ACTIVE ADMINISTRATOR™

ScriptLogic® Active Administrator™ 4 Getting Started Guide

SCRIPTLOGIC

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

1.561.886.2400
www.scriptlogic.com

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

DOCUMENTATION CONVENTIONS

Typeface Conventions

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

CONTACTING SCRIPTLOGIC

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

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

561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support

561.886.2499 Fax

www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

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

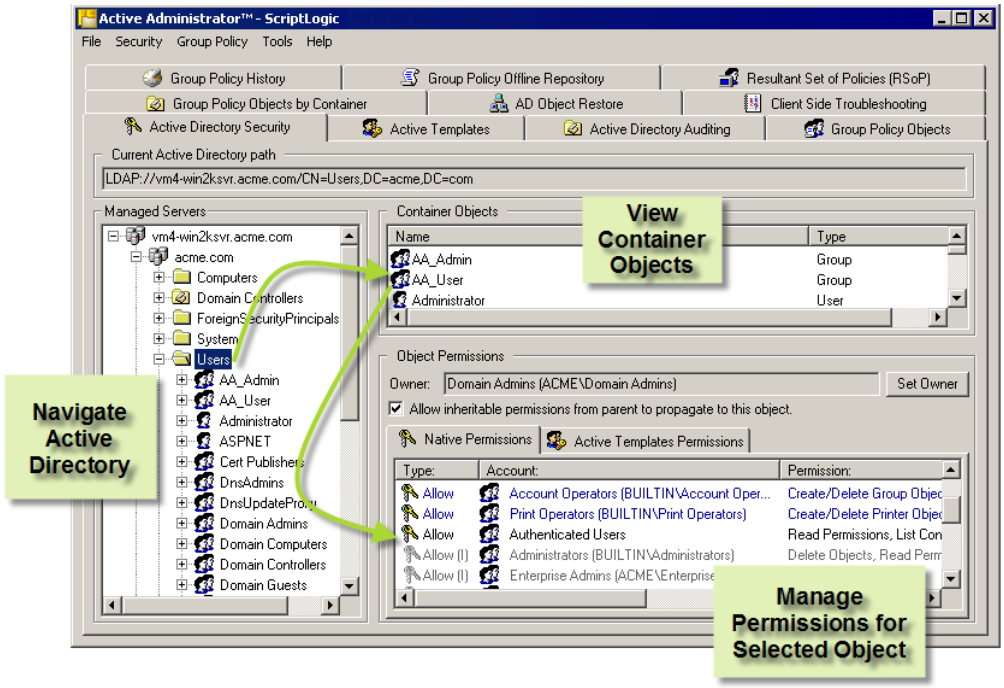
- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search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

Contents

What is Active Administrator?

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.

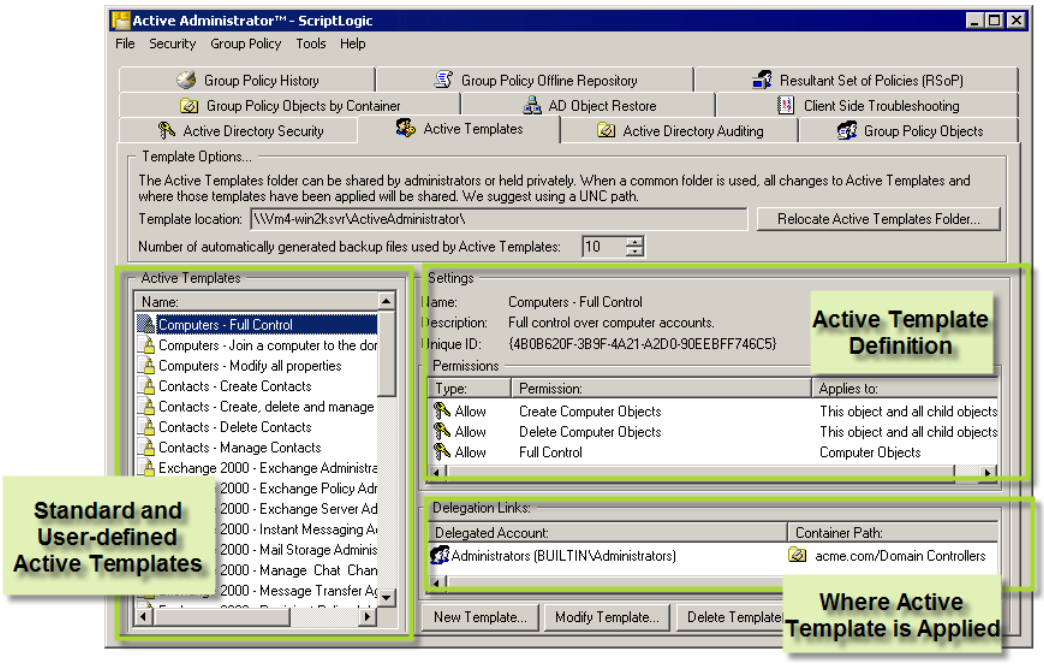


- **Active Directory Backup and Restore.** Administrators can select a domain that contains Windows Server™ 2003 domain controllers and back up all Active Directory objects in that domain. When a situation occurs that require an object to be restored, administrators can select the object from a list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

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

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

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



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.

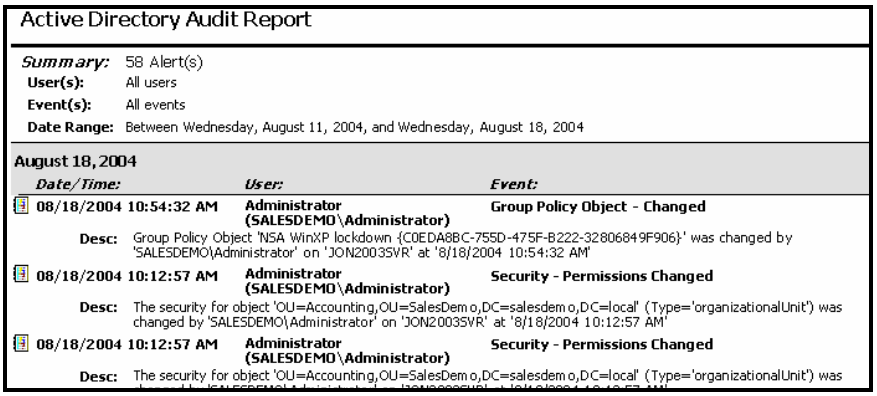
- **Active Templates Auto-Repair.** Active Templates, which are used to grant specific sets of Active Directory rights to an object, can be configured so that they are automatically reapplied if any of their permissions within the template are accidentally removed. Additionally, administrators can be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



Active Directory Audit Report

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

August 18, 2004

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

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

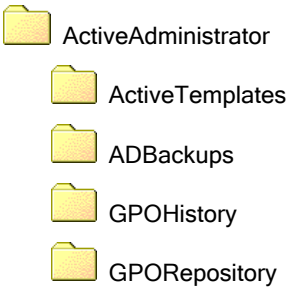
The server installation wizard prompts you to create the security event database in MSDE 2000 on the local computer. You also can create the security event database on an existing Microsoft SQL Server 2000 computer anywhere on your network. See *Setting Up a Security Event Database*.

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.



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.

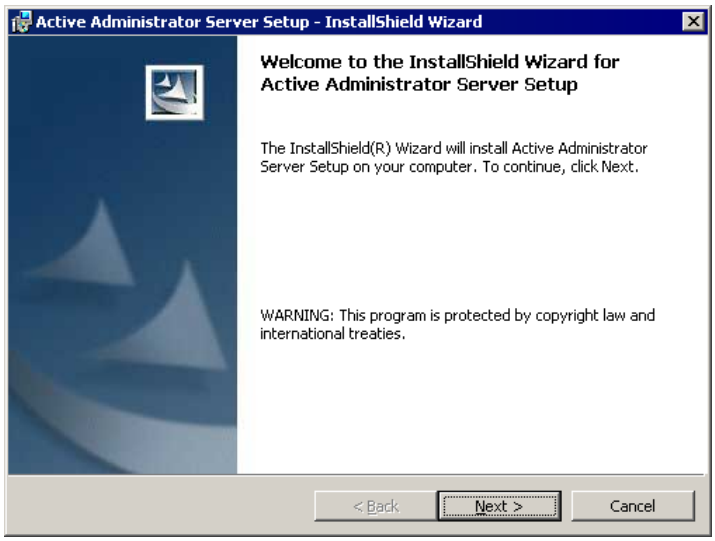
RUNNING THE ACTIVE ADMINISTRATOR SERVER INSTALLATION WIZARD

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.

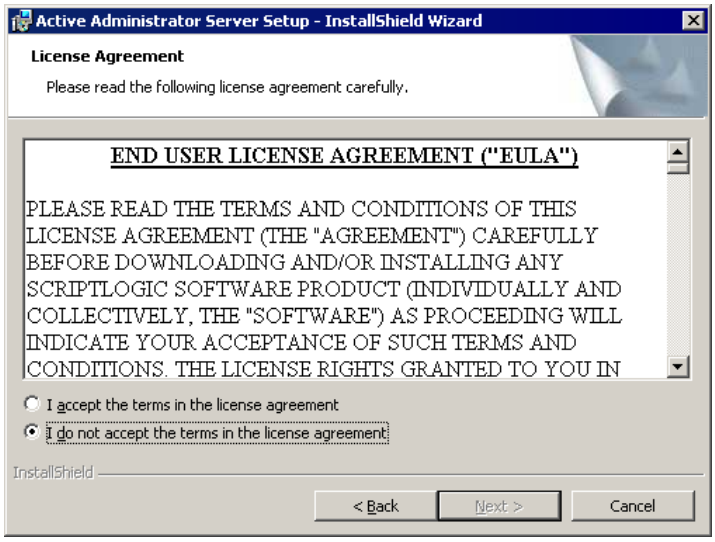
Note: The server setup needs to be installed on only one computer.

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

1. After downloading Active Administrator, double-click the **AAServerSetup4*xx*.msi** file, or right-click the **AAServerSetup4*xx*.msi** file, and then select **Install**. The **Welcome** dialog box appears.

