NETWORK DETECTIVE™

USER GUIDE

IT Assessment Modules

Instructions to Perform IT Assessments with Network Detective

1/22/2024 2:33 PM

Contents

Network Detective User Guide

This document is intended for users of Network Detective. It will guide you through the initial use of the software as well as the more advanced features. Additional guides are available for various modules. This guide is designed to be used in conjunction with other supplementary guides.

It is recommended that you **review the Table of Contents** for this guide and select the sections of the guide for review that are relevant to the assessment you are performing using Network Detective.

Within this guide, information is presented on how to use the following Network Detective modules:

- "Performing a Network Assessment" on page 35
- "Performing a Security Assessment" on page 106
- "Performing an Exchange Assessment" on page 172
- "Perfoming an SQL Server Assessment" on page 197

About Network Detective

Network Detective performs automated assessments to uncover and document network assets, problems and security risks. Service Providers and MSPs save countless hours when proposing or on-boarding new clients and performing periodic network documentation of existing customers, while IT departments benefit from periodic reports to assist in network documentation and compliance projects.

Annual subscribers enjoy the benefit of running an unlimited number of scans and reports along with the Export feature, which integrates with other services, like Autotask, ConnectWise, and Tigerpaw, to automatically populate configuration items.

Network Detective Overview

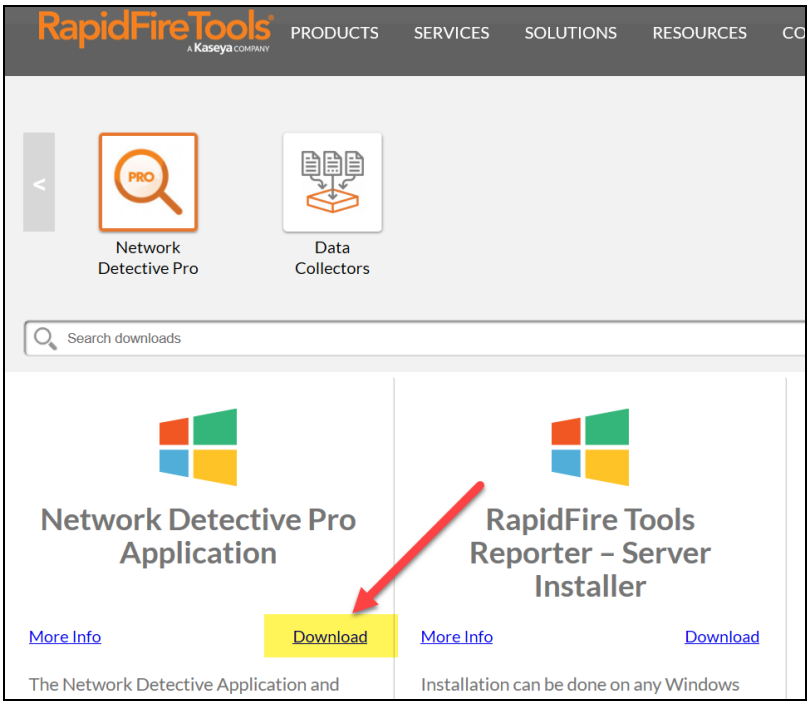
Network Detective is composed of the Network Detective application, the **Network Assessment Data Collectors** (for Network and Security modules), and various other Data Collectors for Exchange and SQL Server assessments, the **Push Deploy Tool** which is used to set up and execute local computer scans from a centralized location on the network, and the optional **External Vulnerability scanner** (available for use within the Security, HIPAA, and PCI Modules).

Network Detective is quick and easy to use; there are just four basic **Phases** used when performing an Assessment:

1. **Run the Network Detective Application to Create Site Files to Manage Your Assessments** — Site files can be created to manage assessments for specific customer accounts, remote office locations, data centers, departments, organizational units, or any structure that is applicable to the environment on which you are performing an IT or Risk assessment.
2. **Start a New Assessment Project** — Once the **Site** is created; you start a new **Assessment** project and perform the type of assessment's data collection process as detailed in the assessment process **Checklist** that you can view in the **Assessment Window**. After each scan type is complete, run the Network Detective app and go to your **Active Assessment project**, and import the scan files generated in step 3 into the assessment.
3. **Perform the Assessment and Data Collection** — Run scans as required for the selected **Assessment** process. If possible, run Network Scans from the Primary Domain Controller on the network and perform scans on local computers and servers as required. The output of the scan will be a .zip file containing module specific scan files (.ndf, .cdf, .sdf). **Be sure that you document the name of the folder used to store scan data results files for later importing into your assessment project.**
4. **Generate Assessment Reports** — Customize the reports to be presented to your customers by setting up your company's branding of the report to be generated with your logos and client information. Then run the reports.

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.

Set Up Network Detective Reports

Either before or after you perform your first assessment using Network Detective, you may wish to configure Network Detective's report generation tool to use your company's logos and business document text format and color themes.

By customizing Network Detective's Reports settings, the reports produced by Network Detective for presentation to your customers will conform to your company's corporate branding and image standards.

Setting Report Branding and Customization Preferences

Network Detective enables the ability for you to brand the reports produced by the tool with your company's standard logos, disclaimers, themes, and cover page images.

Tip: You can now apply several updated document styles to your reports. These new styles enhance the overall look and visual design of the documents. See " Access Updated Report Styles" on page 31 for instructions.

Setting Reports Preferences at the Global or Site Level

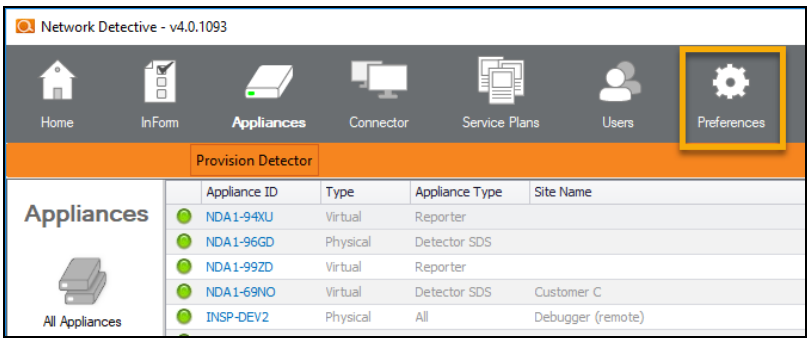
You can configure the report branding by configuring the **Report Defaults** settings at one of two levels:

- at the Global level (for all Sites) using the Network Detective **Preferences** option
- at the Site level through the use of the Site's Preferences

To set the **Report Defaults** necessary to use your company's branding within the reports produced by Network Detective, customize the preferences found throughout this section as referenced below.

Access and Set Reports Defaults Preferences at the Global Level

To set one or more of the **Reports Defaults** preferences, select the **Preferences** option located at the top of the Network Detective application window.



> **Note:** The Report Defaults are global settings and all new Sites and Assessments will rely on these settings when reports are generated after an Assessment has been performed.

By selecting the **Network Detective Preferences** option, the **Reports Preferences** window will be displayed to enable you to set the global branding standards for all reports generated by **Network Detective**. If you select the Global Reports Preference option, please proceed to the section below entitled **Setting Reports Preferences** found on the next page.

Access and Set Reports Defaults Preferences at the Site Level

Network Detective "Site"

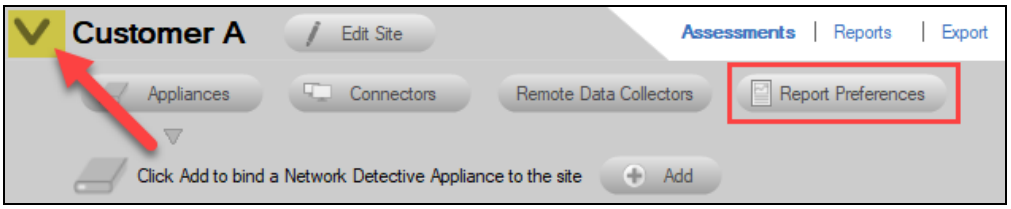
Before starting an **Assessment** using Network Detective, it is required that you create a Network Detective "**Site"**.The Network Detective **Site** is typically associated with a specific client's network or office location. Within a **Site**, **Assessment Projects** are set up, performed, and include the generated **Reports** as a result of the assessment performed.

Setting Reports Preferences

To set one or more of the **Reports Defaults** preferences at the **Site Level**, select the **Site Preferences** option located at the top of the Network Detective application window.

From the Site's Dashboard, select the selector control to the left of the Assessment's name to access the **Report Preferences** setup option.

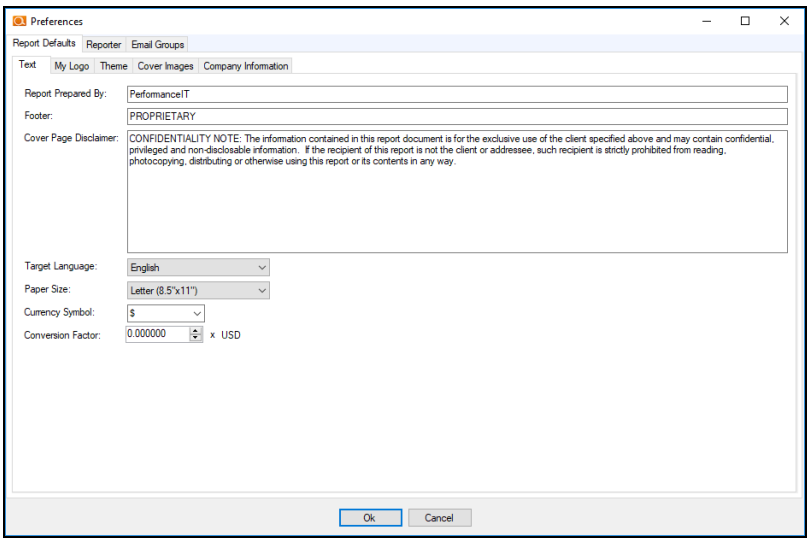
The **Site's Preferences** will be displayed.



By selecting the **Reports Preference** button, the **Reports Preferences** window will be displayed to enable you to set the **Site Level** branding standards for all reports generated for **Assessments** performed within a specific Network Detective **Site**.

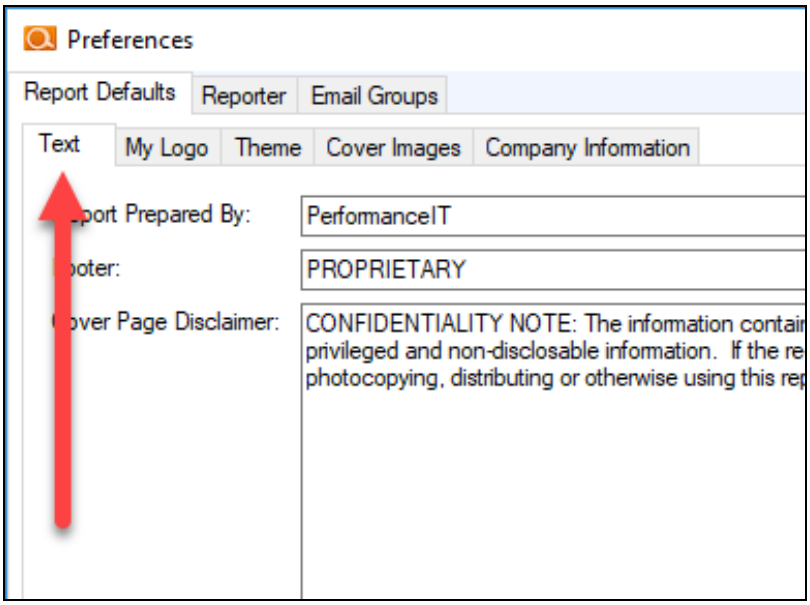
Setting Reports Preferences

Once the **Reports Preferences** window is displayed, the **Report Defaults** options will be available so that you can configure the available options to implement your company's branding standards within the reports. These options include **Text**, **My Logos**, **Theme**, and **Cover Images**.



Set Reports Text Preferences

Select the **Text Tab** of the **Report Defaults** window, to set the **Text** branding preferences.



There are five reports text preferences that can be set within the **Report Defaults Text** page:

1. **Report Prepared By***: This is you, your company, your DBA.
2. **Footer***: This is the footer of the document, and appears on all pages. By default it reads, “PROPRIETARY & CONFIDENTIAL”
3. **Cover Page Disclaimer***: By default this is a confidentiality disclaimer, but could also could serve well for Copyright.
4. **Target Language**: Select the language to be used when producing reports. Target languages include English, German, Spanish, French (Canadian), and Italian.
5. **Paper Size**: Select the default page size to be used when reports are generated and formatted.

Set the **Reports Defaults Text** preferences and then select the **Preferences Window Ok** button to save the preferences.

If you need to set other Reports Defaults preferences then continue by selecting the window tab associated with the **Reports Defaults** preferences that you would like to configure.

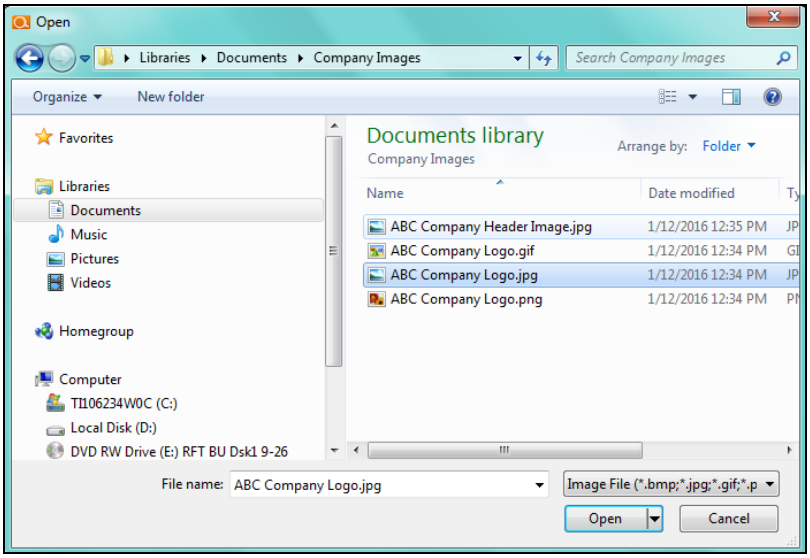
Set Reports Logo Preferences

To incorporate your company’s logos into the Reports generated by Network Detective, you must update the **My Logos Report Defaults** preferences to include your company’s logo files.

Adding the Cover Page Logo Image

Select the **My Logos** tab. To update the **Cover Page Logo image**, select the **Cover Logo Image Upload** button to upload an image that is 600 x 150.

The following window will be displayed to enable you to select the image file to be used for the **Cover Page Logo**.

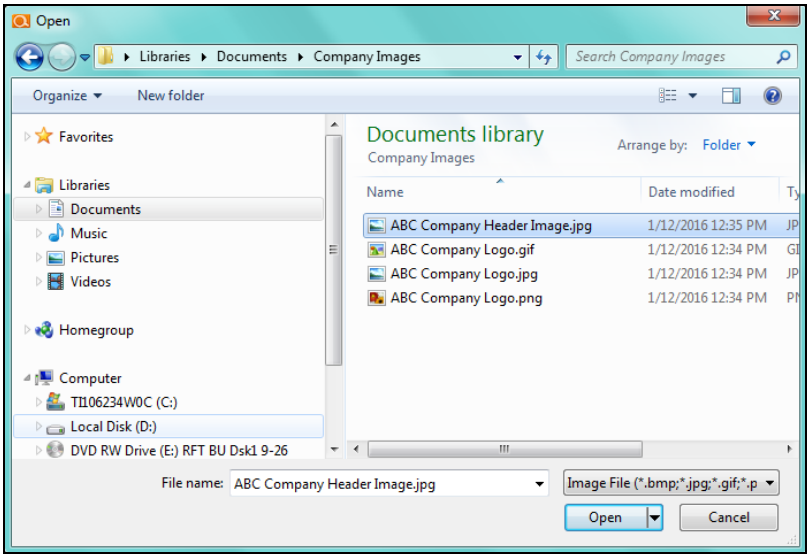


Select the image file to the used for the **Cover Logo Image** and select **Open** to complete the image upload process.

Adding the Header Logo Image

Select the **My Logos** tab. To update the **Header Logo image**, select the **Header Logo Image Upload** button to upload an image that is 300 x 75 or 600 x 150.

The following window will be displayed to enable you to select the image file to be used for the **Header Page Logo**.



Select the image file to the used for the **Header Logo Image** and select **Open** to complete the image upload process.

