ACTIVE ADMINISTRATOR

ScriptLogic[®] Active Administrator[™] 4 Getting Started Guide



© 2005 by ScriptLogic Corporation All rights reserved.

This publication is protected by copyright and all rights are reserved by ScriptLogic Corporation. It may not, in whole or part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from ScriptLogic Corporation. This publication supports Active Administrator 3. It is possible that it may contain technical or typographical errors. ScriptLogic Corporation provides this publication "as is," without warranty of any kind, either expressed or implied.

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

1.561.886.2400 www.scriptlogic.com

Trademark Acknowledgements:

Active Administrator is a registered trademark of ScriptLogic Corporation in the United States and/or other countries. The names of other companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft, Active Directory, Windows, and Windows Server are registered trademarks of Microsoft Corporation.

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:



Boca Raton, Florida 33487-2742 561.886.2400 Sales and General Inquiries 561.886.2450 Technical Support

561.886.2499 Fax

ScriptLogic Corporation

6000 Broken Sound Parkway NW

www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at <u>www.scriptlogic.com</u>. 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
INSTALLING ACTIVE ADMINISTRATOR	4
MINIMUM SYSTEM REQUIREMENTS	4
BEFORE YOU BEGIN	4
User Privilege Requirements	4
Installing Microsoft SQL Server or MSDE 2000	4
Creating a Security Event Database	5
Creating Network Shares to Store Active Administrator Data	5
RUNNING THE ACTIVE ADMINISTRATOR SERVER INSTALLATION WIZARD	5
Storing Active Administrator Data	9
Creating a New Database	10
Configuring Group Policy History Service	11
Configuring Active Template Auto-Repair Service	13
Configure Active Directory Object Level Backup	15
RUNNING THE ACTIVE ADMINISTRATOR CONSOLE INSTALLATION WIZARD	17
Setting the Active Administrator Server	. 20
STARTING ACTIVE ADMINISTRATOR	20
Applying a License File	21
Evaluating the Product	21
MONITORING SERVICES	22
Setting Up a Security Event Database	22
SETTING UP AUDITING ON DOMAIN CONTROLLERS	24
EVENT CONFICURATION UTILITY	26
CONFIGURATION OTILITT	26
Disabling Fmail Notification	26
Setting Individual Event Notifications	27
Setting Global Event Notifications	28
Installing Domain Controller Agents	20
Configuring Event Collection	31
Changing the Account for E-mail Notifications	33
MANAGING THE EVENT MONITORING SERVICE	33
Starting and Stopping the Monitoring Service	33
Modifying the Domain Controller Agents	33
Viewing the Status of Collection Monitors	34
Loading New Event Definitions	34
Puroino Event Data	35
Removing the Manitaring Service	35
CDO HISTORY CONFICUEDATION	36
GEVENISTORY CONFIGURATION	30
A STREET THE ACTIVE ADMINISTRATOR CONSOLE	30
ACTIVE 1EMPLATE REPAIR CONFIGURATION	38
OBJECT LEVEL BACKUP CONFIGURATION	40
CONFIGURING THE BACKUP SERVICE	40
CONFIGURING PASSWORD RECOVERY	42
BACKING UP FROM THE COMMAND LINE	43
TROUBLESHOOTING	44
CLIENT SIDE TROUBLESHOOTING	44
Setting Logging Options	45
SETTING AUDITING PERMISSIONS	46
CHANGING THE ACCOUNT FOR E-MAIL NOTIFICATIONS	48
REMOVING ACTIVE ADMINISTRATOR	49
INDEX	50

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.





Active Directory Backup and Restore. Administrators can select a domain that contains Windows ServerTM 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.

File Security (nistrator™- ScriptLogic Group Policy Tools Help						
🌍 G	roup Policy History		🛒 Group F	Policy Offlin	e Repository	🚮 Re	sultant Set of Policies (RSoP)
😡 G	roup Policy Objects by Cont	ainer		👌 AD	Object Restore		Client Side Troubleshooting
🚯 Activ	e Directory Security	🥵 A	Active Templa	ates	🧭 Active Direc	tory Auditing	🚮 Group Policy Objects
r Template Op	tions						·í
The Active To where those t	emplates folder can be share emplates have been applied	d by admii I will be sh	inistrators or h ared. We sug	neld privatel ggest using	y. When a common fo a UNC path.	lder is used, all cha	anges to Active Templates and
Template loca	ation: \\\Vm4-win2ksvr\Acti	veAdminis	trator\			Rel	locate Active Templates Folder
Number of au	tomatically generated backu	ıp files use	ed by Active T	Femplates:	10 🛨		
C Active Temp	lates		Settings —				
Name: Computer Computer Computer:	s - Full Control s - Join a computer to the do s - Modify all properties	▲ Hi Di r Ui	ame: escription: nique ID: Permissions	Computers Full contro {4B0B620	- Full Control over computer accou F-3B9F-4A21-A2D0-90	ints.)EEBFF746C5}	Active Template Definition
🔒 Contacts -	Create Contacts		Туре:	Permissio	on:		Applies to:
Contacts	Create, delete and manage		🔊 Allow	Create C	omputer Objects		This object and all child objects
Contacts	• Delete Contacts • Manage Contacts • 2000 - Exchange Administr		S Allow	Delete C Full Cont	omputer Objects rol		This object and all child objects Computer Objects
Standard and User-defined Active Templates	2000 - Exchange Policy Ad 2000 - Exchange Server Ad 2000 - Instant Messaging A 2000 - Mail Storage Admini 2000 - Manage Chat Char 2000 - Manage Chat Char	r di s n	Delegation L Delegated A	.inks: Account: ators (BUIL)	TIN\Administrators)	[]	Container Path: 2 acme.com/Domain Controllers
1	2000 - Message Transfer A		New Templa	ate M	odify Template)elete Templatel	Where Active emplate is Applied

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.



- 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.



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.

Α	ctive Dire	ectory Audit	Report			
5	ummary:	58 Alert(s)				
ι	Jser(s):	All users				
E	vent(s):	All events				
0)ate Range:	Between Wednesd	ay, August 11, 2004, ar	nd Wednesday, August 18, 2004		
Au	gust 18, 200)4				
	Date/Time:		User:	Event:		
9	08/18/2004	10:54:32 AM	Administrator (SALESDEMO\Admi	Group Policy Object - Changed inistrator)		
	Desc:	Group Policy Obje 'SALESDEMO\Adm	ct 'NSA WinXP lockdow inistrator' on 'JON2003	vn {C0EDA8BC-755D-475F-B222-32806849F906}' was changed by 35VR' at '8/18/2004 10:54:32 AM'		
9	08/18/2004	10:12:57 AM	Administrator (SALESDEMO\Admi	Security - Permissions Changed inistrator)		
	Desc:	The security for o changed by 'SALE	bject 'OU=Accounting,@ SDEMO\Administrator'	OU=SalesDemo,DC=salesdemo,DC=local' (Type='organizationalUnit') was on 'JON20035VR' at '8/18/2004 10:12:57 AM'		
9	08/18/2004	10:12:57 AM	Administrator (SALESDEMO\Admi	Security - Permissions Changed inistrator)		
	Desc:	The security for o	bject 'OU=Accounting,	OU=SalesDemo,DC=salesdemo,DC=local' (Type='organizationalUnit') was		

Installing Active Administrator

MINIMUM SYSTEM REQUIREMENTS

- Processor: Pentium 600MHz or faster
- Operating System: Windows 2000 or later
- Disk Space: 50 MB
- Memory: 256 MB
- Screen resolution: 1024x768

BEFORE YOU BEGIN

If you have not yet done so, please download the latest version of the Active Administrator program. This can be done at the following link:

http://www.scriptlogic.com/support

The Active Administrator program has two setup files: **AAConsoleSetup4xx.msi** and **AAServerSetup4xx.msi**. Install the Active Administrator console on any computer that requires it. The server setup needs to be installed on only one machine.

User Privilege Requirements

To use Active Administrator, a user must hold administrative rights, which are required for the installation and use of the product, on the servers or workstations.

Installing Microsoft SQL Server or MSDE 2000

Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is a run-time installation of Microsoft SQL Server 2000 and has a connection limit of five simultaneous connections. If the combination of domain controllers and the number of users accessing the information will be greater than five, we recommend installing a full version of Microsoft SQL Server 2000.

Note: MSDE 2000 is included in the installation of Active Administrator. To omit installing MSDE 2000, choose a custom install when prompted.

