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: <u>http://www.vyapin.com/</u> Sales Contact: <u>sales@vyapin.com</u> Technical Support: <u>support@vyapin.com</u>

Table of Contents

1	Gei	neral Information	l
	1.1	About Admin Report Kit for Windows Enterprise (ARKWE)	L
	1.2	System Requirements	2
	1.3	Who Can Use ARKWE?	R
	1.4	How to purchase?	
	1.5	How to register the Software?	5
	1.6	Technical Support	9
2	Get	ting Started	2
	2.1	Configuration Wizard	`
	Confi	guration Settings	5
	2.1.	1 Database Settings	5
	2.1.	2 Computer Enumeration	3
	2.1.	3 Configuring Domain Credentials	9
	2.1.	4 Add a Domain/Server	2
	2.1.	5 Edit a Domain/Server24	1
	2.1.	6 Delete a Domain/Server	5
	2.1.	7 Add Domains from Forest	7
	2.1.	8 Configure SMTP Server	C
	2.1.	9 User Connection Profiles	1
3	Sta	ndard Reports	3
	3.1	How to View Domain Information?	2
			-
	3.2	How to View Shares and Resources Information?	5
	3.3	How to View Users and Groups Information? 40	כ
	3.4	How to View Policies Information?	1
	3.5	How to View Events Information?	Э
	3.6	How to View Service Information?	2
4	Bui	lt-in Reports	1
	4.1	About Built-in Reports	

	4.2	How to View Built-in Permissions Reports?
	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
5	Sys	tem Information
	5.1	About System Info
	5.2	How to View Network Configuration Reports?
	5.3	How to View Operating System & Hot Fixes Reports?
	5.4	How to View Printer Configuration Reports?
	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
6	Add	ditional Features
	6.1	How to customize fields?
	6.2	How to Apply Filters?
	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
7	Pov	ver Export
	7.1	About Power Export
	7.2	Task Manager-Scheduled Tasks Manager114
	7.3	Schedule Standard Reports 116

	7.4	Schedule Built-in Reports
	7.5	Schedule Shares and Resources Built-in Reports154
	7.6	Schedule Users and Groups Built-in Reports164
	7.7	Schedule Domain Built-in Reports
8	Sca	n Profiles Manager
	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
	Refere	ences
	8.13	Troubleshooting
	8.14	How to Uninstall ARKWE? 213
9	Ind	ex

Chapter

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

Processor:	Intel Pentium Processor
Disk Space & Memory:	512 MB RAM and minimum of 20 MB of free disk space.
Operating System:	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.
Database:	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.
a a	

Software: MDAC v2.5/2.6/2.8

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 <u>http://www.vyapin.com/</u>. Please contact our Sales department at <u>sales@vyapin.com</u> 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 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.

Register Admin Report Kit for Windows Enterprise	
License Type: 15-day Evaluation Copy To register the software, copy and paste the license key in the textbox below: See example	
	^
Apply Cancel	<u> </u>

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 ARKWE	×
Copyright © 1999-2019	Cit for Windows Enterprise v8.5 Vyapin Software Systems Private Limited. All Rights Reserved. com Web: <u>www.vyapin.com</u>	ò
Program Folder: C:\P	wks47 : vsswks47.vyapin.local Program Files\ARKWE 8.x\ der: C:\Users\Public\Documents\ARKWE 8.x	
Product:		
License Type:	15-day Evaluation Copy	
License Description:	This software is meant solely for evaluation purposes only. This evaluation version exports and e-mails only the first 10 records.	^
You are on day:	1 of 15	
Remaining Days:	14	
Request license key	Register license key	Close

About screen

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

	Request License Key	x			
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.					
*Contact Name:					
* Company:					
*Email:					
* Phone:					
	(Country Code, Area Code, Phone No.)				
* Order ID:					
* Full Computer Name:	rd85.voyager.local				
License Type:	(Optional)				
	e.g., Single License, Site License				
	Submit Cancel				

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. 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.

ARKWE Configuration Wizard
Welcome to ARKWE configuration wizard. The wizard will guide you through the process of configuring ARKWE.
This wizard allows you to configure the following:
1. Database Settings
2. Computer Enumeration
3. Domain Credentials
Show at startup Back Next > Finish Close

Click **Next** to proceed.

Step 1 of 3: Database Settings

Configuration Settings						
Database Settings Select an option for storing the application data either in MS Access or SQL server. If you choose SQL server, enter a SQL server running SQL Server 2005 / 2008 /2012 (Enterprise / Standard / Express) edition and the user credential having sufficient privileges to connect, create and delete database in the specified SQL server.						
Settings Database Settings Computer Enumeration Domain Credentials E-mail Settings User Connection Profile	 Use MS Access Use SQL Server SQL Server: RD28 e.g., MSSQLSRV1 Database Option Use a single central database for all instances of the application Use a separate database for each instance of the application Use a separate database for each instance of the application SQL Server Authentication (Currently logged on user) SQL Server Authentication User Name: sqllogin3 					
• III •	Password: ••••••					
*	<u>O</u> K <u>C</u> ancel					

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.

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

ARKWE Configuration Wizard	×
Step 2 of 3 : Computer Enumeration	
Select an option 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).	*
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.	
O Use Active Directory Services	
Queries your Directory Server to enumerate its computers. This option requires Domain Administrator privilege to connect to your domain controller.	
Show at startup	

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.

ARKWE Configuration Wizard					
Step 3 of 3 : Domain Credentials Manage alternate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. 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.					
🔒 Add 🛃 Edit 🔒 Del	lete 🐔 Connect 🛕 A	dd domains from forest			
Domain/Server Name	Forest Name	User Name	Status		
RD83	HULK	RD83\Administrator	Connected		
Researchlab	researchlab.local	Researchlab\adminuser3	Connected		
voyager	Voyager.local	voyager\adminuser3	Connected		
Show at startup Finish Close					

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.

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

Configuration Settings					
Domain Credentials Manage alternate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. 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.					
E Settings	🔒 <u>A</u> dd 🛃 <u>E</u> dit 🔒 [elete 式 Connect	t 🛕 Add domains	from forest	
Database Settings	Domain/Server Name	Forest Name	User Name	Status	
Computer Enumeration	RD83	HULK	RD83\Administrator	Connected	
Domain Credentials	Researchlab	researchlab.local	Researchlab\adminu	Connected	
E-mail Settings	voyager	Voyager.local	voyager\adminuser3	Connected	
< <u> </u>					
				Glose	

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:

Configuration Settings	×
SQL server running SQL Se	he application data either in MS Access or SQL server. If you choose SQL server, enter a rver 2005 / 2008 /2012 (Enterprise / Standard / Express) edition and the user credential o connect, create and delete database in the specified SQL server.
Settings Database Settings Omputer Enumeration Omain Credentials E-mail Settings User Connection Profile	 Use MS Access Use SQL Server SQL Server: RD28 e.g., MSSQLSRV1 Database Option Use a single central database for all instances of the application Use a separate database for each instance of the application Windows Authentication (Currently logged on user) SQL Server Authentication User Name: sqllogin3
	<u>O</u> K <u>Cancel</u>

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:

Configuration Settings	
anetwork, the application m	rating computers in your domain. In order to automatically enumerate computers in your ay be configured to use either the Computer Browser Service (uses Windows Network APIs) or ies your AD for Computer Accounts).
Settings 	 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. Use Active Directory Services Queries your Directory Server to enumerate its computers. This option requires Domain Administrator privilege to connect to your domain controller.
۰	

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.

Configuration Settings				—
selected domain. The species information. If you want to s	als for Domain / Directory Se ified credentials will be used specify alternate Domain Adr from forest' option to enumer I domain.	to connect to all comp ninistrator credentials yo	uters in the domain ou may do so by cli	to retrieve report cking on the 'Add' button
E Settings	🔒 <u>A</u> dd 🗗 <u>E</u> dit 🔒	Delete 🖓 Connec	t 🛕 Add dom	ains from forest
Database Settings Computer Enumeration Domain Credentials E-mail Settings User Connection Profile		Forest Name	User Name	Status
5				Qlose

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.

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.

🕌 Domains - Shares (Enterpr	ise - DOMAINS)			
🖸 Refresh 👻 🔜 Export 🛛 🖷	🛛 Filter 🛛 💼 Customize 🖉	E-mail	[]	Find 🗾
Enterprise - DOMAI	Mary Summary Trust	📕 Shares 🌆 A	pplications	
VOYAGER				
🕂 Add Domains				
👬 Domains - Shares (Enterpri	ise - DOMAINS)			
🖸 Refresh 🗸 📑 Export 🛛		E-mail	1	Find
Enterprise - DOMAI	😭 Summary 🛛 🖉 Trust	딣 Shares 🌆 A	pplications	
🖳 RD83	Domain Credentials			
	Manage alternate credentials		Servers. Specify an account name	e that has admin privileges to
VOYAGER			used to connect to all computers main Administrator credentials you	
		'Add domains from forest	option to enumerate domains fro	
	supply necessary credentials	for the selected domain.		
		Add domains from f	orest	
	Domain/Server Name	Forest Name	User Name	Status
	RD83	HULK	RD83\Administrator	Connected
	Researchlab	researchlab.local	Researchlab\adminuser3	Connected
	voyager	Voyager.local	voyager\adminuser3	Connected
4				
< Ⅲ ►				Gose

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

Operation	Description
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 ^BAdd button to add a domain/server to the list.
- 3) The New Add domain/server dialog will be displayed as shown below:

🙀 Add domain/server	-X
Specify a Domain name to retrieve computers preser domain. Clear the 'Log on using current user' checkb specify alternate credentials for connecting to the do server.	oox to
Domain (or) Server Name:	
Log on using current user	
User Name: phoenix\Administrator	-
Password:	
Store the above credentials in Microsoft window Stored User Name and Passwords applet	is 🕐
<u>O</u> K	<u>C</u> ancel

Enter the name of a domain or server.

👬 Add domain/server	x
Specify a Domain name to retrieve computers present in domain. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the domain or server.	or
Domain (or) Server Name: voyager	
Log on using current user	
User Name: voyager\adminuser3	
Password:	
Store the above credentials in Microsoft windows Stored User Name and Passwords applet	0
	el

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.

Configuration Settings				
Domain Credentials Manage alternate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. 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.				
E Settings	🔒 <u>A</u> dd 🛛 🛃 <u>E</u> dit	<mark> D</mark> elete 🛛 🏹 Conr	nect 🛛 🔬 Add domai	ns from forest
Database Settings	Domain/Server Name	Forest Name	User Name	Status
Domain Credentials	RD83	HULK	RD83\Administrator	Connected
	Researchlab	researchlab.local	Researchlab\adminus	Connected
	voyager	Voyager.local	voyager\adminuser3	Connected
				Glose

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:

Configuration Settings				
Domain Credentials Manage alternate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. 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.				
E Settings	🔒 <u>A</u> dd 🛛 🛃 <u>E</u> dit	<u> D</u> elete 🛛 式 Conn	ect 🛛 🛕 Add domai	ns from forest
Database Settings Gomputer Enumeration	Domain/Server Name	Forest Name	User Name	Status
Domain Credentials	RD83	HULK	RD83\Administrator	Connected
🛶 E-mail Settings	Researchlab	researchlab.local	Researchlab\adminuse	Connected
	voyager	Voyager.local	voyager\adminuser3	Connected
				Glose

- **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.

Configuration Settings				
Domain Credentials Manage altemate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. If you want to specify altemate 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.				
⊡… 🌍 Settings	🔒 <u>A</u> dd 🛃 <u>E</u> dit	<u>]</u> Delete 🛛 式 Conn	ect 🛛 🛕 Add domair	ns from forest
Database Settings 	Domain/Server Name	Forest Name	User Name	Status
Domain Credentials	RD83	HULK	RD83\Administrator	Connected
E-mail Settings	Researchlab	researchlab.local	Researchlab\adminuse	Connected
	voyager	Voyager.local	voyager\adminuser3	Connected
٩ 💷 ۲				
				Close

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.

Configuration Settings				
Domain Credentials Manage alternate credentials for Domain / Directory Servers. Specify an account name that has admin privileges to the selected domain. The specified credentials will be used to connect to all computers in the domain to retrieve report information. 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.				
E Settings	🔒 <u>A</u> dd 🛃 <u>E</u> dit	<mark> D</mark> elete 🛛 式 Conr	nect 🛛 🛕 Add domai	ns from forest
Database Settings	Domain/Server Name	Forest Name	User Name	Status
Domain Credentials	RD83	HULK	RD83\Administrator	Connected
🛶 E-mail Settings	Researchlab	researchlab.local	Researchlab\adminus	Connected
User Connection Profile	voyager	Voyager.local	voyager\adminuser3	Connected
۰ III ا				
				Glose

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 \triangle 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:

🔬 Enumerate all Do	mains in a forest			
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.				
Forest Name:				
	name you specify here must nust be able to resolve the sp		er. Domains in forest ()	
🔽 Log on using c	urrent user	Show Domains	<< 21	
User Name:	RD54\Administrator	*		
Password:				
Store the a Store Use	bove credentials in Microsol er Name and Passwords app	it windows Iet		
			<u> </u>	

Enter the name of a forest.

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

🔝 Enumerate all Domains in a forest 🛛 💦 💽					
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.					
Forest Name:	pathfind	ler.local			
		ame you specify here must be visible f ist be able to resolve the specified DN		Domains in forest ()	_
📃 Log on (using cu	rrent user	Show Domains >>		
User Na	ame:	adventure\adminuser 🗸 🗸			
Passwo	ord:	•••••			
Store the above credentials in Microsoft windows Stored User Name and Passwords applet					
				<u> </u>	el

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:

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

🔝 Enumerate all Domains in a forest 🛛 💦 🐼					
Specify a Forest Name. The Forest Name will be used to retrieve domains present in the forest. Clear the 'Log on using current user' checkbox to specify alternate credentials for connecting to the forest.					
Forest Name:	pathfine	ler.local			
		ame you specify here must be visible f st be able to resolve the specified DN		Domains in forest [pathfinder.local]	
Log on using current user		Show Domains >>			
User Na	ame:	Pathfinder\adminuser -		Mathfinder	
Passwo	ord:	•••••			
Store the above credentials in Microsoft windows Stored User Name and Passwords applet					
				<u> </u>	

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

Configuration Settings				—
Domain Credentials Manage alternate credentials for Domain / Directory Servers. The application by default uses the currently logged on user context to enumerate computers and shares and to collect NTFS permissions 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.				
⊑~ 🚳 Settings	🔒 🗛 dd 🛛 🕂 Edit 🗧 🔒 Delete 🛛 🖏 Connect 🛛 🔬 Add domains from forest			
🔤 📕 Database Settings	Domain Name	Forest Name	User Name	Status
Computer Enumeration	adventure	Adventure.local	adventure\adminuser	Connected
- Domain Credentials	pathfinder	pathfinder.local	Pathfinder\adminuser	Connected
E-mail Settings				
🦾 🍳 User Connection Profil				
				Close

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:

Configuration Settings			×
E-mail Settings Specify the SMTP Server na	me and Sender (Fro	om) e-mail address to send the generated reports through	ı e-mail.
Settings Database Settings Omputer Enumeration Domain Credentials E-mail Settings User Connection Profil	SMTP Server: When you send	r is the server that is used for your outgoing e-mail. rd45 le-mail, your name will appear in the from of the ge.Type your name as you would like it to appear. Alex E.Fring@pathfinder.local E.x: someone@example.com	
		<u> </u>	<u>C</u> ancel

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.

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

Configuration Settings					
User Connection Profiles ARKWE can store user credential information as user profiles for Directory Servers using Windows Stored User Name and Passwords applet. To add a user profile, click Add. To delete a user profile, click Remove.					
E Settings	♣ <u>A</u> dd ∥ Ed <u>i</u> t × <u>R</u> emove				
Computer Enumeration	Profile Name	Description			
Computer Enumeration Domain Credentials E-mail Settings User Connection Profile	Treelab\adminuser2 researchlab\adminuser2	Sample			
	, <u> </u>	Glose			

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

New User Profile				
Create a new user profile and store it in windows stored usernames and passwords applet.				
User Name: *	Pathfinder\Scholes			
	e.g. , domain\username			
Password: *	•••••			
Confirm Password: *	•••••			
Description:		*		
		-		
(* mandatory fields)				
		ncel		

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

	Stan	dard Reports		7	
	Ĥ	Domains	•	P	Summary
	88	Users and Groups	•	₫	Trust
	3	Shares and Resources	•	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Shares
	B	Policies	•	-	Applications
	8	Events	•		
Click	-	Services	•		

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 '<u>How to scan specific servers in a domain?</u>'

The output would be displayed as shown below:

🙀 Domains - Summary (VOY	AGER)			
🧿 Refresh 🔹 🚘 Export 🛛 📲	Filter Cust	tomize 🔤 E-mail	Find	
Enterprise - DOMAI	Summary	🐼 Trust 😡 Shares 🌆 Applications		
📇 RD83	Generated on: 30	0 Dec, 2014, 10:35:28 AM Status: Success Filter: Not Applied		
RESEARCHLAB	Host Name	Attribute		
VOYAGER	RD40	P Address: 10.10.10.39		
		OS Install Date: 1/8/2014 10:19:50 AM		
		OS: Microsoft Windows Server 2012 Standard Build 9200		
		Role: DFS		
		Role: LM Server		
		Role: LM Workstation		
		Role: Master Browser		
		Role: NT		
		Role: Primary Domain Controller		
		Role: Timesource		
		Server Type: Primary Domain Controller		
		System Type: x64-based PC		
		Windows Directory: C:Windows		
	RD41	IP Address: 10.10.10.78		
		OS Install Date: 1/8/2014 11:32:46 AM		
		OS: Microsoft Windows Server 2012 Standard Build 9200		
		Role: Backup Browser		
		Role: LM Server		
		Role: LM Workstation		
		Role: NT		
• III •		Role: Potential Browser		
👍 Add Domains		Role: Server NT		

Domain Trust Information

	Stan	dard Reports			
	ř.	Domains	•	P	Summary
	88	Users and Groups	•	₫	Trust
	3	Shares and Resources	•	5	Shares
	-	Policies	•	-	Applications
	8	Events	•		
Click	1 ⁴⁴	Services	•		

to view the trusted and trusting

domains for a given domain.

🚔 Domains - Trust (VOYAGE	R)					- • •
🖸 Refresh 🔹 📾 Export 🛛 🖷	🛛 Filter 🛛 💼 Customize 🕸	🕹 E-mail			Find	2
Enterprise - DOMAI	🚰 Summary 🚺 Trus	📮 Shares 🛙	Applications			
🖲 RD83	Generated on: 30 Dec, 2014		Status: Success	Filter: Not Applied		
	Domain Names	Trusted	Trusting			
VOYAGER	vsslab.local	Yes	Yes			
	venus.Voyager.local	Yes	Yes			
<→						
👍 Add Domains						

Domain Shares Information



to view the shares for a given

domain.

	Summ	Customize	·					Find
1		on: 30 Dec, 201		Applications Status: Succes	s Filter: N	lot Applied		
ESEARCHLAB OYAGER	Host Name	IP Address	Share Name	Path	User Name	Security	Maximum Uses	Comment
	RD40	10.10.10.39	ADMINS	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		
				D:\Folder	BUILTIN\Administ	Allow - Full Control	Unlimited	
	latest setup	D:\latest setup	Everyone	Allow - Full Control	Unlimited	Latest Setup Share		
				D:\latest setup	BUILTIN\Administ	Allow - Full Control	Unlimited	Latest Setup Share
			Module	D:\Module	BUILTIN\Administ	Allow - Full Control	Unlimited	
				D:\Module	Everyone	Allow - Full Control	Unlimited	
			NETLOGON	C:\Windows\SY	Everyone	Allow - Read	Unlimited	Logon server share
				C:\Windows\SY	BUILTIN\Administ	Allow - Full Control	Unlimited	Logon server share
			NTFS Share	C:WTFS Test Fol	VOYAGER\admin	Allow - Full Control	Unlimited	
			NTFSTestFolder	C:\NTFS Test Fol	Everyone	Allow - Read	Unlimited	
			Share	D:\Share	Everyone	Allow - Full Control	Unlimited	
				D:\Share	BUILTIN\Administ	Allow - Full Control	Unlimited	
			share22	D:\share22	BUILTIN\Administ	Allow - Full Control	Unlimited	
				D:\share22	Everyone	Allow - Full Control	Unlimited	
			SPListX Target	D:\SPListX Target	Everyone	Allow - Full Control	Unlimited	
				D:\SPListX Target	BUILTIN\Administ	Allow - Full Control	Unlimited	
- F			SYSVOL	C:\Windows\SY	Everyone	Allow - Read	Unlimited	Logon server share
dd Domains				C:\Windows\SY	NT AUTHORITY\	Allow - Full Control	Unlimited	Logon server share

Domain Application Information



for a given domain.

