

QUICK START GUIDE

Unitrends BDR Quick Assessment

Instructions to Perform a Backup and Disaster Recovery Assessment

7/15/2020 3:55 PM

Contents

Overview of Unitrends BDR Quick Assessment Module	3
Perform a Unitrends BDR Needs Assessment	4
Create a Site	4
Start an Active Unitrends BDR Quick Assessment Project	5
Perform the Unitrends BDR Quick Assessment	7
Step 1 — Complete the Unitrends BDR Needs Worksheet	7
Step 2 — Run BDR Data Collector, then Import Scan	9
Step 3 — Complete Unitrends Backup Selection Preference Worksheet(OPTIONAL) \dots	10
Generating Reports	12
Appendices	.14
Pre-Scan Network Configuration Checklist	15
Checklist for Domain Environments	15
Checklist for Workgroup Environments	17
Unitrends "Quick" BDR Needs Assessment versus "Full" Assessment	19
Running the BDR Data Collector	20
Step 1 — Launch the BDR Data Collector	20
Step 2 — Configure the BDR Data Collector Network Scan	20
Step 3 — Configure the BDR Data Collector Network Scan	21
Step 4 — Configure the Local Domains	22
Step 5 — Configure the Network IP Address Range to be Scanned	22
Step 6 — Verify and Run the Scan	24
Step 7 — Monitor the Network Scan's Collection Progress	25
Step 8 — Complete the BDR Data Collector Network Scan Process	26
Importing the BDR Collector Generated Scan Data	26

Overview of Unitrends BDR Quick Assessment Module

The Unitrends BDR Quick Assessment is a powerful tool for much more than just sizing your customer's back-up requirements. Use it to get detailed information for upselling your services around the proper solution, and to discover issues related to backups that could cause loss of data in the event of a disaster. In addition, you can gather summary information on the servers and workstations on the network.

The software includes the **Network Detective Application**, the **BDR Data Collector**, and **Worksheets** used to collect BDR needs and set a BDR Solution Preference.

The Unitrends BDR Quick Assessment lets you:

- Quickly perform BDR Needs assessments to identify and expand BDR sales opportunities
- Identify the Risks associated with the prospect's current BDR solution that is in place to present the business impact of system downtime and recovery time
- Generate a BDR System Sizing specification

The process to create a Unitrends BDR Quick Assessment involves creating a **Site** and executing two simple assessment steps using Network Detective:

1. Run BDR Data Collector with Network Scan

The BDR Data Collector is wizard driven and takes just a few minutes of your time to set-up. The scan itself typically takes 45-60 minutes on a 50-user network on a single subnet. You can run this from any windows system on the network with domain administrator credentials. The collection runs automatically, so you don't you have to watch it the entire 45-60 minutes.

2. Complete the BDR Needs Worksheet and the Backup Selection Preference Worksheet which take less than a minute each.

Perform a Unitrends BDR Needs Assessment

Follow the steps below to begin your BDR Needs Assessment:

Create a Site

- Go to <u>https://www.rapidfiretools.com/nd</u> to download and install the **Network Detective application** on your workstation or laptop (do not install at your client's site). Then run Network Detective and login with your credentials.
- 2. Create a new **Site** by selecting the **New Site** option.

💽 Network Dete	ctive - v2.3	.1031			
				E	5
Home	Scans	InF	orm	Re	ports
		New Site	Import	Site	View 👻
HOME					
Active Sites					

3. Set the Site Name for the "Site" in Network Detective. Click OK to create the site.

New Site
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer. Site Name:
Customer A - Assessment
Ok Cancel

Start an Active Unitrends BDR Quick Assessment Project

1. From within the Site Window, click the Start button to start the Assessment.



2. Next, select the Unitrends BDR Assessment (Quick) option presented.

Network Detective Wizard
Select Assessment Type
What type of assessments are you performing at this site? (Check all that apply)
IT and Cloud Assessments:
 Network Assessment (Domain) Network Assessment (Workgroup) Security Assessment (Domain) Security Assessment (Workgroup) BDR Assessment (Quick) BDR Assessment (Full) Unitrends BDR Assessment (Full) Unitrends BDR Assessment (Full) Microsoft Cloud Assessment Other (Use for ad-hoc reporting. No checklist provided.)

