

threatsentry

User Guide



privacyware

Published by:
Privacyware
Red Bank, NJ 07701
Email: info@privacyware.com
URL: <http://www.privacyware.com>

Table of Contents:

I. System Requirements	2
II. Product Overview	3
III. Installation	5
IV. Advanced Installation and Configuration.....	9
A. Installation on Multiple Servers.....	10
B. Security Alert Display and Security Alert Log Storage.....	11
C. Security Modes.....	12
V. Product Registration	14
VI. Uninstalling	17
VIII. Using ThreatSentry	18
A. Management.....	20
Services	20
Rules.....	29
B. Using the Behavioral Engine	40
Training Data Display.....	40
Training Data Details.....	43
Training on Existing IIS Logs	45
C. Security Alerts & the Security Alert Log.....	46
Security Alerts.....	46
Security Alert Log.....	47
Working with the Security Alert Log	48
Security Alert Log Reports	50
X. Regular Expression Guidelines.....	51
XI. Contact & Support.....	52

I. System Requirements

ThreatSentry is compatible with the following:

- IIS 7.0/7.5 (Windows Server 2008/R2)
- IIS 6.0 (Windows Server 2003)
- IIS 5.0 (Windows Server 2000)

- For Windows Server 2008/IIS7, the following Role Services must be enabled:
 - "ISAPI Extensions" (in Application Development). Required until we'll switch on Native IIS7 module architecture instead of current ISAPI Filter (IIS5)/ ISAPI Extension (IIS6)
 - "IIS6 Management Compatibility" – required to display correct service status and IIS Import logs

- .NET framework 2.0 (for SQL Server)
- Install ThreatSentry using an account with administrative privileges.

ThreatSentry has been tested for compatibility with most Win32/64 scripting environments/server extensions like ASP, ASP.NET, ColdFusion, PHP, Perl, and JSP.

II. Product Overview

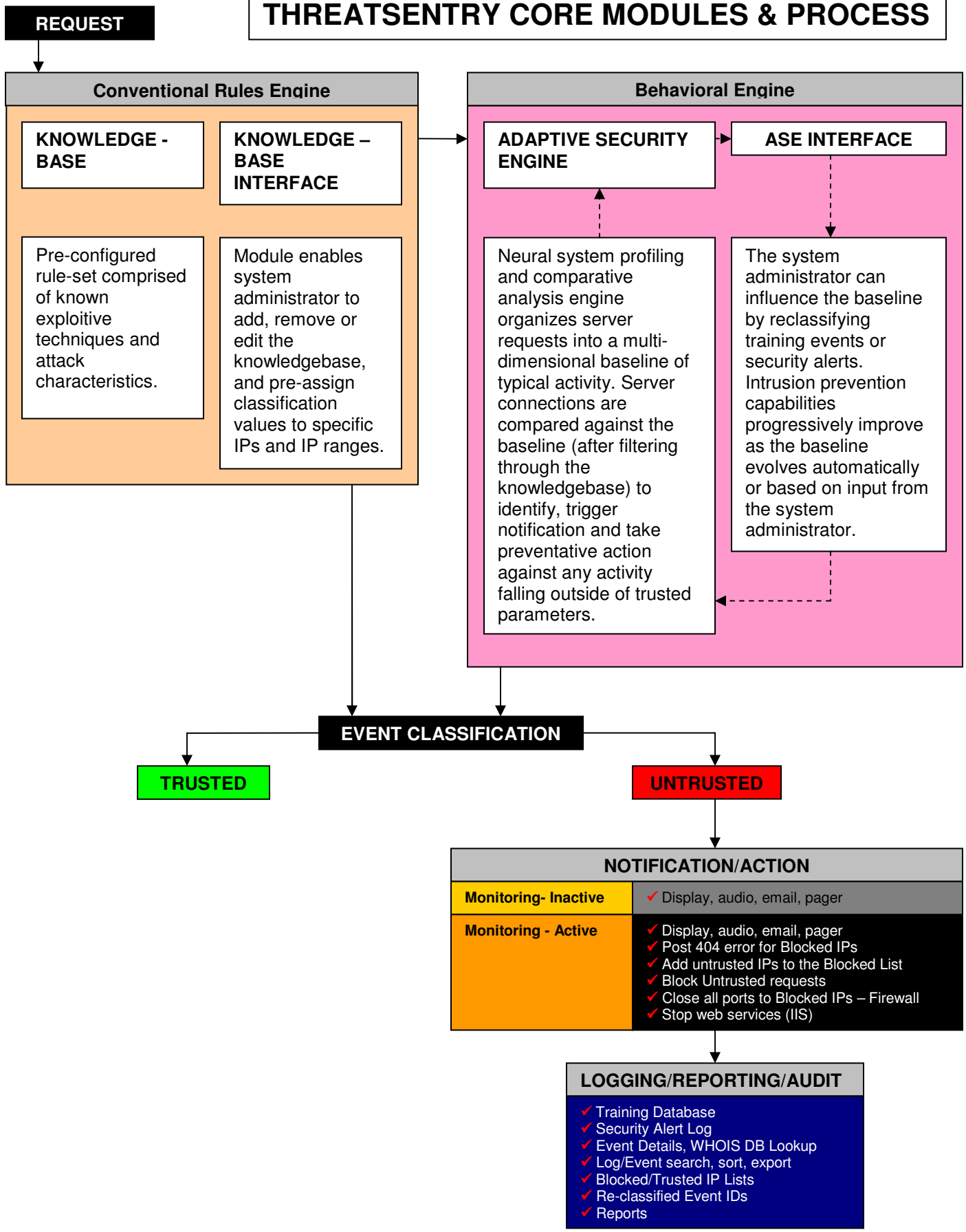
What is ThreatSentry?

ThreatSentry is a multi-layered Web Application Firewall that protects Microsoft Windows Web servers from a broad range of web application threats including Cross Site Request Forgery (CSRF/XSRF), Structured Query Language (SQL) Injection, Cross-Site Scripting (XSS) and other attacks. ThreatSentry combines an advanced web application firewall, a proprietary NDIS driver, and an AI-based intrusion prevention engine to identify and take action against known and new threats. ThreatSentry also helps fulfill the web application layer firewall (WAF) requirement in PCI DSS 6.6 and aids in the web application code review process by revealing vulnerabilities embedded within software code.

How Does It Work?

ThreatSentry is implemented as an ISAPI extension (ISAPI filter in IIS5) which collects and feeds data through a knowledge-based classification framework. Events that match explicit rules (signatures and other settings) are immediately classified as Trusted or Untrusted depending on the applicable rule. ThreatSentry immediately blocks Untrusted events (in Monitoring – Active security mode) before IIS responds and applies whatever other Threat Management policies that may be configured. ThreatSentry also leverages a behavior-based analytic engine, the Adaptive Security Engine (ASE), which profiles typical system behavior and identifies/blocks activity that departs from the baseline. ThreatSentry can identify and prevent any type of activity that could be harmful to the host, regardless of whether it is known (documented) or not (new or unknown threats).

THREATSENTRY CORE MODULES & PROCESS



III. Installation

Installation Notes:

- Please note that administrative privileges are required to install and configure ThreatSentry on Windows servers.
- The setup program is very simple and fully automated, but be advised that IIS will be stopped/restarted during installation (as well as upon uninstall).
- The system will install SQL Express (and MSXML version 3.0 components, when necessary) on the target system/s. The setup program will launch a management console after the successful installation of the product.
- ThreatSentry provides a special set of installation features. Please refer to the **Advanced Installation Options** section for details.

Upgrading from ThreatSentry v3 to ThreatSentry v4

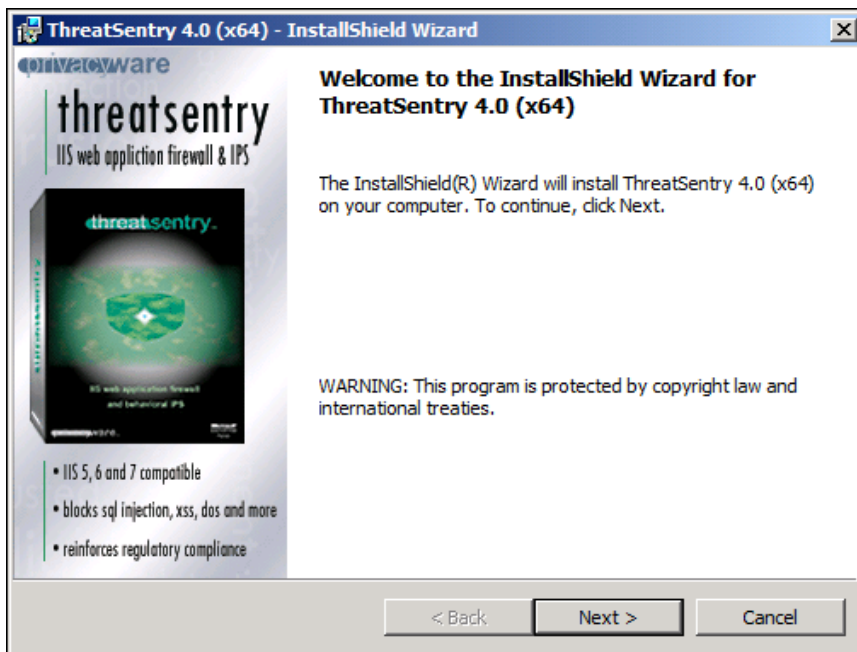
Upgrade support from Threatsentry v3 to ThreatSentry v4 is fully supported.

- The previous installation of ThreatSentry v3 should be uninstalled (Uninstall via Control Panel -> Add/Remove Program)
- ThreatSentry v4 should be installed in the same directory as v3.
- Configuration settings stored in the registry will automatically be migrated to the v4 installation.

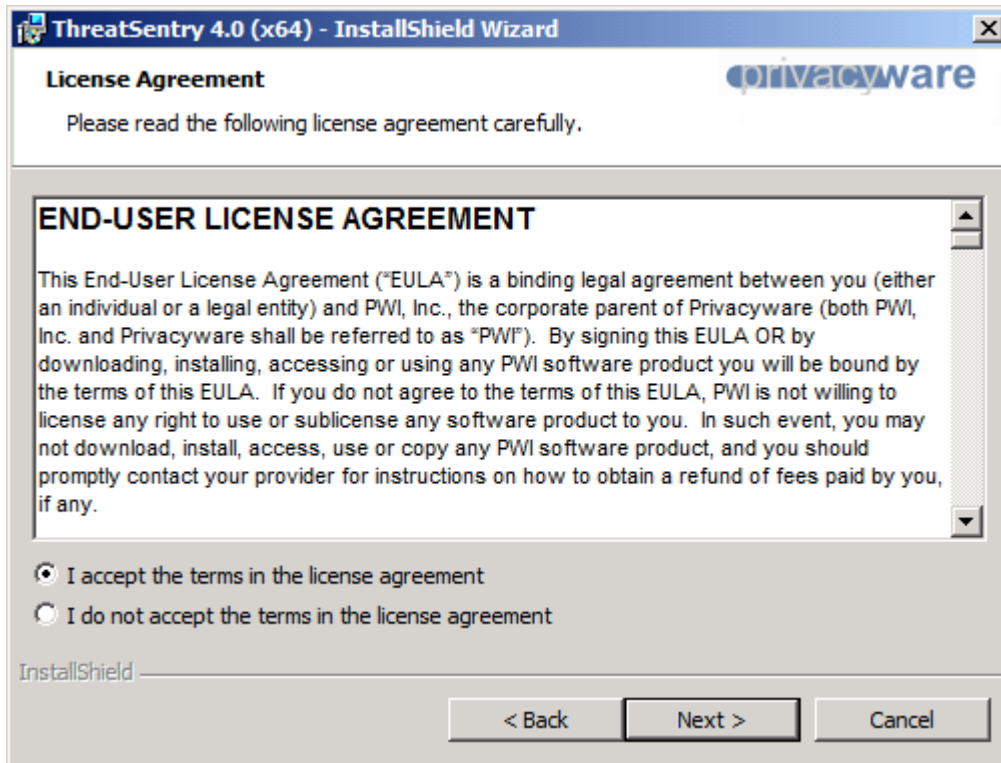
If the **"Preserve existing configuration settings"** option is selected during v4 installation:

- The existing (v3) MappingRules.xml will be migrated to the v4 installation (existing custom settings are higher-priority than default settings. v4 custom settings are higher-priority than v3 settings)
- The IntrusionLog.mdb and YEVS.mdb will be converted to SQL tables and any existing data will be migrated.

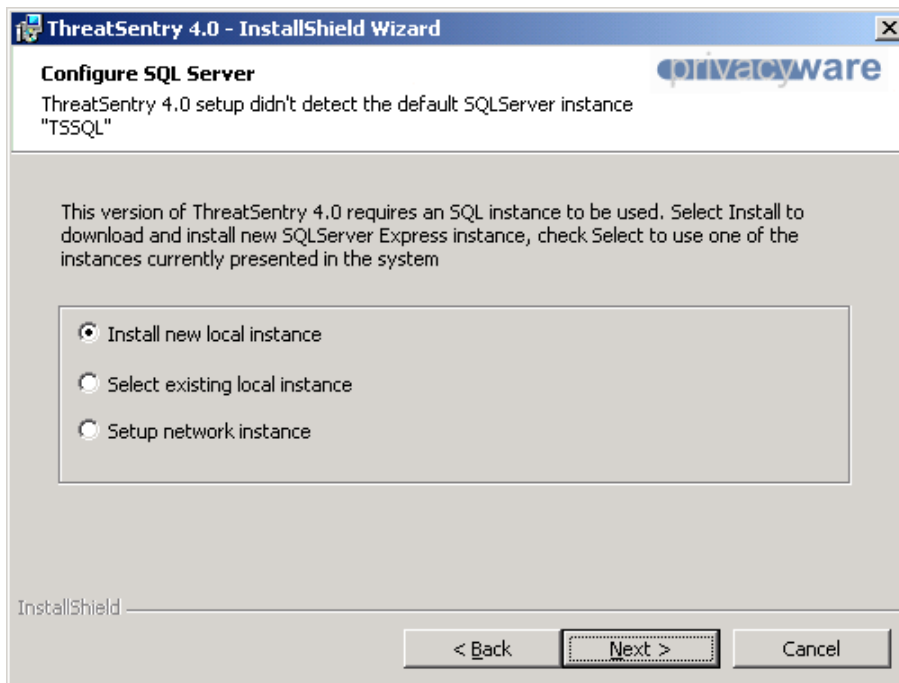
ThreatSentry uses the InstallShield Wizard to facilitate installation. To begin installation, double-click the ThreatSentry executable. The following screens illustrate the activation of the InstallShield Wizard. **Click Next.**



To continue with installation, carefully read the product End-User License Agreement, and select the appropriate radio button indicating that you accept its terms.



ThreatSentry requires an existing SQL database implementation for installation. Check **Select existing local instance** or **Setup network instance** to use existing SQL Server resources or check **Install new local instance** if SQL Server is not already available locally or remotely.



Install new local instance will invoke the Extraction of SQL Server related files and SQL Server installation. This process may take a few minutes. Do not click the Back or Next buttons until the SQL Server installation is complete (hourglass will disappear once complete).

If an existing SQL Server resource is used, the ThreatSentry installer will prompt you for relevant SQL Server connection information.

Data Link Properties

Provider | **Connection** | Advanced | All

Specify the following to connect to SQL Server data:

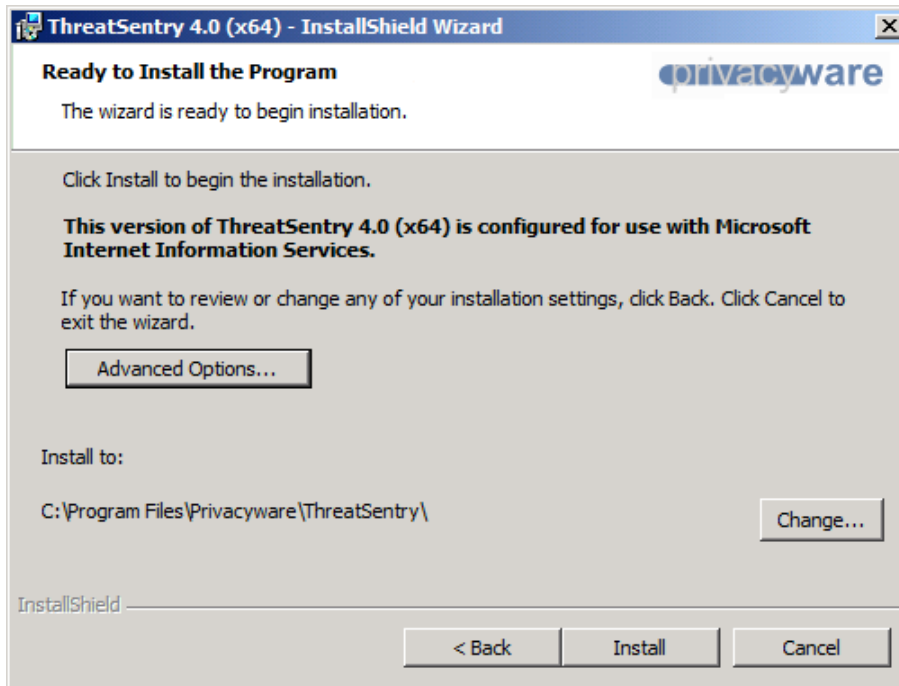
1. Select or enter a server name:
\TSSQL Refresh
2. Enter information to log on to the server:
 Use Windows NT Integrated security
 Use a specific user name and password:
User name: ts_user
Password: ●●●●
 Blank password Allow saving password
3. Select the database on the server:
[Empty dropdown]
 Attach a database file as a database name:
[Empty text box]
Using the filename: [Empty text box] ...

Test Connection

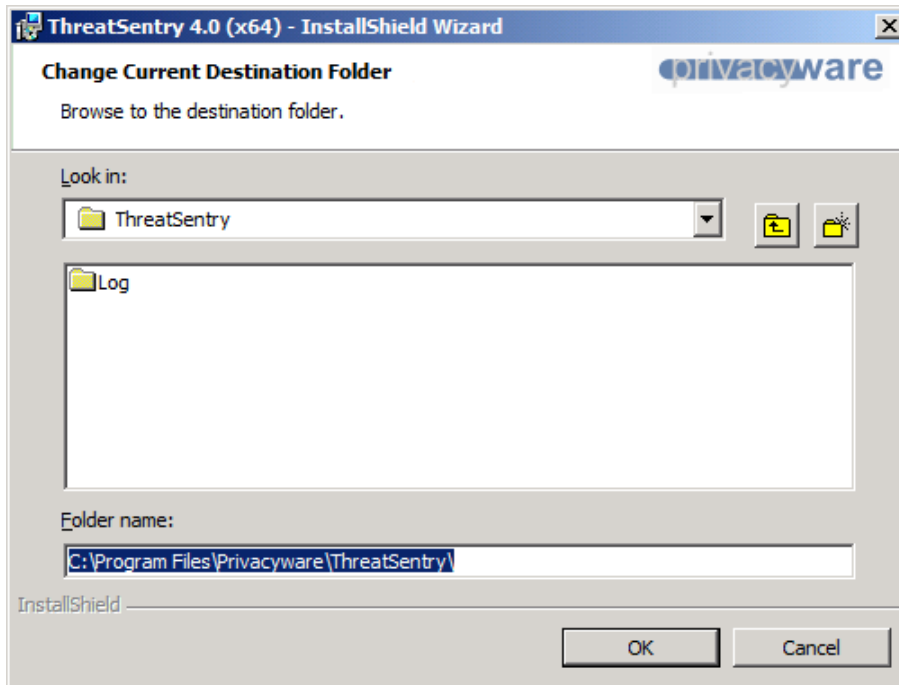
OK Cancel Help

Non-default Installation Location

To designate a non-default installation location for ThreatSentry, select the **Change** button.



This will invoke the screen shown below that will allow you to specify the non-default installation directory.



The installation process can now be concluded by simply clicking the **Install** button. Reboot of the server is not required to complete installation, but you will be prompted to restart IIS. Refer to the next section for an explanation of **Advanced Installation and Configuration Options**.