NOTE: For information on restricting the domain scan for generating this report, please see <u>How to scan specific servers in a domain</u>?

efresh 🔹 📑 Export 🛛 🕎	Filter Dustor	nize 🛛 🚭 E-n	nail				Fi	nd	
Enterprise - DOMAI	Summary	🛛 Trust 🔒	Shares 🛅 App	lications					
	Generated on: 30 D	ec, 2014, 10:38	8:36 AM S	tatus: Success	Filter: Not Ap	pplied			
(E) RESEARCHLAB	Host Name 🔍	IP Address	Application Name	Version	Path	Installed Date	Publisher	Readme	Size (KE
	RD43	10.10.10.31							
		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	2.2.760	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 Educati	15.0.4420.1017	C:\Program Files\	3/7/2014	Microsoft Corporation		166974
		10.10.10.31	Microsoft Educati	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		6/23/2014	Microsoft Corporation		4245
		10.10.10.31	Microsoft Identity	2.0.1459.0		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?



to view the following information:

Share Name, Path, User Name, Security, Maximum, and Comment

		Scan Profiles (Computers) - 🔤 E-mail				Find
Enterprise - SHARES AN	🔊 Shares [🖺 Folders 🗋 Files				
	Generated on: 30	Dec, 2014, 10:42:11 AM Status: Success	Filter: Not Applie	d		
RESEARCHLAB	Share Name	Path	User Name	Security	Maximum Uses	Comment
🖶 🖳 Domain Controllers	ADMIN\$	C:\Windows			Unlimited	
	C\$	C:\		Admin Share	Unlimited	Default share
Servers	D\$	D:\		Admin Share	Unlimited	Default share
	Folder	D:\Folder	BUILTIN\Administrators	Allow - Full Control	Unlimited	
-			Everyone	Allow - Full Control	Unlimited	
Workstations	latest setup	D:\latest setup	BUILTIN\Administrators	Allow - Full Control	Unlimited	Latest Setup Share
- RD72			Everyone	Allow - Full Control	Unlimited	Latest Setup Share
	Module	D:\Module	BUILTIN\Administrators	Allow - Full Control	Unlimited	
📇 RD81			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	
4 11	SPListX Target	D:\SPListX Target	BUILTIN\Administrators	Allow - Full Control	Unlimited	

How to View Permissions of Folders in a Share?



Permissions" dialog appears.

I Shares and Resources - Folders (RD40)		×
🖸 🥵 Refresh 👻 🔝 Export 🍸 Filter 🛅 Customize (Scan Profiles (Computers) - 🔤 E-mail Find	(0)
🖃 🕞 Enterprise - SHARES AN 🔒 Shares 🧮	Folders Folders and Permissions	
₽	All shares	
RESEARCHLAB	Select share(s)	
UVYAGER	Folder	
Domain Controllers	Iatest setup	
RD40	Module	
Erweins RD41		
RD41	MTFS Share	
Workstations	MTFS Test Folder	
RD71	Share	
	Include sub-folders	
	Traverse only 1 vel(s) of sub-folder in the share	
< Þ	Do not display folders that have the same permissions as the parent folder	
Add Domains	QK Cancel	

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 subfolder 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.

The report would be displayed as shown below:

Name Folder BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No Tr Bonain Controllers RD40 Folder BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No Tr Bonain Controllers Polder Folder BUILTIN/Administrators NTAUTHORTIN/SYSTEM Allow - Full Control No Tr Bonain Control RD41 Folder BUILTIN/Administrators VOYAGER/Adminstrator Allow - Full Control No Tr Bonain Control RD43 Iatest setup BUILTIN/Administrators VOYAGER/Adminstrators Allow - Full Control No Tr Bonain Control RD43 Iatest setup BUILTIN/Administrators VOYAGER/Adminstrators Allow - Full Control No Tr Bonain RD71 Iatest setup BUILTIN/Administrators VOYAGER/Administrator Allow - Full Control No Tr Bonain RD71 Iatest setup BUILTIN/Administrators VOYAGER/Adminuterator Allow - Full Control No Tr Bonain<		
ResearchLAB Share Folder Path Sub-Folders Owner User Name Security Inherited A Workader Bonain Controlers R040 Folder BUILTIN/Administrators BUILTIN/Administrators Allow -Full Control No There B R040 R041 Folder Folder BUILTIN/Administrators BUILTIN/Administrators Allow -Full Control No Th B R041 Folder BUILTIN/Administrators VOYAGER/Administrator Allow -Full Control No Th B R041 Folder BUILTIN/Administrators VOYAGER/Administrator Allow -Full Control No Th B R071 Folder BUILTIN/Administrators VOYAGER/Administrator Allow -Full Control No Th B R072 R073 R073 Allow -Full Control No Th B R071 R073 R073 Allow -Full Control No Th B R071 R073 R073 Allow -Full Control No Th B R073 R073 R074		
Servers Solar Folder Path Sub-Folders Owner User Name Security Inherited A B Bomain Controlers Folder Folder BUILTIN/Administrators BUILTIN/Administrators Allow -Full Control No. T B RD40 Folder BUILTIN/Administrators NTA UTHORITY (SYSTEM Allow -Full Control No. T B RD41 Folder BUILTIN/Administrators VYAGER (Administrator NTA UTHORITY (SYSTEM Allow -Full Control No. T B RD41 Folder BUILTIN/Administrators VYAGER (Administrator Allow -Full Control No. T B RD71 Folder BUILTIN/Administrators VYAGER (Administrator Allow -Full Control No. T B RD71 Iatest setup BUILTIN/Administrators VYAGER (Administrator Allow -Full Control No. T B RD73 Iatest setup BUILTIN/Administrators VYAGER (Administrator Allow -Full Control No. T B		
Polder BUILTIN/Administrators NT AUTHORITY(SYSTEM Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Allow - Full Control No Th Image: Servers Servers Servers Servers Servers	Apply To	d Apply To
Index Bervers Folder BUIL TIN-Valminisators NV INCERT (5) Folder/set (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	This folder, subfolders and files	This folder, subfolders and
B R041 Folder BUILTIN-Valministators VOYAGER-Valminuer3 Allow - Full Control No Tit Workstations B R071 Istest setup BUILTIN-Valministrators ULTIN-Valministrators Allow - Full Control No Tit B R071 Istest setup BUILTIN-Valministrators NUTANVAlministrators Allow - Full Control No Tit B R073 Istest setup BUILTIN-Valministrators VOYAGER-Valminuer1 Allow - Full Control No Tit B R073 Istest setup BUILTIN-Valministrators VOYAGER-Valminuer1 Allow - Full Control No Tit B R073 Istest setup BUILTIN-Valministrators VOYAGER-Valminuer1 Allow - Full Control No Tit B R074 Istest setup BUILTIN-Valministrators VOYAGER-Valminuer1 Allow - Full Control No Tit B R073 BUILTIN-Valministrators VOYAGER-Valminuer3 Allow - Full Control No Tit B R074 BUILTIN-Valministrators BUILTIN-Valministrators BUILTIN-Valministrators Allow - Creater Fin. <td>This folder, subfolders and files</td> <td>This folder, subfolders and</td>	This folder, subfolders and files	This folder, subfolders and
BR043 Interstep Folder BUILTIN/Administrators VIXAdeXipdamuser3 Allow - Full Control No Th Idext setup BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No Th Idext setup BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No Th Idext setup BUILTIN/Administrators V0YAGER/Administrators NOYAGER/Administrators Allow - Full Control No Th Idext setup BUILTIN/Administrators V0YAGER/Adminuser3 Allow - Full Control No Th Idext setup BUILTIN/Administrators V0YAGER/Adminuser3 Allow - Full Control No Th Idext setup BUILTIN/Administrators V0YAGER/Adminuser3 Allow - Full Control No Th Idext setup BUILTIN/Administrators V0YAGER/Adminuser3 Allow - Full Control No Th Idext setup BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators Blow - Full Control No <td>This folder, subfolders and files</td> <td>This folder, subfolders and</td>	This folder, subfolders and files	This folder, subfolders and
Iatest setup BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No TT Iatest setup BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No TT Iatest setup BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No TT Iatest setup BUILTIN/Administrators NT AUTHORITY (SYSTEM Allow - Full Control No TT Iatest setup BUILTIN/Administrators VOYAGER/Administrators NOVAGER/Administrators Nov - Full Control No TT Iatest setup BUILTIN/Administrators VOYAGER/Administrators VOYAGER/Administrators Allow - Full Control No TT Iatest setup BUILTIN/Administrators VOYAGER/Administrators VOYAGER/Administrators Allow - Full Control No TT Iatest setup BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators Allow - Full Control No TT Iatest setup RD84 NETLOGON NETLOGON BUILTIN/Administrators Allow - Create Fin. No TT NETLOGON BUILTIN/Administrators BUILTIN/Administrators BUILTIN/Administrators Allow - Create Fin. No TT NETLOGON BUILTIN/Administrator	This folder, subfolders and files	This folder, subfolders and
BRD71 BRD72 BRD72 BRD73 RD72 BRD73 RD73 RD73 RD73 RD73 RD73 RD73 RD74 RD74 RD74 RD75 RD	This folder, subfolders and files	This folder, subfolders and
BULT RD72 Iatest setup BULTINVAdministrators VOYAGER\Administrator Alow - Full Control No Th B RD31 Iatest setup BULTINVAdministrators VOYAGER\adminuser1 Alow - Full Control No Th B RD81 Iatest setup BULTINVAdministrators VOYAGER\adminuser1 Alow - Full Control No Th B RD83 NETLOGON NETLOGON BULTINVAdministrators VOYAGER\adminuser1 Alow - Change No Th NETLOGON NETLOGON BULTINVAdministrators BULTINVAdministrators BULTINVAdministrators Alow - Create Fi No Th NETLOGON BULTINVAdministrators BULTINVAdministrators BULTINVAdministrators Alow - Create Fi No Th NETLOGON BULTINVAdministrators BULTINVAdministrators BULTINVAdministrators Alow - Create Fi No Th NETLOGON BULTINVAdministrators BULTINVAdministrators BULTINVAdministrators Alow - Create Fi No Th	This folder, subfolders and files	This folder, subfolders and
RD81 BAD81 BAD81 RD83 RD84 NETLOGON VRD40\NETLOGON RUILTIN\Administrators RD84 NETLOGON RUILTIN\Administrators RD84 NETLOGON RUILTIN\Administrators RUILTIN\Admi	This folder, subfolders and files	This folder, subfolders and
RD83 RD83 RD84 NETLOGON NETLOGON NETLOGON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Change No Th NetLogON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Create F No Th NetLogON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Create F No Th NetLogON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Create F No Th NetLogON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Full Control No Sc	This folder, subfolders and files	This folder, subfolders and
RD84 NETLOGON BUILTIN'Administrators BUILTIN'Administrators Allow - Create Fi No 17 NETLOGON BUILTIN'Administrators BUILTIN'Administrators Allow - Create F No 17 NETLOGON BUILTIN'Administrators BUILTIN'Administrators Allow - Full Control No 5	This folder, subfolders and files	This folder, subfolders and
NETLOGON BUILTIN\Administrators BUILTIN\Administrators Allow - Create F No TT NETLOGON BUILTIN\Administrators BUILTIN\Administrators BUILTIN\Administrators Allow - Full Control No St	This folder only	This folder only
NETLOGON BUILTIN\Administrators BUILTIN\Administrators Allow - Full Control No Su	This folder only	This folder only
	This folder only	This folder only
	Subfolders and files only	Subfolders and files only
NETLOGON BUILTIN\Administrators BUILTIN\Administrators Allow - List Folde No Th	This folder only	This folder only
NETLOGON BUILTIN\Administrators BUILTIN\Administrators Allow - Read Att No Th	This folder only	This folder only
NETLOGON BUILTIN\Administrators BUILTIN\Administrators Allow - Read Ext No Th	This folder only	This folder only

How to view permissions of files in a share?



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.

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:

efresh 👻 💼 Export 🛛 🕎 Filter	r Ustor	nize 🛛 💽 Scan Pro	files (Comput	:ers) - 🖓	E-mail				Find
Enterprise - SHARES AN	🚽 Shares	s 🧮 Folders	Files						
	Generated of	n: 30 Dec, 2014, 10:5	0:49 AM	Status:	Success Filter	Not Applied			
RESEARCHLAB VOYAGER	Share Name	Folder/File Path	Folder/File Name	Folder/File Type	Owner	User Name	Security	Inherited	Apply To
🛓 🔁 Domain Controllers	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
- E Servers			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
Workstations	latest setup	la	latest setup	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Full Control	No	This folder, subfolders and files
B RD71			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 \adminuser 1	Allow - Full Control	No	This folder, subfolders and files
			latest setup	Folder	BUILTIN\Administrators	VOYAGER \adminuser 3	Allow - Full Control	No	This folder, subfolders and files
	NETLOGON	\\RD40\NETLOGON	NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Change	No	This folder only
🖳 🖶 RD84			NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Create Fi	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
HII +			NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Ext	No	This folder only
🕂 Add Domains			NETLOGON	Folder	BUILTIN\Administrators	BUILTIN\Administrators	Allow - Read Per	No	This folder only

3.3 How to View Users and Groups Information?



User Name, Full Name, Description, Home Path, Logon Script, and User Profile Path.

🛃 Users and Groups - General (R	D40)						×
Refresh 🔹 🕎 Filter 📑 Exp	ort 🛛 💼 Customize	📧 Scan Profiles (Com	puters) 👻 🖼 E-mail		Fit	nd	2
	🚰 General 🖉 Str	atus 🍳 Logon 🧾 I	Privileges 👃 User-Groups 😣 Group-Members				
🗉 🕘 RD83	Generated on: 30 Dec, 2	2014, 10:15:16 AM	Status: Success Filter: Not Applied				
RESEARCHLAB	User Name	Full Name	Description	Home Path	Logon Script	User Profile Path	-
UOYAGER	Administrator		Built-in account for administering the computer/domain				
B RD40	Guest		Built-in account for guest access to the computer/domain				-11
Servers	krbtgt		Key Distribution Center Service Account				
- 🖪 RD41	adminuser1	adminuser 1					
	adfssvcacc	adfssvcacc					
🖶 🚇 Workstations	adminuser2	adminuser2					
🖶 RD71	adminuser3	adminuser3					
	configdbadmin_sp03	configdbadmin_sp03					
📇 RD73	defconaccessacc_sp03	defconaccessacc_sp03					
	portsiteapppool_sp03	portsiteapppool_sp03					
	spapppool1_sp03	spapppool1_sp03					
	spapppool2_sp03	spapppool2_sp03					
	spapppool3_sp03	spapppool3_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					
💠 Add Domains	searchdefacc_sp07-2	searchdefacc_sp07-2					-



information: User Name, Full Name, Description, Account Expiry, Password Editable, Password Age, Account Locked, and Account Disabled.

CHAPTER 2 – Standard Reports

lefresh 🝷 🕎 Filter 🛛 📑 Exp	oort 💼 Customize 🚺	Scan Profiles	(Computers) — 🔄 E-mai	l i i i i i i i i i i i i i i i i i i i			Find	
🚱 Enterprise - USERS AM	😁 General 🔮 Sta	tus 🍳 Logon	🥑 Privileges 🤱 User-(Groups 🎎 Group-	Members			
🗄 🚇 RD83	Generated on: 30 Dec, 2	014, 10:15:16 AM	Status: Success	Filter: No	t Applied			
E RESEARCHLAB	User Name	Full Name	Description	Account Expiry	Password Editable	Password Age	Account Locked	Account Disabled
😑 📇 Domain Controllers	Administrator		Built-in account for admi	Never expires	Yes	96 Day(s), 15 Hr(s), 15 Min	No	No
	Guest		Built-in account for guest	Never expires	No		No	Yes
Servers BD41	krbtgt		Key Distribution Center S	Never expires	Yes	356 Day(s), 3 Hr(s), 53 Min	No	Yes
	adminuser1	adminuser 1		Never expires	Yes	355 Day(s), 7 Hr(s), 40 Min	No	No
Workstations	adfssvcacc	adfssvcacc		Never expires	No	355 Day(s), 6 Hr(s), 38 Min	No	No
RD71	adminuser2	adminuser2		Never expires	Yes	355 Day(s), 6 Hr(s), 31 Min	No	No
📇 RD72	adminuser3	adminuser3		Never expires	Yes	355 Day(s), 6 Hr(s), 30 Min	No	No
	configdbadmin_sp03	configdbadmi		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
📇 RD84	portsiteapppool_sp03	portsiteappp		Never expires	No	355 Day(s), 6 Hr(s), 27 Min	No	No
	spapppool1_sp03	spapppool1		Never expires	No	355 Day(s), 6 Hr(s), 26 Min	No	No
	spapppool2_sp03	spapppool2		Never expires	No	355 Day(s), 6 Hr(s), 26 Min	No	No
	spapppool3_sp03	spapppool3		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
4 11	farmadmin_sp07-2	farmadmin_s		Never expires	No	355 Day(s), 6 Hr(s), 22 Min	No	No
Add Domains	searchdefacc_sp07-1	searchdefacc		Never expires	No	355 Day(s), 6 Hr(s), 21 Min	No	No



information: User Name, Logon Machines, Last Logon.

Refresh 👻 🕎 Filter 🛛 📑 Exp	iort 🛄 Customize 💽 S			Find	9
- 🚱 Enterprise - USERS Al	🚰 General 🛛 🌺 Status	🔍 Logon 🧾 Privileges	s 🤱 User-Groups 🎎 Group-Members		
🗄 🚇 RD83	Generated on: 30 Dec, 2014	, 10:15:16 AM Sta	tus: Success Filter: Not Applied		
	User Name	Logon Machines	Last Logon		
UOYAGER	Administrator	Any Workstation	12/29/2014 7:44:59 PM		
B RD40	Guest	Any Workstation			٦
- I Servers	krbtgt	Any Workstation			
- 🗒 RD41	adminuser1	Any Workstation	12/29/2014 7:49:42 PM		
	adfssvcacc	Any Workstation			
- 🕒 Workstations	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			
	portsiteapppool_sp03	Any Workstation			
	spapppool1_sp03	Any Workstation			
	spapppool2_sp03	Any Workstation			
	spapppool3_sp03	Any Workstation			Т
	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			
4 11	searchdefacc_sp07-1	Any Workstation			
👍 Add Domains	searchdefacc_sp07-2	Any Workstation			1



to view the following

information: Displays privilege lists on a per-user and per-privilege basis.

lefresh 👻 🕎 Filter 🛛 🚔 Exp	oort 🛛 💼 Customize 🖉 💽 Scan Profiles (Comput	ters) 🔹 🙀 E-mail	Find
Enterprise - USERS AN	😁 General 🐼 Status 🔍 Logon 📃 Priv	ileges & User-Groups & Group-Members	
🖻 🚇 RD83	Generated on: 30 Dec, 2014, 10:26:21 AM	Status: Success Filter: Not Applied	
RESEARCHLAB	User Name	Privilege	
VOYAGER	NT AUTHORITY/NETWORK SERVICE	Replace a process level token	
RD40	NT AUTHORITY\LOCAL SERVICE	Replace a process level token	
Servers	NT AUTHORITY\NETWORK SERVICE	Generate security audits	
- B RD41	NT AUTHORITY\LOCAL SERVICE	Generate security audits	
	BUILTIN\Backup Operators	Back up files and directories	
🗄 🚇 Workstations	BUILTIN\Server Operators	Back up files and directories	
	BUILTIN\Administrators	Back up files and directories	
	BUILTIN\Performance Log Users	Log on as a batch job	
	BUILTIN\Backup Operators	Log on as a batch job	
	BUILTIN\Administrators	Log on as a batch job	
	Window Manager\Window Manager Group	Bypass traverse checking	
	BUILTIN\Pre-Windows 2000 Compatible Access	Bypass traverse checking	
	BUILTIN\Administrators	Bypass traverse checking	
	NT AUTHORITY\NETWORK SERVICE	Bypass traverse checking	
	NT AUTHORITY\LOCAL SERVICE	Bypass traverse checking	
	NT AUTHORITY\Authenticated Users	Bypass traverse checking	
	Everyone	Bypass traverse checking	
4 11	BUILTIN\Administrators	Create a pagefile	
Add Domains		Debug programs	



Click on

information: Displays group lists on a per-user and per-group basis.