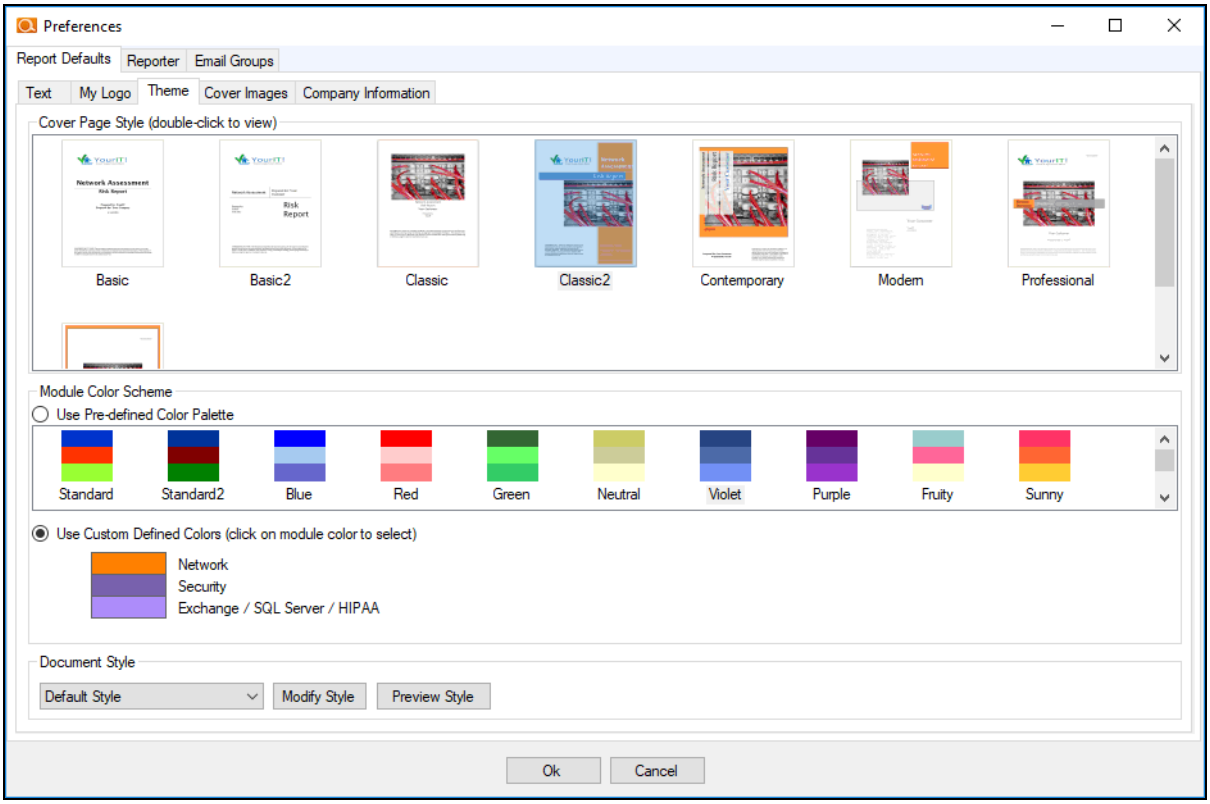
To save your **Cover Logo Image** and **Header Logo Image** settings, select the **Preferences Window Ok** button.

Set Reports Cover Page Styles and Themes Preferences

Each report generated follows a pre-built theme and is color-coded based on the specific Assessment Module the report is generated from after an assessment is performed (i.e. Network Assessment, Security Assessment, and/or Exchange/SQL Server/HIPAA).

Using this option, you can set the **Cover Page Style** for each assessment module's report documents and you can assign a report color palette to be used with each module during report generation.

To set the **Themes preferences**, select the **Themes** tab within the **Reports Defaults** window.



Setting the Reports Cover Page Style

Select the **Cover Page Style** from the available **Cover Page** document styles. If no other **Reports Defaults** preferences are to be set, then select the **Preferences Window Ok** button. Otherwise, continue setting a **Color Scheme** for one or more Modules as detailed below.

Setting the Module Color Scheme

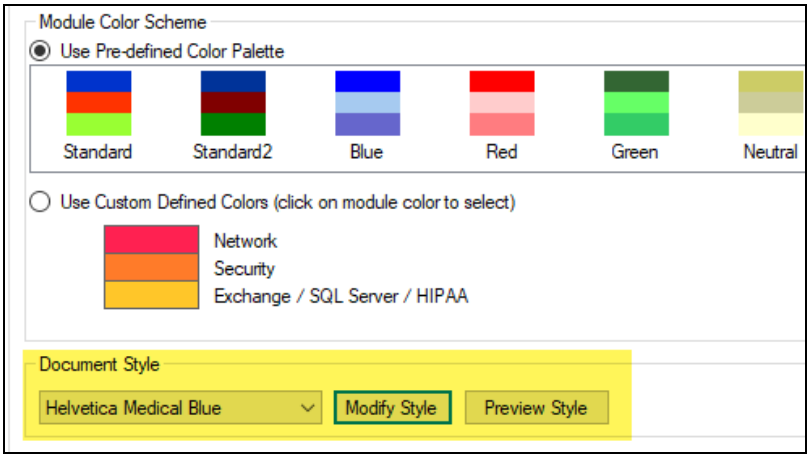
If you desire to assign a specific report color scheme to be used when a specific Network Detective Module generates reports documents, then use the **Module Color Scheme** option. This option enables you select from a pre-defined group of colors assigned to each module type in order to quickly assign a specific color scheme to each module (i.e. Network, Security, and/or Exchange, SQL Server, and HIPAA) for use during the report generation process.

To use the **Module Color Scheme** option, select a color palette from the Pre-defined Color Palettes.

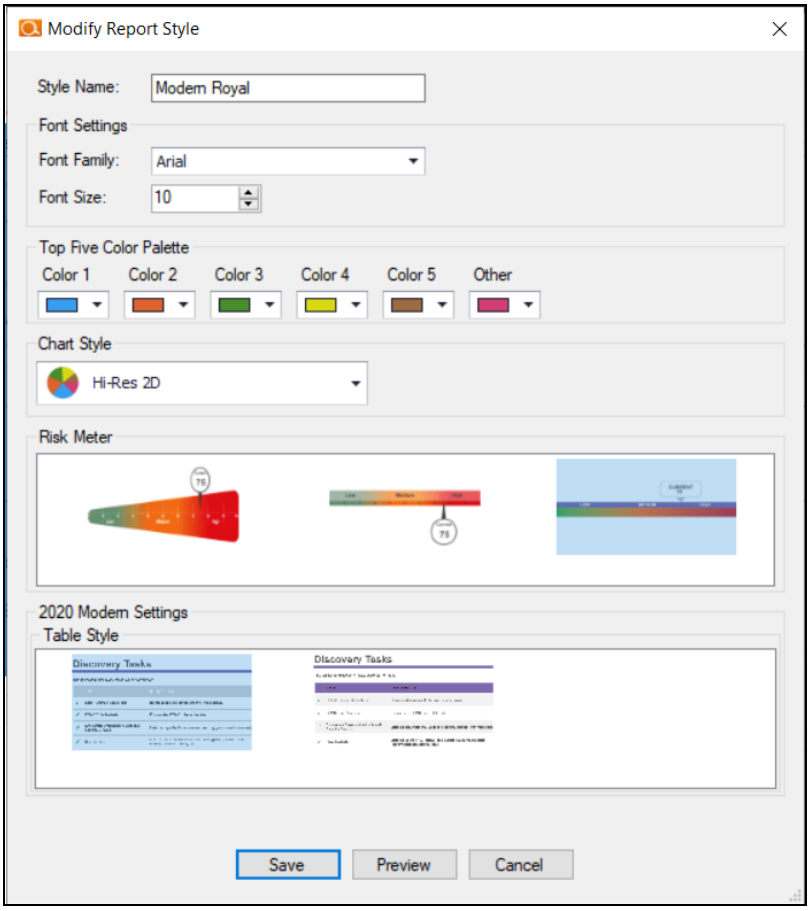
Keep in mind that each **Color Scheme** has bands of three colors that have been predefined. Each color scheme band is assigned to one or more modules as noted in the figure below.

Setting Document Style

Use the Document Style drop-down menu to change the fonts and font colors used in your reports.



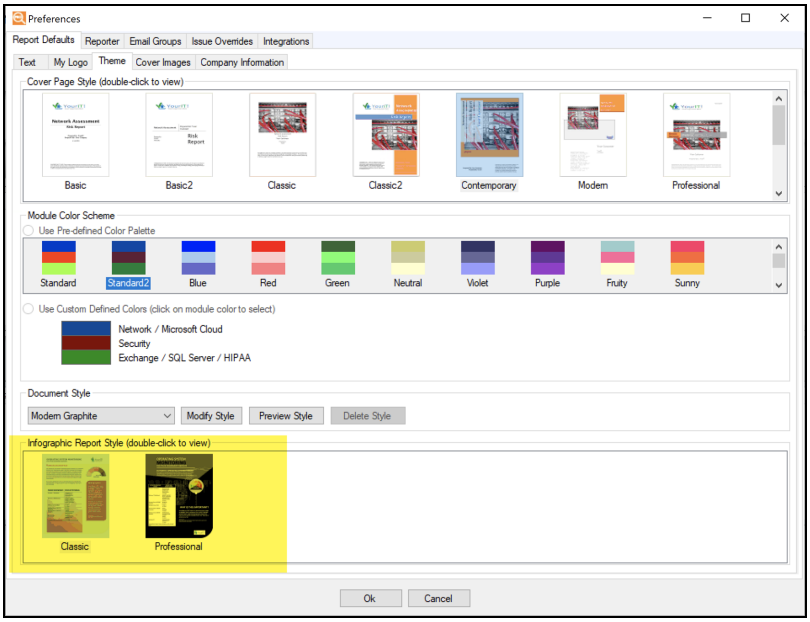
Click the **Modify Style** to make changes to the selected style.



You can then **Preview** and **Save** your changes.

Set Infographic Report Style

You can choose from two Infographic Report styles: **Classic** and **Professional**.



The infographic report style affects the following reports:

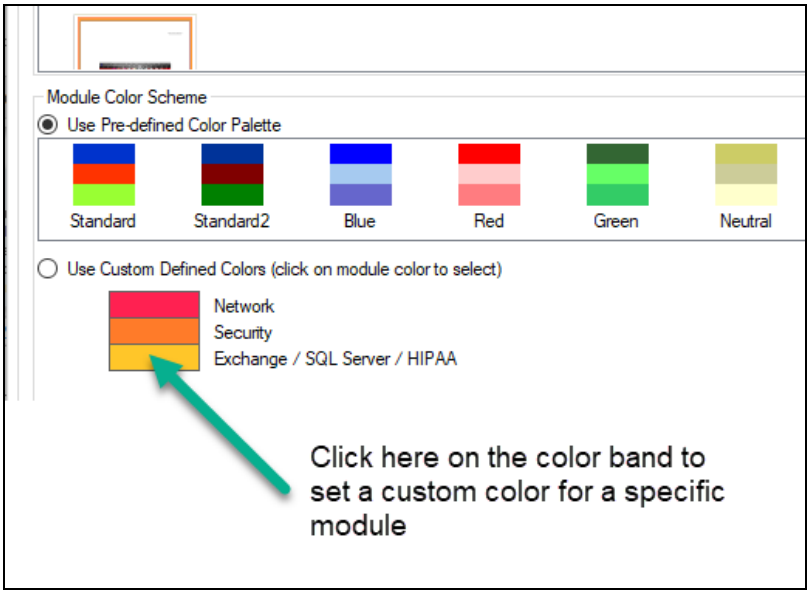
- Outdated Operating Systems Summary
- Outdated Malware Definitions Summary
- Password Policy Summary
- Data Breach Liability Summary
- Executive Summary
- Dark Web ID Summary

Assigning Custom Defined Color Schemes to Each Assessment Module

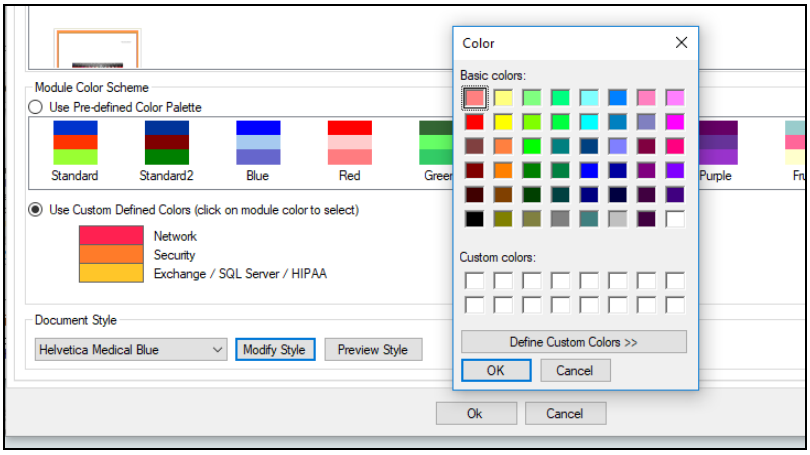
> **Note:** Currently, you cannot define custom color schemes for the "Modern" report styles.

To assign your own color schemes to each Assessment Module, select the **Use Custom Default Colors** option from within the **Themes** window and define your own Module color scheme.

Next, click on the Module color band as noted below, to view a color palette that is used to set the **Color Scheme** that is to be assigned to a specific Module.



Select the color that you want to assign to the Module from the choices presented in the **Color** palette window and then select the **Ok** button in the **Color** window to assign the color to the Module.

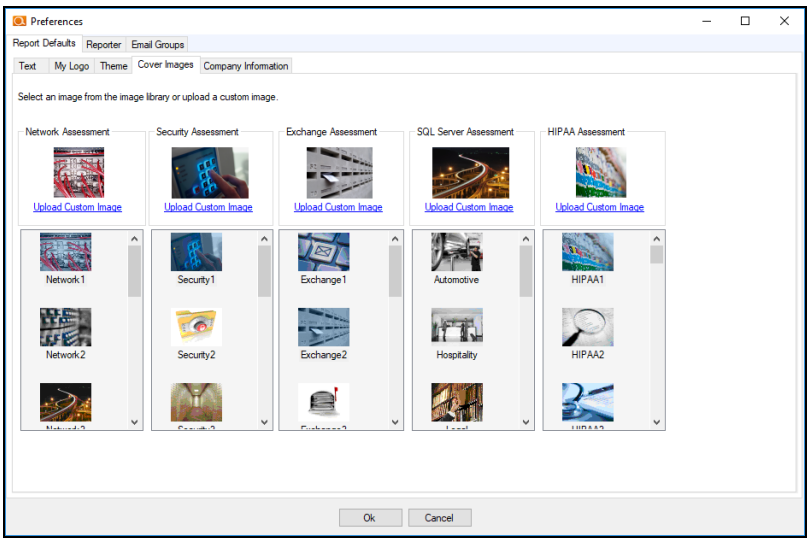


To save the color assignment for the Module's color band you selected, click on the **Preference Window Ok** button. Then set the colors for the other modules. To save your final Theme settings, select the **Preferences Window Ok** button.

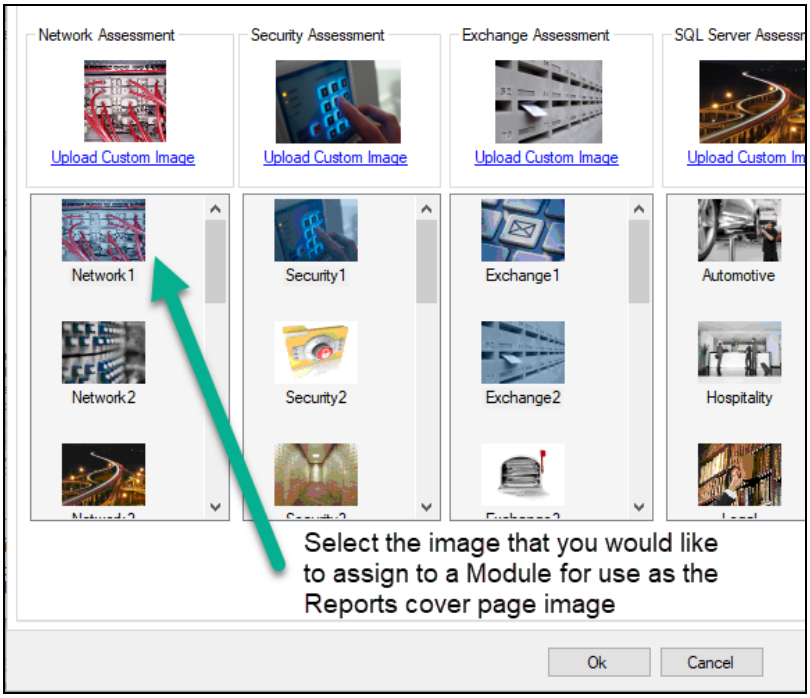
Set Reports Cover Images Preferences

For each Module, you can define the image that should be displayed within the **Reports Cover Page** when a report document is generated.

To assign an image to a specific Module's report cover page, select the **Reports Defaults** preferences and click on the **Cover Images** tab within the **Preferences Window** that is displayed.



Then, for each Module listed in the **Cover Images** page, select that image from the list box containing the available images, and select an image to be module that is referenced above the images list box.



After assigning the images to be used in the **Reports Cover Pages** for the reports output by each module, select the **Preferences Window Ok** button to save your image assignments.

