

# ***ENTERPRISE SECURITY REPORTER™***



## **3ScriptLogic® Enterprise Security Reporter™ 3.0 Discovery Guide**

**SCRIPTLOGIC**

**© 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 computer-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](http://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, and Microsoft SQL Server are registered trademarks of Microsoft Corporation.

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

## 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](http://www.scriptlogic.com)

## SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at [www.scriptlogic.com](http://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

**DISCOVERY CONSOLE** ..... 3

    STARTING THE DISCOVERY CONSOLE ..... 3

    EXAMINING THE DISCOVERY CONSOLE..... 3

*Tabs* ..... 4

*Toolbar* ..... 4

*File Menu* ..... 4

*Tools Menu* ..... 5

*Help Menu* ..... 5

*Status Bar* ..... 6

    INSTALLING THE DISCOVERY ENGINE ..... 6

    CONNECTING TO THE DISCOVERY DATABASE..... 8

    SETTING GLOBAL DISCOVERY OPTIONS..... 8

*Excluding Paths on All Computers*..... 8

*Including/Excluding Registry Keys on All Computers*..... 9

    CONFIGURING DOMAINS FOR DISCOVERY ..... 11

*Adding Domains* ..... 12

*Selecting the Discovery Domain Controller* ..... 12

*Selecting Items for Domain Discovery* ..... 14

*Selecting Active Directory Attributes* ..... 15

*Selecting Organizational Units* ..... 17

*Setting Domain Discovery Options* ..... 18

    CONFIGURING COMPUTERS FOR DISCOVERY..... 20

*Adding Computers* ..... 21

*Searching for Computers*..... 22

*Selecting Items for Computer Discovery* ..... 25

*Including/Excluding Paths in/from the Discovery*..... 27

*Selecting Registry Keys for Discovery*..... 29

*Setting Computer Discovery Options* ..... 30

    USING DISCOVERY GROUPS ..... 31

*Creating a Discovery Group* ..... 32

*Adding Domains to a Discovery Group*..... 33

*Adding Computers to a Discovery Group* ..... 33

*Selecting Items for Group Discovery*..... 34

*Setting Group Discovery Options*..... 36

*Overriding Group Discovery Settings* ..... 38

    EXPORTING DISCOVERY CONFIGURATION SETTINGS ..... 39

    IMPORTING DISCOVERY CONFIGURATION SETTINGS ..... 39

    USING ENTERPRISE SCOPES..... 40

*Adding Enterprise Scopes*..... 40

*Adding Computers to an Enterprise Scope*..... 41

    SCHEDULING DISCOVERY JOBS ..... 41

    LAUNCHING A DISCOVERY ..... 43

    MANAGING THE DISCOVERY SERVER..... 44

*Viewing Server Information*..... 45

    MANAGING DISCOVERY JOBS ..... 46

    MANAGING LICENSES ..... 47

    USING THE COMMAND-LINE UTILITY: DISCOVERYCMD.EXE..... 47

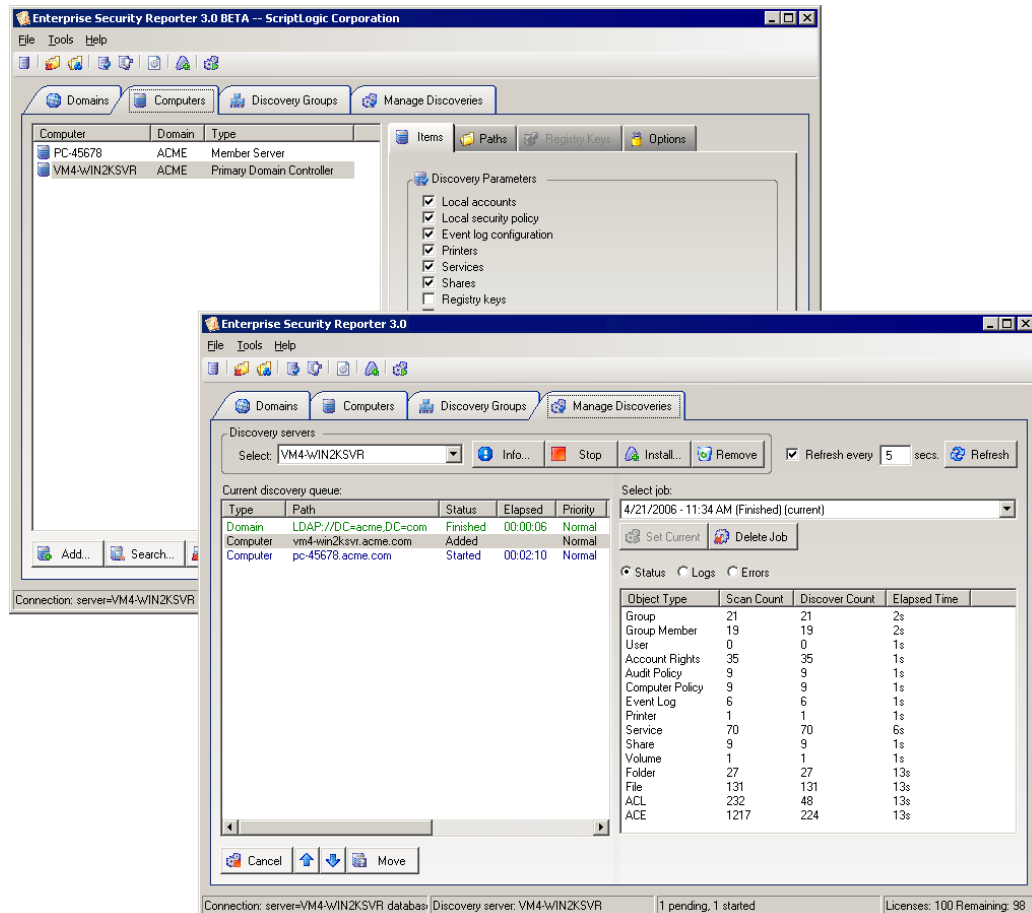
    USING THE COMMAND-LINE UTILITY: PURGEDATA.EXE ..... 48

<b>DATABASE UTILITIES .....</b>	<b>49</b>
STARTING THE DATABASE UTILITIES .....	50
CREATING A NEW DATABASE .....	50
REMOVING AN EXISTING DATABASE.....	52
INCREASING DATABASE SIZE .....	52
SHRINKING A DATABASE.....	53
RUNNING AN SQL SCRIPT .....	54
VIEWING DATABASE STATISTICS .....	54
ATTACHING A DATABASE .....	55
DETACHING A DATABASE .....	56
TRUNCATING THE TRANSACTION LOG .....	56
SAVING CONNECTION INFORMATION .....	57
PERFORMING DATABASE MAINTENANCE.....	57
RESETTING DATABASE SECURITY .....	58
SWITCHING THE SERVER SECURITY MODE.....	59
SETTING THE 'SA' PASSWORD .....	60
MOVING A DATABASE TO ANOTHER SERVER .....	60
USING THE COMMAND-LINE UTILITY: DBWIZARD.EXE .....	61
<i>Specifying Database Connection Information.....</i>	<i>61</i>
<i>Creating a Database.....</i>	<i>61</i>
<i>Dropping a Database .....</i>	<i>61</i>
<i>Running a SQL Script.....</i>	<i>61</i>
<i>Running All Maintenance Tasks .....</i>	<i>62</i>
<i>Running Checkpoint and Truncate Log.....</i>	<i>62</i>
<i>Shrinking the Database Files .....</i>	<i>62</i>
<i>Resetting Database Security.....</i>	<i>62</i>
<i>Controlling Wizard Behavior .....</i>	<i>62</i>
<b>TROUBLESHOOTING .....</b>	<b>63</b>
SETTING THE FREQUENCY OF DISCOVERY STATUS UPDATES.....	63
UNINSTALLING THE DISCOVERY ENGINE .....	63
<b>INDEX .....</b>	<b>64</b>

# 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.



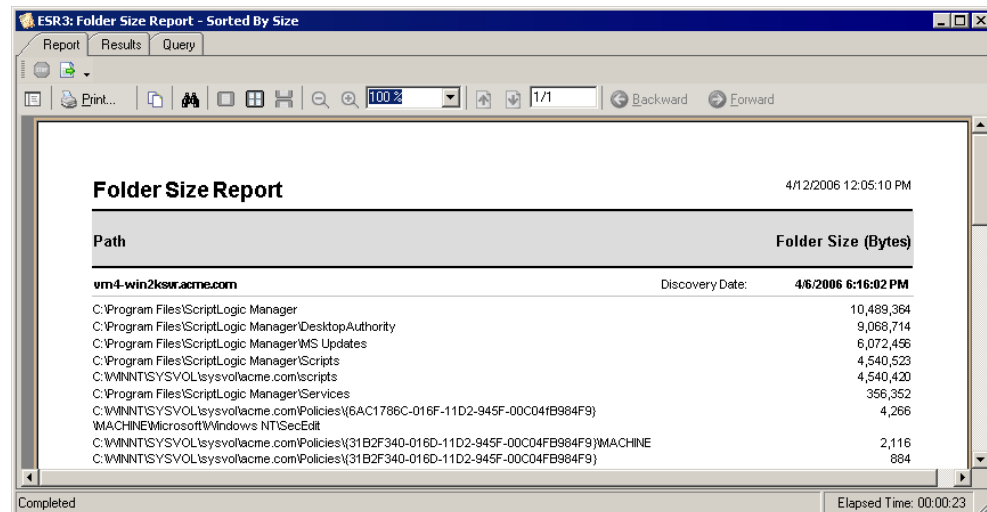
## Comprehensive Discovery

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.



# Discovery Console

Enterprise Security Reporter is designed to collect information from your servers as quickly and efficiently as possible. The processes of discovering data from your servers must be completed before you can run any reports.

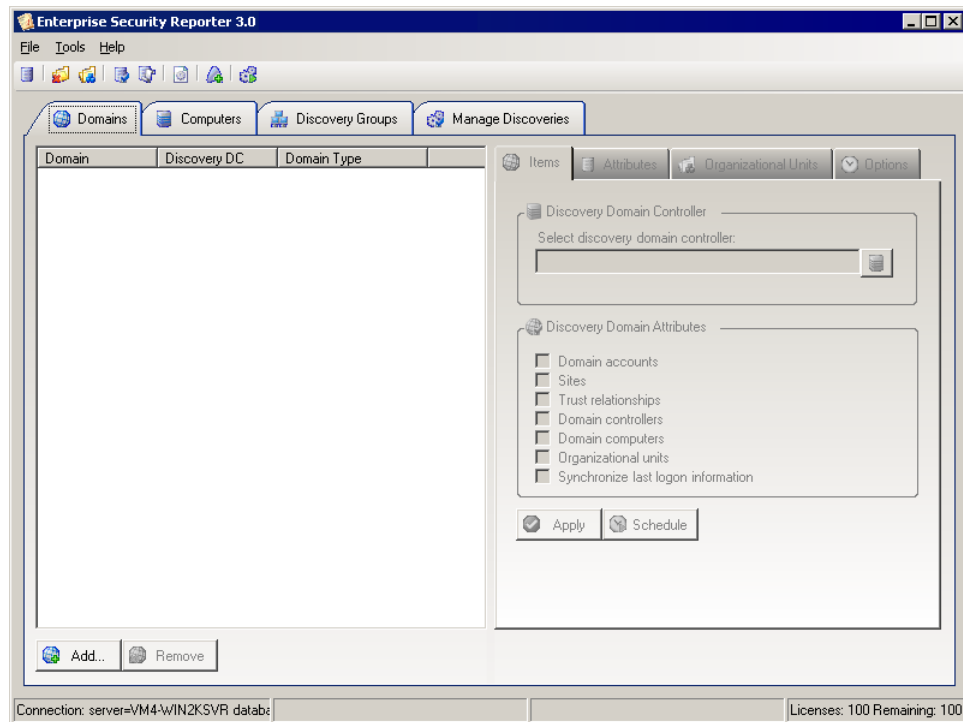
**Important:** If you have not yet done so, create the discovery and reporting databases. The discovery process cannot be configured until this step has been completed. See *Creating a New Database*.

## STARTING THE DISCOVERY CONSOLE

- ▶ Click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **Enterprise Security Reporter 3**, and then select **Discovery Console**.



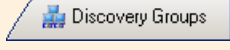
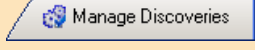
## EXAMINING THE DISCOVERY CONSOLE

After starting the Discovery Console, you see the main application window where you can perform all the actions necessary to configure and manage the discovery process.













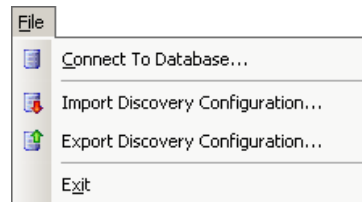
## Tabs

Tab	Description
 Domains	Configure domains for discovery. See <i>Configuring Domains for Discovery</i> .
 Computers	Configure computers for discovery. See <i>Configuring Computers</i> .
 Discovery Groups	Create and configure groups of domains and servers for discovery. See <i>Using Discovery Group</i> .
 Manage Discoveries	Monitor current discovery and schedule discoveries. See <i>Launching a Discovery</i> .

## Toolbar

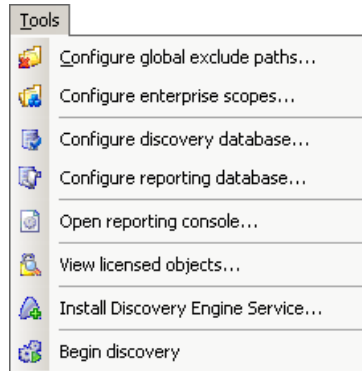
Icons	Description
	Connect to the discovery server and database. See <i>Installing the Discovery Engine</i> .
	Set global options for discovery. See <i>Setting Global Discovery Options</i> .
	Open the <b>Database Maintenance Utility</b> where you can manage the discovery database. See <i>Starting the Database Utilities</i> .
	Open the <b>Database Maintenance Utility</b> where you can manage the reporting database. See <i>Starting the Database Utilities</i> .
	Open the <b>Enterprise Scopes</b> dialog box where you can group multiple computers together into a scope against which you can run a single report.
	Open the <b>Reporting Console</b> where you can select reports to run against the discovery data you collected. See <b>Error! Reference source not found.</b>
	Install the Discovery Engine. See <i>Installing the Discovery Engine</i> .
	Launch the discovery process for the selected domain(s) or group(s). See <i>Launching a Discovery</i> .

## File Menu



Menu Option	Description
Connect to Database	Connect to the discovery server and database. See <i>Installing the Discovery Engine</i> .
Import Discovery Configuration	Load discovery settings from an ESR 3 Discovery Configuration (*.xdc) file. See <i>Exporting Discovery Configuration Settings</i> .
Export Discovery Configuration	Save discovery settings to an ESR 3 Discovery Configuration (*.xdc) file. See <i>Importing Discovery Configuration Settings</i> .
Exit	Exit Enterprise Security Reporter.

## Tools Menu



Menu Option	Description
Configure global exclude paths	Set global options for discovery. See <i>Setting Global Discovery Options</i> .
Configure discovery database	Open the <b>Database Maintenance Utility</b> where you can manage the discovery database. See <i>Starting the Database Utilities</i> .
Configure reporting database	Open the <b>Database Maintenance Utility</b> where you can manage the reporting database. See <i>Starting the Database Utilities</i> .
Configure enterprise scopes	Open the <b>Enterprise Scopes</b> dialog box where you can group multiple computers together into a scope against which you can run a single report. See <i>Using Enterprise Scopes</i> .
Open reporting console	Open the <b>Reporting Console</b> where you can select reports to run against the discovery data you collected. See the <i>Reporting Guide</i> .
View licensed objects	Manage the computers applied to your site license. See <i>Managing Licenses</i> .
Install Discovery Engine Service	Install the Discovery Engine. See <i>Installing the Discovery Engine</i> .
Begin discovery	Launch the discovery process for the selected domain(s) or group(s). See <i>Launching a Discovery</i> .

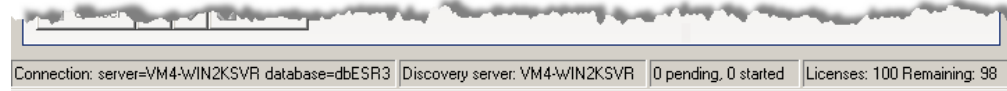
## Help Menu



Menu Option	Description
Contents	Open online help.
About	View information about the version of Enterprise Security Explorer installed on your computer, to apply a license file, or to visit the ScriptLogic website.

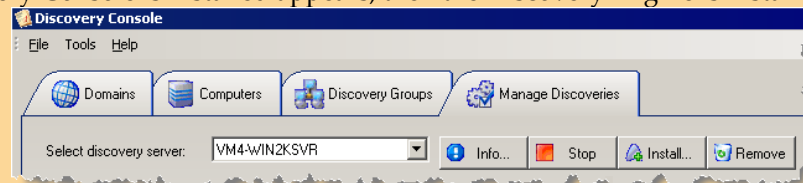
## Status Bar

The status bar at the bottom of the window displays the connection server and database, the discovery server, the number of pending and started discoveries, and the number of total and remaining licenses.



## 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 on 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.

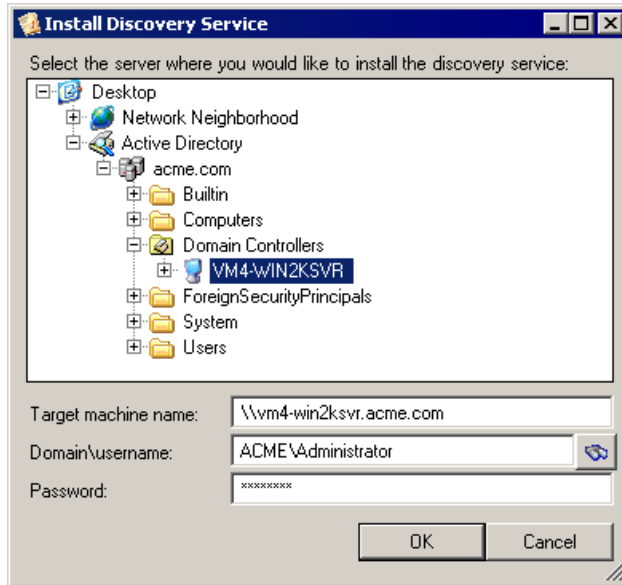
1. Click . Alternatively, select **Install Discovery Engine Service** from the **Tools** menu. The **Install Discovery Service** box opens.

