



Endpoint Security Console

Version 3.0 – User Guide

Table of Contents

Summary	2
System Requirements	3
Installation	4
Configuring Endpoint Security Console as a Networked Service	5
Adding Computers, Groups, and Users	7
Using Endpoint Security Console	10
Menus and Toolbars	10
Global Settings	12
Managed Network	13
Applications	14
Process Monitor	16
Behavioral Settings	17
Process Detection	19
Port Tracking	20
Log Reports	21
Stored Settings	22
Activity Log	23
License Manager	24
Workstation Settings	25

Summary

Endpoint Security Console is a central installation and administrative console for Privatefirewall, Privacyware's desktop/endpoint Personal Firewall and Intrusion Detection Application. Endpoint Security Console enables system administrators to install, monitor, and configure Privatefirewall on any workstation within a server domain. Settings can be customized for each workstation or User Groups configured within Active Directory. Core Privatefirewall features include: Inbound/Outbound Packet Filtering, Port Scanning, IP/Website Protection, Process Detection, Outbound Email Detection, and System Anomaly Detection. For more information regarding Endpoint Security Console, please refer to the Privacyware website at <http://www.privacyware.com>.

System Requirements

To run Endpoint Security Console, your server must meet the following minimum system requirements:

Hardware

- 700 MHz Pentium® III or faster
- 256 MB RAM
- 10 MB of free disk space

Software

One of the following operating systems:

Windows® 2000 Server

Windows® 2003 Server

Windows® 2000 Advanced Server

Windows® XP Home Professional

Windows® Vista - All versions

***Active Directory is required for some features.**

Installation

Endpoint Security Console should be installed on a network server that is managed by a System Administrator. The Endpoint Security service, which will run silently, can either be installed on the networked workstations manually, or through group policy within Active Directory. To begin installation, double-click the Endpoint Security Console executable. Carefully read and agree to the product End-User License Agreement to proceed. Endpoint Security Console will install seamlessly with no prompts.

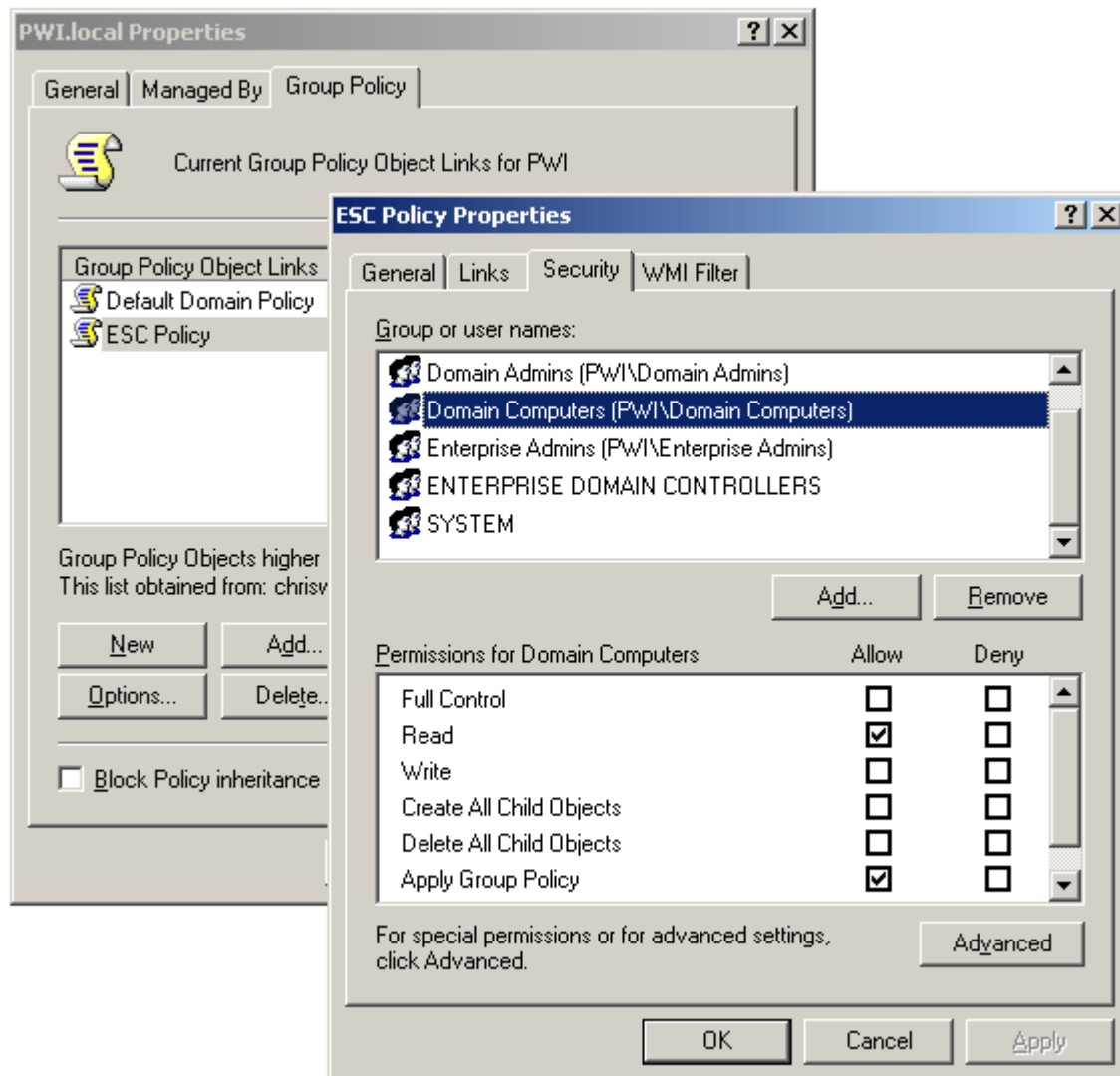


Configuring Endpoint Security Console as a Networked Service

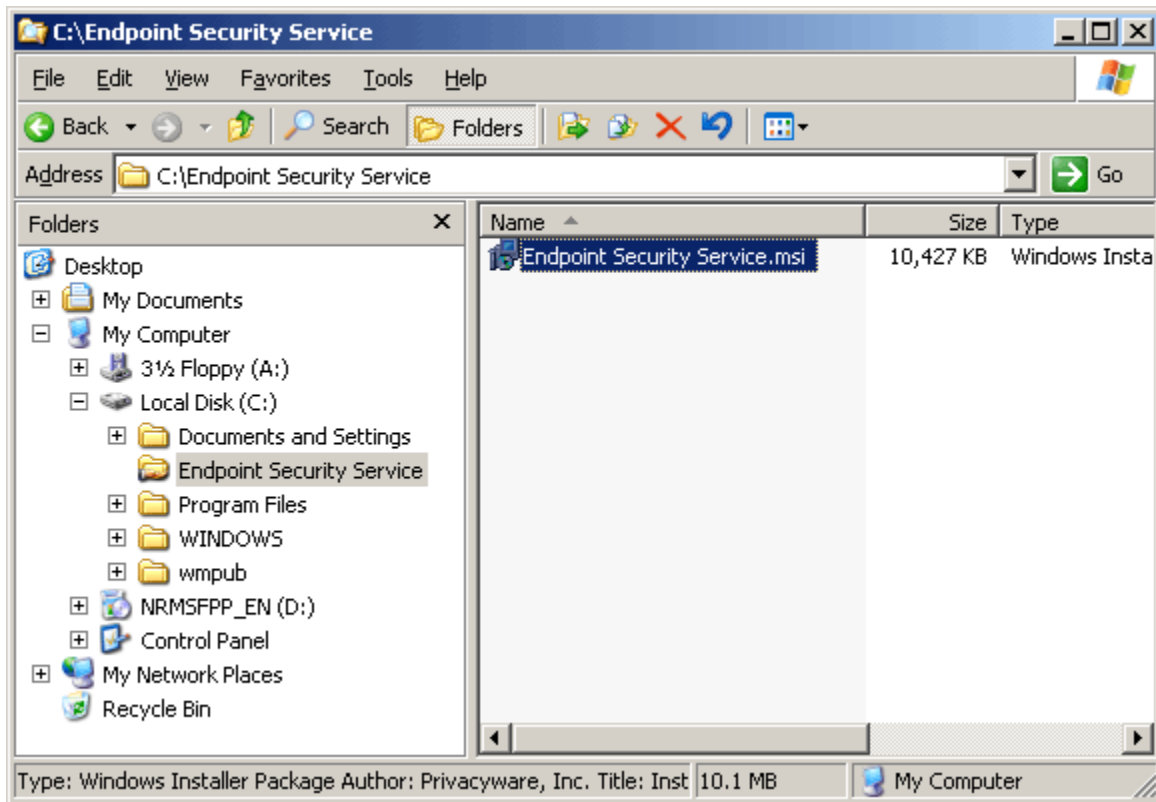
Before Endpoint Security Console can add any Computer/Group/User, the Console must be installed as a Networked Service on that computer. This can be done either manually, by launching the network service executable on each computer, or it can be installed as a Group Policy Software Installation. In order for Group Policy Installation to function, the server must be configured as a Domain Controller and all workstations must be part of that domain.

