



Implementing ITIL Best Practices with ScriptLogic

A ScriptLogic Product Positioning Paper

By Nick Cavalancia

Table of Contents

INTRODUCTION	3
ITIL - BACKGROUND	3
ITIL – BUSINESS PROCESSES AND OBJECTIVES.....	4
SOLUTIONS SUMMARY	6
SOLUTION EXAMPLES	7
Example 1: Designing and Building Group Policies	7
Example 2: Designing and Building a Standard Client Configuration	8
Example 3: Test File Server Migrations.....	9
Example 4: Report and History of Group Policy Changes	10
Example 5: Document Server Security Settings	12
Example 6: Using Active Templates to Delegate Permissions	13
Example 7: Troubleshoot GPO Configuration Failures	14
Example 8: Auditing the Management of Active Directory	15
Example 9: Manage Support Issues	16
Example 10: Remotely Managing Clients	17
Example 11: Backing up and Restoring Group Policies.....	18
Example 12: Backing up and Restoring Active Directory Security	19
Example 13: Backing Up and Restoring Active Directory.....	20
Example 14: Backing up and Restoring Windows, SharePoint and SQL Server Security.....	21
Conclusion.....	23

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 arising from government legislation and industry best-practices. The aim of this document is to highlight ways in which ScriptLogic solutions can be used to implement ITIL best practices in Windows-based networks. Additional information about ScriptLogic solutions and ITIL can be found at <http://www.scriptlogic.com/itil>.

ITIL - BACKGROUND

ITIL (IT Infrastructure Library) is the most widely accepted approach to IT service management in the world. Since its introduction in 1980, ITIL has evolved to provide a complete set of best practices, drawn from international public and private sectors. It is supported by a comprehensive qualification scheme, accredited training organizations, and implementation and assessment tools. ITIL guidance allows both large and small companies to exploit recognized best practices across the IT organization, thereby helping align IT with business objectives and drive IT operational improvements.

Organizations worldwide are adopting ITIL, making it the de-facto standard for IT professionals in a broad range of organizations such as local and central government, energy, public utilities, retail, finance and manufacturing. In May of 2007, ITIL underwent an update to its third version. Adoption of ITIL recommendations enables these kinds of organizations to achieve five key objectives:

- Improve customer satisfaction with services provided by IT
- Increase service availability
- Realize monetary savings from improvements in efficiency and reduction in resources and lost time
- Reduce service "time to market"
- Improve risk optimization and decision making

ITIL – BUSINESS PROCESSES AND OBJECTIVES

While ITIL describes which best practices to pursue, it does not define how to implement detailed processes and work-level procedures that enable those recommendations. ITIL provides high-level guidance on what should be done, but allows each business develop and implement work-level procedures to match their unique requirements. Successful implementation of ITIL best practices requires software-based tools to effectively deploy procedure-level processes to IT staff.

ScriptLogic solutions aid in the implementation of the processes set forth within a number of ITIL disciplines. The following table lists some of the ITIL processes and examples of typical operations IT administrators would perform to implement those processes.

ITIL Discipline	ITIL Process	Objective	Action Required
Service Support	Release Management	To ensure that all technical aspects of a release are dealt with in a coordinated approach.	Plan, design, build, configure and test Group Policies prior to implementation. Plan, design, build, configure and test client machine configurations prior to implementation. Test migration to new file servers to ensure seamless changeover.
	Change Management	To ensure that standardized methods and procedures are used for efficient and prompt handling of all changes.	Report, audit and alert on all Active Directory and Group Policy management changes.
	Configuration Management	To account for all the IT assets and configurations within the organization and its services; to provide accurate information on configurations and their documentation to support all the other Service Management processes; to verify the configuration records against the infrastructure and correct any exceptions	Document all users, groups, group memberships, files, folders, shares, services and local policies. Establishing roles and responsibilities within Active Directory with the ability to control, audit and verify both the roles themselves as well as the use of those roles within Active Directory.

(Continued on the next page)

ITIL Discipline	ITIL Process	Objective	Action Required
Service Support	Incident Management	To restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.	Troubleshoot GPO configuration failures. Rollback and undo AD and GPO changes. Analysis and reporting of events and configuration changes. Alerting on selected events.
	Problem Management	To minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure, and to prevent recurrence of Incidents related to these errors.	Diagnose, investigate and identify problems on client machines, in Active Directory, Group Policies, file security, printer security, and more.
Service Delivery	Availability Management	To optimize the capability of the IT Infrastructure, services and supporting organization to deliver a cost effective and sustained level of Availability that enables the business to satisfy its business objectives	Maximize Active Directory availability by being able to backup <u>and restore</u> Group Policies and AD in real time, without taking services offline. Maximize data availability by being able to backup <u>and restore</u> NTFS permissions rapidly.
Security Management	Security Management	To ensure such a level of security, that the agreed availability of the infrastructure & the IT services, as well as the business functions, is not compromised.	Define security roles within Active Directory and perform audits of Active Directory management.

Table 1: Meeting ITIL process requirements with ScriptLogic

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 ITIL standards.

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 implementing ITIL best practices	
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
BridgeTrak	Help desk solution that centrally manages user issues, from ticket tracking, to escalation to resolution.
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.
Desktop Authority	Comprehensive desktop management platform that provides centralized configuration, inventory, support and security of Windows-based clients.
Secure Copy	Data migration solution that additionally moves all supporting security-related data sets to ensure a secure duplicate of the original data.
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.

The remainder of this paper provides examples of how ScriptLogic products enable administrators to perform the necessary actions to implement ITIL best practices.

Example 1: Designing and Building Group Policies

Related Process: **Release Management**

ScriptLogic Solution: **Active Administrator**

Before a change is ever made in a live environment, a well-implemented Release Management process for Group Policies ensures that configurations affecting tens, hundreds or thousands of users are properly planned and tested. This helps meet the requirements of ITIL’s Availability Management process, ensuring that clients do not receive overly restrictive desktop configurations, and retain access to all appropriate aspects of their OS environment.

Active Administrator facilitates all the actions required to achieve Release Management objectives in the area of Group Policies. The actions ITIL recommends prior to releasing a technical solution such as a Group Policy include: Planning, Designing, Building, Configuring, and Testing

Active Administrator is a comprehensive management application that provides enormous visibility and control over Group Policy Objects (GPOs) to help administrators manage the GPO lifecycle. Figure 1 shows one of Active Administrator’s Group Policy management displays, which gives administrators a complete range of information about a policy from when it was created, to whom it applies to and where it is linked within Active Directory.

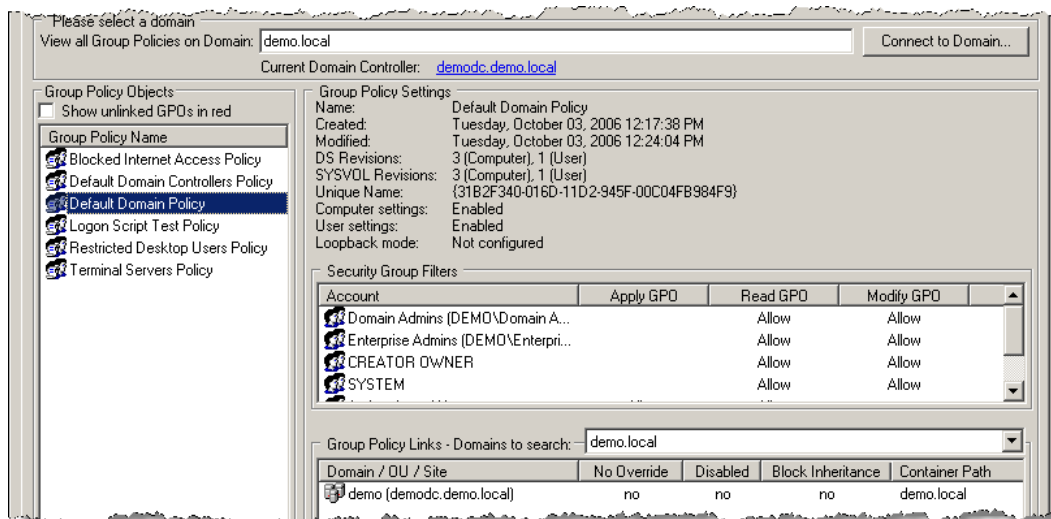


Figure 1: Active Administrator simplifies Group Policy Management with an easy-to-use interface

Active Administrator additionally provides an Offline GPO Repository to be used for making changes to and testing Group Policies without affecting the production environment, as well as an enhanced “Resultant Set of Policies” tool, shown in Figure 2, that analyzes the effect of combined Group Policies on an individual user or computer. Active Administrator goes beyond other RSoP tools with the ability to run what-if scenarios against either live Group Policies or their offline counterparts,

empowering administrations to see the individual effect of each policy on the Resultant Set. And it can do all this for both Windows 2000 and 2003, and report on GPOs and RSoP in a range of formats.