Note: If you already have a Microsoft SQL 2000 server, the agents require mixed mode authentication on the server (using a database username and password, such as *sa*). If your SQL Server is not in mixed mode authentication, run DBWizard.exe, which is located in the Active Administrator installation folder.

Creating a Security Event Database

The server installation wizard prompts you to create the security event database in MSDE 2000 on the local computer. You also can create the security event database on an existing Microsoft SQL Server 2000 computer anywhere on your network. See *Setting Up a Security Event Database*.

On the database server, the database installation creates two local groups that control access to the security event database.

- **AA_Admin group** = users that need to be able to update the database
- AA_User group = users that only need to run reports from the database

Creating Network Shares to Store Active Administrator Data

The Active Administrator Server upgrade program creates the ActiveAdministrator share that contains four subfolders in which Active Administrator data is stored.

ActiveAdministrator
ActiveTemplates
ADBackups
GPOHistory

You can create your own share as long as it resides on a file server that is accessible by all Active Administrator users. Make sure the share has sufficient hard drive capacity. You can estimate that each GPO initially takes 2MB to back up. Each version saved thereafter is significantly smaller, about 10k on average. If you have a large Active Directory database, you should have 10GB available.

RUNNING THE ACTIVE ADMINISTRATOR SERVER INSTALLATION WIZARD

Active Administrator is provided in a Windows® Installer package format, which allows for robust, self-repairing of application files and ease of installation and software distribution. The Windows Installer service is included with Microsoft Windows 2000 and later, for the purposes of this product installation.

Note: The server setup needs to be installed on only one computer.

Note: You may be prompted to restart your system at the completion of the installation process.

1. After downloading Active Administrator, double-click the **AAServerSetup4xx.msi** file, or right-click the **AAServerSetup4xx.msi** file, and then select **Install**. The **Welcome** dialog box appears.

🔂 Active Administrator Serve	er Setup - InstallShield Wizard	×
U	Welcome to the InstallShield Wizard for Active Administrator Server Setup	
	The InstallShield(R) Wizard will install Active Administrator Server Setup on your computer. To continue, click Next.	
	WARNING: This program is protected by copyright law and international treaties.	
	< Back Next > Cancel	

2. Click Next. The License Agreement dialog box appears.

🙀 Active Administrator Server Setup - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	4
END USER LICENSE AGREEMENT ("EULA")	1
PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (THE "AGREEMENT") CAREFULLY BEFORE DOWNLOADING AND/OR INSTALLING ANY SCRIPTLOGIC SOFTWARE PRODUCT (INDIVIDUALLY AND COLLECTIVELY, THE "SOFTWARE") AS PROCEEDING WILL INDICATE YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. THE LICENSE RIGHTS GRANTED TO YOU IN	F
I accept the terms in the license agreement i do not accept the terms in the license agreement InstallShield	

Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or at the time of purchase or evaluation.

3. Select I accept the terms in the license agreement, and then click Next. The Customer Information dialog box appears.

🙀 Active Administrator Server Setup - InstallShield Wizard	×
Customer Information	
Please enter your information.	
User Name:	
Valued Customer	
Organization:	
Microsoft	
Install this application for:	
 Anyone who uses this computer (all users) 	
C Only for me (Valued Customer)	
InstallShield-	
< <u>B</u> ack <u>N</u> e	ext > Cancel

The **User Name** and **Organization** boxes default to the values set when the operating system was installed. You can choose to install the application for all users or just you.

4. Select whether to install the application for just yourself or all users, and then click **Next**. The **Setup Type** dialog box appears.

👘 Active Adminis	strator Server Setup - InstallShield Wizard 🛛 🛛 🔀
Setup Type Choose the set	sup type that best suits your needs.
Please select a	setup type.
• <u>Complete</u>	All program features will be installed. (Requires the most disk space.)
C Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel

Note: MSDE 2000 is installed with the complete install of Active Administrator Server. To omit installing MSDE 2000, choose **Custom**. See *Installing Microsoft SQL Server or MSDE 2000*. 5. Select to do a complete or a custom install, and then click Next.

Note: If you chose a custom installation, expand Microsoft SQL Server Desktop Engine 2000, select This feature will not be available, and then click Next.

Click on an icon	n the list below to change l	how a feature is ins	talled.	
	Active Administrator Setup Nicrosoft SQL Server Deskto	op Engine 2000	Feature Description MSDE 2000 or Micro 2000 is required for	soft SQL Active
	This feature will be installed This feature, and all subfea	on local hard drive tures, will be install	ed on local hard drive.	
	This feature will be installed	when required. lable		on
		3		
install to: C:\Program Files	\ScriptLogic Corporation\Ac	tive Administrator:		Change

The Ready to Install the Program dialog box appears.

🙀 Active Administrator Server Setup - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
InstallShield	
<u> </u>	

6. To begin the installation, click **Install**. The **Installing Active Administrator Console** box displays a status bar that indicates the installation progress.

Storing Active Administrator Data

When the software install completes, the Path Selection box appears.

🖟 Active Administrator Path Setup 🛛 🗙
Active Administrator Path Selection
Please select a local path for storing Active Administrator data.
Path:
This path will be shared as "ActiveAdministrator".
We recommend that you have at least 2GB of free space available on this drive, preferrably 10GB if you have a large Active Directory database.
·
OK Cancel

The Active Administrator Server upgrade program creates the ActiveAdministrator share that contains four subfolders in which Active Administrator data is stored.

ActiveAdministrator
ActiveTemplates
ADBackups
GPOHistory
GPORepository

7. Type a path to the folder where you want Active Administrator to create the share, or click ... to locate a folder.

Note: You should have at least 2GB of free space available on the drive you select. If you have a large Active Directory database, ideally, you should have 10GB free.

Note: If you specify a folder that does not exist, you receive a confirmation message. To create the folder, click **Yes**.

8. Click OK. A warning message appears.

Important: The default permission for the share is Everyone – Full Control. The recommendation is to modify the share permissions so only those service accounts used by Active Administrator services and users who run Active Administrator Console have access to the share.

Active Administrator Security Warning!				
(i)	Active Administrator has created a share named 'ActiveAdministrator' for the selected path.			
7	NOTE! This share has been created with permissions set to "Everyone - Full Control"			
	You should consider modifying the permissions of the share to only allow access by the service accounts used by Active Administrator services, and by the users who will run the Active Administrator console.			
	OK			

9. Click **OK** to continue.

Creating a New Database

The **Database Maintenance Wizard** opens to the **Create a new database** dialog box, which displays the current machine name (default) and the dbActiveAdmin database (default).

- 10. If necessary, type the name of the Microsoft Windows server that is running Microsoft SQL Server 2000 in the **SQL Database Server Name** box, or click ... to locate registered servers that may also be running the database engine.
- 11. If necessary, type the name of the database to create in the **Database Name** box, or click ... to locate existing database names.
- 12. Choose whether to use Windows Authentication or SQL Server Authentication. If you choose **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

Note: If you want to use Windows Authentication, the SQL server must be configured to use trusted security, and the Active Administrator Security Log Monitor service must be configured with a domain account that has access to update the database. See

13. Click **Next**. The database definition dialog box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.

🕼 Database Maintenance Wizard - Create a new database 🛛 🗙				
	Initial Database Size: 50 Initial TX Log Size: 50 ○ Override Default File Locations Data File Path: Tx Log Path: (The paths above should be the local path on the server where the database will be created. Ex: "C:\DB\") ✓ Create default security groups Create security groups as ○ Domain Groups ○ Domain Local Groups ○ Local Groups (non-DC's only)			
	Cancel < <u>B</u> ack <u>Next</u> Einish			

UPDATED 22 DECEMBER 2005

- 14. In the **Initial Database Size** box, type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.
- 15. In the **Initial TX Log Size** box, type an initial size for the transaction log file (*.ldf). If the database needs to grow the log file, it does so automatically.
- 16. To create the database transaction log files in a location other than the default location, select **Override Default File Locations**, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
- 17. By default, Active Administrator creates default security groups as **Local Groups**. You can change this setting to **Domain Groups** or **Domain Local Groups**. If you do not want to create default security groups, clear the **Create default security groups** check box.
- 18. Click Next. The Database Maintenance Wizard displays the options you chose.

