



ACTIVE ADMINISTRATOR™

What's New Guide

Active Administrator 6.0

© 2011 ScriptLogic Corporation
ALL RIGHTS RESERVED.

ScriptLogic, the ScriptLogic logo and Point,Click,Done! are trademarks and registered trademarks of ScriptLogic Corporation in the United States of America and other countries. All other trademarks and registered trademarks are property of their respective owners.

Contents

What's New—Feature Highlights for Version 6.0.....	4
Active Administrator Solution Summary	4
Release Summary.....	4
Active Directory Health.....	5
Active Directory Health Assessment Reporting.....	5
Active Directory Replication Monitoring	6
Active Directory Account Maintenance.....	7
Account Maintenance – Users and Computers	7
User Account Maintenance – Change Your Password Reminder Policy	8
Auditing Your Way	9
Active Auditing – Out of the Box	9
Centralized, Shared Reporting.....	9
New Auditing Events for Authentications	9
Auditing Enhancements – New Search Filters.....	9
Active Alerting.....	10
Alert History	10
Alerting Thresholds.....	10
Alert Quiet Times and Alert Suspensions	11
Alert Notification Policy	11
Change Control & Audit Record.....	11
Administrative Comments	12
Audit Report Workflow – Audit Tags, Comments, & Email Ability.....	12
Security & Delegation	14
Temporary Self-Expiring Active Templates.....	14
Active Template Categories	14
Trustees and Permissions	15
Group Policy Customer Requested Enhancements.....	16
Backup & Recovery – New Quick Recovery	16
Usability Enhancements & New Start Pages	17

What's New—Feature Highlights for Version 6.0

Active Administrator Solution Summary

ScriptLogic® Active Administrator™ is a comprehensive and proactive Active Directory® management platform. Active Administrator solves the five major Active Directory management and reporting challenges within one solution – including centralized event auditing, backup and recovery, Group Policy management with offline editing and rollback, simplified delegation of Active Directory security, and Active Directory health assessment, monitoring, and maintenance.

Active Administrator is a complete solution that is simpler and faster than native Windows tools. It is also more cost effective and efficient than multiple Active Directory point solutions. Active Administrator is a proven product that helps organizations meet compliance regulations, tighten security, increase productivity, and improve business continuity.

Release Summary

Active Administrator 6.0 is going to be the most exciting release ever!

We have extended our award-winning Active Directory product to solve more common pain points in broad new areas around Active Directory health assessment, replication monitoring, account maintenance, and much more! These new features are designed to help assess and proactively solve problems that occur in Active Directory domains every day. We have also added several new features to improve organizational security and compliance, resulting in less work for you!

We have also added more auditing features for Active Directory, as well as more for Active Administrator itself. Now you can enjoy more confidence and peace of mind with Active Administrator, as well as a continued quest for the perfect Active Directory environment. There are many new major improvements in auditing, alerting, and notification. We have also included a variety of small tricks and enhancements to simplify configuration and use. You'll see much more automation and out-of-the-box features, including new Start Pages, more default configurations, and new predefined reports, alerts, and notifications. We have also added convenience with features that make searching in Active Administrator easier and quicker.

With version 6.0, our theme to increase efficiency by working smarter not harder with Active Administrator continues with our new change password reminder policy and automated account management that monitors and cleans up inactive users and computers.

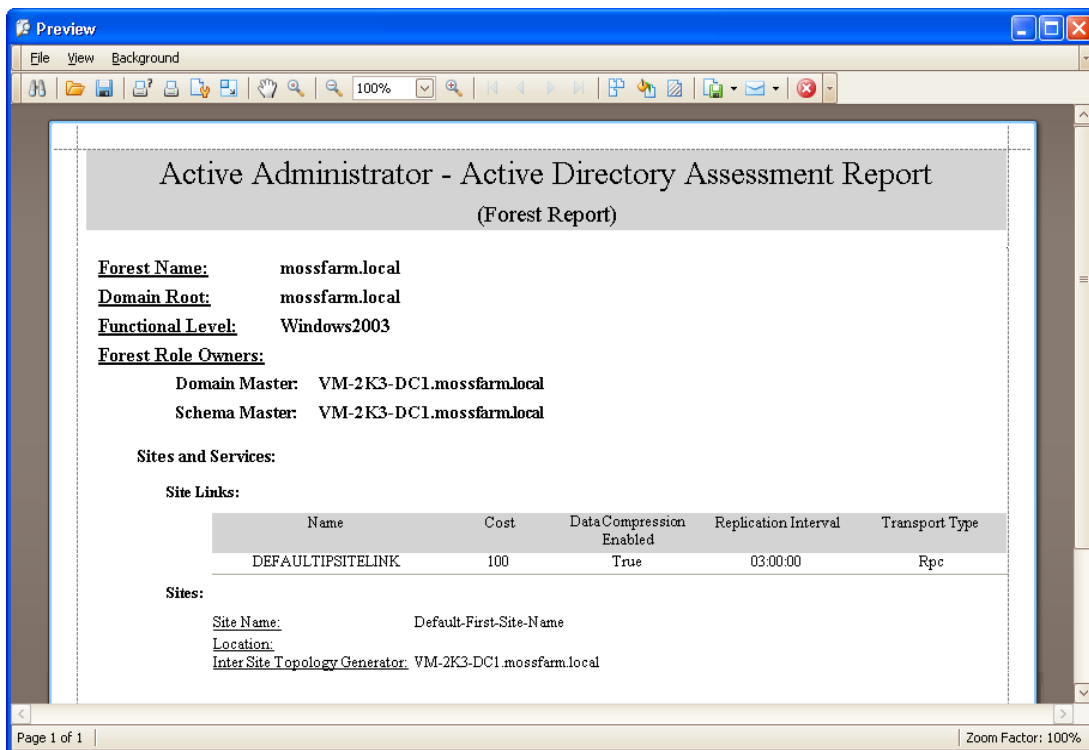
To summarize, this major new release includes a wealth of fresh enhancements and features that add value and solve more challenges than ever before. *After all who has time or money to install, manage, maintain, and pay for multiple Active Directory software solutions when you can use one complete solution like Active Administrator?*

