



Dynamic Security Agent

Version 2.0 – User Guide

Dynamic Security Agent Overview

Privacyware Dynamic Security Agent (DSA) is a security software application that provides Windows desktops and servers with immediate, signature-less protection from known or new malware and all forms of unauthorized use. An intelligent multi-layered application, DSA continuously evaluates applications, system processes, WinAPI calls, registry settings and other system variables to identify, alert, quarantine and block potential threats. DSA features anomaly detection components that baseline normal computer operation and detect unacceptable deviations from typical use.

System Requirements:

Hardware


- 166 MHz Pentium® or faster
- 8 MB RAM
- 5 MB of free disk space

Software

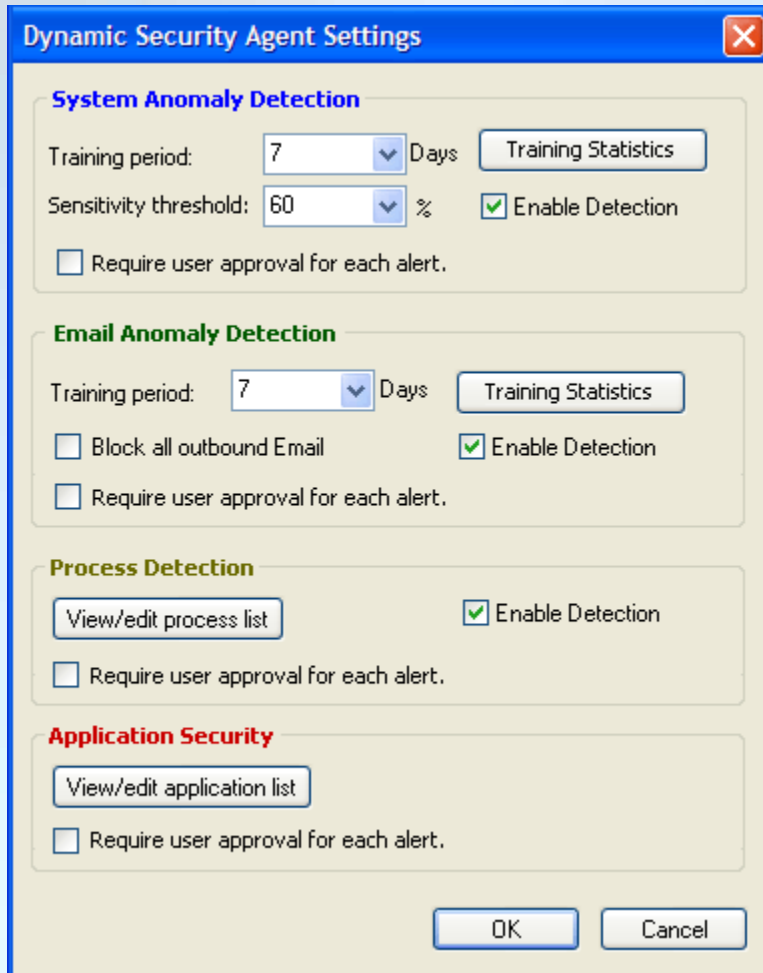
- Operating Systems: Windows® XP (Home, Professional)
Windows® 2000 Professional
Windows® Server 2000, 2003
Windows® Vista (32-bit)

*** You must have administrative privileges to install and operate Dynamic Security Agent.**

*** It is not advisable to attempt remote installation. However, if attempting to install Dynamic Security Agent on a server remotely via Terminal Services, please be advised that DSA may add the Terminal Services application to the quarantine list and you may be unable to access the server once DSA has been installed.**

MAIN MENU (The Main Menu can be accessed by double-clicking the Dynamic Security Agent Windows Desktop Tray Icon )

The DSA Main Menu provides management control over most aspects of the application, including System Anomaly Detection, Email Anomaly Detection, Process Detection, and Application Security.



Dynamic Security Agent Settings

System Anomaly Detection

Training period: 7 Days [Training Statistics](#)

Sensitivity threshold: 60 % Enable Detection

Require user approval for each alert.

Email Anomaly Detection

Training period: 7 Days [Training Statistics](#)

Block all outbound Email Enable Detection

Require user approval for each alert.

Process Detection

[View/edit process list](#) Enable Detection

Require user approval for each alert.