🕼 Database Maintenar	nce Wizard - Create a new d	atabase	×	
	The following actions w A database will following settin Server Name : V Database Name: (** Use Trusted S	ill be performed: be created usin ngs: /M4-WIN2KSVR dbActiveAdmin Security Wizard - Create a p	Windows Authentication	n
	W Database Maintenance	wizaru - creace a n	ewualabase	~
		The following acti	ons will be performed:	
		A database w following se Server Name Database Nam ** Use SQL S User Name Password Initial Date Initial Tx I	nill be created usin ettings: et dbActiveAdmin erver Authenticatio : sa : (not shown) ubase Size: 50 .og Size: 50	g the
SQL Authe	Server ntication	Click the 'H	'inish' button to pr	oceed
		Cancel	< <u>Back</u> Next >	Einish

19. To create the specified database, click **Finish**. A message box displays the progress of creating the database.

Configuring Group Policy History Service

Upon completion, the **Configure the Group Policy History service** dialog box opens.

20. In the **Polling Interval** list, select how often you want the Group Policy History service to poll the domain controllers for Group Policy object (GPO) changes at a specified polling interval.

Note: A polling interval of 60 seconds (default) gives the administrators enough time to make a few changes to the GPO without creating new versions for every change.

- 21. To store GPO history, the installation wizard creates the GPOHistory folder, whose path is displayed in the **Group Policy History Location** box. If you created another share in which to store GPO history, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*.
- 22. Click Add Domain. The Connect to Domain box opens.

Connect to	Domain		×
Domain:	acme.com		Browse
		ОК	Cancel

- 23. In the Domain box, type the domain name, or click Browse to locate the domain.
- 24. Click OK. The domain name appears in the list.

Configure the Group Policy History service	×
Group Policy History The Group Policy History service will keep track of changes to your GPOs	
Check for Group Policy changes every 60 seconds.	
\\VM4-WIN2KSVR\ActiveAdministrator\GPOHistory	
Keep history on the following domains:	
Domains:	Add Domain
acme.com	Remove Domain
Create a log file (kept in the same folder as the service executable - car	n grow large)
Log On	
Please specify a valid username and password for the GPO History Servic	e:
Username: <pre><pre></pre> <pre><pre></pre> <pre><pre></pre> <pre></pre> <pre></pre></pre></pre></pre>	n rights>
Password: **********	
Confirm password: **********	
OK Cancel	

- 25. If you want to see exactly what the GPO History service is doing, select the **Create a log file** check box to create a debug log file.
- 26. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click ... to locate a group/user.
- 27. Click **OK**. An information message displays the account you selected and the right that was granted.

Group Policy History Setup			
٩	The account ACME\Administrator has been granted the 'Log On As A Service' right.		
	ОК		

28. Click **OK** to continue with the install process.

Configuring Active Template Auto-Repair Service

The **Configure the Active Template Auto-Repair Service** box appears. You can configure Active Administrator to repair broken Active Templates automatically. In addition, you have a report of broken templates sent automatically.

Configure the Active Template Auto-Repair Service				
Active Template Auto-Repair The Active Template Auto Repair service will fix broken templates automatically.				
Repair broken Active Templates automatically every 30				
Active Templates Path: \\\\M4-WIN2KSVR\ActiveAdministrator\ActiveTemplates				
Please specify a valid username and password for the Auto-Repair Service:				
Username: <pre> <please a="" admin="" domain="" enter="" name="" of="" rights="" the="" user="" with=""> .</please></pre>				
Password:				
Confirm password: **********				
OK Cancel				

- 29. Active Administrator checks for broken templates every 30 seconds by default. To change the value, choose a value from the **Repair Interval** list.
- 30. If you want to send reports of broken templates to selected users via email, select the **Send a Report of Broken Templates By E-Mail** check box or click **Configure email settings**. The **E-Mail Settings** box appears.

-Mail Settings		×
E-mail Settings		OK.
E-mail server:		Cancel
E-mail Port:	(Leave blank to use default port)	
From User Name:		
From E-Mail Address:		
To User Name:		
To E-Mail Address:		
SMTP Authentication —		
🔲 Use SMTP Authenti	cation	
User Name:		
	Leave blank to use From User Name	
Password:		
Confirm Password:		

.

31. Set up the email service and select a user to receive the broken templates report.

Note: The OK button becomes available when you fill in the necessary boxes.

E-mail server

Name of the email server.

E-mail Port

Name of the email port. Leave blank to use the default port.

From User Name

Name of the user to appear in the **From** box on the email generated to send the broken templates report.

From E-mail Address

Email address of the user whose name appears in the **From** box on the email generated to send the broken templates report.

To User Name

Name of the user to appear in the **To** box on the email generated to send the broken templates report.

To E-Mail Address

Email address to use to send the broken templates report.

Use SMTP Authentication check box

Select to use SMTP Authentication. If you leave the boxes blank, the user name shown in the **From User Name** box is used. Otherwise, type a user name and password in the appropriate boxes.

- 32. Click **OK** to close the **E-mail Settings** box and return to the **Configure the Active Template Auto-Repair Service** box.
- 33. To store Active Templates, the installation wizard creates the ActiveTemplates folder, whose path is displayed in the Active Templates Path box. If you created another share in which to store Active Templates, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*.
- 34. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click ... to locate a group/user.
- 35. Click **OK** to continue with the install process.

Note: If you want to change any of the settings once the install is complete, click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator** and then select **Active Template Repair Configuration**.

Configure Active Directory Object Level Backup

The Configure the Active Directory Backup service dialog box opens.

36. To store Active Directory backups, the installation wizard creates the ADBackups folder, whose path is displayed in the **Active Directory Backup Path** box. If you created another share in which to store Active Directory backups, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*.

Configure the Active Directory Backup service 🗙						
Active Directory Object Level Backup / Restore						
Quickly recover from	Quickly recover from deleted or modified objects in Active Directory.					
Active Directory Backup	Path:					
\\VM4-WIN2KSVR\Activ	/eAdministrator\A	DBackups		***		
Backup the following dor (Note: Windows 2003 Se	mains: ervice Pack 1 or h	nigher is required to	restore pass	words.)		
Domains:		Supports Passwo	rd Restore:	Add Domain		
				Remove Domain		
				Refresh Domain List		
				Password Recovery		
Run the backup:	Run the backup:					
🔲 Create a Log File (ke	Create a Log File (kept in the same folder as the service executable - can grow large)					
Log On Please specify a valid username and password for the Object Level Backup/Restore Service:						
Username: <please a="" admin="" domain="" enter="" name="" of="" rights="" the="" user="" with=""></please>						
Password:	*****					
Confirm password:	Confirm password: **********					
	ОК	Cancel	Backup Now			

37. Click Add Domain, and locate the domain that you want to backup.

Note: If you are using Windows Server[™] 2003 Service Pack 1 (SP1) or higher, Active Administrator can restore passwords when you restore accounts that were deleted.

If the server you select is running Windows Server 2003 SP1, a message box appears asking if you want to enable password recovery. To enable password recovery, click **Yes**, and then click **Refresh Domain List**. **Yes** displays in the **Supports Password Restore** column.



Important: If a domain contains both Windows Server 2003 SP1 and Windows 2000 domain controllers, the No may not change to Yes when you click **Refresh Domain**. To enable password recovery in a mixed environment, use the Forest Prep Utility.

 Select the Windows 2003 Server SP1 domain controller, and then click Password Recovery. See Configuring Password Recovery.

If at a later time you want to change the password recovery setting, you can do so from the Forest Prep Utility. See *Configuring Password Recovery*.

- 38. In the **Run the backup** box, select to run the backup **Every Day** or **Twice a Day**.
- 39. From the **at** list, select a time or times to run the backup.
- 40. If you want to create a log file for the backup, select the Create a Log File check box.
- 41. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click ... to locate a group/user.

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

Note: If you want to back up the domain without waiting for the scheduled time, click **Backup Now**.

42. Click **OK** to continue with the install process.

Note: If you want to change any of the settings once the install is complete or run a backup, click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator** and then select **Object Level Backup Configuration**.

43. When the installation is complete, the **InstallShield Wizard Completed** box appears.

🙀 Active Administrator Server Setup - InstallShield Wizard 🛛 🛛 🔀					
	InstallShield Wizard Completed				
The InstallShield Wizard has successfully installed Active Administrator Server Setup. Click Finish to exit the wizard.					
	< Back Finish Cancel				

- 44. Click Finish. The following Active Administrator components are installed:
 - Active Template Repair Configuration
 Oreate Auditing Database
 - 🔢 Event Configuration Utility 🛛
 - 🗊 Forest Prep Utility
 - 🔞 GPO History Configuration
 - 🚷 Object Level Backup Configuration

During installation, you configured some of these components. If you want to make changes, access each component individually.

RUNNING THE ACTIVE ADMINISTRATOR CONSOLE INSTALLATION WIZARD

Install the Administrator Console on any workstation that requires the use of Active Administrator.