**Note:** You also can install the Discovery Engine on the **Manage Discoveries** tab. See *Managing the Discovery Server*.

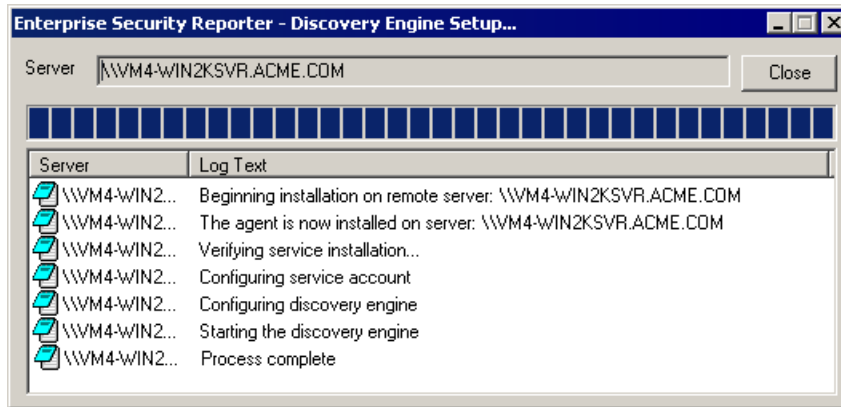
2. In the **Target machine name** box, type the name of the computer where the Discovery Console is installed, or select the computer from the list.
3. In the **Domain\username** box, type the account name that can run the Discovery Engine, or click  to locate an account name.

- In the **Password** box, type the password.

**Important:** You must use an account that has a password. For security reasons, Enterprise Security Reporter will not use a blank password.



- Click **OK**. The **Discovery Engine Setup** window shows the progress of the installation of the discovery engine and service.

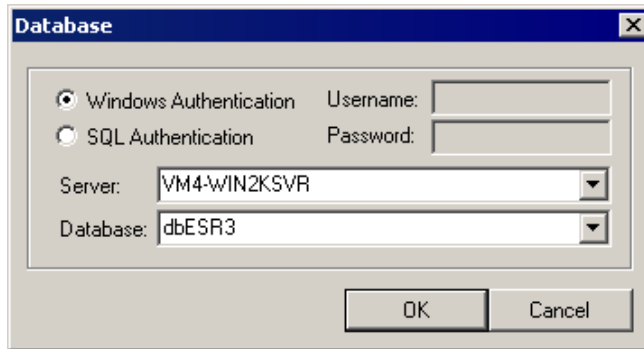


- When you see **Process complete**, click **Close**.

## 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**.


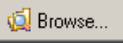
## SETTING GLOBAL DISCOVERY OPTIONS


Some settings that affect the discovery process can be set system wide. These options can be accessed by selecting **Configure global exclude paths** from the **Tools** menu.

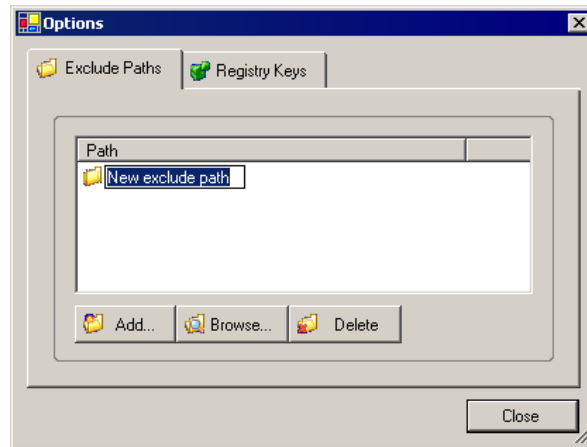
### Excluding Paths on All Computers

Although you can exclude particular paths on a computer-by-computer basis, you may want to exclude folders on all computers that match a certain name, such as **Temporary Internet Files**, **System 32**, or **Winnt**.

**Important:** If you exclude a path and there is a shared folder within that path, those folders are included in the discovery if the **All folders available through public shares** check box is selected on the **Items** tab for a specific computer. See *Selecting Items for Computer Discovery*.

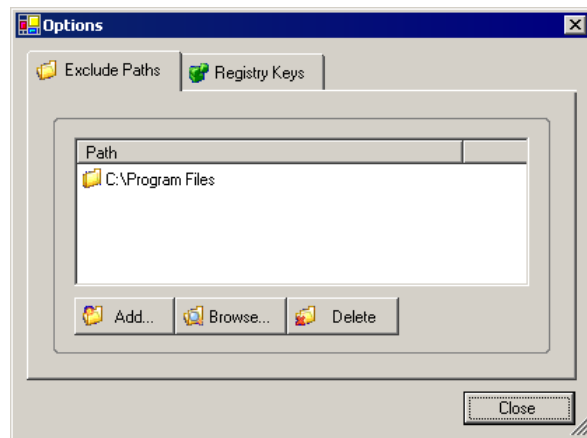
1. Click  or choose **Configure global exclude paths** from the **Tools** menu. The **Options** box opens to the **Exclude Paths** tab.
2. You can add a path by typing the path or by selecting from a list.
  - To select paths from a list, click . The **Browse for Folder** list appears. Select the path, and then click **OK**.


- To add a path by typing the name, click . With **New exclude path** selected, type the path, and then click off the path.



**Important:** The folder names must match exactly (except for case), and no wild cards are permitted. All subfolders are excluded from the discovery.


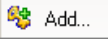
The path displays in the list.



- To remove a selected path from the list, click .

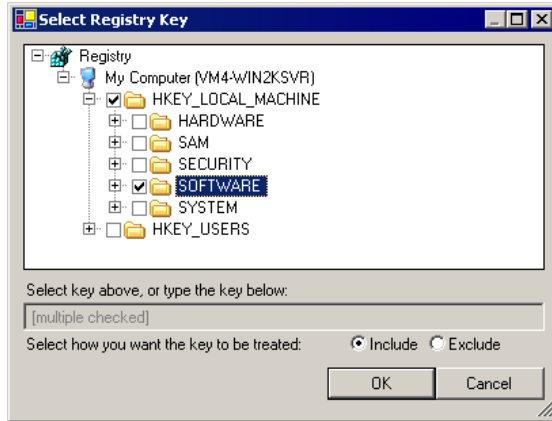
## Including/Excluding Registry Keys on All Computers

Although you can include or exclude particular registry keys on a computer-by-computer basis, you may want to include or exclude registry keys on all computers.

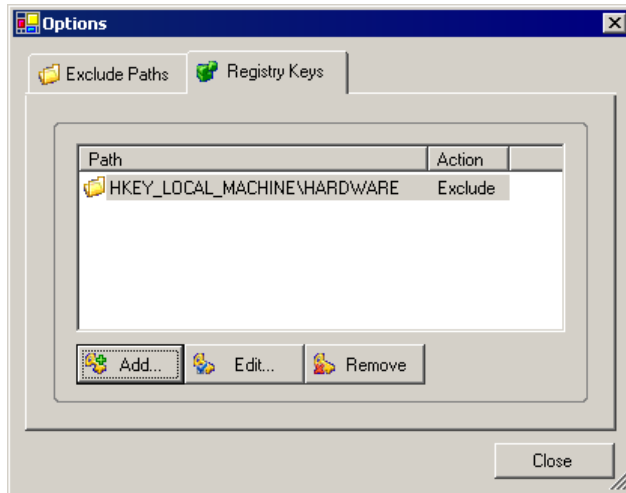
1. Click  or choose **Configure global exclude paths** from the **Tools** menu. The **Options** dialog box opens to the **Exclude Paths** tab.
2. Open the **Registry Keys** tab, and then click . The **Select Registry Key** list box appears.



- Expand the list to locate the key to add or type a path in the **Select key above, or type the key below** box.

**Note:** If you select a key from the list, the **Select key above, or type the key below** box becomes unavailable.



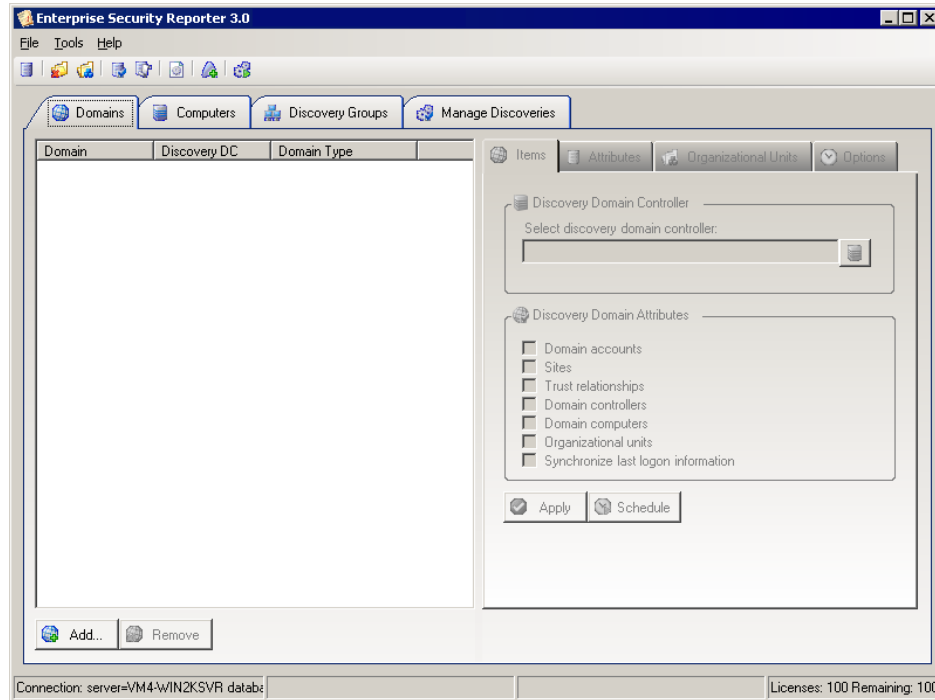
- Select whether to include or exclude the key from the discovery.
- Click **OK**. The key displays in the **Path** column. The **Action** column indicates if the key is included or excluded.

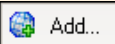
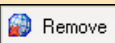
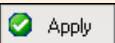
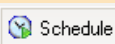


- To change the action (include or exclude) on a selected key, click .
- To delete selected keys from the list, click .



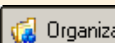
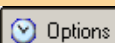
## CONFIGURING DOMAINS FOR DISCOVERY

At the heart of the discovery process are the types of data to be discovered from a selected domain. From the **Domains** tab, you can configure one or more domains at a time by holding down the CTRL or SHIFT keys, and then selecting the domains to configure.



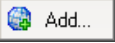
Buttons	Description
	Add a domain to the list. See <i>Adding Domains</i> .
	Remove selected domains.
	Save the selections for the current discovery.
	Schedule a discovery. See <i>Scheduling Discovery Jobs</i> .

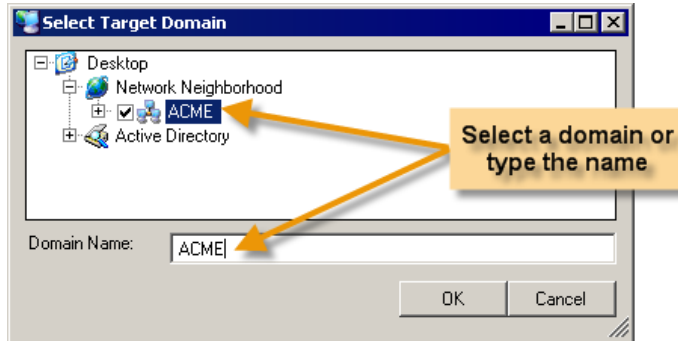
After adding domains and selecting the discovery domain controller, use these four tabs to configure the domain discovery process:

Tab	Description
	Select domain items to include in the discovery. See <i>Selecting Items for Domain Discovery</i> .
	Select Active Directory attributes to include in the discovery. See <i>Selecting Active Directory Attributes</i> .
	Select organizational units to include in the discovery. See <i>Selecting Organizational Units</i> .
	Set options for the domain discovery process. See <i>Setting Domain Discovery Options</i> .

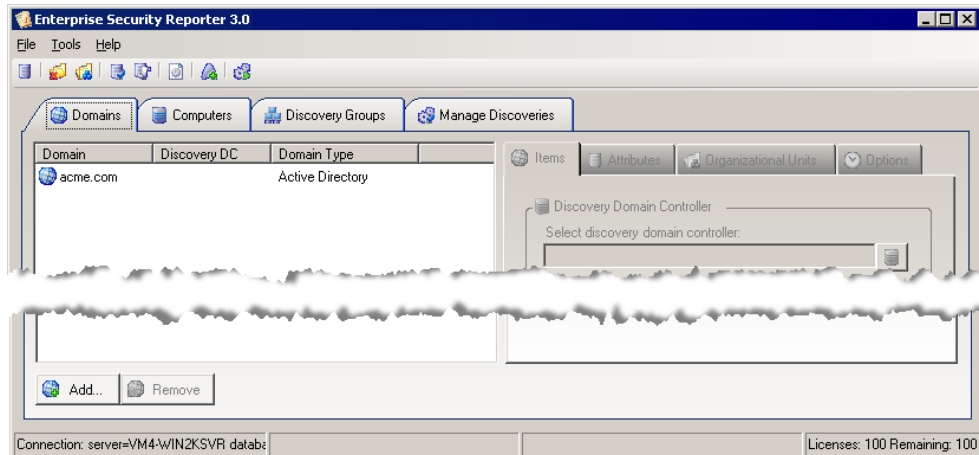


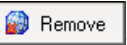
## Adding Domains

1. From the Discovery Console, open the **Domains** tab, and then click . The **Select Target Domain** box appears. Expand the list to view the domains.



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





- To remove selected domains, click .

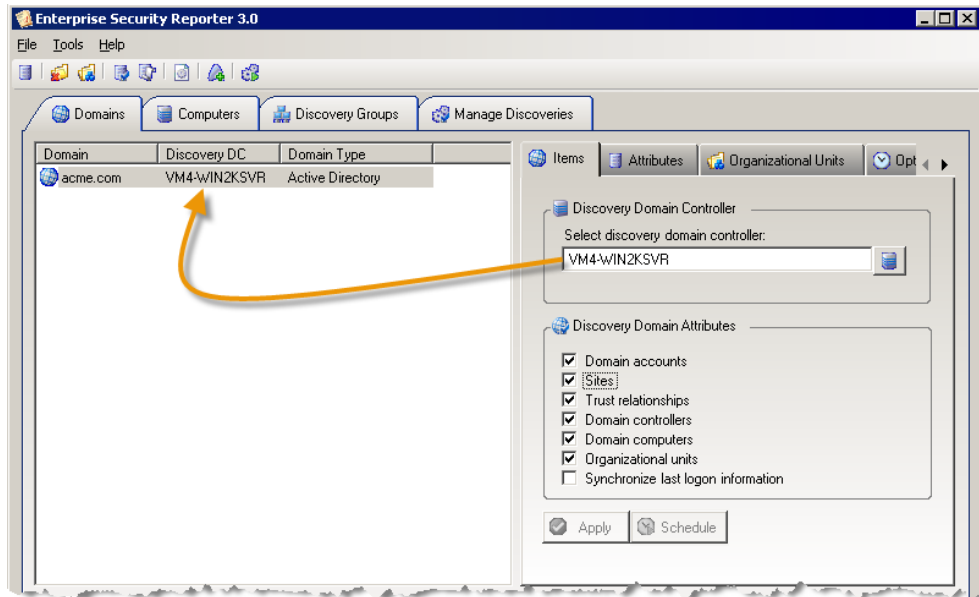
**Important:** When you remove a domain from the list, all discovery data for that domain is deleted.

## Selecting the Discovery Domain Controller

When a discovery is performed, the data collected is stored in the discovery database, which is located on the discovery domain controller.

1. On the **Domains** tab, select the domain in the left pane. The **Items** tab becomes available.
2. In the **Select discovery domain controller** box, type the name of the domain controller or click  to locate a domain controller.

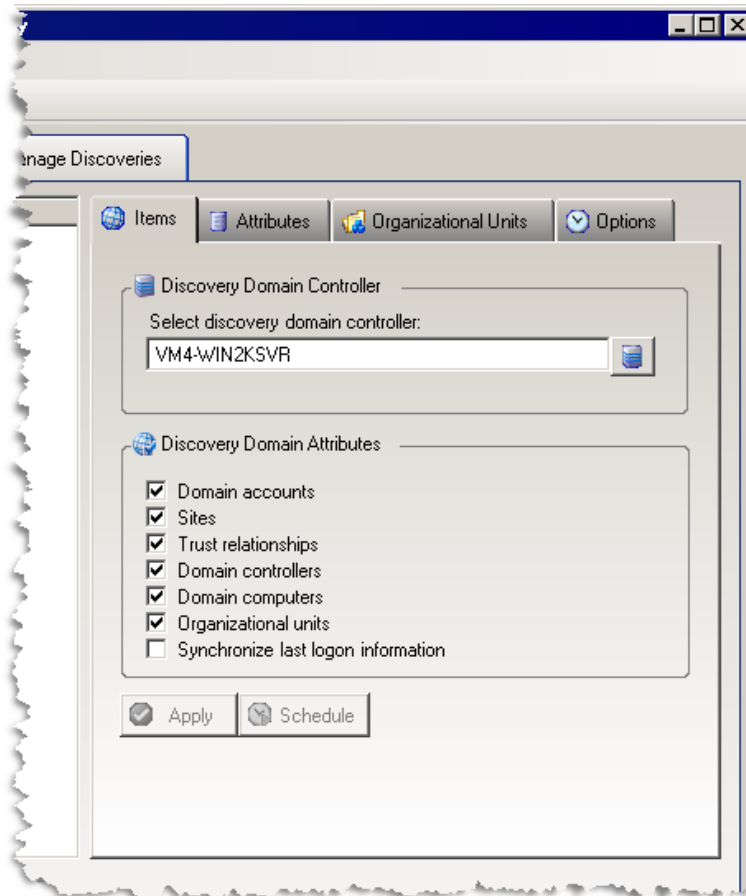
3. Click . The selected discovery domain controller is listed in the **Discovery DC** column in the left pane.