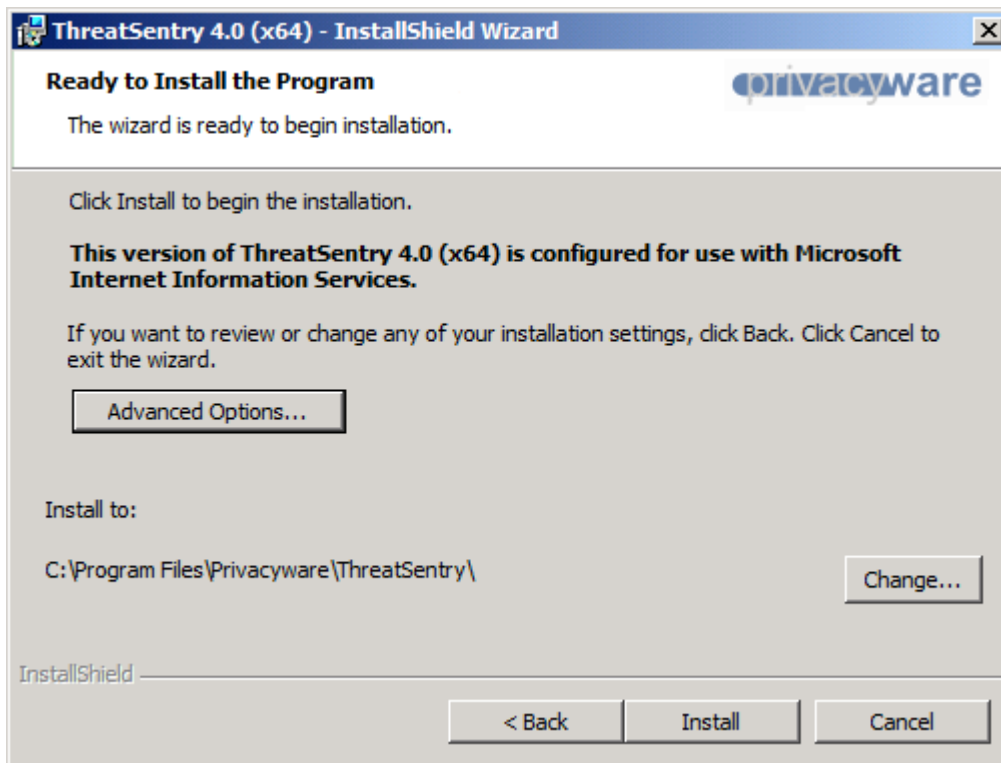
IV. Advanced Installation and Configuration

The **Advanced Options** Button reveals a series of interfaces that provide the ability to:

- A. Install ThreatSentry on [multiple servers](#) within a network.**
- B. Designate whether ThreatSentry's Behavioral Engine should be enabled (and configure related settings), and enable support for Outlook Web Access Operations (prior to training).**
- C. Designate non-default storage and display of Security Alert Logs.**
- D. Select a Security Mode.**

By default, ThreatSentry will operate in [Monitoring – Inactive](#) mode and store logs on the local server. You may alternatively configure ThreatSentry to operate in [Monitoring – Active](#) mode by indicating so via the [Advanced Options](#) available during installation.

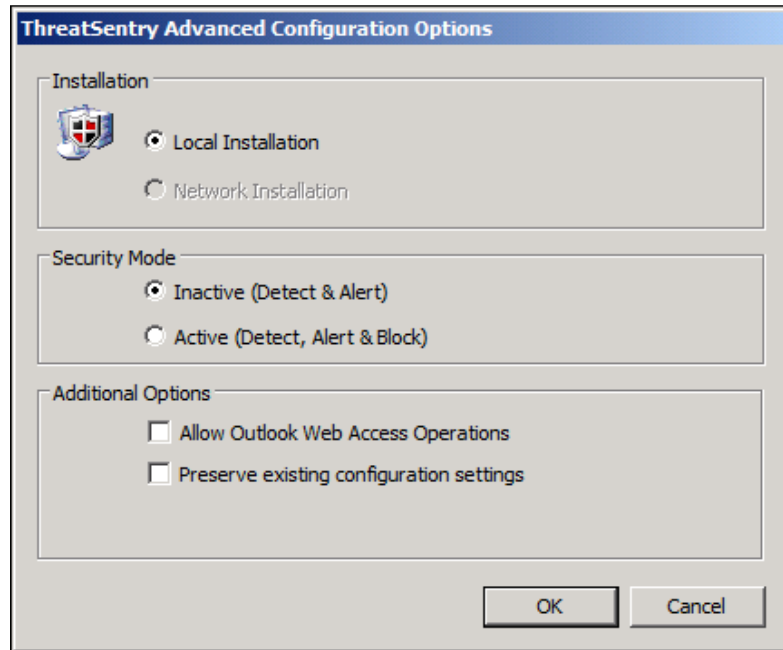
To access the Advanced Options, select the **Advanced Options** button as shown in the following screen capture.



A. Installation on Multiple Servers

To install ThreatSentry on multiple servers, select the **Network Installation** button as shown in the screen below. Then click **Add Servers**.

Note: To deploy ThreatSentry on multiple servers, port TCP 139 (NetBIOS session service), port 135 (for DCOM services), and port UDP 137 (NetBIOS Name Service) should be opened and not blocked by firewall/router.



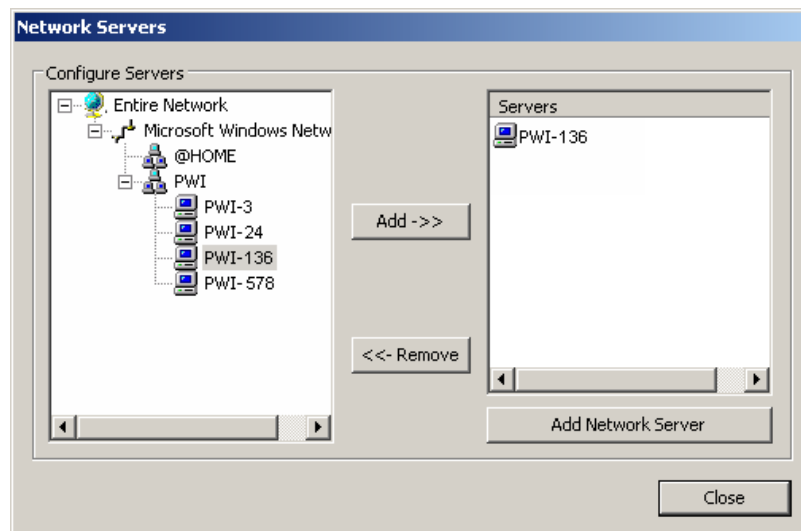
Outlook Web Access Support

Important Note:

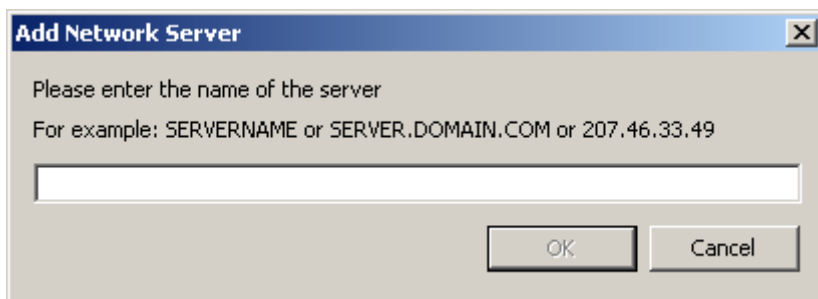
ThreatSentry supports Outlook Web Access operations. If the server on which ThreatSentry is being installed requires OWA support, it is important to indicate this during the installation process so that the Training Database properly classifies OWA-related IIS requests.

To do so, simply check the **Allow Outlook Web Access Operations** box.

Locate the other servers on which ThreatSentry will be installed and click the Add button so that they are visible in the left pane of the screen.



If a particular server is not visible in the left panel, select the **Add Network Server** button shown in the previous screen and enter the name of the server/s manually (as shown below).

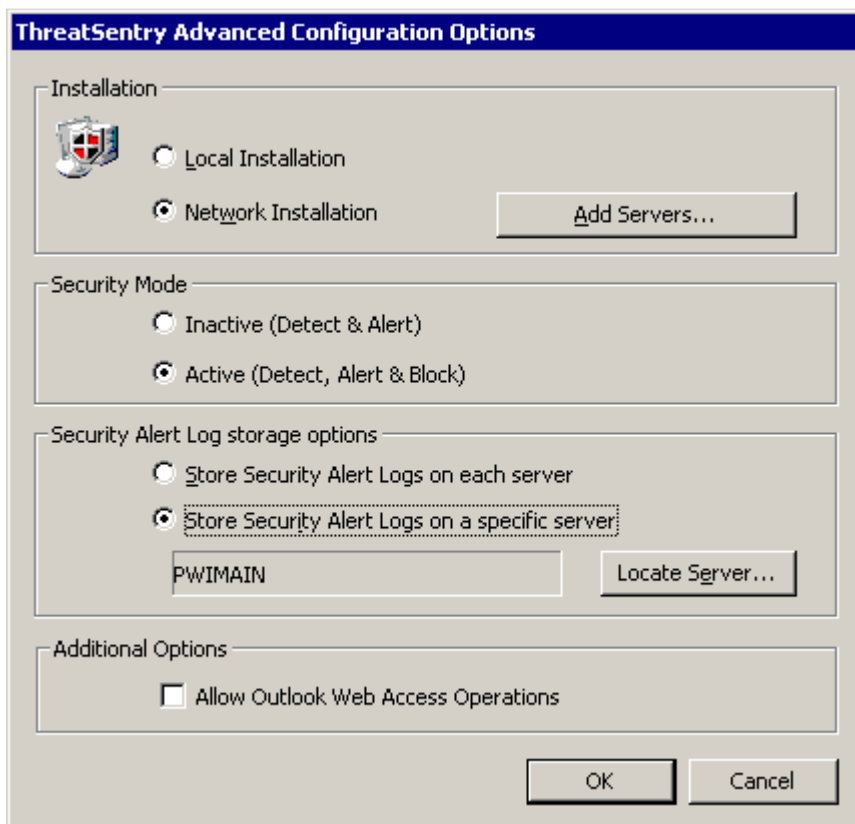


Note: It is also possible to utilize a single training database across a web farm. As another server is added and ThreatSentry is installed from the "primary" console, the file YEVS.mdb (Training Database) can be copied to the ThreatSentry Program File directory, so that training for a server that hosts the same applications to the same groups of users does not have to be established from scratch.

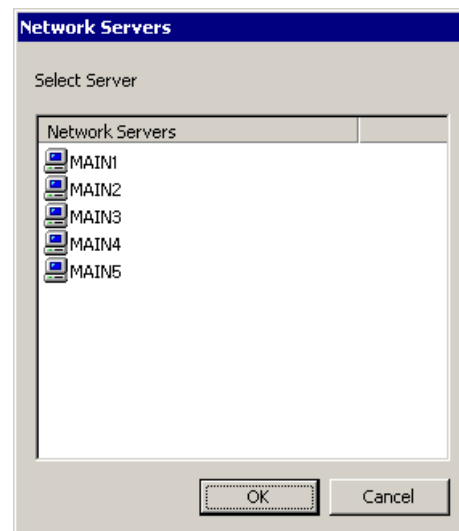
B. Security Alert Display and Security Alert Log Storage

By default, all **Security Alerts** are **displayed** on the server where ThreatSentry is installed, (regardless of the number of ThreatSentry installations). **Note: The server on which Security Alerts are displayed can be re-assigned in the Services Properties interface.** **Note:** On-screen display of Security Alerts will not be visible when accessing a server via Remote Desktop Connection (Terminal Services).

By default, **Security Alert Logs** are **stored** on each server where ThreatSentry is installed. To store Security Alert Logs in a non-default location, select the **Store Security Alert Logs on a specific server** button.



Then, identify the appropriate server from the list and click **OK**.



C. Security Modes

ThreatSentry provides three different modes of operation – aka, Security Modes; Monitoring – Inactive and Monitoring – Active and Training.

Monitoring – Inactive (Default Mode). ThreatSentry Detects and Notifies, but does not block untrusted events. This mode is enabled by default (upon installation) so that the administrator can monitor the ThreatSentry Security Alert Log for any requests that may have been blocked which should not have. Once the admin is comfortable that any related filtering rules have been adequately modified, ThreatSentry can be switched to Monitoring – Active mode.

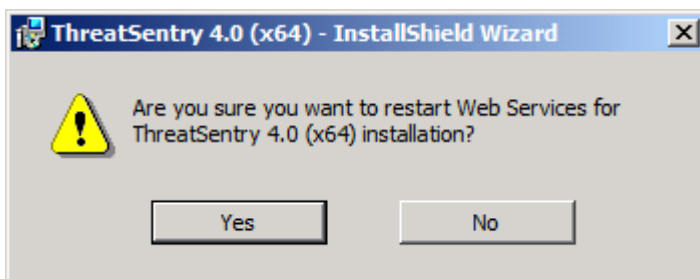
Monitoring – Active: ThreatSentry Detects, Notifies and Blocks.

Training: Training mode is specific to ThreatSentry’s Behavioral Engine (“BE”). The BE is dependent on a baseline of typical activity which is accomplished via a set of IIS requests collected in real time or from an existing IIS log file. Once the required number of training events has been collected and the baseline has been established, ThreatSentry will shift automatically into [Monitoring - Active](#) mode.

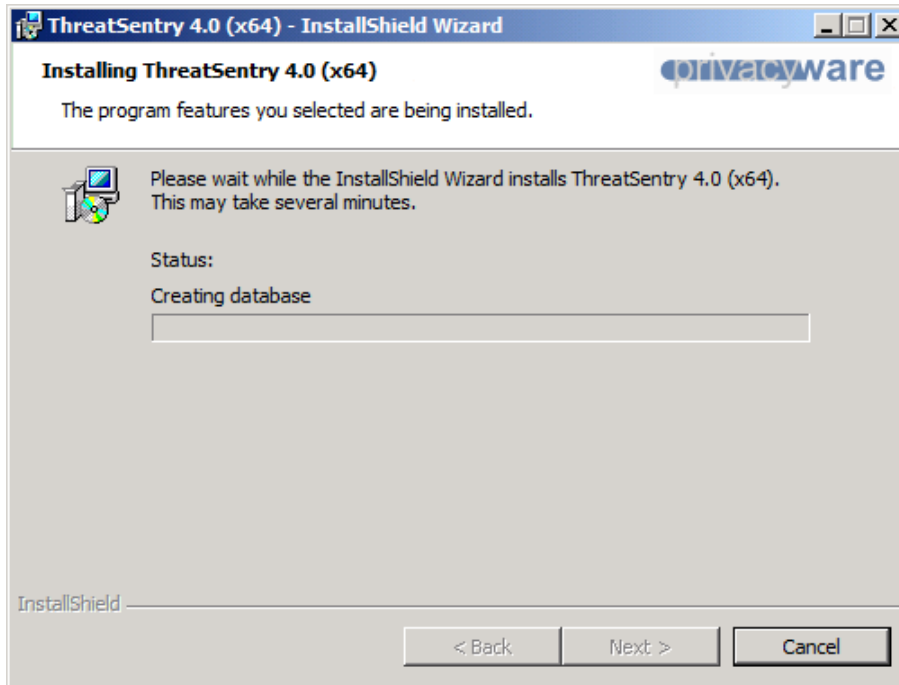
- **Active Security Mode:** ThreatSentry will **Detect, Alert, Block** and trigger whatever other preventative action has been specified (see Threat Management Options), when it classifies an event as Untrusted.



Once any Advanced Installation and Configuration Settings have been designated, you will be notified **that Web Services will be restarted...**

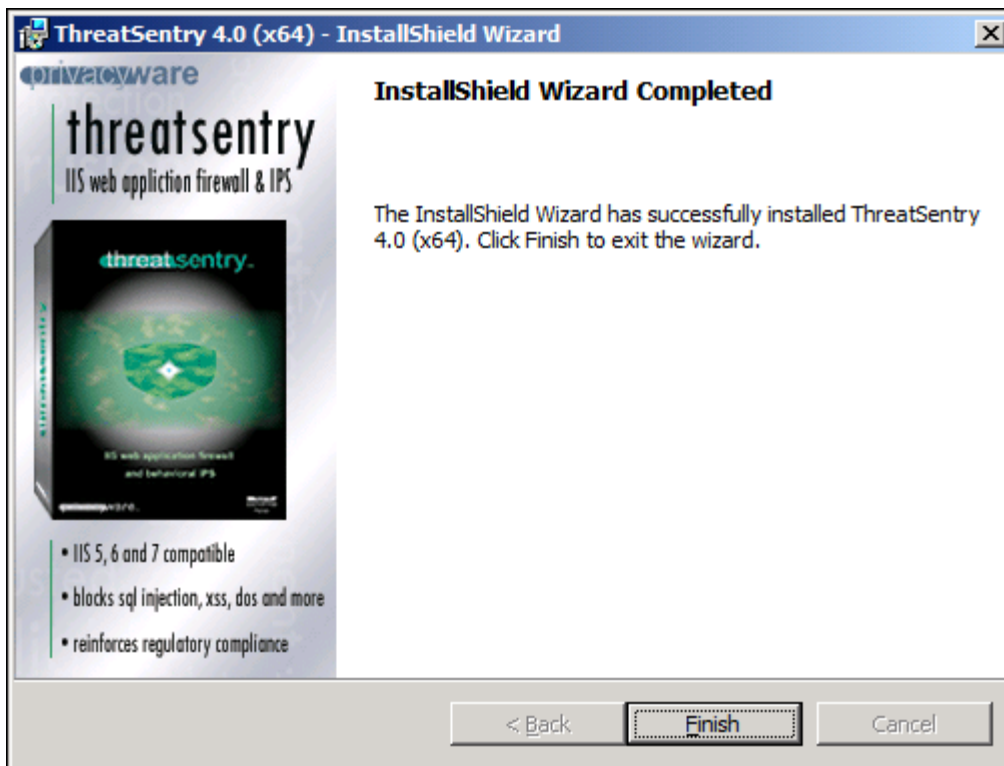


...that program features are being installed,



...and that reboot is required to activate the firewall, (but is not required to complete installation – see Threat Management Options section for more details).

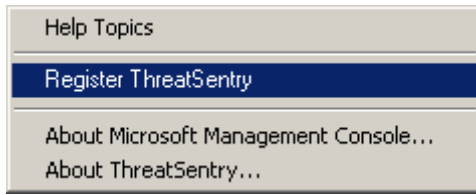
Installation is complete.



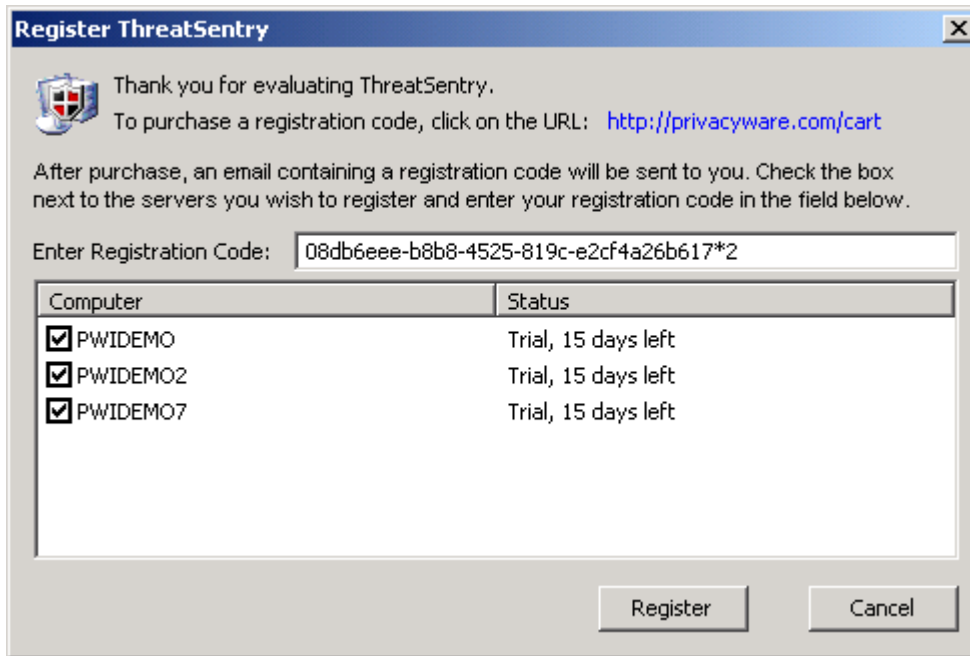
V. Product Registration

A fully functional trial version of ThreatSentry can be evaluated for 30 days. After the trial period has expired, ThreatSentry must be registered by purchasing a Registration Code. This code can be purchased at the following URL: <http://www.privacyware.com/cart>, or by contacting the Privacyware Sales Department at sales@privacyware.com.

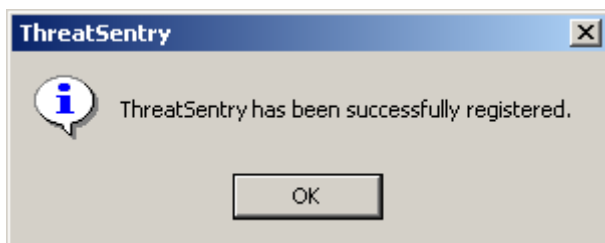
To Register ThreatSentry, Right mouse click the ThreatSentry icon in MMC and select **Register ThreatSentry**, (alternatively, Select **Action** in the **MMC main menu** and Select **Register ThreatSentry**).



