



ENTERPRISE SECURITY REPORTER[®]

VERSION 3

ScriptLogic[®]

Enterprise Security Reporter[™]

VERSION 3

Installation Guide



A QUEST SOFTWARE COMPANY

Copyright © 2011 by ScriptLogic Corporation All rights reserved.

This publication is protected by copyright and all rights are reserved by ScriptLogic Corporation. It may not, in whole or part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from ScriptLogic Corporation. This publication supports Enterprise Security Reporter 3.x. It is possible that it may contain technical or typographical errors. ScriptLogic Corporation provides this publication “as is,” without warranty of any kind, either expressed or implied.

ScriptLogic Corporation

6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

1.561.886.2400

www.scriptlogic.com

Trademark Acknowledgements:

Enterprise Security Reporter is a registered trademark of ScriptLogic Corporation in the United States and/or other countries.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

DOCUMENTATION CONVENTIONS

Typeface Conventions

Bold Indicates a button, menu selection, tab, dialog box title, text to type, selections from drop-down lists, or prompts on a dialog box.

CONTACTING SCRIPTLOGIC

ScriptLogic may be contacted about any questions, problems or concerns you might have at:



ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742



561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support



561.886.2499 Fax



www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search Frequently Asked Questions, for the answers to the most common non-technical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

Contents

INTRODUCTION 1

INSTALLING ENTERPRISE SECURITY REPORTER 3

 MINIMUM REQUIREMENTS 4

 UPGRADING ENTERPRISE SECURITY REPORTER 5

What's New?..... 5

Back Up Your Files 5

Database Upgrade..... 5

 INSTALLING THE DISCOVERY CONSOLE 5

 INSTALLING THE REPORTING CONSOLE..... 9

 STARTING ENTERPRISE SECURITY REPORTER 13

Applying a License File 13

Evaluating the Product..... 14

 CREATING THE DISCOVERY AND REPORTING DATABASES 14

 INSTALLING THE DISCOVERY ENGINE 17

 PORTS AND PROTOCOLS USED BY ENTERPRISE SECURITY REPORTER 18

Changing the Default TCP Port 18

 CONNECTING TO THE DISCOVERY DATABASE..... 19

 CONFIGURING THE REPORTING CONSOLE FOR NON-ADMINISTRATIVE USERS 20

 OPTIONAL REGISTRY SETTINGS 21

 WHERE TO GO NEXT 21

TROUBLESHOOTING 22

 DISCOVERY ENGINE FAILS AFTER THE UPGRADE..... 22

 Removing the Discovery Engine 22

 DISCOVERY ENGINE SERVICE MARKED FOR DELETION 22

 SETTING THE FREQUENCY OF DISCOVERY STATUS UPDATES..... 22

 UNLOCKING THE DISCOVERY CONSOLE 23

 UNINSTALLING THE DISCOVERY ENGINE 23

DBESR3 DATABASE SCHEMA 24

 COMPUTER DISCOVERY OBJECTS..... 24

 DOMAIN DISCOVERY OBJECTS 25

 ACCOUNT OBJECTS 26

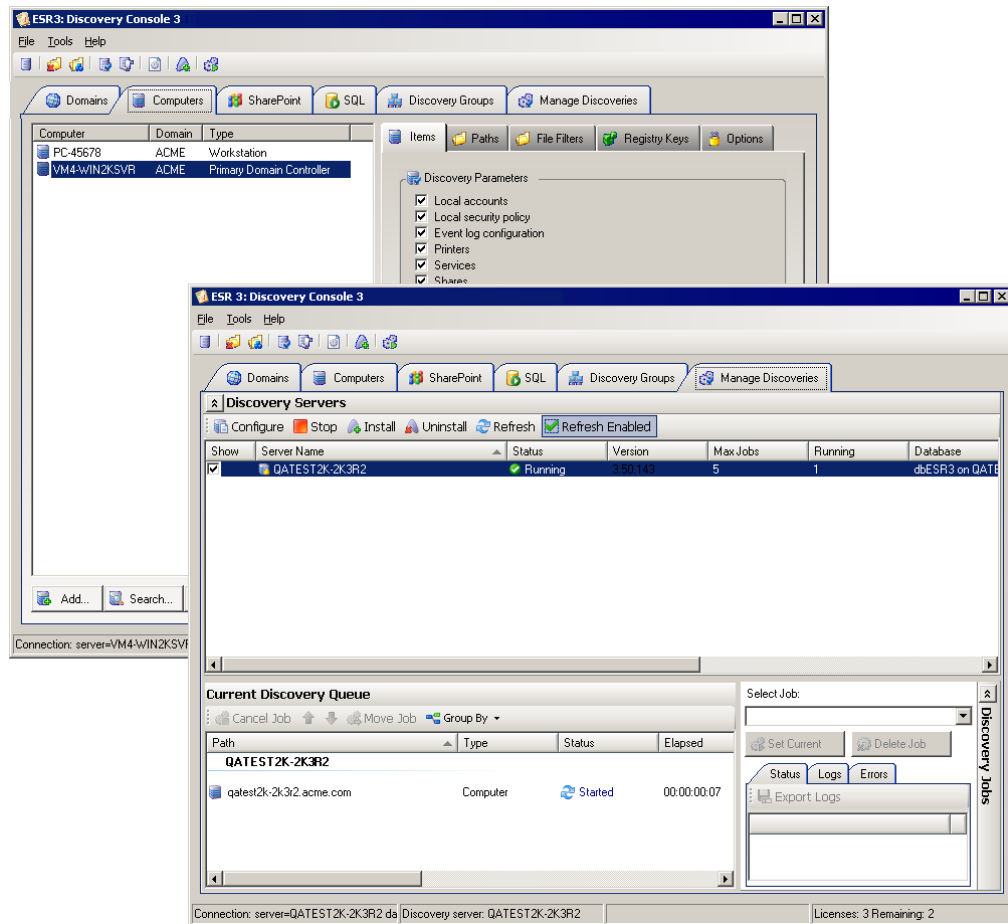
 SHAREPOINT DISCOVERY OBJECTS 27

 SQL DISCOVERY OBJECTS 28

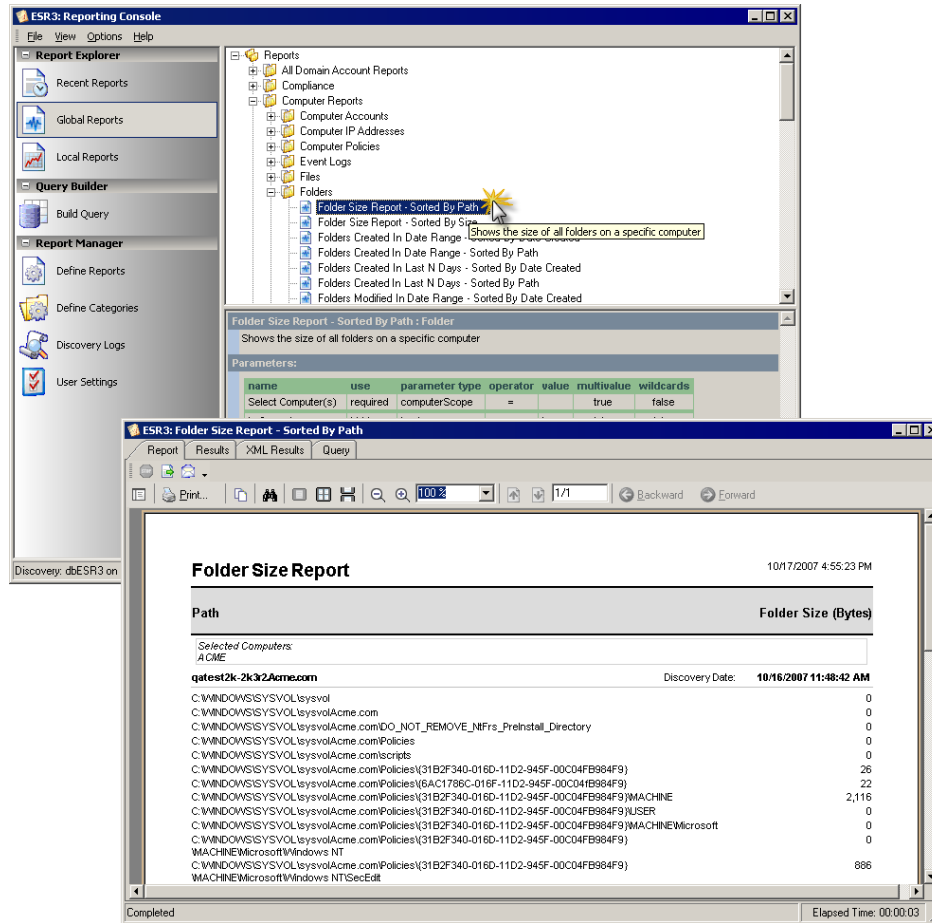
Introduction

Enterprise Security Reporter™ is an agent-less, fast, comprehensive discovery and reporting solution for analyzing file security, group memberships and other security settings on Windows file servers, Active Directory servers, SharePoint servers, and SQL Servers.