🖲 Users and Groups - User-Grou 🔉 Refresh 👻 🍸 Filter 🛛 🙀 Exp		re 🖉 Scan Profiles (Comp		x
Enterprise - USERS AN		Status 🔍 Logon 🧾 Pri		
		Dec, 2014, 10:27:19 AM	Status: Success Filter: Not Applied	-
RESEARCHLAB	User Name	Member of	Membership Group Description	
- E VOYAGER	Administrator	Administrators	Administrators have complete and unrestricted access to the computer/domain	ſ
Domain Controllers BD40		Schema Admins	Designated administrators of the schema	1
Servers		Enterprise Admins	Designated administrators of the enterprise	1
- 🗒 RD41		Group Policy Creator Owners	Members in this group can modify group policy for the domain	1
		Organization Management	Members of this management role group have permissions to manage Exchange objects and their properties in	
		Domain Users	All domain users	1
		Domain Admins	Designated administrators of the domain	
	Guest	Domain Guests	All domain guests	
		Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is	
	krbtgt	Domain Users	All domain users	
		Denied RODC Password R	Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain	
	adminuser1	Administrators	Administrators have complete and unrestricted access to the computer/domain	
		Domain Users	All domain users	
		Schema Admins	Designated administrators of the schema	
		Enterprise Admins	Designated administrators of the enterprise	
		Domain Admins	Designated administrators of the domain	
		DnsAdmins	DNS Administrators Group	
		Organization Management	Members of this management role group have permissions to manage Exchange objects and their properties in	
👍 Add Domains	adfssvcacc	Domain Users	All domain users	



Click on

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

🚇 Users and Groups - Group-M	embers (RD40)			- • •
👩 Refresh 👻 🍸 Filter 🛛 📸 Exp	port 🛛 🛅 Customize 🖉 💽 Scan Prof	files (Computers) 🔹 🔤 E	mail	Find 😥
Enterprise - USERS AM	😁 General 💆 Status 🍳 Log	gon 🧾 Privileges 🤱 U	ser-Groups 🍇 Group-Members	
🗄 🗐 RD83	Generated on: 30 Dec, 2014, 10:29:45	5 AM Status: Suc	cess Filter: Not Applied	
E RESEARCHLAB	Group Name	Description	Account Name	× *
UOYAGER	Domain Users	All domain users	zxgorberen	E
Domain Controllers			Yuvan R. Lee	
E-C Servers			ygorben	
			wsssearch_sp10-1	
			wsssearch_sp07-2	
- 🔄 Workstations			wsssearch_sp07-1	
			Williams T.	
			William K. Tunner / Marketing (Region 5)	
			William Joseph	
			William B. Davis VC (5th Div)	
			Wesley L. Snipes / Support	
			VSSLAB\$	
			Vincent L. George	
			VENUS\$	
			Totti J. Lawrence	
			Thomas Luis	
			SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}	
۰ III +	J		SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}	
🕂 Add Domains			SystemMailbox{1f05a927-07b0-4a24-a61b-a42150f64916}	-

3.4 How to View Policies Information?



Click

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*

Policies - Password (RD40)	-	·~	-			
Refresh				User Rights Assignment	Security Options	Find E
RD83	Generated on: 29 Dec,	2014, 07:17:01 PM	Status: Su	ccess Fitter: N	ot Applied	
RESEARCHLAB VOYAGER Omain Controlk RD40	Enforce password history (passwords remembered)	Maximum password age (days)	Minimum password age (days)	Minimum password length (characters)	Password must meet complexity requirements	Store password using reversible encryption for all domain users
4 Add Domains	24	42	1	7	Enabled	Deabled

	Stan	dard Reports								
	÷.	Domains	►]						
	82	Users and Groups	►							
	3	Shares and Resources	•							
	1	Policies	►	٩	Password					
	8	Events	•	£	Account Lockout					
	<i>#</i> *	Services	•		Audit					
				88	User Rights Assignment					
					Security Options					
Click				2	IP Security	tab	to	view	the	following

information: Account Lockout Duration, Account Lockout Threshold, and Reset Account Lockout



information: Policy Name, Log Success, and Log Failure

CHAPTER 2 – Standard Reports

	🍸 Filter 🛛 💼 Customize 🖉 Scar					Find			
Enterprise - POLIC		Lockout 🔠 Audit				curity			
	Generated on: 29 Dec, 2014, 07:1		tatus: Success		er: Not Applied		_		
UOYAGER	Policy Name Audit system events	Log Success	Log Failu No	ire					
🖻 🚇 Domain Contro	Audit system events	Yes	No						
	Audit object access	Yes	No				_		
🖃 🗐 Servers 🔜 RD41	Audit privilege use	Yes	No						
	Audit process tracking	No	No						
. Workstations	Audit policy change	No	No						
📇 RD71	Audit account management	Yes	No						
📇 RD72	Audit directory service access	Yes	No						
	Audit account logon events	Yes	No						
m									
👍 Add Domains									
		1							
Star	ndard Reports								
Star 1	ndard Reports Domains		•]					
		Dups	+ +						
#1 && _3	Domains Users and Gro Shares and Re		•						
#4 && _= 	Domains Users and Gro Shares and Ro Policies		•	Q	Password				
#1 && _3	Domains Users and Gro Shares and Re		•	Q	Password Account Lockou	ıt			
#4 && _= 	Domains Users and Gro Shares and Ro Policies		•			ıt			
#1 && 	Domains Users and Gro Shares and Ro Policies Events		•	£	Account Lockou				
#1 && 	Domains Users and Gro Shares and Ro Policies Events		•	£ #	Account Lockou Audit	gnment			

information: Privilege, Account Name

🛓 Policies - User Rights Assign			x
💽 Refresh 👻 📑 Export 🛛 🍸	Fi ter 🛛 💼 Customize 🖉 💽 Scan Profiles (Comp	uters) 👻 🖬 🖬 👘 Find	2
Enterprise - POLICIE	R Password 🔬 Account Lockout 📑	Audit 😣 User Rights Assignment 🔒 Security Options 🚇 IP Security	
⊞ E . RD83	Generated on: 29 Dec, 2014, 06:18:20 PM	Status: Success Filter: Not Applied	
RESEARCHLAB	Privilege	Account Name	•
UOYAGER	Replace a process level token	NT AUTHORITY WETWORK SERVICE	
B RD40		NT AUTHORITY'LOCAL SERVICE	=
Servers	Generate security audits	NT AUTHORITY/NETWORK SERVICE	
RD41		NT AUTHORITY/LOCAL SERVICE	
	Back up files and directories	BUILTIN\Backup Operators	
🗄 📇 Workstations		BUILTIN\Server Operators	
		BUILTIN\Administrators	
	Log on as a batch job	BUILTIN/Performance Log Users	
		BUILTIN\Backup Operators	
		BUILTIN\Administrators	
	Bypass traverse checking	Window Manager \Window Manager Group	
		BUILTINIPre-Windows 2000 Compatible Access	
		BUILTIN\Administrators	
		NT AUTHORITY WETWORK SERVICE	
		NT AUTHORITY/LOCAL SERVICE	_
		NT AUTHORITY\Authenticated Users	_
		Everyone	_
	Create a pagefile	BUILTIN\Administrators	_
4 Add Domains	Debug programs	BUILTIN\Administrators	-

	Stan	dard Reports							
	÷.	Domains	•]					
	82	Users and Groups	•						
	3	Shares and Resources	•						
	4	Policies	•	٩	Password				
	8	Events	•	£	Account Lockout				
	-	Services	•		Audit				
'				82	User Rights Assignment				
					Security Options				
lick				2	IP Security	to	view	the	following

information: Policy Name, Value

Click

🛓 Policies - Security Options (RD40)	
🙆 Refresh 👻 🞰 Export 🛛 🍸	Fi ter 🛛 🛅 Customize 🗧 📧 Scan Profiles (Computers) 👻 🖙 E-mail	Find
Enterprise - POLICIE	🧌 Password 🔒 Account Lockout 📓 Audit 🧶 User Rights Assignment 🔒 Security Optio	ins 👰 IP Security
🗈 🖳 RD83	Generated on: 29 Dec, 2014, 06:41:37 PM Status: Success Filter: Not Applied	
RESEARCHLAB	Policy Name	Value
UOYAGER	Recovery console: Allow automatic administrative logon	Disabled
B RD40	Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
- A Servers	Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
- 🖳 RD41	Devices: Allowed to format and eject removable media	Not Defined
	Devices: Restrictfloppy access to locally logged-onuser only	Not Defined
🗄 🚇 Workstations	Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
	Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
	Interactive logon: Prompt user to change password before expiration	5 days
	Interactive logon: Smart card removal behavior	No Action
	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries
	User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
	Interactive logon: Do not require CTRL+ALT+DELETE	Disabled
	Interactive logon: Do not display last user name	Disabled
	Interactive Logon: Display user information when the session is locked	Not Defined
	User Account Control: Detect application installations and prompt for elevation	Enabled
	User Account Control: Run all administrators in Admin Approval Mode	Enabled
	User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
	User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
Add Domains	User Account Control: Virtualize file and registry write failures to per-user locations	Enabled 👻



to view the following

information: Policy Name, Description, Policy Assigned, and Last Modified

CHAPTER 2 – Standard Reports

here a security Options (RD40)			
🙆 Refresh 👻 📾 Export 🛛 🍸	Filter 🛛 🛅 Customize 🖾 Scar	n Profiles (Computers) 👻 🖃 E-mail	Fin	d 🗾
Enterprise - POLIC	🗌 Password 🔬 Account	t Lockout 🛛 👸 Audit 🛛 🍇 User Rights Assignment	Security Options	P Security
⊞	Generated on: 29 Dec, 2014, 06:4	1:37 PM Status: Success Filter: Not A	pplied	
	Policy Name	Description	Policy Assigned	Last Modified
Domain Cont	Server (Request Security)	For all IP traffic, always request security using Kerberos trust. Alow unsecured communication with clients that do not respond to request.	No	8/2/2012 6:-6:12 PM
⊡ 🕒 Servers RD41 및 RD43	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
- 📑 RD73 - 📑 RD83 - 📑 RD84 - 📑 RD85				
Add Domains				

3.5 How to View Events Information?



Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category

Enterprise - EVENTS	Applicati	1	1.000						
- RD83 - BL RESEARCHLAB	Generated on:	29 Dec, 2014, 06:49	2:21 PM Status: Success	Filter: Not Appl	ied				
VOYAGER	Event Date	Event Time	Description	Source	Event Id	Computer Name	User Name	Event Type	Category
🖶 🥘 Domain Controller	12/24/2014	06:13:48 PM							
		06:13:48 PM	Windows detected your registry file i	Microsoft-Windo	1530	RD40.Voyager.l	N/A	Warning	None
E B RD41		08:22:30 PM	The winlogon notification subscriber	Widntfy	6003	RD40.Voyager.l	N/A	Information	None
		08:22:31 PM	The winlogon notification subscriber	Widntfy	6000	RD40.Voyager.l	N/A	Information	None
Workstations		08:26:12 PM	The Desktop Window Manager has e	Desktop Window	9009	RD40.Voyager.l	N/A	Information	None
B RD71		08:26:11 PM	Windows detected your registry file i	Microsoft-Windo	1530	RD40.Voyager.l	N/A	Warning	None
- RD72		10:10:38 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
		10:10:39 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
		10:10:39 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
		10:10:39 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
		10:10:39 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
		10:10:39 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
		10:10:40 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
		10:10:40 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
		10:10:40 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
		10:10:40 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
		10:10:40 PM	svchost (2788) The database engine	ESENT	326	RD40.Voyager.l	N/A	Information	General
4 III		10:10:40 PM	svchost (2788) The database engine	ESENT	327	RD40.Voyager.l	N/A	Information	General
👍 Add Domains	•			m				1	



Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category

Refresh • 🕞 Export 🛛 🐺 F	Applicati		can Profiles (Computers) 🔹 📑 E-mail unity 🔟 System 🛃 Saved Logs	1				Find	
B RD83		29 Dec, 2014, 0	· · · · · · · · · · · · · · · · · · ·	Filter: Not Applied					
RESEARCHLAB VOYAGER	Event Date	Event Time	Description	Source	Event Id	Computer Name	User Name	Event Type	Category
📄 进 Domain Controller	12/29/2014	01:48:29 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
⊜-🥞 Servers		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
🖶 RD41		01:48:36 PM	Special privileges assigned to new logon	Microsoft-Windows-Securi	4672	RD40.Voyager.local	N/A	SuccessAudit	(12548)
Workstations		01:48:36 PM	An account was successfully logged on	Microsoft-Windows-Securi	4624	RD40.Voyager.local	N/A	SuccessAudit	(12544)
RD71		01:48:36 PM	User / Device claims information.Subject	Microsoft-Windows-Securi	4626	RD40.Voyager.local	N/A	SuccessAudit	(12553)
		01:48:36 PM	An account was logged off.Subject:Sec	Microsoft-Windows-Securi	4634	RD40.Voyager.local	N/A	SuccessAudit	(12545)
		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
- 📇 RD83		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
📇 RD84		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:36 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:37 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:37 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:37 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:38 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:38 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
		01:48:38 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)
• III		01:48:38 PM	The Windows Filtering Platform has per	Microsoft-Windows-Securi	5156	RD40.Voyager.local	N/A	SuccessAudit	(12810)



to view the following information:

Event Date, Event Time, Description, Source Name, Event End, Computer Name, User Name, Event Type, and Category

Refresh 👻 📑 Export 🛛 🍸 F	ilter 🛛 💼 Cu	istomize 🛛 💽 S	can Profiles (Computers) 🔹 🔜 E-mail					Find	
Enterprise - EVENTS	📑 Applica	tion 🍳 Sec	urity 📕 System 🛃 Saved Logs						
RD83	Generated o	n: 29 Dec, 2014,	07:14:59 PM Status: Canceled	Filter: Not Applied					
RESEARCHLAB VOYAGER	Event Date	Event Time	Description	Source	Event Id	Computer Name	User Name	Event Type	Category
🖃 🚇 Domain Controller	2/15/2014	11:43:32 AM	File System Filter 'luafv' (6.2, 2012-07-2	Microsoft-Windows-FilterMa		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
- E Servers		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
Workstations		11:43:33 AM	The Remote Procedure Call (RPC) servic	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
B RD71		11:43:33 AM	The Background Tasks Infrastructure Se	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None
- B RD72		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
📇 RD84		11:43:35 AM	The COM+ Event System service entere	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 dient service is started	Microsoft-Windows-Dhcp-Cli	50036	RD40.Voyager.local	N/A	Information	(4)
		11:43:36 AM	DHCPv6 dient service is started	Microsoft-Windows-DHCPv6	51046	RD40.Voyager.local	N/A	Information	(4)
4 III		11:43:36 AM	The DNS Client service entered the runni	Service Control Manager	7036	RD40.Voyager.local	N/A	Information	None

	Stan	dard Reports				
	#1 && 	Domains Users and Groups Shares and Resources Policies	+ + +			
	8	Events	•	I	Application	
	<i>#</i> *	Services	•	٩	Security	
					System	
Click					Saved Logs	to view the following information:

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

3.6 How to View Service Information?



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

efresh • 📑 Export 🛛 🍸 Fi	Iter 🔂 Customize 💽 Scan Profiles (Computer)		nail		Find	
	Generated on: 29 Dec, 2014, 06:57:23 PM	Status: Succe	ss Filter: Not	Applied		
E RESEARCHLAB	Display Name	StartUp	Service Type	Account	 Current State 	
WOYAGER Domain Controllers	Cryptographic Services	Auto	Share Process	NT Authority WetworkService	Running	
B RD40	DN5 Client	Auto	Share Process	NT AUTHORITY WetworkService	Running	
Servers	KDC Proxy Server service (KPS)	Manual	Share Process	NT AUTHORITY WetworkService	Stopped	
	KtmRm for Distributed Transaction Coordinator	Manual	Share Process	NT AUTHORITY WetworkService	Stopped	
- RD43	Workstation	Auto	Share Process	NT AUTHORITY WetworkService	Running	
- 🖳 Workstations	Distributed Transaction Coordinator	Auto	Own Process	NT AUTHORITY WetworkService	Running	
	Network Access Protection Agent	Manual	Share Process	NT AUTHORITY WetworkService	Stopped	
	Network Location Awareness	Auto	Share Process	NT AUTHORITY WetworkService	Running	
- 🛃 RD73	IPsec Policy Agent	Manual	Share Process	NT Authority WetworkService	Running	
	RPC Endpoint Mapper	Auto	Share Process	NT AUTHORITY WetworkService	Running	
	Remote Procedure Call (RPC) Locator	Manual	Own Process	NT AUTHORITY WetworkService	Stopped	
	Remote Procedure Call (RPC)	Auto	Share Process	NT AUTHORITY WetworkService	Running	
	Software Protection	Auto	Own Process	NT AUTHORITY WetworkService	Stopped	
	Telephony	Manual	Own Process	NT AUTHORITY WetworkService	Stopped	
	Remote Desktop Services	Manual	Share Process	NT Authority WetworkService	Running	
	Windows Event Collector	Manual	Share Process	NT AUTHORITY WetworkService	Stopped	
	Windows Remote Management (WS-Management)	Auto	Share Process	NT AUTHORITY WetworkService	Running	
4 III	Application Layer Gateway Service	Manual	Own Process	NT AUTHORITY\LocalService	Stopped	
4 Add Domains	Application Identity	Manual	Share Process	NT Authority\LocalService	Stopped	



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

CHAPTER 2 – Standard Reports

efresh 🔹 📑 Export 🛛 🐺 Fi				🛶 E-mail		Find	
Enterprise - SERVICES	🚰 General 🚺	🗠 Control 🌆	Dependency				
. 👰 RD83	Generated on: 29 D	ec, 2014, 06:57:23	PM Statu	is: Success	Filter: Not Applied		
RESEARCHLAB	Display Name	Service Name	Service Type	Error Control	Group	Path	
UOYAGER	1394 OHCI Complia	1394ohci	Kernel Driver	Normal		C:\Windows\system32\drivers\1394ohci.sys	
Bonan Controllers	3ware	3ware	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\3ware.sys	
Servers	Microsoft ACPI Driv	ACPI	Kernel Driver	Critical	Core	C:\Windows\system32\drivers\ACPI.sys	
RD41	Microsoft ACPIEx D	acpiex	Kernel Driver	Critical	Boot Bus Extender	C:\Windows\system32\Drivers\acpiex.sys	
	ACPIProcessorAge	acpipagr	Kernel Driver	Normal		C:\Windows\system32\drivers\acpipagr.sys	
🗄 📳 Workstations	ACPI Power Meter I	AcpiPmi	Kernel Driver	Normal		C:\Windows\system32\drivers\acpipmi.sys	
	ACPI Wake Alarm D	acpitime	Kernel Driver	Normal	Extended Base	C:\Windows\system32\drivers\acpitime.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 Filter	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 Driv	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	
	amdxata	amdxata	Kernel Driver	Normal	SCSI miniport	C:\Windows\system32\drivers\amdxata.sys	
	AppID Driver	AppID	Kernel Driver	Normal		C:\Windows\system32\drivers\appid.sys	



Display Name, Dependencies

Refresh 👻 📑 Export 🛛 🍸 Fi	lter 🛛 🛅 Customize 🖉 💽 Scan Pro	ofiles (Computers) 👻 🖙 E-mail	Find	2
Billion - SERVICES	😁 General 🔖 Control 🔮	Dependency		
	Generated on: 29 Dec, 2014, 06:57:2	23 PM Status: Success Filter: Not Applied		
RESEARCHLAB	Display Name	Dependencies		
UOYAGER	AppID Driver	FltMgr		
B RD40		discache		
Servers	Cbafilt	FitMgr		
-B RD41	Cluster Client Failover Filter	FitMgr		
	CSV Mini-Filter Driver	FitMgr		
- 🔁 Workstations	CSV NameSpace Filter Driver	FitMgr		
	Datascm	FitMgr		
	DFS Namespace Client Driver	Mup		
	DFS Replication ReadOnly Driver	FitMgr		
RD83 RD84	Windows All-User Install Agent	RpcSs		
	Application Identity	RpcSs		
		AppID		
		CryptSvc		
	Application Information	RpcSs		
		ProfSvc		
	Windows Audio	AudioEndpointBuilder		
		RpcSs		
4		MMCSS		
👍 Add Domains	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.



toolbar.

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

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.



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.

Built-in Reports - List of permissions for specific users and groups on folders Step 1 of 3 : Select Report Select a report from the available Built-in Reports.		
Permissions Image: Second system Image:		Description This report lists the folder permissions assigned to a specific user/group account.
	Back	Next Close

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.

Built-in Reports - List of permissions for speci	fic users and groups on folders		×
Step 2 of 3 : Select User/Group Account Select user and/or group accounts for which y		es/folders.	
Enter account name :		🛟 A <u>d</u> d to list 🕕 🕕	
Accounts from domain\server:	Browse and Select]	
Accounts from Scan Profiles (Users/Groups):	Frequent Scans 🗸] 🕕	
Selected Accounts:			
Account Name	Account Type		Re <u>m</u> ove
Adventure\adminuser			Reset
Adventure\Alan			
Adventure\Alex			
Adventure\Michael			
Builtin\Administrators			
	ſ		
	l	<u>B</u> ack <u>N</u> ext	Close

- 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).

Select Accounts	— ×
View and Select Accounts (Users/Groups) available from computers displayed below.	
□ Scan Profiles (Computers)	
Domains	=
🖶 📲 DISCOVERY	
🗄 👜 Domain Controllers	
E Servers/Workstations	
🖨 🚇 RD54	
RD54\Administrator	
RD54\adminuser	
RD54\Guest	-
Find: Guest OK Clear	ancel

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.

