



# QUICK START GUIDE

---

## Security Assessment Module

Instructions to Perform a Security Assessment

# Contents

---

<b>Performing a Security Assessment</b> .....	<b>3</b>
<u>Security Assessment Overview</u> .....	3
What You Will Need .....	3
Network Prerequisites for Network Detective Scans .....	5
<u>Step 1 — Download and Install the Network Detective Application</u> .....	6
<u>Step 2 — Create a New Site</u> .....	6
<u>Step 3 — Start a Security Assessment</u> .....	8
<u>Step 4 — Initiate External Vulnerability Scan</u> .....	9
<u>Step 5 — Perform Security Scan Data Collection</u> .....	12
Scanning an Active Directory Domain-based Network .....	13
Scanning a Workgroup Network .....	21
<u>Step 6 — Use the Push Deploy Tool to Collect Remaining Data</u> .....	28
<u>Step 7 — Import Scans into Network Detective App</u> .....	33
<u>Step 8 — Generate Security Assessment Reports</u> .....	35
<b>Security Assessment Reports</b> .....	<b>36</b>
<u>Standard Reports</u> .....	36
<u>Infographics</u> .....	40
<u>Change Reports</u> .....	40
<b>Data Breach Liability Scanning and Reporting</b> .....	<b>42</b>
<u>Steps to Perform Scans to Identify PII and Generate the Data Breach Liability Report</u> .....	43

# Performing a Security Assessment

## Security Assessment Overview

The Security Assessment Module allows you to deliver IT security assessment services to your client – even if you aren't an IT security expert. Just run the installation-free scanning tool, import the scan results into our proprietary risk analyzer, customize the reports with your own company name and branding elements, and run the reports. The Security Assessment Module has many uses for your MSP, including:

- Generate executive-level reports that include a proprietary Security Risk Score and Data Breach Liability Report along with summary charts, graphs and an explanation of the risks found in the security scans.
- Identify network "share" permissions by user and computer. Provide comprehensive lists of all network shares, detailing which users and groups have access to which devices and files, and what level of access they have.
- Catalog external vulnerabilities including security holes, warnings, and informational items that can help you make better network security decisions. This is an essential item for many standard security compliance reports.
- Methodically analyze login history from the security event logs. The report uses mathematical modeling and proprietary pattern recognition to highlight potential unauthorized users who log into machines they normally do not access and at times they normally do not log in.

## What You Will Need

Security Assessment Component	Description
<b>Network Detective</b>	The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.

<b>Security Assessment Component</b>	<b>Description</b>
<b>Security Assessment Data Collector</b>	The Network Detective Security Assessment Data Collector (SADC) is a windows application that performs the data collections for the Security Assessment Module.
<b>Push Deploy Tool</b>	The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.



## Network Prerequisites for Network Detective Scans

For a successful network scan:

1. **ENSURE ALL NETWORK ENDPOINTS ARE TURNED ON THROUGHOUT THE DURATION OF THE SCAN.** This includes PCs and servers. The scan can last several hours.
2. **CONFIGURE THE TARGET NETWORK TO ALLOW FOR SUCCESSFUL SCANS ON ALL NETWORK ENDPOINTS.** See [Pre-Scan Network Configuration Checklist](#) for configuration guidance for both Windows Active Directory and Workgroup environments.
3. **GATHER THE INFORMATION BELOW TO CONFIGURE YOUR SCANS FOR THE CLIENT SITE.** Work with the project Technician and/or your IT admin on site to collect the following:
  - **Admin network credentials** that have rights to use WMI, ADMIN\$, and File and Printer Sharing on the target network.
  - **Internal IP range** information to be used when performing internal scans.

**Note:** Network Detective will automatically suggest an IP range to scan on the network. However, you may wish to override this or exclude certain IP addresses.

- **External IP addresses** for the organisation to be used when setting up External Vulnerability Scans.
- **Network Detective User Credentials**
- For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IP address of the domain controller.
- For Windows Workgroup network environments, a list of the Computers to be included in the Assessment and the Local Admin Credentials for each computer.

Follow these steps to perform a Security Assessment.

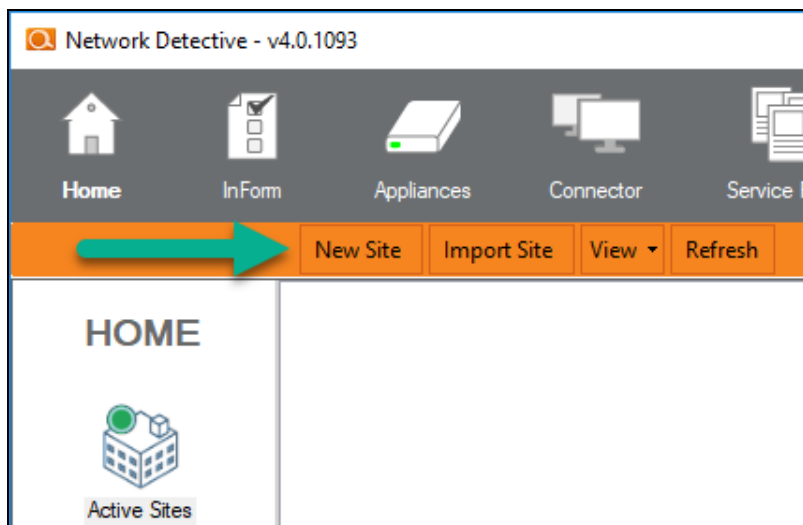
## Step 1 — Download and Install the Network Detective Application

Go to <https://www.rapidfiretools.com/nd-downloads> to download and install the Network Detective application on a PC on the MSP network. Then run Network Detective and log in with your credentials.

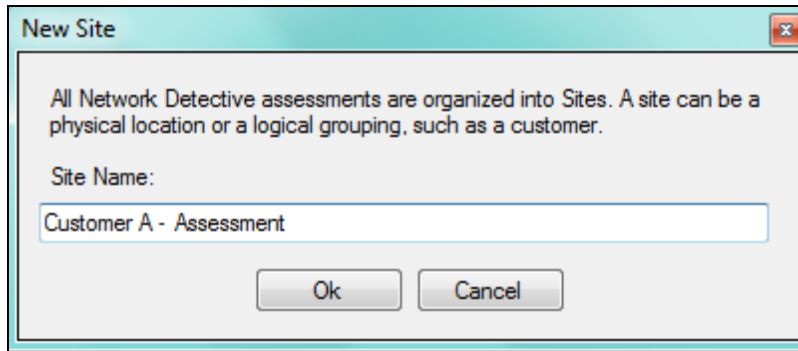
## Step 2 — Create a New Site

To create a new site:

1. Open the Network Detective Application and log in with your credentials.
2. Click **New Site** to create a new Site for your assessment project.



3. Enter a **Site Name** and click **OK**.

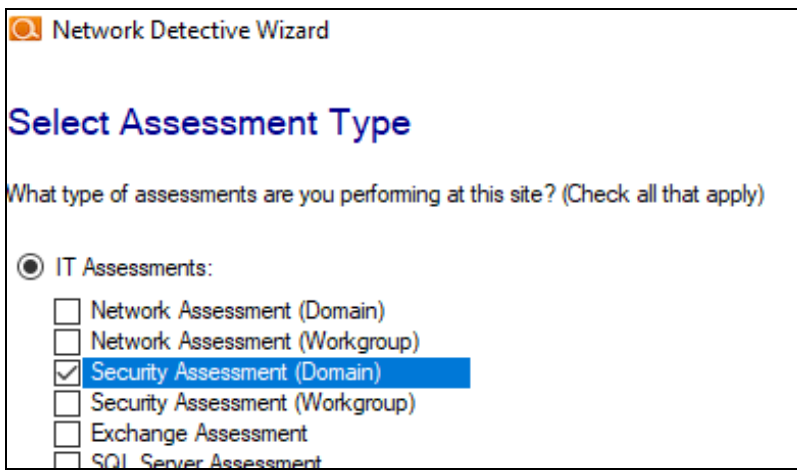


### Step 3 — Start a Security Assessment

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**.

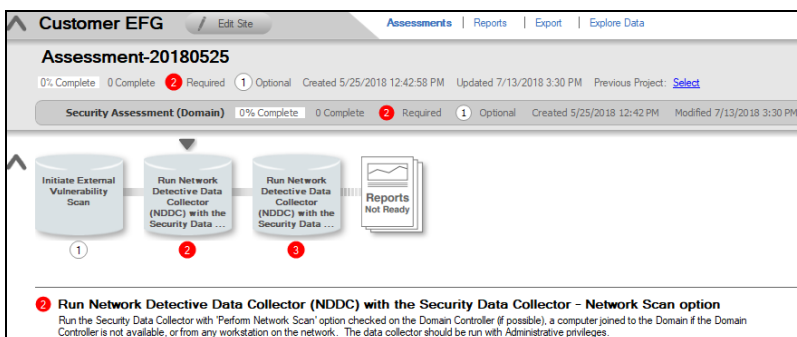


Next, select the **Security Assessment** option presented.



Then follow the prompts presented in the **Network Detective Wizard** to start the new **Assessment**.

2. Once the new **Security Assessment** is started, a “**Checklist**” is displayed in the **Assessment Window** presenting the “**Required**” and “**Optional**” steps that are to be performed during the assessment process. Below is the **Checklist** for a **Security Assessment**.





3. Complete the required **Checklist Items** and use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

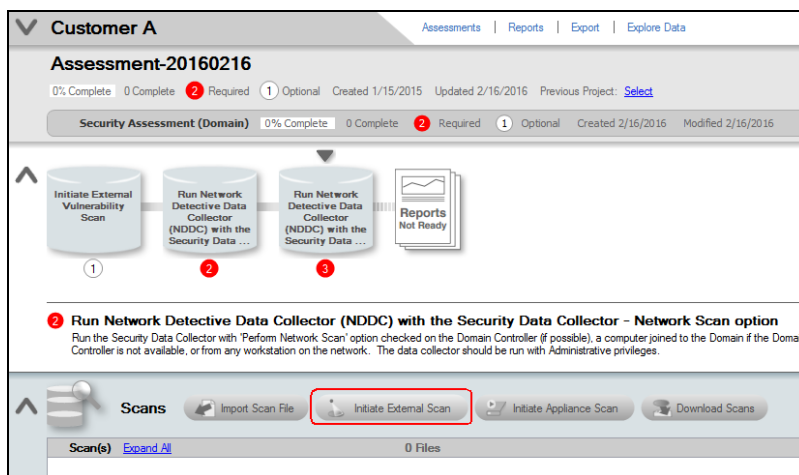
You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.