Application Security

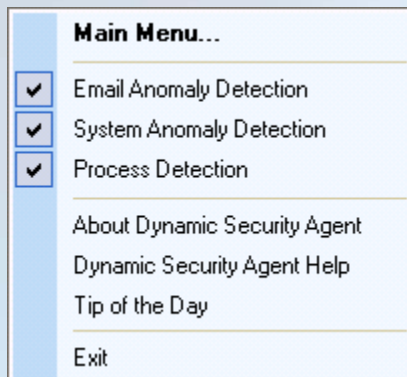
[View/edit application list](#)

Require user approval for each alert.

OK Cancel

Tray Menu

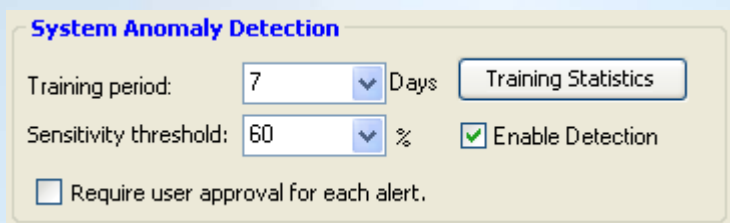
Right-clicking on the Tray Icon will launch the DSA Tray Menu:



From this menu, the System Anomaly, Process Anomaly, or Process Detection functionality can be enabled or disabled by selecting or de-selecting the related check box.

SYSTEM ANOMALY DETECTION

The DSA 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, 14, or 28 days within the Main Menu (the default period is 7 days). The 'Enable Detection' checkbox, must be selected for Training to be active. Upon installation, Training is enabled by default and commences immediately upon installation.



The screenshot shows a configuration window titled "System Anomaly Detection". It contains the following elements:

- Training period:** A dropdown menu set to "7" with the unit "Days" next to it. To the right is a button labeled "Training Statistics".
- Sensitivity threshold:** A dropdown menu set to "60" with the unit "%" next to it. To the right is a checked checkbox labeled "Enable Detection".
- At the bottom, there is an unchecked checkbox labeled "Require user approval for each alert."

User determination regarding each event that generates an alert is required when the "Require User Approval for Each Alert" box is selected. An on-screen alert (see below) 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.

Sensitivity Threshold: The DSA System Anomaly Detection layer generates alerts as it detects system activity that deviates from normal. The sensitivity with which DSA 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. By default, the System Anomaly Detection Sensitivity Threshold is set to 60%. In simple terms, activity deviating more than 60% from normal will generate an alert.

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

System Anomaly Training Statistics									
Application	Mode	Training from	CPU M1 Avg...	CPU M5 Avg...	CPU M15 Avg...	Threads M1...	Threads M5...	Threads M1...	Analyzed
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
csrss	Training	13:25:34 04/24/06	0.06(0.78)	0.06(0.36)	0.04(0.16)	10.00(10.00)	10.00(10.00)	10.00(10.00)	46
drwtsn32	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
dumprep	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
explorer	Training	13:25:34 04/24/06	0.09(1.03)	0.09(0.34)	0.07(0.18)	11.28(13.25)	11.23(12.45)	11.14(11.92)	46
ftp	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
iexplore	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
krnl386	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
lsass	Training	13:25:34 04/24/06	0.02(0.20)	0.02(0.05)	0.01(0.02)	17.73(24.00)	17.48(22.00)	17.22(18.85)	46
msiexec	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
msimn	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
msmsgs	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
pfs	Training	13:25:34 04/24/06	1.16(15.15)	1.13(5.29)	0.80(2.12)	4.13(10.00)	3.93(8.95)	3.59(6.67)	46
rundll32	Training	13:25:34 04/24/06	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
services	Training	13:25:34 04/24/06	0.02(0.49)	0.03(0.15)	0.02(0.06)	16.01(17.75)	16.00(16.35)	16.00(16.12)	46
smss	Training	13:25:34 04/24/06	0.00(0.00)	0.00(0.00)	0.00(0.00)	3.00(3.00)	3.00(3.00)	3.00(3.00)	46
spoolsv	Training	13:25:34 04/24/06	0.02(0.23)	0.02(0.07)	0.01(0.03)	10.65(15.50)	10.48(14.20)	10.22(11.70)	46
svchost	Training	13:25:34 04/24/06	0.03(2.87)	0.03(0.77)	0.03(0.29)	22.12(81.50)	21.95(79.30)	21.62(72.38)	232
taskmgr	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
telnet	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
userinit	Training	13:25:34 04/24/06	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
winlogon	Training	13:25:34 04/24/06	0.02(0.15)	0.02(0.04)	0.02(0.02)	19.63(23.75)	19.51(22.55)	19.31(20.53)	46

