Software

Ensuring enterprise visibility, auditing, and reporting for Windows environments

Written by Susan Olsen and the Dell team

Introduction

Systems and security administrators are tasked with achieving and proving IT compliance and security, supporting Active Directory migrations, and reporting on the configuration of Active Directory, Windows file servers and SQL servers across the enterprise. On a daily basis, they must field questions like:

- Who can do what in Active Directory?
- Who has administrative access to Windows servers and workstations?
- Who has access to what printers, shares, folders, files and SQL databases?
- How my servers are configured, including general computer information, network settings, services running, installed programs and custom registry keys?
- How does the configuration of my servers change over time? What local users and groups exist on every server, and what is the membership of each group?

With manual approaches, answering these questions is a Herculean, error-prone task that introduces the risk of security breaches and compliance failures. Instead, administrators need a tool that enables them to take a proactive approach, allowing them to easily identify and report on who has access to what files, folders and shares, and on what servers. And they need a solution that is scalable, secure and customizable to support large and complex Windows environments with multiple groups of report consumers.

Dell™ Enterprise Reporter delivers that functionality, and more. This technical brief explains how Enterprise Reporter makes it easy to perform tasks such as security assessments, Active Directory pre- and post-migration analysis, and configuration change auditing. Let's begin by looking more closely at the specific challenges facing systems and security administrators today.

The challenges

Achieving, maintaining and proving compliance with regulations and policies

Many organizations today are subject to federal and industry compliance regulations, such as PCI, HIPAA and SOX. And every organization should have internal best practices to help ensure the security of the network, applications and data. Both internal and external regulations change over time, and new policies are often added at an alarming rate.

Systems and security administrators need to achieve and maintain compliance with these regulations year-round, as well as prove that compliance on a regular basis. Therefore, they need complete visibility into configuration across the entire network, including:

- How each server is configured
- What software is installed on each server
- What local users and groups are present on each server, as well as the membership of each group
- What logins exist on each SQL Server database

A lack of easy and accurate insight into these details makes achieving and proving compliance difficult, and can result in compromised security that may go unnoticed until a breach occurs.

However, getting that insight into every aspect of server configuration can be a challenge. Windows servers today have very complicated and complex architectures, with thousands of settings that can influence security and compliance. Each type of server—file, SQL, Active Directory, Exchange—has its own set of settings that must be analyzed. For example, administrators need to understand and control the set of roles on each SQL Server to determine who can access each database on the server. More broadly, they must understand and carefully control who has administrative access to each server because those users can potentially violate security policies.

To ensure compliance and security across the enterprise, administrators need visibility into both current configuration settings and the history of the changes to those settings.

In addition, administrators must ensure that only the appropriate software is installed on each server, and that each application is installed properly, in order to avoid security vulnerabilities. In fact, a complete and accurate software inventory for a server must include not only applications, but also hot fixes and operating system updates, which strongly impact security. Therefore, administrators need an effective, efficient way to ensure that each server is up-to-date.

Ensuring security

As we have seen, to ensure compliance and security across the enterprise, administrators need visibility into both current configuration settings and the change history. Permissions, in particular, create a grave security concern for administrators that must be able to control and monitor who has access to what shares, folders and files on all file servers and network filers. They also need to understand how those permissions change over time.

Unfortunately, the complexities of the native Microsoft access management system make it difficult to understand who has access to what resources. For example, to determine who has access to a given resource, you need to know which users are members of which groups—not only the direct group membership, but also the nested group membership. You also need to factor in all the complications of permissions, including both direct permissions and inherited permissions. You need to know who the owner of each resource is, and how Group Policy is configured.

Understanding who has access to what is further complicated by the enormous volume of data organizations have today—often tens of millions of files spread out across a network of hundreds or thousands of servers. Investigating the access rights of just a single user takes a great deal of time. Multiply that by tens of thousands of users that companies have today, and it’s easy to understand why it's almost impossible to ensure security without appropriate tools. Moreover, manually checking permissions can easily result in errors or omissions, which could spell a security violation. And manually reviewing users and their privileges prevents IT from focusing on core business priorities.

Performing migrations, consolidations or restructuring

Migrations, consolidations and restructuring offer opportunities for organizations to simplify their environments, take advantage of new technologies, and ensure the success of mergers and acquisitions. The first step in any such project is to assess the current environment in a pre-migration analysis. This analysis needs to reveal what assets are in the current environment and how those assets are currently used so that only the data and accounts that are actually needed will be migrated, leaving behind anything that is no longer used. An accurate analysis shortens the migration process, helping the organization meet its deadlines. Moreover, it delivers a cleaner and more effective target environment.