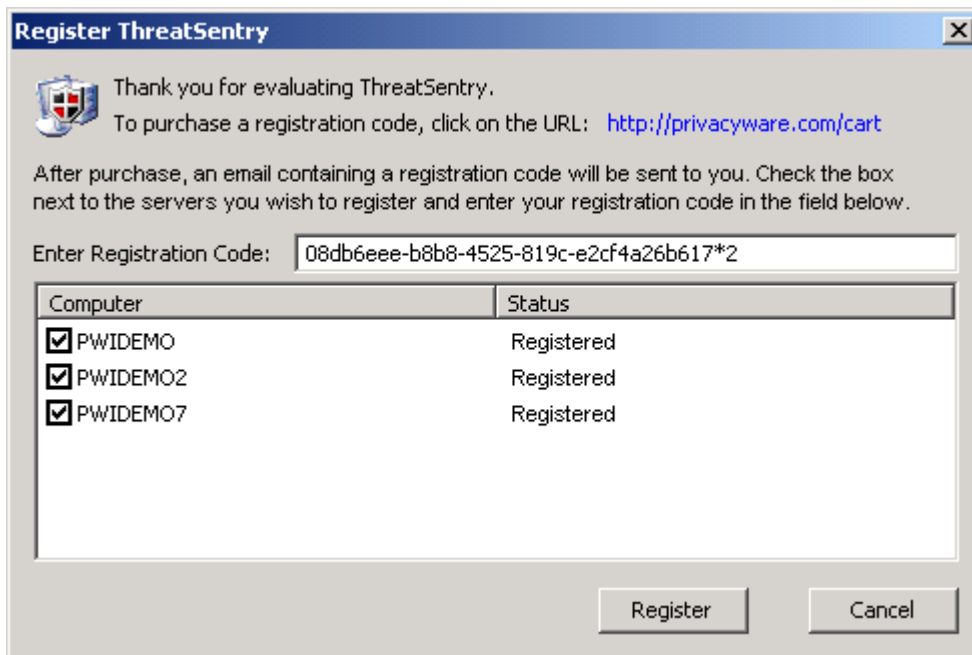
After purchasing ThreatSentry, you will receive a confirmation email with a Registration Code. The Registration Code and associated license tracking mechanism controls the number of licenses purchased and the unique software/server installations. The Registration Code will be valid for the total number of software seats that have been purchased. **Check the box** next the servers you wish to register. Enter your Registration code in the **Enter Registration Code** field and press the **Register** button.



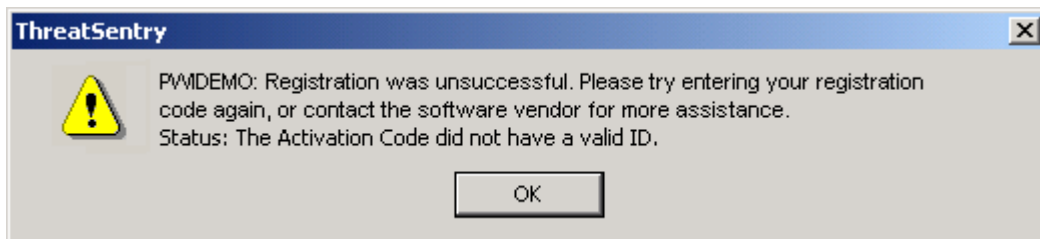
The registration information is electronically sent to Privacyware for approval. If the code is valid, the following confirmation will appear:



And the Status column will reflect the successful product registration.



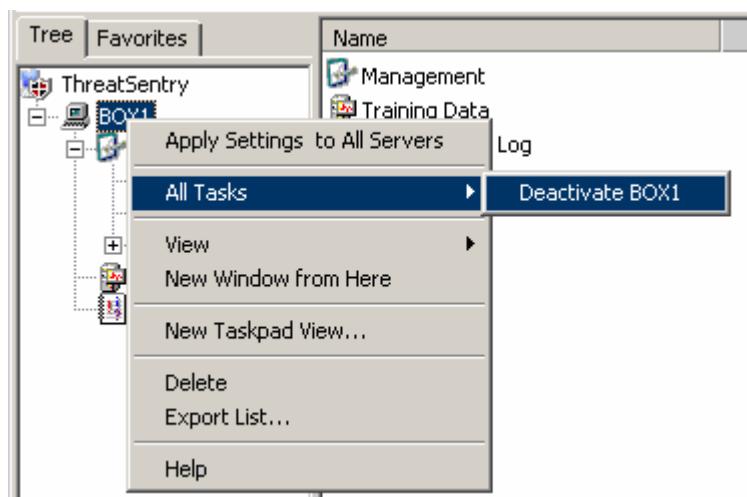
If the registration code is not valid or entered incorrectly, the following or similar screen will be displayed. Please try entering the code again, and if the problem persists, contact Privacyware support for additional assistance.



Deactivating ThreatSentry/Re-registering on a new computer

Note: Please contact Privacyware support (support@privacyware.com) before performing license deactivation.

ThreatSentry must be re-registered if it is uninstalled from one server and re-installed onto another. To re-register ThreatSentry, the license from the old server must first be Deactivated. To do so, **Right mouse-click** the server name that corresponds to the ThreatSentry installation that you wish to Deactivate. Select **All Tasks** -> **Deactivate** server name. Once this is completed, the Registration Code that was used in the original server can be utilized for registration on a new server.



If the Deactivation process is unsuccessful (e.g. if there is no Internet connection, etc.), a new Registration Code will be required to register the new installation of ThreatSentry. A new Registration Code can be obtained by contacting Privacyware. **Please be prepared to provide us with your original purchase information, including the Purchase Order number, Registration Code, and Identification information.**

[Click here to request a new Registration Code.](#)

For additional information, contact Privacyware:

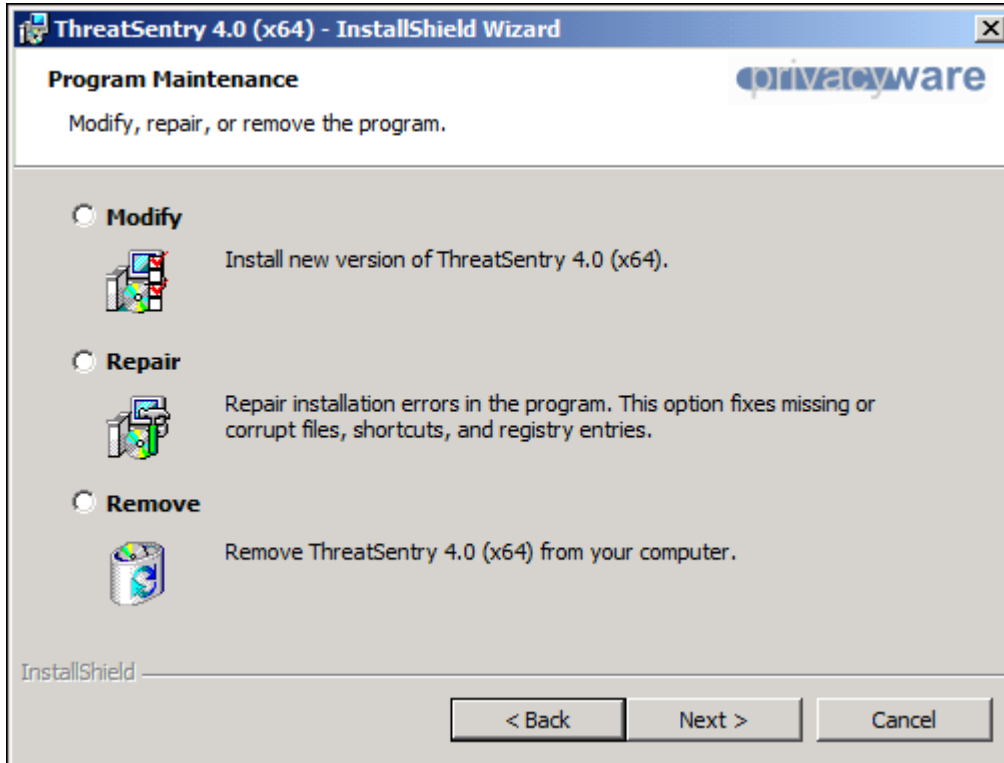
Phone: 732-212-8110

Email: support@privacyware.com

VI. Uninstalling

Uninstalling ThreatSentry is straightforward. From the **Control Panel select ThreatSentry from Add/Remove Programs** and click **Remove**. If ThreatSentry was installed on other servers remotely, make sure those servers are running and are accessible through NetBios services. This should complete the uninstall process.

ThreatSentry can also be **Modified, Repaired or Removed** by **double-clicking the ThreatSentry executable** and following the on-screen instructions as shown in the screen shot below.



VIII. Using ThreatSentry

ThreatSentry Management Console

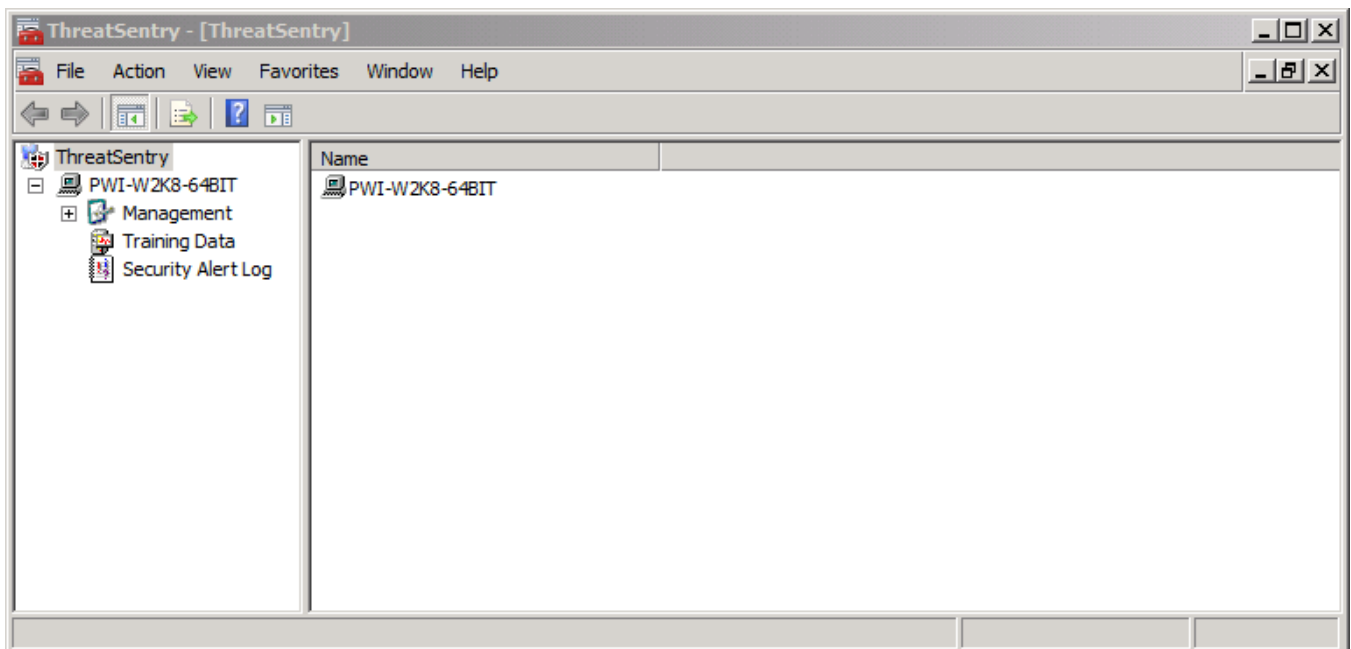
The ThreatSentry Management console allows you to control most system configuration settings and policies, and provides access to the Training Database data and the Security Alert Log. The ThreatSentry Management console can be opened by selecting the **Start Button->Programs ->Privacyware ThreatSentry->Admin Console**, or by **double-clicking the ThreatSentry desktop icon**.

The ThreatSentry management console consists of nodes accessible in the left panel:

A. Management

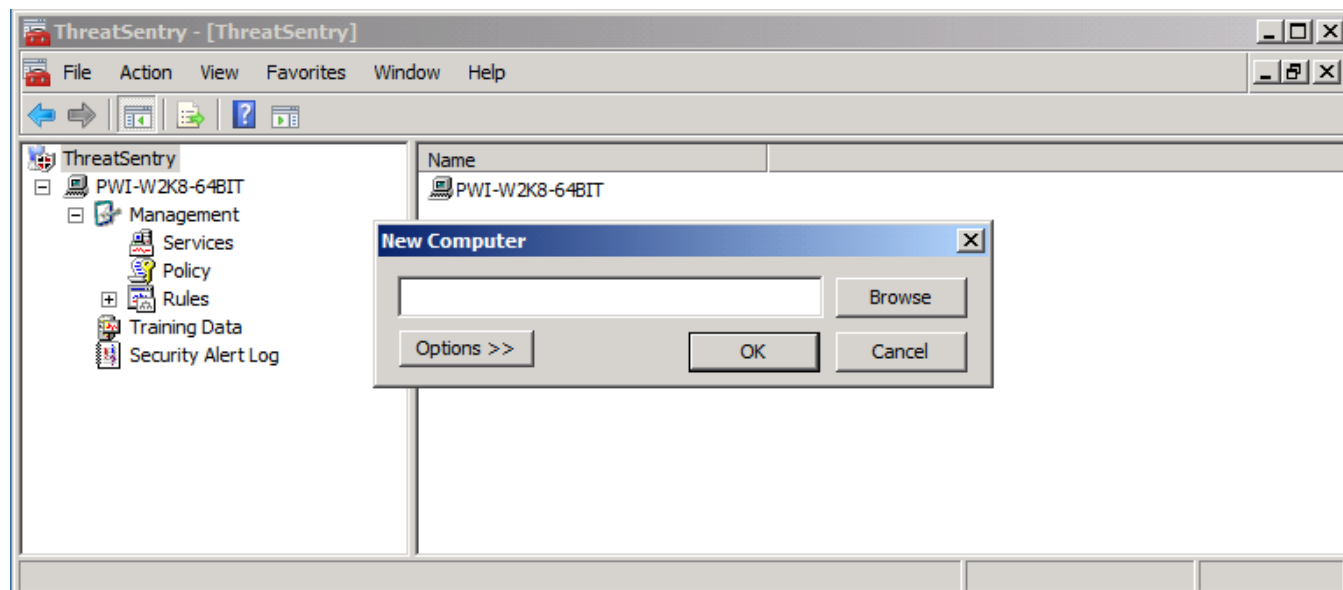
B. Training Data

C. Security Alert Log



Adding New Servers to the ThreatSentry Management Console

The ThreatSentry management console can be used to manage additional Windows servers where ThreatSentry has been installed. To install ThreatSentry on a new server, place the cursor on the **ThreatSentry tree root** (left panel, ThreatSentry) and then **right-click** and select **New -> Computer**. A Dialog box will appear as shown below. After entering the server name, click OK. A new node for the server will be added to the console.



Apply Settings to All Servers

ThreatSentry enables configuration settings established on one server to be applied to others on the network. To do so, **Right mouse-click the server name** that corresponds to the ThreatSentry settings that you would like to apply to the other servers. Then Select **Apply Settings to All Servers**. The "**Apply Settings to All Servers**" action will copy the MappingRules.xml file which contains all of the signatures and other rules, as well as the Blocked/Trusted IPs to the servers selected. If an adjustment is made to the central server (e.g. re-classified event, IP added to Blocked List, new target or header signature is added, etc.), these changes will not be reflected on the other servers unless the "Apply Settings to All Servers" action is initiated. **Note:** "Apply Settings to All Servers" will add Blocked or Trusted IPs from the Management machine to the other servers, but doesn't delete any IPs that may have been added to the other servers previously.

A. Management

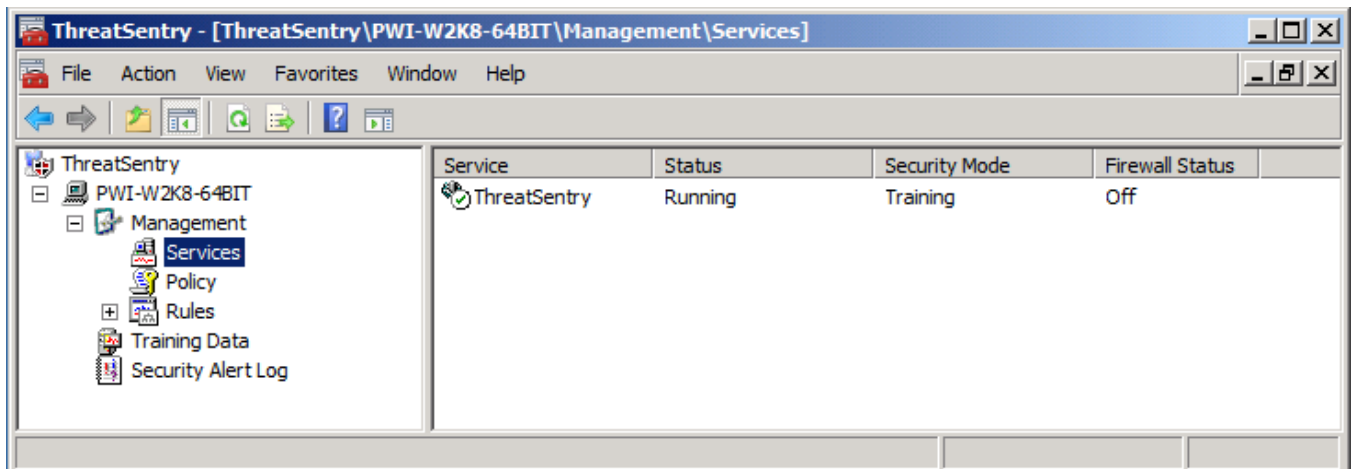
Management interfaces include three subcategories:

- **Services**
- **Policy**
- **Rules**
 - Requests
 - IP Addresses

Services

Selecting the Services node within Management will display vital information regarding ThreatSentry's status:

- Service Name: ThreatSentry
- Status: Running or Down (or Unknown)
- Security Mode:
 - Training (shown below). In this mode, ThreatSentry collects events to establish the behavioral baseline. No system protection is active.
 - Monitoring - Inactive: In this mode, ThreatSentry detects and alerts when untrusted events are identified, but will not block or take any other preventative action.
 - Monitoring - Active: In this mode, ThreatSentry detects, alerts, and blocks untrusted requests, and initiates whatever other action/s that have been designated in the Threat Management Options interface.
- Firewall Status: On/Off

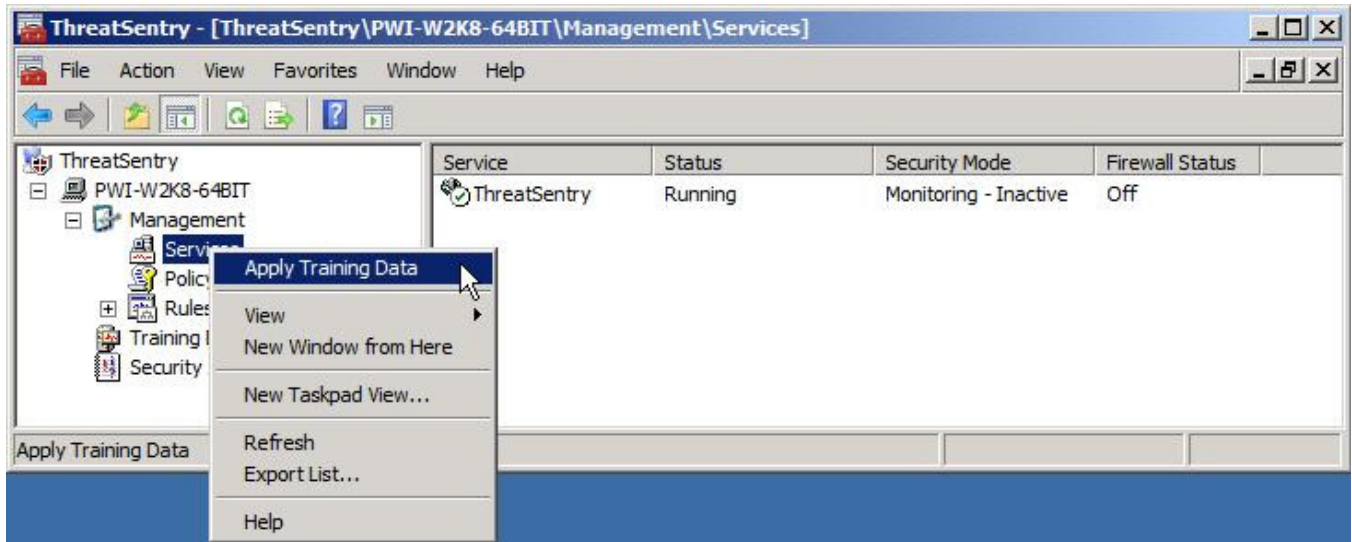


Note: After installation, ThreatSentry may not indicate that the Status is "Running" until the first HTTP request has been received by IIS.

