

# **User Manual**

## **ARK for Windows Enterprise (ARKWE)**



Last Updated: April 2019

Copyright © 1999-2019 Vyapin Software Systems Private Ltd. All rights reserved.

This document is being furnished by Vyapin Software Systems Private Ltd for information purposes only to licensed users of the ARKWE software product and is furnished on an "AS IS" basis, that is, without any warranties, whatsoever, express or implied. ARKWE is a trademark of Vyapin Software Systems Private Ltd. Information in this document is subject to change without notice and does not represent any commitment on the part of Vyapin Software Systems Private Ltd. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software except as specifically allowed in that license. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to the way of: photocopying, recording, or information recording and retrieval systems, without the express written permission of Vyapin Software Systems Private Ltd.



**Vyapin Software Systems Private Limited**

Website: <http://www.vyapin.com/>

Sales Contact: [sales@vyapin.com](mailto:sales@vyapin.com)

Technical Support: [support@vyapin.com](mailto:support@vyapin.com)

# Table of Contents

<b>1</b>	<b><i>General Information</i></b>	<b>1</b>
1.1	About Admin Report Kit for Windows Enterprise (ARKWE)	1
1.2	System Requirements	2
1.3	Who Can Use ARKWE?	3
1.4	How to purchase?	4
1.5	How to register the Software?	5
1.6	Technical Support	9
<b>2</b>	<b><i>Getting Started</i></b>	<b>10</b>
2.1	Configuration Wizard	10
	Configuration Settings	16
2.1.1	Database Settings	16
2.1.2	Computer Enumeration	18
2.1.3	Configuring Domain Credentials	19
2.1.4	Add a Domain/Server	22
2.1.5	Edit a Domain/Server	24
2.1.6	Delete a Domain/Server	26
2.1.7	Add Domains from Forest	27
2.1.8	Configure SMTP Server	30
2.1.9	User Connection Profiles	31
<b>3</b>	<b><i>Standard Reports</i></b>	<b>33</b>
3.1	How to View Domain Information?	33
3.2	How to View Shares and Resources Information?	36
3.3	How to View Users and Groups Information?	40
3.4	How to View Policies Information?	44
3.5	How to View Events Information?	49
3.6	How to View Service Information?	52
<b>4</b>	<b><i>Built-in Reports</i></b>	<b>54</b>
4.1	About Built-in Reports	54

4.2	How to View Built-in Permissions Reports? .....	54
4.3	How to View Built-in Reports for Shares and Resources? .....	70
4.4	How to View Built-in Reports for Users and Groups? .....	74
4.5	How to View Built-in Reports for Domains? .....	78
<b>5</b>	<b><i>System Information</i></b> .....	<b>83</b>
5.1	About System Info .....	83
5.2	How to View Network Configuration Reports? .....	85
5.3	How to View Operating System & Hot Fixes Reports? .....	88
5.4	How to View Printer Configuration Reports? .....	90
5.5	How to View Hardware Configuration Reports? .....	91
5.6	How to View Display Configuration Reports? .....	94
5.7	How to View Internet Explorer Configuration Reports? .....	96
5.8	How to View Current Status Reports? .....	97
5.9	How to View Environment Info Reports? .....	98
<b>6</b>	<b><i>Additional Features</i></b> .....	<b>99</b>
6.1	How to customize fields? .....	99
6.2	How to Apply Filters? .....	100
6.3	How to Refresh Data? .....	102
6.4	How to Export Data? .....	102
6.5	How to E-mail Data? .....	104
6.6	How to Find Data in a Report? .....	108
6.7	How to Scan Specific Servers in a Domain? .....	110
<b>7</b>	<b><i>Power Export</i></b> .....	<b>113</b>
7.1	About Power Export .....	113
7.2	Task Manager-Scheduled Tasks Manager .....	114
7.3	Schedule Standard Reports .....	116

7.4	Schedule Built-in Reports.....	127
7.5	Schedule Shares and Resources Built-in Reports .....	154
7.6	Schedule Users and Groups Built-in Reports .....	164
7.7	Schedule Domain Built-in Reports .....	173
<b>8</b>	<b><i>Scan Profiles Manager.....</i></b>	<b>183</b>
8.1	About Scan Profiles (Computers).....	183
8.2	How to Create Scan Profiles (Computers)?.....	184
8.3	How to Manage Scan Profiles (Computers)? .....	189
8.4	How to Apply Scan Profiles (Computers)? .....	191
8.5	About Scan Profiles (Users/Groups) .....	193
8.6	How to Create Scan Profiles (Users/Groups)? .....	193
8.7	How to Manage Scan Profiles (Users/Groups)? .....	197
8.8	How to Apply Scan Profiles (Users/Groups)? .....	199
8.9	About Scan Profiles (Shares) .....	203
8.10	How to Create Scan Profiles (Shares)? .....	203
8.11	How to Manage Scan Profiles (Shares)? .....	206
8.12	How to Apply Scan Profiles (Shares)? .....	208
	References .....	212
8.13	Troubleshooting.....	212
8.14	How to Uninstall ARKWE? .....	213
<b>9</b>	<b><i>Index.....</i></b>	<b>217</b>

# 1 General Information

## 1.1 About Admin Report Kit for Windows Enterprise (ARKWE)

---

**Admin Report Kit for Windows Enterprise (ARKWE)** is a powerful reporting solution for the Microsoft Windows Network. ARKWE collects configuration information about Windows domains & servers, users/groups, policies, events, services, installed applications, shares, permissions, printers, data sources etc. The reports are presented in a variety of formats that are simple, elegant and highly customizable for System Administrators, IT infrastructure Managers and Systems Audit personnel to use and act on. ARKWE's basket of Built-in reports provides powerful, ready-to-use reports that assist in both Management reporting and Compliance reporting requirements such as SOX and HIPPA. A single solution that serves your everyday needs of administrative tasks as well as complex data preparation tasks for assisting in compliance.

**ARKWE** has been architected using the latest Microsoft .NET technology, bringing you the best-in-breed reporting solution for your entire Windows Network. ARKWE is highly optimized for performance (using native Windows API calls wherever appropriate), resulting in fast data collection of deeply embedded configuration data. Imagine scanning your vast network of workstations and servers without having to wait forever to see your reports! You can create data subsets for your network using our powerful scan options and meaningfully segment your entire network for data collection and reporting.

**ARKWE** supports current versions of Microsoft Windows Server (2000/2003/2008/2012) and localized versions of Windows Server, including German, Spanish and French.

### 1.2 System Requirements

---

#### For the computer running ARKWE

<b>Processor:</b>	Intel Pentium Processor
<b>Disk Space &amp; Memory:</b>	512 MB RAM and minimum of 20 MB of free disk space.
<b>Operating System:</b>	Windows 10 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2016 / Windows Server 2012 / Windows Server 2008 R2 / Windows Server 2008 / Windows Server 2003 / Windows Server 2000 with .NET Framework 4.0 or higher with the latest service packs.
<b>Database:</b>	Microsoft SQL Server 2008 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2005 (Enterprise / Standard / Developer / Express edition) running in local / remote computer with latest Service Pack.
<b>Software:</b>	<u>MDAC v2.5/2.6/2.8</u>

#### For the Computers Reported by ARKWE

Windows 10 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2012 / Windows Server 2008 R2/ Windows Server 2008 / Windows 2003 / Windows 2000 with Microsoft Remote Registry Service enabled.

### **1.3 Who Can Use ARKWE?**

---

Organizations running Microsoft Windows Servers can greatly benefit from ARKWE. It is a powerful reporting tool for Windows Server Administrators. System Administrators can monitor and manage Microsoft Windows Servers across the enterprise network in any location. You can connect to a Windows Server if you are part of global administrator's group.

#### **Typical Users**

- Systems management personnel
- System Administrators
- Other Windows network product developers
- Trainers and educators
- Enterprise network planning personnel

#### **Typical Organizations that would benefit from this Product:**

- Companies having their LAN/WAN based Windows Enterprise Networks
- Windows based data warehousing companies
- Windows Server based Internet Service Providers
- Companies having Windows based Intranets
- Any company having Windows Servers and planning to manage their systems

### **1.4 How to purchase?**

---

You can purchase ARKWE online from our website <http://www.vyapin.com/>. Please contact our Sales department at [sales@vyapin.com](mailto:sales@vyapin.com) for sales and price related queries.

### 1.5 How to register the Software?

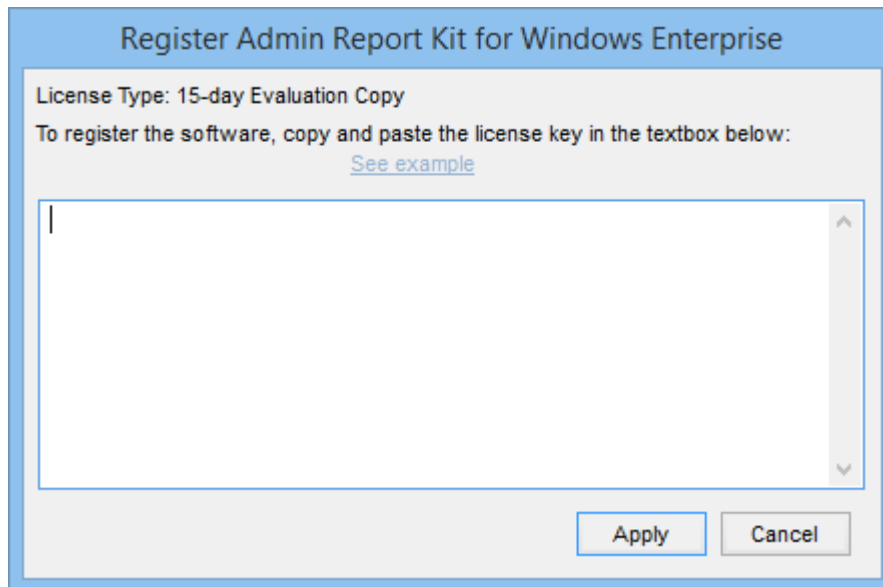
---

Once you purchase the software online or through any one of our resellers, you will receive a sale notification through e-mail from our sales department. We will send you an e-mail with the necessary instructions to activate the software.

In case you do not receive an e-mail from our sales team after you purchase the software, please send the following information to our sales department at [sales@vyapin.com](mailto:sales@vyapin.com) with the sales order number:

- **Company Name:** End-user Company Name
- **Location:** City & Country for the Company Name given above

Please allow 12 to 24 hours from the time of purchase for our sales department to process your orders.

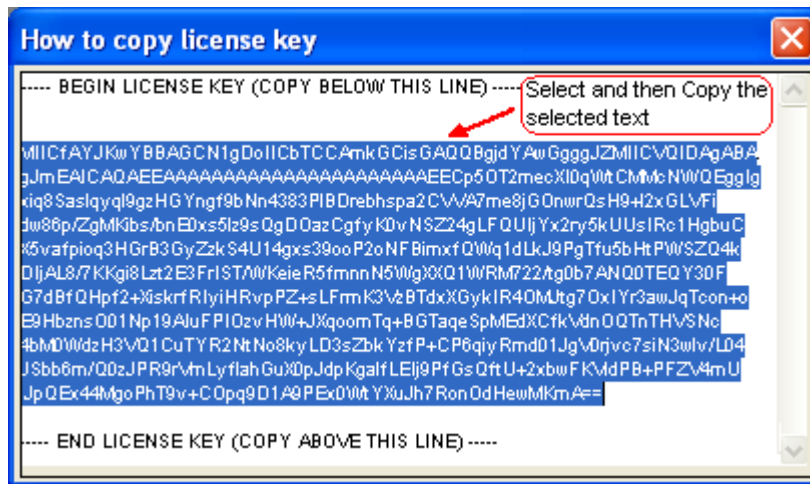


**Image 1 - Register screen**

Perform the following steps to activate the software:

- 1) Download evaluation/trial copy of software from the respective product page available in our website at <http://www.vyapin.com/>
- 2) Install the software on the desired computer.
- 3) You will receive a license key through e-mail as soon as the purchase process is complete.
- 4) Click 'Register license key' in Help -> About -> Register license key option to see the Register dialog (as shown in Image 1).

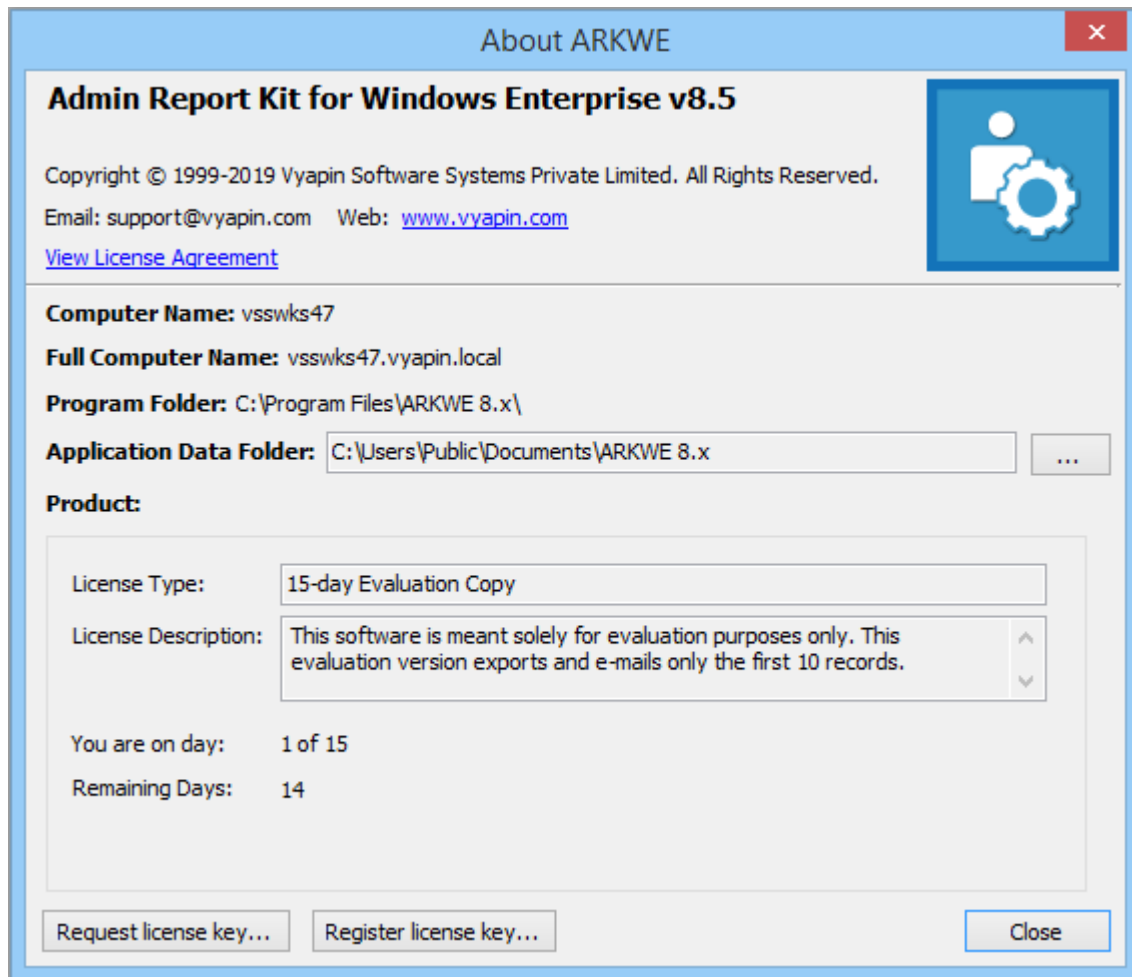
- 5) Copy the license key sent to you through email, and pastes it in the 'License Key' textbox. For help on how to copy the license key, click 'See example' link in the Register dialog (as shown in Image 2).



**Image 2 - How to copy license key screen**

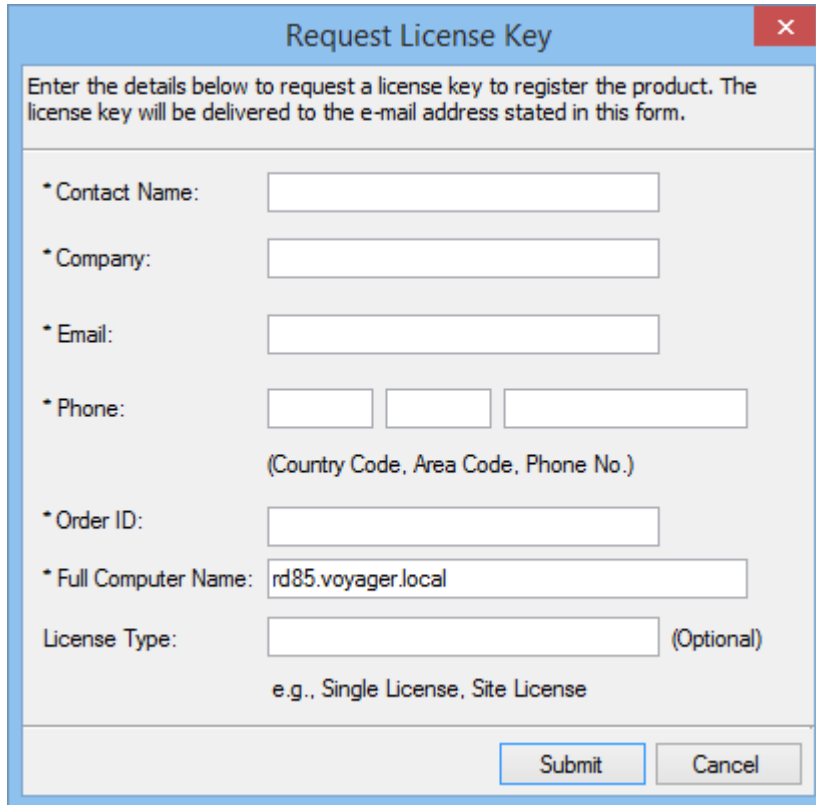
### **Request License Key:**

- Select About ARKWE from File.
- The About ARKWE dialog will appear as shown below:



### About screen

- Click **Request license key...** button. The Request License Key dialog will appear as shown below:



The image shows a Windows-style dialog box titled "Request License Key". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains a text box with the instruction: "Enter the details below to request a license key to register the product. The license key will be delivered to the e-mail address stated in this form." Below this are several labeled input fields: "\* Contact Name:", "\* Company:", "\* Email:", "\* Phone:" (with three sub-inputs for Country Code, Area Code, and Phone No.), "\* Order ID:", "\* Full Computer Name:" (containing "rd85.voyager.local"), and "License Type:" (with a dropdown menu and "(Optional)" text, and an example "e.g., Single License, Site License" below it). At the bottom right are "Submit" and "Cancel" buttons.

### Request License Key screen

- Enter the following details and click Submit to place the license key request through email.
  - **Contact Name:** End-user of the product.
  - **Company:** End-user Company Name.
  - **Email:** Email address where the license key has to be sent.
  - **Phone:** Phone number with country code and area code.
  - **Order ID:** Order/Transaction ID reference.
  - **Full Computer Name:** Full computer name that was purchased.
  - **License Type:** License that was purchased.

### 1.6 Technical Support

---

ARKWE Frequently Asked Questions (FAQ) section is available online at our website <http://www.vyapin.com>.

Please direct all technical support questions to [support@vyapin.com](mailto:support@vyapin.com). Include the following information to expedite a response:

- a) Include the version of the product you are using.
- b) If the problem is associated with installation, include the steps that led to the problem.
- c) If the problem is associated with usage, please state the series of steps you performed.
- d) Include the version of the OS, info about any service packs or hot-fixes and local language of the OS installed.
- e) Attach the Error Log File available in the common application data path of ARKWE (e.g., <Application Data Folder> \ARKWE 8x\ARKWEErrorLog.log).

#### **NOTE:**

<Application Data Folder> is the common area where ARKWE settings will be stored in the machine running ARKWE. The <Application Data Folder> can be found from the Help -> About screen. The default path of <Application Data Folder> is as follows:

- a) Windows XP Windows 2003-C:\Documents and Settings\All Users\Documents
- b) Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 2008, Windows Server 2012 - C:\Users\Public\Documents

## 2 Getting Started

---

### 2.1 Configuration Wizard

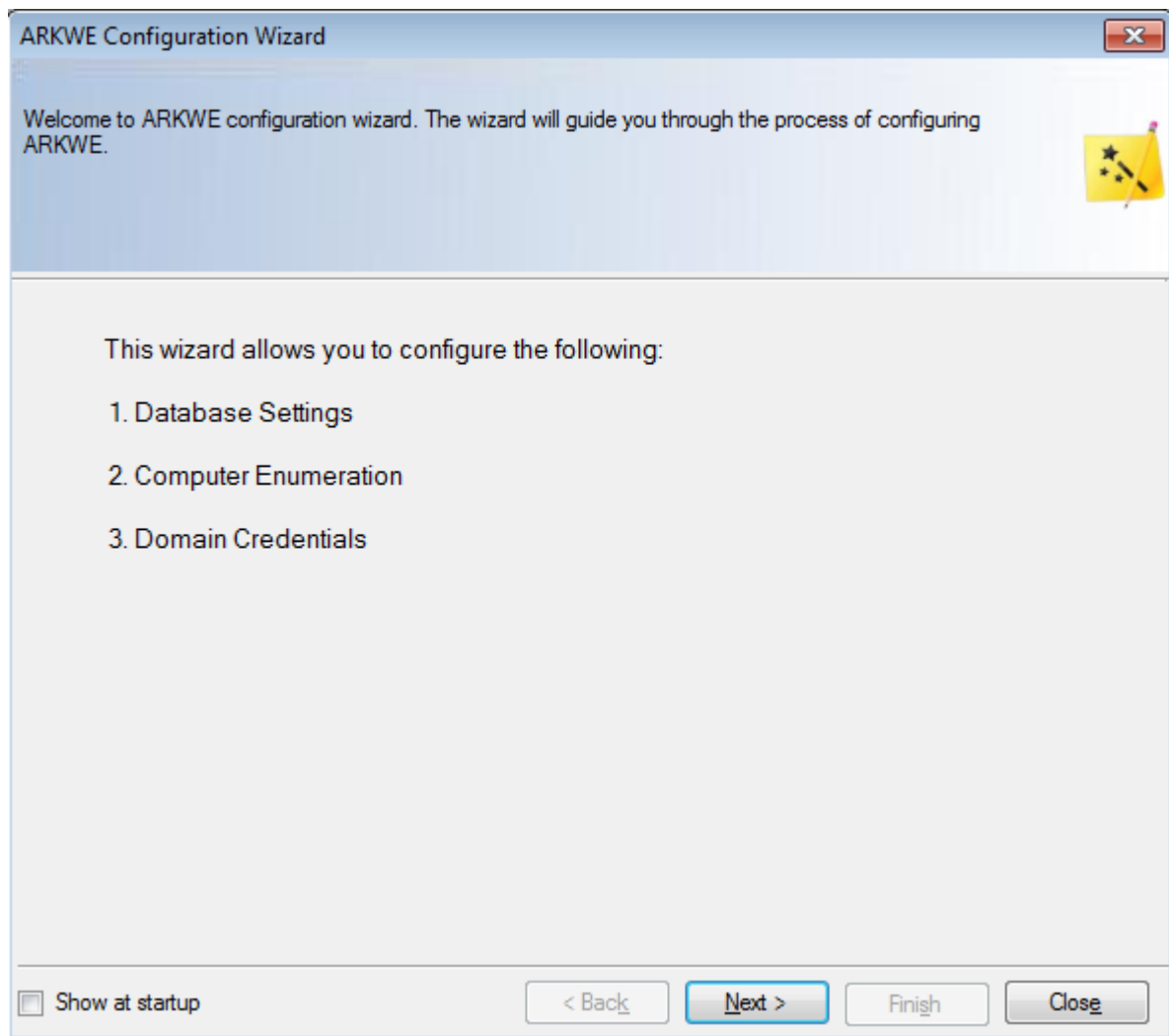
---

#### Configure ARKWE

There are two ways to configure ARKWE - one through the configuration wizard and the other by directly modifying the specific configuration settings.

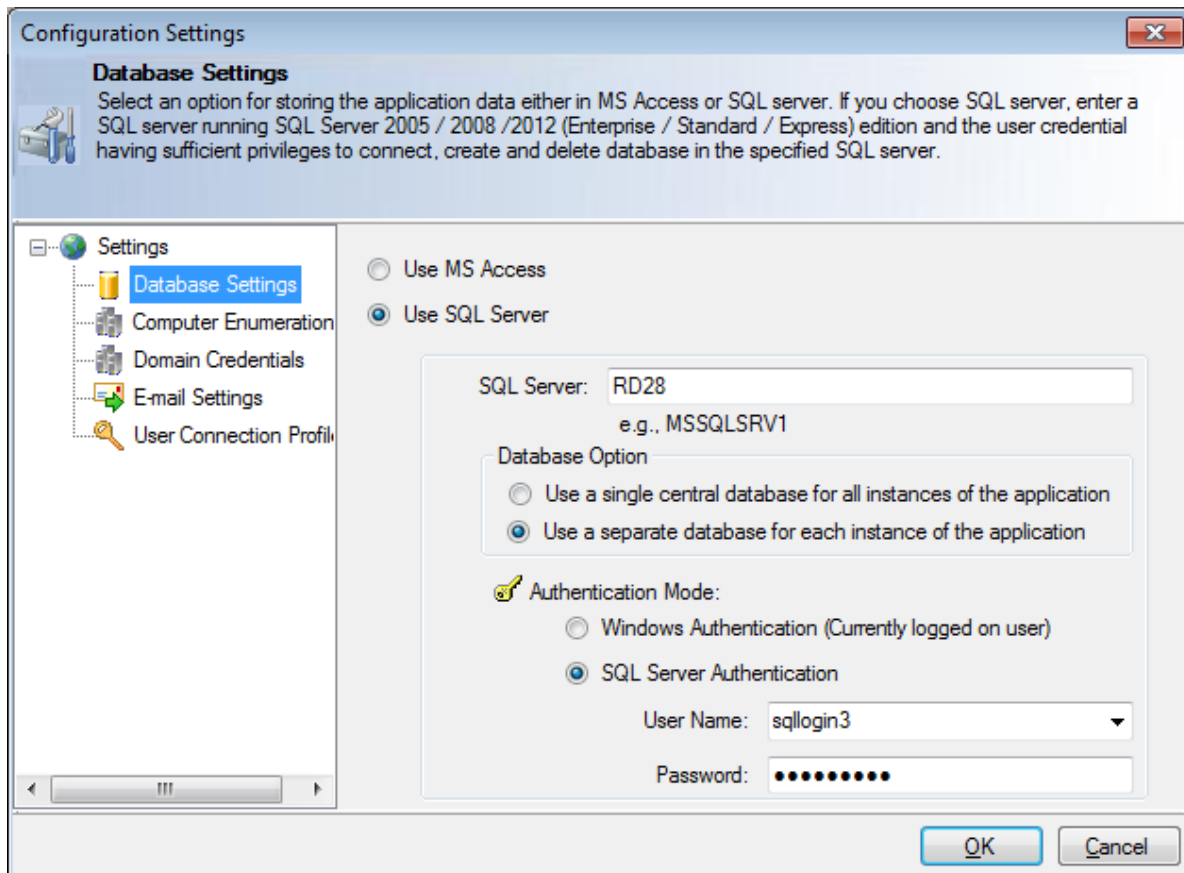
#### Using ARKWE Configuration Wizard

ARKWE configuration wizard will help you configure the application during the startup of the first run. You can access the wizard anytime by choosing **Tools > Configuration Wizard** from the main application menu.



Click **Next** to proceed.

### Step 1 of 3: Database Settings



ARKWE may be configured to use either MS-Access MDB or SQL Server database for its data storage to generate reports. If you choose SQL server, ARKWE requires an SQL Server running SQL Server 2012 / 2008 / 2005 (Enterprise / Standard / Express editions) to connect and create a database. ARKWE will connect to the specified SQL Server based on the authentication mode and the user credentials to create and manage its own application databases. Database will be created in the specified SQL server based on the following database options (whichever is selected):

**1) Use a single central database for all instances of the application**

- A new database will be created in the SQL server by the name ARKWE. Inside the ARKWE database, separate tables will be created for each installation of ARKWE. The table names will be prefixed with the computer name that is running ARKWE application. Thus, each installation of ARKWE will deploy its own tables based on the computer where ARKWE is installed. For example, if you install the software on 3 different computers, single database with 3 different tables will be created inside the single

database and each installed application will generate reports separately independent of each other.

**2) Use a separate database for each instance of the application**

- A new database will be created in the SQL server by the name ARKWE-<COMPUTERNAME>, where COMPUTERNAME stands for the computer name that is running ARKWE application. Thus, each installation of ARKWE will deploy its own database based on the computer where ARKWE is installed. For example, if you install the software on 3 different computers, 3 different databases will be created and each installed application will generate reports separately independent of each other.

Specify the SQL Server name, authentication mode, user name and password in the above screen.

Click **Next** to proceed.

### **Step 2 of 3: Computer Enumeration**

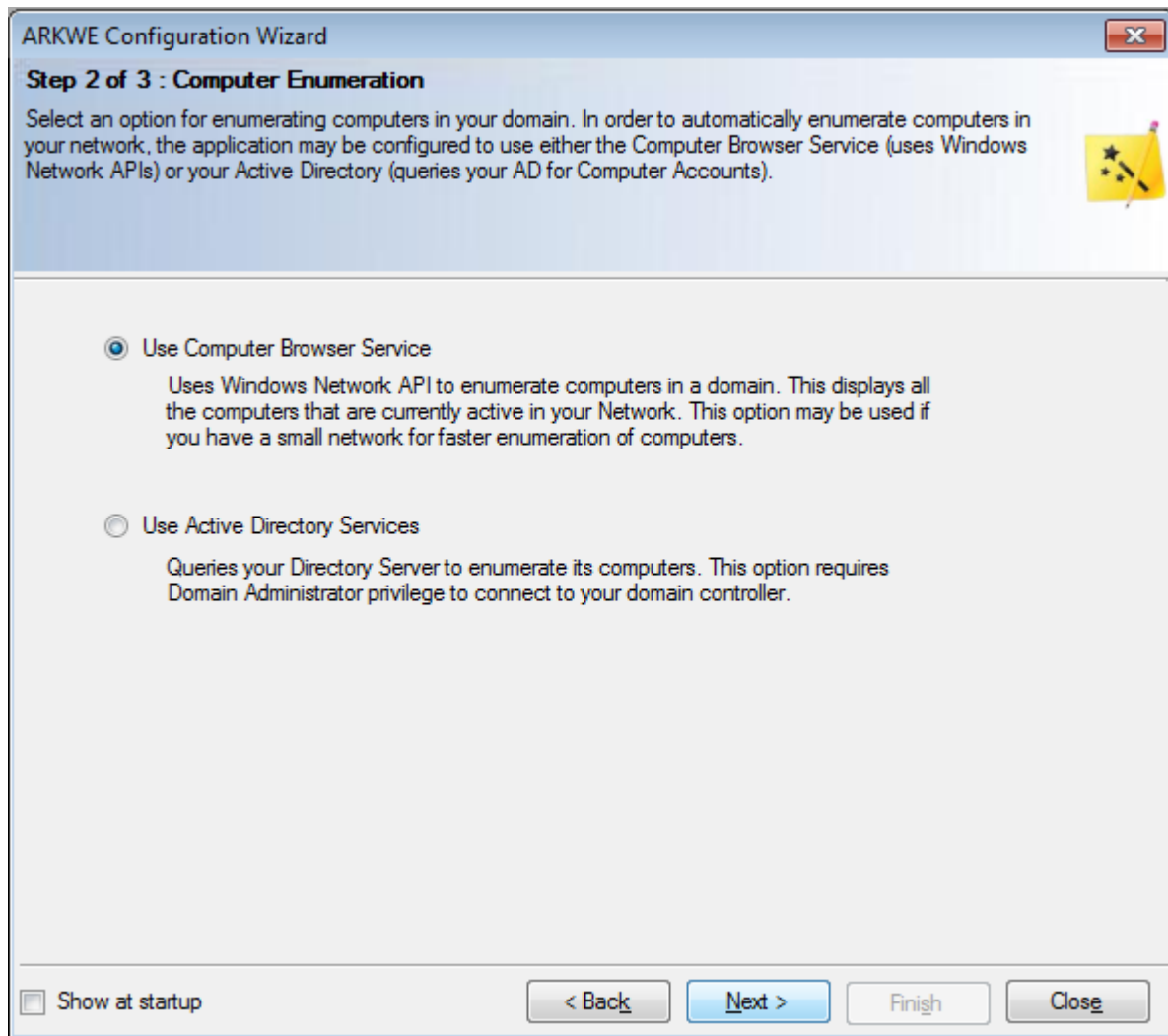
ARKWE uses Computer Browser Services or Active Directory services for enumerating computers in your domain. In order to automatically enumerate computers in your network, the application may be configured to use either the Computer Browser Service (uses Windows Network APIs) or your Active Directory (queries your AD for Computer Accounts).

**1) Use Computer Browser Service**

- Uses Windows Network API to enumerate computers in a domain. This displays all the computers that are currently active in your Network. This option may be used if you have a small network for faster enumeration of computers.

**2) Use Active Directory Services**

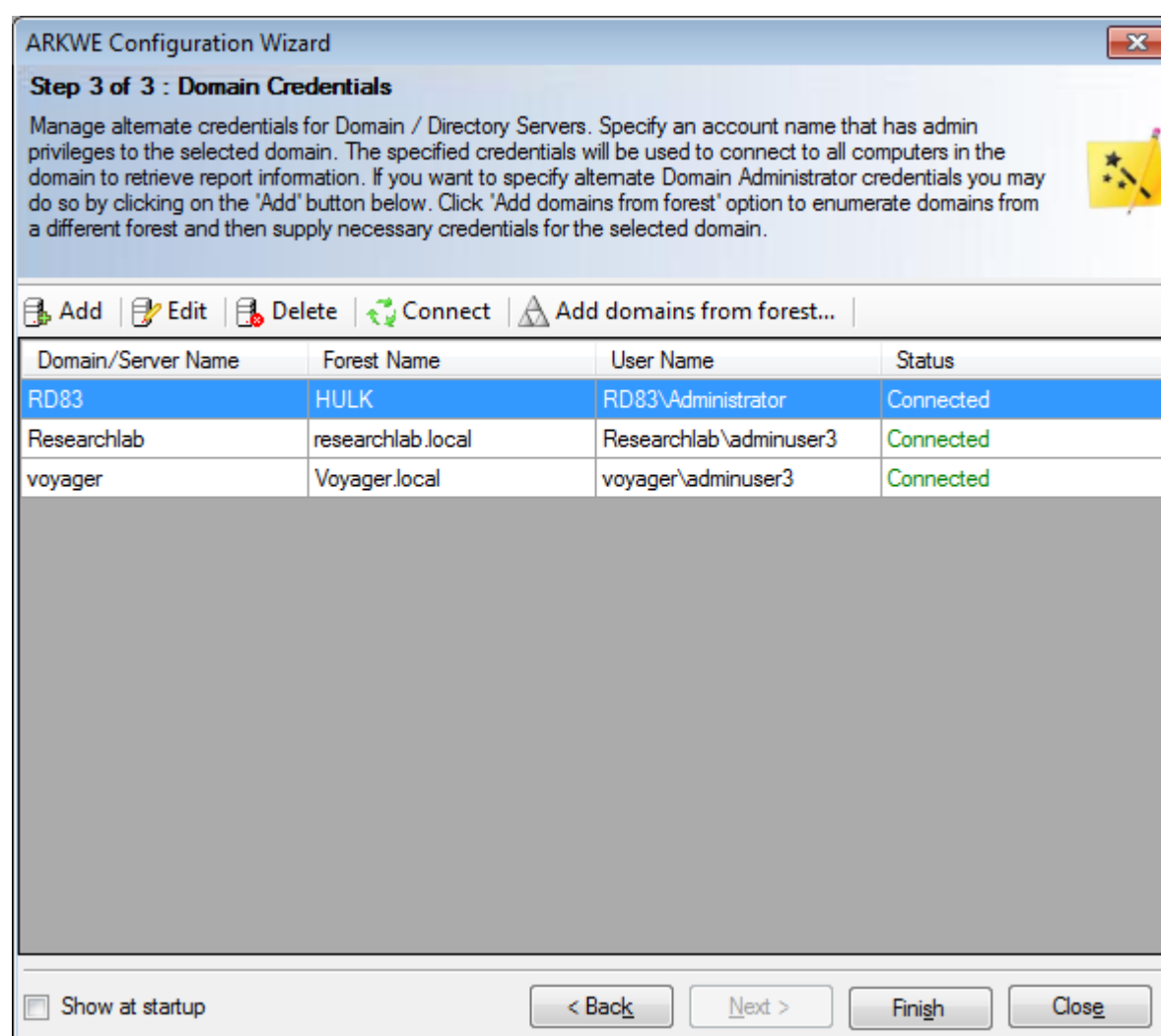
- Queries your Directory Server to enumerate its computers. This option requires Domain Administrator credentials to connect to your domain controller.



Click **Next** to Proceed.

### Step 3 of 3: Domain Credentials

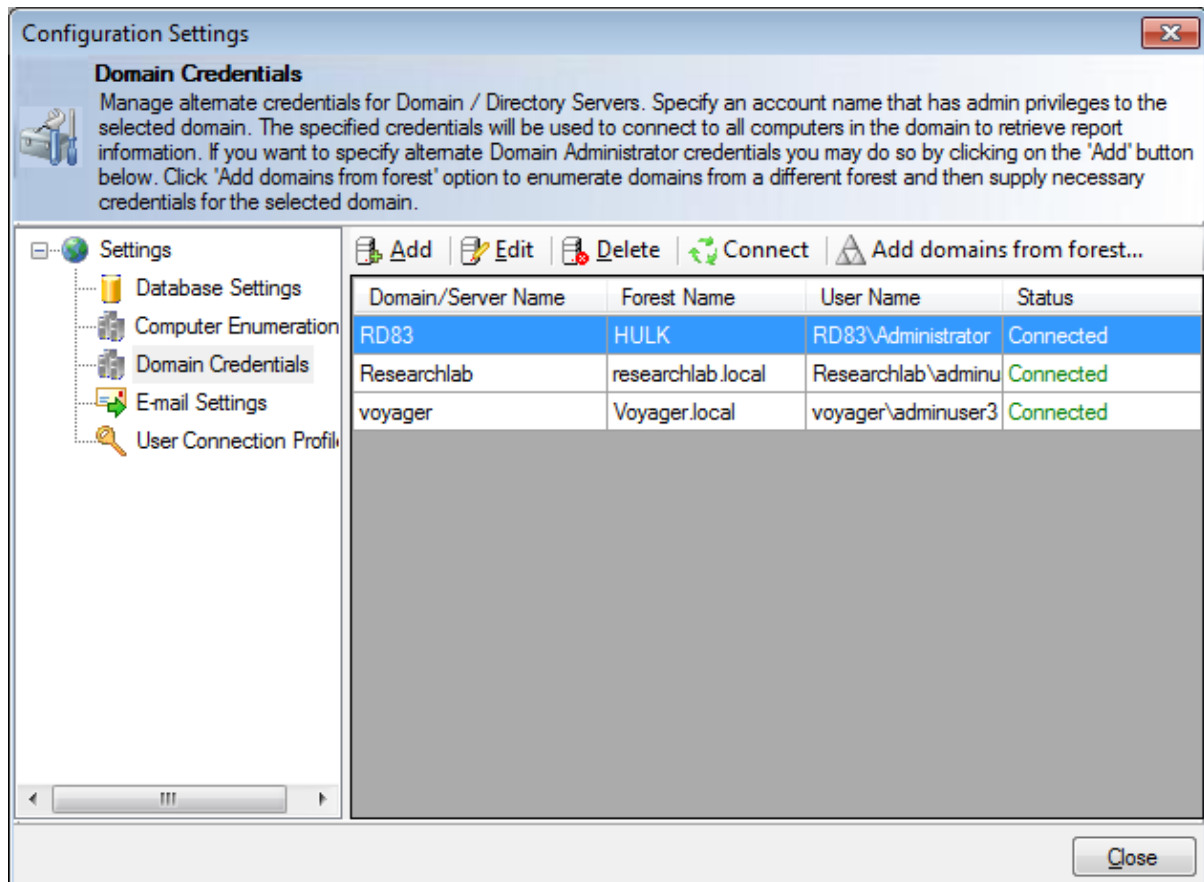
Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers, shares and to collect report data. If you want to specify alternate Domain Administrator credentials you may do so by clicking on the 'Add ' button below. Click 'Add domains from forest' option to enumerate domains from a different forest and then supply necessary credentials for the selected domain.



For more information on Domain Credentials please refer Domain Credentials. Click Finish to save the configuration details.

### Using the Configuration Settings Dialog

You may directly modify the configuration settings, once you get familiar with the user interface. You may access the Configuration Settings menu from the Tools menu in the application. Once you open the Settings window, you will see the different modules for configuration.

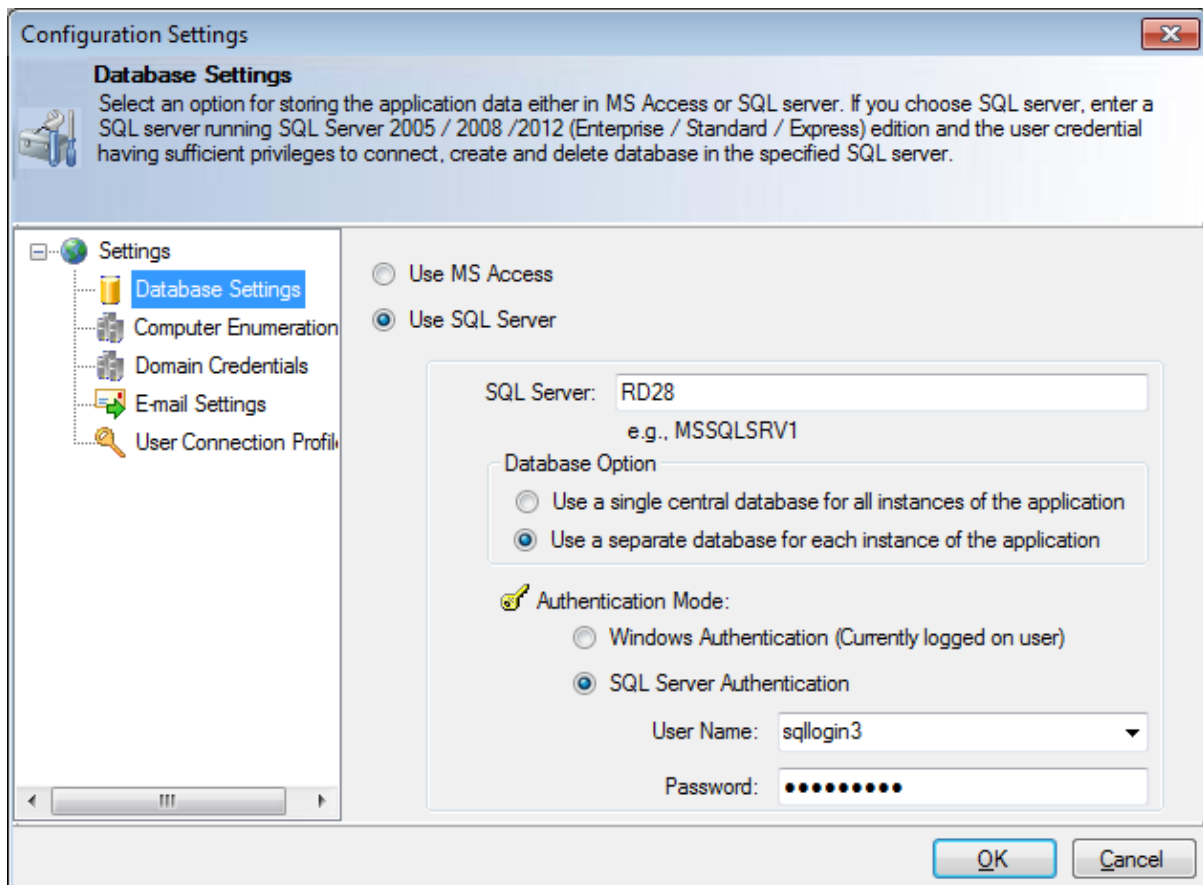


### Configuration Settings

#### 2.1.1 Database Settings

ARKWE may be configured to use either MS-Access MDB or SQL Server database for its data storage to generate reports. If you choose SQL server ARKWE requires an SQL Server running SQL Server 2005 / 2008 / 2012 (Enterprise / Standard / Express editions) to connect and create a new application database. ARKWE will connect to the specified SQL Server based on authentication mode and user credentials to manage its own application database.

You can access the Database settings by clicking Tools -> Configuration Settings menu in the ARKWE main application window and choose Database settings, as shown below:



#### User Authentication

To connect to SQL Server, ARKWE uses the relevant user accounts based on the authentication mode as listed below:

### A. Windows Authentication:

In this method, ARKWE uses the currently logged on user account while running reports

### B. SQL Authentication:

In this method, ARKWE uses the specified SQL user account and password while running reports. ARKWE stores the SQL user name and password as a user profile in 'Stored User Names and Passwords' applet for its usage.

**Note: ARKWE expects the user account to have sufficient privileges to create, add to and delete database in the SQL server.**

### Database Creation

ARKWE creates databases in SQL Server based on the following database options (whichever is selected) as outlined below:

- 1) Use a single central database for all instances of the application
  - A new database will be created in the SQL server by the name ARKWE. Inside the ARKWE database, separate tables will be created for each installation of ARKWE. The table names will be prefixed with the computer name that is running ARKWE application. Thus, each installation of ARKWE will deploy its own tables based on the computer where ARKWE is installed. For example, if you install the software on 3 different computers, single database with 3 different tables will be created inside the single database and each installed application will generate reports separately independent of each other.
- 2) Use a separate database for each instance of the application
  - ARKWE creates a single application database in the default data storage location used by the SQL Server during application launch. ARKWE uses the following naming convention: ARKWE-<COMPUTERNAME>, where COMPUTERNAME is the name of the computer running ARKWE.
  - For example, if the computer running ARKWE is 'CLIENT01', ARKWE creates 'ARKWE-CLIENT01' with data ('ARKWE-CLIENT01.mdf') and log ('ARKWE-CLIENT01\_log.LDF') files stored in the default SQL data folder in the SQL server (for example, C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data).

### Database Cleanup

ARKWE will delete the application database while uninstalling the ARKWE application from the computer.

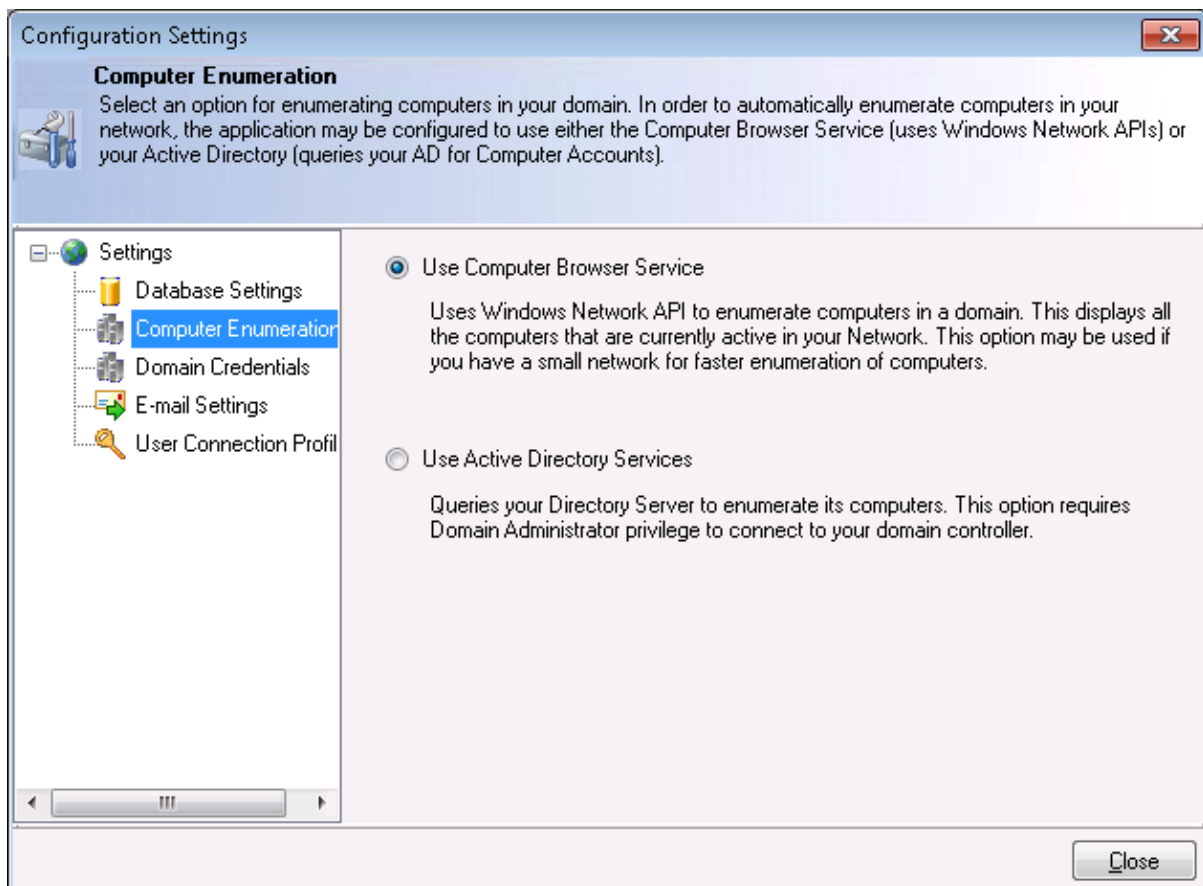
### 2.1.2 Computer Enumeration

#### Configure Computer Enumeration

For enumerating computers in your network automatically, ARKWE uses either Computer Browser Service or Active Directory Services. Select an option for enumerating computers in your domain as shown below. You may use the Browser service if you have a smaller network, as it may take time for the Browser service to respond to data requests on large networks. The advantage of a Browser service is that it lists only those computers that are currently active or alive on your network. You may use the Active Directory Services option if you have a large network and you need a quicker enumeration of computers in your domain. However, this option requires that the domain controller is contacted and queried. Therefore, the currently logged on user must have sufficient privileges to connect to a domain controller or you may specify alternate domain credentials for a domain controller (see configuring the Domain Credentials section in the wizard).

**NOTE:** IF you use the Browser service, ensure that NETBIOS over TCP/IP is enabled in both the client and the computers that need to be reported on. The Browser service must also be running.

You can access the Computer Enumeration settings by clicking Tools -> Configuration Settings menu in the ARKWE main application window and selecting "Computer Enumeration" node as shown below:



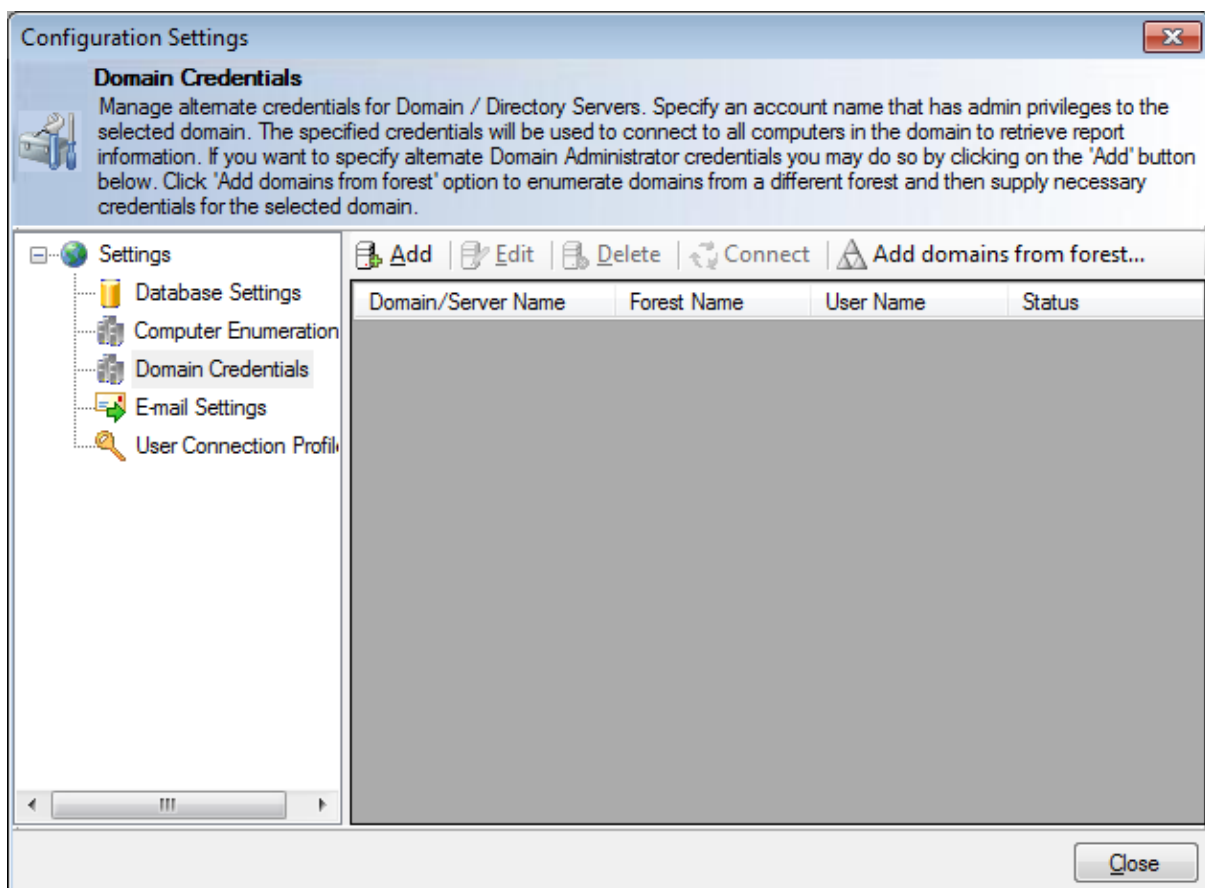
### 2.1.3 Configuring Domain Credentials

#### Domain Credentials

Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers, shares and to collect report data. If you want to specify alternate Domain Administrator credentials you may use this option.

#### Configuring Domain Credentials

You can access the Domain Credentials settings by selecting the Domain Credentials option in the Configuration Settings window.

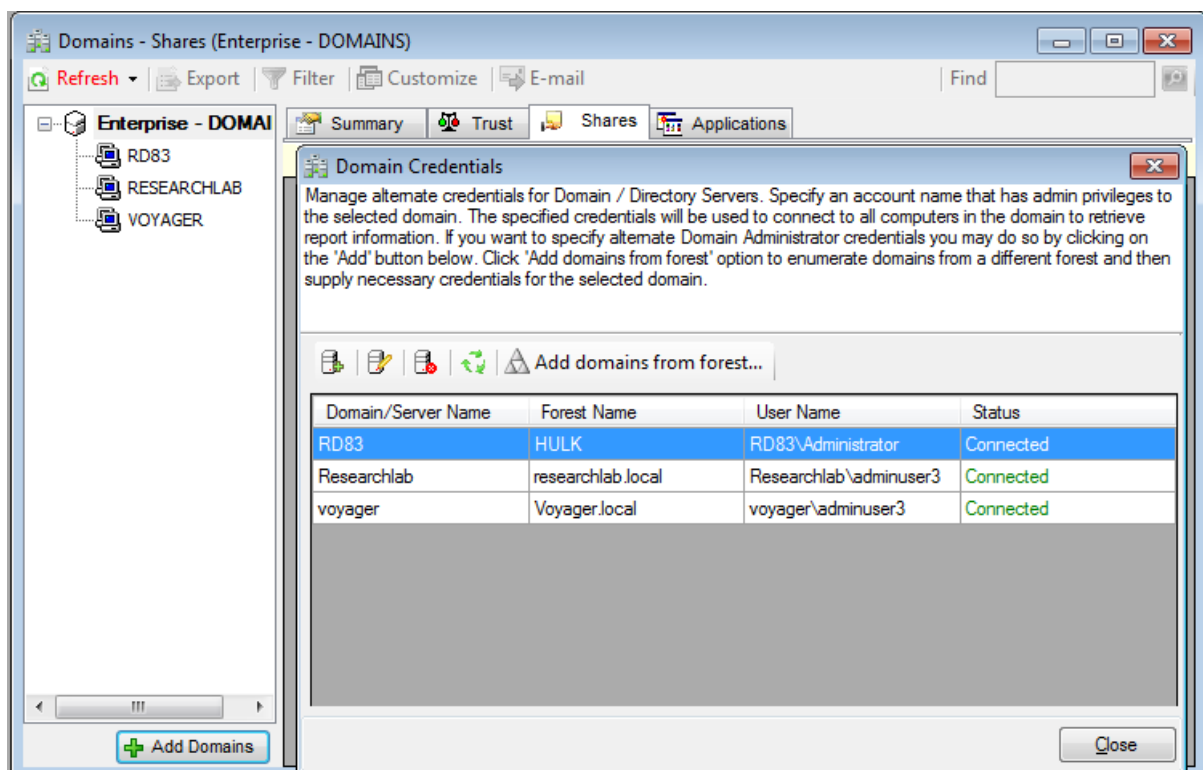
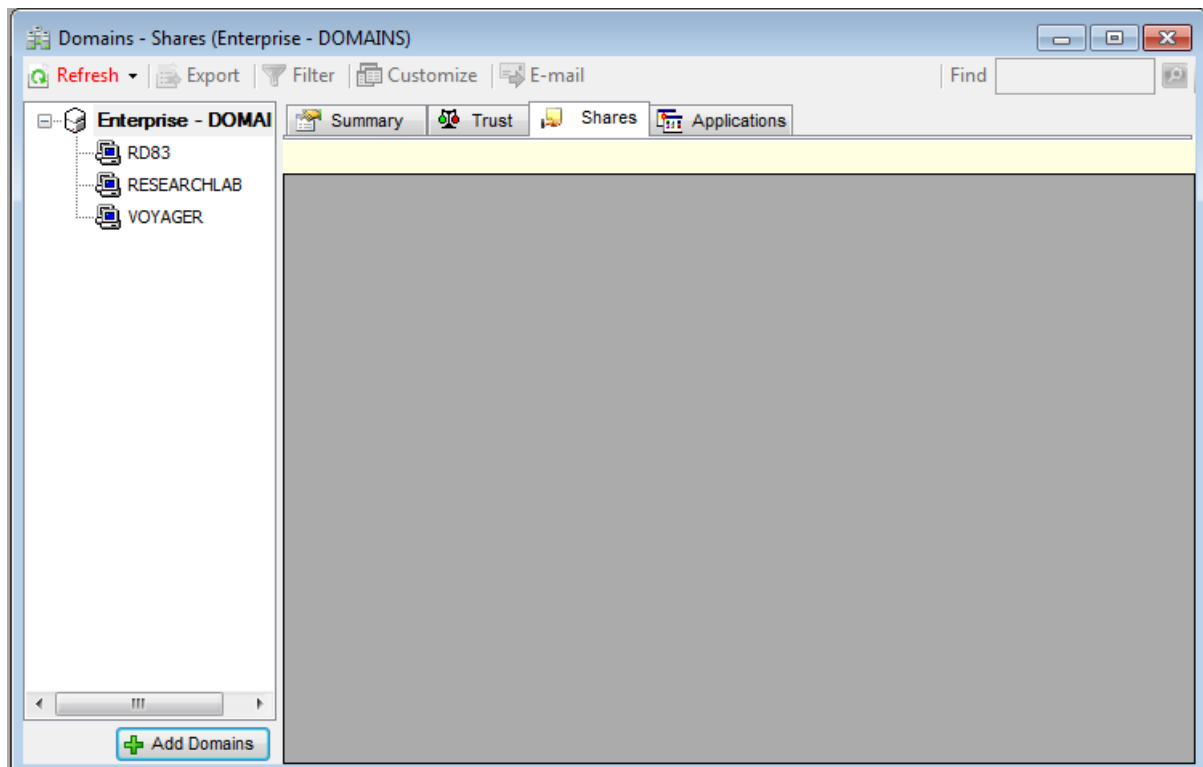


If you have chosen Active Directory Services under the Computer Enumeration settings, you can launch the ARKWE Domain Credentials window within a report window by doing the following:

- 1) Select any one of the reports from the ARKWE main application window. For example Standard Reports -> Domains-Shares option.
- 2) The action will launch the Domains-Shares report window.

## CHAPTER 1 - About Admin Report Kit for Windows Enterprise (ARKWE)

- 3) In the report window, at the bottom of the treeview click **Add Domains** button. This action will launch the "**Domain Credentials**" window as shown below.



The various operations that can be performed in the Domain Credentials screen are given below:


<b>Operation</b>	<b>Description</b>
Add	To Add a new domain to the list.
Edit	To Edit the properties of a domain/server in the list. Select a domain/server and click Edit button.
Delete	To Delete a domain/server from the list. Select a domain/server and click Delete button.
Connect	To connect to a domain/server in the list. Select a domain/server and click Connect button.

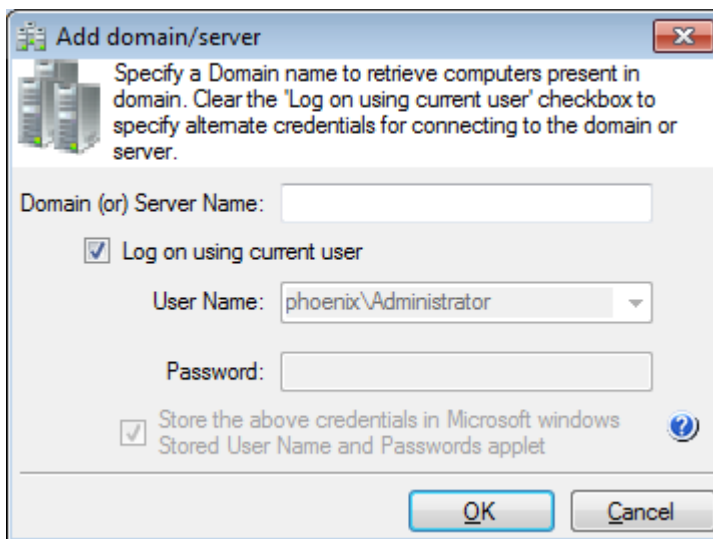
### 2.1.4 Add a Domain/Server

---

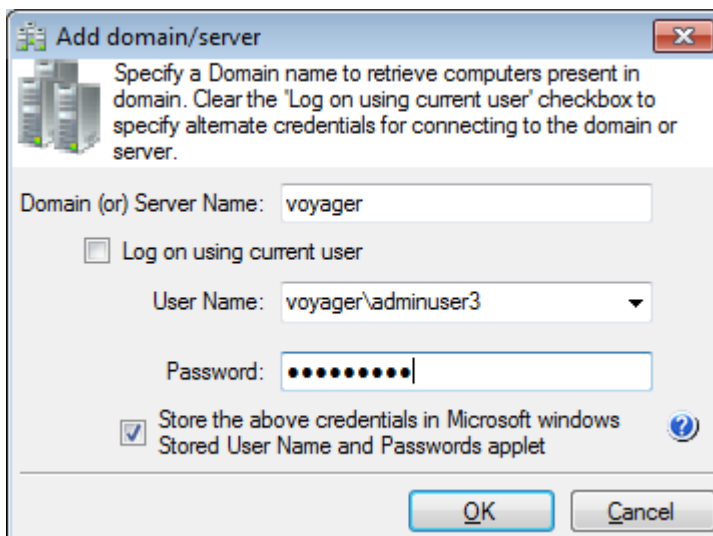
You may also add one single domain or server at a time to the list of domains or servers in the credentials list by using Add Domain/Server feature.

#### Add a domain to the list

- 1) Launch Domain Credentials window.
- 2) In the Domain Credentials window, click  **Add** button to add a domain/server to the list.
- 3) The New **Add domain/server** dialog will be displayed as shown below:



Enter the name of a domain or server.

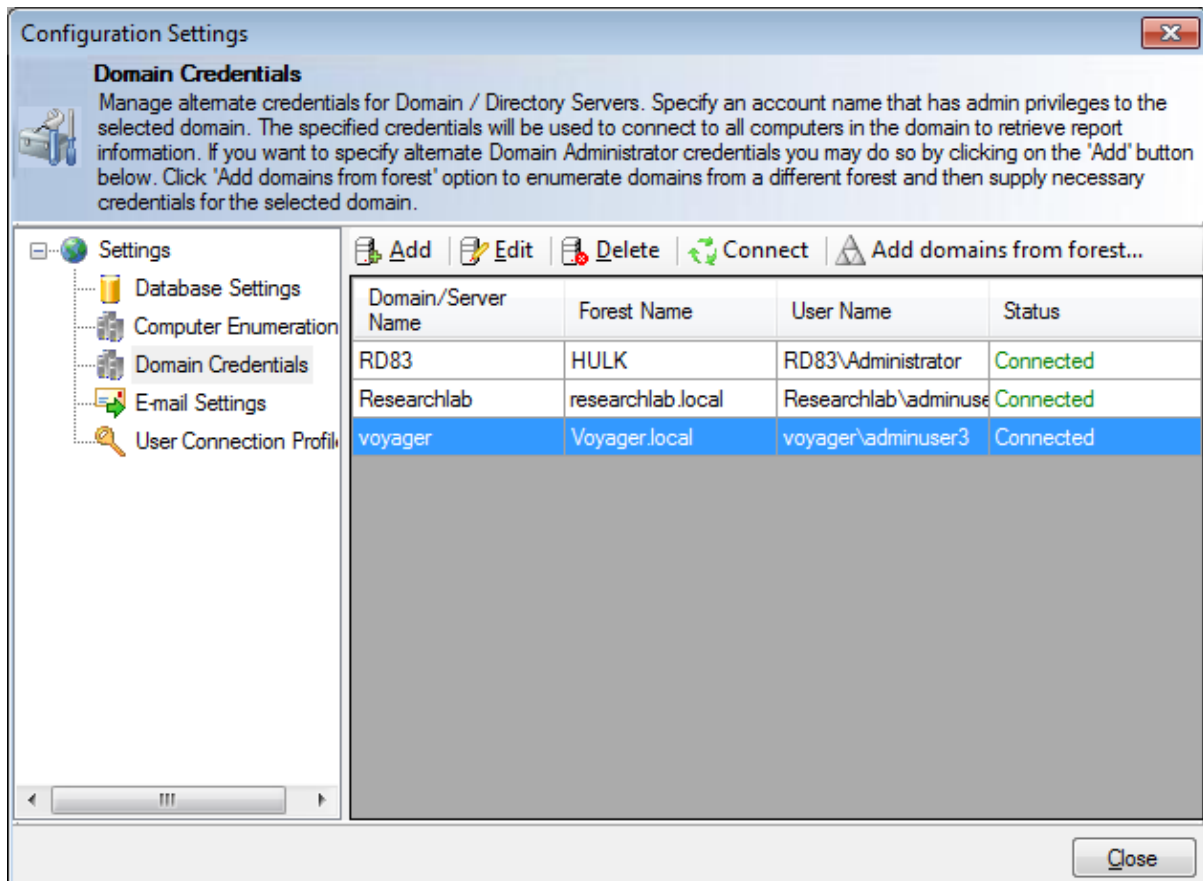


- 4) Specify user name and the corresponding password to connect to the specified domain or server.

**Store the above user credential in Microsoft Windows Stored User Names and Passwords applet** - ARKWE allows the user to enter different user credentials to connect to the domain/server. Uncheck the checkbox 'Log on using current user' if you like to connect to the domain/server using a different user context.

ARKWE will store the user credential to connect to domain/server in the Microsoft Windows Stored User Names and Passwords applet / Credential Manager for security reasons. The stored user profile is tied to the user context (currently logged on user account) in which the profile is created.


- 5) Click OK to add the domain/server to the Domain Credentials list.
- 6) ARKWE will connect to the domain/server with the newly provided connection parameters and add it to the list, upon successful connection to the domain/server.

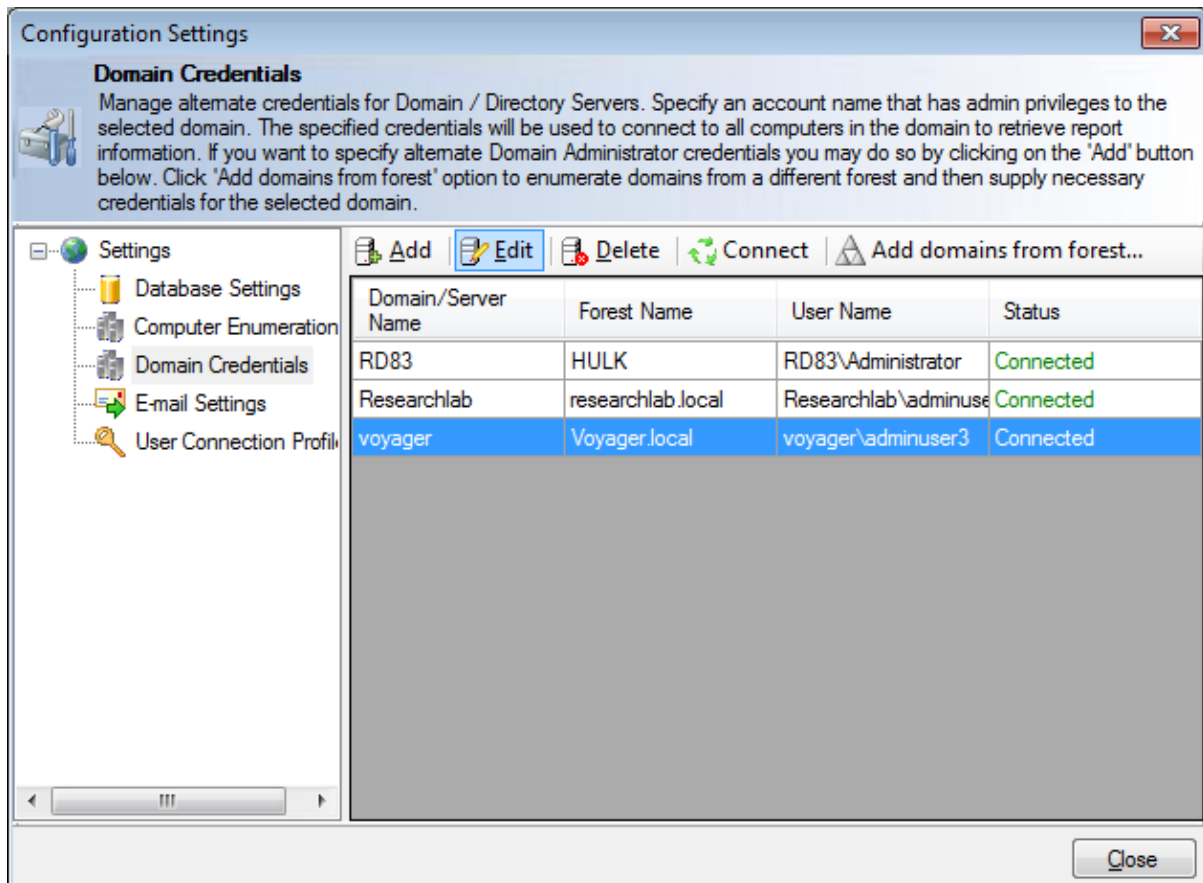


- 7) Click Cancel to abort the add process of the domain/server to the Domain Credentials list.

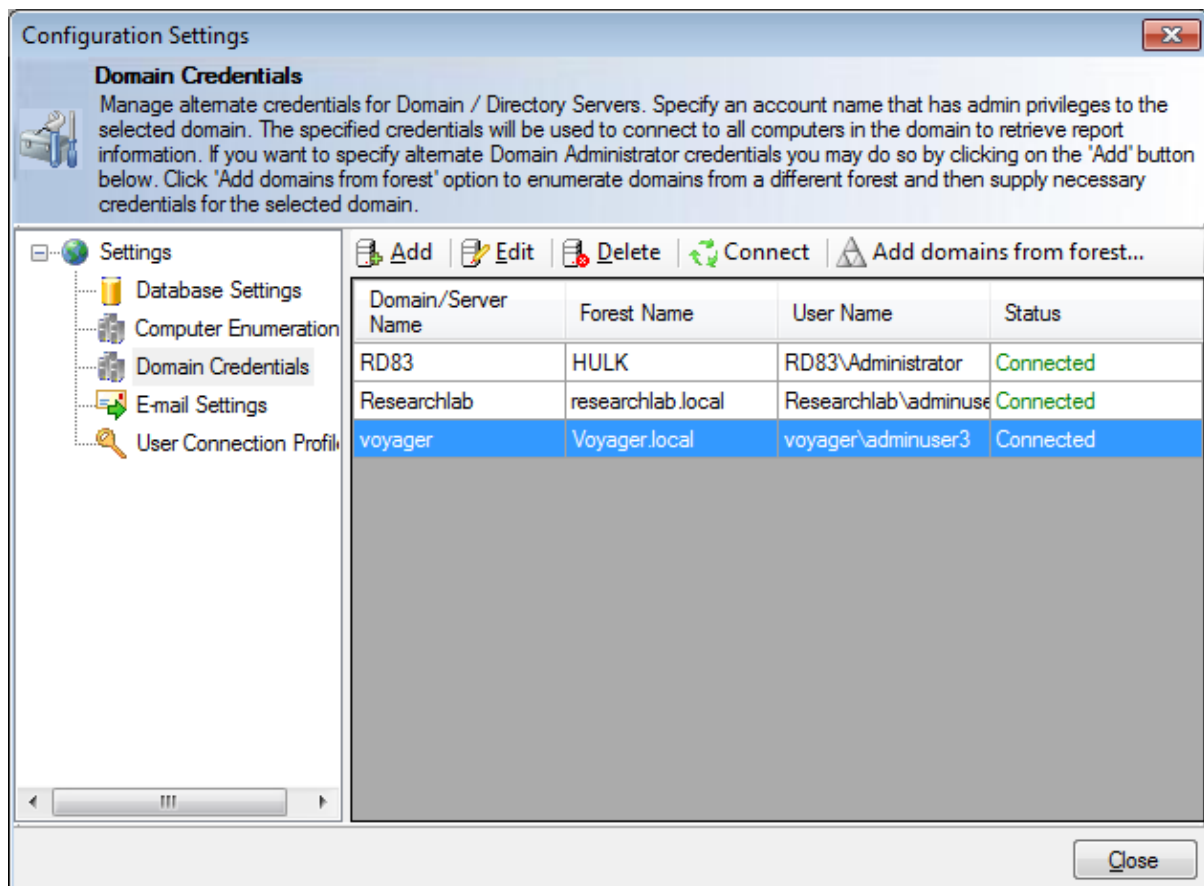
### 2.1.5 Edit a Domain/Server

To Edit a domain/server in the Domain Credentials, follow the steps given below:

- 1) Launch Domain Credentials window.
- 2) In the Domain Credentials window, select any row (domain), Click  **Edit** button to Edit an existing domain/server in the list, as shown below:




- 3) The domain/server name cannot be modified during the edit operation.
- 4) Specify user name and the corresponding password to connect to the specified domain/server.
- 5) Click **OK** to save and connect to the domain/server with the newly provided connection parameters and update the domain/server in the Domain Credentials list.
- 6) ARKWE will connect to the domain/server with the newly provided connection parameters and modify it in the list, upon successful connection to the domain/server.

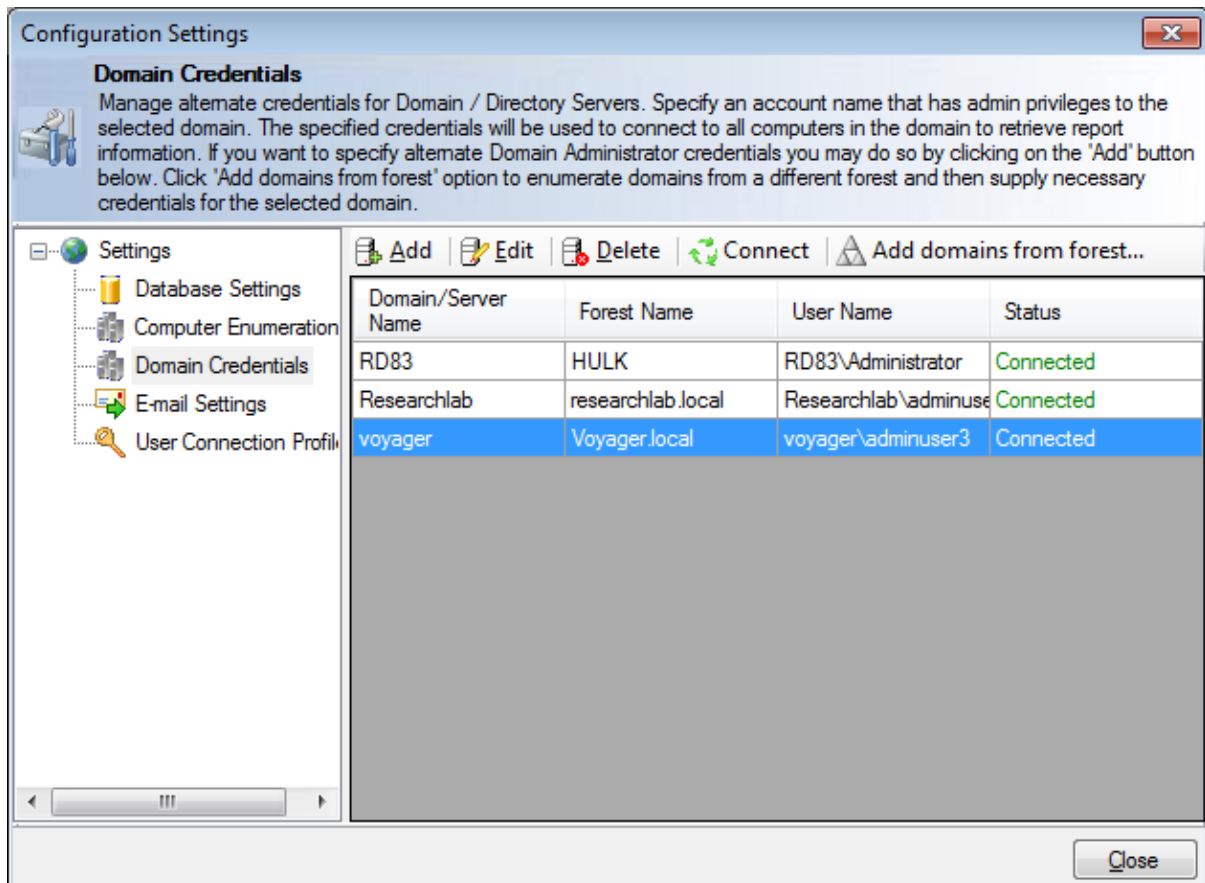


- 7) Click **Cancel** to retain the existing connection parameters of the domain/server in the Domain Credentials list.

