Implementing HIPAA Compliance with ScriptLogic

A ScriptLogic Product Positioning Paper
By Nick Cavalancia

Table of Contents

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 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 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.

HIPAA - BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in August 1996, placing new requirements on thousands of U.S. organizations involved with the provision of health care. Its two principle aims are:

1) To increase availability of healthcare by standardizing the exchange of healthcare information
2) To protect the confidentiality and security of patient records. Organizations that must comply with HIPAA are known as covered entities. These include health plans (e.g., HMOs, group health plans), health care clearinghouses (e.g. billing and repricing companies) and health care providers (e.g. doctors, dentists, hospitals). The HIPAA Privacy Rule came into effect in April 2001, requiring Covered Entities to come into compliance by April 2003, and formalized procedural restrictions on the handling of health care information.

However, the HIPAA Security Rule is much more demanding from an IT perspective since it covers the handling of individually identifiable health information where it is held in electronic form – referred to as electronic protected health information (EPHI). This covers all aspects of information relating to an individual's healthcare, with the goal of protecting the confidentiality, integrity and availability of EPHI whenever it is stored, maintained or transmitted. The final HIPAA Security Rule became effective as of April 21, 2003, with the result that most Covered Entities must be in compliance by April 21, 2005. (Small health plans with annual receipts of $5 million or less have until April 21, 2006).

The HIPAA Security Rule sets out standards requiring the physical safeguard of EPHI in addition to administrative and technical safeguards that lean heavily on IT systems. Software solutions from ScriptLogic play a key role in helping Covered Entities achieve compliance with these standards by giving IT administrators the power and control they need over their Windows-based networks to enforce appropriate safeguards.

ADMINISTRATIVE AND TECHNICAL SAFEGUARDS

The Administrative and technical safeguard requirements of the HIPAA Security Rule include a number of standards that ScriptLogic software solutions help Covered Entities to comply with. The table below highlights some of the required safeguards together with examples of typical operations IT administrators would perform in order to enforce those safeguards:

Control	Safeguard	HIPAA Security Rule Section	Action Required
Security Management Process	Risk Analysis	164.308(a)(1)(ii)(A)	Inspect permission settings for users and groups; ensure access levels are correct Scan systems to ensure up-to-date patches have been applied
	Risk Management	164.308(a)(1)(ii)(B)	Correctly apply security policies and patches to desktops
	Information System Activity Review	164.308(a)(1)(ii)(D)	Audit usage of Active Directory
Workforce Security	Authorization and/or Supervision	164.308(a)(3)(ii)(A)	Establish consistent Active Directory delegations Report on access to resources
Information Access Management	Access Establishment and Notification	164.308(a)(4)(ii)(C)	Centrally establish File System and Windows Share permissions
Security Awareness and Training	Periodic Security Updates	164.308(a)(5)(ii)(A)	Apply patches to Windows desktops and servers
	Protection from Malicious Software	164.308(a)(5)(ii)(B)	Actively scan for known Spyware on desktops
	Log On Monitoring	164.308(a)(5)(ii)(C)	Report on desktop log on activity
	Password Management	164.308(a)(5)(ii)(D)	Manage service account passwords
Contingency Plan	Disaster Recovery Plan	164.308(a)(7)(ii)(B)	Be able to restore AD and AD Security Be able to restore NTFS and Share Security
	Emergency Mode Operation Plan	164.308(a)(7)(ii)(C)	Centralize desktop configuration to facilitate emergency operations
Access Control	Automatic Logoff	164.312(a)(2)(iii)	Logoff inactive users
Audit Controls	Record and Examine Activity	164.312(b)	Audit file system usage

SOLUTIONS SUMMARY

ScriptLogic software solutions give organizations the tools they need to evaluate, secure and audit all aspects of their Windows-based infrastructure, bringing their internal controls into compliance with HIPAA .

In order to bring a covered entity 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 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 HIPAA 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 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 HIPAA compliance.

The remainder of this paper provides examples of how ScriptLogic products enable administrators to perform the necessary actions to ensure that the safeguards required by HIPAA are in place.

SECURITY MANAGEMENT PROCESS – SECTION 164.308(a)(1)

HIPAA's Security Rule first mandates that you "Implement policies and procedures to prevent, detect, contain, and correct security violations." This covers a wide range of actions to be taken by IT; in essence, every one of your desktops and servers, as well as your Active Directory all need to be considered within the context of this mandate.

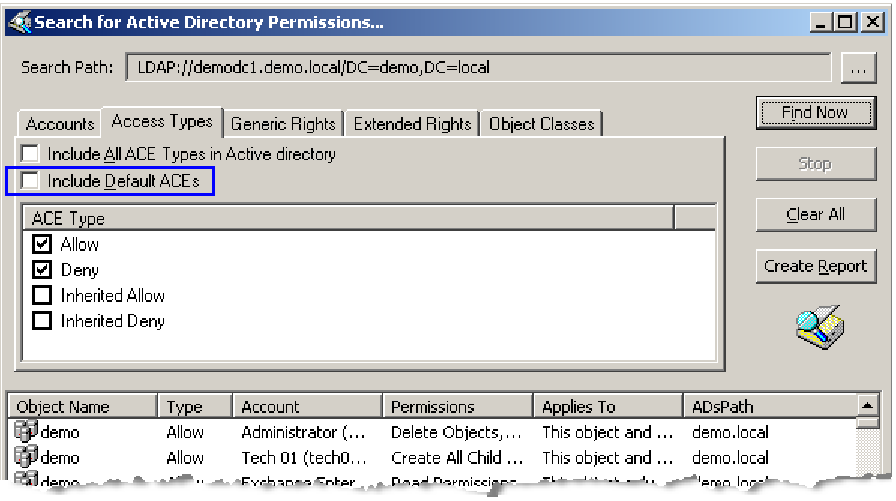
Example 1: Find Over-Privileged Users in Active Directory

Safeguard: **Risk Analysis**
ScriptLogic Solution: **Active Administrator**

At the heart of almost all Windows-based networks, Active Directory manages the security and privileges assigned to staff within a Covered Entity. 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 secured health records
- Addition of new computers into domains



Search for Active Directory Permissions...

Search Path: LDAP://demodc1.demo.local/DC=demo,DC=local

□ Include All ACE Types in Active directory
□ Include Default ACEs

ACE Type
☑ Allow
☑ Deny
□ Inherited Allow
□ Inherited Deny

Object Name	Type	Account	Permissions	Applies To	ADsPath
demo	Allow	Administrator (...	Delete Objects,...	This object and ...	demo.local
demo	Allow	Tech 01 (tech0...	Create All Child ...	This object and ...	demo.local
demo	[illegible]	Exchange Enter	Read Permissions	[illegible]	demo.local

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

Many other sections within the Security Rule require in-depth management and analysis of user security and privileges:

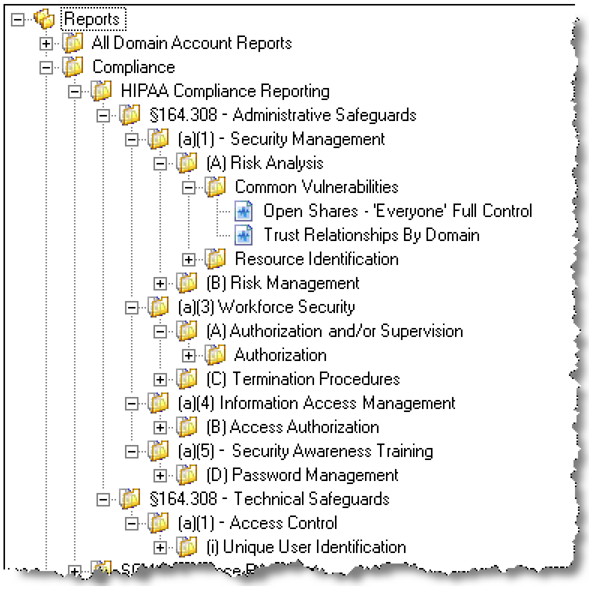
- Authorization Controls 164.308(a)(3)
- Assignment of Security Responsibilities 164.308(a)(2)
- Access Controls 164.312(a)(1)

Many of these requirements have a direct relationship with the management of permissions within Active Directory, making Active Administrator a vital part of any HIPAA compliance strategy in a Windows environment.

Example 2: Assess Permissions to Resources

Safeguard: **Risk Analysis, Workforce Security**
ScriptLogic Solution: **Enterprise Security Reporter, Enterprise Security Reporter for SharePoint**

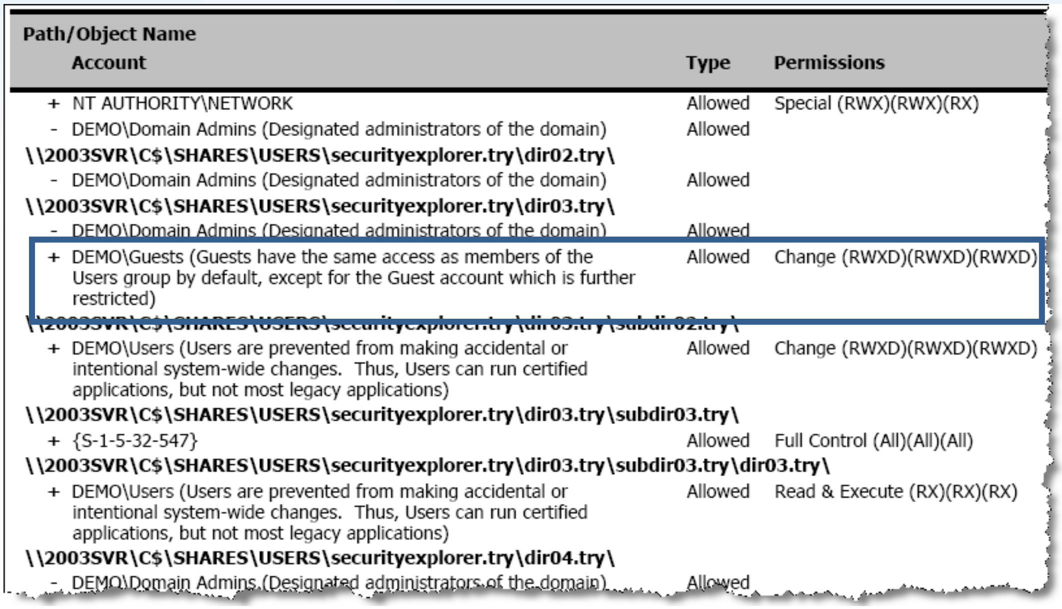
Enterprise Security Reporter scans a network of Windows servers and workstations, and analyzes the results using over 150 customizable, turn-key security reports, with reports categorized for HIPAA specifically (Figure 1). These reports are vital tools to help with various sections of the Security Rule. These reports also provide a formatted analysis of the security controls in place if needed during a review of HIPAA compliance by third parties.



