NETWORK DETECTIVE™

USER GUIDE

HIPAA Compliance Assessment Module

Instructions to Perform a HIPAA Compliance Assessment

11/2/2023 5:01 PM

Contents

About the Network Detective HIPAA Assessment Module **4**

Introduction to HIPAA Assessment Module **5**

HIPAA Compliance Assessment Overview 5

What You Will Need 6

Risk Assessment vs. Risk Profile 7

HIPAA Risk Profile Use for Ongoing HIPAA Compliance Assessments 7

Using the Security Exception Worksheet to Address Compliance Lapses and False Positives 8

Setting up your HIPAA Compliance Assessment Project **9**

Download and Install the Network Detective Application 9

Create a New Site 10

Start a HIPAA Compliance Assessment Project 11

Use the HIPAA Compliance Assessment Checklist 12

Performing a HIPAA Compliance Assessment **13**

Collect Initial HIPAA Compliance Assessment Data 13

Step 1 — Complete the HIPAA On-Site Survey 13

Step 2 — Initiate External Vulnerability Scan 17

Step 3 — Run HIPAA Data Collector selecting the Network Scan option 19

Scanning an Active Directory Domain Network 20

Scanning a Workgroup Network 28

Import the Scan Data from Data Collector into the HIPAA Compliance Assessment Project 36

Step 4 — Run HIPAA Data Collector selecting the Local Computer option on all Workstations/Servers/Laptops 39

Import the Scan Data from Push Deploy Tool into the HIPAA Compliance Assessment Project 46

Step 4.1 — Run the HIPAA Data Collector Local Scan on Computers that could not be accessed by the Push Deploy Tool 48

Import the Scan Data from Data Collector into the HIPAA Compliance Assessment Project 52

Collect Secondary HIPAA Data and Document Exceptions 55
Step 5 — Complete Inactive Computer Identification Worksheet 55
Step 6 — Complete User Identification Worksheet 57
Step 7 — Complete Computer Identification Worksheet 59
Step 8 — Complete Network Share Identification Worksheet 61
Step 9 — Complete Security Exception Worksheet (Optional) 63
Generate HIPAA Compliance Assessment Reports 67
Note on Time to Generate Reports 68
HIPAA Assessment Reports 69
Compliance Reports 69
Supporting Documentation 72
Change Reports 74
Appendices 75
Pre-Scan Network Configuration Checklist 76
Checklist for Domain Environments 76
Checklist for Workgroup Environments 78
Completing Worksheets and Surveys 80
Entering Assessment Responses into Surveys and Worksheets 80
Add Image Attachments to Surveys and Worksheets 82
Add SWOT Analysis to Surveys and Worksheets 82
Time Savings Tip to Reduce Survey and Worksheet Data Input Time 83
Use the InForm Worksheet Tool Bar 83
Bulk Entry for InForm Worksheets 84
Create Word Response Form 86
Important Note on Working with Word Response Forms 87
Import Word Response Form 88
Adding an Inspector to a Site 89
Site Assessment Reports and Supporting Documents Locations 91
Initiate Internal Vulnerability Scan on the Inspector Appliance and Download Results 94
Download Appliance Scans 99

About the Network Detective HIPAA Assessment Module

HIPAA is a risk-based compliance framework, with a Risk Assessment being the first requirement in the HIPAA Security Rule. The Risk Assessment must identify the vulnerabilities to the security of electronic Protected Health Information (ePHI). This includes threats that can act on the vulnerabilities, including the likelihood and the impact if that occurs.

Network Detective's HIPAA Compliance module is the first professional tool to combine and integrate automated data collection with a structured framework for collecting supplemental assessment information not available through automated tools.

It is the first solution to allow for the automatic generation of the key documents that are necessary to demonstrate compliance with the Security Rule. It includes comprehensive checklists that cover the Administrative, Physical, and Technical safeguards defined in the HIPAA Security Rule. More than just documents to satisfy a compliance requirement, Network Detective provides factual evidence, expert advice, and direction to minimize or eliminate the risk of a data breach.

You can compare Network Detective's HIPAA Compliance module to getting a medical exam. Network Detective automates the 'lab tests' for the technology environment. It includes interview and survey features to gather information manually. In addition, it provides a recommended treatment plan.

Introduction to HIPAA Assessment Module

This section covers everything you need to know before getting started with your HIPAA Assessment.

HIPAA Compliance Assessment Overview

Network Detective's HIPAA Compliance Assessment Module combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a HIPAA Compliance Assessment, you will:

- Download and install the required tools
- Create a site and set up a HIPAA Compliance Assessment project
- Collect HIPAA Compliance Assessment data using the Network Detective Checklist
- Generate HIPAA Compliance Assessment reports

What You Will Need

In order to perform a HIPAA Compliance Assessment, you will need the following components:

Note: You can access these at https://www.rapidfiretools.com/nd.

HIPAA Compliance Assessment Component	Description
Network Detective	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.
HIPAA Data Collector	The Network Detective HIPAA Data Collector is a windows application that performs the data collections for the HIPAA Compliance Module. Supports both the Network and Computer scans.
Push Deploy Tool	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.
Surveys and Worksheets	Surveys and worksheets contain questions that require investigation outside of an automated scan. You create and manage these documents directly from the Network Detective Application, where you can also import and export your responses to and from Word.

Risk Assessment vs. Risk Profile

There are two types of HIPAA Compliance Assessments that can be performed:

Assessment Type	Description
HIPAA Risk Assessment	A complete assessment that includes all worksheets and surveys. • Required at least annually • Recommended quarterly as part of a quarterly compliance review • Requires that all manual worksheets be completed **Important:** Allow for at least an entire day to perform the assessment on a typical 15 user network
HIPAA Risk Profile	Updates a Risk Assessment to show progress in avoiding and mitigating risks - and finds new ones that may have otherwise been missed. • Does NOT require worksheets • Requires selecting a prior Risk Assessment (will use existing worksheets) • Requires less than 1 hour for a typical 15 user network **Note:** You can only create a Risk Profile after you have first performed a Risk Assessment.

HIPAA Risk Profile Use for Ongoing HIPAA Compliance Assessments

A HIPAA Risk Analysis should be done no less than once a year. However, the Network Detective includes an abbreviated version of the HIPAA Risk Analysis assessment and reporting process within the Network Detective HIPAA Module. This process is called the HIPAA Risk Profile.

The HIPAA Risk Profile is designed to provide interim reporting in a streamlined and almost completely automated manner.

Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.

An important aspect of this abbreviated process is the need that the HIPAA Module has been already used to perform a HIPAA Risk Assessment of your customer's network on a previous occasion.

Using the Security Exception Worksheet to Address Compliance Lapses and False Positives

Sometimes you may get stuck in an assessment. This might happen for several reasons:

- You cannot resolve every single compliance issue identified in the assessment
- Your scan results differ from what you know is the reality on the target network
- You do not have enough information to enter accurate responses for every form question

If you encounter any of the above, you can always move ahead and complete your assessment using the **Security Exception Worksheet**. This worksheet becomes available near the end of your To Do list. It allows you to document explanations on suspect items. Your explanation can include why various discovered items are not true issues and indicate possible false positives. Additionally, you can explain why a certain compliance requirement should not apply to you – or an alternative way in which you have met the requirement.

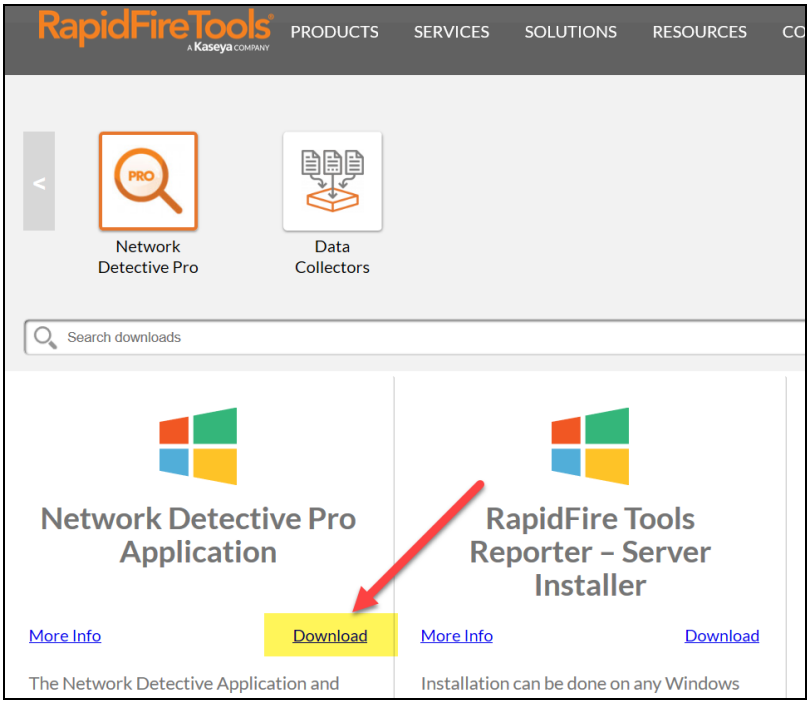
These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The **Security Exception Worksheet** does not alleviate the need for safeguards but allows for description of alternative means of mitigating the identified security risk.

Setting up your HIPAA Compliance Assessment Project

Download and Install the Network Detective Application

Visit https://www.rapidfiretools.com/nd. Download and install the Network Detective Application.

Important: Do not install the Network Detective Application on your client's network. Only the various **Data Collectors** are run on your client's network and computers.



Always accept the prompt to update Network Detective to the latest version.

When you run Network Detective for the first time, it will launch the Network Detective Wizard. You can dismiss the wizard and proceed to create a New Site. Sites are used to manage your customers' IT Assessment Projects.

Note: We recommend you use Sites to manage the assessments you perform for your clients. Sites help organize the scans you perform on your clients' networks and computers.

Create a New Site

The first step in the assessment is creating a “Site”. All Network Detective assessments are organized into Sites. A Site can be a physical location or a logical grouping, such as a customer account name.

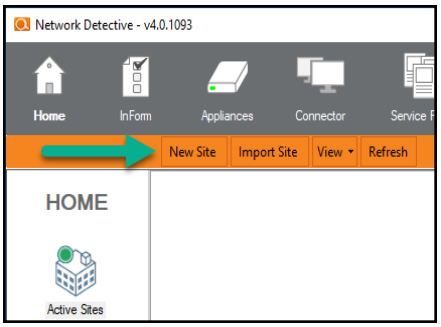
Before making a selection, you must decide on your assessment strategy. For example:

A. For a single location, create one Site.
B. For organizations with multiple locations, decide if you want one set of reports, or separate reports for each location.

> **Note:** Reports are generated on a Site by Site basis.

To create a new Site:

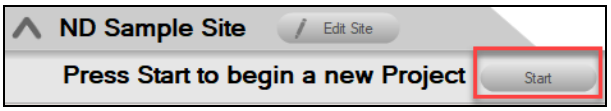
1. Open the Network Detective Application and log in with your credentials.
2. Click **New Site** to create a new Site for your assessment project.



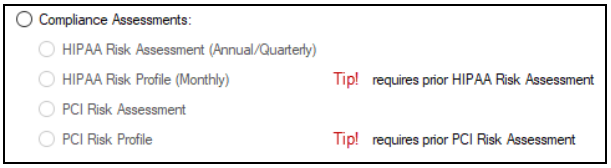
3. Enter a **Site Name** and click **OK**.

Start a HIPAA Compliance Assessment Project

1. From within the Site Window, click **Start** to begin the assessment.



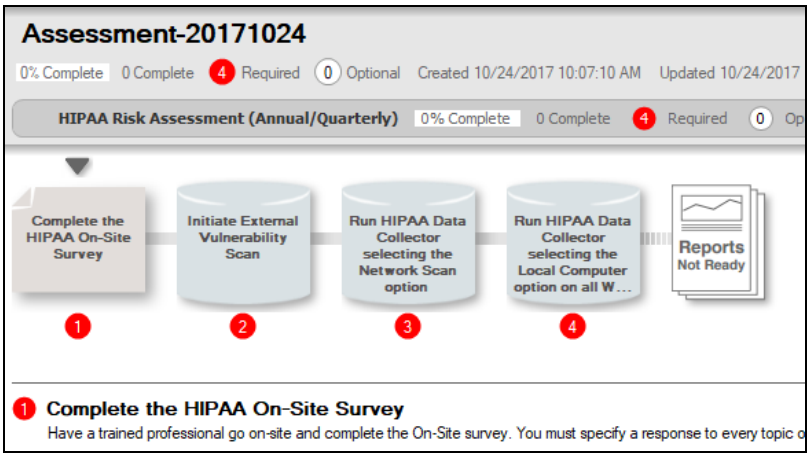
2. Next, select **Compliance Assessments**, and then select your chosen HIPAA Compliance Assessment.



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

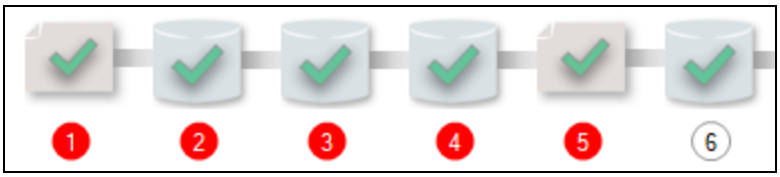
Use the HIPAA Compliance Assessment Checklist

Once you begin the HIPAA Compliance Assessment, a **Checklist** appears in the Assessment Window. The **Checklist** presents the **Required** 1 and **Optional** 1 steps that are to be performed during the assessment process. The **Checklist** will be updated with additional steps to be performed throughout the assessment process.



Complete the required **Checklist Items** in the exact numerical order presented. Use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

When you complete a step, that item will be updated with a green check mark in the checklist.



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

Performing a HIPAA Compliance Assessment

To perform a HIPAA Compliance Assessment, complete the steps detailed in this guide.

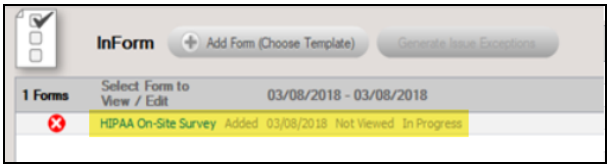
Collect Initial HIPAA Compliance Assessment Data

Step 1 — Complete the HIPAA On-Site Survey

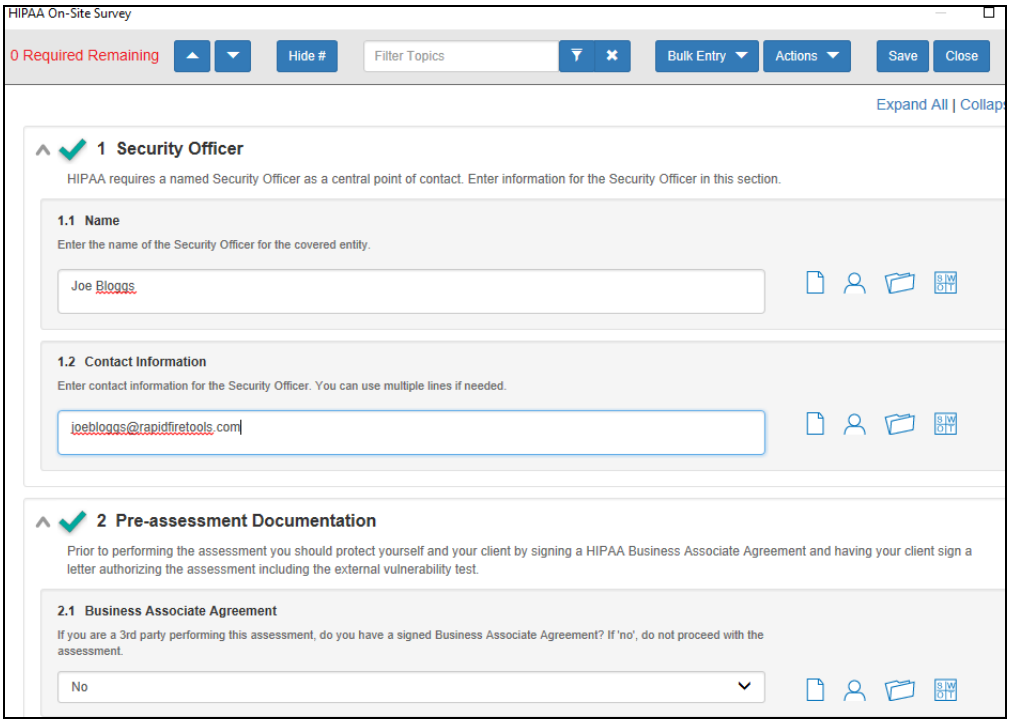
The **On-Site Survey** is the first part of the HIPAA Compliance Assessment process. To complete the on-site survey:

1. Double click on the **Complete the HIPAA On-Site Survey** item within the checklist.

   Or you can click on the HIPAA On-Site Survey in the InForm Bar located at the bottom of the Assessment Window.



HIPAA On-Site Survey will appear.

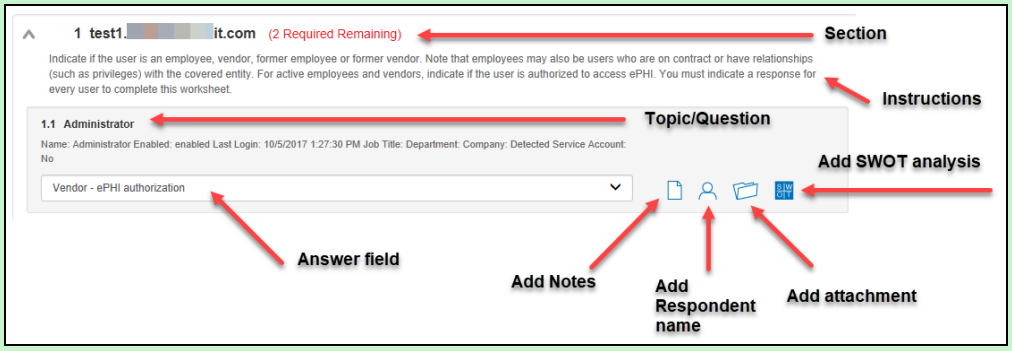


2. Complete each required item within the worksheet.

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 HIPAA Compliance 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" on page 82 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 page 82 for more details.

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

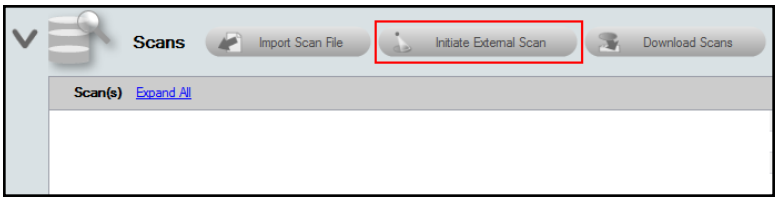
To return to the questionnaire, double click on the icon in the Checklist, or click on the item within the InForm Bar.

Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

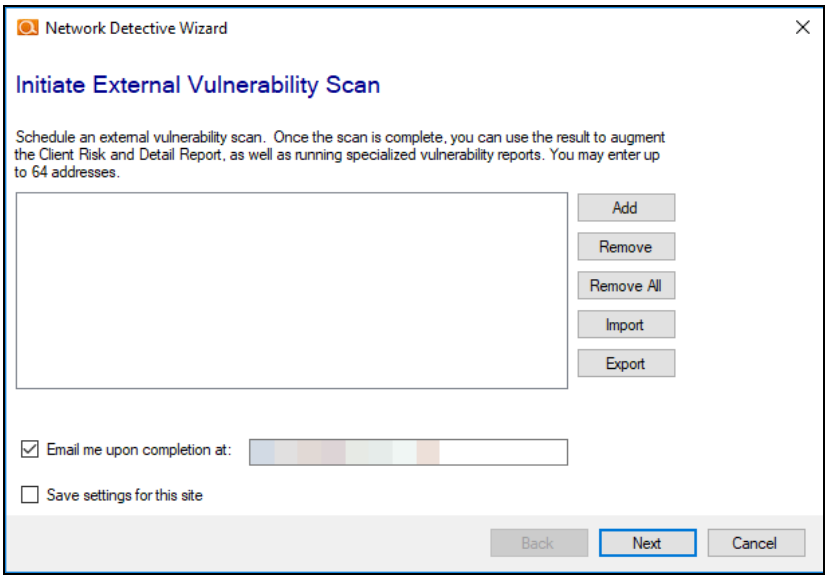
Step 2 — Initiate External Vulnerability Scan

To configure and start the External Vulnerability Scan:

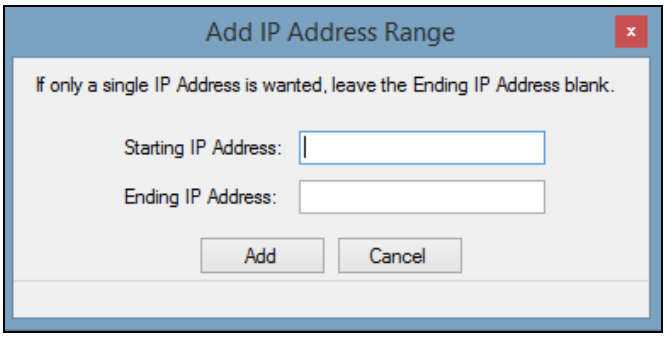
1. From the **Scans Bar** located at the bottom of the Assessment Window, click **Initiate External Scan**.



2. In the **Network Detective Wizard** window, enter the range of IP addresses you would like to scan. **You can enter up up to 64 external addresses**.



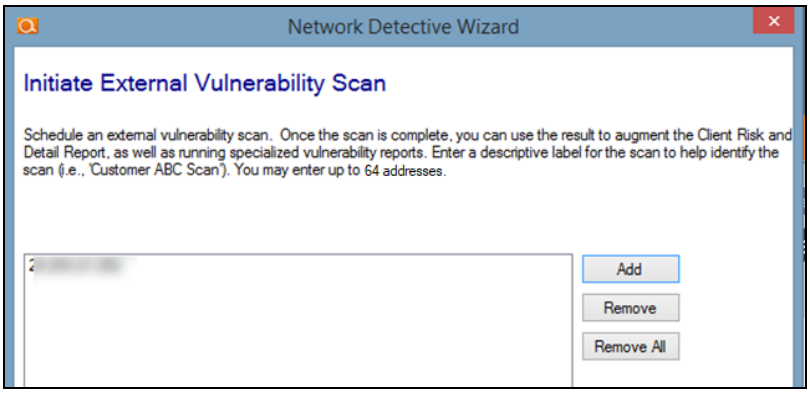
3. Click **Add** to add a range of external IP addresses to the scan.



Tip: If you do not know the external range, you can use websites such as whatismyip.com to determine the external IP address of a customer.

4. Enter the IP range for the scan. If only a single IP Address is wanted, leave the Ending IP Address blank.

Tip: 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.

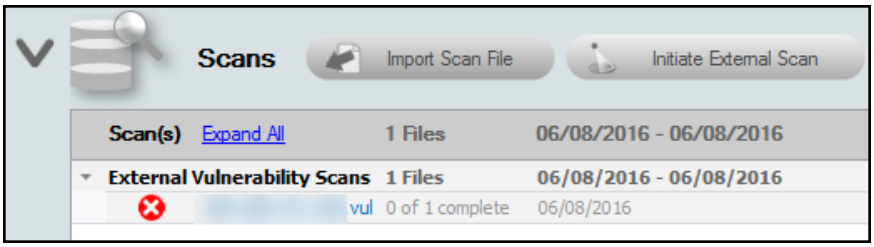


5. In the **Initiate External Vulnerability Scan** window, enter an email address to be notified when the scan is completed.
6. Click **Next** to send the request to the servers that will perform the scan.

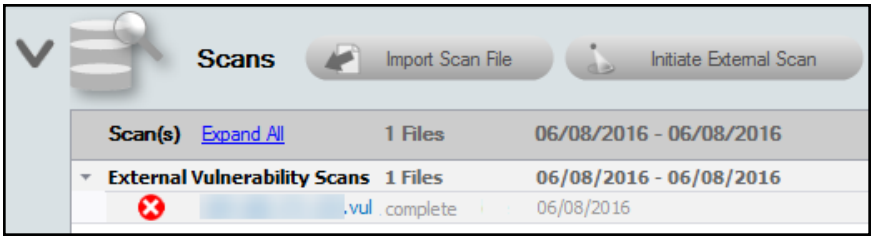
Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several

hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Scans can take several hours to complete. You will receive an e-mail when the scan is complete. Note that the **Assessment Window** will be updated to reflect the **External Vulnerability Scan** has been initiated. Refer to the list under the **Scans Bar** located within the **Assessment Window** as detailed in the figure below.