A complete pre-migration analysis of your current environment should reveal information like:

- The number of domains, users, and groups
- Users that have never logged on and can be excluded from the migration
- Users that have not logged on during the past 30 days, and might be able to be excluded from migration
- The permissions each user has on each server, so you can migrate groups of users and resources together in batches to honor dependencies between users and resources
- Conflicts that might arise during migration, such as naming conflicts between the source and target domains, so you can avoid unpredictable system state issues in the target environment

Of course, after the migration, administrators need to be able to determine whether the new environment meets expectations, including confirmation that users have continued appropriate access to needed resources.

Reporting

Underlying all of the preceding needs is the need for easy, accurate and complete reporting—not only for IT administrators, but also for a wide variety of other consumers, such as auditors, management, legal staff and the human resources department. Being able to easily get the right reports in the right format for each consumer streamlines processes, reduces costs, and improves security and compliance.

Reporting is a challenge for several reasons. The first is the sheer volume of data that organizations have today. Moreover, that data is often widely dispersed across systems and databases; effective reporting requires that it be collected somehow and stored in a centralized location. In addition, running reports manually is time-consuming and error-prone; organizations need an automated reporting process, with options such as delivery through email on schedule.

Most importantly, the challenge is security—ensuring that users can view only the data they should be allowed to view. For example, help desk staff should have access to reports on account lockouts, but not to financial or sales reports.

> Being able to easily get the right reports in the right format for each consumer streamlines processes, reduces costs, and improves security and compliance.

Native tools do not provide the 360-degree visibility administrators need into the current system configurations and user permissions.

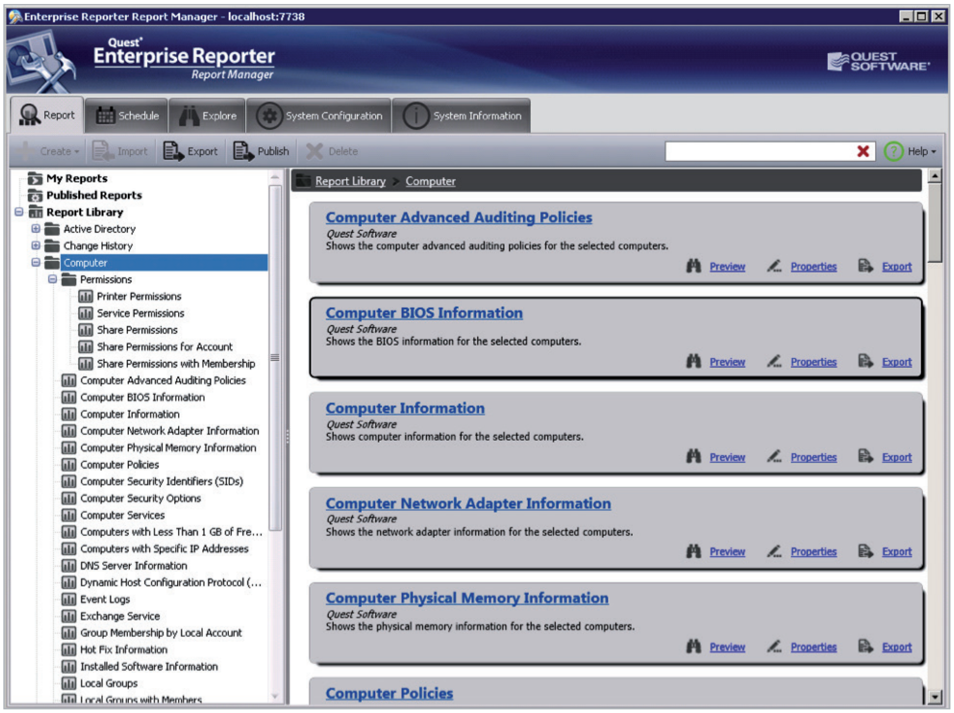
Native solutions for Active Directory, NTFS and SQL Server

Unfortunately, native tools do not enable systems and security administrators to effectively handle these challenges of achieving compliance, ensuring security, performing migrations and enabling flexible reporting. Challenges with native tools include:

- **The inefficiency of having to use multiple tools**—The first major problem with native tools is simply that there are a lot of them, so you have to switch between multiple consoles to access the different parts of your environment. To manage Exchange, you use a console called Exchange System Manager; for Active Directory, you use Active Directory Users and Computers snap-in; for file servers, you must launch Windows Explorer. Administrators must learn all the different tools, install and maintain them, and spend time switching between them to do their jobs.
- **Getting visibility requires time-consuming (and error-prone) manual effort**—Native tools do not provide the 360-degree visibility administrators need into the current system configuration and user permissions. Instead, administrators must dig through multiple screens in a manual and error-prone effort to find the information they need. For instance, in order to understand where a particular user has access, not only do you have to run multiple tools, but you also have to do a lot of manual analysis. This basically means going through the entire file system and opening the Permissions tab one at a time for every folder or file to see where the user has access. That process eats up time of IT staff that could be better spent on other projects. And the process is also error-prone, which puts the organization at risk of security and compliance failures.
- **With no friendly user interface, automation requires scripting**—Native tools offer no built-in automation whatsoever. Administrators can automate certain tasks using PowerShell scripts—if they have the right skills and training. But even if they do have those skills, automating processes still requires a great deal of work. For example, administrators must create many separate scripts to create the multiple reports required to satisfy a compliance requirement, or to get visibility into what resources each user has access to.
- **Lack of flexible reporting leaves many report consumers hanging**—Getting reports using native tools is a tedious, manual process. Moreover, understanding the data the native tools provide often requires skills and knowledge the report consumer may not have. For example, help desk staff might not know a lot about how file servers or Active Directory works, so they cannot be expected to dig through low-level data; like many report consumers, they need a more convenient representation of the raw data.
- **No built-in compliance reports makes it hard to satisfy auditor requests**—Native tools have no built-in expertise; they don't help you know what needs to be collected and reported on to comply with external regulations or security best practices. Therefore, organizations either need to provide training to keep staff up-to-date on regulations, or hire an external consultant to provide that expertise. Then they need to spend time and effort creating the appropriate reports for auditors.
- **Native solutions do not scale well**—Finally, because of the drawbacks listed above, native solutions simply cannot scale to environments of any size and complexity. With large volumes of data across multiple systems and thousands of users accessing a wide variety of resources, organizations simply cannot afford manual, error-prone processes for compliance, security, migrations and reporting.

Enterprise Reporter

Instead of native tools, organizations need a solution that enables administrators, security officers and help desk staff to easily collect, store and report on information about their Active Directory, Windows file servers and SQL servers. The solution should be scalable and provide automation to reduce workload and improve accuracy. And it should be flexible and secure to support large and complex Windows environments with multiple groups of report consumers. Enterprise Reporter delivers that functionality, and more.


Enterprise Reporter Report Manager - localhost:7738
Quest®
Enterprise Reporter
Report Manager
QUEST SOFTWARE®
Report
Schedule
Explore
System Configuration
System Information
Create
Import
Export
Publish
Delete
Help
My Reports
Published Reports
Report Library
Active Directory
Change History
Computer
Permissions
Printer Permissions
Service Permissions
Share Permissions
Share Permissions for Account
Share Permissions with Membership
Computer Advanced Auditing Policies
Computer BIOS Information
Computer Information
Computer Network Adapter Information
Computer Physical Memory Information
Computer Policies
Computer Security Identifiers (SIDs)
Computer Security Options
Computer Services
Computers with Less Than 1 GB of Fre…
Computers with Specific IP Addresses
DNS Server Information
Dynamic Host Configuration Protocol (…
Event Logs
Exchange Service
Group Membership by Local Account
Hot Fix Information
Installed Software Information
Local Groups
Local Groups with Members
Report Library > Computer
Preview
Properties
Export

Computer Advanced Auditing Policies
Quest Software
Shows the computer advanced auditing policies for the selected computers.

Computer BIOS Information
Quest Software
Shows the BIOS information for the selected computers.

Computer Information
Quest Software
Shows computer information for the selected computers.

Computer Network Adapter Information
Quest Software
Shows the network adapter information for the selected computers.

Computer Physical Memory Information
Quest Software
Shows the physical memory information for the selected computers.

Computer Policies

Figure 1. Enterprise Reporter provides unparalleled visibility into the configuration of critical IT assets.

Ultimate visibility into the security and configuration of your servers—plus built-in expertise

With Enterprise Reporter, you gain 360-degree visibility into the configuration of your critical IT assets within Active Directory domains, SQL servers, Windows file servers and NAS devices, enabling you to meet the requirements of security best practices, internal policies and compliance regulations.

Enterprise Reporter knows exactly what data needs to be collected across your environment, automates that data collection, and presents the information in easy-to-understand formats. In fact, Enterprise Reporter includes a library of close to 200 predefined reports, each containing critical expertise. For example, the solution includes reports tailored for each type of server, so you get the information you need to meet security best practices and relevant compliance regulations.

Security through real-time access assessment

With Enterprise Reporter, you can easily determine who has access to what resources, identify users with inappropriate access, and ensure that access is provided on a "business-needs-to-know" basis. To deliver that insight, Enterprise Reporter agents deployed on your Windows file servers build a real-time index of permissions for each user. When you need to investigate permissions, you no longer need to bring up a Permissions dialog on each server and manually compile the results. Instead, you can go to Enterprise Reporter's real-time access assessment, which pulls in the indexed data from the agents and consolidates it for you, providing a convenient, complete and real-time view of user permissions across the entire network. All the complexities discussed earlier, such as nested group membership and permission inheritance, are automatically factored in, so you can quickly see where a user has access.

Enterprise Reporter offers a secure, scalable solution that enables administrators to easily assess who has access to what resources, and deliver reports to consumers across the organization.

