### Please Read

#### Data Collection/Processing Process

The smallest unit of data handled by Logpresso Sonar is a record. A record refers to "a complete logical unit of information." For example, a single line of log from a firewall or web server, a single syslog message, a single SNMP trap message, a single row stored in a relational database table, a single document stored in a MongoDB collection, a single packet observed in a file collected through a PCAP device, or a JSON object (a set of name-value pairs enclosed in curly braces) received in response to an external REST API call are all considered "records" handled by Logpresso Sonar.

The collection menu consists of loggers, parsers, log schemas, and logger models. By installing an [app](https://docs.logpresso.comnull), the necessary parsers, log schemas, and logger models for collecting and processing data from data sources are provided, allowing administrators to configure only the loggers (along with connect profiles if necessary) without any issues in operation. However, understanding the actions performed by each function and their interrelationships is essential for properly understanding and utilizing the collection features.

The following diagram illustrates the process by which data is processed in Logpresso Sonar (click the image to view a larger version).



The logger receives data sent from the data source, or the logger periodically connects directly to the data source to collect data.

* The arrows in the diagram indicate the direction of communication at the TCP/IP or application level.

Using the parser defined in the logger model, the original data is identified on a record-by-record basis, and fields are identified and extracted from each record.

If there are normalization rules defined in the logger model, the fields and field values extracted through the parser are transformed to match the field names and types of the log schema.

The normalized records are stored in tables. The stored records include both the normalized fields and the original logs.

This series of data processing steps is essential for establishing consistent policies and analyzing data. Logs generated from heterogeneous devices are composed in different formats, but they share common attributes, allowing for simplified policy setting and analysis through field normalization. For instance, while logs from heterogeneous firewalls may differ in format, normalizing them under the same field name allows for comparison against the block list configured in the [address groups](https://docs.logpresso.comnull) for the source IP address across all firewalls.

#### Simplified Collection Setup Procedure

The log/data collection setup process, which administrators previously had to configure manually, has been simplified with the introduction of the **[app](/ko/sonar/4.0/ui/chapter-apps)** system. By installing an app, all necessary parsers, log schemas, and logger models for data collection from the integrated system are provided. The collection setup procedure has changed as follows:

|  |  |
| --- | --- |
| Before 4.0.2308.0 | After 4.0.2308.0 |
| 1. Configure log schema | 1. Download the app from [Logpresso Store](https://logpresso.store) |
| 2. Configure original log parser | 2. Install the app |
| 3. Configure normalization parser | 3. Set up connections to data sources, such as connect profiles |
| 4. Configure logger model | 4. Create loggers |
| 5. Configure extraction model | - |
| 6. Create loggers | - |

Administrators can still manually configure [parsers](https://docs.logpresso.comnull), [log schemas](https://docs.logpresso.comnull), and [logger models](https://docs.logpresso.comnull), but in typical situations, it is sufficient to use the components provided by the app without needing to configure everything individually.

#### Internationalized Log Schema

The [log schema](https://docs.logpresso.comnull) has been enhanced to support Korean, English, and Chinese. Now, when requesting explanations from employees, the field names of the logs presented as supporting materials will be displayed in the language used by the employees.

#### When Data Collection is Not Possible

App Development Request

If an app for collecting data from the data source is not available on the [Logpresso Store](https://logpresso.store), please request Logpresso to develop the app. When making an app development request, the following information is required:

* Information about the requesting customer
* Manufacturer, product name, and version of the product to be integrated
* Method of log collection
* Log definition document (if integrating with a database, include database information and table schema)
* Sample logs

Self-App Development

Logpresso provides an app SDK to enable direct app development for systems that integrate with Logpresso Sonar/Maestro. For information needed for app development, please refer to the [Logpresso App Development Guide](https://docs.logpresso.comnull).