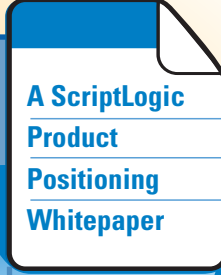




IMPLEMENTING FISMA COMPLIANCE CONTROLS WITH SCRIPTLOGIC

A graphic of a white document with a folded top-right corner, containing text. A blue oval shadow is cast beneath the document, and a vertical dashed line extends downwards from the bottom of the document.

A ScriptLogic
Product
Positioning
Whitepaper

CONTENTS

Introduction	3
FISMA Overview	3
Administrative and Technical Controls	3
Solutions Summary	4
Security Assessment – FISMA Section 3544(b)(1)	5
Example 1: Find Over-Privileged Admins in Active Directory	5
Example 2: Find Over-Privileged Users in Active Directory	5
Example 3: Find Over-Privileged Users on Servers	6
Establish Security Policies – FISMA Section 3544(b)(2)	7
Example 4: Use Active Templates to Delegate Active Directory Permissions	7
Example 5: Review, Clean-Up and Manage File Server Security	8
Evaluate Security Policies – FISMA Section 3544(b)(5)	8
Example 6: Audit Active Directory Usage	8
Example 7: Audit Server Security Configurations	9
Ensure Operational Continuity– FISMA Section 3544(b)(8)	10
Example 8: Backing Up and Restoring Active Directory	10
Example 9: Backing Up and Restoring Active Directory Security	11
Example 10: Backing Up and Restoring Group Policies	12
Example 11: Backing Up and Restoring NTFS Permissions	12
Conclusion	12

INTRODUCTION

ScriptLogic Corporation, headquartered in Boca Raton, Florida, is a leader in network administration software for Microsoft Windows-based networks. ScriptLogic's software solutions are used every day on more than 3.2 million desktops and 86,000 servers at 14,000 customer installations around the world. ScriptLogic's software solutions help many

different types of enterprises comply with the requirements arising from government legislation and industry best practices. The aim of this document is to highlight ways in which ScriptLogic solutions can be used to implement FISMA compliance controls in Windows-based networks.

Additional information about ScriptLogic solutions and FISMA can be found at <http://www.scriptlogic.com/fisma>

FISMA OVERVIEW

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the Electronic Government Act of 2002. It provides a framework to ensure comprehensive measures are taken to secure federal information and assets. FISMA compliance is a matter of national security, and is therefore scrutinized at the highest level of government. Because the Act applies to the information and information systems used by the agency, contractors, and other organizations, it has a wider applicability than previous security laws. Agency IT security programs apply to all organizations which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency, including contractors, grantees, State and local governments, and industry partners. Therefore, Federal security requirements continue to apply, making the agency responsible for ensuring appropriate security controls.

The Act assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies

and procedures to cost-effectively reduce information technology security risks to an acceptable level.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the Act.

The National Institute of Standards and Technology developed a series of standards and guidelines to help government agencies implement their responsibilities under FISMA. These standards, currently published under special publication 800-53, will be mandatory by the end of 2005, published as the Minimum Security Requirements for Federal Information and Information Systems document (known as FIPS 200). ScriptLogic has a specific whitepaper devoted to NIST/FIPS implementation guidelines. [Find out more at www.scriptlogic.com/nist](http://www.scriptlogic.com/nist)

ADMINISTRATIVE AND TECHNICAL CONTROLS

By establishing IT security as a life cycle process, FISMA integrates security with overall IT management and maintenance processes. Throughout the process, ScriptLogic

solutions assist in both the implementation and assessment of security for Windows-based networks.

Control	FISMA Section	Action Required
Security Assessment	3544(b)(1)	Evaluate Active Directory security for over-privileged users Evaluate server security for over-privileged users
Establish Security Policies	3544(b)(2)	Establish Active Directory security roles Establish server security roles
Evaluate Security Policies	3544(b)(5) 3544(c)(2)	Audit Active Directory usage Audit Server Security
Ensure Operational	3544(b)(8)	Establish backup and restore procedures for Active Directory continuity and security Establish backup and restore procedures for server security

Table 1

SOLUTIONS SUMMARY

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

In order to bring an agency 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 FISMA compliance include:	
Active Administrator™	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
Enterprise Security Reporter™	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 management solution that fixes, reports, searches, cleans-up and backs up all security settings on file servers.