## Selecting Items for Domain Discovery

The **Items** tab contains types of data that you can select to include in the discovery process.

1. Open the **Domains** tab, and then select the domain. The **Items** tab becomes available.



**Domain accounts**

By default, domain accounts are included in the discovery. To exclude domain accounts, clear the check box.

**Sites**

By default, sites are included in the discovery. To exclude sites, clear the check box.

**Trust relationships**

By default, trust relationships are included in the discovery. To exclude trust relationships, clear the check box.

**Domain controllers**

By default, domain controllers are included in the discovery. You can configure the discovery parameters for the domain controller on the **Computers** tab. See *Configuring Computers*. To exclude domain controllers, clear the check box.

**Domain computers**

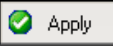
By default, domain computers are included in the discovery. You can configure the discovery parameters for each computer on the **Computers** tab. See *Configuring Computers*. To exclude domain computers, clear the check box.

**Organizational units**

By default, organizational units are included in the discovery. You can select specific organizational units on the **Organizational Units** tab. See *Selecting Organizational Units*. To exclude organizational units, clear the check box.


**Synchronize last logon information**

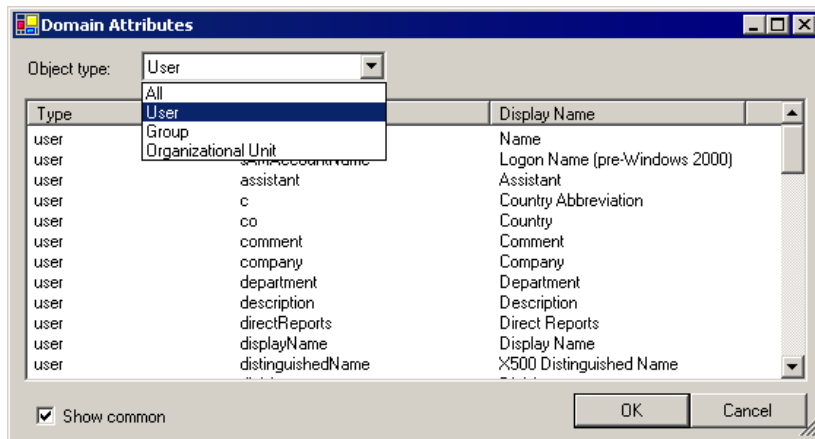
Select to contact each domain controller in the domain, and retrieve the last log on and log off dates/times for all users.

2. Make the selections to define the discovery process, and then click .

### Selecting Active Directory Attributes

When discovering the domain controller for an Active Directory domain, you can select additional LDAP attributes for group and user accounts. Since these additional LDAP attributes are only gathered when discovering the domain controller of an Active Directory domain, you must set that domain controller as the discovery domain controller. See *Selecting the Discovery Domain Controller*.

1. Open the **Domains** tab, select a domain, open the **Attributes** tab, and then click . The **Domain Attributes** box appears.
2. From the **Object type** list, select the type of attributes to display. The choices are **All**, **User**, **Group**, or **Organizational Unit**.



**Show common**

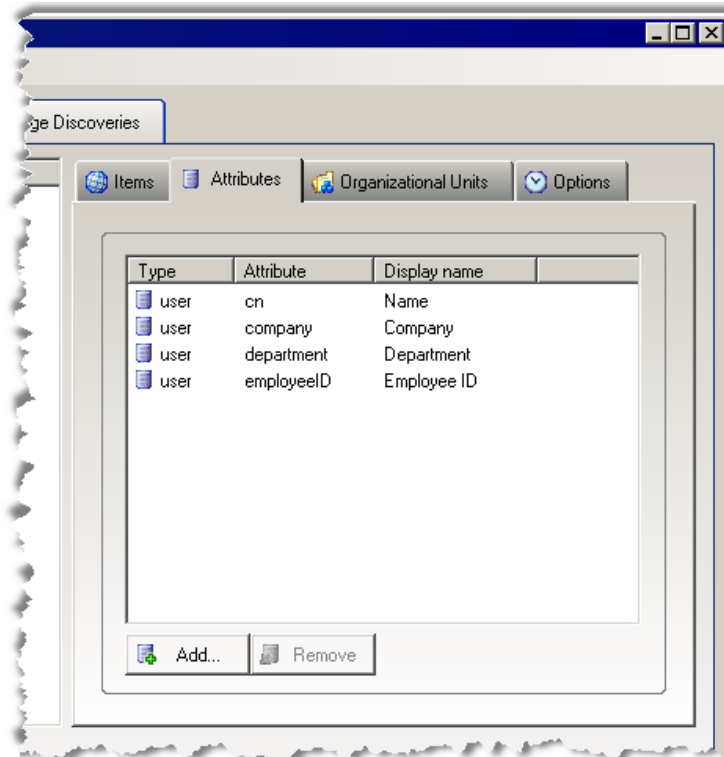
Select to show only attributes in the list that have value in the **Display Name** column.

**Important:** If you select an attribute for which there is no value, the attribute does not appear on a report, but appears to be part of the discovery process. To be sure you select only attributes for which there is a value, select the **Show common** check box, or use the ADSI Edit utility that is provided with Windows XP/2000/2003.

To use the ADSI Edit utility:


1. Click **Start**, and then choose **Run**.
  2. In the **Open** box, type **mmc**, and then press **Enter**.
  3. From the **File** menu, choose **Add/Remove Snap-in**.
  4. Click **Add**, and then select **ADSI Edit** from the list of snap-ins.
  5. Click **Add**, and then click **Close**.
  6. Click **OK**, and then connect to the domain you want to check for attributes.
3. Select each attribute that you want to discover, and then click **OK**. The selected attributes display.

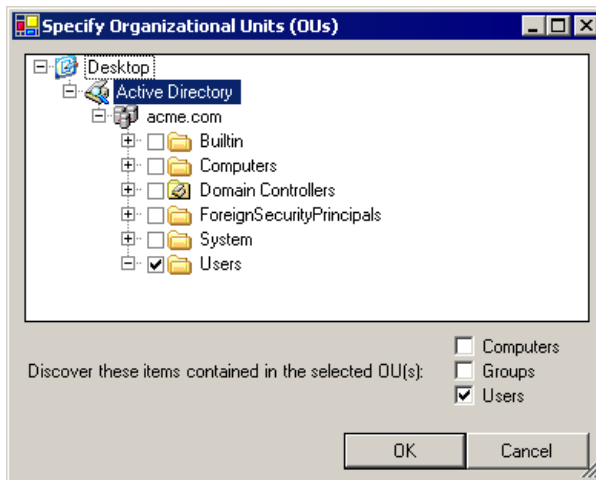
**Note:** When the domain controller is discovered, the selected attributes are added to the **tblGroupAttribute** and **tblUserAttribute** tables.



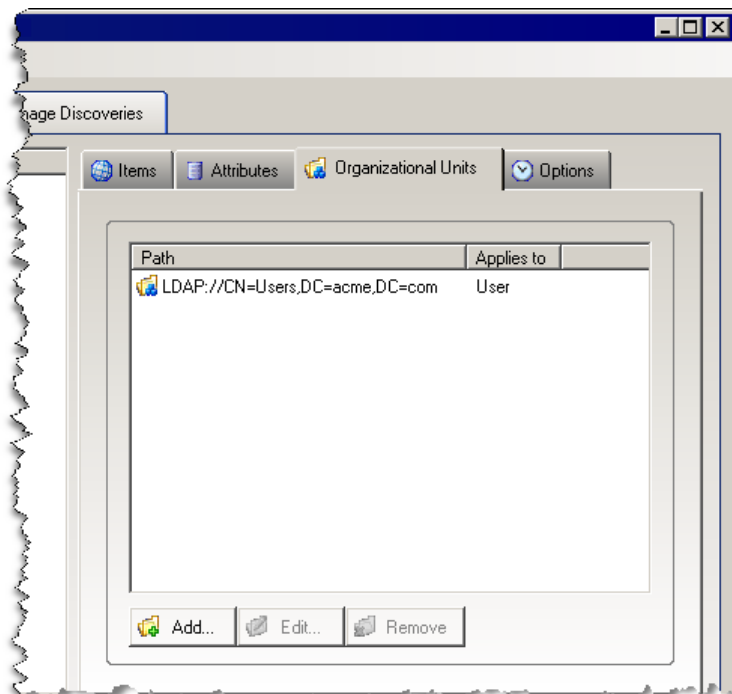
- To remove selected attributes from the list, click .


## Selecting Organizational Units


1. From the **Discovery Console**, open the **Domains** tab, select the domain, open the **Organization Units** tab, and then click .
2. Expand the list, and then select the organizational units to discover.
3. Within the selected organizational units, choose to discover **Computers**, **Groups**, or **Users** by selecting the corresponding check box.

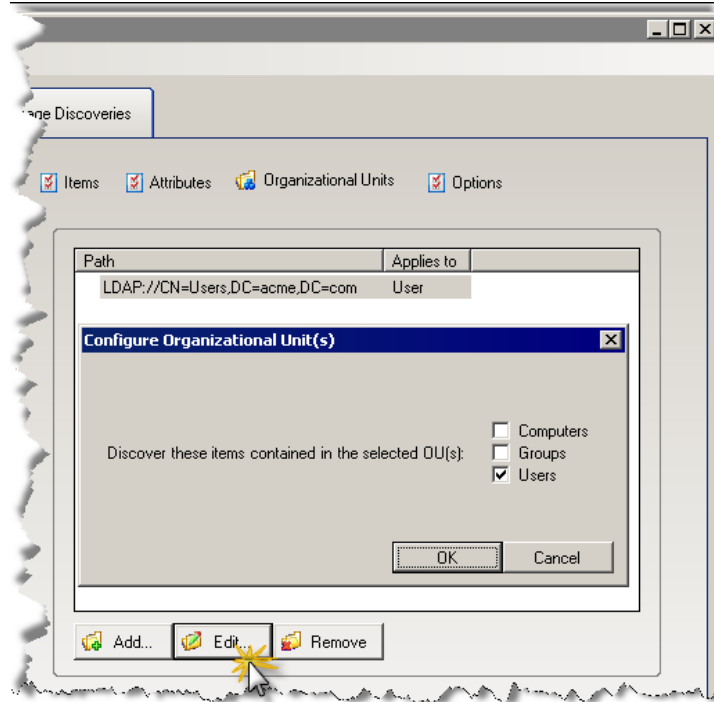


4. Click **OK**. The selected organizational units display.



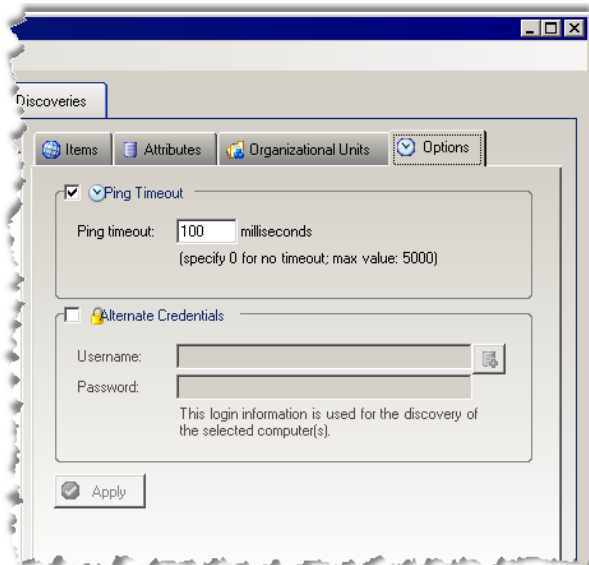
- To remove selected organizational units from the discovery, click .

- To modify selected organizational units, click . The **Configure Organizational Unit(s)** box displays the current selection. You can choose to change the items discovered in the selected OU. The choices are **Computers**, **Groups**, or **Users**.



### Setting Domain Discovery Options

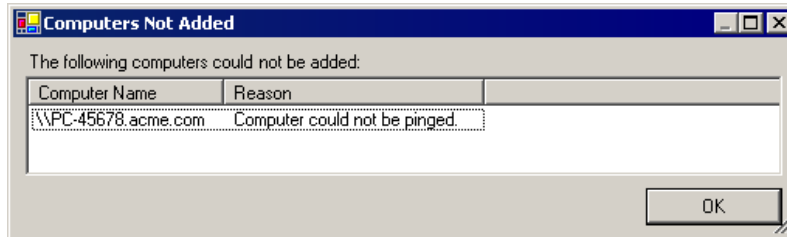
- ▶ From the **Discovery Console**, open the **Domains** tab, select the domain, and then open the **Options** tab.



**Ping Timeout**


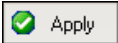
By default, the discovery engine abandons a discovery on a computer after 100 milliseconds. To change the value, type a number between 0 and 5000. If you do not want the ping to time out, type 0.

For example, if you are adding a computer that is not active, the ping times out at the value you specify.

 **Alternate Credentials**

Select to specify the user name and password of the account whose security credentials you wish to use to discover a computer. You can specify one set of credentials for one computer and another set for a different computer. This process creates a network connection to a remote computer in the same way a drive is mapped to a remote computer. If you already have a connection established to the computer you wish to discover, the discovery agent uses the credentials of the established connection instead of establishing a new connection.

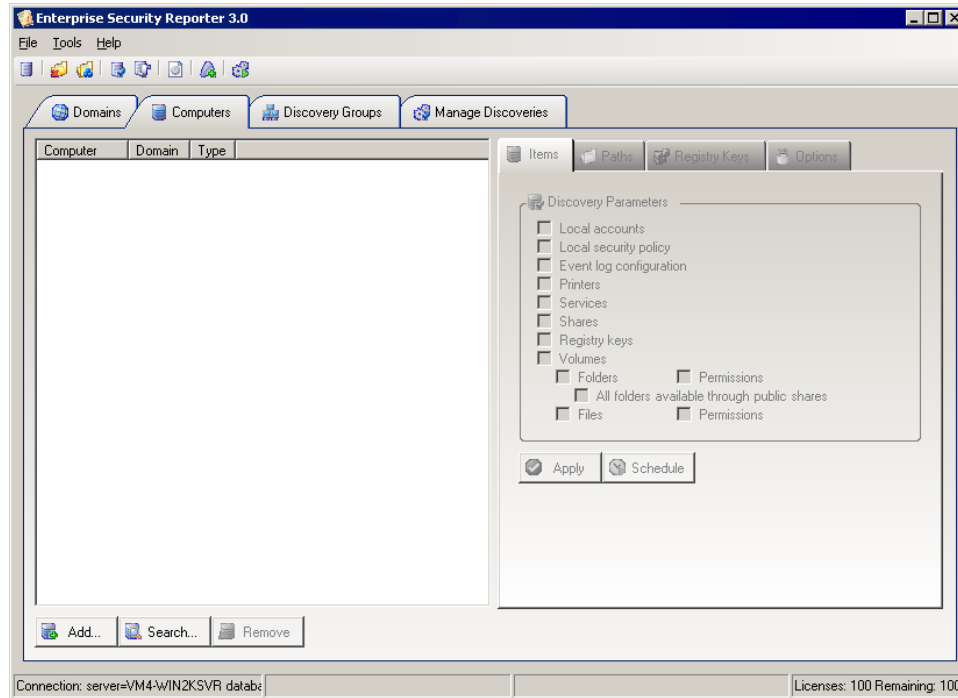
**Note:** By default, Enterprise Security Reporter connects to a computer using the credentials of the logged-in user.


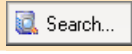
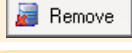
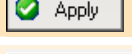
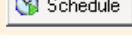
1. In the **User Name** box, type a user name, or click  to select a name from the **Select Users or Groups** list.
2. In the **Password** box, type the password.
3. Click .







## CONFIGURING COMPUTERS FOR DISCOVERY

If you select to discover domain controllers and domain computers on the **Items** tab, you can configure the parameters to discover on the **Computers** tab.



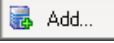
Button	Description
 Add...	Add a computer to the list. See <i>Adding Computers</i> .
 Search...	Search for computers to add to the list. See <i>Searching for Computers</i> .
 Remove	Remove selected computers from the list.
 Apply	Save the selections for the current discovery.
 Schedule	Schedule a discovery. See <i>Scheduling Discovery Jobs</i> .

After adding computers, use these four tabs to configure the computer discovery process:

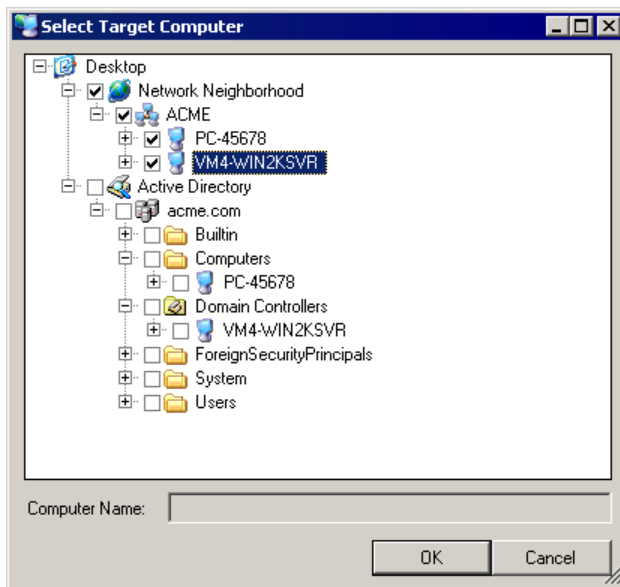
Tab	Description
 Items	Select items to include in the discovery. See <i>Selecting Items for Computer Discovery</i> .
 Paths	Specify paths to include in or exclude from the discovery. See <i>Including/Excluding Paths in/from the Discovery</i> .
 Registry Keys	Select registry keys to include in or exclude from the discovery. See <i>Selecting Registry Keys for Discovery</i> .
 Options	Set options for the computer discovery. See <i>Setting Computer Discovery Options</i> .