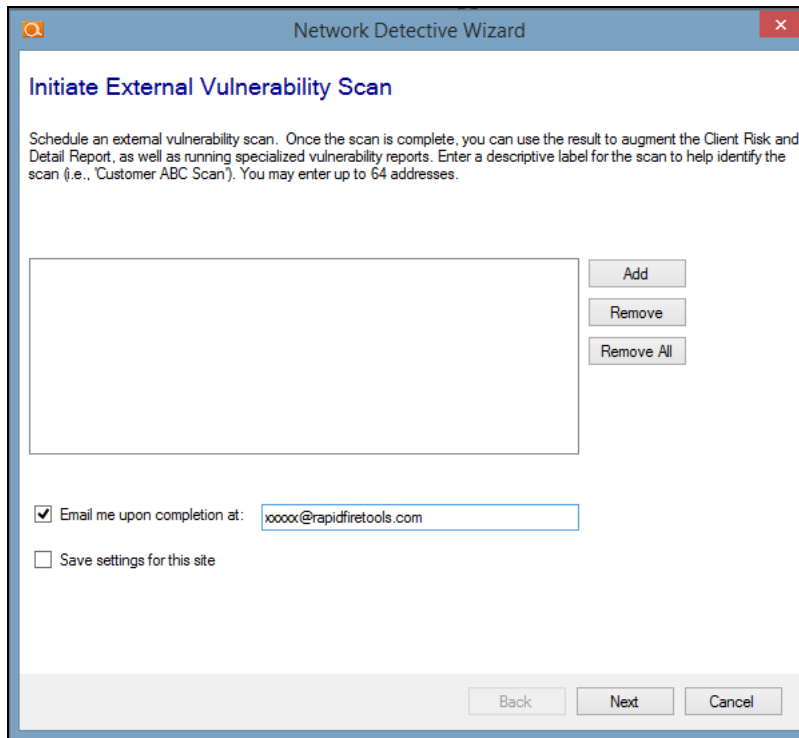
## Step 4 — Initiate External Vulnerability Scan

**Important:** You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Select **Initiate External Scan** button to start an **External Vulnerability Scan**.

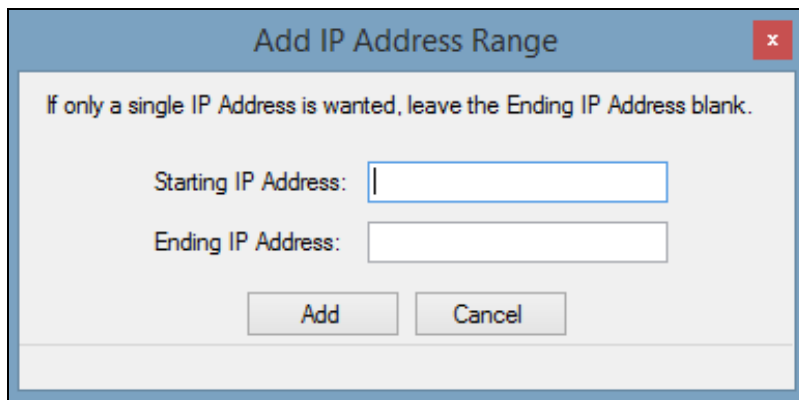


Enter the range of IP addresses you would like to scan. **You may enter up to 64 external addresses.**



The screenshot shows a window titled "Network Detective Wizard" with a red close button in the top right corner. The main heading is "Initiate External Vulnerability Scan". Below the heading is a paragraph of text: "Schedule an external vulnerability scan. Once the scan is complete, you can use the result to augment the Client Risk and Detail Report, as well as running specialized vulnerability reports. Enter a descriptive label for the scan to help identify the scan (i.e., 'Customer ABC Scan'). You may enter up to 64 addresses." Below this text is a large empty rectangular box for entering addresses. To the right of this box are three buttons: "Add", "Remove", and "Remove All". Below the address box is a checkbox labeled "Email me upon completion at:" followed by a text input field containing "xxxxx@rapidfiretools.com". Below that is another checkbox labeled "Save settings for this site". At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

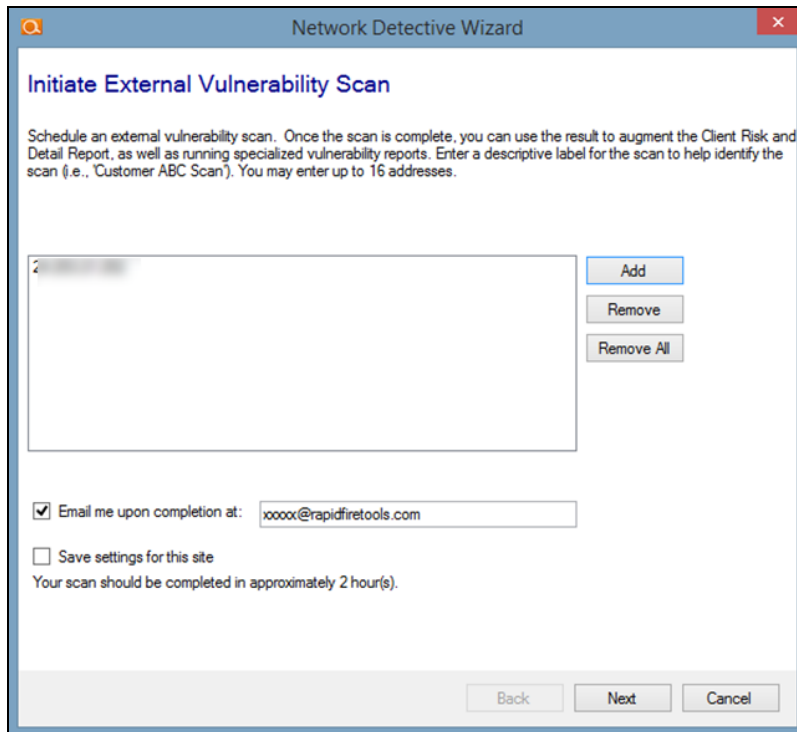
Select **Add** to add a range of external IP addresses to the scan. If you do not know the external range, you can use websites such as [whatismyip.com](http://whatismyip.com) to determine the external IP address of a customer.



The screenshot shows a dialog box titled "Add IP Address Range" with a red close button in the top right corner. The text inside reads: "If only a single IP Address is wanted, leave the Ending IP Address blank." Below this text are two input fields: "Starting IP Address:" followed by an empty text box, and "Ending IP Address:" followed by an empty text box. At the bottom of the dialog are two buttons: "Add" and "Cancel".

Enter the IP range for the scan. For just one address, enter the same value for the **Starting** and **Ending IP Address**.

You can initiate the External Vulnerability Scan before visiting the client's site to perform the data collection. This way, the External Scan data should be available when you are ready to generate the client's reports.



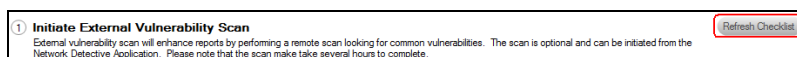
The screenshot shows a window titled "Network Detective Wizard" with a sub-header "Initiate External Vulnerability Scan". The main text reads: "Schedule an external vulnerability scan. Once the scan is complete, you can use the result to augment the Client Risk and Detail Report, as well as running specialized vulnerability reports. Enter a descriptive label for the scan to help identify the scan (i.e., 'Customer ABC Scan'). You may enter up to 16 addresses." Below this is a large text input field. To the right of the field are three buttons: "Add", "Remove", and "Remove All". Below the field is a checkbox labeled "Email me upon completion at:" followed by a text input field containing "xxxxx@rapidfiretools.com". There is also a checkbox labeled "Save settings for this site". Below these is the text "Your scan should be completed in approximately 2 hour(s)". At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

In the **Initiate External Vulnerability Scan** window, enter an email address to be notified when the scan is completed.

Click **Next** to send the request to the servers that will perform the scan.

Scans can take several hours to complete. You will receive an e-mail when the External Vulnerability Scan is complete.

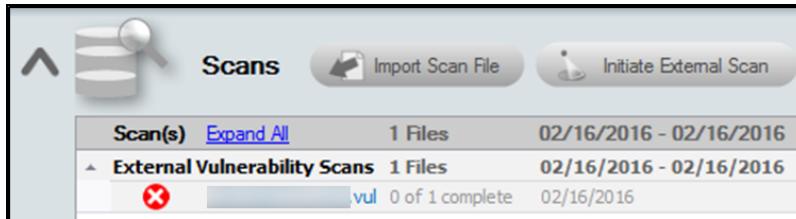
Next, select the **Refresh Checklist** option to update the status of the **External Vulnerability Scan** that is listed under the **Scans** bar.



The screenshot shows a status bar with a red icon and the text "Initiate External Vulnerability Scan". Below this is a small text box: "External vulnerability scan will enhance reports by performing a remote scan looking for common vulnerabilities. The scan is optional and can be initiated from the Network Detective Application. Please note that the scan make take several hours to complete." To the right of the text box is a button labeled "Refresh Checklist".

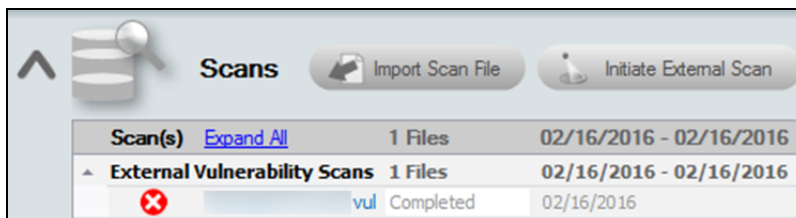
The **Assessment Window** and associated **Scans** listed under the **Scans** bar at the bottom of the **Assessment Window** will be updated to reflect the External Vulnerability Scan has been initiated and its completion is pending.

Refer to the **Scans** list within the **Assessment Window** detailed in the figure below.



The scan's **pending** status of **"0 of 1 complete"** will be updated to **"Completed"** once the scan is completed. An email message stating that "the scan is complete" will also be sent to the person's email address that was specified when the scan was set up to be performed.

Upon the scan's completion, note that the **External Vulnerability Scan** with its **"Completed"** status will be listed as an imported scan under the **Scans** bar at the bottom of the **Assessment Window** as presented below.

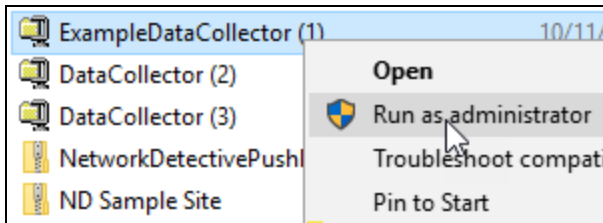


## Step 5 — Perform Security Scan Data Collection

Download and run the **Network Detective Data Collector** on a PC on the target network. Use the Data Collector to scan the target network.

