

ScriptLogic[®] Enterprise Security Reporter[™] 3.0 Getting Started Guide



© 2006 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.

Printed in the United States of America (4/2006)

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 <u>www.scriptlogic.com</u>. 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 nontechnical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

Contents

INTRODUCTION	5
Installing Enterprise Security Reporter	7
BEFORE YOU BEGIN	8
Supported Discovery Platforms	8
Hardware	. 8
Software	. 8
Supported Reporting Platforms	9
Hardware	. 9
Software	. 9
INSTALLING THE DISCOVERY CONSOLE	9
INSTALLING THE REPORTING CONSOLE	4
STARTING ENTERPRISE SECURITY REPORTER	8
Applying a License File	8
Evaluating the Product	8
CREATING THE DISCOVERY AND REPORTING DATABASES	9
INSTALLING THE DISCOVERY ENGINE	22
Changing the Default TCP Port	23
CONNECTING TO THE DISCOVERY DATABASE	23
CONFIGURING THE REPORTING CONSOLE FOR NON-ADMINISTRATIVE USERS	24
WHERE TO GO NEXT	24
QUICK START	25
DISCOVERING YOUR COMPUTER	25
RUNNING GLOBAL REPORTS	31
SUMMARY	35
TROUBLESHOOTING	36
SETTING THE FREQUENCY OF DISCOVERY STATUS UPDATES	36
UNINSTALLING THE DISCOVERY ENGINE	36
INDEX	37

IV

Introduction

Enterprise Security Reporter is a powerful and comprehensive reporting solution for documenting, NTFS, server registries, and file share permissions in Windows-based networks. As networks grow in size and complexity, visibility into overall permissions quickly becomes a business-critical security concern. Native, built-in operating system tools are insufficient to provide the summary or detailed reports needed to understand and proactively manage access. At best, native tools provide inspection of individual properties of your current configuration.

Enterprise Security Reporter is a solution focused on enterprise-wide Windows network permissions. By inspecting Active Directory[™], NTFS, server registries, and file shares, Enterprise Security Reporter produces the vital information needed to document security and take proactive action. Whether directly (such as NTFS permissions) or indirectly (such as group membership reporting), Enterprise Security Reporter provides summarized reports of access to files, folders, shares, registry keys, printers and services.

🍓 Enterprise Security Reporter	3.0 BETA ScriptLogic Corporation	
Eile Tools Help		
🗉 💋 🕼 🖉 🔯 🖓 🖓 🖓	di seconda d	
Domains	Discovery Groups 🕼 Manage Discoveries	
Computer Domain	Type 🥃 Items 🤪 Paths 🚱 Registry Keys 🎒 Options	
PC-45678 ACME	Member Server	
VM4-WINZKSVR ADME	Primary Domain Controller Image Discovery Parameters Image Discovery Parameters Image Discovery Construction Image Discovery Parameters Image Discovery Construction Image Discovery Parameters Image Discovery Construction Image Discovery Construction Image Discovery Construction	X
	Discovery servers	
	Select: VM4-WIN2KSVR 💽 🕄 Info 🧾 Stop 🔏 Install 🐻 Remove 🔽 Refresh every	5 secs. 🤣 Refresh
	Current discovery queue. Status Elapsed Priority 4/21/2006 - 11:34 AM (Einished) (surrent)	
	Domain LDAP://DC=acme,DC=com Finished 00:00:06 Normal	
Add Rough 5	Computer vm4-win2ksvr.acme.com Added Normal	
Kada Kasarch Ka	Computer pc-455/8.acme.com Started 00:02:10 Normal	
Connection: server=VM4-WIN2KSVB	Object Type Scan Count Discover Count	Elapsed Time
J	Group 21 21	2s
	Group Member 19 19	2s
	Account Rights 35 35	15
	Audit Policy 9 9	1s
	Computer Policy 9 9	1s
	Event Log 6 6 Printer 1 1	15
	Service 70 70	6s
	Share 9 9	1s
	Volume 1 1 E-liter 27 27	18
	File 131 131	138
	ACL 232 48	13s
	ACE 1217 224	13s
	🚰 Cancel 🛧 👽 🗟 Move	
	Connection: server=VM4-WIN2KSVR databas Discovery server: VM4-WIN2KSVR 1 pending, 1 started	Licenses: 100 Remaining: 98

Comprehensive Discovery

Enterprise Security Reporter collects data by connecting to and extracting relevant information from servers on your network. You can add servers individually or create discovery groups to define sets of servers to be queried. To minimize server loading, Enterprise Security Reporter performs its discovery and extraction without the use of agents. Enterprise Security Reporter has the granularity to select the information to be collected, including:

