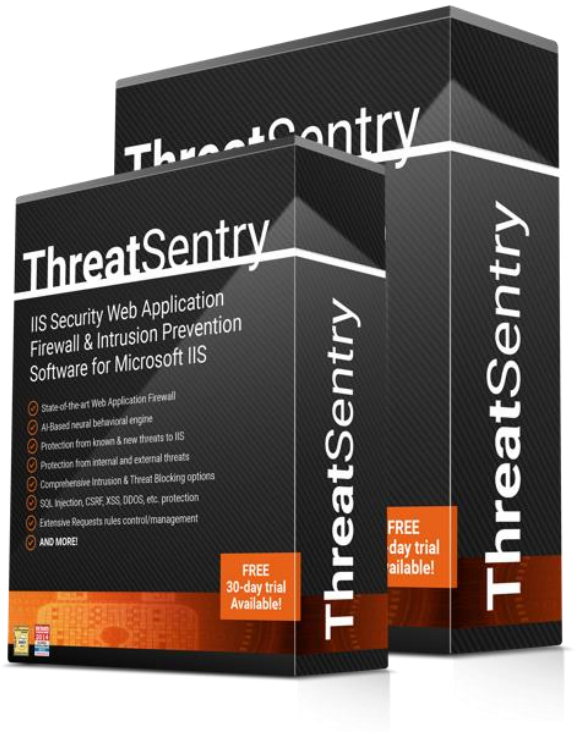
The Ultimate Windows Web Server Security

privacyware

ThreatSentry IIS Web Application Firewall

User Guide



Published by:
Privacyware
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 11
A. Security Modes 12
B. Additional Options 13
V. Product Registration 15
VI. Uninstalling 18
VIII. Using ThreatSentry 19
A. Management 20
Services 20
Rules 31
Filtering Rules and IP Address Backup 45
Training Data Display 46
Training using Existing IIS Logs 51
C. Security Alerts & the Security Alert Log 52
Security Alerts 52
Security Alert Log 53
Working with the Security Alert Log 54
Security Alert Log Reports 56
SQL Server backup and Security Alert Log Maintenance 57
X. Regular Expression Guidelines 58
XI. Central Management of Multiple Server Systems 59
XII. Contact & Support 61

I. System Requirements

ThreatSentry is compatible with the following:
- IIS 10 (Windows Server 2016/2019)
- IIS 8.5 (Windows Server 2012/R2, Windows 8, x86/x64)
- IIS 8.0 (Windows Server 2012, Windows 8, x86/x64)
- IIS 7.0/7.5 (Windows Server 2008/R2 x86/x64)
- IIS 6.0 (Windows Server 2003 – x86/x64)
- IIS 5.0 (Windows Server 2000)
- .NET framework 2.0 or later (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.

Simultaneous filtering of 32 and 64 bit application traffic filtering is supported on IIS8/8.5 and IIS7 via ThreatSentry build for 64 bit IIS. During setup, two dlls will be installed under IIS7 environment: - PWIISAPISES.dll and PWIISAPISES64.dll (first dll handles requests from all 32bit web applications/sites, second from all 64bit applications/sites)

II. Product Overview

What is ThreatSentry?
ThreatSentry is the leading software–based Web Application Firewall and Host IPS for Microsoft Internet Information Services (IIS). ThreatSentry identifies and blocks web application threats such as Structured Query Language (SQL) Injection, DDoS, Cross Site Request Forgery (CSRF/XSRF), Cross-Site Scripting (XSS) and other types of attacks and helps system administrators comply with regulatory demands such as Section 6.6 of the Payment Card Industry Data Security Standard (PCI DSS). ThreatSentry supports Windows Server 2012, 2008/R2, 2003 and 2000 and IIS8 and IIS 7.x (native module), 6 (ISAPI Extension) and 5 (ISAPI Filter) on 32 and 64 bit systems.

ThreatSentry delivers proactive, multi-layered defense for IIS and prevents attacks from exploiting web application vulnerabilities through a complementary set of integrated components.

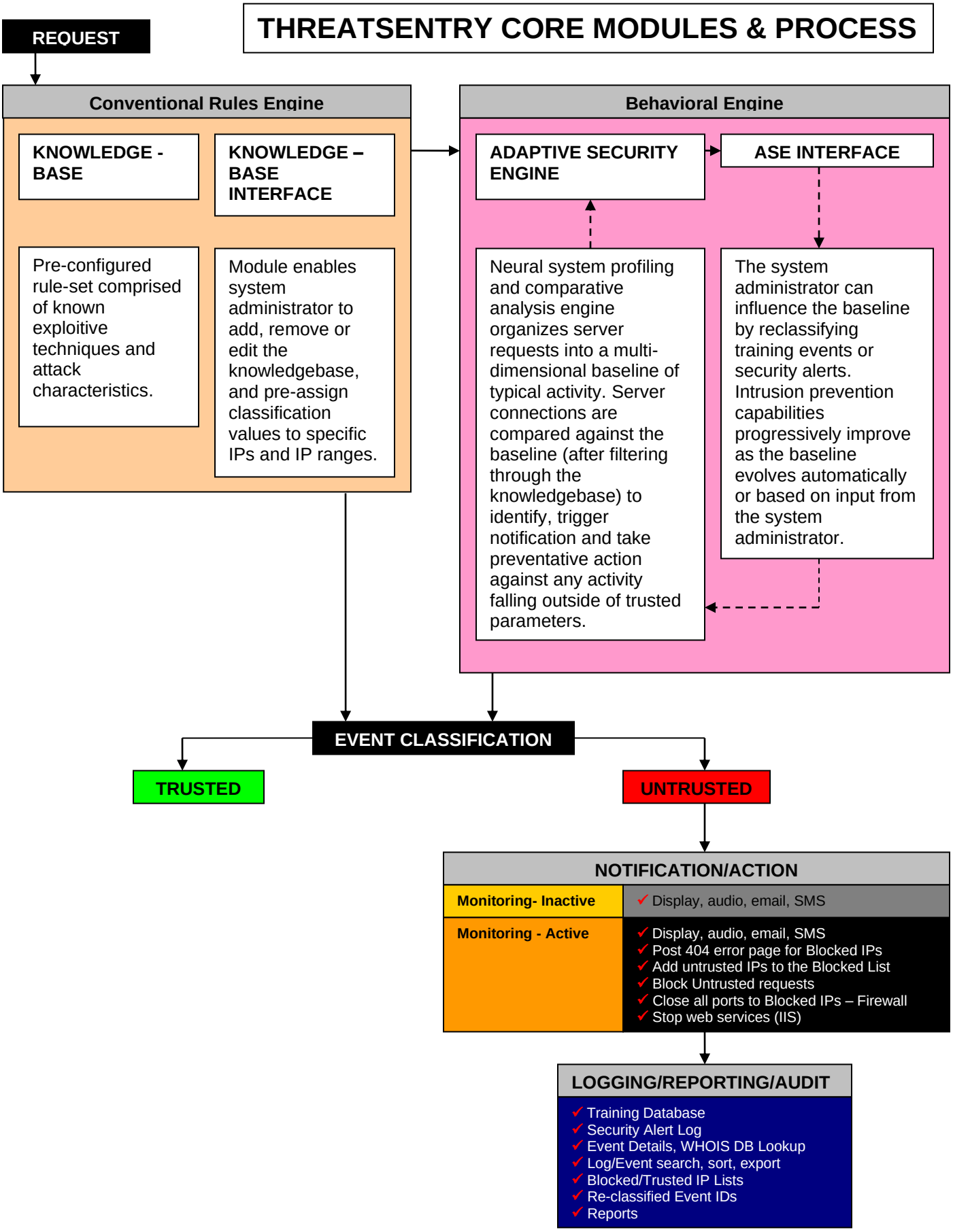
- State-of-the-art Web Application Firewall: Provides configurable rules-based control over HTTP/HTTPS request methods (OPTIONS, GET, POST, HEAD), URL Paths, URL Query String length, and HTTP Request Headers, rule-specific URL/s exclusion capabilities, URI Encoding support, Regular Expression support for parameter rules/filtering, etc.

- Fully integrated Firewall: Proprietary NDIS driver delivers flexible network IP blocking (featuring white list, black list and duration control) at TCP/IP and UDP layers for all ports.

- Behavior-based Intrusion Prevention: Adaptive, behavior-based engine (with sensitivity control) analyzes Web traffic patterns to detect new threats and behavioral anomalies and deviations.

- Anti-DoS/DDoS: Configurable request frequency monitor blocks successive requests to individual or all site pages to reduce the risk of DoS and DDoS attacks.

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

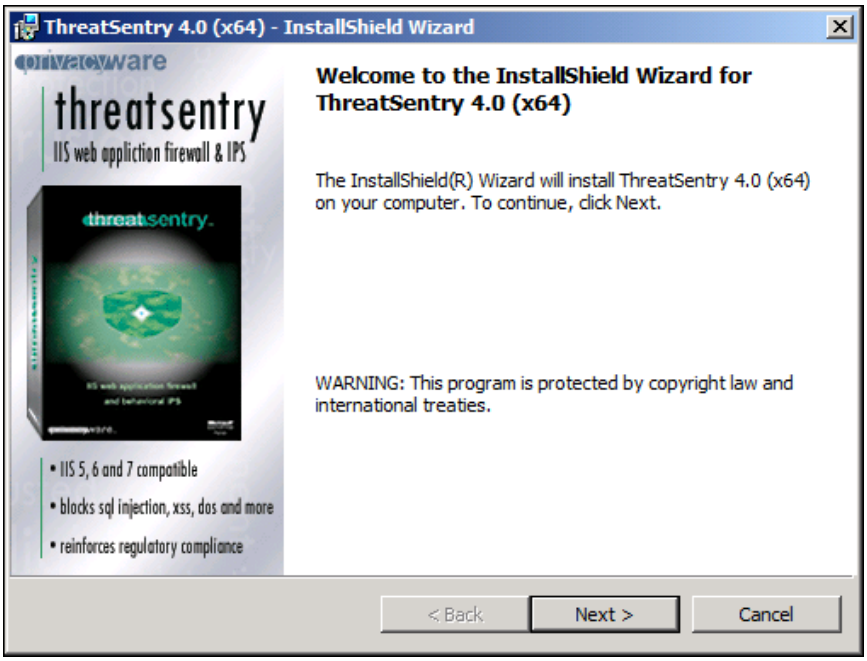
Upgrade support from Threatsentry v3 to ThreatSentry v4 is fully supported.

- 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.

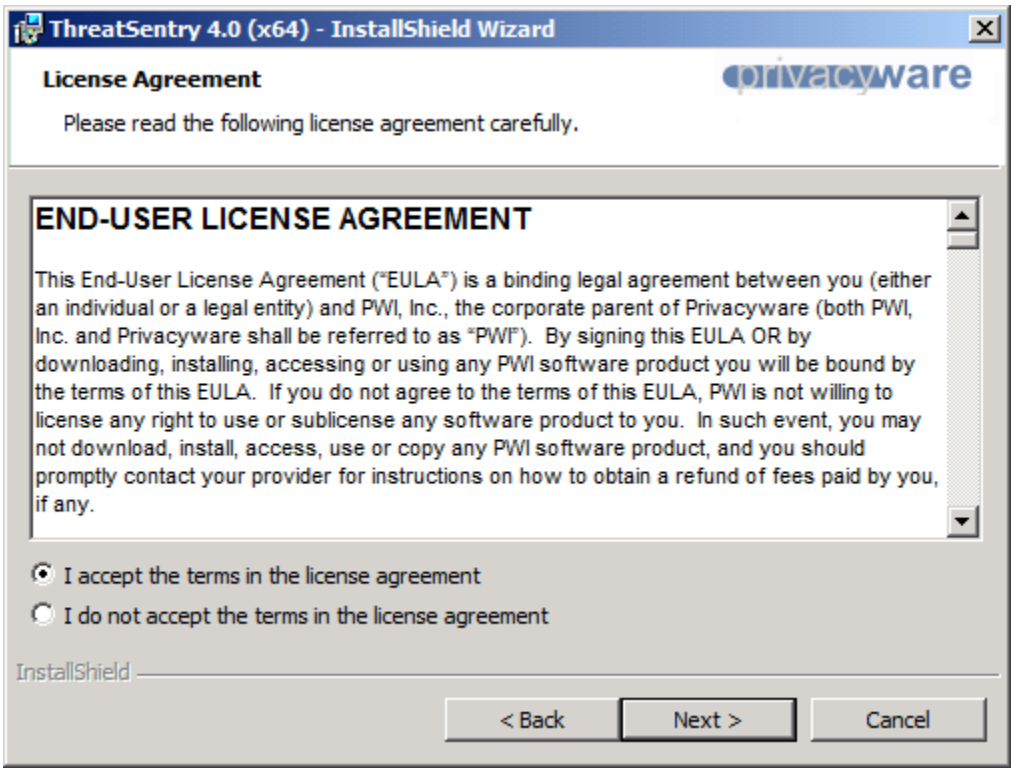
If the **"Preserve existing configuration settings"** option is selected during v4 installation:

- 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 IntrustionLog.mdb and YEVS.mdb will be converted to SQL tables and any existing data will be migrated.

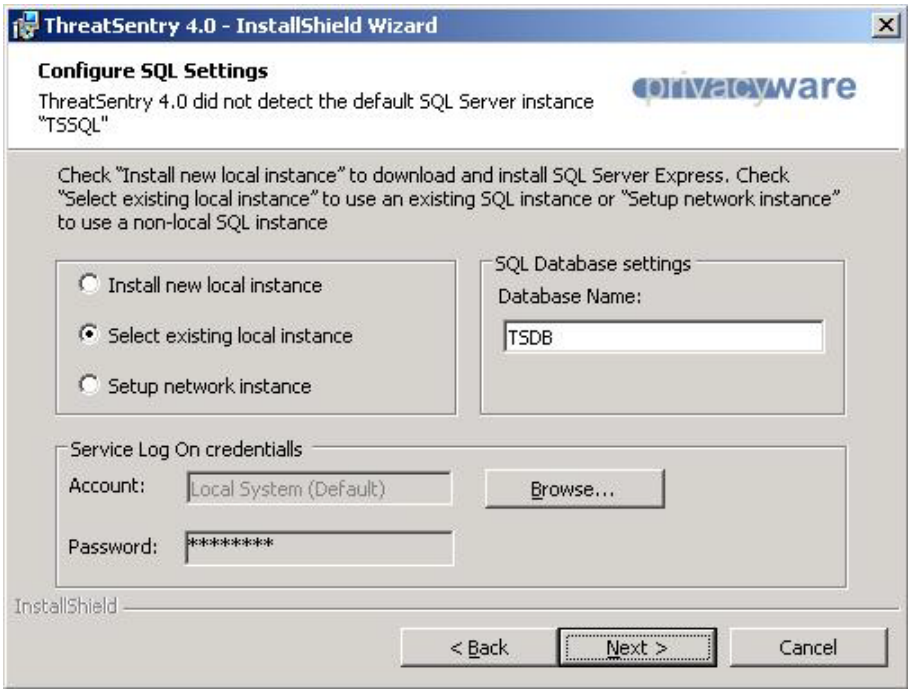
ThreatSentry uses the InstallShield Wizard to facilitate installation. To begin installation, double-click the ThreatSentry executable. The following screens illustrate the activation of the InstallShield Wizard. **Click Next**.



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

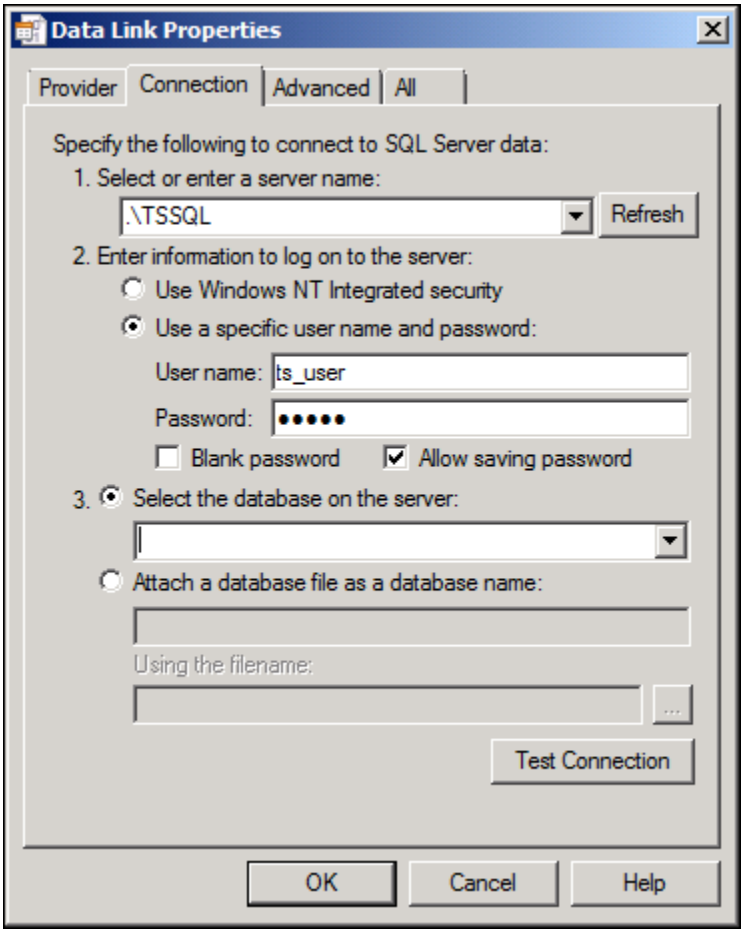


ThreatSentry requires installation of a SQL database. Check **Select existing local instance** or **Setup network instance** to use an existing SQL Server resource or check **Install new local instance of SQL Express** (https://www.microsoft.com/en-us/sql-server/sql-server-downloads) if SQL Server is not already available locally or remotely.



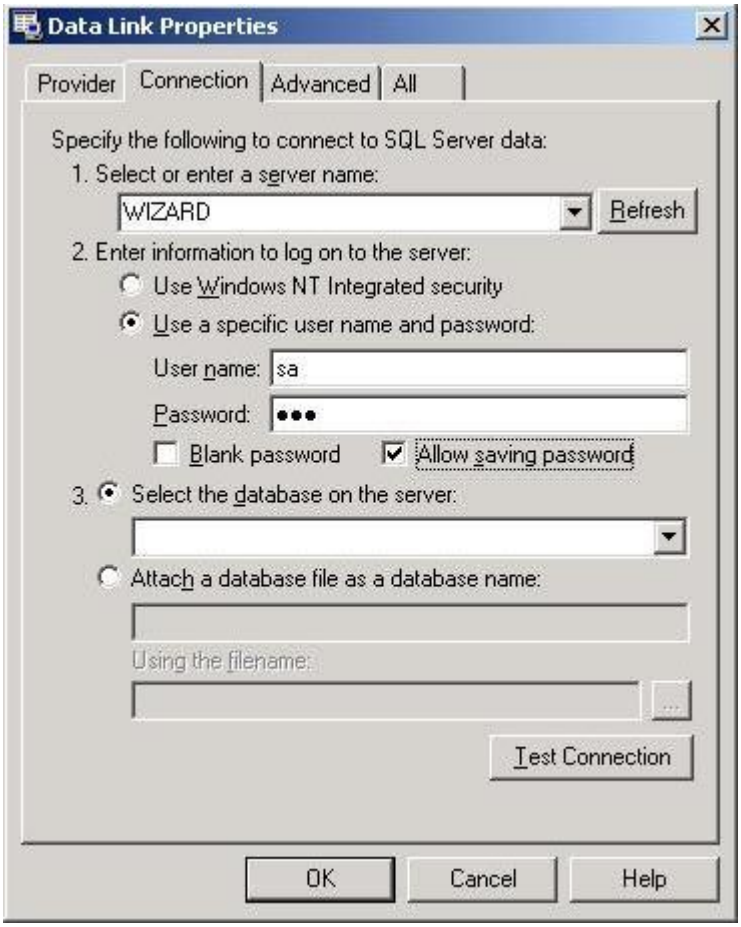
Install new local instance will invoke the Extraction of SQL Server related files and SQL Server installation. This process may take a few minutes. Do not click the Back or Next buttons until the SQL Server installation is complete (hourglass will disappear once complete).

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



There are two possible variants for setup of a Remote SQL server instance and authorization:

Active Directory Login: Where SQL Server has been fully integrated with Active Directory.

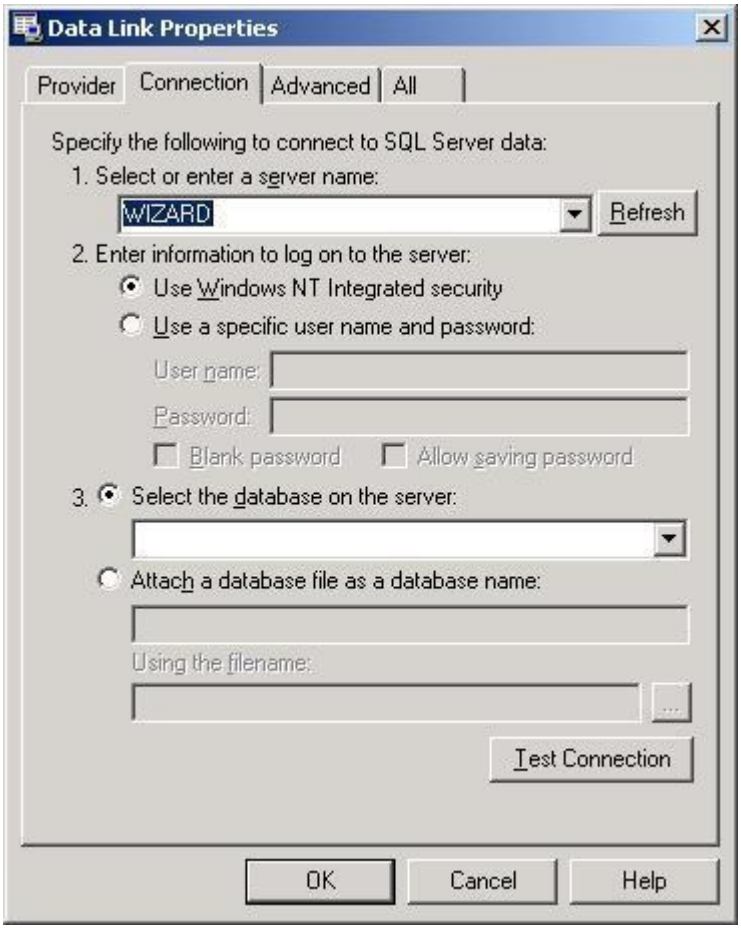


1) Current user (user installing TS with remote SQL instance) requires sufficient privileges for the remote SQL instance.