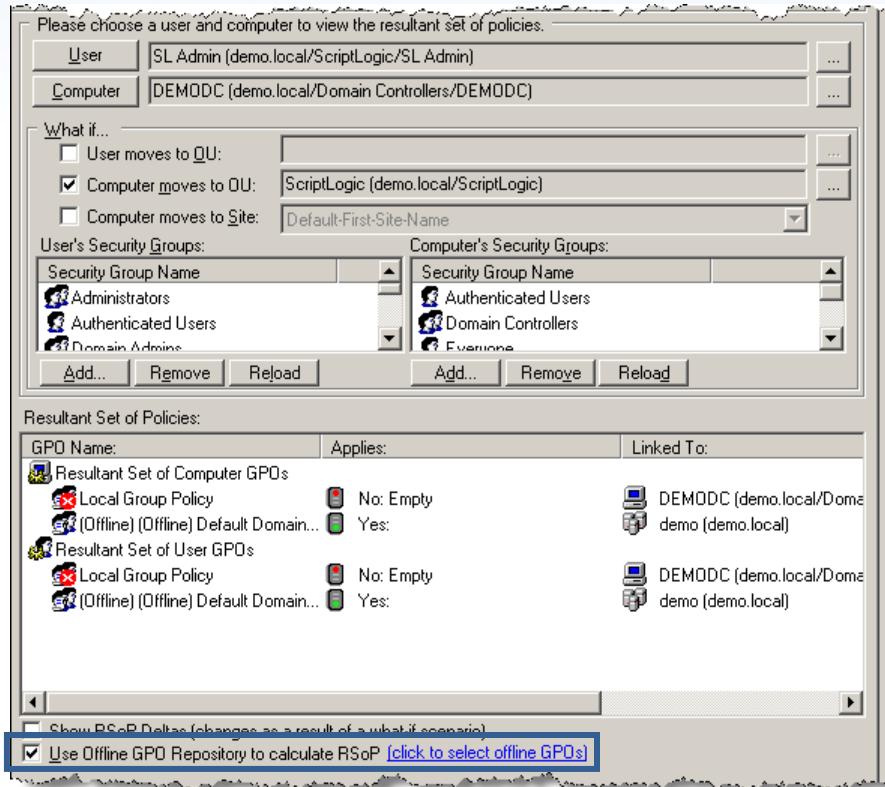


Figure 2: Active Administrator's Offline Repository combined with its RSoP functionality

Example 2: Designing and Building a Standard Client Configuration

Related Processes: **Release Management**

ScriptLogic Solution: **Desktop Authority**

Using Desktop Authority, administrators can design a client's working environment from something as simple as a drive mapping or printer to as advanced as installing multiple patches or removing Spyware. Building and testing this configuration follows the same five actions as in the previous example and, like GPOs, has equal potential to make or break a client's working environment.

Two specific features within Desktop Authority allow it to be used in the Release Management process: Validation Logic and Profiles. Validation Logic is used to determine who will get a particular configuration such as a drive mapping or the latest version of Microsoft Office. By using the 40+ validation types, along with Boolean logic to make selections exponentially more granular, administrators can narrow the scope of selection down to a pilot environment or even a single test user, easily implementing the Release Management process without impacting the general user population.

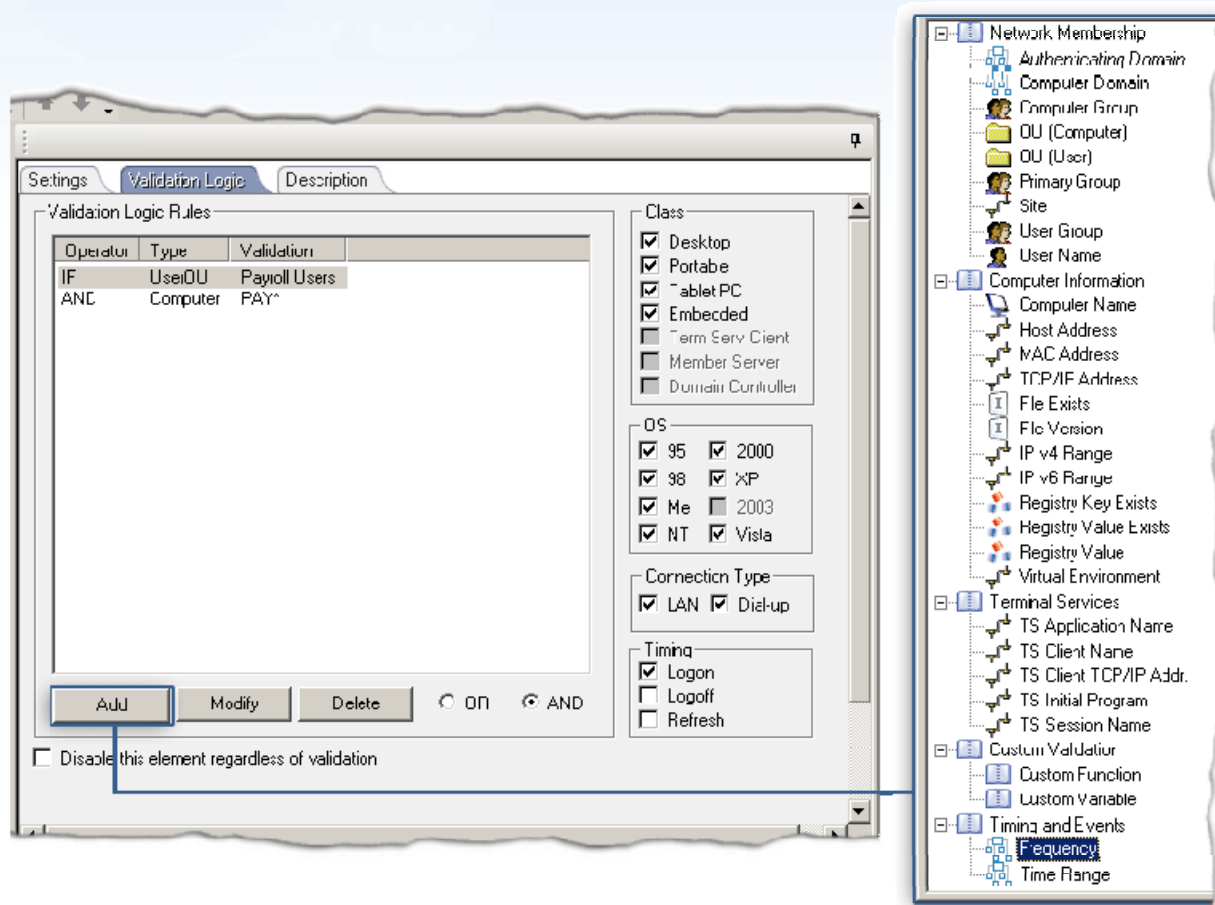


Figure 3: Administrators can restrict the impact of configuration testing by using Desktop Authority’s powerful Validation Logic

Desktop Authority groups configurations into Profiles. When testing a new configuration, a separate profile from those used in production can be created to contain the test configurations. Once the change is scheduled for release, the configuration elements can be copied to a production profile.

Example 3: Test File Server Migrations

Related Processes: [Release Management](#)

ScriptLogic Solution: [Secure Copy](#)

One of the challenges during data migrations is ensuring all data and supporting security has been migrated prior to decommissioning the source server. This challenge is increased with the need to establish a “point in time” migration where data is completely up to date on the target server, allowing administrators to shut down the source server. Because Release Management is focused on proactively testing prior to the release of a new implementation, the traditional method of migration (where a blackout window is established for the migration and services are unavailable) is not acceptable.