Together, these products enable companies to implement controls that secure financial systems, easily maintain those controls, as well as report on their effectiveness, thus fulfilling a key requirement of FISMA compliance.

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

SECURITY ASSESSMENT – FISMA SECTION 3544(b)(1)

To properly assess the risk involved with the current security configuration in a Windows network, begin where all security assignments in a Windows network originate from – Active Directory. By checking the privileges of administrators in Active Directory, you ensure those that administer Active

Directory have appropriate access. Once administrators are in check, identify users that have been granted access to resources via group membership and assess for any inappropriate access. Lastly, validate access rights on servers to ensure security is maintained.

Example 1: Find Over-Privileged Admins in Active Directory

ScriptLogic Solution: Active Administrator™

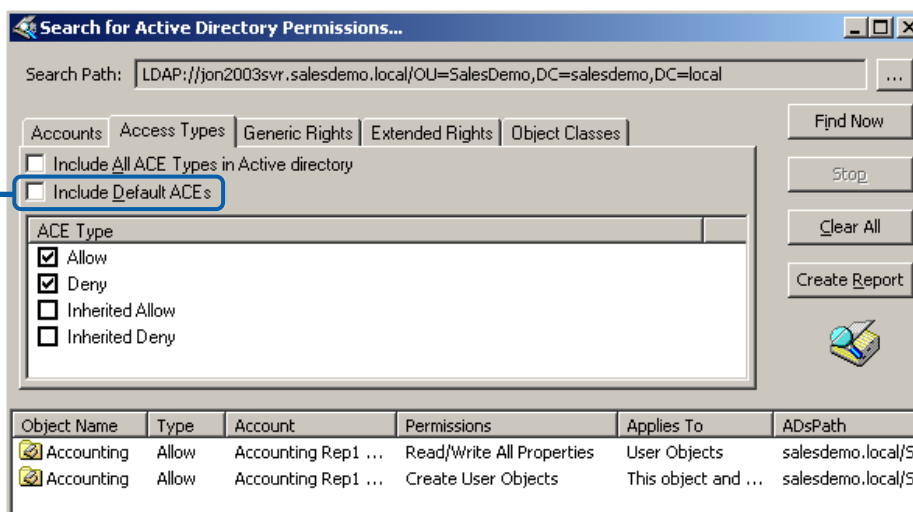
As part of the FISMA standards, IT Administrators are required to perform a risk assessment – section 3544(b)(1). At the heart of almost all Windows-based networks, Active Directory manages the security and privileges assigned to staff within an agency. Active Administrator offers a range of functions which enable effective management of these privileges.

For example, Active Administrator provides the ability to generate reports on permission settings. 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 secured health records
- Addition of new computers into domains

Optionally hide default permissions supplied in the Active Directory schema, making it easier to see “extra” permissions

Figure 1



This control has a direct relationship with the management of permissions within Active Directory, making Active Administrator a vital part of any FISMA compliance strategy in a Windows environment.

Example 2: Find Over-Privileged Users in Active Directory

ScriptLogic Solution: Enterprise Security Reporter™

Enterprise Security Reporter scans a network of Windows servers and workstations, and analyzes the results using over 80 customizable, turn-key security reports. These reports are vital tools to help with the “periodic assessment” requirement in section 3544(b)(1). These reports also provide a formatted analysis of the security controls in place if needed during a review of FISMA compliance.

As an example, one report from Enterprise Security Reporter which is helpful in ensuring the security of Windows-based systems is the Group Membership report. This highlights users who are members of groups which automatically receive administrative privileges.

```

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)

```

With Enterprise Security Reporter, it takes seconds to produce formatted reports like this one which shows Group Memberships

Figure 2

Example 3: Find Over-Privileged Users on Servers

ScriptLogic Solution: Enterprise Security Reporter™

Another useful report – analysis of file permissions – can be run on file servers 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. 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.