2) When installing ThreatSentry, select Remote instance and appropriate SQL server in DataLink dialog. Be sure to use the "Test Connection" and verify the connection. Then complete TS installation.

3) Once ThreatSentry installation is complete, if there is any issue connecting to the remote SQL instance, please do the following:
- Close the ThreatSentry AdminConsole,
- Stop the TSSvc.exe process in Task Manager and stop the ThreaSentry service (from Services).
- Reconfigure the ThreatSentry service properties to log as current domain user instead of Local system account.
- Start ThreatSentry service upon which it should work as expected.

Native SQL Login: Using native SQL Server authorization. No special setup requirements are necessary. Simply enter the configured login and password (sa/sql by default).

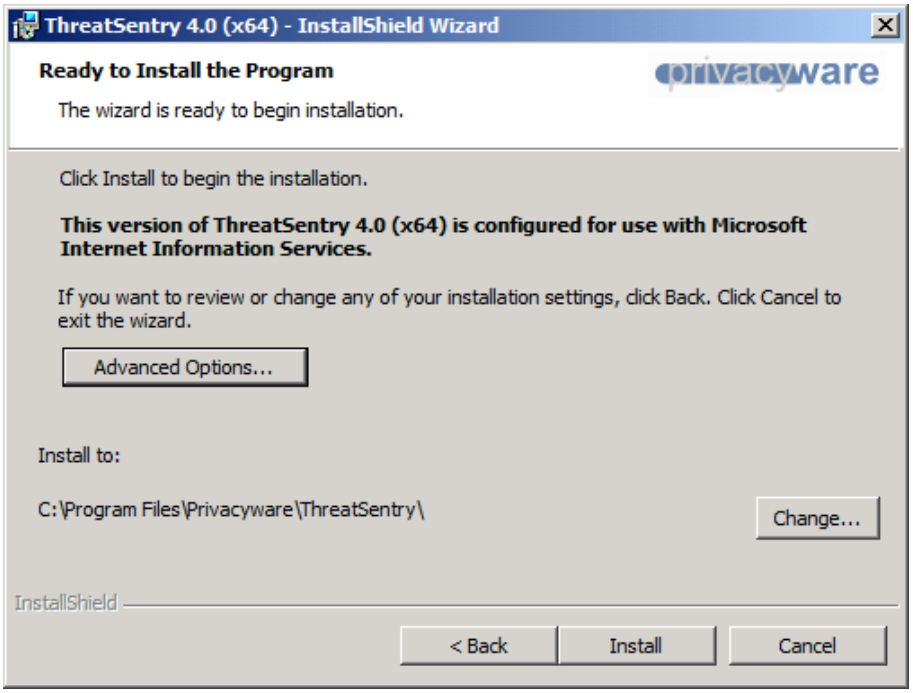


Changing a SQL instance

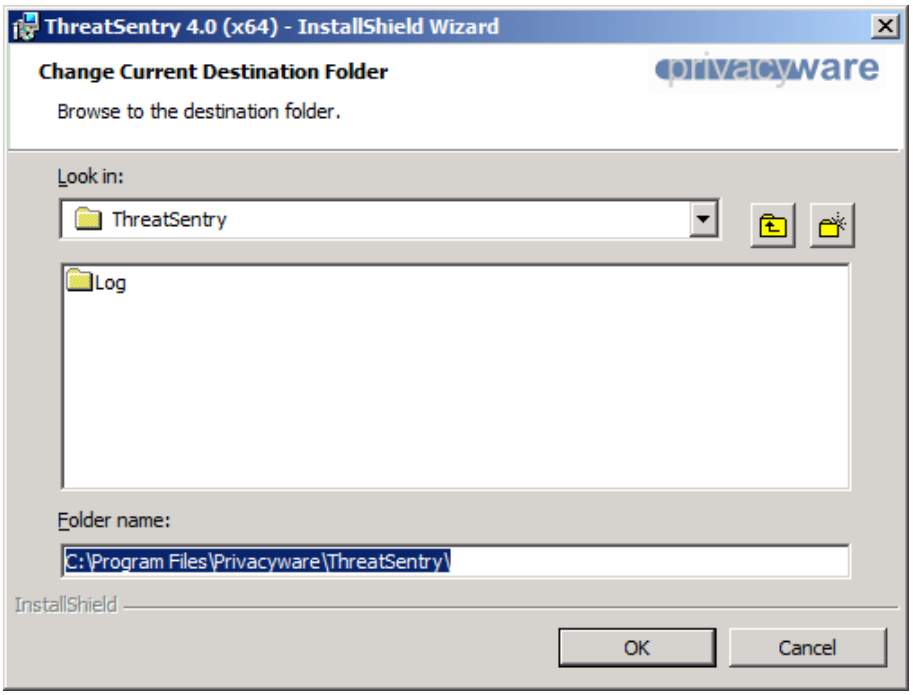
In order to change the SQL database used with ThreatSentry from, for example, a local instance to one installed on a remote server, the following process should be followed:
- Close all ThreatSentry AdminConsole instances.
- Stop the local SQL instance service used currently by ThreatSentry.
- Run the ThreatSentry installer, select the **Modify** option and follow the prompts displayed.

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**.

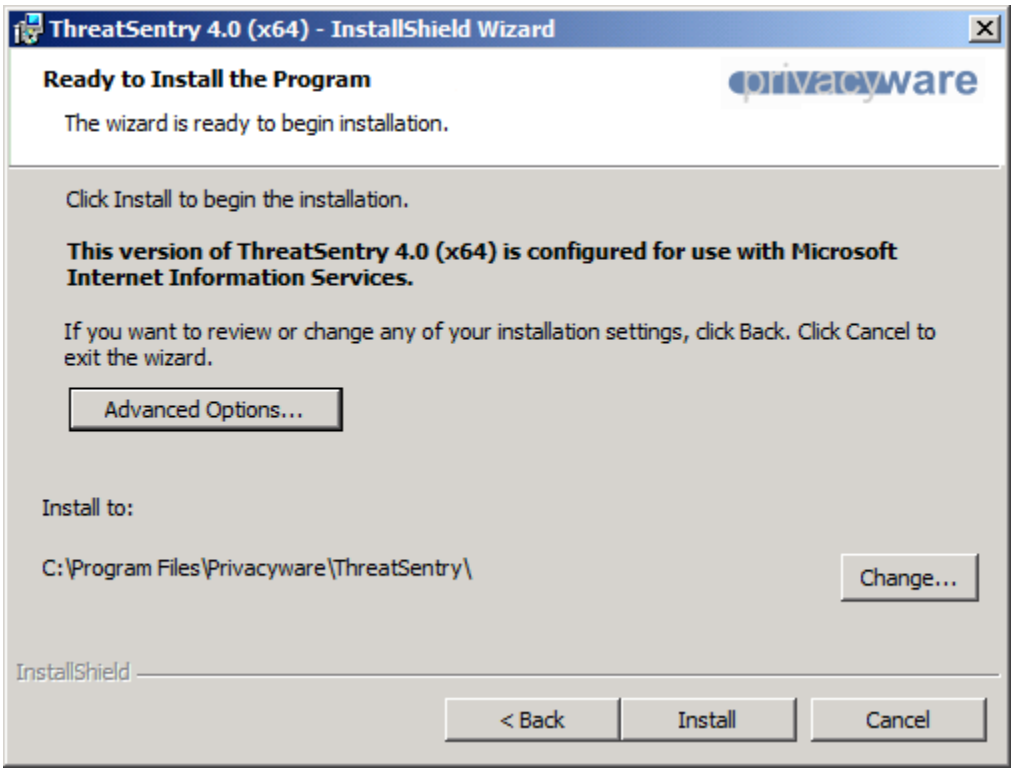
IV. Advanced Installation and Configuration

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

A. Select a Security Mode.
B. Specify Additional Options such as upgrade/migration settings and support for Outlook Web Access Operations.

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. Security Modes

ThreatSentry provides three different Security Modes; Monitoring – Inactive, Monitoring – Active and Training.

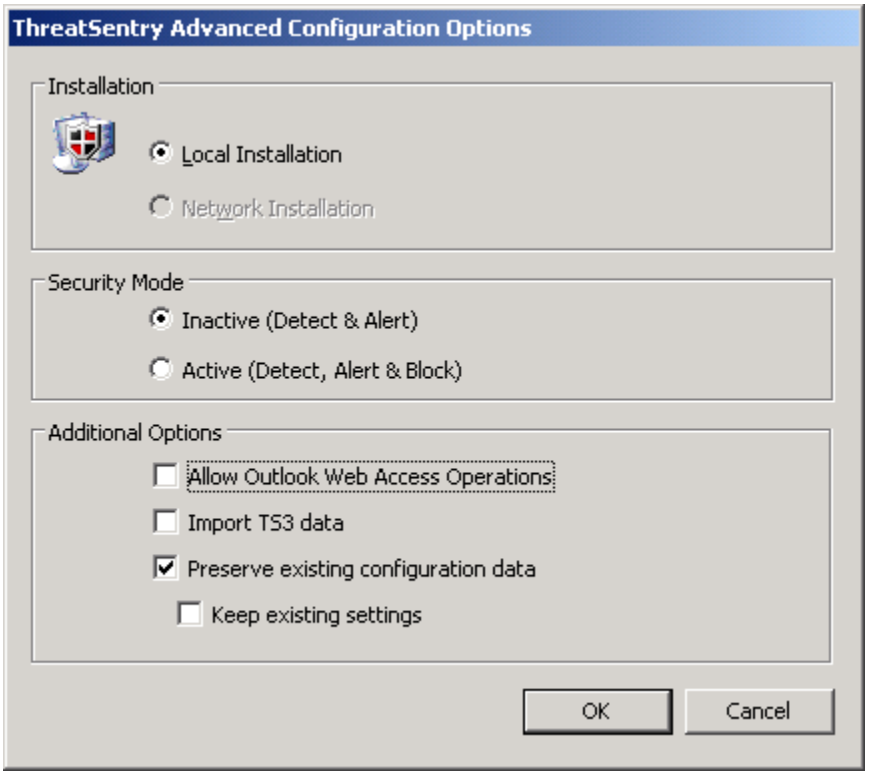
Monitoring – Inactive (Default Mode). ThreatSentry Detects and Notifies, but does not block untrusted events. This mode is enabled by default (upon installation) so that the administrator can monitor the ThreatSentry Security Alert Log for any requests that may have been blocked which should not have. 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.

B. Additional Options



Outlook Web Access Support

Allow Outlook Web Access Operations:
ThreatSentry supports Outlook Web Access operations. If the server on which ThreatSentry is being installed requires OWA support, you may indicate this by checking the **Allow Outlook Web Access Operations** box.

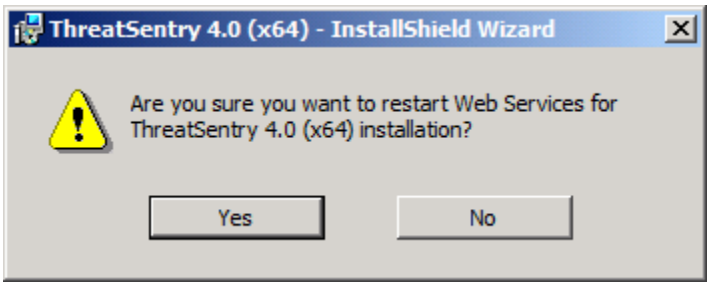
Import TS3 Data:
When ThreatSentry 4 is installed in the same directory used previously by ThreatSentry 3, this option will enable you to import ThreatSentry v3 data - specifically the IntrusionLog.mdb, YEVS.mdb, MappingRules.xml and IP Lists into the ThreatSentry v4 SQL database.

Please note that using this option will prevent ThreatSentry v4 rules from being installed and is not generally recommended.

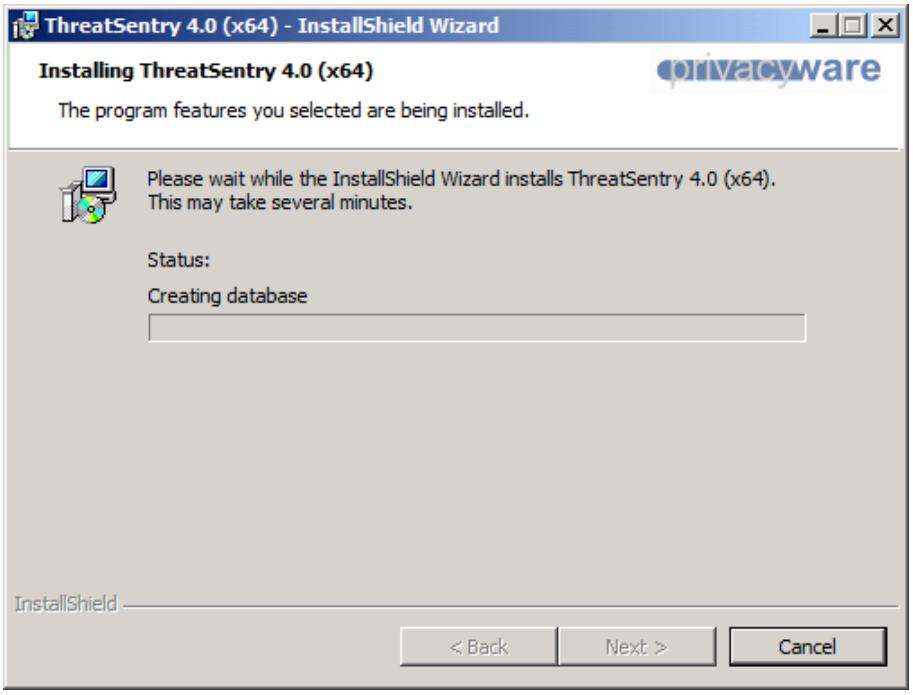
Preserve Existing Data:
This option will enable you to preserve all Security Alert and Training Data when updating ThreatSentry v4 (i.e. from 4.0.25.0 to 4.0.27.0). The option requires that the same SQL instance is used for the update. When unchecked, any existing Security Alerts and Training Data will be cleared upon updating to a new ThreatSentry build and the most current set of default rules and settings will be installed. Existing data can be archived using the SQL Server Management Console

Preserve Existing Rules and Settings:
This option will enable you to preserve ThreatSentry rules and IP Lists (blocked, allowed, previously blocked) when updating ThreatSentry 4 (v4 to v4 only). All new v4 rules will be installed and custom rules will be preserved. Any v4/v4 rule conflicts will defer to the v4 default rule set.

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

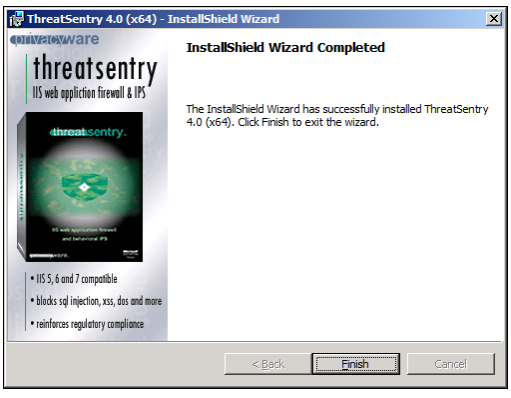


…that program features are being installed,



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

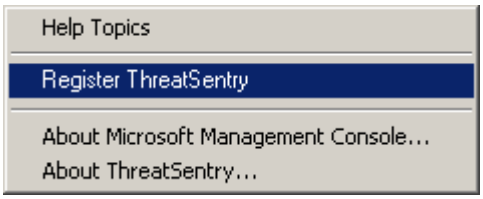
Installation is complete.



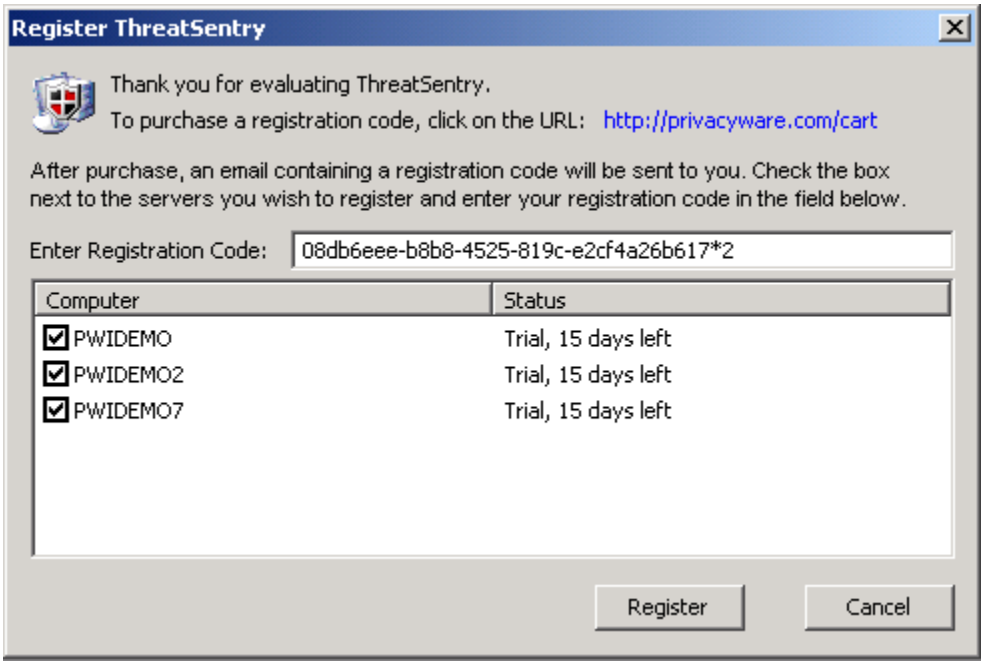
V. Product Registration

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.

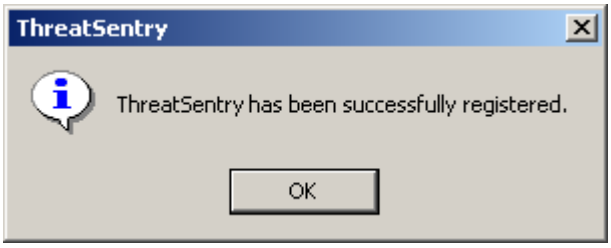
To Register ThreatSentry, Right mouse click the ThreatSentry icon in MMC and select **Register ThreatSentry,** (alternatively, Select **Action** in the **MMC main menu** and Select **Register ThreatSentry**).



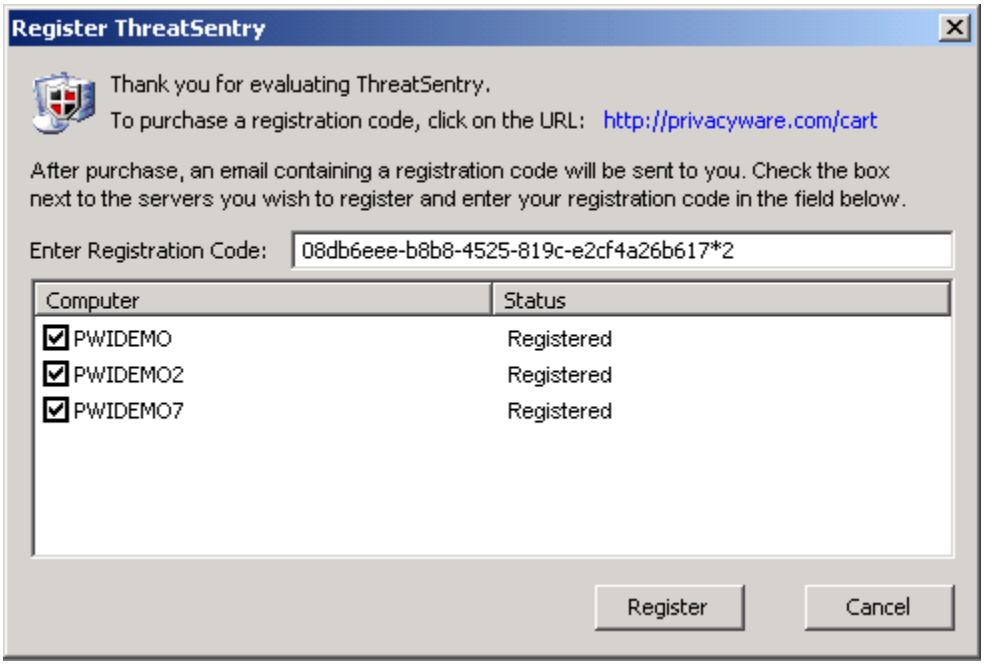
After purchasing ThreatSentry, you will receive a confirmation email with a Registration Code. The Registration Code and associated license tracking mechanism controls the number of licenses purchased and the unique software/server installations. The Registration Code will be valid for the total number 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.