- Reports
  - All Domain Account Reports
  - Compliance
    - HIPAA Compliance Reporting
      - §164.308 - Administrative Safeguards
        - (a)(1) - Security Management
          - (A) Risk Analysis
            - Common Vulnerabilities
              - Open Shares - 'Everyone' Full Control
              - Trust Relationships By Domain
            - Resource Identification
          - (B) Risk Management
        - (a)(3) Workforce Security
          - (A) Authorization and/or Supervision
            - Authorization
          - (C) Termination Procedures
        - (a)(4) Information Access Management
          - (B) Access Authorization
        - (a)(5) - Security Awareness Training
          - (D) Password Management
      - §164.308 - Technical Safeguards
        - (a)(1) - Access Control
          - (i) Unique User Identification

Figure 2: Reports are aligned to HIPAA requirements

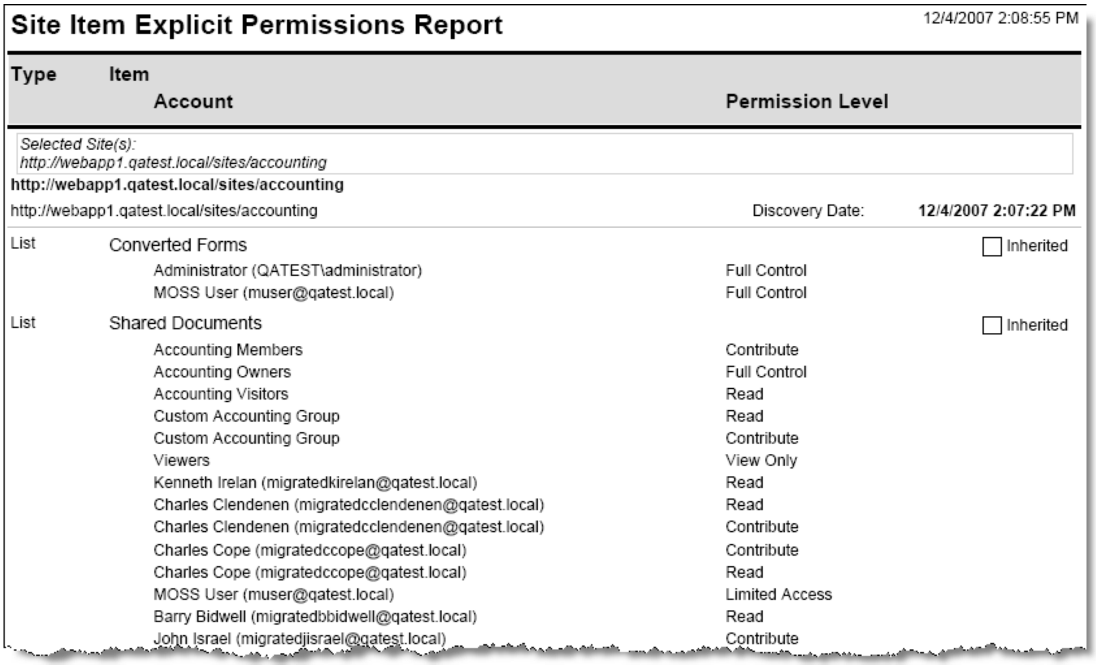
As an example, the analysis of file permissions can be done using the "Delta Permissions Reporting" function, which only shows file and folder permissions which differ from the parent folder to make it easier to identify all permissions which have been "added" to the inherited NTFS permissions, as shown in Figure 3. The result is that this report is an essential report for tracking down over-exposed files and folders, which might reveal a breach of EPHI 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 3: 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 4, highlights the permissions assigned to users and groups to give them access to SharePoint resources that may contain EPHI-related data.



Site Item Explicit Permissions Report 12/4/2007 2:08:55 PM

Selected Site(s):
http://webapp1.qatest.local/sites/accounting

http://webapp1.qatest.local/sites/accounting

http://webapp1.qatest.local/sites/accounting Discovery Date: **12/4/2007 2:07:22 PM**

Type	Item Account	Permission Level	
List	Converted Forms		□ Inherited
	Administrator (QATEST\administrator)	Full Control	
	MOSS User (muser@qatest.local)	Full Control	
List	Shared Documents		□ Inherited
	Accounting Members	Contribute	
	Accounting Owners	Full Control	
	Accounting Visitors	Read	
	Custom Accounting Group	Read	
	Custom Accounting Group	Contribute	
	Viewers	View Only	
	Kenneth Irelan (migratedkirelan@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	

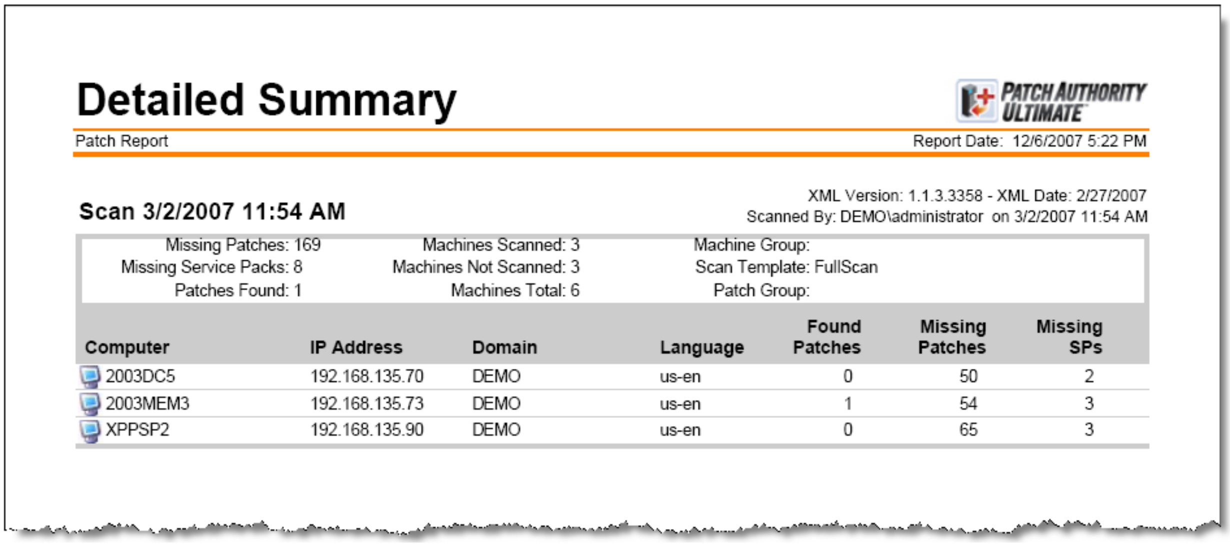
Figure 4: Quickly identify access to SharePoint resources

Example 3: Assess State of Patching

Safeguard: **Risk Analysis**

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 5.



Detailed Summary

PATCH AUTHORITY ULTIMATE

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:

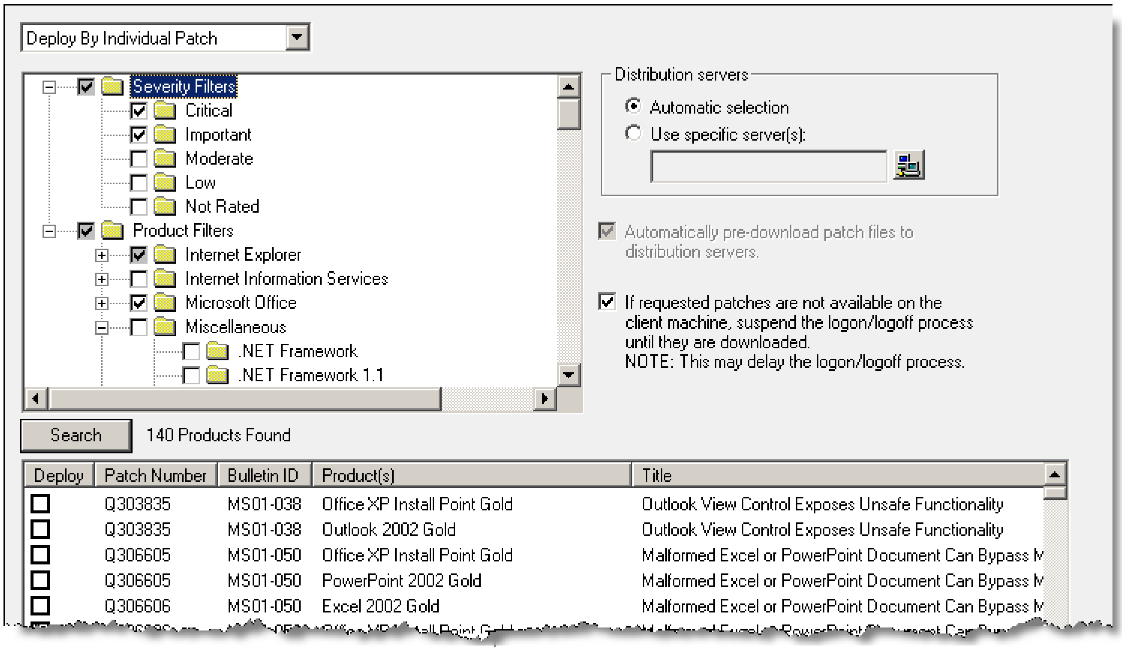
Computer	IP Address	Domain	Language	Found Patches	Missing Patches	Missing SPs
2003DC5	192.168.135.70	DEMO	us-en	0	50	2
2003MEM3	192.168.135.73	DEMO	us-en	1	54	3
XPPSP2	192.168.135.90	DEMO	us-en	0	65	3

Figure 5: Automatically analyze the state of Windows patching with Patch Authority Ultimate

Example 4: Ensure Up-To-Date Patches Have Been Applied

Safeguard: **Risk Management, Periodic Security Updates, Protection From Malicious Software**
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 6, 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.



Deploy By Individual Patch

- ☑ Severity Filters
  - ☑ Critical
  - ☑ Important
  - ☐ Moderate
  - ☐ Low
  - ☐ Not Rated
- ☑ Product Filters
  - ☑ Internet Explorer
  - ☐ Internet Information Services
  - ☑ Microsoft Office
  - ☐ Miscellaneous
    - ☐ .NET Framework
    - ☐ .NET Framework 1.1

Distribution servers
● Automatic selection
○ Use specific server(s):

☑ Automatically pre-download patch files to distribution servers.

☑ If requested patches are not available on the client machine, suspend the logon/logoff process until they are downloaded.
NOTE: This may delay the logon/logoff process.

Search   140 Products Found

Deploy	Patch Number	Bulletin ID	Product(s)	Title
☐	Q303835	MS01-038	Office XP Install Point Gold	Outlook View Control Exposes Unsafe Functionality
☐	Q303835	MS01-038	Outlook 2002 Gold	Outlook View Control Exposes Unsafe Functionality
☐	Q306605	MS01-050	Office XP Install Point Gold	Malformed Excel or PowerPoint Document Can Bypass M
☐	Q306605	MS01-050	PowerPoint 2002 Gold	Malformed Excel or PowerPoint Document Can Bypass M
☐	Q306606	MS01-050	Excel 2002 Gold	Malformed Excel or PowerPoint Document Can Bypass M

Figure 6: Patching both Microsoft and 3rd-party solutions is a critical step to managing your risk

