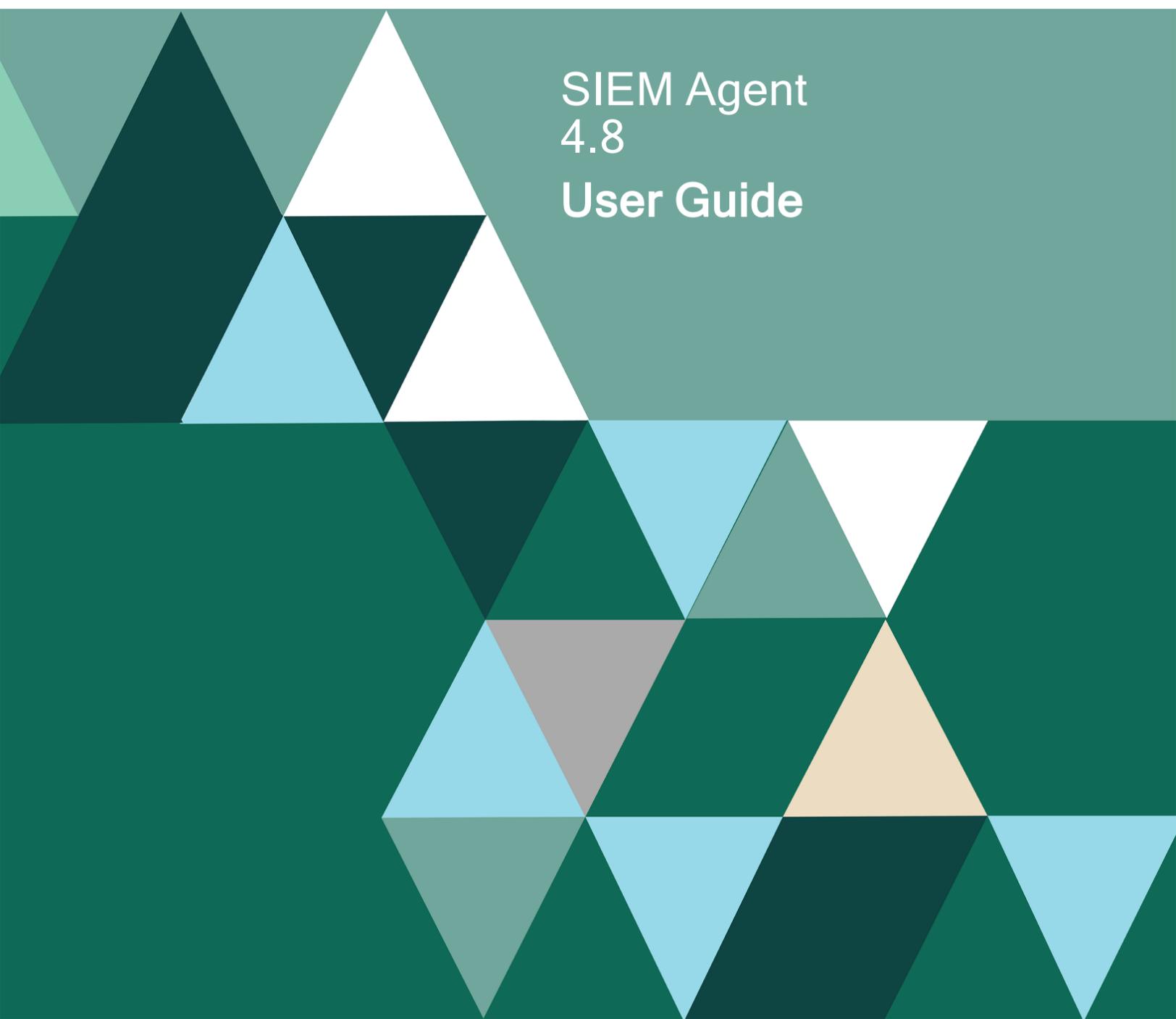


# FORTRA



SIEM Agent  
4.8  
User Guide

## Copyright Terms and Conditions

---

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202410181013

<b>Welcome to Powertech SIEM Agent for IBM i</b>	<b>7</b>
SIEM Agent Overview	7
<b>Implementing Powertech SIEM Agent</b>	<b>9</b>
Configuring SIEM Agent Formats	10
Configuring Outputs	11
Configuring Events and Event Sources	11
Configuring Rules	13
<b>Reference</b>	<b>19</b>
Change Event Description panel	20
Change Event Source panel	24
Change Event Subtype panel	28
Change Extension panel	32
Change Field panel	35
Change Field Substitutions panel	37
Change Format panel	39
Change Output panel	40
Change Rule panel	41
Change Rule Condition panel	42
Copy Event Description panel	43
Copy Event Source panel	44
Copy Event Subtype panel	45
Copy Field panel	46
Copy Format panel	47

Copy Output panel .....	48
Copy Rule panel .....	49
Copy Rule Condition panel .....	50
Create Event Description panel .....	51
Create Event Source panel .....	54
Create Event Subtype panel .....	58
Create Extension panel .....	62
Create Field panel .....	67
Create Field Substitutions panel .....	70
Create Format panel .....	72
Create Output panel .....	79
Create Rule panel .....	87
Create Rule Condition panel .....	92
Display Event Description panel .....	95
Display Event Source panel .....	96
Display Event Subtype panel .....	97
Display Field panel .....	98
Display Field Substitutions panel .....	99
Display Format panel .....	100
Display Output panel .....	105
Display Rule panel .....	106
Display Rule Condition panel .....	107
End Monitor command (PSAENDMON) .....	108

Hold SIEM Monitor command (PSAHLDMON) .....	109
SIEM Agent Main Menu .....	110
Release SIEM Monitor command (PSARLSMON) .....	113
Select Output Target panel .....	114
Start Monitor command (PSASTRMON) .....	117
Trace SIEM Monitor command (PSATRCSIEM) .....	119
Work with Attached Outputs panel .....	122
Work with Event Descriptions panel .....	124
Work with Event Sources panel .....	127
Work with Event Subtypes panel .....	130
Work with Extensions panel .....	133
Work with Fields panel .....	135
Work with Field Substitutions panel .....	139
Work with Formats panel .....	142
Work with Outputs panel .....	144
Work with Rule Conditions panel .....	147
Work with Rules panel .....	150
Work with Utilities panel .....	154
<b>Appendix .....</b>	<b>157</b>
Authority Broker Events .....	158
Command Security Events .....	160
Commands .....	162
Configuring IBM QRadar to Recognize SIEM Agent Output from an IBM i .....	163

Exit Point Manager Events .....	170
Integrating SIEM Agent with Event Manager .....	171
Monitoring Powertech Antivirus with SIEM Agent .....	172
Monitoring SSH Activity with SIEM Agent .....	173
Monitoring Changes to Db2 Data with SIEM Agent .....	174
Implementing JSON .....	179
Making Fields for Journal Entry Formats .....	186
Overriding Host Name / Fully Qualified Host Name in Events .....	188
Selected System Messages .....	190
Audit Journal Events .....	200
Setting up SIEM Agent to use Transport Layer Security (TLS) .....	202
Shutting down SIEM Agent .....	205
Syslog Header Specifications .....	206
Syslog Severity Table .....	209
Work Management .....	210
<b>Glossary .....</b>	<b>211</b>
Event Text .....	211
Extensions .....	211
Monitors .....	213
Rules .....	213
Valid OS Name .....	214
<b>Contacting Fortra .....</b>	<b>215</b>
Fortra Portal .....	215

# Welcome to Powertech SIEM Agent for IBM i

Powertech SIEM Agent for IBM i (SIEM Agent) allows you to:

- Monitor journals and message queues for critical system messages, audit entries, and requests logged by Powertech Exit Point Manager, Authority Broker, and Command Security.
- Filter and extract desired event messages and identify them with custom field substitutions.
- Reformat the data to a preferred format.
- Transmit the messages using your choice of protocols including UDP, TCP, TLS, message queue, or stream file (IFS).

SIEM Agent facilitates real-time notification to an enterprise syslog sever or messaging solution while ensuring only important events are escalated.

## SIEM Agent Overview

SIEM Agent finds informative data, reformats it, and transmits it to another location. The following overview outlines, in general, how SIEM Agent does this.

## Events and Event Sources

IBM i journals and message queues are SIEM Agent's *Event Sources* and the records within are its *Events*. Events are found by one or more monitor jobs running in the PTWRKMGT subsystem. Each Event has an identifier. For journal Events, the identifier is Journal Code + Entry Type (like T:AF). For message queues, the identifier is the message ID. Each Event includes fields that define how to break up the data by offset, length, and data type. Each of these fields can have a *Substitution* associated with it, which is a 'this-for-that data replacement' that can be used during viewing of the Event. You can define the fields and Substitutions for an Event, and one field can be labeled as the field that delivers the Event Subtype value (up to 30 bytes).

Events sometimes have different meanings based on data within the event. An *Event Subtype* divides an Event into different categories (like T-AD with subtype of D (for DLO) or O (for Objects)). The Event Subtype is determined by the content of a specified field.

In order for Events to be comprehended, a *device-event-class-id* is assigned to each Event. The device-event-class-id (user-defined or defined by SIEM Agent) is placed into the output event verbatim. (Previous versions of SIEM Agent (called Interact) surfaced this value as the “Message ID.”) This user-customizable and human-readable message text for the output is called the *Event Text*. The Event Description/Subtype/Rule determines the specific human-readable explanation for the device-event-class-id that was delivered by the Event Subtype above using Event Text (a set of message formatting strings).

See [Configuring Events and Event Sources](#).

## Rules

SIEM Agent uses *Rules* to identify the Events to be transmitted. Rules have the final say in determining whether or not to post a syslog event, to which Output(s) to post the syslog event, and the class and severity for that Event. They are based on *Conditions* that interrogate Event field data. Special fields are available for general information about the event (when, whom, which day of the week, and so forth). This list of special fields may include data from the journal entry “header” that is not available for use in Rules for message queues. Likewise, there may be valuable data for messages that are not available for journals.

Conditions perform the evaluation. Rules supply the values to use in the output event. Rules can specify the severity and proprietary “class” of the output event.

See [Configuring Rules](#).

## Outputs and Formats

Finally, the data is reformatted and written to another location, the *Output*. An *Output Target* object defines this location. A *Format* object attached to an Output specifies output formatting options for that Output. The Format object also specifies the compliance level of the syslog header: RFC3164 or RFC5424. The Output monitor runs in PTWRKMGT. The Output is packaged in a syslog “packet”. The content of the MSG portion of the syslog packet is always formatted in compliance with Micro Focus ArcSight Common Event Format (CEF) v25 dated Sept 2017. The “interesting event details” may be packed into a msg=extension, or laid out as individual extensions as determined by the Format object.

See [Configuring Outputs](#), [Configuring Formats](#), and [Syslog Header Specifications](#).

These instructions are intended as a guide for quick installation and basic configuration, to be supplemented, where referenced, with the *SIEM Agent User Guide*. Find all documentation and reference materials on the Fortra Support Portal at <https://support.fortra.com>.

# Implementing Powertech SIEM Agent

*By the end of this section, you will know how to:*

- *Start SIEM Agent*
- *Configure Formats*
- *Configure Outputs*
- *Configure Events and Event Sources*
- *Configure Rules*

**NOTE:** The Powertech installation procedure creates libraries, profiles, authorization lists, commands, objects, and, in some cases, exit points on your system. Changing the configuration of any of these installed objects may result in product failure.

After you have installed Powertech SIEM Agent, use the following instructions to configure the product.

## To start Powertech SIEM Agent

Starting SIEM Agent requires the following:

- A valid license key must be installed
- Subsystem QSYSWRK must be active
- TCP/IP must be active
- The user profile under which this runs must have \*ALLOBJ special authority or must be a member of the PTADMIN authorization list

Starting Central Administration and SIEM Agent from the command line:

Run the following commands:

**PTPLLIB/PPLSTRMON**  
**PTSALIB/PSASTRMON**

These commands start the required Central Administration and SIEM Agent monitor jobs in the PTWRKMGT subsystem. See [Work Management](#).

To end these jobs, see [Shutting down SIEM Agent](#).

**NOTE:** Before you have “Activated” Event Sources or Outputs, the PSAEVTMON job is the only one running. This is the job that sends product events (such as configuration changes) to Central Administration.

Accessing the SIEM Agent menus:

Submit command **WRKPTSA**, or:

1. On the command line, enter **POWERTECH** to open the Powertech Main Menu.
2. Choose Option **6**. The SIEM Agent [Main Menu](#) appears.

## Committing Configuration Changes

At any point after changing SIEM Agent's configuration settings, to commit your changes, do the following:

1. From the Main Menu, choose option **82**, Work with Utilities.
2. Select option **1**, Commit configuration changes.

## Configuring SIEM Agent Formats

A Format holds settings that control the formatting of syslog event data. These Formats are attached to Outputs such that each Output can transmit syslog events in different formats.

To create or change a SIEM Agent Format:

1. On the SIEM Agent [Main Menu](#), choose option **2**. The [Work with Formats panel](#) appears. CEF, JSON, LEEF, MODERN, and SYSLOG Formats are included by default. You can choose option **2** for a Format to edit an existing Formats, or press **F6** create a new one. See also [Change Format panel](#) and [Create Format panel](#).

**NOTE:** For more information about SYSLOG formats, see [Syslog Header Specifications](#).

2. When you are done defining Formats, press **F3** to return to the Main Menu.

## Configuring Outputs

An Output Target defines a location to which formatted SIEM events are sent. Each Output Target can specify a different output format.

To create an Output:

1. On the SIEM Agent [Main Menu](#), choose option **3**.
2. Press **F6** to create a new Output. The [Work with Outputs panel](#) appears.
3. Enter a name and description for the Output.
4. Set Active to **1** to activate the Output.
5. Select a format and type. Press Enter to reveal additional fields that depend on the Type selected. See [Create Output panel](#) for complete details.
  - \*NETWORK: A network location specification. This could be an IP address or DNS-defined name.
  - \*MSGQ: A message queue.
  - \*STREAM: A stream file in the IFS.
  - \*KAFKA: A Kafka server location specification.
6. Press **Enter** to create the Output.

The Output can now be assigned to one or more Event Sources. See [Configuring Events and Event Sources](#).

## Configuring Events and Event Sources

IBM i Journals and Message Queues that contain the data retrieved by SIEM Agent 4 are called *Event Sources*. The records within these Event Sources are called *Events*. In this section, you will learn how to configure Event Sources in SIEM Agent to identify Events to be extracted, and learn about other options available to you while doing so.

To configure Events and Event Sources:

1. On the SIEM Agent Main Menu, choose option **1**. SIEM Agent includes five existing Event Sources, one for each Event Source Type. See [Work with Event Sources panel](#) for descriptions of the Event Source Types.

2. Enter **9** for an Event Source. The [Work with Event Descriptions panel](#) appears.
  - a. Use option **6** to activate the events you would like to process. For journal events, also use option **8** to activate the desired subtypes.
  - b. For Journal Events, make any desired changes to Event Fields (option **7**) or Subtypes (option **8**). See [Work with Fields panel](#) and [Work with Event Subtypes panel](#).

**EXAMPLE:** Choose **7** for an event and then **7** for a field to open the [Work with Field Substitutions panel](#) where you can translate a field to a human-readable value. A Substitution can be defined by an Event Description, a Subtype, or a Rule.

- c. To add or change the Extension or Event Text– the set of formatting patterns used to generate the human-readable form sent to the Output – choose **2** for an Event or Subtype, then press **F13** or **F14**, respectively. See also [Extensions](#) and [Event Text](#).

**NOTE:** Event text can be defined by an Event Description, Subtype, or Rule.

- d. Use option **9** to define [Rules](#) for an Event. See [Configuring Rules](#).
    - e. Press Enter.
3. Enter **2** for an existing Event Source, or press **F6** to create a new one. The [Change Event Source panel](#) or [Create Event Source panel](#) appears, respectively.
4. Enter the requested information.
5. For Active, enter **1** to activate the Event Source.
6. Press **F8** to attach an Output. See [Work with Attached Outputs panel](#). You can attach multiple Outputs to the same Event Source.
  - a. Press **F6**. The [Select Output Target panel](#) appears.
  - b. Enter **1** for the desired Output. To define an output, see [Configuring Outputs](#).
  - c. Press Enter. You return to the Work with Attached Outputs panel.
7. Press **Enter**.

**NOTE:** See [Monitoring Changes to Db2 Data with SIEM Agent](#) for a sample procedure that describes how to monitor database fields in SIEM Agent.

# Configuring Rules

A relevant piece of data within an event, such as a user profile name, sometimes warrants the inclusion of additional Extensions, an alternative Event Text message, or the need to send the notification to alternative Outputs. SIEM Agent accommodates this need using Rules.

To configure Rules:

1. On the SIEM Agent Main Menu, choose option 1. SIEM Agent includes five existing Event Sources, one for each Event Source Type. See [Work with Event Sources panel](#) for descriptions of the Event Source Types.
2. Enter **9** for an Event Source. The [Work with Event Descriptions panel](#) appears.
3. Enter **9** for an Event. When you add a Rule to an Event, it applies to all Event Subtypes. To add a Rule to a specific Event Subtype, choose **8** for the Event, then **9** for the desired Subtype. The [Work with Rules panel](#) appears.
4. Press **F6** to create a new Rule.
5. Specify the Sequence, Description, and other available options. See [Create Rule panel](#) for details.
6. Press **Enter**. Additional fields appear. When creating a Rule, you are asked to provide the action to take if the Conditions for the Rule succeed, which can be alternative Outputs, additional Extensions (for Subtypes, Extensions in addition to those already defined for the event class), or alternative Event Text. Do one or more of the following:
  - Press **F8** to open the [Work with Attached Outputs panel](#), where you can specify an Output.
    - a. Press **F6** to select an Output Target.
    - b. Enter **1** for a desired target and press **Enter**.
    - c. If you would like to specify multiple Outputs, press **F6** again.
    - d. Press **F12** to return to the Create Rule panel.
  - Press **F13** to open the [Work with Extensions panel](#), where you can specify Extensions.
    - a. Press **F6** to open the [Create Extensions panel](#).
    - b. Enter a Name and Value. See also [Extensions](#).
    - c. Press **Enter**. You return to the Work with Extensions panel.
    - d. Press **F6** to create another Extensions, or press **F12** to return to the Create Rule panel.

- Press F14 to open the [Create Event Text panel](#), where you can define an Event Text message.
  - a. Enter a Reason and Message. See [Event Text](#).
  - b. Press Enter to return to the Create Rule panel.
- 7. Press **Enter** to return to the Work with Rules panel. SIEM Agent 4 evaluates each Rule by comparing data in the event to a Condition or Conditions attached to the Rule.
- 8. Choose **8** for the Rule you just created. The [Work with Rule Conditions panel](#) appears.
- 9. Press **F6**.
- 10. Enter the Sequence, Link, Field, Operator, and Criteria for the Condition. See [Create Rule Condition panel](#) for details.

**EXAMPLE:**

If you wanted a condition that required, for example the PWUSRN field of the TPW-P Subtype of QAUDJRN to be GDORN, you would enter the following:

```

PSR4811                      Powertech SIEM Agent                      12:21:08
                             Create Rule Condition

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Event Description . . . : TPW (Passwords used that are not valid)
Event Subtype . . . . . : P (Password not valid.)
Rule . . . . . : 1 (User is GDORN)

Sequence . . . . . : 0001                      1-9999
Link . . . . . : OR                          AND, OR
Field . . . . . : PWUSRN                      F4 for list
Operator . . . . . : =                        =, <>, >, <, >=, <=
Criteria . . . . . : GDORN

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel

```

- 11. Press **Enter**. You return to the Work with Rule Conditions panel.
- 12. Press **F6** to add an additional Condition.

**EXAMPLE:**

For example, you could use the OR and EQUALS value to create a set of Conditions in the Rule that compares the PWUSRN field of the event to many user profiles. In this case, if a match is found for any, the Rule succeeds.

PSA4810

Powertech SIEM Agent

13:52:49

Work with Rule Conditions

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)

Event Description . . . . : TPW (Passwords used that are not valid)

Event Subtype . . . . . : P (Password not valid.)

Rule . . . . . : 1 (User is GDORN)

Type options, press Enter

2=Change 3=Copy 4=Delete 5=Display

Opt	Seq	Link	Field	Operator	Criteria
-	1	OR	PWUSRN	=	GDORN
-	2	OR	PWUSRN	=	HCELINE
-	3	OR	PWUSRN	=	JMALIK
-	4	OR	PWUSRN	=	SGOODMAN
-	5	OR	PWUSRN	=	SMOON
-	6	OR	PWUSRN	=	HOWARD

Bottom

F3=Exit F5=Refresh F6=Create F12=Cancel

Rule Condition created.

When you have finished adding Conditions, press **F12** to return to the Work with Rules panel.

- Press **F6** to add an additional Rule. An event can contain multiple Rules, which, like Conditions, are evaluated in sequential order. Or, if you are finished adding Rules, press **F12** to return to the previous panel.

When SIEM Agent processes the Event at different levels, Outputs and Event Text are handled differently from Extensions.

When a Rule sets an Output, that Output selection overrides the selection of higher levels. For example, the Output set in a Subtype Rule overrides the standard selection defined at the Event Source (higher level).

When a Rule or a Subtype sets the Event Text, this will replace any Event text defined at higher levels. For instance, an Event Text set at the Subtype level will override that defined in an Event Description Rule (higher), and can in turn be overridden by a Subtype Rule (lower).

In contrast, Extensions are additive. When a Rule or Subtype defines Extensions, the Extensions are added to the Extensions defined at the higher levels. Extensions are then sorted in alphabetical order before the Event is sent to the Output. In the following table, the levels are ordered from highest to lowest.

Level	Output Selection	Event Text	Extensions
Event Source	Select Output		
Event Description		Set Event Text	Add Extension
Event Description Rule	Override Outputs	Override Event Text	Add Extension
Subtype		Override Event Text	Add Extension
Subtype Rule	Override Outputs	Override Event Text	Add Extension

**EXAMPLE:**

To illustrate the hierarchical nature of Rules, consider you have created a Rule at the TPW Event Description level to forward all TPW events to OUTPUTA. However, all TPW-P events should be forwarded to OUTPUTB instead. To configure this, you would create a Rule for the TPW-P Subtype, and set the Rule Output to OUTPUTB. Now, all TPW events are forwarded to OUTPUTA except TPW-P events, which are forwarded to OUTPUTB.

```

PSR4711                               Powertech SIEM Agent           16:10:04
                                   Change Rule

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Event Description . . . : TPW (Passwords used that are not valid)
Event Subtype . . . . . : P (Password not valid.)

Rule sequence . . . . . : 1                1-9999
Description . . . . . : Use OUTPUTB

Active . . . . . : 1                1=Yes, 0=No
Stop evaluation . . . . : 1                1=Yes, 0=No
Event Class ID . . . . . : *                *, *NAME, character value
Severity . . . . . : *                *, 4=Warning, 5=Notice, ...
Class . . . . . : *                *, AUD, VULN, IDS, SYS, STG, ...

Rule Output . . . . . : Present            *, None, F8=Maintain Outputs
Extension . . . . . : None                F13=Extensions
Event text . . . . . : None                F14=Event Text

F3=Exit   F5=Refresh   F8=Maintain Outputs   F12=Cancel
F13=Extensions   F14=Event Text

```

Now, imagine profile TEST is creating many TPW-P events that should be ignored. To omit these extra events, you can create another Rule with Rule Output set to None and a corresponding Condition with PWUSRN = TEST.

```

PSA4711                                Powertech SIEM Agent                16:06:23
                                      Change Rule

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Event Description . . . : TPW (Passwords used that are not valid)
Event Subtype . . . . . : P (Password not valid.)

Rule sequence . . . . . : 2                1-9999
Description . . . . . : Omit invalid pwd events from profile TEST

Active . . . . . : 1                1=Yes, 0=No
Stop evaluation . . . . : 1                1=Yes, 0=No
Event Class ID . . . . . : *            *, *NAME, character value
Severity . . . . . : *                *, 4=Warning, 5=Notice, ...
Class . . . . . : *                *, AUD, VULN, IDS, SYS, STG, ...

Rule Output . . . . . : None            *, None, F8=Maintain Outputs
Extension . . . . . : None            F13=Extensions
Event text . . . . . : None            F14=Event Text

F3=Exit  F5=Refresh  F8=Maintain Outputs  F12=Cancel
F13=Extensions  F14=Event Text

```

```

PSA4811                                Powertech SIEM Agent                16:02:30
                                      Create Rule Condition

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Event Description . . . : TPW (Passwords used that are not valid)
Event Subtype . . . . . : P (Password not valid.)
Rule . . . . . : 2 (Omit invalid pwd events from profile TEST)

Condition sequence . . . : 1                1-9999

Link . . . . . : AND                AND, OR

Field . . . . . : PWUSRN            F4 for list

Operator . . . . . : =                =, <>, >, <, >=, <=

Value . . . . . : TEST

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel

```

Now, TPW-P events initiated from profile TEST are not forwarded to any output. TPW-P events initiated from profiles other than TEST are forwarded to OUTPUTB.