Built-in Reports	Select Shares	×		23
Step 3 of 3 :S				_
Enter the full p folder paths fr			ist of UNC ult	
properties for				1212
	Scan Profiles (Computers)	<u>^</u>		
Share/Folder U			Add	
	🚊 Domains			
Scan Profile (=		
	🛓 🚇 Domain Controllers			
Folder Path			evel 📩	Add From
\\RD49\Addre				
\\RD49\ADMI				Import
\\RD49\C\$	\\RD49\ADMIN\$		E	Remove
\\RD49\D\$				
\\RD49\E\$				
\\RD49\Excha				
\\RD49\F\$				
\\RD49\H\$			+	
•		-	- •	
📝 <u>D</u> o not displ			older Options	ו
	ОК	Cancel	rolder Options	J
		<u>B</u> ack	Einish	Close
Built-in Reports	- List of permissions for specific users and groups on folders			×
Step 3 of 3 :9 Enter the full p folder paths fo	 List of permissions for specific users and groups on folders Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. 	t to import a dify the defa	a list of UNC ault	•••
Step 3 of 3 :9 Enter the full p folder paths fo	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo	t to import a dify the def	h list of UNC ault	
Step 3 of 3 :9 Enter the full p folder paths fo	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder.	t to import a dify the defa	a list of UNC ault	
Step 3 of 3 : 9 Enter the full j folder paths fri properties for	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder.	t to import a dify the def	ault	
Step 3 of 3 : 5 Enter the full j folder paths for properties for Share/Folder U	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder.	dify the def.	ault	Add From
Step 3 of 3 : 5 Enter the full (folder paths for properties for Share/Folder U Scan Profile (Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. JNC Path: (Shares): Sample Scans Include sub-folders	dify the def.	ault	Add From
Step 3 of 3 : S Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. JNC Path: (Shares): Sample Scans Include sub-folders rss True	Folder	Add	
Step 3 of 3 : S Enter the full folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\ADMII \\RD49\C\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. JNC Path: (Shares): Sample Scans Include sub-folders rss True	Folder	ault	Add From
Step 3 of 3 : S Enter the full folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\ADMII \\RD49\C\$ \\RD49\D\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans Include sub-folders ess True N\$ True True True True True True Sample Scans	Folder All All All All	Add	Add From Import
Step 3 of 3 : S Enter the hull folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addres \\RD49\Addres \\RD49\C\$ \\RD49\D\$ \\RD49\E\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans Include sub-folders ess True N\$ True True True	Folder All All All All All All	Add	Add From Import
Step 3 of 3 : S Enter the hull folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addres \\RD49\ADMII \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\Excha	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans ↓ ① Include sub-folders rss True N\$ True True True True angeOAB True	Folder All All All All All All All All All	Add	Add From Import
Step 3 of 3 : S Enter the full j folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\Addree \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans Include sub-folders rss True N\$ True angeOAB True	Folder All All All All All All All All All Al	eult	Add From Import
Step 3 of 3 : S Enter the hull j folder paths fi properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\H\$	select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to no scanning each folder. INC Path: (Shares): Sample Scans ✓ ① Include sub-folders ess True N\$ True True True True True True True True True	Folder All All All All All All All All All	Add	Add From Import
Step 3 of 3 : S Enter the full j folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\Addree \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans Include sub-folders rss True N\$ True angeOAB True	Folder All All All All All All All All All Al	eult	Add From Import
Step 3 of 3 : S Enter the hull folder paths fr properties for Scan Profile (Folder Path \\RD49\Addree \\RD49\Addree \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\H\$	select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to no scanning each folder. INC Path: (Shares): Sample Scans ✓ ① Include sub-folders ess True N\$ True True True True True True True True True	Folder All All All All All All All All All Al	eult	Add From Import
Step 3 of 3 : S Enter the hull j folder paths fi properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans Include sub-folders ess True N\$ True angeOAB True I''	Folder All All All All All All All All All Al	ault	Add From Import
Step 3 of 3 : S Enter the hull j folder paths fi properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans	Folder All All All All All All All All All Al	ault	Add From Import
Step 3 of 3 : S Enter the hull j folder paths fi properties for Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ I RD49\H\$	select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Impor rom a text file. Select a folder in the list below and Click Edit Folder Options to mo scanning each folder. INC Path: (Shares): Sample Scans	Folder All All All All All All All All All Al	ault	Add From Import

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

Folder Options	×
Folder Path: MRD45\ADMIN\$	
Include sub-folders	
$\boxed{1} \underline{I}$ raverse only $\boxed{1}$ $\boxed{1}$ level(s) of sub-folder in the share	
Apply this setting to all folders in list	cel

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:

🔉 Refresh Data 🛛 📴 Report Details	s Export 🛛 📑	E-mail							Find	2
Report Name :	List of permissi	ions for specific u	sers and groups on t	folders						
∋enerated on: 20 Jul,	2011 11:02:397	AM			Statu	s: Success				
User Name 🔺	Folder Path	Sub-Folders	Owner	SID	Account Type	Member of	Acces: Type	Inherited	Security	Apply To
ADVENTURE\Administ	\\RD49\Test s	Test share folder	BUILTIN\Administra	5-1-5-21-3221	User	CN=Organization Managemer CN=Group Policy Creator Ow CN=Domain Admins CN=Enterprise Admins CN=Schema Admins CN=Remote Desktop Users CN=Administrators		No	Full Control	This folder, subf
BUILTIN\Administrato	\\RD49\Excha	ExchangeOAB	BUILTIN \Administra	5-1-5-32-544	Group		Allow	No	Full Control	This folder, subf
		02b2e76b-66c8-4	BUILTIN Administra	5-1-5-32-544	Group		Allow	No	Full Control	This folder, subf
	\\RD49\Group	GroupMetrics	BUILTIN \Administra	5-1-5-32-544	Group		Allow	Yes	Full Control	This folder, subf
	\\RD49\NETLC	NETLOGON	BUILTIN \Administra	S-1-5-32-544	Group		Allow	No	Write Attributes	This folder only
									Take Ownership	This folder only
									Change Permissions	This folder only

How to view Built-in Permissions Reports?

List of Permissions for Folders



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.

Built-in Reports - List of permissions for folders		—
Step 1 of 2 : Select Report Select a report from the available Built-in Reports.		
Permissions 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		Description This report lists the permissions assigned to a specific folder.
	<u>B</u> ack	Next Close

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

Step 2: Select shared folders:

Select one or more servers to retrieve available shares

Built-in Reports - List	of permissions for folders				23
Step 2 of 2 : Selec	· · ·		×	ີ	
	View and select Shares and Folders available from	computers displayed b		UNC	4
Share/Folder UNC P	Scan Profiles (Computers)			Add	
Folder Path	🗄 📲 Sample Scans				Add From
	Domains				
			E		Import
			-		
	E				Remove
	\\RD46\ARKAD Screen Sl	boto			
		locs			
	\\RD46\sampletask				
				•	
Do not display fo	\\RD46\Share			ptions	
Include group me	····· 🛄 \\RD46\ExchangeUM			<u> </u>	
Include SID	\\RD46\Effective		T		
		ок	Cancel		
l l					Close
	f permissions for folders				— X—
Enter the full path of	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load th ext file. Select a folder in the list below and Click Ed ng each folder.			UNC	
Share/Folder UNC Pat	n:			Ad <u>d</u>	
Scan Profile (Shares): Sample Scans	• ()			
Folder Path		Include sub-folders	Folder level	*	Add From
\\RD49\Address		True	All		Import
\\RD49\ADMIN\$		True	All	-	Import
\\RD49\C\$		True	All	E	Remove
\\RD49\D\$		True	All		
\\RD49\E\$ \\RD49\ExchangeOA	B	True True	All All		
(\RD49\EXthangeOA \\RD49\F\$	0	True	All		
\\RD49\H\$		True	All	-	
•				F.	
🔽 Do not display fold	ers that have the same permissions as the parent f	older	Edit Folder	Ontions	
Include group men					
✓ Include <u>S</u> ID					
			Back Fin	nish	Close

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 **Impor**t 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**.

Folder Options
Folder Path: (\\RD45\ADMIN\$
Include sub-folders
$\boxed{ Iraverse only 1 } evel(s) of sub-folder in the share $
Apply this setting to all folders in list

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:

🧿 Refresh Data 💧	🗟 Export 🛛 📑 E	-mail			Find				
Report Details Report Name :	List of permissio	ns for folders							
Generated on: 20 Ju	I, 2011-05:14:53 PI	vi			Status: Canceled				
Folder Path	Sub-Folders	Owner	User Name	SID	Account Type	Access Type	Inherite	Security	Apply To
\\RD49\Address	Address	NT AUTHORITY	BUILTIN\Administrat	S-1-5-32-54	Group	Allow	Yes	Full Control	This folder, subfolder
			NT AUTHORITY\SYS	S-1-5-18	Well Known Sid	Allow	Yes	Full Control	This folder, subfolder
			NT AUTHORITY\Aut	S-1-5-11	Well Known Sid	Allow	No	Read	This folder, subfolder
\\RD49\ADMIN\$	ADMIN\$	NT SERVICE\Tri	BUILTIN\Users	S-1-5-32-54	Group	Allow	No	Read and Execu	This folder only
			NT SERVICE\Trusted	S-1-5-80-95	Well Known Sid	Allow	No	Full Control	Subfolders only
									This folder only
			NT AUTHORITY\SYS	S-1-5-18	Well Known Sid	Allow	No	Full Control	Subfolders and files o
			BUILTIN\Administrat	S-1-5-32-54	Group	Allow	No	Modify	This folder only
								Full Control	Subfolders and files (
			NT AUTHORITY\SYS	S-1-5-18	Well Known Sid	Allow	No	Modify	This folder only
•									

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.



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.

Built-in Reports - List of permissions for specific users and groups on files	—
Step 1 of 3 : Select Report Select a report from the available Built-in Reports.	
Permissions List of permissions for specific users and groups on folders List of permissions for specific users and groups on files List of permissions for files List of permissions for files	Description This report lists the file permissions assigned to a specific user/group account.
Back	Next Close

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.

CHAPTER 3 – Built-in Reports

Built-in Reports - List of permissions for specific users and groups on files	-
Step 2 of 3 : Select User/Group Account(s) Select user and/or group accounts for which you would like to view the permissions on files/folders.	
Enter account name :	
Accounts from domain\server: Browse and Select	
Accounts from Scan Profiles (Users/Groups): Frequent Scans	
Selected Accounts:	
Account Name Account Type	Remove
Adventure\adminuser	Reset
Adventure\Alan	
Adventure\Alex Adventure\Michael	
Builtin\Administrators	
Back Next	Close

- 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).

Select Accounts	X
View and Select Accounts (Users/Groups) available from computers displayed below.	
Scan Profiles (Computers)	*
Domains	≡
DISCOVERY	
🗄 🖙 🚇 Domain Controllers	
🛓 🖳 Servers/Workstations	
📥	
RD54\Administrator	
RD54\adminuser	
RD54\Guest	-
Find: Guest DK Clear	ancel

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.

Built-in Reports	Select Shares	×	1	23
Step 3 of 3 :S	View and select Shares and Folders available from computers displayed below	v		_
Enter the full p folder paths fr			ist of UNC Ult	<mark>الم</mark>
properties for				12222
	Care Brafflag (Carrantana)	*		
	Scan Profiles (Computers)	- Â		
Share/Folder U	<no configure="" found.="" manager.="" profile="" profiles="" scan="" using=""></no>		Add	
	Domains			
Scan Profile (🖶 🚇 ADVENTURE	=		
	🖨 📲 Domain Controllers			
Folder Path			evel	Add From
\\RD49\Addre				Import
\\RD49\ADMII	INRD49\ADMIN\$			
\\RD49\C\$				Remove
\\RD49\D\$				
\\RD49\E\$			-	
\\RD49\Excha				
\\RD49\F\$ \\RD49\H\$				
				~
•		-		
📝 Do not displ			older Options	;
	OK	Cancel		
			_	
		Back	Finish	Close
		<u>B</u> ack	Einish	Close
D		<u>B</u> ack	Einish	
	- List of permissions for specific users and groups on files	Back	<u>E</u> inish	Close
Step 3 of 3 ÷ 5	elect Shared Folder(s)			
Step 3 of 3 : S Enter the full p folder paths fr	elect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to i	port to import (a list of UNC	
Step 3 of 3 : S Enter the full p folder paths fr	elect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp	port to import (a list of UNC	
Step 3 of 3 : S Enter the full p folder paths fr	elect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to i	port to import (a list of UNC	
Step 3 of 3 : 5 Enter the full p folder paths fr properties for	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder.	port to import (a list of UNC ault	
Step 3 of 3 : S Enter the full p folder paths fr	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder.	port to import (a list of UNC	
Step 3 of 3 : 5 Enter the full p folder paths fr properties for Share/Folder U	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder.	port to import (a list of UNC ault	
Step 3 of 3 : 5 Enter the full p folder paths fr properties for	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder.	port to import (a list of UNC ault	
Step 3 of 3 : 5 Enter the full p folder paths fr properties for Share/Folder U	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder.	port to import a modify the def	a list of UNC ault	
Step 3 of 3 : 5 Enter the full ; folder paths fr properties for Share/Folder U Scan Profile (Gelect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp om a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder	port to import a modify the def	a list of UNC ault	Add From
Step 3 of 3 : 5 Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path	Gelect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp om a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder iss True	port to import a modify the def ers Folder	a list of UNC ault	
Step 3 of 3 : S Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre	Gelect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp om a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder iss True	port to import a modify the def ers Folder All	a list of UNC ault	Add From Import
Step 3 of 3 : S Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\ADMIr	Gelect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improm a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder inss True N\$ True	port to import a modify the def ers Folder All All	a list of UNC ault	Add From Import
Step 3 of 3 : 5 Enter the hull ; folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\ADMIr \\RD49\C\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improm a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder rss True N\$ True True True	ers Folder All All	a list of UNC ault	Add From Import
Step 3 of 3 : S Enter the hull p folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\Addre \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improm a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans Include sub-folder rss True N\$ True True True	ers Folder All All All All All All All	a list of UNC ault	Add From Import
Step 3 of 3 : 5 Enter the full r folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\C\$ \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$	iselect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improve a text file. Select a folder in the list below and Click Edit Folder Options to rescanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folder rue Instant Include sub-folde rue True	ers Folder All All All All All All All All All Al	a list of UNC ault	Add From Import
Step 3 of 3 : S Enter the hull p folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\Addre \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\Excha	iselect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improve the second scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans INC Path: (Shares): Sample Scans Include sub-folder Inscience Include sub-folder Inscience Inscience Include sub-folder Inscience Inscience Include sub-folder Inscience Inscince <td>ers Folder All All All All All All All</td> <td>a list of UNC ault</td> <td>Add From Import</td>	ers Folder All All All All All All All	a list of UNC ault	Add From Import
Step 3 of 3 : 5 Enter the full r folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\C\$ \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$	iselect Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improve a text file. Select a folder in the list below and Click Edit Folder Options to rescanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folder rue Instant Include sub-folde rue True	ers Folder All All All All All All All All All Al	a list of UNC ault	Add From Import
Step 3 of 3 : 5 Enter the hull properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\Addre \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improm a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folder rrue Inss Include sub-folder rrue Include sub-folder inss True	ers Folder All All All All All All All All All Al	a list of UNC ault Add	Add From Import Remove
Step 3 of 3 : S Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\D\$ \\RD49\C\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Improve a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans INC Path: Include sub-folder (Shares): Sample Scans (Shares): Sample Scans Include sub-folder Include sub-folder Inside sub-folder True Inside sub-f	ers Folder All All All All All All All All All Al	a list of UNC ault	Add From Import Remove
Step 3 of 3 : S Enter the hull (folder paths fr properties for Scan Profile (Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ < Qo not displ	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folde rss True N\$ True Tr	ers Folder All All All All All All All All All Al	a list of UNC ault Add	Add From Import Remove
Step 3 of 3 : S Enter the full (folder paths fr properties for Share/Folder U Scan Profile (Folder Path \\RD49\Addre \\RD49\D\$ \\RD49\C\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folde rss True N\$ True Tr	ers Folder All All All All All All All All All Al	a list of UNC ault Add	Add From Import Remove
Step 3 of 3 : S Enter the hull (folder paths fr properties for Scan Profile (Scan Profile (Folder Path \\RD49\Addree \\RD49\D\$ \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ < Qo not displ	Select Shared Folder(s) path of a Share or Shared Folder. Click Add From to load the list of shares, Imp rom a text file. Select a folder in the list below and Click Edit Folder Options to a scanning each folder. INC Path: (Shares): Sample Scans (Shares): Sample Scans Include sub-folde rss True N\$ True Tr	ers Folder All All All All All All All All All Al	a list of UNC ault Add	Add From Import Remove

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**.

Folder Options	×
Folder Path: \\\RD45\ADMIN\$	
Include sub-folders	
$\boxed{1}$ Inverse only $\boxed{1}$ $\boxed{1}$ level(s) of sub-folder in the share	
Apply this setting to all folders in list	cel

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:

Refresh Data Report Details	Export 🔤	E-mail					_			F	ind
Report Name	: List of permission	ons for spe	cific users	s and groups or	n files						
enerated on: 21	Jul, 2011-03:58:04 P	м				Statu	s: Canceled				
	Folder/File Path	Folder/File Name	Folder/F Type	Owner	SID	Account Type	Access Type	Membe of	Inherite	Security	Apply To
3UILTIN\Adminis	\\RD49\Address	Address	Folder	NT AUTHORIT	5-1-5-32	Alias	Allow		Yes	Full Control	This folder, subfolders an
ADVENTURE\adn	\\RD49\NTFS Securi	NTFS Secu	Folder	ADVENTURE\a	S-1-5-21	User	Allow		No	Full Control	This folder, subfolders an
UILTIN\Adminis	\\RD49\NTFS Securi	NTFS Secu	Folder	ADVENTURE\a	S-1-5-32	Alias	Allow		No	Full Control	This folder, subfolders an
	\\RD49\SYSVOL	SYSVOL	Folder	BUILTIN\Admir	S-1-5-32	Alias	Allow		No	Create Folders / Ap	This folder only
										Write Attributes	This folder only
										Write Extended Attr	This folder only
										Read Permissions	This folder only
										Change Permissions	This folder only
										Read Extended Attr	This folder only
										Read Attributes	This folder only
										Take Ownership	This folder only
										Create Files / Write	This folder 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.

	Buil	t-in Reports	
	A	Permissions	
	3	Shares and Resources	
	82	Users and Groups	
on	ŧ.	Domains	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

Click

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

Built-in Reports - List of permissions for files Step 1 of 2 : Select Report Select a report from the available Built-in Reports.	— •
Select a report from the available Built-in Reports.	Description This report lists the permissions assigned to files under a specific folder.
B	ack <u>N</u> ext Close

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

Step 2: Select Shared Folders:

Select one or more servers to retrieve available shares

Built-in Reports - List o	of permissions for files				23
	converted for Ebarod Foldore list				_
Enter the full path of folder paths from a t	Select Shares			JNC 🔁	<mark>الم</mark>
properties for scann	View and select Shares and Folders available from co	mputers display	/ed below.		
Share/Folder UNC Pa	Scan Profiles (Computers)				
	Search Strain	Deofilos Manas			
Scan Profile (Share		i Pronies manag	jer.>		
	Domains				
Folder Path					Add From
\\RD49\Address	📄 📲 Domain Controllers				Import
\\RD49\ADMIN\$	Ė E . RD49				Import
\\RD49\C\$	\\RD49\Address				Remove
\\RD49\D\$	\\RD49\ADMIN\$				
\\RD49\E\$					J
\\RD49\ExchangeO4					
\\RD49\F\$					
\\RD49\H\$				-	-
•	₩ \\RD49\ExchangeOAB			4	
🔽 Do not display file				_ Options	1
Include group mer				- options	J
			к <u>с</u> .		
☑ Include <u>S</u> ID		0	K Car	ncel	
			Back	Finish	Close
			<u>Fack</u>		
Built-in Reports - List o	of permissions for files				×
•	•				×
Step 2 of 2 : Select Enter the full path of	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the				
Step 2 of 2 : Select Enter the full path of folder paths from a t	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I				×
Step 2 of 2 : Select Enter the full path of	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I				
Step 2 of 2 : Select Enter the full path of folder paths from a t	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I				
Step 2 of 2 : Select Enter the full path of folder paths from a t	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.				
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pat	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.			fault	
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.			fault	
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pat	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.		co'modify the de	fault	Add From
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pal Scan Profile (Shares Folder Path	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.	 Include sub-fo 	lders Folde	Ad <u>d</u>	
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pal Scan Profile (Shares Folder Path \\RD49\Address	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.	 Include sub-fo 	lders Folde	Ad <u>d</u>	
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pal Scan Profile (Shares Folder Path \\RD49\Address \\RD49\ADMIN\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.	 Include sub-fo 	lders Folde	Ad <u>d</u>	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Share/Folder UNC Pall Scan Profile (Shares Folder Path \\RD49\Address \\RD49\ADMIN\$ \\RD49\C\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.	Folder Option's to Tinclude sub-for True True	lders Folde All	er level	Add From
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Pal Scan Profile (Shares Folder Path \\RD49\Address \\RD49\ADMIN\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder.	Folder Option's to True True True True True True	Iders Folde All All	er level	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Share/Folder UNC Pall Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder. th: Sample Scans	Folder Option's t Tinclude sub-fo True True True True True True	Iders Folde All All All All All	er level	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Share/Folder UNC Pall Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$ \\RD49\E\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder. th: Sample Scans	Folder Option's t Tinclude sub-fo True True True True True True True	Iders Folde All All All All All All	er level	Add From Import
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Path Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\E\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder. th: Sample Scans	Folder Option's t True True True True True True True True True True True True True	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Path Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I ng each folder. th: Sample Scans	Include sub-fo True True True True True True True True	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$	B	Include sub-fo True T	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Path Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I geach folder. (h:): Sample Scans B III III III III III III III III III	Include sub-fo True T	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ < Do not display file: ✓ Include group mer	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I geach folder. (h:): Sample Scans B III III III III III III III III III	Include sub-fo True T	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the full path of folder paths from a t properties for scanni Share/Folder UNC Path Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\D\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ <	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I geach folder. Sample Scans B III III III III III III III III III	Include sub-fo True T	Iders Folde	er level	Add From Import
Step 2 of 2 : Select Enter the hull path of folder paths from a t properties for scanni Scan Profile (Shares Folder Path \\RD49\Address \\RD49\Address \\RD49\C\$ \\RD49\C\$ \\RD49\E\$ \\RD49\E\$ \\RD49\F\$ \\RD49\F\$ \\RD49\H\$ < Do not display file: ✓ Include group mer	server(s) for Shared Folders-list a Share or Shared Folder. Click Add From to load the ext file. Select a folder in the list below and Click Edit I geach folder. Sample Scans B III III III III III III III III III	Include sub-fo True T	Iders Folde	er level	Add From Import
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.**

Folder Options
Folder Path: \\RD45\ADMIN\$
Include sub-folders $\boxed{\ }$ Include sub-folders $\boxed{\ }$ Iraverse only $\boxed{1}$ level(s) of sub-folder in the share
Apply this setting to all folders in list <u>QK</u> <u>Cancel</u>

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:

Refresh Data Report Details	📑 Export 🛛 📑 E-i	mail					Find	Đ
Report Name	List of permissions	for files						
Folder <i>l</i> File Path	Folder/File Name	Folder/ Type	Owner	User Name	Security	Inherited	Apply To	
\\RD45\test1	test1	Folder	BUILTIN\Administrat	Unknown Account	Allow - Special Acces	No	This folder, subfolders and files	
				BUILTIN\Administra	Allow - Full Control	No	This folder only	
					Allow - Special Acces	No	This folder, subfolders and files	
				PATHFINDER\admin	Allow - Full Control	No	This folder, subfolders and files	
				PATHFINDER\croud	Allow - Special Acces	No	This folder, subfolders and files	
				Everyone	Allow - Special Acces	No	This folder, subfolders and files	
			This folder, subfolders and files					
			PATHFINDER\Twst	Allow - Special Acces	No	This folder, subfolders and files		
					Allow - Special Acces	No	This folder and subfolders	
	Application Data Fol	Application Data Fol Folder BUI	BUILTIN\Administrat L	Unknown Account	Allow - Special Acces	Yes	This folder, subfolders and files	
				BUILTIN\Administral	Allow - Special Acces	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.