There are two important commands available in the ThreatSentry Services interface.

1) Apply Training Data: This feature can be invoked by right-clicking on 'Services', or by selecting Action in the MMC menu (below). *Note: This option is only visible when ThreatSentry is in Monitoring Mode, (Active or Inactive).*

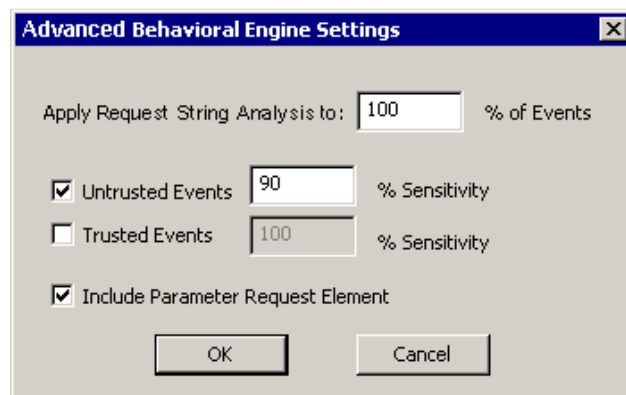
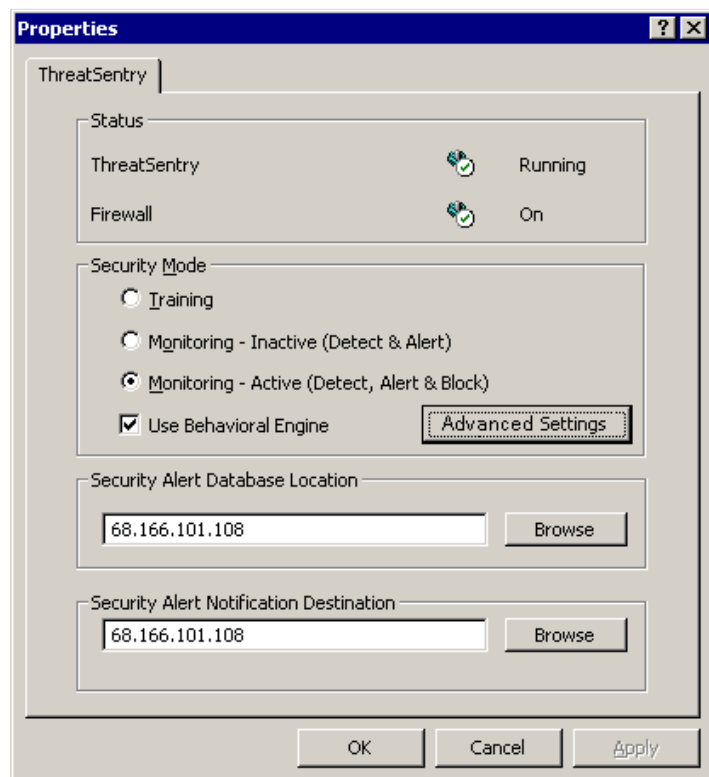
Applying the Training Data will initiate retraining of the meta-base (behavioral baseline). This process recalculates the baseline from existing training data and any event/s that have been reclassified in the Security Alert Log. For more information regarding the Security Alert Log and working with Security Alerts, please refer to the **ThreatSentry Security Alert Log** section.



2) Services Properties: ThreatSentry Services Properties can be invoked by **double-clicking** the **ThreatSentry Services** node in the **right panel of the MMC** or by **selecting ThreatSentry Service** in the **right panel of the MMC** and then **selecting Action** in the **MMC main menu**.

This interface allows you to:

- **Review ThreatSentry status.**
- **Review ThreatSentry Firewall status.**
- **Adjust the Security Mode.**
- **Turn on/off the Behavioral Engine and configure Advanced Settings**
- **Designate where the Security Alert Logs should be stored.**
- **Designate where Security Alerts should be displayed.**

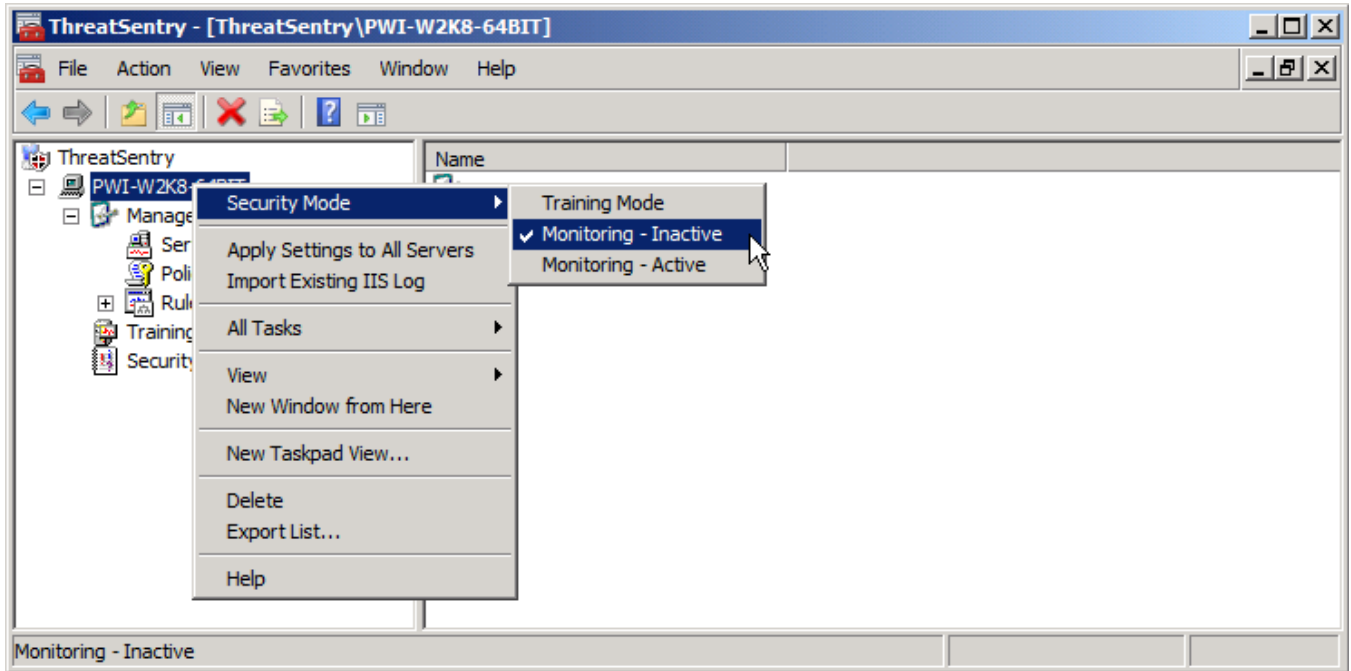


3) ThreatSentry Behavioral Engine Advanced Settings: ThreatSentry analyzes fourteen variables related to an IIS request, but pays special attention to the URL and Parameter elements. The **Advanced Settings** screen enables the manner and sensitivity with which the Behavioral Engine considers the URL and Parameter request elements to be modified.

If, for example, the Sensitivity level is set to 100%, the URL and/or Parameter elements of a request would have to be identical to the new request in order for the Behavioral Engine to classify the event as Untrusted (or Trusted).

By default, Advanced Request String Analysis is applied to 100% (small Training Database), 50% (medium) and 5% (large) of the events processed by ThreatSentry, for the URL Element of Untrusted events. The Sensitivity level is set to 90%. This means that new events comprised of URL (or Parameter) characters meeting 90% of the characters in an existing Untrusted event will also be classified as Untrusted.

Security Modes can also be managed by right clicking on the server node, then selecting Security Mode and the specific mode you would like to invoke:

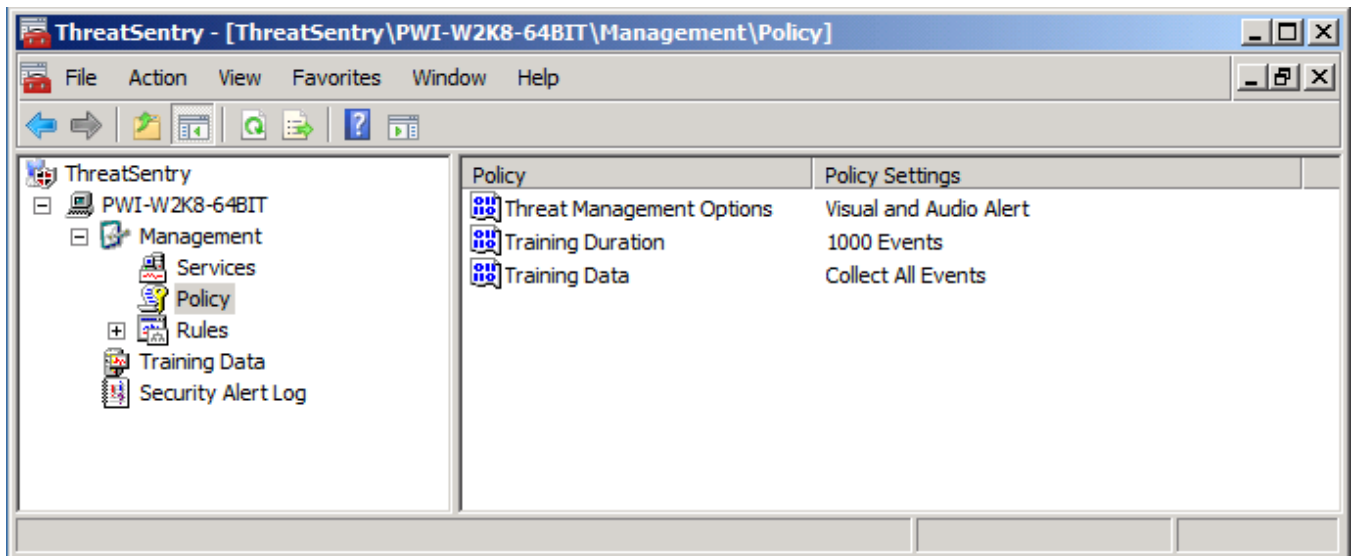


Policy

Policy interfaces provide the ability to specify what action/s ThreatSentry will trigger as untrusted events are identified, adjust the number of events to be collected in the training database, and define the types of events that should be collected.

Policy categories are displayed in the right panel of the MMC when Policy is selected. The categories include:

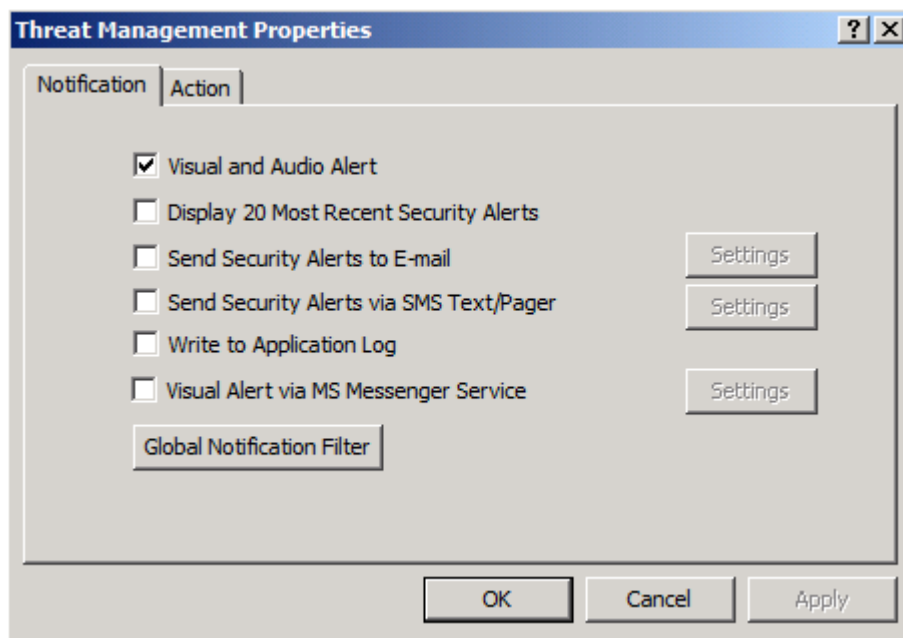
- 1) **Threat Management Options**
- 2) **Training Duration**
- 3) **Training Data**



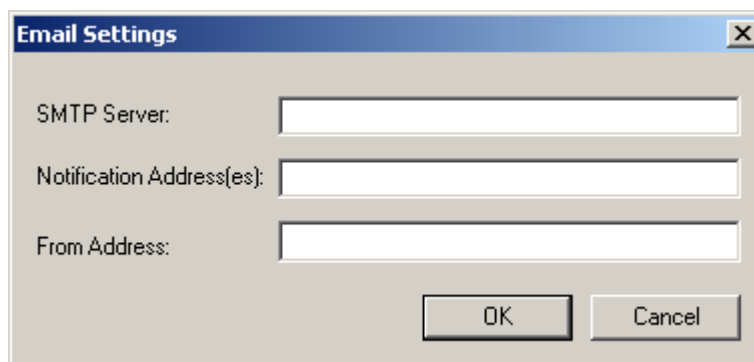
- 1) **Threat Management Options:** The Threat Management Options Properties interface allows you to manage ThreatSentry's response to events that it classifies as untrusted. To invoke the Threat Management Options Properties interface, double-click the Threat Management Options Policy node in the right panel of MMC.

Threat Management Options are divided into two categories – **Notification** and **Action**. Notification provides various options dealing with how ThreatSentry deliver notification of Security Alerts to the Administrator. Action dictates what action ThreatSentry should apply when an Untrusted Event has been identified. Options are described and shown in the screens below, (checked boxes designate the default settings).

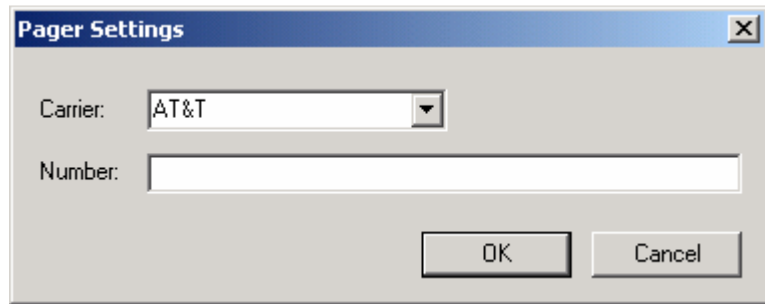
Notification



- **Visual and Audio Alert:** Generates ThreatSentry Security Alert tray pop-up, and Security Alert Event Detail and Management Options window.
- **Display 20 Most Recent Security Alerts:** Displays the 20 most recent Security Alerts as each new Security Alert is generated.
- **Send Security Alerts to Email:** Email Notification of Security Alerts can be configured.

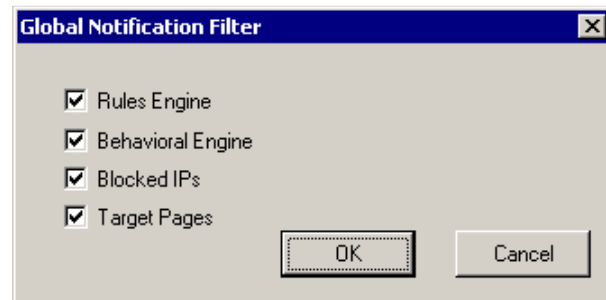


- **Send Security Alerts to SMS/Pager:** SMS and Pager Notification of Security Alerts can be configured.



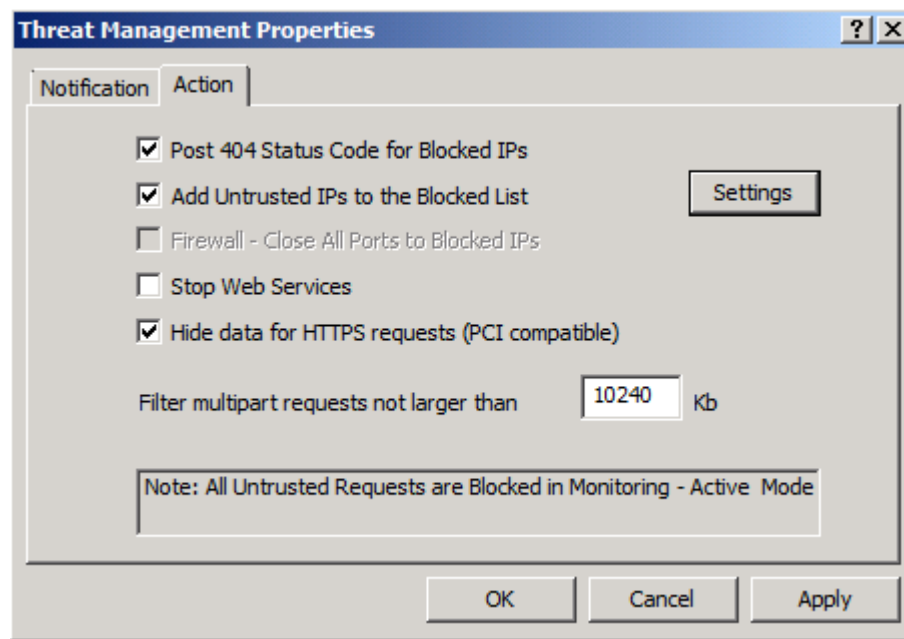
- **Write to Application Log:** Enables ThreatSentry Security Alerts to be displayed and monitored in Microsoft Operations Manager (MOM).
- **Visual Alert via MS Messenger Service:** Enables ThreatSentry Security Alerts to be displayed on PCs or servers that do not have ThreatSentry installed.
- **Global Notification Filter:** Security Alert categories can be filtered from Notification via the Global Notification Filter. By default, Notification is active for all Untrusted events.

Note: Global Filters do not take precedence over Notification defined at the individual level. Please refer to the Rules section for more information.



Action

Action dictates what action ThreatSentry should apply when an Untrusted Event has been identified. Options are described and shown in the screens below.



- **Post 404 Status Code:** Posts 404 error code to IPs on the Blocked List.

- **Add Untrusted IPs to the Blocked List:** Automatically adds IP addresses that have generated untrusted events to the Blocked IP list. No further requests from IPs on the list will be accepted.

Selecting the **Add Untrusted IPs to the Blocked List** feature within the Threat Management Options Properties interface exposes a sub-interface that allows you to qualify when an IP address should be added to the Blocked List based on the frequency that the IP generates a Security Alert within a given period of time.

Important Note: Automatically Adding Untrusted IPs to the Blocked List

When **Add Untrusted IPs to the Blocked List** is selected, ThreatSentry will automatically add any IP that generates a Security Alert to the Blocked IP List. Any new request from the same IP will be blocked and never reach IIS. In addition, any IP that has been manually or automatically added to the Blocked List will be blocked at all ports, if the ThreatSentry Firewall option has been selected.

Benefits: Adding IPs to the Blocked List automatically offers a higher level of protection as IPs generating "untrusted" events will be automatically terminated.

Considerations:

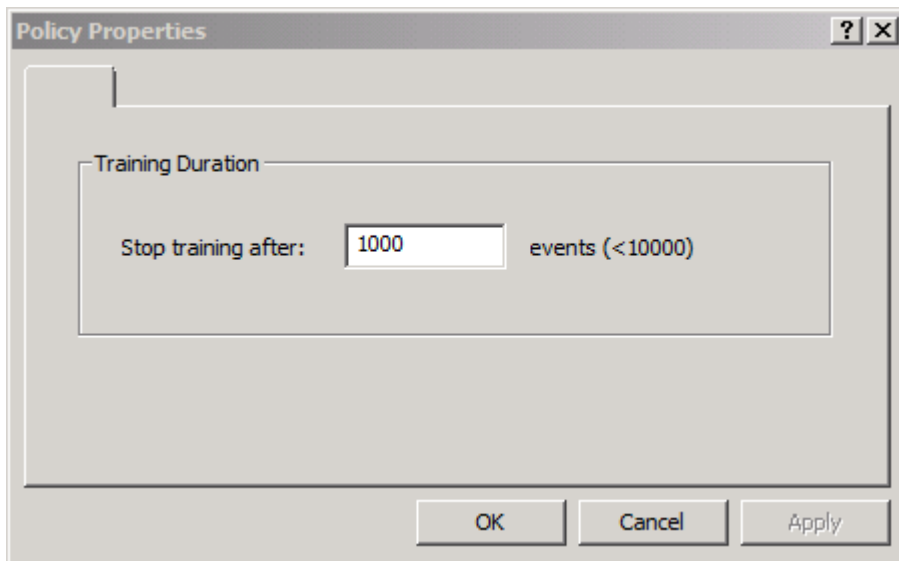
- Maintenance of the blocked IP list is critical when this feature is selected to ensure that legitimate activity is not denied. Just as important is the review and reclassification of "untrusted" events that initiated the IP's addition to the blocked list. This is especially critical during the early stages of ThreatSentry deployment as the application establishes a comprehensive understanding of typical activity within the environment. Upon review and reclassification of events, ThreatSentry should be retrained so that it assimilates the updated information.

