



Windows Event Log



- LightSpeed PM – A Certified Quest Partner

Quest™

Updated 08-25-2020

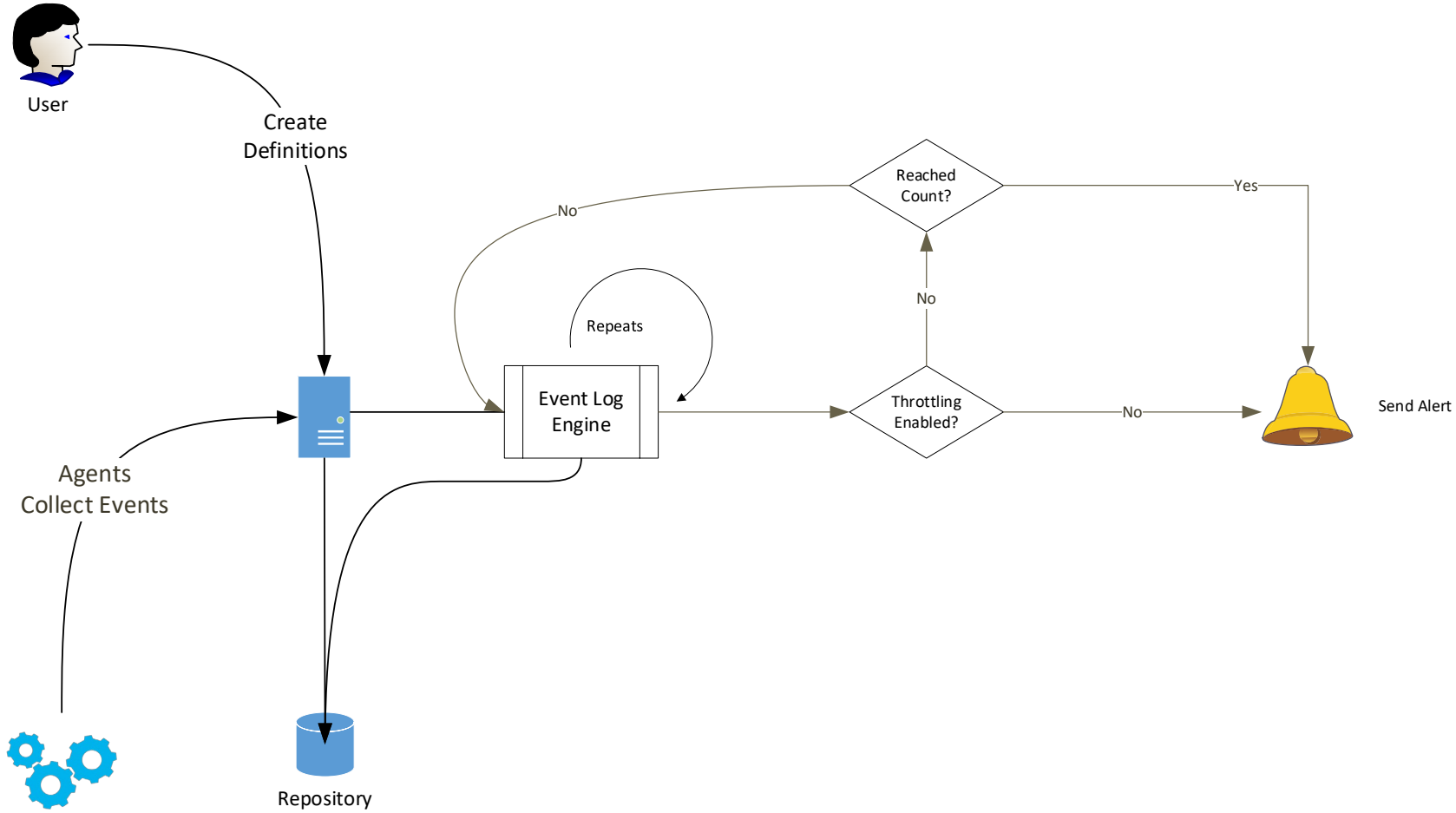
Windows Event Log – Current Solutions

- Out of the box, Foglight provides limited functionality for managing the data it collects for the event logs
 - Basic Data collection via the Agent
 - Very Basic Alerting
 - No control
 - No throttling

Windows Event Log – Solution

- Our Custom Windows Event Log solution simplifies management of incoming events:
 - Generates one Alarm per unique event.
 - Sends one Email per unique event.
 - Sends summary emails per incoming events.
- Ability to specify how long an alarm remains active before it is auto-cleared for specific event(s). (Supports Java Regular Expressions)
- Ability to handle event throttling where an event may be generated x amount of times during a specified period. (Supports Java Regular Expressions)
- The ability not to alert on specific event(s). (Supports Java Regular Expressions)