Active Directory Health

Version 6.0 introduces several new broad areas designed to quickly ease the administrative burden of monitoring the overall health of the Active Directory environment. When Active Directory is not configured or is not working properly, it can create havoc across the entire organization and make it difficult to trace down root cause analysis. The new features in this release are geared towards helping to find big problems fast, do quick checkups, and deliver scheduled reports in less time. Active Administrator now includes basic Active Directory assessment reporting and health checkup functionality in the two most problematic areas that can cause serious issues within Active Directory environments – Active Directory configuration and Active Directory replication.

Active Directory Health Assessment Reporting

The first new feature around Active Directory health reporting is the Active Directory Assessment Report. This brand new report performs a full environmental assessment of the Active Directory infrastructure, including detailed information on the domain, trust, forest, functional level, configurations and more. The report is designed to give administrators an overview of the domain and associated information quickly to spot any potential changes or problem areas. It is also quite useful for compliance snapshots and pre/post system maintenance. The Active Directory Assessment Report can be scheduled to run at recurring intervals and delivered to administrators via email or distributed to file share locations automatically.



The screenshot shows a 'Preview' window displaying an 'Active Directory Assessment Report (Forest Report)'. The report details the following information:

- Forest Name:** mossfarm.local
- Domain Root:** mossfarm.local
- Functional Level:** Windows2003
- Forest Role Owners:**
 - Domain Master: VM-2K3-DC1.mossfarm.local
 - Schema Master: VM-2K3-DC1.mossfarm.local
- Sites and Services:**
 - Site Links:**

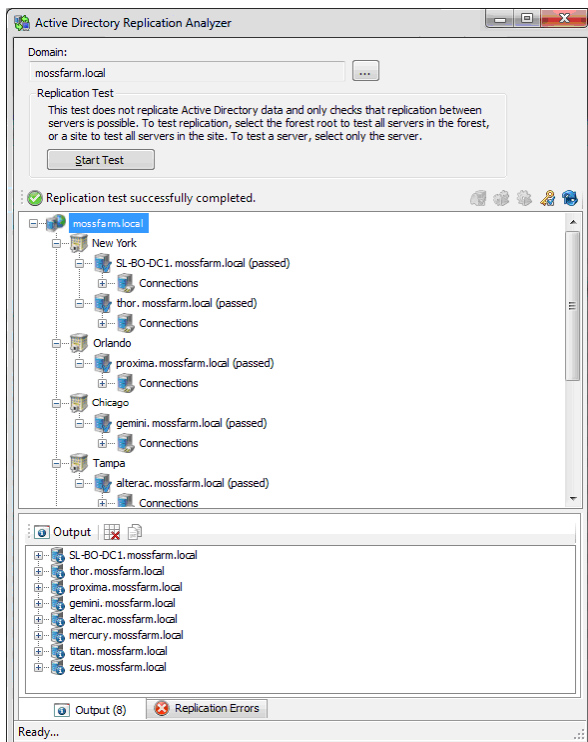
Name	Cost	Data Compression Enabled	Replication Interval	Transport Type
DEFAULTIPSITELINK	100	True	03:00:00	Rpc
 - Sites:**
 - Site Name: Default-First-Site-Name
 - Location:
 - Inter Site Topology Generator: VM-2K3-DC1.mossfarm.local

The window title is 'Preview' and the status bar at the bottom indicates 'Page 1 of 1' and 'Zoom Factor: 100%'.

