

MONITOR MULTIPLE EVENTS ON A REMOTE SYSTEM USING THE SNMP TRAP MONITOR AND THE EVNTWIN.EXE WINDOWS UTILITY

When configuring ipMonitor to monitor event log files on a remote server, there may be instances when the Event Log Monitor cannot be used. For example, if:

- It is not possible to use a Credential to represent the administrative account.
- RPC connectivity is not working properly.
- RPC connectivity is not allowed.

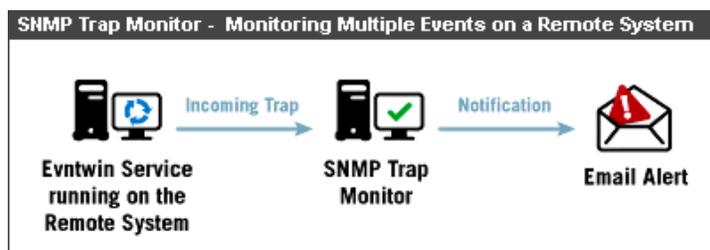
On such occasions, you can use the Evtwin.exe Windows utility and the SNMP Trap Monitor to monitor for specific events in Event Log files. There are a number of advantages to this setup:

- The SNMP Trap Monitor is easy to configure.
- This setup will work on a stand-alone system, as well as across non-trusted domains provided that SNMP connectivity exists between both systems.
- This setup results in a non-intrusive, low network overhead monitoring process.

How the Process Works

The SNMP Trap Monitor listens for incoming traps sent from remote systems and network devices. When a trap is received, it is analyzed to determine if an Information Alert should be sent. If the incoming trap matches the pre-configured trap filtering settings, an Information Alert is sent as configured in a related Notification Profile.

The following diagram illustrates this process:



The above diagram shows that the Evtwin.exe process detects the set condition in the Event Log and sends a trap to the ipMonitor installation. When the trap is received, an Information Alert is sent.

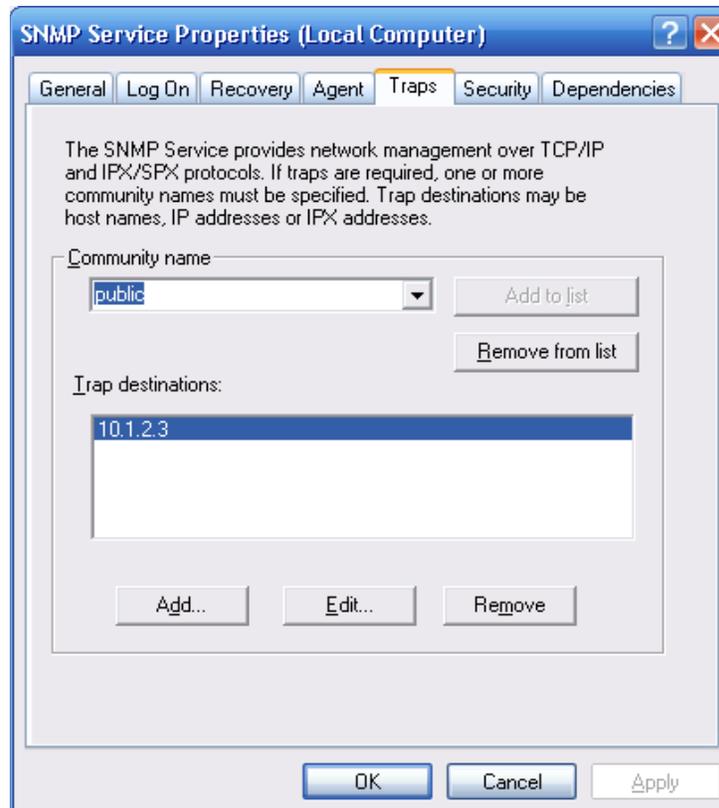
Before you begin

Before creating a SNMP Trap Monitor to implement the example outlined in this tutorial, ensure that the Windows SNMP Service has been configured and enabled on the remote system:

Step 1 - On the remote system:

- **If the SNMP Service has not been installed:**
 1. Click **Start / Control Panel / Add or Remove Programs / Add/Remove Windows Components**.
 2. In **Components**, click **Management and Monitoring Tools** and then click **Details**.
 3. Select the **Simple Network Management Protocol** check box, and then click **OK**.
 4. Click **Next**, and then **Finish**.

