



ACTIVE ADMINISTRATOR[®]

VERSION 6

ScriptLogic[®]

Active Administrator[®]

VERSION 6

Installation Guide

Copyright © 2011 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 6.x. 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.

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

| | |
|---|-----------|
| GETTING READY TO INSTALL | 1 |
| MINIMUM SYSTEM REQUIREMENTS | 1 |
| DOWNLOADING INSTALLATION FILES | 2 |
| USER PRIVILEGE REQUIREMENTS..... | 2 |
| INSTALLING FOR THE FIRST TIME..... | 3 |
| UPGRADING TO VERSION 6.0..... | 4 |
| <i>What's New in Active Administrator 6.0?</i> | 4 |
| <i>Upgrading from version 5.x to version 6.0</i> | 4 |
| <i>Upgrading from version 4.x to version 6.0</i> | 4 |
| INSTALLING THE ACTIVE ADMINISTRATOR SERVER | 5 |
| RUNNING THE SERVER INSTALLATION WIZARD..... | 5 |
| APPLYING A LICENSE FILE | 9 |
| EVALUATING THE PRODUCT..... | 10 |
| CONFIGURING THE SERVER | 11 |
| RUNNING THE SERVER CONFIGURATION WIZARD..... | 11 |
| CONFIGURING THE ACTIVE ADMINISTRATOR DATABASE..... | 12 |
| STORING ACTIVE ADMINISTRATOR DATA..... | 15 |
| SETTING UP THE EMAIL SERVER | 16 |
| SETTING UP SERVICES AND THE OWNER..... | 17 |
| CONFIGURING THE ACTIVE TEMPLATE AUTO-REPAIR SERVICE..... | 18 |
| CONFIGURING THE GROUP POLICY HISTORY SERVICE..... | 19 |
| CONFIGURING ACTIVE DIRECTORY OBJECT LEVEL BACKUP/RESTORE..... | 20 |
| CONFIGURING ACTIVE ADMINISTRATOR TRUSTEES..... | 24 |
| CONFIGURING SERVICE ACCOUNTS | 25 |
| COMPLETING SERVER CONFIGURATION | 26 |
| STARTING ACTIVE ADMINISTRATOR SERVER COMPONENTS..... | 28 |
| SETTING UP AUDITING ON DOMAIN CONTROLLERS | 29 |
| COMPLETING THE UPGRADE PROCESS..... | 30 |
| UPDATING AUDIT AGENTS | 30 |
| REMOVING ORPHANED AGENTS..... | 31 |
| INSTALLING AUDIT AGENTS..... | 32 |
| IMPORTING DATA FROM EXISTING AUDIT DATABASES | 34 |
| CREATING AN ALERT | 34 |
| USING ACTIVE ADMINISTRATOR SERVER | 36 |
| ACTIVE ADMINISTRATOR CONSOLE INSTALLATION | 37 |
| RUNNING THE ACTIVE ADMINISTRATOR CONSOLE INSTALLATION WIZARD..... | 37 |
| SETTING THE ACTIVE ADMINISTRATOR SERVER | 40 |
| STARTING ACTIVE ADMINISTRATOR CONSOLE | 40 |
| USING ACTIVE ADMINISTRATOR CONSOLE | 40 |
| USING ONLINE HELP | 40 |

Getting Ready to Install

MINIMUM SYSTEM REQUIREMENTS

| | |
|--------------------------|--|
| Processor | 1 GHz or higher Pentium-compatible CPU |
| Memory (RAM) | 1 Gigabytes or more recommended |
| Hard Disk Space | 100 Megabytes or more of free disk space, not including the amount required by the Active Administrator database |
| Screen Resolution | 1024x768 |
| Operating System | <p>Both 32-bit or 64-bit architectures are supported. All versions should have the latest service pack installed.</p> <p>Server (ASM.exe) All editions of:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2003 ■ Microsoft Windows Server 2003 R2 ■ Microsoft Windows Server 2008 ■ Microsoft Windows Server 2008 R2 <p>Note: Audit Agents (standard and advanced) are supported on Windows 2000 domain controllers.</p> <p>Console (AAConsole.exe)</p> <ul style="list-style-type: none"> ■ Windows XP Professional ■ Windows Vista Business, Enterprise, or Ultimate ■ Windows 7 Business, Enterprise, or Ultimate <p>Important: When using Windows Vista or Windows 7 64-bit operating systems, you may experience problems when performing some operations on Active Directory objects. When the Microsoft RSAT tools are installed, the adprop.dll.mui and dsadmin.dll.mui files are not installed and are needed by Active Administrator. See the ScriptLogic Knowledge Base and Solution Center for instructions on how to locate and copy these files to the correct location.</p> |
| SQL Server | <p>Both 32-bit or 64-bit architectures are supported. All versions should have the latest service pack installed.</p> <ul style="list-style-type: none"> ■ Microsoft SQL 2000 Server (Enterprise, Standard, Workgroup, and Desktop Engine editions) ■ Microsoft SQL Server 2005 (Enterprise, Standard, Workgroup, and Express editions) ■ Microsoft SQL Server 2008 (Enterprise, Standard, Workgroup, and Express editions) ■ Microsoft SQL Server 2008 R2 (Datacenter, Enterprise, Standard, Workgroup, and Express editions) <p>Note: For SQL collation and sort order, Active Administrator requires either SQL_Latin1_General_CI_AS or SQL_Latin1_General_CS_AS.</p> <p>Important: You must enable Named Pipes communication, which is off by default.</p> |
| Additional | <ul style="list-style-type: none"> ■ Microsoft .NET Framework version 3.5 with Service Pack 1 ■ Microsoft Group Policy Management Console |

DOWNLOADING INSTALLATION FILES

If you have not yet done so, download the latest version of Active Administrator:

<http://www.scriptlogic.com/support/Products/ActiveAdministrator/>

The Active Administrator program has components:

- server (Active Administrator 6.0.x Server.exe)
- console (Active Administrator 6.0.x Console exe)

Install the Console component on any computer that requires it. The Server component needs to be installed on only one computer. Both the Console and Server components can be installed on the same server.

USER PRIVILEGE REQUIREMENTS

- To install Active Administrator, a user must hold administrative rights on the local system and the SQL instance that will host the Active Administrator database.
- To use Active Administrator, a user must hold administrative rights on both the local system and the domain, and be a member of the AA_Admin database access group, which is created during the installation process.

Password Recovery

If you are using Windows Server 2003 SP1 or higher, Active Administrator can restore passwords when you restore accounts that were deleted. To enable password recovery, a minor modification is made to the Schema. To be able to modify the Schema, you must use an account that is a member of the Schema Admins group.

Services

The Domain Administrator account provides the necessary permissions for the various Active Administrator services to operate properly. You can choose to use one account with Domain Admin rights for all services, or you can choose to identify an account for each service.

-  Active Administrator Active Template Repair Service
-  Active Administrator AD Object Backup Service
-  Active Administrator Agent
-  Active Administrator GPO History
-  Active Administrator Maintenance Service
-  Active Administrator Notification Service

When choosing an account, keep these requirements in mind:

- **Active Administrator Active Template Repair Service** needs the ability to access all objects in Active Directory, and to change Active Directory permissions on any Active Directory object.

- **Active Administrator AD Object Backup Service** needs to access all objects in Active Directory, and to back up all objects and restore them, as well as to write/modify their attributes.
- **Active Administrator Advanced Auditing** runs as the Local System account, regardless of the user account configured for the Active Administrator Agent service.
- **Active Administrator Agent** can also run under a domain user account provided it is either a local admin account, which gives it the rights to logon as a service and log on locally, or these two privileges can be granted individually. This user or service account should also be a member of the AA_Admin group, which by default is located in the Local groups of the server where the ActiveAdministrator database is located. If the group is not found in this location, the settings during the initial database creation were modified and it can be found under the Users container object of Active Directory.
- **Active Administrator GPO History** can run under a domain user account that is a local administrator on the Active Administrator server (where the Active Administrator share and services are located).
- **Active Administrator Maintenance Service** needs to access the Service Control Manager (SCM) on all computers running the Audit Agent and the SCM running on the Active Administrator server, and to access the Audit database. The user for the Maintenance service must be a member of the local Administrator group on any computer running the Audit Agents and for the Active Administrative server. The user must be an Administrator on the local computer to open and control the SCM.
- **Active Administrator Notification** service needs to have access to the database.

Audit Database

On the database server, the database installation creates two local groups that control access to the audit 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

INSTALLING FOR THE FIRST TIME

| Steps | Reference |
|--|---|
| 1. Install Active Administrator Server. | <i>Running the Server Installation Wizard</i> |
| 2. Run the Server Configuration Wizard. | <i>Running the Server Configuration Wizard</i> |
| 3. Install Active Administrator Console. | <i>Running the Active Administrator Console Installation Wizard</i> |

UPGRADING TO VERSION 6.0

What's New in Active Administrator 6.0?

