NETWORK DETECTIVE™

USER GUIDE

Unitrends BDR Full Assessment

Instructions to Perform a Backup and Disaster Recovery Assessment

7/15/2020 3:37 PM

Contents

Overview of Unitrends BDR Full Assessment Module

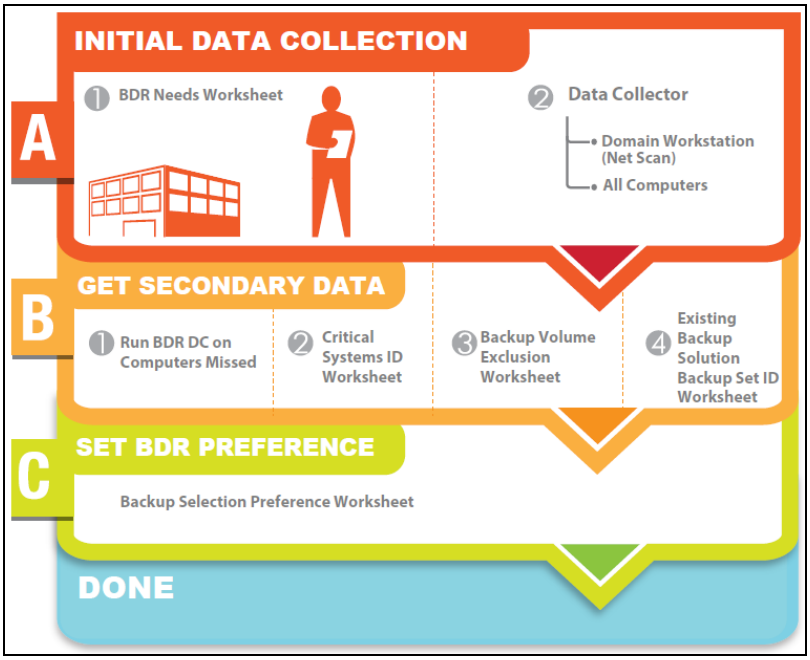
The **Unitrends BDR Full Assessment** is a powerful tool for much more than just sizing your customer's back-up requirements. Use it to get detailed information for upselling your services around the proper solution, and to discover issues related to backups that could cause loss of data in the event 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**, **Worksheets** used to collect "Secondary Data", and the **Push Deploy Tool** used to collect detailed local computer data.

The Unitrends BDR Full Assessmentlets 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
- Calculate Recovery Time Costs associated with prospect's current BDR to justify BDR system upgrades or improvements along with generating a BDR System Sizing specification

The process to create a BDR needs assessment involves creating a Site and executing three major assessment steps using Network Detective: A) BDR network data collection, B) Collecting computer endpoint data using the Push Deploy Tool, and C) Gathering secondary data necessary through the use of worksheets to further specify BDR needs.



Steps of a Unitrends BDR Full Assessment Using Network Detective

The Unitrends BDR Full Assessment is a complete assessment that includes automated data collection and worksheets.

- 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. The collection runs automatically, so you don't you have to watch it the entire 45-60 minutes.
- The **Push Deploy Tool** can be run at the same time as the BDR Data Collector and is used to gather detailed information from each computer on the network. It is also wizard driven, takes only a few minutes to setup, and then will take about an hour to scan a 50 system network. (In the event that systems are not accessible via WMI, a "local" collection can be manually run on each system that you wish to include in the assessment.)
- You will also fill-out the **BDR worksheets**, which take 5-15 minutes depending on the size of the network.

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

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

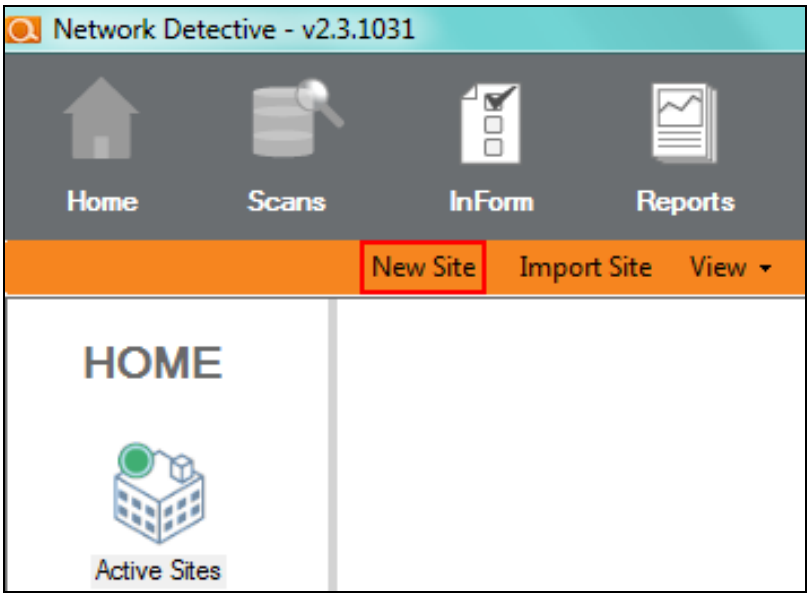
Feature	Quick	Full
Scan Types	Network Only	Network and Local Computer
Unitrends Backup Product Custom Recommendation	✓	✓
Cloud Storage Opportunity Detection		✓
Cloud Application Usage Detection		✓
Non-published Local Attached Storage Detection		✓
Existing Backup Solution Evaluation		✓
RTO Calculator		✓
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		✓

Perform a Unitrends BDR Needs Assessment

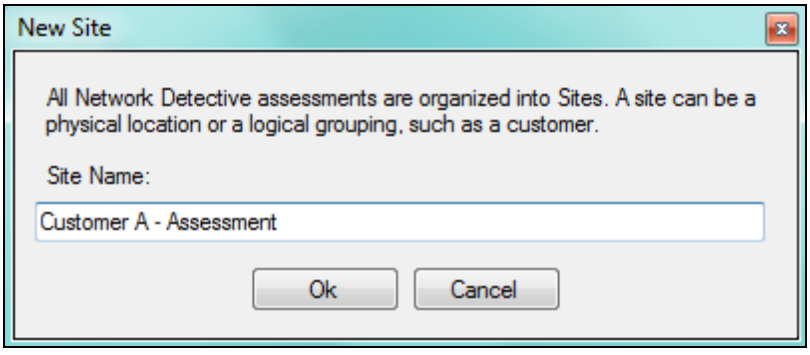
Follow the steps below to begin your BDR Needs Assessment:

Create a Site

1. Go to https://www.rapidfiretools.com/nd 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.



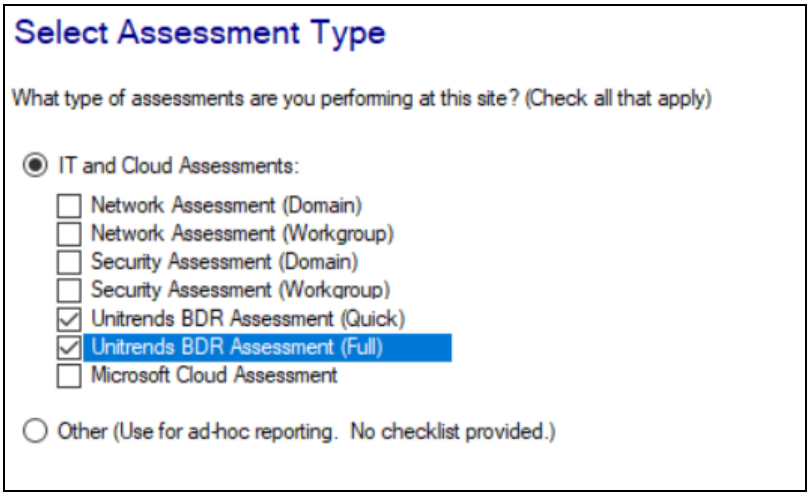
3. Set the **Site Name** for the "**Site**" in Network Detective. Click **OK** to create the site.



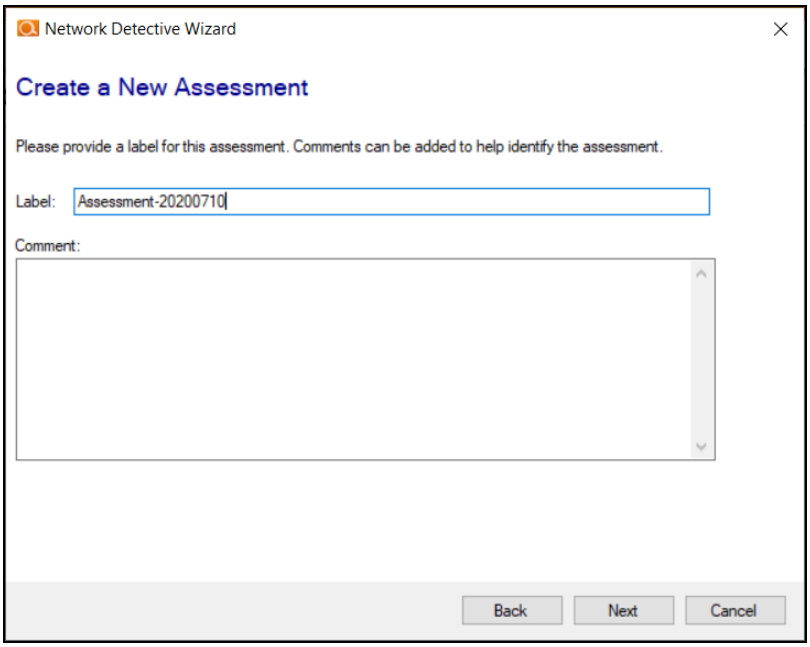
Start an Active Unitrends BDR Full Assessment Project

1. From within the Site Window, select the **Start** button that is located on the far right side of the window to start the Assessment.

2. Next, select **Unitrends BDR Assessment (Full)** presented.

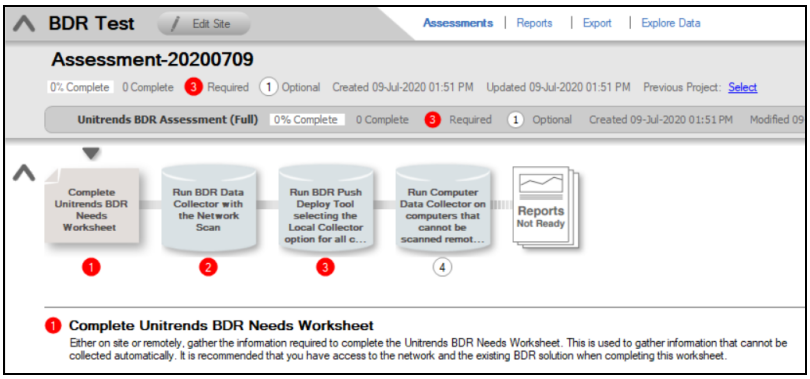


3. Select the **Next** button to continue.
4. In the Create New Assessment Window presented, use the default Label presented OR assign the Label (name) for your Assessment project by typing the name of your Assessment in the Label Name field.



5. Select the **Next** button to Start your Assessment.
6. Select the **Finish** button to complete the creation of your Assessment project.

   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.

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

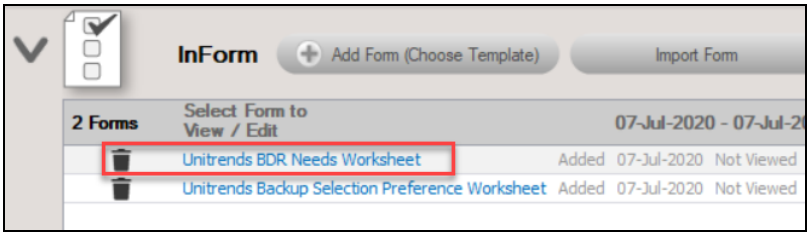
Perform "Full" BDR Needs Assessment

Follow the steps in the order below to perform the "Full" BDR Needs Assessment.

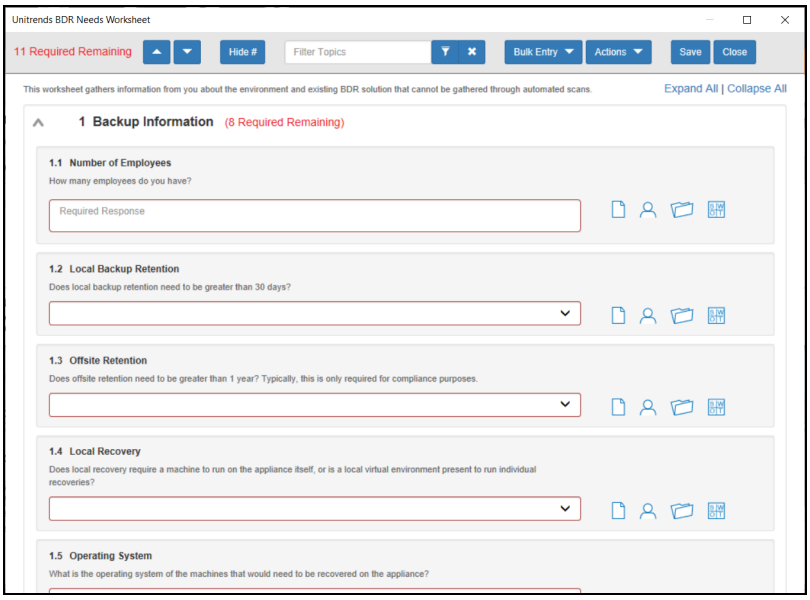
Important: If you perform the steps out of order, your assessment and reports may not work correctly.

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.