## Adding Computers

**Note:** Only computers that can be pinged can be added to the list. To set the ping timeout, see *Setting Domain Discovery Options*.

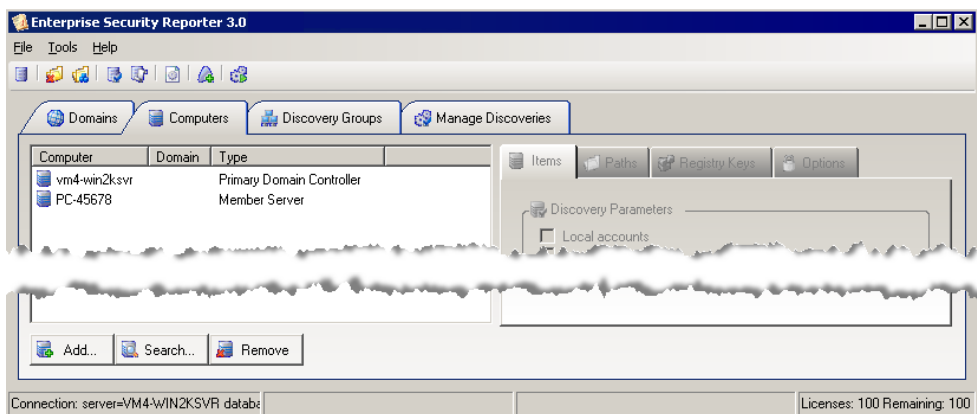
1. Open the **Computers** tab, and then click . The **Select Target Computer** box appears.
2. In the **Computer Name** box, type a single computer name, or select multiple computers from the list.


**Note:** Once you select a computer from the list, the **Computer Name** box becomes unavailable.



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

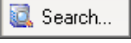
**Note:** If a computer cannot be added, an error box displays the name of the computer and the reason.

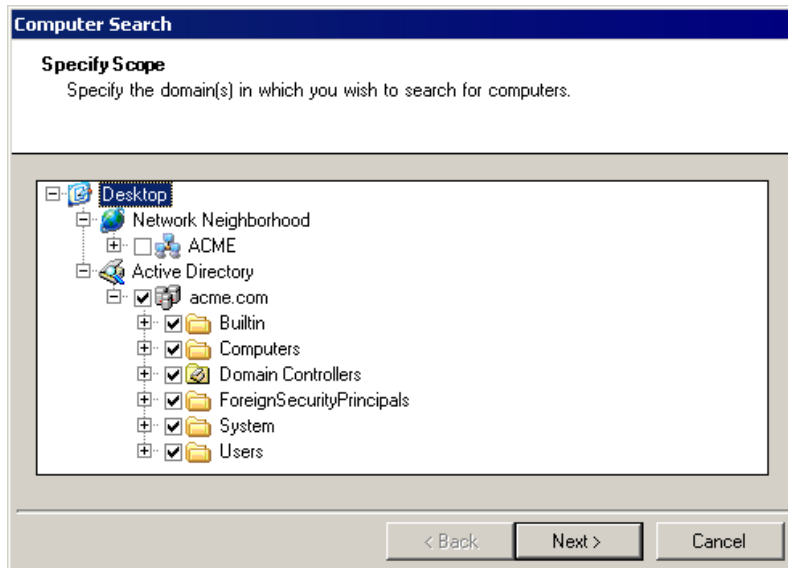


- To remove selected computers, click .

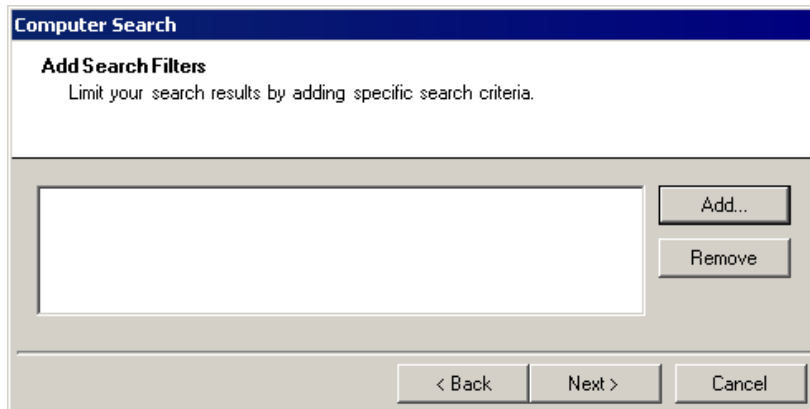
## Searching for Computers

Another way to add computers is by searching for specific computers by machine type, computer name, or operating system. If you have a lot of computers, searching for computers can be a time-saver.

1. Open the **Computers** tab, and then click . The **Specify Scope** box appears.
2. Expand the list and select the domain that you want to search.

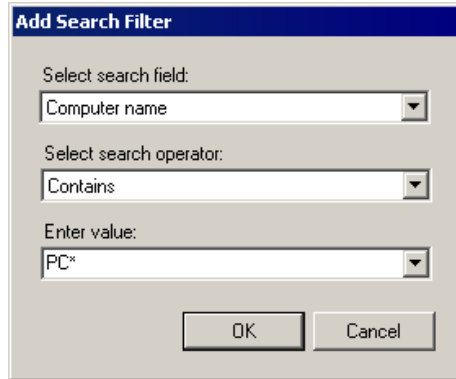


3. Click **Next**. The **Add Search Filters** box appears.

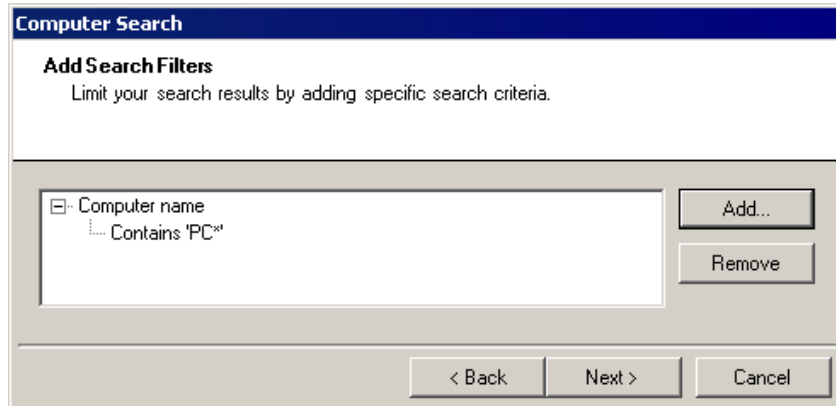


- a. If you want to search for specific computers, click **Add**. The **Add Search Filter** box appears.
- b. From the **Select Search field** list, select the field to search:
  - Operating system version
  - Machine type
  - Computer name

- c. From the **Select search operator list**, select an operator:
  - Is equal to
  - Is not equal to
  - Contains
  - Does not contain
- d. In the **Enter value** box, type the value upon which to search. Wildcards are supported.

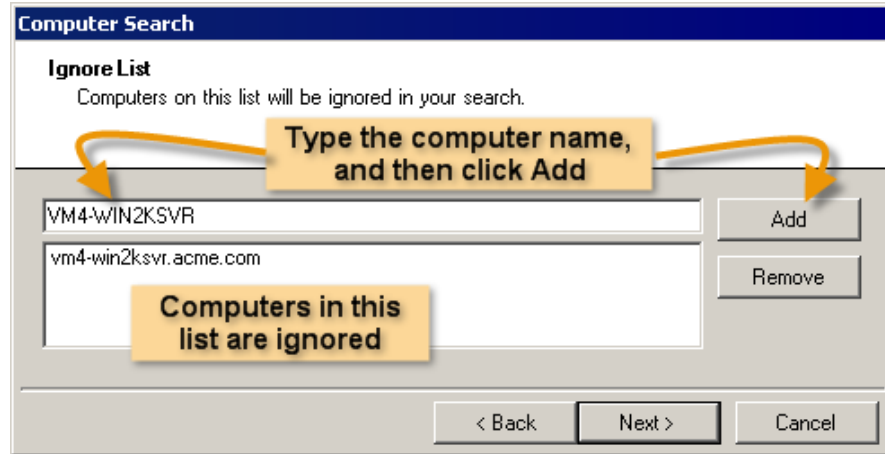


- e. Click **OK**. The search filter displays.

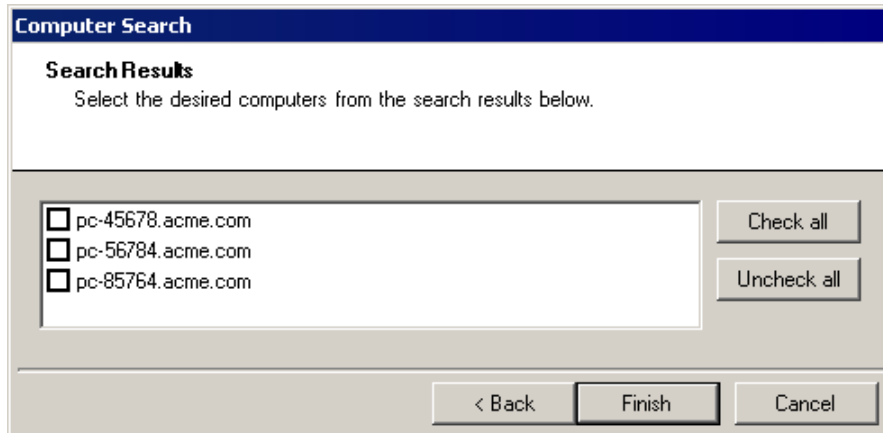


- f. Repeat these steps to add more filters.

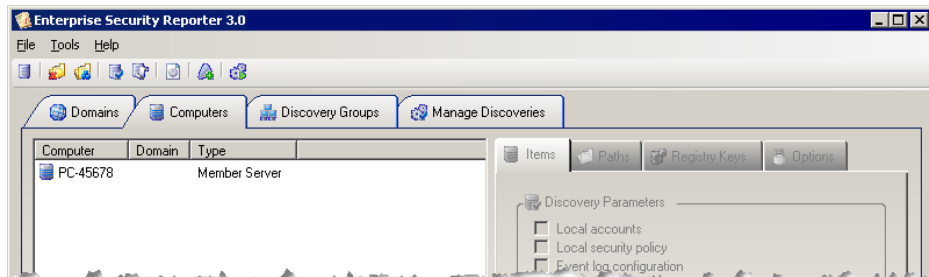
4. Click **Next**. The **Ignore List** box displays.
  - a. If you want to eliminate computers from your search, type the complete computer name in the box, and then click **Add**. The computer is added to the list.



- b. Repeat to add more computers to ignore in the search.
5. Click **Next**. The search begins. When the search is complete, a list of computers appears.

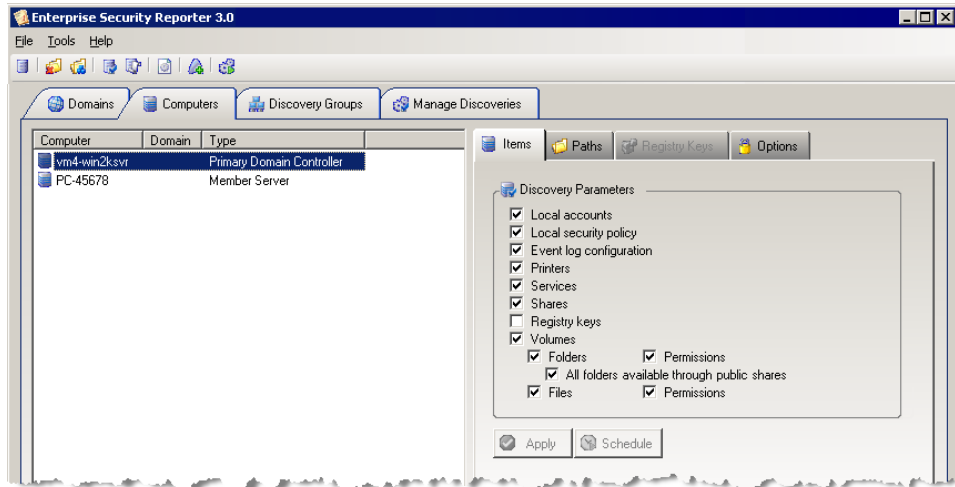


- To select individual computers, select the corresponding check box.
  - To select all the computers, click **Check all**.
  - To clear the selection, click **Uncheck all** or clear the individual check box.
6. Click **Finish**. The selected computers are added to the list.



## Selecting Items for Computer Discovery

1. Open the **Computers** tab, and then select one or more computers. The **Items** tab becomes available.



2. In the Items tab, select the items in the **Discovery Parameters** area to include in the discovery.

**Local accounts**

By default, local accounts are included in the discovery on the selected computer. To exclude local accounts from the discovery, clear the check box.

**Local security policy**

By default, the local security policy is included in the discovery on the selected computer. To exclude the local security policy from the discovery, clear the check box.

**Event log configuration**

By default, the event log configuration is included in the discovery for the selected computer. To exclude the event log configuration from the discovery, clear the check box.

**Printers**

By default, all the printers that are defined on a computer are included in the discovery for the selected computer. If the printer is shared, the share name is discovered and recorded also. To exclude printers from the discovery, clear the check box.

**Services**

By default, all the services and devices that are defined on a computer are included in the discovery for the selected computer. Includes devices that show under the Devices applet in the control panel. To exclude services and devices from the discovery, clear the check box.

**Shares**

By default, all file and administrative shares on a computer are included in the discovery. To discover shared printers, select **Printers** as well. To exclude shares from the discovery, clear the check box.

**Registry Keys**

Select to catalog all the registry information that is defined on a computer and to activate the **Registry Keys** tab. By default, registry keys are not included in the discovery.

 **Volumes**

By default, all local logical drives installed on a computer are included in the discovery. To exclude volumes from the discovery, clear the check box. If cleared, the **Folders**, **Folders Permissions**, **Files**, and **Files Permissions** check boxes become unavailable.

 **Folders**

Available only if the **Volumes** check box is selected. By default, folders defined on a computer are included in the discovery. The behavior of this option is dependent on the selections made on the **Paths** and **Options** tabs. If selected, **Folders Permissions** is selected automatically. To exclude folders from the discovery, clear the check box. If cleared, the **Folders Permissions** check box becomes unavailable.

 **Permissions**

Available only if the **Volumes** and **Folders** check boxes are selected. By default, a complete list of folder permissions is included in the discovery. To exclude folder permissions from the discovery, clear the check box.

 **All folders available through public shares**

Available only if the **Folders** check box is selected. By default, only the folders and permissions under shares that are accessible to the general public (excludes administrative shares) are included in the discovery. If you want to include other folders that are not public, add the path on the **Paths** tab. To include all data, clear the check box.

 **Files**

Available only if the **Volumes** check box is selected. By default, files defined on a computer are included in the discovery. The behavior of this option is dependent on the selections made on the **Paths** and **Options** tabs. If selected, the **Files Permissions** check box is selected automatically. To exclude files from the discovery, clear the check box. If cleared, the **Files Permissions** check box becomes unavailable.

**Important:** Select the **Files** check box only if you specifically need information about the files and their associated permissions. Discovering files dramatically slows down the discovery process and increases the amount of space required to store the data.

 **Files Permissions**

Available only if the **Volumes** and **Files** check boxes are selected. By default, a complete list of file permissions is included in the discovery. To exclude file permissions from the discovery, clear the check box.

3. Click .

## Including/Excluding Paths in/from the Discovery

You can refine the discovery scope by specifying specific folders on a computer that are to be included in or excluded from the discovery. For example, you may care only about a particular folder on a computer and the rest of the data may be irrelevant to what you are working on. In this case, add the folder to the list of paths to be included and only those paths are discovered. In another scenario, you may have a folder that contains information that is of no concern to your security scan, but it is in a publicly accessible area and it takes quite a bit of time to discover the data in it. In this case, you can exclude that path from the discovery.

**Note:** This process configures paths on individual computers. To exclude a path on all servers, see *Excluding Paths on All Computers*.


**Note:** If a path is listed as an include path, only that path and the paths beneath it are discovered; the other folders on the drive are ignored.

**Important:** A path is included in the discovery even if the **All folders available through public shares** check box is selected on the **Items** tab and the path is not public.

**Important:** If you exclude a path and there is a shared folder within that path, those folders are included in the discovery if the **All folders available through public shares** check box is selected on the **Items** tab.

1. Open the **Computers** tab, and then select the computer to configure.

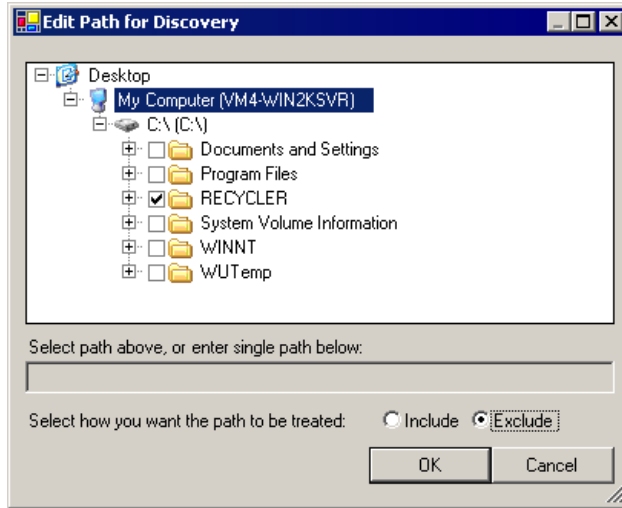
**Note:** Paths are configured on a per-computer basis. The **Paths** tab is not available if multiple computers are selected.