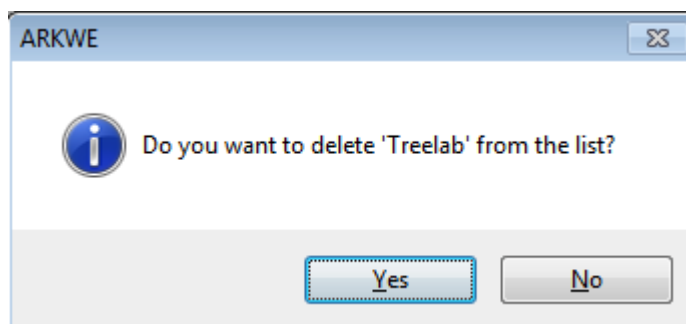
### 2.1.6 Delete a Domain/Server

Perform the following steps to delete a domain/server:

- 1) Launch Domain Credentials window.
- 2) In the Domain Credentials window, select any row (domain), click  **Delete** button to delete the forest from the Domain Enumeration Manager list.



- 3) An alert message asking for confirmation to delete the domain/server will be displayed as shown below:




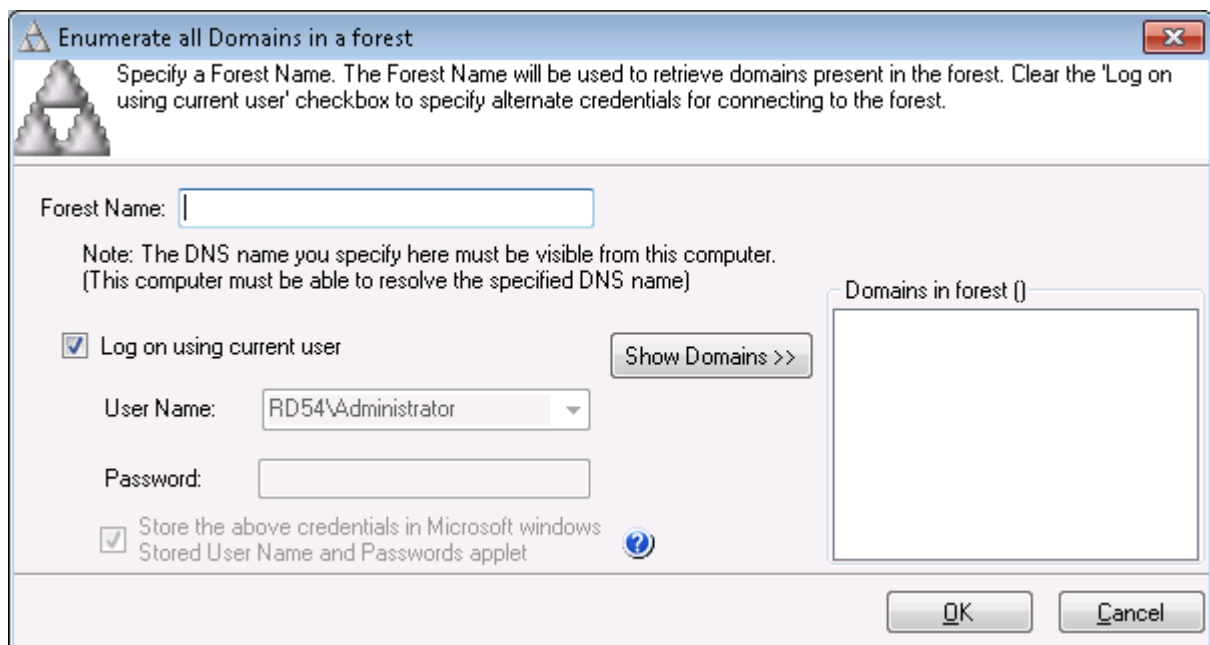
- 4) Click **Yes** to delete the selected forest.
- 5) Click **No** to abort the delete process of the selected forest.

### 2.1.7 Add Domains from Forest

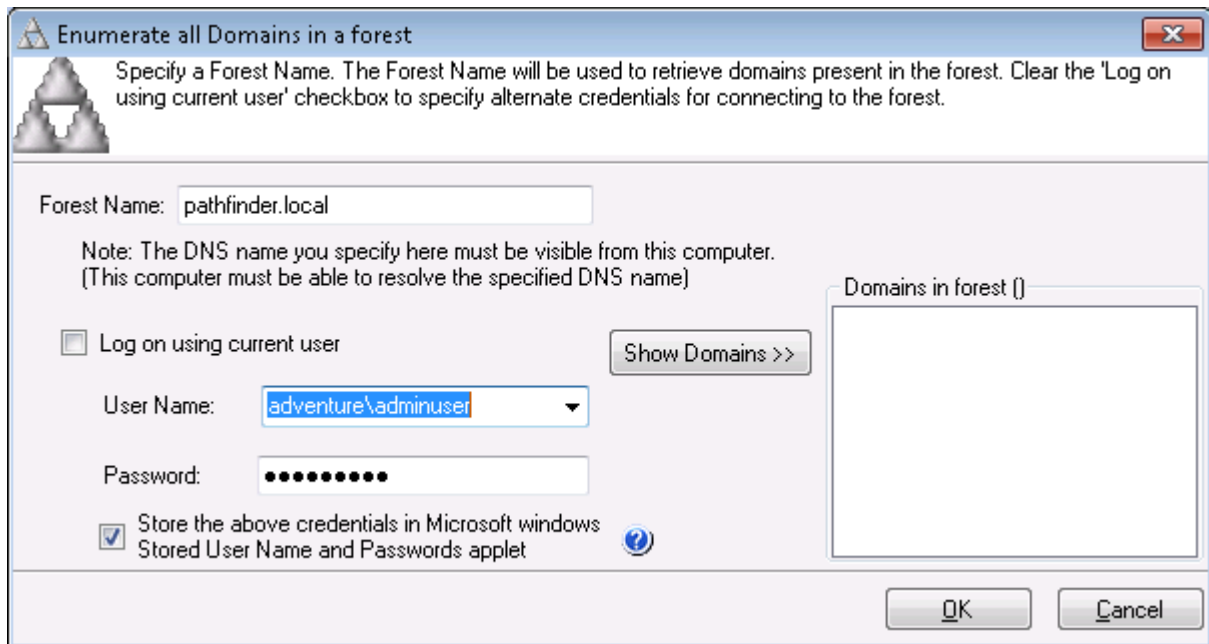
In order to connect to a different forest in your Active Directory and configure these domains for enumerating computers and generating reports on them, you may use the 'Add Domains from Forest' feature.

#### Add domains from forest to the list

- 1) Launch Domain Credentials window.
- 2) In the Domain Credentials window, click  to add domains from forest button to add domains in the forest to the list.
- 3) The **Enumerate All domains in a forest** dialog will be displayed as shown below:



Enter the name of a forest.



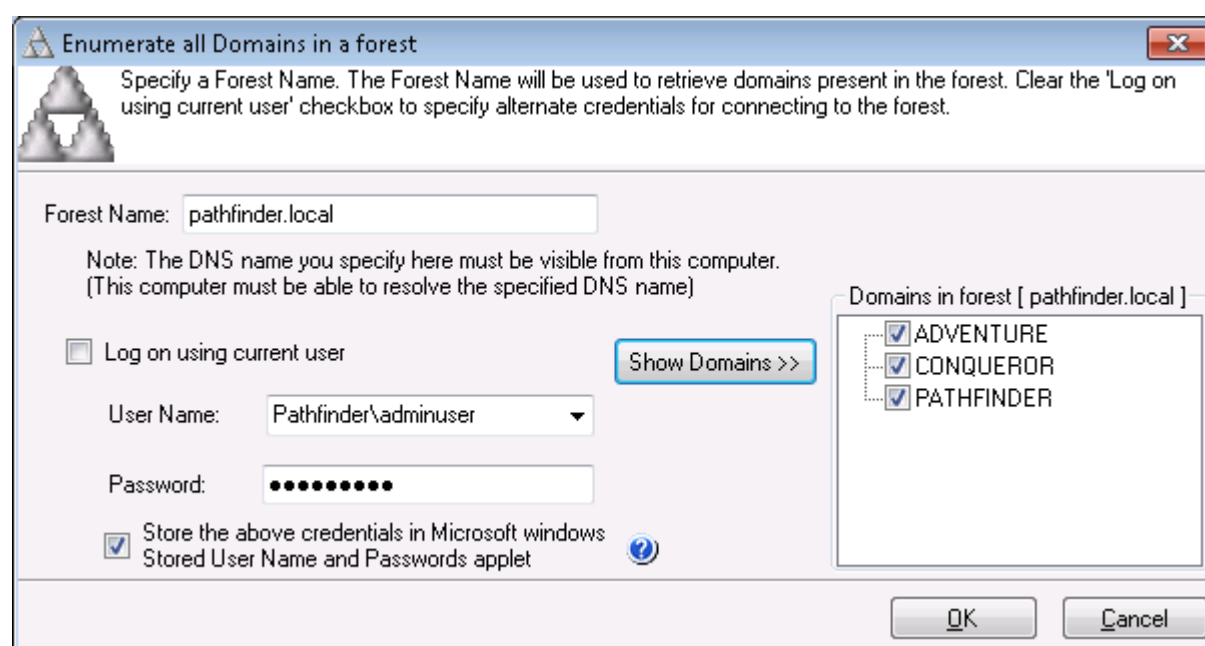
- 4) Specify user name and the corresponding password to connect to the specified forest.

**Store the above user credential in Microsoft Windows Stored User Names and Passwords applet** - ARKWE allows the user to enter different user

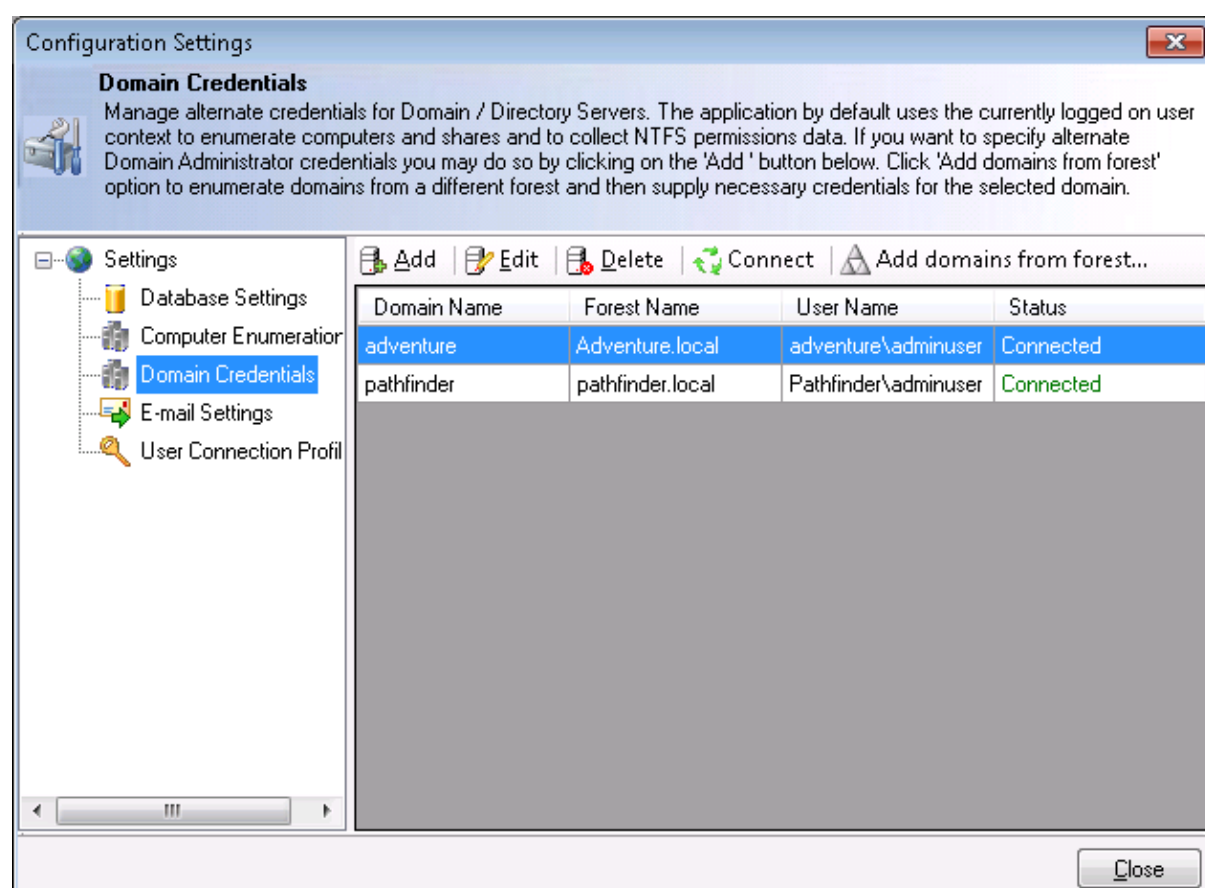
credentials to connect to the forest. Uncheck the checkbox 'Log on using current user' if you like to connect to the forest using a different user context.

ARKWE will store the user credential to connect to forest in the Microsoft Windows Stored User Names and Passwords applet / Credential Manager for security reasons. The stored user profile is tied to the user context (currently logged on user account) in which the profile is created.

- 5) Click 'Show Domains' button to add the domains in the specified forest to the list and select the desired domains in the list. Click OK to add the selected domains to the Domain Credentials list as shown below:



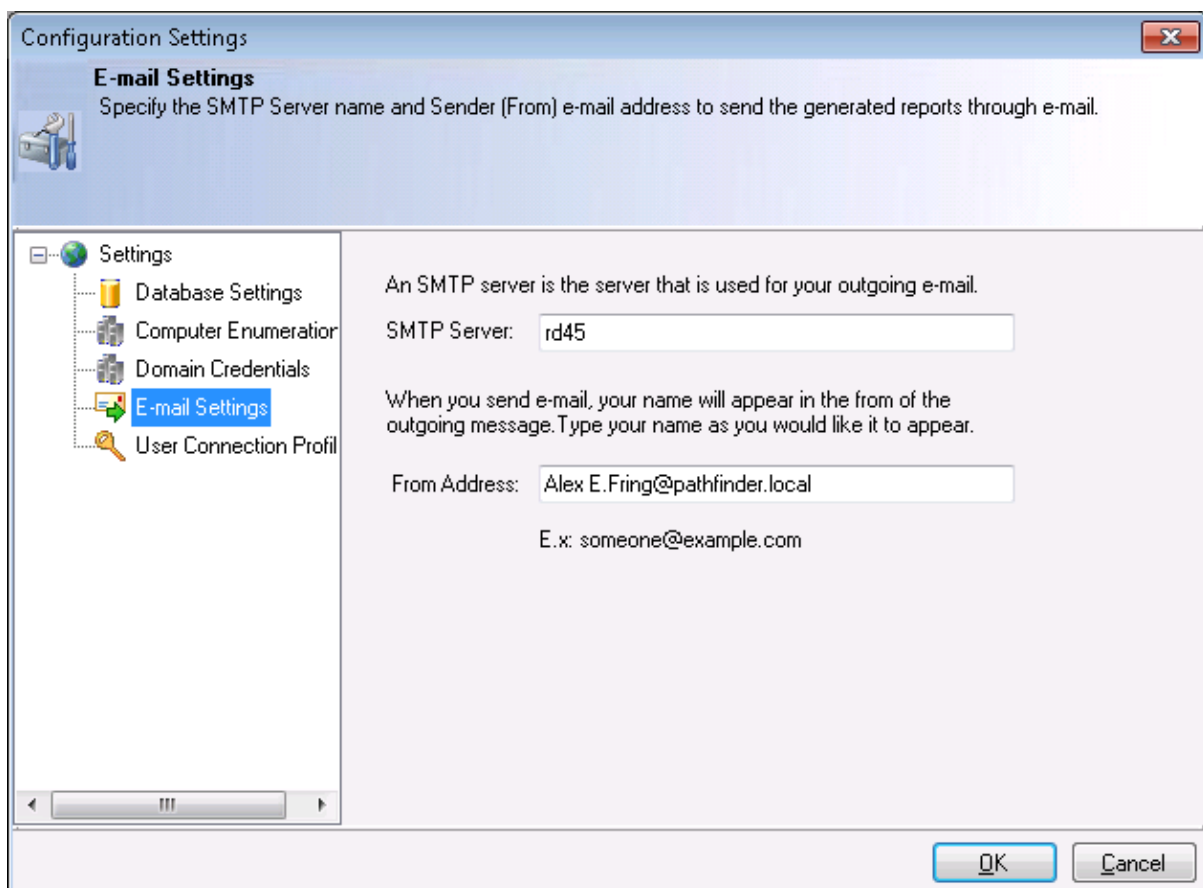
6) ARKWE will add the selected domains to the Domain Credentials list.



### 2.1.8 Configure SMTP Server

ARKWE provides the option to e-mail the reports generated. For e-mailing reports, ARKWE requires SMTP Server, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the e-mail report format. ARKWE maintains a single SMTP Server and a From E-mail Address for use by all reports. You can specify a separate set of "To" e-mail addresses (recipients), e-mail report format, subject and body of the message for each report.

You can set SMTP Server and From Address by clicking Tools -> Configuration Settings menu in the ARKWE main application window, as shown below:



### 2.1.9 User Connection Profiles

---

ARKWE creates a user profile in **Windows Stored User Names and Passwords applet / Credential Manager**, in order to store the domain user context for enumerating servers using ADSI.

The stored user profile will be useful for generating reports using ARKWE under the following scenarios:

- Using an alternate user account to connect to the domain to retrieve servers using ADSI.
- Providing credentials that have sufficient rights to enumerate shares present in computers within a domain.

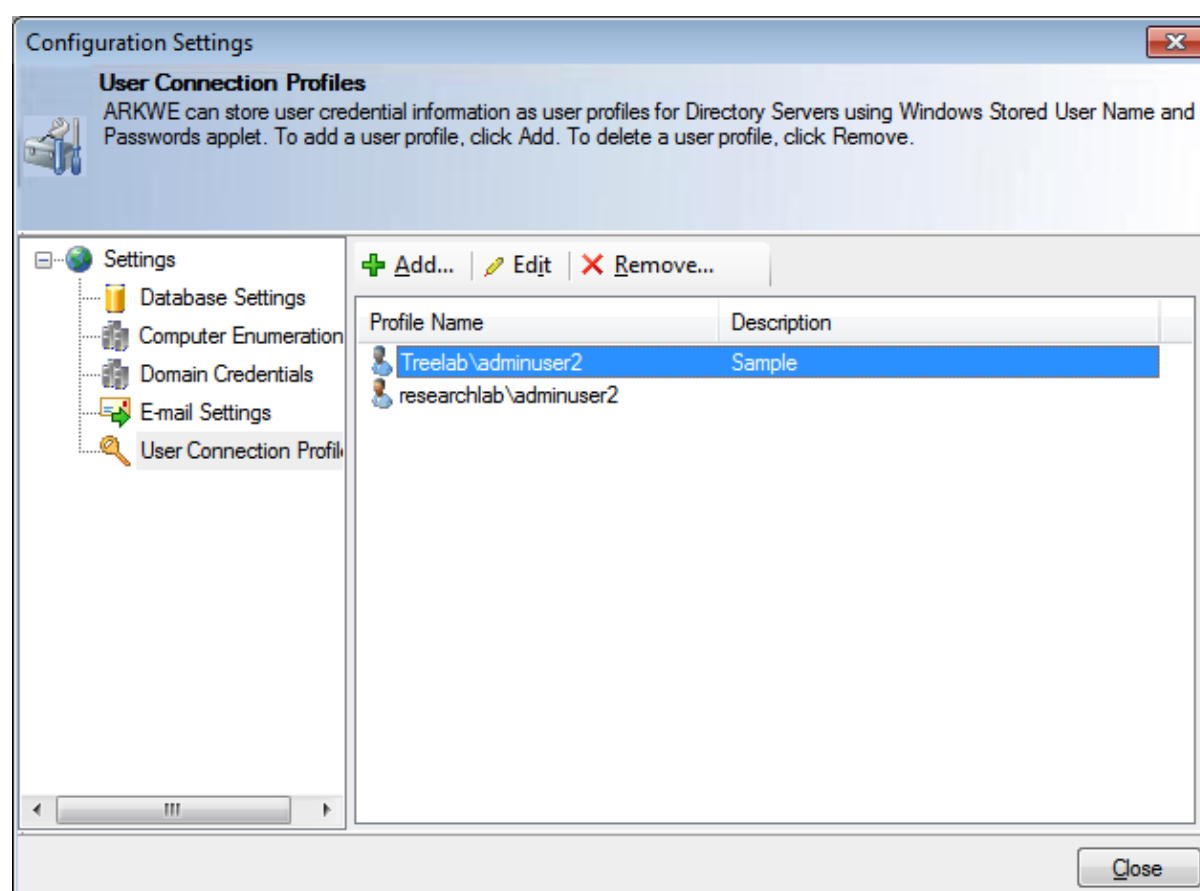
The stored user profile persists for all subsequent logon sessions on the same computer where ARKWE is installed. The stored user profiles are visible to the application under other logon sessions on the same computer.

The stored user profile created by ARKWE is restricted to the Windows User Profile context. If the Windows User Profile is maintained locally, ARKWE stored user profile is accessible only by the same user in the same computer. If the user who creates ARKWE stored user profile, has a Roaming user account in the enterprise, the ARKWE stored user profile can be accessed by the same user in any computer in the Windows enterprise.

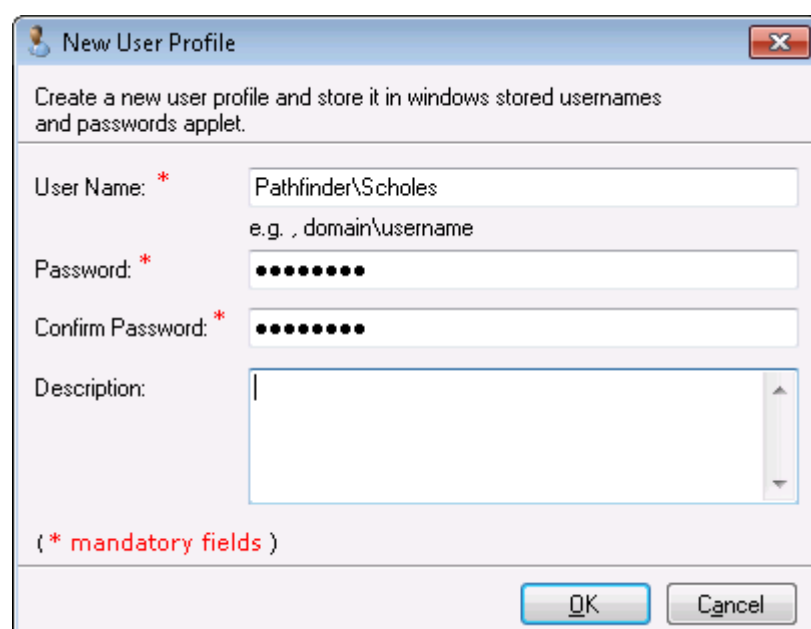
The stored user profile is a generic credential of **Windows Stored User Names and Passwords applet / Credential Manager** and can be used by the application only. The credential information is stored securely in a *256 bit encrypted format* in **Windows Stored User Names and Passwords applet / Credential Manager**.

The stored user profile corresponding to the user account will be used by the application in order to connect to the domain, if 'Use ADSI' is selected in ARKWE Enumeration Settings.

Using the Connection Profile dialog shown below, new profile can be created and available profiles can be removed from the profiles list.



Click **Add** button to add a new profile and a dialog will appear as shown below:



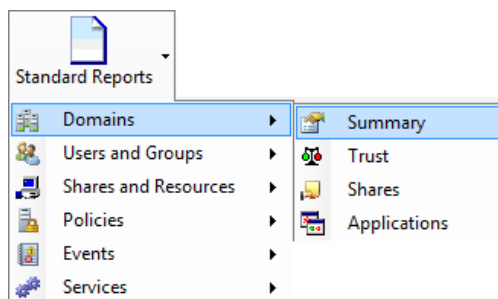
Click **Edit** button in the Connection Profile dialog to *edit* available profiles.


Click **Remove** button in the Connection Profile dialog to *remove* available profiles.

## 3 Standard Reports

### 3.1 How to View Domain Information?

#### Domain Summary Information

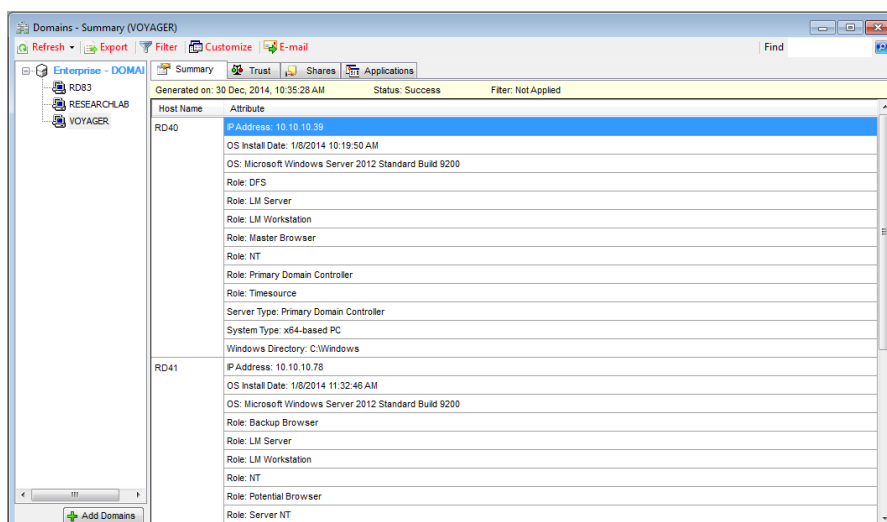


Click  to view domain summary information for a domain.

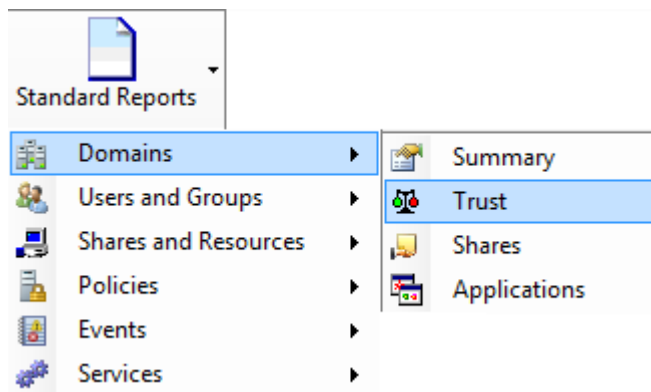
The summary report lists information like computer's operating system, browsing capability, participation in LanMan networks, membership in Windows workgroups etc., for the server(s) in the domain.

NOTE: For information on restricting the domain scan for generating this report, please see '[How to scan specific servers in a domain?](#)'

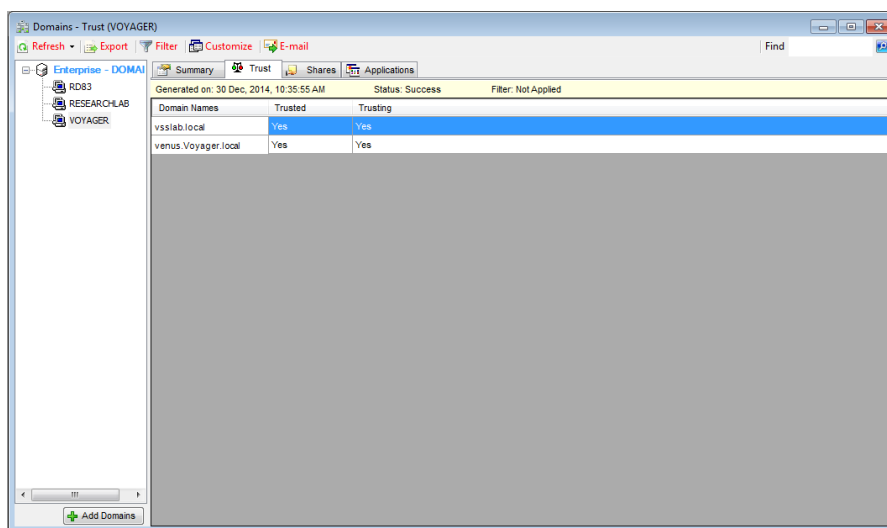
The output would be displayed as shown below:



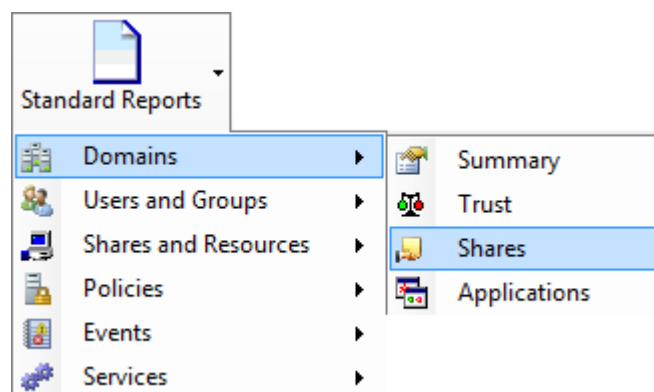
### Domain Trust Information



Click to view the trusted and trusting domains for a given domain.



### Domain Shares Information

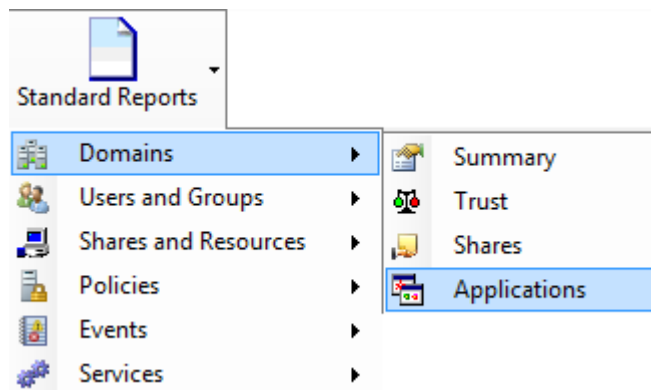


Click to view the shares for a given domain.

## CHAPTER 2 – Standard Reports

Host Name	IP Address	Share Name	Path	User Name	Security	Maximum Uses	Comment
RD40	10.10.10.39	ADMIN\$	C:\Windows		Admin Share	Unlimited	Remote Admin
		CS	C:\		Admin Share	Unlimited	Default share
		DS	D:\		Admin Share	Unlimited	Default share
		Folder	D:\Folder	Everyone	Allow - Full Control	Unlimited	
		latest setup	D:\latest setup	Everyone	Allow - Full Control	Unlimited	Latest Setup Share
		Module	D:\Module	BUILTIN\Administ...	Allow - Full Control	Unlimited	Latest Setup Share
		NETLOGON	C:\Windows\SY...	Everyone	Allow - Read	Unlimited	Logon server share
		NTFS Share	C:\Windows\SY...	BUILTIN\Administ...	Allow - Full Control	Unlimited	Logon server share
		NTFS Test Folder	C:\NTFS Test Fol...	Everyone	Allow - Read	Unlimited	
		Share	D:\Share	Everyone	Allow - Full Control	Unlimited	
		share22	D:\share22	BUILTIN\Administ...	Allow - Full Control	Unlimited	
		SPListX Target	D:\SPListX Target	Everyone	Allow - Full Control	Unlimited	
		SYSVOL	C:\Windows\SY...	Everyone	Allow - Read	Unlimited	Logon server share
			C:\Windows\SY...	NT AUTHORITY\...	Allow - Full Control	Unlimited	Logon server share

### Domain Application Information

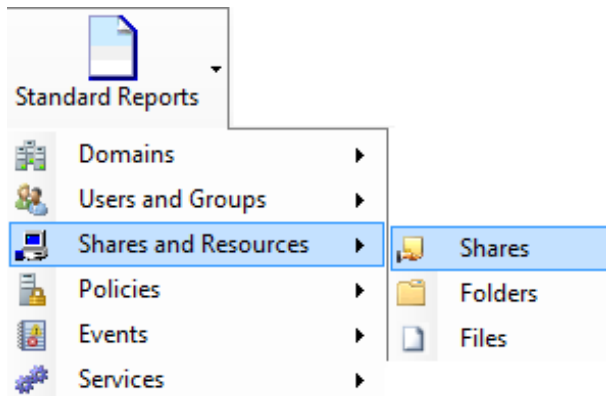


Click to view the applications installed for a given domain.

**NOTE:** For information on restricting the domain scan for generating this report, please see [How to scan specific servers in a domain?](#)

Host Name	IP Address	Application Name	Version	Path	Installed Date	Publisher	Readme Size (KB)
RD43	10.10.10.31	Active Directory	1.0.621.117		3/8/2014	Microsoft Corporation	9196
	10.10.10.31	Admin Report Kit	8.5	C:\Program Files...	6/4/2014	Vyapin Software Systems Private Limited	22514
	10.10.10.31	AppFabric 1.1 fo...	1.1.2106.32	C:\Program Files...	3/6/2014	Microsoft Corporation	
	10.10.10.31	AppFabric 1.1 fo...	1.1.2106.32	C:\Program Files...	3/6/2014	Microsoft Corporation	39902
	10.10.10.31	DockIT for Share...	8.1.0	C:\Program Files...	6/25/2014	Vyapin Software Systems Private Limited	23960
	10.10.10.31	Microsoft Acces...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	6078
	10.10.10.31	Microsoft Acces...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	170040
	10.10.10.31	Microsoft CCR a...	2.2.780	C:\Program Files...	3/6/2014	Microsoft Corporation	2470
	10.10.10.31	Microsoft Docum...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	171313
	10.10.10.31	Microsoft Docum...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	7845
	10.10.10.31	Microsoft Educat...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	166974
	10.10.10.31	Microsoft Educat...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	831
	10.10.10.31	Microsoft Excel...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	160530
	10.10.10.31	Microsoft Excel...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	546944
	10.10.10.31	Microsoft Excel...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	7357
	10.10.10.31	Microsoft Excha...	15.0.516.14	C:\Program Files...	6/23/2014	Microsoft Corporation	4245
	10.10.10.31	Microsoft Identity...	2.0.1459.0	C:\Program Files...	3/6/2014	Microsoft Corporation	118
	10.10.10.31	Microsoft InfoPat...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	1478
	10.10.10.31	Microsoft InfoPat...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	171744
	10.10.10.31	Microsoft Office...	15.0.4420.1017	C:\Program Files...	3/7/2014	Microsoft Corporation	9174

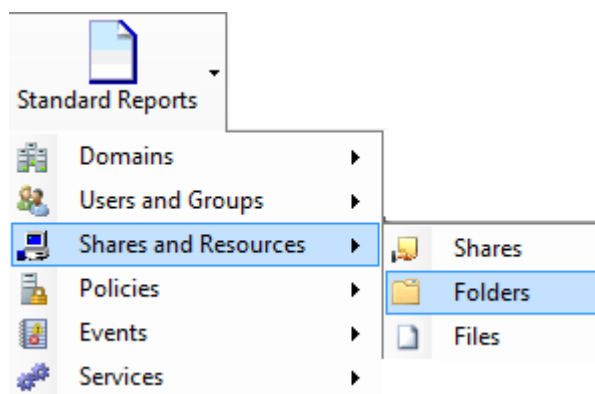
### 3.2 How to View Shares and Resources Information?



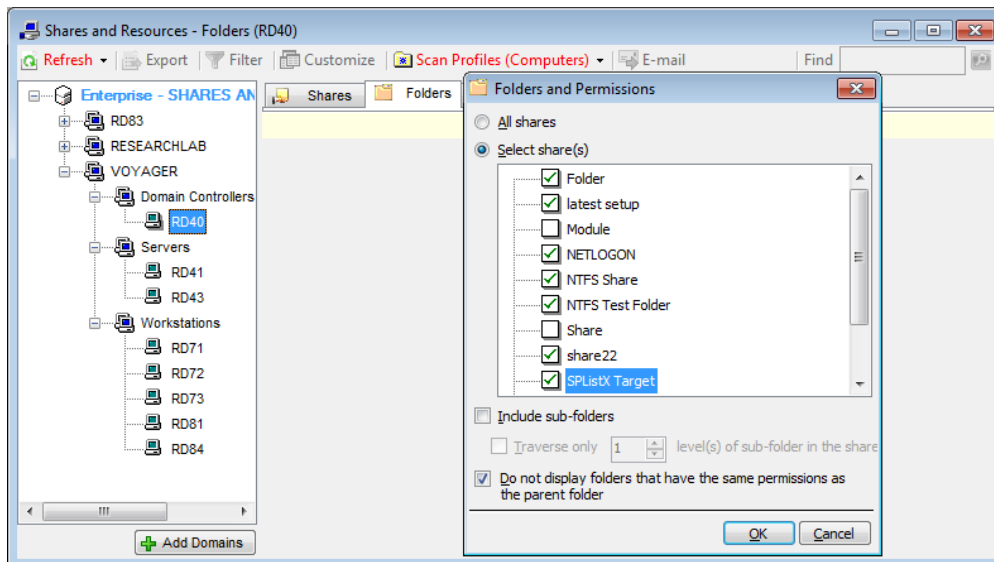
Click **Shares** to view the following information:  
**Share Name, Path, User Name, Security, Maximum, and Comment**

Share Name	Path	User Name	Security	Maximum Uses	Comment
ADMIN\$	C:\Windows		Admin Share	Unlimited	Remote Admin
C\$	C:\		Admin Share	Unlimited	Default share
D\$	D:\		Admin Share	Unlimited	Default share
Folder	D:\Folder	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		Everyone	Allow - Full Control	Unlimited	
latest setup	D:\latest setup	BUILTIN\Administrators	Allow - Full Control	Unlimited	Latest Setup Share
		Everyone	Allow - Full Control	Unlimited	Latest Setup Share
Module	D:\Module	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		Everyone	Allow - Full Control	Unlimited	
NETLOGON	C:\Windows\SYSVOL\sysvol\Voyager.local\SCRIPTS	Everyone	Allow - Read	Unlimited	Logon server share
		BUILTIN\Administrators	Allow - Full Control	Unlimited	Logon server share
NTFS Share	C:\NTFS Test Folder\NTFS Share	VOYAGER\adminuser3	Allow - Full Control	Unlimited	
NTFS Test Folder	C:\NTFS Test Folder	Everyone	Allow - Read	Unlimited	
Share	D:\Share	Everyone	Allow - Full Control	Unlimited	
		BUILTIN\Administrators	Allow - Full Control	Unlimited	
share22	D:\share22	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		Everyone	Allow - Full Control	Unlimited	
SPLISTX Target	D:\SPLISTX Target	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		Everyone	Allow - Full Control	Unlimited	

#### How to View Permissions of Folders in a Share?



Click **Folders** tab. The **"Folders and Permissions"** dialog appears.



You can view permissions of folder(s) in a share or for all the shares in the selected server by selecting "All shares" option or "Select share(s)" option respectively.

You can also optionally include the sub-folder(s) information by selecting the "Include sub-folders" option.

The sub-folder(s) having permissions identical as the parent folder would be shown in bold text with "Same as parent" in both User Name and Security fields in the report. If you do not want folders with identical permissions as the parent folder reported, then select, the "Do not display folders that have same permissions as the parent folder" option. This option will not report folders with identical permissions as the parent folder.

To view up to a certain level of sub-folders, select the "Traverse only 'n' level(s) of sub-folder in the share" option and specify a sub-folder level, where the levels are numbered as follows:

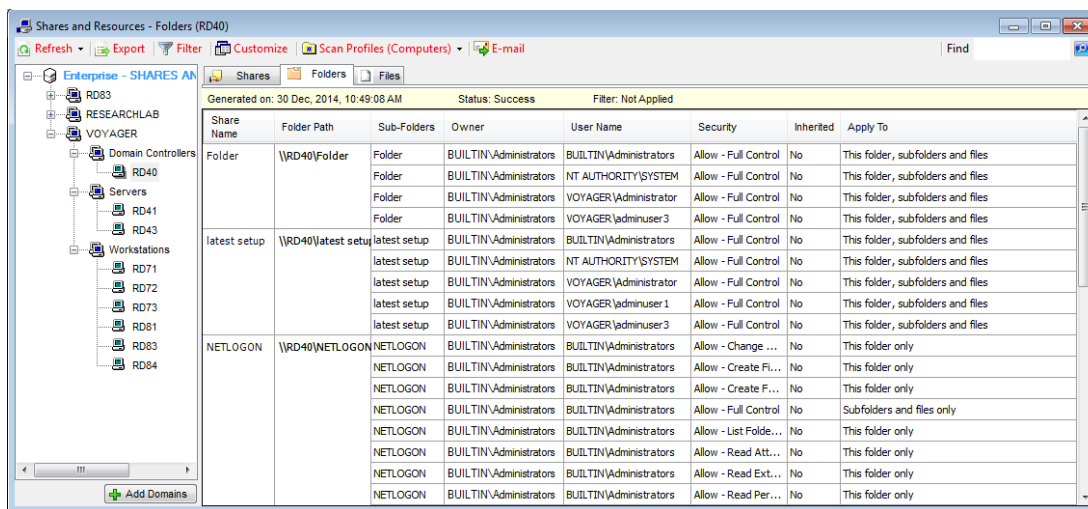
\\server\sharename\Level 1\Level 2\Level 3...

**NOTE:** The "Include sub-folders" option defaults to enumerating all the sub-folders unless you specify a sub-folder level in "Traverse only 'n' level(s) of sub-folder in the share" option.

**NOTE:** The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

## CHAPTER 2 – Standard Reports

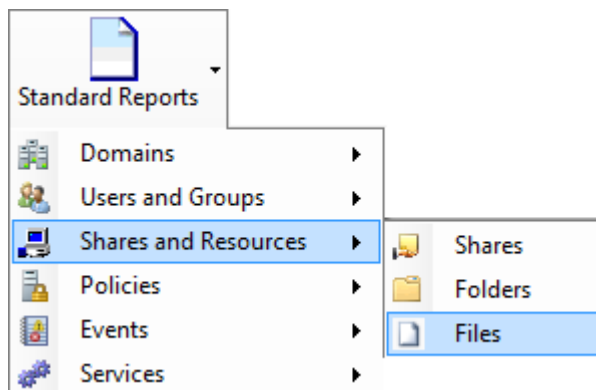
The report would be displayed as shown below:



Generated on: 30 Dec, 2014, 10:49:08 AM Status: Success Filter: Not Applied

Share Name	Folder Path	Sub-Folders	Owner	User Name	Security	Inherited	Apply To
Folder	\\RD40\Folder	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	This folder, subfolders and files
		Folder	BUILTIN\Administrators	NT AUTHORITY\SYSTEM	Allow - Full Control	No	This folder, subfolders and files
		Folder	BUILTIN\Administrators	VOYAGER\Administrator	Allow - Full Control	No	This folder, subfolders and files
		Folder	BUILTIN\Administrators	VOYAGER\adminduser3	Allow - Full Control	No	This folder, subfolders and files
latest setup	\\RD40\latest setup	latest setup	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	This folder, subfolders and files
		latest setup	BUILTIN\Administrators	NT AUTHORITY\SYSTEM	Allow - Full Control	No	This folder, subfolders and files
		latest setup	BUILTIN\Administrators	VOYAGER\Administrator	Allow - Full Control	No	This folder, subfolders and files
		latest setup	BUILTIN\Administrators	VOYAGER\adminduser1	Allow - Full Control	No	This folder, subfolders and files
NETLOGON	\\RD40\NETLOGON	latest setup	BUILTIN\Administrators	VOYAGER\adminduser3	Allow - Full Control	No	This folder, subfolders and files
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Change ...	No	This folder only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Create Fi...	No	This folder only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Create F...	No	This folder only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	Subfolders and files only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - List Folde...	No	This folder only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Att...	No	This folder only
		NETLOGON	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Ext...	No	This folder only

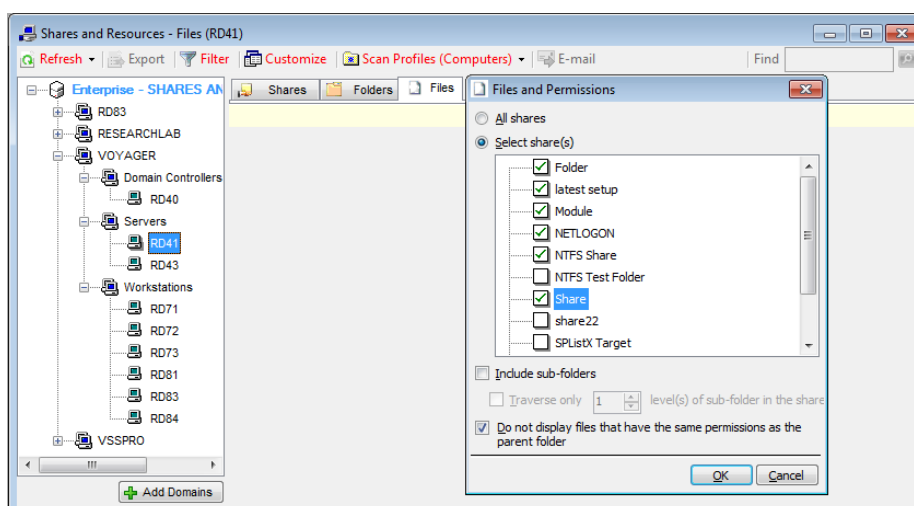
### How to view permissions of files in a share?



Click

tab. The **"Files and Permissions"**

dialog appears.



You can view permissions of files in a share or for all the shares in the selected server by selecting "All shares" option or "Select share(s)" option respectively.

## CHAPTER 2 – Standard Reports

You can also optionally include the sub-folder(s) information by selecting the "Include sub-folders" option.

The files having permissions identical to the parent folder would show up with "Same as parent" in both User Name and Security fields in the report. If you do not want files with identical permissions as the parent folder reported, then select, the "Do not display files that have same permissions as the parent folder" option. This option will not report files with identical permissions as the parent folder.

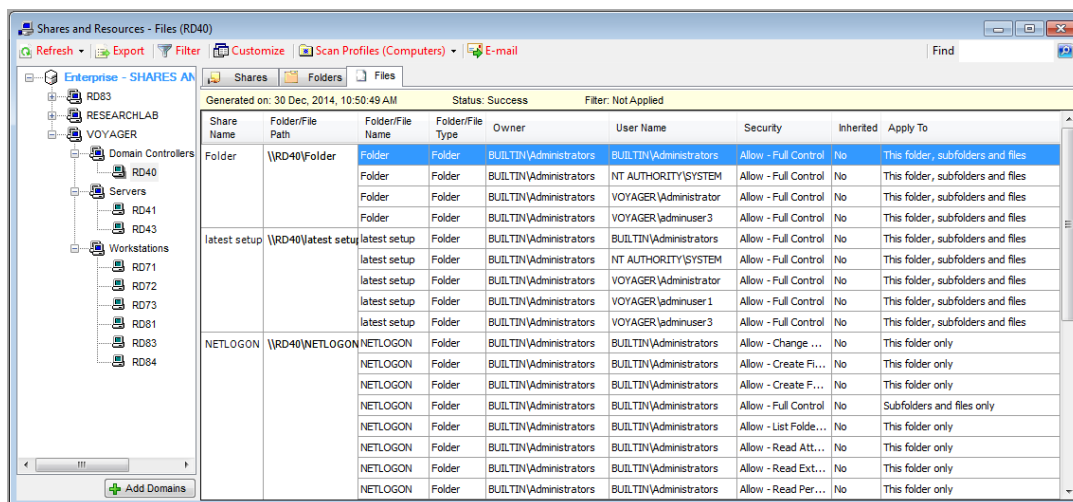
To view up to a certain level of sub-folders and files, select the "Traverse only 'n' level(s) of sub-folder in the share" option and specify a sub-folder level, where the levels are numbered as follows:

\\server\sharename\Level 1\Level 2\Level 3...

**NOTE:** The "Include sub-folders" option defaults to enumerating all the sub-folders unless you specify a sub-folder level in "Traverse only 'n' level(s) of sub-folder in the share" option.

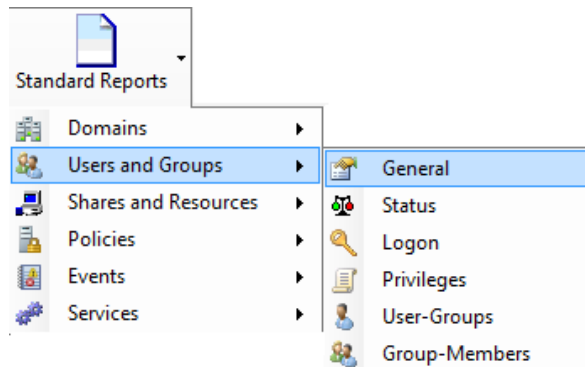
**NOTE:** The "Do not display files that have same permissions as the parent folder" option would be enabled by default.

The report would be displayed as shown below:



Share Name	Folder/File Path	Folder/File Name	Folder/File Type	Owner	User Name	Security	Inherited	Apply To
Folder	\\RD40\Folder	Folder	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	This folder, subfolders and files
		Folder	Folder	BUILTIN\Administrators	NT AUTHORITY\SYSTEM	Allow - Full Control	No	This folder, subfolders and files
		Folder	Folder	BUILTIN\Administrators	VOYAGER\Administrator	Allow - Full Control	No	This folder, subfolders and files
		Folder	Folder	BUILTIN\Administrators	VOYAGER\adminuser3	Allow - Full Control	No	This folder, subfolders and files
	latest setup	latest setup	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	This folder, subfolders and files
		latest setup	Folder	BUILTIN\Administrators	NT AUTHORITY\SYSTEM	Allow - Full Control	No	This folder, subfolders and files
		latest setup	Folder	BUILTIN\Administrators	VOYAGER\Administrator	Allow - Full Control	No	This folder, subfolders and files
		latest setup	Folder	BUILTIN\Administrators	VOYAGER\adminuser1	Allow - Full Control	No	This folder, subfolders and files
		latest setup	Folder	BUILTIN\Administrators	VOYAGER\adminuser3	Allow - Full Control	No	This folder, subfolders and files
		latest setup	Folder	BUILTIN\Administrators	VOYAGER\adminuser3	Allow - Full Control	No	This folder, subfolders and files
NETLOGON	\\RD40\NETLOGON	NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Change ...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Create F...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Create F...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	Subfolders and files only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - List Folde...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Att...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Ext...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Per...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Per...	No	This folder only
		NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Per...	No	This folder only

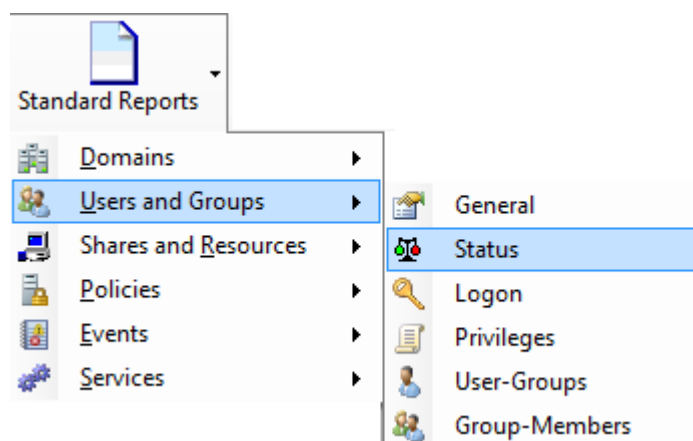
### 3.3 How to View Users and Groups Information?



Click on **General** to view the following information:  
**User Name, Full Name, Description, Home Path, Logon Script, and User Profile Path.**

The screenshot shows a window titled 'Users and Groups - General (RD40)'. It contains a table with the following columns: User Name, Full Name, Description, Home Path, Logon Script, and User Profile Path. The table lists various system and user accounts.

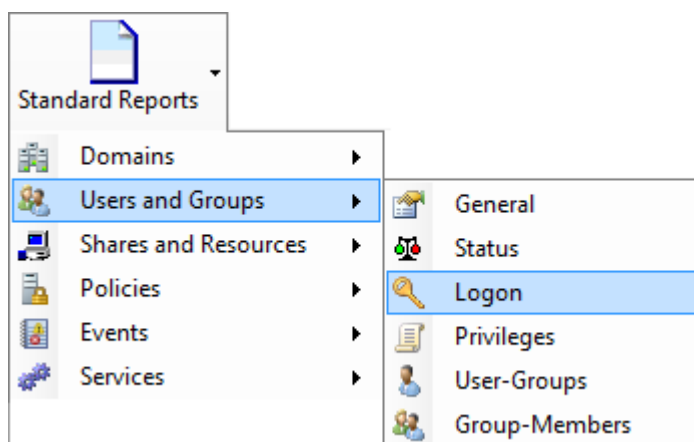
User Name	Full Name	Description	Home Path	Logon Script	User Profile Path
Administrator		Built-in account for administering the computer/domain			
Guest		Built-in account for guest access to the computer/domain			
krbtgt		Key Distribution Center Service Account			
adminuser1	adminuser1				
adfsrvacc	adfsrvacc				
adminuser2	adminuser2				
adminuser3	adminuser3				
configdbadmin_sp03	configdbadmin_sp03				
defconaccessacc_sp03	defconaccessacc_sp03				
portsiteappool_sp03	portsiteappool_sp03				
spappool1_sp03	spappool1_sp03				
spappool2_sp03	spappool2_sp03				
spappool3_sp03	spappool3_sp03				
spsitecoladm1_sp03	spsitecoladm1_sp03				
spsitecoladm2_sp03	spsitecoladm2_sp03				
farmadmin_sp07-1	farmadmin_sp07-1				
farmadmin_sp07-2	farmadmin_sp07-2				
searchdefacc_sp07-1	searchdefacc_sp07-1				
searchdefacc_sp07-2	searchdefacc_sp07-2				



Click on **Status** to view the following information:  
**User Name, Full Name, Description, Account Expiry, Password Editable, Password Age, Account Locked, and Account Disabled.**

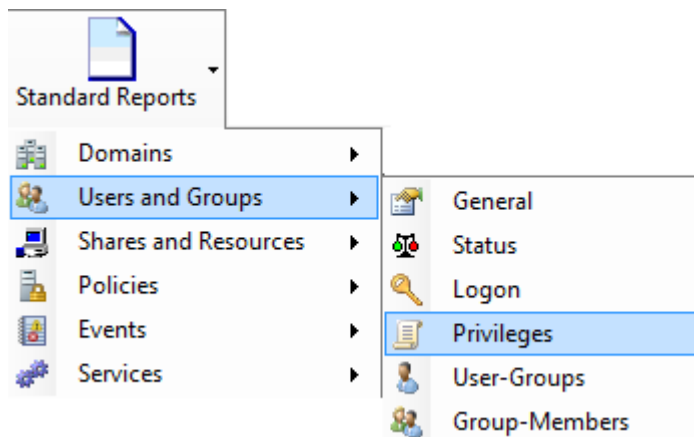
## CHAPTER 2 – Standard Reports

User Name	Full Name	Description	Account Expiry	Password Editable	Password Age	Account Locked	Account Disabled
Administrator		Built-in account for adm...	Never expires	Yes	96 Day(s), 15 Hr(s), 15 Min...	No	No
Guest		Built-in account for guest...	Never expires	No		No	Yes
krbtgt		Key Distribution Center S...	Never expires	Yes	356 Day(s), 3 Hr(s), 53 Min...	No	Yes
adminuser1	adminuser1		Never expires	Yes	355 Day(s), 7 Hr(s), 40 Min...	No	No
adfssvcacc	adfssvcacc		Never expires	No	355 Day(s), 6 Hr(s), 38 Min...	No	No
adminuser2	adminuser2		Never expires	Yes	355 Day(s), 6 Hr(s), 31 Min...	No	No
adminuser3	adminuser3		Never expires	Yes	355 Day(s), 6 Hr(s), 30 Min...	No	No
configdbadmin_sp03	configdbadmin...		Never expires	No	355 Day(s), 6 Hr(s), 29 Min...	No	No
defconaccessacc_sp03	defconaccess...		Never expires	No	355 Day(s), 6 Hr(s), 28 Min...	No	No
portsiteappool_sp03	portsiteapp...		Never expires	No	355 Day(s), 6 Hr(s), 27 Min...	No	No
spappool1_sp03	spappool1...		Never expires	No	355 Day(s), 6 Hr(s), 26 Min...	No	No
spappool2_sp03	spappool2...		Never expires	No	355 Day(s), 6 Hr(s), 26 Min...	No	No
spappool3_sp03	spappool3...		Never expires	No	355 Day(s), 6 Hr(s), 25 Min...	No	No
spsitecoladm1_sp03	spsitecoladm...		Never expires	No	355 Day(s), 6 Hr(s), 24 Min...	No	No
spsitecoladm2_sp03	spsitecoladm...		Never expires	No	355 Day(s), 6 Hr(s), 24 Min...	No	No
farmadmin_sp07-1	farmadmin_s...		Never expires	No	355 Day(s), 6 Hr(s), 22 Min...	No	No
farmadmin_sp07-2	farmadmin_s...		Never expires	No	355 Day(s), 6 Hr(s), 22 Min...	No	No
searchdefacc_sp07-1	searchdefacc...		Never expires	No	355 Day(s), 6 Hr(s), 21 Min...	No	No

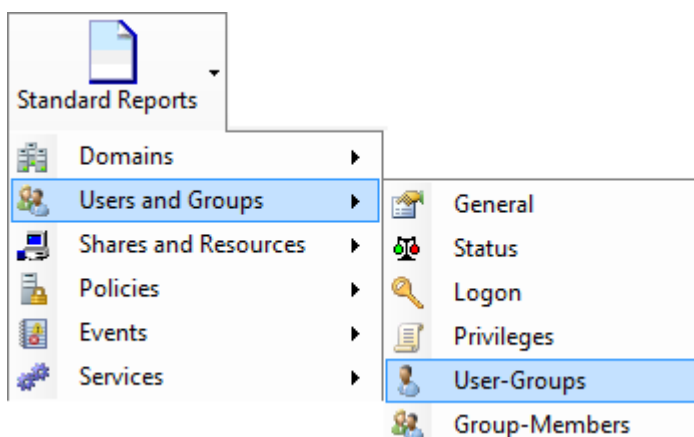
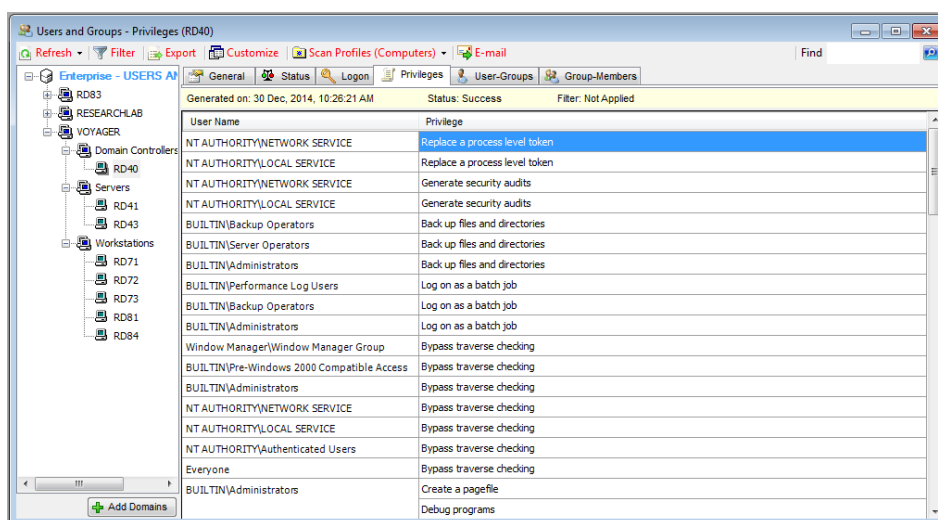


Click on **Users and Groups** to view the following information: **User Name, Logon Machines, Last Logon.**

User Name	Logon Machines	Last Logon
Administrator	Any Workstation	12/29/2014 7:44:59 PM
Guest	Any Workstation	
krbtgt	Any Workstation	
adminuser1	Any Workstation	12/29/2014 7:49:42 PM
adfssvcacc	Any Workstation	
adminuser2	Any Workstation	12/30/2014 10:09:43 AM
adminuser3	Any Workstation	12/30/2014 10:13:58 AM
configdbadmin_sp03	Any Workstation	
defconaccessacc_sp03	Any Workstation	
portsiteappool_sp03	Any Workstation	
spappool1_sp03	Any Workstation	
spappool2_sp03	Any Workstation	
spappool3_sp03	Any Workstation	
spsitecoladm1_sp03	Any Workstation	
spsitecoladm2_sp03	Any Workstation	
farmadmin_sp07-1	Any Workstation	2/25/2014 2:13:05 PM
farmadmin_sp07-2	Any Workstation	
searchdefacc_sp07-1	Any Workstation	
searchdefacc_sp07-2	Any Workstation	

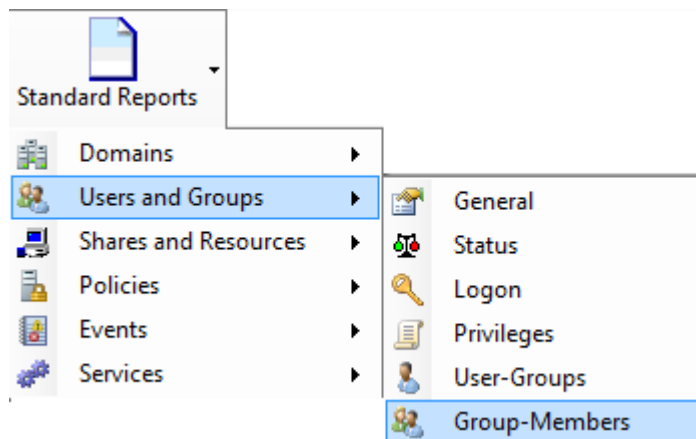
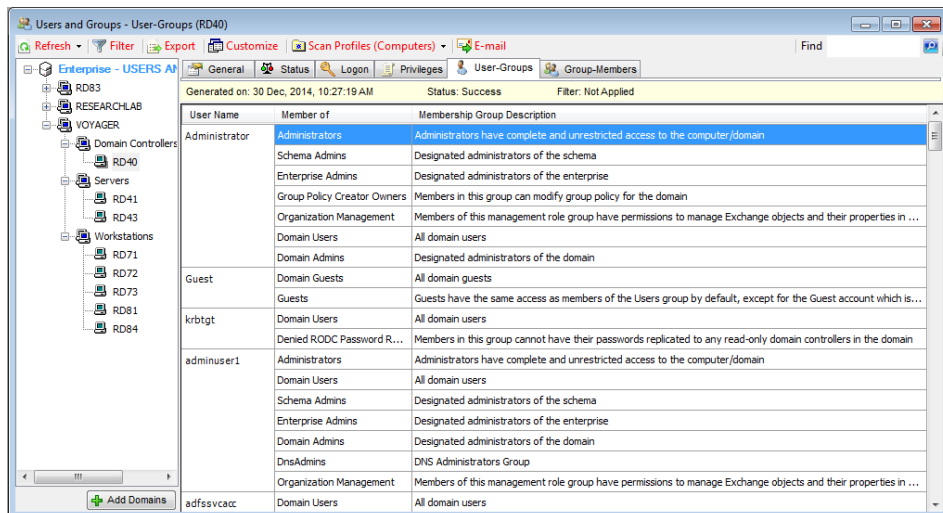


Click on **Privileges** to view the following information: ***Displays privilege lists on a per-user and per-privilege basis.***

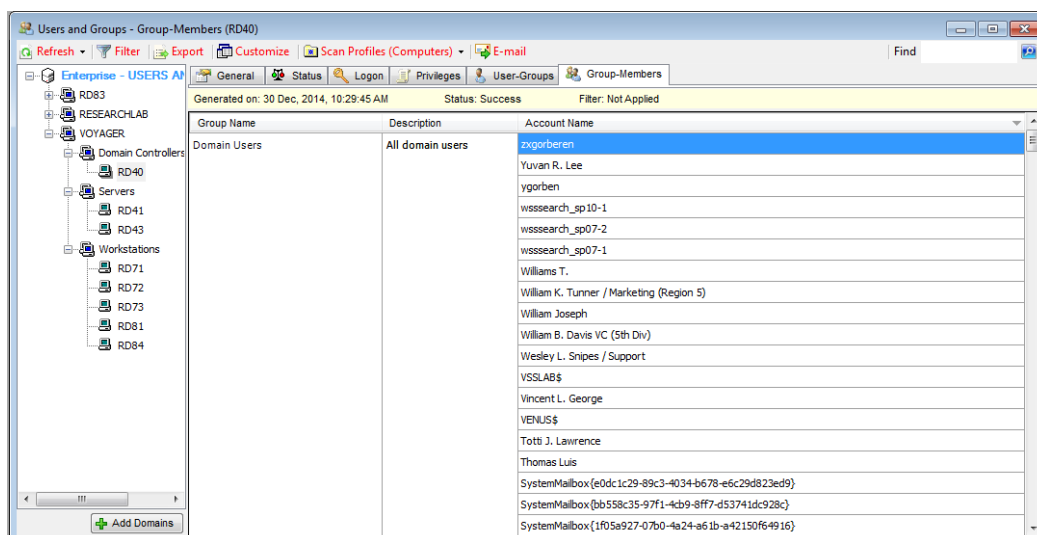


Click on **User-Groups** to view the following information: ***Displays group lists on a per-user and per-group basis.***

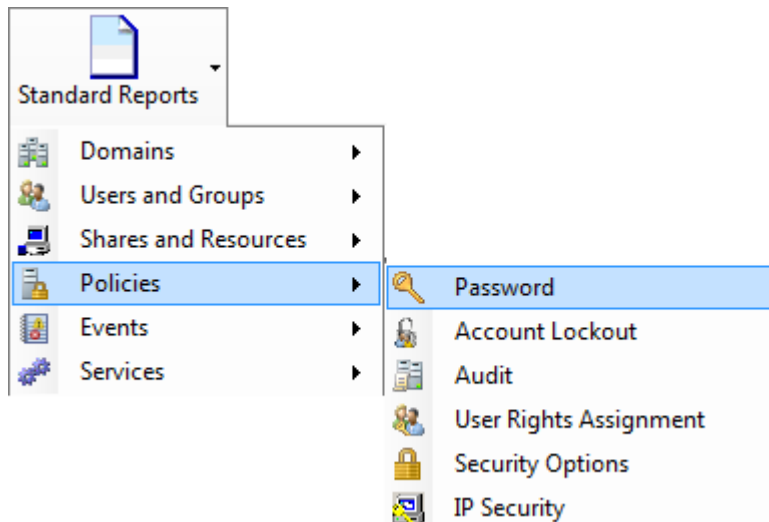
## CHAPTER 2 – Standard Reports



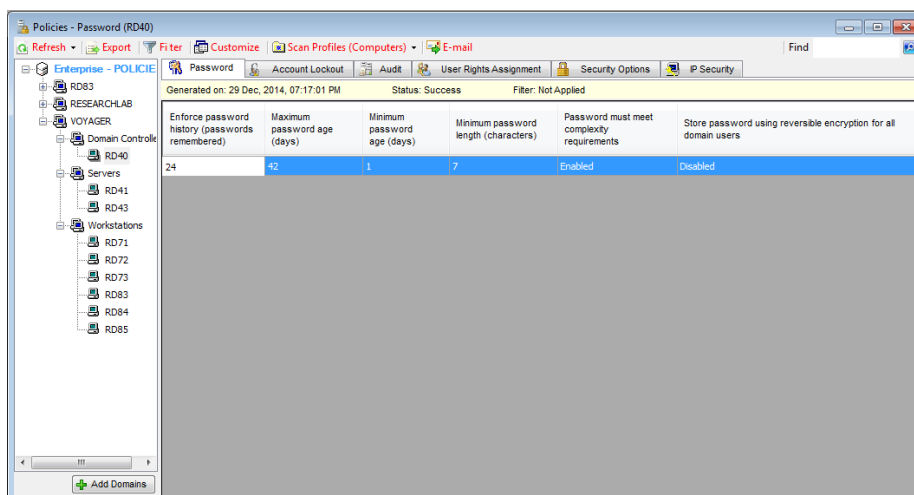
Click on **Group-Members** to view the following information: **Displays group member's lists on a per-group basis**

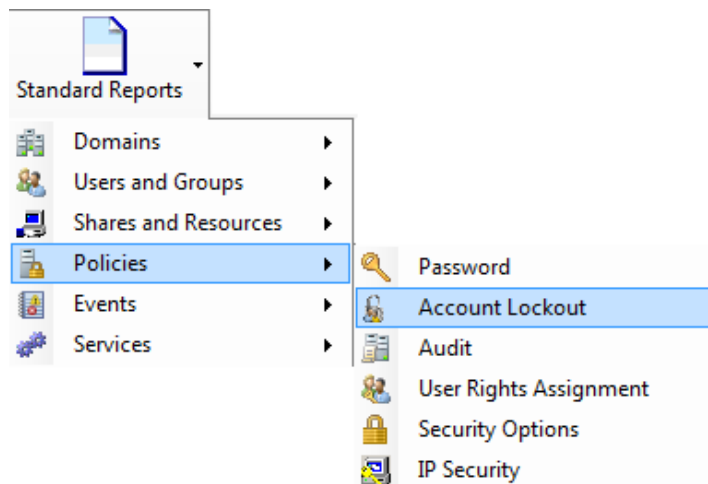


### 3.4 How to View Policies Information?

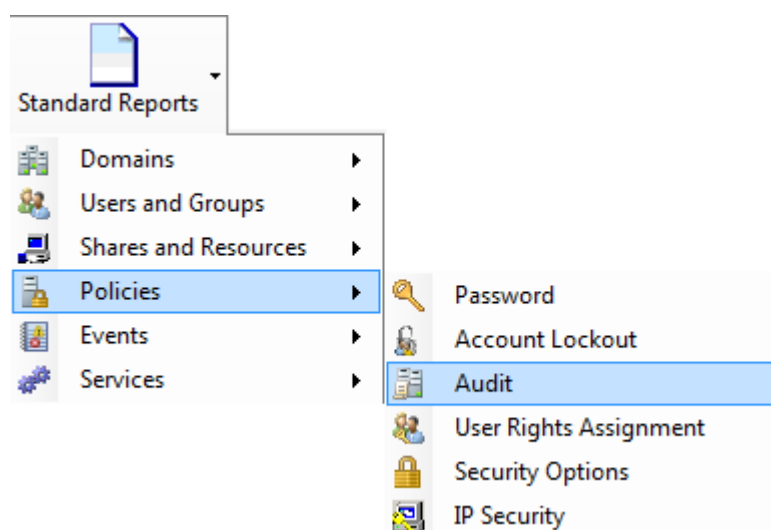
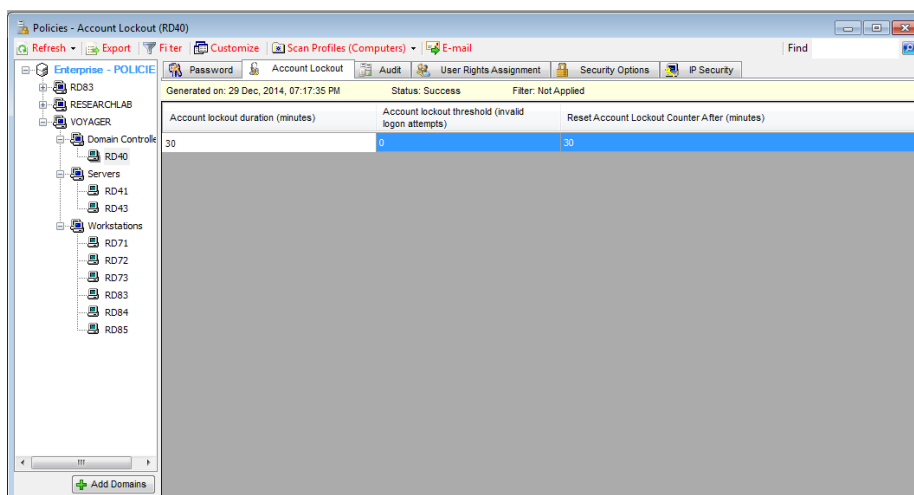


Click **Password** to view the following information: ***Enforce Password History, Maximum Password Age, Minimum Password Age, Minimum Password Length; Password must meet complexity requirements, Store password using reversible encryption for all domain users***



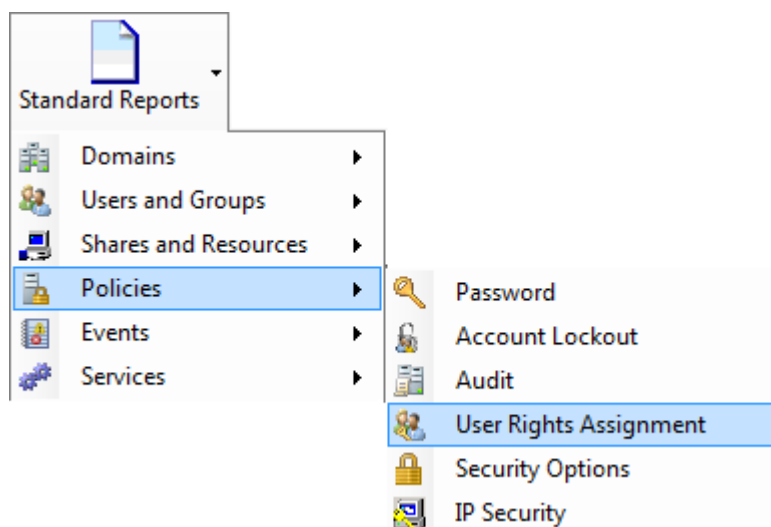
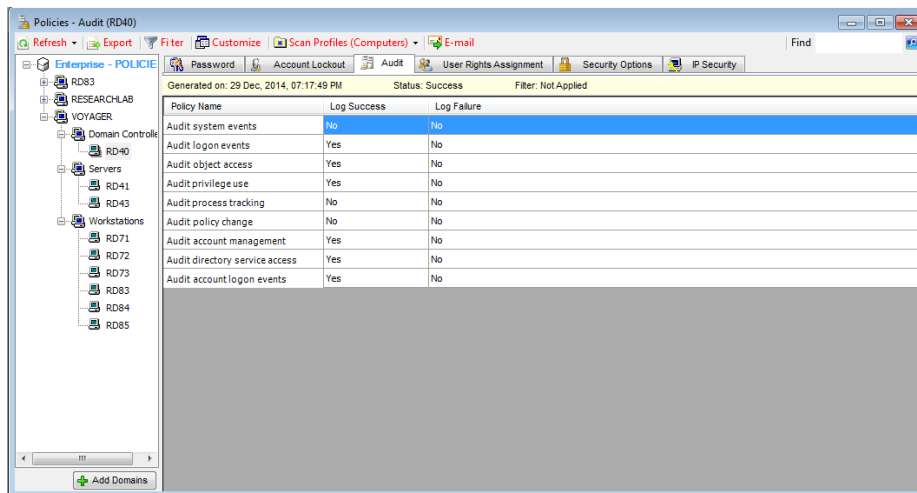


Click **Account Lockout** tab to view the following information: **Account Lockout Duration, Account Lockout Threshold, and Reset Account Lockout**

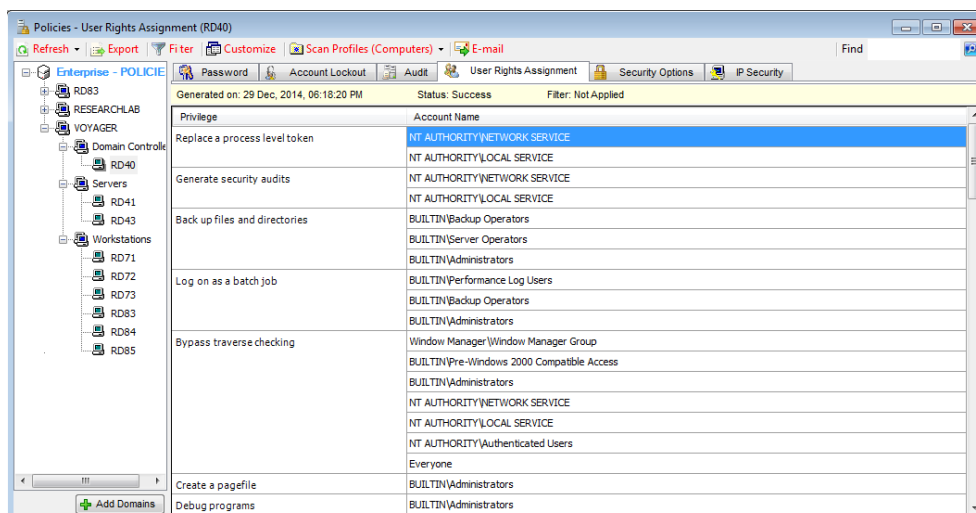


Click **Audit** to view the following information: **Policy Name, Log Success, and Log Failure**

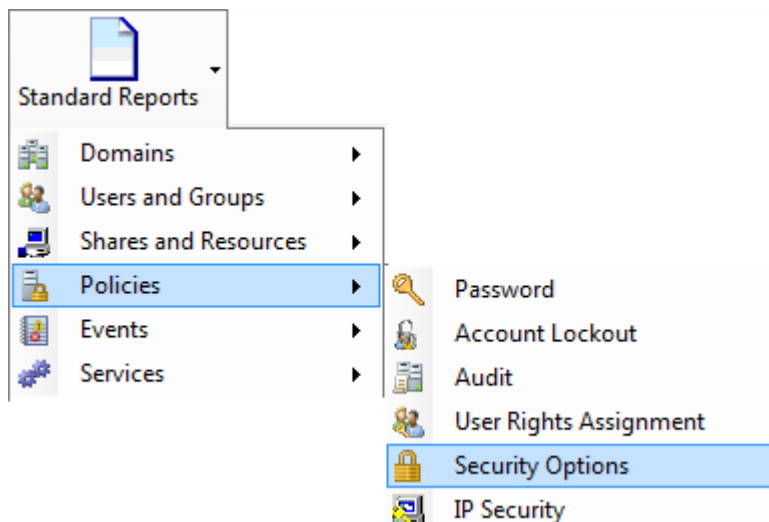
## CHAPTER 2 – Standard Reports



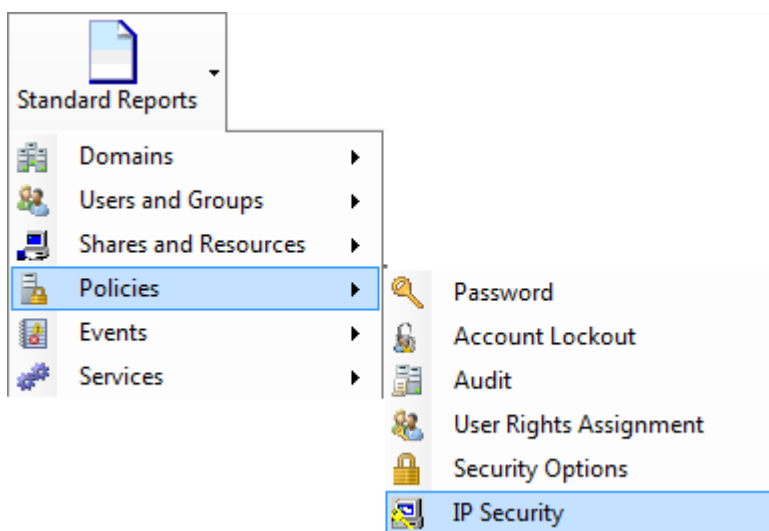
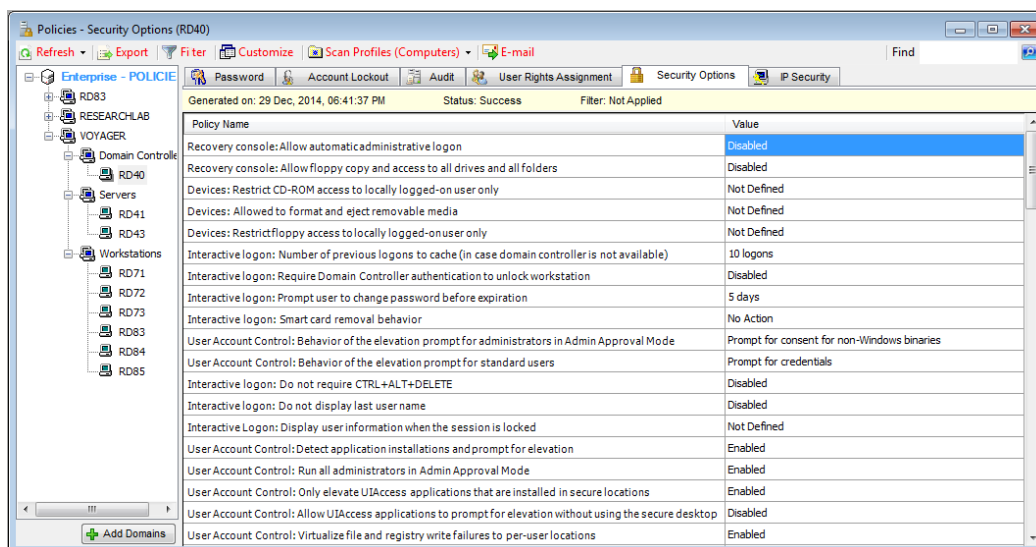
Click **User Rights Assignment** to view the following information: **Privilege, Account Name**



## CHAPTER 2 – Standard Reports



Click to view the following information: ***Policy Name, Value***



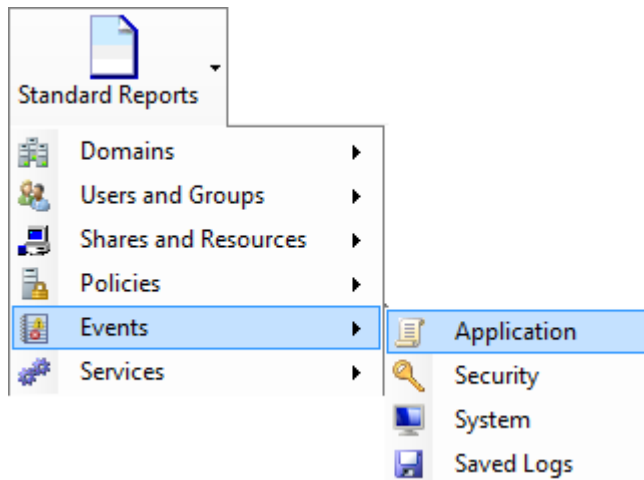
Click to view the following information: ***Policy Name, Description, Policy Assigned, and Last Modified***

## CHAPTER 2 – Standard Reports

The screenshot displays the Group Policy Management console for the 'Enterprise - POLICY' domain. The left pane shows a tree view with 'Domain Controllers' expanded, listing RD40, RD41, RD43, RD71, RD72, RD73, RD83, RD84, and RD85. The right pane shows the 'Security Options' report for RD40, generated on 29 Dec, 2014, 06:41:37 PM. The report status is 'Success' and the filter is 'Not Applied'. The report table lists three policies: 'Server (Request Security)', 'Client (Respond Only)', and 'Secure Server: (Require Security)'. All three policies are currently set to 'No' and were last modified on 8/2/2012 6:46:12 PM.