To configure a Group Policy Installation, the following steps must be taken:

- 1) Either the default Group Policy must be modified or a new Group Policy must be created (suggested). Once the new Group Policy is created, click Properties, select the Security tab, delete 'Authenticated Users' from groups list, add 'Domain Computers' to the groups list and make sure that they are the only group that has 'Apply Group Policy' Permission.

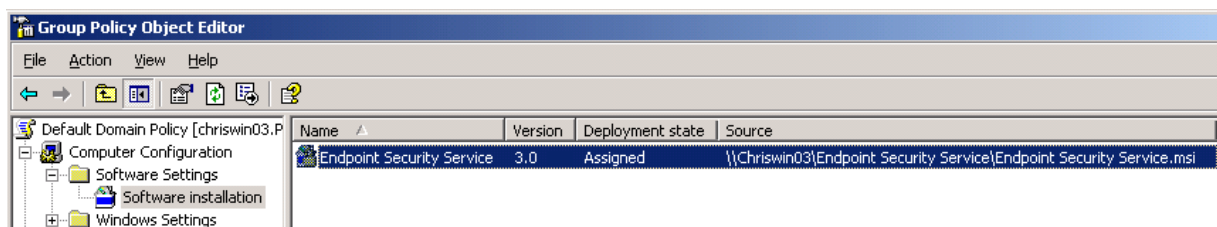


- 2) Once the Group Policy has been configured, an Installation Package must be created ([click here for more information](#)). In order to set up the package correctly, a shared folder must be specified that contains the Endpoint Security Service executable. This folder must allow access from all Active Directory Users.



- 3) Once this is in place, the installation package can be set up by selecting New/Package from the Group Policy Object Editor.

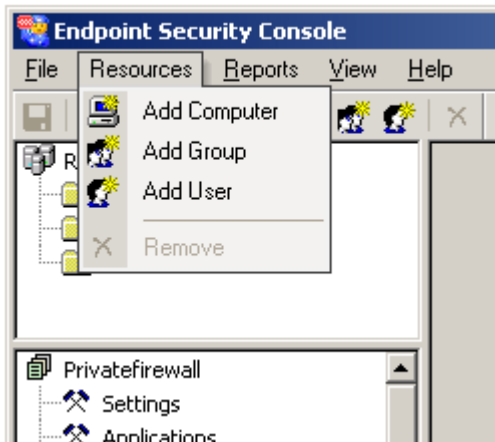
When prompted, navigate to the shared folder (through the mapped network path) where the Privatefirewall Networked Service executable is located and click on the 'Open' button. When completed, the executable should be listed as 'Assigned'.



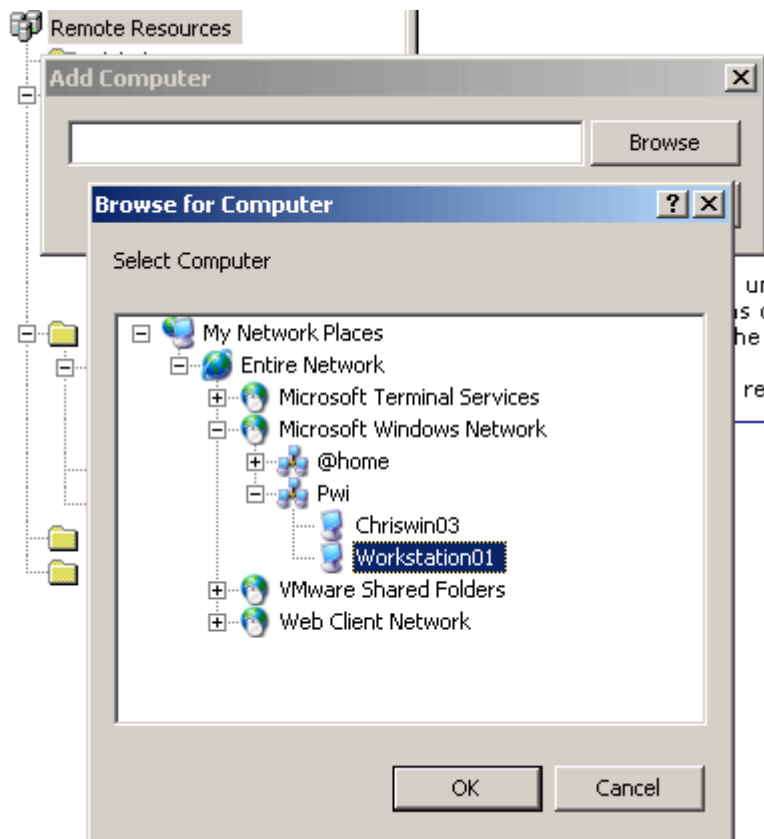
The next time any workstation that is part of the domain logs in, the Privatefirewall Network Service will be automatically installed.

Adding Computers, Groups, and Users

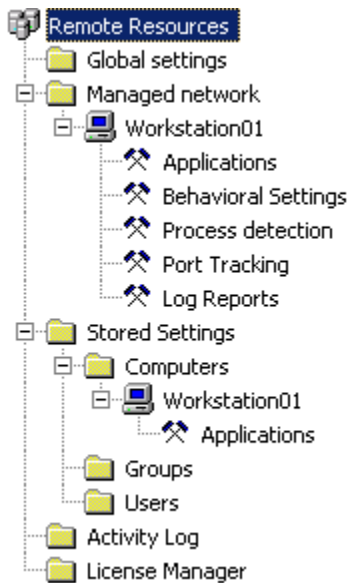
In order to manage any other computers with the Endpoint Security Service, the computer must be added to Endpoint Security Console. Workstations can be added individually, or based on Users or Groups within Active Directory. This can be initiated by selecting 'Resources/Add' From the Main Menu:



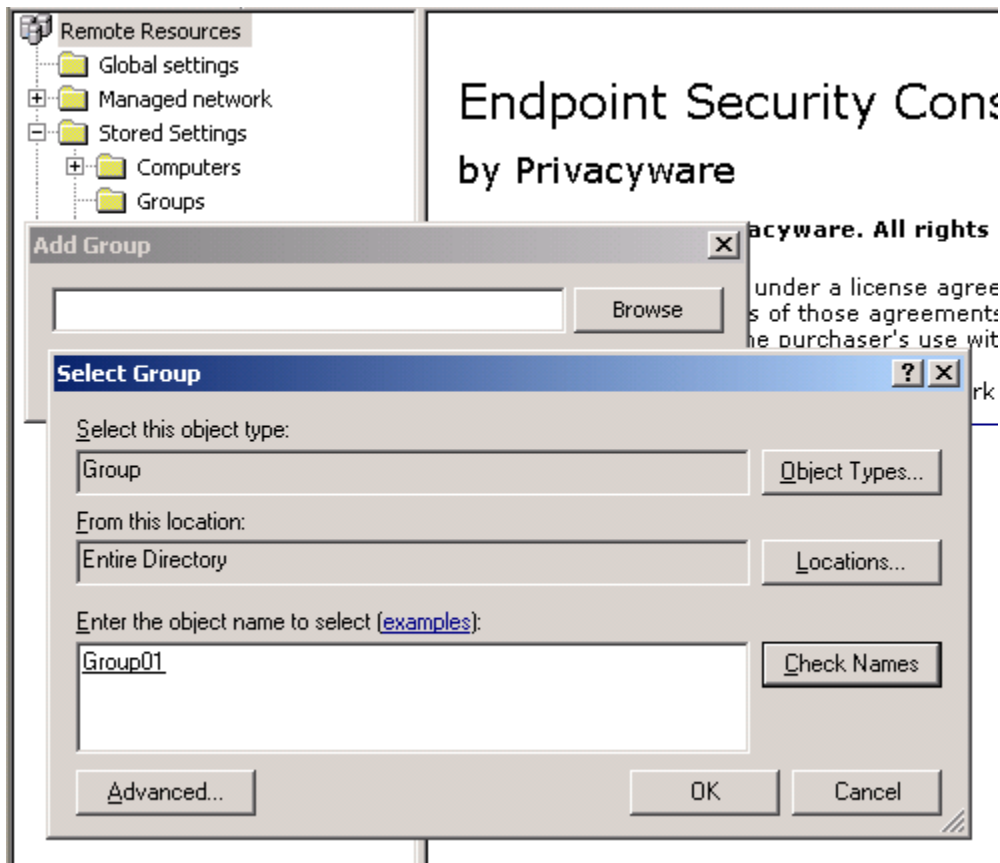
Individual workstations can be added by selecting the desired network computer:



