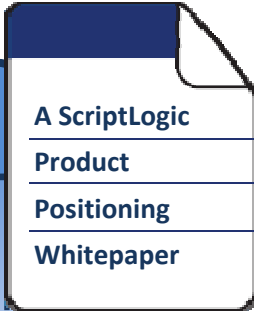




**IMPLEMENTING PCI
COMPLIANCE CONTROLS
WITH SCRIPTLOGIC**



NICK CAVALANCIA

Table of Contents

- INTRODUCTION 3
- PCI - BACKGROUND..... 3
- SECURITY PRINCIPLES AND REQUIREMENTS 4
- SOLUTIONS SUMMARY 6
- BUILD AND MAINTAIN A SECURE NETWORK 7
 - Example 1: Configure the Windows XP Firewall 7
 - Example 2: Managing Services..... 8
- MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM 9
 - Example 3: Scan for Known Spyware on Desktops 9
 - Example 4: Apply Patches to Workstations and Servers 10
 - Example 5: Test New Patches 11
- IMPLEMENT STRONG ACCESS CONTROL MEASURES 12
 - Example 6: Establish Proper Security in Active Directory 12
 - Example 7: Assess Permissions to Resources 14
 - Example 8: Centrally Establish Permissions 15
- ASSIGN UNIQUE IDs TO EACH PERSON WITH COMPUTER ACCESS 16
 - Example 9: Report on Inactive Users 16
 - Example 10: Managing Service Account Passwords 17
 - Example 11: Locking Inactive Users 18
- REGULARLY MONITOR AND TEST NETWORKS..... 19
 - Example 12: Audit File System Use 19
 - Example 13: Auditing Active Directory Usage 21
- REGULARLY TEST SECURITY SYSTEMS AND PROCESSES 23
 - Example 14: Report on Security Settings, Changes and Exceptions 23
- CONCLUSION..... 25

INTRODUCTION

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

ScriptLogic's software solutions help many different types of enterprise comply with the requirements arising from government legislation. The aim of this document is to highlight ways in which ScriptLogic solutions can be used to bring Microsoft Windows-based IT systems into line with the requirements of the Payment Card Industry (PCI) Data Security Standard.

PCI - BACKGROUND

Over the last several years, a number of retailers, banks, service providers and credit card companies have experienced breaches in security resulting in the obtaining of personal and financial data that customers have knowingly or unwittingly entrusted to these firms. Several large, well-known institutions and brands have been boldly exposed in the media and pummeled in the financial markets after major data security breaches within their organization were revealed.

In response, the payment card industry itself developed a security initiative broader in scope and more granular in its requirements than any government-sanctioned regulatory compliance standard might have imposed. The Payment Card Industry Data Security Standard is a comprehensive security standard that establishes common processes and precautions for handling, processing, storing and transmitting credit card data.

In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

SECURITY PRINCIPLES AND REQUIREMENTS

The security principles of the PCI Data Security Standard include a number of requirements that ScriptLogic software solutions help organizations to comply with. The table below highlights some of the security requirements together with examples of typical operations IT administrators would perform in order to enforce those safeguards within a Microsoft Windows network utilizing ScriptLogic solutions:

Control Objective	Requirement	Section	Action Required
Build and Maintain a Secure Network	Install and Maintain a Firewall Configuration to Protect Cardholder Information	1.2	Configure the Windows XP Firewall
	Disable unnecessary services	2.2.2	Manage Windows services
Maintain a Vulnerability Management Program	Protect against malicious software	5.1.1	Actively scan for known spyware on desktops
	Ensure that all system components and software have the latest vendor-supplied security patches	6.1	Patch Windows desktops and servers for both Microsoft and 3 rd -party products
	Testing of all security patches before deployment	6.3.1	“Sandbox” patch deployment on desktops to properly test
Implement Strong Access Control Measures	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	7.1	Search for inappropriate permissions in Active Directory
			Establish security roles to ensure appropriate access is granted via Active Directory
			Collect and Report on security settings, exceptions and trends
			Establish appropriate security settings in file systems, registry, shares, printers, databases and SharePoint sites
	Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.	7.2	Establish new permissions, including Denials, without needing to overwrite existing permissions

(Continued on next page)

Principle	Requirement	Section	Action Required
Assign a unique ID to each person with computer access	Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.5.1	Establish proper delegation within Active Directory Audit Active Directory activity
	Remove inactive user accounts at least every 90 days	8.5.5	Report on inactive users
	Change user passwords at least every 90 days	8.5.9	Centrally modify passwords on Windows service accounts
	Lock workstation after 15 minutes of inactivity	8.5.15	Establish inactivity settings to lock workstation
Regularly Monitor and Test Networks	Implement automated audit trails to reconstruct individual user accesses to cardholder data	10.2.1	Audit file system access on Windows servers
	Implement automated audit trails to reconstruct all actions taken by an individual with administrative privileges	10.2.2	Audit actions taken in Active Directory
Regularly test security systems and processes	Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.	11.1	Report on security settings, changes, and exceptions
	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	11.5	Audit file system access on Windows servers

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 PCI's Data Security Standard. It is important to note that data to be protected may exist within Windows file systems, databases and even on SharePoint sites (as is appropriate to your environment) and these systems need to be addressed to ensure compliance.

In order to bring an organization into compliance, there are a number of software solutions that need to be considered. No single software product can make a company compliant, but software tools play an essential role in helping 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 PCI DSS 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, SQL Servers and SharePoint servers. It also manages service and task security and settings.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.
Desktop Authority	Comprehensive desktop management platform that 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 cardholder data, easily maintain those controls, and then report on their effectiveness, thus fulfilling key requirements of PCI compliance.

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

PCI standards first mandate that “all systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees’ Internet-based access through desktop browsers, or employees’ e-mail access.” This covers a number of actions to be taken by IT; in essence, every one of your desktops and servers, as well as your Active Directory all needs to be considered within the context of this mandate.

Example 1: Configure the Windows XP Firewall

Requirement: **Install and Maintain a Firewall Configuration**

ScriptLogic Solution: **Desktop Authority**

While corporate firewalls are the initial topic of discussion by this requirement, securing the firewall built into Windows XP and Windows Vista will further enhance the intended protection desired by this requirement.

Desktop Authority can centrally configure the Windows Firewall settings, enabling IT to quickly and easily establish the desired security settings, as shown in Figure 1.