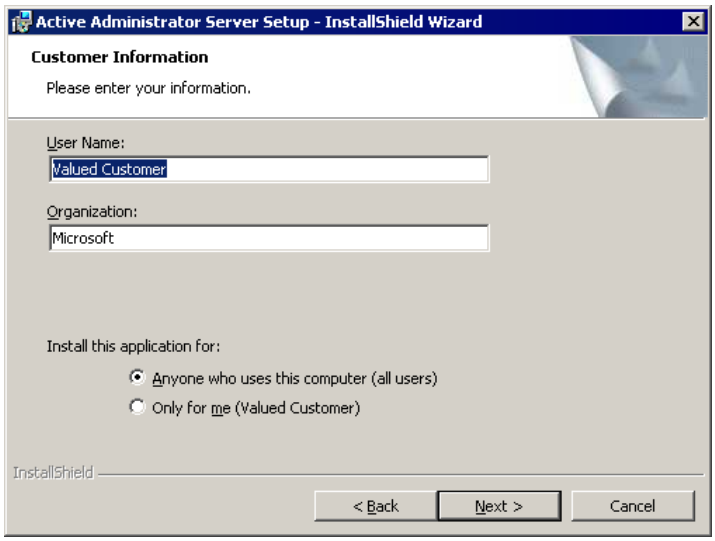


2. Click **Next**. The **License Agreement** dialog box appears.



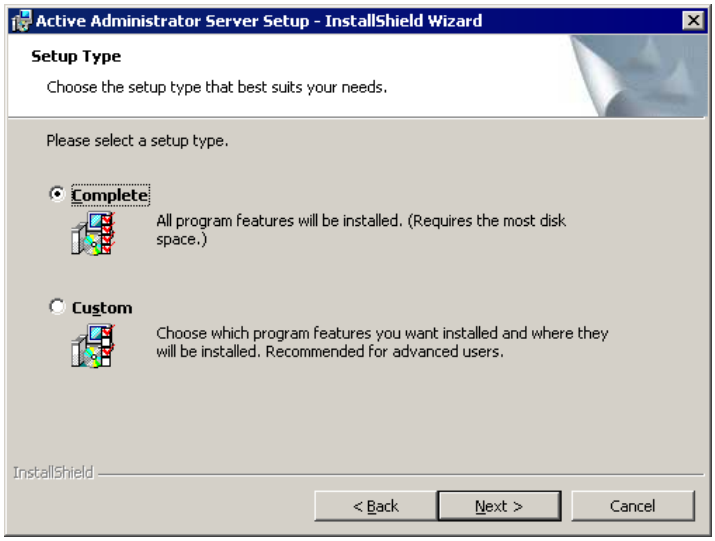
Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or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



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.

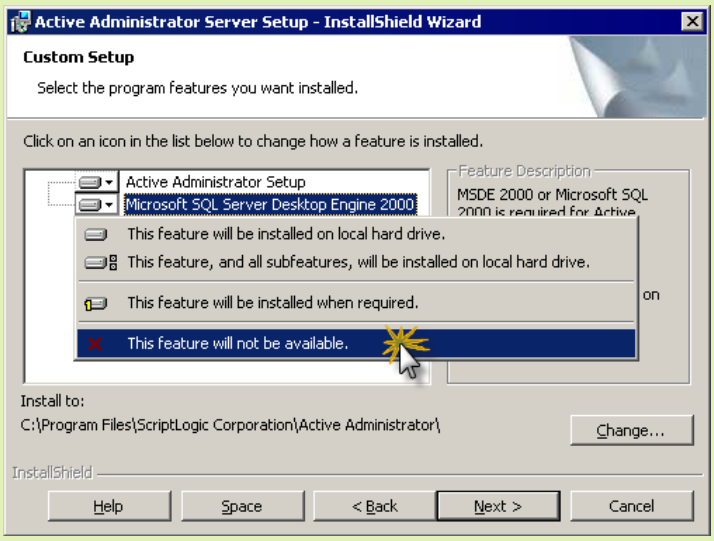
4. Select whether to install the application for just yourself or all users, and then click **Next**. The **Setup Type** dialog box appears.



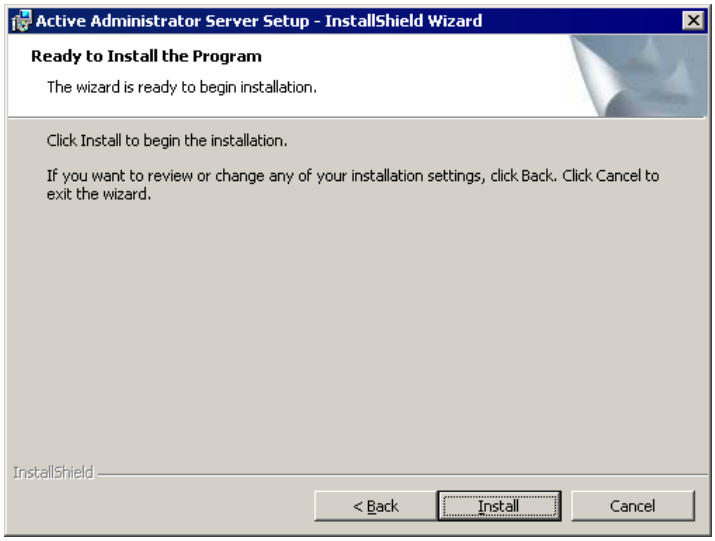
Note: MSDE 2000 is installed with the complete install of Active Administrator Server. To omit installing MSDE 2000, choose **Custom**. See *Installing Microsoft SQL Server or MSDE 2000*.

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**.



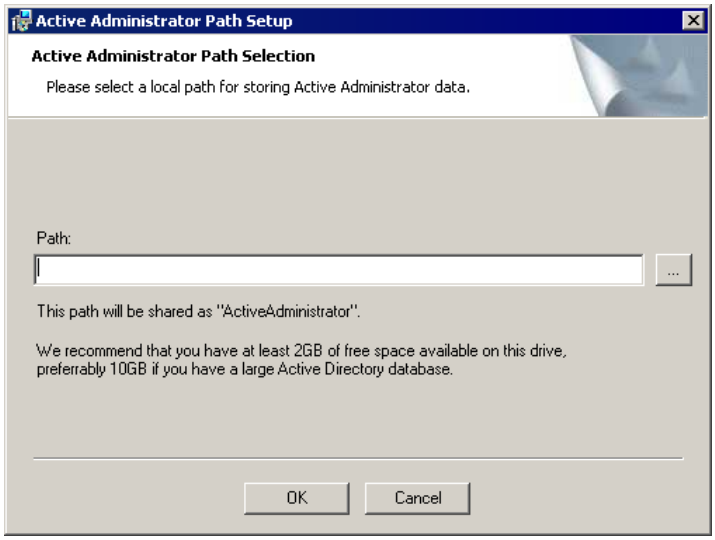
The **Ready to Install the Program** dialog box appears.



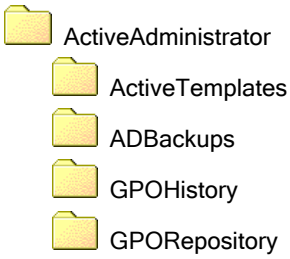
6. To begin the installation, click **Install**. The **Installing Active Administrator Console** box displays a status bar that indicates the installation progress.

Storing Active Administrator Data

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



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



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.

9. Click **OK** to continue.

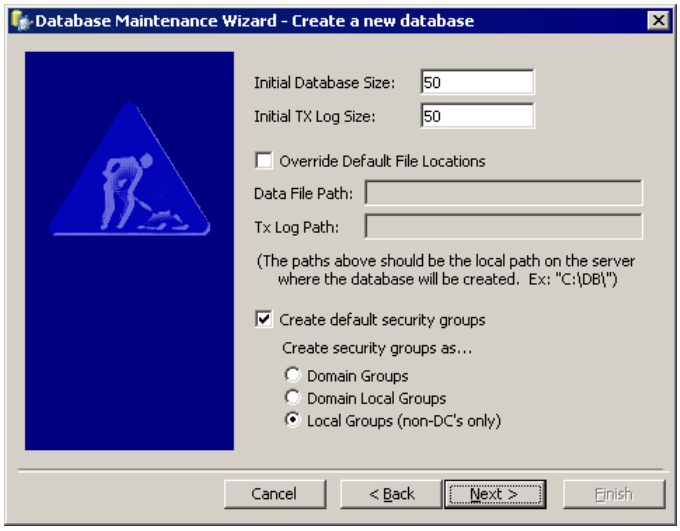
Creating a New Database

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).

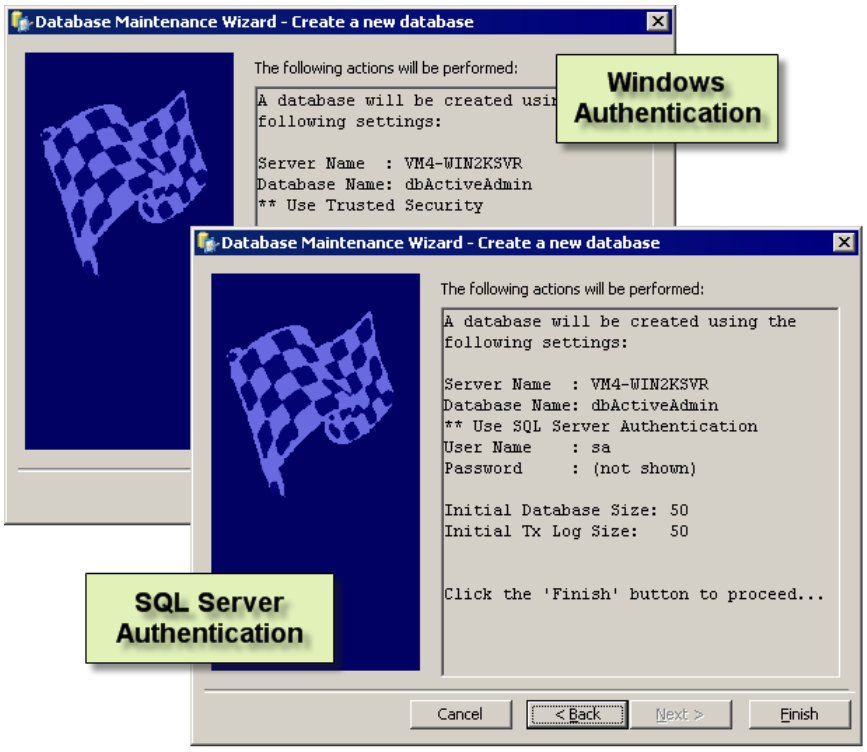
10. If necessary, type the name of the Microsoft Windows server that is running Microsoft SQL Server 2000 in the **SQL Database Server Name** box, or click … to locate registered servers that may also be running the database engine.
11. If necessary, type the name of the database to create in the **Database 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.



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.