1. After downloading Active Administrator, double-click the **AAConsoleSetup4xx.msi** file, or right-click the **AAConsoleSetup4xx.msi** file, and then select **Install**. The **Welcome** dialog box appears.



2. Click Next. The License Agreement dialog box appears.



Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or at the time of purchase or evaluation.

3. Select I accept the terms in the license agreement, and then click Next. The Customer Information dialog box appears.

🖶 Active Administrator Console - InstallShield Wizard	×
Customer Information Please enter your information.	
User Name:	
Valued Customer	
Organization:	
Microsoft	
Install this application for:	
InstallShield	
< <u>B</u> ack	Next > Cancel

The **User Name** and **Organization** boxes default to the values set when the operating system was installed. You can choose to install the application for all users or just you.

4. Select whether to install the application for just yourself or all users, and then click **Next**. The **Setup Type** dialog box appears.

🙀 Active Admini	strator Console - InstallShield Wizard 🛛 🛛 🔀
Setup Type Choose the set	tup type that best suits your needs.
Please select a	setup type.
	All program features will be installed. (Requires the most disk space.)
C Cu <u>s</u> tom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield	< <u>B</u> ack Next > Cancel

5. Click Next. The Ready to Install the Program dialog box appears.

🙀 Active Administrator Console - Inst	allShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation		
Click Install to begin the installation.		
If you want to review or change any of exit the wizard.	your installation settings, click Ba	ck. Click Cancel to
InstellShield	< Back Install	Cancel

6. To begin the installation, click **Install**. The **Installing Active Administrator Console** dialog box displays a status bar dialog that indicates the installation progress.

When the installation is complete, the InstallShield Wizard Completed box appears.

🛱 Active Administrator Console - InstallShield Wizard 🛛 🔀				
	InstallShield Wizard Completed			
A	The InstallShield Wizard has successfully installed Active Administrator Console. Click Finish to exit the wizard.			
	< Back Enish Cancel			

7. Click Finish. The following Active Administrator component is installed:



Important: On each computer running Active Administrator Console, the user must set the server that is running Active Administrator Server.

Setting the 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 Server.
- 3. In the **Server** box, type the name of the server where Active Administrator Server is installed, or click <u>initial</u> to locate a server.

Set Activ	e Administrator Server		×
đ	Please select the Active Administrator server. For help, please contact your Network Adminis	strator.	
Server:	Vm4-win2ksvr		
		ок	Cancel

4. Click OK.

STARTING ACTIVE ADMINISTRATOR

- Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select one of the following components:
 - Active Administrator Console
 - Active Template Repair Configuration
 - Create Auditing Database
 - Event Configuration Utility
 - Forest Prep Utility
 - GPO History Configuration
 - Object Level Backup Configuration

Each time you run some of the components, you are greeted by the splash screen.



Applying a License File

The first time you start Active Administrator Console or the Event Configuration Utility, you see the **New Installation** dialog box, which allows you to apply a license file or evaluate the product without a license, as well as contact ScriptLogic Corporation and visit our website for further information.

New Insta	lation: Active Administrator™	
Active Ad Copyright (http://www	ministrator™ v4.03 © 2001-2005 ScriptLogic Corporation <u>Ascriptlogic.com</u>	
THANK YO a license fil License File Evaluation	U! for choosing Active Administrator [™] . If y le, enter the path to the file below and click e'. If you do not have a license file, click 'Beç 'to start Active Administrator [™] in evaluation	ou have Apply jin n mode.
	Apply License File	
	Begin Evaluation	
	Cancel	

Active Administrator requires a valid license file in order to function properly. If you have a company license file or were provided with an evaluation or temporary license file, you must enter the location and filename in the **License File** box.

The license file is approximately 1KB in size and has a .lic file extension. The Sales account executive or Support Team specialist that you have been dealing with should have emailed this file to you as an attachment.

Important: 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.

Your Active Administrator license does not permit you to manage objects outside of: LDAP://ou=Users,dc=acme,dc=com
ок

If you want to change the scope of the license file, contact your Sales account executive or Support Team specialist.

Click ... to locate the license file, and then click **Apply License File**.

Evaluating the Product

If you are evaluating the software and would like to use the preset values for the number of licenses, objects, and evaluation days, click **Begin Evaluation**.

Note: The full and evaluation versions of Active Administrator are identical. The license file is the sole determinant of program functionality.

Monitoring Services

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, the service sends the information to a centralized SQL Server and optionally generates an email alert to a predetermined address or set of addresses.

Active Administrator also keeps Group Policy History for all Group Policy Objects (GPOs) in your domains. The Group Policy History service watches your domain controllers for GPO changes.

The combination of these two services allows you to determine exactly who made what changes to your Group Policies. If you don't like a change that someone made, you can rollback to a previously saved version of the GPO.

SETTING UP A SECURITY EVENT DATABASE

The security event service uses Microsoft SQL Server 2000 as its back-end database for storing event information. The database should be installed in a central location that can be reached by all of your domain controllers.

Note: The server installation program prompts you to create the security event database in MSDE 2000 on the local computer. You also can create the security event database on an existing Microsoft SQL Server 2000 computer anywhere on your network.

- 1. Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select Create Auditing Database. The Database Maintenance Wizard opens.
 - Cancel
 <Back</td>
 Mext >
 Einish
- 2. From the action list, select **Create a new database**.

3. Click **Next**. The **Create a new database** dialog box displays the current computer name (default) and the dbActiveAdmin database (default).

🕵 Database Maintenance W	izard - Create a new database	×
	SQL Database Server Name:	
	VM4-WIN2KSVR	[
	Database Name:	
	dbActiveAdmin	
	 Use Windows Authentication Use SQL Server Authentication 	
	User Name:	1
	Password:]
	Cancel < <u>B</u> ack <u>N</u> ext >	inish

- 4. If necessary, type the name of the Microsoft Windows server that is running Microsoft SQL Server 2000 in the **SQL Database Server Name** box, or click ... to locate registered servers that may also be running the database engine.
- 5. If necessary, type the name of the database to create in the **Database Name** box, or click ... to locate existing database names.
- 6. Choose whether to use Windows Authentication or SQL Server Authentication. If you choose **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

Note: If you want to use Windows Authentication, the SQL server must be configured to use trusted security, and the Active Administrator Security Log Monitor service must be configured with a domain account that has access to update the database.

7. Click **Next**. The database definition dialog box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.

🞼 Database Maintenance Wizard - Create a new database 🛛 🛛 🗙				
	Initial Database Size: 50 Initial TX Log Size: 50 Override Default File Locations Data File Path: Tx Log Path: (The paths above should be the local path on the server where the database will be created. Ex: "C:\DB\") Image: Create default security groups as Image: Domain Groups Image: Domain Local Groups Image: Local Groups (non-DC's only)			
	Cancel < <u>B</u> ack <u>Next</u> Einish			

8. In the **Initial Database Size** box, type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.

- 9. In the **Initial TX Log Size** box, type an initial size for the transaction log file (*.ldf). If the database needs to grow the log file, it does so automatically.
- 10. To create the database transaction log files in a location other than the default location, select **Override Default File Locations**, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
- 11. By default, Active Administrator creates default security groups as **Local Groups**. You can change this setting to **Domain Groups** or **Domain Local Groups**. If you do not want to create default security groups, clear the **Create default security groups** check box.
- 12. Click Next. The Database Maintenance Wizard displays the options you chose.

🕻 Database Maintenance Wizard - Create a ne	w database 🛛 🔀
The following action A database with following set Server Name Database Name ** Use Truste	ns will be performed: Il be created usin ttings: : VM4-WIN2KSVR :: dbActiveAdmin :d Security cce Wizard - Create a new database
	The following actions will be performed: A database will be created using the following settings: Server Name : VM4-WIN2KSVR Database Name: dbActiveAdmin ** Use SQL Server Authentication User Name : sa Password : (not shown) Initial Database Size: 50 Initial Tx Log Size: 50
SQL Server Authentication	Click the 'Finish' button to proceed

13. To create the specified database, click **Finish**.

SETTING UP AUDITING ON DOMAIN CONTROLLERS

To gather the proper information from the security event logs, the information must first be audited. You need to modify the **Default Domain Controllers Policy** to enable auditing. The processes vary slightly for Windows 2000 Server and Windows Server 2003 domain controllers.

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

- 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. Open the Group Policy Objects tab.
- 3. In the **Group Policy Name** list, right-click the **Default Domain Controllers Policy**, and then select **Edit**. The **Group Policy** window opens.

