ACTIVE ADMINISTRATOR™

Active Administrator is a comprehensive management and auditing solution enabling administrators to efficiently manage Active Directory security and Group Policies in Windows® 2000 and 2003 based networks.

While extremely powerful and flexible, Active Directory quickly becomes very complex to manage in Windows networks of any size. Administrators leave, users are given elevated privileges, applications require special accounts – very soon you have an Active Directory full of security weaknesses with no way to find or audit them. Add to that the difficulty of recovering from accidental deletions of users, groups or OUs, and the risk of editing Group Policies in a live environment… Managing Active Directory using the built-in tools for even simple tasks quickly becomes overwhelming.

Active Administrator is an enterprise solution focused on streamlining Active Directory security and Group Policy Management. With an easy to use interface, Active Administrator provides a single and central point of control for your entire Active Directory environment. Active Administrator reduces your Active Directory cost of ownership with time-saving point-and-click control of essential Active Directory security and Group Policy settings.

ENSURE ACTIVE DIRECTORY SECURITY

Active Administrator gives administrators a window directly into the security of Active Directory objects. The built-in tools require navigating to the Security tab of an object's properties and often several more clicks to view security information in piecemeal fashion. Active Administrator simply navigates up and down the whole Active Directory environment in one pane, showing permissions of selected objects in another. You can easily filter default as well as inherited permissions, viewing only those that have been added or delegated. You can also easily search Active Directory for where a user or group has permissions. Active Administrator provides the power and ease of use for navigating, understanding and viewing Active Directory permissions.
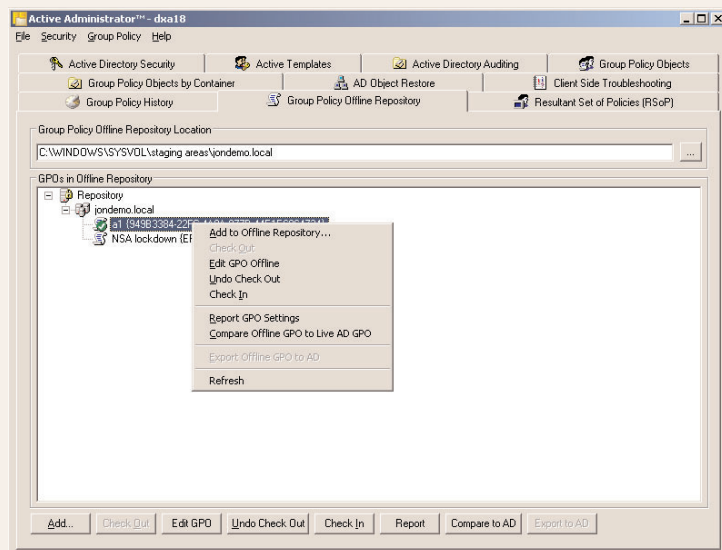
DELEGATE ACTIVE DIRECTORY CONTROL

One of the most difficult tasks in managing Active Directory security is assigning permissions consistently. The built-in Delegation of Control wizard has no mechanism to determine if permissions have changed since initial assignment and no mechanism to easily repair them if required. To assign permissions, Active Administrator uses "Active Templates" - defined sets of permissions required for a particular user role. Templates are defined with appropriate permissions, and then applied to users and other objects when needed, ensuring that permissions are consistently assigned. Active Administrator then monitors those Active Template permissions for any modifications or deletions, and can auto-repair the permissions and notify an administrator of the incident.

MANAGE GROUP POLICIES

Windows' Resultant Set of Policies (RSoP) feature provides administrators the ability to examine the combined security and configuration settings the user will experience in their Windows environment. Active Administrator enhances this with the ability to run what-if scenarios, such as moving the user or computer to another OU or Active Directory site, or adding the user or computer to a group. Active Administrator also removes the risk that modifying a live Group Policy will have real-time negative effects on production users. With Active Administrator, Group Policies can be copied and modified offline, and analyzed with RSoP while completely safe from your production Active Directory. Finally, if you are migrating your Active Directory to a new forest or domain, Active Administrator will also replicate the policies across domain and forest boundaries, keeping all security intact.

Active Administrator's GPO Repository allows offline management of Group Policies

SCRIPTLOGIC®

ACTIVE ADMINISTRATOR™

AUDIT ACTIVE DIRECTORY AND GPO CHANGES

Active Administrator lets you stay on top of changes to Group Policy Objects and Active Directory in a delegated environment. Active Administrator centrally collects audit events from the Security event logs of all Domain Controllers, giving instant visibility of all Active Directory changes and who made them. These audit records are stored centrally in a SQL database to maintain a historic record of changes long after the event logs have been cleared, and an alerting function can send alerts whenever particular types of event occur. Active Administrator also keeps a history of GPO changes, enabling easy rollback of a Group Policy to a previous version and reporting of any changes.

FAULT TOLERANT ACTIVE DIRECTORY

Active Administrator gives administrators unprecedented Active Directory recoverability. Active Administrator's automated history of Group Policy changes and ability to backup/restore and even migrate GPOs between domains makes achieving fault tolerance through rollback of GPOs a cinch. Active Administrator's object-level backup and granular restore capabilities automatically write a record of all Active Directory objects to disk, and make it possible to selectively restore any combination of Active Directory objects and their attributes, or even the entire directory!

Active Administrator audits changes within Active Directory, providing both reporting and notification of those changes

Active Administrator provides administrators the ability to restore individual Active Directory objects.

F.A.Q.

Isn't this the same as Microsoft's GPMC?
No. Active Administrator (AD) manages GPOs and runs RSoP reports in both Windows 2000 and 2003 Server environments. Active Administrator offers a complete GPO management solution including offline GPO management, GPO rollbacks, and auditing and reporting of all AD changes. Beyond Group Policy management, Active Administrator also manages AD security, role-based delegation of AD permissions with Active Templates, and object-level restores of AD.

Does this give me an "Undo" for AD?
Yes! Now you can easily restore deleted or modified objects and rollback Group Policies to any previous version.

Is an Evaluation Available?
Yes! A fully-functional 30-day evaluation download is available at scriptlogic.com.

SYSTEM REQUIREMENTS

Installation
Active Administrator requires installation within a 2000/2003 AD Domain. The auditing component requires a SQL or MSDE database.

Management
The Active Administrator console can be installed on a Domain Controller, Member Server, or Desktop running 2000/2003/XP.

Client Support
Active Administrator can manage a Windows 2000 or Windows 2003-based AD. Restore of AD objects requires that at least oneWindows 2003 Domain Controller be present.

LICENSING

Active Administrator is licensed based on the **number of user accounts** in your Active Directory.

For pricing, contact your ScriptLogic reseller or call ScriptLogic at **1.800.813.6415** or **1.561.886.2420**