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

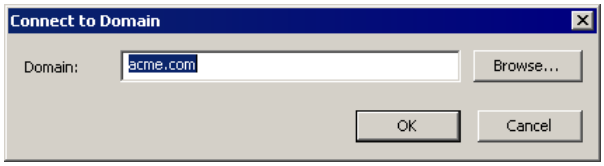
Configuring Group Policy History Service

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

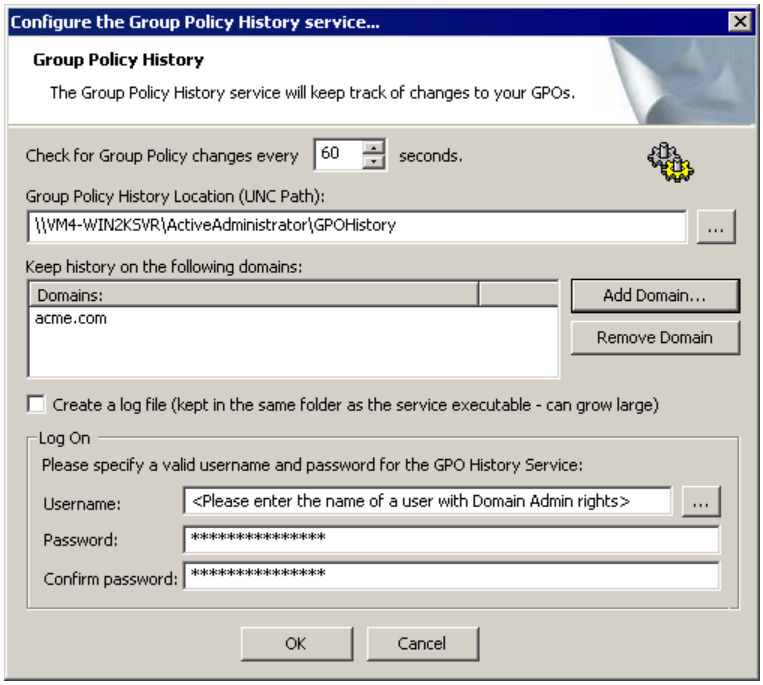
20. In the **Polling Interval** list, select how often you want the Group Policy History service to poll the domain controllers for Group Policy object (GPO) changes at a specified polling interval.

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.

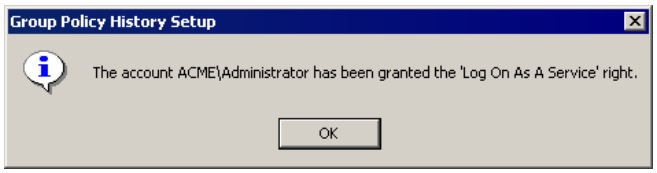
21. To store GPO history, the installation wizard creates the GPOHistory folder, whose path is displayed in the **Group Policy History Location** box. If you created another share in which to store GPO history, click … to locate the share. See *Creating Network Shares to Store Active Administrator Data*.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



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.



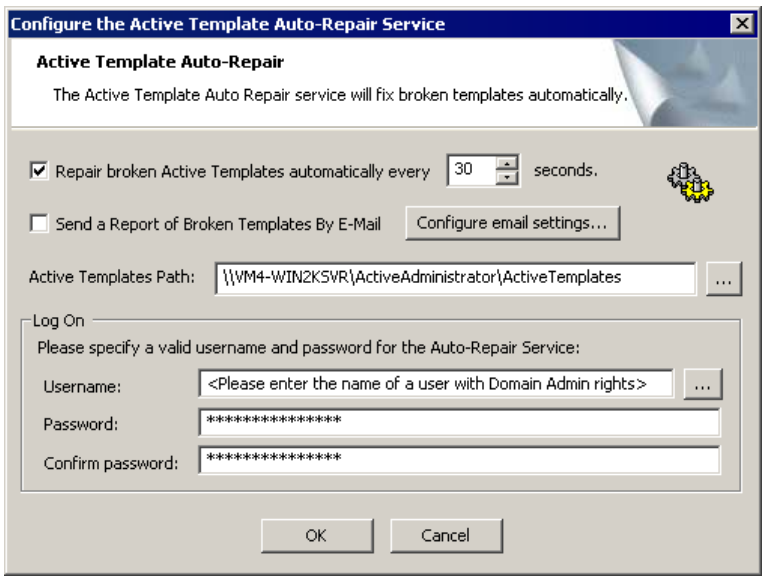
25. If you want to see exactly what the GPO History service is doing, select the **Create a log file** check box to create a debug log file.
26. In the **Log On** area, type a user name and password for a group/user with Domain Admin rights, or click … to locate a group/user.
27. Click **OK**. An information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



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

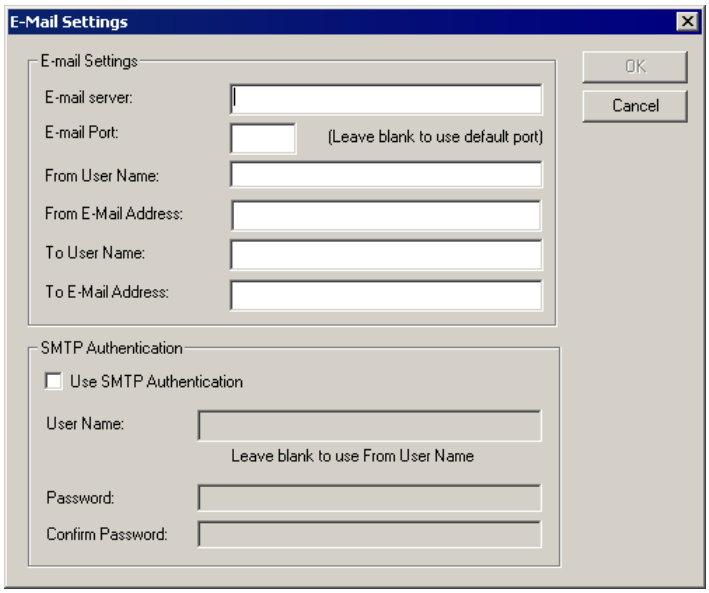
Configuring Active Template Auto-Repair Service

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.



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.



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.

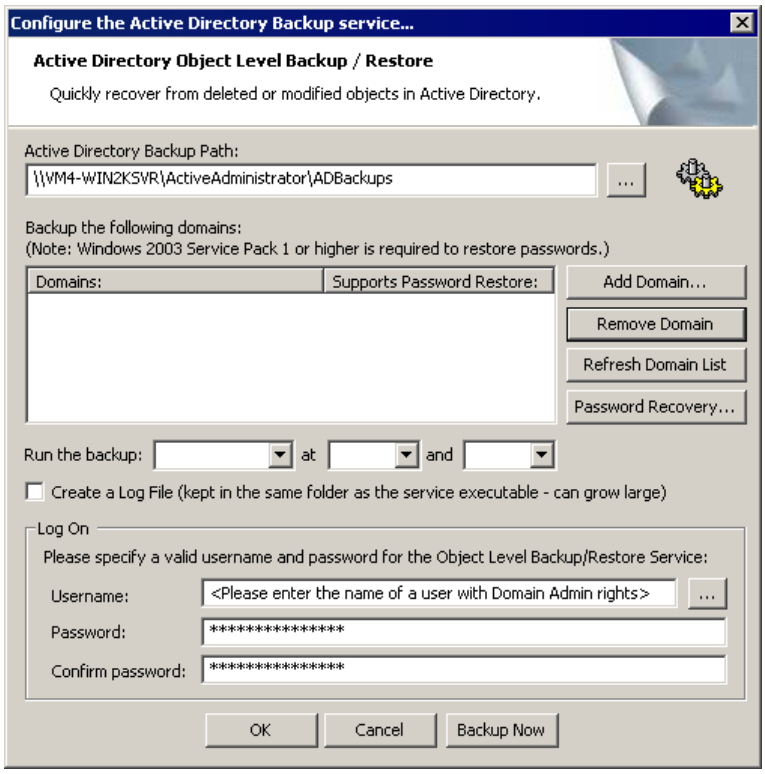
35. Click **OK** to continue with the install process.

    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.

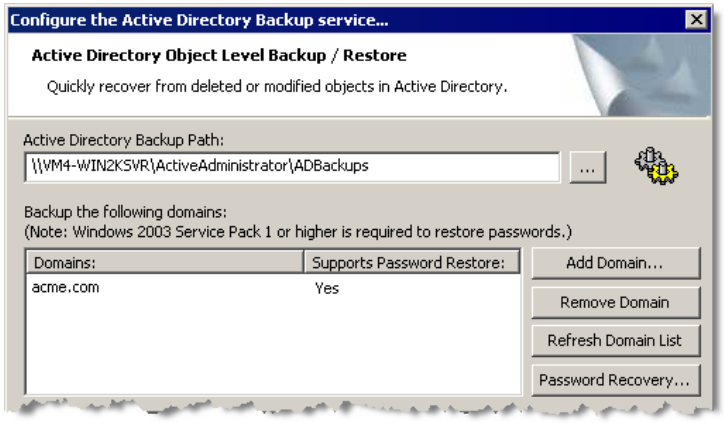
36. To store Active Directory backups, the installation wizard creates the ADBackups folder, whose path is displayed in the **Active Directory Backup Path** box. If you created another share in which to store Active Directory backups, click ... to locate the share. See *Creating Network Shares to Store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



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.

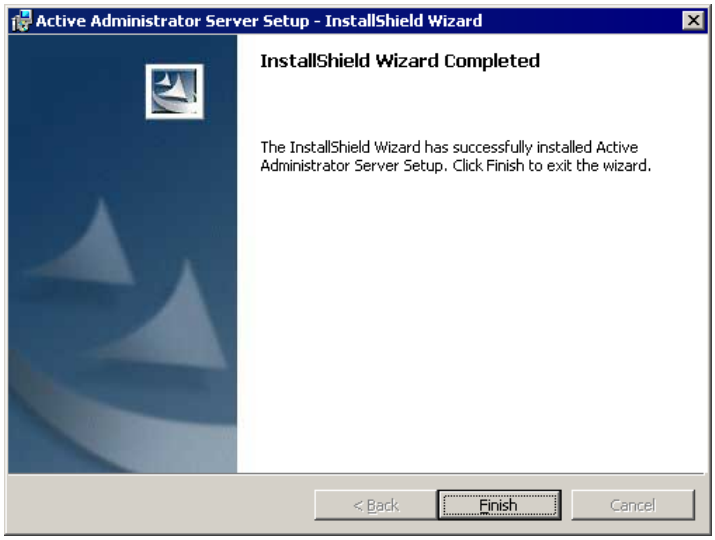
Note: To remove a selected domain from the list, click **Remove Domain**.

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

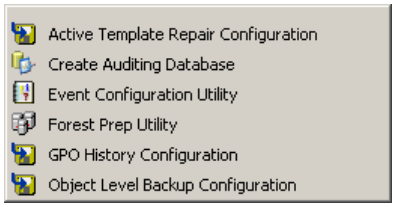
42. Click **OK** to continue with the install process.

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.



