ACTIVE ADMINISTRATOR™

ScriptLogic®
Active Administrator™ 4
User Guide

SCRIPTLOGIC

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

1.561.886.2400
www.scriptlogic.com

Printed in the United States of America (12/2005)

DOCUMENTATION CONVENTIONS

Typeface Conventions

Bold	Indicates a button, menu selection, tab, dialog box title, text to type, selections from drop-down lists, or prompts on a dialog box.

CONTACTING SCRIPTLOGIC

ScriptLogic may be contacted about any questions, problems or concerns you might have at:

✉

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

☎

561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support

📠

561.886.2499 Fax

🖱

www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search Frequently Asked Questions, for the answers to the most common non-technical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

Contents

WHAT IS ACTIVE ADMINISTRATOR? 1

ACTIVE ADMINISTRATOR CONSOLE 4

STARTING ACTIVE ADMINISTRATOR 4
EXAMINING THE MAIN WINDOW 4
Tabs 5
Menu Bar 5
SETTING THE ACTIVE ADMINISTRATOR SERVER 6

ACTIVE DIRECTORY SECURITY 7

SELECTING SERVERS TO MANAGE 8
VIEWING PERMISSIONS FOR ACTIVE DIRECTORY OBJECTS 8
Filtering Permissions 9
VIEWING ACTIVE DIRECTORY OBJECTS BY TYPE 9
SEARCHING FOR ACTIVE DIRECTORY OBJECTS 10
Creating Custom Searches 12
SEARCHING FOR PERMISSIONS ON ACTIVE DIRECTORY OBJECTS 12
MODIFYING PERMISSIONS ON ACTIVE DIRECTORY OBJECTS 16
Disallow Propagation 17
Re-establish Propagation 17
DELEGATING CONTROL USING AN ACTIVE TEMPLATE 18
RESTORING DEFAULT PERMISSIONS ON ACTIVE DIRECTORY OBJECTS 21
MOVING ACTIVE DIRECTORY OBJECTS 22
CREATING NEW ACTIVE DIRECTORY OBJECTS 22
REPORTING ON ACTIVE DIRECTORY OBJECTS 22
BACKING UP SECURITY 25
Scheduling a Backup 25
RESTORING A SECURITY BACKUP 26

ACTIVE TEMPLATES 27

SETTING ACTIVE TEMPLATE OPTIONS 29
CREATING AN ACTIVE TEMPLATE 30
MODIFYING AN ACTIVE TEMPLATE 32
DELETING AN ACTIVE TEMPLATE 32
REPORTING ON ACTIVE TEMPLATES 32
DELEGATING CONTROL USING AN ACTIVE TEMPLATE 33
REPAIRING A BROKEN ACTIVE TEMPLATE 37

ACTIVE DIRECTORY AUDITING 39

GROUP POLICY OBJECTS 42

VIEWING GROUP POLICIES 43
MODIFYING PROPERTIES FOR A GROUP POLICY OBJECT 43
MODIFYING A GROUP POLICY OBJECT 44
Locating a Group Policy Object 44
COPYING GROUP POLICY OBJECTS 45
Save Copy Settings 46
Load Copy Settings 46
Schedule a Copy Job 46

CREATING A NEW GROUP POLICY OBJECT 46
RENAMING A GROUP POLICY OBJECT 47
REPORTING ON GROUP POLICY OBJECTS 47
BACKING UP A GROUP POLICY OBJECT 48
Save Backup Settings 49
Load Backup Settings 49
Schedule a Backup Job 49
RESTORING A GROUP POLICY OBJECT 50
ADDING A GROUP POLICY LINK 51
REMOVING A GROUP POLICY LINK 52

GROUP POLICY OBJECTS BY CONTAINER 53

MODIFYING A GROUP POLICY OBJECT 53
REMOVING BROKEN LINKS 54
LOCATING A GROUP POLICY OBJECT 55
REPORTING ON GROUP POLICY OBJECTS 56

GROUP POLICY HISTORY 57

VIEWING GROUP POLICY HISTORY 57
REPORTING ON GROUP POLICY HISTORY 58
COMPARING HISTORY ON GROUP POLICY OBJECTS 59
ROLLING BACK TO A PREVIOUS VERSION 60

RESULTANT SET OF POLICIES (RSOP) 61

RUNNING A WHAT-IF SCENARIO 61
VIEWING GPO PROPERTIES 65
REPORTING 65
EDITING A GPO 66
LOCATING A GPO 66

GROUP POLICY OFFLINE REPOSITORY 67

SETTING THE STARTING CONTAINER FOR OFFLINE GPOS 68
ADDING A GPO TO THE REPOSITORY 70
EDITING A GPO OFFLINE 71
VIEWING GROUP POLICY SETTINGS 72
Group Policy Settings Report 72
Group Policy Change Report 72
PUBLISHING GPO TO ACTIVE DIRECTORY 73
REMOVING A GPO FROM THE REPOSITORY 73

AD OBJECT RESTORE 74

SELECTING AN ARCHIVE TO RESTORE 76
FINDING OBJECTS IN AN ARCHIVE FILE 76
BROWSING FOR AN OBJECT IN AN ARCHIVE FILE 78
COMPARING ARCHIVED OBJECTS TO ACTIVE DIRECTORY 79
RESTORING AN ARCHIVED OBJECT 80
Removing Objects from the List 82
Specifying Attributes to Restore 82
Specifying How to Restore the Attributes 82
Resetting a User's Password 83
Initiating the Restore Process 84

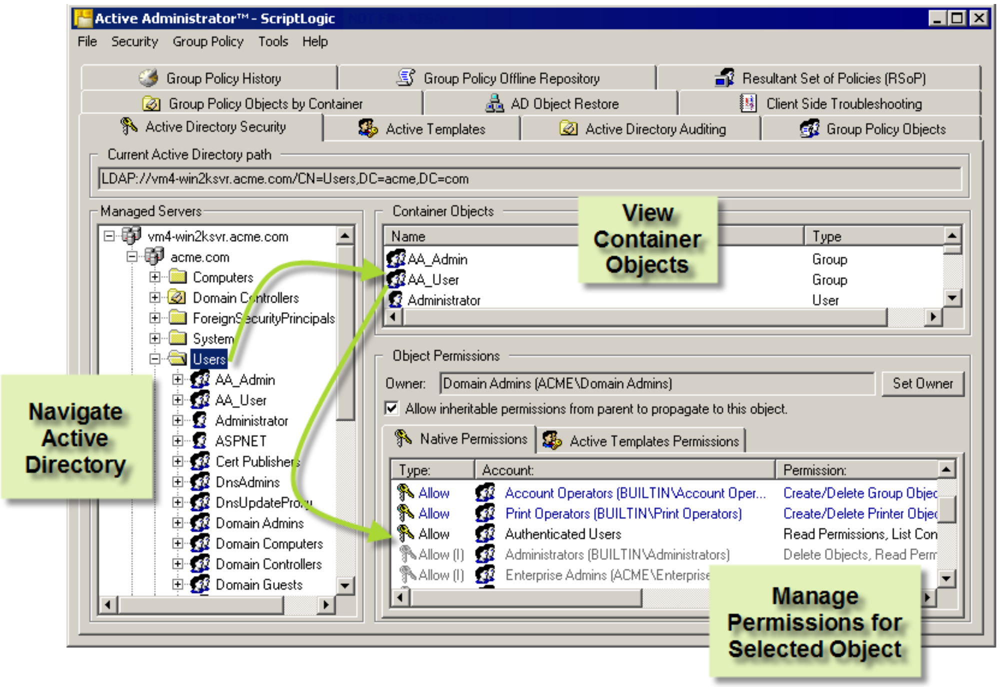
TROUBLESHOOTING.. 86
CLIENT SIDE TROUBLESHOOTING... 86
Setting Logging Options... 87
SETTING AUDITING PERMISSIONS 88
RESOLVING LICENSING ISSUES.. 89
CHANGING THE ACCOUNT FOR E-MAIL NOTIFICATIONS.. 90
REMOVING ACTIVE ADMINISTRATOR.. 90

INDEX.. 91

What is Active Administrator?

Active Administrator™ is an enterprise Active Directory® management and auditing solution that takes over where Active Directory leaves off. If Active Directory security is one of your company's concerns, then Active Administrator is the right tool for you. Its easy-to-use interface gives you single-seat enterprise control over your entire Active Directory security and Group Policies. While Microsoft® native tools give you single object administration to both security and group policies, those tools require endless nested buttons and dialog boxes just to accomplish simple tasks and cause you to focus on the individual task at hand, without a view of the larger picture. Take a look at the features of Active Administrator to see what we mean by the larger picture:

- **Simple Security Administration.** Active Administrator simplifies Active Directory permissions by using a flexible interface, allowing easy navigation of your Active Directory in one pane, with instant access to all permissions in another. Filtering of inherited or assigned permissions also narrow down the focus of your management.



LDAP://vm4-win2ksvr.acme.com/CN=Users,DC=acme,DC=com

Name	Type
AA_Admin	Group
AA_User	Group
Administrator	User

Owner: Domain Admins (ACME\Domain Admins)

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

Type:	Account:	Permission:
Allow	Account Operators (BUILTIN\Account Oper...	Create/Delete Group Objec
Allow	Print Operators (BUILTIN\Print Operators)	Create/Delete Printer Objec
Allow	Authenticated Users	Read Permissions, List Con
Allow (I)	Administrators (BUILTIN\Administrators)	Delete Objects, Read Perm
Allow (I)	Enterprise Admins (ACME\Enterprise	

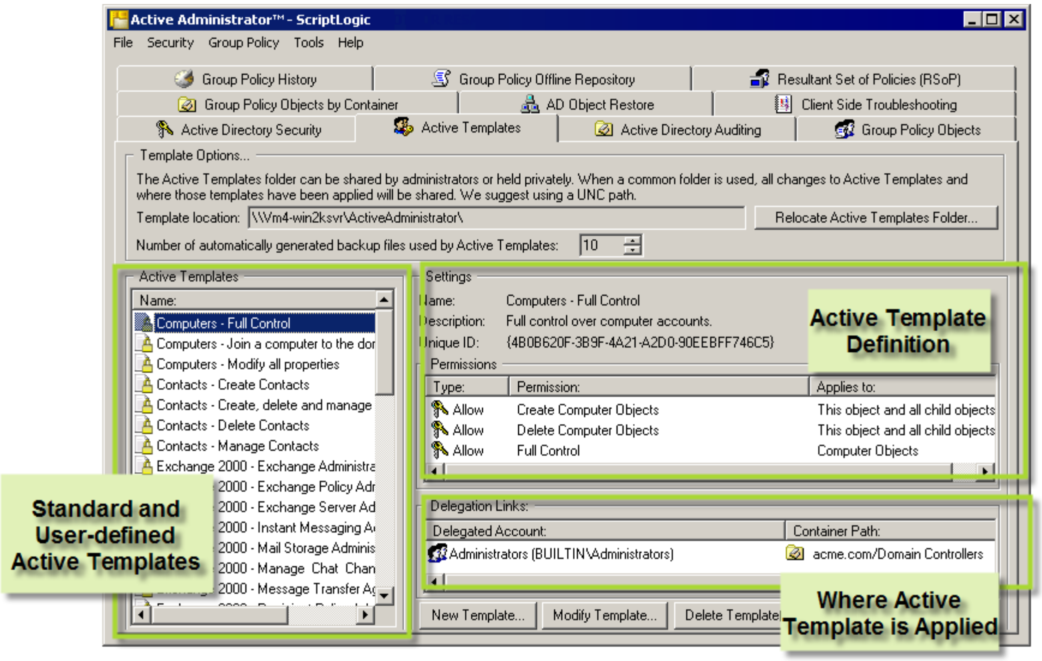
NEW!

- **Active Directory Backup and Restore.** Administrators can select a domain that contains Windows Server™ 2003 domain controllers and back up all Active Directory objects in that domain. When a situation occurs that require an object to be restored, administrators can select the object from a list and restore either the object with all the attributes it possessed when it was backed up, or only attributes the administrator selects. In the case of a container object, administrators have the option of either restoring all objects it contains or all objects it contains of a particular type.

Administrators can preview an object before it's actually restored or compare the attributes of the selected object in the archive with those of the same object in the Active Directory. Backups can either be scheduled or invoked interactively (restores are interactive only).

Important: You must have a Windows 2003 domain controller to restore both attributes and objects to Active Directory. If you have a Windows 2000 domain controller, you can restore only attributes.

- **Active Templates.** Active Administrator exclusively uses Active Templates, which make assigning permissions easier by taking the guesswork out of what permissions need to go where. Several Active Templates are included with your Active Administrator installation, and you also can create your own.


Active Administrator™ - ScriptLogic
File
Security
Group Policy
Tools
Help
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Relocate Active Templates Folder...
New Template...
Modify Template...
Delete Template
Active Template Definition
Standard and User-defined Active Templates
Where Active Template is Applied

Template Options...

The Active Templates folder can be shared by administrators or held privately. When a common folder is used, all changes to Active Templates and where those templates have been applied will be shared. We suggest using a UNC path.

Template location: \\Vm4-win2ksvr\ActiveAdministrator\

Number of automatically generated backup files used by Active Templates: 10

Active Templates

Name:
Computers - Full Control
Computers - Join a computer to the dor
Computers - Modify all properties
Contacts - Create Contacts
Contacts - Create, delete and manage
Contacts - Delete Contacts
Contacts - Manage Contacts
Exchange 2000 - Exchange Administra
2000 - Exchange Policy Adr
2000 - Exchange Server Ad
2000 - Instant Messaging A
2000 - Mail Storage Adminis
2000 - Manage Chat Chan
2000 - Message Transfer Ag

Settings

Name: Computers - Full Control
Description: Full control over computer accounts.
Unique ID: {4B0B620F-3B9F-4A21-A2D0-90EEBFF746C5}

Permissions

Type:	Permission:	Applies to:
Allow	Create Computer Objects	This object and all child objects
Allow	Delete Computer Objects	This object and all child objects
Allow	Full Control	Computer Objects

Delegation Links:

Delegated Account:	Container Path:
Administrators (BUILTIN\Administrators)	acme.com/Domain Controllers

You can create your own Active Template by creating a new template or modifying one of the standard templates. To delegate permissions by using an Active Template, choose the object to be managed, select the user or group to be assigned the permissions, and then select the Active Template.

NEW!

- **Active Templates Auto-Repair.** Active Templates, which are used to grant specific sets of Active Directory rights to an object, can be configured so that they are automatically reapplied if any of their permissions within the template are accidentally removed. Additionally, administrators can be automatically alerted via email when an Active Template is repaired.

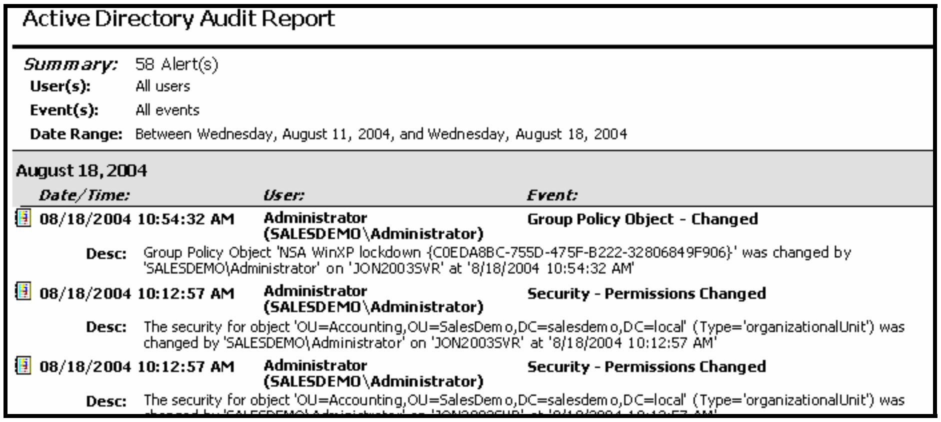
- **Group Policy Management.** Like Active Directory permissions, Active Administrator makes Group Policy administration simple using the same easy interface. Plan Group Policy settings using Resultant Set of Policies calculations to determine the net effect policies have without actually having to implement them.

NEW!

- **Offline GPO Repository.** Administrators can now edit Group Policies offline from Active Directory, protecting the live network from unintended changes in Group Policies. Offline Group Policies can be analyzed, edited, and compared with their live counterparts. In addition, Active Administrator's enhanced RSoP functionality can be run against a mixture of live and offline Group Policy Objects (GPOs) to simulate the effect of GPO changes before they are put into the live environment. Finally, GPO permissions management provides change control and ensures that only senior administrators can publish offline GPOs into the live environment.

- **Group Policy Backups.** Unlike the native backup of group policies via the System State, Active Administrator can back up and restore group policies, allowing faster response to corruption or changes that have a negative impact on users.

- **Auditing.** Active Administrator centrally audits the security event logs on your domain controllers. By auditing the changes made to Active Directory permissions or group policies, you can find out what changes were made in Active Directory and who made changes without having to filter through potentially thousands of event log entries. Active Administrator can even email you when changes are made.



Active Directory Audit Report

Summary: 58 Alert(s)
User(s): All users
Event(s): All events
Date Range: Between Wednesday, August 11, 2004, and Wednesday, August 18, 2004

August 18, 2004

Date/Time:	*User:*	*Event:*
08/18/2004 10:54:32 AM	**Administrator (SALESDEMO\Administrator)**	**Group Policy Object - Changed**
Desc:	Group Policy Object 'NSA WinXP lockdown {C0EDA8BC-755D-475F-B222-32806849F906}' was changed by 'SALESDEMO\Administrator' on 'JON2003SVR' at '8/18/2004 10:54:32 AM'	
08/18/2004 10:12:57 AM	**Administrator (SALESDEMO\Administrator)**	**Security - Permissions Changed**
Desc:	The security for object 'OU=Accounting,OU=SalesDemo,DC=salesdemo,DC=local' (Type='organizationalUnit') was changed by 'SALESDEMO\Administrator' on 'JON2003SVR' at '8/18/2004 10:12:57 AM'	
08/18/2004 10:12:57 AM	**Administrator (SALESDEMO\Administrator)**	**Security - Permissions Changed**
Desc:	The security for object 'OU=Accounting,OU=SalesDemo,DC=salesdemo,DC=local' (Type='organizationalUnit') was	

Active Administrator Console

Active Administrator Console extends the functionality of the built-in Windows management tools for Active Directory by allowing administrators to view and manage security in a much more extensible interface. Active Administrator gives administrators the ability to control permissions inheritance on objects as well as change inherited permissions to explicit permissions.

STARTING ACTIVE ADMINISTRATOR

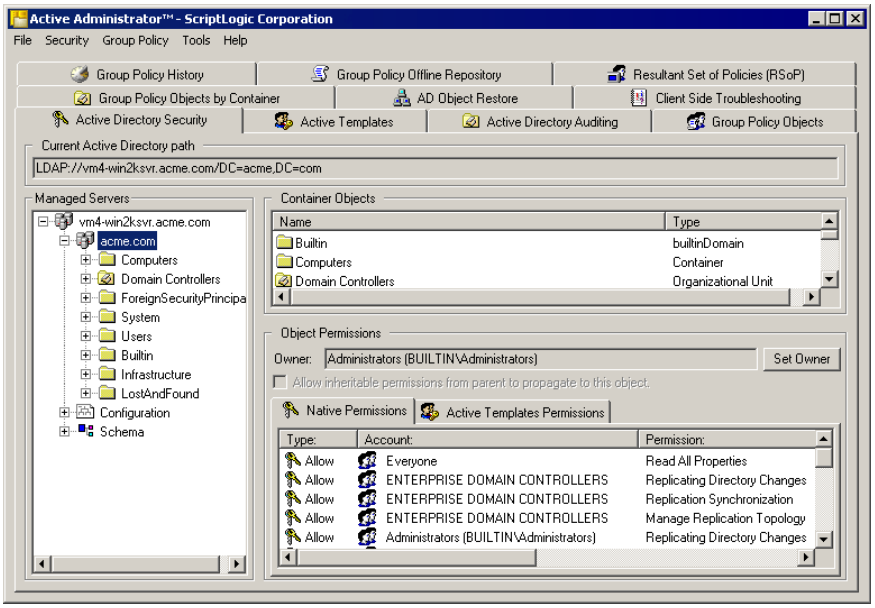
▶ Click **Start**, point to **Programs** > **ScriptLogic Corporation** > **Active Administrator**, and then choose **Active Administrator Console**.

Each time you run the program you are greeted by the splash screen.

ACTIVE
ADMINISTRATOR™
Copyright © 1997–2005 ScriptLogic Corporation. All rights reserved. This program is protected by U.S. and International copyright laws as described in Help About
SCRIPTLOGIC®

EXAMINING THE MAIN WINDOW

Active Administrator was designed to be easy to use. Functions are grouped on tabs and actions are accessible through the menu bar or by right-clicking to view a shortcut menu.



Current Active Directory path: LDAP://vm4-win2ksvr.acme.com/DC=acme,DC=com

Name	Type
Builtin	builtinDomain
Computers	Container
Domain Controllers	Organizational Unit

Owner: Administrators (BUILTIN\Administrators)

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

Type:	Account:	Permission:
Allow	Everyone	Read All Properties
Allow	ENTERPRISE DOMAIN CONTROLLERS	Replicating Directory Changes
Allow	ENTERPRISE DOMAIN CONTROLLERS	Replication Synchronization
Allow	ENTERPRISE DOMAIN CONTROLLERS	Manage Replication Topology
Allow	Administrators (BUILTIN\Administrators)	Replicating Directory Changes

Actions in Active Administrator are grouped by function on various tabs. Within each tab, use the menu bar and convenient shortcut menus to manage your Active Directory.

Tabs

Tab	Description
Active Directory Security	View and modify permissions on Active Directory objects in your entire domain.
Active Templates	Use the standard Active Templates or create your own to quickly create and manage sets of permissions to be applied to objects in Active Directory.
Active Directory Auditing	View the security event logs that occur when changes are made to Active Directory.
Group Policy Objects	Create, delete, or rename Group Policy objects, and add or remove links. Copy a Group Policy object from one domain to another or explore the exact location on the network where the object is stored.
Group Policy Objects by Container	View Group Policy objects by the containers to which they are linked, which allows administrators to quickly view Group Policy object application for a specific container.
AD Object Restore	Select a backup archive copy of an Active Directory object from a list and restore either the object with all the attributes it possessed when it was backed up, or only attributes the administrator selects.
Client Side Troubleshooting	View event log entries on Windows 2000 and later client computers to quickly view Group Policy Object application and errors on remote machines.
Group Policy History	View Group Policy History on all Group Policy objects in your domains. Selectively roll back to a previously saved version.
Group Policy Offline Repository	Make a copy of the GPO to edit without interfering with the normal operation of Active Directory. When editing is complete, the changed GPO can be exported to Active Directory in a single operation.
Resultant Set of Policies (RSoP)	Perform several calculations of what if scenarios, including the addition or removal of objects from OUs, Sites, or Security Groups to quickly view Group Policy Object application and errors on remote machines.

Menu Bar

You mostly use the short-cut menus on each tab to perform most of the tasks with Active Administrator. The top menu bar provides a few other functions.

File Menu

Menu Option	Description
Exit	Close Active Administrator.

Security Menu

Menu Option	Description
Backup	Back up permissions on a selected domain.
Restore	Restore previously backed up permissions.

Group Policy Menu

Menu Option	Description
Copy Group Policy Objects	Copy a Group Policy object to another domain.
Backup Group Policy Objects	Back up selected Group Policy objects.
Restore Group Policy Objects	Restore a previously backed up Group Policy object.

Tools Menu

Menu Option	Description
Set Active Administrator Server	Select the server where Active Administrator Server is installed.
Set Temporary Active Directory Location	Select the starting container for the Offline GPOs. The selected OU is saved in the registry.

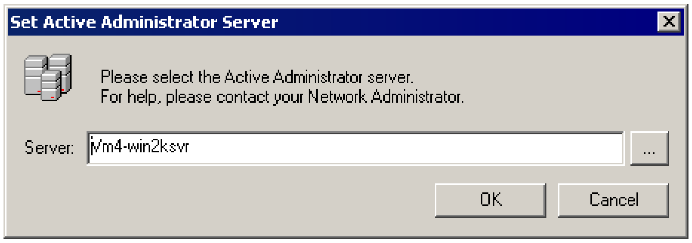
Help Menu

Menu Option	Description
Help Contents	Opens online help.
About Active Administrator	Displays Information about the version of Active Administrator installed on your computer, and provides a means to apply a license file or to visit the ScriptLogic web site.

SETTING THE ACTIVE ADMINISTRATOR SERVER

Before using Active Administrator, link the Active Administrator Console to the server that is running Active Administrator Server.

1. Click **Start**, point to **Programs** > **ScriptLogic Corporation** > **Active Administrator**, and then choose **Active Administrator Console**.
2. From the **Tools** menu, choose **Set Active Administrator Serve**r.
3. In the **Server** box, type the name of the server where Active Administrator Server is installed, or click ... to locate a server.



Set Active Administrator Server

Please select the Active Administrator server.
For help, please contact your Network Administrator.

Server: Vm4-win2ksvr

4. Click **OK**.

Active Directory Security

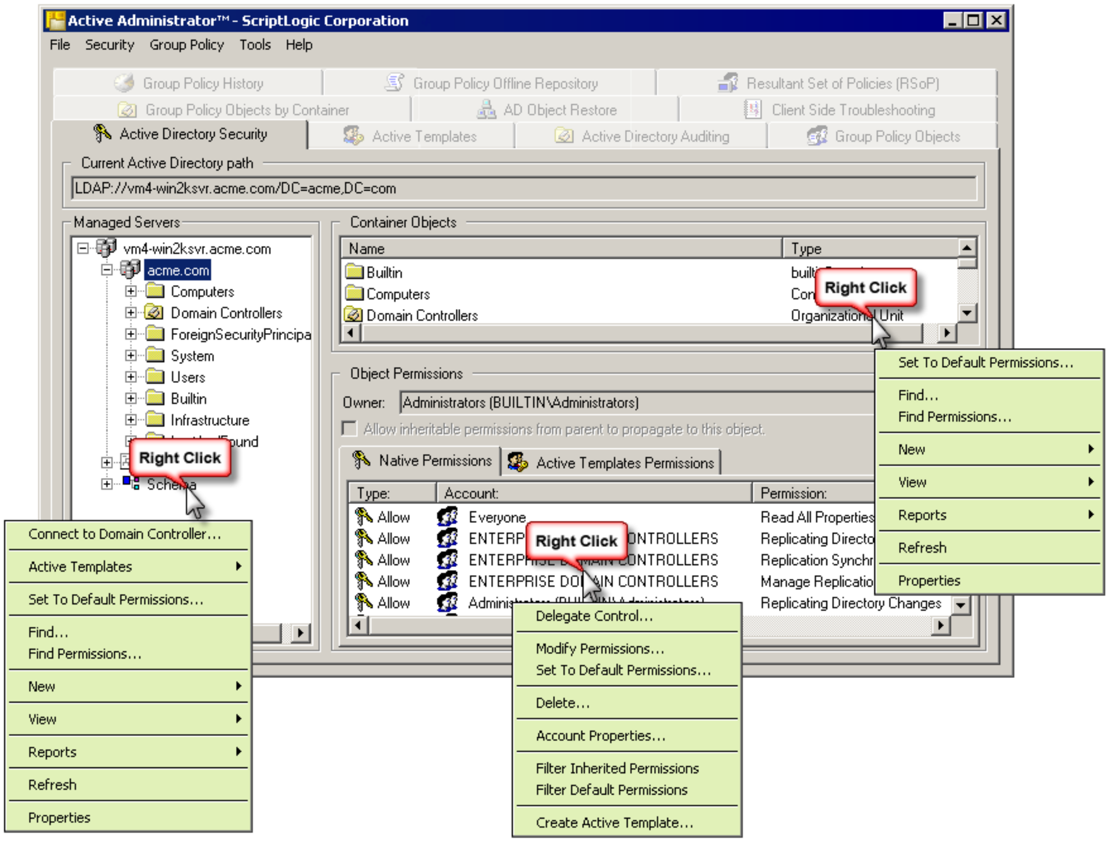
Active Administrator's main permissions display gives extended information in addition to the general rights that are visible in the built-in tools.

- Active Administrator allows you to completely manage your Active Directory domains. From one workstation, you can perform all of the management functions for your entire enterprise, regardless of multiple forests and discontiguous namespaces.

- Active Administrator allows you to select any container in Active Directory and view all of the objects in that container and its subcontainers. You have the ability to display all users, groups, organizational units, and computers in a concise grouping from which you can clearly see the properties of the objects and easily generate reports that contain extended information for these objects.

- Active Administrator simplifies management by providing access to the Active Directory configuration and schema. There is no more need to create custom MMC snap-ins to perform these tasks.

- Active Administrator displays the full Lightweight Directory Access Protocol (LDAP) name for any selected object in the interface, which helps administrators familiarize themselves with the naming convention and provides interoperability by making it easy to provide this information to other applications that may need it.



Active Administrator™ - ScriptLogic Corporation

Current Active Directory path: LDAP://vm4-win2ksvr.acme.com/DC=acme,DC=com

Owner: Administrators (BUILTIN\Administrators)

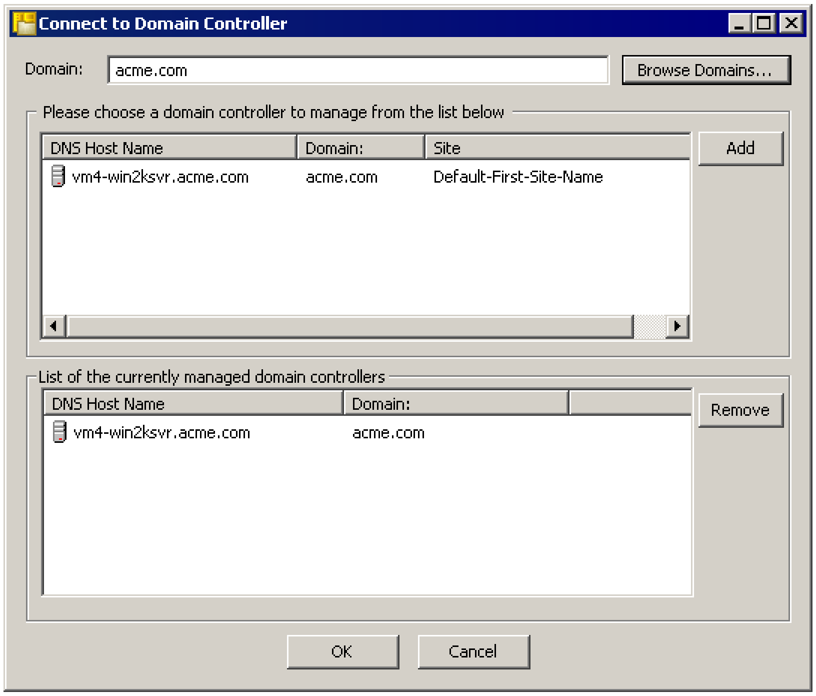
□ Allow inheritable permissions from parent to propagate to this object.

Name	Type
Builtin	builti
Computers	Con
Domain Controllers	Organizational Unit

Type:	Account:	Permission:
Allow	Everyone	Read All Properties
Allow	ENTERP ONTROLLERS	Replicating Directo
Allow	ENTERPRISE D MAIN CONTROLLERS	Replication Synchr
Allow	ENTERPRISE DO IN CONTROLLERS	Manage Replicatio
Allow	Administrators (BUILTIN\Administrators)	Replicating Directory Changes

SELECTING SERVERS TO MANAGE

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. Right click inside the **Managed Servers** list box, and then select **Connect to Domain Controller**. The **Connect to Domain Controller** dialog box opens.
3. In the **Domain** box, type the domain name, or click **Browse Domains** to select a domain. The domain controllers for the selected domain display in the top box.
4. In the top box, select the domain controller(s) that you want to manage, and then click **Add**. The selected domain controller(s) display in the bottom box.



Domain: acme.com

Please choose a domain controller to manage from the list below

DNS Host Name	Domain:	Site
vm4-win2ksvr.acme.com	acme.com	Default-First-Site-Name

List of the currently managed domain controllers

DNS Host Name	Domain:	
vm4-win2ksvr.acme.com	acme.com	

Note: To remove a selected domain controller from the list, click **Remove**.

5. Click **OK**.

Note: To add more domain controllers, repeat the above process for all of the domain controllers that you want to manage.

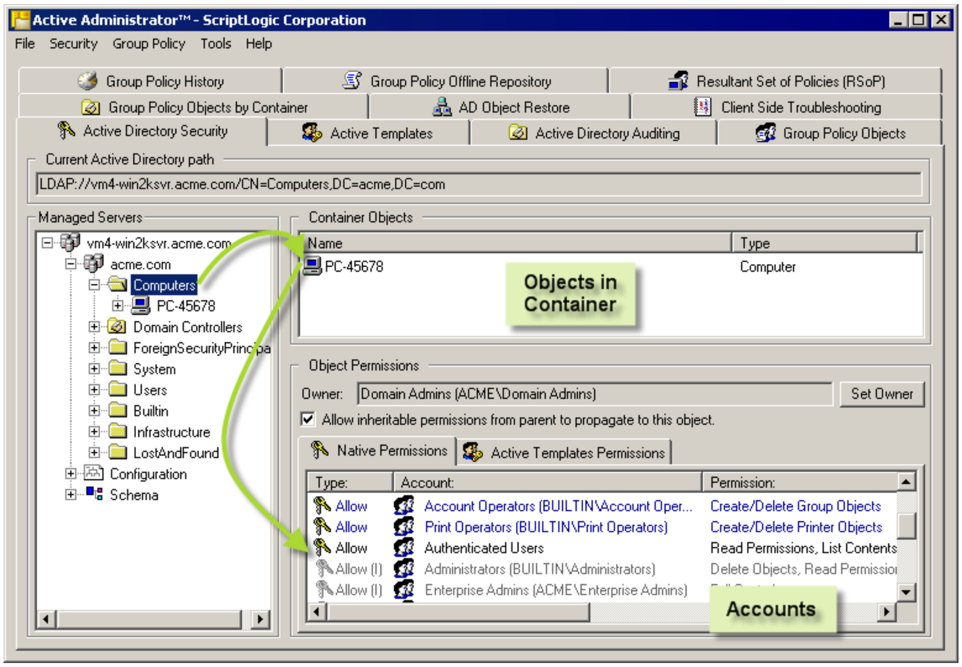
VIEWING PERMISSIONS FOR ACTIVE DIRECTORY OBJECTS

Note: You cannot view permissions on users, groups, OUs, or computers that are not included in the list of licensed OUs. If you select a user, group, OU, or computer that is not within the scope of your license, you see an error message. See *Resolving Licensing Issues*.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, expand the hierarchy, and then select the desired object. The Lightweight Directory Access Protocol (LDAP) path displays in the **Current Active Directory** path box.