1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/nd> and download the **Network Detective Data Collector**.

2. Run the **Network Detective Data Collector** executable program as an Administrator (**right click>Run as administrator**).



**Important:** For the most comprehensive scan, you **MUST** run the data collector as an **ADMINISTRATOR**.

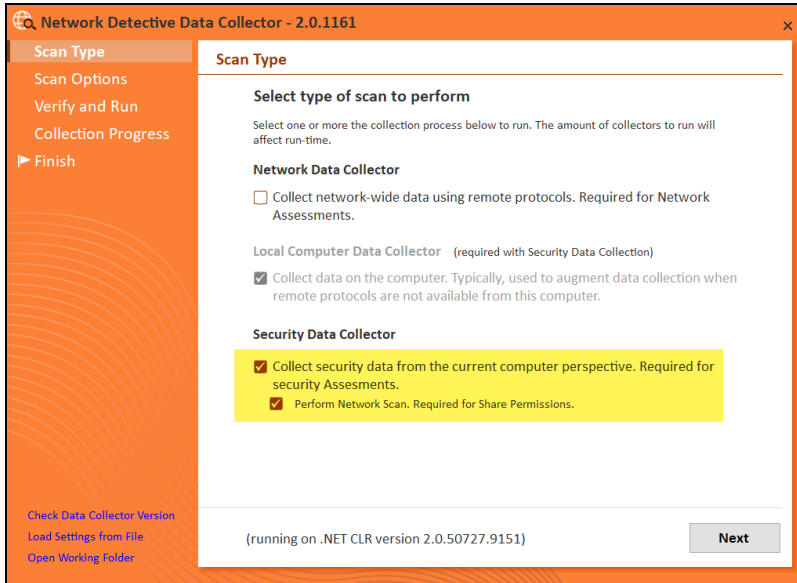
3. **Unzip** the files into a temporary location. The Network Detective Data Collector's self-extracting ZIP file does not install itself on the client computer.
4. The Network Detective Data Collector Scan Type window will appear.

Configure the network scan using the wizard.

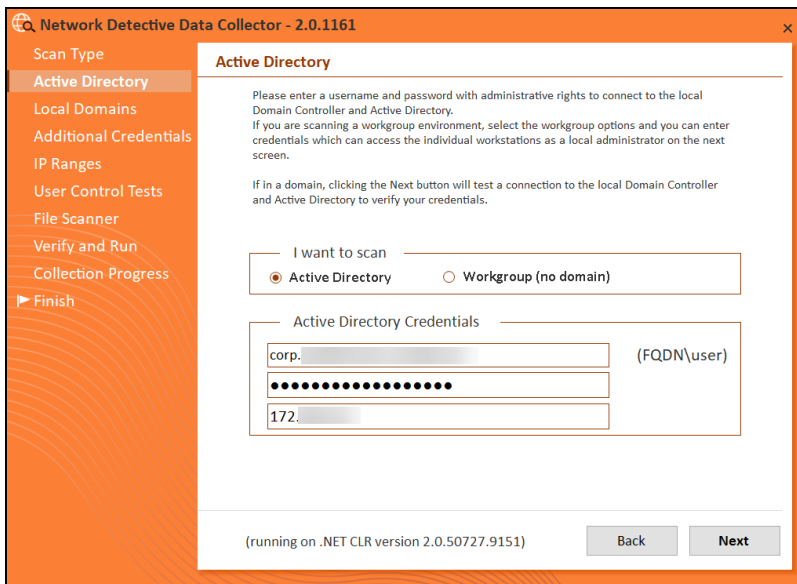
- Look here if you are ["Scanning an Active Directory Domain-based Network" below](#)
- Look here if you are ["Scanning a Workgroup Network" on page 21](#)

## Scanning an Active Directory Domain-based Network

Select the **Security Data Collector** and **Perform Network Scan** options. Click **Next**.



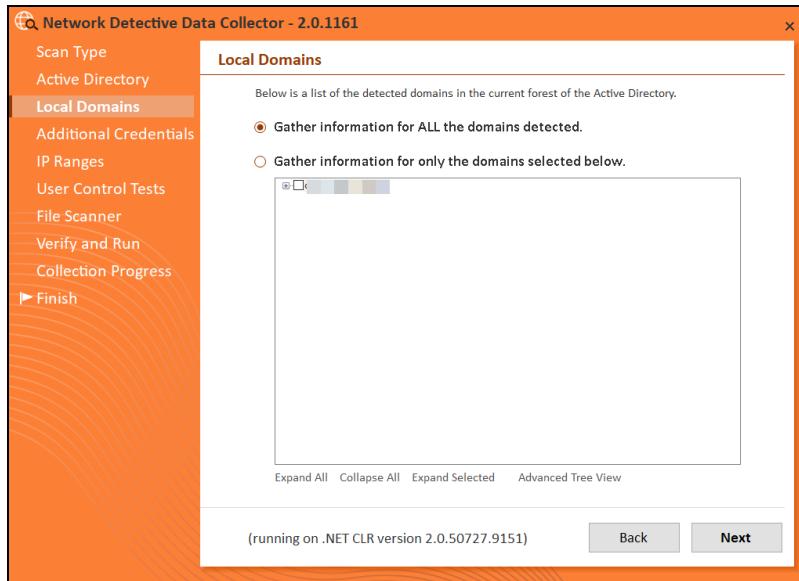
1. The **Active Directory** window will appear. Select the type of network you are scanning (*Active Directory domain*).



2. Next enter the network's **Fully Qualified Domain Name** along with a **username** and **password** with administrative rights to connect to the local Domain Controller and Active Directory.

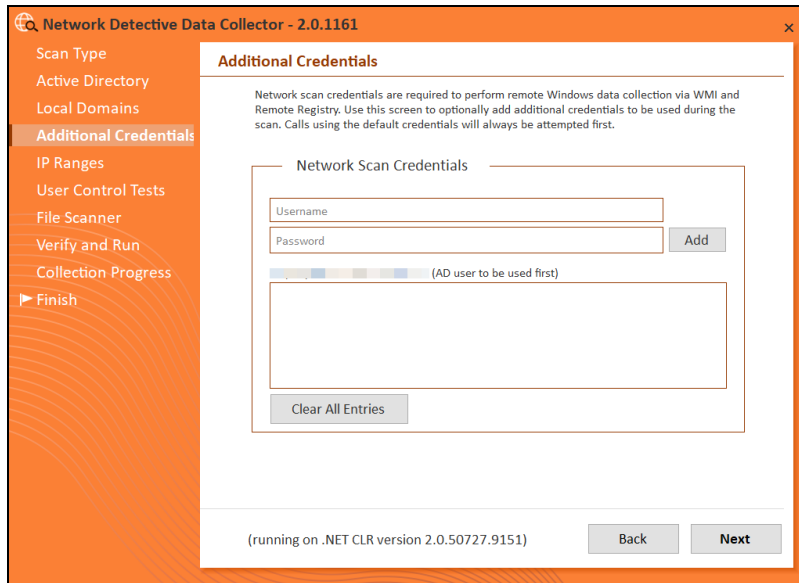
**Note:** For example: `corp.yourprospect.com\username`.

3. Enter the name or IP address of the domain controller.
4. Click **Next** to test a connection to the local Domain Controller and Active Directory to verify your credentials.
5. The **Local Domains** window will appear. Select the Domains to scan. Choose whether to scan all domains or only specific domains and OUs. Click **Next**.

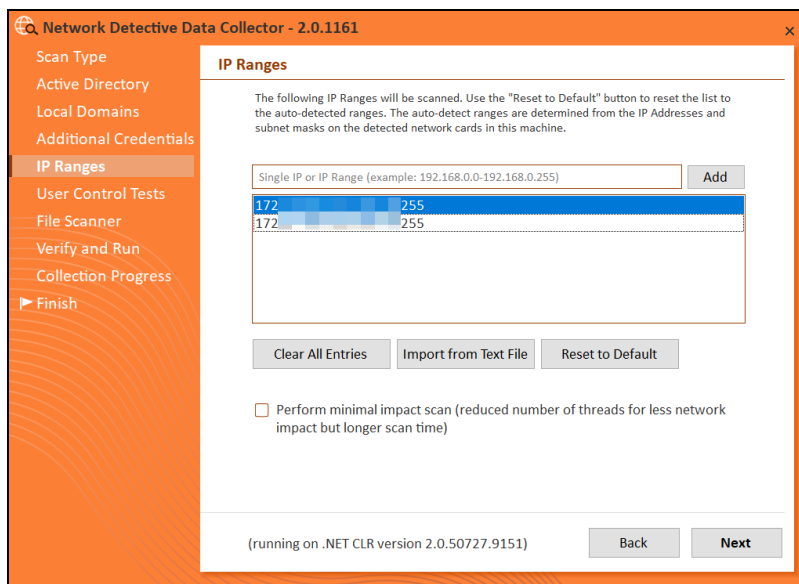


Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

6. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan using the fully qualified domain name. For example: `corp.yourprospect.com\username`. Click **Next**.



7. The **IP Ranges** screen will then appear. The Network Detective Data Collector will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.



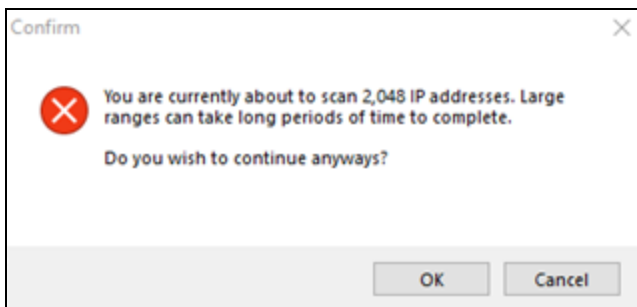
From this screen you can also:



- Click **Reset to Default** to reset to the automatically suggested IP Range.
- Click **Import from Text File** to import a predefined list or range of IP addresses.