44. Click **Finish**. The following Active Administrator components are installed:

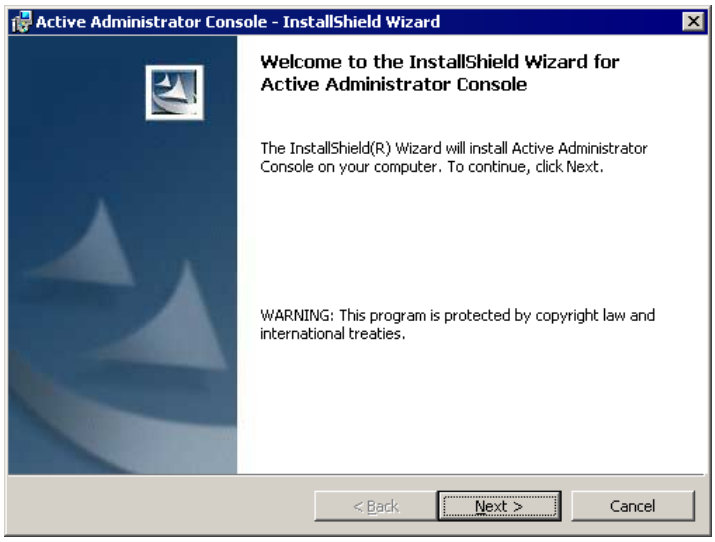


During installation, you configured some of these components. If you want to make changes, access each component individually.

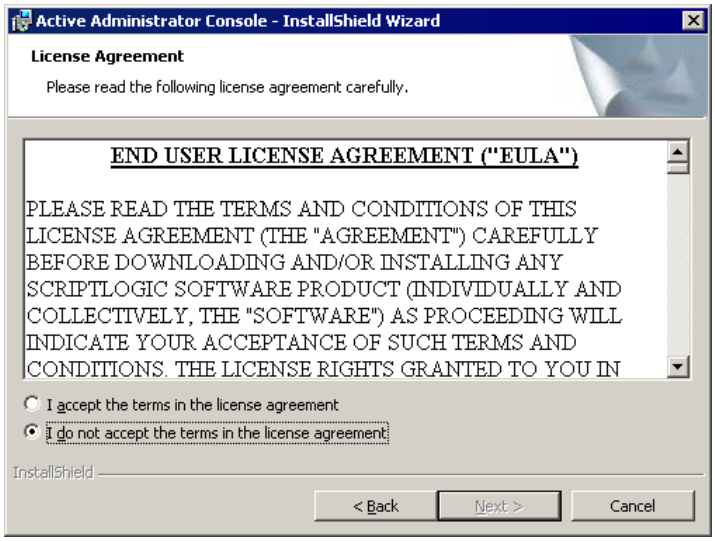
RUNNING THE ACTIVE ADMINISTRATOR CONSOLE INSTALLATION WIZARD

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 **AAConsoleSetup4*xx*.msi** file, and then select **Install**. The **Welcome** dialog box appears.

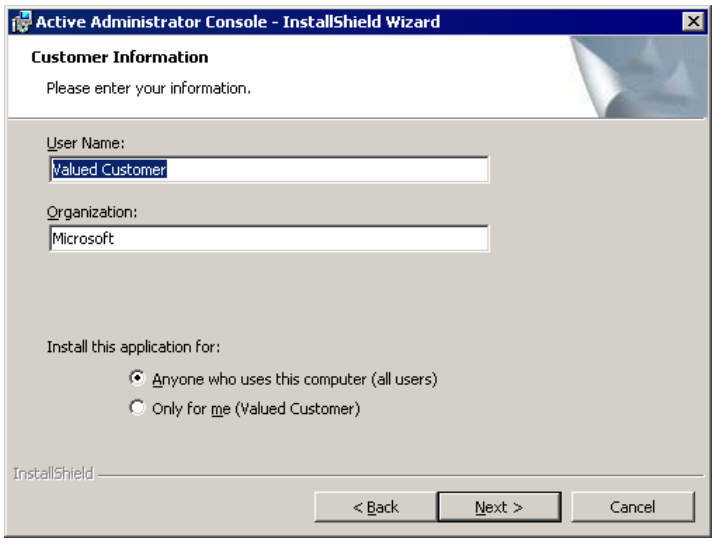


2. Click **Next**. The **License Agreement** dialog box appears.



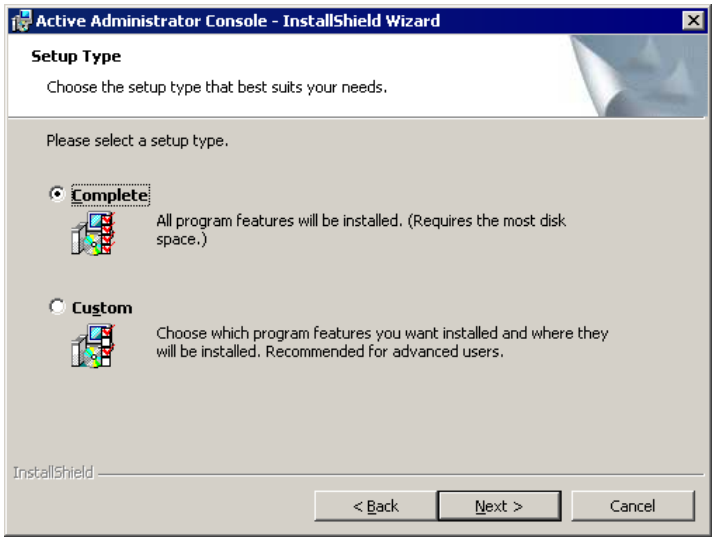
Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or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

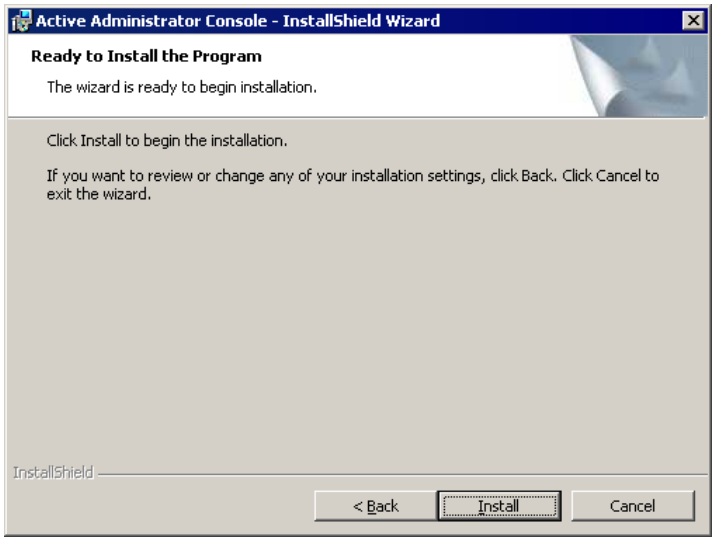


The **User Name** and **Organization** boxes default to the values set when the operating system was installed. You can choose to install the application for all users or just you.

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

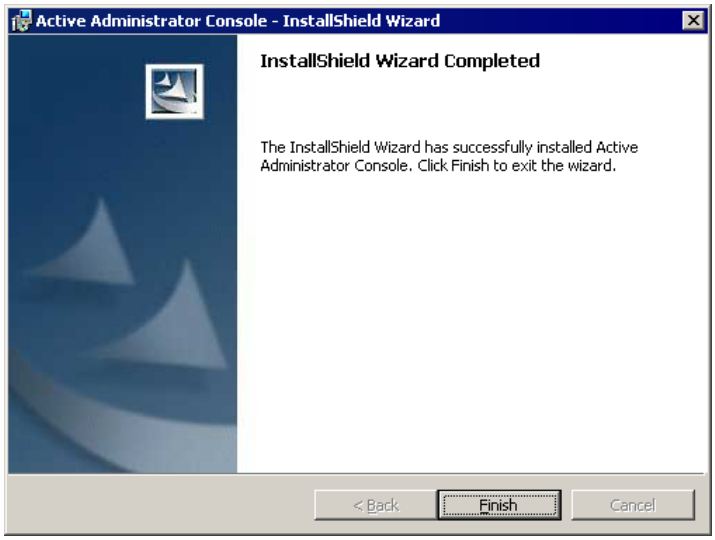


5. Click **Next**. The **Ready to Install the Program** dialog box appears.

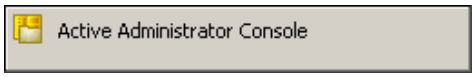


6. To begin the installation, click **Install**. The **Installing Active Administrator Console** dialog box displays a status bar dialog that indicates the installation progress.

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



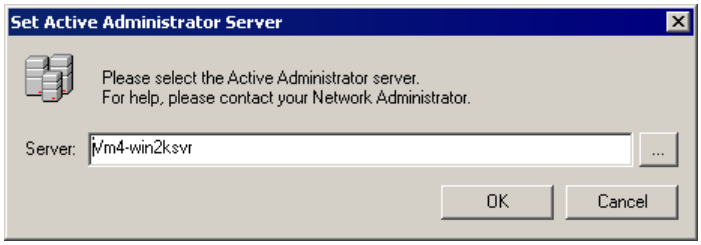
7. Click **Finish**. The following Active Administrator component is installed:



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 ... to locate a server.



4. Click **OK**.

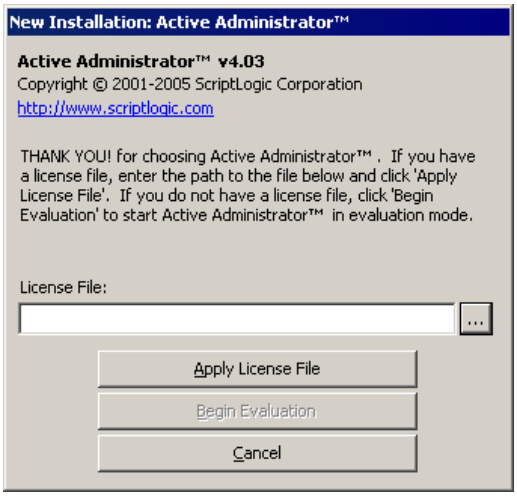
STARTING ACTIVE ADMINISTRATOR

- 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

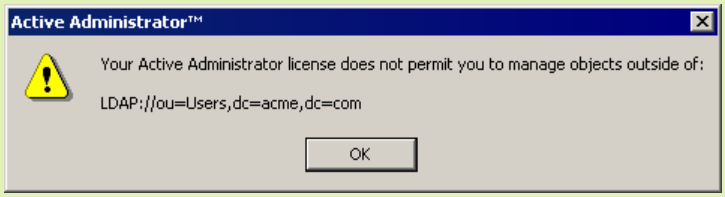
The first time you start Active Administrator Console or the Event Configuration Utility, you see the **New Installation** dialog box, which allows you to apply a license file or evaluate the product without a license, as well as contact ScriptLogic Corporation and visit our website for further information.



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.



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.