Policy Name	Description	Policy Assigned	Last Modified
Server (Request Security)	For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.	No	8/2/2012 6:46:12 PM
Client (Respond Only)	Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.	No	8/2/2012 6:46:12 PM
Secure Server: (Require Security)	For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients.	No	8/2/2012 6:46:12 PM

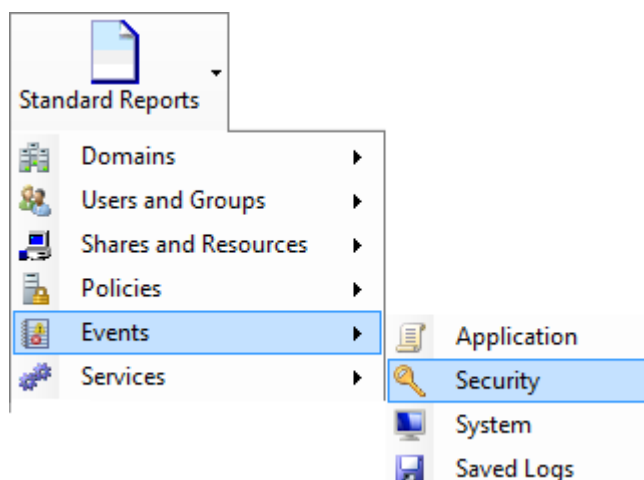
### 3.5 How to View Events Information?



Click to view the following information:  
**Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category**

Generated on: 29 Dec, 2014, 08:49:21 PM Status: Success Filter: Not Applied

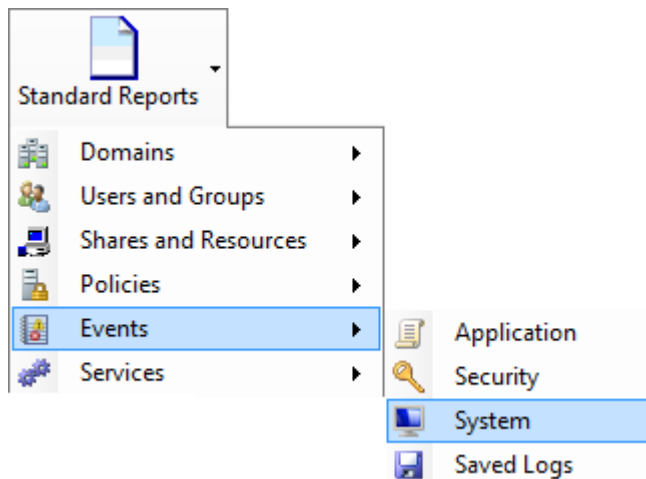
Event Date	Event Time	Description	Source	Event Id	Computer Name	User Name	Event Type	Category
12/24/2014	06:13:48 PM	The Desktop Window Manager has e...	Desktop Window...	9009	RD40.Voyager.I...	N/A	Information	None
	06:13:48 PM	Windows detected your registry file i...	Microsoft-Windo...	1530	RD40.Voyager.I...	N/A	Warning	None
	08:22:30 PM	The winlogon notification subscriber ...	Winlogon	6003	RD40.Voyager.I...	N/A	Information	None
	08:22:31 PM	The winlogon notification subscriber ...	Winlogon	6000	RD40.Voyager.I...	N/A	Information	None
	08:26:12 PM	The Desktop Window Manager has e...	Desktop Window...	9009	RD40.Voyager.I...	N/A	Information	None
	08:26:11 PM	Windows detected your registry file i...	Microsoft-Windo...	1530	RD40.Voyager.I...	N/A	Warning	None
	10:10:38 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:39 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General
	10:10:39 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:39 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General
	10:10:39 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:39 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	326	RD40.Voyager.I...	N/A	Information	General
	10:10:40 PM	svchost (2788) The database engine...	ESSENT	327	RD40.Voyager.I...	N/A	Information	General



Click to view the following information:  
**Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category**

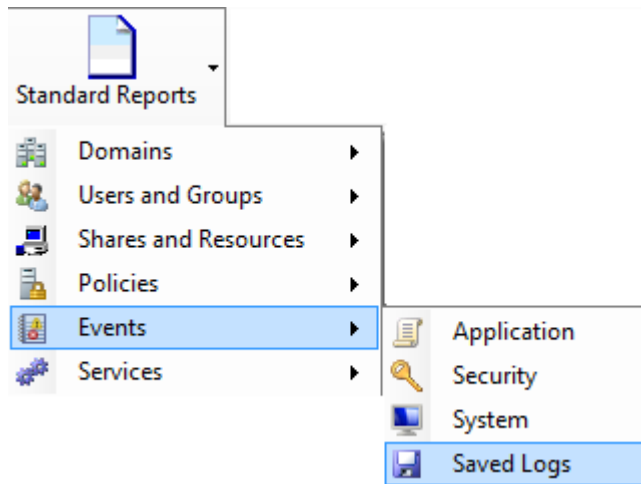
## CHAPTER 2 – Standard Reports

Event Date	Event Time	Description	Source	Event ID	Computer Name	User Name	Event Type	Category
12/29/2014	01:48:29 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	Special privileges assigned to new logon...	Microsoft-Windows-Secur...	4672	RD40.Voyager.local	N/A	SuccessAudit	(12548)
	01:48:36 PM	An account was successfully logged on...	Microsoft-Windows-Secur...	4624	RD40.Voyager.local	N/A	SuccessAudit	(12544)
	01:48:36 PM	User / Device claims information.Subject...	Microsoft-Windows-Secur...	4626	RD40.Voyager.local	N/A	SuccessAudit	(12553)
	01:48:36 PM	An account was logged off.Subject:Sec...	Microsoft-Windows-Secur...	4634	RD40.Voyager.local	N/A	SuccessAudit	(12545)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:36 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:37 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:37 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:38 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:38 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:38 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
	01:48:38 PM	The Windows Filtering Platform has per...	Microsoft-Windows-Secur...	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)



Click to view the following information:  
**Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category**

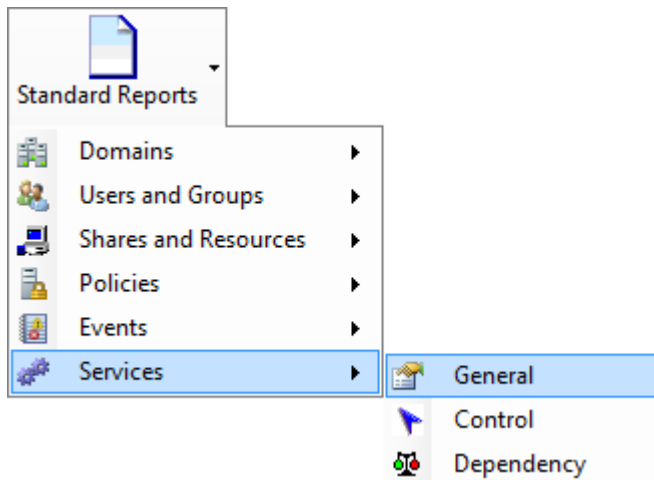
Event Date	Event Time	Description	Source	Event ID	Computer Name	User Name	Event Type	Category
2/15/2014	11:43:32 AM	File System Filter 'usaf' (6.2, 2012-07-2...	Microsoft-Windows-FilterMa...	6	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The Active Directory Domain Services se...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The DCOM Server Process Launcher ser...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The RPC Endpoint Mapper service enter...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The Remote Procedure Call (RPC) servic...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The Background Tasks Infrastructure Se...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:33 AM	The Local Session Manager service enter...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:34 AM	The Windows Event Log service entered...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:34 AM	The Themes service entered the running...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The COM+ Event System service entered...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The User Profile Service service entered...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The System Event Notification Service se...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The Group Policy Client service entered t...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The Network Store Interface Service ser...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:35 AM	The TCP/IP NetBIOS Helper service ente...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
	11:43:36 AM	DHCPv4 client service is started	Microsoft-Windows-Dhcp-Cl...	50036	RD40.Voyager.local	N/A	Information	(4)
	11:43:36 AM	DHCPv6 client service is started	Microsoft-Windows-DHCPv6...	51046	RD40.Voyager.local	N/A	Information	(4)
	11:43:36 AM	The DNS Client service entered the runn...	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None



**Click** to view the following information:

***Opens the saved log stored in current system or network share.***

### 3.6 How to View Service Information?

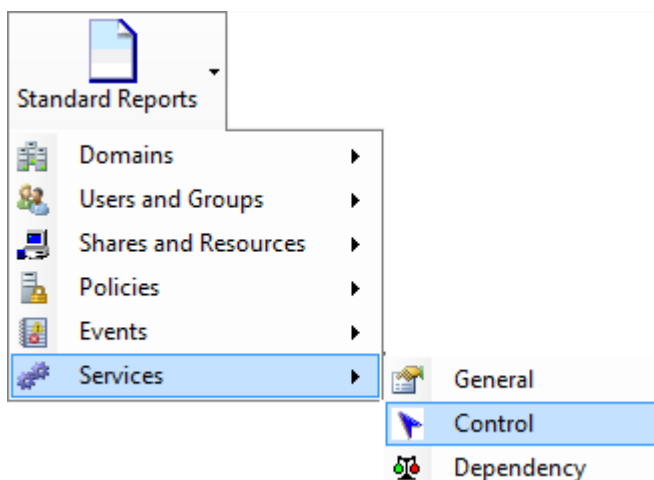


Click to view the following information:

**Display Name, Start up, Service Type, Account, and Current State**

The screenshot shows the 'Services - General (RD40)' window. The 'General' tab is selected, and the 'Filter' is set to 'Not Applied'. The table below lists the services and their status.

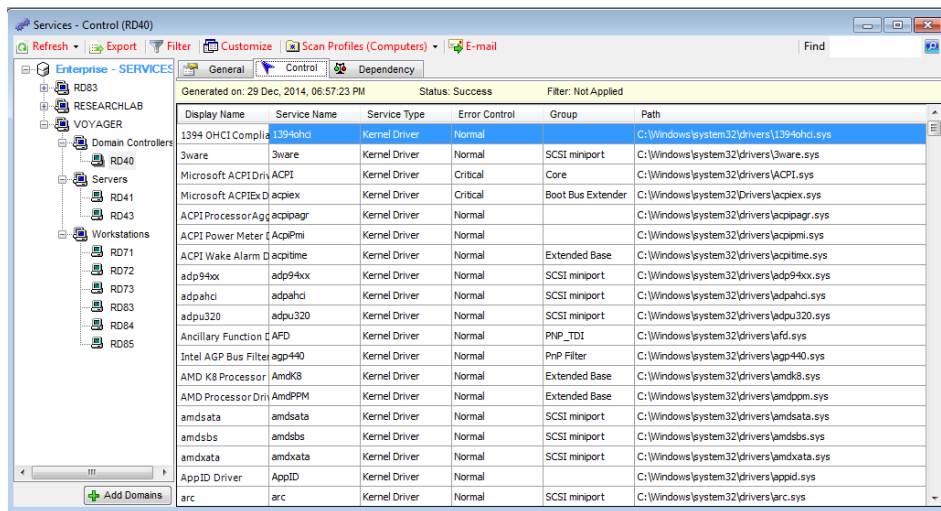
Display Name	StartUp	Service Type	Account	Current State
Cryptographic Services	Auto	Share Process	NT AUTHORITY\NetworkService	Running
DNS Client	Auto	Share Process	NT AUTHORITY\NetworkService	Running
KDC Proxy Server service (KPS)	Manual	Share Process	NT AUTHORITY\NetworkService	Stopped
KtmRm for Distributed Transaction Coordinator	Manual	Share Process	NT AUTHORITY\NetworkService	Stopped
Workstation	Auto	Share Process	NT AUTHORITY\NetworkService	Running
Distributed Transaction Coordinator	Auto	Own Process	NT AUTHORITY\NetworkService	Running
Network Access Protection Agent	Manual	Share Process	NT AUTHORITY\NetworkService	Stopped
Network Location Awareness	Auto	Share Process	NT AUTHORITY\NetworkService	Running
IPsec Policy Agent	Manual	Share Process	NT AUTHORITY\NetworkService	Running
RPC Endpoint Mapper	Auto	Share Process	NT AUTHORITY\NetworkService	Running
Remote Procedure Call (RPC) Locator	Manual	Own Process	NT AUTHORITY\NetworkService	Stopped
Remote Procedure Call (RPC)	Auto	Share Process	NT AUTHORITY\NetworkService	Running
Software Protection	Auto	Own Process	NT AUTHORITY\NetworkService	Stopped
Telephony	Manual	Own Process	NT AUTHORITY\NetworkService	Stopped
Remote Desktop Services	Manual	Share Process	NT AUTHORITY\NetworkService	Running
Windows Event Collector	Manual	Share Process	NT AUTHORITY\NetworkService	Stopped
Windows Remote Management (WS-Management)	Auto	Share Process	NT AUTHORITY\NetworkService	Running
Application Layer Gateway Service	Manual	Own Process	NT AUTHORITY\LocalService	Stopped
ApplicationIdentity	Manual	Share Process	NT AUTHORITY\LocalService	Stopped



Click to view the following information:

**Display Name, Service Name, Error Control, Group, and Path**

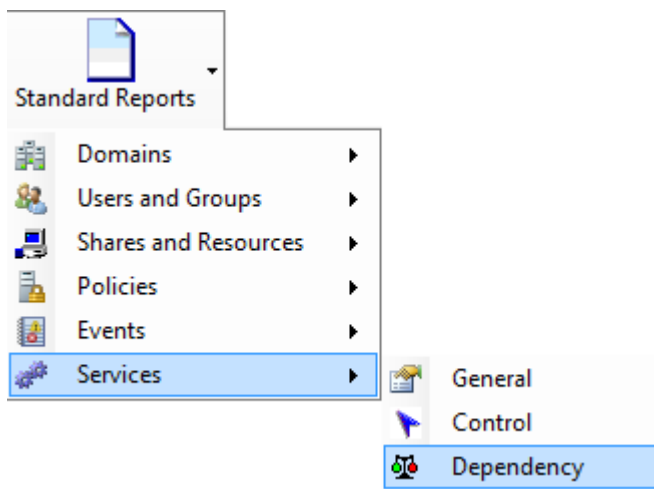
## CHAPTER 2 – Standard Reports



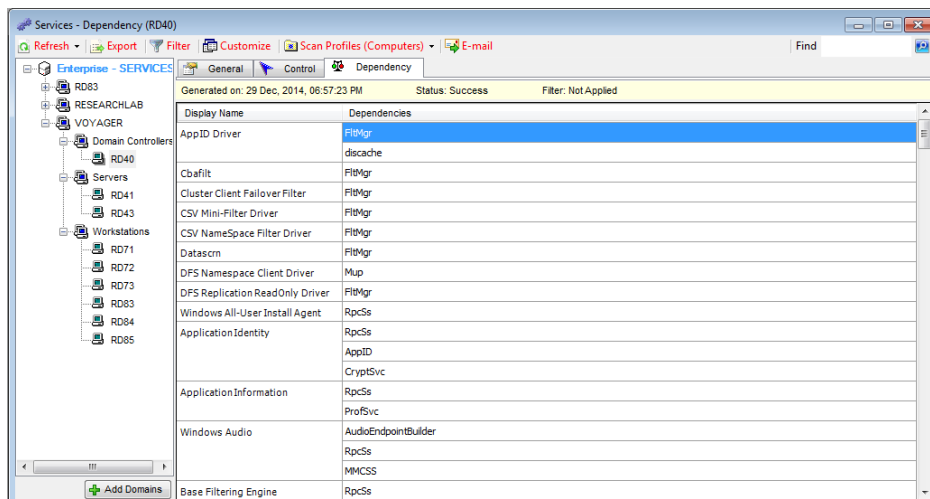
Services - Control (RD40)

Generated on: 29 Dec, 2014, 06:57:23 PM Status: Success Filter: Not Applied

Display Name	Service Name	Service Type	Error Control	Group	Path
1394 OHCI Combi...	1394ohci	Kernel Driver	Normal		C:\Windows\system32\drivers\1394ohci.sys
3ware	3ware	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\3ware.sys
Microsoft ACPI Dr...	ACPI	Kernel Driver	Critical	Core	C:\Windows\system32\drivers\ACPI.sys
Microsoft ACPI Ext...	acpiex	Kernel Driver	Critical	Boot Bus Extender	C:\Windows\system32\drivers\acpiex.sys
ACPI Processor Agg...	acpiagr	Kernel Driver	Normal		C:\Windows\system32\drivers\acpiagr.sys
ACPI Power Meter	AcpiPmi	Kernel Driver	Normal		C:\Windows\system32\drivers\acpipmi.sys
ACPI Wake Alarm D...	acptime	Kernel Driver	Normal	Extended Base	C:\Windows\system32\drivers\acptime.sys
adp94xx	adp94xx	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\adp94xx.sys
adpahci	adpahci	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\adpahci.sys
adpu320	adpu320	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\adpu320.sys
Ancillary Function...	AFD	Kernel Driver	Normal	PNP_TDI	C:\Windows\system32\drivers\afd.sys
Intel AGP Bus Filte...	agp440	Kernel Driver	Normal	PnP Filter	C:\Windows\system32\drivers\agp440.sys
AMD K8 Processor	AmdK8	Kernel Driver	Normal	Extended Base	C:\Windows\system32\drivers\amdK8.sys
AMD Processor Dri...	AmdPPM	Kernel Driver	Normal	Extended Base	C:\Windows\system32\drivers\amdppm.sys
amdsata	amdsata	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\amdsata.sys
amdsbs	amdsbs	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\amdsbs.sys
amdxta	amdxta	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\amdxta.sys
AppID Driver	AppID	Kernel Driver	Normal		C:\Windows\system32\drivers\appid.sys
arc	arc	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\arc.sys



Click **Display Name, Dependencies** to view the following information:



Services - Dependency (RD40)

Generated on: 29 Dec, 2014, 06:57:23 PM Status: Success Filter: Not Applied

Display Name	Dependencies
AppID Driver	FltMgr
	discache
Cbafilt	FltMgr
Cluster Client Failover Filter	FltMgr
CSV Mini-Filter Driver	FltMgr
CSV Namespace Filter Driver	FltMgr
Datascn	FltMgr
DFS Namespace Client Driver	Mup
DFS Replication Read Only Driver	FltMgr
Windows All-User Install Agent	RpcSs
ApplicationIdentity	RpcSs
	AppID
	CryptSvc
ApplicationInformation	RpcSs
	ProfSvc
Windows Audio	AudioEndpointBuilder
	RpcSs
	MMCSS
Base Filtering Engine	RpcSs

## 4 Built-in Reports

### 4.1 About Built-in Reports

Built-in reports are a set of predefined reports that are based on some of the common tasks in Systems management reporting. Built-in reports are easy to use and speeds-up the report generation process.

Built-in reports encompass some of the significant standard resource reports, and added to that, additional reports, all of which could be generated across domains.

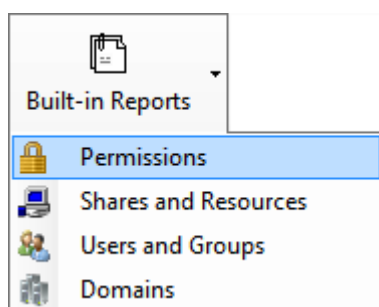
The built-in reports feature provides reports on the following resource categories:

- **Permissions Reports**
- **Shares and Resources**
- **Users and Groups**
- **Domains**

### 4.2 How to View Built-in Permissions Reports?

#### Permissions Reports

Permissions Reports includes reports that focus solely on reporting the access permissions assigned to users and groups on objects such as folders etcetera.



Click on button under **Built-in Reports** in button in the toolbar.

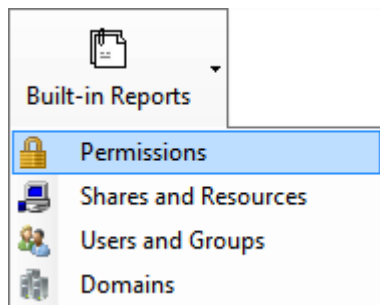
### List of Permissions Reports

Report Name	Description
<b>List of permissions for specific users and groups on folders</b>	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
<b>List of permissions for folders</b>	Reports the permissions associated with a selected set of folders.
<b>List of permissions for specific users and groups on files</b>	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.
<b>List of permissions for files</b>	Reports the permissions associated with files under a selected set of folders

### How to View Built-in Permissions Reports?

#### List of Permissions for Specific Users and Groups on Folders

This report allows you to view folder permissions for specific users and groups.

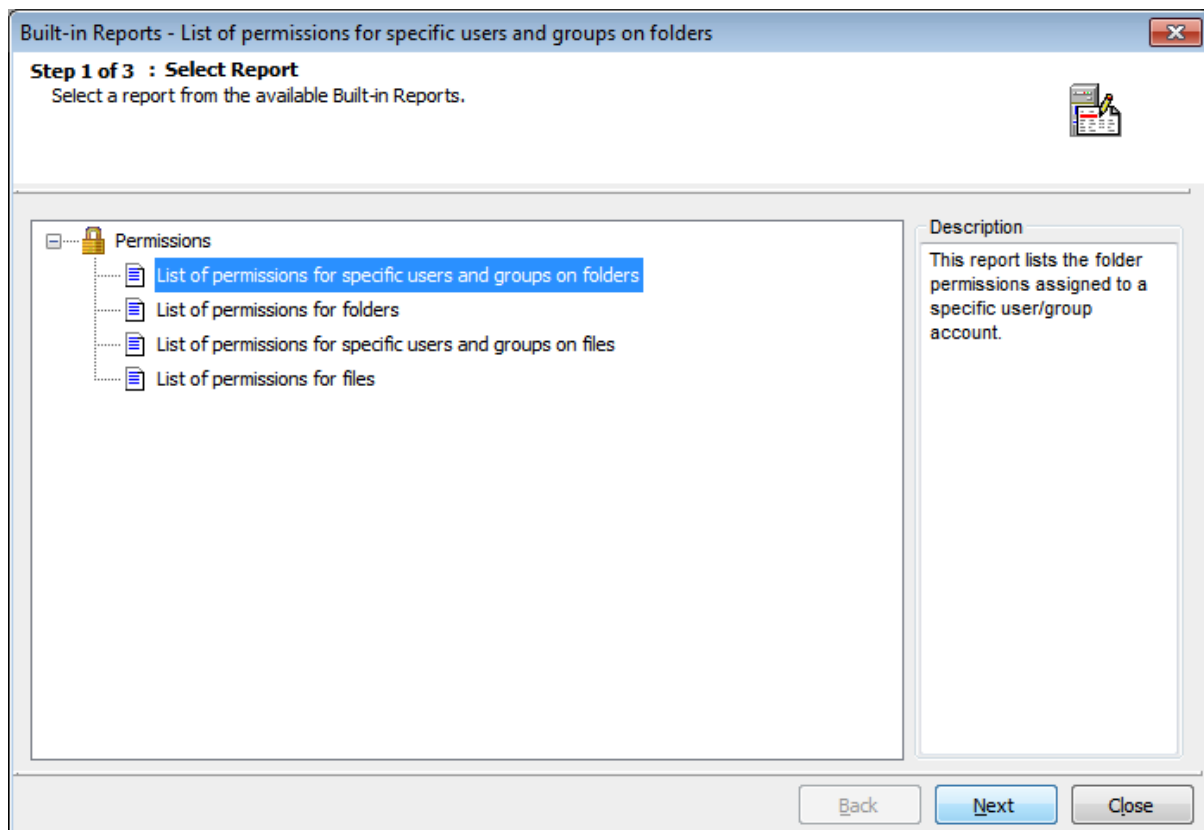


Click on button under Built-in Reports button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

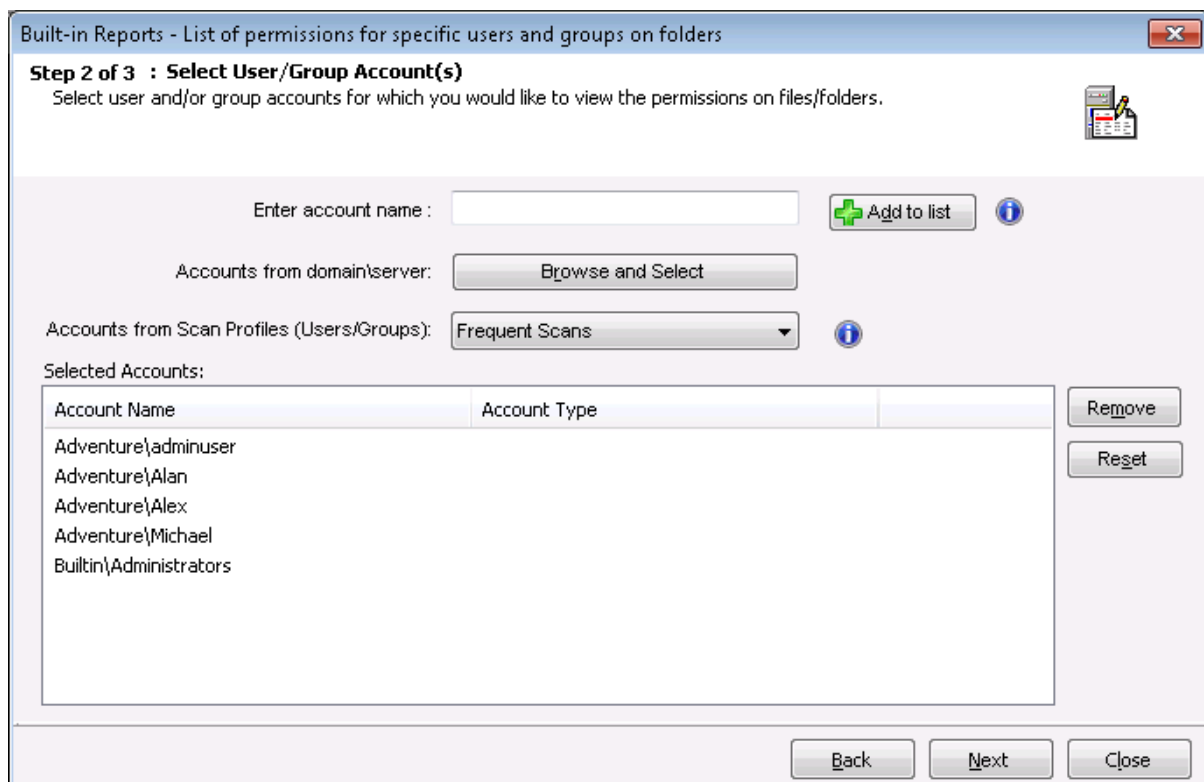
Select the report to be generated. Only one report can be generated at a time.



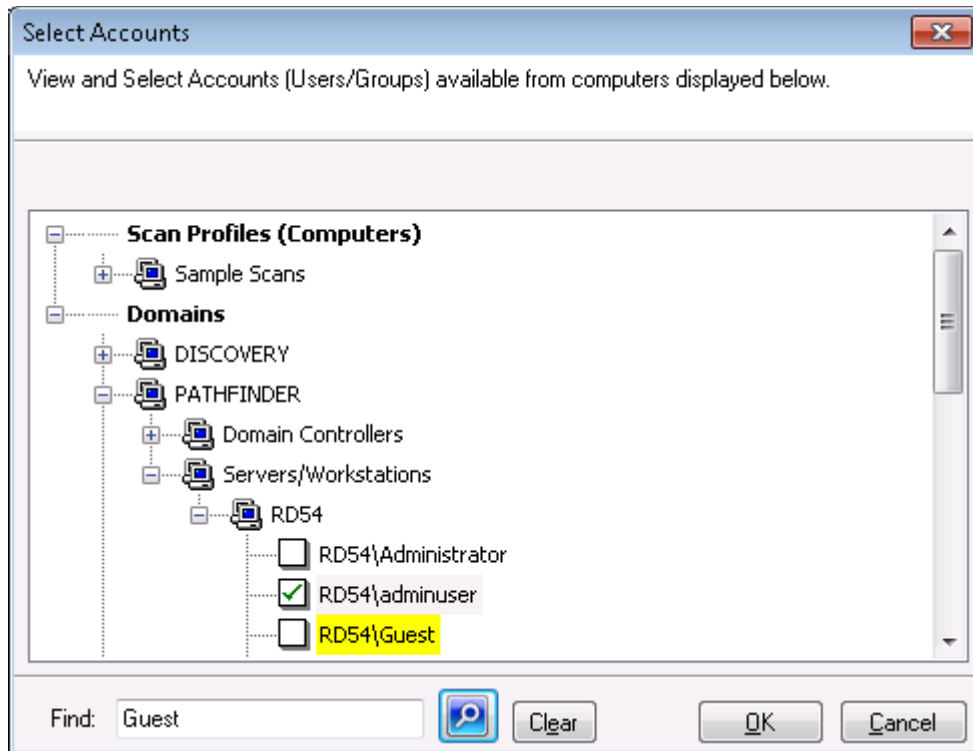
Click **Next** to proceed to the *next* step.

### Step 2: Select User/Group Accounts:

Select user and/or group accounts for which you would like to view the permissions for folders/files.



- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile.
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).

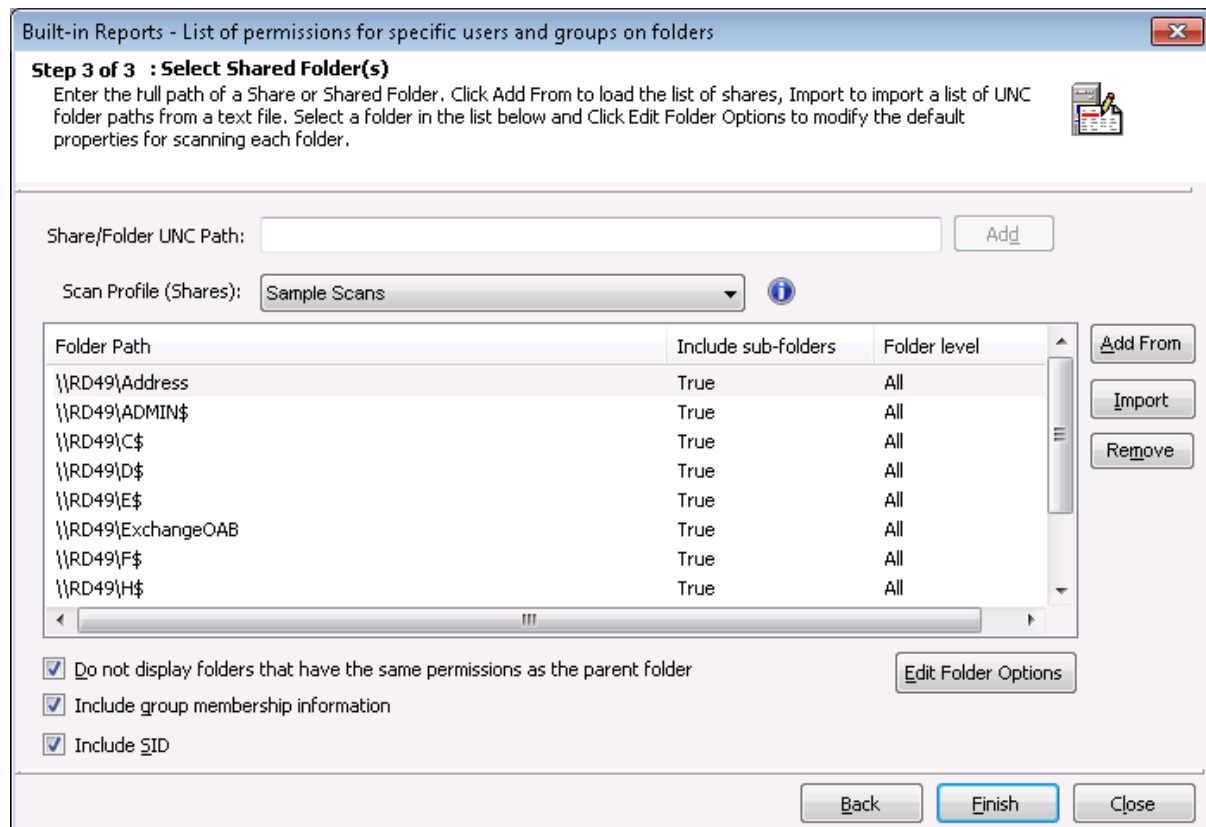
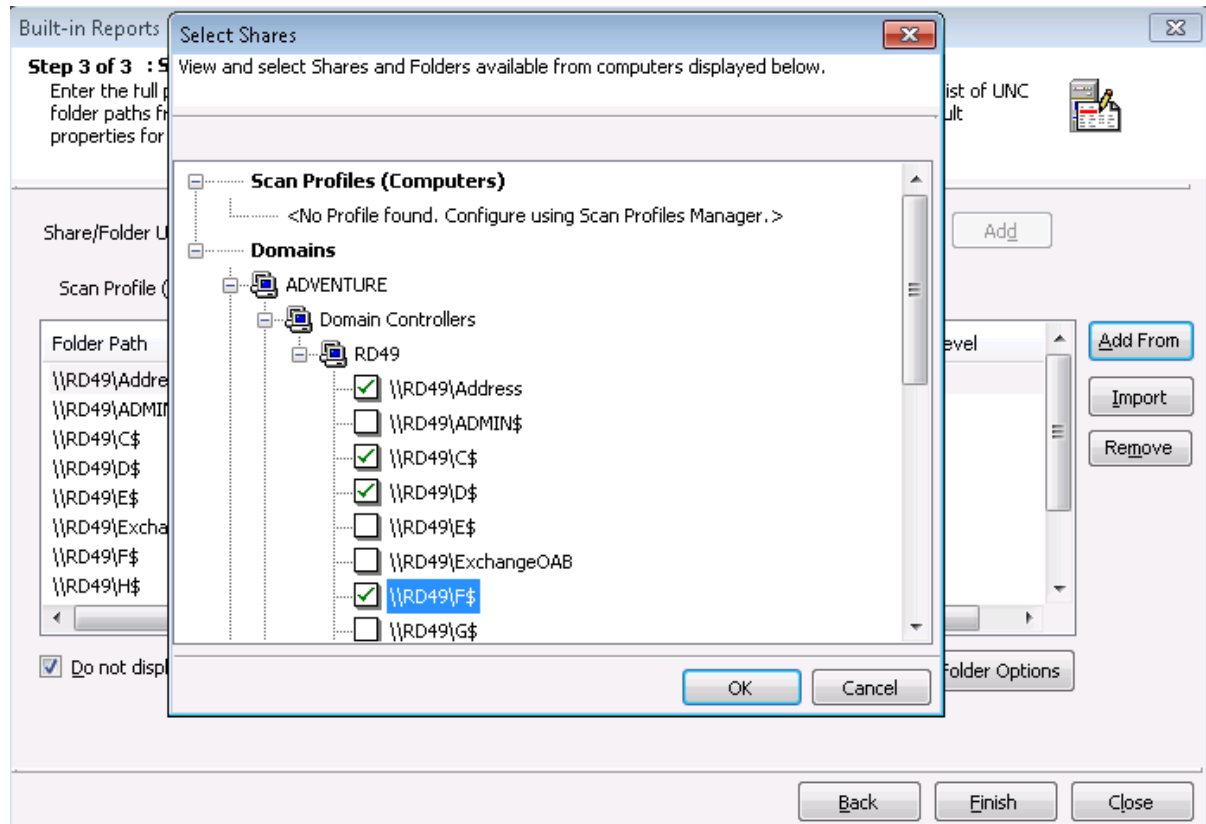


Use the **Find** option to search desired user/group accounts.

Click **Next** to Proceed.

### Step 3: Select shared folders

Select one or more servers to retrieve available shares.



## CHAPTER 3 – Built-in Reports

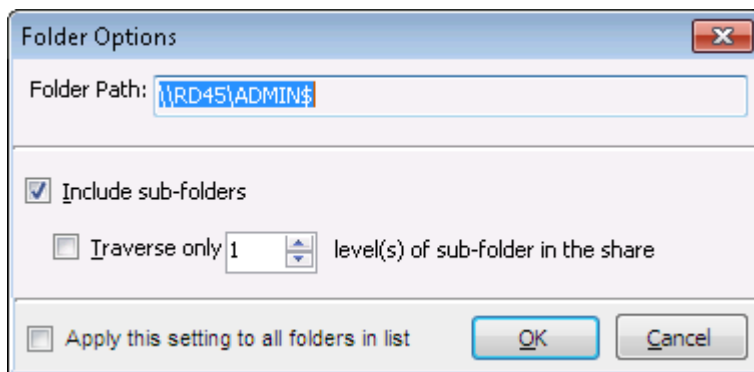
You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.

**NOTE:** The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

ARKWE defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit**

### Folder Options

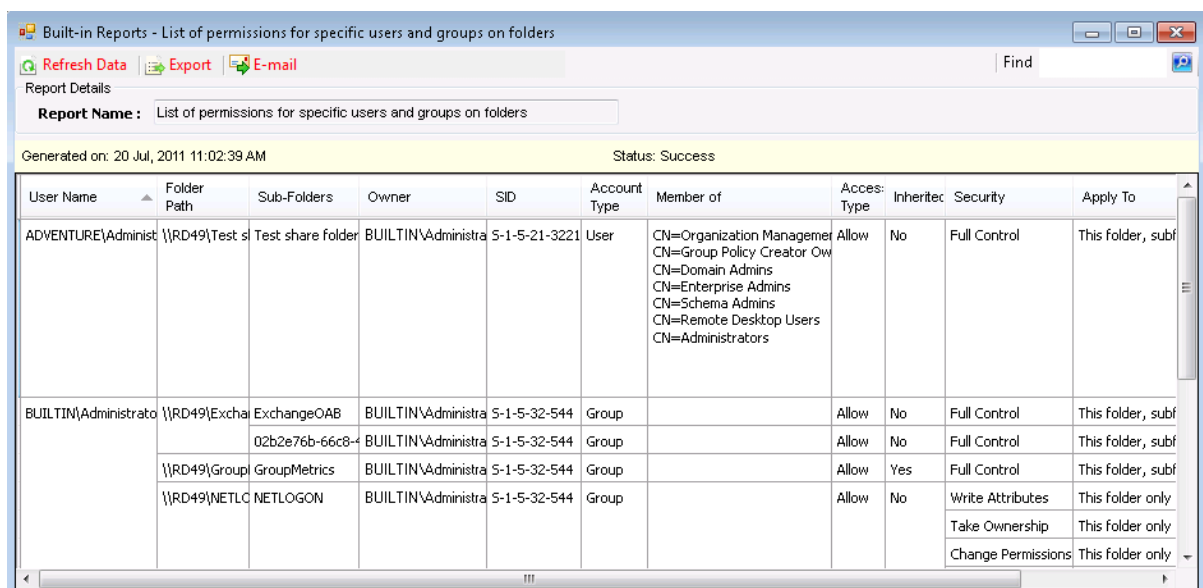


The 'Folder Options' dialog box is shown. It has a title bar with a close button. The 'Folder Path' field contains '\\RD45\\ADMIN\$'. Below this, there is a checked checkbox for 'Include sub-folders'. Underneath, there is an unchecked checkbox for 'Traverse only' followed by a spinner box set to '1' and the text 'level(s) of sub-folder in the share'. At the bottom, there is an unchecked checkbox for 'Apply this setting to all folders in list' and two buttons: 'OK' and 'Cancel'.

Click **OK** to *Proceed*.

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:

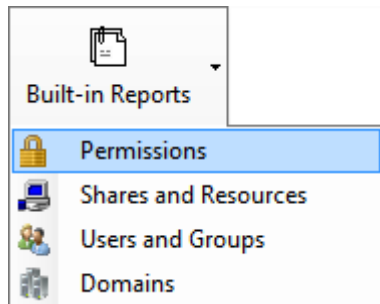


The screenshot shows a window titled 'Built-in Reports - List of permissions for specific users and groups on folders'. It has a menu bar with 'Refresh Data', 'Export', and 'E-mail'. Below the menu bar is a 'Report Details' section with a 'Report Name' field containing 'List of permissions for specific users and groups on folders'. Below this is a status bar showing 'Generated on: 20 Jul, 2011 11:02:39 AM' and 'Status: Success'. The main area is a table with the following columns: User Name, Folder Path, Sub-Folders, Owner, SID, Account Type, Member of, Access Type, Inherit, Security, and Apply To. The table contains several rows of data, including permissions for ADVENTURE\Administrators and BUILTIN\Administrators on various folders like \\RD49\\Test share and \\RD49\\Exchange.

User Name	Folder Path	Sub-Folders	Owner	SID	Account Type	Member of	Access Type	Inherit	Security	Apply To
ADVENTURE\Administrators	\\RD49\\Test share	Test share folder	BUILTIN\Administrators	S-1-5-21-3221	User	CN=Organization Management, CN=Group Policy Creator Owners, CN=Domain Admins, CN=Enterprise Admins, CN=Schema Admins, CN=Remote Desktop Users, CN=Administrators	Allow	No	Full Control	This folder, subfolders and files
BUILTIN\Administrators	\\RD49\\Exchange	ExchangeOAB	BUILTIN\Administrators	S-1-5-32-544	Group		Allow	No	Full Control	This folder, subfolders and files
		02b2e76b-66c8-4000-8000-000000000000	BUILTIN\Administrators	S-1-5-32-544	Group		Allow	No	Full Control	This folder, subfolders and files
	\\RD49\\GroupMetrics	GroupMetrics	BUILTIN\Administrators	S-1-5-32-544	Group		Allow	Yes	Full Control	This folder, subfolders and files
	\\RD49\\NETLOGON	NETLOGON	BUILTIN\Administrators	S-1-5-32-544	Group		Allow	No	Write Attributes, Take Ownership, Change Permissions	This folder only

### How to view Built-in Permissions Reports?

#### List of Permissions for Folders

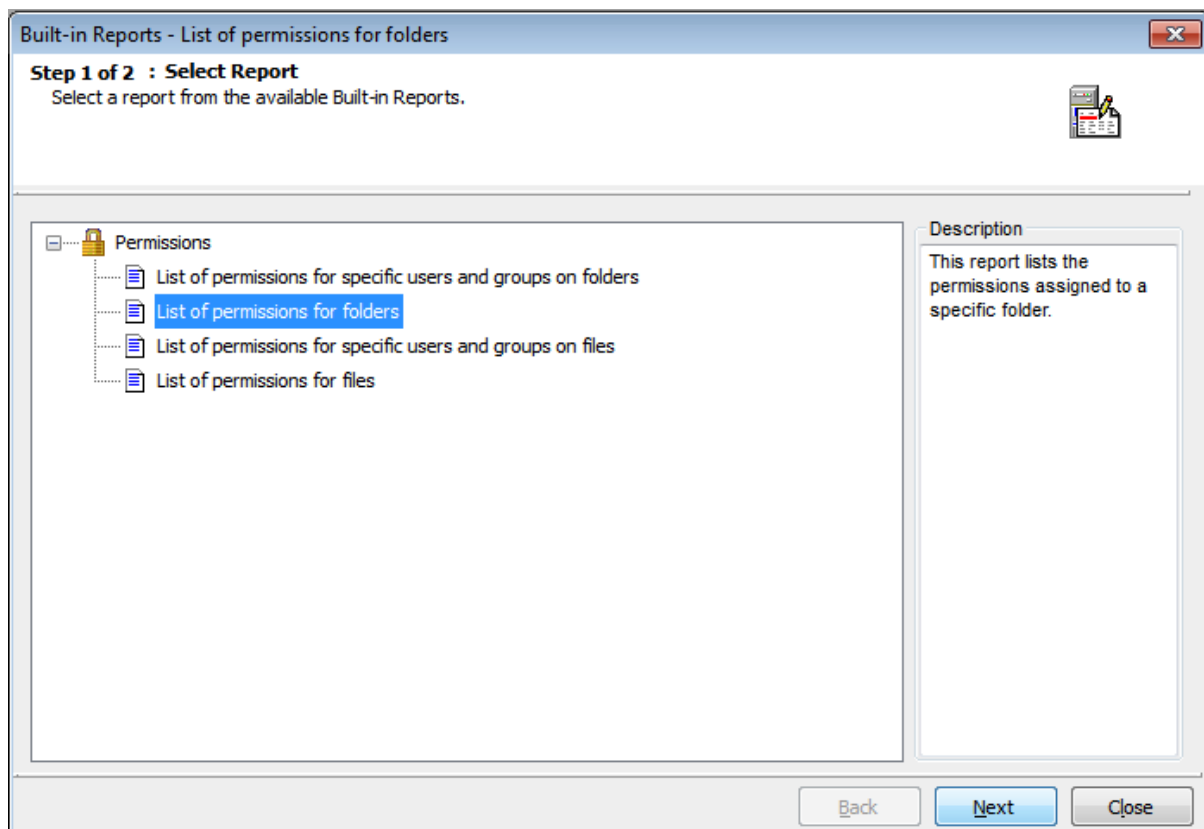


Click on **Permissions** button under Built-in Reports button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

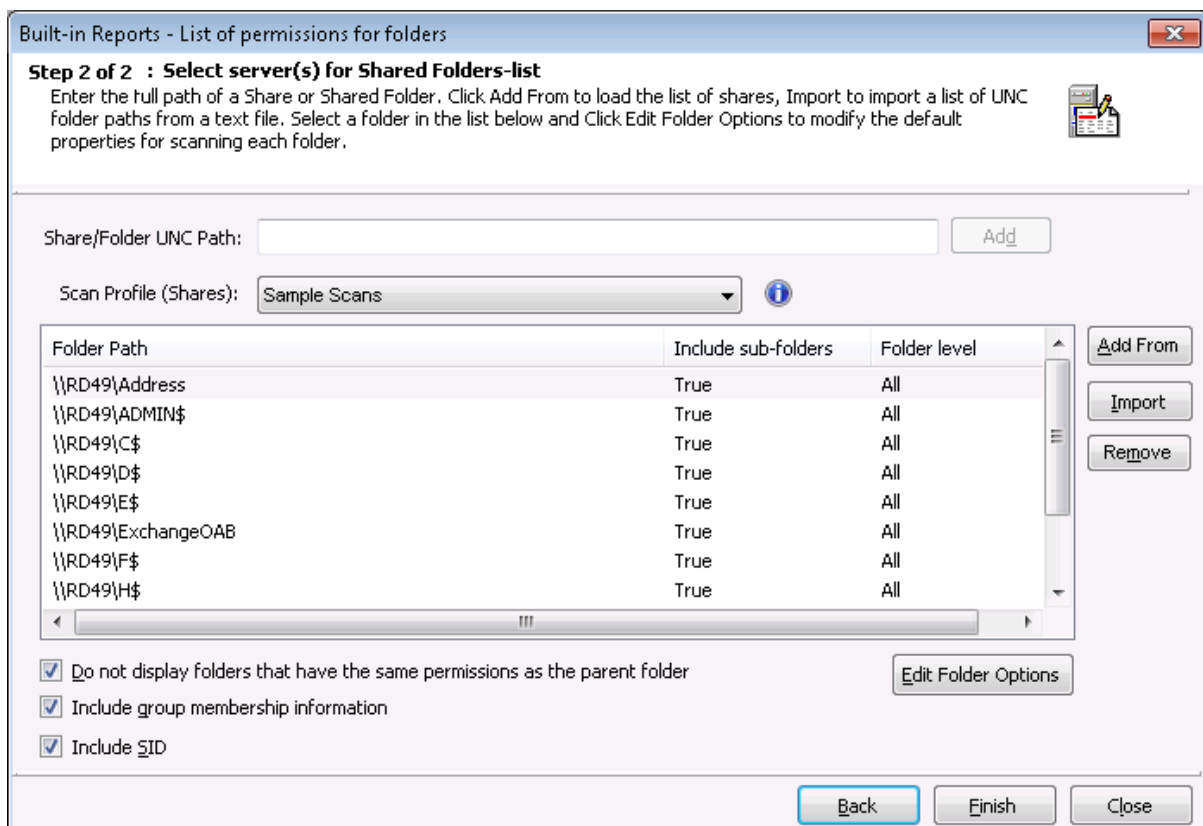
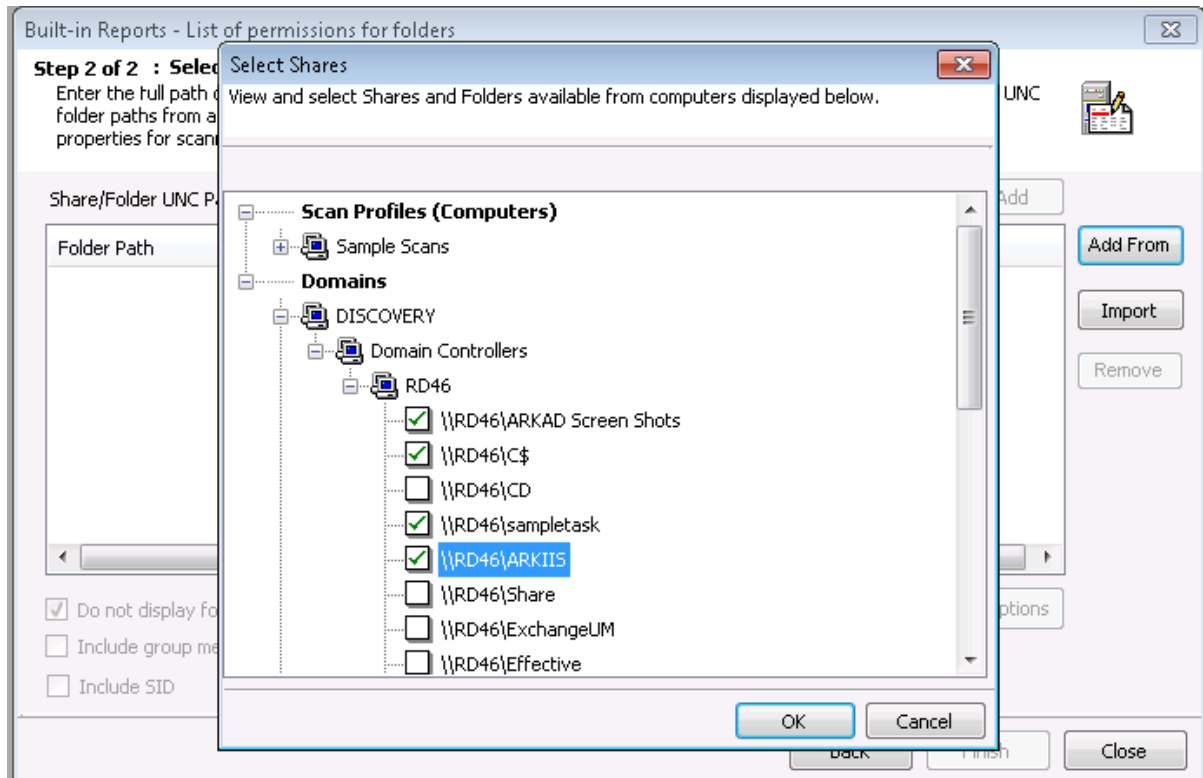
Select the report to be generated. Only one report can be generated at a time.



Click **Next** to the Proceed to the *Next* Step.

### Step 2: Select shared folders:

Select one or more servers to retrieve available shares



You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a

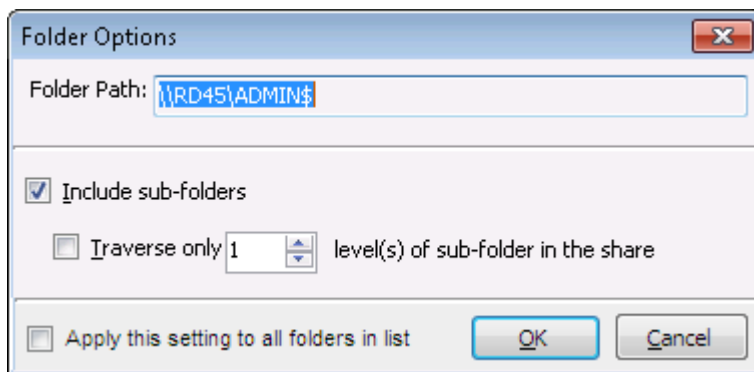
## CHAPTER 3 – Built-in Reports

list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.

**NOTE:** The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

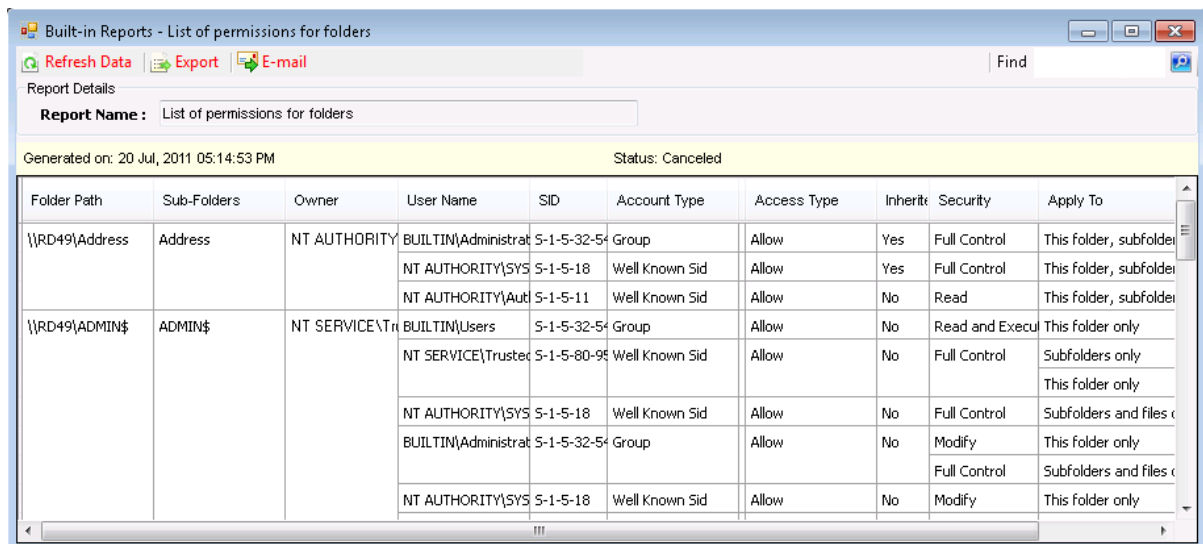
ARKWE defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.



Click **OK** to *Proceed*.

Click **Finish** to generate the selected report.

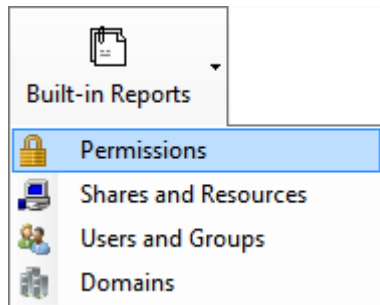
After the data collection process is complete, the report would be generated in a report window as shown below:



### How to view Built-in Permissions Reports?

#### List of Permissions for Specific Users and Groups on Files

This report allows you to view file permissions for specific users and groups.

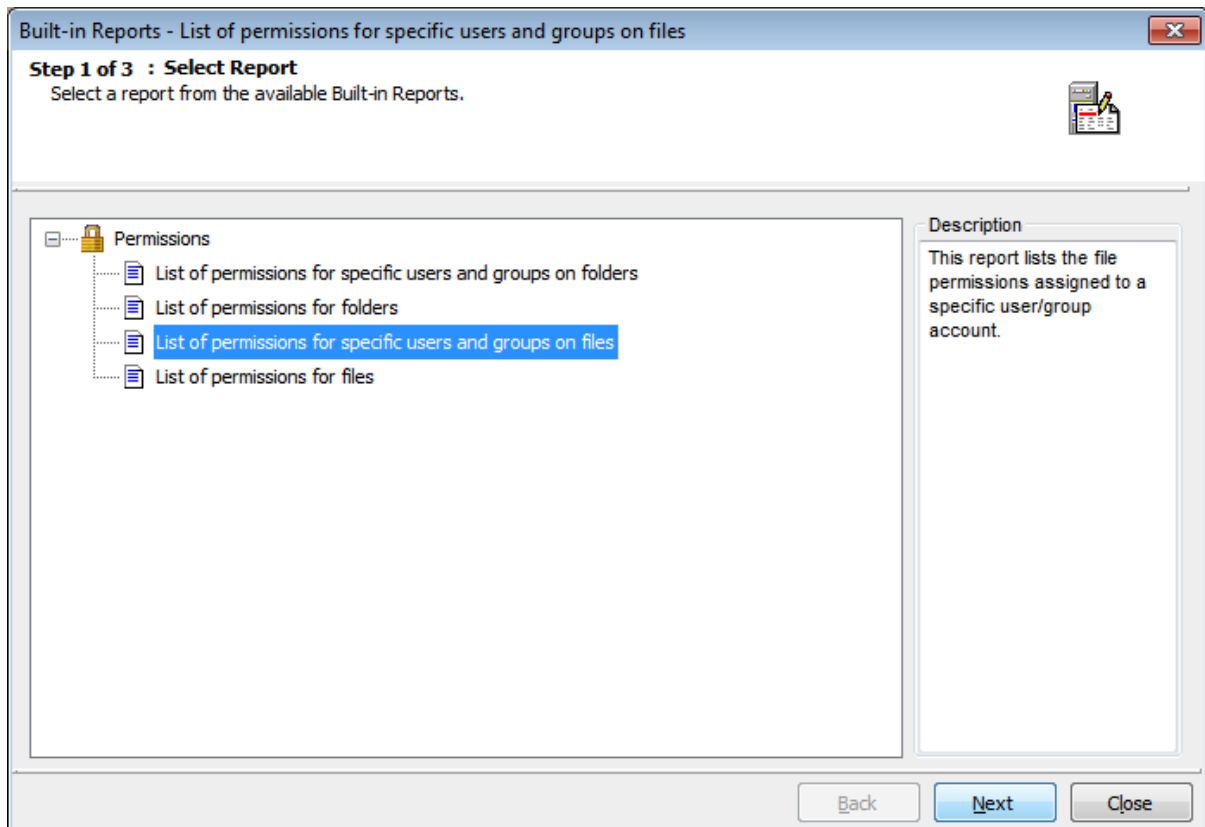


Click on **Permissions** button under Built-in Reports button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

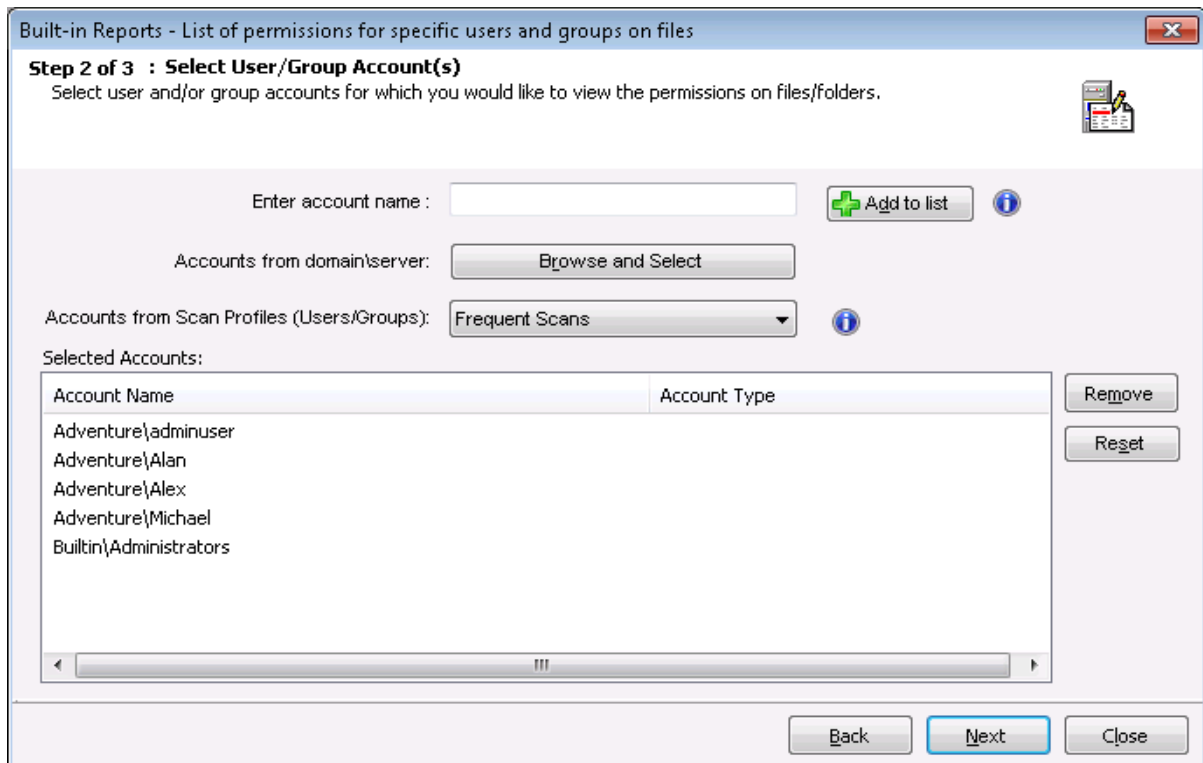
Select the report to be generated. Only one report can be generated at a time.



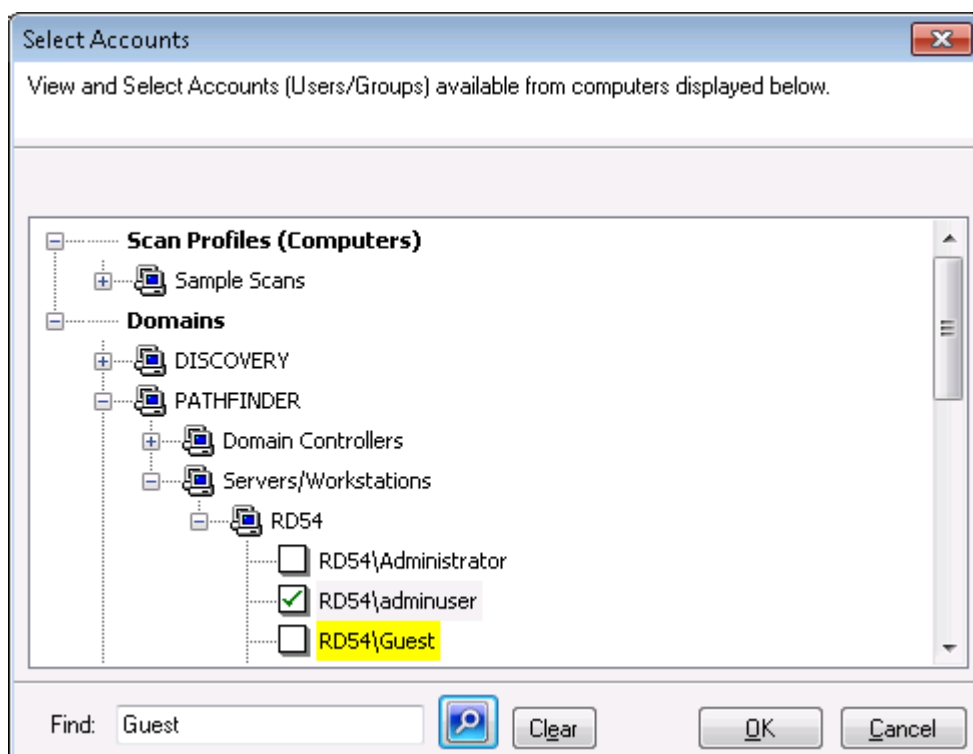
Click **Next** to Proceed to the *Next* step.

#### Step 2: Select User/Group Accounts:

Select user and/or group accounts for which you would like to view the permissions for folders/files.



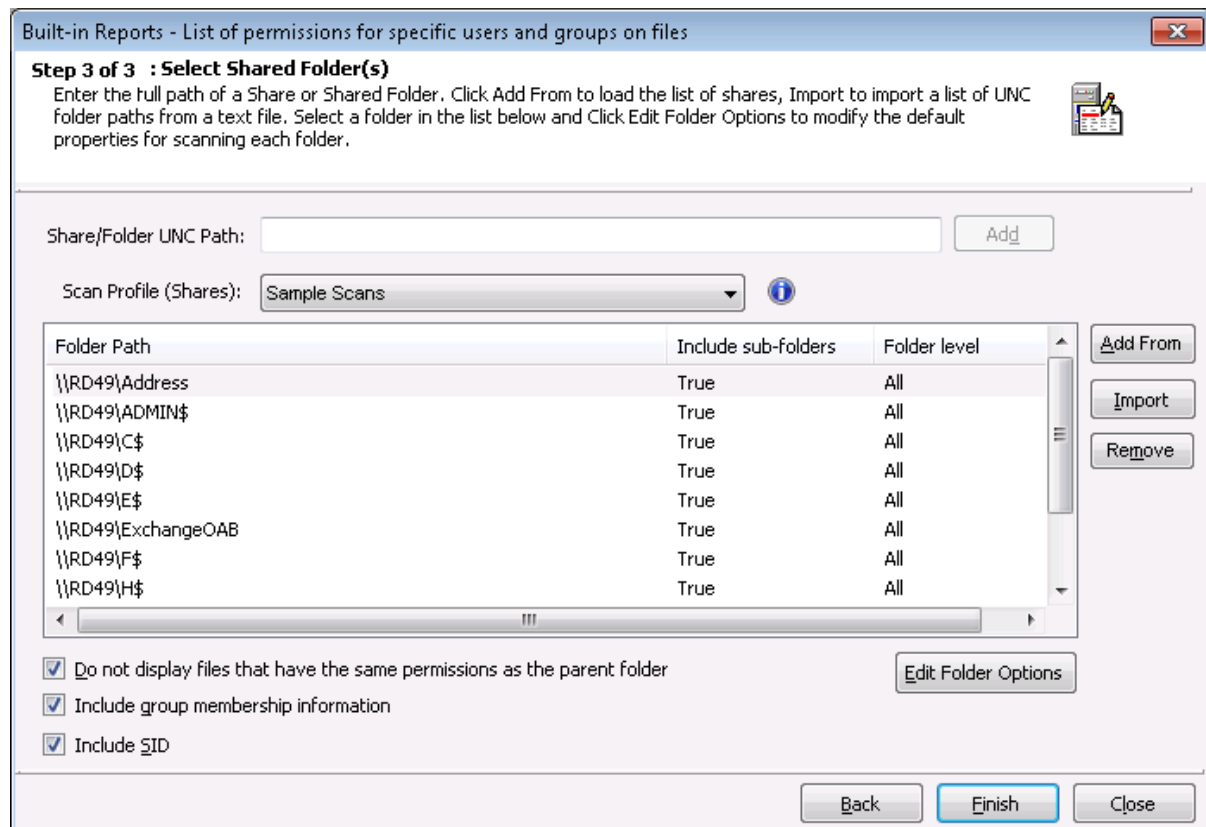
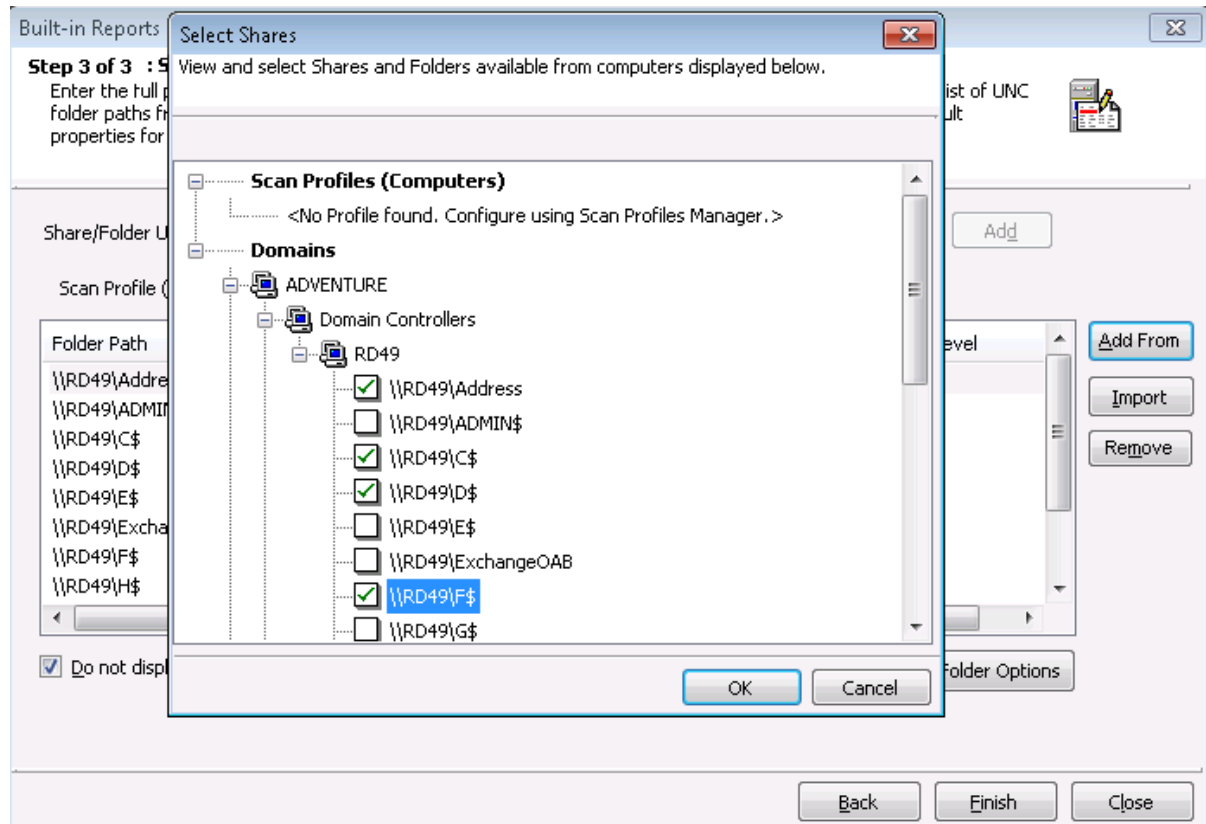
- Enter the name of User/Group in domain\account name format and click **Add to List** to add the name to selected accounts list.
- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile.
- Use **Browse and Select** option to retrieve users and groups from servers or Scan Profile (Computers).



Use the **Find** option to search desired user/group accounts. Click **Next** to Proceed.

### Step 3: Select Shared Folders

Select one or more servers to retrieve available shares.



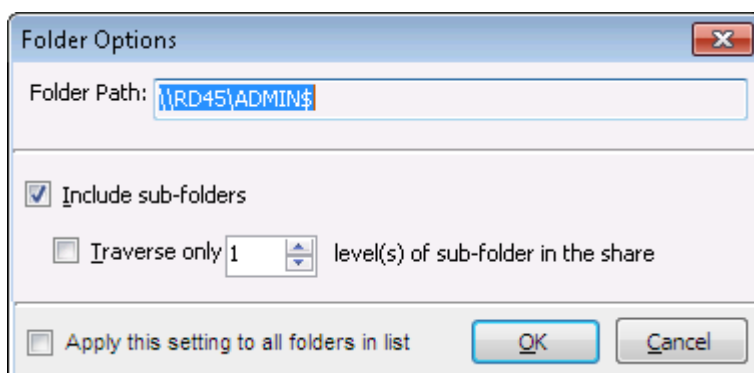
## CHAPTER 3 – Built-in Reports

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.

**NOTE:** The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

ARKWE defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options**.

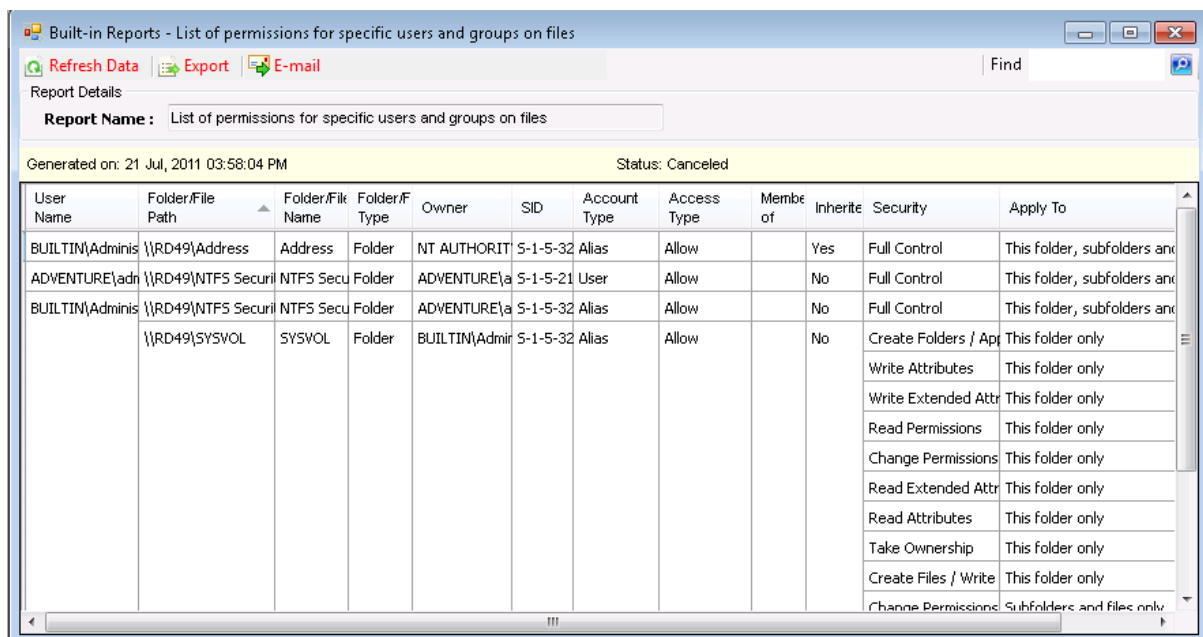


The 'Folder Options' dialog box is shown. It has a title bar with a close button. The 'Folder Path' field contains '\\RD45\\ADMIN\$'. Below this, there is a checked checkbox for 'Include sub-folders'. Underneath, there is an unchecked checkbox for 'Traverse only' followed by a spinner box set to '1' and the text 'level(s) of sub-folder in the share'. At the bottom, there is an unchecked checkbox for 'Apply this setting to all folders in list', and 'OK' and 'Cancel' buttons.

Click **OK** to Proceed.

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



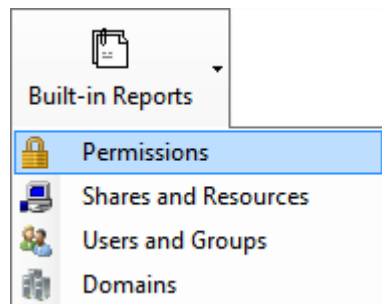
The screenshot shows a window titled 'Built-in Reports - List of permissions for specific users and groups on files'. It has buttons for 'Refresh Data', 'Export', and 'E-mail', and a 'Find' search box. The 'Report Details' section shows 'Report Name: List of permissions for specific users and groups on files'. Below this, it says 'Generated on: 21 Jul, 2011 03:58:04 PM' and 'Status: Canceled'. The main part of the window is a table with the following columns: User Name, Folder/File Path, Folder/File Name, Folder/File Type, Owner, SID, Account Type, Access Type, Member of, Inherit, Security, and Apply To. The table contains several rows of data, including entries for BUILTIN\Administrators and ADVENTURE\adriana on various folders like \\RD49\Address and \\RD49\NTFS Security.

User Name	Folder/File Path	Folder/File Name	Folder/File Type	Owner	SID	Account Type	Access Type	Member of	Inherit	Security	Apply To
BUILTIN\Administrators	\\RD49\Address	Address	Folder	NT AUTHORITY\SYSTEM	S-1-5-32-544	Alias	Allow		Yes	Full Control	This folder, subfolders and files
ADVENTURE\adriana	\\RD49\NTFS Security	NTFS Security	Folder	ADVENTURE\adriana	S-1-5-21-1016106810-1016106810-1016106810-1016106810	User	Allow		No	Full Control	This folder, subfolders and files
BUILTIN\Administrators	\\RD49\NTFS Security	NTFS Security	Folder	ADVENTURE\adriana	S-1-5-32-544	Alias	Allow		No	Full Control	This folder, subfolders and files
	\\RD49\SYSTEM	SYSTEM	Folder	BUILTIN\Administrators	S-1-5-32-544	Alias	Allow		No	Create Folders / Append Data	This folder only
									No	Write Attributes	This folder only
									No	Write Extended Attributes	This folder only
									No	Read Permissions	This folder only
									No	Change Permissions	This folder only
									No	Read Extended Attributes	This folder only
									No	Read Attributes	This folder only
									No	Take Ownership	This folder only
									No	Create Files / Write Data	This folder only
									No	Change Permissions	Subfolders and files only

### How to View Built-in Permissions Reports?

#### List of Permissions for Files

This report allows you to view the associated permissions for specific files.