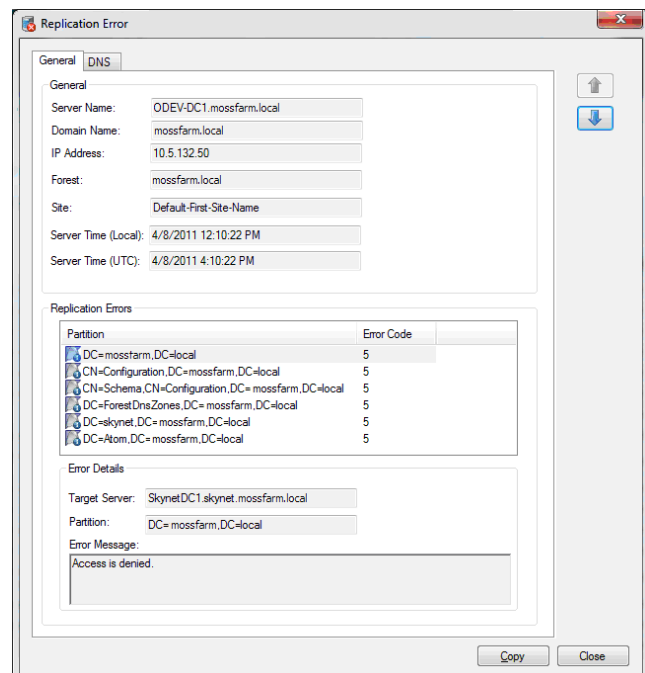
Active Directory Assessment Report

Active Directory Replication Monitoring

Active Administrator can now be used for Replication health checkups and monitoring, which can be scheduled and accessed through a new interactive area; the **Replication Analyzer**. You can configure the areas to analyze as part of the replication health checkups, filtering by forest, site, or individual server. Results are displayed quickly, and more information on the test results is available on the detail view screens, including both general replication errors and DNS test result information. These Replication health checkups are scheduled to run automatically, and an email status report will be delivered to administrators on a recurring basis to help identify any possible issues before the impact becomes critical.



Replication Analyzer



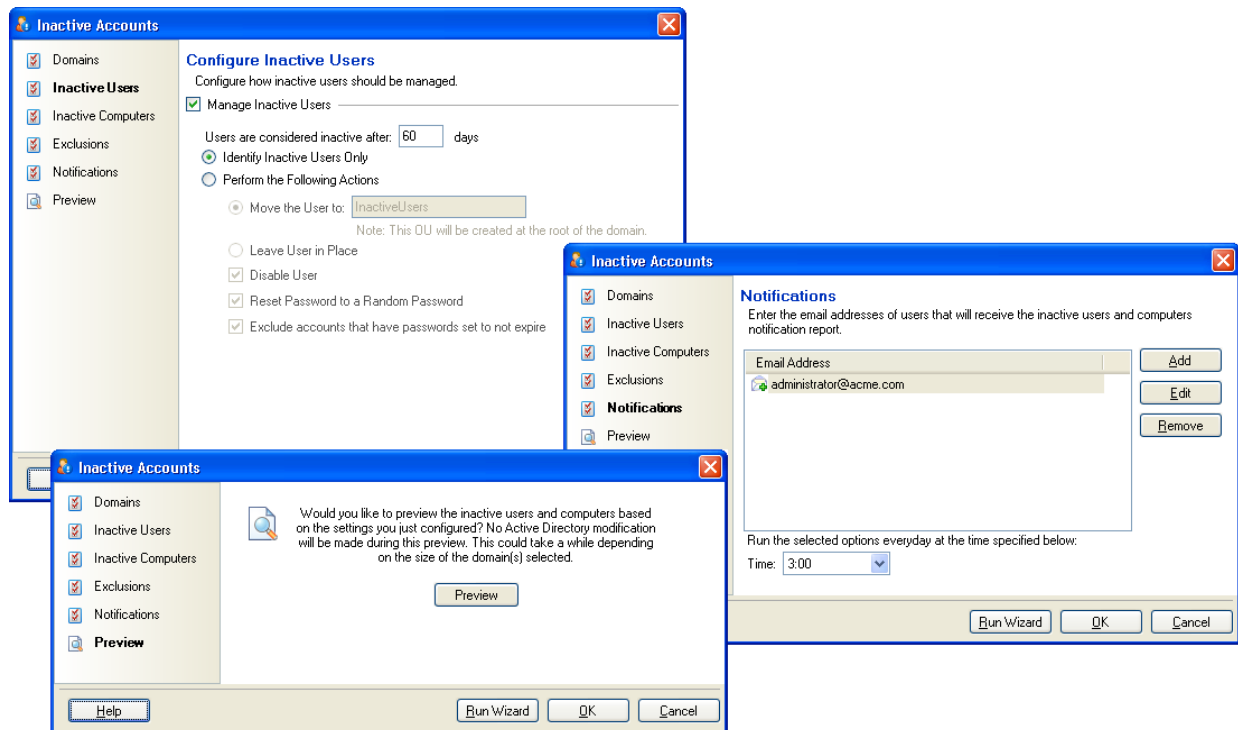
Replication Errors Detail

Active Directory Account Maintenance

This new release introduces two new major automated areas that will help ease the administrative burden and support hassles of maintaining and managing Active Directory users and computers. More and more Active Directory administrators are feeling the pain and after effects that come with managing critical Active Directory environments with reduced staff and limited time. Add to that the growing distribution of company locations, remote users, and remote offices, and the challenge of tracking active/inactive users and computers becomes very real. All too often, the end result is many inactive computers and user accounts still left active in Active Directory. This can easily result in security risks and increased costs.

