SpyLogix for
SiteMinder
Data Sheet

IDENTITYLOGIX™
Continuous Situational Awareness & Real-Time Security Intelligence for Web Access Mangement

HIGHLIGHTS

- **Security Intelligence**
  - Situational Awareness
  - 360º Visibility
  - Analysis and Reporting
    - Policy Data
    - Event Data
    - Performance Data
- **Continuous Data Access**
  - By API (no reliance on logs)
  - SpyLogix Message Design
- **Communication Services**
  - Message Broker
    - Multi-platform
    - Message Store/Forward
    - Message Mirroring
    - 1:Many Routing
  - Message Streaming
  - Web Services (data in)
- **Automatic Data Management**
  - Intelligent Data Handling
  - Historical Database
  - LINQ/Odata Enabled
- **Real-Time Data Actualization**
  - ActionLogix™
    - Policies
    - Alerts | Notifications
    - Event Synthesis
    - Message Forwarder
    - Extensibility Layer
  - Web Services (data out)
  - Interactive Dashboard
    - Data Query and Filter
    - Data Analysis
    - Reports
    - Data Export | Sharing
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - CA Directory
    - CA IdentityMinder
    - CA SiteMinder
    - IdF Gateway (IBM System z and i)
    - LDAPv3 Directory
    - MS Active Directory
    - MS IIS
    - MS FIM 2010
    - MS User Security
    - MS Windows Server
    - RadiantOne VDS
    - Sun Java System Directory Server
    - VMware vSphere
    - Module SDK

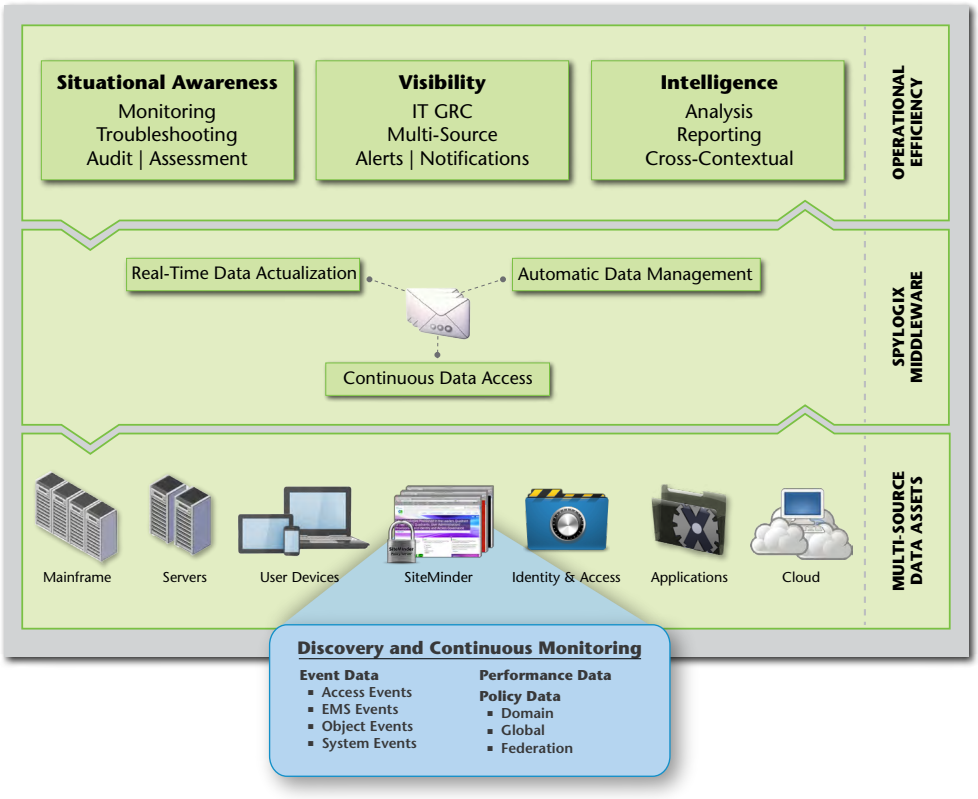
SpyLogix™ for SiteMinder is a module that works in conjunction with SpyLogix Platform to enable continuous monitoring of CA SiteMinder. SpyLogix for SiteMinder provides enhanced 360º visibility into SiteMinder policies, performance and activity in a single tool.

