

# Log Source Virtualization

Log Source Virtualization makes it possible to consume all the available intelligence within individual log source files that contain multiple records from different sources. When virtualization is enabled on a log source, it is referred to as a “parent” log source, and the different records inside it are referred to as either “virtual” or “child” log sources (when referencing log sources, the terms “virtual” and “child” are often used interchangeably).

Child log sources are treated in the same way as other log sources. They are processed in accordance with their assigned MPE policies and they appear in the same lists as the other log sources within the deployment. In contrast to Syslog Virtualization, which applies only to syslog relay logs received by the System Monitor syslog server, Log Source Virtualization can be applied to syslog relay sources, Windows Event Logs, flat files, and any other log source within your deployment that contains multiple records.

To begin Log Source Virtualization, you need to apply properly configured Log Source Virtualization templates to the parent log sources at the System Monitor level. Virtualization templates include child source identifier regular expressions (also called “regexes”) to run against and parse data in the parent sources. When a parent log contains a record that matches an identifier regex, a child log is created. When a parent log contains a record that does not match any of the regexes, the record is assigned to a Catch-All child log source.

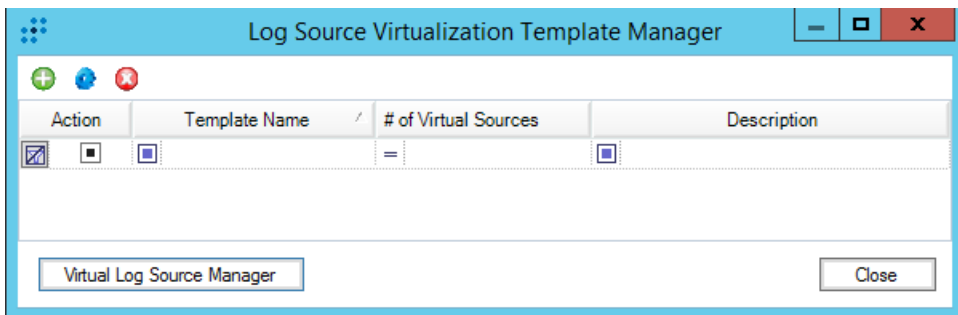
Virtual log sources cannot be edited to the same extent as their non-virtual counterparts because certain properties (including their lifecycle) remain tied to their parent sources. For example, if a parent log source is retired or has its virtualization disabled, its child log sources are also retired or disabled. You can, however, edit the name, regex, MPE policy, and log source type properties for virtual log sources.

You can add, modify, and delete both virtual log sources and virtualization templates from the Log Source Virtualization Template Manager. When you create or modify templates and virtual log sources, you can check their regex parsing and distribution accuracy by pasting sample logs into a testing tool that is provided. Keep in mind that changes made to virtual log source properties or virtualization templates affect only future log sources (existing log sources are unaffected).

## Opening the Log Source Virtualization Template Manager

1. Click the **Deployment Manager** tab.
2. Click **Tools**, click **Administration**, and then click **Log Source Virtualization Template Manager**.

The Log Source Virtualization Template Manager displays.



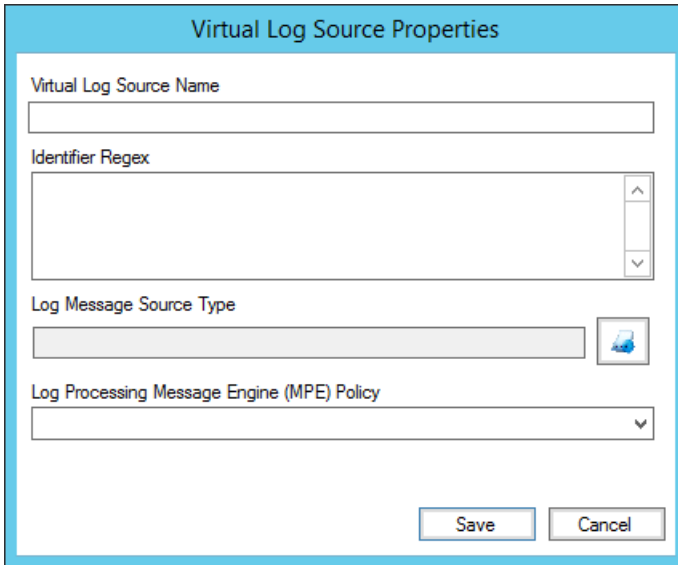
## Creating Virtual Log Sources

1. Open the Log Source Virtualization Template Manager, and then click the **Virtual Log Source Manager** button at the bottom of the dialog box.