- Groups (including memberships)
- Users (including extended information)
- Account Rights
- Computer Policies
- Printers (and permissions)
- Services (and permissions)
- Shares (and permissions)
- Registry keys (and permissions)
- Volumes, Folders, and Files (and permissions)

Turnkey and Custom Reports

Enterprise Security Reporter has over 80 built-in reports, encompassing the most common reporting needs. Reports are based on the information collected using the Discovery Console. A simple selection of the type of report (such as Computer Policies, Group Memberships or Permissions) and the specific report you wish to run, and you instantly have an organized, useful set of information at your fingertips. You also can design custom reports using a report generator that creates customized professional and thorough reports without writing SQL queries.

	Ider Size Report - Sorted By Size	
Report	Results Query	
Í 👝 🖪 🗋		
E & E	int 🗅 🙀 🗖 🎛 🕂 🔾 @ 🚥 😰 🔽 🖈 🕑 1/1 🛛 🕝 Backward 🗇 Eorward	
		_ _
	Folder Size Report 4//2/20	006 12:05:10 PM
	Dath Eoldor	Sizo (Bytec)
		Size (Dytes)
	onna-winzkswiache.com Discovery Date. 4/6/20	006 6:16:02 PM
	C:VProgram Files/ScriptLogic Manager	10,489,364
	011-9/MIZKSM 2D1E20011 UISCUVERY Date: 44020 C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/	10,489,364 9,068,714
	UIT-FWITZKSM ACTRECUTI C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority C:Program Files/ScriptLogic Manager/MS Updates	006 6:16:02 PM 10,489,364 9,068,714 6,072,456
	VITE-WITZKSMachtecturit Discuvery Date: 44024 C:Wrogram Files/ScriptLogic Manager C:Vrogram Files/ScriptLogic Manager/DesktopAuthority 44024 C:Wrogram Files/ScriptLogic Manager/NS Updates C:Vrogram Files/ScriptLogic Manager/Scripts 44024	006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,523
	Onte-Wintzkska Zdrezouti Discuvery Date: 44024 C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthorty 2 C:Program Files/ScriptLogic Manager/Scripts C:Program Files/ScriptLogic Manager/Scripts 2	006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,523 4,540,420
	Onte-Wintzest achiectum Discuvery Date: 44024 CiProgram Files/ScriptLogic Manager C:	006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,523 4,540,420 356,352
	Onte-Wintzestration Discovery Date: 44024 CiProgram Files/ScriptLogic Manager CiProgram Files/ScriptLogic Manager/BesktopAuthority CiProgram Files/ScriptLogic Manager/Scripts CiProgram Files/ScriptScripts CiProgram Files/ScriptScriptScripts CiProgram Files/ScriptScriptScripts CiProgram Files/ScriptScripts CiProgram Files/ScriptScripts CiProgram Files/ScriptScripts CiProgram Files/ScriptScripts CiProgram Files/ScriptScripts CiProgram Files/Scripts	006 6:16:02 PM 10,489,364 9,068,714 6,072,455 4,540,523 4,540,420 356,352 4,266
	Onte-WintzestadDreadurity Discovery Date: 4022 C:Program Files/ScriptLogic Manager C:Virogram Files/ScriptLogic Manager/DesktopAuthority C:Virogram Files/ScriptLogic Manager/NS Updates C:Virogram Files/ScriptLogic Manager/NS Updates C:Virogram Files/ScriptLogic Manager/Scripts C:WINNTSYSVOLlsysvolacme.com/Scripts C:WINNTSYSVOLlsysvolacme.com/Scripts C:WINNTSYSVOLlsysVollsysvolacme.com/Scripts C:WINNTSYSVOLlsysVoll	006 6:16:02 PM 10,489,364 9,068,714 6,072,465 4,540,523 4,540,420 366,352 4,266 2,116
	Onte-WinizeStable.com Discovery Date: 4022 C:VFrogram Files/ScriptLogic Manager C:VFrogram Files/ScriptLogic Manager/Desktop.Authority C:VFrogram Files/ScriptLogic Manager/Scripts C:VFrogram Files/ScriptScripts C:VFrogram Files/ScriptScripts C:VFrogram Files/ScriptScripts C:VFrogram Files/ScriptScriptScripts C:VFrogram Files/ScriptScriptScriptScriptScriptScripts C:VFrogram/ScriptScriptScr	006 6:16:02 PM 10,483,364 9,068,714 6,072,456 4,540,523 4,540,420 356,352 4,266 2,116 884 ▼
<	UNIT-WINIZXSM2DIR2001 Discovery Date: 4402 C:VFrogram Files/ScriptLogic Manager C:VFrogram Files/ScriptLogic Manager/Scripts 4402 C:VFrogram Files/ScriptLogic Manager/Scripts C:VFrogram Files/ScriptLogic Manager/Scripts 4402 C:VFrogram Files/ScriptLogic Manager/Scripts C:VFrogram Files/ScriptLogic Manager/Scripts 4402 C:VMINITS/SVOLIsysvoltacme.com/Scripts C:VFrogram Files/ScriptLogic Manager/Scripts 4402 C:WINITS/SVOLIsysvoltacme.com/Scripts C:WINITS/SVOLIsysvoltacme.com/Scripts 4402 C:WINITS/SVOLIsysvoltacme.com/Scripts C:WINITS/SVOLIsysvoltacme.com/Scripts 4402 C:WINITS/SVOLIsysvoltacme.com/Scripts 4402 4402	006 6:16:02 PM 10,489,364 9,068,714 6,072,458 4,540,523 4,540,420 356,352 4,266 2,116 884 ▼