## Viewing History with Central Administration

You can use Powertech Central Administration to view a record of SIEM Agent history. To do so:

1. From the command line, enter **POWERTECH**.
2. From the Powertech Main Menu, choose option **80**, Central Administration.

3. Choose option **4**, History Menu. Use the options here to view a history of product activity.

# Reference

The topics in this section include reference information including menu and screen descriptions.

# Change Event Description panel

The Change Event Description panel allows you to modify the properties of an existing Event Description.

PSA4211

14:15:48

Powertech SIEM Agent

Change Event Description

Event Description . . . . : AUDIT (IBM i Security Audit Journal)

Name . . . . . : I AF

Journal Code and Entry Type

Description . . . . . : All authority failures

Active . . . . . : 1

1=Yes, 0=No

Event Class ID . . . . . : TAF

\*NAME, character value

Severity . . . . . : 6

4=Warning, 5=Notice, 6=Info, ...

Class . . . . . : AUD

AUD, VULN, IDS, SYS, STG, ...

Extension . . . . . : None

F13=Extensions

Event text . . . . . : Present

F14=Event Text

F3=Exit

F5=Refresh

F12=Cancel

F13=Extensions

F14=Event Text

## How to Get There

Enter **2=Change** for an entry in the [Work with Event Descriptions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Name

The name you use to refer to this Event Description within Powertech SIEM Agent. For events that originate in a journal, this name must be comprised of the Journal Code and Entry Type of the journal entry. For message queue events, this name must be a message ID.

## Description

A short description you assign to the Event Description.

## Active

Indicates whether the Event Description is available for processing. When an Event Description is not active, the event it identifies will not be processed.

## Event Class ID

Event Class ID is simply placed into the syslog output event when using the Legacy Interact 3 Syslog format. Interact 3 formatted this data as a message ID, but you are free to specify whatever data is meaningful to you.

Specify \*NAME to display the Event Description's Name in the output. For journals, this is the Journal Code and Entry Type (for example, TCD). For message queues, \*NAME displays the Message ID (for example, CPF0907).

You can specify a single asterisk (\*) to inherit the value from the parent Event Description at run time.

## Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

0=Emergency

System is unusable; A panic condition.

1=Alert

Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.

2=Critical

Critical conditions; Hard device errors.

3=Error

Error conditions

4=Warning

Warning conditions

5=Notice

Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.

6=Informational

Informational messages

7=Debug

Debug-level messages; Messages that contain information normally of use only when debugging a program.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

- AUD - Audit event
- POL - Policy event
- VULN - Vulnerability event
- FW - Firewall event
- IDS - Intrusion detected event
- SYS - System event
- STG - Storage event

## Extension

At the Event Description level, the Extension field defines the default Extensions. Additional Extensions can be added for individual Subtypes and Rules defined within the Event Description, for example, those specified in the Add Extension field of the respective [Create Event Subtype panel](#) and [Create Rule panel](#).

## Event Text

At the Event Description level, this field defines the default Event Text for the Event Description. If you leave this field blank, most Events will have blank Event Text. The Event Text for Subtypes and Rules defined within this Event Description can be overridden using the Override Event Text field in, for example, the respective [Create Event Subtype panel](#) and [Create Rule panel](#).

## Command Keys

F3=Exit

Exit the program.

F4=Prompt

Displays a list of items from which one or more may be selected.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

# Change Event Source panel

The Change Event Source panel allows you to modify the properties of an existing Event Source.

PSA4111

Powertech SIEM Agent

11:59:01

Change Event Source

Name . . . . . : AUDIT

Description . . . . . : IBM i Security Audit Journal

Type . . . . . : \*AUDIT

\*AUDIT, \*SYSMSG, \*JRN, \*MSGQ, ...

Default Output . . . . . : \*NONE

Name, \*NONE, F4 for list

Facility . . . . . : 4

1=User-level, 4=Security, ...

Active . . . . . : 0

1=Yes, 0=No

Object . . . . . : QAUDJRN

Library . . . . . : QSYS

ASP Group . . . . . : \*SYSBAS

Name, \*SYSBAS

F3=Exit

F4=Prompt

F5=Refresh

F12=Cancel

## How to Get There

Enter **2=Change** for an entry in the [Work with Event Sources panel](#).

## Field Descriptions

### Name

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

### Description

A short description you assign to the Event Source.

## Type

The type of object from which IBM i events will be extracted. Journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue).

### \*AUDIT

Defines the IBM Security Audit Journal, QAUDJRN, to be monitored. This type includes some canned definitions of the journal codes and entry types for the security-related journal entries.

### \*SYSMSG

Defines the IBM System Messages in QSYSOPR or QSYSMSG to be monitored. This type includes some canned definitions of some interesting system management messages.

### \*EPM

Defines the Powertech Exit Point Manager Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Exit Point Manager entries.

### \*AB

Defines the Powertech Authority Broker Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Authority Broker.

### \*CMDSEC

Defines the Powertech Command Security Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Command Security.

### \*MSGQ

Defines a user-defined message queue to be monitored. You define the messages you would like monitored.

### \*JRN

Defines a user-defined journal to be monitored. You define the journal codes and entry types you would like monitored.

## Default Output

Indicates that there is, or is not, a set of Outputs attached to the Event Source that act as Default Outputs.

Names the default Output(s) to which syslog events will be sent for this Event Source. These Outputs will be used when a Rule specifies \*SOURCE for a target Output.

## Facility

Indicates the "facility", as defined by the Common Event Format specification. This value is used in the syslog output event. The allowed values are:

Value	Meaning
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authentication messages
5	Messages generated internally by syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authentication messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Scheduling daemon
16	Locally used facilities (local0 through local7)

## Active

Indicates whether the Event Source is available for processing. When an Event Source is not active, it will not be monitored.

## Object

The name of object from which IBM i events will be extracted.

This name is required to be a [valid OS name](#).

## Library

The library in which the Event Source object is located.

This name is required to be a [valid OS name](#).

## ASP Group

The name of the ASP Group in which the library containing the object resides.

This name is required to be a [valid OS name](#).

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F8=Maintain Outputs

Opens the [Work with Attached Outputs panel](#), where you can attach an output to the Event Source.

### F12=Cancel

Discards changes and returns to the prior panel.

# Change Event Subtype panel

The Change Event Subtype panel allows you to modify the properties of an existing Event Subtype.

PSA4511	Powertech SIEM Agent	14:17:02
Change Event Subtype		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TAD (A change was made to the auditing attribute)		
Field . . . . . : ADETYP (Type of entry)		
Name (1 char) . . . . . : <u>D</u>		
Description . . . . . : <u>CHGDLOAUD command</u>		
Active . . . . .	: <u>1</u>	1=Yes, 0=No
Event Class ID . . . . .	: <u>TAD0004</u>	*, *NAME, character value
Severity . . . . .	: <u>5</u>	*, 4=Warning, 5=Notice, ...
Class . . . . .	: <u>AUD</u>	*, AUD, VULN, IDS, SYS, STG, ...
Add Extension . . . . .	: None	F13=Extensions
Override Event text . . . .	: None	F14=Event Text
F3=Exit    F5=Refresh    F12=Cancel    F13=Extensions    F14=Event Text		

## How to Get There

Enter **2=Change** for an entry in the [Work with Event Subtypes panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Name

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Field

Event Field names the definition of the field whose content determines the Event Subtype at the time an event is intercepted.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

### Name

The name you use to refer to this Event Subtype within Powertech SIEM Agent. The name must match exactly whatever data the "subtype field" can contain in the actual event data at execution time.

### Description

A short description you assign to the Event Subtype.

### Active

Indicates whether the Event Subtype is available for processing. When an Event Subtype is not active, the event it identifies will not be processed.

### Event Class ID

Event Class ID is simply placed into the syslog output event when using the Legacy Interact 3 Syslog format. Interact 3 formatted this data as a message ID, but you are free to specify whatever data is meaningful to you.

Specify \*NAME to display the Event Description's Name followed by the Subtype, separated by a colon. For example, `TCD:A`.

You can specify a single asterisk (\*) to inherit the value from the parent Event Description at run time.

### Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

0=Emergency  
System is unusable; A panic condition.

- 1=Alert  
Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.
- 2=Critical  
Critical conditions; Hard device errors.
- 3=Error  
Error conditions
- 4=Warning  
Warning conditions
- 5=Notice  
Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.
- 6=Informational  
Informational messages
- 7=Debug  
Debug-level messages; Messages that contain information normally of use only when debugging a program.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

- AUD - Audit event
- POL - Policy event
- VULN - Vulnerability event
- FW - Firewall event
- IDS - Intrusion detected event
- SYS - System event
- STG - Storage event

## Add Extension

Indicates whether any Extensions are attached to the Event Subtype.

## Override Event Text

Allows access to the Event Text override for the Event Subtype.

Event Text dictates how to format the event data into a human-readable format. Fields defined for the Event Description can be used to provide data for the text at run time.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

F13=Extensions

Work with any Extensions that may be attached. See [Work with Extensions panel](#).

F14=Event Text

Work with an Event Text that may be attached. See [Create Event Text panel](#).

# Change Extension panel

The Change Extension panel allows you to modify the properties of an existing Extension.

PSA4C11	Powertech SIEM Agent Change Extension	16:31:55
Event Source . . . . . : AUDIT (IBM i Security Audit Journal) Event Description . . . : TCP (Create, change, restore user profiles) Event Subtype . . . . . : None Rule . . . . . : None		
Name . . . . . : EPOCHTIME		
Value . . . . . : %extract(EPOCH from '%*TIMESTAMP%')		
JSON Data Type Override : _ blank, C=Character, N=Numeric		
F3=Exit F5=Refresh F8=Insert field at cursor F9=Insert extension at cursor F12=Cancel		

## How to Get There

Choose **2** for an Extension on the [Work with Extensions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

### Event Subtype

Indicates the Event Subtype to which the listed Rules pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Rule

Indicates the Rule to which the listed Extensions pertain.

## Name

The name used on the left side of the equal sign in an extension.

## Value

The value used on the right side of the equal sign in an extension.

## JSON Data Type Override

This field allows JSON to treat the outcome of a value as character or numeric versus its original field data type.

Possible values are:

**Blank** will leave the default outcome of the value.

**C=Character** will insert double quotation marks around the value.

**N=Numeric** will provide the numeric value without quotation marks.

## Command Keys

### F3=Exit

Exit the program.

### F4=Prompt

Displays a list of items from which one or more may be selected.

### F5=Refresh

Discards changes and remains on this panel.

F8=Insert a field at cursor

Allows you to select and insert a Field reference at the cursor position. Existing text will be moved right to make room for the Field reference.

F12=Cancel

Discards changes and returns to the prior panel.

# Change Field panel

The Change Event Subtype panel allows you to modify the properties of an existing Event Field.

PSA4311	Powertech SIEM Agent Change Field	13:25:07
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . : TAD (A change was made to the auditing attribute)		
Name . . . . . : <u>ADETYP</u>		
Description . . . . . : <u>Type of entry</u>		
Subtype . . . . . : <u>1</u> 1=Yes, 0=No		
Offset . . . . . : <u>0</u> 0-32659		
Length . . . . . : <u>1</u> 1-32660		
Data Type . . . . . : <u>A</u> A=Character, I=Integer, S=Signed,		
CCSID . . . . . : <u>65535</u> 0-65535		
Field Substitution . . . :                      F13=Substitutions		
F3=Exit    F5=Refresh    F12=Cancel		

## How to Get There

Enter **2=Change** for an entry in the [Work with Fields panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Name

The name you use to refer to this Event Description within Powertech SIEM Agent. For events that originate in a journal, this name must be comprised of the Journal Code and Entry Type of the journal entry. For message queue events, this name must be a message ID.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

# Change Field Substitutions panel

The Change Field Substitution panel allows you to modify the properties of an existing Field Substitution.

PSA4411	Powertech SIEM Agent	14:53:44
Change Field Substitution		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . : TAD (A change was made to the auditing attribute)		
Field . . . . . : ADETYP (Type of entry)		
Default . . . . . : <u>0</u> 1=Yes, 0=No		
From value . . . . . : <u>D</u>		
To value . . . . . : <u>CHGDLOAUD command</u>		
F3=Exit F5=Refresh F12=Cancel		

## How to Get There

Enter **2=Change** for an entry in the [Work with Field Substitutions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Field

Field names the definition of the field whose content determines the Event Subtype at the time an event is intercepted.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

## Default

Indicates that this substitution is to be used if no other applies.

## From value

The field value to be translated.

## To value

The new value of the field.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

# Change Format panel

The Change Format panel allows you to modify the attributes of a Format.

The fields and options are the same as those of the [Create Formats panel](#).

PSA4A11	Powertech SIEM Agent Change Format	10:02:12 DWSIEM73
Name . . . . . : <u>SYSLOG</u>		
Description . . . . . : <u>Interact syslog format</u>		
Message Style . . . . . : <u>*SYSLOG</u> *MODERN, *CEF, *SYSLOG, *LEEF, *JSON		
Header specification . . . : <u>RFC3164</u> RFC5424 (Modern), RFC3164 (Legacy)		
Use Header Format		
Compatibility . . . . . : <u>N</u> Y=Yes, N=No		
F3=Exit    F5=Refresh    F12=Cancel		

## How to Get There

Press 2 for a format for a format in the [Work with Formats panel](#).

# Change Output panel

The Change Format panel allows you to modify the attributes of a Format.

The fields and options are the same as those of the [Create Output panel](#).

PSA4B11	Powertech SIEM Agent Change Output	11:47:52
Name . . . . . : <u>ABSJRNSTMF</u>		
Description . . . . . : <u>Authority Broker Journal Stream File Output</u>		
Active . . . . . : <u>1</u>	1=Yes, 0=No	
Format . . . . . : <u>MODERN</u>	F4 for list	
Type . . . . . : <u>*STREAM</u>	*NETWORK, *MSGQ, *STREAM	
CCSID for stream file . . : <u>*UTF8</u> *UTF8, *UTF16, 1 - 65535		
Line ends . . . . . : <u>*CRLF</u> *CR, *LF, *CRLF		
Path . . . . . : <u>/home/sid/siem4/abjrnstmf.log</u>		
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel		

## How to Get There

Press 2 for an output in the [Work with Outputs panel](#).

# Change Rule panel

The Change Rule panel allows you to modify the attributes of a Rule.

The fields and options are the same as those of the [Create Rule panel](#).

PSA4711	Powertech SIEM Agent	14:29:22
	Change Rule	V7R2TEST
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : AJB (All authority failures)		
Event Subtype . . . . . : None		
Rule sequence . . . . . : <u>10</u> 1-9999		
Description . . . . . : <u>Snd message to Security Team</u>		
Active . . . . . : <u>0</u> 1=Yes, 0=No		
Stop evaluation . . . . . : <u>0</u> 1=Yes, 0=No		
Event Class ID . . . . . : <u>*</u> *, *NAME, character value		
Severity . . . . . : <u>*</u> *, 4=Warning, 5=Notice, ...		
Class . . . . . : <u>*</u> *, AUD, VULN, IDS, SYS, STG, ...		
Rule Output . . . . . : <u>*</u> *, None, F8=Maintain Outputs		
Add Extension . . . . . : None F13=Extensions		
Override Event text . . . : None F14=Event Text		
F3=Exit F5=Refresh F8=Maintain Outputs F12=Cancel		
F13=Extensions F14=Event Text		

## How to Get There

In the [Work with Rules panel](#), choose **2** for an existing rule.

# Change Rule Condition panel

The Change Rule Condition panel allows you to change a Condition for a Rule.

The fields and options are the same as those of the [Create Rule Condition panel](#).

PSA4811

Powertech SIEM Agent

14:40:44

Change Rule Condition

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)

Event Description . . . . : TPW (Passwords used that are not valid)

Event Subtype . . . . . : P (Password not valid.)

Rule . . . . . : 1 (User is GDORN)

Sequence . . . . . : 1

1=9999

Link . . . . . : OR

AND, OR

Field . . . . . : PWUSRN

F4 for list

Operator . . . . . : =

=, <>, >, <, >=, <=

Criteria . . . . . : GDORN

F3=Exit

F4=Prompt

F5=Refresh

F12=Cancel

## How to Get There

In the [Work with Rule Conditions panel](#), choose **2** for a Condition.

# Copy Event Description panel

The Copy Event Description panel allows you to create a new Event Description by copying the properties and content of an existing Event Description.

The fields and options are the same as those of the [Change Event Description panel](#).

PSA4211

Powertech SIEM Agent

14:25:48

Copy Event Description

Event Description . . . . : AUDIT (IBM i Security Audit Journal)

Name . . . . . : A JB

Journal Code and Entry Type

Description . . . . . : All authority failures

Active . . . . . : 1

1=Yes, 0=No

Event Class ID . . . . . : TAF

\*NAME, character value

Severity . . . . . : 6

4=Warning, 5=Notice, 6=Info, ...

Class . . . . . : AUD

AUD, VULN, IDS, SYS, STG, ...

Extension . . . . . : None

F13=Extensions

Event text . . . . . : Present

F14=Event Text

F3=Exit

F5=Refresh

F12=Cancel

F13=Extensions

F14=Event Text

## How to Get There

Enter 3=Copy for an entry in the [Change Event Descriptions panel](#).

## Copy Event Source panel

The Copy Event Source panel allows you to create a new Event Source by copying the properties and content of an existing Event Source.

The fields and options are the same as those of the [Change Event Source panel](#).

PSA4111	Powertech SIEM Agent	12:28:30
	Copy Event Source	
Name . . . . . : _____		
Description . . . . . : <u>IBM i Security Audit Journal</u>		
Type . . . . .	: <u>*AUDIT</u>	*AUDIT, *SYSMSG, *JRN, *MSGQ, ...
Default Output . . . . .	: <u>*NONE</u>	Name, *NONE, F4 for list
Facility . . . . .	: <u>4</u>	1=User-level, 4=Security, ...
Active . . . . .	: <u>0</u>	1=Yes, 0=No
Object . . . . . : QAUDJRN		
Library . . . . . : QSYS		
ASP Group . . . . .	: *SYSBAS	Name, *SYSBAS
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel		

## How to Get There

Enter **3=Copy** for an entry in the [Work with Event Sources panel](#).

# Copy Event Subtype panel

The Copy Event Subtype panel allows you to create a new Event Subtype by copying the properties and content of an existing Event Subtype.

The fields and options are the same as those of the [Change Event Subtype panel](#).

PSA4511

Powertech SIEM Agent  
Copy Event Subtype

13:38:34

Event Source . . . . .

AUDIT (IBM i Security Audit Journal)

Event Description . . . . .

TPW (Passwords used that are not valid)

Field . . . . .

PWTYPE (P-Pwd, U-User name, A-APPC, D-)

Name (1 char) . . . . .

Description . . . . .

Password not valid.

Active . . . . .

1

1=Yes, 0=No

Event Class ID . . . . .

TPW0016

\*, \*NAME, character value

Severity . . . . .

5

\*, 4=Warning, 5=Notice, ...

Class . . . . .

IDS

\*, AUD, VULN, IDS, SYS, STG, ...

F3=Exit

F5=Refresh

F12=Cancel

## How to Get There

Enter **3=Copy** for an entry in the [Work with Event Subtypes panel](#).

# Copy Field panel

The Copy Event Subtype panel allows you to create a new Event Field by copying the properties and content of an existing Event Field.

The fields and options are the same as those of the [Change Field panel](#).

PSA4311	Powertech SIEM Agent	13:41:44
Copy Field		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TAD (A change was made to the auditing attribute)		
Name . . . . . : _____		
Description . . . . . : <u>Type of entry</u> _____		
Subtype . . . . . : <u>1</u>	1=Yes, 0=No	
Offset . . . . . : <u>0</u>	0-32659	
Length . . . . . : <u>1</u>	1-32660	
Data Type . . . . . : <u>A</u>	A=Character, I=Integer, S=Signed,	
CCSID . . . . . : <u>65535</u>	0-65535	
Field Substitution . . . . :	F13=Substitutions	
F3=Exit   F5=Refresh   F12=Cancel		

## How to Get There

Enter **3=Copy** for an entry in the [Work with Fields panel](#).

# Copy Format panel

The Copy Format panel allows you to create a new Format by copying the properties and content of an existing Format.

The fields and options are the same as those of the [Create Formats panel](#).

PSA4A11

Powertech SIEM Agent  
Copy Format

10:47:22

Name . . . . .

:

Description . . . . .

:

Interact CEF format

Message Style . . . . .

:

\*CEF

\*MODERN, \*CEF, \*SYSLOG

Header specification . . . . .

:

RFC3164

RFC5424 (Modern), RFC3164 (Legacy)

Microseconds . . . . .

:

\*NONE

\*NONE, 3 digits, 6 digits

Time zone . . . . .

:

\*NONE

\*NONE, \*UTC, \*ZULU

F3=Exit

F5=Refresh

F12=Cancel

## How to Get There

Press 3 for a format in the [Work with Formats panel](#).

## Copy Output panel

The Copy Output Target panel allows you to create a new Output Target by copying the properties and content of an existing Output Target.

The fields and options are the same as those of the [Create Output panel](#).

PSA4B11	Powertech SIEM Agent Copy Output	13:48:23
Name . . . . . : _____		
Description . . . . . : <u>Disabled user profiles</u>		
Active . . . . .	: <u>0</u>	1=Yes, 0=No
Format . . . . .	: <u>MODERN</u>	F4 for list
Type . . . . .	: <u>*NETWORK</u>	*NETWORK, *MSGQ, *STREAM
Location . . . . . : <u>10.xx.xxx.xxx: xxxx</u>		
Port . . . . .	: <u>514</u>	1-65535
Protocol . . . . .	: <u>*UDP</u>	*TCP, *UDP, *TLS
Recovery limit . . . . .	: <u>99</u>	Retries
Time interval . . . . .	: <u>99</u>	Seconds
Special . . . . .	: <u>0</u>	1=Yes, 0=No
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel		

## How to Get There

Press **3** for an output in the [Work with Outputs panel](#).

# Copy Rule panel

The Copy Rule panel allows you to copy a Rule.

The fields and options are the same as those of the [Create Rule panel](#).

PSA4711	Powertech SIEM Agent	11:10:23
Copy Rule		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . : TAF (All authority failures)		
Event Subtype . . . . . : None		
Sequence . . . . . : _____ 1=9999		
Description . . . . . : <u>Specific authority failures</u>		
Active . . . . . : <u>1</u> 1=Yes, 0=No		
Test Run . . . . . : <u>1</u> 1=Yes, 0=No		
Stop evaluation . . . . : <u>1</u> 1=Yes, 0=No		
Event Class ID . . . . . : <u>*NAME</u> *, *NAME, character value		
Severity . . . . . : <u>4</u> *, 4=Warning, 5=Notice, ...		
Class . . . . . : <u>sys</u> *, AUD, VULN, IDS, SYS, STG, ...		
F3=Exit F12=Cancel		

## How to Get There

In the [Work with Rules panel](#), choose **3** for an existing rule.

# Copy Rule Condition panel

The Copy Rule Condition panel allows you to copy a Rule.

The fields and options are the same as those of the [Create Rule Condition panel](#).

PSA4811

Powertech SIEM Agent

15:19:31

Copy Rule Condition

Event Source . . . . .

AUDIT (IBM i Security Audit Journal)

Event Description . . . . .

TPW (Passwords used that are not valid)

Event Subtype . . . . .

P (Password not valid.)

Rule . . . . .

1 (User is GDORN)

Sequence . . . . .

1=9999

Link . . . . .

OR

AND, OR

Field . . . . .

PWUSRN

F4 for list

Operator . . . . .

=

=, <>, >, <, >=, <=

Criteria . . . . .

GDORN

F3=Exit

F4=Prompt

F5=Refresh

F12=Cancel

## How to Get There

In the [Work with Rule Conditions panel](#), choose **3** for a Condition.

# Create Event Description panel

The Create Event Description panel allows you to create an Event Field.

PSA4211		Powertech SIEM Agent	11:06:42
Event Description . . . . : AB (Authority Broker)			
Name . . . . .	: _ _ _	Journal Code and Entry Type	
Description . . . . .	: _ _ _		
Active . . . . .	: 0	1=Yes, 0=No	
Event Class ID . . . . .	: _ _ _ _ _	*NAME, character value	
Severity . . . . .	: _	4=Warning, 5=Notice, 6=Info, ...	
Class . . . . .	: _ _ _ _ _	AUD, VULN, IDS, SYS, STG, ...	
F3=Exit    F5=Refresh    F12=Cancel			

## How to Get There

Press **F6** in the [Work with Event Descriptions panel](#).