4. Expand Computer Configuration > Windows Settings > Security Settings > Local Policies, and then select Audit Policy.

iting
iong Vilia
inea
iting
i

5. Double-click the following policies to edit their Success and Failure settings.

選 Audit account management	Security Policy Setting
🕮 Audit directory service access	Audit account management
🔀 Audit policy change	☑ Define these policy settings
B Audit system events	Audit these attempts:
- •	Success
	✓ Failure
	OK Cancel

- 6. Close the Group Policy window.
- 7. From the command prompt, refresh the Group Policies.
 - In Windows 2000, type secedit /refreshpolicy machine_policy /enforce
 - In Windows XP and Windows Server 2003, type **gpupdate**

Event Configuration Utility

CONFIGURING THE EVENT MONITORING SERVICE

Note: Run the Event Configuration Utility only after you have set up the database. See *Setting Up a Security Event Database*.

The Event Configuration Utility allows you to select which events you want the service to monitor. The events are listed in an action-oriented context, so that it is easy to see what notifications a sent while hiding as much of the complexity as possible.

Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select Event Configuration Utility. The Event Configuration Utility window opens to the Event Definitions tab.

Note: The event definitions are stored in an Event Definitions File (*.edf), which is located in the Active Administrator installation directory.

Event Defini	tions Default Email Addresses Definition Name Computer - Account Changed Computer - Account Created Computer - Account Deleted	🐴 Install DC Agents 🛛 🔎 Co	Email Addresses
	Definition Name Computer - Account Changed Computer - Account Created Computer - Account Deleted		Email Addresses
	Computer - Account Changed Computer - Account Created Computer - Account Deleted		
	Computer - Account Created Computer - Account Deleted		
	Computer - Account Deleted		
	Contact - Changed		
	Contact - Created		
	Contact - Deleted		
	General - AD Object Changed		
	General - AD Object Created		
	General - AD Object Deleted		
	General - AD Object Renamed / Moved		
☑ 📴	Group - Global Distribution Group Change	d	
	Group - Global Distribution Group Created	1	
☑ 📴	Group - Global Distribution Group Deleted		
☑ 📴	Group - Global Group Changed	Email Notification	
	Group - Global Group Created	Enabled by Default	
	Group - Global Group Deleted	Enabled by Delault	
	Group - Group Type Changed		
र।			I⊅ĺ
Set Alert Emai			

By default, email notification is enabled, which is indicated by the \blacksquare check box in the **Enabled** column next to each event definition.

Disabling Email Notification

• To disable email notification for a particular event, clear the check box to the left of the event definition.

Setting Individual Event Notifications

Each event in the list can have its own list of email addresses that will receive notification. You only need to enter an email address for a particular event if that person receiving the email is interested in that event.

- 1. From the Event Configuration Utility, open the Event Definitions tab, if necessary.
- 2. Select the event, and then click **Set Alert Email**. The **Email Addresses** box opens.

💏 Email Addresses 🛛 🔀
Enter specific email addresses that should receive an email message when the selected event is encountered.
Email Address
Edit Email Address
* type email address here

- To clear the Edit Email Address box, click *****
- 3. In the **Edit Email Address** box, type an email address, and then click \checkmark or press **Enter**. The email address displays in the list.

👔 Email Addresses 🛛 🔀
Enter specific email addresses that should receive an email message when the selected event is encountered.
Email Address
SecurityManager@company.com
Edit Email Address

- To remove a selected email address from the **Email Address** list, click ×.
- 4. Click X to close the Email Addresses box. The Event Configuration Utility window displays the email addresses in the Email Addresses column.

🚦 Event Confi	guration Utility		_ 🗆 ×
File Options I	Help		
😝 Event De	finitions 🔗 Default Email Addresses 🚯 In	stall DC Agents	or
Enabled	Definition Name	Email Addresses	▲
	Computer - Account Changed	SecurityManager@company.com	
	Computer - Account Created		
	Computer - Account Deleted		
	Contact - Changed		
	Contact - Created		
	Contact - Deleted		-
Set Alert Er	nail		

5. If necessary, enable email notification by selecting the **☑** check box in the **Enabled** column next to the event.

Setting Global Event Notifications

There may be some persons who want to receive event notifications for every event that is enabled on the **Event Definitions** tab. Set these email addresses as the default.

1. From the Event Configuration Utility, open the Default Email Addresses tab.

📙 Event Configuration	Utility		_ 🗆 ×
File Options Help			
Event Definitions	🔗 Default Email Addresses	Install DC Agents	Collection Monitor
Email Address			
•			
Edit Email Address			
* type emai	l address here		✓ ×

- To clear the Edit Email Address box, click <u>*</u>.
- 2. In the **Edit Email Address** box, type an email address, and then click \checkmark or press **Enter**. The email address displays in the list.

🖁 Event Configuration Utility 📃 🗖 🗙
File Options Help
Event Definitions 😥 Default Email Addresses 🎒 Install DC Agents 🔎 Collection Monitor
Email Address
SecurityDirector@company.com
Edit Email Address
* × ×

- To remove a selected email address from the Email Address list, click X.
- 3. Open the **Event Definitions** tab, and, if necessary, enable email notification by selecting the **☑** check box in the **Enabled** column next to the event.

.

Installing Domain Controller Agents

The Event Configuration Utility provides you with a means of locating all of the domain controllers in a particular domain that have the monitoring service installed. Additionally, you can select domain controllers that do not have the monitoring service installed and remotely install it.

1. From the Event Configuration Utility window, open the Install DC Agents tab.

🚼 Event Configuration Utility
File Options Help
Event Definitions 🔗 Default Email Addresses 🚯 Install DC Agents
Select Domain: Find DC's 🏼 🏚
Configure Install

- 3. In the **Domain** box, type the domain name; or click **Browse** to locate a domain.
- 4. Click **OK**. The servers in the selected domain are listed and the **Service Status** column displays (**Click 'Refresh' to update status**).

📙 Event Configuration Utilit	y .				_ 🗆 ×
File Options Help					
Event Definitions	Default Email Addresses	ins 💽	tall DC Agents	Collection M	onitor
Select Domain: acme.com				Fir	nd DC's 🕴
Server Name	Service Status		Startup Mode	Login Account	Version
🍓 vm4-win2ksvr.acme.com	(Click 'Refresh' to update	status)			
	stall				

5. Click to refresh the service. To enable the **Install** button, (**not installed**) must display in the **Service Status** column.

🚦 Event Configuration Utilit	.y				_ 🗆 ×	
File Options Help						
Event Definitions	Default Email Addresses	ins 🔁	tall DC Agents		onitor	
Select Domain: acme.com				Find	DC's 🔹	
Server Name	Service Status		Startup Mode	Login Account	Version	
wm4-win2ksvr.acme.com	(not installed)					
Configure Install						

Note: You also can click **Find DC's** to search for all domain controllers in the selected domain and query them to see if they have the service installed. If the service is installed, the information displays in the list, otherwise (not installed) displays in the **Service Status** column. If necessary, click 🔹 to refresh the service.

6. Select the domain controller, and then click **Install**. The **Set Service Information** dialog box opens.

Note: You must have privileges to write to the remote server's registry in order to store these settings.

💁 Set Service Information	×			
Set Service Startup Mode	Set Service Polling Interval			
Service Startup Mode: Automatic	Polling Interval: (number of seconds, 1-60)			
🔽 Set Database Logon Information				
SQL Server Name:	SQL Database Name:			
VM4-WIN2K5VR	dbActiveAdmin			
Use SQL Authentication O Use Wind	lows Authentication			
SQL Username (i.e. 'sa'):	Password:			
sa				
	Confirm Password:			
A. the setting Materia				
Authentication Notes: When using Windows Authentication, the agent service will configured with the supplied Windows username and password. This account must have privileges on the domain controller for reading the security event log and running a service. Additionally, the account must have privileges on the database server to insert data into the database. When using SQL Authentication, then agent will be configured to run under the LocalSystem account and the supplied SQL username and password will be used to connect to the database.				
<u>Q</u> K	Cancel			

Set Service Startup Mode

From the **Service Startup Mode** list, select whether the service starts automatically when the computer is started, needs to be started manually, or is disabled.

Set Polling Interval

In the **Polling Interval** box, type the number of seconds that may elapse between checking for new events in the Security event log. This number is initially set to 5 seconds, but may be adjusted to as long as 60 seconds.

Set Database Logon Information

Specify the database connection information that the remote service is to use to connect to the central auditing database.

Note: To use Windows Authentication, leave the User Name and Password boxes blank.

Note: To use Windows Authentication, the SQL server must be configured to use trusted security, and the Active Administrator Security Log Monitor service must be configured with a domain account that has access to update the database.