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.



7

BEFORE YOU BEGIN

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

Supported Discovery Platforms

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

Operating Systems

- Windows 2000: Professional, Server
- Windows XP Professional
- Windows Server[™] 2003: Standard, Server, Enterprise Edition

Hardware

- 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

Software

- Microsoft .NET Framework 1.1 Service Pack 1
- Microsoft Data Engine (MSDE) 2000; or Microsoft SQL Server 2000 and Data Access Components (MDAC) 2.7

Note: MSDE and MDAC are included with Enterprise Security Reporter.

Important: While the Discovery Console does not support Windows NT® 4.0, You can discover computers running on Windows NT 4.0, and any other Windows operating system. 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 Reporting Platforms

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

Operating Systems

- Windows 2000: Professional, Server
- Windows XP Professional
- Windows Server[™] 2003: Standard, Server, Enterprise Edition

Hardware

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

Software

Microsoft .NET Framework 1.1 Service Pack 1

INSTALLING THE DISCOVERY CONSOLE

Enterprise Security Explorer is provided in a Microsoft® Windows® Installer package format, which allows for robust, self-repairing of application files and ease of installation and software distribution. The Windows Installer service is included with Windows 2000 and later, for the purposes of this product installation.

Note: You are 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.

Important: If you have Enterprise Security Reporter already installed and are upgrading to the latest version, please see the *Release Notes* for complete upgrade instructions.

1. Double-click the ESR3Setup_DiscoveryConsole.msi file.

Note: If you do not have Microsoft .NET Framework 1.1 Service Pack 1 installed, a message box appears.



To install Microsoft .NET Framework 1.1 Service Pack 1, 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.

🙀 Enterprise Security Reporter - Discovery Console - InstallShield Wiz	ard 🛛 🗙
License Agreement Please read the following license agreement carefully.	
END USER LICENSE AGREEMENT	_
READ THE TERMS OF THIS LICENSE AGREEMEN "AGREEMENT") CAREFULLY BEFORE DOWNLO OR INSTALLING THE SOFTWARE (TOGETHER WI WHERE APPLICABLE, ASSOCIATED DATABASE SERVICES AND CERTAIN ADDITIONAL SOFTWAR FUNCTIONALITY, COLLECTIVELY THE "SOFTWAR	NT (THE ADING TH, S, DATA RE RE ").
 I accept the terms in the license agreement I do not accept the terms in the license agreement 	Print
InstallShield < <u>Back</u> <u>N</u> ext >	Cancel

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 **Destination Folder** dialog box appears.

🙀 Enterpris	se Security Reporter - Discovery Console - InstallShield Wizard	×
Destinat i Click Net	ion Folder xt to install to this folder, or click Change to install to a different folder.	1
	Install Enterprise Security Reporter - Discovery Console to: C:\Program Files\ScriptLogic Corporation\ESR3\Discovery Console\	
InstallShield	< Back Cancel	

- If you want to change the installation destination, click **Change**, and then select a new location.
- 4. Click Next. The Setup Type box appears.

🔡 Enterprise Sec	curity Reporter - Discovery Console - InstallShield Wizard	×
Setup Type Choose the set	tup type that best suits your needs.	
Please select a	e setup type.	
• <u>Complete</u>	All program features will be installed. (Requires the most disk space.)	
C Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.	
InstallShield	< <u>B</u> ack <u>N</u> ext > Car	icel

Note: MSDE 2000 is installed with the complete install. To omit installing MSDE 2000, choose **Custom**.