## Field Descriptions

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

### Name

The name you use to refer to this Event Description within Powertech SIEM Agent. For events that originate in a journal, this name must be comprised of the Journal Code and Entry Type of the journal entry. For message queue events, this name must be a message ID.

### Description

A short description you assign to the Event Description.

## Active

Indicates whether the Event Description is available for processing. When an Event Description is not active, the event it identifies will not be processed. 1=Active, 0=Inactive.

## Event Class ID

Event Class ID is simply placed into the syslog output event when using the Legacy Interact 3 Syslog format. Interact 3 formatted this data as a message ID, but you are free to specify whatever data is meaningful to you.

Specify \*NAME to display the Event Description's Name in the output. For journals, this is the Journal Code and Entry Type (for example, TCD). For message queues, \*NAME displays the Message ID (for example, CPF0907).

## Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

- 0=Emergency  
System is unusable; A panic condition.
- 1=Alert  
Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.
- 2=Critical  
Critical conditions; Hard device errors.
- 3=Error  
Error conditions
- 4=Warning  
Warning conditions
- 5=Notice  
Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.
- 6=Informational  
Informational messages
- 7=Debug  
Debug-level messages; Messages that contain information normally of use only when debugging a program.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

AUD - Audit event  
POL - Policy event  
VULN - Vulnerability event  
FW - Firewall event  
IDS - Intrusion detected event  
SYS - System event  
STG - Storage event

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

# Create Event Source panel

The Create Event Source panel allows you to provide the properties for a new Event Source.

For information on defining Event Sources, see [Configuring Event Sources](#).

PSA4111	Powertech SIEM Agent	16:41:42
Create Event Source		
-		
Name . . . . .	:	_____
Description . . . . .	:	_____
Type . . . . .	:	*AUDIT, *SYSMSG, *JRN, *MSGQ, ...
Facility . . . . .	:	1=User-level, 4=Security, ...
Active . . . . .	:	0
Default Output . . . . .	:	*NONE
F3=Exit    F5=Refresh    F8=Maintain Outputs    F12=Cancel		

## How to Get There

Enter **F6** for an entry in the [Work with Event Sources panel](#).

## Field Descriptions

### Name

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

### Description

A short description you assign to the Event Source.

## Type

The type of object from which IBM i events will be extracted. Journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue).

### \*AUDIT

Defines the IBM Security Audit Journal, QAUDJRN, to be monitored. This type includes some canned definitions of the journal codes and entry types for the security-related journal entries.

### \*SYSMSG

Defines the IBM System Messages in QSYSOPR or QSYSMSG to be monitored. This type includes some canned definitions of some interesting system management messages.

### \*EPM

Defines the Powertech Exit Point Manager Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Exit Point Manager entries.

### \*AB

Defines the Powertech Authority Broker Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Authority Broker.

### \*CMDSEC

Defines the Powertech Command Security Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Command Security.

### \*MSGQ

Defines a user-defined message queue to be monitored. You define the messages you would like monitored.

### \*JRN

Defines a user-defined journal to be monitored. You define the journal codes and entry types you would like monitored.

## Facility

Indicates the "facility", as defined by the Common Event Format specification. This value is used in the syslog output event. The allowed values are:

Value	Meaning
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons

Value	Meaning
4	Security/authentication messages
5	Messages generated internally by syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authentication messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Scheduling daemon
16	Locally used facilities (local0 through local7)

## Active

Indicates whether the Event Source is available for processing. When an Event Source is not active, it will not be monitored.

## Object

The name of object from which IBM i events will be extracted.

This name is required to be a [valid OS name](#).

## Library

The library in which the Event Source object is located.

This name is required to be a [valid OS name](#).

## ASP Group

The name of the ASP Group in which the library containing the object resides.

This name is required to be a [valid OS name](#).

## Default Output

Indicates that there is, or is not, a set of Outputs attached to the Event Source that act as Default Outputs.

Names the default Output(s) to which syslog events will be sent for this Event Source. These Outputs will be used when a Rule specifies \*SOURCE for a target Output.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

# Create Event Subtype panel

The Change Event Subtype panel allows you to modify the properties of an existing Event Subtype.

PSA4511	Powertech SIEM Agent	14:17:02
Create Event Subtype		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TAD (A change was made to the auditing attribute)		
Field . . . . . : ADETYP (Type of entry)		
Name (1 char) . . . . . : <u>D</u>		
Description . . . . . : <u>CHGDLOAUD command</u>		
Active . . . . .	: <u>1</u>	1=Yes, 0=No
Event Class ID . . . . .	: <u>TAD0004</u>	*, *NAME, character value
Severity . . . . .	: <u>5</u>	*, 4=Warning, 5=Notice, ...
Class . . . . .	: <u>AUD</u>	*, AUD, VULN, IDS, SYS, STG, ...
Add Extension . . . . .	: None	F13=Extensions
Override Event text . . . .	: None	F14=Event Text
F3=Exit    F5=Refresh    F12=Cancel    F13=Extensions    F14=Event Text		

## How to Get There

Press **F6** in the [Work with Event Subtypes panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Name

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Field

Event Field names the definition of the field whose content determines the Event Subtype at the time an event is intercepted.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

## Name

The name you use to refer to this Event Subtype within Powertech SIEM Agent. The name must match exactly whatever data the "subtype field" can contain in the actual event data at execution time.

## Description

A short description you assign to the Event Subtype.

## Active

Indicates whether the Event Subtype is available for processing. When an Event Subtype is not active, the event it identifies will not be processed.

## Event Class ID

Event Class ID is simply placed into the syslog output event when using the Legacy Interact 3 Syslog format. Interact 3 formatted this data as a message ID, but you are free to specify whatever data is meaningful to you.

Specify \*NAME to display the Event Description's Name followed by the Subtype, separated by a colon. For example, `TCD:A`.

You can specify a single asterisk (\*) to inherit the value from the parent Event Description at run time.

## Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

0=Emergency  
System is unusable; A panic condition.

- 1=Alert  
Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.
- 2=Critical  
Critical conditions; Hard device errors.
- 3=Error  
Error conditions
- 4=Warning  
Warning conditions
- 5=Notice  
Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.
- 6=Informational  
Informational messages
- 7=Debug  
Debug-level messages; Messages that contain information normally of use only when debugging a program.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

- AUD - Audit event
- POL - Policy event
- VULN - Vulnerability event
- FW - Firewall event
- IDS - Intrusion detected event
- SYS - System event
- STG - Storage event

## Add Extension

This field indicates whether additional Extensions should be attached beyond those specified for the Event Description (see [Change Event Description panel](#)).

An extension is simply a user-specified "name=value" string appended to a syslog event.

## Override Event Text

Allows access to the Event Text override for the Event Subtype. Event Text dictates how to format the event data into a human-readable format. Fields defined for the Event Description can be used to provide data for the text at run time. If this field is left undefined, the default Event Text (from the Event Description) will be shown. See [Change Event Description panel](#).

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

### F13=Extensions

Work with any Extensions that may be attached. After typing data and pressing Enter, this option appears.

### F14=Event Text

Work with an Event Text that may be attached. After typing data and pressing Enter, this option appears.

# Create Extension panel

The Create Extension panel allows you to provide the properties for a new Extension.

See [Extensions](#) and [Configuring Events and Event Sources](#).

PSA4C11	Powertech SIEM Agent Create Extension	16:27:44
Event Source . . . . .	: AUDIT (IBM i Security Audit Journal)	
Event Description . . . . .	: TCP (Create, change, restore user profiles)	
Event Subtype . . . . .	: None	
Rule . . . . .	: None	
Name . . . . .	:	
Value . . . . .	:	
JSON Data Type Override : _	blank, C=Character, N=Numeric	
F3=Exit F5=Refresh F8=Insert field at cursor		
F9=Insert extension at cursor F12=Cancel		

## How to Get There

Press **F6** on the [Work with Extensions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

This field indicates the Event Source to which the Event Description belongs.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Subtype

Indicates the Event Subtype to which the listed Extensions pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Rule

Indicates the Rule to which the listed Extensions pertain.

## Name

The name used on the left side of the equal sign in an extension.

## Value

The value used on the right side of the equal sign in an extension. Options for the values are journal header fields, journal entry specific fields, message queue header fields, message queue variables, other extensions and functions.

**NOTE:** The value of message variables (message fields) can be used in Extensions. See [Including message variables](#).

## JSON Data Type Override

This field allows JSON to treat the outcome of a value as character or numeric versus its original field data type.

Possible values are:

**Blank** will leave the default outcome of the value.

**C=Character** will insert double quotation marks around the value.

**N=Numeric** will provide the numeric value without quotation marks.

## Journal header fields

Journal header fields are common to all journal entries and start with an asterisk, for example \*JOBNAME. A complete list can be accessed via "F8=Insert field at cursor" and then

"F8=Common Fields". Common field must be delimited by an & when placed in the value field, &\*JOBNAM&.

## Journal entry specific fields

Journal entry specific fields are common to an event description and any subtypes. For example a TCO event description and its subtypes N and R have access to the same set of variables. Examples COONAM and COOLIB. Entry specific fields must be delimited by an & when placed in the value field, &COONAM&.

## Message queue header fields

Message queue header fields are common to all message queue entries and start with an asterisk, for example \*CURUSR. Message queue header fields must be delimited by an & when placed in the value field, &\*CURUSR&.

## Message queue variables

Message queue variables (message fields) can be used in Extensions. For example, if a CPF1234 message is sent, and includes a message variable, the value of that message variable can be included in an Extension.

To do this, specify the field on the Value line of the Create Extension panel as follows:

*&number of message field*

Example for message field #1:

&1

## Functions

Available functions:

%extract, %int, %substr, %subst, %sst, %len, %length, %ltrim, %triml, %rtrim, %trimr and %trim

Function names are not case sensitive. Character fields must be enclosed in single quotes.

**NOTE:** %extract function is:

- Not currently available for \*TIMESTAMP in Event Source type of \*SYSMSG.
- Available on IBM i 7.3 with TR5, IBM i 7.4 and higher.

**EXAMPLE:**

- %trimr(%substr('&CAUNAM&',1,5))
- %extract(EPOCH from '&\*TIMESTAMP&')

## Extensions

An extension may reference another extension. This is useful when building output for the JSON format. To specify an extension the extension name must be delimited by { and }.

**EXAMPLE:**

```
{myExtension}
```

In the output, extensions appear sorted by level first, then alphabetically by the name of the extension.

**EXAMPLE:** If you have extensions on Entry Type TPW, and some more on entry Subtype P, and then on a Rule:

```
TPW: a=&FLD1&, b=&FLD2&, c=&FLD3&
P: a=&FLDX&, b=&FLDY&
Rule A: a=&FLDn&
```

They appear in the output as: a=1 b=2 c=3 a=X b=Y a=n

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F8=Insert a field at cursor

Allows you to select and insert a Field reference at the cursor position. Existing text will be moved right to make room for the Field reference.

F12=Cancel

Discards changes and returns to the prior panel.

# Create Field panel

The Create Field panel allows you to create an Event Field.

PSA4311	Powertech SIEM Agent	13:47:56
Create Field		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TAD (A change was made to the auditing attribute)		
Name . . . . . : _____		
Description . . . . . : _____		
Subtype . . . . . : _	1=Yes, 0=No	
Offset . . . . . : _____	0-32659	
Length . . . . . : _____	1-32660	
Data Type . . . . . : _	A=Character, I=Integer, S=Signed,	
CCSID . . . . . : _____	0-65535	
Field Substitution . . . . :	F13=Substitutions	
F3=Exit    F5=Refresh    F12=Cancel		

## How to Get There

Press **F6** in the [Work with Fields panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Name

The name used to identify an Event Field within an Event Description.

## Description

A short description assigned to the Event Field.

## Subtype

Indicates if an Event Field is defined as a Subtype or not.

## Offset

Indicates the distance from the beginning of the journal entry or message data. The first byte within the entry-specific data is offset zero.

## Length

The number of bytes associated with a specific Event Field.

## Data Type

Indicates the type of data the Event Field contains. The possible values are:

Value	Meaning
A	Character
D	Zoned
I	Integer
L	Date
P	Packed
T	Time
U	Unsigned
V	Varying
Z	Timestamp

## CCSID

Indicates the coded character set identifier (CCSID) associated with the Event Field.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

# Create Field Substitutions panel

The Create Field Substitution panel allows you to provide the properties for a new Field Substitution.

PSA4411

Powertech SIEM Agent

15:07:27

Create Field Substitution

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)

Event Description . . . : TAD (A change was made to the auditing attribute)

Field . . . . . : ADETYP (Type of entry)

Default . . . . . : ☐

1=Yes, 0=No

From value . . . . . :

To value . . . . . :

F3=Exit

F5=Refresh

F12=Cancel

## How to Get There

Press **F6** in the [Work with Field Substitutions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Field

Field names the definition of the field whose content determines the Event Subtype at the time an event is intercepted.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

## Default

Indicates that this substitution is to be used if no other applies.

## From value

The field value to be translated.

## To value

The new value of the field.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

# Create Format panel

The Create Format panel allows you to create a Format.

See also [Configuring Formats](#).

PSA4A11	Powertech SIEM Agent Create Format	10:00:29
Name . . . . . : MYFORMAT		
Description . . . . . : myformat		
Message Style . . . . . : *SYSLOG      *MODERN, *CEF, *SYSLOG, *LEEF, *JSON		
Header specification . . . . . :      RFC5424 (Modern), RFC3164 (Legacy)		
Use Header Format		
Compatibility . . . . . : Y      Y=Yes, N=No		
F3=Exit    F5=Refresh    F12=Cancel		

## How to Get There

Press **F6** on the [Work with Formats panel](#).

## Field Descriptions

### Name

The name you use to refer to this Format within Powertech SIEM Agent.

This name is required to be a [valid OS name](#).

### Description

A short description you assign to the Format.

## Message Style

Message style determines the order and format of the event data in the message section of the output syslog event. Styles are provided that mimic the Powertech Interact 3 output formats. The following styles are provided:

Style	Description
*CEF	<p>This legacy style mimics the output produced by Powertech Interact 3 when using Host role *CEF.</p> <p><b>EXAMPLE:</b>  Mar 15 14:47:02 DWSIEM73 CEF:0 Powertech SIEM  Agent 4.4 TOW0001 Changes to object ownership 6 src=10.60.33.177  dst=10.60.135.40 cat=AuditJournal cs1Label=eventType cs1=JRN  cs2Label=eventClass cs2=AUD cnt=1 fname=QUSRSYS/PSATSTUSR  fileType=*MSGQ suser=PSATSTUSR dproc=537013/QSECOFR/QPADEV0002  cs3Label=programName cs3=PSATESTPAS duser=QSECOFR  cs6Label=Sequence cs6=1579233 msg=The message queue  QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR  to user profile PSATSTUSR.</p>

This style constructs the output syslog event message section entirely from Extensions you provide for Event Descriptions, Event Subtypes and Rules.

\*MODER  
N

**EXAMPLE:**  
1 2021-03-15T14:59:06.100-6:00 DWSIEM73.HELPSYSTEMS.COM - -  
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to object  
ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was  
changed from user profile QSECOFR to user profile PSATSTUSR.

Style	Description
*LEEF	<p>The LEEF (Log Event Extended Format) style conforms to the LEEF 2.0 header format standards for IBM QRadar. SIEM Agent adds IBM i-specific name value pairs, which provide additional value for messages related to IBM i events.</p> <p><b>EXAMPLE:</b>  LEEF:2.0 HelpSystems SIEM Agent 4.4 TOW0001   cat=AUDIT devTime=2021-03-15T14:32:18.987-6:00 devTimeFormat=yyyy-MM-dd hh:mm:ss.SSS Z sev=4 src=10.60.33.177 dst=10.60.135.40 usrName=QSECOFR jobNumber=537013 jobUser=QSECOFR jobName=QPADEV0002 resource=DWSIEM73 domain=DWSIEM73.HELPSYSTEMS.COM pgmName=PSATESTPAS pgmLib=PSATEST journalReceiverLib=QSYS journalReceiverName=AUDRCV0057 journalID=AUDRCV0057 journalSeqNumber=1576885 reason=Changes to object ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR to user profile PSATSTUSR.</p>
	<p>This style (JavaScript Object Notation) is an open standard file format.</p>
*JSON	<p><b>EXAMPLE:</b>  {"FullyQualifiedJob":  {"JobName":"QPADEV0002","JobNumber":"537013","JobUser":"QSECOFR"},  "CurrentUser":"QSECOFR","EventID":"TOW0001","EventText":"User profile &amp;CPONAM&amp; was created."}</p>
*SYSLOG	<p>This legacy style mimics the output produced by Powertech Interact 3 when using Host role *SYSLOG.</p> <p><b>EXAMPLE:</b>  1 2021-03-15T14:53:10.175-6:00 DWSIEM73.HELPSYSTEMS.COM - -  Changes to object ownership src=10.60.135.40 dst=10.60.33.177  msg=TYPE:JRN CLS:AUD JJOB:QPADEV0002 JUSER:QSECOFR  JNBR:537013 PGM:PSATESTPAS DETAIL:A PSATSTUSR QUSRSYS *MSGQ  QSECOFR PSATSTUSR 0 0 * * MSG: The message queue  QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR  to user profile PSATSTUSR.</p>

## Header specification

The specification compliance level of the syslog header.

### RFC3164

The syslog event will conform to the legacy RFC 3164 specification.

### RFC5424

The syslog event will conform to the modern RFC 5424 specification.

**LEEF**

The LEEF (Log Event Extended Format) format conforms to the LEEF 2.0 header format standards for IBM QRadar. SIEM Agent adds IBM i-specific name value pairs, which provide additional value for messages related to IBM i events.

**\*NONE**

No header included in the event output. This is the default value for \*JSON Formats.

For more details, see [Syslog Header Specifications](#).

**EXAMPLE:****Header specification: RFC3164 (Legacy)**

```
<38>Mar 15 15:28:06 DWSIEM73 TOW0001 src=10.60.33.177
dst=10.60.135.40 reason=Changes to object ownership msg=The
message queue QUSRSYS/PSATSTUSR ownership was changed from user
profile QSECOFR to user profile PSATSTUSR.
```

**Header specification: RFC5424 (Modern)**

```
<38>1 2021-03-15T15:28:06-6:00 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

## User Header Format Compatibility

The User Header Format Compatibility flag, if set to **Y**, outputs the header in the format that was used by SIEM Agent/Interact prior to version 4.2 of SIEM Agent. This setting may be preferred when the SYSLOG configuration is dependent on the format from the legacy product versions. A setting of **N** provides a more accurate representation of the syslog standard.

**EXAMPLE:****User Header Format Compatibility: N**

```
<38>1 2021-03-15T14:32:18.987-6:00 DWSIEM73.HELPSYSTEMS.COM - -
The message queue QUSRSYS/PSATSTUSR ownership was changed from
user profile QSECOFR to user profile PSATSTUSR. src=10.60.135.40
dst=10.60.33.177 msg=TYPE:JRN CLS:AUD JJOB:QPADEV0002
JUSER:QSECOFR JNBR:537013 PGM:PSATESTPAS DETAIL:A PSATSTUSR
QUSRSYS *MSGQ QSECOFR PSATSTUSR      0 0 * *
```

**User Header Format Compatibility: Y**

```
<38>1 2021-03-15T14:32:18.987-6:00 DWSIEM73.HELPSYSTEMS.COM - -
CEF:0|Powertech|SIEM Agent|4.4|TOW0001|The message queue
QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR
to user profile PSATSTUSR.|6| src=10.60.135.40 dst=10.60.33.177
msg=TYPE:JRN CLS:AUD JJOB:QPADEV0002 JUSER:QSECOFR JNBR:537013
```

```
PGM:PSATESTPAS DETAIL:A PSATSTUSR QUSRSYS *MSGQ QSECOFR PSATSTUSR
0 0 * *
```

## Microseconds

Specifies the number of microsecond digits to be used in the formatted timestamp when using the Modern header specification. The Legacy header specification (RFC3164) does not support microseconds. You can specify *\*NONE* (zero digits), or 3 or 6 microsecond digits. Within the LEEF Format, Microseconds are fixed to a value of 3.

### EXAMPLE:

#### Microseconds: *\*NONE*:

```
<38>1 2021-03-25T07:16:32-6:00 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

#### Microseconds: *3*:

```
<38>1 2021-03-25T07:16:32.400-6:00 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

#### Microseconds: *6*:

```
<38>1 2021-03-15T07:16:32.100080-6:00 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

## Time zone

Specifies the time zone indication to be applied to the syslog event timestamp when using the Modern header specification. The Legacy header specification (RFC3164) displays only a simplistic month and day without a year, and offers no formatting options for the timestamp. Within the LEEF Format, Time zone is fixed to *\*UTC*.

#### *\*NONE*

The timestamp is formatted as a local time with no time zone indication is provided.

#### *\*UTC*

The timestamp is formatted as a local time with the Universal Coordinated Time (UTC) offset appended.

#### *\*ZULU*

The timestamp is formatted as Universal Coordinated Time with a "Z" appended.

**EXAMPLE:****Time Zone: \*NONE:**

```
<38>1 2021-03-25T15:25:41.334 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

**Time Zone: \*UTC:**

```
<38>1 2021-03-15T15:25:41.334-6:00 DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

**Time Zone: \*ZULU:**

```
<38>1 2021-03-15T15:25:41.334Z DWSIEM73.HELPSYSTEMS.COM - -
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to
object ownership msg=The message queue QUSRSYS/PSATSTUSR
ownership was changed from user profile QSECOFR to user profile
PSATSTUSR.
```

Let's use Elton John's birthday as an example. Elton was born March 25, 1947 at 2:00:00am in Pinner, Middlesex, England. In Minneapolis (Central Standard Time), the local time would be March 24, 1947 at 8:00:00pm (UTC-06:00). One of the following results can be achieved (without microseconds).

time zone	Formatted output
*NONE	1947-03-24T20:00:00
*UTC	1947-03-24T20:00:00-06:00
*ZULU	1947-03-25T02:00:00Z

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

# Create Output panel

The Create Output Target panel allows you to create an Output Target.

For information on configuring an output, see [Configuring Outputs](#).

PSA4B11Powertech SIEM Agent10:13:21

Create Output

Name . . . . . :

Description . . . . . :

Active . . . . . : 1=Yes, 0=No

Format . . . . . : F4 for list

Type . . . . . : \*NETWORK, \*MSGQ, \*STREAM

Location . . . . . :

Port . . . . . : 1-65535

Protocol . . . . . : \*TCP, \*UDP, \*TLS

Recovery limit . . . . . :

Time interval . . . . . :

Special . . . . . : 1=Yes, 0=No

F3=Exit F4=Prompt F5=Refresh F12=Cancel

## How to Get There

On the [Select Output Target panel](#) or [Work with Outputs panel](#), press **F6**.

## Field Descriptions

### System

System indicates the target of any operations you perform. When you add items, for example, those items will be sent to, and will affect processing on, the System named.

### Name

The name you use to refer to this Output Target within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Description

A short description you assign to the Output Target.

## Active

Indicates whether the Output Target is available for processing. When the Output Target is not active, it will not have syslog events transmitted to it.

## Format

Names the Format that controls how the output event is constructed. See [Create Format](#) for more details.

## Type

The type of output location defined by the Output Target. The allowed values are:

Value	Meaning
*NETWORK	The output syslog events are sent to a network location, typically an IP address or registered DNS name. Several protocols are available for network locations.
*MSGQ	<p>The output syslog events are sent to a message queue on the local system. You must create the message queue.</p> <div> <p><b>NOTE:</b> When creating the message queue, set the MSGQFULL attribute to *WRAP in order for the system to accommodate wrapping the message queue when it becomes full. If MSGQFULL is not set to *WRAP, errors and job logs may result within SIEM Agent during message processing, due to the message queue becoming full. Also, consider the size of the message queue. Be sure it is able to store an adequate number of messages before wrapping and over-writing the oldest messages.</p> </div>
*STREAM	The output syslog events are sent to a stream file in the Integrated File System. The file will be created if it does not exist.
*KAFKA	The selected output events are sent to a Kafka server location, typically an IP address or registered DNS name. Generally, ports used for Kafka are 9092 or 9093. Several protocols are available for network locations.

## \*NETWORK

### Location

A network location specification. This could be an IP address, a DNS-defined name, or something completely different, as long as the name can be resolved by your network configuration.

### Port

A port at the target location.

### Protocol

Indicates the protocol used to communicate with the syslog server.

Specify one of the following values:

#### **\*UDP**

The User Datagram Protocol (UDP) is used to transmit syslog events.

#### **\*TCP**

The Transmission Control Protocol (TCP) is used to transmit syslog events.

#### **\*TLS**

The Transmission Control Protocol (TCP) is used with Transport Layer Security (TLS) technology to transmit syslog events.