   If the selected object is a container, the container objects are listed in the **Container Objects** area. You can select an object here also to view permissions.

The permissions for the selected object display in the **Object Permissions** area. Inherited permissions display in gray.



Current Active Directory path: LDAP://vm4-win2ksvr.acme.com/CN=Computers,DC=acme,DC=com

Name	Type
PC-45678	Computer

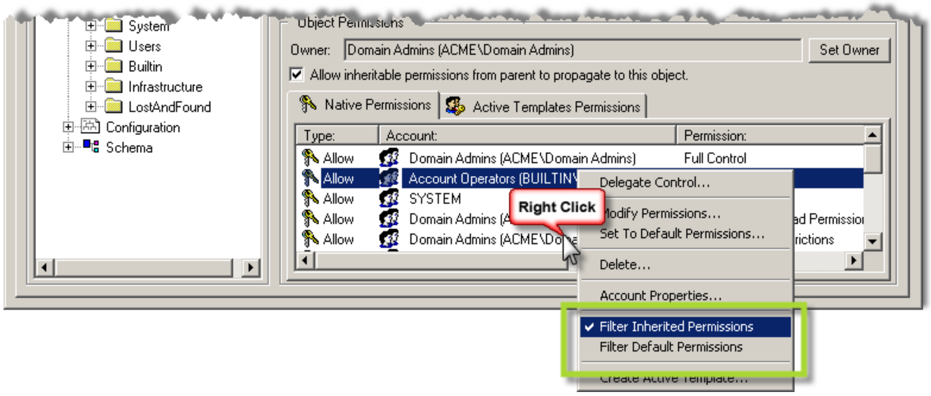
Owner: Domain Admins (ACME\Domain Admins)

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

Type:	Account:	Permission:
Allow	Account Operators (BUILTIN\Account Oper...	Create/Delete Group Objects
Allow	Print Operators (BUILTIN\Print Operators)	Create/Delete Printer Objects
Allow	Authenticated Users	Read Permissions, List Contents
Allow (I)	Administrators (BUILTIN\Administrators)	Delete Objects, Read Permissio
Allow (I)	Enterprise Admins (ACME\Enterprise Admins)	

Filtering Permissions

Right-click in the **Object Permissions** area, and then select to filter out **Inherited Permissions**, **Default Permissions**, or both.



Owner: Domain Admins (ACME\Domain Admins)

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

Type:	Account:	Permission:
Allow	Domain Admins (ACME\Domain Admins)	Full Control
Allow	Account Operators (BUILTIN\	
Allow	SYSTEM	
Allow	Domain Admins (A	ad Permissio
Allow	Domain Admins (ACME\Do	rictions

VIEWING ACTIVE DIRECTORY OBJECTS BY TYPE

With Active Administrator, you can view all objects of a specific type within a container and its subcontainers.

Note: You cannot view permissions on users, groups, OUs, or computers that are not included in the list of licensed OUs. If you select a user, group, OU, or computer that is not within the scope of your license, you see an error message. See *Resolving Licensing Issues*.

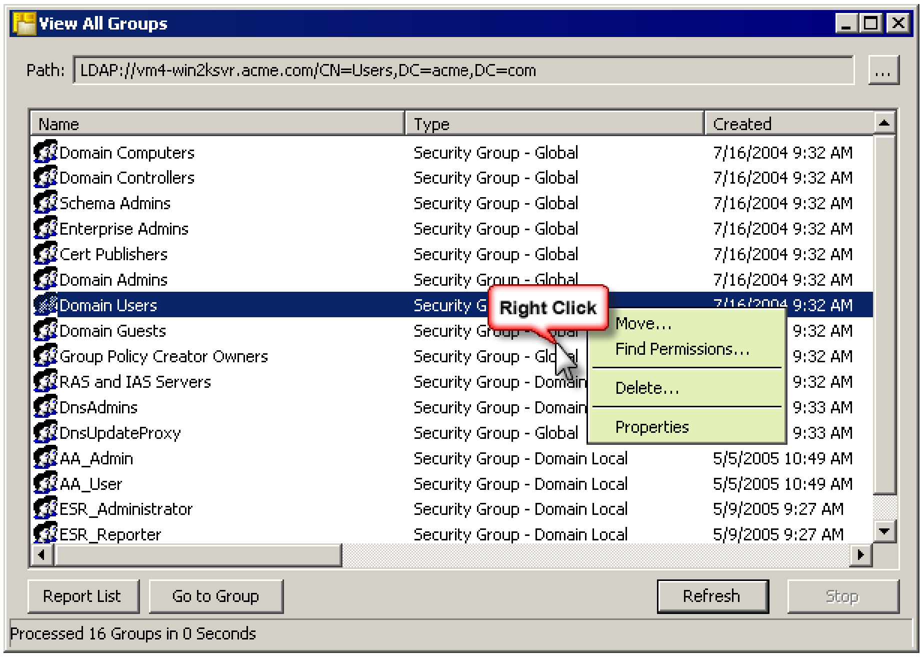
1. From the Active Administrator Console, open the **Active Directory Security** tab.

2. In the **Managed Servers** list, right-click an object, point to **View**, and then select a type to view: **All Users**, **All Groups**, **All Organizational Units**, or **All Computers**.

   Note: If the search is taking too long, click **Stop**.

   The **View** window opens and the selected types display. Right-click an item to access the shortcut menu.

   Note: If you make any changes via the shortcut menus, click **Refresh**.



Path: LDAP://vm4-win2ksvr.acme.com/CN=Users,DC=acme,DC=com

Name	Type	Created
Domain Computers	Security Group - Global	7/16/2004 9:32 AM
Domain Controllers	Security Group - Global	7/16/2004 9:32 AM
Schema Admins	Security Group - Global	7/16/2004 9:32 AM
Enterprise Admins	Security Group - Global	7/16/2004 9:32 AM
Cert Publishers	Security Group - Global	7/16/2004 9:32 AM
Domain Admins	Security Group - Global	7/16/2004 9:32 AM
Domain Users	Security G	7/16/2004 9:32 AM
Domain Guests	Security Group - Global	9:32 AM
Group Policy Creator Owners	Security Group - Global	9:32 AM
RAS and IAS Servers	Security Group - Domain	9:32 AM
DnsAdmins	Security Group - Domain	9:33 AM
DnsUpdateProxy	Security Group - Global	9:33 AM
AA_Admin	Security Group - Domain Local	5/5/2005 10:49 AM
AA_User	Security Group - Domain Local	5/5/2005 10:49 AM
ESR_Administrator	Security Group - Domain Local	5/9/2005 9:27 AM
ESR_Reporter	Security Group - Domain Local	5/9/2005 9:27 AM

Processed 16 Groups in 0 Seconds

   The **Path** box displays the path to the selected object. To change the path to a different object, click ..., and then select a new path.

   - To print the list, click **Report List**. The **Report Preview** window displays the report, which you can view or print.
   - To go to the item, select an item in the list, and then click **Go to**. The **View** window closes and the selected item is highlighted in the **Managed Servers** list and its permissions display in the **Object Permissions** area.

SEARCHING FOR ACTIVE DIRECTORY OBJECTS

Note: You cannot search for permissions on users, groups, OUs, or computers that are not included in the list of licensed OUs. If you select a user, group, OU, or computer that is not within the scope of your license, you see an error message. See *Resolving Licensing Issues*.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, expand the hierarchy, right-click the object to search, and then select **Find**. The **Find Users, Contacts, and Groups** dialog box opens.

   Note: You also can select an object in the **Container Objects** list, and then click **Find**.

3. From the **Find** list, select an object to find. Options are **Users, Contacts, and Groups**; **Computers**; **Printers**; **Shared Folders**; **Organizational Units**; **Custom Search**; or **SQL Server Publications**. The initial tab changes to reflect the object you selected.

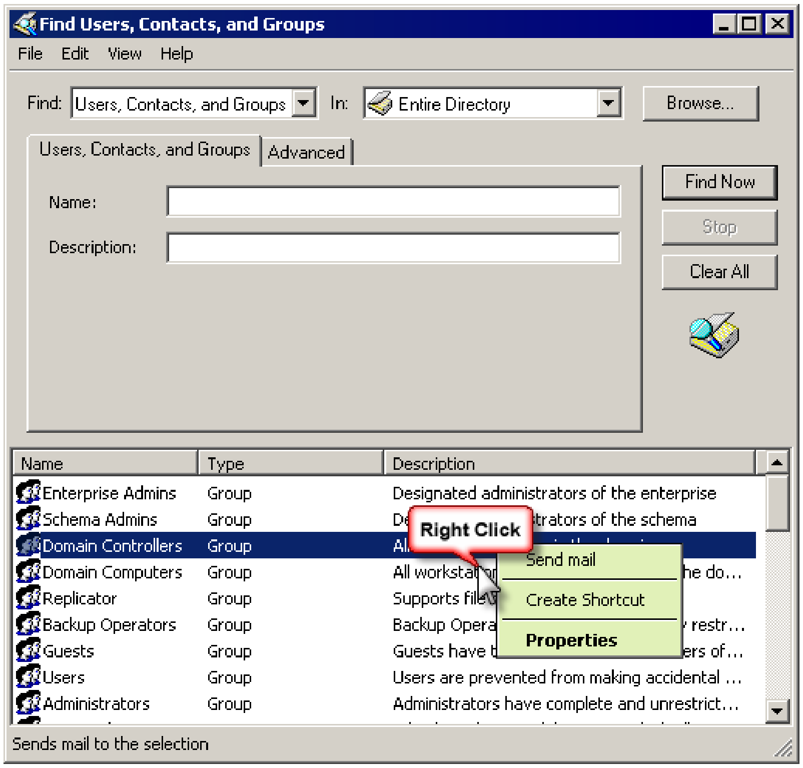
4. From the **In** list, select where to search. Options are **Entire Directory**, **Domain Controllers**, and any named domains in your system.

   Note: You also can click **Browse** to locate a search area.

5. Specify additional search criteria for the chosen object. The choice of tabs changes for each object. Open the other tabs to specify more detailed criteria.

   Note: To locate all items, leave all boxes blank.

6. To initiate the search, click **Find Now**. The results of the search display in the bottom pane. Right-click on an item to access a shortcut menu, which is different for each item type.



Find: Users, Contacts, and Groups
In: Entire Directory

Name:

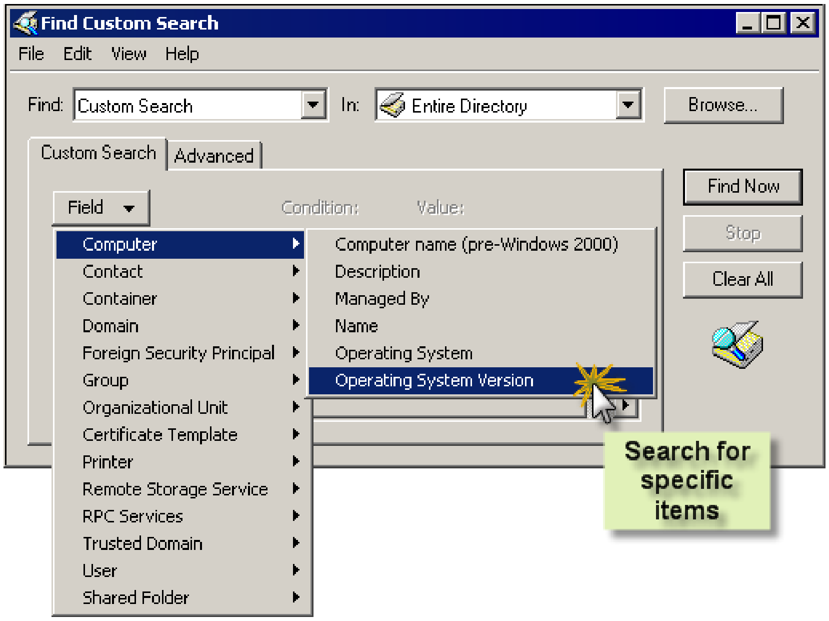
Description:

Name	Type	Description
Enterprise Admins	Group	Designated administrators of the enterprise
Schema Admins	Group	De trators of the schema
Domain Controllers	Group	Al
Domain Computers	Group	All workstat he do...
Replicator	Group	Supports file
Backup Operators	Group	Backup Opera restr...
Guests	Group	Guests have ers of...
Users	Group	Users are prevented from making accidental ...
Administrators	Group	Administrators have complete and unrestrict...

Sends mail to the selection

Creating Custom Searches

Opening the **Advanced** tab for an item, or selecting **Custom Search** allows you to select very specific search criteria. In addition to searching on a specific field, you can add a condition and a value. The **Advanced** tab for **Custom Search** lets you enter a LDAP query.



Search for specific items

SEARCHING FOR PERMISSIONS ON ACTIVE DIRECTORY OBJECTS

Active Administrator provides the ability to search your Active Directory environment for permissions on objects, which makes it possible to get a concise picture of where users may have directory access that is either too restrictive or too liberal. By default, all accounts, access types, generic rights, extended rights, and object classes are included in the search. By opening the various tabs, you can select to search for specific values.

Note: You cannot search for permissions on users, groups, OUs, or computers that are not included in the list of licensed OUs. If you select a user, group, OU, or computer that is not within the scope of your license, you see an error message. See *Resolving Licensing Issues*.

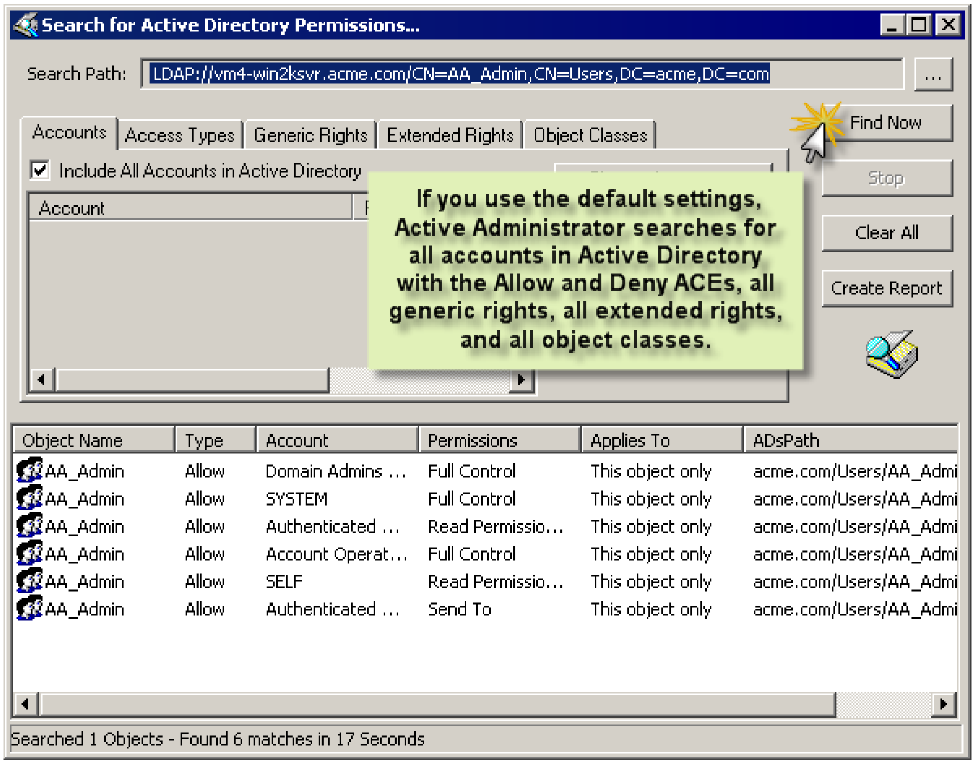
1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** or **Container Objects** list, right-click the object to search, and then choose **Find Permissions**. The **Search for Active Directory Permissions** dialog box opens to the **Accounts** tab.

   The **Search Path** box displays the path to the selected object. To change the search path, click ... and select a new path to search.

   Note: If you click **Find Now** without changing any settings, Active Administrator searches for all accounts in Active Directory with the Allow and Deny ACEs, all generic rights, all extended rights, and all object classes.

   Note: To stop a search that is taking too long, click **Stop**.

The results are listed in the lower pane. To produce a report for printing, click **Create Report**. To clear the results from the lower pane, click **Clear All**.



Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

☑ Include All Accounts in Active Directory

Account

If you use the default settings, Active Administrator searches for all accounts in Active Directory with the Allow and Deny ACEs, all generic rights, all extended rights, and all object classes.

Object Name	Type	Account	Permissions	Applies To	ADsPath
AA_Admin	Allow	Domain Admins ...	Full Control	This object only	acme.com/Users/AA_Admi
AA_Admin	Allow	SYSTEM	Full Control	This object only	acme.com/Users/AA_Admi
AA_Admin	Allow	Authenticated ...	Read Permissio...	This object only	acme.com/Users/AA_Admi
AA_Admin	Allow	Account Operat...	Full Control	This object only	acme.com/Users/AA_Admi
AA_Admin	Allow	SELF	Read Permissio...	This object only	acme.com/Users/AA_Admi
AA_Admin	Allow	Authenticated ...	Send To	This object only	acme.com/Users/AA_Admi

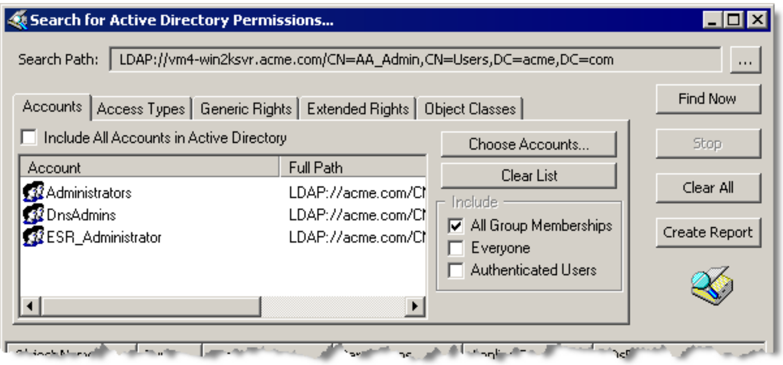
Searched 1 Objects - Found 6 matches in 17 Seconds

Searching by Account

If you want to limit the search to selected accounts, clear the **IncludeAll Accounts in Active Directory** check box, click **Choose Accounts**, and then select the accounts to include in the search.

The check boxes in the **Include** area are available only if you are searching for specific accounts. When you select these check boxes, the accounts are added to the list.

Note: To remove the accounts from the list, click **Clear List**.



Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

☐ Include All Accounts in Active Directory

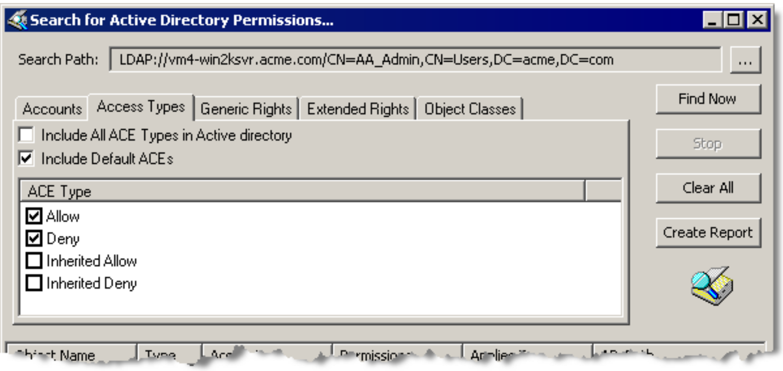
Account	Full Path
Administrators	LDAP://acme.com/Cl
DnsAdmins	LDAP://acme.com/Cl
ESR_Administrator	LDAP://acme.com/Cl

Include
☑ All Group Memberships
☐ Everyone
☐ Authenticated Users

Searching by Access Type

By default, the Allow and Deny ACE types are included in the search. To use only specific ACEs in the search, open the **Access Types** tab, and then select the ACEs to include in the search.

If you select the **Include All ACE Types in Active directory** check box, all four check boxes are selected and become unavailable.



Search for Active Directory Permissions...

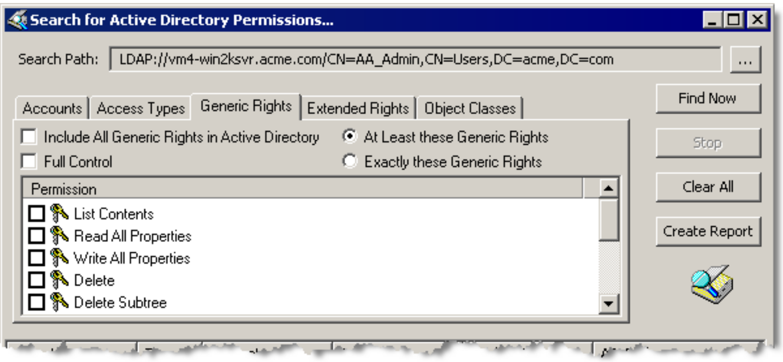
Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

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

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

Searching by Generic Rights

By default, all generic rights are included in the search. To use only specific rights in the search, open the **Generic Rights** tab, clear the **Include All Generic Rights in Active Directory** check box, and then select the specific generic rights.



Search for Active Directory Permissions...

Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

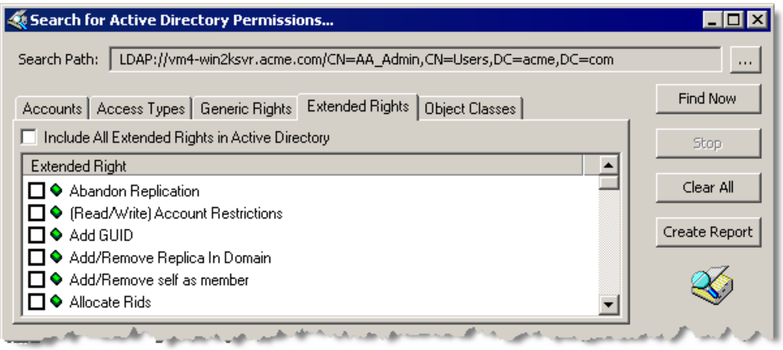
□ Include All Generic Rights in Active Directory
□ Full Control

● At Least these Generic Rights
○ Exactly these Generic Rights

Permission
□ List Contents
□ Read All Properties
□ Write All Properties
□ Delete
□ Delete Subtree

Searching by Extended Rights

By default all extended rights are included in the search. To use only specific rights in the search, open the **Extended Rights** tab, clear the **Include All Extended Rights in Active Directory** check box, and then select the specific extended rights.



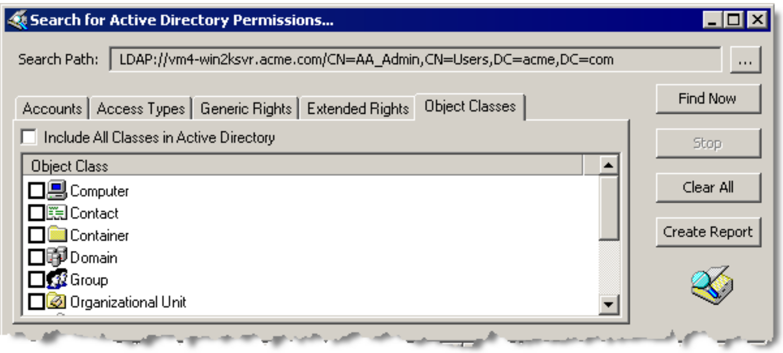
Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

□ Include All Extended Rights in Active Directory

Extended Right
- □ Abandon Replication
- □ (Read/Write) Account Restrictions
- □ Add GUID
- □ Add/Remove Replica In Domain
- □ Add/Remove self as member
- □ Allocate Rids

Searching by Object Classes

By default all classes are included in the search. To use only specific classes in the search, open the **Object Classes** tab, clear the **Include All Classes in Active Directory** check box, and then select the specific classes.



Search Path: LDAP://vm4-win2ksvr.acme.com/CN=AA_Admin,CN=Users,DC=acme,DC=com

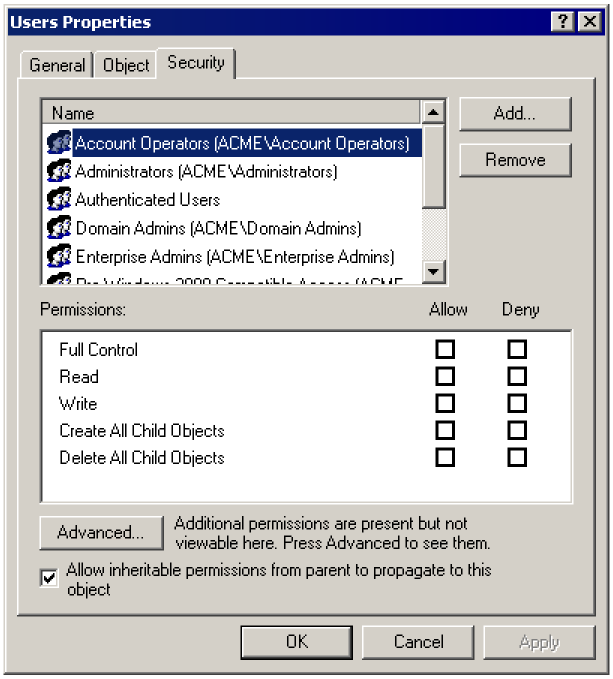
□ Include All Classes in Active Directory

Object Class
- □ Computer
- □ Contact
- □ Container
- □ Domain
- □ Group
- □ Organizational Unit

MODIFYING PERMISSIONS ON ACTIVE DIRECTORY OBJECTS

Note: Before modifying permissions, it is recommended to back up the security settings. See *Backing Up Security*.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Object Permissions** list, double-click an account. The **Properties** dialog box opens to the **Security** tab.



Name

- Account Operators (ACME\Account Operators)
- Administrators (ACME\Administrators)
- Authenticated Users
- Domain Admins (ACME\Domain Admins)
- Enterprise Admins (ACME\Enterprise Admins)
- Pre-Windows 2000 Compatible Access (ACME

Permissions:	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□

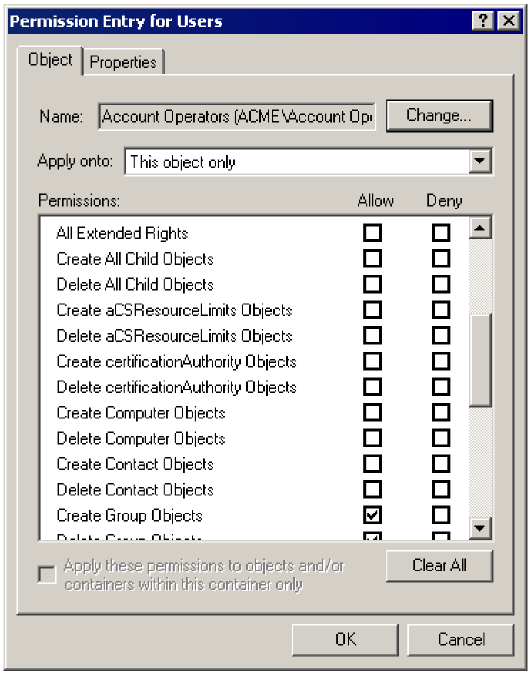
Additional permissions are present but not viewable here. Press Advanced to see them.

☑ Allow inheritable permissions from parent to propagate to this object

Note: You also can access the **Security** tab of the **Properties** dialog box by one of these other methods:

- In the **Managed Servers** or **Container Objects** list, right-click an object, and then choose **Properties**. The **Properties** dialog box opens to the **General** tab. Open the **Security** tab.
- In the **Object Permissions** list, right-click an account, and then choose **Modify Permissions**. The **Properties** dialog box opens to the **Security** tab.

3. Modify the permissions that display, or click **Advanced**, and then click **View/Edit**. The **Permission Entry** dialog box opens.



Permission Entry for Users

Name: Account Operators (ACME\Account Op

Apply onto: This object only

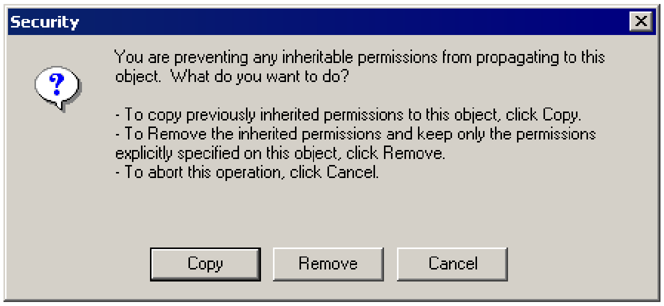
Permissions:	Allow	Deny
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create aCSResourceLimits Objects	□	□
Delete aCSResourceLimits Objects	□	□
Create certificationAuthority Objects	□	□
Delete certificationAuthority Objects	□	□
Create Computer Objects	□	□
Delete Computer Objects	□	□
Create Contact Objects	□	□
Delete Contact Objects	□	□
Create Group Objects	☑	□

□ Apply these permissions to objects and/or containers within this container only

By default, permissions are propagated from parent to child. To disallow propagation to the selected object, clear the **Allow inheritable permissions from parent to propagate to this object** check box.

Disallow Propagation

Clear the **Allow inheritable permissions from parent to propagate to this object** check box. A message box appears.



Security

You are preventing any inheritable permissions from propagating to this object. What do you want to do?

- To copy previously inherited permissions to this object, click Copy.
- To Remove the inherited permissions and keep only the permissions explicitly specified on this object, click Remove.
- To abort this operation, click Cancel.

- To add the formerly inherited permissions as explicitly defined permissions, click **Copy**.
- To remove the inheritable permissions from the object, click **Remove**.

Re-establish Propagation

Select the **Allow inheritable permissions from parent to propagate to this object** check box. A message box displays for confirmation. Click **Yes**.

DELEGATING CONTROL USING AN ACTIVE TEMPLATE

Note: You can delegate control from the **Active Templates** tab also. See *Delegating Control Using an Active Template*.

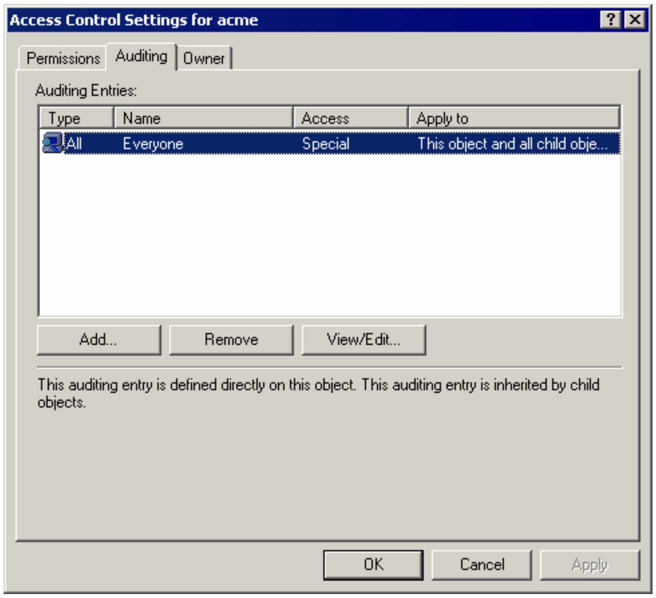
Note: You cannot delegate, manage, or view the delegated permission report of Active Templates on any object that is not included in the list of licensed OUs. An error message displays. The only operation you can perform on Active Templates while an unlicensed object is selected is to create an Active Template. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

1. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
2. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
3. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.
4. Open the **Auditing** tab.



Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

5. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
6. From the **Apply onto** list, select **This object and all child objects,** if necessary.
7. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

   ☑ **Write All Properties**

   ☑ **Delete**

   ☑ **Delete Subtree**

   ☑ **Modify Permissions**

   ☑ **Modify Owner**

   ☑ **All Validated Writes**

   ☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

   ☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

   Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

8. Open the **Properties** tab.
9. From the **Apply onto** list, select **This object and all child objects,** if necessary.
10. In the **Access** list, select the **Successful** checkboxes for the following:

    ☑ **Write All Properties**

    ☑ **Write Description**

    ☑ **Write flags**

    ☑ **Write gPLink**

    ☑ **Write gPOptions**

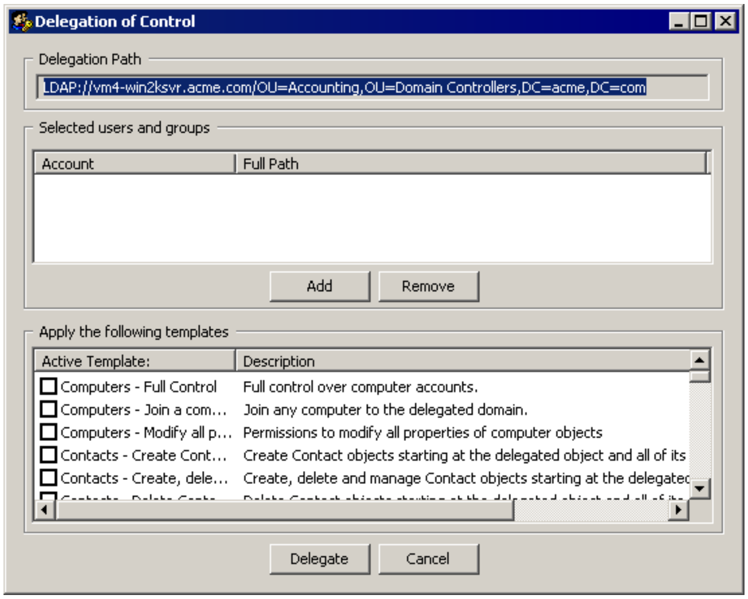
    ☑ **Write managedBy**

    Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

11. Click **OK.**

Resolving Licensing Issues.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, right-click the OU to delegate, point to **Active Templates**, and then choose **Delegate Control**. The **Delegation of Control** dialog box displays the LDAP path to the OU in the **Delegation Path** box.



