



IMPLEMENTING GLBA COMPLIANCE CONTROLS WITH SCRIPTLOGIC

A ScriptLogic
Product
Positioning
Whitepaper

CONTENTS

Introduction	3
GLBA Overview	3
Administrative and Technical Controls	3
Solutions Summary	4
Security Assessment – GLBA Section 6801(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 – GLBA Section 6801(b)(1), 6801(b)(3)	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 – GLBA Section 6801(b)(1)	8
Example 6: Audit Active Directory Usage	8
Example 7: Audit Server Security Configurations	9
Protect Against Threats – GLBA Section 6801(b)(2)	10
Example 8: Protecting against Spyware	10
Example 9: Protect against known Vulnerabilities	11
Example 10: Patching Desktops and Servers	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 GLBA compliance controls in Windows-based networks.

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

GLBA OVERVIEW

The Financial Modernization Act, also known as the "Gramm-Leach-Bliley Act" (GLBA), was signed into law in 1999 and includes provisions to protect consumers' personal financial information held by financial institutions which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.

There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The Financial Privacy Rule seeks the protection of customers' personal financial information by financial institutions, while the pretexting provisions seeks to protect

consumers from individuals and companies obtaining personal financial information under false pretenses.

It is the Safeguards Rule that is of concern to IT. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. In a Windows-based network, this must start with administrative delegation in Active Directory (to ensure only appropriate access is granted to network users), followed by protecting the financial data itself by securing NTFS, server registries and network shares from inappropriate access. Additionally, GLBA requires client machines be protected against any outside threats, such as Spyware, worms, viruses, etc.

ADMINISTRATIVE AND TECHNICAL CONTROLS

While GLBA focuses on the proactive measures used to protect customer information, IT should look at this protection as a process that begins with the proactive controls, and finishes with reactive assessment of the imposed security. Throughout the process, ScriptLogic solutions assist in

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

Table 1 lists the controls required by GLBA and necessary actions to be taken in order to comply with GLBA standards.

Control	GLBA Section	Action Required
Security Assessment	6801(b)(1))	Evaluate Active Directory security for over-privileged users Evaluate server security for over-privileged users
Establish Security Policies	6801(b)(1) 6801(b)(3)	Establish Active Directory security roles Establish server security roles
Evaluate Security Policies	6801(b)(1)	Audit Active Directory usage Audit Server Security
Protect Against Threats	6801(b)(2)	Patch desktops and servers; protect against Spyware

Table 1

SOLUTIONS SUMMARY

ScriptLogic software solutions give agencies that are implementing internal controls in order to comply with GLBA 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 GLBA 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.
Patch Authority Plus™	Distributes OS and application patches to desktops and servers to protect against known vulnerabilities.
Desktop Authority's Patch Distribution for Desktops Option	Distributes OS and application patches to desktops to protect against known vulnerabilities in addition to Desktop Authority's comprehensive desktop management capabilities.
Desktop Authority's Spyware Detection and Removal Option	Detects known spyware and can either quarantine or remove from desktops.

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 GLBA compliance.

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

SECURITY ASSESSMENT – GLBA SECTION 6801(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 (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™**

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.

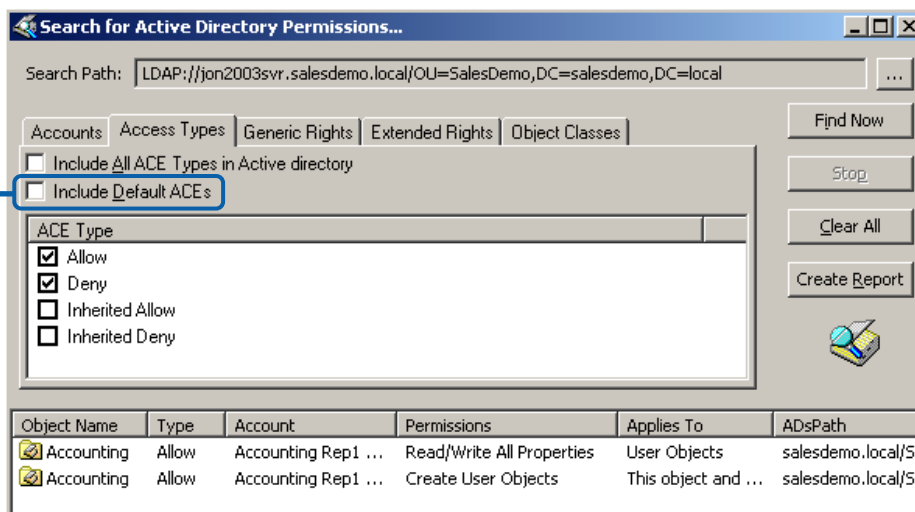
For example, Active Administrator provides the ability to generate reports on permission settings. These can be used