After you have finished setting the **Reports Defaults** preferences, you can proceed to performing assessments and generating reports that will use your company's branding.

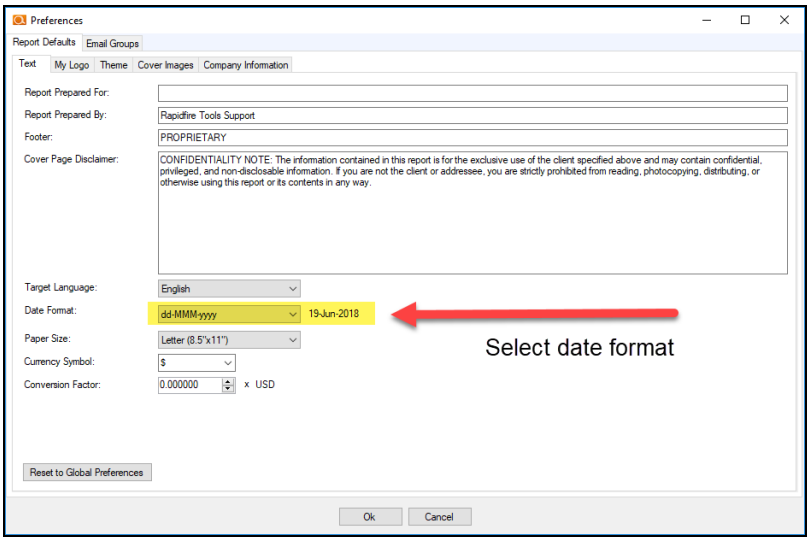
Note that the reports produced by Network Detective are delivered to you as Microsoft® Word and/or Excel documents so that you are able to add information to the report, or extract information to be included in your own documentation, sort and analyze, in Excel, etc.

Configure Report Date Format in Network Detective

You can configure the format for dates displayed in Network Detective Reports. For example, you can decide whether you want a *USA date* format or *international date* format. To configure dates that appear in reports:

1. First decide whether you want to change the report date format for ALL of your Sites - or just for specific Sites:
   A. If you want to change the date format for ALL of the reports you generate using Network Detective, click **Preferences** from the top menu.
   B. If you want to change the date format for reports you generate for a specific Site (or client), click the top selector icon  and then click **Report Preferences**.
2. Then, under **Report Defaults**, open the **Text** tab.
3. Select your preferred date format from the menu.

> **Note:** You can see a preview of how the date will appear next to the date format code.



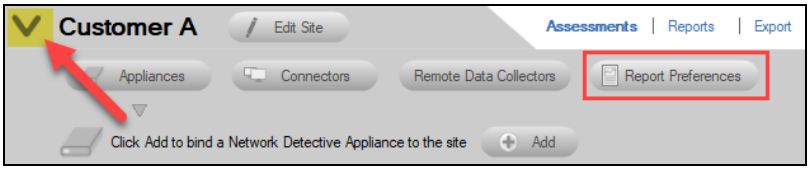
4. Click **Save**. Your newly generated reports will now have the specified date format.

Assigning the Global Reports Preferences to a Site

If you want to assign the Reports Preferences that you set globally for Network Detective to a particular site, follow these steps:

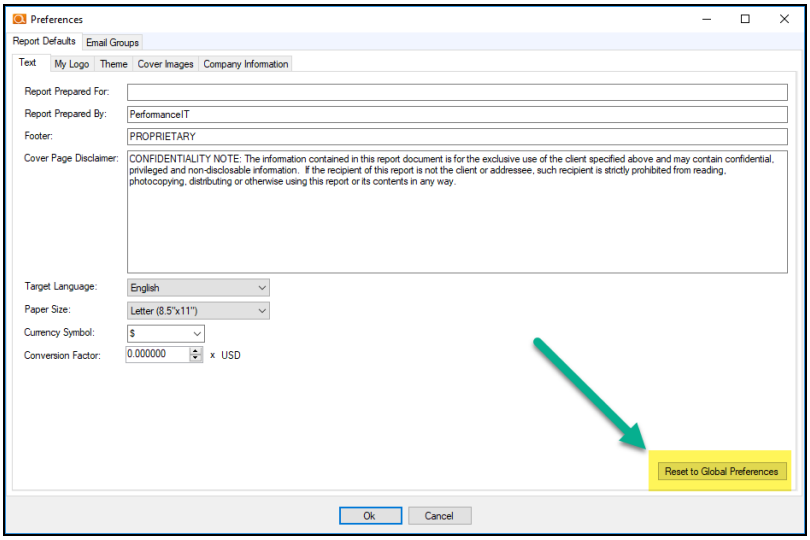
From the Site's Dashboard, select the selector control to the left of the Assessment's name to access the **Report Preferences** setup option.

The **Site's Preferences** will be displayed.



Next, select the **Report Preferences** button to enable you to access the **Site Level** branding standards for all reports generated for **Assessments** performed within a specific Network Detective **Site**. The **Site's Reports Preferences** window will be displayed.

Next, select the **Reset to Global Preferences** button.



Select the **OK** button to apply the **Global Reporting Preferences** to the **Site Level**.

Access Updated Report Styles

You can now select updated styles for your reports. These new designs give your reports a modern, info-graphic-like feel. Follow these steps to access these updates styles.

Make Changes at the Global or Site Level

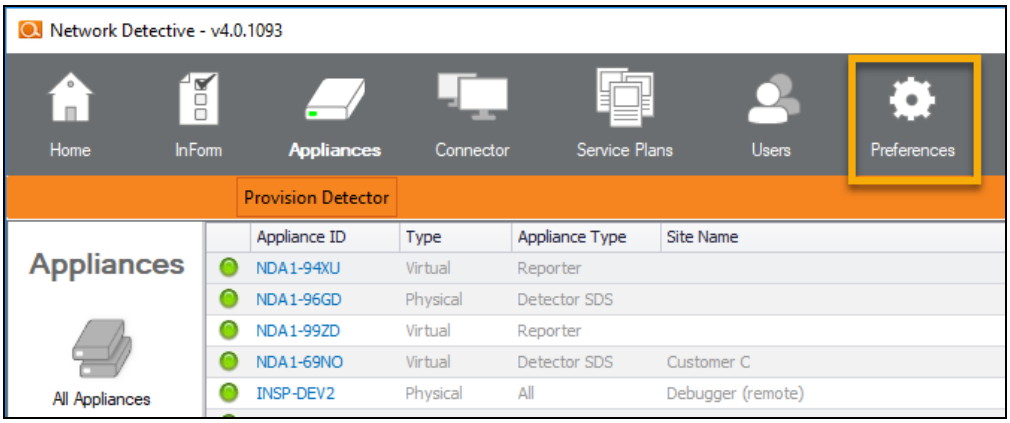
First, choose whether you want to change the report themes for all of your sites (global level) or for just individual sites (site level):

- "Update Report Styles at the Global Level" below
- "Update Report Styles at the Site Level" on the facing page

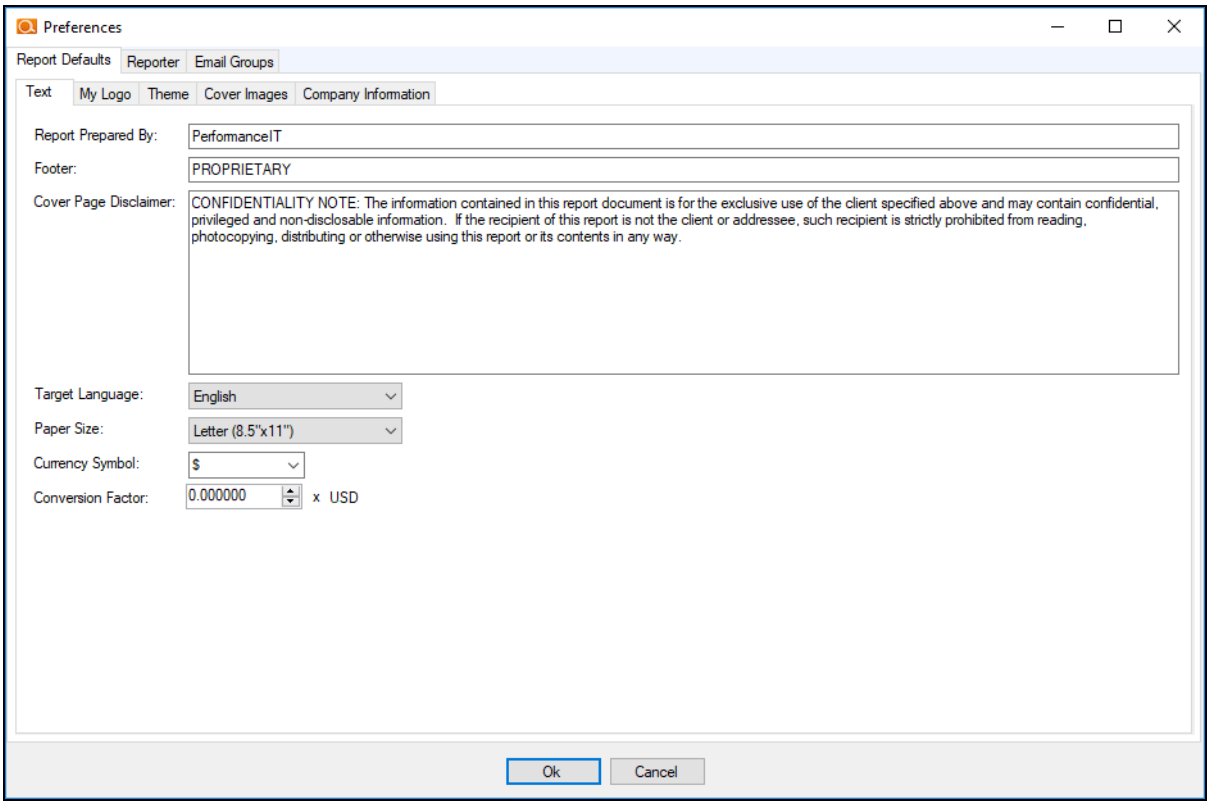
Update Report Styles at the Global Level

To change report styles for **all** of your Network Detective sites:

1. To change report styles for all of your sites, click on **Preferences** icon from the top menu.



2. The **Report Defaults** menu will appear.



3. Then continue to "Assign Updated Theme in Report Defaults" on the next page.

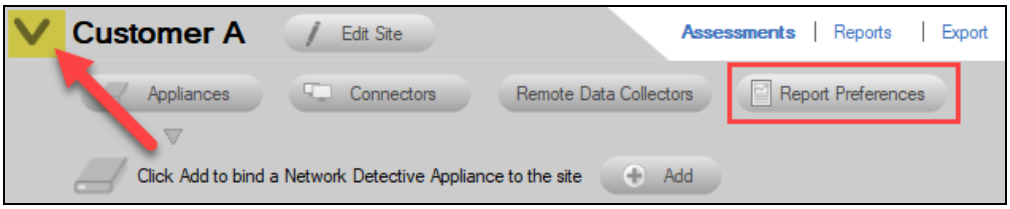
> **Note:** If you have set preferences at the site level, these will continue to override the global settings.

Update Report Styles at the Site Level

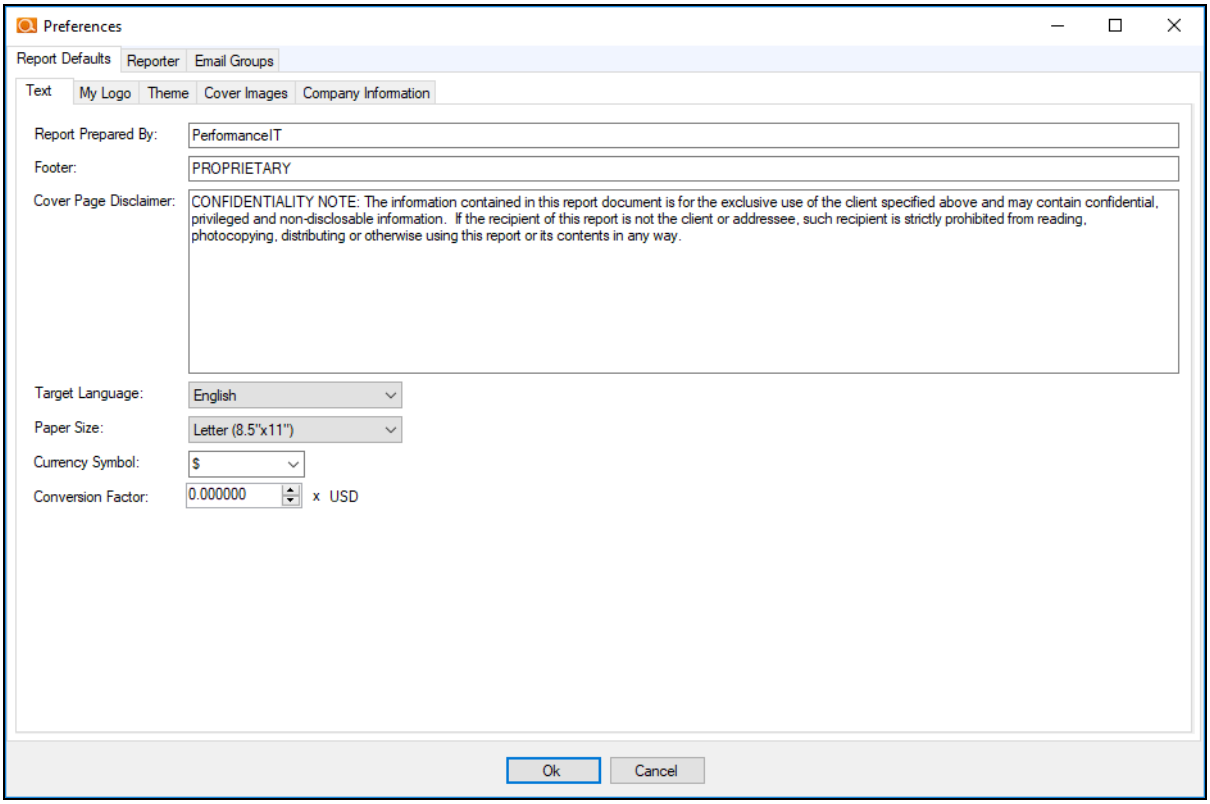
To change report styles for one or more individual Network Detective sites:

1. Open the site that you wish to modify.
2. Click on the chevron to the right of the site name to open the **Site Configuration Options**.

3. Click **Report Preferences**.



The **Report Defaults** menu will appear.

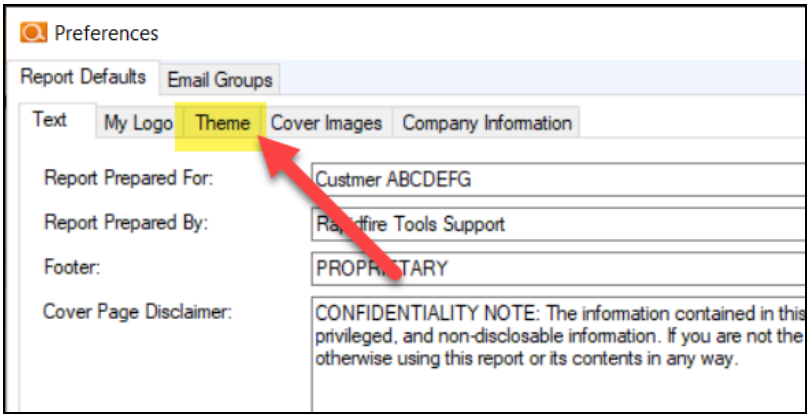


4. Then continue to "Assign Updated Theme in Report Defaults" below.

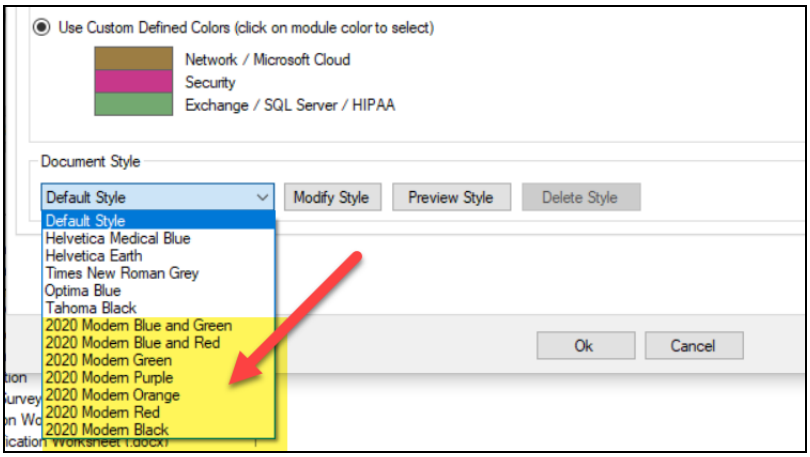
Assign Updated Theme in Report Defaults

Once you have opened the **Reports Defaults** menu from the global level or from a specific site:

1. Click the **Theme** tab.



2. Under **Document Style**, select one of the new **2020 Modern** styles.



3. You can also choose to modify or preview the style. See also "Setting Document Style" on page 23
4. When you are finished, click **OK** to save the changes. When you generate reports, they will now feature your selected **2020 Modern** document style.