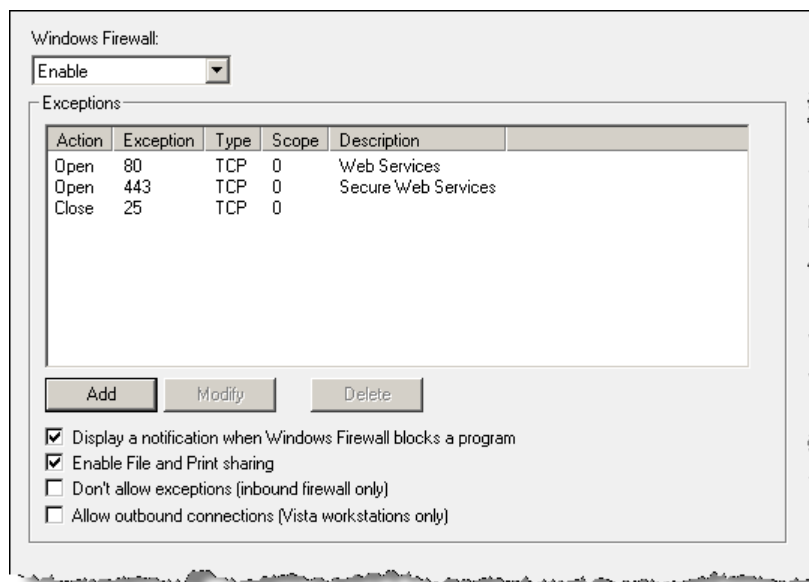


Figure 1: Centrally configure the Windows Firewall on your workstations

Example 2: Managing Services

Requirement: **Disable Unnecessary Services**

ScriptLogic Solution: **Security Explorer**

Services on Windows desktops and servers may provide access through currently unknown breaches in security. Disabling unnecessary services will help to limit the potential exposure those services may possess.

Security Explorer, in addition to centrally managing NTFS, Share, Registry and Printer permissions, manages Windows services. Figure 2 shows how a simple query of services based on criteria such as the service account name, the service name, startup type and more will result in a list of services that can be managed. With Security Explorer, the resultant set of services can be simultaneously managed, also shown in Figure 2, such as disabling the selected services.

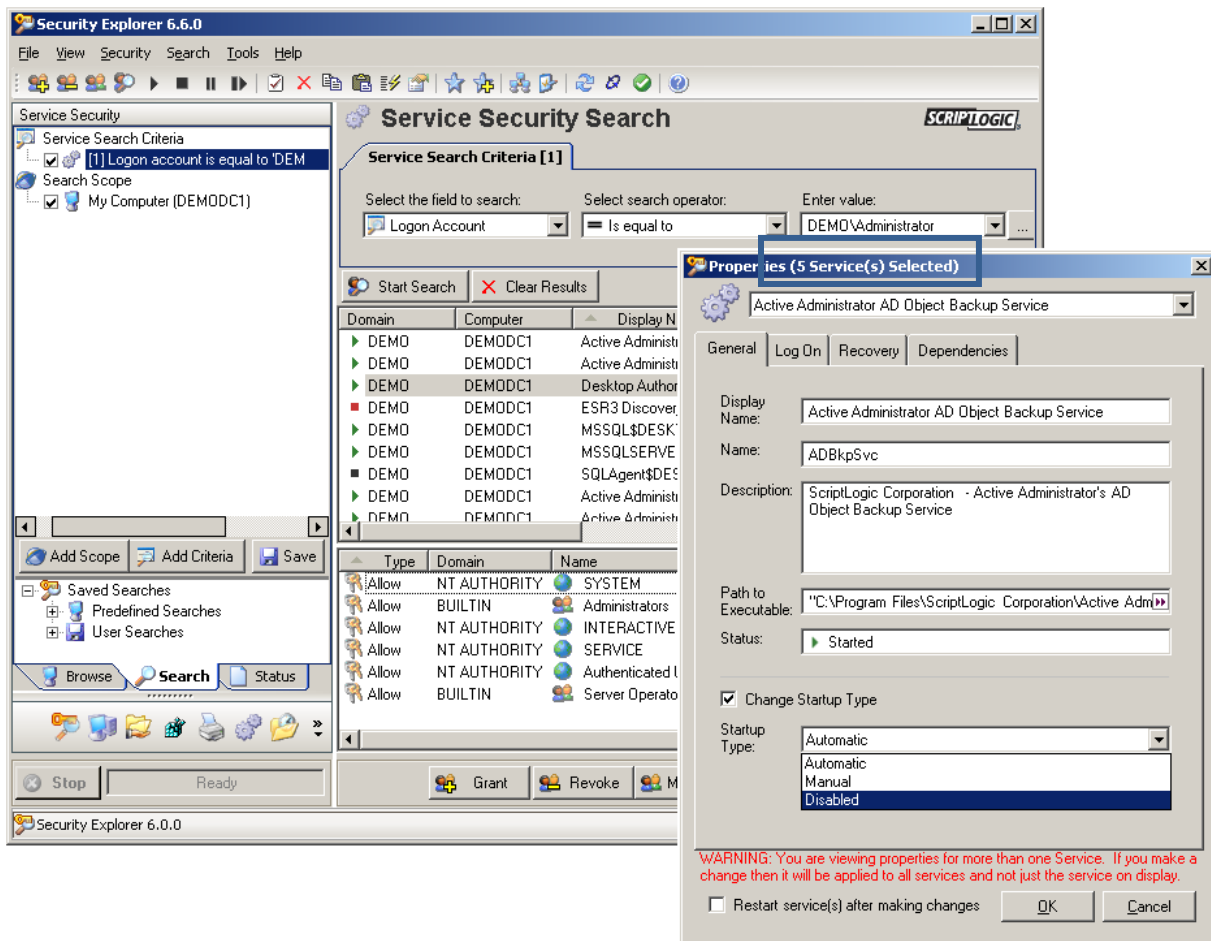


Figure 2: Services are queried using the Search field based on several Service-specific criteria and the results can be modified at once to modify service startup types or other properties

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

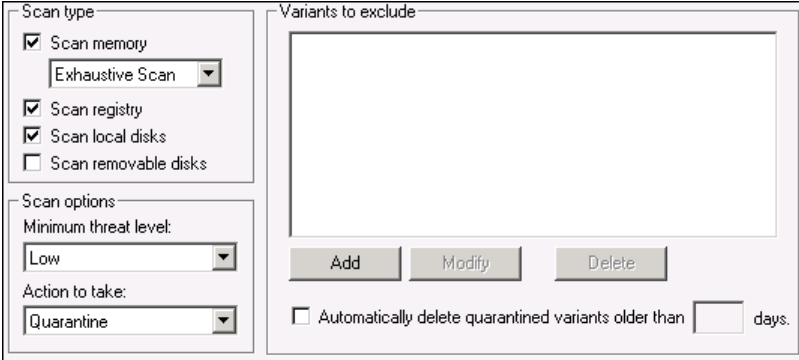
After the strong foundation of the network is established, constantly protecting it against vulnerabilities is a priority to maintain security for cardholder data.

Example 3: Scan for Known Spyware on Desktops

Requirement: **Protect Against 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 3 shows the configuration options available and Figure 4 shows DA's Spyware reporting capabilities.



