



Implementing COBIT Compliance with ScriptLogic

A ScriptLogic Product Positioning Paper

By Nick Cavalancia

Table of Contents

INTRODUCTION	3
COBIT OVERVIEW	3
ADMINISTRATIVE AND TECHNICAL CONTROLS	4
Planning & Organization	4
Acquisition & Implementation.....	4
Delivery & Support.....	5
Planning & Organization	5
SOLUTIONS SUMMARY	6
Example 1: Ensure External Compliance.....	7
Example 2: Use Active Templates to Delegate AD Permissions	7
Example 3: Enforce AD Permissions through Self-Healing Active Templates.....	8
Example 4: Centrally Establish File System, Share, Database and SharePoint Permissions.....	9
Example 5: Manage Group Policies to Secure Users and Desktops.....	10
Example 6: Maintain GPO History.....	11
Example 7: Distributing Software	12
Example 8: Auditing Active Directory Usage.....	14
Example 9: Restore Active Directory and Active Directory Security.....	15
Example 10: Restoring Server Security	17
Example 11: Audit Server Security Permissions.....	18
Example 12: Ensure Up-To-Date Patches Have Been Applied	20
Example 13: Scan for Known Spyware on Desktops.....	21
Example 14: Remotely Manage Clients	22
Example 15: Assess State of Patching.....	22
Example 16: Audit File System Usage	23
CONCLUSION.....	26

INTRODUCTION

ScriptLogic is a leading global provider of systems lifecycle management solutions spanning physical, virtual and terminal server 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 19,000 customers of varying size and industry use ScriptLogic solutions to manage approximately 4.7 million desktops and servers every day.

ScriptLogic's software solutions help many different types of enterprises comply with the requirements that arise 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 Health Insurance Portability and Accountability Act.

COBIT OVERVIEW

Control Objectives for Information and related Technology (COBIT), now in its 3rd edition, was designed by the IT Governance Institute to better define IT processes and resources and tie them to business strategies and goals. Its 318 detailed control objectives and 34 high-level control objectives fall into four main categories, or "domains:" Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. By viewing IT as a process (which the four domains outline) and tying that process to business objectives, IT not only ensures adequate control over its systems, but the business itself also gains an advantage over its competition.

Additional information on COBIT can be found at <http://www.isaca.org/cobit>.

ADMINISTRATIVE AND TECHNICAL CONTROLS

Because there are 318 specific control objectives and only 4 domains (one being too detailed and the other not enough), in this document, we will focus at the level of the 34 control objectives, covering those objectives that ScriptLogic solutions assist with implementing in Windows-based networks.

The following table lists the control objectives dictated by COBIT (separated into the four domains) that ScriptLogic assist with and the necessary actions to be taken in order to comply with COBIT standards.

Planning & Organization

Objective	COBIT Control	Action Required
P08: Ensure Compliance with External Requirements	8.2 Practices and Procedures for Complying with External Requirements	Identify the controls that you need in order to comply with legal requirements
P08: Ensure Compliance with External Requirements	8.2 Practices and Procedures for Complying with External Requirements	Identify the controls that you need in order to comply with legal requirements

Acquisition & Implementation

Objective	COBIT Control	Action Required
AI3: Acquire and Maintain Technology Infrastructure	3.3 System Software Security	Ensure security of data and programs based on configuration
	3.6 System Software Change Controls	Ensure controlled changes to systems
	3.7 Use and Monitoring of System Utilities	Monitor and evaluate the use of systems
AI6: Manage Changes	6.2 Impact Assessment	Monitor changes made to systems in real time for change management purposes
	6.3 Control of Changes	Ensure controlled changes to systems
	6.8 Distribution of Software	Ensure the correct software is installed on the correct machines

Delivery & Support

Objective	COBIT Control	Action Required
DS4: Ensure Continuous Service	4.3 IT Continuity Plan Contents	Develop procedures to restore systems to a pre-incident state
DS5: Ensure Systems Security	5.1 Manage Security Measures	Assess the impact on a potential change and monitor the implementation of that change
	5.2 Identification, Authentication and Access	Restrict access to resources to appropriate personnel
	5.5 Management Review of User Accounts	Review access rights periodically
	5.6 User Control of User Accounts	Be alerted to unusual administrative activity
	5.7 Security Surveillance	Administrative security violations should be recorded and reported
	5.19 Malicious Software Prevention, Detection and Correction	Protect machines from malicious software
DS8: Assist and Advise Customers	8.1 Help Desk	Establish a help desk function
DS9: Manage the Configuration	9.2 Configuration Baseline	Establish a configuration baseline
	9.3 Status Accounting	Establish history of changes
	9.4 Configuration Control	Periodically check recording of IT configuration
DS11: Manage Data	11.23 Back-up and Restoration	Implement Backup and restore procedures

Planning & Organization

Objective	COBIT Control	Action Required
M1: Monitor the Process	1.4 Management Reporting	Generate reports depicting progress toward identifiable goals
	2.1 Internal Control Monitoring	Monitor access made to systems in real time to audit implemented controls
	2.4 Operational Security and Internal Control Assurance	Monitor changes made to systems in real time to ensure operations are made within established controls

Together, these products enable companies to implement controls that secure systems, easily maintain those controls, and then report on their effectiveness, thus fulfilling key requirements of COBIT compliance.

The remainder of this paper provides examples of how ScriptLogic solutions enable administrators to perform the necessary actions to implement COBIT compliance controls.

SOLUTIONS SUMMARY

ScriptLogic software solutions give organizations that are implementing internal controls in order to comply with COBIT the tools they need to evaluate, secure and audit all aspects of their Windows-based infrastructure.

In order to bring an organization 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 agencies manage internal controls. ScriptLogic’s software solutions provide the power to implement, maintain and report on internal access and security controls with minimal additional administrative burden.

ScriptLogic solutions that assist with COBIT compliance	
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
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, 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, SQL, and SharePoint servers. It also manages service and task security and settings.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.
Desktop Authority	Comprehensive desktop management platform the provides centralized configuration, inventory, support and security of Windows-based clients.
Patch Authority Ultimate	Centralized patching solution providing both Microsoft and select third-party patching of Windows desktops and servers.

Together, these products enable companies to implement controls that secure systems containing patient health information, easily maintain those controls, and then report on their effectiveness, thus fulfilling key requirements of COBIT compliance.

The remainder of this paper provides examples of how ScriptLogic products enable administrators to perform the necessary actions to implement COBIT compliance controls.

Example 1: Ensure External Compliance

Related Objective: **P08 - Ensure Compliance with External Requirements**

Section 8.2 states that an organization should “ensure that appropriate corrective actions are taken to guarantee compliance with external requirements.” ScriptLogic solutions assist in the compliance of regulatory standards such as Sarbanes-Oxley, HIPAA, GLBA, FISMA, and FIPS 200 using the very same solutions and features listed throughout this document. Visit <http://www.scriptlogic.com/compliance> for more information.

Example 2: Use Active Templates to Delegate AD Permissions

Related Objectives: **A13 - Acquire and Maintain Technology Infrastructure / DS5 - Ensure Systems Security / DS9 - Manage the Configuration**

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 1. 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.

Active Templates harness the power and granularity of Active Directory without the complexity and guesswork of dealing with lists of user rights, and can be easily granted and revoked. Active Templates ease the job of the IT Administrator using Active Directory to comply with COBIT requirements.