Delta Permissions Reporting enables you to quickly find unusual permissions – this folder has somehow gained access for users in the Guests group

Path/Object Name	Account	Type	Permissions
+ NT AUTHORITY\NETWORK		Allowed	Special (RWX)(RWX)(RX)
- SALESDEMO\Domain Admins (Designated administrators of the domain)		Allowed	
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir02.try\			
- SALESDEMO\Domain Admins (Designated administrators of the domain)		Allowed	
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\			
- SALESDEMO\Domain Admins (Designated administrators of the domain)		Allowed	
+ SALESDEMO\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)
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir02.try\			
+ SALESDEMO\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)
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir03.try\			
+ {S-1-5-32-547}		Allowed	Full Control (All)(All)(All)
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir03.try\subdir03.try\dir03.try\			
+ SALESDEMO\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)
\\JON2003SVR\C\$\SHARES\USERS\securityexplorer.try\dir04.try\			
- SALESDEMO\Domain Admins (Designated administrators of the domain)		Allowed	

Figure 3

ESTABLISH SECURITY POLICIES – FISMA SECTION 3544(b)(2)

Once security vulnerabilities in Active Directory and on servers have been identified, the goal of section 3544(b)(2) is to “cost-effectively reduce information security risks to an acceptable level.” The appropriate steps to reduce risks are to

implement security policies that can be enforced. Like the assessment tasks, the establishment of security begins with defining roles in Active Directory, and ends with implementing security on servers.

Example 4: Use Active Templates to Delegate Active Directory Permissions

ScriptLogic Solution: Active Administrator™

Active Administrator uses Active Template technology to simplify control over the delegation of user rights in Active Directory. 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. Additionally, custom templates can be created to define complex sets of permissions to be assigned to individuals.

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 FISMA standards by ensuring a consistent assignment of permissions.

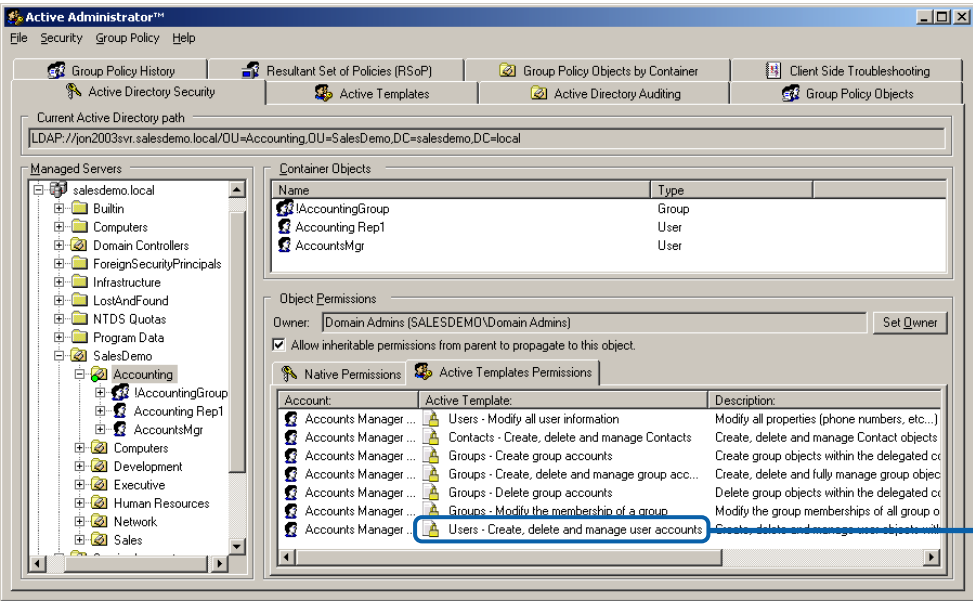


Figure 4

Each Active Template grants or revokes one or more user permissions, simplifying delegation

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 FISMA standards, or Active Administrator can be configured to automatically reinforce the permissions originally assigned through an Active Template.