Built-in Reports	x
Step 1 of 3 : Select Report This window shows the list of Built-in reports available for the selected Built-in report category. Select any Report to proceed.	
Shares and Resources List of Shares List of Shares with permissions	
<u>B</u> ack <u>N</u> ext	Close

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.

Built-in Reports - List of Shares with permissions	×
Step 2 of 3 : Select Domain(s)/Server(s) You can either generate the report across domains by selecting All Domains or for a specific domain/server by selecting the Select Domain/Server option. This report can also be generated specifically for a single server by selecting the Server option.	
 All Domains Select Domain/Server Add Domains 	
RD83 RESEARCHLAB RO40 RD41 RD43 RD43	
Select Scan Profile:	

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.

Built-in Reports - List of Shares with permissions								
Step 3 of 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.								
Share Type:								
Folder Share								
Admin Share								
<u>B</u> ack <u>E</u> inish	Iļose							

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:

esh Data 🛛 🞰 Exp Details	port 🖓 E-maii					Find
	of Shares with permissio	ons				
ted on: 30 Dec, 201	I4, 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: Vatest setup	BUILTIN\Administrators	Allow - Full Control	Unlimited	Latest Setup Share
		D: Vatest 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 \adminuser 3	Allow - Full Control	Unlimited	
	NTFS Test Folder	C: WTFS 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	

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.

Bui	lt-in Reports
0	Permissions
3	Shares and Resources
88	Users and Groups
商	Domains

Click on La 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.

button under Built-in Reports in button in the

Built-in Reports - List of User accounts	— ×
Step 1 of 3 : Select Report This report lists all Built-in and Custom User accounts in a machine.	
 Users and Groups List of Users and Groups List of User accounts List of Local and Global groups List of disabled user accounts List of locked-out user accounts List of locked-out user accounts (Password never expires etc.) Members of Local Administrators group Log on rights assigned for all accounts (Log on locally etc.) Privileges assigned for all accounts Group membership with nested groups 	
Back Next	Close

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.

Built-in Reports - List of User accounts	—						
Step 2 of 3 : Select Domain(s)/Server(s)							
You can either generate the report across domains by selecting All Domains or for a specific domain/server by selecting the Select Domain/Server option. This report can also be generated specifically for a single server by selecting the Server option.							
All Domains							
● Select Domain/Server							
ESEARCHLAB							
Select Scan Profile:							
<u>B</u> ack <u>N</u> ext	Close						

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.

Built-in Reports - List of User accounts	-X
Step 3 of 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.	
User Type:	
<u>B</u> ack <u>Finish</u>	Close

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:

🖳 Bi	🖳 Built-in Reports - List of User accounts 📃 💷 💽							
Repo	efresh Data 🚔 Export ort Details eport Name : List of User				Find			
	Domain/Server	User Name	Description			A		
►	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			Ŧ		

List of Reports:

Report Name	Description
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.



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.

Built-in Reports - List of trusted and trusting domains	- ×
Step 1 of 3 : Select Report This window shows the list of Built-in reports available for the selected Built-in report category. Select any Report to proceed.	
Domains List of trusted and trusting domains List of machines with their OS and service pack List of Windows Servers List of Domain Controllers List of Application Servers (IIS, Exchange Server, SQL Server etc.) List of machines that run TCPIP services (FTP, telnet etc.) List of machines that have auditing enabled (or disabled)	
Back Next	Close

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.

Built-in Reports - List of trusted and trusting domains	x							
Step 2 of 3 : Select Domain(s)/Server(s) You can either generate the report across domains by selecting All Domains or for a specific domain by	⊡ a							
selecting the Select Domain option.								
All Domains								
Select Domain Add Domains								
TREELAB								
Select Scan Profile:Select a Profile								
Back Next	Close							

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.

Built-in Reports - List of trusted and trusting domains	
Step 3 of 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.	
Trusted/Trusting Domains:	
Trusted	
Trusting	
<u>B</u> ack <u>Finish</u>	Close

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:

Repo	ilt-in Reports - List fresh Data 🙀 Ex rt Details port Name : 🛛 List	Find			
	Domain Name	Domain Name(T)	Trusted	Trusting	
	RESEARCHLAB	VSSLAB	Yes	Yes	
		CHILD	Yes	Yes	
		TREELAB	Yes	Yes	
	VSSLAB	RESEARCHLAB	Yes	Yes	
		VOYAGER	Yes	Yes	

List of Reports:

Report Name	Description
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)

Chapter

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.mspx#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 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 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.

Refresh 👻 📷 Export 🛛 🍸 Filte	r 🔲 Customize	📑 E-mail				Find		2
te: All System Info reports require WI	MI to be installed and	enabled. Click here fo	or more information	<u>n</u>				
- G Enterprise - NETWORKC(IP Configuratio	on 🔒 Login Profile	es 🏾 🖼 Network	Adapters 3	Network Protocols			
RESEARCHLAB	Generated on: 20 M	ar, 2013, 03:21:21 PM	1 Stat	us: Success	Filter: Not Ap	plied		
E TREELAB	Host Name	Network Adapter Name	IP Address	Subnet Mask	DHCP Enabled	Default Gateway	DHCP Server	
	RD30	[00000012] Microso	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		10.10.10.83	255.0.0.0	Yes	10.10.10.1	10.10.10.1	

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

Network Configuration - Login F							x
🛿 Refresh 👻 🚌 Export 🛛 🍸 Filte						Find	2
ote: All System Info reports require Wi	MI to be installed and e	enabled. Click here for more int	formation				
	上 IP Configuratio	n 🛕 Login Profiles 🔳	Network Adapters	ra— Netv	vork Protocols		
RESEARCHLAB	Generated on: 20 M	ar, 2013, 03:26:05 PM	Status: Success	s	Filter: Not Applied		
E TREELAB	Host Name	Account Name	Last Logon to Con	nputer			
	RD30	NT AUTHORITY\SYSTEM					
		NT AUTHORITY/LOCAL SEP	=				
		NT AUTHORITY/NETWORK	:				
		TREELAB\adminuser2	3/20/2013 3:24:47	PM			
		RESEARCHLAB\adminuser1	3/20/2013 11:59:54	4 AM			
		RESEARCHLAB\adminuser2	3/20/2013 3:24:47	PM			
		RESEARCHLAB\adminuser3	3/20/2013 3:13:49	PM			
		RESEARCHLAB\Administrat	3/19/2013 4:12:35	PM			1
4 III		VSSLAB\adminuser1	3/20/2013 11:59:54	4 AM			
👍 Add Domains		VSSLAB\adminuser2	3/20/2013 3:24:47	PM			

Click		Network Adapters	tab	to	view	the	following	information:	Host	Name,	Adapter
Name	e, Ad	lapter Type, .	Adap	ter	· ID, I	Dese	cription, a	and Physical	Addr	ess.	

🕯 Refresh 👻 😹 Export 🛛 🍸 Filte	er 🔲 Customize	🖃 E-mail				Find	
ote: All System Info reports require W			r more information				
- 🚱 Enterprise - NETWORKCO	IP Configuratio	n 🔒 Login Profile	s 🔳 Network Ad	lapters 😙 Netwo	ork Protocols		
RESEARCHLAB	Generated on: 20 M	ar, 2013, 03:28:36 PM	I Status:	Success	Filter: Not Applied		
E TREELAB	Host Name 🔍	Adapter Name	Adapter Type	Adapter ID	Description	Physical Address	
	RD30	WAN Miniport (SST		{4AE6B55C-6DD6-4	WAN Miniport (SST		
		WAN Miniport (IKE		{CB94342D-DEED-	WAN Miniport (IKE		
		WAN Miniport (L2T		{66973E50-CF44-4	WAN Miniport (L2T		
		WAN Miniport (PPT		{F93EB786-8968-4	WAN Miniport (PPT		
		WAN Miniport (PPP		{6A16EDEB-24DF-	WAN Miniport (PPF		
		WAN Miniport (IPv		{F4373218-ED19-4	WAN Miniport (IPv		
		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	
4		Microsoft ISATAP A	Tunnel	{36393700-3DDC-4	MicrosoftISATAPA		
Add Domains		WAN Miniport (IP)			WAN Miniport (IP)		

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

Setwork Configuration - Network Protocols (RESEARCHLAB)								
🔉 Refresh 👻 📾 Export 🍸 Filter 🛅 Customize 🚭 E-mail 🛛 🛛 🗛 Find								
Note: All System Info reports require WI	MI to be installed and	enabled. Click here for more inforr	nation					
Enterprise - NETWORKC	IP Configuratio	n 🔒 Login Profiles 🏾 🗰 Net	work Adapters 🤤 Network Pro	otocols				
	Generated on: 20 M	ar, 2013, 03:30:46 PM	Status: Success Filter	: Not Applied				
E TREELAB	Host Name	Protocol Name	Description	Installed Date	A			
	RD30	MSAFD Tcpip [TCP/IP]	@%SystemRoot%\system32\tcp	3/30/2012 10:29:18 PM				
		MSAFD Tcpip [UDP/IP]	@%SystemRoot%\system32\tcp	3/30/2012 10:29:18 PM				
		MSAFD Tcpip [TCP/IPv6]	@%SystemRoot%\system32\tcp	3/30/2012 10:29:18 PM	=			
		MSAFD Tcpip [UDP/IPv6]	@%SystemRoot%\system32\tcp	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					
• III •	RD11	MSAFD Tcpip [TCP/IP]	@%SystemRoot%\system32\tcp	9/7/2011 10:47:35 AM				
Add Domains		MSAFD Tcpip [UDP/IP]	@%SystemRoot%\system32\tcr	9/7/2011 10:47:35 AM	-			

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).

📮 Operating System & Hot Fixes - Operating System Configuration (RESEARCHLAB)								
💁 Refresh 👻 📾 Export 🍸 Filter 💼 Customize 🖏 E-mail 🛛 🛛 😰								
Note: All System Info reports require WI	Ito be installed	and enabled. Click here for more information						
Enterprise - OPERATING	🛃 Operating	g System Configuration 🙀 Hot Fixes						
RESEARCHLAB	Generated on:	20 Mar, 2013, 03:49:30 PM Status: S	uccess	Filter: Not	Applied			
E TREELAB	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		
👍 Add Domains	•					Þ		

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

🛐 Refresh 👻 📑 Export 🛛 🍸 Filt	ter 🛛 💼 Customiz	ze 🛛 📑 E-mail			Find	<u>,</u>			
ote: All System Info reports require \	VMI to be installed a	ind enabled. Click her	re for more information	<u></u>					
Enterprise - OPERATING	🔒 Operating	System Configuration	n 😥 Hot Fixes						
RESEARCHLAB	Generated on: 2	Generated on: 20 Mar, 2013, 03:54:01 PM Status: Success Filter: Not Applied							
ITREELAB	Host Name	Hot Fix	Description	Installed By	Installed Date	Fix Comments			
	RD30	KB958488	Update	RESEARCHLAB\ad	lminuser1				
		KB976902	Update						
		KB976932	Service Pack						
	RD11	KB976902	Update						
		KB976932	Service Pack						

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.

r Customize Mito be installed and e	enabled. Click here for more inform	nation			Find		
🍓 Printers		nation					
	ar 2013 03:55:34 PM						
Generated on: 20 M	lar 2013 03:55:34 PM						
		Status: Succes	SS	Filter: Not A	Filter: Not Applied		
Host Name	Printer Name	Description	Location	Share Name	Port Name	Driver Nar	
RD30	Microsoft XPS Document Writer				XPSPort:	Microsoft.	
RD11	Microsoft XPS Document Writer				XPSPort:	Microsoft.	
		RD11 Microsoft XPS Document Writer XPSPort:					

5.5 How to View Hardware Configuration Reports?



Click on 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.

🛃 Hardware Info - Summary (RESE/	ARCHLAB)									
👩 Refresh 👻 📾 Export 🍸 Filter	r 🛛 💼 Custon	nize 🛛 📑 E-mai	I				Find	2		
Note: All System Info reports require WMI to be installed and enabled. Click here for more information										
Enterprise - HARDWARE	Summar 🚰	y 📣 BIOS Inf	o 🔲 Processo	rs 📖 Physic	al Memory 🧼	Disk Drives				
RESEARCHLAB	Generated on	: 20 Mar, 2013, 04	1:00:14 PM	Status: Suc	cess	Filter: Not Applied	i			
ITREELAB	Host Name	Number of Processor(s)	System Model	System Manufacturer	System Type	Total Physical Memory (MB)	BIOS Version	Boot Device		
	RD30	1	Veriton Series	Acer	x64-based PC	16204.98	ACRSYS - 1072009	\Device\Harddi		
	RD11	1	Veriton Series	Acer	x64-based PC	7991.12	ACRSYS - 2011013	\Device\Harddi		
< ► Add Domains	4							,		

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

🚽 Hardware Info - BIOS Info (RESEA	ARCHLAB)				- • ×
🖸 🖸 Refresh 👻 📷 Export 🍸 Filte	r 📑 Customize	📑 E-mail		Find	1
Note: All System Info reports require WI	It to be installed and	enabled. Click here for more information			
Enterprise - HARDWARE	Summary 🗸	> BIOS Info 🔲 Processors 🎟 Physica	al Memory 🧼 Disk Drives		
RESEARCHLAB	Generated on: 20 M	lar, 2013, 04:04:15 PM Status: Succ	cess Filter: Not App	lied	
ITREELAB	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	
 ■ 					
Add Domains					

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

🚚 Hardware Info - Processors (RESE						
🖸 Refresh 👻 📑 Export 🍸 Filter	Customize	e 🔄 🖬 E-mail			Find	2
Note: All System Info reports require WI	It to be installed a	nd enabled. Click here for more info	ormation			
Enterprise - HARDWARE	Summary	SIOS Info Processors	Physical Men	nory 🧼 Disk Drives		
	Generated on: 2	0 Mar, 2013, 04:05:57 PM	Status: Success	Filter: Not Applied		
TREELAB	Host Name	Processor	Туре	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 5	Central Processor	Intel64 Family 6 Model 37 Stepp		1
< الله الله الله الله الله الله الله الل						

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

🐧 Refresh 👻 📾 Export 🛛 🍸 Filte	er 🛛 💼 Customize	📑 E-mail				Find			
lote: All System Info reports require W	MI to be installed and	enabled. Click here for n	nore information						
	Summary								
RESEARCHLAB	Generated on: 20 N	Generated on: 20 Mar, 2013, 04:08:32 PM Status: Success Filter: Not Applied							
TREELAB	Host Name	Memory Identifier	Туре	Capacity (MB)	Memory Bank				
	RD30	Physical Memory 0	Unknown	4096	BANK1				
		Physical Memory 1	Unknown	4096	BANK2				
		Physical Memory 2	Unknown	4096	BANK3				
		Physical Memory 3	Unknown	4096	BANK4				
	RD11	Physical Memory 0	Unknown	4096	BANK0				
		Physical Memory 1	Unknown	2048	BANK1				
		Physical Memory 3	Unknown	2048	BANK3				
4									
Add Domains									

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

, 🛃 Hardware Info - Disk Drives (RESI	EARCHLAB)					
👩 Refresh 👻 📑 Export 🛛 🍸 Filte	r 📑 Customize	📑 E-mail				Find 😥
Note: All System Info reports require WI	It to be installed and	enabled. Click here fo	or more information			
Enterprise - HARDWAREI	Summary	> BIOS Info 🔲 F	Processors 📖 Ph	ysical Memory 🤍	Disk Drives	
RESEARCHLAB	Generated on: 20 M	ar, 2013, 04:10:12 Pi	M Status:	Success	Filter: Not Applied	
TREELAB	Host Name	Drive	File System	Capacity (GB)	Space Used (GB)	Space Free (GB)
	RD30	C:	NTFS	118.01	38.17 (32.35%)	79.84 (67.65%)
		E:	NTFS	347.66	274.26 (78.89%)	73.4 (21.11%)
	RD11	C:	NTFS	278.46	239.24 (85.92%)	39.22 (14.08%)
۲ الله معالم المعالم ال معالم Add Domains						

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.

🛃 Display Configuration - Monitor	Info (RESEARCHLA	B)				
👩 Refresh 🔹 📾 Export 🛛 🍸 Filter	r 📑 Customize	📑 E-mail			Fir	nd 🗵
Note: All System Info reports require WI	It to be installed and	enabled. Click here for more	information			
Enterprise - DISPLAYCON	📑 Monitor Info	📑 Video Adapter Info				
	Generated on: 20 M	ar, 2013, 04:11:59 PM	Status: S			
TREELAB	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)
< □□ ►						

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

🧟 Refresh - 🛛 📾 Export 🛛 🍸 Filte	r Gustomize	E Famail				Find	
lote: All System Info reports require W		· ·	a information			TING	
iote. All System into reports require w	mi to be installed and	enabled. Click here for mon	e information	-			
Enterprise - DISPLAYCON	Monitor Info	📕 Video Adapter Info					
E RESEARCHLAB	Generated on: 20 M	/ar, 2013, 04:11:59 PM	Status	Success	Filter: N	lot Applied	,
E TREELAB	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
4 III +	J						
🕂 Add Domains	4						

5.7 How to View Internet Explorer Configuration Reports?



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.

🚽 Internet Explorer Configuration -	Summary (RESEAR	CHLAB)					×
🙆 Refresh 👻 🗟 Export 🕎 Filte	r 🛛 💼 Customize	📑 E-mail			Find		2
Note: All System Info reports require W	Ito be installed and	enabled. Click here fo	or more infor	mation			
Enterprise - INTERNET E	Summary						
RESEARCHLAB	Generated on: 20 M	ar, 2013, 04:16:17 PM	4	Status: Success	Filter: Not Applied		
TREELAB	Host Name	Version	Cipher Strength	Product ID	Build Number	Content Advisor	Loca
	RD30	8.0.7601.17514	256-bit	55041-628-5052896-84972	87601	Disabled	C:\P
	RD11	8.0.7601.17514	256-bit	55041-628-5052896-84710	87601	Disabled	C:\P
< Þ							
Add Domains	•						Þ

5.8 How to View Current Status Reports?



Click on **Environment Into** 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.

Current Status - Summary (RESE								
Refresh Image: Refresh Refresh Image: Refresh Refresh Image: Refresh Refresh Image: Refresh Image: Refresh Image: Refresh Image: Refresh Image: Refresh Refresh Image: Refresh			here for more inform	ation			Find	2
Enterprise - CURRENT S	🚰 Sum	imary						
RESEARCHLAB	Generated	d on: 20 Mar, 2013, 04:22	2:00 PM	Status: Success	Filt	er: Not Applie	d	
E TREELAB	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	2013 4:22:05 PM 3/20/2013 10:22:16	0 Day(s), 5 Hr(s 62.	62.38 0	0	RESEARCHLAB\adminuser2	3/20/2013
							RESEARCHLAB\adminuser3	3/20/2013
🕂 Add Domains	•							Þ

5.9 How to View Environment Info Reports?



Click on 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.

🚚 Environment Info - Summary	(RESEARCHLA	(B)						• 🔀		
👩 Refresh 👻 📑 Export 🍸 F	ilter 🛛 🛅 Cust	omize 🛛 📑 E-	mail				Find	2		
Note: All System Info reports require	lote: All System Info reports require WMI to be installed and enabled. Click here for more information									
Enterprise - ENVIRONI	🚰 Summar	У								
RESEARCHLAB	Generated on	20 Mar, 2013, ()4:25:34 PI	M S	tatus: Success	Filter: Not App	lied			
TREELAB	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\s		
	RD11	Windows_NT	C:	C:\Windows	C:\Windows\TEMP	C:\Windows\TEMP	.COM;.EXE;.BAT;.C	C:\Windows\s		
🕂 Add Domains	•							Þ		



6 Additional Features

6.1 How to customize fields?



for customizing the information.

🕈 Custom View - Domains-	-Shares 🛛 🔀
Customization PATHFINDER	:
 Share Name Path User Name Security Maximum Uses Comment 	
Select All Clear <u>A</u> ll	<u>O</u> K <u>C</u> ancel

Click Select All for selecting all the check boxes.

Click Clear <u>All</u> for clearing all the check boxes.

Click button for confirming the changes.

Click Click button for cancelling the operation.

6.2 How to Apply Filters?



The ARKWE Filter window will be displayed. .

🝸 Filter - Domains-Shares	
Eield Operat	
[Host Name]	▼ RD45 ▼
<u>A</u> dd to Filter	'O <u>R</u> ' to Filter
	[] \$ ¥ 💥 🕅
	<u>O</u> K <u>C</u> ancel

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 Add to Filter
- 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).

🏆 Filter - Domains-Shar	es						(×
Eield	Operator		<u>/</u> alues					
[Host Name] 🔹 🔻	=	▼ F	RD45					•
<u>A</u> ND to Filter				'0	<u>R</u> ' to Fil	ter		
				()	*	X	×	
[Host Name] = 'RD45'								
				<u>0</u> K			ance	

5) Click OK to apply the filter.

NOTE:

- > Use the <u>AND to Filter</u>, <u>'OR' to Filter</u> 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 \bowtie 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	T Filtered	

6.3 How to Refresh Data?

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



Click on 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.