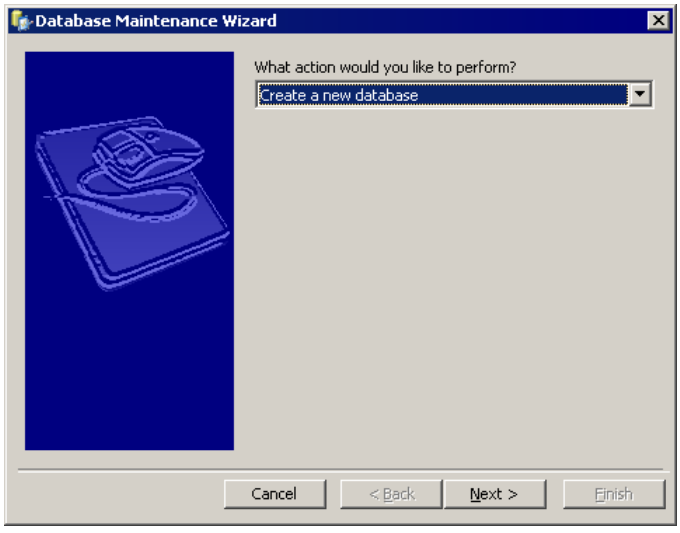
SETTING UP A SECURITY EVENT DATABASE

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.

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).

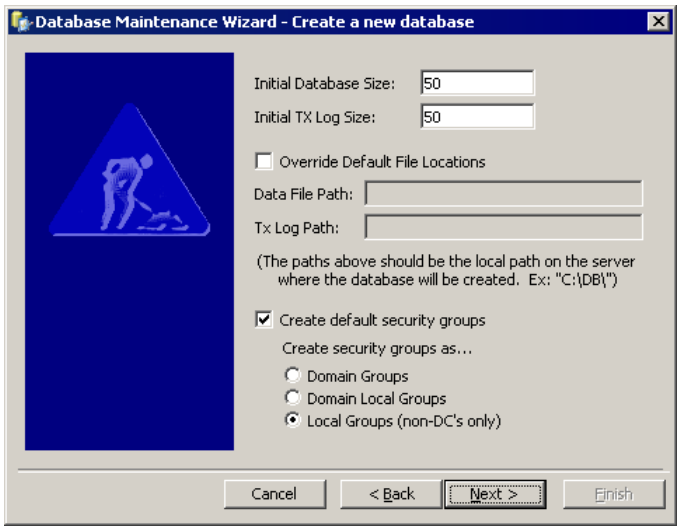
4. If necessary, type the name of the Microsoft Windows server that is running Microsoft SQL Server 2000 in the **SQL Database Server Name** box, or click … to locate registered servers that may also be running the database engine.

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.

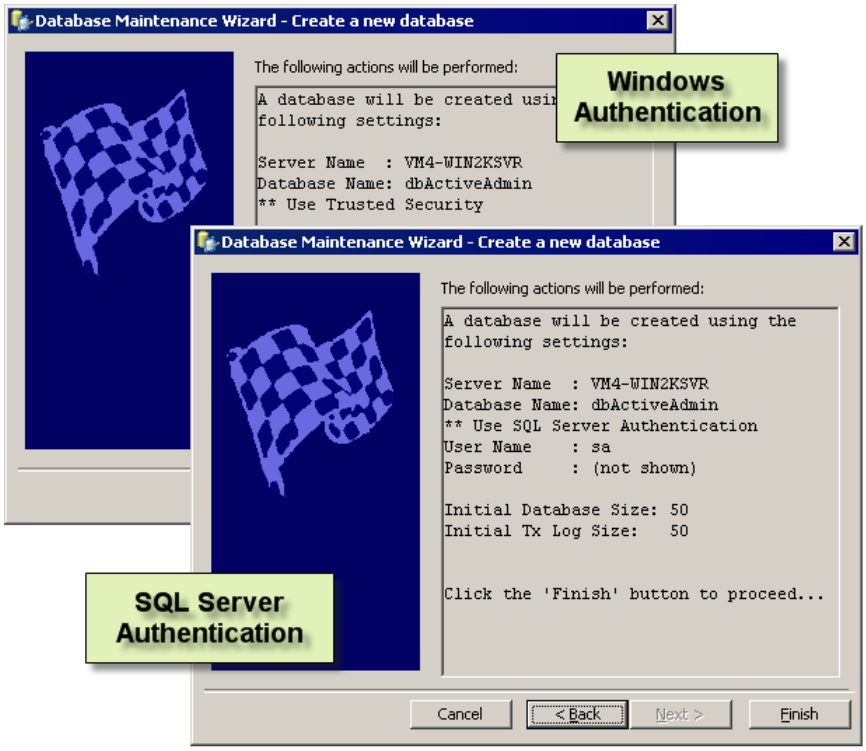
Note: If you want to use Windows Authentication, the SQL server must be configured to use trusted security, and the Active Administrator Security Log Monitor service must be configured with a domain account that has access to update the database.

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



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.



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

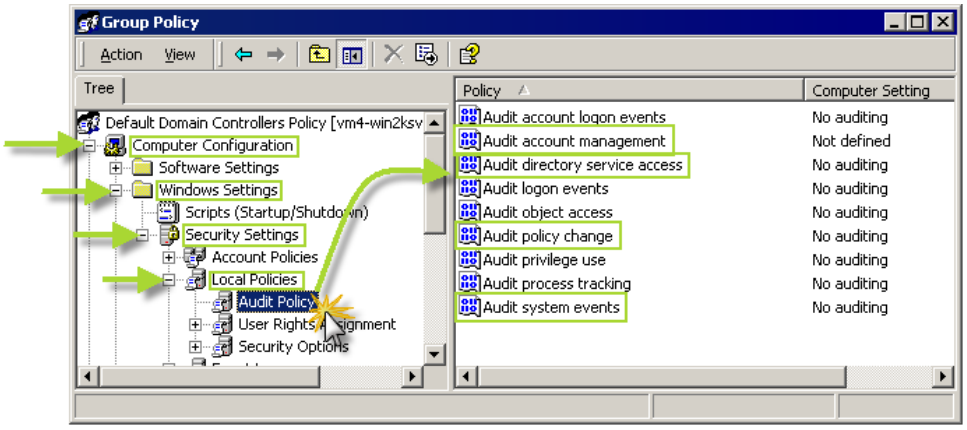
SETTING UP AUDITING ON DOMAIN CONTROLLERS

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.

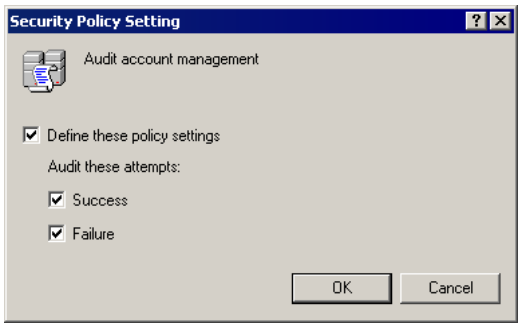
1. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator**, and then select **Active Administrator Console**. The **Active Administrator Console** opens to the **Active Directory Security** tab.
2. Open the **Group Policy Objects** tab.
3. In the **Group Policy Name** 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**.



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

   - **Audit account management**
   - **Audit directory service access**
   - **Audit policy change**
   - **Audit system events**



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

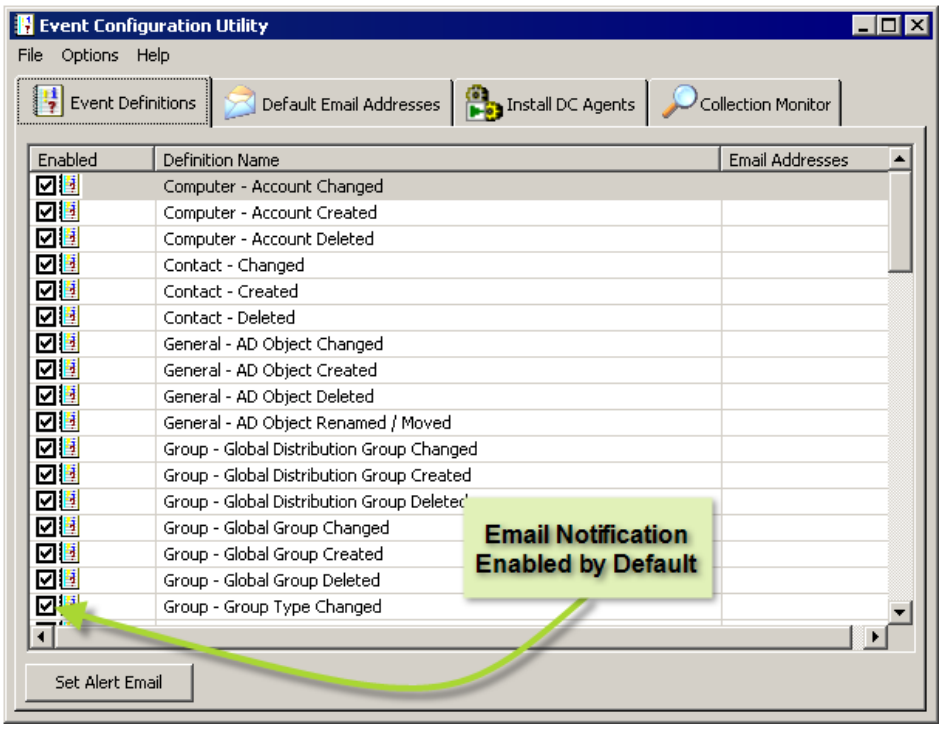
CONFIGURING THE EVENT MONITORING SERVICE

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.



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

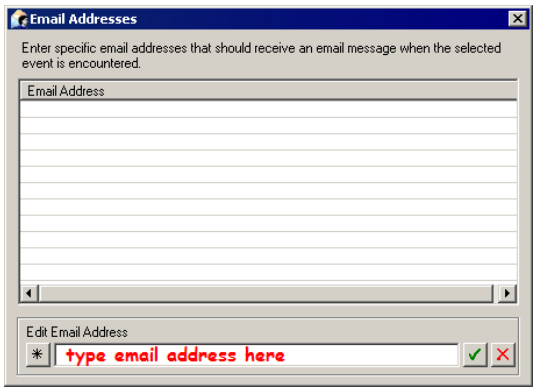
Disabling Email Notification

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

Setting Individual Event Notifications

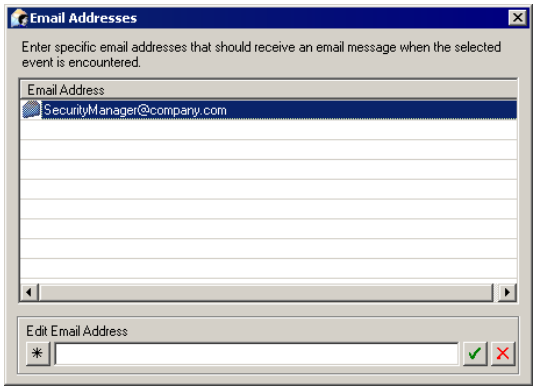
Each event in the list can have its own list of email addresses that will receive notification. You only need to enter an email address for a particular event if that person receiving the email is interested in that event.

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.