- **The SNMP Service on the remote system must be configured to send traps to the ipMonitor installation:**
 1. Click **Start / Control Panel / Administrative Tools**, and then double-click the **Services** MMC Snap-in.
 2. Right-click on the SNMP Service, and select **Properties**.
 3. Ensure that the **Startup Type** is set to **Automatic** under the **General** tab.
 4. Click the **Traps** tab and enter the **Community Name** to use. Add the **IP Address** of the ipMonitor installation in the **Trap destinations** field.
 5. Click **OK**.



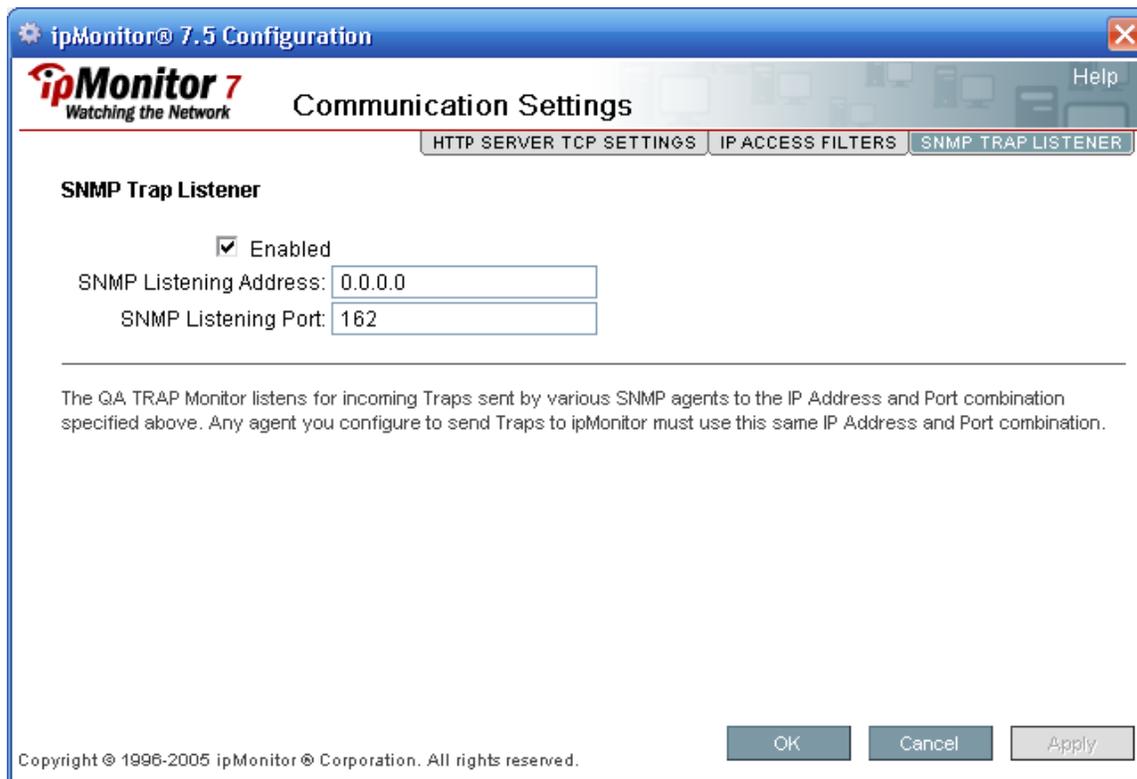
Step 2- On the ipMonitor 7 host:

- **The SNMP Trap Service must be disabled on the ipMonitor host machine (otherwise, it will interfere with the SNMP Trap Monitor):**

Note: If the SNMP component was not installed on the ipMonitor 7 host, the SNMP Trap Service will not be listed. In that case, please proceed to the next section.