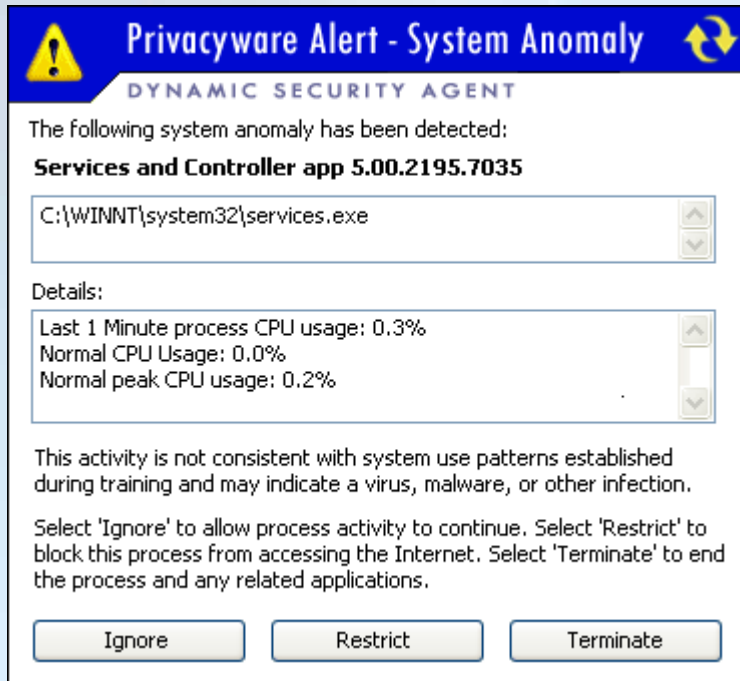
The Anomaly Detection Engine will start immediately after the end of the training period, and will generate an alert whenever there is any activity that is not consistent with system use patterns established during the training period. If there is an alert and the nature of the activity is unknown, it may be prudent to select 'Details/Options' on the tray alert to see more detailed information.



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

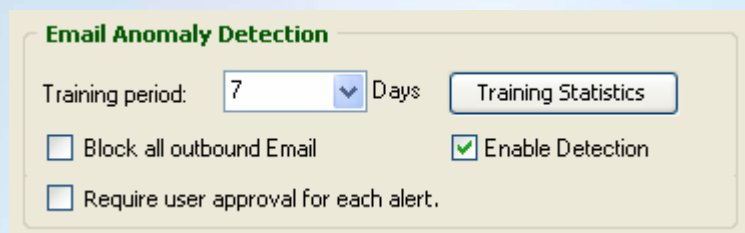
Click 'Details/Options' in the Tray Alert to display an expanded Alert (see below), which contains more detailed information about the suspicious activity and additional threat management options. If the 'Require user approval for each alert' box is checked in the

Main Menu, the 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 ('services.exe' in the alert below) will be performed in your default browser.



EMAIL ANOMALY DETECTION

The DSA Email Anomaly Detection layer analyzes the normal use patterns of outbound email delivery and generates alerts as it detects unusual activity. The Email Anomaly Detection Engine applies a sophisticated algorithm to establish a baseline of normal use based on several email-related variables such as total emails sent and number of email recipients. These variables are monitored over a specific period of time, called the 'Training Period', which can be set to 7, 14, or 28 days within the Main Menu (the default period is 7 days). The 'Enable Detection' checkbox, must be selected for Training to be active. Upon installation, Training is enabled by default and commences immediately upon installation.