Secure Copy facilitates the migration of file, folders, NTFS security, associated shares and share security, compression settings, and local groups given permissions to the data being migrated, creating a comprehensive, complete migrated data set. To rectify the “point in time” issue and to comply with the intent of Release Management, Secure Copy can be initially configured to copy all files, as shown in Figure 4, to establish a baseline of files and then can be configured to copy all changed files to bring the target server in sync with the source server. This means during migrations, the target server’s settings (data, security, shares, etc) can be verified prior to the cutover, instead of having to use the blackout window method.

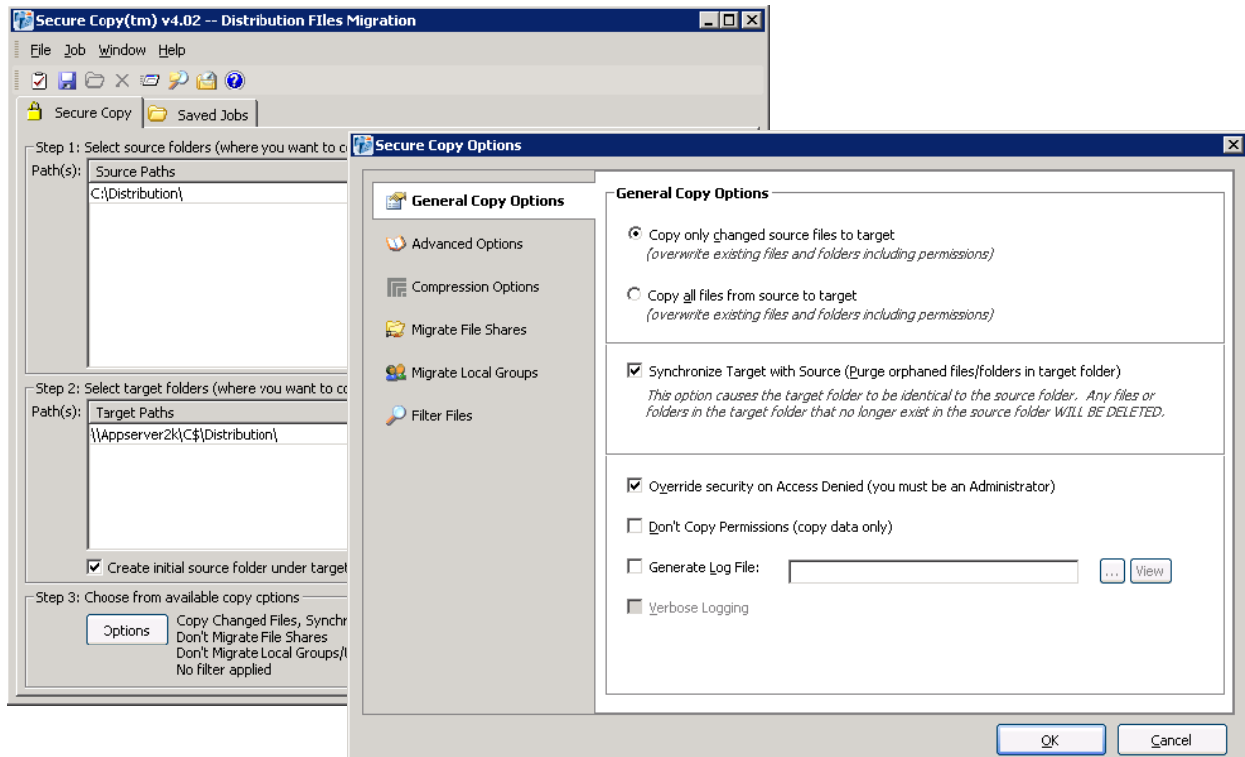


Figure 4: Perform comprehensive migrations in a proactive manner using flexible migration options.

Example 4: Report and History of Group Policy Changes

Related Processes: [Change Management](#)

ScriptLogic Solution: [Active Administrator](#)

As changes are released, those changes need to be reported to management. The process of Change Management handles this aspect of Service Support. Active Administrator’s Group Policy management capabilities extend into the area of reporting on changes (both before release, as in the case of RSoP reports based on offline GPOs) as well as reporting on historical change. In addition to its Offline GPO Repository, Active Administrator also maintains a database of GPO History. As a GPO is modified, a copy is retained and can be compared with the current version in order to report on changes, as shown in Figure 5

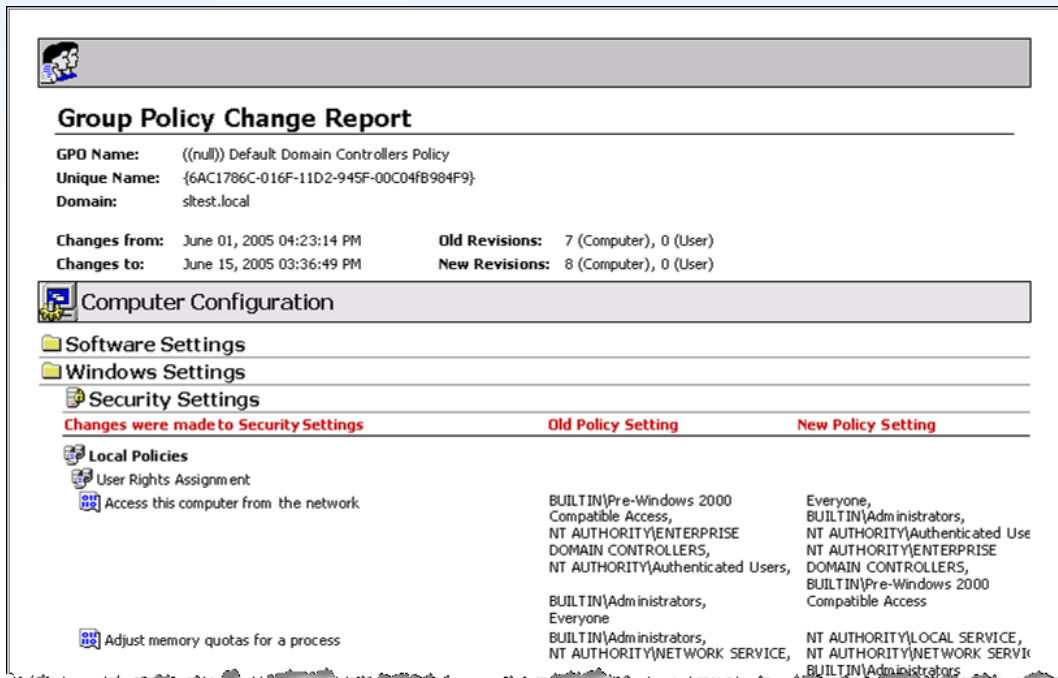


Figure 5: Report on changes to Group Policies with Active Administrator

If the current GPO is found to be problematic, an older version can be selected and a “rollback” can be performed to replace the current GPO with the version stored in GPO History, as shown in Figure 6.

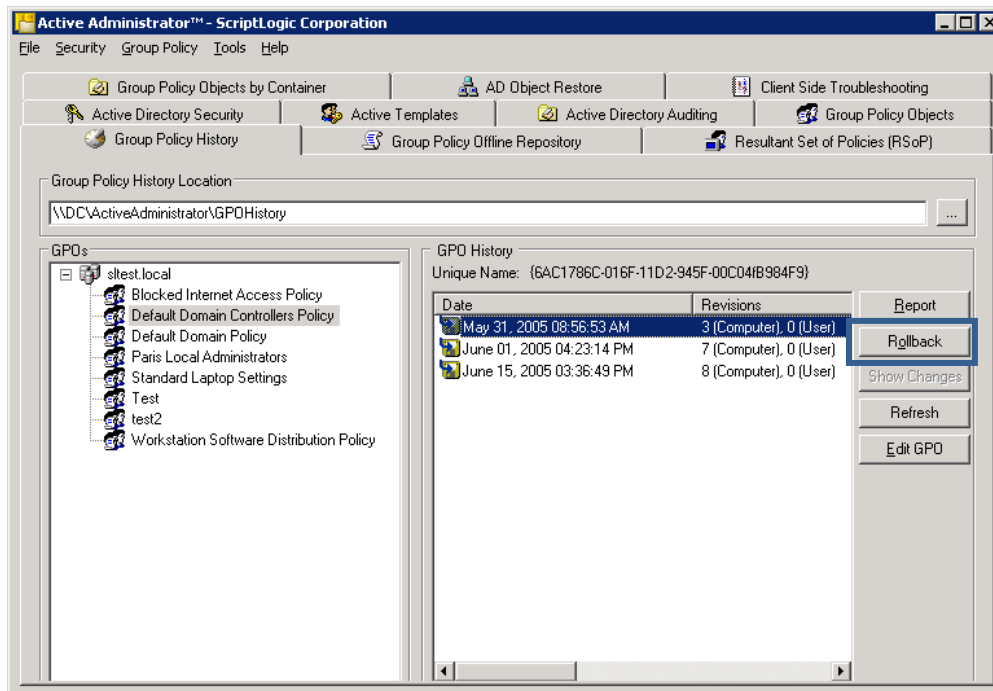


Figure 6: Rollback previous version of GPOs easily with Active Administrator

Example 5: Document Server Security Settings

Related Processes: [Configuration Management](#) / [Security Management](#) / [Problem Management](#)

ScriptLogic Solution: [Enterprise Security Reporter](#)

Configuration Management centers on first understanding the current configuration of systems. Enterprise Security Reporter (ESR) provides administrators with the ability to centrally capture security information on Windows and SharePoint servers throughout the network and then generate reports to be used in support of other ITIL processes, as well as during any audits. ESR, shown in Figure 7, collects information from Active Directory, Servers/Workstations, SharePoint, and more.