The scan's status of **0 of 1 complete** will be updated to **complete** once the scan is completed. You will also receive an email notification. The External Vulnerability Scan's **"complete"** status is shown below.



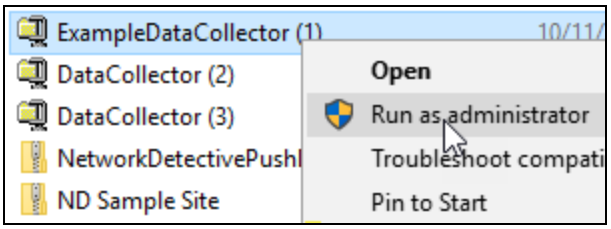
Step 3 — Run HIPAA Data Collector selecting the Network Scan option

In this step, you will perform a network scan on the target network using the HIPAA Data Collector. This scan can be performed from any computer connected to the network. For more information on network prerequisites to ensure a successful scan, see "Pre-Scan Network Configuration Checklist" on page 76.

- Look here if you are "Scanning an Active Directory Domain Network" on the facing page
- Look here if you are "Scanning a Workgroup Network" on page 28

Scanning an Active Directory Domain Network

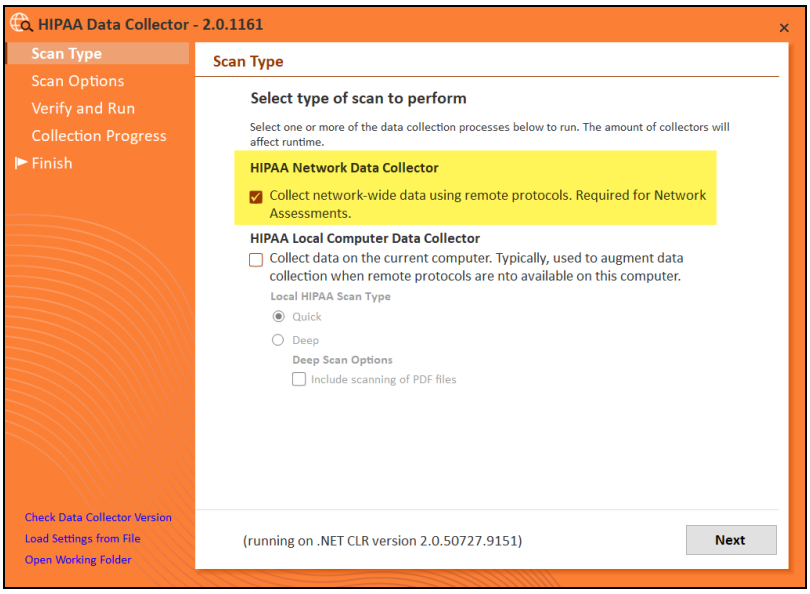
1. Visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the HIPAA Data Collector.
2. Run the **HIPAA Data Collector** executable program as an Administrator (**right click>Run as administrator**).



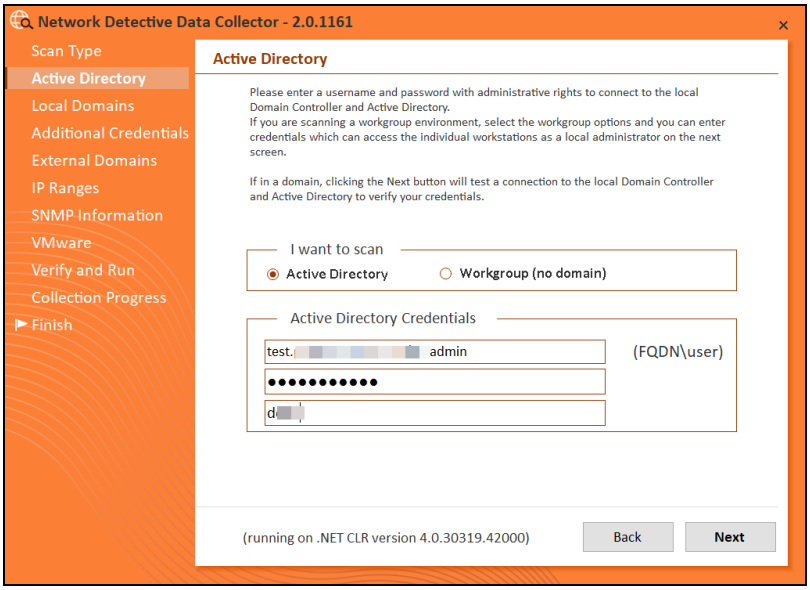
Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

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

   Select the **HIPAA Network Data Collector** option. Click **Next**.



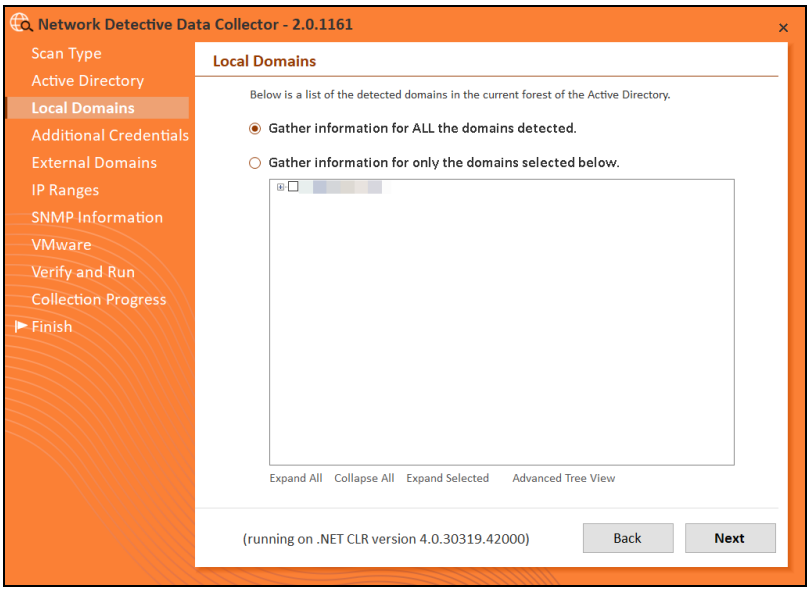
5. The **Active Directory** window will appear. Select the type of network you are scanning (*Active Directory domain*).



6. 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.

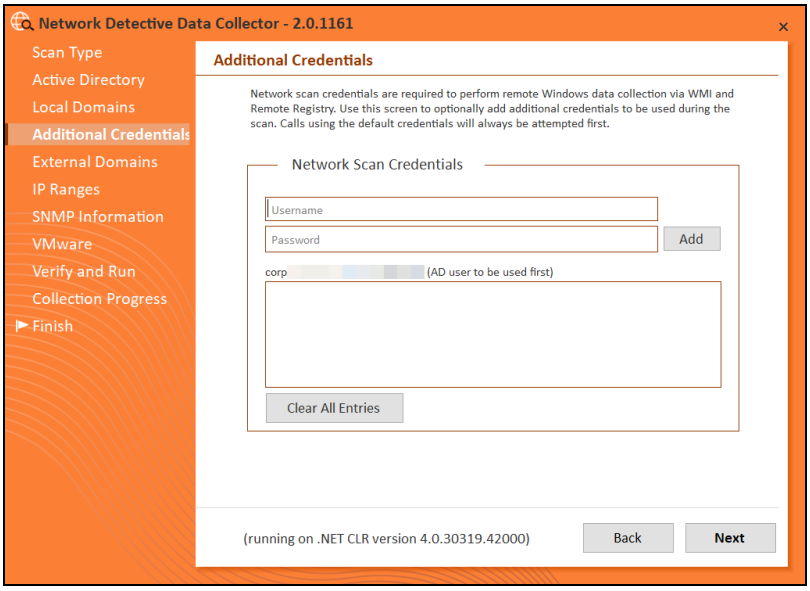
> **Note:** For example: **corp.yourclient.com\username.**

7. Enter the **name or IP address** of the **Domain Controller**.
8. 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**.

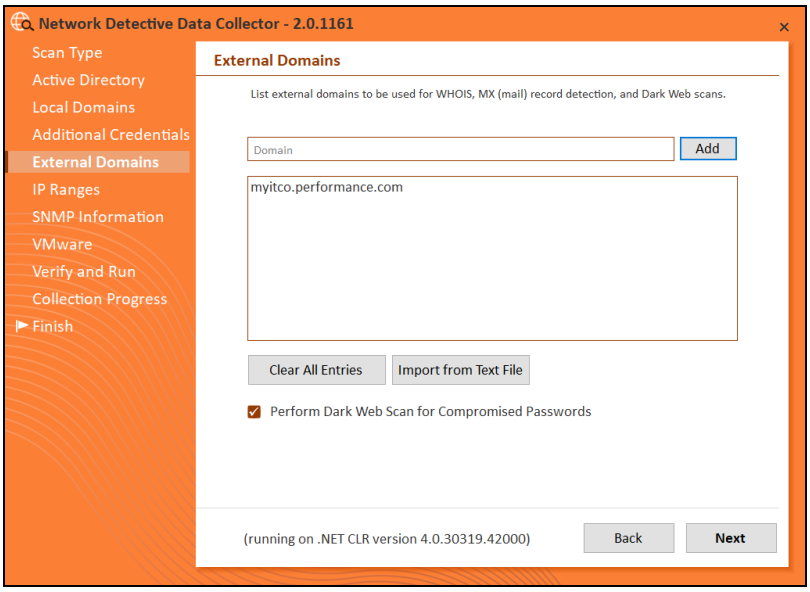


Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

9. 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**.



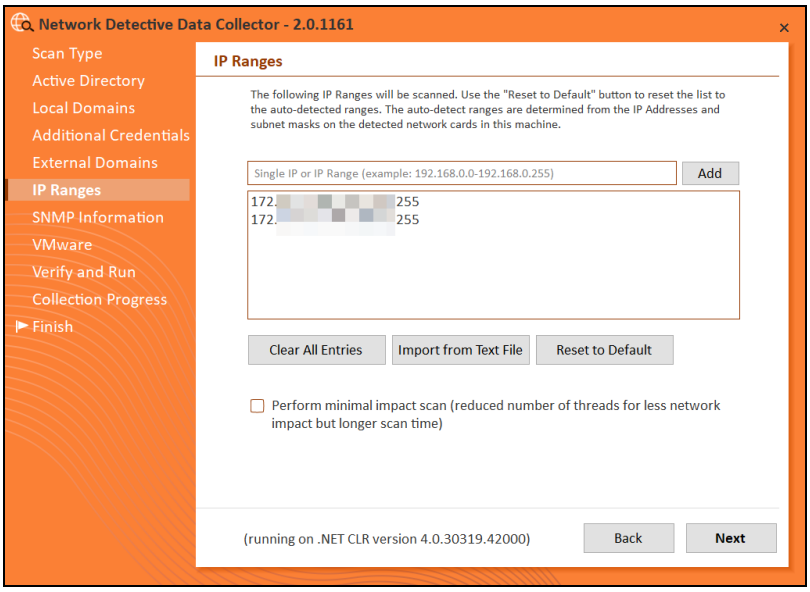
10. The **External Domains** screen will appear. Enter the name(s) of the organization's **External Domains**. Click **Next**.



A Whois query and MX (mail) record detection will be performed on the external domains.

> **Note:** **Perform Dark Web Scan for Compromised Passwords***: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. This service will return the first 5 compromised passwords for each domain specified. If any compromised credentials exist for these domains, they will appear in your assessment reports for the **Security Assessment Module** (SAM).
>
> *To access the Dark Web Scan results, you must have a subscription to the Security Assessment Module and you must generate Security Assessment reports using your data. See also Dark Web Scan Summary for Security Assessment Module.

11. The **IP Ranges** screen will then appear. The HIPAA 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**.

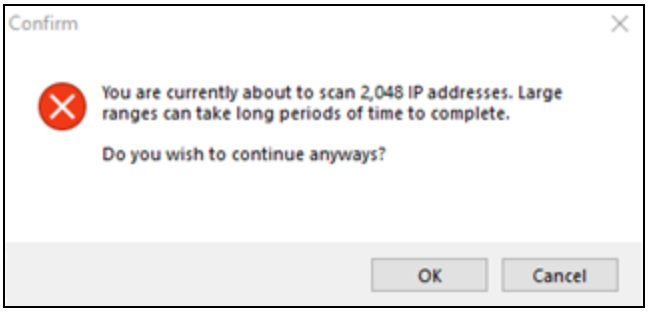


From this screen you can also:

- 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.

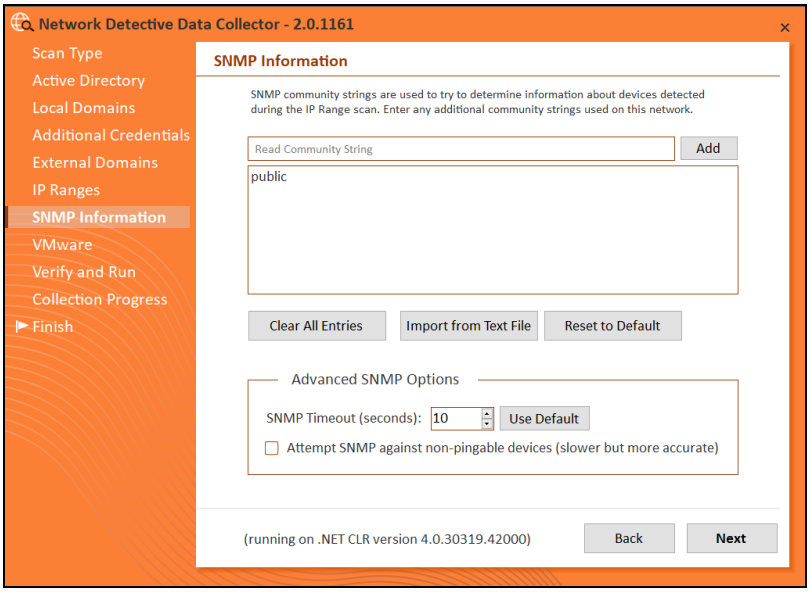
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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



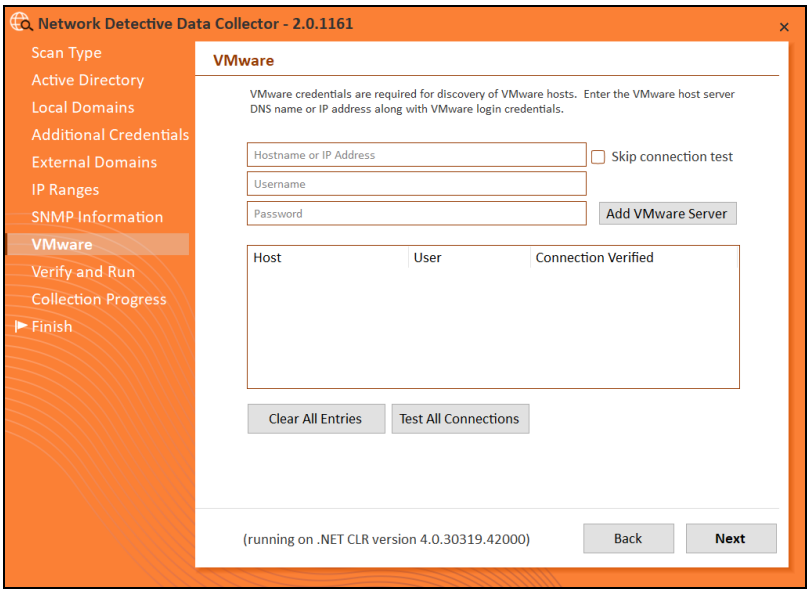
Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

12. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next**.

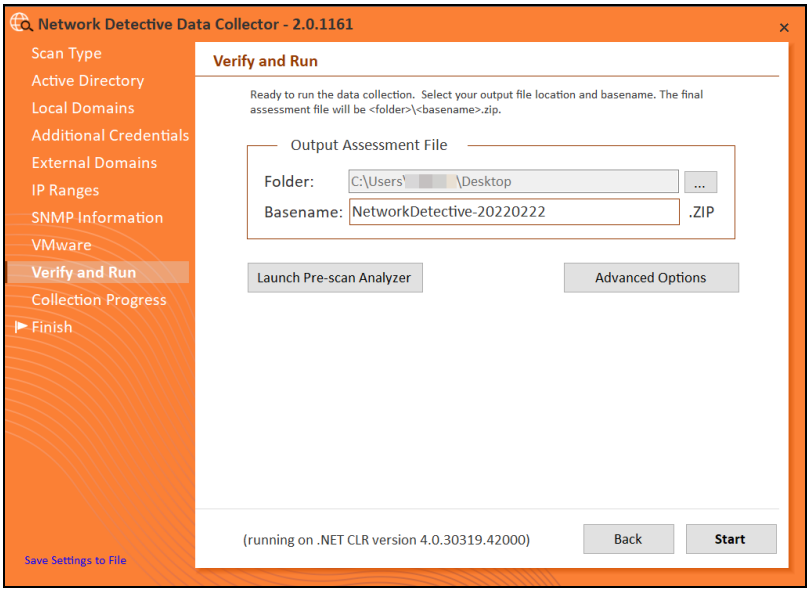


Important: As of 9/28/2018, the Microsoft Base Security Analyzer (MBSA) has been removed from the Data Collector. MBSA is in the process of being deprecated by Microsoft. Microsoft no longer supports MBSA in newer versions of Windows (i.e. v10 and Windows Server 2016). MSBA is only useful for earlier versions of Windows (Windows 7, Windows 8, 8.1, and Windows Server 2008, Windows Server 2008 R2, Windows 2012, and Windows 2012 R2). Follow the steps in this guide and **use the Push Deploy Tool as instructed**. This will collect information such as Patch Analysis for all Windows operating systems.

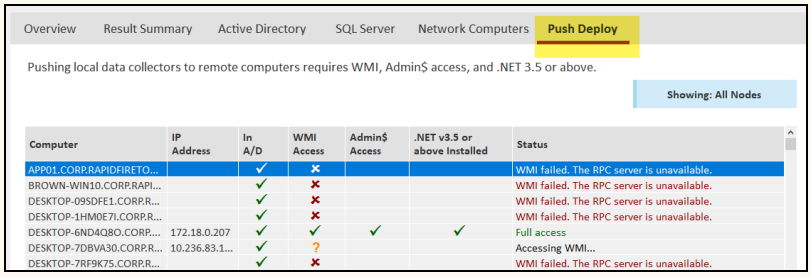
13. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next**.



14. 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 **.HDF** file.

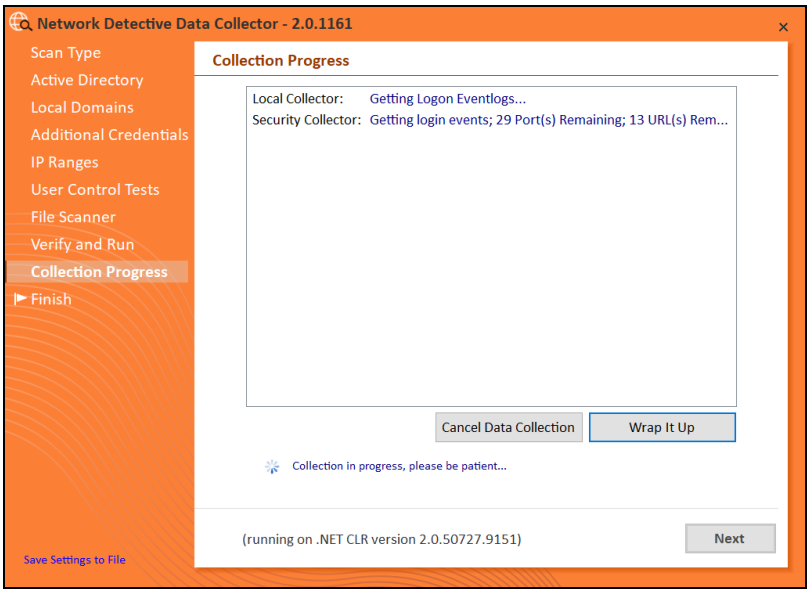


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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



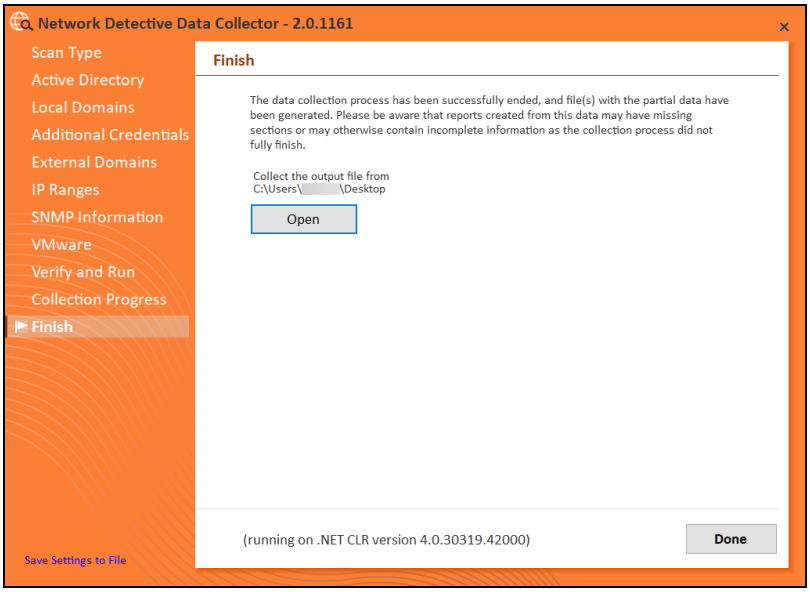
Enter any **Comments** and then click **Start**.

15. 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.

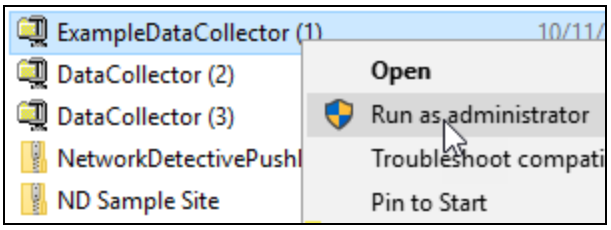
Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.



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

Scanning a Workgroup Network

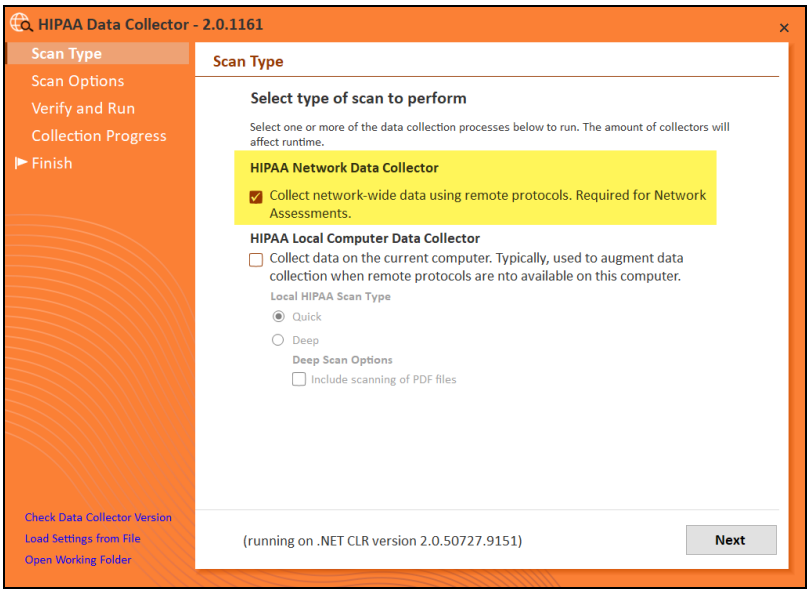
1. Visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the HIPAA Data Collector.
2. Run the **HIPAA Data Collector** executable program as an Administrator (**right click>Run as administrator**).