_____ 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.

Export		×
Select the export pat to be exported.	th, format, file name and table name for the	e report
File Format: HTML	ers\Public\Documents\ARKWE 8x\Expo 	t
Export to time-sta	amped sub-folder	
	ОК	Cancel

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:

😰 E-mail	l Report		— ×
	Specify S format ar	MTP Server name, From Address, To address, Subject, Body of the e-mail message, attac nd option to attach the report as zip file format.	:hment
:	SMTP Server:	rd45	
	Erom:	Erings@pathfinder.local	
	<u>I</u> o	AmyRecker@Pathfinder.local	💕 Check
<u>S</u> end	S <u>u</u> bject:	Domains - Shares	
Attach	ment Format:	HTML 💌 🗹 Compress the attachment	

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.



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 mailenabled 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**.

💁 Check Names	—
Admin Report Kit for Windows Enterprise Founds more than one "de" Do you want to: Delete this Recipients from the list Change to 	OK Cancel
Deco D. Canavaro[deco@pathfinder.local] Social Design[Design@pathfinder.local] De üäĤļßé user[DEueaeAPAsseuser@pathfinder.local] Social Development[Development@pathfinder.local] dethgtgh[rggggggg@pathfinder.local]	Properties

> To get more information about the listed recipients under Change to, select the

name, and then **click** Properties...

🛃 Deco D. Canavar	0			×
Details				
First Name:	Deco	Initials:	D	
Last Name:	Canavaro			
Display Name:	Deco D. Canavaro			.
Title:		Department:		
Company:				
Alias:	deco	Mobile number:	:	-
E-mail:	deco@pathfinder.local			
Webpage:				
			OK Car	ncel

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

😒 Check Names	×
Admin Report Kit for Windows Enterprise does not recognize "tz"	
Do you want to:	ОК
Oelete this Recipients from the list	
Change to	Cancel
(No suggestions)	Properties

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 Lo...** 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.**

Find Names						×
Find Na <u>m</u> es in:	All Global Address	List				•
<u>D</u> isplay Name	de					
Last Name			First <u>n</u> ame			
<u>T</u> itle			<u>A</u> lias			
<u>C</u> ompany			Department			
<u>O</u> ffice			Cjty			
					E	ind
Name		Phone	Alias	Office	Job Title	С
	∛Á¼Bé contact		DEüäĤÄ			
	∜üBé user	éúĺŰ	DEüääÅ	ñÁÓį	çîÀE«	è
	Canavaro		deco			
Sesign &			Design			
📕 👗 dethgtgh			19999999			
용 Develop	ment		Development			
•						F.
Add re	cipient to	Cc	Bcc	Prope	rties Clo	ose

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

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 Find everyone [20]

- **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.

🧟 Refresh 🕁 Print/Preview	📑 Export 🖓 F	ilter 🛛 💼 Customiz	e 🛛 🐳 E-mail			Find everyone	
Enterprise - DOMAINS	딣 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\Exc	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	Remoti
		Bharath Source Coo	F:\Bharath\Bharath	PATHFINDER\AD	Allow - Full Control	Unlimited	
		Bulk export for patc	F:\Bulk export for pa	Everyone	Allow - Read	Unlimited	
		C\$	C:\		Admin Share	Unlimited	Defaul
		F\$	F()		Admin Share	Unlimited	Defaul
		G	G:\	Everyone	Allow - Read	Unlimited	
		NETLOGON	C:WINDOWS\SYSV	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\Exc	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.

Scan option for 'VOYAGER'
Scan Entire Domain Selecting this option may take significant amount of time to complete depending on the size of the domain.
✓ Domain Controllers ✓ Servers ✓ Workstations
Scan Selected Server(s) in Domain Enter Computer Name
Add
RD40 Add Erom
Remove
Select Scan Profile:Select a Profile
<u>O</u> K <u>C</u> ancel

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:

进 Select	Servers for 'VOYAGER'
······	RD40
🔽	RD41
🔽	RD43
	RD71
🖸	RD72
	RD73
🖸 I	RD81
	RD83
	RD84
	<u>O</u> K <u>C</u> ancel

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.

Chapter 6

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:

Scheduled Tasks					×
⊡ Scheduled Tasks	Task Name	Run as	Schedule	Report Type	Exported Files
Builtin Report Ta: Builtin Domain Ta	Builtin Report Task	TREELAB\adminuser3	At 1:25 PM every day, starting 3/22/2013	Built-in Report	<u>Click here to view</u>
Builtin User Task Standard Domain	Builtin Domain Task	TREELAB\adminuser3	At 2:45 PM every day, starting 3/22/2013	Built-in Report	<u>Click here to view</u>
Standard Server		TREELAB\adminuser3	At 4:30 PM every day, starting 3/22/2013	Built-in Report	<u>Click here to view</u>
Operating System	Standard Domain Reports	TREELAB\adminuser3	At 8:21 PM every day, starting 3/22/2013	Standard Report	<u>Click here to view</u>
	Standard Server Reports	TREELAB\adminuser3	At 8:23 PM every day, starting 3/22/2013	Standard Report	<u>Click here to view</u>
	Current Status Report	TREELAB\adminuser3	At 8:25 PM every day, starting 3/22/2013	Standard Report	Click here to view
	Operating System Information	TREELAB\adminuser3	At 8:27 PM every day, starting 3/22/2013	Standard Report	Click here to view
۰ III + I	Edit Task Delet	e Task			Close

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:

Report Shares an	d Resources-Shares
Domain Name	Server Name
PATHFINDER	RD45
PATHFINDER	RD53
PATHFINDER	RD47
PATHFINDER	RD49
PATHFINDER	RD54
PATHFINDER	RD52

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



Export Wizard.

Step 1: Report Selection

🔀 Power Export - Standard Reports	x
Step 1 of 6 : Report Selection	
Select the desired report(s) using the checkboxes given below.	\mathbf{X}
	S 💊
Domain Reports	<u>_</u>
⊕ ····· I Operating System & Hot Fixes	=
Server Reports	
Users and Groups	
General	
▼ Status	
	-
< <u>Back</u> <u>Next></u>	Close

- **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.

X Power Export - Standard Reports			×
Step 2 of 6 : Domain Selection For each of the following reports, select the list of domains for Double-click on a report or click Add Domains. The report for as a separate file.	-	2 .	×
Domains-Summary Domains-Trust Domains-Shares Domains-Applications NetworkConfigurations-IP Configuration NetworkConfigurations-Login Profiles NetworkConfigurations-Network Adapters NetworkConfigurations-Network Protocols OSInfos-Operating System Configuration OSInfos-Hot Fixes PrinterInfos-Printers HardwareInfos-Summary HardwareInfos-BIOS Info HardwareInfos-Processors		Domain Name No Domain Selected	omains
		< <u>B</u> ack <u>N</u> ext>	Close

 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.

Select Domain(s)/Server(s)
Select one or more domains. Click on the Apply To button in order to apply the same list of domains for all the selected Reports. To generate the report for all servers in a domain, select the domain, or select a set of servers to restrict the domain scan. Or you may select a Scan Profile.
Select Domain/Server
TREELAB
i≟
Select Scan Profile:Select a Profile
Apply to Reports OK Cancel

- 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:

🔀 Power Export - Standard Reports			- ×
Step 2 of 6 : Domain Selection For each of the following reports, select the list of domains for Double-click on a report or click Add Domains. The report for e as a separate file.	-		\varkappa
Domains-Summary Domains-Trust Domains-Shares Domains-Applications NetworkConfigurations-IP Configuration NetworkConfigurations-Login Profiles NetworkConfigurations-Network Adapters NetworkConfigurations-Network Protocols OSInfos-Operating System Configuration OSInfos-Hot Fixes PrinterInfos-Printers HardwareInfos-BIOS Info HardwareInfos-Processors		Domain Name TREELAB [Full Scan] Add E	<u>)</u> omains
		< <u>Back</u> <u>N</u> ext>	Close

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.

🔀 Power Export - Standard Reports		x
Step 3 of 6 : Server Selection		
For each of the following reports, select the list of servers for which yo Double-click on a report or click Add Servers. The report for each of the a separate file.		X
Users and Groups-General	Server Name	
Users and Groups-Status	No Server Selected	
	Add Se	rvers
	< <u>B</u> ack <u>N</u> ext>	Close

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.

)
Select Domain(s)/Server(s)
Select one or more domains. Click on the Apply To button in order to apply the same list of domains for all the selected Reports.
Select Domain/Server
TREELAB
È
Select Scan Profile:Select a Profile ▼
Apply to Reports OK Cancel

- **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:

🔀 Power Export - Standard Reports	—
Step 3 of 6 : Server Selection	
For each of the following reports, select the list of servers for whic Double-click on a report or click Add Servers. The report for each of a separate file.	
Users and Groups-General	Server Name
Users and Groups-Status	TREELAB\RD50
	TREELAB\RD73
	VSSLAB\RD20
	VSSLAB\RD21
	VSSLAB\RD22
	VSSLAB\RD24
	VSSLAB\RD25
	VSSLAB\RD26
	VSSLAB\RD23
	VSSLAB/RD05
	VSSLAB\VMSRV02
	Add Servers
	< <u>Back</u> <u>Next></u> Close

4) Click Next to proceed to the Next step.

Step 4: Delivery Options

🔀 Power Export - St	andard Reports	×
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	×
Export Type:	HTML •	
Export		
Export Path :	C:\Users\Public\Documents\ARKWE 8.x\Export	
🔲 E-mail		
To Address:	Additional E-mail Settings	
	☑ Compress the attachment	
Note: This evalua	tion version exports / e-mails only the first 10 records.	
	< <u>Back</u> <u>N</u> ext>	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 🗾
	an customize the SMTP Server, From and To s, Subject and body of the e-mail message.
S <u>M</u> TP Server:	rd45
<u>F</u> rom:	jamie@pathfinder.local
<u>T</u> o:	Tom Ford@pathfinder.local
S <u>u</u> bject:	Reports generated by ARKWE
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise
-	OK Cancel

Step 5: Schedule Settings

🔀 Power Export -	Standard Reports	x
-	Schedule Settings	s e
Enter a unique ta	ask name and specify its schedule settings.	X
Task Name	Standard Reports Task	
Specify an acco Domains/Server	unt that has sufficient privileges to retrieve report information from the selected 's.	
Run As	PATHFINDER\adminuser Set Password	
Schedule Task:	Daily Start time: 05:00 PM Advanced	
-Schedule Task	Daily	
Every 1	day(s)	
	< <u>Back</u> <u>N</u> ext>	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 -	Standard Reports			×
Step 6 of 6 : Click Finish to s	Summary ave the task details.			\mathbf{x}
Task Name:	Standard Reports Tas			Report Standard
Run As: Schedule:	PATHFINDER \adminu	ser day, starting 3/21/201	3	Å •
Report Name		Servers/Domains	Export As	Export Folder (Export Path\Task Name)
Domains-Summ	ary	<u>Click here to view</u>	HTML	C: \Users \Public \Documents \ARKWE 8.x \Export \Standard Reports Task
Domains-Trust		Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
Domains-Share	S	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
Domains-Applic	ations	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
NetworkConfig Configuration	urations-IP	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
NetworkConfig	urations-Login Profiles	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task
•		III		•
				< <u>Back</u> <u>Finish</u> 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:

Output Description of the second s						x
Scheduled Tasks Scheduled Tasks TestEvents Standard Report	Task Name: Run As: Report Type: Schedule:	Standard Reports Task PATHFINDER \adminuser Standard Report Exported Files: Click here to vie At 5:00 PM every day, starting 3/21/2013			4 1	
	Report Name		Servers/Domains	Export As	Export Folder (Export Path\Task Name)	
	ComputerStatusI	infos-Summary	<u>Click here to view</u>	HTML	C: \Users \Public \Documents \ARKWE 8.x \Export \Standard Reports Task	Ξ
	DisplayConfigura	tions-Monitor Info	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	DisplayConfigura Info	tions-Video Adapter	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	Domains-Applicat	ions	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	Domains-Shares		Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	Domains-Summar	у	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	Domains-Trust		Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	
	EnvironmentInfo	s-Summary	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Standard Reports Task	+
	•					
•	Edit Task	Delete Task			Close	

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

This will bring up the Power Export Wizard.

Step 1: Report Selection

🔀 Power Export - Built-in Reports	×
Step 1 of 6 : Report Selection Select the desired report to proceed. Only one report can be selected in this category.	$\left \right\rangle$
List of permissions for specific users and groups on folders List of permissions for specific users and groups on files List of permissions for specific users and groups on files List of permissions for files	
< <u>B</u> ack <u>N</u> ext>	Cļose

- 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) of and groups from.	or a Scan Profile (Users/Groups) to retrieve available users 🛛 📈
Report Name: List of permissions for specific us	sers and groups on folders
Enter account name :	Add to list
Accounts from domain\server:	Browse and Select
Accounts from Scan Profiles (Users/Groups):	Select a Profile 🔻 🕕
Selected Accounts	
Account Name	Account Type Remove Reset
•	III → < <u>Back</u> <u>N</u> ext> Close
🔀 Power Export - Built-in Reports	

Report Name: Li:	st of permissions for specific u	sers and grou	ups on folders			
	Enter account name :			🞝 Add	to list	0
Ad	counts from domain\server:	Bro	wse and Select			
Accounts from S	can Profiles (Users/Groups):	Frequent S	cans	- 🕕		
Selected Account	s					
Account Name			Account Type		-	Remove
TREELAB\Admir	histrator		User			
TREELAB\admin	user1		User			Reset
TREELAB\admin	user2		User		=	
TREELAB\admin	user3		User			
TREELAB\albert	0		User			
TREELAB\barto	n		User			
TREELAB\shane	;		User			
TREELABitony			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

🔀 Power Export	- Built-ii	n Reports			—			
Step 3 of 6	: Share	ed Folder Selection						
of UNC folder	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 I	List of p	ermissions for specific (users and groups on folders					
UNC Path:				Add				
Scan Profile (S	ihares):	<no found.="" profile=""></no>	• ()					
Folder Path			Include sub-fold	Folder level	Add From			
\\RD50\ADMI	N\$		True	All	≡ Import			
\\RD50\ARKV	VE		True	All	Tubou			
\\RD50\C\$			True	All	Remove			
\\RD50\E\$			True	All				
\\RD50\new			True	All	T			
•				•				
	play folde	ers that have the same perm	hissions as the parent	it Folder Options.				
📃 Include gro	up membe	ership information 🛛 🔲 Inclu	ude <u>S</u> ID					
🔲 <u>V</u> alidate for	^r Errors	📝 Incl <u>u</u> de Error Details						
Generate report ignoring any errors found								
🔘 Gener	C Generate report only if no errors were found. Send error report through e-mail E-mail Settings							
			< <u>B</u> a	ack 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.

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	icel

- 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 - St	andard Reports	-X
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	×
Export Type:	HTML -	
Export		
Export Path :	C:\Users\Public\Documents\ARKWE 8.x\Export	
E-mail		
To Address:	Additional E-mail Settings	
	☑ Compress the attachment	
Note: This evalua	tion version exports / e-mails only the first 10 records.	
	< <u>Back</u> <u>N</u> ext>	Close

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

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

Chapter-6-Power Export

Additional E-mail	Settings 🗾
	in customize the SMTP Server, From and To s, Subject and body of the e-mail message.
S <u>M</u> TP Server:	rd45
<u>F</u> rom:	jamie@pathfinder.local
<u>T</u> o:	Tom Ford@pathfinder.local
S <u>u</u> bject:	Reports generated by ARKWE
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise
	OK Cancel

Step 5: Schedule Settings

🔀 Power Export	- Built-in Reports	x
Step 5 of 6	: Schedule Settings	
Enter a unique	etask name and specify its schedule settings.	×
Task Name	Folder Specific User Perm	
Specify an ac Domains/Serv	count that has sufficient privileges to retrieve report information from the selected rers.	
Run As	TREELAB\adminuser3 Set Password	
<u>S</u> chedule Task	k: Daily Start time: 04:30 PM 🚔 Advanced	
Schedule Tas	sk Daily	
Every 1	day(s)	
	< <u>Back</u>	Cļose

- **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					×
-	Summary ave the task detai	ls.				$\left \right\rangle$
Task Name:	Folder Specific L	Jser Perm		F	Report	Built-in Report
Run As:	TREELAB\admin	user3				
Schedule:	At 04:30 PM er	very day, starting	3/22/2013			* *
Report Name		User/Group Accounts	Shared Folders	Export As	Export Folde (Export Path	r \Task Name)
List of permission users and group	ns for specific os on folders	<u>Click here to</u> view	<u>Click here to view</u>	HTML	C:\Users\Pub 8.x\Export\Fi	lic\Documents\ARKWE older Specific User Per
•		III				Þ
				< <u>B</u> ack	<u> </u>	h C <u>l</u> ose

- 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

This will bring up the Power Export Wizard.

Step 1: Report Selection

🔀 Power Export - Built-in Reports	EX
Step 1 of 5 : Report Selection Select the desired report to proceed. Only one report can be selected in this category.	s e
select the desired report to proceed. Only one report can be selected in this category.	\mathbf{X}
 List of permissions for specific users and groups on folders List of permissions for folders 	
List of permissions for folders List of permissions for specific users and groups on files	
E List of permissions for files	
	Vext> Close

- 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			×
Enter the full path of a of UNC folder paths f	red Folder Selection a Share or Shared Folder. Click Add From rom a text file. Select a folder in the list be scanning each folder.			
Report List of	permissions for folders			
UNC Path:			Adg	<u>1</u>
Scan Profile (Shares):	<no found.="" profile=""></no>	• ()		
Folder Path		Include sub-fold	Folder level	Add From
\\RD50\ADMIN\$		True	All	E Import
\\RD50\ARKWE		True	All	imporc
\\RD50\C\$		True	All	Remove
\\RD50\E\$		True	All	
\\RD50\new		True	All	T
•			•	
Do not display fol folder	ders that have the same permissions as t	he parent	it Folder Options	
📃 Include group mem	bership information 🛛 🔲 Include SID			
🔄 <u>V</u> alidate for Errors	📝 Incl <u>u</u> de Error Details			
 Generate rep 	ort ignoring any errors found			
🔘 Generate rep	ort only if no errors were found. Send er	ror report through e-r	nail 🛛 E-mail Se <u>t</u> t	ings
		< <u>B</u>	ack <u>N</u> ex	t> 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: [<u>\\RD49\Address</u>	
Include sub-folders	
Traverse only 1 📄 level(s) of sub-folder in the share	
Apply this setting to all folders in list	icel

- 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 t to proceed to the *Next* step.

Step 3: Delivery Options

🔀 Power Export - St	andard 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:	Additional E-mail Settings			
	✓ Compress the attachment			
Note: This evalua	tion version exports / e-mails only the first 10 records.			
	< <u>Back</u> <u>Next></u>	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 ca addres	n customize the SMTP Server, From and To s, Subject and body of the e-mail message.		
S <u>M</u> TP Server:	rd45		
<u>F</u> rom:	jamie@pathfinder.local		
<u>I</u> o:	Tom Ford@pathfinder.local		
S <u>u</u> bject:	Reports generated by ARKWE		
Please find the at Windows Enterpri	tached report generated by Admin Report Kit For ise		
	OK Cancel		

Step 4: Schedule Settings

🔀 Power Export -	Built-in Reports	x
Step 4 of 5 :	Schedule Settings	
Enter a unique t	task name and specify its schedule settings.	<
Task Name	Folder Permissions	
Specify an acco Domains/Serve	ount that has sufficient privileges to retrieve report information from the selected rs.	
Run As	TREELAB\adminuser3 Set Password	
<u>S</u> chedule Task:	Daily Start time: 05:30 PM Advanced	
-Schedule Task	k Daily	
Every 1	aay(s)	
	< <u>Back</u> <u>N</u> ext> Clos	e

- **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 🧱				
-	Summary ave the task details.			$\left \right>$
Task Name:	Folder Permissions		Report	Built-in Report
Run As:	TREELAB\adminuser3			
Schedule:	At 05:30 PM every day	/, starting 3/	22/2013	4 7
Report Name	Shared Folders	Export As	Export Folder (Export Path\Task Name)	Printer E
List of permission for folders	ons <u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Folder Permissions	
•				
			< <u>B</u> ack	nish C <u>l</u> ose

- 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

This will bring up the Power Export Wizard.

Step 1: Report Selection

🔀 Power Export - Built-in Reports	
Step 1 of 6 : Report Selection	
Select the desired report to proceed. Only one report can be selected in this category.	×
E 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	
< <u>B</u> ack	Cļose

- 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.
- 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
Step 2 or 6 : Osen/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 :
Accounts from domain\server: Browse and Select
Accounts from Scan Profiles (Users/Groups):Select a Profile
Account Name Account Type Remove
Re <u>s</u> et ∢►
< <u>B</u> ack <u>N</u> ext> Close
Yewer 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 :

Step 2 of 6 : User/Group Selection			
Select a server or a Scan Profile (Computers) and groups from.	or a Scan Profile (Users/Groups) to retrieve available usa	ers 🔀
Report Name: List of permissions for specific u	sers and groups on folders		
Enter account name :		🛃 Add to list) 🕕
Accounts from domain\server:	Browse and Select		
Accounts from Scan Profiles (Users/Groups):	Frequent Scans	• ()	
Selected Accounts			
Account Name	Account Type	^	Remove
TREELAB\Administrator	User		
TREELAB\adminuser1	User		Reset
TREELAB\adminuser2	User	E	
TREELAB\adminuser3	User		
TREELAB\alberto	User		
TREELAB\barton	User		
TREELAB\shane	User		
TREELABltony	User	T	
•		P	
		<back next=""></back>	Close

- 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

🔀 Power Export - Built	t-in Reports			—			
Step 3 of 6 : Shared Folder Selection							
of UNC folder paths t	a Share or Shared Folder. Click Add Froi from a text file. Select a folder in the list r scanning each folder.			V.			
Report List of	f permissions for specific users an	d groups on folders	i				
UNC Path:			Adg	<u>i</u>			
Scan Profile (Shares)	K ≤No Profile found.>	• ()					
Folder Path		Include sub-fold	Folder level	Add From			
\\RD50\ADMIN\$		True	All	≡ <u>I</u> mport			
\\RD50\ARKWE		True	All				
\\RD50\C\$		True	All	Remove			
\\RD50\E\$		True	All				
11RD501new		True	All	T			
			•				
Do not display fo folder	lders that have the same permissions as	the parent	lit Folder Options				
🔲 Include group men	nbership information 🔲 Include SID						
Validate for Errors	; 📝 Incl <u>u</u> de Error Details						
Generate rep	port ignoring any errors found						
🔘 Generate rep	port only if no errors were found. Send a	error report through e-r	nail 🛛 E-mail Sețt	ings			
		< <u>B</u>	ack <u>N</u> ex	t> 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) 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.