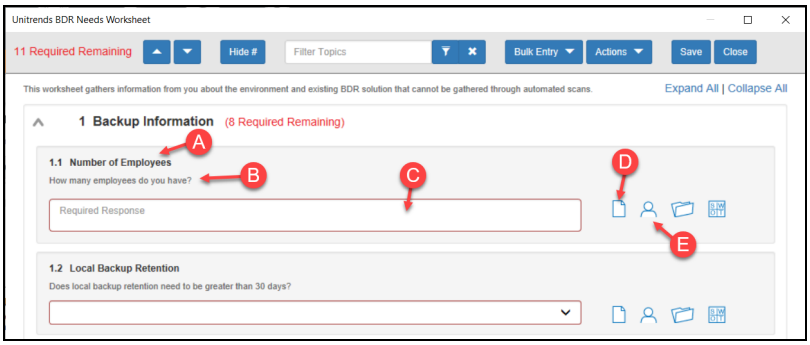


2. **Open** the **Unitrends BDR Needs Worksheet** listed under the **InForm Bar** by clicking on the **Unitrends BDR Needs Worksheet's** name label. The **Unitrends BDR Needs Worksheet** window will be displayed.
3. Enter **Responses** in the **Response Field** for each **Topic** listed throughout the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



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:



A. Select and Review the "**Topic**".

B. Review the **Topic Question** or **Instructions**. Instructions provide guidance and are not included in the reports.

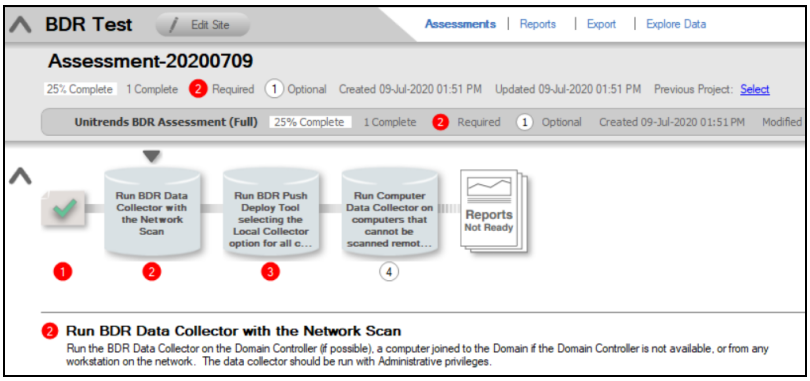
C. Enter a "**Response**" for each of the **"Required"** questions.

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 **Unitrends 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.

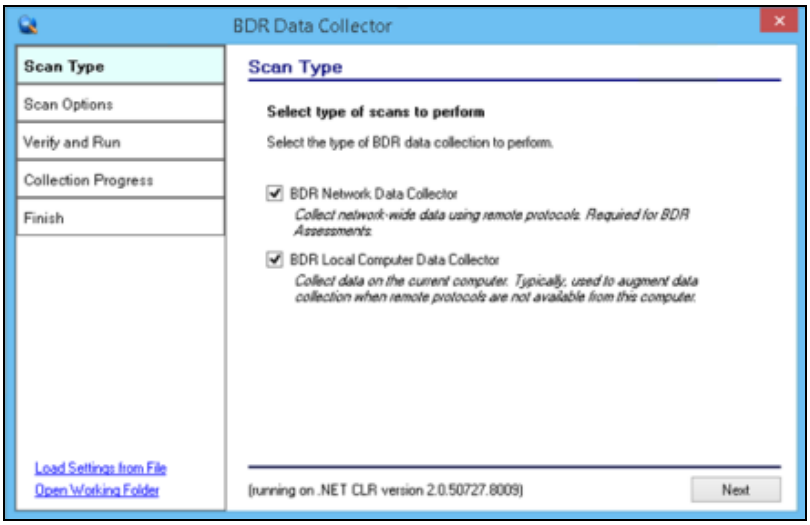
4. After the **Unitrends BDR Needs Worksheet** has been completed, the **Checklist** will be updated to show that the **Unitrends BDR Needs Worksheet** has been **Completed**.



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

Step 2 — Run BDR Data Collector using Network Scan and Import Scan

1. Download, install, and run the BDR Data Collector from https://www.rapidfiretools.com/nd.

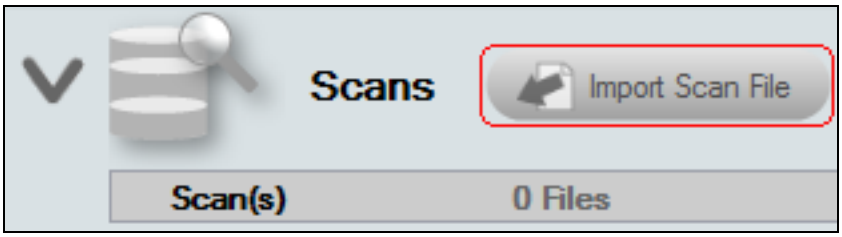


2. Follow the steps outlined in "Running the BDR Data Collector" on page 32 to perform the BDR Network Data Collection.

> **Note:** To run this scan, WMI must be enabled within the network. See "Pre-Scan Network Configuration Checklist" on page 28 for complete information.

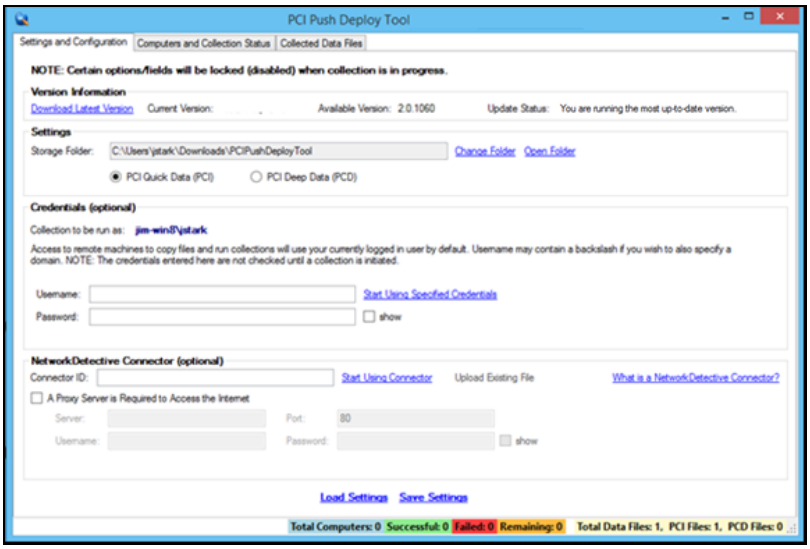
3. After the BDR Data Collector Scan is complete, select the **Import Scan File** option

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



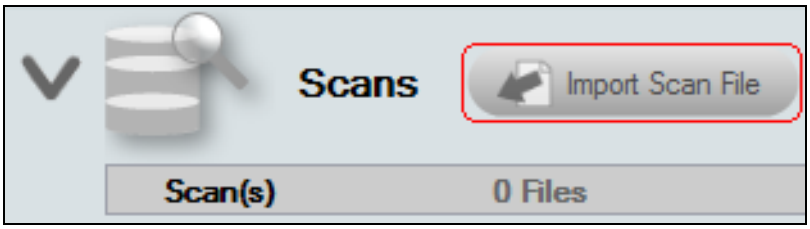
Step 3 — Run Push Deploy Tool Selecting the Local Collector to Scan Local Computers

1. Visit https://www.rapidfiretools.com/nd to download, and install the BDR Push Deploy Tool on a computer within the Network you are assessing.
2. Run the BDR Push Deploy Tool to Initiate the BDR Push Local Computer Data Scan. Note: WMI must be enabled within the network to run this scan.



3. Follow the steps outlined in "Using the BDR Push Deploy Tool to Collect Local Computer Scan Data" on page 42 to perform scans and data collection on local computer endpoints and import the scan results into the Assessment.
4. After the Push Deploy Local Computer Data Scan is complete, select the **Import Scan File** option in the Assessment window to Import the scan results into the

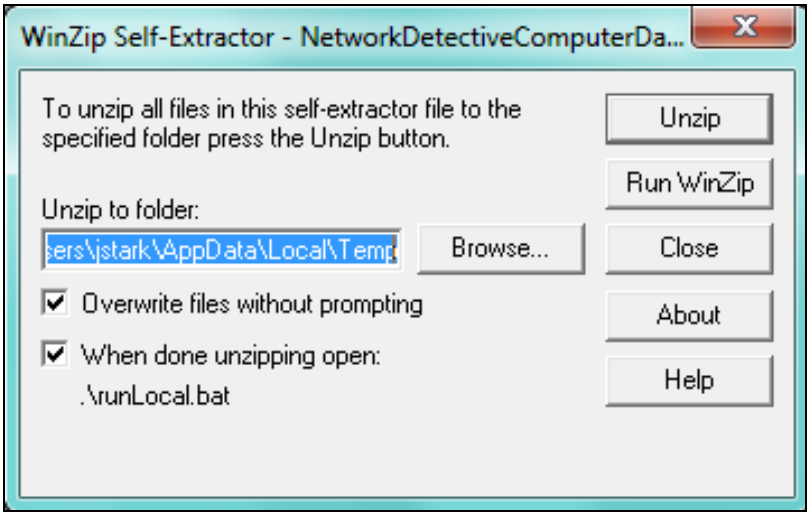
Assessment.



Step 4 — Run Computer Data Collector on Computers that cannot be Scanned Remotely (Optional)

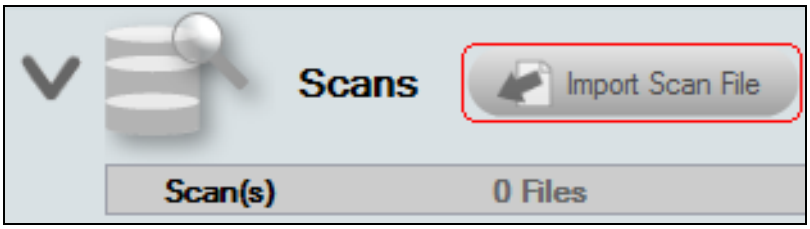
In this optional step, you can scan computers that you couldn't access using the Push Deploy Tool. This might include computers not connected to the network, or that could not be accessed on the network because of security restrictions. To perform this step:

1. Download, install, and run the **Computer Data Collector** from https://www.rapidfiretools.com/nd .



2. Run the Computer Data Collector Tool to Initiate a Local Computer Data Scan on a single computer.
3. Follow the steps outlined in "Using the Computer Data Collector to Scan Unreachable Computers" on page 50 to perform scans and data collection on local computer endpoints and import the scan results into the Assessment.
4. After the Computer Data Collector generated Local Computer Data Scan is complete, select the **Import Scan File** option in the Assessment window to Import

the scan results into the Assessment.

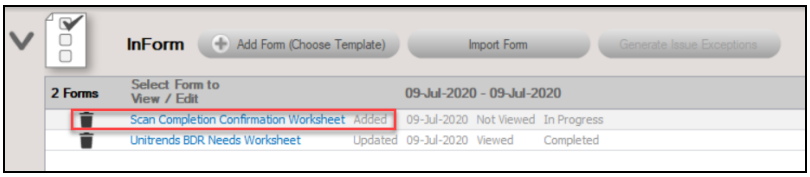


Step 5 — Confirm that Data Collection is Complete using the Scan Completion Confirmation Worksheet

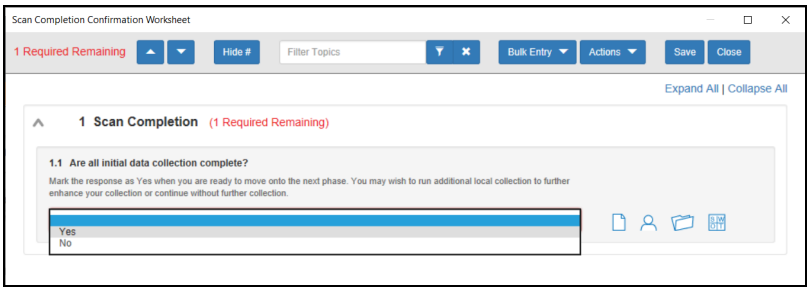
In this step, confirm that you've collected all of the data you want before you move forward. It's important to be sure you've completed all of the scans you want, because the next phase of the assessment relies on your scan data.

After you have performed all required data collection and are ready to move forward, open and mark this worksheet as complete.

1. To complete the Scan Completion Confirmation Worksheet, click on the  selector on the left side of the InForm Bar located towards the bottom of the Assessment window to display the Worksheet for selection.
2. Open the **Scan Completion Confirmation Worksheet** listed under the InForm Bar by selecting the Scan Completion Confirmation Worksheet's name label.

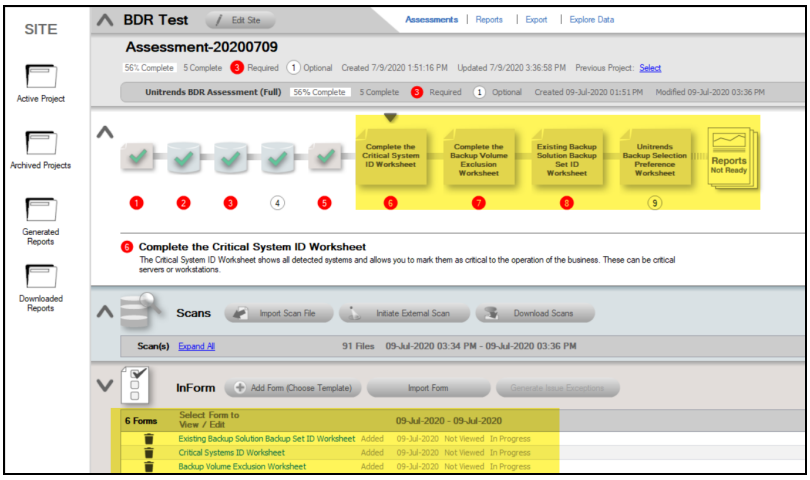


The Scan Completion Confirmation Worksheet window will be displayed.



3. If the BDR Collector Scan and all local computer scans have been performed and Imported into the Assessment, then select the “Yes” Response to confirm that the scans are complete.
4. After completing the Scan Completion Confirmation Worksheet, select the Save button to save your response. Then select the Close button to close the worksheet’s window.

   After the Scan Completion Confirmation Worksheet has been completed, the Checklist will be updated to show that this worksheet has been Completed. After the completion of this worksheet, new steps will be added to the Checklist that require additional worksheets be completed.

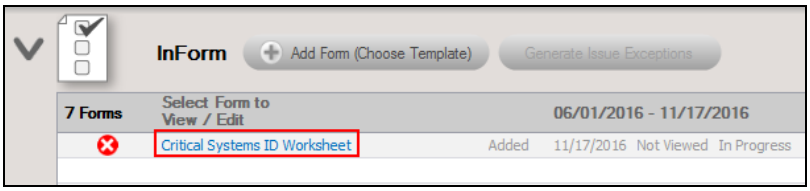


These additional worksheets will be accessible for editing and completion in a list located under the InForm bar at the bottom of the Assessment Window.