With Enterprise Reporter, you can easily determine who has access to what resources, identify users with inappropriate access, and ensure that access is provided on a "business-needs-to-know" basis.

Pre-migration and post-migration analysis

Enterprise Reporter helps ensure a smooth domain migration or consolidation project by helping you inventory what needs to be migrated in the planning phase, and then verifying that the migration was completed as planned. The solution includes predefined reports for each step of the pre-migration planning process—you can quickly inventory your users, groups, resources and permissions to plan more effectively.

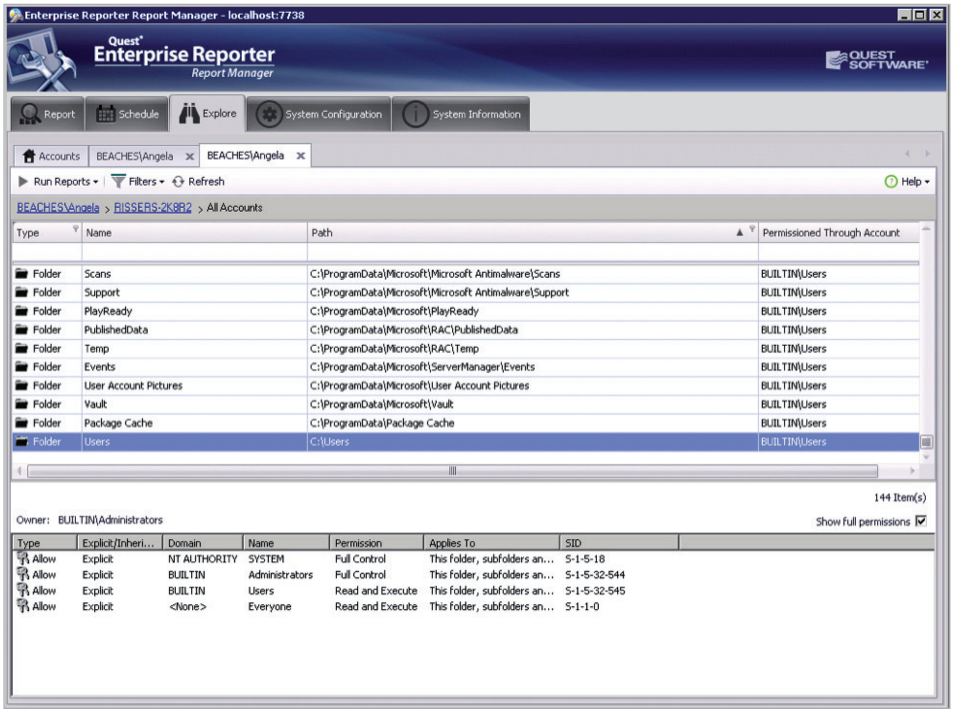
For example, with Enterprise Reporter you can run a report showing all users who did not log in for the past 30 days, a report on user accounts that are disabled, and a report listing all groups that are empty. Armed with that information, you can clean up your source environment before the migration project starts, meet your migration timeline more easily, and enjoy a target environment that is easier to understand and manage.

Enterprise Reporter also includes reports that compare users and groups in two or more domains to identify naming conflicts. With that report, you can create an account matching map that can be used as input for a migration tool, such as Dell™ Migration Manager, to resolve the conflicts during the migration process.

Change review

To further improve compliance and minimize the risk of business disruptions due to unnoticed and unwanted changes, Enterprise Reporter also enables you to easily implement a change review process. Enterprise Reporter captures the historical configuration of Active Directory, Windows file servers and SQL Servers, and provides reports that detail all changes to:

- Group membership
- Active Directory domains
- Computer configuration
- NTFS files, folders or shares
- Registry keys or values
- SQL servers or databases



Type	Name	Path	Permissioned Through Account
Folder	Scans	C:\ProgramData\Microsoft\Microsoft Antimalware\Scans	BUILTIN\Users
Folder	Support	C:\ProgramData\Microsoft\Microsoft Antimalware\Support	BUILTIN\Users
Folder	PlayReady	C:\ProgramData\Microsoft\PlayReady	BUILTIN\Users
Folder	PublishedData	C:\ProgramData\Microsoft\RAC\PublishedData	BUILTIN\Users
Folder	Temp	C:\ProgramData\Microsoft\RAC\Temp	BUILTIN\Users
Folder	Events	C:\ProgramData\Microsoft\ServerManager\Events	BUILTIN\Users
Folder	User Account Pictures	C:\ProgramData\Microsoft\User Account Pictures	BUILTIN\Users
Folder	Vault	C:\ProgramData\Microsoft\Vault	BUILTIN\Users
Folder	Package Cache	C:\ProgramData\Package Cache	BUILTIN\Users
Folder	Users	C:\Users	BUILTIN\Users

