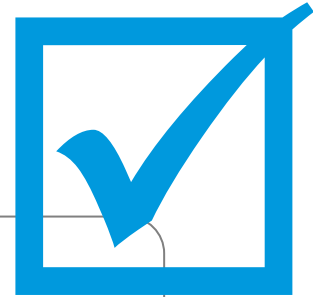


Access Rights

Reporting & Monitoring



Complete Audit Of: **User Accounts**
Access Rights
Administrative Changes
User Activity

Assess

*Automated
Audit Reporting*

- **Detailed Reporting** on any attribute including schema extensions & data that is not available in native event logs
- **Fine-Grained Filtering** enables highly relevant audit reports
- **Report Scheduling** reduces manual effort & ensures regular audits
- **Flexible Event Handling** enables selective post-processing

Inspect

*Calculated
Access Rights*

- **Comprehensive Access Rights Reporting** based on explicit permission assignments, group memberships, and inherited rights
- **File System** effective rights on files and folders
- **Directory Object** effective rights on OU's, domain objects, etc.
- **Detailed Reports** on HOW permissions are granted
- **Industry Best-Practice** reports identify direct user rights assignments and explicitly denied permissions

Monitor

*Real-Time
Event Analysis*

- **Real-Time Processing** enables alerts, policy breaches & automated remediation
- **Best-Practice** templates and policies enable quick, relevant results
- **Directory Monitoring** watches user accounts, group memberships, authentication attempts, or any object-attribute combination
- **File System Monitoring** monitors sensitive files and folders

Report

*Comprehensive
& Flexible*

- **Pre-Configured Reports** enable immediate results based on best practices & common industry requirements
- **Custom Reports** can be configured to meet special requirements
- **Personalized View** gives each user a customized report view
- **Data Export Options** enable quick export to PDF or CSV formats

Prove the effectiveness of security controls and account management processes by showing exactly who has access to what resources.

Detect inappropriate changes to accounts or access rights in real time. And get immediate alerts on inappropriate use of permissions, administrative mistakes, and other policy breaches.

Identify risk based on account profiles, access rights, and best practice assurance.

Simplify your response process and exceed audit requirements in a fraction of the time it would take to manually compile reports.

Focused
Who Has Access to What?

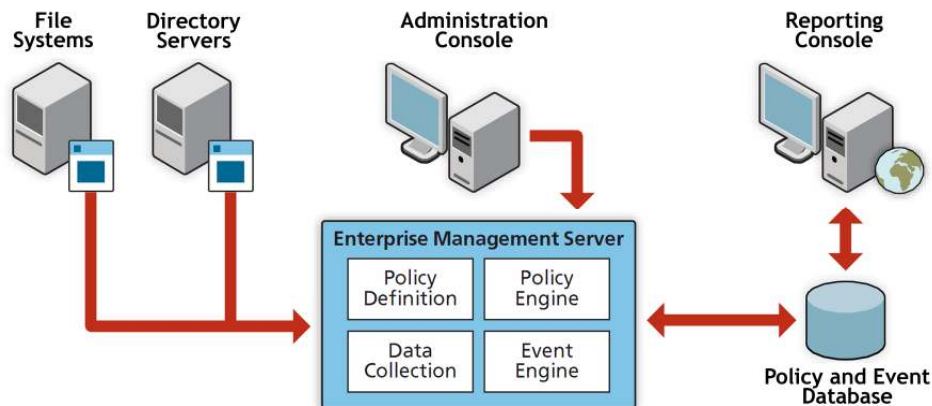
Independent
True Third Party Audit

Cross Platform
Covers Microsoft™ & Novell™
networking platforms

Simple
Easy to Use Interface
Pre-Configured Reports
Built-In Expertise



SIMON is NetVision's Managed Service removing all of the obstacles typically associated with software ownership. SIMON includes hardware, software, install & configuration, maintenance, patches, capacity planning, etc. Your data remains on-site and in your control. SIMON eliminates the operational headaches.



Founded in 1995, NetVision is a pioneer in identity & access monitoring and reporting. NetVision provides periodic assessment and real-time monitoring capabilities with superior event filtering and from-the-source data collection. NetVision is focused on providing relevant answers to critical identity & access questions across platforms on core network directories and file systems.



NetVision, Inc.
752 East 1180 South
Suite 100
American Fork, UT 84003
Phone: 1-877-828-9180

NetVision answers [Who Has Access to What?](#)

Assess

Automated Audit Reporting of User Accounts and Group Memberships

Understanding User Accounts, Attributes, and Group Memberships is a key aspect of answering audit questions about access rights.

NetVision's **Assess** capabilities enable you to report on any combination of object and attribute within the network directory.

This includes answers to common questions such as:

- What Accounts Exist?
- Which Accounts are Enabled or Disabled?
- Which Accounts are Dormant or Unused?
- Which Accounts have Specific Attributes (job titles, departments, etc.)?
- What Groups Exist?
- Which Accounts are Members of Which Groups?