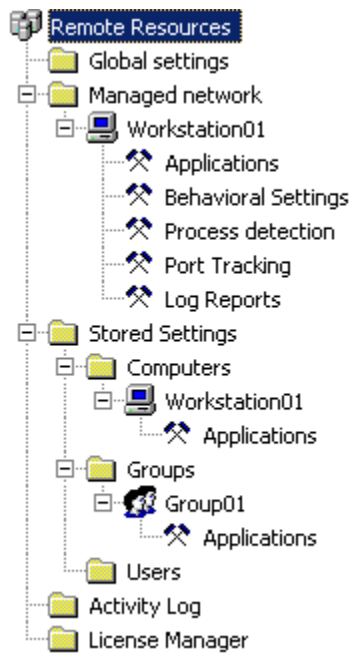
The name of the workstation will appear within the tree menu after it is successfully added:



Using the same process, Groups or Users can also be added from an existing Active Directory structure:



The name of the group or user will appear within the tree menu after it is successfully added:



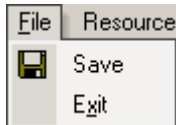
Using Endpoint Security Console

From the Management Console, the system administrator can manage all workstations, AD Users or AD Groups that have been configured with the Endpoint Security Service.

Menus and Toolbars

Endpoint Security Console Menus

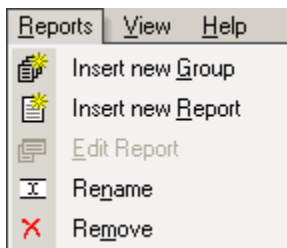
File Menu - Save your settings or Exit from ESC.



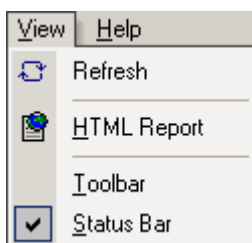
Resources Menu - (Within the Stored Settings section) Add or Remove a Workstation Computer, Activity Directory Group or User.



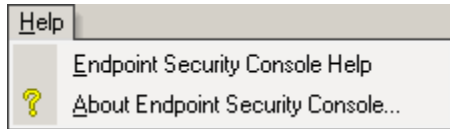
Reports Menu - (Within the Log Reports section) Insert a New Group or Report, Edit an existing report, Rename or Remove a Report.



View Menu - Refresh the current view, run a HTML report (within the Log Reports section), display the Toolbar or Status Bar.



Help Menu - View the Endpoint Security Console Help file, view the program version number.



Endpoint Security Console Toolbars



Save - Save your settings

Apply - Apply any settings changes

Distribute - Distribute any settings changes to other Computers, Groups, or Users

Refresh - Refresh the current view

HTML Report - Run a HTML report (within the Log Reports section)

About - View the program version number.



(Within the Stored Settings section)

Add Computer - Add a Workstation Computer

Add Groups - Add an Active Directory Group

Add User - Add an Active Directory User

Delete - Remote a Computer, Group, or User



(Within the Applications node from Managed Network or Stored Settings section)

Add - Add a new application

Customize - Edit a rule within an existing application

Remove - Remove an existing application

Allow - Set all Application rules to Allow

Filter - Set all Application rules to Filter

Deny - Set all Application rules to Deny



(Within the Log Reports section)

Insert Group - Create a new Log Report Group

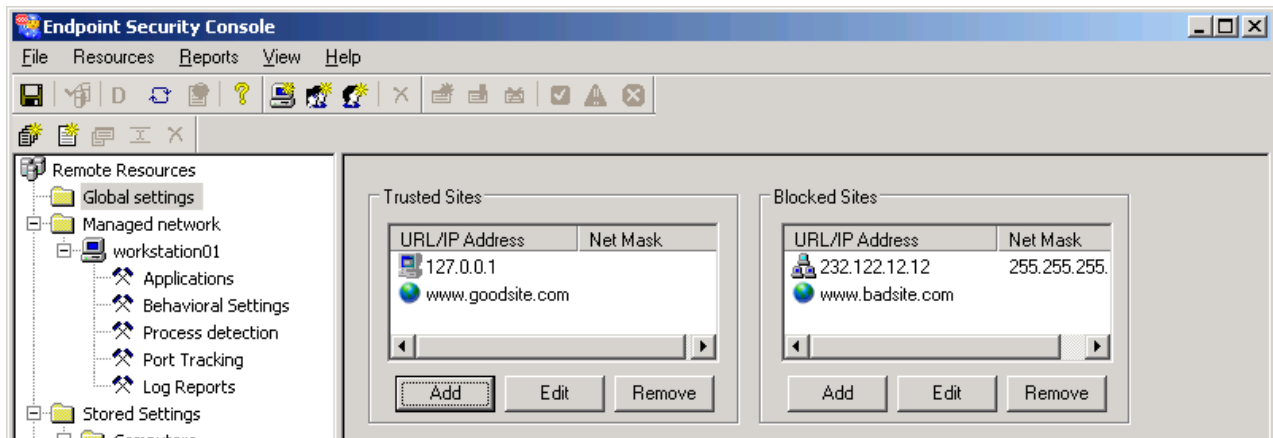
Insert Report - Create a new Log Report

Edit Report - Change an existing Log Report

Rename - Rename an existing Log Report

Remove - Remove an existing Log Report

Global Settings

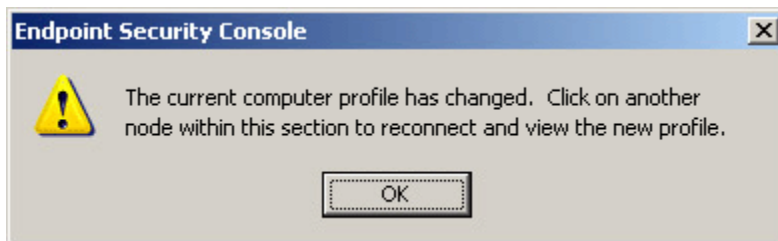


Global Settings are applied to all Computers, Groups, or Users running the Endpoint Security service. They include Trusted and Blocked websites and IP Addresses.