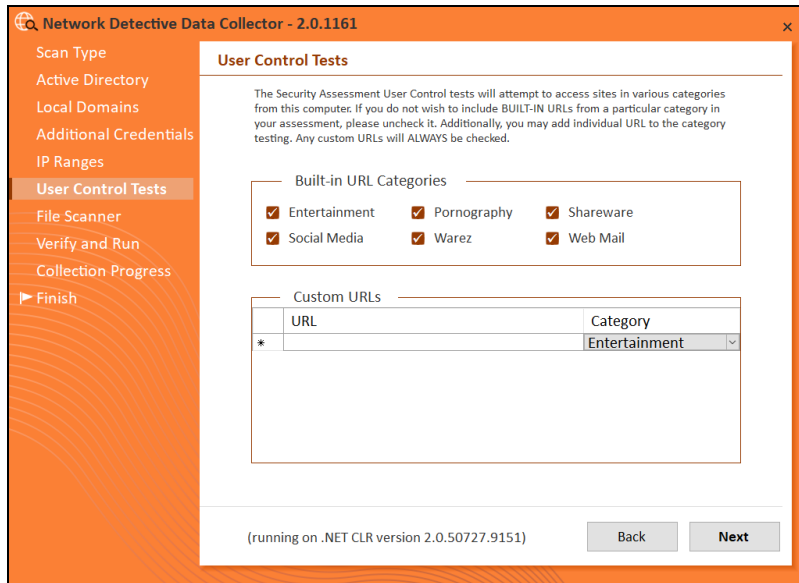
**Important:** Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

When you have entered all IP Ranges to scan, click **Next**.

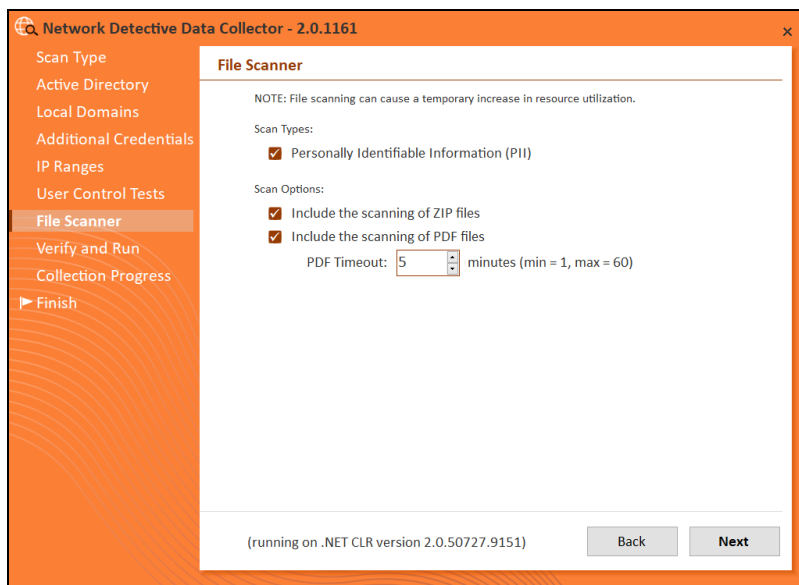


**Important:** If you are scanning a large number of IP addresses, confirm that you wish to continue.

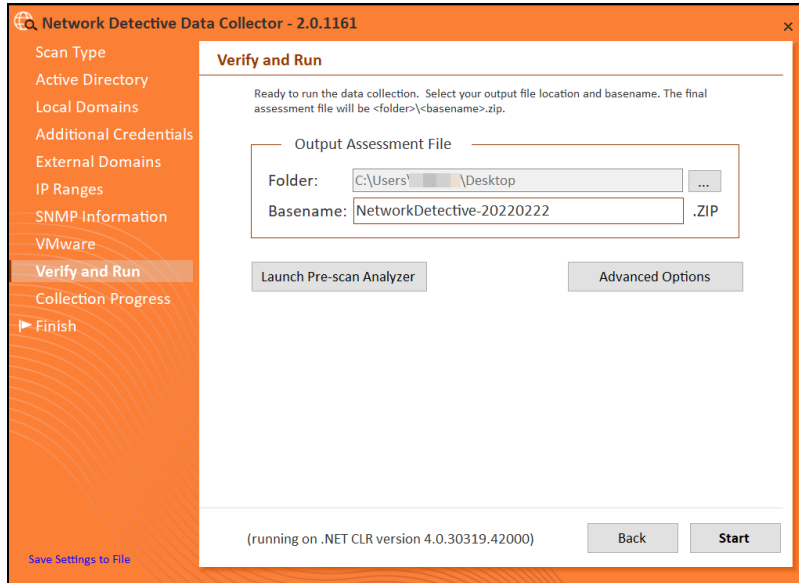
8. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your own custom URLs and categories to test. Then click **Next**.



9. The **File Scanner** screen will appear. Choose whether to scan for PII (Personally Identifiable Information) and click **Next**.



10. The **Verify and Run** window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan's **Output Assessment File Folder** location and **Basename** for the scan data. The file will be output as a **.NDF** file.

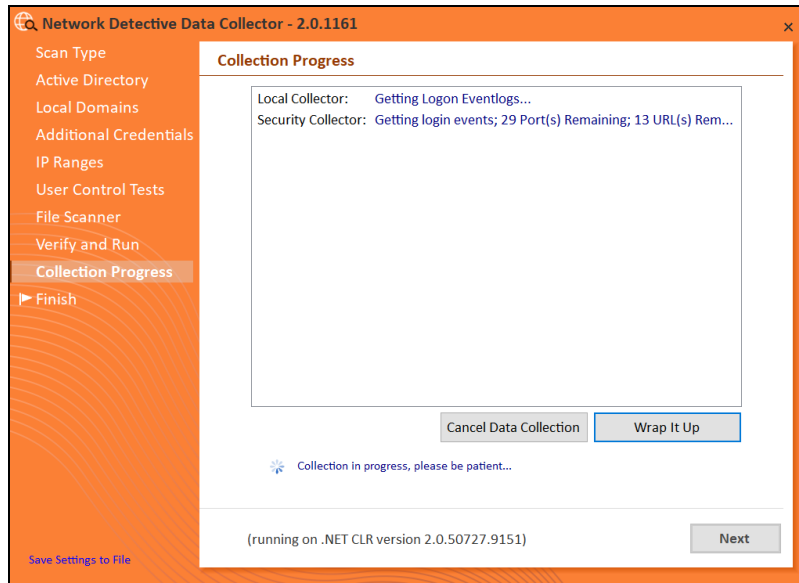


**Tip:** Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion of the pre-scan.

Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01.CORP.RAPIDFIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORP.RAP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-095DFE1.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HM0E71.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4Q8O.CORP...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORP.R...	10.236.83.1...	✓	?			Accessing WMI...
DESKTOP-7RF9K75.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.

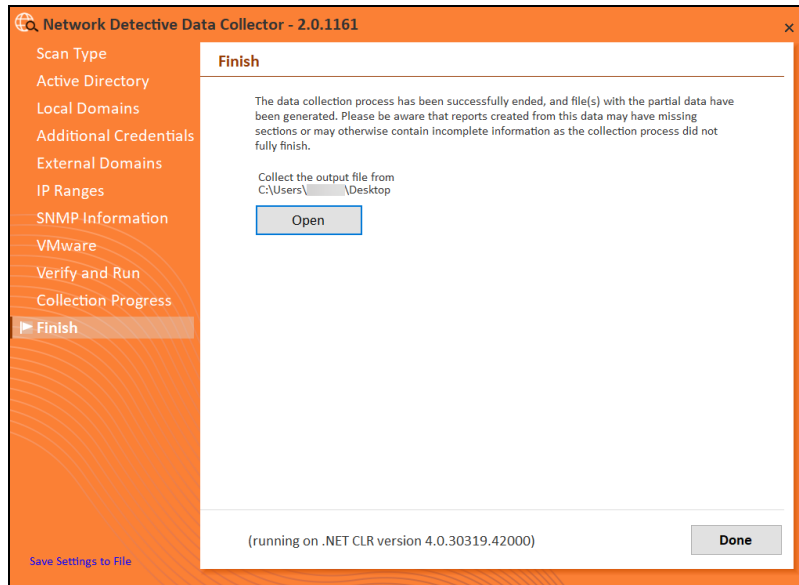
Enter any **Comments** and then click **Start**.

- The **Collection Progress** window will appear. 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.

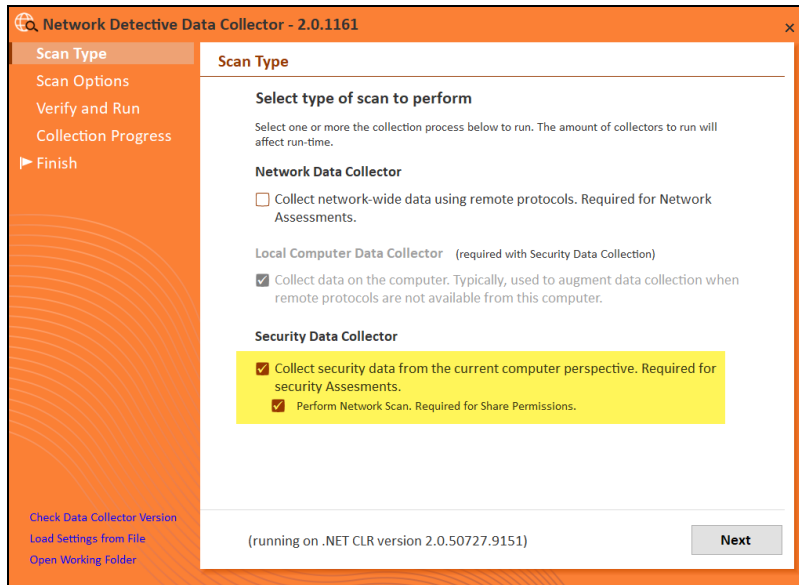
Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.



