SpyLogix for FIM 2010
DATA SHEET

IDENTITYLOGIX™

Continuous Security Intelligence and Real-Time Data Actualization for Enterprise Information Assurance

HIGHLIGHTS

- Data View and Analysis
  - Quickview
  - Save favorite views
  - Query and analyze data "on demand"
  - Advanced view management capabilities
- Object and Activity Management
  - On-demand data discovery
    - FIM 2010 Events and Objects
    - Management Agent Events
    - Meta-verse via FIM2010
  - Continuous inline workflow activity monitoring
- Data Management Automation
  - Communications
  - Object / Event Handlers
  - Data pre- and post processing
  - Message streaming for high throughput
- Advanced Output Management
  - Report Scheduler
  - Program executable scheduler
  - ActionLogix
  - Exchange Data (PDF, Excel, HTML, CSV, and more)

SpyLogix Enterprise

- **SpyLogix Platform**
- **SpyLogix Modules**
  - User Security
  - Active Directory
  - Windows Server
  - VMware
  - Microsoft FIM 2010
  - LDAP Directory
  - CA SiteMinder
  - Radiant Logic
  - IdF Gateway (Mainframes)
  - Module SDK

SpyLogix for FIM 2010 is designed as an independent standalone system for increasing visibility into FIM 2010 activity. FIM 2010 activity is accessed through a provided custom logging activity for continuously monitoring details about requests processed within the FIM workflow engine, along with a baseline of existing/historical FIM 2010 audit data. This SpyLogix Module is configured and deployed through the FIM portal, so a FIM administrator can easily add the activity recorder to a workflow using the FIM Workflow Designer. The administrator can view data using an interactive console or automate monitoring using provided data actualization features.

Existing audit data may be periodically extracted to form an activity baseline of historical FIM audit data. Activities are continuously monitored, and changes are added to the baseline data recorded. Baseline data is essential for proper security reporting. Reports can be generated day one based on historical activity. Baseline security data is combined with continuously monitored activity workflow audit data by SpyLogix to form a complete system for reporting or automation.

All baseline and real-time audit data is made actionable by SpyLogix for data translation, event synthesis, alerting or triggering pre-programmed actions. SpyLogix helps to monitor proper FIM 2010 activity and assists organizations wanting enhanced efficiency and effectiveness for information security governance, risk control, and compliance services being conducted within the IT organization.

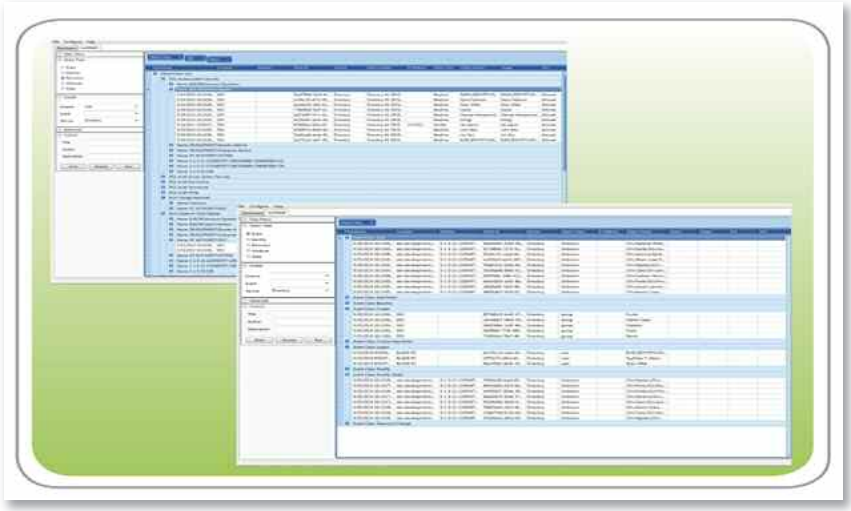

Figure 1. Interactive Console view of SpyLogix for FIM 2010

SpyLogix for FIM 2010 (Continued)

SpyLogix provides a complete audit and monitoring system for security intelligence and data actualization. SpyLogix will enable workflow monitoring, troubleshooting, and compliance reporting for FIM 2010 and other related enterprise resources involved with business information security.

SpyLogix for FIM 2010 is unique due to its architecture for efficient and effective organization and leverage of security data directly from FIM 2010's audit APIs and workflow activities. Data is intelligently stored to eliminate redundant data. Unreadable or obscure data elements can be synthesized into human readable form automatically. Programmable logic gateways make the data "actionable" for further automation. SpyLogix employs standardization, centralization, and automation to enable maximum process cost savings, reduce staff burden which raises productivity, and results in fewer resources to accomplish superior results.