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 GLBA 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 ensuring the “security and confidentiality” requirement in section 6801(b)(1). These reports also provide a formatted analysis of the security controls in place if needed during a review of GLBA 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)
SALESDEMO\...

```

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 – GLBA SECTION 6801(b)(1), 6801(b)(3)

Once security vulnerabilities in Active Directory and on servers have been identified, the goal of section 6801(b)(3) is to “protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.” The appropriate

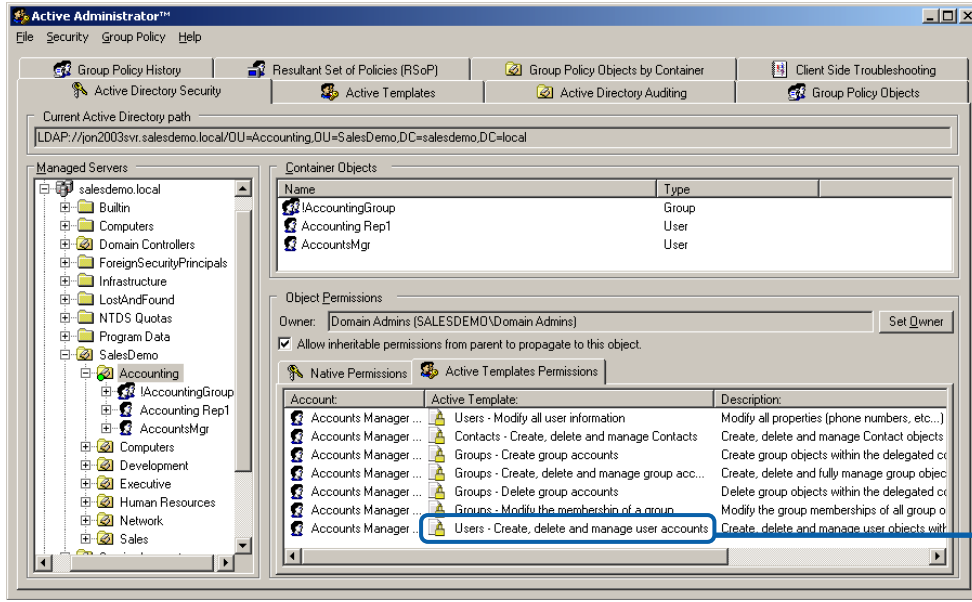
steps to reduce risks are to implement security policies that can be enforced. Like the assessment tasks, the establishment of security begins with **defining roles in Active Directory**, and ends with **implementing security on servers**.

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

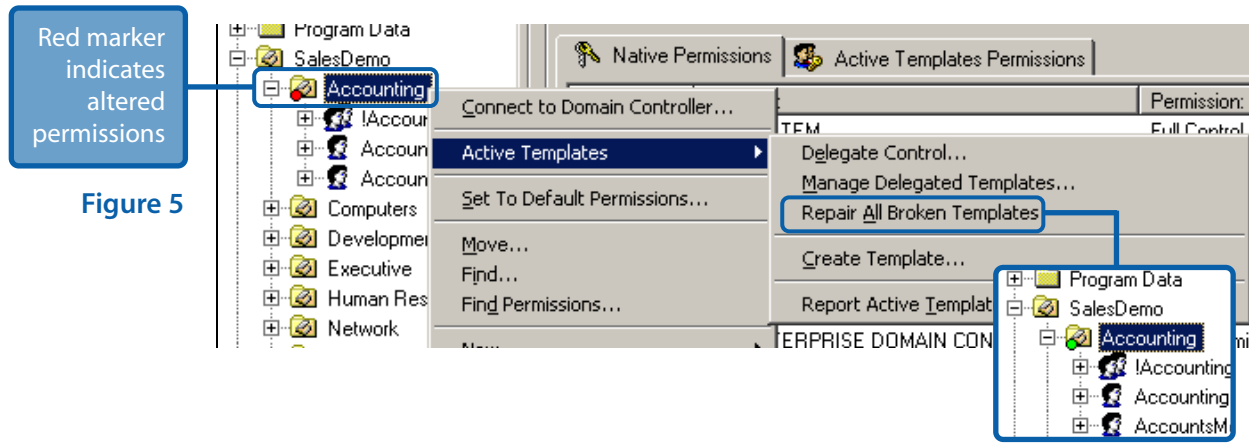


Figure 5

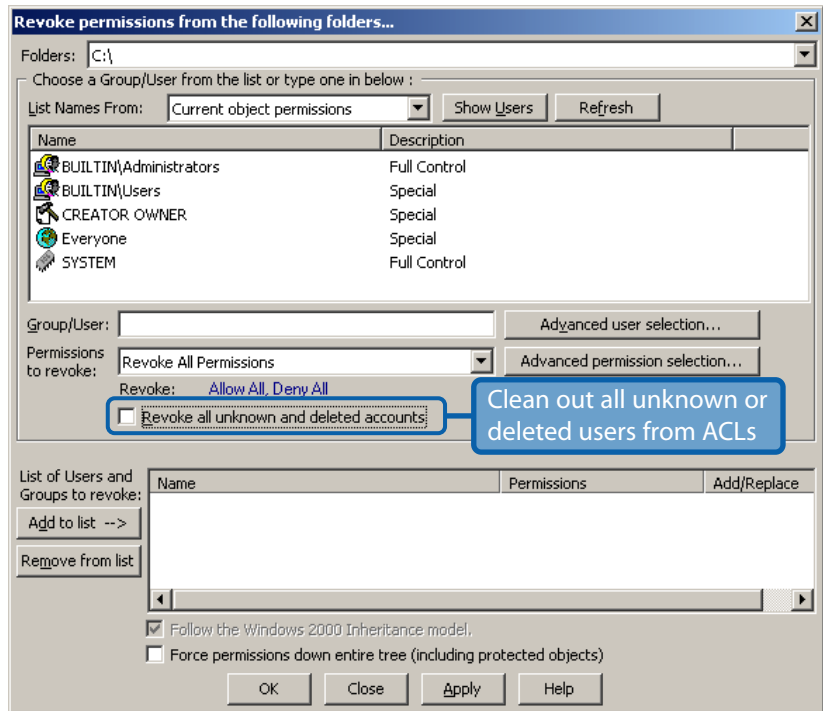
Example 5: Review, Clean-Up and Manage File Server Security

ScriptLogic Solution: Security Explorer®