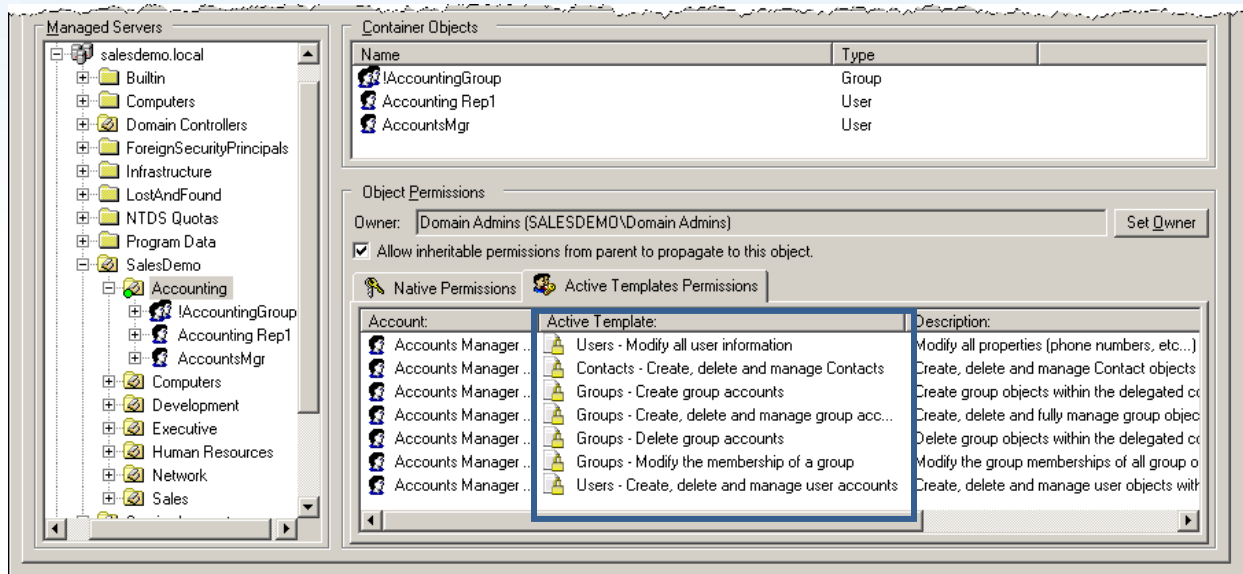


Figure 1: Each Active Template grants or revokes permissions consistently, simplifying delegation

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: Enforce AD Permissions through Self-Healing Active Templates

Related Objectives: **A13 - Acquire and Maintain Technology Infrastructure / DS5 - Ensure Systems Security / DS9 - Manage the Configuration**

ScriptLogic Solution: **Active Administrator**

Active Administrator also makes it possible to quickly review all delegated permissions that were set with Active Templates by first identifying those locations that use Active Templates with a green marker, and highlights those that have since been modified by other changes to Active Directory by changing the marker to red. Active Administrator lets administrators instantly re-apply the Active Template to restore the user rights required for compliance with COBIT standards, or Active Administrator can be configured to automatically reinforce the permissions originally assigned through an Active Template.

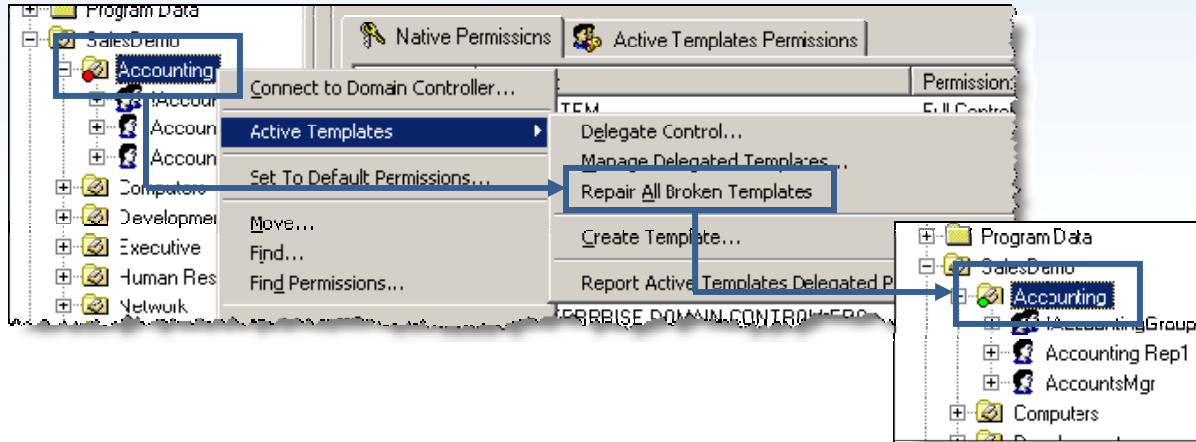


Figure 2: Active Directory security can be manually repaired or automatically reinforced.

Example 4: Centrally Establish File System, Share, Database and SharePoint Permissions

Related Objectives: **A13 - Acquire and Maintain Technology Infrastructure / DS5 - Ensure Systems Security**

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

While Windows, SQL and SharePoint servers can be secured in a one-off fashion, the consistency desired by sections 3.3 (System Software Security) and 5.2 (Identification, Authentication and Access) can only be accomplished by using a solution that will both centrally establish permissions and be able to replicate the permissions across multiple servers, shares, file systems, databases and Sites. As shown in Figure 3, Security Explorer can not only manage permissions on these various systems, but permissions can be cloned to maintain consistency.

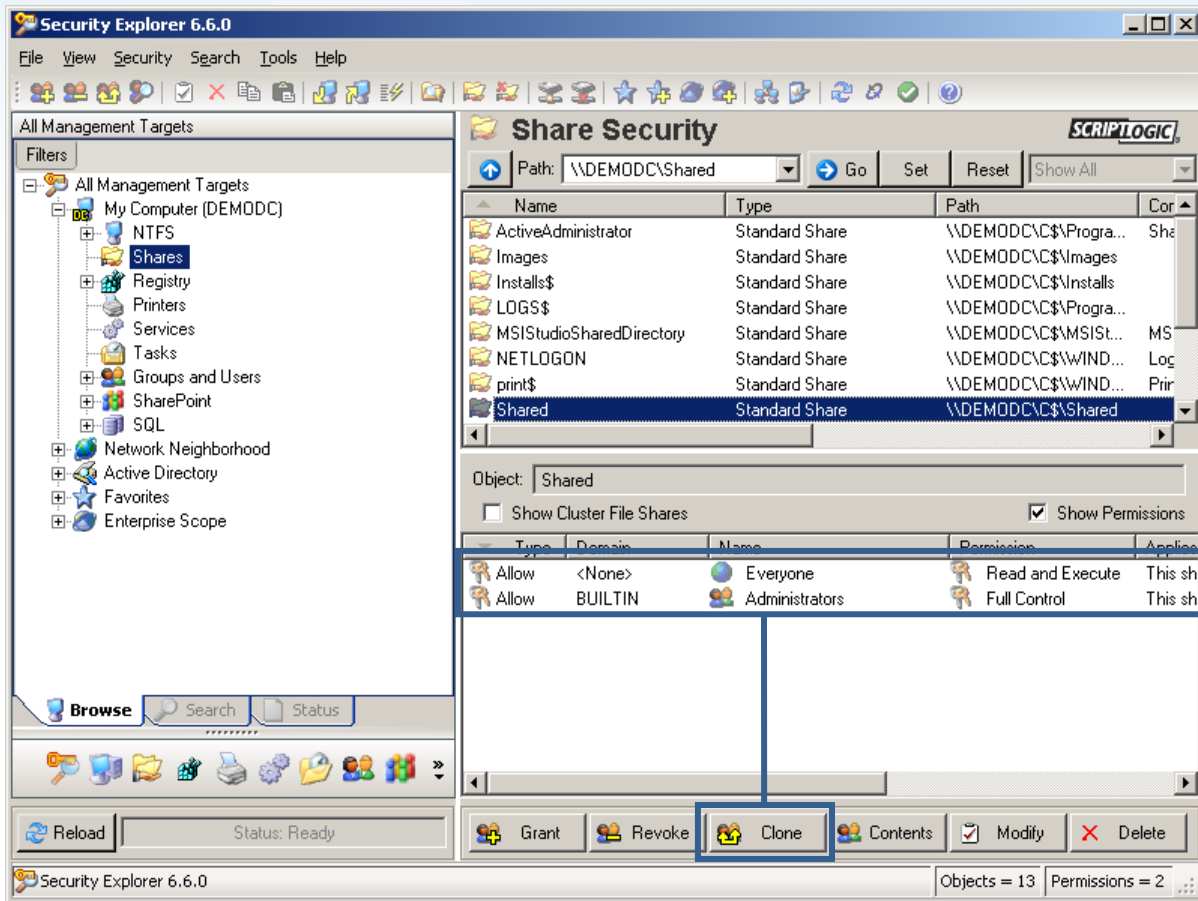


Figure 3: Centralized Assignment and Cloning of permissions with Security Explorer

Example 5: Manage Group Policies to Secure Users and Desktops

Related Objectives: **A13 - Acquire and Maintain Technology Infrastructure / A16 - Manage Changes / DS5 - Ensure Systems Security**

ScriptLogic Solution: **Active Administrator**

Section 3.6 (System Software Change Controls) seeks to make certain change control is in place. One aspect of a Windows network where changes can have a major impact is modification of Group Policy Objects (GPO). Active Administrator is a comprehensive management application that provides enormous visibility and control over GPOs to help administrators manage the GPO lifecycle.