OVERVIEW

Data Access

SpyLogix for FIM 2010 Module acquires FIM 2010 security (audit) data via product APIs to independently collect:

- Baseline historical FIM 2010 activity workflow audit data
- New activity workflow audit data

Security data is simply mapped into a standardized message format, and then communicated efficiently and safely for automatic processing by one or more centralized SpyLogix Platform server(s). SpyLogix for FIM 2010 Module technologies compromising Data Access may be described as:

- *Discovery* modules used to proactively create a baseline of persistently stored audit data using the FIM 2010 API, to which monitored changes may be subsequently compared.
- *Resource Monitoring* technologies are designed to consume real-time data from FIM 2010 APIs over a network connection using the included SpyLogix FIM 2010 activity workflow component.

Communication Services

Communication Services are available for safely communicating via a network connection or locally well-formed messages to the Message Services layer. Default message communication mode is high-performing streaming, unless remote sources are connected via unreliable network connection. Communication Services automatically support safe mode delivery of messages over less-reliable networks. Communication to Message Services is configurable (standard TCP/IP network link and configurable firewall port) and multi-threaded, so as to handle high-throughput utilizing multi-CPU servers.

Message Services

Message Services processes incoming well-formed messages employing either a SpyLogix Binary protocol or XML format. Web Services (data in) interface is provided to easily send (via a standard TCP/IP network and configurable firewall port) external data into SpyLogix Platform. Message Streaming efficiently moves messages to the Data Management layer for persistent storage.

Data Management

Data Management persistently manages all incoming data. Well-formed messages are 100% parsed. Selectively, non-human readable data types can be automatically translated into a human readable form. All data types are supported. Parsed and translated data with metadata is passed to the Storage Engine, a high performing component that ensures all security data types are persistently recorded non-redundantly with proper date/time context.

In-line workflow identity security visibility for IT governance, risk control and compliance.

For more Information

To learn more about IdentityLogix SpyLogix Platform, please visit identitylogix.com.

DATA Actualization

Data Actualization provides multiple post-storage processing services to effectively use incoming messages in real-time:

- *ActionLogix* is a series of components used to automatically analyze (filter) message content and trigger an action (see Alerts), synthesize events or forward messages to SpyLogix Platform(s):

  Policy Engine employs configurable programmatic logic gates (PLG) incorporating Boolean logic to automatically process message data. PLG deployment is expedited using message metadata, including: basic, state, RBAC, and utility. Any message passing PLG processing may trigger an action, for example, generate an Alert.

Basic (by meta-data	State (by object state)	RBAC (by Identity)	Utility
Service Name	Added	RBAC added	Counter
Service Category	Moved	RBAC Deleted	Timer
Event Class	Modified	RBAC Added To	
Object Class	Deleted	RBAC Deleted	
Object Name	None		
Identity			
Time			
Location			
Attribute (new)			
Attribute (old)			

  Alerts are embellished messages generated by blending standardized text with selected message data passing the Policy Engine rules, and then written to email, RSS, net send, a file, an application, Windows Event Log or SQL database. New output targets may be easily added.

  Synthesizers are Module specific events that are generated by analyzing message payload, drawing measured conclusions and storing a synthesized event persistently.

  Message Forwarder communicates intact well-formed messages to another network connected SpyLogix Platform. This capability is appropriate for cloud computing infrastructures or distributed SpyLogix Platform message aggregation for security data mining.

- Web Services (data out) provides as easy to use interface for sharing data with other software.
- Interactive Console enhances security intelligence visibility through tools for querying, analyzing and reporting on stored security data.
- Scheduler enables scheduling of Interactive Console reports for background execution. Other system assessment or scripts may be scheduled for periodic execution and feed data output into SpyLogix for Data Management, security intelligence or Data Actualization.

SpyLogix meets the performance and scalability requirements of some of the world's largest IT environments. SpyLogix Platform and Modules are designed to scale horizontally, vertically and functionally, making it possible for SpyLogix components to be distributed across computing realms to manage hundreds of thousands of users, thousands of applications and millions of entitlements.

SUMMARY

SpyLogix for FIM 2010 is an enabling technology for achieving business objectives tagged to identity management infrastructure using FIM 2010. Business and IT staffs are empowered with greatly improved visibility into FIM 2010 system operation.
Data Actualization features facilitate automated monitoring so businesses can accomplish more with fewer resources.

OPERATING ENVIRONMENT

- SpyLogix Platform is a prerequisite and runs on Windows. Recommended operation system platforms includes Server 2003, 2008 and 2008 R2
- SpyLogix for FIM 2010 Module runs on WIndows and requires network connectivity for access to its companion SpyLogix activity workflow component on a FIM 201 system.

IDENTITYLOGIX™ 9800 Connecticut Drive, Crown Point, IN 46307 ■ +1.219.379.5560 ■ info@idenitylogix.com