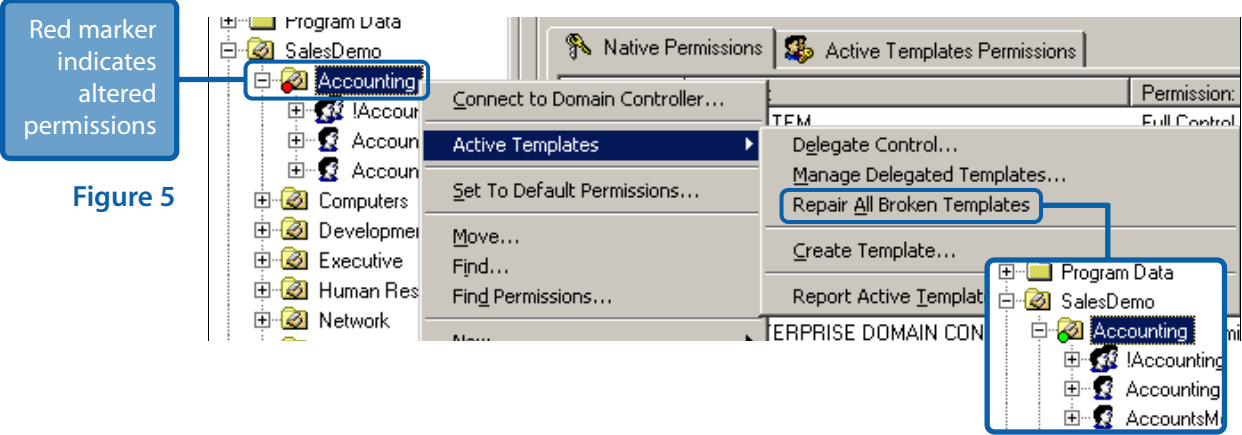


Figure 5

Red marker indicates altered permissions

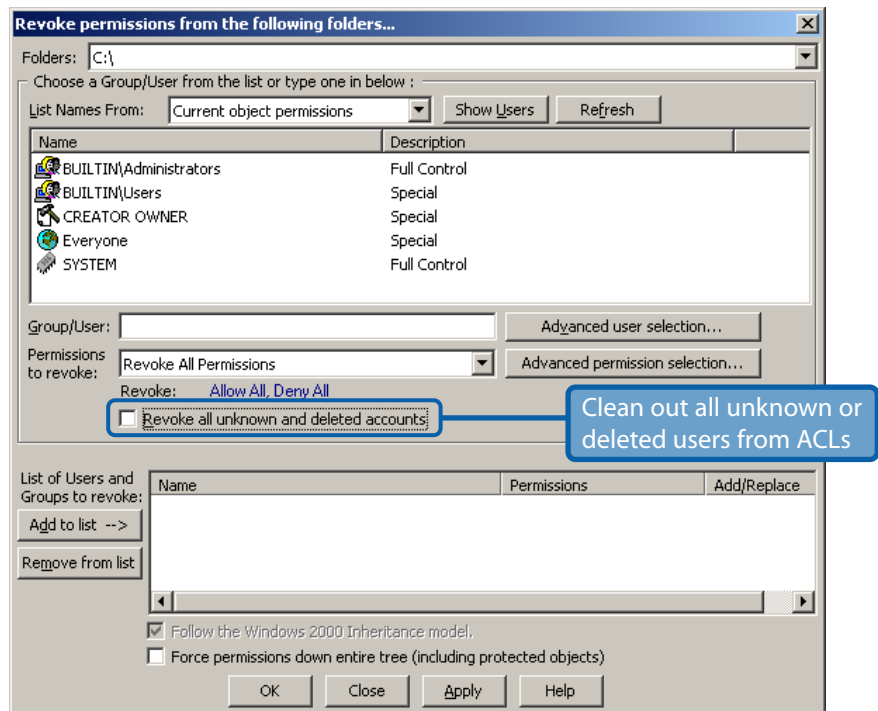
Example 5: Review, Clean-Up and Manage File Server Security

ScriptLogic Solution: Security Explorer®

To continue reducing “information security risks” as set forth by FISMA, management of server security becomes as critical a task as the securing of Active Directory. Because Security Explorer is focused on the NTFS, Registry and Share security settings on servers, it dramatically eases the task of managing server security. With Security Explorer, the ability

to modify permissions and ownership of files throughout a file system is absolute, regardless of current ownership or inheritance settings. Security Explorer can even force a standard set of permissions down a directory tree, overwriting all existing permissions for cleaning-up and securing file servers.

Figure 6: Security Explorer also has the ability to remove all permissions associated with unknown or deleted user accounts. For example, this prevents access to files from parallel Operating Systems that may be installed on workstations and servers.



EVALUATE SECURITY POLICIES – FISMA SECTION 3544(b)(5)

FISMA mandates that an agency perform “periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.” This means an agency

would, at least annually, utilize the same ScriptLogic solutions to audit the very controls they were used to implement.

Example 6: Audit Active Directory Usage

ScriptLogic Solution: Active Administrator™

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 7). 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.