- 3. Select the **Next** button to continue.
- 4. In the **Create New Assessment Window** presented, use the default **Label** presented OR assign the **Label** (name) for your **Assessment** project by typing the name of your **Assessment** in the **Label Name** field.
- 5. Select the Next button to Start your Assessment.
- 6. Select the Finish button to complete the creation of your Assessment project.
- 7. Once the new **BDR Assessment Project** is started, a "**Checklist**" is displayed in the **Assessment Window**.



This **Checklist** presents the "**Required**" and "**Optional**" steps that are to be performed during the assessment process. Throughout the assessment process, **Complete** the **Checklist Items** in the order presented.

Note: The successful completion of your Assessment is dependent on the completion of each Checklist item in the numerical order presented.

Important: Do not attempt to complete checklist items out of order. Doing so will cause you to produce an invalid assessment.



8. You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.

Continue to start your Unitrends BDR Needs Assessment.

Perform the Unitrends BDR Quick Assessment

Follow the steps in the order below to perform the Unitrends BDR Quick Assessment.

Step 1 — Complete the Unitrends BDR Needs Worksheet

1. To complete the Unitrends BDR Needs Worksheet, click on the selector on the left side of the InForm Bar located towards the bottom of the Assessment window to display the Unitrends BDR Needs Worksheet for selection.



- 2. Open the Unitrends BDR Needs Worksheet listed under the InForm Bar by clicking on the Unitrends BDR Needs Worksheet's name label. The Unitrends BDR Needs Worksheet window will be displayed.
- 3. Enter **Responses** in the **Response Field** for each **Topic** listed throughout the worksheet in order to document the **BDR** needs for your client.

ds BDR Needs Worksheet			- 0	×
quired Remaining A THide # Filter Topics T X Bulk Entry Ac	tions 🔻	Save	Close	
worksheet gathers information from you about the environment and existing BDR solution that cannot be gathered through automated scans.		Expand	I All Collap	se All
1 Backup Information (8 Dequired Demaining)				
r Backup information (o Required Remaining)				
1.1 Number of Employees				
How many employees do you have?				
Required Response	08	D	SW	
1.2 Local Backup Retention Does local backup retention need to be greater than 30 days?				
			la bal	
· · · · · · · · · · · · · · · · · · ·	U X		STT .	
4.3. Officie Description				
Does offsite retention need to be greater than 1 year? Typically, this is only required for compliance purposes.				
<pre>v</pre>		-	SIW	
			<u>ö</u> Ť	
1.4 Local Recovery				
Does local recovery require a machine to run on the appliance itself, or is a local virtual environment present to run individual				
recoveries?				
· · ·		D	SW	
1.5 Operating System				

Topics that require **Responses** are labeled with a **"Required"** tag next to the questions posed.

To document the "**responses**" to the Instructions/Questions presented in this worksheet:

Unitrande DDD Naade Workshoot		~
onitiends bork needs worksheet	,	~
11 Required Remaining Hide # Filter Topics T X Bulk Entry A	Actions 🔻 Save Close	
This worksheet gathers information from you about the environment and existing BDR solution that cannot be gathered through automated scans.	Expand All Collapse Al	
1 Backup Information (8 Required Remaining)		
1.1 Number of Employees How many employees do you have?	P	
Required Response	0 2 10 11	
1.2 Local Backup Retention	B	
Does local backup retention need to be greater than 30 days?		
×	0 2 🕫 🎬	

- A. Select and Review the "Topic".
- B. Review the **Topic Question** or **Instructions**. Instructions provide guidance and are not included in the reports.
- C. Enter a "Response" for each of the "Required" questions.
- D. Select the **Note** icon to enter any "**Notes**" relevant to the topic's response. (OPTIONAL)
- E. Select the **Respondent** icon and enter the name of individual that responded or provided information to respond to the topic's question or requirement in the **Response** field. (OPTIONAL)
- F. After completing the **BDR Needs Worksheet**, select the **Save** button to save your responses. Once your responses are saved, select the **Close** button to close the worksheet window.
- 4. After the **Unitrends BDR Needs Worksheet** has been completed, the **Checklist** will be updated to show that the **BDR Needs Worksheet** has been **Completed**.

