SpyLogix for Active Directory
DATA SHEET

IDENTITYLOGIX™

Dynamically audit and monitor Active Director real-time...

HIGHLIGHTS

- Discovery and Continuous Monitoring
- Fast and Easy-to-Use
- Scheduling Services
- Automated Data Management
- Active Direcory Message Simplification
- View, Analyze, and Report
- 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)
- Custom Module Toolkit

SpyLogix for Active Directory enables transparency and accountability for local network security provided by Microsoft's Active Directory (AD). Log management tools alone monitor AD event logs, leaving administrators to manually analyze and manage AD log data. SpyLogix for Active Directory discovers/monitors objects, permissions, and identity data, and makes it easy to audit AD local network access security.

The primary features of the Microsoft® Windows Server family security model are user authentication and access control. Active Directory directory service ensures that administrators can manage these features easily and efficiently.

Along with user authentication, administrators are allowed to control access to resources or objects on the network. To do this, administrators assign security descriptors to objects that are stored in Active Directory. A security descriptor lists the users and groups that are granted access to an object and the specific permissions assigned to those users and groups. A security descriptor also specifies the various access events to be audited for an object. Examples of objects include users, groups, files, printers, and services. By managing properties on objects, administrators can set permissions, assign ownership, and monitor user access.

It follows then, that as information-driven businesses grow, efficient and effective means to audit enterprise-wide use of AD is essential for ongoing governance, risk control, and compliance.

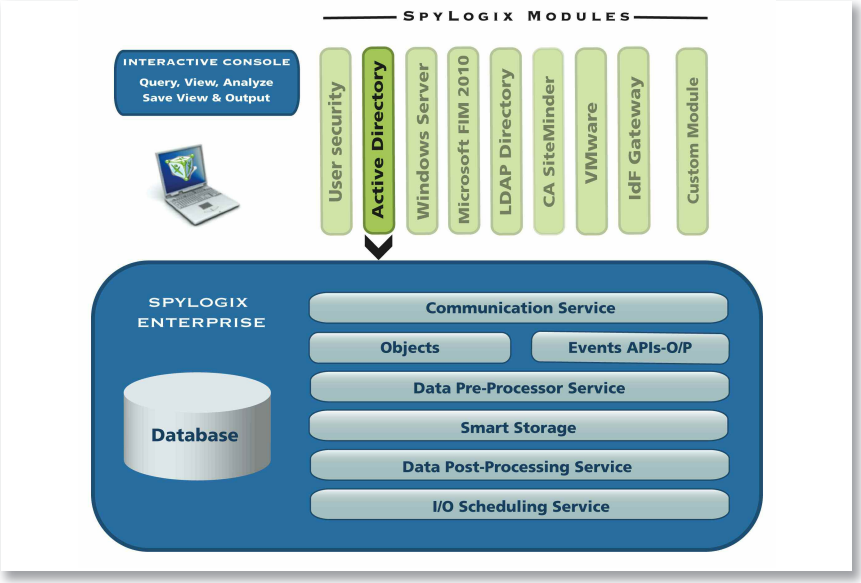

Figure 1. SpyLogix Enterprise Platform

SpyLogix for Active

DirectorySpyLogix for Active Directory enables businesses to manage this very important resource controlling user access for local network resources. The key to protecting enterprise business data begins with local network security provided by Active Directory (AD), because the local network is the entry point for users accessing and using business information.

OVERVIEW

Active Directory provides protected storage of user account and group information by using access control on objects and user credentials. Because Active Directory stores not only user credentials but also access control information, users who logon to the network obtain both authentication and authorizationto access system resources. For example, when a user logs on to access network resources, an assigned AD security system authenticates and authorizes the user with information stored in Active Directory. Then, when this user attempts to access a service on the network, the system checks access rights defined in the user's security descriptor.

Because Active Directory allows administrators to create group accounts, administrators can manage system security more efficiently. For example, by adjusting a file's properties, an administrator can permit all users in a group to read that file. In this way, access to objects in Active Directory is based on group membership.

Local network information security for a growing number of network resources, such as desktops, shared file services and applications, depend on Active Directory stored objects, attributes and permissions to enable secure access.
By periodically discovering and continuously monitoring AD using SpyLogix for Active Directory, governance, risk control, and compliance activities are simplified and conducted using less time, money, and human resources.