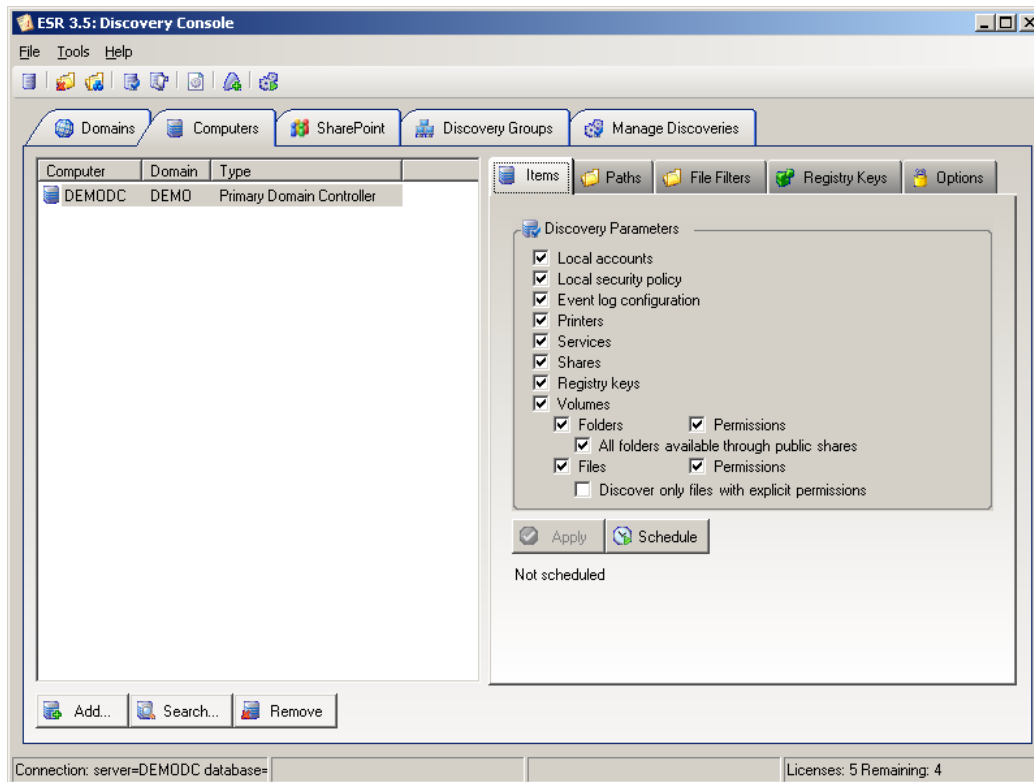


Figure 7: ESR comprehensively collects information to be used by several ITIL processes

Once collected, ESR reports on all of the various data types collected using pre-defined or custom reports. Figure 8 shows an example of a report generated with ESR. The information reported on by ESR can be used as documentation in the Configuration Management process, as well as by Security Management processes to ensure proper security is in place.

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

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

Figure 8: All of ESR's reports have a common look and feel

Example 6: Using Active Templates to Delegate Permissions

Related Processes: **Configuration Management / Security Management**

ScriptLogic Solution: **Active Administrator**

Both Configuration Management and Security Management deal with ensuring only the agreed upon security configuration is in place. Active Administrator's Active Templates simplify control over the delegation of user rights in Active Directory. For example, Active Templates can be used to quickly delegate admin tasks such as the ability to update user information or group memberships to department managers and junior administrators.

Active Templates, shown giving the Accounts Manager user account privileges in Figure 9, 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.

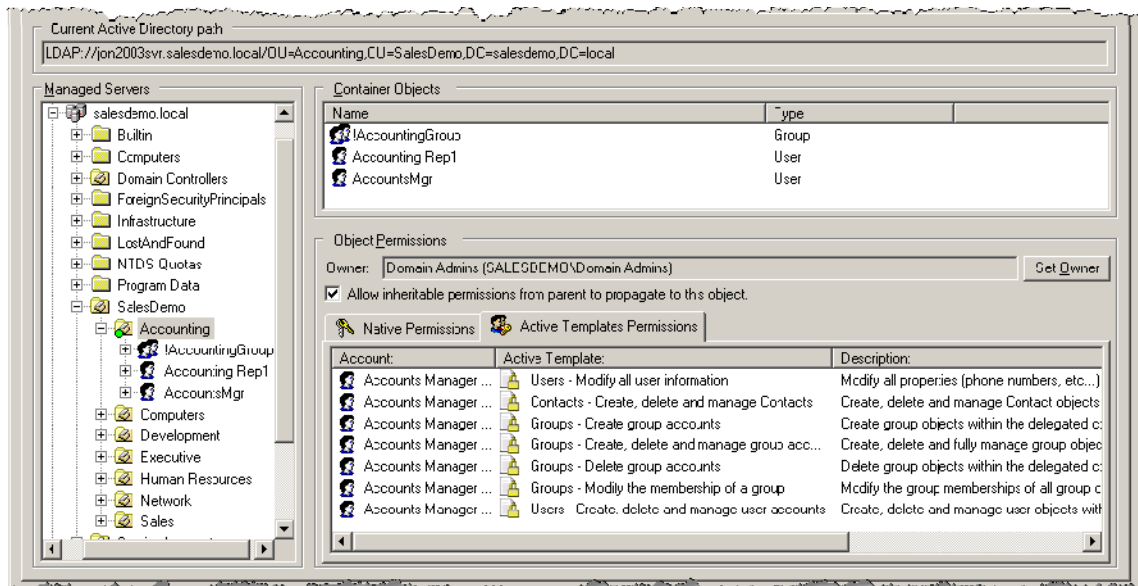


Figure 9: Each Active Template grants or revokes one or more user permissions, simplifying delegation

Active Templates are a proactive method of applying delegated permissions throughout Active Directory. Active Administrator also reactively enforces all delegated permissions that were set with Active Templates using an Active Template Repair function that runs as a service. Active Administrator can be configured to automatically instantly re-apply the Active Template to restore the user rights required for compliance with established security standards within an organization.

Example 7: Troubleshoot GPO Configuration Failures

Related Processes: **Incident Management, Configuration Management, Availability Management, Security Management**

ScriptLogic Solution: **Active Administrator**

In the event a desktop computer is having difficulty with a configuration specified with Group Policies, support staff can use Active Administrator's Client Side Troubleshooting feature to enable Group Policy logging, as well as to view the client's Application Log, Application Deployment Log and User Configuration Log, as shown in Figure 10.