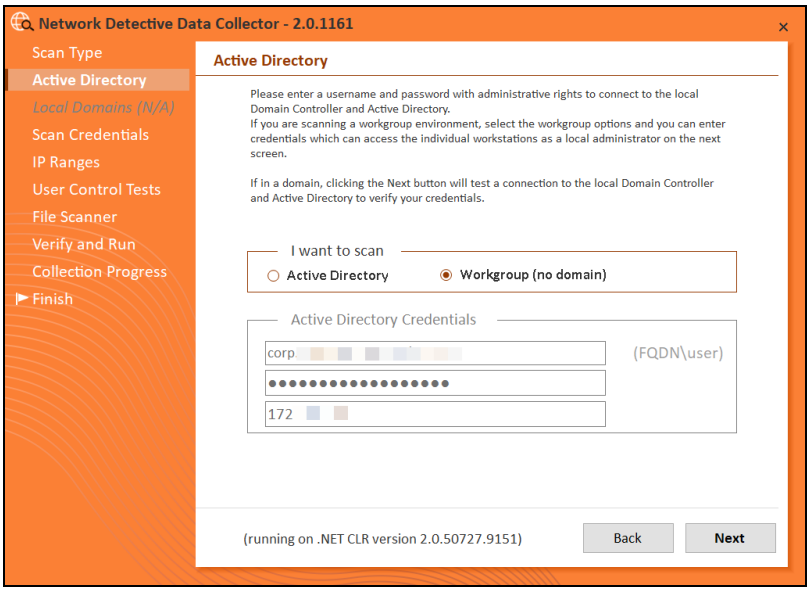
Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

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

   Select the **HIPAA Network Data Collector** option. Click **Next**.

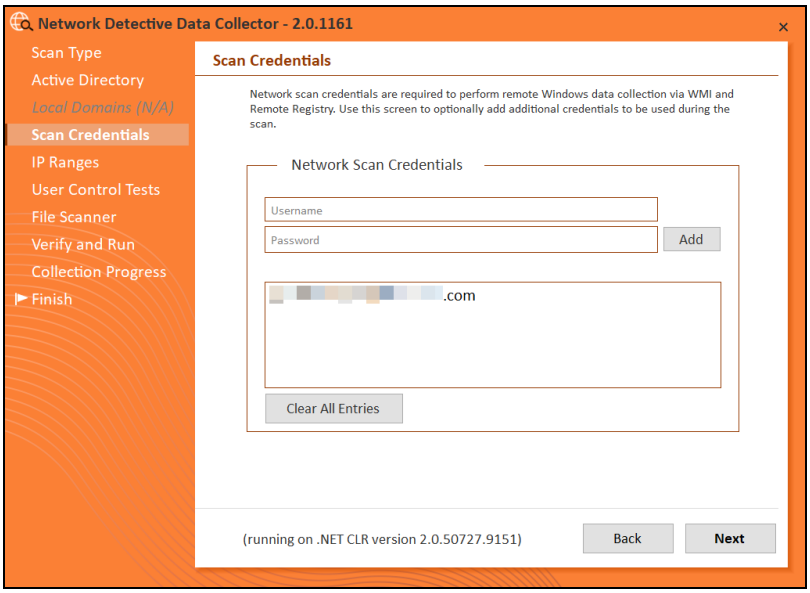


5. The **Active Directory** window will appear. Select the type of network you are scanning (*Workgroup*).

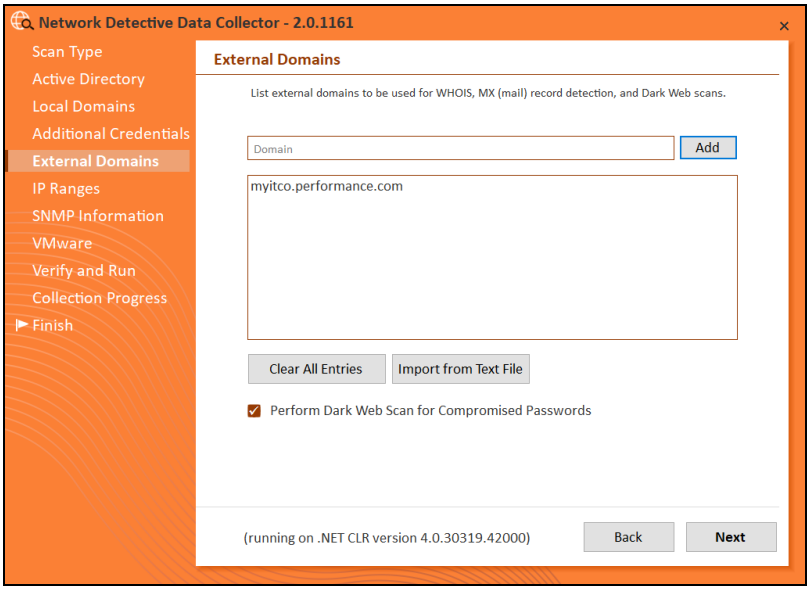


6. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator.

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 these PCs.



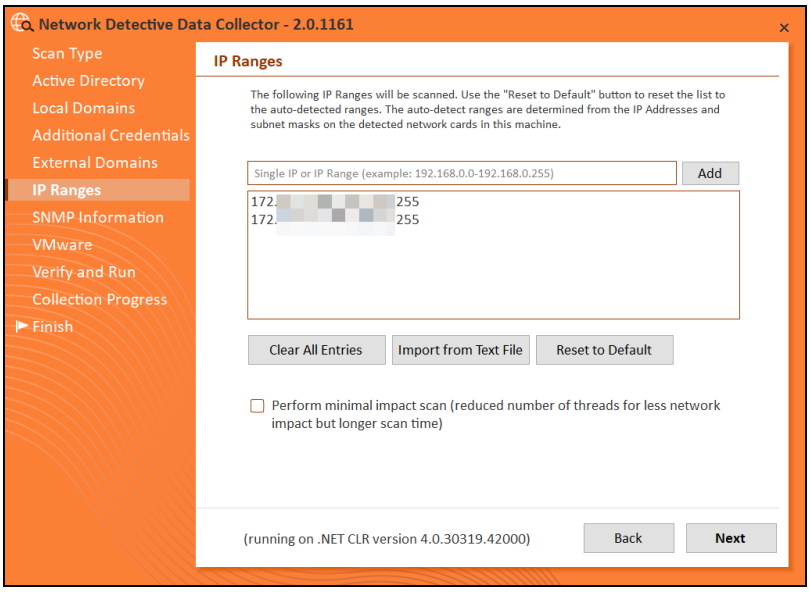
7. The **External Domains** screen will appear. Enter the name(s) of the organization's **External Domains**. Click **Next**.



A Whois query and MX (mail) record detection will be performed on the external domains.

> **Note: Perform Dark Web Scan for Compromised Passwords***: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. This service will return the first 5 compromised passwords for each domain specified. If any compromised credentials exist for these domains, they will appear in your assessment reports for the **Security Assessment Module** (SAM).
>
> *To access the Dark Web Scan results, you must have a subscription to the Security Assessment Module and you must generate Security Assessment reports using your data. See also Dark Web Scan Summary for Security Assessment Module.

8. The **IP Ranges** screen will then appear. The HIPAA 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**.

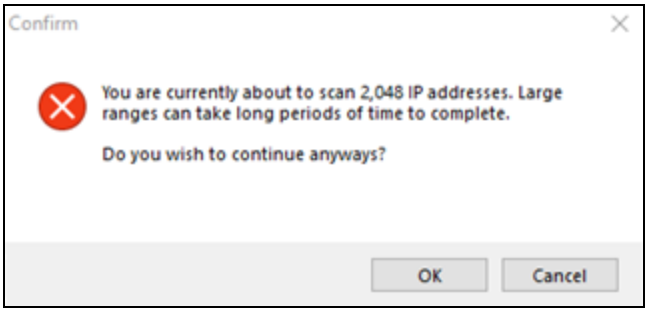


From this screen you can also:

- 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.

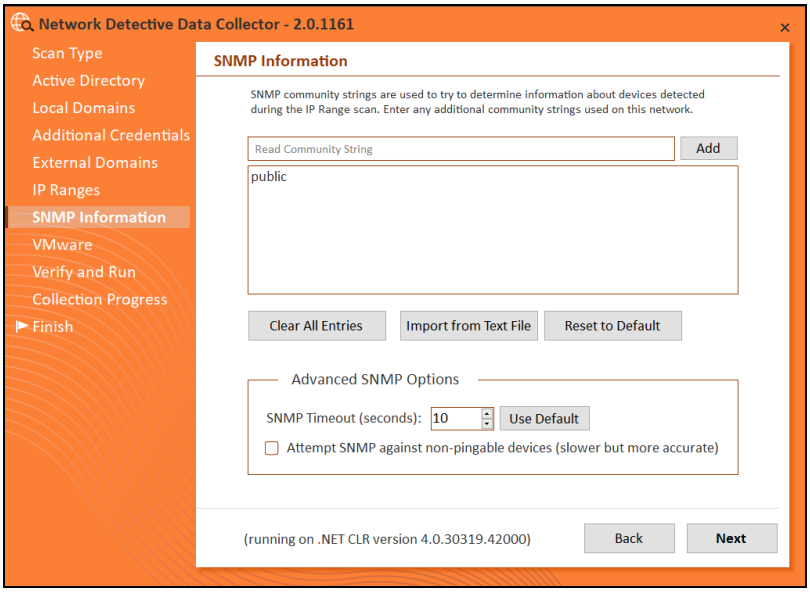
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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



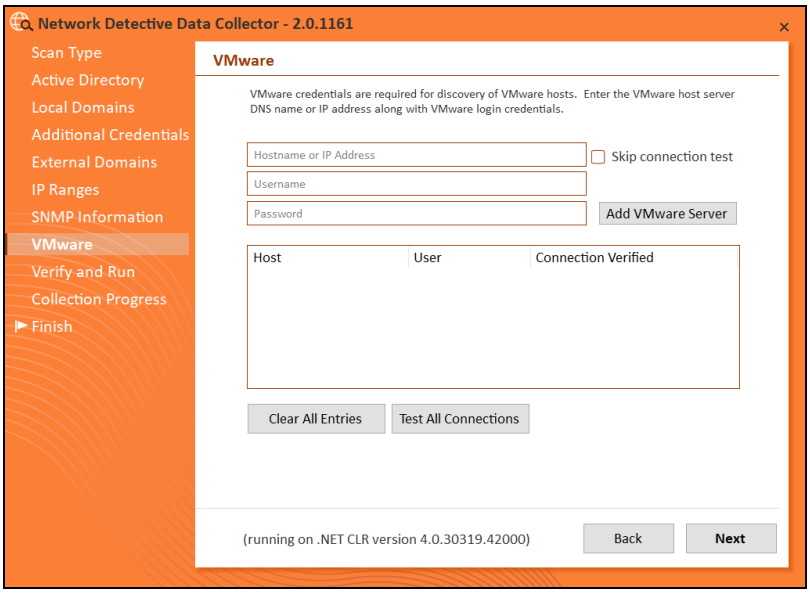
Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

9. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next**.

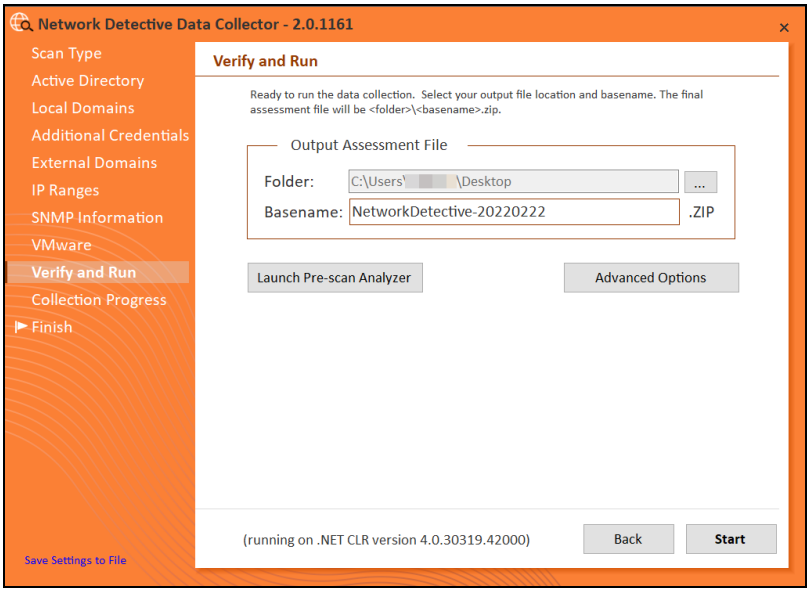


> **Important:** As of 9/28/2018, the Microsoft Base Security Analyzer (MBSA) has been removed from the Data Collector. MBSA is in the process of being deprecated by Microsoft. Microsoft no longer supports MBSA in newer versions of Windows (i.e. v10 and Windows Server 2016). MSBA is only useful for earlier versions of Windows (Windows 7, Windows 8, 8.1, and Windows Server 2008, Windows Server 2008 R2, Windows 2012, and Windows 2012 R2). Follow the steps in this guide and **use the Push Deploy Tool as instructed**. This will collect information such as Patch Analysis for all Windows operating systems.

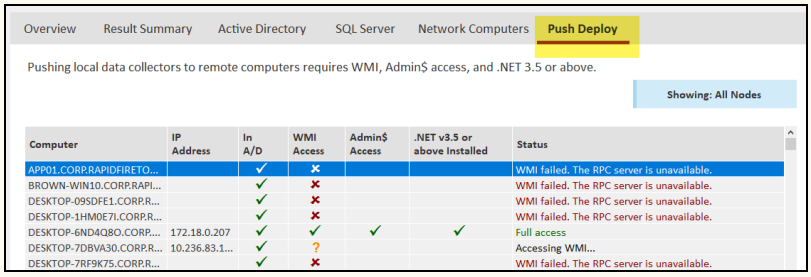
10. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next**.



11. 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 **.HDF** file.

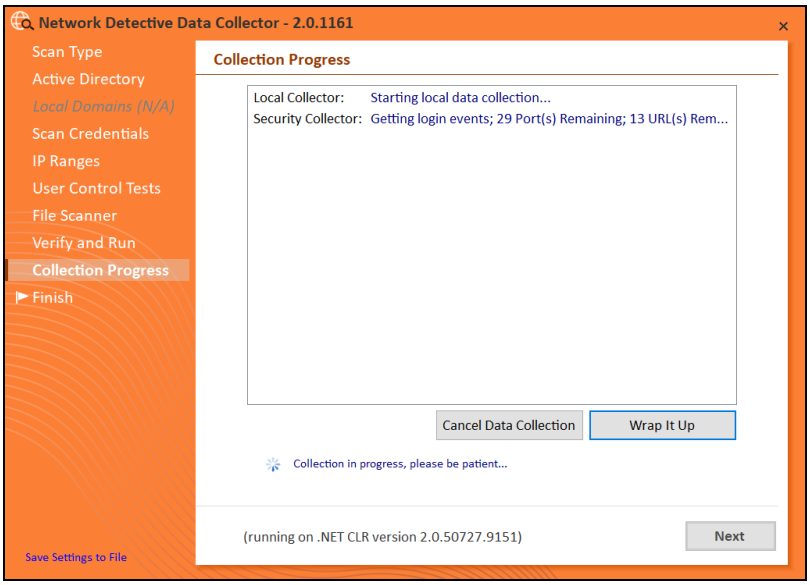


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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



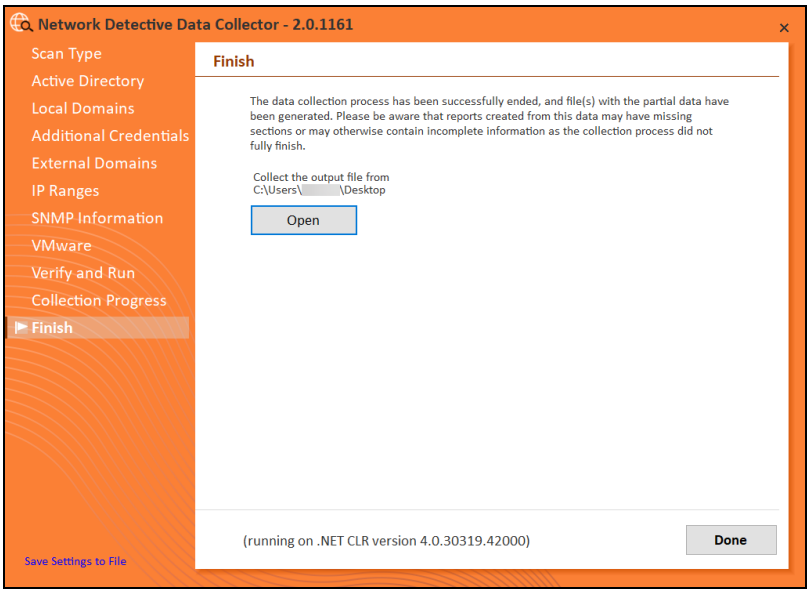
Enter any **Comments** and then click **Start**.

12. 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**.

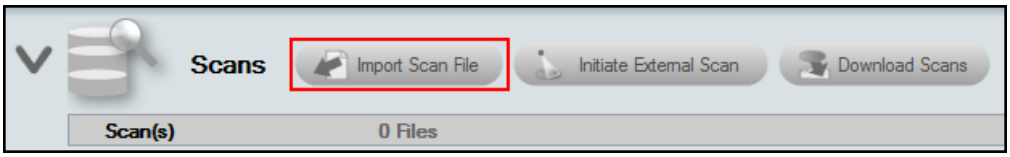


Click **Done** to close the **HIPAA Data Collector** window. Note the location where the scan's output file is stored.

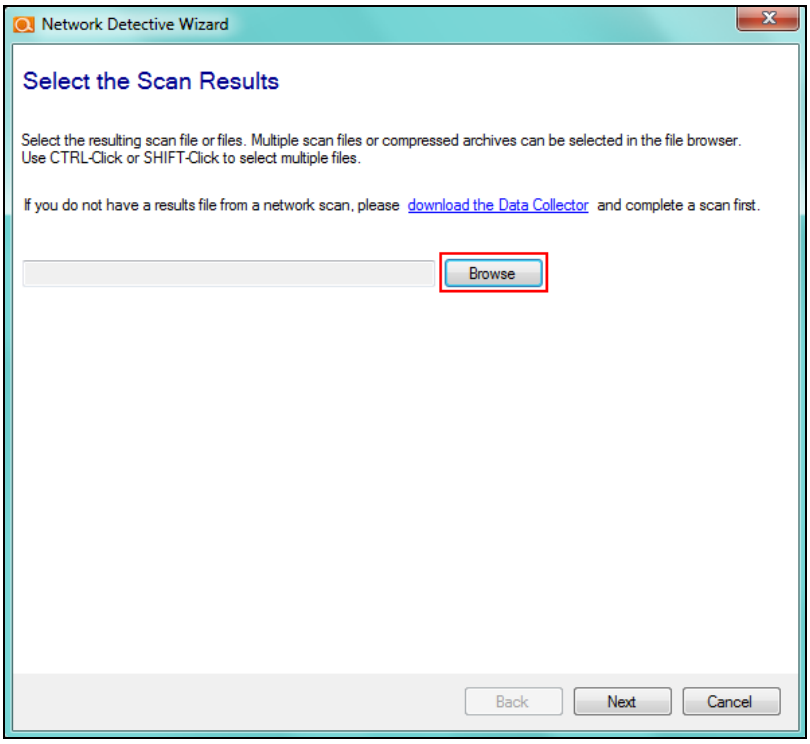
Import the Scan Data from Data Collector into the HIPAA Compliance Assessment Project

Now import the data collected by the Data Collector into the HIPAA Compliance Assessment.

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

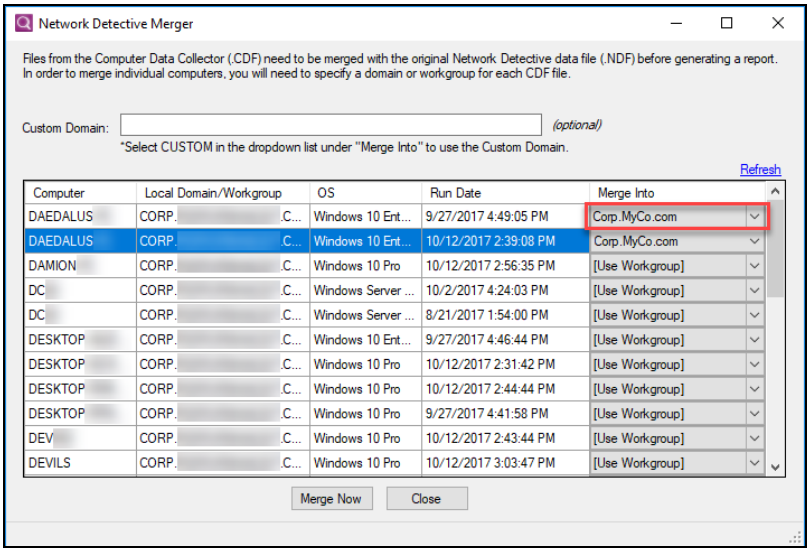


The **Select the Scan Results** window will be displayed.



2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. Click **Open** button to import the scan data. Then click **Next**.
4. 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.

MORE INFO:

Technologies and approaches used by the HIPAA Data Collector

The HIPAA Data Collector is a self-extracting zip file that executes an ".EXE" and is completely non-invasive. It is not "installed" on the domain controller or any other machine on the client's network, and does not make any changes to the system.

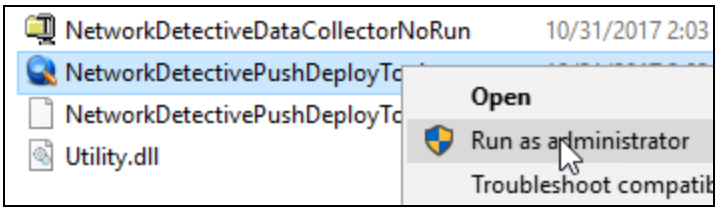
The HIPAA Data Collector makes use of multiple technologies/approaches for collecting information on the client network, including:

- Network Scan
- Active Directory
- WMI
- Remote Registry
- ICMP
- File System Scanning
- Windows Registry
- Windows Shares and Permissions
- Security Center

Step 4 — Run HIPAA Data Collector selecting the Local Computer option on all Workstations/Servers/Laptops

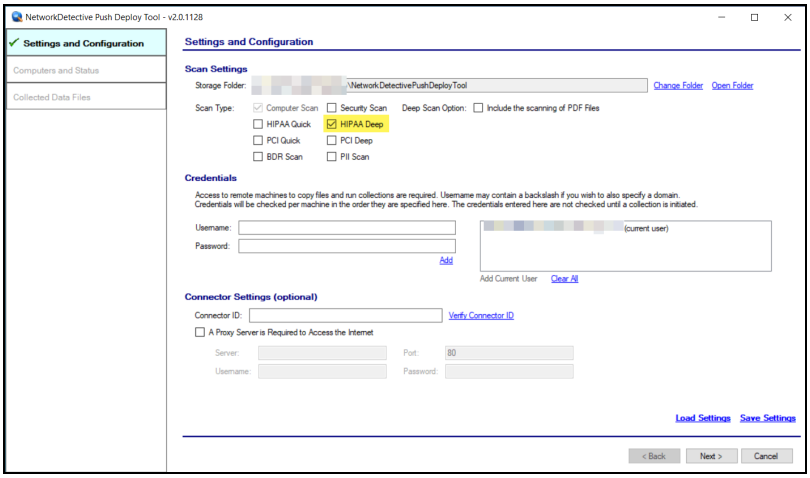
In this step, you will use the Push Deploy Tool to perform a more in-depth HIPAA scan on all endpoints on the network.