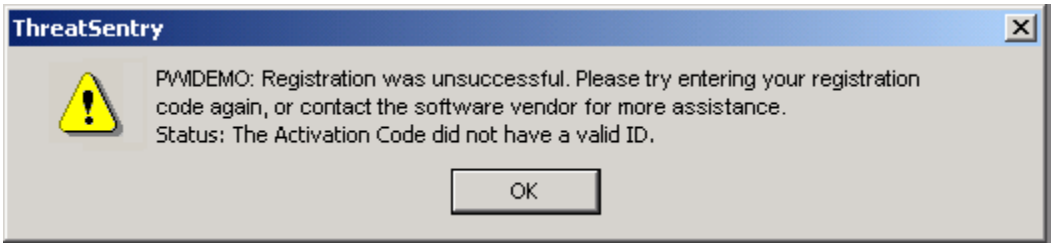
The registration information is electronically sent to Privacyware for approval. If the code is valid, the following confirmation will appear:



And the Status column will reflect the successful product registration.



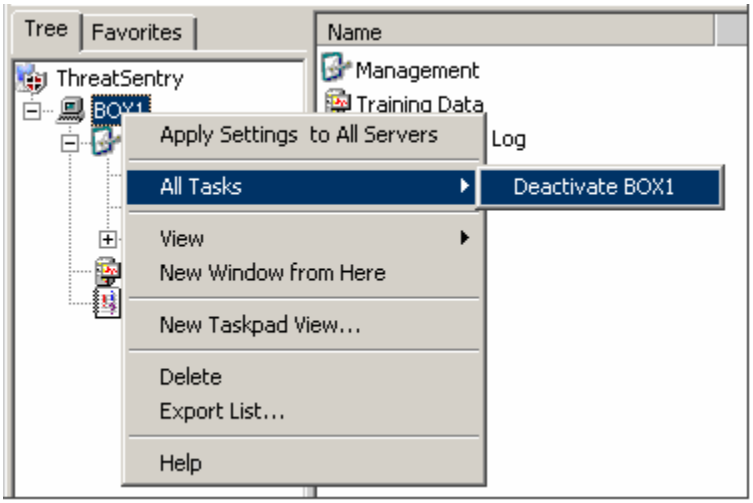
If the registration code is not valid or entered incorrectly, the following or similar screen will be displayed. Please try entering the code again, and if the problem persists, contact Privacyware support for additional assistance.



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.**

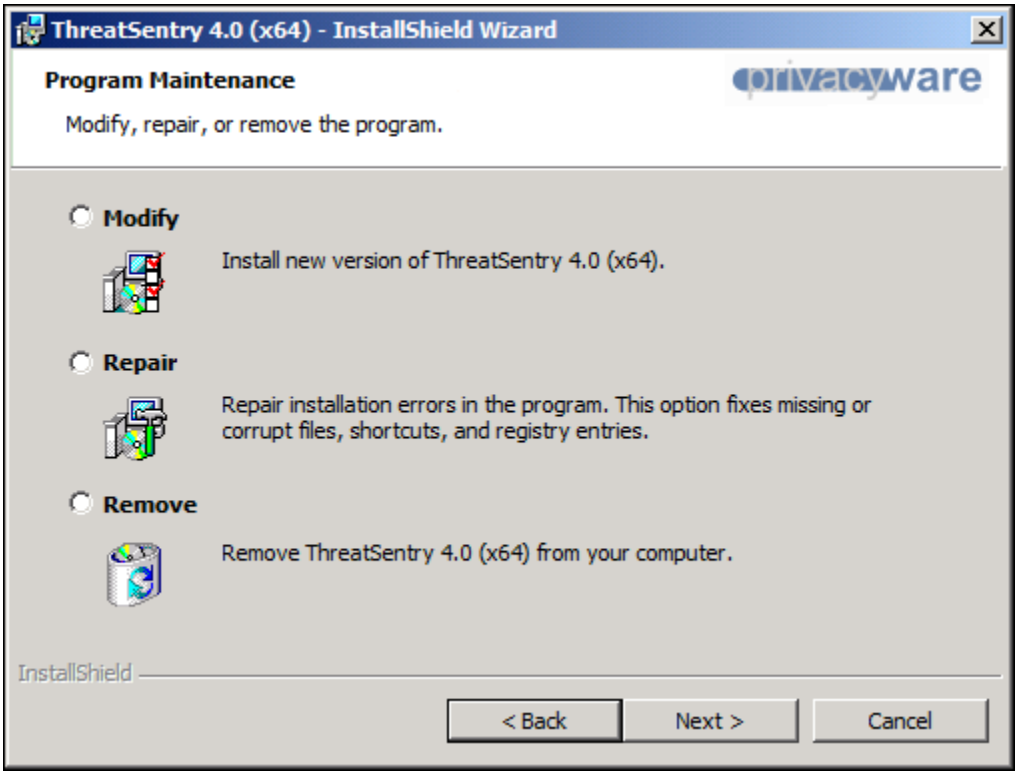
Click here to request a new Registration Code.

For additional information, contact Privacyware:
Phone: 614-656-1956
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.



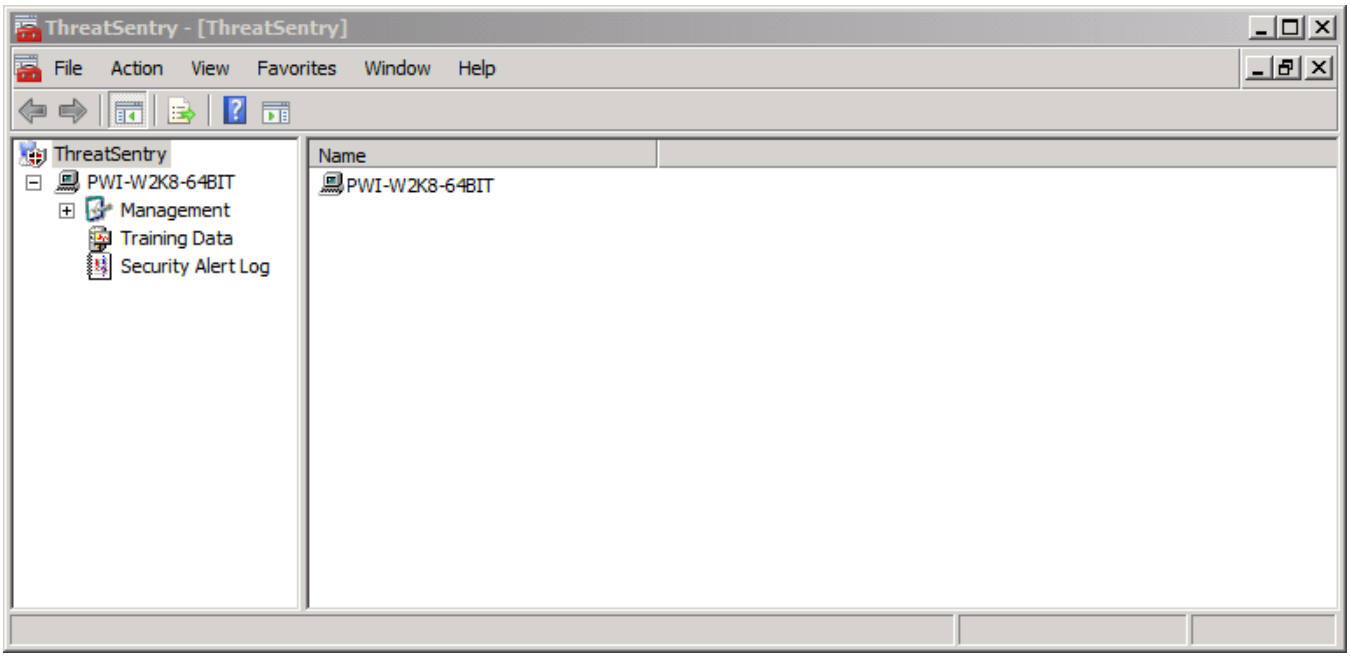
VIII. Using ThreatSentry

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



A. Management

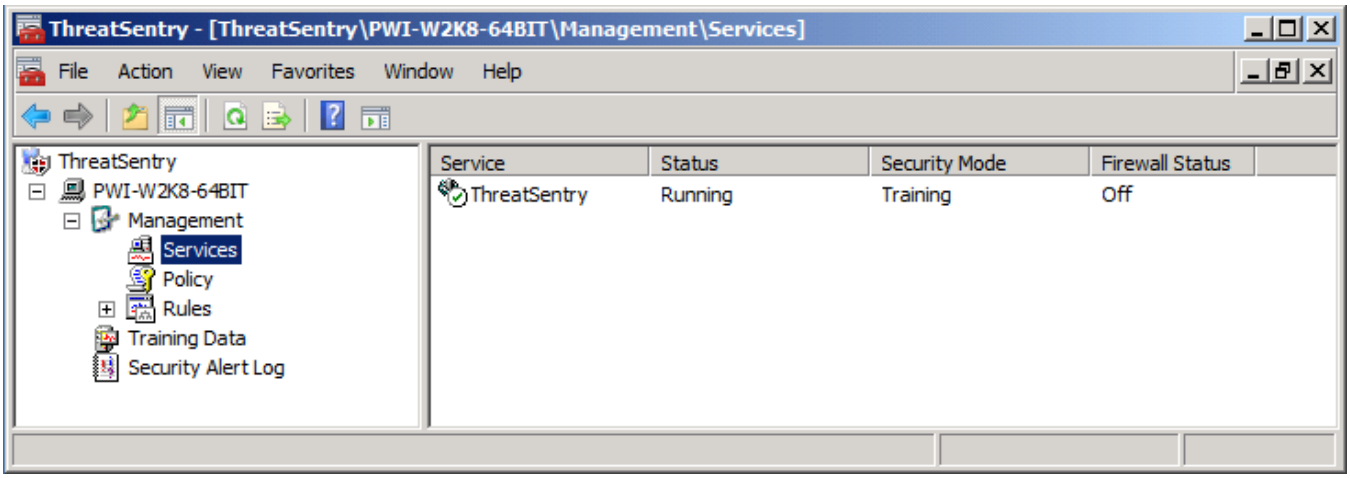
Management interfaces include three subcategories:

- **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

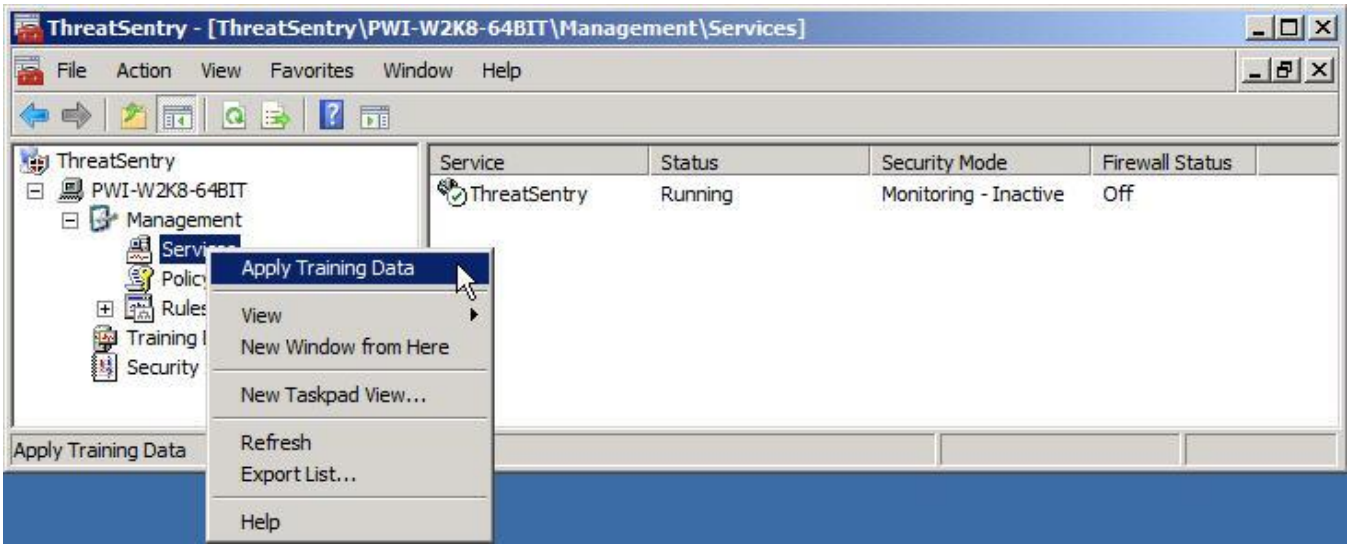


Note: After installation, ThreatSentry may not indicate that the Status is "Running" until the first HTTP request has been received by IIS.

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).

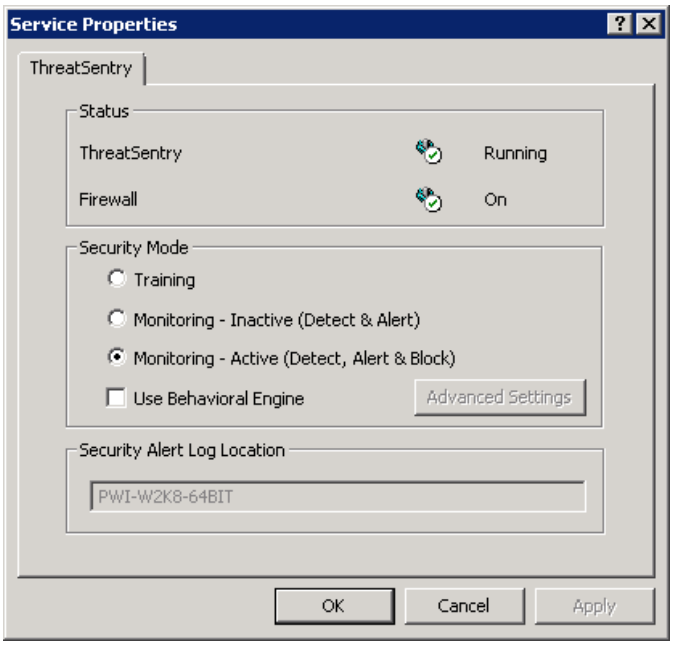
Applying the Training Data will initiate retraining of the meta-base (behavioral baseline). This process recalculates the baseline from existing training data and any event/s that have been reclassified in the Security Alert Log. For more information regarding the Security Alert Log and working with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

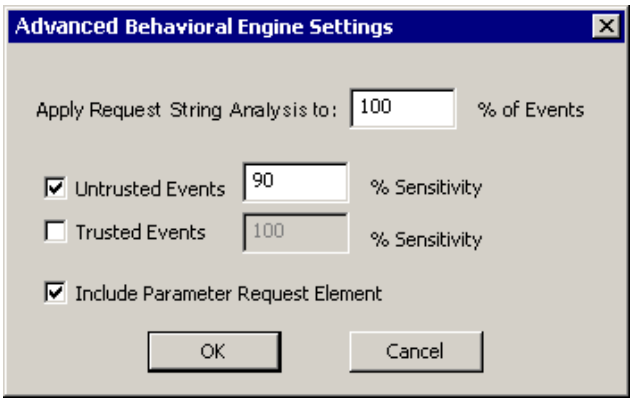


2) Services Properties: ThreatSentry Services Properties can be invoked by **double-clicking** the **ThreatSentry Services** node in the **right panel of the MMC** or by **selecting ThreatSentry Service** in the **right panel of the MMC** and then **selecting Action** in the **MMC main menu**.

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**



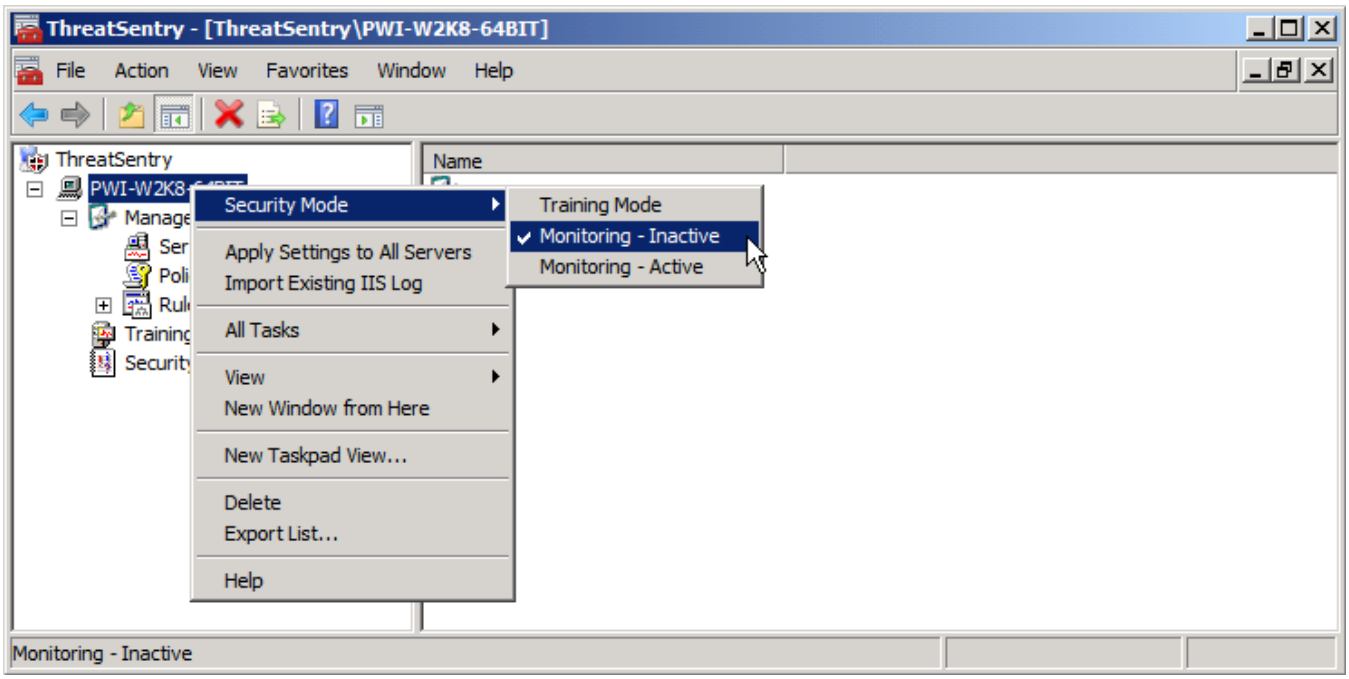


3) ThreatSentry Behavioral Engine Advanced Settings: ThreatSentry analyzes fourteen variables related to an IIS request, but pays special attention to the URL and Parameter elements. The **Advanced Settings** screen enables the manner and sensitivity with which the Behavioral Engine considers the URL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

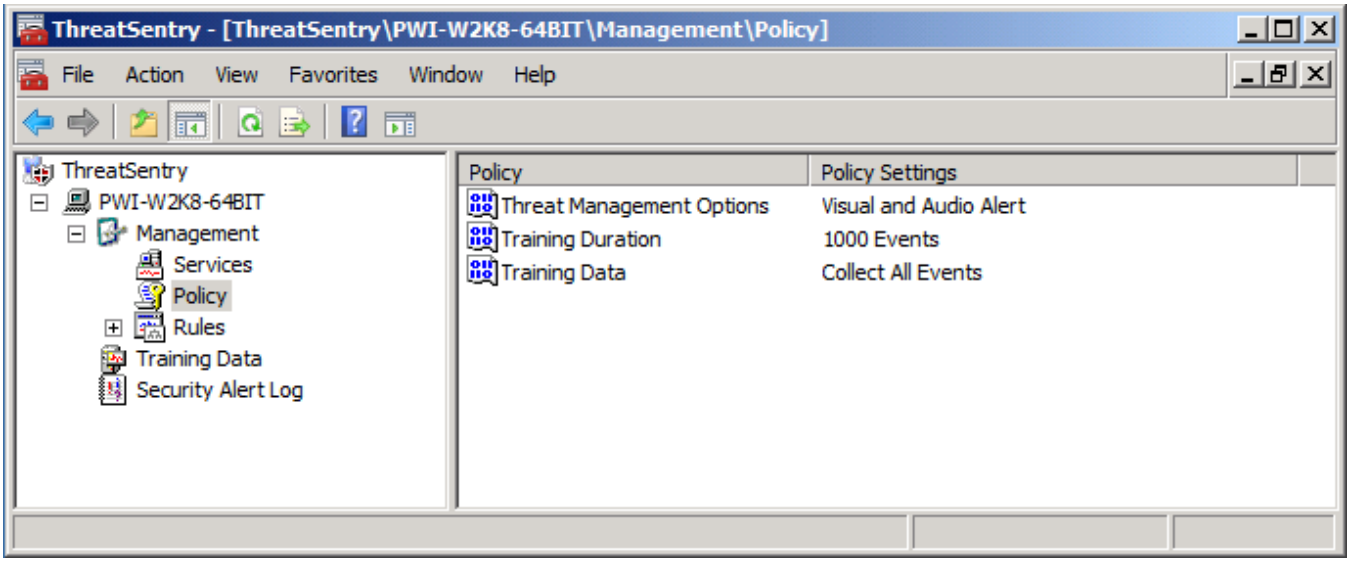
Policy interfaces provide the ability to specify what action/s ThreatSentry will trigger as untrusted events are identified, adjust the number of events to be collected in the training database, and define the types of events that should be collected.