Enterprise Security Reporter retrieves and stores data on NTFS permissions, security policies, user accounts, group memberships, Active Directory, SharePoint and SQL Server security.



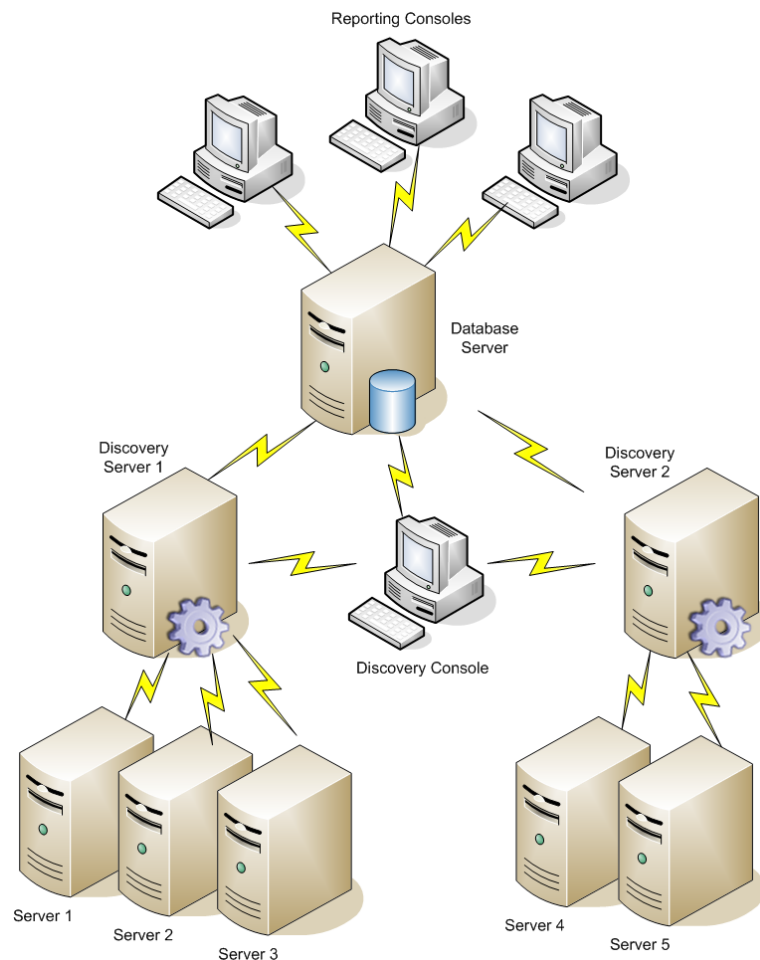
Enterprise Security Reporter also provides the administrator with tools to compare, analyze, query and report on the security and configuration of the network. Enterprise Security Reporter includes numerous ready-made and customizable reports, with output in eight popular file formats.



Installing Enterprise Security Reporter

Enterprise Security Explorer is flexible in that you can create a simple system by installing the entire package on one server to discover and report on the servers on your network, or you can create a more complex system to manage the discovery process. Take some time to map out how you want your system to operate to maximize efficiency.

In this example, Discovery Server 1 can discover Server 1, Server 2, Server 3, and itself. Discovery Server 2 can discover Server 4, Server 5, and itself. The Discovery Console controls the discovery of Discovery Servers 1 and 2. The Database Server contains the discovery and reporting databases. The Reporting Consoles connect to the Database Server to run reports.



MINIMUM REQUIREMENTS

Discovery Console

Enterprise Security Reporter's Discovery Console can be installed on Windows XP/2003/2008/2008 R2/Vista/7 and requires SQL Express 2005/2008 or SQL Server 2000/2005/2008/2008 R2.

Discovery Engines

Discovery Engines can be installed on Windows XP/2003/2008/2008 R2/Vista/7.

Reporting

Enterprise Security Reporter's Reporting Console can be installed on Windows XP/2003/2008/2008 R2/Vista/7.

Client Support

Enterprise Security Reporter can discover information on Windows NT/XP/2000/2003/2008/2008 R2/Vista/7 operating systems, NT domains, and Windows 2000/2003/2008 Active Directory.

Important: While the Discovery Console does not support Windows NT® 4.0 or Windows 2000, you can still discover computers on those operating systems. There are no hardware limitations on the computers you can discover. MSDE can handle the discovery of 1 domain, up to 20 computers, and up to 2 million files.

Supported Versions of SharePoint for Enterprise Security Reporter

- Microsoft Office SharePoint Server 2007
 - Windows SharePoint Services 3.0
- Microsoft SharePoint Server 2010
 - SharePoint Foundation 2010

Hardware

The computers on which you install the Discovery Console and Discovery Engine, must meet the following minimum criteria.

- Intel®Pentium® 4 or higher processor
- 1.5 GHz or higher
- 512 MB RAM
- 50 MB free hard disk space for installation
- 2 GB free hard disk space for the discovery and reporting databases

The computers on which you install the Reporting Console, must meet the following minimum criteria.

- Intel®Pentium® 4 or higher processor
- 1.5 GHz or higher
- 512 MB RAM
- 50 MB free hard disk space for installation

UPGRADING ENTERPRISE SECURITY REPORTER

What's New?

To see what is new in Enterprise Security Reporter 3, please see article **Q13442: *Enterprise Security Reporter 3.x Version History***, which you can access at: <http://www.scriptlogic.com/support/Products/ESR/>

Back Up Your Files

As with all software installations, it is recommended that you back up your files before installing the new software. The simplest way to back up your files is to navigate to the directory on the server where Enterprise Security Reporter is installed. Press CTRL-A to select all files in this folder. Press CTRL-C to copy the files to the clipboard. Create a new folder and press CTRL-V to paste these files into this new backup folder.

Database Upgrade

Enterprise Security Reporter 3 checks the version of your databases against the version of the software installed and automatically upgrades the databases if necessary.

INSTALLING THE DISCOVERY CONSOLE

If you have not yet done so, please download the latest version of Enterprise Security Reporter at the following link: <http://www.scriptlogic.com/support>

Note: You may be prompted to restart the computer following installation of Enterprise Security Reporter. If you are running Microsoft SQL Server 2000, exit the application now or when prompted during the installation process.

1. Double-click the **ESR3Setup_DiscoveryConsole.msi** file. If you are upgrading, double-click the **ESR3Setup_DiscoveryConsoleUpgrade.msi** file.

Note: If you do not have Microsoft .NET Framework 3.5 installed, a message box appears. To install Microsoft .NET Framework 3.5, make sure you are connected to the Internet, and then click **Yes**. When the install completes, you are prompted to reboot. Restart the install process for the Discovery Console.

The **Welcome** box appears.