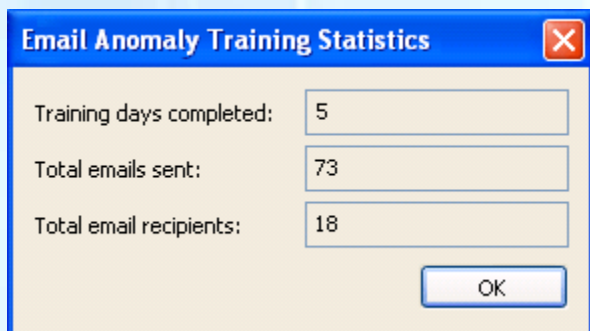


The screenshot shows the 'Email Anomaly Detection' settings panel. It includes a 'Training period' dropdown menu set to '7' days, a 'Training Statistics' button, and three checkboxes: 'Block all outbound Email' (unchecked), 'Require user approval for each alert.' (unchecked), and 'Enable Detection' (checked).

User determination regarding each event that generates an alert is required when the "Require User Approval for Each Alert" box is selected. An on-screen alert (see below) 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.

Selecting the Training Statistics button will display the Email behavior data collected during training. These may be viewed during or after the Training period (see screenshot).

The Block All Outbound Email box can be selected in the event that a worm or virus may have taken control of the computer. Once the threat has been removed, outbound email activity can be resumed by de-selecting this option.

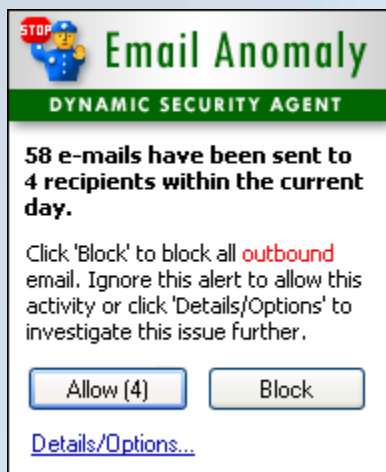


The screenshot shows the 'Email Anomaly Training Statistics' dialog box. It displays the following data:

Category	Value
Training days completed:	5
Total emails sent:	73
Total email recipients:	18

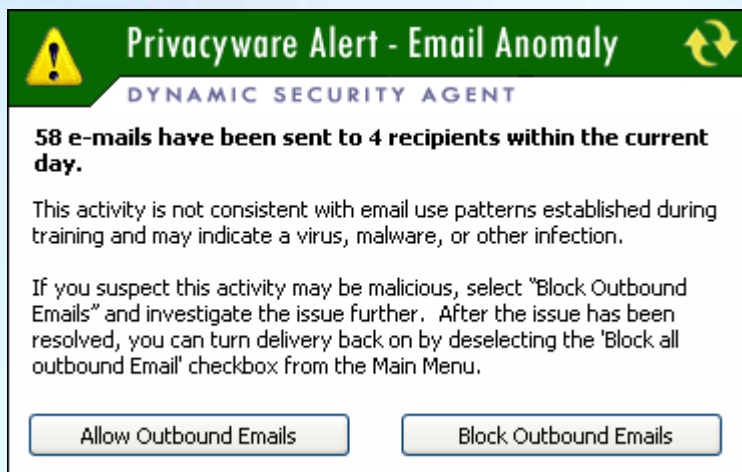
An 'OK' button is located at the bottom right of the dialog box.

After the training period, DSA will generate an alert whenever there is email activity that is not consistent with patterns established during the training period. 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 or suspicious, it may be prudent to select 'Block all outbound e-mail' within the alert and investigate the activity to ensure there are no worms or viruses causing the activity (run virus/spyware or malware scan, etc.). If the activity is determined to be safe, or the threat/infection has been removed, the 'Block all outbound Email' checkbox can then be de-selected from the Main Menu (see above).



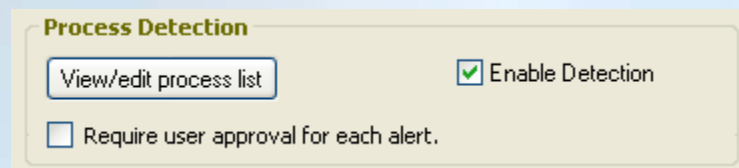
NOTE: DSA will display a Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Allowed.

Click 'Details/Options' in the Tray Alert to display an expanded Alert (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 Main Menu, the expanded Alert will appear automatically and no tray alerts will be displayed.



