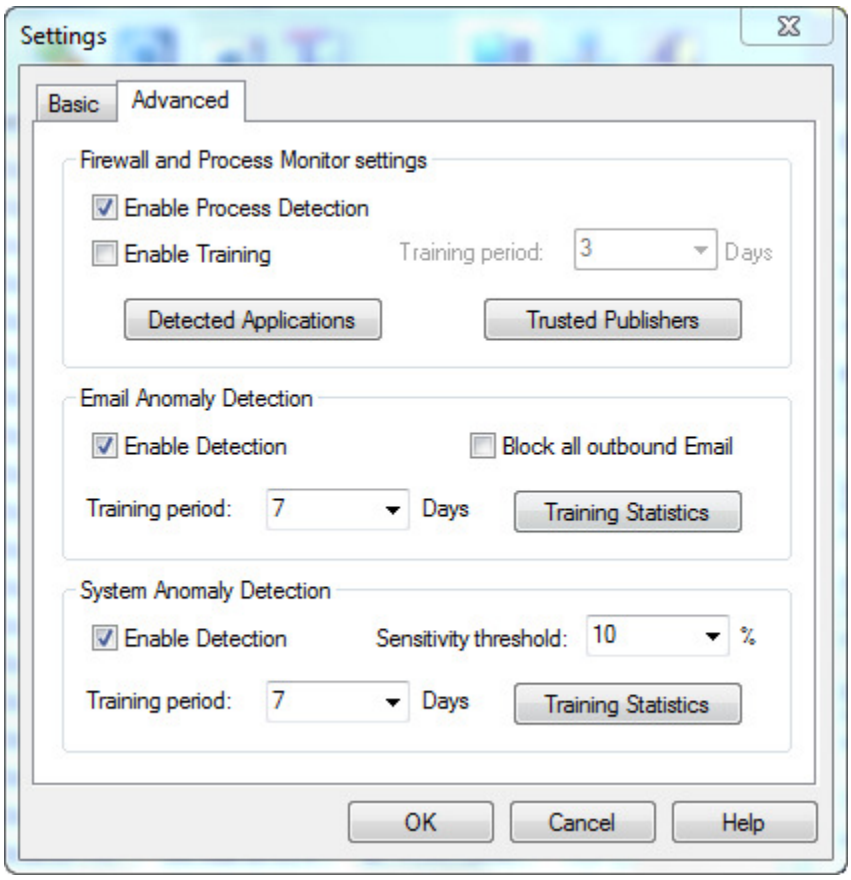
Program Menus

File/Settings Menu

(This menu can be accessed by selecting 'File/Settings' from the Main Menu)

The settings section allows the adjustment of menu/alert display, Firewall settings, and Advanced application and Anomaly detection settings.





Import/Export Settings
(This feature can be invoked by selecting 'File/Import or Export Settings' from the Main Menu)

Privatefirewall custom settings and rules can be imported or exported between systems with the same configuration (same installation application path, including system application).

The settings that will be exported to an .xml file (PF-Settings.xml) include:
- Common firewall and PM settings (mode, rules, etc)
- Profile settings (trusted/untrusted lists, mode, rules, etc.)
- Allowed Parent list
- IPC rules for applications
- Network rules for application.

View Menu
(This menu can be accessed by selecting 'View' from the Main Menu)

Hide Privatefirewall - This option minimizes Privatefirewall so only the tray icon is displayed.

HTML Port Tracking Report - This report is identical to the Port Tracking Report within the Main Interface, but in HTML Format for easier viewing. The report can also be saved/viewed

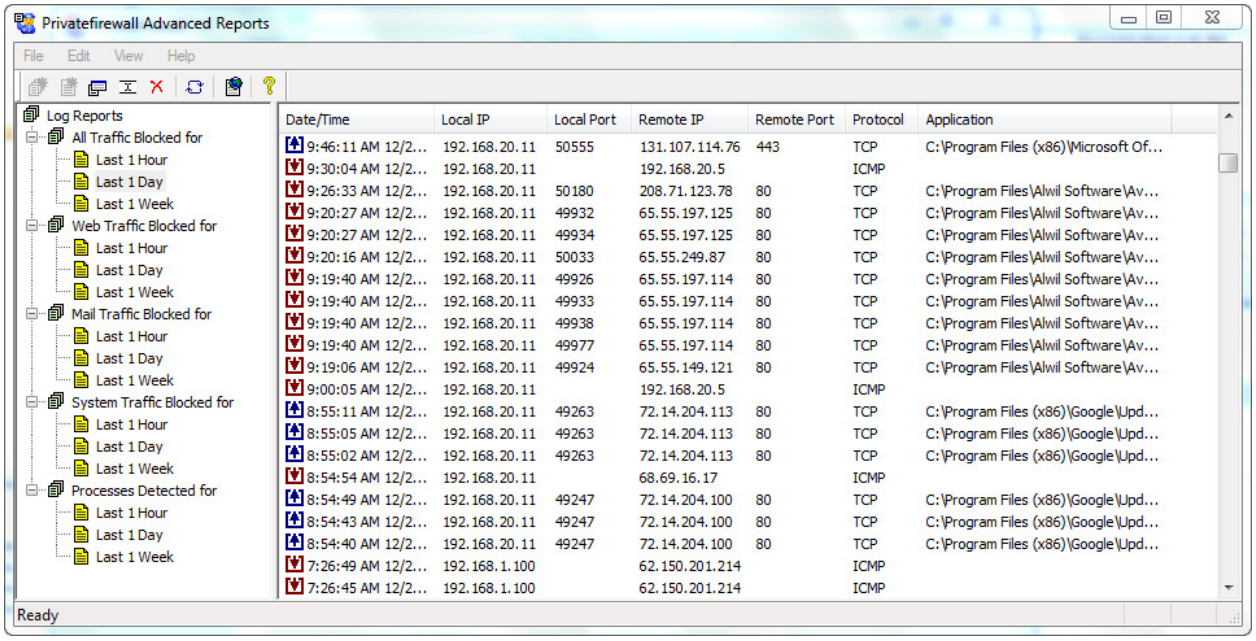
in the *.txt format by right clicking anywhere within the Port Tracking Report from the main interface and selecting the 'Save Report As..' option.