The Virtual Log Source Manager displays.


2. On the upper-left side of the Virtual Log Source Manager dialog box, click the **New Template Item** icon.

The Virtual Log Source Properties dialog box displays.

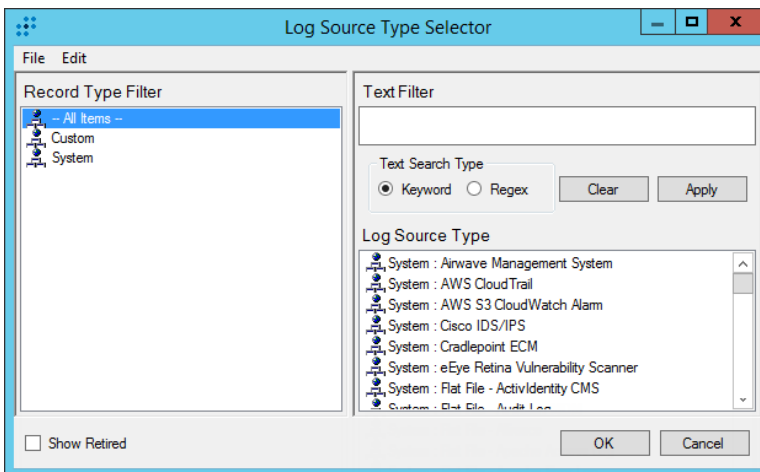


The screenshot shows the "Virtual Log Source Properties" dialog box. It contains the following fields and controls:

- Virtual Log Source Name:** A text input field.
- Identifier Regex:** A text input field with a vertical scrollbar on the right.
- Log Message Source Type:** A dropdown menu with a blue icon button to its right.
- Log Processing Message Engine (MPE) Policy:** A dropdown menu.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

3. In the **Virtual Log Source Name** field, enter a name.
4. In the **Identifier Regex** text box, enter an identifier regex for the virtual log source.
5. Click the **Log Message Source Type** icon .

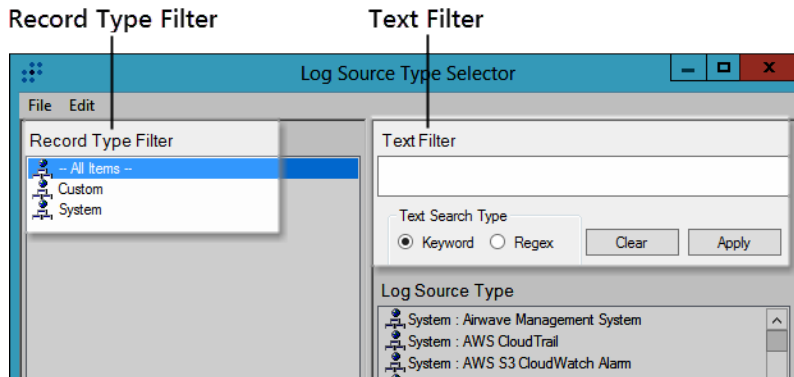
The Log Source Type Selector dialog box displays.



The screenshot shows the "Log Source Type Selector" dialog box. It features a menu bar with "File" and "Edit". The main area is divided into two panes:

- Record Type Filter:** A tree view showing "All Items --", "Custom", and "System".
- Text Filter:** A text input field, a "Text Search Type" section with radio buttons for "Keyword" (selected) and "Regex", and "Clear" and "Apply" buttons.
- Log Source Type:** A list box containing several system types, such as "System : Airwave Management System", "System : AWS CloudTrail", "System : AWS S3 CloudWatch Alarm", "System : Cisco IDS/IPS", "System : Cradlepoint ECM", "System : eEye Retina Vulnerability Scanner", "System : Flat File - ActivIdentity CMS", and "System : Flat File - Audit Log".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.
- Checkbox:** "Show Retired" checkbox at the bottom left.

6. In the Log Source Type Selector dialog box, do the following:
  - a. (Optional) To narrow the list of log source types, select a **Record Type Filter** and/or enter a **Text Filter**.



- b. (Optional) To include retired log source types in the list, select the **Show Retired** check box in the lower-left corner of the dialog box.
    - c. In the **Log Source Type** list box, select the appropriate log source type, and then click **OK**.
7. From the **Log Processing Message Engine (MPE) Policy** drop-down list, select an MPE policy.
8. Click **Save**.

The virtual log source is created and ready to use.