1. Click **Start / Control Panel / Administrative Tools**, and then double-click the **Services** MMC Snap-in.
2. Select the **SNMP Trap Service**, and then click the **Action** drop-down menu and select **Properties**.
3. Stop the Service (if it is started) and set the **Startup Type** to **Disabled**.
4. Click **Apply**, and then click **OK**.
5. Close the **Services** window.

- **You must also ensure that the ipMonitor installation is configured to listen to incoming traps:**
 1. Access the ipMonitor 7 Configuration program from **Start / Program Files / ipMonitor 7 / Configure ipMonitor 7**.
 2. Select **Communications Settings**.
 3. Select the **IP Access Filters** tab and ensure the remote server IP address is not in the **Denied access** list.
 4. Select the **SNMP Trap Listener** tab and configure the settings as follows:
 - a. Check the **Enabled** checkbox.
 - b. Enter the **SNMP Listening Address**. Entering 0.0.0.0 will have the ipMonitor installation listen for incoming traps on all IP Addresses bound to the system.
 - c. Set the **SNMP Listening Port**. The default SNMP Listening Port number is 162.



[Top](#)

AVAILABLE RESOURCES



Click the XML icon to download resources designed to be used with this tutorial. The XML file includes a preconfigured SNMP Trap Monitor.

[Top](#)

CONFIGURING THE EVNTWIN.EXE WINDOWS UTILITY ON THE REMOTE SYSTEM

Beginning with Windows 2000, Windows Operating Systems now include the Eventwin.exe utility. This utility allows you to configure the remote system to forward specific event(s) to another system using an SNMP trap. Since Eventwin.exe is a graphical tool that connects to the Event viewer, it's easy to select which event(s) should be forwarded to the ipMonitor installation. More information on the Evtwin.exe utility can be found in the [Additional Information](#) section of this tutorial.

This tutorial illustrates how the Evtwin.exe utility can be used to help monitor specific security events on a remote system. Throughout this article, we will be referring to the following events:

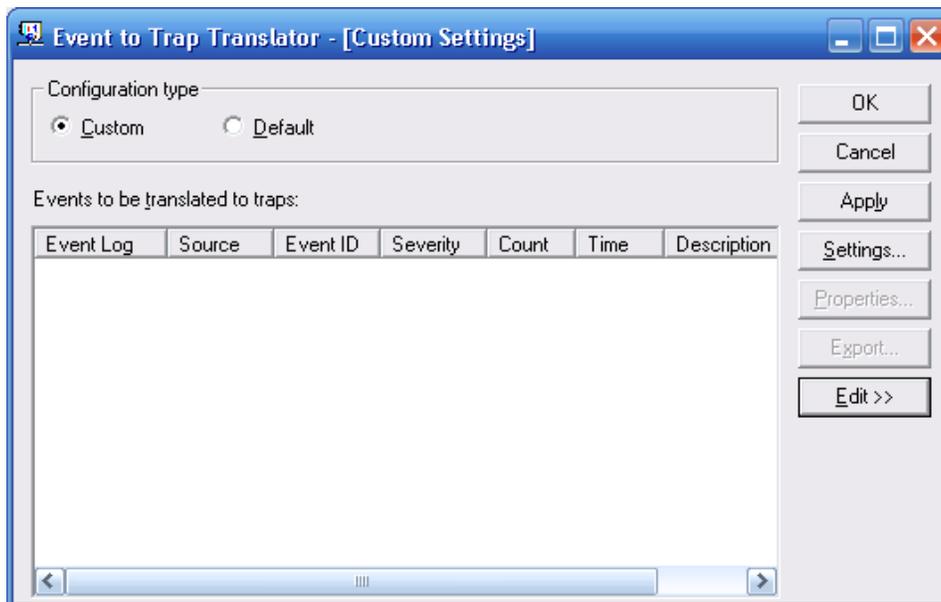
Event ID: 529 | Type: Failure | Audit Description: Logon Failure | Reason: Unknown user name or bad password