To see what is new in Active Administrator, please see *Active Administrator 6.x Version History* in the ScriptLogic Knowledge Base, which you can access at: <http://www.scriptlogic.com/support/products/activeadministrator/>

Upgrading from version 5.x to version 6.0

If you are upgrading from a previous installation of version 5, you only need to update the audit agents once installation is complete.

| Steps | Reference |
|--|---|
| 1. Install Active Administrator Server. | <i>Running the Server Installation Wizard</i> |
| 2. Run the Server Configuration Wizard. | <i>Running the Server Configuration Wizard</i> |
| 3. Update Audit Agents. | <i>Updating Audit Agents</i> |
| 4. Install Active Administrator Console. | <i>Running the Active Administrator Console Installation Wizard</i> |

Upgrading from version 4.x to version 6.0

Besides installing the software, you will need to do a few other procedures if you are upgrading from a previous version of Active Administrator. The software installation will take care of uninstalling old processes and then installing new.

| Steps | Reference |
|---|---|
| 1. Uninstall any version 4 agents using the Event Configuration Utility in Active Administrator 4. | |
| 2. Install Active Administrator Server. | <i>Running the Server Installation Wizard</i> |
| 3. Run the Server Configuration Wizard | <i>Running the Server Configuration Wizard</i> |
| 4. Remove orphaned Audit Agents. | <i>Removing Orphaned Agents</i> |
| 5. Install new Audit Agents. | <i>Installing Audit Agents</i> |
| 6. Import data from your version 4 databases. | <i>Importing Data From Existing Audit Databases</i> |
| 7. Create new alert notifications. | <i>Creating an Alert</i> |
| 8. Install Active Administrator Console. | <i>Running the Active Administrator Console Installation Wizard</i> |

Installing the Active Administrator Server

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

Important: If you are upgrading from version 4.x, you must uninstall any version 4 agents using the **Event Configuration Utility** in Active Administrator 4 prior to running the Server Installation Wizard.

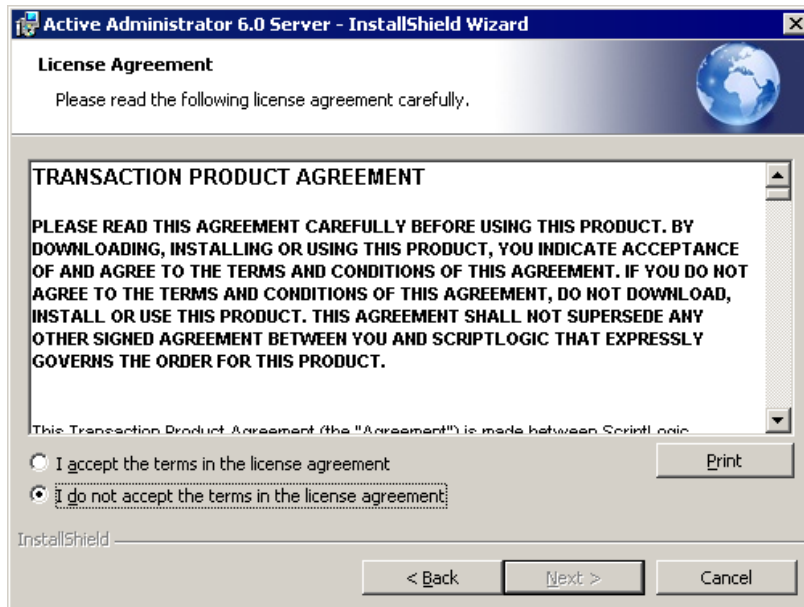
RUNNING THE SERVER INSTALLATION WIZARD

Note: You may be prompted to restart your computer at the end of the install process.


1. Double-click the **Active Administrator 6.0.x Server.exe** file, or right-click the file, and then select **Install**. The **Welcome** page appears.

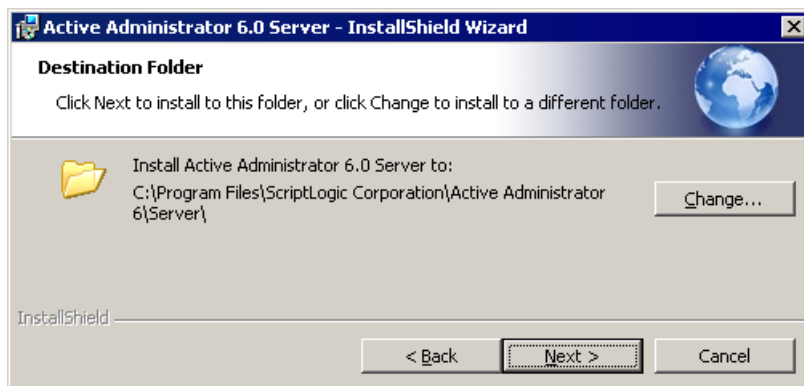



- Click . The **License Agreement** page displays the Transaction Product Agreement.




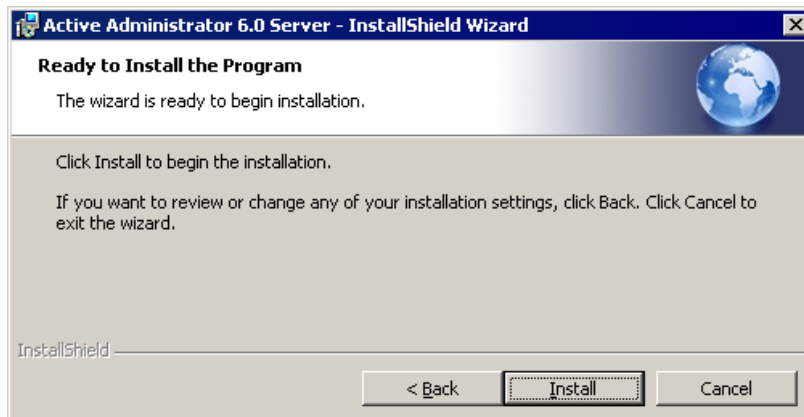
Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or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

- Select **I accept the terms in the license agreement**, and then click . The **Destination Folder** page appears.



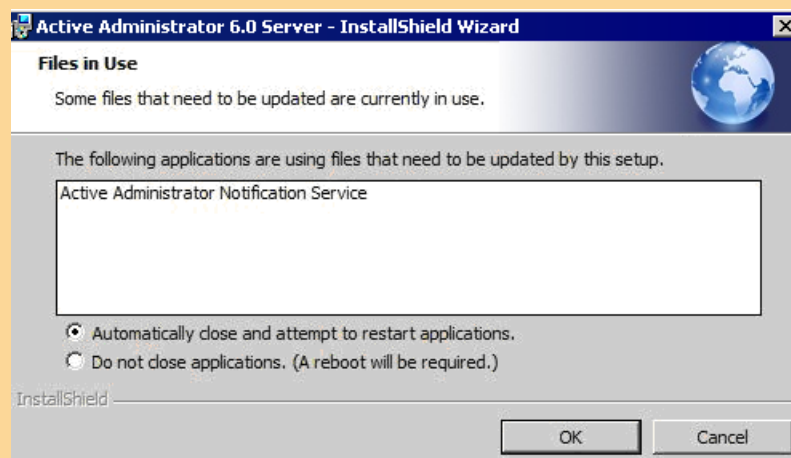
- To change the location of the program files, click . The **Change Current Destination Folder** page opens. Choose a new location for the installation directory.

4. Click . The **Ready to Install the Program** page appears.

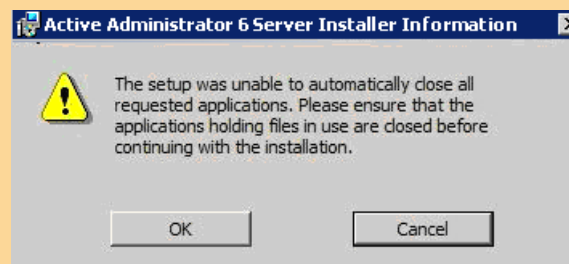


5. To begin the installation, click . The **Installing Active Administrator Server Setup** box displays a status bar that indicates the installation progress.

Upgrade Note: If you receive a message that some files are currently in use, click **OK** to close the applications automatically.



If you receive a message that setup was unable to close the applications, close the applications manually, and then click **OK**.



When installation is complete, you have the option of starting the Server Configuration Wizard upon finishing the wizard.



Launch Configuration Wizard (recommended)

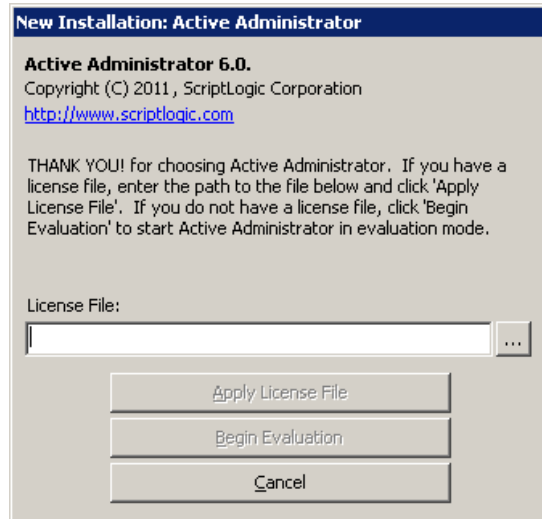
By default, the option to start the Server Configuration Wizard is selected. It is recommended that you go through the configuration wizard to set up your database and Active Administrator services.

6. Click . The following Active Administrator components are installed:




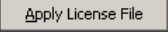
APPLYING A LICENSE FILE

The first time you start the **Active Administrator Server Management** component, 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.

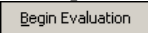
The license file is approximately 1KB in size and has a .lic file extension. The Sales account executive or Support Team specialist that you have been dealing with should have emailed this file to you as an attachment.


- ▶ Click  to locate the license file, and then click .