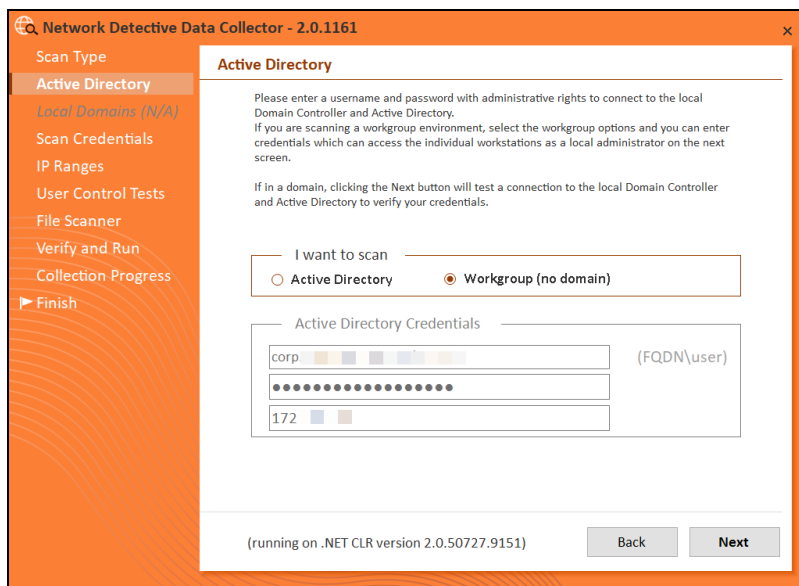
Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

## Scanning a Workgroup Network

1. Select the **Security Data Collector** and **Perform Network Scan** options. Click **Next**.

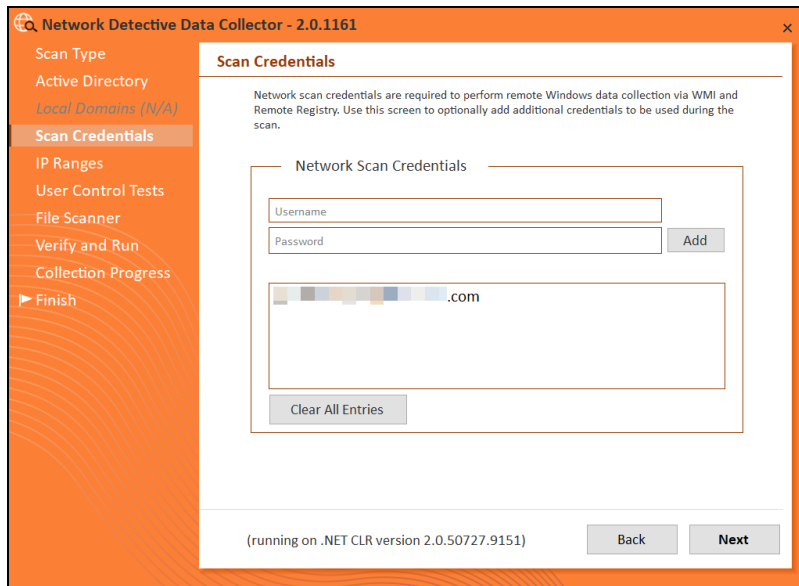


2. The **Active Directory** window will appear. Select the type of network you are scanning (*Active Directory domain* or *Workgroup*).

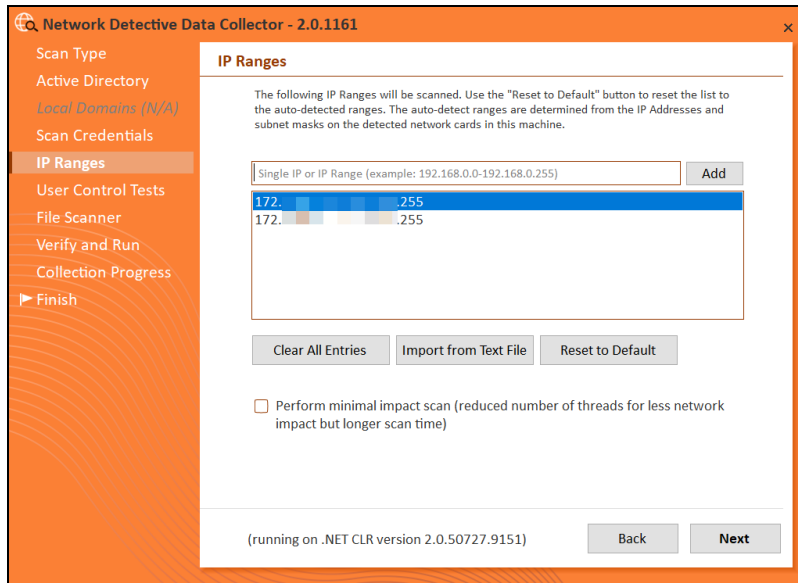


3. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator. Then click **Next**.

**Important:** If each workgroup PC has its own unique Admin username and password credentials, you will need to enter each set of credentials here in order to scan all of these PCs.



4. The **IP Ranges** screen will then appear. The Network Detective Data Collector will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

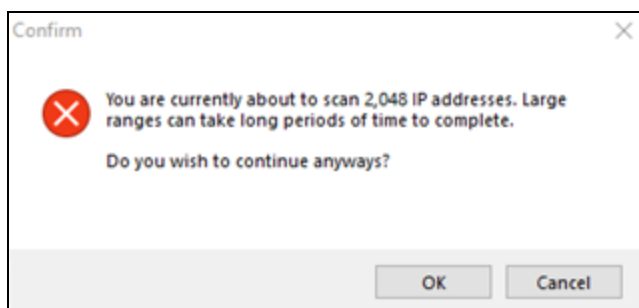


From this screen you can also:

- Click **Reset to Default** to reset to the automatically suggested IP Range.
- Click **Import from Text File** to import a predefined list or range of IP addresses.

**Important:** Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

When you have entered all IP Ranges to scan, click **Next**.

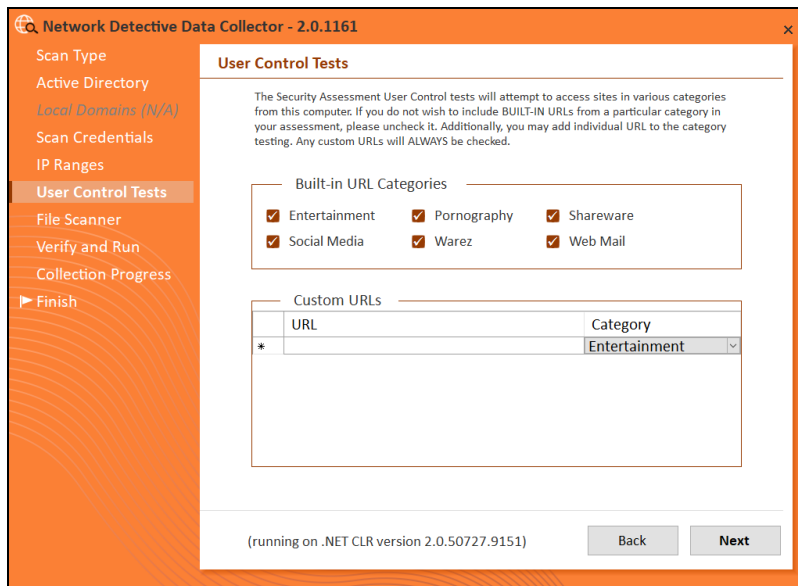


**Important:** If you are scanning a large number of IP addresses, confirm that you wish to continue. Consider performing multiple scans on smaller IP ranges. You

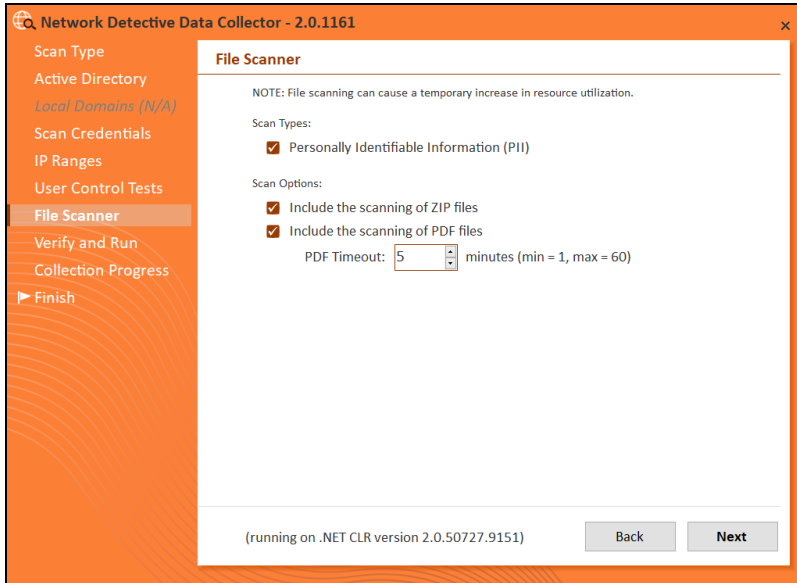


can then upload each "batch" of scan files into the assessment, where they will be merged for complete results.

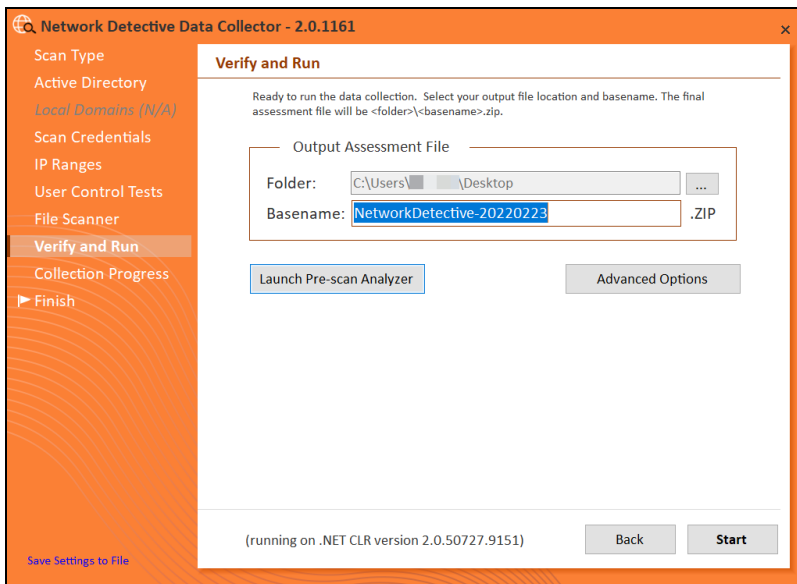
5. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your own custom URLs and categories to test. Then click **Next**.



6. The **File Scanner** screen will appear. Choose whether to scan for PII (Personally Identifiable Information) and click **Next**.



7. The **Verify and Run** window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan’s **Output Assessment File Folder** location and **Basename** for the scan data. The file will be output as a **.NDF** file.