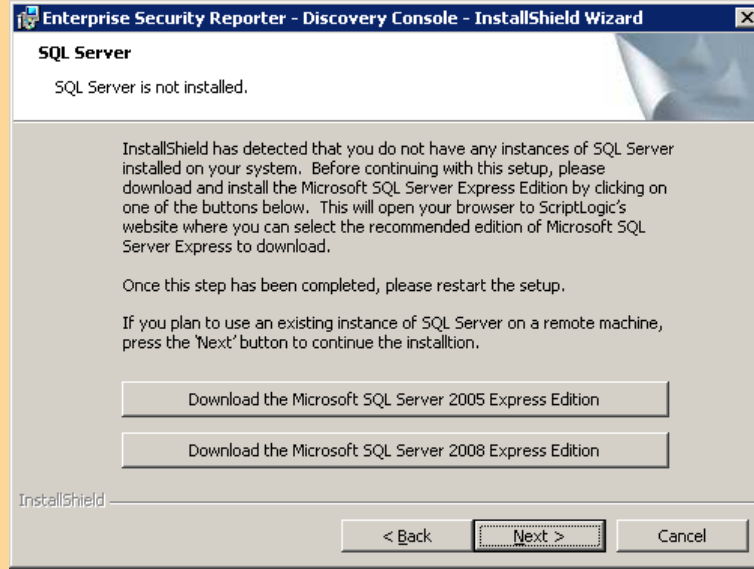


2. Click **Next**. The **License Agreement** dialog box appears.

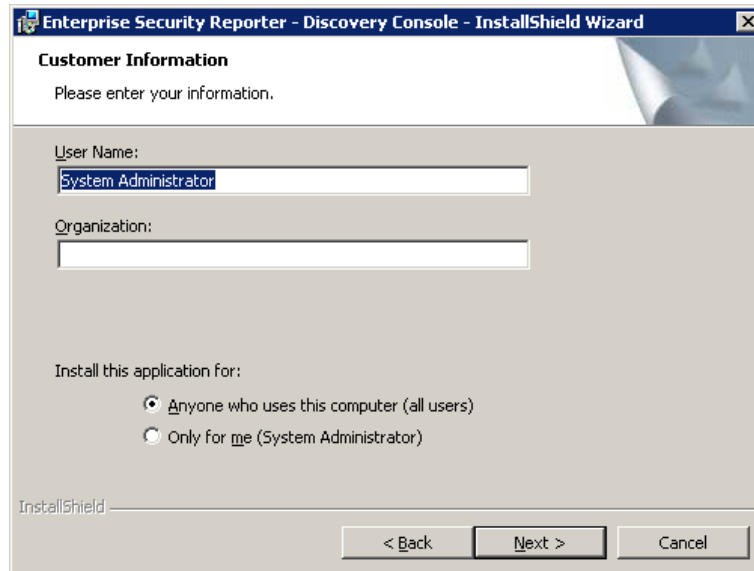


Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or at the time of purchase or evaluation.

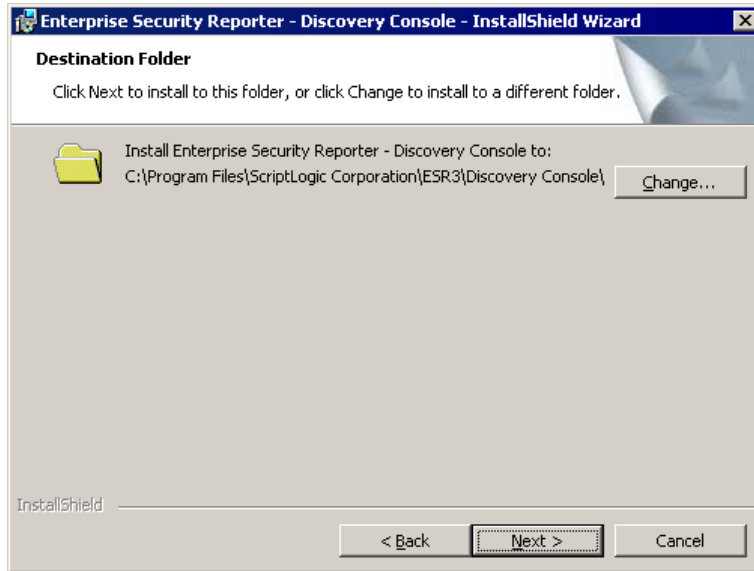
Note: If SQL Server is not detected, a message box displays prompting you to download and install Microsoft SQL Server 2005 Express Edition or Microsoft SQL Server 2008 Express Edition. When the install is complete, restart the Enterprise Security Reporter Server install process.



3. Select **I accept the terms in the license agreement**, and then click **Next**. The **Customer Information** page appears.

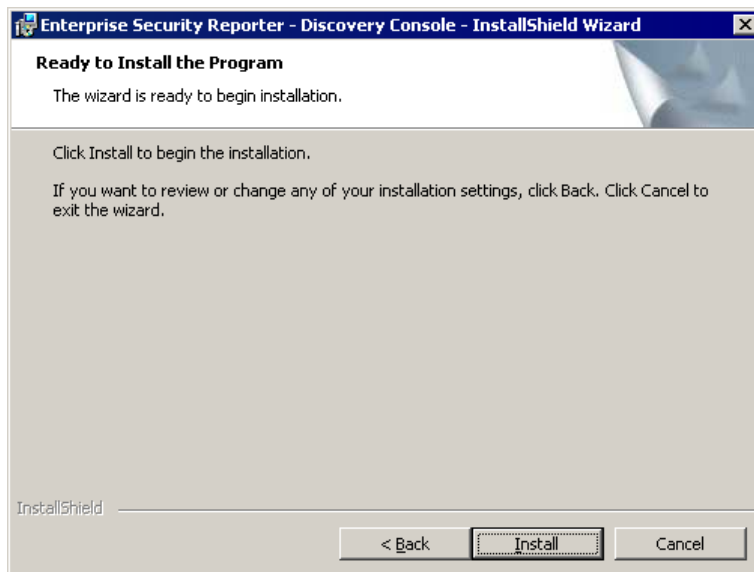


4. Select who can use the application, and then click **Next**. The **Destination Folder** dialog box appears.



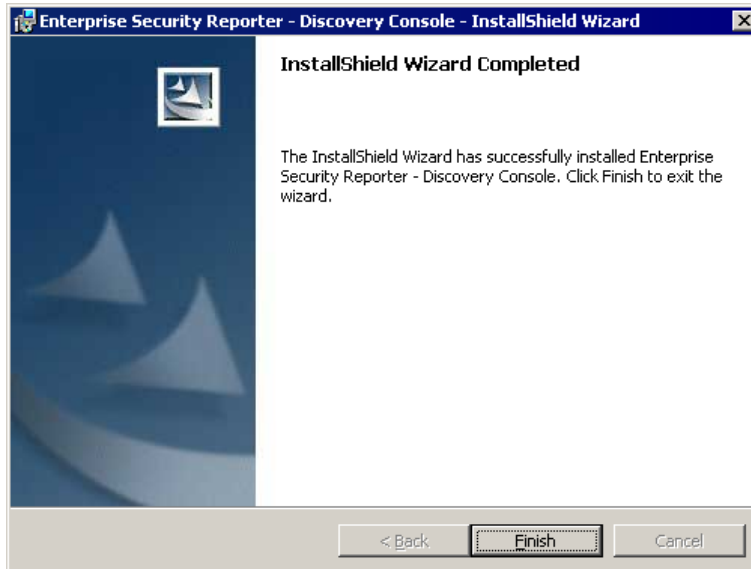
- If you want to change the installation destination, click **Change**, and then select a new location.

5. Click **Next**. The **Ready to Install the Program** box appears.



6. Click **Install**. As the install progresses, a message box displays.

When the installation is complete, the **InstallShield Wizard Completed** box appears.