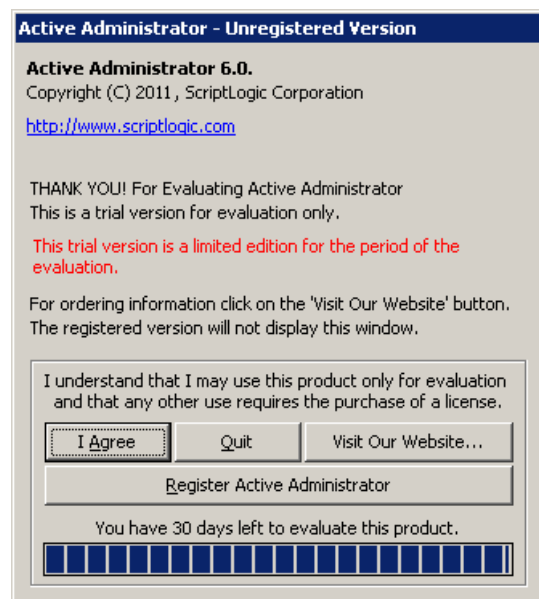
EVALUATING THE PRODUCT

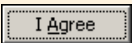
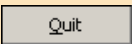
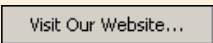
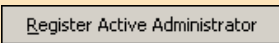
Note: The full and evaluation versions of Active Administrator are identical. The license file is the sole determinant of program functionality. Limitations during the free 30-day evaluation period include:

- Auditing of domain controllers is unlimited.
- Perform Active Directory and GPO backups on two domains only.
- Reports generated have an Evaluation watermark.

- If you are evaluating the software and would like to use the preset values for the number of licenses, objects, and evaluation days, click . The **Unregistered Version** box appears.

Once you accept the evaluation, this box will appear each time you open Active Administrator for the duration of the evaluation period. If you receive a license file, click  to access the **New Installation** box.



| Button | Description |
|---|---|
|  | Accept the conditions of the evaluation |
|  | Exit |
|  | Go to the ScriptLogic web site |
|  | Apply a license file |

Configuring the Server

Note: After this initial configuration, you can modify the server configuration from the Active Administrator Server Management module. See the *Active Administrator Server Management Guide*.

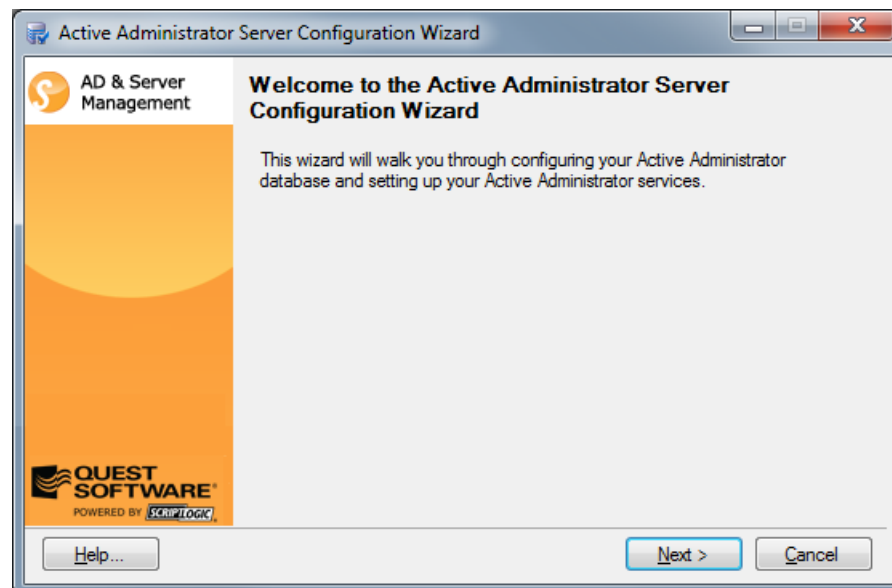
RUNNING THE SERVER CONFIGURATION WIZARD

The **Server Configuration Wizard** guides you through configuring the various services that are required to run Active Administrator.

- Active Administrator Active Template Repair Service.
- Active Administrator AD Object Backup Service.
- Active Administrator GPO History.
- Active Administrator Maintenance Service
- Active Administrator Notification Service

Note: If you are upgrading Active Administrator, your previous settings appear in the **Server Configuration Wizard**. You can quickly page through the wizard accepting the current settings or take the opportunity to make changes to your setup.

Note: If the **Server Configuration Wizard** did not start automatically, click **Start**, point to **ScriptLogic Corporation > Active Administrator 6**, and then choose **AA Server Configuration Wizard**.



- To advance to the next page, click .

CONFIGURING THE ACTIVE ADMINISTRATOR DATABASE

Important: An instance of Microsoft SQL Server 2000 or higher must be installed and running on a server that can be accessed by the Active Administrator server, Active Administrator Console, and all installed Audit Agents. If you need to install Microsoft SQL Server, you can click either [Download Microsoft SQL Express 2008](#) or [Download Microsoft SQL Express 2005](#) to download a free copy of Microsoft SQL Server.

Server Name

If the Active Administrator database you want to use is located on a server other than the one displayed in the **Server Name** box, select the server from the list, and then click

Refresh.

Log on to server

Choose whether the server displayed in the **Server Name** box uses **Windows** or **SQL Server Authentication**. If you choose **SQL Server Authentication**, enter the **User Name** and **Password**.

Connect to database

Choose the database from the **Database Name** list.

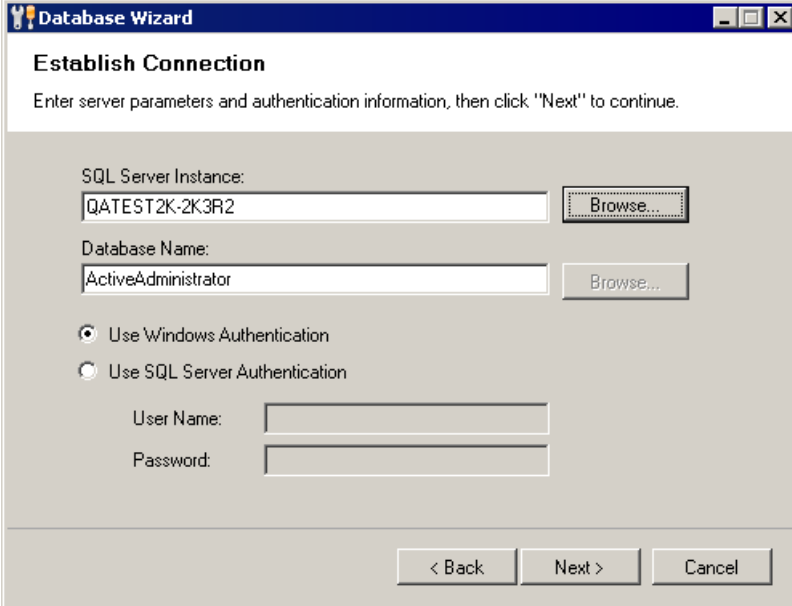
Note: Only databases associated with the server displayed in the **Server Name** box are listed. You may need to create a new database or change to a different server if the database you want is not listed

Create New Database

Click to open the Database Wizard to create a new database on the server displayed in the **Server Name** box. After the Database Wizard is finished, and closed, the database name displays in the **Database Name** box.

Note: The Audit Agent service uses Microsoft SQL Server as its backend database for storing event information. The database should be installed in a central location that can be reached by all domain controllers.

1. From the **Database Wizard Main Menu**, select **Create New Database**.
2. Click **Next >**. The **Establish Connection** box displays the default database name: **ActiveAdministrator**.



SQL Server Instance

If necessary, type the name of the server that is running Microsoft SQL Server, or click **Browse...** to locate registered servers that may also be running the database engine.

Database Name

To change the name of the database from the default, type a name in the box.

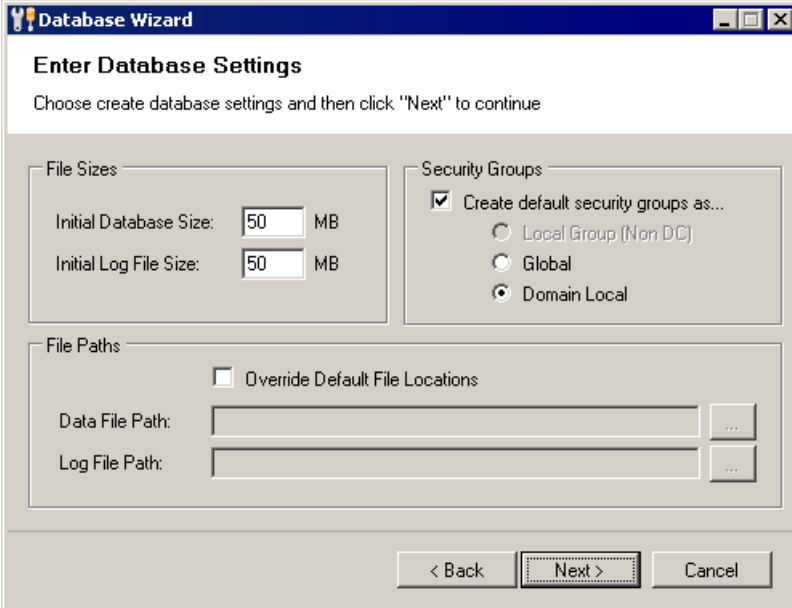
Use Windows Authentication

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

Use SQL Server Authentication

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.

- Click . The **Enter Database Settings** box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.



Initial Database Size

Type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.

Initial TX Log Size

Type an initial size for the transaction log file (*.ldf). If the database needs to grow the log file, it does so automatically.

Security Groups

Select how to create default security groups: **Local Group (Non DC)**, **Global**, or **Domain Local**. If you do not want to create default security groups, clear the **Create default security groups** as check box.

Note: These default Security Groups are required for Windows Authentication.

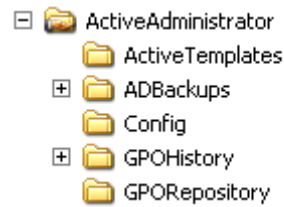
Override Default File Locations

Select to create the database transaction log files in a location other than the default location. Type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.