Active Administrator additionally provides an Offline GPO Repository to be used for making changes to and testing Group Policies without affecting the production environment. It is here that change control comes into play. Administrators with Read permissions to GPOs in AD have the ability within Active Administrator to add a GPO to the Offline Repository, edit and report on it, but not publish the offline GPO to the live environment. Only an administrator with Change permissions or higher can move the offline GPO back into production, thereby enforcing change control.

To make use further use of the offline GPOs, Active Administrator features an enhanced “Resultant Set of Policies” tool, shown in Figure 4, that analyzes the effect of combined Group Policies

on an individual user or computer. Active Administrator goes beyond other RSoP tools with the ability to run what-if scenarios against both live Group Policies or their offline counterparts, empowering administrations to see the individual effect of each policy on the Resultant Set. And it can do all this for both Windows 2000 and 2003, and report on GPOs and RSoP in a range of formats.

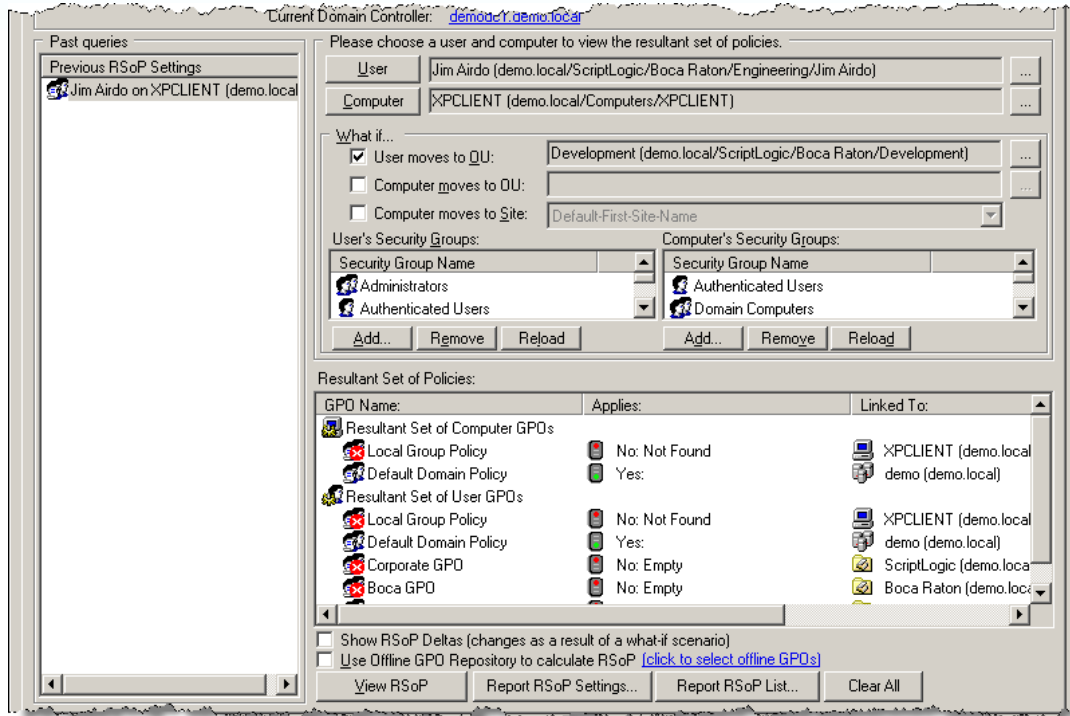


Figure 4: Calculating the RSoP allows you to ensure required security is enforced

Example 6: Maintain GPO History

Related Objective: **DS9 - Manage the Configuration**

ScriptLogic Solution: **Active Administration**

Section 9.3 focuses on maintaining a history of changes and a status of all changes. Active Administrator provides these capabilities for GPO Management through its GPO History functionality. Group Policy History, shown in Figure 5, automatically maintains a history for each version of a GPO within Active Directory. Historical versions can be compared with each other, with the current live GPO version and can be edited as well as rolled back into production.

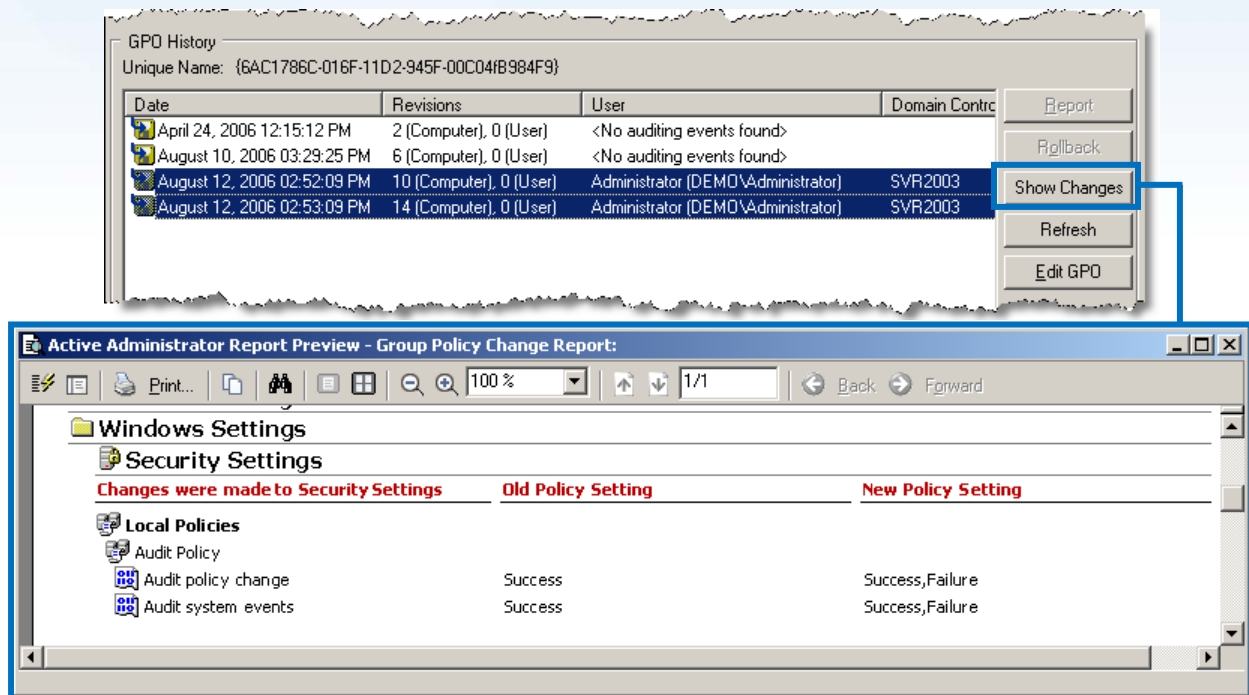


Figure 5: Reviewing Group Policy management activity with Active Administrator

Example 7: Distributing Software

Related Objective: **AI6 - Manage Changes**

ScriptLogic Solution: **Desktop Authority**

Securing access to systems is not only a matter of securing AD or file servers; it is also a matter of ensuring only the correct software is on each client machine. Desktop Authority's Application Launcher, shown in Figure 6, gives administrators the ability to not only launch application installs at logon or logoff, but also can be accomplished with elevated privileges, bypassing the need to give users local admin rights.