Delegation Path

LDAP://vm4-win2ksvr.acme.com/OU=Accounting,OU=Domain Controllers,DC=acme,DC=com

Selected users and groups

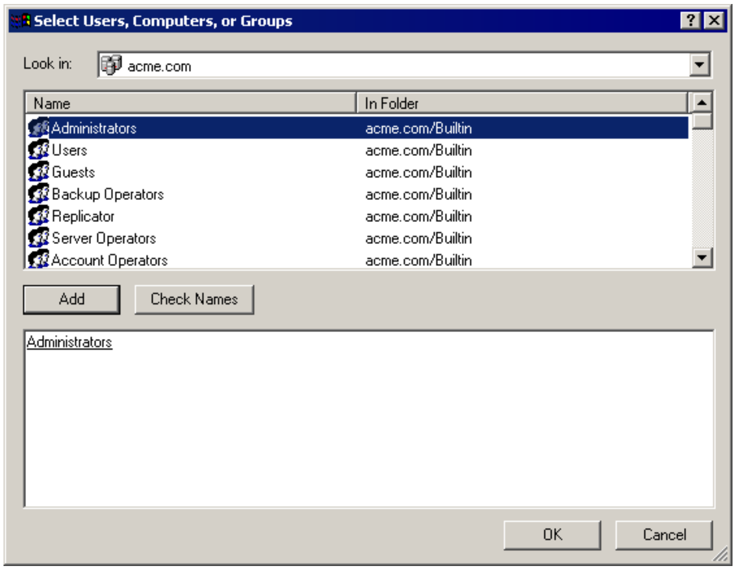
Account	Full Path

Apply the following templates

Active Template:	Description
□ Computers - Full Control	Full control over computer accounts.
□ Computers - Join a com…	Join any computer to the delegated domain.
□ Computers - Modify all p…	Permissions to modify all properties of computer objects
□ Contacts - Create Cont…	Create Contact objects starting at the delegated object and all of its
□ Contacts - Create, dele…	Create, delete and manage Contact objects starting at the delegatec

3. In the **Selected User and Groups** area, click **Add**. The **Select Users, Computers, or Groups** box displays the users, computers, and groups for the current domain.

4. Select the users, computers, and/or groups, click **Add**. The selected item appears in the bottom pane.



Look in: acme.com

Name	In Folder
Administrators	acme.com/Builtin
Users	acme.com/Builtin
Guests	acme.com/Builtin
Backup Operators	acme.com/Builtin
Replicator	acme.com/Builtin
Server Operators	acme.com/Builtin
Account Operators	acme.com/Builtin

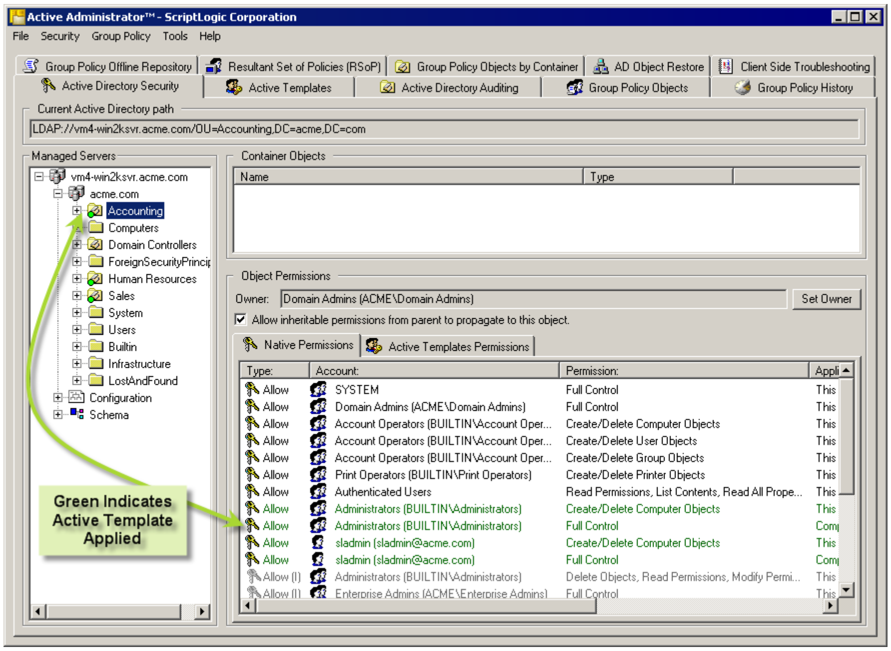
Administrators

5. Repeat step 4 to add more groups/users.

6. When you are finished adding groups/users, click **OK**. The **Delegation of Control** dialog box displays the selections in the **Selected users and groups** area.

7. In the **Apply the following templates** area, select the templates to apply, and then click **Delegate**. Each selected template is applied to each account at the selected path.

   A green dot displays next to the object. The green dot indicates all permissions in the Active Template are intact. Permissions associated with Active Templates display in green.



Current Active Directory path: LDAP://vm4-win2ksvr.acme.com/OU=Accounting,DC=acme,DC=com

Object Permissions

Owner: Domain Admins (ACME\Domain Admins)

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

Type:	Account:	Permission:	Appli
Allow	SYSTEM	Full Control	This
Allow	Domain Admins (ACME\Domain Admins)	Full Control	This
Allow	Account Operators (BUILTIN\Account Oper...	Create/Delete Computer Objects	This
Allow	Account Operators (BUILTIN\Account Oper...	Create/Delete User Objects	This
Allow	Account Operators (BUILTIN\Account Oper...	Create/Delete Group Objects	This
Allow	Print Operators (BUILTIN\Print Operators)	Create/Delete Printer Objects	This
Allow	Authenticated Users	Read Permissions, List Contents, Read All Prope...	This
Allow	Administrators (BUILTIN\Administrators)	Create/Delete Computer Objects	This
Allow	Administrators (BUILTIN\Administrators)	Full Control	Com
Allow	sladmin (sladmin@acme.com)	Create/Delete Computer Objects	This
Allow	sladmin (sladmin@acme.com)	Full Control	Com
Allow (I)	Administrators (BUILTIN\Administrators)	Delete Objects, Read Permissions, Modify Permi...	This
Allow (I)	Enterprise Admins (ACME\Enterprise Admins)	Full Control	This

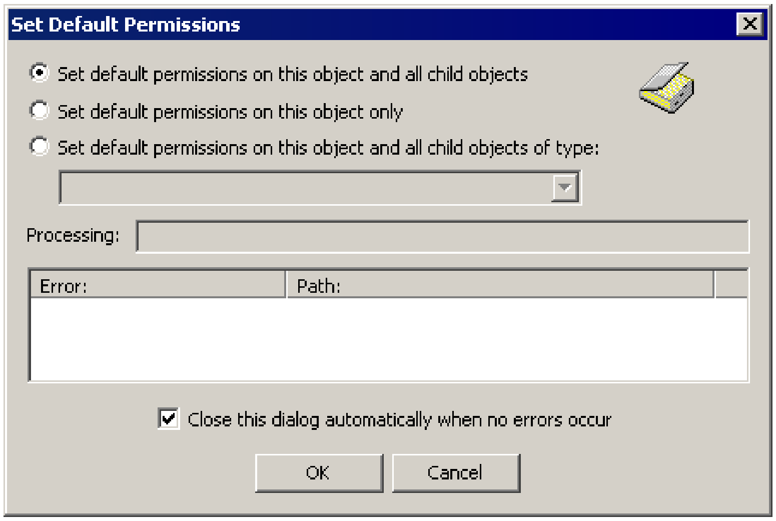
Green Indicates Active Template Applied

Note: If you wish to add domain controllers from other domains, repeat the above process from steps 4 through 6 until you have selected all of the domain controllers that you wish to manage.

RESTORING DEFAULT PERMISSIONS ON ACTIVE DIRECTORY OBJECTS

You can restore the default permissions on an Active Directory object and all or none of its child objects. You also can choose to apply the default permissions to an entire type of Active Directory object, such as contact, computer, group, organizational unit, or user.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, right-click a container, and then select **Set to Default Permissions**. The **Set Default Permissions** dialog box appears.



● Set default permissions on this object and all child objects

○ Set default permissions on this object only

○ Set default permissions on this object and all child objects of type:

Processing:

Error:	Path:

☑ Close this dialog automatically when no errors occur

3. Select how to apply the default permissions.

● **..Set default permissions on this object and all child objects**
Sets default permissions starting at the selected object and includes all child objects (default).

● **Set default permissions on this object only**
Sets default permissions only on the selected object.

● **Set default permissions on this object and all child objects of type**
Sets default permissions on the selected object and all child objects of the same type.

Note: If you want the dialog box to remain open even if no errors occur during processing, clear the **Close this dialog automatically when no errors occur** check box

4. Click **OK**. Errors that occur during processing are listed along with the path to the object causing the error.

MOVING ACTIVE DIRECTORY OBJECTS

Note: Objects are moved immediately without confirmation. To test the move, perform a what-if scenario on the **Resultant Set of Polices (RSoP)** tab. See *Resultant Set of Policies (RSoP)*.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, right-click an object, and then choose **Move**. The **Move** list box opens.
3. Choose the container where you want to relocate the selected object, and then click **OK**.

CREATING NEW ACTIVE DIRECTORY OBJECTS

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Servers** list, right-click a container, point to **New**, and then choose an object type. Options are **Computer**, **Contact**, **Group**, **Organizational Unit**, **Printer**, **Shared Folde**r, **User**, and **User (Copy From...)**.

   Note: To create a new user using other accounts as a template, which can be useful during large account roll-outs where uniformity is a must, choose **User (Copy From...)**.

3. In the box that appears, define the object, and then click **OK**.

REPORTING ON ACTIVE DIRECTORY OBJECTS

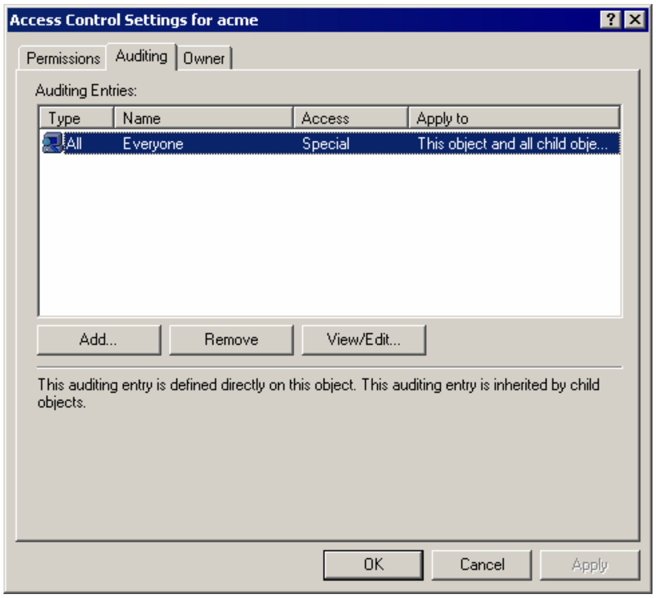
Note: You cannot view reports on users, groups, OUs, or computers that are not included in the list of licensed OUs. If you select a user, group, OU, or computer that is not within the scope of your license, you see an error message. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

12. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
13. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
14. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.
15. Open the **Auditing** tab.



Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

16. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
17. From the **Apply onto** list, select **This object and all child objects,** if necessary.
18. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Delete**

☑ **Delete Subtree**

☑ **Modify Permissions**

☑ **Modify Owner**

☑ **All Validated Writes**

☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

19. Open the **Properties** tab.
20. From the **Apply onto** list, select **This object and all child objects,** if necessary.
21. In the **Access** list, select the **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Write Description**

☑ **Write flags**

☑ **Write gPLink**

☑ **Write gPOptions**

☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

22. Click **OK.**

Resolving Licensing Issues.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. In the **Managed Server** list, right-click the object or container, and point to **Reports**. There are three reports from which to choose.

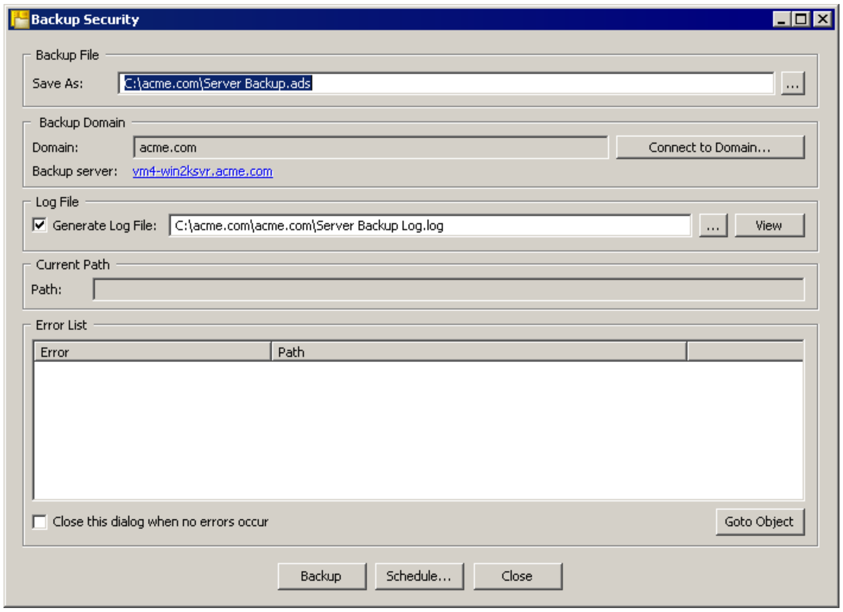
Report	**Description**
Object Class Summary	Lists the number of objects in a particular class in the selected container and all subcontainers
Delegated Permissions	Lists delegated permissions for the object and all child objects
Active Templates Delegated Permissions	Lists the Active Template applied to the selected object

Note: If you choose either the **Object Class Summary** or **Delegated Permissions** reports, a confirmation of the report and the path to be reported on appears. To display the report, click **Report**.

BACKING UP SECURITY

1. From the **Security** menu, choose **Backup**. The **Backup Security** dialog box opens.
2. In the **Save As** box, type the path to the Active Administrator Security Backup file (*.ads) where you want to store the backup, or click ... to locate and name a file.
3. To select a domain, click **Connect to Domain**, and then choose the domain.
4. To create a log file for the backup process, select the **Generate Log File** check box, and then type the name of the .log file, or click ... to locate a file.

   Note: To view a log file displayed in the box, click **View**.



Save As: C:\acme.com\Server Backup.ads

Domain: acme.com

Backup server: vm4-win2ksvr.acme.com

☑ Generate Log File: C:\acme.com\acme.com\Server Backup Log.log

☐ Close this dialog when no errors occur

   Note: To schedule the backup, click **Schedule**. See *Scheduling a Backup*.

5. To initiate the backup, click **Backup**. When the backup is complete, a message box appears. The **Path** box displays the number of items processed and the current path. Any errors display in the **Error List** box.
6. If you selected the **Close this dialog when no errors occur** check box, the dialog box closes automatically. Otherwise, click **Close** to close the dialog box.

   Note: If an error occurs, you can go to the object by clicking **Goto Object**.

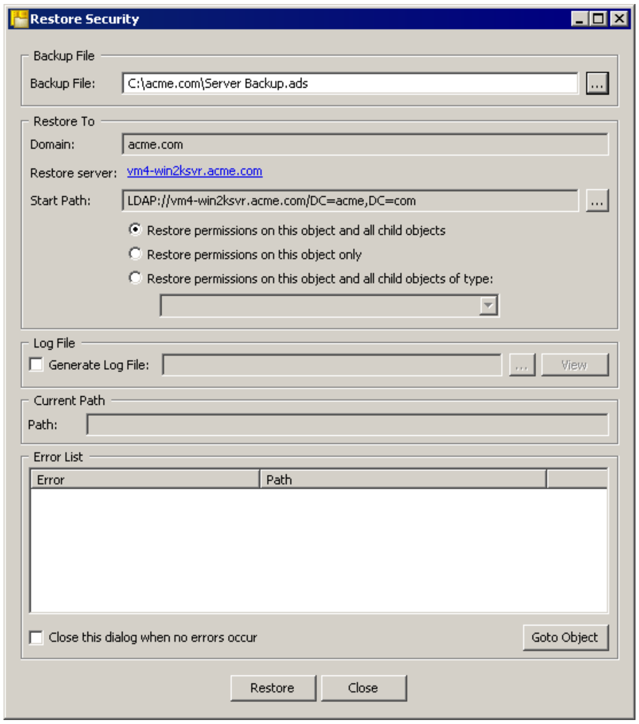
Scheduling a Backup

1. Click **Schedule**. The **Schedule a Backup job** box opens.
2. In the **Job Name** box, type a name for the copy job.
3. In the **Save Job in Folder** box, click ... and choose a folder in which to store the backup job.
4. Click **Schedule**. The Microsoft Windows scheduling service opens.
5. Schedule the backup job, and then click **OK**.

Note: To edit a previously scheduled backup job, click **Manage Schedule Jobs**. The **Scheduled Tasks** window opens where you can modify scheduled jobs.

RESTORING A SECURITY BACKUP

1. From the **Security** menu, choose **Restore**. The **Restore Security** dialog box opens.
2. In the **Backup File** box, type the path to the Active Administrator Security Backup File (*.ads) file or click ... to locate the file. The default domain and start path displays in the **Restore to** area.



Backup File: C:\acme.com\Server Backup.ads

Domain: acme.com

Restore server: vm4-win2ksvr.acme.com

Start Path: LDAP://vm4-win2ksvr.acme.com/DC=acme,DC=com

● 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:

☐ Generate Log File:

☐ Close this dialog when no errors occur

3. To change the start path, click ..., and then select a new object from which to start the restore process.
4. In the **Restore To** area, set options for the restore process.

   ◉ **Restore permissions on this object and all child objects**
   Restores permissions starting at the object specified in the **Start Path** box and includes all child objects (default).

   ◉ **Restore permissions on this object only**
   Restores permissions only on the object specified in the **Start Path** box.

   ◉ **Restore permissions on this object and all child objects of type**
   Restores permissions on the object specified in the **Start Path** box and all child objects of the same type.

5. To create a log file for the back up process, select the **Generate Log File** check box, and then type the name of the .log file or click ... to locate the file.

   Note: To view a log file displayed in the box, click **View**.

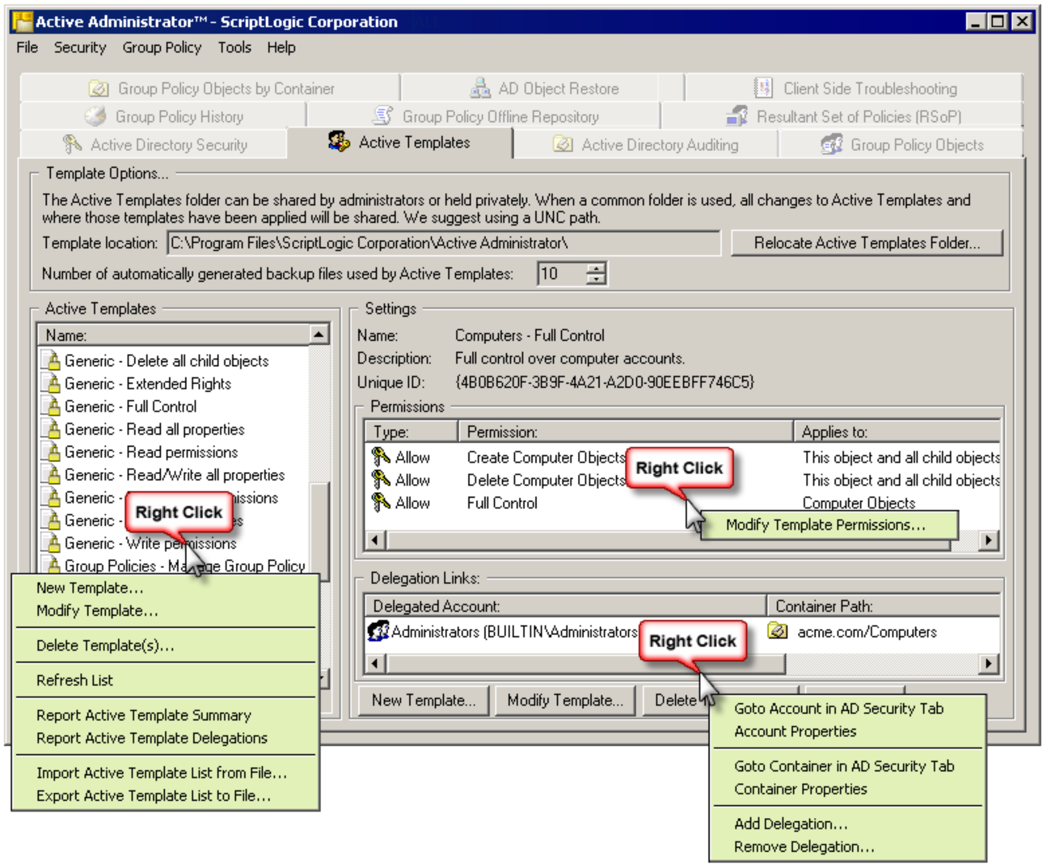
6. To initiate the restore process, click **Restore**. When the restore process is complete, a message box appears. The **Path** box displays the number of items processed and the current path. Any errors display in the **Error List** box.
7. If you selected the **Close this dialog when no errors occur** check box, the dialog box closes automatically. Otherwise, click **Close** to close the dialog box.

   Note: If an error occurs, you can go to the object by clicking **Goto Object**.

Active Templates

Active Templates in Active Administrator greatly expand on the limited Windows 2000 Delegation of Control wizard. These advanced templates allow administrators to quickly create and manage sets of permissions to be applied to objects in Active Directory. Unlike the Delegation of Control wizard, any changes made to security using Active Templates can be repaired or removed. Simple graphical indicators allow administrators to see where the templates are applied and their statuses. Custom templates can be made and standardized easily.

Using Active Templates, even for simple permission modification, provides powerful features to ensure those permissions remain intact. Take granting full control for instance. It isn't difficult to grant full control using the built in tools. What if someone deletes that permission? You won't know until someone complains that they can't get access to the specific object. Even using a simple Full Control Active Template can be very useful in the sense that you can determine where that access has been removed or broken.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Relocate Active Templates Folder...
Right Click
Right Click
Right Click
Modify Template Permissions...
New Template...
Modify Template...
Delete Template(s)...
Refresh List
Report Active Template Summary
Report Active Template Delegations
Import Active Template List from File...
Export Active Template List to File...
Goto Account in AD Security Tab
Account Properties
Goto Container in AD Security Tab
Container Properties
Add Delegation...
Remove Delegation...
New Template...
Modify Template...
Delete

Template Options...

The Active Templates folder can be shared by administrators or held privately. When a common folder is used, all changes to Active Templates and where those templates have been applied will be shared. We suggest using a UNC path.

Template location: C:\Program Files\ScriptLogic Corporation\Active Administrator\

Number of automatically generated backup files used by Active Templates: 10

Active Templates

Name:
Generic - Delete all child objects
Generic - Extended Rights
Generic - Full Control
Generic - Read all properties
Generic - Read permissions
Generic - Read/Write all properties
Generic - ...issions
Generic - ...s
Generic - Write permissions
Group Policies - Manage Group Policy

Settings

Name: Computers - Full Control
Description: Full control over computer accounts.
Unique ID: {4B0B620F-3B9F-4A21-A2D0-90EEBFF746C5}

Permissions

Type:	Permission:	Applies to:
Allow	Create Computer Objects	This object and all child objects
Allow	Delete Computer Objects	This object and all child objects
Allow	Full Control	Computer Objects

Delegation Links:

Delegated Account:	Container Path:
Administrators (BUILTIN\Administrators)	acme.com/Computers

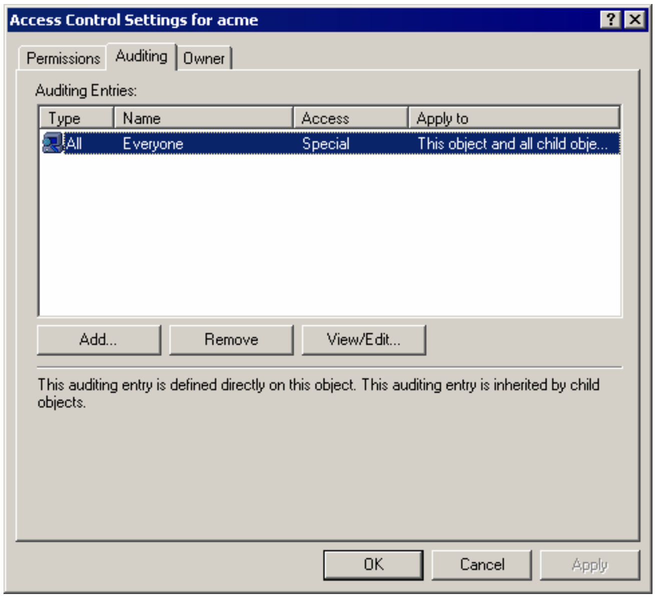
Note: You cannot delegate, manage, or view the delegated permission report of Active Templates on any object that is not included in the list of licensed OUs. An error message displays. The only operation you can perform on Active Templates while an unlicensed object is selected is to create an Active Template. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

23. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
24. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
25. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.
26. Open the **Auditing** tab.



Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

27. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
28. From the **Apply onto** list, select **This object and all child objects,** if necessary.
29. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Delete**

☑ **Delete Subtree**

☑ **Modify Permissions**

☑ **Modify Owner**

☑ **All Validated Writes**

☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

30. Open the **Properties** tab.
31. From the **Apply onto** list, select **This object and all child objects,** if necessary.
32. In the **Access** list, select the **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Write Description**

☑ **Write flags**

☑ **Write gPLink**

☑ **Write gPOptions**

☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

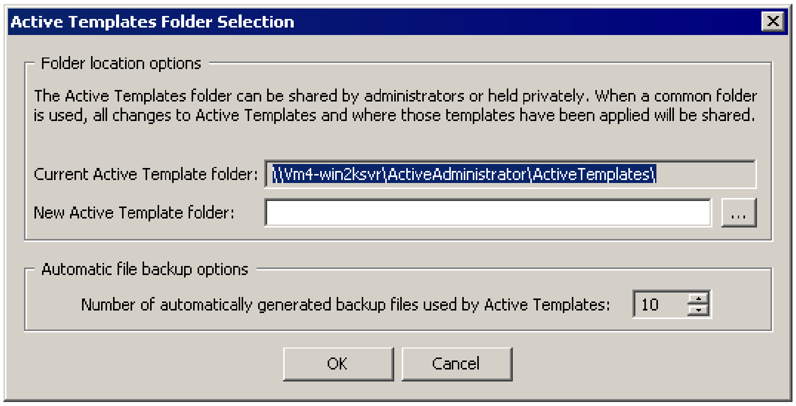
33. Click **OK.**

Resolving Licensing Issues.

SETTING ACTIVE TEMPLATE OPTIONS

The **Template Options** area of the **Active Template** tab displays the path to the Active Templates folder and the number of automatically generated backup files used by Active Templates.

▶ To change Active Template options, click **Relocate Active Templates Folder**. The **Active Templates Folder Selection** box displays the path to the current Active Templates folder.



Active Templates Folder Selection

Folder location options

The Active Templates folder can be shared by administrators or held privately. When a common folder is used, all changes to Active Templates and where those templates have been applied will be shared.

Current Active Template folder: \\Vm4-win2ksvr\ActiveAdministrator\ActiveTemplates\

New Active Template folder:

Automatic file backup options

Number of automatically generated backup files used by Active Templates: 10

- To use a different Active Template folder, type the path to the new location or click ..., locate the folder, and then click **OK**.

- To change the number of backup options, select a number from the list, and then click **OK**.

CREATING AN ACTIVE TEMPLATE

1. From the Active Administrator Console, open the **Active Templates** tab.

2. Click **New Template** or right-click a template in the Active Templates list, and then select **New Template**. The **Create a new Active Template** window opens.

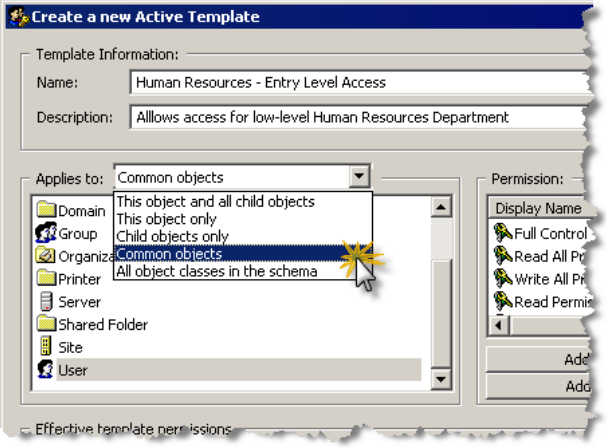
   Note: You also can create a new template on the **Active Directory** tab. In the **Managed Servers** list, right click the object, point to **Active Templates**, and then choose **Create Template**.

3. In the **Template Information** area, type a name and description for the new Active Template.

4. From the **Applies to** drop-down list, choose how apply the template security. You can select common object types, all object types on the system, or an inheritance level.

   When selecting an inheritance level such as **This object and all child objects**, **This object only**, or **Child objects only**, you can select the permissions available to domains, organizational units, containers, and sites, which are the common objects that truly utilize the Active Directory inheritance model for permissions.

   The **Applies to** list shows common object types or all object types. If you are adding an access right based on the Active Directory inheritance model, this list is disabled.



Create a new Active Template

Template Information:

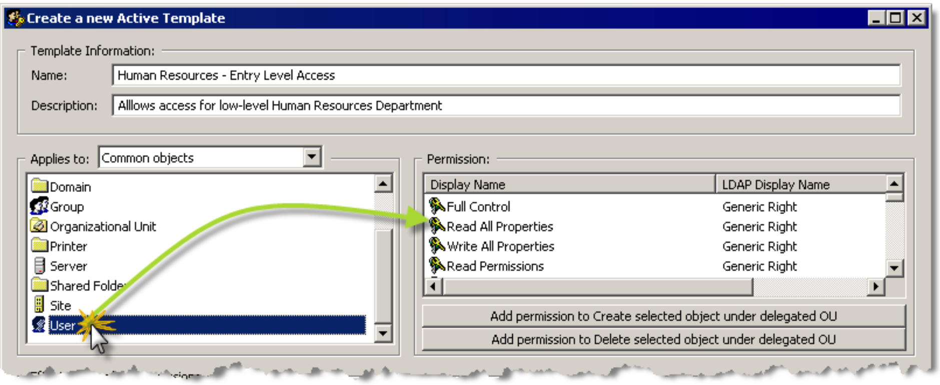
Name: Human Resources - Entry Level Access

Description: Alllows access for low-level Human Resources Department

Applies to: Common objects

5. In the **Applies to** list, select the object.

   The **Permission** list displays all permissions specific to the object type you selected in the **Applies to** list. In the case of **This object and all child objects**, **This object only**, or **Child objects only**, the list reflects all permissions available to domains, organizational units, containers, and sites. This list includes all generic rights, extended rights, property rights and the ability to create and/or delete child objects of these classes.



Create a new Active Template

Template Information:

Name: Human Resources - Entry Level Access

Description: Allows access for low-level Human Resources Department

Applies to: Common objects

Permission:

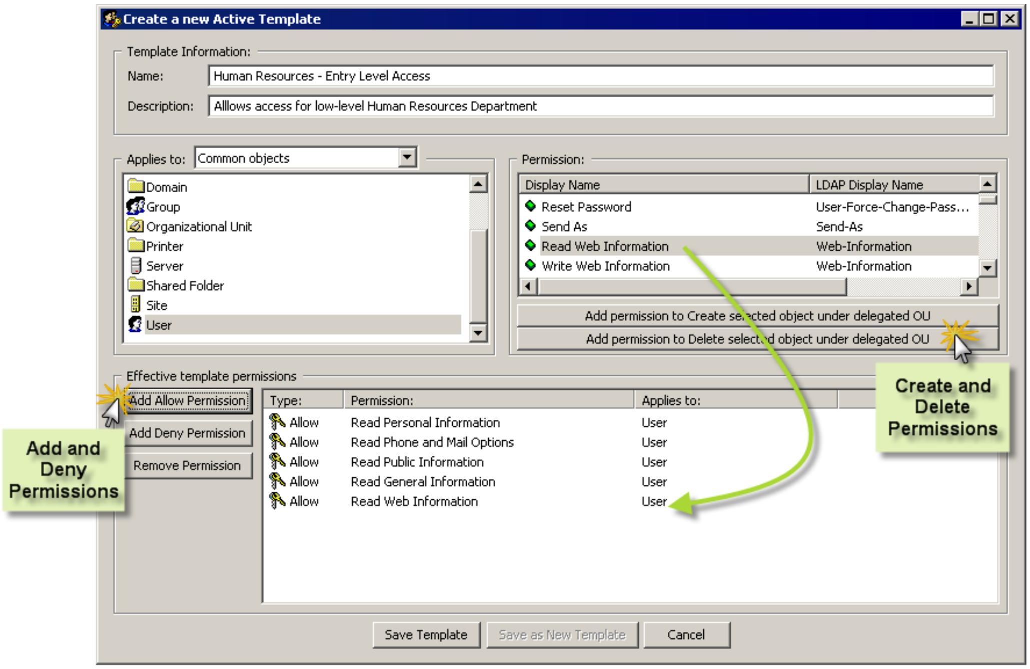
Display Name	LDAP Display Name
Full Control	Generic Right
Read All Properties	Generic Right
Write All Properties	Generic Right
Read Permissions	Generic Right

Add permission to Create selected object under delegated OU
Add permission to Delete selected object under delegated OU

6. In the **Permissions** list, select the security to apply to the selected object, and then click a button to apply the permission.

Button	Description
Add permission to Create selected object under delegated OU	Adds a create permission for the selected object
Add permission to Delete selected object under delegated OU	Adds a delete permission for the selected object
Add Allow Permission	Adds an allow permission for the selected object
Add Deny Permission	Adds a deny permission for the selected object
Remove Permission	Removes a selected permission from the list

The **Effective template permissions** area lists the selected permissions. To remove a permission from the list, click **Remove Permission**.



Create a new Active Template

Template Information:

Name: Human Resources - Entry Level Access

Description: Allows access for low-level Human Resources Department

Applies to: Common objects

Permission:

Display Name	LDAP Display Name
Reset Password	User-Force-Change-Pass…
Send As	Send-As
Read Web Information	Web-Information
Write Web Information	Web-Information

Add permission to Create selected object under delegated OU
Add permission to Delete selected object under delegated OU
Create and Delete Permissions
Add and Deny Permissions
Add Allow Permission
Add Deny Permission
Remove Permission

Effective template permissions

Type:	Permission:	Applies to:
Allow	Read Personal Information	User
Allow	Read Phone and Mail Options	User
Allow	Read Public Information	User
Allow	Read General Information	User
Allow	Read Web Information	User

7. Once you have the security set up for the template, click **Save Template**. The new template is listed in the **Active Templates** list in alphabetical order.

Note: You may need to click **Refresh List** to see the new Active Template in the list.

MODIFYING AN ACTIVE TEMPLATE

Active Administrator has several pre-defined Active Templates that you can use as a basis for creating new templates.

1. From the Active Administrator Console, open the **Active Templates** tab.
2. In the **Active Templates** list, double-click a template. The **Modify existing Active Template** window opens.

   Note: You also can right-click a template in the **Active Templates** list, and then choose **Modify Template**; select a template in the **Active Templates** list, and then click **Modify Template**; double-click a permission in the Permissions list; or right-click a permission in the **Permissions** list, and then choose **Modify Template Permissions**.