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	cel

- 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 - St	andard Reports	-X				
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:	Additional E-mail Settings					
	✓ Compress the attachment					
Note: This evalua	ation version exports / e-mails only the first 10 records.					
	< <u>Back</u> <u>N</u> ext> C	ljose				

- 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.					
S <u>M</u> TP Server:	rd45				
<u>F</u> rom:	jamie@pathfinder.local				
<u>T</u> o:	Tom Ford@pathfinder.local				
S <u>u</u> bject:	Reports generated by ARKWE				
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise				
	OK Cancel				

Step 5: Schedule Settings

🔀 Power Export -	- Built-in Reports	×
	ask name and specify its schedule settings.	\mathbf{i}
Task Name	Specific User File Perm	
Specify an acco Domains/Serve	ount that has sufficient privileges to retrieve report information from the selected rrs.	
Run As	TREELAB\adminuser3 Set Password	
<u>S</u> chedule Task:	Daily Start time: 04:30 PM Adyanced	
-Schedule Tasl	k Daily	
Every 1	🚔 day(s)	
	< <u>Back</u>	Cļose

- **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					×
-	Summary ave the task detail	ls.				\gg
Task Name:	Specific User File	e Perm		F	Report	Built-in Report
Run As:	TREELAB\adminu	user3				
Schedule:	At 04:30 PM ev	very day, starting	3/22/2013			* *
Report Name		User/Group Accounts	Shared Folders	Export As	Export Folder (Export Path)	
List of permission users and group		<u>Click here to</u> <u>view</u>	Click here to view	HTML	C:\Users\Publ 8.x\Export\Sp	ic\Documents\ARKWE becific User File Perm
<		m				Þ
				< <u>B</u> ack	<u> </u>	Cļose

- **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.

Po	wer Export				
	Built-in Reports	•	A	Permissions	
	Standard Reports		3	Shares and Resources	
Æ	Scheduled Tasks		88	Users and Groups	
t			ŧ.	Domains	option under Power Export.

Select

This will bring up the Power Export Wizard.

Step 1: Report Selection

🔀 Power Export - Built-in Reports	_
Step 1 of 5 : Report Selection	
Select the desired report to proceed. Only one report can be selected in this category.	$\boldsymbol{\varkappa}$
Eist 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	
< <u>B</u> ack <u>N</u> ext>	Close

- 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 R	leports						
Step 2 of 5 : Shared Folder Selection							
	are or Shared Folder. Click Add From t a text file. Select a folder in the list bel nning each folder.						
Report List of peri	missions for files						
UNC Path:			Adg	1			
Scan Profile (Shares): 🖃	No Profile found.>	• ()					
Folder Path		Include sub-fold	Folder level	Add From			
\\RD50\ADMIN\$		True	All	E			
\\RD50\ARKWE		True	All	= <u>I</u> mport			
\\RD50\C\$		True	All	Remove			
\\RD50\E\$		True	All				
\\RD50\new		True	All	T			
•			1				
Do not display files that	at have the same permissions as the p	arent folder <u>E</u> di	it Folder Options.				
🔲 Include group members	hip information 🔲 Include SID						
Validate for Errors	📝 Include Error Details						
 Generate report ig 	noring any errors found						
Generate report or	nly if no errors were found. Send erro	or report through e-m	nail 🛛 E-mail Se <u>t</u> t	tings			
		<u></u> 8	ack Next	t> 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) 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:

Folder Options	×
Folder Path: MRD49\Address	
Include sub-folders	
Iraverse only level(s) of sub-folder in the share	
Apply this setting to all folders in list	icel

- 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 - St	andard Reports	×
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	×
Export Type:	HTML -	
Export		
Export Path :	C: \Users \Public \Documents \ARKWE 8.x \Export	
🔲 E-mail		
To Address:	Additional E-mail Settings]
	✓ Compress the attachment	
Note: This evalua	tion version exports / e-mails only the first 10 records.	
	< <u>Back</u> <u>Next></u>	Close

Change the Export or E-mail settings as necessary.
 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.			
S <u>M</u> TP Server:	rd45		
<u>F</u> rom:	jamie@pathfinder.local		
<u>T</u> o:	Tom Ford@pathfinder.local		
S <u>u</u> bject:	Reports generated by ARKWE		
Please find the attached report generated by Admin Report Kit For Windows Enterprise			
	OK Cancel		

Step 4: Schedule Settings

🔀 Power Export -	- Built-in Reports	×
Step 4 of 5 :	: Schedule Settings	
Enter a unique t	task name and specify its schedule settings.	ŝ
Task Name	File Permissions	
Specify an acco Domains/Serve	ount that has sufficient privileges to retrieve report information from the selected ers.	
Run As	TREELAB\adminuser3 Set Password	
<u>S</u> chedule Task:	: Daily Start time: 06:30 PM Advanced	
-Schedule Task	k Daily	
Every 1	aay(s)	
	< <u>Back</u> <u>N</u> ext>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 5: Summary

🔀 Power Export -	Built-in Reports			×
-	Summary ave the task details.			\times
Task Name:	File Permissions		Report	Built-in Report
Run As:	TREELAB\adminuser3			
Schedule:	At 06:30 PM every day	y, starting 3,	/22/2013	÷
Report Name	Shared Folders	Export As	Export Folder (Export Path\Task Name)	Printer E-m
List of permission for files	ons <u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\File Permissions	
•			III	4
			< <u>B</u> ack	inish 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

Po	wer Export	-		
匙	Built-in Reports	A	Permissions	
	Standard Reports	3	Shares and Resources	
23	Scheduled Tasks	82	Users and Groups	
		()	Domains	option under Power Export.

This will bring up the Power Export Wizard.

Step 1: Report Selection

Click

🔀 Power Export - Built-in Reports	x
Step 1 of 7 : Report Selection	
Select the desired report(s) using the checkboxes given below. More than one report may be selected in this category.	X
Shares and Resources Subscription: Shares Subscription:	
	lose

- **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

🔀 Power Export - Built-in Reports	×
Step 2 of 6 : Server Selection For each of the following reports, please select the list of servers for report. Double-click on a Report or click Add Servers. The report for ea exported as a separate file.	
List of Shares List of Shares with permissions	Server Name No Server Selected Add Servers
	< <u>Back</u> <u>N</u> ext> Close

- 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:

🔀 Power Export - Built-in Reports	
Step 2 of 6 : Server Selection For each of the following reports, please select the list of servers for report. Double-click on a Report or click Add Servers. The report for exported as a separate file.	
List of Shares List of Shares with permissions	Server Name PATHFINDER\RD45 PATHFINDER\RD53 PATHFINDER\RD47 PATHFINDER\RD49 PATHFINDER\RD54 PATHFINDER\RD52
	< <u>B</u> ack <u>N</u> ext> Close

3) Click Next to proceed to the next step.

Step 3: Report Criteria (Optional)

🔀 Power Export - Built-in Reports			
Step 3 of 6 : Report Criteria (Optional) You may specify a criteria for each of the following reports to filter data. Click Next to keep the current criteria as described under Criteria Description or click Edit Criteria to modify it.			
	Criteria Description:		
List of Shares	(Share Type = 'Folder Share')		
	<u>E</u> dit Criteria		
	< <u>Back N</u> ext> Close		

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:

Criteria Sett	ings			×
Report	List of Shares			
Share Type:				
	er Share in Share			
		(ОК	Cancel

- **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:

🔀 Power Export - Built-in Reports 🛛 💽			
Step 3 of 6 : Report Criteria (Optional) You may specify a criteria for each of the following reports to filter data. Click Next to keep the current criteria as described under Criteria Description or click Edit Criteria to modify it.			
Server Reports	Criteria Description:		
List of Shares	(Share Type = 'Folder Share' OR Share Type = 'Admin Share')		
	<u>E</u> dit Criteria		
	< <u>B</u> ack <u>N</u> ext> Close		

6) Click Next to proceed to the Next step.

Step 4: Delivery Options

🔀 Power Export - St	andard Reports	_X
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	×
Export Type:	HTML -	
Export		
Export Path :	C: \Users\Public\Documents\ARKWE 8.x\Export	
E-mail		
To Address:	Additional E-mail Settings	
	✓ Compress the attachment	
Note: This evalua	tion version exports / e-mails only the first 10 records.	
	< <u>B</u> ack <u>Next></u>	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.

Additional E-mail	Settings 💽	
	in customize the SMTP Server, From and To s, Subject and body of the e-mail message.	
S <u>M</u> TP Server:	rd45	
<u>F</u> rom:	jamie@pathfinder.local	
<u>I</u> o:	Tom Ford@pathfinder.local	
S <u>u</u> bject:	Reports generated by ARKWE	
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise	
	OK Cancel	

Step 5: Schedule Settings

🔀 Power Export - I	Built-in Reports	×
Step 5 of 6 :S	chedule Settings	
Enter a unique ta	isk name and specify its schedule settings.	×
Task Name	Builtin Report Task	
Specify an accou Domains/Server:	unt that has sufficient privileges to retrieve report information from the selected s.	
Run As	PATHFINDER\adminuser Set Password	
<u>S</u> chedule Task:	Daily Start time: 1:25 PM 🔄 Advanced	
-Schedule Task	Daily	
Every 1	day(s)	
	< <u>B</u> ack <u>N</u> ext> 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

•	Summary ave the task details.			X
Task Name: Run As:	Builtin Report Task PATHFINDER\adminuse	r	Report	Built-in Report
Schedule:	At 01:25 PM every da	y, starting 3/2	22/2013	÷.
Report Name	Servers/Domains	Export As	Export Folder (Export Path\Task Name)	Printer
List of Shares	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task	
List of Shares with permission	S Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task	
4				1

- 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:

Scheduled Tasks						X
E	Task Name:	Builtin Report Task				
		PATHFINDER\adminu:	ser			
	Report Type:	Built-in Report		Exported Files:	Click here:	to view
	Schedule:	At 1:25 PM every da	v starting 3/22			*
			,,			Ŧ
	Report Name	Servers/Domains	Export As	Export Folder (Export Path\Task Name)	*	Printer
	List of Shares	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task		
	List of Shares with permissions	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Report Task		
	•	1	11			Þ
۰ III +	Edit Task	<u>D</u> elete Task				Close

7.6 Schedule Users and Groups Built-in Reports

	Po	ower Export	_		
	k	Built-in Reports	4	Permissions	
		Standard Reports	3	Shares and Resources	
	2	Scheduled Tasks	82	Users and Groups	
k			ħ	Domains	option under Power Export.

Click

Step 1: Report Selection

🔀 Power Export - Built-in Reports	×
Step 1 of 7 : Report Selection Select the desired report(s) using the checkboxes given below. More than one report may be selected in this category.	\mathbf{x}
 Users and Groups Users and Groups Ust of Users and Groups Ust of User accounts Ust of Local and Global groups Ust of disabled user accounts Ust of locked-out user accounts Ust of locked-out user accounts (Password never expires etc.) Password settings of all user accounts (Log on locally etc.) On rights assigned for all accounts Or privileges accounts Or privileges Or privileges Or privileges Or p	
< <u>B</u> ack <u>N</u> ext>	Close

- **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

🔀 Power Export - Built-in Reports	
Step 2 of 6 : Server Selection	
For each of the following reports, select the list of servers for which yo Double-click on a report or click Add Servers. The report for each of the a separate file.	
List of Users and Groups	Server Name
🖹 List of User accounts	No Server Selected
El List of Local and Global groups	
List of disabled user accounts	
List of locked-out user accounts	
Password settings of all user accounts (Password never exp	
Members of Local Administrators group	
Log on rights assigned for all accounts (Log on locally etc.)	
Privileges assigned for all accounts	
Group membership with nested groups	
۰ III ا	Add Servers
	< <u>B</u> ack <u>N</u> ext> Close

- 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.
- 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:

🔀 Power Export - Built-in Reports	
Step 2 of 6 : Server Selection	
For each of the following reports, select the list of servers for which yo Double-click on a report or click Add Servers. The report for each of the a separate file.	-
List of Users and Groups	Server Name
Elist of User accounts	TREELAB\RD50
List of Local and Global groups	TREELAB\RD71
List of disabled user accounts	VSSLAB\RD05
List of locked-out user accounts	VSSLAB\RD20
Password settings of all user accounts (Password never exp	VSSLAB\RD21
Members of Local Administrators group	VSSLAB\RD22
Log on rights assigned for all accounts (Log on locally etc.)	VSSLAB\RD26
Privileges assigned for all accounts	
Group membership with nested groups	
4 III >	Add Servers
	< <u>Back</u> <u>N</u> ext> Close

3) Click Next to proceed to the next Step.

Step 3: Report Criteria (Optional)

🔀 Power Export - Built-in Reports	
Step 3 of 6 : Report Criteria (Optional) You may specify a criteria for each of the following reports to filter data criteria as described under Criteria Description or click Edit Criteria to mo	
Server Reports List of Users and Groups List of User accounts List of Local and Global groups List of Local and Global groups List of locked-out user accounts Password settings of all user accounts (Password nev Members of Local Administrators group Log on rights assigned for all accounts (Log on locally Privileges assigned for all accounts Group membership with nested groups	Criteria Description: (Account Type = 'Built-in User')
	Edit Criteria

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:

Criteria Set	tings 💌
Report	List of Users and Groups
	- <mark>in User</mark> tom User al Group
	OK Cancel

- **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:

criteria as described under Criteria Description or click Edit Criteria to mo	. Click Next to keep the current
	Criteria Description:
 List of Users and Groups List of User accounts List of Local and Global groups List of disabled user accounts List of locked-out user accounts Password settings of all user accounts (Password nev Members of Local Administrators group Log on rights assigned for all accounts (Log on locally Privileges assigned for all accounts Group membership with nested groups 	(Account Type = 'Built-in User' OR Account Type = 'Custom User' OR Account Type = 'Local Group' OR Account Type = 'Global Group')
۰	Edit Criteria

6) Click Next to proceed to the Next step.

Step 4: Delivery Options

🔀 Power Export - St	andard Reports	_X
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	╳
Export Type:	HTML -	
Export		
Export Path :	C:\Users\Public\Documents\ARKWE 8.x\Export	
E-mail		
To Address:	Additional E-mail Settings	
	✓ Compress the attachment	
Note: This evalua	ation version exports / e-mails only the first 10 records.	
	< <u>Back</u> <u>N</u> ext> C	lose

- **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 💽
	in customize the SMTP Server, From and To s, Subject and body of the e-mail message.
S <u>M</u> TP Server:	rd45
<u>F</u> rom:	jamie@pathfinder.local
<u>I</u> o:	Tom Ford@pathfinder.local
S <u>u</u> bject:	Reports generated by ARKWE
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise
	OK Cancel

Step 5: Schedule Settings

🔀 Power Export -	Built-in Reports 🗾
-	Schedule Settings
Enter a unique ta	ask name and specify its schedule settings.
Task Name	Builtin User Task
Specify an acco Domains/Server	ount that has sufficient privileges to retrieve report information from the selected rs.
Run As	TREELAB\adminuser3 Set Password
<u>S</u> chedule Task:	Daily Start time: 04:30 PM Advanced
-Schedule Task	Daily
Every 1	🖨 day(s)
	< <u>Back</u> <u>N</u> ext> 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

•	Summary /e the task details					X
	Builtin User Task TREELAB\adminu: At 04:30 PM eve	ser3 ery day, starting 3/22/2	013	Report	Built-in Re	port
Report Name		Servers/Domains	Export As	Export Folder (Export Path\Task Name	3)	
List of Users and	Groups	<u>Click here to view</u>	HTML	C:\Users\Public\Docume 8.x\Export\Builtin User		
List of User accounts		<u>Click here to view</u>	HTML	C:\Users\Public\Docume 8.x\Export\Builtin User	nts\ARKWE	
List of Local and Global groups		Click here to view	HTML	C:\Users\Public\Docume 8.x\Export\Builtin User	nts\ARKWE Task	
List of disabled user accounts		Click here to view	HTML	C:\Users\Public\Docume 8.x\Export\Builtin User		
List of locked-out user accounts		Click here to view	HTML	C:\Users\Public\Docume 8.x\Export\Builtin User		
Password setting accounts (Passw	gs of all user ord never expires	Click here to view	HTML	C:\Users\Public\Docume	nts\ARKWE	
•						•

- 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:

	Task Name:	Builtin User Task				
	Report Type:	Built-in Report	00.0		Exported Files: Click here to vie	
 Builtin User Task		· · · · · · · · · · · · · · · · · · ·	/ day, starting 3/22/20	10		<u></u>
<u> </u>	Schedule.	AL4.30 FM EVEL)	, day, starting 3/22/20	15		Ŧ
	Report Name		Servers/Domains	Export As	Export Folder (Export Path\Task Name)	
	List of Local and	Global groups	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	List of disabled u	ser accounts	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	Members of Loca group	l Administrators	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	=
	List of locked-ou	t user accounts	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	Password setting accounts (Passw etc.)	gs of all user ord never expires	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	Log on rights ass accounts (Log or		Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	List of User acco	unts	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin User Task	
	Privileges assign		<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8 v\Evport\Builtip User Tack	•
	•					•

7.7 Schedule Domain Built-in Reports

	Po	wer Export	_		
	B.	Built-in Reports	4	Permissions	
		Standard Reports	3	Shares and Resources	
	Æ	Scheduled Tasks	82	Users and Groups	
Click			ħ	Domains	option under Power Export.

This will bring up the Power Export Wizard.

Step 1: Report Selection

🔀 Power Export - Built-in Reports	— ×-
Step 1 of 7 : Report Selection Select the desired report(s) using the checkboxes given below. More than one report may be selected in this category.	$\left \right>$
 Comains Ust of trusted and trusting domains Ust of machines with their OS and service pack Ust of Windows Servers Ust of Domain Controllers Ust of Application Servers (IIS, Exchange Server, SQL Server etc.) Ust of machines that run TCPIP services (FTP, telnet etc.) Ust of machines that have auditing enabled (or disabled) 	
<back next=""></back>	Close

- **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

🔀 Power Export - Built-in Reports	—
Step 2 of 6 : Domain Selection For each of the following reports, select the list of domains for which y Double-click on a report or click Add Domains. The report for each of th as a separate file.	
List of trusted and trusting domains List of machines with their OS and service pack List of Windows Servers List of Domain Controllers List of Application Servers (IIS, Exchange Server, SQL Server) List of machines that run TCPIP services (FTP, telnet etc.) List of machines that have auditing enabled (or disabled)	Domain Name No Domain Selected Add Domains
	<back next=""> Close</back>

- **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:

🗶 Power Export - Built-in Reports	X
Step 2 of 6 : Domain Selection For each of the following reports, select the list of domains for which Double-click on a report or click Add Domains. The report for each of the as a separate file.	
List of trusted and trusting domains List of machines with their OS and service pack List of Windows Servers List of Domain Controllers List of Application Servers (IIS, Exchange Server, SQL Server) List of machines that run TCPIP services (FTP, telnet etc.) List of machines that have auditing enabled (or disabled)	Domain Name RESEARCHLAB TREELAB VSSLAB
	< <u>B</u> ack <u>N</u> ext> Close

3) Click Next to proceed to the next Step.

Step 3: Report Criteria (Optional)

🔀 Power Export - Built-in Reports	
Step 3 of 6 : Report Criteria (Optional) You may specify a criteria for each of the following reports to filter data criteria as described under Criteria Description or click Edit Criteria to mo	
Domain Reports List of trusted and trusting domains List of machines with their OS and service pack List of Windows Servers List of Domain Controllers List of Application Servers (IIS, Exchange Server, SQ List of machines that run TCPIP services (FTP, telnet List of machines that have auditing enabled (or disable)	Criteria Description: (Domains = 'Trusted')
	< <u>B</u> ack <u>N</u> ext> Close

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:

Criteria Set	tings 💌
Report	List of trusted and trusting domains
	sting Domains:
Trus	
	OK Cancel
- **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:

Step 3 of 6 : Report Criteria (Optional) You may specify a criteria for each of the following reports to filter data. C criteria as described under Criteria Description or click Edit Criteria to modi	Click Next to keep the current 🔹 🛝
List of trusted and trusting domains	Criteria Description: (Domains = 'Trusted' OR Domains = 'Trusting')
List of Application Servers (IIS, Exchange Server, SQ List of machines that run TCPIP services (FTP, telnet List of machines that have auditing enabled (or disabl	
4 III	Edit Criteria

6) Click Next to proceed to the Next step.