Event ID: 533 | Type: Failure | Audit Description: Logon Failure | Reason: User not allowed to logon at this computer

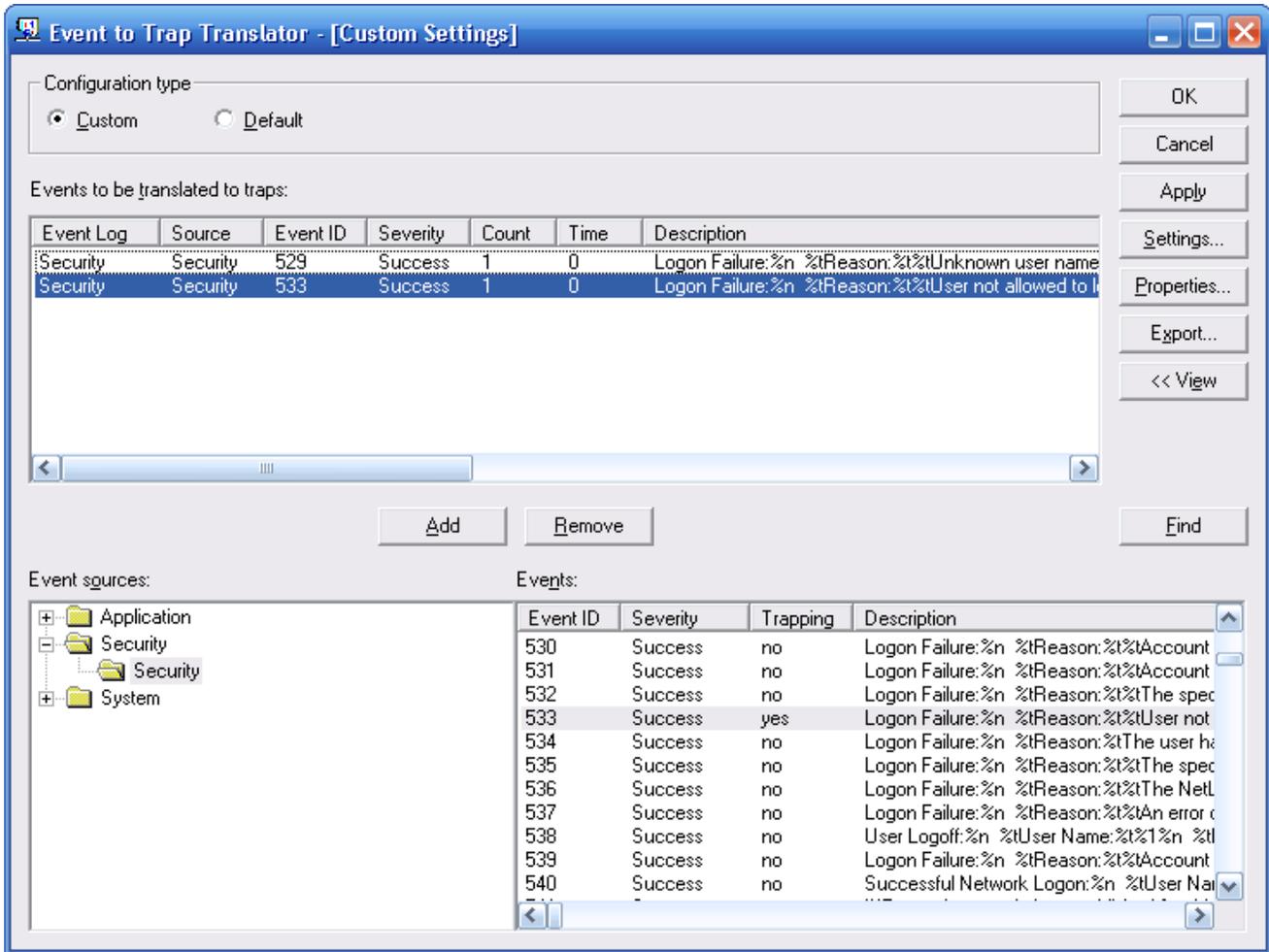
For a more comprehensive list of suggested Security Events to monitor, refer to the [Additional Information](#) section of this tutorial.

