

Advanced Tuning Parameters Reference Document

Overview

Introduction

This document introduces you to the advanced tuning parameters that are available for RealSecure network sensor version 7.0 and gigabit network sensor.

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 network 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 network sensor. General information about RealSecure sensors, such as managing policies, configuring responses, and configuring sensors, is described in the following guides:

- *RealSecure Workgroup Manager User Guide*
- *RealSecure SiteProtector Strategy Guide*
- *RealSecure Network Sensor and Gigabit Network Sensor Policy Guide*.

Code version documented

This document describes the protocol analysis module (PAM) version 1.6.102.138, which was included in the network sensor version 7.0 and gigabit network sensor for Windows release.

Definition: PAM

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

Audience

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

In this document

This document includes the following topics:

Topic	Page
Introduction to Advanced Tuning Parameters	3
Accessing the Sensor Properties Window	4
Pre-defined Name/Value Pairs	5
Configuring Pre-defined Name/Value Pairs for a Sensor	8

Topic	Page
Configuring Pre-defined Name/Value Pairs for a Policy File	9
Managing PAM Memory Usage on Network Sensor	10
Modifying User-defined Issues with Tuning Parameters	13
Name/Value Pairs for User-defined Issues	14
Configuring User-defined Issues for a Sensor	15
Configuring User-defined Issues for a Policy File	16
Assigning an Issue ID Number	17
Enabling or Disabling an Issue	18
Naming an Issue	19
Setting the Priority for an Issue	20
Assigning Responses to an Issue	21

Introduction to Advanced Tuning Parameters

Introduction

The network sensor version 7.0 software includes an advanced tuning parameter feature. This feature allows you to configure (or tune) certain parameters of the network sensor to better meet your security needs or 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 the following:

- pre-defined name/value pairs
- PAM memory usage
- RSKill response routing
- user-defined issues

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. The system saves these settings in the policy file, and you must apply the policy to the network sensors for the changes to take effect.

Because you can apply the policy to as many network sensors as you want, you can use the Policy Editor window to make global changes. However, the changes made must be appropriate for all of the network sensors to which you apply the policy.

Sensor Properties window

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

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. In this case, 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 network sensors to behave differently from the majority of your network 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 window from the Workgroup Manager and from SiteProtector.

Procedure for Workgroup Manager

To access the Sensor Properties window:

1. Select a network sensor in the Managed Assets window.
2. From the Sensor menu, select **Properties**.
The Sensor Properties window opens.

Procedure for SiteProtector

To access the Sensor Properties window:

1. Select the **Sensor** tab, and then right-click the sensor.
2. Select **Server Sensor**.
3. From the pop-up menu, select **Edit Properties**.
The Sensor Properties window opens.

Pre-defined Name/Value Pairs

Introduction

This topic describes the name/value pairs that are pre-defined for the network sensor.

Definition: pre-defined

A name/value pair is pre-defined because the network sensor has a default setting (or value) for the name/value pair.

Default settings

The network sensor uses the default settings for pre-defined name/value pairs until you change them. The pre-defined name/value pairs do not appear on the Sensor Properties window or the Sensor Tuning window unless you change the default settings.

Note: The default settings satisfy most customer security needs.

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 inner 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 configuring pre-defined 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 using one `pam.tcpport.<service_name>` parameter with multiple port numbers. Use a `pam.tcpport.<service_name>` parameter for each port you want to add.
- 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 look for a certain number of ports in a certain time period.

List of name/value pairs

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

Name	Description	Field Type/ Values	Default Value
pam.http.heuristic	Controls a heuristic method used to determine whether HTTP traffic is transmitted or received on a port other than port 80.	boolean/ true, false	true
pam.login.any	Enables the sensor to detect a specific login attempt using the specified protocol. The login.any parameter detects specified logins on any supported protocol.	string/ username:password Examples: <ul style="list-style-type: none"> • jdoe:doey1 • all private • netopia:netopia Note: The colon and password are optional.	N/A
pam.login.maxpass	Defines the maximum length a password can be without generating an issue. Issues are generated as follows: <ul style="list-style-type: none"> • FTP - 2001307 • POP3 - 2000702 • RLOGIN - 2002103 • Telnet - 2000903 	number/ number of characters	100
pam.login.vnc.count	Defines the number of Virtual Network Computing (VNC) login failures that must occur within the set interval for an event to be detected. Note: The interval is defined within the pam.login.vnc.interval parameter.	number/ number of login failures	4

Name	Description	Field Type/ Values	Default Value
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.POP3	Defines the port on which POP version 3 is analyzed.	number/ port number	110
pam.tcpport.SMTP	Defines the port on which SMTP is analyzed.	number/ port number	25

Configuring Pre-defined Name/Value Pairs for a Sensor

Introduction

You can configure pre-defined 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.