3. Make any changes to the permissions. See *Creating an Active Template*.
4. If you are creating a new template from an existing template, type a new name and description in the **Template Information** area.
5. To save the template, click **Save Template**. To save the template with a different name, click **Save as New Template**.

   Note: To save as a new template, you must change the template name in the **Name** box.

DELETING AN ACTIVE TEMPLATE

1. From the Active Administrator Console, open the **Active Templates** tab.
2. In the **Active Templates** list, select the template(s) to delete, right-click the selection, and then choose **Delete Template(s)**. A confirmation message box appears.

   Note: You also can select templates in the **Active Templates** list, and then click **Delete Template(s)**.

3. To delete the selected template(s), click **Yes**.

REPORTING ON ACTIVE TEMPLATES

Note: You also can run reports on Active Templates from the **Active Directory Security** tab. See *Reporting on Active Directory Objects*.

1. From the Active Administrator Console, open the **Active Templates** tab.
2. In the **Active Templates** list, right-click a template, and then select from these two reports:

Report	Description
Active Template Summary	Lists the accounts and associated permissions for each template
Active Template Delegations	Lists the delegation links for the current domain

DELEGATING CONTROL USING AN ACTIVE TEMPLATE

Note: You also can add delegations from the **Active Directory Security** tab. See *Delegating Control Using an Active Template*.

Note: You cannot delegate an Active Template to a list of paths or a single path if any selected object is not included in the list of licensed OUs. An error message displays and none of the objects are added. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

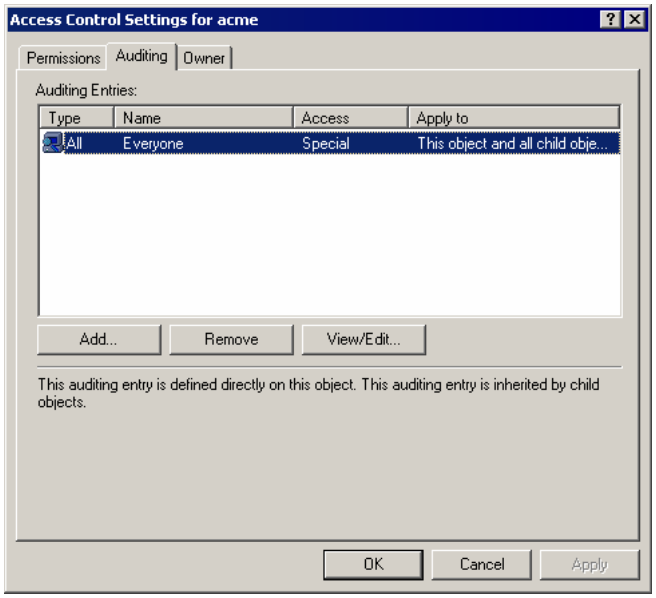
Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

34. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.

35. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.

36. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.

37. Open the **Auditing** tab.



Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

38. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
39. From the **Apply onto** list, select **This object and all child objects,** if necessary.
40. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

    ☑ **Write All Properties**

    ☑ **Delete**

    ☑ **Delete Subtree**

    ☑ **Modify Permissions**

    ☑ **Modify Owner**

    ☑ **All Validated Writes**

    ☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

    ☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

    Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

41. Open the **Properties** tab.
42. From the **Apply onto** list, select **This object and all child objects,** if necessary.
43. In the **Access** list, select the **Successful** checkboxes for the following:

    ☑ **Write All Properties**

    ☑ **Write Description**

    ☑ **Write flags**

    ☑ **Write gPLink**

    ☑ **Write gPOptions**

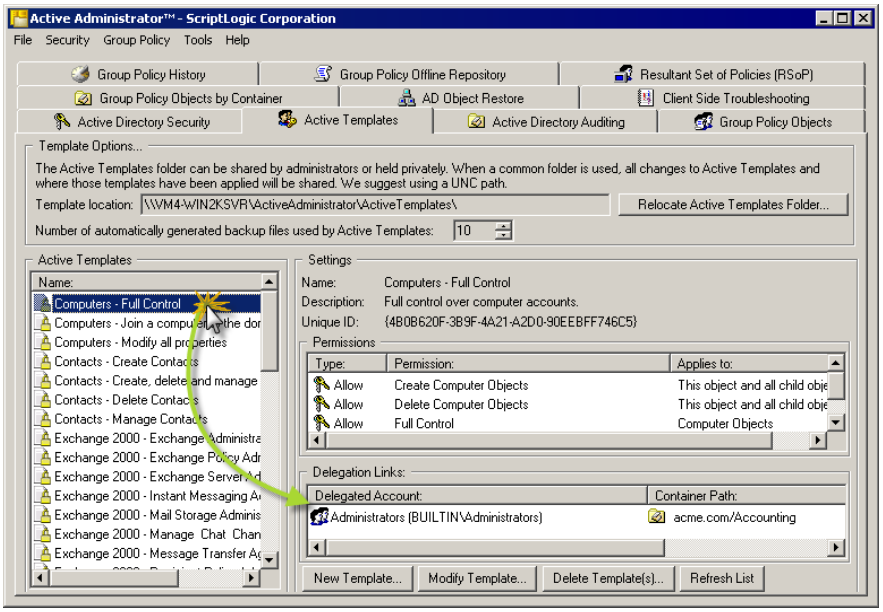
    ☑ **Write managedBy**

    Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

44. Click **OK.**

Resolving Licensing Issues.

1. From the Active Administrator Console, open the **Active Templates** tab.
2. In the **Active Templates** list, select an Active Template. Any delegated accounts for the selected Active Template display in the **Delegation Links** list.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Template Options...
Active Templates
Settings
Permissions
Delegation Links:
New Template...
Modify Template...
Delete Template(s)...
Refresh List
Relocate Active Templates Folder...

The Active Templates folder can be shared by administrators or held privately. When a common folder is used, all changes to Active Templates and where those templates have been applied will be shared. We suggest using a UNC path.

Template location: \\VM4-WIN2KSVR\ActiveAdministrator\ActiveTemplates\

Number of automatically generated backup files used by Active Templates: 10

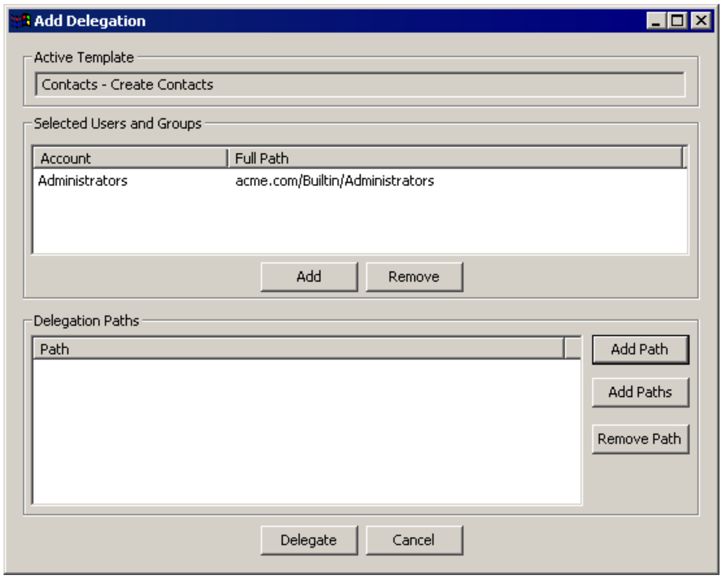
Name:
Computers - Full Control
Computers - Join a compu... the dor
Computers - Modify all properties
Contacts - Create Contacts
Contacts - Create, delete and manage
Contacts - Delete Contacts
Contacts - Manage Contacts
Exchange 2000 - Exchange Administra
Exchange 2000 - Exchange Policy Adr
Exchange 2000 - Exchange Server Ad
Exchange 2000 - Instant Messaging A
Exchange 2000 - Mail Storage Adminis
Exchange 2000 - Manage Chat Chan
Exchange 2000 - Message Transfer Ag

Name: Computers - Full Control
Description: Full control over computer accounts.
Unique ID: {4B0B620F-3B9F-4A21-A2D0-90EEBFF746C5}

Type:	Permission:	Applies to:
Allow	Create Computer Objects	This object and all child obje
Allow	Delete Computer Objects	This object and all child obje
Allow	Full Control	Computer Objects

Delegated Account:	Container Path:
Administrators (BUILTIN\Administrators)	acme.com/Accounting

3. In the **Delegations Links** list, right click anywhere in the box and then choose **Add Delegation**. The **Add Delegation** dialog box displays the selected Active Template.
4. In the **Selected Users and Groups** area, click **Add**, and then select the users or groups to include in the delegation.

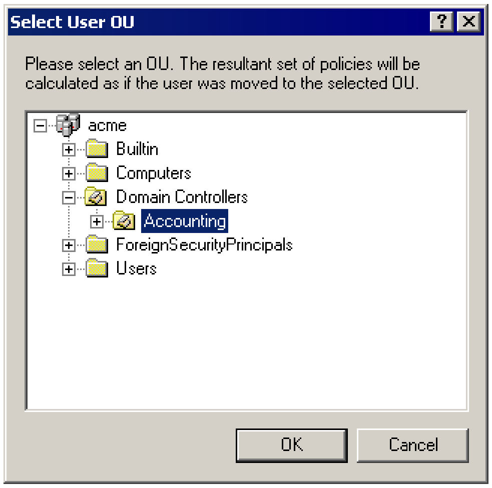


Active Template: Contacts - Create Contacts

Account	Full Path
Administrators	acme.com/Builtin/Administrators

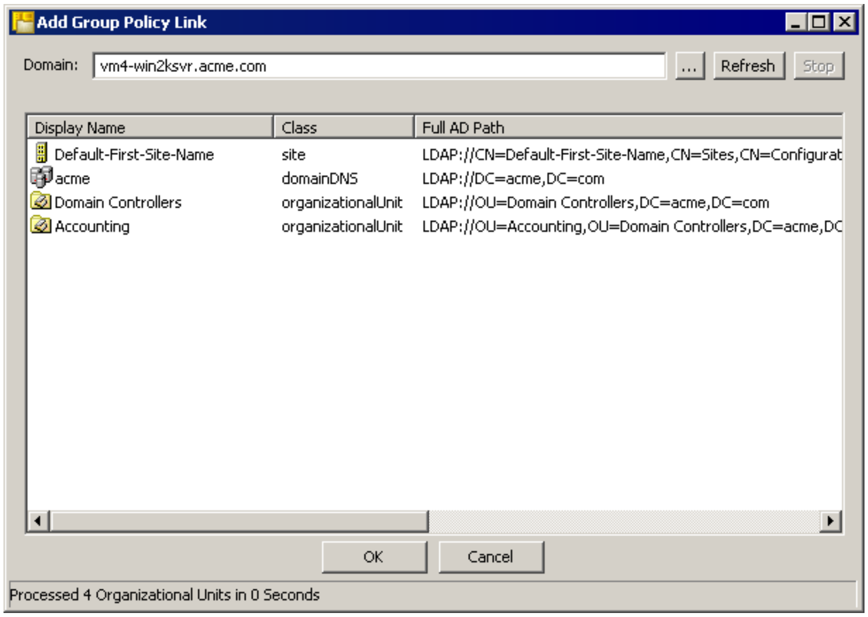
5. In the **Delegation Paths** area, click **Add Path** or **Add Paths** depending on whether you want to change domains or not.

- To browse the local domain to select an OU, click **Add Path**. The **Select User OU** box displays the local domain. Select an OU, and then click **OK**.



Please select an OU. The resultant set of policies will be calculated as if the user was moved to the selected OU.

- To browse all domains on the network and view the full LDAP path of the OU, click **Add Paths**. The **Group Policy Link** box displays the local domain. To change domains, click ... . You may need to click **Refresh** to view the OUs for the selected domain. Select one or more OUs, and then click **OK**.

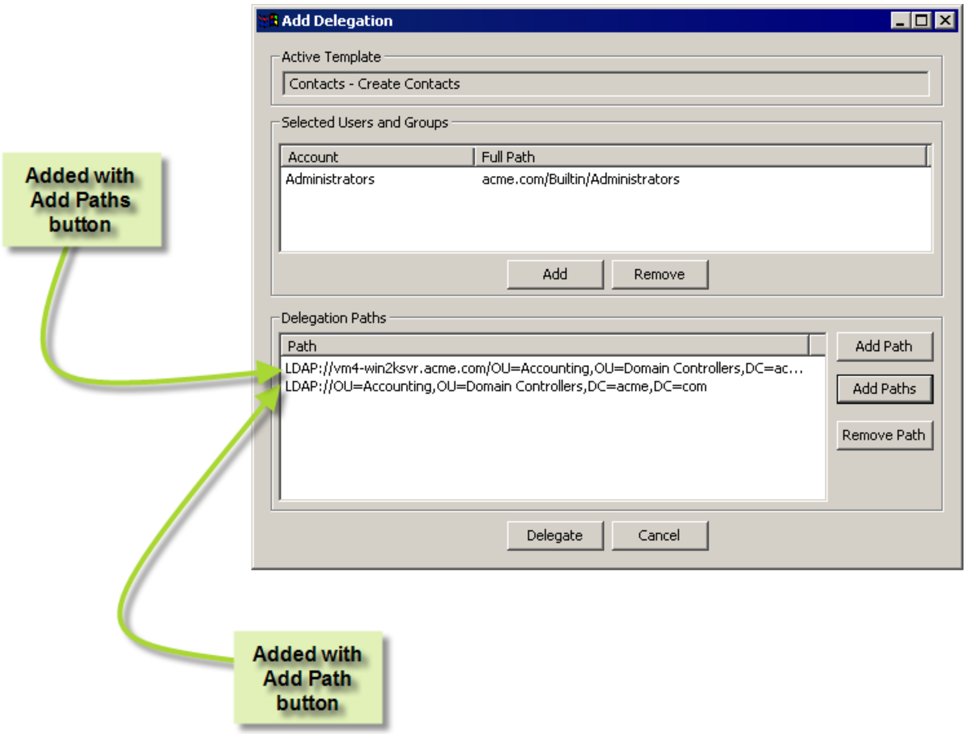


Domain: vm4-win2ksvr.acme.com

Display Name	Class	Full AD Path
Default-First-Site-Name	site	LDAP://CN=Default-First-Site-Name,CN=Sites,CN=Configurat
acme	domainDNS	LDAP://DC=acme,DC=com
Domain Controllers	organizationalUnit	LDAP://OU=Domain Controllers,DC=acme,DC=com
Accounting	organizationalUnit	LDAP://OU=Accounting,OU=Domain Controllers,DC=acme,DC

Processed 4 Organizational Units in 0 Seconds

6. Click **OK**. The **Add Delegation** box shows the delegated paths.



Active Template: Contacts - Create Contacts

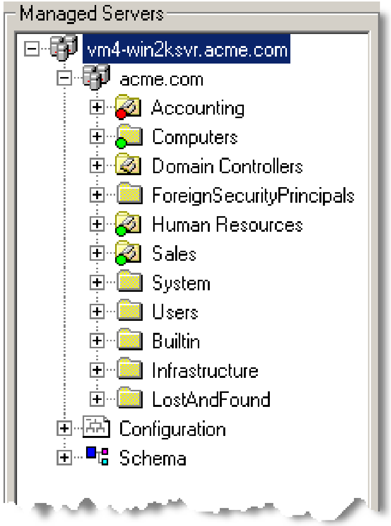
Account	Full Path
Administrators	acme.com/Builtin/Administrators

Path
LDAP://vm4-win2ksvr.acme.com/OU=Accounting,OU=Domain Controllers,DC=ac…
LDAP://OU=Accounting,OU=Domain Controllers,DC=acme,DC=com

7. When you are finished added OUs, click **Delegate**.

REPAIRING A BROKEN ACTIVE TEMPLATE

A green dot next to an object indicates that there is an applied Active Template. If you see a red dot, one or more of the permissions are missing at that location. Active Templates can easily be broken by someone modifying the permissions of an object through the Microsoft native tools. With Active Administrator, you quickly can repair a broken Active Template or delete it from the object.


Managed Servers

- vm4-win2ksvr.acme.com
  - acme.com
    - Accounting
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Human Resources
    - Sales
    - System
    - Users
    - Builtin
    - Infrastructure
    - LostAndFound
  - Configuration
  - Schema

Quick Repair

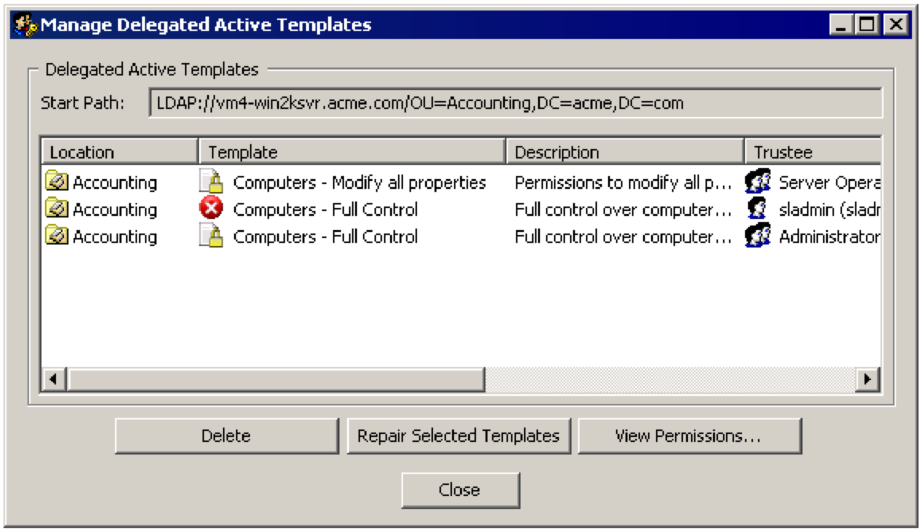
To quickly repair all broken Active Templates in an object, right-click the object in the **Managed Servers** list, point to **Active Templates**, and then choose **Repair All Broken Templates**.

This repairs all broken templates starting at the selected object and moving down all of its child objects.

Note: You can set up Active Administrator to fix broken Active Templates automatically. See *Configuring the Active Template Auto-Repair Service* in the *Getting Results Guide*.

1. From the Active Administrator Console, open the **Active Directory Security** tab.
2. Right-click an object in the **Managed Servers** list, point to **Active Templates**, and then choose **Manage Delegated Templates**. The **Manage Delegated Active Templates** list box displays all the delegated Active Templates for the current object.

   The red X indicates the permissions defined in the template and those defined for the object do not match.



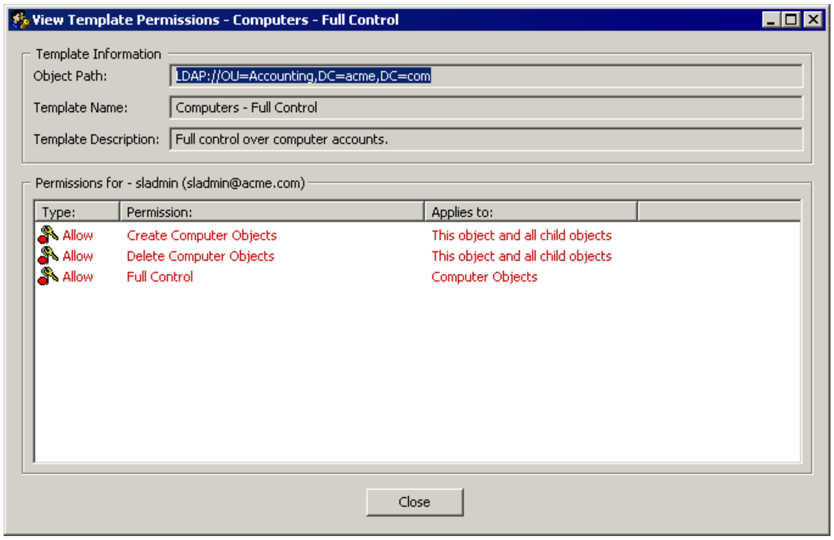
Manage Delegated Active Templates

Delegated Active Templates

Start Path: LDAP://vm4-win2ksvr.acme.com/OU=Accounting,DC=acme,DC=com

Location	Template	Description	Trustee
Accounting	Computers - Modify all properties	Permissions to modify all p...	Server Opera
Accounting	☒ Computers - Full Control	Full control over computer...	sladmin (sladr
Accounting	Computers - Full Control	Full control over computer...	Administrator

- To delete the delegated permissions, select the Active Template, and then click **Delete**. A confirmation message box appears. To delete the delegated permissions, click **Yes**.
- To reapply the permissions, select the Active Template, and then click **Repair Selected Templates**.
- To view the permissions, select an **Active Template**, and then click **View Permissions**. The **View Template Permissions** list box displays the permission that does not match in red. This permission was deleted from the object but still exists in the Active Template.



View Template Permissions - Computers - Full Control

Template Information

Object Path: LDAP://OU=Accounting,DC=acme,DC=com

Template Name: Computers - Full Control

Template Description: Full control over computer accounts.

Permissions for - sladmin (sladmin@acme.com)

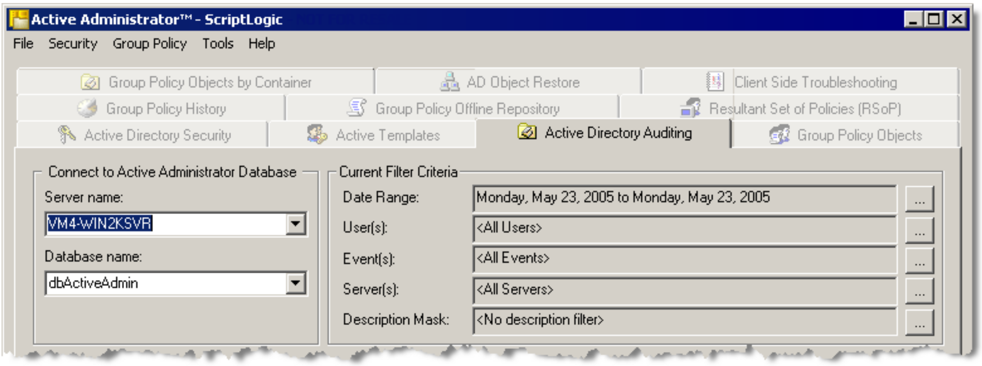
Type:	Permission:	Applies to:
Allow	Create Computer Objects	This object and all child objects
Allow	Delete Computer Objects	This object and all child objects
Allow	Full Control	Computer Objects

Active Directory Auditing

Active Administrator includes a security event monitoring service that notifies you of changes that occur to Active Directory. This service actively monitors the security event logs on each domain controller on which it is installed. Upon finding an event of interest, it sends the information to centralized Microsoft SQL 2000 Server and optionally generates an email alert to a predetermined address. See *Setting Event Notifications* in the *Getting Started Guide.*.

Note: The Active Directory security event monitoring service should already be configured and running. See *Setting Up Monitoring Services* in the *Getting Started Guide*.

1. From the Active Administrator Console, open the **Active Directory Auditing** tab.
2. From the **Server name** list, if necessary, select the server where the auditing dataset is located.
3. From the **Database name** list, if necessary, select the auditing database.


Active Administrator™ - ScriptLogic
File
Security
Group Policy
Tools
Help
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Connect to Active Administrator Database
Current Filter Criteria
...

Server name: VM4-WIN2KSVR

Database name: dbActiveAdmin

Date Range: Monday, May 23, 2005 to Monday, May 23, 2005

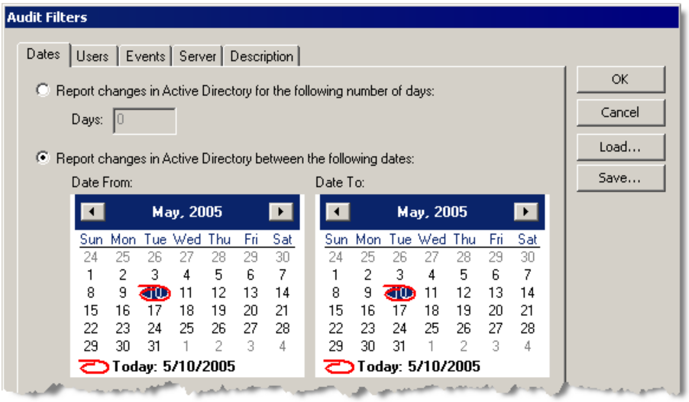
User(s): <All Users>

Event(s): <All Events>

Server(s): <All Servers>

Description Mask: <No description filter>

4. In the **Current Filter Criteria** area, set filters by either clicking ... to set an individual filter or clicking **Filters** to open the **Audit Filters** dialog box where you can set all the filter types.



○ Report changes in Active Directory for the following number of days:

Days: 0

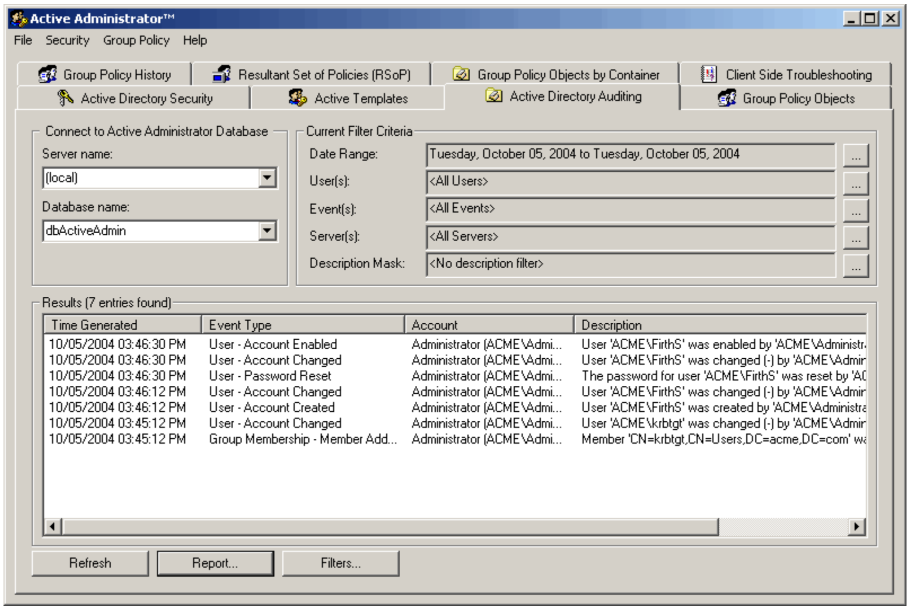
● Report changes in Active Directory between the following dates:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

- To save a set of filter criteria, click **Save**, type a name of the filter set, and then click **OK**.
- To load a saved set of filter criteria, click **Load**, select a filter set from the list, and then click **OK**.

5. Click **Refresh**. The events that match the filter criteria display in the **Results** area.


Active Administrator™
File
Security
Group Policy
Help
Group Policy History
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
Client Side Troubleshooting
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Refresh
Report...
Filters...

Connect to Active Administrator Database

Server name: (local)

Database name: dbActiveAdmin

Current Filter Criteria

Date Range: Tuesday, October 05, 2004 to Tuesday, October 05, 2004

User(s): <All Users>

Event(s): <All Events>

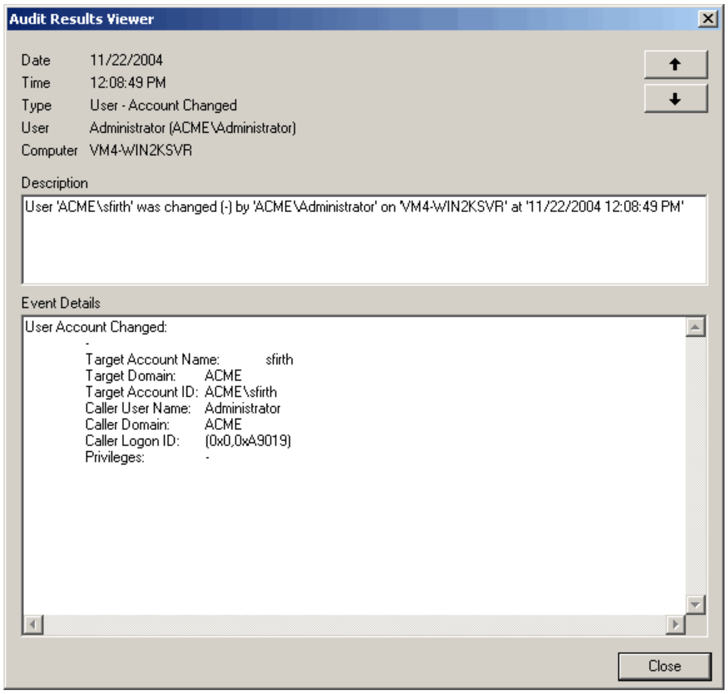
Server(s): <All Servers>

Description Mask: <No description filter>

Results (7 entries found)

Time Generated	Event Type	Account	Description
10/05/2004 03:46:30 PM	User - Account Enabled	Administrator (ACME\Admi...	User 'ACME\FirthS' was enabled by 'ACME\Administr
10/05/2004 03:46:30 PM	User - Account Changed	Administrator (ACME\Admi...	User 'ACME\FirthS' was changed (-) by 'ACME\Admir
10/05/2004 03:46:30 PM	User - Password Reset	Administrator (ACME\Admi...	The password for user 'ACME\FirthS' was reset by 'AC
10/05/2004 03:46:12 PM	User - Account Changed	Administrator (ACME\Admi...	User 'ACME\FirthS' was changed (-) by 'ACME\Admir
10/05/2004 03:46:12 PM	User - Account Created	Administrator (ACME\Admi...	User 'ACME\FirthS' was created by 'ACME\Administra
10/05/2004 03:45:12 PM	User - Account Changed	Administrator (ACME\Admi...	User 'ACME\krbtgt' was changed (-) by 'ACME\Admir
10/05/2004 03:45:12 PM	Group Membership - Member Add...	Administrator (ACME\Admi...	Member 'CN=krbtgt,CN=Users,DC=acme,DC=com' wa

- To view the details, double-click an event. The **Audit Results Viewer** opens. Use the up and down arrows to scroll through the list of events.



Date 11/22/2004

Time 12:08:49 PM

Type User - Account Changed

User Administrator (ACME\Administrator)

Computer VM4-WIN2KSVR

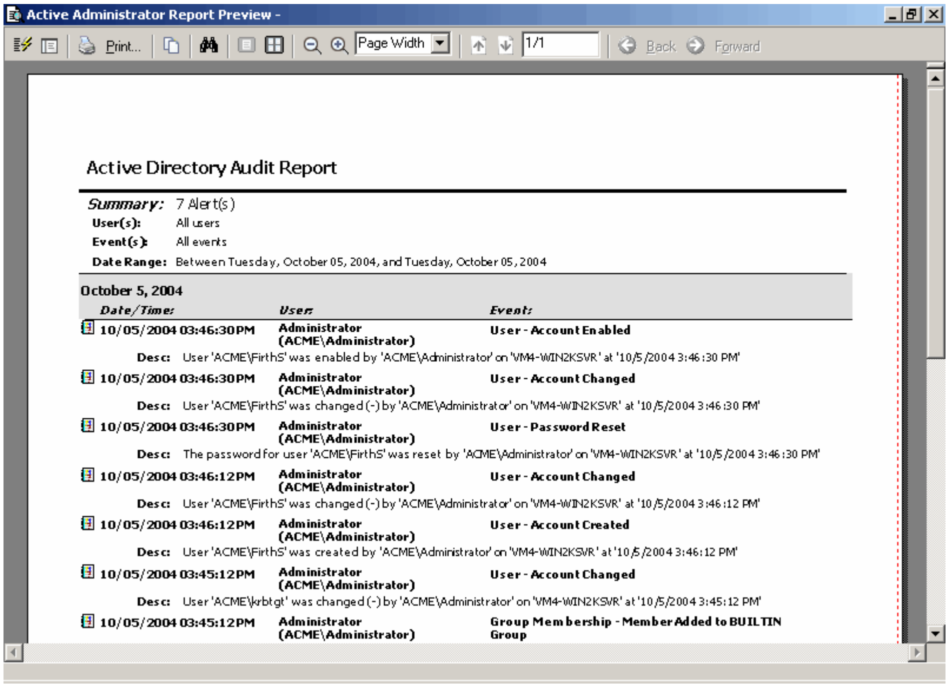
Description

User 'ACME\sfirth' was changed (-) by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '11/22/2004 12:08:49 PM'

Event Details

```
User Account Changed:
          -
          Target Account Name:        sfirth
          Target Domain:      ACME
          Target Account ID:  ACME\sfirth
          Caller User Name:   Administrator
          Caller Domain:      ACME
          Caller Logon ID:    (0x0,0xA9019)
          Privileges:         -
```

- To create a report for all events in the filter, click **Report**.