2. Open the **Paths** tab, and then click . The **Edit Path for Discovery** box opens.

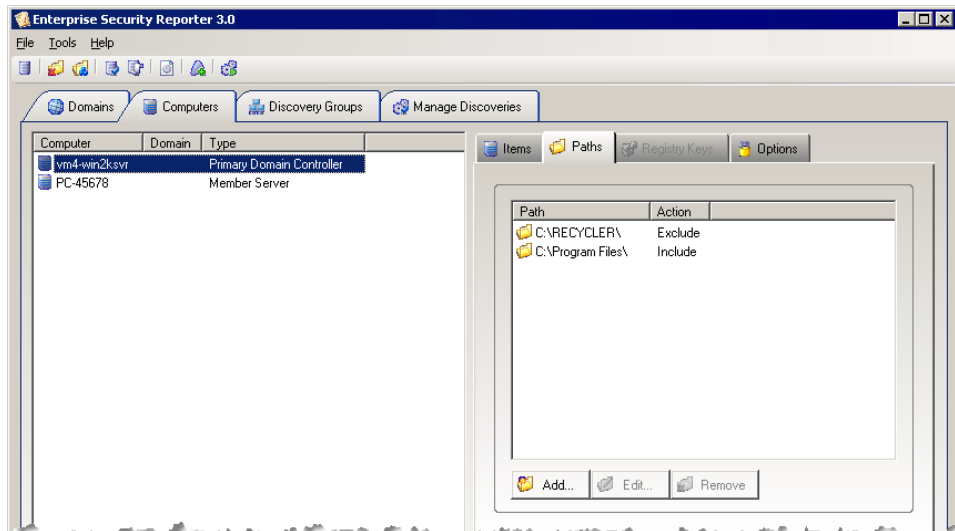


- Expand the list to locate the path to add or type a path in the **Select path above, or enter single path below** box.

**Note:** If you select a path from the list, the **Select path above, or enter single path below** box becomes unavailable.




- Select whether to include or exclude the path from the discovery.
- Click **OK**. The path displays in the **Path** column. The **Action** column indicates if the path is included or excluded.



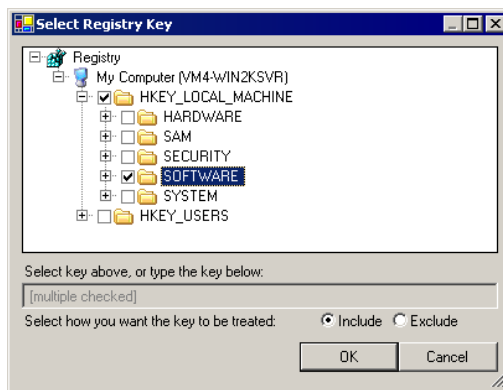
- To change the action (include or exclude) on a selected path, click **Edit...**. You also can double-click the path to toggle between **Include** and **Exclude**.
- To delete selected paths from the list, click **Remove**.

## Selecting Registry Keys for Discovery

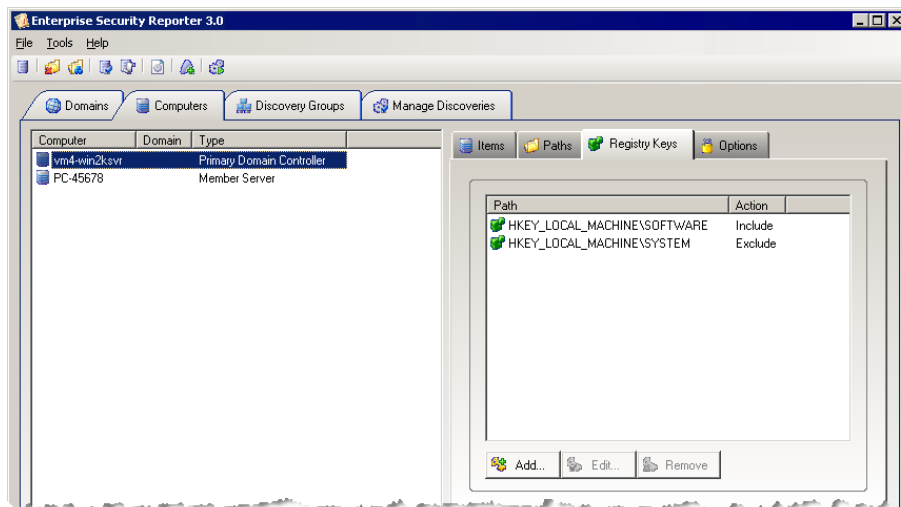
**Note:** To enable the **Registry Keys** tab, you must select the **Registry keys** check box on the **Items** tab for the selected computer.



1. Select the computer, open the **Items** tab and then select the **Registry keys** check box to enable the **Registry Keys** tab.
2. Open the **Registry Keys** tab, and then click .
3. Expand the list to locate the key to add or type a path in the **Select key above, or type the key below** box.

**Note:** If you select a key from the list, the **Select key above, or type the key below** box becomes unavailable.



4. Select whether to include or exclude the key from the discovery.
5. Click **OK**. The key displays in the **Path** column. The **Action** column indicates if the key is included or excluded.



- To change the action (include or exclude) on a selected key, click .
- To delete selected keys from the list, click .

## Setting Computer Discovery Options

The options that you set for an individual computer override any other options that were set on a global basis.

1. Open the **Computers** tab, and then select the computer to configure.
2. Open the **Options** tab.

The screenshot shows the 'Options' tab in the Enterprise Security Reporter interface. It features three main sections, each with a checkbox and a descriptive text block:


- Alternate Credentials:** Includes 'Username:' and 'Password:' text boxes. Below them is the text: "This login information is used for the discovery of the selected computer(s)." There is a small icon to the right of the password box.
- Discovery Server:** Includes a 'Discovery server:' text box. Below it is the text: "This discovery server will always be used to discover the selected computer(s)." There is a small icon to the right of the text box.
- Folder Depth:** Includes a 'Folder depth:' text box. Below it is the text: "Indicates how deep into the hierarchy you wish to discover folders. Specify '0' to discovery only the top-level paths to be discovered."

An 'Apply' button with a green checkmark icon is located at the bottom left of the options panel.

### Alternate Credentials


By default, Enterprise Security Reporter connects to a computer using the credentials of the logged-in user. Select this check box to specify the user name and password of the account whose security credentials you wish to use to discover a computer.

You can specify one set of credentials for one computer and another set for a different computer. This process creates a network connection to a remote computer in the same way a drive is mapped to a remote computer. If you already have a connection established to the computer you wish to discover, the discovery agent uses the credentials of the established connection instead of establishing a new connection.

- In the **User Name** box, type a user name, or click  to select a name. In the **Password** box, type the password.

**Discovery Server**

If you have more than one discovery server, by default, Enterprise Security Reporter selects the next computer in the queue and assigns it to the first available discovery server. Select this check box to assign a specific discovery server for the discovery of the selected computer.

- In the **Discovery Server** box, type the name of the discovery server or click  to locate a discovery server.

**Folder Depth**

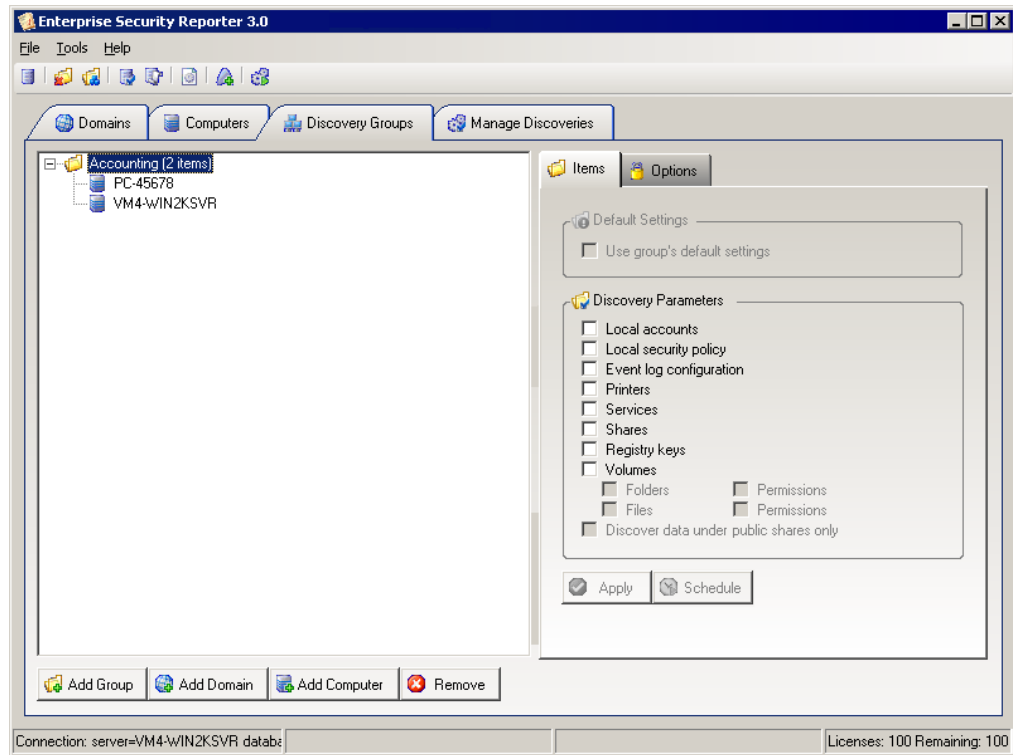
By default, Enterprise Security Reporter discovers all nested folders below the selected folder. Select this check box to specify the folder depth to use during the discovery process.



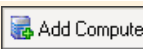
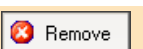
- In the **Folder Depth** box, type the number that represents the level below the folder to which you want nested folders discovered. For example, to include only the first level of subfolders, type 1.

3. Click .



## USING DISCOVERY GROUPS

To save time, create a discovery group to configure a discovery for multiple domains and/or groups. You can set the discovery properties on the group, and then override the properties on computers where you need to discovery something differently.

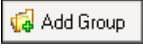


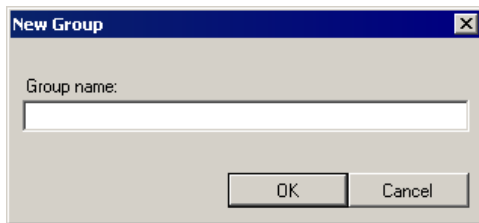
Button	Description
	Add a group to the list. See <i>Creating a Discovery Group</i> .
	Add domains to a selected group. See <i>Adding Domains to a Discovery Group</i> .
	Add computers to a selected group. See <i>Adding Computers to a Discovery Group</i> .
	Remove selected groups, domains, and computers from the list.

After adding groups, use these two tabs to configure the group discovery process:

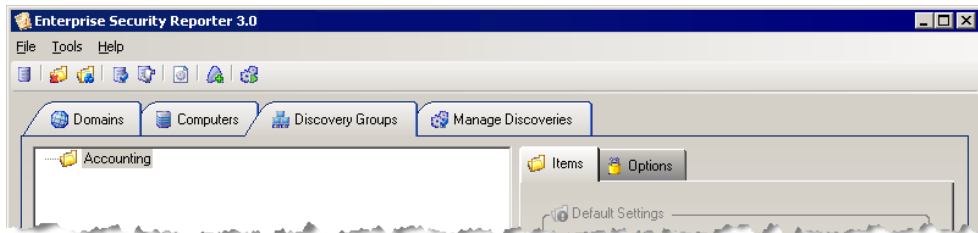
Tab	Description
	Select items to include in the discovery. See <i>Selecting Items for Group Discovery</i> .
	Set options for the group discovery. See <i>Setting Group Discovery Options</i> .


### Creating a Discovery Group

1. Open the **Discovery Groups** tab, and then click . The **New Group** box appears.



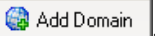
2. In the **Group name** box, type a name for the discovery group, and then click **OK**. The group name displays in the left pane.

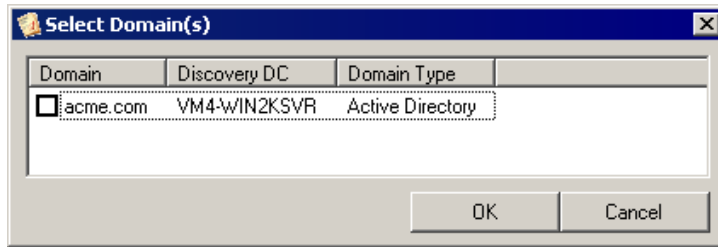


- To remove selected groups, click .

**Note:** You can add domains and/or computers to the group. See *Adding Domains to a Discovery Group* and *Adding Computers to a Discovery Group*. If you choose to add a domain to the group, you need to use the **Domains** tab to configure the domain for discovery as the **Discovery Groups** tab options are unavailable.

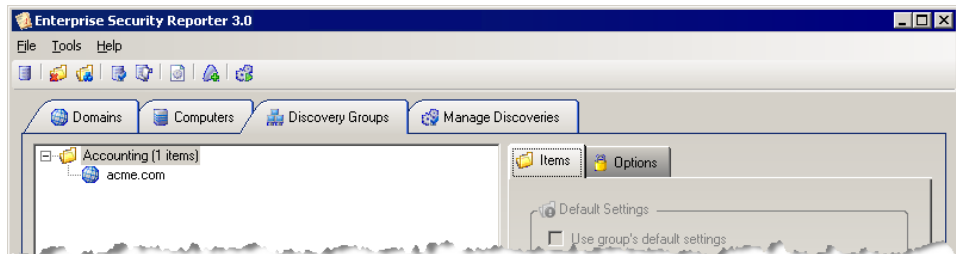
### Adding Domains to a Discovery Group

1. On the **Discovery Groups** tab, select a group, and then click . The **Select Domains** list displays the domains available for selection.




**Note:** Only the domains listed on the **Domains** tab appear in the **Select Domains** list. If you do not see a domain listed, you need to add it. See *Adding Domains*.

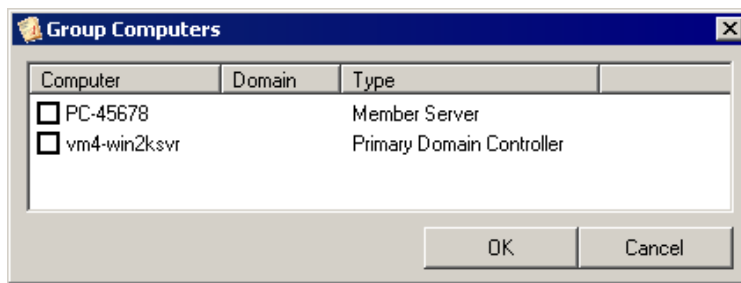
2. Select one or more domains, and then click **OK**. The selected domains display under the group name.



- To remove selected domains from a discovery group, click .

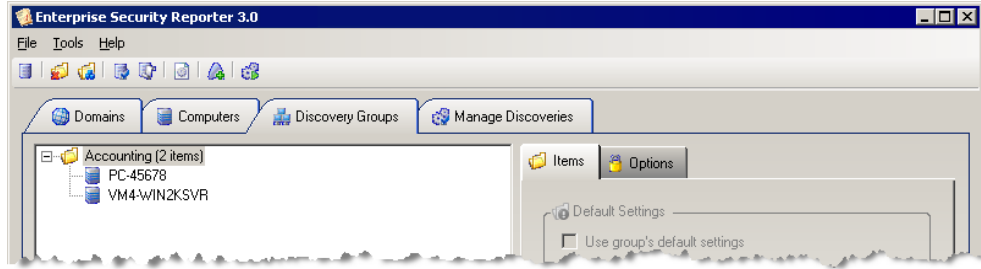
### Adding Computers to a Discovery Group

1. On the **Discovery Groups** tab, select a group, and then, click . The **Group Computers** list displays the computers available for selection.



**Note:** Only the computers that are listed on the **Computers** tab appear in the **Group Computers** list. If you do not see a computer listed, you need to add it. See *Adding Computers*.

2. Select the computers for the group, and then click **OK**. The selected computers display under the group name.

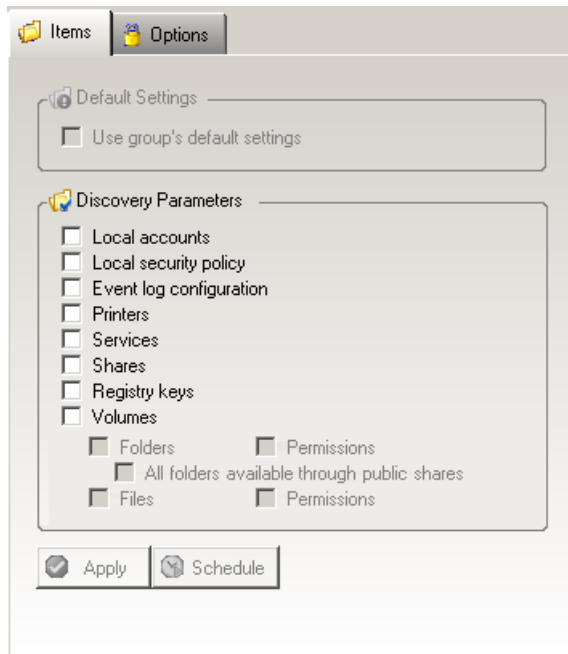


- To remove selected computers from the group, click  **Remove**.

### Selecting Items for Group Discovery

**Note:** The discovery items and options that you choose for the group apply to all members of that group. If you want to override the configuration on an individual domain, use the **Domains** tab. See *Configuring Domains for Discovery*. If you want to override the configuration on an individual computer, see *Overriding Group Discovery Settings*.

1. On the **Discovery Groups** tab, select a group name, click **Items**, if necessary.



2. Select the items in the **Discovery Parameters** area to include in the discovery.

**Use group's default settings**

Available only if an individual computer is selected in the left pane. See *Overriding Group Discovery Settings*.

**Local accounts**

Select to include local accounts in the discovery on the selected group.  
By default, local accounts are excluded the discovery.

 **Local security policy**

Select to include the local security policy in the discovery on the selected group.  
By default, the local security policy is excluded from the discovery.

 **Event log configuration**

By default, the event log configuration is included in the discovery for the selected computer.

 **Printers**

By default, all the printers that are defined on a computer are included in the discovery for the selected computer. If the printer is shared, the share name is discovered and recorded also.

 **Services**

By default, all the services and devices that are defined on a computer are included in the discovery for the selected computer. Includes devices that show under the Devices applet in the control panel.

 **Shares**

By default, all file and administrative shares on a computer are included in the discovery. To discover shared printers, select the **Printers** check box as well.

 **Registry Keys**

Select to catalog all the registry information that is defined on a computer and to activate the **Registry Keys** tab.

 **Volumes**

By default, all local logical drives installed on a computer are included in the discovery.