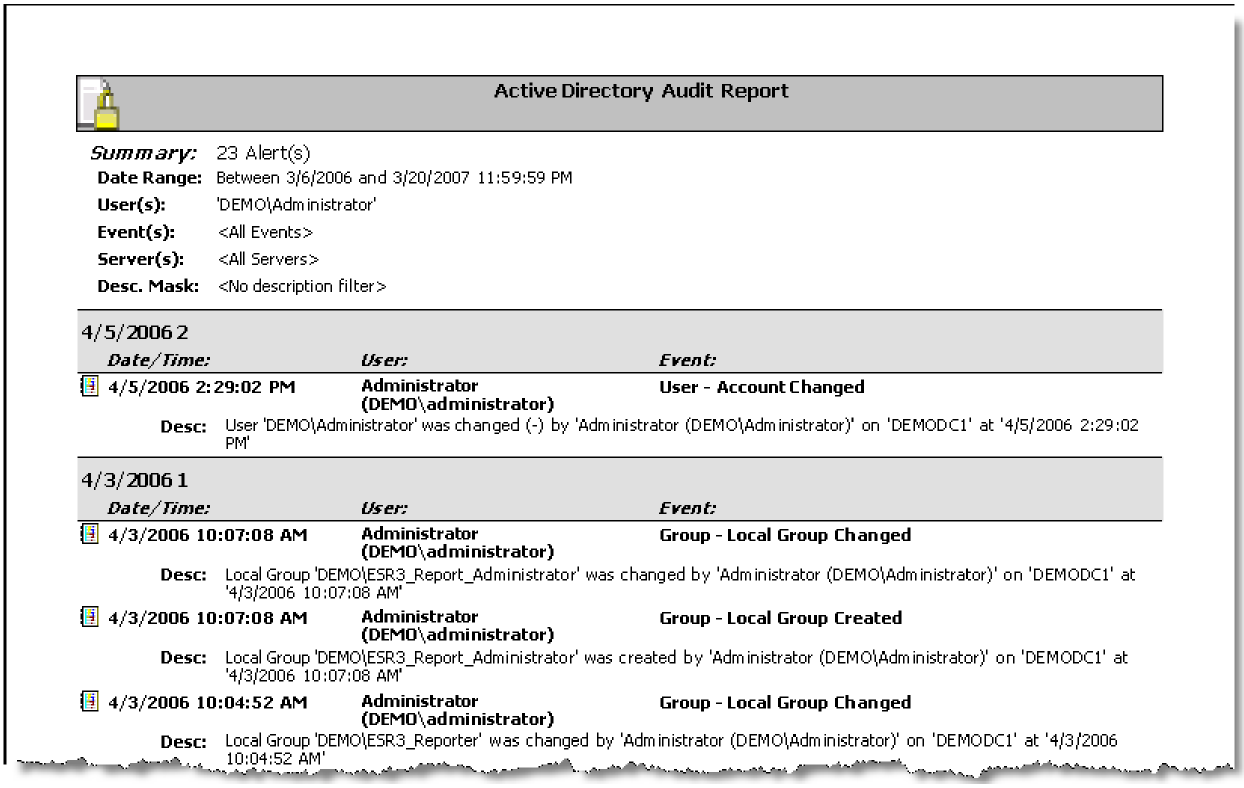
If you prefer a solution that patches both desktops and servers, Patch Authority Ultimate will patch Microsoft operating systems, enterprise applications (such as Exchange, SQL, etc), Microsoft applications (such as Office) and select 3rd party applications centrally.

Example 5: Auditing Active Directory Usage

Safeguard: **Information System Activity Review**

ScriptLogic Solution: **Active Administrator**

HIPAA Standards require a review of security changes in a Covered Entity's IT systems, as well as the ability to audit and analyze security settings for potential risks (this also applies to the Audit Controls required in section 164.312). 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 7. It also allows for long term storage of audit logs without the need for enormous event logs on individual servers.



Active Directory Audit Report

Summary: 23 Alert(s)
Date Range: Between 3/6/2006 and 3/20/2007 11:59:59 PM
User(s): 'DEMO\Administrator'
Event(s): <All Events>
Server(s): <All Servers>
Desc. Mask: <No description filter>

4/5/2006 2

Date/Time:	*User:*	*Event:*
4/5/2006 2:29:02 PM	**Administrator (DEMO\administrator)**	**User - Account Changed**

Desc: User 'DEMO\Administrator' was changed (-) by 'Administrator (DEMO\Administrator)' on 'DEMODC1' at '4/5/2006 2:29:02 PM'

4/3/2006 1

Date/Time:	*User:*	*Event:*
4/3/2006 10:07:08 AM	**Administrator (DEMO\administrator)**	**Group - Local Group Changed**
4/3/2006 10:07:08 AM	**Administrator (DEMO\administrator)**	**Group - Local Group Created**
4/3/2006 10:04:52 AM	**Administrator (DEMO\administrator)**	**Group - Local Group Changed**

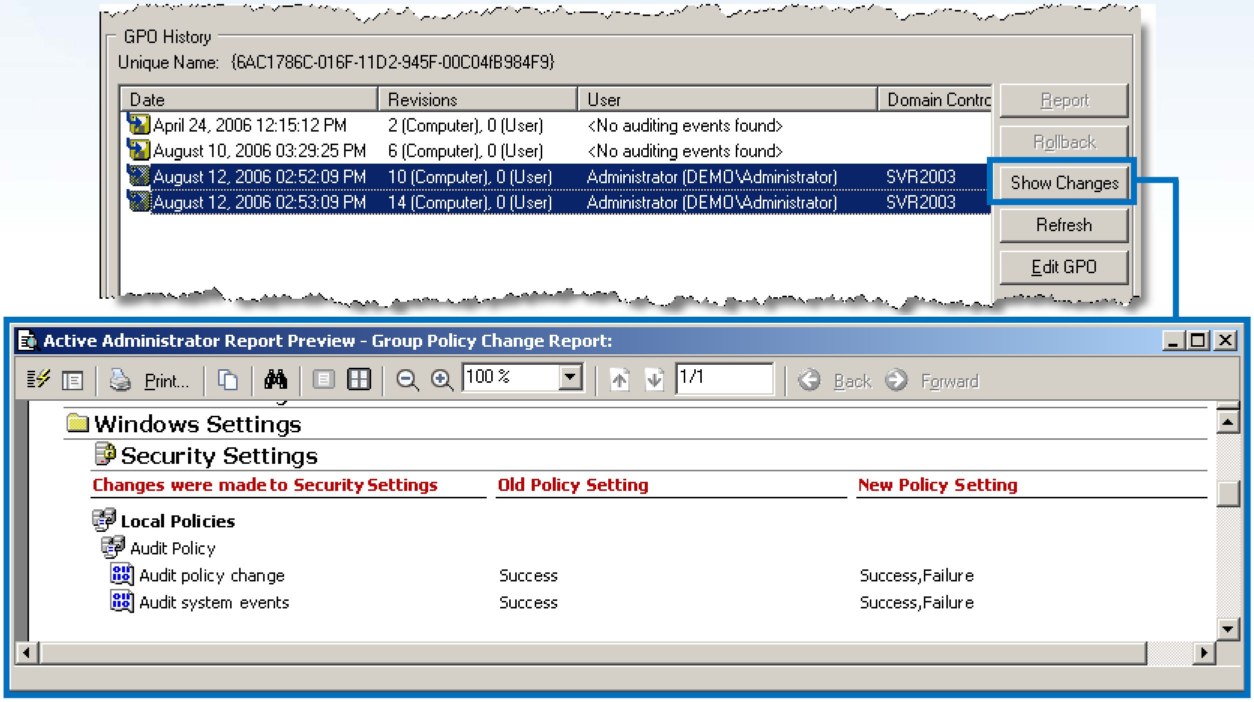
Desc: Local Group 'DEMO\ESR3_Report_Administrator' was changed by 'Administrator (DEMO\Administrator)' on 'DEMODC1' at '4/3/2006 10:07:08 AM'

Desc: Local Group 'DEMO\ESR3_Report_Administrator' was created by 'Administrator (DEMO\Administrator)' on 'DEMODC1' at '4/3/2006 10:07:08 AM'

Desc: Local Group 'DEMO\ESR3_Reporter' was changed by 'Administrator (DEMO\Administrator)' on 'DEMODC1' at '4/3/2006 10:04:52 AM'

Figure 7: 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 8.



GPO History

Unique Name: {6AC1786C-016F-11D2-945F-00C04fB984F9}

Date	Revisions	User	Domain Contro
April 24, 2006 12:15:12 PM	2 (Computer), 0 (User)	<No auditing events found>	
August 10, 2006 03:29:25 PM	6 (Computer), 0 (User)	<No auditing events found>	
August 12, 2006 02:52:09 PM	10 (Computer), 0 (User)	Administrator (DEMO\Administrator)	SVR2003
August 12, 2006 02:53:09 PM	14 (Computer), 0 (User)	Administrator (DEMO\Administrator)	SVR2003

Active Administrator Report Preview - Group Policy Change Report:

Windows Settings

Security Settings

Changes were made to Security Settings	Old Policy Setting	New Policy Setting
Local Policies		
Audit Policy		
Audit policy change	Success	Success,Failure
Audit system events	Success	Success,Failure

Figure 8: Reviewing Group Policy management activity with Active Administrator

WORKFORCE SECURITY – SECTION 164.308(a)(3)

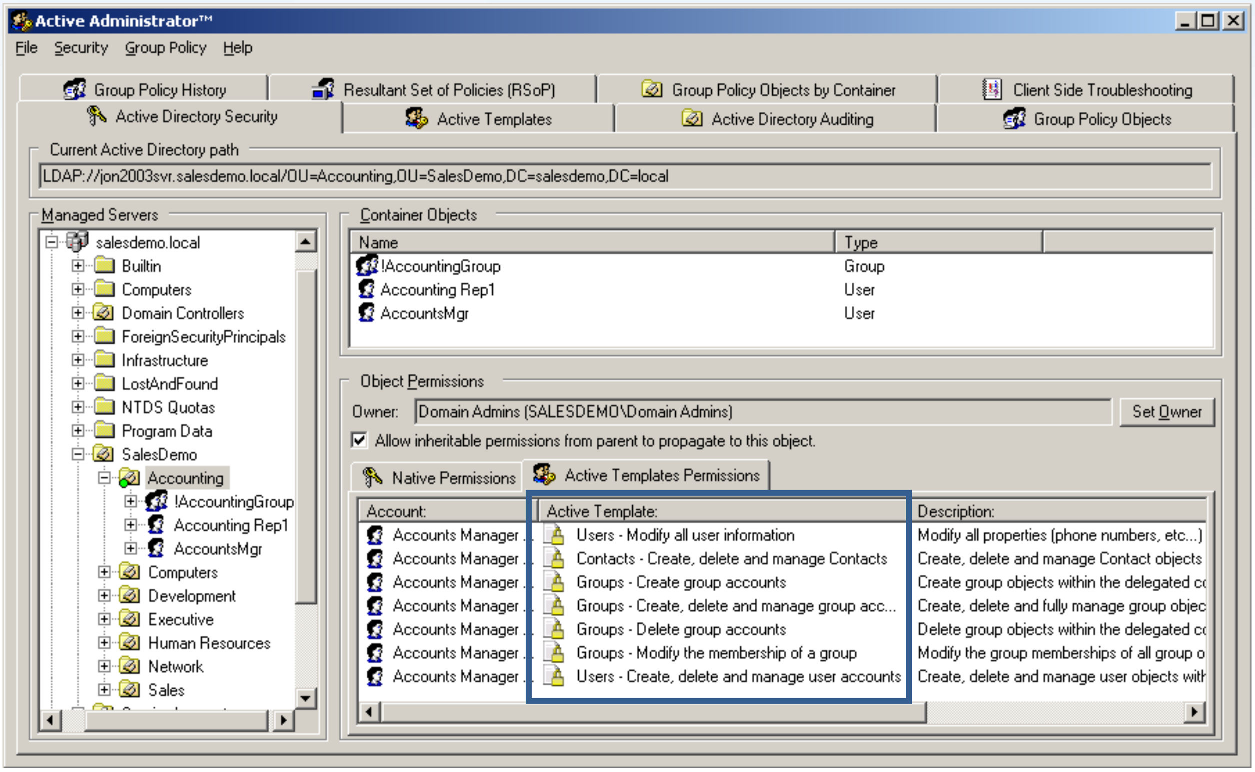
Workforce Security safeguards are in place to ensure a covered entity’s emphasis is on ensuring that “all members of its workforce have appropriate access to electronic protected health information.”

Example 6: Establish Consistent Active Directory Delegations

Safeguard: **Authorization and/or Supervision**
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 9. 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 HIPAA Access Controls, Assigned Security Responsibility and Security Management requirements.



Current Active Directory path: LDAP://jon2003svr.salesdemo.local/OU=Accounting,OU=SalesDemo,DC=salesdemo,DC=local

Name	Type
!AccountingGroup	Group
Accounting Rep1	User
AccountsMgr	User

Owner: Domain Admins (SALESDEMO\Domain Admins)

☑ Allow inheritable permissions from parent to propagate to this object.