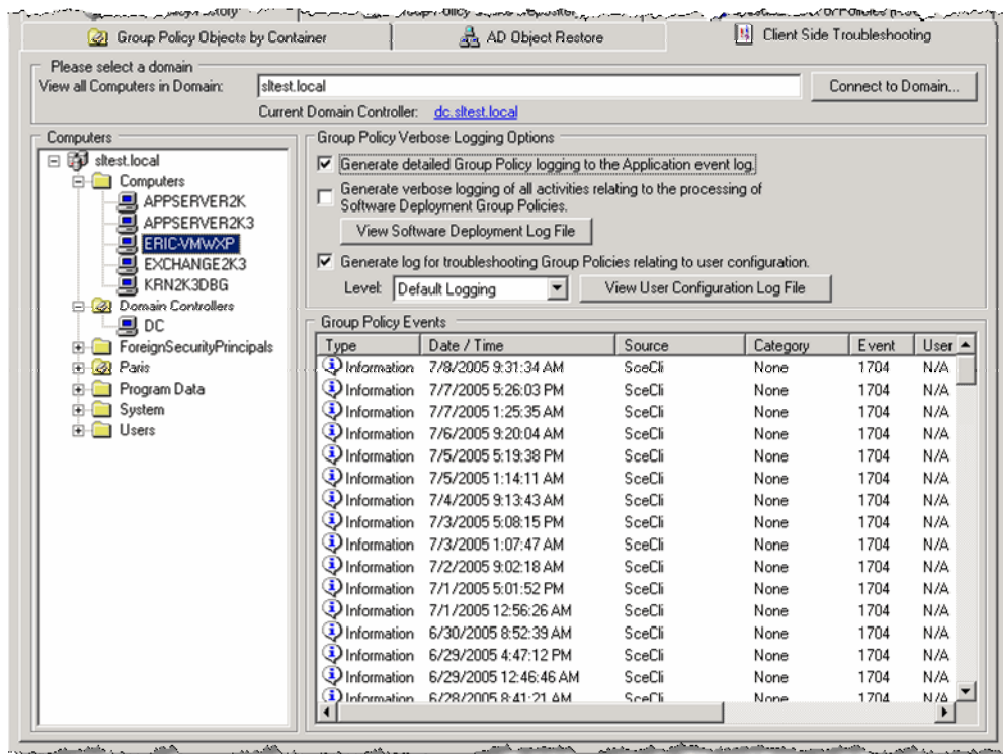


Figure 10: Determine the cause of applying group policies with Client-Side Troubleshooting

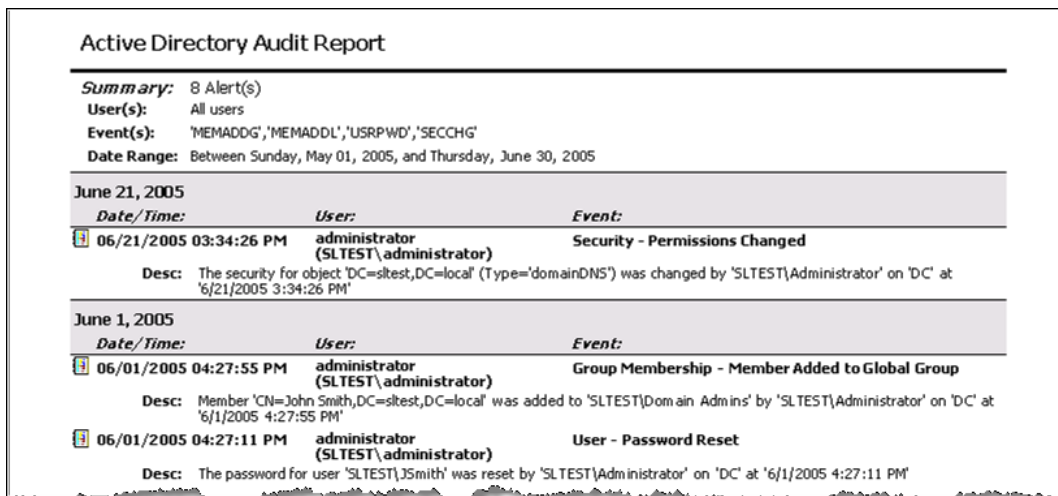
Client Side Troubleshooting is a vital tool in using Group Policies to manage server and desktop configurations, ensuring security, availability, and correct user workflows.

Example 8: Auditing the Management of Active Directory

Related Processes: **Configuration Management, Security Management**

ScriptLogic Solution: **Active Administrator**

To be aware of changes being made to your Active Directory, Active Administrator takes analysis of Active Directory audit logs to a new level, combining and filtering logs from all domain controllers, storing them in a database, and providing powerful reporting capabilities. This can be used to track new delegations and permission changes, and who made them (Figure 11). It can also be used to determine who reset a password, changed group memberships, or performed any other action within Active Directory. Active Administrator allows for long term storage of audit logs without the need for enormous Event Logs on individual domain controllers.



Active Directory Audit Report

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

June 21, 2005		
Date/Time:	User:	Event:
06/21/2005 03:34:26 PM	administrator (SLTEST\administrator)	Security - Permissions Changed
Desc: The security for object 'DC=sitest,DC=local' (Type='domainDNS') was changed by 'SLTEST\Administrator' on 'DC' at '6/21/2005 3:34:26 PM'		

June 1, 2005		
Date/Time:	User:	Event:
06/01/2005 04:27:55 PM	administrator (SLTEST\administrator)	Group Membership - Member Added to Global Group
Desc: Member 'CN=John Smith,DC=sitest,DC=local' was added to 'SLTEST\Domain Admins' by 'SLTEST\Administrator' on 'DC' at '6/1/2005 4:27:55 PM'		
06/01/2005 04:27:11 PM	administrator (SLTEST\administrator)	User - Password Reset
Desc: The password for user 'SLTEST\Jsmith' was reset by 'SLTEST\Administrator' on 'DC' at '6/1/2005 4:27:11 PM'		

Figure 11: Audit any changes made to Active Directory

Active Administrator can even send email alerts when selected events occur, for example when new users are added, or given extra permissions, as shown in Figure 12.

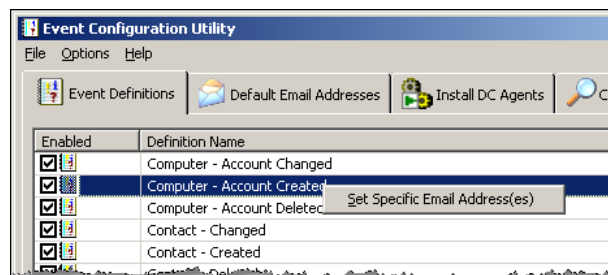


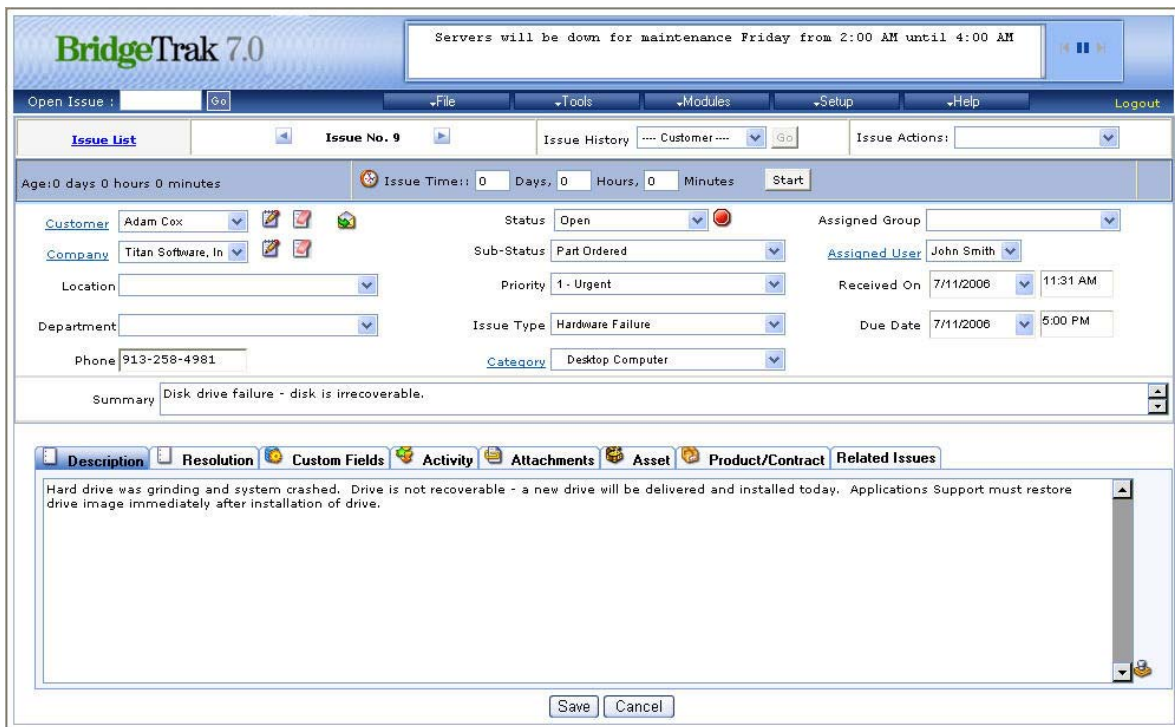
Figure 12: Auditing is enhanced by configuring real-time notification of Active Directory changes

Example 9: Manage Support Issues

Related Processes: **Incident Management**

ScriptLogic Solution: **BridgeTrak**

To restore normal service operation as quickly as possible and minimize the adverse impact on business operations, utilizing a helpdesk solution will assist in accomplishing the activities related to Incident Management (incident detection and recording, classification and initial support, investigation and diagnosis, and resolution and recovery). BridgeTrak provides a comprehensive set of tools to properly submit, track, document and resolve user issues as they occur.