Active Directory Audit Report

Summary: 7 Alert(s)
User(s): All users
Event(s): All events
Date Range: Between Tuesday, October 05, 2004, and Tuesday, October 05, 2004

October 5, 2004

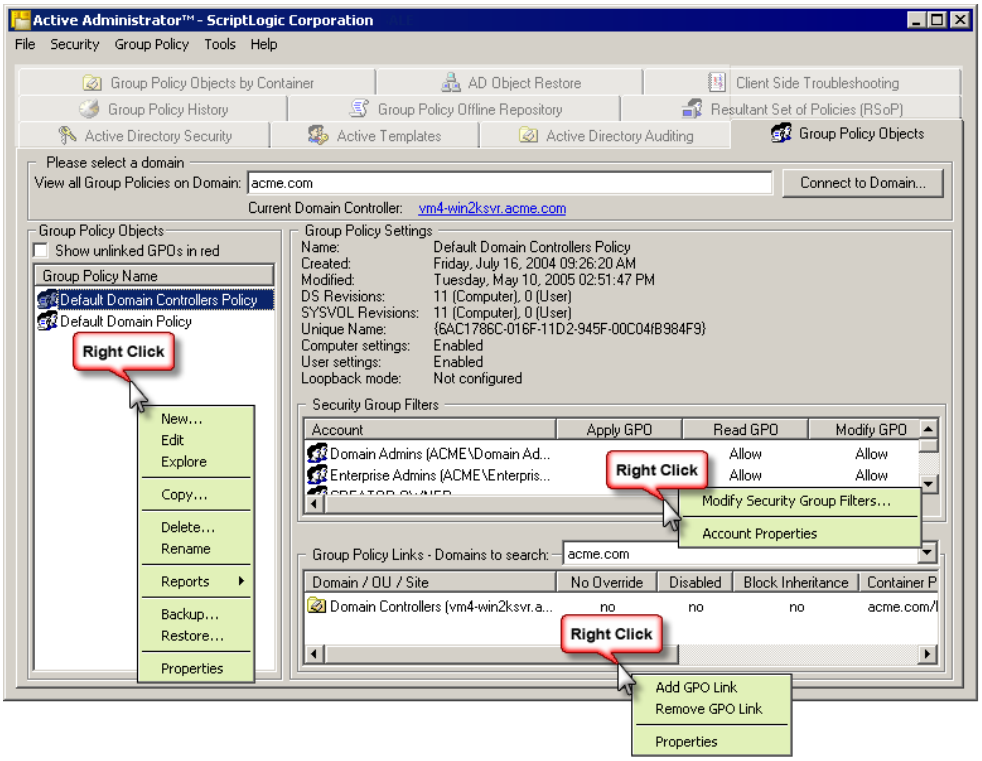
Date/Time:	***User:***	***Event:***
10/05/2004 03:46:30PM	**Administrator (ACME\Administrator)**	**User - Account Enabled**
Desc: User 'ACME\FirthS' was enabled by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:46:30 PM'		
10/05/2004 03:46:30PM	**Administrator (ACME\Administrator)**	**User - Account Changed**
Desc: User 'ACME\FirthS' was changed (-) by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:46:30 PM'		
10/05/2004 03:46:30PM	**Administrator (ACME\Administrator)**	**User - Password Reset**
Desc: The password for user 'ACME\FirthS' was reset by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:46:30 PM'		
10/05/2004 03:46:12PM	**Administrator (ACME\Administrator)**	**User - Account Changed**
Desc: User 'ACME\FirthS' was changed (-) by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:46:12 PM'		
10/05/2004 03:46:12PM	**Administrator (ACME\Administrator)**	**User - Account Created**
Desc: User 'ACME\FirthS' was created by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:46:12 PM'		
10/05/2004 03:45:12PM	**Administrator (ACME\Administrator)**	**User - Account Changed**
Desc: User 'ACME\krbtgt' was changed (-) by 'ACME\Administrator' on 'VM4-WIN2KSVR' at '10/5/2004 3:45:12 PM'		
10/05/2004 03:45:12PM	**Administrator (ACME\Administrator)**	**Group Membership - Member Added to BUILTIN Group**

Group Policy Objects

Active Administrator provides unparalleled functionality in the area of Group Policy object management. Many familiar functions can be performed through the intuitive interface. Administrators can create, delete, and rename Group Policy objects. They can also add and remove links.

Much of the vital information about a Group Policy object can be viewed simply by highlighting the object. This includes the links for the Group Policy object in any domain the administrator chooses, security group filters for the object and revision and statistical information relevant to its usage.

Active Administrator adds some new functionality to the world of Active Directory Management. An administrator can copy a Group Policy object from one domain to another or even explorer the exact location on the network where the object itself is stored.



View all Group Policies on Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

☐ Show unlinked GPOs in red

Group Policy Name
Default Domain Controllers Policy
Default Domain Policy

Name:	Default Domain Controllers Policy
Created:	Friday, July 16, 2004 09:26:20 AM
Modified:	Tuesday, May 10, 2005 02:51:47 PM
DS Revisions:	11 (Computer), 0 (User)
SYSVOL Revisions:	11 (Computer), 0 (User)
Unique Name:	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Computer settings:	Enabled
User settings:	Enabled
Loopback mode:	Not configured

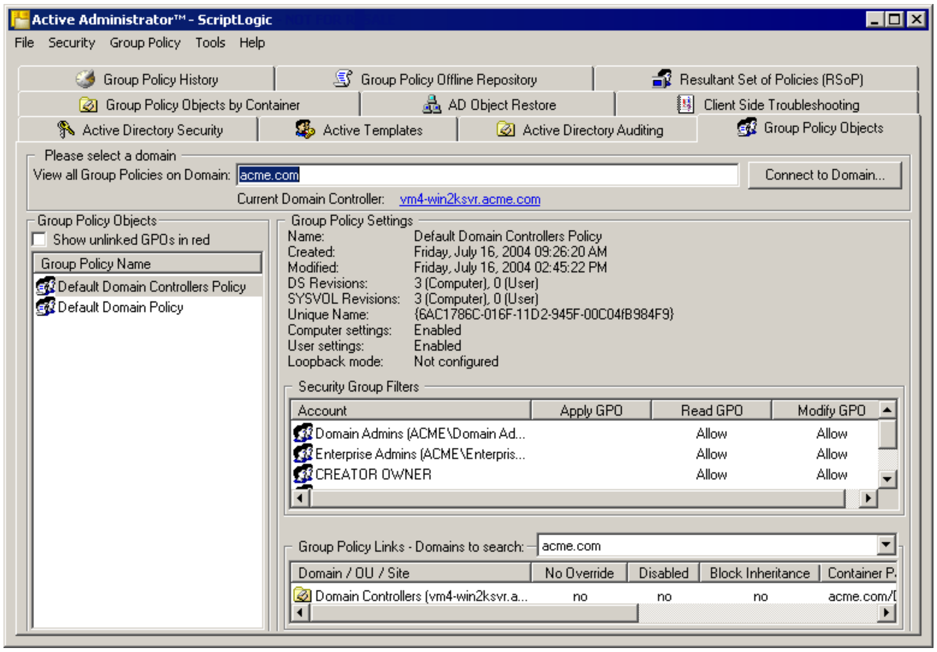
Account	Apply GPO	Read GPO	Modify GPO
Domain Admins (ACME\Domain Ad...		Allow	Allow
Enterprise Admins (ACME\Enterpris...		Allow	Allow
CREATOR OWNER			

Group Policy Links - Domains to search: acme.com

Domain / OU / Site	No Override	Disabled	Block Inheritance	Container P
Domain Controllers (vm4-win2ksvr.a...	no	no	no	acme.com/I

VIEWING GROUP POLICIES

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller. The **Group Policy Objects** list displays the GPOs for the selected domain. The **Group Policy Settings** area displays information about the selected GPO.


Active Administrator™ - ScriptLogic
File
Security
Group Policy
Tools
Help
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Connect to Domain...

Please select a domain

View all Group Policies on Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Group Policy Objects

□ Show unlinked GPOs in red

Group Policy Name
Default Domain Controllers Policy
Default Domain Policy

Group Policy Settings

Name:	Default Domain Controllers Policy
Created:	Friday, July 16, 2004 09:26:20 AM
Modified:	Friday, July 16, 2004 02:45:22 PM
DS Revisions:	3 (Computer), 0 (User)
SYSVOL Revisions:	3 (Computer), 0 (User)
Unique Name:	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Computer settings:	Enabled
User settings:	Enabled
Loopback mode:	Not configured

Security Group Filters

Account	Apply GPO	Read GPO	Modify GPO
Domain Admins (ACME\Domain Ad...		Allow	Allow
Enterprise Admins (ACME\Enterpris...		Allow	Allow
CREATOR OWNER		Allow	Allow

Group Policy Links - Domains to search: acme.com

Domain / OU / Site	No Override	Disabled	Block Inheritance	Container P.
Domain Controllers (vm4-win2ksvr.a...	no	no	no	acme.com/[

- To display unlinked GPOs in red, select the **Show unlinked GPOs in red** check box.

MODIFYING PROPERTIES FOR A GROUP POLICY OBJECT

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.

   There are several ways to open the Access Control List (ACL) editor to view and/or modify the properties on a Group Policy object.

   - In the **Group Policy Objects** list, right-click a GPO, and then select **Properties**. The ACL editor opens to the **General** tab.
   - In the **Security Group Filters** list, double-click an account. The ACL editor opens to the **Security** tab.
   - In the **Group Policy Links** list, right-click a link, and then select **Properties**. The ACL editor opens to the **Group Policy** tab.

MODIFYING A GROUP POLICY OBJECT

Caution: If you modify a GPO online and it is in use, changes you make may not be applied to the object using that GPO. To control the GPO change process, edit the GPO offline. Right-click the GPO, and then select **Add to Offline Repository**. See *Editing Group Policy Offline*.

1. From the Active Administrator Console, open the **Group Policy Objects** tab.

   Note: You also can edit a Group Policy object in Windows Explorer on the **Group Policy Objects by Container** tab. See *Modifying a Group Policy Object*.

2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. In the **Group Policy Objects** list, double-click a GPO, or right-click a GPO, and then choose **Edit**. The **Group Policy** window opens.

   Note: If you do not have proper permissions to modify the Group Policy object you receive an access denied message.

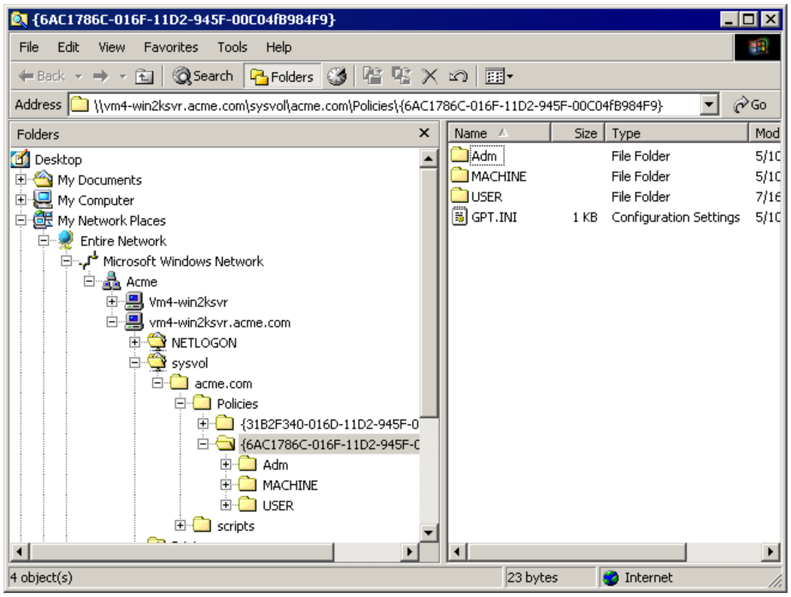
5. Modify the GPO, and then close the window. The settings display in the **Group Policy Settings** area of the **Group Policy Objects** tab.

Locating a Group Policy Object

1. From the Active Administrator Console, open the **Group Policy Objects** tab.

   Note: You also can locate a Group Policy object in Windows Explorer on the **Group Policy Objects by Container** tab. See *Locating a Group Policy Object*.

2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. In the **Group Policy Objects** list, right-click the GPO, and then select **Explore**. Microsoft Windows Explorer opens displaying the path to the GPO in the Address box and highlighting the GPO in the hierarchy.



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

Address \\vm4-win2ksvr.acme.com\sysvol\acme.com\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}

Name	Size	Type	Mod
Adm		File Folder	5/1C
MACHINE		File Folder	5/1C
USER		File Folder	7/16
GPT.INI	1 KB	Configuration Settings	5/1C

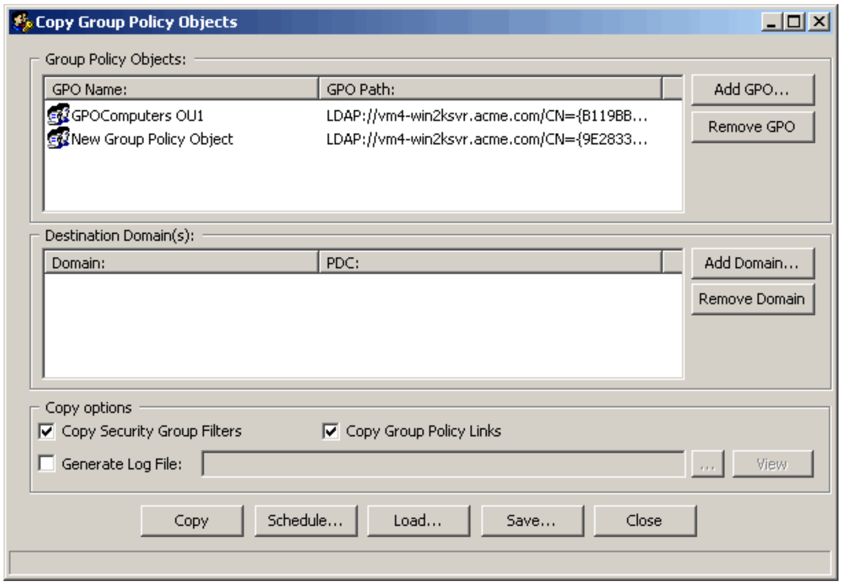
4 object(s) 23 bytes Internet

COPYING GROUP POLICY OBJECTS

One of the truly unique features of Active Administrator is the ability to copy Group Policy Objects between domains. The process is outlined below in some detail. It shows just how easy it can be to use this product to perform a function that would otherwise not be possible.

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. In the **Group Policy Objects** list, select the object(s) to copy, right-click the selection, and then choose **Copy**. The **Copy Group Policy Objects** dialog box displays the selections.

   Note: You also can choose **Copy Group Policy Objects** from the **Group Policy** menu to open this dialog box.



Group Policy Objects:

GPO Name:	GPO Path:
GPOComputers OU1	LDAP://vm4-win2ksvr.acme.com/CN={B119BB...
New Group Policy Object	LDAP://vm4-win2ksvr.acme.com/CN={9E2833...

Destination Domain(s):

Domain:	PDC:

Copy options

☑ Copy Security Group Filters ☑ Copy Group Policy Links

☐ Generate Log File:

- To add more GPOs to the list, click **Add GPO**.
- To remove GPOs from the list, select one or more GPOs, and then click **Remove GPO**.

5. To add a destination domain, click **Add Domain**. The **Connect to Domain** box opens.
6. In the **Domain** box, type a domain name, or click **Browse** to locate a domain. The selected domain displays in the **Destination Domain** area.
7. In the **Copy Options** area, set options for the copy process.

   ☑ **Copy Security Group Filters**
   By default, the copy process includes the security group filters.

   ☑ **Copy Group Policy Links**
   By default, the copy process includes the Group Policy links.

   ☑ **Generate Log File**
   Generates a .txt log file for the copy process. Type the name of the .txt file or click ... to locate the file.

   Note: To view the log file shown in the box, click **View**.

8. To initiate the copy, click **Copy**.

   Note: Each GPO has a Globally Unique Identifier (GUID). If these are the same between domains, the current GPO is overwritten. You can view the GUID in the **Group Policy Objects** area of the **Copy Group Policy** dialog box.

Save Copy Settings

▶ To save the copy settings as a Group Policy Copy Job File (*.gpc), click **Save**, choose a location for the file, type a name for the file, and then click **Save**.

Load Copy Settings

▶ To load a previously saved Group Policy copy job file (*.gpc), click **Load**, choose the location for the file, select the file, and then click **Open**.

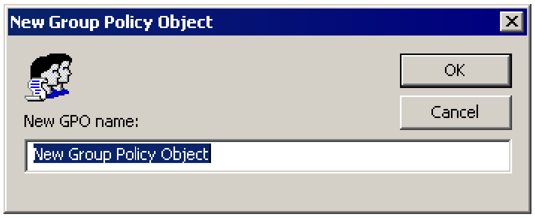
Schedule a Copy Job

1. Click **Schedule**. The Schedule a GPOCopy job box opens.
2. In the Job Name box, type a name for the copy job.
3. In the Save Job in Folder box, click [...] and then choose a folder in which to store the copy job.
4. Click **Schedule**. The Microsoft Windows scheduling service opens.
5. Schedule the copy job, and then click **OK**.

   Note: To edit a previously scheduled copy job, click **Manage Scheduled Jobs**. The **Scheduled Tasks** window opens where you can modify scheduled jobs.

CREATING A NEW GROUP POLICY OBJECT

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. Right-click in the **Group Policy Name** list box, and then choose **New**. The **New Group Policy Object** box displays the default GPO name.



New GPO name: New Group Policy Object

5. In the **New GPO name** box, type a name, and then click **OK**. The new GPO name displays in the **Group Policy Name** list and the default settings display in the **Group Policy Settings** area.

   Note: If you make a mistake typing, you can rename the GPO. Right-click the GPO, and then choose **Rename**.

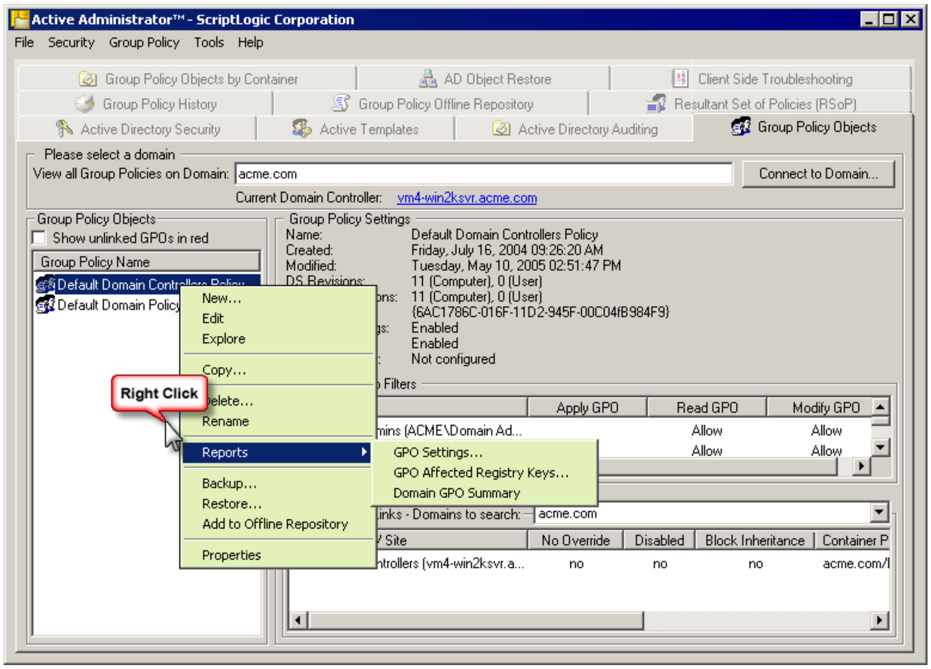
RENAMING A GROUP POLICY OBJECT

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. In the **Group Policy Objects** list, right-click the GPO, and then choose **Rename**.
5. Type a new name for the GPO, and then press **Enter**.

REPORTING ON GROUP POLICY OBJECTS

Active Administrator can generate reports for administrators that provide relevant and useful information about Group Policy objects. This information is available in a wide variety of formats and can be exported to popular formats for portability.

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain,** and then select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Connect to Domain...
Right Click
New...
Edit
Explore
Copy...
Delete...
Rename
Reports
Backup...
Restore...
Add to Offline Repository
Properties
GPO Settings...
GPO Affected Registry Keys...
Domain GPO Summary

Please select a domain
View all Group Policies on Domain: acme.com
Current Domain Controller: vm4-win2ksvr.acme.com

Group Policy Objects
□ Show unlinked GPOs in red

Group Policy Name
Default Domain Controllers Policy
Default Domain Policy

Group Policy Settings
Name: Default Domain Controllers Policy
Created: Friday, July 16, 2004 09:26:20 AM
Modified: Tuesday, May 10, 2005 02:51:47 PM
DS Revisions: 11 (Computer), 0 (User)
ons: 11 (Computer), 0 (User)
{6AC1786C-016F-11D2-945F-00C04fB984F9}
gs: Enabled
Enabled
Not configured

Filters

	Apply GPO	Read GPO	Modify GPO
mins (ACME\Domain Ad...		Allow	Allow
		Allow	Allow

Links - Domains to search: acme.com

Site	No Override	Disabled	Block Inheritance	Container P
ntrollers (vm4-win2ksvr.a...	no	no	no	acme.com/l

4. In the **Group Policy Objects** list, right-click a Group Policy object, point to **Reports**, and then choose one of the following report options.

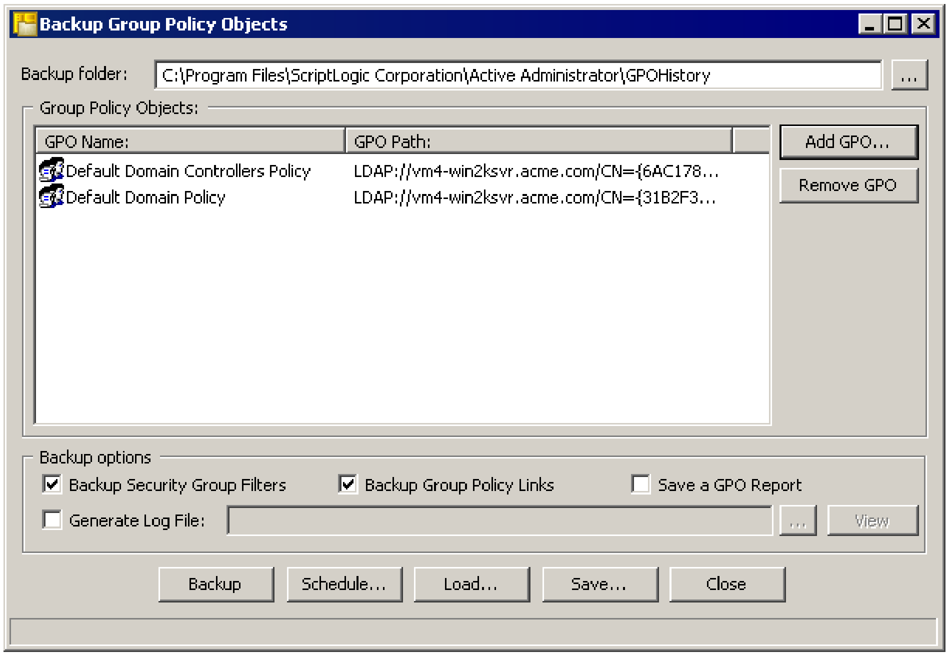
Report	Description
GPO Settings	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
GPO Affected Registry Keys	Shows the registry keys affected by the selected Group Policy object in the selected domain.
Domain GPO Summary	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for all Group Policy objects in the selected domain.

BACKING UP A GROUP POLICY OBJECT

Another feature unique to Active Administrator is the ability to back up an entire Group Policy Object (GPO) to a folder structure from where it can be restored if needed. This feature provides a high level of fault tolerance and recoverability that was never before possible with any other tool.

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. In the **Group Policy Objects** list, select the object(s) to backup, right-click the selection, and then select **Backup**. The **Backup Group Policy Objects** dialog box displays the selections.

Note: You also can choose **Backup Group Policy Objects** from the **Group Policy** menu to open this dialog box.



Backup Group Policy Objects

Backup folder: C:\Program Files\ScriptLogic Corporation\Active Administrator\GPOHistory

Group Policy Objects:

GPO Name:	GPO Path:
Default Domain Controllers Policy	LDAP://vm4-win2ksvr.acme.com/CN={6AC178...
Default Domain Policy	LDAP://vm4-win2ksvr.acme.com/CN={31B2F3...

Backup options

☑ Backup Security Group Filters ☑ Backup Group Policy Links □ Save a GPO Report

□ Generate Log File:

- To add more GPOs to the list, click **Add GPO**.
- To remove GPOs from the list, select one or more GPOs, and then click **Remove GPO**.

5. In the **Backup folder** box, type the path to the folder where you want to store the backup or click ... to locate a folder.
6. In the **Backup options** area, set options for the copy process.

   ☑ **Backup Security Group Filters**
   By default, the backup process includes the security group filters.

   ☑ **Backup Group Policy Links**
   By default, the backup process includes the Group Policy links.

   ☑ **Save a GPO Report**
   Creates a Group Policy Settings report saved as **Settings.PDF**.

   ☑ **Generate Log File**
   Generates a .txt log file for the backup process. Type the name of the .txt file or click ... to locate the file. To view a log file displayed in the box, click **View**.
7. To initiate the backup, click **Backup**. When the backup is complete, a message box appears.
8. Click **OK**.

Save Backup Settings

▶ To save the backup settings as a Group Policy backup job file (*.gpb), click **Save**, choose a location for the file, type a name for the file, and then click **Save**.

Load Backup Settings

▶ To load a previously saved Group Policy backup job file (*.gpb), click **Load**, choose the location for the file, select the file, and then click **Open**.

Schedule a Backup Job

1. Click **Schedule**. The **Schedule a GPOBackup job** box opens.
2. In the **Job Name** box, type a name for the copy job.
3. In the **Save Job in Folder** box, click ... and choose a folder in which to store the backup job.
4. Click **Schedule**. The Microsoft Windows scheduling service opens.
5. Schedule the backup job, and then click **OK**.

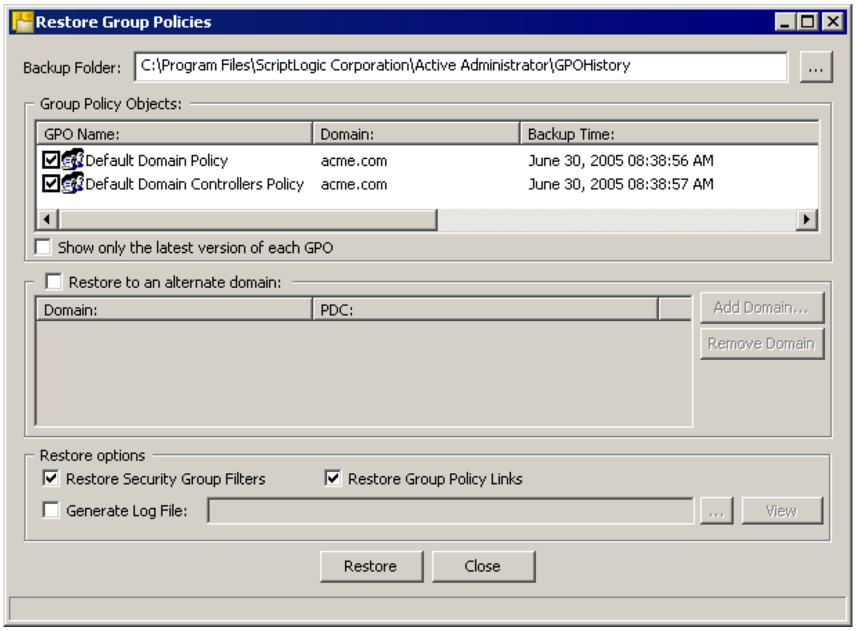
Note: To edit a previously scheduled backup job, click **Manage Schedule Jobs**. The **Scheduled Tasks** window opens where you can modify scheduled jobs.

RESTORING A GROUP POLICY OBJECT

Active Administrator allows you to restore the Group Policy Objects (GPO) that you have backed up. This functionality can easily allow you to repair damaged GPOs or those that were accidentally deleted.

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller, and then select a domain controller.
4. Right-click in the **Group Policy Objects** list, and then select **Restore**.

Note: You also can choose **Restore Group Policy Objects** from the **Group Policy** menu to open this dialog box.



Restore Group Policies

Backup Folder: C:\Program Files\ScriptLogic Corporation\Active Administrator\GPOHistory

Group Policy Objects:

GPO Name:	Domain:	Backup Time:
☑ Default Domain Policy	acme.com	June 30, 2005 08:38:56 AM
☑ Default Domain Controllers Policy	acme.com	June 30, 2005 08:38:57 AM

☐ Show only the latest version of each GPO

☐ Restore to an alternate domain:

Domain:	PDC:

Restore options

☑ Restore Security Group Filters ☑ Restore Group Policy Links

☐ Generate Log File:

5. In the **Backup folder** box, type the path to the folder where the backup is located or click … to locate the folder.
6. In the **Group Policy Objects** list, select the GPOs to restore. To shorten the list, select **Show only the latest version of each GPO**.
7. To restore the selection to an alternate domain, select **Restore to an alternate domain**. Click **Add Domain** to add a domain to the list.
8. In the **Restore options** area, set options for the copy process.

   ☑ **Restore Security Group Filters**
   By default, the restore process includes the security group filters.

   ☑ **Restore Group Policy Links**
   By default, the restore process includes the Group Policy links.

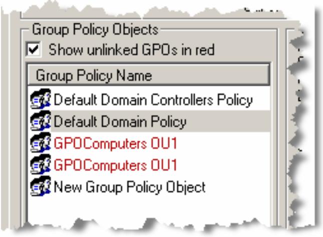
   ☑ **Generate Log File**
   Generates a .txt log file for the restore process. Type the name of the .txt file or click … to locate the file. To view a log file displayed in the box, click **View**.

9. To initiate the restore process, click **Restore**. A confirmation message appears.

10. To overwrite the existing GPO, click **Yes**. When the restore process is complete, a message box appears.
11. Click **OK**.

ADDING A GROUP POLICY LINK

Active Administrator includes the ability to view and link Group Policy objects (GPOs). Sometimes Group Policy objects can be created, but not linked to anything, which can make keeping track of these objects problematic and time consuming for administrators. With Active Administrator, you can easily see which GPOs are not linked as you can choose to display them in red.

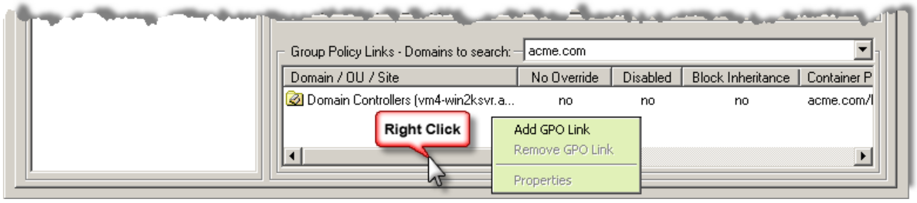


Group Policy Objects

☑ Show unlinked GPOs in red

Group Policy Name
Default Domain Controllers Policy
Default Domain Policy
GPOComputers OU1
GPOComputers OU1
New Group Policy Object

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. In the **Group Policy Links** area, if necessary, open the **Domains to search** list to select a domain.
3. Right-click in the **Group Policy Links** list box, and then choose **Add GPO Link**.



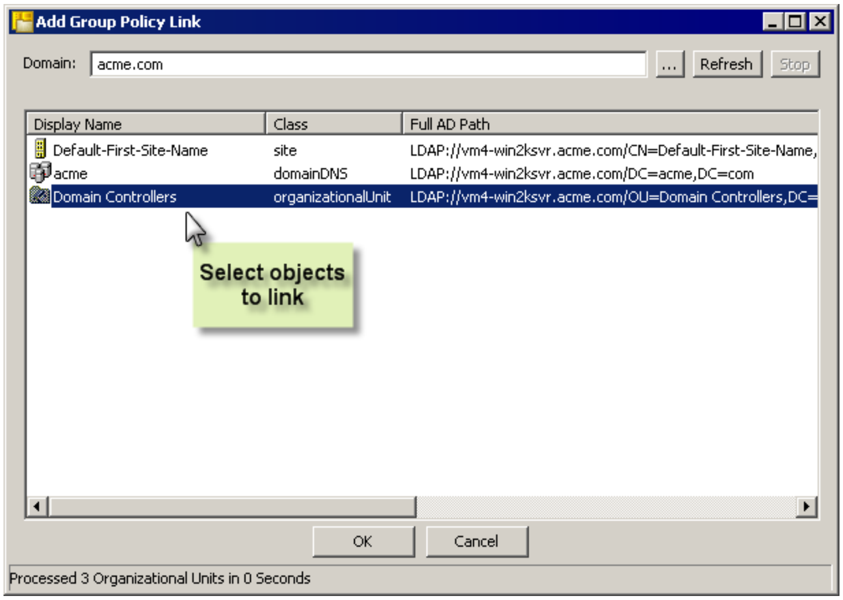
Group Policy Links - Domains to search: acme.com

Domain / OU / Site	No Override	Disabled	Block Inheritance	Container P
Domain Controllers (vm4-win2ksvr.a...	no	no	no	acme.com/I

The **Add Group Policy Link** list box opens to the selected domain. Active Administrator searches the selected domain and then lists the objects that can be linked to the Group Policy object.

Note: If the search is taking too long, you can click **Stop**.

Note: To change to a different domain, click ..., and then select a domain. Click **Refresh** to populate the list box.



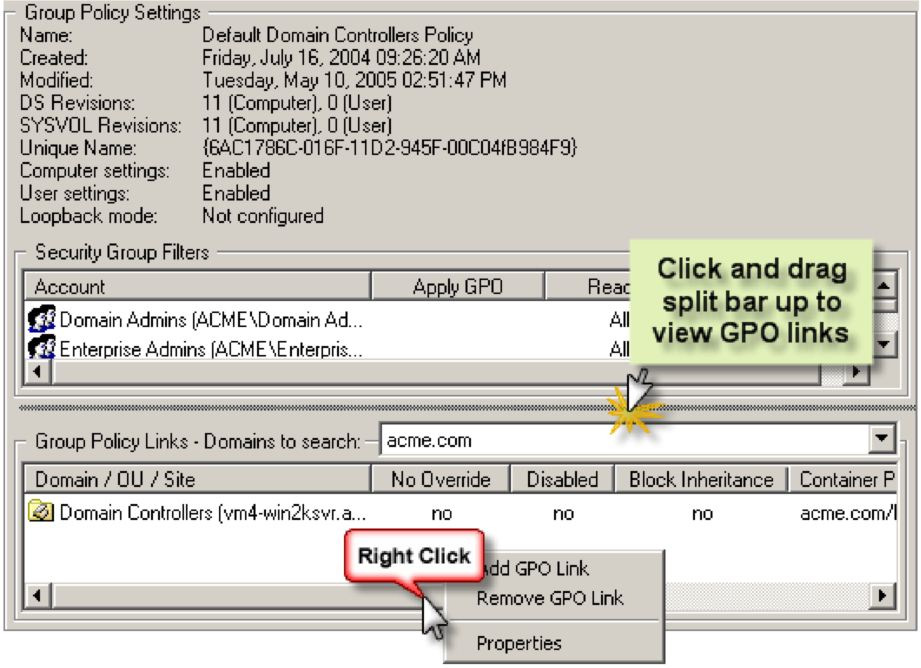
Add Group Policy Link

Domain: acme.com

Display Name	Class	Full AD Path
Default-First-Site-Name	site	LDAP://vm4-win2ksvr.acme.com/CN=Default-First-Site-Name,
acme	domainDNS	LDAP://vm4-win2ksvr.acme.com/DC=acme,DC=com
Domain Controllers	organizationalUnit	LDAP://vm4-win2ksvr.acme.com/OU=Domain Controllers,DC=

Processed 3 Organizational Units in 0 Seconds

4. Select the objects to link, and then click **OK**. The linked objects display in the **Group Policy Links** list box. You can size the area upward to increase the viewing area.



