

Ironstream for IBM i

Data forwarding for increased visibility

Ironstream® for IBM i enables critical logs and other machine data from your IBM i environment to be streamed and correlated with data from the rest of your enterprise in near real-time within Splunk or other SIEM solution.

The IBM i systems power mission-critical applications around the world. But many organizations are still flying blind, with no easy way to derive operational intelligence from the vast amounts of machine data generated by these critical systems.

Data streams from IBM i systems have not been as accessible as your other data streams when it comes to analytics for IT operational analytics (ITOA), or for security information and event management (SIEM). They are all quite accessible now – thanks to Ironstream for IBM i, from Syncsort.

With Ironstream for IBM i, you collect log data from the System Audit Journal, the Accounting Journal, Collection Services and from built-in queries for system objects, profiles, system values, jobs, spool files and much more. All this data can be forwarded in near-real time or user-defined interval to Splunk or other leading SIEM Consoles. That gives you complete visibility into your IBM i environment without the need for costly IBM i monitoring systems or for specialized, scarce, and costly IBM i expertise.

Comprehensive and powerful business intelligence reporting is at hand as users can easily search, analyze, and visualize IBM i log data along with log data from mainframe, distributed, and open-source systems. [Total visibility](#) in other words!

“ Ironstream for IBM i gives you complete visibility into your IBM i environment without the need for costly IBM i monitoring systems or for specialized, scarce, and costly IBM i expertise.



Features

Syncsort extends its market-leading data forwarding capabilities with Ironstream for IBM i. This release enables the forwarding of IBM i Machine (Log) data for IT Operations Analytics (ITOA) and Security Information and Event Management (SIEM) use cases.

- [Simple to install and configure](#)

Ironstream is fast to install and easily configurable through a user interface with no impact or modifications required on existing applications

- [Asynchronous and near real-time collection](#)

Provides the user with the flexibility to forward data near real-time (configurable to user-defined intervals right down to 1 second)

- [Multiple journals and data sources supported](#)

Data sources supported include the System Audit Journal, the Accounting Journal, System Examiner for system objects, values, profiles and more, Collection Services for operations and performance data

- [Multiple use cases supported](#)

Ironstream for IBM i supports a number of use cases for IT operations monitoring, service delivery, security monitoring, threat detection, problem detection and isolation, workload and resource management.

- [Multiple output formats and targets](#)

Ironstream for IBM support multiple output formats and configurable to forward data to Splunk and many other SIEM Consoles

- [Comprehensive log data streams available for ITOA and SIEM use cases](#)

Log data forwarded with Ironstream for IBM i includes security logs, message logs, system operations, performance data and more

- [User-defined formatting of information](#)

Flexibility in the formatting of the data forwarded to Splunk and other SIEMs is a key feature of Ironstream for IBM i. Users can also modify and filter the data to forward only what is most important to their specific use case

- [User Interface with powerful custom queries](#)

Through an intuitive User Interface, pre-built queries can be easily configured to select desired data fields and values