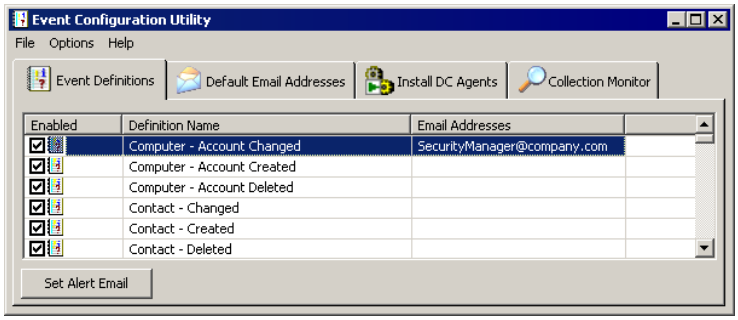
- To clear the **Edit Email Address** box, click ✳.

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



- To remove a selected email address from the **Email Address** list, click ✕.

4. Click ✕ to close the **Email Addresses** box. The **Event Configuration Utility** window displays the email addresses in the **Email Addresses** column.

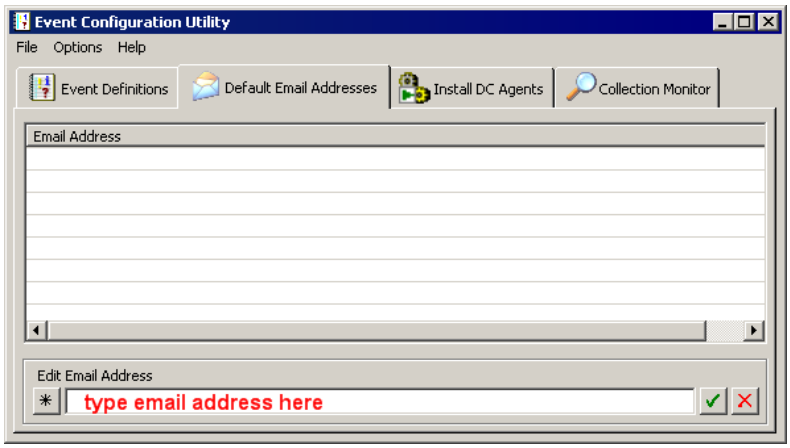


5. If necessary, enable email notification by selecting the ☑ check box in the **Enabled** column next to the event.

Setting Global Event Notifications

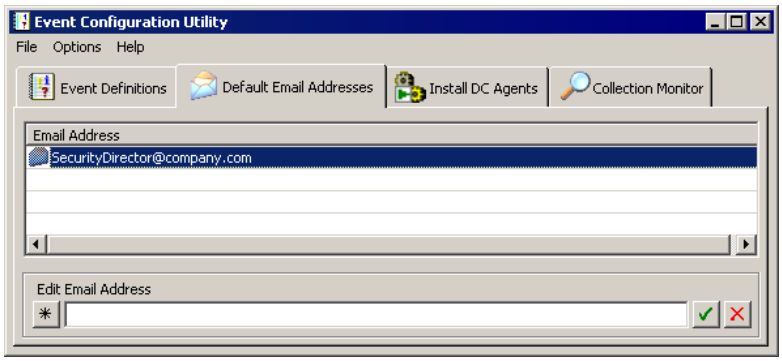
There may be some persons who want to receive event notifications for every event that is enabled on the **Event Definitions** tab. Set these email addresses as the default.

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



   - To clear the **Edit Email Address** box, click ✳.

2. In the **Edit Email Address** box, type an email address, and then click ✓ or press **Enter**. The email address displays in the list.



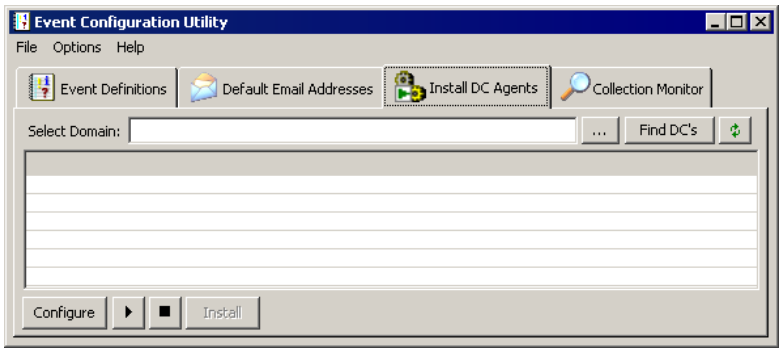
   - To remove a selected email address from the **Email Address** list, click ✕.

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.

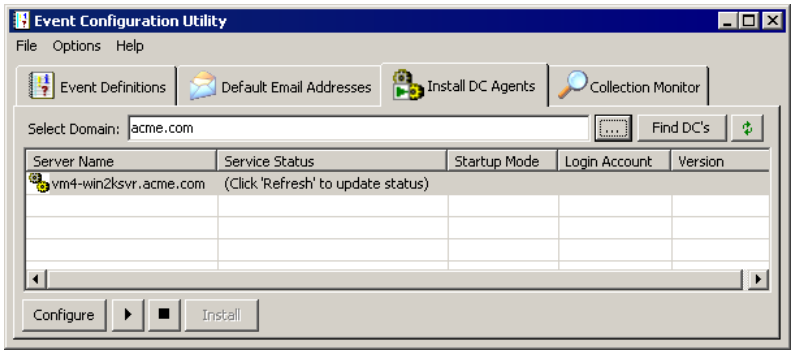
Installing Domain Controller Agents

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.

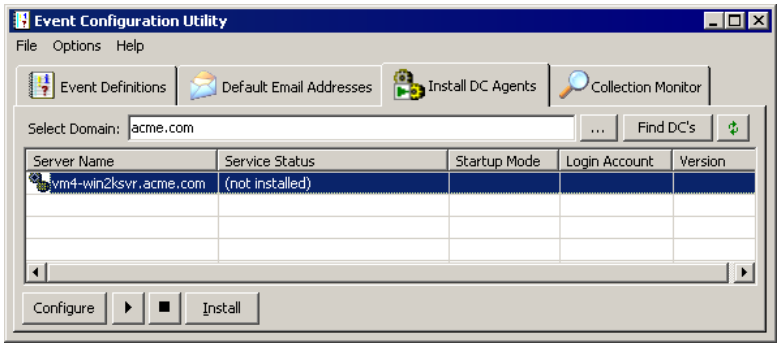
1. From the **Event Configuration Utility** window, open the **Install DC Agents** tab.



2. Click ... . The **Connect to Domain** box opens.
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)**.



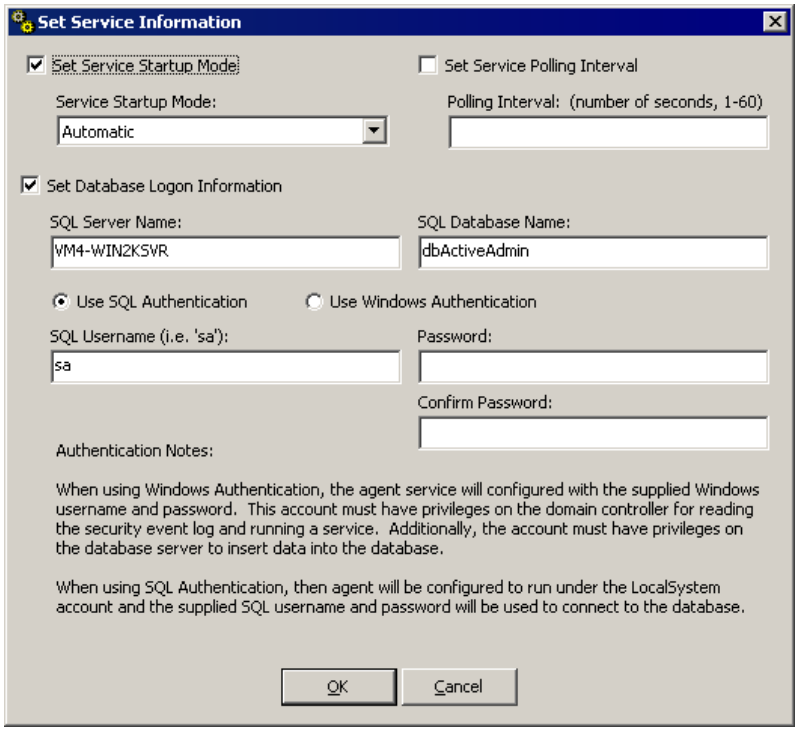
5. Click to refresh the service. To enable the **Install** button, **(not installed)** must display in the **Service Status** column.



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 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.

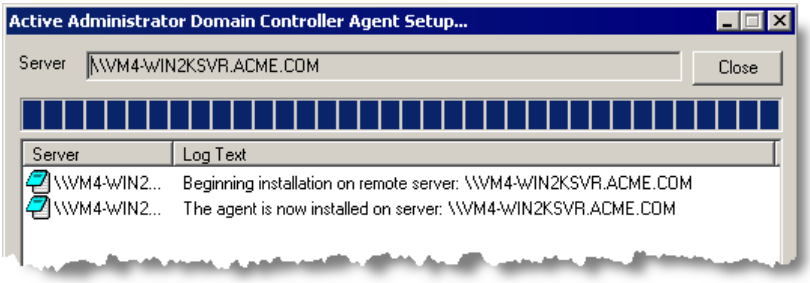
Set Polling Interval
In the **Polling Interval** box, type the number of seconds that may elapse between checking for new events in the Security event log. This number is initially set to 5 seconds, but may be adjusted to as long as 60 seconds.

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.



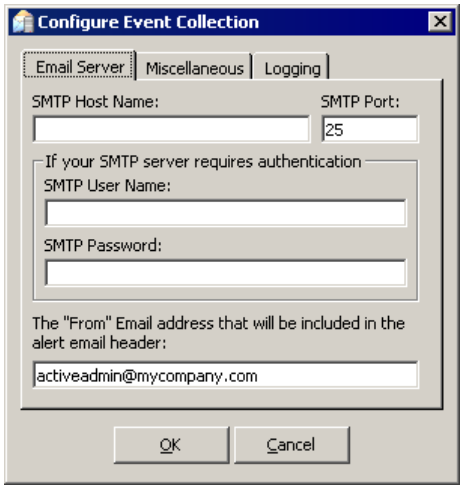
8. When the installation is complete, click **Close**. The **Service Status** column displays **Stopped**.

9. Select the domain controller, and then click ▶ 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.



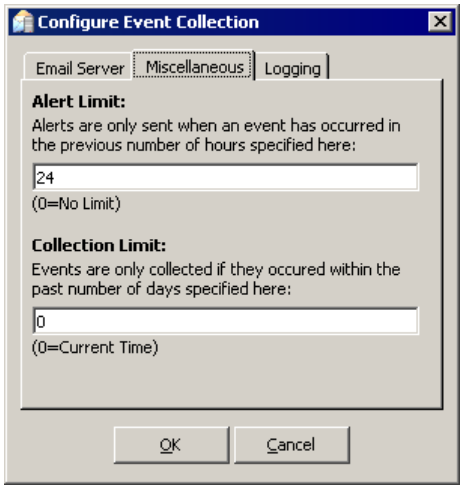
2. In the **SMTP Host Name box**, type the name of the SMTP server that sends the alert emails.