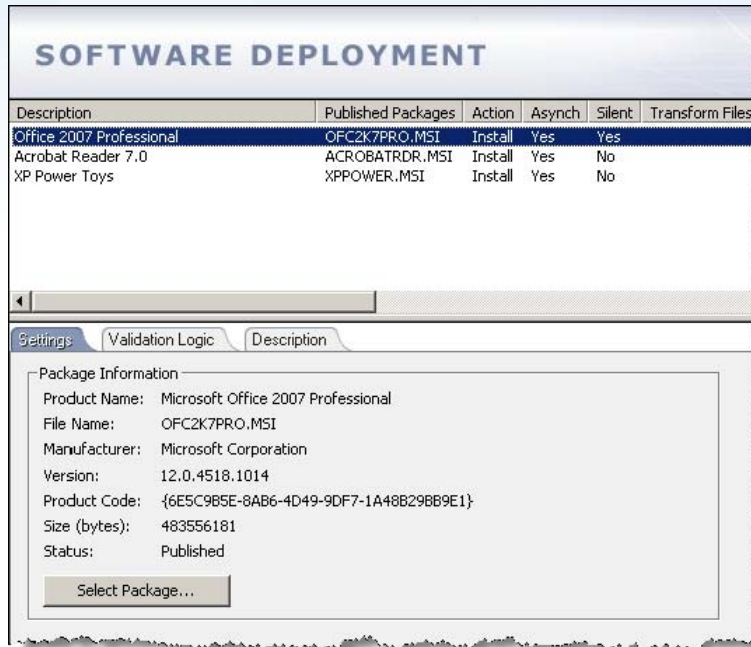


Figure 6: Software can be deployed without the need for local administrative privileges

What makes the application launcher so applicable to COBIT’s need to “ensure distribution of the correct software element to the right place” is Desktop Authority’s Validation Logic, shown in Figure 7. Validation Logic is used to determine who will get a particular configuration such as a drive mapping or an application. By using the 40+ validation types, along with Boolean logic to make selections exponentially more granular, administrators can narrow the scope of selection down to a specific group of users or even a single user.

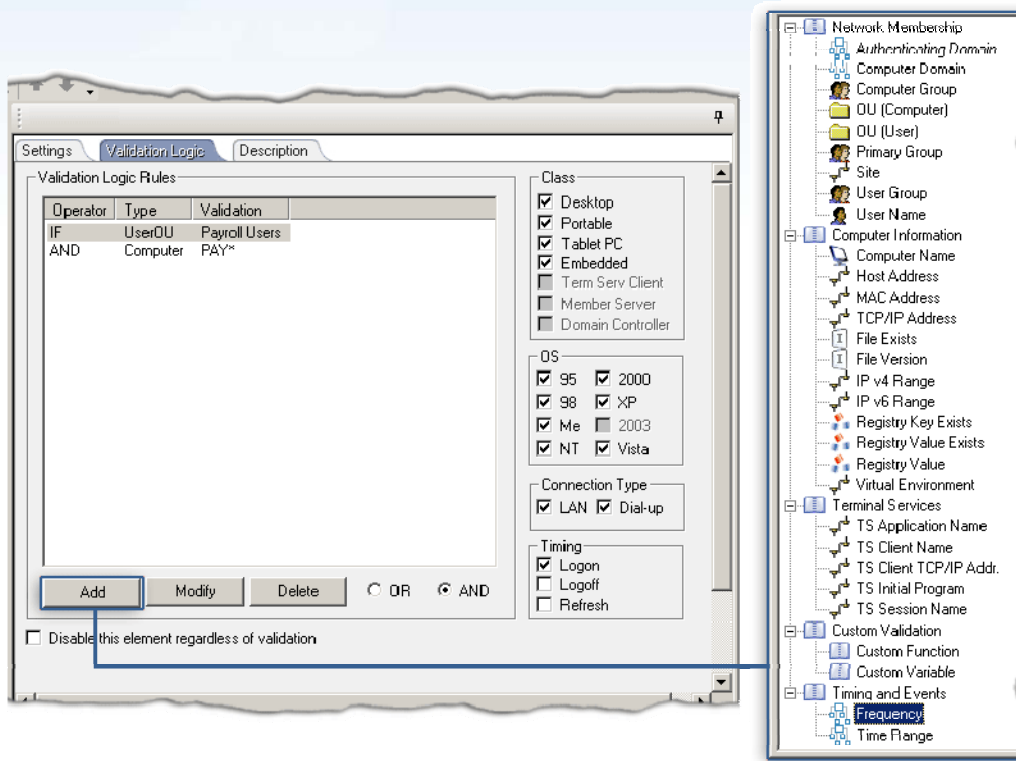


Figure 7: Validation Logic allows granular selection of deployment and desktop configuration

Example 8: Auditing Active Directory Usage

Related Objectives: **A13 - Acquire and Maintain Technology Infrastructure / A16 - Manage Changes / DS5 - Ensure Systems Security / M1 - Monitor the Process**

ScriptLogic Solution: **Active Administrator**

Several COBIT controls call for the monitoring the use of systems and imposed security. To be aware of changes being made to your Active Directory, 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 database, and providing powerful reporting capabilities. This can be used to track new delegations and permission changes, and who made them (Figure 8). It can also be used to determine who reset a password, changed group memberships, or performed any other action within Active Directory. Active Administrator allows for long term storage of audit logs without the need for enormous Event Logs on individual domain controllers.

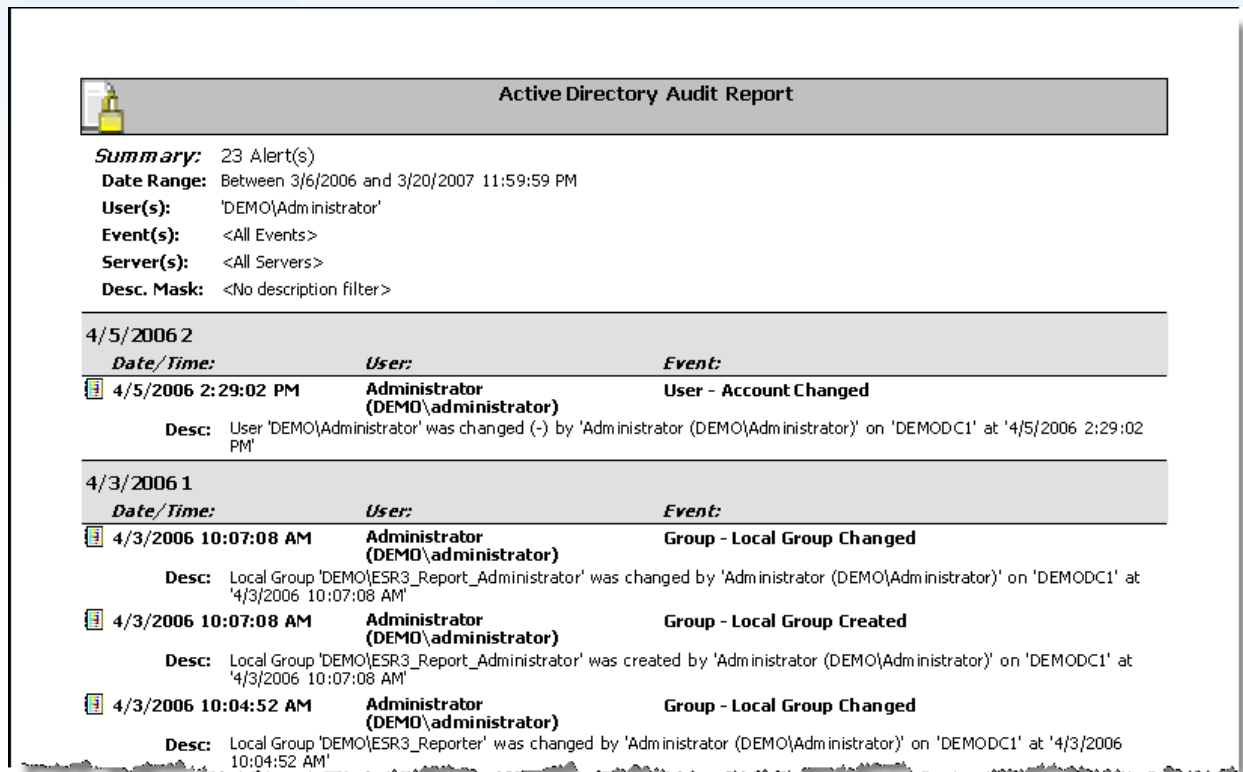


Figure 8: Active Administrator provides centralized reporting on all Active Directory activity

Example 9: Restore Active Directory and Active Directory Security

Related Objectives: **DS4 - Ensure Continuous Service / DS11 - Manage Data**

ScriptLogic Solution: **Active Administrator**

Windows 2003-based Active Directories (even mixed-mode AD environments within only a single Windows Server 2003 Domain Controller) can take advantage of Active Directory object-level restores. When an object is deleted within Active Directory, it is actually “tombstoned” and not permanently deleted until after 45 days (by default with pre-SP1 Windows 2003, and for as long as 180 days with SP1). Windows 2003 allows recovery of objects through an Authoritative Restore, but this does not allow for selective recovery of objects and also loses many attributes including group memberships. Active Administrator backs up Active Directory and gives administrators the ability to recover “deleted” objects, and can also fully restore selective or all attributes on both Windows 2000 and 2003, as shown in Figure 9.