Step 6 — Complete Critical System ID Worksheet

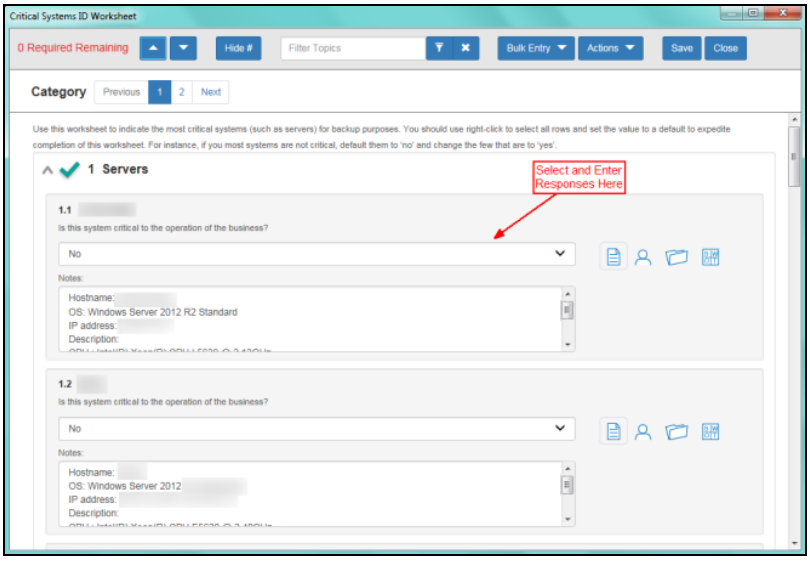
The **Critical Systems ID Worksheet** shows all detected systems and allows you to mark them as critical to the operation of this business. These systems can be either servers or workstations.

1. To complete the **Critical System ID Worksheet**, open the Critical System ID Worksheet listed under the InForm Bar located towards the bottom of the Assessment window by selecting the Critical System ID Worksheet’s name label.



The Critical System ID Worksheet window will be displayed.

2. Enter Responses in the Response Field for each Topic Question listed throughout the worksheet's Category pages in order to document the BDR needs for your client.

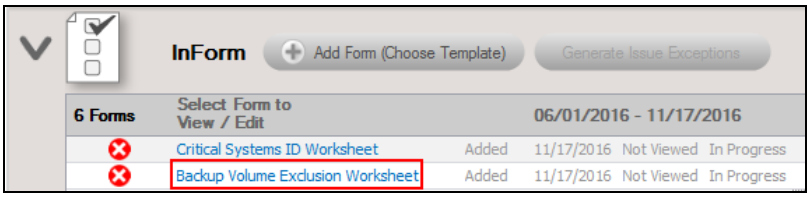


3. Select each Category page within the worksheet to assign Responses all of the questions associated with the servers or workstations identified within the Network.

To save time completing this worksheet, use the Bulk Data Entry feature detailed in . Use the Bulk Data Entry feature to set all of the responses to Topic Questions in the worksheet's to the "No" Response. Then, one by one, set the Response to "Yes" only for the Computers that are deemed as Critical to the business.

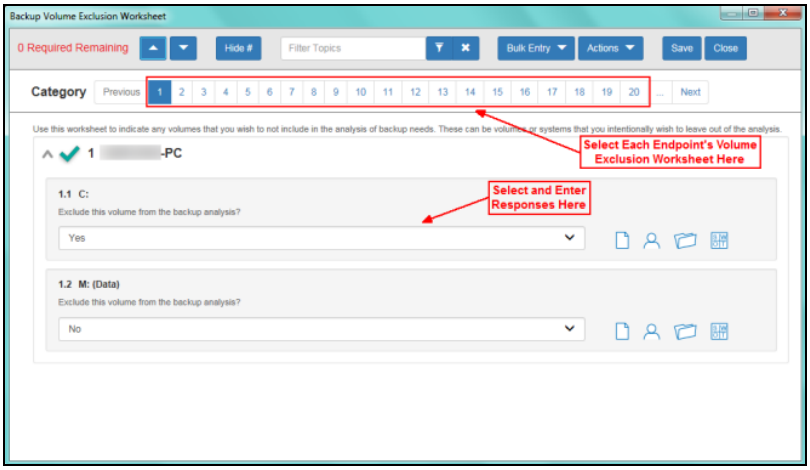
Step 7 — Complete Backup Volume Exclusion Worksheet

This worksheet lists all volumes by computer and allows you to identify volumes to exclude from the analysis. By default, no volumes are excluded, but you may use this worksheet to identify some volumes (such as backup file drives) that are not to be included.



2. Open the Backup Volume Exclusion Worksheet listed under the InForm Bar located towards the bottom of the Assessment window by selecting the Backup Volume Exclusion Worksheet's name label.

   The Backup Volume Exclusion Worksheet window will be displayed.



3. Select each available Category page within the worksheet to assign responses to the questions posed about the need to include identified drive volumes for each of the servers and workstations identified within the Network.

4. Enter Responses in the Response Field for each Topic Question listed throughout the worksheet in order to document the BDR needs for your client.

The Default Responses in this worksheet are set to “No” in order to save you time in completing this worksheet. Select the “Yes” Response for computer volumes that are to be excluded.

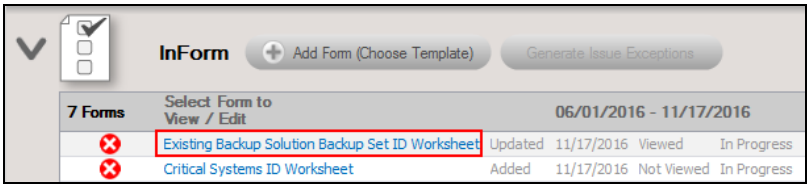
5. After completing the Backup Volume Exclusion Worksheet, select the Save button to save your responses. Then select the Close button to close the worksheet’s window.

   After the Backup Volume Exclusion Worksheet has been completed, the Checklist will be updated to show that the worksheet has been Completed.

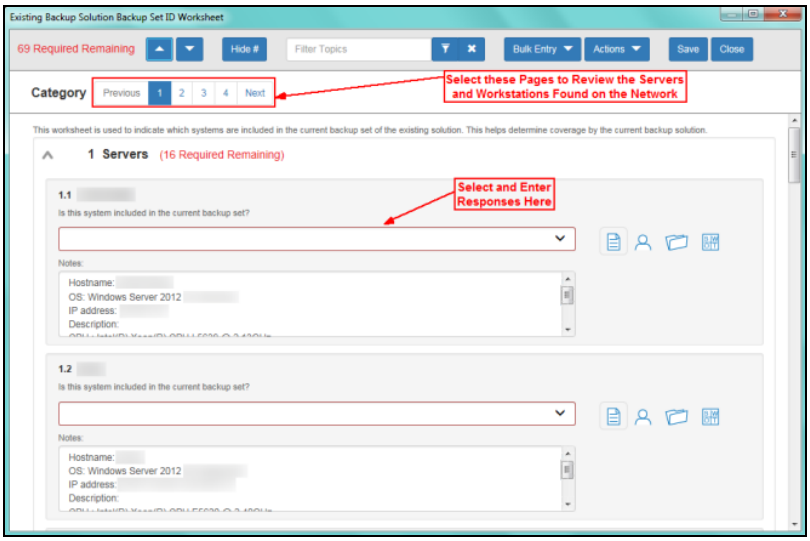
Step 8 – Complete Existing Backup Solution Backup Set ID Worksheet

This worksheet allows you to identify which systems are in the current backup set within the existing backup solution that is in place.

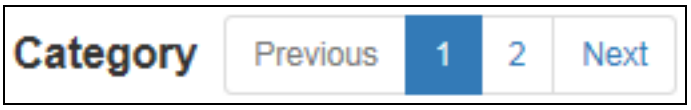
1. To complete the **Existing Backup Solution Backup Set ID Worksheet**, open the Existing Backup Solution Backup Set ID Worksheet listed under the InForm Bar located towards the bottom of the Assessment window by selecting the Existing Backup Solution Backup Set ID Worksheet’s name label.



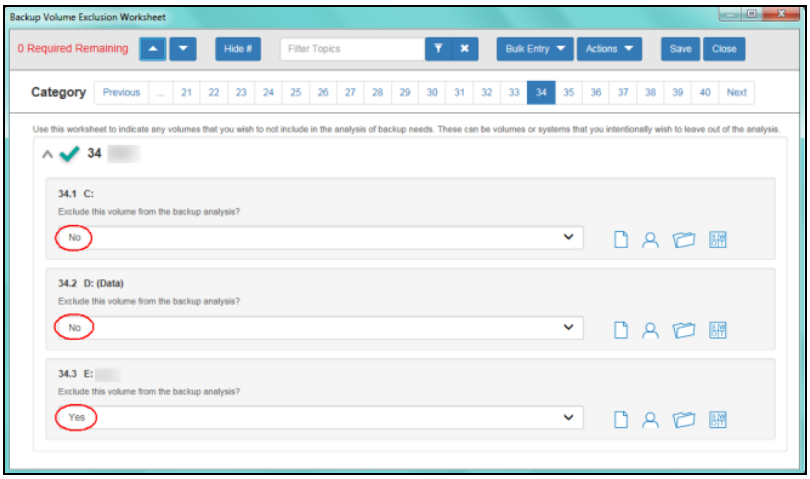
2. The Existing Backup Solution Backup Set ID Worksheet window will be displayed.



3. Select each Category page within the worksheet to assign responses to the questions associated with the servers or workstations identified within the Network.



Enter Responses in the Response Field for each Topic Question listed throughout the worksheet in order to document the BDR needs for your client.



To save time completing this worksheet, use the Bulk Data Entry feature detailed in "Completing Worksheets and Surveys" on page 56. Use the Bulk Data Entry feature to set all of the answers to Topic Questions in the worksheet's to the "No"

Response. Then, one by one, set the Response to "Yes" only for the Computers that are included in the currently implemented backup solution's Backup Set.

4. After completing the Existing Backup Solution Backup Set ID Worksheet, select the Save button to save your responses. Then select the Close button to close the worksheet's window.

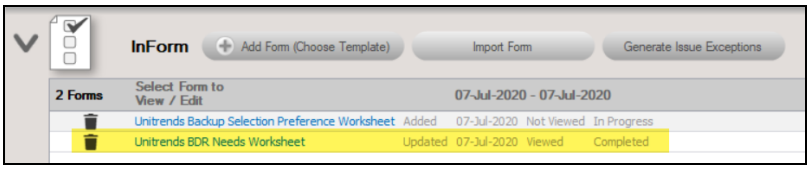
   After the Existing Backup Solution Backup Set ID Worksheet has been completed, the Checklist will be updated to show that the Existing Backup Solution Backup Set ID Worksheet has been Completed.

Step 9 — Complete Unitrends Backup Selection Preference Worksheet (OPTIONAL)

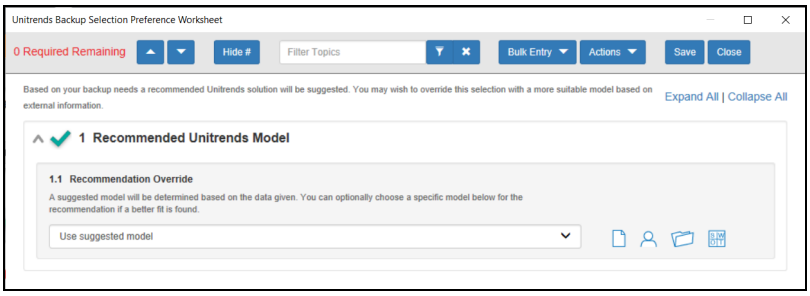
When you generate the Unitrends BDR Needs Analysis Report at the end of the assessment, you will be presented with a recommend Unitrends Recovery Series product for your BDR requirements. This OPTIONAL worksheet allows you to override the suggested Unitrends Model.

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

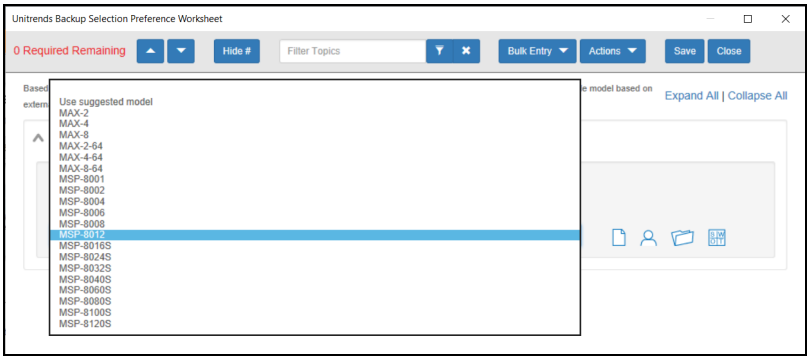
1. To complete the **Unitrends Backup Selection Preference Worksheet**, open the **Backup Selection Preference Worksheet**.



2. 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.



> **Note:** You can view more details about the available Unitrends Recovery Series appliances here. https://www.unitrends.com/wp-content/uploads/Recovery-Series-Backup-Appliances-DataSheet.pdf

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**.

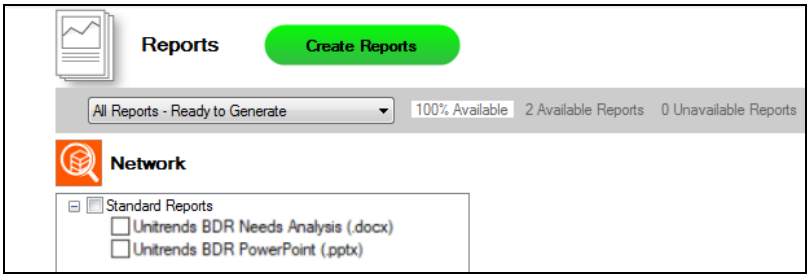
Generating Reports

> **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

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 *Windows Management Instrumentation (WMI)* 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 *Remote Registry* “read only” access on computers targeted for scanning.

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 *Internet Control Message Protocol (ICMP)* 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) adminstrator user account credentials for entry into the scan settings wizard.