To continue reducing “unauthorized access to or use of” customer information as set forth by GLBA, 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 – GLBA SECTION 6801(b)(1)

GLBA mandates that an agency “insure the security and confidentiality of customer records and information.” To accomplish this, it is not enough to simply assess the current state of security and implement new security controls; it also means an organization would utilize the same ScriptLogic

solutions to audit the very controls they were used to implement. This section showcases a few uses of ScriptLogic solutions already covered initially to implement security that can also be used to audit that same security.

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.

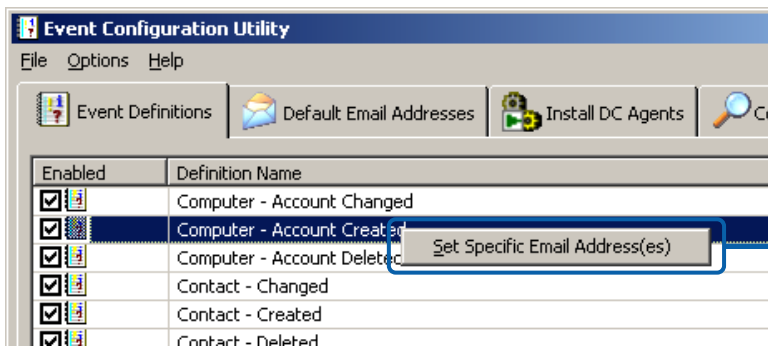


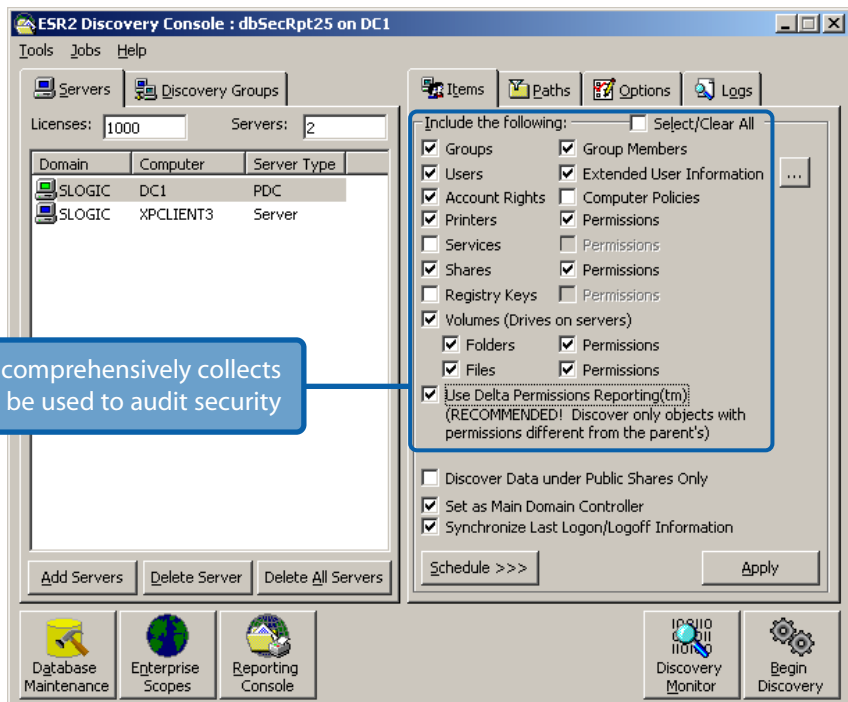
Figure 8

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			Printed on 10/19/2004 5:53:44 PM
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

PROTECT AGAINST THREATS – GLBA SECTION 6801(b)(2)

Even with Active Directory and servers being secured, organizations need to address the possibility of rogue software being run on desktops via either Spyware or attacks on known Windows vulnerabilities. These types of software could be