7. Change the default settings if desired, and then click **OK**. The **Active Administrator Domain Controller Agent Setup** message box displays the progress of the installation.



- 8. When the installation is complete, click **Close**. The **Service Status** column displays **Stopped**.
- 9. Select the domain controller, and then click \blacktriangleright to start the service. The Service Status column displays Running.

Configuring Event Collection

In addition to installing the monitoring service, you need to set up some additional collection options that apply to all services.

1. From the **Event Configuration Utility** window, open the **Options** menu, and then choose **Configure Collection Service**. The **Configure Event Collection** dialog box opens to the **Email Server** tab.

Configure Event Collection Email Server Miscellaneous Lo	igging
SMTP Host Name:	SMTP Port:
If your SMTP server requires aut SMTP User Name: SMTP Password:	hentication
The "From" Email address that will a	be included in the
activeadmin@mycompany.com	
<u>O</u> K <u>C</u> a	ancel

- 2. In the **SMTP Host Name box**, type the name of the SMTP server that sends the alert emails.
- 3. In the **SMTP Port** box, type the number of the TCP/IP port on which the SMTP server is listening.
- 4. If your SMTP server requires authentication, type the username and password in the SMTP User Name and SMTP Password boxes.
- 5. In the **"From" Email Address** box, type the email address that to appear in the **From** box of the alert email. By entering something meaningful, you can use the **From** box to filter your email.

6. Open the Miscellaneous tab.

🔒 Configur	Event Collection		X
Email Serv	r Miscellaneous I	Logging	
Alert Limi Alerts are o the previou	t: nly sent when an eve s number of hours sp	ent has occurred in ecified here:	
24			
(0=No Limit)		
Collection Events are past numbe	Limit: only collected if they r of days specified he	occured within the ere:	
Collection Events are past numbe	Limit: only collected if they r of days specified he	occured within the ere:	1
Collection Events are past numbe 0 (0=Current	Limit: only collected if they r of days specified he Time)	occured within the ere:	

- 7. In the **Alert Limit** box, type the number of hours to use as a limit for issuing alerts. For example, if an alert occurred within the last 24 hours (by default), an alert email is sent. However, if the event occurred further out than the number shown here, no alert email is generated, but the event is recorded in the database.
- 8. In the **Collection Limit** box, type the number of days to go back when looking for events. By default, all pertinent events are collected, but if you are not interested in retrieving historical events, you can limit the collection to a given number of days. You might find this option useful for the initial collection of data to prevent very large event logs from being examined in full.
- 9. Open the **Logging** tab.

ø	Configure Event Collection	×
	Email Server Miscellaneous Logging	
	Create a local collection log	
	Local collection logs are text files that are created on the domain controller in the service installation directory. These logs contain detailed logging information about each collection cycle that takes place, and are always overwritten with each subsequent collection.	
	<u>O</u> K <u>C</u> ancel	

Create Local Collection Log

Select to create a log file that contains detailed logging information about each ollection cycle.

10. Click OK.

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.

- 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.

MANAGING THE EVENT MONITORING SERVICE

Starting and Stopping the Monitoring Service

From the configuration screen you can also start and stop the monitoring services.

- 1. From the Event Configuration Utility window, open the Install DC Agents tab.
- 2. Select the server in the list whose monitoring service you want to start or stop.
- 3. To start the service, click \blacktriangleright . To stop the service, click \blacksquare .

Modifying the Domain Controller Agents

1. From the **Event Configuration Utility** window, open the **Install DC Agents** tab.

Note: If no domain controllers are listed, click _____. In the **Domain** box, type the domain name or click **Browse** to locate a domain.

- 2. Select the domain controller, click to stop the service, and then click **Configure**. The **Set Service Information** dialog box opens. See *Installing Domain Controller Agents*.
- 3. Change the settings, and then click **OK**.

Viewing the Status of Collection Monitors

Viewing the collection status can help you determine if there is an issue with the service on a particular server. The list on the **Collection Monitor** tab shows the last event that the collection service analyzed.

- 1. From the Event Configuration Utility window, open the Collection Monitor tab.
- 2. Click to refresh the list. The **Current collection status** area displays the date and time of the last event log entry that was collected for a particular server.

📙 Event Configuration	n Utility			_ 🗆 ×
File Options Help				
Event Definitions	🔗 Default Email Addresses	install DC Agents	Collection Monitor	
Current collection status	of each server			
Server	Last Event			
ACME\VM4-WIN2K5VR	3/25/2005 1:36:47 PM			
The second second		and device all car	and the second second	and the

- To open an event log, right click the server, and then choose **Open Event Log**. The **Event View Window** appears.
- To reset the last event for a server, right-click the server, and then choose Remove Server from Monitor. A confirmation message box appears. To reset the last event for the server and refresh the event log, click Yes.

Loading New Event Definitions

The event definitions file – **EventDefinitions.edf** – is located in the Active Administrator installation directory. Occasionally new event definition files are made available. You can import these new event definitions into your auditing database.

Important: When event definitions are imported, existing definitions with the same name are overwritten.

- 1. From the **Event Configuration Utility** window, open the **Options** menu, and then choose **Load Event Definitions**. The **Select Event Definitions File** window opens.
- 2. Locate the Event Definitions File (*.edf), and then click **Open**. A message box appears upon successful loading.
- 3. Click OK.

Purging Event Data

To manage disk space, you may want to purge the event data periodically or compress the event database.

- 1. From the **Event Configuration Utility** window, open the **Options** menu, and then choose **Purge Event Data**. The **Purge Event Data** box displays the date of the oldest event and the total number of events.
- 2. In the **Purge all data older than** list, select a date to use as the cutoff for the purge.

🞼 Purge Event I	Data	×
This option will pur database that is of	rge all event data stored in your Ider than the date specified.	
Oldest Event:	5/23/2005	
Number of Events	: 11	
	urge all data older than: 5/25/2005	
	<u>OK</u> _Cancel	

Compress Database Files

Select to compress the event database.

3. Click **OK**. A confirmation message appears.



- 4. Click Yes to proceed with the purge. A completion message appears.
- 5. Click OK.

Removing the Monitoring Service

1. From the **Event Configuration Utility** window, open the **Install DC Agents** tab.

Note: If no domain controllers are listed, click _____. In the **Domain** box, type the domain name or click **Browse** to locate a domain, and then click **OK**.

- 2. Select the domain controller, and then click **•** to stop the monitoring service.
- 3. Click Uninstall. A message box appears asking for confirmation.
- 4. Click **Yes** to uninstall the monitoring service. The **Active Administrator Domain Controller Agent Setup** message box displays the progress.
- 5. When removal is complete, click Close.

GPO History Configuration

The Group Policy History service should be installed on only one machine. The service needs to be configured to run as a domain account that has enough privileges to read all of the Group Policy object (GPO) settings on the domain, as well as to write permissions to the Group Policy History Path.

Note: The Group Policy History service was configured during the installation process, so you only need to access this utility to make changes to the configuration.

Note: You can run the Group Policy History service from the command line. Stop the service, and then type **SWGPOSvc.exe** –**debug** at the command line.

1. Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select GPO History Configuration. The Configure the Group Policy History service window displays the choices made during the installation process.

Configure the Group Policy History service 🗙				
Group Policy Histo The Group Policy H	ry istory service will keep track of changes to your GPOs.			
Check for Group Policy Group Policy History Lo	v changes every 🔟 📻 seconds. ocation (UNC Path):			
\\VM4-WIN2KSVR\Ac	tiveAdministrator\GPOHistory			
Keep history on the fo	llowing domains:			
Domains:		Add Domain		
acme.com	acme.com Remove Domain			
Create a log file (k	ept in the same folder as the service executable - can	grow large)		
Log On				
Please specify a vali	id username and password for the GPO History Service	:		
Username:	ACME\Administrator			
Password:	*****			
Confirm password:	****			
	OK Cancel			

Note: To store GPO history, the installation wizard creates the GPOHistory share, whose path is displayed in the **Group Policy History Location** box. If you created another share in which to store GPO history, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*.

2. In the **Polling Interval** list, select how often you want the Group Policy History service to poll the domain controllers for Group Policy object (GPO) changes at a specified polling interval.

Note: The GPO service polls the domain controllers for GPO changes at a specified polling interval. The polling interval is set to 60 seconds by default. We recommend a polling interval of 60 seconds as this gives the administrators enough time to make a few changes to the GPO without creating new versions for every change.

3. If necessary, click **Add Domain**, and then locate the domain on which you want to keep history.

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

- 4. If you want to see exactly what the GPO History service is doing, select the **Create a log file** check box to create a debug log file.
- 5. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click to locate a group/user.
- 6. Click OK.