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

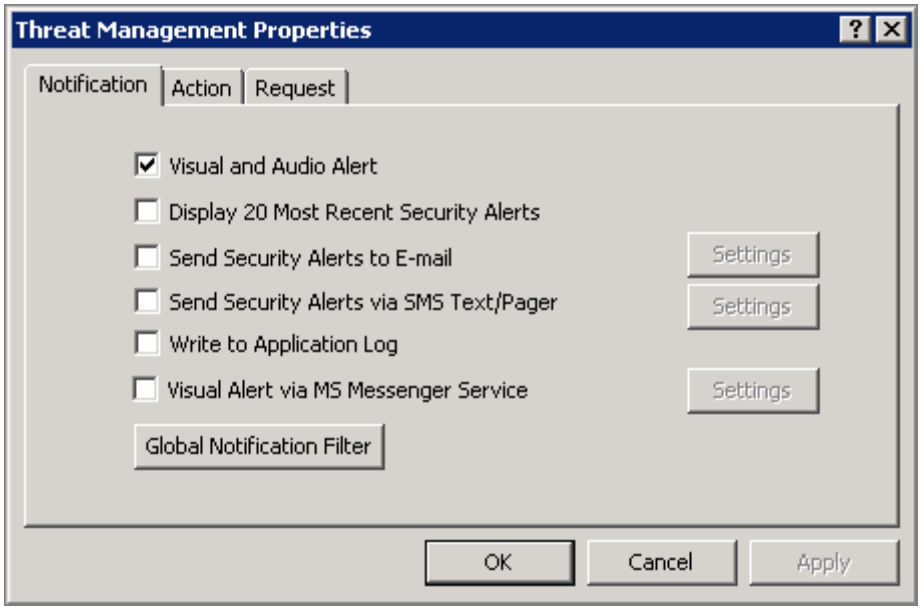
3) Training Data



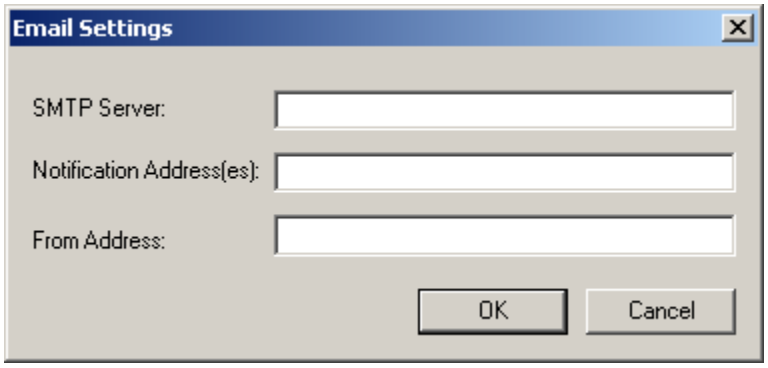
1) **Threat Management Options:** The Threat Management Options Properties interface allows you to manage ThreatSentry's response to events that it classifies as untrusted. To invoke the Threat Management Options Properties interface, double-click the Threat Management Options Policy node in the right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

   Threat Management Options are divided into three categories – **Notification, Action** and **Request**. Notification provides various options dealing with how ThreatSentry delivers notification of Security Alerts to the Administrator. Action dictates what action ThreatSentry should apply when an Untrusted Event has been identified. The Request tab provides options related to X-Forwarded-For Addressing and Request data masking for PCI DSS. Options are described and shown in the screens below, (checked boxes designate the default settings).

Notification

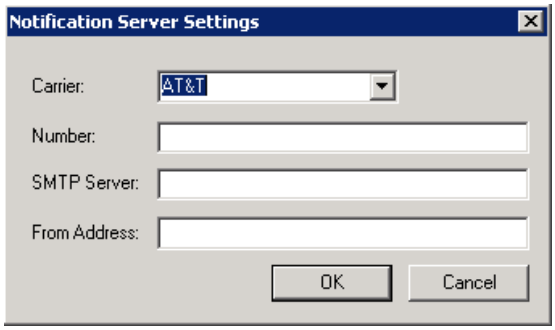


- **Visual and Audio Alert:** Generates ThreatSentry Security Alert tray pop-up, and Security Alert Event Detail and Management Options window.
- **Display 20 Most Recent Security Alerts:** Displays the 20 most recent Security Alerts as each new Security Alert is generated.
- **Send Security Alerts to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

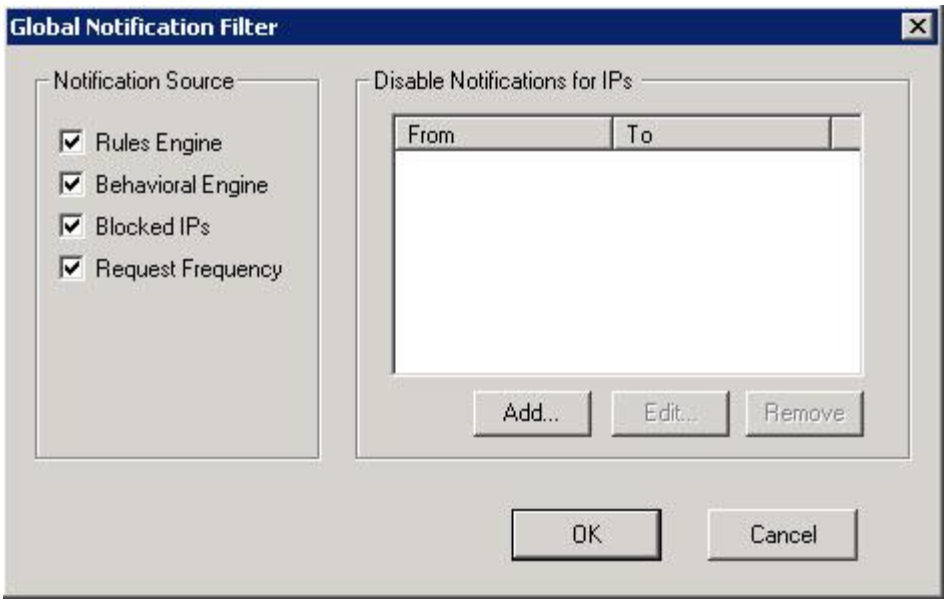


Send Security Alerts to SMS/Pager: SMS Notification of Security Alerts can be configured.

Note: Notification for isolated or first in an alert series will be sent immediately. Alerts occurring immediately subsequent to an initial alert (within 90 seconds) will be batched in sets of ten (maximum) and sent immediately after expiration of the 90 second period.



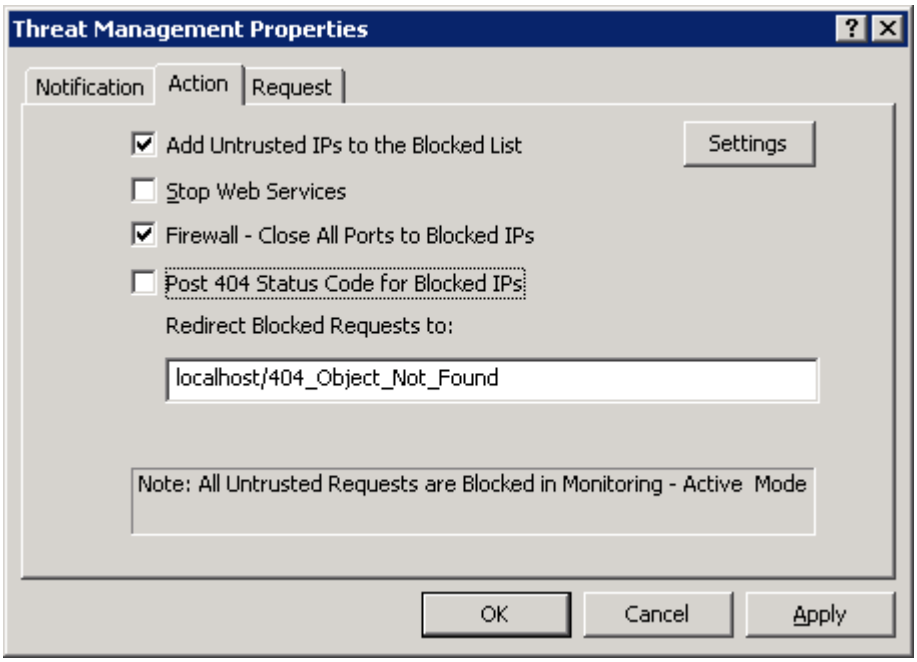
- **Write to Application Log:** Enables ThreatSentry Security Alerts to be displayed and monitored in Microsoft Operations Manager (MOM).
- **Visual Alert via MS Messenger Service:** Enables ThreatSentry Security Alerts to be displayed on PCs or servers that do not have ThreatSentry installed.
- **Global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



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

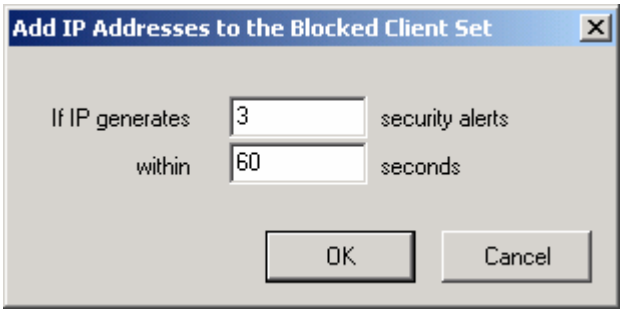
Action

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.
- **Redirect Blocked Requests to:** Redirects blocked requests to specific web page (defaults to localhost/404_Object_Not_Found).
- **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

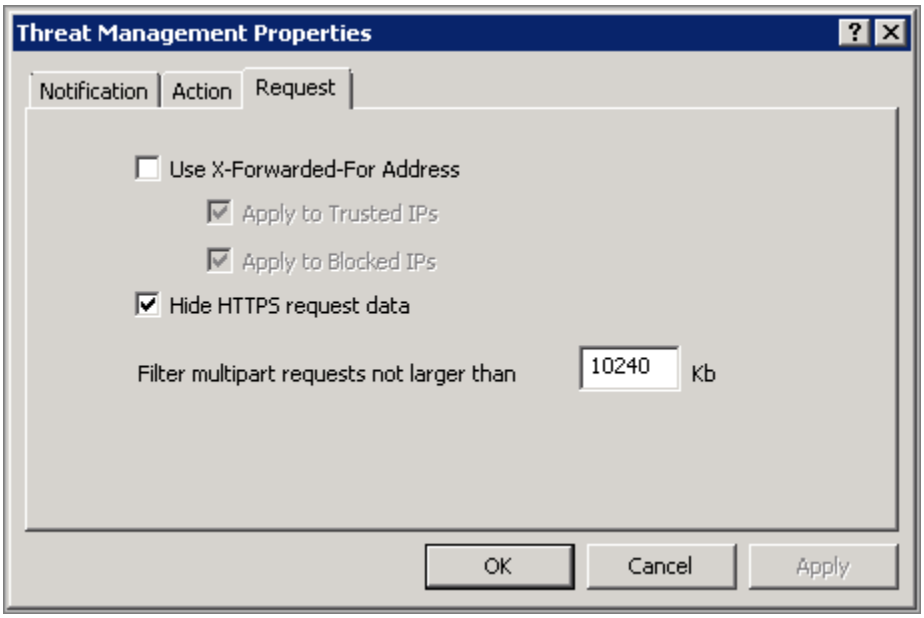
When **Add Untrusted IPs to the Blocked List** is selected, ThreatSentry will automatically add any IP that generates a Security Alert to the Blocked IP List. Any new request from the same IP will be blocked and never reach IIS. In addition, any IP that has been manually or automatically added to the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

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

- **Stop Web Services**: Shuts down IIS as Security Alerts occur.
- **Firewall:** Applies an all-port firewall block for any IP that has been manually or automatically added to the Blocked List. See above. In ThreatSentry v4, this feature is not supported on Windows Server 2003 64bit or Windows XP 64bit).

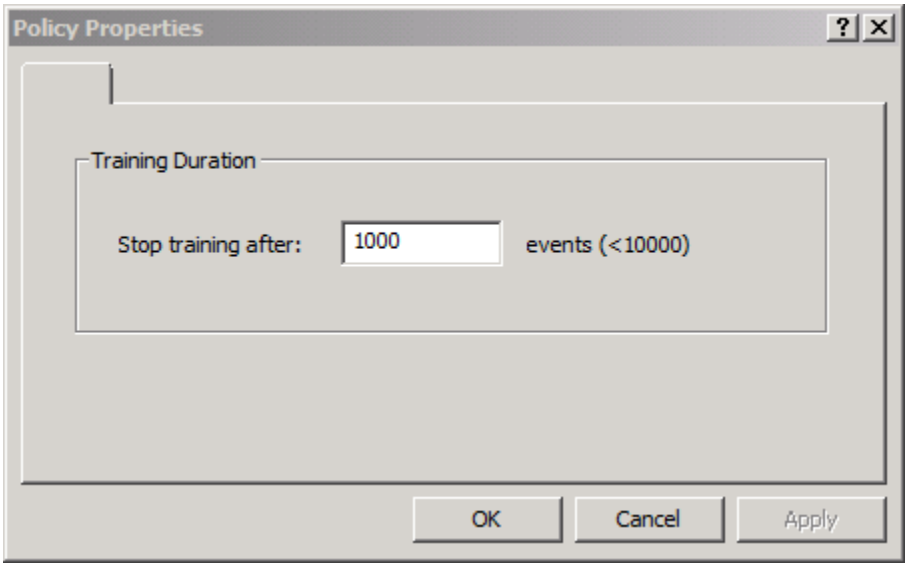
Request

The **Request** tab provides options related to how specific types of requests and alert display should be handled.

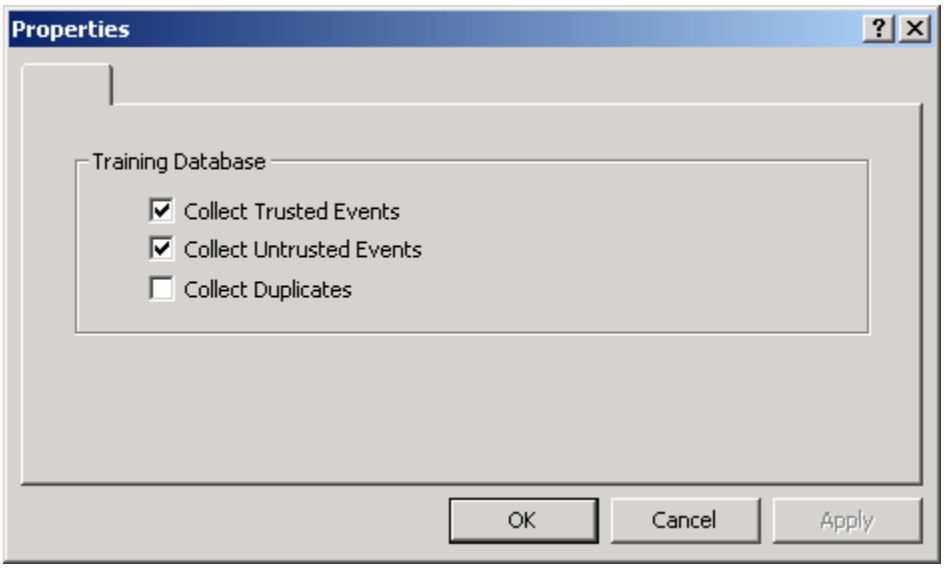


- **Use X-Forwarded-For Address:** X-Forwarded-For Addressing options.
- **Hide HTTPS request data:** When checked, sensitive data will not be displayed in the ThreatSentry (Security Alert Log, Alerts, Event Details, etc.)
- **Filter multi-part requests not larger than:** Provides an ability to define 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.

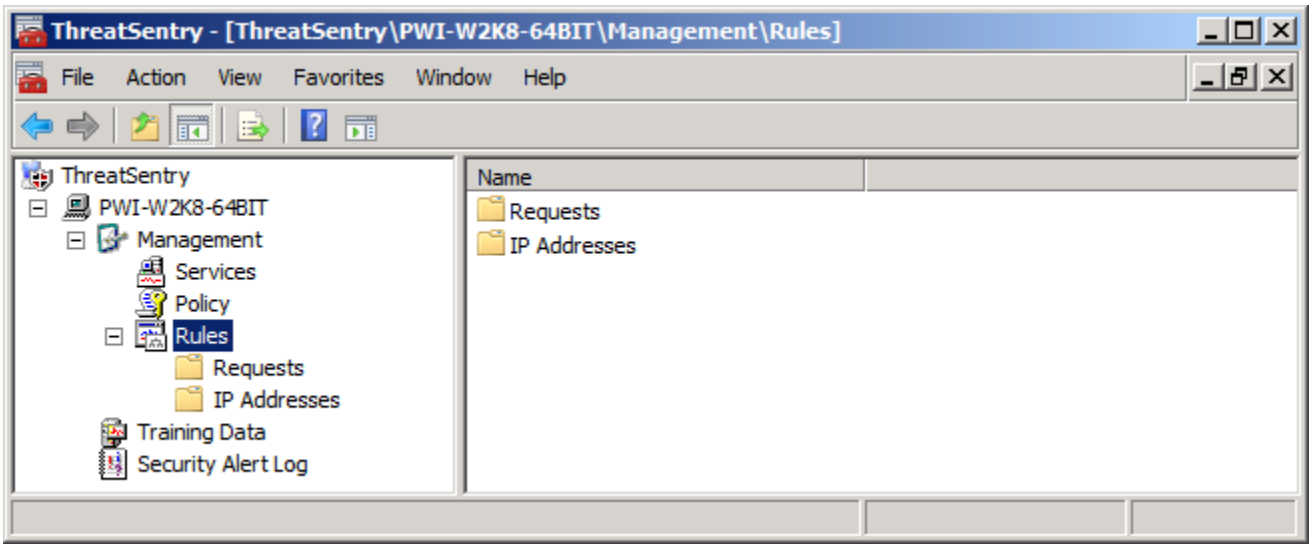
Two categories of rules exist:

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.

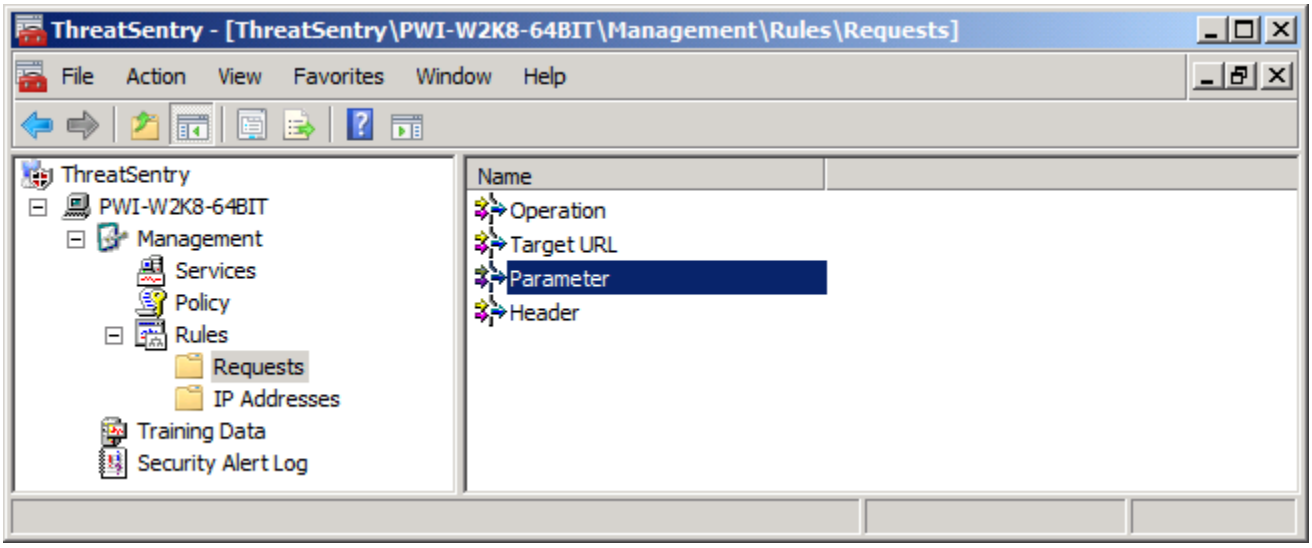


1) Requests

Most request filtering rules can be managed via the categories available in the right panel within the Requests folder. Although relatively simple to modify, adjusting any Request element rule requires special consideration of the web applications hosted on the server. Assistance is available through the technical support team at Privacyware (http://www.privacyware.com/TS_support.html).

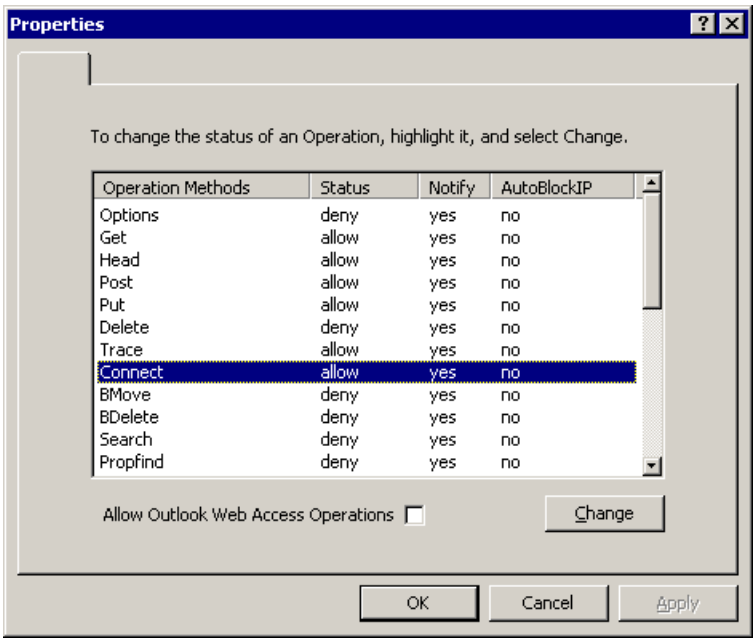
Note: Where a conflict exists, Deny Rules always supersede Allow rules. If, for example, a Deny rule specified in Parameter conflicts with an Allow Rule in Target, the Parameter Deny rule will take precedence over the Target Allow rule.