Active Directory Audit Report

Summary: 8 Alert(s)
User(s): All users
Event(s): 'MEMADDG','MEMADDL','USRPWD','SECCHG'
Date Range: Between Sunday, May 01, 2005, and Thursday, June 30, 2005

June 21, 2005		
Date/Time	User	Event
06/21/2005 03:34:26 PM	administrator (SLTEST\administrator)	Security - Permissions Changed
Desc: The security for object 'DC=sltest,DC=local' (Type='domainDNS') was changed by 'SLTEST\Administrator' on 'DC' at '6/21/2005 3:34:26 PM'		
June 1, 2005		
Date/Time	User	Event
06/01/2005 04:27:55 PM	administrator (SLTEST\administrator)	Group Membership - Member Added to Global Group
Desc: Member 'CN=John Smith,DC=sltest,DC=local' was added to 'SLTEST\Domain Admins' by 'SLTEST\Administrator' on 'DC' at '6/1/2005 4:27:55 PM'		
06/01/2005 04:27:11 PM	administrator (SLTEST\administrator)	User - Password Reset
Desc: The password for user 'SLTEST\JSmith' was reset by 'SLTEST\Administrator' on 'DC' at '6/1/2005 4:27:11 PM'		

Figure 7

Audit any changes made to Active Directory

Active Administrator can even send email alerts when selected events occur, for example when new users are added, or given extra permissions, as shown in Figure 8.

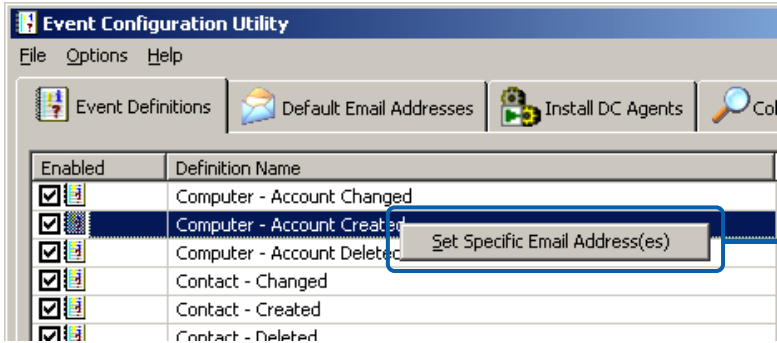


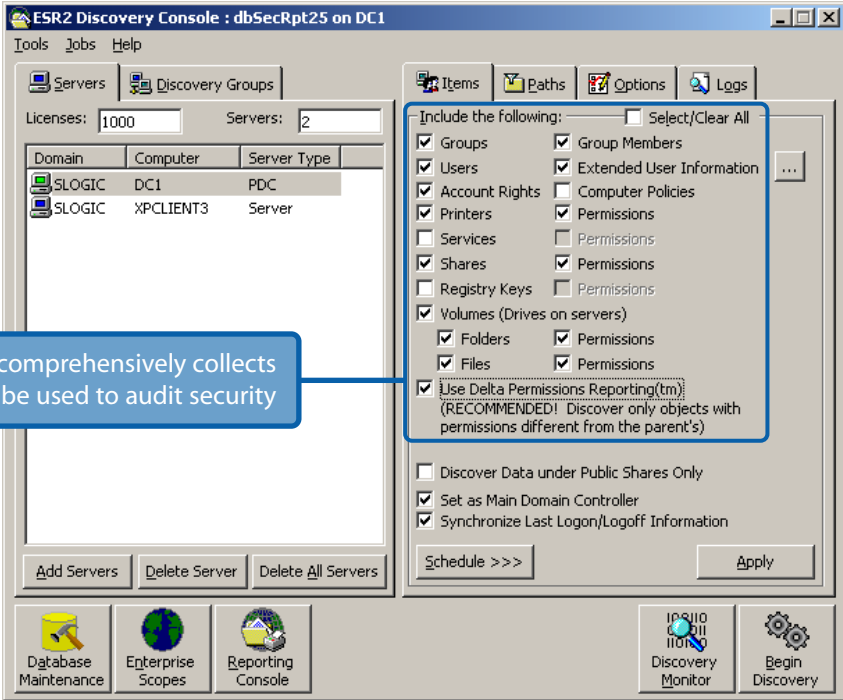
Figure 8

Auditing is enhanced by configuring real-time notification of Active Directory changes

Example 7: Audit Server Security Configurations

ScriptLogic Solution: Enterprise Security Reporter™

Enterprise Security Reporter (ESR) provides administrators with the ability to centrally capture security information on servers throughout the network and then generate reports to be used in support of any audits of security. ESR, shown in Figure 9, collects information on users, groups, printers, shares, services, registries, policies, permissions, and more.