	BDR Assessment (Quick)	33% Complete 1 Complete 2 Required 0 Optional Created 7/7/2016 Modified 7/7/201
^	Run BDR Data Collector with the Network Scan	Backup Selection Preference Worksheet
		•

Proceed to the next step below to start the BDR Scan Data Collection Process.

Step 2 — Run BDR Data Collector, then Import Scan

 On your customer's network, download and run the BDR Data Collector on any Window's system from <u>www.rapidfiretools.com/bdr</u>. Alternatively, you can bring the Data Collector to your customer's site and run from a USB drive.

8	BDR Data Collector	ĸ
Scan Type	Scan Type	
Scan Options	Select type of scans to perform	
Verify and Run	Select the type of BDR data collection to perform.	
Collection Progress	BDB Network Data Collector	
Finish	Collect network-wide data using remote protocols. Required for BDR Assessments	
Load Settings from File	BDR Local Computer Data Collector Collect data on the current computer. Typically, used to augment data collection when remote protocols are not available from this computer.	
Open Working Folder	(running on .NET CLR version 2.0.50727.8009) Next	Ì

2. Follow the steps outlined in <u>"Running the BDR Data Collector" on page 20</u> to perform the **BDR Network Data Collection**.

Note: WMI must be enabled within the network to run this scan.

3. After the **BDR Data Collector Scan** is complete, from your laptop or workstation, run the Network Detective application, click into the **Site**, and select the **Import**

Scan File option in the Assessment window to Import the Scan File into the Assessment.



After the BDR Collector Data Scan is finished, select **Import File** within the Network Detective BDR Assessment Window to select the scan data file and Import the file into the Assessment.

Step 3 — Complete Unitrends Backup Selection Preference Worksheet(OPTIONAL)

When you generate the Unitrends BDR Needs Analysis Report at the end of the assessment, you will be presented with a **recommend Unitrends Recovery Series product** for your BDR requirements. This OPTIONAL worksheet allows you to override the suggested Unitrends Model.

Note: You can skip this step and begin generating reports.

1. To complete the Unitrends Backup Selection Preference Worksheet, open the Backup Selection Preference Worksheet.



 The worksheet is listed under the InForm Bar located towards the bottom of the Assessment window. To open the worksheet, select the Unitrends Backup Selection Preference Worksheet's name label. The Unitrends Backup Selection Preference Worksheet window will be displayed.



3. In the **Response** field, select the **Unitrends BDR Solution** option override that you want to assign to this assessment.

Unitrends Backup Selection Preference Worksheet		- 🗆 X
0 Required Remaining Hide # Filter Topics Y X Butk Entry V	Actions 🔻	Save Close
Based Use suggested model MAX-2 MAX-4 MAX-2-54 MAX-464 MAX-4-64 MAX-84-64 MAX-8-64 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MAX-84 MSP-8001 MSP-8002 MSP-8005 MSP-8008 MSP-8018 MSP-8018 MSP-8019 MSP-8018 MSP-80105 MSP-80105 MSP-8005 MSP-8005 MSP-8005 MSP-80005 MSP-81005 MSP-81005 MSP-81005 MSP-81005	e model based on	Expand All Collapse All

Note: You can view more details about the available Unitrends Recovery Series appliances here: <u>https://www.unitrends.com/backup-appliance-models</u>

4. After completing the **Unitrends Backup Selection Preference Worksheet**, select the **Save** button to save your responses. Next, select the **Close** button to close this worksheet's window.

After the Unitrends Backup Selection Preference Worksheet has been completed, the Checklist will be updated to show that the Unitrends Backup Selection Preference Worksheet has been Completed.

Generating Reports

Note: This step is NOT performed at the client site or network. Network Detective should be installed on your workstations or laptop. Install Network Detective from https://www.rapidfiretools.com/nd if you have not already done so.