Procedure

To configure tuning parameters:

1. In the Sensor Properties window, select the **Advanced** 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 follow table:

Field	Description
Name	Type the name of the tuning parameter you want to configure.
Type	Select the type of value to configure for the tuning parameter. The valid types are as follows: <ul style="list-style-type: none">• boolean• number• string
Value	Select or type a value for the tuning parameter depending on the type you selected: <ul style="list-style-type: none">• 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.

Reference: Refer to Pre-defined Name/Value Pairs on page 5 for more information.

4. Click **OK**.
5. Repeat Steps 2 through 4 for each parameter name you are configuring.
6. Click **OK**.

Configuring Pre-defined 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.

Procedure

To configure tuning parameters:

1. In the Policy Editor window, select the group of signatures for which you want to configure tuning parameters.
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:

Field	Description
Name	Type the name of the tuning parameter you want to configure.
Type	Select the type of value to configure for the tuning parameter. The valid types are as follows: <ul style="list-style-type: none">• boolean• number• string
Value	Select or type a value for the tuning parameter depending on the Type you selected: <ul style="list-style-type: none">• 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.

Reference: Refer to Pre-defined Name/Value Pairs on page 5 for more information.

5. Click **OK**.
6. Repeat Steps 2 through 4 for each parameter name you are configuring.
7. Click **OK**.
8. In the Policy Editor window, click **Save**.

Managing PAM Memory Usage on Network Sensor

Introduction

Protocol Analysis Module (PAM) can use a significant amount of memory because it tracks TCP connections. The network sensor includes a pre-defined setting for maximum memory usage. This topic describes this tuning parameter and how to change its default setting.

How the parameter works

The sensor.pammaxmemoryusagefactor parameter has a default setting of 75. This default setting causes the sensor to allocate a maximum of 75% of installed physical memory to PAM on startup. If the sensor runs out of memory, the PAM DLL is unloaded, memory resources are freed, and PAM is restarted with a fresh allocation of memory. Using this process, the sensor recovers without crashing.

Changing the setting

You can change the sensor.pammaxmemoryusagefactor parameter default setting if you experience memory-related issues due to high traffic volume. Change this parameter on the Advanced tab of the Sensor Properties window.

Important: Although the valid range is 25-900% of available physical memory, a setting above 90% causes PAM to use swap space (virtual memory). Using swap space significantly reduces sensor performance. Additionally, for settings over 100%, configure sufficient swap space for the computer on which the network sensor is installed.

Procedure

To change the PAM memory usage parameter:

1. In the Sensor Properties window, select the **Advanced** tab.
2. Select the sensor.pammaxmemoryusagefactor parameter, and then click **Edit**.
The Advanced Value window appears.
3. Select or type a number in **Value**.
4. Click **OK**.
5. Click **OK**.

Configuring Routing for the RSKill Response

Introduction

Previous versions of network sensor sent the RSKill response on the monitoring interface. Network sensor 7.0, however, includes a high-performance driver that allows you to select a separate kill interface. Since the high-performance driver is read only, the sensor must send kills on another interface.

Typical scenario

A typical scenario that requires split adapter kills is as follows:

Adapter	Configuration
1	Management adapter with IP stack on network segment 1
2	Stealth adapter on network segment 2 / Adapter to Send Kills
3	Stealth adapter using high-performance driver on network segment 2 / Adapter of Monitored Network

Routing Kills

When kills are issued, they use the MAC addresses that were encoded in the packet(s) that triggered the RSKill response. Therefore, if you want to specify a kill adapter **that is not on the same segment** as the monitoring interface, the kills will not work properly. There is a simple work around, however, that will allow this setup to work correctly. Let's assume the following setup:

- Adapter 1 = kill adapter on the 10.10.10.x segment
 - Adapter 2 = high performance driver monitoring the 172.16.10.x segment
- In this situation, the kills will need to reset connections on the 172.16.10.x network, but must do so from the 10.10.10.x network. In order to make this happen, we must determine what the MAC address is for the 10.10.10.x segment's router.