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

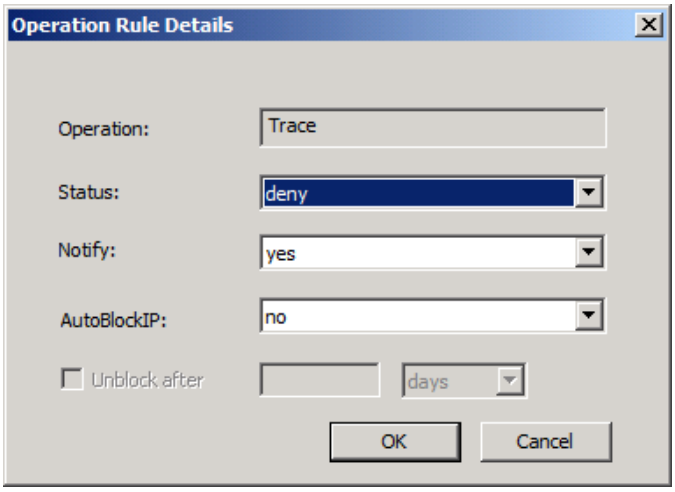
Specifies whether a particular Operation method should be allowed or blocked. To change the status of an Operation method, simply highlight it and select **Change**.



Important Note:
Outlook Web Access Support

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.

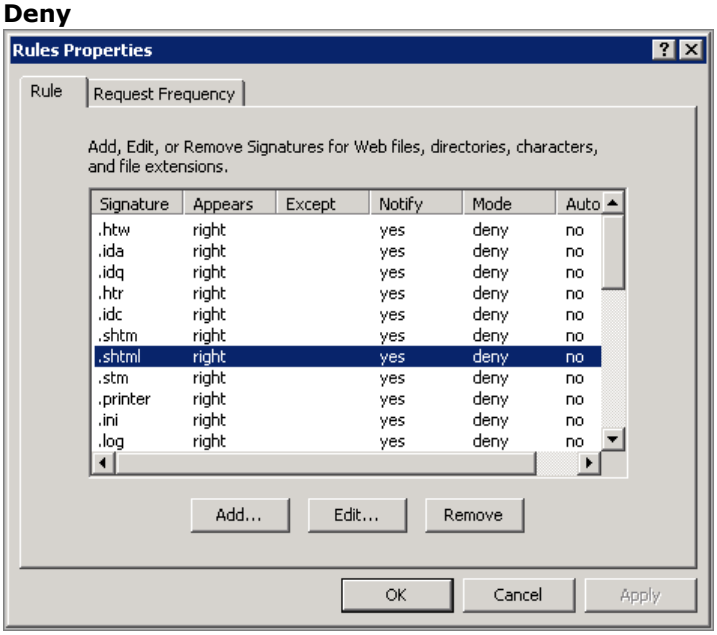


ThreatSentry offers several possibilities when changing the status of an Operation Method. The Operation may be **Allowed** or **Denied** and **Notification** can be **activated** or **deactivated**. In addition, the source **IP** generating the Untrusted event can be **added to the Blocked IP List automatically** 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.

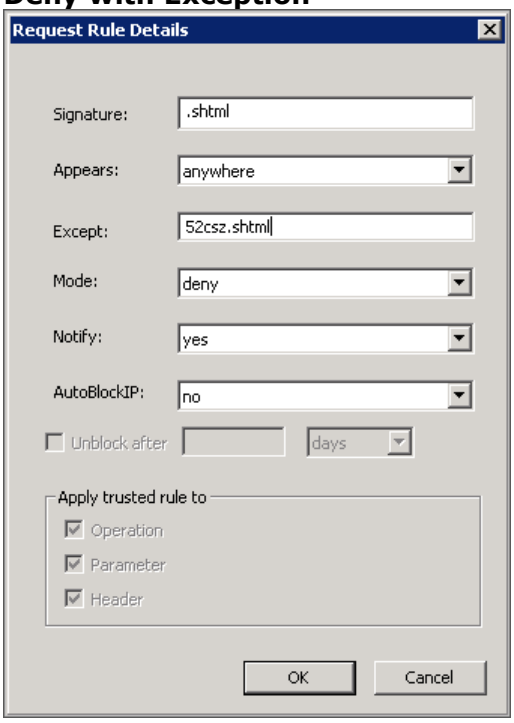
Target URL

Target URL Signatures can be **Denied** (Blocked), or **Denied with Exceptions**. In addition, specific web pages or page types can be designated **Trusted** (see White Listing/Positive Security Model details below). Denied or Trusted Target rules can also be **Disabled**. Signatures may also be Added, Edited and/or Deleted.

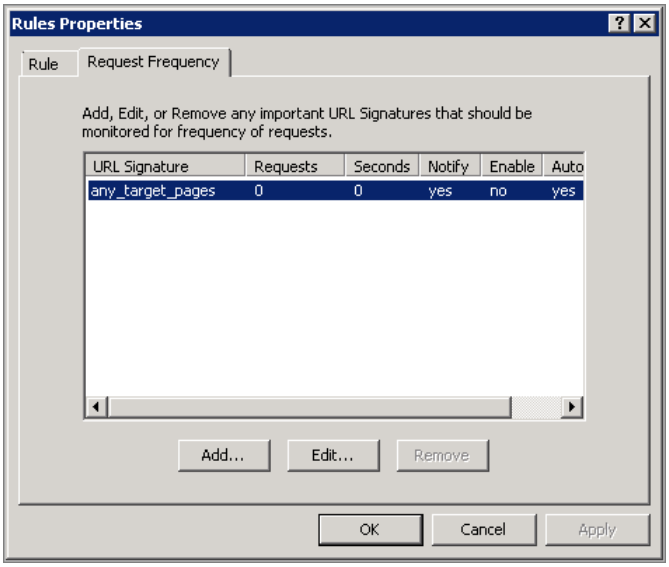
Deny

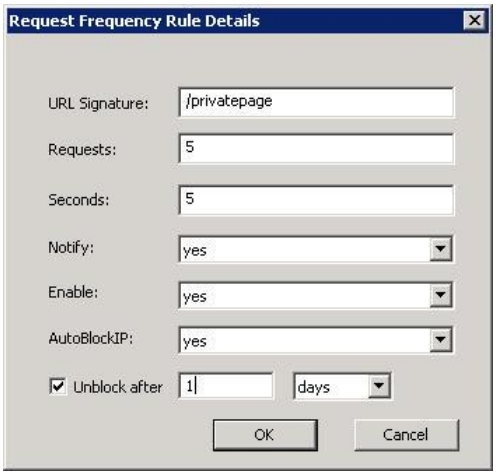


Deny with Exception

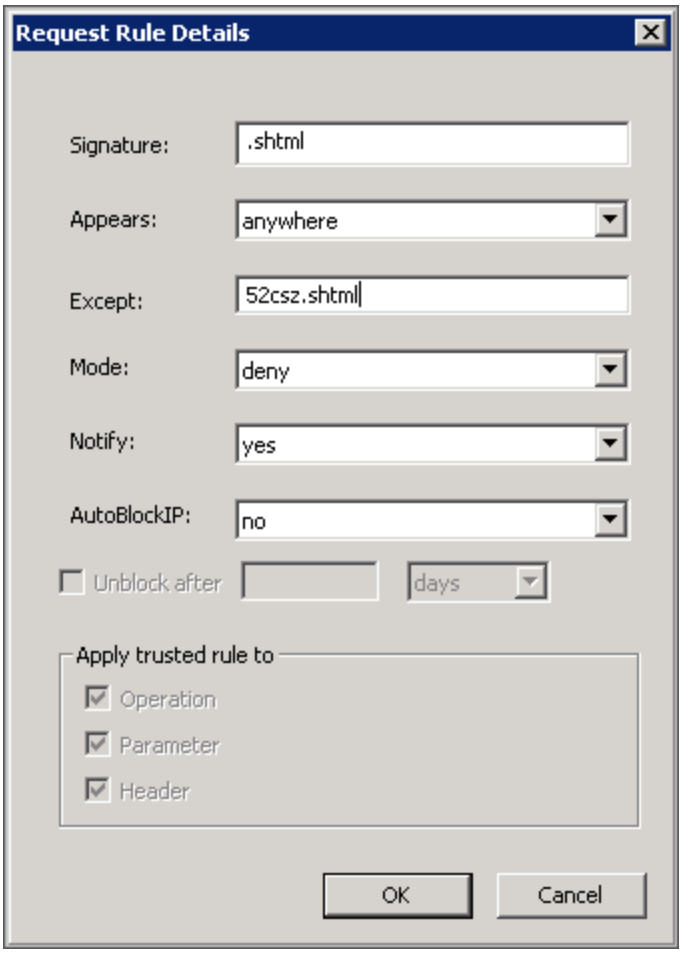


In addition to the general Target signature settings, specific rules and actions can also be applied to individual web pages via the **Target Pages** tab.





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



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

Target rules may be **configured to Deny, Disabled or Trusted. Trusted** application pages are white listed bypassing all or qualified (by Operation, Parameter and/or Header) threat filtering.

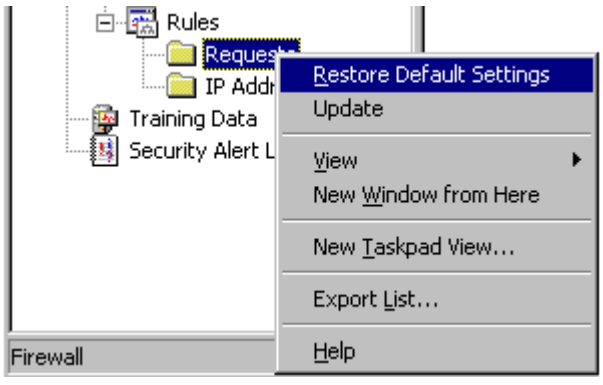
One or more exceptions may be defined for the Target and multiple exceptions may be entered and must be separated by a semi-colon ";".

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.

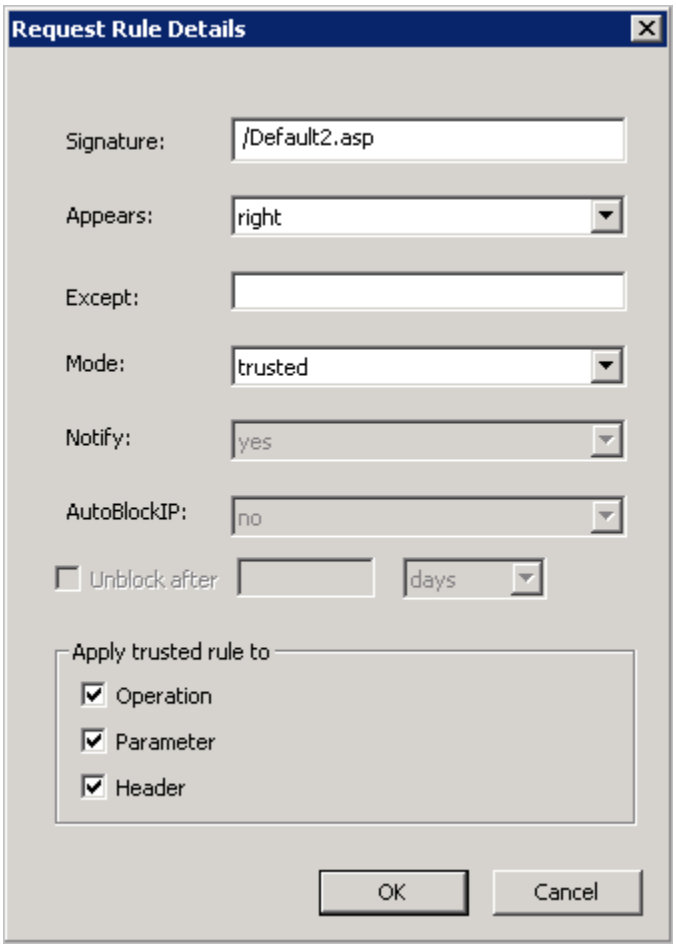
Note: To reset all rules to their default settings, **right-click** the **Requests** node in the left panel and select **Restore Default Settings**.



White Listing Web Application Pages

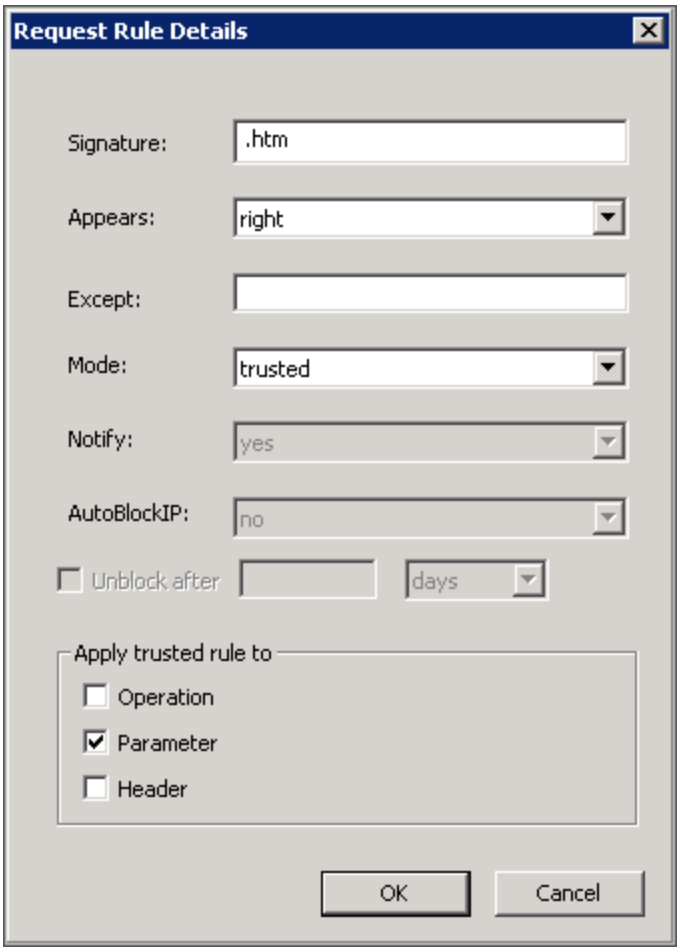
It's often desirable for testing or generally to be able to white list specific or broad types web pages. Pages designated as such in ThreatSentry are bypassed from all levels of filtering unless the source IP requesting the page is listed on the Blocked IP List (in this case, the Blocked IP List will take precedence over the Trusted status of the page itself).

Single page White Listing
Web application pages can be white listed individually as illustrated in the following screen shot. Go to **Rule**, **Requests** and double click **Target URL**. Select **Add** and enter the page name in the Signature field. From the **Mode** drop-down list, select **Trusted** and click **OK**. In the example provided, the Default2.asp page (located in any folder of server website) is added to the white list.



White Listing by Page Type

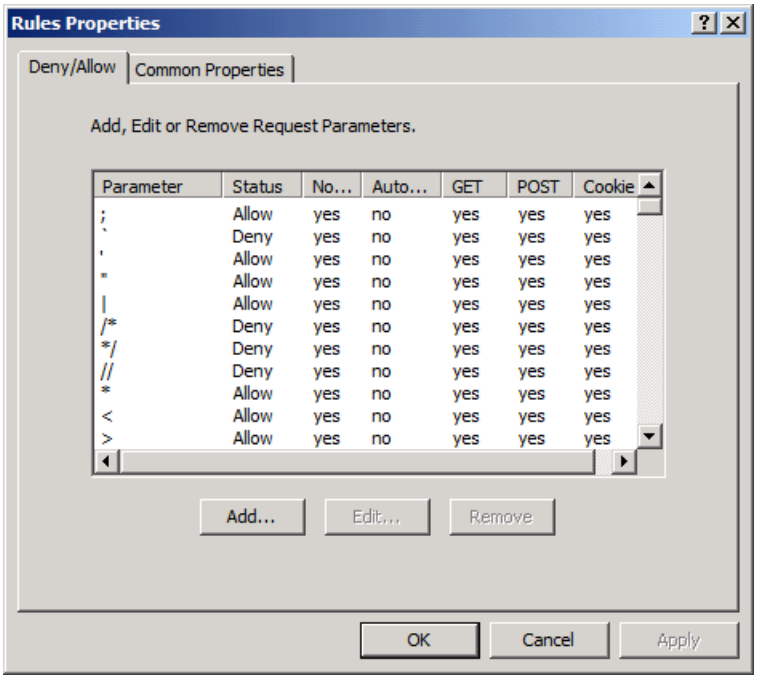
White Lists can also apply to broad types of application pages. For example, as illustrated in the screen shot below, the Signature .htm can be added with Appears - "right". Requests to all htm pages hosted on the server will be trusted (i.e. White Listed).



Exceptions can also be defined by adding the pages for which the white list should not apply. For example, adding “localhost/index.htm" in the **Except** field in the rule described above, will block all .htm pages with the exception of localhost/index.html.

Trusted rules may also be applied to one or more specific parts of the request – **Operation**, **Parameter** or **Header**.

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.

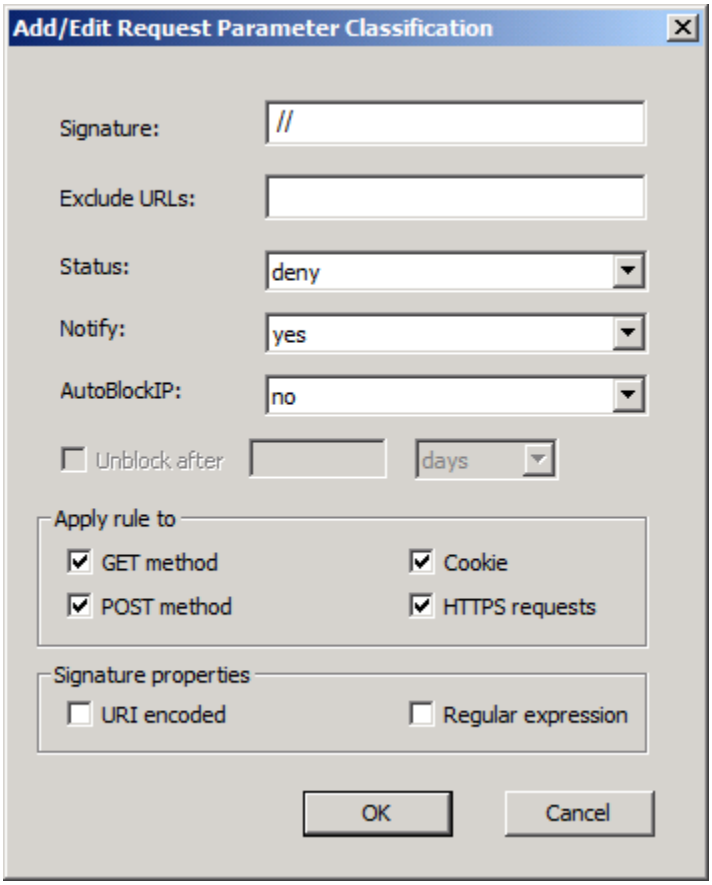
ThreatSentry provides a variety of configuration options for values passed within the parameter.

Exclude URLs: designates specific URLs that should be excluded from the rule. Multiple URLs should be delimited using ";" (e.g. /abc.html; def.php;…). A maximum of 2048 characters may be utilized in the Exclude fields.

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

Signature Properties:
- URI encoded: URI Encoding support enables text entered in the signature field to be decoded and then compared with decoded request string. For example, the "%20and%20" signature will be decoded as "and".