To incorporate your company's brand in the reports, use the custom Reporting Branding Preference features in Network Detective. To learn more about how to use the Report Branding Preference feature, refer to the Network Detective User Guide available at www.rapidfiretools.com/bdr.

Follow these steps to run the BDR Analysis Reports:

- 1. Run Network Detective and login with your credentials.
- 2. Then select the **Site**, go to the **Active BDR Assessment**, and then select the **Reports** link located in the center of the **Assessment Window** in order select the reports to be generated.
- 3. Then select which of the **Unitrends BDR Needs Assessment** reports that you want to generate.



4. Select the **Create Reports** button and follow the prompts to generate the reports you selected. You may be prompted to add information to the report to include for whom the report is prepared.

At the end of the report generation process, the generated reports will be made available for you to open and review.

The BDR Needs Assessment module can generate the following reports and assessment worksheets:

Report name	Description
Unitrends BDR Needs Analysis Report	Reporting showing analysis of the Backup/Disaster Recovery needs for an environment. It includes both discovered information regarding the storage needs of an environment, along with analysis of both onsite and offsite backup requirements.
Unitrends BDR PowerPoint	PowerPoint slide deck for use in presenting your finding from the BDR Needs Analysis with your client.
Unitrends BDR Needs Assessment Worksheets	All of the worksheets that were completed during an assessment can be generated. The generated worksheets will contain the Response input that was placed into each worksheet during the assessment process.

Appendices

Refer to the appendices listed below for the supplementary information referenced in this user guide:

Pre-Scan Network Configuration Checklist	
Checklist for Domain Environments	
Checklist for Workgroup Environments	
Unitrends "Quick" BDR Needs Assessment versus "Full" Assessment	19
Running the BDR Data Collector	20
Step 1 — Launch the BDR Data Collector	
Step 2 — Configure the BDR Data Collector Network Scan	
Step 3 — Configure the BDR Data Collector Network Scan	21
Step 4 — Configure the Local Domains	
Step 5 — Configure the Network IP Address Range to be Scanned	
Step 6 — Verify and Run the Scan	24
Step 7 — Monitor the Network Scan's Collection Progress	
Step 8 — Complete the BDR Data Collector Network Scan Process	
Importing the BDR Collector Generated Scan Data	

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation - and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

Note: You must have .NET 3.5 installed on machines in order to use all data collector and appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
	GPO Configuration for Windows Firewall (Inbound Rules)
	Allow <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall
	This includes the following rules:
	Windows Management Instrumentation (ASync-In)
	Windows Management Instrumentation (WMI-In)
	Windows Management Instrumentation (DCOM-In)
	Allow File and printer sharing to operate through Windows Firewall
	This includes the following rules:
	File and Printer Sharing (NB-Name-In)
	File and Printer Sharing (SMB-In)
	File and Printer Sharing (NB-Session-In)
	Enable <i>Remote Registry</i> "read only" access on computers targeted for scanning.

RapidFireTools*

Complete	Domain Configuration	
	Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.	
	Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.	
	Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:	
	 operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices to send ICMP echo reply messages in response to an ICMP echo request 	
	Note: ICMP requests are used to detect active Windows computers and network devices to scan.	
	GPO Configuration for Windows Services	
	Windows Management Instrumentation (WMI) • Startup Type: Automatic	
	Windows Update Service • Startup Type: Automatic	
	Remote Registry • Startup Type: Automatic	
	Remote Procedure Call • Startup Type: Automatic	
	Network Shares	
	 Admin\$ must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group) 	

Complete	Domain Configuration	
	3rd Party Firewalls	
	 Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. 	
	Note: This is a requirment for both Activity Directory and Workgroup Networks.	

Checklist for Workgroup Environments

Share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

Complete?	Workgroup Configuration	
	Network Settings	
	• Admin\$ must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan	
	• File and printer sharing must be enabled on the computers you wish to scan	
	 Ensure the Windows Services below are running and allowed to communicate through Windows Firewall: Windows Management Instrumentation (WMI) Windows Update Service Remote Registry Remote Desktop Remote Procedure Call 	
	 Workgroup computer administrator user account credentials. Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard. 	

