



ENTERPRISE SECURITY REPORTER™ FOR SQL SERVER

Enterprise Security Reporter™ for SQL Server is an agent-less, fast, comprehensive reporting solution for Microsoft SQL Server that collects information on SQL databases, objects, permissions, users and roles. Pre-defined reports compile, query and analyze this data to give administrators a complete view of the security and integrity of their entire SQL Server environment.

Analyzing and reporting on the security of SQL Servers is a complex task with no easy solutions. Growing regulatory compliance requirements and the increasing number of attacks from both inside and outside the corporate network make security management and reporting a critical part of database administration. Since each database application can have very different access requirements, it's all too easy to leave unexpected security holes in your database infrastructure.

Enterprise Security Reporter for SQL Server focuses on enterprise-wide SQL Server security reporting. Using a fast, agent-less discovery system, ESR can collect vast amounts of information on SQL databases, objects, schemas, permissions, users and roles. ESR provides a powerful analysis engine that creates understandable, comprehensive reporting on all aspects of SQL Server security.

EASY, FAST AND THOROUGH REVIEWS OF SQL SERVER SECURITY

ESR's discovery engines remotely collect security information from SQL Servers and store it in a database for analysis and reporting. Servers, instances, and databases can be selected for individual discovery. The discovery console gives administrators complete control over defining discovery jobs, viewing job status and results across any number of discovery engines.

This data is then presented in reports that include:

- Database and object listings
- Database object and schema permissions
- Database user and server logins
- Database and server role memberships

SECURITY LIFECYCLE MAP

Assess	Assign	Audit
	Accessibility	
	Accountability	
	Assurance	

<http://www.scriptlogic.com/slm>

KEY BENEFITS

Simplified Security Reporting

Centralized consoles allow for scheduling automated collection and reporting of security data. Results can also be emailed directly to necessary recipients making reporting on your enterprise an easy task.

Assists with Compliance

Proactive maintenance and reporting on access controls helps meet the requirements of regulatory and best practice standards.

Enhances Windows Security

Find weaknesses, over-exposed files, over privileged users and complete security audits in a fraction of the time.

KEY FEATURES

Pre-defined SQL Server Reports

Over a dozen pre-defined reports provide a detailed look at your entire SQL Server environment including SQL databases, objects, schemas, permissions, users and roles.

Distributed Discovery Servers

Placing discovery servers at remote sites further increases the speed of discovery and collection and reduces WAN traffic. Easily manage all discovery servers from a single screen.

Report Customization

Using the Report Composer, reports can be built using a simple wizard, without needing to know SQL statements. Those familiar with SQL can directly edit queries, if desired.

Ad-Hoc Query Builder

Quickly and easily build queries for any security data with a step-by-step, drag and drop query builder. Save and schedule queries and export results to Microsoft Excel for further analysis. Query settings can now be imported directly into the Report Composer making custom report creation easier than ever.

Automated Report Delivery

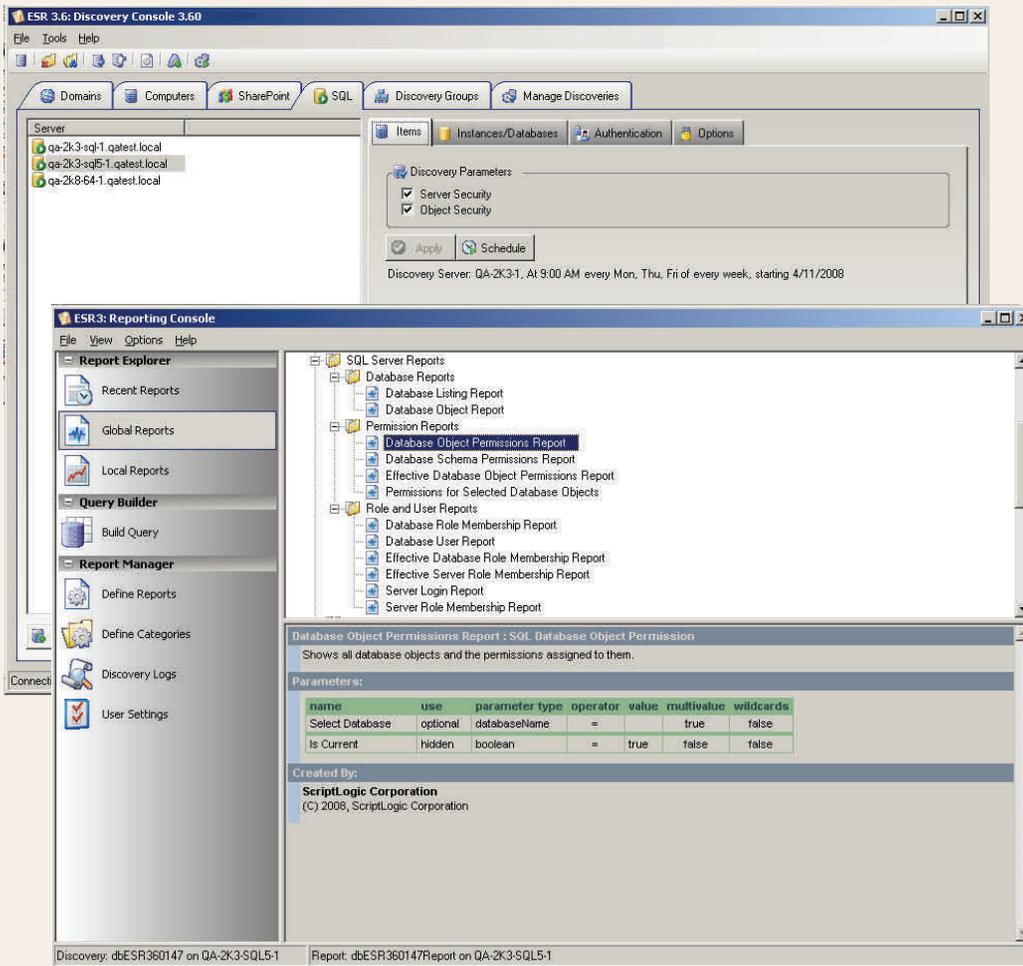
Reports can be scheduled and emailed via any SMTP-based email system. Delta Reports can now be scheduled to run the last two discoveries to see the latest changes.