The screenshot displays the configuration interface for Desktop Authority's Anti-Spyware option. It is divided into two main sections: 'Scan type' and 'Scan options' on the left, and 'Variants to exclude' on the right.

- Scan type:** Includes checkboxes for 'Scan memory' (checked), 'Scan registry' (checked), 'Scan local disks' (checked), and 'Scan removable disks' (unchecked). A dropdown menu is set to 'Exhaustive Scan'.
- Scan options:** Includes a 'Minimum threat level' dropdown set to 'Low' and an 'Action to take' dropdown set to 'Quarantine'.
- Variants to exclude:** A large empty text area for listing variants, with 'Add', 'Modify', and 'Delete' buttons below it.
- Automatic deletion:** A checkbox for 'Automatically delete quarantined variants older than' followed by an empty input field and the word 'days'.

Figure 3: Desktop Authority's powerful Anti-Spyware option is comprised of flexible options mixed with multiple configurations using Validation Logic

SCRIPTLOGIC **DESKTOP AUTHORITY**

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 responsible 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.2K3DDOMAIN\DESKTOP\ISAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM
DESKTOP1	CONSCORR.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP\SPYWA RE\ISAMPLE 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.2K3DDOMAIN\DESKTOP\ISAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM
DESKTOP1	180AX.EXE	C:\DOCUMENTS AND SETTINGS\TESTER\DESKTOP\SPYWA RE\ISAMPLE SPYWARE\	REMOVE	SUCCESS	9/21/2005 3:24 PM

Figure 4: Centralized reporting ensures IT is aware of the Spyware outbreaks and their removal

Example 4: Apply Patches to Workstations and Servers

Requirement: **Ensure the Latest Vendor-Supplied Patches Have Been Applied**

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 as little as 0 days! In order to ensure machines accessing cardholder data 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 5, patches desktop machines based on product and patch severity utilizing DA's exclusive Validation Logic to establish patch deployment granularity for testing or general availability of a patch.

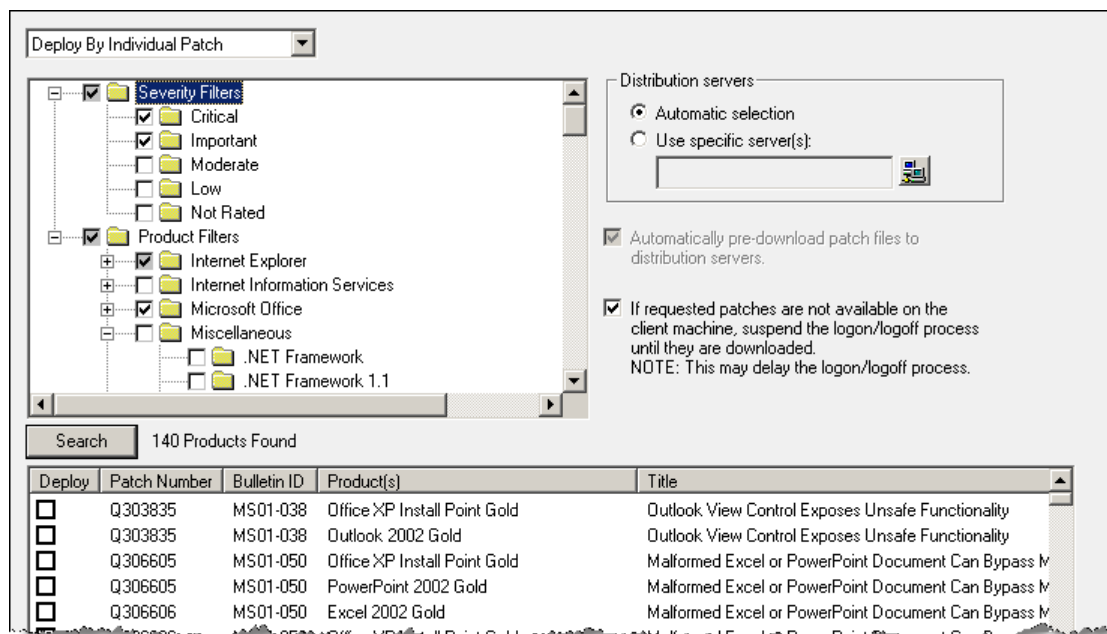


Figure 5: Patching both Microsoft and 3rd-party solutions is a critical step to managing your risk

If you prefer a solution that patches both desktops and servers, ScriptLogic's 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: Test New Patches

Safeguard: **Testing all Patches Before Deployment**

ScriptLogic Solution: **Desktop Authority**

Before a patch is deployed to the entire organization, it should first be tested to ensure it will not cause a disruption of service (namely the user's workstation). Desktop Authority's patented Validation Logic allows the deployment of patches (as well as any configuration element within Desktop Authority) to be limited in scope, facilitating a pilot test of the deployment.

Figure 6 shows a simple example of limiting patches based on group membership, but Validation Logic extends to class of machine, OS, connection type, computer/user name, Active Directory Sites/OUs, IP addressing, Thin Client settings, and more. Once a patch is determined to be safe for general use, the Validation Logic can be broadened to include a larger user base, up to the entire organization.

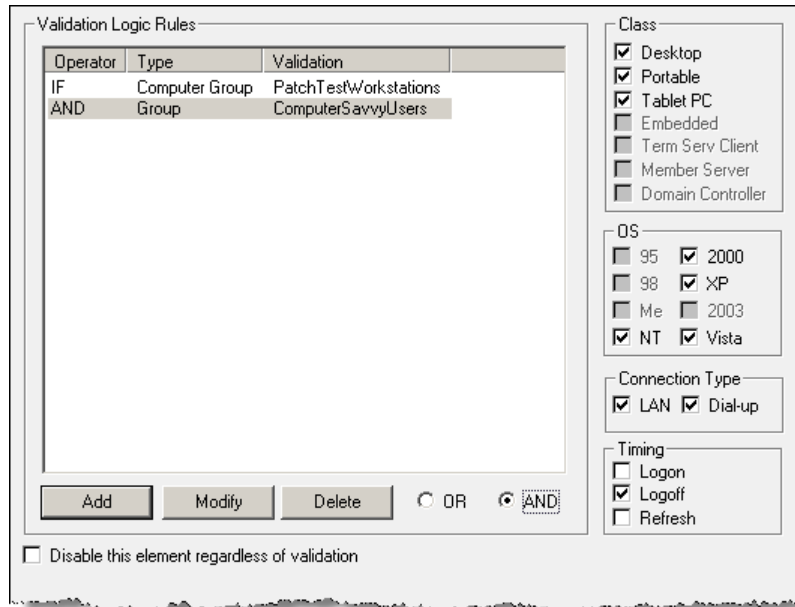


Figure 6: Patches can be deployed to a limited test group of machines and users based on over 40 criteria.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Once the network is protected from outside influences, the next step is to ensure users within the organization only have proper access to resources. This starts with Active Directory and finds its way down to the files and folders potentially containing cardholder data.