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

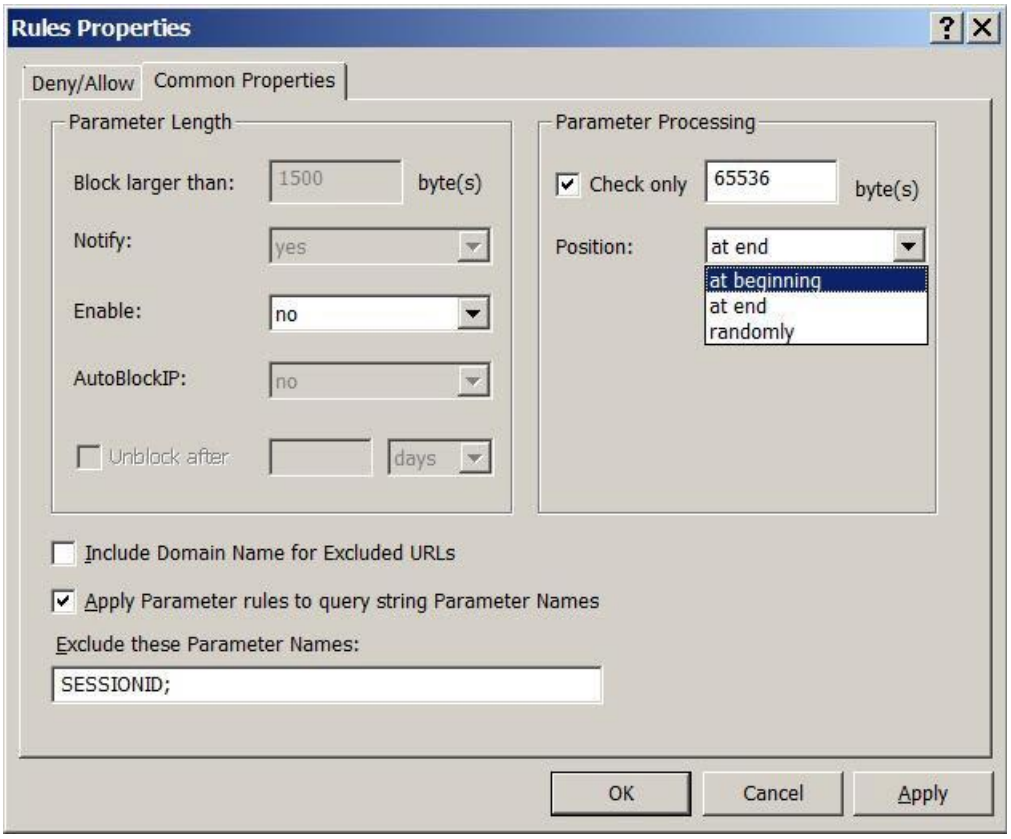


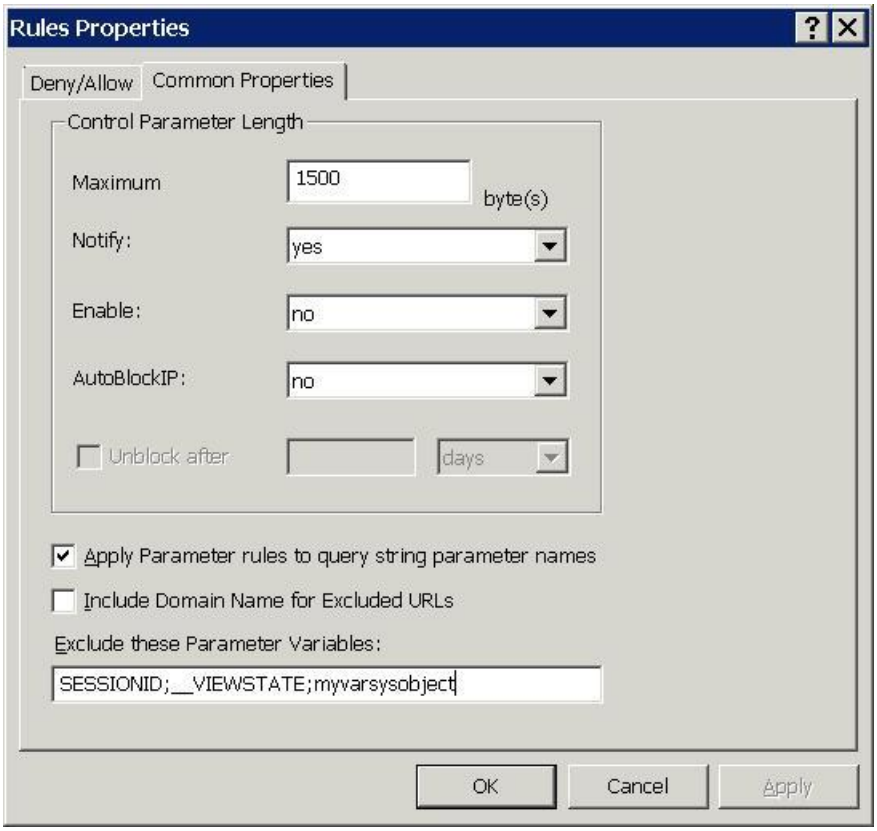
The Common Properties tab provides an ability to define the maximum parameter length within a request string. When this option is enabled, requests with parameters length that exceeds the maximum defined will be blocked.

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.

To optimize performance, request filtering can be restricted to a specific part of the parameter. Qualifying Parameter Processing on the basis of size, position and special presets for rules using Regular Expression (RegExp) are possible.





Other options on the Common Properties tab include:

- **Apply Parameter rules to query string parameter names***: ThreatSentry will consider the query string Name when filtering parameter rules (Excluded variables to this option can be defined).
- **Include Domain Name for Excluded URLs**:

*Note: A typical request might look something like the following:
"http://localhost/page1.htm?Xposition=100&Yposition=200"

Here, the full parameter string is: "Xposition=100&Yposition=200"

And, as in this example, typically consists of pairs: name=value. Here, the (variable) names are: "Xposition" and "Yposition"
And the values are: "100" and "200"

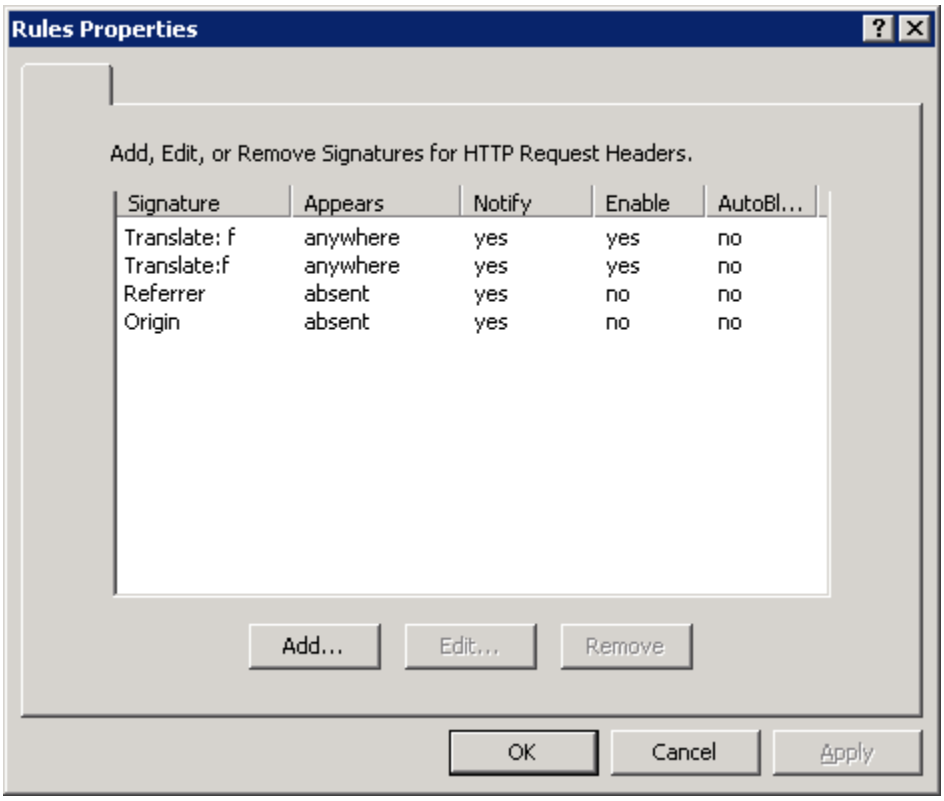
Sometimes, constants can be malicious for the Value, but benign for the Name. For example "sysobjects"
"http://localhost/page1.htm?myvarsysobject=yes" is a normal request (for Name), but constant "sysobjects" being used in Value often indicates a Javascript injection attempt.

On the other hand, some rules (for example "onload *=") are always dangerous for both Names and Values.
In such cases, "Apply Parameter rules to query string parameter names" can be enabled so that the entire parameter string (…?Xposition=100&Yposition=200") will be analyzed.

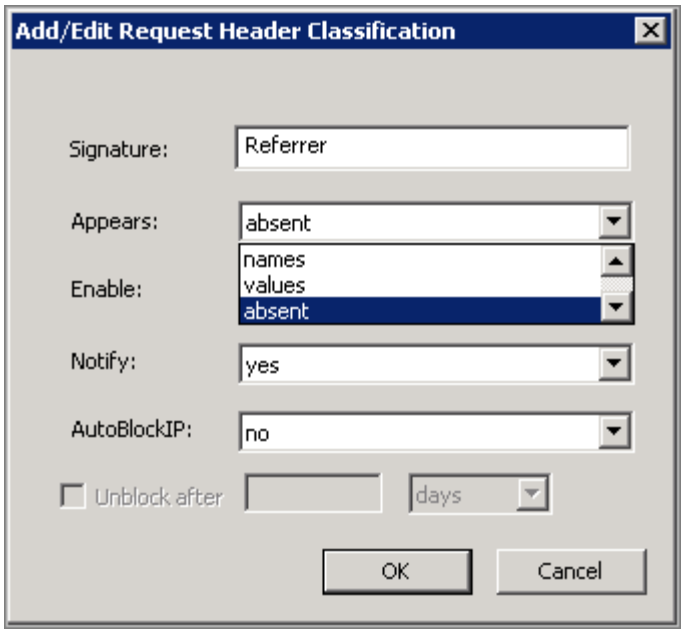
However, sometimes the Web Application uses predefined Names to store specific data (often in binary format). For example: "http://localhost/page1.htm?myvarsysobject=yes&var1=%0x.. & __VIEWSTATE=..'...%..&..". In this case, __VIEWSTATE contains dangerous symbols, but the data is compressed to avoid problems. In this case, variables can be excluded from analysis. In this example then, only "var1=%0x.. " will be analyzed.

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.



Highlighting a Header signature and clicking the Edit button enables the signature to be enabled or disabled and its properties to be modified.



Cross Site Request Forgery – CSRF

Cross Site Request Forgery (CSRF) - Header rules "referrer" and "origin" in absent mode can be effective in addressing Cross Site Request Forgery (CSRF) attacks.

Headers can be filtered and controlled as they might appear in four different locations (select Appears drop down menu).

1) "anywhere": Signature value will be matched as a simple substring in Raw headers, for example (request with headers):
GET /index.htm?var=simple HTTP/1.1
translate:F
x-referrer:localhost
Host: localhost
Accept: */*
X-customheader: encodedheader

2) "names": Signature value (including substring in Name) will be matched with header names only (i.e. left part, before ":" delimiter).

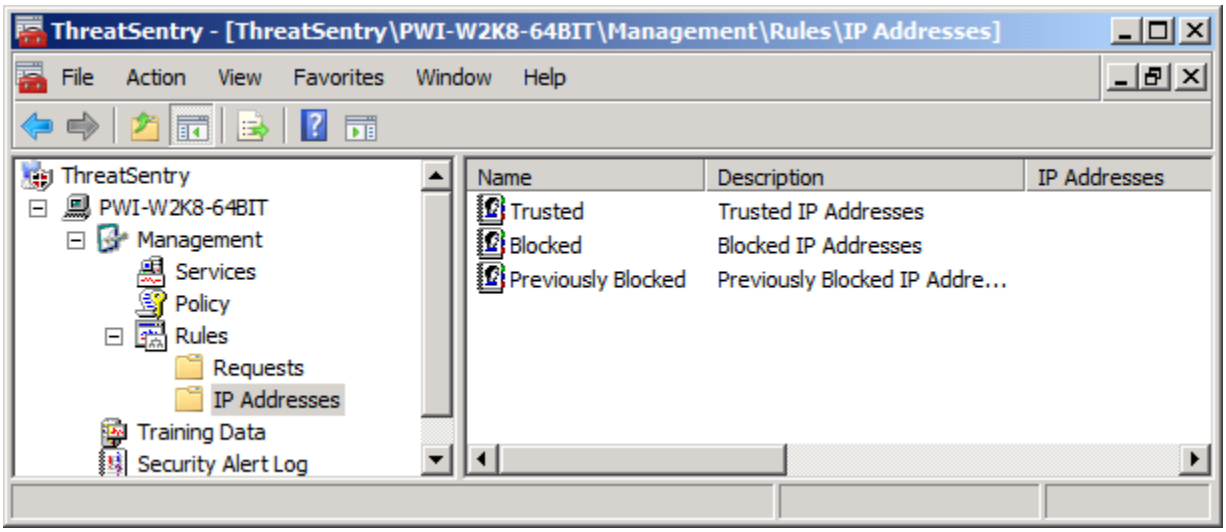
3) "values": Filters for requests which contain specified Signature value in header part after ":" delimiter).

4) "absent": Filters for requests missing the specified header name.

Note: Cross Site Request Forgery (CSRF) - Header rules "referrer" and "origin" in absent mode can be effective in addressing Cross Site Request Forgery (CSRF) attacks.

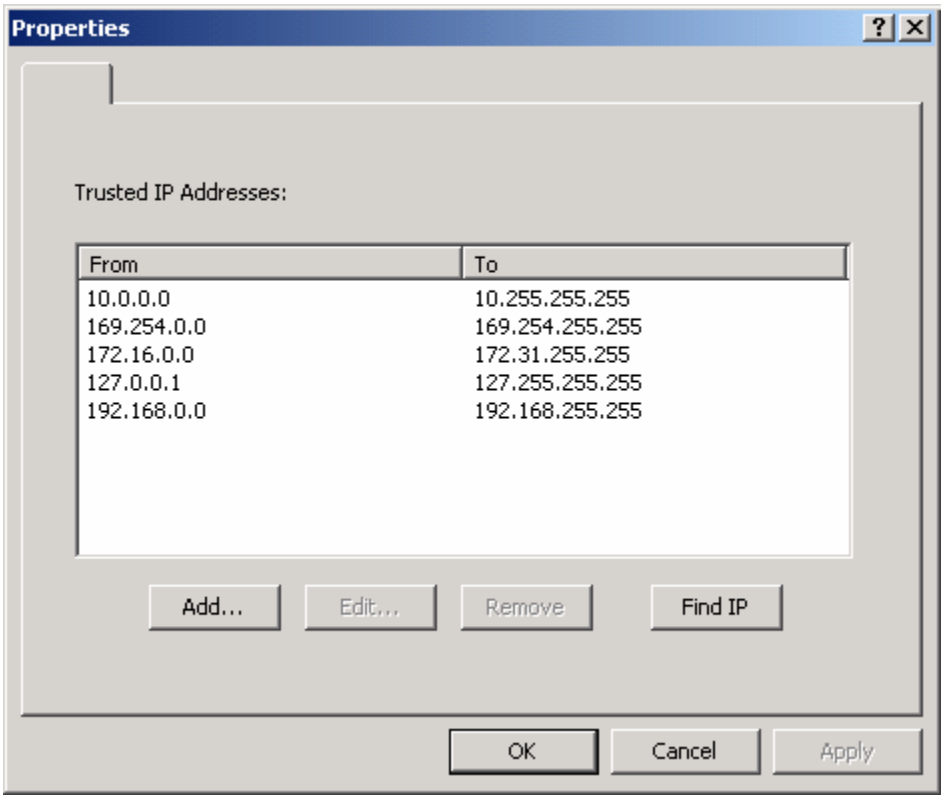
2) IP Addresses

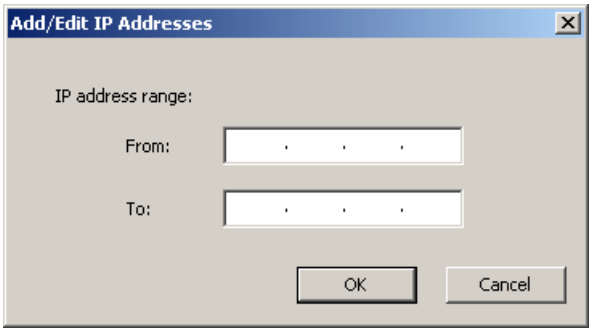
The **IP Addresses** node allows IP addresses and IP ranges to be designated as **Trusted** or **Blocked**. IPs that were at one point designated Untrusted can be viewed by double-clicking **Previously Blocked** in the right panel.



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.

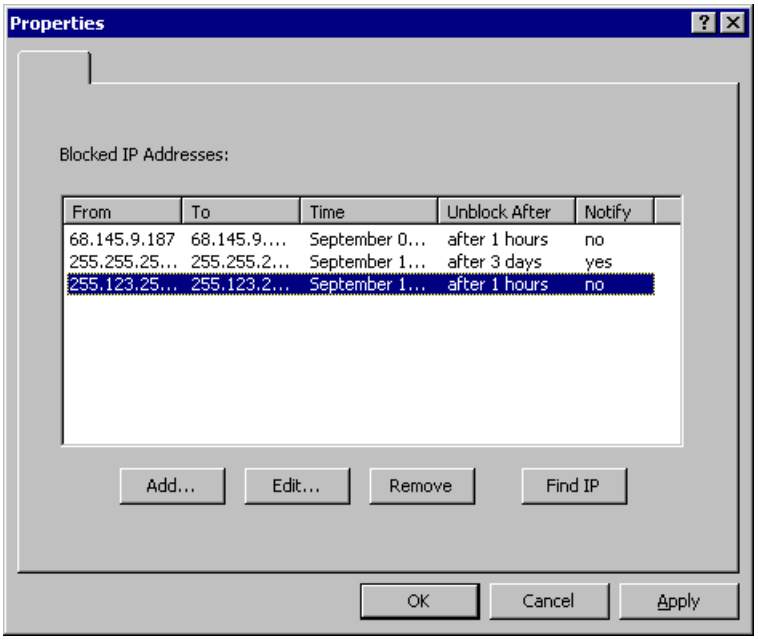


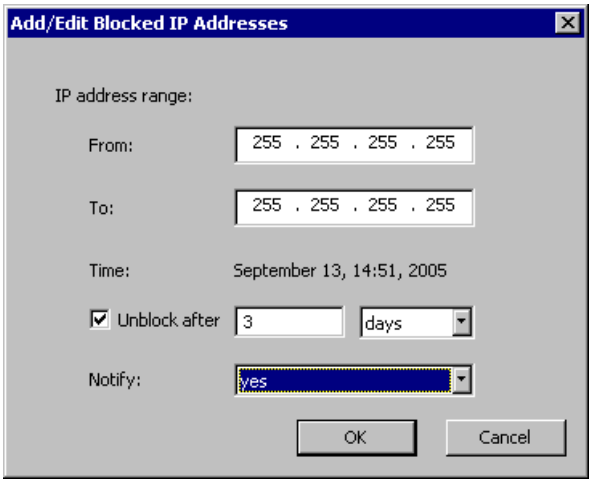


Address ranges dedicated to a particular purpose (i.e. WebDAV, Network Printer IPs or Network File Server IPs, etc.) can be added to the Trusted IPs. If the IP range is a single IP, the identical IP address should be entered into both the **From** and **To** fields.

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.

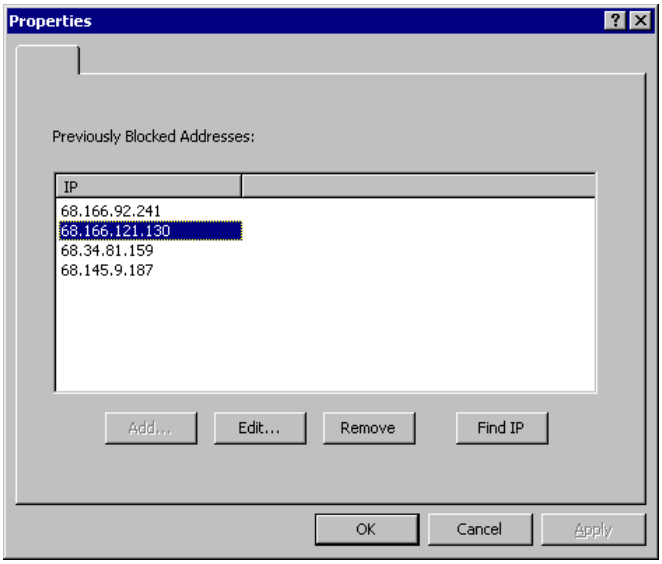
The IP/s can be released from the Blocked List after a specified time period.

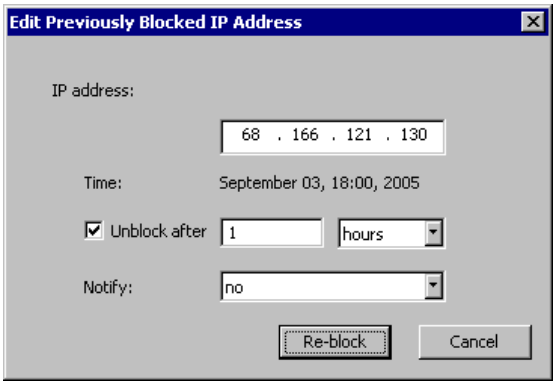
The Time the IP was added to the Blocked List is recorded.

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.

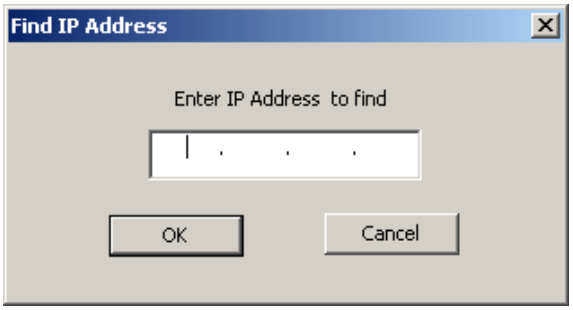




Previously Blocked IPs can also be Re-Blocked.

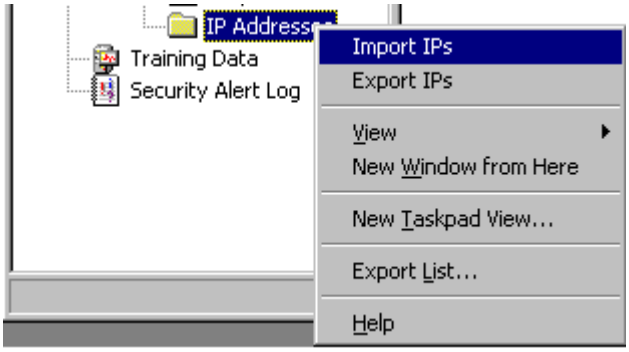
Find an IP Address

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.



