



**IMPLEMENTING SOX
COMPLIANCE CONTROLS
WITH SCRIPTLOGIC**

A graphic of a white document with a blue header and a folded top-right corner, containing the following text:

**A ScriptLogic
Product
Positioning
Whitepaper**

JON ROLLS |

Table of Contents

INTRODUCTION 3

SARBANES-OXLEY - BACKGROUND 3

IMPLICATIONS ON IT 4

SOLUTIONS SUMMARY 5

REVIEW, DEVELOP AND IMPLEMENT ACCESS CONTROLS 6

 Example 1: Find Over-Privileged Users in Active Directory 6

 Example 2: Establish Consistent Active Directory Delegations..... 7

 Example 3: Manage Group Policies to Secure Users and Desktops..... 8

 Example 4: Review, Clean-Up, and Manage File Server, SQL and SharePoint Security 9

 Example 5: Securing the User’s Desktop 11

 Example 6: Securing Service Account Passwords 12

MAINTAIN ACCESS CONTROLS..... 13

 Example 7: Restore Active Directory Delegated Permissions..... 13

 Example 8: Auditing Active Directory Usage..... 13

 Example 9: Backup and Restore Windows, SQL and SharePoint Security 15

 Example 10: Audit File System Use 16

REPORT ON ACCESS CONTROLS 18

 Example 11: Report on Windows Security..... 18

 Example 12: Report on Active Directory Security..... 20

 Example 13: Report on Permissions 20

CONCLUSION..... 22

INTRODUCTION

ScriptLogic is a leading global provider of systems lifecycle management solutions spanning physical, virtual and terminal environments enabling IT professionals to proactively save time, increase security, and maintain regulatory compliance through the seamless management of Windows desktops, servers, and Active Directory. More than 22,000 customers of varying size and industry use ScriptLogic solutions to manage approximately 5.2 million desktops and servers every day.

ScriptLogic's software solutions help many different types of enterprise comply with the requirements arising from government legislation. The aim of this document is to highlight ways in which ScriptLogic solutions can be used to bring Microsoft Windows-based IT systems into line with the requirements of the Sarbanes-Oxley Act.

SARBANES-OXLEY - BACKGROUND

The Sarbanes-Oxley Act (SOX) was signed into law in July 2002 following a series of high profile scandals. Its objective is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. Sarbanes-Oxley imposes stiff penalties for company officers who fail to ensure the accuracy of their financial reports and further penalizes anyone who obstructs fraud investigations by destroying or altering records.

Publicly traded companies, public accounting firms and firms providing auditing services are all required to comply with Sarbanes-Oxley. Those with valuations over \$75 million are required to comply for fiscal years ending on or after November 15, 2004. All other public companies must comply for fiscal years ending on or after July 15, 2005.

With increased compliance requirements from legislation such as Sarbanes-Oxley, public companies need to have extensive internal control systems. Since much of a company's financial data resides on servers, responsibility for these internal control requirements fall on IT professionals. Network administrators and their management need tools to implement, maintain and report on access controls across the whole range of computer systems and data stores in their enterprise.

IMPLICATIONS ON IT

A large part of the legislation in Sarbanes-Oxley deals with accountancy practices such as procedures for dealing with auditors and the filing of SEC reports. The sections with most impact on IT systems are those that require companies to implement controls to minimize the risk of inaccurate financial statements or misuse of financial records, and to continually ensure that those controls are effective.

In simple terms, the sections of the Sarbanes-Oxley Act which are of most relevance to IT professionals are:

Section	Requirements
302: Corporate Responsibility for Financial Reports	Public company officers must certify the reliability of quarterly and annual financial statements, and must state that the company has established and maintained internal controls to ensure timely and accurate disclosure, highlighting any weaknesses in those controls.
404: Management Assessment of Internal Controls	Public companies must annually review and report on the effectiveness of their internal controls over financial reporting. The independent company auditor must also attest to, and report on, the accuracy of the report.
409: Real Time Issuer Disclosures	Public companies must be aware of, and declare, changes in their financial condition or operations within 48 hours of material events.
802/1102: Corporate and Criminal Fraud Accountability	Defines criminal penalties for altering or destroying documents relating to financial reports.

These sections affect a number of areas of a company's IT infrastructure, but one of the most important is that of managing access controls – securing the activities of users who come into contact with financial data, ensuring that only desired users can access it, and the security of the data itself. It is therefore critical to establish procedures and tools to inspect, document, repair and modify access controls for compliance with Sarbanes-Oxley. Timely reports, along with powerful, fast action tools are needed to ensure that the controls are in place and compliance is achieved.

SOLUTIONS SUMMARY

For companies implementing internal controls in order to comply with Sarbanes-Oxley, ScriptLogic software solutions give IT administrators the tools they need to secure and audit all aspects of their Windows-based infrastructure. Data related to SOX compliance can exist in File Systems, SQL databases and SharePoint sites within an organization and the security of all three need to be evaluated.

In order to bring a company into compliance, there are a number of software solutions that need to be considered. No single software product can make a company compliant, but software tools play an essential role in helping companies manage internal controls. ScriptLogic's software solutions give public companies the power to implement, maintain and report on internal access and security controls with minimal additional administrative burden.

ScriptLogic solutions that assist with Sarbanes-Oxley compliance	
Enterprise Security Reporter Enterprise Security Reporter for SharePoint	Reporting solution that generates instant, formatted reports on file permissions, users, groups, group memberships, printers, file shares, password weaknesses, security policies, SharePoint security and more.
Security Explorer Security Explorer for SQL Server Security Explorer for SharePoint	Security management solution that fixes, reports, searches, cleans-up and backs up all security settings on file servers, SQL Server and SharePoint. It also manages service and task security and settings.
Desktop Authority	Comprehensive desktop management platform that provides centralized configuration, inventory, support and security of Windows-based clients.
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.

Together, these products enable companies to implement controls that secure financial records, easily maintain those controls, and then report on their effectiveness, thus fulfilling a key requirement of Sarbanes-Oxley compliance. Implementing these controls can be divided up into three phases:

Three phases assisting with Sarbanes-Oxley compliance	
Review, Develop and Implement Access Controls	Review current internal controls, develop and implement new ones as needed. This should have been completed by 2004 or 2005, depending on company size.
Maintain Access Controls	Continual checks to ensure controls are in place and effective, at least quarterly, to enable management to report on effectiveness.
Report on Access Controls	Annual review of all internal controls, with extensive reporting requirements for auditors.

The remainder of this paper provides examples of how ScriptLogic products enable administrators to perform the necessary actions to ensure compliance with Sarbanes-Oxley.

REVIEW, DEVELOP AND IMPLEMENT ACCESS CONTROLS

When a company is reviewing its IT infrastructure in order to bring internal controls into line with Sarbanes-Oxley requirements, its IT administrators need tools to find and fix potential weaknesses, including:

- Over-privileged users
- Unsecured files and folders
- Improper group memberships
- Weak local computer policies
- Passwords set to never expire

When putting new controls in place for compliance, IT administrators need tools that simplify complex security settings and let them rapidly implement controls, including:

- Delegated permissions
- Group Policies
- Desktop Security
- Logon accounts used by Services

Example 1: Find Over-Privileged Users in Active Directory

ScriptLogic Solution: **Active Administrator**

At the heart of almost all Windows-based networks, Active Directory manages the security and privileges assigned to staff within an organization. ScriptLogic's Active Administrator offers a range of functions that enable effective management of these privileges.