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

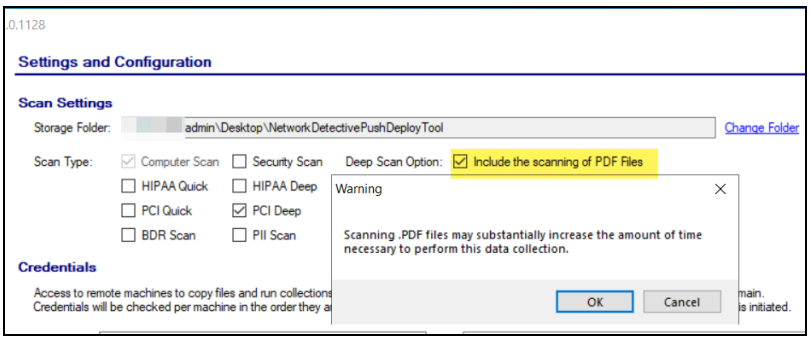


Important: For the most comprehensive scan, you MUST run the Push Deploy Tool as an ADMINISTRATOR.

The Push Deploy Tool Settings and Configuration window will appear.



4. Select the **HIPAA Deep Scan** option. Also select whether you want to scan PDF files. Note that this may significantly increase total scan time.



5. Set the **Storage Folder location**.

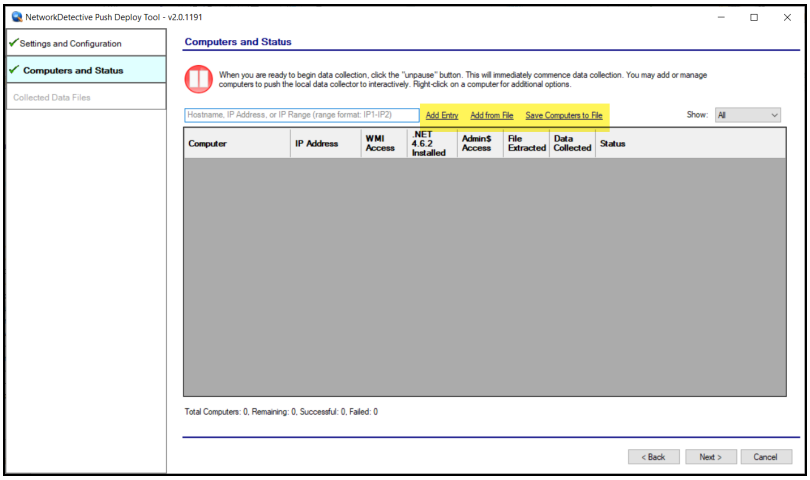
> **Tip:** For your convenience, create a shared network folder to centralize and store all scan results data files created by the **Push Deploy Tool**. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

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 a Single Computer** to be scanned
   - **Add** (computers) **from File** that are to be scanned
   - **Add** (computers) **from IP Range** that are to be scanned

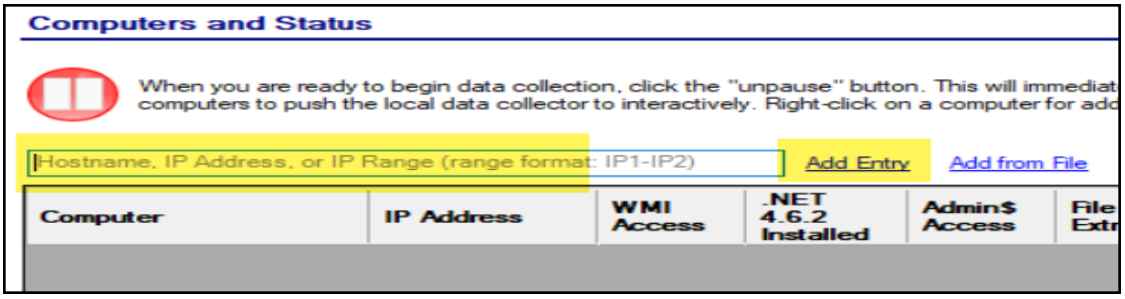
- Or **Save Computers to File** in order to export a list of computers to be scanned again in future assessments



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

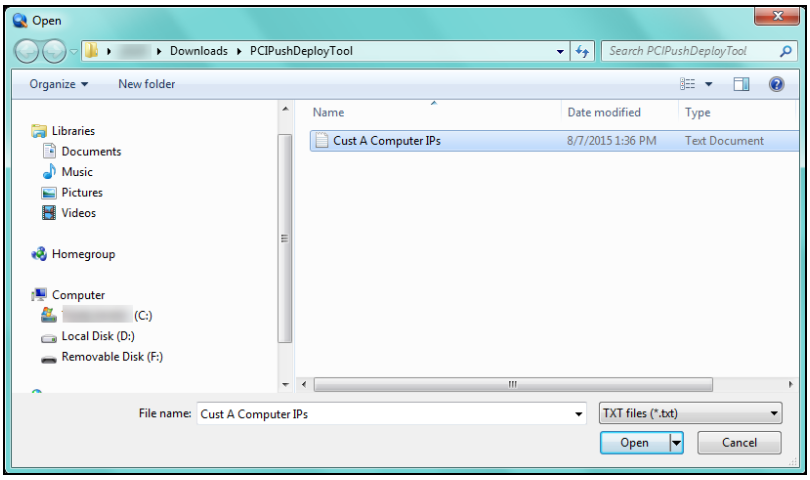
Method 1 — Add a Single Computer to be Scanned

To use the **Add Single Computer** method to select computers to be scanned, then type in the computer's IP address as shown below, then click on the **Add Single Computer** link to the right of the IP address entry field.



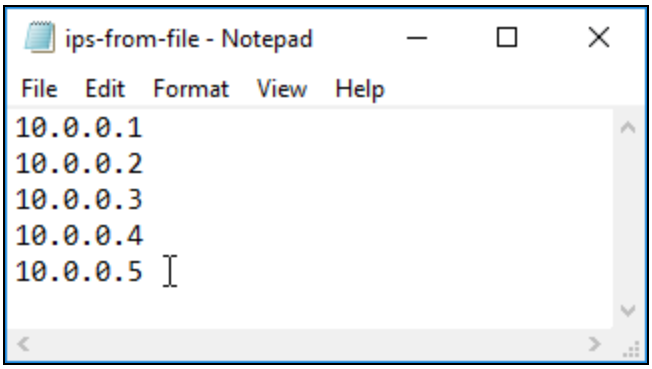
Method 2 — Add (computers) **from File that are to be Scanned**

Click on the **Add from File** link and select the text file that contains the computer IP addresses that are to be included within the scanning process.



Select the file that contains the IP addresses to be scanned, and then click on the **Open** button.

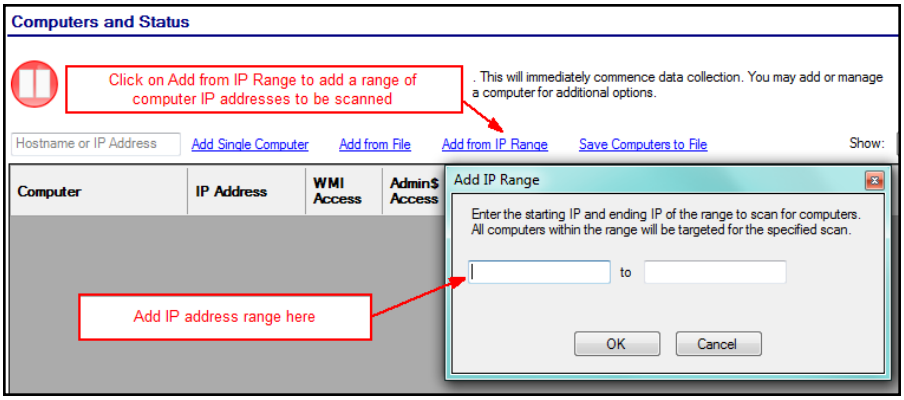
The file that contains the IP addresses can be created using the Push Deploy Tools' **Save Computers to File** feature, or created manually with a text editor using the required text formatting structure so that the IP addresses are recognized by the **Push Deploy Tool**.



Upon the file's selection and opening the IP address and computer information will be imported into the **Push Deploy Tool** and presented in the **Computers and Status** window for verification prior to starting the scan.

Method 3 — Add (computers) **from IP Range that are to be Scanned**

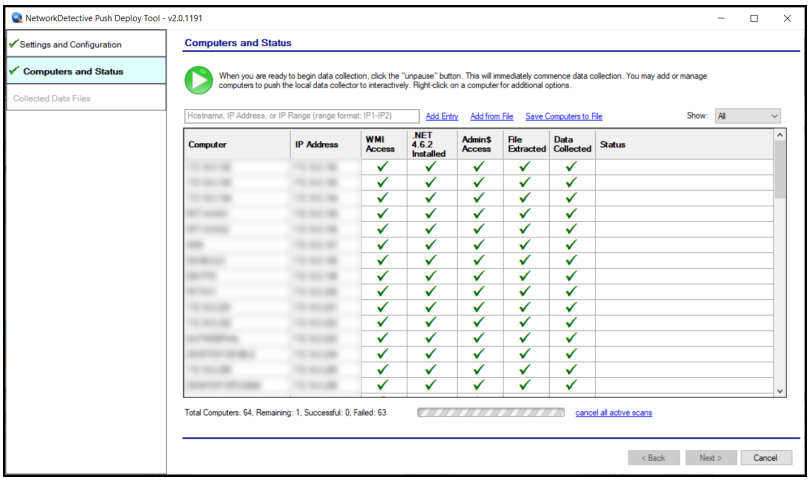
Click on the **Add from IP Range** and to define the Starting and Ending computer IP addresses range that are to be included within the scanning process.



When you have input the IP address range into the **IP Range** window, select the **OK** button.

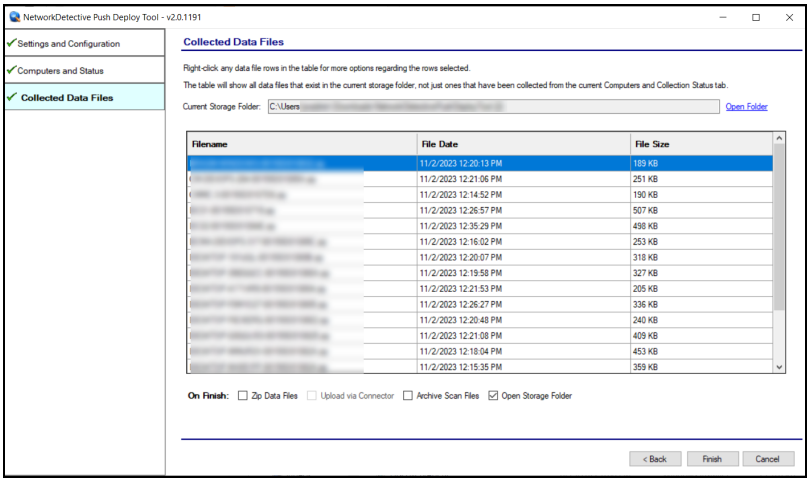
After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the **Computers and Status** window.

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**.

9. 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.



10. 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.

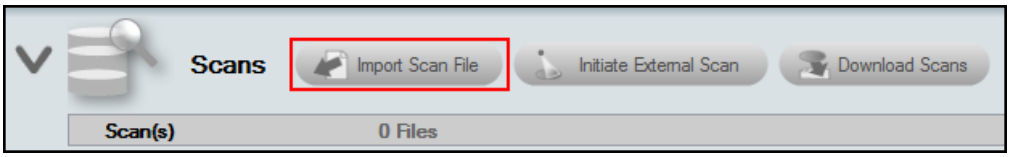
The output files (.ZIP, files) from the local scans can be stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.

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

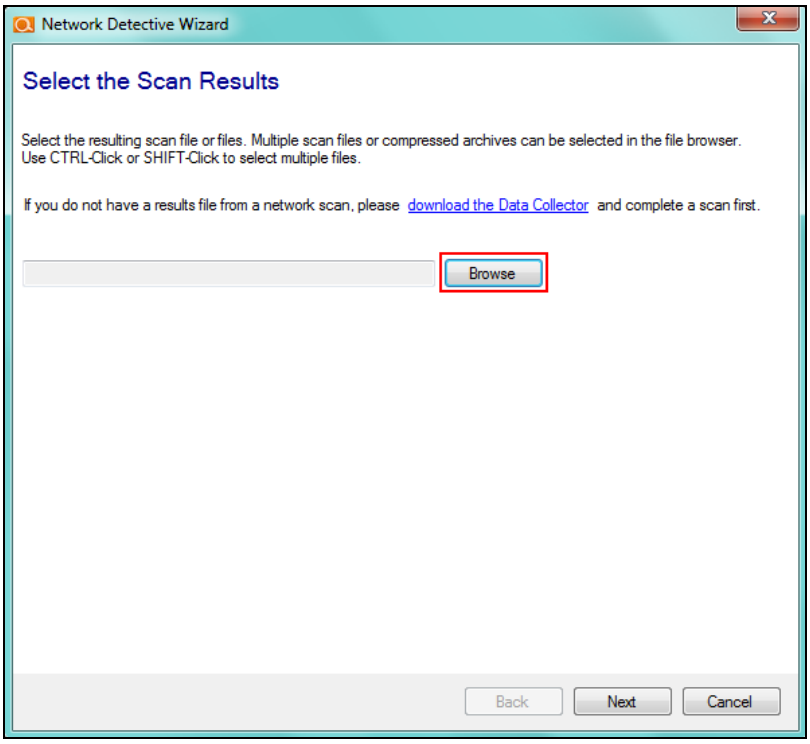
Import the Scan Data from Push Deploy Tool into the HIPAA Compliance Assessment Project

Now import the data collected by the Push Deploy Tool into the HIPAA Compliance Assessment.

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

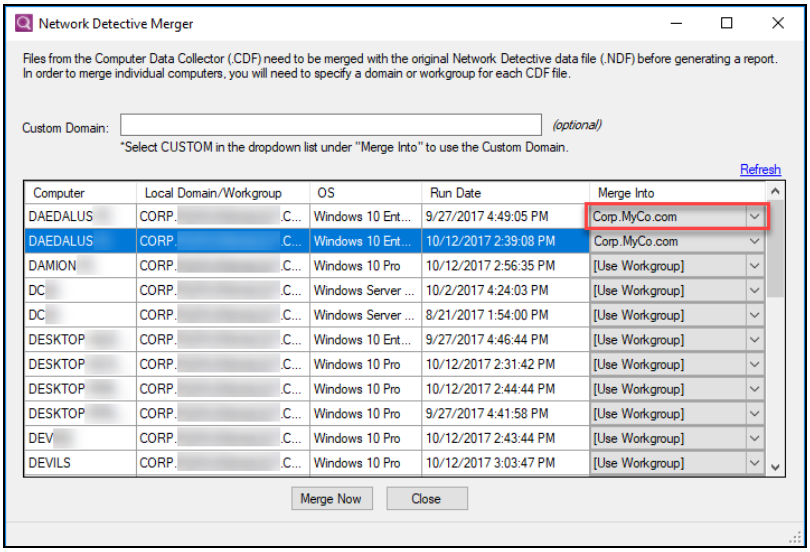


The **Select the Scan Results** window will be displayed.



2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. Click **Open** button to import the scan data. Then click **Next**.
4. 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.

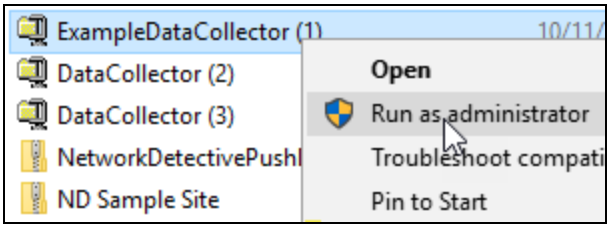


The **Scans** bar will be updated with the imported scan files.

Step 4.1 — Run the HIPAA Data Collector Local Scan on Computers that could not be accessed by the Push Deploy Tool

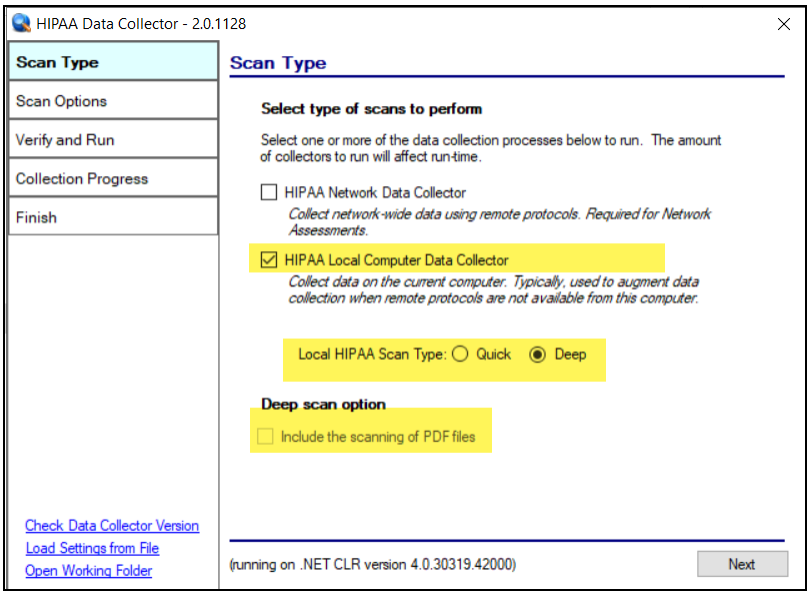
In this step, you will use the HIPAA Data Collector to perform local scans on the computers that could not be scanned by the Push Deploy Tool. You will need to log in to each of these computers and perform a local scan on each one. You will then upload and merge the scan files into your assessment project.

1. If you have not done so already, visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the HIPAA Data Collector.
2. Run the **HIPAA Data Collector** executable program as an Administrator (**right click>Run as administrator**).

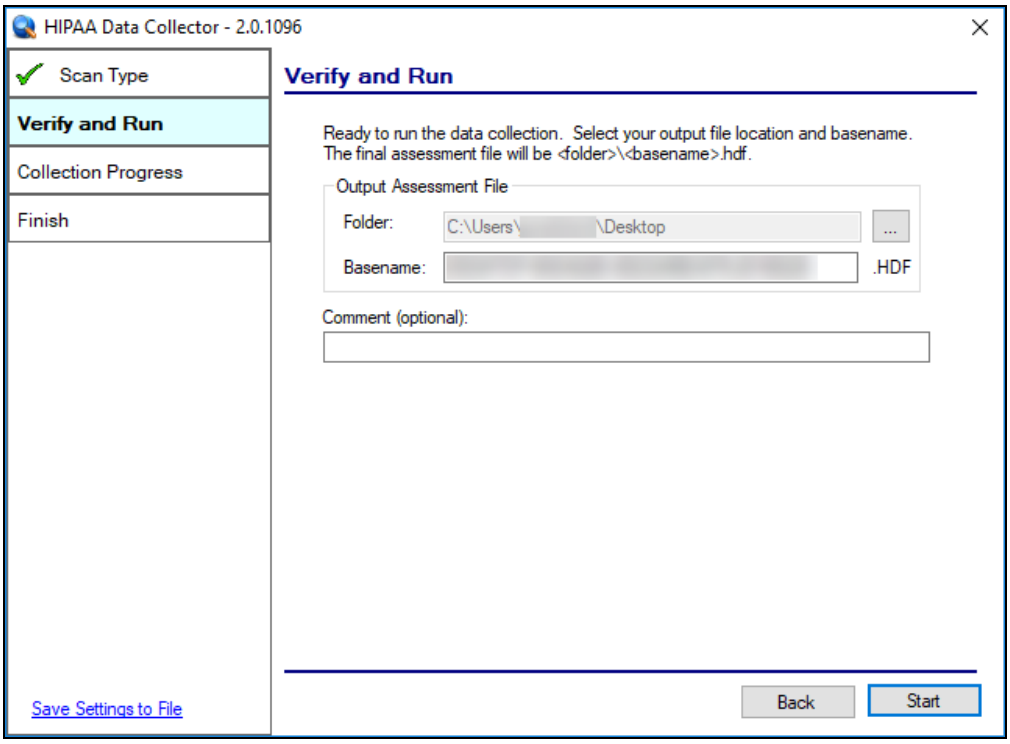


Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

3. **Unzip** the files into a temporary location. The HIPAA Data Collector's self-extracting ZIP file does not install itself on the client computer.
4. The HIPAA Data Collector Scan Type window will appear.
5. Select the **HIPAA Local Computer Data Collector** option and set the **Local HIPAA Scan Type** to **HIPAA Deep Scan**. Click **Next**. Also specify whether to include PDF files in the scan.

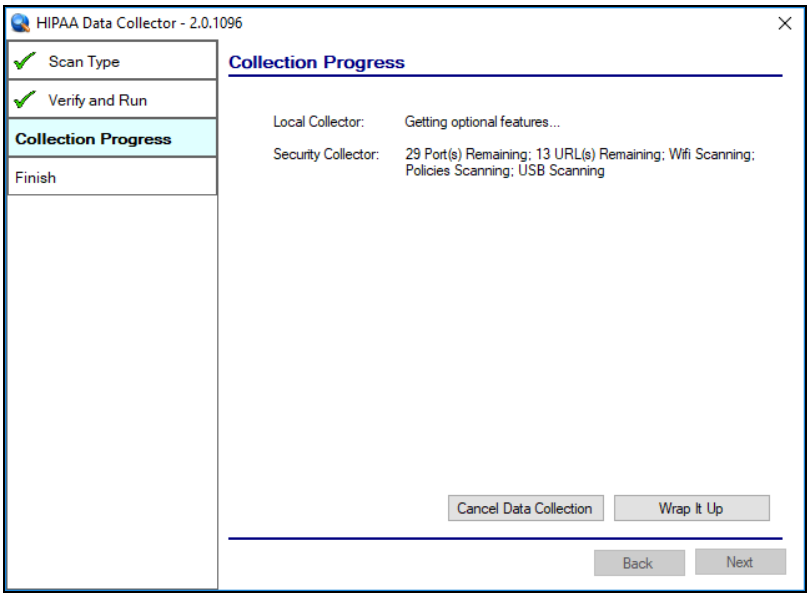


The Verify and Run window will be displayed. The **Verify and Run** window enables you to change the output location for the scan data, change the name of the file, and add comments.



6. After setting the **Output Assessment File**'s **folder location**, the **Basename** of the scan's output file, and adding **a Comment**, select **Start** to initiate the scan.

   The **Collection Progress** window will be displayed during the scan process.

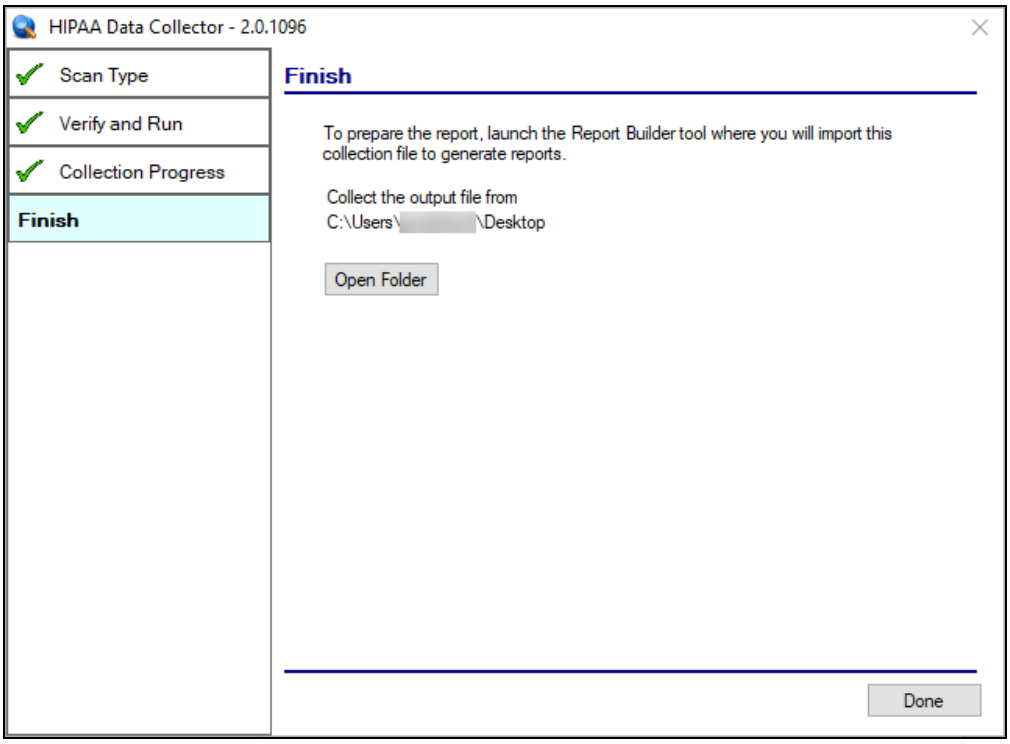


Track the scan's progress through the **Collection Progress** window.