Complete?	Workgroup Configuration
☐	Enable the *Internet Control Message Protocol (ICMP)* 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.

Running the BDR Data Collector

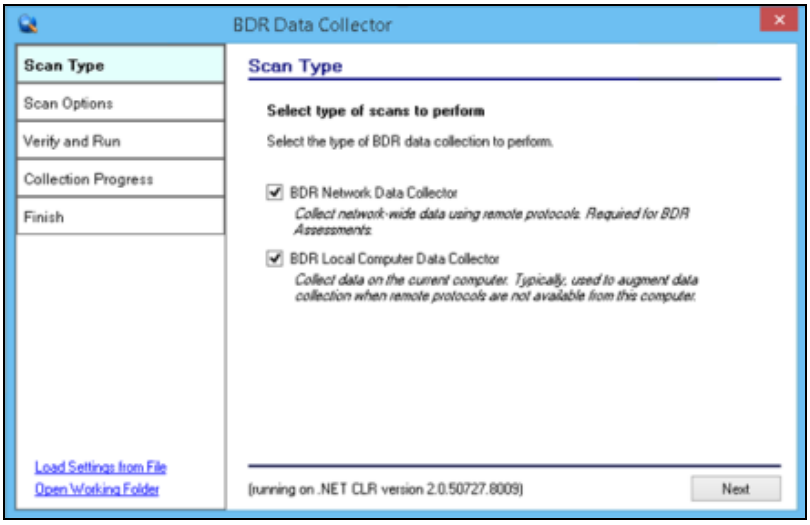
Prerequisite: The **BDR Data Collector** scan depends on the availability of WMI within the network environment being scanned. Please verify that WMI is enabled before proceeding with the steps below.

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 (https://www.rapidfiretools.com/nd) 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.

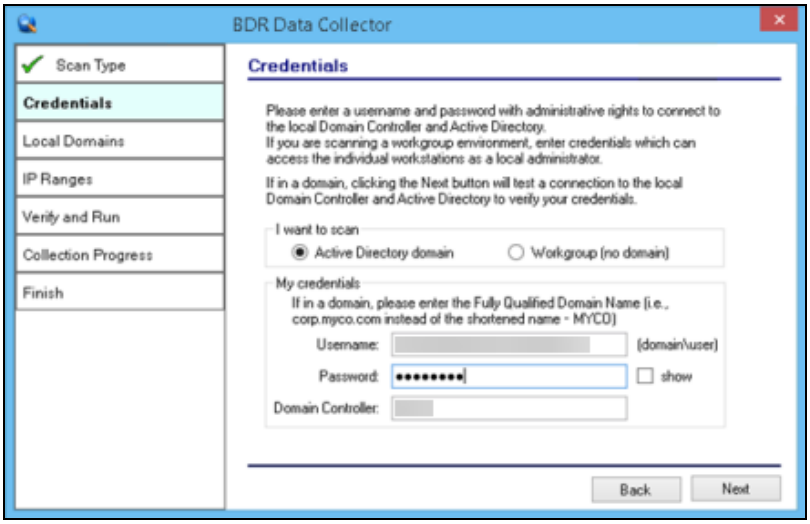
To start the **BDR Data Collector**, right-click on the **BDRDataCollector.exe** and run **BDRDataCollector.exe** using the **RUN AS ADMINISTRATOR MENU** option. Use the **unzip** option to unzip the files into a temporary location and start the collector.



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.



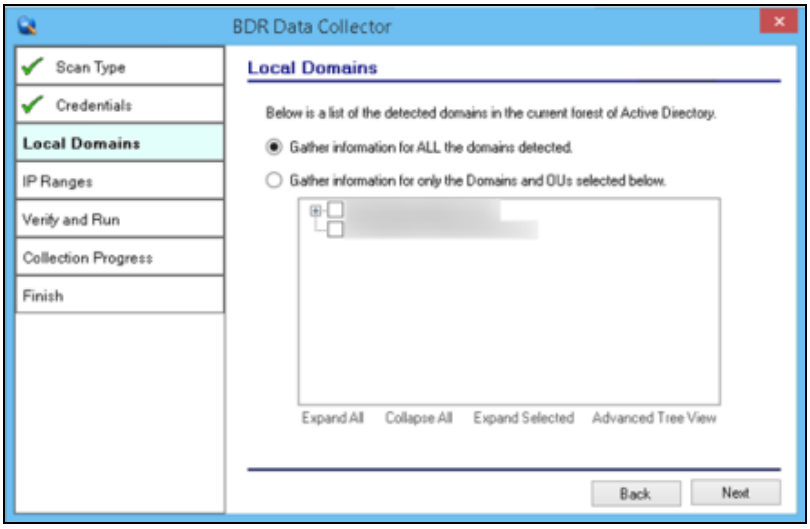
Step 3 — Configure the BDR Data Collector Network Scan

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.

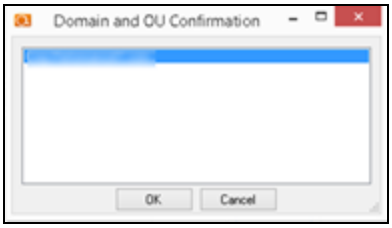
At this point in the process, the **Local Domains** window will be presented.



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:

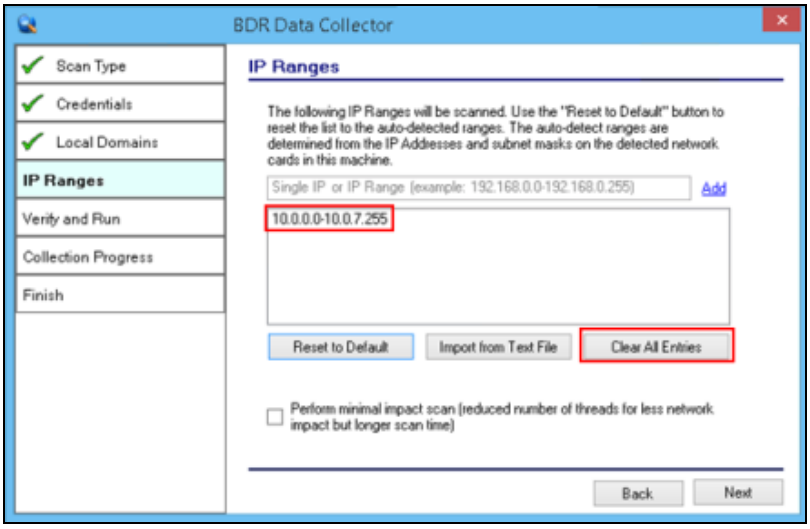
1. Select Gather information for only the Domains and OUs you select, and make your selections.



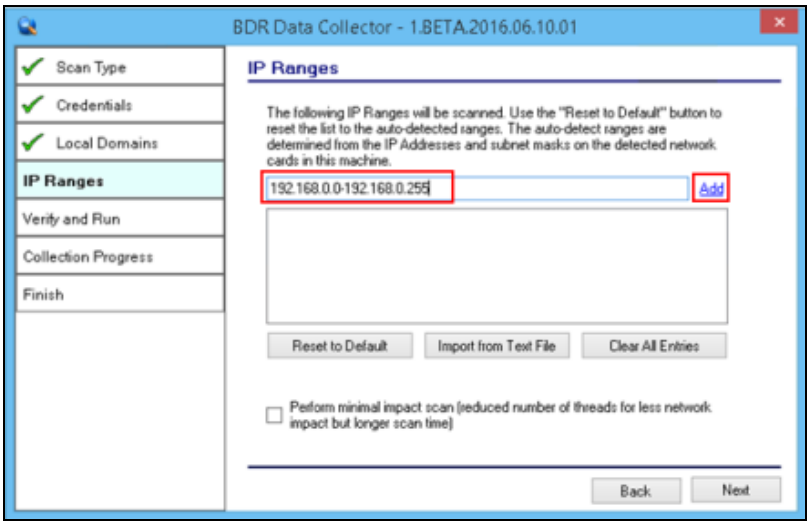
2. Select the **Next** button.
3. Confirm the Domain and OU when the **Domain and OU Confirmation** window is presented.
4. Select the **OK** button to confirm the Domain and OUs you have selected

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**.



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.

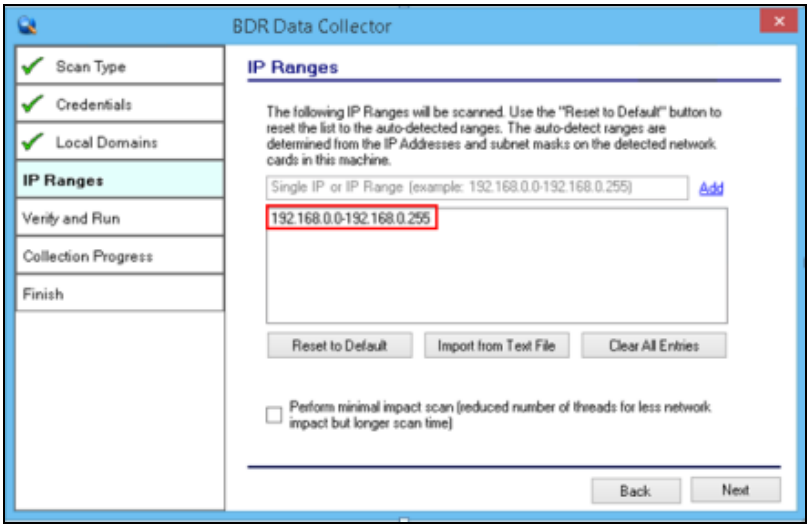


Next, enter the **Starting and Ending IP Addresses** for the range(s) you want to scan in the IP range field using the following format:

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.

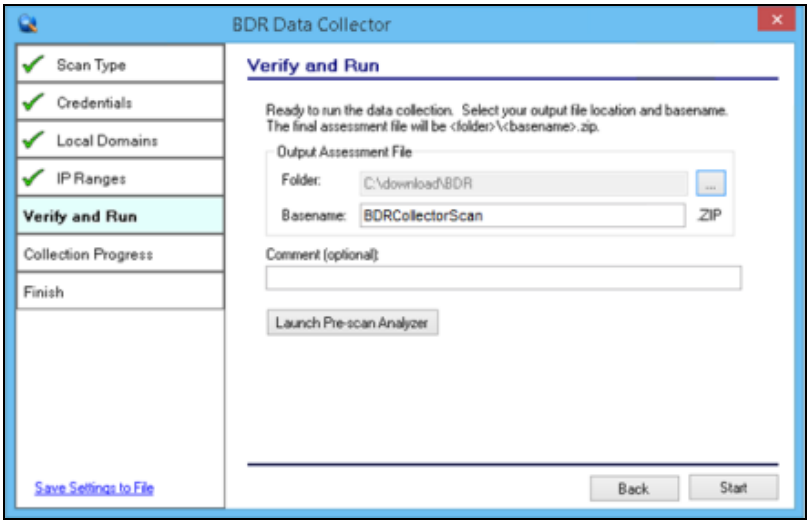


Note: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue. Then select the **Next** button.

The **Verify and Run** window will be presented.

Step 6 — Verify and Run the Scan

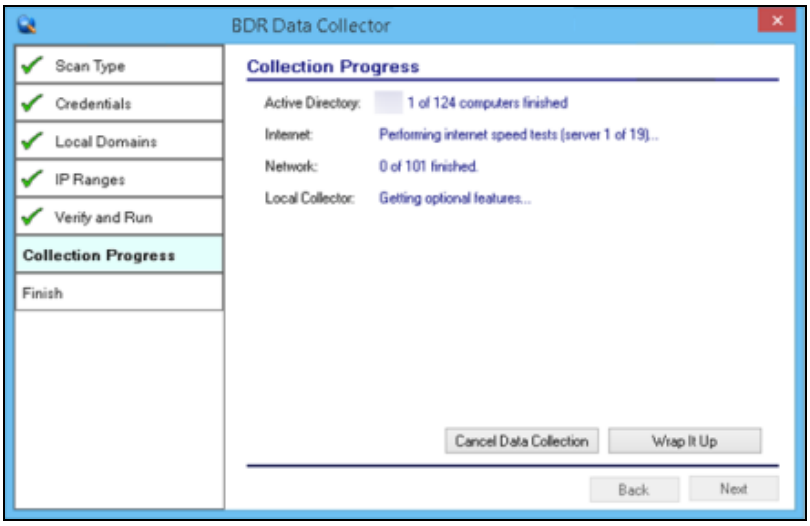
Select the folder that you want to store the scan data file in after the scan is completed. You may change the scan's **Output Assessment File Folder** location and **Basename** for the scan data.



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

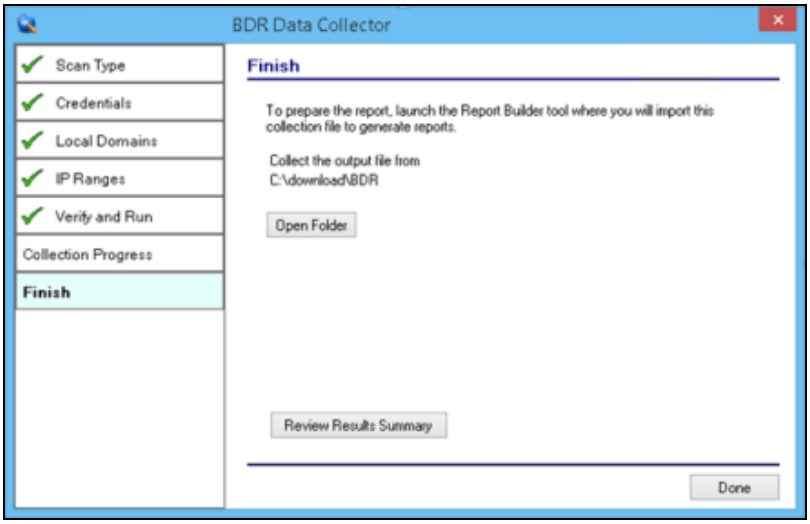


The **Network Scan's** status is detailed in the **Collection Progress** window.

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.



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**.