Example 6: Establish Proper Security in Active Directory

Requirements: **Limit Access to Resources and Cardholder Information, Control the addition, deletion, and modification of user IDs**

ScriptLogic Solution: **Active Administrator**

At the heart of almost all Windows-based networks, Active Directory manages the security and privileges assigned to employees within an organization. ScriptLogic's Active Administrator offers a range of functions that enable effective management of these privileges. Two functions covered in this paper are reactively searching for over-privileged users in Active Directory (who can potentially grant inappropriate access to cardholder resources via group membership) and, more importantly, proactively establishing consistent permissions to ensure this never happens.

Active Administrator provides the ability to search for and generate reports on permission settings, as shown in Figure 7. 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

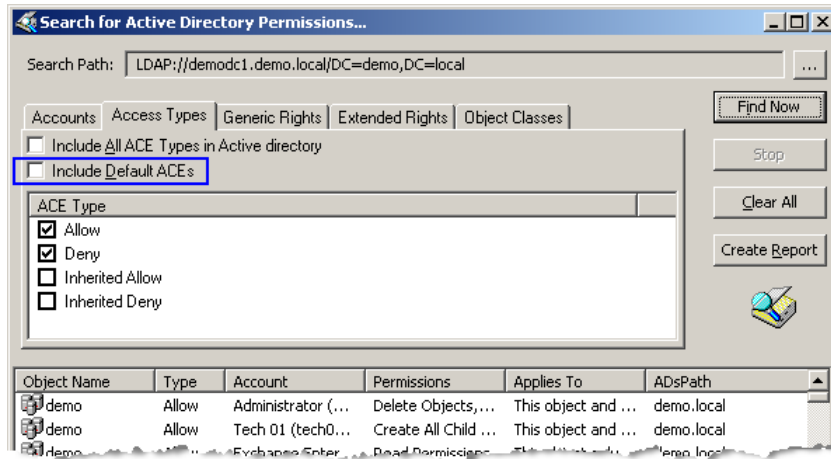


Figure 7: Optionally hide default permissions supplied in the AD Schema, making it easier to see added permissions.

The root of all access to cardholder resources lies within Active Directory: access to cardholder 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 8. 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 PCI requirements.

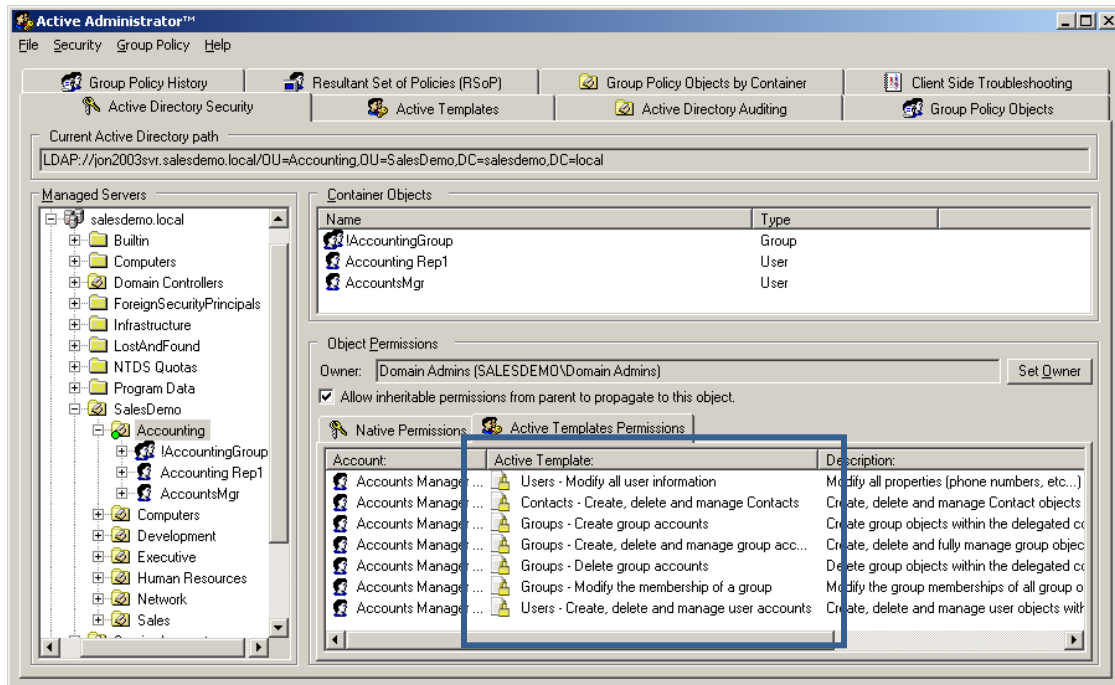


Figure 8: Each Active Template grants or revokes permissions consistently, simplifying delegation

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.

The delegation of permissions not only assist in compliance with Requirement 7 (limiting access to resources), but also Requirement 8.5.1 (controlling user IDs, credentials, etc).

Example 7: Assess Permissions to Resources

Requirement: **Limit Access to Resources and Cardholder Information**

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

Enterprise Security Reporter scans a network of Windows servers, Windows workstations and SharePoint sites and analyzes the results using over 160 customizable, turn-key security reports. These reports are vital tools to help with the assessment of permissions needed to properly limit access. These reports also provide a formatted analysis of the security controls in place if needed during a review of PCI compliance by third parties.

As an example, the analysis of file permissions can be done using the “Delta Permissions Reporting” function, which only shows file and folder permissions which differ from the parent folder to make it easier to identify all permissions which have been “added” to the inherited NTFS permissions, as shown in Figure 9. The result is that this report is an essential report for tracking down over-exposed files and folders, which might reveal a breach of intended 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 9: 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 10, highlights the permissions assigned to users and groups to give them access to SharePoint resources that may contain PCI-related data.

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

Figure 10: Quickly identify access to SharePoint resources

Example 8: Centrally Establish Permissions

Requirement: **Limit Access to Resources and Cardholder Information**

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

Cardholder information can reside on Windows file systems, inside SQL Server databases and on SharePoint sites. While these servers can be secured in a one-off fashion, the consistency desired by Requirement 7 can only be accomplished by using a solution that will both centrally establish permissions and be able to replicate the permissions across multiple servers, file systems, databases and SharePoint sites.

As shown in Figure 11, Security Explorer can not only search for and manage permissions, but permissions can be cloned to maintain consistency. This allows IT to easily establish both grants and denials of permissions not just centrally, but consistently across all your servers.