Windows Event Log – Flow



Windows Event Log – Changing Settings

File Event Log Registry Settings - Local FMS

Save | Undo | Filter

Name	Value	Scoping		
Debug				
PSO.FileEventLog.Debug	true			Whether or not to enable debug mode in the File Event Log
Error Log				
Alarm				
PSO.FileEventLog.Alarm.GenerationSeverity	Warning,Critical,Fatal			Defines the Foglight severity levels that will cause an alarm
Individual Notification				
PSO.FileEventLog.Email.NotificationSeverity	Warning,Critical,Fatal			Defines the Foglight severity levels that will trigger an email notification
PSO.FileEventLog.Email.Recipient.Critical				Comma separated list of email addresses to which to send critical notifications
PSO.FileEventLog.Email.Recipient.Fatal				Comma separated list of email addresses to which to send fatal notifications
PSO.FileEventLog.Email.Recipient.Warning				Comma separated list of email addresses to which to send warning notifications
Summary Notification				
PSO.FileEventLog.Email.NotificationSeverity.Summary	Warning,Critical,Fatal			Defines the Foglight severity levels that will trigger a summary notification
PSO.FileEventLog.Email.Recipient.Summary				Comma separated list of email addresses to which to send summary notifications

- Remote Administration of the solution across servers

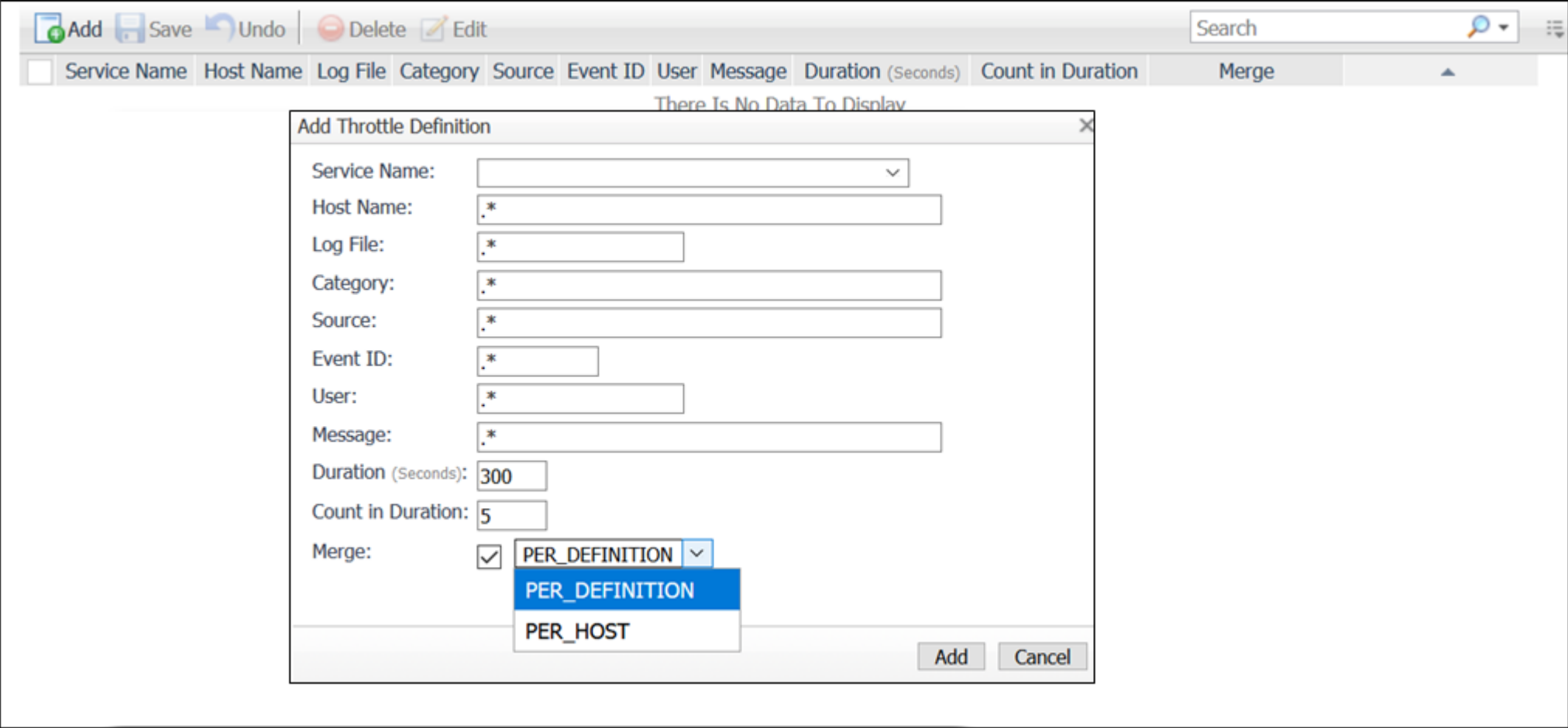
Windows Event Log – Rule Management

The screenshot shows the 'Windows Event Log Rule Management - Local FMS' interface. On the left is a navigation pane with 'Expert View' selected. The main area displays a table of rules with columns for 'Category / Title', 'Enabled', and a description. The rules are grouped into 'Alerting', 'Clean Up', and 'FMS' categories.

