FORUM SENTRY BEST PRACTICES

IMPORTANT LOG MESSAGES TO MONITOR

Forum Systems Sentry™ Important Log Messages to Monitor

D-ASF-SE-010029

Contents

INTRODUCTION

Scope of this Document

This document is intended to provide a general introduction to the Forum Sentry logs and specifically list out important log messages to monitor for.

This best practices guide does not include all of the details of configuring logs and logging strategies with Sentry. Sentry Administrators should review the Additional Documentation listed below for more information.

Additional Documentation

For more details on logging with Forum Sentry, review the "FS Sentry v8.1 Logging Guide", the "FS Sentry v8.1 Monitoring and Reporting Guide", and the "FS Sentry v8.1 IDP Rules Guide".

Much of the information in this Best Practices Guide is taken from these documents.

Platforms

The information is applicable to all available Forum Sentry form factors:

 FIPS 140-2 Hardware					
✓	✓	✓	✓	✓	✓

Types of Logs in Forum Sentry

There are three types of logs in Sentry: Audit Logs, System Logs, and Access Logs. All of the logging information stored locally, for all 3 logs, can also be sent off the system via Remote Syslog policies.

Audit Logs

Audit logs are a comprehensive view of user activities and policy additions, modifications or deletions. Each entry in the Audit logs includes a unique Document ID, Time (date and timestamp of each event), session number, event code number, log level flag and system process message. Most columns of data may be sorted.

System Logs

System logs capture the changes that occur in the life of a document as well as changes in movement for a document. As a request is received by the system and the document passes through various processes, tracking messages are written to the System log. Each entry in the System log includes a unique Document ID, Time (date and timestamp of each event), session number, event code number, log level flag and system process message. Most columns of data may be sorted.

Access Logs

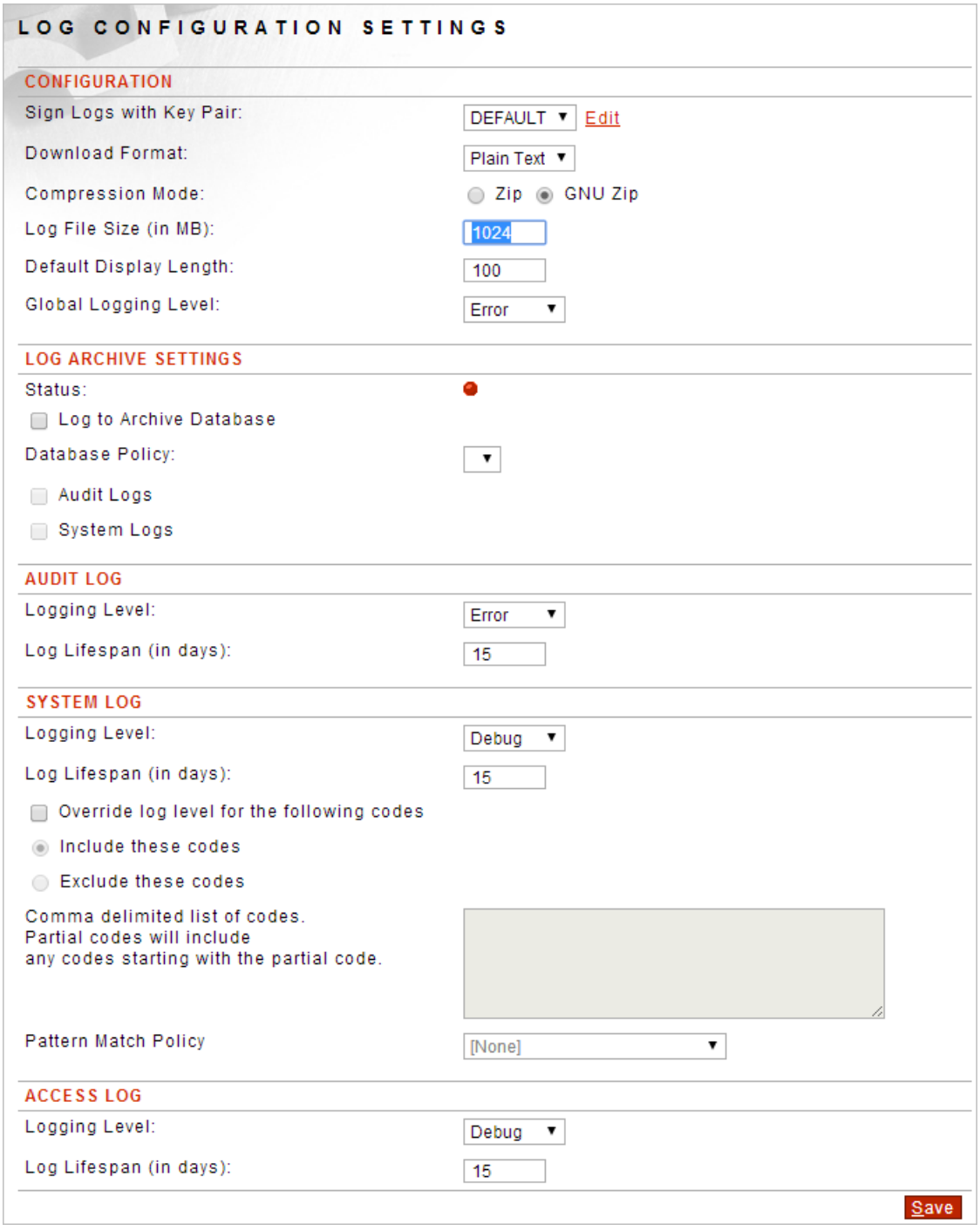
Access logs capture a minimal amount of data for each document being processed. The data captured (columns in the log) are the Time (date and timestamp), Session ID, Client IP, TYPE (HTTP Method) HTTP Code, URI, and Length of each document that is processed by the system. They hyperlinked Session ID links to the same Session ID for this document in the System log.