Note: The Evtwin.exe utility is only able to send traps for security events visible in the system's Security log. In order to log security events, the Audit policy must be activated on the system:

1. Start the evtwin.exe process:
 - a) Open the **Start Menu**.
 - b) Click **Run**.
 - c) Type in **evtwin.exe** and click **OK**.
2. In the **Configuration type** section, select the **Custom** radio button.



3. Click the **Edit** button and select the **Security** folder located in the bottom-left **Event sources** pane.
4. In the bottom-right **Events** pane, select the **Event ID** you would like to monitor.



5. Click the **Add** button.

6. You will likely want to modify the settings in the **Generate trap** section of the resulting **Event ID Properties** screen to better filter what type of scenario will trigger the utility to send a trap to the ipMonitor installation.

For example, with Event ID 529, it may not be desirable to send a trap when a password is mistyped. However, if the password is mistyped more than 5 times over the course of 3 minutes, this may indicate a potential intrusion attempt you would want to be notified about.

Properties

Source: Security

Enterprise OID: 1.3.6.1.4.1.311.1.13.1.8.83.101.99.117.114.105.116

Log: Security

Event: 529

Trap specific ID: 529

Generate trap

if event count reaches 5

within time interval 180 seconds

Description:

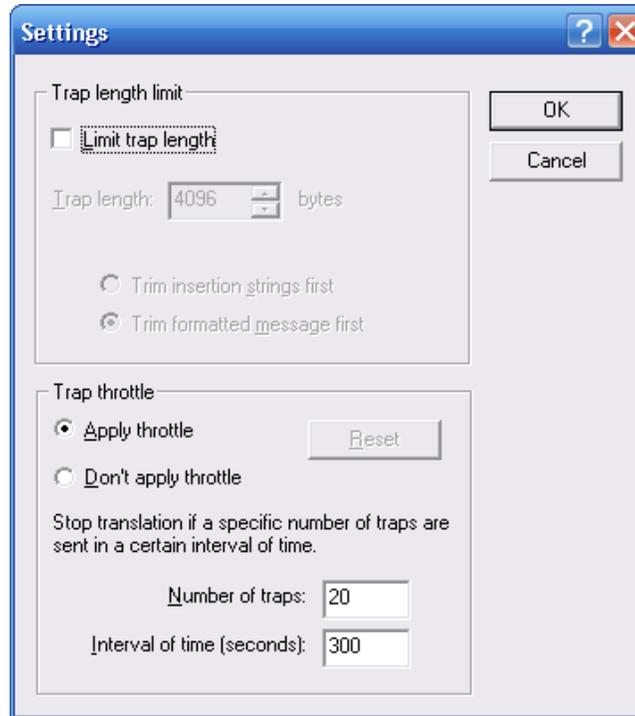
Logon Failure: %n %tReason: %t%tUnknown user name or bad password%n %tUser Name: %t%1%n %tDomain: %t%t%2%n %tLogon Type: %t%3%n %tLogon Process: %t%4%n %tAuthentication Package: %t%5%n %tWorkstation Name: %t%6

OK

Cancel

7. Once done, click the **OK** button.

Note: Clicking the **Settings** button from the **Custom Settings** window will allow you to view and configure general settings for the traps to be sent. For example, you may choose to control the maximum number of traps to be sent within a specific amount of time.



The resulting process will parse the Security Event Log file and will send a trap when the specified Event IDs are detected. Since evntwin.exe was previously configured, it will run by default when the server is rebooted without requiring you to be logged in.