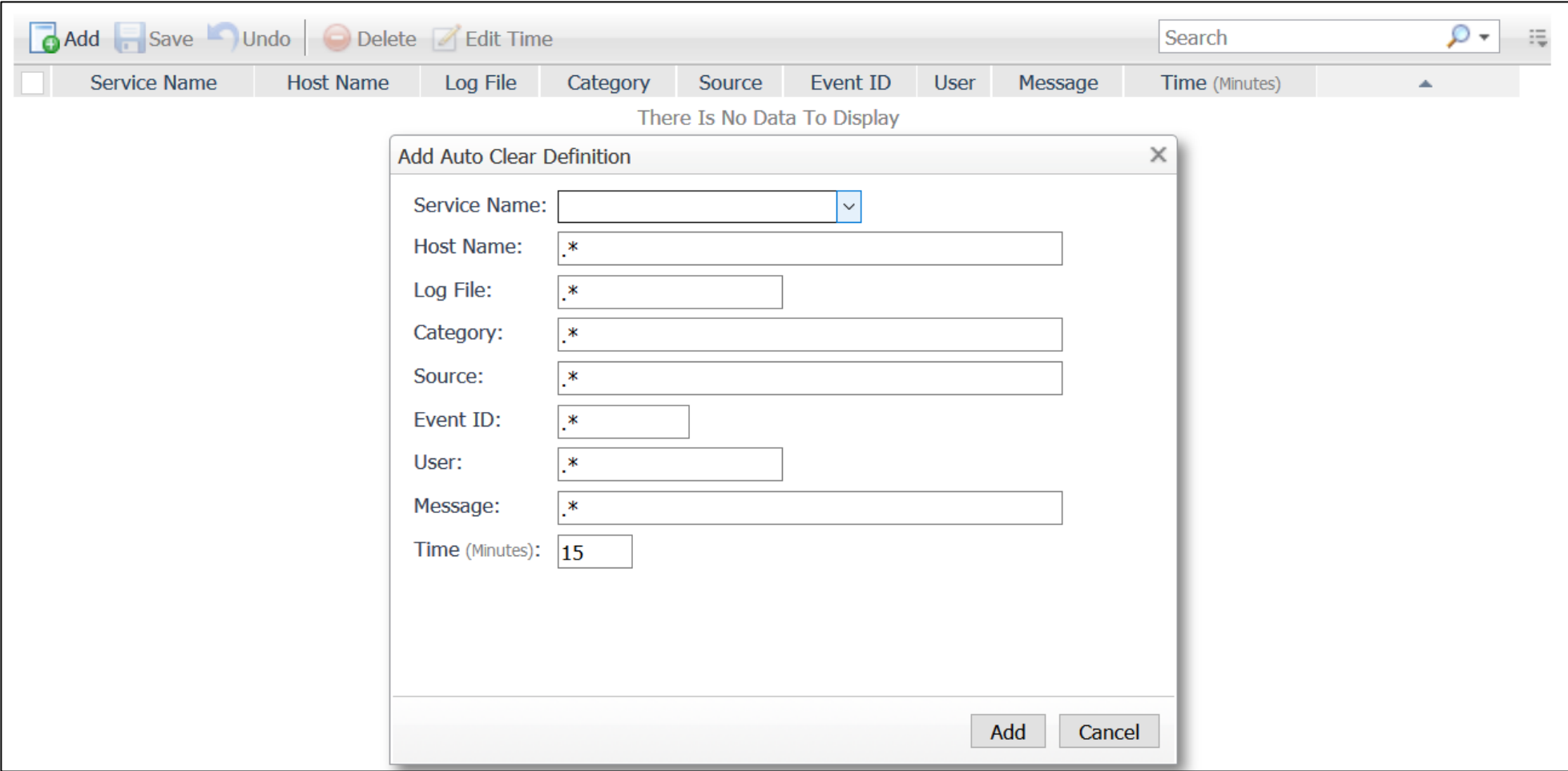
Category / Title	Enabled	Description
Alerting		
<input type="checkbox"/> Windows Event Log		Generates alarms for event logs based on the Throttle definitions.
<input type="checkbox"/> Windows Event Log Record		Generates alarms for event logs based on the Throttle definitions.
Clean Up		
<input type="checkbox"/> Auto Clear Alarms		Handles auto clearing of the various generated event log alarms based on the def
FMS		
<input type="checkbox"/> Ping		Handles updating the FMS Ping Time

- Remote Administration of the solution across servers

Windows Event Log – Throttling Definition



Windows Event Log – Auto Clear Definition



Windows Event Log – System Requirements

- **Minimum required FMS version**

5.9.3

- **Supported Databases**

Microsoft SQL

Oracle

MySQL

PostgreSQL

Minimum Version

2008 (version 10.0.1600 or later)

9i R2

5.1.45

9.4.0