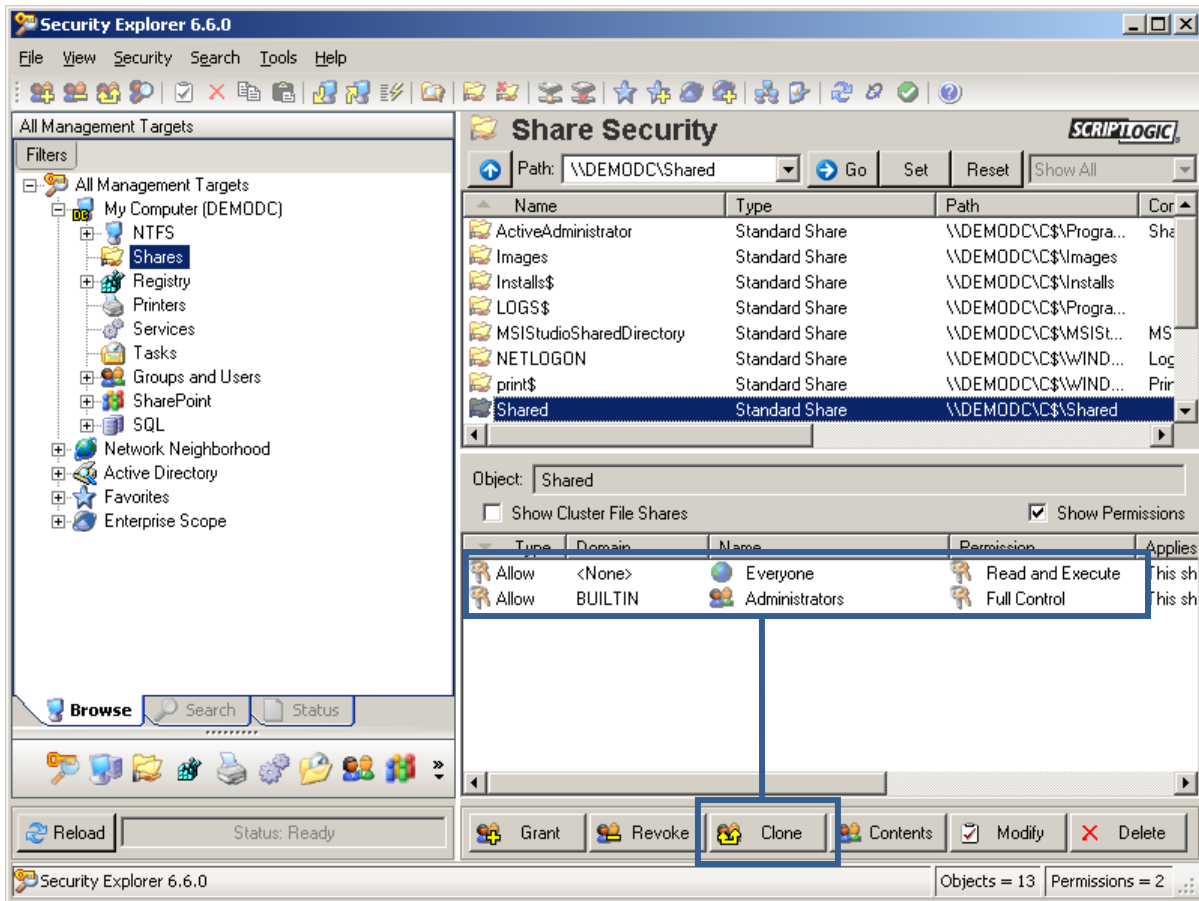


Figure 11: Centralized Assignment and Cloning of permissions with Security Explorer

ASSIGN UNIQUE IDs TO EACH PERSON WITH COMPUTER ACCESS

This requirement is key to ensuring that only appropriate users access cardholder data and that audit trails of activity are accurate.

Example 9: Report on Inactive Users

Requirement: **Remove inactive user accounts at least every 90 days**

ScriptLogic Solution: **Enterprise Security Reporter**

Removing inactive users keeps overlooked accounts from creeping back onto the network and potentially accessing cardholder data. This is a simple matter of reporting on last logon date. Enterprise Security Reporter, among its other 160+ turnkey reports, can quickly determine which users have not logged on within the 90 days (or shorter durations if specified) in order to take action on those accounts, as shown in Figure 12.

No Logon Report				5/17/2007 2:24:13 PM	
Account	Last Logon Date	# of Logons	Disabled? Locked?		
<i>Selected Domain(s):</i> demo.local <i>Selected Date Range:</i> Not In The Past 90 Days					
demo.local			Discovery Date:	3/8/2007 3:44:59 PM	
Bob Smith (bsmith@demo.local)	2/15/2007 2:25:18 PM	496	<input type="checkbox"/>	<input type="checkbox"/>	
Jim Jones (jjones@demo.local)	2/6/2007 5:47:08 PM	9	<input type="checkbox"/>	<input type="checkbox"/>	
Ryan Allan (rallan@demo.local)	2/6/2007 5:47:12 PM	15	<input type="checkbox"/>	<input type="checkbox"/>	

Figure 12: Quickly report on users who have not logged on within 90 days

Example 10: Managing Service Account Passwords

Requirement: **Change user passwords at least every 90 days**

ScriptLogic Solution: **Security Explorer**

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

As previously mentioned in this whitepaper, Security Explorer manages Services and the accounts using them. With Security Explorer, a simple query of services using a particular service account or containing a part of a service name (such as “SQL”) will result in a list of services that can be simultaneously managed, as shown in Figure 13, where the service account passwords can be changed.

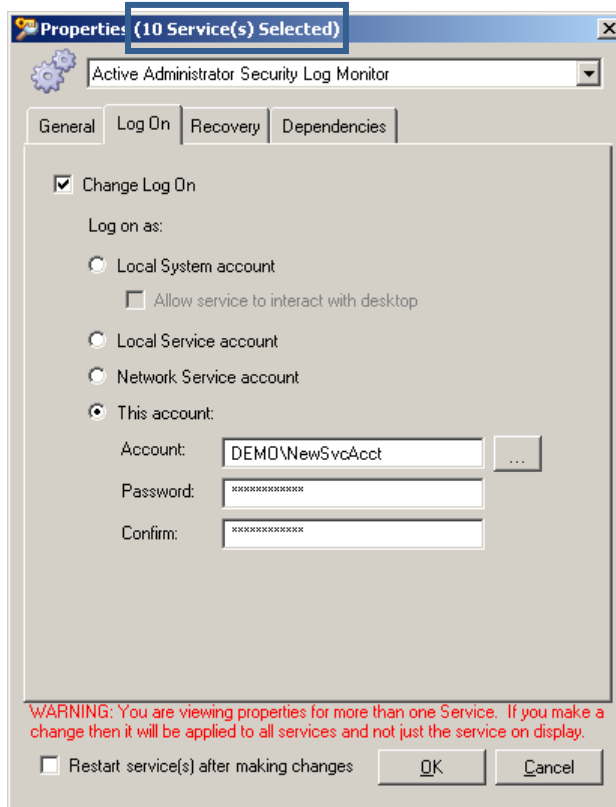


Figure 13: Multiple Services can be modified at once to modify service account passwords or other properties

Example 11: Locking Inactive Users

Requirement: **Lock workstation after 15 minutes of inactivity**

ScriptLogic Solution: **Desktop Authority**

Automatic locking of a user is required to ensure the protection of cardholder data 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 lockout, logoff or even shutdown after a specified period of inactivity, as shown in Figure 14. This works on all PCs running Windows 95, 98, Me, NT4, XP, 2000, 2003 or Vista.