SETTING UP THE ACTIVE ADMINISTRATOR CONSOLE

The main Active Administrator Console needs to know about the path to the Group History Location as well as the security event database server and name.

Note: Be sure the user you are logged in as has read access to the security event database and Group Policy History file share.

- 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. Open the Group Policy History tab.
- 3. In the **Group Policy History Location** box, type the full UNC path to the share you created to store the GPOs or click ... to locate the share.

Note: During the install process, a GPOHistory share is created.

Kan and the Haministrator™ - ScriptLogic C	Corporation			_ 🗆 ×
File Security Group Policy Tools Help				
🔯 Group Policy Objects by Contai	iner 🔰 뤒 A	D Object Restore	🔠 Clie	ent Side Troubleshooting
🚯 Active Directory Security	langle Active Templates	Active Directory	Auditing	🚮 Group Policy Objects
🎯 Group Policy History	🛒 Group Policy Offi	ine Repository	🚮 Resulta	ant Set of Policies (RSoP)
Group Policy History Location				
\\VM4-WIN2KSVR\ActiveAdministrator\0	GPOHistory			
GPOs				
Unique Name:				
	Date	and the second second	Revisions	Report

- 4. Open the Active Directory Auditing tab.
- 5. In the **Server name** box, choose the server where the event monitoring database is located.
- 6. In the **Database name** box, choose the name of the security event database.

Active Administrator™ - ScriptLogic Corporation						
ile Security Group Policy Tools Help						
🙆 Group Policy Objects by Container		<u>a</u> .	AD Object Restore	📕 🔡 Client !		
🍏 Group Policy History	<u> </u>	Group Policy O	ffline Repository	🚮 Resultant S		
🐘 Active Directoru Securitu 🛛 🗖	Active	Templates	🧭 Active Directo	ry Auditing 🛛 💡		
Connect to Active Administrator Database - Current Filter Criteria						
vm4-win2ksvr.acme.com	User(:	s):	<pre></pre> <pre><</pre>	, raodaj, maj ro, 200		
Database name:	Even	:(s):	<all events=""></all>	1		
dbActiveAdmin 💌	Serve	#(s):	<all servers=""></all>			
	Desci	iption Mask:	<no description="" filter=""></no>			

Active Template Repair Configuration

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 alerted automatically via email when an Active Template is repaired.

Note: The Active Template Auto-Repair service was configured during the installation process, so you only need to access this utility to make changes to the configuration.

 Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select Active Template Repair Configuration. The Configure the Active Template Auto-Repair Service box displays the choices made during the installation process.

Configure the Active T	Configure the Active Template Auto-Repair Service				
Active Template Auto-Repair The Active Template Auto Repair service will fix broken templates automatically.					
Repair broken Active Templates automatically every 30 30 seconds. Send a Report of Broken Templates By E-Mail Configure email settings					
Active Templates Path:	\\VM4-WIN2K5VR\ActiveAdministrator\ActiveTemplates				
Please specify a valid	username and password for the Auto-Repair Service:				
Username:	ACME\sladmin				
Password:	******				
Confirm password:	****				
OK Cancel					

Note: To store Active Templates, the installation wizard creates the ActiveTemplates share, whose path is displayed in the **Active Templates Path** box. If you created another share in which to store Active Templates, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*

2. Active Administrator checks for broken templates every 30 seconds by default. To change the value, choose a value from the **Repair broken Active Templates automatically every** list.

3. If you want to send reports of broken templates to selected users via email, select the **Send a Report of Broken Templates By E-Mail** check box, and then click **Configure email settings**. The **E-Mail Settings** box appears.

-Mail Settings		X
E-mail Settings		ОK
E-mail server:		Cancel
E-mail Port:	(Leave blank to use default port)	
From User Name:		
From E-Mail Address:		
To User Name:		
To E-Mail Address:		
SMTP Authentication		
Use SMTP Authent	ication	
User Name:		
	Leave blank to use From User Name	
Password:		
Confirm Password:		

4. Set up the email service and select a user to receive the broken templates report.

E-mail server

Name of the email server.

E-mail Port

Name of the email port. Leave blank to use the default port.

From User Name

Name of the user to appear in the From box on the email generated to send the broken templates report.

From E-mail Address

Email address of the user whose name appears in the From box on the email generated to send the broken templates report.

To User Name

Name of the user to appear in the To box on the email generated to send the broken templates report.

To E-Mail Address

Email address to use to send the broken templates report.

- 5. To use SMTP Authentication, select the **Use SMTP Authentication** check box, and then enter a user name and password.
- 6. Click **OK** to close the E-mail Settings box and return to the **Configure the ActiveTemplate Auto-Repair Service** box.
- 7. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click to locate a group/user.
- 8. Click OK.

Object Level Backup Configuration

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. See *AD Ojbect Restore* in the *User Manual*.

CONFIGURING THE BACKUP SERVICE

 Click Start, point to Programs > ScriptLogic Corporation > Active Administrator, and then select Object Level Backup Configuration. The Configure the Active Directory Backup service dialog box opens.

Note: To store Active Directory backups, the installation wizard creates the ADBackups share, whose path is displayed in the **Active Directory Backup Path** box. If you created another share in which to store Active Directory backups, click ... to locate the share. See *Creating Network Shares to Store Active Administrator Data*

Configure the Active Directory Backu	ıp service	×
Active Directory Object Level Bacl Quickly recover from deleted or modif	kup / Restore ied objects in Active Directory.	44
Active Directory Backup Path: \\VM4-WIN2KSVR\ActiveAdministrator\4	ADBackups	
Backup the following domains: (Note: Windows 2003 Service Pack 1 or h	nigher is required to restore passo	words.)
Domains:	Supports Password Restore:	Add Domain
		Remove Domain
		Refresh Domain List
		Password Recovery
Run the backup:	▼ and ▼	
🔲 Create a Log File (kept in the same fo	older as the service executable - o	an grow large)
Log On		
Please specify a valid username and p	assword for the Object Level Bac	kup/Restore Service:
Username: <pre></pre> <pre></pre>	the name of a user with Domain A	dmin rights>
Password: **********	***	
Confirm password:	***	
OK	Cancel Backup Now	

2. If necessary, click Add Domain, and then locate the domain that you want to back up.

Note: If you are using Windows Server[™] 2003 Service Pack 1 (SP1) or higher, Active Administrator can restore passwords when you restore accounts that were deleted.

If the server you select is running Windows Server 2003 SP1, a message box appears asking if you want to enable password recovery. To enable password recovery, click **Yes**, and then click **Refresh Domain List**. **Yes** displays in the Supports Password Restore column.

ingure the nettre birt		
Active Directory Obje	ct Level Backup / Restore	
Quickly recover from de	eleted or modified objects in Active Directory.	
ctive Directory Backup Pa	ith:	
WM4-W/IN2KSVR) ActiveAdministrator) ADBackups		
	kanininstrator (ADBatkups	*
ackup the following doma lote: Windows 2003 Serv	ins: ice Pack 1 or higher is required to restore passwor	****
ackup the following doma lote: Windows 2003 Serv Domains:	ins: irs: ice Pack 1 or higher is required to restore passwori Supports Password Restore:	ds.) Add Domain
(1994-will2kSyR(Active) ackup the following doma lote: Windows 2003 Serv Domains: acme.com	ins: ice Pack 1 or higher is required to restore passwork Supports Password Restore: Yes	ds.) Add Domain
(1994-will2kSyR(Active) ackup the following doma Note: Windows 2003 Serv Domains: acme.com	ins: vice Pack 1 or higher is required to restore passwork Supports Password Restore: Yes	ds.) Add Domain Remove Domain
((VM4-WINZKSVR(ACtive) ackup the following doma Note: Windows 2003 Serv Domains: acme.com	ins: irice Pack 1 or higher is required to restore password Supports Password Restore: Yes	ds.) Add Domain Remove Domain Refresh Domain List

Note: To remove a selected domain from the list, click **Remove Domain**. To enable or disable password recovery, click **Password Recovery**. See *Configuring Password Recovery*

- 3. In the **Run the backup** box, select to run the backup **Every Day** or **Twice a Day**.
- 4. From the **at** list, select a time or times to run the backup.
- 5. If you want to create a log file for the backup, select the **Create a Log File** check box.
- 6. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click ... to locate a group/user.

Note: If you want to back up the domain without waiting for the scheduled time, click **Backup Now**.