This 360º visibility information is critical for situational awareness, effective troubleshooting, performance monitoring, change management, or generating compliance and management reports. Benefits include improved business information security, lower IT costs, and improved staff effectiveness in maintaining application uptime.

SiteMinder velocity and volume of content creation only registers by recognizing that SiteMinder policy server can **process 10s of 1000s of logins/authorizations per minute** and SiteMinder debug logging facility can exceed **10 million log lines per hour** per policy server. Coupling SiteMinder enormous fine-grain monitoring with Spylogix for SiteMinder forensic sifting and data actualization technologies, helps focus system engineers and staff members efforts to solve the root cause of the imminent or potential problem in the system ecosystem.

The organizational impact of seamless integration of product features enables a reduction to meantime to recover (MTTR) and meantime between system incidents (MTBSI) simultaneously. Moreover, SpyLogix automation enables savings by not having to hire additional people or consume staff time in reducing MTTR and MTBSI.

SpyLogix for SiteMinder helps save time, money and resources for organizations supporting SiteMinder by monitoring, organizing and leveraging its policies, performance and event data in real-time. Data is pre-processed intelligently and managed automatically within historical context. SpyLogix Platform embeds data actualization technologies that includes an interactive dashboard for data query, analysis and output of security information in popular formats for reporting or exchange with other systems. ActionLogix™ post-processes automatically data for alerting, event synthesis, or message forwarding (to other SpyLogix Platform servers). In addition, a web services interface enables data to be shared with other software systems or information security processes.



OVERVIEW

SpyLogix for SiteMinder module designed to:

- Interface natively with SiteMinder and stream or collect policy, performance and activity data
- Build data into well-formed messages, and
- Send messages to any SpyLogix Platform server(s) for
    - Automatic data management
    - Real-time data actualization.

See the SpyLogix Enterprise data sheet for more information on automated data management, actualization, interactive console and more features included with prerequisite SpyLogix Platform software.

This SiteMinder data may be characterized by high volume, velocity and variety. SpyLogix for SiteMinder in conjunction with its prerequisite SpyLogix Platform is designed to handle SiteMinder's complex "Big Data" feed. This data may be used for management, troubleshooting or situational awareness of SiteMinder or any SiteMinder-enabled products, such as CA Federation Security Services, Federation Manager or SOA Manager.

SiteMinder support staff can use other modules, such as SpyLogix for Active Directory, CA Directory, CA IdentityMinder and/or other complimentary SpyLogix modules.

Event Data

SpyLogix for SiteMinder activity data is used for continuous awareness, troubleshooting and management. All activity data is acquired natively using the following SiteMinder's policy server event API:

Access Events

Authentication	**Authorization**
User authentication accepted	User authorization accepted
User authentication rejected	User authorization rejected
User authentication attempted	
User authentication challenged	
User session validated	
Administration	**Affiliate**
Administrator login	Visit occurred
Administrator rejected	
Administrator logout	

SpyLogix for SiteMinder provides enhnanced visibility into policies, performance metrics, and activities for efficient and effective continuous management of SiteMinder and enbled CA products.

For more information or to learn more about SpyLogix Enterprise, please visit
www.identitylogix.com

Entitlement Management Services (EMS) Events

EMS events occur when object created, updated or deleted actions are performed on directory objects, and relationships are formed between objects, such as membership.

Directory objects associated with EMS events include users, roles, organizations or generic (user-defined). Each object is associated with create, delete or modify events.