At any time you may **Cancel Data Collection** without saving any data.

You may select **Wrap It Up** to stop a scan and use the incomplete data that was collected.

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

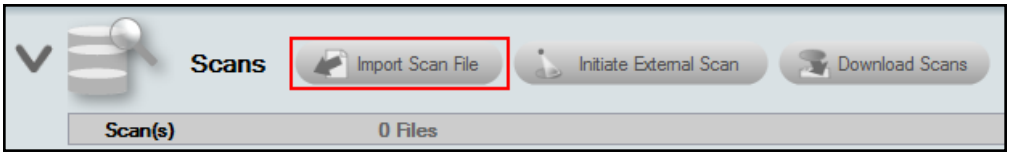


Note the scan **output file's** location and click on the **Done** button to complete the process.

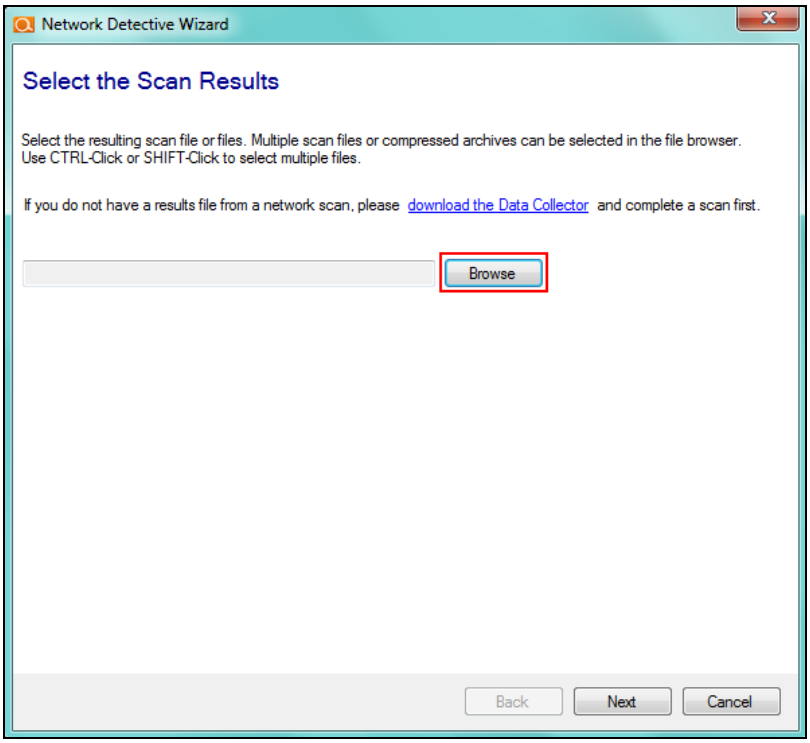
Import the Scan Data from Data Collector into the HIPAA Compliance Assessment Project

Now import the data collected by the Data Collector into the HIPAA Compliance Assessment.

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



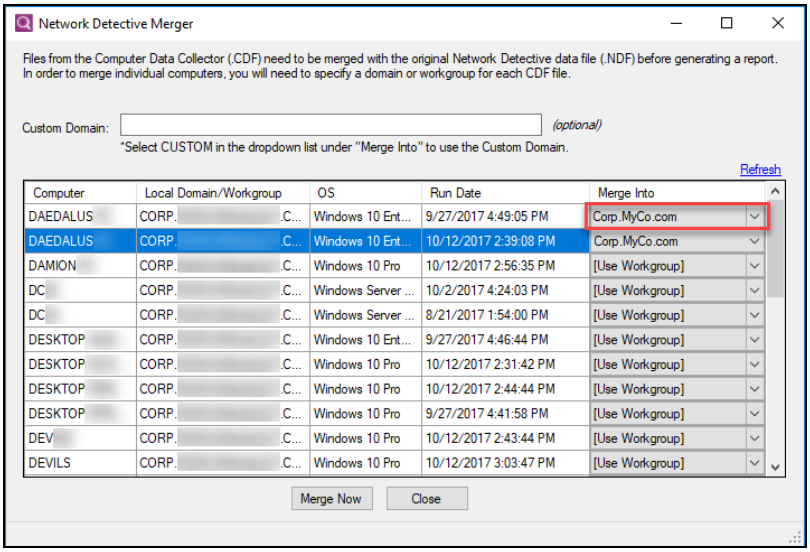
The **Select the Scan Results** window will be displayed.



2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. Click **Open** button to import the scan data. Then click **Next**.
4. 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**.

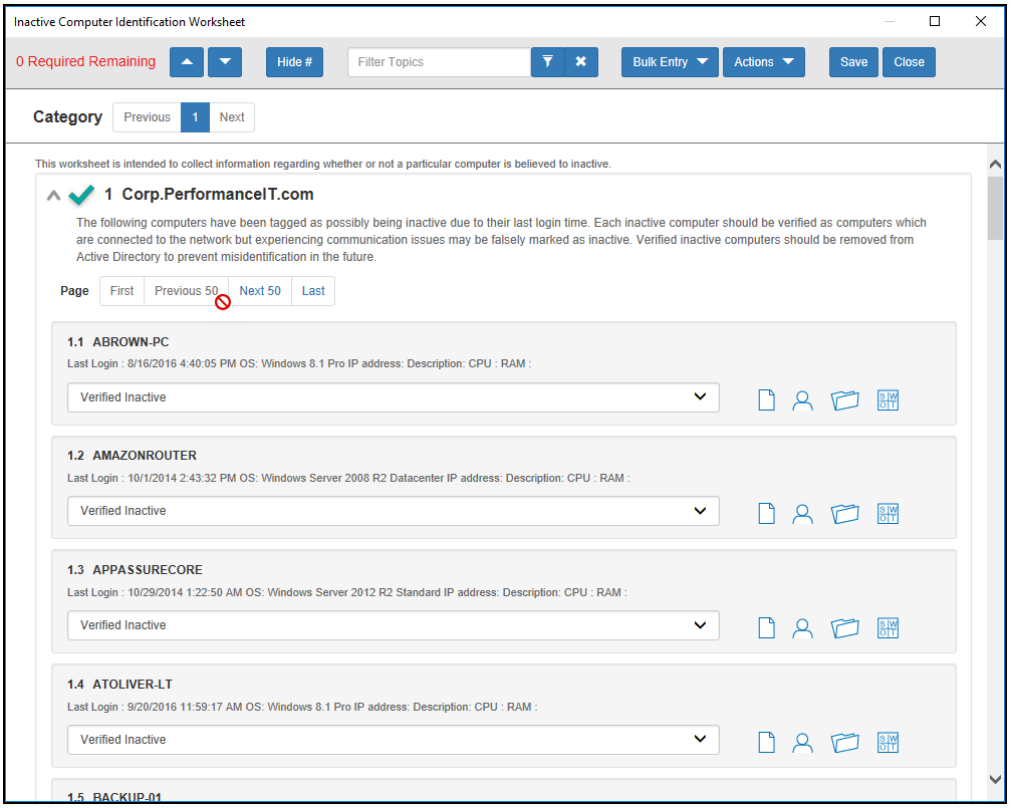


The **Scans** bar will be updated with the imported scan files.

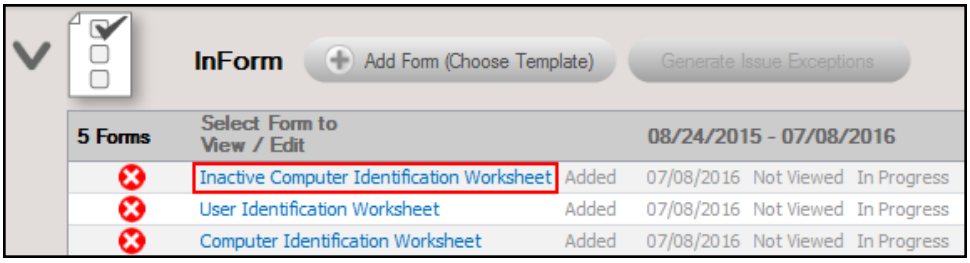
Collect Secondary HIPAA Data and Document Exceptions

Step 5 — Complete Inactive Computer Identification Worksheet

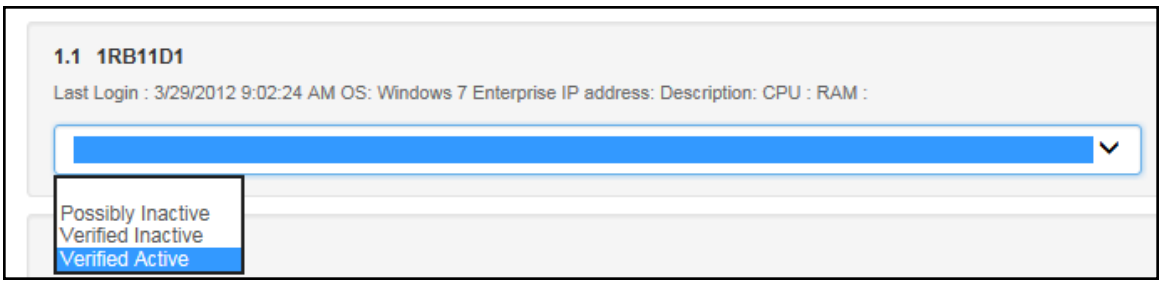
The **Inactive Computer Identification Worksheet** contains a list of computers that have not been logged into for a long period of time. This list of computers is identified during the network scan phase of the automated data collection.



To open and complete the **Inactive Computer Identification Worksheet**, click on the **name label** for the **Inactive Computer Identification Worksheet** entry in the **InForm** Questionnaire/Worksheet list located below the **InForm Bar** at the bottom of the **Assessment** window.

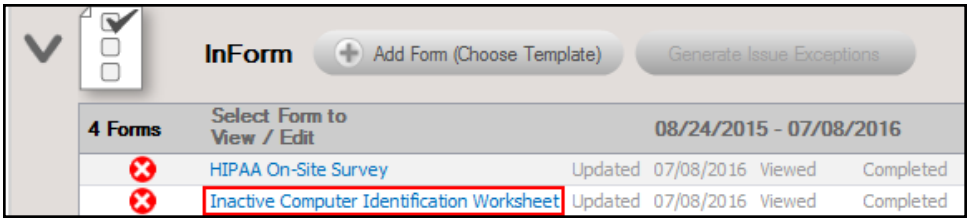


In this worksheet, document the usage status of each computer (for example: Verified Active, Possibly Active, or Verified Inactive).



Complete the worksheet for all of the inactive computers listed. You can optionally include the name of the respondent and any relevant notes.

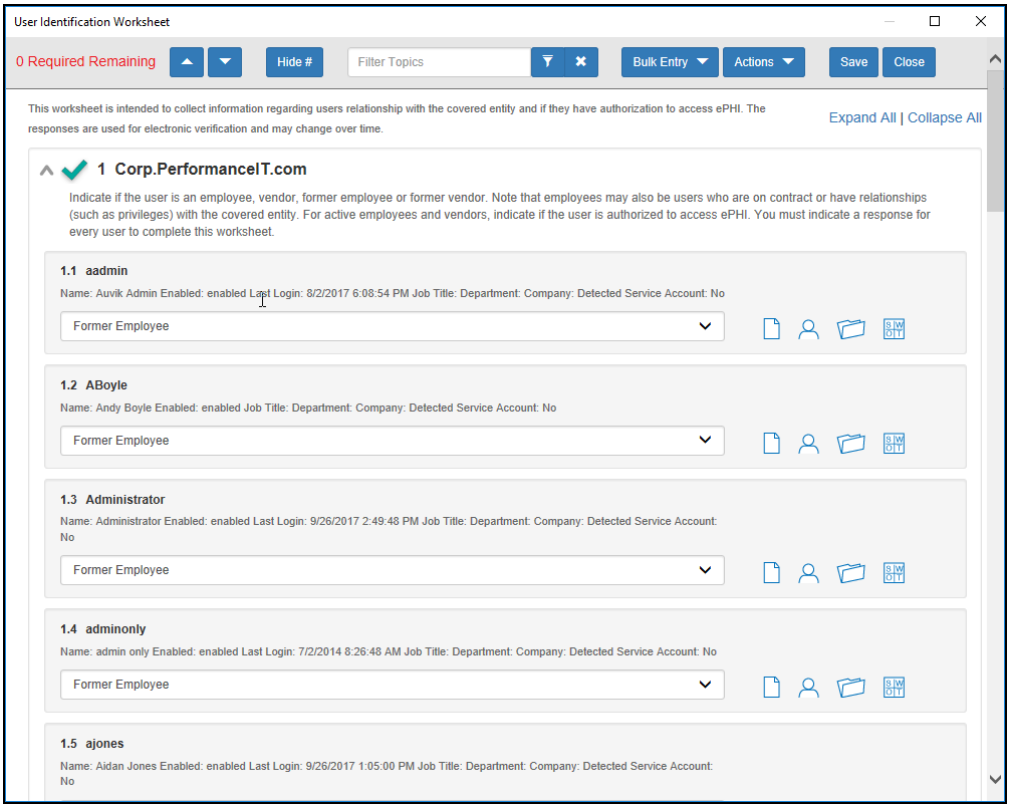
You can return to the **Inactive Computer Identification Worksheet** by clicking on the **name label** for the **Inactive Computer Identification Worksheet** located under the **InForm Bar** at the bottom of the **Assessment Window**.



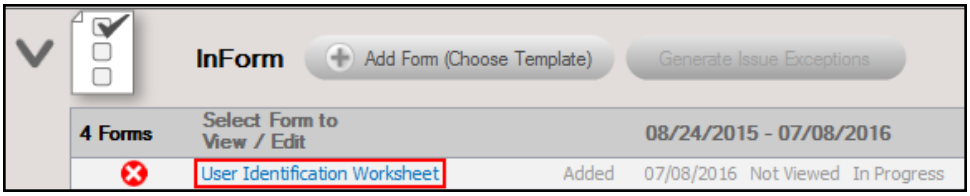
Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

Step 6 — Complete User Identification Worksheet

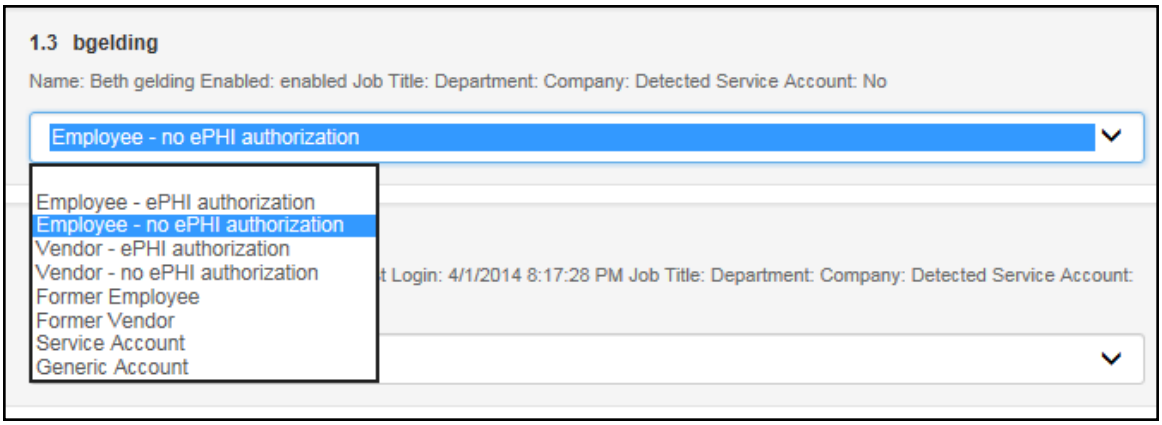
The **User Identification Worksheet** enables you to identify each user and document if they are authorized to access electronic Protected Health Information (ePHI). This worksheet contains a list of users that have been identified as having ePHI access rights during the network scan phase of the automated data collection.



To open and complete the **User Identification Worksheet**, click on the **name label** for the **User Identification Worksheet** entry in the **InForm** Questionnaire/Worksheet list located below the **InForm Bar** at the bottom of the **Assessment** window.

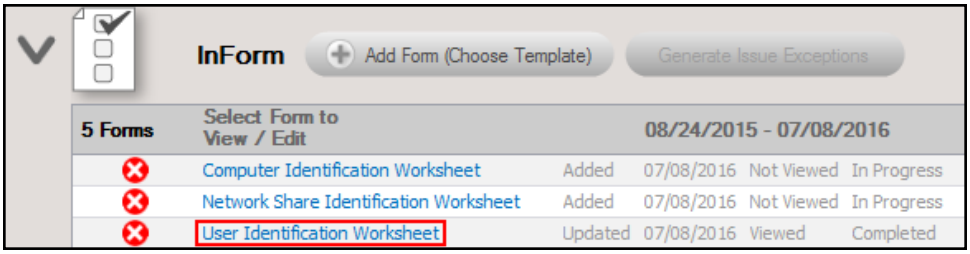


In this worksheet, you document **the type of user account** (for example: Employee – ePHI Authorization, Employee - no ePHI Authorization, Vendor – ePHI Authorization, Vendor – no ePHI Authorization, Former Employee, Former Vendor, Service Account, etc.).



Complete the worksheet for all of the users listed. You can optionally include the name of the respondent and any relevant notes.

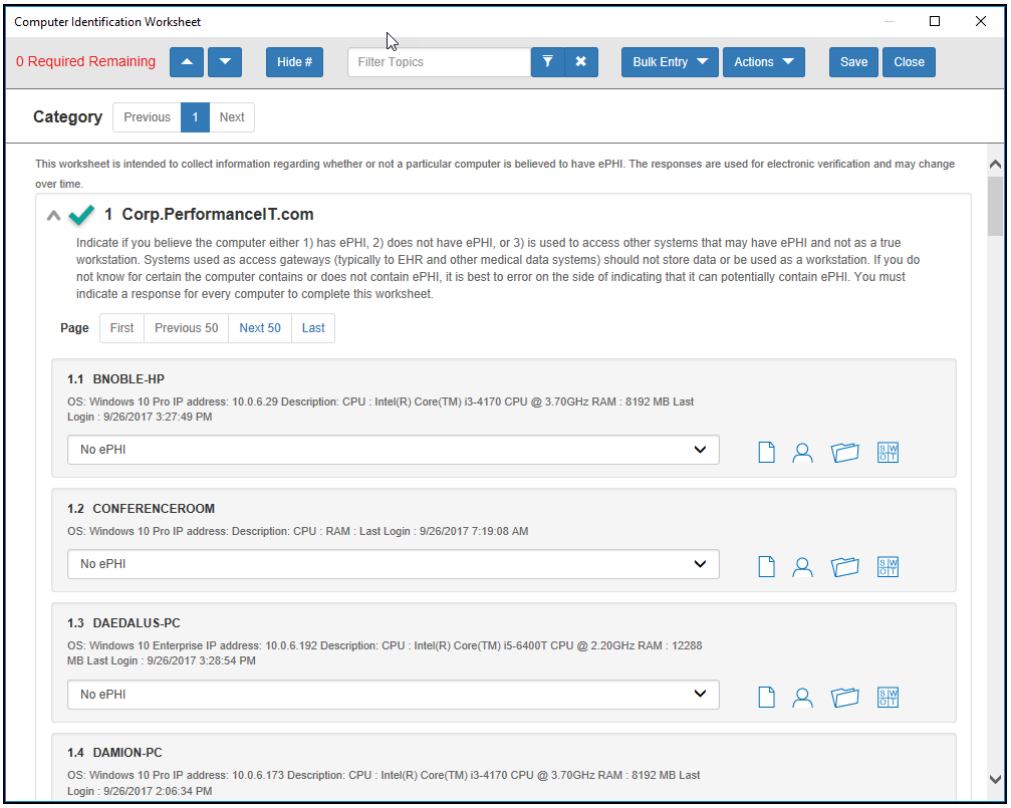
You can return to the **User Identification Worksheet** by clicking on the **name label** for the **User Identification Worksheet** located under the **InFormBar** at the bottom of the **Assessment Window**.



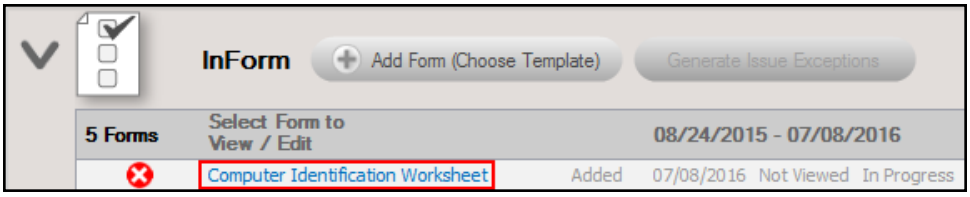
Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

Step 7 — Complete Computer Identification Worksheet

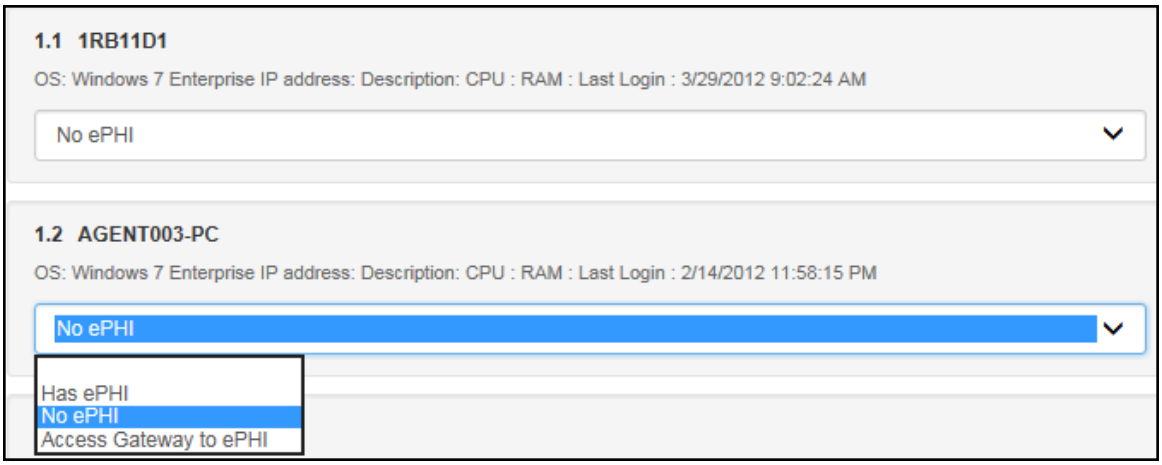
The **Computer Identification Worksheet** contains a list of the computers that have been identified during the network scan phase of the automated data collection. The computers identified are operating within a particular domain or workgroup. The list also includes non-domain devices. In this worksheet, you identify each computer that stores ePHI, does not store ePHI, or accesses ePHI.



To open and complete the **Computer Identification Worksheet**, click on the **name label** for the **Computer Identification Worksheet** entry in the **InForm** Questionnaire/Worksheet list located below the **InForm Bar** at the bottom of the **Assessment** window.

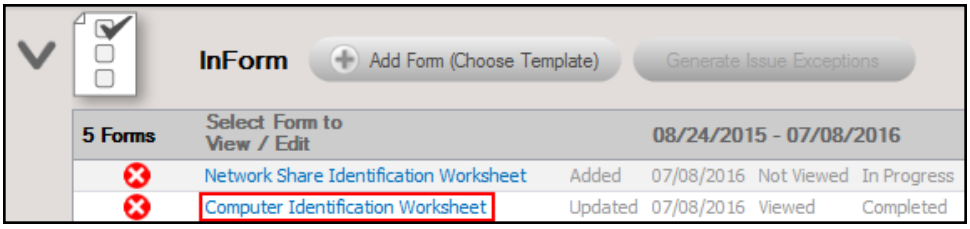


For each device, either the machine name or IP address of the device is displayed in the **Topic** column. There additional details about the devices listed in the worksheet that are documented in the **Notes** field, including OS version, IP address, Description data, Last Login, and possibly a CPU version.