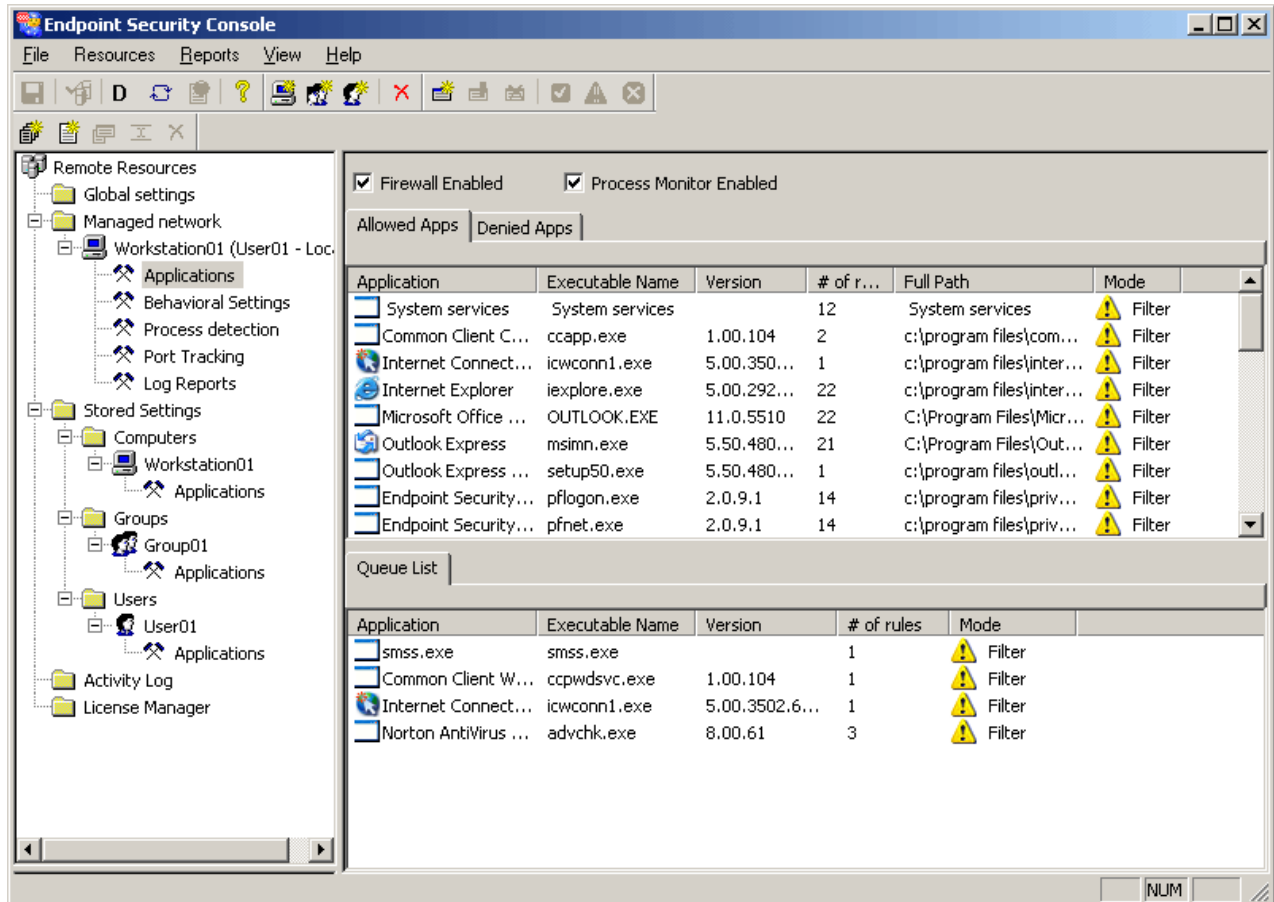
Managed Network

(Note: Active Directory required for all features involving Users and Groups)

The Managed Network section lists all active workstations running the Endpoint Security Service. The Managed Network is where the primary configuration of Endpoint Security Console takes place, including Application Security, Process Detection and Monitoring, and System/Email Anomaly Detection. For every active Workstation listed in the Managed network, there is a corresponding user name and Profile Name (formatted as: *Computer Name (User Name - Profile Name)*). The user name is whoever is currently logged on the Workstation. The Profile name can either be 'Local' or an AD User/Group Name. If the profile is 'Local', all rules and settings will be stored on the Workstation. If the profile is an AD User/Group Name, rules and settings will be stored within Active Directory in the Domain Controller. The default profile for any newly added computer is 'Local', but if any changes are made to a AD User/Group within the Stored Settings section, the profile will change to that AD User/Group. You will see the following message whenever the profile has changed.