Step 4: Delivery Options

🔀 Power Export - St	andard Reports	_X
Select the report export option, for	elivery Options delivery options. You can Export and E-mail the reports using the options below. In case of each task, a sub-folder with the task name will be created under the specified export path. ts will be exported to a time-stamped folder in the format "yyyy-mm-dd hh.mm.ss" under the	╳
Export Type:	HTML -	
Export		
Export Path :	C:\Users\Public\Documents\ARKWE 8.x\Export	
E-mail		
To Address:	Additional E-mail Settings	
	✓ Compress the attachment	
Note: This evalua	ation version exports / e-mails only the first 10 records.	
	< <u>Back</u> <u>N</u> ext> C	lose

- 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 💽
	in customize the SMTP Server, From and To s, Subject and body of the e-mail message.
S <u>M</u> TP Server:	rd45
<u>F</u> rom:	jamie@pathfinder.local
<u>T</u> o:	Tom Ford@pathfinder.local
S <u>u</u> bject:	Reports generated by ARKWE
Please find the at Windows Enterpr	tached report generated by Admin Report Kit For ise
	OK Cancel

Step 5: Schedule Settings

🔀 Power Export -	Built-in Reports	×
Step 5 of 6 :	Schedule Settings	
Enter a unique ta	ask name and specify its schedule settings.	$\boldsymbol{\times}$
Task Name	Builtin Domain Task	
Specify an acco Domains/Server Run As <u>S</u> chedule Task:	TREELAB\adminuser3	
Schedule Task	cDaily	
	< <u>Back</u> <u>N</u> ext>	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

•	Summary ave the task deta	ils.			X
Task Name: Run As: Schedule:	Builtin Domain T TREELAB\admir At 02:45 PM e		2/2013	Report	Built-in Report
Report Name		Servers/Domains	Export As	Export Folder (Export Path\Task Name)	
List of trusted domains	and trusting	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\A 8.x\Export\Builtin Domain Ta	
List of machine and service pa		Click here to view	HTML	C:\Users\Public\Documents\A 8.x\Export\Builtin Domain Ta	
List of Window	s Servers	Click here to view	HTML	C:\Users\Public\Documents\A 8.x\Export\Builtin Domain Ta	
List of Domain	Controllers	Click here to view	HTML	C:\Users\Public\Documents\A 8.x\Export\Builtin Domain Ta	
	on Servers (IIS, er, SQL Server	Click here to view	HTML	C:\Users\Public\Documents\A 8.x\Export\Builtin Domain Ta	
····				all contractions and the	

- 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:

domains List of m and serv List of V List of D List of A Exchang etc.)	Name			
domains List of m and serv List of V List of D List of A Exchang etc.)		Servers/Domains	Export As	Export Folder (Export Path\Task Name)
and serv List of W List of D List of A Exchang etc.) List of m	usted and trusting	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
List of A List of A Exchang etc.) List of m	achines with their OS ice pack	⁵ <u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
List of A Exchangetc.) List of m	indows Servers	Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
Exchang etc.) List of m	omain Controllers	<u>Click here to view</u>	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
	oplication Servers (II: e Server, SQL Server		HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
361 41663	achines that run TCP (FTP, telnet etc.)	PIP Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
	achines that have enabled (or disabled)) Click here to view	HTML	C:\Users\Public\Documents\ARKWE 8.x\Export\Builtin Domain Task
•				



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

r		
Scan Profile (Computers)		x
You can specify a computer list by using either the computers from the network. Or you may select sp		
Profile Name:		
Profile		
Select computers from network		
Select specific <u>W</u> indows version(s)		
Import list of computers from text file		
Import list of IP addresses from text file		
Enter Computer <u>N</u> ame (Domain\Server Name)		_
DISCOVERY\SP45	Add	
ADVENTURE/RD49	Add	
ADVENTURE/RD55		_
PATHFINDER\RD45	Remove	
		_
	<u>O</u> K <u>C</u> ancel	

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

Scan Profile (Computers)	
You can specify a computer list by using either the Import option or by selecti computers from the network. Or you may select specific versions of Windows	
Profile Profile ○ Select computers from network ④ Select specific Windows version(s) ○ Import list of computers from text file ○ Import list of IP addresses from text file	
Windows Versions Image: Select specific domains Image: Windows Vista Image: Select specific domains Image: Windows 2003 Server Image: Select specific domains Image: Windows 2000 Professional Image: Windows 2000 Server Image: Windows 2000 Server Image: Windows 2000 Server	
	cel

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

Scan Profile (Computers)
	y a computer list by using either the Import option or by selecting n the network. Or you may select specific versions of Windows.
P <u>r</u> ofile Name:	
Profile	
Select com	puters from network
Select species	cific <u>W</u> indows version(s)
Import list	of co <u>m</u> puters from text file
🔘 Import list	of IP addresses from text file
File C	:\Users\Administrator\Desktop\WorkStationsList.txt
	e should contain computer names in the format puter' with each entry <u>Click here to view a sample.</u>
	Import
	OK <u>C</u> ancel

- 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:

 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:

Sample - Computer List	— ×
research\rd1	*
research\rd2	
pathfinder\rd45	
	*

 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:

Entries Import	ed .	—
This window sho	ws the list of entries imported	l.
Host Name	Domain Name	
RD45	PATHFINDER	
RD49	ADVENTURE	
RD55	ADVENTURE	
		⊆lose

- 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

-		
Scan Profile (C	Computers)	×
	a computer list by using either the Import option or by selectin the network. Or you may select specific versions of Windows.	g
P <u>r</u> ofile Name:	Research Computers	
Profile		
🔘 <u>S</u> elect comp	outers from network	
💿 Select speci	ific <u>W</u> indows version(s)	
🔘 Import list o	of computers from text file	
Import list o	of IP addresses from text file	
File C:	Users\Administrator\Desktop\VorkStationsList.txt	
	should contain valid IP addresses with each entry in a separat <u>e to view a sample.</u>	e
	Import Verify Imported	
		el

- i. Select Import list of IP addresses from text file option.
- **ii.** 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:

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

—
*
-

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:

Entries Importe	Entries Imported					
This window show	vs the list of entries imported.					
IP Address	Host Name					
10.10.10.44	ADVENTURE\RD49					
		⊆lose				

- 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)?

	Too	lls Customize	F2				
	-	Filter	F3				
		Export	F7				
		E-mail					
	<u>s</u>	Scan Profiles Ma	anager	۲.	×	Computers	F9
lick	20	Configuration S	ettings		æ	Users and Groups	F10

to launch the Scan

Profiles Manager. The Scan Profiles Manager shows the list of Scan Profiles available.

📧 Scan Profiles Manager (Computers)				
You can setup Scan Profiles to scan a subset of computers in the network and save these profiles for repeated use.				
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.				
Database Servers	New			
Resource Serve				
Win2k11 Workstations	Edit			
	<u>D</u> elete			
	Preview			
About Scan Profiles 🔻	⊆lose			

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

- 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 offline 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 Scan Profiles (Computers) -

Apply Profile...

Clear Profile 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 from the application toolbar. This action will launch the Scan Profiles Manager (Users/Groups) dialog as shown below.

🚁 Scan Profile Manager (Users/Groups)				
You can setup Scan Profiles (Users/Groups) to scan a subset of users in servers and save these profiles for repeated use.				
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.				
Frequent Checks RestrictedUsers Roaming Users	<u>N</u> ew <u>E</u> dit <u>D</u> elete Preview			

 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 account	ts for which you would like to create a profile.	
Profile Name: Account Name:		
Add Accounts from domain\server:	B <u>r</u> owse and Select	
Selected Accounts:		
Account Name	Account Type	R <u>e</u> move
	<u> </u>	<u>C</u> ancel

- **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:

🌆 Scan Profile (L	lsers/Groups)		×
Select User/Gro	up Account(s)		
Select the User a	nd/or Group accounts for which you would	like to create a profile.	
Profile Name:	Sample Profile		
Add Accounts			
Account Name:	ADVENTURE\Adminuser	🖨 Add 🚺	
Accounts from	domain\server: Browse and Select	t	
Selected Accou	nts:		
Account Name	•	Account Type	Remove
			<u>O</u> K <u>C</u> ancel

🕭 Scan Profile (U	Jsers/Groups)	—
Select User/Gro	oup Account(s)	
Select the User a	nd/or Group accounts for which you would like to create a	profile.
Profile Name: Add Accounts -	Sample Profile	
Account Name:		Add
Accounts from Selected Accou		
Account Name	e Account Type	Remove
ADVENTURE\/		
adventure\sci	holes	
•	III	•
		OK Cancel

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

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

	Too	ls View Wi	ndow H	lelp					
		Customize	F2						
	T	Filter	F3					•	
		Export	F7						
	-	E-mail							
		Scan Profiles M	lanager	•	*	Computers	F9]	
Click	×0	Configuration	Settings			Users and Groups	F10	t a	lau
Click					1			"to	lau

launch the Scan

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

🕭 Scan Profile Manager (Users/Groups)	X				
You can setup Scan Profiles (Users/Groups) to scan a subset of users in servers and save these profiles for repeated use.					
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.					
Frequent Checks RestrictedUsers Roaming Users	<u>N</u> ew <u>E</u> dit <u>D</u> elete <u>P</u> review				
	<u>C</u> lose				

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)

- 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

Preview - RestrictedUsers		
Profile Name: RestrictedUsers		
Account Name	Account Type	
ADVENTURE\Administrator	User	
ADVENTURE\adminuser	User	
ADVENTURE\Hygiene Management	Global Group	
adventure\Scholes		
ADVENTURE\SM_79673cede89848	User	

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



- 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.

Built-in Reports - List of permissions for specif	Built-in Reports - List of permissions for specific users and groups on folders			
Step 2 of 3 : Select User/Group Account(Select user and/or group accounts for which ye		ns on files/folders.		
Enter account name :		👍 A <u>d</u> d to list 🛛 🕕		
Accounts from domain\server:	Browse and Select			
Accounts from Scan Profiles (Users/Groups):	Select a Profile	• ()		
Selected Accounts:				
Account Name	Account	: Туре	Remove	
			Reset	
•		•		
		Back Next	Close	

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:

Built-in Reports - List of permissions for speci	fic users and groups on fo	olders			-X
Step 2 of 3 : Select User/Group Account(Select user and/or group accounts for which y		rmissions on files/	'folders.		
Enter account name :			👍 A <u>d</u> d to list	0	
Accounts from domain\server:	B <u>r</u> owse and Se	lect			
Accounts from Scan Profiles (Users/Groups):	Frequent Scans	•	0		
Selected Accounts:					
Account Name	A	ccount Type			Remove
Adventure\adminuser Adventure\Alan Adventure\Alex Adventure\Michael					Reset
Builtin\Administrators	m			•	
			Back Ne	ext	Cļose

 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

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) (and groups from.	or a Scan Profile (Users/Groups) to retrieve available users
Report Name: List of permissions for specific u	sers and groups on folders
Enter account name :	Add to list
Accounts from domain\server:	B <u>r</u> owse and Select
Accounts from Scan Profiles (Users/Groups):	Select a Profile
Selected Accounts	
Account Name	Account Type Remove
	Reset
•	III •
	< <u>B</u> ack <u>N</u> ext> Close

➤ 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 u	sers and groups on folders		
Enter account name :	Add to lis	t 🕕	
Accounts from domain\server:	Browse and Select		
Accounts from Scan Profiles (Users/Groups): Selected Accounts	Frequent Scans 🔹 🕡		
Account Name	Account Type	Remove	
Adventure\adminuser			
Adventure\Alan		Reset	
Adventure\Alex			
Adventure\Michael			
Builtin\Administrators			
•	III •		
	< <u>B</u> ack <u>N</u> ex	t> Close	

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).



from the application toolbar. This action will

launch the Scan Profiles Manager (Shares) dialog as shown below:

🚁 Scan Profile Manager (Shares)	—		
You can setup Scan Profiles (Shares) to scan a subset of shares in servers ar profiles for repeated use.	nd save these		
This window lists available profiles. Click New to create a new profile. Click Edit to modify selected profile. Click Delete to delete a profile. Click Preview to view the contents of a profile.			
Frequent Scans Sample Profile1	<u>N</u> ew		
	<u>E</u> dit		
	<u>D</u> elete		
	Preview		
	<u>C</u> lose		

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 Shar folder paths from a text file.	e or Shared Folder. Click Add From to load the list of shares, Imp	port to import a	list of UNC
Profile Name:	Sample Profile		
Share/Folder UNC Path:		Ad <u>d</u>	
Folder Path			Add From
			Import
			Remove
		<u>o</u> k	<u>C</u> ancel

- 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 Shar folder paths from a text file.	e or Shared Folder. Click Add From to load the list of shares, Irr	port to import a	list of UNC
Profile Name:	Sample Profile		
Share/Folder UNC Path:	\\RD55\TestLocagroups	Ad <u>d</u>	
Folder Path			Add From
			Import
			Remove
		<u>o</u> k (<u>C</u> ancel

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:

Scan F Enter t folder p			t a list of UNC
Shar Fol	No Profile found. Configure using Scan Profiles Manager.> Omains Omain Controllers Omain Controllers Image: State of the stat		Add From Import Remove
	····□ \\RD49\F\$ ····□ \\RD49\G\$ OK C	ancel	

Scan Profiles (Shares)			X
Enter the full path of a Share folder paths from a text file.	e or Shared Folder. Click Add From to load the list of shares, Imp	port to import a	list of UNC
Profile Name:	Sample Profile]	
Share/Folder UNC Path:		Ad <u>d</u>	
Folder Path			Add From
\\RD49\Address \\RD49\ExchangeOAB			Import
\\RD49\NTFS Security M \\RD49\Test share folde	-		Remove
\\RD55\TestLocagroups			
		<u>o</u> k (<u>C</u> ancel

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

8.11 How to Manage Scan Profiles (Shares)?



to launch the Scan Profiles Manager (Shares). The

Scan Profiles Manager (Shares) shows the list of available profiles.

🛃 Scan Profile Manager (Shares)	x
You can setup Scan Profiles (Shares) to scan a subset of shares in servers an profiles for repeated use.	nd save these
This window lists available profiles. Click New to create a new profile. Click Ex selected profile. Click Delete to delete a profile. Click Preview to view the con	
Frequent Scans Sample Profile1	<u>N</u> ew
	<u>E</u> dit
	<u>D</u> elete
	<u>Preview</u>
	<u>C</u> lose

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)

- 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.

Preview - Frequent Scans 📃	3	
Profile Name: Frequent Scans]	
Share Name		
\\RD49\Address		
\\RD49\NTFS Bulk Share2		
\\RD49\NTFS BulkTest Share		
\\RD49\NTFS Security Manager		
\\RD49\Test share folder		
⊆lose		

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



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:

Built-in Reports - List of pe	ermissions for folders			X	
Step 2 of 2 : Select server(s) for Shared Folders-list 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.					
Share/Folder UNC Path:			Add		
Scan Profile (Shares):	Select a Profile	• ()			
Folder Path		Include sub-folders	Folder level	Add From	
				Import	
				Remove	
•	m		•		
Do not display folders	that have the same permissions as the parent fo	lder	Edit Folder Options]	
Include group member				J	
Include <u>S</u> ID					
-		<u>B</u> ack	Einish	Close	

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

Built-in Reports - List of permissions for folders Step 2 of 2 : Select server(s) for Shared Folders-list 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.						
Share/Folder UNC Path:			Add			
Scan Profile (Shares):	Frequent Scans	• (1)				
Folder Path		Include sub-folders	Folder level	Add From		
\\RD49\Address \\RD49\NTF5 Bulk Share2 \\RD49\NTF5 BulkTest Sh \\RD49\NTF5 Security Ma \\RD49\Test share folder	are anager	True True True True True	All All All All All	Import Re <u>m</u> ove		
Do not display folders Include group member: Include SID	that have the same permissions as the pa ship information	rent folder	Edit Folder Options			
		Ba	ck <u>F</u> inish	Close		

> 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

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:

🔀 Power Expo	rt - Built-ii	n Rep	oorts									×
Step 2 of 5	: Shared	d Fol	lder S	electio	on							
Enter the full of UNC folde default prop	r paths fro	om a te	ext file.3	Select a	a folder in					•		$\left \right\rangle$
Report	List of p	ermi	ssions	for fol	lders							
UNC Path:										Add		
Scan Profile	(Shares):	Se	ect a P	rofile			•	0				
Folder Path							Include s	ub-fold	Folder	level	Add	d From
												[mport
											F	temove
•					m							
folder	isplay folde roup memb				_	isions as t ide <u>S</u> ID	he parent	Ec	lit Folder	Options		
								< <u>B</u>	ack	Next>		Cļose

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

🔀 Power Export	: - Built-ir	n Reports					×
	Step 2 of 5 : Shared Folder Selection						
of UNC folder	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 I	List of p	ermissions for fo	olders				
UNC Path:						Add]
Scan Profile (S	ihares):	Frequent Scans		• ()			
Folder Path				Include sub-fold	i Folder le	vel 🔺	Add From
\\RD49\Addre	ess			True	All		Import
\\RD49\NTFS	Bulk Shar	e2		True	All	=	Tubore
\\RD49\NTFS	BulkTest	Share		True	All		Remove
\\RD49\NTFS	Security	Manager		True	All		
\\RD49\Test :	share fold	er		True	All	-	•
•						P.	
Do not dis folder	play folde	rs that have the sa	me permissions as t	he parent	<u>E</u> dit Folder C	ptions	
🔲 Include gro	oup memb	ership information	Include SID				
					< <u>B</u> ack	<u>N</u> ext>	Cļose

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:

ARKWE Uninstall Wizard	×
Welcome to ARKWE Uninstall Wizard This wizard helps you to deanup and uninstall ARKWE completely.	ò
This wizard will guide you through the steps to cleanup the files that are created by ARKWE application. Using this wizard you can: * Cleanup scheduled tasks. * Cleanup ARKWE application settings * Cleanup log files * Cleanup Scan Profiles created by ARKWE Scan Profile Manager * Uninstall ARKWE application	
< Back Next > Finish Ca	incel

Click Next to Proceed

2) Select required Cleanup Options as shown below:

ARKWE Uninstall Wizard ×
Step 1 of 2: Cleanup Options Cleaning up the information based on your selection
 Uninstall ARKWE application Remove all application files and uninstall ARKWE application from the machine. Uninstall ARKWE application and cleanup application settings Remove all application files and uninstall ARKWE application from the machine. Also deanup all scheduled tasks, log file, exported files and other reports settings. Delete entire ARKWE database
< Back Next > Finish Cancel

Click **Next** to Proceed.

3) Confirm the Cleanup and/or Uninstall Process.

ARKWE Uninstall Wizard
Step 2 of 2: Cleanup Process Cleaning up the information based on your selection
Click 'Finish' button to proceed with the deanup process or click 'Cancel' button to terminate the uninstall wizard.
< Back Next > Finish Cancel

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	Domain Controllers, 104				
About Built-in Reports, 51	Domains, 51, 170				
About Power Export, 109	Edit Task, 193				
About Scan Profiles (Computers), 179	Enterprise network planning personnel, 3				
About Scan Profiles (Users/Groups), 189 About System Info, 79	Error Control, 49 Error Log File, 6, 208				
Active Directory, 101, 102					
Additional E-mail Settings, 119, 156,	evaluation/trial, 4				
166, 175	Hardware, 87				
Additional Features, 95	HIPPA., 1				
Admin Report Kit for Windows	How to activate the software?, 4				
Enterprise, 1, 209	How to Apply Filters?, 96				
applet, 209	How to apply Scan Profiles				
Application Data, 208	(Computers)?, 187				
ARKWE, 1, 2, 3, 6, 96, 100, 101, 103, 104, 107, 108, 109, 110, 208, 209,	How to apply Scan Profiles (Users/Groups)?, 195				
211	How to create Scan Profiles				
Built-in Reports, 51, 67, 71, 75, 123, 124, 150, 160, 169, 196	(Computers)?, 180				
Create Task, 79	How to create Scan Profiles (Users/Groups)?, 189				
CSV, 109	How to customize fields?, 95				
data warehousing, 3	How to E-mail data?, 100				
Domain, 30, 169, 170	How to Export data?, 98				
Domain Admins, 104	How to find data in a report?, 104				

How to manage Scan Profiles (Computers)?, 185

How to manage Scan Profiles (Users/Groups)?, 193

How to Refresh data?, 98

How to scan specific servers in a domain?, 106

How to Uninstall ARKWE?, 209

How to view Built-in Permissions Reports, 51

How to view Built-in Reports for Domains?, 75

How to view Built-in Reports for Shares and Resources, 67

How to view Built-in Reports for Users and Groups, 71

How to view Current Status reports?, 93

How to view Display Configuration reports?, 90

How to view Domain information?, 30

How to view Environment Info reports?, 94

How to view Events information?, 46

How to view Hardware Configuration reports?, 87

How to view Internet Explorer Configuration reports?, 92

How to view Network Configuration reports?, 81

How to view Operating System and Hot Fixes reports?, 84

How to view Policies information?, 41

How to view Printer Configuration reports?, 86

How to view Service information?, 49

How to view Shares and Resources information?, 33

How to view Users and Groups information?, 37

Interactive Report, 187, 195

Internet Service Providers, 3

Intranets, 3

IP address, 184

IT infrastructure Managers, 1

LAN, 3

license key, 4, 5

MDB, 109

Microsoft Windows Network., 1

Operating System, 84

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		
Server-based Reports, 187, 188	Manager, 110		
Server-based Reports., 187	Technical Support, 6		
Shares and Resources, 33, 51, 67, 123,	TIFF, 109		
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,		
Standard Reports (Working with	160, 195		
Reports), 30	WAN, 3		
System Administrators, 1, 3	Windows network product developers, 3		
System Information, 79	Windows Servers, 3, 78		
System requirements, 2			