7. Click **Finish**.

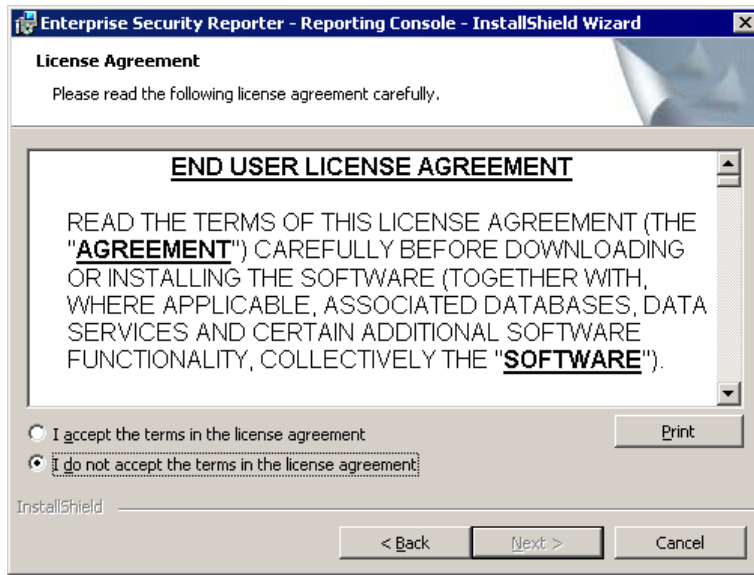
INSTALLING THE REPORTING CONSOLE

You can install the Reporting Console on any computer in your network.

1. Double-click the **ESR3Setup_ReportingConsole.msi** file. The **Welcome** box appears.



2. Click **Next**. The **License Agreement** box appears.

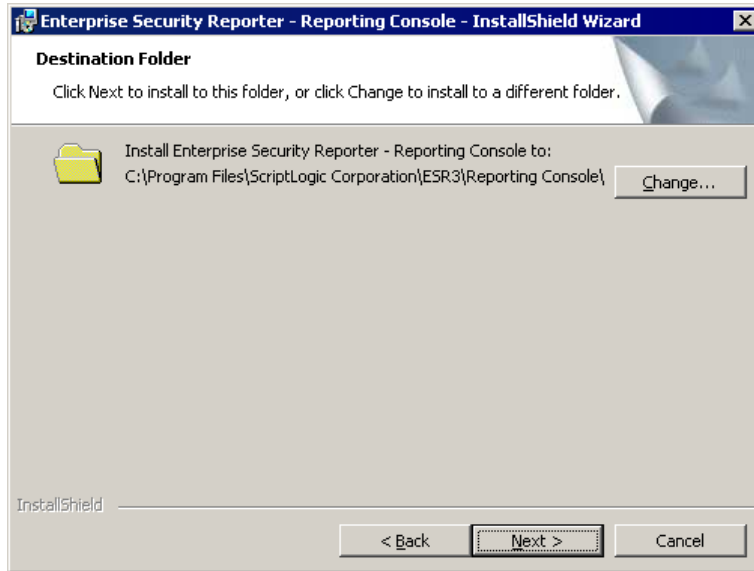


Note: You must accept the terms of the license agreement in order to continue with the installation. The software may also be governed by other applicable laws and copyrights not specifically enumerated in the license agreement, or as dictated by supplemental documentation included with the product or at the time of purchase or evaluation.

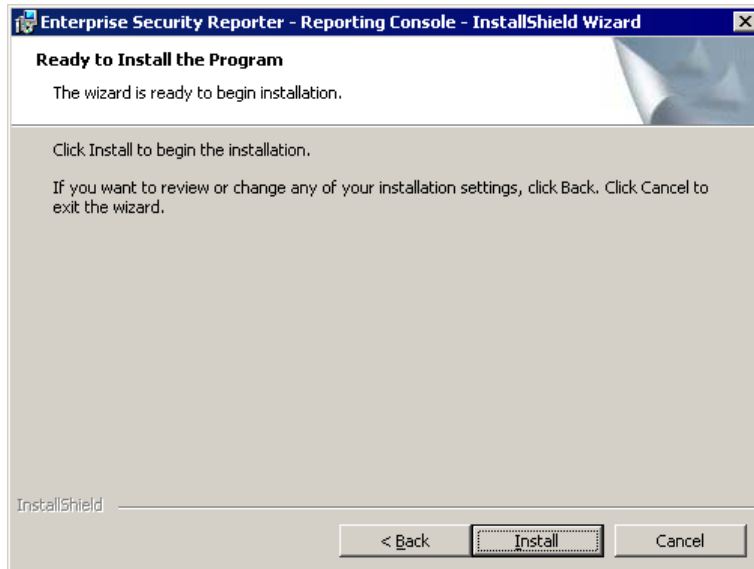
3. Select **I accept the terms in the license agreement**, and then click **Next**. The **Customer Information** page appears.



4. Select who can use the application, and then click **Next**. The **Destination Folder** dialog box appears.

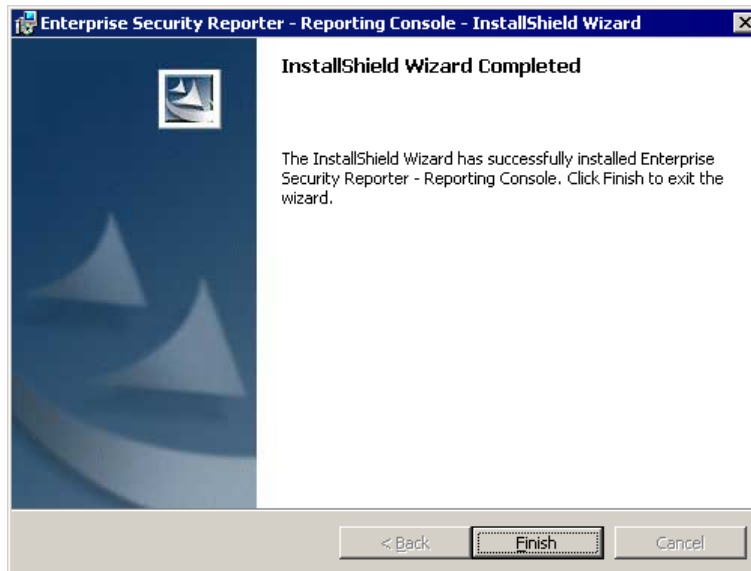


- If you want to change the installation destination, click **Change**, and then select a new location.
5. Click **Next**. The **Ready to Install the Program** box appears.



6. Click **Install**. A bar displays the progress.

When the installation is complete, the **InstallShield Wizard Completed** box appears.



7. Click **Finish**.

STARTING ENTERPRISE SECURITY REPORTER

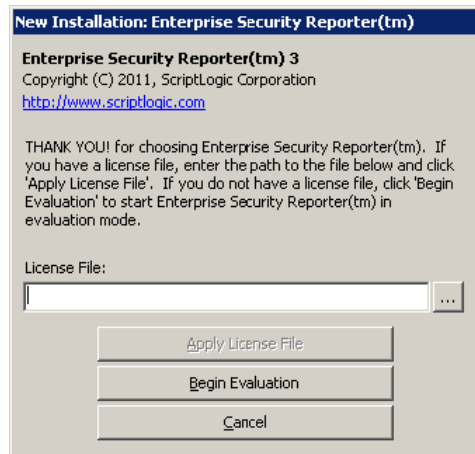
- ▶ Click **Start**, point to **Programs > ScriptLogic Corporation > Enterprise Security Reporter 3**, and then select one of the following options:

Programs	Use
Database Utilities > Discovery Database Wizard	Set up and manage the discovery database.
Database Utilities > Reporting Database Wizard	Set up and manage the reporting database.
Discovery Console	Create and run jobs on selected computers to discover data for use in reports.
Reporting Console	Create and run reports using discovered data in the reporting database.
Discovery Guide	Open the user manual for the Discovery Console.
Reporting Guide	Open the user manual for the Reporting Console.

Note: You also can access the Database Wizards and Reporting Console from the Discovery Console.

Applying a License File

The first time you start Enterprise Security Reporter, you see the **New Installation** dialog box, which allows you to apply a license file or evaluate the product without a license, as well as contact ScriptLogic Corporation and visit our website for further information.



Enterprise Security Reporter requires a valid license file in order to function properly. If you have a company license file or were provided with an evaluation or temporary license file, you must enter the location and filename in the **License File** box.

The license file is approximately 1KB in size and has a .lic file extension. Your sales account executive or a licensing team specialist should have sent this file to you as an email attachment.