For example, Active Administrator provides the ability to search for and generate reports on permission settings, as shown in Figure 1. These can be used to identify and restrict over-privileged users, preventing security risks such as:

- Unauthorized creation and modification of user accounts
- Changed group memberships to gain access to privileged information
- Addition of new computers into domains

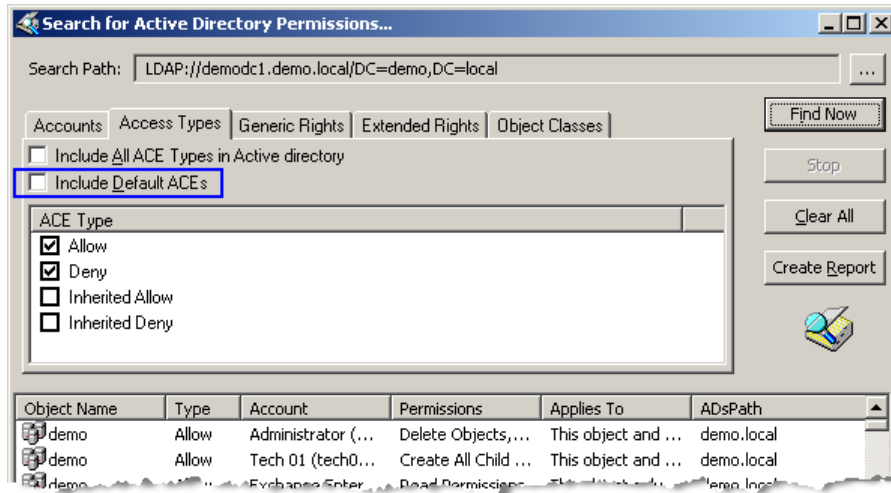


Figure 1: Optionally hide default permissions supplied in the AD Schema, making it easier to see added permissions.

Without these controls in place then the company might not be aware of fraudulent activity, and could not accurately report it as required by section 302(a)(5)(B) of the Sarbanes-Oxley Act.

Example 2: Establish Consistent Active Directory Delegations

ScriptLogic Solution: **Active Administrator**

The root of all delegation of permissions to resources lies within Active Directory: access to patient information on a server is granted via a group membership, whose membership management is assigned to an individual within IT, who was granted those permissions by an AD admin. So you see, it is important that your delegation of responsibility with AD be consistent. Active Administrator's Active Templates simplify control over the delegation of user rights in Active Directory, as shown in Figure 2. For example, Active Templates can be used to quickly delegate admin tasks such as the ability to update user information or group memberships to department managers and junior administrators.

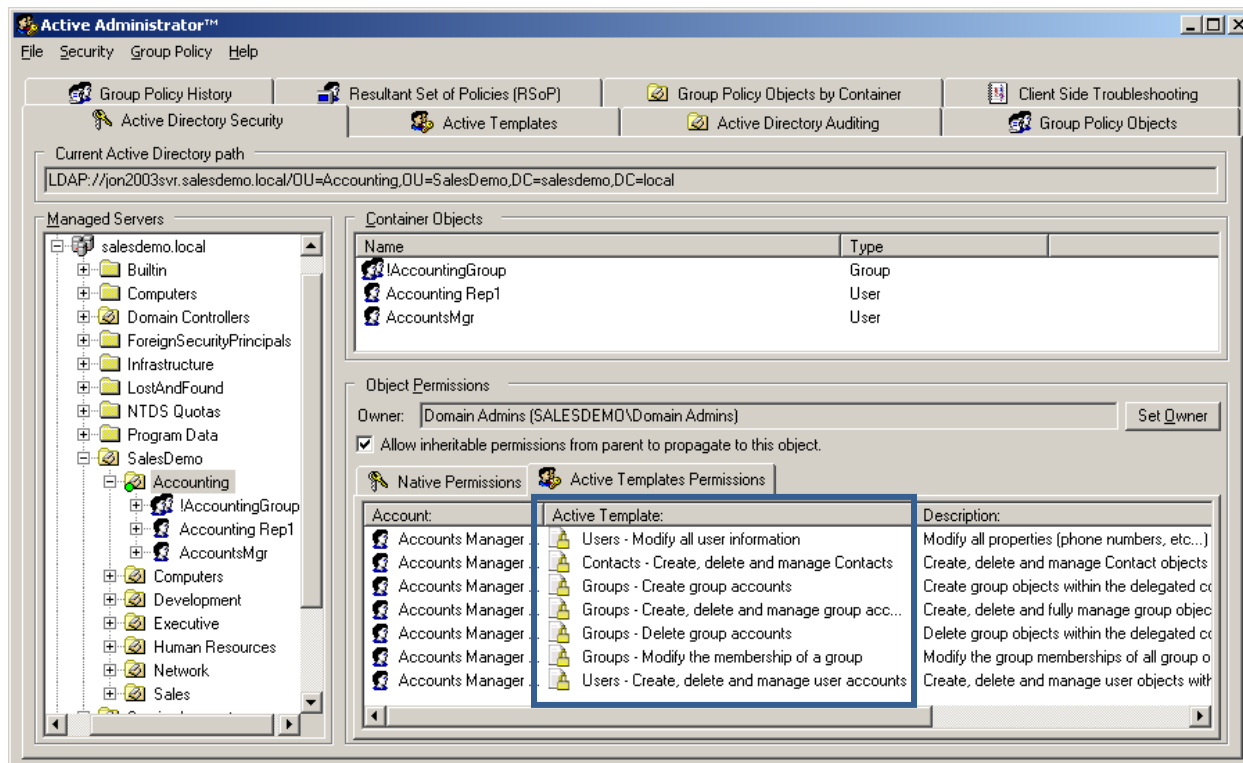


Figure 2: Each Active Template grants or revokes permissions consistently, simplifying delegation

Active Administrator can be configured to enforce the permissions assigned via Active Templates when changes are manually made to potentially circumvent established security standards. A service monitors all permissions delegated through Active Templates and can a) notify IT via email, b) re-enforce the delegated permissions or c) both.

Example 3: Manage Group Policies to Secure Users and Desktops

ScriptLogic Solution: Active Administrator

In Active Directory, Group Policies define security settings for computers and users whenever they connect to the network, and are a valuable tool for implementing the access controls required for compliance. Active Administrator provides management tools that provide enormous visibility and control over Group Policy Objects (GPOs) to help administrators manage the lifecycle of GPOs.

Active Administrator also provides an enhanced “Resultant Set of Policies” tool that analyzes the effect of combined Group Policies on an individual user or computer, as shown in Figure 3. Active Administrator goes beyond other RSoP tools with the ability to run what-if scenarios, and see the individual effect of each policy on the Resultant Set, including policies residing in Active Administrator’s Offline GPO Repository, where policies can be modified without affecting production desktops. Active Administrator can determine the RSoP for both Windows 2000 and 2003 Active Directory environments, and report on GPOs and RSoP in a range of formats.