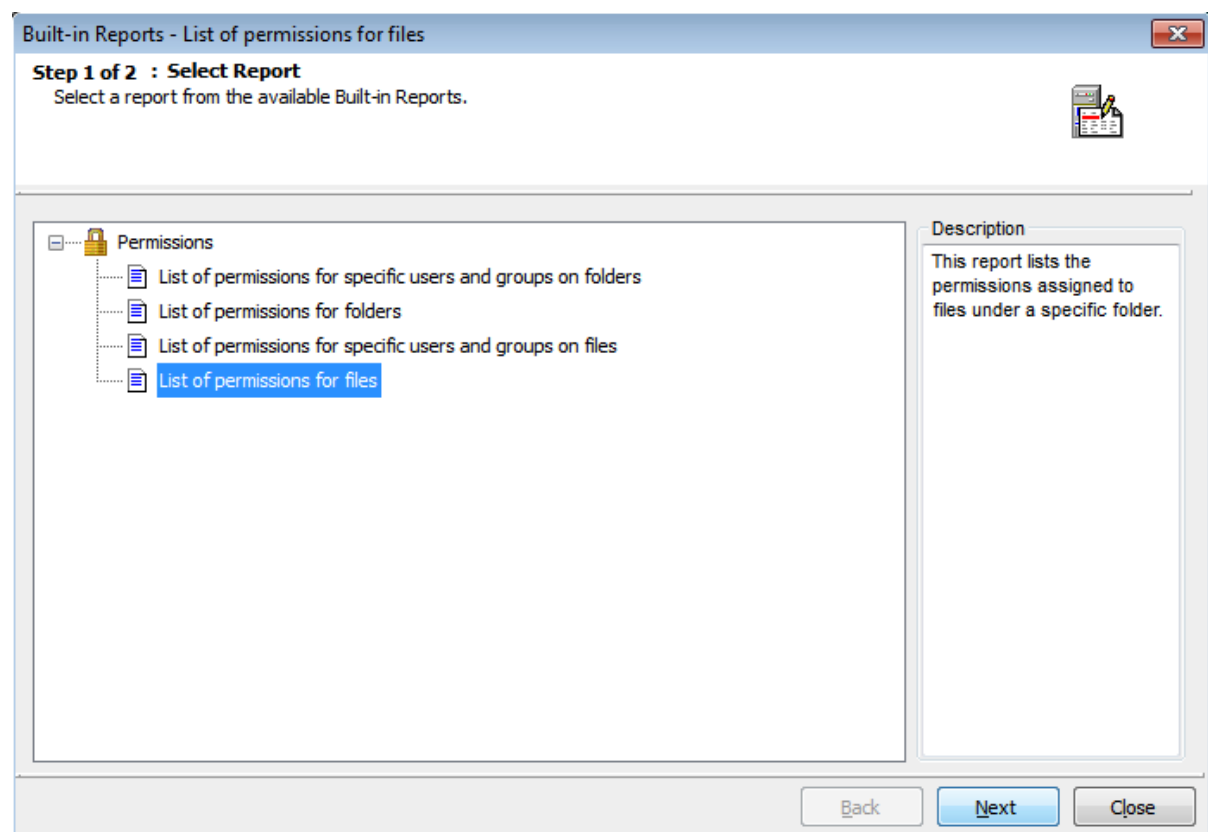


Click on **Permissions** button under Built-in Reports button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

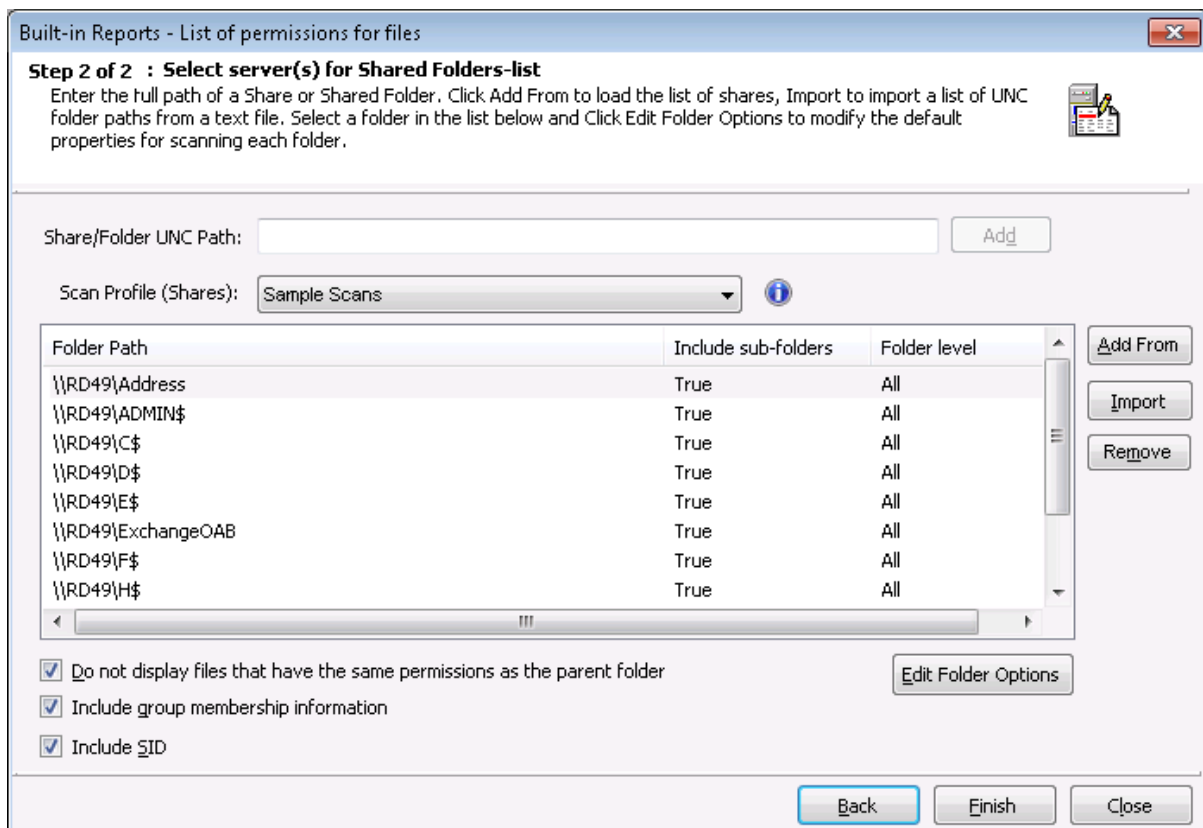
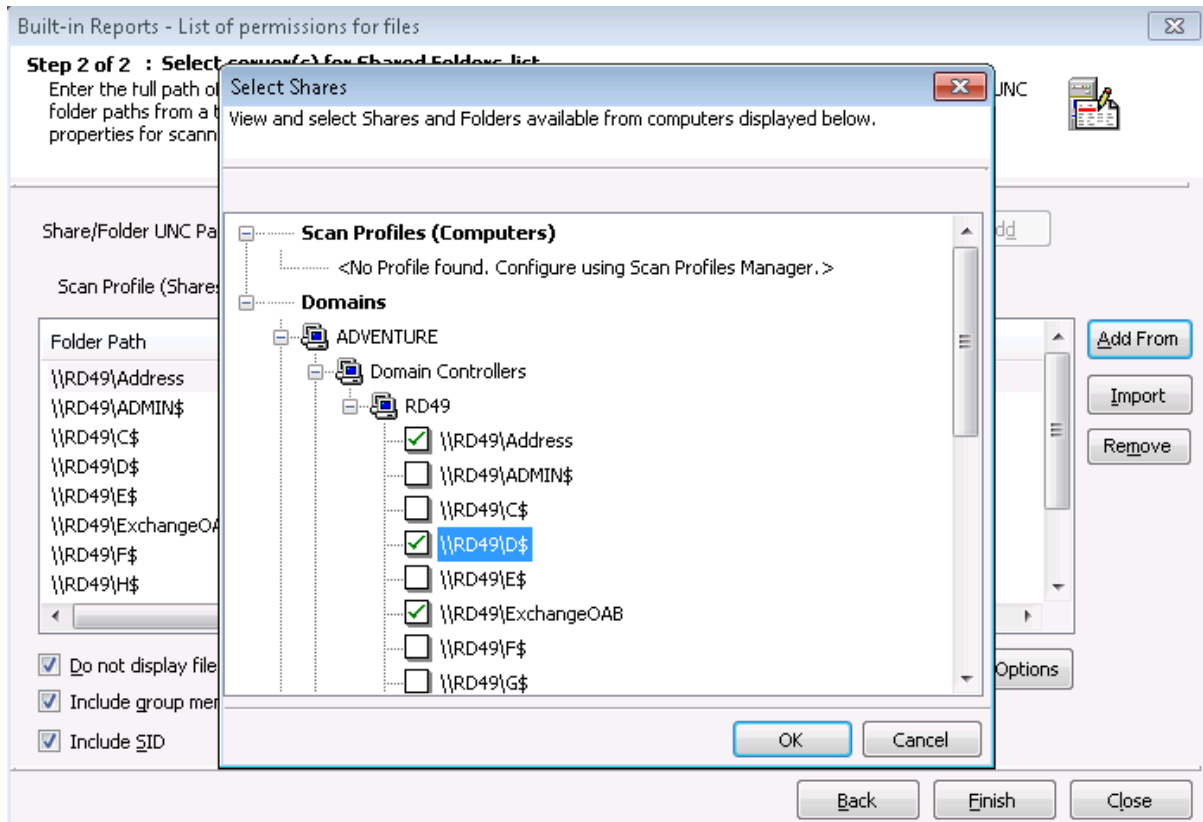
Select the report to be generated. Only one report can be generated at a time.



Click **Next** to Proceed to the *Next* step.

### Step 2: Select Shared Folders:

Select one or more servers to retrieve available shares



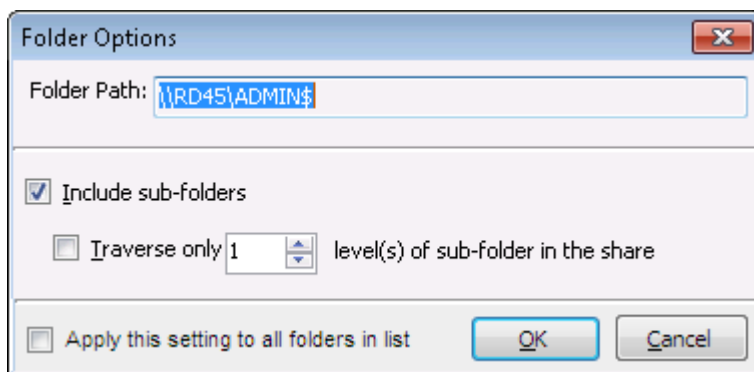
## CHAPTER 3 – Built-in Reports

You may also type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click **Add**, to add it to the list. In addition, you may also import a list of UNC paths to shared and non-shared folders from a text file by using the **Import** button.

Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.

**NOTE:** The "Do not display folders that have same permissions as the parent folder" option would be enabled by default.

ARKWE defaults to scanning all the sub-folders under a given shared folder. If you want to change the Include sub-folders and Folder level options click **Edit Folder Options-folders and Folder level options click Edit Folder Options**.

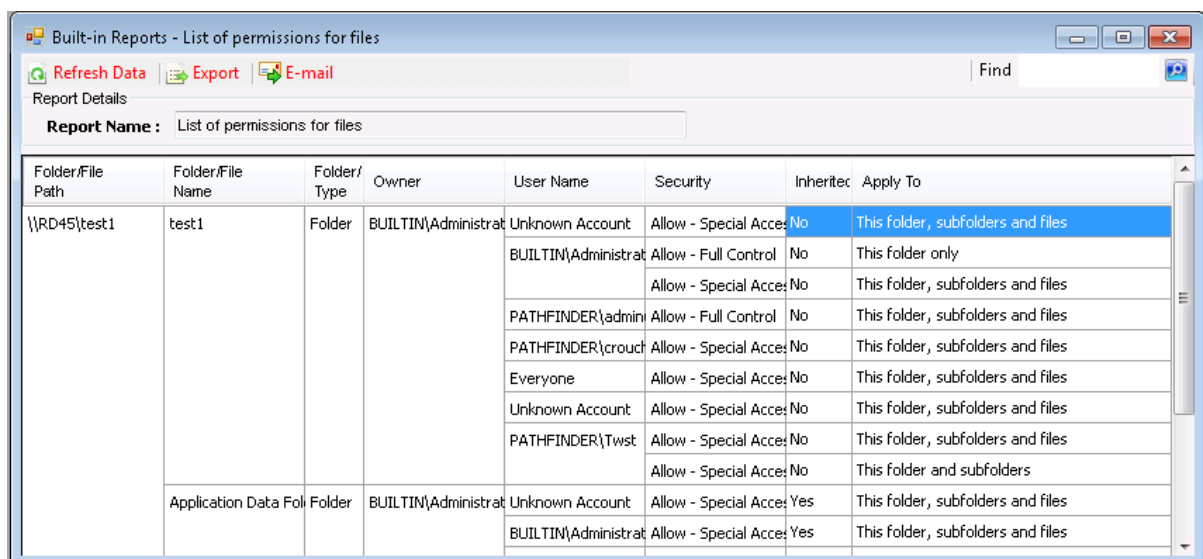


The 'Folder Options' dialog box is shown. It has a title bar with a close button. The 'Folder Path' field contains '\\RD45\\ADMIN\$'. Below this, there is a checked checkbox for 'Include sub-folders'. Underneath, there is an unchecked checkbox for 'Traverse only' followed by a spinner box set to '1' and the text 'level(s) of sub-folder in the share'. At the bottom, there is an unchecked checkbox for 'Apply this setting to all folders in list', and 'OK' and 'Cancel' buttons.

Click **OK** to *Proceed*.

Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



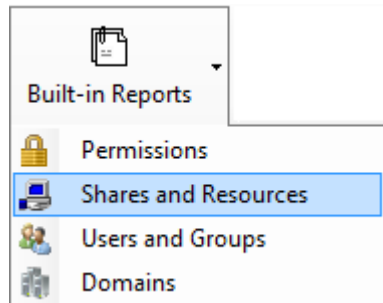
The 'Built-in Reports - List of permissions for files' window is shown. It has a title bar with standard window controls. Below the title bar, there are buttons for 'Refresh Data', 'Export', and 'E-mail', and a 'Find' search box. The 'Report Details' section shows 'Report Name: List of permissions for files'. The main area is a table with the following columns: Folder/File Path, Folder/File Name, Folder/Type, Owner, User Name, Security, Inheritec, and Apply To.

Folder/File Path	Folder/File Name	Folder/Type	Owner	User Name	Security	Inheritec	Apply To
\\RD45\\test1	test1	Folder	BUILTIN\Administrat	Unknown Account	Allow - Special Acce	No	This folder, subfolders and files
				BUILTIN\Administrat	Allow - Full Control	No	This folder only
					Allow - Special Acce	No	This folder, subfolders and files
				PATHFINDER\admin	Allow - Full Control	No	This folder, subfolders and files
				PATHFINDER\crouc	Allow - Special Acce	No	This folder, subfolders and files
				Everyone	Allow - Special Acce	No	This folder, subfolders and files
				Unknown Account	Allow - Special Acce	No	This folder, subfolders and files
				PATHFINDER\Twst	Allow - Special Acce	No	This folder, subfolders and files
					Allow - Special Acce	No	This folder and subfolders
	Application Data Foli	Folder	BUILTIN\Administrat	Unknown Account	Allow - Special Acce	Yes	This folder, subfolders and files
				BUILTIN\Administrat	Allow - Special Acce	Yes	This folder, subfolders and files

### 4.3 How to View Built-in Reports for Shares and Resources?

#### Shares and Resources Reports

The Shares and Resources reports can be generated against domain(s) and specific server(s) as well.

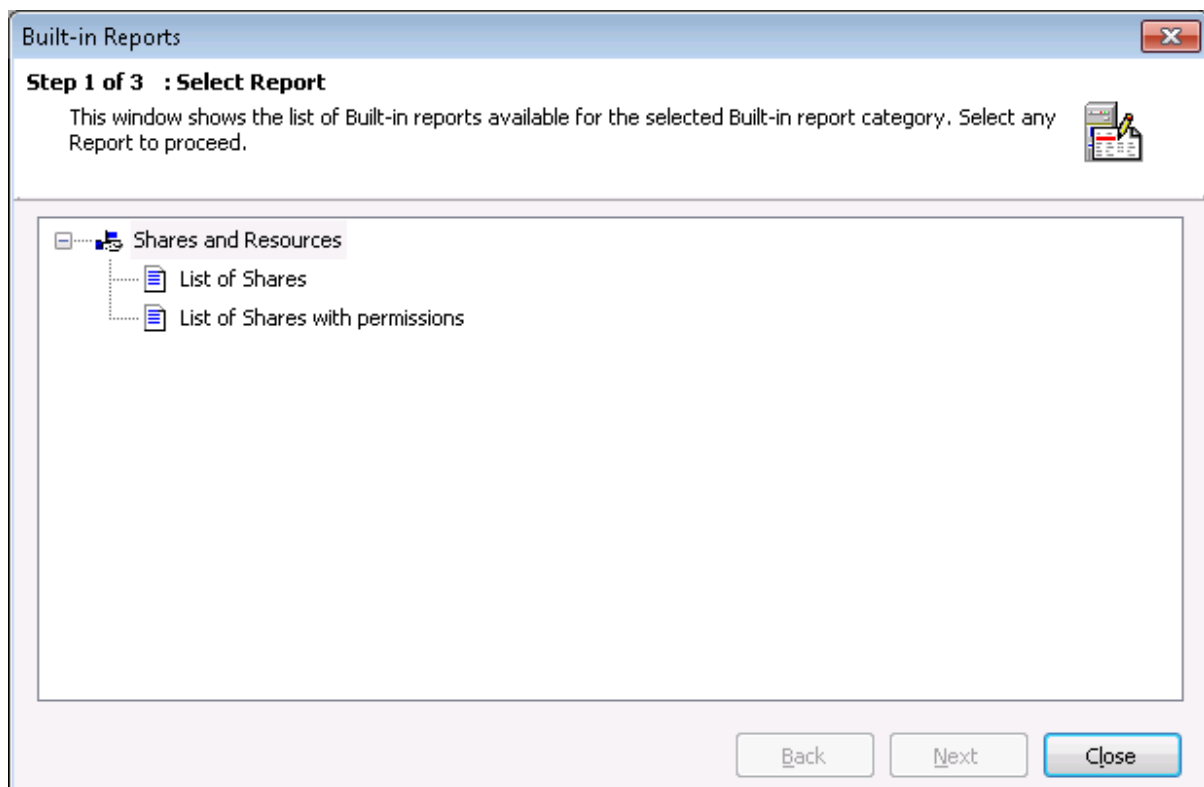


Click on button under Built-in Reports in button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

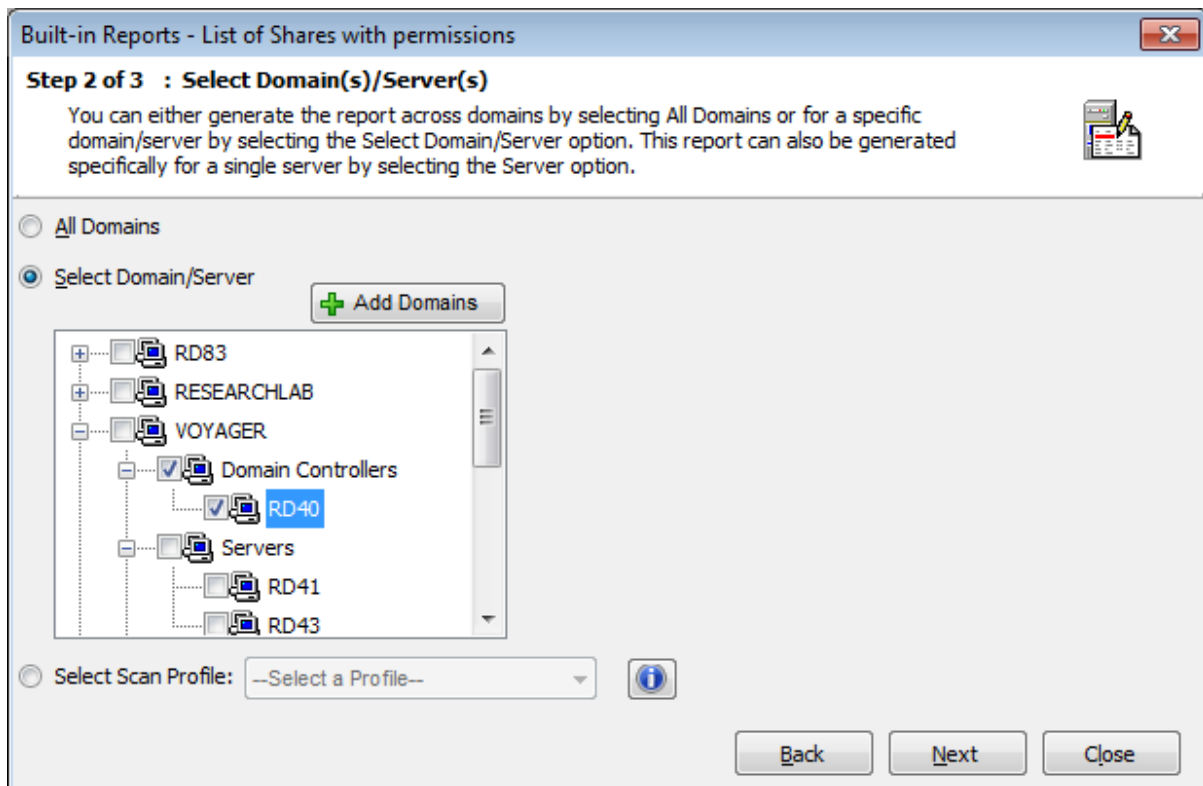
Select the report to be generated. Only one report can be generated at a time. Click Next to proceed to the next step.



### Step 2: Select Domain (s) / Server(s)

Select the server(s)/Domain (s), for which the report needs to be generated.

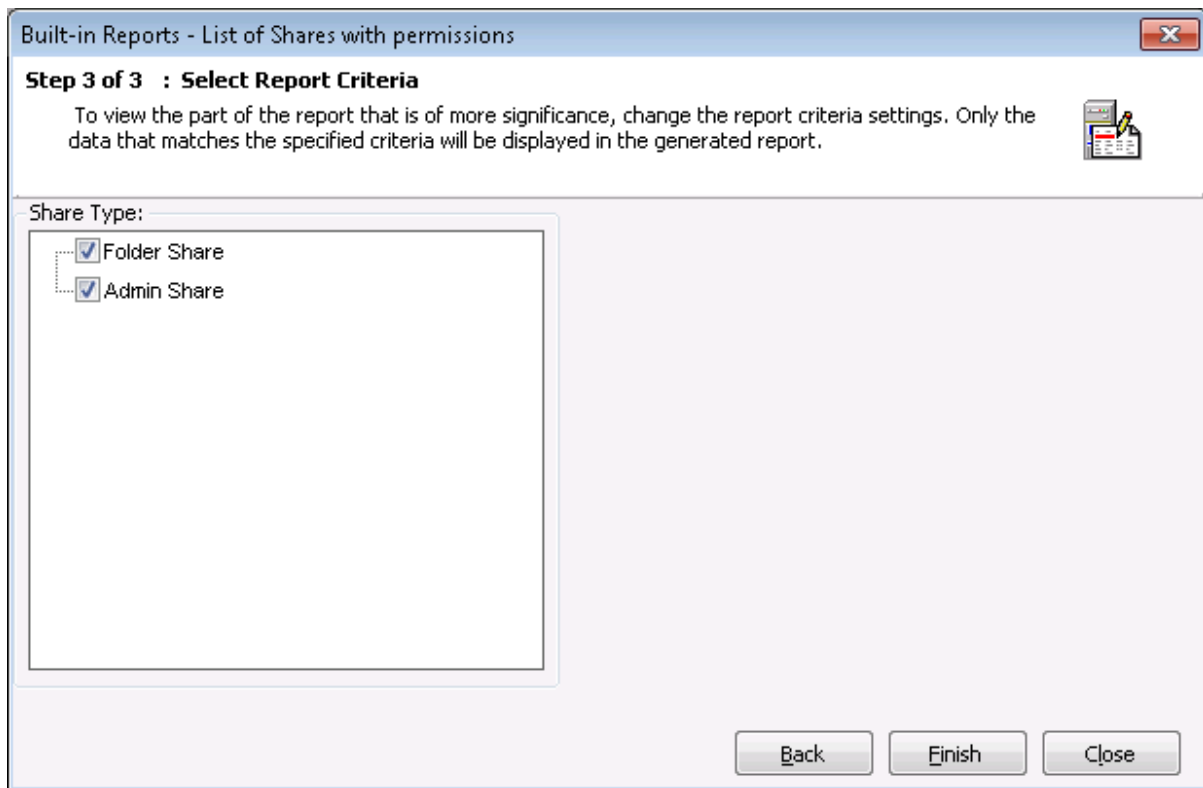
The default option selected is All Domains, for all the reports.



**Click Next** to proceed to the next step.

### Step 3: Select Report Criteria

To view the part of the report that is of more significance, change the report criteria settings. Only the data that matches the specified criteria will be displayed in the generated report.



Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:

**Built-in Reports - List of Shares with permissions**

Refresh Data Export E-mail Find

Report Details

Report Name: List of Shares with permissions

Generated on: 30 Dec, 2014, 11:04:16 AM Status: Success

Domain/Server	Share Name	Path	User Name	Security	Maximum Uses	Comment
RD40	ADMIN\$	C:\Windows		Admin Share	Unlimited	Remote Admin
	C\$	C:\		Admin Share	Unlimited	Default share
	D\$	D:\		Admin Share	Unlimited	Default share
	Folder	D:\Folder	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		D:\Folder	Everyone	Allow - Full Control	Unlimited	
	latest setup	D:\latest setup	BUILTIN\Administrators	Allow - Full Control	Unlimited	Latest Setup Share
		D:\latest setup	Everyone	Allow - Full Control	Unlimited	Latest Setup Share
	Module	D:\Module	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		D:\Module	Everyone	Allow - Full Control	Unlimited	
	NETLOGON	C:\Windows\SYSVOL\sysvol\Voyager.local\SCRIPTS	Everyone	Allow - Read	Unlimited	Logon server share
		C:\Windows\SYSVOL\sysvol\Voyager.local\SCRIPTS	BUILTIN\Administrators	Allow - Full Control	Unlimited	Logon server share
	NTFS Share	C:\NTFS Test Folder\NTFS Share	VOYAGER\adminduser3	Allow - Full Control	Unlimited	
	NTFS Test Folder	C:\NTFS Test Folder	Everyone	Allow - Read	Unlimited	
	Share	D:\Share	Everyone	Allow - Full Control	Unlimited	
		D:\Share	BUILTIN\Administrators	Allow - Full Control	Unlimited	
	share22	D:\share22	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		D:\share22	Everyone	Allow - Full Control	Unlimited	
	SPListX Target	D:\SPListX Target	BUILTIN\Administrators	Allow - Full Control	Unlimited	
		D:\SPListX Target	Everyone	Allow - Full Control	Unlimited	

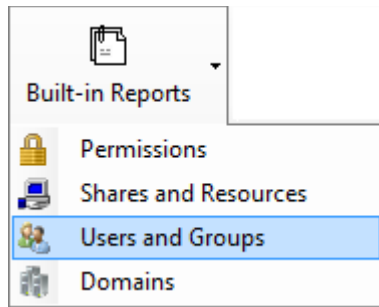
### List of Reports:

Report Name	Description
List of Shares	Reports all the shares and their properties excluding the permission information.
List of Shares with Permissions	Reports all the shares and their properties including the permission information.

### 4.4 How to View Built-in Reports for Users and Groups?

#### Users and Groups Reports

The Users and Groups reports, contains reports that can be generated against domain(s) and specific sever(s) as well.

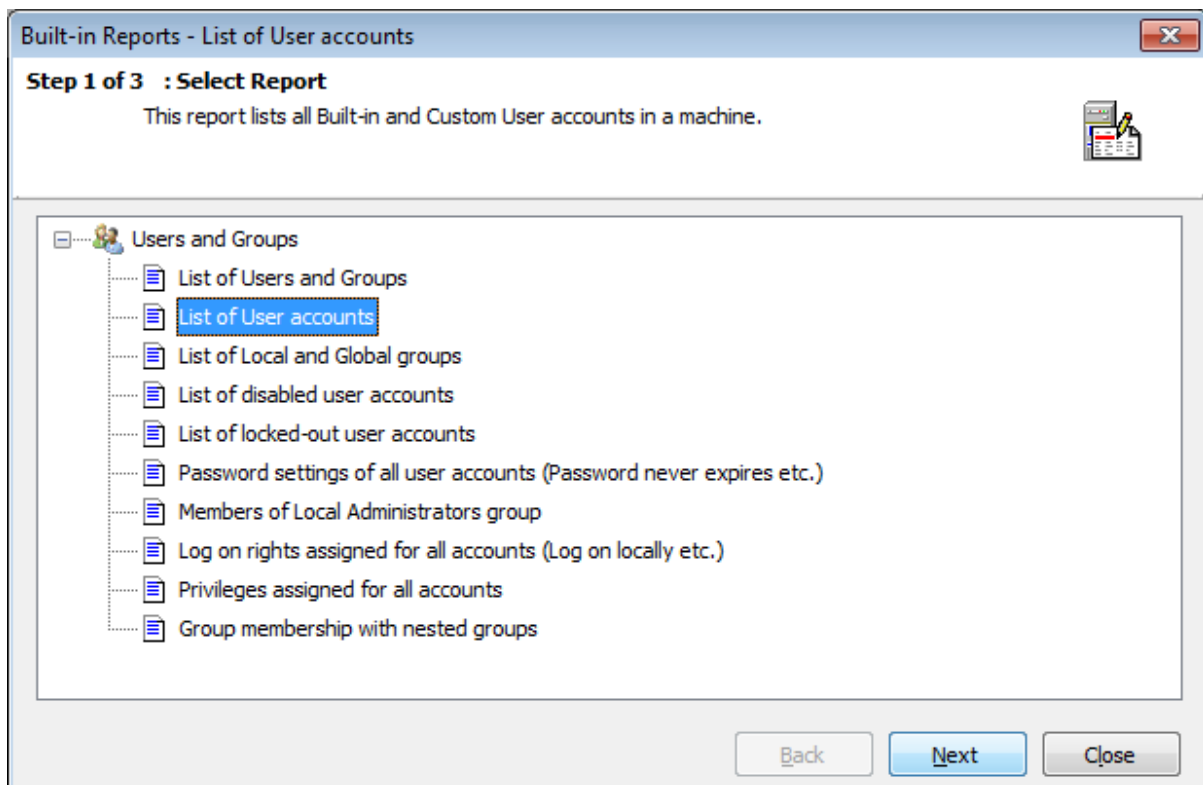


Click on button under Built-in Reports in button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

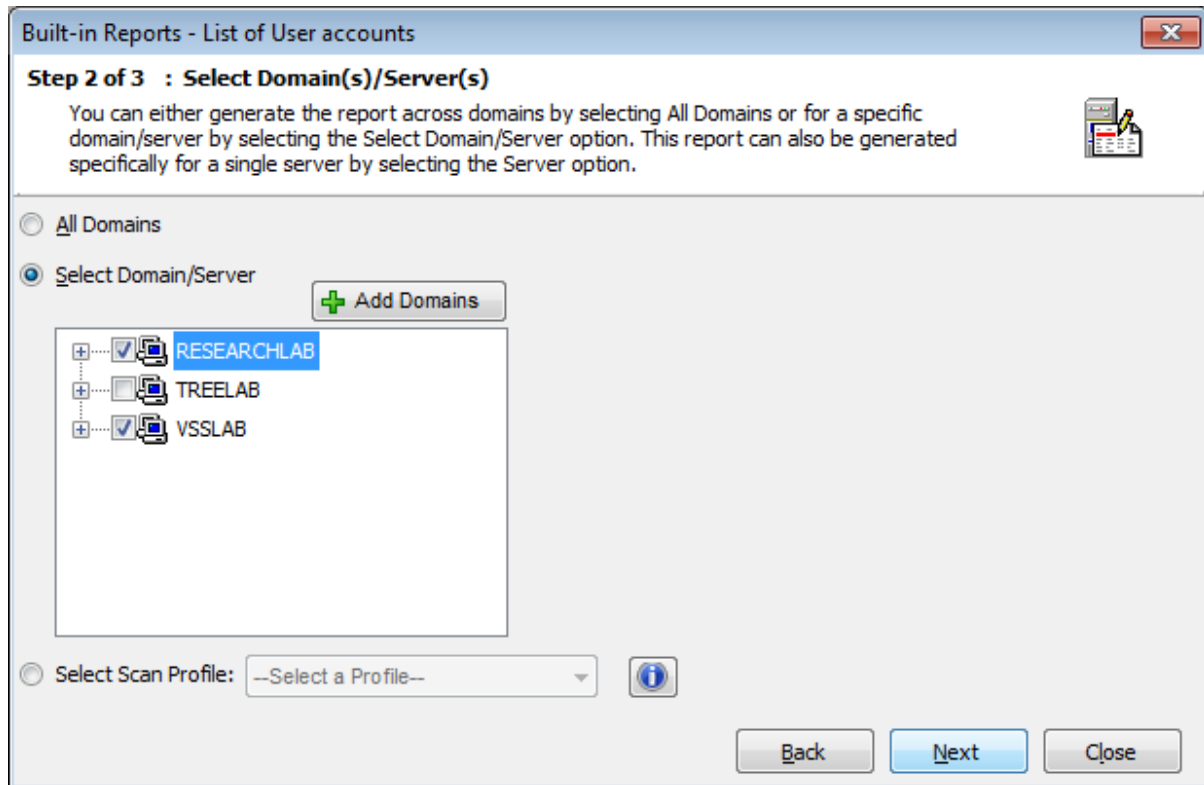
Select the report to be generated. Only one report can be generated at a time. Click **Next** to proceed to the next step.



### Step 2: Select Domain (s) / Server(s)

Select the server(s)/Domain (s) or Select a Scan Profile, for which the report needs to be generated.

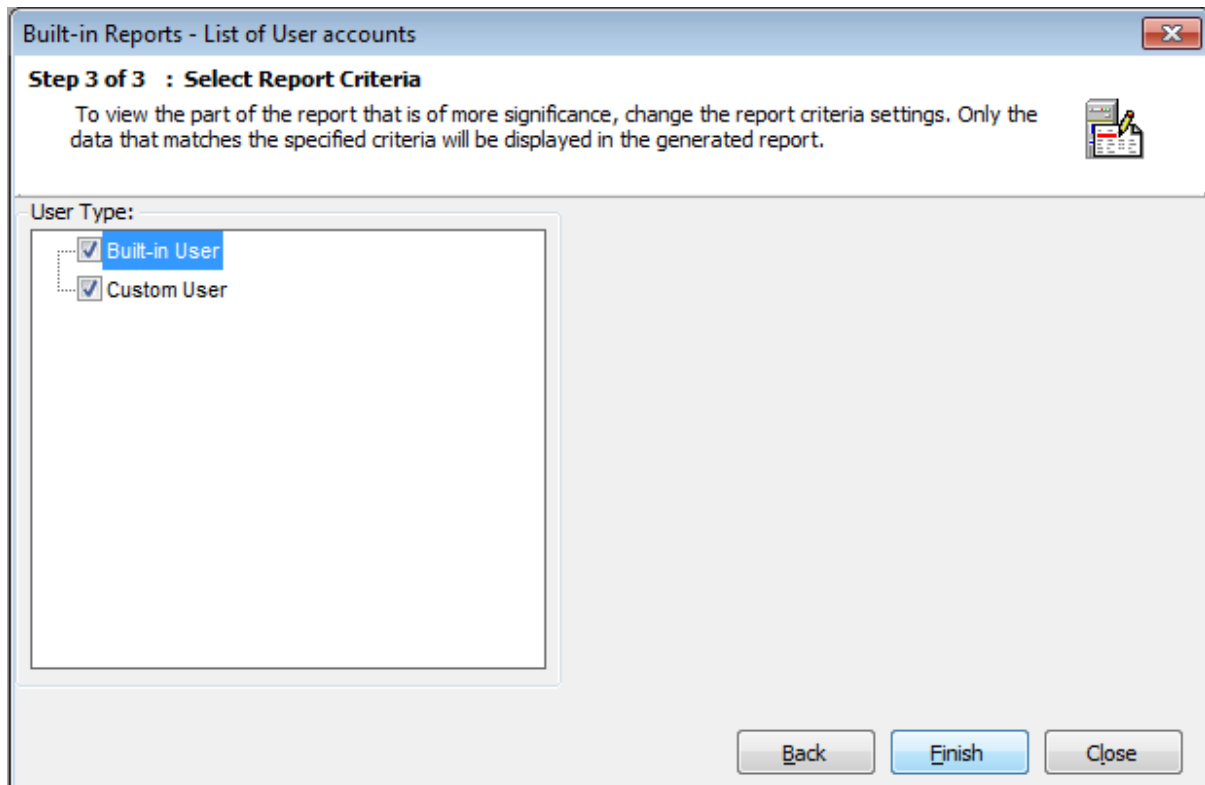
The default option selected is All Domains, for all the reports.



Click **Next** to proceed to the next step.

### Step 3: Select Report Criteria

To view the part of the report that is of more significance, change the report criteria settings. Only the data that matches the specified criteria will be displayed in the generated report.



Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:

**Built-in Reports - List of User accounts**

Refresh Data Export E-mail Find

Report Details

Report Name: List of User accounts

	Domain/Server	User Name	Description
▶	RESEARCHLAB\RD30	Administrator	Built-in User
		Guest	Built-in User
		krbtgt	Custom User
		adminuser 1	Custom User
		alex	Custom User
		andy	Custom User
		bennoit	Custom User
		david	Custom User
		esan	Custom User
		gavin	Custom User
		ilia	Custom User

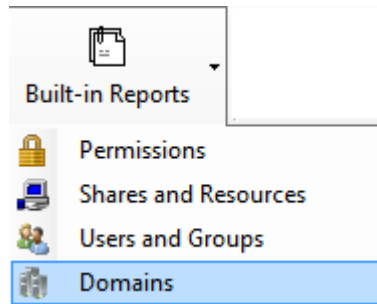
**List of Reports:**

<b>Report Name</b>	<b>Description</b>
List of Users and Groups	Reports both the user and group accounts.
List of User accounts	Reports only the user accounts. This report lists both built-in and custom users.
List of Local and Global groups	Reports only the group accounts with member information. This report lists all Local groups for all the servers and also the Global groups if the server happens to be a PDC.
List of disabled user accounts	Reports only the user accounts, both built-in and custom, that have been disabled and/or otherwise.
List of locked-out user accounts	Reports only the user accounts, both built-in and custom, that have been locked out and/or otherwise.
Password settings of all user accounts (Password never expires etc.)	Reports password settings of the users' viz., Password never expires, User must change password at next logon, User cannot change password.
Members of Local Administrators group	Reports user and/or group members for the given group(s).
Log on rights assigned for all accounts (Log on locally etc.)	Reports user and/or group accounts having the logon rights viz., Log on locally, Log on as a service, Log on as a batch job.
Privileges assigned for all accounts	Reports the assigned privileges for both user and group accounts.
Group membership with nested groups	Reports all the members of a group along with their sub-group members.

### 4.5 How to View Built-in Reports for Domains?

#### Domains Reports

Domain Reports are generated across for the entire domain.

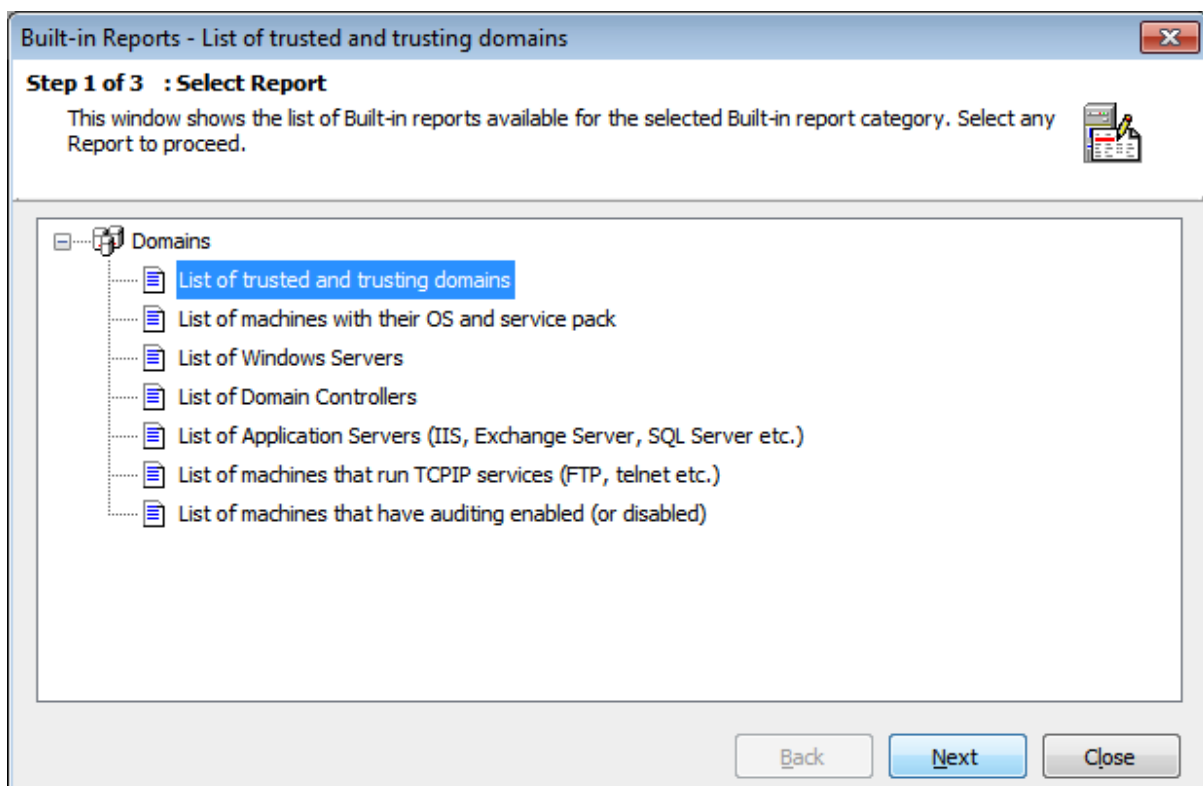


Click on Domains button under Built-in Reports in button in the toolbar.

The Built-in Reports window with the list of reports will be displayed as shown below:

#### Step 1: Report Selection

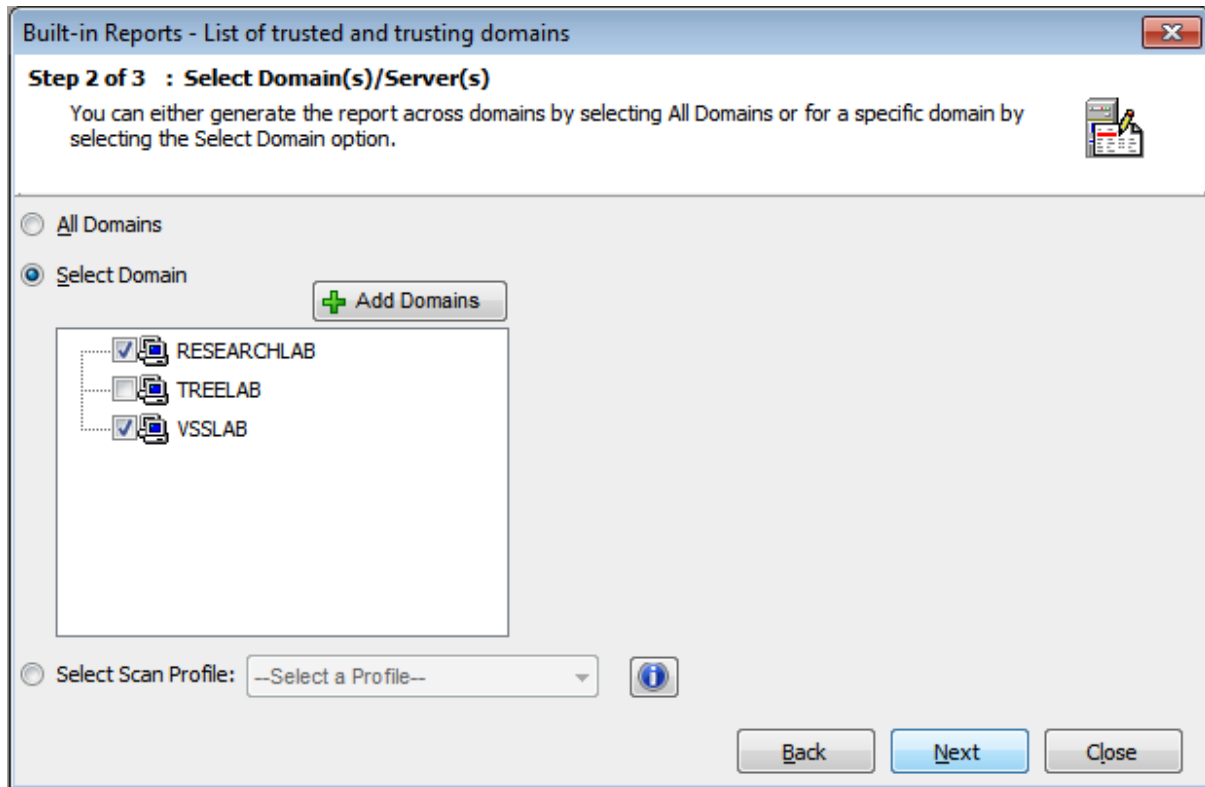
Select the report to be generated. Only one report can be generated at a time. Click **Next** to proceed to the next step.



### Step 2: Select Domain (s) / Server(s)

Select the server(s)/Domain (s) or Select a Scan Profile, for which the report needs to be generated.

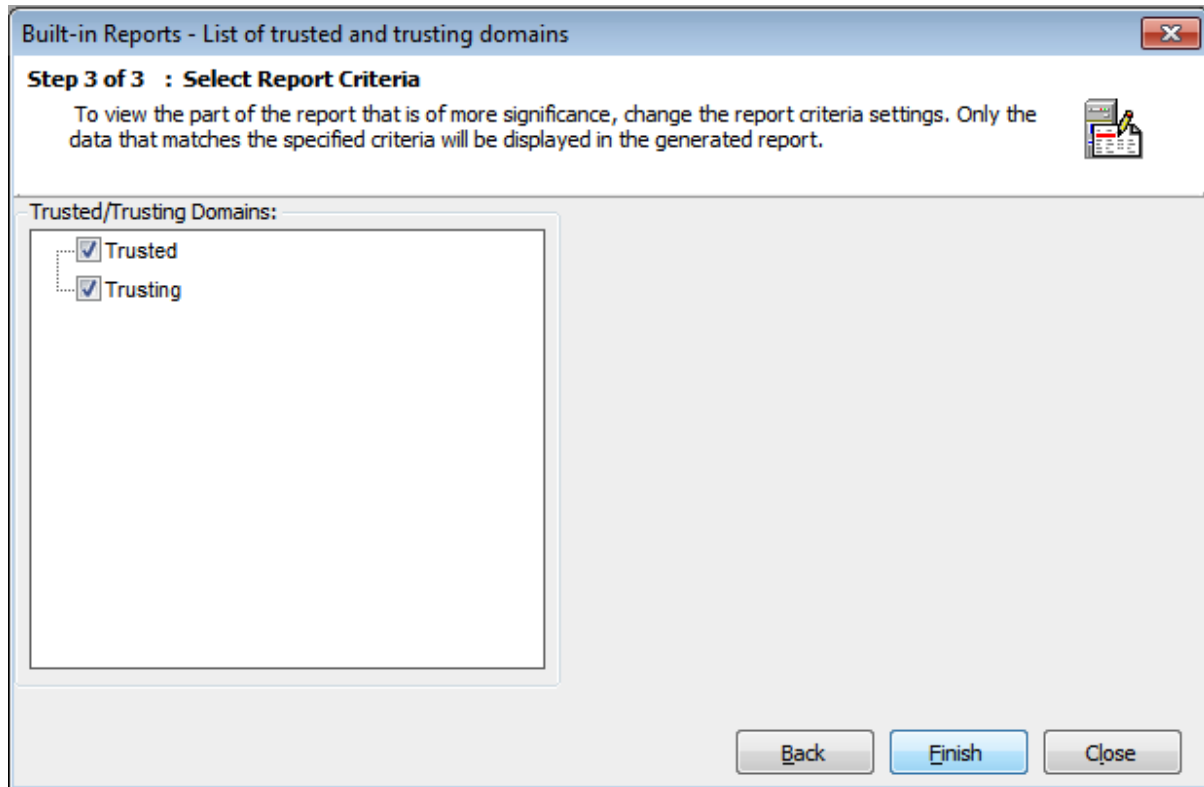
The default option selected is All Domains, for all the reports.



Click **Next** to proceed to the next step.

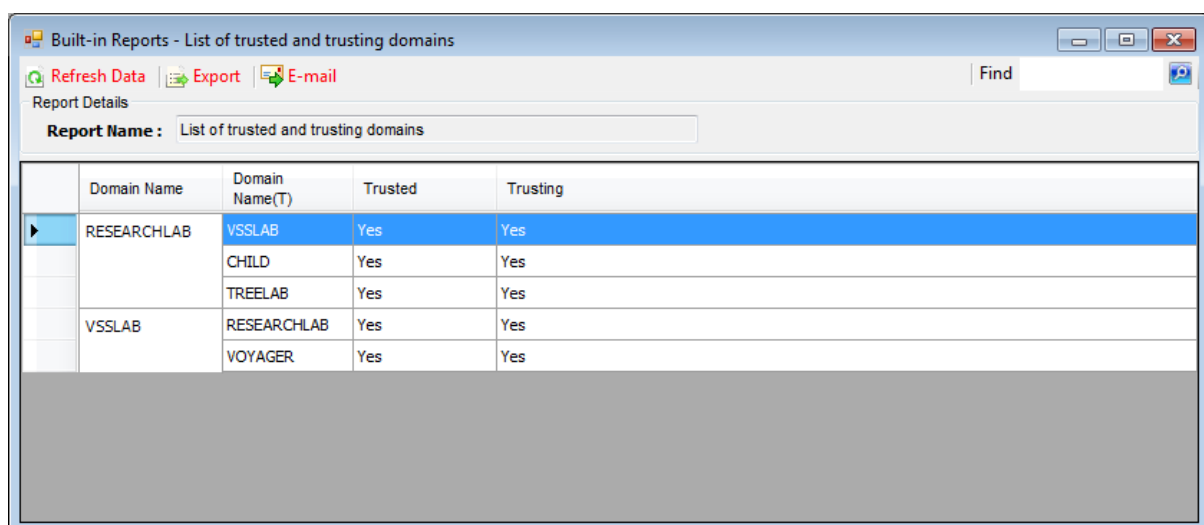
### Step 3: Select Report Criteria

To view the part of the report that is of more significance, change the report criteria settings. Only the data that matches the specified criteria will be displayed in the generated report.



Click **Finish** to generate the selected report.

After the data collection process is complete, the report would be generated in a report window as shown below:



**List of Reports:**

<b>Report Name</b>	<b>Description</b>
List of trusted and trusting domains	Reports the trusted and/or trusting domains.
List of machines with their OS and service pack	Reports the configuration information of all the servers in the domain(s).
List of Windows Servers	Reports the OS installed in all the servers in the domain(s).
List of Domain Controllers	Reports the Primary and/or Backup Domain Controllers in the domain(s).
List of Application servers (IIS, Exchange Server, SQL Server etc.)	Reports servers running IIS and/or Exchange Server and/or SQL Server in the domain(s).
List of machines that run TCPIP services (FTP, telnet etc.)	Reports Servers running network services viz., TCP/IP, FTP, and Telnet in the domain.
List of machines that have auditing enabled (or disabled)	Reports the Auditing status of servers in the domain(s)...



## 5 System Information

---

### 5.1 About System Info

---

This page covers the following topics:

- **Introduction**
- **Prerequisites and Initial Configuration**
- **System Info reports**

#### **Introduction**

The System Info feature provides significant hardware and software inventory-based reports that can be generated across domains. Further, all the System Info reports can also be scheduled for off-line generation using the Power Export tool.

Please be aware that the System Info feature uses WMI (Windows Management Instrumentation) to collect report data. Hence, all System Info reports require WMI to be installed and enabled on the source computer and target computers. For more information refer to "Prerequisites and Initial Configuration" section.

#### **Prerequisites and Initial Configuration**

The System Info feature uses WMI to collect report data. WMI uses DCOM protocol and is affected by Windows Firewall and DCOM security settings. In order to generate System Info reports both Windows Firewall and DCOM must be properly configured. Windows Firewall and DCOM, when not properly configured on your remote computers, can cause errors such as an "RPC Server Unavailable" error or an "Access is denied" error. Also, ensure that the current user context or specified user context, under which the application runs, is a local administrator on target computers.

In order to generate System Info reports ensure the following settings are set appropriately:

- Remote Administration setting is enabled on Windows Firewall. By default, Windows Firewall blocks all unsolicited incoming traffic except for Group Policy. This is a

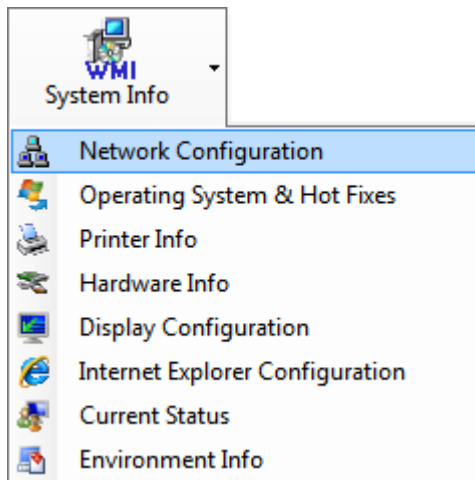
common issue you might encounter while generating System Info reports. To resolve this issue, you need to enable the remote administration setting on the Firewall. For more information see Technical FAQ #19. For more information about configuring the Windows Firewall connections with a script, see <http://www.microsoft.com/technet/community/columns/scripts/sg1104.msp#EJAA>

- WMI is installed and the Startup Type for WMI service is set to Automatic and the service is running under Local System Account.
- DCOM is enabled and ensure that security settings for DCOM allow remote connections
  - 1) Run the DCOM Configuration Utility (dcomcnfg.exe)
  - 2) In the **Component Services** dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and click **Properties**
  - 3) In the **My Computer Properties** dialog box, click the **Default Properties** tab
  - 4) **Select Enable Distributed COM on this computer**
  - 5) The **Default Authentication Level** is set to **Connect** and the **Default Impersonation Level** is set to Identify in Windows XP and later operating systems. For Windows NT, however, the **Default Authentication Level** is set to **Connect** and **Default Impersonation Level is set to Impersonate**
  - 6) The default DCOM security settings for **Access Permissions** and **Launch and Activation Permissions** in the **COM Security** tab in the **My Computer Properties** dialog includes at least INTERACTIVE, SYSTEM and Administrators
- In Windows XP SP2 and later operating systems the SERVICE account is granted **Impersonate a client after authentication** right under **User Rights Assignment** under **Local Policies**
- The **Data Execution Prevention** in Windows XP SP2 and Windows 2003 SP1 is enabled for essential windows programs only

**System Info Reports:** The System Info feature provides reports on the following resource categories:

- **Network Configuration**
- **Operating System & Hot Fixes**
- **Printer Info**
- **Hardware Info**
- **Display Configuration**
- **Internet Explorer Configuration**
- **Current Status**
- **Environment Info**

### 5.2 How to View Network Configuration Reports?



Click on **Network Configuration** under System Info button to view Network Configuration information available under each tab as listed below.


**NOTE:** For information on restricting the domain scan for generating Network Configuration reports, please see How to scan specific servers in a domain?

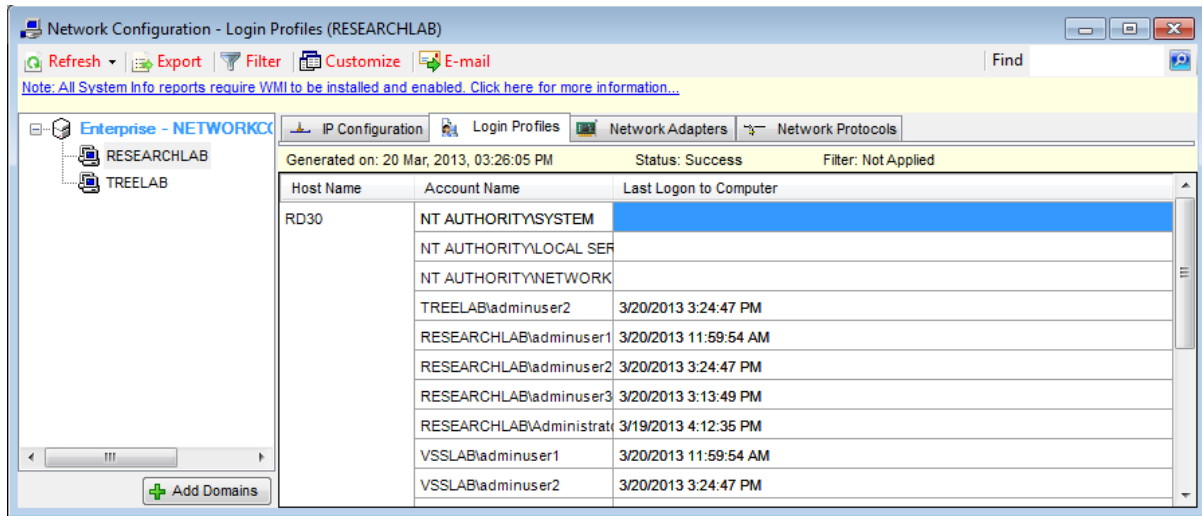
Click **IP Configuration** tab to view the following information: **Network Adapter Name, IP Address, Subnet Mask, DHCP Enabled, Default Gateway, DHCP Server, DNS Servers, DNS Domain DHCP Lease Obtained, and DHCP Lease Expires.**

A screenshot of a window titled 'Network Configuration - IP Configuration (RESEARCHLAB)'. The window has a toolbar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail' buttons, and a 'Find' text box. Below the toolbar is a note: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The main area shows a tree view on the left with 'Enterprise - NETWORKCX' expanded, containing 'RESEARCHLAB' and 'TREELAB'. The right pane shows the 'IP Configuration' tab selected. At the top of the right pane, it says 'Generated on: 20 Mar, 2013, 03:21:21 PM', 'Status: Success', and 'Filter: Not Applied'. Below this is a table with the following data:

Host Name	Network Adapter Name	IP Address	Subnet Mask	DHCP Enabled	Default Gateway	DHCP Server
RD30	[00000012] Microsc	10.10.10.30	255.0.0.0	Yes	10.10.10.6	10.10.10.1
				Yes	10.10.10.1	10.10.10.1
						10.10.10.1
RD11	[00000012] Microsc	10.10.10.83	255.0.0.0	Yes	10.10.10.1	10.10.10.1
				Yes		10.10.10.1


## CHAPTER 4 - System Information

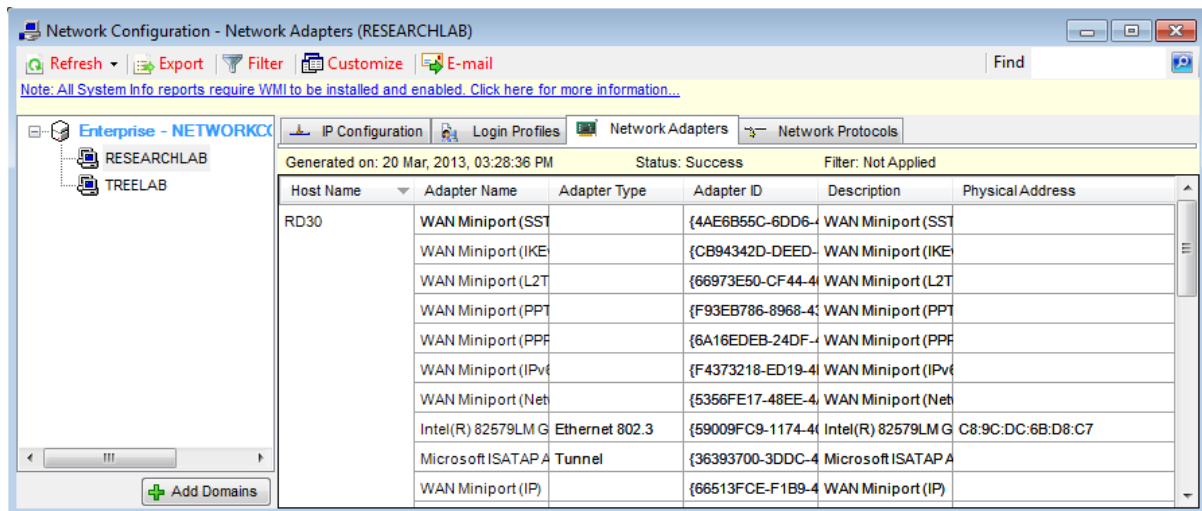
Click  **Login Profiles** tab to view the following information: **Host Name, Account Name, and Last Logon to Computer.**



The screenshot shows the 'Login Profiles' tab in the Network Configuration window. The left pane shows a tree view with 'Enterprise - NETWORKC' and 'TREELAB'. The main pane displays a table of login profiles for host 'RD30'. The table has columns: Host Name, Account Name, and Last Logon to Computer. The data is as follows:

Host Name	Account Name	Last Logon to Computer
RD30	NT AUTHORITY\SYSTEM	
	NT AUTHORITY\LOCAL SERVICE	
	NT AUTHORITY\NETWORK SERVICE	
	TREELAB\administrator2	3/20/2013 3:24:47 PM
	RESEARCHLAB\administrator1	3/20/2013 11:59:54 AM
	RESEARCHLAB\administrator2	3/20/2013 3:24:47 PM
	RESEARCHLAB\administrator3	3/20/2013 3:13:49 PM
	RESEARCHLAB\Administrator	3/19/2013 4:12:35 PM
	VSSLAB\administrator1	3/20/2013 11:59:54 AM
	VSSLAB\administrator2	3/20/2013 3:24:47 PM


Click  **Network Adapters** tab to view the following information: **Host Name, Adapter Name, Adapter Type, Adapter ID, Description, and Physical Address.**

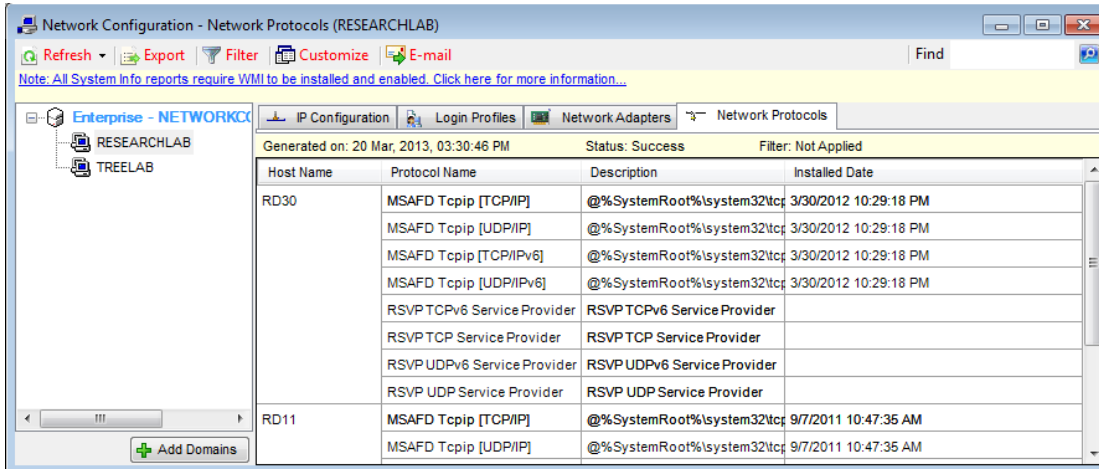


The screenshot shows the 'Network Adapters' tab in the Network Configuration window. The left pane shows a tree view with 'Enterprise - NETWORKC' and 'TREELAB'. The main pane displays a table of network adapters for host 'RD30'. The table has columns: Host Name, Adapter Name, Adapter Type, Adapter ID, Description, and Physical Address. The data is as follows:

Host Name	Adapter Name	Adapter Type	Adapter ID	Description	Physical Address
RD30	WAN Miniport (SSTAP)		{4AE6B55C-6DD6-4...	WAN Miniport (SSTAP)	
	WAN Miniport (IKEv2)		{CB94342D-DEED-4...	WAN Miniport (IKEv2)	
	WAN Miniport (L2TP)		{66973E50-CF44-4...	WAN Miniport (L2TP)	
	WAN Miniport (PPTP)		{F93EB786-8968-4...	WAN Miniport (PPTP)	
	WAN Miniport (PPPoE)		{6A16EDEB-24DF-4...	WAN Miniport (PPPoE)	
	WAN Miniport (IPv6)		{F4373218-ED19-4...	WAN Miniport (IPv6)	
	WAN Miniport (Net)		{5356FE17-48EE-4...	WAN Miniport (Net)	
	Intel(R) 82579LM G	Ethernet 802.3	{59009FC9-1174-4...	Intel(R) 82579LM G	C8:9C:DC:6B:D8:C7
	Microsoft ISATAP A	Tunnel	{36393700-3DDC-4...	Microsoft ISATAP A	
	WAN Miniport (IP)		{66513FCE-F1B9-4...	WAN Miniport (IP)	

## CHAPTER 4 - System Information

Click  **Network Protocols** tab to view the following information: **Host Name, Protocol Name, Description, and Installed Date.**



Network Configuration - Network Protocols (RESEARCHLAB)

Refresh Export Filter Customize E-mail Find

Note: All System Info reports require WMI to be installed and enabled. Click here for more information...

Enterprise - NETWORK RESEARCHLAB TREELAB

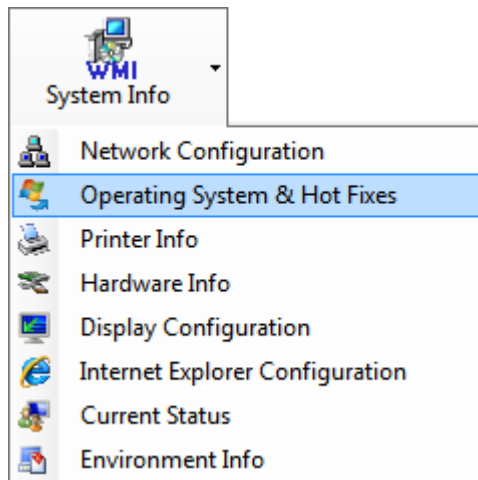
IP Configuration Login Profiles Network Adapters **Network Protocols**


Generated on: 20 Mar, 2013, 03:30:46 PM Status: Success Filter: Not Applied

Host Name	Protocol Name	Description	Installed Date
RD30	MSAFD Tcpip [TCP/IP]	@%SystemRoot%\system32\tcpip	3/30/2012 10:29:18 PM
	MSAFD Tcpip [UDP/IP]	@%SystemRoot%\system32\udpip	3/30/2012 10:29:18 PM
	MSAFD Tcpip [TCP/IPv6]	@%SystemRoot%\system32\tcpip	3/30/2012 10:29:18 PM
	MSAFD Tcpip [UDP/IPv6]	@%SystemRoot%\system32\udpip	3/30/2012 10:29:18 PM
	RSVP TCPv6 Service Provider	RSVP TCPv6 Service Provider	
	RSVP TCP Service Provider	RSVP TCP Service Provider	
	RSVP UDPv6 Service Provider	RSVP UDPv6 Service Provider	
	RSVP UDP Service Provider	RSVP UDP Service Provider	
RD11	MSAFD Tcpip [TCP/IP]	@%SystemRoot%\system32\tcpip	9/7/2011 10:47:35 AM
	MSAFD Tcpip [UDP/IP]	@%SystemRoot%\system32\udpip	9/7/2011 10:47:35 AM


Add Domains

### 5.3 How to View Operating System & Hot Fixes Reports?



Click on  under System Info button to view OS and Hot Fixes information available under each tab as listed below.


**NOTE:** For information on restricting the domain scan for generating Operating System and Hot Fixes reports, please see How to scan specific servers in a domain?

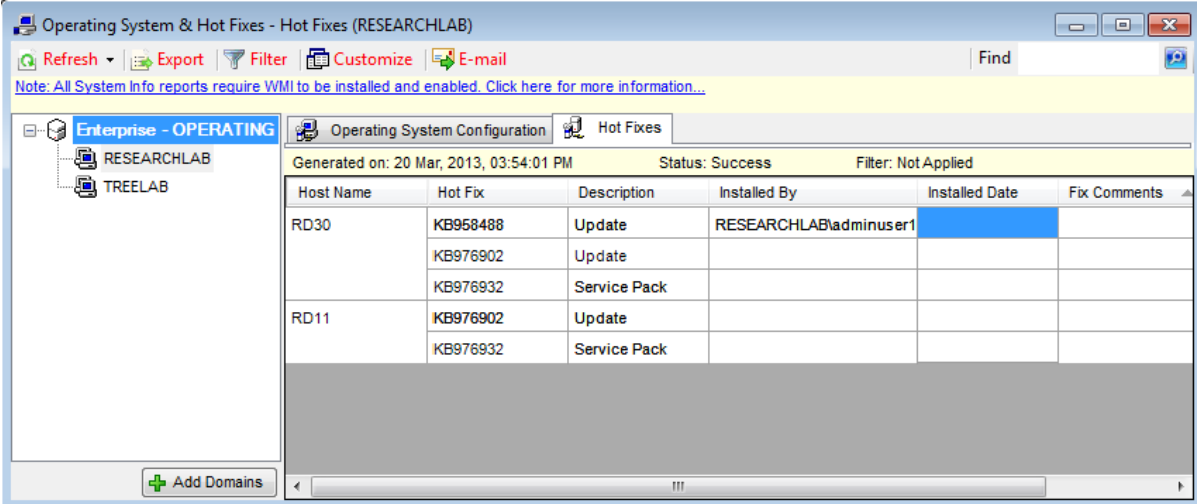
Click  Operating System Configuration tab to view the following information: **Host Name, Operating System, Service Pack, Version, Product ID, Build Type, Total Virtual Memory (MB), Installed Date, Time Zone, and Page File Location(s).**

A screenshot of the 'Operating System & Hot Fixes - Operating System Configuration (RESEARCHLAB)' window. The window has a menu bar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail'. Below the menu bar is a note: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The main area has two tabs: 'Operating System Configuration' (selected) and 'Hot Fixes'. The 'Operating System Configuration' tab shows a table with columns: Host Name, Operating System, Service Pack, Version, Product ID, and Build Type. The table contains two rows of data: RD30 and RD11. The 'Enterprise - OPERATING' tree on the left shows 'RESEARCHLAB' and 'TREELAB'. The 'Add Domains' button is at the bottom left.

Host Name	Operating System	Service Pack	Version	Product ID	Build Type
RD30	Microsoft Windows Server 2008 R2 Enterprise	Service Pack 1	6.1.7601	55041-628-5052896-8	Multiprocessor
RD11	Microsoft Windows Server 2008 R2 Standard	Service Pack 1	6.1.7601	55041-628-5052896-8	Multiprocessor

## CHAPTER 4 - System Information

Click  tab to view the following information: **Host Name, Hot Fix, Description, Installed By, Installed Date, Fix Comments, and Service Pack.**



Operating System & Hot Fixes - Hot Fixes (RESEARCHLAB)

Refresh Export Filter Customize E-mail Find

Note: All System Info reports require WMI to be installed and enabled. [Click here for more information...](#)

Enterprise - OPERATING

RESEARCHLAB

TREELAB

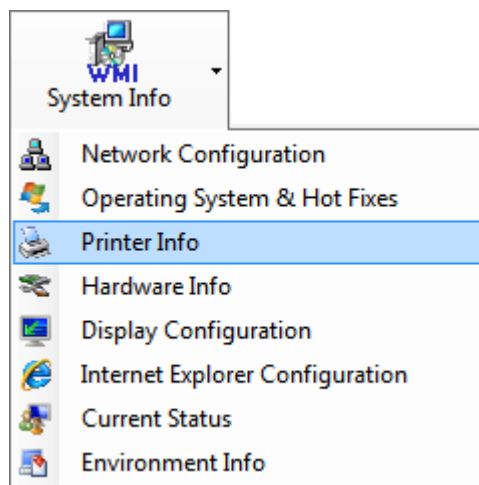
Operating System Configuration Hot Fixes


Generated on: 20 Mar, 2013, 03:54:01 PM Status: Success Filter: Not Applied

Host Name	Hot Fix	Description	Installed By	Installed Date	Fix Comments
RD30	KB958488	Update	RESEARCHLAB\adminuser1		
	KB976902	Update			
	KB976932	Service Pack			
RD11	KB976902	Update			
	KB976932	Service Pack			

Add Domains

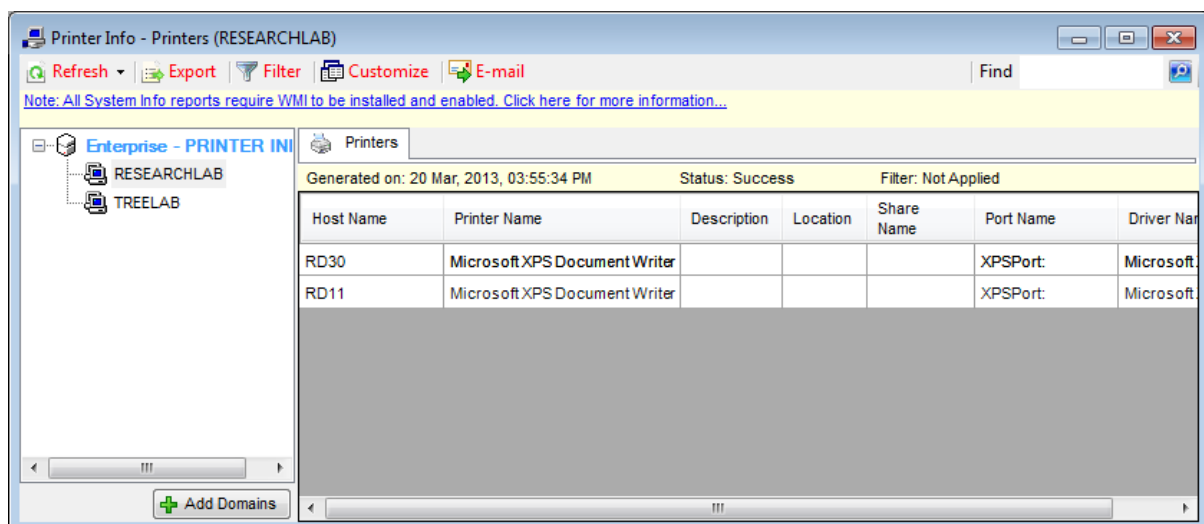
### 5.4 How to View Printer Configuration Reports?



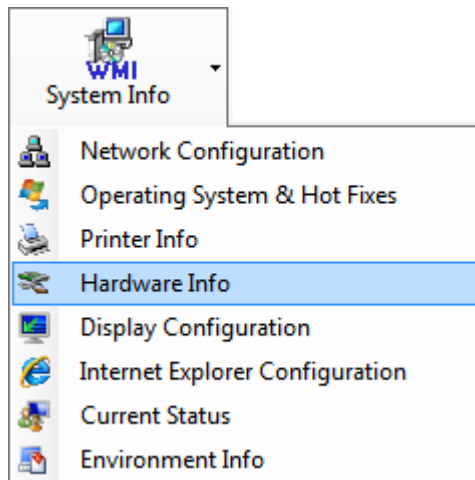
Click on  under System Info button to view Printer Configuration information available under each tab as listed below.

**NOTE:** For information on restricting the domain scan for generating Printer Configuration reports, please see How to scan specific servers in a domain?

Click  Printers tab to view the following information: **Host Name, Printer Name, Description, Location, Share Name, Port Name, and Driver Name.**



### 5.5 How to View Hardware Configuration Reports?



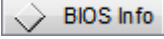
Click on **Hardware Info** under System Info button to view Hardware Configuration information available under each tab as listed.

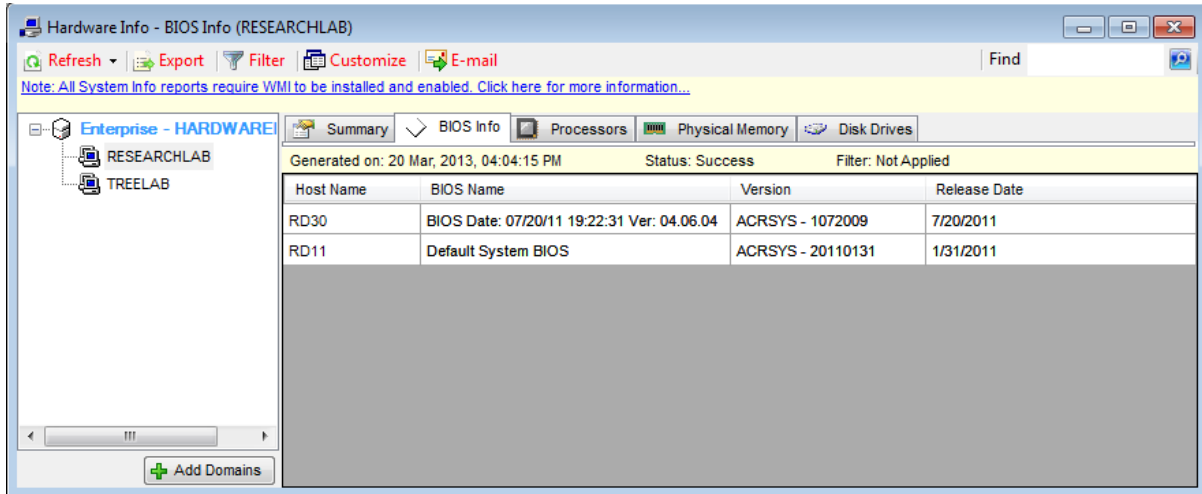
**NOTE:** For information on restricting the domain scan for generating Hardware Configuration reports, please see How to scan specific servers in a domain?