5. Select to do a complete or a custom install, and then click **Next**.

Note: If you chose **Custom**, expand **Microsoft SQL Server Desktop Engine 2000**, select **This feature will not be available**, and then click **Next**.

🙀 Enterprise Security Reporter - Discovery Co	nsole - InstallShield Wizard 🛛 🔀	
Custom Setup Select the program features you want installed.		
Click on an icon in the list below to change how a feat All Components Microsoft SQL Server Desktop Engine 7 This feature will be installed on local he B This feature, and all subfeatures, will	ure is installed. Feature Description MSDE 2000 or Microsoft SQL 2000 is required for Enterprise ard drive. Se. be installed on local hard drive.	
 This feature will be installed when require the second seco	n	
installShield	ck Next > Cancel	

The **Ready to Install the Program** box appears.

🚏 Enterprise Security Reporter - Discovery Console - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
InstaliShield	



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.

🚏 Enterprise Security Reporter - Reporting Console - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	
END USER LICENSE AGREEMENT	
READ THE TERMS OF THIS LICENSE AGREEMENT (THE "AGREEMENT") CAREFULLY BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE (TOGETHER WITH, WHERE APPLICABLE, ASSOCIATED DATABASES, DATA SERVICES AND CERTAIN ADDITIONAL SOFTWARE FUNCTIONALITY, COLLECTIVELY THE "SOFTWARE").	
○ I accept the terms in the license agreement Print	
• I do not accept the terms in the license agreement	
InstallShield	
< <u>B</u> ack <u>M</u> ext > Cancel	

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 **Destination Folder** dialog box appears.

👹 Enterpris	se Security Reporter - Reporting Console - InstallShield Wizard	×
Destinat i Click Ne:	ion Folder xt to install to this folder, or click Change to install to a different folder.	1
	Install Enterprise Security Reporter - Reporting Console to: C:\Program Files\ScriptLogic Corporation\ESR3\Reporting Console\	
InstallShield	< Back Next > Cancel	

- If you want to change the installation destination, click **Change**, and then select a new location.
- 4. Click **Next**. The **Setup Type** box appears.

🛃 Enterprise See	curity Reporter - Reporting Console - InstallShield Wizard	×
Setup Type Choose the se	etup type that best suits your needs.	
Please select a	a setup type.	
	e All program features will be installed. (Requires the most disk space.)	
C Cu <u>s</u> tom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.	
InstallShield ——	< <u>B</u> ack <u>N</u> ext > Ca	ncel





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

🔂 Enterpris	e Security Reporter - Reporting Console - InstallShield Wizard 📃 🔲 🗙
Installing The prog	Enterprise Security Reporter - Reporting Console ram features you selected are being installed.
17	Please wait while the InstallShield Wizard installs Enterprise Security Reporter - Reporting Console. This may take several minutes.
	Status:
InstallShield	
	< Back Next > Cancel

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
Discovery Database Wizard	Set up and manage the ESR3 discovery database
Reporting Database Wizard	Set up and manage the ESR3 reporting database.
Discovery Console	Create and run jobs on selected computers to discover data for use in reports
	Note: You also can access the Database Wizards and Reporting Console from the Discovery Console.
Reporting Console	Create and run reports using discovered data in the ESR3 reporting database

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 support 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.

CREATING THE DISCOVERY AND REPORTING DATABASES

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.

 Click Start, point to Programs > ScriptLogic Corporation > Enterprise Security Reporter 3, and then choose Discovery Database Wizard. The Database Maintenance Wizard opens.

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



2. Select **Create a new database** from the list, and then click **Next**. The database selection dialog box displays the **dbESR3** database (default).

Note: If you are installing the reporting database using the Reporting Database Wizard, **dbESR3Report** displays as the default database.

SQL Database Server Name: VM4-WIN2KSVR Database Name: dbESR3 • Use Windows Authentication • Use SQL Server Authentication User Name: Password:

- 3. In the **SQL Database Server Name** box, type the name of the server that is running MSDE 2000 or Microsoft SQL Server 2000, or click ... to locate a server.
- 4. In the **Database Name** box, type the name of the database to create or click <u>...</u> to locate existing database names.
- 5. 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 Windows Authentication, the SQL Server must be configured to use trusted security.