> **Note:** Site level changes will only apply to reports for this specific site. If you made this change at the global level, this change will apply to all sites for which there are no site level report settings.

Performing a Network Assessment

To perform a Network Assessment, complete the four phases detailed in this guide.

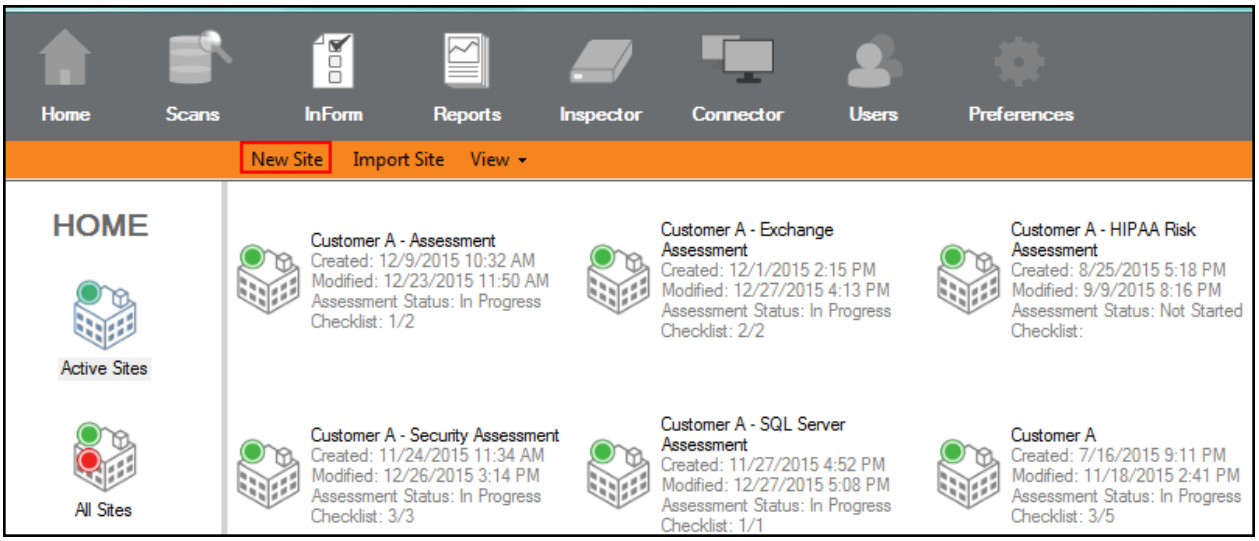
Phase 1 – Initial Network Assessment Project Setup

Creating a Site

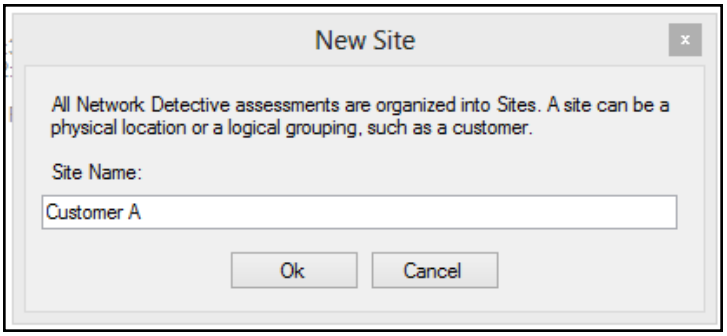
The first step in the assessment is creating a **"Site"**. All Network Detective assessment projects are organized into Sites. A **Site** can be a physical location or a logical grouping, such as a customer account name.

a. For a single location you will create one **Site**.

b. For organizations with multiple locations you must decide if you want one set of reports, or separate reports for each location.



Select **New Site**.



Enter the **Site Name**. For sites with multiple locations, enter a more detailed description.

Setting Report Branding for a Site

Reports produced by Network Detective can be “branded” with your company’s standards through the use of the **Reports Preference**s feature. Report Branding can be set at the **Global Level** (for all Sites), or at the **Site Level**. If you want to set the **Report Preferences** at the **Site Level**, please go to "Set Up Network Detective Reports" on page 16.

Adding a Connector to a Site

To add a Connector to a **Site**, please go to "Adding a Connector to a Site" on page 255.

> **Note:** Also see the Network Detective Remote Data Collector User Guide.

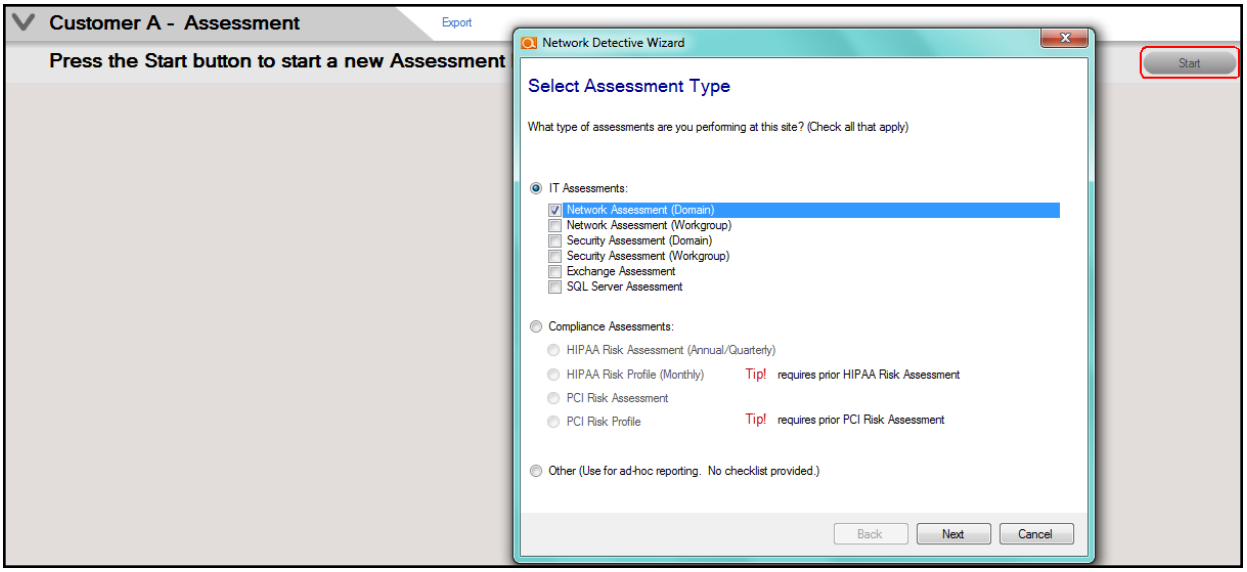
Adding an Inspector to a Site

To add an Inspector to a **Site**, please go to "Adding an Inspector to a Site" on page 257.

Phase 2 – Starting a Network Assessment Project

Starting a Network Assessment Project

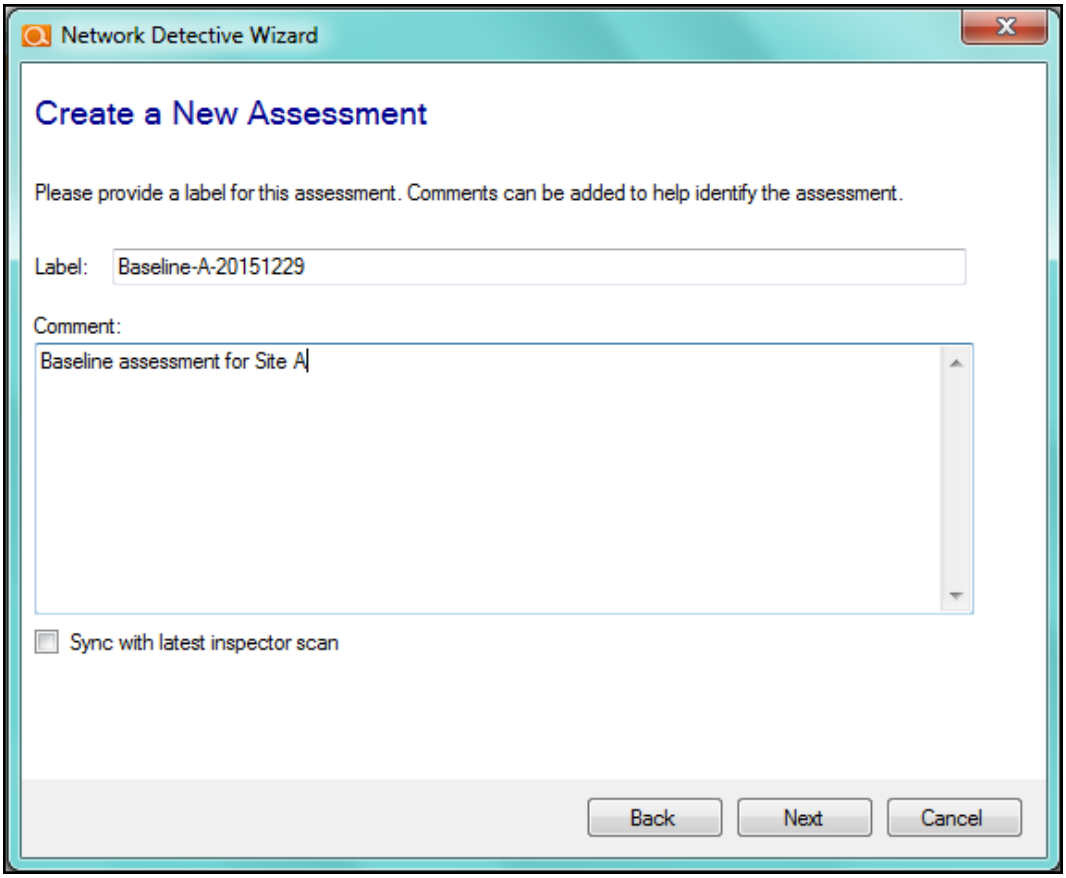
From the Site's Dashboard, click the "**Start**" button on the "Assessment" bar to start an **Assessment**.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more **Assessment Types**.

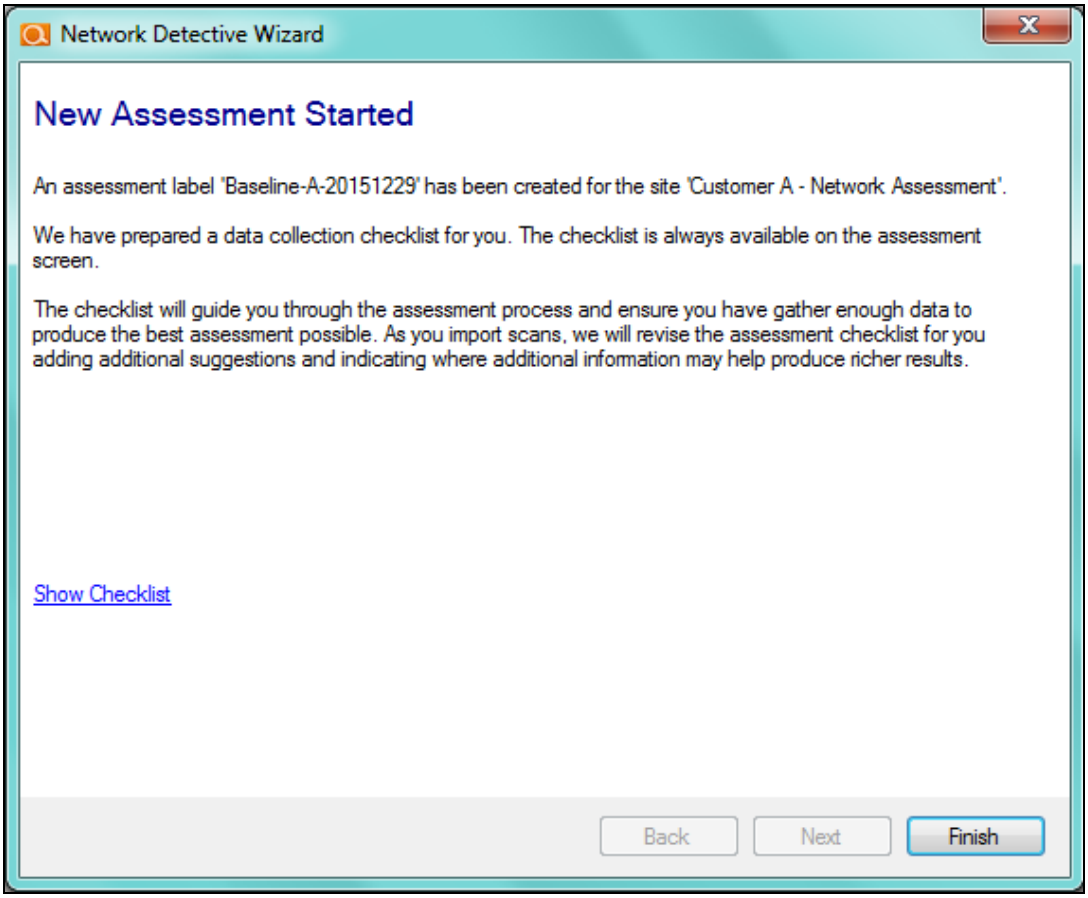
To create a **Network Assessment Project**, select the Network Assessment option and click on the **Next** button.



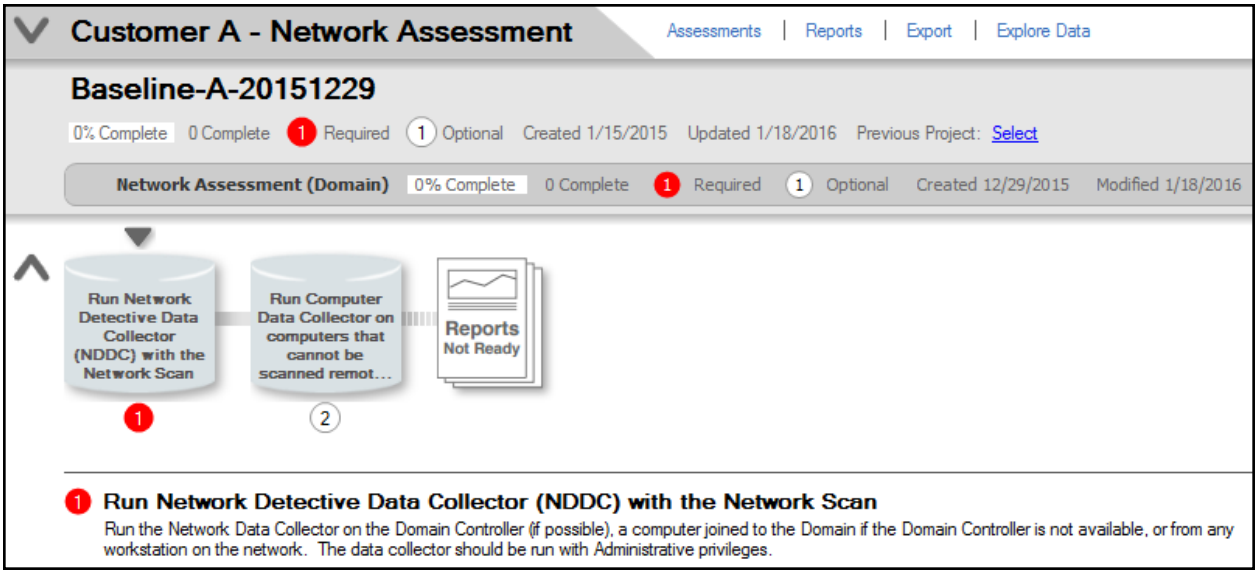
Enter a **Label** to identify the assessment project.

Enter a **Comment** to help further identify the assessment project.

Select the **Next** button to proceed to create/start the new assessment project.



The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment**.