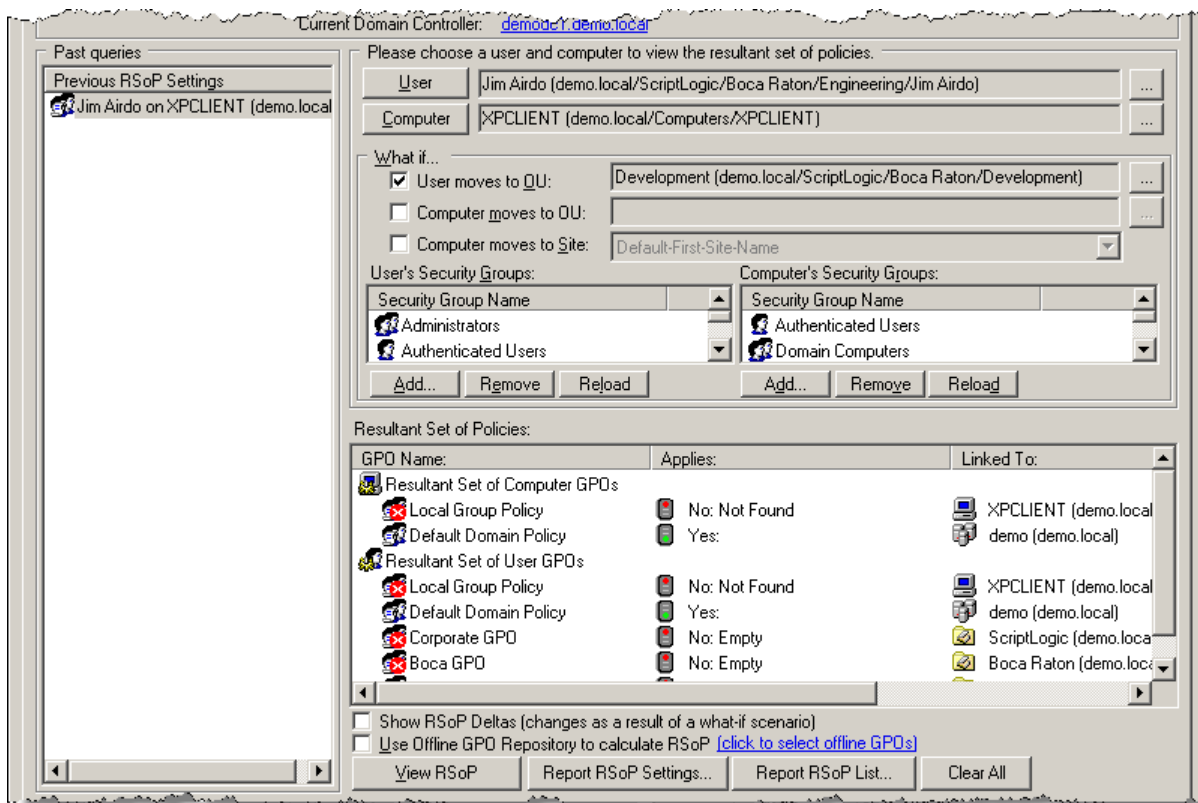


Figure 3: Calculating the RSoP allows you to ensure required security is enforced

Example 4: Review, Clean-Up, and Manage File Server, SQL and SharePoint Security

ScriptLogic Solution: **Security Explorer, Security Explorer for SQL Server, Security Explorer for SharePoint**

Security Explorer is a powerful and comprehensive security platform that inspects, reports and manages Windows NT/2000/XP/Vista and 2003 security on NTFS volumes, Registry keys, file shares, Printers, Services and Tasks. It additionally can provide the same functionality to SQL Server and SharePoint related data sets.

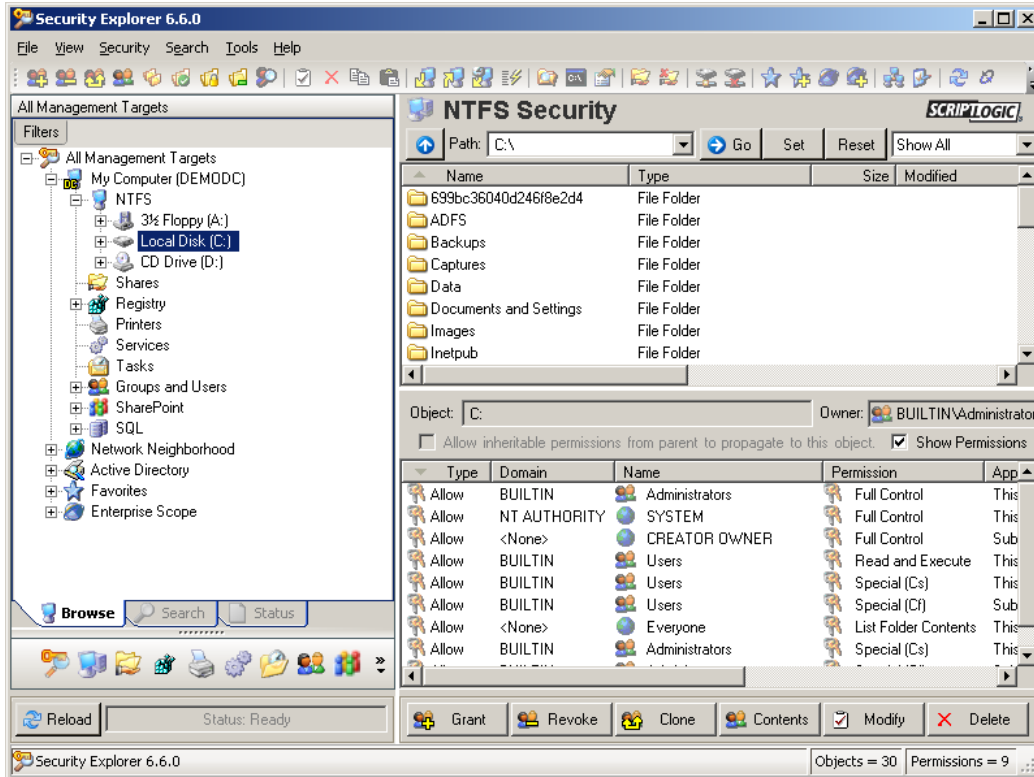


Figure 4: Security Explorer comprehensively manages Windows, SQL Server and SharePoint security

In the file system, Security Explorer dramatically eases the task of modifying permissions and ownerships of files throughout a file system, regardless of current ownership or inheritance settings. It can even force a standard set of permissions down a directory tree, overwriting all existing permissions for cleaning-up and securing file servers. Similarly, permissions to SharePoint sites and SQL Server-based databases and tables can be easily identified and modified as needed.

To ensure compliancy, file, database and SharePoint security are critical to enforcing control of access to financial data.

Security Explorer also has the ability to remove all permissions associated with unknown or deleted user accounts, as shown in Figure 5. For example, this prevents access to files from other Operating Systems that may be installed on workstations and servers.