ESR comprehensively collects information to be used to audit security

Figure 9

Explicit Permissions Under Folder		
Path/Object Name	Type	Permissions
Account		
SALESDemo\JON2003SVR		
\\JON2003SVR\C\$\SHARES\		
+ CREATOR OWNER	Allowed	Special (n/s)(All)(All)
+ NT AUTHORITY\SYSTEM	Allowed	Full Control (All)(All)(All)
+ SALESDemo\Administrators (Administrators have complete and unrestricted access to the computer/domain)	Allowed	Full Control (All)(All)(All)
+ SALESDemo\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)
\\JON2003SVR\C\$\SHARES\DEPARTMENTS\common\background-client*.*		
+ SALESDemo\administrator	Allowed	Full Control (All)
- SALESDemo\Users (Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications)	Allowed	
\\JON2003SVR\C\$\SHARES\DEPARTMENTS\desktop\		
- CREATOR OWNER	Allowed	

Once collected, ESR reports on all of the various data types collected using pre-defined or custom reports. Figure 10 shows an example of a report generated with ESR. The information reported on by ESR can be used as documentation that proper security is in place.

Figure 10

ENSURE OPERATIONAL CONTINUITY – FISMA SECTION 3544(b)(8)

FISMA is not just focused on system security; it is equally mindful of systems availability by requiring agencies to establish “plans and procedures to ensure continuity of operations for information systems that support the

operations and assets of the agency.” ScriptLogic solutions help with the availability of both Active Directory as well as with file servers.

Example 8: Backing Up and Restoring Active Directory

ScriptLogic Solution: Active Administrator™

Windows 2003-based Active Directories (even mixed-mode Active Directory 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 11 and Figure 12.

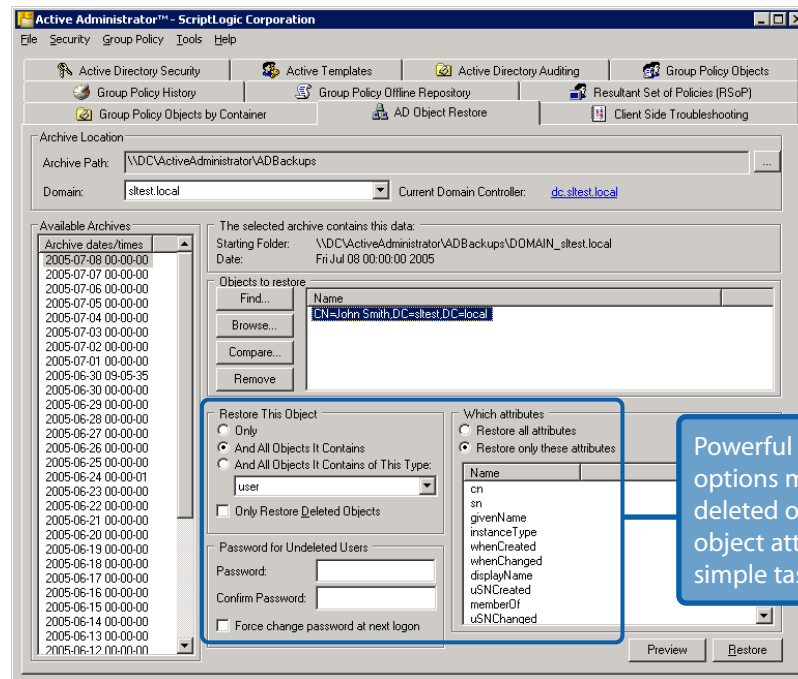
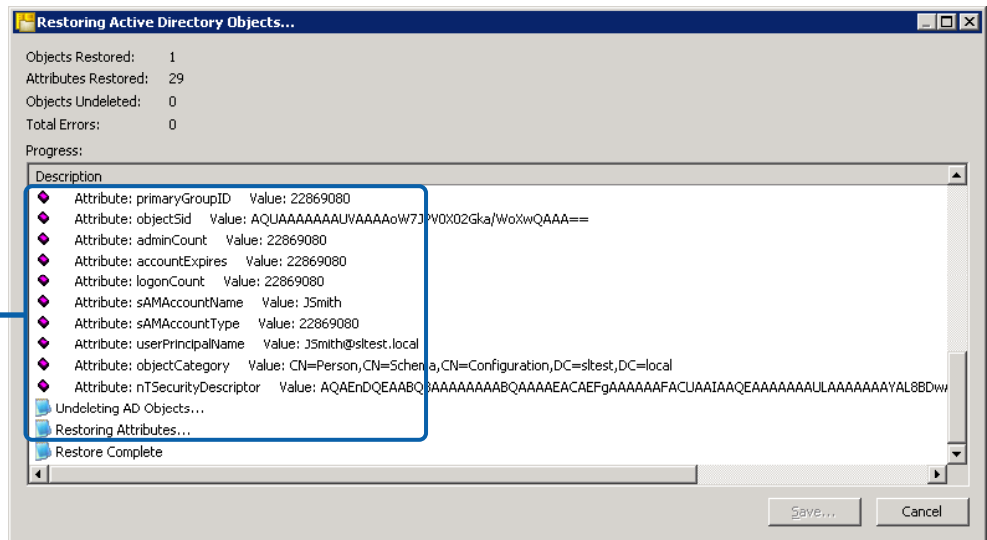