Using the Checklist Feature for Assessment Process Guidance

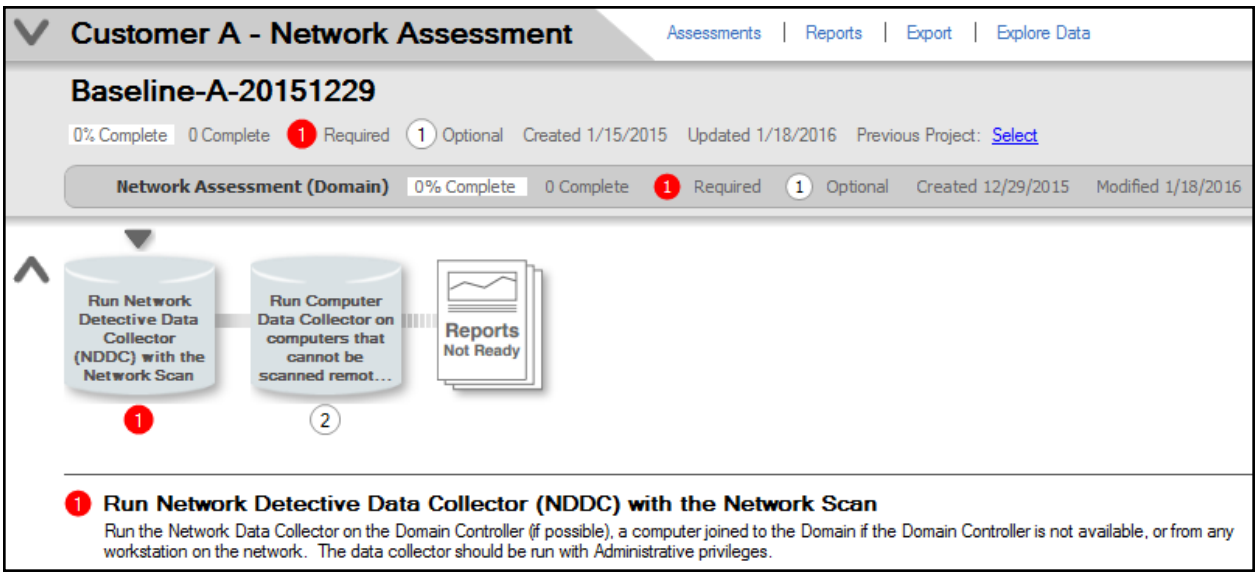
The **Checklist** will guide you through the assessment process and ensure you have gathered enough data to produce the best assessment possible. As you import scans, complete surveys, and fill out worksheets, the **Checklist** will automatically be revised adding additional suggestions and indicating where additional information may help produce richer results.

The assessment's **Checklist** is always available on the **Assessment Window**.

The **Checklist** is a helpful outline of the information you will need to collect to complete the **Assessment**.

> **Note:** The specific items represented in the Checklist will differ depending on the assessment module you are using.

The **Checklist** is continuously updated to reflect completed items and changes to your **Assessment**. By using the **Checklist**, you can make sure that your tasks are complete, on schedule, and that all relevant data you collect is integrated into your reports.



The **Checklist** will be updated continuously as you complete your **Assessment**.

Required items must be completed in order to complete the **Assessment** and generate reports.

> **Note:** Note that Reports will not be available until required data has been added to the Assessment.

As you work through the assessment, the **Checklist** will be updated to reflect completed **Checklist** items.

As you complete **Checklist** items, the completed Items will be represented with the checkmark symbol √ to reflect your progress.

Throughout the assessment process, the **Checklist** will update the list of **Open Items** and **Completed Items** to present to you a list of assessment actions that have been completed and a list of outstanding actions.

Required actions will be referenced throughout the **Checklist** and noted with a **red circle** ●.

This **Checklist** will have new **Open Items** (i.e. assessment tasks) added to the **Checklist** based on the phase and/or steps that have been performed by the user within the specific assessment process.

These **Checklist** items created and updated within the **Checklist** are related to the performance and importing of scans, the answering of surveys, or the completion of worksheets that are dynamically added to the **Checklist** throughout the assessment process.

Planning the On-site Data Collection

There are various ways to collect data for a **Network Assessment**. These methods can vary based on time, cost, client expectation, level of detail needed to identify remediation needs, etc.

Initial Assessment

Types of collections:

Network Assessment

- Quick Assessment
  - Network Scan + Computer Scans on 1-3 computers
- Full Assessment
  - Network Scan + Computer Scans on all computers

Scans Performed During the Network Assessment Process

The Initial Data Collection phase of the **Network Assessment** consists of the following required and optional scans:

- **Network Scan** Using the **Network Assessment Data Collector**
- **Scans on Local Computers** using the **Push Deploy Tool**
- **Local Computer Scans** using the **Computer Data Collector** for unreachable computers

The **Network Assessment Data Collector** scans make 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

See also: "Pre-Scan Network Configuration Checklist" on page 249.

Optional Local Scanning of Unreachable Computers and the Optional Internal Network Vulnerability Scan

Throughout the assessment process, “**Optional**” scans may need to be undertaken based on the availability of servers and workstations during automated and network scans, based on a need to sample scan machines outside of the network that you are

assessing, or based on the need to more thoroughly scan for internal network vulnerabilities.

These scans would include:

Optional Scan Type	Description
Run Computer Data Collector scan on the Computers that were unreachable *Refer to "Task 3: Run the Computer Data Collector to Perform Local Scans on the Computers that were Unreachable during Push Deploy Tool Scanning (OPTIONAL)" on page 75*	Run the "Local" Scan on any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible). Run the Local Scan directly on the computer itself.
Internal Vulnerability Scan (requires Inspector) *(Refer to the Inspector User Guide for instructions on how to run this scan)*	An Inspector initiated scan that checks for Open Ports and Protocol Vulnerabilities that could be exploited ONCE a hacker is in your network – or by employees. Essentially "INSIDE attacking INSIDE". This scan complements the external vulnerability scan performed with the Security, HIPAA, and PCI modules, which finds weaknesses at the network "edge" that could be exploited by external sources.

Phase 3 – Performing the Assessment and Data Collection

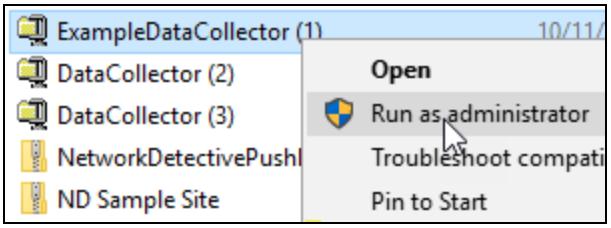
To perform the Assessment and the associated Data Collections, the following tasks must be performed:

- "Task 1: Initiate the Network Scan Using the Network Detective Data Collector and Import Scan Results" below
- "Task 2: Use the Push Deploy Tool to Collect Remaining Data and Import Scan Results" on page 64
- "Task 3: Run the Computer Data Collector to Perform Local Scans on the Computers that were Unreachable during Push Deploy Tool Scanning (OPTIONAL)" on page 75
- "Task 4: Document Exceptions that Mitigate Identified Risks and Improve Risk Scoring" on page 82

Task 1: Initiate the Network Scan Using the Network Detective Data Collector and Import Scan Results

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

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



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

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

Configure the network scan using the wizard.

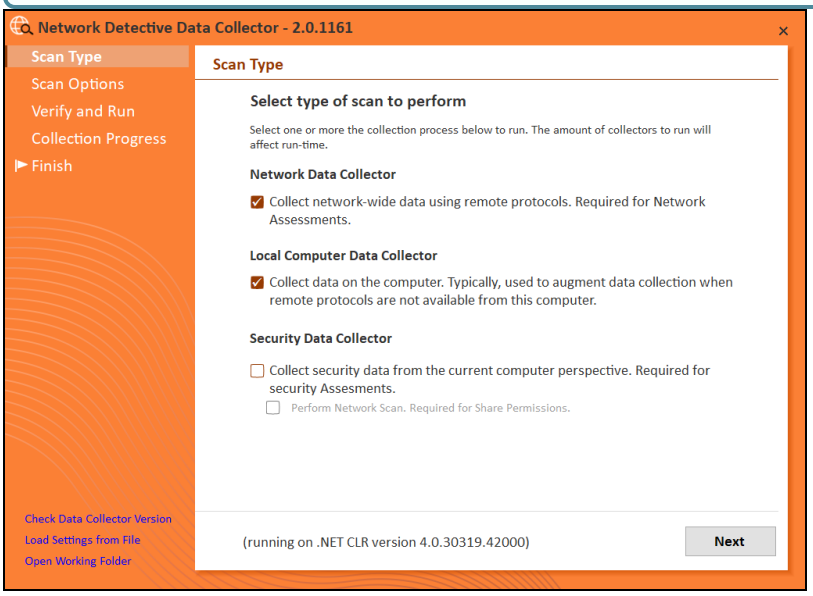
- Look here if you are "Scanning an Active Directory Domain-based Network" below
- Look here if you are "Scanning a Workgroup Network" on page 53

Scanning an Active Directory Domain-based Network

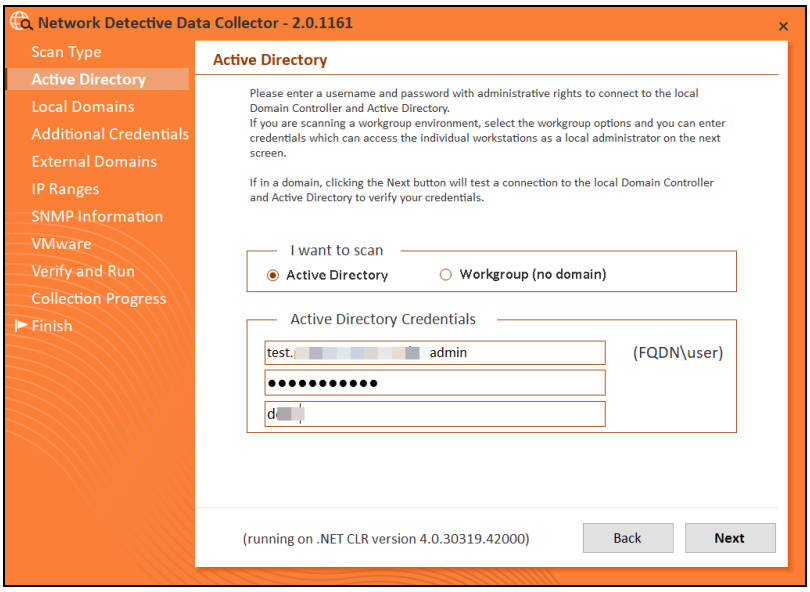
Once you run the Data Collector, the Scan Type screen will appear.

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

> **Note:** You can optionally choose to run the **Local Computer Data Collector**, too, to collect data from the local machine that you are using to run the network scan.



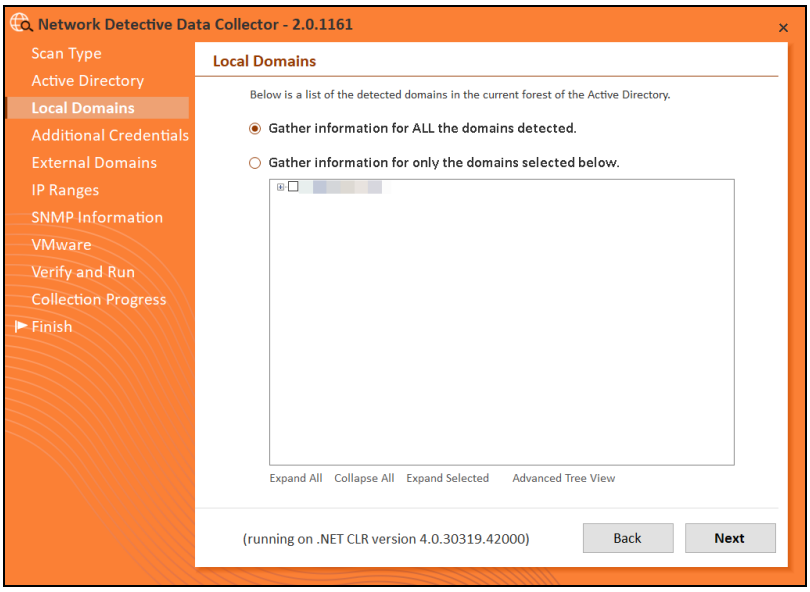
2. The **Active Directory** window will appear. Select the type of network you are scanning: *Active Directory domain*.



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

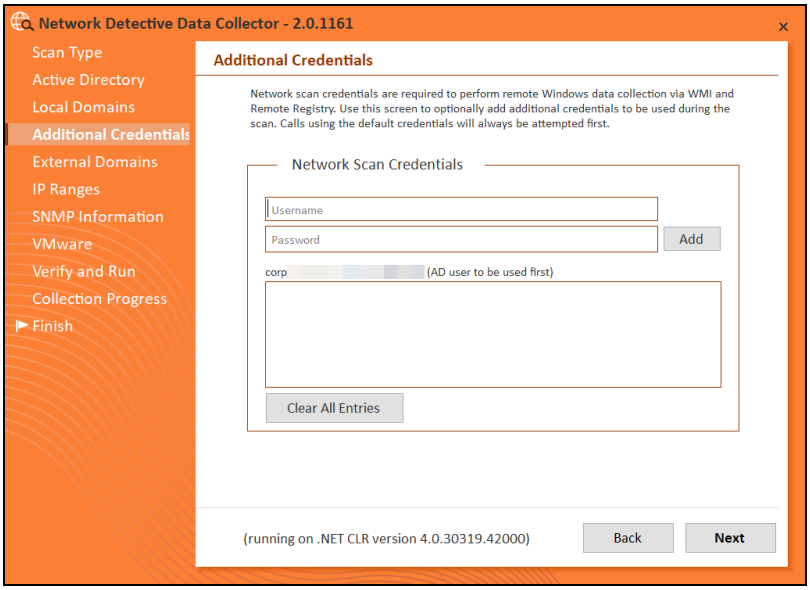
   Note: For example: **corp.yourprospect.com\username.**

4. Enter the name or IP address of the domain controller.
5. Click **Next** to test a connection to the local Domain Controller and Active Directory to verify your credentials.
6. 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**.

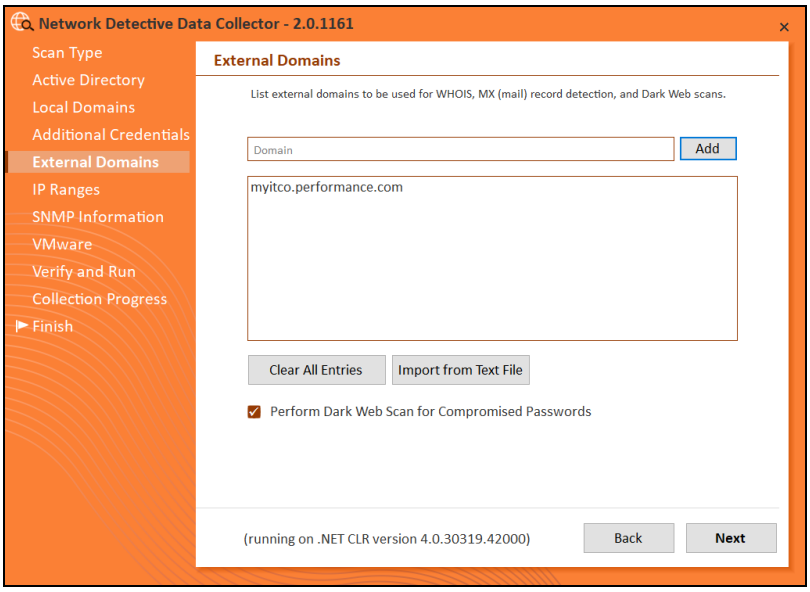


Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

7. 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**.

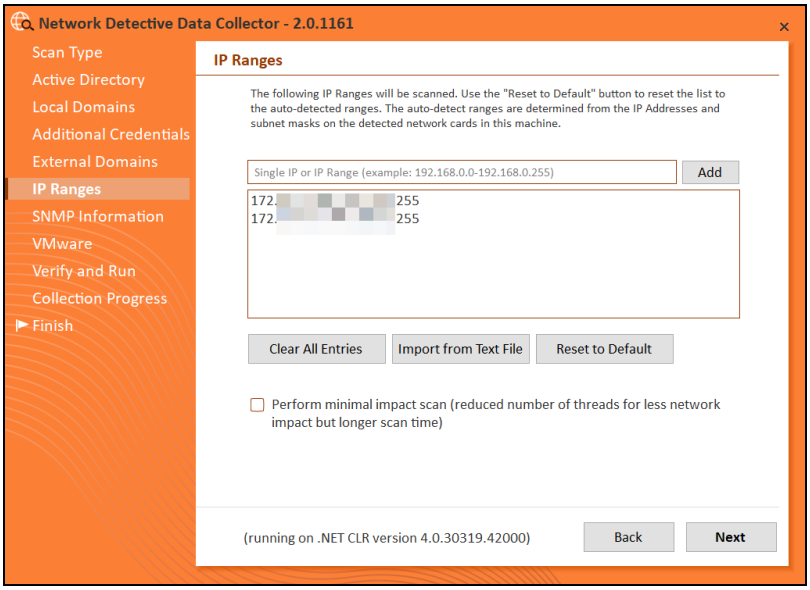


8. The **External Domains** screen will appear. Enter the name(s) of the organization's **External Domains**. Click **Next**.