used to track passwords, execute code or take control of the machine, each making customer financial information potentially accessible. ScriptLogic solutions assist in securing the desktop from these threats.

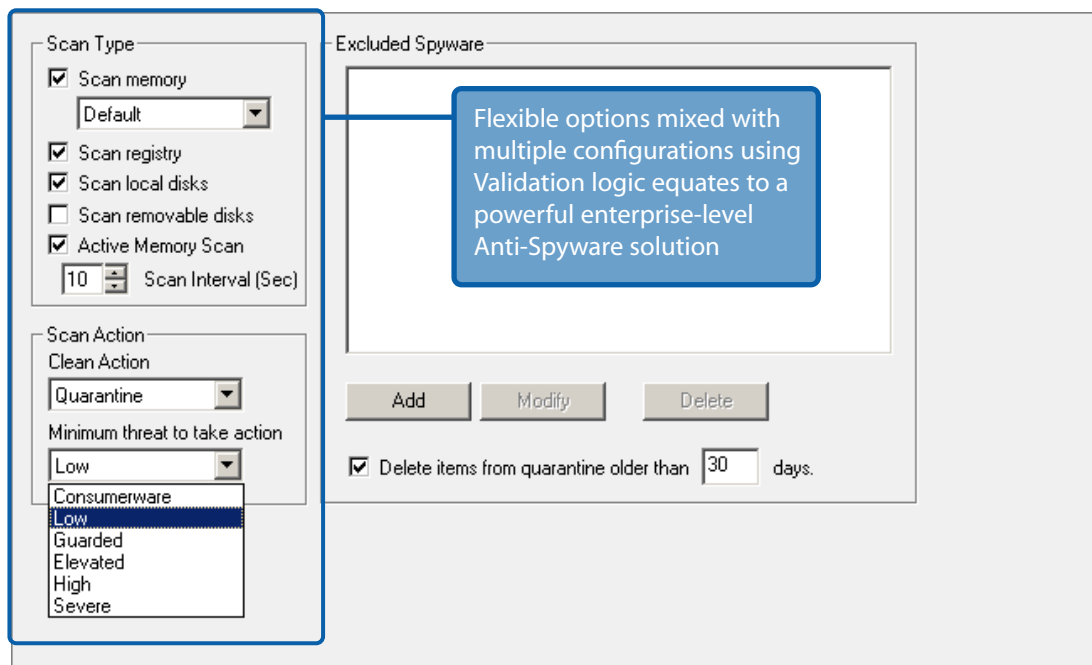
Example 8: Protecting against Spyware

ScriptLogic Solution: Desktop Authority's Spyware Detection and Removal option

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 11



Anti-Spyware Activity

Report Parameters: Variant Last Action Start Date: 1/1/1900, Variant Last Action End Date: 12/31/3000

Threat Level: ELEVATED

Variant Name: WebSearch Category: SEARCHPAGE Last Action: 6/3/2005 12:47 PM

Description: This is a toolbar that also serves as a search page hijacker. Websearch is also related to Wintools/Huntbar. Their toolbar and FAQs are located at http://www.websearch.com

Computer Name	Infection File Name	Infection Path	Action	Result	Action Time
TEST2	x.class	C:\Sample Spyware\Settings\Administrator.ANARCHY\Local Settings\Temp\VMwareDnD\	QUARANTINE	SUCCESS	6/3/2005 12:47 PM

Threat Level: GUARDED

Variant Name: ADeleterInternet Category: ADWARE Last Action: 6/3/2005 12:47 PM

Description: software that use popup as part of it advertising

Computer Name	Infection File Name	Infection Path	Action	Result	Action Time