### Recovery limit

After having failed to communicate, this specifies the number of times to retry the connection to the network location before giving up.

### Time interval

After having failed to communicate, this specifies the number of seconds between attempts to re-connect to the network location.

### ArcSight compatibility

Indicates whether output syslog events are to be formatted specially for the ArcSight syslog event manager server. Specify 1 to indicate that the Output targets an ArcSight server;

specify 0 otherwise. Note the effect of this setting in the following output example: the dst and src attributes are swapped.

**EXAMPLE:**

**ArcSight compatibility: N:**

```
1 2021-03-15T21:28:06.100Z DWSIEM73.HELPSYSTEMS.COM - - TOW0001
src=10.60.33.177 dst=10.60.135.40 reason=Changes to object
ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was
changed from user profile QSECOFR to user profile PSATSTUSR.
```

**ArcSight compatibility: Y:**

```
1 2021-03-15T21:47:06.684Z DWSIEM73.HELPSYSTEMS.COM - - TOW0001
dst=10.60.33.177 src=10.60.135.40 reason=Changes to object
ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was
changed from user profile QSECOFR to user profile PSATSTUSR.
```

**\*MSGQ**

## Message queue; Library

Syslog output will be written to this message queue in the form of messages. The syslog event is provided in the message second-level text.

## ASP Group

The name of the ASP group on which the message queue can be found.

**\*STREAM**

## CCSID for stream file

The CCSID of the text data written to the stream file.

## Line ends

The line endings that will terminate each syslog event written to the stream file. The following values are supported:

Value	Meaning
*CR	A carriage return character will terminate each line.

Value	Meaning
*LF	A line feed character will terminate each line.
*CRLF	A carriage return and line feed character will terminate each line.

## Path

Path names the stream file to which each syslog event will be written. Each event will be written as a "line", terminated by the line end specified by the Line ends property.

When creating the path, begin with / and end with the log file name. You must include the log file name or no log will be created. Full access rights must be given to the user profile PTUSER.

In the following example the log file name is SIEM4LOG.

The complete path and log name might look like `/home/SIEM4log`

Name . . . . .	: <u>IFSSIEMLOG</u>	
Description . . . . .	: <u>IFS log /home/SIEM4LOG</u>	
Active . . . . .	: <u>1</u>	1=Yes, 0=No
Format . . . . .	: <u>SYSLOG</u>	F4 for list
Type . . . . .	: <u>*STREAM</u>	*NETWORK, *MSGQ, *STREAM
CCSID for stream file . . . . .	: <u>*UTF16</u>	*UTF8, *UTF16, 1 - 65535
Line ends . . . . .	: <u>*CRLF</u>	*CR, *LF, *CRLF
Path . . . . .	: <u>/home/SIEM4LOG</u>	

## \*KAFKA

### Kafka Location

A Kafka server location specification. This could be an IP address, a DNS name, or other name so long as it can be resolved by your network configuration.

### Kafka Port

A port at the target location.

### Kafka Protocol

Indicates the protocol used to communicate with the Kafka server.

Specify one of the following values:

**\*TCP**

The Transmission Control Protocol (TCP) is used to transmit syslog events.

**\*TLS**

The Transmission Control Protocol (TCP) is used with Transport Layer Security (TLS) technology to transmit syslog events.

## Kafka Topic

A Kafka topic must be entered. This should be a topic that has already been configured on the Kafka server configuration.

## Kafka Truststore

A Kafka truststore path must be entered that points to the location of the truststore file used in TLS protocol with the Kafka server. A truststore must be created on the Kafka server and the security certificate must be imported into the truststore and then stored on the IFS for successful TLS communication.

## Kafka Truststore Password

A Kafka truststore password must be entered for the truststore file used in TLS protocol with the Kafka server.

## Encrypt Password

A Kafka truststore password can be encrypted using a Y in this field. N will not encrypt the field. Valid values are Y or N.

**NOTE:** Changing the value from a Y to N, requires the entry of the password.

## Kafka Jar Path

A Kafka jar path must be entered that points to the location of the jar file used to communicate with the Kafka server. During the installation process, kafka-clients-2.5.0.jar and slf4j-api-1.7.30.jar are loaded into the Powertech/SIEMAgent directory. These jar files are needed to communicate with the IBM i systems.

## Kafka KeyStore

A Kafka keystore path must be entered that points to the location of the keystore file used in TLS protocol with the Kafka server. A keystore must be created on the Kafka server and the security certificate must be imported into the keystore and then stored on the IFS for successful TLS communication.

## Kafka KeyStore Password

A Kafka keystore password must be entered for the keystore file used in TLS protocol with the Kafka server.

## Encrypt Password

A Kafka keystore password can be encrypted using a Y in this field. N will not encrypt the field.

**NOTE:** Changing the value from a Y to N, requires the entry of the password.

## Kafka Key Password

A Kafka key password must be entered for the key file used in TLS protocol with the Kafka server.

## Encrypt Password

A Kafka key password can be encrypted using a Y in this field. N will not encrypt the field.

**NOTE:** Changing the value from a Y to N, requires the entry of the password.

## Command Keys

F3=Exit

Exit the program.

#### F4=Prompt

Displays a list of items from which one or more may be selected.

#### F5=Refresh

Discards changes and remains on this panel.

#### F12=Cancel

Discards changes and returns to the prior panel.

# Create Rule panel

The Create Rule panel allows you to provide the properties for a new Rule.

PSA4711	Powertech SIEM Agent	14:29:22
Create Rule		
Event Source . . . . .	AUDIT (IBM i Security Audit Journal)	
Event Description . . . . .	AJB (All authority failures)	
Event Subtype . . . . .	None	
Rule sequence . . . . .	<u>10</u>	1-9999
Description . . . . .	<u>Snd message to Security Team</u>	
Active . . . . .	<u>0</u>	1=Yes, 0=No
Stop evaluation . . . . .	<u>0</u>	1=Yes, 0=No
Event Class ID . . . . .	<u>*</u>	*, *NAME, character value
Severity . . . . .	<u>*</u>	*, 4=Warning, 5=Notice, ...
Class . . . . .	<u>*</u>	*, AUD, VULN, IDS, SYS, STG, ...
Rule Output . . . . .	<u>*</u>	*, None, F8=Maintain Outputs
Add Extension . . . . .	None	F13=Extensions
Override Event text . . . . .	None	F14=Event Text
F3=Exit F5=Refresh F8=Maintain Outputs F12=Cancel		
F13=Extensions F14=Event Text		

## How to Get There

Press **F6** in the [Work with Rules panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Subtype

Indicates the Event Subtype to which the listed Rules pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Sequence

Sequence is a unique number used to determine the order in which rules are evaluated.

## Description

A short description you assign to the Rule.

## Active

Indicates whether the Rule is available for processing. When a Rule is not active its values will not be used in determining contents sent to the SYSLOG server.

## Stop evaluation

Stop evaluation determines whether to end rule processing after a rule whose conditions are all satisfied.

## Event Class ID

Event Class ID is simply placed into the syslog output event when using the Legacy Interact 3 Syslog format. Interact 3 formatted this data as a message ID, but you are free to specify whatever data is meaningful to you.

**Journal Events:** Specify \*NAME to display the Event Description's Name in the output. For journals, this is the Journal Code and Entry Type (for example, TCD).

**Message Queue Events:** For message queues, \*NAME displays the Message ID (for example, CPF0907).

Journal Event Subtypes: Specify \*NAME to display the Event Description's Name followed by the Subtype, separated by a colon. For example, TCD:A.

You can specify a single asterisk (\*) to inherit the value from the parent Event Description or Event Subtype at run time.

## Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

- 0=Emergency  
System is unusable; A panic condition.
- 1=Alert  
Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.
- 2=Critical  
Critical conditions; Hard device errors.
- 3=Error  
Error conditions
- 4=Warning  
Warning conditions
- 5=Notice  
Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.
- 6=Informational  
Informational messages
- 7=Debug  
Debug-level messages; Messages that contain information normally of use only when debugging a program.
- \*=Inherit  
You can specify a single asterisk (\*) to inherit the value from the parent Event Description or Event Subtype at run time.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

- AUD - Audit event
- POL - Policy event
- VULN - Vulnerability event
- FW - Firewall event
- IDS - Intrusion detected event
- SYS - System event
- STG - Storage event

You can specify a single asterisk (\*) to inherit the value from the parent Event Description or Subtype at run time.

## Rule Output

Indicates whether any Outputs are attached to the Rule. See [Work with Outputs](#).

## Add Extension

This field indicates whether additional Extensions should be attached beyond those specified for the Event Description (see [Change Event Description panel](#)).

An extension is simply a user-specified "name=value" string appended to a syslog event.

## Override Event Text

Allows access to the Event Text override for the Event Subtype. Event Text dictates how to format the event data into a human-readable format. Fields defined for the Event Description can be used to provide data for the text at run time. If this field is left undefined, the default Event Text (from the Event Description) will be shown. See [Change Event Description panel](#).

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F8=Display Outputs

Opens the [Work with Attached Outputs panel](#), where you can attach an output to the Event Source.

### F12=Cancel

Discards changes and returns to the prior panel.

## F13=Extensions

Work with any Extensions that may be attached. After typing data and pressing Enter, this option appears.

## F14=Event Text

Work with an Event Text that may be attached. After typing data and pressing Enter, this option appears.

# Create Rule Condition panel

The Create Rule Condition panel allows you to add a Condition to a Rule.

PSA4811	Powertech SIEM Agent	09:17:15
Create Rule Condition		
Event Source . . . . .	AUDIT (IBM i Security Audit Journal)	
Event Description . . . . .	TAD (A change was made to the auditing attribute)	
Event Subtype . . . . .	None	
Rule . . . . .	1 (Rule)	
Sequence . . . . .	_____	1-9999
Link . . . . .	_____	AND, OR
Field . . . . .	_____	F4 for list
Operator . . . . .	_____	=, <>, >, <, >=, <=
Value . . . . .	_____	
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel		

## How to Get There

Press **F6** in the [Work with Rule Conditions panel](#).

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Subtype

Indicates the Event Subtype to which the listed Rules pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Rule

Indicates the Rule to which the Condition pertains.

## Sequence

Sequence is a unique number used to determine the order in which Conditions are evaluated.

## Link

The Link determines how a Condition relates to other Conditions for a Rule.

Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence. The Condition with the lowest sequence number is ignored.

## Field

Name of the Field to be evaluated at run time against the Criteria.

The valid values are dependent upon the Event Source as well as Event Description associated with the Rule.

## Operator

The logical operator used when comparing a field value to the Criteria.

## Value

The value to be compared against the field at run time. This value is case-sensitive.

## Command Keys

F3=Exit

Exit the program.

F12=Cancel

Discards changes and returns to the prior panel.

## Display Event Description panel

The Display Event Description panel displays Event Description properties but does not allow them to be changed.

The properties are described in the [Change Event Description panel](#).

PSA4211	Powertech SIEM Agent	14:33:18
Display Event Description		
Event Description . . . : AUDIT (IBM i Security Audit Journal)		
Name . . . . .	T AF	Journal Code and Entry Type
Description . . . . .	All authority failures	
Active . . . . .	1	1=Yes, 0=No
Event Class ID . . . . .	TAF	*NAME, character value
Severity . . . . .	6	4=Warning, 5=Notice, 6=Info, ...
Class . . . . .	AUD	AUD, VULN, IDS, SYS, STG, ...
Extension . . . . .	None	F13=Extensions
Event text . . . . .	Present	F14=Event Text
F3=Exit   F5=Refresh   F12=Cancel   F13=Extensions   F14=Event Text		

## How to Get There

Enter **5=Display** for an entry in the [Work with Event Descriptions panel](#).

# Display Event Source panel

The Display Event Source panel displays Event Source properties but does not allow them to be changed. The properties are described in the [Change Event Source panel](#).

PSA4111Powertech SIEM Agent14:39:10  

Display Event Source

Name . . . . . : AUDIT

Description . . . . . : IBM i Security Audit Journal

Type . . . . . : \*AUDIT\*AUDIT, \*SYSMMSG, \*JRN, \*MSGQ, ...

Facility . . . . . : 41=User-level, 4=Security, ...

Active . . . . . : 01=Yes, 0=No

Default Output . . . . . : \*NONEF8=Display Outputs

Journal

Object . . . . . : QAUDJRN

Library . . . . . : QSYS

ASP Group . . . . . : \*SYSBAS

F3=Exit   F5=Refresh   F8=Display Outputs   F12=Cancel

## How to Get There

Enter **5=Display** for an entry in the [Work with Event Sources panel](#).

# Display Event Subtype panel

The Display Event Subtype panel displays Event Subtype properties but does not allow them to be changed.

The properties are described in the [Change Event Subtype panel](#).

PSA4511	Powertech SIEM Agent	14:34:21
Display Event Subtype		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : AJB (All authority failures)		
Field . . . . . : AFVIOL (Violation type)		
Name (1 char) . . . . . : A		
Description . . . . . : Not authorized to object		
Active . . . . . : 1	1=Yes, 0=No	
Event Class ID . . . . . : TAF0001	*, *NAME, character value	
Severity . . . . . : 5	*, 4=Warning, 5=Notice, ...	
Class . . . . . : IDS	*, AUD, VULN, IDS, SYS, STG, ...	
Add Extension . . . . . : None	F13=Extensions	
Override Event text . . . : None	F14=Event Text	
F3=Exit   F5=Refresh   F12=Cancel   F13=Extensions   F14=Event Text		

## How to Get There

Enter **5=Display** for an entry in the [Work with Event Subtypes panel](#).

# Display Field panel

The Display Field panel displays Event Field properties but does not allow them to be changed.

The fields are the same as those of the [Change Field panel](#).

PSA4311

Powertech SIEM Agent

13:43:30

Display Field

Event Source . . . . .

AUDIT (IBM i Security Audit Journal)

Event Description . . . . .

TAD (A change was made to the auditing attribute)

Name . . . . .

ADE Typ

Description . . . . .

Type of entry

Subtype . . . . .

1

1=Yes, 0=No

Offset . . . . .

0

0-32659

Length . . . . .

1

1-32660

Data Type . . . . .

A

A=Character, I=Integer, S=Signed,

CCSID . . . . .

65535

0-65535

Field Substitution . . . . .

F13=Substitutions

F3=Exit

F5=Refresh

F12=Cancel

## How to Get There

Enter **5=Display** for an entry in the [Work with Fields panel](#).

## Display Field Substitutions panel

The Display Field Substitution panel displays Field Substitution properties but does not allow them to be changed.

The fields and options are the same as those of the [Change Field Substitution panel](#).

PSA4411	Powertech SIEM Agent	15:28:51
Display Field Substitution		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . : TAD (A change was made to the auditing attribute)		
Field . . . . . : ADETP (Type of entry)		
Default . . . . . : 0                      1=Yes, 0=No		
From value . . . . . : D		
To value . . . . . : CHGDLOAUD command		
F3=Exit    F5=Refresh    F12=Cancel		

### How to Get There

Enter **5=Display** for an entry in the [Work with Field Substitutions panel](#).

# Display Format panel

The Display Format panel displays Format properties but does not allow them to be changed.

PSA4A11	Powertech SIEM Agent	10:05:41
	Display Format	
Name . . . . . : SYSLOG		
Description . . . . . : Interact syslog format		
Message Style . . . . .	*SYSLOG	*MODERN, *CEF, *SYSLOG, *LEEF, *JSON
Header specification . . .	RFC3164	RFC5424 (Modern), RFC3164 (Legacy)
Use Header Format		
Compatibility . . . . .	N	Y=Yes, N=No
F3=Exit F12=Cancel		

## How to Get There

Press **5** for a format in the [Work with Formats panel](#).

## Field Descriptions

### Name

The name you use to refer to this Format within Powertech SIEM Agent.

This name is required to be a valid OS name.

### Description

A short description you assign to the Format.

## Message Style

Message style determines the order and format of the event data in the message section of the output syslog event. Styles are provided that mimic the Powertech Interact 3 output formats. The following styles are provided:

Style	Description
*CEF	<p>This legacy style mimics the output produced by Powertech Interact 3 when using Host role *CEF.</p> <p><b>EXAMPLE:</b>  Mar 15 14:47:02 DWSIEM73 CEF:0 Powertech SIEM  Agent 4.4 TOW0001 Changes to object ownership 6 src=10.60.33.177  dst=10.60.135.40 cat=AuditJournal cs1Label=eventType cs1=JRN  cs2Label=eventClass cs2=AUD cnt=1 fname=QUSRSYS/PSATSTUSR  fileType=*MSGQ suser=PSATSTUSR dproc=537013/QSECOFR/QPADEV0002  cs3Label=programName cs3=PSATESTPAS duser=QSECOFR  cs6Label=Sequence cs6=1579233 msg=The message queue  QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR  to user profile PSATSTUSR.</p>

This style constructs the output syslog event message section entirely from Extensions you provide for Event Descriptions, Event Subtypes and Rules.

\*MODER  
N

**EXAMPLE:**  
1 2021-03-15T14:59:06.100-6:00 DWSIEM73.HELPSYSTEMS.COM - -  
TOW0001 src=10.60.33.177 dst=10.60.135.40 reason=Changes to object  
ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was  
changed from user profile QSECOFR to user profile PSATSTUSR.

Style	Description
*LEEF	<p>The LEEF (Log Event Extended Format) style conforms to the LEEF 2.0 header format standards for IBM QRadar. SIEM Agent adds IBM i-specific name value pairs, which provide additional value for messages related to IBM i events.</p> <p><b>EXAMPLE:</b>  LEEF:2.0 HelpSystems SIEM Agent 4.4 TOW0001   cat=AUDIT devTime=2021-03-15T14:32:18.987-6:00 devTimeFormat=yyyy-MM-dd hh:mm:ss.SSS Z sev=4 src=10.60.33.177 dst=10.60.135.40 usrName=QSECOFR jobNumber=537013 jobUser=QSECOFR jobName=QPADEV0002 resource=DWSIEM73 domain=DWSIEM73.HELPSYSTEMS.COM pgmName=PSATESTPAS pgmLib=PSATEST journalReceiverLib=QSYS journalReceiverName=AUDRCV0057 journalID=AUDRCV0057 journalSeqNumber=1576885 reason=Changes to object ownership msg=The message queue QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR to user profile PSATSTUSR.</p>
	<p>This style (JavaScript Object Notation) is an open standard file format.</p>
*JSON	<p><b>EXAMPLE:</b>  {"FullyQualifiedJob": {"JobName": "QPADEV0002", "JobNumber": "537013", "JobUser": "QSECOFR"}, "CurrentUser": "QSECOFR", "EventID": "TOW0001", "EventText": "User profile &amp;CPONAM&amp; was created."}</p>
*SYSLOG	<p>This legacy style mimics the output produced by Powertech Interact 3 when using Host role *SYSLOG.</p> <p><b>EXAMPLE:</b>  1 2021-03-15T14:53:10.175-6:00 DWSIEM73.HELPSYSTEMS.COM - - Changes to object ownership src=10.60.135.40 dst=10.60.33.177 msg=TYPE:JRN CLS:AUD JJOB:QPADEV0002 JUSER:QSECOFR JNBR:537013 PGM:PSATESTPAS DETAIL:A PSATSTUSR QUSRSYS *MSGQ QSECOFR PSATSTUSR 0 0 * * MSG: The message queue QUSRSYS/PSATSTUSR ownership was changed from user profile QSECOFR to user profile PSATSTUSR.</p>

## Header specification

The specification compliance level of the syslog header.

### RFC3164

The syslog event will conform to the legacy RFC 3164 specification.

### RFC5424

The syslog event will conform to the modern RFC 5424 specification.

**\*NONE**

No header included in the event output. This is the default value for \*JSON Formats.

For more details, see [Syslog Header Specifications](#).

**Microseconds**

Specifies the number of microsecond digits to be used in the formatted timestamp when using the Modern Header specification. The Legacy header specification does not display microseconds. You may specify \*NONE (zero digits), or 3 or 6 microsecond digits. Within the LEEF Format, Microseconds are fixed to a value of 3.

**User Header Format Compatibility**

The User Header Format Compatibility flag, if set to **Y**, outputs the header in the format that was used by SIEM Agent/Interact prior to version 4.2 of SIEM Agent. This setting may be preferred when the SYSLOG configuration is dependent on the format from the legacy product versions. A setting of **N** provides a more accurate representation of the syslog standard.

**Time zone**

Specifies the time zone indication to be applied to the syslog event timestamp when using the Modern header specification. The Legacy header specification only displays a very simplistic month and day without a year and offers no formatting options for the timestamp. Within the LEEF Format, Time zone is fixed to \*UTC.

**\*NONE**

The timestamp is formatted as a local time with no time zone indication is provided.

**\*UTC**

The timestamp is formatted as a local time with the Universal Coordinated Time (UTC) offset appended.

**\*ZULU**

The timestamp is formatted as Universal Coordinated Time with a "Z" appended.

**EXAMPLE:** Elton John was born on March 25, 1947 at 2:00:00am UTC (Coordinated Universal Time) in Pinner, Middlesex, England. In Minneapolis, MN, USA (Central Standard Time), the local date and time was March 24, 1947 at 8:00:00pm (UTC-06:00). The following time information will be output depending on the time zone setting:

time zone	Formatted output
*NONE	1947-03-24T20:00:00
*UTC	1947-03-24T20:00:00-06:00

time zone	Formatted output
*ZULU	1947-03-25T02:00:00Z

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

# Display Output panel

The Display Output panel displays Output properties but does not allow them to be changed.

PSA4B11	Powertech SIEM Agent	12:00:03
Display Output		
Name . . . . . : ABSJRNSTMF		
Description . . . . . : Authority Broker Journal Stream File Output		
Active . . . . . : 1                      1=Yes, 0=No		
Format . . . . . : MODERN              F4 for list		
Type . . . . . : *STREAM              *NETWORK, *MSGQ, *STREAM		
CCSID for stream file . . : *UTF8              *UTF8, *UTF16, 1 - 65535		
Line ends . . . . . : *CRLF              *CR, *LF, *CRLF		
Path . . . . . : /home/sid/siem4/abjrnstmf.log		
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel		

## How to Get There

Press 5 for an output in the [Work with Outputs panel](#).

# Display Rule panel

The Display Rule panel displays Rule properties but does not allow them to be changed.

The fields are the same as those of the [Create Rule panel](#).

PSA4711	Powertech SIEM Agent	14:37:57
Display Rule		
Event Source . . . . .	AUDIT (IBM i Security Audit Journal)	
Event Description . . . . .	AJB (All authority failures)	
Event Subtype . . . . .	None	
Rule sequence . . . . .	10	1-9999
Description . . . . .	Snd message to Security Team	
Active . . . . .	0	1=Yes, 0=No
Stop evaluation . . . . .	0	1=Yes, 0=No
Event Class ID . . . . .	*	*, *NAME, character value
Severity . . . . .	*	*, 4=Warning, 5=Notice, ...
Class . . . . .	*	*, AUD, VULN, IDS, SYS, STG, ...
Rule Output . . . . .	*	*, None, F8=Display Outputs
Add Extension . . . . .	None	F13=Extensions
Override Event text . . . . .	None	F14=Event Text
F3=Exit F5=Refresh F8=Display Outputs F12=Cancel		
F13=Extensions F14=Event Text		

## How to Get There

Enter **5=Display** for an entry in the [Work with Rules panel](#).

## Display Rule Condition panel

The Display Rule Condition panel displays Condition properties but does not allow them to be changed.

The fields are the same as those of the [Create Rule Condition panel](#).

PSA4811	Powertech SIEM Agent	09:32:26
Display Rule Condition		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TPW (Passwords used that are not valid)		
Event Subtype . . . . . : None		
Rule . . . . . : 1 (Include more Extensions if user = admin)		
Sequence . . . . . : 1	1-9999	
Link . . . . . : OR	AND, OR	
Field . . . . . : PWLLOC	F4 for list	
Operator . . . . . : =	=, <>, >, <, >=, <=	
Value . . . . . : LOCAL		
F3=Exit F12=Cancel		

## How to Get There

In the [Work with Rule Conditions panel](#), choose 5 for a Condition.

## End Monitor command (PSAENDMON)

The End Monitor (PSAENDMON) command submits a request to end one or more of the SIEM Agent monitor jobs.

Restrictions:

Monitor (MONITOR)

Specify \*ALL to end all monitors, or indicate which monitor you would like to end by specifying one of the following values:

- \*ALL  
Ends all monitor jobs.
- \*EVENT  
End only the event monitor job.
- \*SIEM  
End only the SIEM Agent Event Source Monitors.

### Command Keys

F3=Exit

Exit the program.

F4=Prompt

Displays a list of items from which one or more may be selected.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

F24=More keys

Shows more Command Keys.

## Hold SIEM Monitor command (PSAHLDMON)

The Hold SIEM Monitor (PSAHLDMON) command causes the monitor for one Event Source or Output Target to cease operation.