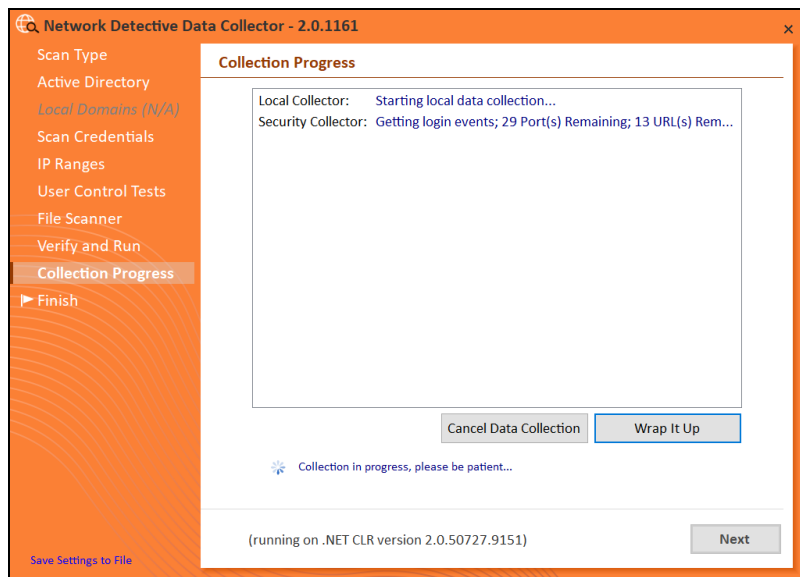


**Tip:** Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion of the pre-scan.

Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above installed	Status
APP01-CORPBRAPDIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORP.RAP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-995DFE1.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HM0E7L.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4Q8O.CORP...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORP.R...	10.236.83.1...	✓	?			Accessing WMI...
DESKTOP-7RF9K75.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.

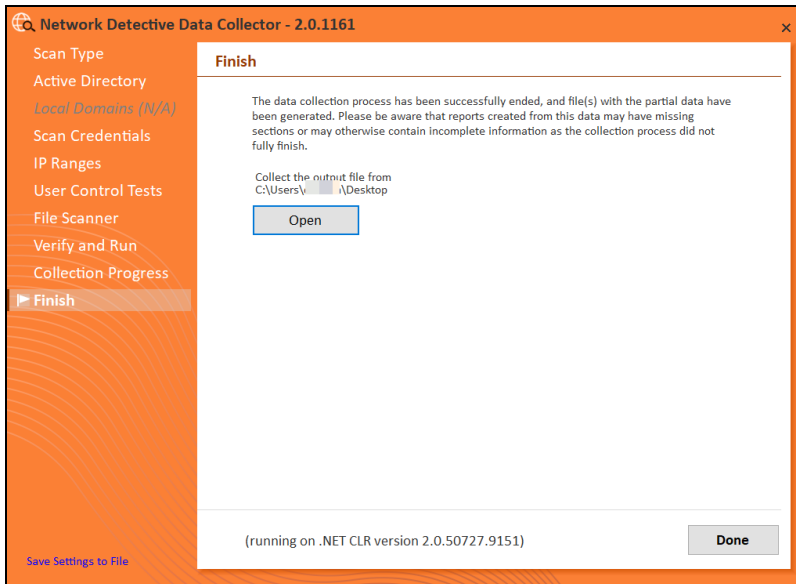
Enter any **Comments** and then click **Start**.

- The **Collection Progress** window will appear. 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 appear. 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 **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

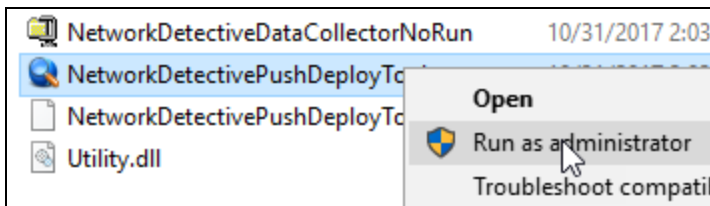
## Step 6 — Use the Push Deploy Tool to Collect Remaining Data

**Tip:** The **Push Deploy Tool** performs a localized scan on each workstation on the target network. **Perform this required step** to gather maximum data for the most detailed reports.

Download and run the Push Deploy Tool on a PC on the target network. Use it to perform local data scans on all computers.

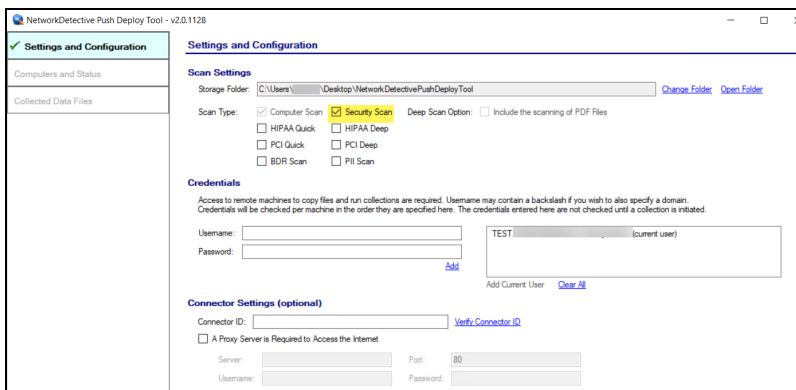
1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/nd> and download the Push Deploy Tool.
2. **Unzip** the files onto a USB drive or directly onto any machine on the target network.

- From within the unzipped folder, run the **NetworkDetectivePushDeployTool.exe** executable program as an Administrator (**right click>Run as administrator**).



**Important:** For the most comprehensive scan, you **MUST** run the Push Deploy Tool as an **ADMINISTRATOR**.

The Push Deploy Tool Settings and Configuration window will appear.



- You can optionally perform a PII (Personal Identifiable Information) Scan as part of your Security Assessment. This will result in more detail regarding the presence and location of PII on the network, such as in the Data Breach Liability Report. See ["Data Breach Liability Scanning and Reporting" on page 42](#) for more details.
- Set the **Storage Folder location** and select the **Security Scan** option.

**Tip:** For your convenience, create a shared network folder to centralize and store all scan results data files created by the **Push Deploy Tool**. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

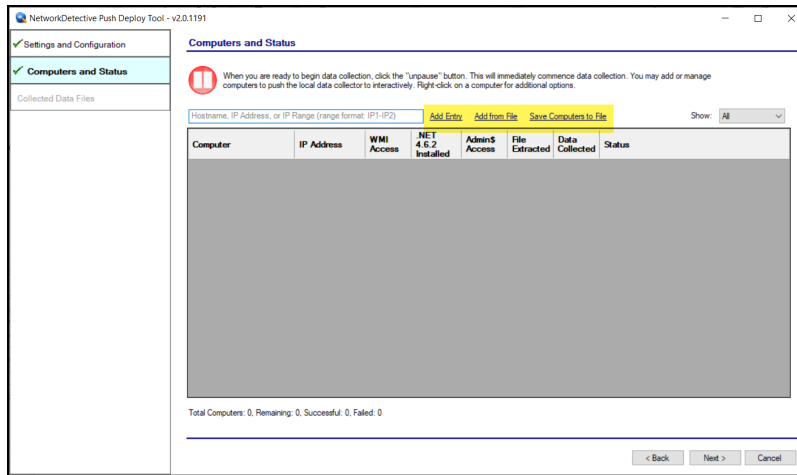
If additional credentials are required, type in the administrator level **Username** and **Password** necessary to access the local computers on the network to be scanned. Then click **Add**.

**Important:** For the **Push Deploy Tool** to push local scans to computers throughout the network, ensure that the following prerequisites are met:

- **Ensure that the Windows Management Instrumentation (WMI) service is running** and able to be managed remotely on the computers that you wish to scan. Sometimes Windows Firewall blocks Remote Management of WMI, so this service may need to be allowed to operate through the Firewall.
- **Admin\$ must be present on the computers you wish to scan**, and be accessible with the login credentials you provide for the scan. Push/Deploy relies on using the Admin\$ share to copy and run the data collector locally.
- **File and printer sharing must be enabled** on the computers you wish to scan.
- **For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same.** In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials box.

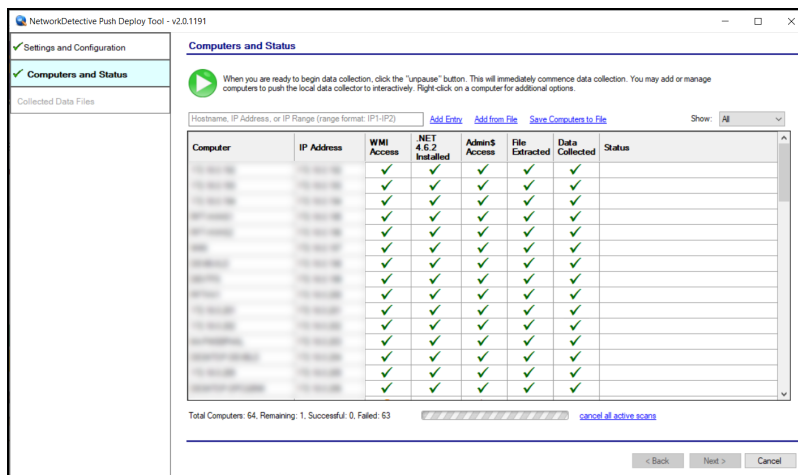
6. Click **Next** after you have configured the Push Deploy Tool.
7. The **Computers and Status** window will appear. From here you can:
  - **Add Entry** to be scanned (Add single IP or IP range)
  - **Add (computers) from File** that are to be scanned
  - Or **Save Computers to File** in order to export a list of computers to be

scanned again in future assessments



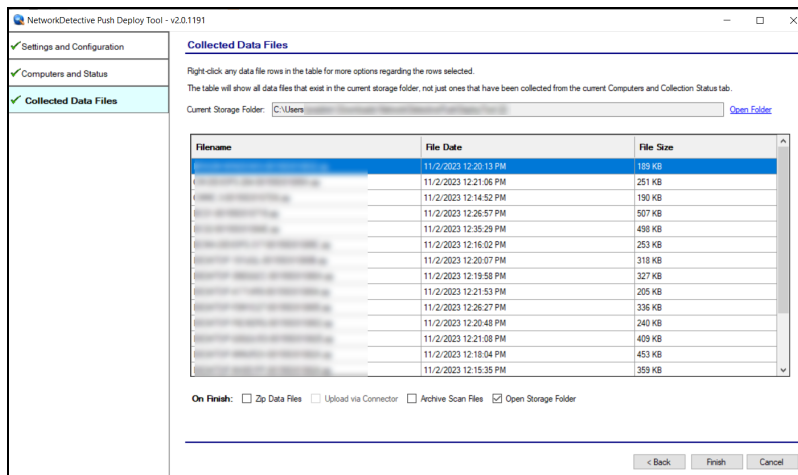
After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the **Computers and Status** window.

8. Start the scan either by selecting the **“unpause”** button in the **Computer and Status** window, or, by selecting the **Next** button in the **Computer and Status** window and the scan will be initiated. The status of each computer’s scan activity will be highlighted within the **Computers and Status** window as presented below.



Upon the completion of all of the scheduled scans, the scan data collected is stored within the **Storage Location** folder presented in the **Collected Data Files** window of the **Push Deploy Tool**.