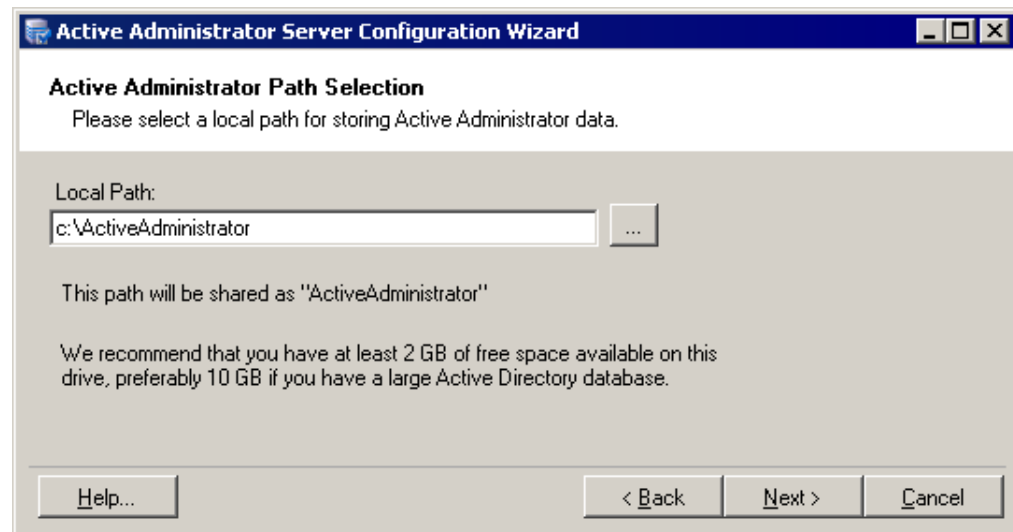
- Click . The **Create New Database** displays the database name.
- To create the specified database, click . A task progress box displays the progress of creating the database. When the database creation is complete, a message box appears.
- Click **OK** to return to the **Active Administrator Database Configuration** page.
- Click to check if the server can connect to the selected database and to verify that the selected database is an Active Administrator database.
- To advance to the next page, click .

STORING ACTIVE ADMINISTRATOR DATA

The **Active Administrator Path Selection** page displays the default path to the folder where the Active Administrator data is stored.



Note: The install process creates the ActiveAdministrator share, which contains five subfolders in which Active Administrator data is stored. You can create your own share as long as it resides on a 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.

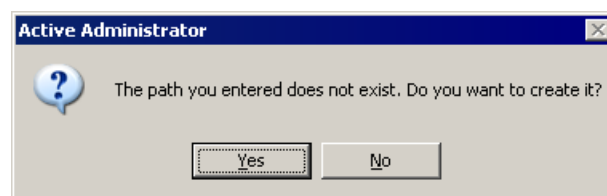


Local Path

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.

- When you click , if the folder you entered does not exist, you receive a confirmation message.



To create the folder, click . A security warning displays.



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

- To advance to the next page, click .

SETTING UP THE EMAIL SERVER

The Notification Service sends automatic emails to specified recipients. On this page, identify the email server to use for the Notification Service.

SMTP Host Name

Type the name of the SMTP server that sends the alert emails.

SMTP Port

Type the number of the TCP/IP port on which the SMTP server is listening.

If your SMTP server requires authentication

Type the username and password in the **SMTP User Name** and **SMTP Password** boxes.

“From” Email Address

Type the email address to appear in the **From** box of the alert email. By entering something meaningful, you can use the **From** box to filter your email.

Message format

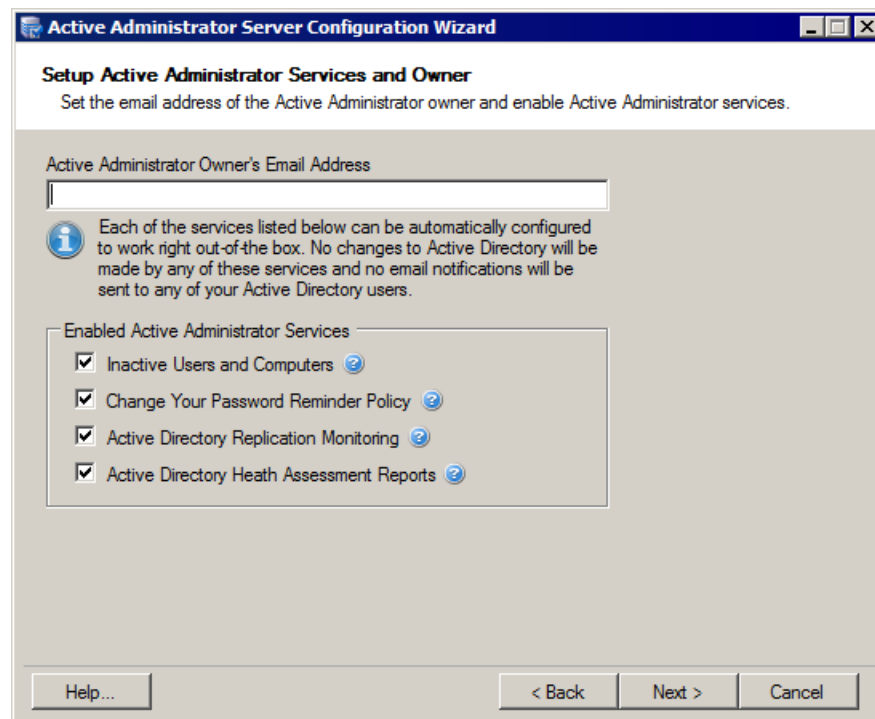
Choose a format for the email.

Click to test the settings.

- To advance to the next page, click .

SETTING UP SERVICES AND THE OWNER

On many tasks, an email is sent to the Administrator’s email address. Type a valid email address in the box.



By default, four Active Administrator Services are enabled. To see an explanation of each service, hover the cursor over .

Note: The first time you run the Server Configuration Wizard, the check boxes are enabled. No changes are made to Active Directory. The next time you run Server Configuration Wizard, the check boxes are disabled, so you need to use Active Administrator Server Management to enable/disable the services.

Inactive Users and Computers



To modify the service, finish the wizard, start Active Administrator Server Management, and then click [Inactive Users and Computers](#) on the **Start Page**. Alternatively, open the **Tools** menu, point to **Inactive Users and Computers**, and then choose **Settings**.



Change Your Password Reminder Policy

To modify the service, finish the wizard, start Active Administrator Server Management, and then click [Change Your Password Reminder Policy](#) on the **Start Page**. Alternatively, open the **Tools** menu, point to **Change Your Password Reminder Policy**, and then choose **Settings**.



Active Directory Replication Monitoring

To modify the service, finish the wizard, start Active Administrator Server Management, and then click [Active Directory Replication Monitoring](#) on the **Start Page**. Alternatively, open the **Tools** menu, and then choose **Active Directory Replication Monitoring**.



Active Directory Health Assessment Reports

To modify the service, finish the wizard, start Active Administrator Server Management, and then click [Active Directory Assessment Reports](#) on the **Start Page**. Alternatively, open the **Tools** menu, and then choose **Schedule Assessment Reports**.

- To advance to the next page, click .

CONFIGURING THE ACTIVE TEMPLATE AUTO-REPAIR SERVICE

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, you can alert administrators automatically via email when an Active Template is repaired.

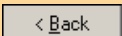
Automatically repair broken Active Templates

By default, Active Administrator checks for broken templates every 30 seconds.

- To disable Active Template Auto-Repair, clear the check box.
- To change the polling interval, choose a value from the list.

Send a Report of Broken Templates by E-mail

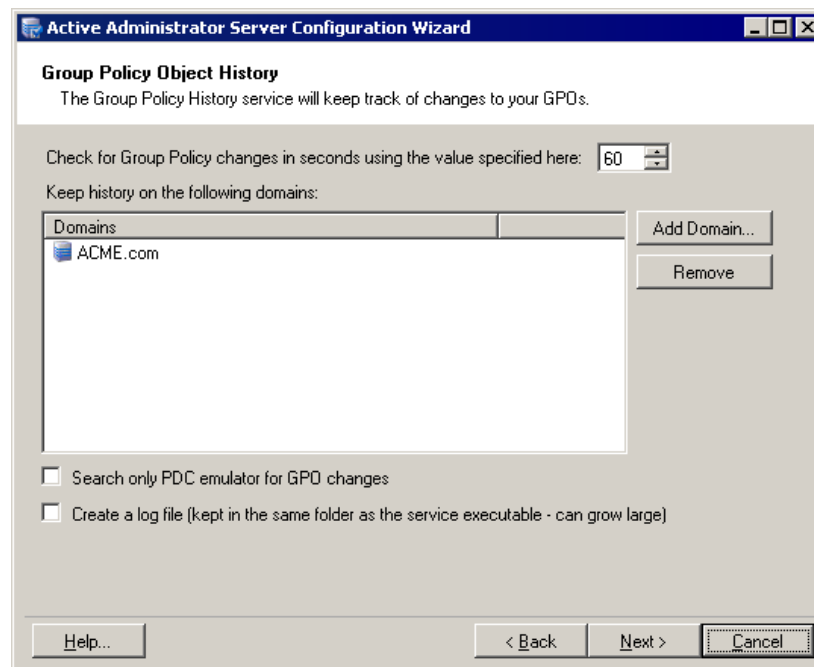
Select to send reports of broken templates to selected users via email. In the **To email address** box, type the email address of the recipient.

Note: You must have configured the Email Server to continue. If necessary, click  to return to the **Email Server Settings** page. See *Setting Up the Email Server*.

- To advance to the next page, click .

CONFIGURING THE GROUP POLICY HISTORY SERVICE

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.




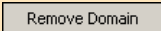
Check for Group Policy changes

From the **Check for Group Policy changes** 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.

Keep History on the following domains

The GPO History Service checks for GPO Policy changes on the listed domains.

| Button | Description |
|---|--|
|  | Add a domain to the list. |
|  | Remove selected domain(s) from the list. |

Search only PDC emulator for GPO changes

Select to monitor only the domain controller acting as the primary domain controller.