Restrictions:

Event Source name (SOURCE)

Monitor type (TYPE)

Specify the type of monitor whose name you entered for the MONITOR\ parameter.  
The valid types are \*SOURCE for an Event Source, or \*OUTPUT for an Output Target.

### Command Keys

F3=Exit

Exit the program.

F4=Prompt

Displays a list of items from which one or more may be selected.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

F24=More keys

Shows more Command Keys.

# SIEM Agent Main Menu

The Powertech SIEM Agent Main Menu offers a launchpad for maintaining and reporting on SIEM Agent configuration.

PSA4000 R04M041210305	Powertech SIEM Agent Main Menu	09:57:23  ALERTS
--------------------------	-----------------------------------	------------------------

Select one of the following:

1. Work with Event Sources
2. Work with Formats
3. Work with Outputs

10. Commit configuration changes

82. Work with Utilities

Selection or command  
==> \_\_\_\_\_

---

F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve  
F13=Information Assistant   F16=System Main Menu   F21=Alerts   F22=Status

## Options

### 1. Work with Event Sources

The Work with Event Sources panel allows you to define and work with Event Sources.

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources. See [Work with Event Sources](#).

### 2. Work with Formats

The Work with Formats panel allows you to manage Formats.

A Format is an entity attached to an Output that provides various options used in determining how SIEM events are specifically formatted. See [Work with Formats](#).

### 3. Work with Outputs

The Work with Outputs panel allows you to manage Output targets.

Output target defines a location to which formatted SIEM events are sent. Each Output target can specify a different output format. See [Work with Outputs](#).

### 10. Commit configuration changes

When a database setting has been changed, the changes will not take affect until the changes have been committed and the servers have been stopped and restarted. One option to commit these changes is to run this option or when starting the servers using the PSASTRMON command set the "Commit changes" COMMIT(\*YES) parameter. After running this option the servers need to be stopped and started again.

### 82. Work with Utilities

The Work with Utilities screen offers some utilities for the product. See [Work with Utilities](#).

### Command Line

To run a command, type the command and press Enter. For assistance in selecting a command, press F4 (Prompt) without typing anything. For assistance in entering a command, type the command and press F4 (Prompt). To see a previous command you entered, press F9 (Retrieve).

### Command Keys

F3=Exit

Exit the program.

F4=Prompt

Provides assistance in entering or selecting a command.

F5=Refresh

Discards changes and remains on this panel.

## F9=Retrieve

Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

## F13=Information Assistant

Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the i5/OS system, such as, what's new for this release of the i5/OS system, how to comment on information, and where to look for i5/OS information in books and online.

## F16=System Main Menu

Displays the i5/OS Main Menu (MAIN).

## F21=Alerts

Displays the list of Alerts.

## F22=Status

Displays the Operational Resources popup window containing the status of several operation aspects of Powertech products.

## Release SIEM Monitor command (PSARLSMON)

The Release SIEM Monitor (PSARLSMON) command allows the monitor for one Event Source or Output Target to resume operation.

Restrictions:

Monitor (MONITOR)

Specify the name of the Event Source or Output Target whose monitor is to be released.

Monitor type (TYPE)

Specify the type of monitor whose name you entered for the MONITOR parameter. The valid types are \*SOURCE for an Event Source, or \*OUTPUT for an Output Target.

### Command Keys

F3=Exit

Exit the program.

F4=Prompt

Displays a list of items from which one or more may be selected.

F5=Refresh

Discards changes and remains on this panel.

F12=Cancel

Discards changes and returns to the prior panel.

F24=More keys

Shows more Command Keys.

# Select Output Target panel

The Work with Outputs panel allows you to manage Output Targets.

Output Target defines a location to which formatted SIEM events are sent. Each Output Target can specify a different output format.

PSA4B15	Powertech SIEM Agent Select Output Target	15:53:14
Attach Default Outputs to Event Source Select one Output Target with a 1.		
Opt Name	Act Format	Description
- ADF	*MISSING	
- ADFS	SYSFORMAT	SYSLOG
- LAKDJ	*MISSING	
- MYJRN	SYSFORMAT	My Custom Journal
- SIDVICIOUS	ADSF	
- SYSLOG	SYSFORMAT	SYSLOG
F3=Exit   F5=Refresh   F6=Create   F11=View   F12=Cancel		Bottom

## How to Get There

On the [Work with Attached Outputs panel](#), press F6.

## Field Descriptions

### System

System indicates the target of any operations you perform. When you add items, for example, those items will be sent to, and will affect processing on, the System named.

### Opt

Enter a valid option from the list of options provided on the list panel.

## Name

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Active

Indicates whether the Output Target is available for processing. When the Output Target is not active, it will not have syslog events transmitted to it.

## Format

Names the Format that controls how the output event is constructed.

## Description

A short description you assign to the Output Target.

## Property summary

Shows a summary of some of the Output Target's properties.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F6=Create

Creates a new item.

F7=Select system

Allows user to select a different system.

F11=View

Toggles the panel between different views.

F12=Cancel

Discards changes and returns to the prior panel.

# Start Monitor command (PSASTRMON)

The Start Monitor (PSASTRMON) command starts one or all of the SIEM Agent monitor jobs.

Restrictions:

Monitor (MONITOR)

Specify \*ALL to start all monitors, or indicate which monitor you would like to start by specifying one of the following values:

- \*ALL  
Start all monitor jobs.
- \*EVENT  
Start only the event monitor job.
- \*SIEM  
Start only the SIEM Agent Event Source Monitors.

Commit (COMMIT)

Changes to configuration settings will not become active until they are committed. Automatic restart of the server jobs does not commit pending changes.

- \*YES  
Commit pending configuration changes upon manual restart.
- \*NO  
Do not commit pending configuration changes upon manual restart.

Start from (START)

You can start the journal or message queue monitors at a specific point in time using this parameter.

Single Values

- \*RESUME  
Resume operation after the last journal or message queue event that was processed.
- \*CURRENT  
Begins operation on the date and time the monitor job starts.
- Other values  
Element 1: Date  
Determines the date of the first journal or message queue event to be processed.  
date  
Specify a valid date in the past.  
Element 2: Time

Determines the time of the first journal or message queue event to be processed on the date specified.

time

Specify a valid time in the past.

## Command Keys

### F3=Exit

Exit the program.

### F4=Prompt

Displays a list of items from which one or more may be selected.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

### F24=More keys

Shows more Command Keys.

## Trace SIEM Monitor command (PSATRCSIEM)

Specify the name of the monitor for which tracing will be started or stopped. Event Source monitor names are shown on the [Work with Event Sources panel](#) (for example, AB, AUDIT, and SYMSG). Output Target names are user defined, and appear on the [Work with Outputs panel](#).

In order to add tracing, stop the monitor, attach tracing, then restart the monitor. Stop the monitor before To end tracing, first stop the monitor.

**NOTE:** Tracing can create a large volume of data in a short time period and should not be left active for longer than necessary.

```

Trace SIEM Monitor (PSATRCSIEM)

Type choices, press Enter.

Monitor . . . . . _____ Name, *MAIN
Start or stop tracing . . . . . _____ *START, *STOP

Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys

```

## How to get there

On the **Work with Utilities** panel, choose option 2.

## Options

## Monitor (MONITOR)

Specify the name of the monitor for which tracing will be started or stopped. Event Source monitor names are shown on the Work with Event Sources panel (for example, AB, AUDIT,

and SYSMSG). Output Target names are user defined, and appear on the Work with Outputs panel.

**\*MAIN**

Controls tracing for the main SIEM Monitor Controller.

**Name**

Controls tracing for an Event Source or Output Target monitor you name.

## Start or stop tracing (TRACE)

Indicate whether you would like to start or stop tracing the specified monitor.

## Monitor type (TYPE)

Specify the type of monitor whose name you entered for the MONITOR parameter. The valid types are \*SOURCE for an Event Source, or \*OUTPUT for an Output Target.

## Output path (PATH)

Specify the fully-qualified path to the stream file that will receive the trace output data. The stream file will be created when the monitor begins tracing its operation. The stream file will be created with CCSID 1208 (UTF-8).

## Command Keys

### F3=Exit

Exit the program.

### F4=Prompt

Displays a list of items from which one or more may be selected.

### F5=Refresh

Discards changes and remains on this panel.

### F12=Cancel

Discards changes and returns to the prior panel.

## F13=Information Assistant

Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the i5/OS system, such as, what's new for this release of the i5/OS system, how to comment on information, and where to look for i5/OS information in books and online.

## F24=More keys

Shows more Command Keys.

# Work with Attached Outputs panel

The Work with Attached Outputs panel allows you to modify the properties of an existing Event Source.

PSA4910		Powertech SIEM Agent		15:16:08
Work with Attached Outputs				
Type options, press Enter				
4=Remove 5=Display				
Opt	Name	Act	Format	Description
1	SYSLOG	1	SYSFORMAT	SYSLOG
Bottom				
F3=Exit F5=Refresh F6=Attach F11=View F12=Cancel				
Output attached.				

## How to Get There

On the [Change Event Source panel](#), press **F8**.

## Field Descriptions

### Opt

Enter a valid option from the list of options provided on the list panel.

### Name

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Active

Indicates whether the Output Target is available for processing. When the Output Target is not active, it will not have syslog events transmitted to it.

## Format

Names the Format that controls how the output event is constructed.

## Description

A short description you assign to the Output Target.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F6=Create

Creates a new item.

### F11=View

Toggles the panel between different views.

### F12=Cancel

Discards changes and returns to the prior panel.

# Work with Event Descriptions panel

The Work with Event Descriptions panel allows you to define and work with Event Descriptions.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

```
PSA4210                                Powertech SIEM Agent                12:38:19
                                Work with Event Descriptions

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Position to Name      _____
Type options, press Enter
  2=Change   3=Copy       4=Delete   5=Display   6=Toggle active
  7=Fields   8=Subtypes   9=Rules
Opt  Act Name      Description
-    0  TAD        A change was made to the auditing attribute
-    0  TAF        All authority failures
-    0  TAP        A change was made to program adopt
-    0  TAU        Attribute change
-    0  TAX        Row and column access control
-    0  TCA        Changes to object authority
-    0  TCD        A change was made to a command string
-    0  TCO        Create object
-    0  TCP        Create, change, restore user profiles
-    0  TCQ        A change was made to a change request descriptor
-    0  TCU        Cluster operation
More...

F3=Exit   F5=Refresh   F6=Create   F12=Cancel   F17=Print this list
```

## How to Get There

Enter **9=Event Descriptions** for an entry in the [Work with Event Sources panel](#).

## Field Descriptions

### Event Source

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Position to Name

Type a value here to position the list to the first Event Description whose name begins with the characters you typed.

## Opt

Enter a valid option from the list of options provided on the list panel.

- 2=Change  
Opens the [Change Event Description panel](#), where you can modify the properties of an existing Event Description.
- 3=Copy  
Opens the [Copy Event Description panel](#), where you can create a new Event Description by copying the properties and content of an existing Event Description.
- 4=Delete  
Deletes the event.
- 5=Display  
Opens the [Display Event Description panel](#), where you can display the Event Description properties.
- 6=Toggle Active  
Opens the status of the event from active (1) to inactive (0), or vice versa.
- 7=Fields  
Opens the [Work with Fields panel](#), where you can manage Event Description fields.
- 8=Subtypes  
Opens the [Work with Event Subtypes panel](#), which allows you to define and work with Event Subtypes for a particular Event Description.
- 9=Rules

## Active

Indicates whether the Event Description is available for processing. When an Event Description is not active, the event it identifies will not be processed.

## Name

The name you use to refer to this Event Description within Powertech SIEM Agent. For events that originate in a journal, this name must be comprised of the Journal Code and Entry Type of the journal entry. For message queue events, this name must be a message ID.

## Description

A short description you assign to the Event Description.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F6=Create

Creates a new item.

F11=View

Toggles the panel between different views.

F12=Cancel

Discards changes and returns to the prior panel.

# Work with Event Sources panel

The Work with Event Sources panel allows you to define and work with Event Sources.

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

PSA4110		Powertech SIEM Agent		11:30:29	
Work with Event Sources					
Type options, press Enter					
2=Change 3=Copy 4=Delete 5=Display 9=Event Descriptions					
Opt	Name	Type	Description		
-	AB	*AB	Authority Broker		
-	AUDIT	*AUDIT	IBM i Security Audit Journal		
-	CMDSEC	*CMDSEC	Command Security		
-	EPM	*EPM	Exit Point Manager		
-	SYSMSG	*SYSMSG	IBM i System messages		
Bottom					
F3=Exit F5=Refresh F6=Create F7=Select System F12=Cancel					

## How to Get There

On the [Main Menu](#), choose option **1. Work with Event Sources**.

## Options

### Opt

Enter a valid option from the list of options provided on the list panel.

#### 2=Change

Opens the [Change Event Source panel](#), which allows you to modify the properties of an existing Event Source.

#### 3=Copy

Opens the [Copy Event Source panel](#), which allows you to create a new Event Source by copying the properties and content of an existing Event Source.

#### 4=Delete

Deletes the Event Source. You are prompted to confirm.

**5=Display**

Opens the [Display Event Source panel](#), which displays Event Source properties but does not allow them to be changed.

**9=Event Description**

Opens the [Work with Event Descriptions panel](#), which allows you to define and work with Event Descriptions.

## Facility

The name you use to refer to this Event Source within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Type

The type of object from which IBM i events will be extracted. Journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue).

**\*AUDIT**

Defines the IBM Security Audit Journal, QAUDJRN, to be monitored. This type includes some canned definitions of the journal codes and entry types for the security-related journal entries.

**\*SYSMSG**

Defines the IBM System Messages in QSYSOPR or QSYSMSG to be monitored. This type includes some canned definitions of some interesting system management messages.

**\*EPM**

Defines the Powertech Exit Point Manager Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Exit Point Manager entries.

**\*AB**

Defines the Powertech Authority Broker Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Authority Broker.

**\*CMDSEC**

Defines the Powertech Command Security Journal to be monitored. This type includes canned definitions of the journal codes and entry types for Command Security.

**\*MSGQ**

Defines a user-defined message queue to be monitored. You define the messages you would like monitored.

**\*JRN**

Defines a user-defined journal to be monitored. You define the journal codes and entry types you would like monitored.

## Default Output

Indicates that there is, or is not, a set of Outputs attached to the Event Source that act as Default Outputs.

Names the default Output(s) to which syslog events will be sent for this Event Source. These Outputs will be used when a Rule specifies \*SOURCE for a target Output.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Refreshes the panel with the most current data.

### F6=Create

Creates a new item.

### F12=Retrieve

Discards changes and returns to the prior panel.

## Work with Event Subtypes panel

The Work with Event Subtypes panel allows you to define and work with Event Subtypes for a particular Event Description.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

PSA4510		Powertech SIEM Agent		14:14:08	
Work with Event Subtypes					
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)					
Event Description . . . . : TAD (A change was made to the auditing attribute)					
Event Field . . . . . : ADETYP (Type of entry)					
Position to Name _____					
Type options, press Enter					
2=Change 3=Copy 4=Delete 5=Display 6=Toggle active 9=Rules					
Opt	Act	Name	Description		
-	1	D	CHGDLOAUD command		
-	1	O	CHGOBJAUD or CHGAUD command		
-	0	S	The scan attribute was changed		
-	1	U	CHGUSRAUD command		
Bottom					
F3=Exit F5=Refresh F6=Create F11=View F12=Cancel					
F17=Print this list					

### How to Get There

On the [Work with Event Descriptions panel](#), choose option **8=Subtypes**.

### Field Descriptions

#### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

## Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Field

Indicates the Event Field that defines the event data that delivers the subtype value when an event is processed.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

## Position to

Type a value here to position the list to the Event Subtype whose name is equal to or greater than the value you entered.

## Options

### Opt

Enter a valid option from the list of options provided on the list panel.

#### 2=Change

Choose this option for an Event Subtype to open the Change Event Subtype panel where you can modify the properties of an existing Event Subtype.

#### 3=Copy

Choose this option for an Event Subtype to open the Copy Event Subtype panel where you can create a new Event Subtype by copying the properties and content of an existing Event Subtype.

#### 4=Delete

Choose this option for an Event Subtype to delete the Event Subtype.

#### 5=Display

Choose this option for an Event Subtype to open the Display Event Subtype panel where you can display the Event Subtype properties.

#### 6=Toggle active

Choose this option to toggle the status of the Event Subtype from active (1) to inactive (0), or vice versa.

#### 9=Rules

Choose this option for an Event Subtype to work with Event Subtype Rules.

## Active

Indicates whether the Event Subtype is available for processing. When an Event Subtype is not active, the event it identifies will not be processed.

## Name

The name you use to refer to this Event Subtype within Powertech SIEM Agent. The name must match exactly whatever data the "subtype field" can contain in the actual event data at execution time.

## Description

A short description you assign to the Event Subtype.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Refreshes the panel with the most current data.

### F6=Create

Creates a new item.

### F11=View

Toggles the panel between different views.

### F12=Cancel

Discards changes and returns to the prior panel.

# Work with Extensions panel

Use these settings to configure an Extension. See [Extensions](#).

```
PSA4C10                                Powertech SIEM Agent                    12:12:39
                                         Work with Extensions

Event Source . . . . . : AUDIT (IBM i Security Audit Journal)
Event Description . . . : TAD (A change was made to the auditing attribute)
Event Subtype . . . . . : None
Rule . . . . . : None
Type options, press Enter
  2=Change   4=Delete   5=Display
Opt Name      Value
_  fname      &ADONAM&

                                         Bottom

F3=Exit   F5=Refresh   F6=Create   F12=Cancel

Extension created.
```

## How to Get There

On the [Change Event Description panel](#), press **F13**.

## Options

### 2=Change

Choose this option to open the Change Extension panel, where you can change an existing Extension.

### 4=Delete

Choose this option to delete an existing Extension.

### 5=Display

Choose this option to display the configuration of an Extension.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F6=Create

Creates a new item. See [Create Extension panel](#).

F12=Cancel

Discards changes and returns to the prior panel.

# Work with Fields panel

The Work with Fields panel allows you to manage Event Description Fields.

PSA4310		Powertech SIEM Agent		14:08:18			
		Work with Fields					
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)							
Event Description . . . . : TAD (A change was made to the auditing attribute)							
Type options, press Enter							
2=Change 3=Copy 4=Delete 5=Display 7=Substitutions							
Opt	Sub	Name	Description	Offset	Length	Type	Subs
-	>	ADEtyp	Type of entry	0	1	A	*
-		ADONAM	Name of object	1	10	A	
-		ADOLIB	Library name	11	10	A	
-		ADOTYP	Object type	21	8	A	*
-		ADORAUD	Current object audit value	29	10	A	
-		ADUCMD	Y - CHGUSRAUD AUDLVL(*CMD)	39	1	A	
-		ADUCRT	Y - CHGUSRAUD AUDLVL(*CREA	40	1	A	
-		ADUDLT	Y - CHGUSRAUD AUDLVL(*DELE	41	1	A	
-		ADUJOB	Y - CHGUSRAUD AUDLVL(*JOB	42	1	A	
-		ADUMGT	Y - CHGUSRAUD AUDLVL(*OBJM	43	1	A	
							More...
F3=Exit F5=Refresh F6=Create F12=Cancel F17=Print this list							

## How to Get There

On the [Work with Event Descriptions panel](#), choose option **7=Fields**.

## Field Descriptions

### Event Source

Indicates the Event Source to which the Event Description belongs.

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Options

### Opt

Enter a valid option from the list of options provided on the list panel.

#### **2=Change**

Opens the [Change Field panel](#), where you can change a field.

#### **3=Copy**

Opens the [Copy Field panel](#), where you can copy a field.

#### **4=Delete**

Opens the [Confirm Choices panel](#), where you can confirm the deletion.

#### **5=Display**

Opens the [Display Field panel](#), where you can display the field details.

#### **7=Substitutions**

Opens the [Work with Field Substitutions panel](#), where you can manage Event Description Field Substitutions.

## Subtype

Indicates if an Event Field is defined as a Subtype or not. A greater-than symbol (>) indicates it is a Subtype.

## Name

The name used to identify an Event Field within an Event Description.

## Description

A short description assigned to the Event Field.

## Offset

Indicates the distance from the beginning of the journal entry or message data. The first byte within the entry-specific data is offset zero.

## Length

The number of bytes associated with a specific Event Field.

## Data Type

Indicates the type of data the Event Field contains. The possible values are:

Value	Meaning
A	Character
D	Zoned
I	Integer
L	Date
P	Packed
T	Time
U	Unsigned
V	Varying
Z	Timestamp

## Subs

Conveys existence of Field Substitutions.

Blanks

No Field Substitutions exist for the field.

1

Field Substitutions exist for the field.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F6=Create

Creates a new item.

F12=Cancel

Discards changes and returns to the prior panel.

# Work with Field Substitutions panel

The Work with Field Substitutions panel allows you to manage Event Description Field Substitutions.

PSA4410	Powertech SIEM Agent	14:19:37
Work with Field Substitutions		
Event Source . . . . . : AUDIT		
Event Description . . . : TAD (A change was made to the auditing attribute)		
Field . . . . . : ADETYP (Type of entry)		
Type options, press Enter		
2=Change 3=Copy 4=Delete 5=Display		
Opt	Dft	From value To value
-	D	CHGDLOAUD command
-	O	CHGAUD command
-	S	CHGATR command or the Qp01SetAttr API
-	U	CHGUSRAUD command
		Bottom
F3=Exit F5=Refresh F6=Create F12=Cancel		

## How to Get There

On the [Work with Fields panel](#), choose option **7=Substitutions**.

## Field Descriptions

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Field

Indicates the Event Field to which the Field Substitutions belong.

An Event Field is a specification that defines how to interpret different sections of the IBM i event's data.

## Opt

Enter a valid option from the list of options provided on the list panel.

### **2=Change**

Opens the [Change Field Substitution panel](#), where you can modify the properties of an existing Field Substitution.

### **3=Copy**

Opens the [Copy Field Substitution panel](#), where you can create a new Field Substitution by copying the properties and content of an existing Field Substitution.

### **4=Delete**

Opens the [Confirm Choices panel](#), where you can confirm the deletion.

### **5=Display**

Opens the [Display Field Substitution panel](#), where you can display the field details.

## Default

Indicates that this substitution is to be used if no other applies.

## From value

The field value to be translated.

## To value

The new value of the field.

## Command Keys

### F3=Exit

Exit the program.

## F5=Refresh

Refreshes the panel with the most current data.

## F6=Create

Creates a new item.

## F12=Cancel

Discards changes and returns to the prior panel.

# Work with Formats panel

The Work with Formats panel allows you to manage Formats.

A Format holds settings that control how the syslog event data are formatted. These Formats are attached to Outputs such that each Output can transmit syslog events in different formats.

For information on configuring a Format, see [Configuring Formats](#).

PSA4A10	Powertech SIEM Agent Work with Formats	10:18:04
Type options, press Enter		
2=Change 3=Copy 4=Delete 5=Display		
Opt	Name	Spec Description
=	CEF	Legacy Interact CEF format
-	JSON	None JSON format
-	LEEF	LEEF LEEF format
-	MODERN	Modern SIEM Agent Modern format
-	SYSLOG	Legacy Interact syslog format
		Bottom
F3=Exit F5=Refresh F6=Create F12=Cancel		
Configuration changes pending. Press F1 for more help.		

## How to Get There

On the [Main Menu](#), choose 2.

## Options

### Opt

Enter a valid option from the list of options provided on the list panel.

#### 2=Change

Opens the [Change Format panel](#), where you can modify the attributes of a Format.

#### 3=Copy

Opens the [Copy Format panel](#), where you can modify the attributes of a Format.

#### 4=Delete

Deletes the format. You are prompted to confirm.

#### 5=Display

Opens the [Display Format panel](#), which displays Format properties but does not allow them to be changed.

## Name

The name you use to refer to this Format within Powertech SIEM Agent.

This name is required to be a valid OS name.

## Header specification

The specification compliance level of the syslog header.

RFC3164

The syslog event will conform to the legacy RFC3164 specification.

RFC5424

The syslog event will conform to the modern RFC5424 specification.

## Description

A short description you assign to the Format.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F6=Create

Creates a new item. See [Create Format panel](#).

F12=Cancel

Discards changes and returns to the prior panel.

# Work with Outputs panel

The Work with Outputs panel allows you to manage Output Targets.

An Output Target defines a location to which formatted SIEM events are sent. Each Output Target can specify a different output format.