Complete?	Workgroup Configuration
Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICM request messages and ICMP echo reply messages to be sent and received by computers and network devices. Windows firewall rules on Windows computers may need to be created/enable computer:	
	 operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices to send ICMP echo reply messages in response to an ICMP echo request Note: ICMP requests are used to detect active Windows computers and network devices to scan.

Unitrends "Quick" BDR Needs Assessment versus "Full" Assessment

The table below outlines the major differences between the **Quick** and **Full** BDR assessment.

Feature	Quick	Full
Scan Types	Network Only	Network and Local Computer
Unitrends Backup Product Custom Recommendation	1	1
Cloud Storage Opportunity Detection		✓
Cloud Application Usage Detection		✓
Non-published Local Attached Storage Detection		✓
Existing Backup Solution Evaluation		✓
RTO Calculator		1
Critical System Identification	Use default setting of servers as critical and workstations as not	Allows you to hand pick which systems are critical
Exclude Individual Volumes from Assessment		✓
Requires Completion of InForm Worksheets		1

RapidFireTools°

Running the BDR Data Collector

Prerequisite: The **BDR Data Collector** scan depends on the availability of WMI within the network environment being scanned. Please verify that WMI is enabled before proceeding with the steps below.

Step 1 — Launch the BDR Data Collector

The BDR Network scan is performed at your client's site. You can bring and run the BDR Data Collector from a USB drive, or, from any Windows system, visit the RapidFire Tools software download website (<u>https://www.rapidfiretools.com/nd</u>) and download and run the **BDR Data Collector** named **BDRDataCollector.exe**.

The **BDR Data Collector** is a self-extracting .ZIP file that does not install on the client computer.

To start the **BDR Data Collector**, right-click on the **BDRDataCollector.exe** and run **BDRDataCollector.exe** using the **RUN AS ADMINISTRATOR MENU** option. Use the **unzip** option to unzip the files into a temporary location and start the collector.

<u> </u>	BDR Data Collector	×
Scan Type	Scan Type	_
Scan Options	Select type of scans to perform	
Verify and Run	Select the type of BDR data collection to perform.	
Collection Progress	RDB Network Data Collector	
Finish	Collect network wide data using remote protocols. Required for BDR Assessments	
Load Sations from File	BDR Local Computer Data Collector Collect data on the current computer. Typically, used to augment data collection when remote protocols are not available from this computer.	
Open Working Folder	(running on .NET CLR version 2.0.50727.8009) Next	t

Step 2 — Configure the BDR Data Collector Network Scan

Starting the BDR Data Collector will present the following screen.

Select the **Next** button and the **Credentials** window will be presented.

<u>a</u>	BDR Data Collector	
🖌 Scan Type	Credentials	
Credentials	Please enter a username and password with administrative rights to connect to	
Local Domains	the local Domain Controller and Active Directory. If you are scenning a workgroup environment, enter credentials which can be added and a statisticate and a directivity of the statisticate of the statisti	
IP Ranges	access the individual workstellions as a local administrator. If in a domain, clicking the Next button will test a connection to the local	
Verify and Run	Domain Controller and Active Directory to verify your credentials.	
Collection Progress	Active Directory domain Workgroup (no domain)	
Finish My credentials If in a domain, please enter the Fully Qualified Domain Name (i.e., corp. myco. com instead of the shortened name - MYCD)		
	Username: (domain\user)	
	Password: •••••••	
	Domain Controller:	
	Back. Next	

Step 3 — Configure the BDR Data Collector Network Scan

The **Credentials** window will be displayed to enable you to enter the required administrative credentials necessary to access the network environment during the scanning process.

Enter the Credentials by performing these steps:

- 1. Enter a username and password with administrative rights to connect to a Domain Controller and Active Directory. If in a domain, clicking the **Next** button will test a connection to the a Domain Controller and Active Directory to verify your credentials.
- 2. Select the Next button.

At this point in the process, the **Local Domains** window will be presented.