Figure 11

Figure 12

Restoring deleted objects and object attributes makes Active Directory data available to users and administrators



Example 9: Backing up and Restoring Active Directory Security

ScriptLogic Solution: Active Administrator™

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 13) 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.

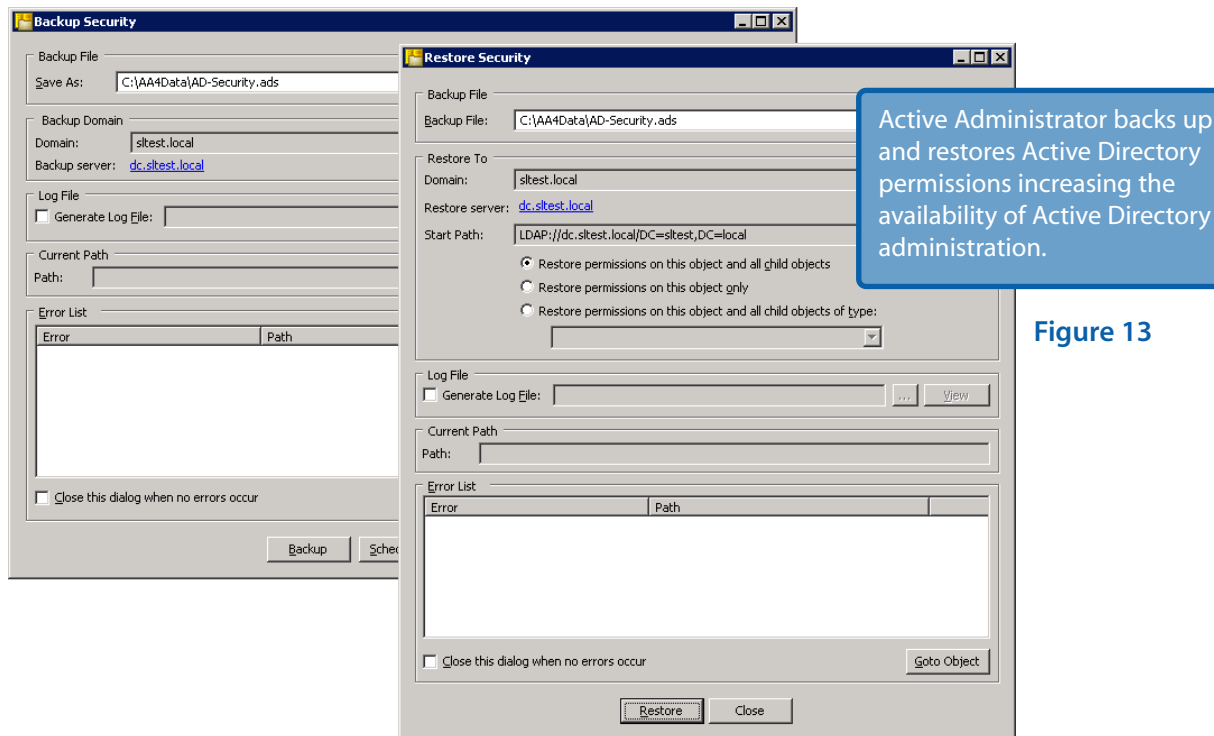


Figure 13

Example 10: Backing up and Restoring Group Policies

ScriptLogic Solution: Active Administrator™

The cornerstone of making Windows-based networks available is a well-maintained Active Directory with up-to-date information. The less time it takes administrators to restore deleted or unintentionally modified objects and group policies, and to restore proper security, the faster users can continue to utilize a secure and functional network environment.