Determining the MAC address

To determine the MAC address:

Note: You can also ask your system administrator for the MAC address for the router.

1. On the sensor machine, go to the command line and ping a host on the monitoring network.

Example: ping 172.16.10.1

2. Type arp -a.

A list of IP to MAC address translations appears.

Example:

```
Interface: 10.10.10.20 on Interface 0x1000003
```

```
Internet Address      Physical Address      Type
10.10.10.1           00-02-73-2e-6f-51    dynamic
```

Note: Routers are usually given the .1 address, so we now have what we need.

Configuring RSKill Routing

Configure RSKill routing for the sensor at the Workgroup Manager or SiteProtector console. To configure routing for the RSKill response:

1. In the Sensor Properties window, select the **Advanced** tab, and then click **Add**.
The Advanced Value window appears.
2. Continue according to the follow table:

Field	Description
Name	Type <code>sensor.tcpkillmacdstaddr</code>
Type	Select String.
Value	Type the physical address that you determined from the <code>arp -a</code> command in the previous procedure. Note: Type the address exactly as it appeared. The address from the previous example is: <code>00-02-73-2e-6f-51</code>
Description	Type a description that indicates the purpose of this tuning parameter.

3. Click **OK**.
4. Click **OK**.
The sensor status changes to Updating.
5. After the update is complete, stop and restart the sensor.

Modifying User-defined Issues with Tuning Parameters

Introduction

You can use tuning parameters to change the default settings for user-defined issues. The following paragraphs describe how to modify a user-defined issue with tuning parameters.

What you can modify

You can configure tuning parameters to modify a user-defined issue as follows:

- Assign an issue ID number.
- Enable or disable the issue.
- Name the issue.
- Set the priority for the issue.
- Assign responses to the issue.

Tuning parameters for user-defined issues

Use the following tuning parameters to modify user-defined issues:

- issue.<issue_ID>.enabled
- issue.<issue_ID>.name
- issue.<issue_ID>.priority
- issue.<issue_ID>.response

Default settings

The following table describes the default settings for user-defined issues.

Parameter	Default Setting
Enabled	True
Name	UserIssue_<issue_ID>, where <issue_ID> is the 7-digit issue ID number
Priority	2
Response	DISPLAY:default,LOGDB:logwithoutraw

Rule

You cannot globally change the default settings for user-defined issues. You must change the default settings separately for each issue, using the syntax and instructions provided in the following procedures.

Name/Value Pairs for User-defined Issues

Introduction

You can configure (or tune) certain parameters for the RealSecure network sensor that correspond to BlackICE user-defined issue IDs. These parameters describe patterns for which the sensor scans, along with a user-specified issue ID that identifies the attack or vulnerability.

Issue ID range recommendation

Internet Security Systems (ISS) recommends that you use an issue ID range of 2010000-2020000. These ranges correspond to the issue IDs that are reserved for BlackICE functionality.

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 inner 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.

List of name/value pairs

The following table describes name/value pairs that allow you to create user-defined issues.

Note: The <issue_id> variable in the name specifies the signature number assigned to the intrusion.

Name	Description	Values
pam.ftp.filename. <user_issue_id> Example: pam.ftp.filename.2013601	Defines the file specification for various FTP intrusions. Note: These specifications prevent intruders from accessing sensitive system files.	Filename Example: */passwd

Configuring User-defined Issues for a Sensor

Introduction

You can configure tuning parameters for a sensor on the Advanced tab of the Sensor Properties window. The changes you make apply only to the selected sensor.

Procedure

To configure tuning parameters for a sensor:

1. In the Sensor Properties window, select the **Advanced** tab.
2. Click **Add**, and then follow the procedure to accomplish the appropriate task:
 - Assigning an Issue ID Number, page 17
 - Enabling or Disabling an Issue, page 18
 - Naming an Issue, page 19
 - Setting the Priority for an Issue, page 20
 - Assigning Responses to an Issue, page 21

Configuring User-defined Issues for a Policy File

Introduction

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

Procedure

To configure tuning parameters for a policy file:

1. In the Policy Editor window, select a group of signatures.
2. Click **Tuning**.
The Sensor Tuning window appears.
3. Click **Add**, and then follow the procedure to accomplish the appropriate task:
 - Assigning an Issue ID Number, page 17
 - Enabling or Disabling an Issue, page 18
 - Naming an Issue, page 19
 - Setting the Priority for an Issue, page 20
 - Assigning Responses to an Issue, page 21

Assigning an Issue ID Number

Introduction

You can assign an issue ID number in the range of 2010000-2020000 to a user-defined event.

