Server Sensor Version 7.0 for Windows Advanced Tuning Parameters Reference Document

6303 Barfield Road • Atlanta, GA 30328-4233 Tel: 404.236.2600

Table of Contents

Overview

Introduction

This document introduces the advanced tuning parameters that are available for RealSecure server sensor version 7.0 and later for Windows platforms.

Purpose

This document explains the different types of advanced tuning parameters and describes how to configure them to suit your security needs.
Important: The default server sensor configuration should meet the security and performance needs of most users. If, however, your security or performance needs are not met, use the information in this document to reconfigure the settings.

Scope

This document describes advanced tuning parameters that are specific to the server sensor. General information about server sensor, such as managing policies, configuring responses, and configuring sensors, is described in the following guides:

- *RealSecure Server Sensor Policy Guide*
- *SiteProtector User Guide for Security Managers*

Definition: PAM

The protocol analysis module (PAM) combines advanced protocol anomaly detection with proven signature-based detection technology to interpret network activity and to detect attacks at all layers of the protocol stack.

Audience

This document is intended for advanced users of server sensor software. Before you change advanced tuning parameter settings, you must fully understand the effects of making such changes.

Introduction to Advanced Tuning Parameters

Introduction

The server sensor version 7.0 software supports advanced tuning parameters. Advanced tuning parameters allow you to configure (or tune) the server sensor to better meet your security needs or to enhance the performance of your hardware.

Name/value pairs

Tuning parameters are composed of name/value pairs.

Using tuning parameters

You can use tuning parameters to configure predefined name/value pairs.

Windows used for tuning parameters

You can configure tuning parameters using the following windows:

- Policy Editor window
- Sensor Properties window

Policy Editor window

When you configure tuning parameters in the Policy Editor window, the parameters apply to the policy file you have open. You must save any setting changes and then apply the policy to a server sensor for the changes to take effect.

Because you can apply the policy to as many server sensors as you want, you can use the Policy Editor window to make global configurations. You should, however, ensure that the changes you have made are appropriate for all of the sensors you apply the policy to.

Sensor Properties window

When you configure tuning parameters in the Sensor Properties window, the parameters apply only to that server sensor. Using this window allows you to configure tuning parameters that are sensible only for a certain server.

Tuning a parameter in both windows

You can specify one value for a tuning parameter in the Policy Editor window and another value for the same parameter in the Sensor Properties window. If you do this, the value specified in the Sensor Properties window overrides the value specified in the Policy Editor window. This is beneficial if you want a small number of server sensors to behave differently from the majority of your server sensors.

Accessing the Sensor Properties Window

Introduction

Some of the procedures in this document are performed in the Sensor Properties window. This topic describes how to access the Sensor Properties.

Procedure

To access the Sensor Properties window:

1. In the **Agent** view for the group that contains the sensor you want to configure, right-click the sensor.
2. Select **Properties**.
3. Select **Agent Properties**.
4. Click **Edit agent properties**.
   The Server Sensor Properties window opens.

Predefined Name/Value Pairs

Introduction

This topic describes the name/value pairs that are predefined for server sensor for Windows platforms.

Definition: predefined

A name/value pair is predefined when the server sensor has a default setting (or value) for the name/value pair.

Default settings

The server sensor uses the default settings for predefined name/value pairs until you change those settings. Only commonly used predefined name/value pairs appear in the Sensor Properties window or on the Sensor Tuning window. Less commonly used predefined name/value pairs will not appear in the Sensor Properties window unless you change the default settings.

Important information about X-Press Updates (XPUs)

Adjusting the settings for name/value pairs fine-tunes the performance of the sensor. Therefore, name/value pairs relate directly to the behavior of the sensor. Improvements to the sensor can invalidate some pairs and change the interpretation of others. While ISS makes reasonable efforts to keep the behavior of name/value pairs consistent from one XPU to the next, no guarantee is provided. If you use name/value pairs, pay close attention to documentation changes from one XPU to the next.

Guidelines

Follow these guidelines when you configure predefined name/value pairs:

- You can add a port on which the sensor listens for an event using the `pam.tcpport.<service_name>` parameter, where <service_name> is the service that you are assigning to the port number.
  Example: The parameter `pam.tcpport.TELNET` with a value of 23 causes Telnet signatures to parse traffic on port 23.
- You cannot assign multiple ports in one `pam.tcpport.<service_name>` parameter. You must use a separate `pam.tcpport.<service_name>` parameter for each port you want to add, and then distinguish each instance with an identifier enclosed in brackets.
  Example: To cause Telnet signatures to parse traffic on port 23 and on port 24, define two parameters as follows:
  ```
  pam.tcpport.TELNET[1] =23
  pam.tcpport.TELNET[2] =24
  ```
- You can assign the same service to more than one port, but you cannot assign the same port to more than one service.
- You cannot adjust the number of ports or the time period for port scan signatures. These signatures no longer check for a certain number of ports in a specified period of time.