 **Folders**

Available only if the **Volumes** check box is selected. By default, folders defined on a computer are included in the discovery. The behavior of this option is dependent on the selections made on the **Paths** and **Options** tabs on the **Computers** tab. If selected, the **Folders Permissions** check box is selected automatically.

 **Permissions**

Available only if the **Volumes** and **Folders** check boxes are selected. By default, a complete list of folder permissions is included in the discovery.

 **All folders available through public shares**

Available only if the **Folders** check box is selected. By default, only the folders and permissions under shares that are accessible to the general public (excludes administrative shares) are included in the discovery. If you want to include other folders that are not public, add the path on the **Paths** tab. To include all data, clear the check box.



**Files**

Available only if the **Volumes** check box is selected. By default, files defined on a computer are included in the discovery. The behavior of this option is dependent on the selections made on the **Paths** and **Options** tabs on the **Computers** tab. If selected, the **Files Permissions** check box is selected automatically.

**Important:** Select the **Files** check box only if you specifically need information about the files and their associated permissions. Discovering files dramatically slows down the discovery process and increases the amount of space required to store the data.

 **Permissions**

Available only if the **Volumes** and **Files** check boxes are selected. By default, a complete list of file permissions is included in the discovery.

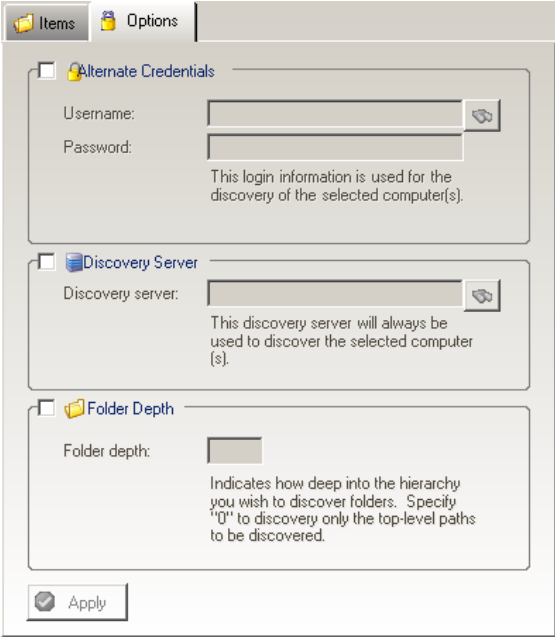
3. Click .

## Setting Group Discovery Options

---

The options that you set for a group override any other options that were set on a global basis.

1. Open the **Discovery Groups** tab, select the group to configure, and then open the **Options** tab.



The screenshot shows the 'Options' tab in the software interface. It contains three sections, each with a checkbox and a text input field:


- Alternate Credentials:** Includes fields for 'Username' and 'Password'. A note below states: "This login information is used for the discovery of the selected computer(s)." There is a small icon to the right of the password field.
- Discovery Server:** Includes a 'Discovery server' field. A note below states: "This discovery server will always be used to discover the selected computer(s)." There is a small icon to the right of the field.
- Folder Depth:** Includes a 'Folder depth' field. A note below states: "Indicates how deep into the hierarchy you wish to discover folders. Specify '0' to discovery only the top-level paths to be discovered."

An 'Apply' button is located at the bottom left of the tab.

 **Alternate Credentials**


By default, Enterprise Security Reporter connects to a computer using the credentials of the logged-in user. Select this check box to specify the user name and password of the account whose security credentials you wish to use to discover all the computers in the group.

**Note:** If you want to specify different credentials for computers in the group, you need to override the group's settings. See *Overriding Group Discovery Settings*.

- In the **User Name** box, type a user name, or click  to select a name. In the **Password** box, type the password.

**Discovery Server**

If you have more than one discovery server, by default, Enterprise Security Reporter selects the next group in the queue and assigns it to the first available discovery server. Select this check box to assign a specific discovery server for the discovery of the domains and computers in the selected group.

- In the **Discovery Server** box, type the name of the discovery server or click  to locate a discovery server.

**Folder Depth**

By default, Enterprise Security Reporter discovers all nested folders below the selected folder. Select this check box to specify the folder depth to use during the discovery process.

- In the **Folder Depth** box, type the number that represents the level below the folder to which you want nested folders discovered. For example, to include only the first level of subfolders, type 1.

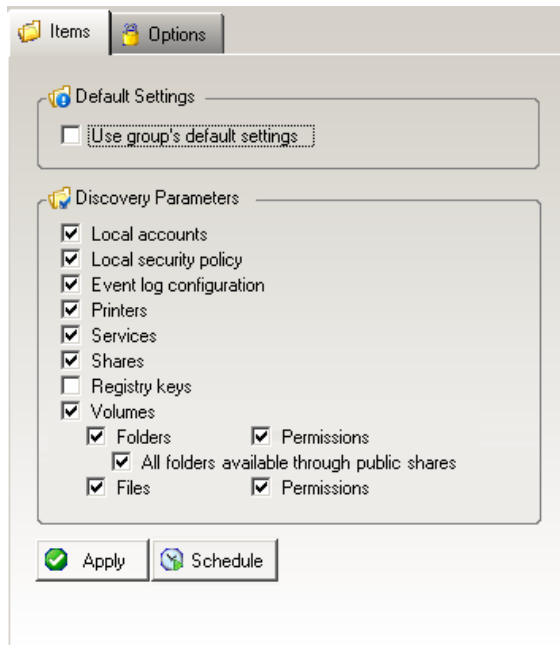
2. Click .

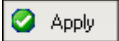
## Overriding Group Discovery Settings

The discovery settings for the group apply to all the domains and computers in the group. You may find it necessary to override the settings of the group for a particular domain or computer. It may be a special case computer and you don't want to remove it from the group, but you do want slightly different settings.

**Note:** If you want to configure a domain separate from the group, open the **Domains** tab and configure the domain on the **Items** tab. See *Configuring Domains for Discovery*.

1. Select the computer in the discovery group list, and then clear the **Use group's default settings** check box. The **Discovery Parameters** area and the **Options** tab become available.



2. Select the items for discovery of the selected computer. See *Selecting Items for Computer Discovery*.
3. Set any options for discovery of the selected computer. See *Setting Computer Discovery Options*.
4. Click .

## EXPORTING DISCOVERY CONFIGURATION SETTINGS

To facilitate moving discovery configuration parameters between databases, or simply for the purpose of backing up your discovery configuration, you can export, and then import an ESR3 Discovery Configuration (\*.xdc) file.

1. From the **Tools** menu, choose **Export Discovery Configuration**.  
**ESR 3 Discovery Configuration Files (\*.XDC)** displays in the **Save as type** box.
2. In the **Save in** box, locate a folder.
3. In the **File name** box, type the name for the file, and then click **Save**. A message box confirms that the discovery configuration export is complete.
4. Click **OK**.

## IMPORTING DISCOVERY CONFIGURATION SETTINGS

Discovery configuration settings are exported as ESR3 Discovery Configuration (\*.xdc) files.



1. From the **Tools** menu, choose **Import Discovery Configuration**.  
**ESR 3 Discovery Configuration Files (\*.XDC)** displays in the **Files of type** box.
2. In the **Look in** box, locate the folder where the file is stored.
3. Select the file to load, and then click **Open**. A message box confirms that the discovery configuration import is complete.
4. Click **OK**.

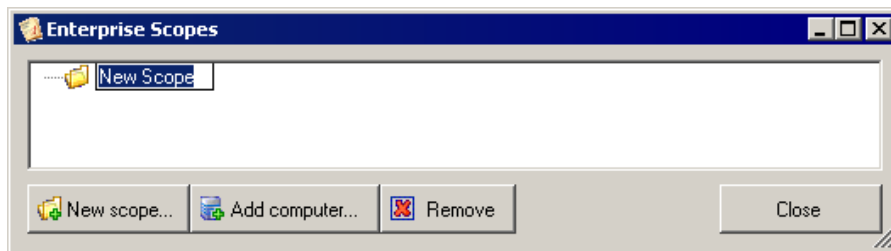
## USING ENTERPRISE SCOPES

Enterprise scopes allow you to group multiple computers together, regardless of type or discovery configuration, so that a single report can be run against the discoveries done on those computers. You may wish to group computers together by function, by type or by geographic location to name a few. Once you have the computers in the enterprise scope, then you can select a report with the phrase “in scope” in the name and that report will run against all the computers in the scope you select.

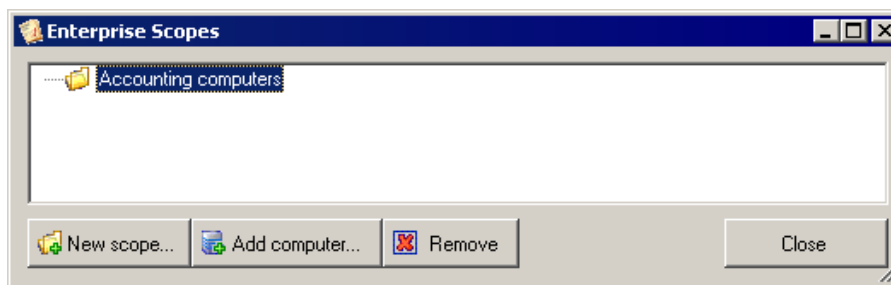
**Note:** Enterprise scopes allow you to prepare a report on various finished discoveries on the named computers. If you want to group computers together to perform a discovery, you want to create a discovery group. See *Using Discovery Groups*.

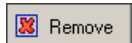
### Adding Enterprise Scopes

1. From the Discovery Console, click . The **Enterprise Scopes** box opens.
2. Click . A new scope is added to the list.



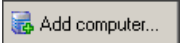
3. Type a name for the scope, and then press **ENTER** or click anywhere in the window.

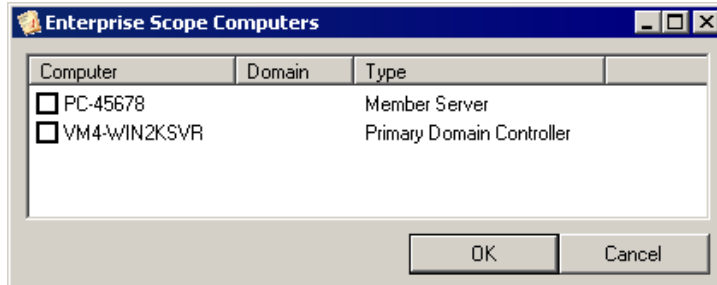


- To rename a selected enterprise scope, press **F2**, type a name for the scope, and then press **ENTER** or click anywhere in the window.
- To remove a selected enterprise scope, click .

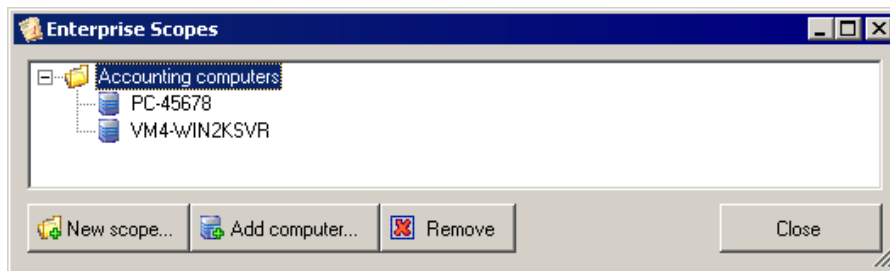
**Note:** Removing an enterprise scope removes only the definition of the scope from the database. The discovery data associated with the computers in the is unaffected.

## Adding Computers to an Enterprise Scope

1. From the **Enterprise Scopes** box, select a scope, and then click . The **Enterprise Scope Computers** list appears.



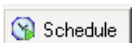
2. Select the servers to add to the scope, and then click **OK**. The selected servers display beneath the scope name.



- To remove a selected computer from the enterprise scope, click .

**Note:** Removing a computer from the enterprise scope does not remove the discovery data associated with that computer.

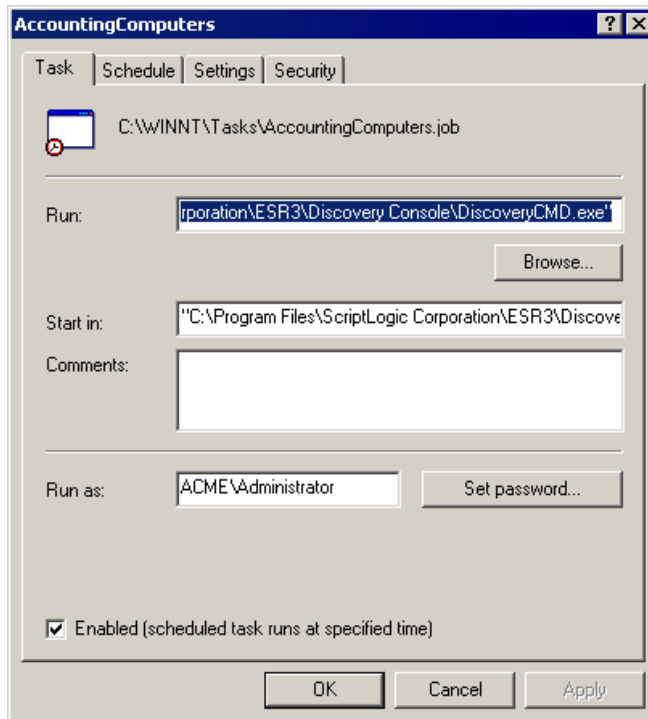
## SCHEDULING DISCOVERY JOBS

1. Click . The **Scheduled Task Wizard** opens.
2. Type a name for the task, select how often the discovery should run, and then click **Next**.
3. Set the time, recurrence, and start date for the discovery job, and then click **Next**.

4. Enter the user name and password of the account that can run the Discovery Engine, and then click **Next**. The job summary displays.



5. Select the **Open advanced properties for this task when I click Finish** checkbox, and then click **Finish**. The **Task** tab opens.
6. In the **Run** box, add parameters after the closing quote mark. See *Using the Command-Line Utility: DiscoveryCMD.exe*.

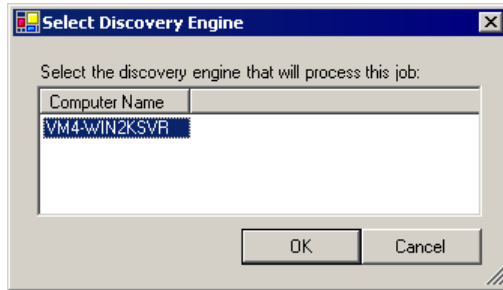


7. Click **OK**.

## LAUNCHING A DISCOVERY

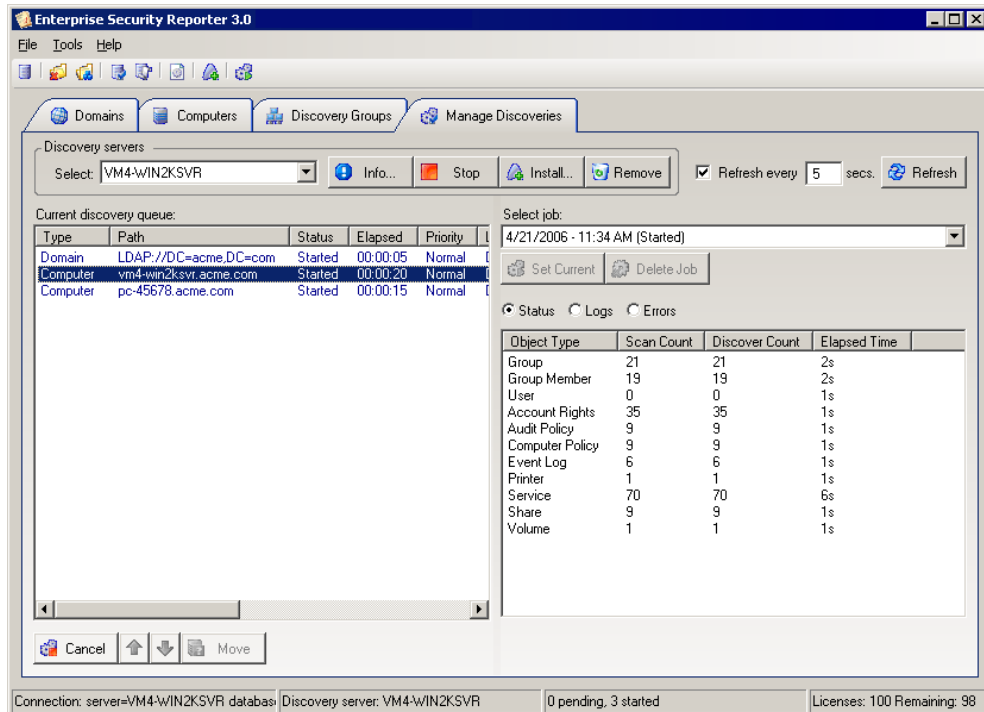
The Discovery Monitor is a window into the discovery process enabling you to control what happens while the discovery is running.

1. From the **Discovery Console**, click . The **Select Discovery Engine** box lists the servers with the discovery engine installed.



2. Select the server to run the discovery, and then click **OK**. To see the status of the discovery, open the **Manage Discoveries** tab.
3. 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.

**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.





**Status**

By default, the status of the selected discovery displays. The status shows the objects included in the discovery, how many objects were scanned and written to the dbESR3.mdf file, and the length of time for each object type to be discovered. To see the total length of time for the discovery, select **Logs**.

**Logs**

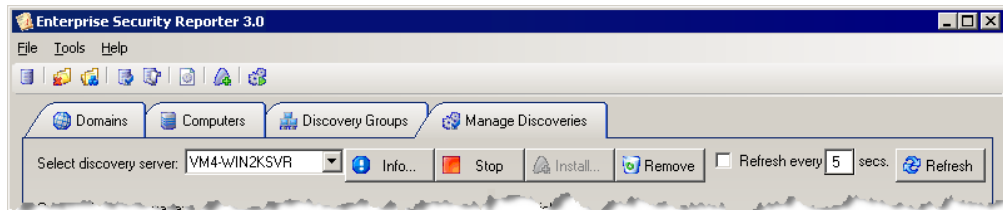
Select to view the entries to the dbESR3\_Log.dbf file that are associated with each discovery job on an individual server. The log shows the total amount of time elapsed for the discovery job.