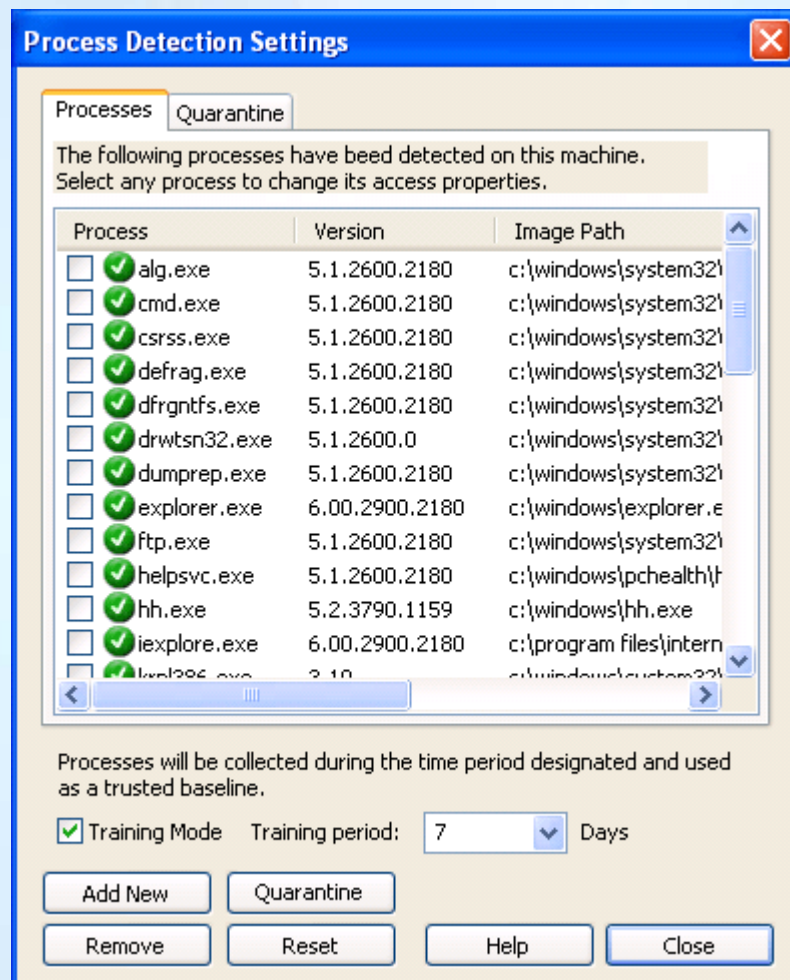
PROCESS DETECTION

The DSA Process Detection feature records all processes that are launched during the 'Training Period', which can be set to 1, 3, or 7 days within the Process Detection Settings 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 for a period of 7 days.



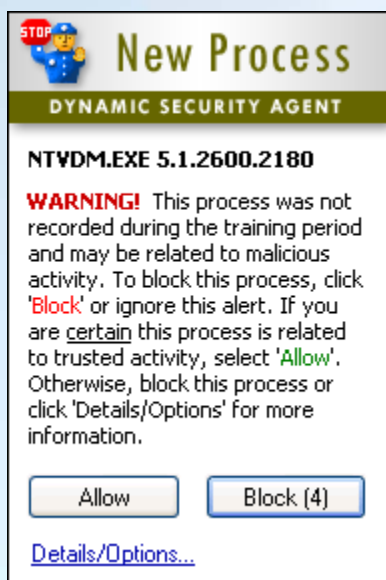
User determination regarding each event that generates an alert is required when the "Require User Approval for Each Alert" box is selected. An on-screen alert (see below) will be displayed immediately as potential threats are detected. The alert provides event details and threat management options. Tray alerts will not be displayed when this option is selected.

The Process Detection functionality will start immediately after the end of the training period. Processes recorded during the training period can be viewed by clicking the 'View/edit process list' button from the Main Menu (see screenshot). These processes will be considered 'trusted' when the training period ends.



Click 'Add New' to manually add a process to the trusted list. Click 'Quarantine' to move a process to the Quarantine list and thereby blocking access to that application. Click 'Remove' to delete a process from the trusted list. Click 'Reset' to revert to DSA default trusted process list.

After the training period, DSA will generate a Tray Alert 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 (see above).