<u>a</u>	BDR Data Collector
🖌 Scan Type	Local Domains
🖌 Credentials	Below is a list of the detected domains in the current forest of Active Directory.
Local Domains	Gather information for ALL the domains detected.
IP Ranges	Gather information for only the Domains and OUs selected below.
Verify and Run	
Collection Progress	
Finish	
	Expand All Collapse All Expand Selected Advanced Tree View
	Back Next

Step 4 — Configure the Local Domains

For most SMB networks, simply click **Next** to gather information from ALL Domains. For larger clients you may want to narrow the scope of the assessment. If so, select the Domains to gather information by performing these steps:

1. Select Gather information for only the Domains and OUs you select, and make your selections.

	Domain and OU Confirmation	-	×
ľ			
L			
L			
	OK Cancel]	

- 2. Select the **Next** button.
- 3. Confirm the Domain and OU when the **Domain and OU Confirmation** window is presented.
- 4. Select the **OK** button to confirm the Domain and OUs you have selected

Step 5 — Configure the Network IP Address Range to be Scanned

You may use the default **IP Range** presented and select the **Next button**, or define an **IP Range**.

<u>a</u>	8DR Data Collector		
🖌 Scan Type	IP Ranges		
Credentials	The following IP Ranges will be scanned. Use the "Reset to Default" button to		
Local Domains reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network.			
IP Ranges	Single IP or IP Range (example: 192.168.0.0-192.168.0.255)		
Verify and Run	10.0.0-10.0.7.255		
Collection Progress			
Finish			
	Reset to Default Import from Text File Clear All Entries		
	Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)		
	Back. Nest		

You can specify an IP Range by clearing the default IP address range entry detected within the network by selecting the **Clear All Entries** option.

2	BDR Data Collector - 1.8ETA.2016.06.10.01		
🖌 Scan Type	IP Ranges		
🖌 Credentials	The following IP Ranges will be scanned. Use the "Reset to Default" button to		
🖌 Local Domains	reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network and/e this machine.		
IP Ranges	192.168.0.0-192.168.0.255 Add		
Verity and Run			
Collection Progress			
Finish			
	Reset to Default Import from Text File Clear All Entries		
	Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)		
	Back Next		

Next, enter the **Starting and Ending IP Addresses** for the range(s) you want to scan in the IP range field using the following format:

Starting Address of IP Range Address<hyphen>Ending Address of IP Range.

Then select the **Add** link to add the IP Range you specified.

Note that you can add multiple IP ranges if you need to scan remote locations or multiple subnets.

<u>a</u>	BDR Data Collector		
🖌 Scan Type	IP Ranges		
🖌 Credentials	The following IP Ranges will be scanned. Use the "Reset to Default" button to		
 Local Domains 	reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network.		
IP Ranges	Single IP or IP Range (example: 192.168.0.0-192.168.0.255)		
Verify and Run	192.168.0.0-192.168.0.255		
Collection Progress			
Finish			
	Reset to Default Import from Text File Clear All Entries		
	Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)		
	Back. Next		

Note: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue. Then select the **Next** button.

The Verify and Run window will be presented.

Step 6 — Verify and Run the Scan

Select the folder that you want to store the scan data file in after the scan is completed. You may change the scan's **Output Assessment File Folder** location and **Basename** for the scan data.

BDR Data Collector					
🖌 Scan Type	Verify and Run				
🖌 Credentials	Ready to run the data collection. Select your output file location and basename.				
🖌 Local Domains	The final assessment file will be <folder>\<basename>.zip. Output Assessment File</basename></folder>				
🖌 IP Ranges	Folder: C:\download\8DR				
Verify and Run	Basename: BDRCollectorScan		.ZIP		
Collection Progress	Progress Comment (optional):				
Finish					
	Launch Pre-scan Analyzer				
Save Settings to File		Back	Start		

Enter any **Comments** and then select **Start**. The **Collection Progress** window will then be displayed as presented below.