The screenshot displays the BridgeTrak 7.0 web interface. At the top, a notification banner states: "Servers will be down for maintenance Friday from 2:00 AM until 4:00 AM". Below this is a navigation menu with options: Open Issue, File, Tools, Modules, Setup, Help, and Logout. The main content area is titled "Issue List" and shows "Issue No. 9". It includes a search bar for "Issue History" and "Issue Actions". A status bar indicates "Age: 0 days 0 hours 0 minutes" and "Issue Time: 0 Days, 0 Hours, 0 Minutes" with a "Start" button. The form fields are organized into two columns:

Customer: Adam Cox	Status: Open	Assigned Group:
Company: Titan Software, Inc	Sub-Status: Part Ordered	Assigned User: John Smith
Location:	Priority: 1 - Urgent	Received On: 7/11/2006 11:31 AM
Department:	Issue Type: Hardware Failure	Due Date: 7/11/2006 5:00 PM
Phone: 913-258-4981	Category: Desktop Computer	

The "Summary" field contains the text: "Disk drive failure - disk is irrecoverable." Below the form is a tabbed interface with tabs for Description, Resolution, Custom Fields, Activity, Attachments, Asset, Product/Contract, and Related Issues. The "Description" tab is active, showing the text: "Hard drive was grinding and system crashed. Drive is not recoverable - a new drive will be delivered and installed today. Applications Support must restore drive image immediately after installation of drive." At the bottom of the form are "Save" and "Cancel" buttons.

Figure 13: BridgeTrak provides centralized Incident Management, improving productivity and meeting SLAs

In addition to issue tracking and resolution, BridgeTrak provides an arsenal of add-on modules to facilitate user submission and management of their issues using a user-facing knowledgebase, automatic escalation of issues, easier receipt of issues via email and powerful searching capabilities, all in an effort to provide better service to users.

Example 10: Remotely Managing Clients

Related Processes: Incident Management, Problem Management

ScriptLogic Solution: Desktop Authority, Desktop Authority Remote Management Gateway

Both the Incident Management and Problem Management processes focus on the minimization of impact, as well as the amount of time required to fix a problem. Problems arising on client machines can be diagnosed identified and resolved remotely using Desktop Authority's Remote Management client. Using a Java-enabled web browser, administrators and helpdesk personnel can remotely access client machines, not just for the purpose of remotely controlling, but for the purpose of remotely managing a client machine.

In addition to troubleshooting a client problem by interactively controlling the desktop remotely, Desktop Authority's Remote Management client (shown in Figure 14) can also accomplish performance monitoring, management of disks, the registry, processes, services, users, groups and more all without disturbing the user while they work.

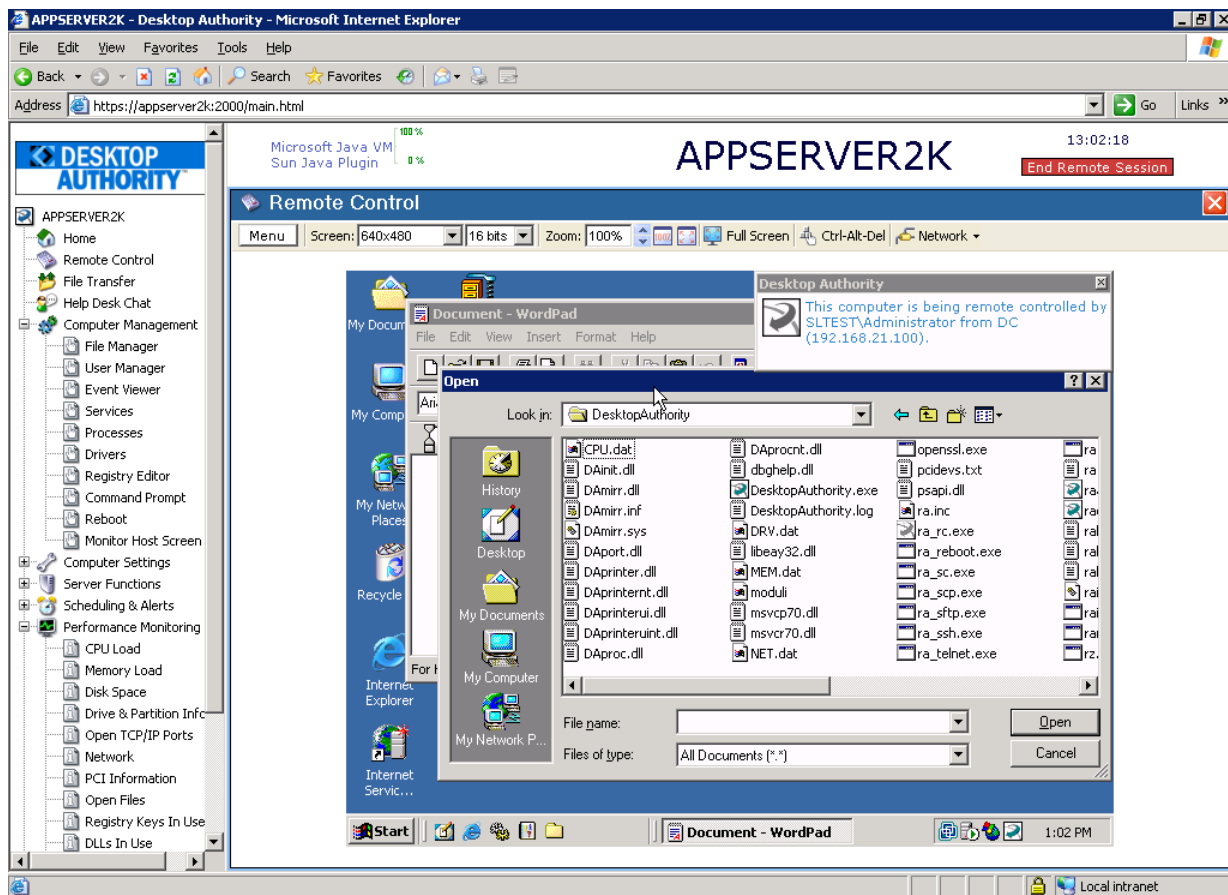


Figure 14: Troubleshooting a client problem remotely is a simple task with Desktop Authority's Remote Management client.

Desktop Authority Remote Management Gateway extends the reach of support professionals beyond the walls of the organization to allow the same remote management and control of machines both on and off the domain, regardless of their proximity to the corporate network. By using a gateway service residing on a perimeter network, users and support professionals can easily come together to quickly resolve issues remotely.

Example 11: Backing up and Restoring Group Policies

Related Processes: [Availability Management](#)

ScriptLogic Solution: [Active Administrator](#)

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

Active Administrator provides backup and restore functionality for several data sets within Active Directory. The first is Group Policies (shown in Figure 15), which can be backed up individually or as a whole and can be performed as a one-off backup, or scheduled. Restores of Group Policies are as easy as backing them up. Administrators can restore a Group Policy by simply selecting the backup location, and the policy or policies to be restored.