- ▶ Click **[...]** to locate the license file, and then click **Apply License File**.

Evaluating the Product

- ▶ If you are evaluating the software and would like to use the preset values for the number of licenses, objects, and evaluation days, click **Begin Evaluation**.

Note: The full and evaluation versions of Enterprise Security Reporter are identical. The license file is the sole determinant of program functionality. You are limited to 3 servers and 5,000 items for discovery.

CREATING THE DISCOVERY AND REPORTING DATABASES

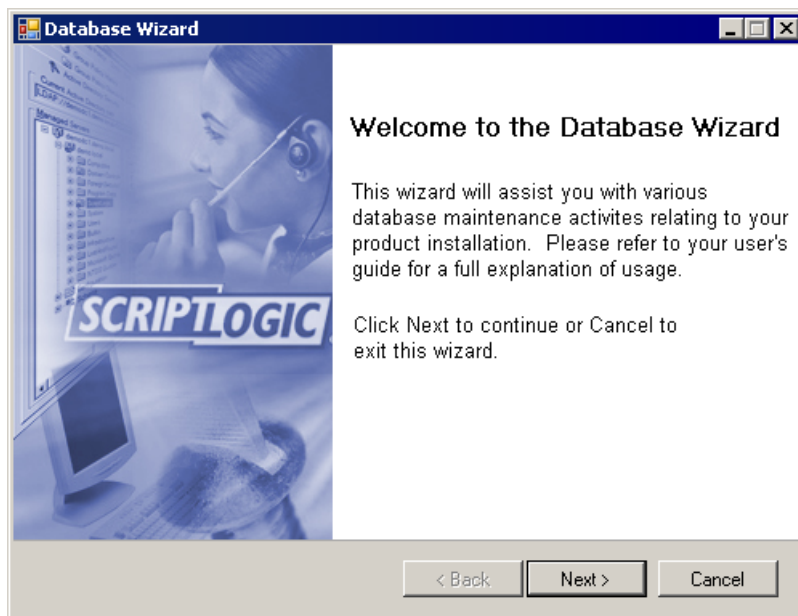
Important: For new installations only. If you are upgrading, your databases are upgraded automatically.

You must create the discovery and reporting databases before you can perform any tasks using Enterprise Security Reporter 3. Create the discovery database first, and then repeat the process for the reporting database. The default discovery database is dbESR3.mdf and the default reporting database is dbESR3Report.mdf.

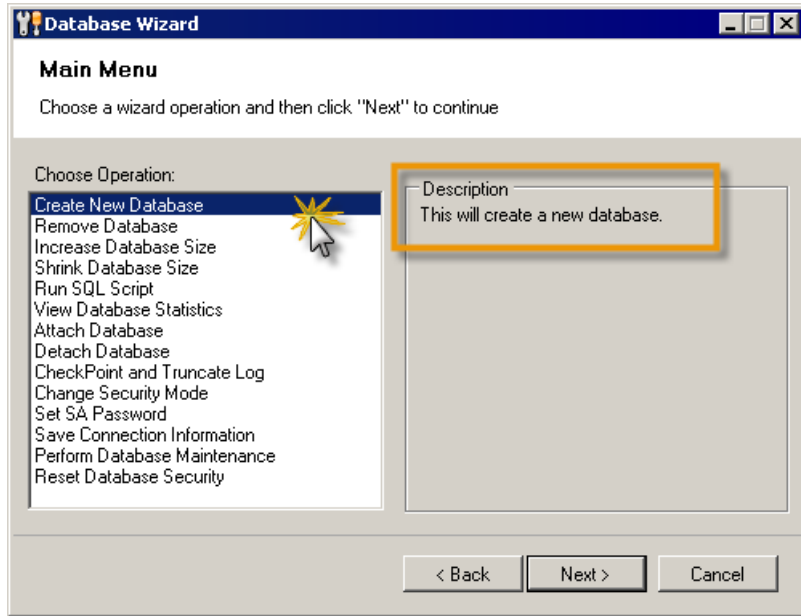
Important: Databases created with Enterprise Security Reporter 3 are not compatible with those created with Enterprise Security Reporter 2 or 1.

1. Click **Start**, point to **Programs > ScriptLogic Corporation > Enterprise Security Reporter 3 > Database Utilities**, and then choose **Discovery Database Wizard**. The **Welcome to the Database Wizard** box appears.

Note: After creating the discovery database, repeat this same process only choose the **Reporting Database Wizard**.

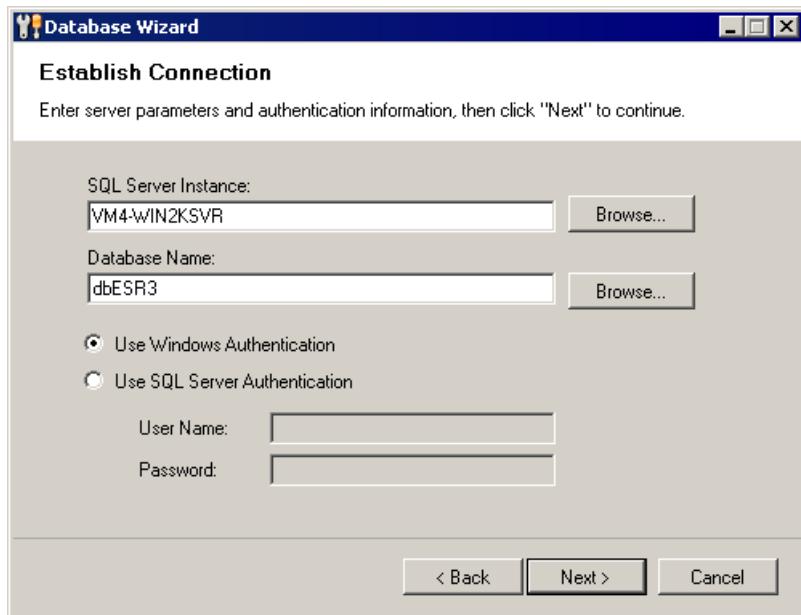


- Click **Next** to display the main menu. When you choose an operation from the list, a brief description displays.



- Select **Create New Database**, and then click **Next**. The **Establish Connection** box appears.
- In the **SQL Server Instance** box, type the name of the SQL Server, or click **Browse...** to locate the server.
- In the **Database Name** box, type the name of the auditing database to create. To view existing database names, click **Browse...**.

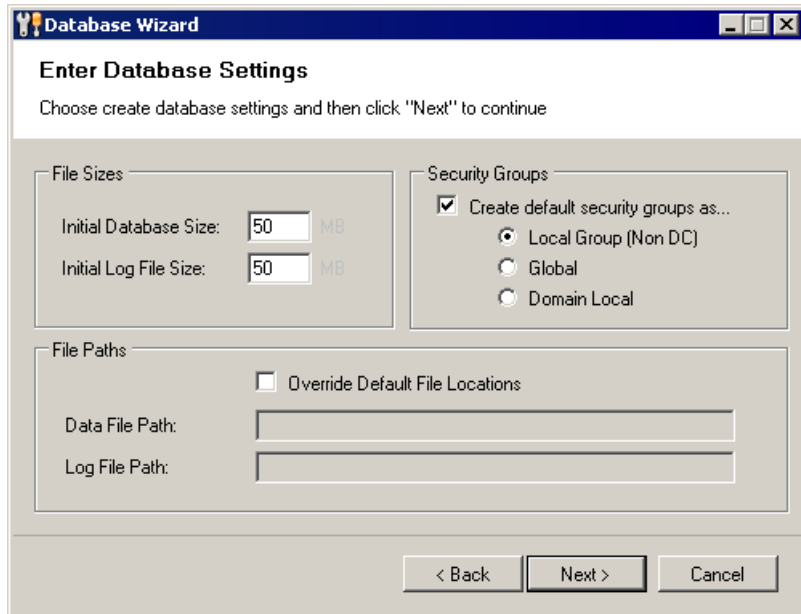
Note: The default discovery database is dbESR3.mdf. The default reporting database is dbESR3Report.mdf.