- If "Add IP to the client Blocked List" option is not selected, the administrator can maintain the blocked IP address list manually by reviewing the Security Alert Log and adding IPs that generate "untrusted" events. ThreatSentry will block all untrusted events and generate alerts, but will not add the IP to the blocked list.

- **Firewall:** Applies an all-port firewall block for any IP that has been manually or automatically added to the Blocked List.
- **Stop Web Services:** Shuts down IIS as Security Alerts occur.
- **Hide HTTPS request data:** When checked, sensitive data will not be displayed in the ThreatSentry (Security Alert Log, Alerts, Event Details, etc.)
- **Filter multi-part requests not larger than:** Provides an ability to define a maximum size of requests that should be filtered by ThreatSentry.

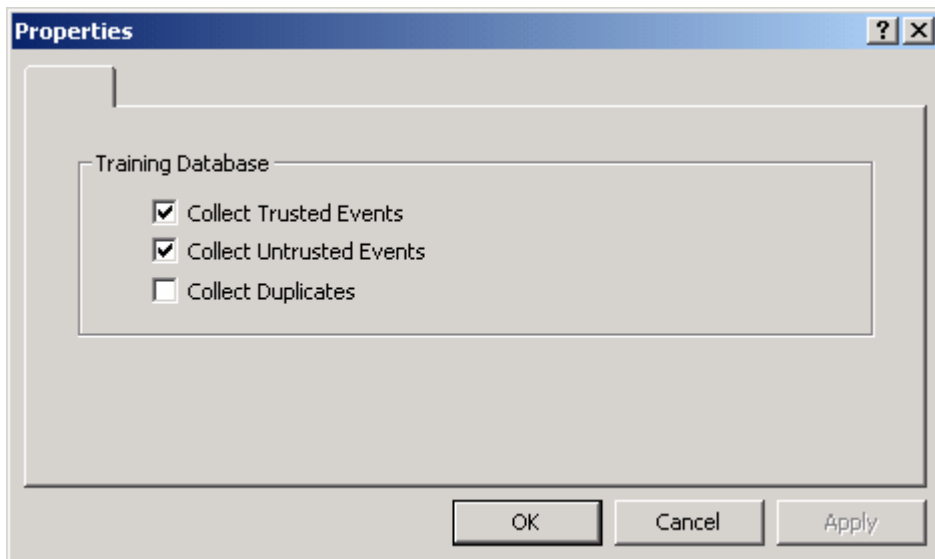
2) Training Duration:

Although ThreatSentry automatically determines the optimal number of events required for training, the training period can be adjusted manually by double-click or right mouse function and selecting Properties.



3) Database Training Events:

This properties page allows you to specify what types of events should be collected during training.



Rules

In conjunction with the behavior-based system profiling and comparative analysis engine, ThreatSentry also relies on a comprehensive knowledgebase of known hacking approaches and exploitive techniques. The knowledgebase is comprised of **signatures**, **rules**, and **parameters** that are configured based on generally accepted global policies and/or nuances of the particular system. This knowledgebase should be reviewed and tuned as necessary to ensure that trusted traffic is allowed and untrusted traffic is blocked. This section will describe the various facets of the rules-engine embedded in ThreatSentry and the rules may be modified to meet the specific requirements of your environment.

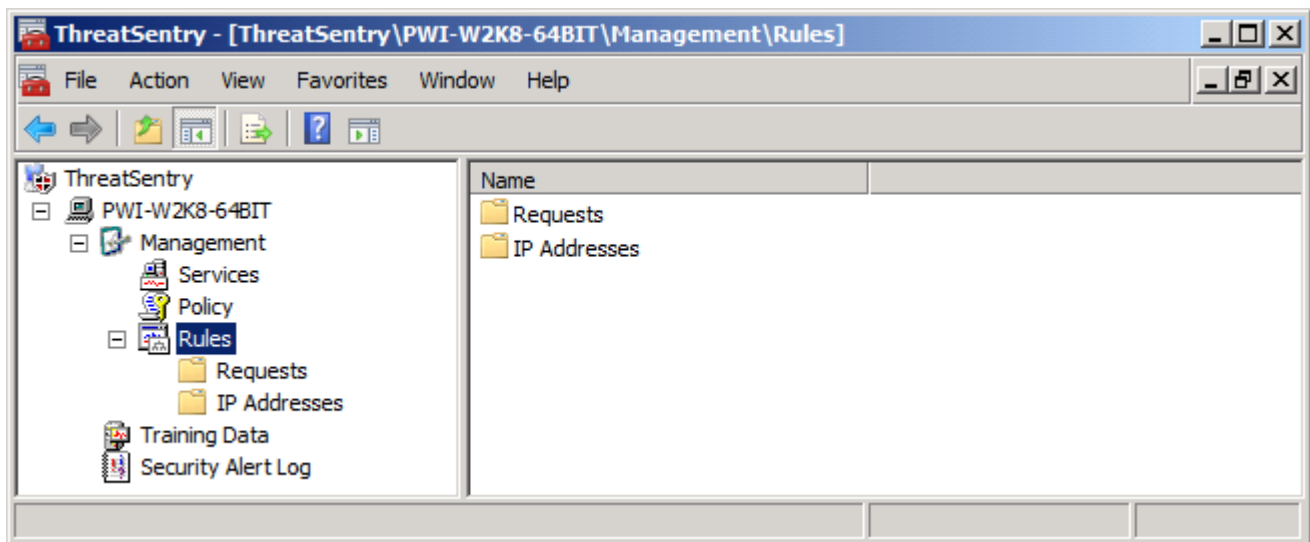
Two categories of rules exist:

1) Requests:

Enables you to define how specific elements of a request should be classified.

2) IP Addresses:

Enables you to manage Trusted and Blocked (untrusted) IPs.

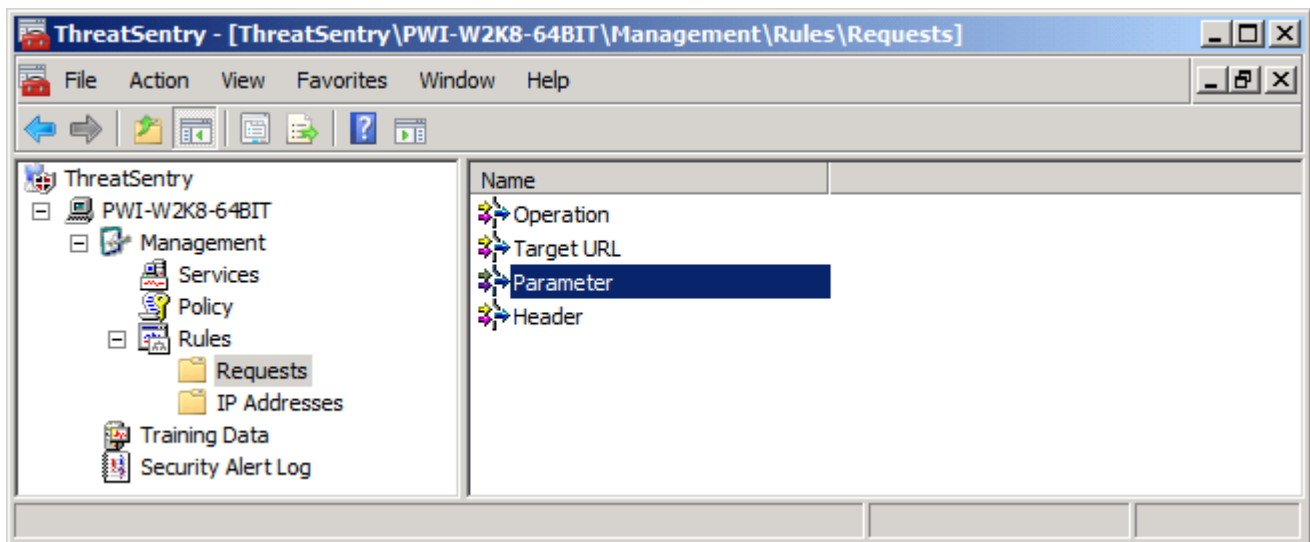


1) Requests

Defines the manner in which HTTP request elements are mapped to the multidimensional digital vector – the representation that ThreatSentry uses to organize, correlate and classify incoming requests. Elements that can be modified are displayed in the right panel when the Requests node is selected. Although relatively simple to modify, adjusting any Request element rule requires special consideration and expertise regarding ThreatSentry and the types of requests typical within the computing system. Assistance is available through the technical support team at Privacyware (http://www.privacyware.com/TS_support.html).

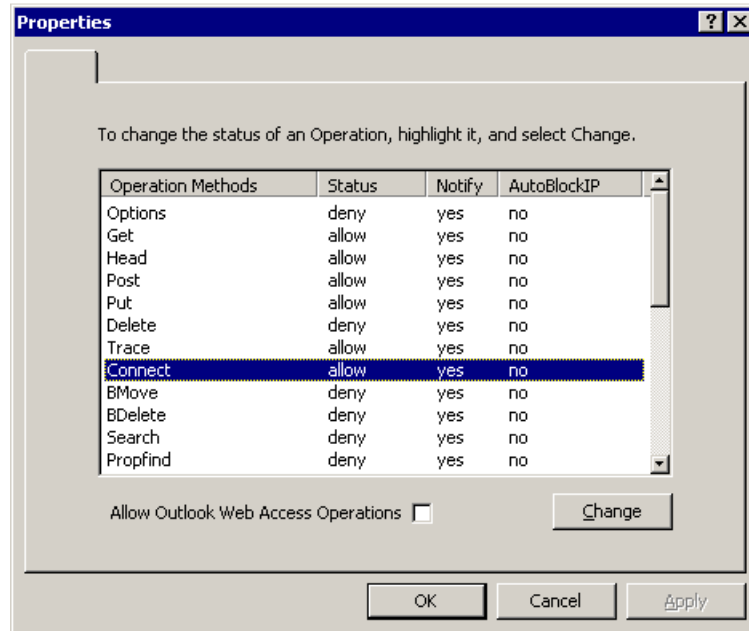
Note: Where a conflict exists, Deny Rules always supersede Allow rules. If, for example, a Deny rule specified in Parameter conflicts with an Allow Rule in Target, the Parameter Deny rule will take precedence over the Target Allow rule.

To invoke the Requests Properties screen, double-click any of the Element Names (**Operation**, **Target**, **Parameter**, **Header**) in the right panel, or right-mouse click and select properties.



Operation

Specifies whether a particular Operation method should be allowed or blocked. To change the status of an Operation method, simply highlight it and select **Change**.

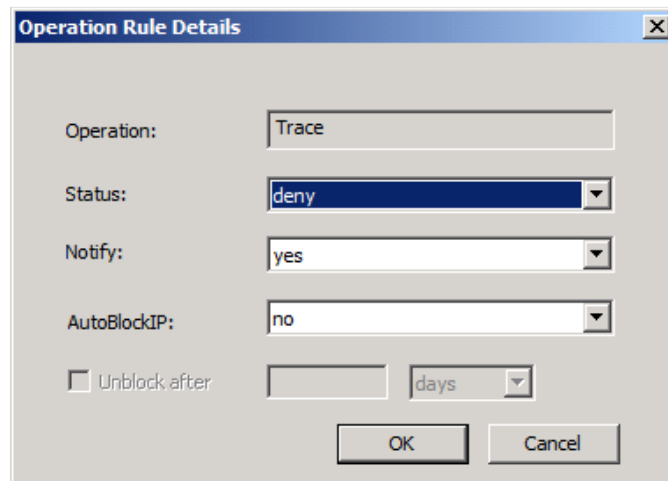


Important Note: Outlook Web Access Support

ThreatSentry is compatible with Outlook Web Access (OWA) in Exchange 2000 and 2003.

To enable OWA, simply check the "**Allow Outlook Web Access Operations**" box on the Operation screen.

OWA support must be activated prior to training. If OWA is implemented after ThreatSentry has been deployed, the existing Training Database must be deleted and a new Training Database should be created.

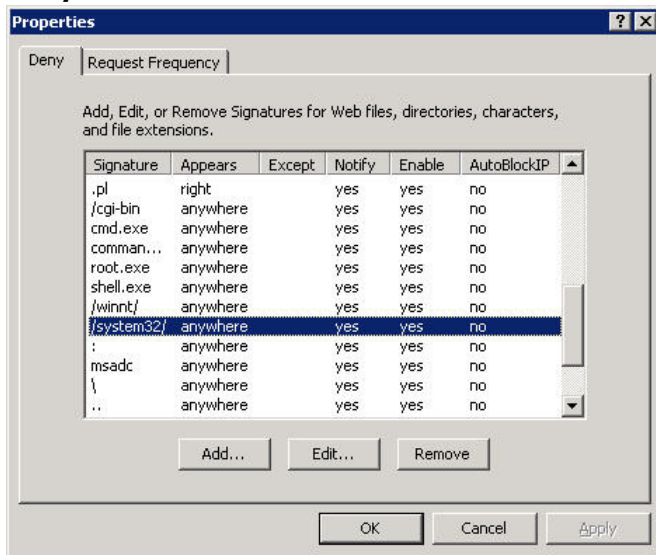


ThreatSentry offers several possibilities when changing the status of an Operation Method. The Operation may be **Allowed** or **Denied** and **Notification** can be **activated** or **deactivated**. In addition, the source **IP** generating the Untrusted event can be **added to the Blocked IP List automatically** if a Security Alert is generated. The **IP** can also be **released from the Blocked IP List** after a designated period of time has elapsed.

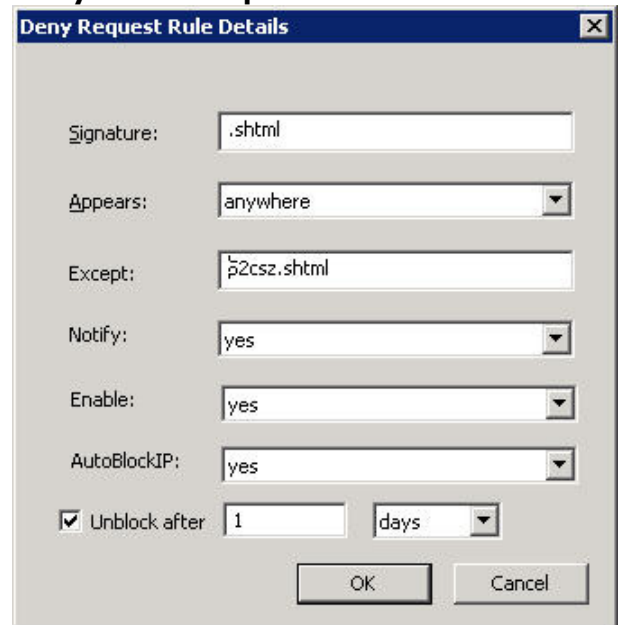
Target

Target Signatures can be **Denied** (Blocked), or **Denied with Exceptions**. Signatures may also be Added, Edited and/or Deleted.

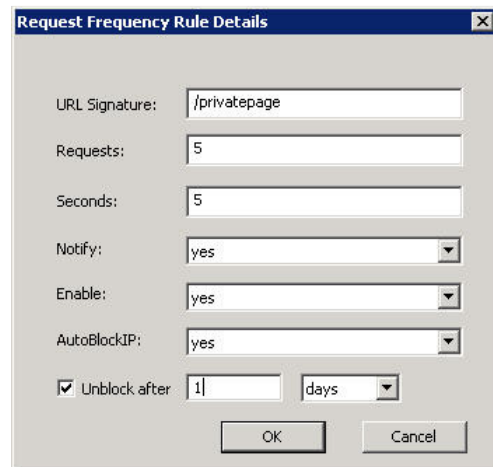
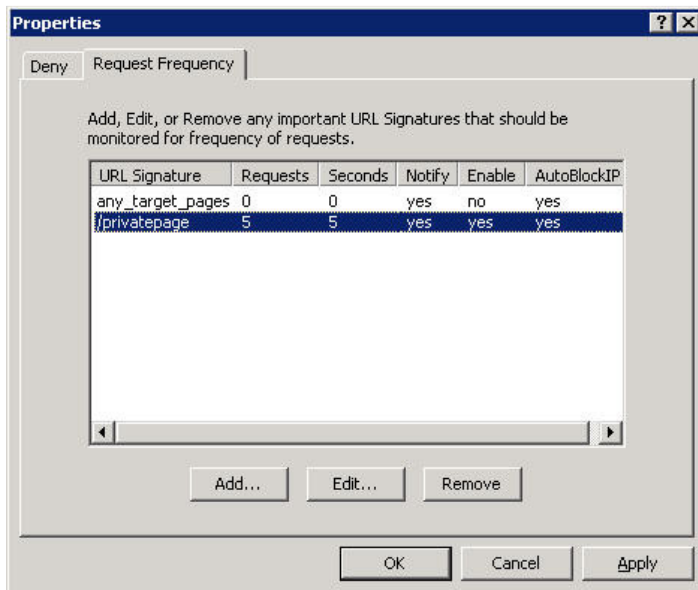
Deny



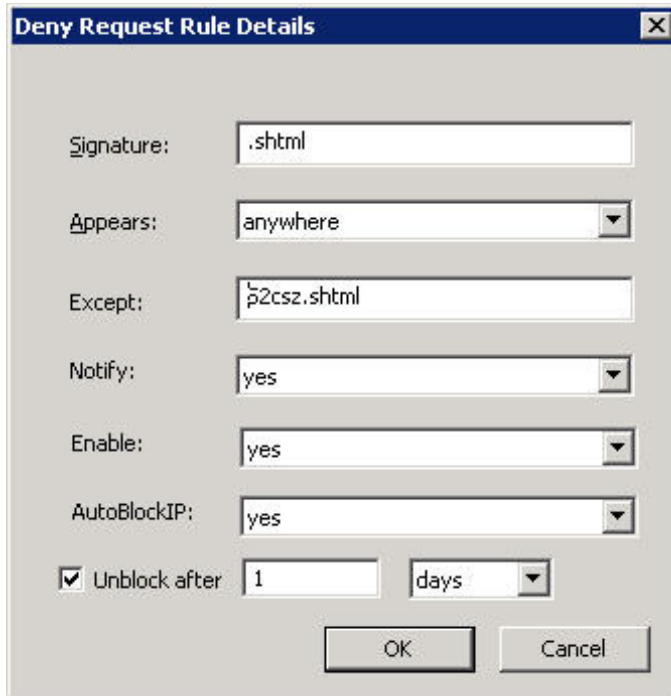
Deny with Exception



In addition to the general Target signature settings, specific rules and actions can also be applied to individual web pages via the **Target Pages** tab.



Special rules can be applied to web pages of particular interest or that require more sensitive monitoring and protection.



Deny Request Rule Details

Signature:

Appears:

Except:

Notify:

Enable:

AutoBlockIP:

Unblock after

OK Cancel

Several options are available when changing the status of a specific Target signature.

Target rules may be **Allowed** or **Denied**.

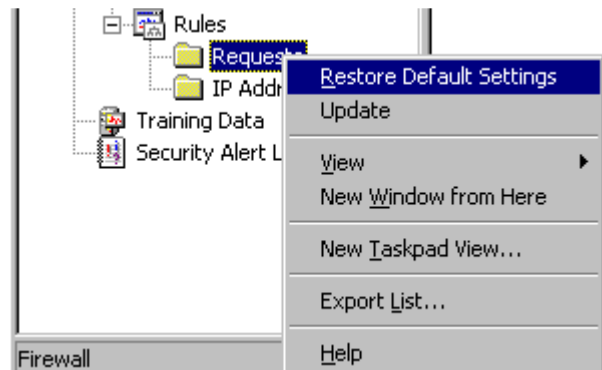
One or more exceptions may be defined for the Target and multiple exceptions may be entered and must be separated by a semi-colon ";".

Notification can be **activated** or **deactivated**.