Note: Prior to performing **Step 6** above, you can run the **Pre-Scan Analyzer**. **The Pre-Scan Analyzer** checks to verify that WMI is available. The **Pre-Scan Analyzer** can also identify any "**unreachable**" computers that should be turned on to be made accessible before you start the **BDR Collector Scan**, or identify **unreachable** computers that you need to later scan with the **Computer Data Collector**.

Step 7 — Monitor the Network Scan's Collection Progress

۵.	BDR Data Collector			
🖌 Scan Type	Collection Pro	Collection Progress		
🖌 Credentials	Active Directory:	1 of 124 computers finished		
🖌 Local Domains	Internet:	Performing internet speed tests (server 1 of 19)		
🖌 IP Ranges	Network:	0 of 101 finished.		
🖌 Verify and Run	Local Collector:	Getting optional features		
Collection Progress				
Finish				
		Cancel Data Collection Wrap It Up		
		Back Next		

The Network Scan's status is detailed in the Collection Progress window.

The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.

At any time you can **Cancel Data Collection** which will not save any data. By selecting **Wrap It Up** you can terminate the scan and generate reports using the incomplete data collected.

Upon the completion of the scan, the **Finish** window will be displayed.

<u>a</u>	BDR Data Collector
🖌 Scan Type	Finish
🖌 Credentials	To prepare the report, launch the Report Builder tool where you will import this
🖌 Local Domain:	collection file to generate reports.
🖌 IP Ranges	Collect the output hie from C:Vdownload/8DR
 Verify and Run 	Open Folder
Collection Progress	
Finish	
	Review Results Summary
	Done

Step 8 — Complete the BDR Data Collector Network Scan Process

The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.

Click on **Done button** to close the **BDR Data Collector** window. Note the location where the scan's output file is stored and gather the output zip file(s) for importing into the Network Detective application.

Importing the BDR Collector Generated Scan Data

The final step in this process is to import the data collected during the **BDR Network Scan** into the Network Detective application in the **Active** BDR needs assessment.

Perform the following steps to Import the Scan Data:

1. Click on the **Import Scans File** button in the Network Detective Assessment window.



The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP file produced by the **BDR Network Data Scan** into the **Assessment**.

2. **Browse** and **Select** the **BDR Network Scan** data file from the data collection you completed at your client's site.

Network Detective Wizard	x	
Select the Scan Results		
Select the resulting scan file or files. Multiple scan files or compressed archives can be selected in the file browser. Use CTRL-Click or SHIFT-Click to select multiple files.		
If you do not have a results file from a network scan, please download the Data Collector and complete a scan first.		
Browse		
Back Next Cancel		

Then click the **Next** button to import the scan data.

3. The Network Detective Merge window will be displayed.

RapidFireTools°

Network Deter	Network Detective Merger				
Files from the Con In order to merge	Files from the Computer Data Collector (CDF) need to be merged with the original Network Detective data file (NDF) before generating a report. In order to merge individual computers, you will need to specify a domain or workgroup for each CDF file.				
Custom Domain:	"Select CUSTOM in the dropdown	n list under "Merge Into	(ign "to use the Custom Domain.	iona) Befreiti	
Computer	Local Domain/Workgroup	OS	Run Date	Merge Into	
US-PC	WORKGROUP	Windows 7 Hom	8/24/2015 10:13:16 AM	[Use Workgroup] 🔻	
	(Merge Now 0	Dose		
				.i	

The success of the scan's import will be confirmed by the **Scan Archive Created** window being displayed.



4. Select the **Finish** button to complete the scan file import process.

After the **BDR Data Collector** scan file is imported into the assessment, the **Scans** section of the **Assessment Window** will be updated to list the **Network Scans** files imported into the assessment.

V		R	Scans Import Sca	in File	L Initiate External Scan Download Scans
		Scan(s)	Expand All	1 Files	06/12/2016 - 06/12/2016
	-	Network	Scans	1 Files	06/12/2016 - 06/12/2016
		- 😣	NetworkDetectiveSampleData.nd	f Completed	06/12/2016

In addition, the **Status and Check List** information indicators will be updated to present the assessment's current status. Refer to the figure to the right.



RapidFireTools^{*}