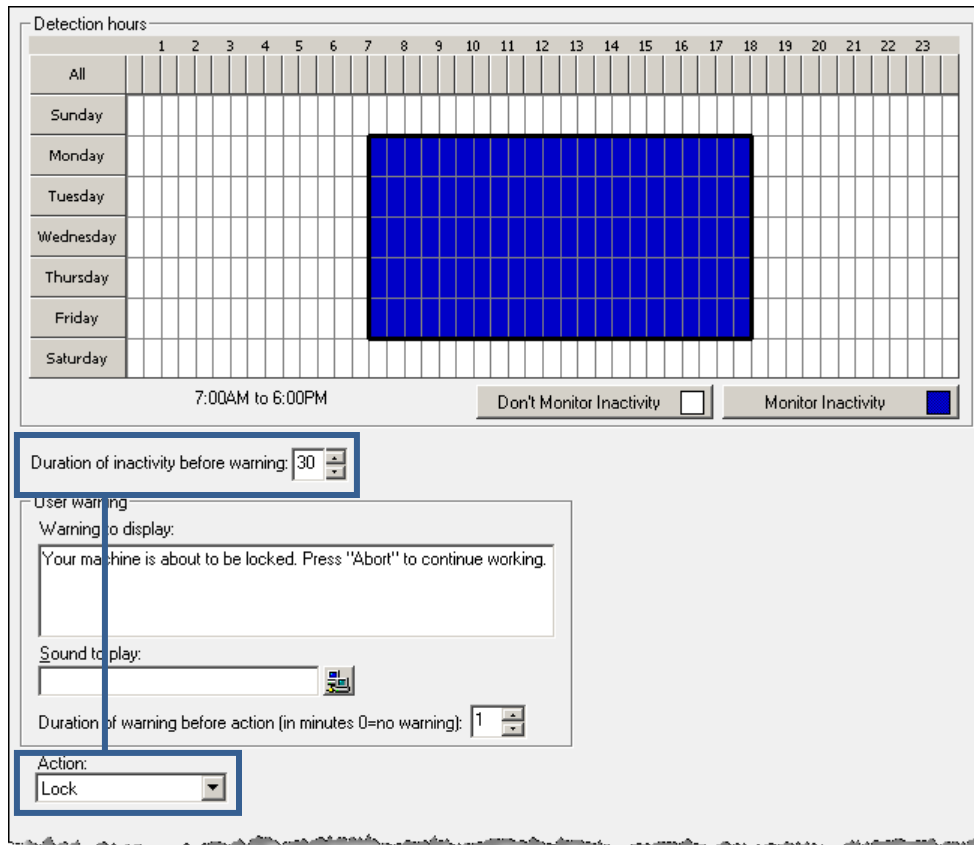


Figure 14: After a specified period of inactivity, users can be locked, logged off, shutdown or rebooted, as desired.

REGULARLY MONITOR AND TEST NETWORKS

It's not enough to simply setup what is believed to be a secure network; the security must be consistently tested to ensure its intended level of control is being maintained. This is primarily accomplished through audits of access to sensitive data systems which can include both Windows servers and Active Directory.

Example 12: Audit File System Use

Requirement: **Implement Audit Trails of access to cardholder data**

Deploy file integrity monitoring software

ScriptLogic Solution: **File System Auditor**

Since cardholder information can find its way into formal letters, accounting spreadsheets, etc, it is vital to proactively have in place a solution that will detect, and notify IT of access (and denied access) to protected information. File System Auditor monitors all file system activity on Windows servers and centrally secures the logged activity information into a secure SQL Server-based audit trail.

Activity can be reported on (as well as scheduled to be emailed when it occurs) using very simple to use criteria, shown in Figure 15.

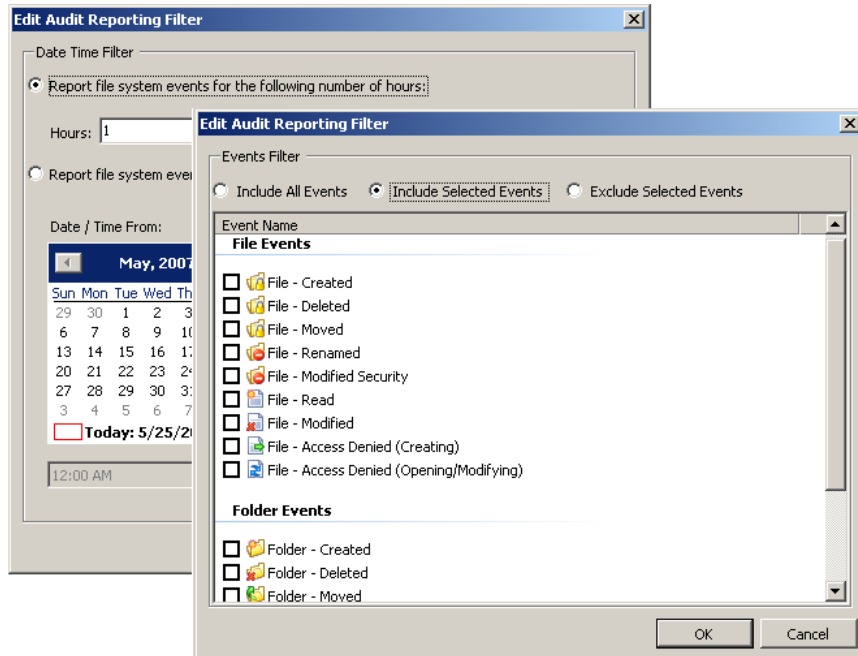


Figure 15: Selection of auditing criteria is a simple process.

Criteria is based on six elements, each graphically represented to promote a fast and simple method of retrieving audit results, as shown in Figure 16.