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

💱 Database Maintenance Wi	zard - Create a new database	x
	Initial Database Size: 50 Initial TX Log Size: 50 Override Default File Locations Data File Path: TX Log Path: (The paths above should be the local path on the server where the database will be created. Ex: "C:\DB\") ✓ Create default security groups Create security groups a C Domain Groups Domain Local Groups C Local Groups (non-DC's only)	
_	Cancel < Back Next > Einish	

- 7. In the **Initial Database Size** box, type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.
- 8. In the **Initial TX Log Size** box, type an initial size for the transaction log file (*.ldf). If the database needs to grow the log file, it will do so automatically.
- 9. To create the database transaction log files in a location other than the default location, select the **Override Default File Locations** check box, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
- 10. By default, default security groups are created as local groups on non-domain controllers only. You can select to create default domain groups or domain local groups. To bypass the creation of default security groups, clear the **Create default security groups** check box.
- 11. Click Next. The Database Maintenance Wizard displays the options you chose.
- 12. To create the specified database, click **Finish**.

As the action runs, a progress bar displays the action occurring and the progress towards completion. When the action is finished, a message box appears.

13. Click OK, and then close the Database Maintenance Wizard.

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 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.

- 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 stole 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.

Enterprise Security	Reporter - Discovery Engine Setup	_ 🗆 X
Server KVM4-WIN	N2KSVR.ACME.COM	Close
Server	Log Text	
Image: Window	Beginning installation on remote server: \\VM4-WIN2KSVR.ACME.COM The agent is now installed on server: \\VM4-WIN2KSVR.ACME.COM Verifying service installation Configuring service account Configuring discovery engine Starting the discovery engine Process complete	

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

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.

D	atabase				×
	 Window SQL Aut 	s Authentication hentication	Username: Password:		
	Server: Database:	VM4-WIN2KSVR dbESR3			- -
			10	<	Cancel

- 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**.
- 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 Setting**s 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.

🍓 ESR3: Report Console Se	ttings 📃 🗌 🗙
Application Settings	Database Settings:
General	Discovery Database
Database	Windows Authentication Username: SQL Authentication Password:
Advanced	Server: VM4-WIN2KSVR Database: dbESR3
	Report Database Image: SqL Authentication Username: Image: SqL Authentication Password: Server: VM4-WIN2KSVR Database: Image: dbESR3Report Database: Image: dbESR3Report Database Timeouts Image: dbESR3Report
	OK Cancel

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

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.

Quick Start

In this section you are taken step-by-step through discovering your computer and generating reports from the data. In this Quick Start you discover data on your computer, and then run a Global report.

Important: This tutorial assumes that you have already completed the entire installation process, including creating the discovery and reporting databases, installing the Discovery Engine Service, and connecting to the databases.

DISCOVERING YOUR COMPUTER

1. If you haven't already done so, click Start, point to Programs > ScriptLogic Corporation > Enterprise Security Reporter 3, and then choose Discovery Console.

Enterprise Security Reporter 3.0	×
ile <u>T</u> ools <u>H</u> elp	
🚳 Domains 📲 Computers 🔛 Discovery Groups 🤯 Manage Discoveries	
Domain Discovery DC Domain Type 💮 Items 📑 Attributes 🎲 Organizational Units 💽 Options	
Discovery Domain Controller	
Select discovery domain controller:	
Discovery Domain Attributes	
Domain accounts Sites Tust relationships	
Domain computers Organizational units	
Synchronize last logon information	
Apply S Schedule	
Add	
onnection: server=VM4-wIN2KSVR database=dbESR3	

If you haven't added a domain, your screen should appear similar to this. The first step is to add domains.

25

2. Click Add... The **Select Target Domain** box appears. Expand the list to view the domains.



- 3. Select one or more domains from the list or type a domain name in the box.
- 4. Click **OK**. Each domain is listed along with the domain type.

🕵 Enterprise Security Reporter 3.0	
<u>File T</u> ools <u>H</u> elp	
Domains 📓 Computers 📓 Discovery Groups 🚱 Manage D	iscoveries
Domain Discovery DC Domain Type	🕼 Items 📋 Attributes 🙀 Organizational Units 💽 Options
	Select discovery domain controller
Add Remove	
Connection: server=VM4-WIN2KSVR database=dbESR3	

- 5. Select the domain in the left pane. The **Items** tab becomes available.
- 6. In the **Select discovery domain controller** box, type the name of the domain controller or click **l** to locate a domain controller.

Click Apply . The selected discovery domain controller is listed in the Discovery DC column in the left pane.