Filtering Rules and IP Address Backup

ThreatSentry provides an ability to backup/archive rules and settings for filtering rules and IP Addresses.

1) **Import/Export Rules** - Right mouse click the **Requests** folder and select **Export Settings** to export the rules to an xml formatted file. This file can be similarly imported via right mouse click and selecting **Import Settings**.

2) **Import/Export IPs** - Right mouse click the **IP Addresses** folder and select **Export IPs** to export the rules to an xml formatted file. This file can be similarly imported via right mouse click and selecting **Import IPs**.

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 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.

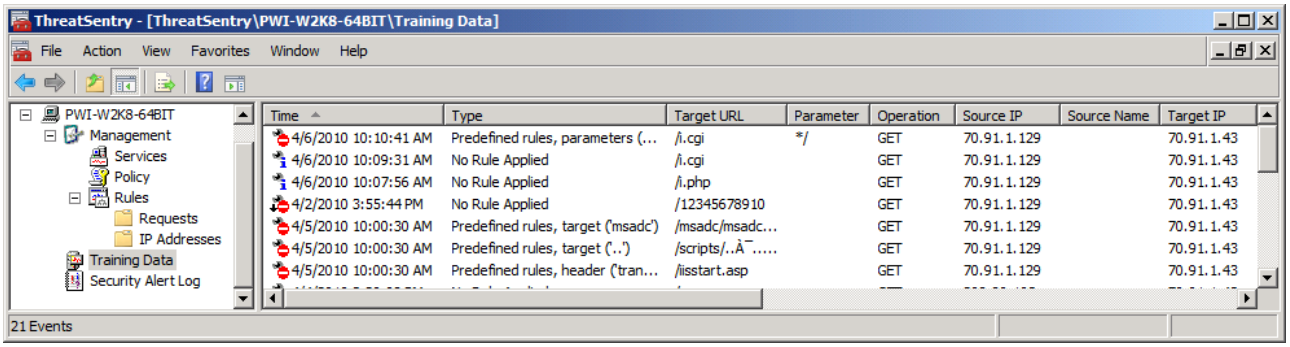
Note: When using existing IIS logs for training, ThreatSentry will process the log from the earliest date first. So, if a log spanning 12/1/2009-12/31/2009 is selected, and ThreatSentry has determined that 1000 events are required for the baseline, the 1000 events within the log that have the earliest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

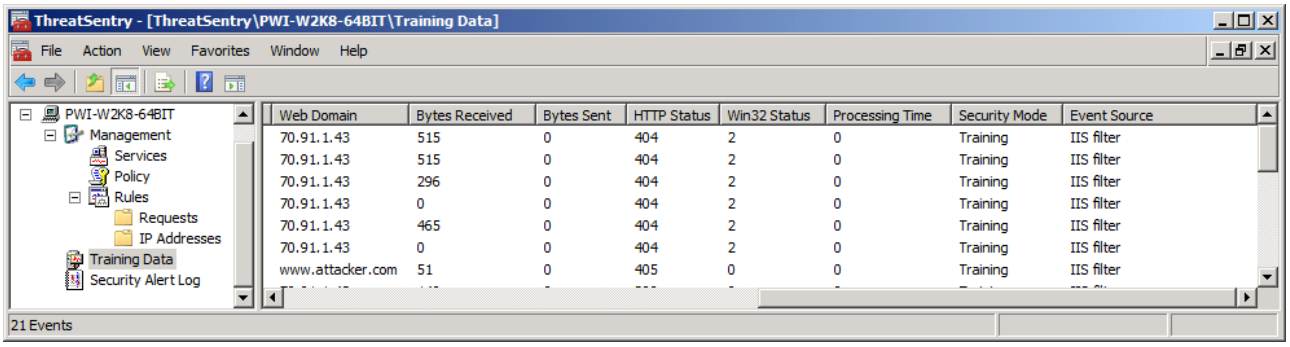
The Training Data view can be invoked by selecting the Training Data node in the left pane. By default, events are listed in the order in which they occurred, the most recent appearing on the top of the window. Events may also be sorted by column. Events displaying a **red icon** are considered **Untrusted**.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

Training Data Display

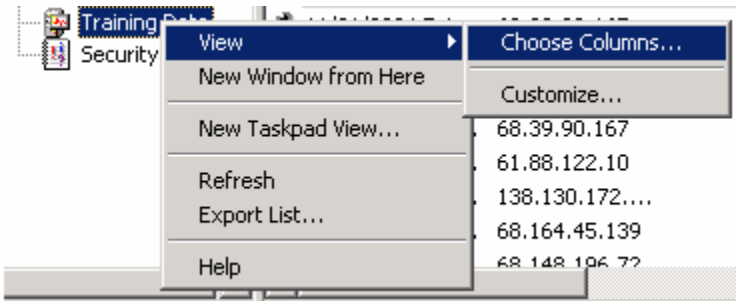
The screen shot below shows the first eight columns that are displayed in the Training Data view: **Time, Type, Target URL (URL Path), Parameter, Operation, Source IP, Source Name and Target IP.**



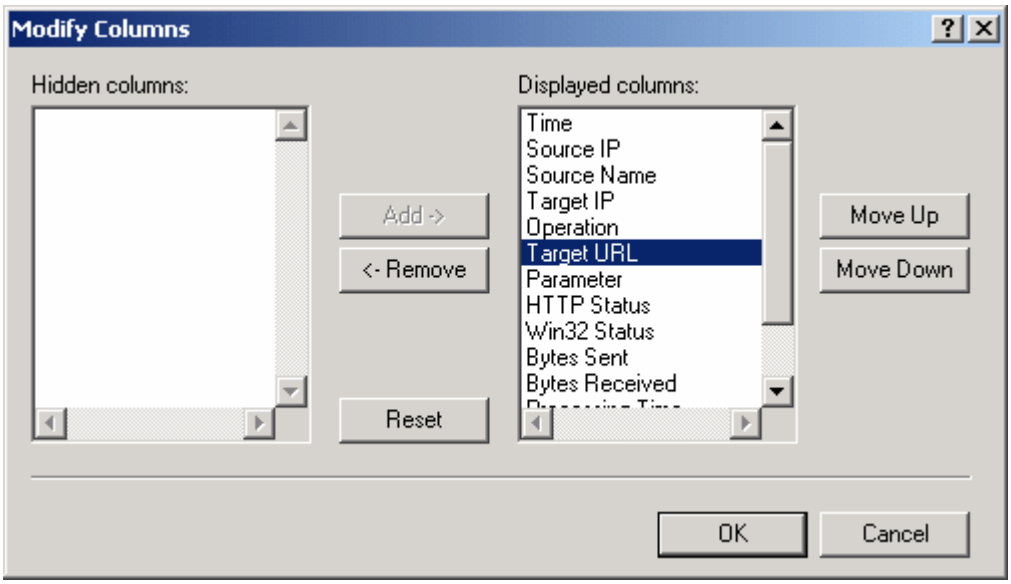
The following screen shows the other columns in the Training Data view: **Web Domain, Bytes Received, Bytes Sent, HTTP Status, Win32 Status, Processing Time, Security Mode and Event Source.**



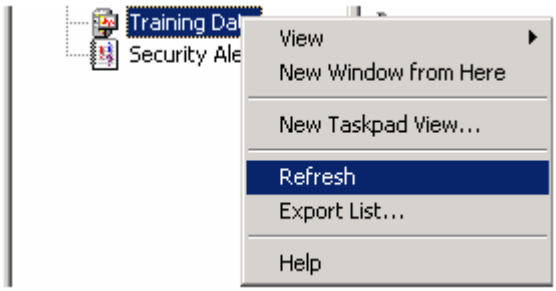
The columns displayed in the Training Data view can be modified by **right mouse clicking the Training Data node** and selecting **Choose Columns**.



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

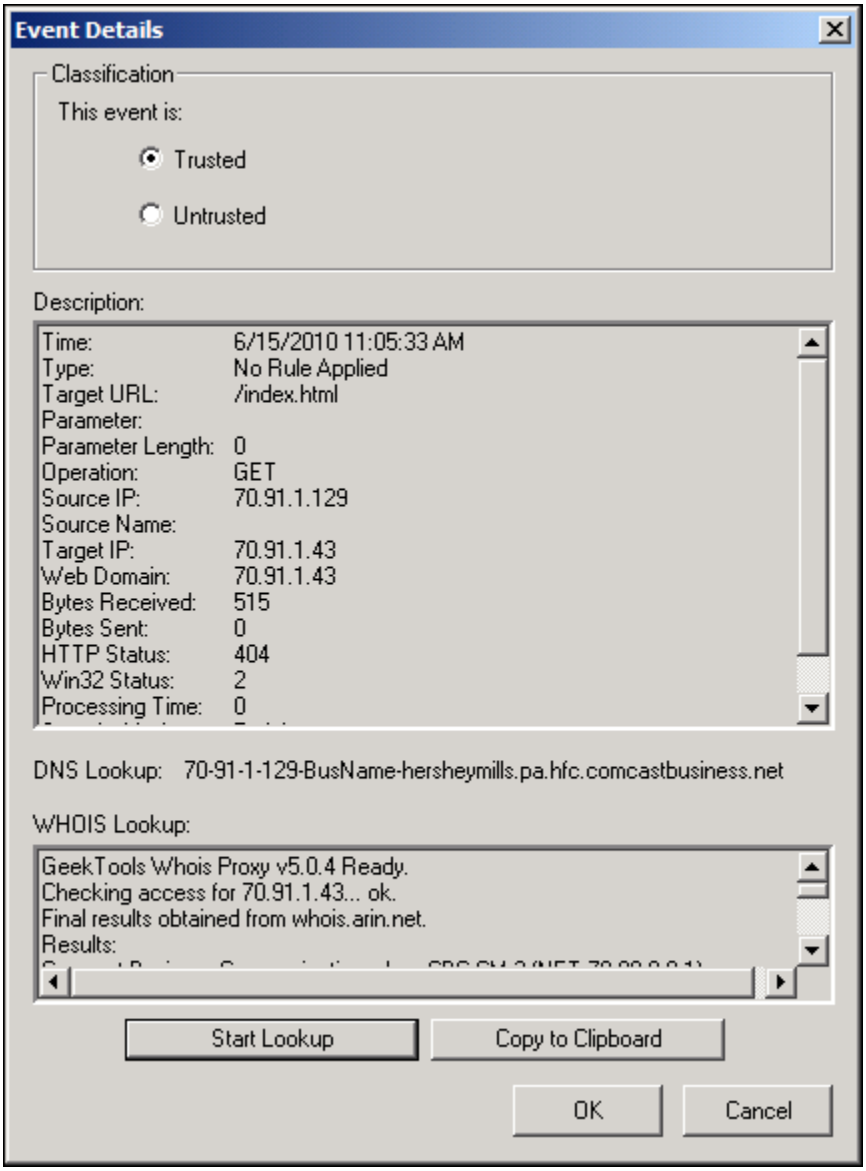


You may also **Refresh**, **View** or **Export** the Training Data to another location by Right mouse-clicking the **Training Data** node in the ThreatSentry tree root.



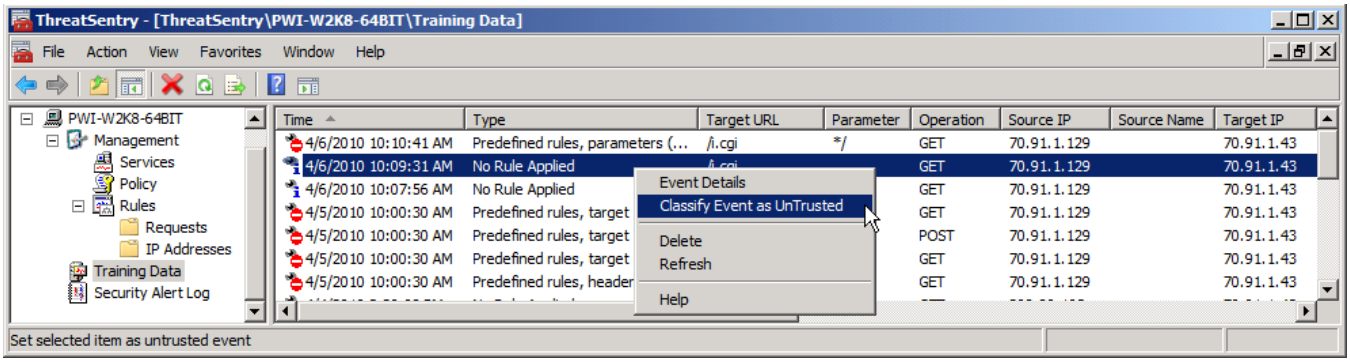
Training Data Details

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.

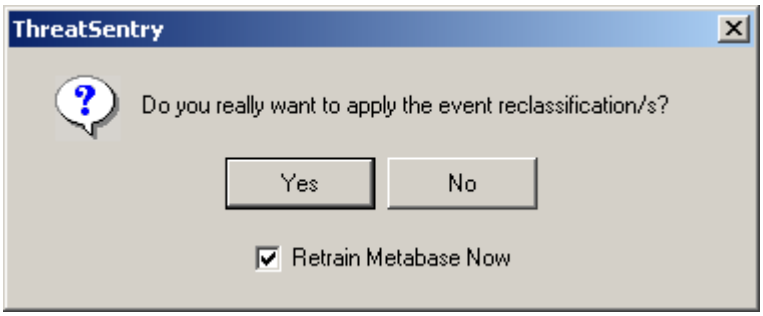


Note: Events will not be added to the Training Database if generated from an IP on the Trusted IP List.

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.**



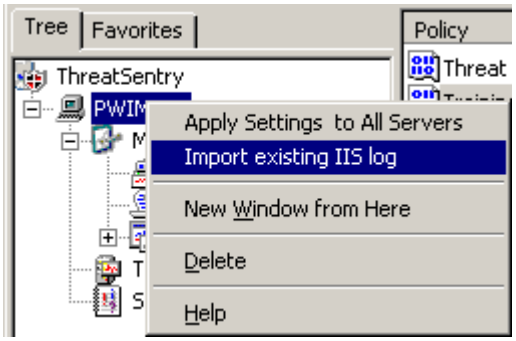
Events that have been reclassified from **Untrusted** to **Trusted** will be designated with a small arrow at the left of the blue icon.

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**.

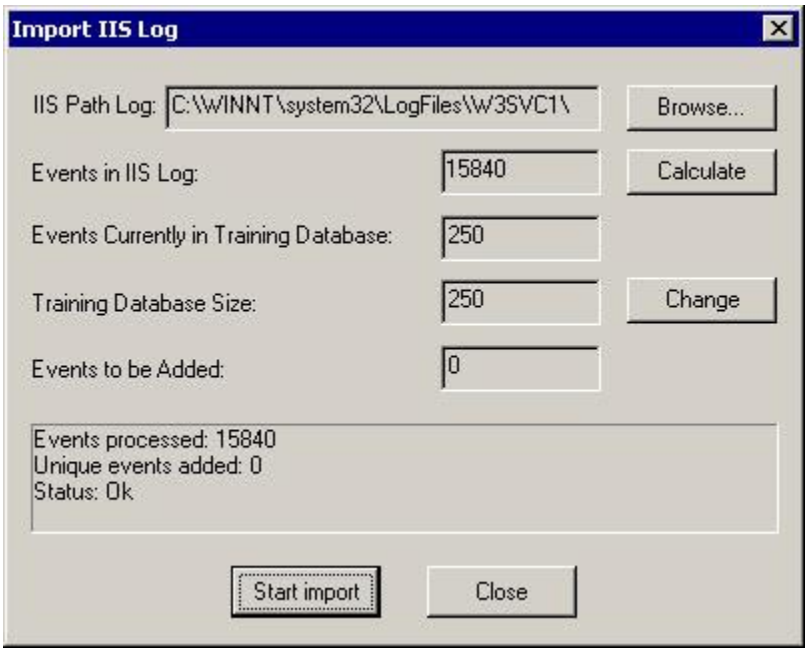
Training using Existing IIS Logs

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.

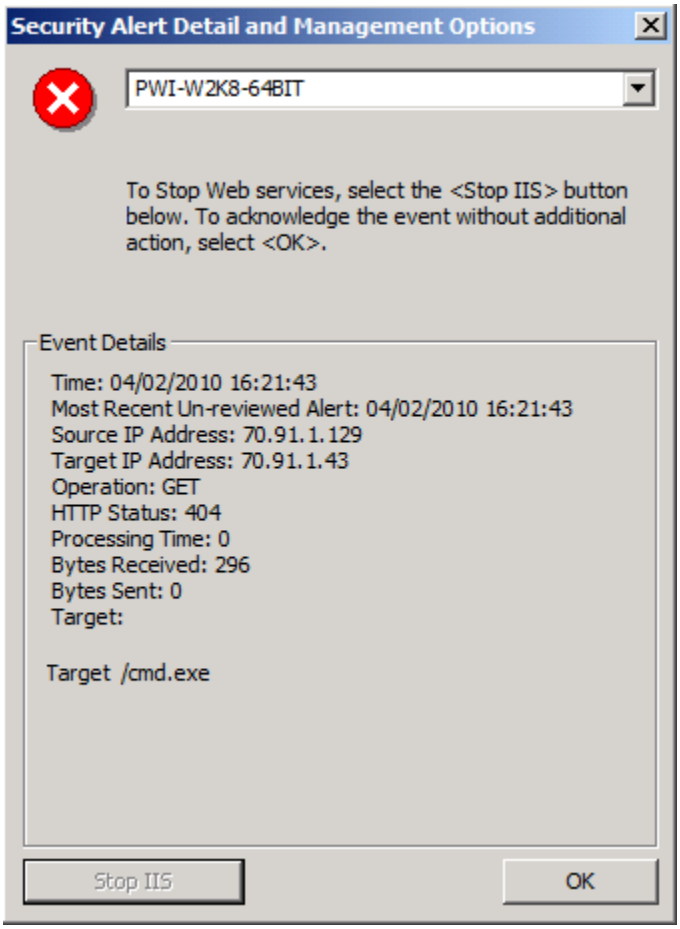
When using existing IIS logs for training, ThreatSentry will process the log from the earliest date first. So, if a log spanning 12/1/2009-12/31/2009 is selected, and ThreatSentry has determined that 1000 events are required for the baseline, the 1000 events within the log that have the earliest dates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

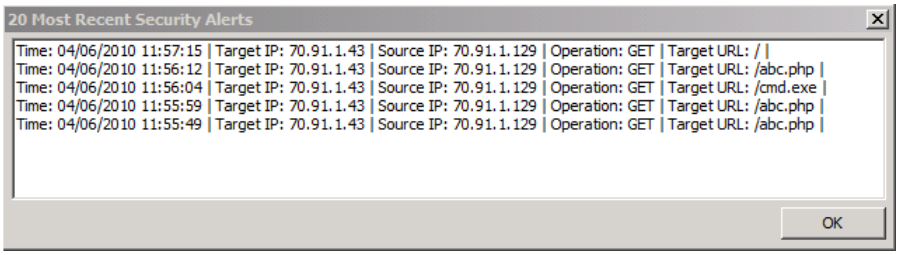
Security Alerts

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.

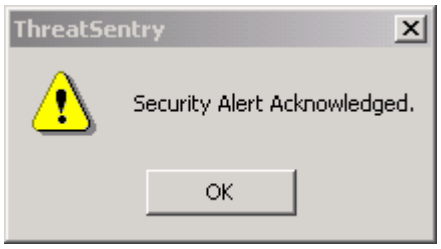


- Selecting **OK** will simply acknowledge the event and eliminate the window.
- If the event has been misclassified, the **Security Alert Log** should be reviewed and the event reclassified. The Security Alert Log can be viewed by double-clicking the Security Alert Balloon or selecting the Security 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.



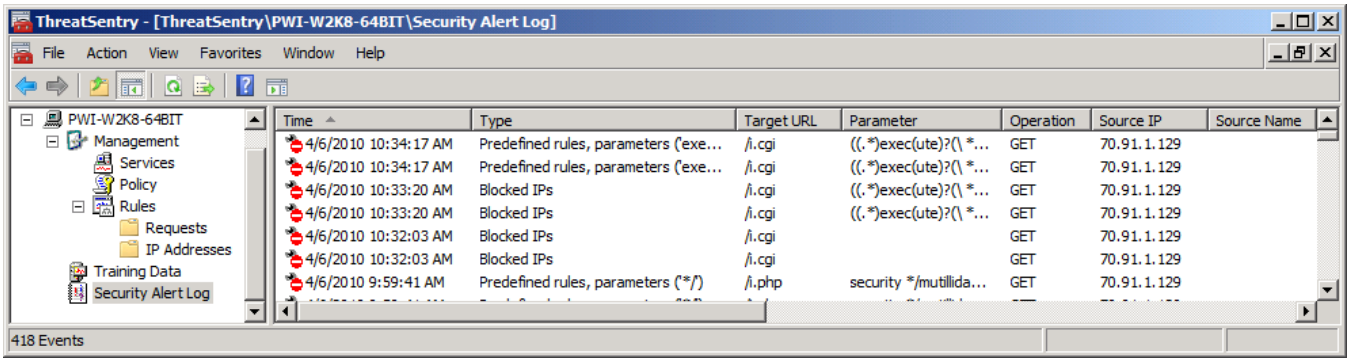
Once the Security Alert has been acknowledged, one final window will appear.