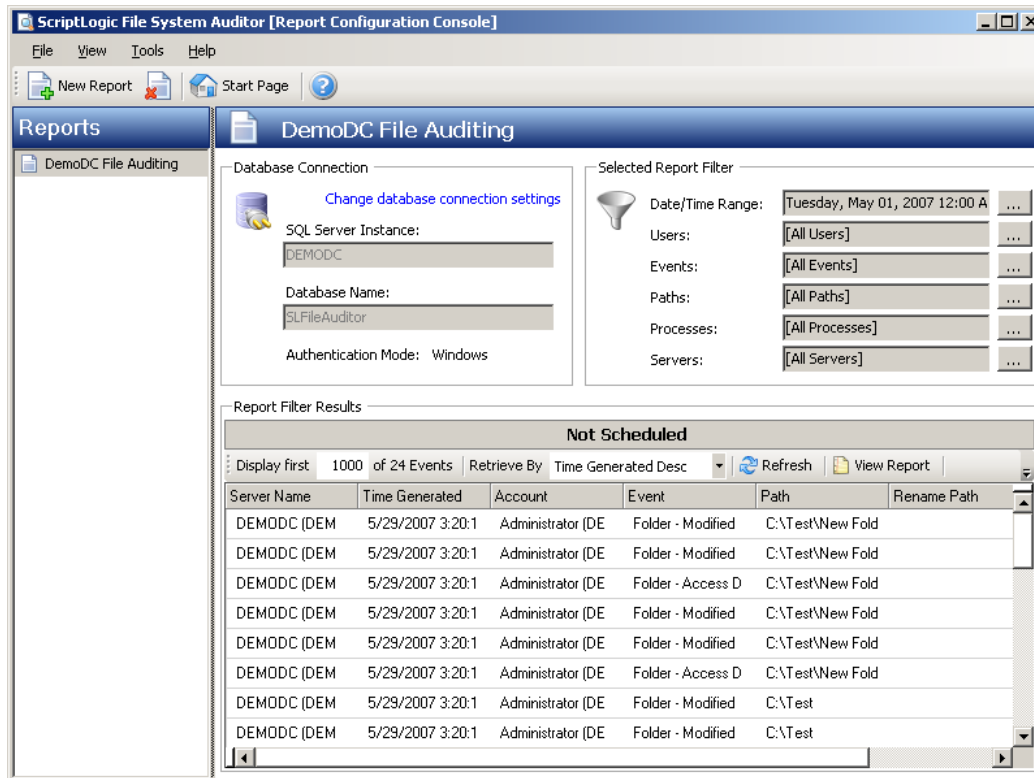


Figure 16: File system activity is centrally audited providing a trail for compliance use

The auditing of file system activity not only assist with meeting the needs of Requirement 10, but also meets Requirement 11.5's need to alert IT to unauthorized modification of critical files.

Example 13: Auditing Active Directory Usage

Requirement: **Implement audit trails of actions by individuals with administrative privileges**

ScriptLogic Solution: **Active Administrator**

A review of security changes in an organization's IT systems, as well as the ability to audit and analyze security settings for potential risks is required by the PCI standard, which includes 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 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 17. It also allows for long term storage of audit logs without the need for enormous event logs on individual servers.

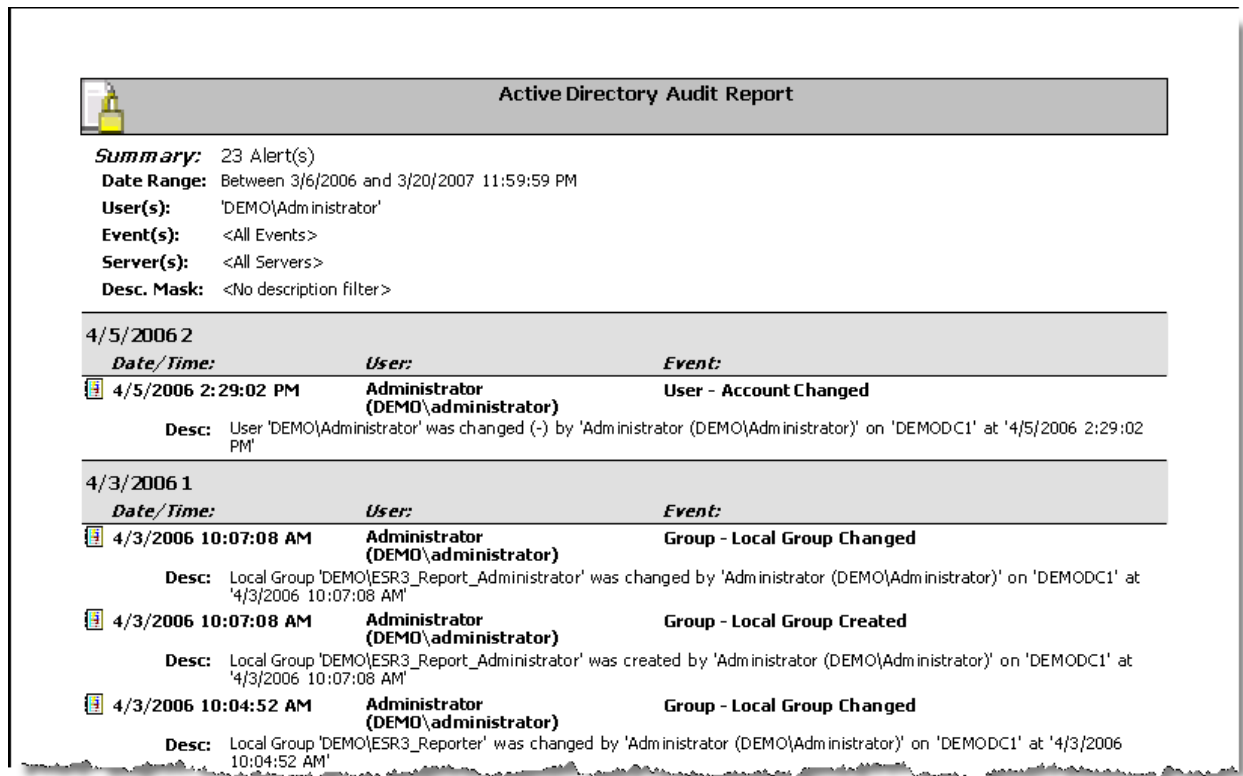
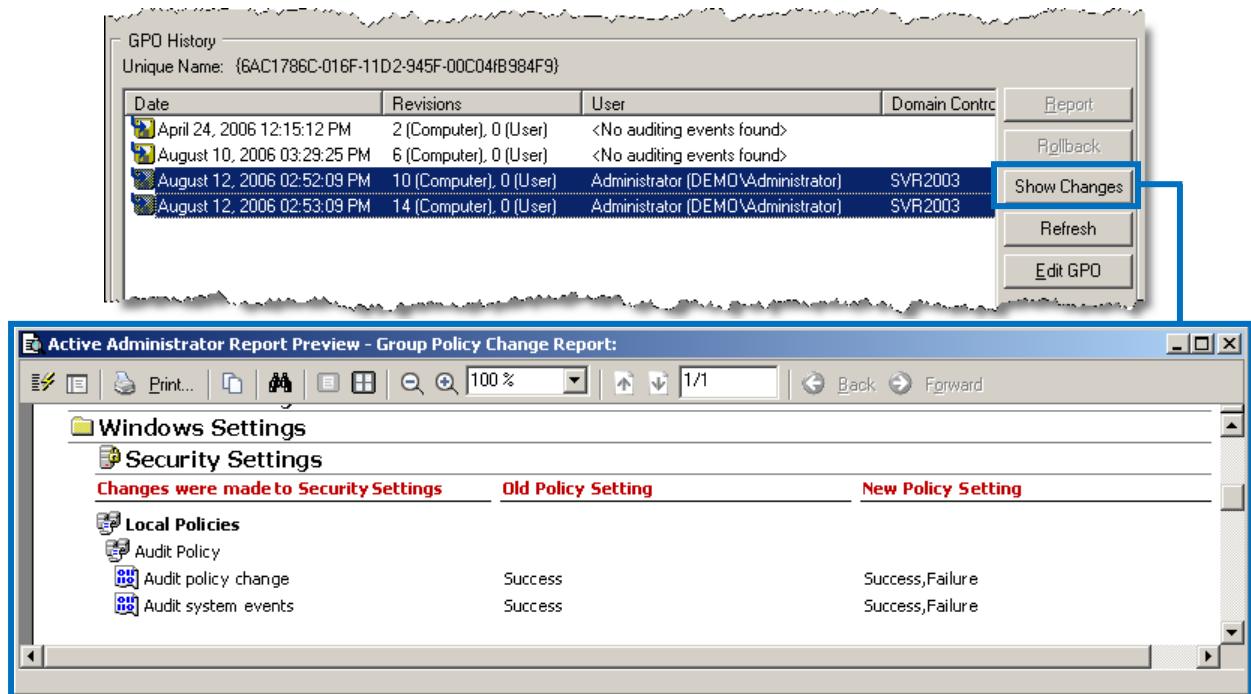