Complete the worksheet for all of the computers listed. You can optionally include the name of the respondent and any relevant notes.

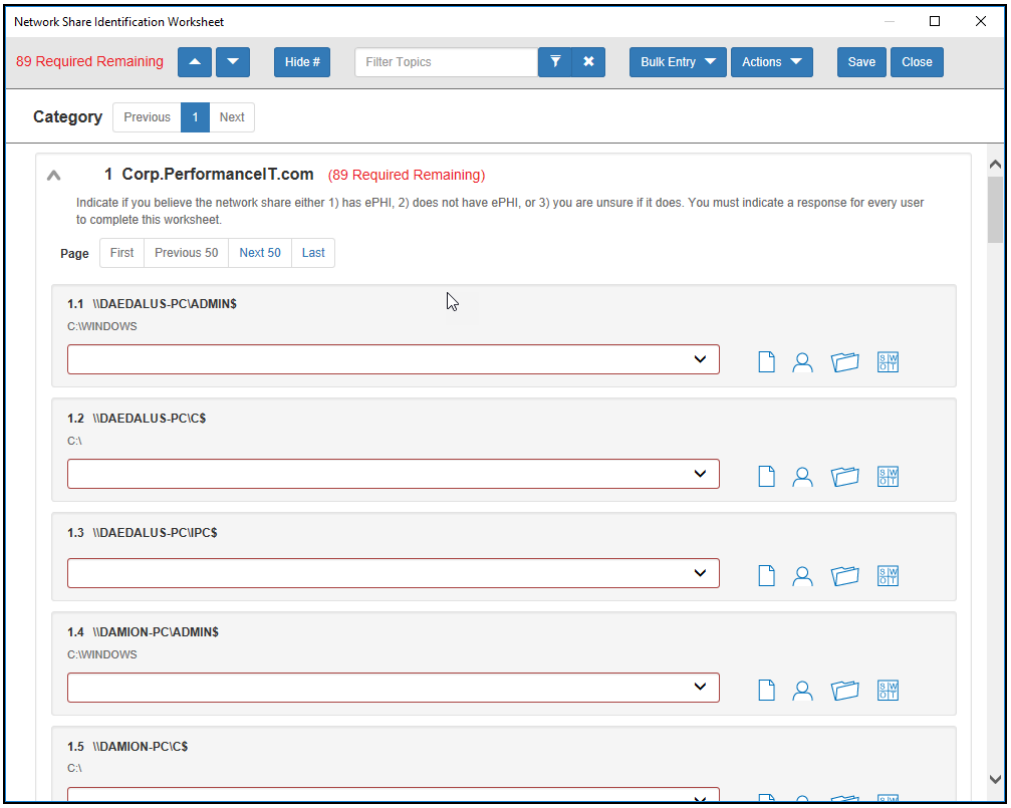
You can return to the **Computer Identification Worksheet** by clicking on the **name label** for the **Computer Identification Worksheet** located under the **InForm Bar** at the bottom of the **Assessment Window**.



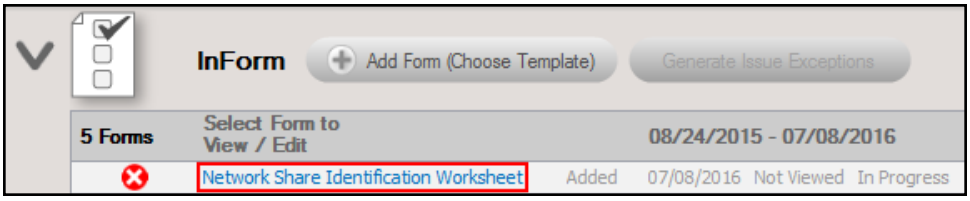
Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

Step 8 — Complete Network Share Identification Worksheet

The Network Share Identification Worksheet is used to identify and document each network share operating within the environment scanned by the HIPAA Module. You must document whether the network share contains ePHI, does not contain ePHI, or document that you do not know if the share contains ePHI or not.



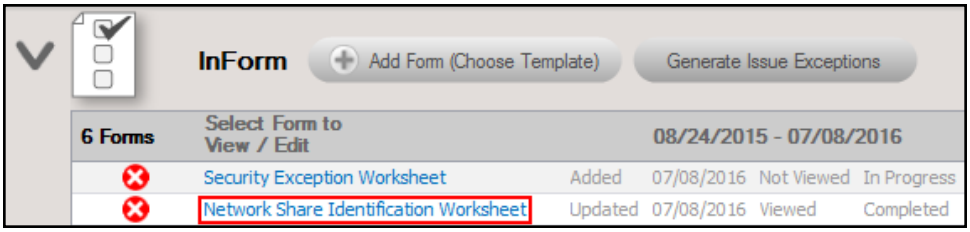
To open and complete the **Network Share Identification Worksheet**, click on the **name label** for the **Network Share Identification Worksheet** entry in the **InForm** Questionnaire/Worksheet list located below the **InForm Bar** at the bottom of the **Assessment** window.



The **Network Share Identification Worksheet** presents a list of network share locations with the network. These network share locations are listed in the worksheet to enable you to document an examination of the features contained within the applications. The final **Network Share Identification** assessment will be a result of responses to a series of questions used to document whether ePHI is stored in the share location, ePHI is not stored in the share location, or if you do not know if the share location contains ePHI or not.

Complete the worksheet for all of the share locations listed. You can optionally include the name of the respondent and any relevant notes.

You can return to the **Network Share Identification Worksheet** by clicking on the **name label** for the **Network Share Identification Worksheet** located under the **InForm Bar** at the bottom of the **Assessment Window**.

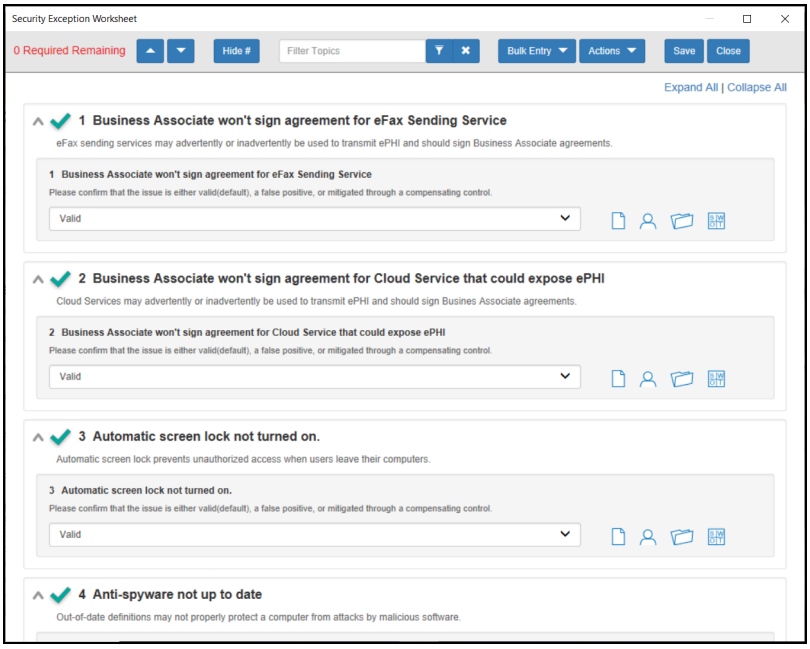


Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

Step 9 — Complete Security Exception Worksheet (Optional)

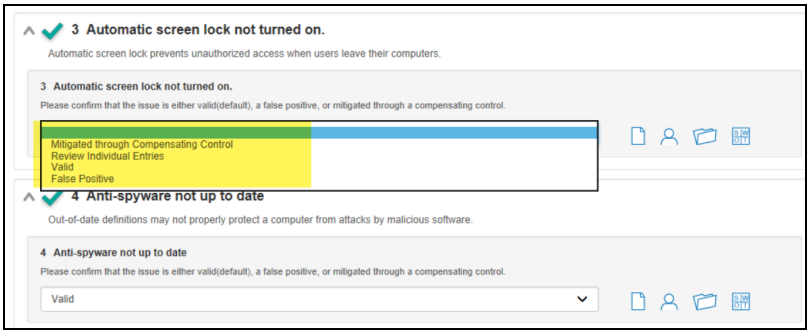
The **Security Exception Worksheet** is an optional worksheet that compiles the issues discovered by the Push Deploy Tool Scans, HIPAA Data Collector, Surveys, and Assessment Worksheets used throughout the HIPAA assessment process to enable security exceptions to be specified along with compensating controls to manage the exceptions.

> **Tip:** Use the **Security Exception Worksheet** to handle "false positives" or explain why certain issues have been resolved. Your entries will affect the overall risk score and other areas in your assessment documentation.



To use the Security Exception Worksheet:

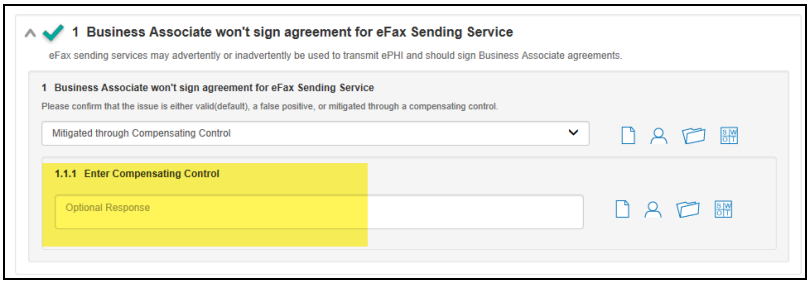
1. For each issue in the form, select one of the available options.



A. **Mitigated through Compensating Control**

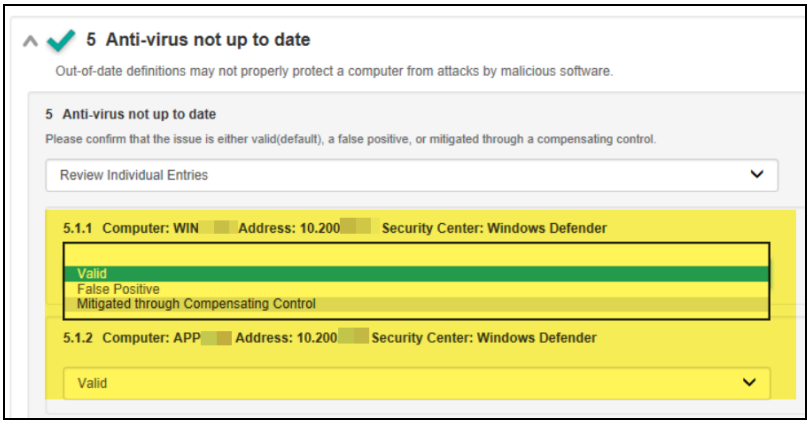
i. Choose this option to enter a blanket response as to why all instances of the issue have been mitigated. For example, why do you not need signed agreements with your business associates that transmit ePHI?

ii. When you indicate that an issue has been mitigated, enter an **Optional Response** explaining how the issue has been resolved or why it's not relevant. These notes will appear in your final assessment documentation.



B. **Review Individual Entries**

i. You can also choose to review each issue separately. This is useful if you need to explain why some of your PCs are detected as not having anti-virus or account lockout enabled, for example. When you choose to review individual entries, you can likewise indicate whether each entry is mitigated, valid, or a false positive.



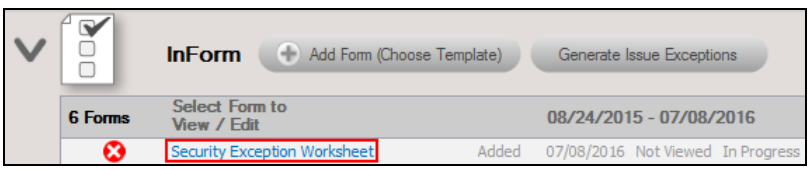
C. **Valid**: Indicates that the issue is valid and has not been addressed.

D. **False Positive**: Indicates that the issue is NOT valid and does not need to be addressed. Choose this option if you have trouble with the results from an automated scan, for example.

Important: Assessments completed and archived before 3/8/2019 will use the legacy Security Exception Worksheet. In order to access the new version of the worksheet:

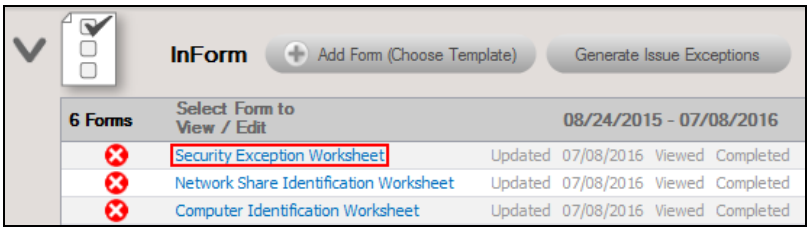
1. Open your archived assessment.
2. Open the Security Exception Worksheet from your archived assessment.
3. Generate a Word Reports Form containing responses to maintain a record of the Security Exceptions documented using the legacy Security Exception Worksheet.
4. Delete the old Security Exception Worksheet.
5. A new Security Exception Worksheet will be generated in its place. Complete all required entries in the worksheet and proceed with your assessment.

To open and complete the Security Exception Worksheet, click on the name label for the **Security Exception Worksheet** entry in the InForm Questionnaire/Worksheet list located below the InForm Bar at the bottom of the Assessment window.



Exceptions are grouped by a number of exception types that may include: Business Associate Agreements, Former Employee/Vendor Enabled Accounts, Remote Access Cloud Services, Firewall, Office Environment, Wireless, Endpoint Protection, and External Vulnerability Scan categories.

You can return to the Security Exception Worksheet by clicking on the name label located under the InForm Bar at the bottom of the Assessment Window.

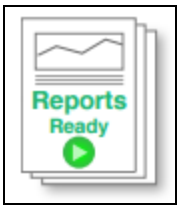


Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 83 for helpful time-saving features when using InForm.

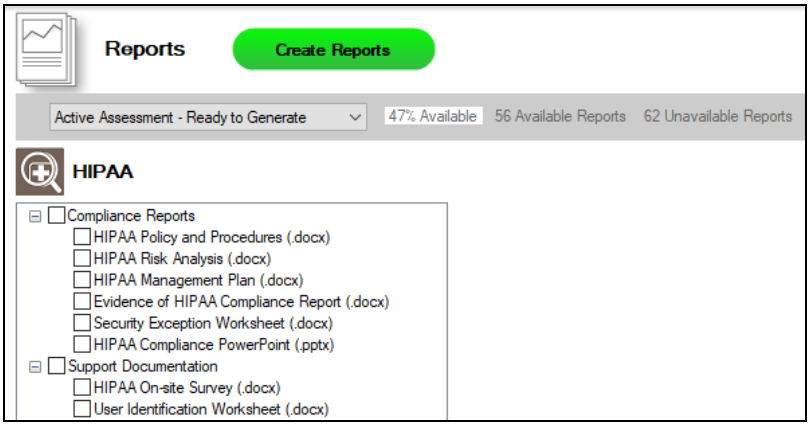
Generate HIPAA Compliance Assessment Reports

Once the assessment is complete, you can generate reports and supporting documentation. To do this:

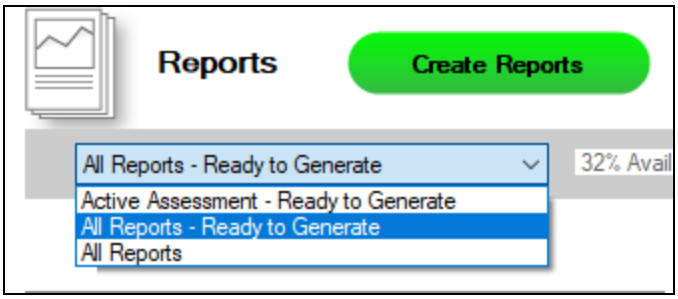
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



4. Select which of the HIPAA Compliance Assessment reports that you want to generate.

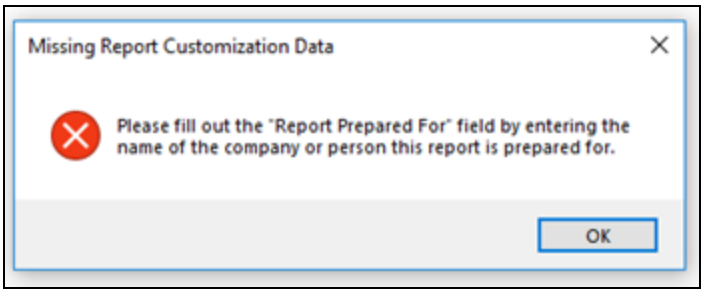


You can use the Reports drop-down menu to filter reports related to the active assessment project, reports that are ready to generate, or to browse all available reports.



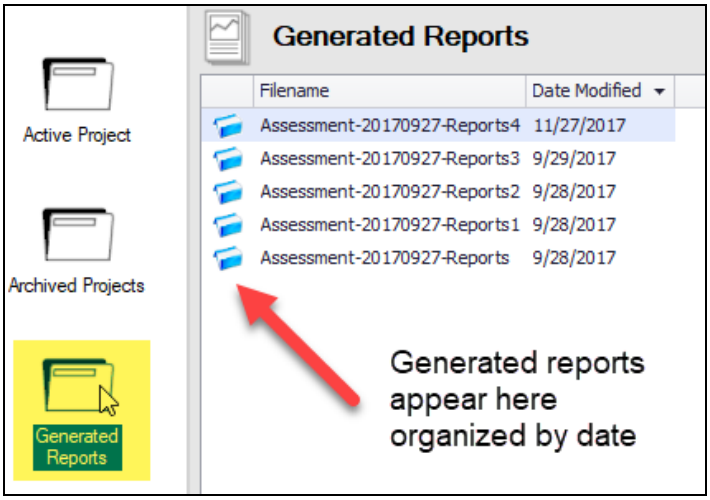
5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.

    i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



> **Tip:** See the Network Detective User Guide for instructions on how to customize your reports with your company's branding.

Click **Generated Reports** from the left-hand Site menu to access previously generated reports. Double click a set of assessment reports to open the folder in Windows Explorer.



Note on Time to Generate Reports

> **Important:** Larger data sets will require more time to generate reports. If the data set is especially large — in the range of several thousand users, for example — a full set of reports may take several hours to complete.

HIPAA Assessment Reports

The HIPAA Assessment Module can generate the following reports and supporting documents:

Compliance Reports

These reports show where you are in achieving HIPAA compliance. In addition, these documents identify and prioritize issues that must be remediated to address HIPAA related security vulnerabilities through ongoing managed services.

Report Name	Description
Evidence of HIPAA Compliance	Just performing HIPAA-compliant tasks is not enough. Audits and investigations require evidence that compliance tasks have been carried out and completed. Documentation must be kept for six years. The Evidence of Compliance includes log-in files, patch analysis, user & computer information, and other source material to support your compliance activities. When all is said and done, the proof to proper documentation is accessibility and the detail to satisfy an auditor or investigator included in this report.
HIPAA Compliance PowerPoint	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.
HIPAA Management Plan	Based on the findings in the Risk Analysis, the organization must create a Risk Management Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, Network Detective provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Management plan defines the strategies and tactics the organization will use to address its risks.
HIPAA Policies & Procedures	The Policy and Procedures are the best practices that our industry experts have formulated to comply with the technical requirements of the HIPAA Security Rule. The policies spell out what your organization will do while the procedures detail how you will do it. In the event of an audit, the first thing an auditor will

Report Name	Description
	inspect are the Policies and Procedures documentation. This is more than a suggested way of doing business. The Policies and Procedures have been carefully thought out and vetted, referencing specific code sections in the Security Rule and supported by the other reports include with the HIPAA Compliance module.
HIPAA Risk Analysis	HIPAA is a risk-based security framework and the production of a Risk Analysis is one of primary requirements of the HIPAA Security Rule's Administrative Safeguards. In fact, a Risk Analysis is the foundation for the entire security program. It identifies the locations of electronic Protected Health Information (ePHI,) vulnerabilities to the security of the data, threats that might act on the vulnerabilities, and estimates both the likelihood and the impact of a threat acting on a vulnerability. The Risk Analysis helps HIPAA Covered Entities and Business Associates identify the locations of their protected data, how the data moves within, and in and out of, the organization. It identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of ePHI. The value of a Risk Analysis cannot be overstated. Every major data breach enforcement of HIPAA, some with penalties over $1 million, have cited the absence of, or an ineffective, Risk Analysis as the underlying cause of the data breach. The Risk Analysis must be run or updated at least annually, more often if anything significant changes that could affect ePHI.
HIPAA Risk Profile	A Risk Analysis should be done no less than once a year. However, Network Detective has created an abbreviated version of the Risk Analysis called the HIPAA Risk Profile designed to provide interim reporting in a streamlined and almost completely automated manner. Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.
Security Exception Worksheet	The report is used present the details associated with security exceptions and how compensating controls will be or have been implemented to enable HIPAA compliance. This worksheet allows the HIPAA Compliance readiness specialist to document

Report Name	Description
	explanations on suspect items. The readiness specialist is enabled to document and explain why various discovered items are not true issues and possible false positives. These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The Security Exception Worksheet compiles the issues discovered by the HIPAA Compliance Data Collection including the completion of the questionnaires and worksheets. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements. The Security Exception Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk. The process is consistent with industry standard HIPAA assessment and risk management processes

Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
Computer Identification Worksheet	The Computer Identification Worksheet takes the list of computers gathered by the Data Collector and lets you identify those that store or access ePHI. This is an effective tool in developing data management strategies including secure storage and encryption. To save time the system allows you to enter default settings for all computers and just change some as needed. There is also an inactive computer identification worksheet.
Disk Encryption Report	Encryption is such an effective tool used to protect data that if an encrypted device is lost then it does not have to be reported as a data breach. The Disk Encryption Report identifies each drive and volume across the network, whether it is fixed or removable, and if Encryption is active.
External Network Vulnerability Scan Detail by Issue	Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.
File Scan Report	The underlying cause identified for many data breaches is that the organization did not know that protected data was stored on a device that was lost or stolen. After a breach of 4 million patient records a hospital executive said, "Based on our policies that data should not have been on those systems." The File Scan Report identifies data files stored on computers, servers, and storage devices. It does not read the files or access them, but just looks at the title and file type. This report is useful to identify local data files that may not be protected. Based on this information, the risk of a breach could be avoided if the data was moved to a more secure location, or mitigated by encrypting the device to protect the data and avoid a data breach investigation.
HIPAA On-Site Survey	The On-site Survey is an extensive list of questions about physical and technical security that cannot be gathered automatically. The survey includes questions ranging from how

Report Type	Description
	facility doors are locked, firewall information, how faxes are managed, and whether servers are on-site, in a data center, or in the Cloud.
Inactive Computer Identification Worksheet	In this worksheet you identify computers that are detected as inactive for a long period of time. Such computers pose a potential data risk as they are likely not managed and/or secured.
Login History by Computer Report	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.
Network Share Identification Worksheet	The Network Share Identification Worksheet takes the list of network shares gathered by the Data Collector and lets you identify those that store or access ePHI. This is an effective tool in developing data management strategies including secure storage and encryption. To save time the system allows you to enter default settings for all network shares and just change some as needed
Share Permission Report	Comprehensive lists of all network "shares" by computer, detailing which users and groups have access to which devices and files, and what level of acfcess they have.
User Identification Worksheet	The User Identification Worksheet takes the list of users gathered by the Data Collector and lets you identify whether they are an employee or vendor. Users who should have been terminated and should have had their access terminated can also be identified. This is an effective tool to determine if unauthorized users have access to protected information. It also is a good indicator of the efforts the organization goes to so terminated employees and vendors have their access quickly disabled. Another benefit is that you can review the user list to identify generic log-ons, such as Nurse, Billing Office, etc., which are not allowed by HIPAA since each user is required to be uniquely identified. To save time the system allows you to enter default settings for all users and just change some as needed.

Change Reports

Report Name	Description
Baseline HIPAA Management Plan	The Risk Management plan defines the strategies and tactics the organization will use to address its risks.
Baseline HIPAA Risk Profile	The Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks.