**NOTE:** Fortra's Core Event Manager offers a robust SIEM solution that can be integrated with Powertech SIEM Agent as an Output. Event Manager keeps track of many different points of system access, activity, and events, and notifies the appropriate security personnel or system administrators so that action can be taken before the business is impacted. Because it gathers audit information from multiple operating systems, applications, and devices, it keeps all of your security monitoring in a single location. See [Event Manager](#) for more details.

```
PSA4B10                               Powertech SIEM Agent          11:24:42
                                   Work with Outputs

Type options, press Enter
2=Change  3=Copy  4=Delete  5=Display  6=Toggle Active

Opt Name      Act Format      Description
- ABSJRNSTMF  1  MODERN    Authority Broker Journal Stream File Output
- JRNSIDASPA  1  MODERN    Stream File 2
- QAUDJNSTMF  1  MODERN    Stream File 1
- SIDDTAJRN3  1  MODERN    Stream File 3

                                           Bottom
F3=Exit  F5=Refresh  F6=Create  F7=Select System  F11=View  F12=Cancel
```

## How to Get There

On the [Main Menu](#), choose **3**.

## Field Descriptions

### System

System indicates the target of any operations you perform. When you add items, for example, those items will be sent to, and will affect processing on, the System named.

## Opt

Enter a valid option from the list of options provided on the list panel.

### 2=Change

Opens the [Change Output panel](#), where you can modify the attributes of an Output Target.

### 3=Copy

Opens the [Copy Output panel](#), which allows you to create a new Output Target by copying the properties and content of an existing Output Target.

### 4=Delete

Deletes the output. You are prompted to confirm.

### 5=Display

Opens the [Display Output panel](#), which displays Output Target properties but does not allow them to be changed.

### 6=Toggle Active

Opens the status of the event from active (1) to inactive (0), or vice versa.

## Name

The name you use to refer to this Output Target within Powertech SIEM Agent. It does not need to match the name of any object on the system; it is a name you invent for your reference.

This name is required to be a [valid OS name](#).

## Active

Indicates whether the Output Target is available for processing. When the Output Target is not active, it will not have syslog events transmitted to it.

## Format

Names the Format that controls how the output event is constructed.

## Description

A short description you assign to the Output Target.

## Command Keys

F3=Exit

Exit the program.

F5=Refresh

Discards changes and remains on this panel.

F6=Create

Creates a new item. See [Create Output panel](#).

F11=View

Toggles the panel between different views.

F12=Cancel

Discards changes and returns to the prior panel.

# Work with Rule Conditions panel

The Work with Rule Conditions panel allows you to define and work with Rule Conditions.

PSA4810	Powertech SIEM Agent	11:51:17
Work with Rule Conditions		
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)		
Event Description . . . . : TPW (Passwords used that are not valid)		
Event Subtype . . . . . : P (Password not valid.)		
Rule . . . . . : 1 (User is GDORN)		
Type options, press Enter		
2=Change 3=Copy 4=Delete 5=Display		
Opt	Seq Link	Field Operator Value
-	1 OR	PWUSRN = GDORN
-	2 OR	PWUSRN = HCELINE
-	3 OR	PWUSRN = JMALIK
-	4 OR	PWUSRN = SGOODMAN
-	5 OR	PWUSRN = SMOON
-	6 OR	PWUSRN = HOWARD
F3=Exit F5=Refresh F6=Create F12=Cancel		Bottom

## How to Get There

On the [Work with Rules panel](#), choose option **8** for a Rule.

## Options

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

### Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Subtype

Indicates the Event Subtype to which the listed Rules pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Rule

Indicates the Rule to which the Condition pertains.

## Field Descriptions

### Opt

Enter a valid option from the list of options provided on the list panel.

### Sequence

Sequence is a unique number used to determine the order in which rules are evaluated.

### Link

The Link determines how a Condition relates to other Conditions for a Rule.

Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence. The Condition with the lowest sequence number is ignored.

### Field

Name of the Field to be evaluated at run time against the Criteria.

The valid values are dependent upon the Event Source as well as Event Description associated with the Rule.

## Operator

The logical operator used when comparing a field value to the Criteria.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

### F6=Create

Creates a new item. See [Create Rule Condition panel](#).

### F12=Cancel

Discards changes and returns to the prior panel.

# Work with Rules panel

The Work with Rules panel allows you to define and work with Rules.

The purpose of Rules is to deliver a set of values to be placed within columns of the notification event sent to a syslog server.

PSA4710	Powertech SIEM Agent	10:26:26														
Work with Rules																
Event Source . . . . . : AUDIT (IBM i Security Audit Journal)																
Event Description . . . : TAF (All authority failures)																
Event Subtype . . . . . : None																
Type options, press Enter																
2=Change 3=Copy 4=Delete 5=Display 8=Conditions 9=Toggle Active																
<table border="1"> <thead> <tr> <th>Opt</th> <th>Seq</th> <th>Act</th> <th>Sev</th> <th>Class</th> <th>End</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>1</td> <td>1</td> <td>4</td> <td>sys</td> <td>1</td> <td>Specific authority failures</td> </tr> </tbody> </table>			Opt	Seq	Act	Sev	Class	End	Description	-	1	1	4	sys	1	Specific authority failures
Opt	Seq	Act	Sev	Class	End	Description										
-	1	1	4	sys	1	Specific authority failures										
Bottom																
F3=Exit F5=Refresh F6=Create F11=Switch View F12=Cancel																

## How to Get There

For events, on the [Work with Event Descriptions panel](#), choose option **9** for an event.

For event subtypes, on the [Work with Event Subtypes panel](#), choose option **9** for an event subtype.

## Options

### Event Source

An Event Source is a location from which IBM i events are extracted. Currently, journals and message queues are supported as Event Sources. Common event sources are QAUDJRN (journal) and QSYSOPR (message queue). You may define your own journals and message queues as Event Sources.

## Event Description

Indicates the Event Description to which the listed Event Subtype pertains.

An Event Description is a specification that defines how to identify the IBM i events in which you are interested.

## Event Subtype

Indicates the Event Subtype to which the listed Rules pertain.

An Event Subtype is a specification that further defines how to identify the IBM i events in which you are interested. Many times an Event Description will represent an action that occurred, and this "subtype" will indicate the subject of the action or different classes of the action.

## Opt

Enter a valid option from the list of options provided on the list panel.

## Sequence

Sequence is a unique number used to determine the order in which rules are evaluated.

## Active

Indicates whether the Rule is available for processing. When a Rule is not active its values will not be used in determining contents sent to the SYSLOG server.

## Severity

Indicates the severity of the event. This severity is used in the output syslog packet.

0=Emergency

System is unusable; A panic condition.

1=Alert

Action must be taken immediately; A condition that should be corrected immediately, such as a corrupted system database.

2=Critical

Critical conditions; Hard device errors.

3=Error

Error conditions

- 4=Warning  
Warning conditions
- 5=Notice  
Normal but significant conditions; Conditions that are not error conditions, but that may require special handling.
- 6=Informational  
Informational messages
- 7=Debug  
Debug-level messages; Messages that contain information normally of use only when debugging a program.

## Class

Class is simply placed into the syslog output event when using the Legacy Interact 3 formats. Typical values implemented by Interact 3 include:

- AUD - Audit event
- POL - Policy event
- VULN - Vulnerability event
- FW - Firewall event
- IDS - Intrusion detected event
- SYS - System event
- STG - Storage event

## End

End determines whether to end rule processing after a rule whose conditions are all satisfied.

## Description

A short description you assign to the Rule.

## Command Keys

### F3=Exit

Exit the program.

### F5=Refresh

Discards changes and remains on this panel.

**F6=Create**

Creates a new item. See [Create Rule panel](#).

**F11=View**

Toggles the panel between different views.

**F12=Cancel**

Discards changes and returns to the prior panel.

# Work with Utilities panel

The Work with Utilities screen offers some utilities for the product.

PSA4R10	Powertech SIEM Agent Work with Utilities	14:50:09
Select one of the following: 1. Commit configuration changes 2. Start/stop trace		
Selection or command ==> _____		
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve F13=Information Assistant   F16=System Main Menu   F21=Alerts   F22=Status		

## How to Get There

On the [Main Menu](#), choose **82**.

## Options

### 1. Commit configuration changes

When a database setting has been changed, the changes will not take affect until the changes have been committed and the servers have been stopped and restarted. One option to commit these changes is to run this option or when starting the servers using the PSASTRMON command set the "Commit changes" COMMIT(\*YES) parameter. After running this option the servers need to be stopped and started again.

### 2. Start/stop Trace

Start or stop tracing for a server. This option runs the command PSATRC SIEM.

## Command Line

To run a command, type the command and press Enter. For assistance in selecting a command, press F4 (Prompt) without typing anything. For assistance in entering a command, type the command and press F4 (Prompt). To see a previous command you entered, press F9 (Retrieve).

## Command Keys

### F3=Exit

Exit the program.

### F4=Prompt

Provides assistance in entering or selecting a command.

### F5=Refresh

Discards changes and remains on this panel.

### F9=Retrieve

Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

### F13=Information Assistant

Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the i5/OS system, such as, what's new for this release of the i5/OS system, how to comment on information, and where to look for i5/OS information in books and online.

### F16=System Main Menu

Displays the i5/OS Main Menu (MAIN).

## F21=Alerts

Displays the list of Alerts.

## F22=Status

Displays the Operational Resources popup window containing the status of several operation aspects of Powertech products.

# Appendix

Refer to the following topics for notes and troubleshooting information.

# Authority Broker Events

## Understanding the MSG ID

For Authority Broker events, message IDs are numbered according to the following scheme:

### The first letter in the message ID:

U = Powertech user defined journal entries from QAUDJRN which are from Authority Broker.

### The second two letters in the message ID:

BG = Begin swap

BH = User profile swap logging

CA = Screen capture access

EN = End profile swap

ER = Authority Broker action logged

FC = FireCall logged

FL = Action failure

HP = History Purged

JA = Timed switch performed

### The four-digit number at the end of the message ID:

All Authority Broker message IDs currently use '0001'.

Below is a compilation of Authority Broker events.

## Authority Broker Events

MSGID	MSG
UBG0001	Begin swap
UBH0001	Begin Swap extended info
UCA0001	Screen Capture Access

MSGID	MSG
UEN0001	End Swap
UER0001	Entry Reason
UFC0001	Firecall
UFL0001	Swap Failed
UHP0001	History Purged
UJA0001	Timed Switch Performed

# Command Security Events

## Understanding the MSG ID

For Command Security events, message IDs are numbered according to the following scheme:

### The first letter in the message ID:

U = Powertech user defined journal entries from PCSJRN, which are from Command Security.

### The second two letters in the message ID:

AE = Action executed

AF = Action failed

MA = Monitored command termination (allowed)

MI = Monitored command initiation

MM = Monitored command termination (could not and rejected)

MN = Monitored command termination (could not and allowed)

MR = Monitored command termination (rejected)

## Command Security Events

MSGID	MSG
UAE	Action Executed
UAF	Action Failed
UMA	Monitored Command Termination (allowed)
UMI	Monitored Command Initiation
UMM	Monitored Command Termination (could not and rejected)
UMN	Monitored Command Termination (could not and allowed)

MSGID	MSG
UMR	Monitored Command Termination (rejected)

# Commands

Command	Type	Library	Description
PSACVTINT	*CMD	PTSALIB	Imports settings from the previous SIEM Agent version.
PSAHLDMON	*CMD	PTSALIB	Causes the monitor for one Event Source or Output Target to cease operation. See <a href="#">Hold SIEM Monitor command</a> .
PSARLSMON	*CMD		Allows the monitor for one Event Source or Output Target to resume operation. See <a href="#">Release SIEM Monitor</a> .
PPLSTRMON	*CMD	PTPLLIB	<p>The Start Monitor (PPLSTRMON) command starts the Central Administration Event and Communications monitors.</p> <p>Restrictions:</p> <p>You must have authority to process the command.</p>
PSASTRMON	*CMD	PTSALIB	Starts one or all of the SIEM Agent monitor jobs. See <a href="#">Start Monitor command</a> .
PSAENDMON	*CMD	PTSALIB	Ends one or all of the SIEM Agent monitor jobs. See <a href="#">End Monitor command</a> .
WRKPTSA	*CMD	PTSALIB	Open the SIEM Agent <a href="#">Main Menu</a> .
PSATRCSIEM	*CMD	PTSALIB	Starts or stops tracing for a monitor. See <a href="#">Trace SIEM Monitor command</a> .

# Configuring IBM QRadar to Recognize SIEM Agent Output from an IBM i

This article explains how to configure IBM QRadar to receive events from SIEM Agent and to correctly parse them.

The Universal LEEF Log Source Type controls the parsing of records into QRadar. This Source Type accepts the QRadar LEEF format and a certain number of pre-defined event attributes that form part of the LEEF format. The Event Name in the record is based on the QID—QRadar Identifier, which is a numeric representation of a specific type of event—that is selected for that event. QRadar also determines low-level and high-level categories based on that QID. Once an event type has been learned/mapped into QRadar under the Universal LEEF Log Source Type, the event type is interpreted correctly for any IBM i that sends events into QRadar. When you map that event type, it is saved into a log source extension for Universal LEEF format.

Use the following instructions to get started using QRadar with SIEM Agent, including configuration, mapping, and parsing, as well as setting up and automatically creating Log Sources.

**NOTE:** For complete instructions on QRadar, consult the QRadar documentation or the IBM QRadar support.

The Event Name in QRadar is based on the QID associated with each event. The QID is included in events sent by SIEM Agent to QRadar. For instance, it can be a TCO0014 'Object Created' event originating in the IBM i security audit journal, or a CPF1393 'User Profile Disabled' event coming out of SYSMSG. For each of these event types, the following process can be used to get QRadar to further recognize them.


When you first enter into QRadar's Event UI as a new IBM i is sending events, those events are likely categorized as 'Unknown', as are the log source and low-level category. The event name, log source, and low-level category can be learned/discovered with some initial setup. From then on, when IBM i systems send those types of events to QRadar, these types of events and log source types will already be known to QRadar.

## Recognizing initial IBM i events

Create a Log Source for your IBM i (by IP or Host Name) and point it to the Log Source Type 'Universal LEEF'. To do so:

1. In QRadar, go into **Admin > Log Source > Log Sources > New Log Source** (Upper Right).
2. Use the following settings as a guide:

Log Source Summary



**DWSIEM74**  
 Universal LEEF  
 Status: OK

10. xx.xxx.xxx  
 Last Updated 4 hours ago

Overview

Protocol

ID	79
Name	DWSIEM74
Description	
Enabled	Yes
Log Source Type	Universal LEEF
Protocol Type	Syslog
Groups	Other
Extension	UniversalLEEF_ext
Language	English
Target Event Collector	eventcollector0 :: EDPRQRADAR04
Disconnected Log Collector	Not Set
Credibility	5
Internal	No
Deployed	Yes
Coalescing Events	Yes
Store Event Payloads	Yes

Close

Delete

Edit

Note that in this example, a log source extension has been defined ("Extension: UniversalLEEF\_ext"). A log source extension may not be available unless you have previously customized or mapped events in the DSM Editor and saved those changes. It is important to set the Log Source Type to Universal LEEF, as this will ensure that the received events are parsed (analyzed) in the intended manner by QRadar. Other settings can be adjusted as required.

After this initial setup has been performed, log sources are recognized and created automatically, based on settings you can set within the DSM editor - Configuration tab. Use Log Source Auto-Detection settings and the Log Source Name Template to configure that

automatic recognition process. This allows you to specify the location of log sources, that is, other IBM i systems that will send events to QRadar. An easy way to access the DSM Editor is to right-click an event and select the DSM Editor from there. At that point, you are editing that event type, and can further customize it.

You can map an event type (on the Event Mappings tab), further customize how it is parsed (on the Properties tab), or make other configuration changes related to auto-detection or auto-discovery within the DSM Editor.

If you are, for example, looking at an event (type) like TCO0014 (Audit–Object Created) on the Event Mappings tab, you are able to see all of the events that have been mapped for this log source type. When you select an event (type) for mapping, your objective is to assign it a QID that identifies it.

### Assigning a QID to an event

1. While editing the event mapping (in the Event Mappings tab), choose the event name and select Edit.
2. In the QID window, choose an appropriate high-level category for the event, a low-level category, and then the log source type (“IBM” works well for the log source type).
3. Once you have picked those three values, enter some real text to search within the QID/Name value (like ‘object created’), and click the Search box.
4. Now, you can scroll and find an appropriate mapped QID for that message.

Future Log Sources can “piggyback” on the event mapping set up for Universal LEEF, so you only need to do this one time for each event type. You can also create your own QID if you cannot find what you are looking for. The Event Name, Low Level, and High Level Category fields should all be populated when a QID entry has been defined for the event type.

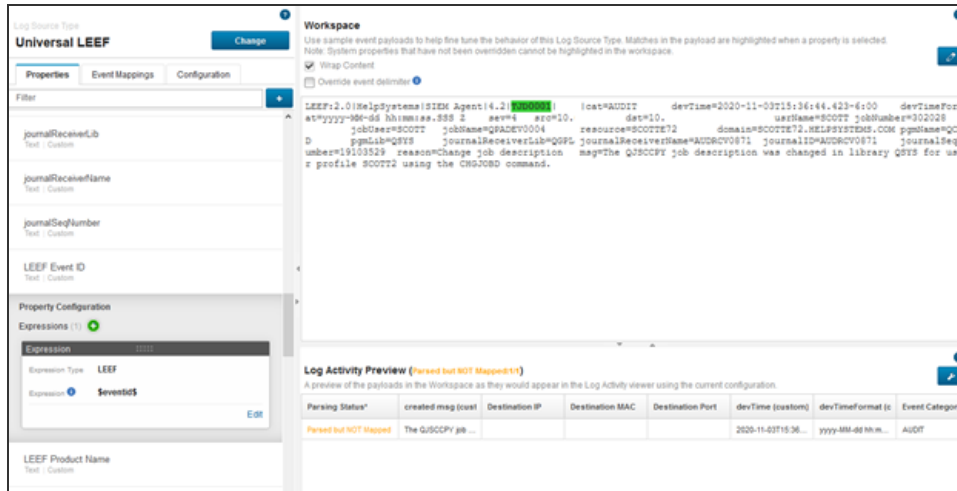
In the Properties tab of the DSM Editor, you can see which parts of an event’s payload have been recognized. You should see all the value pairs, and the label and value for each. LEEF should be the expression type for each of these. The payload should be fully parsed with minimal customization, if any, required. Selecting an event will cause the ‘value’ portion of a payload to be highlighted.

### Assigning a QID to an Event that has not yet been mapped

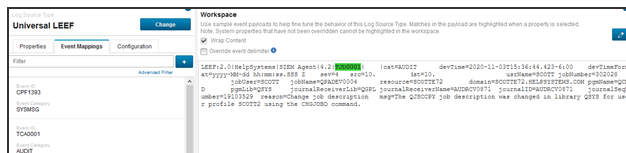
Use the following instructions to configure QRadar so that it can easily classify events sent to it by SIEM Agent in LEEF format. The configuration maps event IDs to other QRadar attributes. Once configured, QRadar performs the mapping automatically. Doing this simplifies the process of integrating SIEM Agent with QRadar.

If QRadar has already received example instances of the event:

1. Find an event within the Event Viewer (list of events coming in) that you would like to map.
2. Right-click it and select **View in DSM Editor**.
3. Within the DSM Editor's Properties Tab, scroll down and click **LEEF Event ID** to select it. The associated LEEF Event ID value in the Workspace portion of the screen is now highlighted (in green).



4. Click the Event Mappings Tab.



5. Click + (plus) to the right of Filter to see the following:

**Create a new Event Mapping**

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

**Unknown Event Mappings**

This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

Event ID	Event Category
TJD0001	AUDIT

Event ID ?

Event Category ?

QID Record

[Choose QID...](#)

[Create](#) [Close](#)

6. Click **Choose QID**.

- On the QID Records window, change the Log Source Type to **IBM i**, and put in some specific search text associated with the message you are attempting to find a QID for. Click the **Search** to see the results.

By changing to the Log Source Type to IBM i, you are going to be searching within IBM i specific messages. You may need to perform several searches with different text strings to find what you are looking for. In the example below, 'User Parameter' was used as search text because it was found directly in the body of the message.

**QID Records**  
Search for an existing QID record to assign, or create a new one.

High Level Category: Any  
Low Level Category: Any  
Log Source Type: IBM i  
QIDName: User Parameter

**Search**

**Search Results**

Name	Severity	High Level Category	Low Level Category
Change to user parameter of job description Actions related to job descriptions including changing the user profile of a job desc	1	System	System Configuration
The USER parameter of a job description changed The USER parameter of a job description was changed.	1	System	Successful Configuration Modific

Total: 2 Selected: 0    10 | 25 | 50

**Create New QID Record**    **OK**    **Cancel**

- Select the search result you want and click **OK**. If you cannot find a suitable QID in your search efforts, you can also click **Create New QID Record**, and create your own.

**Create a new Event Mapping**  
Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

**Unknown Event Mappings**  
This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

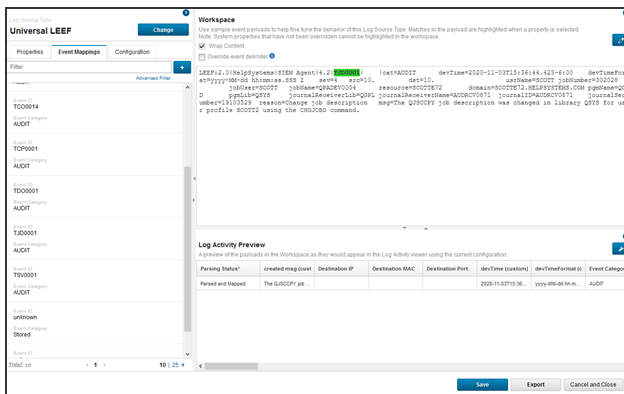
Event ID	Event Category
TJD0001	AUDIT

Event ID: TJD0001  
Event Category: AUDIT

QID Record:  
QID Record: The USER parameter of a job description changed

**Create**    **Close**

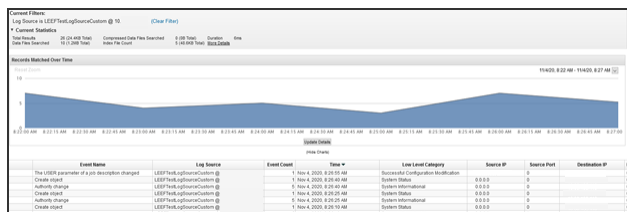
- Click **Create**. You should see something like the following screen. Your Log Activity Preview at the bottom should show your event Parsed and Mapped. Your newly mapped event should now show up in the list of Mapped events in the left panel of the screen.



10. Click **Save** to accept your changes.

Now that you have successfully mapped the event, QRadar will automatically assign the Event Name, Low Level Category, and High Level Category to subsequently received events that have this Event ID.

**NOTE:** QRadar will not retroactively map events that were received before you configured the mapping.



If QRadar has not received examples of the events, but you want to pre-configure the mapping:

1. Display the Event Mappings tab.
2. Click **+** (plus) next to Create a new Event Mapping.
3. Key in the Event ID you would like to map (i.e. "CPF1393" or "TCO0014"). Have an idea of what the event related message text will be to aid the search process, or have a separate screen up with SIEM Agent audit events and subtypes or SYSMSG events to refer to as you are performing searches.
4. Key in the Event ID (case-sensitive).
5. Click **Choose QID**, and follow the steps outlined above to create your preferred event mappings.

All of your Mapped Events will show up in the left margin (on the Mappings Tab), by Event ID.

### Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

Event ID ⓘ

Event Category ⓘ

QID Record

[Choose QID...](#)

Create

Close

## Deploying your changes

After you have performed configuration, changes must be deployed to take effect. To do so:

1. Select the Admin tab.
2. Use the 'Deploy Changes' selection (top left).

After deployment, changes take effect on new event records coming in. Changes are not applied retroactively to older events. A good check to test your changes is to submit a "Last 5 Minutes" selection and observe the displayed values.

# Exit Point Manager Events

## Understanding the MSG ID

For Exit Point Manager events, message IDs are numbered according to the following scheme:

### The first letter in the message ID:

U = Powertech user defined journal entries from QAUDJRN which are from Exit Point Manager.

### The second two letters in the message ID:

Corresponds to the two-letter audit journal code (e.g., NA = Exit Point Manager Allow).

### The four-digit number at the end of the message ID:

The first two digits corresponds to the server (e.g. 03 = \*DDM). The last two digits correspond to the function (e.g. 16 = Open).

The following illustrates the message numbering of common Exit Point Manager event messages:

Message ID	MSG
UNA0801	Exit Point Manager Allow (Session initialization)
UNF0801	Exit Point Manager Failed (Session initialization)
UNR0801	Exit Point Manager Reject (Session initialization)

# Integrating SIEM Agent with Event Manager

Event Manager can be integrated with Powertech SIEM Agent as an Output. Event Manager is a Security Information Event Management (SIEM) solution that gives organizations insights into potential security threats across critical networks through data normalization and threat prioritization, relaying actionable intelligence and enabling proactive vulnerability management. This is possible via a centralized analysis of security data pulled from a variety of systems.