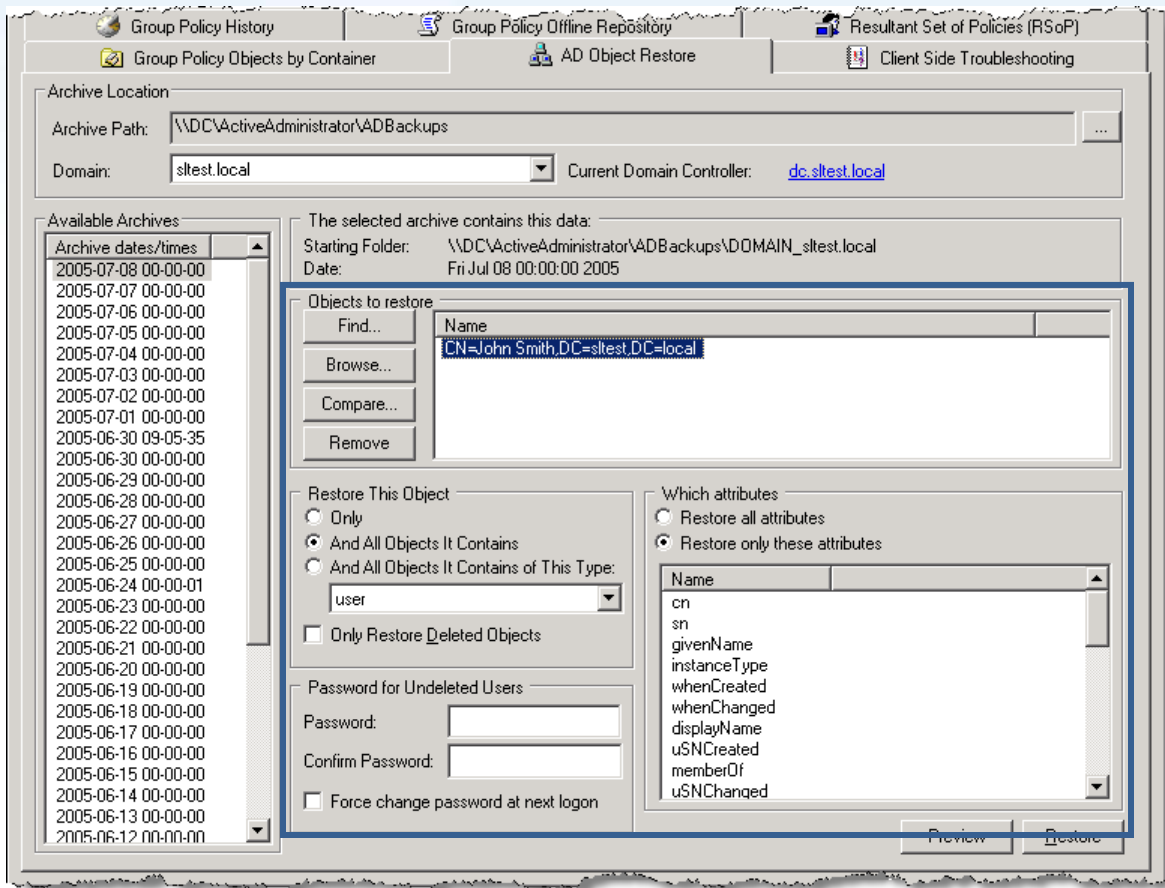


Figure 9: Powerful selection options make restoring deleted objects and object attributes a simple task

An administrator's ability to function within Active Directory is directly impacted by a change in delegated permissions. While Active Templates aid in maintaining proper permissions, it is important to have a backup of those delegations throughout Active Directory. Active Administrator makes backing up Active Directory permissions (shown in Figure 10) a simple task by only requiring a backup filename and a chosen domain. Restores can be as granular as restoring only permissions to a select object or as broad as restoring permissions to the entire Directory.

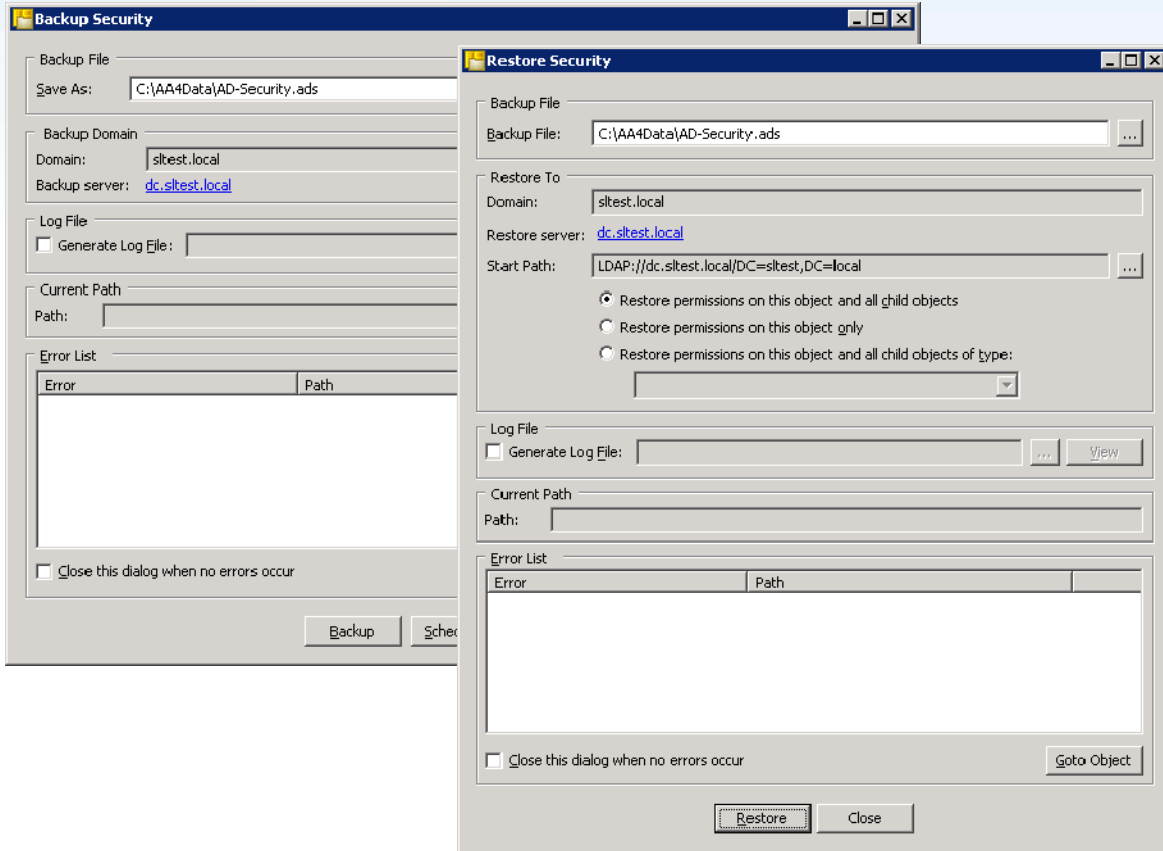


Figure 10: Active Administrator backs up and restores AD permissions increasing the availability of AD administration.