Owner: BUILTIN\Administrators

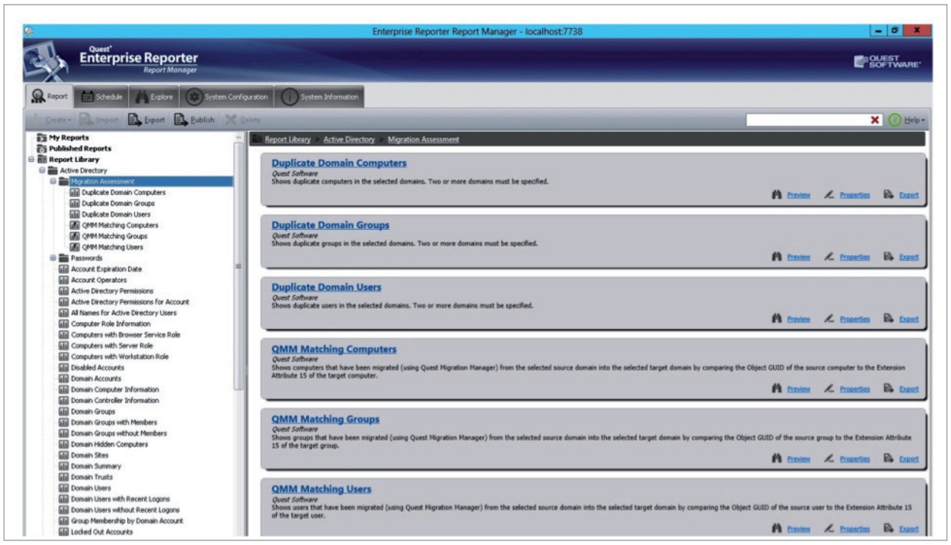
Type	Explicit/Inheri...	Domain	Name	Permission	Applies To	SID
Allow	Explicit	NT AUTHORITY	SYSTEM	Full Control	This folder, subfolders an...	S-1-5-18
Allow	Explicit	BUILTIN	Administrators	Full Control	This folder, subfolders an...	S-1-5-32-544
Allow	Explicit	BUILTIN	Users	Read and Execute	This folder, subfolders an...	S-1-5-32-545
Allow	Explicit	<None>	Everyone	Read and Execute	This folder, subfolders an...	S-1-1-0

Figure 2. With Enterprise Reporter's real-time access assessments, you can quickly determine who has access to what.

Flexible, automated reporting

- Automated reporting workflows—Enterprise Reporter delivers a fully automated workflow. You can automate report generation and delivery for multiple report consumers according to different schedules. This feature ensures auditors, help desk staff, IT managers and others can get the reports they requested in a format they understand. Reports will be delivered by email or uploaded to a file share, according the needs of the audience.
- Customizable reports—Enterprise Reporter includes an easy-to-use report designer that makes it easy to customize the predefined reports or to create new reports to meet the unique informational needs of your organization. Granular control enables you to customize nearly every aspect of report appearance. Advanced filtering ensures you present exactly the information that's needed. You can also choose from a wide variety of formats, including PDF, HTML, MHT, RTF, XLS, XLSX, CSV, text and images.
- Common reporting portal—Enterprise Reporter is integrated with the Dell Knowledge Portal, a reporting interface that unifies reporting from the entire Dell family of compliance solutions. These solutions include ChangeAuditor™,

Enterprise Reporter helps ensure a smooth domain migration or consolidation project by helping you inventory what needs to be migrated in the planning phase, and then verifying that the migration completed as planned.



My Reports
Published Reports
Report Library
Active Directory
Migration Assessment
Duplicate Domain Computers
Duplicate Domain Groups
Duplicate Domain Users
QMM Matching Computers
QMM Matching Groups
QMM Matching Users
Passwords
Account Expiration Date
Account Operators
Active Directory Permissions
Active Directory Permissions for Account
All Names for Active Directory Users
Computer Role Information
Computers with Browser Service Role
Computers with Server Role
Computers with Workstation Role
Disabled Accounts
Domain Accounts
Domain Computer Information
Domain Controller Information
Domain Groups
Domain Groups with Members
Domain Groups without Members
Domain Hidden Computers
Domain Sites
Domain Summary
Domain Trusts
Domain Users
Domain Users with Recent Logons
Domain Users without Recent Logons
Group Membership by Domain Account
Locked Out Accounts

Duplicate Domain Computers
Quest Software
Shows duplicate computers in the selected domains. Two or more domains must be specified.
Preview Properties Export

Duplicate Domain Groups
Quest Software
Shows duplicate groups in the selected domains. Two or more domains must be specified.
Preview Properties Export