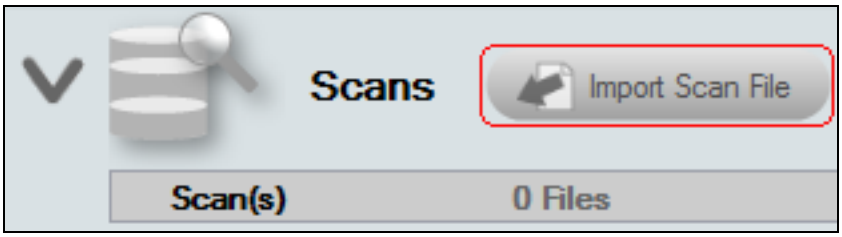
Click on **Done button** to close the **BDR Data Collector** window. Note the location where the scan's output file is stored and gather the output zip file(s) for importing into the Network Detective application.

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.

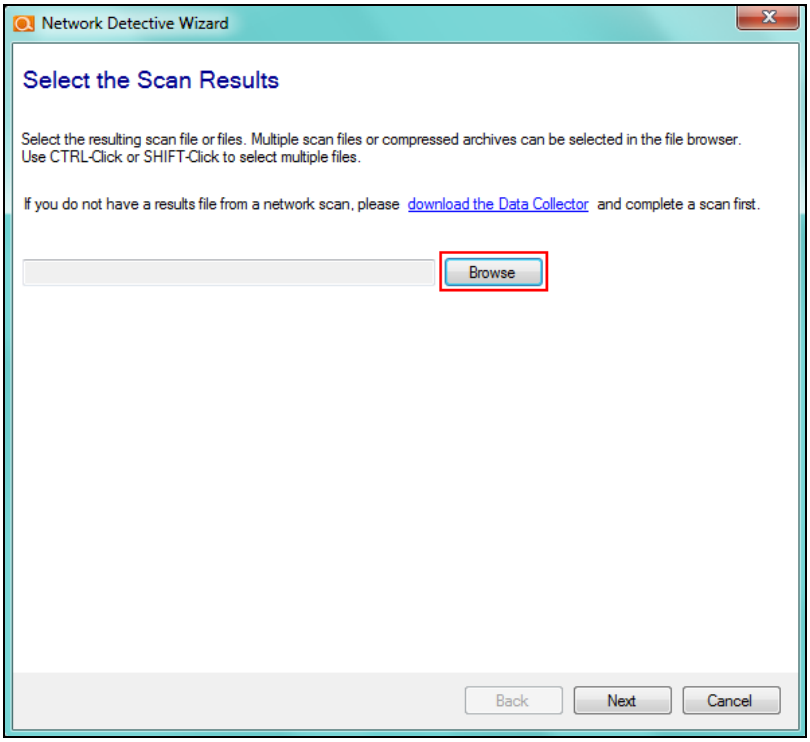
Perform the following steps to Import the Scan Data:

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



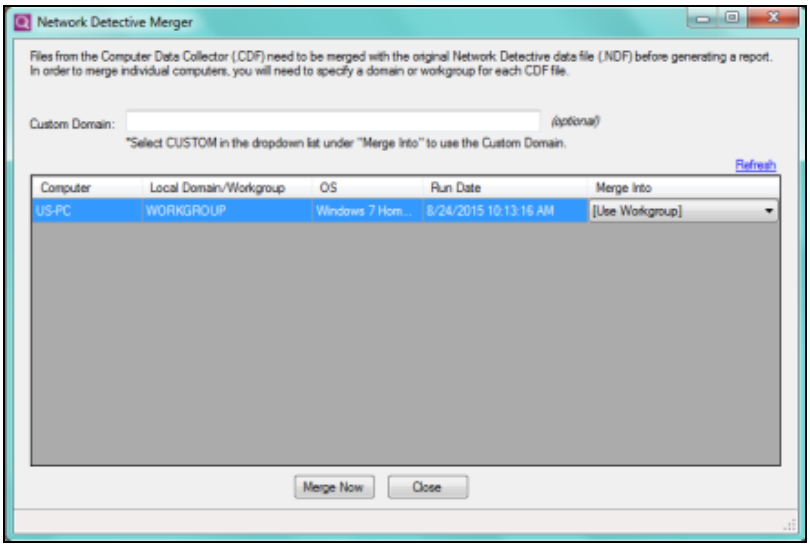
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP file produced by the **BDR Network Data Scan** into the **Assessment**.

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



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

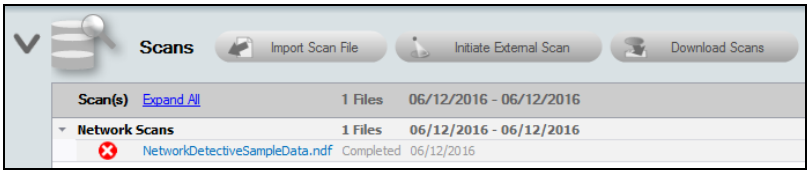
3. The **Network Detective Merge** window will be displayed.



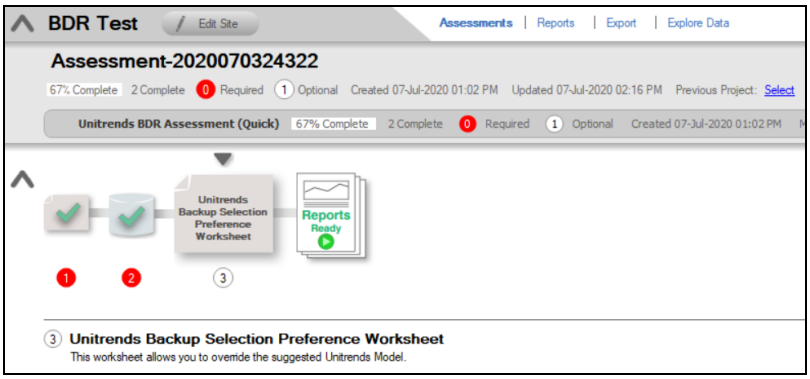
The success of the scan's import will be confirmed by the **Scan Archive Created** window being displayed.

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.



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.



Using the BDR Push Deploy Tool to Collect Local Computer Scan Data

The **BDR Push Deploy Tool** 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. See "Pre-Scan Network Configuration Checklist" on page 28 for a complete list of requirements.

Running the BDR Push Deploy Tool to Perform Local Computer Scans

The BDR Assessment Push Deploy Tool pushes the Local Data Collector to machines in a specified IP range, the local scans are executed on each computer, and then each computer scan file is saved to a specified directory (which can also be a network share). This directory (i.e. folder) is defined during the set-up of the Push Deploy Tool based scan.

The benefit of the tool is that a local scan can be run simultaneously on each computer within the network from a centralized location. The Push Deploy Tool is used to reduce or eliminate the need you to spend time at each computer within the network to run a local computer scan.

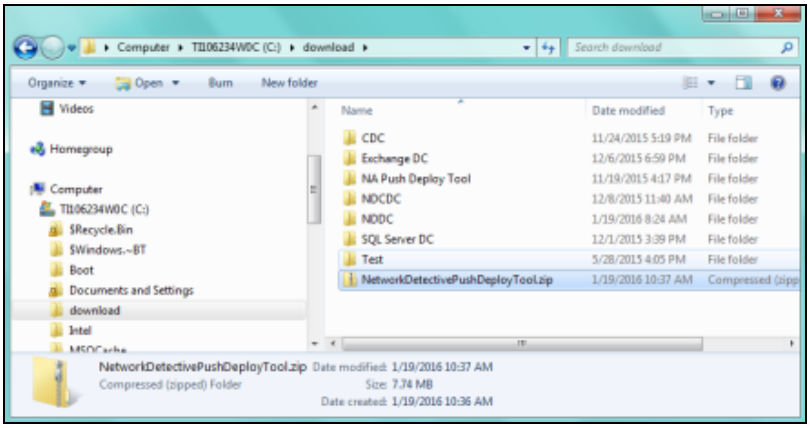
The output files (.CDF files) from the local scans can either be:

1. stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.
2. automatically uploaded to the RapidFire Tools secure cloud storage area using the Client Connector (a Network Detective add-on) and later downloaded from the secure cloud storage area directly to the Network Detective application for use in report generation.

To use the BDR Assessment Push Deploy Tool to perform local scans for computers within a network, please follow the steps detailed below.

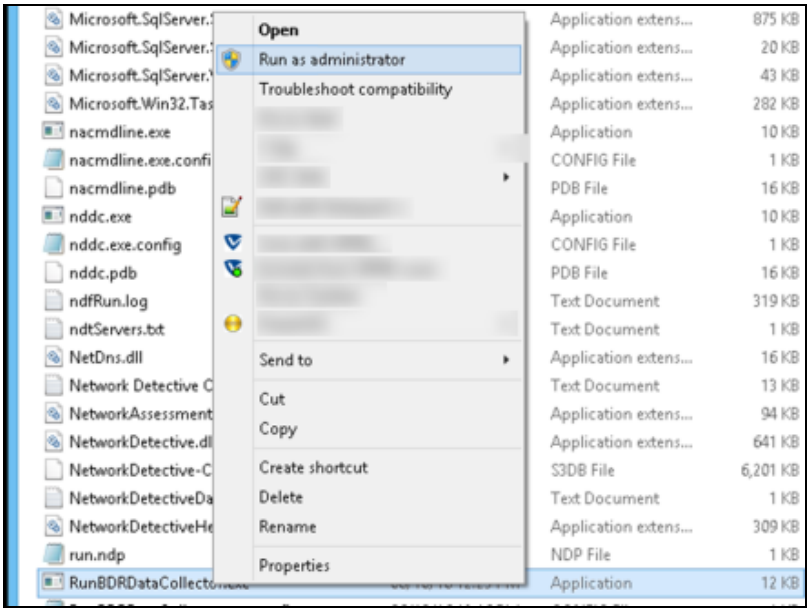
Step 1 – Download and Run the BDR Needs Assessment Push Deploy Tool

To perform a local computer scan, download the BDR Push Deploy Tool named BDRPushDeployTool.zip from the RapidFire Tools download page at https://www.rapidfiretools.com/nd.

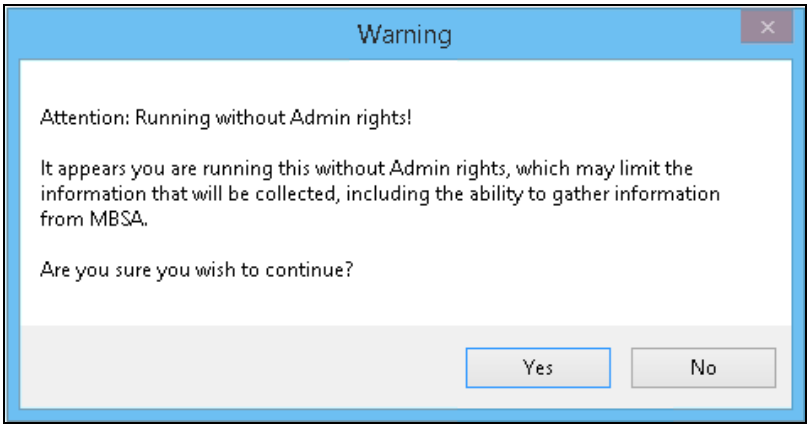


Then extract the contents of the BDR Push Deploy Tool .ZIP file to any machine on the target network or to a USB drive for use.

Within the folder named BDRPushDeployTool that was created by the .ZIP file extraction, right-click and run BDRPushDeployTool.exe using the **RUN AS ADMINISTRATOR** option.



If you do not run the BDRPushDeployTool.exe as an administrator, you will see the following Warning message.



Step 2 – Configure BDR Assessment Push Deploy Tool to Perform Local Computer Scan

Starting the BDR Assessment Push Deploy Tool will present the following window.

First, set the “I want to collect” option to be Computer Data (.CDF).

Step 3 – Set the Storage Folder Location for the Local Computer Scans Collected

Set the Storage Folder location used to store the scan data collected from the computers scanned.

> **Note:** This Storage Folder location can be located on a network share drive to centralize scan file storage.

If the individual performing the BDR Assessment Push Deploy Tool-based scans is logged into the network using Domain Administrator credentials, then the need to enter credentials as part of configuring the Push Deploy Tool scans is optional.

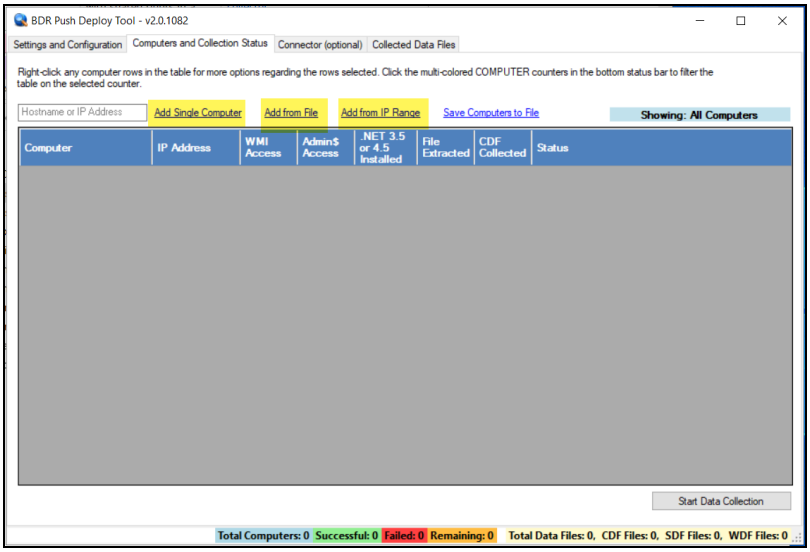
Step 4 – Enter User Name and Password Credentials

If the entry of credentials is required, then type in the administrator level Username and Password Credentials necessary to access the local computers on the network to be scanned.

Next, select the Computers and Collection Status tab.

Step 5 – Define the IP Address Range of the Computers to Scanned

The **Computers and Collection Status** window allows you to:

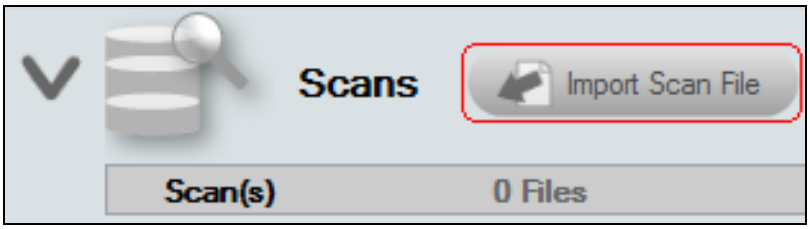


- Add (computers) from IP Range that are to be scanned
- Add a Single Computer to be scanned
- Add (computers) from File that are to be scanned
- Or to Save Computers to File in order to export a list of computers to be scanned again in future assessments

Methods for the Set-up Process Used to Configure Computers to be Scanned

As previously referenced, there are three methods to creating/adding a list of computers to be scanned by the Push Deploy tool. These methods are explained below.