Time Saver: Selecting the **Search Only PDC emulator for GPO changes** check box can reduce network traffic.

Create a log file (kept in the same folder as the service executable – can grow large

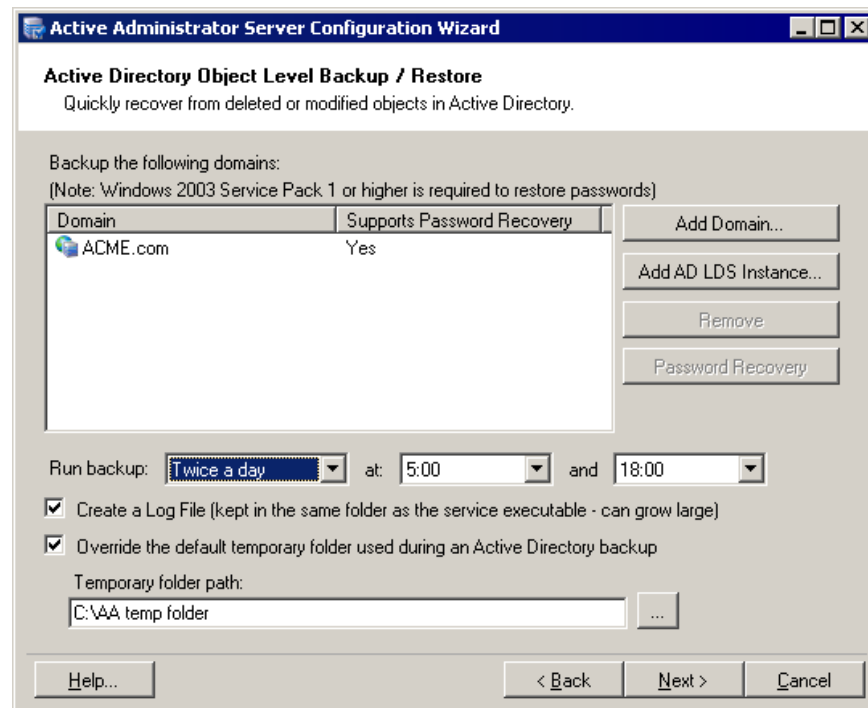
Select to create a debug log file to see exactly what the GPO History service is doing.

Note: The log file is located in the **Program Files/ScriptLogic Corporation/Active Administrator 6/Server** folder. The name of the log file is based on the date and time of the GPO event, such as **5_2_2008_11_18_57_AM.Log**.

- To advance to the next page, click .

CONFIGURING ACTIVE DIRECTORY OBJECT LEVEL BACKUP/RESTORE

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




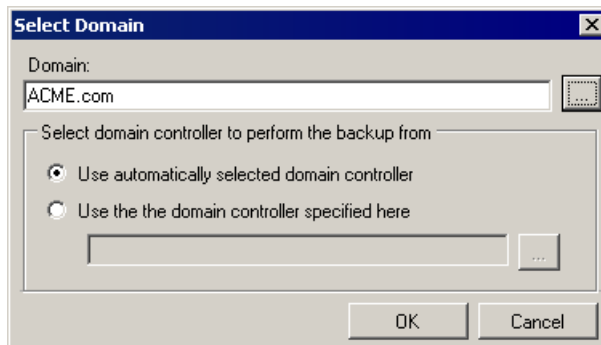
Backup the following domains


The Active Administrator AD Object Backup Service backs up the listed domains based on the settings in the **Run backup** boxes.

Add Domain...

Click to add a domain. The **Select Domain** box opens.

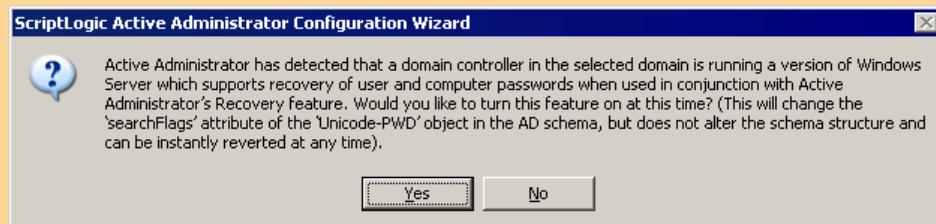
1. In the **Domain** box, type a domain name, or click  to locate a domain.




You can specify the domain controller to perform the backup. By default, Active Administrator uses a domain controller selected by Active Directory. If you wish to use a different domain controller, select **Use the domain controller specified here**, and then click  to locate a domain controller.

2. Click . The domain name is added to the list.

Note: If you are using Windows Server 2003 Service Pack 1 (SP1) or higher, a message box displays.

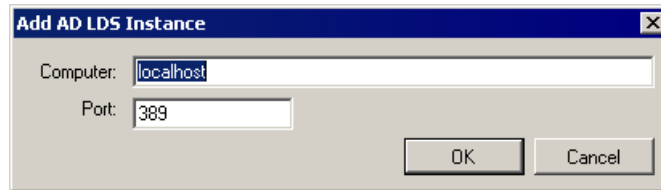


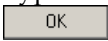
Active Administrator can restore passwords when you restore accounts that were deleted. Click  to enable Password Recovery. **Yes** displays in the **Supports Password Recovery** column.

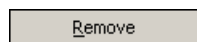
Add AD LDS Instance...

Note: For more information on AD LDS, see the Windows Server TechCenter article at [http://technet.microsoft.com/en-us/library/cc755080\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc755080(WS.10).aspx)

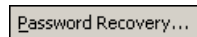
Active Administrator can back up and restore AD LDS instances the same way it can back up and restore Active Directory domains. Since AD LDS can run on any computer running Windows XP or higher, and does not require a domain, AD LDS instances are identified by server and port number.




The default computer is **localhost** and the default port is **389**. Type the computer name and port of the AD LDS instance, if necessary, and then click .

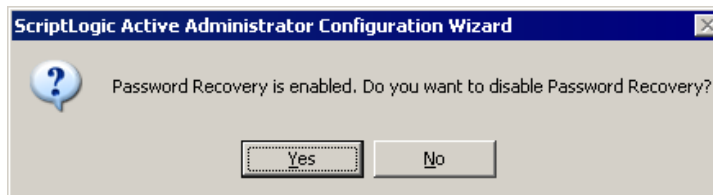


Click to remove a selected domain or AD LDS instance from the list.




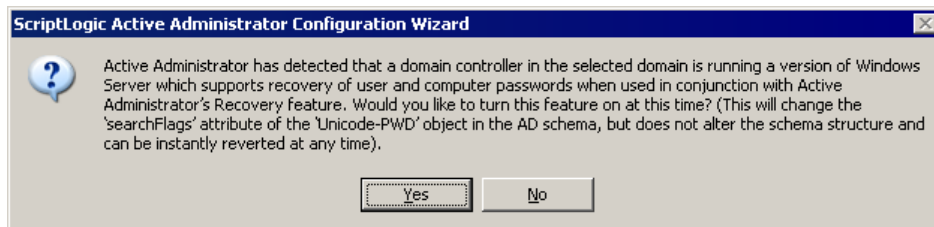
If you are using Windows Server 2003 Service Pack 1 (SP1) or higher, Active Administrator can restore passwords when you restore accounts that were deleted.

- ▶ To disable Password Recovery, select the domain, and then click . A message box displays.



Click  to disable Password Recovery. **No** displays in the **Supports Password Recovery** column.

- ▶ To enable Password Recovery, select the domain, and then click . A message box displays.



Click  to enable Password Recovery. **Yes** displays in the **Supports Password Recovery** column.

Run backup

By default, backups occur twice a day at 6:00 A.M. and 6:00 P.M. To change the frequency, select to run the backup **Every Day** or **Twice a Day** in the **Run backup** box. To change the time, select a time or times from the **at** list.


 Create a log file (kept in the same folder as the service executable – can grow large)

Select to create a log file for the backups.

Note: The log file is located in the **Program Files/ScriptLogic Corporation/Active Administrator 6/Server** folder. The name of the log file is based on the date and time of the backup, such as **5_2_2008_11_18_57_AM.Log**.

 Override the default temporary folder used during an Active Directory backup

By default, an Active Directory backup creates temporary files in the Active Administrator share, under the folder **C:\ActiveAdministrator\ADBackups\DOMAIN_***domainname* (where *domainname* is the fully qualified name of the domain being backed up).

To change the temporary folder, click  and then select a folder.

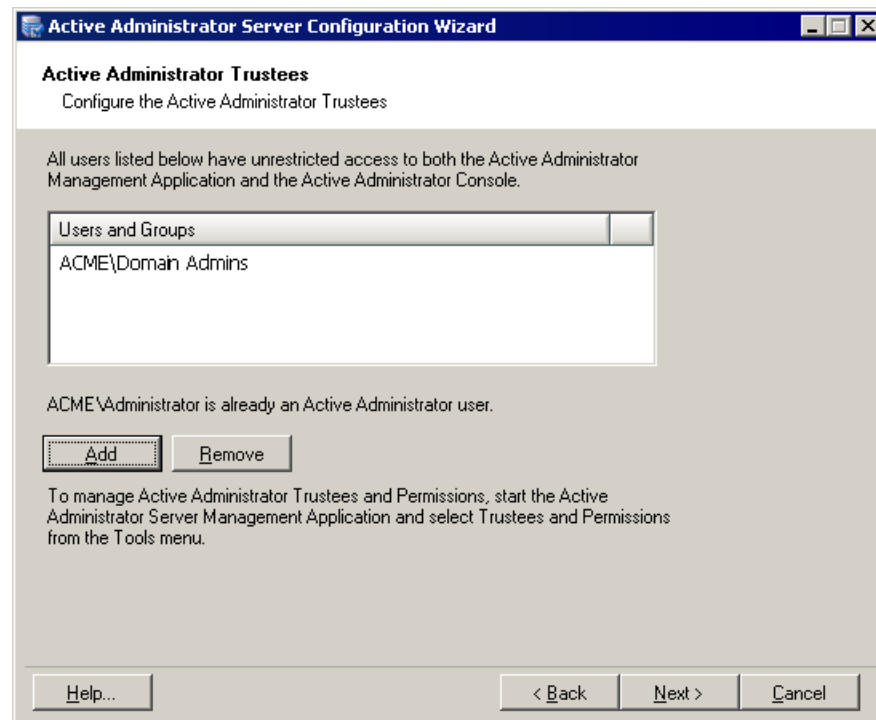
If you want to use the default temporary folder, which is located in the **Program Files\ScriptLogic Corporation\Active Administrator 6\Server** folder, clear the check box.