Account:	Active Template:	Description:
Accounts Manager	Users - Modify all user information	Modify all properties (phone numbers, etc...)
Accounts Manager	Contacts - Create, delete and manage Contacts	Create, delete and manage Contact objects
Accounts Manager	Groups - Create group accounts	Create group objects within the delegated co
Accounts Manager	Groups - Create, delete and manage group acc...	Create, delete and fully manage group objec
Accounts Manager	Groups - Delete group accounts	Delete group objects within the delegated co
Accounts Manager	Groups - Modify the membership of a group	Modify the group memberships of all group o
Accounts Manager	Users - Create, delete and manage user accounts	Create, delete and manage user objects with

Figure 9: 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.

INFORMATION ACCESS MANAGEMENT – SECTION 164.308(a)(4)

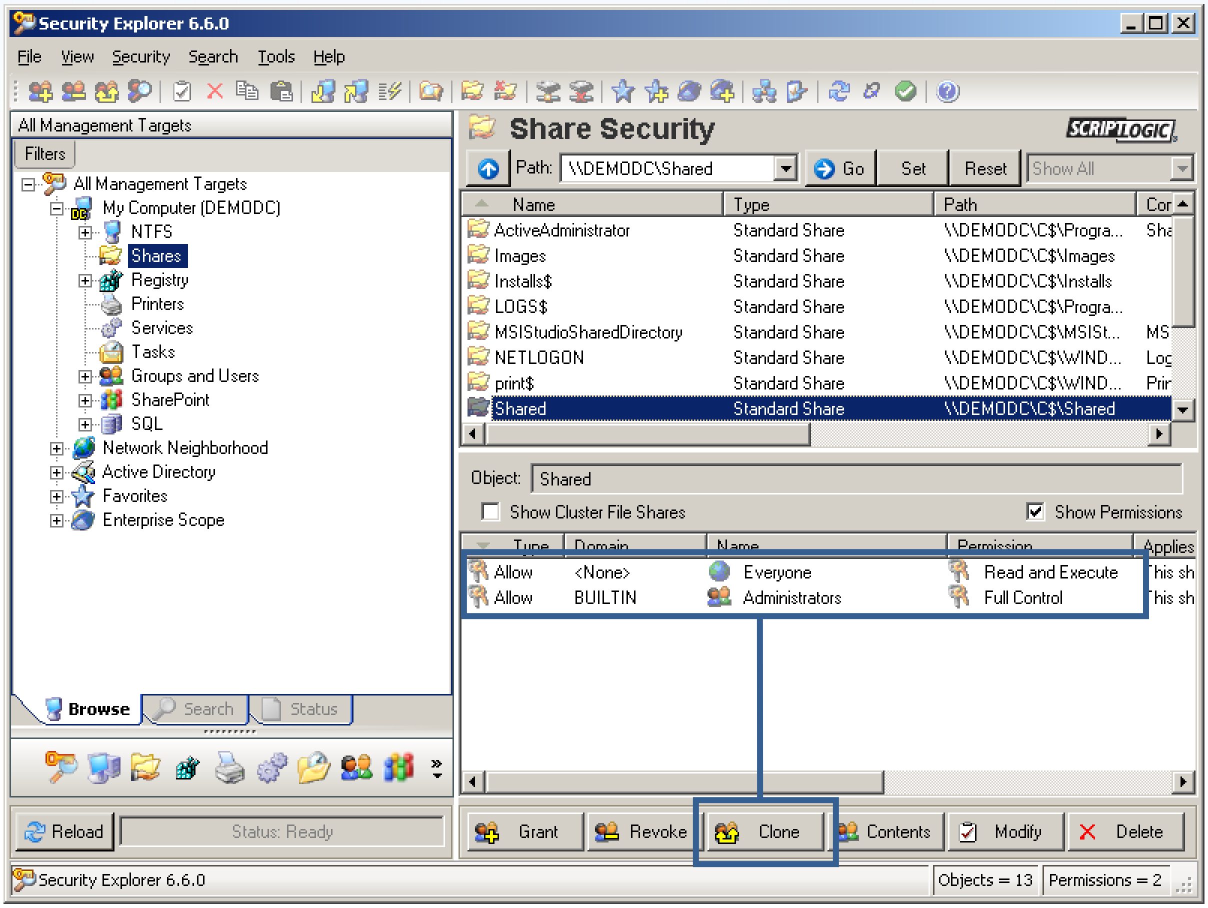
This section of the HIPAA Security Rule focuses on implementing "policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements." So the task in this section is to implement that you planned for in previous sections of the Security Rule.

Example 7: Centrally Establish File System, Share, SQL and SharePoint Permissions

Safeguard: **Access Establishment and Notification**
ScriptLogic Solution: **Security Explorer, Security Explorer for SQL, Security Explorer for SharePoint**

While data residing on Windows, SQL and SharePoint servers can be secured in a one-off fashion, the consistency desired by Section 164.308(a)(4) 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 SharePoint sites.

As shown in Figure 10, Security Explorer can manage and clone permissions consistently on NTFS volumes, Shares, SQL databases and tables, and SharePoint sites.



Path: \\DEMODC\Shared

Name	Type	Path	Cor
ActiveAdministrator	Standard Share	\\DEMODC\C$\Progra...	Sha
Images	Standard Share	\\DEMODC\C$\Images	
Installs$	Standard Share	\\DEMODC\C$\Installs	
LOGS$	Standard Share	\\DEMODC\C$\Progra...	
MSIStudioSharedDirectory	Standard Share	\\DEMODC\C$\MSISt...	MS
NETLOGON	Standard Share	\\DEMODC\C$\WIND...	Log
print$	Standard Share	\\DEMODC\C$\WIND...	Prir
Shared	Standard Share	\\DEMODC\C$\Shared	

Object: Shared

☐ Show Cluster File Shares ☑ Show Permissions

Type	Domain	Name	Permission	Applies
Allow	<None>	Everyone	Read and Execute	This sh
Allow	BUILTIN	Administrators	Full Control	This sh

Figure 10: Centralized Assignment and Cloning of permissions with Security Explorer

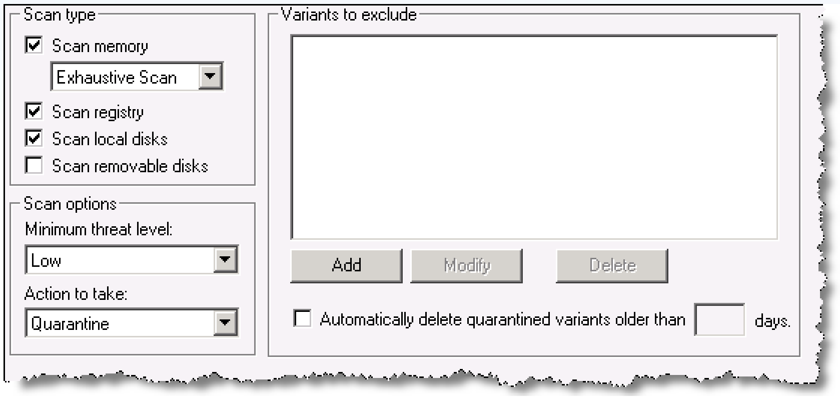
SECURITY AWARENESS AND TRAINING – SECTION 164.308(a)(5)

While the verbiage of this section seems to point to simply making the workforce and management aware of security risks, the implementation steps all have to do with the actual securing of systems against known vulnerabilities, which include Spyware, security flaws, password management and others.

Example 8: Scan for Known Spyware on Desktops

Safeguard: **Protection From Malicious Software**
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 11 shows the configuration options available and Figure 12 shows DA's Spyware reporting capabilities.



Scan type

☑ Scan memory

Exhaustive Scan

☑ Scan registry

☑ Scan local disks

☐ Scan removable disks

Scan options

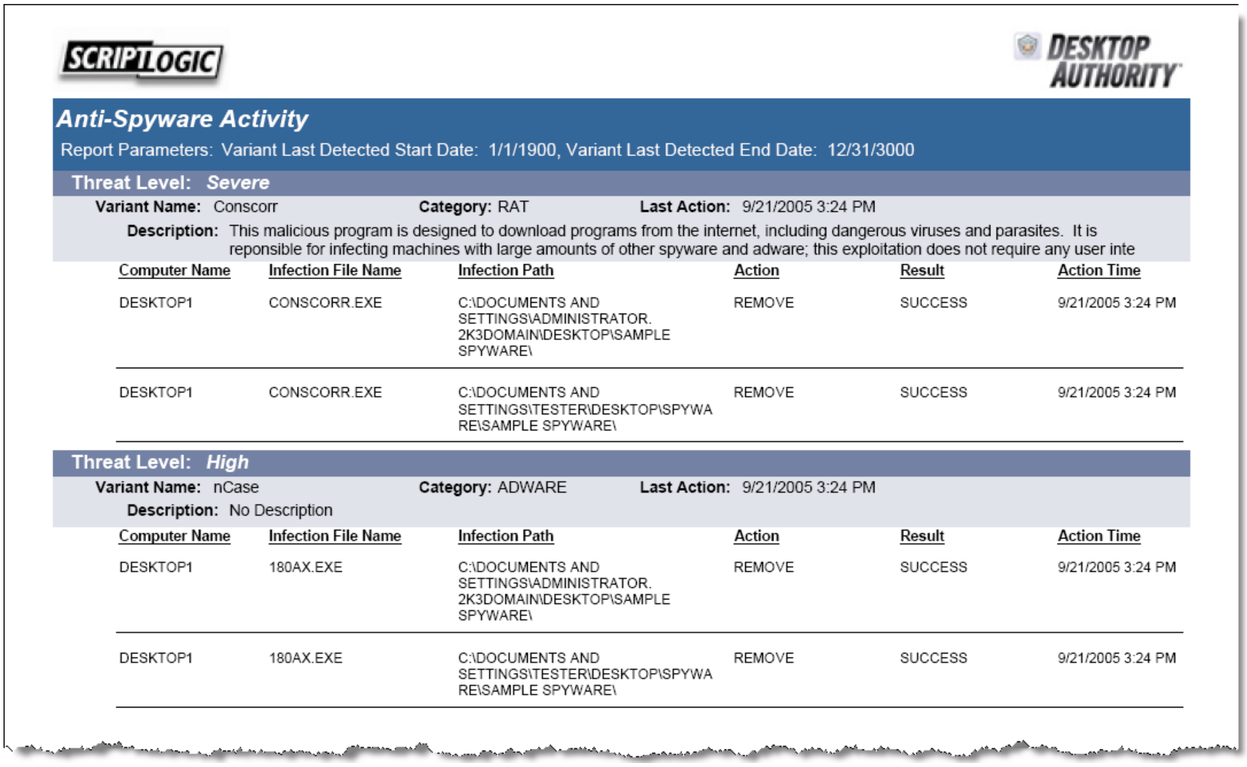
Minimum threat level: Low

Action to take: Quarantine

Variants to exclude

☐ Automatically delete quarantined variants older than ☐ days.