Appendices

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

Pre-Scan Network Configuration Checklist 76
Checklist for Domain Environments 76
Checklist for Workgroup Environments 78

Completing Worksheets and Surveys 80
Entering Assessment Responses into Surveys and Worksheets 80
Add Image Attachments to Surveys and Worksheets 82
Add SWOT Analysis to Surveys and Worksheets 82
Time Savings Tip to Reduce Survey and Worksheet Data Input Time 83
Use the InForm Worksheet Tool Bar 83
Bulk Entry for InForm Worksheets 84
Create Word Response Form 86
Import Word Response Form 88

Adding an Inspector to a Site 89

Site Assessment Reports and Supporting Documents Locations 91

Initiate Internal Vulnerability Scan on the Inspector Appliance and Download Results 94
Download Appliance Scans 99

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 the .NET 4.6.2 framework installed on machines in order to use all data collector and server/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 Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

Before you perform a workgroup assessment, run the following PowerShell commands on the target network and the machine that will perform the scan. These three configurations should help you avoid most issues in a workgroup environment. Each command is followed by an explanation and link to Microsoft documentation.

1. `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`

   By default, UAC only allows remote administration tasks to be performed by the Built-in Administrator account. To work around this, this command sets the LocalAccountTokenFilterPolicy registry key to 1. This allows any local admin to perform remote administrative tasks (i.e. access to system shares C$, Admin$, etc.).

   https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows

2. `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes`

   This command creates an Inbound firewall rule to allow access to the WMI service and namespaces.

   https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista

3. `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`

This command creates an Inbound firewall rule which enables File and Printer Sharing on the machine. File and printer sharing is required in order to access the Admin$ share on remote machines.

https://answers.microsoft.com/en-us/windows/forum/all/turning-on-file-and-printer-sharing-windows-10/bb3066eb-f589-4021-8f71-617e70854354

You can also 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.
☐	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:

Complete?	Workgroup Configuration
	• 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.

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:

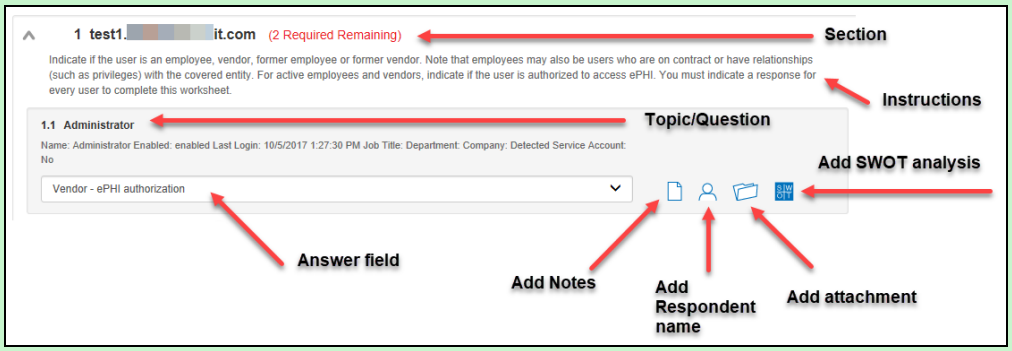
- use of automated scans
- importing responses from Word documents
- typing the information directly into surveys and worksheets forms

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 HIPAA Compliance 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" on the facing page 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" below 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.

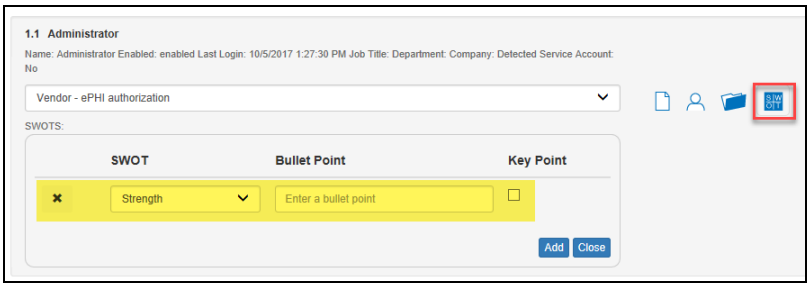
> **Note:** Once you complete your assessment and generate reports, your attached images will appear alongside the form item in the published report and/or supporting document.

Add SWOT Analysis to Surveys and Worksheets

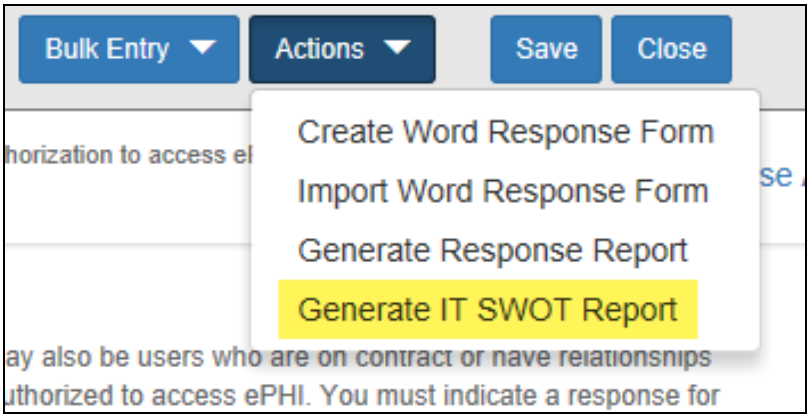
The IT SWOT analysis is a structured method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats affecting an IT network. The analysis involves identifying internal and external issues that are favorable and unfavorable to increasing the overall network health and security of the environment.

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**.

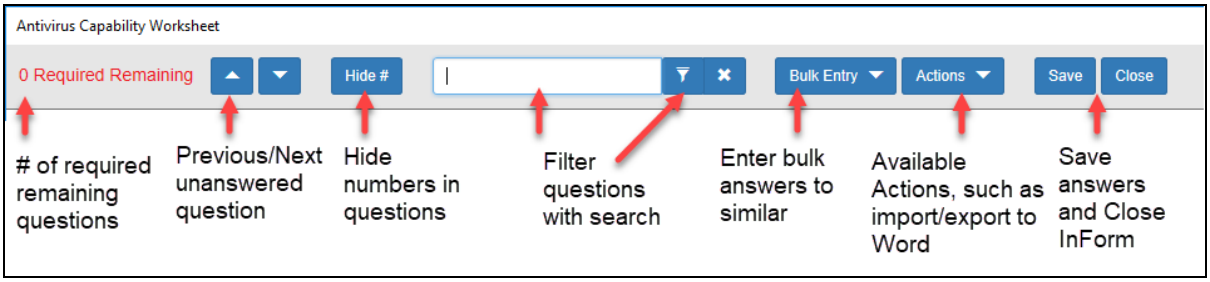


Note: A folder will open with your generated IT SWOT Report. You must generate this report separately for each InForm in your assessment.

Time Savings Tip to Reduce Survey and Worksheet Data Input Time

Use the InForm Worksheet Tool Bar

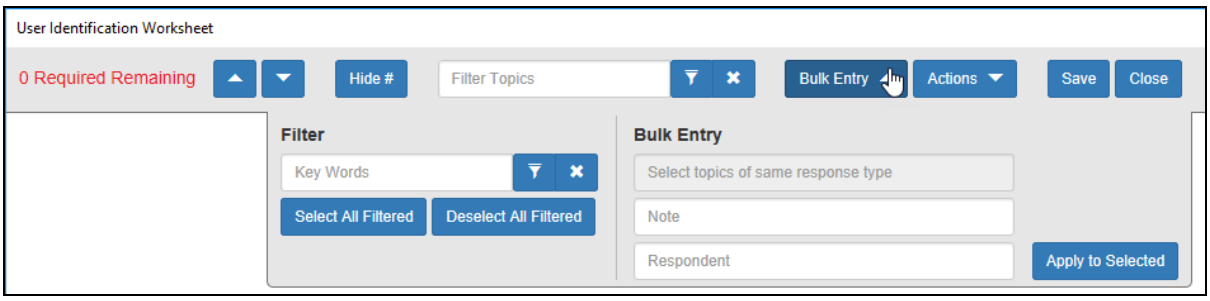
Use the InForm tool bar to save time when completing worksheets.



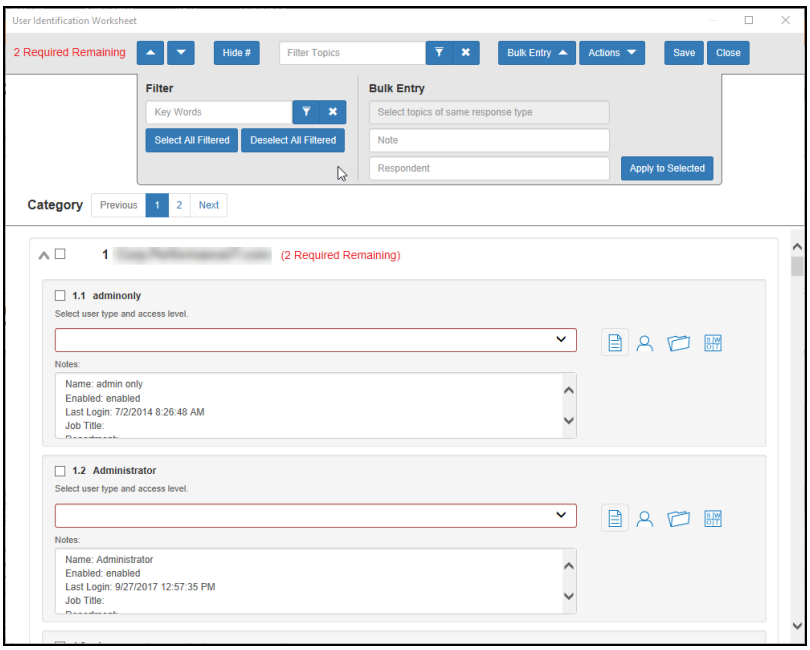
Bulk Entry for InForm Worksheets

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:

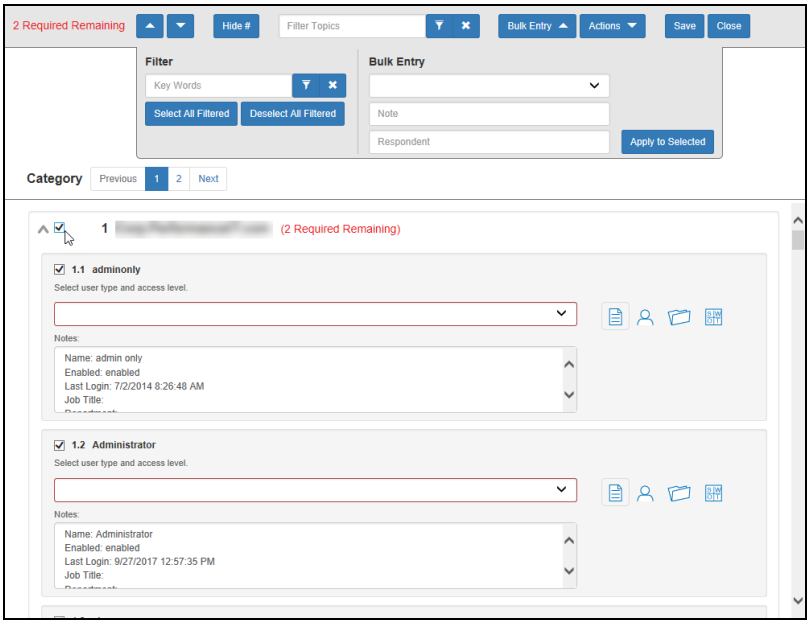
1. Click **Bulk Entry** from the Inform tool bar.



Check boxes will appear next to the response topics.

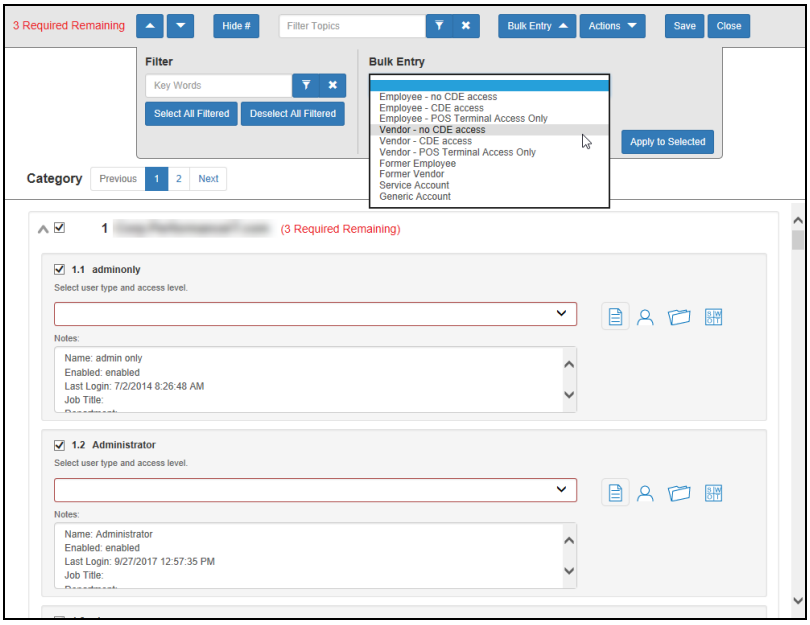


2. Select the check boxes for the topics for which you wish to enter bulk responses.

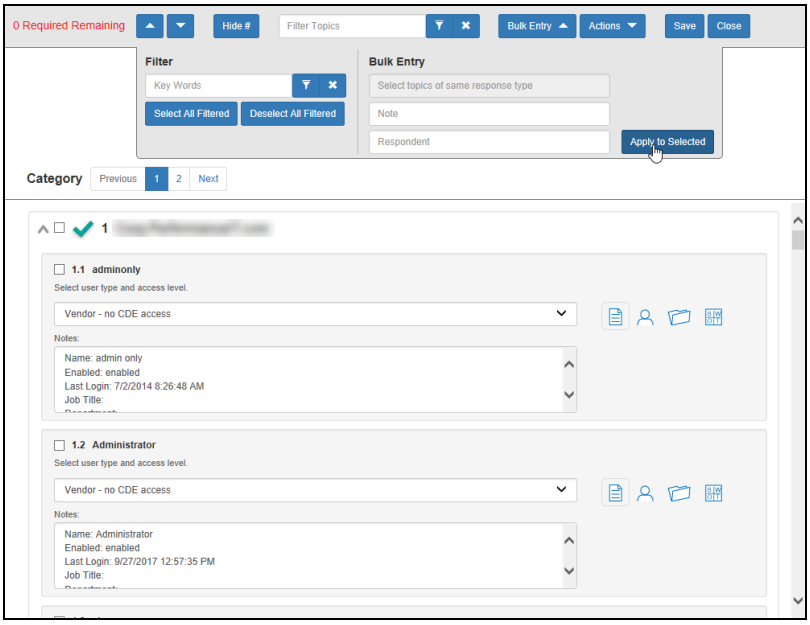


Note: You can select individual topics, or you can click the check box next to the section heading to select all topics within the section. You can also **Filter** topics using terms like "Admin." Note that each topic within the section must require the same types of responses in order to enter bulk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

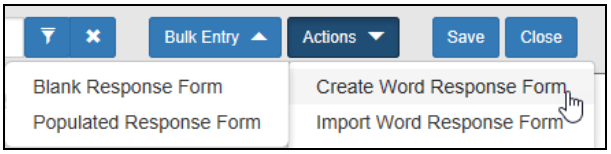
You can export InForm worksheets in your assessment project to Word. This allows you or others to complete worksheets without using Network Detective. For example, you can create a Word response form and send it to a client at a site. The client can then help you gather the required information and enter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

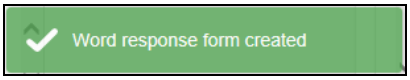
1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
    a. Click **Blank Response Form** to generate a Word document with blank fields ready for data entry.

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.



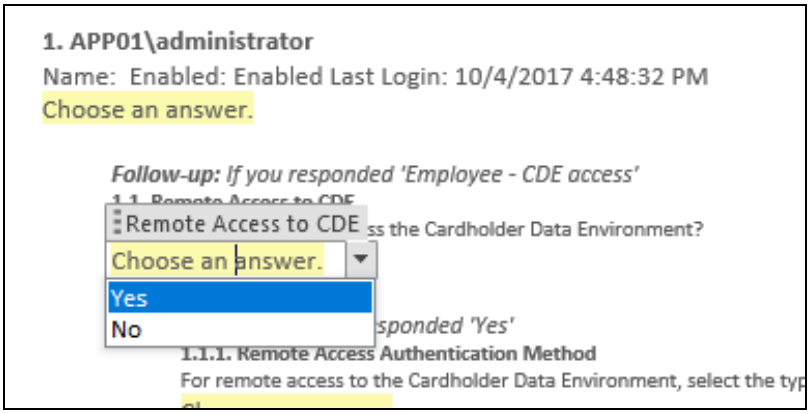
Important Note on Working with Word Response Forms

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

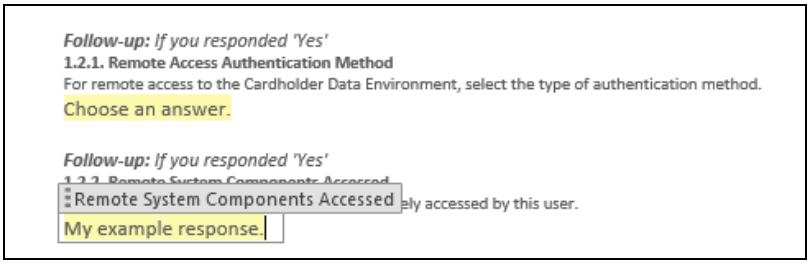
- **DO NOT DELETE** the field controls embedded in the response form! The response fields appear in the images below for your reference:

  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.

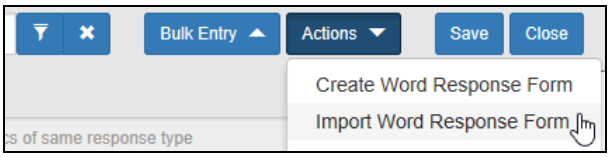
Step 2: Send it to a client to enter additional information about the site using Word.

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.

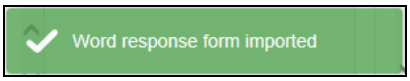
To import a Word response form:

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**.

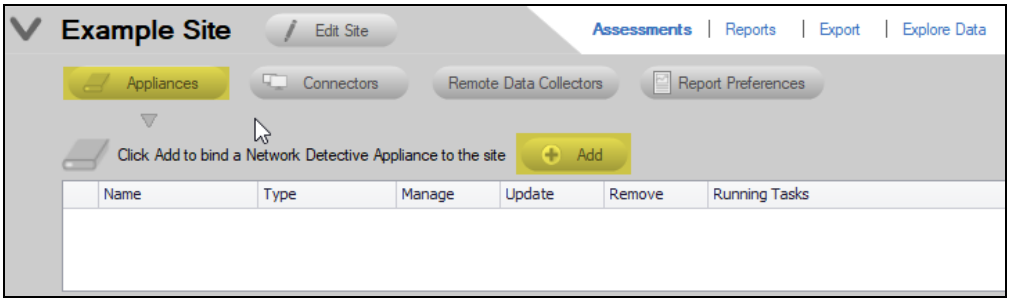
A confirmation message will appear. The InForm worksheet fields will be updated with the imported responses.



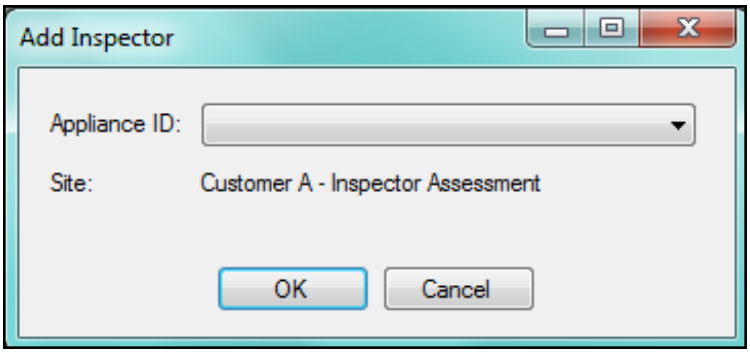
Adding an Inspector to a Site

After starting a new assessment, or within an existing assessment, in order to "Associate" and Inspector Appliance with the Assessment Project, you must first select the **V** symbol to expand the assessment properties view.

This action will expand the Assessment's properties for you to view and to add an Inspector to the Assessment.

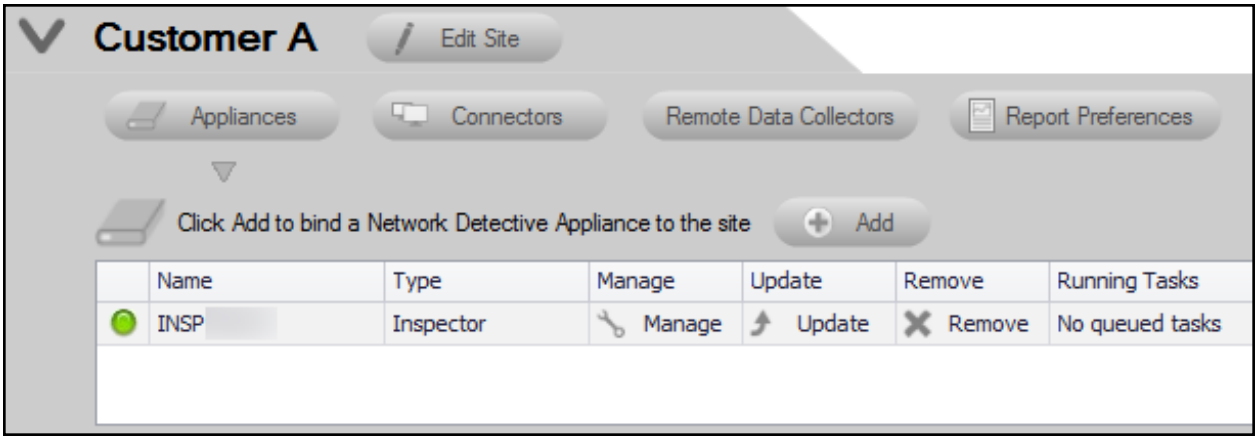


To add an Inspector to an Assessment, from the Assessment's dashboard select the **Inspector** button, then the **Inspector Add** button as noted above.

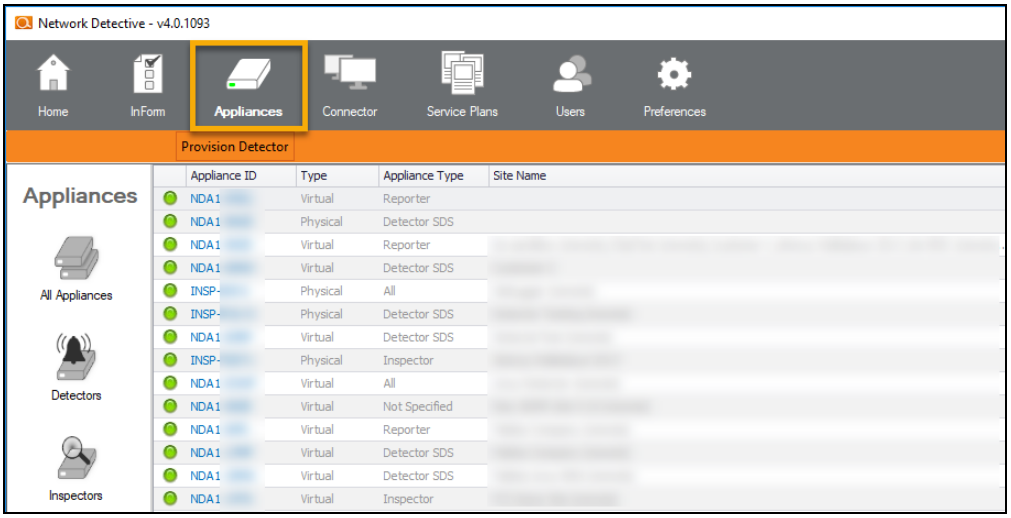


Select the **Inspector ID** of the Inspector from the drop down menu. Note that the Inspector ID can be found on a printed label on the Inspector Appliance.

After successfully adding an Inspector it will appear under the **Inspector** bar in the Assessment's dashboard.