Account Maintenance – Users and Computers

Active Administrator can quickly scan, assess, and identifies inactive users and computers in a domain environment. It will also clean up these accounts and ease the burdens of management going forward in an automated, proactive manner. The new features in 6.0 are designed to provide simplicity in previewing, assessing, and reporting on inactive users. Special actions are then taken with these accounts, such as moving or disabling them. This process can be configured to your environment, previewed and tested quickly, and scheduled for ongoing maintenance. There are also administrator notifications and a comprehensive historical audit record with reporting for compliance purposes, making it simple to show and monitor the active and computer accounts.



User Account Maintenance – Change Your Password Reminder Policy

Active Administrator now includes a simple way for administrators to reduce user/password maintenance headaches. Administrators have told us that they often spend time correcting Active Directory user accounts for individuals who simply forgot to change their password before it expired. This new policy allows the administrator to schedule and automate a friendly and customized password reminder email that is automatically sent to all individuals who have passwords nearing expiration. This friendly reminder message can include things like instructions on how to change a password, as well as any special notes on your password policies.

Auditing Your Way

This new release includes many new related items for the auditing, alerting and notification areas designed to streamline just how, when and where Administrators access and view the data they need most.

Active Auditing – Out of the Box

With the last release, we introduced the concept of one consolidated audit record for Active Directory, GPOs and Active Administrator. With this release, there are many new features to greatly enhance the entire auditing area. There are new predefined reports and alerts out-of-the-box to simplify configuration and illustrate value.

Centralized, Shared Reporting

Report creation can now be centrally managed, and reports can be shared—a common request for organizations with multiple administrators or auditors. With this new release, the reporting architecture has been consolidated, with the actual report files stored in our centralized database and no longer on local computers. To help organize shared reporting, there are also new user-defined report categories and a new ‘favorites’ category to help make it easier to manage multiple custom audit reports.

New Auditing Events for Authentications

There are several new Active Administrator event definitions that enable auditing, reporting, and alerting on changes within Active Administrator itself, such as the GPO repository when GPOs are added, removed, published to Active Directory, restored, and checked in or out. New auditing event definitions for Active Directory authentication related events have also been added including:

- Account Logon and network authentication (event IDs 540 and 4624)
- Kerberos authentication ticket (TGT) for (event IDs 672 and 4768)

Auditing Enhancements – New Search Filters

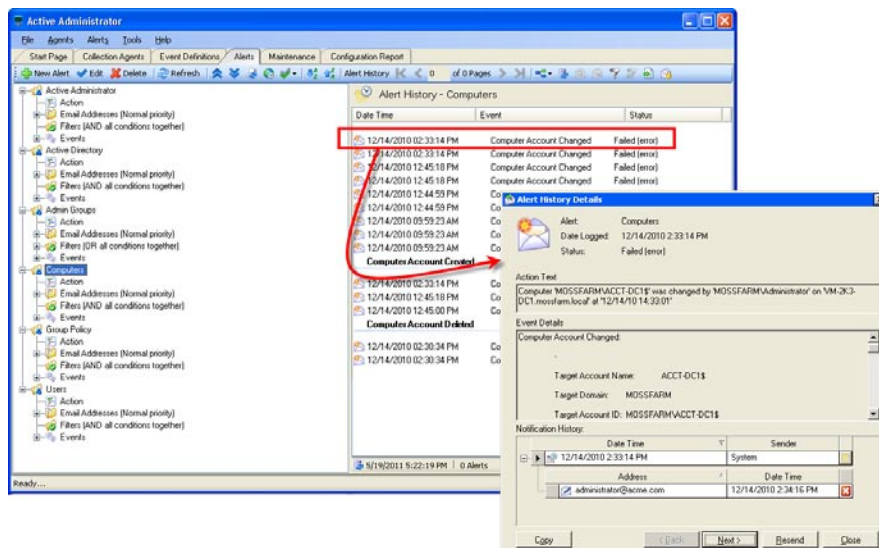
The Auditing area has experienced several enhancements that provide more access and query options for searching and reporting on the auditing data. The auditing Event Description Mask filter now provides new ability to search the text details of an event (instead of only the event's description). There is also a new **Attribute** filter to search on. Quick search filter options have been added to several screens to make it simple to find the event definitions needed.