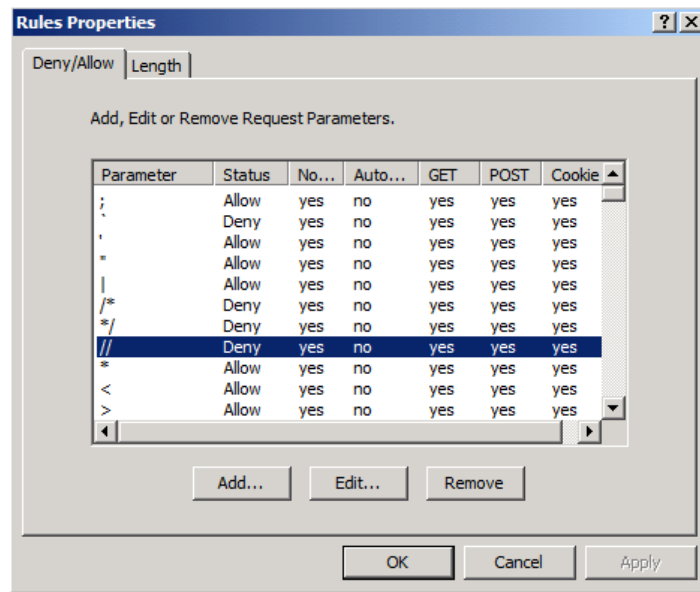
The Target rule can be Enabled or Disabled.

The **AutoBlockIP** feature will add the source **IP** generating the Untrusted event to the **Blocked IP List** automatically if a Security Alert is generated. The **IP** can also be **released from the Blocked IP List** after a designated period of time has elapsed.

Note: To reset all rules to their default settings, **right-click** the **Request Elements Mapping** node in the left panel and select **Restore Default Settings**.



Parameter



Deny or Allow rules can be applied to **Parameter** Signatures. Signatures can also be Added, Edited and/or Deleted. Parameter signatures are either allowed or denied by default and should be reviewed to ensure that they are configured properly.

ThreatSentry provides a variety of configuration options for values passed within the parameter.

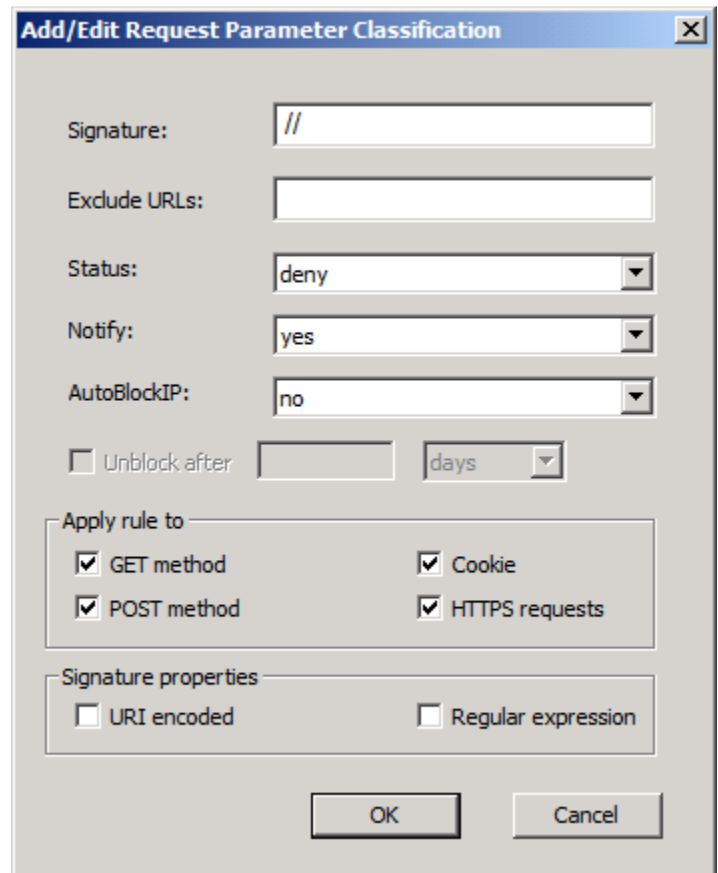
Exclude URLs: designates specific URLs that should be excluded from the rule. Multiple URLs should be delimited using ";" (e.g. /abc.html; def.php;...).

Apply Rule to: allows admin to specify to what types of requests the rule should apply.

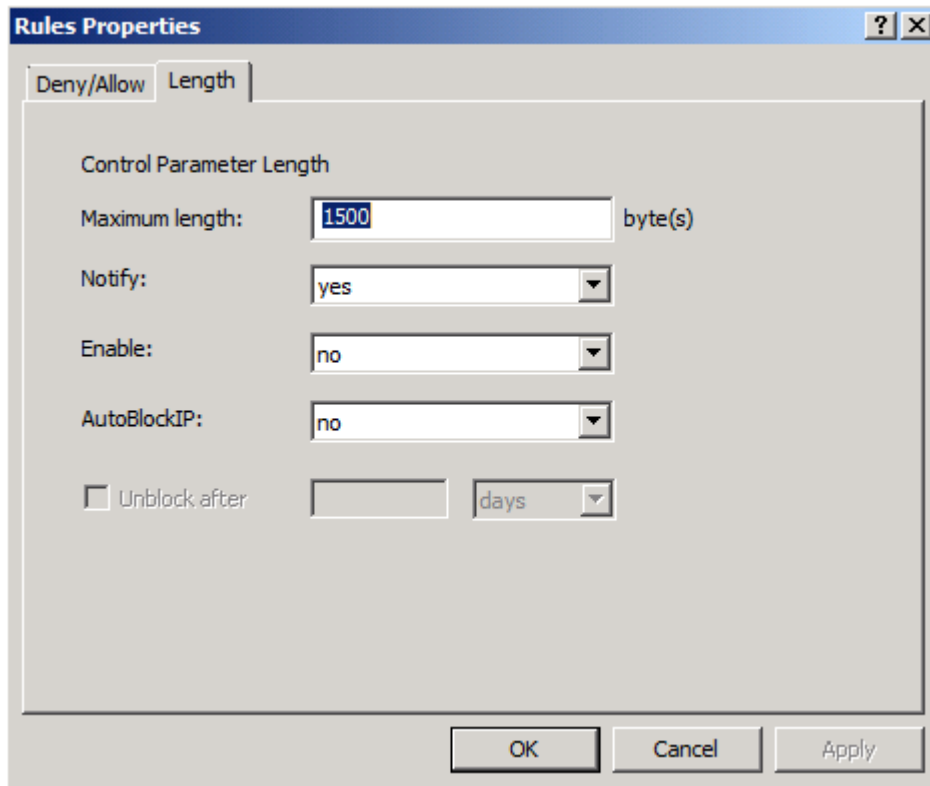
Signature Properties:

- URI encoded: URI Encoding support enables, for example, ThreatSentry to filter the "%20and%20" signature as "and".

- Regular Expression: ThreatSentry uses the Microsoft standard syntax for Regular Expressions (from ATL Server Classes library).



The Parameter threshold value defines the maximum allowable request string length. This number can be adjusted based on the request string length typical on the installed server.



The screenshot shows a dialog box titled "Rules Properties" with a "Length" tab selected. The "Control Parameter Length" section contains the following fields:

- Maximum length: 1500 byte(s)
- Notify: yes
- Enable: no
- AutoBlockIP: no
- Unblock after: [] days

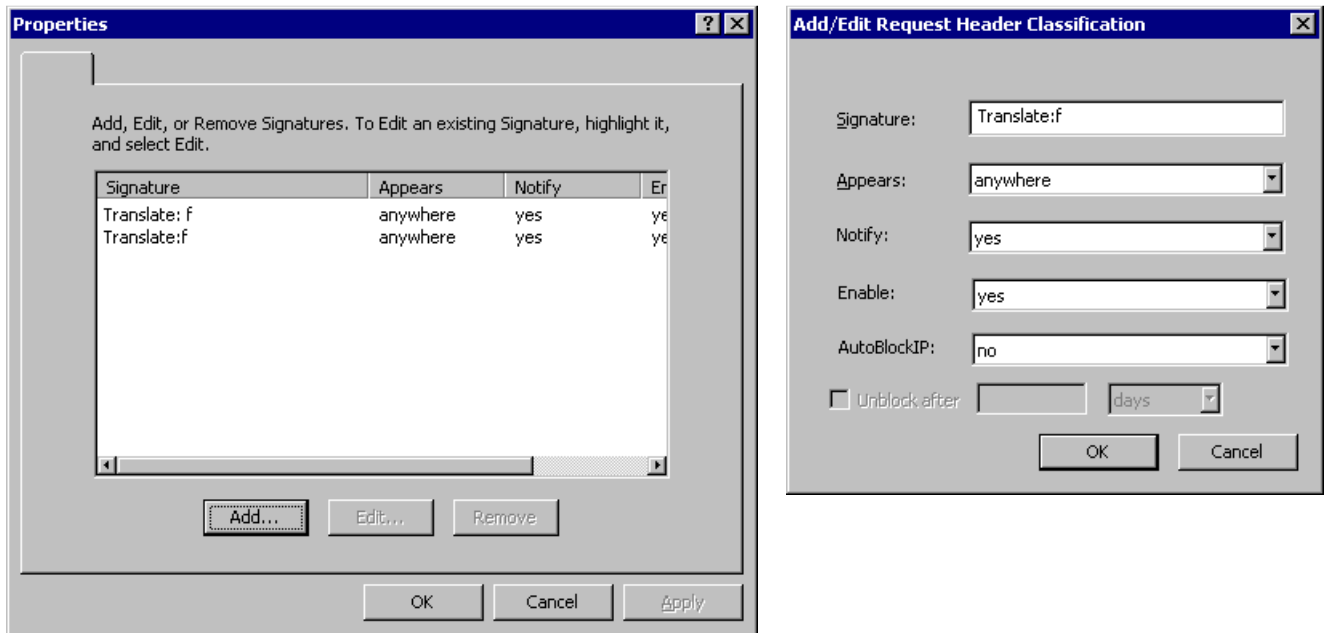
Buttons at the bottom: OK, Cancel, Apply.

In addition to the maximum request string length, the administrator can specify whether notification should be sent when an Untrusted Event matching this rule is detected. The rule itself may be enabled or disabled.

The offending IP can be added to the Blocked IP List automatically, and released after a specified period.

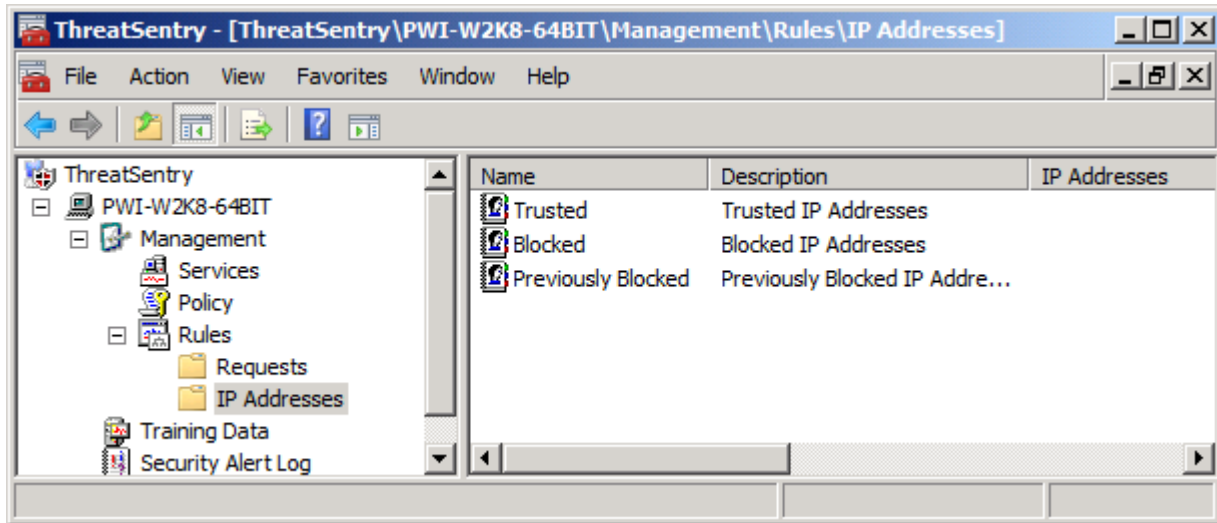
Header

Lists Request Headers that should be considered Untrusted. Request Headers can be Added, Edited or Deleted using the same features described for Operation, Target and Parameter.



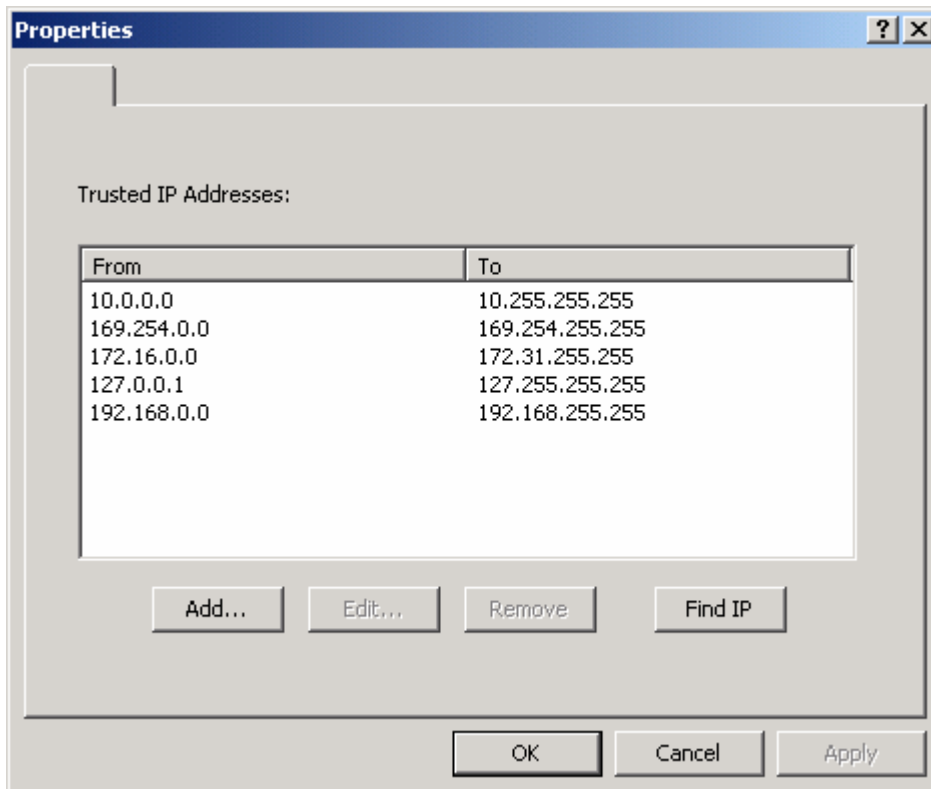
2) IP Addresses

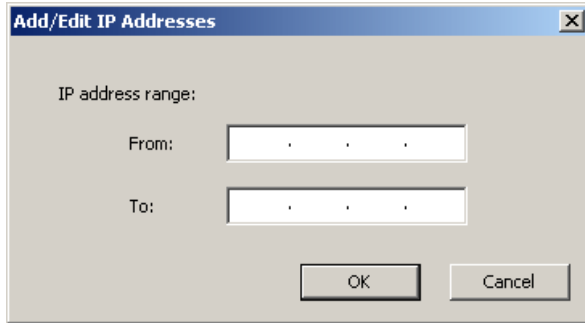
The **IP Addresses** node allows IP addresses and IP ranges to be designated as **Trusted** or **Blocked**. IPs that were at one point designated Untrusted can be viewed by double-clicking **Previously Blocked** in the right panel.



Working with Trusted IPs

Double-clicking or **right-clicking** and **selecting properties** on the Trusted IP icon will allow you to Add, Edit or Delete IP addresses from the list.

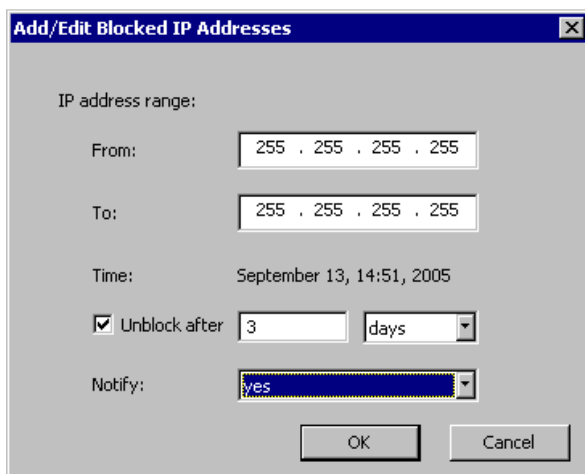
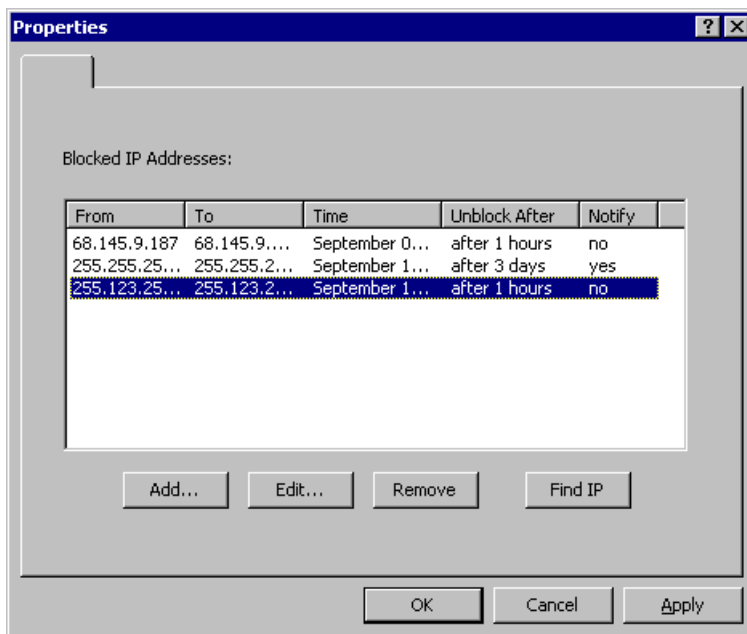




Address ranges dedicated to a particular purpose (i.e. WebDAV, Network Printer IPs or Network File Server IPs, etc.) can be added to the Trusted IPs. If the IP range is a single IP, the identical IP address should be entered into both the **From** and **To** fields.

Working with Blocked IPs

Double-clicking or **right-clicking** and **selecting properties** on the Blocked IP icon will allow you to Add, Edit or Delete IP addresses from the list.



Untrusted IPs and IP ranges can be specified in the From and To fields.

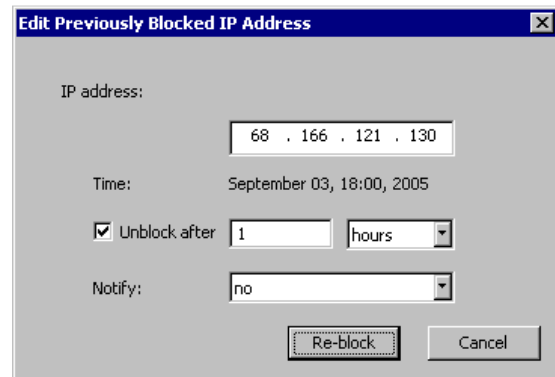
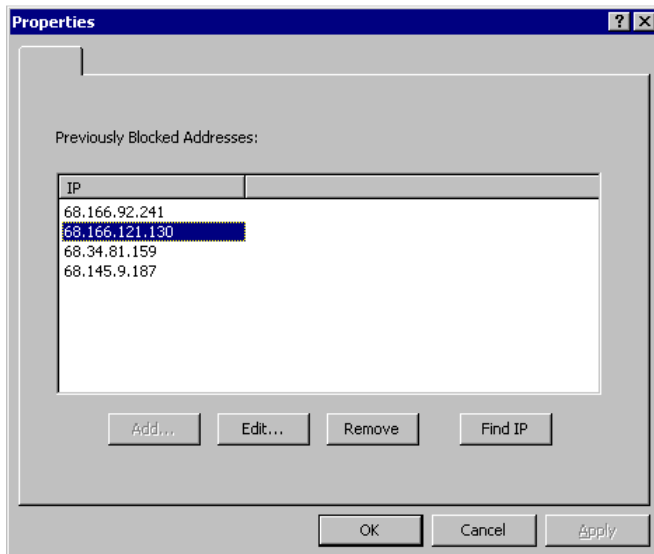
The IP/s can be released from the Blocked List after a specified time period.

The Time the IP was added to the Blocked List is recorded.

Notification can be enabled or disabled.

Working with Previously Blocked IPs

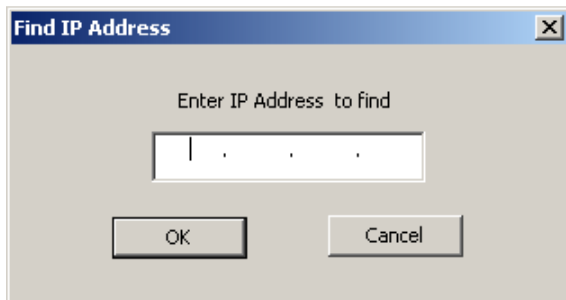
Double-clicking or **right-clicking** and **selecting properties** on the Previously Blocked IP icon will allow you to Edit or Remove IP addresses from the list.