- The default selection for authentication is **Use Windows Authentication**. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

Important: If you want to use SQL Authentication, the SQL Server must be configured to use Mixed Mode authentication method

- Click **Next**. The database definition dialog box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.



File Sizes

By default, the database and log files are created at 50 MB each. If you want to change the default, type a value in the appropriate box. The data and log files grow automatically starting from the initial value specified here. You can change the size of the data file at a later time.

Create default security groups

By default, default security groups are created as local groups on non-domain controllers only. You can select to create default domain global or local groups. To bypass the creation of default security groups, clear the check box.

Override Default File Locations

Select to create the database transaction log files in a location other than the default location, Type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.



- Click **Next**. The **Create New Database** box displays the database name.
- Click **Finish**.

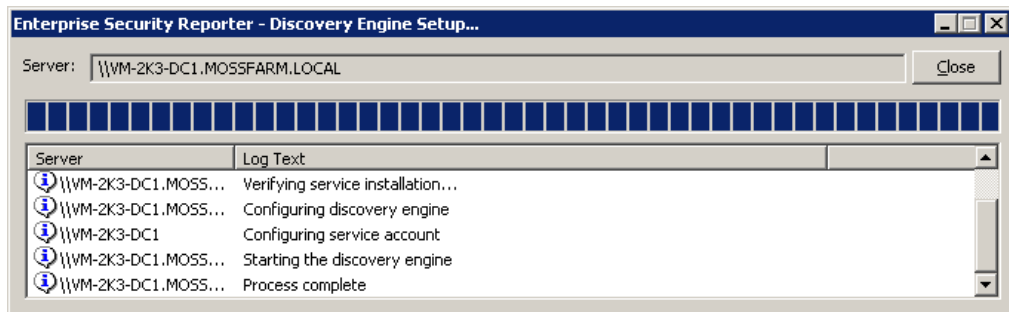
Note: If you are finished creating the discovery database, repeat the same process for the reporting database.

INSTALLING THE DISCOVERY ENGINE

Important: You must install the Discovery Engine before starting a discovery. To check if the Discovery Engine is installed, open the **Manage Discoveries** tab, and then open the **Select discovery server** drop-down list. If the computer where the Discovery Console is installed appears, then the Discovery Engine is installed.

Important: Installing the Discovery Engine to a computer that is running other ScriptLogic products may cause the computer to reboot. To prevent the reboot, temporarily shut down any ScriptLogic products or services running on the target computer before installing the Discovery Engine.

1. Click **Start**, point to **Programs > ScriptLogic Corporation > Enterprise Security Reporter 3**, and then choose **Discovery Console**. The Discovery Console opens.
2. Click . The **Install Discovery Service** box opens.
3. In the **Target machine name** box, type the name of the computer where the Discovery Console is installed, or select the computer from the list.
4. In the **Domain\username** box, type the account name that can run the Discovery Engine, or click  to locate an account name.
5. In the **Password** box, type the password.
6. Click **OK**. The **Discovery Engine Setup** window shows the progress of the installation of the discovery engine and service.



7. When you see **Process complete**, click **Close**.

PORTS AND PROTOCOLS USED BY ENTERPRISE SECURITY REPORTER

The Discovery Engine, Management Console, and Reporting Console use TCP/IP and Named Pipes protocols to communicate with the dbESR3 SQL Server database. By default SQL Server uses port 1433.

During discovery, the Discovery Servers communicate via port 8104 with the computer where the Discovery Console is installed in order to update the status of the discovery as far as job progress, completion, and cancellation.

If the Discovery Engine service is not installed on the server(s) to be discovered then the Discovery Engine uses RPC communication to perform the discovery on remote servers. RPC ports are well-known, and are usually 135-139 TCP or UDP.

Changing the Default TCP Port

The default TCP port used to communicate between the Discovery Console and the Discovery Engine is 8104. If you need to change the TCP port, adjust the registry key on the computer where the Discovery Console is installed and the computer on which the Discovery Engine is installed.

HKEY_LOCAL_MACHINE\SOFTWARE\ScriptLogic Corporation\Enterprise Security Reporter\v3\Config

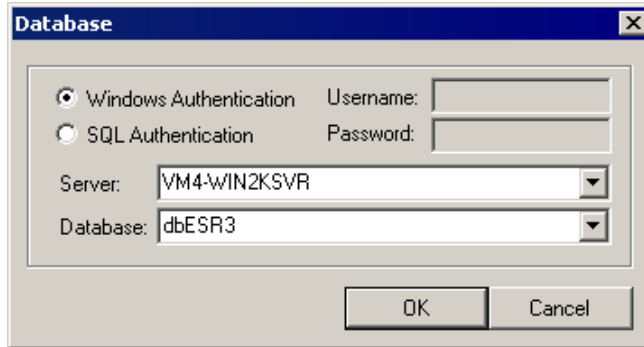
Value Name:	Port
Value Type:	REG_DWORD (decimal)
Value:	Enter the port number (8104 is the default)

After you change the registry key, both the Discovery Console and the Discovery Engine service must be stopped and restarted.

CONNECTING TO THE DISCOVERY DATABASE

If you have more than one discovery server and database, you need to connect to the one that you want to use.

1. From the **File** menu, choose **Connect to database**. The **Database** box displays the current discovery server and database. The default database created during the install process is dbESR3.mdf.



2. Choose the type of authentication to use. If you choose SQL Authentication, enter the user name and password.
3. Choose the discovery server and database to use, and then click **OK**.

CONFIGURING THE REPORTING CONSOLE FOR NON-ADMINISTRATIVE USERS

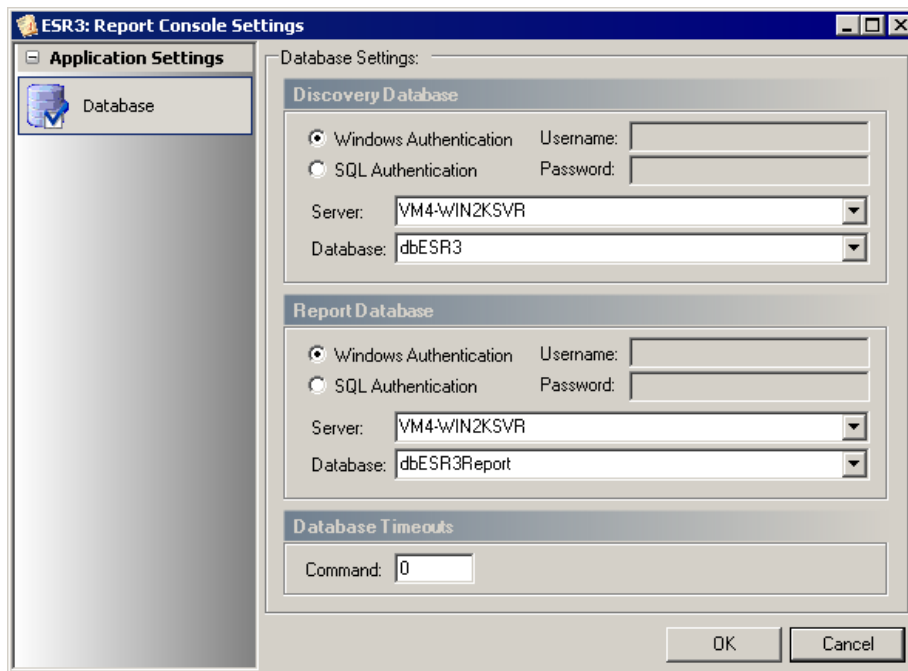
Since the reporting console often is used by people who are not involved in the discovery process, we have made it very easy to distribute the reporting console to end users and have it pull the configuration data from a master server. All you need to do is configure one server with the reporting console, and then configure each user’s reporting console to pull its configuration data from that master server.

1. Click **Start**, point to **Programs > ScriptLogic Corporation > Enterprise Security Reporter 3**, and then select **Reporting Console**.