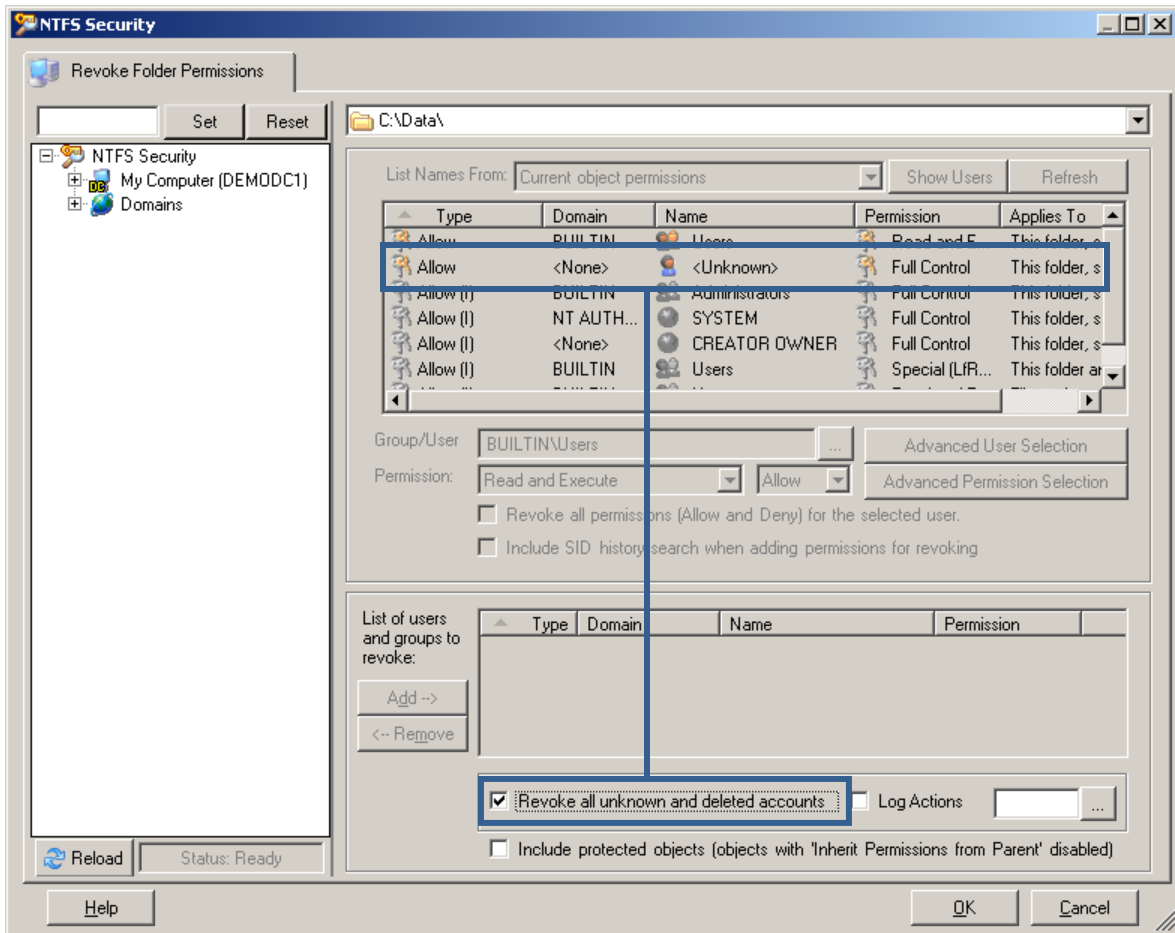


Figure 5: Security Explorer Cleans out all unknown or deleted accounts from ACLs

Example 5: Securing the User's Desktop

ScriptLogic Solution: **Desktop Authority**

The industry's leading desktop management solution for Windows-based networks, Desktop Authority enables administrators to proactively configure, manage and support desktops from a central location.

Desktop Authority includes such capabilities as:

- Roll-out Patches and Service Packs
- Deploy Anti-Spyware to protect against known vulnerabilities
- Lock down usage of USB ports, removable storage, wireless networking and more
- Deploy new security policies onto desktops with a high degree of granular control
- Restrict users from logging onto multiple desktops

Example 6: Securing Service Account Passwords

ScriptLogic Solution: **Security Explorer**

While most organizations take advantage of the default options to require users to change passwords, the most elevated accounts remain with password unchanged for countless days or months – Service Accounts. Often privileged with Domain Admin group membership, these accounts rarely have their passwords changed due to the sheer magnitude of work it would take to update, say, 20 services on 50 servers every 90 days!

Security Explorer is an enterprise-focused solution for managing the security of Windows operating systems. In addition to its ability to manage NTFS, Share, Printer and Registry security on Windows NT/2000/XP/2003 and Vista machines, it also manages Services and the accounts using them. With Security Explorer, a simple query of services using a particular service account or containing a part of a service name (such as “SQL”) will result in a list of services that can be simultaneously managed, as shown in Figure 6, where the service account passwords can be changed.

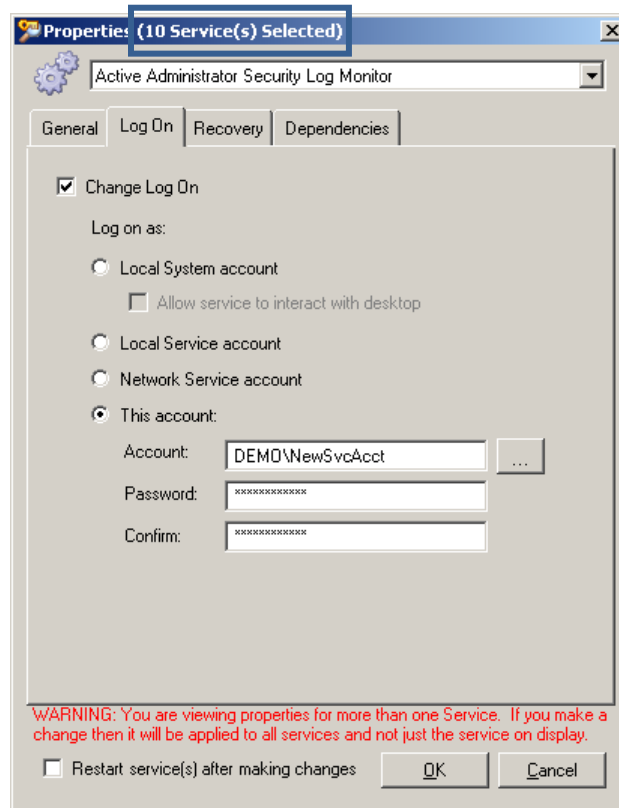


Figure 6: Multiple Services can be modified at once to modify service account passwords or other properties

MAINTAIN ACCESS CONTROLS

Sarbanes-Oxley and associated standards require that internal controls are also maintained once they have been established. IT administrators need tools that quickly help them assess whether controls have been weakened and let them recall security settings to restore compliance.

Example 7: Restore Active Directory Delegated Permissions

ScriptLogic Solution: **Active Administrator**

Active Administrator makes it possible to quickly review all delegated permissions that were set with Active Templates, and highlights those that have since been modified by other changes to Active Directory. Active Administrator lets administrators instantly re-apply the Active Template established permissions, as shown in Figure 7 to restore the user rights required for internal controls to be effective. Active Administrator also utilizes a service that can automatically repair and re-enforce the assigned delegations, ensuring a secure Active Directory.