- To advance to the next page, click .

CONFIGURING ACTIVE ADMINISTRATOR TRUSTEES

Active Administrator Trustees have unrestricted access to Active Administrator Server Management and the Active Administrator Console. By default, the user installing and running the Server Configuration Wizard is automatically considered an Active Administrator Trustee.

Note: Upon initial installation, the Domain Admins group is added automatically to the trustees list.



Add

Click to add groups and users to the list of Active Administrator Trustees.

Remove

Click to remove selected groups and users from the list.

Note: If you remove the Domain Admins group from the list and do not add any groups or users to the list, the Domain Admins group is added automatically the next time you start the Configuration Wizard.

- To advance to the next page, click .

CONFIGURING SERVICE ACCOUNTS


The Domain Administrator account provides the necessary permissions for the various Active Administrator services to operate properly. You can choose to use one account with Domain Admin rights for all services, or you can choose to identify an account for each service.

Note: For more information on the types of accounts you can use, see *User Privilege Requirements*.

The screenshot shows the 'Active Administrator Server Configuration Wizard' dialog box, specifically the 'Service Accounts' step. The title bar reads 'Active Administrator Server Configuration Wizard'. Below the title bar, the text says 'Service Accounts' and 'Configure the Active Administrator Service Accounts'. There are two main options: 'Use the following service account for all services' and 'Customize each service account'. The first option is selected, and the 'Username' field contains 'ACME\Administrator' with a browse button (three dots in a square) to its right. Below the username field, a note states 'Username must be in the format of 'Domain\Username''. The 'Password' field is empty. The 'Customize each service account' checkbox is unchecked. Below this, there is a table with three columns: 'Service', 'Username', and 'Password'. The table lists five services: 'Active Template Repair Service', 'Active Directory Backup Service', 'GPO History Service', 'Maintenance Service', and 'Notification Service'. Each service has an empty 'Username' field and a 'Password' field with three dots in the middle. At the bottom of the dialog, there are three buttons: 'Help...', '< Back', 'Next >', and 'Cancel'. A link at the bottom reads 'For more detail on privileges and permissions required, please visit the Knowledge Base at www.scriptlogic.com/support'.

| Service | Username | Password |
|---------------------------------|----------|----------|
| Active Template Repair Service | | ... |
| Active Directory Backup Service | | ... |
| GPO History Service | | ... |
| Maintenance Service | | ... |
| Notification Service | | ... |

Use the following service account for all services

In the **Username** box, type a user name for a group/user with Domain Admin rights, or click  to locate a group/user. In the **Password** box, type the account's password.


Customize each service account

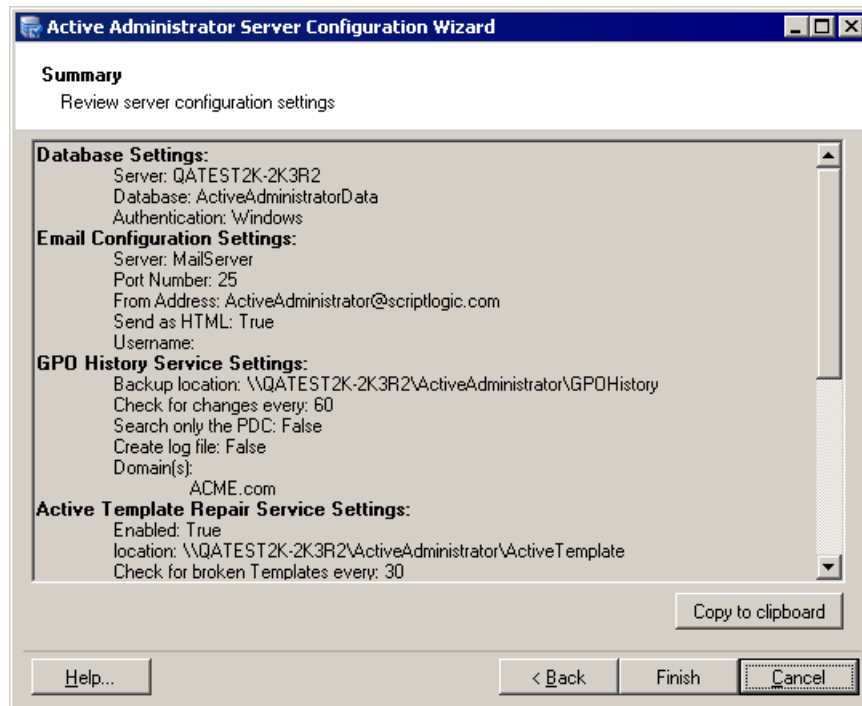
Select to enter a user name and password for each service. Leave the check box blank to use one username and password for all services.

Note: If you select to customize each service account, you must enter a valid username and password for each service.

- To advance to the next page, click .

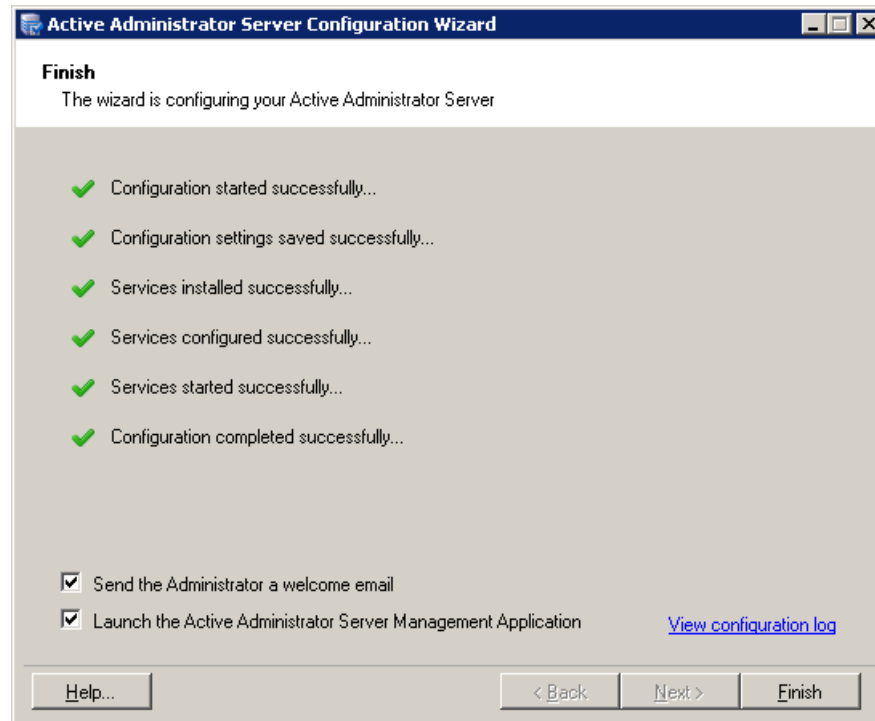
COMPLETING SERVER CONFIGURATION

The **Summary** page displays the choices that you made. If you want a copy, click  and then paste into a document.



- To advance to the next page, click .

The **Finish** box shows the progress of the installation. Upon completion, you can click [View configuration log](#) to examine details of the process.



Send the Administrator a welcome email






By default, an email is sent to the Administrator's email address.

Launch the Active Administrator Server Management Application

By default, the Server Management application launches when you exit the wizard.

- To close the **Active Administrator Server Configuration Wizard**, click .

The following services are installed:

-  Active Administrator Active Template Repair Service.
-  Active Administrator AD Object Backup Service.
-  Active Administrator GPO History.
-  Active Administrator Maintenance Service
-  Active Administrator Notification Service

STARTING ACTIVE ADMINISTRATOR SERVER COMPONENTS

1. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator 6**, and then select one of the following server components:

| Component | Description |
|---|--|
| Server Configuration Wizard | Configure the various Active Administrator services. |
| Server Management | Manage servers, Active Administrator services, and databases. |
| Server Tools > Diagnostic Tools | Collect information about your Active Administrator installation in a report that you can share with ScriptLogic Support Service. |
| Server Tools > Database Management Wizard | Create and manage auditing databases. |
| Server Tools > Forest Prep Utility | If using Windows Server 2003 Service Pack 1 (SP1) or higher, modify the schema to allow restoration of passwords when you restore accounts that were deleted. |
| Server Tools > Uninstall Audit Agents Utility | Uninstall Audit Agents from a specified server. You must have Administrator Rights on the server. Note: It is recommended that you use Server Management to remove Audit Agents. |

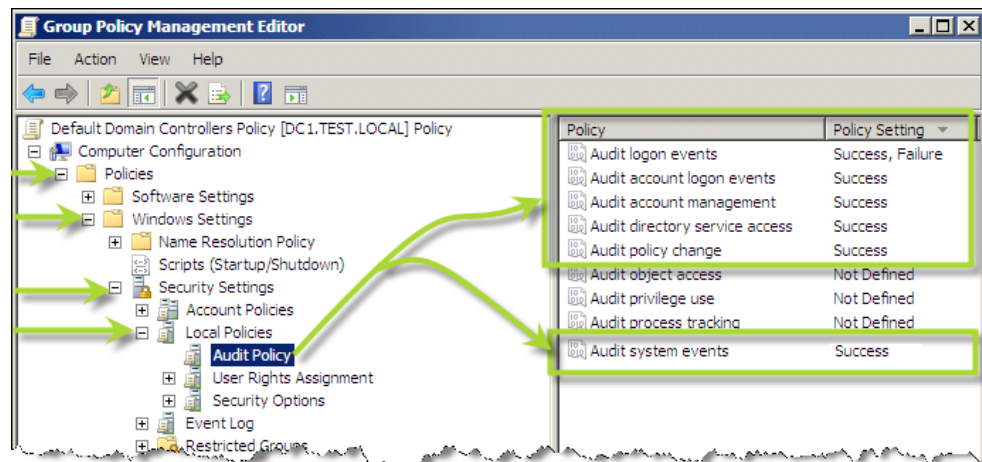
For more information on Active Administrator Server Components, see the *Active Administrator Server Management Guide* or access the help contents within the Active Administrator Console application

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.