Previously Blocked IPs can also be Re-Blocked.

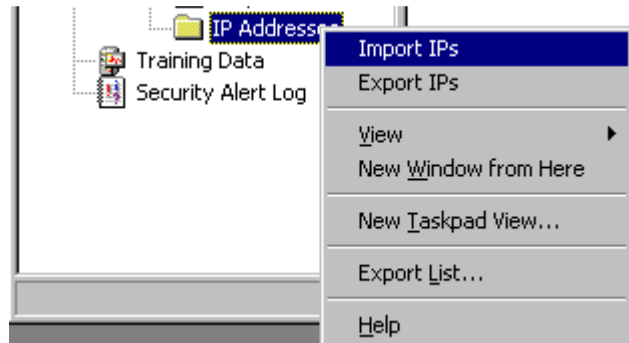
Find an IP Address

To search for a particular IP within the Blocked, Trusted or Previously Blocked list, select **Find IP** in the main Properties window.



Import IP Addresses

Blocked or Trusted IPs can also be imported by right mouse-clicking the IP Addresses folder.



B. Using the Behavioral Engine

Note: The ThreatSentry Behavioral Engine (BE) is disabled by default. Enabling the BE should be considered only after comprehensive validation of that the ThreatSentry filtering rules have been configured properly. Please contact Privacyware support for assistance: support@privacyware.com

Training Data (and Training Mode) is specific to ThreatSentry's Behavioral Engine ("BE"). The BE is disabled by default, but when activated, is dependent on a baseline of typical activity which is created by organized a set of IIS requests collected in real time or from an existing IIS log file.

ThreatSentry collects new training events "live" once training has been invoked. It is possible, however, to establish the behavioral baseline utilizing existing IIS logs. To do so, select the **Use Existing IIS logs** for training radio button, identify the IIS log path, and continue with the training process. Once the required number of training events has been collected and the baseline has been established, ThreatSentry will shift automatically into **Monitoring - Inactive** mode. Once adequate review of the training database has been completed (reclassifying events as needed), ThreatSentry can be switched to **Monitoring - Active** mode.

Note: When using existing IIS logs for training, ThreatSentry will process the log from the earliest date first. So, if a log spanning 12/1/2009-12/31/2009 is selected, and ThreatSentry has determined that 1000 events are required for the baseline, the 1000 events within the log that have the earliest dates will be used to form the baseline.

The **Training Database** forms the baseline for the BE's perspective of what is normal for your server. It is therefore important to review the events in the Training Database to ensure that ThreatSentry has classified them accurately. ThreatSentry automatically determines the optimal size of the Training Database and establishes the baseline on newly collected data or via import of existing IIS Logs. This option can be configured during installation, (please refer to Section III – Installation of this User Guide for more information) or after installation is complete, (see Training on Existing IIS Logs section at the end of this chapter).

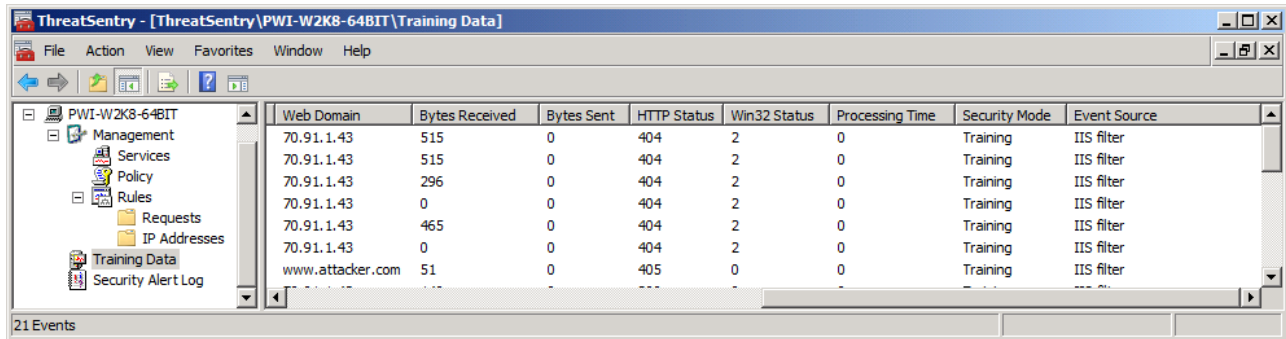
The Training Data view can be invoked by selecting the Training Data node in the left pane. By default, events are listed in the order in which they occurred, the most recent appearing on the top of the window. Events may also be sorted by column. Events displaying a **red icon** are considered **Untrusted**. Events displaying a **blue icon** are considered **Trusted**.

Training Data Display

The screen shot below shows the first eight columns that are displayed in the Training Data view: **Time, Type, Target URL (URL Path), Parameter, Operation, Source IP, Source Name and Target IP.**

Time	Type	Target URL	Parameter	Operation	Source IP	Source Name	Target IP
4/6/2010 10:10:41 AM	Predefined rules, parameters (...)	/i.cgi	*/	GET	70.91.1.129		70.91.1.43
4/6/2010 10:09:31 AM	No Rule Applied	/i.cgi		GET	70.91.1.129		70.91.1.43
4/6/2010 10:07:56 AM	No Rule Applied	/i.php		GET	70.91.1.129		70.91.1.43
4/2/2010 3:55:44 PM	No Rule Applied	/12345678910		GET	70.91.1.129		70.91.1.43
4/5/2010 10:00:30 AM	Predefined rules, target (msadc)	/msadc/msadc...		GET	70.91.1.129		70.91.1.43
4/5/2010 10:00:30 AM	Predefined rules, target (...)	/scripts/..Ã~.....		GET	70.91.1.129		70.91.1.43
4/5/2010 10:00:30 AM	Predefined rules, header (tran...	/iisstart.asp		GET	70.91.1.129		70.91.1.43

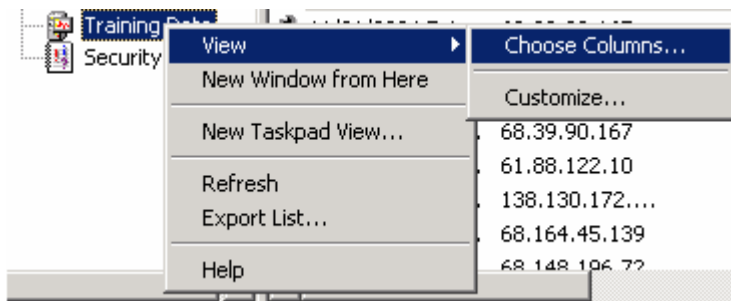
The following screen shows the other columns in the Training Data view: **Web Domain, Bytes Received, Bytes Sent, HTTP Status, Win32 Status, Processing Time, Security Mode and Event Source.**



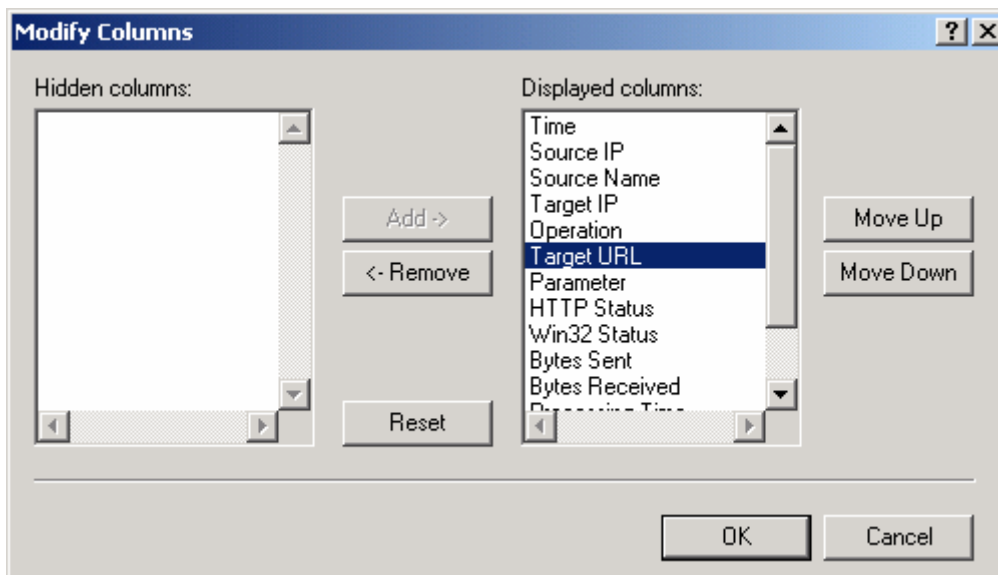
The screenshot shows the ThreatSentry interface with the Training Data view. The table displays the following data:

Web Domain	Bytes Received	Bytes Sent	HTTP Status	Win32 Status	Processing Time	Security Mode	Event Source
70.91.1.43	515	0	404	2	0	Training	IIS filter
70.91.1.43	515	0	404	2	0	Training	IIS filter
70.91.1.43	296	0	404	2	0	Training	IIS filter
70.91.1.43	0	0	404	2	0	Training	IIS filter
70.91.1.43	465	0	404	2	0	Training	IIS filter
70.91.1.43	0	0	404	2	0	Training	IIS filter
www.attacker.com	51	0	405	0	0	Training	IIS filter

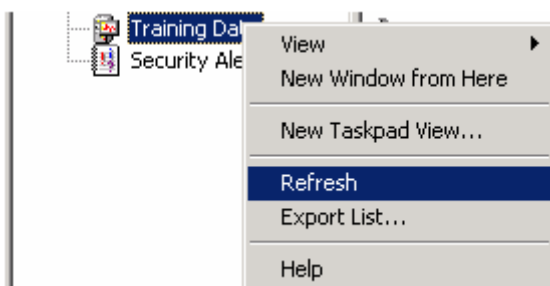
The columns displayed in the Training Data view can be modified by **right mouse clicking the Training Data node** and selecting **Choose Columns**.



The following screen will be invoked allowing columns to be added, removed, or displayed in different orders.

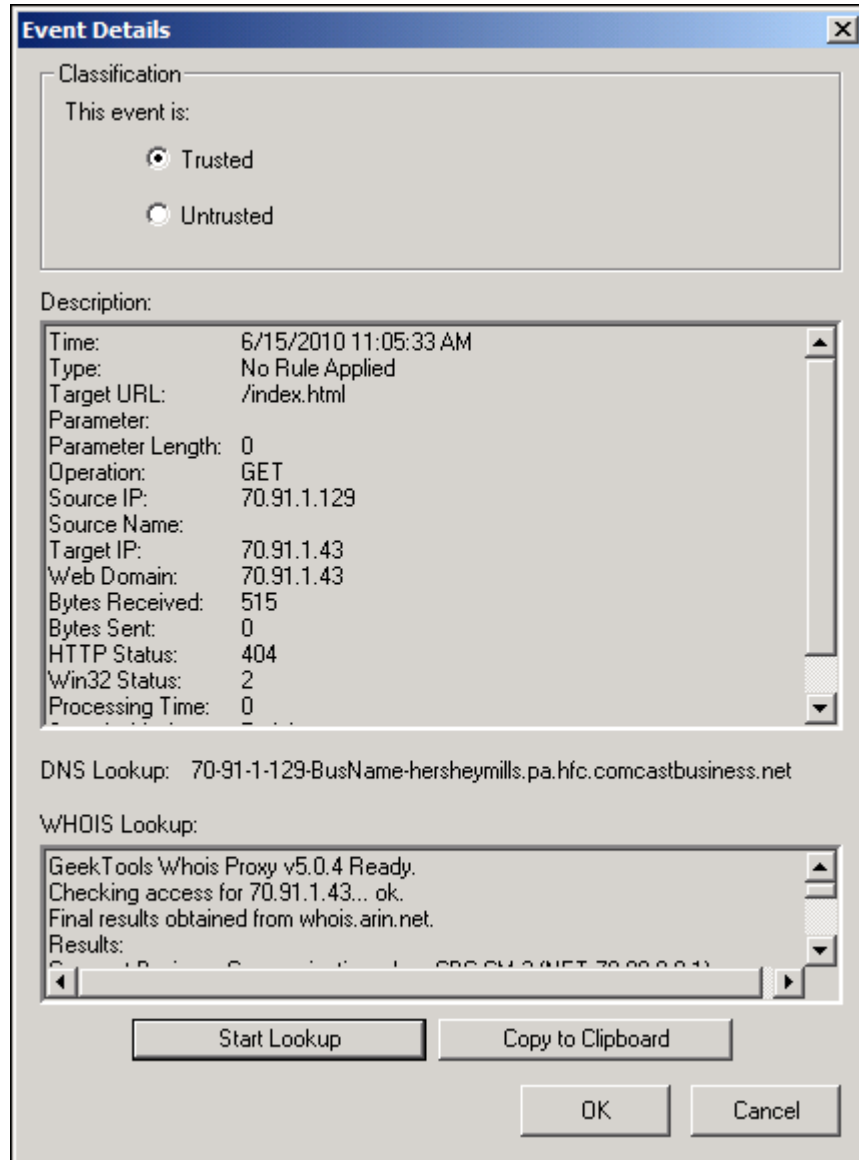


You may also **Refresh, View** or **Export** the Training Data to another location by Right mouse-clicking the **Training Data** node in the ThreatSentry tree root.



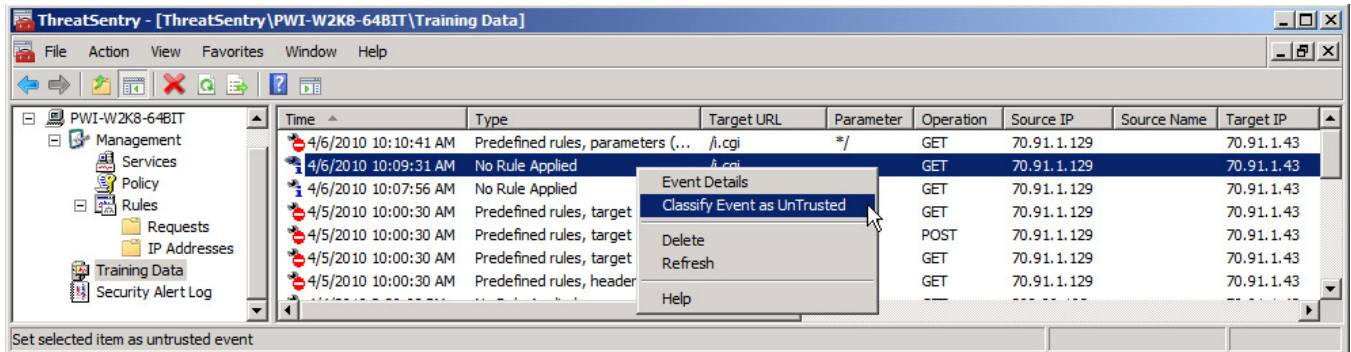
Training Data Details

Double-clicking a training event will invoke a window that displays **details about the event**, the **ability to reclassify the event**, and a **WHOIS Lookup** capability. The WHOIS information can be copied to the clipboard, and pasted to a word processing application, spreadsheet or other relevant form.

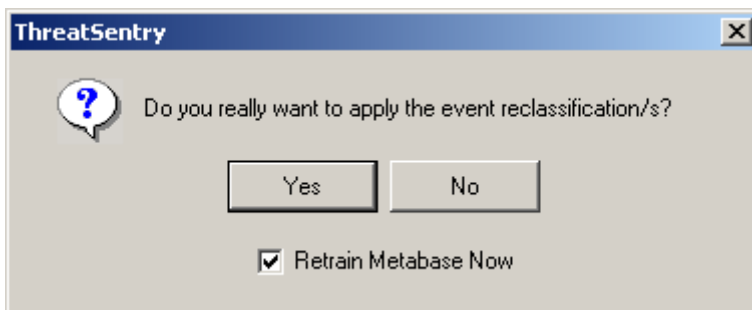


Note: Events will not be added to the Training Database if generated from an IP on the Trusted IP List.

Right-mouse clicking a single event or group of events in the **Training Database** enables you to **display Event Details, Re-classify Events**, and/or **Add IPs to the Blocked List**. To reclassify multiple events, hold down the SHIFT or CTRL key to select a set of events and apply the right mouse button to reclassify.



Once events have been reclassified, ThreatSentry will prompt you to apply these changes and retrain the metabase. **Retraining of the metabase requires that the ThreatSentry NT service be restarted. Event re-classifications will not take affect unless the baseline has been re-trained.**



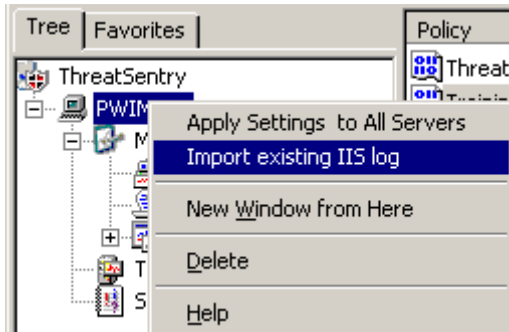
Events that have been reclassified from **Untrusted** to **Trusted** will be designated with a small arrow at the left of the blue icon.

Events that have been reclassified from **Trusted** to **Untrusted** will be designated with a small arrow at the left of the red icon.

If for some reason event reclassifications are not applied immediately, the baseline can be retrained later by right-clicking **Management ->Services** and selecting **Apply Training Data**.

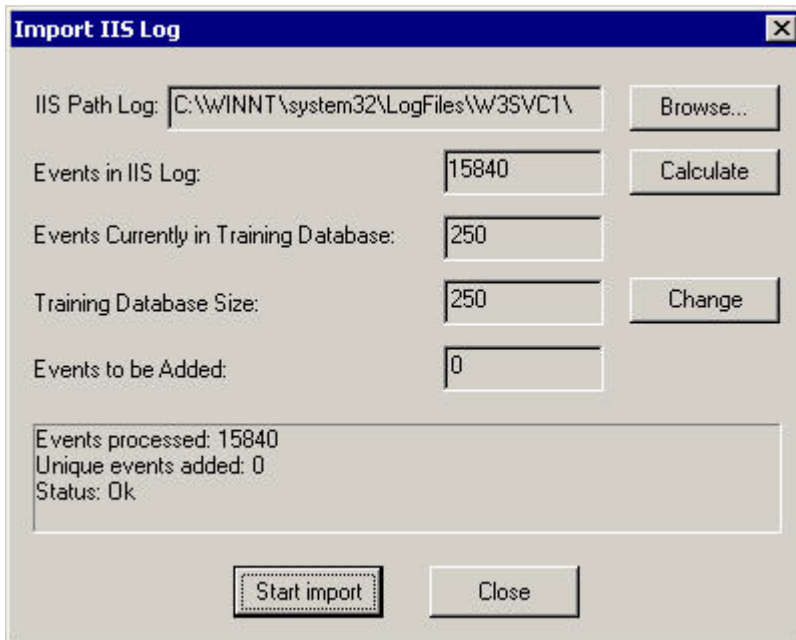
Training on Existing IIS Logs

Existing IIS logs can be used by ThreatSentry to establish a behavioral baseline.



To do so, **Right-mouse click the server name** and select **Import Existing IIS Log**.

The screen below will be invoked that will allow you to Calculate the number of events in the IIS log, the number to import based on the difference between the events already collected and the limit established by the Training Database size (which can also be increased as needed). Once the import settings have been defined, click the Start Import button to commence the log import.



Then select Start Import. ThreatSentry will process the imported logs or events in the same manner that it processes events that are collected normally after installation. Once Training is complete, ThreatSentry will shift into Monitoring Mode.

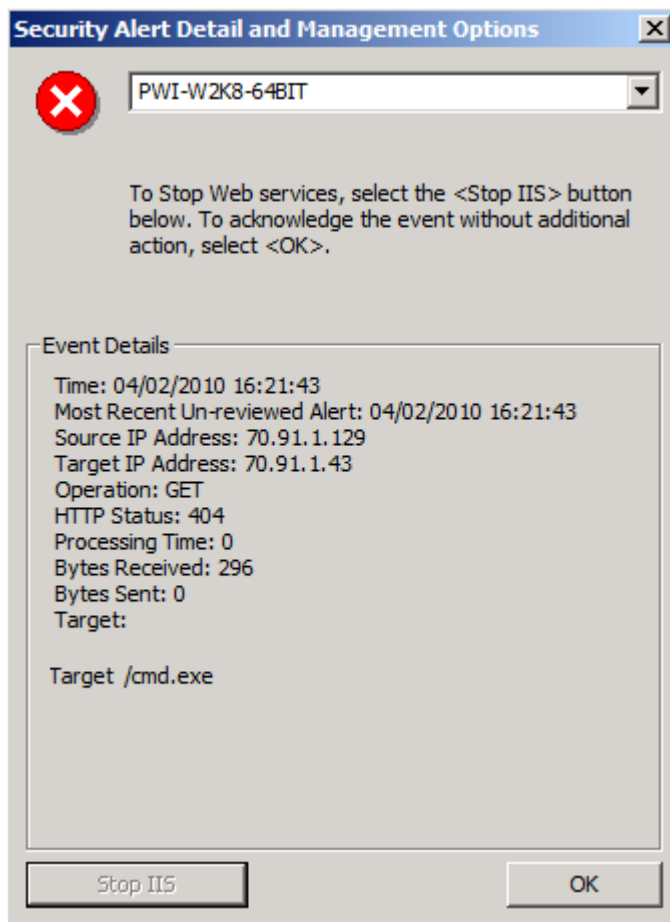
When using existing IIS logs for training, ThreatSentry will process the log from the earliest date first. So, if a log spanning 12/1/2009-12/31/2009 is selected, and ThreatSentry has determined that 1000 events are required for the baseline, the 1000 events within the log that have the earliest dates will be used to form the baseline.