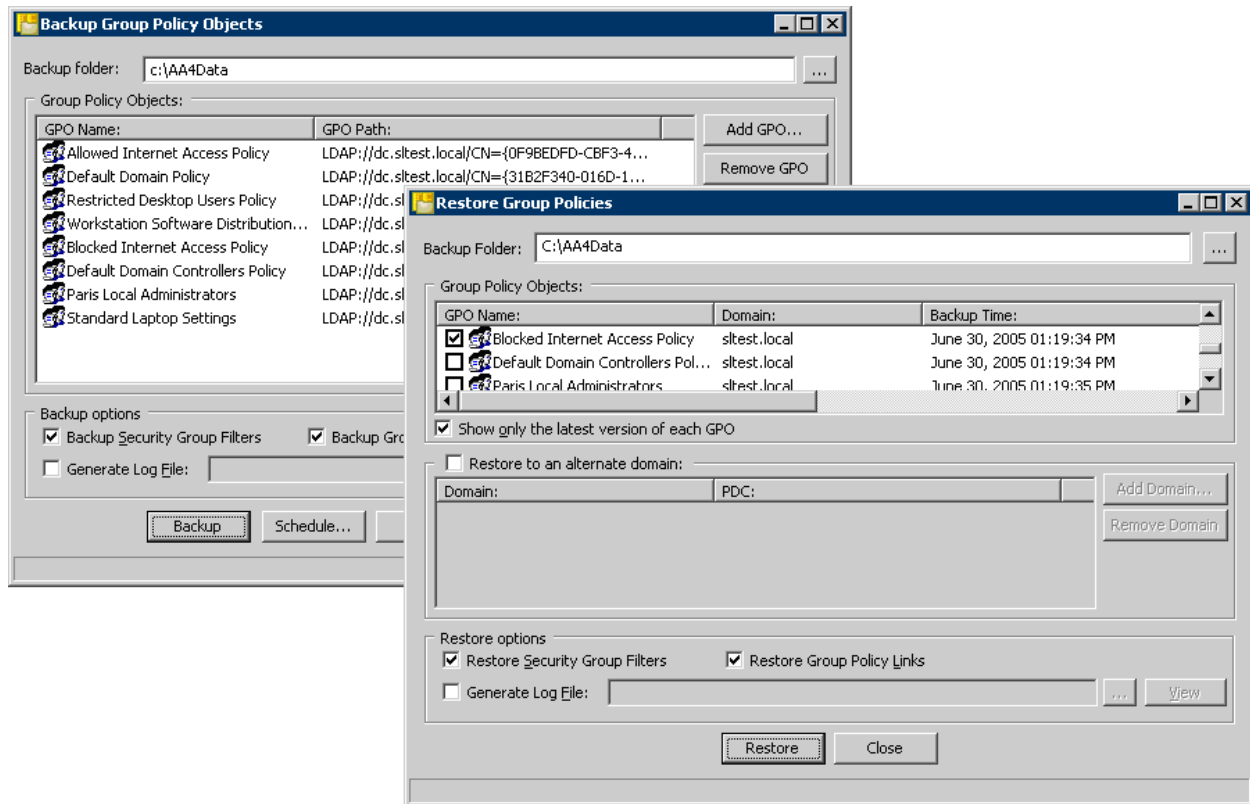


Figure 15: Active Administrator can backup and restore Group Policies making Group Policies highly available.

Example 12: Backing up and Restoring Active Directory Security

Related Processes: **Availability Management / Security Management**

ScriptLogic Solution: **Active Administrator**

An administrator's ability to function within Active Directory is directly impacted by a change in delegated permissions. While Active Templates aid in maintaining proper permissions, it is important to have a backup of those delegations throughout Active Directory. Active Administrator makes backing up Active Directory permissions (shown in Figure 16) a simple task by only requiring a backup filename and a chosen domain. Restores can be as granular as restoring only permissions to a select object or as broad as restoring permissions to the entire Directory.

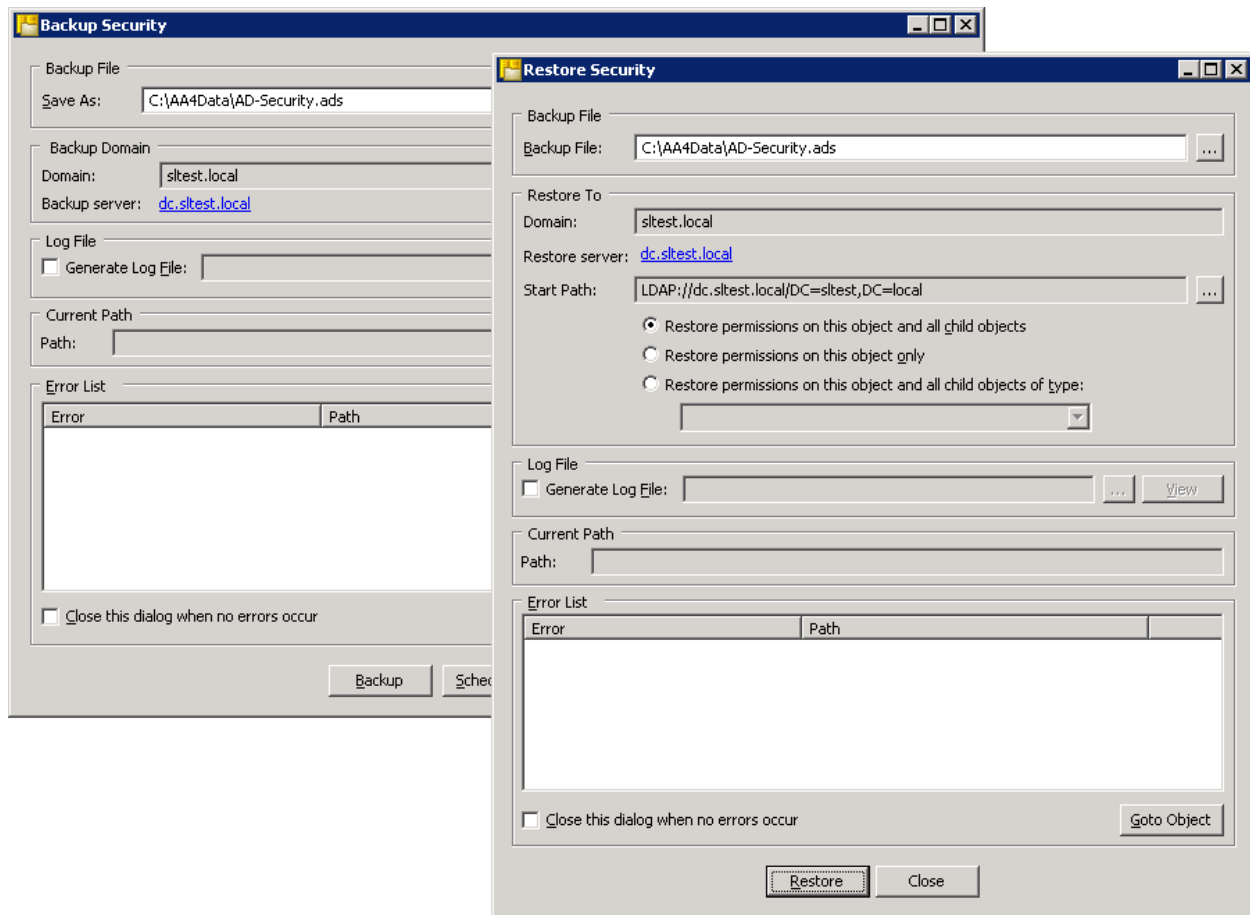


Figure 16: Active Administrator backs up and restores Active Directory permissions increasing the availability of Active Directory administration.

Example 13: Backing Up and Restoring Active Directory

Related Processes: [Availability Management](#) / [Security Management](#) / [Problem Management](#)

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 17 and Figure 18.