7. Click OK.

CONFIGURING PASSWORD RECOVERY

If you are using Windows Server 2003 SP1 or higher, Active Administrator can restore passwords when you restore accounts that were deleted. When you add a domain that is running Windows Server 2003 SP1 to the Active Directory Object Level Backup/Restore utility, you are prompted to enable password recovery. You also can use the Forest Prep Utility to enable or disable password recovery.

- 1. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator**, and then choosing **Forest Prep Utility**.
- 2. Select the domain, and then click **Password Recovery**. The **Forest Prep Utility** dialog box opens.
- 3. In the Enter Domain box, type the domain name, or click, and then select a domain.

Active Ac	lministrator - Forest Prep Utility 🛛 🔀	
IJ	Note: Windows 2003 Service Pack 1 or higher is required to restore passwords.	
	Enter Domain: (fully qualified domain or dc name - domain.com or dc.domain.com)	
	acme.com	
	Supports Password Restore: Refresh	
	Allow Active Directory to save passwords in the object's tombstoned state (requires a small modification to one object in the schema)	
	Modify Schema to Allow the Restoration of Passwords	
	Revert Schema to Not Allow the Restoration of Passwords	
	Close	

Important: The domain must be running Windows Server 2003 (SP1) to allow the restoration of passwords.

4. To allow the restoration of passwords, click **Modify Schema to Allow the Restoration of Passwords**. Click **Refresh. Yes** displays in the **Supports Password Restore** box.

To disallow the restoration of passwords, click **Revert Schema to Not Allow the Restoration of Passwords**. Click **Refresh**. **No** displays in the Supports Password Restore box.

5. Click **Close**. The **Configure the Active Directory Backup Service** dialog box displays the selected settings.

BACKING UP FROM THE COMMAND LINE

Active Administrator includes a command line function — **ADBkpSvc.exe** — that you can use to access the backup service. The file is located in the Active Administrator installation directory.

ADBkpSvc.exe -config

Opens the **Configure the Active Directory Backup service** dialog box. See *Configuring the Backup Service*.

ADBkpSvc.exe -backupnow

Backs up the domains specified in the **Configure the Active Directory Backup service** dialog box.

ADBkpSvc.exe -help

Displays the help window for the command.

ADBkpSva	×
(i)	Active Administrator - Active Directory Backup Service
	Copyright (2005) - ScriptLogic Corporation http://www.scriptlogic.com
	A service to backup Active Directory objects for online restore. Usage: ADBkpSvc.exe [-install -uninstall -debug -config -help -backupnow]
	<u>ОК</u>]

ADBkpSvc.exe -debug

Opens the Active Directory Backup Log window.

A	Active Administrator - Active Directory Backup Log 📃 🔲 🔀			
	Time	Description		
	6/3/2005 3:46:12 PM	Loading schedule		
	6/3/2005 3:46:12 PM	Next scheduled backup is at 03:00		
	6/3/2005 3:46:13 PM	You can run 'SWADBkpSvc.exe -backupnow' to run the backup immed		
	4			
1				
		Stop		

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™ - ScriptLogi	c Corporation						_ 🗆 >
File Security Group Policy Tools Help							
Group Policy History	Grou	p Policy Offline Repository	 	🚮 Re:	sultant Set of	Policies (RS	SoP)
Active Directory Security	Active Iem	iplates 🛛 🖄 Ai	tive Directo	ry Auditing	ի 💽 և	roup Policy	Ubjects
Group Policy Objects by Cor	tainer	🚠 AD Object Res	ore	19	Client Side T	roubleshoo	ting
Please select a domain View all Computers in Domain: acm Curre	e.com nt Domain Controller:	vm4-win2ksvr.acme.cor	2		C	ionnect to D	Iomain
Computers	Group Policy Vert	bose Logging Options —					
Computers Computers Computers PC-45578 Opain Controllers W14-WIN2KSVR ForeignSecurityPrincipals Officient System	☐ Generate det Generate veri Software Dep View Softw Generate log Level: Defa	ailed Group Policy logging bose logging of all activitie oloyment Group Policies, vare Deployment Log File for troubleshooting Group ault Logging	to the Appli s relating to Policies rela View Us	cation event log. the processing o ating to user confi ser Configuration I	if iguration. Log File		
	- Group Policy Eve	ents					
	Tune	Date / Time	Sour	ce [[Category	Event	∐ser ▲
	Information Information	6/29/2005 1:48:58 PM 6/29/2005 9:07:27 AM 6/20/2005 11:10:13 AM 6/3/2005 8:05:48 AM 7/27/2004 8:51:43 AM 7/26/2004 9:09:44 AM 7/22/2004 8:41:18 AM 7/22/2004 11:04:37 AM	Scel Scel Scel Scel Scel Scel Scel Scel	Cli P Cli P Cli P Cli P Cli P Cli P Cli P Cli P	None None None None None None None None	1704 1704 1704 1704 1704 1704 1704 1704	N/A N/A N/A N/A N/A N/A N/A N/A 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 Proper	ties			×
Date: Time: Type: User: Computer:	11/16/2004 9:03:35 AM Information N/A VM4-WIN2KSVR	Source: Category: Event ID:	SceCli None 1704	+ +
Description Security p	: olicy in the Group polic	:y objects ar	re applied successfull	y.

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.

🖉 userenv.log - Notepad
File Edit Format Help
USERENV(cc.b4) 12:53:19:888 LoadProfileInfo: Failed to open profile mapping key with USERENV(cc.d8) 12:59:50:297 ReadMembershipList: Group S-1-5-21-1960408961-507921405-72 USERENV(cc.660) 11:21:36:312 ProcessGPORegistryFile: CreateFile failed with 1351 USERENV(cc.660) 11:21:36:312 ProcessGPORegistryPolicy: ParseRegistryFile failed. USERENV(cc.660) 11:21:36:312 ProcessGPOREgistryPolicy: ParseRegistryFolicy failed. USERENV(cc.660) 11:21:36:312 ProcessGPOS: Extension Registry ProcessGroupPolicy failed USERENV(cc.660) 11:21:36:546 ProcessGPOS: Extension Security ProcessGroupPolicy failed
Y NOT THE REPORT OF THE REPORT

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.

- 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.
- Access Control Settings for acme

4. Open the **Auditing** tab.

Type	Name Everyone		Access Special	Apply to This object and all child obje.
Add	i	Remove	View/Edit	
Add his auditir bjects.	1	Remove ned directly on t	View/Edit	uditing entry is inherited by child
Add his auditir bjects.	l	Remove ned directly on I	View/Edit	uditing entry is inherited by child

- 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.

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.

- 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.
- 6. Right-click the Active Administrator Even Notification Service, and then click **Properties**.
- 7. Open the Log On tab, and then specify the account to run the service.
- 8. 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

.edf file, 26, 34 .ldf file, 10 .lic file, 21 .mdf file, 10

Α

AA_Admin group, 5 Active Administrator removing, 49 Active Directory, 1 backing up, 15 Active Template, 2 repair broken, 13 ADBkpSvc.exe, 43 Appmgmt.log file, 45 auditing, 3 setup, 46

В

back up Active Directory, 15 backing up Active Directory, 40

С

collection monitor removing server, 34 viewing, 34 command line ADBkpSvc.exe, 43 configuring password recovery, 42 console setting up, 37 console install, 17 create new database, 10, 22

D

database create new, 10, 22 DBWizard.exe, 4 domain control agents modifying, 33 download Active Administrator, 4

Ε

email broken template notification, 13 email notification, 26 e-mail notification changing accoutn that runs, 33, 48 email server configuring, 31 evaluate product, 21 Event Configuration Utility, 29 event data purging, 35 event log opening, 34 event monitoring service, 26 event notification, 28 Event Notification Service changing account that runs, 33, 48 EventDefinitions.edf, 34

G

GPO history, 11, 36 GPO History, 36, 38 GPO History share, 5 GPOHistory folder, 12, 14, 15, 36, 38, 40 Group Policy, 2 Group Policy History service, 11

L

license file, 21 loading event definitions, 34 log file Appmgmt.log, 45 UserEnv.log, 45

Μ

Microsoft SQL Server, 4 monitoring service removing, 35 starting, 33 stopping, 33 MSDE 2000, 4

Ρ

password recovery

50

UPDATED 22 DECEMBER 2005

configuring, 42 passwords restoring, 42 polling interval, 11, 36 purging event data, 35

R

removing monitoring service, 35 restoring passwords, 42

S

security event database, 5

server opening event log, 34 removing from collection monitor, 34 server install, 5 start monitoring service, 33 status collection monitor, 34 stop monitoring service, 33

U

UserEnv.log, 45