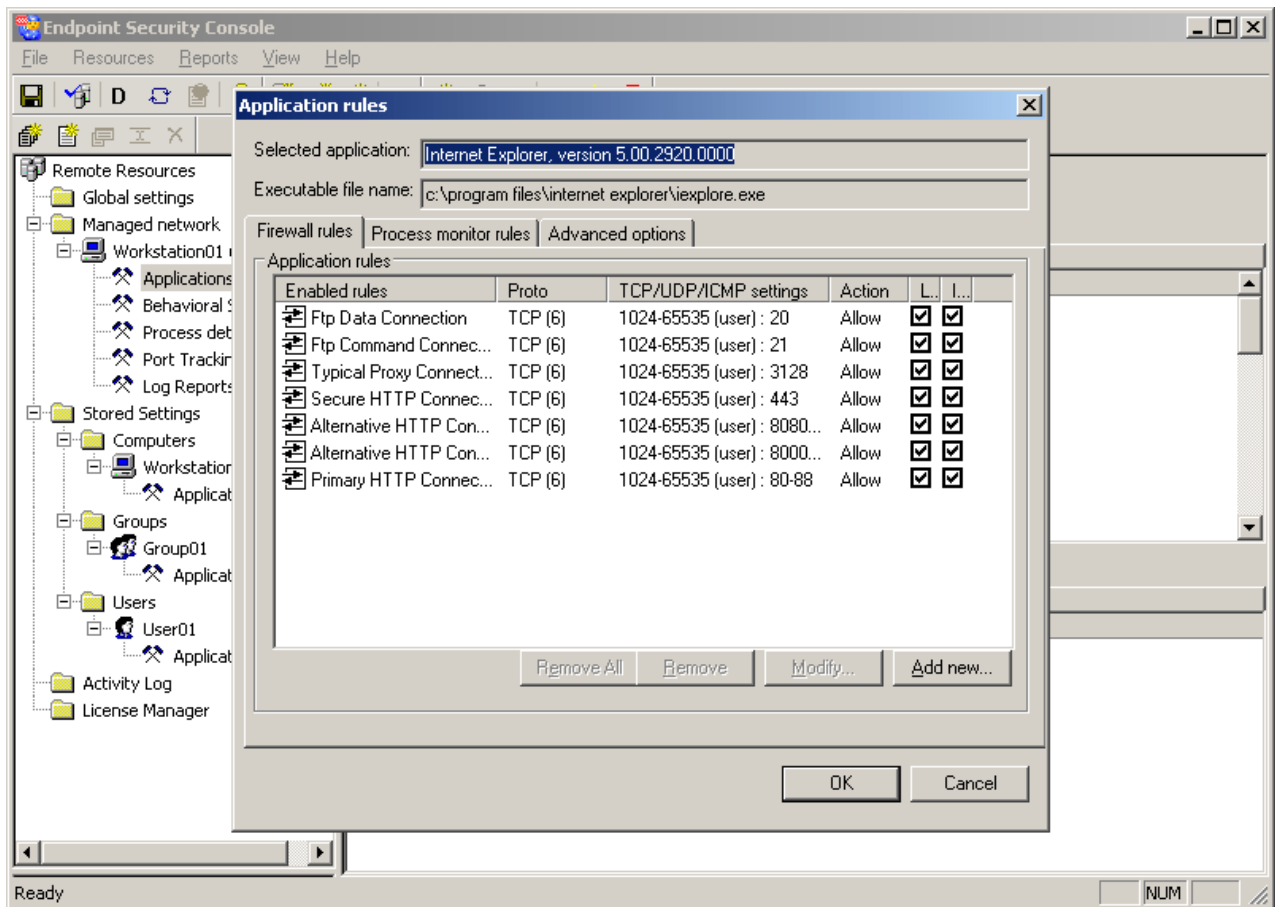


Applications

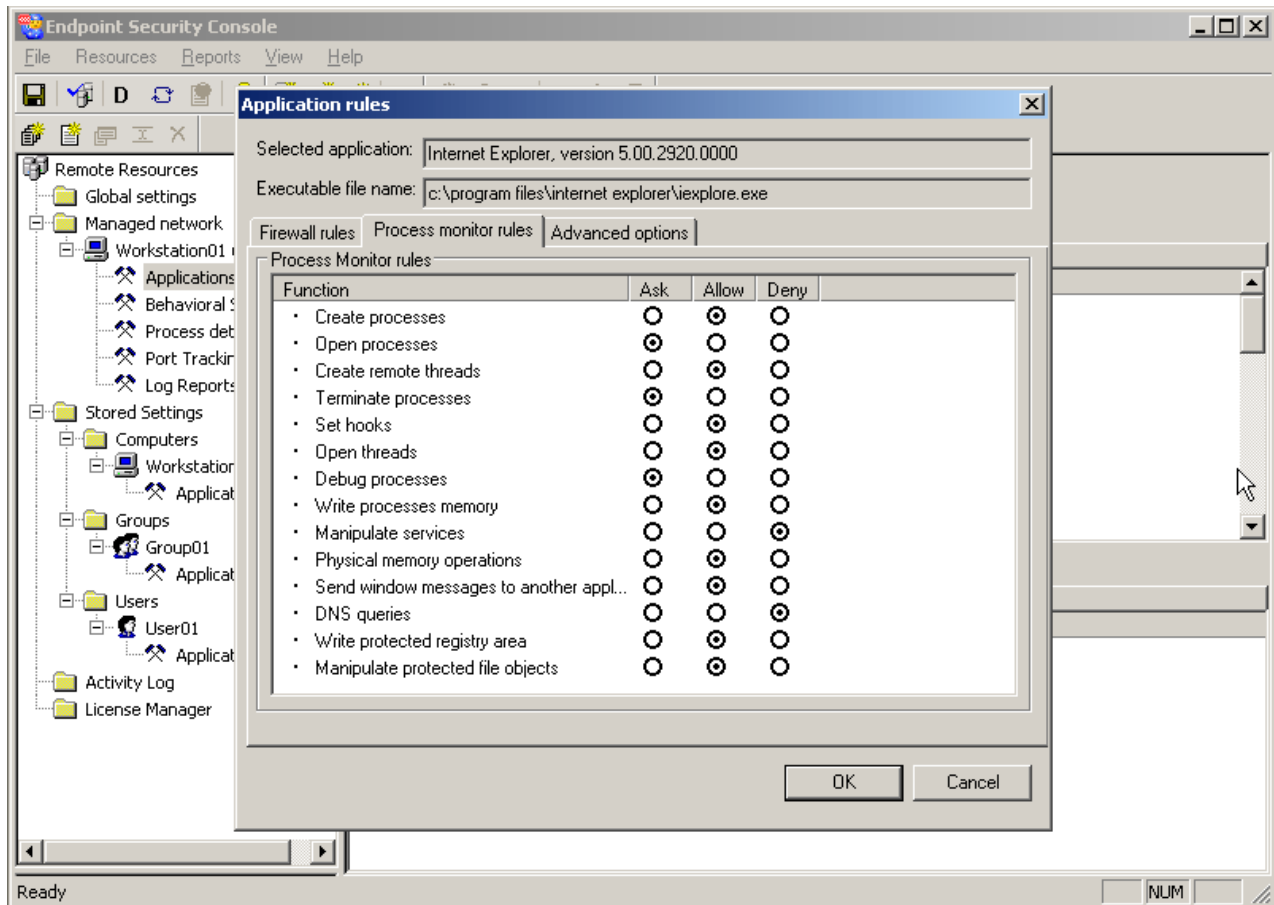


The Applications screen consists of all the Application and Process Monitor related rules that Endpoint Security Console is enforcing for the Applications listed. The Process Monitor filters processes for potentially malicious system API calls used by programmers (and hackers) to launch process executables. The screen includes the Application and file executable name, version number, number of rules being enforced, and the classification 'Mode' of those rules, which can be set to either allow, deny, or filter incoming or outgoing traffic.

The top window displays all 'Allowed/Filtered' or 'Denied' Applications, and the bottom windows displays a 'Queue List', which contains all Application/Process Monitor activity from Computers/Users/Groups that requires approval from the Administrator. The Administrator can view all proposed rules for each queue list item by right-clicking on an item and selecting 'View Suggested Rules' (see below). Any rules that are set for the application will be applied when the Mode is set to 'Filter' Traffic. If the Mode is set to 'Allow' all rules will be disabled and all activity related to the application will be allowed. If the Mode is set to 'Block', no activity will be allowed.



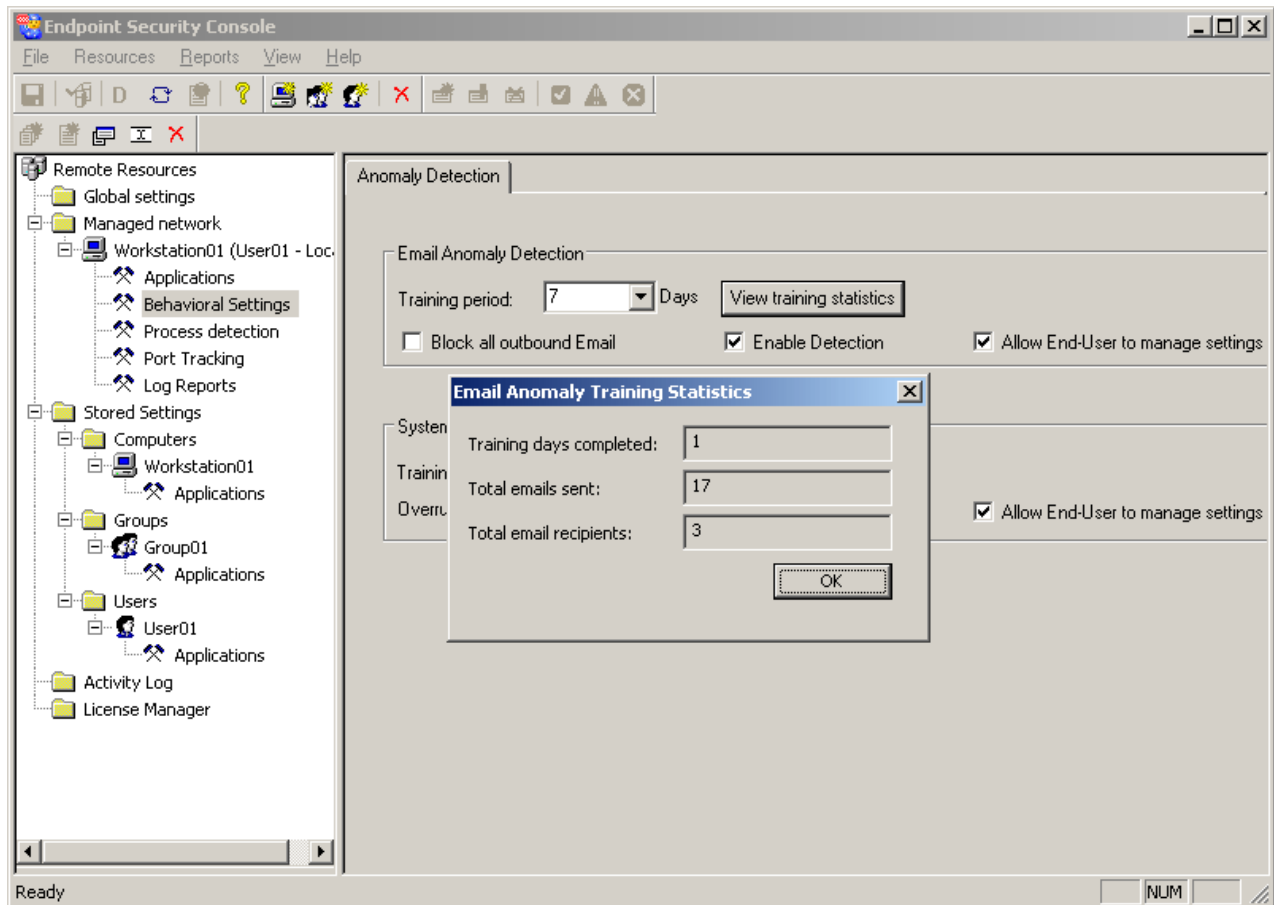
Process Monitor



Endpoint Security Console maintains a list of processes that are being filtered for potentially malicious system API calls used by programmers (and hackers) to launch process executables. The process list is maintained in the Applications node, and a separate list of Process monitor rules is maintained. As you can see from the screenshot above, you can Allow, Deny, or Ask the administrator for each Process-related function listed. A set of default processes that are related to commonly used applications, such as Internet Explorer, are set to 'Allow'. Non-default processes that are detected by Endpoint Security Console will be set to 'Filter' if allowed or 'Deny' if not allowed.