- To verify the inclusion of the scan data produced by the **Push Deploy Tool** within your assessment, select the **Next** button within the **Push Deploy Tool**. The **Collected Data Files** window will be displayed.



- To review or access the files produced by the **Push Deploy Tool's** scans, select the **On Finish: Open Storage Folder** option in the **Collected Data Files** window. Then click **Finish**.

#### MORE INFO:

The Push Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.

The output files (.ZIP, files) from the local scans can be stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.

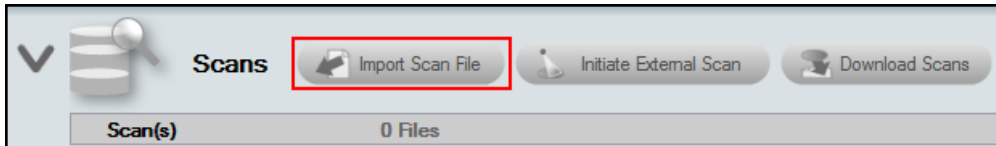
After all of the **Security Scans** are complete, the next phase in the process is to import the scan data files produced by the **Security Scan** into the current assessment.



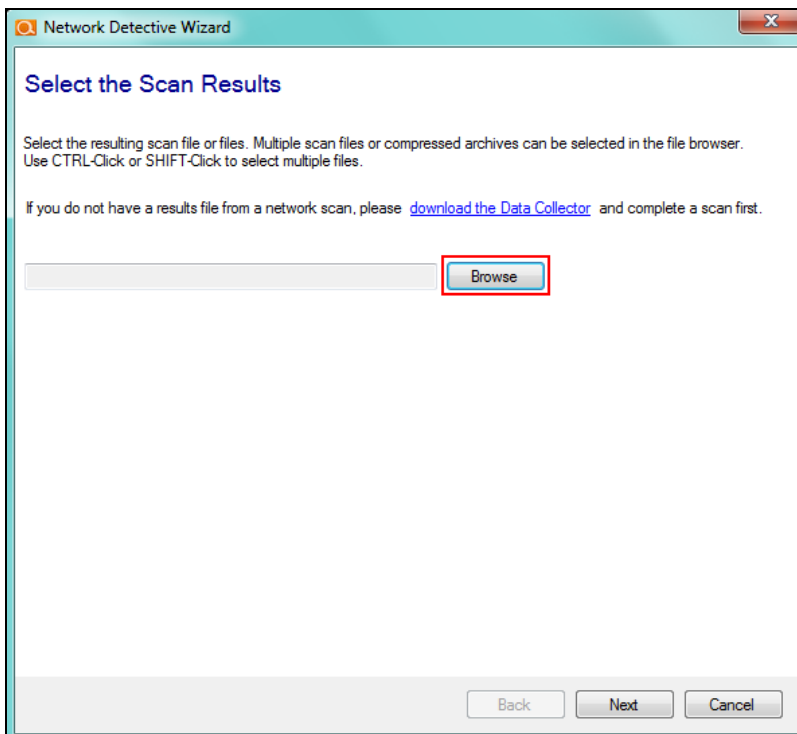
## Step 7 — Import Scans into Network Detective App

Make sure you can access all of the scan data files from the PC on the MSP network where you have Network Detective installed. Then, import the data collected by the Data Collector into the assessment.

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

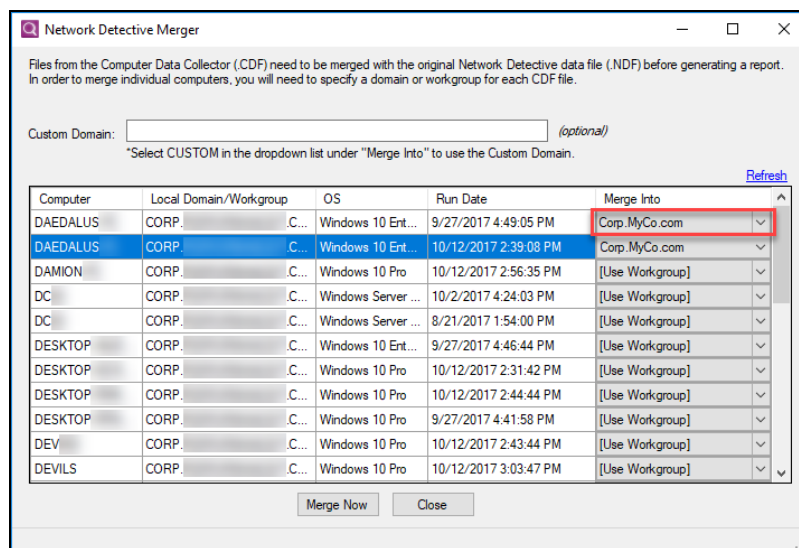


The **Select the Scan Results** window will be displayed.



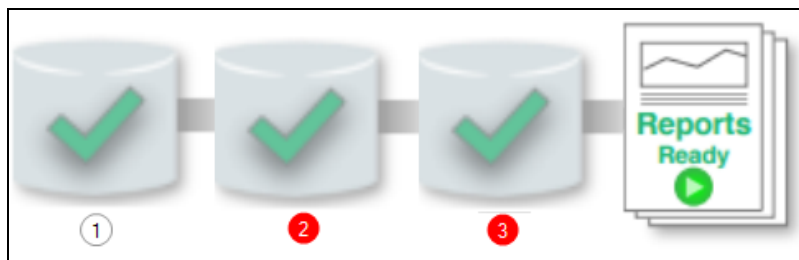
2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. For a Security Scan, these will be:

- .cdf file for the computer scans
  - .sdf file for the security data scans
  - .ndf file for the network scans
4. Click **Open** button to import the scan data. Then click **Next**.
  5. An archived copy of the scan will be created in the Network data directory. You can access this at **%APPDATA%\NetworkDetective\** on your PC. Click **Finish**.
    - i. *If prompted*, use the **Network Detective Merger** to merge the data file(s) into the assessment. Select the Domain into which the file will be merged. Click **Merge Now**.



The **Scans** bar will be updated with the imported scan files.

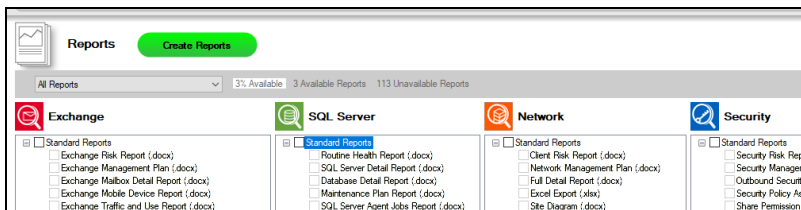
Once all of the scan data is imported into the **Assessment**, the assessment's **Checklist** will indicate that the **Reports** are ready to be generated.



## Step 8 — Generate Security Assessment 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-downloads> if you have not already done so. To generate the reports for your Security Assessment, follow the steps below:

1. Run Network Detective and log in with your credentials.
2. Then select the **Site**, go to the **Active Assessment**, and then select the **Reports** link to the center of the **Assessment Window** in order select the reports you want to generate.



3. Select the **Create Reports** button and follow the prompts to generate the reports you selected.
4. At the end of the report generation process, the generated reports will be made available for you to open and review.

# Security Assessment Reports

The **Security Assessment** allows you to generate the following reports:

## Standard Reports

Report Name	Description
<b>Anomalous Login Report</b>	The Anomalous Login Report shows suspicious logins by user and computer based on various probability criteria. The includes: A) logins into specific computers users don't normally log into, and B) logins by users outside of their regular pattern (not only by day of week, but also by time of day).
<b>Consolidated Security Report Card</b>	The Computer Security Report Card assesses individual computers at a high level based on various security criteria. Devices discovered on the network are assigned an overall score, as well as a specific score for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F'). The report card should be viewed as a relative measure as to how well a computer complies with security best practices. There may be specific reasons or compensating controls that may make it unnecessary to achieve an "A" in all categories to be considered secure.
<b>Cyber Liability and Data Breach Report</b>	Identifies specific and detailed instances of personal identifiable information (PII) and cardholder data throughout a computer network that could be the target of hackers and malicious insiders. It also calculates the potential monetary liability and exposure based upon industry published research.
<b>Data Breach Liability Report</b>	Small and midsize businesses need to manage their exposure to the financial risk that accompanies cyber threats. Data breaches come in many shapes and sizes. The average person hears "data breach" and probably thinks of hackers. But there are many kinds of cyber incidents, and most don't come from malware or ransomware. Instead they are the result of insider data breaches, data theft by employees, and employee mistakes. A breach is an event in which an individual's name plus a medical, financial, debit/credit card and other personal or sensitive information is potentially put at risk in electronic form. A compromised record is one that has been lost or stolen as a result of a data breach. The report not only identifies specific and detailed instances of personal identifiable information (PII) throughout your

Report Name	Description
	computer network that could be the target of hackers and malicious insiders but also calculates the potential monetary liability based upon industry published research.
<b>Data Breach Liability Report Excel</b>	Data Breach Liability Report in MS Excel format.
<b>External Network Vulnerabilities Summary Report</b>	This report provides a priority ordered listing of issues by their CVSS to enable technicians to prioritize the issues they are working on. This report provides an extremely compact view of all issues to provide a quick survey of the various issues that were detected in an environment.
<b>External Vulnerabilities Scan Detail Report</b>	A comprehensive output including security holes and warnings, informational items that can help make better network security decisions, plus a full NMap Scan which checks security holes, warnings, and informational items that can help you make better network security decisions. This is an essential item for many standard security compliance reports.
<b>External Vulnerability Scan Detail by Issue Report</b>	A more compact version of the External Vulnerability Scan Detail report that is organized by issues. Devices that are affected are listed within an issue type. This report is useful for technicians that are looking to resolve specific issues identified within the environment, rather than performing remediation on a particular system.
<b>External Vulnerability Scan Detail in Excel Format</b>	An Excel version of the External Vulnerability Scan Detail report listing issues by device.
<b>Internal Network Vulnerabilities Summary Report*</b>	The Internal Network Vulnerabilities Summary Report breaks down issues discovered during the internal scan, organized by risk severity. This report also details the affected endpoints and offers a brief recommended course of action for each issue. (*Requires Inspector)
<b>Internal Vulnerability Scan detail by Issue Report*</b>	This detailed report provides extensive data on each discovered internal vulnerability organized by issue type. This includes insight into the technical nature of each issue, a proposed solution, affected assets, as well as several graphical breakdowns of the numerical disposition of issues on the target network. (*Requires Inspector)