Click **Summary** tab to view the following information: **Host Name, Number of Processor(s), System Model, System Manufacturer, System type, Total Physical Memory (MB), BIOS Version, Boot Device, Windows Directory, System Directory, System Locale, Processor(s), Network Adapter(s), IP Address, Disk(s), Disk Capacity (GB), and Number of Partitions in Disk.**


A screenshot of the 'Hardware Info - Summary' window. The window title is 'Hardware Info - Summary (RESEARCHLAB)'. It has a menu bar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail'. Below the menu bar is a note: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The main area has a tree view on the left showing 'Enterprise - HARDWARE' and 'RESEARCHLAB' with a sub-item 'TREELAB'. The right pane shows the 'Summary' tab selected. It displays a table of system information for two hosts: RD30 and RD11. The table has columns: Host Name, Number of Processor(s), System Model, System Manufacturer, System Type, Total Physical Memory (MB), BIOS Version, and Boot Device. The data for RD30 is: 1 processor, Veriton Series, Acer, x64-based PC, 16204.98 MB, ACRSYS - 1072009, and \Device\Harddis. The data for RD11 is: 1 processor, Veriton Series, Acer, x64-based PC, 7991.12 MB, ACRSYS - 2011013, and \Device\Harddis. The window also shows 'Generated on: 20 Mar, 2013, 04:00:14 PM', 'Status: Success', and 'Filter: Not Applied'.

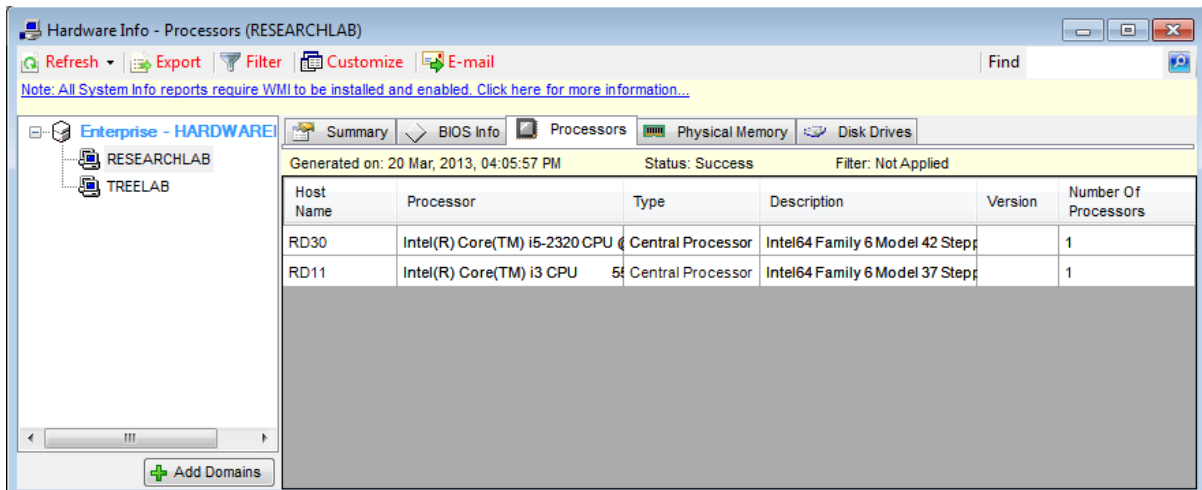
## CHAPTER 4 - System Information

Click  **BIOS Info** tab to view the following information: **Host Name, BIOS Name, Version, and Release Date.**



Host Name	BIOS Name	Version	Release Date
RD30	BIOS Date: 07/20/11 19:22:31 Ver: 04.06.04	ACRSYS - 1072009	7/20/2011
RD11	Default System BIOS	ACRSYS - 20110131	1/31/2011

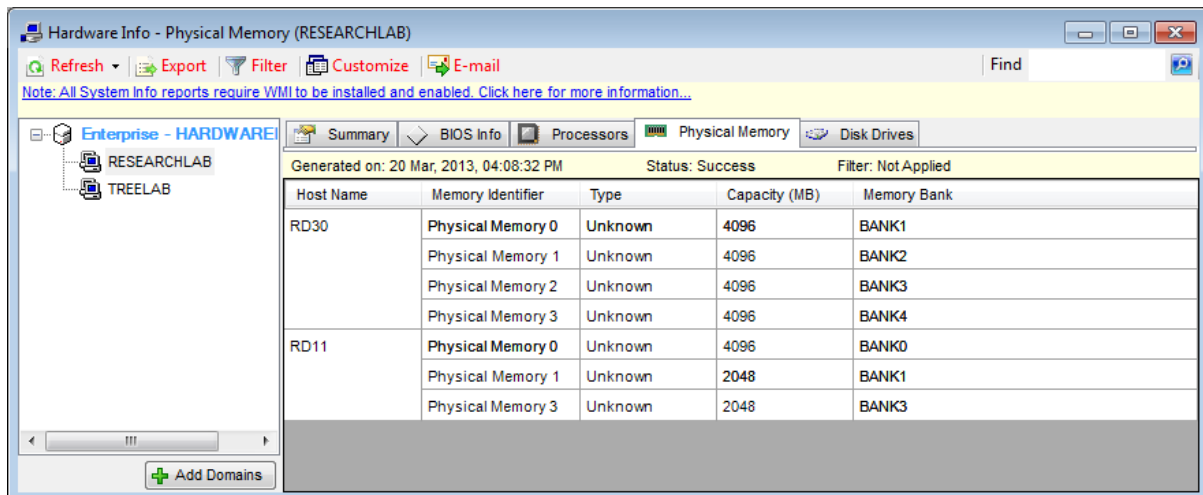
Click  **Processors** tab to view the following information: **Host Name, Processor, Type, Description, Version, and Number of Processors.**




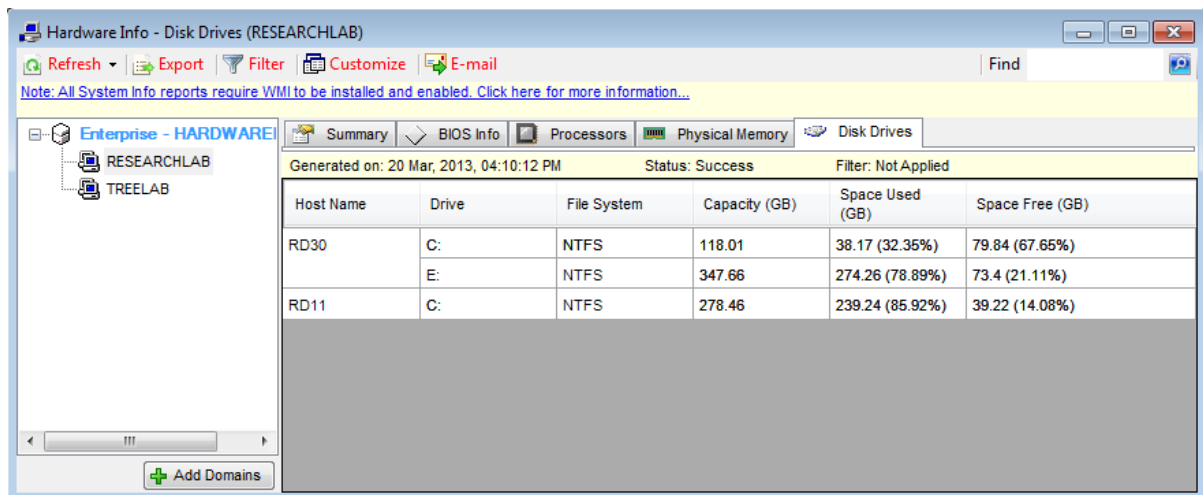
Host Name	Processor	Type	Description	Version	Number Of Processors
RD30	Intel(R) Core(TM) i5-2320 CPU	Central Processor	Intel64 Family 6 Model 42 Stepp		1
RD11	Intel(R) Core(TM) i3 CPU	Central Processor	Intel64 Family 6 Model 37 Stepp		1

Click  **Physical Memory** tab to view the following information: **Host Name, Memory Identifier, Type, Capacity (MB), and Memory Bank.**

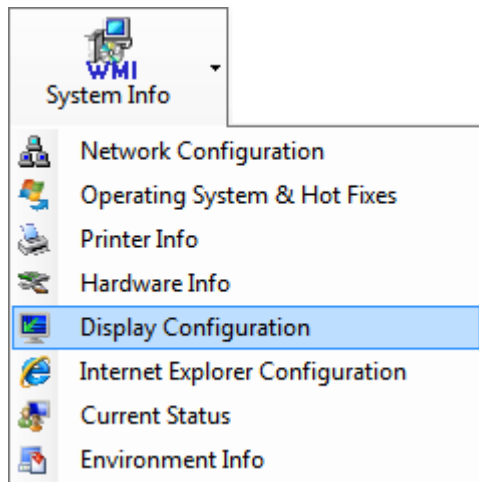
## CHAPTER 4 - System Information




Click  **Disk Drives** tab to view the following information: **Host Name**, **Drive**, **Type**, **Capacity (GB)**, **Space Used (GB)**, and **Space Free (GB)**.




### 5.6 How to View Display Configuration Reports?



Click on  under System Info button to view Display configuration information available under each tab as listed below.

**NOTE:** For information on restricting the domain scan for generating Display configuration reports, please see How to scan specific servers in a domain?

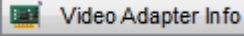
Click  **Monitor Info** tab to view the following information: **Host Name, Monitor Name, DPI Setting, Screen Refresh Rate, Screen Resolution, and Manufacturer.**

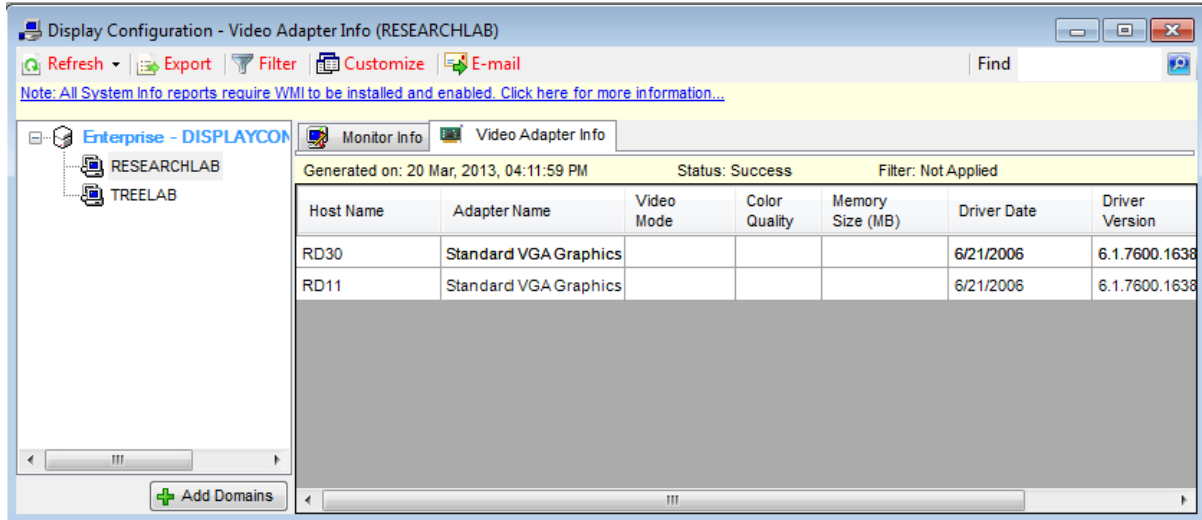
A screenshot of a web application window titled 'Display Configuration - Monitor Info (RESEARCHLAB)'. The window has a toolbar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail' buttons, and a search bar. Below the toolbar is a note: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The main content area has two tabs: 'Monitor Info' (selected) and 'Video Adapter Info'. Below the tabs, it shows 'Generated on: 20 Mar, 2013, 04:11:59 PM', 'Status: Success', and 'Filter: Not Applied'. A table displays the following data:

Host Name	Monitor Name	DPI Setting	Screen Refresh Rate	Screen Resolution	Manufacturer
RD30	Generic PnP Monitor	96 DPI			(Standard monitor types)
RD11	Generic Non-PnP Monitor	96 DPI			(Standard monitor types)

The table is followed by a large grey rectangular area. At the bottom left of the window is an 'Add Domains' button.

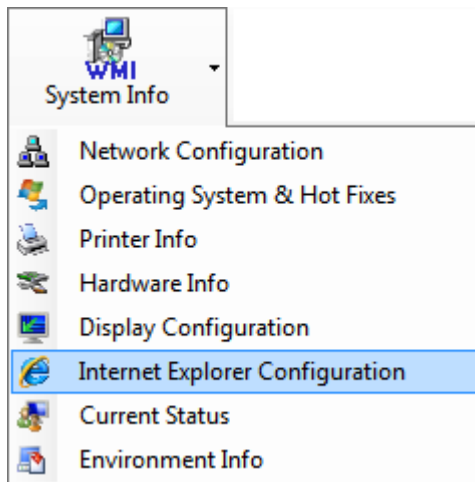
## CHAPTER 4 - System Information


Click  tab to view the following information: **Host Name, Adapter Name, Video Mode, Color Quality, Memory Size (MB), Driver Date, Driver Version, and DAC Type.**




Host Name	Adapter Name	Video Mode	Color Quality	Memory Size (MB)	Driver Date	Driver Version
RD30	Standard VGA Graphics				6/21/2006	6.1.7600.1638
RD11	Standard VGA Graphics				6/21/2006	6.1.7600.1638

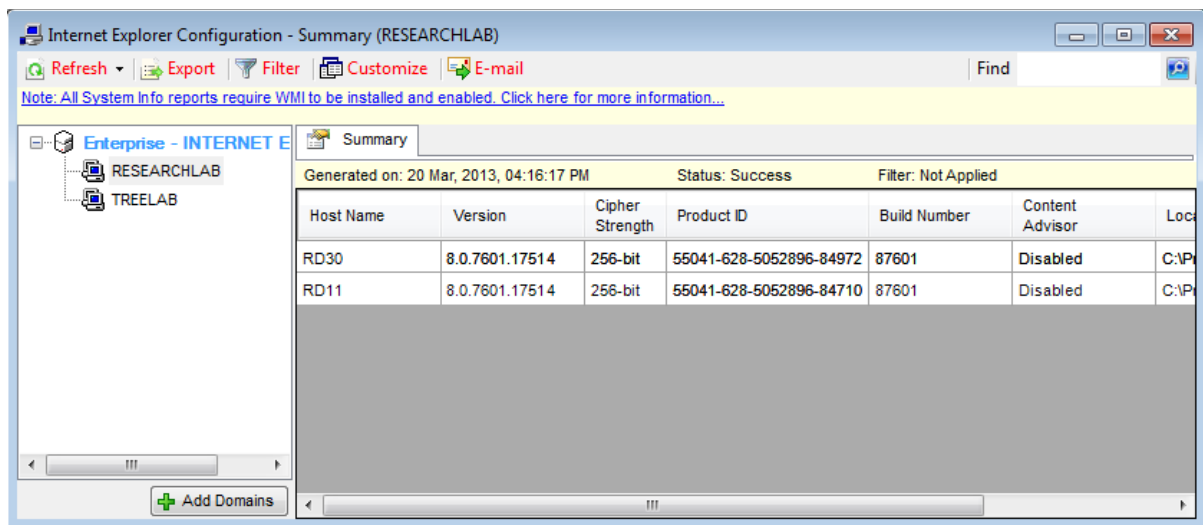
### 5.7 How to View Internet Explorer Configuration Reports?



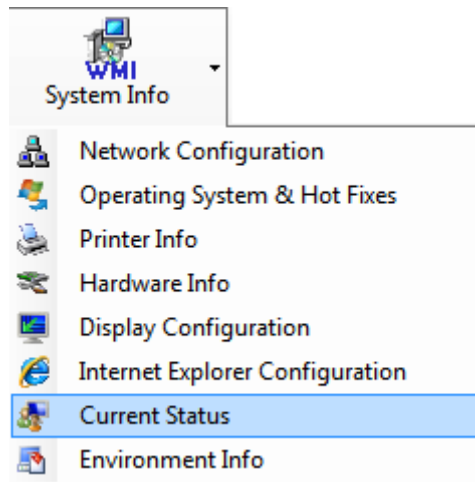
Click on  under System Info button to view Internet Explorer configuration information available under each tab as listed below:

*NOTE:* For information on restricting the domain scan for generating Internet Explorer configuration reports, please see How to scan specific servers in a domain?

Click  Summary tab to view the following information: **Host Name, Version, Cipher Strength, Product ID, Build Number, Content Advisor, Location, and Language.**



### 5.8 How to View Current Status Reports?



Click on **Current Status** under System Info button to view Current Status information available under each tab as listed below:

**NOTE:** For information on restricting the domain scan for generating Current Status reports, please see How to scan specific servers in a domain?

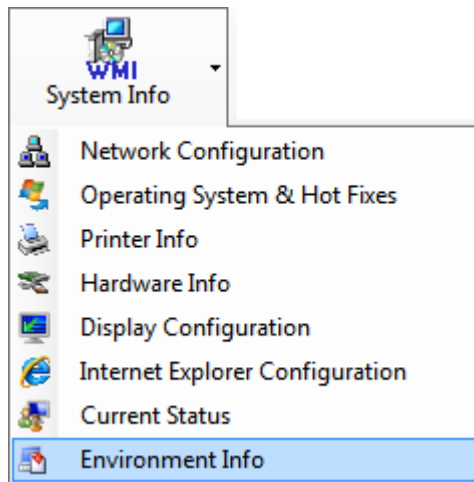
Click **Summary** tab to view the following information: **Host Name, Current Local Time, Last Boot up Time, System Uptime, Percentage of Memory Used, CPU Busy (in percentage), Currently Logged on User, User Logged on Since, Time Elapsed since Logon, and Status Recorded as on.**

**NOTE:** The **Current Local Time** field displays the local time of the target computer (reported in Host Name field). **The Status Recorded as on** field displays the time at which report data was collected for the respective target computer.

A screenshot of the 'Current Status - Summary' application window. The window title is 'Current Status - Summary (RESEARCHLAB)'. It has a toolbar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail' buttons, and a search bar. A note at the top states: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The left sidebar shows a tree view with 'Enterprise - CURRENT S' and sub-items 'RESEARCHLAB' and 'TREELAB'. The main area displays a table of system information for two hosts: RD30 and RD11. The table has columns for Host Name, Current Local Time, Last Boot Up Time, System Uptime, Percentage of Memory Used, CPU Busy (in percentage), Currently Logged on User, and User Log on Since. The data for RD30 shows it was generated on 20 Mar, 2013, at 04:22:00 PM, with 85.75% memory used and 7% CPU busy. The data for RD11 shows it was generated on 3/20/2013 at 4:22:05 PM, with 62.38% memory used and 0% CPU busy. The 'Currently Logged on User' for RD11 is RESEARCHLAB\adminuser2 and RESEARCHLAB\adminuser3.

Host Name	Current Local Time	Last Boot Up Time	System Uptime	Percentage of Memory Used	CPU Busy (in percentage)	Currently Logged on User	User Log on Since
RD30	3/20/2013 4:22:04 PM	3/20/2013 11:28:21	0 Day(s), 4 Hr(s)	85.75	7	No user has logged in	
RD11	3/20/2013 4:22:05 PM	3/20/2013 10:22:16	0 Day(s), 5 Hr(s)	62.38	0	RESEARCHLAB\adminuser2	3/20/2013
						RESEARCHLAB\adminuser3	3/20/2013

### 5.9 How to View Environment Info Reports?



Click on **Environment Info** under System Info button to view Environment Information available under each tab as listed below.

NOTE: For information on restricting the domain scan for generating Environment Info reports, please see How to scan specific servers in a domain?

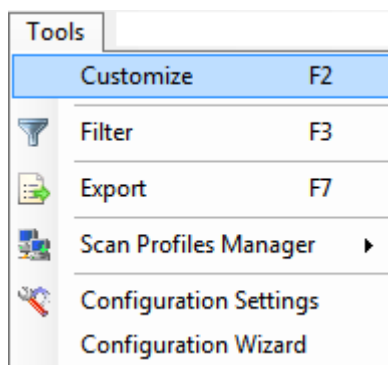
Click **Summary** tab to view the following information: **Host Name, OS, System Drive, System Root, Temp (System), Tmp (System), Path extension, Path, Default User Domain User DNS Domain, Common Program Files, Program Files, All Users APP Data, All User Profile, and Command Prompt Location.**

A screenshot of the 'Environment Info - Summary (RESEARCHLAB)' window. The window has a toolbar with 'Refresh', 'Export', 'Filter', 'Customize', and 'E-mail' buttons. A note at the top states: 'Note: All System Info reports require WMI to be installed and enabled. Click here for more information...'. The left sidebar shows a tree view with 'Enterprise - ENVIRONI', 'RESEARCHLAB', and 'TREELAB'. The main area displays a table of system information for two hosts: RD30 and RD11. The table has columns for Host Name, OS, System Drive, System Root, Temp(System), Tmp(System), Path Extension, and Path. The data for both hosts is identical.

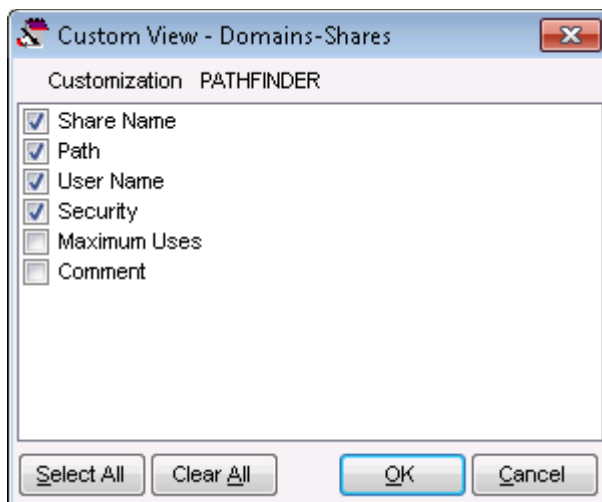
Host Name	OS	System Drive	System Root	Temp(System)	Tmp(System)	Path Extension	Path
RD30	Windows_NT	C:	C:\Windows	C:\Windows\TEMP	C:\Windows\TEMP	.COM;.EXE;.BAT;.C	C:\Windows\ls
RD11	Windows_NT	C:	C:\Windows	C:\Windows\TEMP	C:\Windows\TEMP	.COM;.EXE;.BAT;.C	C:\Windows\ls

## 6 Additional Features

### 6.1 How to customize fields?



Click on **Customize** for customizing the information.



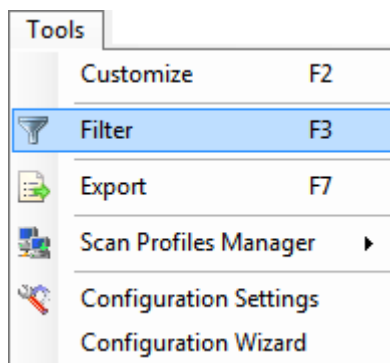
Click **Select All** for selecting all the check boxes.


Click **Clear All** for clearing all the check boxes.

Click **OK** button for confirming the changes.

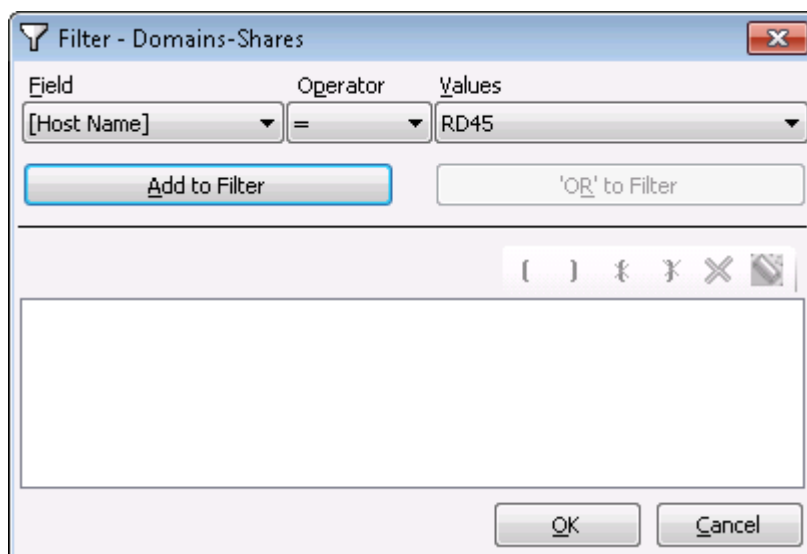
Click **Cancel** button for cancelling the operation.

## 6.2 How to Apply Filters?





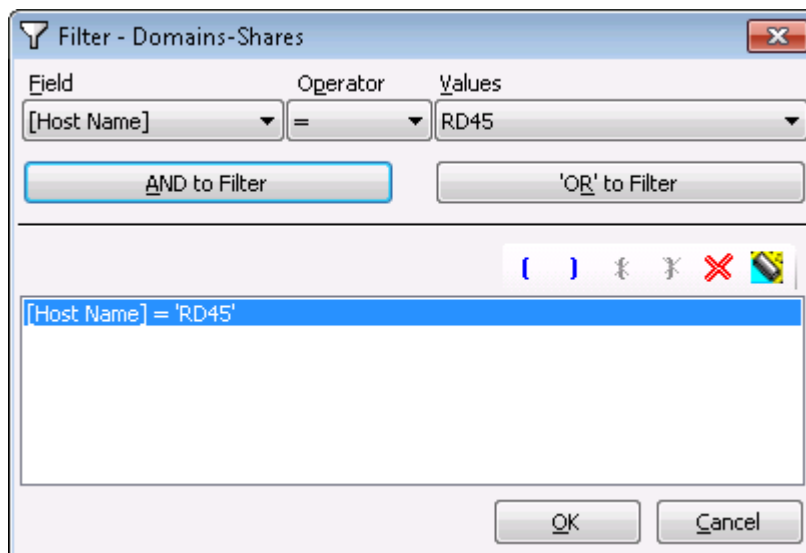
Click  for setting filter options

The **ARKWE Filter** window will be displayed. .










To set a filter condition, follow these steps.

- 1) Click  (Clear All) button and clear the filter.
- 2) **Choose** a field name, an operator and a possible value from the respective dropdown options.
- 3) Click 
- 4) **The Add to Filter will change to AND to Filter. The OR to Filter button will be enabled.** The selected condition will be set as a filter and displayed (as shown below).



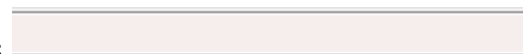
5) Click **OK** to apply the filter.

**NOTE:**

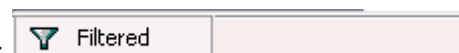
- Use the  ,  and   to build enhanced filter condition as shown below:
- (Field A = Value 1 AND Field B = Value 2) OR (Field C = Value 3 AND Field D = Value 4)
- Use   to remove the parenthesis
- Use  to delete a selected condition.

**The status bar's FILTERED** indicator is used to indicate whether the current data is filtered or not.

For a normal view, the status bar will appear as

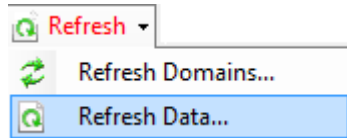


For a filtered view, the status bar will appear as



### 6.3 How to Refresh Data?

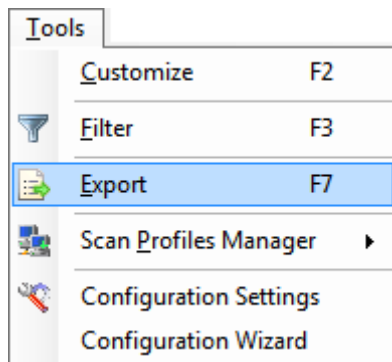
Refresh the current report data to view the latest information from the Domain Controller.



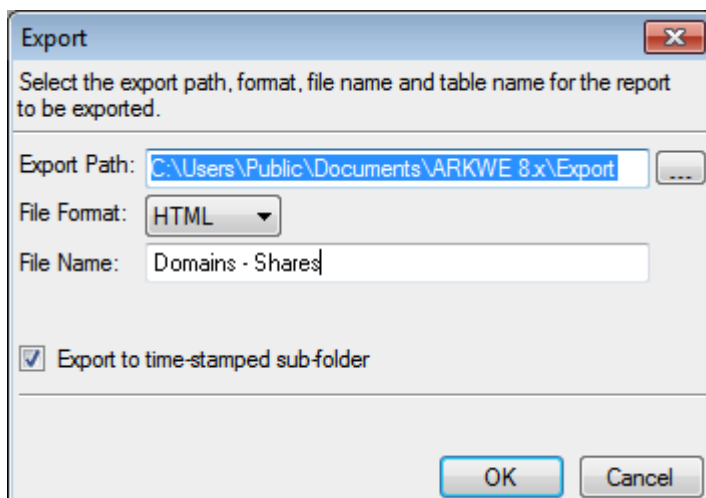
Click on **Refresh Data...** button in the toolbar available in the report window or press F5 to refresh report data. Alternatively, you can right-click on the grid, in the right pane of the report window, and then select 'Refresh Data' from the context menu. The existing data will be cleared and latest data will be loaded in the report window.

### 6.4 How to Export Data?

The **Export** feature helps the user to export report data generated by ARKWE to a file using various formats namely HTML/CSV/XLSX/SQL.



**Click** for exporting the information in the desired format or select Export option under Tools menu to export report data to a file in the desired format.



Specify a file name to export report data to or accept the default file name. Specify the export path and select a desired file format. The path refers to the destination location where the output file generated should be stored. It can be given using the Browse button. To avoid overwrite existing files, if any, in the specified export path, By default, the report will be exported to a time-stamped sub-folder, in the format 'YYYY-MM-DD HH.MM.SS', under the specified export path.

In XLSX file format, the information is stored as sheets in Excel file. For each report, a XLSX file will be generated. The name of the XLSX file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared. The XLSX file will be stored under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path, if "Export to time-stamped folder" option is set.


In CSV file format, the information is stored as comma separated values. For each report, a CSV file will be generated. The name of the CSV file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

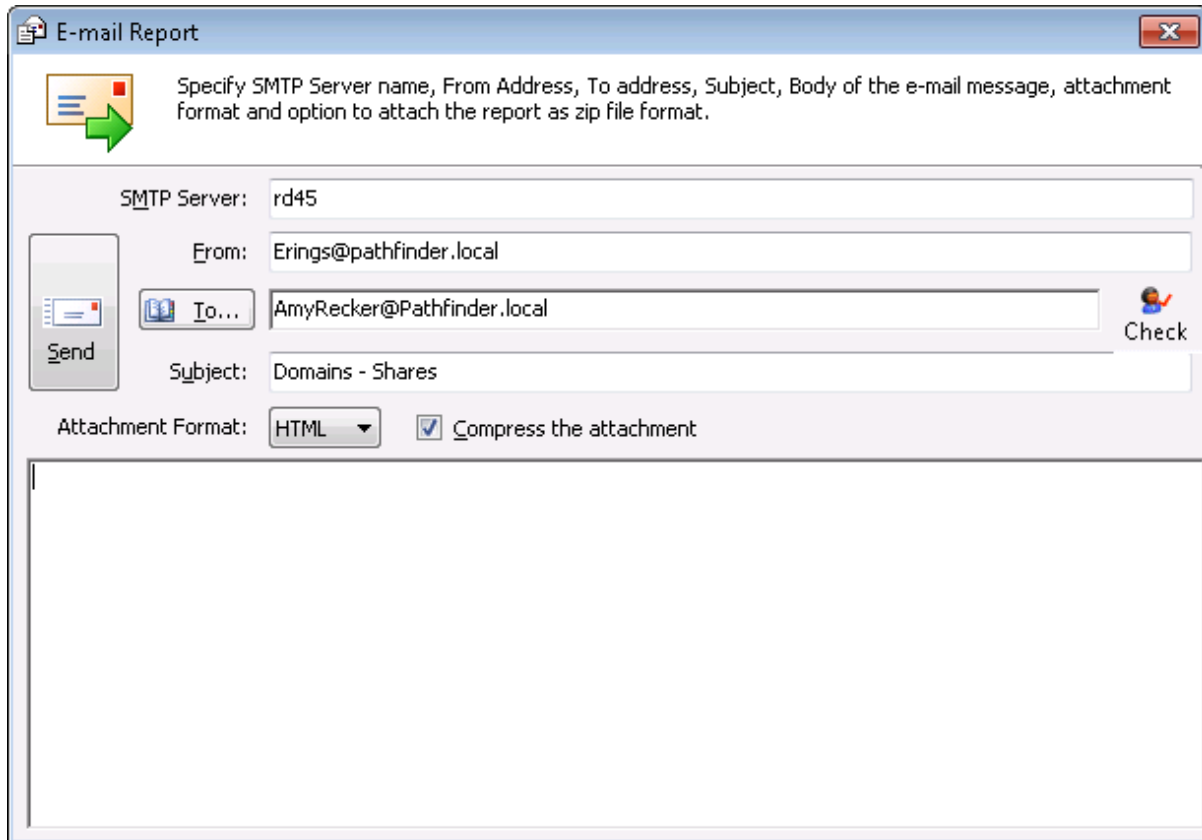
In SQL table format, the information is stored as SQL tables in the application database in the specified SQL server based on the selected SQL database option. For each report, a separate table will be created. The name of the table will be the name of the report.

In HTML file format, the information is stored as an html file. For each report, a HTML file will be generated. The name of the HTML file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

## 6.5 How to E-mail Data?

ARKWE provides the option to e-mail the reports generated.

**Click**  button in the toolbar to e-mail the report to e-mail recipients. E-mail dialog will be displayed as shown below:



The 'E-mail Report' dialog box contains the following fields and options:

- SMTP Server:** rd45
- From:** Erings@pathfinder.local
- To...** AmyRecker@Pathfinder.local
- Subject:** Domains - Shares
- Attachment Format:** HTML (dropdown menu)
- ☒ **Compress the attachment**
- Send** button (with envelope icon)
- Check** button (with checkmark icon)


For e-mailing reports, ARKWE requires SMTP Server, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the report attachment format.

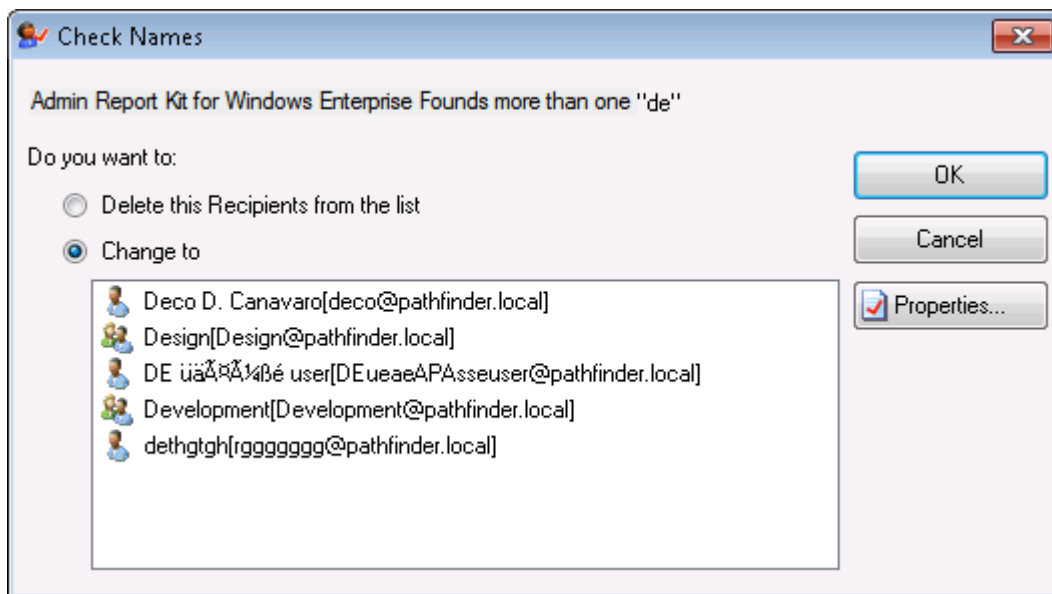
Specify SMTP server name, from Address, "To" address, mail subject, mail content, attachment format and option to compress the attachment.



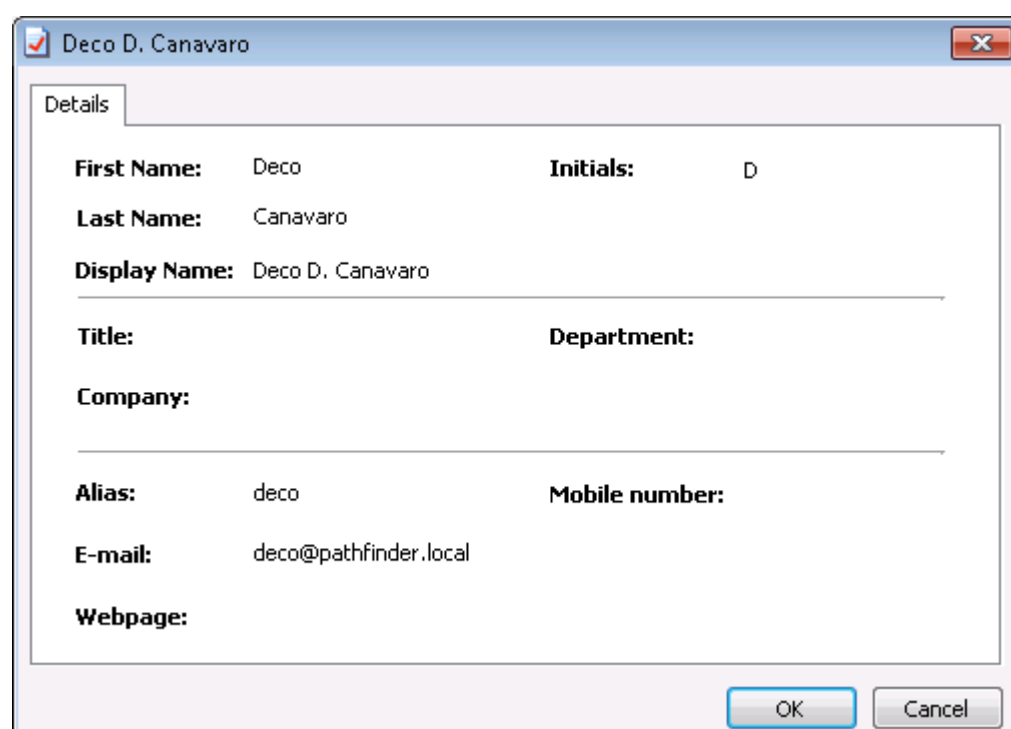
**Click**  button to send the report by e-mail to the selected recipients.

## Check names

ARKWE provides check name feature to check the existence of corresponding mail-enabled recipient object in Active Directory. To check name, **click**  button. If the entered name matches with a mail object in the Active directory / its trusted domain, name entered in From Address textbox will be replaced by the corresponding active directory recipient object. If there is more than one match, a dialog which contains matching Active Directory recipients will appear as shown below. You can select one or more recipient and click **OK**.



- To get more information about the listed recipients under **Change to**, select the name, and then **click** .

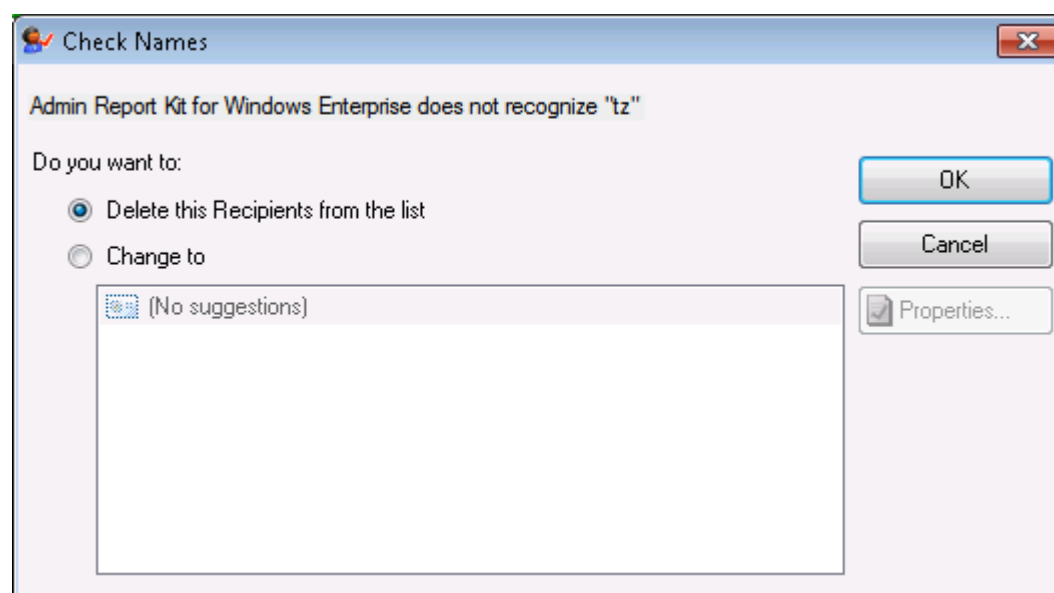


The screenshot shows a Windows-style dialog box titled "Deco D. Canavaro". It has a "Details" tab. The form contains the following fields:

<b>First Name:</b>	Deco	<b>Initials:</b>	D
<b>Last Name:</b>	Canavaro		
<b>Display Name:</b>	Deco D. Canavaro		
<b>Title:</b>	<b>Department:</b>		
<b>Company:</b>			
<b>Alias:</b>	deco	<b>Mobile number:</b>	
<b>E-mail:</b>	deco@pathfinder.local		
<b>Webpage:</b>			

At the bottom right, there are "OK" and "Cancel" buttons.

If there is no match for the name entered by the user in Active Directory, a dialog will appear as shown below:



The screenshot shows a Windows-style dialog box titled "Check Names". It contains the following text and controls:

Admin Report Kit for Windows Enterprise does not recognize "tz"

Do you want to:

- ☒ Delete this Recipients from the list
- ☐ Change to

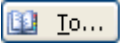
Below the radio buttons is a text box containing "(No suggestions)".

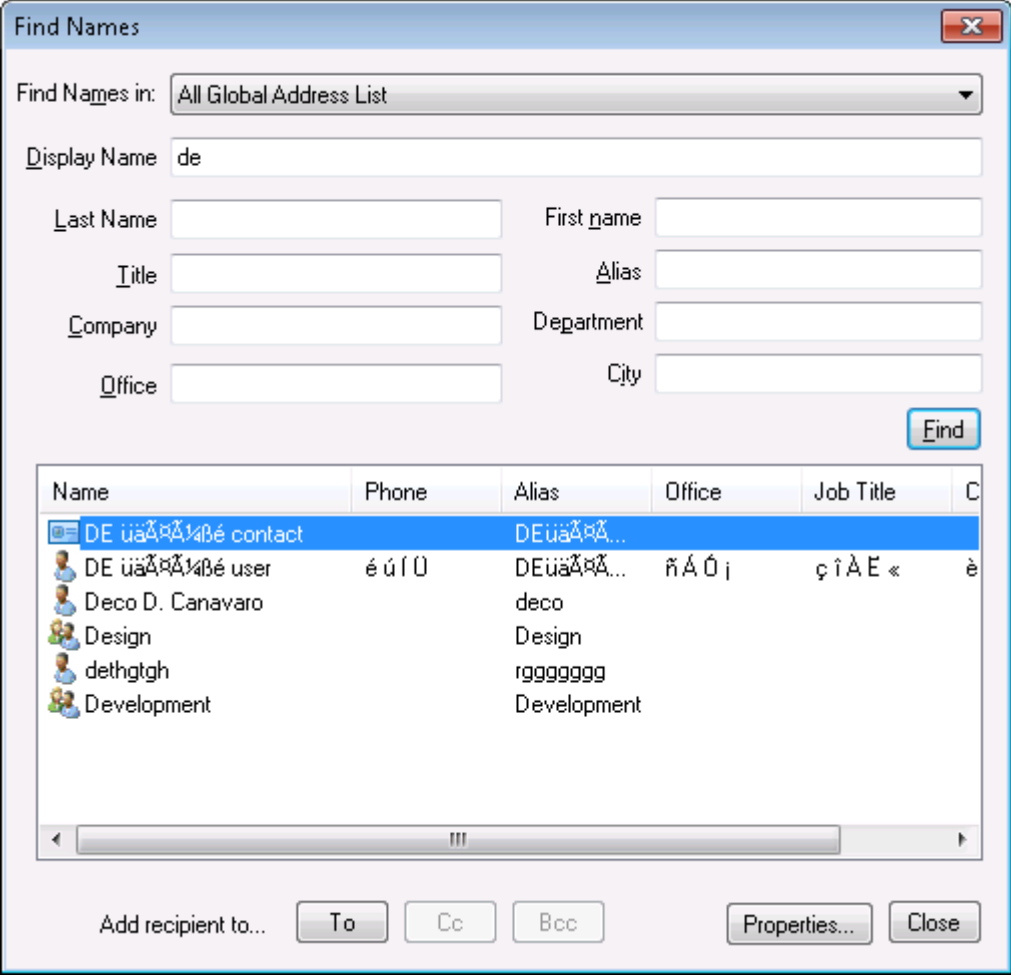
On the right side, there are three buttons: "OK", "Cancel", and "Properties..." (which has a small icon to its left).

Select Delete option in the above dialog to remove the recipient name from to address text box. Click Cancel button to close this dialog and the unresolved recipient(s) will appear in **red** color.

## Address Book

ARKWE provides Address Book feature to search for any mail enabled recipient object (say, person, distribution list, contact, public folder) you want to send a message to.

Click  button and then use the **Find Names** dialog box to search for the recipient object you want to send a message to. (Note that you can't use the **Find Names** dialog box to search for distribution lists in your Contacts folder.) Select the object's name in the list and then click **Add recipient to...To**.




The **Find Names** dialog box is shown with the following fields and controls:

- Find Names in:** All Global Address List (dropdown menu)
- Display Name:** de (text input)
- Last Name:** (text input)
- First name:** (text input)
- Title:** (text input)
- Alias:** (text input)
- Company:** (text input)
- Department:** (text input)
- Office:** (text input)
- City:** (text input)
- Find** button

Name	Phone	Alias	Office	Job Title	City
DE uäÄÄÄ14Bé contact		DEuäÄÄÄ...			
DE uäÄÄÄ14Bé user	é ú f U	DEuäÄÄÄ...	ñ Á Ó j	ç î À E «	è
Deco D. Canavaro		deco			
Design		Design			
dethgtgh		rggggggg			
Development		Development			

At the bottom of the dialog box, there are buttons for:

- Add recipient to...** (dropdown menu)
- To** button
- Cc** button
- Bcc** button
- Properties...** button
- Close** button


- To get more information about one of the names in the list, such as department or phone number, select the name, and then **click** .

## 6.6 How to Find Data in a Report?

---

You can use the find feature in ARKWE to search for specific data in a report.

To search for data in a report, just type the characters or words you want to find in the

find edit box available in the report window and click on  . .

- 1) ARKWE performs a case insensitive search of the specified search criteria in the report.
- 2) The search criteria should not be enclosed within quotation marks.
- 3) You can use the "\*" wildcard character in the search criteria. The "\*" wildcard character act as a place holder for zero or more characters. However, note that you cannot use the "?" wildcard character in the search criteria.

For instance, if you want to search for 'Domain' in a report, Type Domain, without quotations, in the edit box, and then clicks on Find Button.

By default, ARKWE adds an asterisk as a suffix to the specified search criteria, if no wildcard character is present in it. In this case, ARKWE finds a match in the report for all fields that have the text Domain followed by zero or more characters, that is, Domain, Domain Controllers, Domain Admins, etc.

For all the matches found, ARKWE highlights the corresponding columns in the grid, and scrolls the grid automatically to the first occurrence.

- 4) ARKWE finds additional occurrences of the specified search criteria instantaneously. To locate other occurrences of the same search criteria in a report you need to scroll the report grid downwards.

Domains - Shares (PATHFINDER)

Refresh Print/Preview Export Filter Customize E-mail Find everyone

Enterprise - DOMAINS

- ADVENTURE
- DISCOVERY
- PATHFINDER
- V5SPRO
- VYAPINLAB

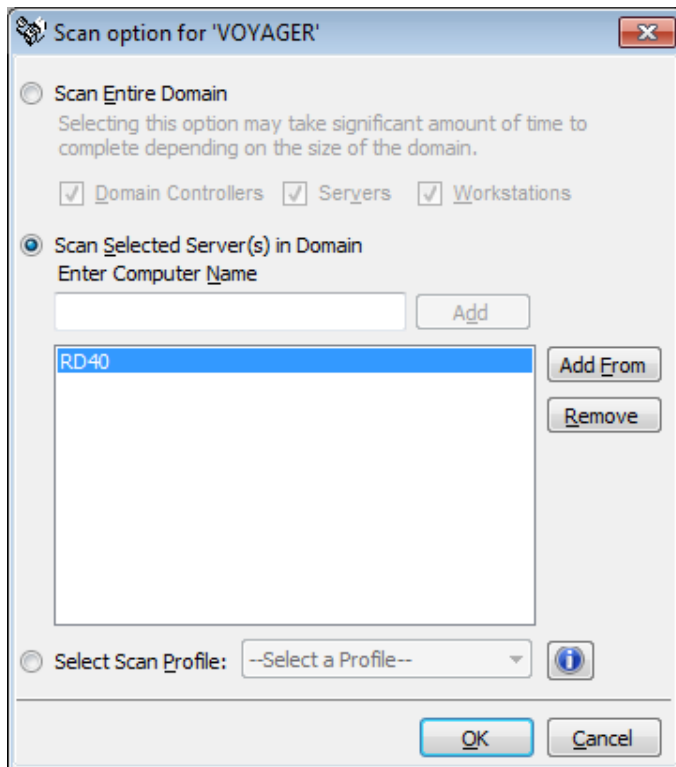
Shares

Host Name	Share Name	Path	User Name	Security	Maximum Uses	Comr
RD45	ADChangeTracker\$	F:\Bharath\ADChang	Everyone	Allow - Full Control	Unlimited	
	Address	C:\Program Files\Ext	Everyone	Allow - Read	Unlimited	"Acce:
			BUILTIN\Administ...	Allow - Full Control	Unlimited	"Acce:
			PATHFINDER\RD4...	Allow - Full Control	Unlimited	"Acce:
	ADMIN\$	C:\WINDOWS		Admin Share	Unlimited	Remot
	Bharath Source Cod	F:\Bharath\Bharath	PATHFINDER\AD...	Allow - Full Control	Unlimited	
	Bulk export for pat	F:\Bulk export for pe	Everyone	Allow - Read	Unlimited	
	C\$	C:\		Admin Share	Unlimited	Default
	F\$	F:\		Admin Share	Unlimited	Default
	G	G:\	Everyone	Allow - Read	Unlimited	
	NETLOGON	C:\WINDOWS\SYS	BUILTIN\Administ...	Allow - Full Control	Unlimited	Logon
			PATHFINDER\Do...	Allow - Full Control	Unlimited	Logon
			PATHFINDER\Do...	Allow - Full Control	Unlimited	Logon
			Everyone	Allow - Read	Unlimited	Logon
	RD45.LOG	C:\Program Files\Ext	BUILTIN\Administ...	Allow - Full Control	Unlimited	Exchai

## 6.7 How to Scan Specific Servers in a Domain?

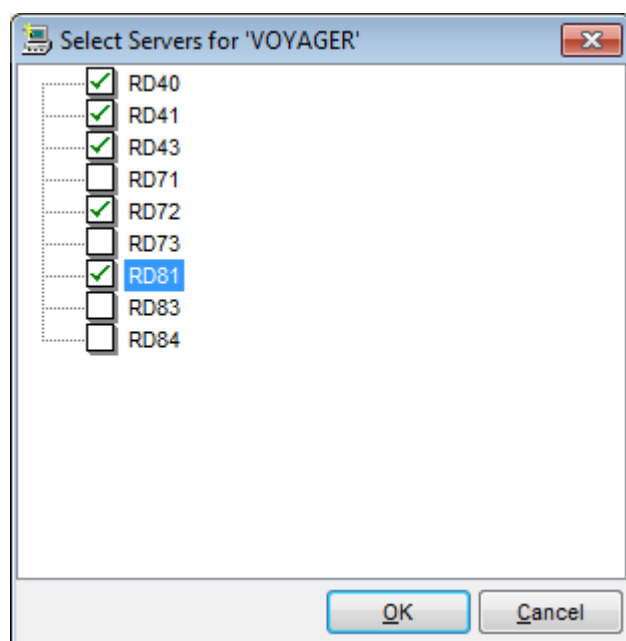
You can have the System Info reports and summary information of a domain (namely Summary, Shares and Applications) generated either for an entire domain or for selected servers in the domain, using the 'Scan option for ...' dialog.

**NOTE:** This dialog appears, if either it is the first time the report is run against the domain or when you refresh the report.

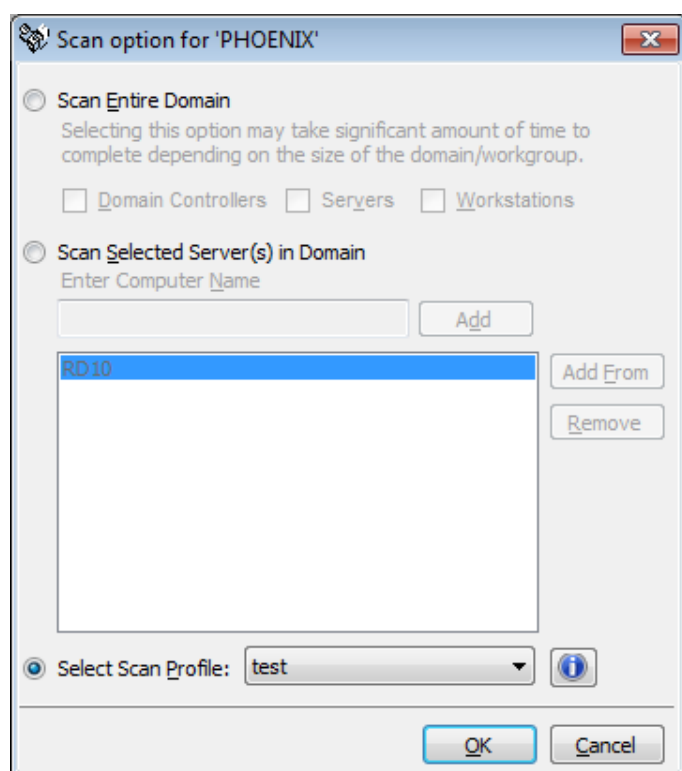


ARKWE defaults to scanning the entire domain, with the provision to enumerate Domain Controllers, Servers, Workstations only. To scan only selected servers, you can either select the computers by using Scan Selected Server(s) in Domain option or by selecting Select a Scan Profile option.



By using the **Scan Selected Server(s) in Domain** option you can specify a computer list by manually typing in the computer name and adding it to the list, or by selecting computers from the network using the **Add From** button as shown below:



You may also apply a scan profile to the report to restrict the list of computers for which you want the report to be generated.



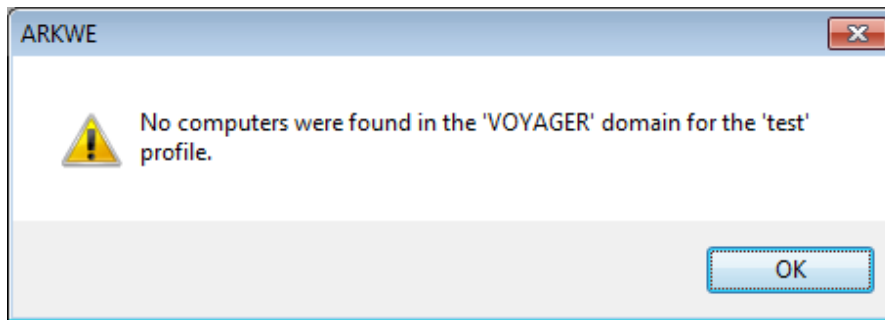
A Scan Profile essentially contains a list of computers that ARKWE can read and generate the report only for computers in the selected profile.

Click  button to create a new Scan Profile. Click  button to edit an existing Scan Profile.

However, please be aware, that the report will be generated only for computers, in the applied profile, belonging to the currently selected domain. This restriction does not apply if the report is being generated off-line using **Power Export tool**.

Click **OK** in the "Scan Option for..." dialog to generate the report.

If ARKWE could not find any computers belonging to the currently selected domain in the applied Scan Profile, you may see the following message show up on screen:



**NOTE:** Clicking **Cancel** in "Scan option for..." dialog will display previously collected report data (if any) for the domain.

## 7 Power Export

### 7.1 About Power Export

---

ARKWE provides a powerful offline report generation tool called Power Export. Power Export allows the user to select multiple reports to be run for several domains and servers across the enterprise at scheduled intervals. The Power Export tool has the ability to export the reports in different file formats.

Please note the following while using the Power Export Wizard:

- a)** Scheduled reports will be created as a "task" in Windows Task Scheduler.
- b)** The scheduled job will generate and export the reports in different file formats (HTML MDB, CSV, PDF, XLSX and TIFF) to the desired folder path/printer.
- c)** By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected Reports will be exported to a time-stamped sub-folder, in the format "yyyy-mm-dd hh.mm.ss", under the task name folder. Therefore, the full folder path for all the exported reports refers to the following directory: <Export path><Task name><Time stamp>.
- d)** A separate file will be created for each report in the desired file format. For example, in the HTML file format, each report will be created as an .html file.

**NOTE:**

ARKWE Power Export Wizard will help you create and store the settings for a task, which you may view or modify later using the Scheduled Tasks Manager. The task will be created with the settings (Schedule Type and Run As parameter) provided using the Power Export Wizard. A valid password must be specified for the Run As parameter of the task.

You can schedule the two types of reports (Standard report and Built-in report) available in ARKWE.

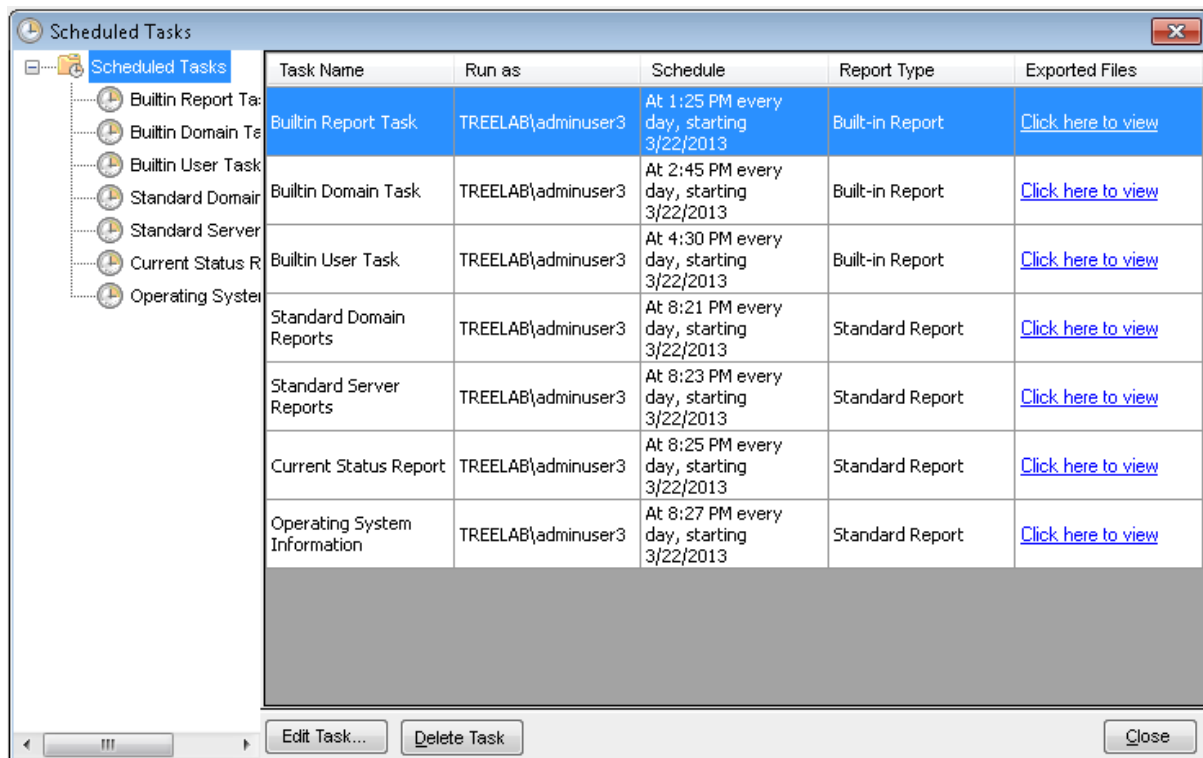
## 7.2 Task Manager-Scheduled Tasks Manager

The Scheduled Tasks Manager allows you to perform the following operations:

- View summary information for the tasks created
- View exported files of the task
- Edit an existing task
- Delete a task

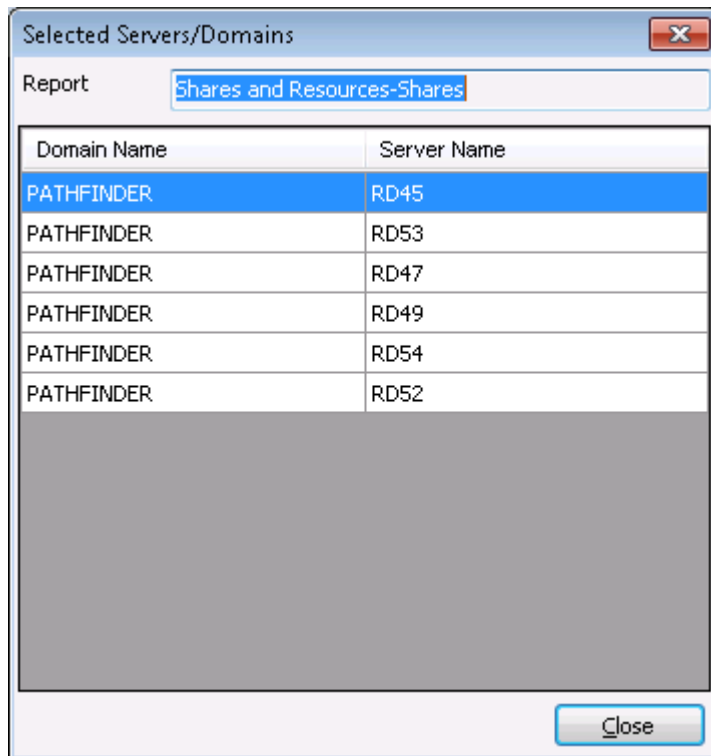
### View Summary Information of a Task

The pane on the left hand side in the Scheduled Tasks Manager window lists the tasks maintained in ARKWE. To view summary information of a task, select the desired task on the left pane. The summary information of the selected task will be displayed in the right pane as shown below:



The task summary includes information about the task information, reports selected, export settings.

To view the selected servers/domains for a report in the task, click on the hyperlink in the **Servers/Domains** column in the right pane. The **Selected Servers/Domains** window will be displayed as shown below:



### View Exported Files

To view the reports generated and exported by the task, perform either one of the following steps:

- Select **Scheduled Tasks** node on the left pane, and then click on the hyperlink in the **Exported Files column** in the right pane for the desired task.

**OR**

- Select the desired task on the left pane, and then click on the hyperlink next to **Exported Files**.

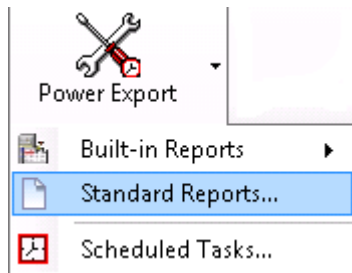
### Edit Task

- 1) Select a task from the Scheduled Tasks Manager Window and Click **Edit Task**.
- 2) Perform the steps as in Schedule Standard Report or Schedule Built-in Report based on the scheduled report type. While proceeding through the wizard you may change the settings, add a new report, delete a report, edit a report, change the export path etc.,
- 3) The new settings will be used when the task runs the next time.

### Delete Task

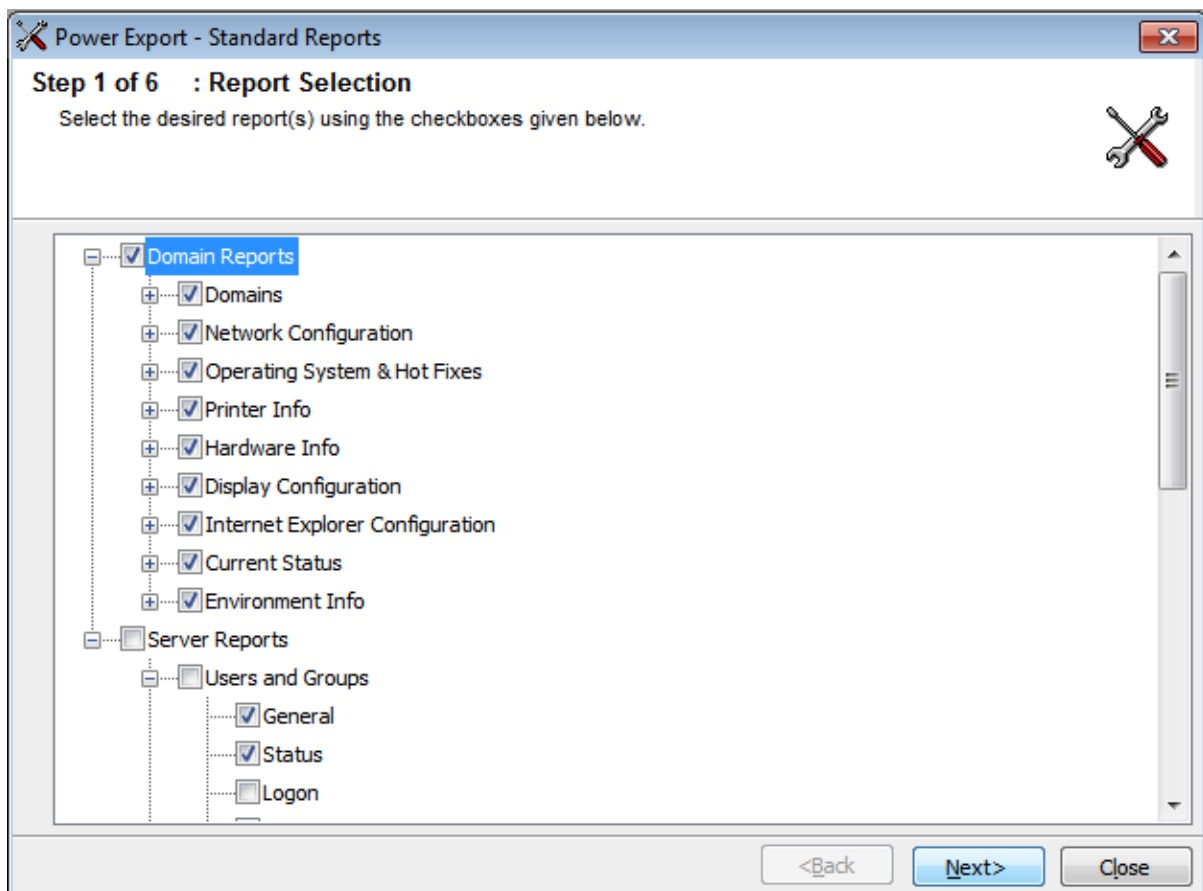
To delete a task from the Power Reports Task Manager Window, select the task and Click Delete Task. The deleted task will be removed permanently from the Windows Task Scheduler.

### 7.3 Schedule Standard Reports



Select **Standard Reports...** option under Power Export. This will bring up the Power Export Wizard.

#### Step 1: Report Selection

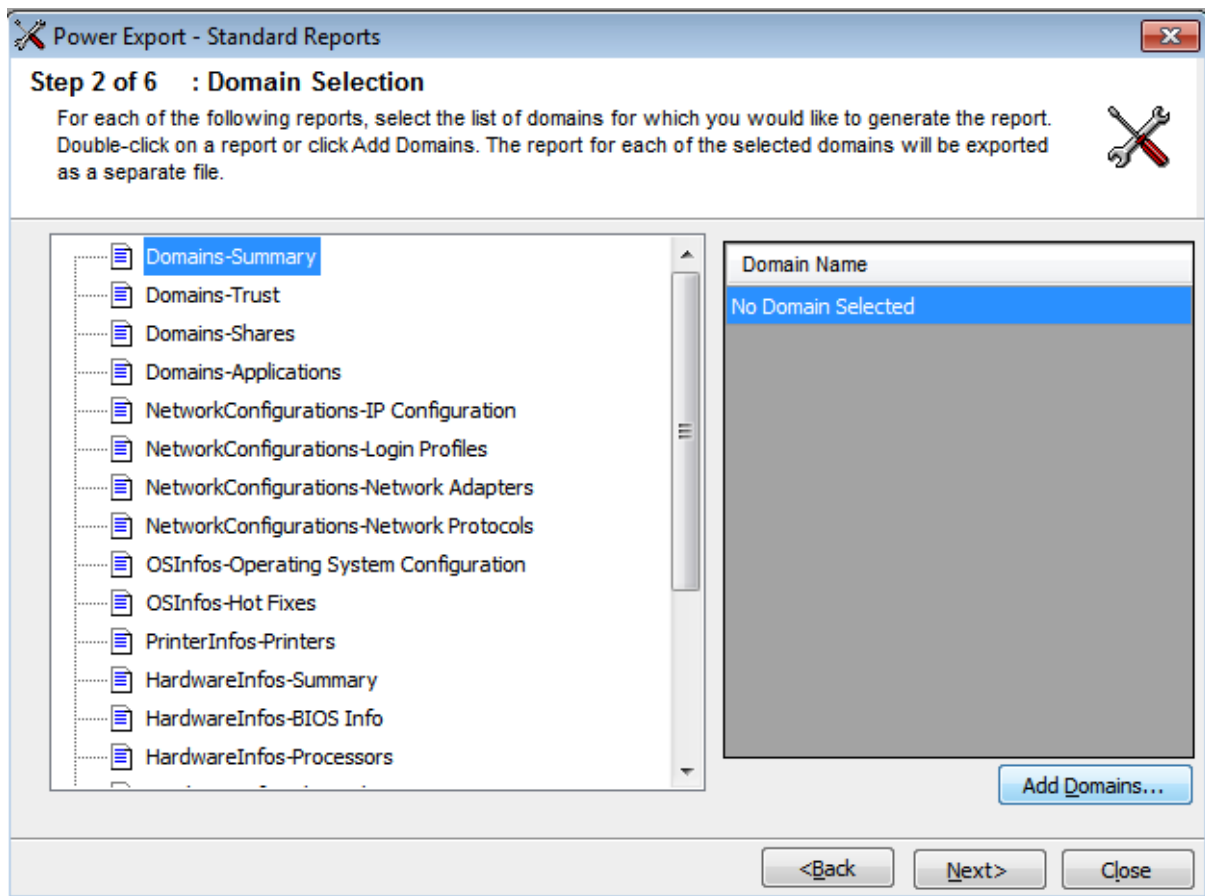


- 1) **Select** the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
- 2) There are two categories of reports - Domain Reports and Server Reports.
- 3) Reports falling under 'Domain Reports' default to scanning and collecting data for the entire domain. However, you can also restrict the domain scope and scan and collect data only for a specific set of servers and have the domain reports generated (viz., Summary, Shares, and Applications).

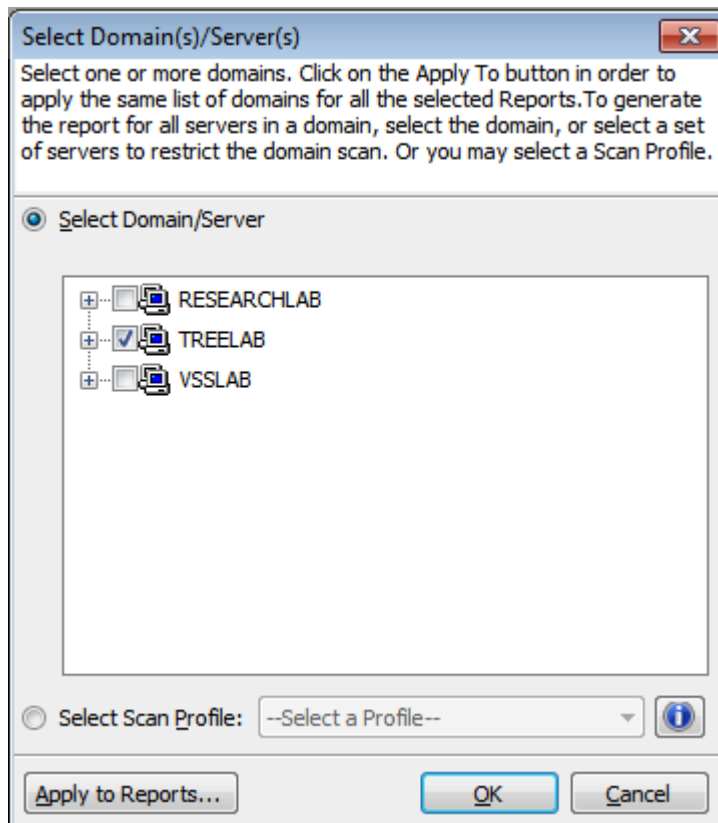
- 4) Reports falling under 'Server Reports' scan each server and collect data specific to each server. They are further classified by the category they report on (viz. Users, Policies, and Events etc.).
- 5) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

## Step 2: Domain Selection for Domain Reports

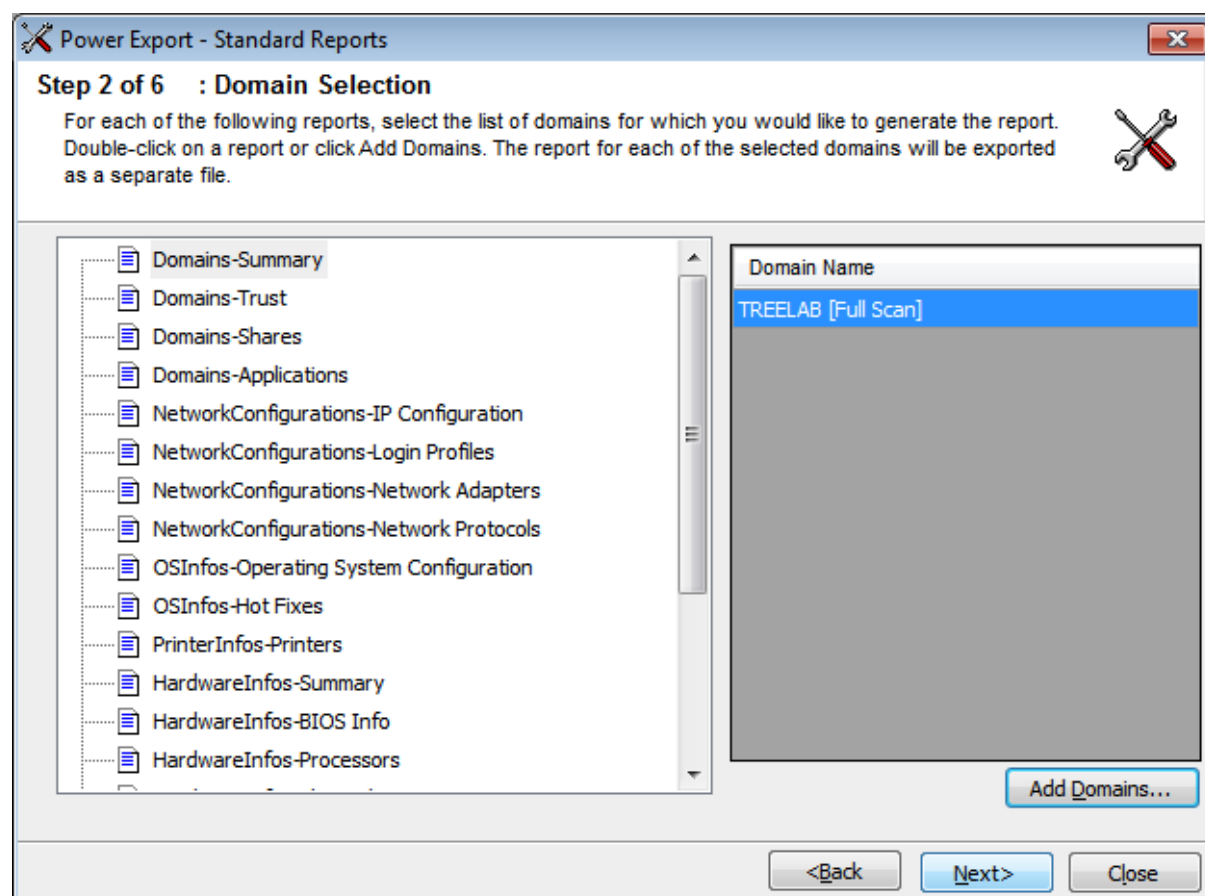
**NOTE:** This step is applicable only if a Domain Report is selected in step 1.



- 1) Click **Add Domains** button to select the domains for which you wish to run the domain reports selected in Step 1. This will display a window where you can select the domains you want to add.



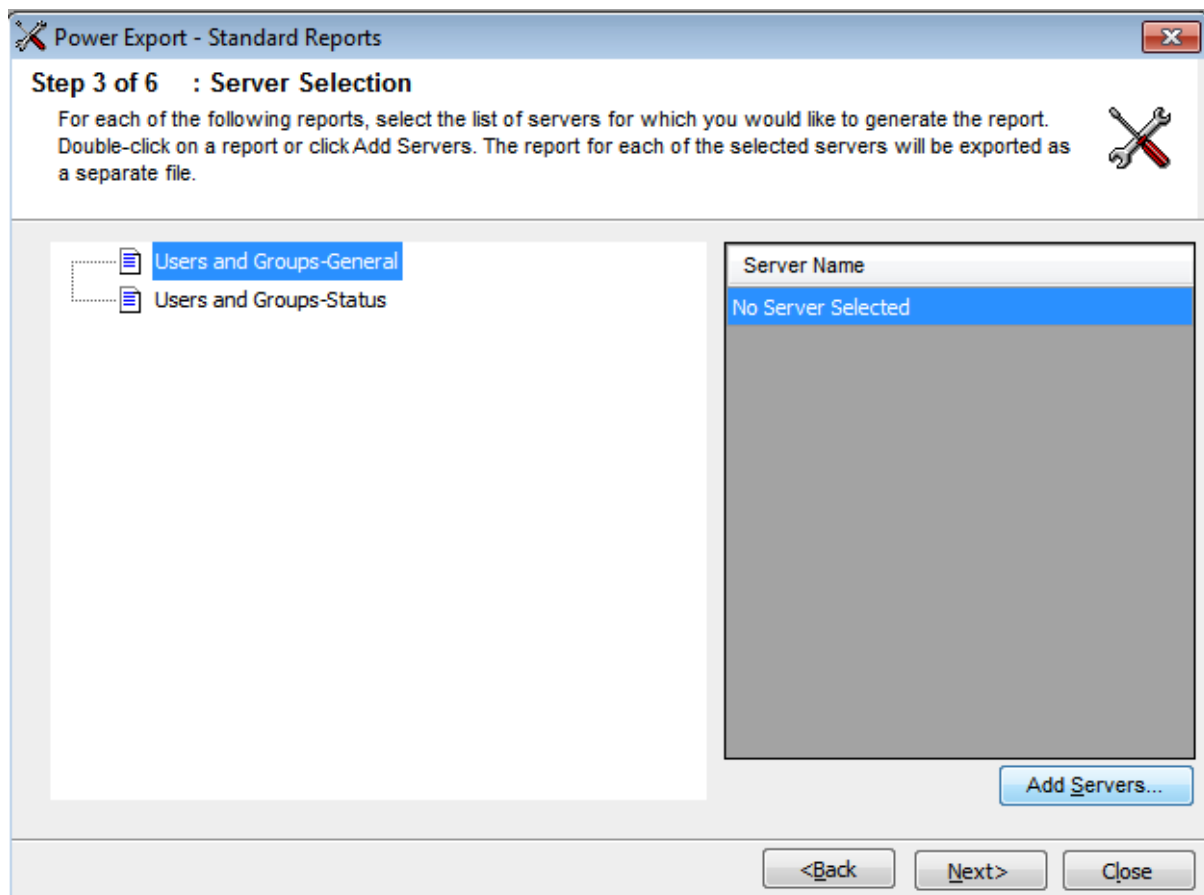
- 2) You can restrict the domain scope and scan and collect data only for a specific set of computers by either selecting specific computers under a domain or by selecting a Scan Profile.
- 3) Click **OK** to apply the selected domains or a Scan Profile to the current report or click **Apply to Reports** to apply the selection to the rest of the selected domain reports. The selected domains will be added to the wizard as shown below:



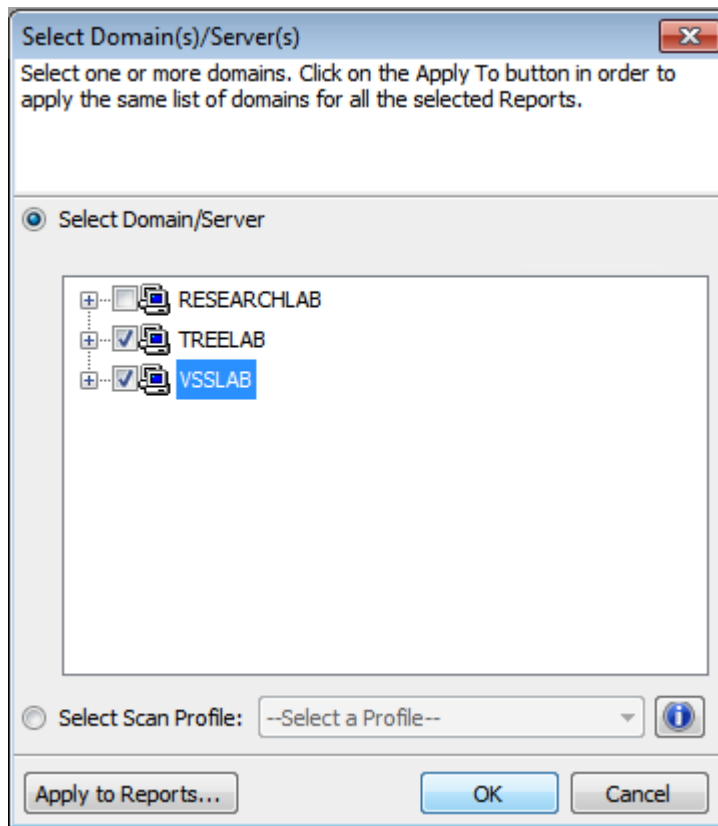
4) Click **Next** to proceed to the next Step.