Behavioral Settings

Email Anomaly Detection



This feature tracks outbound Email delivery behavior and provides alerts if there is unusual outbound email activity based on type and amount of emails delivered within a certain period of time. The Email Anomaly Detection Engine is based on the specific behavior of each workstation's email activity over a period of time called the 'Training Period', which can be set to 7, 14, or 28 days. 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 (see screenshot).

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, 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.

Sensitivity Threshold - The System Anomaly Detection layer generates alerts as it detects system activity that deviates from normal. The sensitivity with which Endpoint Security

Console 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.

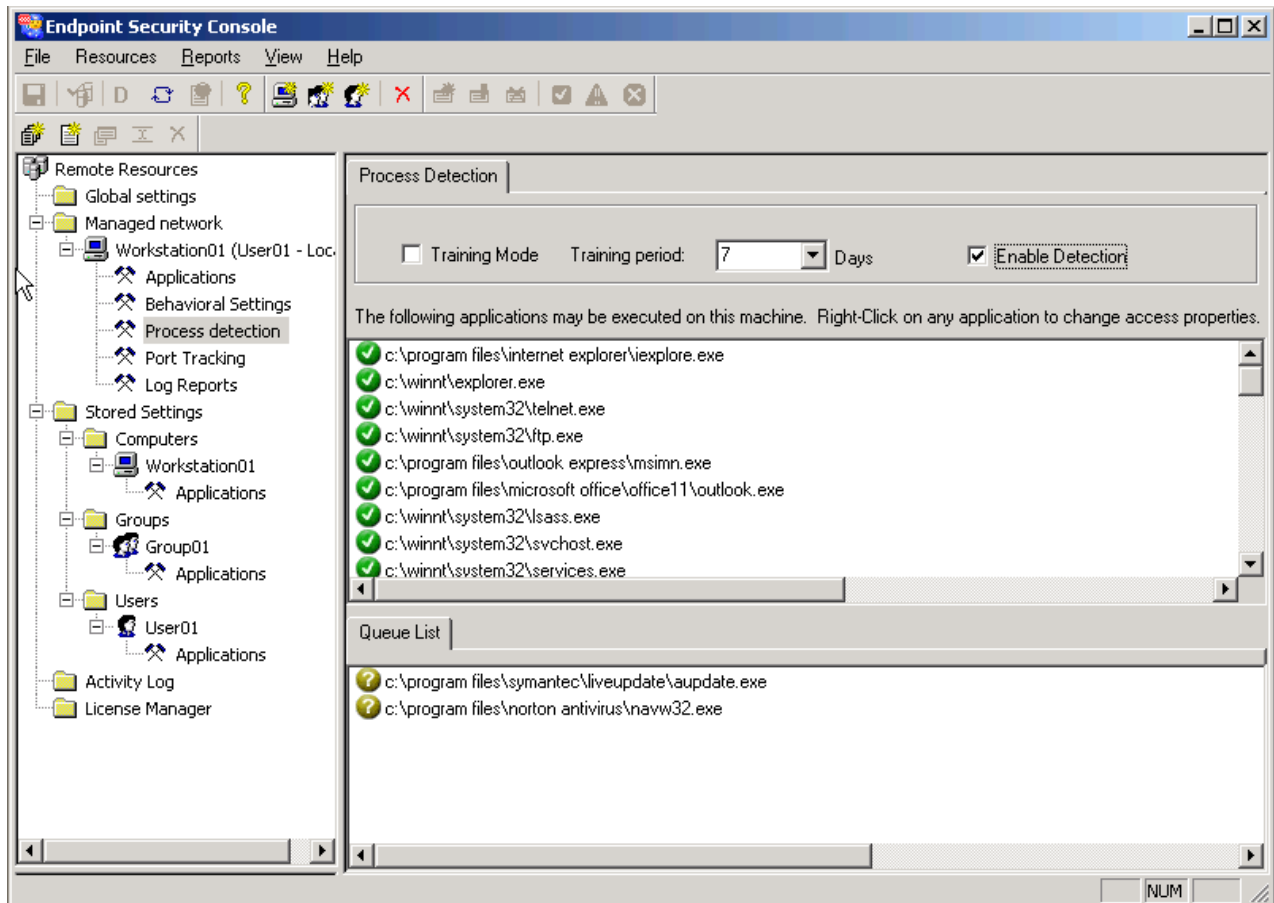
Selecting the Training Statistics button will display the System behavior data collected during training. These may be viewed during or after the Training period (see screenshot).

The screenshot shows the Endpoint Security Console interface. The main window displays the 'Anomaly Detection' settings for 'Email Anomaly Detection' and 'System Anomaly Detection'. The 'System Anomaly Detection' section is active, showing a training period of 7 days and an overrun threshold of 60%. A 'View training statistics' button is visible. A dialog box titled 'System Anomaly Training Statistics' is open, displaying a table of application training data.

Application	Mode	Training from	CPU M1 Av...	CPU M5 Av...
winword	Training	14:15:34 03/14/08	0.33(2.11)	0.45(0.70)
ccpwwdsvc	Training		0.00(0.00)	0.00(0.00)
setup50	Training		0.00(0.00)	0.00(0.00)
winmgmt	Training	11:59:29 03/14/08	0.00(0.05)	0.00(0.02)
shmgate	Training		0.00(0.00)	0.00(0.00)
ie4uinit	Training		0.00(0.00)	0.00(0.00)
vmwareuser	Training	11:59:29 03/14/08	0.01(0.08)	0.01(0.03)
ccapp	Training	11:59:29 03/14/08	0.02(0.56)	0.02(0.13)
icwconn1	Training		0.00(0.00)	0.00(0.00)
unregmp2	Training		0.00(0.00)	0.00(0.00)
mstask	Training	11:59:29 03/14/08	0.02(0.13)	0.02(0.06)
regsvr32	Training		0.00(0.00)	0.00(0.00)
pfnet	Training	11:45:26 03/14/08	4.61(707.10)	4.73(141.43)
pflogon	Training	12:36:08 03/14/08	0.02(0.05)	0.00(0.00)
drwtsn32	Training		0.00(0.00)	0.00(0.00)
spoolsv	Training	11:45:26 03/14/08	0.00(0.41)	0.01(0.11)

The Anomaly Detection Engine will start immediately after the end of the training period, and will generate an alert whenever in the Activity Log whenever there is any activity that is not consistent with system use patterns established during the training period. Additional event details are located in the 'Reason' column within the Activity Log.