Logging Settings in Forum Sentry

Settings

The Settings screen manages individual settings for each category of logs. In the WebAdmin interface go to the Diagnostics >> Logging >> Settings and the LOG CONFIGURATION SETTINGS screen appears.

For detailed information on these settings please review the Forum Systems Sentry Version 8.1 Logging Guide.



Log Levels in Forum Sentry

Logging Levels

The Logging Level drop down list includes four categories which represent the level of detail for log messages; these are ERROR, WARNING, INFO, and DEBUG log messages.

- All ERROR level messages will be shown in all other log levels.
- All WARNING level messages will be shown in WARNING, INFO, and DEBUG log levels.
- All INFO level messages will be shown in INFO and DEBUG log levels.
- DEBUG level messages will only be shown in DEBUB log levels.

Log thresholds can be set globally (for all policies) or on a per policy basis.

Log thresholds do not need to be set the same for local and syslog policies.

Note that use of DEBUG logging can introduce signifigant processing overhead and is not recommended for production environments.

For detailed information on Logging Levels please review the Forum Systems Sentry Version 8.1 Logging Guide.

Log Codes in Forum Sentry

Log Codes

When viewing the logs in the WebAdmin interface, there is a column titled “Code”. Each specific log message has a unique code. When viewing the logs through the Sentry WebAdmin interface, the logs can be filtered and sorted by codes.

For instance, the “*Document entered communications layer*” log message will always use code 08401.

Always Log Codes

It is possible to always logs specific codes, regardless of the log level settings, with the “Override Log Level” option to “***Include these codes***”.

This can be enabled globally or on a per policy basis.

Exclude Codes

It is possible to always never log specific codes, regardless of the log level settings, with the “Override Log Level” option to “***Exclude these codes***”.

This can be enabled globally or on a per policy basis.

Log Storage in Forum Sentry

Local

All log messages for all three Sentry log files are written to local files and stored locally. There is no way to disable storing the logging information locally.

A new local log is generated each night at midnight. The previous day's log is compressed and stored on disk according to the Log Lifespan setting.

Local logs hae a log file size limit, set on the Log Settings page. When this limit is reached, the log is deleted and starts again (all previous data is deleted).

Remote Syslog Policies

All log messages for all three Sentry log files can be sent off the system via the syslog protocol in real-time to a remote system capable of handling incoming syslog messages.

For detailed information on Remote Syslog Policies in Sentry please review the Forum Systems Sentry Version 8.1 Logging Guide.

Important Runtime Log Messages

Intrusion Detection and Prevention (IDP) Failures

When Forum Sentry blocks a request or response message, or encounters a processing failure, an IDP Rule failure will occur. Examples of IDP Failures include:

Authentication failures
Size limits exceeded
Rate limits exceeded
Malicious requests
Virus detection

For detailed information on the IDP Rules in Sentry please review the Forum Systems Sentry Version 8.1 IDP Rules Guide.

Important Notes:

1. All IDP failures are logged at WARNING (W) level.
2. All IDP failures are logged with Code 0600D
3. IDP Rules are customizable, and the Sentry log displays the IDP Rule names (and groups) which are configurable. Therefore filters for these messages need to be written for the specific IDP Rule Names configured by the Sentry admin.
4. The Process Error IDP Rule can be triggered for multiple reasons, including: Task List Failure, unable to decode documents.
5. IDP Rules can also be configured to send alerts via SNMP traps and emails (in addition to the even being logged).

Below is a table outling all IDP Failure messages generated by Sentry. These IDP failures are the important events to take note of and filter for.