Group Policy Settings

Name:	Default Domain Controllers Policy
Created:	Friday, July 16, 2004 09:26:20 AM
Modified:	Tuesday, May 10, 2005 02:51:47 PM
DS Revisions:	11 (Computer), 0 (User)
SYSVOL Revisions:	11 (Computer), 0 (User)
Unique Name:	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Computer settings:	Enabled
User settings:	Enabled
Loopback mode:	Not configured

Security Group Filters

Account	Apply GPO	Reac
Domain Admins (ACME\Domain Ad...		All
Enterprise Admins (ACME\Enterpris...		All

Click and drag split bar up to view GPO links

Group Policy Links - Domains to search: acme.com

Domain / OU / Site	No Override	Disabled	Block Inheritance	Container P
Domain Controllers (vm4-win2ksvr.a...	no	no	no	acme.com/I

Right Click

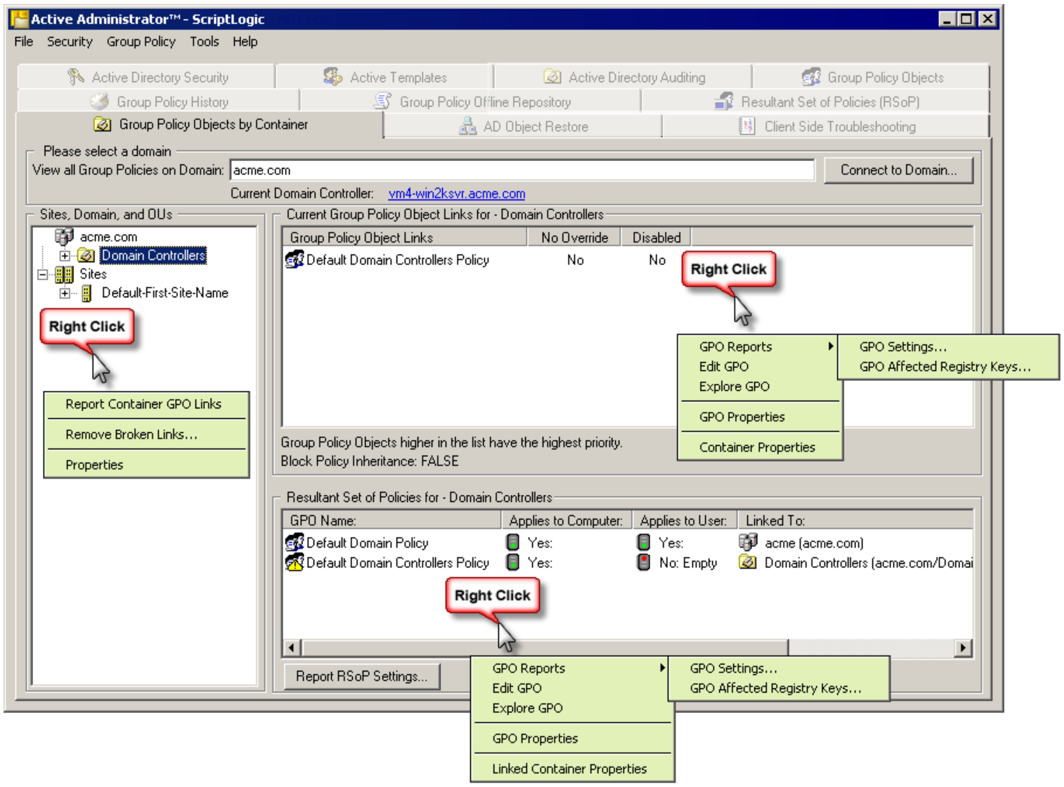
- To view an object's properties, right-click on the object in the **Group Policy Links** list, and then choose **Properties**.

REMOVING A GROUP POLICY LINK

1. From the Active Administrator Console, open the **Group Policy Objects** tab.
2. In the **Group Policy Links** area, if necessary, open the **Domains to search** list to select a domain.
3. In the **Group Policy Links** list box, right-click an object, and then choose **Remove GPO Link**. A confirmation message box appears.
4. To remove the GPO link, click **Yes**.

Group Policy Objects by Container

Active Administrator includes the ability to view Group Policy objects by the containers to which they are linked, which allows administrators to quickly view Group Policy object application for a specific container. After locating a desired container object, applied GPOs are displayed, and a Resultant Set of Policies calculation can be provided immediately.



Please select a domain

View all Group Policies on Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Current Group Policy Object Links for - Domain Controllers

Group Policy Object Links	No Override	Disabled
Default Domain Controllers Policy	No	No

Group Policy Objects higher in the list have the highest priority.
Block Policy Inheritance: FALSE

Resultant Set of Policies for - Domain Controllers

GPO Name:	Applies to Computer:	Applies to User:	Linked To:
Default Domain Policy	Yes:	Yes:	acme (acme.com)
Default Domain Controllers Policy	Yes:	No: Empty	Domain Controllers (acme.com/Domai

MODIFYING A GROUP POLICY OBJECT

Note: You also can edit a Group Policy object in Windows Explorer on the **Group Policy Objects** tab. See *Modifying a Group Policy Object*.

1. From the Active Administrator Console, open the **Group Policy Objects by Container** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller hyperlink, and then select a domain controller. The **Sites, Domain, and OUs** list displays objects that have at least one GPO setting applied.

4. Depending on the type of information you want to modify, select one of the following methods:

   Note: If you do not have proper permissions to modify a Group Policy object you receive an access denied message.

   - **Sites, Domain, and OUs** list
     - Right-click a container, and then select **Properties**. The **Properties** dialog box opens to the **Group Policy** tab.

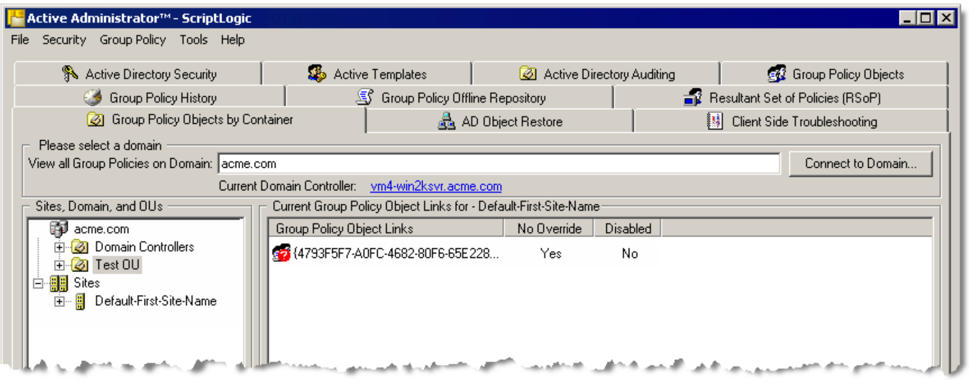
   - **Current Group Policy Object Links for** list
     - Double-click a GPO, or right-click a GPO, and then choose **Container Properties**. The **Properties** dialog box opens to the **Group Policy** tab.
     - Right-click a GPO, and then choose **Edit GPO**. The **Group Policy** window opens.
     - Right-click a GPO, and then choose **GPO Properties**. The **Default Domain Controllers Policy Properties** dialog box opens to the **General** tab.

   - **Resultant Set of Policies for** list
     - Double-click a GPO, or right-click a GPO, and then choose **Linked Container Properties**. The **Properties** dialog box opens to the **Group Policy** tab.
     - Right-click a GPO, and then choose **Edit GPO**. The **Group Policy window** opens.
     - Right-click a GPO, and then choose **GPO Properties**. The **Default Domain Controllers Policy Properties** dialog box opens to the **General** tab.

REMOVING BROKEN LINKS

1. From the Active Administrator Console, open the **Group Policy Objects by Container** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller hyperlink, and then select a domain controller.

   In the event that a GPO link is broken, a question mark appears next to the link.



View all Group Policies on Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Current Group Policy Object Links for - Default-First-Site-Name

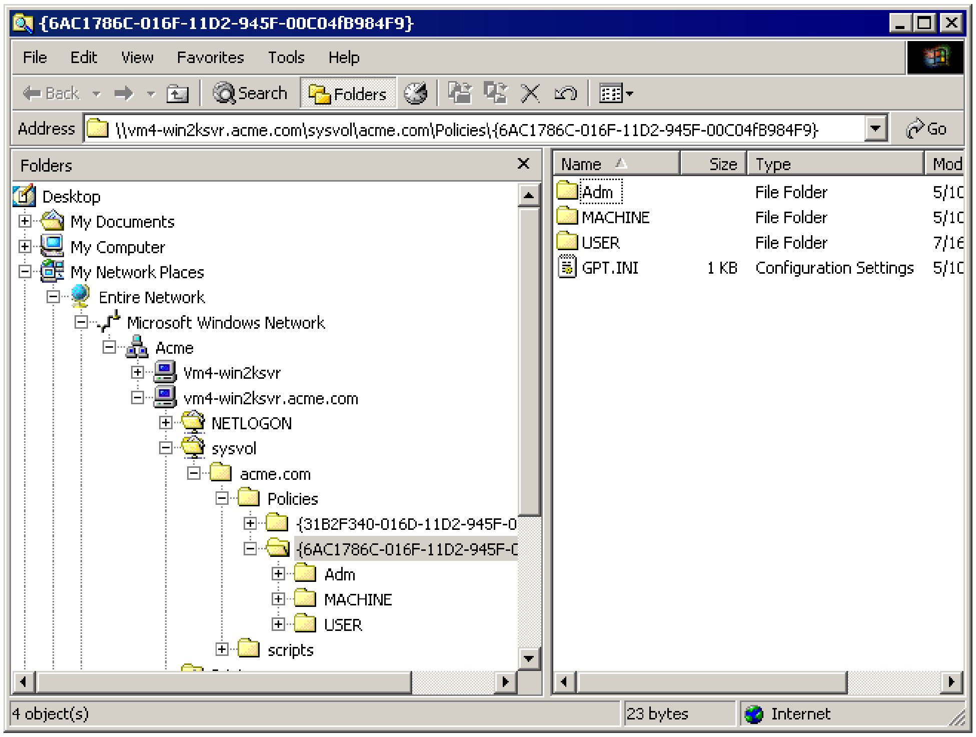
Group Policy Object Links	No Override	Disabled
{4793F5F7-A0FC-4682-80F6-65E228...	Yes	No

4. In the **Sites, Domain, and OUs** list, right-click an object, and then choose **Remove Broken Links**. If any broken links are found, the **Confirm Remove Broken GPO Links** list box displays the broken link(s).
5. To delete the broken link(s), click **Yes**.

LOCATING A GROUP POLICY OBJECT

Note: You also can locate a Group Policy object in Windows Explorer on the **Group Policy Objects** tab. See *Locating a Group Policy Object*.

1. From the Active Administrator Console, open the **Group Policy Objects by Container** tab.
2. If necessary, in the **View all Group Policies on Domain** box, type the domain name, or click **Connect to Domain** and select a domain.
3. If necessary, click the current domain controller hyperlink, and then select a domain controller.
4. In the **Sites, Domain, and OUs** list, select the container.
5. In either the **Current Group Policy Objects Links for** or the **Resultant Set of Policies for** lists, right-click a GPO, and then choose **Explore GPO**. Windows Explorer opens displaying the path to the GPO in the **Address** box and highlighting the GPO in the hierarchy.



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

Address \\vm4-win2ksvr.acme.com\sysvol\acme.com\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}

Name	Size	Type	Mod
Adm		File Folder	5/1C
MACHINE		File Folder	5/1C
USER		File Folder	7/16
GPT.INI	1 KB	Configuration Settings	5/1C

4 object(s) 23 bytes Internet

REPORTING ON GROUP POLICY OBJECTS

▶ From the **Sites, Domains, and OUs** list, right-click a container, and then select **Report Container GPO Links**.

Report	Description
Container GPO Links	Shows the Group Policy links and their settings for the selected container.

▶ From either the **Current Group Policy Objects Links for** or **Resultant Set of Policies for** areas, right-click a GPO, point to **GPO Reports**, and then choose a report.

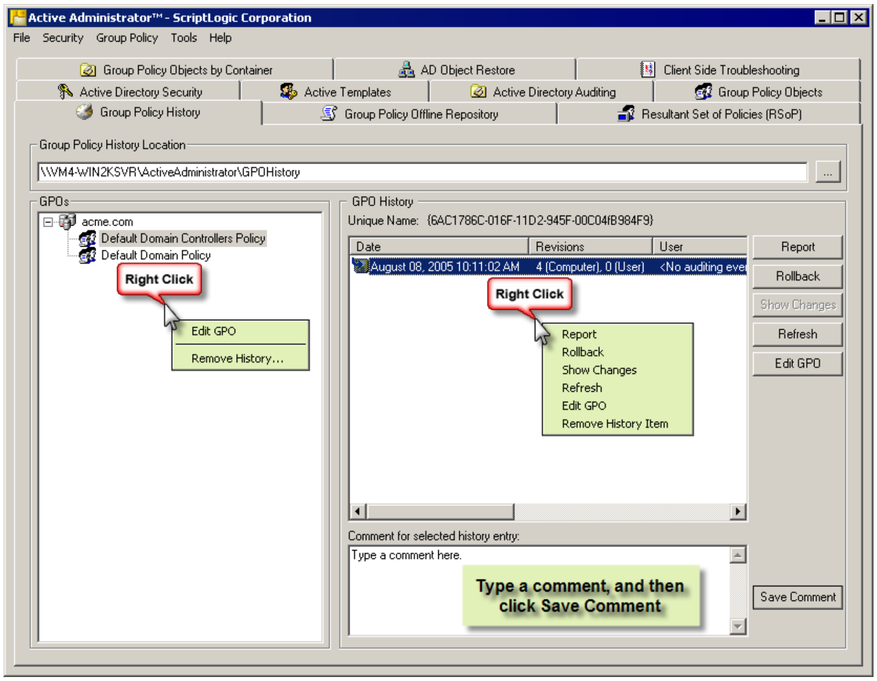
Report	Description
GPO Settings	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
GPO Affected Registry Keys	Shows the registry keys affected by the selected Group Policy object in the selected domain.

▶ From the **Sites, Domains, and OUs** list, select a container, or from either the **Current Group Policy Objects Links for** or **Resultant Set of Policies for** areas, select a GPO, and then click **Report RSoP Settings**.

Report	Description
Resultant Set of Policies	Shows the settings, computer configuration, and user configuration for the selected container or GPO.

Group Policy History

Group Policy history is kept for all GPOs in your domains. A specialized service watches your domain controllers for GPO changes. The combination of these two services allows you to determine exactly who made changes to your Group Policies and what they changed. If you don't like a change that someone made, you can roll back to a previous version of the GPO.



Group Policy History Location: \\VM4-WIN2KSVR\ActiveAdministrator\GPOHistory

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

Date	Revisions	User
August 08, 2005 10:11:02 AM	4 (Computer), 0 (User)	<No auditing eve

Comment for selected history entry:

Type a comment here.

Right Click

Right Click

Type a comment, and then click Save Comment

VIEWING GROUP POLICY HISTORY

The Group Policy history service automatically checks for Group Policy object (GPO) changes and saves the changes to a file share on your network. The default folder created during installation is GPOHistory. The administrator in charge of setting up the Group Policy History service should let you know the UNC path to the Group Policy history.

1. From the Active Administrator Console, open the **Group Policy History** tab. The UNC path to the Group Policy history folder displays in the **Group Policy History Location** box.

2. To change to a different folder, type the UNC path to the folder, or click … to locate the folder. The domain displays in the **GPOs** list.

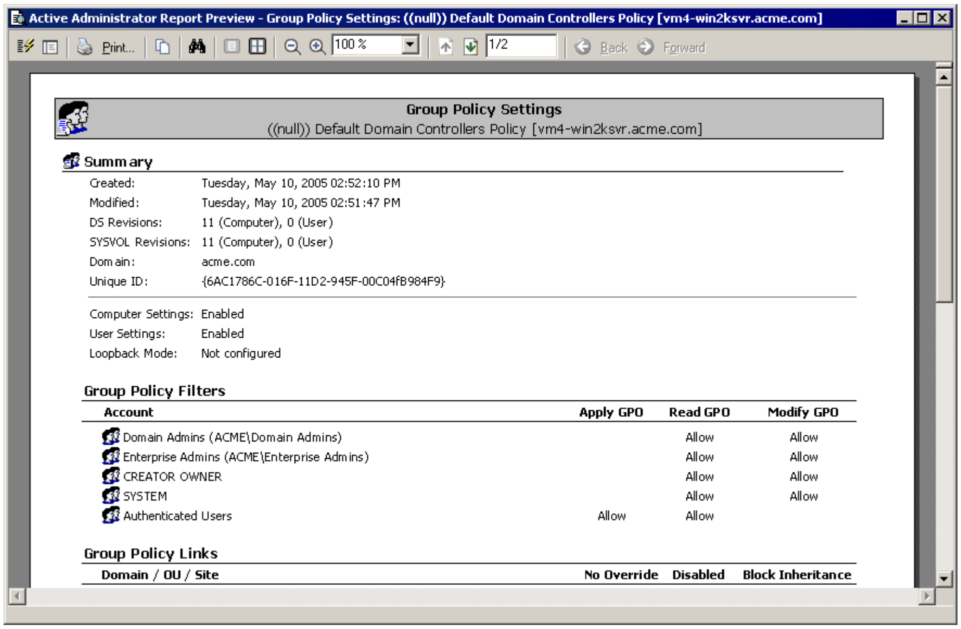
3. In the **GPOs** list, expand the hierarchy, and select a GPO. The **GPO History** list displays the versions, which are ordered by date of when the changes were made. You can view the revisions of the GPO, who made the changes, and on which domain controller the change was made. You can add a comment to the version by typing text in the box, and then clicking **Save Comment**.

REPORTING ON GROUP POLICY HISTORY

You may wish to see a report showing the exact settings of a Group Policy Object (GPO) as they were at a previous time in history.

1. From the Active Administrator Console, open the **Group Policy History** tab.
2. In the GPOs list, select a GPO. The versions display in the **GPO History** list.
3. In the GPO list, double-click a version. The **Report Preview** window displays the **Group Policy Settings** report.

   Note: You also can select a version, and then click **Report**; or right-click a version, and then choose **Report**.


Active Administrator Report Preview - Group Policy Settings: ((null)) Default Domain Controllers Policy [vm4-win2ksvr.acme.com]
Print...
100 %
1/2
Back
Forward

Group Policy Settings
((null)) Default Domain Controllers Policy [vm4-win2ksvr.acme.com]

Summary

Created:	Tuesday, May 10, 2005 02:52:10 PM
Modified:	Tuesday, May 10, 2005 02:51:47 PM
DS Revisions:	11 (Computer), 0 (User)
SYSVOL Revisions:	11 (Computer), 0 (User)
Domain:	acme.com
Unique ID:	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Computer Settings:	Enabled
User Settings:	Enabled
Loopback Mode:	Not configured

Group Policy Filters

Account	Apply GPO	Read GPO	Modify GPO
Domain Admins (ACME\Domain Admins)		Allow	Allow
Enterprise Admins (ACME\Enterprise Admins)		Allow	Allow
CREATOR OWNER		Allow	Allow
SYSTEM		Allow	Allow
Authenticated Users	Allow	Allow	

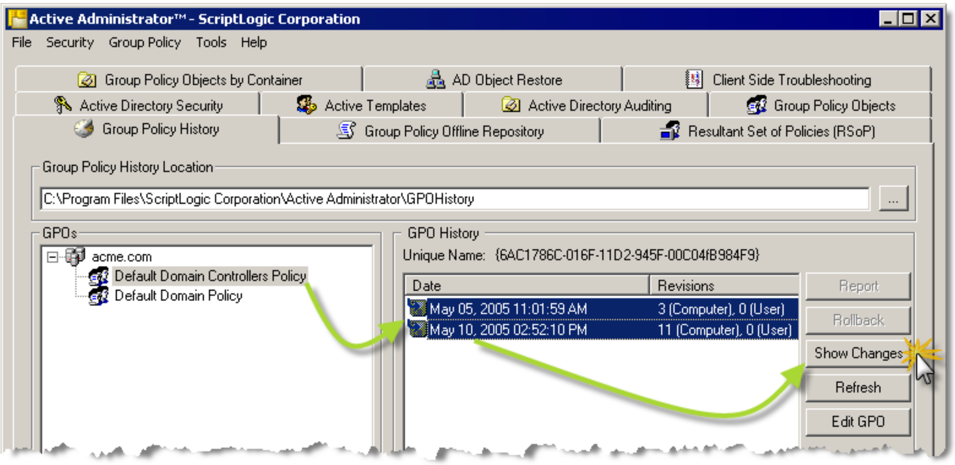
Group Policy Links

Domain / OU / Site	No Override	Disabled	Block Inheritance

COMPARING HISTORY ON GROUP POLICY OBJECTS

You may be interested in the differences between two historical versions of a Group Policy object (GPO) to see exactly what changes were made between two points in time.

1. From the Active Administrator Console, open the **Group Policy History** tab.
2. In the **GPOs** list, select a GPO. The versions display in the **GPO History** list.
3. In the **GPO History** list, select any two versions, and then click **Show Changes**; or right-click the selection, and then choose **Show Changes**.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy History Location
...
GPOs
GPO History
Report
Rollback
Show Changes
Refresh
Edit GPO

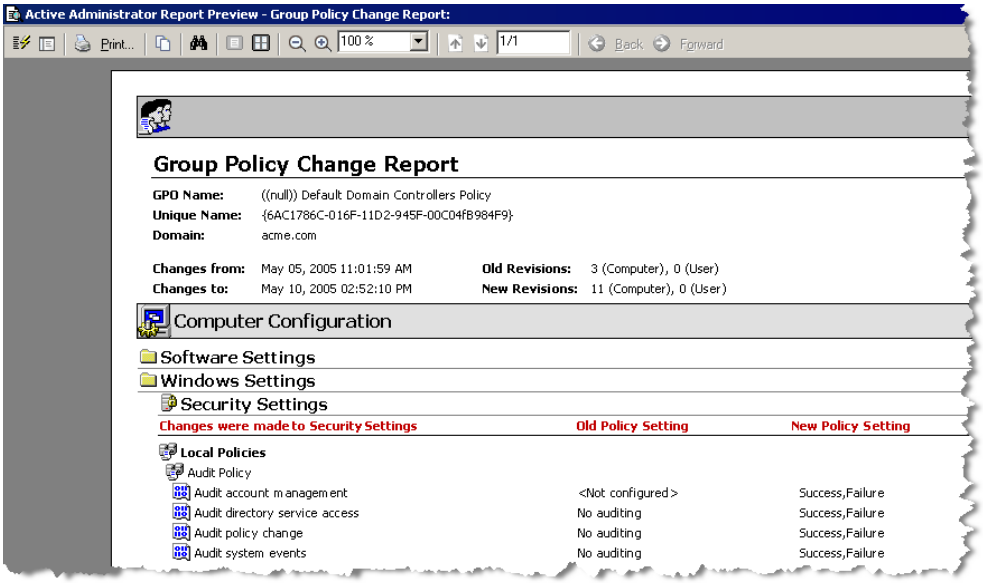
Group Policy History Location: C:\Program Files\ScriptLogic Corporation\Active Administrator\GPOHistory

GPOs:
- acme.com
  - Default Domain Controllers Policy
  - Default Domain Policy

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

Date	Revisions
May 05, 2005 11:01:59 AM	3 (Computer), 0 (User)
May 10, 2005 02:52:10 PM	11 (Computer), 0 (User)

The **Report Preview** window displays the Group Policy Change Report.


Active Administrator Report Preview - Group Policy Change Report:
Print...
100 %
1/1
Back
Forward

Group Policy Change Report

GPO Name:	((null)) Default Domain Controllers Policy		
Unique Name:	{6AC1786C-016F-11D2-945F-00C04fB984F9}		
Domain:	acme.com		
Changes from:	May 05, 2005 11:01:59 AM	**Old Revisions:**	3 (Computer), 0 (User)
Changes to:	May 10, 2005 02:52:10 PM	**New Revisions:**	11 (Computer), 0 (User)

Computer Configuration

Software Settings

Windows Settings

Security Settings

Changes were made to Security Settings	Old Policy Setting	New Policy Setting
Local Policies		
Audit Policy		
Audit account management	<Not configured>	Success,Failure
Audit directory service access	No auditing	Success,Failure
Audit policy change	No auditing	Success,Failure
Audit system events	No auditing	Success,Failure

ROLLING BACK TO A PREVIOUS VERSION

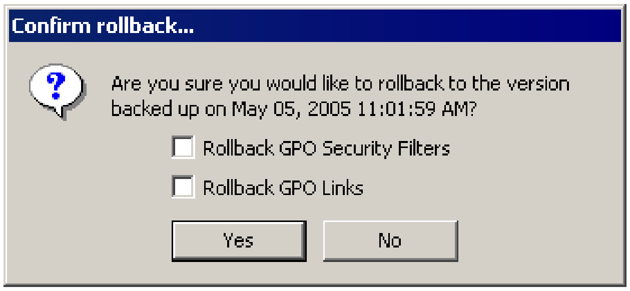
If you notice changes that were not supposed to occur, you can roll back to a previous version of the Group Policy object (GPO). Rolling back causes the GPO to be set back in time to the exact settings as they were at a previous date.

Note: You might want to view the Group Policy settings of the previous version before you select it for rollback. See *Reporting on Group Policy History*.

1. From the Active Administrator Console, open the **Group Policy History** tab.
2. In the **GPOs** list, select the GPO to roll back. The versions display in the **GPO History** list.

   Note: If you want to make changes to the GPO before you select if for rollback, select the GPO version, and then click **Edit GPO**.

3. Select a version to roll back to, and then click **Rollback**. The **Confirm rollback** message box appears.

   Confirm rollback...

   Are you sure you would like to rollback to the version backed up on May 05, 2005 11:01:59 AM?

   □ Rollback GPO Security Filters

   □ Rollback GPO Links

4. Select if you want to roll back the **GPO Security Filters** and/or **GPO Links**, and then click **Yes**.

   Note: If the default domain policy is included in the version, a warning message displays. To overwrite the default, click **Yes**, otherwise, click **No**.

   When the rollback is complete, a message box appears.

5. Click **Yes** to close the message box.

   Note: Upon completion of the rollback, the list of GPO revisions increase by one to ensure that the GPO is applied the next time polices are refreshed.

Resultant Set of Policies (RSoP)

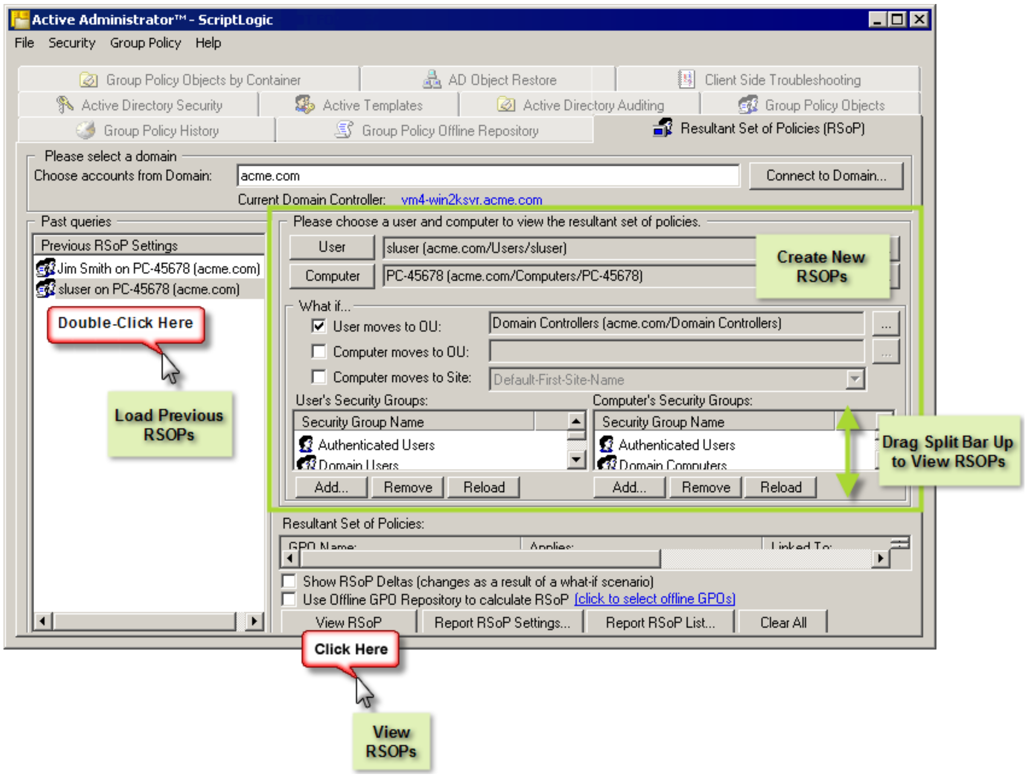
Active Administrator provides increased levels of manageability by way of a Resultant Set of Policies (RSoP) function, which allows you to select a user and computer and view or report on the Group Policy objects that affect those accounts. To get an exact picture of how your actions will affect Group Policy application, you can perform several calculations of what if scenarios, including the addition or removal of these objects from OUs, Sites, or Security Groups. This allows administrators to quickly view Group Policy Object application and errors on remote machines. Recent calculations are automatically saved for easy retrieval at a later time. Changes in RSoP calculations as a result of what-if scenarios can be seen by showing RSoP Deltas.

Reporting on Resultant Sets of Policies allow administrators to see exactly how objects are affected by Group Policy objects and quickly troubleshoot where application of Group Policies have not been correctly handled. Active Administrator provides clear and concise reports that not only show what Group Policy objects are applied, but the effective settings of such policies.

RUNNING A WHAT-IF SCENARIO

1. Start the Active Administrator Console, and then open the **Resultant Set of Policies (RSoP)** tab.

   Previous what-if scenarios display in the **Previous RSoP Settings** list. You can double-click a past query to load the RSoP settings.



Please select a domain

Choose accounts from Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Past queries

Previous RSoP Settings

- Jim Smith on PC-45678 (acme.com)
- sluser on PC-45678 (acme.com)

Please choose a user and computer to view the resultant set of policies.

User sluser (acme.com/Users/sluser)

Computer PC-45678 (acme.com/Computers/PC-45678)

What if...

☑ User moves to OU: Domain Controllers (acme.com/Domain Controllers)

☐ Computer moves to OU:

☐ Computer moves to Site: Default-First-Site-Name

User's Security Groups:

Security Group Name
Authenticated Users
Domain Users

Computer's Security Groups:

Security Group Name
Authenticated Users
Domain Computers

Resultant Set of Policies:

☐ Show RSoP Deltas (changes as a result of a what-if scenario)

☐ Use Offline GPO Repository to calculate RSoP (click to select offline GPOs)

Double-Click Here

Load Previous RSOPs

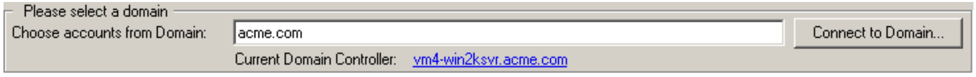
Create New RSOPs

Drag Split Bar Up to View RSOPs

Click Here

View RSOPs

2. Choose a domain and domain controller.



Please select a domain

Choose accounts from Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

- To choose a domain, type the domain name in the **Choose accounts from Domain** box or click **Connect to Domain**.
- To select a different server on the current domain to use in viewing RSoP results, click the **Current Domain Controller** hyperlink. The **Connect to Domain Controller** box opens where you can select a different domain controller.

3. Select a user and computer.

Important: Only users and computers that are contained in the list of licensed OUs can be selected. If you select a user or computer that is not within the scope of your license, you see an error message. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

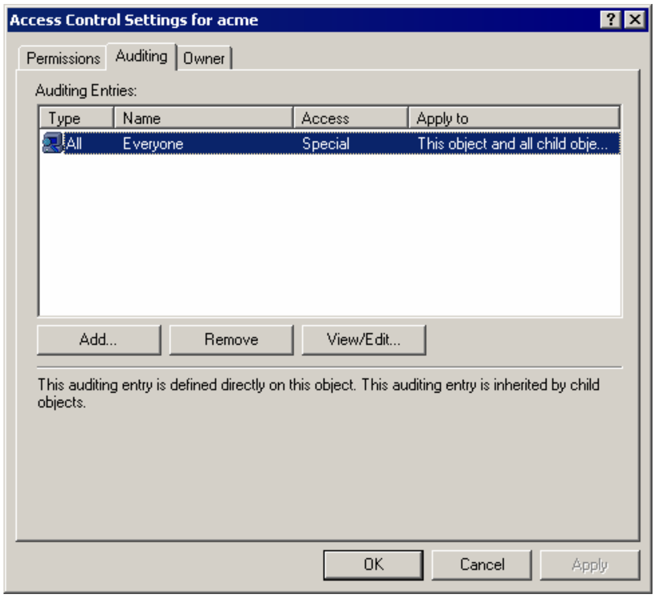
Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

45. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.

46. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.

47. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.

48. Open the **Auditing** tab.



Access Control Settings for acme

Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

49. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
50. From the **Apply onto** list, select **This object and all child objects,** if necessary.
51. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Delete**

☑ **Delete Subtree**

☑ **Modify Permissions**

☑ **Modify Owner**

☑ **All Validated Writes**

☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

52. Open the **Properties** tab.
53. From the **Apply onto** list, select **This object and all child objects,** if necessary.
54. In the **Access** list, select the **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Write Description**

☑ **Write flags**

☑ **Write gPLink**

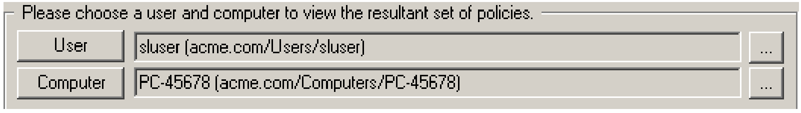
☑ **Write gPOptions**

☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

55. Click **OK.**

Resolving Licensing Issues.



Please choose a user and computer to view the resultant set of policies.

User sluser (acme.com/Users/sluser)

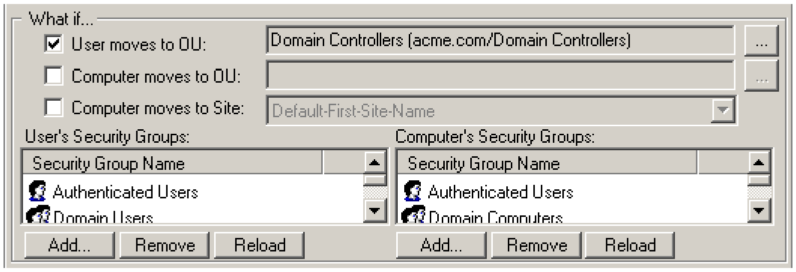
Computer PC-45678 (acme.com/Computers/PC-45678)

- To select a user, click **User** or …. The user's name displays in the box and the groups in which the user is a member display in the **User's Security Groups** list.

- To select a computer, click **Computer** or ... to select a computer. The computer name displays in the box and the groups in which the computer is a member display in the **Computer's Security Groups** list.

Note: The user or computer does not have to be a direct member of a listed group. If the user or computer belongs to a group that is a member of another group, that user or computer is a member of the parent group as well and is listed here.

4. In the **What if** area, set up your scenario.



What if...