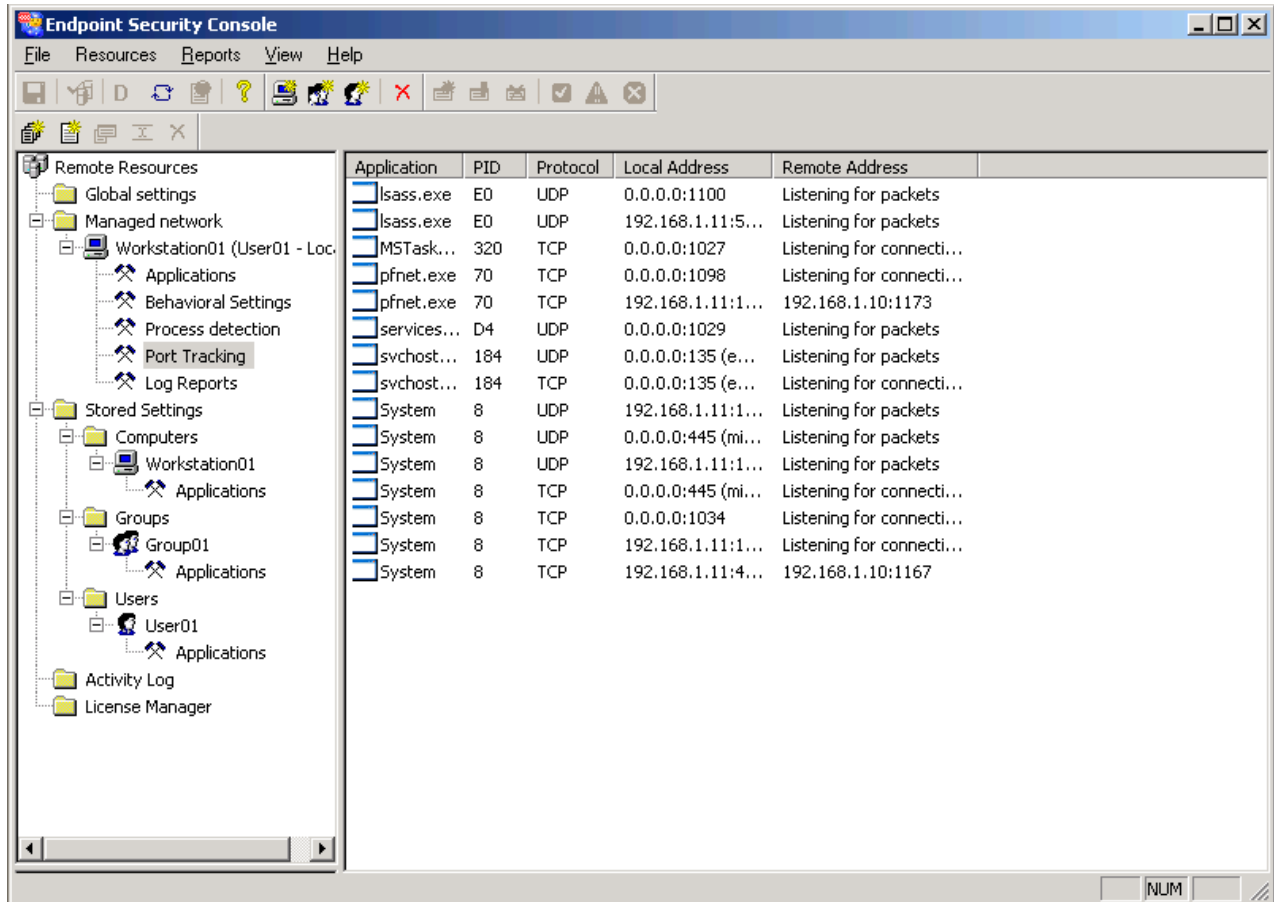
Process Detection



The Process Detection feature records all processes that are launched during the 'Training Period', which can be set to 1, 3, or 7 days. Training is enabled by default and commences immediately upon installation. All processes detected during the Training Period will be added to the trusted process list. After the training period, a Tray Alert will be generated 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.

The top window displays all Trusted (allowed) processes, and the bottom window displays a 'Queue List', which contains all detected Processes from Computers/Users/Groups that require review by the Administrator. The Administrator can right-click on each item in the Queue List to Allow or Deny the process.

Port Tracking



The Port Tracking report monitors all system ports and protects them against any unauthorized entry. In most cases, Endpoint Security Console goes one step further and makes all system ports invisible to intruders (referred to as "Stealth" mode). The following details are included:

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 - The Internet address from where incoming packets are originating. This will display either a specific IP, or if one is not currently detected, it will give a status (such as "Listening for packets/connections").

Log Reports

Date/Time	Local IP	Local Port	Remote IP	Remote Port	Protocol	Application
04:04:12 04/15/08	192.168.1.11	1591	64.94.110.11	80	TCP	C:\Program F
04:04:06 04/15/08	192.168.1.11	1591	64.94.110.11	80	TCP	C:\Program F
04:04:02 04/15/08	192.168.1.11	1591	64.94.110.11	80	TCP	C:\Program F
04:03:49 04/15/08	192.168.1.11	1590	12.158.80.10	80	TCP	C:\Program F
04:03:43 04/15/08	192.168.1.11	1590	12.158.80.10	80	TCP	C:\Program F
04:03:39 04/15/08	192.168.1.11	1590	12.158.80.10	80	TCP	C:\Program F
04:03:26 04/15/08	192.168.1.11	1589	64.94.110.11	80	TCP	C:\Program F
04:03:20 04/15/08	192.168.1.11	1589	64.94.110.11	80	TCP	C:\Program F
04:03:16 04/15/08	192.168.1.11	1589	64.94.110.11	80	TCP	C:\Program F
04:03:03 04/15/08	192.168.1.11	1588	12.158.80.10	80	TCP	C:\Program F
04:02:57 04/15/08	192.168.1.11	1588	12.158.80.10	80	TCP	C:\Program F
04:02:53 04/15/08	192.168.1.11	1588	12.158.80.10	80	TCP	C:\Program F
23:48:51 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:51 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:49 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:49 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:47 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:47 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:45 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:45 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:43 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:41 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:41 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:39 04/15/08	169.254.255....	137	169.254.198....	137	UDP	
23:48:39 04/15/08	169.254.255....	137	169.254.198....	137	UDP	

Firewall log records can be sorted by type and time of occurrence. Each of these reports can also be sorted going back 1 Hour, 1 Day, or 1 Week. Separate reports are maintained for Web Traffic, Mail Traffic, System Traffic, and Processes detected. The following details are included:

Time/Date - When the packet was detected.

Local IP (Internet address) - The Internet address from which the packet was sent.

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).

Stored Settings

(Note: Active Directory required for all features involving Users and Groups)

Endpoint Security Console can store Application and Process Monitor rules for Computers as well as Active Directory Users and Groups anywhere within the Domain environment. This allows the Administrator to maintain security settings for Users that are not currently logged into any workstation. Settings within this section are similar to the Applications section within the Managed Network node.

The screenshot displays the Endpoint Security Console interface. On the left, a tree view shows the navigation structure: Remote Resources, Managed network, Workstation01, Applications, Behavioral Settings, Process detection, Port Tracking, Log Reports, Stored Settings, Computers, Workstation01, Applications, Groups, Group01, Applications, Users, User01, Applications, Activity Log, and License Manager. The main area shows 'Firewall Enabled' and 'Process Monitor Enabled' checked. Below this, there are tabs for 'Allowed Apps' and 'Denied Apps'. A table lists various applications with columns for Application, Executable Name, Version, # of r..., and Mode. The 'nprotect.exe' application is highlighted in blue.

Application	Executable Name	Version	# of r...	Mode
System services	System services		12	Filter
smss.exe	smss.exe		1	Filter
nmain.exe	nmain.exe		1	Filter
nprotect.exe	nprotect.exe		1	Filter
navw32.exe	navw32.exe		1	Filter
ccapp.exe	ccapp.exe		2	Filter
ccpwsdvc.exe	ccpwsdvc.exe		1	Filter
cmd.exe	cmd.exe		1	Filter
csrss.exe	csrss.exe		15	Filter
drwtsn32.exe	drwtsn32.exe		14	Filter
explorer.exe	explorer.exe		20	Filter
ftp.exe	ftp.exe		2	Filter
icwconn1.exe	icwconn1.exe		2	Filter
ie4uinit.exe	ie4uinit.exe		2	Filter
iexplore.exe	iexplore.exe		22	Filter
krnl386.exe	krnl386.exe		1	Filter
lsass.exe	lsass.exe		24	Filter
msiexec.exe	msiexec.exe		15	Filter
msimn.exe	msimn.exe		21	Filter
mstask.exe	mstask.exe		2	Filter
navw32.exe	navw32.exe		0	Filter

Activity Log

The Activity Log lists all types of events generated from any workstation in the Managed Network. This includes Application or 'Firewall' events, Process Monitor, New Processes, System Anomaly, and Email Anomaly. Each event has its own icon type, and the information provided in the Log includes: event time, workstation name, User Name (if Active Directory is installed), Application or executable name, alert type, and the reason for the alert. Each event in the Activity Log can be allowed or blocked by the Administrator.