**Errors**

Select to view any errors generated during the discovery.

## MANAGING THE DISCOVERY SERVER

You can control the ESR Discovery Engine service on the **Manage Discoveries** tab, which offers the same functionality as the Services applet in Windows.




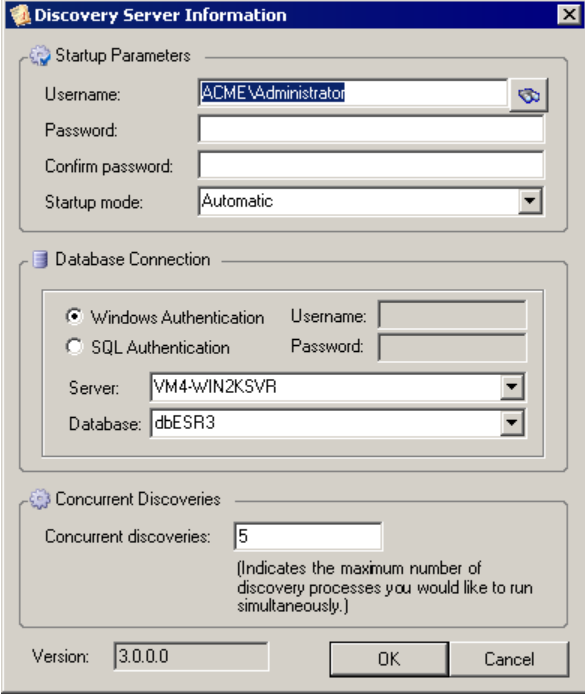
Button	Description
	Display information about the selected server. See <i>Viewing Server Information</i> .
	Stop the ESR Discovery Engine service on the selected server.
	Start the ESR Discovery Engine service on the selected server.
	Install the ESR Discovery Engine service on the selected server.
	Remove the ESR Discovery Engine service from the selected server.
	Update the <b>Current discovery queue</b> list.

**Refresh every**  **secs.**

Select to refresh the discovery queue by the specified number of seconds. By default, the **Current discovery queue** list does not refresh until you click **Refresh**.


## Viewing Server Information

1. Open the **Manage Discoveries** tab.
2. From the **Select discovery server** list, select the discovery server, and then click  **Info...**. The **Discovery Server Information** dialog box displays the current settings for the selected discovery server.



**Note:** If you make any changes, you are prompted to restart the ESR3 Discovery Engine service. The changes do not take effect until the service is restarted.

### Startup Parameters

Displays the user name of the account running the Discovery Engine service. To change to a different account, click , and then type the password. You can also specify the startup mode for the Discovery Engine service.

### Database Connection

Displays the current discovery server and database. To connect to a different server and database, choose the discovery server and database to use.

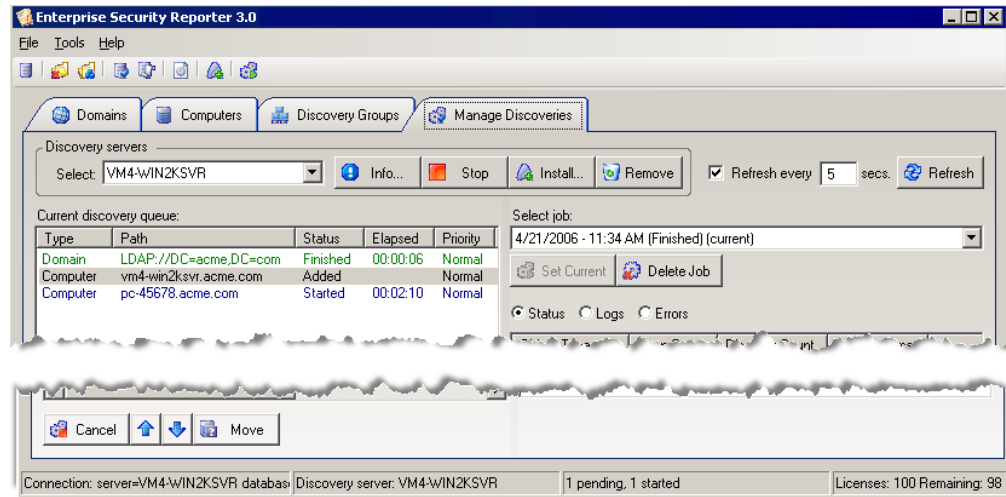
### Concurrent Discoveries

So as not to overload the capabilities of your computer, the discovery engine processes only a set number of servers concurrently. By default, the limit is set to five in the **Concurrent discoveries** box.

- If you increase the value, more servers begin processing immediately.
- If you decrease the value, all currently running servers are allowed to finish, and new discoveries can begin once the number of currently running servers drops below the concurrent limit.

## MANAGING DISCOVERY JOBS

When you begin a discovery, the status of the job changes from **Added** to **Started** and then to **Finished**. The color of the job reflects its status as well as the value in the **Status** column. While a job is pending, you can move the job up and down the queue or move it to a different discovery server. When a job is finished, it is available for selection as the current discovery job, which is the job from which reports are generated.



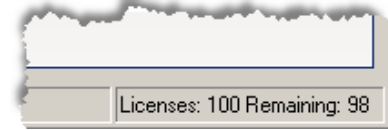
Button	Description
	Set the selected discovery job to current.
	Delete the selected discovery job.
	Cancel the selected pending or running discovery job. The status changes to Cancelled.
	Move a pending job up the queue.
	Move a pending job down the queue.
	Move a pending job to a different discovery server.

**Note:** To see a change in the discovery queue after you perform an action, you must click or select the **Refresh every 5 secs.** check box.

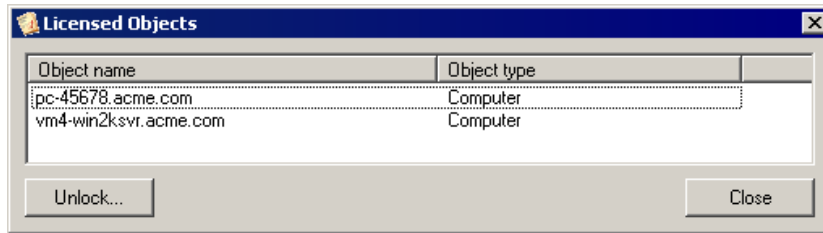
**Note:** If you want to stop a discovery job and restart it at a later time, cancel the job. When the job status shows **Cancelled**, you can right-click the job, and then choose **Begin Discovery**.

## MANAGING LICENSES

As soon as you start a discovery on a computer, a license is applied. You can check the status bar to see how many licenses you have and how many are remaining. In this example, 2 licenses have been used out of 100, so 98 licenses remain.

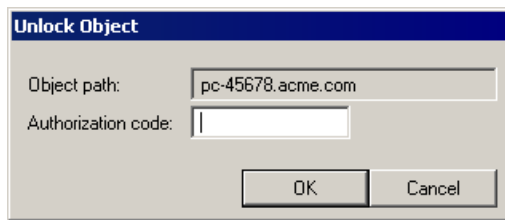


- ▶ To view the computers that were applied to your license count, choose **View licensed objects** from the **Tools** menu. The **Licensed Objects** box lists the computers on which discoveries were started.



**Important:** If you started a discovery on a computer that you did not want applied to your licenses, call ScriptLogic Technical Support to obtain an authorization code.

- ▶ To unlock a computer, select the computer, and then click **Unlock**. In the **Authorization code** box, type the code given to you, and then click **OK**.



## USING THE COMMAND-LINE UTILITY: DISCOVERYCMD.EXE

In the Discovery Console folder of the installation directory, Enterprise Security Reporter includes a command-line utility — `DiscoveryCMD.exe` — that you can use to discover computers, domains, or groups manually.

### Usage

```
DiscoveryCMD.exe "<type>" "<object_path>" "<discovery_engine>"
```

There are three types of discoveries: computer, domain, or group. The discovery engine is the name of the computer where the ESR3 Discovery Engine is installed. If you do not supply arguments, the command provides options from which you can select arguments.

### Example

```
DiscoveryCMD.exe "Computer", "mycomputer.testdomain.local", "DISC_SERVER"
DiscoveryCMD.exe "Domain", "LDAP://DC=testdomain,DC=local" "DISC_SERVER"
DiscoveryCMD.exe "Group", "Test Group", "DISC_SERVER"
```

## USING THE COMMAND-LINE UTILITY: PURGEDATA.EXE

In the Discovery Console folder of the installation directory, Enterprise Security Reporter includes a command-line utility — PurgeData.exe — that clears data from the discovery database. You can specify either a date or the number of days to use as the basis of clearing data.

### Usage

PurgeData.exe	Purges data from the discovery database.
/Date="<date>"	[ <i>Optional</i> ]. All jobs older than the specified date (but not including) are removed from the discovery database.
/Days="<number_of_days>"	[ <i>Optional</i> ]. All jobs that were discovered at least the number of days specified prior to the current date are purged from the database.

**Note:** You can specify a date or the number of days, but not both.

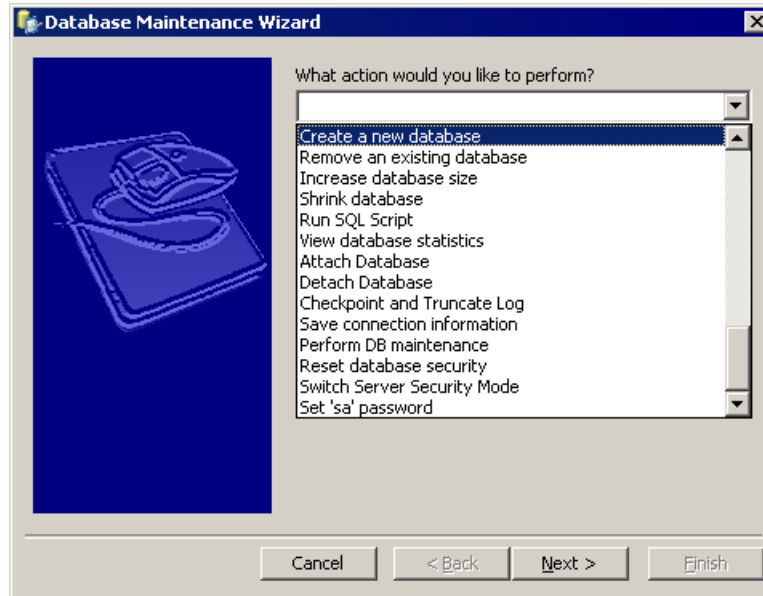
/Keep="<number_of_jobs>"	[ <i>Optional</i> ]. Leave at least "n" jobs for each discovery object.
--------------------------	---

For example, you specify 02/15/2006 as the date and 10 as the number of jobs to keep. The discovery database contains 12 jobs that occurred before that date and 5 days that occurred after that date. After you run the command, only 7 of the jobs in the date range are deleted because the "Keep" parameter overrides the date/days parameters.

If you always want to keep the discovery data from the current job, specify a "Keep" value of 1.

# Database Utilities


Use the Database Maintenance Wizard to manage the discovery and reporting databases. The default discovery database is dbESR3.mdf and the default reporting database is dbESR3Reporting.mdf.



**Note:** Enterprise Security Reporter includes a run-time version of Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), which is data engine built and based on core SQL Server technology. This database engine has some limitations over the full version of Microsoft SQL Server 2000, such as a 2GB database limit and a restriction on the number of concurrent users. If you have a large enterprise, you may want to consider purchasing a full version of Microsoft SQL Server 2000 for use with this product.

## STARTING THE DATABASE UTILITIES

There are three ways to start the Database Utilities.

- ▶ From the Windows desktop, click **Start**, point to **Programs** > **ScriptLogic Corporation** > **Enterprise Security Reporter 3** > **Database Utilities**, and then select either **Discovery Database Wizard** or **Reporting Database Wizard**.
- ▶ From the Discovery Console, click , and then choose either **Discovery Database** or **Reporting Database**.

**Note:** Some actions, such as **Removing a database** and **Detaching a database**, require that the database not be in use. For these actions, do not access the Database Utilities from the Discovery Console.

- ▶ From the command line, type **DBWizard.exe**. See *Using the Command-Line Utility: DBWizard.exe*.

## CREATING A NEW DATABASE

When you first install Enterprise Security Reporter, the Database Wizard opens automatically for you to create new databases. The default discovery database is dbESR3.mdf and the default reporting database is dbESR3Reporting.mdf.

Follow these this procedure if you bypassed this step during installation, or wish to create another database to use.

**Important:** You must create a database before you can perform any tasks using Enterprise Security Reporter 3. Databases created with Enterprise Security Reporter 3 are not compatible with those created with Enterprise Security Reporter 2 or 1.

1. From the **Database Maintenance Wizard** main page, select **Create a new database** from the list, and then click **Next**. The database selection dialog box displays the current computer and database names (default).



Database Maintenance Wizard - Create a new database

SQL Database Server Name: WM4-WIN2K5VR



Database Name: dbSecRpt25

Use Windows Authentication  
 Use SQL Server Authentication

User Name:

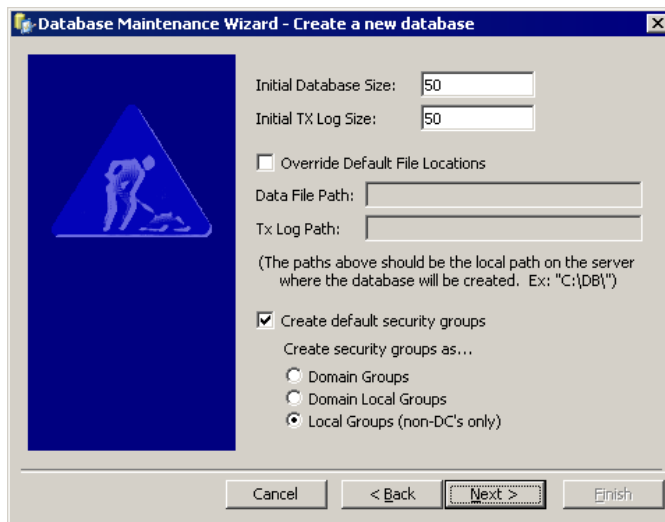
Password:

Cancel < Back Next > Finish

2. 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.
3. In the **Database Name** box, type the name of the database to create or click  to locate existing database names.

**Note:** The default discovery database is dbESR3.mdf. The default reporting database is dbESR3Reporting.mdf.

4. 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.
5. Click **Next**. The database definition dialog box displays the default sizes for the database (\*.mdf) and transaction log (\*.ldf) files.



6. In the **Initial Database Size** box, type an initial size for the database file (\*.mdf file). If the database needs to grow the data file, it will do so automatically.
7. In the **Initial TX Log Size** box, type an initial size for the database transaction log file (\*.ldf). If the database needs to grow the log file, it will do so automatically.
8. To create the database transaction log files in a location other than the default location, select **Override Default File Locations**, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
9. 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.
10. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
11. 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.
12. Click **OK**.



## REMOVING AN EXISTING DATABASE

Removing a database permanently removes it from the system. If you just want to detach the database, see *Detaching a Database*.

**Note:** The database cannot be in use. Exit the Discovery Console, if necessary, and then start the Database Maintenance Utility.

1. From the **Database Maintenance Wizard** main page, select **Remove an existing database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database to remove or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.

**Caution:** Removing a database deletes it permanently from the system.

6. To permanently delete the 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.
7. Click **OK**.

## INCREASING DATABASE SIZE

Microsoft SQL Server automatically increases the size of the database file as needed, but if this happens while discoveries are running, it can significantly slow down the discovery process. If a discovery process seems to be running normally, and then suddenly slows down, you may want to increase the size of the database manually.

1. From the **Database Maintenance Wizard** main page, select **Increase database size** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database to resize or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.

5. Click **Next**. The **Database Maintenance Wizard** displays the existing size of the database.



**Note:** Enter the total size of the new database, not the additional size of the database. For example, if the database is 50MB and you want to add another 50MB, then you would enter 100 as the new database size.

6. In the **New Database Size** box, type a numeric value in megabytes that is greater than the existing value and represents the total size of the database, and then click **Next**. The **Database Maintenance Wizard** displays the options you chose.
7. Click **Finish**, and then click **OK**.

## SHRINKING A DATABASE

If you need to reclaim space, you can shrink the database, which reduces the size of the database to the minimum amount based on the size of the data.

Another database to monitor is the tempdb database, which is the working area that Microsoft SQL Server uses to process queries and perform other actions. You might shrink the tempdb database periodically to reclaim the disk space that is no longer needed.

1. From the **Database Maintenance Wizard** main page, select **Shrink database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database to shrink, or click **...** to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**, and then click **OK**.

## RUNNING AN SQL SCRIPT

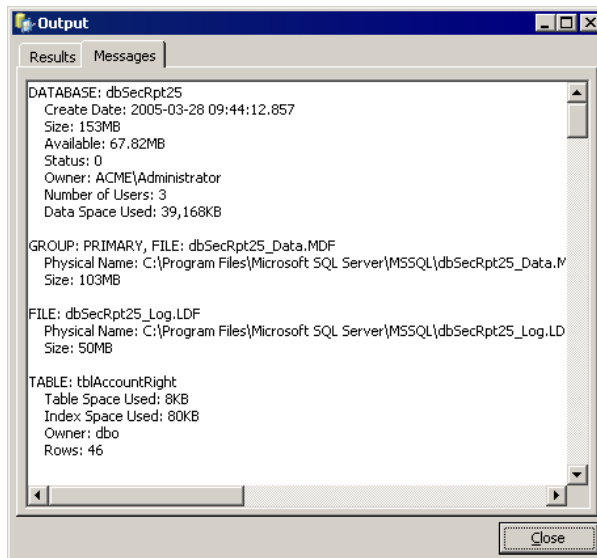
1. From the **Database Maintenance Wizard** main page, select **Run SQL Script** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the Microsoft Windows server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database on which to run the SQL script, or click **...** to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the SQL Script selection box.
6. In the **Select a SQL Script file to run** box, type the full path to the SQL Script File (\*.sql) or click **...** to locate the file. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
7. Click **Finish**. A progress bar shows the progress of the action. Upon completion, the **Output** message box opens to the **Results** tab. To see messages regarding the action, open the **Messages** tab.
8. Click **Close**, and then click **OK**.