List of name/value pairs

The following table describes the name/value pairs and includes the default value for each pair.

Name	Description	Type/ Values	Default Value
advancedeventconsolidation .enabled	Defines whether Advanced Consolidation of Events (ACE) is enabled. **Note:** This parameter was introduced in Service Release 4.2.	boolean/ true, false	true
advancedeventconsolidation .housekeepinginterval	Specifies how frequently the sensor calls PAM to clean up resources. **Note:** This parameter was introduced in Service Release 4.2.	number/ seconds between calls	1
advancedeventconsolidation .combine	Specifies whether ACE should merge similar events	boolean/ true, false	true
advancedeventconsolidation .listsize	Specifies the maximum number of events to keep in the ACE queue	number/ number of events	50
advancedeventconsolidation .deltatime	Specifies the maximum number of seconds that the ACE module delays reporting an event while looking for related events	number/ time in seconds	60
advancedeventconsolidation .spoofthreshold	Specifies the number of related events from different intruders against one victim that ACE must witness at the same time before determining that the intruder address is spoofed	number/ number of events	8
advancedeventconsolidation .spoofshow	Specifies the number of spoofed intruder events to report individually (not combined)	number/ number of events	3
advancedeventconsolidation .retrythreshold	Specifies the number of related events from the same intruder using different source ports against one victim (retry events) that ACE must witness at the same time before combining them	number/ number of events	4
advancedeventconsolidation .retryshow	Specifies the number of retry events to report individually (not combined)	number/ number of events	2

Name	Description	Type/ Values	Default Value
AllowAllAcknowledgement Packets	Allows packets across connections initiated from the sensor for port 1024 or above **Note:** This parameter was introduced in Service Release 4.2.	boolean/ true, false	false
BlockEnabled	Defines sensor-level blocking behavior. A setting of **true** enables sensor-level blocking. A setting of **false** disables sensor-level blocking. **Reference:** For more information about blocking, see the Help.	boolean/ true, false	false
evidence.logging	Defines evidence logging behavior. A setting of **true** enables evidence logging. A setting of **false** disables evidence logging. **Reference:** For more information about evidence logging, see the management console Help.	boolean/ true, false	true
packetLog.logging	Defines packet logging behavior. A setting of **true** enables packet logging. A setting of **false** disables packet logging. **Reference:** For more information about packet logging, see the management console Help.	boolean/ true, false	false
pam.ip.protocol. <layered_protocol> **Example:** pam.ip.protocol.17	Defines the protocol that is layered on top of the IP to be ignored for IP Unknown protocol. The layered protocol numbers of most interest are: • 1 – ICMP • 6 – TCP • 17 – UDP A setting of **true** indicates that the protocol is in use, so do not trigger IP Unknown. A setting of **false** indicates that the protocol should not be in use, so trigger IP Unknown.	boolean/ true, false	Protocols 0-100 are set to true, and do not trigger IP Unknown.

Name	Description	Type/ Values	Default Value
pam.report.filterall	Filters all events from the specified IP address or network. Filter additional events by adding an index number to the end of the parameter. For example, pam.report.filterall.0, pam.report.filterall.1, etc. **Example:** pam.report.filterall ip addr 123.255.255.255 **Note:** This parameter was introduced in Service Release 4.2.	string/ip addr <IP address or network address/ subnet mask>	N/A
pam.report.filter.<algorithm id>	Filters the specified event from the specified IP address or network. **Note:** Locate the algorithm id in the Event Details. **Example:** pam.report.filter.2000301 ip addr 123.255.255.255 **Note:** This parameter was introduced in Service Release 4.2.	string/ip addr <IP address or network address/ subnet mask>	N/A
pam.tcpport.FTP	Defines the port on which FTP is analyzed. Several ports can be specified by including a different tcpport configuration line for each port.	number/ port number	21
pam.tcpport.HTTP	Defines the port on which HTTP is analyzed.	number/ port number	80
pam.tcpport.parser.disable	Defines the parser to disable	string/name of the parser to disable	N/A
pam.tcpport.SMTP	Defines the port on which SMTP is analyzed.	number/ port number	25
TclMinWorkers	Defines the minimum number of Tcl workers available to assist with Tcl processing.	number/ number of workers	2
TclMaxWorkers	Defines the maximum number of Tcl workers available to assist with Tcl processing.	number/ number of workers	16