Figure 11: Desktop Authority's powerful Anti-Spyware option is comprised of flexible options mixed with multiple configurations using Validation Logic



Anti-Spyware Activity

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

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 reponsible for infecting machines with large amounts of other spyware and adware; this exploitation does not require any user inte

Computer Name	Infection File Name	Infection Path	Action	Result	Action Time
DESKTOP1	CONSCORR.EXE	C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR. 2K3DOMAIN\DESKTOP\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM
DESKTOP1	CONSCORR.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP\SPYWARE\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

Computer Name	Infection File Name	Infection Path	Action	Result	Action Time
DESKTOP1	180AX.EXE	C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR. 2K3DOMAIN\DESKTOP\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM
DESKTOP1	180AX.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP\SPYWARE\SAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM

Figure 12: Centralized reporting ensures IT is aware of the Spyware outbreaks and their removal

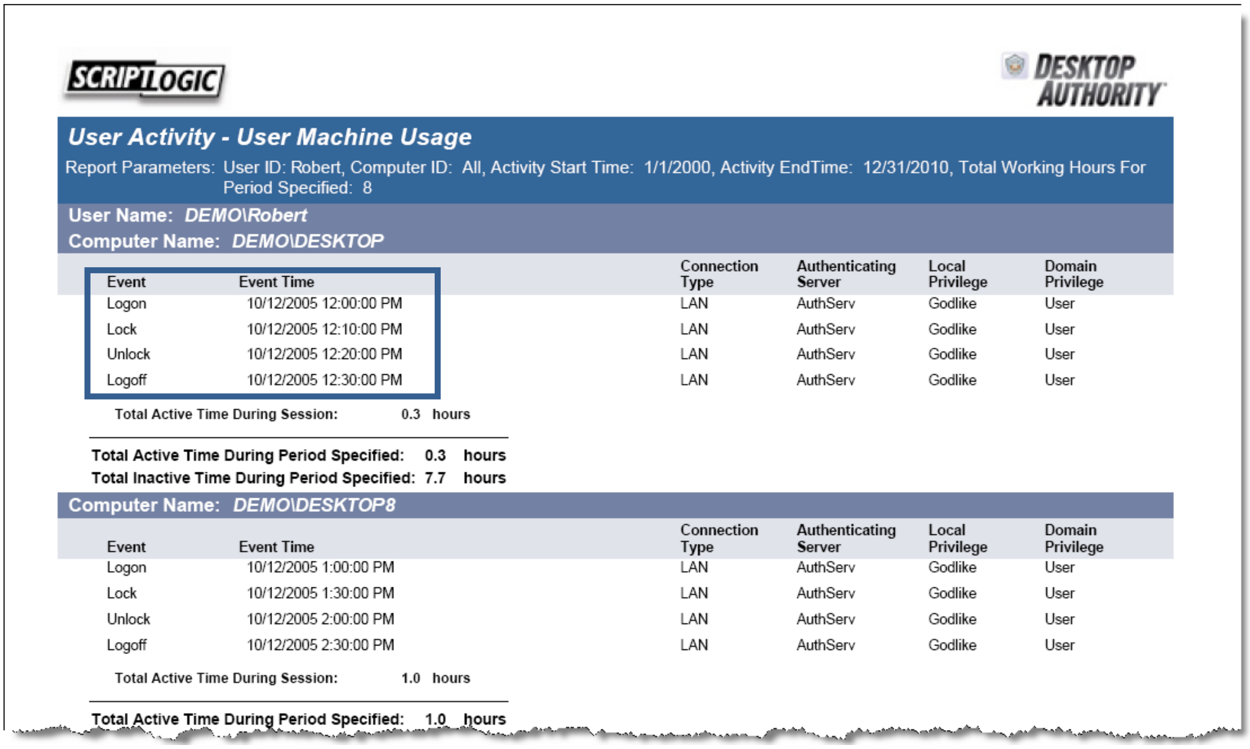
Example 9: Monitor Desktop Logon Activity

Safeguard: **Log On Monitoring**

ScriptLogic Solution: **Desktop Authority**

Monitoring the logging onto your network will allow you to look for inconsistencies (the CEO logging in from a desktop in the mailroom, for example) to identify potential risks; either those where someone is maliciously logging on using another user’s credentials to steal information, or someone logging onto an inappropriate machine where access to patient information may be gained, should the user step away from the machine.

Desktop Authority logs each users activity, from logging on, to locking and unlocking a secured desktop, to logging off, giving IT a comprehensive view, as shown in Figure 13, into user activity throughout the business day.



User Activity - User Machine Usage

Report Parameters: User ID: Robert, Computer ID: All, Activity Start Time: 1/1/2000, Activity EndTime: 12/31/2010, Total Working Hours For Period Specified: 8

User Name: DEMO\Robert
Computer Name: DEMO\DESKTOP

Event	Event Time	Connection Type	Authenticating Server	Local Privilege	Domain Privilege
Logon	10/12/2005 12:00:00 PM	LAN	AuthServ	Godlike	User
Lock	10/12/2005 12:10:00 PM	LAN	AuthServ	Godlike	User
Unlock	10/12/2005 12:20:00 PM	LAN	AuthServ	Godlike	User
Logoff	10/12/2005 12:30:00 PM	LAN	AuthServ	Godlike	User

Total Active Time During Session: 0.3 hours

Total Active Time During Period Specified: 0.3 hours
Total Inactive Time During Period Specified: 7.7 hours

Computer Name: DEMO\DESKTOP8

Event	Event Time	Connection Type	Authenticating Server	Local Privilege	Domain Privilege
Logon	10/12/2005 1:00:00 PM	LAN	AuthServ	Godlike	User
Lock	10/12/2005 1:30:00 PM	LAN	AuthServ	Godlike	User
Unlock	10/12/2005 2:00:00 PM	LAN	AuthServ	Godlike	User
Logoff	10/12/2005 2:30:00 PM	LAN	AuthServ	Godlike	User

Total Active Time During Session: 1.0 hours

Total Active Time During Period Specified: 1.0 hours

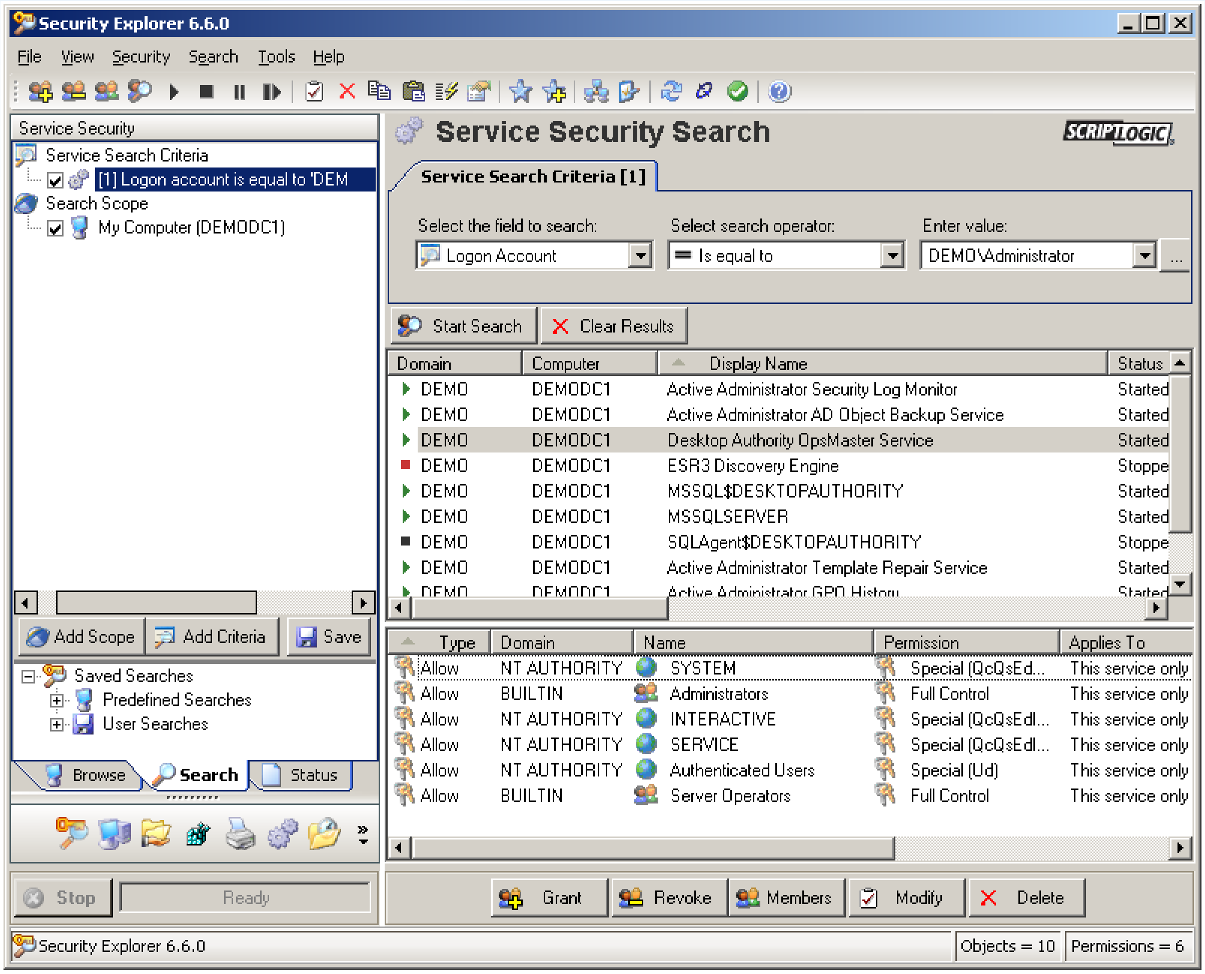
Figure 13: Reporting on user logons, as well as desktop locks/unlocks and logoffs with Desktop Authority

Example 10: Managing Service Account Passwords

Safeguard: **Password Management**
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 60 days!

Security Explorer, in addition to centrally managing NTFS, Share, Registry and Printer permissions, also manages Services and the accounts using them. Figure 14 shows how a simple query of services based on criteria such as the service account name, the service name, startup type and more. With Security Explorer, the resultant set of services can be simultaneously managed, as shown in Figure 15.



Select the field to search: Logon Account

Select search operator: = Is equal to

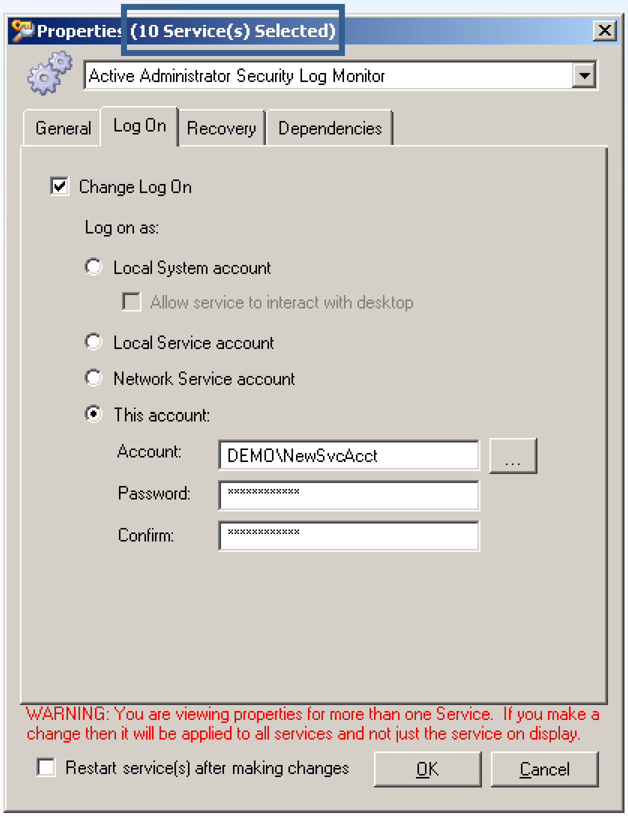
Enter value: DEMO\Administrator

Domain	Computer	Display Name	Status
DEMO	DEMODC1	Active Administrator Security Log Monitor	Started
DEMO	DEMODC1	Active Administrator AD Object Backup Service	Started
DEMO	DEMODC1	Desktop Authority OpsMaster Service	Started
DEMO	DEMODC1	ESR3 Discovery Engine	Stoppe
DEMO	DEMODC1	MSSQL$DESKTOPAUTHORITY	Started
DEMO	DEMODC1	MSSQLSERVER	Started
DEMO	DEMODC1	SQLAgent$DESKTOPAUTHORITY	Stoppe
DEMO	DEMODC1	Active Administrator Template Repair Service	Started
DEMO	DEMODC1	Active Administrator GPO History	Started

Type	Domain	Name	Permission	Applies To
Allow	NT AUTHORITY	SYSTEM	Special (QcQsEd...	This service only
Allow	BUILTIN	Administrators	Full Control	This service only
Allow	NT AUTHORITY	INTERACTIVE	Special (QcQsEdI...	This service only
Allow	NT AUTHORITY	SERVICE	Special (QcQsEdI...	This service only
Allow	NT AUTHORITY	Authenticated Users	Special (Ud)	This service only
Allow	BUILTIN	Server Operators	Full Control	This service only

Security Explorer 6.6.0 | Objects = 10 | Permissions = 6

Figure 14: Services are queried using the Search field based on several Service-specific criteria



Properties (10 Service(s) Selected)

Active Administrator Security Log Monitor

☑ Change Log On

Log on as:

○ Local System account

□ Allow service to interact with desktop

○ Local Service account

○ Network Service account

● This account:

Account: DEMO\NewSvcAcct

Password: ************

Confirm: ************

WARNING: You are viewing properties for more than one Service. If you make a change then it will be applied to all services and not just the service on display.