2. From the **Reporting Console** main window, click **User Settings**. Alternatively, select **Settings** from the **Options** menu. The **Report Console Settings** box opens to **General Settings**.
3. Click **Database**. The **Database Settings** box appears.

On each computer where the Reporting Console resides, you must set the discovery server, and the discovery and reporting database. You also can adjust the amount of time before the computer times out trying to access the databases.



4. Select the servers where the databases reside, and select the databases.
5. Click **OK**.

OPTIONAL REGISTRY SETTINGS

There are a few settings you can add to the registry on a user's computer to configure the Report Console.

HKEY_CURRENT_USER\SOFTWARE\ScriptLogic Corporation\Enterprise Security Reporter\v3\ReportExecutingSettings

RenderWarningPageCount

When a report reaches 10,000 pages, report generation pauses and a message displays asking the user to continue or not. You can suppress this message by setting this value to -1.

CacheRowLimit (default value is 50,000)

Determines the number of rows that a data set must contain in order to cause the report to be cached to disk. Disk caching is slower, and therefore should not be used unless the report is very large.

RenderMaxVirtualMemorySize (default value is 1,536,000,000) (or 1.5GB)

Sets the amount of memory that may be consumed by the report before rendering is automatically stopped. Some reports can get beyond a size that can fit in memory, even when using disk caching. If the computer runs out of virtual memory, it will cause unpredictable behavior, therefore, by default, rendering stops once 1.5GB of memory is consumed. If the report will not render in 1.5GB of memory, then you can increase this value or modify the report design to remove graphical elements, such as the ScriptLogic icon in the page footers.

MaxGridMemorySize (default value is 512000000) (or 500MB)

Sets the maximum amount of virtual memory that the results grid is allowed to consume. Although the data grid may not be allowed to display all rows (because it does not support a disk caching mechanism), the full dataset is still available via the export option on that grid. The full dataset can be exported to a CSV or XML file.

MaxGridRowCount (default value is 1000 rows)

Sets the number of rows that the grid can display. If this number is very large, the **MaxGridMemorySize** value limits the amount of data displayed.

TempFolder (default value is C:\Documents and Settings\userID\Local Settings\Temp)

Designate the folder for generation of .xml report file. Type the full path to the folder.

WHERE TO GO NEXT

See the *Enterprise Security Reporter 3 Discovery Guide* for information on using the Database Maintenance Utility and the Discovery Console.

See the *Enterprise Security Reporter 3 Reporting Guide* for information on using the Reporting Console.

Troubleshooting

ScriptLogic Corporation has a library of articles in its Knowledge Base, which may provide an answer to a problem you are experiencing. Before calling technical support, check to see if your problem is documented here. You might also browse the Discussion Forums to see if anyone else is experiencing the same issue.

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

DISCOVERY ENGINE FAILS AFTER THE UPGRADE

If the discovery engine fails after the upgrade, remove and then reinstall the discovery engine.

Removing the Discovery Engine

Type the following at the command line on the computer on which the discovery engine is installed:

```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>Installutil.exe /u
"C:\Program Files\ScriptLogic Corporation\ESR3\Discovery
Engine\ESR3DiscoveryEngine.exe"
```

Once the discovery engine has been successfully uninstalled, the installation directory must be removed before another install can be completed (C:\Program Files\ScriptLogic Corporation\ESR3\Discovery Engine\).

DISCOVERY ENGINE SERVICE MARKED FOR DELETION

If you see a message stating that "the service has been marked for deletion" and are unable to install the discovery engine on the target server, reboot the target server, and then reinstall the discovery engine.