Importing the Local Computer Scan Data into the BDR Needs Assessment



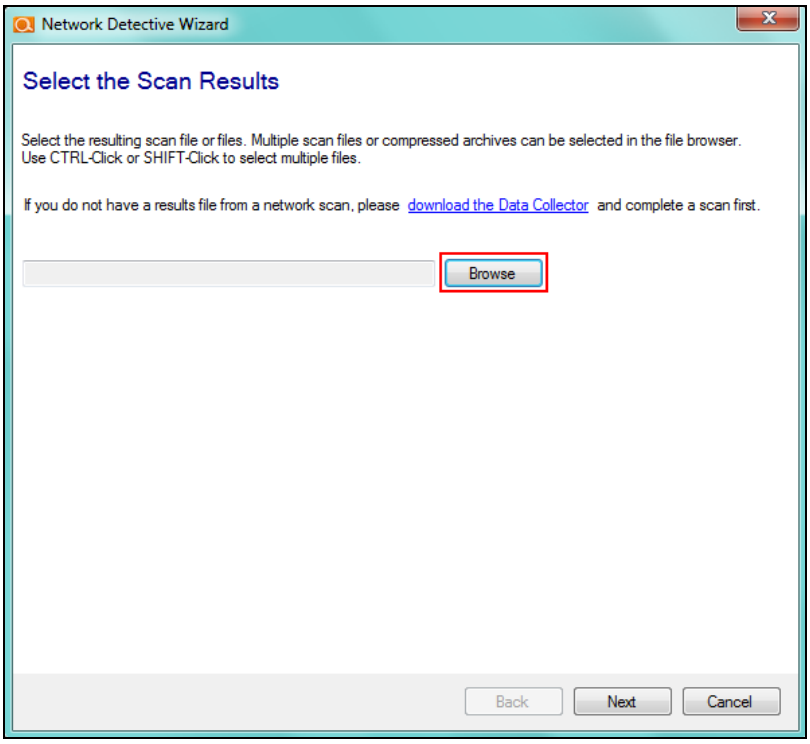
The final step in this process is to import the Local Computer Scan data collected during the Push Deploy Tool Scan into the Active BDR needs assessment.

Perform the following steps to Import the Local Computer Scan Data files:

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

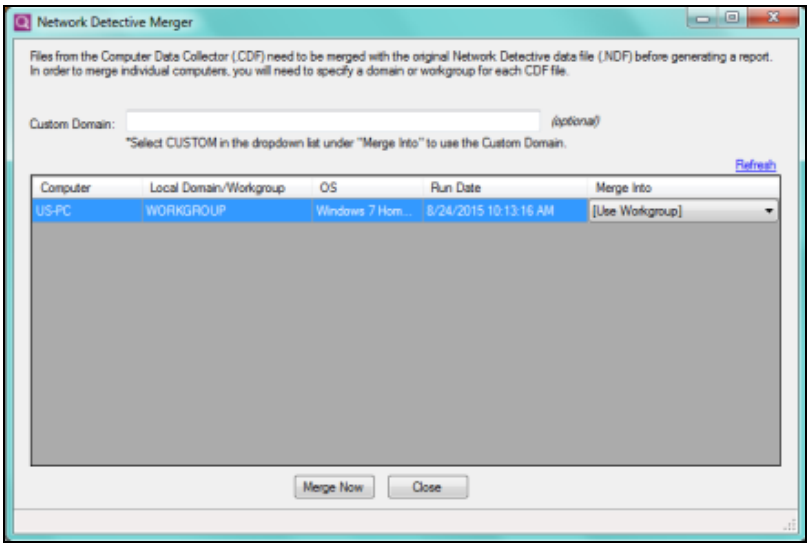
   The **Select the Scan Results** window will be displayed thereby allowing you to import the .CDF files produced by the Push Deploy Tools Local Computer Scans into the Assessment.

2. Browse and Select the Local Computer Scan data files from the Storage Folder location you selected during the setup of the Push Deploy Tool Scan process.

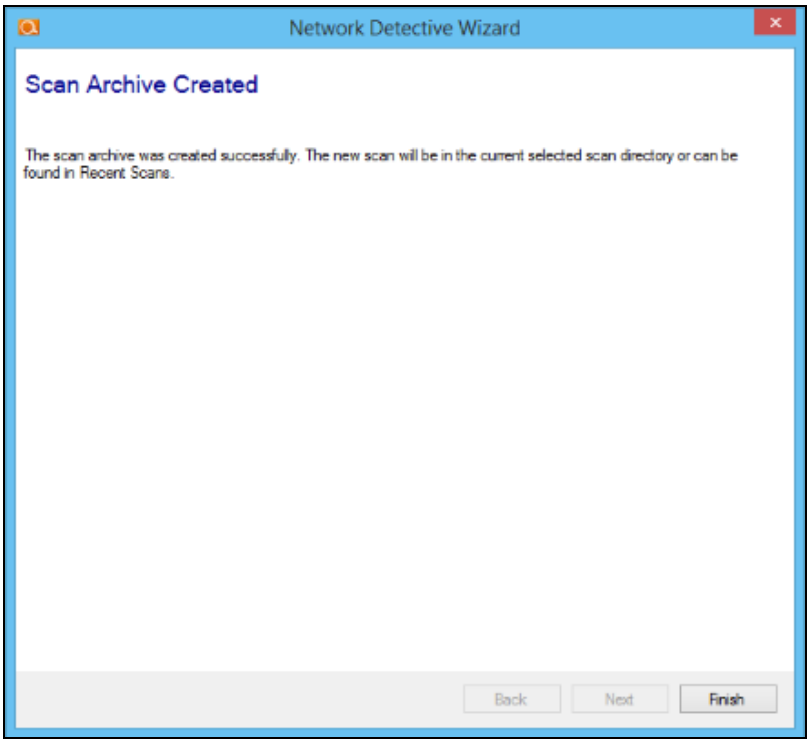


3. Then click the Next button to import the scan data.

   The **Network Detective Merge** window will be displayed.

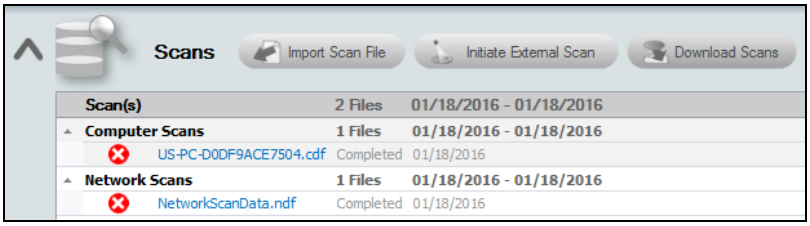


   The success of the scan's import will be confirmed by the **Scan Archive Created** window being displayed as presented below.

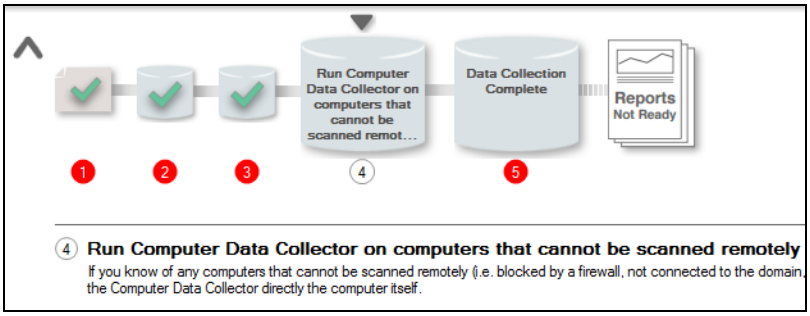


4. Select the **Finish** button to complete the scan file import process.

After the Local Computer scan files are imported into the assessment, the Scans section of the Assessment Window will be updated to list the Computer Scans files imported into the assessment.



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.



Using the Computer Data Collector to Scan Unreachable Computers

Use the Computer Data Collector to perform a local scan on any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible).

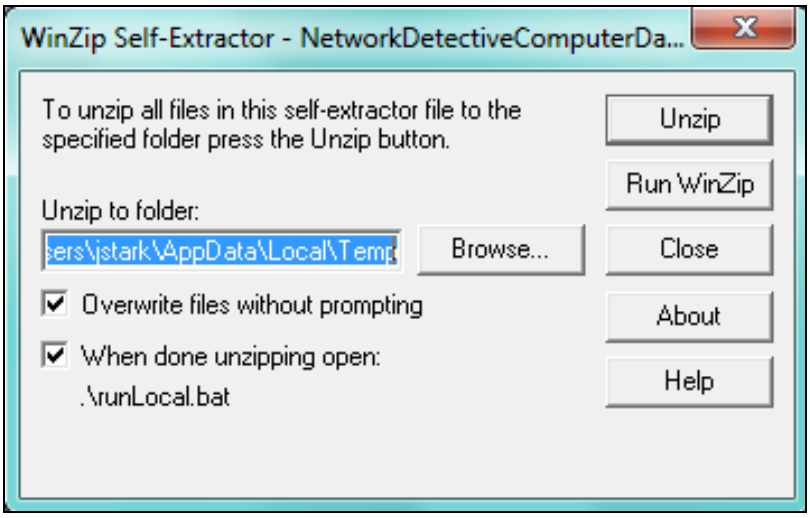
For computers that were unreachable during the Local Scans that were to be performed using the Push Deploy Tool and still require scanning, you will need to download and run the Computer Data Collector from the RapidFire Tools software download website to a folder on a local computer or a USB drive. The Computer Data Collector is a self-extracting .zip file named

NetworkDetectiveComputerDataCollector.exe that executes as an ".EXE" and is completely non-invasive – it is not "installed" on the local computer being scanned or any other machine on the client's network, and does not make any changes to the system.

Step 1 — Running the Computer Data Collector to Perform a Local Computer Scan

Before starting the use of the Computer Data Collector, always download the latest version of the Computer Data Collector. Please follow these steps to download the run the Computer Data Collector.

1. Visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download to a Storage Folder and run the Computer Data Collector named NetworkDetectiveComputerDataCollector.exe This file is a self-extracting ZIP file that does not install on the client computer.
2. After download, run NetworkDetectiveComputerDataCollector.exe and use the Unzip option to unzip the files into a temporary location.



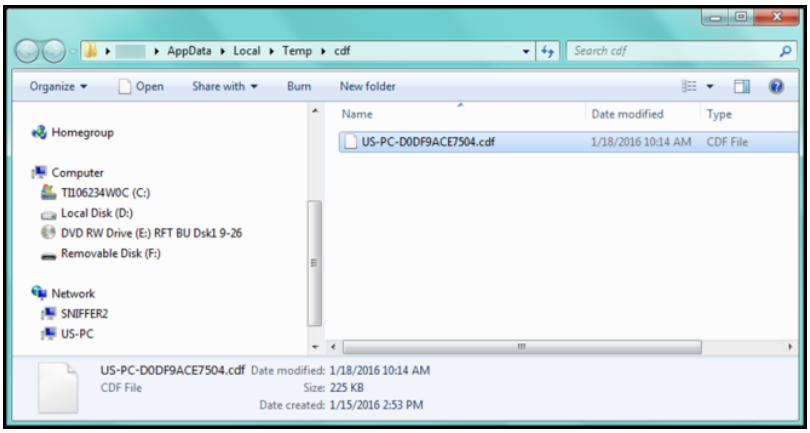
The Computer Data Collector will automatically start running.

> **Note:** After the Computer Data Collector Scan is complete, the scan data file will be located in the Storage Folder you selected during the download and running of the Computer Data Collector.

Note, that the Computer Data Collector will have to be downloaded and run on each local computer that is to be included in the Network Assessment that you are performing.

Step 2 — Monitoring the Computer Data Collector Scan on a Local Computer

Once you unzip the Computer Data Collector, the Computer Data Collector application in the Storage Folder you selected, the program will automatically start and you will be presented with the following window indicating that the Computer Data Collector is performing the local scan.



Step 3 — Review Local Scan File Location

Upon completion of the Local Computer Scan using the Computer Data Collector, a window will be presented to you displaying the location of the scan output file that has a file extension of .CDF.

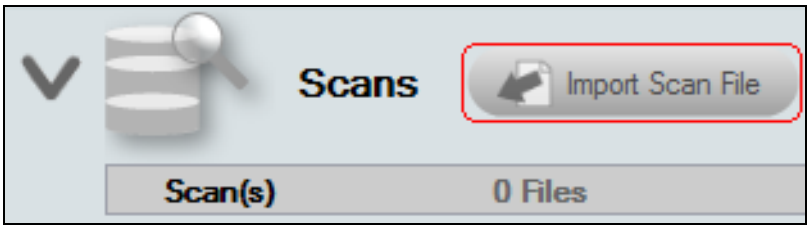
This .CDF file should be retrieved and imported into your assessment.