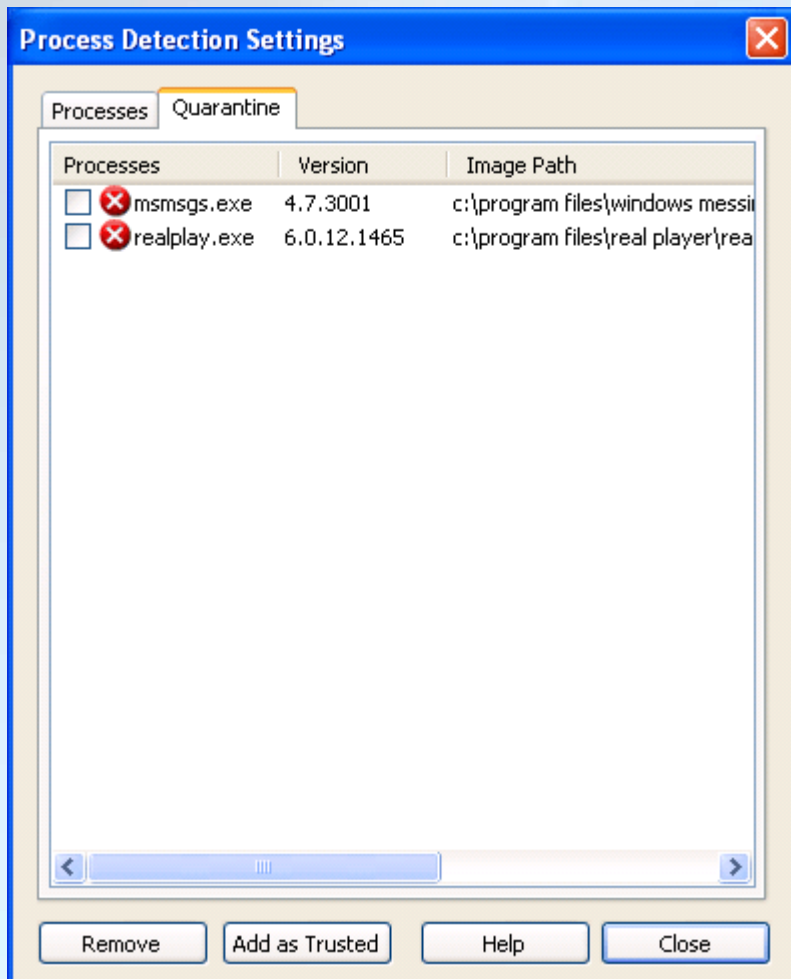


NOTE: DSA will display a Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

Click 'Details/Options' in the Tray Alert to display an expanded Alert (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 Main Menu, the 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 ('ntvdm.exe' in the alert below) will be performed in your default browser.

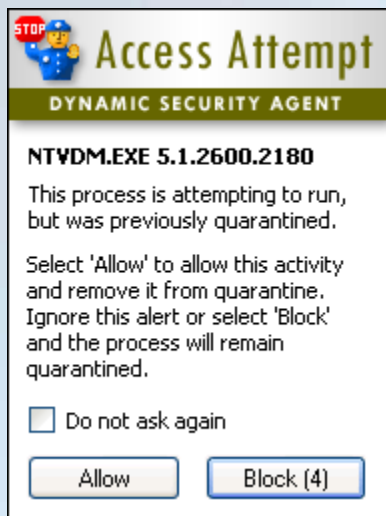


If the process is not related to legitimate system use, select 'Block' and the process will be placed in the Quarantine list.



If it is determined that a Quarantined process should be trusted, check the box next to the process and click 'Add as Trusted'. The process will be removed from Quarantine and added to the Trusted Processes list. The process can also be removed and not added to the trusted list by clicking 'Remove'.

Every time a quarantined process attempts to run, DSA will display the following alert:

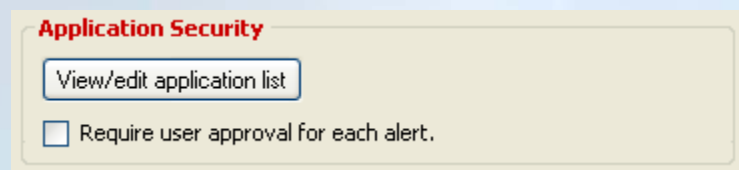


If it is determined that this process should be trusted, select 'Allow' and the item will be removed from Quarantine and added to the Trusted Process list. If 'Block' is selected, the item will remain quarantined. Check the 'Do not ask again' and the alert will not appear again.

