

Directory Security Administrator™

Minimizes Active Directory security risks by easing administration of permissions

Overview

NetIQ's Directory Security Administrator provides innovative Active Directory permissions management capabilities, which include powerful role-based security, auditing and advanced analysis. Its straightforward graphic interface makes it simple for you to manage, analyze, audit and modify Active Directory access control lists (ACLs). With Directory Security Administrator, you can easily manage Active Directory permissions to reduce security risks.

Solutions for Today

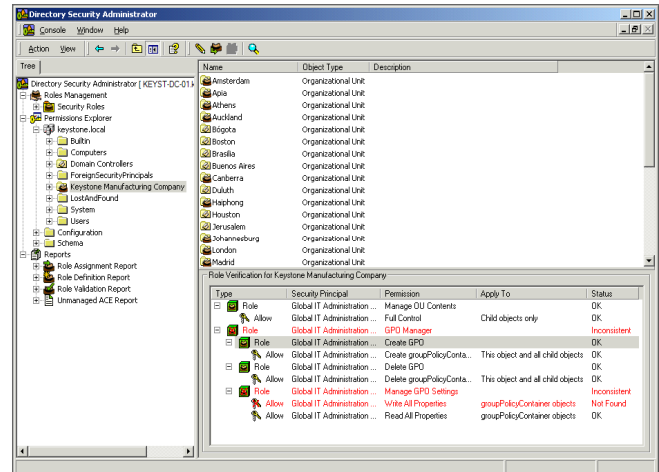
Your Active Directory security depends on your ability to carefully manage ACLs to develop and maintain an effective Active Directory security model. However, this task presents a significant challenge since defining and implementing your security model is difficult and only becomes more so over time. In a dynamic environment, determining where permissions have been granted and their sources is nearly impossible, making it extremely difficult to take the appropriate and necessary actions to fill any existing security gaps.

NetIQ's Directory Security Administrator allows you to set up your security model via role-based security capabilities. You can define privilege-level policies within Active Directory, and use its search and advanced permissions analysis to methodically audit Active Directory permissions.

Key Benefits

Improves security – Simplifies the set up and configuration of your Active Directory security model and gives you the power to assess and analyze security vulnerabilities. Directory Security Administrator simplifies the decision making about how to address security gaps.

Enables security audits – Allows you to assess security vulnerabilities within Active Directory permissions. Administrators can quickly determine where permissions in Active Directory have been granted to users, groups or machines.



Directory Security Administrator allows you to quickly and easily determine whether or not roles applied in the directory still match their definitions, enabling the enforcement of Active Directory permissions policies.

Simplifies control over permissions – Provides the ability to quickly and easily manage permissions, reducing the security exposure that permissions configuration errors may introduce. Administrators can quickly audit their permissions to verify security in Active Directory.

Reduces total cost of ownership – Lowers administrator learning curves when implementing access control for Active Directory by reducing the complexity of permissions administration.

Enables task-appropriate directory access – Reduces operational costs and enhances an organization's security posture by leveraging NetIQ's unique Layered Security Architecture (LSA). Using LSA, organizations can assign directory access options, based on needs and privilege level. The access options include native, so administrators can perform tasks within AD requiring elevated levels of privilege; protected, which gives help desk administrators access to perform tasks requiring low privilege but high automation; and offline, which allows policy administrators to perform tasks requiring testing and approval before promotion to a live environment.

Directory Security Administrator™

Technical Features

- Defines and implements security roles based on native Active Directory permissions
- Allows role definitions and application to be stored in Active Directory
- Generates audit events to identify who did what and when with role management actions
- Allows you to see and fix role definition/application discrepancies with role validation reports
- Quickly searches the directory for all objects where any given permissions have been granted to users and groups
- Enables you to determine the origin of permissions granted in Active Directory
- Supplies convenient GUIs to help you browse the directory and view the ACEs on any object
- Provides tight integration with native Active Directory management tools, reducing administrator learning curve
- Uses the same icons as native Active Directory management tools for quick object recognition
- Shows permissions for directory objects from a single interface
- Enables you to perform permissions management actions from scripts or batch files using command-line interface
- Eliminates superfluous information from displays with search filters
- Supports any existing object type, as well as any new object types created in Active Directory
- Leverages Active Directory scalability by storing role information inside the directory itself
- Provides access to various domains from a single console
- Is built using MMC technology
- Utilizes caching to ensure optimal performance

Contacts

Worldwide Headquarters

NetIQ Corporation
3553 North First Street
San Jose, CA 95134
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

NetIQ EMEA

+44 (0) 1784 454500
info@netiq.com

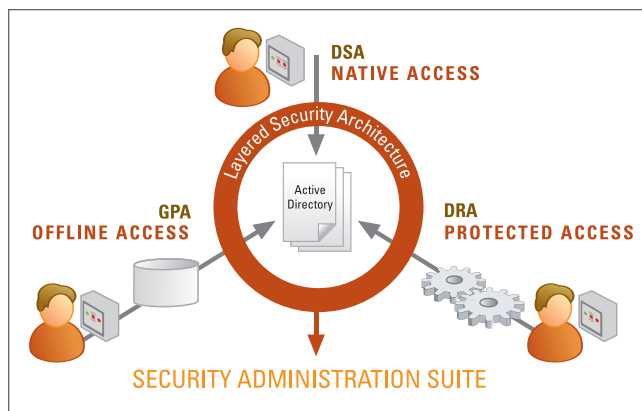
NetIQ Japan

+81 3 5909 5400
info-japan@netiq.com
www.netiq.co.jp

NetIQ Australia

& New Zealand
+61 2 9925 2100
www.netiq.com.au

For our offices in Latin America & Asia Pacific,
please visit our web site at www.netiq.com/contacts



Directory Security Administrator allows you to rapidly audit where users have been granted permissions in Active Directory. You can easily find out what permissions have been granted and determine the origin of those permissions.

System Requirements

System/Operating Requirements Hardware:

Intel platform

- 133 MHz or higher processor
- 64MB RAM minimum
- 24MB drive space minimum

System/Operating Requirements Software:

- Windows 2000 Professional Server, Advanced Server - SP2 or Windows XP Professional
- Windows .NET Server Administration Tools for Windows XP Professional