Importing the Local Computer Scan Data into the BDR Needs Assessment

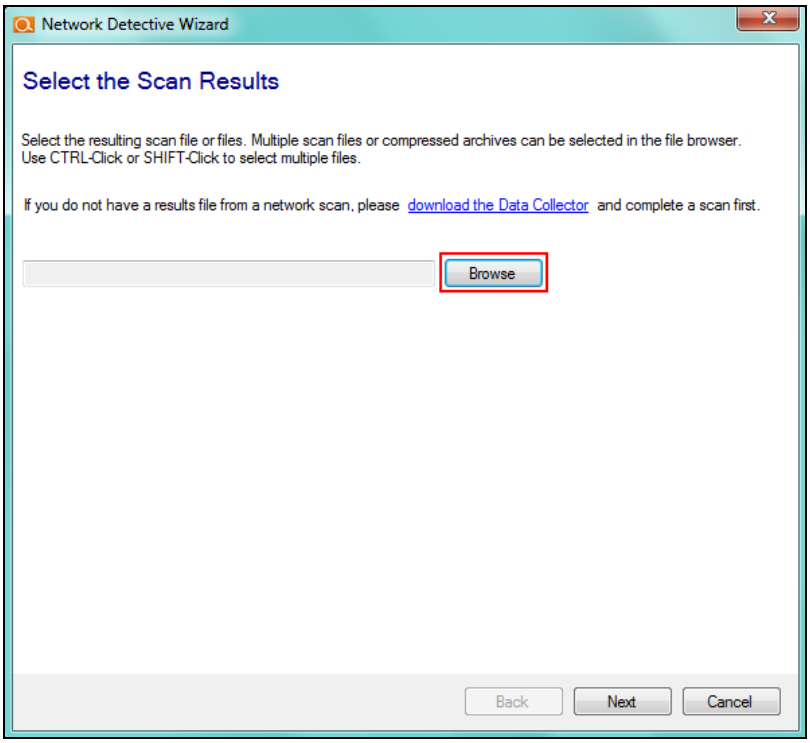
The final step in this process is to import the Local Computer Scan data collected during the Push Deploy Tool Scan into the Active BDR needs assessment.

Perform the following steps to Import the Local Computer Scan Data files:

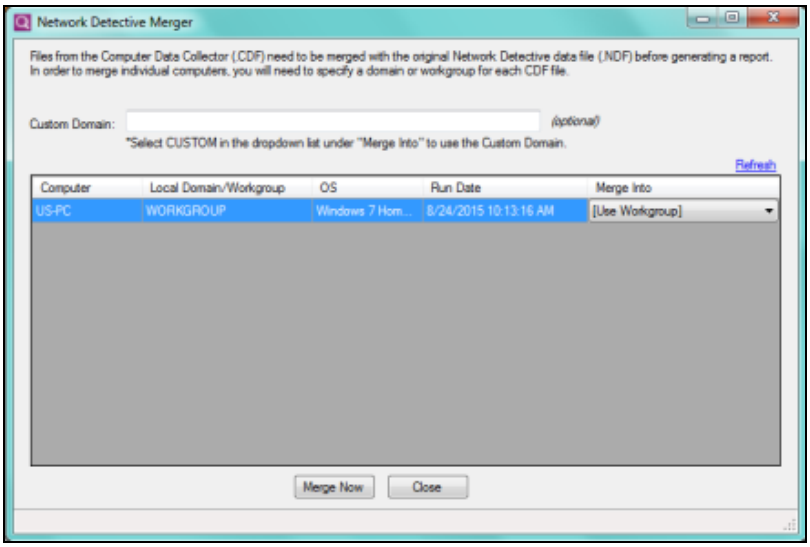
3. Click on the Import Scans File button in the Network Detective Assessment window.



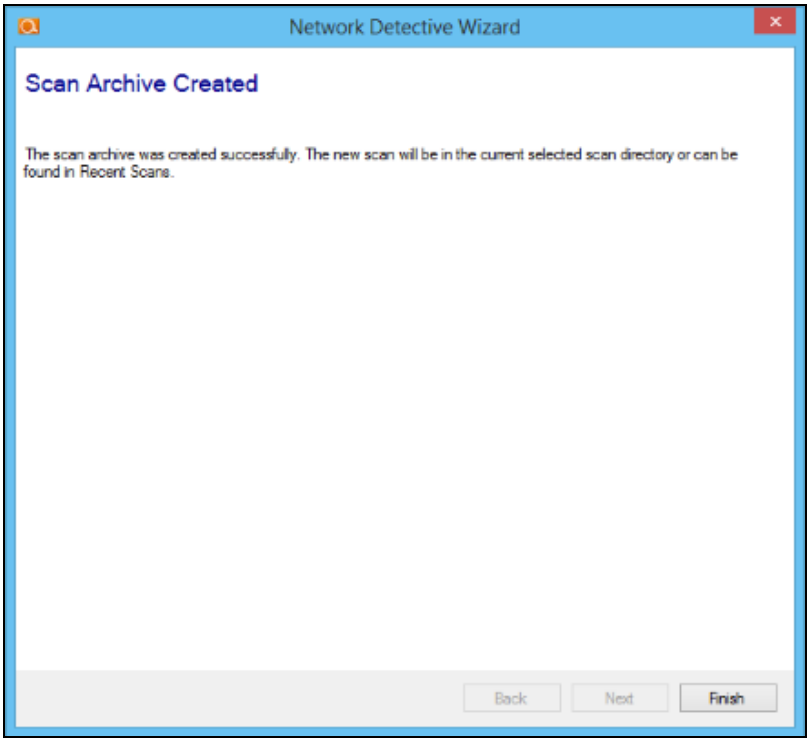
The Select the Scan Results window will be displayed thereby allowing you to import the .CDF file produced by the Computer Data Collector into the Assessment.



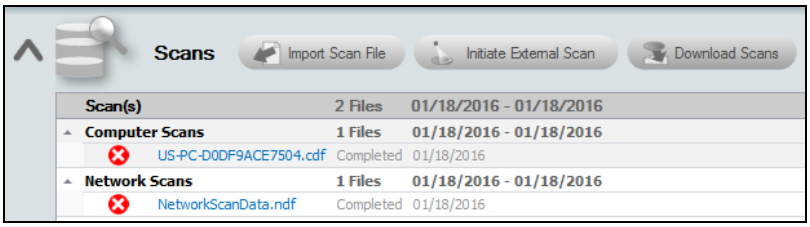
4. Browse and Select the Local Computer Scan data files from the Storage Folder location you selected during the setup of the Computer Data Collector installation process.
5. Then click the Next button to import the scan data.
6. The Network Detective Merge window will be displayed.



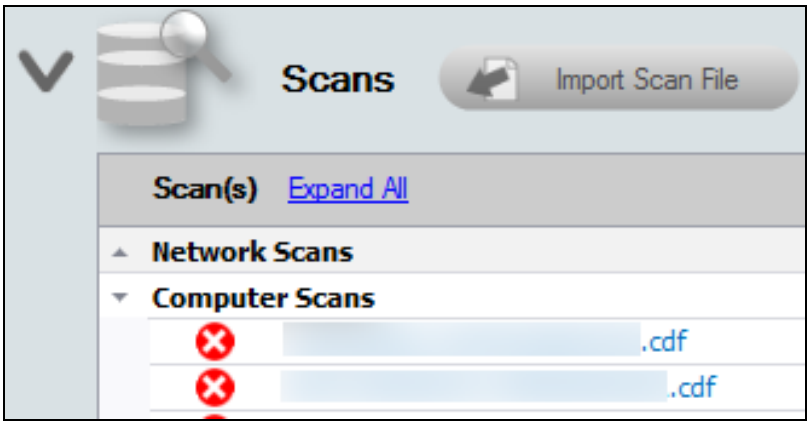
The success of the scan's import will be confirmed by the Scan Archive Created window being displayed as presented below.



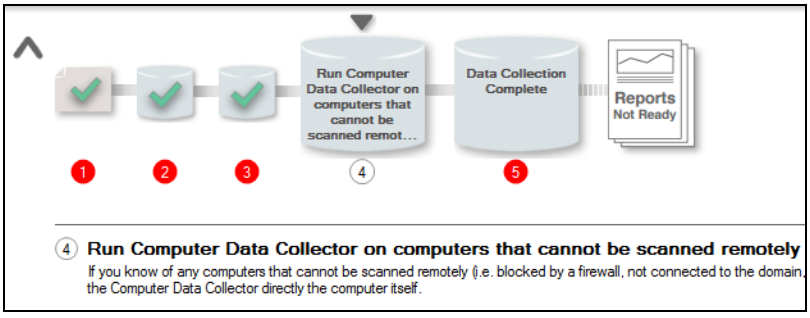
7. Select the Finish button to complete the scan file import process.



After the Local Computer scan files are imported into the assessment, the Scans section of the Assessment Window will be updated to list the Computer Scans files imported into the assessment.



Please note, the Status and Check List information indicators for this step will not be updated in the Checklist until you complete the Scan Completion Confirmation Worksheet.



To verify that the scan file produced by the Computer Data Collector was imported into your assessment, view the Computer Scans file list located under the Scans Bar.

Completing Worksheets and Surveys

Throughout the assessment process, assessment data is gathered though the use of automated scans and by documenting information in a series of surveys and worksheets.

These surveys and worksheets are dynamically generated when the assessment is initially started and when data is collected throughout the assessment process.

Assessment response data is collected through:

- use of automated scans
- importing responses from Word documents
- typing the information directly into surveys and worksheets forms

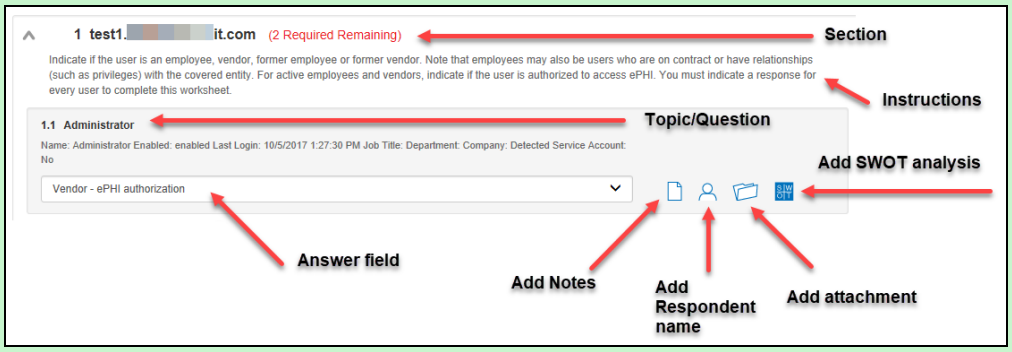
Entering Assessment Responses into Surveys and Worksheets

Throughout the assessment process a number of **Surveys** and **Worksheets** will be generated and require completion.

EXAMPLE:

To complete an InForm worksheet (or survey or questionnaire), follow these steps:

i. Review the *Topic* (i.e. the specific field or question within the form).



ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.

iii. Enter the *Response*. There are three types of responses:

Response Type	Description	Example Use
Text Response	Free-form text response	"Describe the condition of the data center."
Multiple Choice	Multiple fixed responses	"Does the firewall have IPS?" (Yes/No)
Checklist Item	An item that is marked off if completed	"Check the security of the door locks."

Note: With few exceptions, you must respond to each form entry to complete the all of the surveys within the Unitrends BDR Full Assessment process.

iv. (Optional) Enter any *Notes* relevant to the topic's response.

v. (Optional) Enter the name of *Respondent* (i.e. the person who provided you with the information, if applicable).

vi. (Optional) Add any relevant *Attachments*. See "Add Image Attachments to Surveys and Worksheets" below for more details.

Note: Only image attachments (.png, .jpg) are supported at this time.

vii. (Optional) Add a *SWOT Analysis*, examining Strengths, Opportunities, Weaknesses, and Threats. See "Add SWOT Analysis to Surveys and Worksheets" on the facing page for more details.

viii. Save your answers periodically and **Save** and **Close** when you are done.

Add Image Attachments to Surveys and Worksheets

You can add images to worksheets and surveys. You might include pictures of key personnel or diagrams that explain certain security exceptions.

Attachments can be added to each item or question listed in a worksheet. To do this:

1. Open the InForm in your assessment in Network Detective.
2. Underneath an InForm item, click on the folder icon.

3. Click **Add**.
4. Select the attachment from your computer and click **Open**.
5. Continue adding attachments until you are finished.

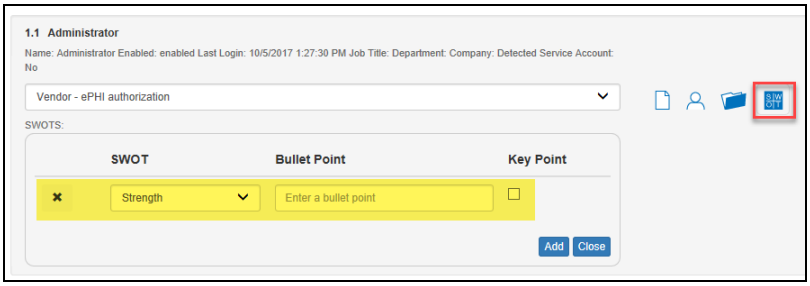
> **Note:** Once you complete your assessment and generate reports, your attached images will appear alongside the form item in the published report and/or supporting document.

Add SWOT Analysis to Surveys and Worksheets

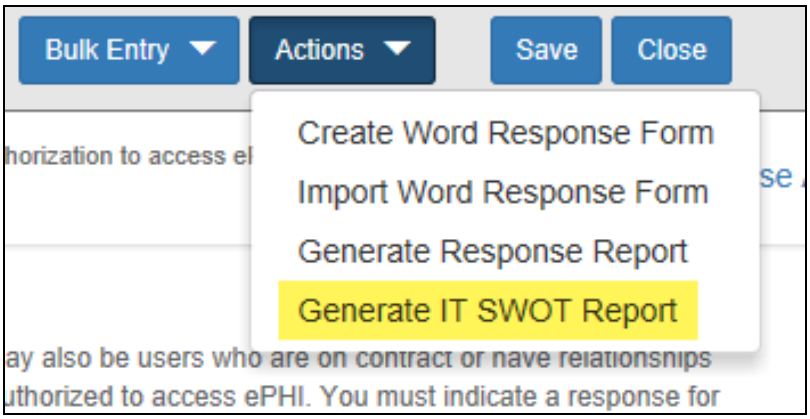
The IT SWOT analysis is a structured method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats affecting an IT network. The analysis involves identifying internal and external issues that are favorable and unfavorable to increasing the overall network health and security of the environment.

To add SWOT to your inform items:

1. Open the InForm in your active assessment in Network Detective.
2. Underneath an InForm item, click on the SWOT icon.



3. Fill in the required fields for each SWOT entry:
   - **Bullet Point**: Enter a short description of the issue here.
   - **Key Point**: Check this to make the entry appear in the SWOT table in the report. Otherwise, it will appear with the rest of the issues in the SWOT list in the report.
4. When you have finished entering all SWOT items for an InForm, click **Actions** and select **Generate IT SWOT Report**.