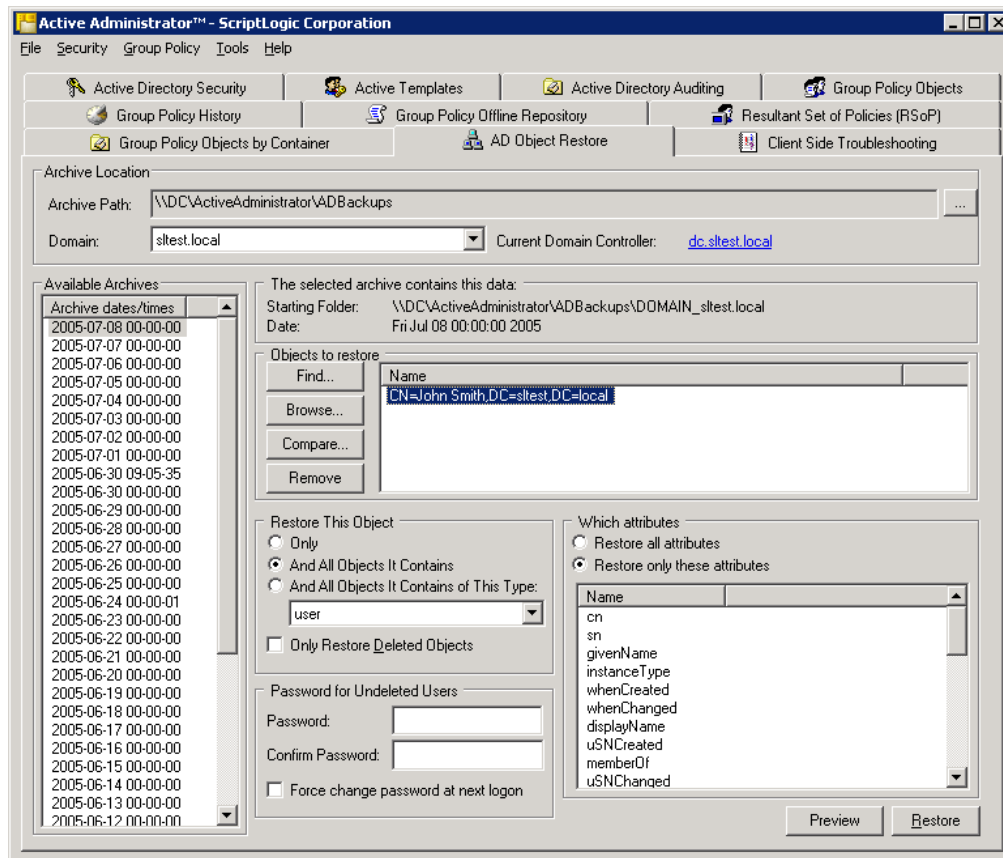


Figure 17: Powerful selection options make restoring deleted objects and object attributes a simple task.

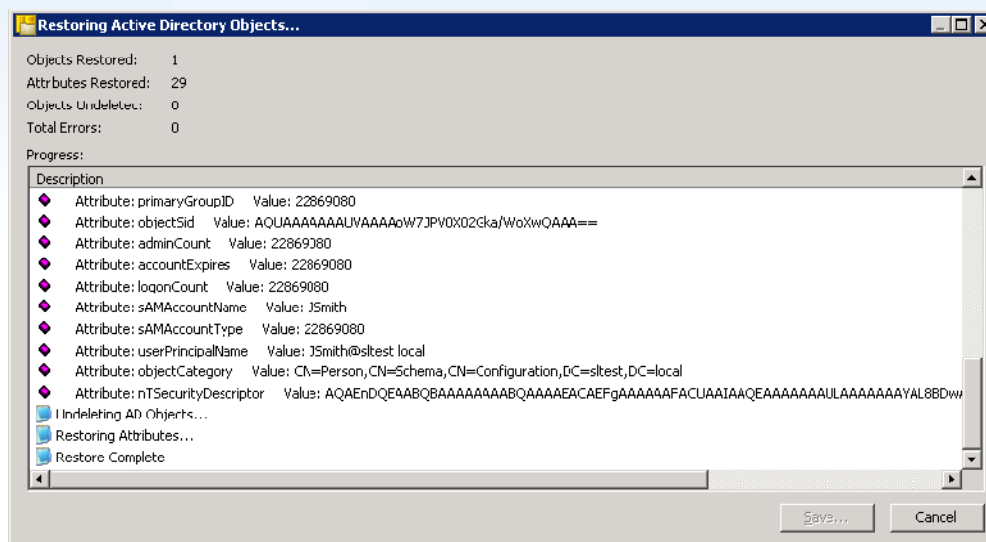


Figure 18: Restoring deleted objects together with all object attributes

Example 14: Backing up and Restoring Windows, SharePoint and SQL Server Security

Related Processes: **Availability Management, Security Management**

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

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

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

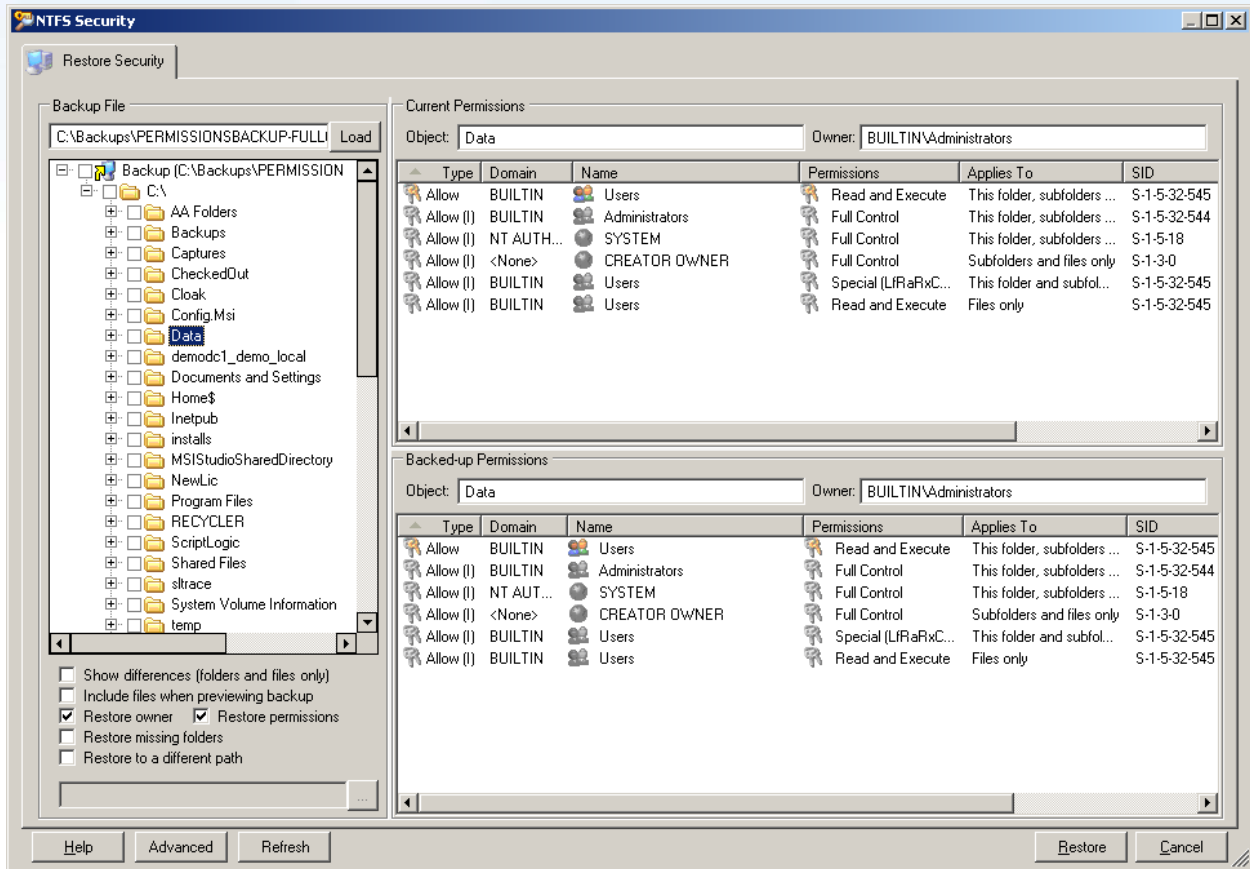


Figure 19: Using NTFS backups to restore permissions keeps files and services available.

Conclusion

ITIL establishes best practices but does not specify methods of implementation, forcing administrators of Windows-based networks are to decide for themselves how to implement and maintain ITIL best practices.

ScriptLogic products give administrators the tools they require to implement ITIL processes in the areas of Release, Change, Configuration, Incident, Problem, Availability and Security Management by empowering them to easily plan, design, report, make available, secure, and support Windows-based networks.

ScriptLogic solutions that assist with implementing ITIL best practices	
Active Administrator	Comprehensive Active Directory management solution that reduces the complexity of Active Directory security, delegation, group policies and recoverability.
BridgeTrak	Help desk solution that centrally manages user issues, from ticket tracking, to escalation to resolution.
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.
Desktop Authority	Comprehensive desktop management platform that provides centralized configuration, inventory, support and security of Windows-based clients.
Secure Copy	Data migration solution that additionally moves all supporting security-related data sets to ensure a secure duplicate of the original data.
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.

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