Procedure

To assign an issue ID number:

1. In the Name field, type the syntax from the table of name/value pairs in the preceding pages.
Example: `pam.ftp.filename.2010000`
2. In the Type field, select **String**.
3. In the Value field, type the appropriate value as described in the table of name/value pairs in the preceding pages.
4. **Example:** `myscript.vbs`
5. In the Description field, type a description that indicates the purpose of this tuning parameter.
6. Click **OK**.

The name/value pair is added to the list of tuning parameters in the Sensor Properties window or the Sensor Tuning window.

Enabling or Disabling an Issue

Introduction

After you assign an issue ID number to a user-defined issue, you must enable it using the `issue.<issue_ID>.enabled` parameter. You can also use this parameter to disable the user-defined issue without deleting it.

Procedure

To enable or disable an issue:

1. In the Name field, type `issue.<issue_ID>.enabled`.

Example: `issue.2010000.enabled`

2. In the Type field, select **Boolean**.
3. In the Value field, select **True** to enable or **False** to disable.
4. In the Description field, type a description that indicates the purpose of this tuning parameter.
5. Click **OK**.

The name/value pair is added to the list of tuning parameters in the Sensor Properties window or the Sensor Tuning window.

Naming an Issue

Introduction

You can assign a name to a user-defined issue using the issue.<issue_ID>.name parameter. The name you assign becomes part of the event data for events that are detected by this issue.

Procedure

To name an issue:

1. In the Name field, type issue.<issue_ID>.name.
Example: issue.2010000.name
2. In the Type field, select **String**.
3. In the Value field, type a name.
4. In the Description field, type a description that indicates the purpose of this tuning parameter.
5. Click **OK**.
The name/value pair is added to the list of tuning parameters in the Sensor Properties window or the Sensor Tuning window.

Setting the Priority for an Issue

Introduction

You can change the priority of a user-defined issue using the issue.<issue_ID>.priority parameter. The priority you assign to the issue determines whether the event appears as high, medium, or low on the Workgroup Manager or SiteProtector console.

Procedure

To set the priority for an issue:

1. In the Name field, type issue.<issue_ID>.priority.

Example: issue.2010000.priority

2. In the Type field, select **Number**.
3. In the Value field, select a priority as follows:
 - **1** for high
 - **2** for medium
 - **3** for low
4. In the Description field, type a description that indicates the purpose of this tuning parameter.
5. Click **OK**.

The name/value pair is added to the list of tuning parameters in the Sensor Properties window or the Sensor Tuning window.

Assigning Responses to an Issue

Introduction

You can assign responses to a user-defined issue using the `issue.<issue_ID>.response` parameter.

Procedure

To assign responses to an issue:

1. In the Name field, type `issue.<issue_ID>.response`.
2. In the Type field, select **String**.
3. In the Value field, type the responses you want in this format `<response_type>:<response_name>`, separated by commas.

Example: `DISPLAY:Default,LOGDB:LogWithoutRaw`

The response types are as follows:

- `DISPLAY:Default`
- `LOGDB:LogWithoutRaw`
- `LOGDB:LogWithRaw`
- `LOGDB:LogFiltered`
- `LOGEVIDENCE:Default`
- `EMAIL:Default`
- `SNMP:Default`
- `OPSEC:LockSrcAddr`
- `OPSEC:LockDestAddr`
- `OPSEC:LockSrcOrDestAddr`
- `OPSEC:LockService`
- `RSKILL:Default`
- `USER SPECIFIED`
- `VIEWSESSION:Default`

Note: Refer to the Help for additional information about these responses.

4. In the Description field, type a description that indicates the purpose of this tuning parameter.
5. Click **OK**.

The name/value pair is added to the list of tuning parameters in the Sensor Properties window or the Sensor Tuning window.