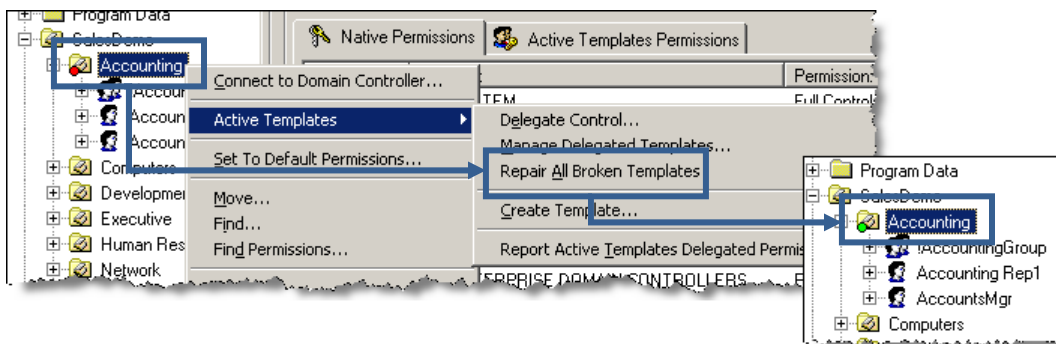


Figure 7: Broken delegations can be manually repaired or automatically enforced

Example 8: Auditing Active Directory Usage

ScriptLogic Solution: **Active Administrator**

Maintaining access controls requires an review of security changes in a organization's IT systems, as well as the ability to audit and analyze security settings for potential risks. Active Administrator takes analysis of Active Directory audit logs to a new level, combining and filtering logs from all domain controllers, storing them in a centralized secure database, and providing powerful reporting capabilities. This can be used to track new delegations and permission changes, the creation, modification and deletion of Active Directory objects and who made the changes, as shown in Figure 8. It also allows for long term storage of audit logs without the need for enormous event logs on individual servers.

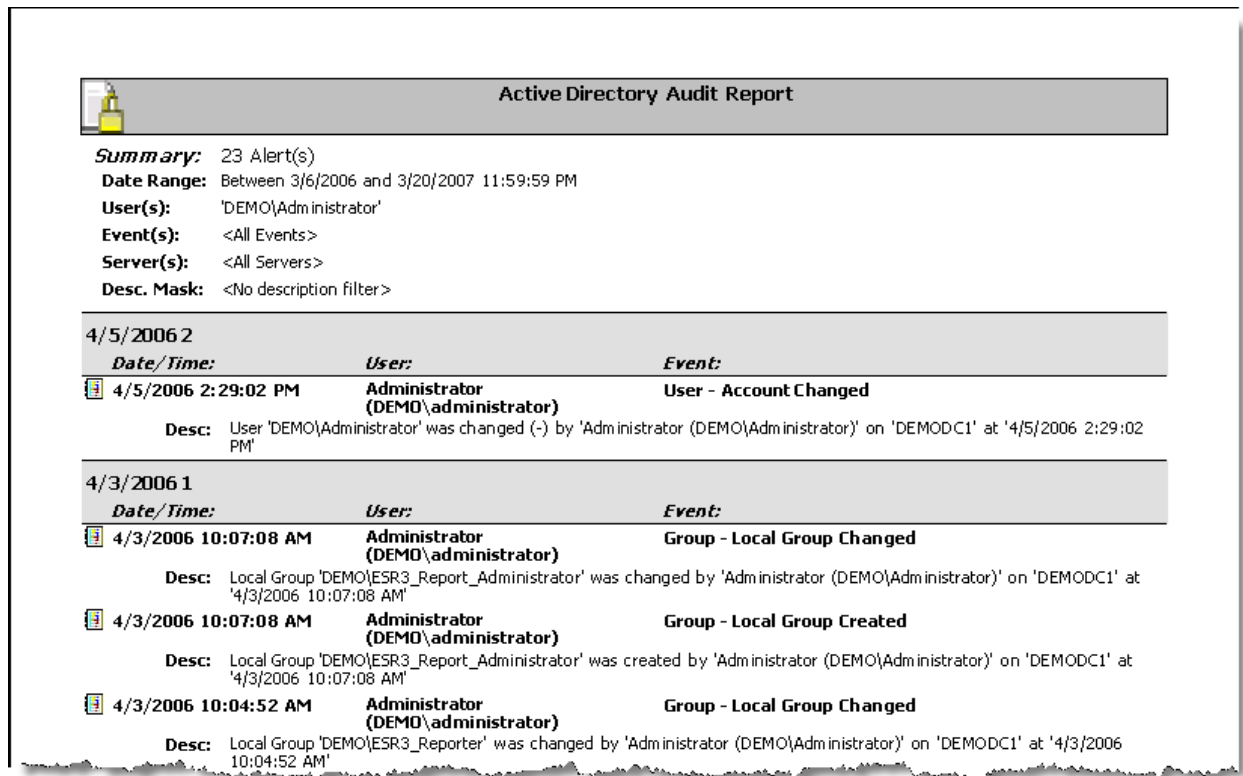


Figure 8: Active Administrator provides centralized reporting on all Active Directory activity

Active Administrator also provides the ability to track and audit changes in Group Policy Objects (GPOs). It shows the history of changes to GPOs and who made them, and allows the administrator to compare any two GPOs in history to see what was changed and undo changes if desired, as shown in Figure 9.