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 6**, and then select **Active Administrator Console**. The **Active Administrator Console** opens to the **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 Management Editor** window opens.
4. Expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies**, and then select **Audit Policy**.



5. Verify that the following policies are defined. If not, double-click the following policies to edit their **Success** and **Failure** settings.

| | |
|---|---------------------------|
|  Audit logon events | [Success, Failure] |
|  Audit account logon | [Success] |
|  Audit account management | [Success] |
|  Audit directory service access | [Success] |
|  Audit policy change | [Success] |
|  Audit system events | [Success] |


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


Note: Auditing policy changes may take a long time to take effect.


Completing the Upgrade Process

Now that you have installed and configured the server, there are a few more tasks to complete the upgrade process.

UPDATING AUDIT AGENTS

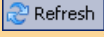
If the Audit Agent on the domain controller(s) does not match what is installed on the server, the version number displays in red  6.0.1.3. If this is the case, you need to update the Audit Agent on the domain controller(s).

If the Audit Agent on the domain controller(s) matches the version installed on the server, a green check mark displays next to the version number  6.0.1.5.

- ▶ To update the Audit Agent on the selected domain controller(s), click . Alternatively, choose **Update** from the **Agents** menu.

Note: You also can update the Audit Agent on the **Properties** page for the domain controller.

- ▶ To update the Audit Agent on all listed domain controllers, click . Alternatively, choose **Update All** from the **Agents** menu.

Note: You may need to refresh the Audit Agents to correct the display. Click , or right-click selected Audit Agents, and then choose **Refresh Selected** or **Refresh All**.

REMOVING ORPHANED AGENTS

If you are upgrading, there may be Audit Agents that are left over from previous installations. These Audit Agents do not display. Use the **Remove Orphaned Agents** option on the **Agents** menu to remove these Audit Agents.

Note: Prior to version 5, the Active Administrator Agent service was named Active Administrator Security Log Monitor, so you may see this term in the product in various places.

Removing Version 4 Audit Agents

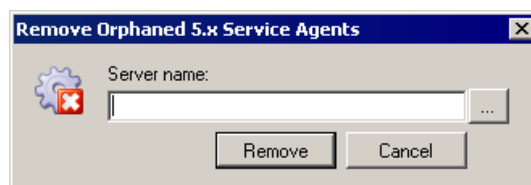
Important: You must remove all version 4 Audit Agents installed on the computer prior to installing version 6 Audit Agents.

1. Click **Start**, point to **Programs > ScriptLogic Corporation > Active Administrator 6**, and then select **AA Server Management**.
2. From the **Agents** menu, point to **Remove Orphaned Agents**, and then choose **4.0 Agents**. The **Remove 4.x Service Agents** window opens.
3. In the **Domain** box, type the domain name; or click to locate a domain.
4. Click . Domain controllers on the current domain are listed.
5. Select the domain controllers on which you want to remove the service agent. You can select the domain controllers individually, or click .
6. Click . A message box appears.
7. Click . The domain controllers are removed from the **Remove 4.x Service Agents** window.
8. Click .

Removing Version 5 Audit Agents

Important: You must remove all version 5 Audit Agents installed on the computer prior to installing version 6 Audit Agents.

1. From the **Agents** menu, point to **Remove Orphaned Agents**, and then choose **5.0 Agents**.




2. In the **Server name** box, type the name of the server with the orphaned Audit Agent, and then click .





INSTALLING AUDIT AGENTS

To collect data on a computer, you must install and activate the Audit Agent.

Important: Before installing the Audit Agent on a computer, run the **Remove Orphaned Agents** option on the **Agents** menu.

1. Click [Install Audit Agents](#) on the **Start Page**. Alternatively, choose **Install** from the **Agents** menu or click  on the **Collection Agents** tab. The **Audit Agent Installation Wizard** opens to the **Welcome** page.

Important: Auditing must be enabled in Active Directory. See *Setting Up Auditing on Domain Controllers*.


2. Click . The **Select Domain Controllers** page opens.
3. In the **Domain** box, type the domain name; or click  to locate a domain.
4. Click . Domain controllers on the current domain are listed.
 - To select all listed Domain Controllers, click [Check all](#).
 - To clear all the check boxes, click [Clear all](#).
5. Select the domain controllers from which you want to audit activity, and then click . The **Audit Agent Installation Options** page opens.

You can install the Audit Agent on the selected domain controllers themselves or on another computer in the current domain. A single Audit Agent should be able to monitor activity on up to five domain controllers, depending on the type and frequency of activities being audited.

Install on target Domain Controller(s)

By default, the Audit Agent is installed on the domain controllers you selected on the previous page.

Audit from an agent on the following computer

Select to install the Audit Agent on a computer in the domain. Type a computer's fully qualified domain name in the box, or click  to locate a computer.

Important: If you choose to do remote monitoring, the Advanced Agent is not installed on the selected domain controllers.

Start collecting events immediately after installation of the agent.

By default, the Audit Agent is activated and collection begins immediately upon completion of the installation process. Clear the check box if you want to activate the Audit Agents manually.

Note: To change the default setting of this feature, select **Settings** from the **Tools** menu, click **Agent Installation**, and then change the **Default Installation Action Option**.


Enable agent monitoring and recovery

By default, Active Administrator monitors the status of the Audit Agent.



6. Click . The **Audit Agent Startup Account** page opens.

7. In the **Run as** box, type an account with domain admin rights, or click to locate an account, and then enter the password.

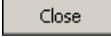
Note: The Active Administrator Agent service can also run under a domain user account provided it is either a local admin account, which gives it the rights to logon as a service and log on locally, or these two privileges can be granted individually. This user or service account should also be a member of the AA_Admin group, which by default is located in the Local groups of the server where the ActiveAdministrator database is located. If the group is not found in this location, the settings during the initial database creation were modified and it can be found under the Users container object of Active Directory.

8. Click . The **SQL Server Authentication Type** page opens.
9. Select whether to use the Audit Agent startup account or SQL Server authentication.



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

10. Click . The **Summary** page displays the selections you made.
11. Click  to begin the installation process. The **Finish** page displays the progress.

Upon completion, you can click [View log file](#) to open the **AuditAgentInstall*.log** file, which is located in the **Program Files\ScriptLogic Corporation\ Active Administrator 6\Server\Logging** folder.

12. Click . The **Collection Agents** tab lists the domain controllers you selected, the time and date of the last event collected, the status of the Audit Agent and the Advanced Audit Agent, the name of server on which Active Administrator is installed, and the version number of the Audit Agent installed on the domain controller.

Note: By default, the Audit Agent is activated upon installation. To change the default setting, choose **Settings** from the **Tools** menu, and then click **Agent Installation**.



- If the Audit Agent on the domain controller(s) does not match what is installed on the server, the version number displays in red  6.0.1.3. If this is the case, you need to update the Audit Agent on the domain controller(s).
- If the Audit Agent on the domain controller(s) matches the version installed on the server, a green check displays next to the version number.  6.0.1.5.


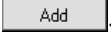
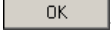








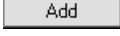
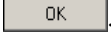


IMPORTING DATA FROM EXISTING AUDIT DATABASES

If you are upgrading from Active Administrator 4.x, you can import data from those existing databases into the version 6.x Audit Database.

1. From the **Tools** menu, choose **Import Auditing data from 4.x to 6.x**. The **Import Wizard** opens to the **Welcome** page.
2. Click **Next**. The **Select Source Database** page opens.
3. From the **Server Name** list, chose the SQL server.
4. In the **Log on to server** area, chose whether the server uses **Windows** or **SQL Server Authentication**. If you chose **SQL Server Authentication**, type the **User Name** and **Password**.
5. From the **Database Name** list, choose the database from which to import data.
6. Click **Next**. The **Resolve Domain Names** page opens listing any NetBios Names and the associated Fully Qualified Domain Name (FQDN). For data to be imported into the version 6 database, you must either enter a FQDN for each NetBios name, or exclude the NetBios name from the data import.
 - a. Select a NetBios name, and then click **Edit**. The **Edit Domain Name** box opens.
 - b. Type a FQDN or select the **Exclude** check box.
 - c. Click **OK**. If you chose to exclude the data, a red minus sign appears on the icon.
 - d. Click **Resolve**. If there are any NetBios name still unresolved, you see a warning message.
7. When all NetBios names are resolved, click **Next**. The **Summary** page lists the choices you made.
8. Click **Next**. The **Import Audit Data** page displays the progress of the import process. When complete, you have the option to view an import log.