SETTING THE FREQUENCY OF DISCOVERY STATUS UPDATES

If you are running discoveries against a remote database, you might want to adjust the rate at which the Discovery Engine records the status of discovery jobs in the discovery database. The default rate is 5 seconds. The valid range is 1-60 seconds.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ScriptLogic Corporation\Enterprise Security Reporter\v3\Config
Value Name:      DiscoveryStatusUpdateInterval
Value Type:      REG_DWORD (decimal)
Default Value:   5
```

UNLOCKING THE DISCOVERY CONSOLE

If, for any reason, the licensing objects become corrupted, the Discovery Console locks and you see a message box when you start the application. To unlock the discovery console, you need an unlock code. Click **Request unlock code** to send an email to ScriptLogic. When you receive the unlock code via email, type the code in the **Unlock code** box, and then click **OK**.

UNINSTALLING THE DISCOVERY ENGINE

Type the following at the command line on the computer on which the discovery engine is installed:

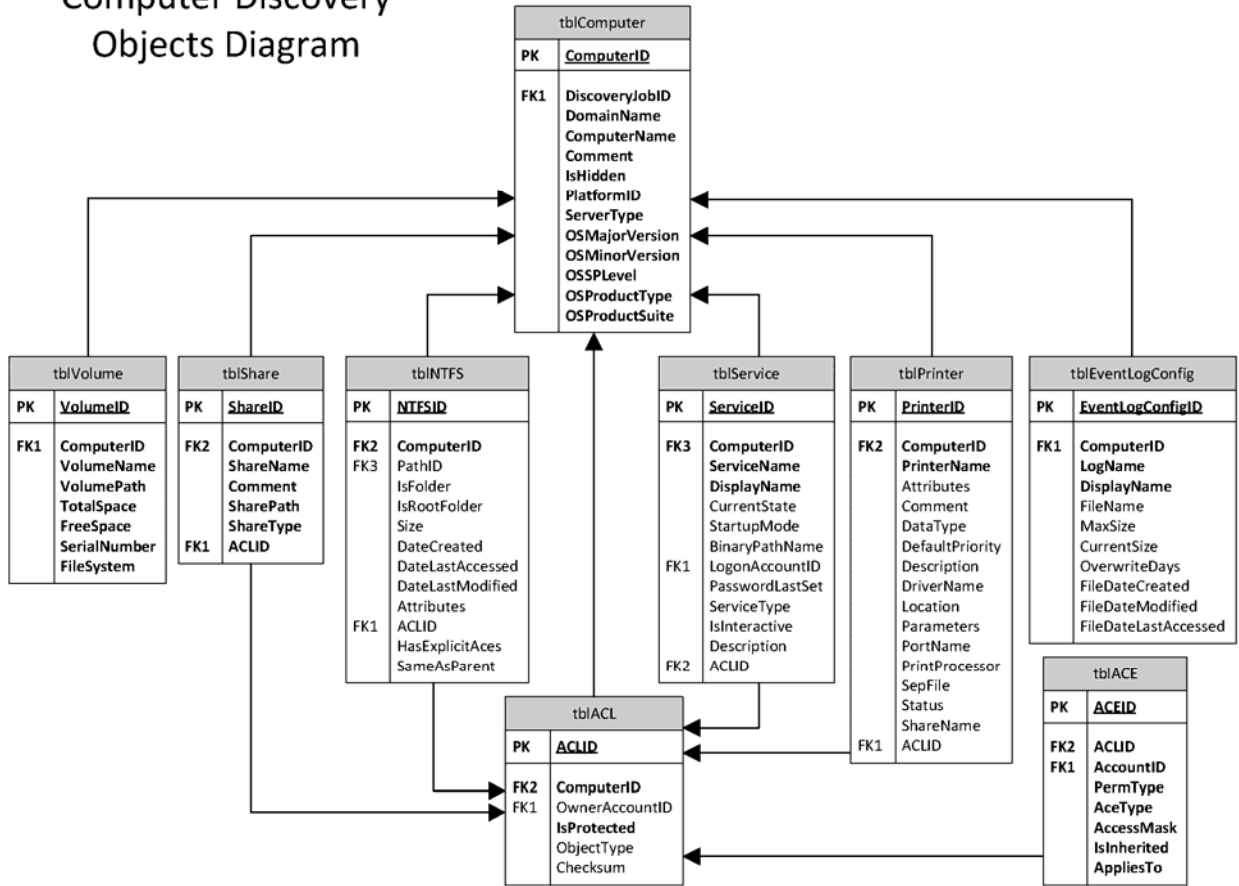
```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>Installutil.exe /u
"C:\Program Files\ScriptLogic Corporation\ESR3\Discovery
Engine\ESR3DiscoveryEngine.exe"
```

Once the discovery engine has been successfully uninstalled, the installation directory must be removed before another install can be completed (C:\Program Files\ScriptLogic Corporation\ESR3\Discovery Engine\).

dbESR3 Database Schema

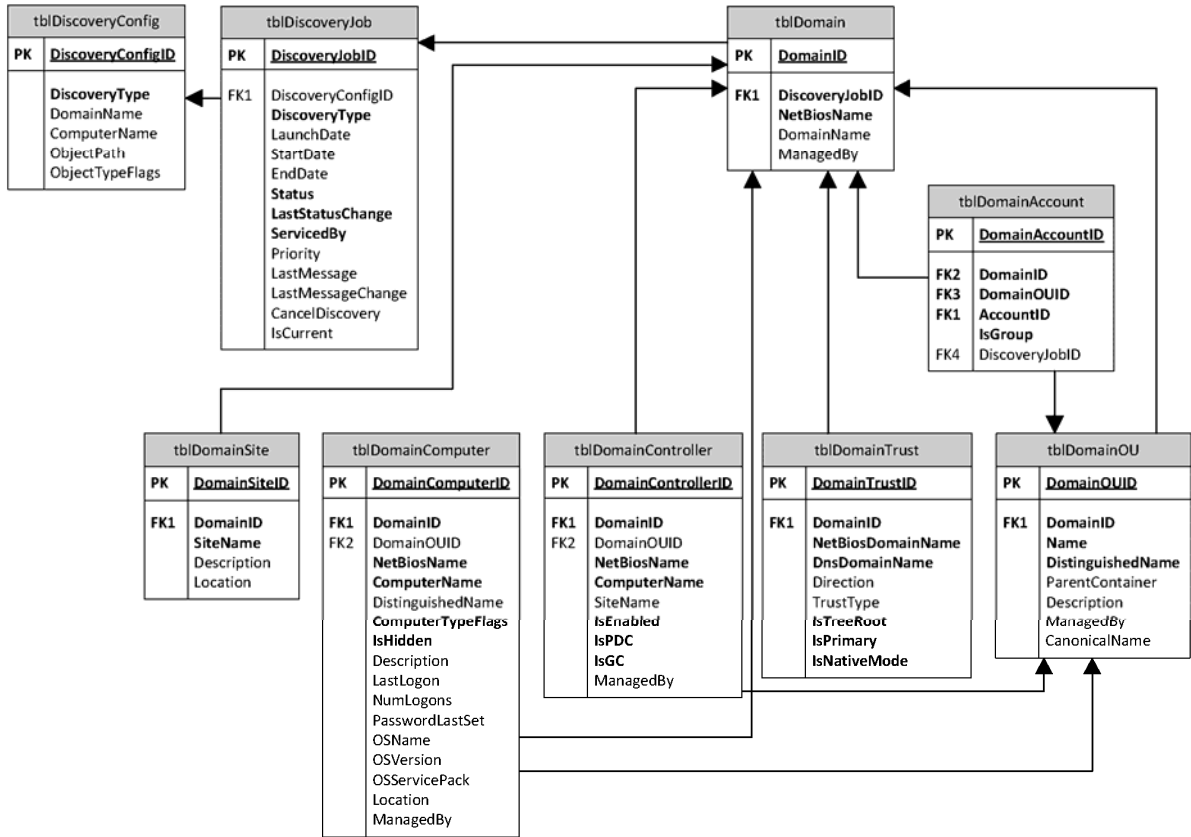
COMPUTER DISCOVERY OBJECTS

Computer Discovery Objects Diagram



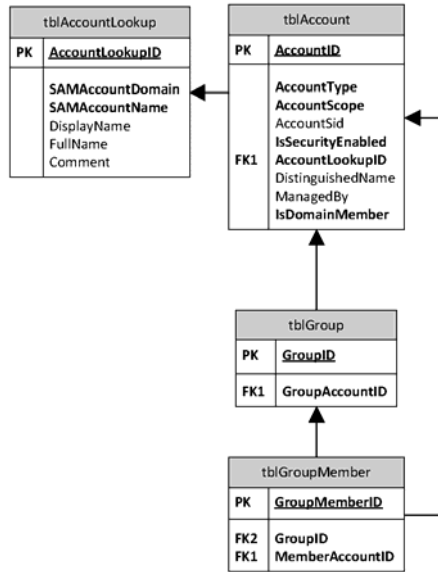
DOMAIN DISCOVERY OBJECTS

Domain Discovery Objects Diagram



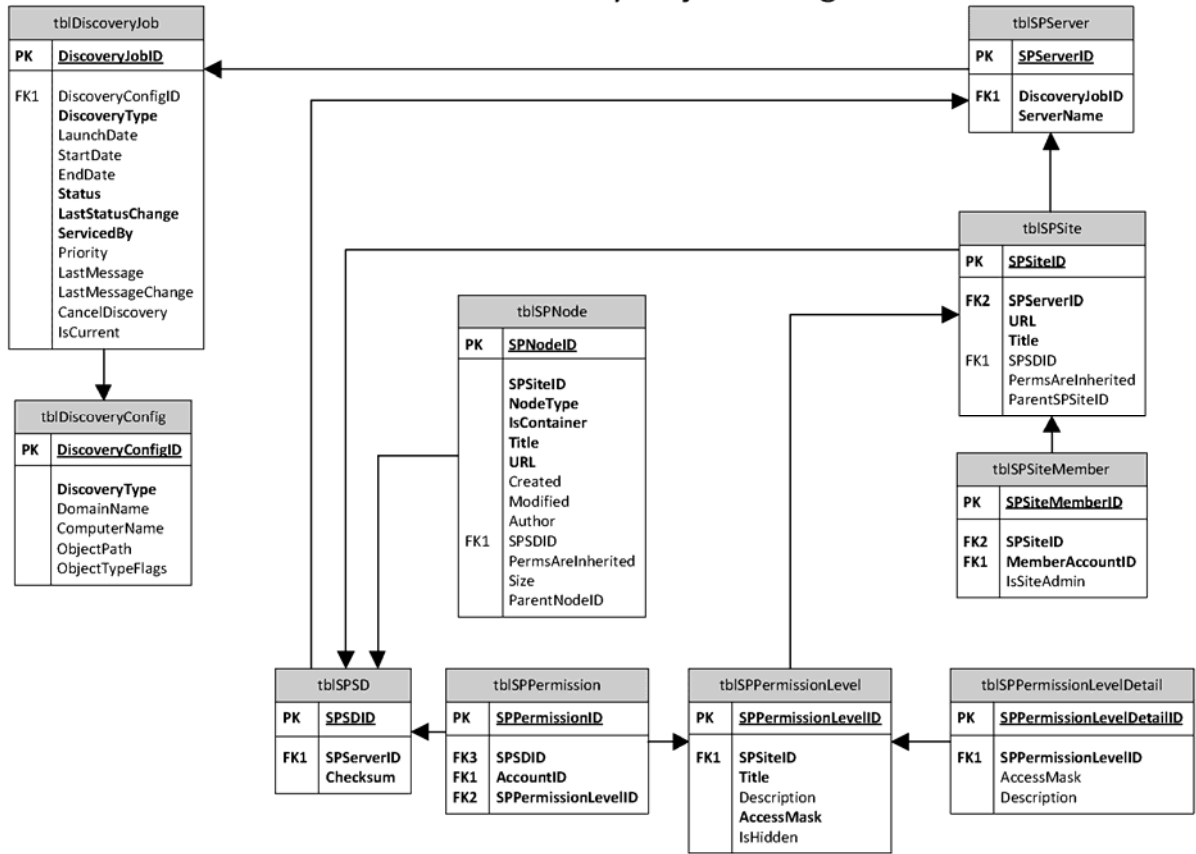
ACCOUNT OBJECTS

Account Objects Diagram



SHAREPOINT DISCOVERY OBJECTS

SharePoint Discovery Objects Diagram



SQL DISCOVERY OBJECTS

SQL Discovery Objects Diagram