1	interprise Se	curity Reporter 3.0						
File	<u>T</u> ools <u>H</u> elp							
	i 💋 📢 i 📑							
/	🎯 Domains	Computers	🚔 Discovery Groups	👸 Manage 🛙	liscoveries			
	Domain	Discovery DC	Domain Type		🎒 Items	Attributes	🛃 Organizational Units	🕑 Opt 👞 🕨
					Select VM4	covery Domain Co st discovery doma I-WIN2KSVR covery Domain At	nhroller	
					이 다 다 다 다 다 다 다 아 다 다 다 아 아 아 아 아 아 아 아 아	ites rust relationships romain controllers romain computers Irganizational unit ynchronize last lo	s gon information	
	A	and the state of the	and the second second second			oply 🚱 Scher	dule	

Now add your computer to the list.

8. Open the **Computers** tab. If you haven't added any computers, your screen should be similar to this one.

🚱 Domains 🛛 🔋 Computers	🛔 Discovery Groups	🚱 Manage Discoveries		
Computer Domain Type		Items I	Paths	
💰 Add 🛛 🗟 Search 🖉 F	iemove		pply 🕼 Schedule	

 Select your computer from the list. The computer name displays in the Computer Name box. If you want to select more than one computer, do so now. The Computer Name box becomes unavailable if you select more than one computer.

📲 Select Target Computer	
Desktop Network Neighborhood PC-45678 PC-45678 Active Directory Active Directory Desktop PC-45678	
Computer Name:	
OK Ca	ancel

11. Click **OK**. The selected computers display in the left pane.

🕵 Enterprise Security Reporter 3.0 📃 🗆 🗙
Ele Lools Help
Domains 🗟 Computers 🕌 Discovery Groups 😵 Manage Discoveries
Computer Domain Type
Image: Server win2ksvr Primary Domain Controller PC-45678 Member Server Image: Discovery Parameters Image: Local accounts
Connection: server=VM4-WIN2KSVR database=dbESR3

Now that we've added computers to the discovery process, the next step is to configure the discovery. Here on the **Computers** tab, you can configure each computer separately, but if you open the **Discovery Groups** tab, you can create and configure a group of computers.

For now, let's just discover your own computer. In this example, my computer is the PDC. When I select it, the check boxes on the **Items** tab become available.

🕵 Enterprise Security Reporter 3.0	
<u>File Iools H</u> elp	
Computers Computers]
Computer Domain Type 🕘 Items 💋 Paths 🚱 Registry Keys 🍎 Options	
Image Domain Controller Image Decktor	
ر میں جرب کا مصافر میں جانب کی جانب کا میں جو ہوتی ہے کہ میں اور انہیں جب کا میں ا	, and the second se

By default, all discovery parameters except for Registry keys are selected. For this exercise, let's discover the folders and permissions on the computer.

- 12. Clear all the check boxes except for the **Volumes**, **Folders**, and **Permissions** check boxes.
- 13. Click 🖉 Apply

There are many other selections we could apply to our discovery, but let's start with these simple selections. Your screen should appear similar to this one.

📢 Enterprise Security Reporter 3.0
Elle Tools Help
Onmains Computers Discovery Groups Manage Discoveries Computer Domain Type Items Paths Registry Keys Options MdAv/IN2KSVR ACME Primary Domain Controller Items Paths Registry Keys Options Computer Domain Type Items Paths Registry Keys Options Colocal accounts Local accounts Local accounts Shares Shares Shares Viniter Folders Permissions Volders Permissions Viniter Files Permissions Apply Schedule Add Remove Bemove Eventor Schedule
Connection: server=VM4-WIN2KSVR database=dbESF

Now we're ready to begin the discovery.

14. In the toolbar, click . The **Select Discovery Engine** box lists the servers with the discovery engine installed.

Select Discovery Er	ngine	×
Select the discovery e	ngine that will process this job:	
Computer Name		1
VM4-WIN2KSVR		
	OK Cancel	L.
	Cancer	1

- 15. Select the server to run the discovery, and then click **OK**. To see the status of the discovery, open the **Manage Discoveries** tab.
- 16. In the Select discovery server box, select the discovery server that is running the discovery, and then click Refresh. The discoveries are listed in the Current discovery queue list. The status updates as the job runs.

Note: If you want the **Current discovery queue** to refresh automatically, select the **Refresh every 5** secs check box, and then change the duration, if desired.

🕵 Enterprise Security Reporter 3.0
Ele Tools Help
liscovery Groups 🖓 Manage Discoveries
Select discovery server: VM4-WIN2KSVR 🔽 3 Info 🖪 Stop 🖓 Install 3 Remove 🔽 Refresh every 5 secs. 3 Refresh
Current discovery queue: Select job:
Type Path Status Elapsed Priority Last M 3/9/2006 - 12:06 PM (Finished) (current)
Computer vm4-wm2ksvr.acme.com Finished UU:UU:37 Normal Discov
• Status C Logs C Errors
Discover Count Elapsed Time
Folder 774 774 36s
File 0 0 36s ACL 774 62 36s
ACE 4469 376 36s
Cancel 1 M W Move

When the job finishes, the status column changes to Finished. The Select job box lists the job as the current job, which is the job that the Reporting Console uses to run reports on that computer.