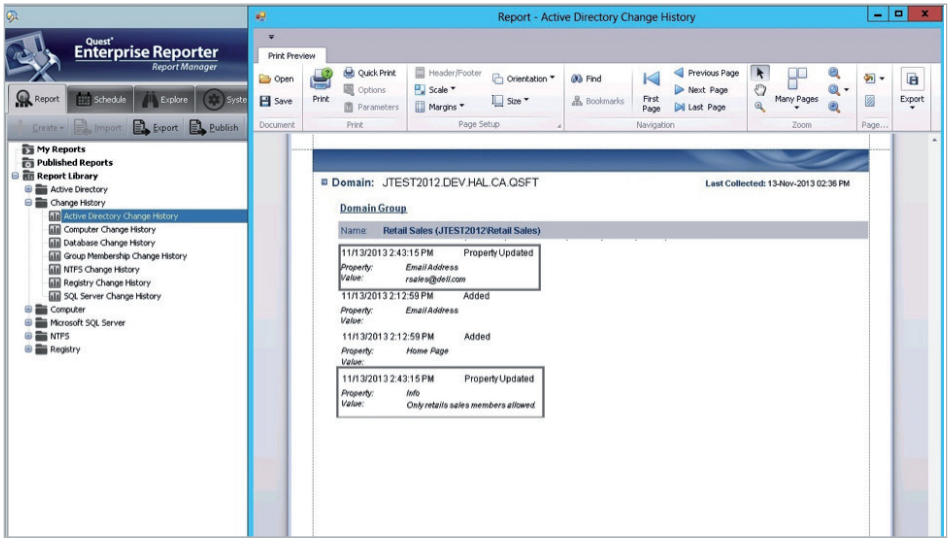
Duplicate Domain Users
Quest Software
Shows duplicate users in the selected domains. Two or more domains must be specified.
Preview Properties Export

QMM Matching Computers
Quest Software
Shows computers that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source computer to the Extension Attribute 15 of the target computer.
Preview Properties Export

QMM Matching Groups
Quest Software
Shows groups that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source group to the Extension Attribute 15 of the target group.
Preview Properties Export

QMM Matching Users
Quest Software
Shows users that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source user to the Extension Attribute 15 of the target user.
Preview Properties Export

Figure 3. Pre-migration planning is easy with Enterprise Reporter.



My Reports
Published Reports
Report Library
Active Directory
Change History
Active Directory Change History
Computer Change History
Database Change History
Group Membership Change History
NTFS Change History
Registry Change History
SQL Server Change History
Computer
Microsoft SQL Server
NTFS
Registry

Domain: JTEST2012.DEV.HAL.CA.QSFT — Last Collected: 13-Nov-2013 02:36 PM

Domain Group

Name: Retail Sales (JTEST2012\Retail Sales)

11/13/2013 2:43:15 PM Property Updated
Property: *Email Address*
Value: *rsales@dell.com*

11/13/2013 2:12:59 PM Added
Property: *Email Address*
Value:

11/13/2013 2:12:59 PM Added
Property: *Home Page*
Value:

11/13/2013 2:43:15 PM Property Updated
Property: *Info*
Value: *Only retails sales members allowed*

Figure 4. Change history reporting minimizes business disruption due to unplanned changes.

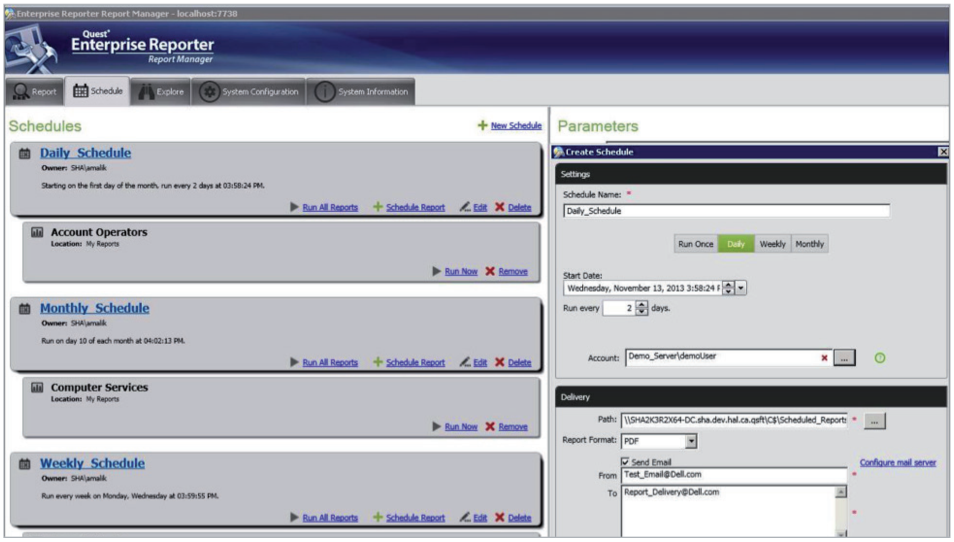
Enterprise Reporter delivers a fully automated workflow.