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

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

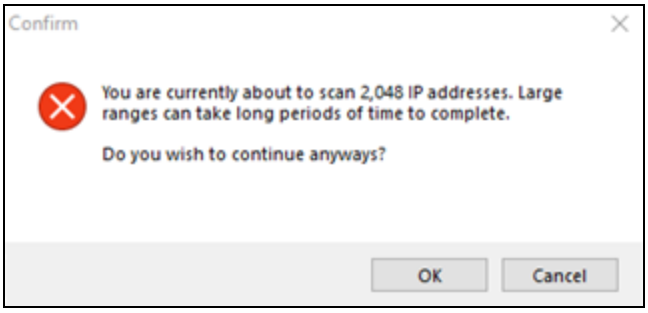


From this screen you can also:

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

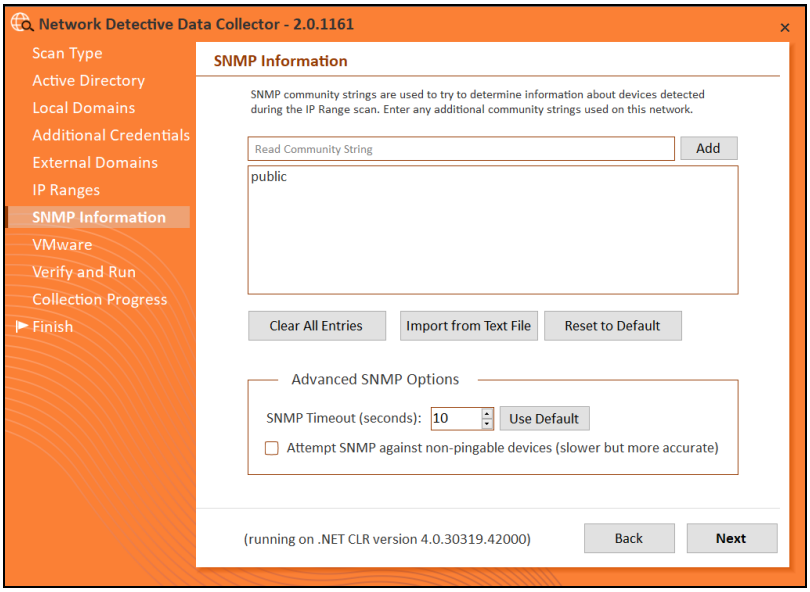
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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

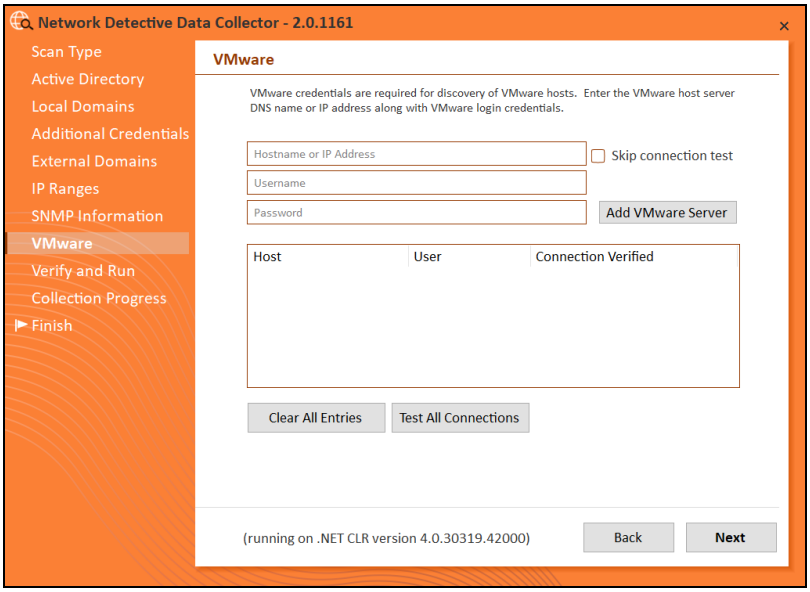


Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

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



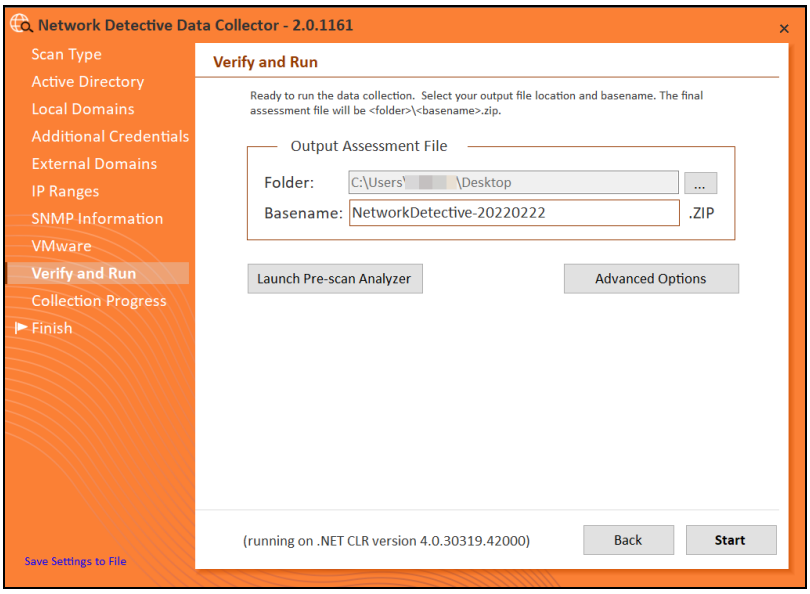
11. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next**.



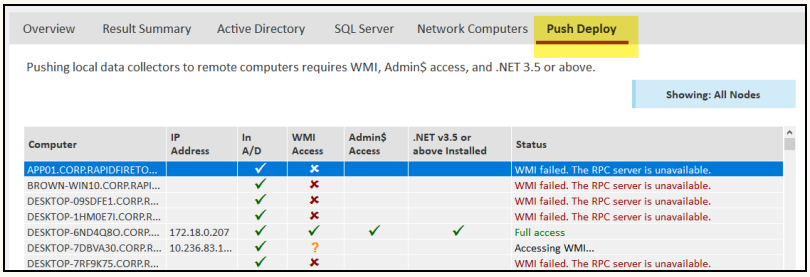
12. The **Verify and Run** window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan's **Output Assessment File Folder** location and **Basename** for the scan data.

> **Tip:** If you are using a USB flash drive, select a folder on that drive.

The file will be output as a **.PCI** file.

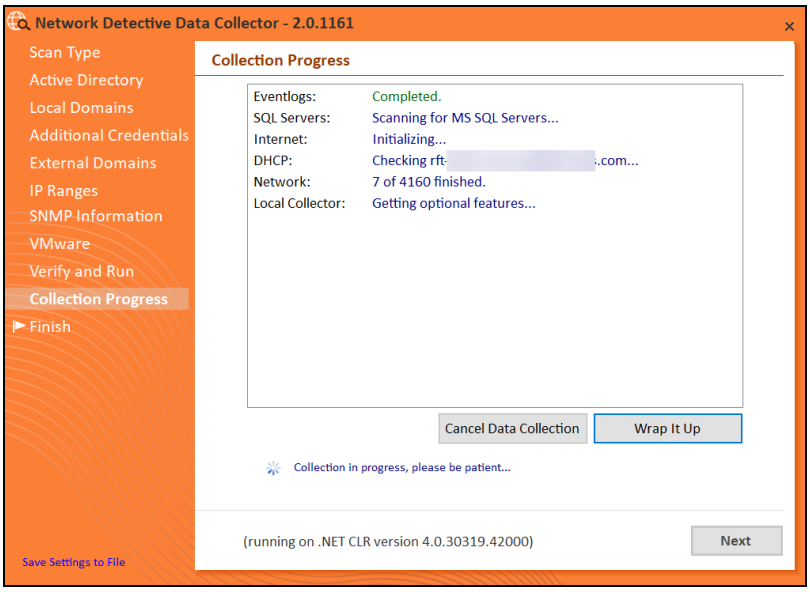


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which devices are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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



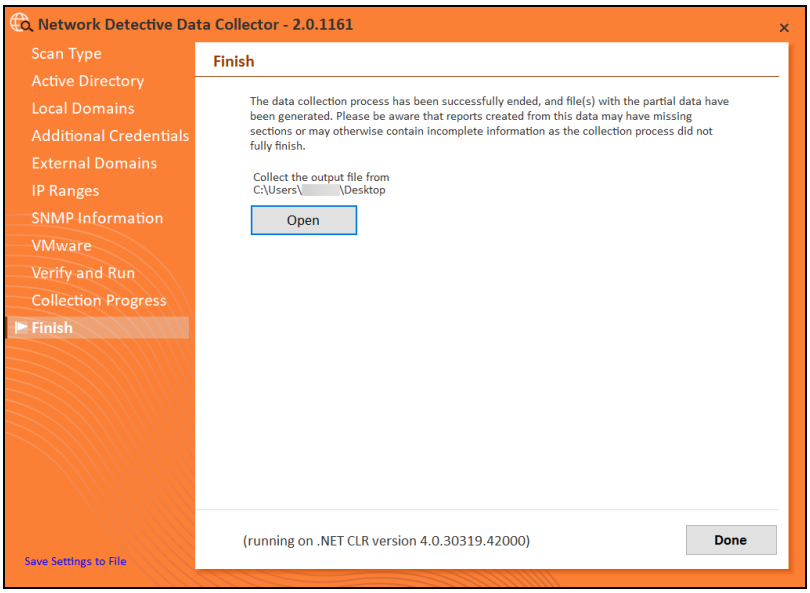
Enter any **Comments** and then click **Start**.

13. The **Collection Progress** window will appear. The **Network Scan's** status is detailed in the **Collection Progress** window. The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.



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

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

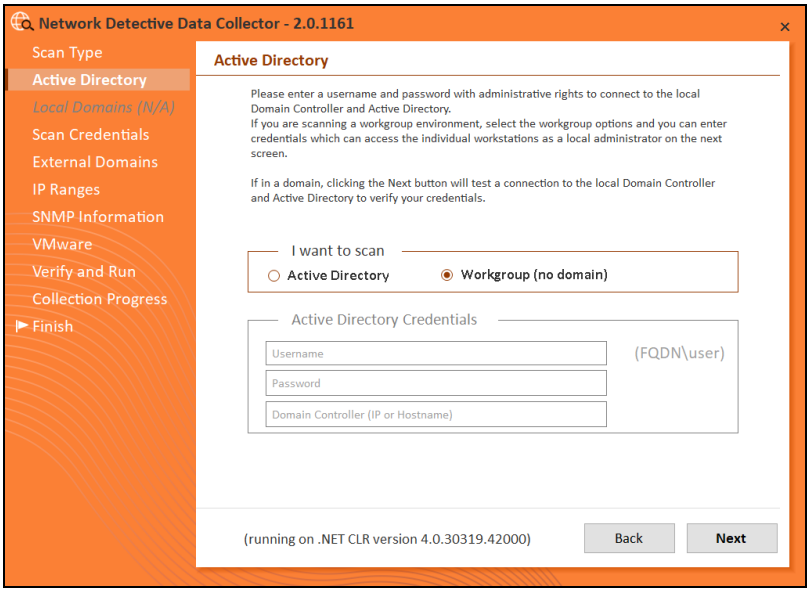


Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

Scanning a Workgroup Network

Once you run the Data Collector, the Scan Type screen will appear.

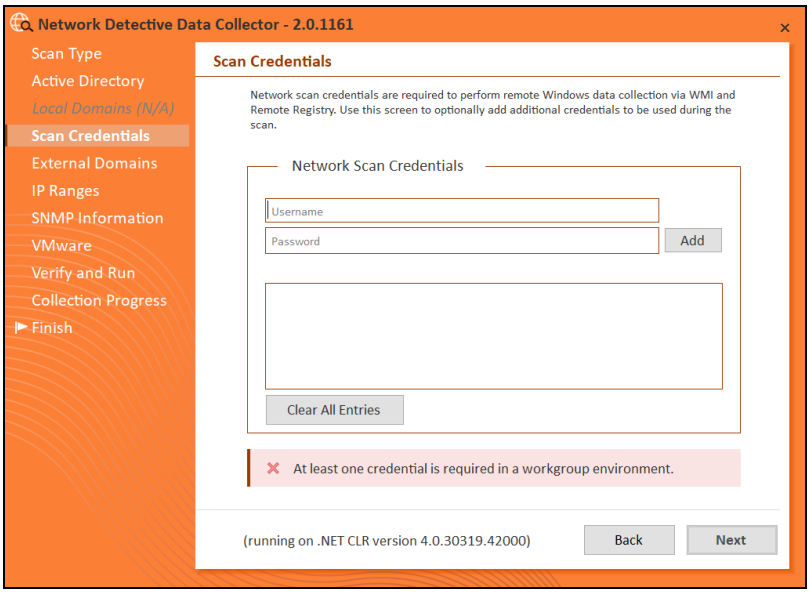
1. The **Active Directory** window will appear. Select the type of network you are scanning: *Workgroup*).



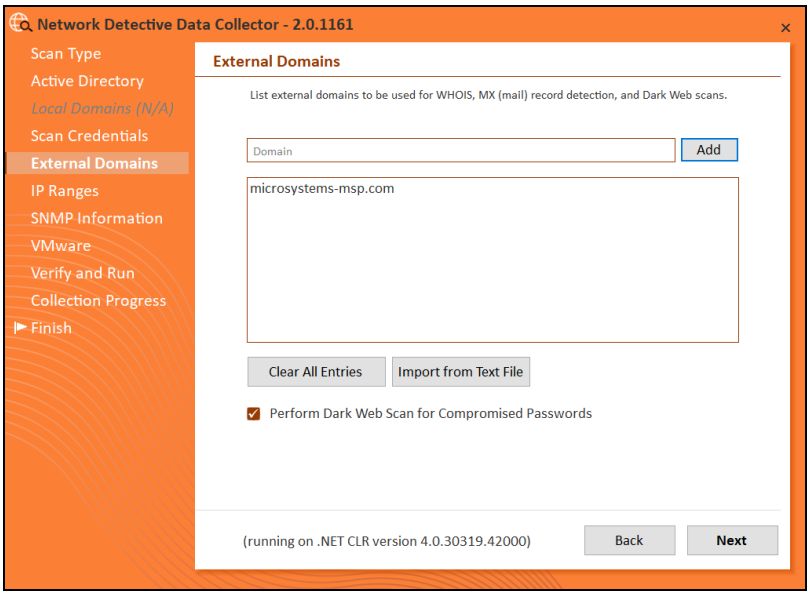
2. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator.

   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.

   Then click **Next**.

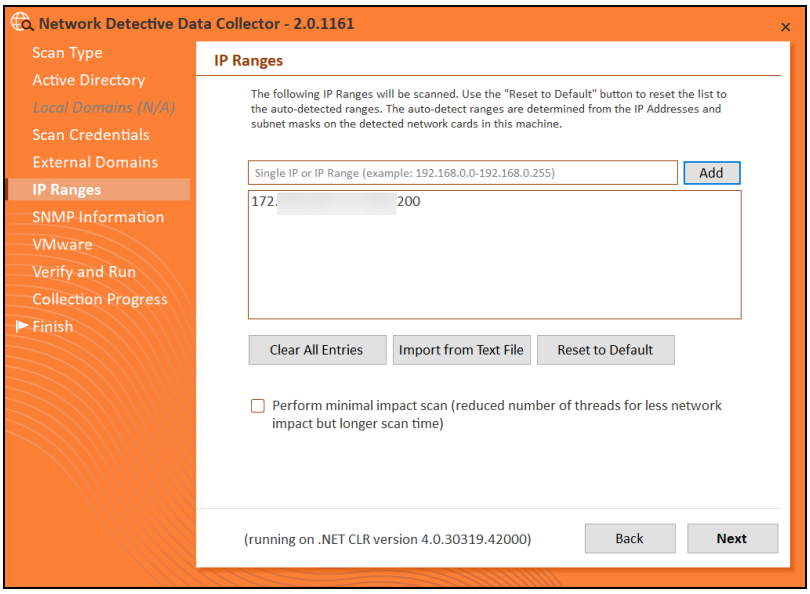


3. The **External Domains** screen will appear. Enter the name(s) of the organization's **External Domains**. Click **Next**.