Inspect

Calculated Access Rights on File System and Directory Objects

Directory and File System Access Rights are complicated to capture. Actual permissions are often granted or denied based on a combination of explicitly assigned rights, group memberships, inherited rights, and denied rights.

NetVision's **Access Rights Inspector** enables you to get detailed answers on Access Rights across your directory and file system. Flexible reporting is available based on a combination of selections:

<u>Principals</u>	<u>Resources</u>	<u>Format</u>	<u>Permissions</u>
User(s) or Group(s)	Files & Folders or Directory Objects	Table View or Tree View	View, Write, Execute, Delete, etc.

Report Types Include:

- **Effective Rights:** Reports on calculated rights accounting for group memberships, inheritance, direct assignments, and other factors.
- **Explicit Rights:** Reports on individual permission assignments.
- **Direct User Assignments:** Reports on instances where a user account has been granted access directly to a resource.
- **Deny Entries:** Reports on instances of explicitly denied permissions.
- **Group Memberships:** Reports on group membership assignments.

Real-Time Monitoring enables Continuous Audit.

Monitor

Automated Audit Reporting of User Accounts and Group Memberships

One of NetVision's core capabilities is real-time monitoring of access rights, administrative changes, and user behavior.

Data is collected directly from the source for immutable, non-repudiable, and complete information sets. Events are filtered and analyzed in real time to ensure extremely high relevance in reports and alerts.

Some of the activities that NetVision Monitors include:

- Account Creations
- Account Deletions
- Account Status Changes
- Account Attribute Changes
- Group Membership Changes
- File or Folder Permission Changes
- File or Folder Property Changes
- User Authentications
- User File or Folder Activity

NetVision provides extremely powerful and flexible tools to specify which events are important to your organization. This ensures highly **relevant information** and prevents mountains of useless data.

Once events have been identified and filtered, NetVision **takes action** by recording the event, initiating a task, or sending an alert.



3-Phase Process

1. Event Collection

From-the-source collection ensures **accurate & reliable** information.

Fine-grained filtering ensures **relevant** results.

2. Real-Time Event Analysis

Once filtered, events are checked against policies in real time for **optimal security & comprehensive audit** records

3. Flexible Event Processing

Based on policy, selected events can be written to a database or file, sent in an alert, or can initiate an external process

NetVision Event Filtering

Event Filtering can be configured to include or exclude any combination of the following:

Event Type	Day or Time	Server	Domain	Tree Location	Operator
Object Type	Selected Object(s)	Affected Attribute(s)		Success/Fail Status	

NetVision provides Quick Access to Flexible Answers.

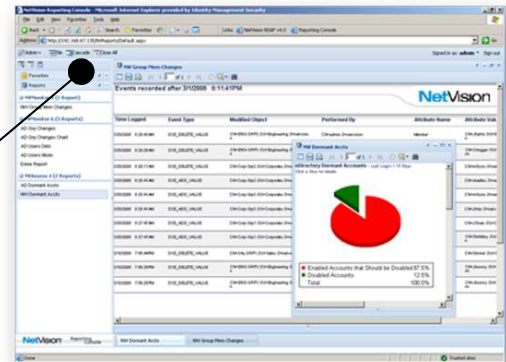
Report

Automated Audit Reporting of User Accounts and Group Memberships

NetVision's Reporting Console provides a single point of access for audit and monitoring information across network directories and file systems. The console is flexible enough to accommodate various report types and charts or graphs when appropriate.

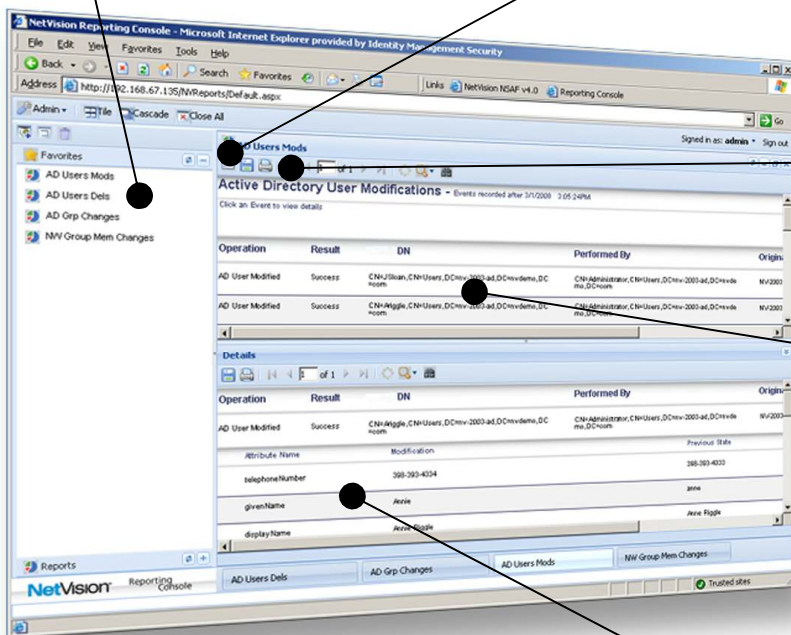
NetVision provides commonly used report templates upon installation and also incorporates unique customer requirements to meet each organization's specific reporting needs.