EMS events are classified according to category:

- **Administrative events** are generated when a user with sufficient privilege to modifies objects in a directory.
- **Session events** are generated when a session is initialized or terminated.
- **End-user events** are generated when a user self-registers or modifies their own profile.
- **Workflow Preprocess** events are generated when a workflow preprocess step is completed.

Object Events

SiteMinder environments contain elements called objects, such as: domains, policies, realms and user directories. Collectively, these persistent objects form an object store.

The following SiteMinder objects are associated with object events:

Object	Object Event Mapping
Agents	Agent Groups
Agent Types	Agent Type Attributes
Domains	Administrators
Policies	Policy Links
Password Policies	Registration
User Policies	User Directories
Realms	Management Commands
Responses	Response Groups
Response Attributes	Certification Mapping
Rules	Rule Groups
Authentication	Authentication and Authorization Mapping
Authentication Schemes	ODBC Query
Root	Root Configuration

After calling an object event, SiteMinder logs session activities to the objects. When an application logs into the object store, a new session is created. SiteMinder validates the login session and reports an appropriate event.

Authentication events are recorded upon user/application login for creative/modifying/updating an object, logout by user/application or login rejected.

Management commands produce object events about management functions, such as flushing cache and changing keys.

SpyLogix performs an on-demand baseline of all current object event data, and then continuously monitors objects events for changes, which are properly recorded.

System Events

SpyLogix records SiteMinder system events reflecting system and server-related activities.

SpyLogix records the following server activities:

- The server is initializing
- Which server initialization failed
- Which server is up/running
- Which server is down
- Text log cannot be opened
- Server heartbeat (every 30 seconds)

SpyLogix records the following system activities:

- Agent information
- Agent connection, connection failure and connect end to/from policy server
- Policy server connection, connection failure and connect end to/from database
- Policy server connection or connection failure to the LDAP directory
- Ambiguous resource match
- Ambiguous RADIUS match
- Agent DoManagement request

Performance Data

The following performance metrics are provided by SiteMinder and are recorded in SpyLogix for historical reference or trend analysis:

User Store Access	Policy Store Access	Key Store Access
Cache Find Count	Cache Success Count	Cache Miss Count
Protected	Authorizations	Validations
Threads Available	Threads in Use	Max Threads
Acct	Az	LogOuts
Admin	System	
Queue Length	Max Queue Length	
Priority Queue Length	Max Priority Queue Length	
Sockets Count	Max Sockets	

Policy Data

SpyLogix for SiteMinder retrieves policy object's and association's natively using SiteMinder's Policy Management API, then monitors objects and records changes, such as add, delete and modification activities.

Classification	SpyLogix Function	Captures content of a/an/all
Global / Domain	Rule	rule objects
Global / Domain	Policy	policy object
Global / Domain	PolicyLink	policy links associated with the specified policy object
Domain	Realm	realm object
Global / Domain	Response	response object
Domain	ResponseAttr	response attributes for the specified response
Domain	UserDir	user directory object
Global	Scheme	authentication scheme object
Global	Agent	agent object
Global	AgentTypeAttr	all agent type attributes
Global	Domain	the domain object
Global	Admin	administrator object
Global	ODBCQueryScheme	ODBC query scheme
Global	RegistrationScheme	registration scheme object
Global	PasswordPolicy	password policy object
Global	AuthAzMap	authentication and authorization directory map
Global	CertMap	certificate map
Global	VariableType	specified variable type object
Global	Variable	specified variable object
Global	TrustedHost	trusted host object
Global	HostConfig	host configuration object
Global	AgentConfig	agent configuration object
Global	Association	configuration parameters for an agent configuration object
Global	RegularExpression	regular expressions object belonging to a given password policy
Domain	SharedSecretPolicy	the current shared secret policy object
Federation	AffiliateDomain	affiliate domain object
Federation	Affiliate	affiliate object
Federation	SAMLAffiliation	existing SAML affiliation objects