3. In the **SMTP Port** box, type the number of the TCP/IP port on which the SMTP server is listening.

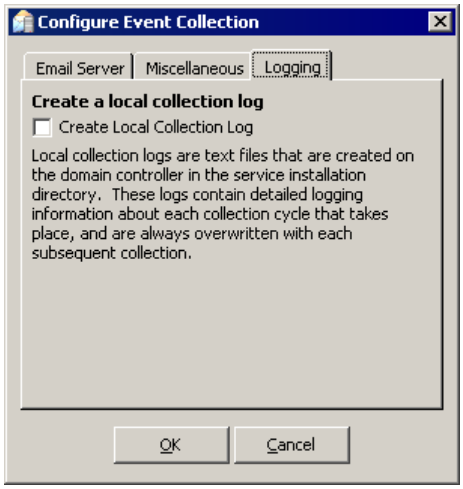
4. If your SMTP server requires authentication, type the username and password in the **SMTP User Name** and **SMTP Password** boxes.

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.



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.



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.

1. On the computer where the Event Notification service is running, click **Start**, point to **Programs > Administrative Tools**, and then choose **Services**. The Services applet opens.
2. Right-click the **Active Administrator Even Notification Service**, and then click **Properties**.
3. Open the **Log On** tab, and then specify the account to run the service.
4. Restart the service.

Alternatively, you can add the computer account to the AA_Admin group, which has access to the Active Administrator database. When the Active Administrator database is created, two groups are created: AA_Admin and AA_User. Depending on the options you selected during the creation of the database, these two groups may be local groups on the SQL server, Domain Local Groups, or Domain Groups.

- On the computer where the Event Notification service is running, open the AA_Admin group, and then add the computer account to the AA_Admin group. The service now run as Local System and can access the database.

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 ▸. To stop the service, click ■.

Modifying the Domain Controller Agents

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

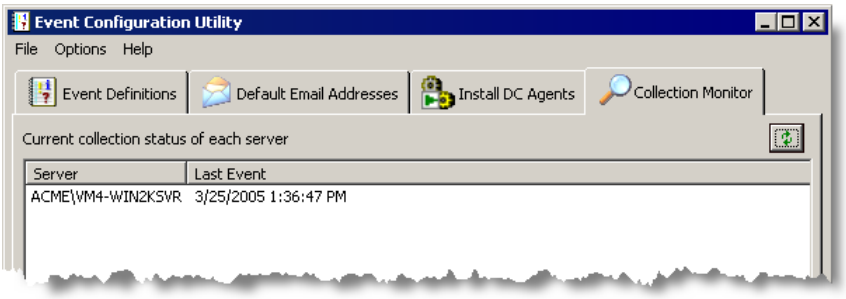
   Note: If no domain controllers are listed, click ⋯. In the **Domain** box, type the domain name or click **Browse** to locate a domain.

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.



- 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.

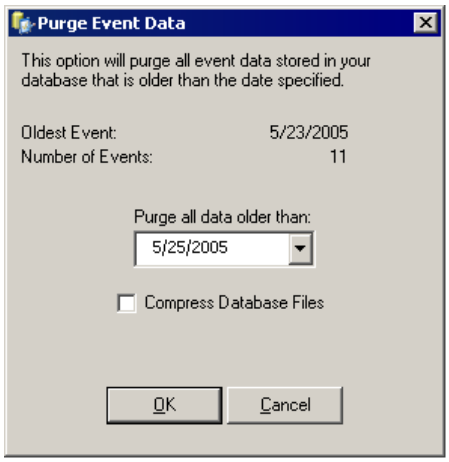
Important: When event definitions are imported, existing definitions with the same name are overwritten.

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

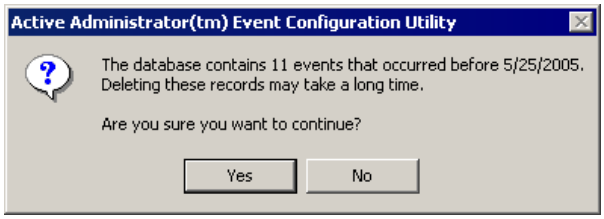
To manage disk space, you may want to purge the event data periodically or compress the event database.

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.



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**.

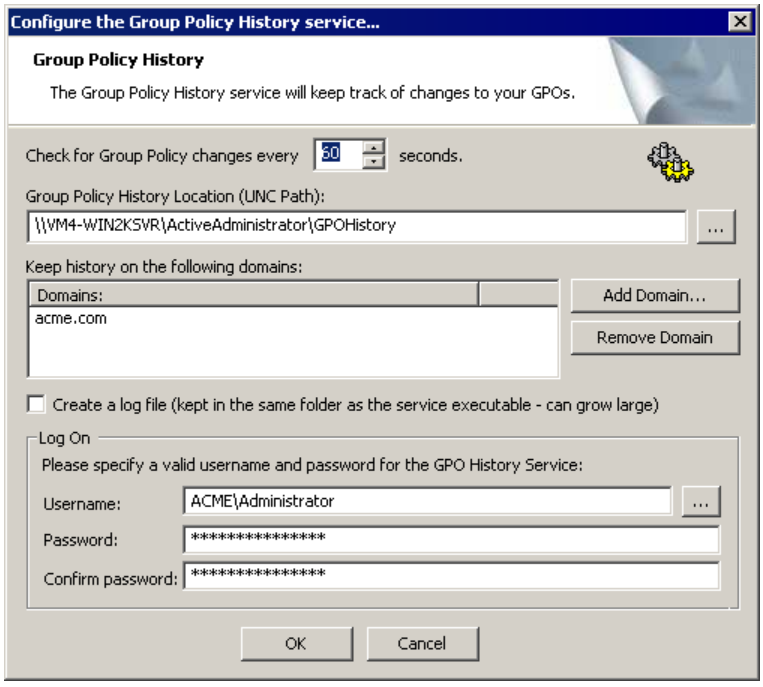
GPO History Configuration

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.



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.

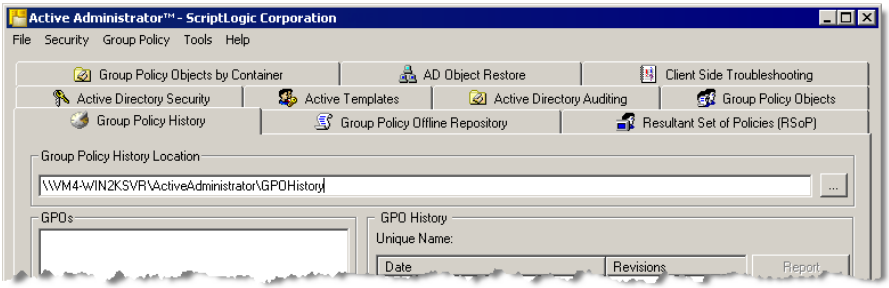
Note: Be sure the user you are logged in as has read access to the security event database and Group Policy History file share.

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.

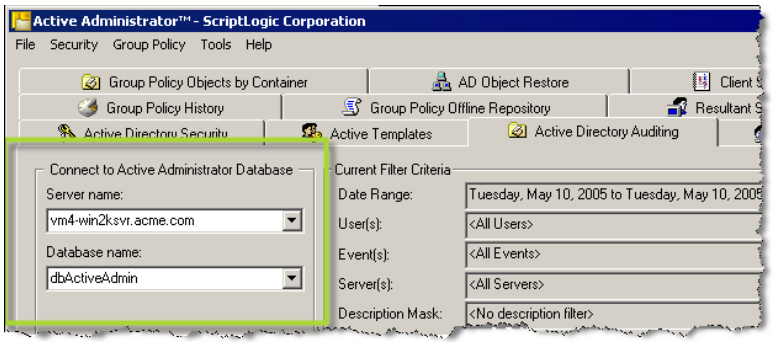
   Note: During the install process, a GPOHistory share is created.



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.

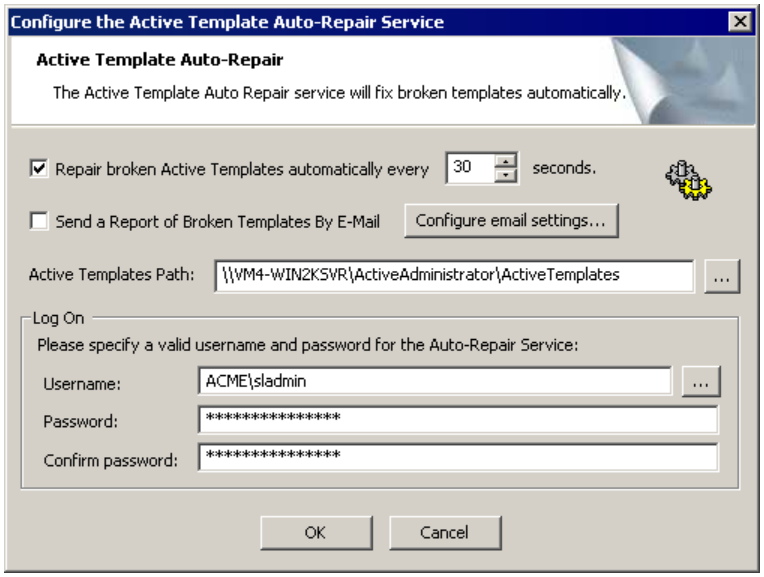


Active Template Repair Configuration

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.

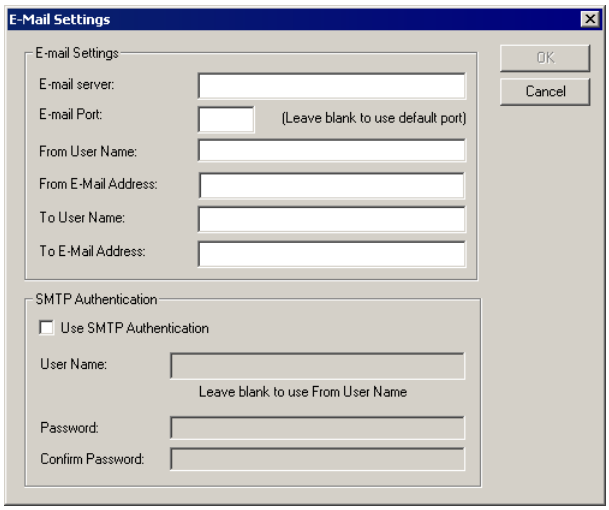
1. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator**, and then select **Active Template Repair Configuration**. The **Configure the Active Template Auto-Repair Service** box displays the choices made during the installation process.



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.



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**.