CREATING AN ALERT

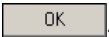
1. Open the **Alerts** tab, and then click . Alternatively, choose **New Alert** from the **Alerts** menu or click [Create an Alert](#) on the **Start Page**. The **Alert Wizard** opens to the **Event Definitions** page.
2. Select the Event Definitions to include in the Alert.
 - To filter the list, type **text** in the **Filter** box. The list changes as you type characters. The definitions displayed contain the characters you type. For example, if you type **com**, the definitions displayed may contain the words **Completed** or **Computer**.
 - To clear the filter and restore the list, click .
 - To show only selected definitions, open the **Show** box, and then choose **Selected**.
 - To show only unselected definitions, open the **Show** box, and then choose **Unselected**.


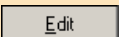
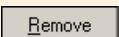
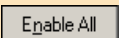



3. Click . The **Email Addresses** page opens.
4. In the **Email Addresses** box, click . The **To Address** box opens.
5. In the **To Address** box, type one or more email addresses. Separate multiple addresses with a semi-colon (;).
6. Click . The email addresses are added to the **Email Addresses** box.
7. In the **Priority** box, select **Normal**, **Low**, or **High** priority.
 - To remove selected email addresses from the list, click .
8. Click . The **Alert Action** page opens.
 - Enable Alert Action**
Select to assign a program with arguments to execute when the Alert Condition is met.
 - In the **Program or script** box, type the full path to the executable or click  to locate the executable.
 - In the **Arguments** box, click  to open the list of **Alert Action Variables**. Select a variable in the top box, and then click .
 - In the **Execute program or script in this folder (optional)** box, type the path to a folder that contains the executable or click  to locate the folder.
 - Execute the action using the Notification service account**
By default, the action is executed using the Notification service account.
 - Execute the action using another account**
Select to use another account to execute the action. Click , and then enter a user name and password.
9. Click . The **Alert Filters** page opens.
10. Click . The **Alert Filter** box opens.
11. From the **Contain Operator** list, select if the email **Contains** or **Does not contain** the condition text.
12. In the **Condition Text** box, type the text to find in either the subject or body of the email.
13. Click . The Alert Condition is added to the list. Continue to add more alert conditions.
 - By default the filter conditions are combined using the **OR** operator. If you want to connect with the **AND** operator, select **AND**.
 - To remove a selected alert condition from the list, click .
14. Click . The **Alert Quiet Times** page opens.

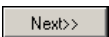



15. Click . The **Alert Quiet Time** box opens.

Define the quiet time during which no notifications are sent. Alerts that are triggered during the quiet time are still logged to the Alert History.

Note: If you do not want the actions associated with the Alert to execute, clear the **Execute Action During Quiet Time** check box.

16. Click . The Alert Quiet Time is added to the list.

| Button | Description |
|---|---|
|  | Add an Alert Quiet Time. |
|  | Modify a selected Alert Quiet Time. |
|  | Remove selected Alert Quiet Times. |
|  | Enable all Alert Quiet Times. To enable a selected Alert Quiet Time, click  , and then select the Enabled check box. |
|  | Disable all Alert Quiet Times. To disable a selected Alert Quiet Time, click  , and then clear the Enabled check box. |

17. Click . The **Name** window opens.
18. In the **Alert Name** box, type a name for the Alert.
19. Click . The **Summary** page lists the settings you entered.
- To modify any of the settings, click .
 - To copy the contents to the clipboard so you can paste into a text editor, click [Copy to clipboard](#).
20. Click . The Alert is added to the list.

USING ACTIVE ADMINISTRATOR SERVER

For more information on using the Active Administrator Server, see the *Active Administrator Server Management Guide* or access the help contents within the Active Administrator Server Management application.

Active Administrator Console Installation

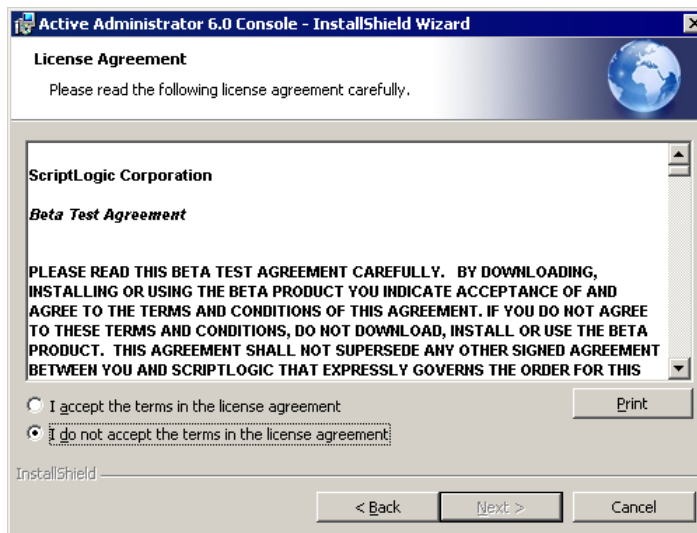
Install the Administrator Console on any workstation that requires the use of Active Administrator.

RUNNING THE ACTIVE ADMINISTRATOR CONSOLE INSTALLATION WIZARD


1. After downloading the **Active Administrator 6.0.x Console exe** file, double-click the file name/icon, or right-click the file name/icon, and then select **Install**. The InstallShield Wizard opens to the **Welcome** page.

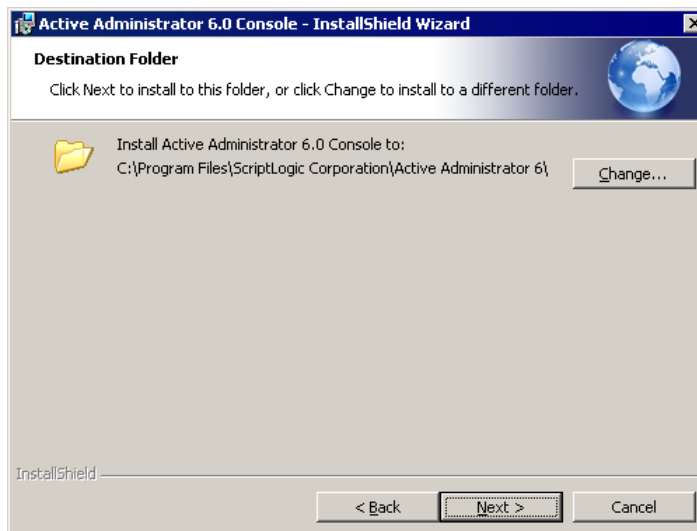


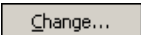
2. Click . The **License Agreement** page displays the Transaction Product Agreement.




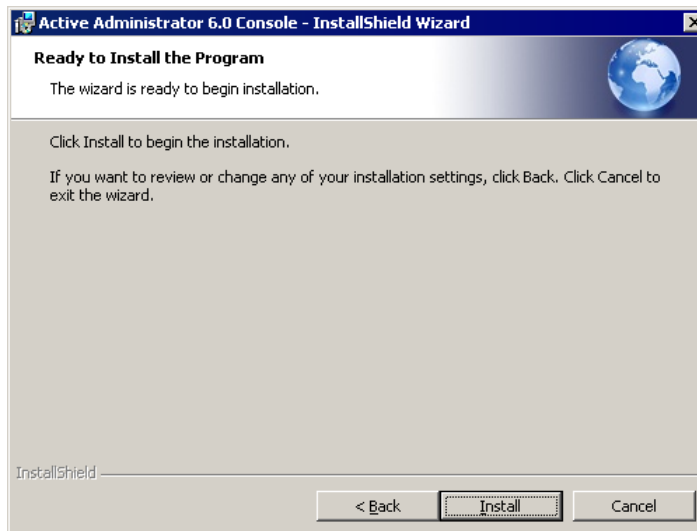
Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or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

3. Select **I accept the terms in the license agreement**, and then click . The **Destination Folder** page appears.



- To change the location of the program files, click . The **Change Current Destination Folder** page opens. Choose a new location for the installation directory.

4. Click . The **Ready to Install the Program** page appears.




5. To begin the installation, click **Install**. When the installation is complete, the **InstallShield Wizard Completed** page opens.



Launch Active Administrator 6.0 Console

By default, the option to start the Active Administrator Console is selected. If you do not want to start the console, clear the check box.

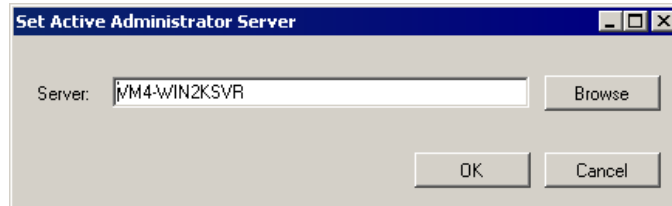
6. Click . The following Active Administrator component is installed:

SETTING THE ACTIVE ADMINISTRATOR SERVER

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

The first time the Active Administrator console opens, you are asked to set the Active Administrator Server.

1. In the **Server** box, type the name of the server where Active Administrator Server is installed, or click to locate a server.



2. Click .

Note: If you want to change the server, choose **Set Active Administrator Server** from the **Tools** menu.

STARTING ACTIVE ADMINISTRATOR CONSOLE

- ▶ Click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **Active Administrator 6**, and then choose **Active Administrator Console**.

USING ACTIVE ADMINISTRATOR CONSOLE

For more information on using the Active Administrator Console, see the *Active Administrator Console User Guide* or access the help contents within the Active Administrator Console application.

USING ONLINE HELP

Important: If Windows Internet Browsing Security is turned on, you may see a warning message when you access some topics in the online help file. If Internet Explorer Enhanced Security is disabled, this message does not appear.