### Step 3: Server Selection for Server Reports

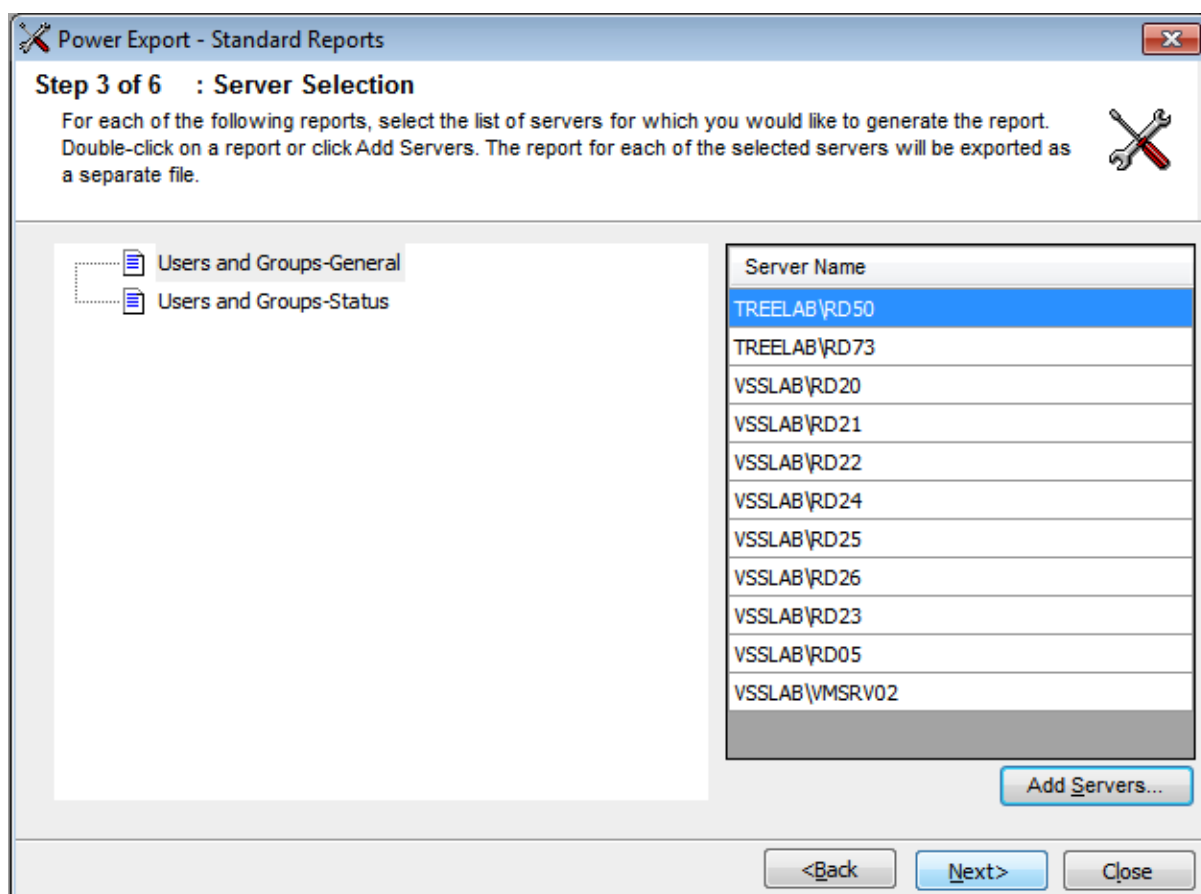
**NOTE:** This step is applicable only if a Server Report is selected in step 1.



- 1) Click **Add Servers** button to select the servers for which you wish to run the server reports selected in Step 1. This will display a window where you can select the servers you want to add. Selecting a domain will add all the servers in that domain to the report.



- 2) You can restrict the domain scope and scan and collect data only for a specific set of computers by either selecting specific computers under a domain or by selecting a Scan Profile.
- 3) Click **OK** to apply the selected servers or a Scan Profile to the current report or click **Apply to Reports** to apply the selection to the rest of the selected server reports. The selected servers will be added to the wizard as shown below:



- 4) Click **Next** to proceed to the Next step.

**Step 4: Delivery Options**

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

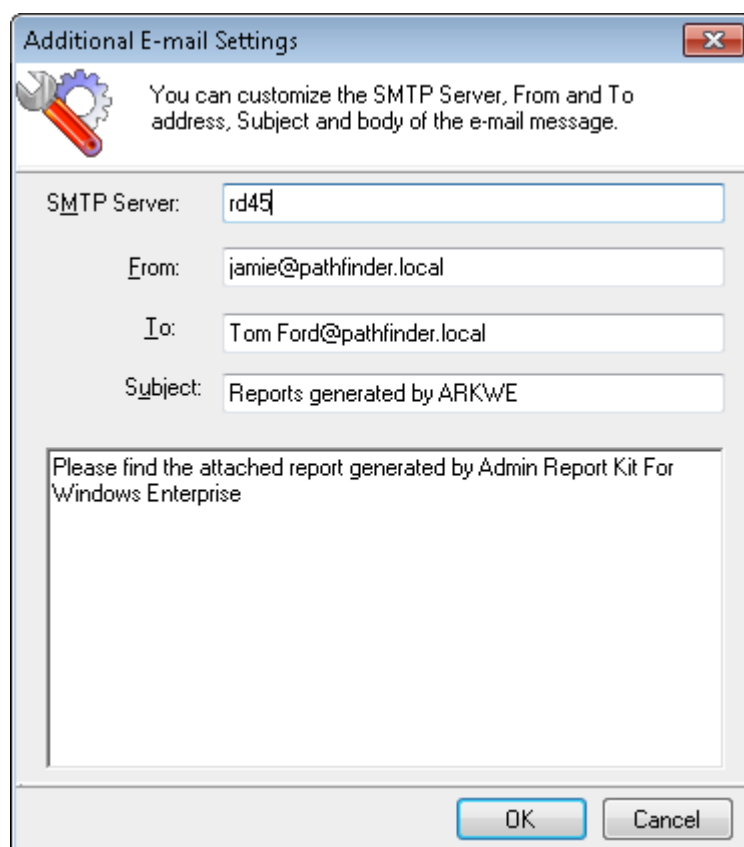
To Address:

☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.
  - Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below:



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

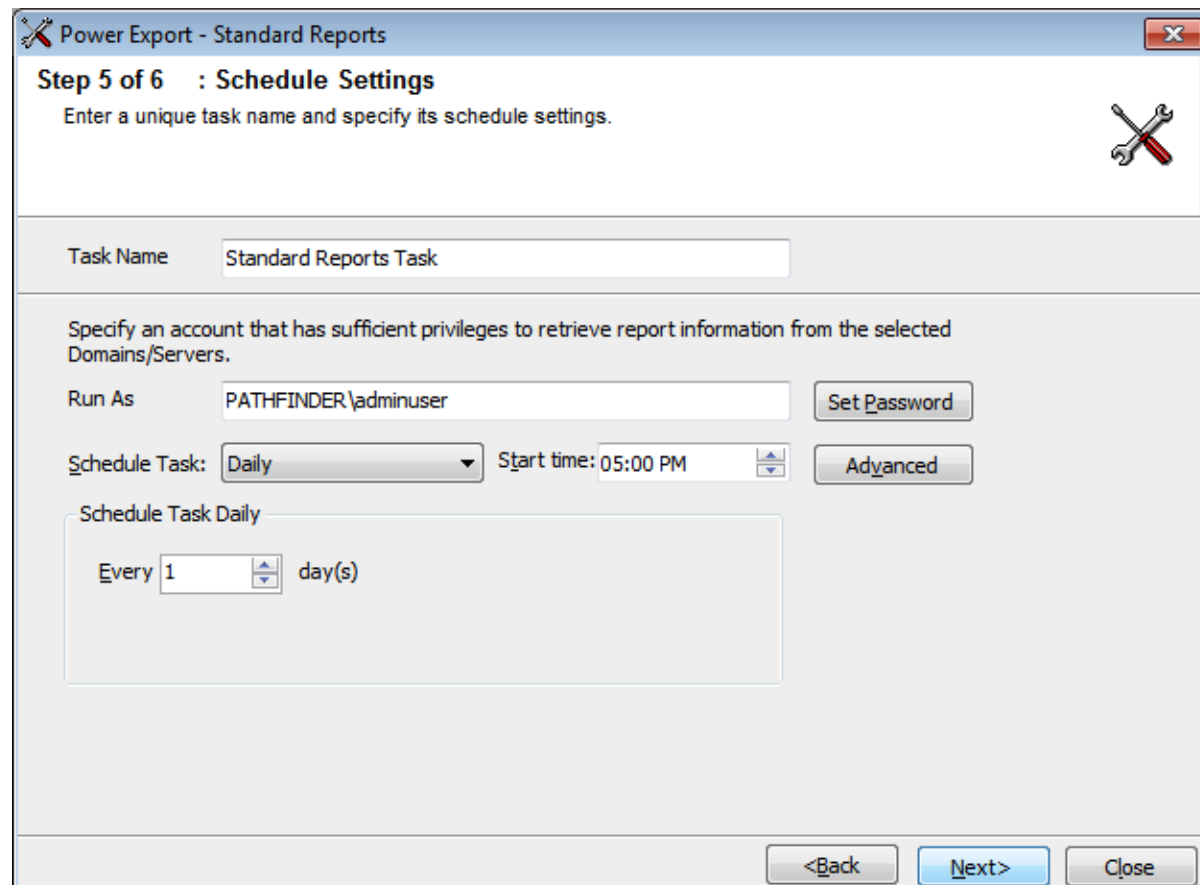
From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

### Step 5: Schedule Settings



**Power Export - Standard Reports**

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

Schedule Task:  Start time:

Schedule Task Daily

Every  day(s)

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

### Step 6: Summary

**Power Export - Standard Reports**

**Step 6 of 6 : Summary**  
Click Finish to save the task details.

**Task Name:** Standard Reports Task **Report:** Standard

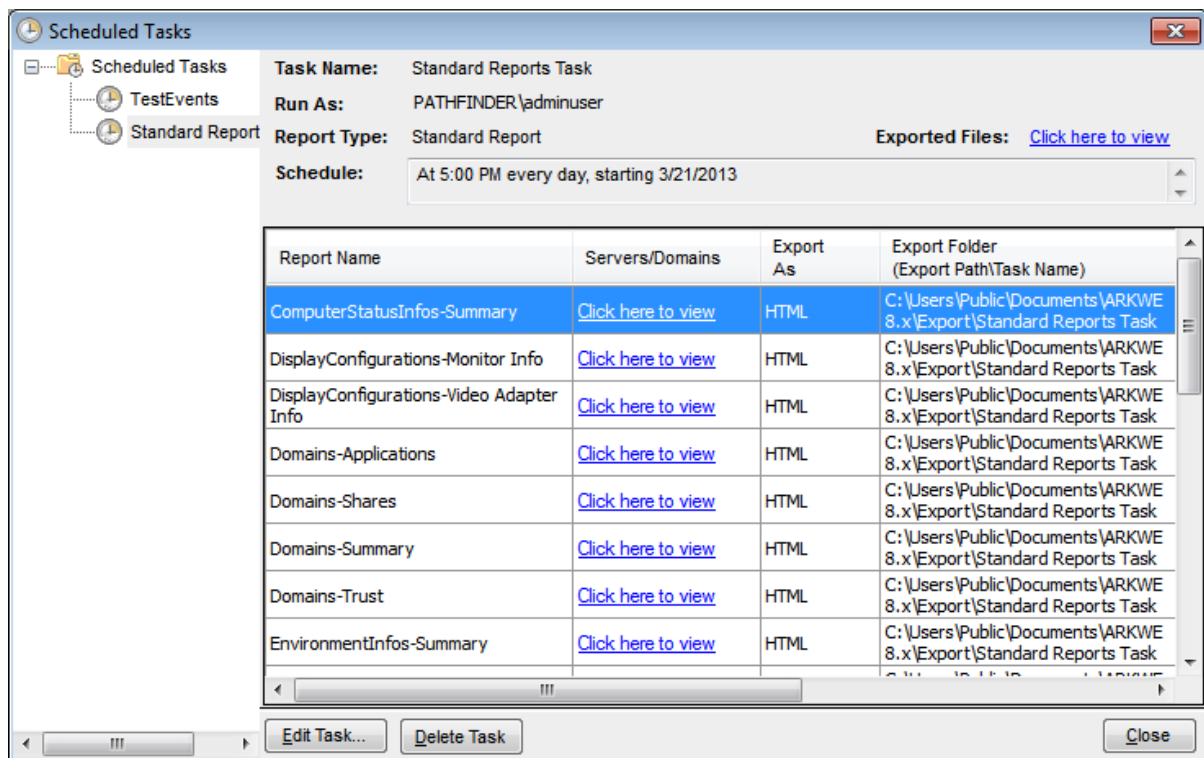
**Run As:** PATHFINDER\adminuser

**Schedule:** At 05:00 PM every day, starting 3/21/2013

Report Name	Servers/Domains	Export As	Export Folder (Export Path\Task Name)
Domains-Summary	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
Domains-Trust	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
Domains-Shares	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
Domains-Applications	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
NetworkConfigurations-IP Configuration	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
NetworkConfigurations-Login Profiles	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task

<Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:



## 7.4 Schedule Built-in Reports

---

The built-in reports have been categorized to the following:

- **Permissions Reports**
- **Shares and Resources reports**
- **Users and Groups reports**
- **Domains reports**

## Schedule Permissions Built-in Reports

### Permissions Reports

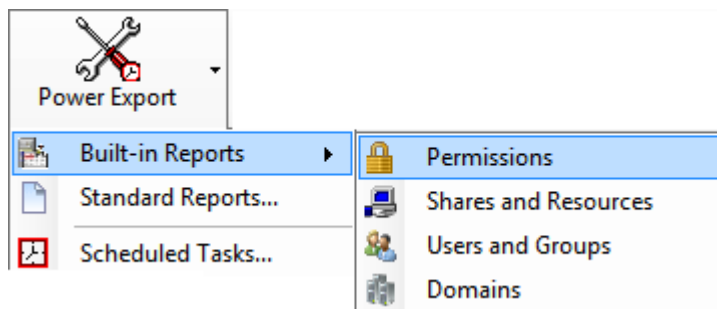
Permissions Reports includes reports that focus solely on reporting the access permissions assigned to users and groups on objects such as folders etcetera.

- **List of permissions for specific users and groups on folders**
- **List of permissions for folders**
- **List of permissions for specific users and groups on files**
- **List of permissions for files**

## Schedule Permissions Built-in Reports

### List of Permissions for Specific Users and Groups on Folders

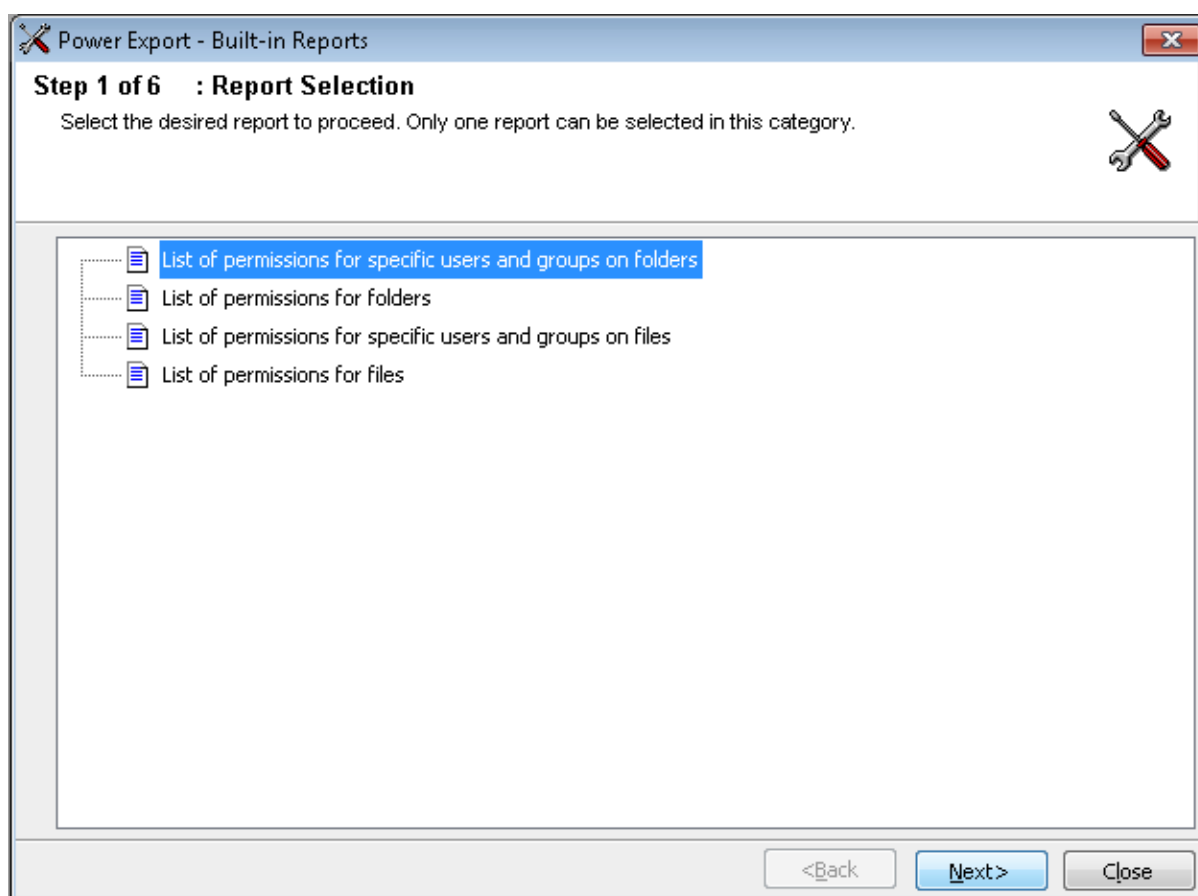
This report allows you to view folder permissions for specific users and groups.



**Select** option under Power Export.

This will bring up the Power Export Wizard.

### Step 1: Report Selection



- 1) Select "**Permissions Reports**" from the select report category drop-down list.
- 2) Select the desired report. Only one report may be selected to run in a single task.
- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.



**Step 2: User and/or Group Selection**

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on folders

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts



Account Name	Account Type
--------------	--------------

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on folders

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts

Account Name	Account Type
TREELAB\Administrator	User
TREELAB\adminuser1	User
TREELAB\adminuser2	User
TREELAB\adminuser3	User
TREELAB\alberto	User
TREELAB\barton	User
TREELAB\shane	User
TREELAB\tony	User

- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, click About Scan Profiles (Users/Groups).
- 1) Select the user or group, for which you wish to run the permissions report.
- 2) The selected users will be added to the wizard as shown above:
- 3) Click **Next** to proceed to the Next step.

### Step 3: Shared Folder Selection

**Step 3 of 6 : Shared Folder Selection**

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.

Report: **List of permissions for specific users and groups on folders**

UNC Path:

Scan Profile (Shares): <No Profile found.>

Folder Path	Include sub-fold...	Folder level
\\RD50\ADMIN\$	True	All
\\RD50\ARKWE	True	All
\\RD50\C\$	True	All
\\RD50\E\$	True	All
\\RD50\new	True	All

☒ Do not display folders that have the same permissions as the parent folder

☐ Include group membership information ☐ Include SID

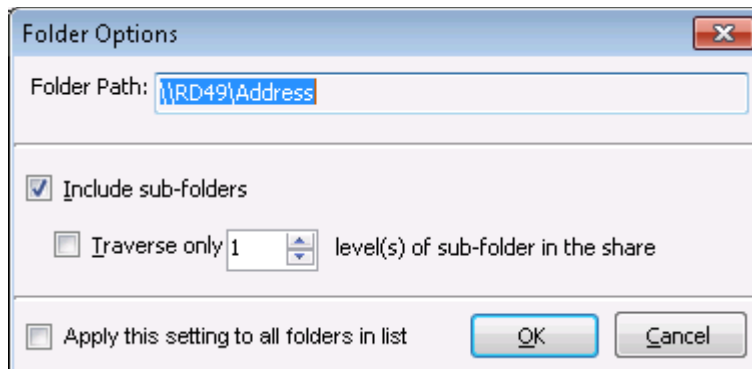
☐ Validate for Errors ☒ Include Error Details

☒ Generate report ignoring any errors found

☐ Generate report only if no errors were found. Send error report through e-mail

- 1) Select the desired folder(s) for which you wish to run the permissions report.
- 2) You may also click **Import** button to import a list of UNC folder paths from a text file.
- 3) Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.

- 4) ARKWE defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



- 5) Modify the folder options as required and click **OK**.
- 6) Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
- **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
  - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users
- 7) You may select **Include Error Details** option for including the error information of folders / files into report data.
- 8) Click **Next** to proceed to the Next step.

**Step 4: Delivery Options**

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export ...

☐ **E-mail**

To Address: ...

☒ **Compress the attachment**

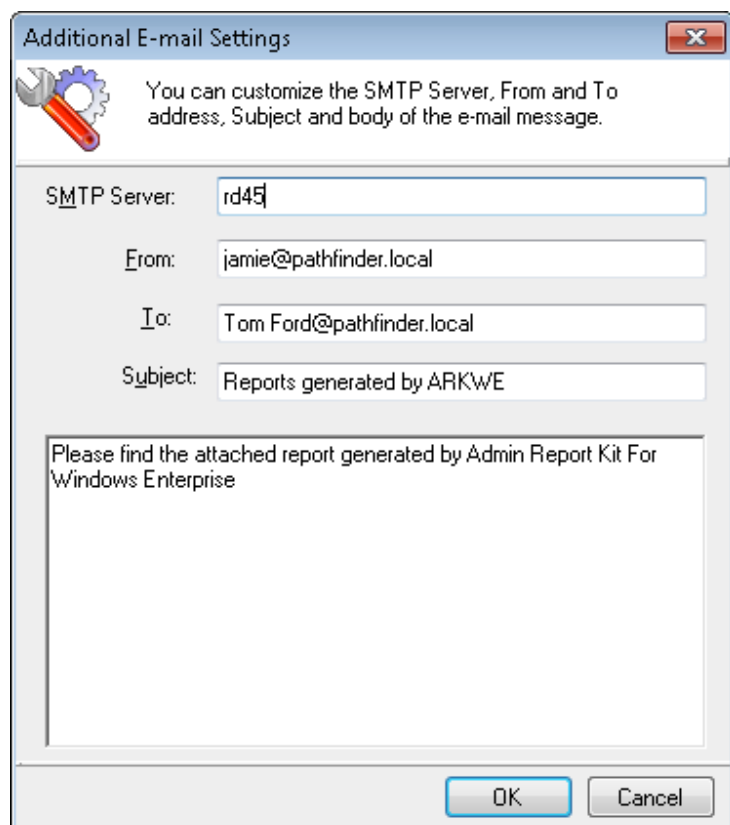
**Note: This evaluation version exports / e-mails only the first 10 records.**

**Additional E-mail Settings...**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

Click **Additional E-mail** Settings button to specify optional e-mail settings as shown below:



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

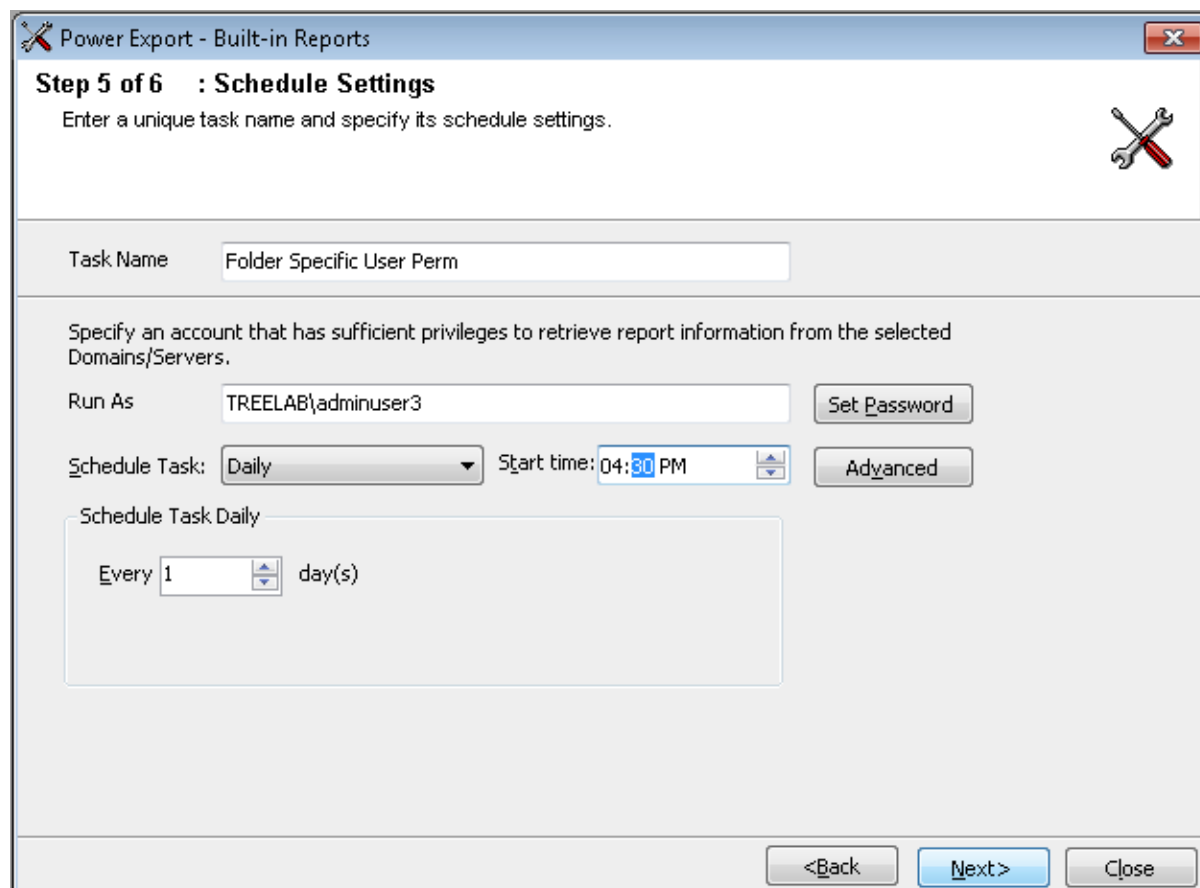
From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

### Step 5: Schedule Settings



**Power Export - Built-in Reports**

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

Schedule Task:  Start time:

Schedule Task Daily

Every  day(s)

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

### Step 6: Summary

**Power Export - Built-in Reports**

**Step 6 of 6 : Summary**  
Click Finish to save the task details.

**Task Name:** Folder Specific User Perm **Report:** Built-in Report

**Run As:** TREELAB\adminuser3

**Schedule:** At 04:30 PM every day, starting 3/22/2013

Report Name	User/Group Accounts	Shared Folders	Export As	Export Folder (Export Path\Task Name)
List of permissions for specific users and groups on folders	<a href="#">Click here to view</a>	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKW... 8.x\Export\Folder Specific User Perm

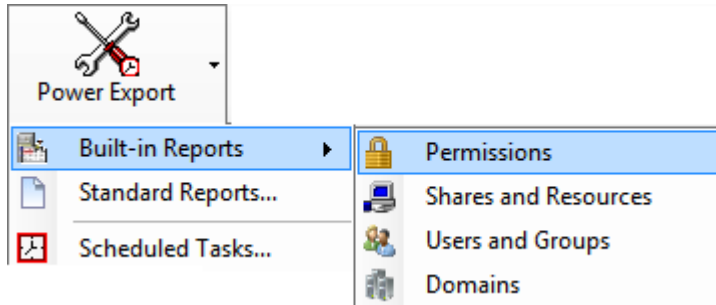
<Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Schedule Tasks.

## Schedule Permissions Built-in Reports

### List of Permissions for Folders

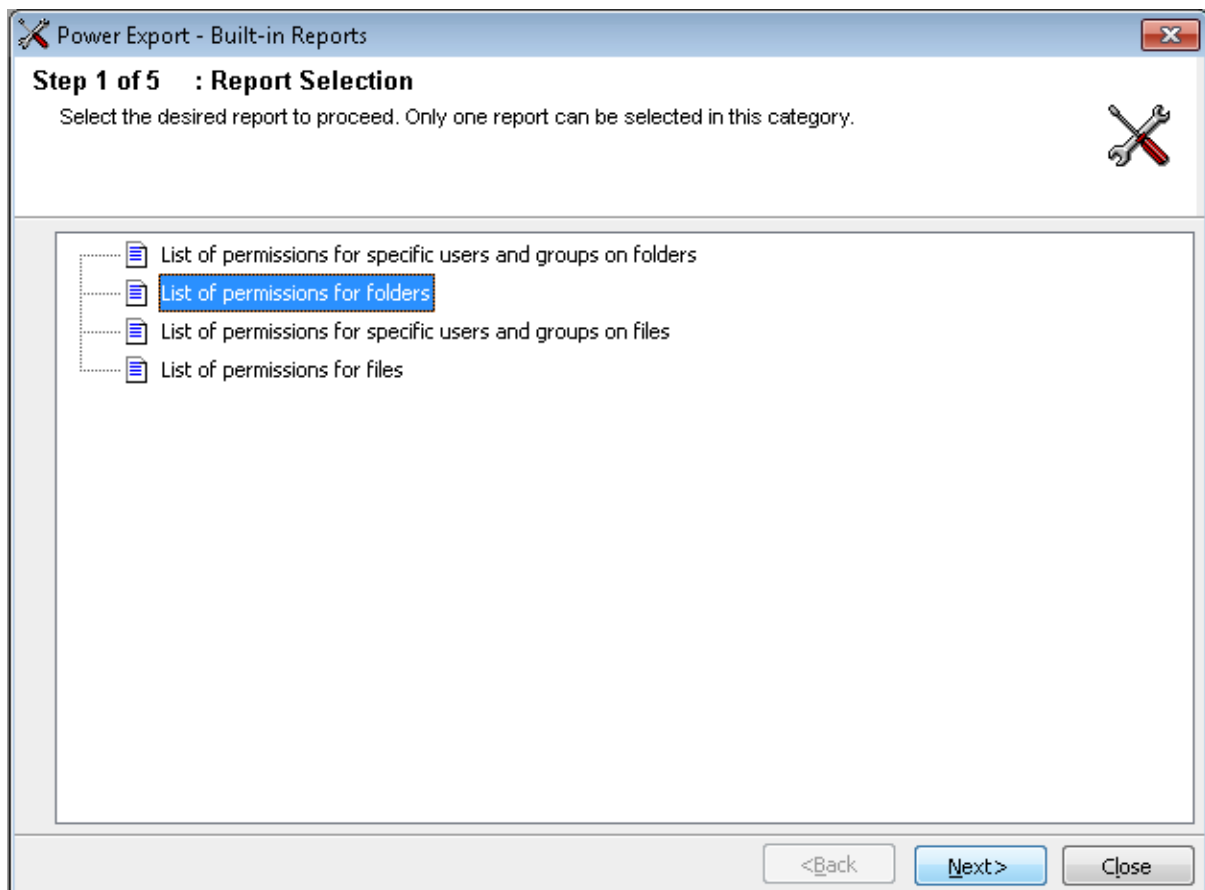
This report, allows you to view the associated folder permissions for a set of folders.



**Select** option under Power Export.

This will bring up the Power Export Wizard.

### Step 1: Report Selection



- 1) Select **"Permissions Reports"** from the select report category drop-down list.
- 2) Select the desired report. Only one report may be selected to run in a single task.
- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

**Step 2: Shared Folder Selection**

**Step 2 of 5 : Shared Folder Selection**

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.

Report **List of permissions for folders**

UNC Path:  Add

Scan Profile (Shares): <No Profile found.>

Folder Path	Include sub-fold...	Folder level
\\RD50\\ADMIN\$	True	All
\\RD50\\ARKWE	True	All
\\RD50\\C\$	True	All
\\RD50\\E\$	True	All
\\RD50\\new	True	All

Add From... Import Remove

☒ Do not display folders that have the same permissions as the parent folder Edit Folder Options...

☐ Include group membership information ☐ Include SID

☐ Validate for Errors ☒ Include Error Details

☒ Generate report ignoring any errors found

☐ Generate report only if no errors were found. Send error report through e-mail E-mail Settings

<Back Next> Close

- 1) Select the desired folder(s) for which you wish to run the permissions report.
- 2) You may also click **Import** button to import a list of UNC folder paths from a text file.
- 3) Folders that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want folders with identical permissions as the parent folder reported, then select **Do not display folders that have same permissions as the parent folder** option. This option will not report folders with identical permissions as the parent folder.
- 4) ARKWE defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:

**Folder Options**

Folder Path: \\RD49\\Address

☒ Include sub-folders

☐ Traverse only 1 level(s) of sub-folder in the share

☐ Apply this setting to all folders in list

OK Cancel

- 5) Modify the folder options as required and click **OK**.
- 6) Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
  - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
  - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
- 7) You may select **Include Error Details** option for including the error information of folders / files into report data.
- 8) Click **Next** to proceed to the *Next* step.

### Step 3: Delivery Options

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

To Address:

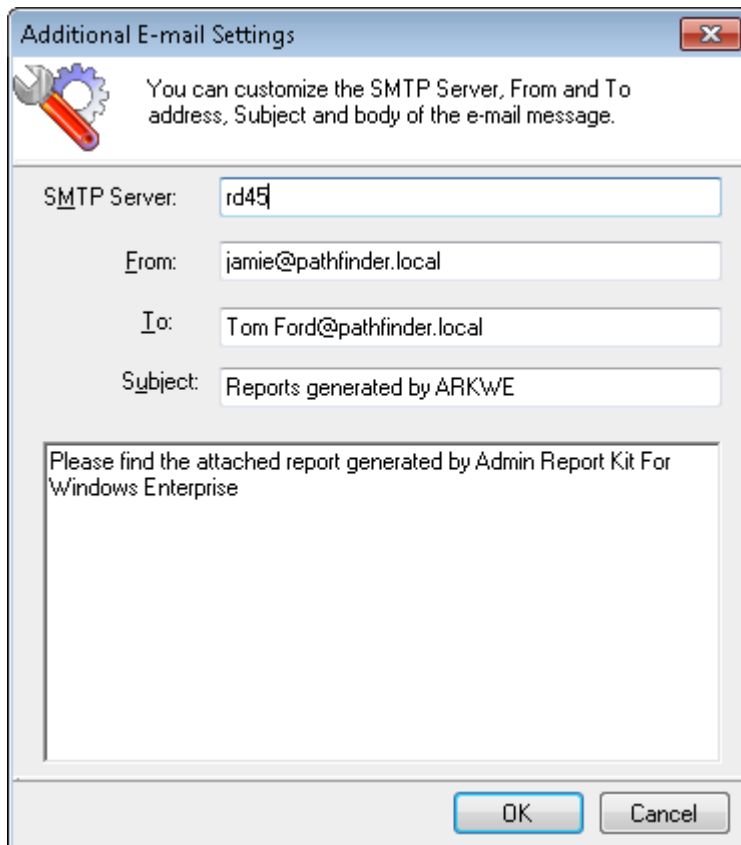
☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back   Next>   Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below:



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

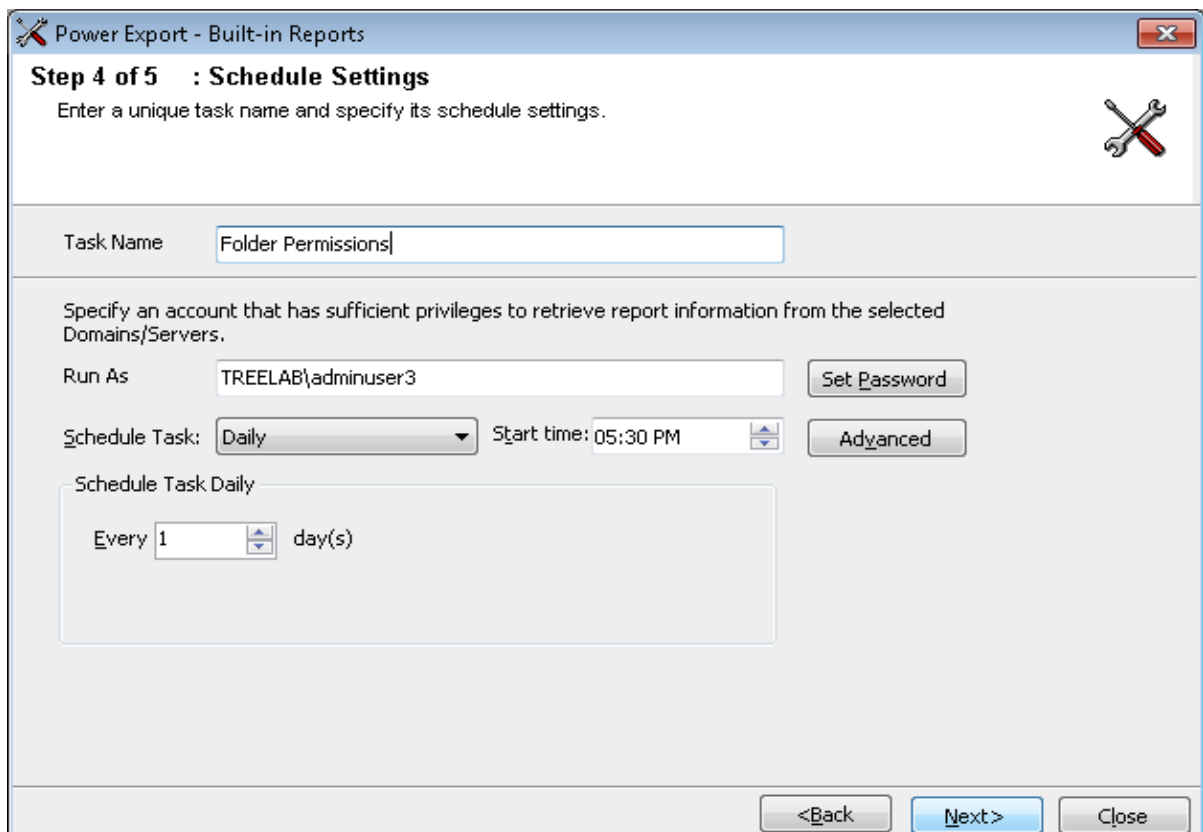
From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

#### Step 4: Schedule Settings



**Power Export - Built-in Reports**

**Step 4 of 5 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

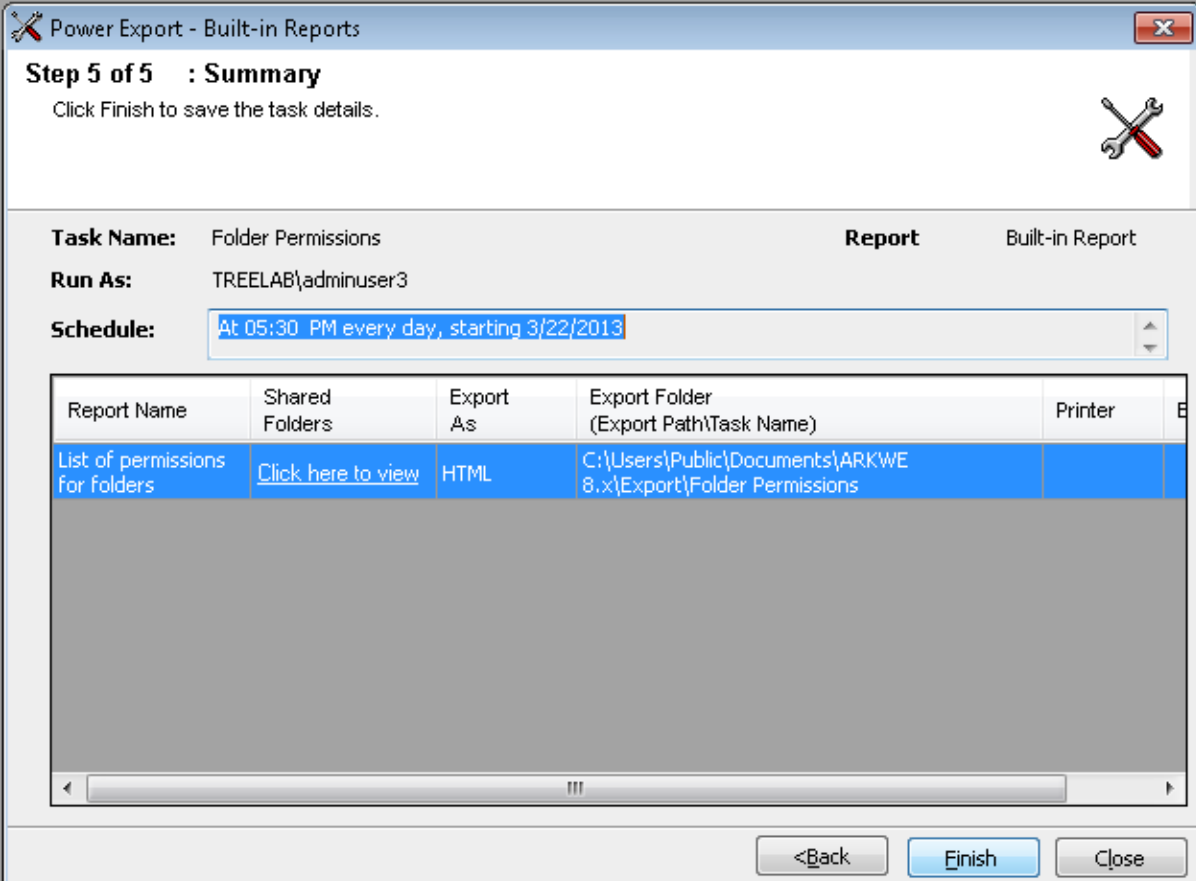
Schedule Task:  Start time:

Schedule Task Daily

Every  day(s)

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

### Step 5: Summary



**Power Export - Built-in Reports**

**Step 5 of 5 : Summary**  
Click Finish to save the task details.

**Task Name:** Folder Permissions **Report:** Built-in Report

**Run As:** TREELAB\adminuser3

**Schedule:** At 05:30 PM every day, starting 3/22/2013

Report Name	Shared Folders	Export As	Export Folder (Export Path\Task Name)	Printer
List of permissions for folders	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Folder Permissions	

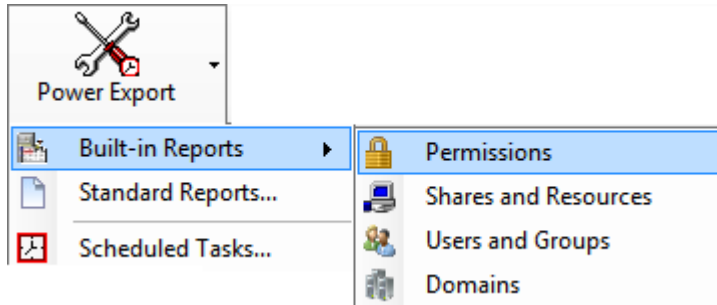
<Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Schedule Tasks.

## Schedule Permissions Built-in Reports

### List of Permissions for Specific Users and Groups on Files

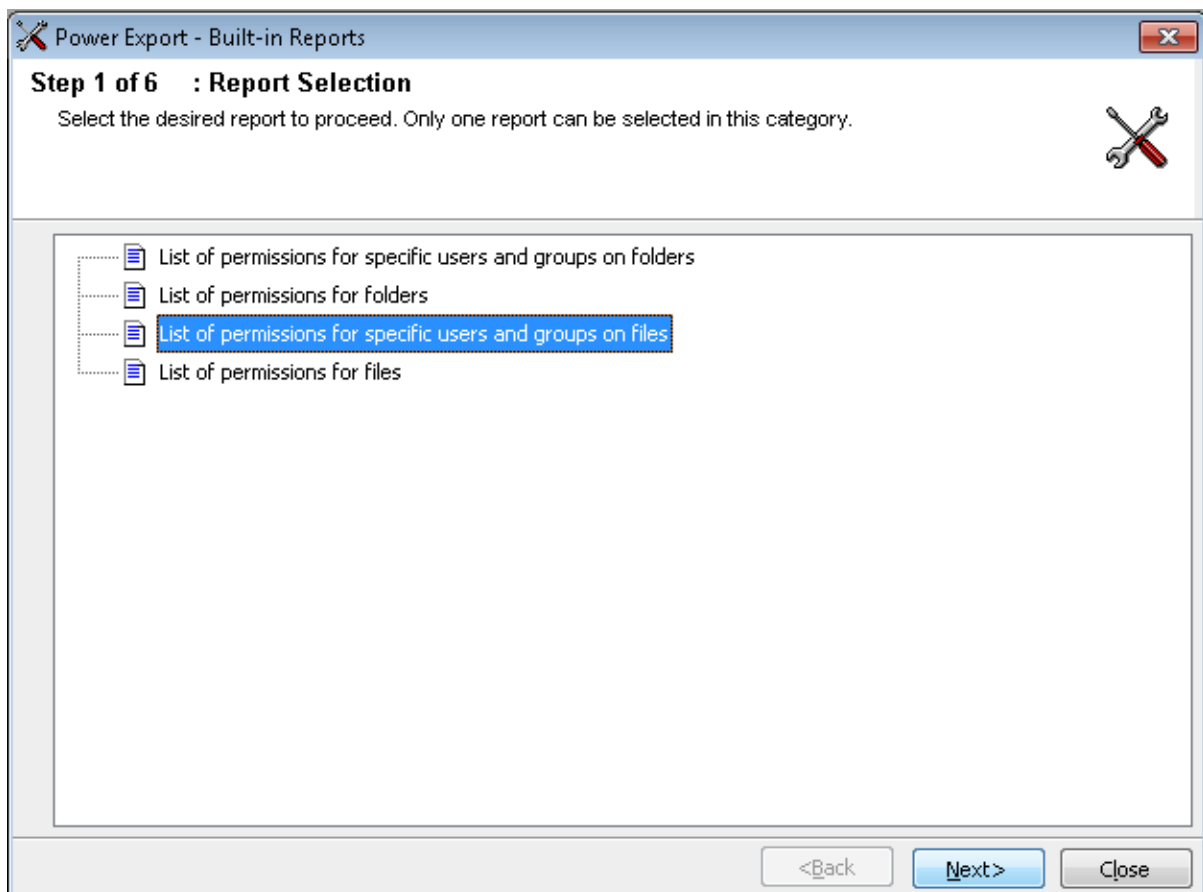
This report allows you to view file permissions for specific users and groups.



**Select** option under *Power Export*.

This will bring up the *Power Export Wizard*.

### Step 1: Report Selection



- 1) Select "**Permissions Reports**" from the select report category drop-down list.
- 2) Select the desired report. Only one report may be selected to run in a single task.
- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.



**Step 2: User and/or Group Selection**

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on files

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts



Account Name	Account Type
--------------	--------------

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on folders

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts

Account Name	Account Type
TREELAB\Administrator	User
TREELAB\adminuser1	User
TREELAB\adminuser2	User
TREELAB\adminuser3	User
TREELAB\alberto	User
TREELAB\barton	User
TREELAB\shane	User
TREELAB\tony	User

- Use **Select a Scan Profile (Users/Groups)** option to use the users and groups added in the profile. For more information on Scan Profiles, Please refer, "About Scan Profiles (Users/Groups)."

- 1) Select the user or group, for which you wish to run the permissions report.
- 2) The selected users will be added to the wizard as shown above:
- 3) Click **Next** to proceed to the *Next* step.

### Step 3: Shared Folder Selection

**Step 3 of 6 : Shared Folder Selection**

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.

Report: **List of permissions for specific users and groups on folders**

UNC Path:

Scan Profile (Shares):

Folder Path	Include sub-fold...	Folder level
\\RD50\ADMIN\$	True	All
\\RD50\ARKWE	True	All
\\RD50\C\$	True	All
\\RD50\E\$	True	All
\\RD50\new	True	All

☒ Do not display folders that have the same permissions as the parent folder

☐ Include group membership information ☐ Include SID

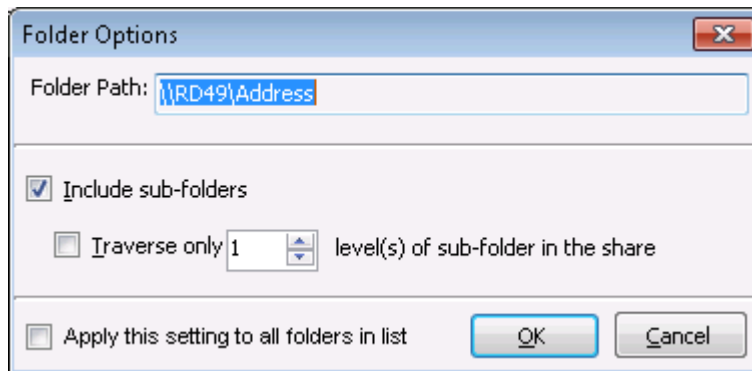
☐ Validate for Errors ☒ Include Error Details

☒ Generate report ignoring any errors found

☐ Generate report only if no errors were found. Send error report through e-mail

- 1) Select the desired folder(s) for which you wish to run the permissions report.
- 2) You may also click **Import** button to import a list of UNC folder paths from a text file.
- 3) Files that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want files with identical permissions as the parent folder reported, then select **Do not display files that have same permissions as the parent folder** option. This option will not report files with identical permissions as the parent folder.

- 4) ARKWE defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



- 5) Modify the folder options as required and click **OK**.
- 6) Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
- **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
  - **Generate report only if no error were found. Send error report through e-mail**– This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
- 7) You may select **Include Error Details** option for including the error information of folders / files into report data.
- 8) Click **Next**.

## Step 4: Delivery Options

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

To Address:

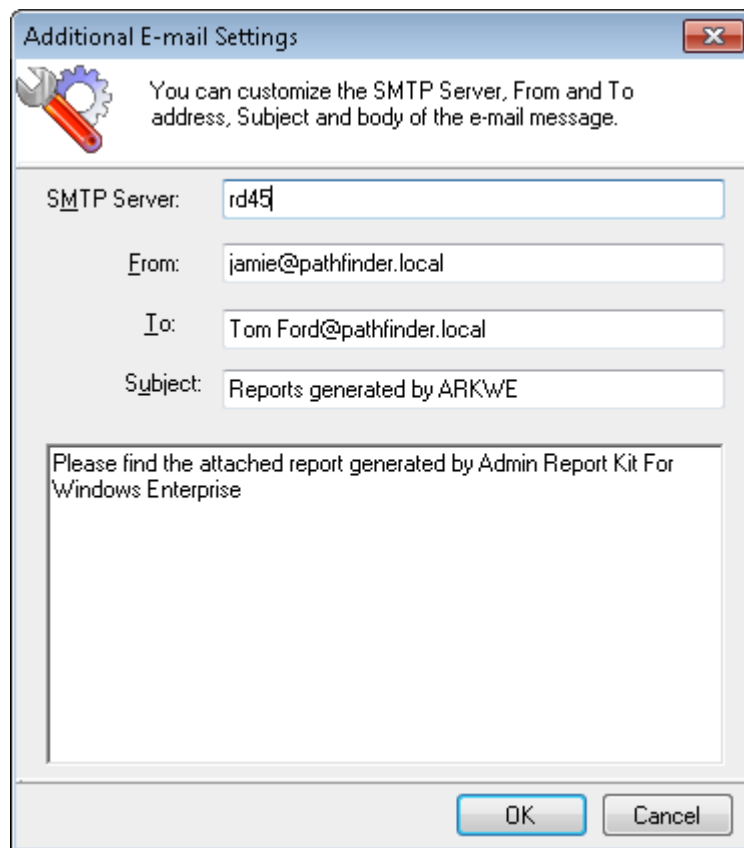
☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below:



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

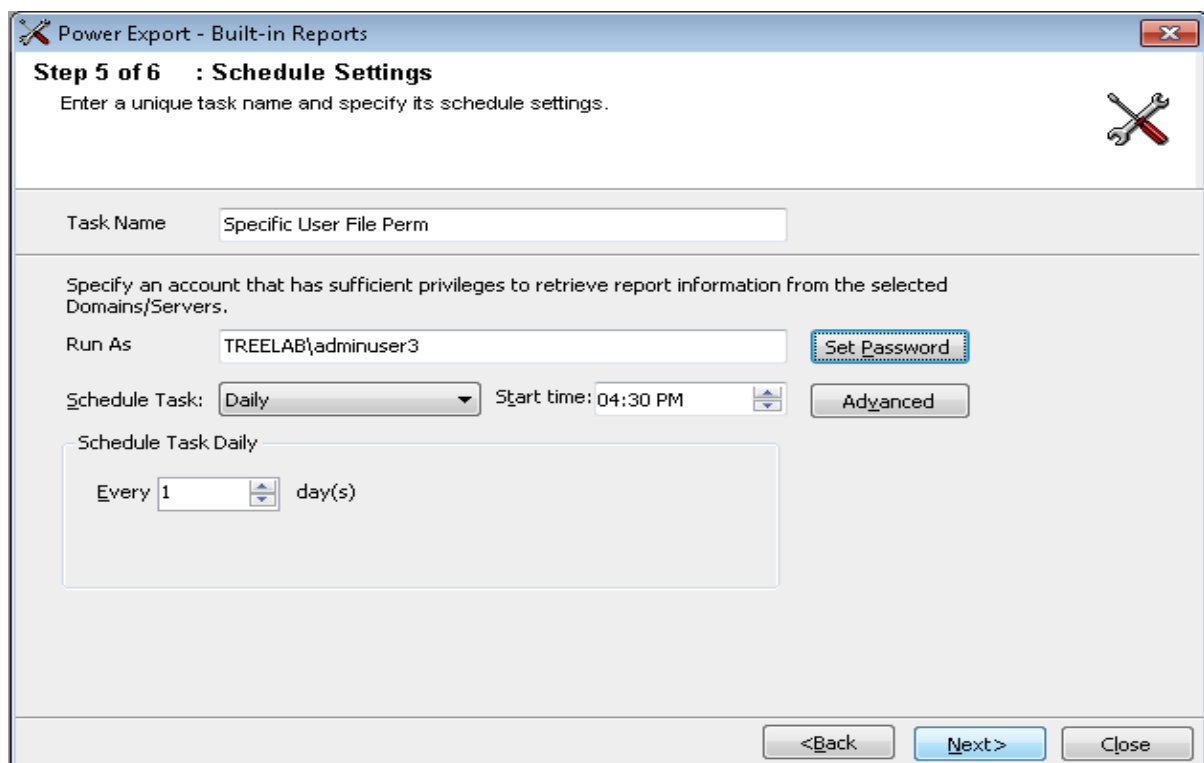
From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

### Step 5: Schedule Settings



**Power Export - Built-in Reports**

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

Schedule Task:  Start time:

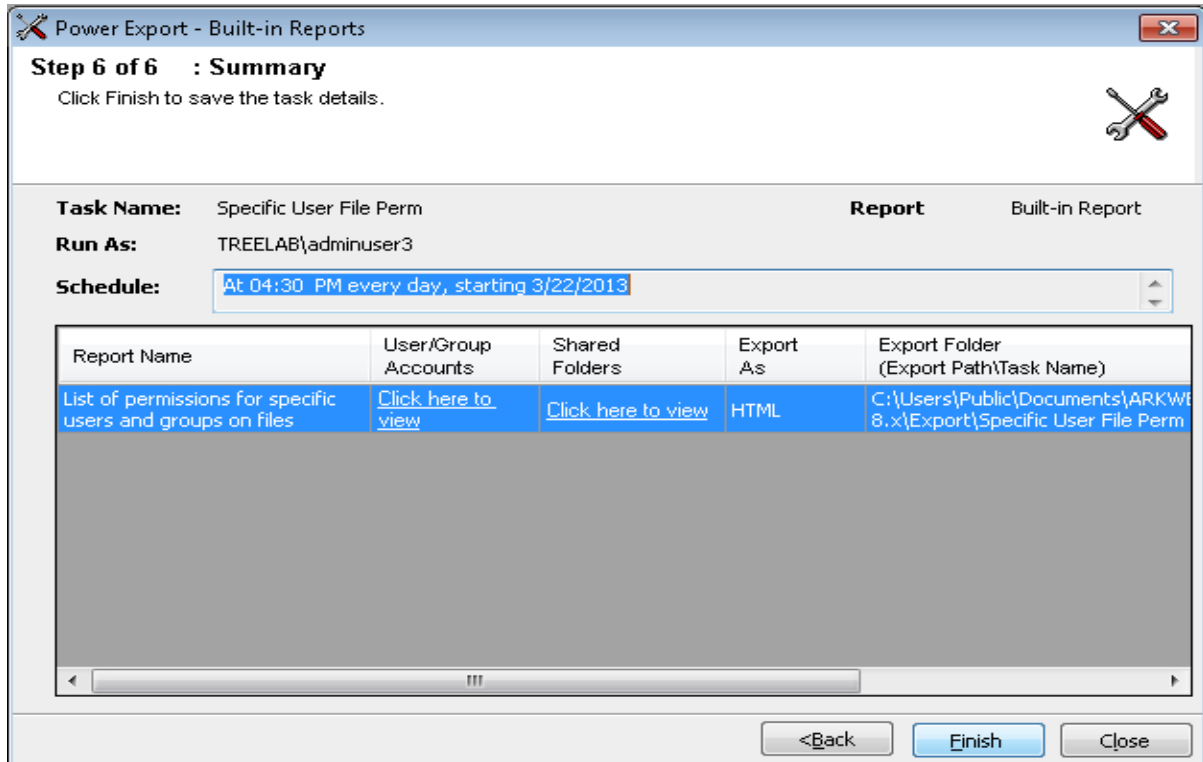
Schedule Task Daily

Every  day(s)

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.

- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

### Step 6: Summary



**Power Export - Built-in Reports**

**Step 6 of 6 : Summary**  
Click Finish to save the task details.

**Task Name:** Specific User File Perm **Report** Built-in Report

**Run As:** TREELAB\adminuser3

**Schedule:** At 04:30 PM every day, starting 3/22/2013

Report Name	User/Group Accounts	Shared Folders	Export As	Export Folder (Export Path\Task Name)
List of permissions for specific users and groups on files	<a href="#">Click here to view</a>	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKW...8.x\Export\Specific User File Perm

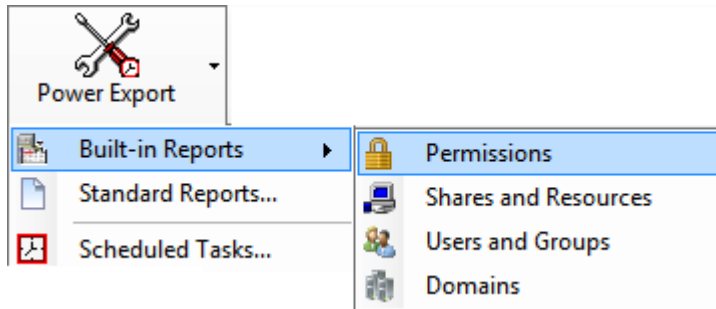
<Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Scheduled Tasks folder.

## Schedule Permissions Built-in Reports

### List of Permissions for Files

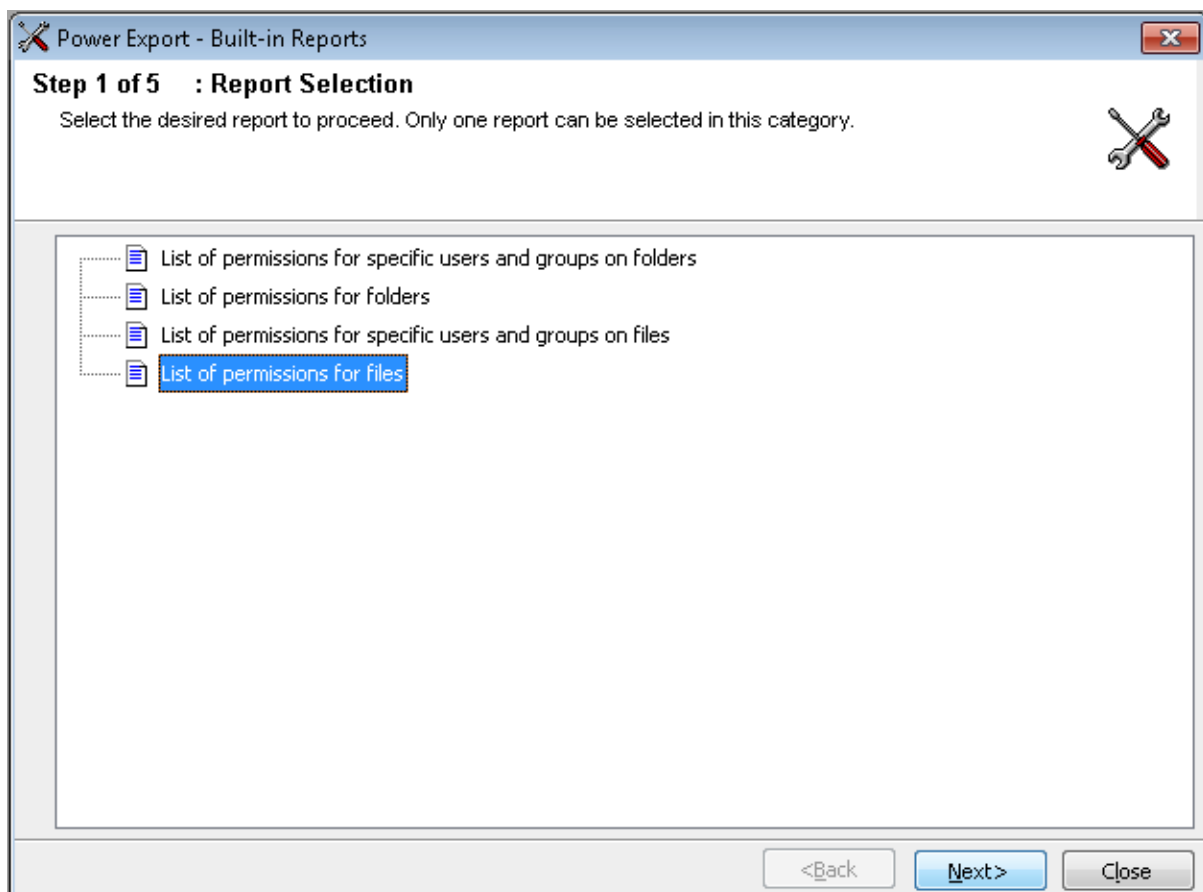
This report allows you to view the associated file permissions under a specific set of folders.



**Select** option under Power Export.

This will bring up the Power Export Wizard.

### Step 1: Report Selection



- 1) Select "**Permissions Reports**" from the select report category drop-down list.
- 2) Select the desired report. Only one report may be selected to run in a single task.

- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

## Step 2: Shared Folder Selection

**Power Export - Built-in Reports**

**Step 2 of 5 : Shared Folder Selection**

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file. Select a folder in the list below and Click Edit Folder Options to modify the default properties for scanning each folder.

Report: **List of permissions for files**

UNC Path:

Scan Profile (Shares):

Folder Path	Include sub-fold...	Folder level
\\RD50\ADMIN\$	True	All
\\RD50\ARKWE	True	All
\\RD50\C\$	True	All
\\RD50\E\$	True	All
\\RD50\new	True	All

☒ Do not display files that have the same permissions as the parent folder

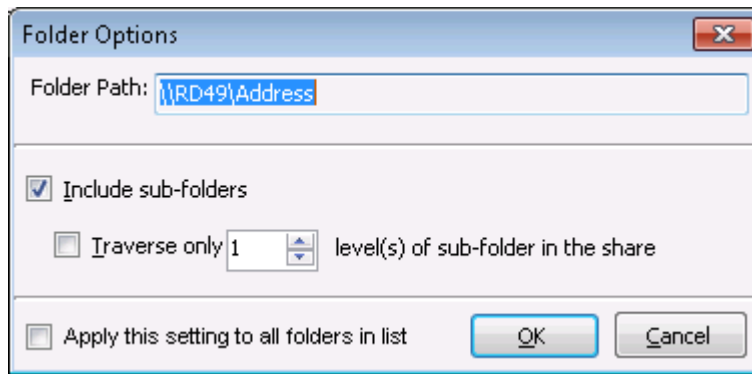
☐ Include group membership information ☐ Include SID

☐ Validate for Errors ☒ Include Error Details

☒ Generate report ignoring any errors found

☐ Generate report only if no errors were found. Send error report through e-mail

- 1) Select the desired folder(s) for which you wish to run the permissions report.
- 2) You may also click **Import** button to import a list of UNC folder paths from a text file.
- 3) Files that have identical permissions as the parent folder would show up with "Same as parent" in User Name and/or Security fields in the report. However, if you do not want files with identical permissions as the parent folder reported, then select **Do not display files that have same permissions as the parent folder** option. This option will not report files with identical permissions as the parent folder.
- 4) ARKWE defaults to scanning all the sub-folders for a given folder. If you want to modify the Include sub-folders and sub-folder level options click **Edit Folder Options** button. That will show up a window as shown below:



- 5) Modify the folder options as required and click **OK**.
- 6) Select the **Validate for Errors** option for validating the folders / files based on the folder traversal option selected, before proceeding to report generation.
  - **Generate report ignoring any errors found** – This option will validate the folders/ files path(s) and generate the report even if errors are encountered during the validation option.
  - **Generate report only if no error were found. Send error report through e-mail** – This option will validate the folders/ files path(s) and skip the report generation if errors were encountered during the validation option. It will then email the error(s) encountered during the validation process to users.
- 7) You may select **Include Error Details** for including the error information of folders / files into report data.
- 8) Click **Next** to proceed to the *Next* step.

**Step 3: Delivery Options**

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

To Address:

☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below:

**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

#### Step 4: Schedule Settings

**Power Export - Built-in Reports**

**Step 4 of 5 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

Schedule Task:  Start time:

Schedule Task Daily

Every  day(s)

- 1) Enter a unique name for the task.

- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

### Step 5: Summary

**Power Export - Built-in Reports**

**Step 5 of 5 : Summary**  
Click Finish to save the task details.

**Task Name:** File Permissions **Report:** Built-in Report

**Run As:** TREELAB\adminuser3

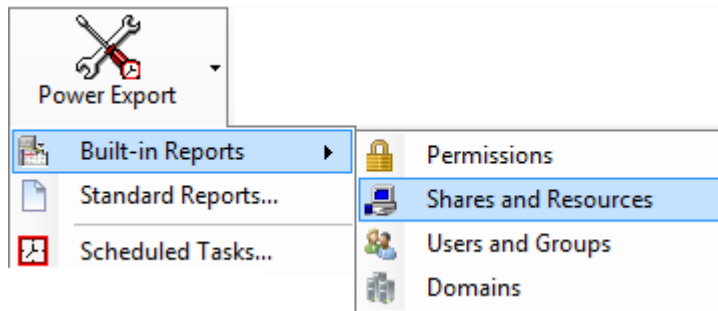
**Schedule:** At 06:30 PM every day, starting 3/22/2013

Report Name	Shared Folders	Export As	Export Folder (Export Path\Task Name)	Printer	E-m
List of permissions for files	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\File Permissions		

<Back Finish Close

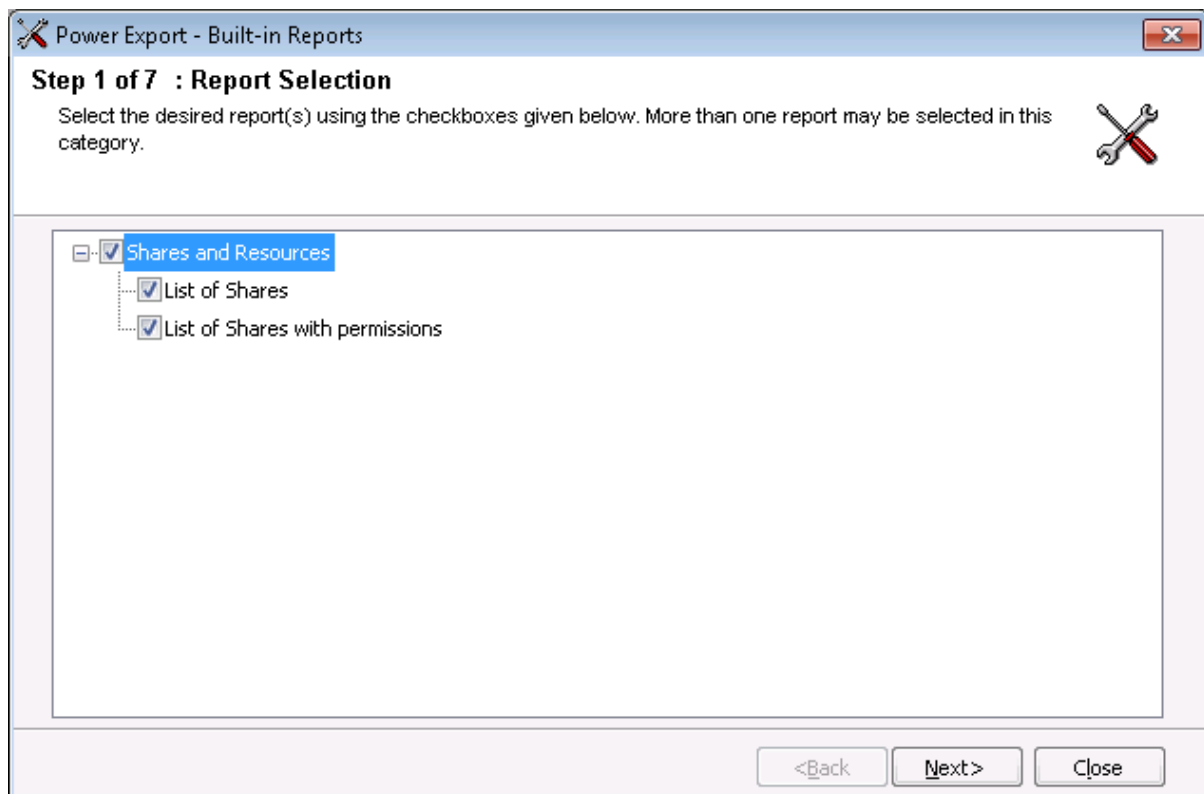
- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Scheduled Tasks folder.

## 7.5 Schedule Shares and Resources Built-in Reports



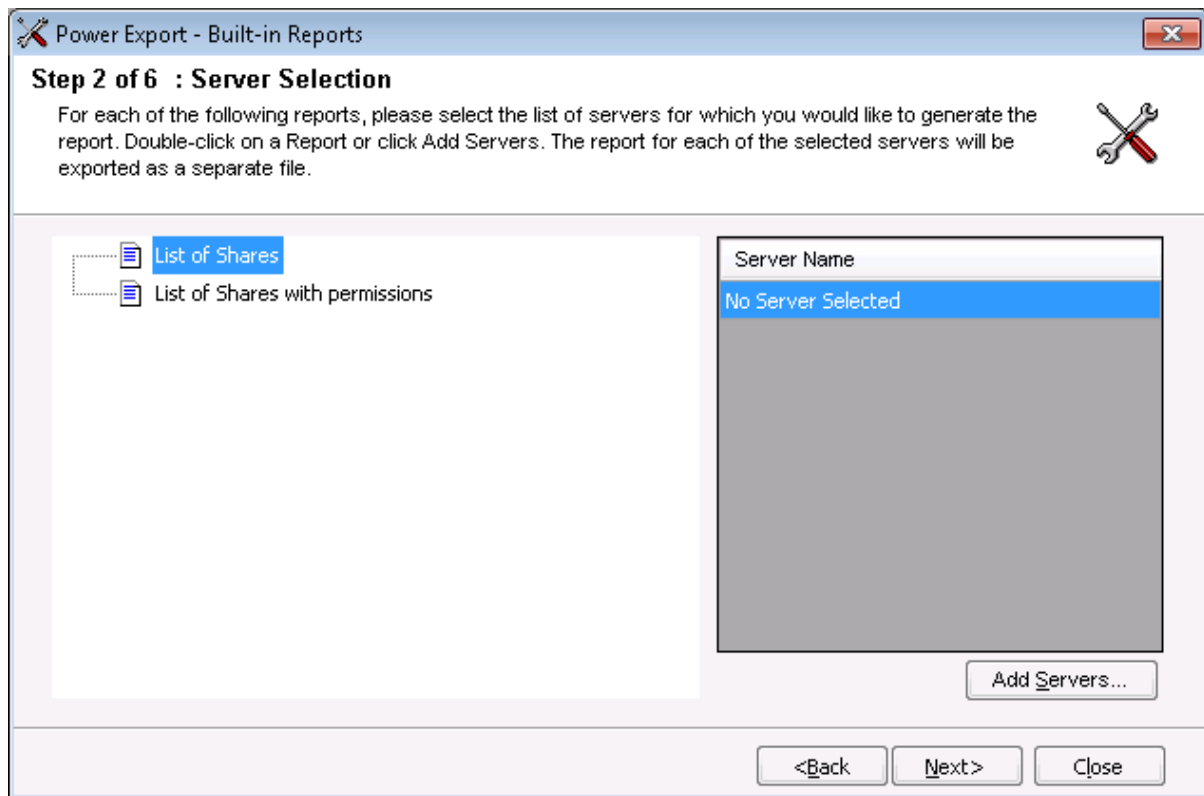
**Click** option under Power Export. This will bring up the Power Export Wizard.

### Step 1: Report Selection

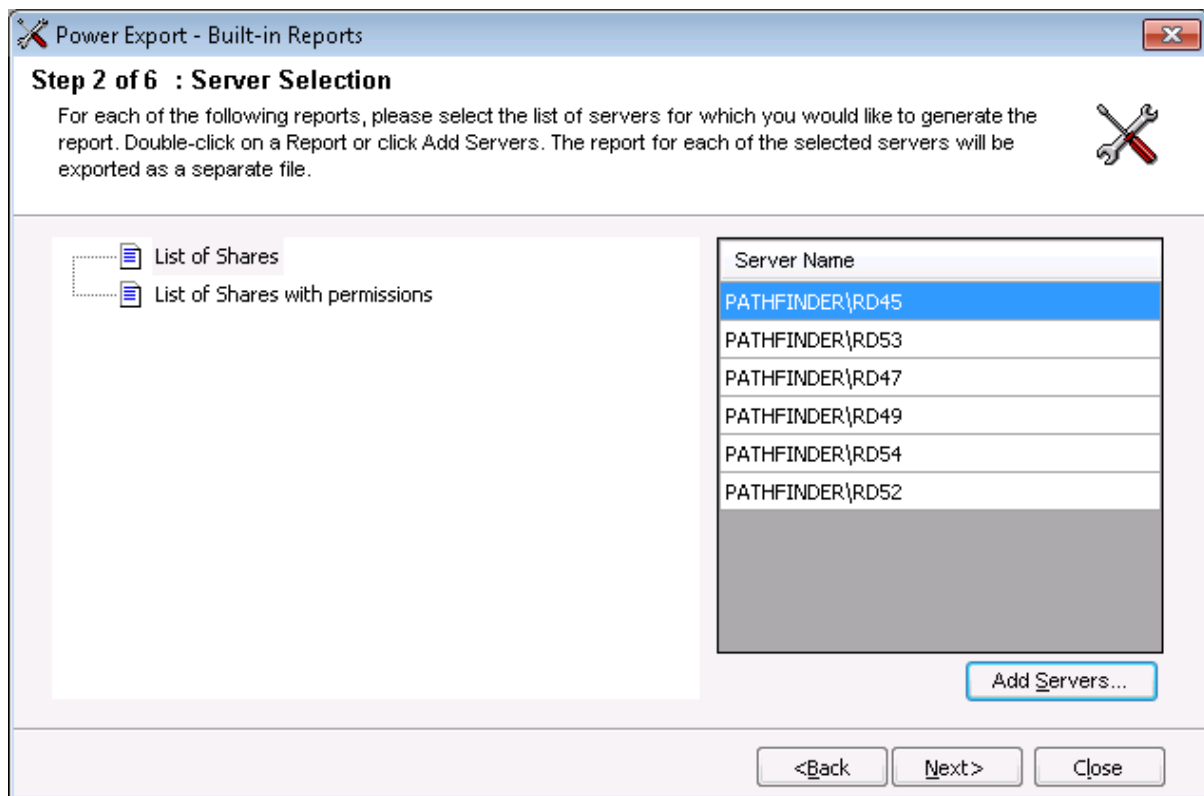


- 1) Select the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
- 2) The above reports collect data on a server-basis.
- 3) Click Next to proceed to the next step. You may Click Back button anytime to come back to a previous step.

