SpyLogix for
SiteMinder
Data Sheet

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

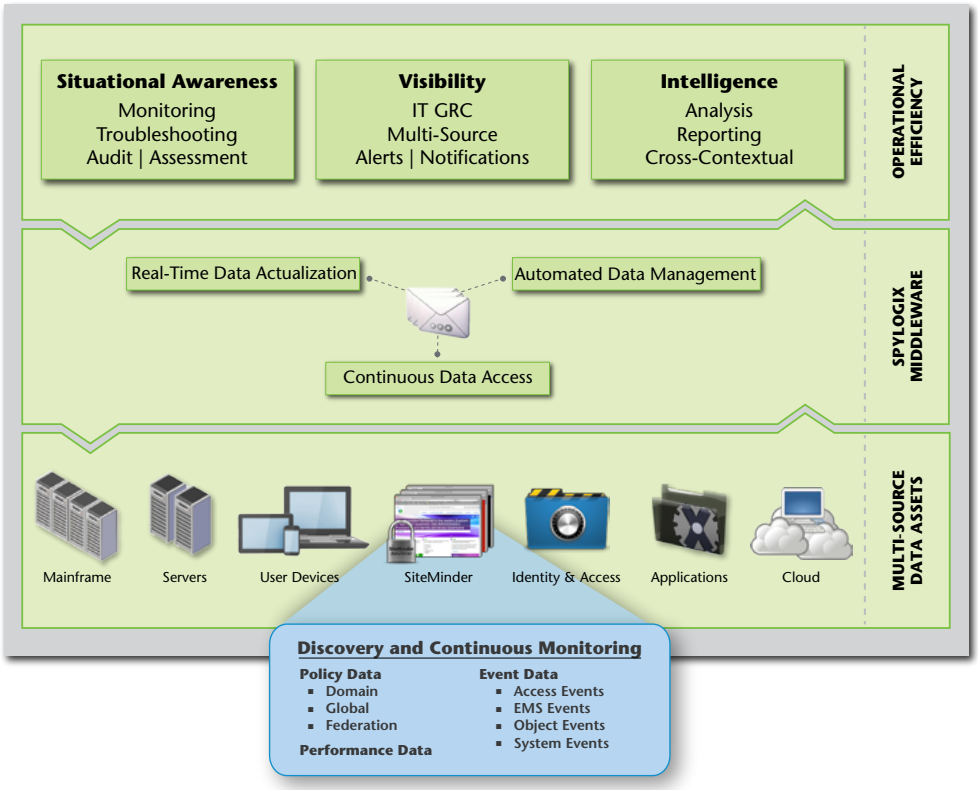
HIGHLIGHTS

- **Continuous Security Intelligence**
  - Situational Awareness
  - Enhanced Visibility
  - Analysis and Reporting
    - Policy Data
    - Event Data
    - Performance Data
- **Native 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)
- **Automated 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)
  - Report Scheduler
  - Interactive Console
    - Data Query and Filter
    - Data Analysis
    - Reports
    - Data Export | Sharing
- **SpyLogix Enterprise**
  - SpyLogix Platform
  - SpyLogix Modules
    - User Security
    - Active Directory
    - Windows Server
    - VMware vSphere
    - Microsoft FIM 2010
    - LDAP Directory
    - CA SiteMinder
    - Radiant Logic
    - IdF Gateway (IBM System z and i)
    - Module SDK

SpyLogix™ for SiteMinder is a module that works in conjunction with SpyLogix Platform to enable continuous management for enterprise web applications under SiteMinder control. This SpyLogix Enterprise system provides enhanced visibility into SiteMinder policies, performance and activity in a single tool. This information is critical for operational efficiency, effective troubleshooting, performance monitoring and change management, as well as, providing detailed reporting for compliance and governance activities. Organizations providing for continuous management greatly improve governance, risk and compliance control over critical information assets secured by SiteMinder.

Without SpyLogix separate tools and skills are needed to manage SiteMinder. Policies are viewed through the administration console. Performance data requires a separate tool. And activity would be tracked by enabling logging at appropriate points and periodically harvesting and preparing the data using an appropriate log management tool. But many organizations can miss detailed event information captured by policy server trace logs, which are difficult to process and correlate with smaccess log data. SiteMinder security data management requires significant investments in time, money and resources.

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



OVERVIEW

SpyLogix for SiteMinder is a module that is designed to continuously collect and leverage native security data from SiteMinder's policy servers to centralized SpyLogix Platform servers for advanced processing. SiteMinder policy, performance and activity data (acquired via native APIs) is organized into well-formed messages and sent by way of a message broker to one or more SpyLogix Platform servers for advanced processing.

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 operational awareness of SiteMinder or any SiteMinder-enabled products, such as CA Federation Security Services, Federation Manager or SOA Manager.

SiteMinder support staff may find it advantageous to use other modules, such as SpyLogix for Active Directory, LDAP and/or Radiant Logic. However, this data sheet covers only the SiteMinder module.

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 providers:

Access Events

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

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.

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 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

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	

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 nicely as an innovative and enterprise extensible security 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