InTrust™ and ActiveRoles™ Server and other products. The Knowledge Portal helps you achieve, maintain and prove compliance with regulations such as HIPAA, PCI and SOX and others. Dell's compliance report packs build a mapping between the requirements of compliance regulations and specific reports provided by different products, making it easier for you to prove compliance to your auditors.

- The Knowledge Portal can also be used as a delegation tool, enabling you to delegate access to certain reports to various people. For instance, help desk operators can be delegated access only to a handful of reports related to account lockouts. Moreover, access can be restricted even further to honor departmental boundaries. For example, department managers can review only permissions of users and groups they directly manage.

Scalable data collection

Enterprise Reporter scales to environments of any size and geographic distribution. You can schedule collections during off-peak hours to minimize the impact to network and server performance, as well as leverage its distributed collection architecture for load balancing. For



Daily_Schedule
Owner: SHA\amalik
Starting on the first day of the month, run every 2 days at 03:58:24 PM.

Account Operators
Location: My Reports

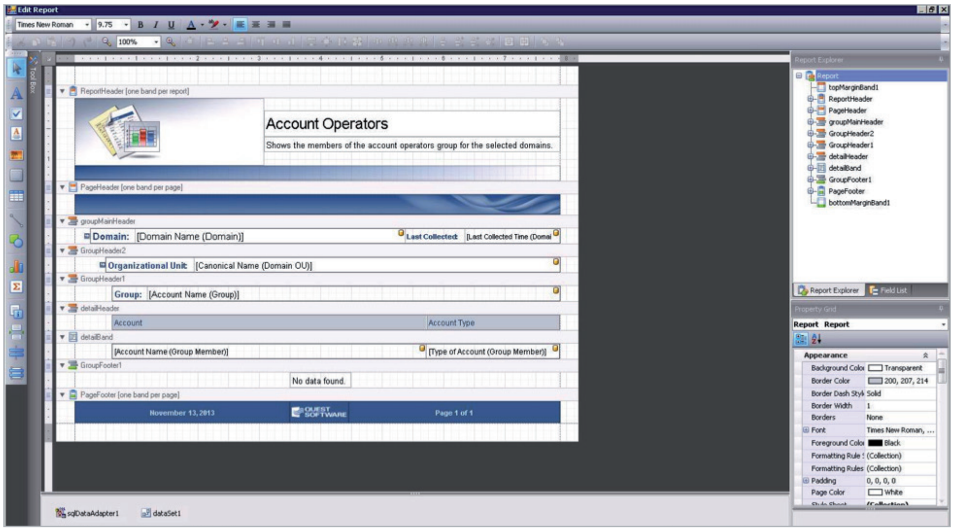
Monthly_Schedule
Owner: SHA\amalik
Run on day 10 of each month at 04:02:13 PM.

Computer Services
Location: My Reports

Weekly_Schedule
Owner: SHA\amalik
Run every week on Monday, Wednesday at 03:59:55 PM.

Schedule Name: * Daily_Schedule
Start Date: Wednesday, November 13, 2013 3:58:24 F
Run every 2 days.
Account: Demo_Server\demoUser
Path: \\SHA2K3R2X64-DC.sha.dev.hal.ca.qsft\C$\Scheduled_Report: *
Report Format: PDF
☑ Send Email
From Test_Email@Dell.com *
To Report_Delivery@Dell.com *

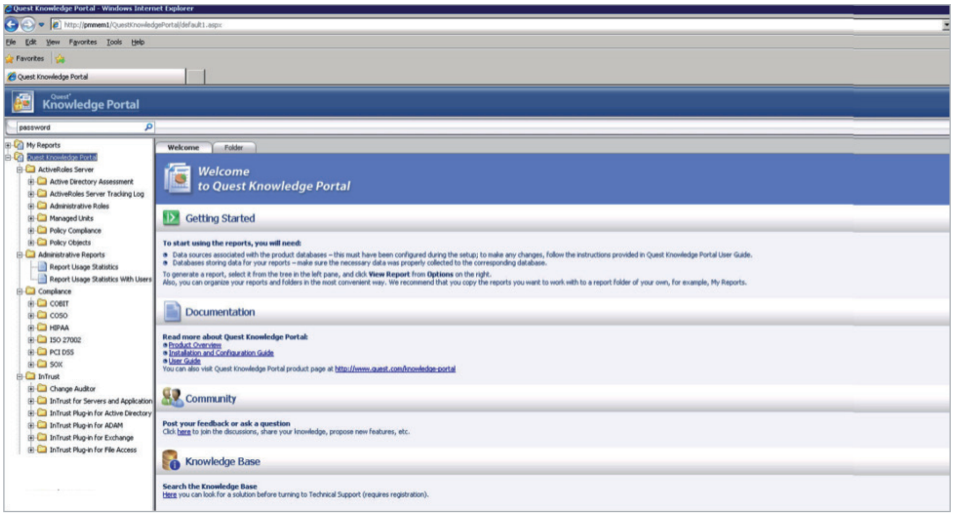
Figure 5. Set up report generation and delivery schedules for individuals or groups of report consumers.