[Top](#)

SAMPLE MONITOR SETTINGS

Monitor Name	SNMP Trap :: Event trap
Monitor Type	SNMP Trap
Community	public
Allowed IP Address Range (start)	10.0.0.0
Allowed IP Address Range (end)	10.255.255.255
Generic Type	Any
Enterprise OID	1.3.6.1.4.1.311.1.13.1.*

Note: The imported Monitor is initially disabled. This allows you to make changes to the default settings before the Monitor is enabled to go live in a production environment. Once the Monitor is imported, the following settings will need to be verified (and if necessary, modified) for the Monitor:

- Community
- Allowed IP Address Range (start)
- Allowed IP Address Range (end)

To learn more about modifying the above parameters, please refer to the [Configuring the SNMP Trap Monitor](#) section of this tutorial.

TIP

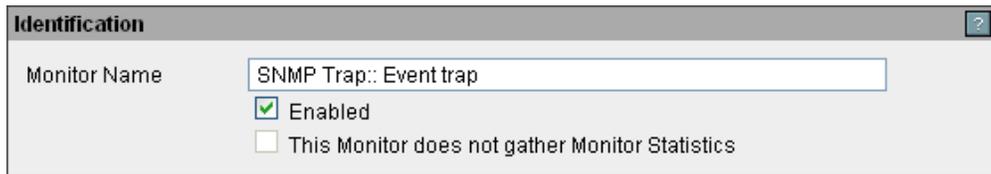
For detailed instructions regarding importing XML files into your ipMonitor installation, please refer to the tutorial entitled "[How to Import and Export Configuration Settings](#)".

[Top](#)

CONFIGURING THE SNMP TRAP MONITOR

For the purposes of this tutorial, we'll be referring to the preconfigured Monitor included in the XML resource download. Alternatively, you can create a new Monitor by clicking the **Monitors** menu option and then clicking **Add a Monitor**. Choose the **SNMP Trap** Monitor from the list provided.

Identification

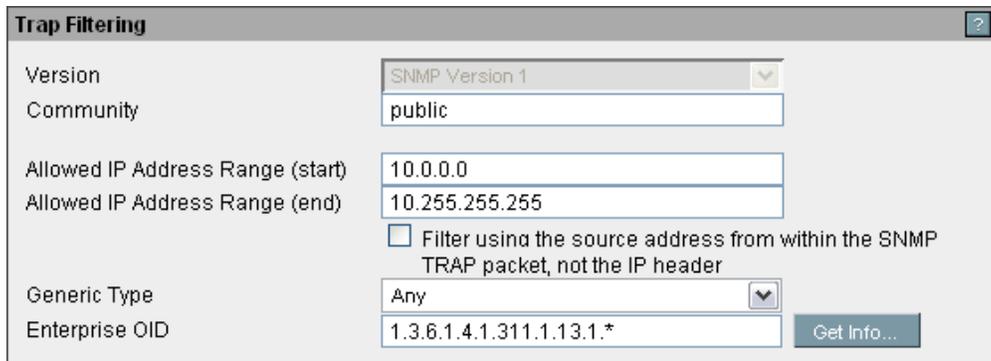


The screenshot shows the 'Identification' configuration window. It has a title bar with a question mark icon. The window contains the following fields and options:

- Monitor Name:** A text input field containing 'SNMP Trap:: Event trap'.
- Enabled:** A checked checkbox.
- This Monitor does not gather Monitor Statistics:** An unchecked checkbox.