Name	Description	Type/ Values	Default Value
TclCmdQSize	Defines the limit on the number of requests held in the queue.	number/ number of requests	512
TclCmdQThreshold	Defines the length the request queue can reach before additional Tcl workers should be added to assist with Tcl processing.	number/ number of requests	5
TclCmdWaitTimeout	Defines how long a command can wait before additional Tcl workers are added to assist with Tcl processing.	number/ number of seconds	2
vpatch.BaseConfig. <operation>	Defines the action the sensor should take when it detects a buffer overflow exploit in a protected directory. Operation is any unique descriptor for the operation. **Example:** vpatch.BaseConfig.FileOperation **Example:** vpatch.BaseConfig.ProcOperation **Note:** This parameter was introduced in Service Release 4.2.	string/file or process creation action	N/A
vpatch.Exclude.<file>	Allows you to define a unique action for a program file where file is a unique word for the program file you want to change the action for. **Example:** vpatch.Exclude.MyApplication **Example:** vpatch.Exclude.SuspiciousApplication **Note:** This parameter was introduced in Service Release 4.2.	string/path to program file and actions the sensor should take for process creation and file creation operations	N/A

Name	Description	Type/ Values	Default Value
vpatch.Include.<name_of_ directory>	Defines a directory to monitor for buffer overflow exploits where name_of_directory is any unique word that identifies the directory the sensor will monitor. **Example:** vpatch.Include.MyDirectory **Note:** This parameter was introduced in Service Release 4.2.	string/path to or name of the directory to monitor	N/A
pcd.packetfilters	Specifies whether packets from a specific IP address should be excluded from analysis. **Note:** This parameter was introduced in Service Release 4.4. See the *RealSecure Server Sensor Policy Guide* for detailed configuration information.	string/ ip address/ CIDR prefix length/ protocol/ direction	N/A

Configuring Predefined Name/Value Pairs for a Sensor

Introduction

Configure predefined name/value pairs for a sensor on the Advanced tab of the Sensor Properties window. The changes you make apply only to the selected sensor.

Prerequisite

Before you configure a Name/Value pair, refer to the guidelines on page 8 in this document.

Procedure

To configure a tuning parameter:

1. In the Sensor Properties window, select the **Advanced Parameters** tab.
2. Do you want to edit a tuning parameter that is already in the list of parameters?
   - If *yes*, select the **Name/Value** pair to edit, and then click **Edit**.
   - If *no*, click **Add**.

   The Advanced Value window appears.
3. Continue according to the following table:

Option	Description
Name	Type the name of the tuning parameter you are configuring.
Type	Select the type of value for the tuning parameter. Valid types are as follows: • boolean • number • string
Value	Select or type a value for the tuning parameter as follows: • for boolean, select true or false • for number, select a number from the list • for string, type the text
Description	Type a description that indicates the purpose of this tuning parameter.

4. Click **OK**.
5. Click **OK**.

Configuring Predefined Name/Value Pairs for a Policy File

Introduction

You can configure tuning parameters for a policy file in the Policy Editor window. In the Policy Editor window, you select a group of signatures and configure tuning parameters for the entire group. You can apply the changes you make in a policy file to multiple sensors.

Prerequisite

Before you configure a Name/Value pair, refer to the guidelines on page 8 in this document.

Procedure

To configure a tuning parameter:

1. In the Policy Editor window, select any group of signatures.
2. Click **Tuning**.
   The Sensor Tuning window appears.
3. Do you want to edit a tuning parameter that is already in the list of parameters?
   - If yes, select the **Name/Value** pair to edit, and then click **Edit**.
   - If no, click **Add**.

   The Advanced Tuning Value window appears.
4. Continue according to the follow table:

Option	Description
Name	Type the name of the tuning parameter you are configuring.
Type	Select the type of value for the tuning parameter. Valid types are as follows: • boolean • number • string
Value	Select or type a value for the tuning parameter as follows: • for boolean, select true or false • for number, select a number from the list • for string, type the text
Description	Type a description that indicates the purpose of this tuning parameter.

5. Click **OK**.
6. Click **OK**.
7. In the Policy Editor window, click **Save**.
8. Apply the policy to each sensor you want to use this tuning parameter.