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

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

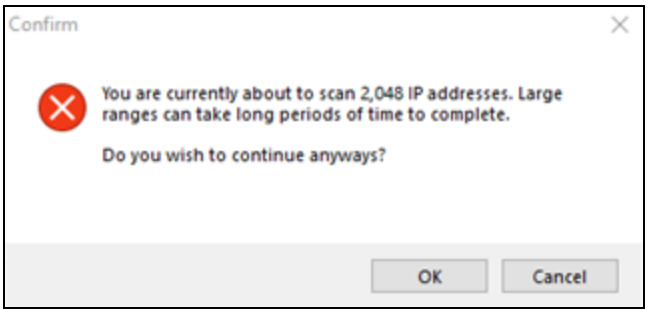


From this screen you can also:

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

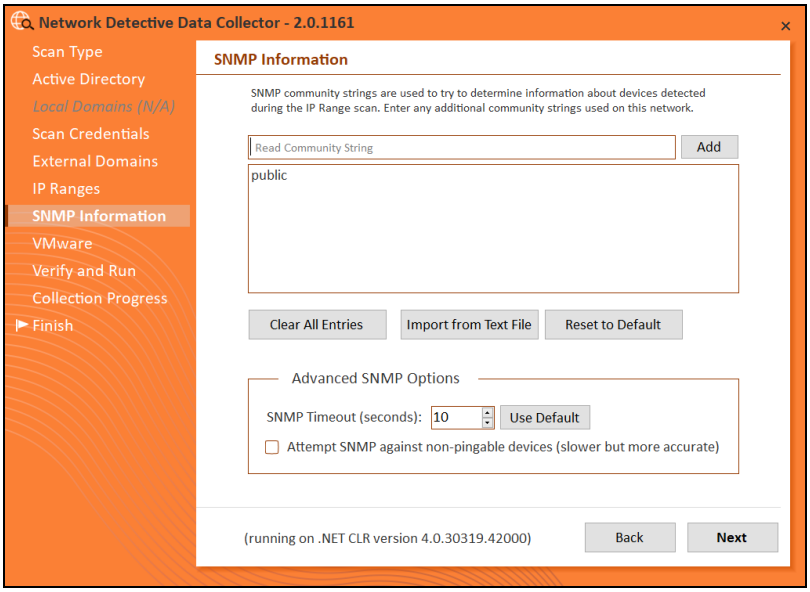
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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



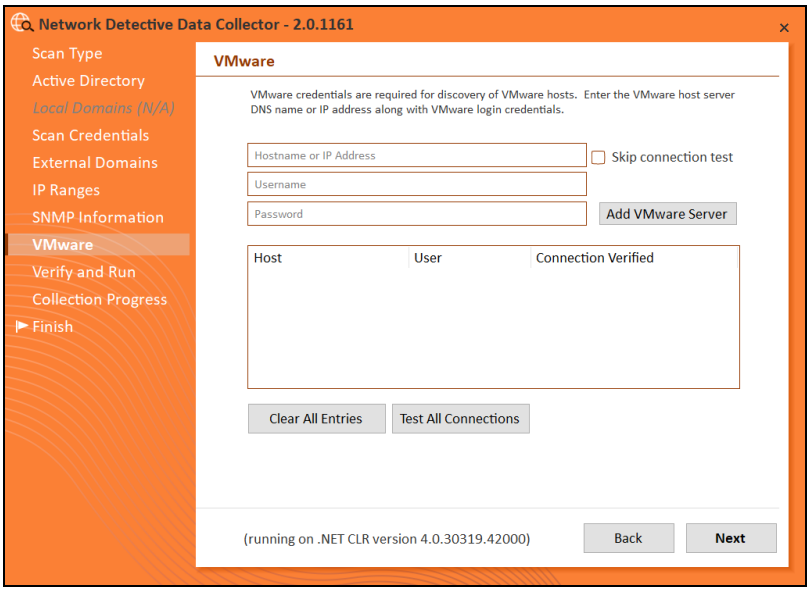
Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

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

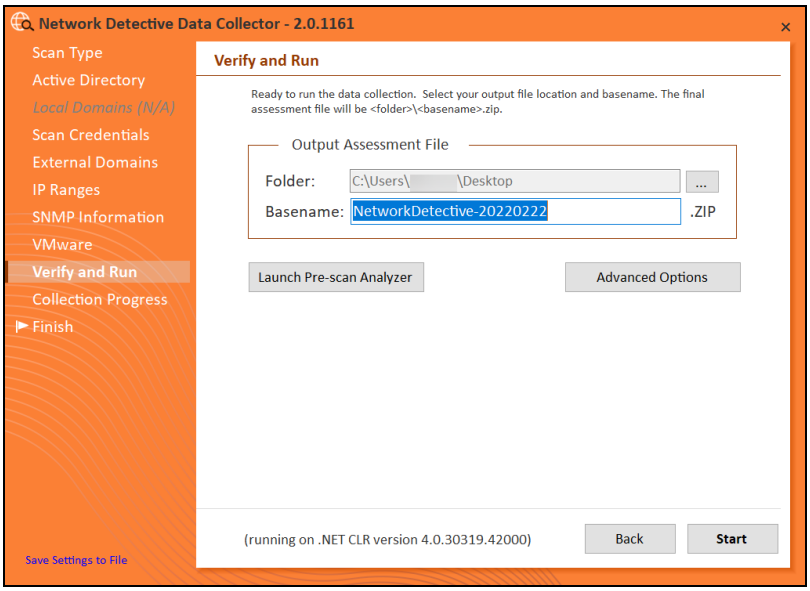


Important: As of 9/28/2018, the Microsoft Base Security Analyzer (MBSA) has been removed from the Data Collector. MBSA is in the process of being deprecated by Microsoft. Microsoft no longer supports MBSA in newer versions of Windows (i.e. v10 and Windows Server 2016). MSBA is only useful for earlier 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.

6. 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**.

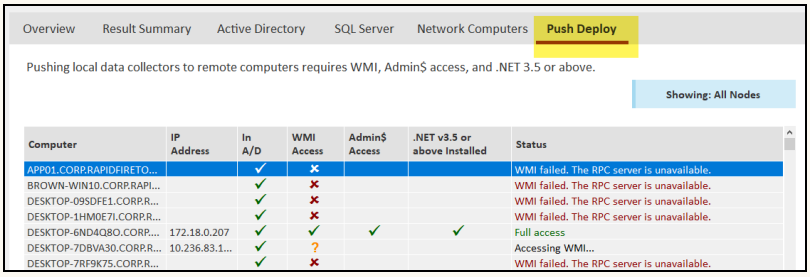


7. The Verify and Run window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan's **Output Assessment File Folder** location and **Basename** for the scan data. The file will be output as a **.PCI** file.



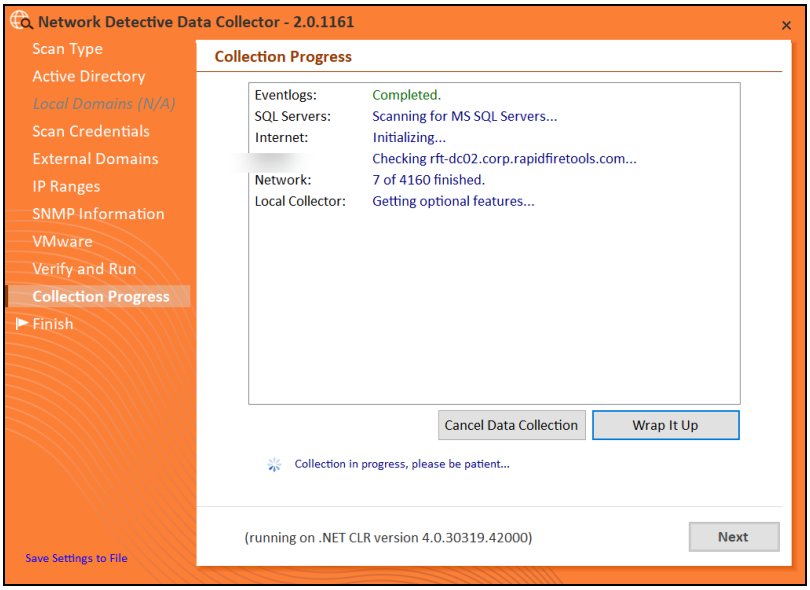
Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which devices are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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

scan.



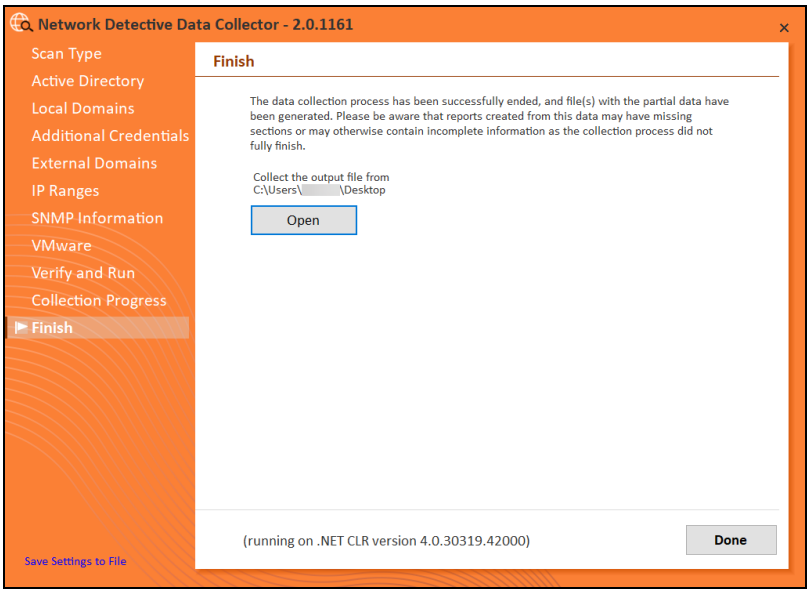
Enter any **Comments** and then click **Start**.

8. The **Collection Progress** window will appear. The **Network Scan's** status is detailed in the **Collection Progress** window. The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.



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

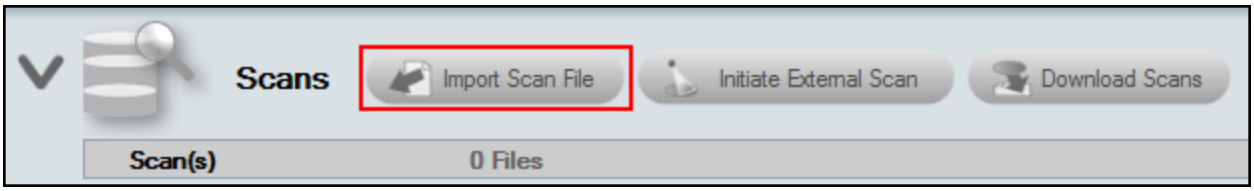
Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.



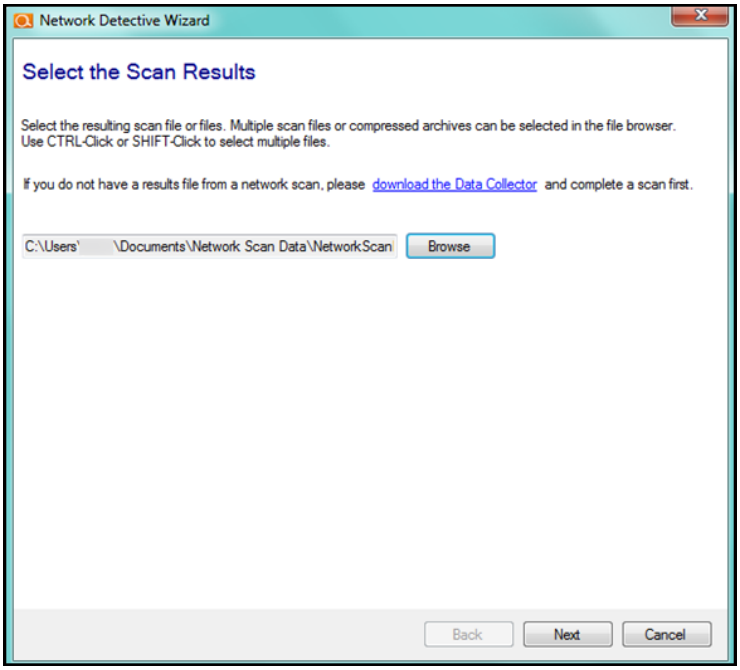
Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

Importing the Network Assessment Network Scan Data in the Assessment

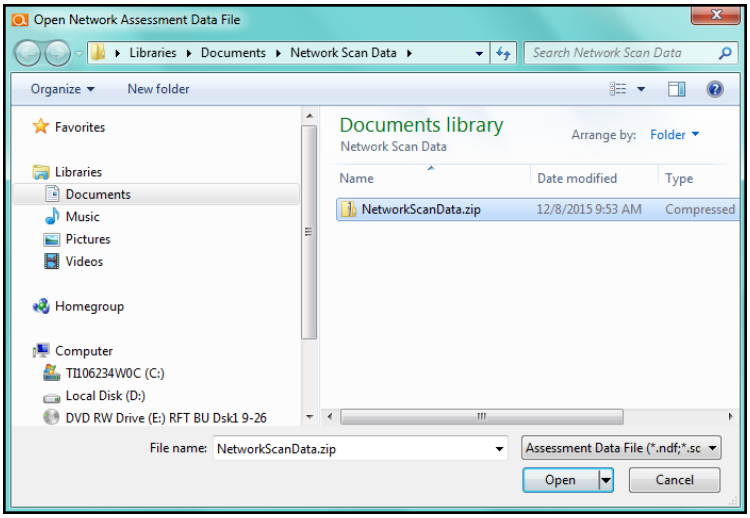
The final step in this process is to import the data collected during the **Network Assessment Network Scan** into the **Active** Network assessment. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:



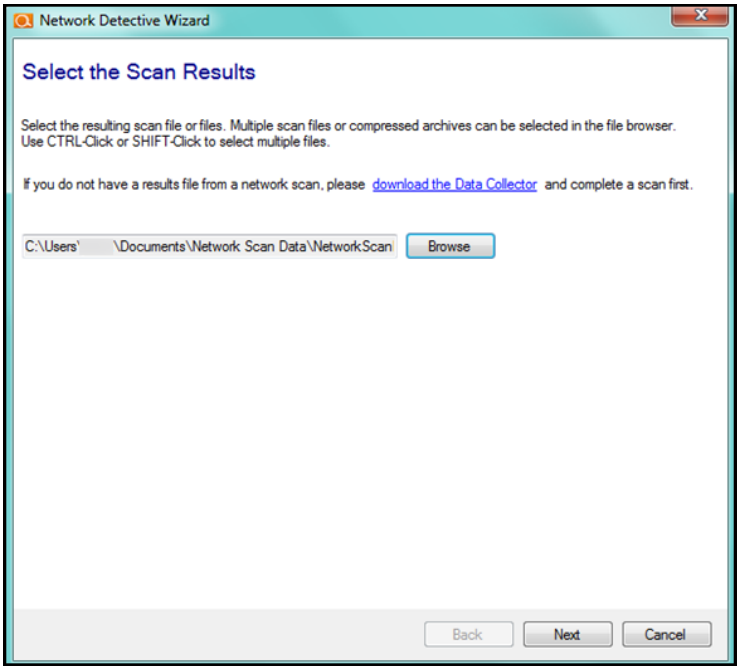
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP file produced by the **Network Assessment Data Collector Network Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Network Scan** data file.

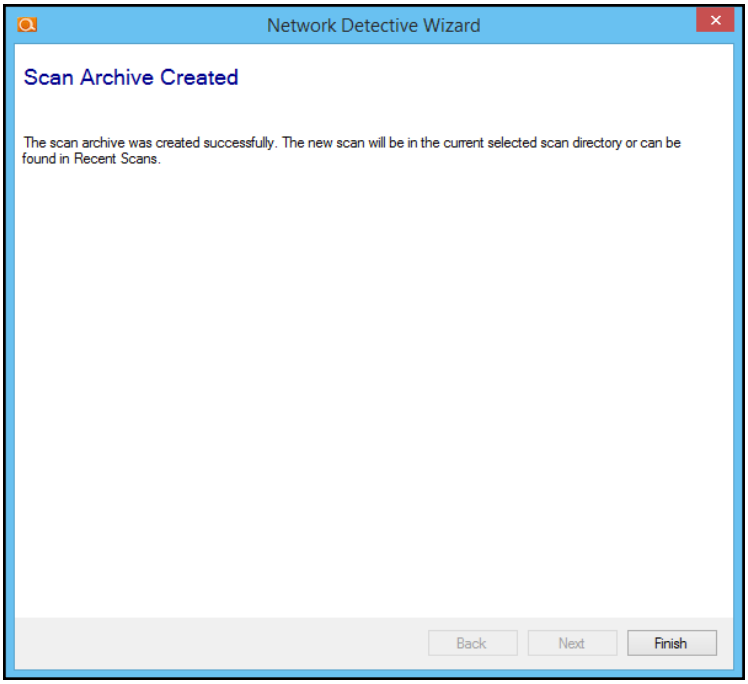


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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

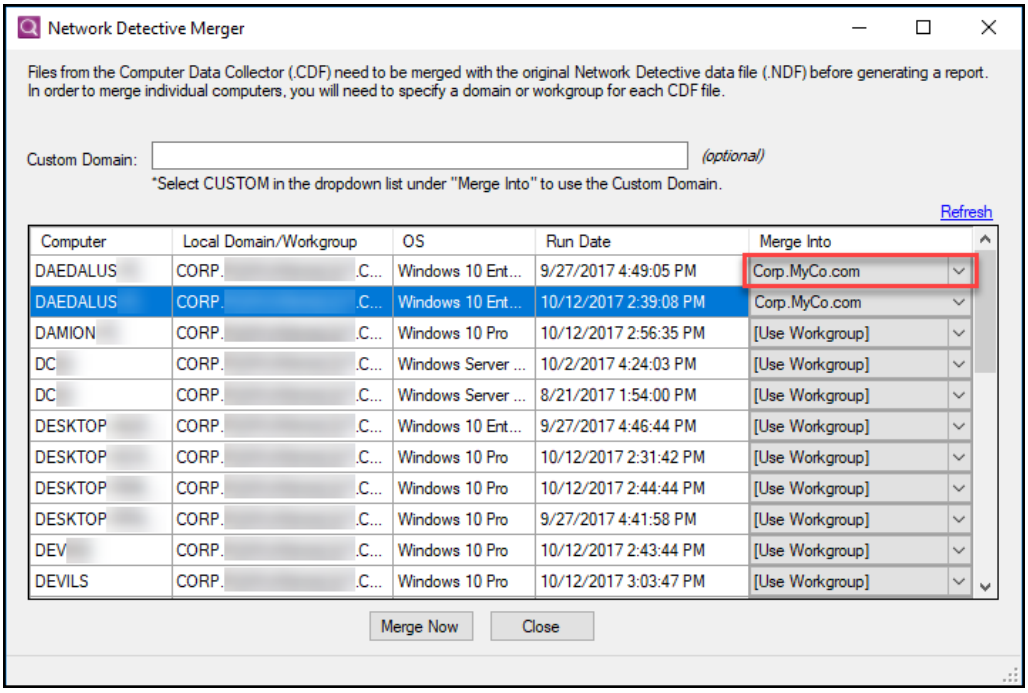


Select the **Finish** button to complete the scan file import process.