HTML Firewall Log - This report is identical to the Firewall Log within the Main Interface, but in HTML Format for easier viewing. The report can also be saved/viewed in the *.txt format by right clicking anywhere within the Firewall Log from the main interface and selecting the 'Save Report As..' option.

Advanced Reports - Firewall log records can be sorted by type and time of occurrence within Privatefirewall Advanced Reports. Reports can be sorted by Web, Mail, or System access attempts. Each of these reports can also be sorted going back 1 Hour, 1 Day, or 1 Week.

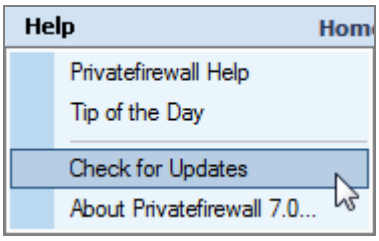
Privatefirewall Advanced Reports lists the following:

Time/Date - When the packet was detected.
Local IP (Internet address) - The Internet address from which the packing is coming from.
Local Port - The port from the local computer involved in the access attempt.
Remote IP - The Internet address to which the packet is traveling.
Remote Port - The port from the remote computer involved in the access attempt.
Protocol - The Network Protocol, or type of network connection used to send the packet.
Application (if applicable) **-** The name of the application to which the packet was attempting to be sent (if any).



Help Menu

(This menu can be accessed by selecting 'Help' from the Main Menu)



The Privatefirewall Help menu offers several informational and functional options.

- Privatefirewall Help: Selecting this option will launch the integrated Privatefirewall User Guide.

- Tip of the Day: Selecting this option will display a description for a Privatefirewall feature that you may not have been aware of.

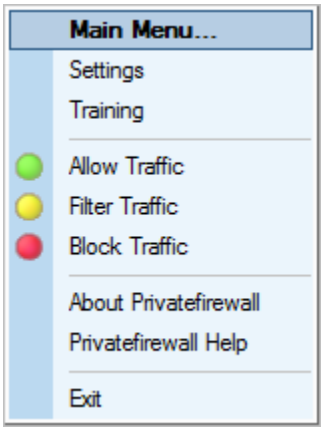
- Check for Updates: This option will allow you to verify that the version of Privatefirewall currently installed on your system is up to date and download any newer builds that may be available. Note: Privatefirewall automatically performs version-check every 24 hours and upon system restart and will display an on-screen notification when a newer version that the one installed is available for download. This feature was added in version 7.0.24.10 (posted July 18, 2011).

- About Privatefirewall: Selecting this option will display the version number of the Privatefirewall build currently installed on your system as well as copyright notice and a link to the Privatefirewall product support page.

Tray Icon Menu

(This menu can be accessed by right-clicking on the Privatefirewall Tray Icon)

Privatefirewall works automatically after installation and the Privatefirewall tray icon should appear in the lower right corner of the Windows Tray. Privatefirewall can also be accessed by right-clicking on the tray icon. A pop-up box appears (see right) and contains the following options: Main Menu, Help, Settings, Training, Allow, Filter, or Deny Internet Traffic, About, and Exit.



Privatefirewall Toolbars

Main Settings Toolbar

Settings – This will display the settings menu, which consists of various Main Manu and alert display options.

Reset Default Settings - This will reset all Security and Application settings to factory defaults. This is useful when application rules have been allowed or blocked in error, etc.

Outbound Email Anomaly Detection - This will allow or block all outbound email based on the information provided by the Email Anomaly Detection feature.

Exit – This will minimize the main Privatefirewall screen display, but will not disable Privatefirewall.

Profile Settings Toolbar

Every Privatefirewall profile can be configured and defined by adjusting the Network, Internet, and IP Security settings within the Main Menu. Click on the appropriate Firewall Profile Icon to modify the rules/settings for that Profile.

Home Profile – This profile is used for home or home-networked environment with no other existing firewall protection. Suggested settings: Internet - HIGH, Network - HIGH for single computer, LOW for home network.

Office Profile – This profile is used within a networked environment where an existing company firewall is present. Suggested settings: Internet - HIGH, Network - LOW; Check with your systems administrator to confirm settings.

Remote Profile – This profile is used when connecting to a company network where there is no firewall protection, or a local network where security is unknown. Suggested settings: Internet - HIGH, Network - HIGH

One example where Privatefirewall's "one-click" adjustment of these profiles may be beneficial is when a computer is used for Home and Office use. At Home, the computer is not likely connected to a network, may not be protected by a hardware-based firewall, and is connected via broadband or dial-up connection. At the office, the computer is connected to the company network which requires that other local users have access, uses a company-wide firewall, and has broadband Internet access. These two scenarios may require Privatefirewall to be configured in two different ways.

Privacyware Privatefirewall

Version 7.0 – User Guide