Now that we have our discovery data, we can run reports against it.

RUNNING GLOBAL REPORTS

Enterprise Security Reporter had several standard reports that you can run with a single click of a button. You can run reports against any data that you discover.

- 1. Open the Reporting Console using one of these three methods.
 - Click Start, point to Programs > ScriptLogic Corporation > Enterprise Security Reporter 3, and then select Reporting Console.
 - From the Discovery Console, click . or choose **Open reporting console** from the **Tools** menu.

After starting the Reporting Console, you see the main application window where you can run reports and create custom reports. The **Enterprise Security Reporter Reporting Console** main window opens to the list of **Recent Reports**, which on initial installation will be empty. As you run reports, this list will grow.



In our example, we discovered the volume, folders, and folder permissions on our computer, so we are able to run those types of reports.

Notice the names of the discovery and reporting databases and the servers on which they reside display in the status bar. If you want to connect to a different database server, click User Settings.

2. Click Global Reports. Expand Computer Reports, and then Folders. Click Folder Size Report-Sorted By Path. A description of the report and the required parameters display in the lower right pane. Notice that there are two parameters, one required and one hidden. You will select the computer to use for the report (required) and the report uses the current discovery (hidden).



3. To run the report, double-click the report name, or right-click the report name, and then select **Run Report**.

There is only one required parameter for the report we selected, so the **Select Computer(s)** box opens with the default selection.

📢 ESR3: Folder Size Repo	rt - Sorted By Size Param	neters
Select Computer(s) [Req Select the computers to	uired] include in this report	
(1) Select Computer(s)	Select Computers By: Enterprise Scope Domain Computer Name Description IP Address Computer Type	Select or enter Enterprise Scope:
		Cancel < Back Next > Finish

We did a discovery on a specific computer, so we will use the computer name to locate the data in the discovery database.

- 4. In the Select Computers By list, select Computer Name.
- 5. From the **Select or enter Computer Name** box, select your computer, and then click +. The selected computer is added to the list.

🍕 ESR3: Folder Size Repo	rt - Sorted By Size Para	ameters 📃 🗆 🗙
Select Computer(s) [Rec Select the computers to	uired) include in this report	
(1) Select Computer(s)	Select Computers By: C Enterprise Scope C Domain C Computer Name C Description C IP Address C Computer Type	Select or enter Computer Name: vm4-win2ksvr.acme.com
		Cancel < Back Next > Finish

Since this is the only parameter, the **Next** button is unavailable. If there were more parameters to enter, you would click **Next** to enter the next parameter.