APPLICATION SECURITY

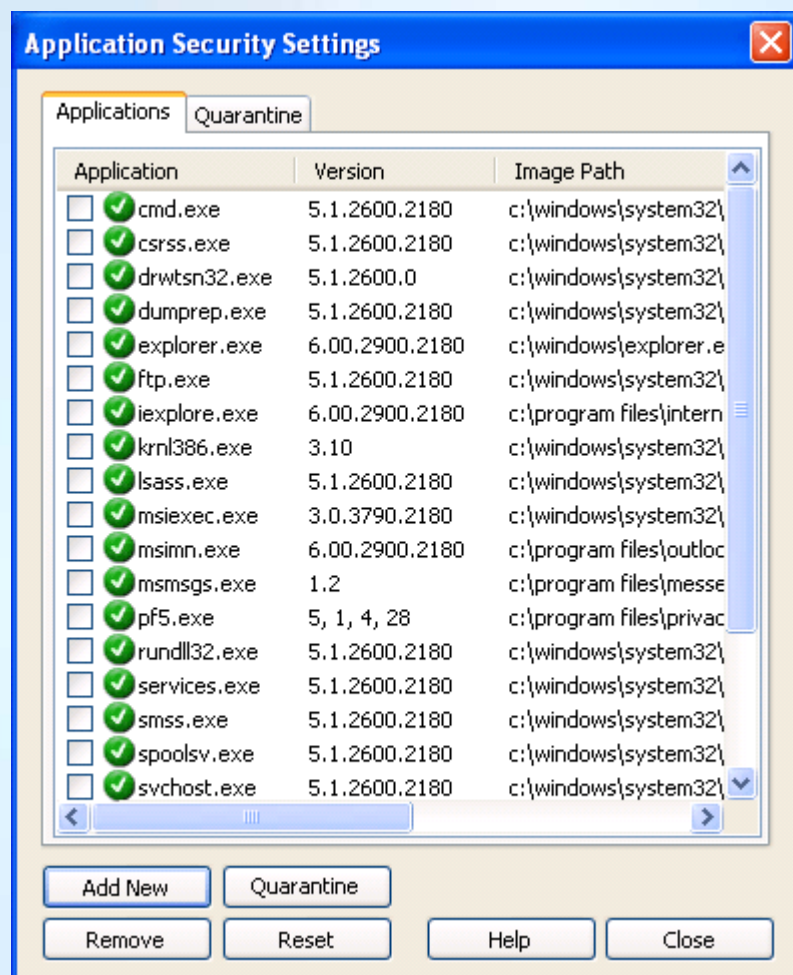
The DSA Application Security layer monitors all inbound and outbound Application-specific Internet activity as well as [WinAPI](#) calls for system processes.

(Click [here](#) for more information about WinAPI Calls)



User determination regarding each event that generates an alert is required when the "Require User Approval for Each Alert" box is selected. An on-screen alert (see below) 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.

View the trusted Applications/Processes by clicking the 'View/edit application list' button from the Main Menu (see screenshot).



Click 'Add New' to manually add an application to the trusted list. Click 'Quarantine' to move an application to the Quarantine list and thereby blocking access to that application.

Click 'Remove' to delete an application from the trusted list. Click 'Reset' to revert to DSA default trusted application list.





Application Security Alerts



After the training period, DSA will provide alerts when any Application attempts to access the Internet or when process-related WinAPI activity is detected. If the alert is related to known/trusted activity, 'Details/Options' should be selected and the application/process should be allowed, which will also add it to the trusted application list (see above).