Example 10: Restoring Server Security

Related Objectives: **DS4 - Ensure Continuous Service / DS11 - Manage Data**

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

The Security Explorer platform provides the capability to backup and restore all NTFS, Share, Registry database, 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 data security to the last-known fully-secured state.

Security Explorer can also dramatically simplify the recreation of permissions after a hardware failure and recreation of the file system from backup tapes. The ability to quickly restore permissions settings, as shown in Figure 11, ensures that security is maintained and data is only available where intended.

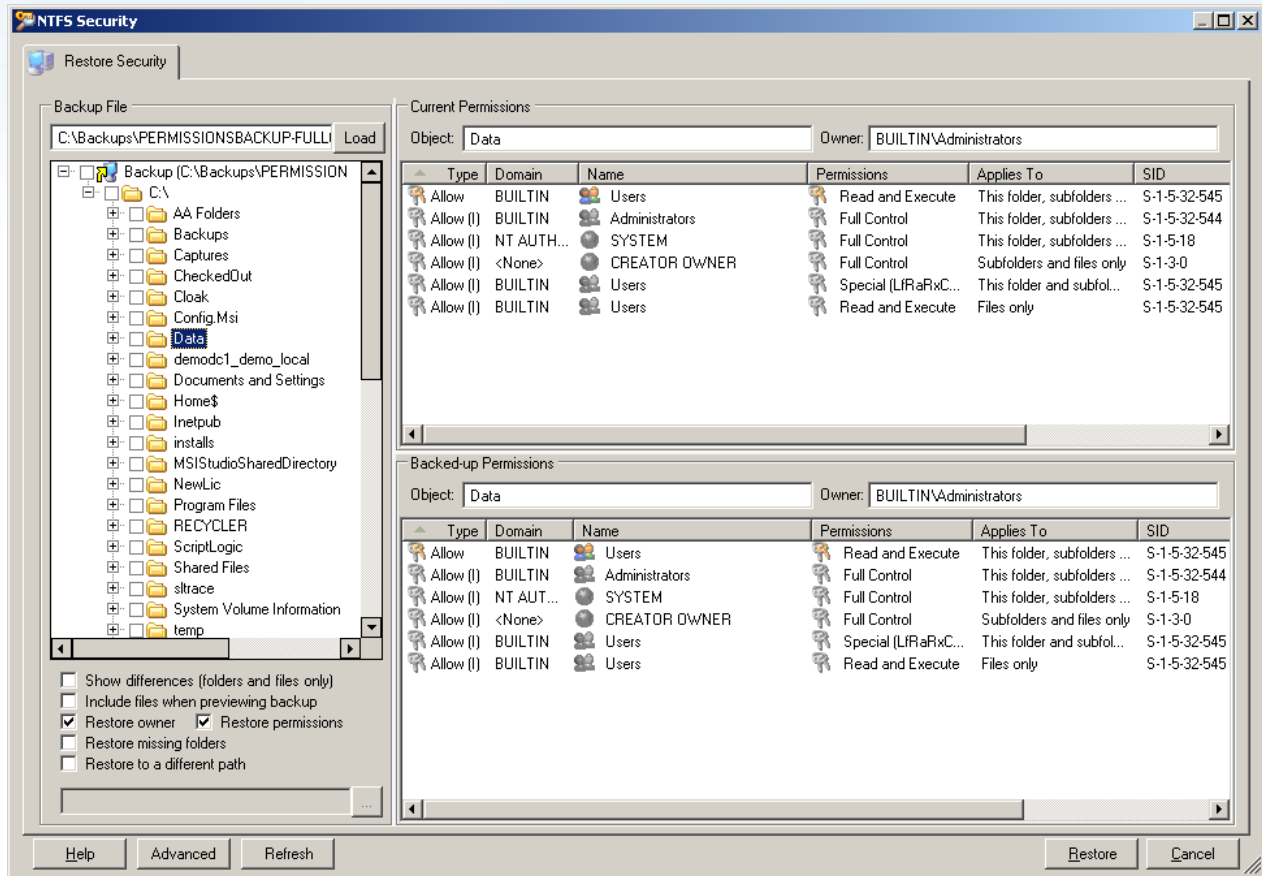


Figure 11: Restoring Share and Registry permissions is similar to restoring NTFS permissions, shown here

Example 11: Audit Server Security Permissions

Related Objective: **DS5 - Ensure Systems 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 servers and analyzes the results using over 160 customizable, turn-key security reports. These reports provide a formatted analysis of the security controls in place if needed during a review of COBIT compliance by third parties.

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 12. The result is that this report is an essential report for tracking down over-exposed files and folders, which might reveal a breach of security.

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

Also, diving into the membership of assigned groups will further enable you to assess the state of security. Enterprise Security Reporter’s Group Membership report, shown in Figure 13, highlights who will be receiving permissions based on group memberships.

SALESDEMO\ExecutiveUser1 (Executive User1)
SALESDEMO\Domain Admins (Designated administrators of the domain)
SALESDEMO\Administrator
SALESDEMO\SLAdmin (SL Admin)
SALESDEMO\Domain Guests (All domain guests)
SALESDEMO\Guest
SALESDEMO\Domain Users (All domain users)
SALESDEMO\AccountingRep1 (Accounting Rep1)
SALESDEMO\accountsmgr (Accounts Manager)
SALESDEMO\Administrator
SALESDEMO\DevelopmentUser1 (Development User1)
SALESDEMO\ExecutiveUser1 (Executive User1)
SALESDEMO\HRUser1 (HR User1)
SALESDEMO\krbtgt
SALESDEMO\NetworkAdmin1 (Network Admin1)
SALESDEMO\SalesRep1 (Sales Rep1)
SALESDEMO\SLAdmin (SL Admin)
SALESDEMO\SLUser (SL User)
SALESDEMO\SUPPORT_388945a0 (CN=Microsoft Corporation,L=Redmond,S=Washington,C=US)
SALESDEMO\Enterprise Admins (Designated administrators of the enterprise)

Figure 13: Quickly identify users with elevated permissions via memberships

Example 12: Ensure Up-To-Date Patches Have Been Applied

Related Objective: **DS5 - Ensure System Security**

ScriptLogic Solutions: **Desktop Authority, Patch Authority Ultimate**

Once a patch is released by Microsoft to secure a known vulnerability, the average time it takes for an exploit to rear its ugly head is less than 25 days. In order to ensure machines accessing customer information are secure, patching needs to take place as soon as possible, once a patch is released. DA's Patch Deployment for Desktops option, shown in Figure 14, patches desktop machines based on product and patch severity utilizing DA's exclusive Validation Logic to establish patch deployment granularity for testing or general availability of a patch.

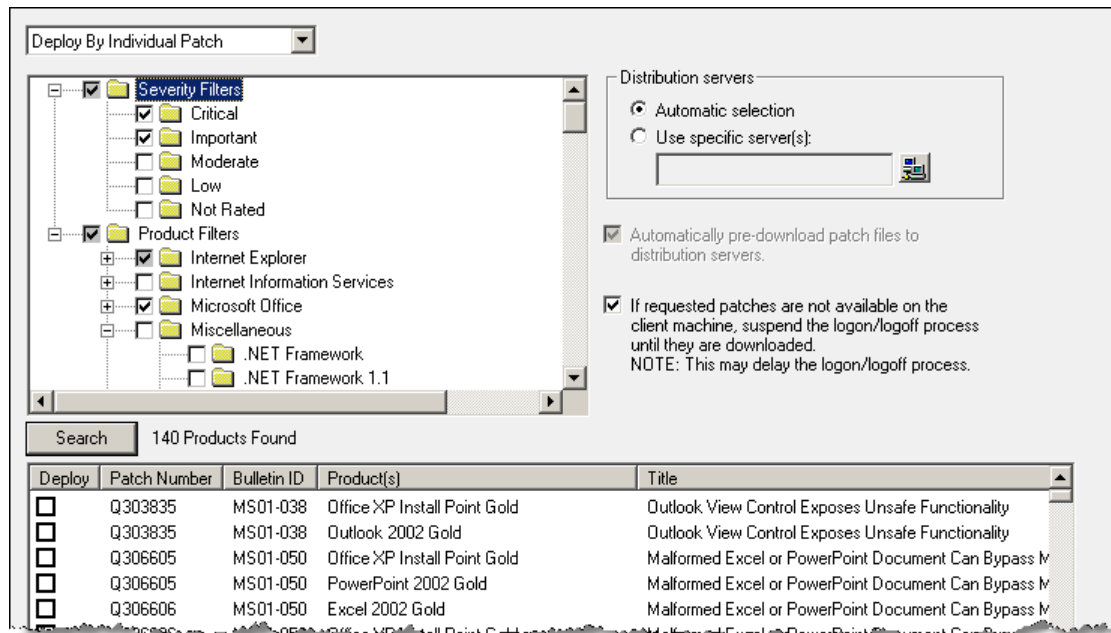


Figure 14: Patching both Microsoft and 3rd-party solutions is a critical step to managing your risk

If you prefer a solution that patches both desktops and servers, Patch Authority Ultimate will patch Microsoft operating systems, enterprise applications (such as Exchange, SQL, etc), Microsoft applications (such as Office) and select 3rd party applications centrally.