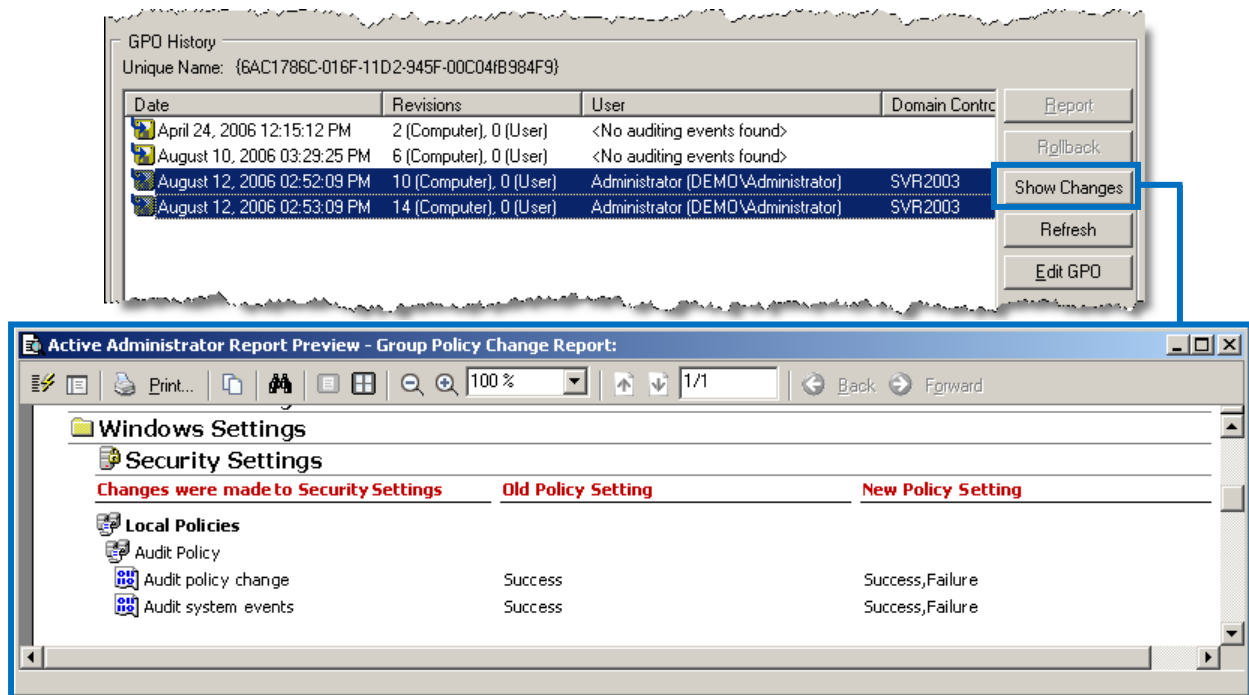


Figure 9: Reviewing Group Policy management activity with Active Administrator

Example 9: Backup and Restore Windows, SQL and SharePoint Security

ScriptLogic Solution: [Security Explorer](#), [Security Explorer for SQL Server](#), [Security Explorer for SharePoint](#)

Security Explorer provides the capability to backup all NTFS, Share, Registry, SQL and SharePoint permissions. Some administrators even use Security Explorer to perform hourly backups of the permission settings on their security-sensitive servers so that if a security breach is suspected and permissions appear to have changed, they can quickly reset all permission to the last-known fully-secured state without affecting the modified data.

Security Explorer can also dramatically simplify the recreation of permissions after a hardware failure and recreation of the file system, database or SharePoint site from backup tapes. The ability to quickly restore permissions settings, as shown in Figure 10, ensures that security is maintained and data is only available where intended.

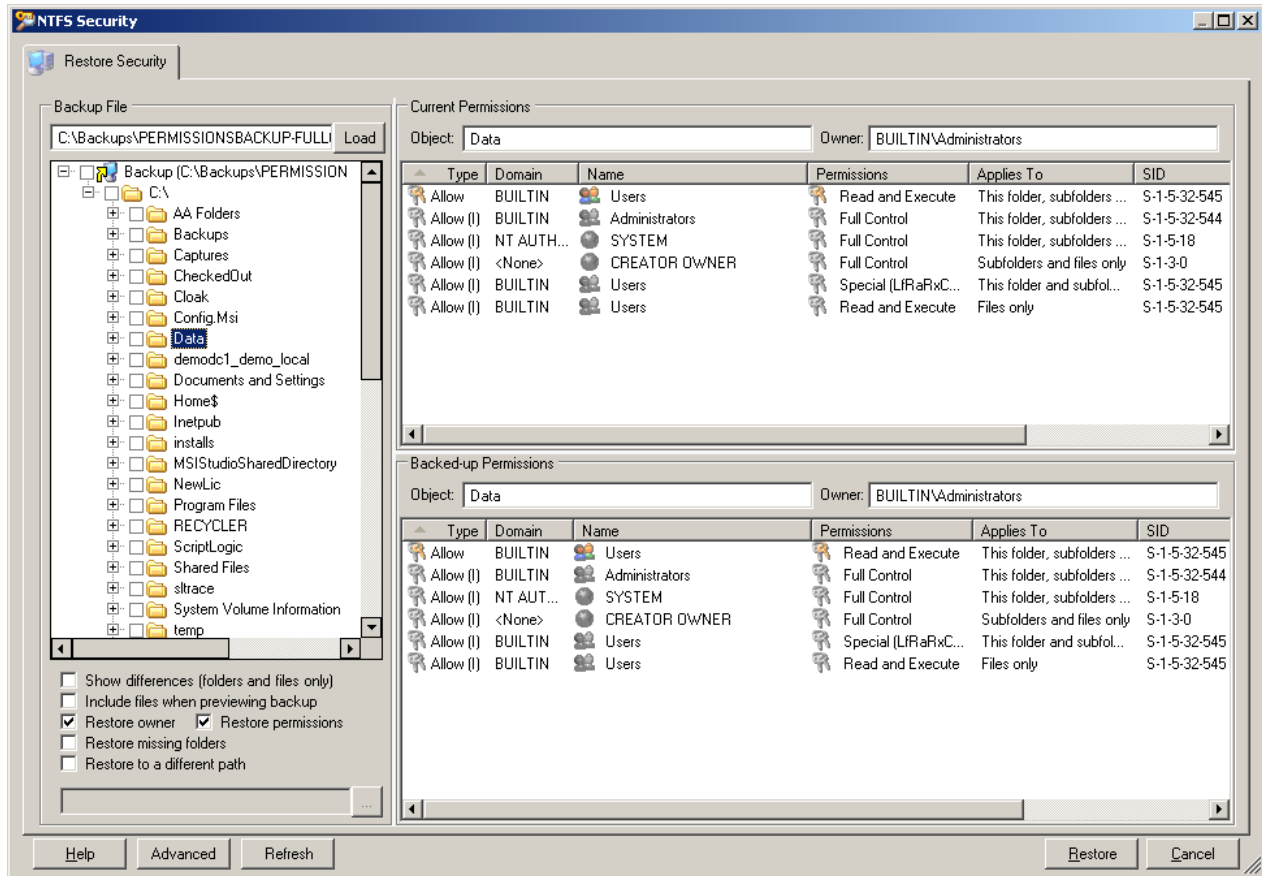


Figure 10: Restoring Share, Registry, SQL and SharePoint permissions is similar to restoring NTFS permissions, shown here

Example 10: Audit File System Use

ScriptLogic Solution: File System Auditor

Since information can find its way into formal letters, accounting spreadsheets, etc, it is vital to proactively have in place a solution that will detect, and notify IT of access (and denied access) to protected information. File System Auditor monitors all file system activity on Windows servers and centrally secures the logged activity information into a secure SQL Server-based audit trail. Activity can be reported on (as well as scheduled to be emailed when it occurs) using very simple to use criteria, shown in Figure 11.

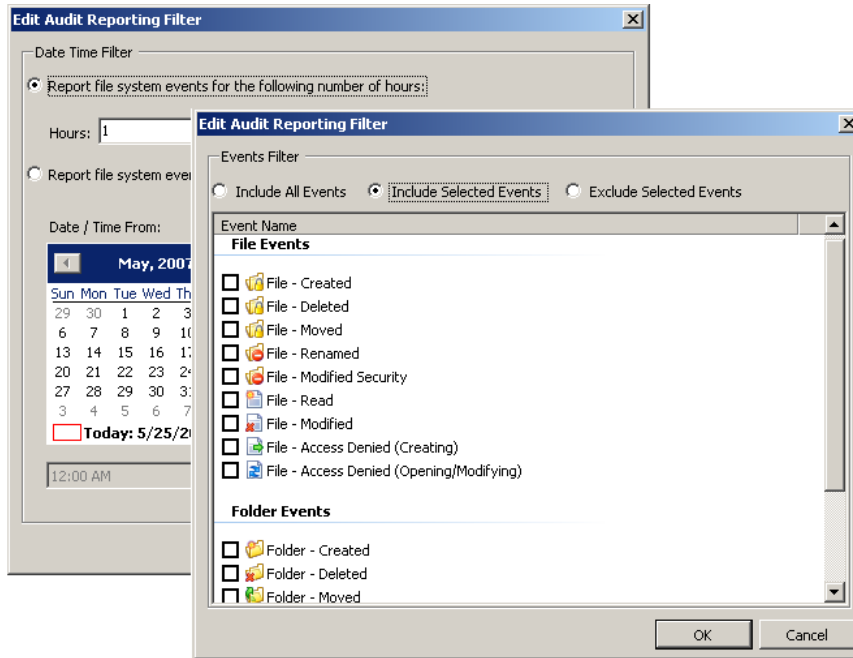


Figure 11: Selection of auditing criteria is a simple process.