1. Enter a unique, descriptive name for the Monitor in the **Name** field.
2. Check the **Enabled** checkbox.

Trap Filtering



The screenshot shows the 'Trap Filtering' configuration window. It has a title bar with a question mark icon. The window contains the following fields and options:

- Version:** A dropdown menu set to 'SNMP Version 1'.
- Community:** A text input field containing 'public'.
- Allowed IP Address Range (start):** A text input field containing '10.0.0.0'.
- Allowed IP Address Range (end):** A text input field containing '10.255.255.255'.
- Filter using the source address from within the SNMP TRAP packet, not the IP header:** An unchecked checkbox.
- Generic Type:** A dropdown menu set to 'Any'.
- Enterprise OID:** A text input field containing '1.3.6.1.4.1.311.1.13.1.*'.
- Get Info...:** A button.

3. Enter the SNMP **Community** string that allows Traps to communicate with ipMonitor.
4. Enter **the Allowed IP Address Range (start)**. This is the start of the range of IP Addresses used to determine which SNMP Traps will be accepted.
5. Specify the **Allowed IP Address Range (end)**. This is the end of the range of IP Addresses used to determine which SNMP Traps will be accepted.
6. Specify the **Generic Type**. The incoming generic-trap must be one of the predefined SNMPv1 Trap types:
 - **Any** indicates that any of the Trap types listed below will be accepted.
 - **coldStart(0)** signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

- **warmStart**(1) signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.
- **linkDown**(2) signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
- **linkUp**(3) signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.
- **authenticationFailure**(4) signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.
- **egpNeighborLoss**(5) signifies that an EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.
- **enterpriseSpecific**(6) signifies that the sending protocol entity recognizes that some enterprise-specific event has occurred. The specific-trap field identifies the particular trap which occurred.

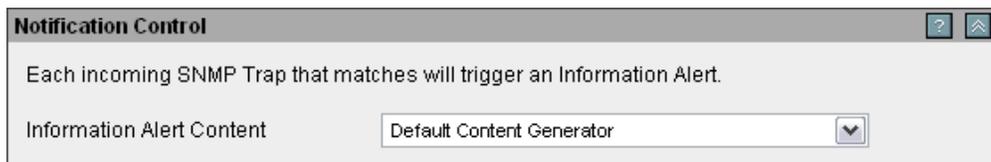
7. Enter the **Enterprise OID**.

Analysis of Test Results



Note: For this setup, it is not necessary to analyze and filter the incoming traps based on their bindings.

Notification Control



The SNMP Trap Monitor uses Information Alerts to notify you that a trap was received. The Information Alert can use the Default Content Generator, or you can create a Custom Content Generator to include the content of the received trap in the Information Alert being sent.

For more information regarding Information Alerts and Content Generators, refer to the **Information Alerts** section of ipMonitor's Context-Sensitive Help system. The Context-Sensitive Help can be accessed by clicking the **Help** link located in the top right corner of ipMonitor's Administration web interface.

[Top](#)

Evtwin.exe

For more information regarding the Evtwin.exe utility, refer to the following Microsoft technical article:

<http://www.microsoft.com/technet/prodtechnol/sms/sms2/proddocs/admhlp/sms2hl18.msp>

SNMP Trap Monitor

For more information regarding the SNMP Trap Monitor, refer to the **Monitors** section of ipMonitor's Context-Sensitive Help system, and then select **Monitor Types**, followed by **QA Trap**. The Context-Sensitive Help can be accessed by clicking the **Help** link located in the top right corner of ipMonitor's Administration web interface.

Event IDs to Monitor

To monitor additional events, refer to the list of suggested Event IDs below. Please note that this is not a comprehensive list of all available events that can be monitored.

- Event ID 529 : Unknown user name or bad password
- Event ID 530 : Logon time restriction violation
- Event ID 531 : Account disabled
- Event ID 532 : Account expired
- Event ID 533 : Workstation restriction - not allowed to logon at this computer
- Event ID 534 : Inadequate rights - as in user account attempting console login to server
- Event ID 535 : Password expired
- Event ID 536 : Net Logon service down
- Event ID 539 : Logon Failure: Account locked out
- Event ID 627 : NT AUTHORITY\ANONYMOUS is trying to change a password
- Event ID 644 : User account Locked out
- Event ID 675 : Pre-authentication failed