Active Alerting

Version 6.0 introduces **Active Alerting**, which is a collection of many small but powerful new options that provide more control and flexibility in configuring and limiting the amount of information, types of alerts and notification level details. Active Alerting includes smarter alerts, providing the information that you care about. Active Administrator system also retains all of the information for historical reporting, if necessary.

Alert History

The new **Alert History** area includes a detailed audit record that stores everything related to Active Administrator alerts, including the alert detailed information, recipient, alerting status, ability to resend the alert manually, ability to query and filter, and ability report on history. All of the alert history data is stored in the central database and becomes part of the permanent audit record. This alert audit record can be useful for security risk investigations to help trace and show that proper auditing and alerting was in place and notifications were sent during specific incidents. You can also manually resend alerts in situations where it might be necessary, such as an Administrator on vacation or out sick. This alert history record can also be useful to help troubleshoot email or system notification problems as it makes it easy to see that alert notifications were triggered when appropriate.



Use Alert History Details to Troubleshoot

Alerting Thresholds

Alert Notification Thresholds introduces intelligent and active alerting by allowing custom notification threshold rules to be configured as part of an alert. For example, you may not want to be notified if one user is disabled, but if 10 users are disabled in a short period of time, it may be a critical situation requiring notification.

Alert Quiet Times and Alert Suspensions

Alert Quiet Times are new and configurable predefined times when the system will not send alerts. During Alert Quiet Times, such as late evening or early morning hours, no alerts will be delivered. This eliminates unnecessary interruptions to notify administrators of common scheduled tasks being performed.

Let's say that you just received 100 email notifications and you realize that one of your junior administrators must have started the import of 1000 new users. Now with the new **Alert Suspension** feature, you simply log into Active Administrator, and then suspend one or all alerts until the important task is completed.

Alert Notification Policy

The new **Alert Notification Policy** enables Active Administrator to automatically watch, tailor, and limit the number of notifications that can be sent within time periods. The system will stop sending the alerts, but will still record the alert and its associated history to the database so it can be reported on or resent manually at a later time if needed.

Change Control & Audit Record

There are several new features in key areas that help administrators quickly see more information on change control within Active Directory, on GPOs, and within Active Administrator. All information is stored in a centralized database, and historical reporting is available as well.

Administrative Comments

Comments are optional textual records that can be related to specific events and entered into Active Administrator if desired. The comments framework is designed to be flexible for administrators who need to save and associate more detailed information on important changes in their environments. The administrative comments are saved with the audit record and include the date, time, user, and any custom text that was entered. To facilitate the change control process and easier compliance, the comments can be shown in reports. The following features in Active Administrator now provide the ability to include administrative comments:

- **GPO Repository Check In** – comments can be added when a GPO is checked into the GPO Repository
- **GPO Restore** – comments can be included when objects are restored
- **Active Directory Restore** – comments can be added when Active Directory objects are restored
- **Audit Report Item** – comments can be added to one or more specific audit items

Audit Report Workflow – Audit Tags, Comments, & Email Ability

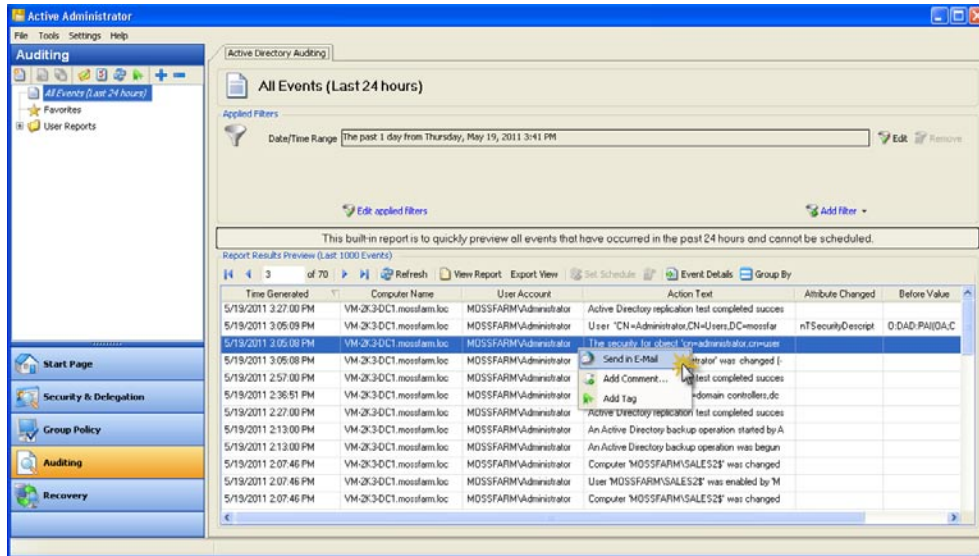
The new report creation process has been simplified and the Auditing viewer area has several smaller workflow enhancements that can be used together or individually.