Figure 17: Active Administrator provides centralized reporting on all Active Directory activity

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 18.



REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

This requirement is important because it introduces the concept that new vulnerabilities can be introduced. While usually this concept conjurs up thoughts of hackers and viruses, it should be considered that a new vulnerability can be as simple as someone new to the organization has left their password on a post-it note on their monitor. Testing the security regularly ensures there are no “surprises.”

Example 14: Report on Security Settings, Changes and Exceptions

Requirement: **Test security controls and limitations**

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

Testing the controls in place can require countless hours of data collection, sorting through the data and determining the state of security. Enterprise Security Reporter automates this task and turns days into literally minutes. Its agentless discovery engine will collect security-related data sets from Windows servers, Active Directory and SharePoint and provides over 160 turnkey reports, shown in Figure 19, to verify and validate the state of security.

Special reports, such as the Snapshot Comparison reports show the changes in security to identify any irregularities in administration that may leave cardholder data exposed.

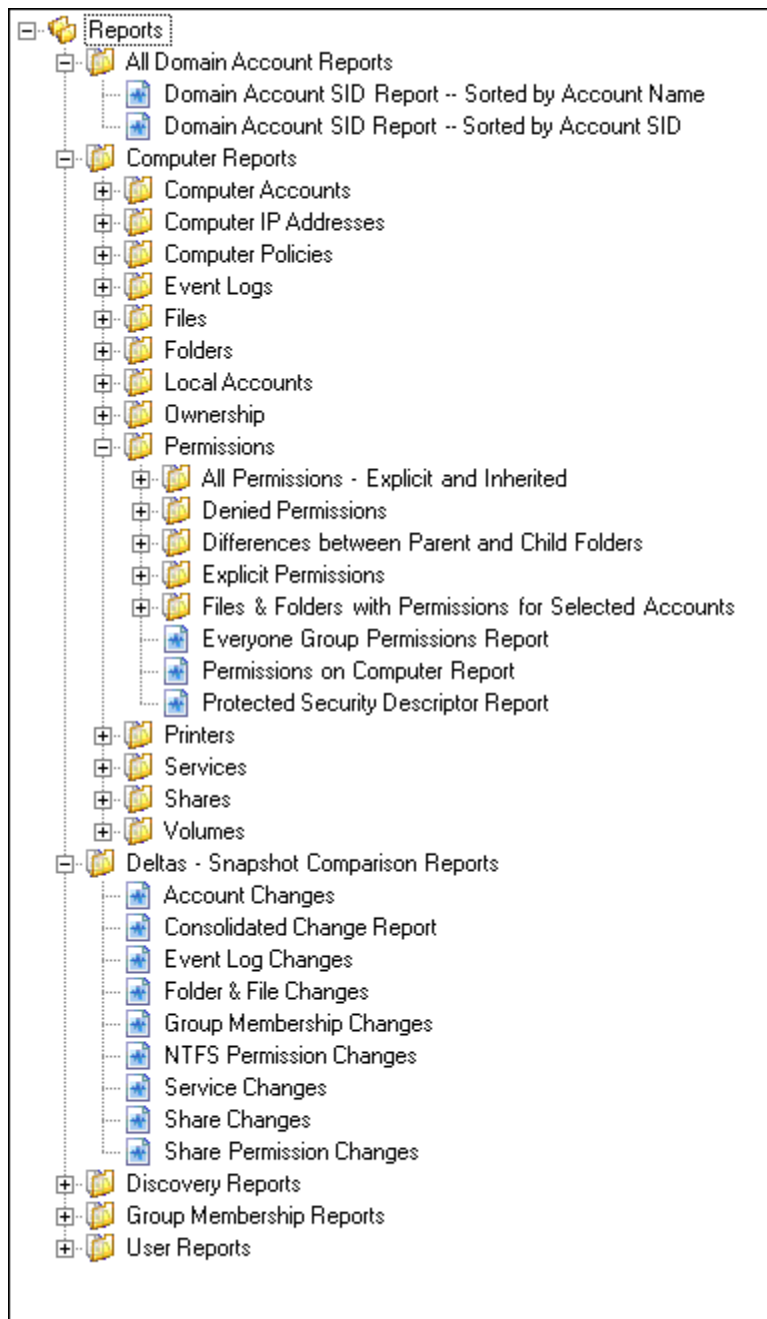


Figure 19: Enterprise Security Reporter has over 160 turnkey reports to test the state of security

CONCLUSION

The PCI Data Security Standard requires considerable effort by organizations 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 cardholder data across their enterprise.

The requirements of the Data Security Standard 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 PCI requirements requires extensive reporting and investigative capabilities.

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

ScriptLogic solutions that assist with PCI DSS 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, SQL Servers and SharePoint servers. It also manages service and task security and settings.
File System Auditor	Centrally audits, reports and alerts on Windows file system activities.
Desktop Authority	Comprehensive desktop management platform that 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 PCI compliance please visit www.scriptlogic.com/pci, or contact your ScriptLogic sales representative or Authorized ScriptLogic Channel Partner.