## Step 2: Server Selection

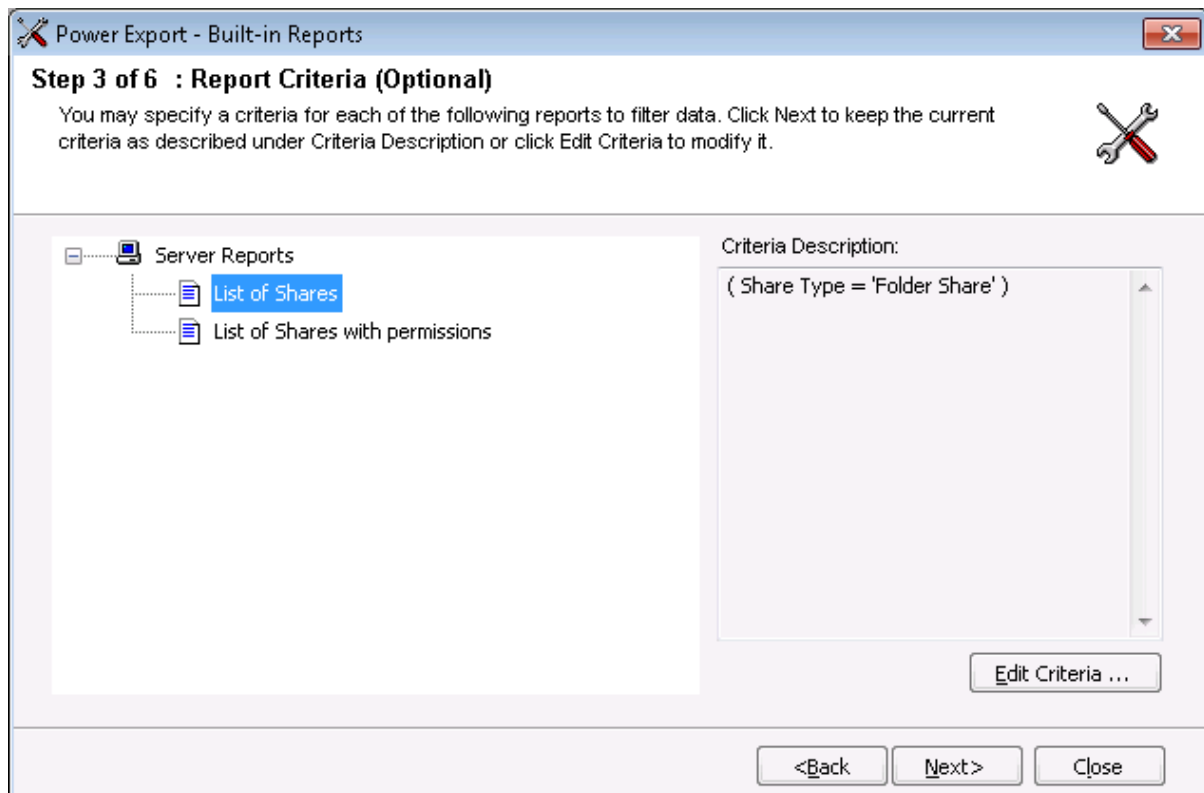


- 1) Click **Add Servers** button to select the servers for which you wish to run the server reports selected in Step 1. This will display a window where you can select the servers you want to add. Selecting a domain will add all the servers in that domain to the report.
- 2) Click **OK** to apply the selected servers to the current report or click **Apply to Reports** to apply the servers to the rest of the selected server reports. The selected servers will be added to the wizard as shown below:



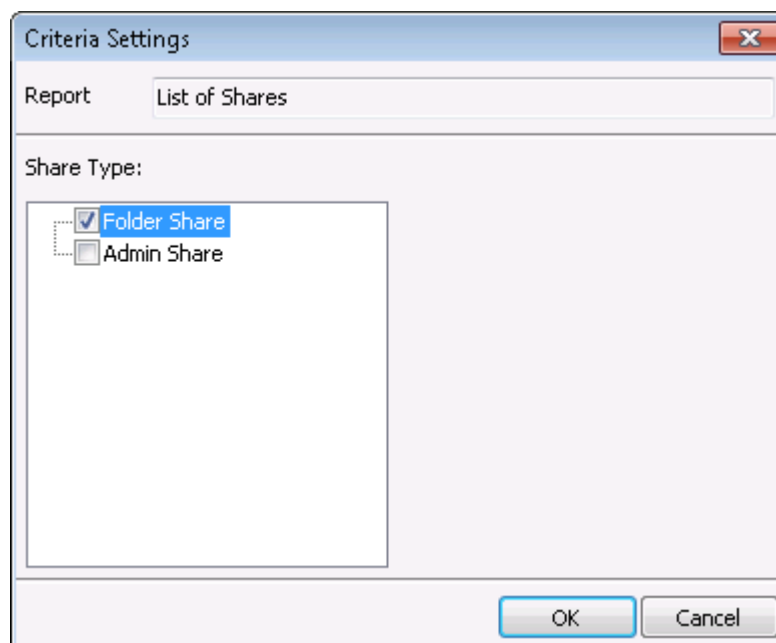
3) Click **Next** to proceed to the next step.

### Step 3: Report Criteria (Optional)

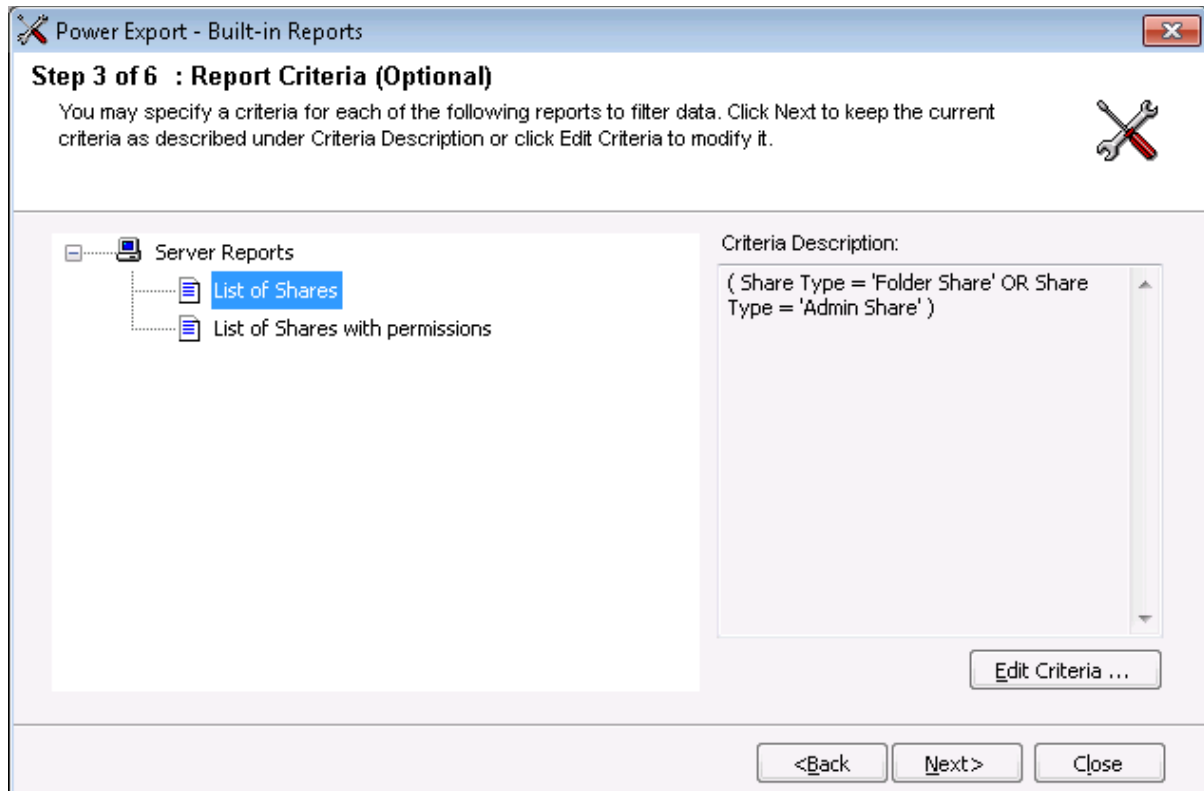


This step allows you to apply specific conditions for filtering report data.

- 1) To set criteria for a report, select a report and Click **Edit Criteria** or Double Click the report.
- 2) The Criteria Settings window will be displayed as shown below:



- 3) Specify the criteria to filter the report data using the checkboxes.
- 4) Click **OK** in Criteria Settings window to go back to the wizard.
- 5) A description of the selected criteria will be displayed under Criteria Description as shown below:



- 6) Click **Next** to proceed to the Next step.

## Step 4: Delivery Options

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ Export

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ E-mail

To Address:

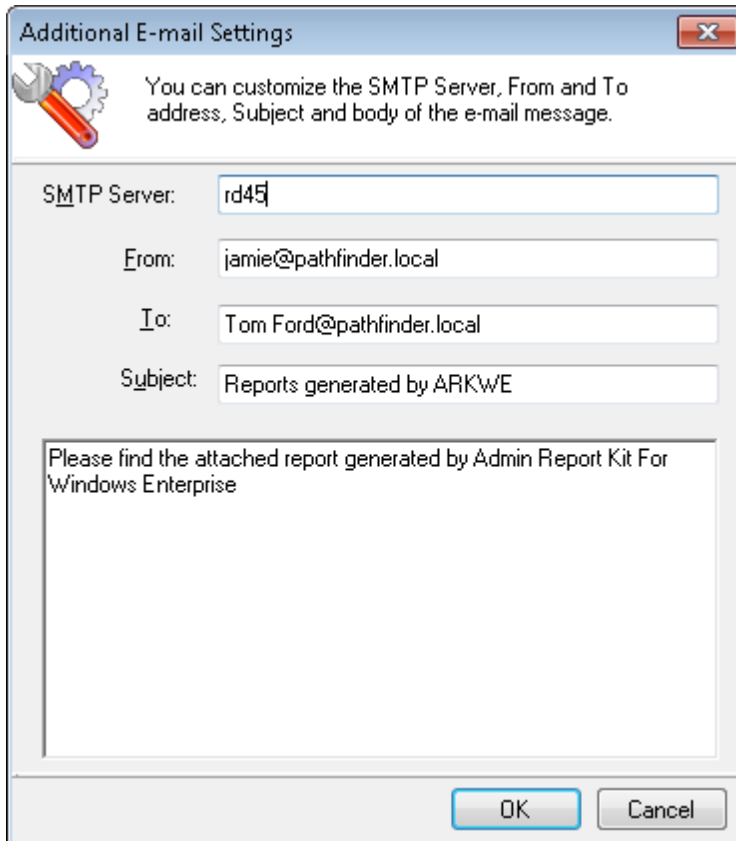
☒ Compress the attachment

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.
- 3) Click **Next** to proceed to the next step.

- Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.



The screenshot shows a Windows-style dialog box titled "Additional E-mail Settings". It features a gear icon and a message: "You can customize the SMTP Server, From and To address, Subject and body of the e-mail message." Below this, there are four text input fields: "SMTP Server:" with the value "rd45", "From:" with the value "jamie@pathfinder.local", "To:" with the value "Tom Ford@pathfinder.local", and "Subject:" with the value "Reports generated by ARKWE". At the bottom, there is a large text area containing the text "Please find the attached report generated by Admin Report Kit For Windows Enterprise". The dialog box has "OK" and "Cancel" buttons at the bottom right.

**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server: rd45

From: jamie@pathfinder.local

To: Tom Ford@pathfinder.local

Subject: Reports generated by ARKWE

Please find the attached report generated by Admin Report Kit For Windows Enterprise

OK Cancel

**Step 5: Schedule Settings**

Power Export - Built-in Reports

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name: Builtin Report Task

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As: PATHFINDER\adminuser [Set Password]

Schedule Task: Daily Start time: 01:25 PM [Advanced]

Schedule Task Daily

Every 1 day(s)

<Back Next> Close

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

## Step 6: Summary

**Power Export - Built-in Reports**

**Step 6 of 6 : Summary**  
Click Finish to save the task details.

**Task Name:** Builtin Report Task **Report** Built-in Report

**Run As:** PATHFINDER\adminuser

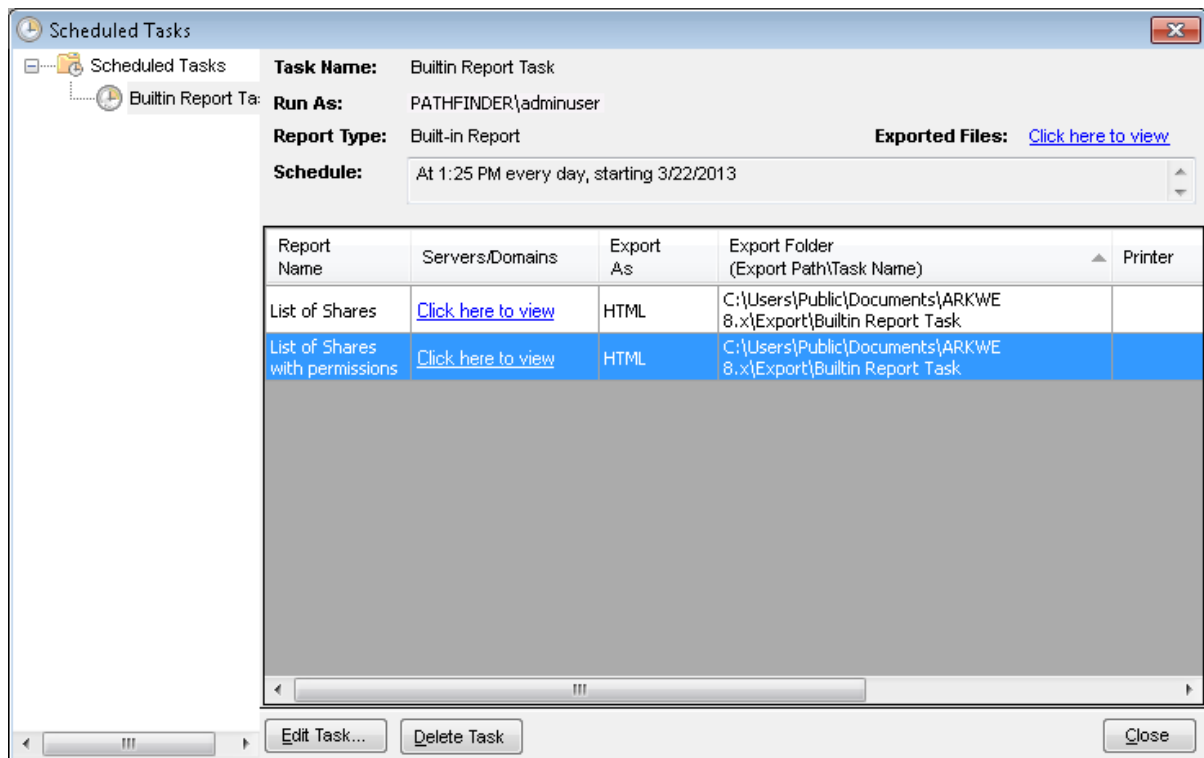
**Schedule:** At 01:25 PM every day, starting 3/22/2013

Report Name	Servers/Domains	Export As	Export Folder (Export Path\Task Name)	Printer
List of Shares	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task	
List of Shares with permissions	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task	

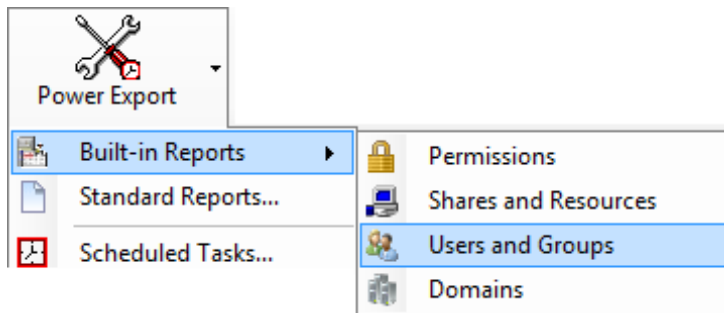
< Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.

- 3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:

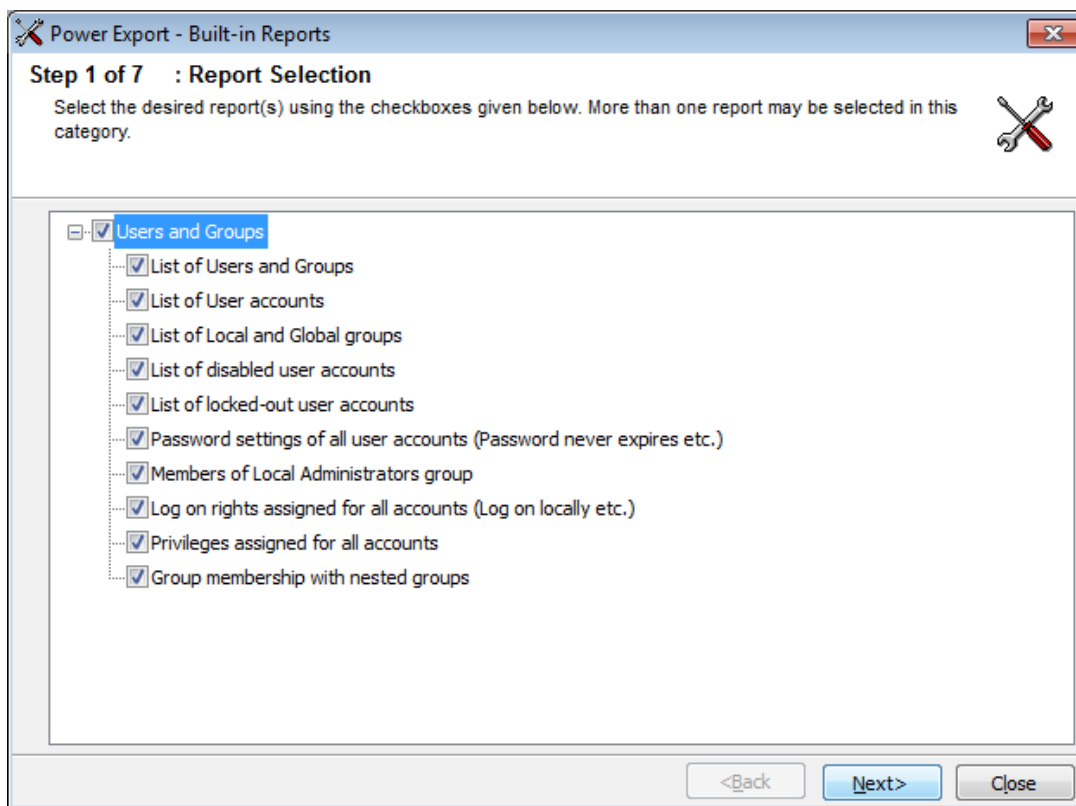


## 7.6 Schedule Users and Groups Built-in Reports



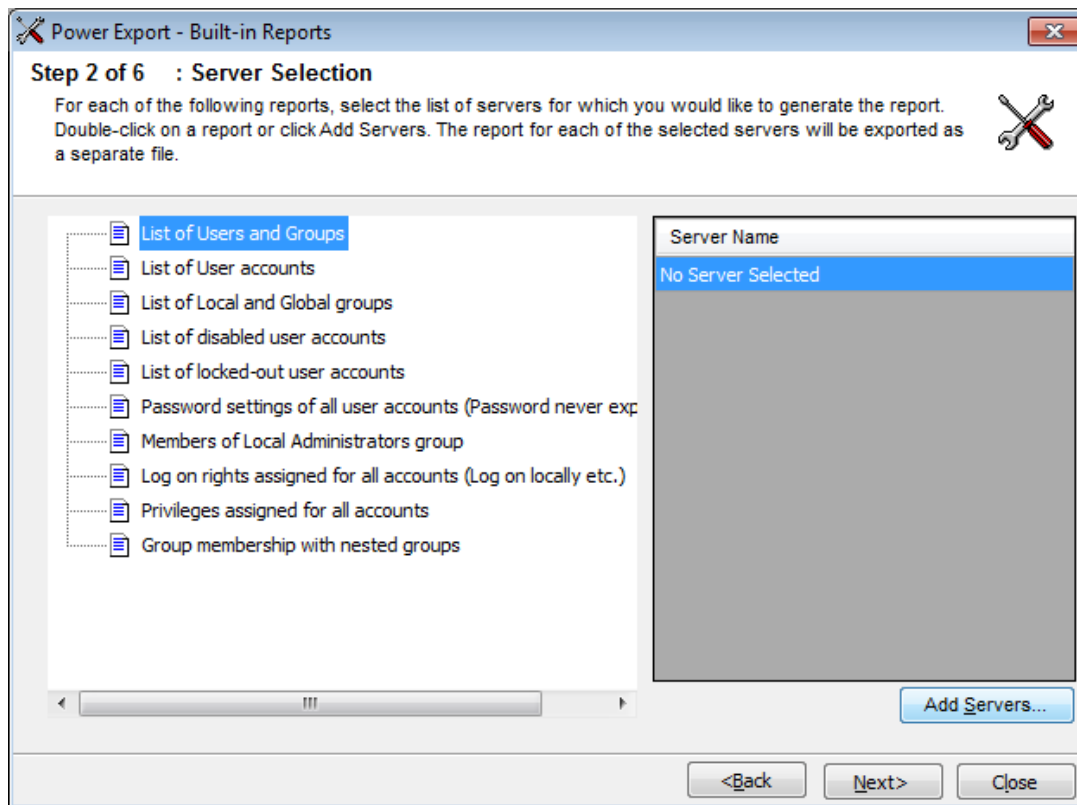
Click option under Power Export.

### Step 1: Report Selection

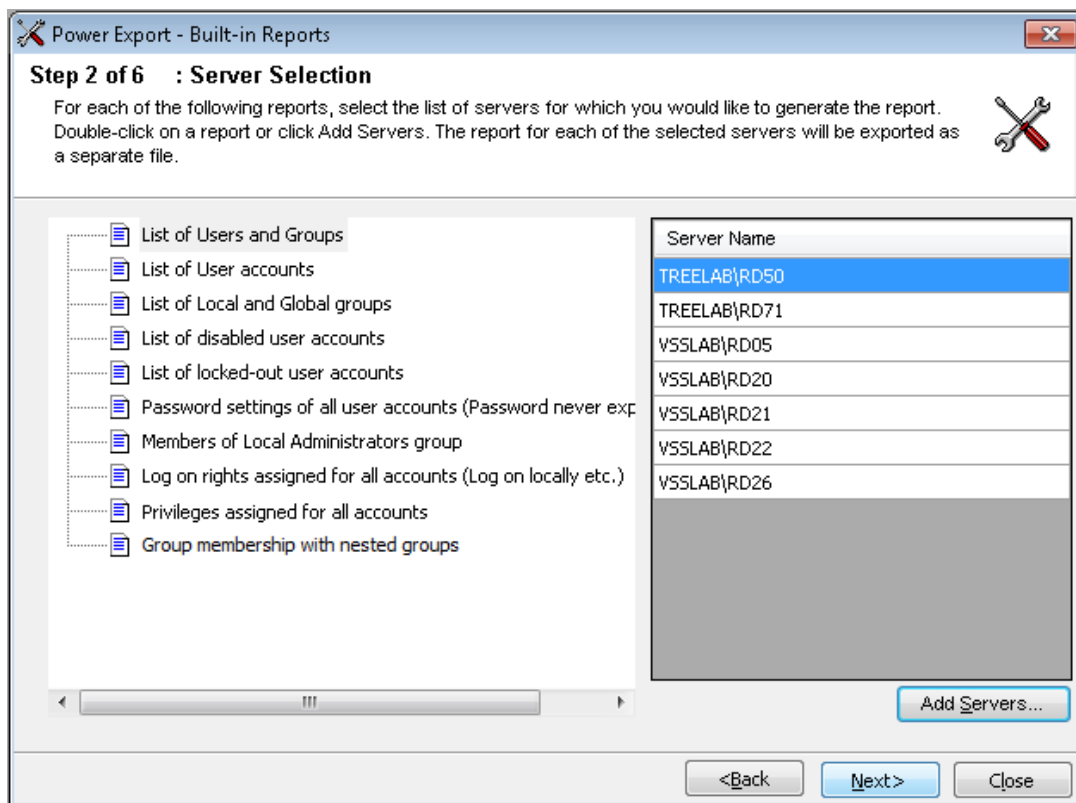


- 1) **Select** the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
- 2) The above reports collect data on a server-basis.
- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

## Step 2: Server Selection

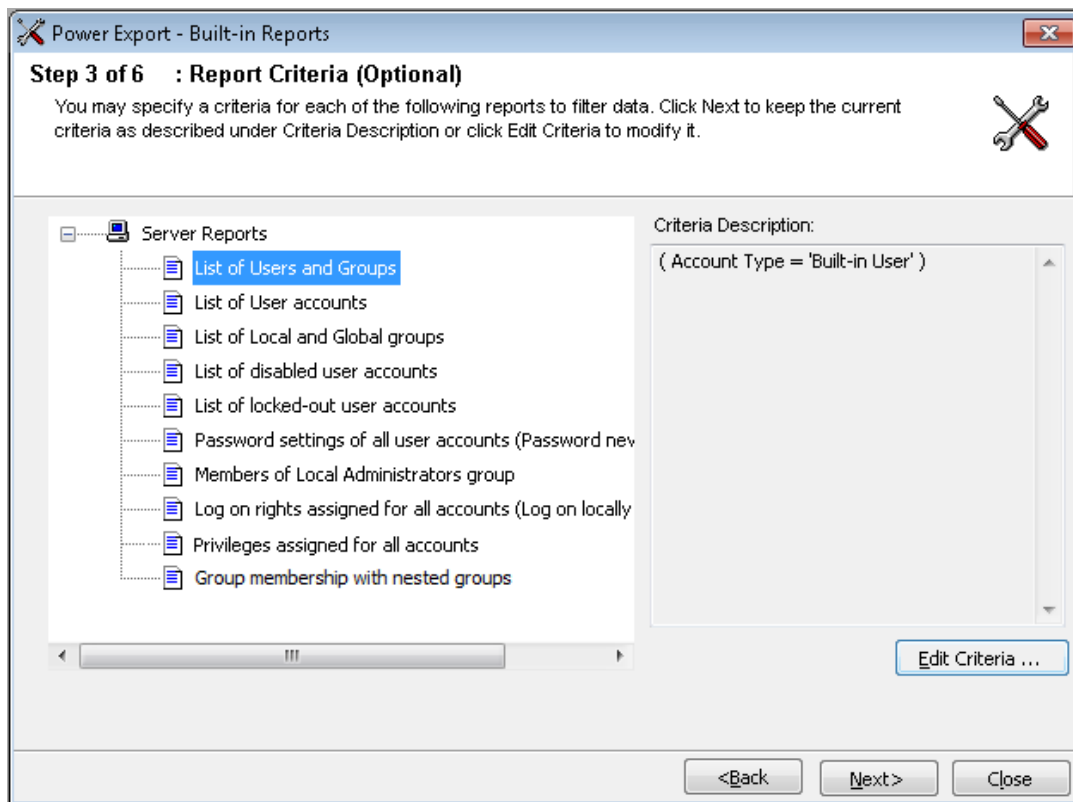


- 1) Click **Add Servers** button to select the servers for which you wish to run the server reports selected in Step 1. This will display a window where you can select the servers you want to add. Selecting a domain will add all the servers in that domain to the report.
- 2) Click **OK** to apply the selected servers to the current report or click **Apply to Reports** to apply the servers to the rest of the selected server reports. The selected servers will be added to the wizard as shown below:



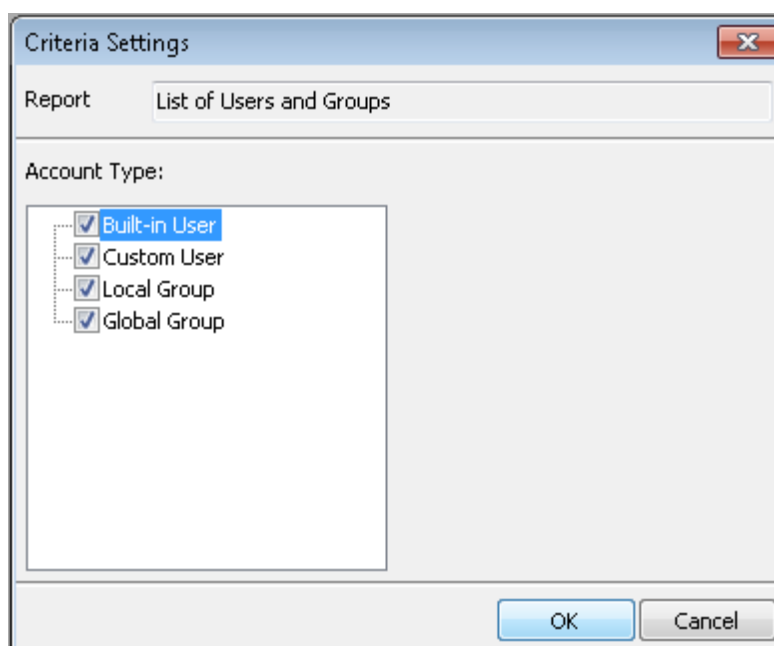
3) Click **Next** to proceed to the next Step.

### Step 3: Report Criteria (Optional)

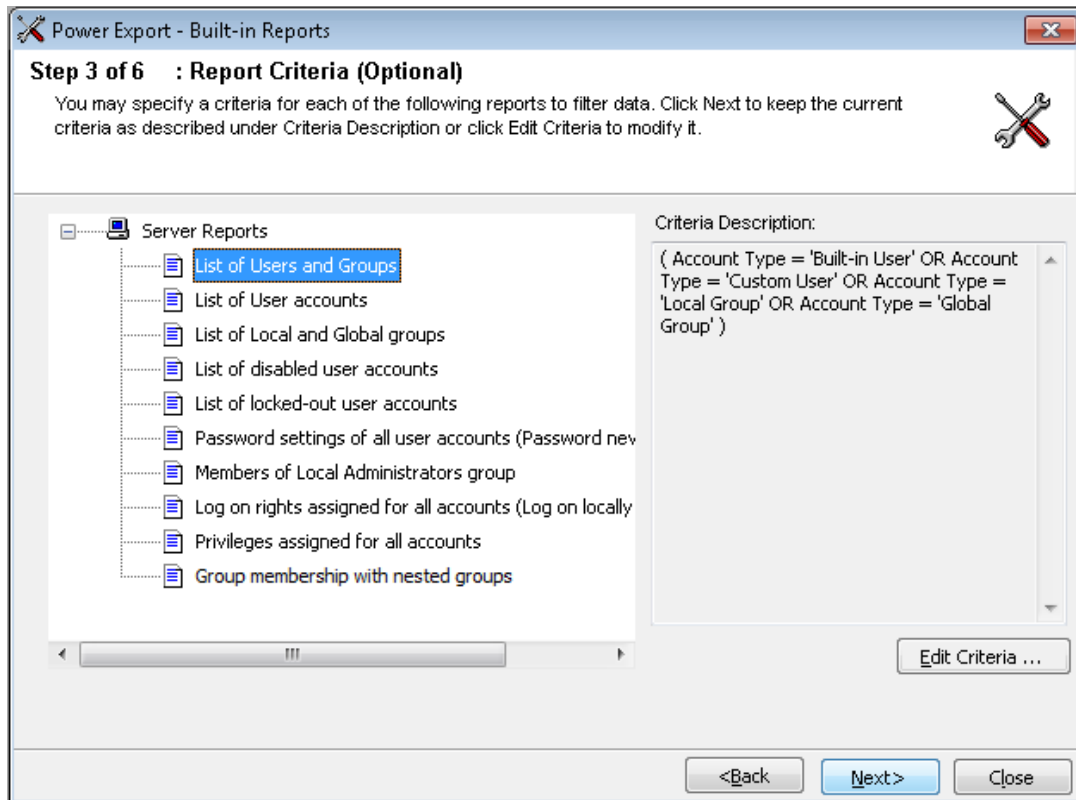


This step allows you to apply specific conditions for filtering report data.

- 1) To set criteria for a report, select a report and Click **Edit Criteria** or Double Click the report.
- 2) The Criteria Settings window will be displayed as shown below:



- 3) Specify the criteria to filter the report data using the checkboxes.
- 4) Click **OK** in Criteria Settings window to go back to the wizard.
- 5) A description of the selected criteria will be displayed under Criteria Description as shown below:



- 6) Click **Next** to proceed to the Next step.

## Step 4: Delivery Options

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

To Address:

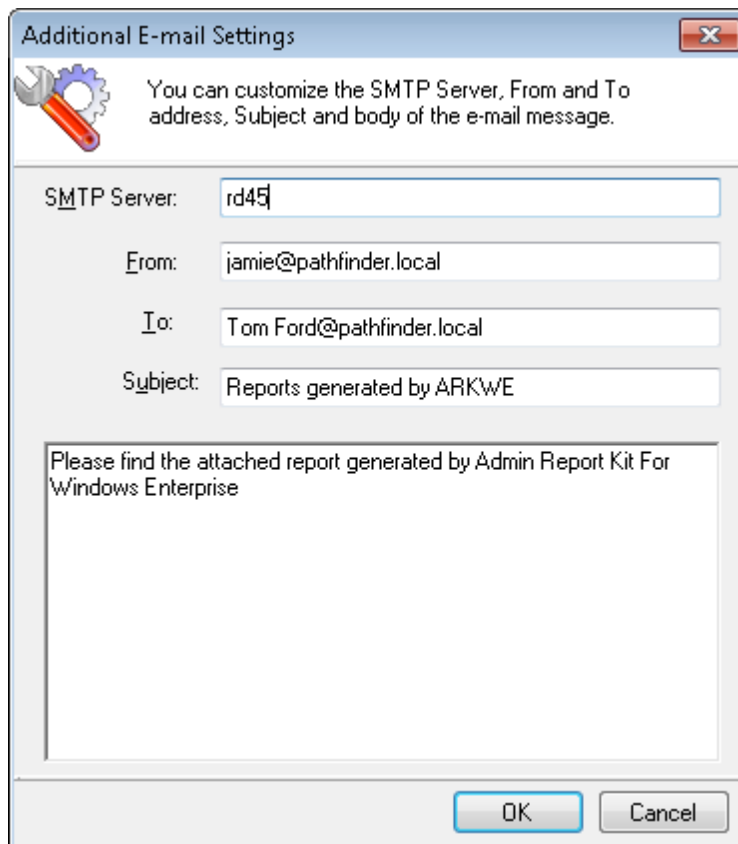
☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

- Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

OK Cancel

## Step 5: Schedule Settings

**Power Export - Built-in Reports**

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

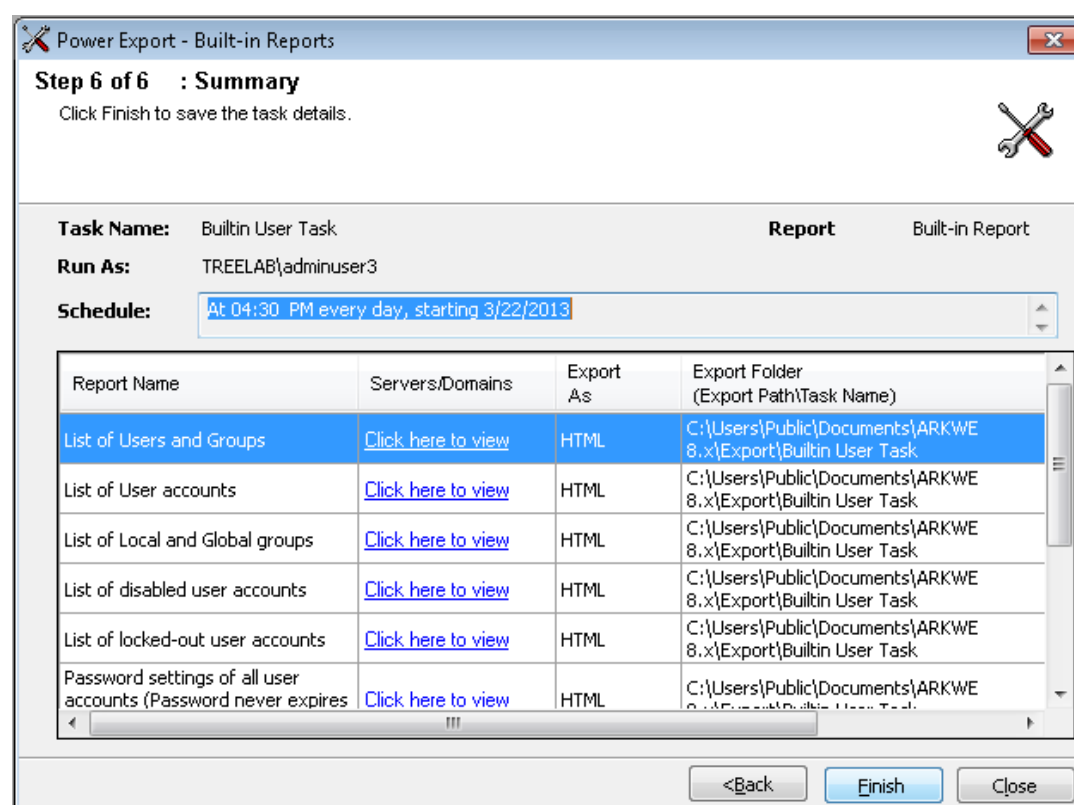
Schedule Task:  Start time:

Schedule Task Daily

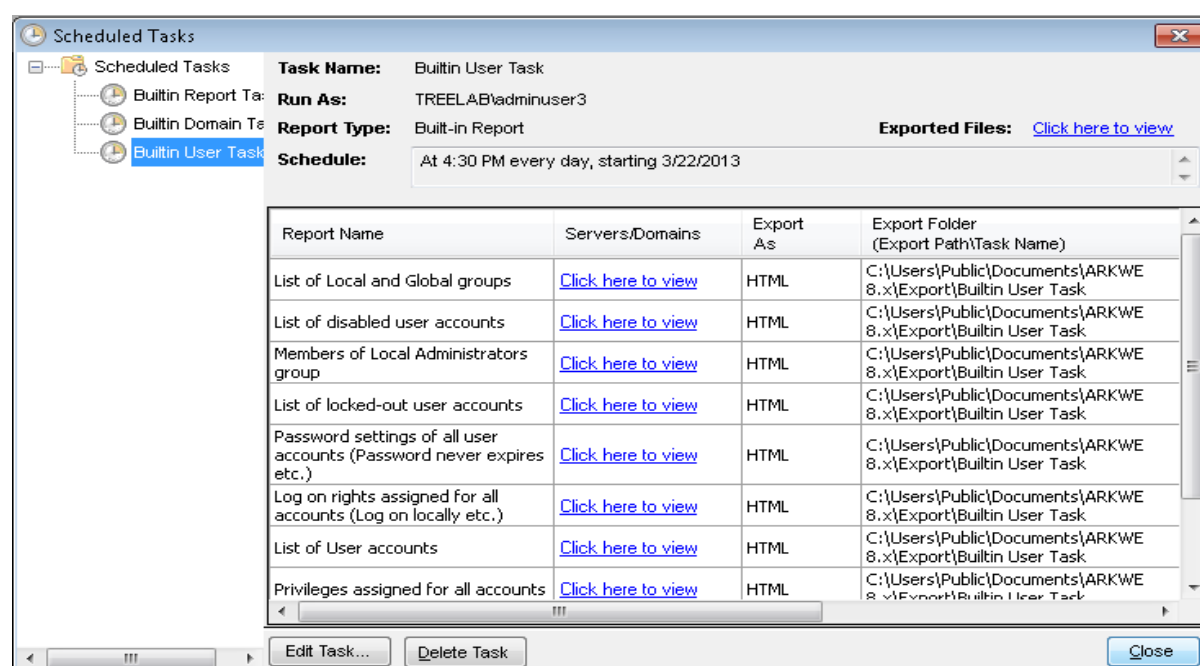
Every  day(s)

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

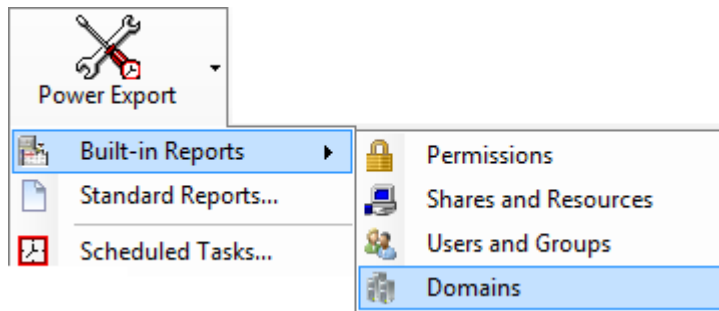
## Step 6: Summary



- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.
- 3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:



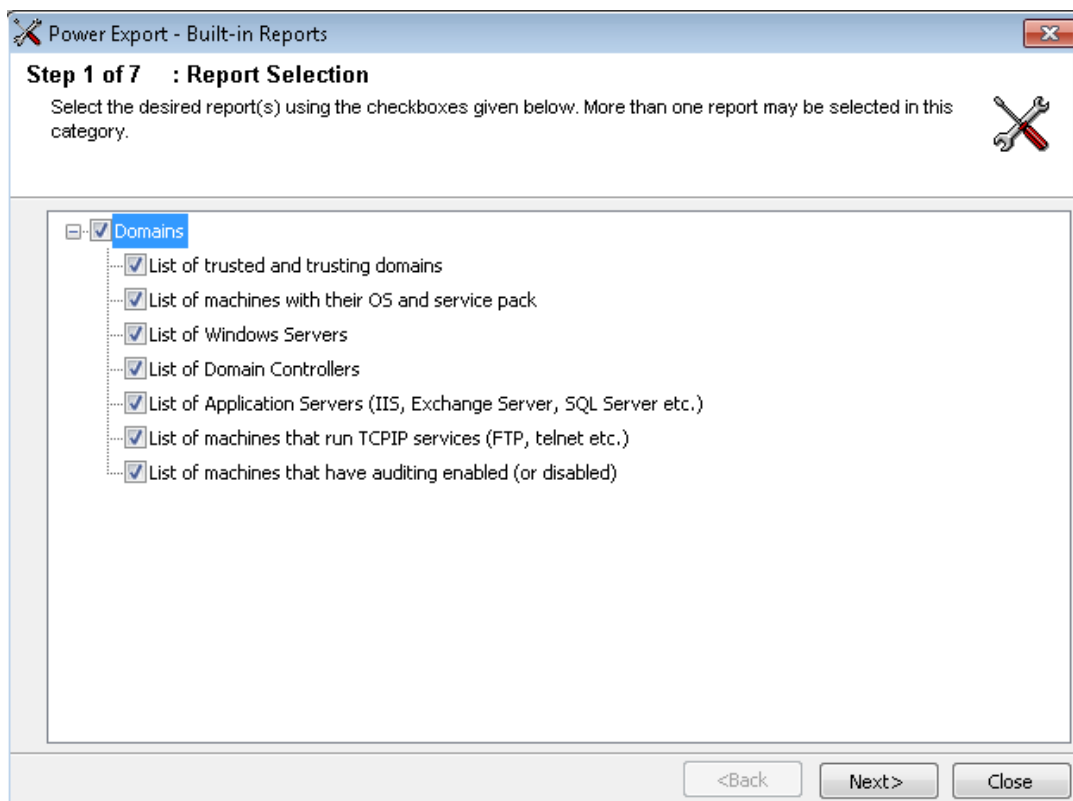
## 7.7 Schedule Domain Built-in Reports



Click **Domains** option under Power Export.

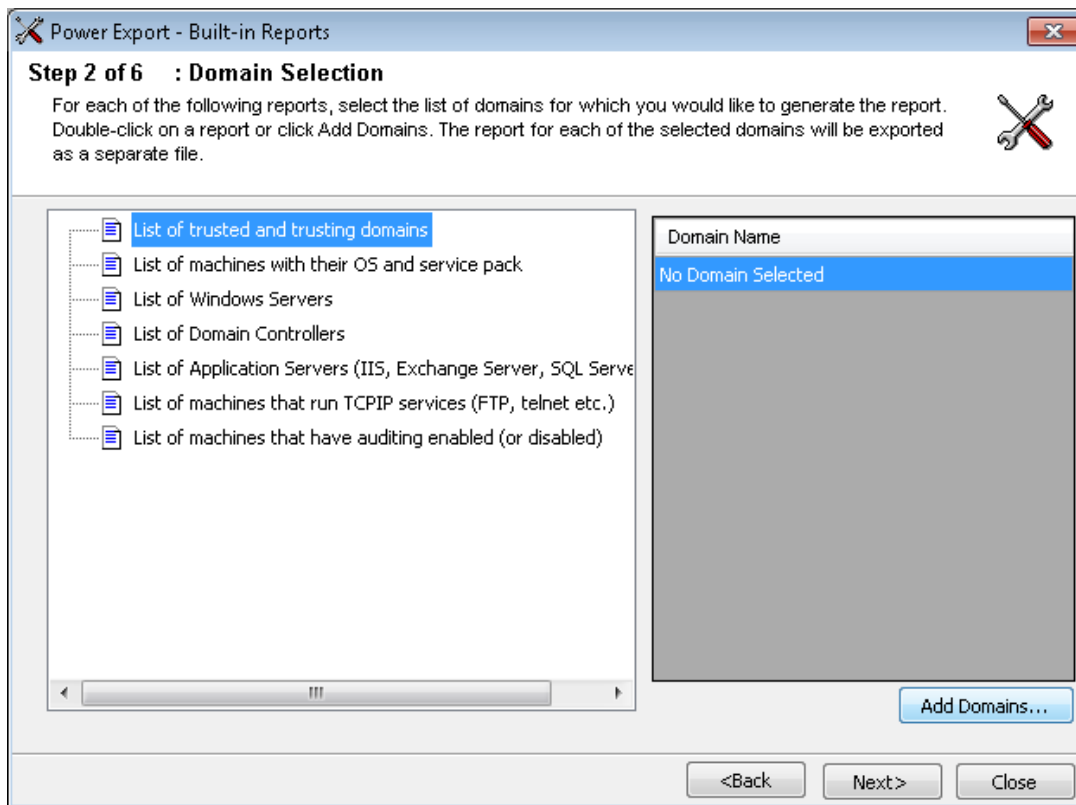
This will bring up the Power Export Wizard.

### Step 1: Report Selection

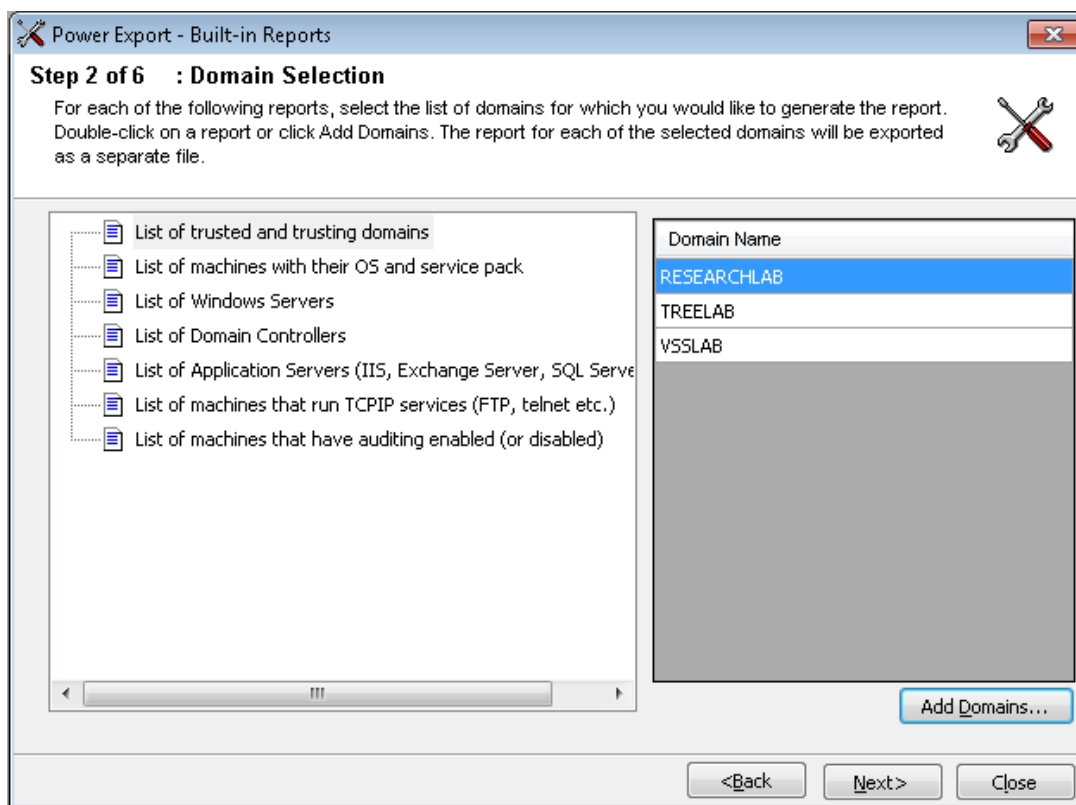


- 1) **Select** the report(s) using the checkboxes to the left of the reports. You may select any number of reports to run in a single task.
- 2) The above reports collect data for the entire domain.
- 3) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

## Step 2 Domain Selection

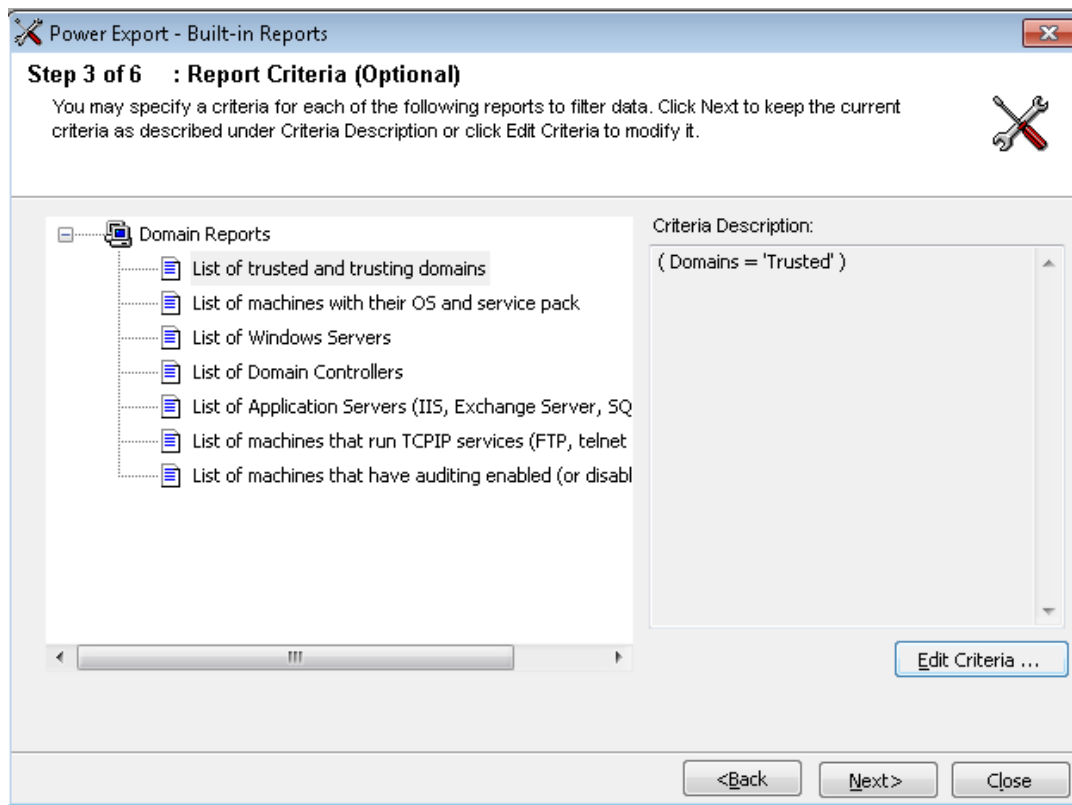


- 1) Click **Add Domains** button to select the domains for which you wish to run the domain reports selected in Step 1. This will display a window where you can select the domains you want to add.
- 2) Click **OK** to apply the selected domains to the current report or click **Apply to Reports** to apply the domains to the rest of the selected domain reports. The selected domains will be added to the wizard as shown below:



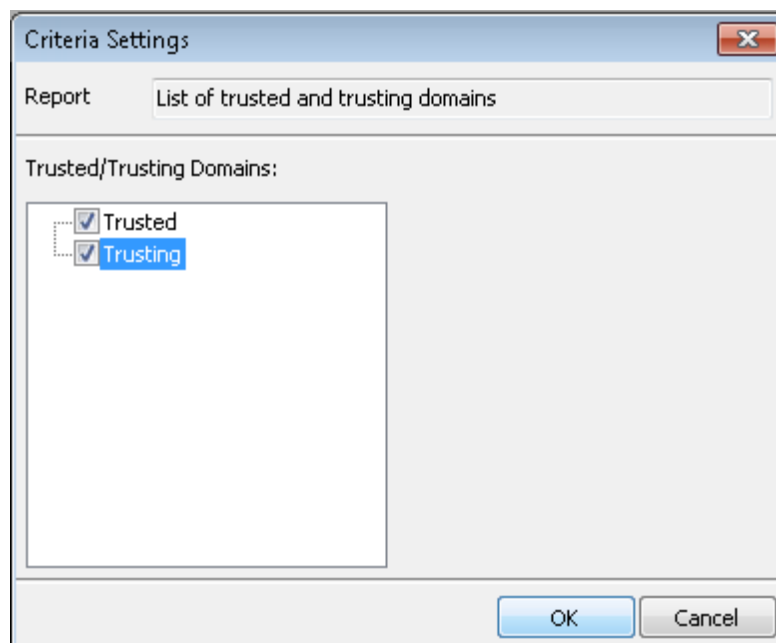
3) Click **Next** to proceed to the next Step.

### Step 3: Report Criteria (Optional)

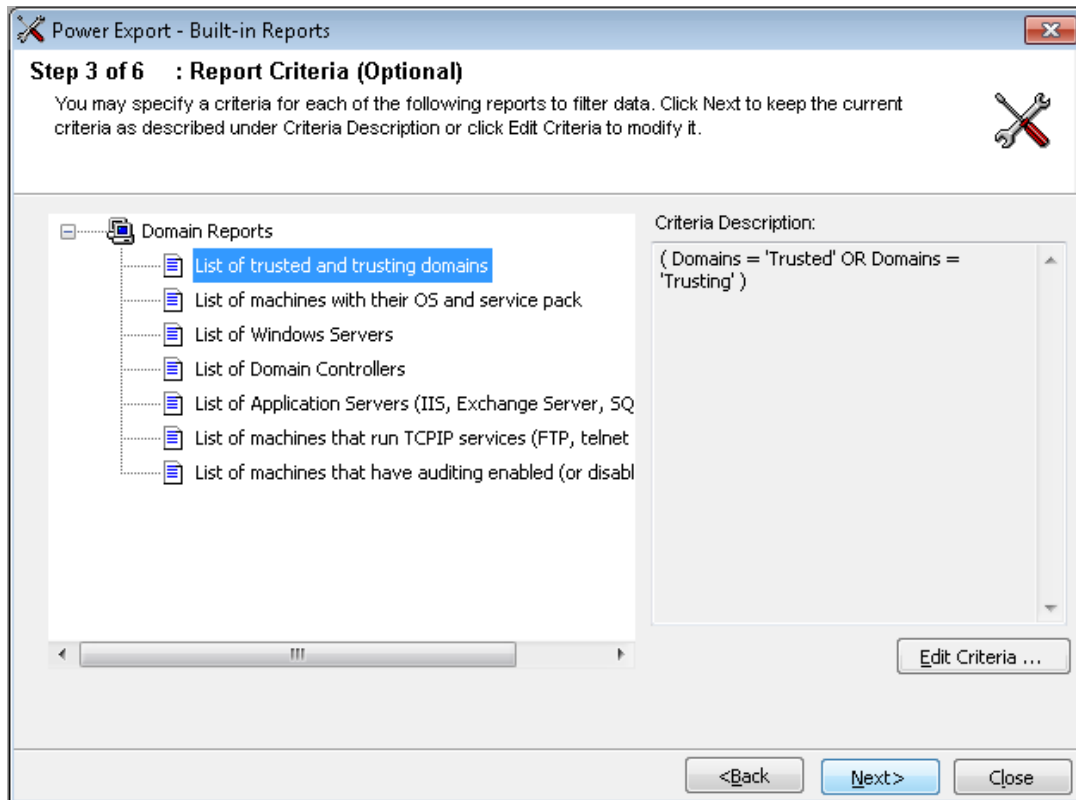


This step allows you to apply specific conditions for filtering report data.

- 1) To set a criterion for a report, select a report and Click **Edit Criteria** or Double Click the report.
- 2) The Criteria Settings window will be displayed as shown below:



- 3) Specify the criteria to filter the report data using the checkboxes.
- 4) Click **OK** in Criteria Settings window to go back to the wizard.
- 5) A description of the selected criteria will be displayed under Criteria Description as shown below:



- 6) Click **Next** to proceed to the Next step.

## Step 4: Delivery Options

**Power Export - Standard Reports**

**Step 4 of 6 : Delivery Options**

Select the report delivery options. You can Export and E-mail the reports using the options below. In case of export option, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the task name folder.

Export Type: **HTML**

☒ **Export**

Export Path : C:\Users\Public\Documents\ARKWE 8.x\Export

☐ **E-mail**

To Address:

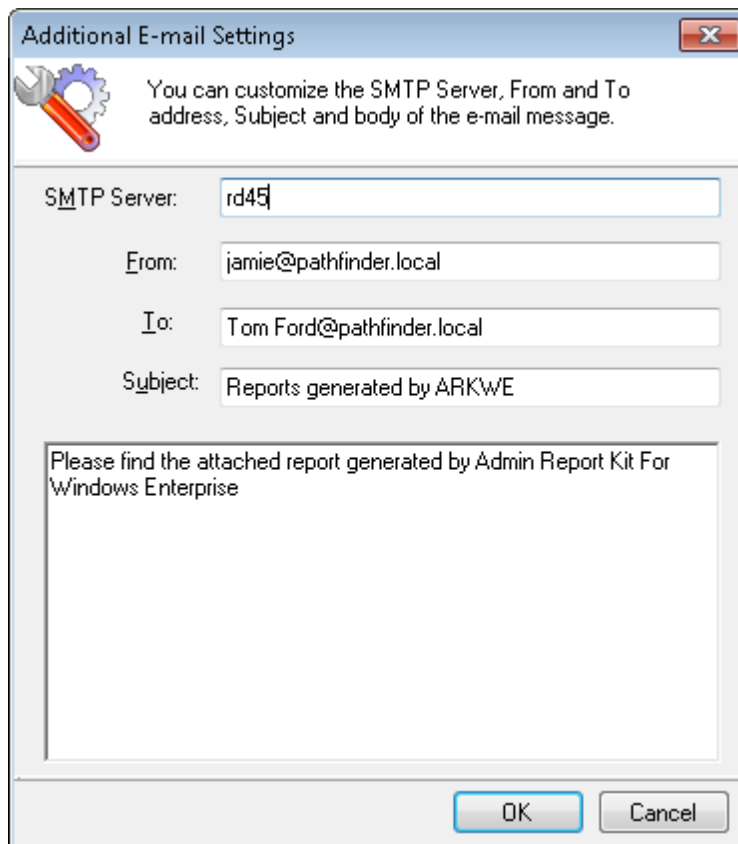
☒ **Compress the attachment**

**Note: This evaluation version exports / e-mails only the first 10 records.**

<Back Next> Close

- 1) Change the Export or E-mail settings as necessary.
- 2) Use Browse button to change the export path.

- Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below.



**Additional E-mail Settings**

You can customize the SMTP Server, From and To address, Subject and body of the e-mail message.

SMTP Server:

From:

To:

Subject:

Please find the attached report generated by Admin Report Kit For Windows Enterprise

OK Cancel

## Step 5: Schedule Settings

**Power Export - Built-in Reports**

**Step 5 of 6 : Schedule Settings**

Enter a unique task name and specify its schedule settings.

Task Name:

Specify an account that has sufficient privileges to retrieve report information from the selected Domains/Servers.

Run As:

Schedule Task:  Start time:

Schedule Task Daily

Every

- 1) Enter a unique name for the task.
- 2) Change the Run as parameter, if necessary and set the password for the specified user.
- 3) Change the task schedule settings as required.
- 4) Click **Next** to proceed to the next and final step.

## Step 6: Summary

**Power Export - Built-in Reports**

**Step 6 of 6 : Summary**  
Click Finish to save the task details.

**Task Name:** Built-in Domain Task **Report:** Built-in Report

**Run As:** TREELAB\adminuser3

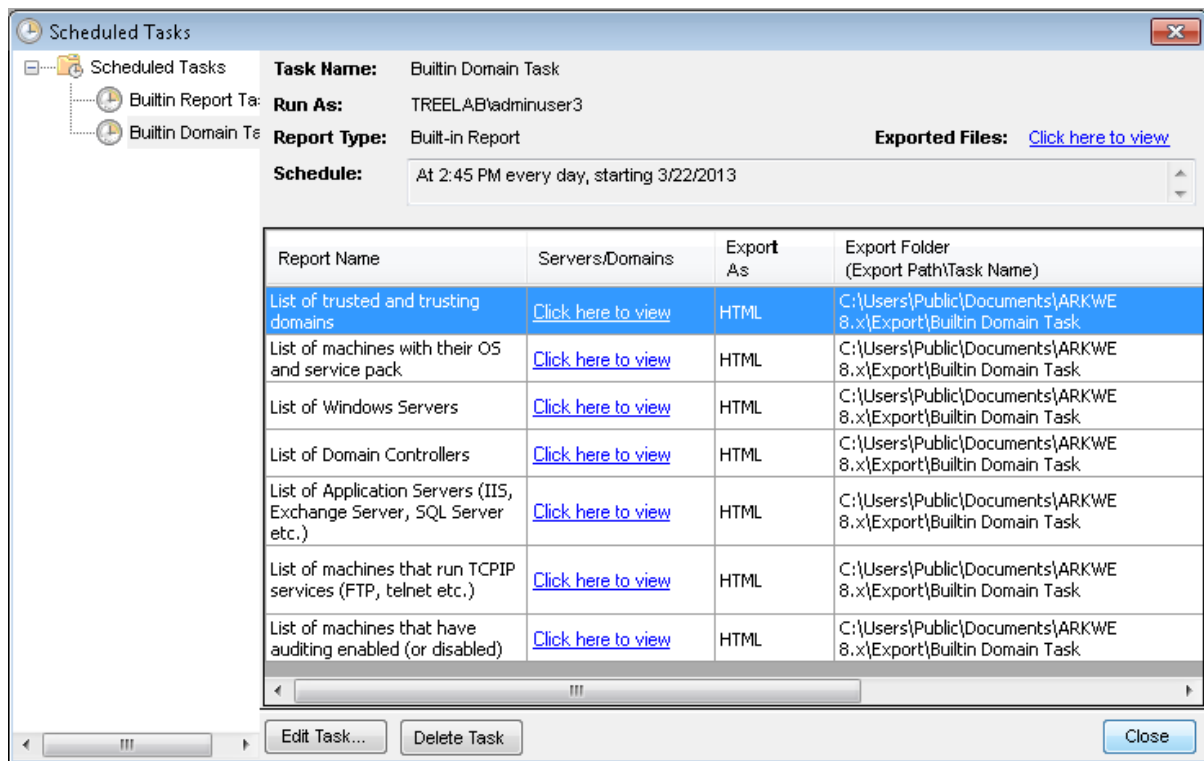
**Schedule:** At 02:45 PM every day, starting 3/22/2013

Report Name	Servers/Domains	Export As	Export Folder (Export Path\Task Name)
List of trusted and trusting domains	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task
List of machines with their OS and service pack	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task
List of Windows Servers	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task
List of Domain Controllers	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task
List of Application Servers (IIS, Exchange Server, SQL Server etc.)	<a href="#">Click here to view</a>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task
List of machines that use TCP/IP			C:\Users\Public\Documents\ARKWE 8.x\Export\Built-in Domain Task

<Back Finish Close

- 1) This step displays the summary information of the task.
- 2) Click **Finish** to save the task details.

- 3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:



## 8 Scan Profiles Manager

---

### 8.1 About Scan Profiles (Computers)

---

You can setup Scan Profiles to scan a subset of computers in the network and save these profiles for repeated use while generating reports (useful for repeatedly scanning and reporting on different subsets of computers).

You can create Scan Profiles in one of the following ways:

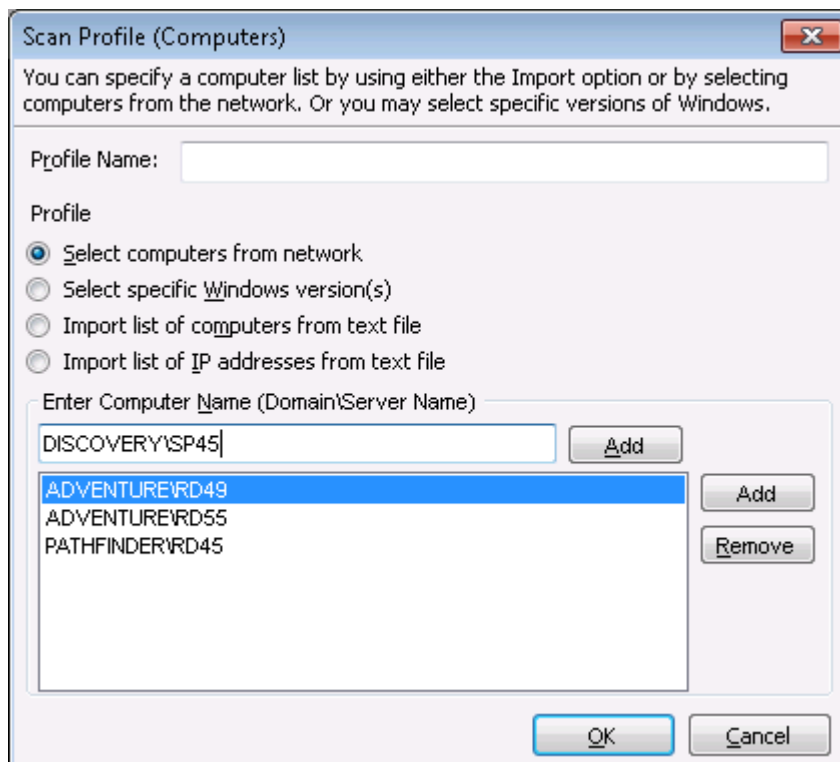
- Selecting specific computers in the network
- Selecting specific Windows versions
- Importing list of computers from a text file
- Importing list of IP addresses from a text file

## 8.2 How to Create Scan Profiles (Computers)?

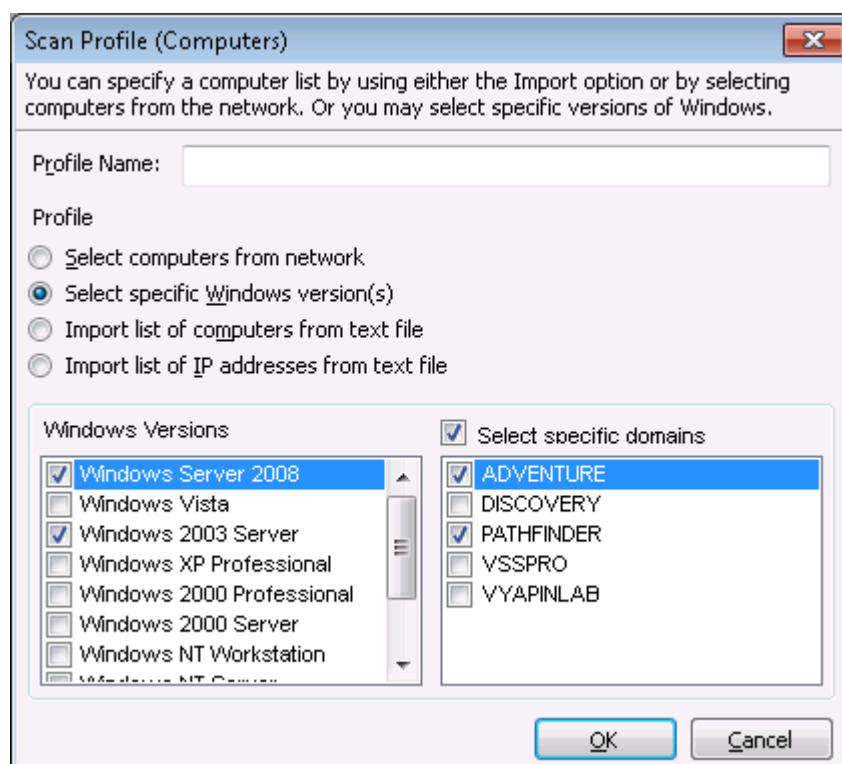
The Scan Profile Dialog allows you to create or edit a Scan Profile. During edit operation, the name of a Scan Profile and its type cannot be modified. You can access the Scan Profile Dialog from the Scan Profiles Manager.

Perform the following steps to create a Scan Profile.

- 1) **Click New** button in the Scan Profiles Manager window. The Scan Profile dialog will show up on screen.
- 2) **Specify** a name for the Scan Profile. You must give a unique name for the Scan Profile.
- 3) **Specify** how you want to create the profile by selecting appropriate profile type. You can create Scan Profiles in one of the following ways:
  - A. Selecting computers from network



- I. **Select computers from network option.**
  - II. You can type in computer name, in the format "Domain Name\Computer Name", and then click Add button to manually add it to the list. Or you may click **Add from** button to browse the network and select specific computers.
- B. Selecting specific Windows versions

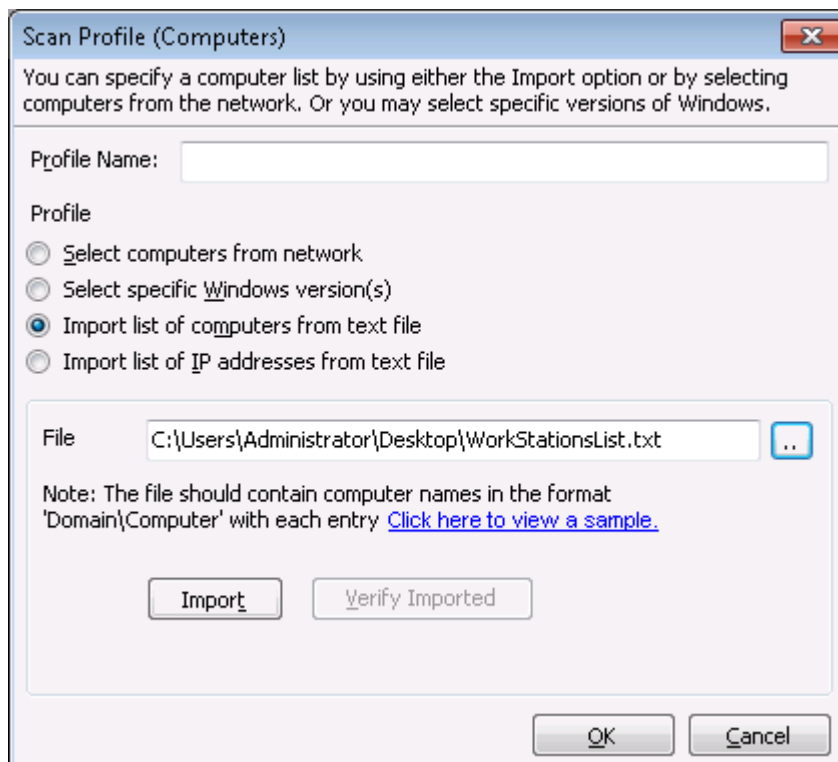


- I. **Choose Select specific Windows version(s) option.**
- II. Select one or more Windows versions. Only computers running the selected Windows version will be included in the computer list.
- III. You may optionally select specific domains, from the list of domains, to include computers only from the selected domains. If you choose not to select any domains, then the Scan Profile includes all domains in the network.

**NOTE:**

- This type of profile is dynamic in nature, in that the list of computers are prepared at run-time; that is at report generation time.

### C. Importing list of computers from a text file



- i. Select **Import list of computers from text file option**.
- ii. Click browse ("...") button to select a file that contains the list of computers to be imported.
- iii. In the "Select File" dialog that shows up, select a text (.txt) file, and then click Open.
- iv. Click **Import** button to import the list of computers from the selected file.

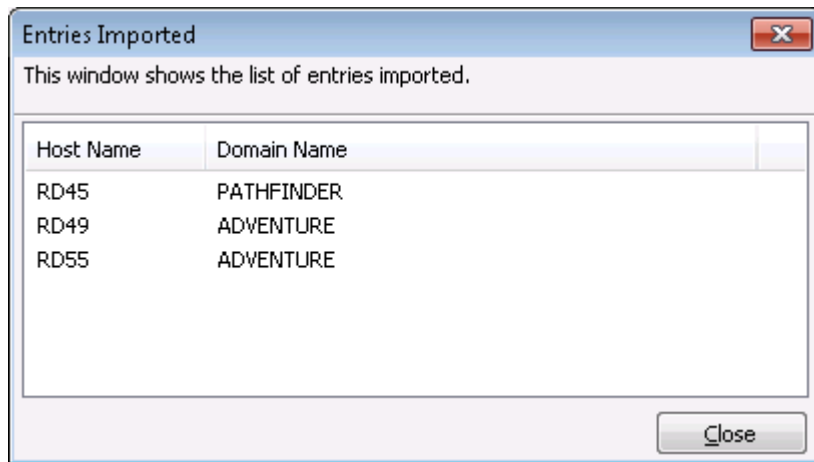
#### NOTE:

- o The text file should contain computer names in the format "Domain Name\Computer Name" (both Domain and Computer name should be a NETBIOS name) with each entry in a separate line as shown below:



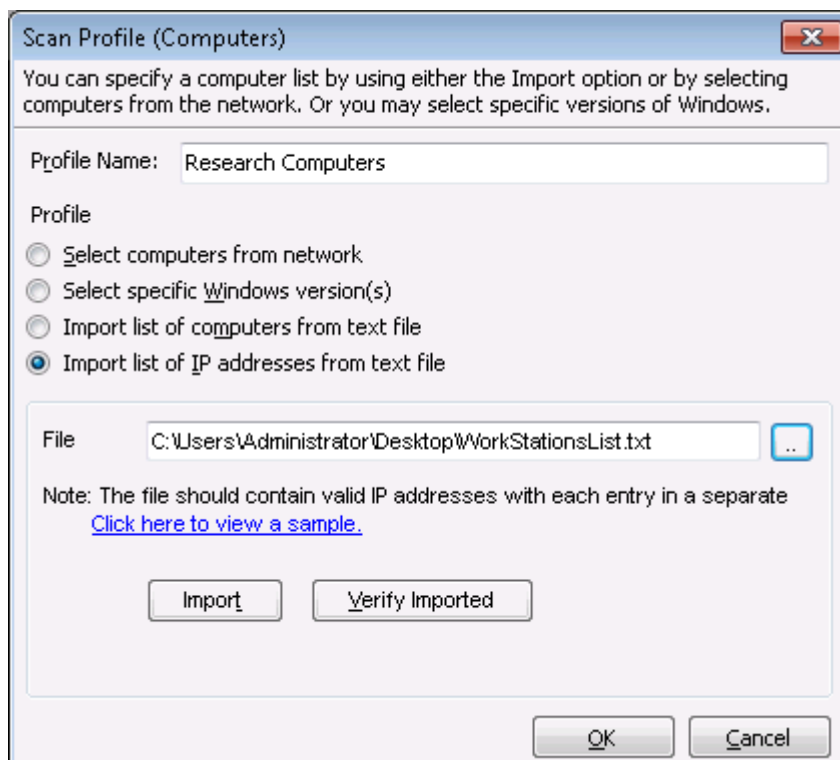
- o Only valid entries of the form "Domain Name\Computer Name" will be imported, and invalid entries will be ignored. Please note that the domain specified will be matched with the domain name to which the computer belongs. The computer entry will be ignored either if the domain name

does not match or if an error occurs retrieving the domain name. To view the list of entries imported, click **Verify Imported List button**. The list of computer names imported will be displayed as shown below:



- Changes to the external text file will not automatically be reflected in the Scan Profile. You need to edit the Scan Profile and re-import the updated computer list from the file.

**D. Importing list of IP addresses from a text file**

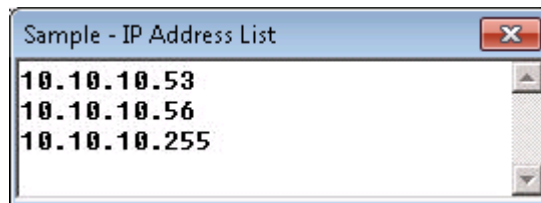


- Select Import list of IP addresses from text file option.**
- Click browse ("...") button to select a file that contains the list of IP addresses to be imported.

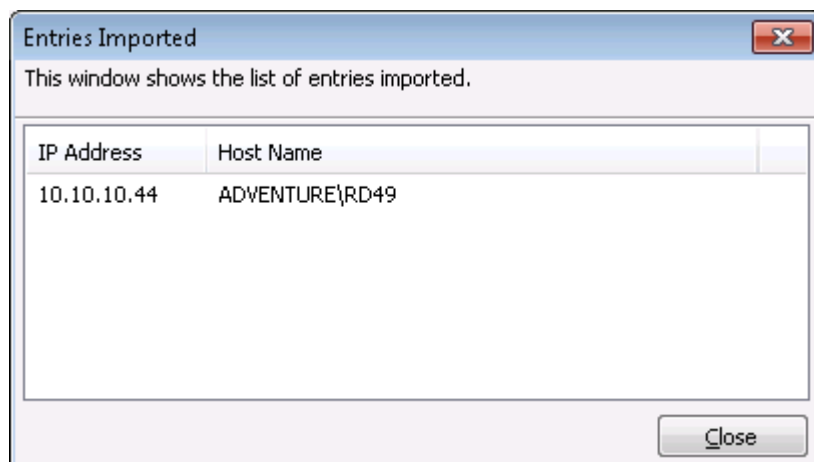
- iii. In the "Select File" dialog that shows up, select a text (.txt) file, and then click Open.
- iv. Click **Import** button to import the list of IP addresses from the selected file.