Enterprise Security Reporter offers comprehensive discovery and reporting on SQL Server database and object security and role memberships.

The screenshot shows the ESR 3.60 Discovery Console interface. The main window displays a table of Discovery Servers with columns for Server Name, Status, Version, Max Jobs, Running, Database, and Service. Below this is a 'Current Discovery Job Queue' table with columns for Path, Type, Status, Elapsed, and Priority. On the right side, a 'Discovery Jobs' panel is open, showing a table of scan results for a job named '3/28/2008 - 8:06 AM [Finished] (current)'. The table has columns for Object Type, Scan Count, and Discover Count.

Object Type	Scan Count	Discover Count
Instances	1	1
Databases	49	49
Logins	19	19
Server Roles	8	8
Sv Role Members	6	6
DB Users	287	287
DB Roles	584	584
Role Members	139	139
Schemas	682	682
Tables	1195	287
Views	1053	1053
Synonyms	0	0
SP's	5849	5849
Functions	276	276
Assemblies	0	0
Permissions	12220	273

ENTERPRISE SECURITY REPORTER FOR SQL SERVER



Enterprise Security Reporter for SQL Server makes it easy to select specific SQL Servers, include or exclude any instance or database and discover exactly the information you need. Over a dozen pre-defined SQL Server reports give you comprehensive information on your SQL databases, objects, schemas, permissions, and role membership.

F.A.Q

How does reporting help with compliance?

Regulatory and best practice standards such as HIPAA, SOX, ITIL and ISO 17799 require the auditing of access and security controls. The ready-made reports supplied in Enterprise Security Reporter address many of these requirements, and custom reporting can focus on specific aspects of compliance.

Can Enterprise Security Reporter for SQL Server show me who has effective access to my databases?

Yes! Enterprise Security Reporter will determine the Windows group and database role memberships for a given account. These group memberships are then used to determine the effective access the account has to databases and individual objects within those databases.

What formats do reports come in?

Acrobat (PDF), RTF, CSV, HTML, TXT, TIF.

Is an evaluation available?

Yes! A 30-day evaluation download is available at scriptlogic.com.

SYSTEM REQUIREMENTS

Discovery Console

Enterprise Security Reporter's Discovery Console can be installed on Windows 2000, 2003, 2008, XP and Vista operating systems and requires MSDE, SQL Server Express, SQL Server 2000 or 2005.

Discovery Agents

Discovery Agents can be installed on Windows 2000, 2003, 2008, XP and Vista operating systems.

Reporting Console

Enterprise Security Reporter's Reporting Console can be installed on Windows 2000, 2003, 2008, XP and Vista operating systems.

Client Support

Enterprise Security Reporter can discover information on all versions of Windows NT, 2000, 2003, 2008, XP and Vista operating systems; as well as NT domains and Windows 2000, 2003, and 2008 Active Directory domains.

LICENSING

Enterprise Security Reporter is licensed on a **per-server** basis.

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

SQL: Database Object Permissions Report

4/7/2008 10:20:13 AM

Instance Name	Database Name
QA-2K3-SQL5-1	
MSSQLSERVER	
dbESR300Report	
Function	
dbo.GetCategoryPath	Grant ESR3_Report, Grant ESR3_Report
dbo.GetDBVersion	Grant ESR3_Report, Grant ESR3_Report
StoredProc	
dbo.AddCategory	Grant ESR3_Report,
dbo.AddReportDefinition	Grant ESR3_Report,
dbo.DeleteCategory	Grant

SQL: Database Role Membership Report

4/7/2008 10:28:01 AM

Instance Name	Database Name
QA-2K3-SQL5-1	
MSSQLSERVER	
ActiveAdministrator500	
Role: AA_Admin_Role	AA_Administrator
Role: AA_User_Role	AA_User
Role: db_owner	dbo
dbActiveAdmin	
Role: AA_Admin_Role	AA_Admin
Role: AA_User_Role	AA_User
Role: db_owner	dbo
dbESR300	

SQL: Database Object Permissions Report

4/14/2008 4:58:41 PM

Instance Name	Database Name
Effective Permissions for Account:	
QATest Service (qasvc@qatest.local)	
QA-2K8-64-1	Discovery Date: 3/28/2008 8:25:16 AM
SQLEXPRESS	Version: 9.00.3042.00
dbESR360110	
Function	
dbo.EffectiveGroupMembersForAccount	Grant \QA-2K8-64-1\ESR3_Administrator Select
dbo.ExpandedGroupMembersForAccountID	Grant \QA-2K8-64-1\ESR3_Administrator Select
dbo.ExpandedGroupMembersForAccountLookupID	Grant \QA-2K8-64-1\ESR3_Administrator Select
dbo.GetAllNTFSUnderNTFS	Grant \QA-2K8-64-1\ESR3_Administrator Select
dbo.GetAllPathsUnderPath	Grant \QA-2K8-64-1\ESR3_Administrator Select