Code	Level	Sample Log Message
0600D	W	'Authentication Failure', IDP Group 'System Group', Associated Policy: System, Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. No basic authentication credentials given
0600D	W	'Authorization Failure', IDP Group 'System Group', Associated Policy: System, Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: testuser2.
0600D	W	'IDP_Rule Attempted XML external URI reference', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: testuser. External reference found in the document.
0600D	W	'IDP_Rule Maximum Attachment Count 1', IDP Group 'ALL IDP RULES XML POLICIES', Associated Policy: XML Policy: 'IDP Testing', Triggered 1 time(s) on Request, Policy: IDP Testing, Client IP: 192.168.82.72, User: -. The number of attachments, 2, exceeds the maximum number of attachments allowed, 1.
0600D	W	'IDP_Rule Maximum Byte Count 10k', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The current rate of 18.3KB per second, exceeds the maximum rate of 10KB per second.
0600D	W	'IDP_Rule Maximum Document Count 1', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The current rate of 2 documents per second, exceeds the maximum rate of 1 documents per second.
0600D	W	'IDP_Rule Maximum Element Children 1', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The number of element children in the document, 5, exceeds the maximum element children for a
0600D	W	'IDP_Rule Maximum Element Count 1', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The number of elements in the document, 4, exceeds the maximum number of elements for a document
0600D	W	'IDP_Rule Maximum Element Depth 1', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The element depth of the document, 4, exceeds the maximum element depth for a document, 1.
0600D	W	'IDP_Rule Maximum Internal Reference Expansion', IDP Group 'ALL IDP RULES XML POLICIES', Associated Policy: XML Policy: 'IDP Testing', Triggered 1 time(s) on Request, Policy: IDP Testing, Client IP: 192.168.82.72, User: testuser. The internal reference expansion limit of has been exceeded
0600D	W	'IDP_Rule Maximum XML Document Size 10k', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The size of the XML document, 18.3KB, exceeds the maximum document size, 10KB.
0600D	W	'IDP_Rule Minimum Document Size 10k', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The size of the XML document, 358B, does not meet the minimum size required, 10KB.

0600D	W	'IDP_Rule New Client IP Address', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. First access from IP address 192.168.82.72.
0600D	W	'IDP_Rule New Operation', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. First access of operation {http://crosschecknet.com/}Echo.
0600D	W	'IDP_Rule New User', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: testuser. First access by user testuser.
0600D	W	'IDP_Rule Pattern Match Policy Violation', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: testuser. Pattern match policy violation: SQL_Keywords
0600D	W	'IDP_Rule SOAP Fault Received by Remote Server', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Error, Policy: training, Client IP: 192.168.82.72, User: testuser. SOAP fault received from remote: 'CloudPortFault'
0600D	W	'IDP_Rule_Max Payload Size 10k', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The size of the document including the payload, 18.3KB, exceeds the maximum payload allowed, 10KB.
0600D	W	'Invalid HTTP Message', IDP Group 'System Group', Associated Policy: System, Triggered 1 time(s) on Error, Policy: training, Client IP: 192.168.82.72, User: -. No matching message type filter.
0600D	W	Invalid WSDL Message', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. The root element '{http://crosschecknet.com/}EchoBAD' found within the SOAP body does not match the name and namespace of any message defined in the WSDL file.
0600D	W	'No Matching XML', IDP Group 'ALL IDP RULES WSDL POLICIES', Associated Policy: WSDL Policy: 'training', Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: testuser. No matching XML filter.
0600D	W	'Process Error', IDP Group 'System Group', Associated Policy: System, Triggered 1 time(s) on Request, Policy: IDP Testing, Client IP: 192.168.82.72, User: testuser.
0600D	W	'Virus Detected', IDP Group 'System Group', Associated Policy: System, Triggered 1 time(s) on Request, Policy: training, Client IP: 192.168.82.72, User: -. Virus check result: Access denied.

Conclusion

Sentry log messages are always stored locally on disk. It is recommended to send all or at least important log messages to a remote syslog server.

Syslog servers can receive log messages from multiple Sentry instances for log aggregation. Most syslog servers can also be configured to filter for and alert on specific log messages. Sentry administrators should build alerts on the syslog server to be notified of IDP failure messages.

About Forum Systems

Forum Systems, a wholly owned subsidiary of Crosscheck Networks, Inc., is a leader in Service Oriented Architecture (SOA) and secure service mediation. Through comprehensive Threat mitigation and Trust enablement, Forum's family of hardware, software, and cloud-based instances provides enterprises and government organizations with the foundation for achieving secure service mediation. Processing more than one billion transactions per day worldwide, the FIPS- and DoD-certified Forum products offer the industry's most comprehensive protection against XML- and SOAP-based vulnerabilities. Forum Sentry has been issued an industry-first patent (7,516,333) for XML security functions such as XML Encryption, XML Decryption, and XML Signatures using a network appliance. For more information, please visit www.forumsys.com.