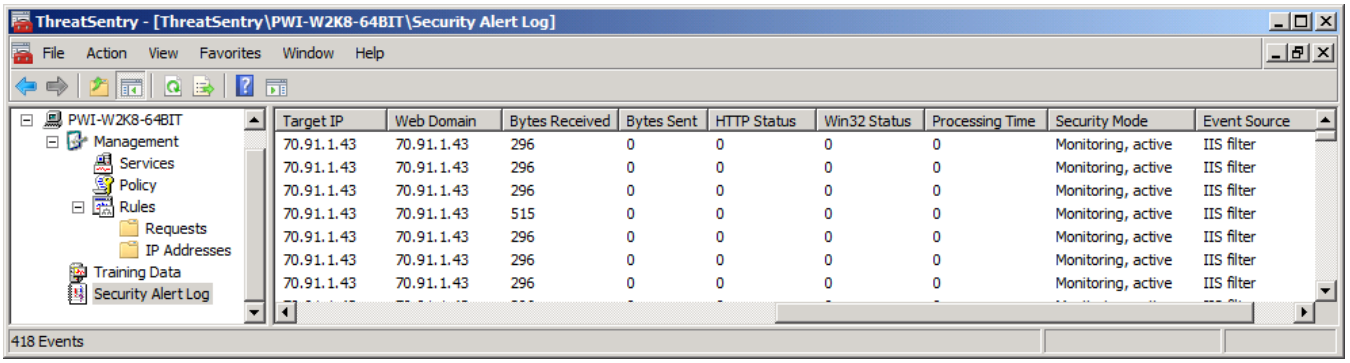
Security Alert Log

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.

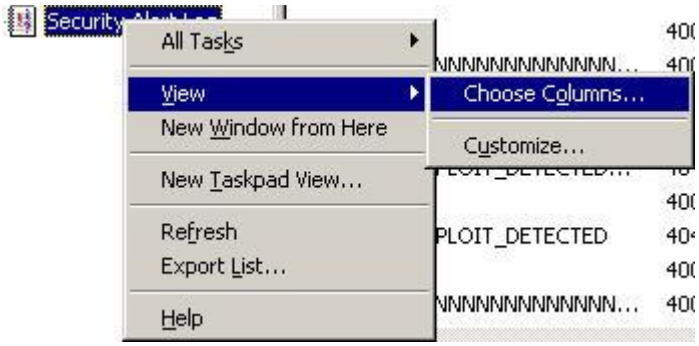
The screen shot below shows the first seven columns that are displayed in the Security Alert Log: **Time, Type, Target URL, Parameter, Operation, Source IP and Source Name**.



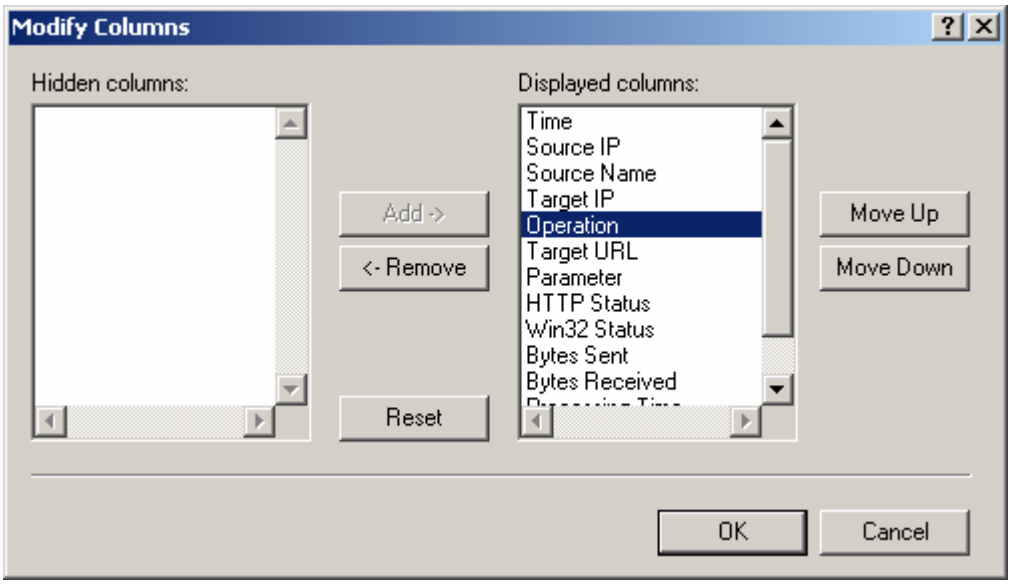
The following screen shot shows the other columns in the Security Alert Log: **Target IP, Web Domain, Bytes Received, Bytes Sent, HTTP Status, Win32 Status, Processing Time, Security Mode and Event Source**.



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.

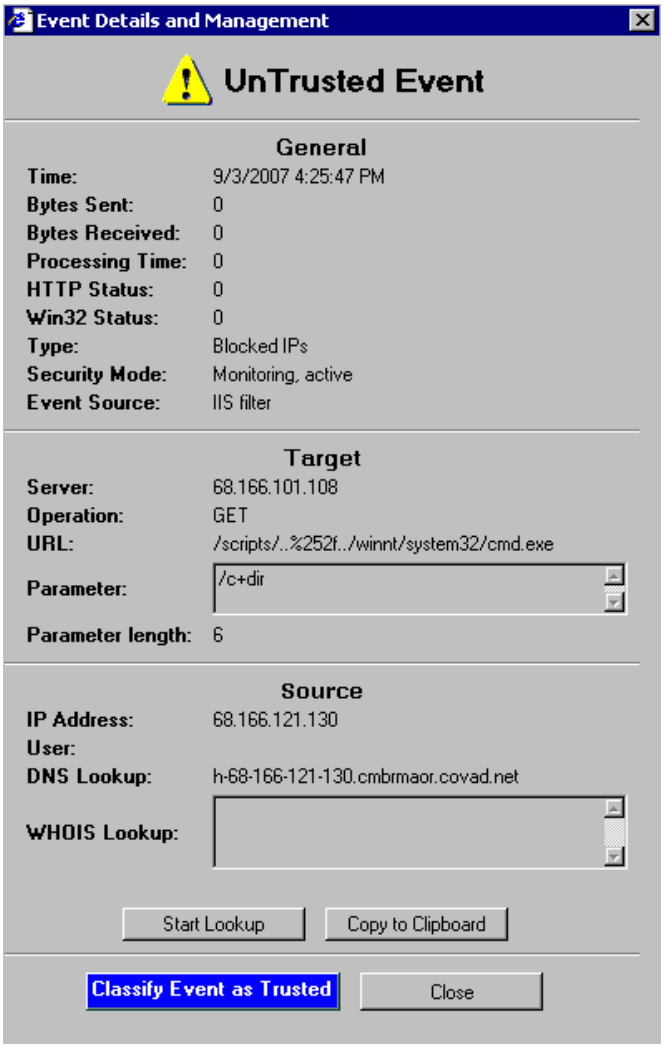


Working with the Security Alert Log

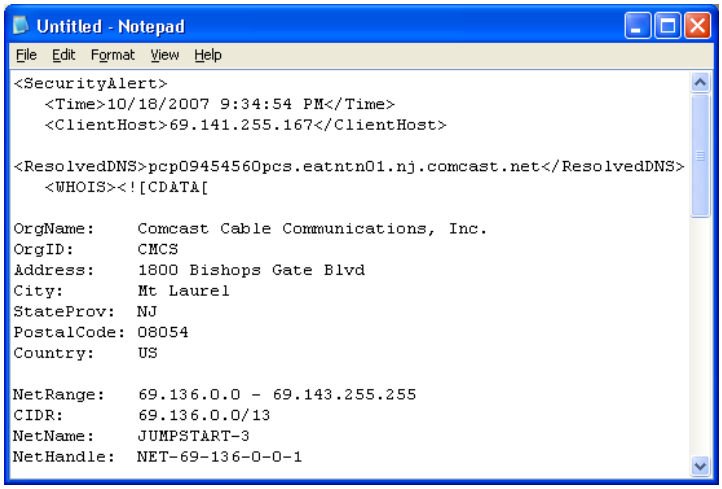
The process of event review, reclassification, and periodic retraining is a key maintenance requirement of ThreatSentry's Behavioral Engine that ensures optimal protection and accuracy. Regular attention applied to proper classification of events, adjustments to the knowledgebase, and maintenance of 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.

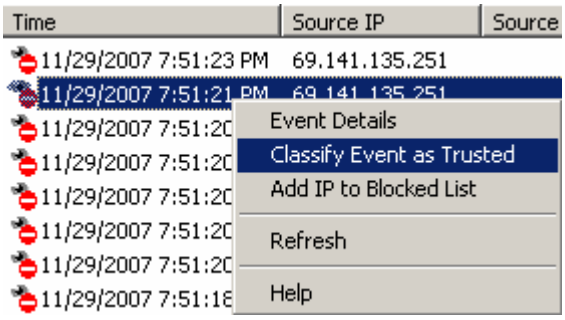


- Information in the Event Details and Management screen corresponds to the information in columns of the Security Alert Log.
- WHOIS Lookup can be used to identify the source IP and other information about the request source.
- WHOIS information can be copied to the clipboard for further reference and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

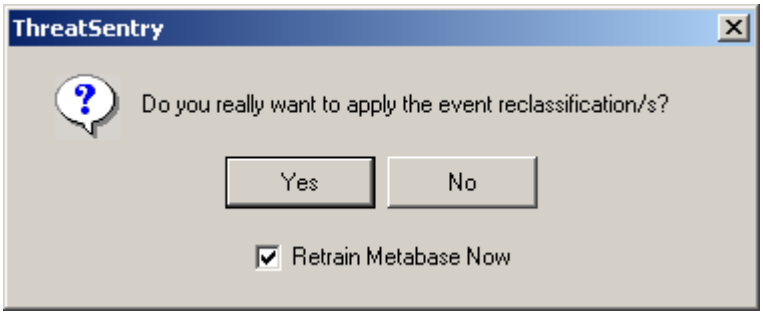


- Event reclassification can be applied.

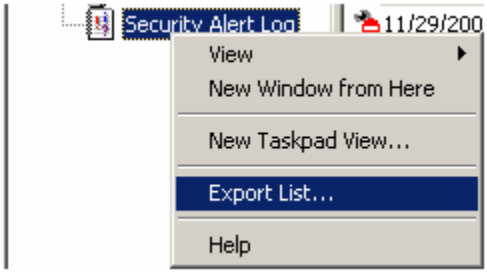
Right mouse-clicking an event in the Security Alert Log also provides the ability to re-classify an event immediately.



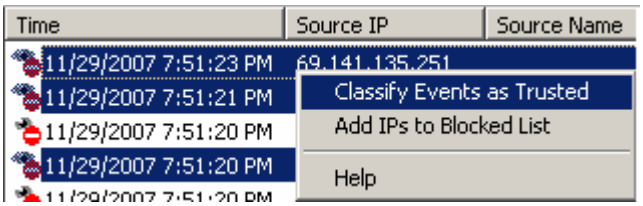
Once selected, ThreatSentry will prompt you to ensure that the event reclassification is accurate.



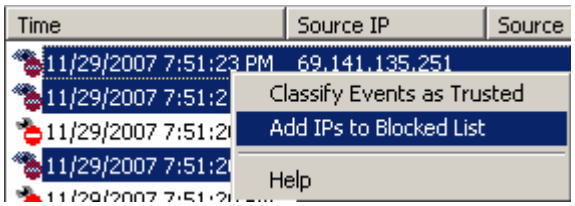
The Security Alert Log can be exported by right mouse-clicking the Security Alert Log node in the ThreatSentry console.



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

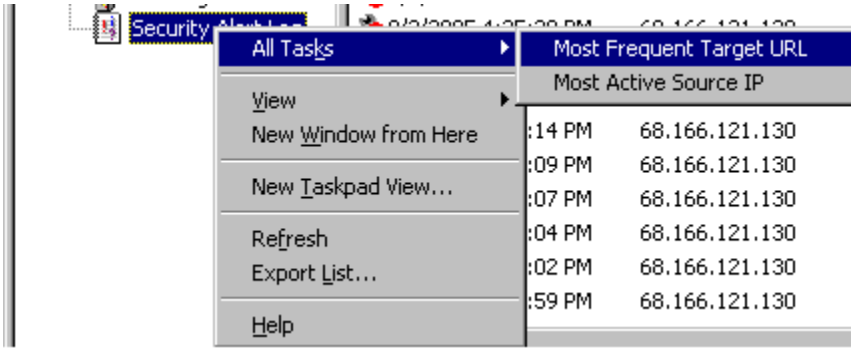


Single or multiple IPs that generated the Security Alert's can also be added to the Blocked List via the right mouse function.



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**.



SQL Server backup and Security Alert Log Maintenance

ThreatSentry limits the display of events to display in the Security Alert Log to 100,000 (for optimal SQl Server and MMC performance). If this threshold is met, all requests continue to be monitored and filtered, but those determined to be bad (via the rules-engine, firewall or behavioral engine) are simply not written to the relevant SQL Server tables. The following steps provide a native mechanism for backing up (archiving) the SQL Database and Security Alert Log.

3) In the left panel of ThreatSentry, apply right mouse to the server name and select Backup Database (a .bak file will be stored within the log folder in the ThreatSentry Program Files Directory).

4) Then Purge Older Security Alerts (via same right mouse click on server name) - reducing the number to a few hundred or so events.

X. Regular Expression Guidelines

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

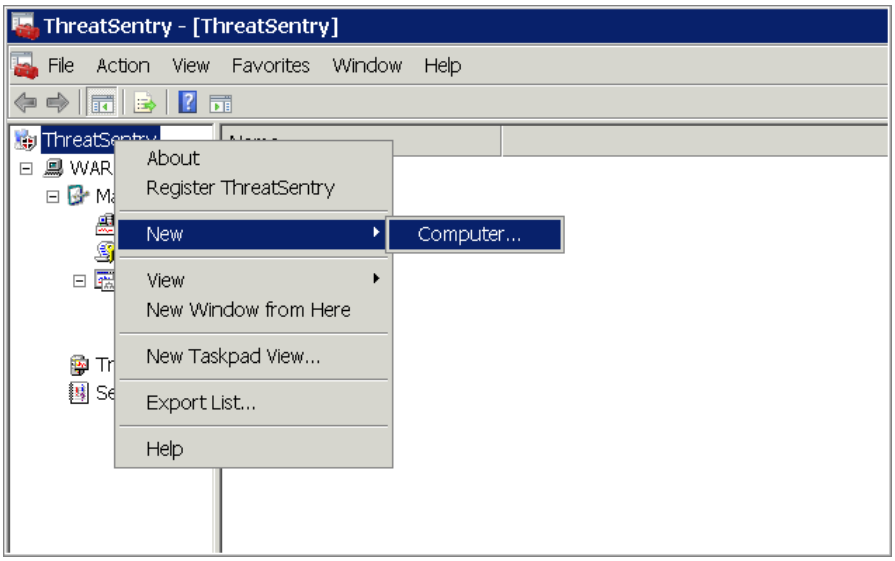
Metacharacter	Meaning
.	Matches any single character.
[ ]	Indicates a character class. Matches any character inside the brackets (for example, [abc] matches "a", "b", and "c").
^	If this metacharacter occurs at the start of a character class, it negates the character class. A negated character class 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 *n*, it matches the *n*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.

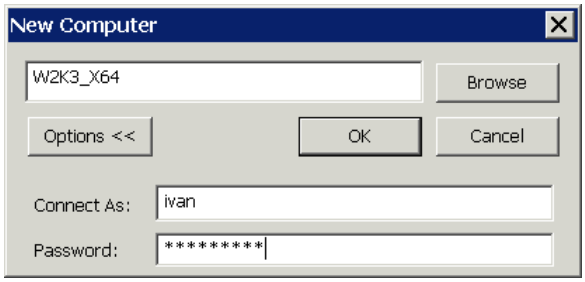
XI. Central Management of Multiple Server Systems

Multiple installations of ThreatSentry (where ThreatSentry has been installed on multiple servers within the same domain\workgroup) can be managed natively from a single "master" MMC console. To do so, open the ThreatSentry AdminConsole on the server that will be used as the master console.

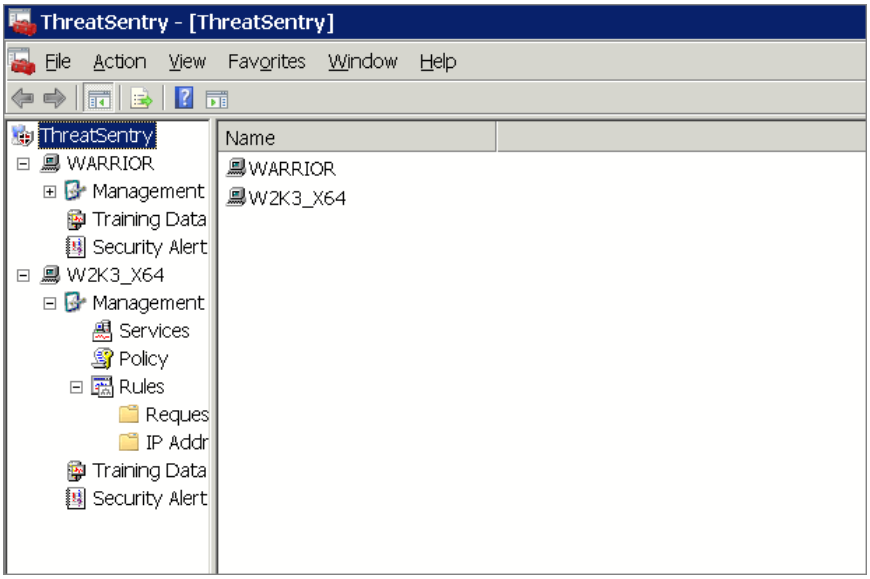
Select "New->Computer... " from root of ThreatSentry AdminConsole



A "New Computer" dialog will appear. Use the "Browse" button to view the available servers or enter the server Name manually. If current user doesn't have permissions to access other domain/workgroup servers, use the "Options" button to enter other credentials



If the target server is not accessible or ThreatSentry has not yet been installed, a "The computer is not accessible on your network!" error message will be displayed. If ThreatSentry is detected, the new server will be added to the master MMC tree.

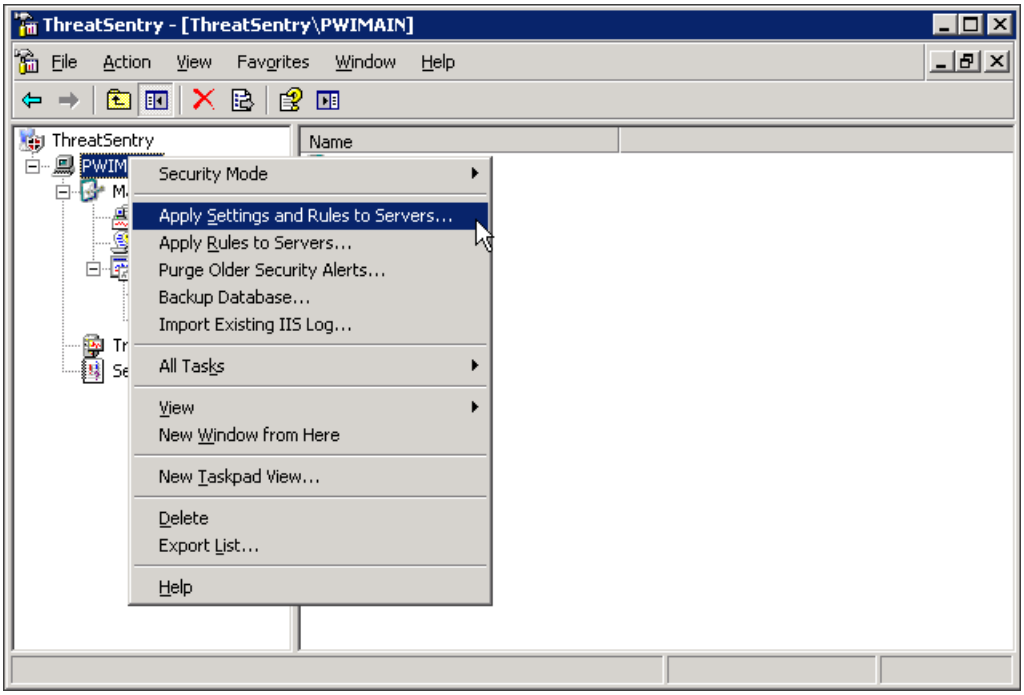


The remote Server W2K3_X64 can now be controlled exactly in same way as the local instance. Each server in the ThreatSentry

MMC tree has separate settings and data (Policy, Rules, Training Database and Security Alert Log, IP address lists, etc.).

Copying ThreatSentry rules configuration and settings to other servers

Select the Server for which settings should be copied and select either, **Apply Settings and Rules to Servers** (copies Settings, Policy, Rules and IP Address Lists from primary server to all other servers) or **Apply Rules to Servers** (copies only Rules and IP Addresses from primary server to all other servers).



Note: The Security Mode setting will be copied except if the target server is in Training mode.

XII. Contact & Support

Mailing Address

Privacyware.com
5195 Hampsted Village Center Way, #121
New Albany, OH 43054

614-656-1956 voice
614-408-8898 fax

Email Addresses

General Information:
info@privacyware.com

Sales:
sales@privacyware.com

Support:
support@privacyware.com

Partnership Information:
partners@privacyware.com

Privacyware is an innovative provider of award-winning web application firewall, pc security and security data analytics software. Privacyware products leverage conventional and advanced 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 member of the Microsoft Partner Network with Silver OEM and Independent Software Vendor (ISV) competencies.

CONTACT: Sales, Privacyware: sales@privacyware.com

www.privacyware.com

ThreatSentry
User Guide

Document Version

ThreatSentry, Edition 4.4 - (February, 2020), 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