Account Operators
Shows the members of the account operators group for the selected domains.
Domain: [Domain Name (Domain)] Last Collected: [Last Collected Time (Domai
Organizational Unit [Canonical Name (Domain OU)]
Group: [Account Name (Group)]
Account | Account Type
[Account Name (Group Member)] [Type of Account (Group Member)]
No data found.
November 13, 2013 Page 1 of 1

Background Colo	Transparent
Border Color	200, 207, 214
Border Dash Styl	Solid
Border Width	1
Borders	None
Font	Times New Roman, ...
Foreground Colo	Black
Formatting Rule :	(Collection)
Formatting Rules	(Collection)
Padding	0, 0, 0, 0
Page Color	White

Figure 6. It's easy to customize reports to meet your needs.


Quest Knowledge Portal - Windows Internet Explorer
http://pmmem1/QuestKnowledgePortal/default1.aspx
File Edit View Favorites Tools Help
Favorites
Quest Knowledge Portal
Quest Knowledge Portal
password
My Reports
Quest Knowledge Portal
ActiveRoles Server
Active Directory Assessment
ActiveRoles Server Tracking Log
Administrative Roles
Managed Units
Policy Compliance
Policy Objects
Administrative Reports
Report Usage Statistics
Report Usage Statistics With Users
Compliance
COBIT
COSO
HIPAA
ISO 27002
PCI DSS
SOX
InTrust
Change Auditor
InTrust for Servers and Application
InTrust Plug-in for Active Directory
InTrust Plug-in for ADAM
InTrust Plug-in for Exchange
InTrust Plug-in for File Access
Welcome
Folder

Welcome
to Quest Knowledge Portal

Getting Started

To start using the reports, you will need:

- Data sources associated with the product databases – this must have been configured during the setup; to make any changes, follow the instructions provided in Quest Knowledge Portal User Guide.
- Databases storing data for your reports – make sure the necessary data was properly collected to the corresponding database.

To generate a report, select it from the tree in the left pane, and click **View Report** from **Options** on the right.
Also, you can organize your reports and folders in the most convenient way. We recommend that you copy the reports you want to work with to a report folder of your own, for example, My Reports.

Documentation

Read more about Quest Knowledge Portal:
- Product Overview
- Installation and Configuration Guide
- User Guide

You can also visit Quest Knowledge Portal product page at http://www.quest.com/knowledge-portal

Community

Post your feedback or ask a question
Click here to join the discussions, share your knowledge, propose new features, etc.

Knowledge Base

Search the Knowledge Base
Here you can look for a solution before turning to Technical Support (requires registration).

Figure 7. Consolidate data into a single pane of glass for reporting across Dell compliance solutions.

example, if you have a highly distributed environment, you can create multiple clusters consisting of nodes that are co-located with the data to be collected, and that can be invoked on an ad hoc basis in response to an increasing or decreasing workload. That approach speeds up data collection and minimizes network traffic to the central database where the data is consolidated.

Efficient storage

As discussed, Enterprise Reporter stores all the data it collects in a central database. To minimize storage requirements, the solution compares collections and stores only the changes detected between them. For example, in a scenario where data collection is scheduled to run every week, the first collection will establish a set of data in the database. When subsequent collections run, Enterprise Reporter will compare the newly collected data with what is already stored in the database, and save only those items that have changed. Saving only the changes rather than a complete new version of the data reduces storage requirements tremendously.

Conclusion

To meet compliance regulations, ensure security, and support migrations and consolidations, IT administrators need quick and accurate insight into the configuration of Active Directory, Windows file servers and SQL servers across the enterprise. Native tools are simply not up to the task in today's large and complex organizations. Enterprise Reporter offers a secure, scalable solution that enables administrators to easily assess who has access to what resources. Plus, it delivers reports to consumers across the organization to get the information they need in a secure, automated, flexible fashion. For more information, please visit http://software.dell.com/products/enterprise-reporter/

Enterprise Reporter is integrated with the Dell Knowledge Portal, a reporting interface that unifies reporting from the entire Dell family of compliance solutions.

For More Information

© 2013 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

Dell Software: Delivering complete and connected solutions

Dell Software empowers organizations of all sizes to experience Dell's "power to do more" by delivering scalable yet simple-to-use solutions that can increase productivity, responsiveness and efficiency. Dell Software is uniquely positioned to address today's most pressing business and IT challenges with holistic, connected software offerings across five core solution areas, encompassing data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, helps customers simplify IT, mitigate risk and accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.