Audit Report Item Tagging is the new ability to tag specific audit items that may be important or related, so you can easily search and report on specific event(s) that were tagged and important for your environment. You will also have the ability to search and report on these new audit tags just like any audit filter. Tags are user-defined and text based. To try this new feature, we recommend that you tag a few consistent events that make sense for your business and environment. Consider using tags like hardware maintenance, upgrade, new user creation, and admin error, etc.

To help with the overall audit record and in managing Active Directory change control, we have added a new ability to store related **Administrative Comments** in auditing and several other areas across the product. You can include more text information, such as internal change control records and notes, for reporting and historical purposes later on.

From the Auditing viewer is a new feature that will assist with troubleshooting and investigation to **Email Audit Events** – simply right-click your mouse to create an email that includes the audit event item details. For example, if there is a particular auditing change in the logs that doesn't look quite right, it's easy to send a note to another administrator asking for clarification on what happened or why the change was made. You may then want to tag that audit item as *'needs follow up'* to help remind yourself to follow up on it at a later time.

It should be clear now. All of these new small features are designed to work together and provide greater access to the power of auditing information streamlining everyday workflows.

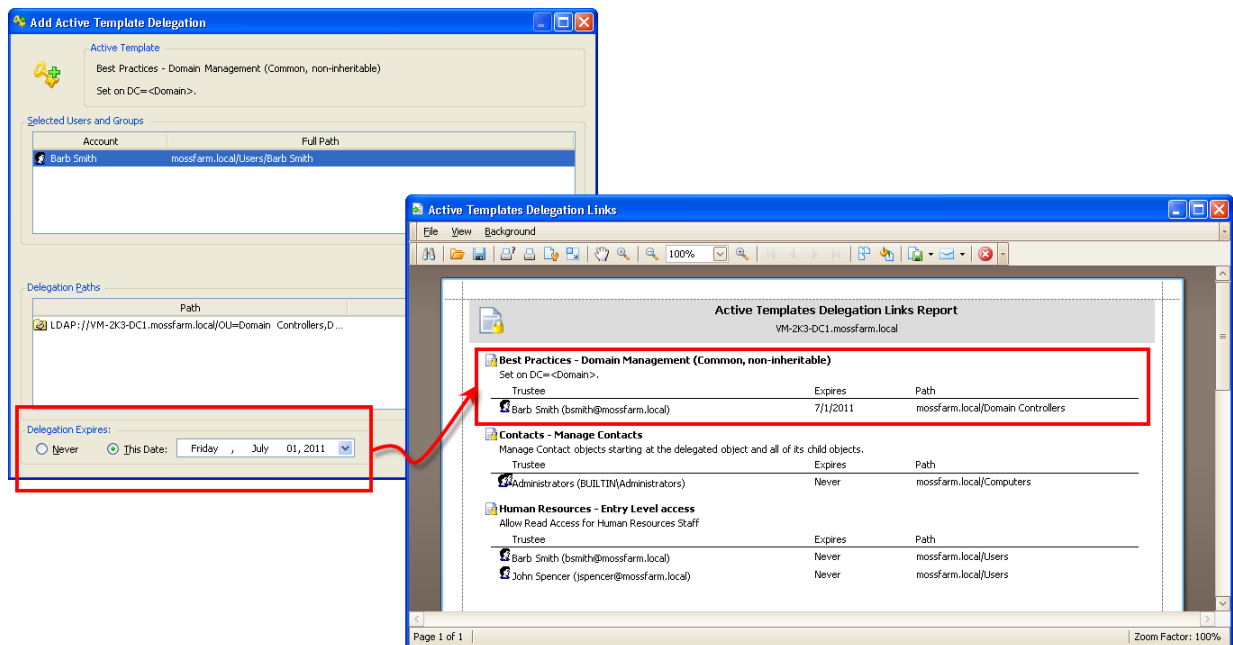


Easily tag and comment on events, or send e-mail from the Auditing Viewer

Security & Delegation

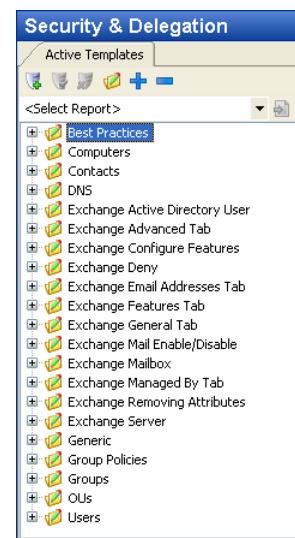
Temporary Self-Expiring Active Templates

Active templates can now include an effective stop date for permissions delegations, which is useful for temporary security delegations for individuals who need limited periods of access or for consultants who may be in for a known period of time. When the stop date is reached, the system will expire the permissions and then notify the administrator. Active Template reports have been expanded to show this information.