C. Security Alerts & the Security Alert Log

Note: IIS logging must be enabled on all Web sites to support ThreatSentry Security Alert Log functionality.

Security Alerts

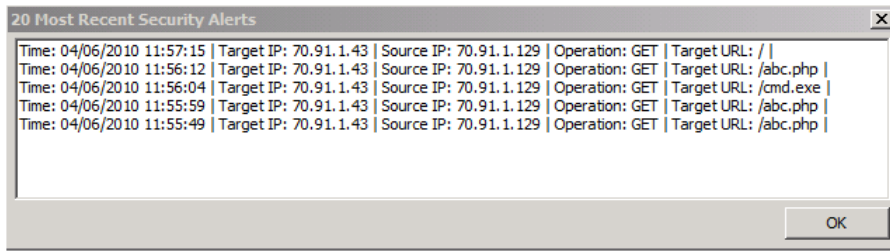
Two types of alerts appear as "untrusted" events are identified. A ThreatSentry Security Alert pop-up balloon will appear from the tray (below right) and the Security Alert Event Detail and Management Options window, (below left). The latter displays details of the untrusted event and actions that can be taken in response to the alert.



- Selecting **OK** will simply acknowledge the event and eliminate the window.
- If the event has been misclassified, the **Security Alert Log** should be reviewed and the event reclassified. The Security Alert Log can be viewed by double-clicking the Security Alert Balloon or selecting the Security Alert Log in the main menu tree.
- If the event and/or environment are critical, IIS can be stopped immediately.

If the "Display 20 Most Recent Security Alerts" option has been selected in Threat Management Options, the interface below will also be displayed when Security Alerts are generated.

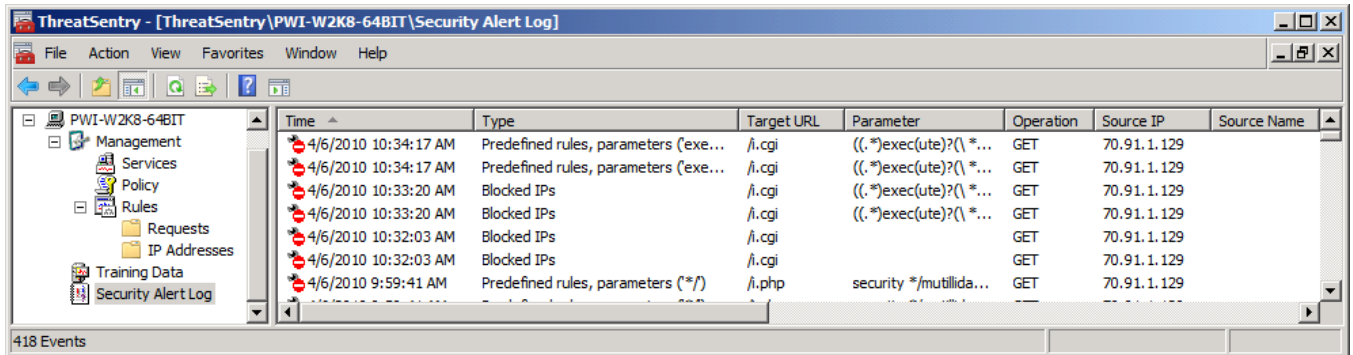
Once the Security Alert has been acknowledged, one final window will appear.



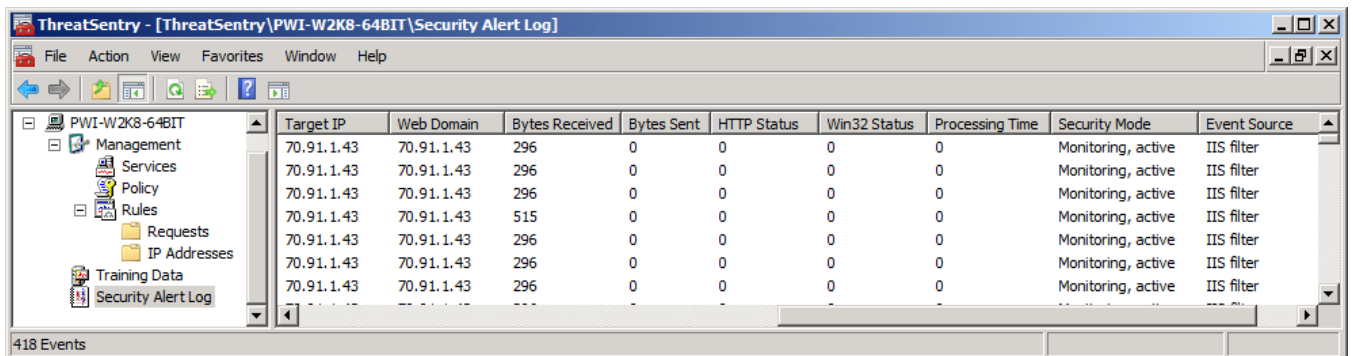
Security Alert Log

The Security Alert Log can be displayed by selecting the Security Alert Log node in the left pane. Untrusted Events are listed in the order in which they occurred, the most recent appearing on the top of the window. Events may also be sorted by column.

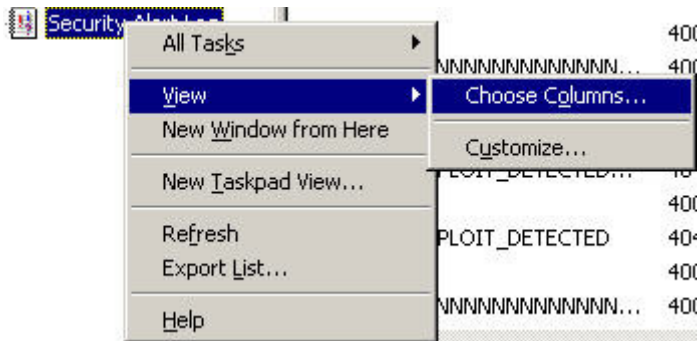
The screen shot below shows the first seven columns that are displayed in the Security Alert Log: **Time, Type, Target URL, Parameter, Operation, Source IP and Source Name.**



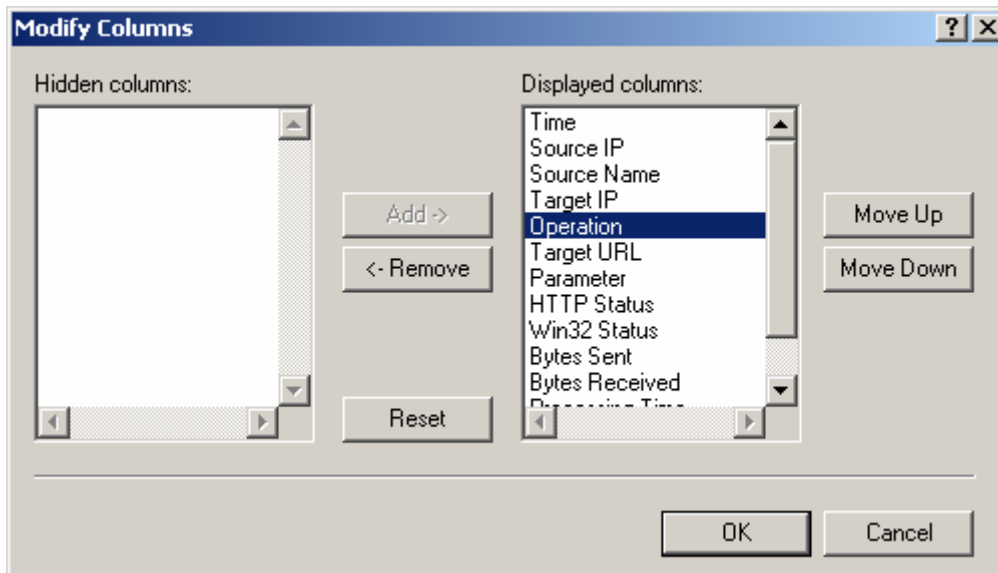
The following screen shot shows the other columns in the Security Alert Log: **Target IP, Web Domain, Bytes Received, Bytes Sent, HTTP Status, Win32 Status, Processing Time, Security Mode and Event Source.**



The columns displayed in the Security Alert Log can be modified by **right mouse clicking** the **Security Alert Log node** and selecting **Choose Columns**.



The following screen will be invoked allowing columns to be added, removed, or displayed in different orders.

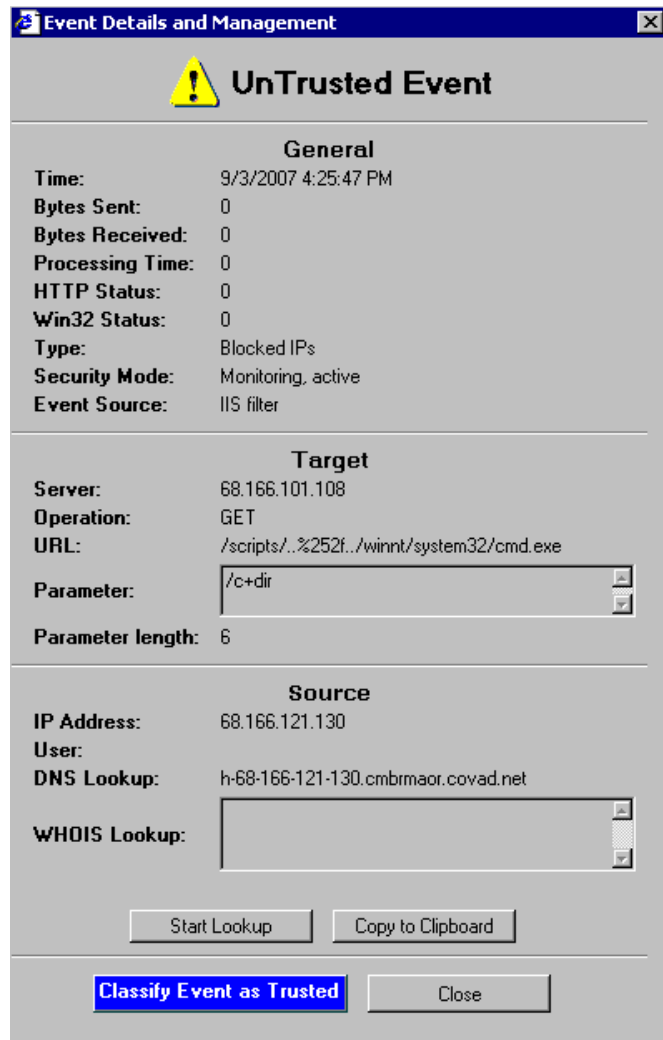


Working with the Security Alert Log

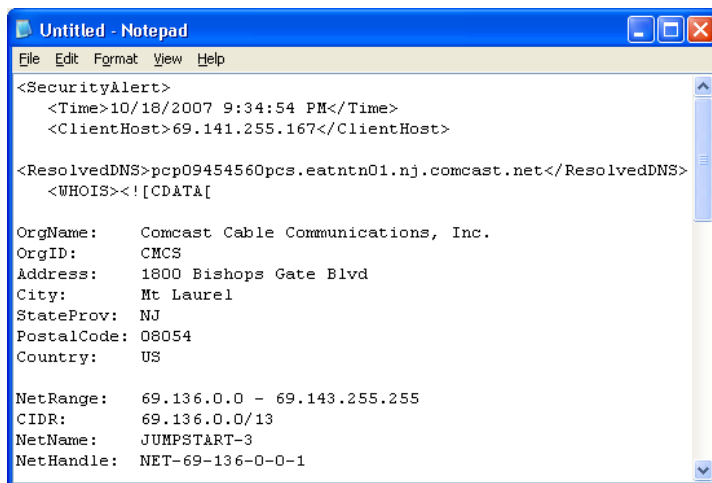
The process of event review, reclassification, and periodic retraining is a key maintenance requirement of ThreatSentry's Behavioral Engine that ensures optimal protection and accuracy. Regular attention applied to [proper classification of events](#), [adjustments to the knowledgebase](#), and [maintenance of the blocked IP address list](#) will ensure progressively effective and precise results.

To review the details of an Untrusted Event, **double click** the event or **apply the right-mouse click** and **select Event Details**.

The Event Details interface displays the details regarding the Untrusted Event.



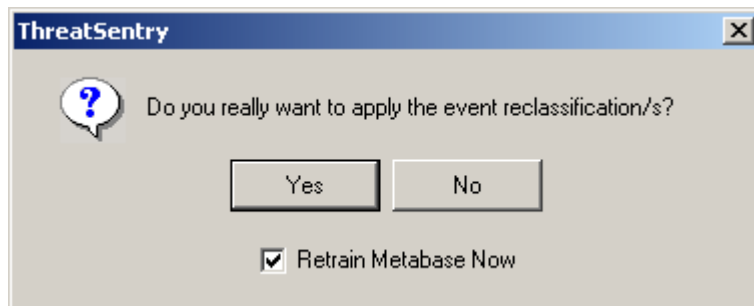
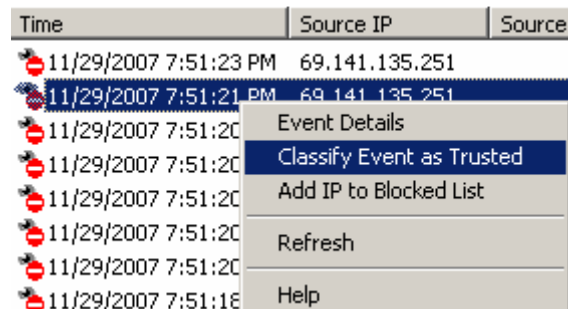
- Information in the Event Details and Management screen corresponds to the information in columns of the Security Alert Log.
- WHOIS Lookup can be used to identify the source IP and other information about the request source.
- WHOIS information can be copied to the clipboard for further reference and distribution.



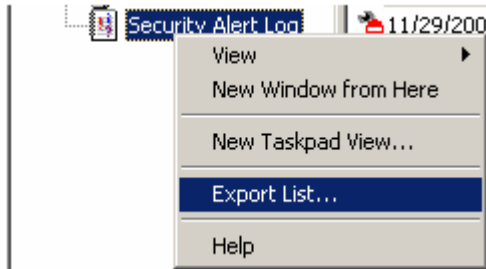
- Event reclassification can be applied.

Right mouse-clicking an event in the Security Alert Log also provides the ability to re-classify an event immediately.

Once selected, ThreatSentry will prompt you to ensure that the event reclassification is accurate.



The Security Alert Log can be exported by right mouse-clicking the Security Alert Log node in the ThreatSentry console.



Multiple untrusted events can be selected for reclassification by holding down the SHIFT or CTRL keys.

Time	Source IP	Source Name
11/29/2007 7:51:23 PM	69.141.135.251	
11/29/2007 7:51:21 PM		Classify Events as Trusted
11/29/2007 7:51:20 PM		Add IPs to Blocked List
11/29/2007 7:51:20 PM		Help
11/29/2007 7:51:20 PM		

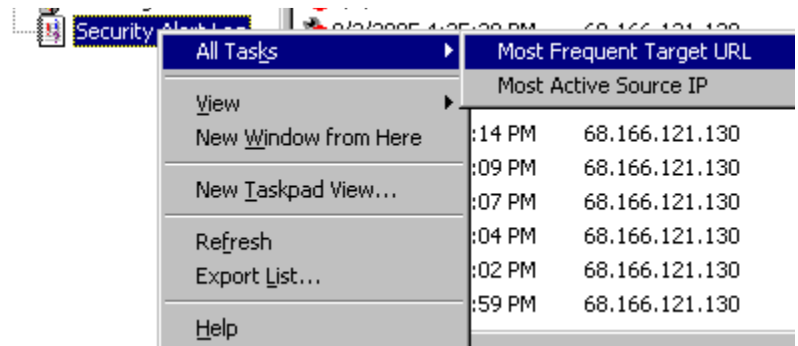
Single or multiple IPs that generated the Security Alert's can also be added to the Blocked List via the right mouse function.

Time	Source IP	Source
11/29/2007 7:51:23 PM	69.141.135.251	
11/29/2007 7:51:21 PM		Classify Events as Trusted
11/29/2007 7:51:20 PM		Add IPs to Blocked List
11/29/2007 7:51:20 PM		Help
11/29/2007 7:51:20 PM		

Security Alert Log Reports

HTML formatted reports can be generated via right mouse-clicking the Security Alert log:

- 1) **Most Frequent Target URL**
- 2) **Most Active Source IP.**



X. Regular Expression Guidelines

Regular Expression Syntax - ThreatSentry uses the Microsoft standard syntax for Regular Expressions (from ATL Server Classes library).

Metacharacter	Meaning
.	Matches any single character.
[]	Indicates a character class. Matches any character inside the brackets (for example, [abc] matches "a", "b", and "c").
^	If this metacharacter occurs at the start of a character class, it negates the character class. A negated character class matches any character except those inside the brackets (for example, [^abc] matches all characters except "a", "b", and "c").
^	If ^ is at the beginning of the regular expression, it matches the beginning of the input (for example, ^[abc] will only match input that begins with "a", "b", or "c").
-	In a character class, indicates a range of characters (for example, [0-9] matches any of the digits "0" through "9").
?	Indicates that the preceding expression is optional: it matches once or not at all (for example, [0-9][0-9]? matches "2" and "12").
+	Indicates that the preceding expression matches one or more times (for example, [0-9]+ matches "1", "13", "456", and so on).
*	Indicates that the preceding expression matches zero or more times.
??, +?, *?	Non-greedy versions of ?, +, and *. These match as little as possible, unlike the greedy versions that match as much as possible (for example, given the input "<abc><def>", <.*?> matches "<abc>" while <.*> matches "<abc><def>").
()	Grouping operator. Example: (\d+)*\d+ matches a list of numbers separated by commas (for example, "1" or "1,23,456").
{ }	Indicates a match group.
\	Escape character: interpret the next character literally (for example, [0-9]+ matches one or more digits, but [0-9]\+ matches a digit followed by a plus character). Also used for abbreviations (such as \a for any alphanumeric character; see the following table).
\	If \ is followed by a number <i>n</i> , it matches the <i>n</i> th match group (starting from 0). Example: <{.*?}>.*?\<0> matches "<head>Contents</head>".
\$	At the end of a regular expression, this character matches the end of the input (for example, [0-9]\$ matches a digit at the end of the input).
	Alternation operator: separates two expressions, exactly one of which matches (for example, T the matches "The" or "the").
!	Negation operator: the expression following ! does not match the input (for example, a!b matches "a" not followed by "b").

Note: match groups (i.e. {}) are not currently supported.

XI. Contact & Support

Mailing Address

Privacyware.com
68 White Street
2nd Floor
Red Bank, NJ 07701

732-212-8110 voice
732-212-9210 fax

Email Addresses

General Information:
info@privacyware.com

Sales:
sales@privacyware.com

Service:
service@privacyware.com

Support:
support@privacyware.com

Partnership Information:
partners@privacyware.com

Privacyware is an innovative provider of award-winning pc security, web application firewall and security data analytics software. Privacyware products leverage conventional and neural analytics technologies to help systems administrators, IT security and compliance personnel more effectively identify, understand and prevent malicious, unauthorized and/or deviant computing system activity. Privacyware is a Microsoft Gold Certified Partner.

CONTACT: Sales, Privacyware: sales@privacyware.com

Privacyware products include:

- >> **[Adaptive Security Analyzer](#): Neural Security Data Analysis Software**
- >> **[ThreatSentry](#): IIS Web Application Firewall and Host IPS**
- >> **[Privatefirewall](#): Free Personal Firewall and Desktop HIPS**

www.privacyware.com

ThreatSentry

User Guide

Document Version

ThreatSentry, Edition 4.0 (June, 2010), Privacyware/PWI, Inc.

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 © 2003-2010 Privacyware/PWI, Inc.. 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.