SpyLogix for CA SiteMinder
DATA SHEET

HIGHLIGHTS

- Continuous Monitoring Real-Time
- Aggregates Security Events
- Interactive Console
- Smart Storage
- Secure Delegation
- Analyze, Report and Output
- Scheduled Reporting
- Automate Alerts & Actionable Triggers

IDx Enterprise Suite

- SpyLogix Pro
- SpyLogix Enterprise
- SpyLogix Modules

SpyLogix Modules

- User Security
- Windows Server
- VMware
- Active Directory
- LDAP Directory
- CA SiteMinder
- Microsoft FIM 2010
- IdF Gateway (Mainframes)
- Microsoft FIM 2010
- Custom Module Toolkit

Dynamically audit and monitor SiteMinder platform real-time...

SpyLogix for CA SiteMinder is an advanced software system that enables organizations to capture, aggregate, and analyze critical SiteMinder event information real-time directly from SiteMinder's event API. This information is critical for troubleshooting performance and availability issues, as well as providing detailed audit reporting for compliance and governance activities. Organizations that are able to provide continuous monitoring greatly improve their security posture, resulting in greater control of critical information assets that are secured by SiteMinder.

Without SpyLogix for CA SiteMinder, the security audit events are either logged locally or to a database but many organizations need the detailed event information that is only captured by in the SiteMinder Policy Server trace log. This information is logged to a text file but sorting through thousands of events that occur within a second is nearly impossible and correlating this information to the SMACCESS LOG requires significant investment in resources.

SpyLogix for CA SiteMinder continuously aggregates all security events with source context. Event data is parsed, classified, and packed into well-formed security messages for automated handling by SpyLogix Enterprise. Event data is automatically processed and intelligently stored with historical context. Unreadable or obscure data elements can be synthesized into human readable form automatically. Triggers make the data "actionable" for further automation. Finally, an interactive console enables viewing, analysis and output of security information in popular formats for reporting or exchange with other systems.

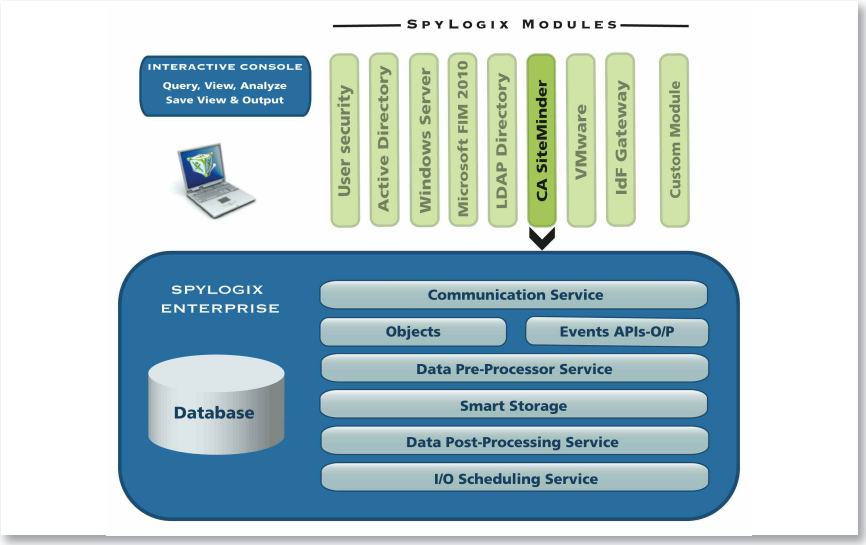

Figure 1. SpyLogix Enterprise Platform

SpyLogix for CA SiteMinder

SpyLogix for CA SiteMinder may be run with other SpyLogix modules, such as SpyLogix for Active Directory or LDAP Directories, to further enhance compliance and management reporting or security automation benefits.

SPYLOGIX ENTERPRISE

SpyLogix for CA SiteMinder and all SpyLogix modules leverage centralized automated data management and information exchange features of SpyLogix Enterprise, including:

- Network Services
- Message Handling
- Data Synthesis
- Smart Storage
- Alert/Action Triggers
- View, Analyze and Output
- Scheduling Service
- Integration

SpyLogix for CA SiteMinder is designed to work with SpyLogix Enterprise, a platform for managing security information from key business application or data realms, such as local/remote networks, Web (intranet and Internet), Unix/Linux, IBM mainframe, midrange and cloud based applications.

OVERVIEW

SpyLogix for CA SiteMinder is a security information and event management system for SiteMinder's Event API. Using SpyLogix helps automate burdensome management tasks and reduce complexity. For example:

- Send an email to the administrator when an application starts or a new policy is created
- Adjust event date/time stamps for reporting across multiple time zones
- Document automatically administrative activity for information security compliance audits

EVENT TYPES

SiteMinder generates four types of events that SpyLogix will consume.

Access Events

Access events result from four categories of user activities, including:

1. Authentication
   a. User authentication accepted
   b. User authentication rejected
   c. User authentication attempted
   d. User authentication challenged
   e. User session validated
2. Authorization
   a. User authorization accepted
   b. User authorization rejected
3. Administration
   a. Administrator login
   b. Administrator rejected
   c. Administrator logout
4. Affiliate - Visit occurred

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 modify 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 complete.
Workflow Post-process events are generated when a workflow post-process step is complete.

Object Events

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

Recorded object | object event mappings include:

Object	Object Event Mapping
Agents	Agent Groups
Agent Types	Agent Type Attributes
Agent Keys	Key Management
Domains	Administrators
Policies	Policy Links
Password Policies	Registration
User Policies	User Directories
Realms	Management Commands
Responses	Response Groups
Response Attributes	Certificate 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 in to the object store, a new session is created. SiteMinder validates the login session and reports an appropriate event.

SpyLogix records object events for an application or user login for changing an object, logout and login rejected.

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

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

HIGH AVAILABILITY BENEFITS

Troubleshooting SiteMinder high availability environments is significantly more complicated because these environments have multiple policy servers, which could span multiple data centers and time zones. Without SpyLogix organizations that deploy a high available architecture that uses dynamic web server and web agent load balancing are forced to route traffic to specific servers to facilitate troubleshooting activities.

SpyLogix for CA SiteMinder employs a design that supports dynamic event aggregation across multiple web servers and agents, thus avoiding traffic rerouting to facilitate troubleshooting activities.

IDENTITYLOGIX™ 9800 Connecticut Drive, Crown Point, IN 46307 ■ +1.219.922.8831 ■ info@idenitylogix.com