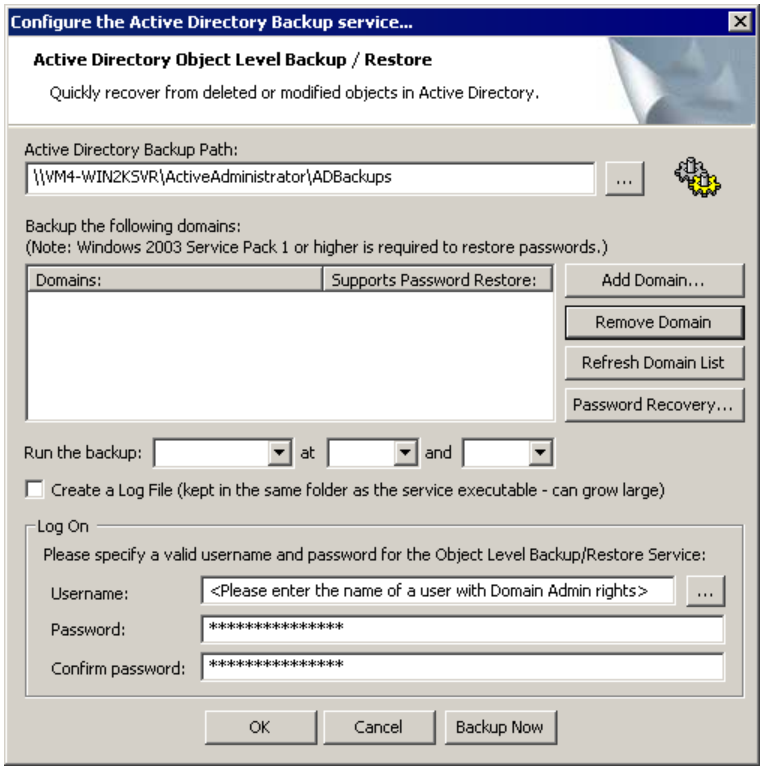
Object Level Backup Configuration

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

1. 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.

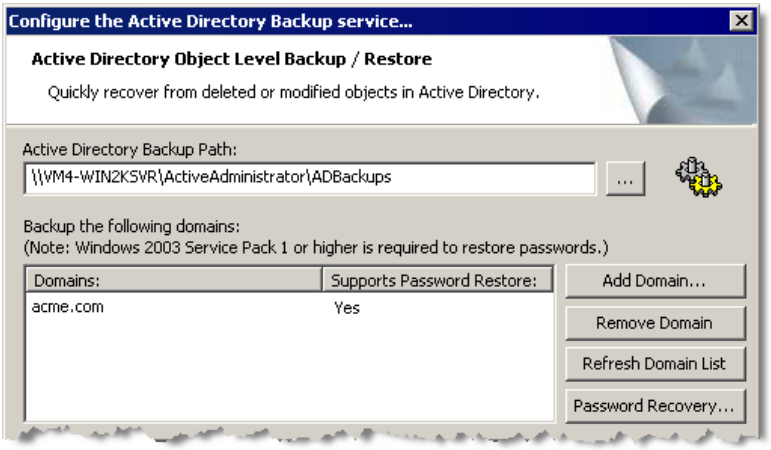
Note: To store Active Directory backups, the installation wizard creates the ADBackups share, whose path is displayed in the **Active Directory Backup Path** box. If you created another share in which to store Active Directory backups, click … to locate the share. See *Creating Network Shares to Store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



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.



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.

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`**

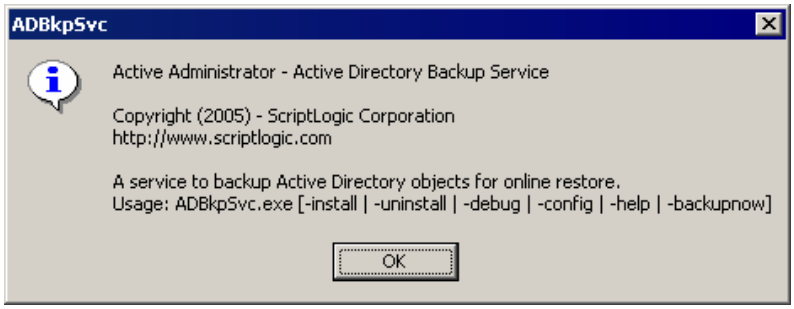
  Opens the **Configure the Active Directory Backup service** dialog box. See *Configuring the Backup Service*.

- **`ADBkpSvc.exe -backupnow`**

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

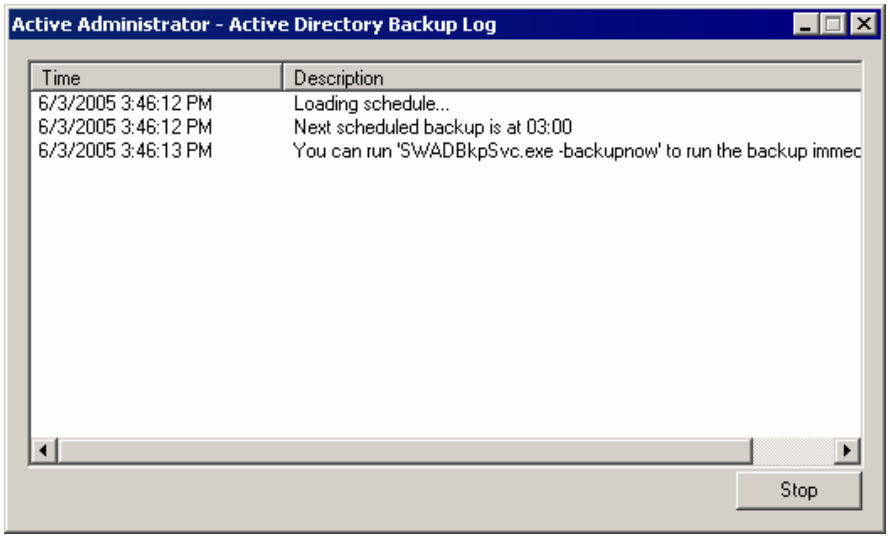
- **`ADBkpSvc.exe -help`**

  Displays the help window for the command.



- **`ADBkpSvc.exe -debug`**

  Opens the **Active Directory Backup Log** window.



Troubleshooting

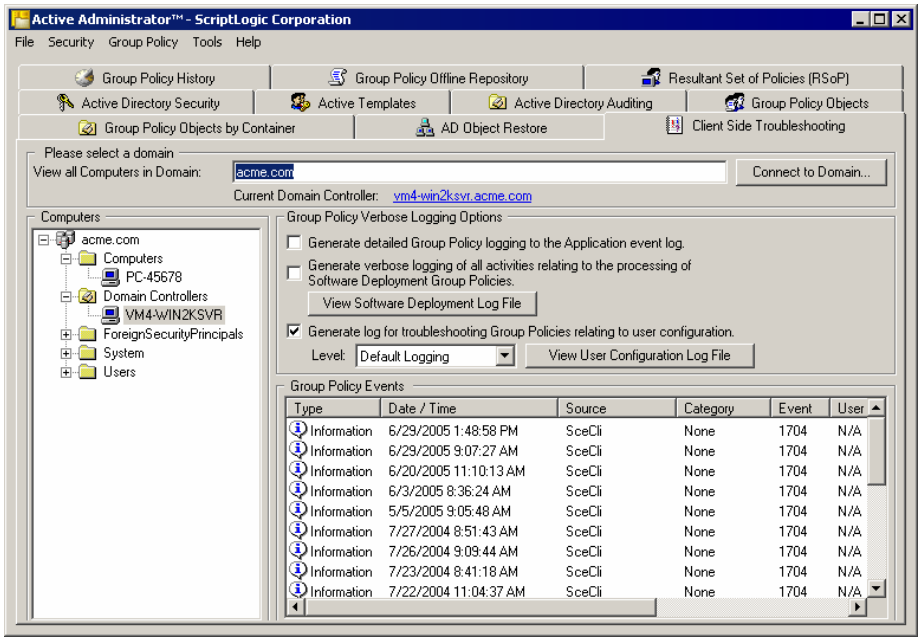
In its Knowledge Base, ScriptLogic Corporation has a library of articles that may provide an answer to a problem you are experiencing. Before calling technical support, check to see if your problem is documented here. You might also browse the Discussion Forums to see if anyone else is experiencing the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



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.

Setting Logging Options

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

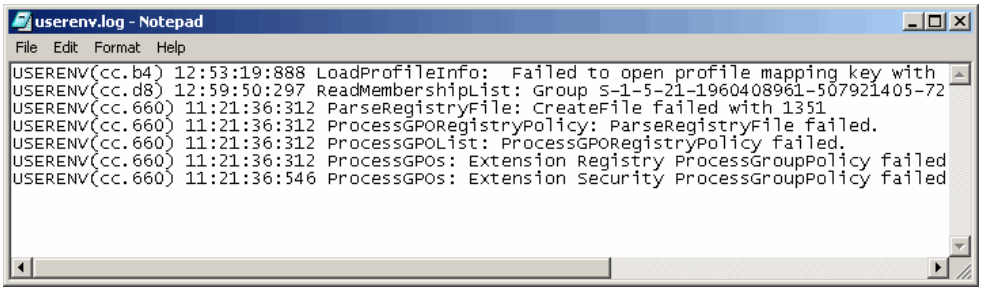
☑ **Generate verbose logging of all activities relating to the processing of Software Deployment Group Policies**
Enabling Group Policy Software Deployment logging slows down the logon process and generates an Appmgmt.log file that records the steps of the Group Policy Application Deployment component.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

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

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

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

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



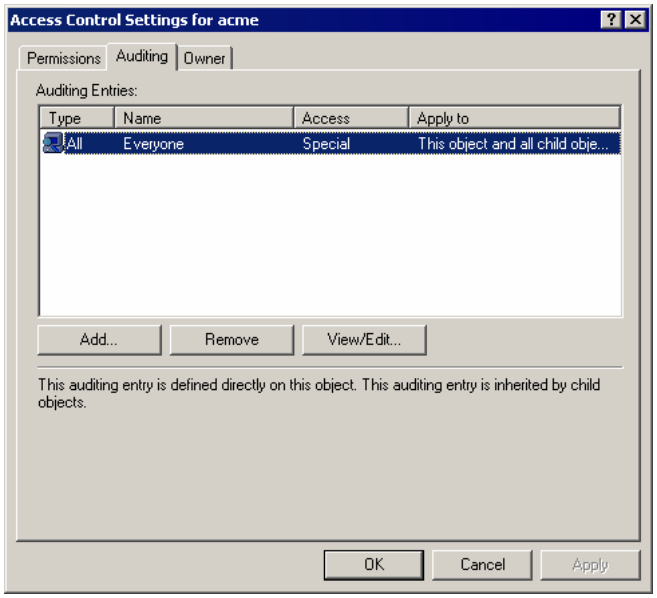
SETTING AUDITING PERMISSIONS

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

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

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

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



- 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.

5. 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

R

S

U