6. To generate the report, click **Finish**. The report displays.

🍓 ESR3: Folder Size Report - Sorted By Size		_ 🗆 ×
Report Results Query		
□ 😓 Eint 🗅 🛤 🗆 🖽 🔍 🔍 💷 🗶 📝 1/1 🔤 🤤	Backward O Eorw	vard
Folder Size Report		4/12/2006 12:05:10 PM
Path		Folder Size (Bytes)
vm4-win2ksvr.acme.com	Discovery Date:	4/6/2006 6:16:02 PM
vm4-win2ksvr.acme.com C:Vprogram Files\ScriptLogic Manager	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364
vm4-win2ksw.acme.com C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714
vm4-win2ksvr.acme.com C:\Program Files\ScriptLogic Manager C:\Program Files\ScriptLogic ManagerDesktopAuthority C:\Program Files\ScriptLogic ManagerWS Updates	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714 6,072,436
vm4-win2ksw.acme.com C.\Program Files\ScriptLogic Manager C.\Program Files\ScriptLogic Manager\DesktopAuthority C.\Program Files\ScriptLogic Manager\ScriptSupAuthorits C.\Program Files\ScriptLogic Manager\Scripts	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714 6,072,455 4,540,523
vm4-win2ksw.acme.com C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority C:Program Files/ScriptLogic Manager/Scripts C:Program Files/ScriptLogic Manager/Scripts C:WNNT/S:YS/OL'sysvollacme.com/scripts	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,523 4,540,420
vm4-win2ksw.acm.ecom C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority C:Program Files/ScriptLogic Manager/SCripts C:WNINTS/SYS/OLJsysv0/acme.com/scripts C:WnINTS/SYS/OLJsysv0/acme.com/scripts C:Program Files/ScriptLogic Manager/Services	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,523 4,540,420 356,352
wm4-win2kswr.acm.e.com C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority C:Program Files/ScriptLogic Manager/Scripts C:Program Files/ScriptLogic Manager/Scripts C:WMINT/SYSVOLsysvolkacme.com/scripts C:WMINT/SYSVOLsysvolk	Discovery Date:	446/2006 6:16:02 PM 10,469,364 9,068,714 6,072,456 4,540,523 4,540,420 356,352 4,266
	Discovery Date:	4/6/2006 6:16:02 PM 10,463,364 9,068,714 6,072,456 4,540,420 356,352 4,266 2,116
wm4-win2ksw.acme.com C:Program Files/ScriptLogic Manager C:Program Files/ScriptLogic Manager/DesktopAuthority C:Program Files/ScriptLogic Manager/Scripts C:Program Files/ScriptLogic Manager/Scripts C:WNINT/SYSVOL/sysvolacme.com/Scripts C:WMINT/SYSVOL/sysvolacme.com/Scripts C:WMINT/SYSVOL/sysvolacme.com/Scripts/scriptscripts/scripts/scripts/scripts/scripts/scripts/scripts/scripts/scrip	Discovery Date:	4/6/2006 6:16:02 PM 10,489,364 9,068,714 6,072,456 4,540,420 356,352 4,540,420 356,352 4,266 2,116 884
um4-win2ksw.acm.e.com C:\Program Files\ScriptLogic Manager C:\Program Files\ScriptLogic Manager\DesktopAuthortly C:\Program Files\ScriptLogic Manager\DesktopAuthortly C:\Program Files\ScriptLogic Manager\Scripts C:\WINNTIS\YSVOL\sysvollacme.com\scripts C:\WINNTIS\YSVOL\sysvollacme.com\Scripticies\(31B2F340-016D-11D2-945F-00C04FB984F9)\MAC C:\WINNTIS\YSVOL\sysvollacme.com\Scripticies\(31B2F340-016D-11D2-945F-00C04FB984F9)	Discovery Date:	446/2006 6:16:02 PM 10,489,364 9,066,714 6,072,455 4,540,523 4,540,420 356,352 4,266 2,116 884 ▼

At this point, you can print the report or export it to a one of several different formats, such as Rich Text Format (*.rtf) or Microsoft Excel Worksheet (*.xls).

ES B	R3: Folder Si eport Besul	ze Report - Sor	ted By Size				
2							
-	•						
	StartDate	DomainName	ComputerNa	ParentFolder	FolderName	Size	
•	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	ScriptLogic M	10489364	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	DesktopAuth	9068714	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	MS Updates	6072456	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	Scripts	4540523	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	scripts	4540420	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	Services	356352	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	SecEdit	4266	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	MACHINE	2116	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	SecEdit	884	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	RemoteInstall	40	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	{31B2F340-0	26	
	4/6/2006	ACME	vm4-win2ksvr	C:\WINNT\SY	{6AC1786C-0	22	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	Docs	0	
	4/6/2006	ACME	vm4-win2ksvr	C:\Program F	Logs	0	
	4/6/2006	ACME	um Amin 2 vor	C-\Program F	Reports	n	

• To see the query that built the report, open the **Query** tab.



7. When you are finished, close the **Print Preview** window.

Other standard reports you could run on our discovered data are located in **Global Reports**. Take a few minutes to look at the other types of reports you can run, which also gives you a sense of the types of data you need to discover to run specific reports.



SUMMARY

In this Quick Start you discovered data on your computer, and then generated a Global report. To learn more about Enterprise Security Reporter, please consult online help, the *Discovery Guide*, or the *Reporting Guide*.

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

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

UNINSTALLING THE DISCOVERY ENGINE

If you need to uninstall the Discovery Engine, type the following at the command line on the computer on which it is installed:

```
C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\Installutil.exe" /u ESR3DiscoveryEngine.exe
```

A

Active Directory, 5

С

changing TCP port, 23

D

Database Maintenance Utility starting, 18 Discovery Console starting, 18 discovery database connecting to, 23 setting update frequency, 36 Discovery Engine installing, 22 discovery groups, 6 downloading Enterprise Security Reporter, 8

F

file extensions .ldf, 21 .mdf, 21

I

installing Discovery Engine, 22 Discovery Service, 22

L

license agreement, 10, 14 license file applying, 18

Ν

NTFS permissions, 5

R

Reporting Console configuring for the Non-Admin user, 24 starting, 18

S

starting Enterprise Security Reporter, 18

Т

TCP port changing, 23