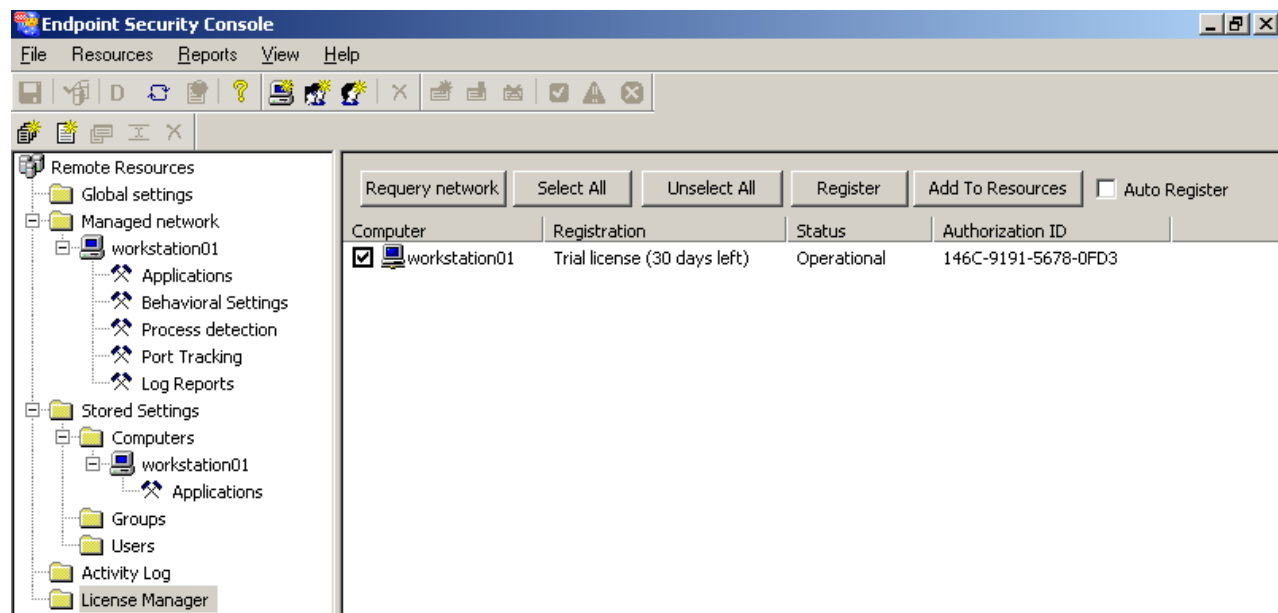
Time	Workstation	User Name	Application	Type	Reason
17:32:55 1...	WORKSTATION01	User01	csrss.exe	System Anomaly	Last 1 Minute pro...
17:32:40 1...	WORKSTATION01	User01	OUTLOOK.EXE	System Anomaly	Last 1 Minute pro...
17:32:36 1...	WORKSTATION01	User01	C:\Program Fi...	New Process	INFORMEXEC
17:32:36 1...	WORKSTATION01	User01	c:\winnt\sys...	Process Monitor ...	OPEN_PROCESS
17:32:35 1...	WORKSTATION01	User01	C:\Program Fi...	Firewall event	NO_RULE
17:32:20 1...	WORKSTATION01	User01	c:\Program Fil...	Process Monitor ...	FILEWRITE
17:32:12 1...	WORKSTATION01	User01	C:\Program Fi...	Firewall event	NO_RULE
17:32:00 1...	WORKSTATION01	User01	c:\program fil...	Process Monitor ...	CREATE_PROCESS
17:32:00 1...	WORKSTATION01	User01	c:\winnt\sys...	Process Monitor ...	CREATE_PROCESS
17:31:54 1...	WORKSTATION01	User01	ccApp.exe	System Anomaly	Last 1 Minute Thre...
17:31:09 1...	WORKSTATION01	User01	services.exe	System Anomaly	Last 1 Minute pro...
17:30:54 1...	WORKSTATION01	User01	OUTLOOK.EXE	System Anomaly	Last 1 Minute Thre...
17:30:33 1...	WORKSTATION01	User01	c:\program fil...	Process Monitor ...	FILEWRITE
17:29:22 0...	WORKSTATION01	User01	c:\winnt\sys...	Process Monitor ...	FILEWRITE
17:29:18 0...	WORKSTATION01	User01	c:\winnt\sys...	Process Monitor ...	REGISTRY
17:13:21 0...	WORKSTATION01	User01	C:\WINNT\ex...	Firewall event	restricted ip: 64....
17:12:58 0...	WORKSTATION01	User01	C:\WINNT\ex...	Firewall event	restricted ip: 64....

License Manager

A fully functional trial version of Endpoint Security Console can be evaluated for 30 days. After the trial period has expired, Endpoint Security Console must be registered by purchasing a Registration Code. This code can be purchased at the following URL:

<http://www.privacyware.com/cart>

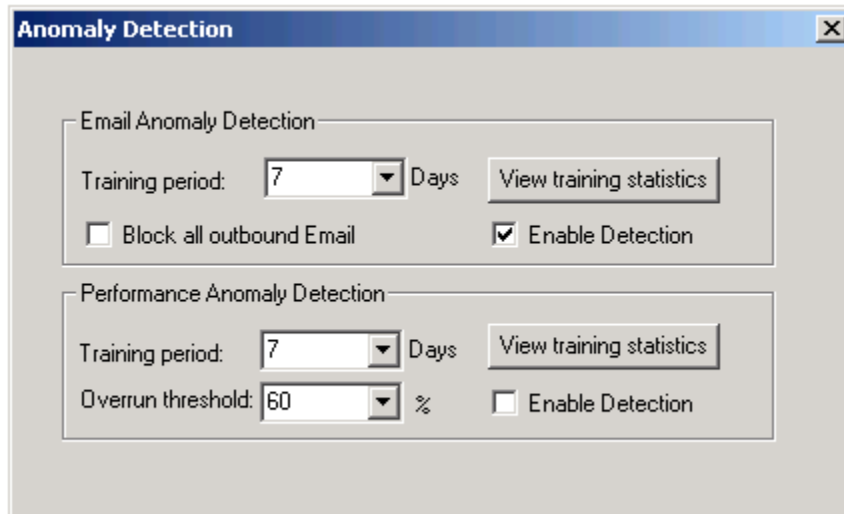
When the purchase is completed, you will receive a confirmation email with a Registration Code. **If more than one license is purchased, the same registration code should be used for all installations.** The code must be entered in the License Manager section within Endpoint Security Console.



All unregistered workstations that have the Endpoint Security Service installed will be listed in this section. The 'Authorization ID' is unique for each workstation and is used in the registration process. The 'Add To Resources' button will add any workstation to the Managed Network if it is not already listed. To complete registration, check the box next to the workstation(s) and press the 'Register' button. You will then be prompted to enter in your registration code.

Workstation Settings

The workstation user has the option to Allow or Deny behavior-based activity and will also see several types of informational alerts that do not require any workstation user-decision. Also, the administrator can allow the user to turn off the System Anomaly and Email Anomaly Detection features. The following menu can be accessed by the workstation user by double-clicking on the ESC Tray Icon (These options will be grayed-out if the Administrator prohibits the Workstation user from access).



The screenshot shows a window titled "Anomaly Detection" with a close button in the top right corner. The window is divided into two sections: "Email Anomaly Detection" and "Performance Anomaly Detection".

Email Anomaly Detection

- Training period: 7 Days (with a dropdown arrow) [View training statistics]
- Block all outbound Email
- Enable Detection

Performance Anomaly Detection

- Training period: 7 Days (with a dropdown arrow) [View training statistics]
- Overrun threshold: 60 % (with a dropdown arrow)
- Enable Detection

Workstation Alerts



This is the alert the workstation user will see for any unapproved Application Security, Process Monitor, or Process Detection activity. No action is required by the workstation user.



This is the workstation alert for any unapproved System Anomaly activity. The user can either Allow or Block access, and the activity will be listed in the Endpoint Security Console Activity List for Administrator review regardless of the user's decision.



This is the workstation alert for any unapproved Email Anomaly activity. The user can either Allow or Block outbound emails, and the activity will be listed in the ESC Activity List for Administrator review.

Endpoint Security Console

User Guide

Document Version

Endpoint Security Console, Privacyware.

There is no warranty of any kind with respect to the completeness or accuracy of this manual. Privacyware may make improvements and/or changes to the product(s) and/or programs described in this User Guide at any time and without notice.

Copyright & Trademarks

Copyright © 2008 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.