Features include:

- Real-time threat prioritization
- Normalized language for meaningful interpretation
- Integration with third party applications
- Event correlation for in depth forensic analysis
- Logging and customized reporting for regulation compliance

To learn more about Event Manager's capabilities, see [Event Manager](#).

To integrate Powertech SIEM Agent with Event Manager

1. In SIEM Agent, set up an Output for the IP address of the Event Manager system. See [Configuring Outputs](#).
2. Configure Event Sources to use the new Output as desired. For example, to forward Events from the security audit journal to Event Manager, add the new Output to the Default Output for the AUDIT Event Source. See [Configuring Events and Event Sources](#).
3. In Event Manager, configure an Asset for SIEM Agent. See [Adding an Asset](#) in the Event Manager User Guide.

# Monitoring Powertech Antivirus with SIEM Agent

[Powertech Antivirus](#) is a security solution that detects and removes malware stored on IBM i and also protects IBM i systems against ransomware.

While Powertech SIEM Agent does not monitor Powertech Antivirus events directly, it can be configured to monitor for the messages created by Powertech Antivirus on the same system.

See [Monitoring](#) in the Powertech Antivirus User Guide for information on the messages generated within Powertech Antivirus that can be configured for monitoring in SIEM Agent.

# Monitoring SSH Activity with SIEM Agent

This section provides an overview of monitoring SSH (Secure Shell) activity with Powertech SIEM Agent for IBM i.

**NOTE:** Detailed instructions can be found in the Fortra article: [Setting up and testing monitoring of SSH Activity with SIEM Agent](#).

## Requirements

Successful monitoring of SSH Activity with SIEM Agent requires the following:

1. SSH is already configured and working on the IBM i.
2. You can connect via SSH from another system to the IBM i in order to test the configuration.
3. Basic configuration of Powertech SIEM Agent for IBM i has been performed. Specifically, Outputs have been defined and events are flowing to them.
4. The path of the SSHD configuration file is known.

**TIP:** The path is typically: `/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config`

## Data Flow

Correct configuration results in the following flow of data:

1. An SSH client connects to an SSH server and performs actions.
2. On the IBM i server, the SSH daemon sends events to the local Syslog daemon.
3. The Syslog daemon sends events to a local log file.
4. Events added to the log file cause journal entries to be created.
5. SIEM Agent ingests the journal entries.
6. SIEM Agent forwards the journal entries as events to the defined Outputs.

**NOTE:** See the Fortra article: [Setting up and testing monitoring of SSH Activity with SIEM Agent for more information](#).

# Monitoring Changes to Db2 Data with SIEM Agent

## Overview

These instructions describe a sample setup of SIEM Agent that enable monitoring access and modifications to Db2 database files.

## Example Scenario

This example uses the following scenario:

1. We will monitor access to a physical file that contains the company's payroll.
2. The file is journaled.
3. The file contains the following fields: EMPLOYEE; SALARY; SSN; DEPARTMENT.

## Configuration Overview

When a file is journaled, each modification to the file causes a journal entry to be created that describes the modification. The journal entry type reflects the type of action that was performed on the file, and the journal entry fields describe details of the action, such as the data that was inserted, or the job that performed the action. SIEM Agent allows you to monitor the journal and convert the journal entries into events that are sent out.

## Setup

1. In SIEM Agent, add a new Event Source as follows:
  - a. Name: PAYROLL
  - b. Description: Monitors changes to the Payroll file
  - c. Type: \*JRN
  - d. Facility: 4 (example)
  - e. Active: 1
  - f. Default Output: Add one or more Outputs
  - g. Journal: Configure *Object*, *Library*, and *ASP Group* to the journal that is used to journal access to the Payroll file.

## 2. Add Event Descriptions

### a. **F MC** (Member added)

#### i. Add Event Description

1. Journal Code: F, Entry Type: MC
2. Description: Member added
3. Active: 1
4. Event Class ID: \*NAME
5. Severity: 5 (example)
6. Class: FIL (example)

#### ii. Add Field

1. Name: MEMBER
2. Description: Name of new member
3. Subtype: 0
4. Offset: 20, Length: 10, Data Type: A
5. CCSID: 0

#### iii. Define Event Text

1. In the FMC Event Description, change the Event Text as follows:
  - a. Reason: Member added
  - b. Message: &\*CURUSR& added file member &MEMBER& to the Payroll file

### b. Repeat the above steps, but with the differences noted here:

#### i. **F MD** = Member deleted

1. Fields: (*none*)
2. Event Text
  - a. Reason: Member deleted
  - b. Message: &\*CURUSR& deleted file member &\*JRNMBR& from the Payroll file

#### ii. **F OP** = File opened

1. Fields: (*none*)
2. Event Text
  - a. Reason: File opened
  - b. Message: &\*CURUSR& opened the Payroll file

#### iii. **R DL** = Record deleted

1. Fields: (none)
2. Event Text
  - a. Reason: Record deleted
  - b. Message: &\*CURUSR& deleted record number &\*COUNTRRN& from the Payroll file.

iv. **R PT = Record added**

1. Fields:
  - a. Add Fields specific to the fields (columns) that exist in the PAYROLL file and that you want to use in the Event Text. In this example, add one field to the configuration for each of the file fields EMPLOYEE, SALARY, SSN and DEPARTMENT.
  - b. Set Subtype to 0.
  - c. You can use the Display File Fields (DSPFFD) command to display the fields that exist in the file. Note that in SIEM Agent, field offsets start at 0. The DSPFFD output shows offsets (“buffer position”) as starting from 1. If DSPFFD shows a field as starting at buffer position 100, the Field in SIEM Agent has to be configured as having offset 100-1 = 99.
2. Event Text
  - a. Reason: Record added
  - b. Message: Create a message text template using the file-specific Fields that you defined. For example: &\*CURUSR& added a record to Payroll. Values are: Employee name-&EMPLOYEE &Salary-&SALARY& SSN-&SSN& Department-&DEPARTMENT&

v. **R PX = Record added using a Relative Record Number**

1. Copy this from the R PT Event Description so you can reuse the Fields defined there, and just update the Entry Type and the Description. Journal entry types R PT and R PX are the two varieties of journal entry for “record added” Events.

vi. **R UB = Record updated—pre-update values**

1. Copy this from the R PT Event Description so you can reuse the Fields defined there.
2. Event Text:

- a. Reason: Record updated
  - b. Message: &\*CURUSR& changed Payroll for Employee &EMPLOYEE&. Values before update were: Salary-&SALARY& SSN-&SSN& Department-&DEPARTMENT&
- vii. **R UP = Record updated—contains post-update values**
  - 1. Copy this from the R UB Event Description so you can reuse the Fields defined there.
  - 2. Event Text
    - a. Reason: Record updated
    - b. Message: &\*CURUSR& changed Payroll for Employee &EMPLOYEE&. Values after update are: Salary-&SALARY& SSN-&SSN& Department-&DEPARTMENT&

## Monitoring Read Access to Files

The default settings for journaling a file will create entries only when the file is modified, but not when it is read. If you want to additionally set up monitoring for read accesses to a file, perform the following additional steps.

1. Configure the journaling of the file to include read accesses:  
CHGJRNOBJ OBJ((YOURLIB/YOURFILE \*FILE)) ATR(\*OMTJRNE) **OMTJRNE (\*NONE)**
2. Note that if the same job repeatedly opens and closes the same file, only the first few file-opens for that file and job will be logged in the journal. This is normal Db2 behavior.

## General Notes

1. Even though you enter the name of Event Descriptions in two fields, for example; “F MC”, in the list of Event Descriptions, the name is displayed as a *single* field, for example; “FMC”.
2. This example only covers a subset of journal codes. For production usage you should configure additional journal codes to reflect activities such as Clear Member, etc. Each Event Description for monitoring a \*JRN Event Source must correspond to an IBM i journal code. The journal codes are documented here: [https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_74/rzaki/rzakijournalfinderall2.htm](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzaki/rzakijournalfinderall2.htm).
3. To define Fields that correspond to file fields with a data type other than Character/Alphanumeric, see the following help topic: [Making fields for Journal Entry Formats](#).

4. If multiple files are journaled to the same journal, you can use [Rules](#) to distinguish between Events from different files and only send out Events for particular files, or to customize Event Text to reflect the file name.
5. To be able to output the pre-update changes, the file journaling will need to be configured to include pre-change data. Use the following command:  
`CHGJRNOBJ OBJ((YOURLIB/YOURFILE *FILE)) ATR(*IMAGES) IMAGES(*BOTH)`
6. If you have a requirement for creating reports of database modifications, [Powertech Database Monitor for IBM i](#) offers powerful ways to monitor database activity and create reports of it.

# Implementing JSON

These instructions describe how to configure SIEM Agent to output Events in JSON format. JSON is entirely dependent on using [Extensions](#).

JSON support was added in version 4.2 of SIEM Agent, primarily to support event transfer to Apache Kafka, which requires events to be sent in JSON format.

Support for JSON and Kafka allows you to integrate your IBM i systems into a multi-system, Kafka-based event processing workflow.

## The JSON Format

JSON, pronounced “Jason,” is a data format used for data exchange. If you are familiar with XML, you can think of it as a lightweight version of XML. The acronym stands for “JavaScript Object Notation.” JSON is an open-source format that is used by many applications.

The JSON format is flexible. In contrast to formats like Syslog or LEEF, there is no fixed header, and there are no fixed attributes. In the context of integration with SIEM Agent, sending JSON to Kafka requires additional information about the structure of the data being received.

The central concept in JSON is the *object*. An object is an unordered collection of key-value pairs, the *attributes*.

Values can have different data types, most importantly string, number, and object.

In JSON, objects are surrounded by curly brackets. An object can be empty, and would be represented simply like this:

```
{ }
```

In an attribute, the key and value are separated from each other by colons. Keys are surrounded by quotation marks. Values are surrounded by quotation marks if they are string (text) values.

This is a JSON object containing a single attribute:

```
{"EventID": "TCP0001" }
```

The key of the attribute is "EventID". Its value is "TCP0001".

Attributes are separated from each other by commas.

```
{"EventID":"TCP0001","EventText":"User profile FRITZ was created"}
```

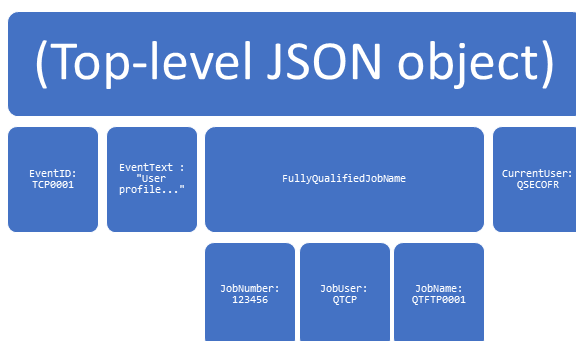
As a value can be of type object, objects can be nested—that is—an attribute value (and hence the object that it resides in) can in-turn contain an object. The following is an example of a JSON object with a nested object:

```
{ "EventID" : "TCP0001" ,
  "EventText" : "User profile FRITZ was created" ,
  "FullyQualifiedJobName" : {
    "JobNumber" : "123456" ,
    "JobUser" : "QTCP" ,
    "JobName" : "QTFTP0001" } ,
  "CurrentUser" : "QSECOFR" }
```

This example object is intended to represent information about TCP0001 (User profile created/modified). Events in an \*AUDIT Event Source.

The object contains the attributes named "EventID", "EventText", "FullyQualifiedJobName", and "CurrentUser". Most of those attributes have text values, but the value of the "FullyQualifiedJobName" consists of a nested object, which contains the attributes named "JobNumber", "JobUser", and "JobName".

The object's structure can be charted as:



A schema is a generalized version of a JSON object that describes what JSON structure is expected (similar to an XML schema).

**NOTE:** Whitespace (blanks, tabs, line ends) is ignored during processing (although, if it is contained in text values, it is preserved).  
Aside from nested objects, the order of the attributes is irrelevant.

## To use SIEM Agent to create JSON output

- 1) Use the JSON format for Output, and,
- 2) You must define Extensions for all Events and/or Subtypes for which you want to output Events.

## Using the JSON Format in SIEM Agent

A preset Format named JSON is included with SIEM Agent. It is based on the \*JSON Message Style.

For Outputs of Type \*KAFKA, always specify JSON as the Format.

You can also use JSON as a Format on \*STREAM Output, which allows you to see the data in JSON format in a stream file. This is useful for debugging.

## How SIEM Agent constructs JSON data

In JSON-formatted Event data output by SIEM Agent, each Event is represented by a single JSON object.

When SIEM Agent processes an Event, it matches the Event to a particular (1) Event Description. If the Event Source supports Subtypes, the Event is also matched to a (2) Subtype. The Event may be additionally matched to (3) Rules on the Event Description and/or Subtype. All of those items—Event Descriptions, Subtypes, and Rules—can also include Extensions. The JSON object that is output for an Event is constructed from those Extensions.

The Extensions define both what values will be included in the JSON event data, and the hierarchical structure, that is, whether any attributes are nested within other attributes.

The JSON object reflects all Extensions that are added for the Event while that Event is being processed. If ten Extensions are added, ten attributes are included in the JSON output.

The JSON object will not reflect other data, especially the Event Text defined by the Event Description or Rule. This differs from SIEM Agent's other Formats/Message Styles: For Syslog and the other Formats, Event data is constructed either from a fixed set of items, including the Event Text, or from a mixture of fixed items and Extensions. In contrast, when

the JSON format is used, if no Extensions have been defined for an Event, no output is created.

This also means that if you want to include Event Text, the Event ID, or a timestamp in the JSON data, you must create Extensions for them.

## How to configure extensions

Refer to the SIEM Agent User Guide for general instructions on how to define Extensions.

When no JSON structure exists, use your own best judgment to select information to go into the JSON data. Examples are:

- Time stamp
- Event Text
- Event ID
- Fully qualified Job Name
- Current User

Assign attribute names consistently across Event Descriptions. If you call something "Current User" in one place, do not call it "CrntUsr" in another place.

When a JSON structure exists:

For the following, we will assume that a sample JSON object or schema exists.

First, create one Extension (on Event Descriptions, Subtypes, or Rules, depending on requirements) per JSON attribute as follows:

1. As the Extension's name, use the attribute's name.

**EXAMPLE:** If an attribute is named "Key source", the Extension's name should also be "Key source".

2. Set the Extension's value to the following:

- a. If the JSON attribute contains a fixed value, specify that as the Extension's value.

**EXAMPLE:** An attribute should always contain the string value "This is a Production system". Set the Extension's value to the same string.

- b. For a numerical value, the value must not include a leading zero.

**EXAMPLE:** ".2345" and "-10.092" are correct. "0.2345" and "-0010.092" are incorrect.

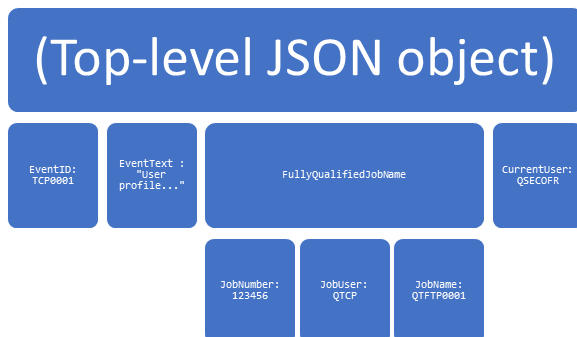
- c. If the JSON attribute contains a variable value, try to find a corresponding value in the Fields or Common Fields available in the Extension's Value field, and insert that.

**EXAMPLE:** If the attribute calls for the inclusion of a system value, you can insert the \*SYSNAM (System name) field from the Common Fields.

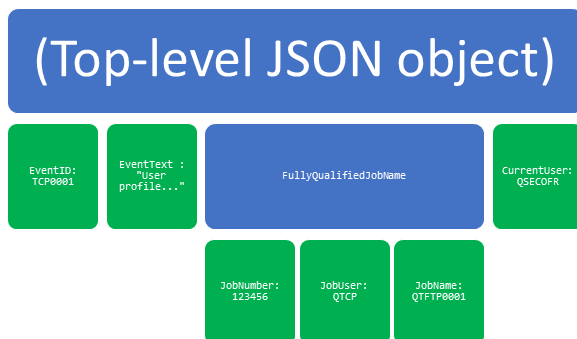
- d. If no corresponding value exists in the Fields, then discern what value can be used instead.
- e. If the JSON attribute contains an object, at this point, insert a placeholder value like "XXX".

After this first pass, define the values for nested objects, that is, attributes whose value is made up from other attributes.

Think back to the example a few pages back:



After the first pass described above, you would have configured actual values for the attributes that themselves do not contain nested attributes, shown in green below:



After the first pass, work "up" from JobNumber/JobUser/JobName and define the actual value of FullyQualifiedJobName as follows.

Create a new Extension:

- Name: FullyQualifiedJobName
- Value: Insert the following Extensions in this order, pressing F9 to insert the Extensions and positioning the cursor at the end of the Value field:
  - JobNumber
  - JobUser (Note: First, position cursor after the {JobNumber})
  - JobName (Note: First, position cursor after the {JobUser})

The Extension's value should look like this:

```
{JobNumber} {JobUser} {JobName}
```

The final list of Extensions should look like this:

Opt	Name	Value
—	CurrentUser	&*CURUSR&
—	EventID	TCP0001
—	EventText	User profile &CPONAM& was created.
—	FullyQualifiedJo	{JobNumber} {JobUser} {JobName}
—	JobName	&*JOBNAM&
—	JobNumber	&*JOBNBR&
—	JobUser	&*JOBUSR&

At this point, you have mapped the example's JSON structure to Extensions in SIEM Agent.

Generally speaking, work your way up from the attributes without nesting to those that are nested. For example, for a four-layer hierarchical structure, start with the bottom layer, then move up to the next, until you arrive at the top. If there is no nesting, only a single pass is required. If there are two layers, do the first pass, then configure the Extensions that include other Extensions, and then again for the third layer, and so forth.

You do not need to create an Extension for the top-level JSON object, SIEM Agent generates it for you. You also do not need to include any of the markup (curly brackets, commas, quotation marks) in the Extensions. SIEM Agent inserts those for you.

## Extensions are shared between Outputs

Extensions that are defined for an Event Source are applied to all Outputs that are used by that Event Source, for example, by being set up as the Default Output for the Event Source, and that support Extensions. If you are sending to more than just one Output, this may or may not be the desired configuration.

**EXAMPLE:**

1) Event Source AUDIT has Outputs OUTPUT\_JSON and OUTPUT\_MODERN configured as its Default Outputs.

2) OUTPUT\_JSON uses the JSON Format, whereas OUTPUT\_MODERN uses the MODERN Format. Both Formats support Extensions.

3) OUTPUT\_JSON forwards Events to an Apache Kafka SIEM, while OUTPUT\_MODERN forwards Events to Core Security Event Manager.

4) You have configured Extensions in Event Source AUDIT.

In this scenario, Extensions defined in AUDIT define the structure of the Event data sent to OUTPUT\_JSON. However, the same Extensions are also included as part of the Event data sent to OUTPUT\_MODERN.

If you have this kind of setup and want to define separate Extensions for both Outputs, use two separate Event Sources in order to maintain two separate sets of Extensions. In the example given here, create a new Event Source of type \*AUDIT, either by copying the existing built-in Event Source, or by creating it from scratch. Then assign OUTPUT\_JSON as the Default Output to one of them, and OUTPUT\_MODERN as the Default Output to the other. Then proceed to modify the Extensions in one of them as desired.

## JSON arrays are not supported

JSON objects are enclosed in curly quotes { }. JSON also supports a structure called arrays, used to represent lists. Arrays are enclosed in square brackets [ ]. If your JSON code contains square brackets (outside of text values), it cannot be replicated in SIEM Agent 1:1. SIEM Agent supports JSON objects, with nesting, but not arrays.

**NOTE:** JSON schemas may contain square brackets for a different purpose, to represent a list of possible values, which SIEM Agent does support.

**TIP:** To check sample JSON structures, you can use tools like Notepad++ that offer syntax highlighting. (In Notepad++, to use the highlighting, set the Language to "JSON").

**TIP:** To include Event Text in the JSON output, manually copy the definition of the Event Text and create a new Extension for it. There are no shortcuts—you have to create the Extension manually.

# Making Fields for Journal Entry Formats

Character and Zoned fields are simply the length of the field. For example,

```
Char(16) = DataType(A=Character), Length(16 bytes)
```

Char(\*) means the length is arbitrary (and probably stated in the value of another field).

```
Zoned(20,0) = DataType(D=Zoned), Length(20 bytes)
```

Packed fields are stored such that the length (in bytes) of the field is calculated as follows:

- Round even numbers of digits up to next odd number (if 8 digits, then 9).
- Add 1 digit. Divide by two. Gives *bytes*.
- Packed(15,0) = DataType(P=Packed), Length(8 bytes) because  $((15 + 1) / 2) = 8$ .

Date, Time, Timestamp:

Timestamps come in two flavors (three, if you count message queue dates).

- "Unformatted Timestamp" is an unsigned integer of 20 digits.
- 26 bytes ISO timestamp (yyyy-mm-dd-hh.mm.ss.micros)
- There is one in message descriptions that is date, time and micros all separate (CYYMMDD, HHMMSS then NNNNNN).

Dates

- CYYMMDD - DataType(L=Date), Length(7 bytes)
- YYMMDD - DataType(L=Date), Length(6 bytes)
- YYYY-MM-DD - DataType(L=Date), Length(10 bytes)

Times

- HHMMSS is DataType(T=Time), Length(6)
- HH.MM.SS is DataType(T=Time), Length(8)

Integer data

Sometimes IBM represents integer data measured in bytes, sometimes in bits.

- Bytes:
  - Binary(2) = DataType(I=Integer), Length(2 bytes)
  - Binary(4) = DataType(I=Integer), Length(4 bytes)
  - Binary(8) = DataType(I=Integer), Length(8 bytes)
- Bits:
  - Bin(15) = DataType(I=Integer), Length(2 bytes)
  - Bin(31) = DataType(I=Integer), Length(4 bytes)
  - Bin(63) = DataType(I=Integer), Length(8 bytes)
  - Bin(16) = DataType(U=Unsigned), Length(2 bytes)
  - Bin(32) = DataType(U=Unsigned), Length(4 bytes)
  - Bin(64) = DataType(U=Unsigned), Length(8 bytes)

# Overriding Host Name / Fully Qualified Host Name in Events

Events sent to outputs typically contain the host name or, depending on the format selected for the output, the fully qualified host name of the IBM i system. Powertech SIEM Agent allows overriding the host name / fully qualified host name information that is sent to the outputs. You can also display and remove host name overrides.

## NOTE:

- The host name is usually identical to the system name.
- The fully qualified host name also contains the domain name. For example, if the host name is “mysystem”, the fully qualified host name could be “mysystem.domain.com”.

In some cases, it is useful to include a different host name / fully qualified host name in events. Examples include:

- If the host name has changed, and the events are sent to a SIEM that filters events based on the system name.
- Where the system name and host name differ from each other.

## Displaying Host Name / Fully Qualified Host Name Overrides

To display any override of the host name / fully qualified host name, execute the following SQL statement on the IBM i system:

```
SELECT * FROM PTSALIB.PSASYP WHERE sytnam in ('HostName', 'FQHostName')
```

If the results include only the SYPNAM and SYPVAL column headings, no override has been configured. Otherwise, the overrides are displayed, the SYPNAM column contains the override type, and the SYPVAL value contains the override setting (the host name).

## Overriding Host Name / Fully Qualified Host Name

To force a specific host name / fully qualified host name to be used in events, follow these steps:

1. End Powertech SIEM Agent.
2. Follow step 2a or 2b to execute a SQL statement on the IBM i system:
  - a. Change the (unqualified) host name information:

```
MERGE INTO PTSALIB.PSASYP AS mt USING (SELECT * FROM TABLE (VALUES ('HostName',
'MyNewHostName')))) AS vt(sypnam, sypval) ON (mt.sypnam = vt.sypnam) WHEN MATCHED
THEN UPDATE SET sypval = vt.sypval WHEN NOT MATCHED THEN INSERT (sypnam, sypval)
VALUES (vt.sypnam, vt.sypval)
```

- b. Change the fully qualified host name information:

```
MERGE INTO PTSALIB.PSASYP AS mt USING (SELECT * FROM TABLE (VALUES
('FQHostName', 'MyNewFullyQualifiedHostName')))) AS vt(sypnam, sypval) ON
(mt.sypnam = vt.sypnam) WHEN MATCHED THEN UPDATE SET sypval = vt.sypval WHEN NOT
MATCHED THEN INSERT (sypnam, sypval) VALUES (vt.sypnam, vt.sypval)
```

3. Replace MyNewHostName / MyNewFullyQualifiedHostName with the desired information.
4. Start Powertech SIEM Agent.

## Removing Host Name / Fully Qualified Host Name Overrides

1. End Powertech SIEM Agent.
2. Follow step 2a or 2b to execute a SQL statement on the IBM i system:
  - a. Remove the override of the (unqualified) host name:

```
DELETE FROM PTSALIB.PSASYP WHERE sypnam = 'HostName'
```

- b. Remove the override of the fully qualified host name:

```
DELETE FROM PTSALIB.PSASYP WHERE sypnam = 'FQHostName'
```

3. Start Powertech SIEM Agent.

# Selected System Messages

## Understanding the MSG ID

Message IDs beginning with the letters 'CP' are Critical Operating System messages. SIEM Agent employs the same message numbering for these messages that is used by IBM. The following illustrates the message numbering of a common Critical Operating System Message:

*The following illustrates the message numbering of a common Critical Operating System message:*

Message ID	MSG
CPF1393	Subsystem disabled user profile on device (Typically a user profile is disabled after invalid signons.)