Report Name	Description
<b>Internal Vulnerability Scan Detail Excel*</b>	Internal vulnerability breakdown in MS Excel format.
<b>Internal Vulnerability Scan Detail Report*</b>	This detailed report provides extensive data on each discovered internal vulnerability organized by each affected asset. This includes insight into the technical nature of each issue, a proposed solution, as well as several graphical breakdowns of the numerical disposition of issues on the target network. (*Requires Inspector)
<b>Login Failures by Computer Report</b>	This report provides a list of systems that have had failed interactive and network login attempts along with a count of the number of failed logins over the past 1, 7 and 30 days. Use this to identify an employee who has forgotten their credentials. In an extreme scenario, the report may help you detect a hacker trying to enter the network through an employee's legitimate account, or an attempt to access a highly sensitive system such as the CEO's workstation.
<b>Login History by Computer Report</b>	Same data as User Behavior but inverted to show you by computer. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive machine for failed login attempts. An example would be CEO's laptop – or the accounting computer where you want to be extra diligent in checking for users trying to get in.
<b>Outbound Security Report</b>	Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet content accessibility.
<b>Resulting Set of Policies Reports</b>	This report analyzes the various Resulting Sets of Policy (RSOP) based on user settings on computers in the environment and helps point out commonalities in the sets and which users/computer combinations have the configurations applied. There are separate reports for both user settings and computer settings.
<b>Security Assessment PowerPoint</b>	Use our generated PowerPoint presentation as a basis for conducting a meeting presenting your findings from the Network Detective. General summary information along with the risk and issue score are presented along with specific issue recommendations and next steps.
<b>Security Health</b>	This report measures the overall risk to the environment by the number

Report Name	Description
<b>Report</b>	of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur. This report will also compare the results of a previous assessment with the current assessment.
<b>Security Management Plan</b>	Network Management Plan This report will help prioritize issues based on the issue's risk score. A listing of all security related risks are provided along with recommended actions.
<b>Security Policy Assessment Report</b>	A detailed overview of the security policies which are in place on both a domain wide and local machine basis.
<b>Security Risk Report</b>	This report includes a proprietary Security Risk Score and chart showing the relative health (on a scale of 1 to 10) of the network security, along with a summary of the number of computers with issues. This powerful lead generation and sales development tool also reports on outbound protocols, System Control protocols, User Access Controls, as well as an external vulnerabilities summary list.
<b>Share Permission Report</b>	Comprehensive lists of all network “shares” by computer, detailing which users and groups have access to which devices and files, and what level of access they have.
<b>Share Permission Report by User</b>	Comprehensive lists of all network “shares” by user. Each subsection details the share and file system permissions granted to each user account within the above domain.
<b>Share Permission Report by User Excel</b>	Comprehensive lists of all network “shares” by user in MS Excel format.
<b>Share Permission Report Excel</b>	Comprehensive lists of all network “shares” by computer in MS Excel format.
<b>User Behavior Analysis Report</b>	Shows all logins, successful and failure, by user. Report allows you to find service accounts which are not properly configured (and thus failing to login) as well as users who may be attempting (and possibly succeeding) in accessing resources (computers) which they should not be.

Report Name	Description
<b>User Permissions Report</b>	Organizes permissions by user, showing all shared computers and files to which they have access.

## Infographics

Report Name	Description
<b>Password Policies Summary</b>	This report provides a risk assessment of logins that are not following best practices against security intrusions. For the most common mitigation practices, the report details which logins currently present a risk to intrusion. This allows readers to quickly understand where immediate action is required.
<b>Data Breach Liability Summary</b>	This report provides a risk assessment of systems with one or more potential security liabilities. For the most common liabilities, the report details the estimated cost of breach and the worst offending systems. This allows readers to quickly understand where immediate action is required.

## Change Reports

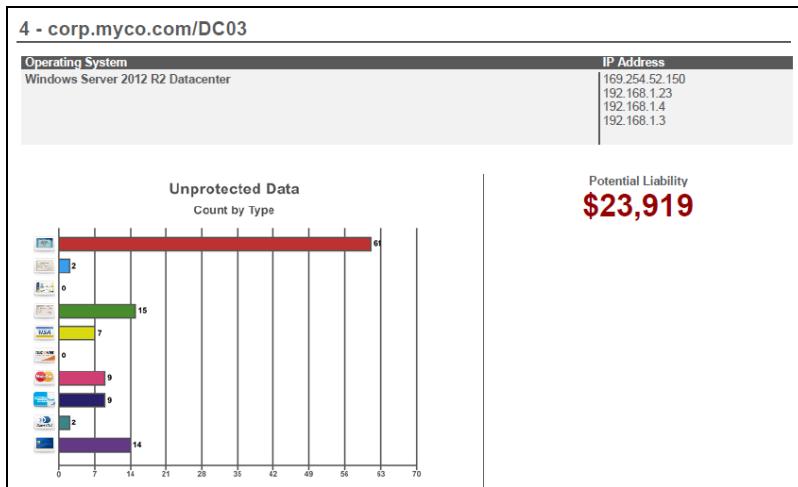
Report Name	Description
<b>Baseline Security Health Report</b>	This report measures the overall risk to the environment by the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur. This report will also compare the results of a previous assessment with the current assessment.
<b>Baseline Security Management Plan</b>	The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the Overall Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first. This report will also compare the results of a previous assessment with the current assessment.
<b>Baseline</b>	This report details the Risk Score for both the current and previous



Report Name	Description
<b>Security Risk Report</b>	assessment, focusing in particular on security issues and vulnerabilities. At the same time, the report breaks down each issue and conveys whether the issue is increasing or decreasing in risk level. For example, are your computers missing more or fewer security patches since the previous assessment? This report will tell you.
<b>Login Failures by Computer Change Report</b>	Compares the results of the current and previous login failures report by computer.
<b>Login History by Computer Change Report</b>	Compares the results of the current and previous login history by computer.
<b>User Behavior Analysis Change Report</b>	Compares the results of the current and previous user behavior analysis.

# Data Breach Liability Scanning and Reporting

The **Data Breach Liability Report** helps you assess and manage your financial exposure to a cyber security incident. The report identifies specific and detailed instances of *personal identifiable information* (PII) throughout your computer network that could be the target of hackers and malicious insiders.



At the same time, the report calculates the potential monetary liability based upon industry published research.

**RISK SUMMARY**

**Total Potential Liability**  
**\$149,142**

Computer	IP Address	Missing Critical Patches	Anti-virus/ Anti-spyware	Sensitive Data Count	Potential Liability (\$)
corp.myco.com/darkhorse	169.254.24.150 169.254.58.236 192.168.6.80	0	✓	623	\$125,223
corp.myco.com/DC03	169.254.52.150 192.168.1.23 192.168.1.4 192.168.1.3	0	✓	119	\$23,919

The Data Beach Liability Report anomalously details specific types of detected PII, including:

- Visa card
- Mastercard
- Discover Card

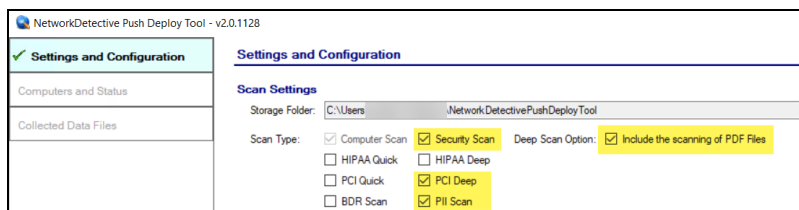
- Diners Club United States & Canada
- Mastercard Diners Club Alliance
- American Express
- Date of Birth
- SSN
- Drivers License
- ACH (bank transfer information)

In order to collect this PII and generate the most detailed Data Breach Liability Report, you need to perform a couple of extra scans during your Security Assessment. This topic details the extra steps you should take to get the most out of your report.

## Steps to Perform Scans to Identify PII and Generate the Data Breach Liability Report

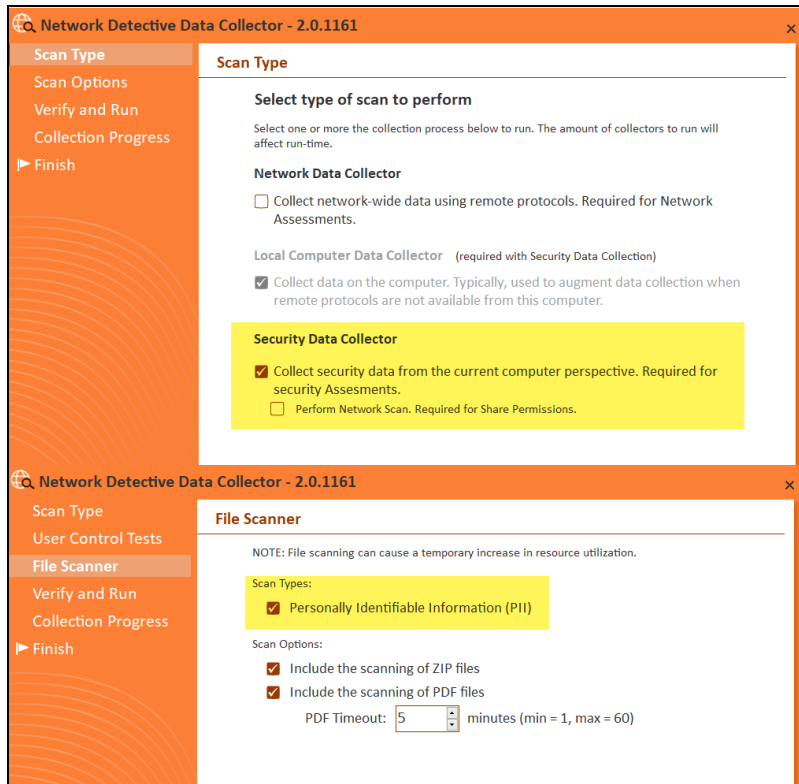
You can perform the extra scans needed for a complete Data Breach Liability Report as part of a normal Security Assessment. To do this:

1. Use the Network Detective Data Collector to perform a network scan.
2. Next, use the Push Deploy Tool to perform the **Push Deploy Scan**. When you configure the scan, select the following scans settings: **Computer Scan**, **Security Scan**, **PII Scan**, and **PCI scan**.



**Note:** Also select whether you want to scan PDF files. Note that this may significantly increase total scan time.

3. For computers that cannot be scanned using the Push Deploy Tool, use the Network Detective Data Collector to perform a local Security Scan. Be sure to select to scan for PII on the File Scanner screen when configuring the data collection.



- Then, import the scan data into your assessment. You can then generate the Data Breach Liability Report with complete PII scan details.