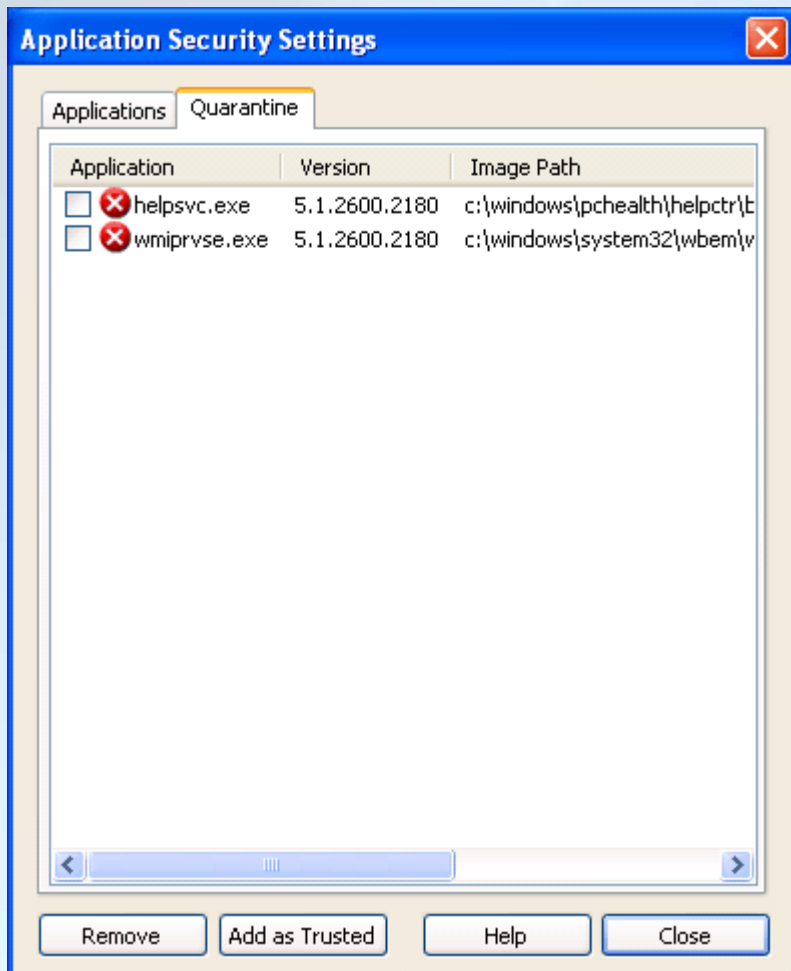
NOTE: DSA will display a Tray Alert for 30 seconds. If no action is taken, the alert will expire and the activity will be Blocked.

Click 'Details/Options' in the Tray Alert to display an expanded Alert (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 Main Menu, the 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 ('firefox.exe' in the alert below) will be performed in your default browser.

 Privacyware Alert - Incoming Traffic  DYNAMIC SECURITY AGENT Access to the Network/Internet has been blocked for: Firefox 1.5.0.1 C:\Program Files\Mozilla Firefox\firefox.exe Details: 4/18/2006 3:55:07 PM - An incoming packet TCP (6) has been blocked from 207.200.98.25:80 (http) to 192.168.1.2:3271 <input type="checkbox"/> Remember this setting Allow Access Block Access	 Privacyware Alert - Outgoing Traffic  DYNAMIC SECURITY AGENT Access to the Network/Internet has been blocked for: Firefox 1.5.0.1 C:\Program Files\Mozilla Firefox\firefox.exe Details: 4/18/2006 3:55:09 PM - An outgoing packet TCP (6) has been blocked from 207.200.98.25:80 (http) to 192.168.1.2:3271 <input type="checkbox"/> Remember this setting Allow Access Block Access
---	---

**Privacyware Alert - Process Monitor** 
DYNAMIC SECURITY AGENT
Activity related to the following process has been blocked:
awft.exe
c:\program files\atelier web\awft\awft.exe
Details:
An attempt to open a foreign process has been detected.
Target PID: 1820
Image Name: explorer.exe
If this event is not related to legitimate system use, select 'Block' and investigate the issue further.
 Remember this setting
Allow Block

If the application/process is not related to legitimate system use, select the 'Deny access' button and the process will be placed in the 'Quarantine' list.



If it is determined that a Quarantined item should be trusted, check the box next to the Application and click the 'Add as Trusted' button. The Application will be removed from Quarantine and added to the Trusted Application list. The application can also be removed and not added to the trusted list by clicking 'Remove'.

Every time a quarantined application/process attempts to run, DSA will generate the following alert:



If it is determined that this item should be trusted, select 'Allow' and the item will be removed from Quarantine and added to the Trusted list. If 'Block' is selected, the item will remain quarantined. Check the 'Do not ask again' and the alert will not appear again.

Program Changes

After an application has been installed and added to the Trusted Application List, DSA will generate 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 DSA is installed, the Program Change Alert will be displayed and the 'Block program' button should be selected so the issue can be investigated and resolved.

Privacyware Dynamic Security Agent

Version 2.0 – User Guide

Copyright © 2007 Privacyware. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or non-disclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use without the written permission of Privacyware.

All other trademarks and registered trademarks are the property of their respective holders.