KEY FUNCTIONS

FAST AND EASY-TO-USE

Fast and Easy-to-Use self-service access to Active Directory objects, attributes and permissions empowers users with information that helps keep business data safe. IT staff used to providing information to consumers by writing scripts or supporting complex tools can recapture time for productive pursuits. An interactive console is used to sift quickly through potentially tens of thousands of identities or millions of object permissions using an interactive console to answer which accounts can change passwords or what accounts are in which groups.

To make data analysis and reporting more meaningful, date and time fields are reported by default relative to the local user.

SCHEDULING SERVICE

Scheduling service will free users from needing to access the console to run favorite reports. A simple scheduler will run SpyLogix in the background, a saved view, and an associated script to customize report delivery.

DISCOVERY AND CONTINUOUS MONITORING

Discovery and continous monitoring of Active Directory (AD) provides a complete reporting system on day one.
An on-demand discovery process records a baseline of AD so identity security and permissions analysis or reporting may commence day one. AD changes are recorded with date and time context. The result is a complete and independent historical analysis and reporting local network security audit system for enhanced management, risk control, and compliance reporting with no reliance on log management.

Each object or event record is prepared in a standard way to facilitate automated processing and usage of the data. Data records are parsed and well-formed messages are queued for safe delivery to a central SpyLogix server for processing.

AUTOMATED DATA MANAGEMENT

Automated data management means tedious burdensome IT staff work is eliminated, costs are reduced, and fewer resources are consumed to provide for managing and controlling enterprise AD networks. SpyLogix harvests messages and processes each data element per self-defining metadata. A pre-processor step handles translation of non-human attributes to human readable form.

Table A is a sample of SpyLogix User Account Control pre-processing:

SpyLogix UAC Event	AD Reported Event Description	
UAC: Script Executed	0x00000001	Logon script executed
UAC: Account Disabled	0x00000002	User account is disabled
UAC: Lockout	0x00000010	Account currently locked out
UAC: Interdomain Trust Account	0x00000800	Account from a trusted domain
UAC: Smartcard Required	0x00040000	user log on requires smart card

This capability improves IT staff productivity as log managers record for example, "user John modified userAccountControl: 509," which would have to be tediously translated to understand or act upon.

Arguably the power of AD for managing tens of thousands of identities and millions of permissions lies in its object inheritance model. However, this can make auditing of permissions quite difficult. SpyLogix for Active Directory navigates through AD access control lists (ACLs) to recover and report human readable permissions.

Table B is a sample of object ACL pre-processing performed by translating ACE bitmasks into discrete SpyLogix fields:

SpyLogix Permission	ACE Bitmask Description
Delete	The right to delete the object
CreateChild	The right to create children of the object
DeleteChild	The right to delete children of the object
ReadProperty	The right to read properties of the object
WriteDACL	The right to modify the DACL in the object Security descriptor

SpyLogix also correctly parses dynamic extended rights on AD objects. These values are retrieved from the AD scheme at runtime, for example mailbox permissions.

For efficiently storing audit data to save space and maximize online audit data for routine usage, SpyLogix uses a "smart storage" process to eliminate storing redundant audit data. Date and time context is preserved to accurately report.

A post-processor simplifies or synthesizes events by translating stored and/or incoming data, and re-stores an event that is human readable.

Table C illustrates simplification of user events by SpyLogix:

SpyLogix Simplification	Audit Data Conditions
Bad Password	if badPwdCount changed and badPasswordTime changed
Logon	If logonCount changed and lastLogon changed
Password Reset	if pwdLastSet changed

Table D illustrates synthesized identity events recorded by SpyLogix's post-processor that are derived from a single AD edit operation by an administrator:

SpyLogix Identity Events	
User Created	User Deleted
User Added to Group	User Removd from Group
Group Created	Group Deleted
Group Added to Group	Group Removed from Group

NOTE: *These events would not appear in any AD log.*

AUDITLOGIX

AuditLogix makes stored security data actionable without human involvement to perform more work with less time, money, and resources. This is an especially effective capability for sending alerts to confirm AD identity edits, like notifying managers when users have password change permission or reminding administrators to change their password. Any audit data change can trigger a programmable action.

SpyLogix enables businesses to manage risks associated with making information available so businesses can operate efficiently and effectively.

For more Information

To learn more about IdentityLogix SpyLogix for Active Directory, please visit Identitylogix.com.

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