SPYLOGIX PLATFORM OVERVIEW

SpyLogix for SiteMinder module streams or sends standardized, well-formed messages to one or more SpyLogix Platform servers for efficient and effective treatment by two major solution components:

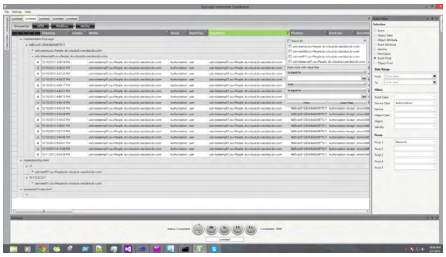
Data Management automatically pre-processes messages, stores and serves data, and

Data Actualization which provides multiple capabilities for using historic and real-time data.

Data Analysis

Data Actualization - Grid Editor

Grid Editor is designed to be intuitive for multi-source, cross-contextual analysis of stored data. For example, to easily view and analyze current activity and historic object changes. Or provide the flexibility to dynamically create views through drag and drop operations, presenting a single view of a user's session regardless of the location of activity.

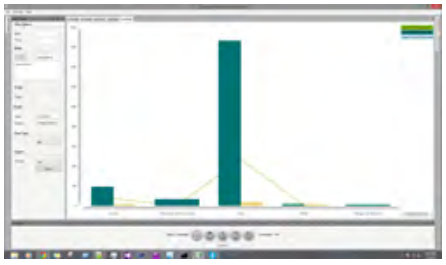


Feature Set	
Multi-source enabled	Grid Analysis
Object browser	- Manage multiple views
Data query editor	- Data element change detection
- Granular selection	- Row drill-down for details
- Pivot row/column selection	- Dynamically pivot | Group | Sort | Filter
- Run or run/refresh continuously	- Dynamically search on all data elements
	- Save favorite views

Data Visualized

Data Actualization - Chart Editor

Chart Editor is designed with maximum flexibility providing capabilities for charting any numeric or non-numeric data. Plots with millions of historical data points may be simultaneously refreshed in real-time to create operational dashboards or historical data trending.



Feature Set	
Granular data selection	Multi-source charting
Historical or streaming	Flexible data filter options
Plots millions of data points	Multiple chart selection
Numeric or non-numeric	Docking charts
Dynamic dra-able scales	Save favorite charts

ActionLogix

Data Actualization - Policy Based Analysis

ActionLogix analyzes streaming messages in real-time using graphically configured policies. Selectable actions include configurable alerts and pluggable actions. All message data is filterable using flexible state data, such as static and dynamic thresholds, within limits or Boolean logic. Events may be synthesized and saved based on streaming data. Messages may be filtered and forwarded to other SpyLogix Platform servers or IT services for closed-loop integration.

Feature Set	
Intelligent Alerts & Notifications	Event/Message Synthesis
- Policy Builder	- Build events for specific condition/result
- Easy to use workflow interface	Message Forwarder
- Real-time streaming analysis of incoming data	- Forward any message to any SpyLogix Platform or Dashboard
- Granular data filtering	Invoke automated actions such as scripts, widgets and applications
- All data elements actionable	
- Send via Email, RSS, Other	

Data Sharing

Data Actualization - Repurpose Data

A web service enables easy access and quick sharing of stored data with existing tools or IT services.

Stored data may also be shared interactively:

- By exporting viewed data to popular formats
  - PDF, HTML, Excel, CSV, Word, etc.
- Using existing Odata-enabled BI tools
  - CA, SAP, Excel Powerpivot and others
- Web Services (data out)
  - Restful Style Interface

SUMMARY

SpyLogix for SiteMinder organizes and leverages the "Big Data" (high data velocity, variety and volume) produced by SiteMinder, especially in multi-policy server environments. It can be positioned as an innovative and enterprise extensible security and governance middleware solution for continuous visibility for policy, performance and activity data. People and IT service process involved with SiteMinder can become more efficient and effective using SpyLogix for SiteMinder and SpyLogix Platform.

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