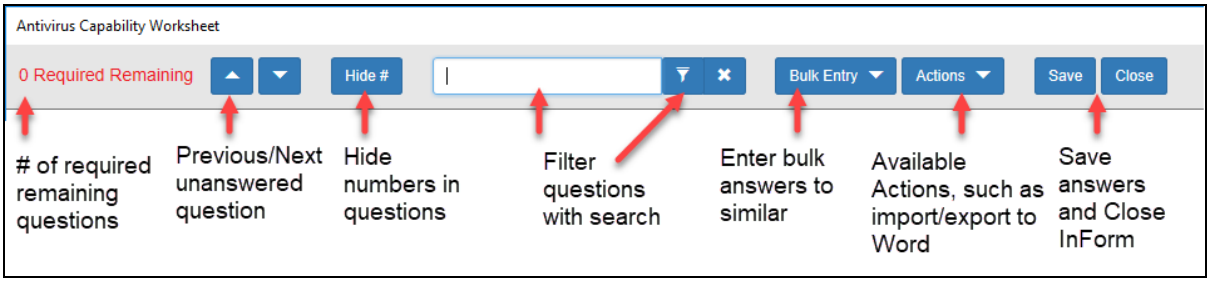


Note: A folder will open with your generated IT SWOT Report. You must generate this report separately for each InForm in your assessment.

Time Savings Tip to Reduce Survey and Worksheet Data Input Time

Use the InForm Worksheet Tool Bar

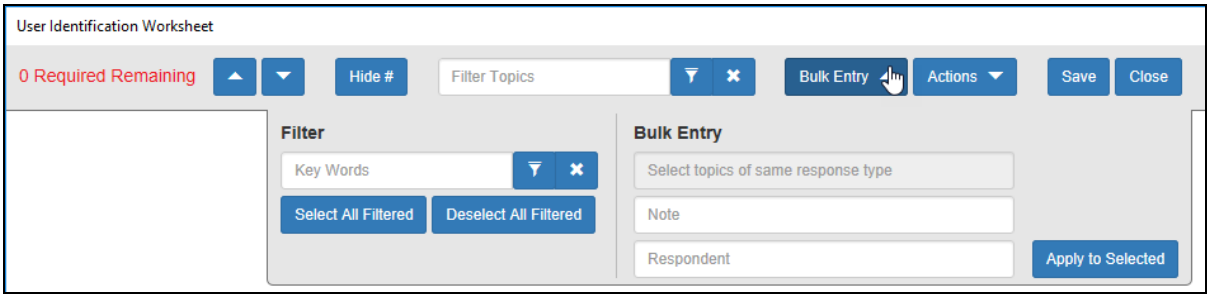
Use the InForm tool bar to save time when completing worksheets.



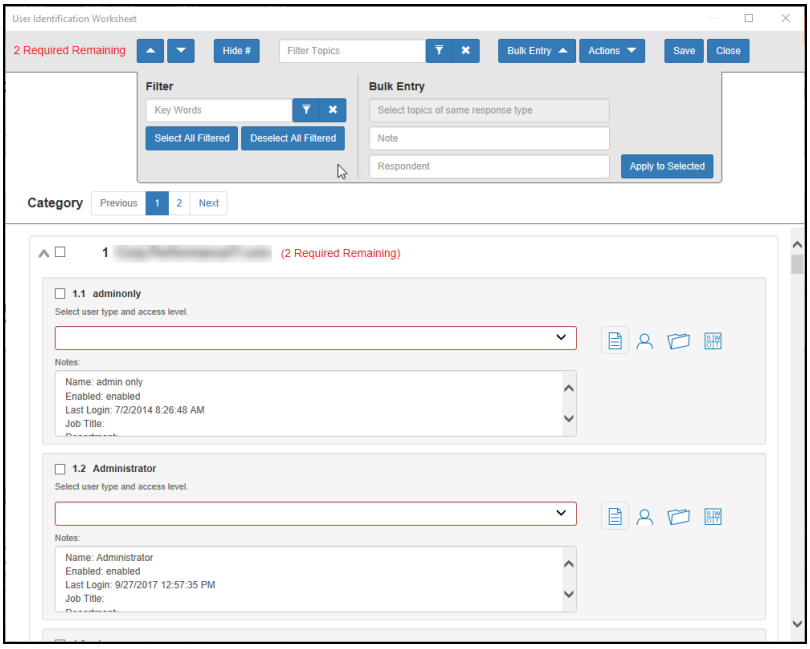
Bulk Entry for InForm Worksheets

InForm allows you to enter bulk responses for worksheet questions. Note that you can only enter bulk responses for questions that require the same types of responses. To use the bulk entry feature:

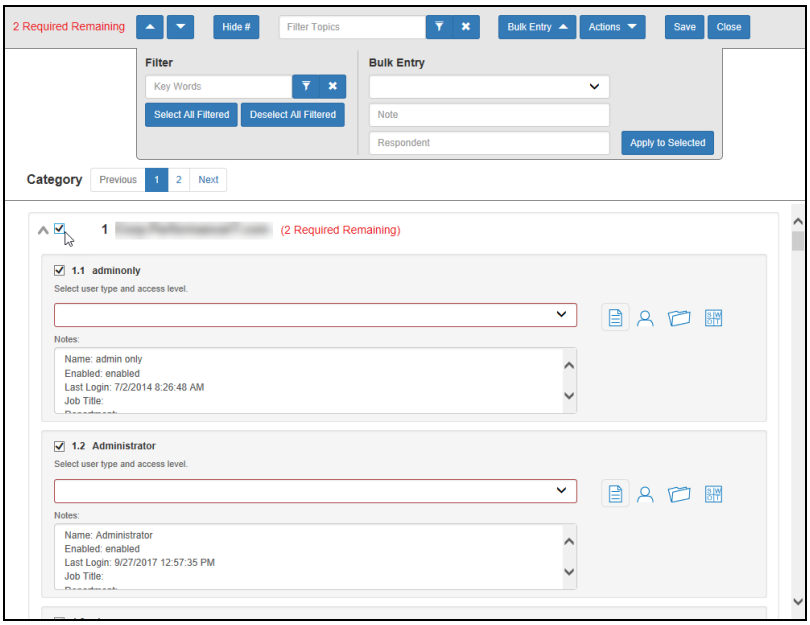
1. Click **Bulk Entry** from the Inform tool bar.



Check boxes will appear next to the response topics.

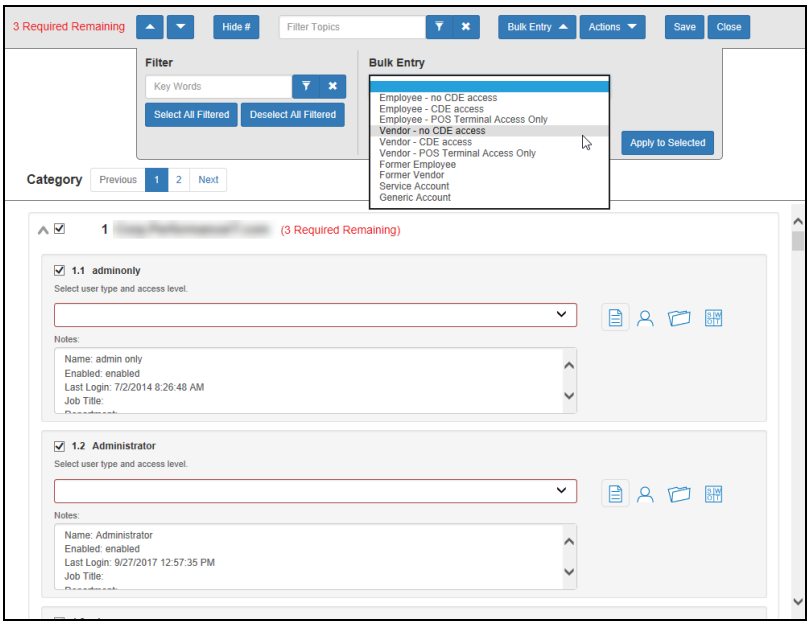


2. Select the check boxes for the topics for which you wish to enter bulk responses.

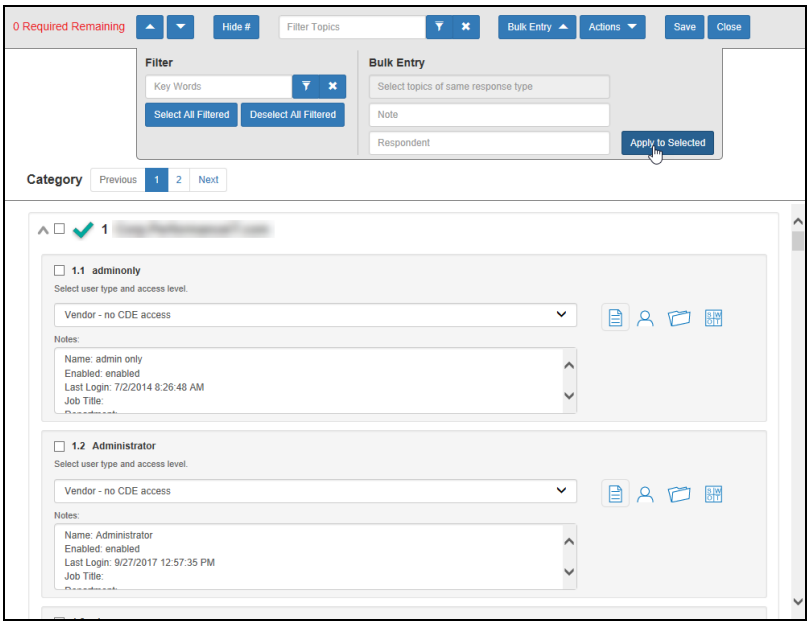


Note: You can select individual topics, or you can click the check box next to the section heading to select all topics within the section. You can also **Filter** topics using terms like "Admin." Note that each topic within the section must require the same types of responses in order to enter bulk responses.

3. Select the response from the Bulk Entry menu. You can likewise enter any relevant notes or the name of a respondent.



4. Then click **Apply to Selected**.



Your chosen response will be entered into the selected topics.

Create Word Response Form

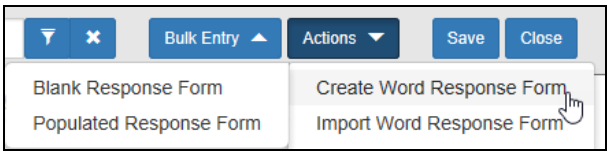
You can export InForm worksheets in your assessment project to Word. This allows you or others to complete worksheets without using Network Detective. For example, you can create a Word response form and send it to a client at a site. The client can then help you gather the required information and enter it in the response form.

Important: In order to import your data, you must enter your responses in the fields contained in the Word document. See "Important Note on Working with Word Response Forms" on the next page for detailed instructions.

To create a Word response Form:

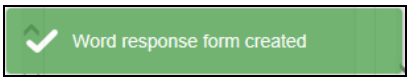
1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
    a. Click **Blank Response Form** to generate a Word document with blank fields ready for data entry.
    b. Click **Populated Response Form** to generate a Word document with the

responses already entered using InForm.



3. Select the location to save the file. Click **Save**.

   A confirmation message will appear.



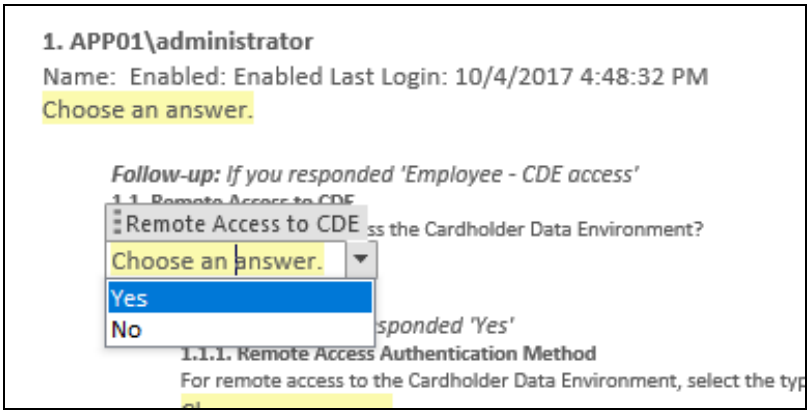
Important Note on Working with Word Response Forms

When you export a Word response form from your assessment, keep in mind the following important tips:

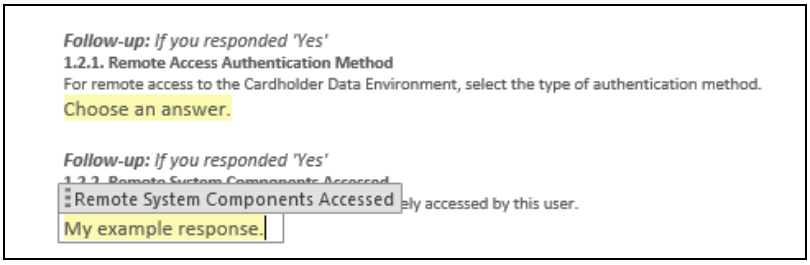
- **DO NOT DELETE** the field controls embedded in the response form! The response fields appear in the images below for your reference:

  Important: If you delete these fields, your data cannot be imported into the assessment!

  Multiple choice response field



  Text response field



- You must use the Word fields to enter your responses. Any content you enter not included in these fields will not be imported into your assessment.

Import Word Response Form

You can import a Word response form into your assessment using InForm. This allows you to collaborate with others to gather information and complete worksheets.

EXAMPLE:

Step 1: Create/export a Word response form for one of the worksheets in your assessment.

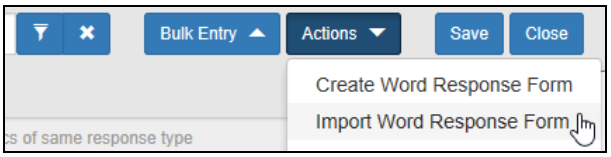
Step 2: Send it to a client to enter additional information about the site using Word.

Step 3: The client can then send you the worksheet as an email attachment.

Step 4: Import the Word document back into your assessment with the client's responses and make any final changes to the worksheet.

To import a Word response form:

1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
3. Click **Import Word Response Form**.



4. Select the file to import. Click **Open**.

A confirmation message will appear. The InForm worksheet fields will be updated with the imported responses.