TEST2	stntreco.exe	C:\Documents and Settings\Administrator.ANARCHY\Local Settings\Temp\VMwareDnD\	QUARANTINE	SUCCESS	6/3/2005 12:47 PM
TEST2	wupdnff.exe	C:\Documents and Settings\Administrator.ANARCHY\Local Settings\Temp\VMwareDnD\	QUARANTINE	SUCCESS	6/3/2005 12:47 PM

Threat Level: HIGH

Variant Name: nCase Category: THIEFWARE Last Action: 6/3/2005 12:47 PM

Description: No Description

Computer Name	Infection File Name	Infection Path	Action	Result	Action Time
TEST2	180ax.exe	C:\Documents and Settings\Administrator.ANARCHY\Local	QUARANTINE	SUCCESS	6/3/2005 12:47 PM

Report Date/Time: 6/13/2005 7:25 PM Page 4 of 5

Desktop Authority's Anti-Spyware reporting gives administrators a centralized bird-eye view of the state of their Windows network

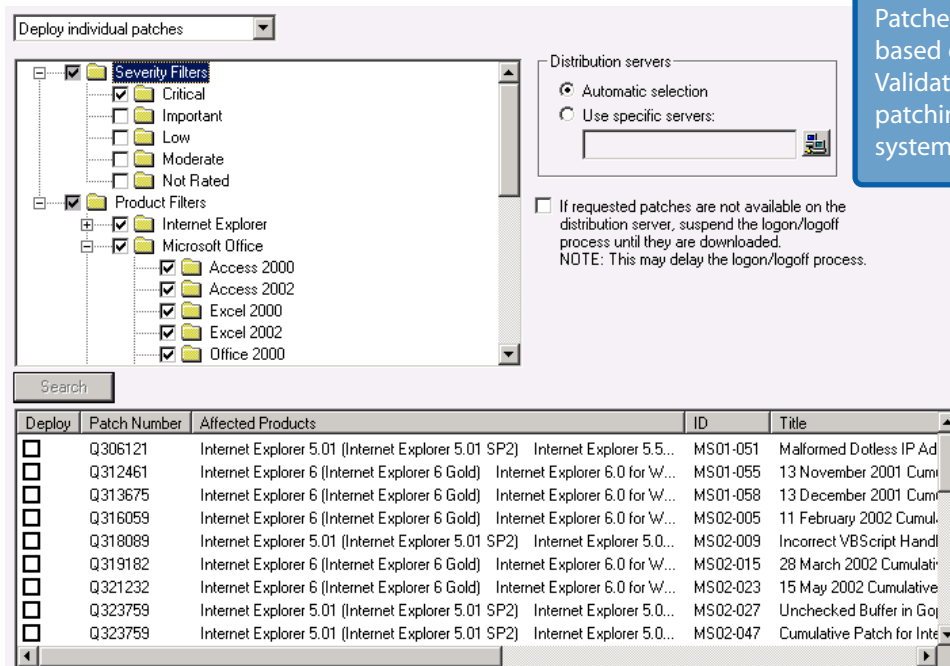
Figure 12

Example 9: Protect against known Vulnerabilities

ScriptLogic Solution: Desktop Authority's Patch Deployment for Desktops option

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 25 days. In order to ensure machines accessing customer financial 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 13, 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.



Patches can be selected based on Severity or Product. Validation Logic focuses the patching on only those systems you want affected.