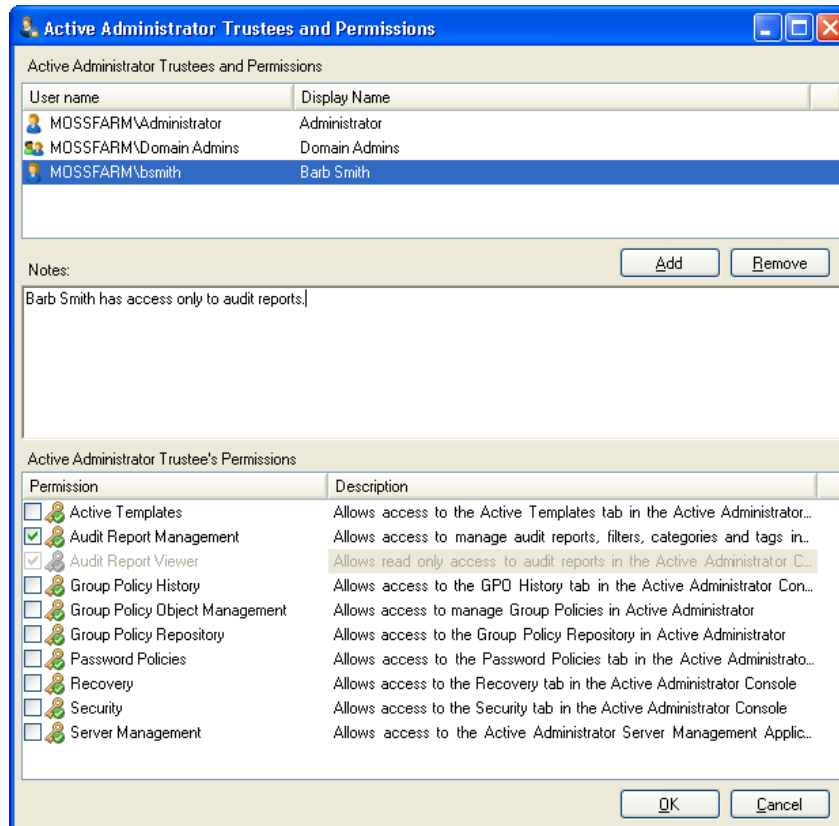
Active Template Categories

Similar to report categories, the Active Templates area now supports categories, which are logical groups that can be used to help organize and manage Active Templates. Included are several out-of-the-box categories, which you can personalize to meet your specific organizational needs.



Trustees and Permissions

The application level security roles and permissions have been expanded to support a more detailed level of application level restrictions. More detailed access levels within Group Policy was a common request for sites with multiple administrators, and this feature can be combined with the new ability to give junior administrators the control to manage the Offline GPO Repository.



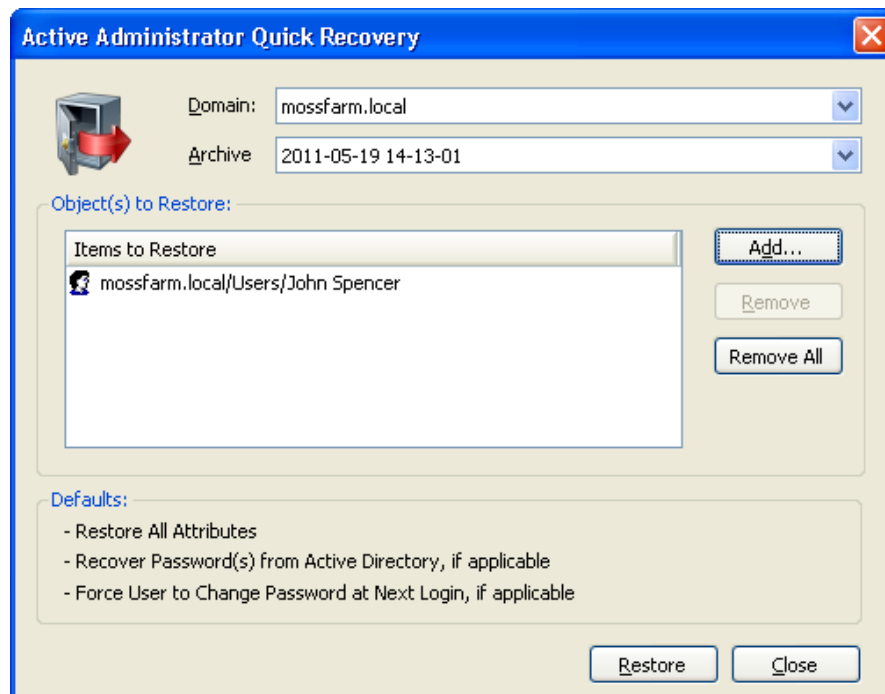
Group Policy Customer Requested Enhancements

Several Group Policy enhancements requested by our customers have been added to provide new functionality and more security. It is now possible for individuals who do not have administrative rights in the domain to be able to manage GPOs in the Offline Repository, which was a common request for junior administrators.