□ Restart service(s) after making changes

Figure 15: Multiple Services can be modified at once to modify service accounts or other properties

CONTINGENCY PLAN – SECTION 164.308(a)(7)

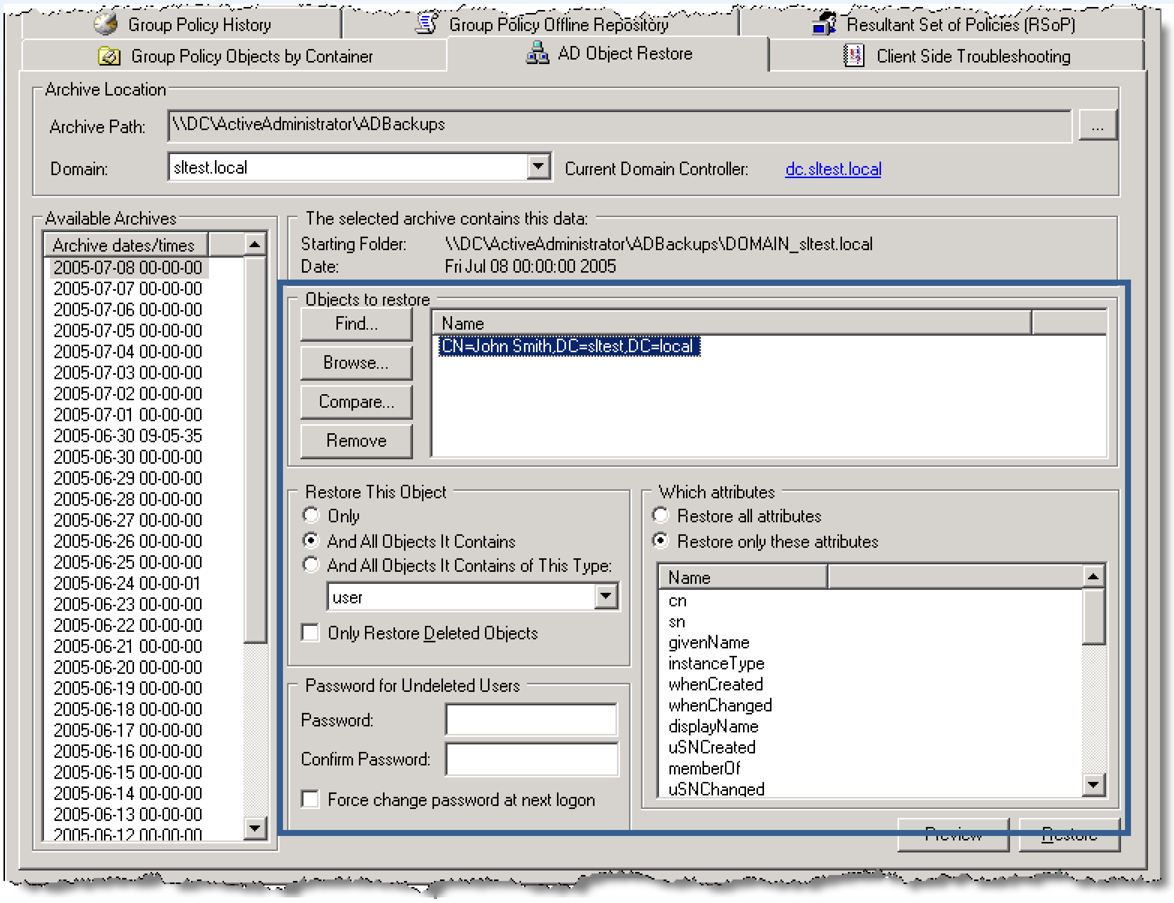
While the concept of a contingency plan is probably a familiar one, this section of the Security Rule is really about being able to either reestablish or recreate the environment that contains protected health information.

Example 11: Restore Active Directory and Active Directory Security

Safeguard: **Disaster Recovery Plan**

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 16.


Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
...
Find...
Browse...
Compare...
Remove
Preview
Restore

Archive Location

Archive Path: \\DC\ActiveAdministrator\ADBackups

Domain: sltest.local ▼ Current Domain Controller: dc.sltest.local

Available Archives

Archive dates/times
2005-07-08 00-00-00
2005-07-07 00-00-00
2005-07-06 00-00-00
2005-07-05 00-00-00
2005-07-04 00-00-00
2005-07-03 00-00-00
2005-07-02 00-00-00
2005-07-01 00-00-00
2005-06-30 09-05-35
2005-06-30 00-00-00
2005-06-29 00-00-00
2005-06-28 00-00-00
2005-06-27 00-00-00
2005-06-26 00-00-00
2005-06-25 00-00-00
2005-06-24 00-00-01
2005-06-23 00-00-00
2005-06-22 00-00-00
2005-06-21 00-00-00
2005-06-20 00-00-00
2005-06-19 00-00-00
2005-06-18 00-00-00
2005-06-17 00-00-00
2005-06-16 00-00-00
2005-06-15 00-00-00
2005-06-14 00-00-00
2005-06-13 00-00-00
2005-06-12 00-00-00

The selected archive contains this data:
Starting Folder: \\DC\ActiveAdministrator\ADBackups\DOMAIN_sltest.local
Date: Fri Jul 08 00:00:00 2005

Objects to restore

Name
CN=John Smith,DC=sltest,DC=local

Restore This Object
○ Only
● And All Objects It Contains
○ And All Objects It Contains of This Type:
user ▼
□ Only Restore Deleted Objects

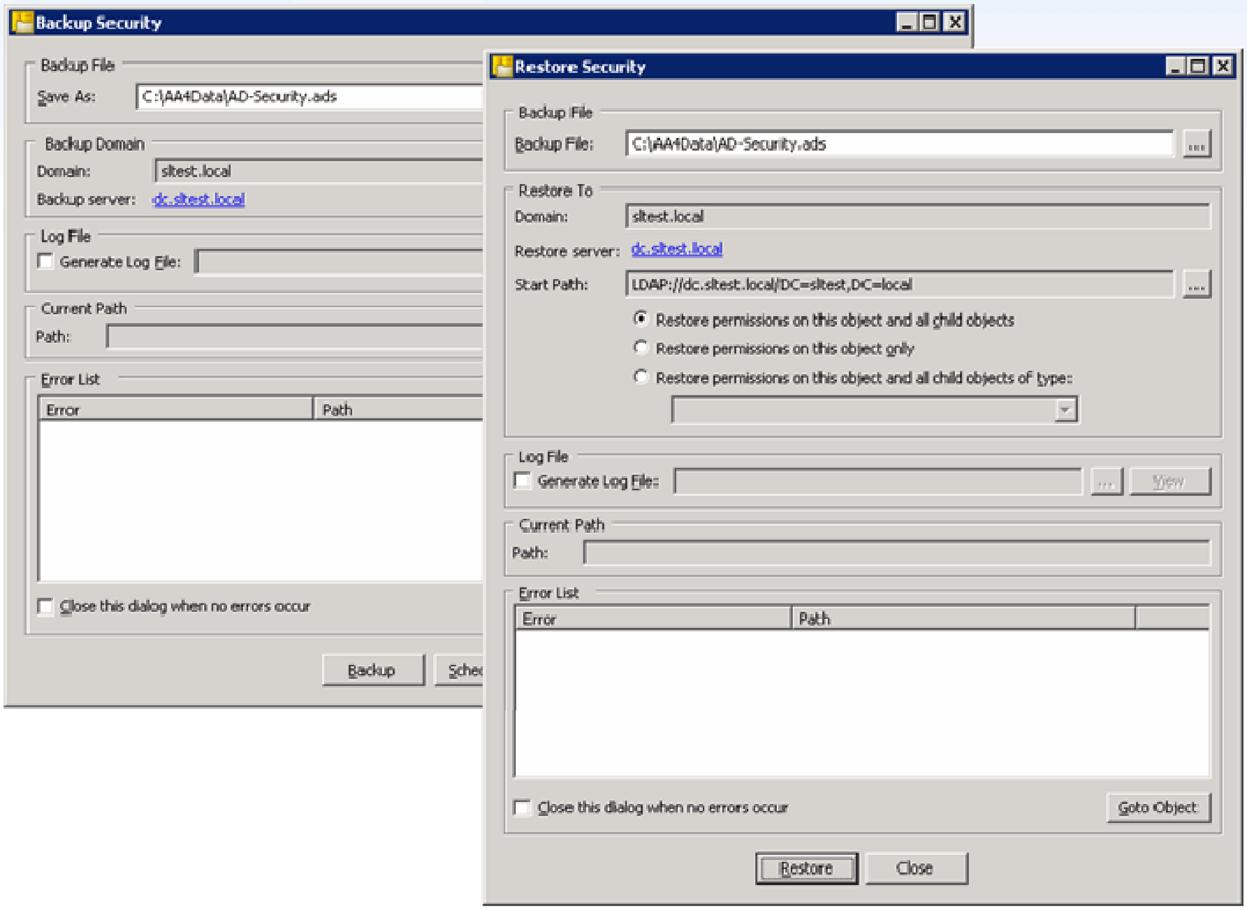
Which attributes
○ Restore all attributes
● Restore only these attributes

Name
cn
sn
givenName
instanceType
whenCreated
whenChanged
displayName
uSNCreated
memberOf
uSNChanged

Password for Undeleted Users
Password:
Confirm Password:
□ Force change password at next logon

Figure 16: 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 17) 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.



Backup Security

Backup File
Save As: C:\AA4Data\AD-Security.ads

Backup Domain
Domain: sltest.local
Backup server: dc.sltest.local

Log File
□ Generate Log File:

Current Path
Path:

Error List

Error	Path

□ Close this dialog when no errors occur

Restore Security

Backup File
Backup File: C:\AA4Data\AD-Security.ads

Restore To
Domain: sltest.local
Restore server: dc.sltest.local
Start Path: LDAP://dc.sltest.local/DC=sltest,DC=local
● Restore permissions on this object and all child objects
○ Restore permissions on this object only
○ Restore permissions on this object and all child objects of type:

Log File
□ Generate Log File:

Current Path
Path:

Error List

Error	Path

□ Close this dialog when no errors occur

Figure 17: Active Administrator backs up and restores AD permissions increasing the availability of AD administration.