To view a list of all Inspectors and their associated Sites, navigate to the **Appliances** tab from the top bar of the Network Detective Home screen. This will show a summary of all Inspectors, their activity status, and other useful information.



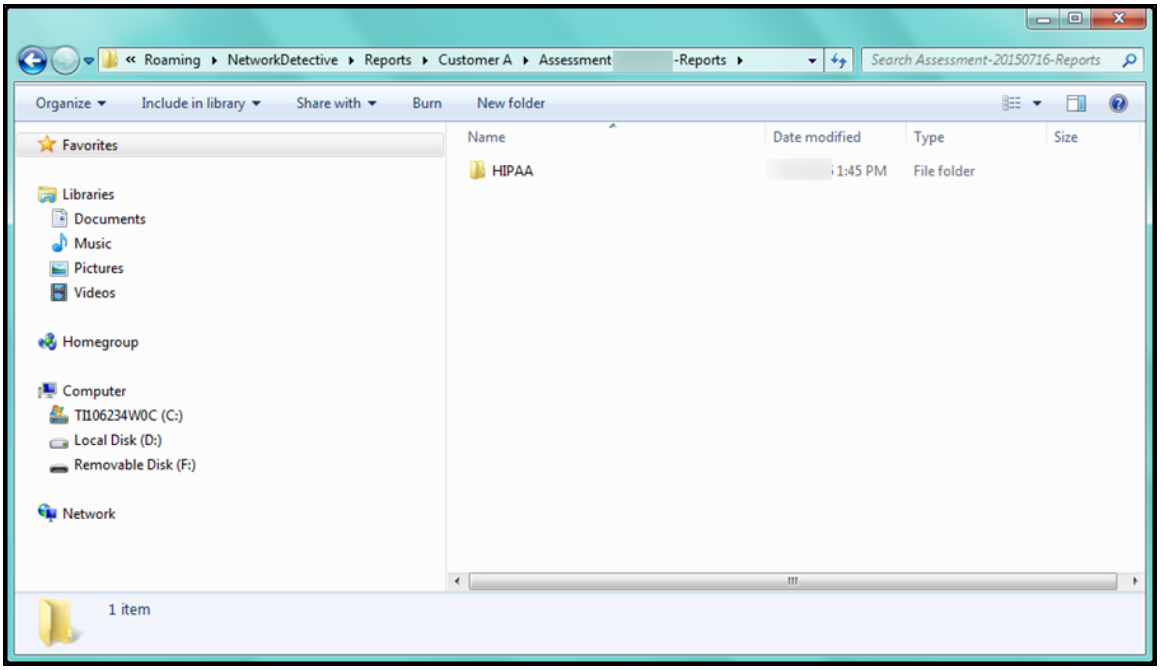
To return to the **Site** that you are using to perform your assessment, click on Home above and select the Site that you are using to perform your assessment.

Site Assessment Reports and Supporting Documents Locations

The reports document files produced by the HIPAA Module are stored in a folder located on the hard disk of the computer operating the HIPAA Module.

For example, the figure below illustrates the location of the Assessment Report folder a HIPAA assessment for a site named **Customer A**.

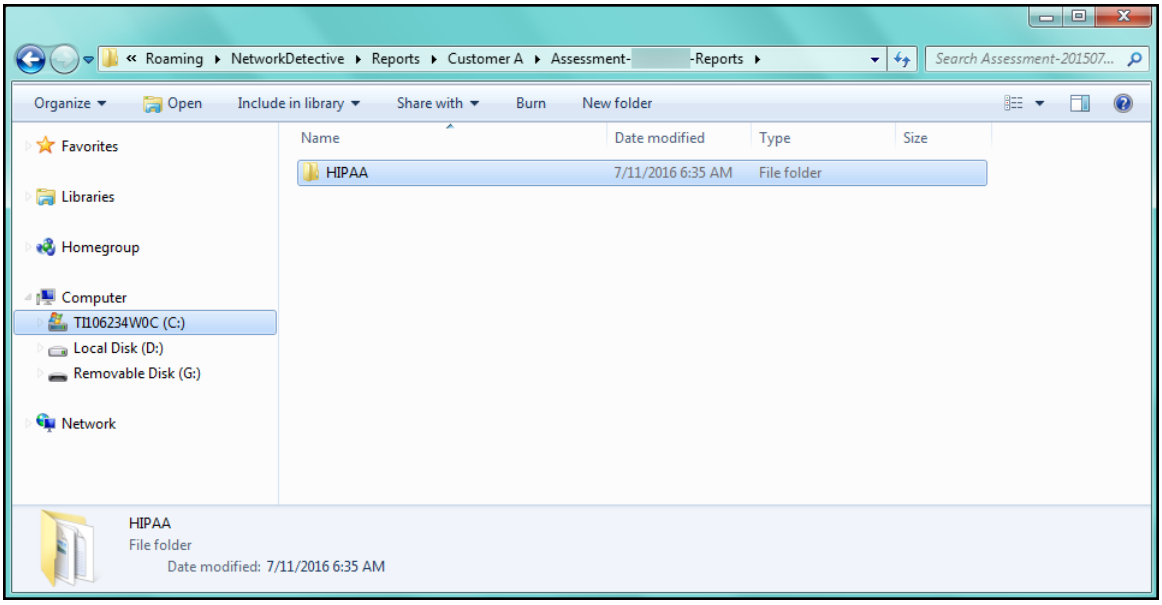
In the folder path referenced in the Windows Explorer folder window displayed below, the reference to **Customer A** is a reference to the HIPAA assessment's Site Name associated with the actual assessment.



To access the reports, you would double click on the assessment reports folder.

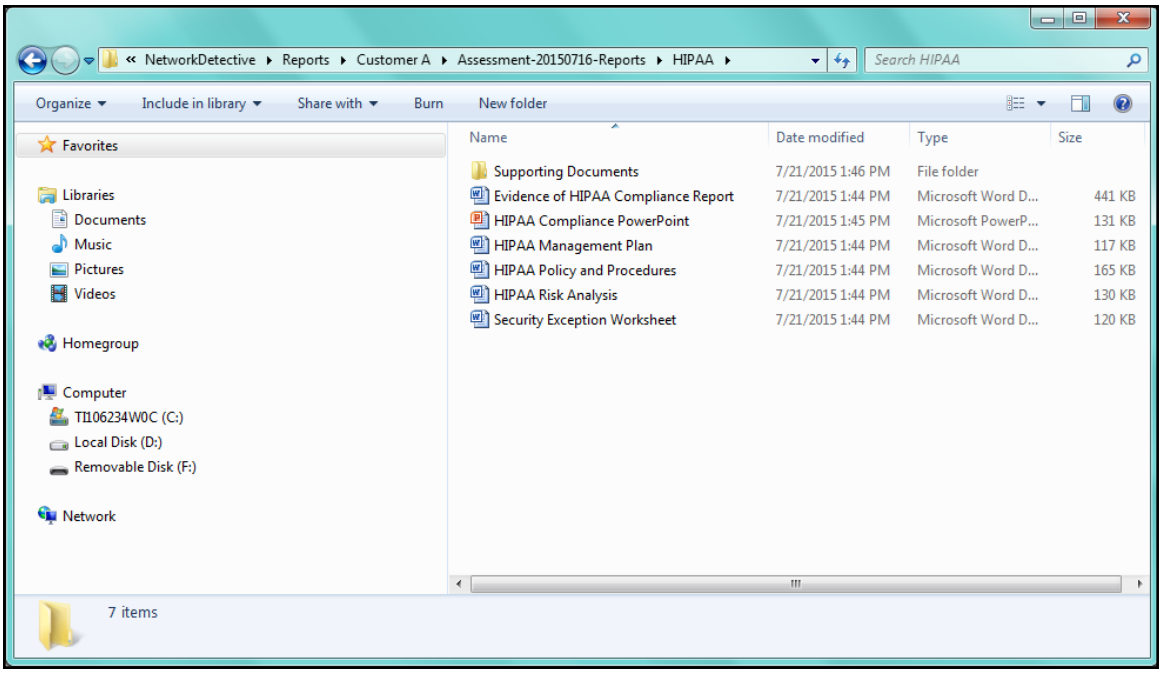
In this example the assessment reports folder is named: **Assessment 20150716-Reports**.

Windows Explorer will then display folder named **HIPAA** as shown below.



The **HIPAA folder** is the location where the HIPAA assessment's report documents, HIPAA Evidence of Compliance, and supporting survey and worksheet documents are stored.

Upon doubling clicking the **HIPAA folder** in Windows Explorer, the reports and supporting documents for the assessment are available for viewing and editing.

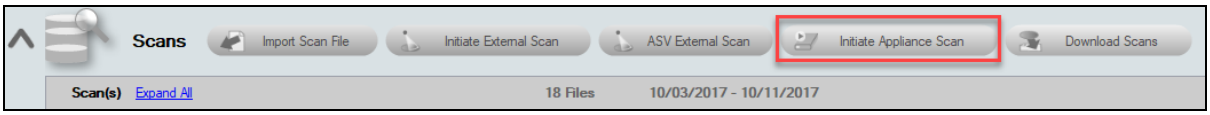


Opening the **Supporting Documents** folder will enable access to all of the supporting documents as seen below.

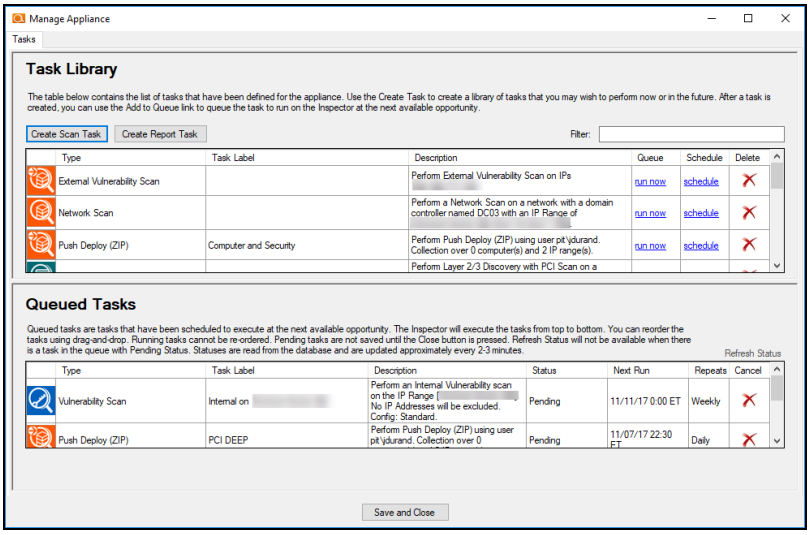
Initiate Internal Vulnerability Scan on the Inspector Appliance and Download Results

If you have an Inspector Appliance, an internal vulnerability scan of the target network can enhance your HIPAA assessment. The scan is initiated from the Network Detective Application. Please note that the scan may take several hours to complete.

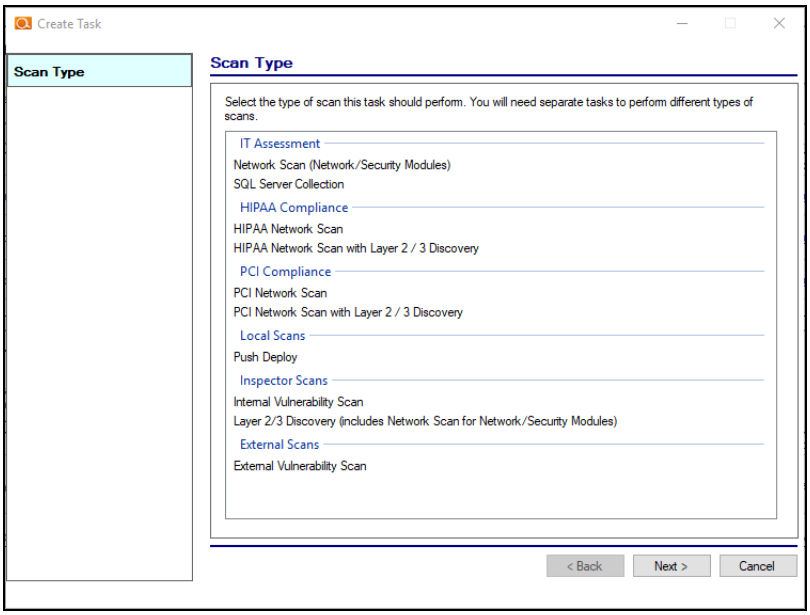
1. Click on the **Initiate Appliance Scan** button located on the Scans Bar.



2. The Manage Appliance window will appear. Click **Create Scan Task**.

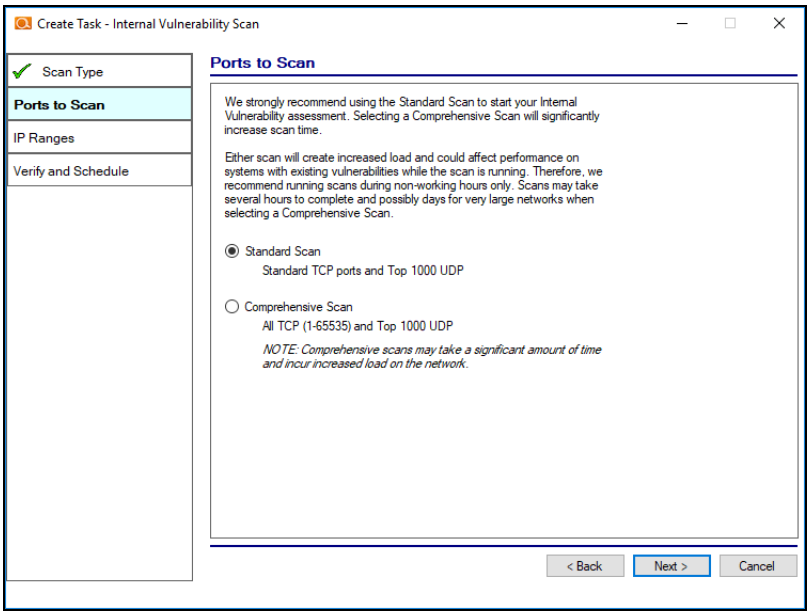


3. The Create Task window will appear. Under Inspector Scans, select the **Internal Vulnerability Scan** option, and then click **Next**.



4. The Ports to Scan window will be displayed. The Ports to Scan setup option allows you to select one of two available scanning options.
    - **Standard Scan** is used to scan Standard TCP ports and Top 1000 UDP ports.
    - **Comprehensive Scan** is used to execute a comprehensive scan of all TCP ports and Top 1000 UDP ports.

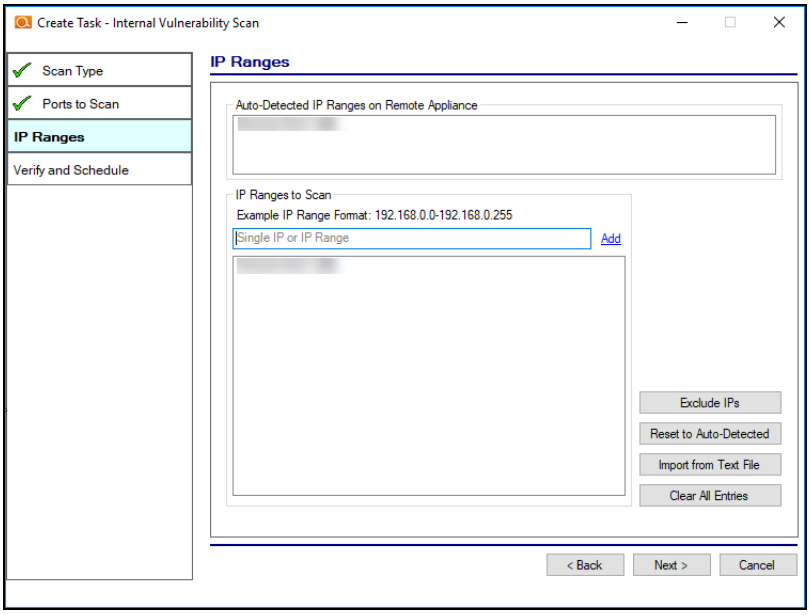
    To proceed, select the appropriate number of ports to scan for your assessment's purposes. Then click **Next**.



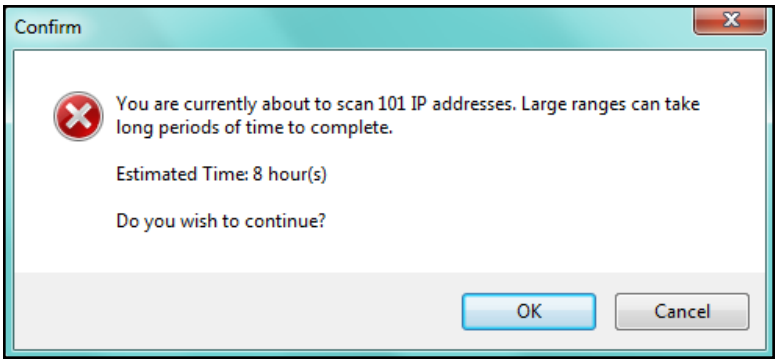
5. At this point the Network Detective HIPAA Module will connect with the Inspector appliance and Auto-Detect an IP address range that can be scanned. The IP Ranges screen will then be displayed. You can also manually set the IP address range that you would like to scan during the scheduled Internal Vulnerability Scan. Define the IP Range that you would like to scan and click **Next**.

> **Important:** The Auto-Detect feature will identify the IP range of the internal subnet that is from the Inspector. This could result in a substantially larger number of IP addresses that will be scanned verses the actual number of workstations, servers, and other IP-based network components (which could be a far smaller number). If the internal vulnerability scan is configured to scan a large number of IP addresses that are not used by any device, the vulnerability scan may take much longer than necessary.

> **Note:** To reduce the scan time, research the specific ranges of IP addresses used within the network to identify the smallest range to use for the scan.

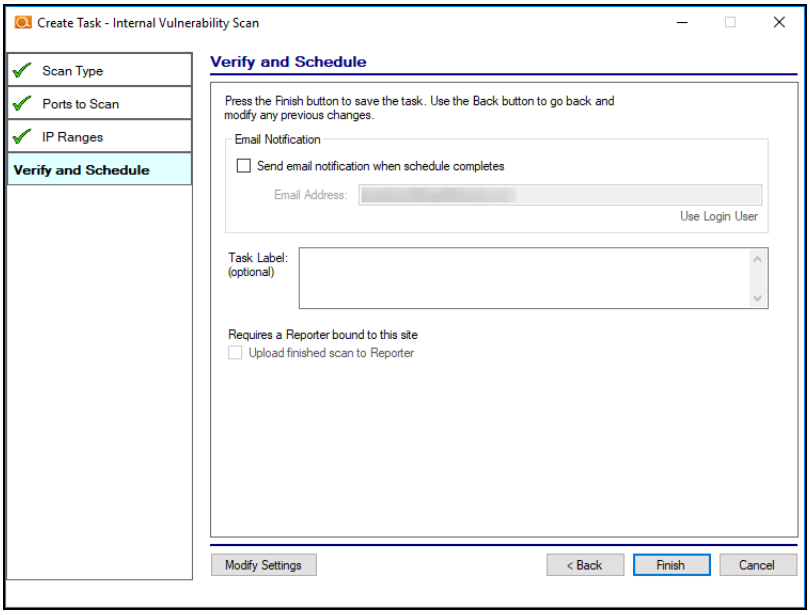


6. You will be then notified about the estimated amount of time necessary to perform the scan on the IP Range that you specified.



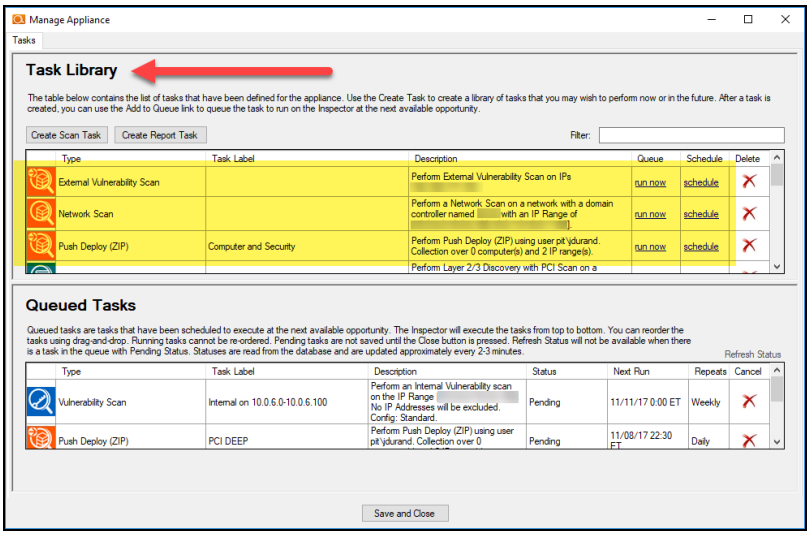
Before proceeding, be sure to note the time estimated within the Confirm Window. Click **OK**.

7. The Verify and Schedule window will be displayed. To have an Email Notification sent to you when the scan task completes, select the **Send email notification when schedule completes** option, and type in the email address where the notification should be sent.



8. Click **Finish**.

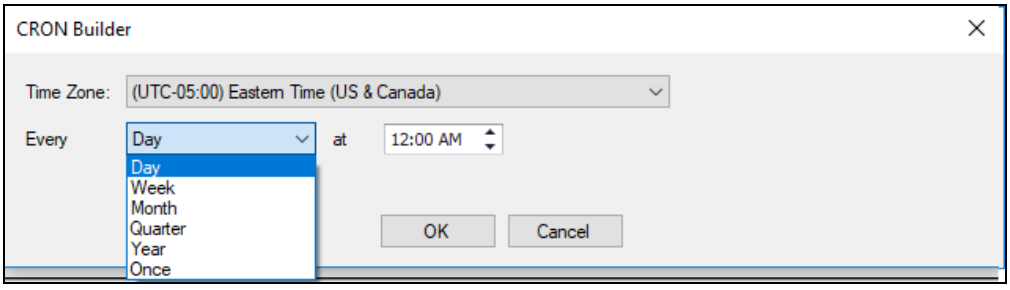
Once you create the scan task, it will appear as a task in the appliance Task Library.



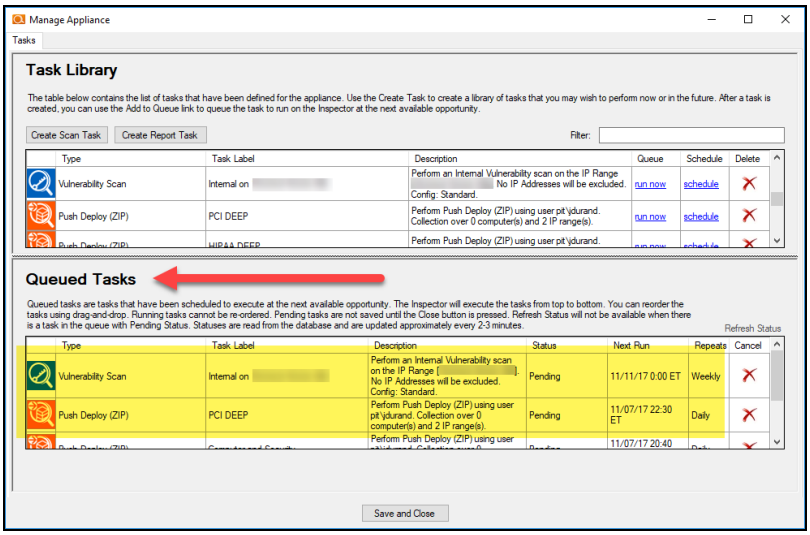
In order to initiate the scan, you will need to move the scan from the Task Library into the list of Queued Tasks. There are two ways to do this:

a. Select the **run now** option link under the Queue column to initiate the scan. This will place the scan directly into the Queued Tasks list.

b. Or, click **schedule** to execute the scan sometime in the future. When you click the schedule link, the CRON Builder scheduler window is displayed and is used to set the schedule action's execution time.



Whether you choose to run the scan now or schedule the scan to take place in the future, it will be added to the Queued Tasks list, where you can check its status. This is the final step in initiating (or scheduling) a scan.



Download Appliance Scans

1. Select the appliance for which you would like to download scans.