☑ User moves to OU: Domain Controllers (acme.com/Domain Controllers)

☐ Computer moves to OU:

☐ Computer moves to Site: Default-First-Site-Name

User's Security Groups:

Security Group Name
Authenticated Users
Domain Users

Computer's Security Groups:

Security Group Name
Authenticated Users
Domain Computers

Note: At any time, you can clear the what-if scenario settings by clicking **Clear All**.

☑ User moves to OU

Requests what-if information based on the selected user account moving to a different OU. The **Select User OU** list box opens where you can select an OU. You also can click ... to open the **Select User OU** list box.

☑ Computer moves to OU

Requests what-if information based on the selected computer moving to a different OU. The **Select Computer OU** list box opens where you can select an OU. You also can click ... to open the **Select Computer OU** list box.

☑ Computer moves to Site

Requests what-if information based on the selected computer moving to a different site. Choose a site from the list.

User's Security Groups and Computer's Security Groups

Add or remove groups from the what-if scenario.

Button	Description
Add...	Add a group to the what if scenario
Remove	Remove a group from the what if scenario
Reload	Reload the groups of which the user or computer is currently a member

☑ Show RSoP Deltas (changes as a result of a what-if scenario)

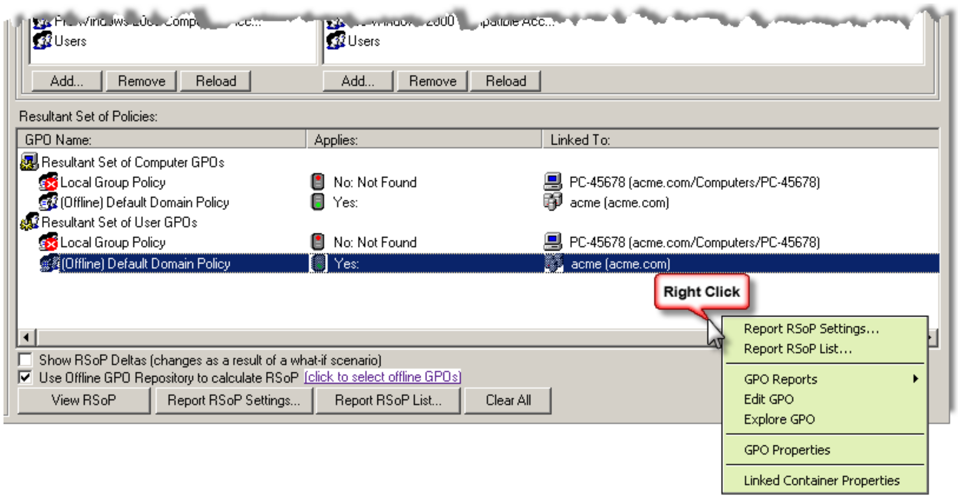
Displays only changes that would result if you applied the Group Policy.

☑ Use Offline GPO Repository to calculate RSoP (click to select offline GPOs)

Uses a GPO copy that is stored in the repository to calculate the RSoP. When you select this check box, a window opens where you can select a GPO that exists in the repository to use in the RSoP.

5. When you are finished setting up the what-if scenario, click **View RSoP**. The resultant set of policies displays.

Note: You can drag the split bar up to enlarge the **Resultant Set of Policies** area.



Resultant Set of Policies:

GPO Name:	Applies:	Linked To:
Resultant Set of Computer GPOs		
Local Group Policy	No: Not Found	PC-45678 (acme.com/Computers/PC-45678)
(Offline) Default Domain Policy	Yes:	acme (acme.com)
Resultant Set of User GPOs		
Local Group Policy	No: Not Found	PC-45678 (acme.com/Computers/PC-45678)
(Offline) Default Domain Policy	Yes:	acme (acme.com)

☐ Show RSoP Deltas (changes as a result of a what-if scenario)

☑ Use Offline GPO Repository to calculate RSoP (click to select offline GPOs)

Note: If you selected the **Use Offline GPO Repository to calculate RSoP** check box, the GPOs that you selected from the repository have **(Offline)** next to the name to indicate you are working with read-only copies of the GPOs that exist in the GPO Repository.

VIEWING GPO PROPERTIES

Note: If you are working with an offline version of the GPO, you are viewing the properties of the GPO as it exists in the GPO Offline Repository.

- To view properties, double-click an item in the list; or right-click an item, and then choose **GPO Properties** or **Linked Container Properties**.

REPORTING

- To view a complete report on the results of the what-if scenario, click **Report RSoP Settings**; or right-click an item, and then choose **Report RSoP Settings**.
- To view a summary report, click **Report RSoP List**; or right-click an item, and then choose **Report RSoP List**.
- To view reports on a GPO, right-click a GPO, point to **GPO reports**, and then select one of the following reports:

Report	Description
GPO Settings	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
GPO Affected Registry Keys	Shows the registry keys affected by the selected Group Policy object in the selected domain.

Note: If you are working with an offline version of the GPO, you are prompted to check out the GPO. Check in the GPO when you are done running reports. See *Editing a GPO Offline*.

EDITING A GPO

You can edit a GPO directly from the **Resultant Set of Policies (RSoP)** tab.

Note: If you are working with an offline version of the GPO, you are prompted to check out the GPO.

- Right-click a GPO, and then choose **Edit GPO**. The **Group Policy** window opens.

Note: If you are working with an offline version of the GPO, you are editing the GPO as it exists in the GPO Offline Repository. Once the GPO is edited, you must open the **Group Policy Offline Repository** tab to check in the GPO, and then export it to Active Directory. See *Editing a GPO Offline* and *Publishing GPO to Active Directory*.

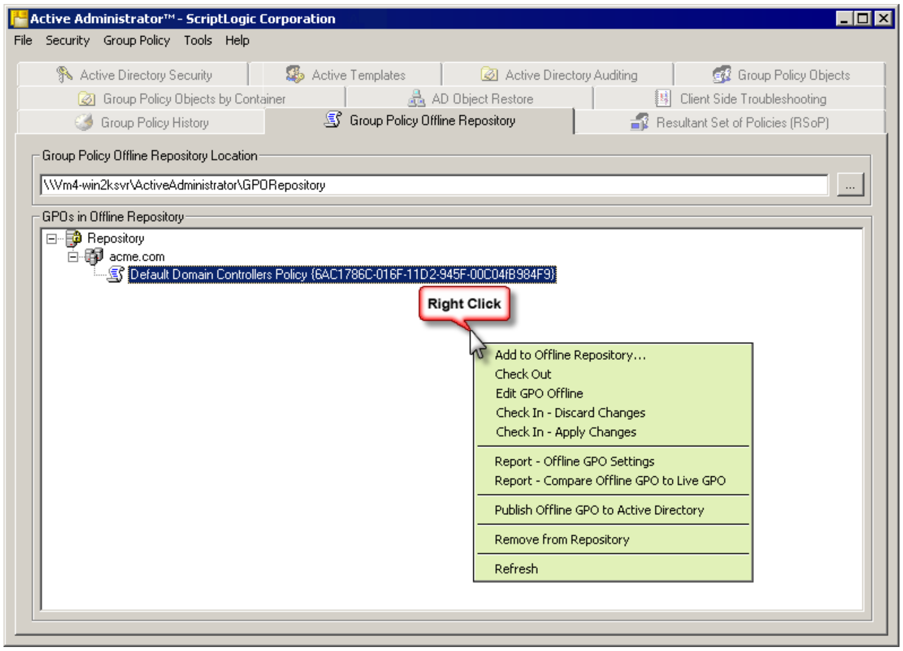
LOCATING A GPO

- Right-click a GPO, and then select **Explore GPO**. Microsoft Windows Explorer opens displaying the path to the GPO in the **Address** box and highlighting the GPO in the hierarchy.

Group Policy Offline Repository

Active Administrator provides an offline repository for editing Group Polices. Editing GPOs offline protects your users in the event a GPO is used at the same time it is changing. If an administrator wants to make changes to a GPO, the state of that GPO is indeterminate while the GPO is being changed. If the GPO is used while it is being edited, there is no way to know which changes, if any, to the GPO were actually applied to the object that used it.

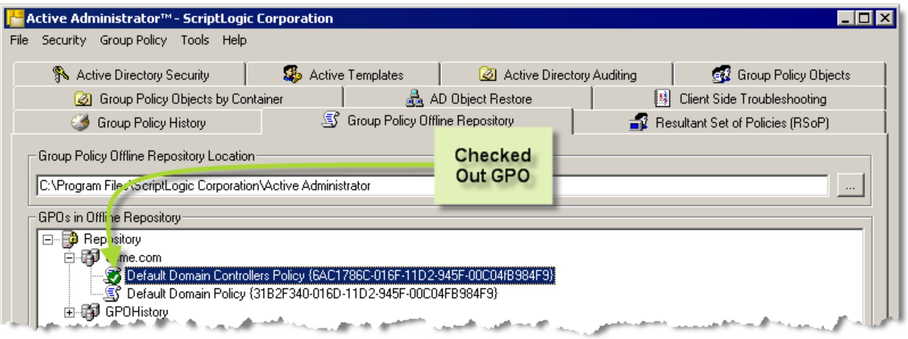
The offline repository makes a copy of the GPO that you can edit without interfering with the normal operation of Active Directory. When editing is complete, you can publish the changed GPO to Active Directory in a single operation. The eliminates the possibility of ambiguity in applying GPOs.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Offline Repository Location
GPOs in Offline Repository
Repository
acme.com
Right Click
Add to Offline Repository...
Check Out
Edit GPO Offline
Check In - Discard Changes
Check In - Apply Changes
Report - Offline GPO Settings
Report - Compare Offline GPO to Live GPO
Publish Offline GPO to Active Directory
Remove from Repository
Refresh

Group Policy Offline Repository Location: \\Vm4-win2ksvr\ActiveAdministrator\GPORepository

Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}

The offline repository uses a system of checking in and checking out to maintain the integrity of the GPO's in the repository. When a GPO is added to the repository, it is actually a copy of the GPO that gets added; the actual GPO is not affected. The copy in the repository can then be checked out and changed, and then checked in and applied when needed. When a GPO is published from the repository, a copy of the GPO is then copied over the online GPO, thus effectively making any changes to that GPO live.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Checked Out GPO
Group Policy Offline Repository Location
GPOs in Offline Repository
Repository
acme.com
GPOHistory

Group Policy Offline Repository Location: C:\Program Files\ScriptLogic Corporation\Active Administrator

Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}
Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}

SETTING THE STARTING CONTAINER FOR OFFLINE GPOS

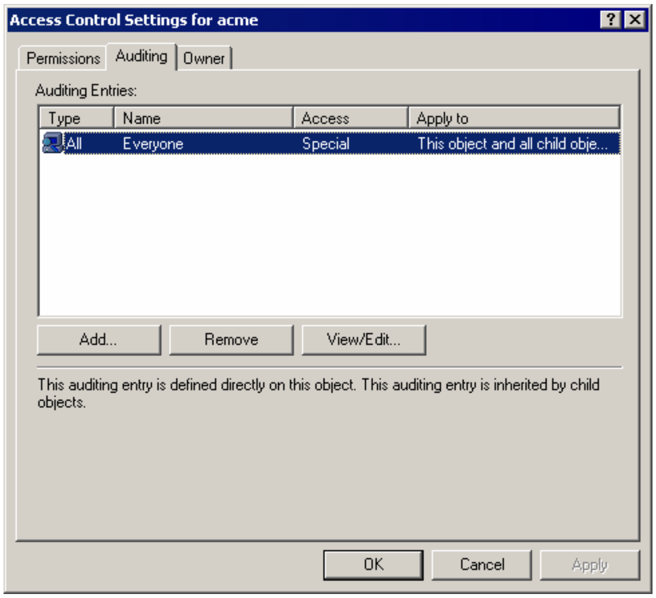
The System OU is the default starting container for storage of offline GPOs. If your license file restricts your access to some OUs (see *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

56. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
57. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
58. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.
59. Open the **Auditing** tab.



Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

60. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
61. From the **Apply onto** list, select **This object and all child objects,** if necessary.

62. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

- ☑ **Write All Properties**
- ☑ **Delete**
- ☑ **Delete Subtree**
- ☑ **Modify Permissions**
- ☑ **Modify Owner**
- ☑ **All Validated Writes**
- ☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)
- ☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

63. Open the **Properties** tab.

64. From the **Apply onto** list, select **This object and all child objects,** if necessary.

65. In the **Access** list, select the **Successful** checkboxes for the following:

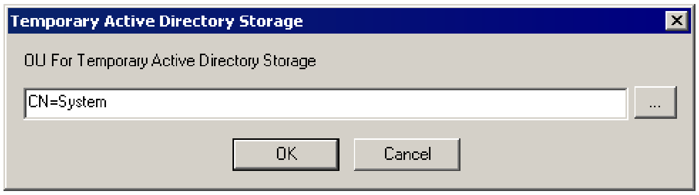
- ☑ **Write All Properties**
- ☑ **Write Description**
- ☑ **Write flags**
- ☑ **Write gPLink**
- ☑ **Write gPOptions**
- ☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

66. Click **OK.**

Resolving Licensing Issues), you need to set the starting OU for your Offline GPO Repository.

1. From the **Tools** menu, choose **Set Temporary Active Directory Location**. The Temporary Active Directory Storage box opens to the currently selected OU (CN=System is the default).



Temporary Active Directory Storage

OU For Temporary Active Directory Storage

CN=System

2. Click ..., choose an OU, and then click **OK**.

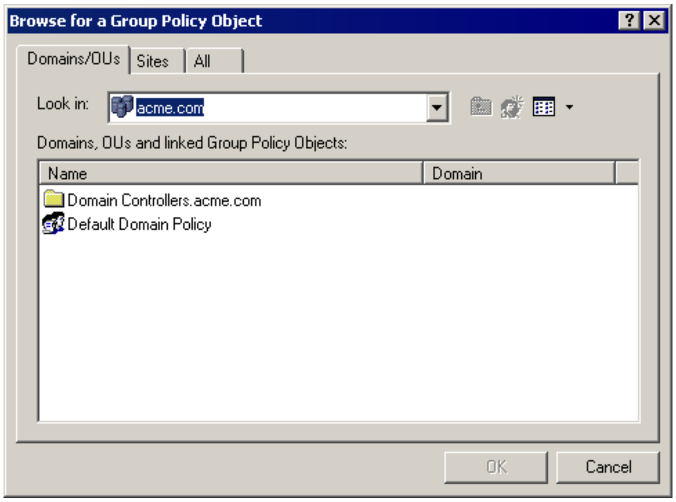
ADDING A GPO TO THE REPOSITORY

Note: You also can right-click a GPO in the **Group Policy Name** list on the **Group Policy Objects** tab, and then choose **Add to Offline Repository**. You may need to refresh the repository to see the GPO. Open the **Group Policy Offline Repository** tab, right-click an object, and then choose **Refresh**.

1. From the Active Administrator Console, open the **Group Policy Offline Repository** tab.
2. In the **Group Policy Offline Repository Location** box, type the path to where you want to store the repository, or click ... to locate a path.

   Note: During installation, Active Administrator creates the **GPORepository** folder, which is located in the Active Administrator installation directory.

3. To add a Group Policy to the repository, right-click an object in the GPOs in Offline Repository list, and then choose **Add to Offline Repository**. The **Browse for a Group Policy Object** box appears.


Browse for a Group Policy Object
Domains/OUs
Sites
All
Look in:
Domains, OUs and linked Group Policy Objects:
Name
Domain
OK
Cancel

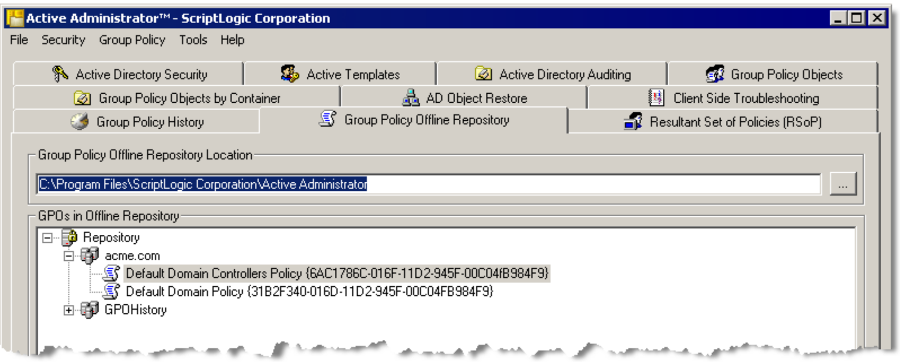
Look in: acme.com

Domain Controllers.acme.com
Default Domain Policy

Use the tabs to search for Group Policy Objects.

Tab	Description
Domains/OUs	Search Domains, Organization Units, and linked Group Policy Objects
Sites	Search Group Policy Objects linked to a site
All	Search all Group Policy Objects stored in a domain

4. Select a GPO, and then click **OK**. The GPO is listed under the domain where it resides. You may need to expand the hierarchy to locate the GPO.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Offline Repository Location
...
GPOs in Offline Repository

Group Policy Offline Repository Location: C:\Program Files\ScriptLogic Corporation\Active Administrator

Repository
acme.com
Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}
Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
GPOHistory

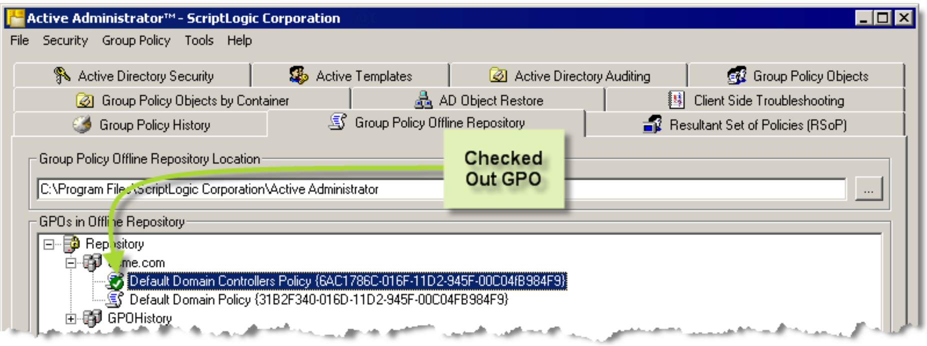
Once the GPO is in the repository, you can check it out for editing. See *Editing a GPO Offline*.

EDITING A GPO OFFLINE

Once GPO is in the repository, you can check it out for editing.

1. To check out a GPO, right-click the GPO, and then choose **Check Out**. A confirmation message appears. To continue with the check-out, click **Yes**.

   A green check mark appears next to the GPO to indicate that it is checked out as a copy. The original GPO is still available for use until you export your edits to Active Directory.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Offline Repository Location
GPOs in Offline Repository
Checked Out GPO

Group Policy Offline Repository Location: C:\Program File.\ScriptLogic Corporation\Active Administrator

GPOs in Offline Repository:
- Repository
  - ...me.com
    - ✓ Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}
    - Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
  - GPOHistory

Note: To cancel the checkout and restore the GPO to its original settings, right-click the GPO, and then choose **Check In – Discard Changes**.

2. In the **GPOs in Offline Repository** list, right-click a checked-out GPO, and then choose **Edit GPO Offline**. The **Group Policy** window opens.

   Note: If you do not have proper permissions to modify the Group Policy object you receive an access denied message.

3. Modify the GPO, and then close the window.

4. To check in the GPO, right-click the GPO, and then choose **Check In – Apply Changes**. A confirmation message appears. To continue with the check-in, click **Yes**. The GPO is made read-only in the repository. The change is not applied to the GPO until you publish it to Active Directory. See *Publishing GPO to Active Directory*.

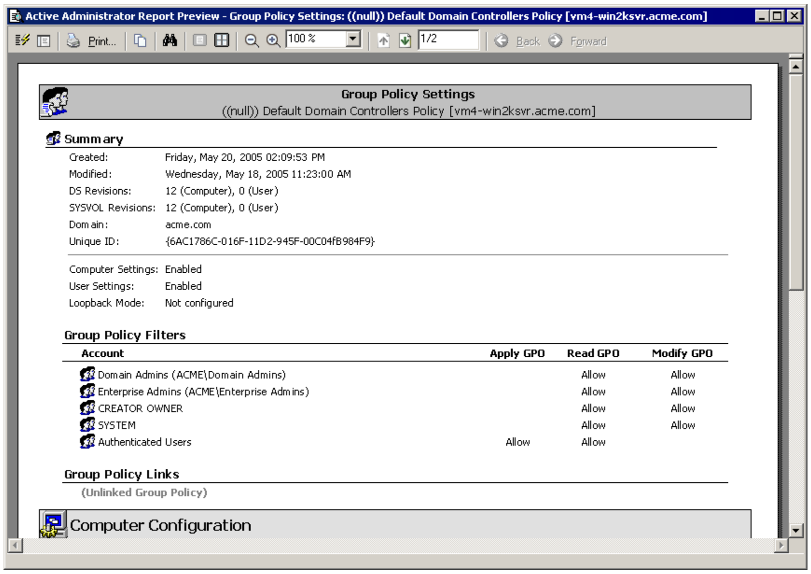
VIEWING GROUP POLICY SETTINGS

To help you manage the changes make to GPOs in the repository, Active Administrator offers two reports that show the settings of the GPO as it exists in the repository.

Group Policy Settings Report

You can create a report showing the settings on a selected GPO in the repository.

- Right-click a GPO, and then choose **Report – Offline GPO Settings**. The **Print Preview** window displays the settings of the GPO as it exists in the repository.



Active Administrator Report Preview - Group Policy Settings: ((null)) Default Domain Controllers Policy [vm4-win2ksvr.acme.com]

Group Policy Settings
((null)) Default Domain Controllers Policy [vm4-win2ksvr.acme.com]

Summary

Created:	Friday, May 20, 2005 02:09:53 PM
Modified:	Wednesday, May 18, 2005 11:23:00 AM
DS Revisions:	12 (Computer), 0 (User)
SYSVOL Revisions:	12 (Computer), 0 (User)
Domain:	acme.com
Unique ID:	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Computer Settings:	Enabled
User Settings:	Enabled
Loopback Mode:	Not configured

Group Policy Filters

Account	Apply GPO	Read GPO	Modify GPO
Domain Admins (ACME\Domain Admins)		Allow	Allow
Enterprise Admins (ACME\Enterprise Admins)		Allow	Allow
CREATOR OWNER		Allow	Allow
SYSTEM		Allow	Allow
Authenticated Users	Allow	Allow	

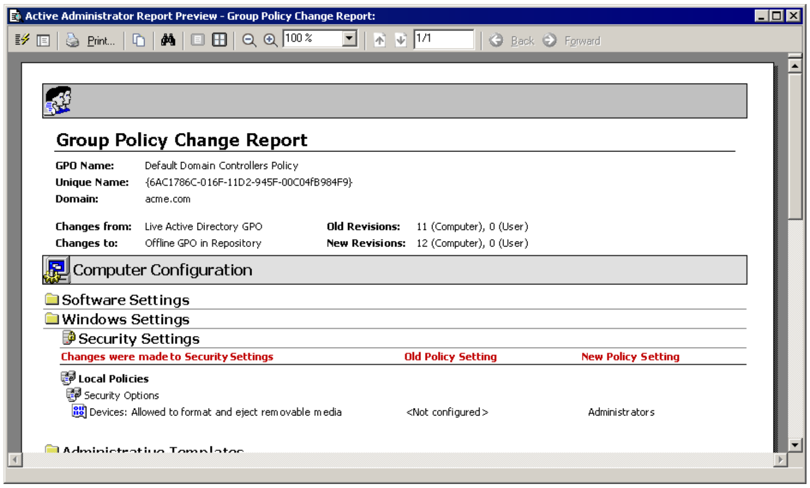
Group Policy Links
(Unlinked Group Policy)

Computer Configuration

Group Policy Change Report

You can create a report that shows the differences between the GPO as it exists in the repository and the GPO as it exists in Active Directory.

- Right-click a GPO, and then choose **Report - Compare Offline GPO to Live AD GPO**. The **Print Preview** window displays the differences in the settings between the GPO in the repository and Active Directory.



Active Administrator Report Preview - Group Policy Change Report:

Group Policy Change Report

GPO Name:	Default Domain Controllers Policy		
Unique Name:	{6AC1786C-016F-11D2-945F-00C04fB984F9}		
Domain:	acme.com		
Changes from:	Live Active Directory GPO	**Old Revisions:**	11 (Computer), 0 (User)
Changes to:	Offline GPO in Repository	**New Revisions:**	12 (Computer), 0 (User)

Computer Configuration

Software Settings

Windows Settings

Security Settings

Changes were made to Security Settings	Old Policy Setting	New Policy Setting
Local Policies		
Security Options		
Devices: Allowed to format and eject removable media	<Not configured>	Administrators

Administrative Templates

PUBLISHING GPO TO ACTIVE DIRECTORY

While the GPO is in the repository, it exists in a read-only state. To make a GPO live, you need to publish it to Active Directory.

Note: Prior to publishing the GPO, you may want to compare the settings of the GPO in the repository to those in Active Directory. See the *Group Policy Change Report*.

▶ Right-click a GPO, and then choose **Publish Offline GPO to Active Directory**.
A confirmation message appears. To continue, click **Yes**. A second confirmation message appears. To continue, click **Yes**.

REMOVING A GPO FROM THE REPOSITORY

Note: Removing a GPO from the repository does not remove it from the system. The GPO in the repository is a read-only copy of the GPO that resides in Active Directory.

▶ Right-click a GPO, and then choose **Remove from repository**. A confirmation message appears. To continue, click **Yes**.

AD Object Restore

Administrators can select a domain that contains Windows Server 2003 domain controllers and back up all Active Directory objects in that domain. When a situation occurs that requires an object to be restored, administrators can select the object from a list and restore either the object with all the attributes it possessed when it was backed up, or only attributes the administrator selects. In the case of a container object, administrators have the option of either restoring all objects it contains or all objects it contains of a particular type.

The preview and compare functions allow administrators to preview the object before it is restored or compare the attributes of the selected object in the archive with those of the same object in the Active Directory. Backups can either be scheduled or invoked interactively. Restores are interactive only.

Important: You must have a Windows 2003 domain controller to restore both attributes and objects to Active Directory. If you have a Windows 2000 domain controller, you can restore only attributes.

Important: While all objects are available for selection, you cannot restore an object that is not contained in at least one OU that is in the list of licensed OUs. If you attempt to restore an object that is not in the list of licensed OUs, you see an error message. No objects are restored. *See Setting Auditing Permissions*

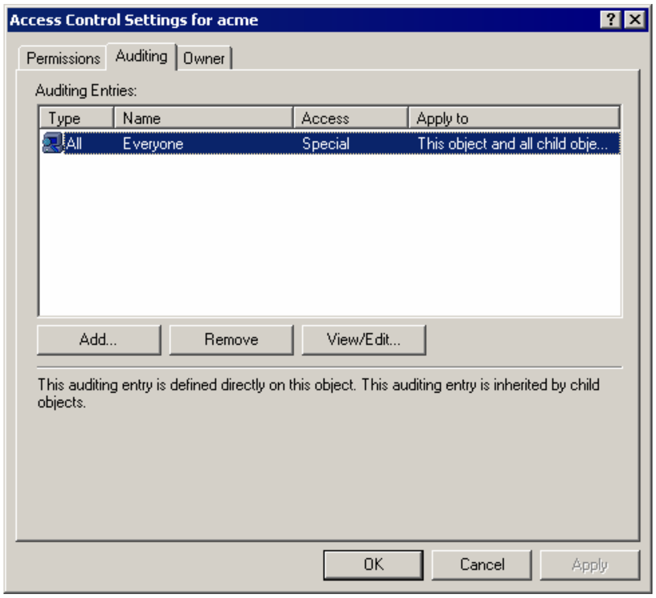
When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

67. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
68. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
69. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.

70. Open the **Auditing** tab.



Access Control Settings for acme

Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

71. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.

72. From the **Apply onto** list, select **This object and all child objects,** if necessary.

73. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Delete**

☑ **Delete Subtree**

☑ **Modify Permissions**

☑ **Modify Owner**

☑ **All Validated Writes**

☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

74. Open the **Properties** tab.

75. From the **Apply onto** list, select **This object and all child objects,** if necessary.

76. In the **Access** list, select the **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Write Description**

☑ **Write flags**

☑ **Write gPLink**

☑ **Write gPOptions**

☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

77. Click **OK.**

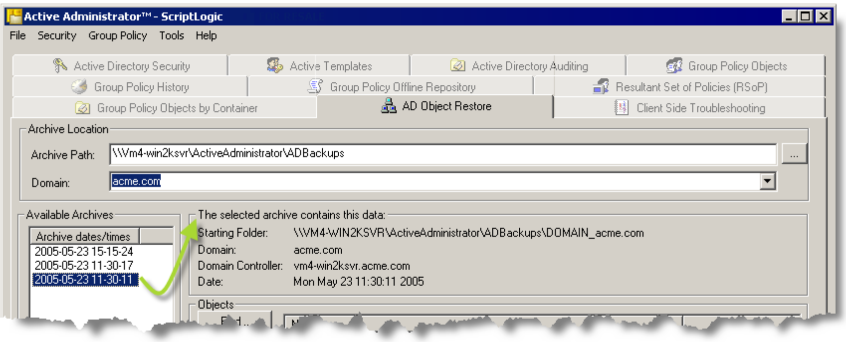
Resolving Licensing Issues.

SELECTING AN ARCHIVE TO RESTORE

1. From the Active Administrator Console, open the **AD Object Restore** tab.
2. In the **Archive Path** box, type the path to the folder where the archive files are stored, or click ... to locate the folder.

Note: The archive files are in a folder whose name begins with **DOMAIN_**. Do not browse to that folder; browse instead to that folder's parent.

3. From the **Domain** list, select a domain name. The **Available Archives** list shows the dates and times of backups performed on that domain.
4. From the **Available Archives** list, select an archive. The selected archive contains this data area displays information about the selected archive file.


Active Administrator™ - ScriptLogic
File Security Group Policy Tools Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Archive Location
...
Available Archives
Archive dates/times
Objects

Archive Path: \\Vm4-win2ksvr\ActiveAdministrator\ADBackups

Domain: acme.com

2005-05-23 15-15-24
2005-05-23 11-30-17
2005-05-23 11-30-11

The selected archive contains this data:

Starting Folder: \\VM4-WIN2KSVR\ActiveAdministrator\ADBackups\DOMAIN_acme.com
Domain: acme.com
Domain Controller: vm4-win2ksvr.acme.com
Date: Mon May 23 11:30:11 2005

The next step is to locate objects within the archive file to restore. You can find objects by searching the archive file or browsing the hierarchical structure of the archive file.

FINDING OBJECTS IN AN ARCHIVE FILE

You can use search criteria to locate objects in an archive file.

1. After selecting an archive file to restore, click **Find**. The **Find Objects to Restore** dialog box opens. The **Select Objects of This Type** list shows types of objects that may have been backed up.

Note: All types is selected by default. If you click **Find Now** without adding any other search criteria, all object types in the archive file are located.

2. To search for a specific object type, select a type from the **Select Objects of this type** list.

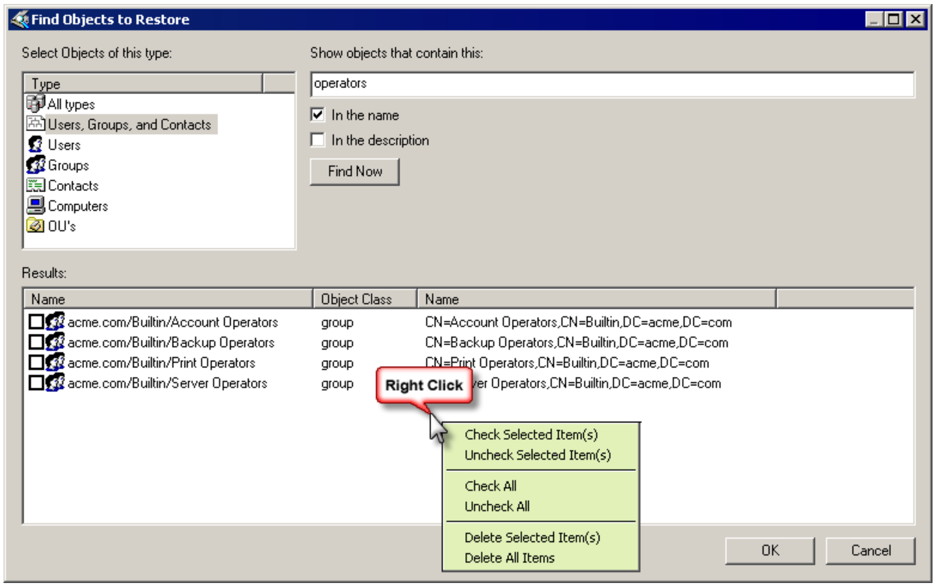
3. To search for a specific object, type search criteria in the **Show objects that contain this** box.

   - To search for objects of the selected type with the specified string of characters in the name, select the **In the name** check box.

   - To search for objects of the selected type with the specified string of characters in the description, select the **In the description** check box.

   Note: If both check boxes are selected, only objects that have the specified string of characters in both the name and the description are added to the **Results** list.

4. To begin the search, click **Find Now**. When the search is complete, objects that meet the specified criteria display in the **Results** list.



Find Objects to Restore

Select Objects of this type:

Type
All types
Users, Groups, and Contacts
Users
Groups
Contacts
Computers
OU's

Show objects that contain this: operators

☑ In the name

☐ In the description

Results:

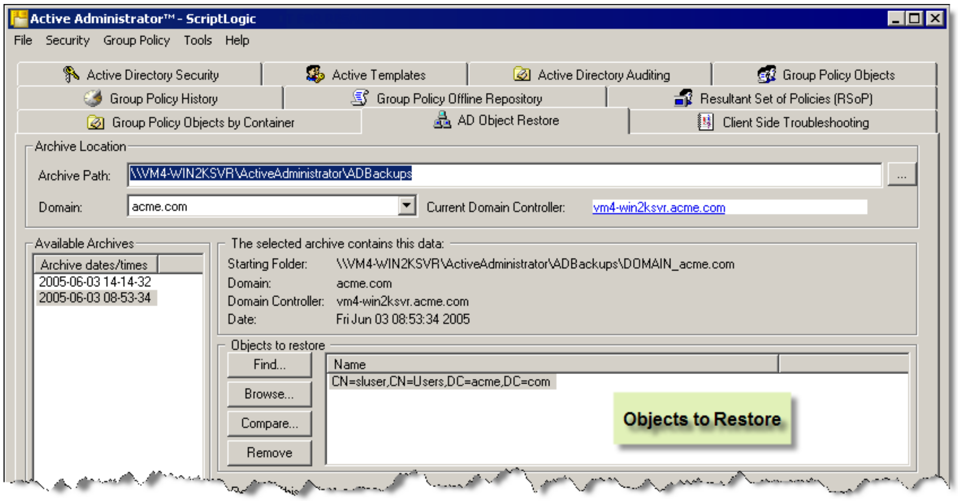
Name	Object Class	Name
☐ acme.com/Builtin/Account Operators	group	CN=Account Operators,CN=Builtin,DC=acme,DC=com
☐ acme.com/Builtin/Backup Operators	group	CN=Backup Operators,CN=Builtin,DC=acme,DC=com
☐ acme.com/Builtin/Print Operators	group	CN=Print Operators,CN=Builtin,DC=acme,DC=com
☐ acme.com/Builtin/Server Operators	group	ver Operators,CN=Builtin,DC=acme,DC=com

5. In the **Results** list, select the objects to restore.

   Note: There is a right-click menu on the results list. All of the selected items may be checked or unchecked, all of the items in the list may be checked or unchecked, the selected items in the list may be deleted, or all of the items in the list may be deleted.