Criteria is based on six elements, each graphically represented to promote a fast and simple method of retrieving audit results, as shown in Figure 12.

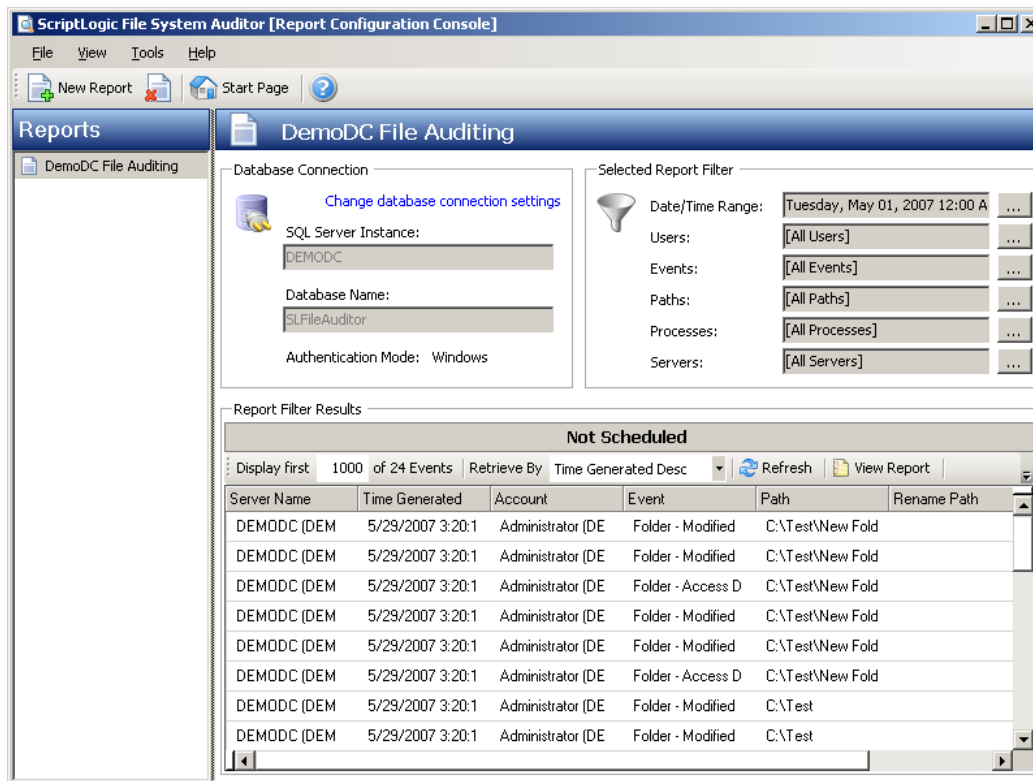


Figure 12: File system activity is centrally audited providing a trail for compliance use

REPORT ON ACCESS CONTROLS

Sarbanes-Oxley also requires that all internal controls can be reviewed and audited by independent third parties. IT administrators require tools that let them produce comprehensive reports on access controls, including:

- Permissions on files, folders, computers, group memberships, security policies and more
- Users, Groups, Computers (including OS/Service Pack) and other Active Directory objects
- “Special” settings on folders, which give access to selected users and groups

Example 11: Report on Windows Security

ScriptLogic Solution: **Enterprise Security Reporter, Enterprise Security Reporter for SharePoint**

Enterprise Security Reporter scans a network of Windows servers and workstations, as well as SharePoint sites, and analyzes the results using over 160 customizable, turn-key security reports. These reports also provide a formatted analysis of the security controls in place if needed during a review of SOX compliance by third parties. SOX-specific reports are already aligned to the security standards and are categorized within Enterprise Security Reporter, as shown in Figure 13.

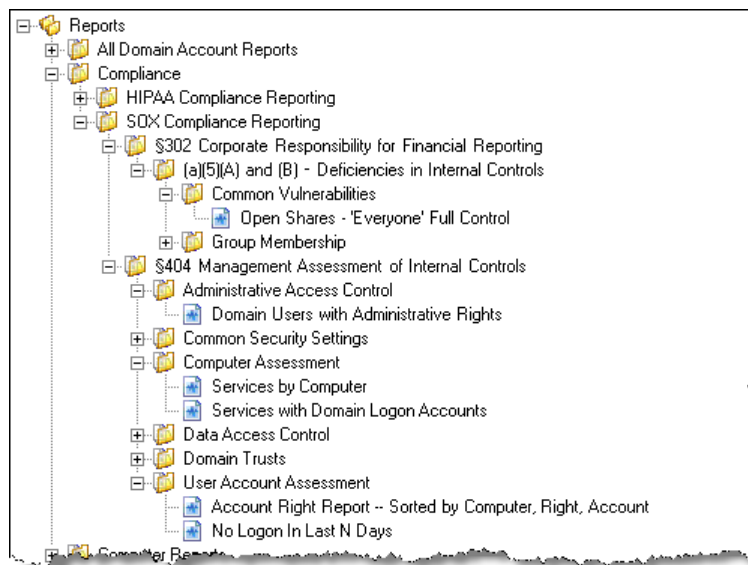


Figure 13: SOX Reporting is easy with Enterprise Security Reporter

As an example, the analysis of file permissions can be done using the “Delta Permissions Reporting” function, which only shows file and folder permissions which differ from the parent folder to make it easier to identify all permissions which have been “added” to the inherited NTFS permissions, as shown in Figure 14. The result is that this report is an essential report for tracking down over-exposed files and folders, which might reveal a breach of SOX requirements.

Path/Object Name	Account	Type	Permissions
+ NT AUTHORITY\NETWORK		Allowed	Special (RWX)(RWX)(RX)
- DEMO\Domain Admins (Designated administrators of the domain)		Allowed	
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir02.try\			
- DEMO\Domain Admins (Designated administrators of the domain)		Allowed	
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\			
- DEMO\Domain Admins (Designated administrators of the domain)		Allowed	
+ DEMO\Guests (Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted)		Allowed	Change (RWXD)(RWXD)(RWXD)
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir02.try\			
+ DEMO\Users (Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications)		Allowed	Change (RWXD)(RWXD)(RWXD)
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir03.try\			
+ {S-1-5-32-547}		Allowed	Full Control (All)(All)(All)
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir03.try\dir03.try\			
+ DEMO\Users (Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications)		Allowed	Read & Execute (RX)(RX)(RX)
\\2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir04.try\			
- DEMO\Domain Admins (Designated administrators of the domain)		Allowed	

Figure 14: Unusual permissions (such as granting access to the Guests group) can easily be found

Also, diving into the specific permissions assigned to resources will further enable you to assess the state of security. Enterprise Security Reporter’s ability to collect and report on SharePoint security dives all the way down to specific items stored on a SharePoint site. For example, the Site Item Explicit Permissions report, shown in Figure 15, highlights the permissions assigned to users and groups to give them access to SharePoint resources that may contain SOX-related data.