A button on the Reporting Console opens NetVision's Access Rights Inspector giving immediate access to explicit rights assignments and calculated effective rights for both file system and directory object permissions.



Favorites enable quick-access to a user's most frequently used reports.

Report parameters provide an additional layer of flexibility to accommodate specific requirements or temporary reporting needs.



Report information can be exported to PDF or XLS formats.

Reports provide critical information such as the event type and result, object DN, who the operation was performed by, the originating server, and when the event occurred.

Many reports provide a detail pane that offers additional information such as affected attributes and before and after values.

NetVision has spent more than a decade building expertise.
With SIMON, we've **Perfected its Delivery.**

SIMON

Managed Service Delivery

NetVision delivers monitoring and reporting of access rights with none of the typical hassles associated with traditional software solutions.

Managed Service

- Virtually Touchless Deployment
- Lower Cost vs. Traditional Software
- Zero Configuration & Administration
- No Pre-Requisite Knowledge, Expertise, or Training Required
- Data Stays Securely On-Site
- No Hardware Requirement
- Unaffected by Staff Changes

Built-In Expertise

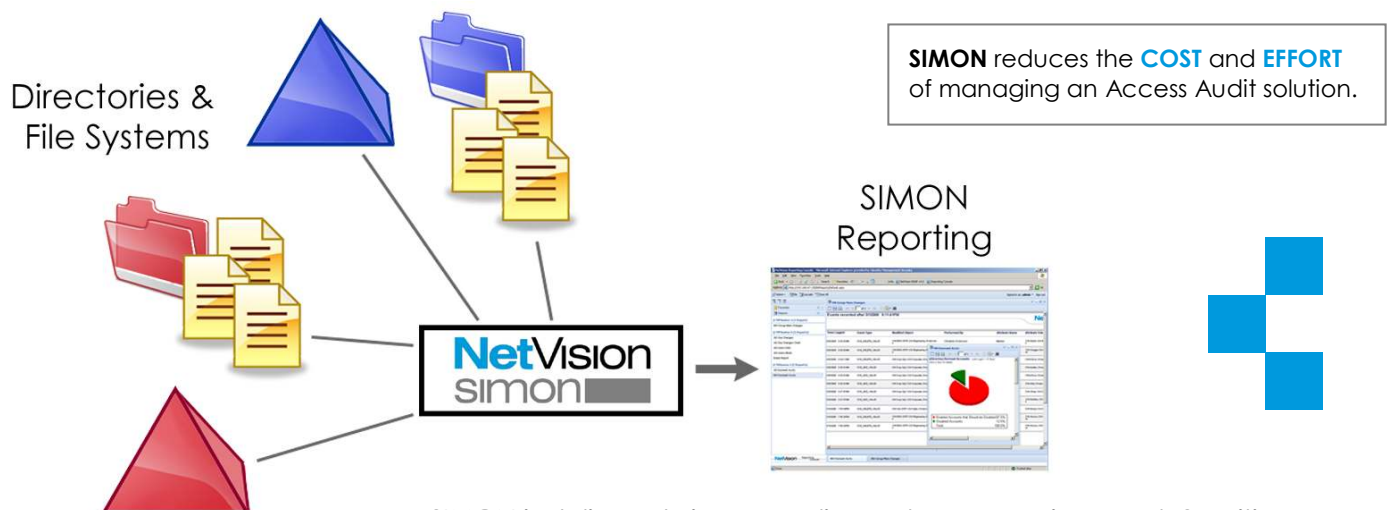
- Best-Practice Policies and Reports are Pre-Configured
- System Watches Critical Events and Knows When to Alert
- Real-Time Policy Validation and Remediation Tasks
- Eliminates Manual Log Analysis
- Immediate ROI

Superior Technology

- Advanced Event Filtering Ensures Relevant Results
- From-The-Source Data Collection Generates Irrefutable Evidence
- Independent of System Logs and Vendors for True Third-Party Audit
- Easy-to-Use Reporting Interface
- Captures Information That Is Otherwise Unavailable

SIMON Includes:

- ✓ Application Software
- ✓ Required Hardware
- ✓ Hardware Maintenance
- ✓ OS License, Install, Configuration, and Security Hardening
- ✓ Supporting Software Licenses, Install, and Configuration
- ✓ Capacity Planning
- ✓ Setup and Configuration of Best-Practice Policies, Filters, and Reports
- ✓ Immediate Updates to New Reports, Templates & Policies Over Time
- ✓ Touch-Free Upgrades
- ✓ Health Monitoring
- ✓ On-Going Optimization
- ✓ Support for Software Diagnosis & Repair
- ✓ Support for Hardware Diagnosis & Repair
- ✓ Guaranteed Availability of Trained Staff



SIMON is delivered via an appliance to your environment. Sensitive security information remains within your network and in your control.