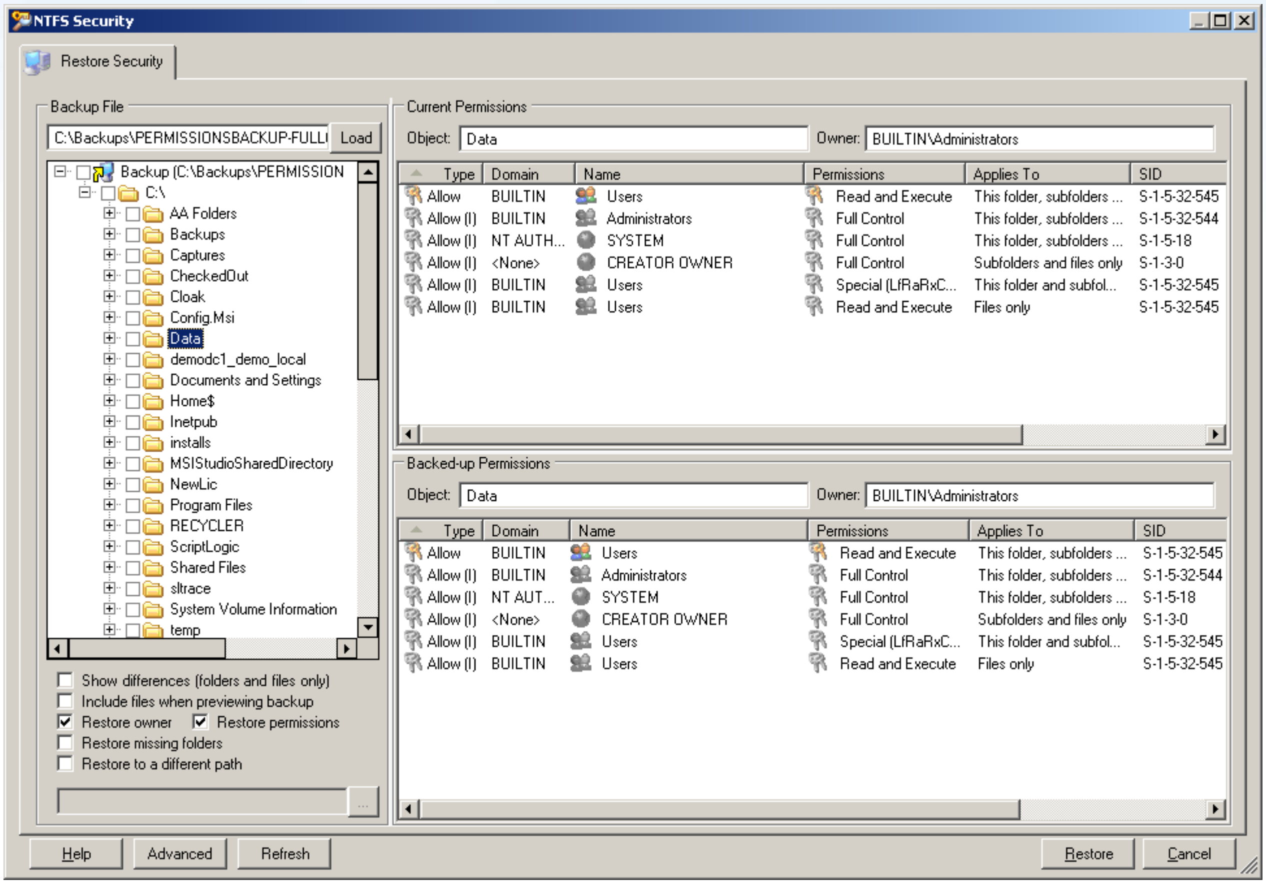
Example 12: Restoring Windows, SQL and SharePoint Security

Safeguard: **Disaster Recovery Plan**

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 Server and SharePoint permissions. Some administrators even use Security Explorer to perform hourly backups of the permission settings on their security-sensitive file, SQL and SharePoint servers so that if a security breach is suspected and permissions appear to have changed, they can quickly reset all data 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 18, ensures that security is maintained and data is only available where intended.



Backup File: C:\Backups\PERMISSIONSBACKUP-FULL(Load

- □ Backup (C:\Backups\PERMISSION
  - □ C:\
    - □ AA Folders
    - □ Backups
    - □ Captures
    - □ CheckedOut
    - □ Cloak
    - □ Config.Msi
    - □ Data
    - □ democd1_demo_local
    - □ Documents and Settings
    - □ Home$
    - □ Inetpub
    - □ installs
    - □ MSIStudioSharedDirectory
    - □ NewLic
    - □ Program Files
    - □ RECYCLER
    - □ ScriptLogic
    - □ Shared Files
    - □ sltrace
    - □ System Volume Information
    - □ temp

□ Show differences (folders and files only)
□ Include files when previewing backup
☑ Restore owner ☑ Restore permissions
□ Restore missing folders
□ Restore to a different path

Current Permissions

Object: Data Owner: BUILTIN\Administrators

Type	Domain	Name	Permissions	Applies To	SID
Allow	BUILTIN	Users	Read and Execute	This folder, subfolders ...	S-1-5-32-545
Allow (I)	BUILTIN	Administrators	Full Control	This folder, subfolders ...	S-1-5-32-544
Allow (I)	NT AUTH...	SYSTEM	Full Control	This folder, subfolders ...	S-1-5-18
Allow (I)	<None>	CREATOR OWNER	Full Control	Subfolders and files only	S-1-3-0
Allow (I)	BUILTIN	Users	Special (LfRaRxC...	This folder and subfol...	S-1-5-32-545
Allow (I)	BUILTIN	Users	Read and Execute	Files only	S-1-5-32-545

Backed-up Permissions

Object: Data Owner: BUILTIN\Administrators

Type	Domain	Name	Permissions	Applies To	SID
Allow	BUILTIN	Users	Read and Execute	This folder, subfolders ...	S-1-5-32-545
Allow (I)	BUILTIN	Administrators	Full Control	This folder, subfolders ...	S-1-5-32-544
Allow (I)	NT AUT...	SYSTEM	Full Control	This folder, subfolders ...	S-1-5-18
Allow (I)	<None>	CREATOR OWNER	Full Control	Subfolders and files only	S-1-3-0
Allow (I)	BUILTIN	Users	Special (LfRaRxC...	This folder and subfol...	S-1-5-32-545
Allow (I)	BUILTIN	Users	Read and Execute	Files only	S-1-5-32-545

Figure 18: Restoring Share, Registry, SQL and SharePoint permissions is similar to restoring NTFS permissions, shown here

Example 13: Create the Disaster-Proof Desktop

Safeguard: **Emergency Mode Operation Plan**

ScriptLogic Solution: **Desktop Authority**

To maintain privacy of patient health information even in an emergency, systems must be properly configured. Usually desktops are managed by a variety of solutions: Group Policies, scripts, a patching solution, etc. Each of these solutions doesn't necessarily adapt well or even support working in an alternative configuration during an emergency. To have a desktop DR plan, two things need to be in place: first, the configuration of the desktop must be centrally controlled. Second, there must be a way to have an alternate configuration. Desktop Authority manages nearly every aspect of the user's desktop, as shown in Figure 19.

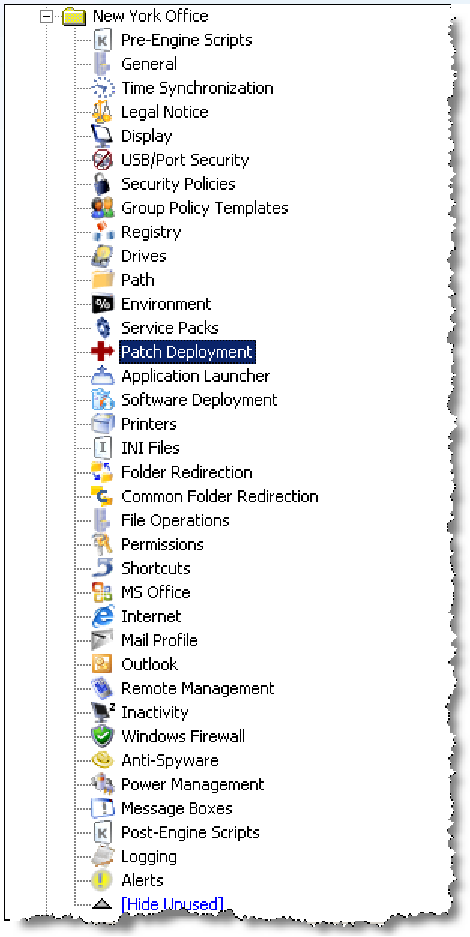
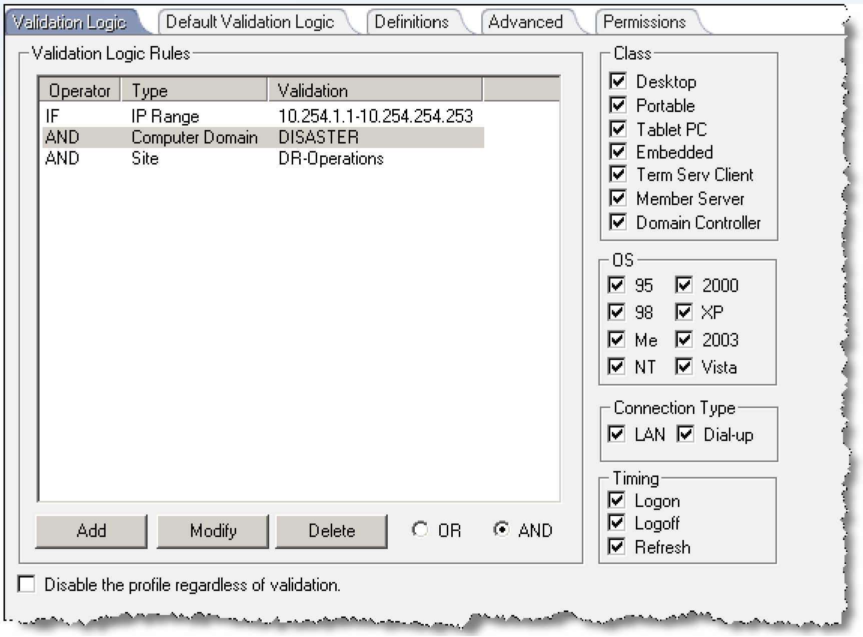


Figure 19: Desktop Authority's comprehensive configuration centralizes all of your desktop settings

The challenge for most IT professionals is how to get the same configuration working in a disaster scenario – different server names, printers, IP addresses, etc. Desktop Authority uses two technologies to accomplish this issue quickly and easily. The first is the concept of a *profile* which groups settings together. With Desktop Authority, you can have one profile for normal operations and one for disaster scenarios. The second concept is Desktop Authority's patented Validation Logic, which is used to determine who will get the configuration of a profile or a specific configuration element within the profile. With Desktop Authority, a DR profile would be created and Validation Logic, shown in Figure 20, would be configured to only run with DR conditions were met (such as running from a specific IP address range or if the users were logging in from a specific domain.



Validation Logic Rules

Operator	Type	Validation
IF	IP Range	10.254.1.1-10.254.254.253
AND	Computer Domain	DISASTER
AND	Site	DR-Operations

○ OR ● AND

Class
☑ Desktop
☑ Portable
☑ Tablet PC
☑ Embedded
☑ Term Serv Client
☑ Member Server
☑ Domain Controller

OS
☑ 95 ☑ 2000
☑ 98 ☑ XP
☑ Me ☑ 2003
☑ NT ☑ Vista

Connection Type
☑ LAN ☑ Dial-up

Timing
☑ Logon
☑ Logoff
☑ Refresh

□ Disable the profile regardless of validation.