Site Item Explicit Permissions Report			12/4/2007 2:08:55 PM
Type	Item	Account	Permission Level
Selected Site(s): http://webapp1.qatest.local/sites/accounting			
http://webapp1.qatest.local/sites/accounting			Discovery Date: 12/4/2007 2:07:22 PM
List	Converted Forms		<input type="checkbox"/> Inherited
		Administrator (QATEST\administrator)	Full Control
		MOSS User (muser@qatest.local)	Full Control
List	Shared Documents		<input type="checkbox"/> Inherited
		Accounting Members	Contribute
		Accounting Owners	Full Control
		Accounting Visitors	Read
		Custom Accounting Group	Read
		Custom Accounting Group	Contribute
		Viewers	View Only
		Kenneth Ireland (migratedkireland@qatest.local)	Read
		Charles Clendenen (migratedcclendenen@qatest.local)	Read
		Charles Clendenen (migratedcclendenen@qatest.local)	Contribute
		Charles Cope (migratedccope@qatest.local)	Contribute
		Charles Cope (migratedccope@qatest.local)	Read
		MOSS User (muser@qatest.local)	Limited Access
		Barry Bidwell (migratedbbidwell@qatest.local)	Read
		John Israel (migratedjisrael@qatest.local)	Contribute

Figure 15: Quickly identify access to SharePoint resources

Example 12: Report on Active Directory Security

ScriptLogic Solution: **Active Administrator**

Active Administrator produces reports in a selection of formats for all users (across OUs), all computers managed by AD, all OUs, all Groups, and all non-default user rights and delegations, shown in Figure 16. These types of reports are critical to an auditor understanding where access originated; not just to finding group membership, but understanding who in the organization had permissions to assign group membership – truly all the way back to the source of a potential security problem.

The screenshot displays two overlapping report windows from the Active Administrator tool. The top window, titled "All Users", shows details for the "Administrator" user. The bottom window, titled "All Computers", shows details for two computers: "JON2003SVR" and "CLIENT".

All Users
LDAP://jon2003svr.salesdemo.local/DC=salesdemo,DC=local

Administrator
LDAP://jon2003svr.salesdemo.local/CN=Administrator,CN=Users,DC=salesdemo,DC=local
Full Name: Administrator Principal Name:
Last Name: First Name: MI:
Created: 4/23/2004 7:58 PM Title:
Changed: 8/11/2004 2:16 AM Home Directory: \\server\users\Administrator
Department: E-Mail:
Description: Built-in account for administering the computer/domain

All Computers
LDAP://jon2003svr.salesdemo.local/DC=salesdemo,DC=local

JON2003SVR
LDAP://jon2003svr.salesdemo.local/CN=JON2003SVR,OU=Domain Controllers,DC=salesdemo,DC=local
Operating System: Windows Server 2003 Version: 5.2 (3790) Service Pack:
Created: 4/23/2004 8:55 PM Changed: 8/10/2004 8:32 PM
DNS Host Name: jon2003svr.salesdemo.local Division:

CLIENT
LDAP://jon2003svr.salesdemo.local/CN=CLIENT,OU=Desktops,OU=Computers,OU=SalesDemo,DC=salesdemo,DC=local
Operating System: Windows XP Professional Version: 5.1 (2600) Service Pack:

Figure 16: Quickly report on the state of your Active Directory security

Example 13: Report on Permissions

ScriptLogic Solutions: **Security Explorer, Security Explorer for SQL Server, Security Explorer for SharePoint**

Security Explorer can produce reports on permissions for chosen groups or users on a selected volumes, shares, SQL Server databases, and SharePoint sites, (Figure 17 shows an example of NTFS permissions). To help discover over-exposed data and “unusual” permissions settings, Security Explorer can optionally reports permissions only where they differ from the parent folder.

Path	Account Domain	Account	Permissions	Owner	Owner
\\Jon2003srv\Users\	BUILTIN	Administrators	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\	NT AUTHORITY	SYSTEM	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\		CREATOR OWNER	Special(Not specified)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\	BUILTIN	Users	Special(RXCcCf)(RX)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	BUILTIN	Administrators	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	SALESDEMO	Domain Admins	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	SALESDEMO	!AccountingGroup	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	BUILTIN	Administrators	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	NT AUTHORITY	SYSTEM	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\		CREATOR OWNER	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\	BUILTIN	Users	Special(RXCcCf)(RX)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	BUILTIN	Administrators	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	NT AUTHORITY	SYSTEM	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	BUILTIN	Users	Special(RXCcCf)(RX)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	SALESDEMO	Domain Admins	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	BUILTIN	Administrators	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	SALESDEMO	Domain Admins	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	SALESDEMO	!AccountingGroup	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	NT AUTHORITY	SYSTEM	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\		CREATOR OWNER	Full Control(All)(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\	BUILTIN	Users	Special(RXCcCf)(RX)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\some data.txt	BUILTIN	Administrators	Full Control(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\some data.txt	NT AUTHORITY	SYSTEM	Full Control(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\some data.txt	BUILTIN	Users	Read & Execute(RX)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\some data.txt	SALESDEMO	Domain Admins	Full Control(All)	BUILTIN	Administrators
\\Jon2003srv\Users\AccountingRepl\Data\some data.txt	SALESDEMO	!AccountingGroup	Full Control(All)	BUILTIN	Administrators

Figure 17: Assess the permissions assigned to NTFS files and folders.

CONCLUSION

The Sarbanes-Oxley Act requires considerable effort by most public companies in order to have controls in their financial reporting and into compliance by 2004-5. Much of the work is in developing and implementing business processes, and ensuring that employees handling financial data work within those controls.

However, it is equally important that public companies fulfill the wider security and access control implications of Sarbanes-Oxley and accompanying standards from other bodies. These largely fall on the shoulders of IT administrators, who need tools to implement, maintain and report on access controls across the whole range of computer systems and data stores in their enterprise.

For Windows-based systems, ScriptLogic software solutions give IT administrators the tools they need to manage these controls throughout their lifecycle, and ensure they play their part in bringing their company into compliance with Sarbanes-Oxley.

ScriptLogic solutions that assist with Sarbanes-Oxley compliance	
Enterprise Security Reporter Enterprise Security Reporter for SharePoint	Reporting solution that generates instant, formatted reports on file permissions, users, groups, group memberships, printers, file shares, password weaknesses, security policies, SharePoint security and more.
Security Explorer Security Explorer for SQL Server Security Explorer for SharePoint	Security management solution that fixes, reports, searches, cleans-up and backs up all security settings on file servers, SQL Server and SharePoint. It also manages service and task security and settings.
Desktop Authority	Comprehensive desktop management platform that provides centralized configuration, inventory, support and security of Windows-based clients.
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.

For more information on how ScriptLogic can help you achieve SOX compliance please visit www.scriptlogic.com/sox, or contact your ScriptLogic sales representative or Authorized ScriptLogic Channel Partner.