Example 13: Scan for Known Spyware on Desktops

Related Objective: **DS5 - Ensure System Security**

ScriptLogic Solution: **Desktop Authority**

In an organization with tens, hundreds, or even thousands of desktops, a standalone anti-Spyware application is not a viable solution. Desktop Authority (DA) provides an enterprise-scalable platform for configuring and securing desktops from a central interface. DA's Spyware Detection and Removal option empowers administrators to centrally scan, remove and report on any found Spyware utilizing DA exclusive Validation Logic to select who will receive the configuration. Figure 15 shows the configuration options available and Figure 16 shows DA's Spyware reporting capabilities.

Figure 15: Desktop Authority's powerful Anti-Spyware option is comprised of flexible options mixed with multiple configurations using Validation Logic

Computer Name		Infection File Name	Infection Path	Action	Result	Action Time
Threat Level: Severe						
Variant Name: Conscorr		Category: RAT		Last Action: 9/21/2005 3:24 PM		
Description: This malicious program is designed to download programs from the internet, including dangerous viruses and parasites. It is responsible for infecting machines with large amounts of other spyware and adware; this exploitation does not require any user inte						
DESKTOP1	CONSCORR.EXE	C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR.2K3DOMAIN\DESKTOP1\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM	
DESKTOP1	CONSCORR.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP1\SPYWA RE\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM	
Threat Level: High						
Variant Name: nCase		Category: ADWARE		Last Action: 9/21/2005 3:24 PM		
Description: No Description						
DESKTOP1	180AX.EXE	C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR.2K3DOMAIN\DESKTOP1\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM	
DESKTOP1	180AX.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP1\SPYWA RE\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM	

Figure 16: Centralized reporting ensures IT is aware of the Spyware outbreaks and their removal

Example 14: Remotely Manage Clients

Related Objective: **DS8 - Assist and Advise Customers**

ScriptLogic Solution: **Desktop Authority**

Both the Incident Management and Problem Management processes focus on the minimization of impact, as well as the amount of time required to fix a problem. Problems arising on client machines can be diagnosed identified and resolved remotely using Desktop Authority's Remote Management client. Using a Java-enabled web browser, administrators and helpdesk personnel can remotely access client machines, not just for the purpose of remotely controlling, but for the purpose of remotely managing a client machine. In addition to troubleshooting a client problem by interactively controlling the desktop remotely, Desktop Authority's Remote Management client (shown in Figure 17) can also accomplish performance monitoring, management of disks, the registry, processes, services, users, groups and more all without disturbing the user while they work.

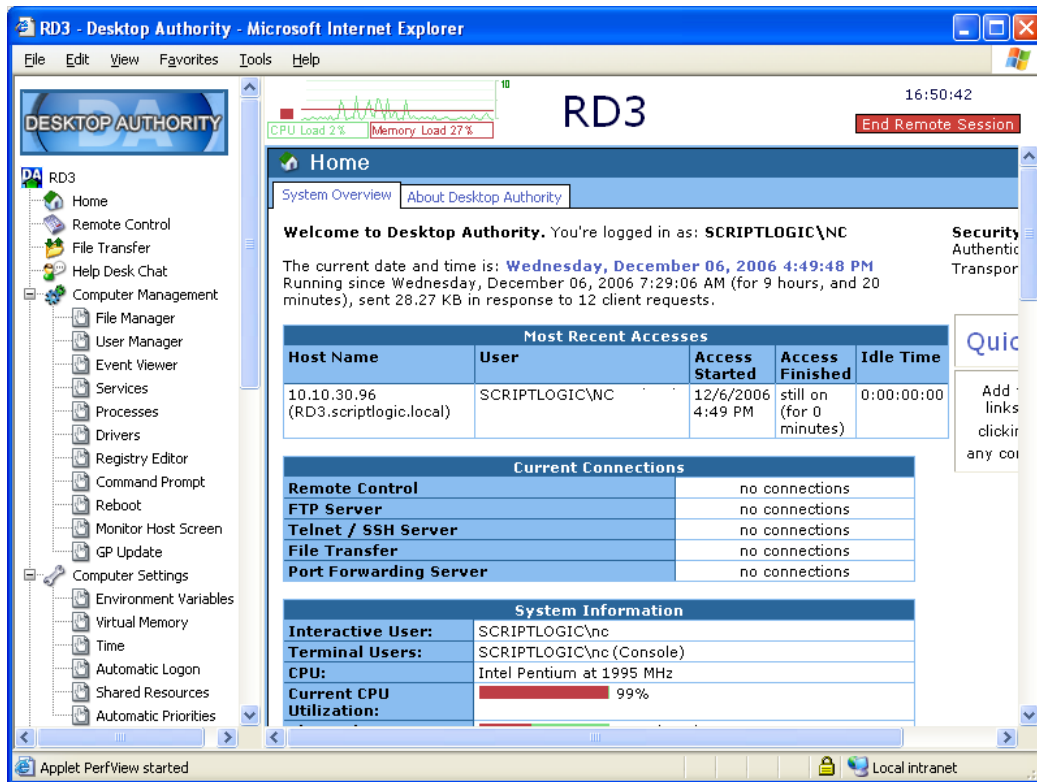


Figure 17: Troubleshooting a client problem remotely is a simple task with Desktop Authority's Remote Management client

Example 15: Assess State of Patching

Related Objective: **M1 - Monitor the Process**

ScriptLogic Solution: **Patch Authority Ultimate**

Before you can manage your risk, you need to assess the current state. Before patching any Windows desktops and servers, Patch Authority Ultimate can perform scans of managed systems and automatically generate and email reports showing the state of your patching, as shown In Figure 18.

Detailed Summary



Patch Report

Report Date: 12/6/2007 5:22 PM

Scan 3/2/2007 11:54 AM

XML Version: 1.1.3.3358 - XML Date: 2/27/2007
Scanned By: DEMO\administrator on 3/2/2007 11:54 AM

Missing Patches: 169	Machines Scanned: 3	Machine Group:
Missing Service Packs: 8	Machines Not Scanned: 3	Scan Template: FullScan
Patches Found: 1	Machines Total: 6	Patch Group:

Computer	IP Address	Domain	Language	Found Patches	Missing Patches	Missing SPs
2003DC5	192.168.135.70	DEMO	us-en	0	50	2
2003MEM3	192.168.135.73	DEMO	us-en	1	54	3
XPPSP2	192.168.135.90	DEMO	us-en	0	65	3

Figure 18: Automatically analyze the state of Windows patching with Patch Authority Ultimate

Example 16: Audit File System Usage

Related Objective: **M1 - Monitor the Process / A13 - Acquire and Maintain Technology Infrastructure**

ScriptLogic Solution: **File System Auditor**

Since sensitive information can exist in letters, accounting spreadsheets, etc, it is vital to have in place a solution that will proactively 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 19.