   Note: Deleting objects from this list does not affect objects in the archive file or the Active Directory.

6. To add the selected objects to the **Objects** list, click **OK**.


Active Administrator™ - ScriptLogic
File Security Group Policy Tools Help
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
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
Objects to Restore

Archive Location

Archive Path: \\VM4-WIN2KSVR\ActiveAdministrator\ADBackups

Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Available Archives

Archive dates/times
2005-06-03 14-14-32
2005-06-03 08-53-34

The selected archive contains this data:

Starting Folder: \\VM4-WIN2KSVR\ActiveAdministrator\ADBackups\DOMAIN_acme.com
Domain: acme.com
Domain Controller: vm4-win2ksvr.acme.com
Date: Fri Jun 03 08:53:34 2005

Objects to restore

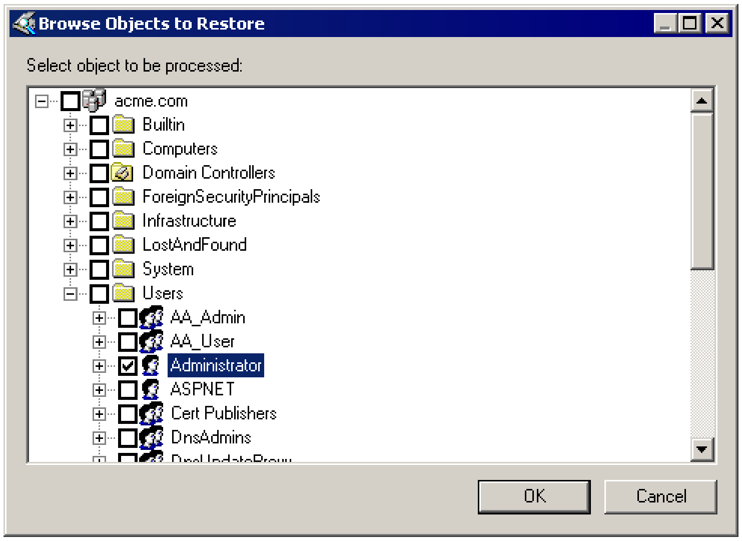
Name
CN=sluser,CN=Users,DC=acme,DC=com

Important: You must have a Windows 2003 domain controller to restore both attributes and objects to Active Directory. If you have a Windows 2000 domain controller, you can restore only attributes.

BROWSING FOR AN OBJECT IN AN ARCHIVE FILE

You can navigate through the hierarchical structure of the archive file to select an object to restore.

1. After selecting an archive file to restore, click **Browse**. The **Browse Objects to Restore** box opens.



Select object to be processed:

- □ acme.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ LostAndFound
  - □ System
  - □ Users
    - □ AA_Admin
    - □ AA_User
    - ☑ Administrator
    - □ ASPNET
    - □ Cert Publishers
    - □ DnsAdmins
    - □ DnsUpdateProxy

2. Locate and select the object to restore, and then click **OK**. The selected object appears in the **Objects** list.

COMPARING ARCHIVED OBJECTS TO ACTIVE DIRECTORY

Before restoring an archived object, you might want to compare the attributes with those of the same object in the Active Directory.

1. Select an object in the **Objects** list, and then click **Compare**. The **Compare Attributes** window appears.
2. In the **Attributes to Display** area, select which attributes to view.

   ◉ **Only attributes that differ**
   Select to show only the attributes whose values are different in the archived file and Active Directory.

   ◉ **Only attributes that are the same**
   Select to show only the attributes whose values are the same in the archived file and Active Directory.

   ◉ **Show all attributes**
   Select to show all the attributes in the archived file and Active Directory.
3. Click **Refresh**.

RESTORING AN ARCHIVED OBJECT

After you select the archive file and locate the object to restore, either by finding or browsing for an object, the selected object displays in the **Objects** area. Before restoring the object, you can compare the archived version to the current version.

Important: You must have a Windows 2003 domain controller to restore both attributes and objects to Active Directory. If you have a Windows 2000 domain controller, you can restore only attributes.

Important: If you choose to restore an entire domain, back up your system before initiating the restore process. Restoring an entire domain is not a supported operation.

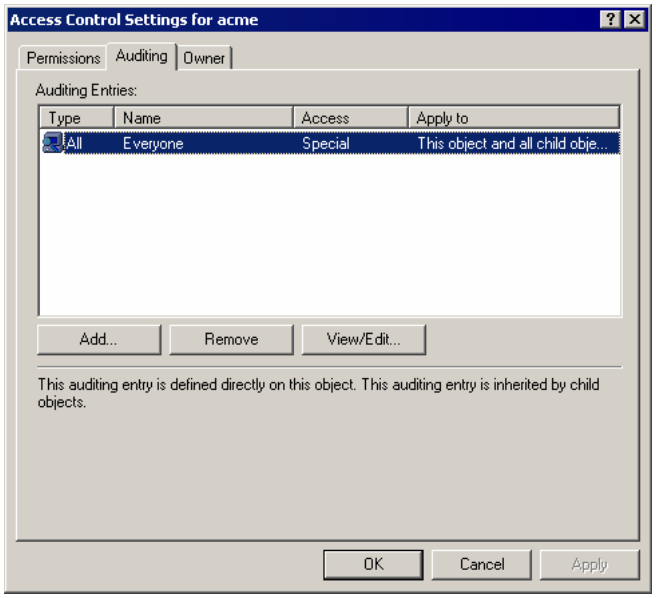
Important: While all objects are available for selection, you cannot restore an object that is not contained in at least one OU that is in the list of licensed OUs. If you attempt to restore an object that is not in the list of licensed OUs, you see an error message. No objects are restored. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

78. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.
79. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.
80. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.
81. Open the **Auditing** tab.


Access Control Settings for acme

Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

82. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.
83. From the **Apply onto** list, select **This object and all child objects,** if necessary.
84. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Delete**

☑ **Delete Subtree**

☑ **Modify Permissions**

☑ **Modify Owner**

☑ **All Validated Writes**

☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

85. Open the **Properties** tab.
86. From the **Apply onto** list, select **This object and all child objects,** if necessary.
87. In the **Access** list, select the **Successful** checkboxes for the following:

☑ **Write All Properties**

☑ **Write Description**

☑ **Write flags**

☑ **Write gPLink**

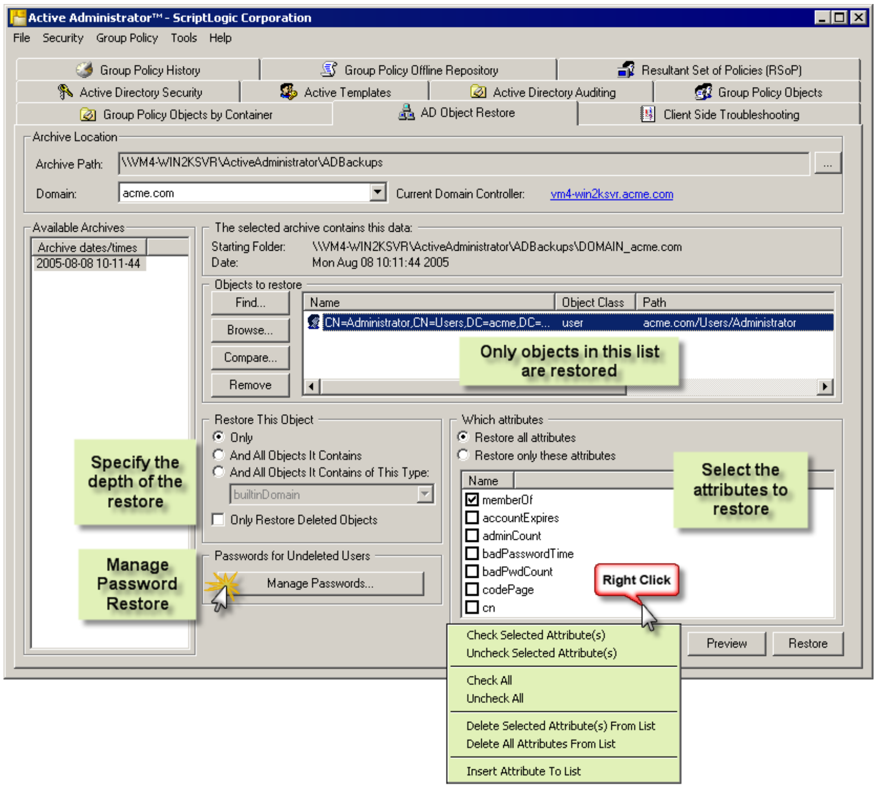
☑ **Write gPOptions**

☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

88. Click **OK.**

Resolving Licensing Issues.



Active Administrator™ - ScriptLogic Corporation
File Security Group Policy Tools Help
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Archive Location
Available Archives
Archive dates/times
Objects to restore
Find...
Browse...
Compare...
Remove
Name
Object Class
Path
Restore This Object
Which attributes
Passwords for Undeleted Users
Manage Passwords...
Check Selected Attribute(s)
Uncheck Selected Attribute(s)
Check All
Uncheck All
Delete Selected Attribute(s) From List
Delete All Attributes From List
Insert Attribute To List
Preview
Restore

Archive Path: \\VM4-WIN2KSVR\ActiveAdministrator\ADBackups

Domain: acme.com Current Domain Controller: vm4-win2ksvr.acme.com

2005-08-08 10-11-44

The selected archive contains this data:
Starting Folder: \\VM4-WIN2KSVR\ActiveAdministrator\ADBackups\DOMAIN_acme.com
Date: Mon Aug 08 10:11:44 2005

Name	Object Class	Path
CN=Administrator,CN=Users,DC=acme,DC=...	user	acme.com/Users/Administrator

● Only
○ And All Objects It Contains
○ And All Objects It Contains of This Type:
builtinDomain
□ Only Restore Deleted Objects

● Restore all attributes
○ Restore only these attributes

Name
☑ memberOf
□ accountExpires
□ adminCount
□ badPasswordTime
□ badPwdCount
□ codePage
□ cn

Only objects in this list are restored

Specify the depth of the restore

Manage Password Restore

Select the attributes to restore

Right Click

Removing Objects from the List

Note: Only the objects that are listed in the **Objects** area are restored.

- To remove selected object(s) from the list, click **Remove**.

Specifying Attributes to Restore

If only one object is selected in the **Objects** area, select the attributes to restore in the **Which attributes** area.

Note: The **Which Attributes** area is enabled when only one object is listed in the **Objects** area.

● Restore all attributes

Restores all attributes for the specified object (default).

● Restore only these attributes

Restores only the attributes selected in the list.

Specifying How to Restore the Attributes

Select how to restore the attributes specified in the **Which Attributes** area.

● Only

Restores the specified attributes only for the selected object (default).

● And All Objects it Contains

If the selected object is a container, the specified attributes for objects contained by the selected object are restored.

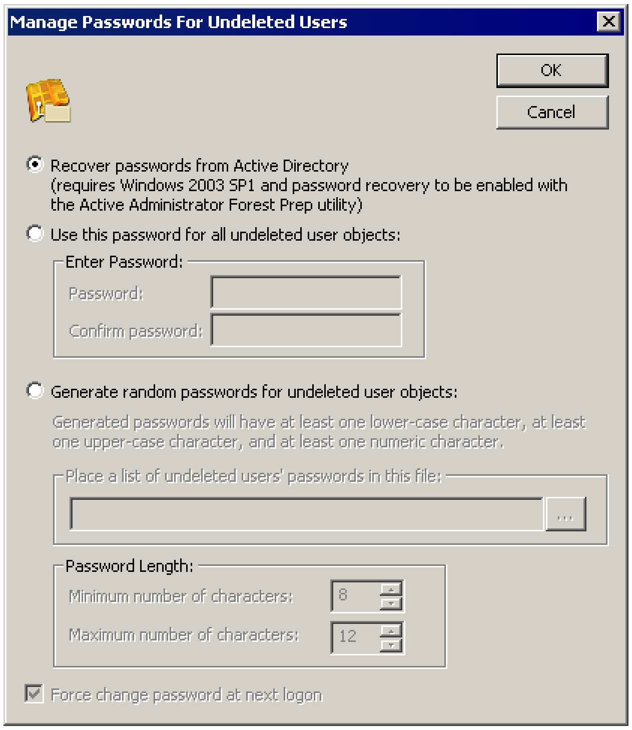
● And All Objects it Contains of This Type

If the selected object is a container, the specified attributes for objects of the selected type contained by the selected object are restored.

Resetting a User's Password

When restoring a user that was deleted previously, you can enter a new password and force them to reset the password when they first log on.

▶ Click **Manage Passwords**. The **Manage Passwords for Undeleted Users** dialog box opens.



Manage Passwords For Undeleted Users

OK

Cancel

● Recover passwords from Active Directory
(requires Windows 2003 SP1 and password recovery to be enabled with the Active Administrator Forest Prep utility)

○ Use this password for all undeleted user objects:

Enter Password:

Password:

Confirm password:

○ Generate random passwords for undeleted user objects:

Generated passwords will have at least one lower-case character, at least one upper-case character, and at least one numeric character.

Place a list of undeleted users' passwords in this file:

...

Password Length:

Minimum number of characters: 8

Maximum number of characters: 12

☑ Force change password at next logon

● Recover passwords from Active Directory

Select to use passwords stored in Active Directory. The server must be running Windows Server 2003 Service Pack 1 and password recovery must be enabled through the Active Administrator Forest Prep Utility.

- To enable password recovery, click **Start**, point to **Programs** > **ScriptLogic Corporation** > **Active Administrator**, and then choose **Forest Prep Utility**. Select the domain, and then click **Modify Schema to Allow the Restoration of Passwords**. See the *Getting Started Guide* for more information.

○ Use this password for all undeleted user objects.

Select to type a password in the **Password** and **Confirm Password boxes** (default).

○ Generate random passwords for undeleted user objects.

Select to let Active Administrator generate passwords. Click ... to create a text file in which to record the passwords that are generated. You can change the minimum and maximum number of characters in the password. Each password has at least one lower-case character, one upper-case character, and one numeric character.

☑ Force change password at next logon

Forces the user to change their password once they log on with the password you specified here (default).

Initiating the Restore Process

Important: If you attempt to restored an object that is not in the list of licensed OUs, you see an error message. No objects are restored. See *Setting Auditing Permissions*

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

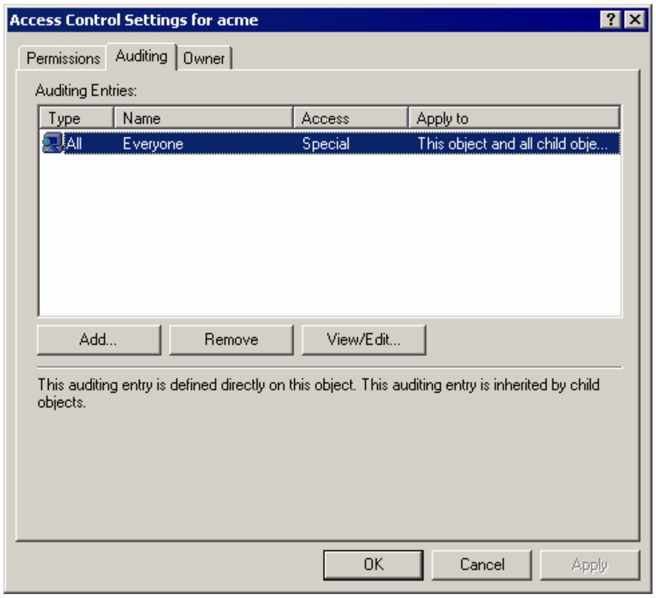
Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

89. Click **Start,** point to **Programs > ScriptLogic Corporation > Active Administrator,** and then select **Active Administrator Console.** The **Active Administrator Console** opens to the **Active Directory Security** tab.

90. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties.** The **Properties** box for the root domain object opens to the **General** tab.

91. Open the **Security** tab, and then click **Advanced.** The **Access Control Settings** box opens to the **Permissions** tab.

92. Open the **Auditing** tab.



Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add.**
- To remove a selected group/user, click **Remove.**
- To modify a selected group/user, click **View/Edit.**

If you clicked **Add** or **View/Edit,** the **Select User, Computer, or Group** box opens.

93. In the **Name** box, type the account name or select one from the list, and then click **OK.** The **Auditing Entry** box opens.

94. From the **Apply onto** list, select **This object and all child objects,** if necessary.

95. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

    ☑ **Write All Properties**

    ☑ **Delete**

    ☑ **Delete Subtree**

    ☑ **Modify Permissions**

    ☑ **Modify Owner**

    ☑ **All Validated Writes**

    ☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)

    ☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

    Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

96. Open the **Properties** tab.

97. From the **Apply onto** list, select **This object and all child objects,** if necessary.

98. In the **Access** list, select the **Successful** checkboxes for the following:

    ☑ **Write All Properties**

    ☑ **Write Description**

    ☑ **Write flags**

    ☑ **Write gPLink**

    ☑ **Write gPOptions**

    ☑ **Write managedBy**

    Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

99. Click **OK.**

Resolving Licensing Issues.

- To check the object before you start the restore process, click **Preview**. The names and values of the attributes display.

- To start the restore process, click **Restore**.

  Note: You are not prompted for confirmation when you click **Restore**. The process starts immediately.

- To cancel the restore process, click **Cancel Operation.**

Troubleshooting

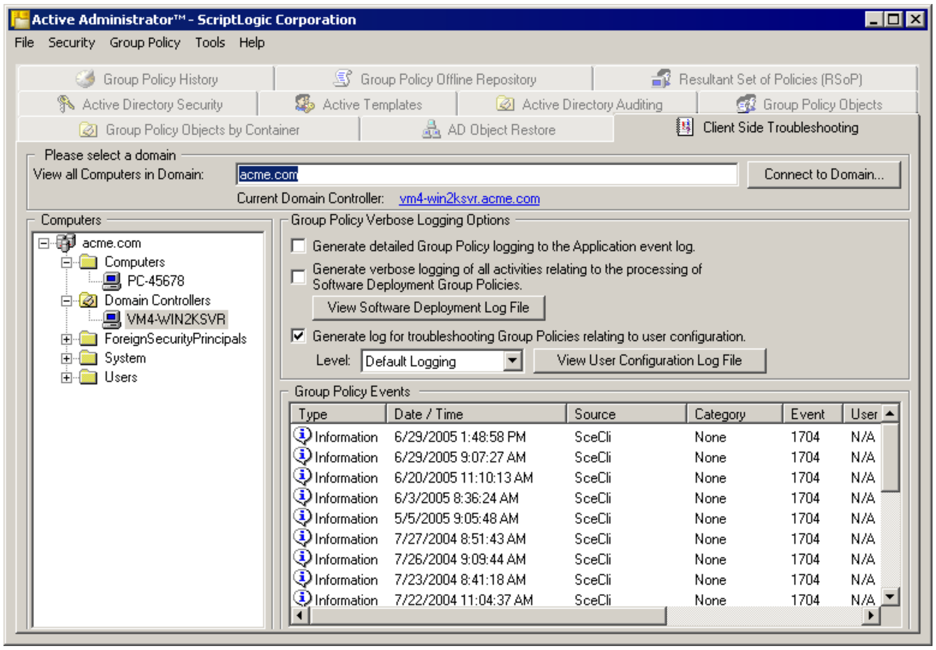
In its Knowledge Base, ScriptLogic Corporation has a library of articles that may provide an answer to a problem you are experiencing. Before calling technical support, check to see if your problem is documented here. You might also browse the Discussion Forums to see if anyone else is experiencing the same issue.

http://www.scriptlogic.com/support

CLIENT SIDE TROUBLESHOOTING

Active Administrator includes the ability to view event log entries on Windows 2000 and later client computers so administrators can quickly view Group Policy Object application and errors on remote machines. Client Side Troubleshooting provides several options to make management easier.

1. Start the Active Administrator Console, and then open the **Client Side Troubleshooting** tab.
2. If necessary, type the domain in the **View all Computers in Domain** box; or click **Connect to Domain** and choose a domain.
3. In the **Computers** list, select the computer whose logging options you want to set or logs you want to view.


Active Administrator™ - ScriptLogic Corporation
File
Security
Group Policy
Tools
Help
Group Policy History
Group Policy Offline Repository
Resultant Set of Policies (RSoP)
Active Directory Security
Active Templates
Active Directory Auditing
Group Policy Objects
Group Policy Objects by Container
AD Object Restore
Client Side Troubleshooting
Connect to Domain...
Computers
acme.com
Computers
PC-45678
Domain Controllers
VM4-WIN2KSVR
ForeignSecurityPrincipals
System
Users
View Software Deployment Log File
View User Configuration Log File

Please select a domain

View all Computers in Domain: acme.com

Current Domain Controller: vm4-win2ksvr.acme.com

Group Policy Verbose Logging Options

☐ Generate detailed Group Policy logging to the Application event log.

☐ Generate verbose logging of all activities relating to the processing of Software Deployment Group Policies.

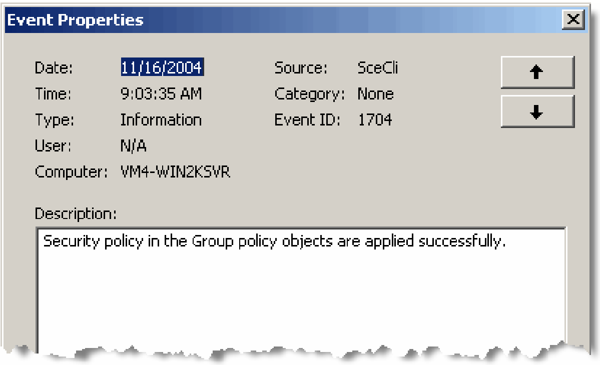
☑ Generate log for troubleshooting Group Policies relating to user configuration.

Level: Default Logging

Group Policy Events

Type	Date / Time	Source	Category	Event	User
Information	6/29/2005 1:48:58 PM	SceCli	None	1704	N/A
Information	6/29/2005 9:07:27 AM	SceCli	None	1704	N/A
Information	6/20/2005 11:10:13 AM	SceCli	None	1704	N/A
Information	6/3/2005 8:36:24 AM	SceCli	None	1704	N/A
Information	5/5/2005 9:05:48 AM	SceCli	None	1704	N/A
Information	7/27/2004 8:51:43 AM	SceCli	None	1704	N/A
Information	7/26/2004 9:09:44 AM	SceCli	None	1704	N/A
Information	7/23/2004 8:41:18 AM	SceCli	None	1704	N/A
Information	7/22/2004 11:04:37 AM	SceCli	None	1704	N/A

All Group Policy Events for the selected computer display in the **Group Policy Events** list. You can scroll to the right to view all the information or double-click a specific event to view its properties. You can then use the up and down arrows to scroll vertically though the Group Policy Events list.



Event Properties

Date: 11/16/2004 Source: SceCli
Time: 9:03:35 AM Category: None
Type: Information Event ID: 1704
User: N/A
Computer: VM4-WIN2KSVR

Description:
Security policy in the Group policy objects are applied successfully.

Setting Logging Options

☑ **Generate detailed Group Policy logging to the Application event log**
Select to enable detailed Group Policy logging to the Application log, which slows down the logon process and can affect the rate at which the Application log grows in size. Upon selecting this option, a warning message asks for your confirmation.

☑ **Generate verbose logging of all activities relating to the processing of Software Deployment Group Policies**
Enabling Group Policy Software Deployment logging slows down the logon process and generates an Appmgmt.log file that records the steps of the Group Policy Application Deployment component. Upon selecting this option, a warning message asks for your confirmation.

Note: To start logging, reboot the computer after selecting this option or have the user log off and then back on.

▶ To view the Appmgmt.log file, click **View Software Deployment Log File**.

☑ **Generate log for troubleshooting Group Policies relating to user configuration**
By default, Active Administrator generates a troubleshooting file. To enable detailed logging, select Verbose Logging from the Level list. Verbose Logging significantly increases the size of the UserEnv.log file on the target computer. Upon selecting this option, a warning message asks for your confirmation.

▶ To view the UserEnv.log file, click **View User Configuration Log File**.

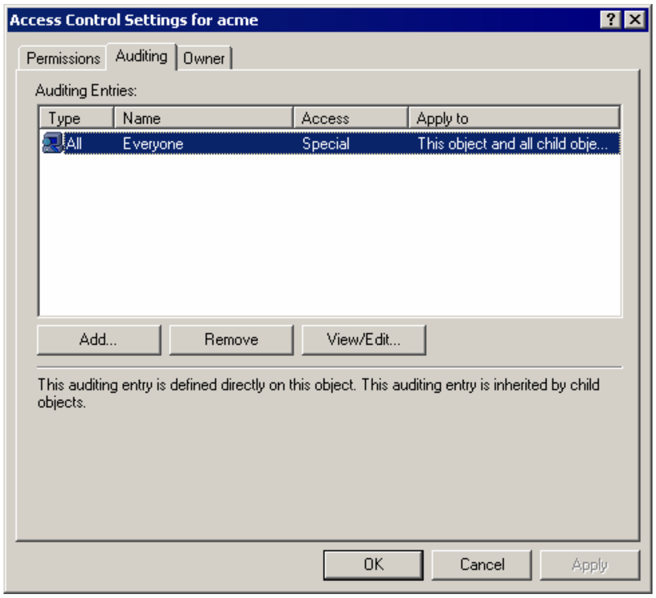
SETTING AUDITING PERMISSIONS

When you installed Active Administrator, you were prompted to enter a user name and password for a group/user with Domain Admin rights. Active Administrator set up the correct permissions for that group/user to access the database where the auditing data is stored.

In the event that you want to modify the group/user permissions, or something happened to alter those permissions, you can set the permissions manually.

Note: If you have not installed Active Administrator Console, you can use the Active Directory Users and Computers MMC snap-in.

100. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator**, and then select **Active Administrator Console**. The **Active Administrator Console** opens to the **Active Directory Security** tab.
101. Expand the hierarchical structure in the **Managed Servers** list, right-click the root of the domain, and then choose **Properties**. The **Properties** box for the root domain object opens to the **General** tab.
102. Open the **Security** tab, and then click **Advanced**. The **Access Control Settings** box opens to the **Permissions** tab.
103. Open the **Auditing** tab.



Type	Name	Access	Apply to
All	Everyone	Special	This object and all child obje...

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

- To add another group/user, click **Add**.
- To remove a selected group/user, click **Remove**.
- To modify a selected group/user, click **View/Edit**.

If you clicked **Add** or **View/Edit**, the **Select User, Computer, or Group** box opens.

104. In the **Name** box, type the account name or select one from the list, and then click **OK**. The **Auditing Entry** box opens.
105. From the **Apply onto** list, select **This object and all child objects**, if necessary.

106. In the **Access** list, select the ☑ **Successful** checkboxes for the following:

- ☑ **Write All Properties**
- ☑ **Delete**
- ☑ **Delete Subtree**
- ☑ **Modify Permissions**
- ☑ **Modify Owner**
- ☑ **All Validated Writes**
- ☑ **Create All Child Objects** (selects the checkboxes for all subsequent creates)
- ☑ **Delete All Child Objects** (selects the check boxes for all subsequent deletes)

Note: By default, Windows Server 2003 does not have these entries in the SACL. Windows 2000 has these entries configured, but it is a best practice to verify them before continuing.

107. Open the **Properties** tab.

108. From the **Apply onto** list, select **This object and all child objects**, if necessary.

109. In the **Access** list, select the **Successful** checkboxes for the following:

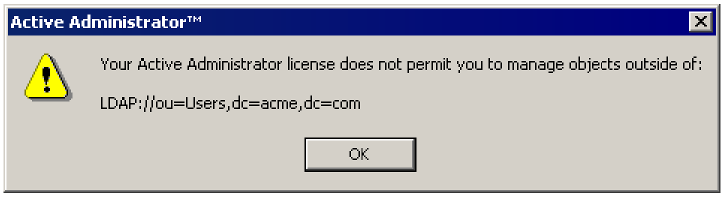
- ☑ **Write All Properties**
- ☑ **Write Description**
- ☑ **Write flags**
- ☑ **Write gPLink**
- ☑ **Write gPOptions**
- ☑ **Write managedBy**

Note: Because of the way ACLs on Directory Service objects work, you only need to set up the auditing once at the root of the domain. Child objects inherit these settings.

110. Click **OK**.

RESOLVING LICENSING ISSUES

Your license file may be specific to the organizational unit (OU) for which you purchased a license. If you attempt to perform an operation outside of the OU specified in the license file, you see an error message.



Active Administrator™

Your Active Administrator license does not permit you to manage objects outside of:

LDAP://ou=Users,dc=acme,dc=com

If you want to change the scope of the license file, contact your Sales account executive or Support Team specialist.

CHANGING THE ACCOUNT FOR E-MAIL NOTIFICATIONS

If the Active Administrator database exists on a server separate from the computer where the Event Notification service is running, the Active Administrator e-mail notifications may not function as intended. Since e-mail alerts are handled by the Active Administrator Event Notification service, the account that runs the service must have access to the database. By default the Active Administrator Event Notification Service runs as Local System.

One way to resolve this situation is to change the account that the Event Notification Service uses.

1. On the computer where the Event Notification service is running, click **Start**, point to **Programs > Administrative Tools**, and then choose **Services**. The Services applet opens.
2. Right-click the **Active Administrator Even Notification Service**, and then click **Properties**.
3. Open the **Log On** tab, and then specify the account to run the service.
4. Restart the service.

Alternatively, you can add the computer account to the AA_Admin group, which has access to the Active Administrator database. When the Active Administrator database is created, two groups are created: AA_Admin and AA_User. Depending on the options you selected during the creation of the database, these two groups may be local groups on the SQL server, Domain Local Groups, or Domain Groups.

- On the computer where the Event Notification service is running, open the AA_Admin group, and then add the computer account to the AA_Admin group. The service now run as Local System and can access the database.

REMOVING ACTIVE ADMINISTRATOR

Proper removal of Active Administrator can be achieved in a few ways. You can use the **Add/Remove Programs** control panel applet for a full removal. There are two programs that you remove:

- Active Administrator Console
- Active Administrator Server Setup

1. From the Windows Control Panel, double-click **Add/Remove Programs**. The **Add/Remove Programs** window opens.
2. From the list of currently installed programs, select **Active Administrator Console**.
3. Click **Remove**. A message box prompts you for confirmation.
4. To remove the application, click **Yes**. A status dialog box displays for the few seconds necessary to remove the application.
5. Repeat steps 2 through 4 for **Active Administrator Server Setup**.

After removal is complete, Active Administrator will have been removed from your system. The installation directory that contained Active Administrator remains after the process is complete. This directory contains the license file for the product and any files created after the product was installed. These may be deleted manually if you wish to completely remove Active Administrator.

Index

A

Active Administrator
- overview 1
- removing........76
- starting........4

Active Directory 1
- comparing archived objects 67
- creating new objects 21
- finding in archive file 65, 66
- modifying permissions 16
- moving objects 20
- reporting on objects 21
- searching for objects........10
- searching for permissions 12

Active Template........2

Active Templates
- creating........25
- delegating control 18, 29
- deleting........28
- modifying 27
- repairing a broken........31
- reporting on 28

adding
- GPO link........45
- GPO to the repository........60

archive file
- browsing for an Active Directory object 66
- selecting one to restore 64

auditing........3
- setup 74

B

backing up
- GPO........42
- security 22

browsing
- object in archive file 66

C

check in
- GPO to repository........61

check out
- GPO from repository 61

Client Side Troubleshooting 72

comparing
- Active Directory archives........67
- GPO history........53

Copying Group Policy Objects 39

creating
- Active Directory objects 21
- Active Templates........25
- Group Policy objects........40

D

delegating control
- using an Active Template 18, 29

delegating control........18

delegating control........29

deleting
- Active Template........28

disallow propagation 16

E

editing
- GPO offline........61

e-mail notification
- changing accoutn that runs........76

error message
- licensing issues 75

Event Notification Service
- changing account that runs........76

F

File menu........5

G

generate log file
- GPO backup........42
- security backup 22

GPO
- set starting container 60

Group Policy 2

Group Policy history
- managing 36
- reporting on........52
- rolling back 54

Group Policy menu 6

Group Policy object
- adding a Link 45
- backing up........42
- comparing history 53
- copying 39
- creating new........40
- locating 38
- managing 36
- modifying........37, 38
- removing a link 46
- renaming 41

reporting ... 41, 42, 52
restoring ... 44
viewing ... 37, 51

H

Help menu ... 6

L

licensing
resolving issues ... 75
setting starting container ... 60
locating
a GPO ... 38

M

managing
GPOs ... 36
menu bar ... 5
modifying
Active Template ... 27
GPO properties ... 37
GPOs ... 47
permissions on Active Directory objects ... 16
moving
Active Directory objects ... 20

O

offline GPO
setting starting container ... 60
offline repository
adding a GPO ... 60
editing GPO offline ... 61
publishing GPO ... 63

P

propogation ... 16
publishing
GPO to Active Directory ... 63

R

red GPO links ... 45
removing
broken links ... 48
Group Policy link ... 46
renaming
GPO ... 41
repairing ... 31
reporting
Active Directory objects ... 21
Active Templates ... 28
Group History ... 52
Group Policy Objects ... 41
repository
adding a GPO ... 60
editing a GPO offline ... 61
publishing a GPO ... 63
restoring
Active Directory objects ... 64, 68
default permissions on Active Directory objects . 20
GPO ... 44
security backup ... 23
rolling back ... 54

S

searching
Active Directory objects ... 10
permissions on Active Directory objects ... 12
Security menu ... 5
selecting servers to manage ... 8
setting up
Active Template options ... 25
Starting
Active Administrator ... 4
stopping
a search for GPO link ... 45

V

Viewing
Active Directory objects by type ... 9
GPO properties ... 45
Group Policies ... 37
Group Policy history ... 51
Group Policy settings ... 62
permissions for Active Directory objects ... 8