Figure 13

Example 10: Patching Desktops and Servers

ScriptLogic Solution: Patch Authority Plus™

For those organizations wanting a single solution to patch both desktops **and** servers, ScriptLogic's Patch Authority Plus is the answer. Patching servers is not limited to just OS and applications; Patch Authority Plus, shown in Figure 14, secures

even the enterprise applications you run, such as IIS, SQL Server, Exchange, BizTalk and many more, making your entire Windows-based network secure from known vulnerabilities.

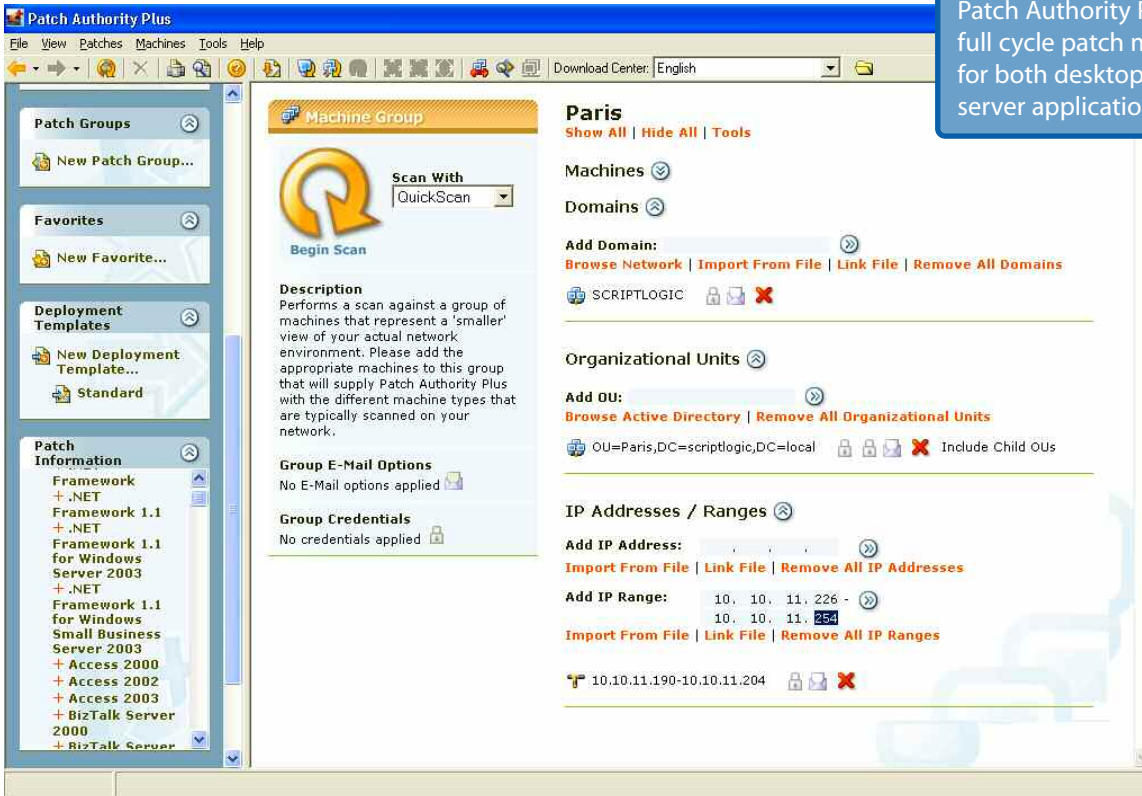


Figure 14

CONCLUSION

Because GLBA does not specify how to implement controls to protect customer financial information, organizations will utilize different tools and processes to achieve compliance. Protecting customer information requires a proactive assessment and enforcement of security controls in Active

Directory, on servers and on desktops, as well as a reactive assessment of those same imposed controls to ensure their effectiveness. ScriptLogic solutions give administrators the tools they need to assess, assign and audit security in Windows-based networks.

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