Figure 20: Easily establish a DR-specific configuration using Validation Logic to identify DR settings

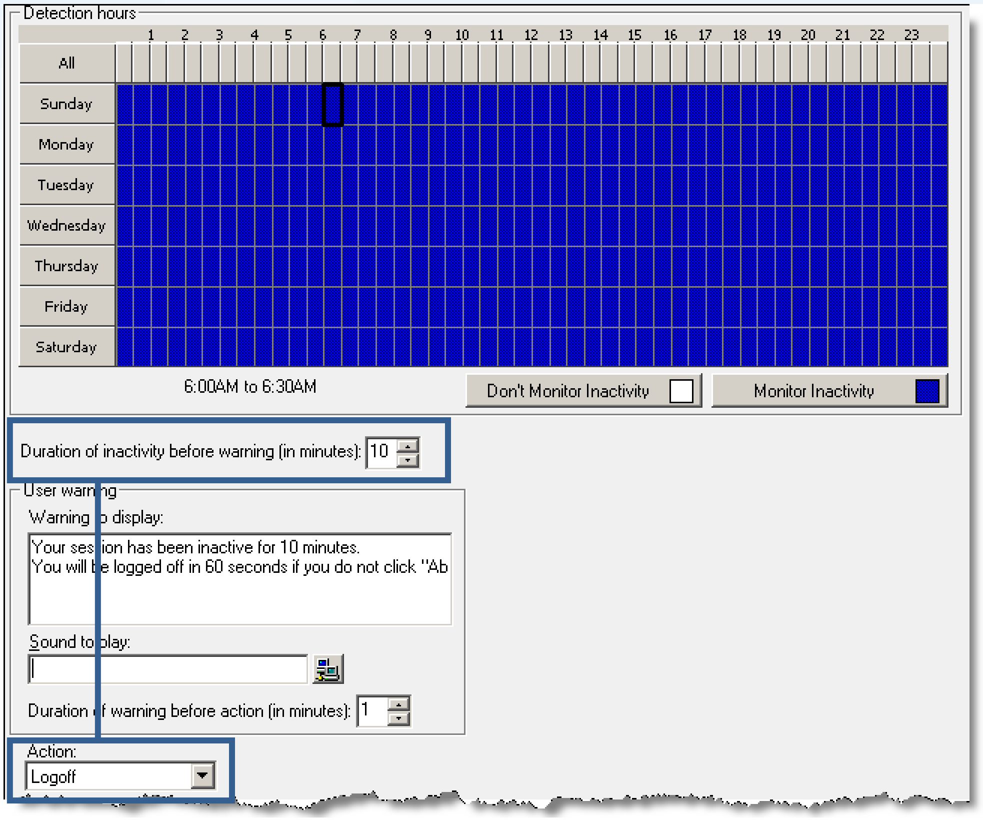
ACCESS CONTROLS – SECTION 164.312(a)(2)

This section is all about user's having the minimum access required ("Allow access only to those persons or software programs that have been granted access rights") to tighten both the number of individuals who have access to patient health information, but also the type of access those individuals have as well.

Example 14: Logging Off Inactive Users

Safeguard: **Automatic Logoff**
ScriptLogic Solution: **Desktop Authority**

Automatic logoff of a user is required to ensure the protection of EPHI when an authenticated user leaves their workstation without logging-off or locking it. Desktop Authority offers the administrator a highly configurable method for ensuring user logoff, lockout or even shutdown after a specified period of inactivity, as shown in Figure 21. This works on all PCs running Windows 95, 98, Me, NT4, XP, 2000, 2003 or Vista.



6:00AM to 6:30AM

Duration of inactivity before warning (in minutes): 10

Warning to display:

Your session has been inactive for 10 minutes.
You will be logged off in 60 seconds if you do not click "Ab

Sound to play:

Duration of warning before action (in minutes): 1

Action: Logoff

Figure 21: After a specified period of inactivity, users can be logged off, shutdown or rebooted, as desired.

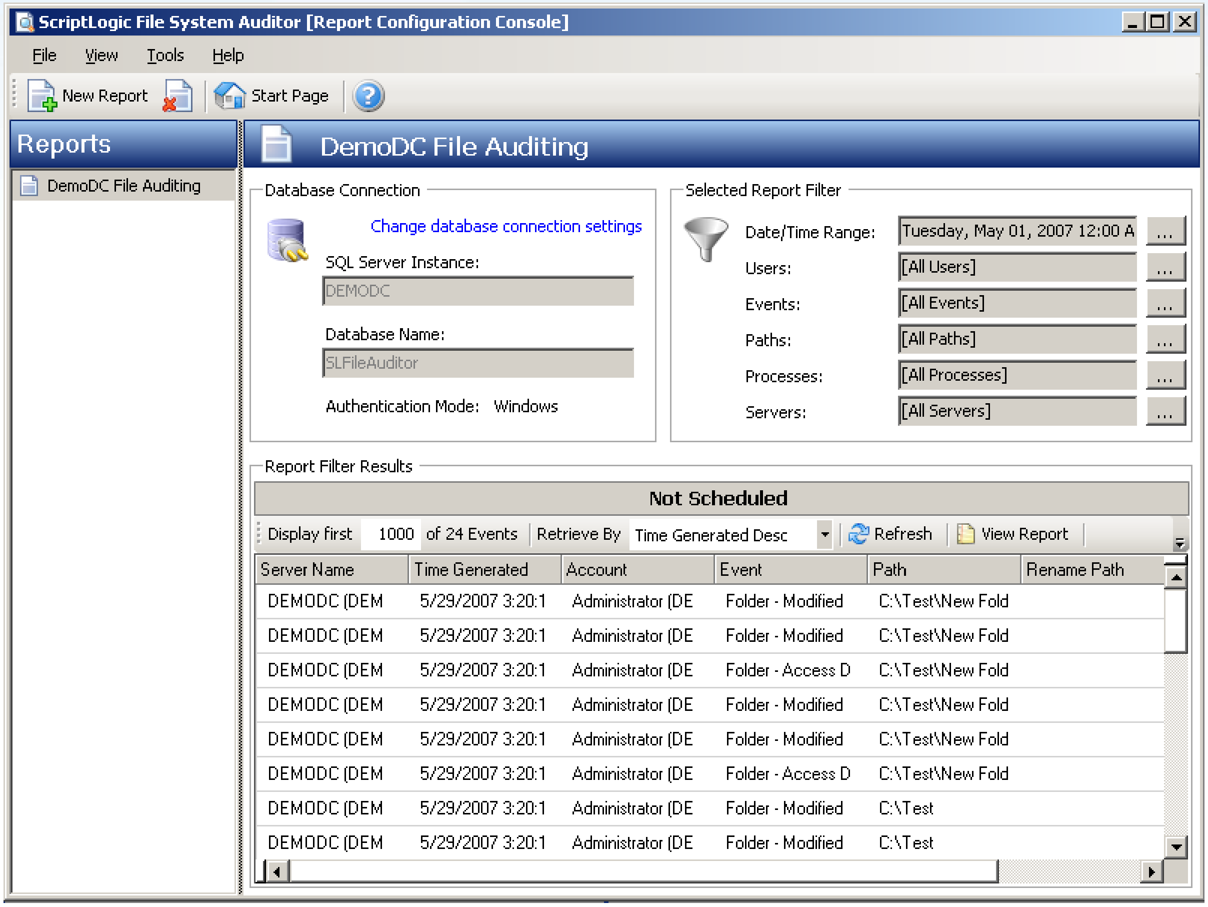
AUDIT CONTROLS – SECTION 164.312(b)

Once the Access Controls are put into place, the Security Rule seeks to ensure you have your eyes on systems by requiring you to put into place "mechanisms that record and examine activity in information systems that contain or use electronic protected health information." With proper auditing in place, the access controls can be validated as providing adequate security.

Example 15: Audit File System Usage

Safeguard: **Record and Examine Activity**
ScriptLogic Solution: **File System Auditor**

Since patient health information can find its way into formal letters from Doctors, 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 22.



DemoDC File Auditing

Database Connection

Change database connection settings

SQL Server Instance: DEMODC

Database Name: SLFileAuditor

Authentication Mode: Windows

Selected Report Filter

Date/Time Range:	Tuesday, May 01, 2007 12:00 A
Users:	[All Users]
Events:	[All Events]
Paths:	[All Paths]
Processes:	[All Processes]
Servers:	[All Servers]

Report Filter Results

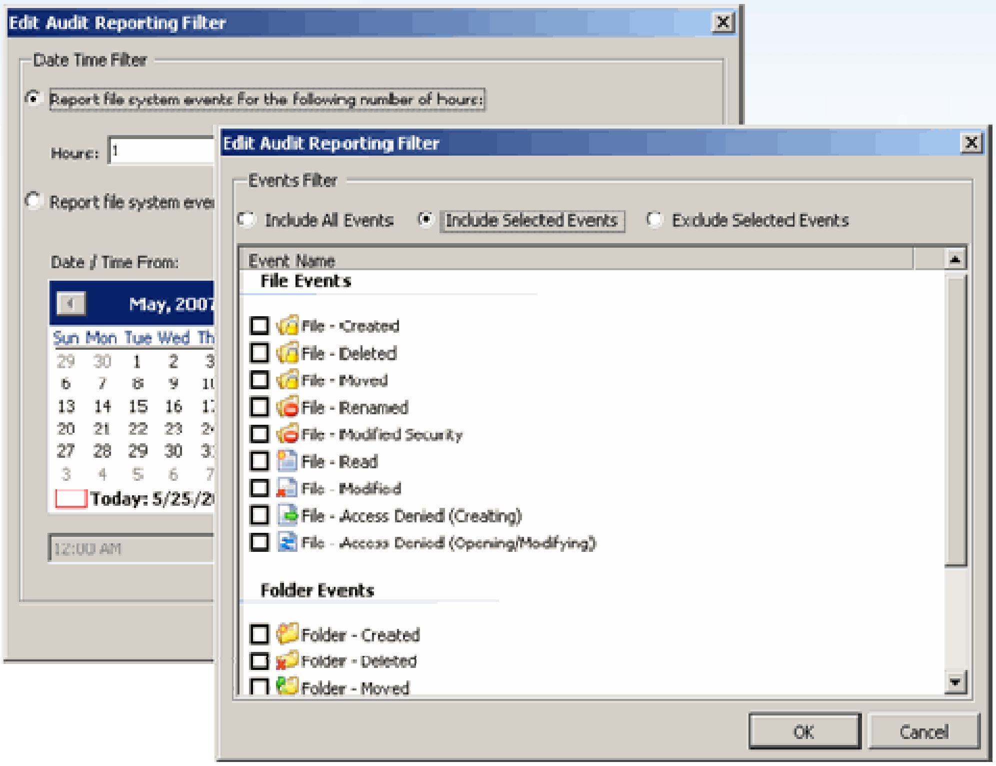
Not Scheduled

Display first 1000 of 24 Events Retrieve By Time Generated Desc Refresh View Report

Server Name	Time Generated	Account	Event	Path	Rename Path
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Access D	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Access D	C:\Test\New Fold	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test	
DEMODC (DEM	5/29/2007 3:20:1	Administrator (DE	Folder - Modified	C:\Test	

Figure 22: 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 23.



Edit Audit Reporting Filter

Date Time Filter

● Report file system events for the following number of hours:

Hours: 1

○ Report file system eve

Date / Time From:

12:00 AM

Edit Audit Reporting Filter

Events Filter

○ Include All Events ● Include Selected Events ○ Exclude Selected Events

Event Name

File Events

□ File - Created
□ File - Deleted
□ File - Moved
□ File - Renamed
□ File - Modified Security
□ File - Read
□ File - Modified
□ File - Access Denied (Creating)
□ File - Access Denied (Opening/Modifying)

Folder Events

□ Folder - Created
□ Folder - Deleted
□ Folder - Moved

Figure 23: Selection of auditing criteria is a simple process

CONCLUSION

The HIPAA Security Rule requires considerable effort by Covered Entities to bring their administrative and technical systems into compliance. Many of the increased security and system maintenance requirements fall squarely onto the shoulders of IT administrators, who need tools to ensure the security of EPHI across their enterprise.

The requirements of the Administrative and Technical Safeguards specified in the Security Rule imply the need for a wide variety of IT solutions including Active Directory security, NTFS file security, desktop management and password management tools. Furthermore, the need for continual evaluation of the extent to which security processes meet HIPAA requirements requires extensive reporting and investigative capabilities.

ScriptLogic products give administrators the power they need to ensure EPHI security throughout their Windows-based networks, and to scan and report on security settings to demonstrate HIPAA 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 HIPAA compliance.

ScriptLogic solutions that assist with HIPAA 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 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 HIPAA compliance please visit www.scriptlogic.com/hipaa, or contact your ScriptLogic sales representative or Authorized ScriptLogic Channel Partner.