Group Policies (shown in Figure 14) can be backed up individually or as a whole and can be performed as a one-off backup, or scheduled. Restores of Group Policies are as easy as backing them up. Administrators can restore a Group

Policy by simply selecting the backup location, and the policy or policies to be restored.

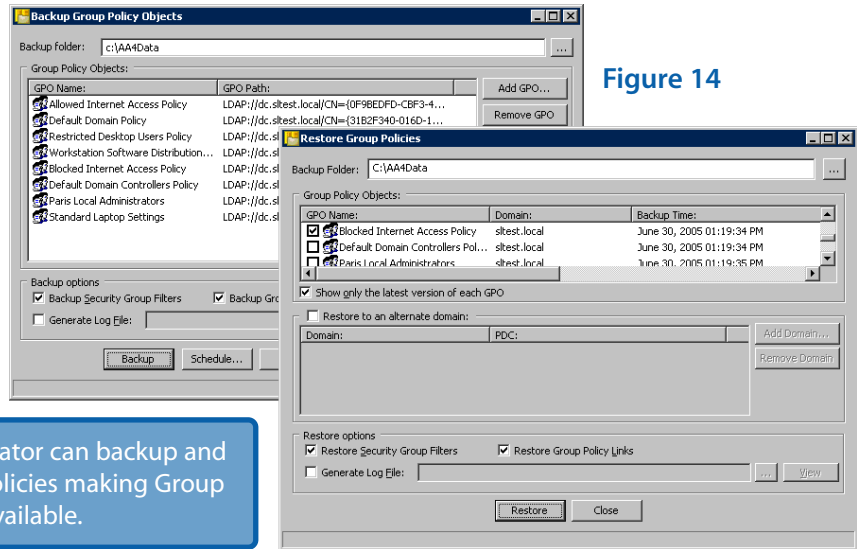


Figure 14

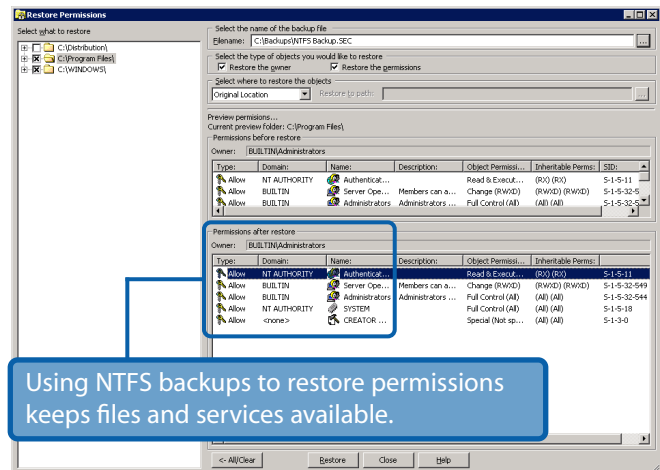
Active Administrator can backup and restore Group Policies making Group Policies highly available.

Example 11: Backing up and Restoring NTFS Permissions

ScriptLogic Solution: Security Explorer®

Security Explorer provides the capability to backup all NTFS permissions on selected file shares. Some administrators even use Security Explorer to perform hourly backups of the permission settings on their security-sensitive file servers so that if a security breach is suspected and permissions appear to have changed, they can quickly reset all files to the last-known fully-secured state.

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



Using NTFS backups to restore permissions keeps files and services available.

Figure 15

CONCLUSION

While FISMA 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 government agencies utilize varying systems and will, therefore, utilize different methods to achieve compliance.

ScriptLogic solutions give administrators the tools they need to assess, assign, make available and audit security in Windows-based networks.

For more information, contact ScriptLogic at: www.scriptlogic.com | 1.800.424.9411 | 1.561.886.2400