There is also the new ability to reorder GPO links to OUs, and a new feature that supports blocking and unblocking GPO inheritance on an OU. There are several new auditing event definitions surrounding GPO state changes and GPO areas within Active Administrator as well, and GPO changes now support the inclusion of administrative comments for more change control records.

Backup & Recovery – New Quick Recovery

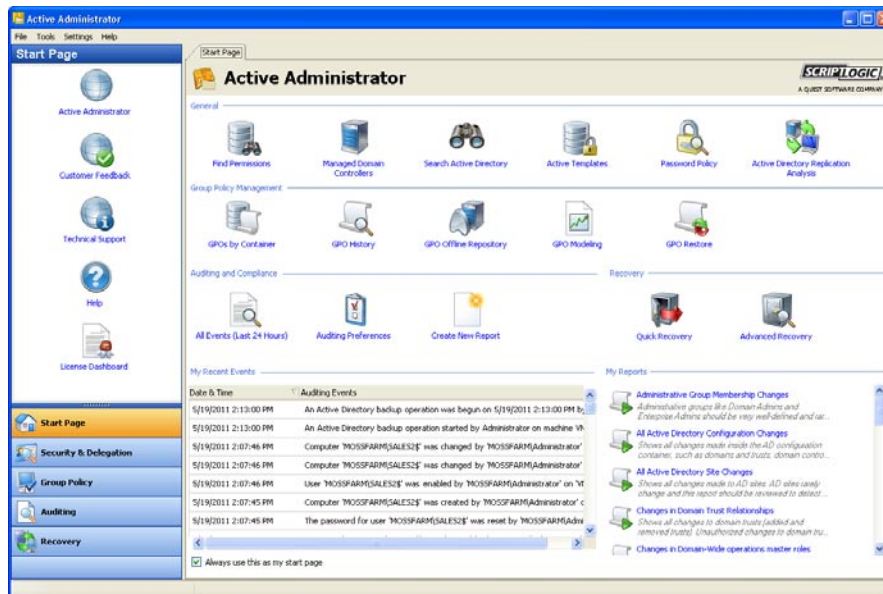
Backup and Recovery within Active Administrator is even easier to use, thanks to an intuitive new **Quick Recovery** option, which is available on the Console Start Page. This option is designed to enable an almost instant restore of Active Directory objects using a set of common, best-practice settings during the Active Administrator recovery process. Only a few clicks are needed to recover Active Directory objects when time is of the essence — *just pick the domain, pick the backup archive file, pick the objects to restore, and then go.*



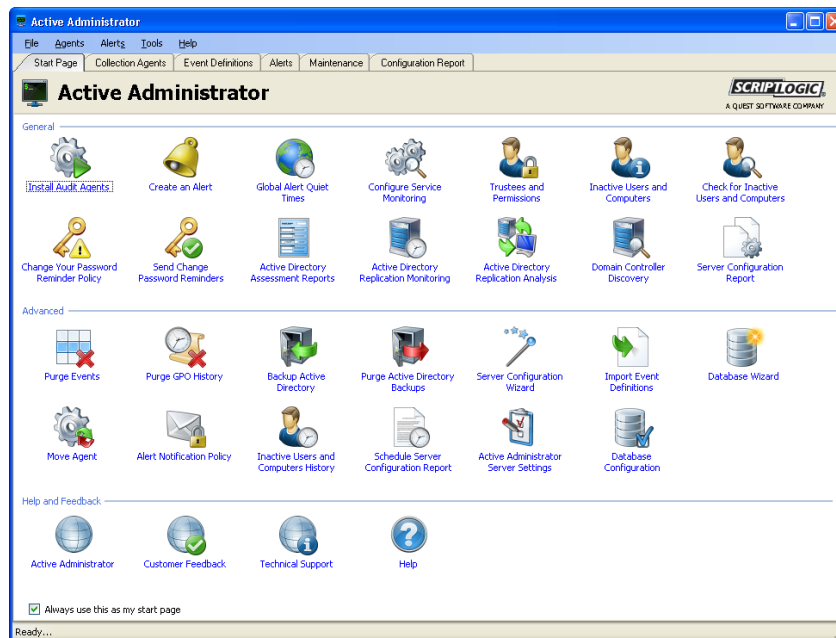
Quick Recovery

Usability Enhancements & New Start Pages

With this release, we continue to aim to improve our software. We have redesigned the Start Pages and added more features for one-click access. There is new context-sensitive help to make it easier to find information in our documentation. We also added many smaller usability features that we hope will add value beyond the major items noted above. *Thank you for your continued support of Active Administrator and for sharing your experiences with our products!*



Active Administrator Console Start Page



Active Administrator Server Management Start Page

For more information, please visit <http://www.scriptlogic.com/products/activeadmin/>