## VIEWING DATABASE STATISTICS

View the current database settings and statistics on the size of the database and each table in the database, which is helpful for diagnosing problems in the event that SQL Server is not functioning properly.

1. From the **Database Maintenance Wizard** main page, select **View database statistics** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database, or click **...** to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.

- Click **Finish**, and then click **OK**. The **Output** dialog box opens to the **Messages** tab, which displays the database statistics.



- To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application of your choice.
- When you are finished viewing the statistics, click **Close**.

## ATTACHING A DATABASE

When you create a database, it is automatically attached to Enterprise Security Reporter. If you detach a database, you can attach it again to use it.

- From the **Database Maintenance Wizard** main page, select **Attach database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
- In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
- In the **Database Name** box, type the name of the database to attach, or click **...** to locate the database.
- Choose whether Windows or SQL Server Authentication is used. 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.
- Click **Next**. The data file selection box appears.
- In the **Select the MDF (data) file to attach** box, type the full path to the data file or click **...** to locate the data file to attach.
- Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
- Click **Finish**, and then click **OK**.

## DETACHING A DATABASE

Detaching a database removes it from Enterprise Security Reporter, but does not delete it from the system. To permanently delete a database, see *Removing an Existing Database*.

**Note:** The database cannot be in use. Exit the Discovery Console, if necessary, and then start the Database Maintenance Utility.

1. From the **Database Maintenance Wizard** main page, select **Detach database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database to detach, or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**. The **Output** message box opens to the **Messages** tab, which displays information about the process.
  - ▶ To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application of your choice.
7. Click **Close**, and then click **OK**.

## TRUNCATING THE TRANSACTION LOG

When a transaction log becomes full, it forces the database to expand it. However, since Enterprise Security Reporter does not use the transaction log, and there is no way to disable the transaction log for a database, you may need to periodically truncate the transaction log to tell the SQL Server that the data is no longer needed.

1. From the **Database Maintenance Wizard** main page, select **Checkpoint and Truncate Log** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database whose log file you want to truncate, or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.

5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**, and then click **OK**.

## SAVING CONNECTION INFORMATION

This option writes the database connection settings to the registry.

1. From the **Database Maintenance Wizard** main page, select **Save connection information** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database, or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the settings to be written to the registry.
6. Click **Finish**, and then click **OK**.

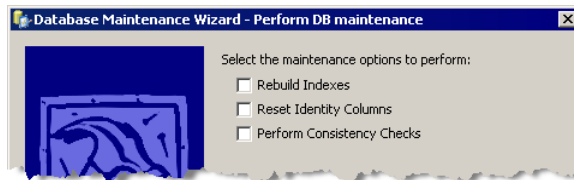
## PERFORMING DATABASE MAINTENANCE

Performing regular database maintenance can help maintain the performance of SQL Server. Run this action if you feel SQL Server is not performing at the same level it once did. You can select to rebuild indexes, reset identify columns, and perform consistency checks.

Many SQL database administrators are familiar with Database Consistency Checker (DBCC) commands. The **Perform DB Maintenance** action performs the following DBCC commands.

DBCC Command	Description
CHECKCATALOG	Checks the system tables for consistency.
CHECKFILEGROUP	Performs a physical consistency check on all indexes and tables.
CHECKTABLE REPAIR_REBUILD	Performs a consistency check of the data in each table and rebuilds indexes if necessary.
CHECKIDENT	Checks the identity values of each table and resets them if necessary.
CHECKINDEX	Checks the physical database allocation of indexes and repairs if necessary.

1. From the **Database Maintenance Wizard** main page, select **Perform DB Maintenance** from the drop-down list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database, or click **...** to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The maintenance options selection box appears.



**Rebuild Indexes**

Select to run CHECKINDEX and CHECKTABLE REPAIR\_REBUILD.

**Reset Identify Columns**

Select to run CHECKIDENT.

**Perform Consistency Checks**


Select to run CHECKCATALOG, CHECKFILEGROUP, CHECKTABLE REPAIR\_REBUILD, and CHECKINDEX.

6. Choose the maintenance options to perform, and then click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
7. Click **Finish**. When the process is complete, the **Database Maintenance Results** box opens to the **Messages** tab.
  - ▶ To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application.
8. Click **Close**, and then click **OK**.

## RESETTING DATABASE SECURITY



Resetting the database security re-creates the Windows NT security groups, database roles, and logins, and then re-applies the default security to all tables/functions/stored procedures in the Enterprise Security Reporter database.

1. From the **Database Maintenance Wizard** main page, select **Reset database security** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.

3. In the **Database Name** box, type the name of the database, or click  to locate the database.
4. Choose whether to use Windows or SQL Server 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.
5. Click **Next**. The **Database Maintenance Wizard** displays actions to be performed.
6. Click **Finish**, and then click **OK**.

## SWITCHING THE SERVER SECURITY MODE

Depending on your system setup, you may want to switch the security mode on the SQL Server to enhance performance of some applications. For example, if you have Active Administrator™ set up to use one mode and Enterprise Security Reporter to use the other, you may want to switch the security mode on the SQL Server to **SQL Server and Windows**.

1. From the **Database Maintenance Wizard** main page, select **Switch Server Security Mode**, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database, or click  to locate the database.
4. Choose whether to use Windows or SQL Server 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the security mode options.



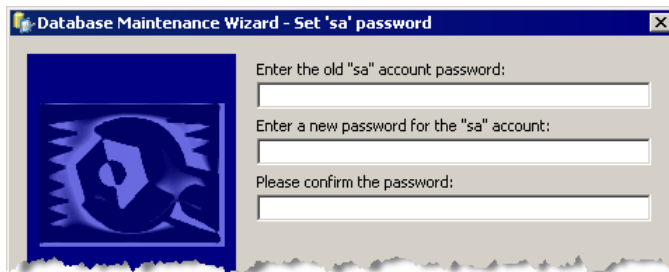
6. Select either **SQL Server and Windows** or **Windows only**, and then click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
7. Click **Finish**, and then click **OK**.



## SETTING THE 'SA' PASSWORD

If the SQL Server is set up in mixed mode (SQL Server and Windows), set a password for the SQL Server administrator ("sa" account). You also can use this option to change the password for security purposes.

1. From the **Database Maintenance Wizard** main page, select **Set 'sa' password**, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click  to locate the server.
3. In the **Database Name** box, type the name of the database, or click  to locate the database.
4. Choose whether Windows or SQL Server Authentication is used. 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.
5. Click **Next**. The **Set "sa" password** box opens.



6. In the **Enter the old "sa" account password** box, type the existing password.
7. In the **Enter a new password for the "sa" account** box, type the new password.
8. In the **Please confirm the password** box, retype the new password.
9. Click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
10. Click **Finish**, and then click **OK**.

## MOVING A DATABASE TO ANOTHER SERVER

If you need to move a database from one server to another, we recommend using the Microsoft SQL Server 2000 client utilities.

**Note:** Client utilities are available only on a full version of SQL Server 2000, which is not included with Enterprise Security Reporter 3.

1. Open SQL Enterprise Manager.
2. Locate the database to move, right-click, point to **All Tasks**, and then choose **Detach Database**.

3. Open the folder where the data files for that database are stored, and then copy the \*.mdf and \*.ldf files for that database to the new server.
4. In SQL Enterprise Manager, navigate to the new server where you want to attach the database, right-click on the **Database** folder, point to **All Tasks**, and then choose **Attach Database**.
5. Select the \*.mdf file you just copied to the computer, and then complete the operation.

## USING THE COMMAND-LINE UTILITY: DBWIZARD.EXE

In the Database folder of the installation directory, Enterprise Security Reporter includes a command-line utility — DBWizard.exe — that starts the Database Maintenance Utility.

### Specifying Database Connection Information

/SERVER=" [server-name] "	Name of the server running SQL Server.
/DATABASE=" [database-name] "	Name of the database.
/USERNAME=" [username] "	[Optional] Name of the SQL Server user account.
/PASSWORD=" [password] "	[Optional] Password for the SQL Server user account.

**Note:** If you do not specify a user name and password, trusted security is used.

### Creating a Database

/CREATE	Create the specified database.
<b>Important:</b> Database must not already exist.	
/DBSIZE=" [size] "	[Optional] Initial size of the *.mdf file (data).
/LOGSIZE=" [size] "	[Optional] Initial size of the *.ldf file (log).
/DBPATH=" [mdf-path] "	[Optional] Full path to the *.mdf file, including the file name.
/LOGPATH=" [ldf-path] "	[Optional] Full path to the *.ldf file, including the file name.

### Dropping a Database

/DROP	Drop the specified database.
-------	------------------------------

### Running a SQL Script

/RUN=" [script-path] "	Run the specified SQL Server script.
------------------------	--------------------------------------

## Running All Maintenance Tasks

---

`/MAINT` Run all the maintenance tasks supported by the wizard.  
See *Performing Database Maintenance*.

## Running Checkpoint and Truncate Log

---

`/TRUNCATE` Truncate the log file of the specified database.

## Shrinking the Database Files

---

`/SHRINK` Shrink the database file.

`/LOGONLY` Shrink only the log file and not the database file.

## Resetting Database Security

---

`/RESETSECURITY` Reset the database security and add accounts if necessary

## Controlling Wizard Behavior

---

`/Q[UIET]` [*Optional*] Do not display any user interface elements.

`/CLOSEONFINISH` [*Optional*] Close the wizard automatically when finished (not applicable for QUIET mode).

# 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
```

# Index

▪

.ldf file, 51  
.mdf file, 44, 49  
.sql file, 54  
.xdc files, 39

## A

Active Directory, 1  
  discovering attributes, 15  
  removing attributes from discovery, 16  
adding  
  computers to discovery, 21, 22  
  computers to discovery group, 33  
  domains, 12  
  domains to discovery group, 33  
  enterprise scopes, 40  
  path to discovery, 27  
ADSI Edit, 16  
alternate credentials, 19, 30, 36  
assigning  
  discovery server, 31  
attaching  
  databases, 55

## B

beginning  
  discovery, 43

## C

cancelling  
  discovery job, 46  
command line utility  
  DBWizard.EXE, 61  
  DiscoveryCMD.exe, 47  
  PurgeData.exe, 48  
computers  
  adding to discovery, 21, 22  
  adding to discovery group, 33  
  adding to enterprise scope, 41  
  configuring for discovery, 20  
  removing from discovery, 21  
  searching for, 22  
  selecting groups for discovery, 34  
  selecting items for discovery, 25  
  setting discovery options, 30  
concurrent discoveries, 45  
configuring

  computers for discovery, 20  
  domains for discovery, 11  
connecting  
  to a computer, 19  
  to discovery database, 45  
creating  
  databases, 50  
  discovery group, 32

## D

database utilities  
  starting, 50  
databases  
  attaching, 55  
  creating, 50  
  detaching, 56  
  increasing size, 52  
  maintaining, 57  
  moving to another server, 60  
  removing, 52  
  resetting security, 58  
  setting sa password, 60  
  shrinking, 53  
  switching server security mode, 59  
  viewing statistics, 54  
DBCC commands, 57  
dbESR3.mdf, 49  
dbESR3\_Log.mdf, 44  
dbESR3Reporting.mdf, 49  
DBWizard.exe, 61  
deleting  
  discovery groups, 32  
  discovery job, 46  
  paths from discovery, 9  
  registry keys from discovery, 10, 29  
detaching  
  databases, 56  
DiscoverCMD.EXE, 61  
discovering  
  Active Directory attributes, 15  
  computers, 21  
  domain accounts, 14  
  domain computers, 15  
  domain controllers, 14  
  event log configuration, 25, 35  
  file permissions, 26, 36  
  files, 26, 36  
  folder permissions, 26, 35  
  folders, 26, 35  
  group local accounts, 35  
  LDAP attributes, 15  
  local accounts, 25

- local security policy, 25, 35
- organizational units, 15, 17
- printers, 25, 35
- regisrtry keys, 26
- registry keys, 29, 35
- services, 25, 35
- shares, 25, 35
- sites, 14
- trust relationships, 14
- volumes, 26, 35
- discovery
  - launching, 43
  - logs, 44
  - starting, 43
  - status, 44
- discovery configuration
  - exporting, 39
  - importing, 39
  - saving, 39
- Discovery Console
  - starting, 3
  - tabs, 4
- discovery database
  - connecting to, 8, 45
  - setting update frequency, 63
- discovery domain controller
  - selecting, 12
- discovery engine
  - uninstalling, 63
- Discovery Engine
  - installing, 6
- discovery groups, 2, 31
  - adding computers, 33
  - adding domains, 33
  - creating, 32
  - deleting, 32
  - overriding, 38
  - setting options, 36
- discovery job
  - cancelling, 46
  - deleting, 46
  - managing, 46
  - moving down, 46
  - moving to another server, 46
  - moving up, 46
  - scheduling, 41
  - setting current, 46
- discovery options
  - ping timeout, 19
- discovery parameters
  - loading, 39
- discovery queue
  - refreshing, 44
- discovery server
  - managing, 44
  - moving jobs, 46
  - selecting, 31, 37
  - viewing information, 45
- discovery service
  - installing, 44
  - removing, 44
  - starting, 44

- stopping, 44
- DiscoveryCMD.exe, 47
- domain accounts
  - discovering, 14
- domain computers
  - discovering, 15
- domain controllers
  - discovering, 14
- domains
  - adding, 12
  - adding to discovery group, 33
  - configuring for discovery, 11
  - deleting from discovery group, 33, 34
  - removing, 11, 12
  - selecting items for discovery, 14
  - setting discovery options, 18

## E

- enterprise scopes, 40
  - adding, 40
  - adding computers, 41
  - removing, 40, 41
  - renaming, 40
- errors
  - discovery, 44
- ESR3 Discovery Configuration file, 39
- event log configuration
  - discovering, 25, 35
- excluding
  - path from discovery, 8
  - paths from discovery, 27
  - registry keys from discovery, 9
- exit program, 4
- exporting
  - discovery configuration, 39

## F

- File menu, 4
- files
  - discovering, 26, 36
  - discovering permisisions, 26
  - discovering permissions, 36
- folder depth, 31, 37
- folders
  - discovering, 26, 35
  - discovering permissions, 26, 35

## G

- global discovery options
  - setting, 8
- group discovery
  - overriding settings, 34

## H

- Help menu, 5

**I**

- importing
  - discovery configuration, 39
- including
  - registry keys in discovery, 9
- increasing
  - database size, 52
- installing
  - Discovery Engine, 6
  - discovery service, 44
  - Discovery Service, 6
- items
  - selecting for computer discovery, 25
  - selecting for domain discovery, 14
  - selecting for group discovery, 34

**L**

- launching
  - discovery, 43
- LDAP attributes
  - discovering, 15
- licenses
  - managing, 47
  - unlocking, 47
- loading
  - discovery configuration, 39
- local accounts
  - discovering, 25
  - discovering group, 35
- local security policy
  - discovering, 25, 35
- logs
  - discovery queue, 44

**M**

- maintaining
  - databases, 57
- managing
  - discovery jobs, 46
  - discovery server, 44
- maximum folder depth, 31, 37
- menus
  - File, 4
  - Help, 5
  - Tools, 5
- Microsoft Data Engine 2000, 49
- modifying
  - organizational units from discovery, 18
  - paths in discovery, 28
  - registry key discovery, 10, 29
- moving
  - databases to another server, 60
- MSDE, 49

**N**

- NTFS permissions, 1

**O**

- options
  - setting group, 36
- organizational units
  - discovering, 15, 17
  - modifying, 18
  - removing from discovery, 17
- overriding
  - discovery settings, 38
  - group discovery, 34

**P**

- paths
  - excluding from discovery, 8, 27
  - including in discovery, 27
  - modifying, 28
  - removing from discovery, 28
- permissions
  - discovering, 26
- ping timeout, 19
- printers
  - discovering, 25, 35
- public shares
  - discovering only, 26, 35
- PurgeData.exe, 48

**R**

- reducing
  - database size, 53
- refresh
  - discovery queue, 43, 44
- registry keys
  - discovering, 26, 29, 35
  - excluding from discovery, 9
  - including in discovery, 9
  - modifying discovery, 29
  - removing from discovery, 29
- removing
  - attributes from discovery, 16
  - computers from discovery, 20, 21
  - computers from discovery group, 34
  - databases, 52
  - discovery group members, 32
  - discovery service, 44
  - domains, 11, 12
  - domains from discovery group, 33
  - enterprise scopes, 40, 41
  - organizational units from discovery, 17
  - paths from discovery, 9, 28
  - registry keys from discovery, 10
- renaming
  - enterprise scopes, 40

**S**

- sa password
  - setting, 60
- saving

- connection information, 57
- discovery configuration, 39
- scheduling
  - discovery jobs, 41
- searching
  - for computers, 22
- security
  - resetting database, 58
- selecting
  - discovery domain controller, 12
  - discovery server, 31, 37
- server security
  - switching modes, 59
- servers
  - moving databases, 60
- services
  - discovering, 25, 35
- setting
  - computer discovery options, 30
  - current discovery job, 46
  - folder depth, 31, 37
  - for domain discovery options, 18
  - global discovery options, 8
  - group discovery options, 36
  - ping timeout, 19
  - sa password, 60
- shares
  - discovering, 25, 35
- shrinking
  - databases, 53
- sites
  - discovering, 14
- SQL Script
  - running, 54
- starting
  - database utilities, 50
  - discovery, 43
  - Discovery Console, 3
  - discovery service, 44

- status
  - discovery queue, 44
- status bar, 6
- stopping
  - discovery service, 44
- synchronizing
  - last logon information, 15

## T

- tempdb database, 53
- toolbar, 4
- Tools menu, 5
- transaction logs
  - truncating, 56
- truncate
  - transaction logs, 56
- trust relationships
  - discovering, 14

## U

- using
  - alternate credentials, 19, 30, 36

## V

- viewing
  - database statistics, 54
  - discovery errors, 44
  - discovery logs, 44
  - discovery server information, 45
  - discovery status, 44
  - licenses, 47
- volumes
  - discovering, 26, 35