**NOTE:**

- o The text file should contain valid IP addresses with each entry in a separate line as shown below:



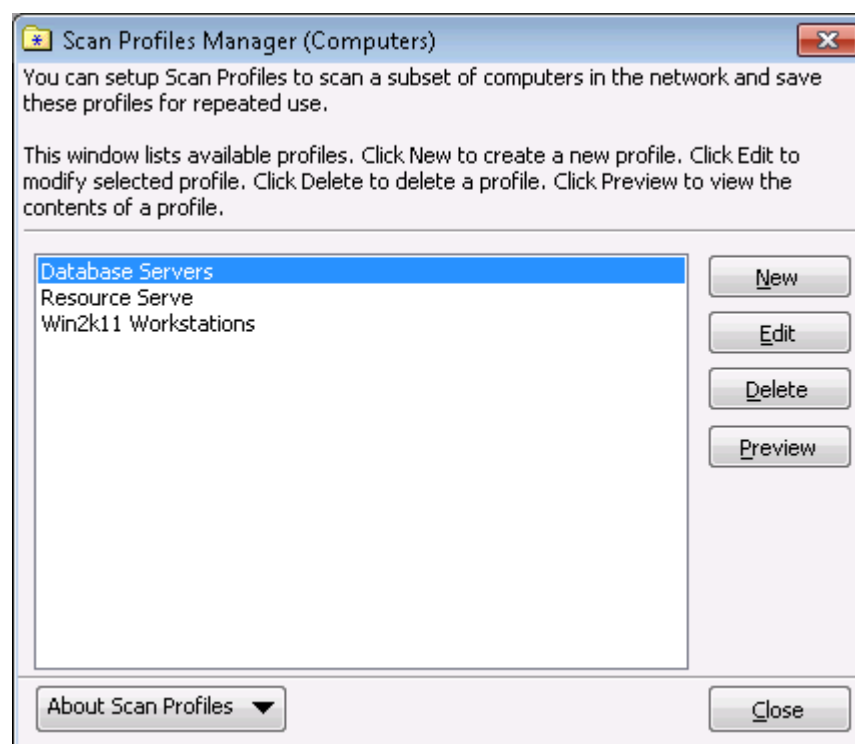
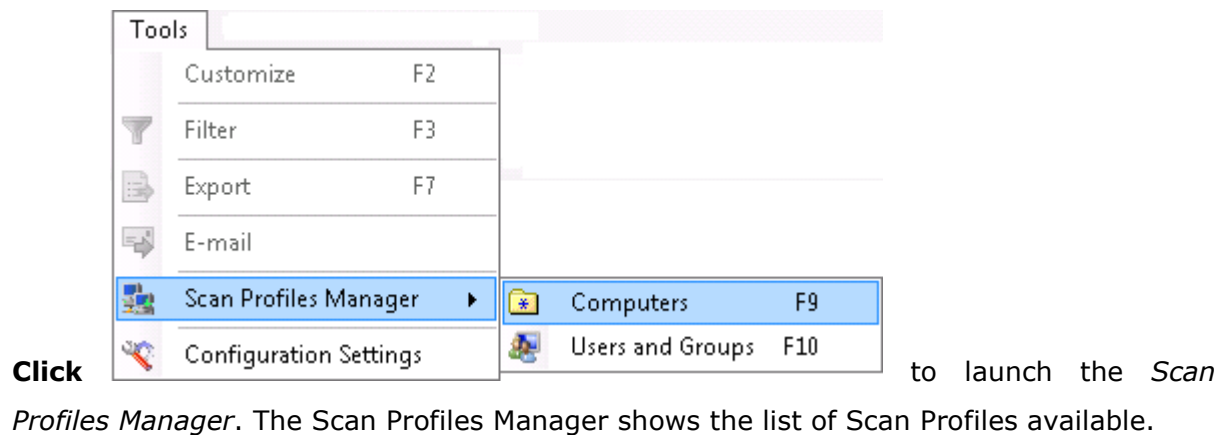
- o During the import process each IP address will be translated to a corresponding computer name. Hence, only valid entries will be imported. To view the list of entries imported, click **Verify Imported List** button. The list of IP addresses and their corresponding computer names will be displayed as shown below:



- o Changes to the external text file will not automatically be reflected in the Scan Profile. You need to edit the Scan Profile and re-import the updated IP address list from the file.

- 4) Click **OK** to save the Scan Profile for later use.

### 8.3 How to Manage Scan Profiles (Computers)?



The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile
- Edit an existing Scan Profile
- Delete a Scan Profile
- Preview the list of computers in a Scan Profile

#### Create a new Scan Profile

- 1) To create a new Scan Profile click New
- 2) Follow the steps as outlined in How to create Scan Profiles?

### **Edit an existing Scan Profile**

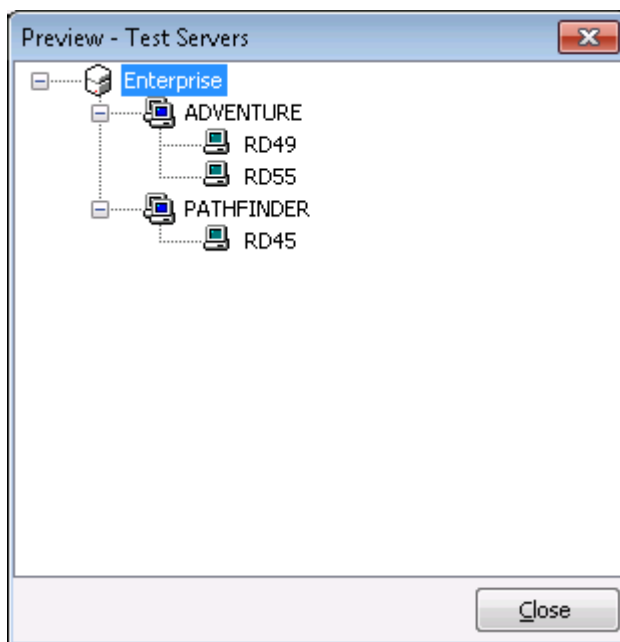
- 1) To edit a Scan Profile click Edit button in the Scan Profiles Manager. The Scan Profile Dialog will appear on the screen which will allow you to edit the selected Scan Profile.
- 2) During edit operation you can modify the computer list; however, you cannot modify the type of the Scan Profile.

### **Delete a Scan Profile**

To delete a Scan Profile, select the profile you want to delete, and then click Delete button. The selected Scan Profile will be deleted permanently. Please note, that reports associated with the Scan Profile deleted may fail to run when generated.

### **Preview the List of Computers in a Scan Profile**

To preview the list of computers in a Scan Profile, select a Scan Profile, and then click **Preview** button. The computer list will be displayed in a tree view as shown below:



The Preview window shows the list of domains and computers selected in the Scan Profile if the computer list was either imported or selected from the network. Whereas, if specific Windows versions were selected, then only the computers that match the selected Windows versions will show up. Furthermore, if specific domains were associated with the Scan Profile, then only the selected domains will show up, otherwise all the domains in the network will show up. The Preview window allows you to view what computers in the network will be included in the profile.

## 8.4 How to Apply Scan Profiles (Computers)?

---

You can apply a Scan Profile to one or more reports to restrict the list of computers during report generation. This is especially useful if you want to generate reports for a subset of computers.

This page covers the following topics with regard to usage of Scan Profiles:

- Scan Profiles and Power Export Tool (off-line report generation)
- Scan Profiles and Interactive Report Generation

### **Scan Profiles and Power Export Tool (off-line report generation)**

You can apply a Scan Profile to one or more reports using the Power Export Tool (for off-line generation) to restrict the domain scope and to scan and collect data for a subset of computers in the network. The report data will be collected for all computers in the applied Scan Profile. However, if the applied Scan Profile becomes unavailable during report generation (likely to happen if the Scan Profile is accidentally deleted); the report data will not be collected at all and will result in an error. Furthermore, if there are no computers to be found in the Scan Profile for a domain for which the report is being generated, then the report generation will fail as well. This is likely to happen if the domain is not included in the Scan Profile or none of the computers in the domain are running the Windows version setup in the Scan Profile.

### **Scan Profiles and Interactive Report Generation**

You may also apply a Scan Profile to reports and view the data in interactive mode. The way in which a Scan Profile is applied and the data collection methodology adopted slightly differs in interactive mode from off-line report generation mode (using Power Export Tool). The data collection methodology adopted also depends on the type of Scan Profile applied (static or dynamic) to the report.

For instance, if a Scan Profile is associated with multiple domains, in interactive mode, data will be collected only for computers that belong to the currently selected domain. On the other hand, if there are no computers to be found for the currently selected domain, in the applied profile, the report data will not be collected at all. This is likely to happen if the currently selected domain was not included in Scan Profile (if it is a static profile) or the Scan Profile includes a Windows version filter, say Windows Computers only, and the domain does not have any computers running Windows XP.

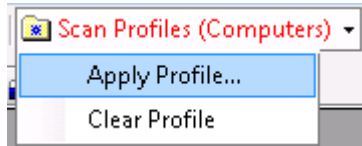
In addition, in interactive mode, there are differences on how Scan Profiles are applied to **Domain-based Reports and Server-based Reports.**

### Scan Profiles and Domain-based Reports

In interactive mode, for domain-based reports, you can apply a Scan Profile by using the Scan Option Dialog. The report will be generated for the list of computers in the applied Scan Profile for the currently selected domain as mentioned earlier.

### Scan Profiles and Server-based Reports

For server-based reports, you can apply a Scan Profile by clicking the



button in the report window. The Scan Profiles Manager will show up on screen, select a Scan Profile, and then click **Apply** button to apply the selected profile.

For server-based reports, however, a Scan Profile when applied reloads the tree view, in the left pane in the report window, with the list of computers in the selected Scan Profile. After a Scan Profile is applied, you can select the desired computer in the tree view in the report window to generate the report. Click the **Clear** button to clear the applied profile. This will reload tree view with the list of all domains in the network.

## 8.5 About Scan Profiles (Users/Groups)

---

You can setup Scan Profiles (Users/Groups) to scan a subset of users/groups present in computers and save these profiles for repeated use (useful for repeatedly scanning and reporting on different subsets of users and groups permissions on share folders).

- How to create Scan Profiles (Users/Groups)?
- How to manage Scan Profiles (Users/Groups)?
- How to apply Scan Profiles (Users/Groups)?

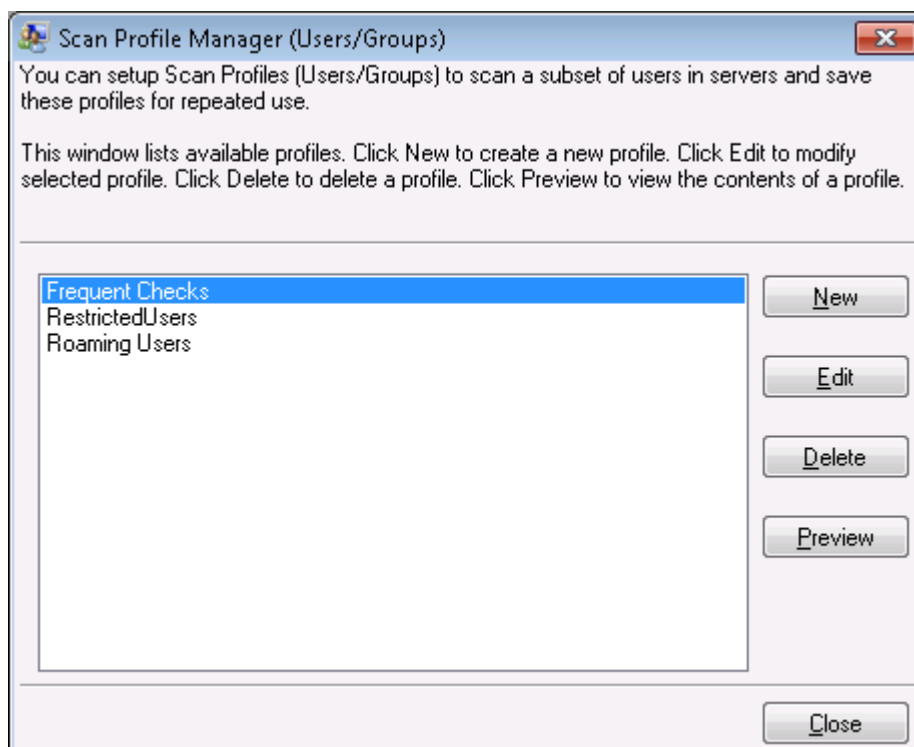
## 8.6 How to Create Scan Profiles (Users/Groups)?

---

Perform the following steps to create a Scan Profile (Users/Groups).



- 1) Select **Users and Groups** from the application toolbar. This action will launch the Scan Profiles Manager (Users/Groups) dialog as shown below.



- 2) Click **new** button in the Scan Profiles Manager (Users/Groups) dialog. This action will launch the **Scan Profiles (Users/Groups)** Wizard as shown below.

**Scan Profile (Users/Groups)**

**Select User/Group Account(s)**

Select the User and/or Group accounts for which you would like to create a profile.

Profile Name:

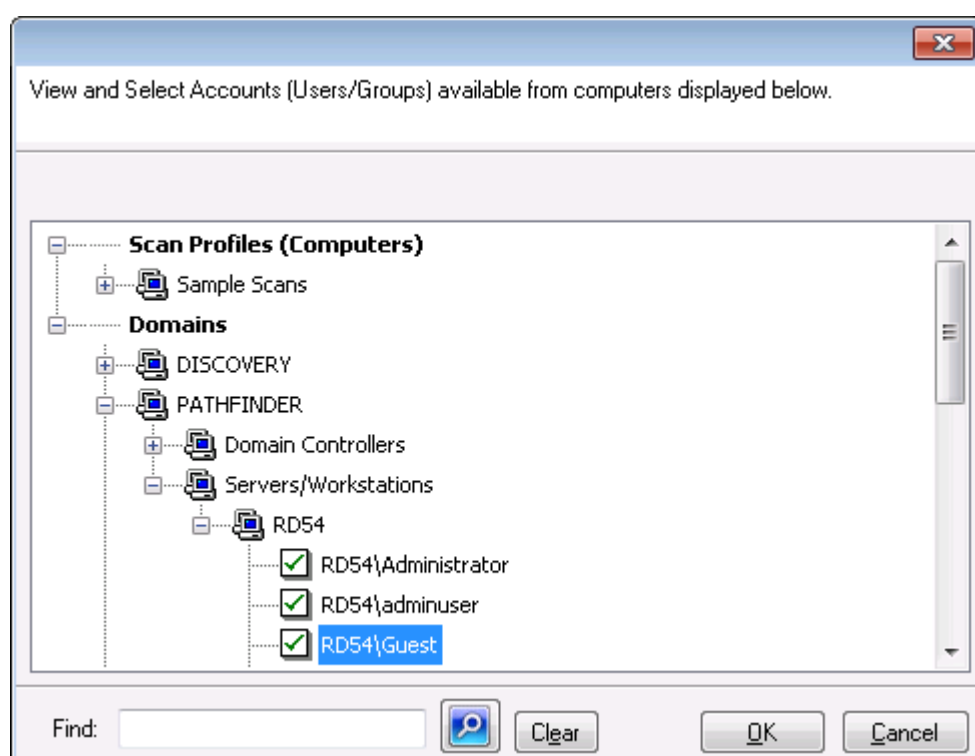
Account Name:  Add

Add Accounts from domain\server:

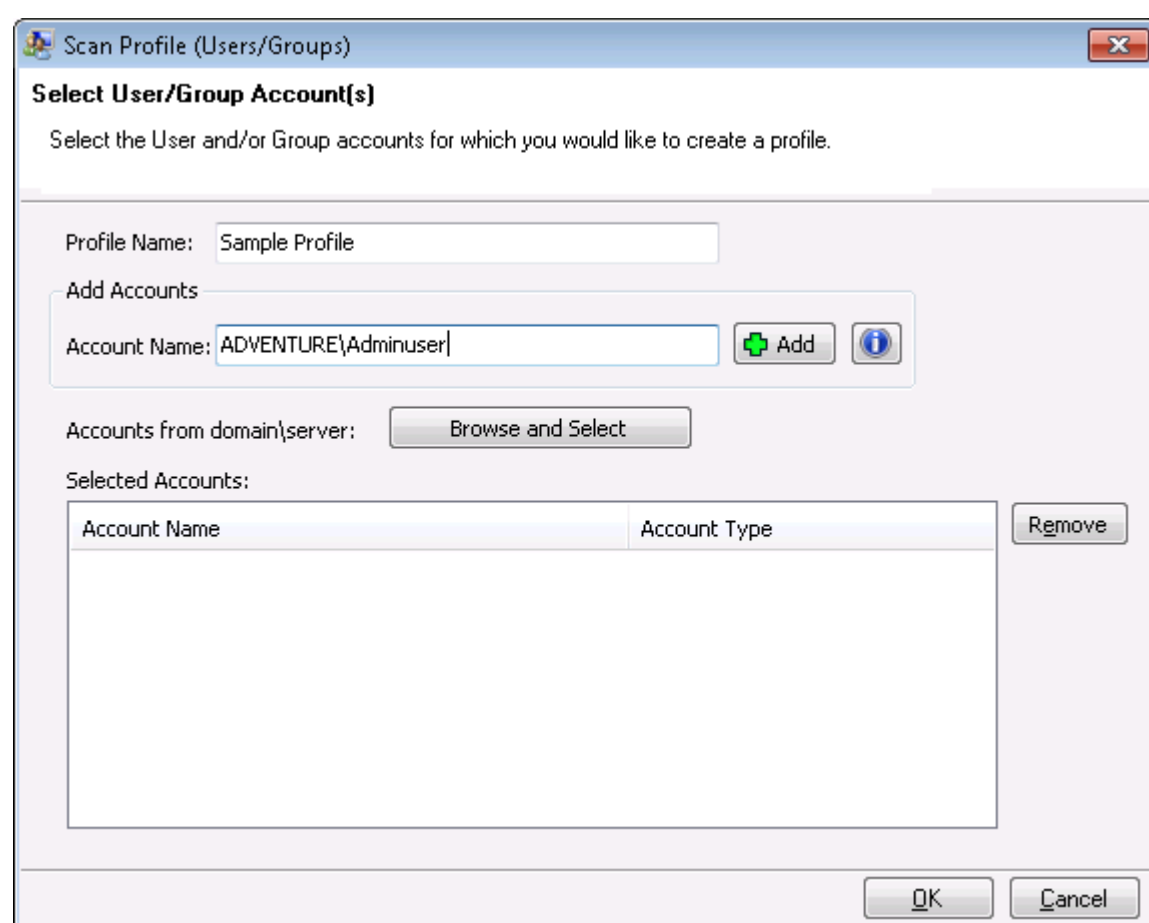
Selected Accounts:

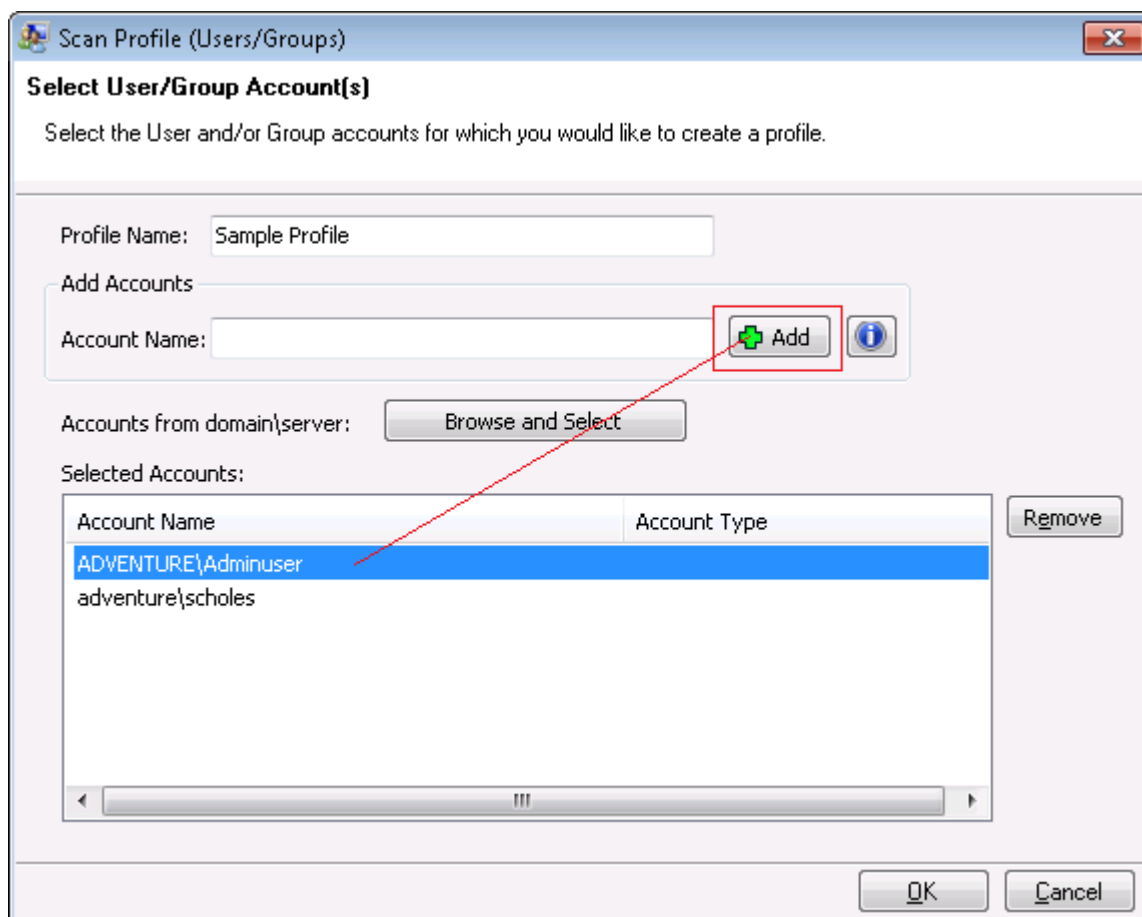
Account Name	Account Type
--------------	--------------

- 1) Enter a name for the profile.
- 2) Use the Browse and Select button to enumerate users/groups from servers or Scan Profiles Computers as shown below:



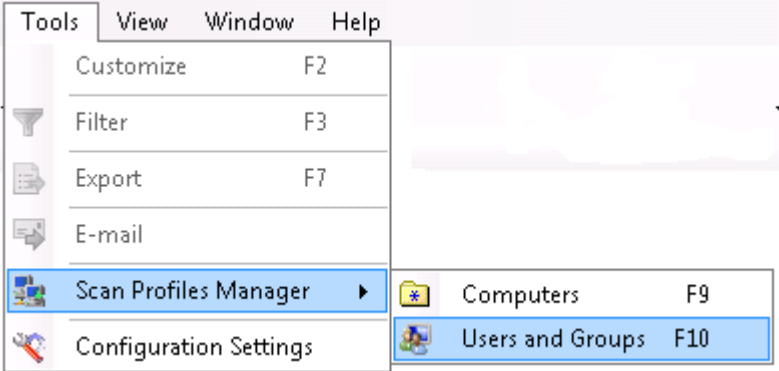
- 3) You can enter users / groups name and add to the selected account list for creating a profile. Enter the users/groups name in 'Domain\User Name' format and click the Add button to add the entered account to the list as shown below:

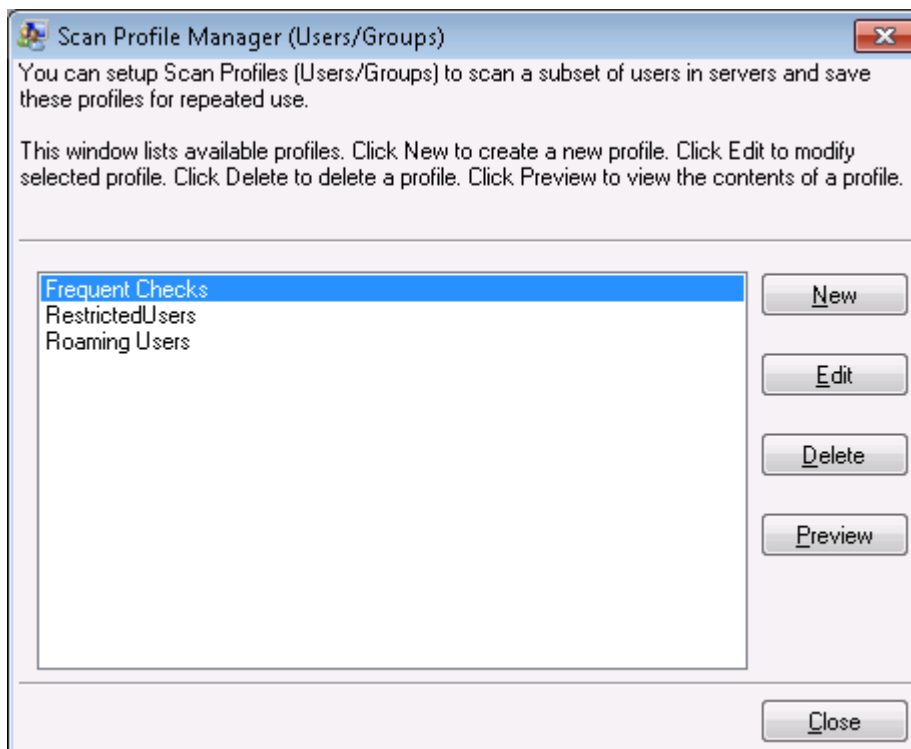




5) Click **Finish** to save the Users/Groups profile for future use.

## 8.7 How to Manage Scan Profiles (Users/Groups)?

Click  to launch the **Scan Profiles Manager (Users/Groups)**. The Scan Profiles Manager (Users/Groups) shows the list of available profiles.



The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile (Users/Groups)
- Edit an existing Scan Profile (Users/Groups)
- Delete a Scan Profile (Users/Groups)
- Preview the list of users and groups in a Scan Profile (Users/Groups)

**Create a new Scan Profile (Users/Groups)**

- 1) To create a new Scan Profile (Users/Groups) click New
- 2) Follow the steps as outlined in How to create Scan Profiles?

**Edit an existing Scan Profile (Users/Groups)**

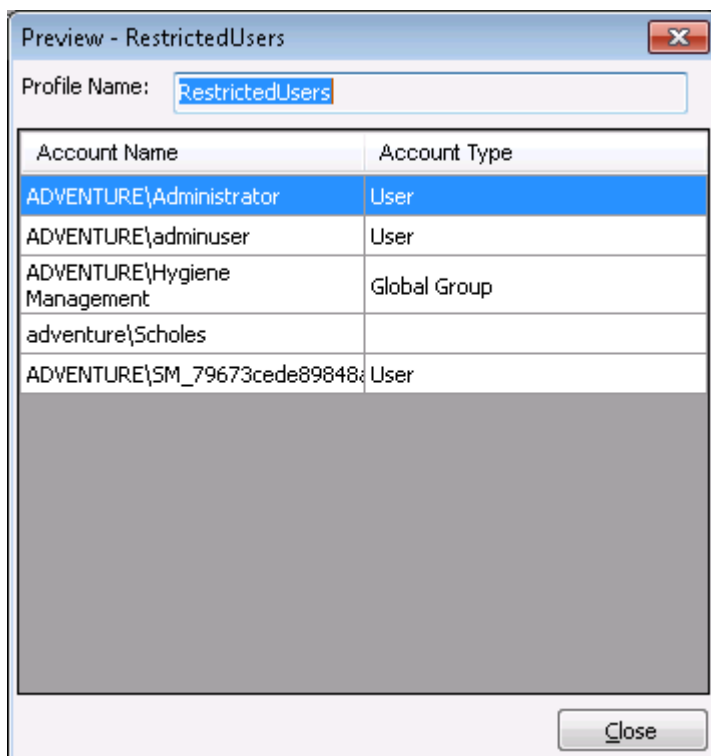
- 1) To edit a Scan Profile (Users/Groups) click Edit button in the Scan Profiles Manager. The Scan Profile (Users/Group) wizard will appear on the screen which will allow you to edit the selected profile.
- 2) During edit operation you can modify the Users/Groups list.

**Delete a Scan Profile (Users/Groups)**

To delete a Scan Profile (Users/Groups), select the profile you want to delete, and then click **Delete** button. The selected Scan Profile (Users/Groups) will be deleted permanently. Please note, that reports associated with the Scan Profile (Users/Groups) deleted may fail to run when generated.

**Preview the List of Users and Groups in a Scan Profile (Users/Groups)**

To preview the list of users and groups in a profile, select a profile, and then click **Preview** button



The Preview window allows you to view what users and groups will be included in the profile.

## 8.8 How to Apply Scan Profiles (Users/Groups)?

---

You can apply Scan Profile (Users/Groups) to permissions reports that involve generating permissions for specific users and groups on share folders. This is especially useful, if you want to generate permissions reports for certain users and groups frequently.

The following shows permissions reports that involves specific users and groups

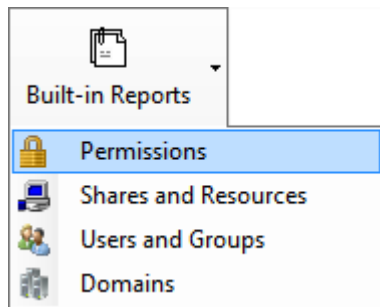
Report Name	Description
List of permissions for specific users and groups on folders	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
List of permissions for specific users and groups on files	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.

### **Scan Profiles (Users and Groups) and Permission Reports for Specific Users and Groups**

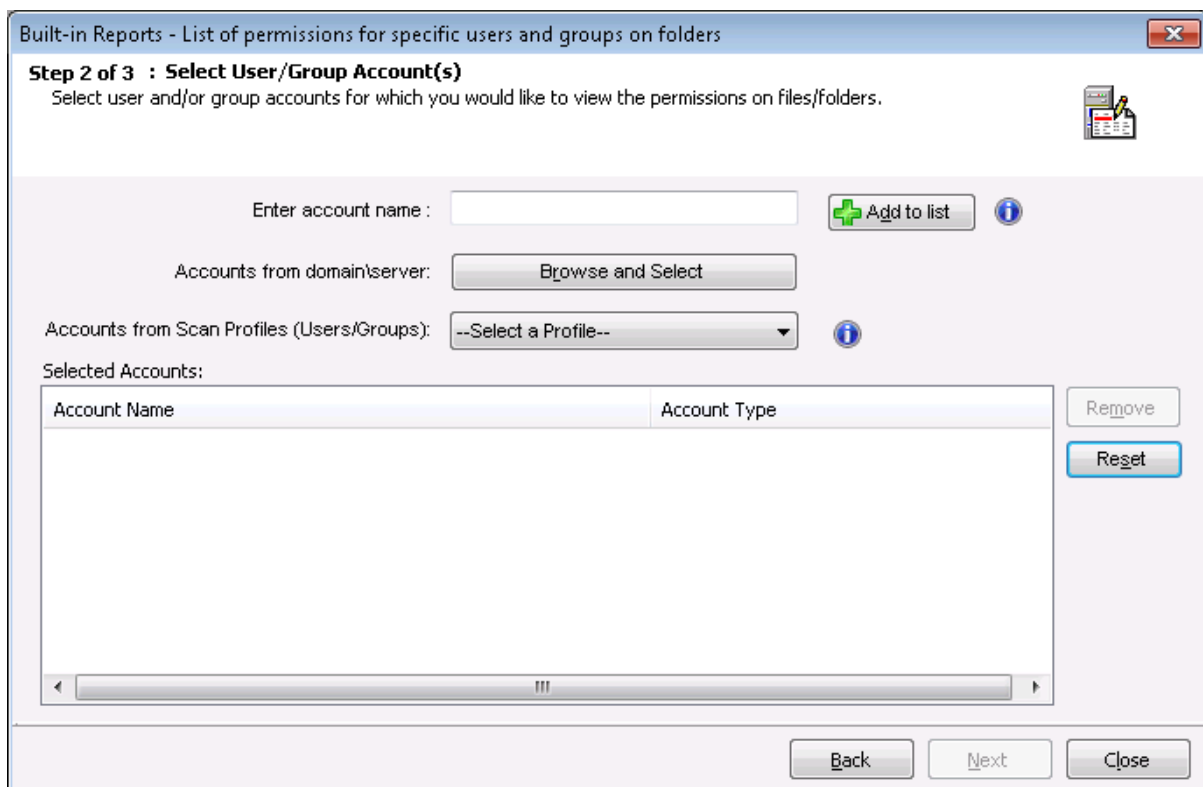
You can apply a Scan Profile (Users/Groups) to permissions reports either using Power Export Tool (for off-line generation) or Interactive Report Generation .This option will useful, if permissions for certain Users and Groups need to be monitored frequently. Rather than searching for Users and Groups, adding then to account list and viewing their permissions. You can use create a subset of Users and Groups, save them as a profile, generating permissions reports for subset that of users and groups. The following shows how Scan Profiles (Users/Groups) can be applied to permission reports for specific users and groups in Interactive report generation and Power export tool.

### **Scan Profiles (Users/Groups) and Interactive Report Generation**

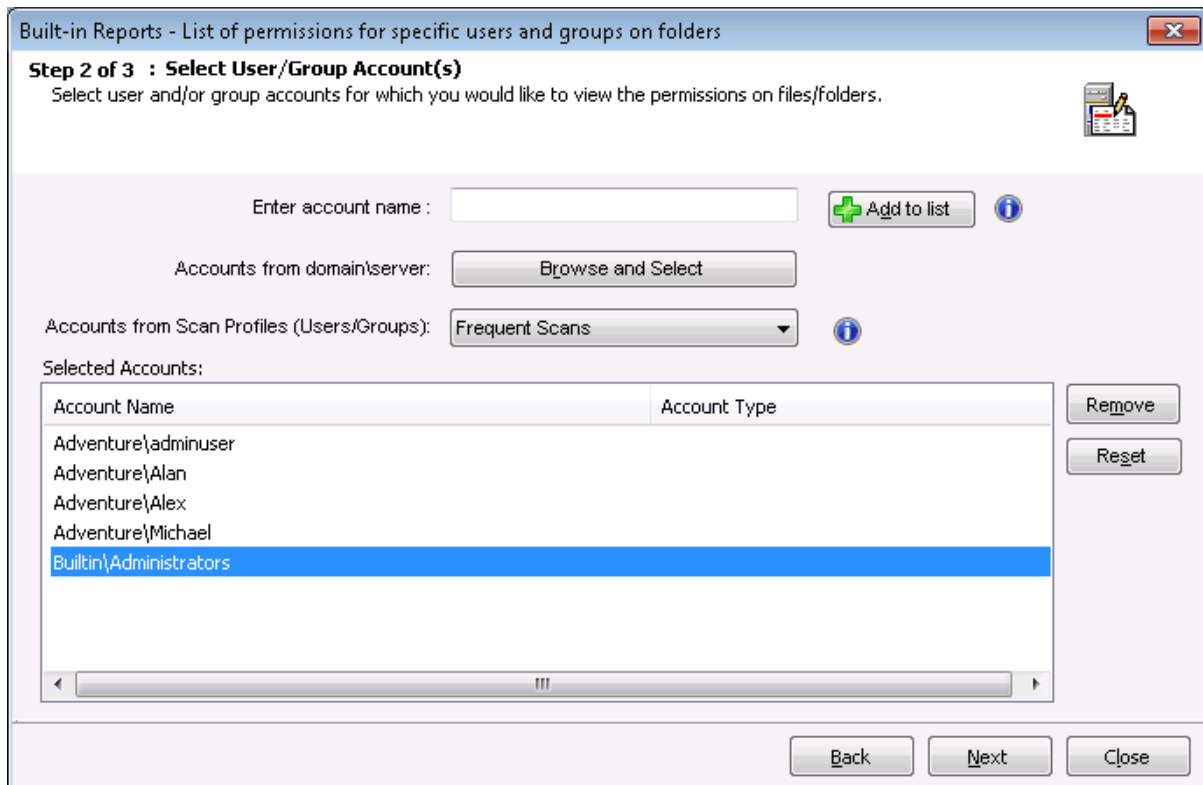
Perform the following steps for applying Scan Profiles (Users/Groups) to permission reports in Interactive report generation



- 1) Click on **Permissions** under Built-in Reports in the tool bar.
- 2) Select any one of the permissions reports listed above and click **Next** to proceed.
- 3) In the next step, select the option 'Select a Scan Profiles (Users/Groups) ' as shown below.



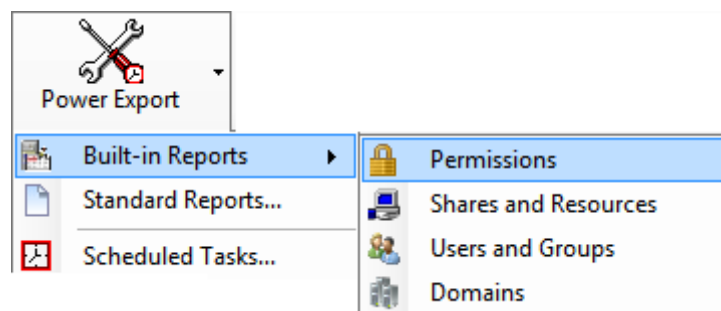
- In this step the list of users and/or groups present in Scan Profile (Users/Groups) will be loaded to the selected Account list as shown below:

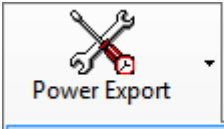


- In the Succeeding steps, select needed details for generating reports for selected Users and Groups.

### Scan Profiles (Users/Groups) and Power Export Tool (Off-line Report Generation)

You can apply a Scan Profile (Users/Groups) to permissions reports using Power Export Tool (for off-line generation).





- 1) Click on the  button in the toolbar.
- 2) Select any one of the permissions reports listed above and click Next to proceed.
- 3) In the next step, select the option 'Select a Scan Profiles (Users/Groups)' as shown below.

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on folders

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts

Account Name	Account Type
--------------	--------------



- In this step the list of users and groups present in Scan Profile (Users/Groups) will be loaded to the selected account list as shown below:

**Power Export - Built-in Reports**


**Step 2 of 6 : User/Group Selection**

Select a server or a Scan Profile (Computers) or a Scan Profile (Users/Groups) to retrieve available users and groups from.

Report Name: List of permissions for specific users and groups on folders

Enter account name :   Add to list 

Accounts from domain\server:

Accounts from Scan Profiles (Users/Groups):  

Selected Accounts

Account Name	Account Type
Adventure\adminuser	
Adventure\Alan	
Adventure\Alex	
Adventure\Michael	
Builtin\Administrators	

In the succeeding steps select needed details for generating reports for selected Scan Profile (Users/Groups).

## 8.9 About Scan Profiles (Shares)

---

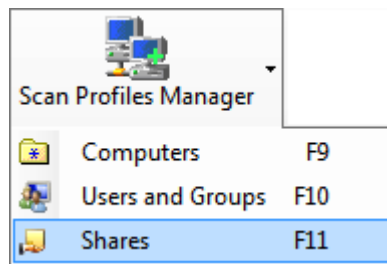
You can setup Scan Profiles (Shares) to scan a subset of shares present in computers and save these profiles for repeated use (useful for repeatedly scanning and reporting on different subsets of share folders permissions).

- **How to create Scan Profiles (Shares)?**
- **How to manage Scan Profiles (Shares)?**
- **How to apply Scan Profiles (Shares)?**

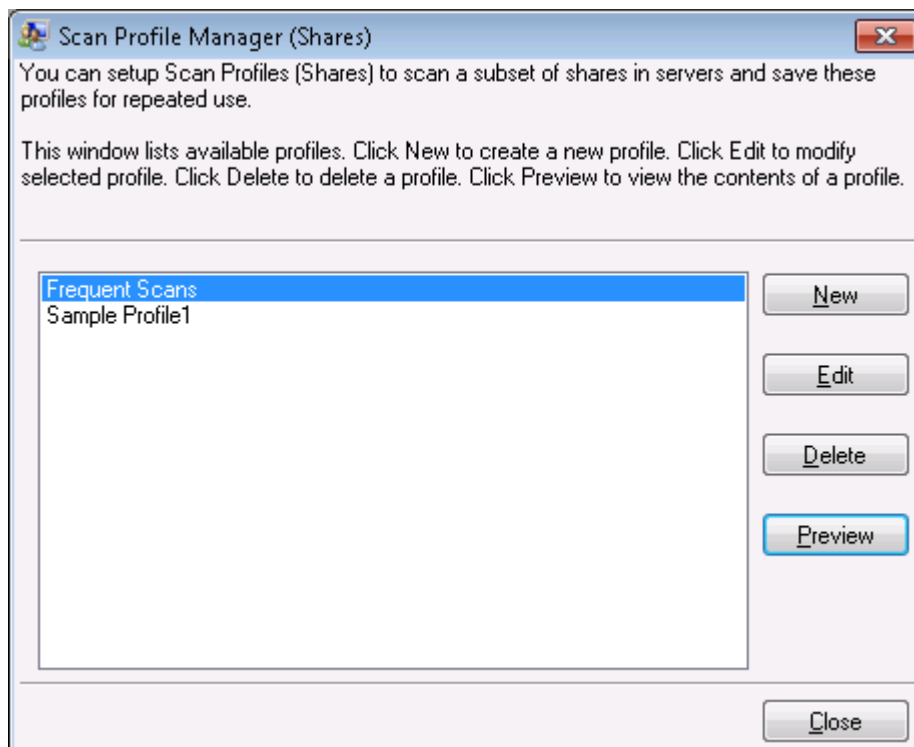
## 8.10 How to Create Scan Profiles (Shares)?

---

Perform the following steps to create a Scan Profiles (Shares).



- 1) **Select** from the application toolbar. This action will launch the Scan Profiles Manager (Shares) dialog as shown below:



- 2) Click **New** button in the **Scan Profiles Manager (Shares)** dialog. This action will launch the **Scan Profiles (Shares)** dialog as shown below:

Scan Profiles (Shares)

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.

Profile Name: Sample Profile

Share/Folder UNC Path:  Add

Folder Path

Add From

Import

Remove

OK Cancel

- 1) Enter a name for the profile.
- 2) You may type the UNC path of a folder that is not in the list, such as a folder that is not shared, and then click Add, to add it to the list as shown below:

Scan Profiles (Shares)

Enter the full path of a Share or Shared Folder. Click Add From to load the list of shares, Import to import a list of UNC folder paths from a text file.

Profile Name: Sample Profile

Share/Folder UNC Path: \\RD55\TestLocagroups | Add

Folder Path

Add From

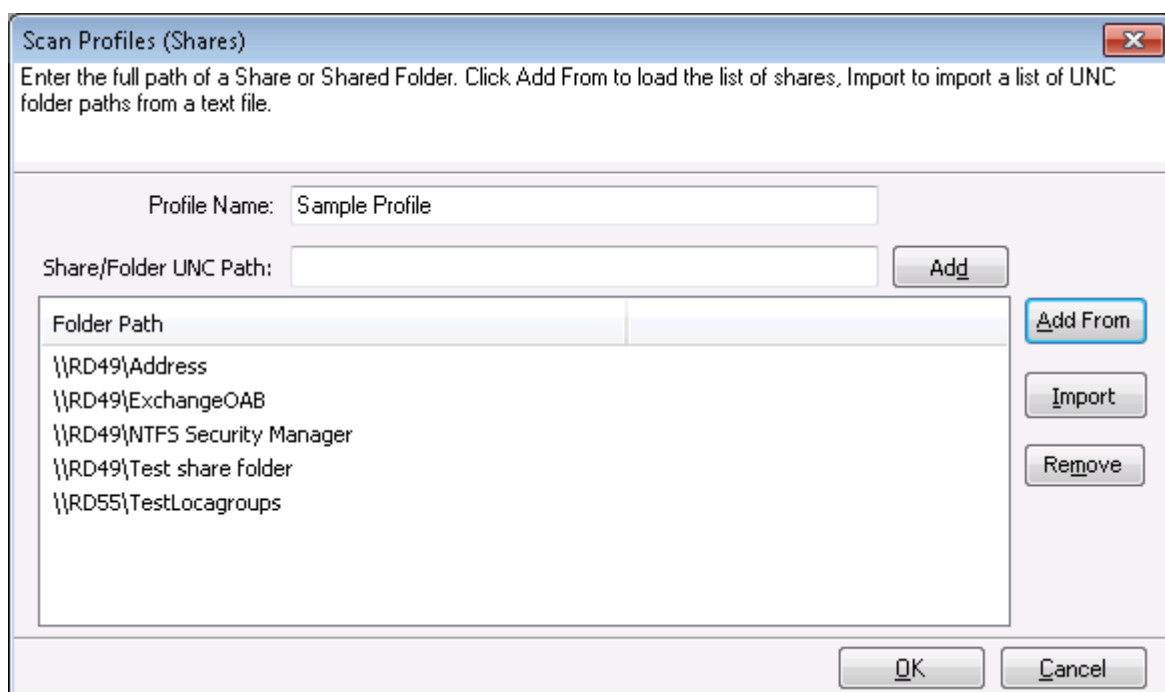
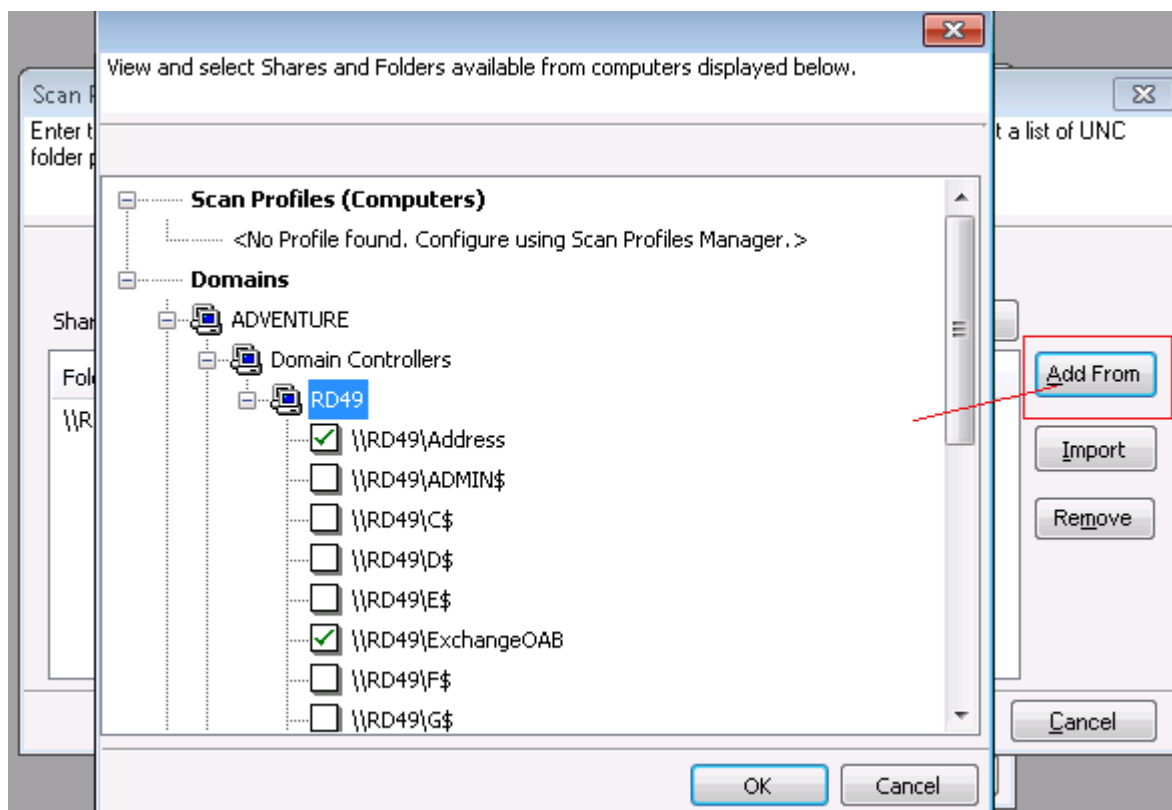
Import

Remove

OK Cancel

- 3) You may also import a list of UNC paths to shared and non-shared folders from a text file by using the Import button.

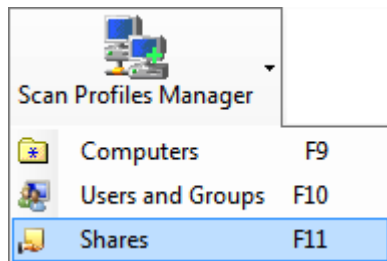
- 4) Click 'Add From' to add list of share folders from computers as shown below:



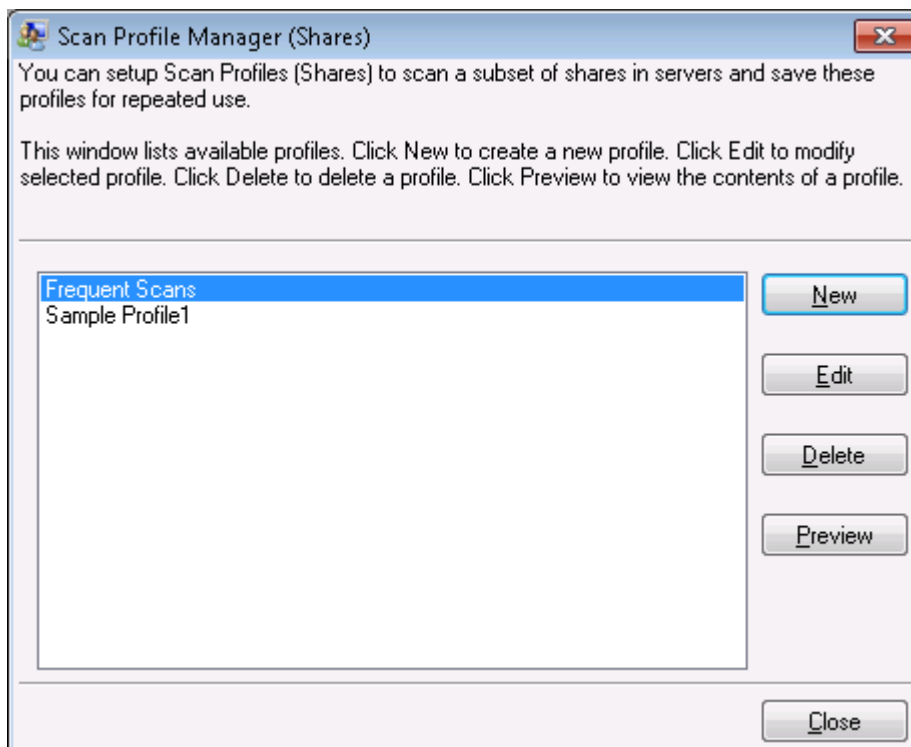
- 5) Click Finish to save the Shares profile for future use.

## 8.11 How to Manage Scan Profiles (Shares)?

---



**Click** to launch the Scan Profiles Manager (Shares). The Scan Profiles Manager (Shares) shows the list of available profiles.



The Scan Profiles Manager allows you to perform the following operations:

- Create a new Scan Profile (Shares)
- Edit an existing Scan Profile (Shares)
- Delete a Scan Profile (Shares)
- Preview the list of Shares in a Scan Profile (Shares)

### Create a new Scan Profile (Shares)

- 1) To create a new Scan Profile (Shares) click New
- 2) Follow the steps as outlined in How to create Scan Profiles?

### Edit an existing Scan Profile (Shares)

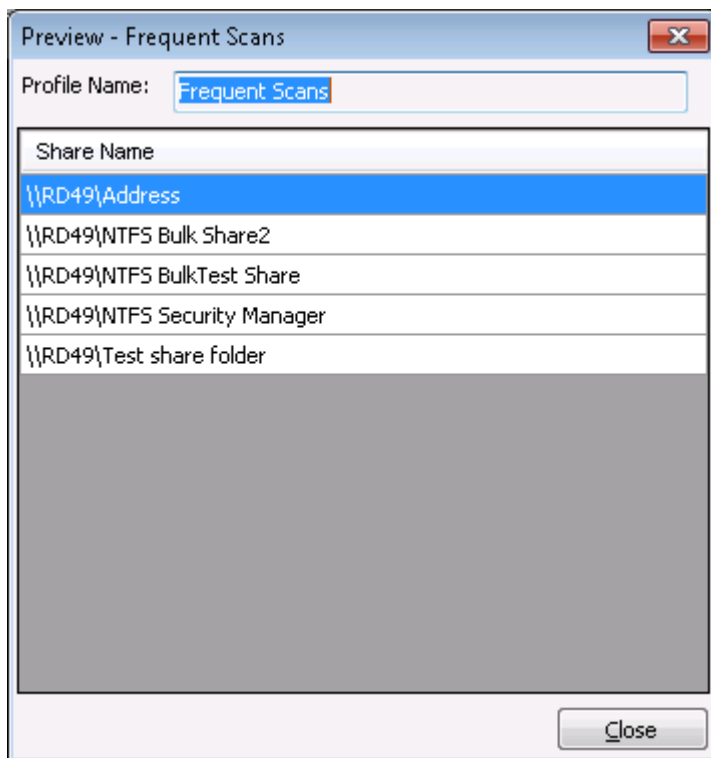
- 1) To edit a Scan Profile (Shares) click **Edit** button in the Scan Profiles Manager. The Scan Profile (Shares) wizard will appear on the screen which will allow you to edit the selected profile.
- 2) During edit operation you can modify the Shares list.

### Delete a Scan Profile (Shares)

To delete a Scan Profile (Shares), select the profile you want to delete, and then click Delete button. The selected Scan Profile (Shares) will be deleted permanently. Please note, that reports associated with the Scan Profile (Shares) deleted may fail to run when generated.

### Preview the List of Shares in a Scan Profile (Shares)

To preview the list of shares in a profile, select a profile, and then click **Preview** button.



The Preview window allows you to view what shares will be included in the profile.

## 8.12 How to Apply Scan Profiles (Shares)?

You can apply Scan Profile (Shares) to permissions reports. This is especially useful, if you want to generate permissions reports for certain Shares frequently.

The following shows permissions reports that involves shares profile

List of Permissions Reports:

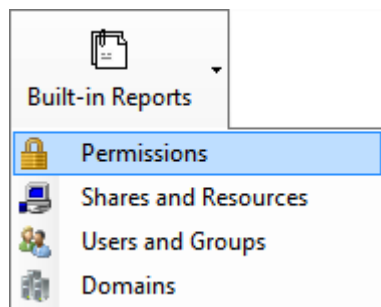
Report Name	Description
List of permissions for specific users and groups on folders	Reports the folder permissions assigned to specific users and/or groups on a selected set of folders.
List of permissions for folders	Reports the permissions associated with a selected set of folders.
List of permissions for specific users and groups on files	Reports the files permissions assigned to specific users and/or groups under a selected set of folders.
List of permissions for files	Reports the permissions associated with files under a selected set of folders.

### Scan Profiles (Shares) and Permission Reports

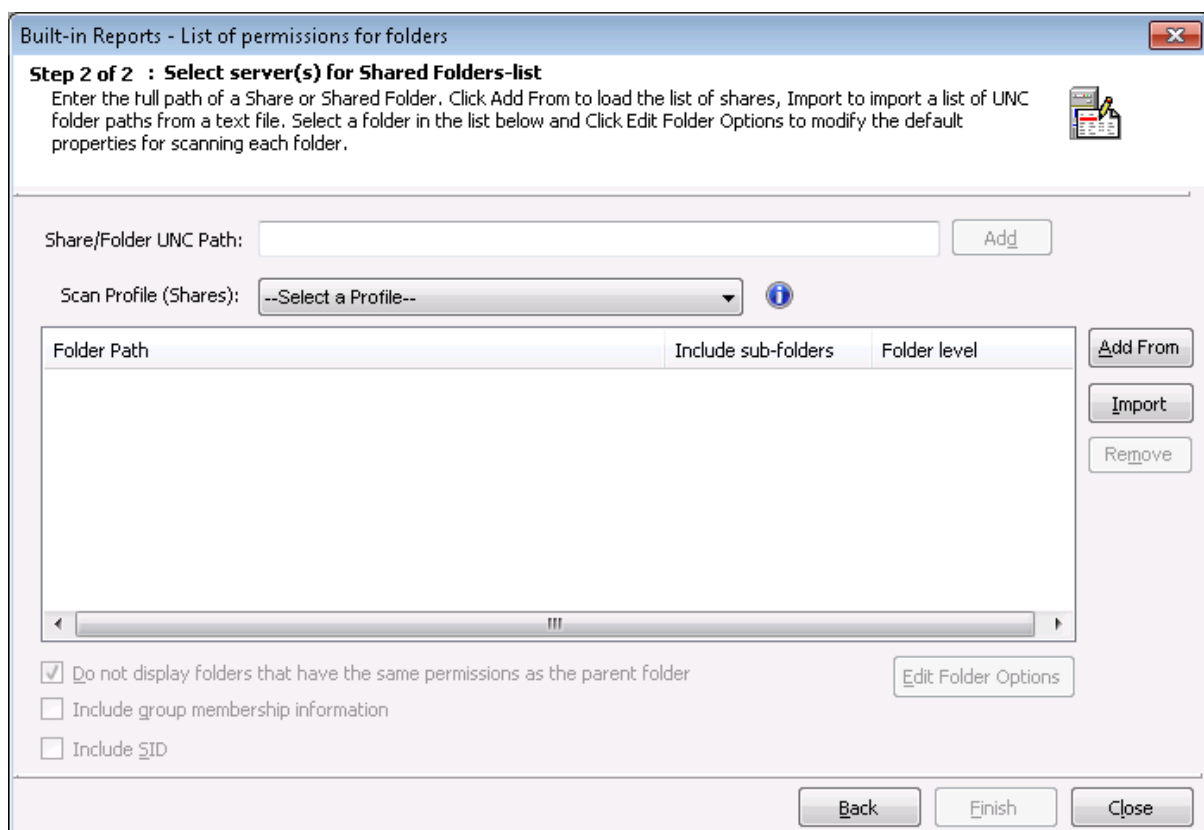
You can apply a Scan Profile (Shares) to permissions reports either using Power Export Tool (for off-line generation) or Interactive Report Generation .This option will useful, if permissions for certain shares need to be monitored frequently. Rather than searching for shares, adding them to list and viewing their permissions. You can create a subset of shares, save them as a profile, generating permissions reports for them. The following shows how Scan Profiles (Shares) can be applied to permission reports in Interactive report generation and Power export tool.

### Scan Profiles (Users/Groups) and Interactive Report Generation

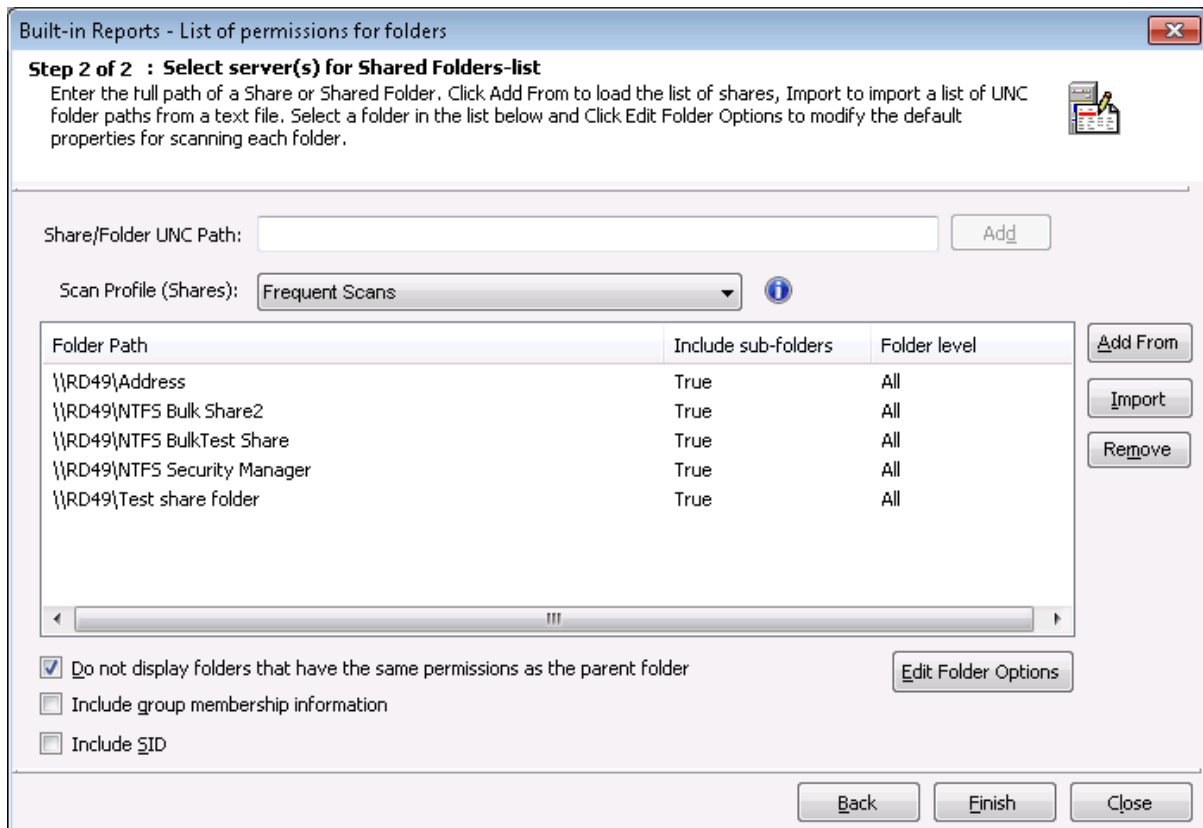
Perform the following steps for applying Scan Profiles (Shares) to permission reports in Interactive report generation



- Click on **Permissions** under *Built-in Reports* in the tool bar.
- Select any one of the permissions reports listed above and click next to proceed.
- In the next step, select the option 'Select a Scan Profiles (Shares) ' as shown below:



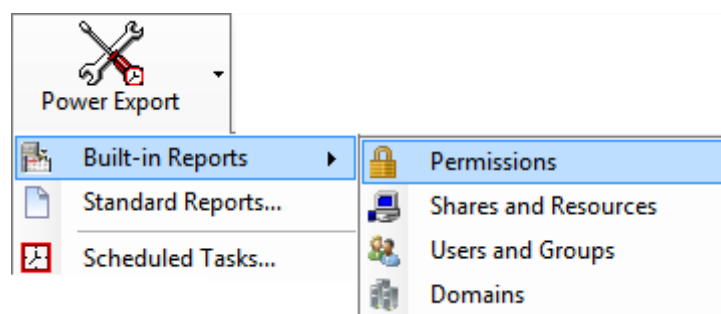
- In this step the list of shares present in Scan Profile (Shares) will be loaded to the selected account list as shown below:



- In the succeeding steps select needed details for generating reports for selected shares.

### Scan Profiles (Users/Groups) and Power Export Tool (Off-line Report Generation)

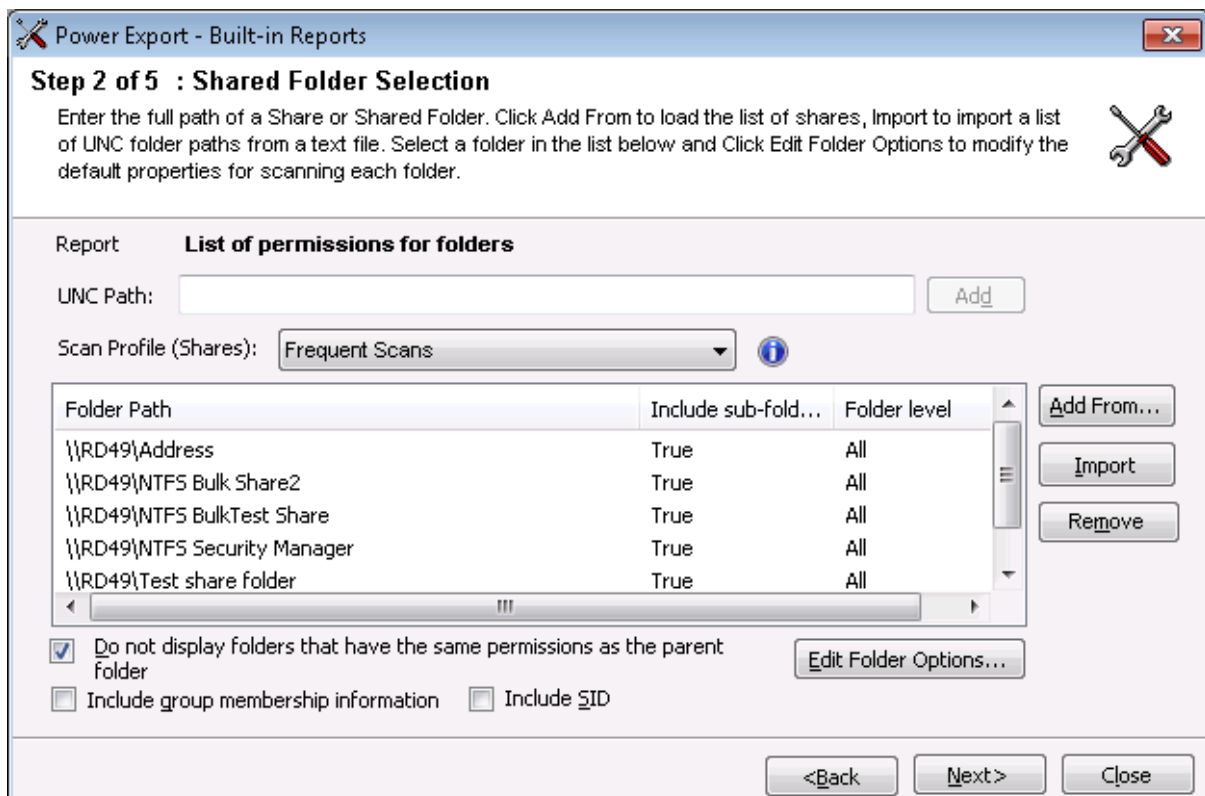
You can apply a Scan Profiles (Shares) to permissions reports using Power Export Tool (for off-line generation).



- Click on the button in the toolbar.
- Select any one of the permissions reports listed above and click Next to proceed.
- In the next step, select the option 'Select a Scan Profiles (Shares)' as shown below:



- In this step the list of shares present in Scan Profile (Shares) will be loaded to the selected account list as shown below:



In the succeeding steps select needed details for generating reports for selected shares.

## References

### 8.13 Troubleshooting

---

If and when a problem arises, please forward the following information to support@vyapin.com to revert back to you with a solution. These files will be available where ARKWE is installed.

#### **Error Log File**

E.g., <Application Data Folder>\ARKWE 8.x\ARKWEErrorLog.log

#### **NOTE:**

<Application Data Folder> is the common area where ARKWE settings will be stored in the machine running ARKWE. The <Application Data Folder> can be found from the Help -> About screen. The default path of <Application Data Folder> is as follows:

- a)** Windows XP Windows 2003-C:\Documents and Settings\All Users\Documents
- b)** Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 2008, Windows Server 2012 - C:\Users\Public\Documents

## 8.14 How to Uninstall ARKWE?

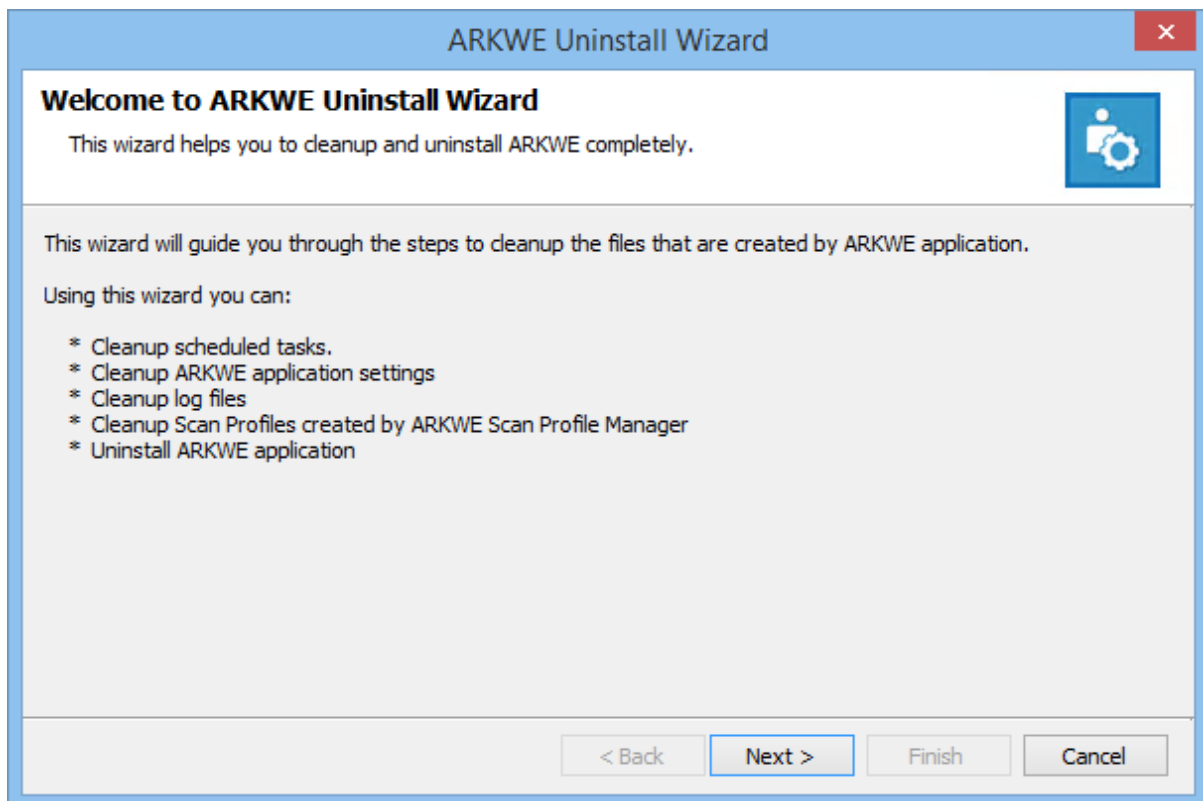
---

When you uninstall ARKWE through Control Panel - Add / Remove Programs applet, Windows Installer program will remove only the application files from your machine. But, the application related files created by ARKWE remain in the computer. In order to remove ARKWE worker files completely, the uninstall wizard provides a set of cleanup options to perform the cleanup operation based your selection.

Use this wizard to cleanup the files that are created by ARKWE application selectively and uninstall ARKWE completely from the machine.

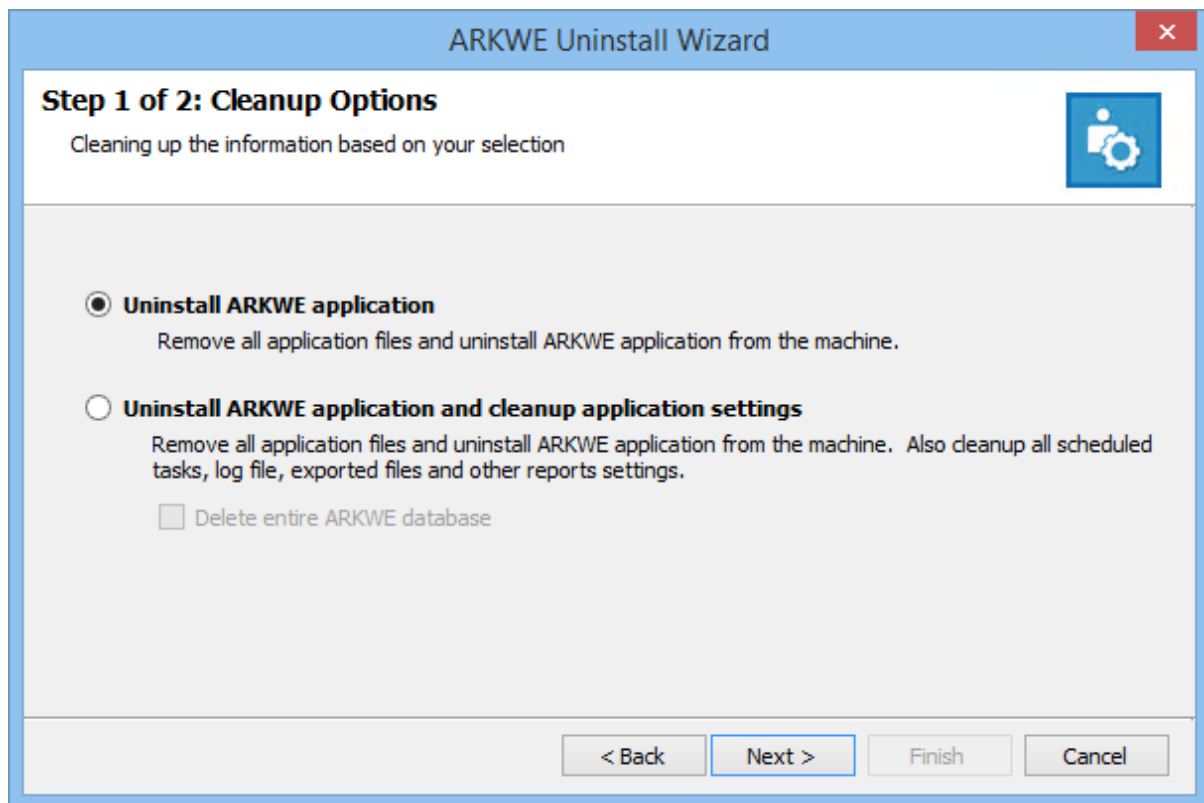
- 1) Launch the uninstall wizard by clicking **Start -> Programs -> Admin Report Kit for Windows Enterprise v8.x -> Uninstall ARKWE.**

The **ARKWE Uninstall Wizard** dialog will be shown as below:



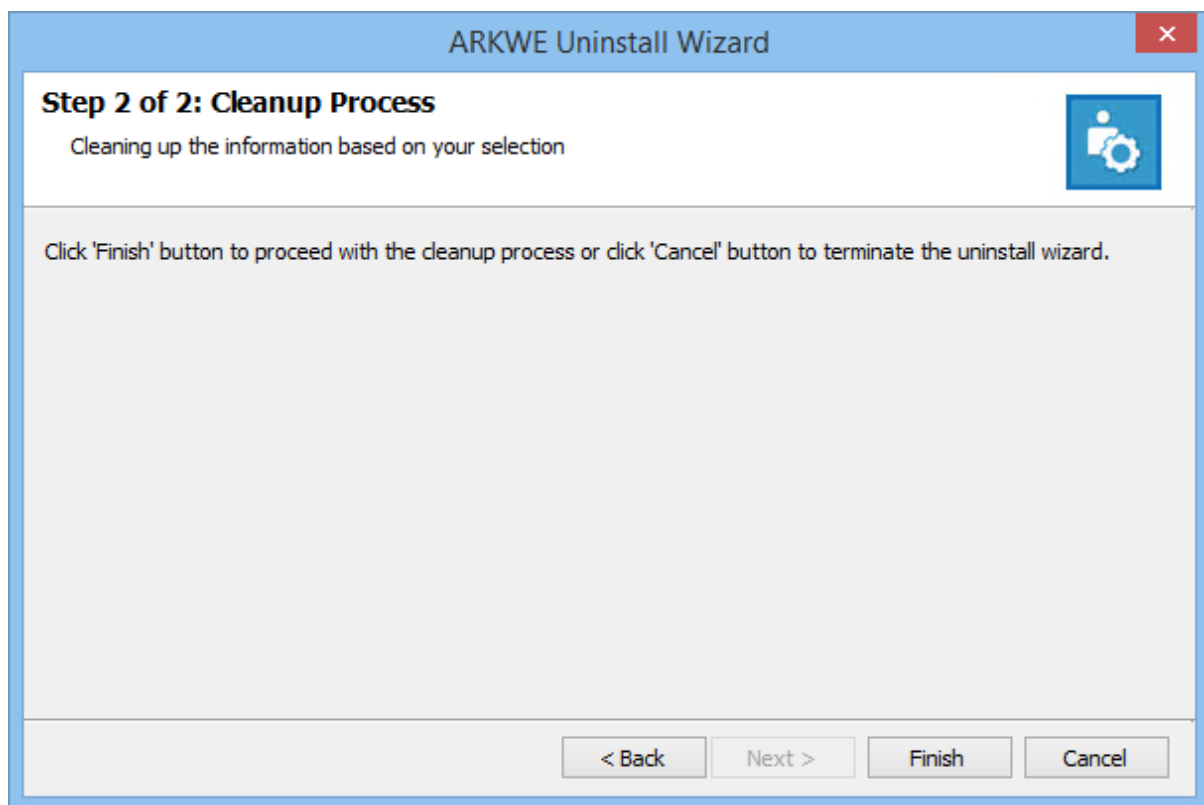
Click **Next** to Proceed

2) Select required **Cleanup Options** as shown below:



Click **Next** to Proceed.

**3) Confirm the Cleanup and/or Uninstall Process.**



Click **Finish** to run cleanup and/or uninstall process. Click **Cancel** to close the wizard.

- 4)** Once the file cleanup process is complete, the uninstall wizard will automatically run *Windows Installer* program to remove **ARKWE** application from the machine.



## 9 Index

---

- (ARKWE), 1
- About Built-in Reports, 51
- About Power Export, 109
- About Scan Profiles (Computers), 179
- About Scan Profiles (Users/Groups), 189
- About System Info, 79
- Active Directory, 101, 102
- Additional E-mail Settings, 119, 156, 166, 175
- Additional Features, 95
- Admin Report Kit for Windows Enterprise, 1, 209
- applet, 209
- Application Data, 208
- ARKWE, 1, 2, 3, 6, 96, 100, 101, 103, 104, 107, 108, 109, 110, 208, 209, 211
- Built-in Reports, 51, 67, 71, 75, 123, 124, 150, 160, 169, 196
- Create Task, 79
- CSV, 109
- data warehousing, 3
- Domain, 30, 169, 170
- Domain Admins, 104
- Domain Controllers, 104
- Domains, 51, 170
- Edit Task, 193
- Enterprise network planning personnel, 3
- Error Control, 49
- Error Log File, 6, 208
- evaluation/trial, 4
- Hardware, 87
- HIPPA., 1
- How to activate the software?, 4
- How to Apply Filters?, 96
- How to apply Scan Profiles (Computers)?, 187
- How to apply Scan Profiles (Users/Groups)?, 195
- How to create Scan Profiles (Computers)?, 180
- How to create Scan Profiles (Users/Groups)?, 189
- How to customize fields?, 95
- How to E-mail data?, 100
- How to Export data?, 98
- How to find data in a report?, 104

How to manage Scan Profiles (Computers)?, 185	How to view Operating System and Hot Fixes reports?, 84
How to manage Scan Profiles (Users/Groups)?, 193	How to view Policies information?, 41
How to Refresh data?, 98	How to view Printer Configuration reports?, 86
How to scan specific servers in a domain?, 106	How to view Service information?, 49
How to Uninstall ARKWE?, 209	How to view Shares and Resources information?, 33
How to view Built-in Permissions Reports, 51	How to view Users and Groups information?, 37
How to view Built-in Reports for Domains?, 75	Interactive Report, 187, 195
How to view Built-in Reports for Shares and Resources, 67	Internet Service Providers, 3
How to view Built-in Reports for Users and Groups, 71	Intranets, 3
How to view Current Status reports?, 93	IP address, 184
How to view Display Configuration reports?, 90	IT infrastructure Managers, 1
How to view Domain information?, 30	LAN, 3
How to view Environment Info reports?, 94	license key, 4, 5
How to view Events information?, 46	MDB, 109
How to view Hardware Configuration reports?, 87	Microsoft Windows Network., 1
How to view Internet Explorer Configuration reports?, 92	Operating System, 84
How to view Network Configuration reports?, 81	Permissions Reports, 51, 52, 123, 124
	Power Export, 109
	Power Export tool., 79, 108
	Scan Profile, 107, 108, 114, 117, 180, 181, 183, 184, 185, 186, 187, 188, 189, 193, 194, 195
	Scan Profiles, 179, 180, 185, 186, 187, 188, 189, 190, 193, 194, 195, 196

Scan Profiles Manager, 179	Systems Audit personnel, 1
Schedule Built-in Reports, 123	Systems management personnel, 3
Schedule Standard Reports, 112	Task Manager-Scheduled Tasks Manager, 110
Server-based Reports, 187, 188	Technical Support, 6
Server-based Reports., 187	TIFF, 109
Shares and Resources, 33, 51, 67, 123, 150	Troubleshooting, 208
SMTP server, 100	uninstall, 209, 211
SMTP Server, 100	uninstall wizard, 209
SOX, 1	Users and Groups, 37, 51, 71, 74, 123, 160, 195
Standard Reports (Working with Reports), 30	WAN, 3
System Administrators, 1, 3	Windows network product developers, 3
System Information, 79	Windows Servers, 3, 78
System requirements, 2	