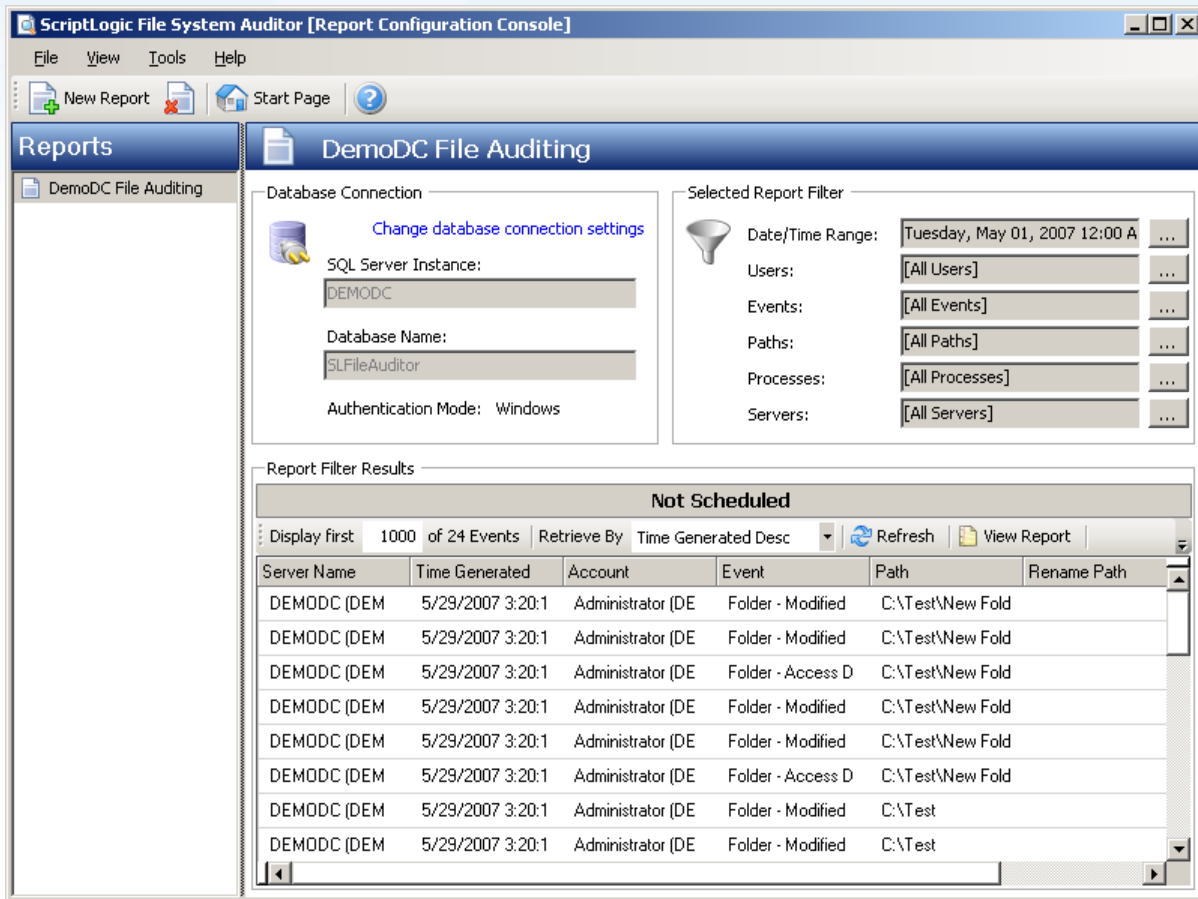


Figure 19: File system activity is centrally audited providing a trail for compliance use

Criteria is based on six elements, each graphically represented to promote a fast and simple method of retrieving audit results, as shown in Figure 20.

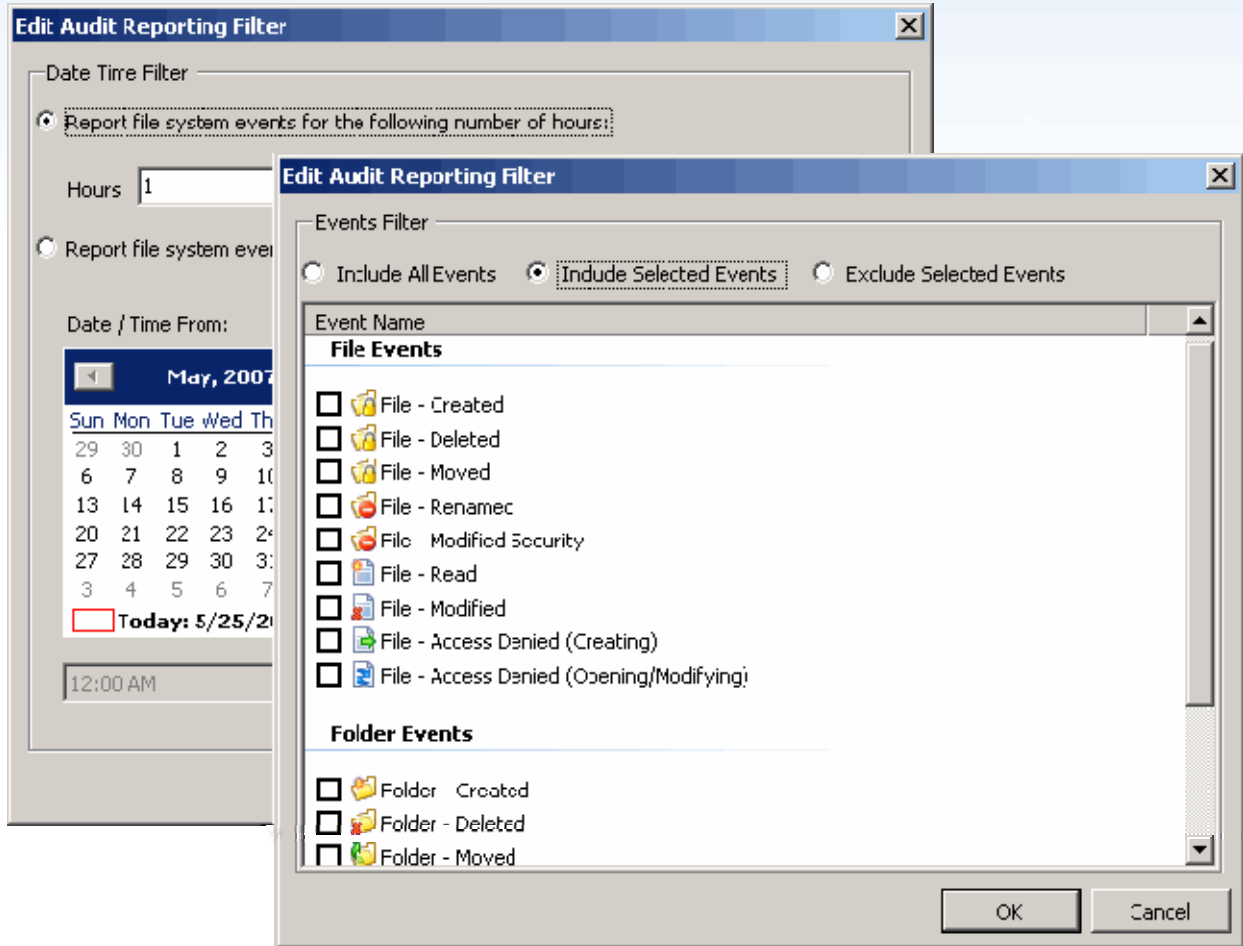


Figure 20: Selection of auditing criteria is a simple process

CONCLUSION

While COBIT lists specific control objectives in the areas of assessment, assignment, auditing and availability of security, it makes no mention on how to implement these controls, as organizations utilize varying systems and will, therefore, utilize different methods to achieve compliance.

ScriptLogic products give administrators the power they need to ensure security throughout their Windows-based networks, and to scan and report on security settings to demonstrate COBIT compliance when required. This white paper has only touched a few key functions in ScriptLogic's range of solutions, but these functions and many more like them combine to enable IT administrators to play their part in achieving their organization's COBIT compliance.

ScriptLogic solutions that assist with COBIT compliance	
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
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, 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, SQL, and SharePoint servers. It also manages service and task security and settings.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.
Desktop Authority	Comprehensive desktop management platform the provides centralized configuration, inventory, support and security of Windows-based clients.
Patch Authority Ultimate	Centralized patching solution providing both Microsoft and select third-party patching of Windows desktops and servers.

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