Below is a compilation of selected System Messages with the shipped criticality and class for each. For more information refer to IBM's message descriptions.

### CRITICALITY

The Criticality value is used by remote consoles to determine how to flag an event when it is displayed. The possible values are:

- 1 - This event will have a \*HIGH criticality.
- 2 - This event will have a \*MEDIUM criticality.
- 3 - This event will have a \*LOW criticality.
- 0 - This event will be a \*NOPASS event. SIEM Agent will ignore this event. No record will be sent to an external console.

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPF0907	Serious storage condition may exist. Press HELP.	STG	80	*NOPASS (0)	*HIGH (1)
CPF111C	System scheduled to power down.	SYS	50	*NOPASS (0)	*MEDIUM (2)
CPF111D	IBM is powering down.	SYS	50	*NOPASS (0)	*MEDIUM (2)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPF1269	Program start request received on communications device was rejected with reason codes.	SYS	0	*NOPASS (0)	*NOPASS (0)
CPF1393	Subsystem disabled user profile on device.	IDS	70	*LOW (3)	*MEDIUM (2)
CPF1397	Subsystem varied off work station for user.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPI0948	Mirrored protection is suspended on disk unit.	STG	99	*NOPASS (0)	*HIGH (1)
CPI0949	Mirrored protection suspended on disk unit.	STG	99	*NOPASS (0)	*HIGH (1)
CPI0950	Storage unit now available.	STG	99	*NOPASS (0)	*HIGH (1)
CPI0953	ASP storage threshold reached.	STG	90	*NOPASS (0)	*HIGH (1)
CPI0954	Storage limit exceeded for ASP.	STG	90	*NOPASS (0)	*HIGH (1)
CPI0955	System ASP unprotected storage limit exceeded.	STG	80	*NOPASS (0)	*HIGH (1)
CPI0964	Weak battery condition exists.	SYS	80	*NOPASS (0)	*HIGH (1)
CPI0965	Failure of battery backup feature in system unit	SYS	80	*NOPASS (0)	*HIGH (1)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPI0966	Failure of the battery backup feature in expansion unit.	SYS	80	*NOPASS (0)	*HIGH (1)
CPI0988	Mirrored protection resuming on disk unit.	SYS	40	*NOPASS (0)	*MEDIUM (2)
CPI0989	Mirrored protection resumed on disk unit.	SYS	40	*NOPASS (0)	*MEDIUM (2)
CPI0998	Error occurred on disk unit.	STG	90	*NOPASS (0)	*HIGH (1)
CPI099C	Critical storage lower limit reached.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1117	Damaged job schedule in library deleted.	SYS	60	*NOPASS (0)	*MEDIUM (2)
CPI1136	Mirrored protection still suspended.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1138	Storage overflow recovered for ASP.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPI1139	Storage overflow recovery failed for ASP.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPI1153	System password bypass period ended.	SYS	99	*NOPASS (0)	*HIGH (1)
CPI1154	System password bypass period will end in days.	SYS	99	*NOPASS (0)	*HIGH (1)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPI1159	System Unique Identifier will expire with more installs.	SYS	99	*NOPASS (0)	*HIGH (1)
CPI1160	System Unique Identifier expired or not valid.	SYS	99	*NOPASS (0)	*HIGH (1)
CPI1161	Unit with device parity protection not fully operational.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1162	Unit with device parity protection not fully operational.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1165	One or more device parity protected units still not fully operational.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1166	Units with device parity protection fully operational.	STG	40	*NOPASS (0)	*MEDIUM (2)
CPI1167	Temporary I/O processor error occurred.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPI1168	Error occurred on disk unit.	STG	99	*NOPASS (0)	*HIGH (1)
CPI1169	Disk unit not operating.	STG	99	*NOPASS (0)	*HIGH (1)
CPI2209	User profile deleted because it was damaged.	IDS	70	*MEDIUM (2)	*MEDIUM (2)
CPI2283	QAUDCTL system value changed to *NONE	SYS	50	*NOPASS (0)	*MEDIUM (2)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPI2284	QAUDCTL system value changed to *NONE	SYS	50	*NOPASS (0)	*MEDIUM (2)
CPI8A13	QDOC library nearing system object limit.	STG	80	*NOPASS (0)	*HIGH (1)
CPI8A14	QDOC library has exceeded System object limit.	STG	80	*NOPASS (0)	*HIGH (1)
CPI8898	An optical system bus failure is detected	SYS	60	*NOPASS (0)	*MEDIUM (2)
CPI9014	Password received from device not valid.	IDS	50	*LOW (3)	*MEDIUM (2)
CPI94A0	Disk error on device.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPI94CE	A system processor error is detected.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPI94CF	Main Storage card failure is detected.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPI94FC	Disk error on device.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPI9490	Disk error on device.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPI96C0	Protected password could not be validated.	AUD	50	*NOPASS (0)	*MEDIUM (2)
CPI96C1	Sign-on request GDS variable was not correct.	AUD	10	*NOPASS (0)	*LOW (3)
CPI96C2	User password could not be changed.	AUD	10	*NOPASS (0)	*LOW (3)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPI96C3	Message &4 returned on system call.	AUD	10	*NOPASS (0)	*LOW (3)
CPI96C4	Password not correct for user profile.	AUD	10	*NOPASS (0)	*LOW (3)
CPI96C5	User &4 does not exist.	AUD	10	*NOPASS (0)	*LOW (3)
CPI96C6	Return code &4 received on call to CPI-Communications.	AUD	10	*NOPASS (0)	*LOW (3)
CPI96C7	System failure in APPC sign-on transaction program.	AUD	10	*NOPASS (0)	*LOW (3)
CPPEA02	*Attention* Contact your hardware service provider now. (Internal analysis of an exception indicates that hardware service is required now.)	AUD	99	*NOPASS (0)	*HIGH (1)
CPPEA04	*Attention* Contact your hardware service provider now. (Internal analysis of an exception indicates that hardware redundancy has been lost due to a permanent failure.)	AUD	99	*NOPASS (0)	*HIGH (1)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPPEA05	*Attention* Contact your hardware service provider now. (Internal analysis of an exception indicates data protection facilities have been lost due to a permanent failure.)	AUD	99	*NOPASS (0)	*HIGH (1)
CPPEA12	*Attention* Contact your hardware service provider now. (Internal analysis of an exception indicates that an I/O card is operating at a reduced performance level.)	AUD	99	*NOPASS (0)	*HIGH (1)
CPPEA13	*Attention* Contact your hardware service provider now. (Internal analysis of exception data indicates that hardware service is recommended to maintain system performance.)	AUD	70	*NOPASS (0)	*MEDIUM (2)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPPEA26	*Attention* Contact your hardware service provider now. (Internal analysis of exception data indicates that hardware service is recommended to maintain system availability.)	AUD	70	*NOPASS (0)	*MEDIUM (2)
CPPEA32	Storage subsystem configuration error.	AUD	70	*NOPASS (0)	*MEDIUM (2)
CPPEA38	*Attention* Contact your hardware service provider now. (A system error has occurred.)	AUD	99	*NOPASS (0)	*HIGH (1)
CPPEA39	*Attention* Contact your hardware service provider now. (A critical system error has occurred. The system will automatically IPL using redundant resources.)	AUD	99	*NOPASS (0)	*HIGH (1)
CPP0DDA	A system processor failure is detected in slot 9	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP0ddb	A system processor failure is detected in slot 10	SYS	70	*NOPASS (0)	*MEDIUM (2)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPP0DDC	A system processor error is detected.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP0DDD	System processor diagnostic code detected an error.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP0DDE	A system processor error is detected.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP0DDF	A system processor is missing.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP0DD9	A system processor failure is detected.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP1604	*Attention* Impending DASD failure. Contact your hardware service provider now. (Internal measurements on disk device &28 indicate that an unrecoverable error resulting in data loss is about to occur.)	AUD	90	*NOPASS (0)	*HIGH (1)
CPP29BA	Hardware error on device under controller.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP29B0	Recovery threshold exceeded on device under controller.	SYS	70	*NOPASS (0)	*MEDIUM (2)

MSGID	MSG	CLASS	SEVERITY	CRITICALITY Shipped	CRITICALITY Powertech Recommendation
CPP29B8	RAID protection suspended on controller.	STG	70	*NOPASS (0)	*MEDIUM (2)
CPP29B9	Power protection suspended on controller.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP951B	Battery Power Unit fault.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9522	Battery Power Unit fault.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP955E	A Battery Power Unit is not installed in the 9406 system unit.	SYS	60	*NOPASS (0)	*MEDIUM (2)
CPP9575	The Battery Power Unit in the 9406 needs to be replaced.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9576	The Battery Power Unit in the 9406 needs to be replaced.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9589	Test of the Battery Power Unit is complete.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9616	A Battery Power Unit is not installed.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9617	A Battery Power Unit needs to be replaced.	SYS	70	*NOPASS (0)	*MEDIUM (2)
CPP9618	A Battery Power Unit needs to be replaced.	SYS	70	*NOPASS (0)	*MEDIUM (2)

# Audit Journal Events

## Understanding the MSG ID

For Audit Journal events, message IDs are numbered according to the following scheme:

### The first letter in the message ID:

T = Audit trail journal entries from QAUDJRN.

### The second two letters in the message ID:

Corresponds to the two-letter audit journal code (e.g., AF = Authority Failure).

### The four-digit number at the end of the message ID:

For type T entries, the four digits represent the subcode of the journal entry. The final digits correspond to the letter of the alphabet for the journal entry code.

The following illustrates the message numbering of common Audit Journal event messages:

Message ID	MSG
TPW0016	Password not valid.
TCO0014	Create of new object
TCP0001	Change to a user profile
TSV0001	Change to system values

## IP address of the originating client for audit journal entries

SIEM Agent events that begin with the letter T are entries that have been written to the security audit journal by the operating system.

In version 3.0 the originating client IP address for all audit journal events, where it is provided in the journal entry, is now presented:

- Src = Always shows the IP address of the IBM i on which the event was generated and written to the journal.
- Dst = Where applicable, shows the IP address of an associated client.

This is most useful in password failure entries. Knowing the originating IP address can help you track down where attempts to hack the system or crack passwords are coming from.

**Let's look at an example:**

May 8 13:27:58 MYAS400 CEF:0|PowerTech|SIEM Agent|3.0|TPW0016|An invalid password was entered for user profile JERRYB.|2|src=10.0.1.185 dst=10.0.1.38 msg=TYPE:JRN CLS:IDS JJOB:QBASE JUSER:QSYS JNBR:003752 PGM:QWTMCMNL OBJECT: LIBRARY: MEMBER: DETAIL:P JERRYB QPADEV000B

- Src= 10.0.1.85 shows the IP address of the IBM i where this event was written to the journal.
- Dst= 10.0.1.38 shows the IP address of the personal computer that was connected to the IBM i.

# Setting up SIEM Agent to use Transport Layer Security (TLS)

SIEM Agent allows you to protect the communication between SIEM Agent and SIEMS. Protection is provided by use of the TLS (Transport Layer Security) protocol. SIEM Agent supports TLS version 1.2.

In order to use TLS to encrypt a SIEM Agent connection, you must use a digital certificate. If your organization has already purchased a trusted digital certificate, copy the certificate file to your SIEM server and configure your SIEM solution settings accordingly. If a certificate is not available, you can create one using IBM's Digital Certificate Manager. See [To create a self-signed digital certificate](#).

## To configure SIEM Agent to use TLS

1. Grant PTUSER \*RX authority to the /QIBM/UserData/ICSS/Cert directory and all its subdirectories.

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/') USER(PTUSER) DTAAUT(*RX)
SUBTREE(*ALL)
```

2. Create a new Output of type \*NETWORK, or modify an existing Output as follows.
  - a. In SIEM Agent, from the Main Menu, choose option 3, Work with Outputs.
  - b. Press F6 to create a new Output or select option 2 on an existing Output to modify it.
  - c. Configure the Output to send data to the SIEM server. Specify the following to secure the connection:
    - i. Type: \*NETWORK
    - ii. Location: the IP address specified in the Certificate Authority
    - iii. Port: the port specified in the Certificate Authority
    - iv. Protocol: \*TLS

**NOTE:** Consult the documentation of your SIEM solution for more information about identifying the required IP address and port required to use the Certificate Authority.

The following example demonstrates how to do this for the Kiwi Free Syslog server.

**EXAMPLE:** To configure the certificate on a Kiwi server:

1. Import the certificate to your Kiwi server:
  - a. Copy the certificate file to the server.
  - b. Start / Run / **mmc** [Enter]
  - c. Choose **File > Add/Remove Snap-in...**
  - d. Choose **Available snap-ins > Certificates**.
  - e. Select **Add**.
  - f. Select **Computer account** and then **Next**.
  - g. Select **Local computer**, then **Finish**.
  - h. Choose **OK**.
  - i. Expand **Certificates (Local Computer)**.
  - j. Right-click **Personal**, choose **All Tasks > Import**.
  - k. Find the certificate file you copied over from the IBM i.
    - l. Enter the password you entered when the certificate was exported and click **Next**.
  - m. Select Certificate Store 'Personal' and click **Next**.
  - n. Click **Finish**.
2. Point Kiwi to this certificate.
  - a. Choose **File > Setup**.
  - b. Scroll down and expand **Inputs**.
  - c. Click **UDP** and un-check **Listen for UDP Syslog messages**.
  - d. Click on **TCP** and un-check **Listen for TCP Syslog messages**.
  - e. Click on **Secure TCP**.
  - f. Check **Listen for secure (TLS) TCP Syslog messages**.
  - g. Click **Select Certificate**.
  - h. In the **Certificate Store** drop-down, choose **My**.
    - i. In the list of available certificates, find the one where 'CN=xxx' matches the common name noted during step 1 above.
    - j. Highlight that entry and click **Select**.
  - k. Enter the TCP port number you would like to use.
    - l. Click **OK**.
3. Configure a \*NETWORK Output in SIEM Agent that uses the \*TLS protocol and the same port you entered in Kiwi. See above.

To create a self-signed digital certificate

1. Open the Digital Certificate Manager by going to:

`http://your_server_name:2001/QIBM/ICSS/Cert/admin/qycucm1.ndm/main0`

**NOTE:** Ensure the HTTP Admin server is running. To start the HTTP server, use the following command:

**STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*admin)**

2. If no certificate authority was previously configured, click **Create a Certificate Authority (CA)** on the left side menu.
3. Enter the requested information and click **Continue**.
4. For 'Install Local CA Certificate,' review the text and click **Continue**.
5. For 'Certificate Authority (CA) Policy Data,' verify information and click **Continue**.
6. On the 'Policy Data Accepted' screen, click **Continue** again.
7. On the Create a Server or Client Certificate screen, you are prompted to create the Certificate store \*SYSTEM. Enter the requested information and click **Continue**.
8. Select applications that should trust the Certificate Authority and click **Continue**.
9. Continue to create an Object Signing Certificate.
10. Copy the certificate file to your SIEM server and configure your SIEM solution settings accordingly.

# Shutting down SIEM Agent

Submit the following commands to shut down the SIEM Agent and Central Administration monitor jobs in the PTWRKMGT subsystem:

**PTSALIB/PSAENDMON**

SIEM Agent

**PTPLLIB/PPLENDMON**

Central Administration

# Syslog Header Specifications

There are two main conventions for the structure and contents of syslog messages, both described in Request for Comment (RFC) documents created by the Internet Engineering Task Force. The older convention is RFC 3164, the more recent one is RFC 5424. When defining a Format, one of these two conventions must be specified in the “Header specification” parameter of the [Create Format panel](#) (with the exception of JSON, which defaults to None since there is no header, and LEEF, which has its own proprietary header specification).

See the following for header descriptions.

## The RFC 3164 (“Legacy”) Header Convention

RFC 3164, also referred to as “BSD-syslog” or “legacy syslog”, is the older of the two formats.

The RFC 3164 has the following structure:

- PRI(ority), calculated from:
  - Severity
  - Facility
- HEADER
  - Timestamp
  - Host name
  - Application name
- A Colon
- MSG

### EXAMPLE:

```
<38>Apr 16 08:31:50 V7R3M0#O SYSLOG:0|Powertech|SIEM
Agent|4.4|TIP0013|IPC Reason|6| src=V7R3M0#O dst=0.0.0.0
msg=TYPE:JRN CLS:AUD JJOB:QRMCCTRMCD JUSER:QSYS JNBR:020706
PGM:QP0ZPCP2 DETAIL:N/A
```

The RFC 3164 standard also:

- Is limited to a total message length of 1,024 bytes.
- Specifies the timestamp in the format “Mmm dd hh:mm:ss”, where “Mmm” is a three-letter abbreviation for the English name of month, e.g. “Aug” for “August”. (ISO-compatible timestamps are also used.)

RFC 3164 has a simple, relatively flat structure. Don't select RFC 3161 as header specification for a Format unless you need to, for example, in order to provide compatibility with a legacy SIEM solution.

## The RFC 5424 ("Modern") Header Convention

Messages following RFC 5424 (also referred to as "IETF-syslog") have the following structure:

- HEADER
  - PRI(riority), calculated from
    - Severity
    - Facility
  - Version
  - Timestamp
  - Host name
  - Application name
  - Process ID [or corresponding OS construct]
  - Message ID
- STRUCTURED DATA (optional)
  - Data Block 1
    - Block ID 1
      - Name-value pair 1-1
      - Name-value pair 1-2
      - Name-value pair 1-3
      - ...
  - Data Block 2
    - Block ID 2
      - Name-value pair 2-1
      - Name-value pair 2-2
      - Name-value pair 2-3
      - ...
- MSG

### EXAMPLE:

```
<38>1 2021-04-16T08:27:50-5:00 V7R3M0-ON-POWER8.HELPSYSTEMS.COM -  
- SYSLOG:0|Powertech|SIEM Agent|4.4|TIP0013|IPC Reason|6|
```

```
src=V7R3M0#O dst=0.0.0.0 msg=TYPE:JRN CLS:AUD JJOB:QRMCCTRMCD  
JUSER:QSYS JNBR:020706 PGM:QP0ZPCP2 DETAIL:N/A
```

**NOTE:** The example uses the CEF message style in combination with the RFC 5424 header specification.

RFC 5424 is the recommended header specification.

## Syslog Severity Table

Value	Severity	Keyword	Description	Condition
0	Emergency	emerg	System is unusable	A panic condition.
1	Alert	alert	Action must be taken immediately	A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	crit	Critical conditions	Hard device errors.
3	Error	err	Error conditions	
4	Warning	warning	Warning conditions	
5	Notice	notice	Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.
6	Informational	info	Informational messages	
7	Debug	debug	Debug-level messages	Messages that contain information normally of use only when debugging a program.

# Work Management

SIEM Agent jobs, like those of other Powertech products, are active in subsystem PTWRKMGT.

The PTWRKMGT subsystem description is created during installation. The subsystem description is contained in a library also named PTWRKMGT. This library contains a class description. You can configure those objects in order to tune the Powertech products' run-time behavior with respect to storage, time slice, run priority, etc.

By default, SIEM Agent does not start automatically when the system is IPLed. To start SIEM Agent automatically at system startup, add the SIEM Agent start commands to the system startup program. See [Start Monitor command \(PSASTRMON\)](#) for more details.

The following table lists the SIEM Agent jobs.

Monitors	Description
PSAEVTMON	Routes product audit events to Central Administration - PGM-PSA5100
PSAMGRMON	Event Source and Output Manager - PGM-PSA5200
PSAMGRMON	Monitors for user-defined Event Sources and user-defined Outputs

# Glossary

## Event Text

Event Text is a set of formatting patterns used to generate the human-readable form of several values in the notification event that is routed to an Output. Event Text is specific to a particular Event or Subtype.

Replaceable variables in the formatting string (beginning and ending with an ampersand) will be replaced with the value of the named field from the Event data in the output. Further, the values of replaceable fields can themselves be transformed to other values by Substitutions.

Only journal-based sources use these formatting strings; message queue-based sources package and send the message text as-is from the message queue.

## Extensions

An *Extension* is a formatting pattern used to generate the human-readable form of several values in the notification event that is routed to an Output. These Extensions are used by the Modern, LEEF, and JSON formats (they do not affect the legacy formats). Extensions are placed into the syslog output event in the form “name=value”. A single space always precedes the “name=” phrase.

At the Event Description level, the Extension field defines the default Extensions. Additional Extensions can be added for individual Subtypes and Rules defined within the Event Description, for example, those specified in the Add Extension field of the respective [Create Event Subtype panel](#) and [Create Rule panel](#).

Extensions do not stand alone; they must be attached to other entities. These entities are arranged in a hierarchical fashion; same-named Extensions at higher levels “appends” those at lower levels.

Hierarchy (1 is lowest level):

1. Event Source
2. Event Description
3. Event Subtype
4. Rule

Replaceable fields in the formatting string will be replaced with the value of the field from the Event data at the time the event is captured and processed. Further, the values of fields can themselves be further transformed to other values by Substitutions.

Available functions: %extract, %int, %substr, %subst, %sst, %len, %length, %ltrim, %triml, %rtrim, %trimr and %trim.

The %extract arguments that are available are:

Date Values	Time Values
EPOCH	HOUR
MILLENNIUM	HOURS
MILLENNIUMS	MINUTE
CENTURY	MINUTES
CENTURIES	SECOND
DECADE	SECONDS
DECADES	MILLISECOND
YEAR	MILLISECONDS
YEARS	MICROSECOND
QUARTER	MICROSECONDS
MONTH	
WEEK	
DAY	
DAYS	
DOW	
DOY	

**NOTE:** %extract function is:

- Not currently available for \*TIMESTAMP in Event Source type of \*SYSMSG.
- Available on IBM i 7.3 with TR5, IBM i 7.4 and higher.

Function names are not case sensitive. Character fields must be enclosed in single quotes.

**EXAMPLE:**

```
%trimr(%substr('&CAUNAM',1,5))
```

**EXAMPLE:**

```
%extract (EPOCH from '&*TIMESTAMP&')
```

In the output, extensions appear sorted by level first, then alphabetically by the name of the extension.

**EXAMPLE:** If you have extensions on Entry Type TPW, and some more on entry Subtype P, and then on a Rule:

TPW: a=&FLD1&, b=&FLD2&, c=&FLD3&

P: a=&FLDX&, b=&FLDY&

Rule A: a=&FLDn&

They appear in the output as: a=1 b=2 c=3 a=X b=Y a=n

## Including message variables

The value of message variables (message fields) can be used in Extensions. For example, if a CPF1234 message is sent, and includes a message variable, the value of that message variable can be included in an Extension.

To do this, specify the field on the Value line of the [Create Extension panel](#) as follows:

```
&[number of message field]
```

For example, for message field #1:

```
&1
```

## Monitors

Monitors are SIEM Agent jobs that run in the PTWRKMGT subsystem. For details, see [Work Management](#).

## Rules

Rules have the final say in determining whether to post a syslog event, to which Output(s) to post the syslog event, and the class and severity for that event. Rules take effect based on Conditions that interrogate event Field data. Special fields allow you to specify general information about the event (when, who, day of week, et cetera). This list of special fields may include data from the journal entry “header” (not available for use in Rules for message queues - similarly, there may be data for messages not available for journals).

Conditions perform the evaluation. Fields can be compared to other Fields. Rules supply the values to use in the output event. Rules can specify the severity and proprietary “class” of the output event.

## Valid OS Name

A valid OS name is required to begin with an alphabetic character (A-Z) or one of @ (at sign), # (pound sign), or \$ (dollar sign). The remaining characters may be alphabetic (A-Z), numerals (0-9), @ (at sign), # (pound sign), \$ (dollar sign), . (period), or \_ (underscore).

# Contacting Fortra

Please contact Fortra for questions or to receive information about SIEM Agent. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

## Fortra Portal

For additional resources, or to contact Technical Support, visit the [Fortra Support Portal](https://support.fortra.com) at <https://support.fortra.com>.

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.