Merge of Local Computer Scan Data Collected by the Network Assessment Data Collector

In the case that you performed a **Network Scan** along with a **Local Computer Scan** from the same computer using the **Network Assessment Data Collector**, the **Local Computer Scan** data will need to be merged into the **Network Scan** data file during the scan file import process.

In this instance, during the scan file import process the **Merge Window** will be displayed.



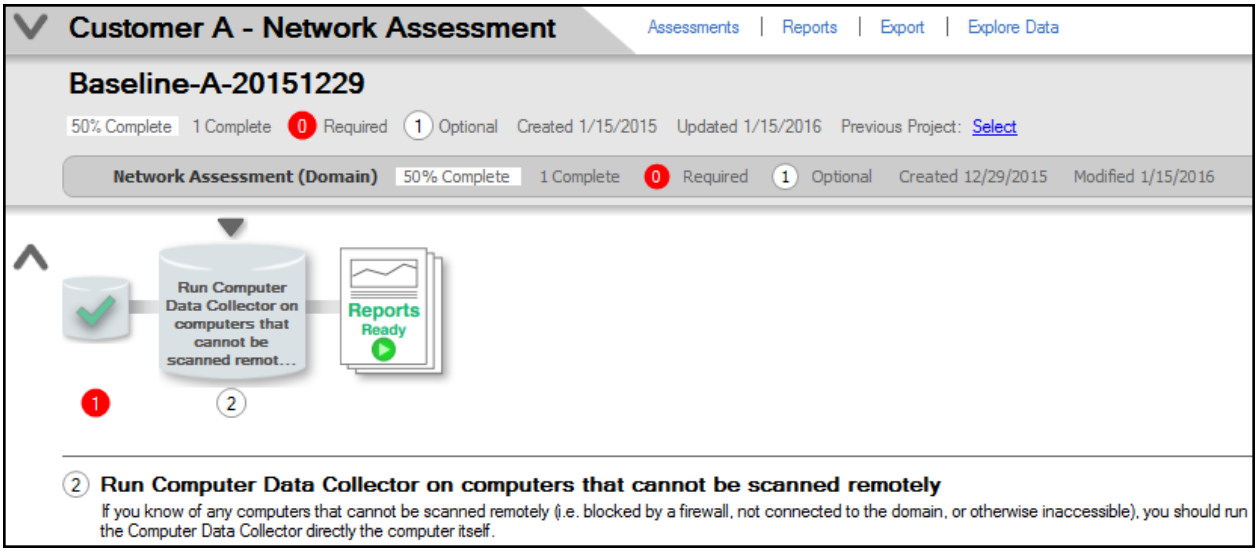
During the Merge process be sure to select a **Merge Into** option based on the type of scan you are performing. When performing local scans of computers that are within a domain by using the **Network Assessment Data Collector**, be sure to reference the domain name of the network being assessed from the **Merge Into** list within the Merge Window.

After the local computer scan's file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Local Computer Scan** data under the **Scans** section of the **Assessment Window**.

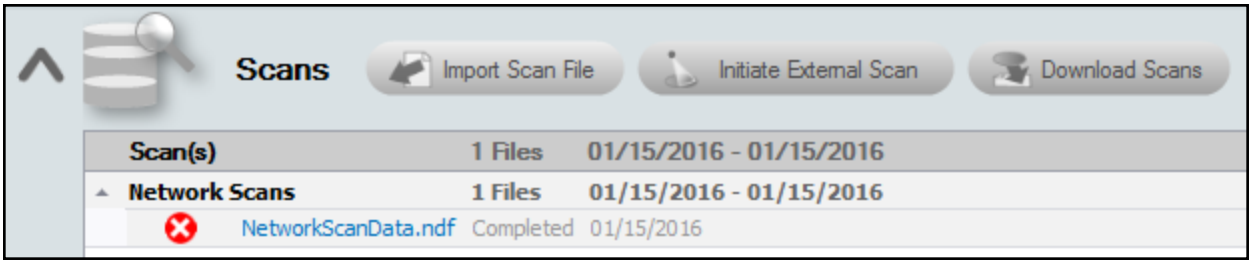
Scans List Updated Upon Completion of Imported Network Scan

After the network scan's .NDF file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Network Assessment's Network Scan** data under the **Scans** section of the **Assessment Window**.

In addition, the **Checklist** information indicators will be updated to present the assessment's current status. Refer to the figure below.



After the network scan file is imported, the **Scans** section of the **Assessment Window** will be updated to list the files imported into the assessment as seen below.



The next step is to proceed with using the **Push Deploy Tool** to configure and perform **Local Computer Scans** on computers that are available within the network as instructed in "Task 2: Use the Push Deploy Tool to Initiate Push of Local Computer Scans on Selected Systems and Import Scan Results" on page 1.

Task 2: Use the Push Deploy Tool to Collect Remaining Data and Import Scan Results

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

The Push Deploy Tool 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

Process to Run the Push Deploy Tool to Perform Local Computer Scans

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

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

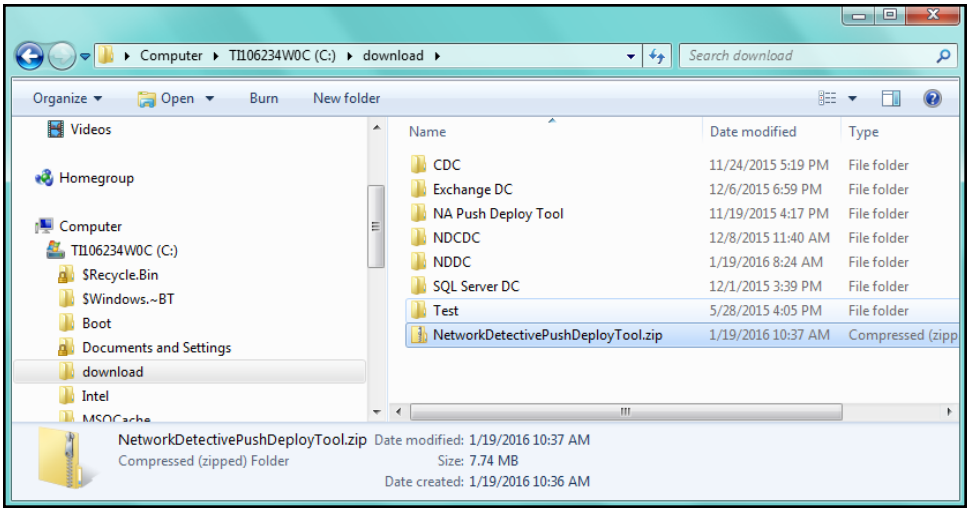
The output files (.ZIP files) from the local scans can either be:

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

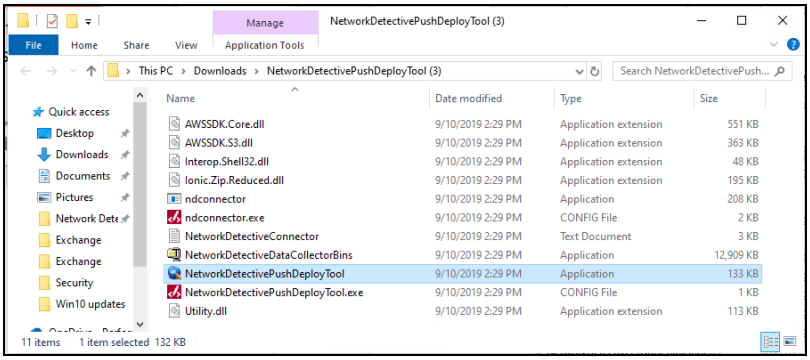
To use the **Push Deploy Tool** to perform local scans for computers within a network, please follow the steps detailed below.

Step 1 – Download and Run the Push Deploy Tool

To perform a local computer scan, download the **Network Detective Push Deploy Tool** from the RapidFire Tools download page at https://www.rapidfiretools.com/nd. Then extract the contents of the **Network Detective Push Deploy Tool** .ZIP file to a USB drive or directly to any machine on the target network.



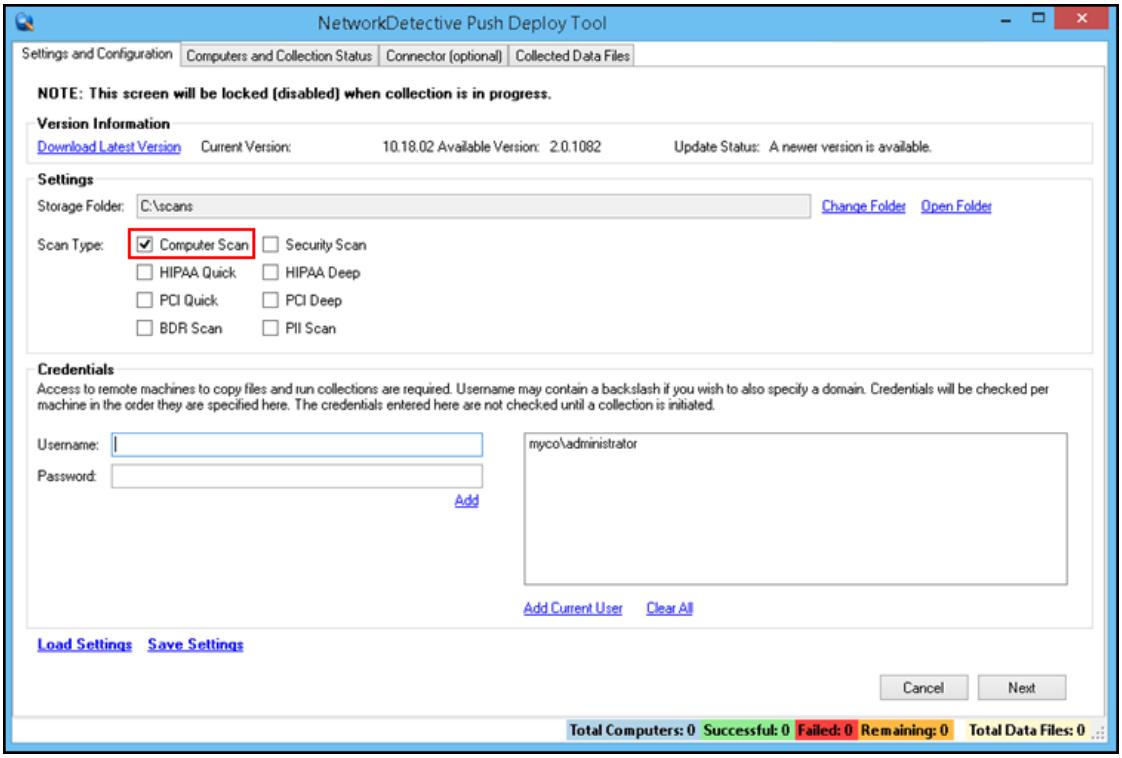
Then right click on the **NetworkDetectivePushDeployTool.exe** application contained within the folder named **NetworkDetectivePushDeployTool** that was created by the .ZIP file extraction. Do not select the config file.



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

Step 2 – Configure the Push Deploy Tool to Perform Local Computer Scan and Add Credentials

Starting the **Push Deploy Tool** will present the following window.



First, set the **Storage Folder location** used to store the scan data collected from the computers scanned.

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

Next, select the **Computer Scan** option.

If the individual performing the **Push Deploy Tool-based** scans is logged into the network using Domain Administrator credentials, then the need to enter credentials as part of configuring the **Push Deploy Tool** scans may not be required as the **Domain Administrator** credentials may be entered in the Credentials list by default.

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

> **Note:** For the Push Deploy Tool to push the local scans to computers throughout the network to perform local computer scans, you need to 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. Push/Deploy also relies on using the Admin$ share to copy and run the data collector locally. Admin$ must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan.

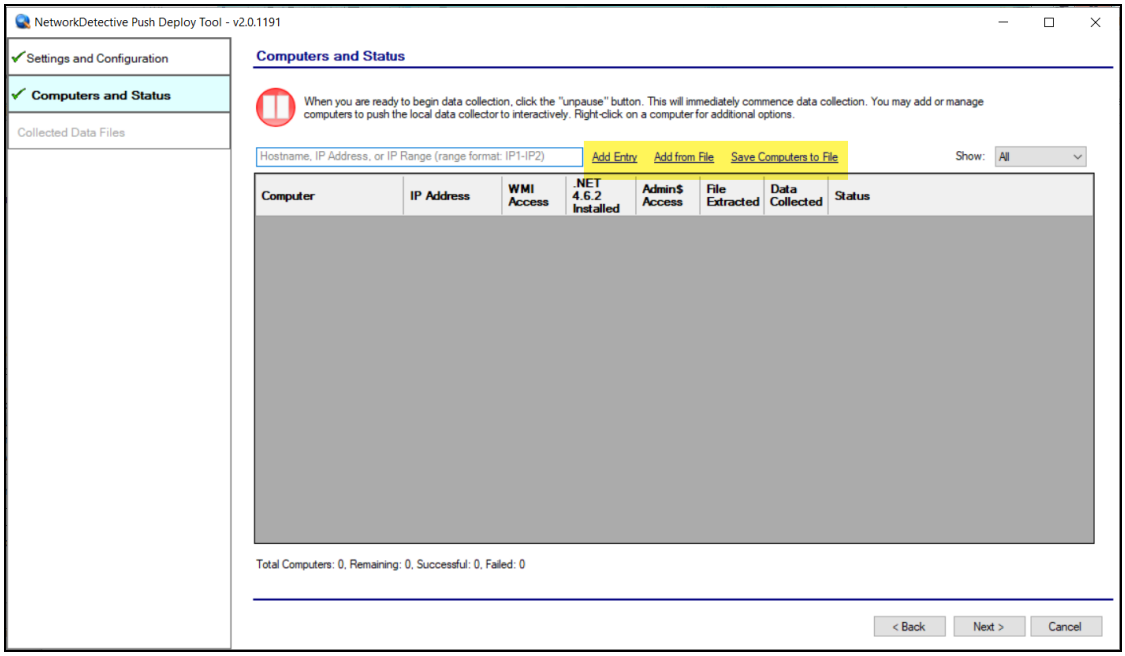
> **Note:** For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same. In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials.

Next, select the **Computers and Collection Status** tab.

Step 3 – Add the Computers to Scan

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

- **Add Entry** to be scanned (Add single IP or IP range)
- **Add** (computers) **from File** that are to be scanned
- Or **Save Computers to File** in order to export a list of computers to be scanned again in future assessments

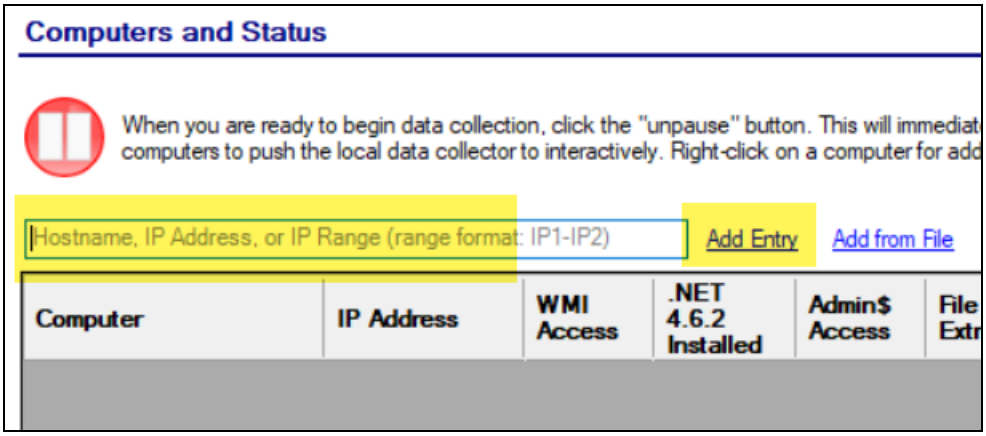


Scan Setup Process Methods used to Configure Computers to be Scanned

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

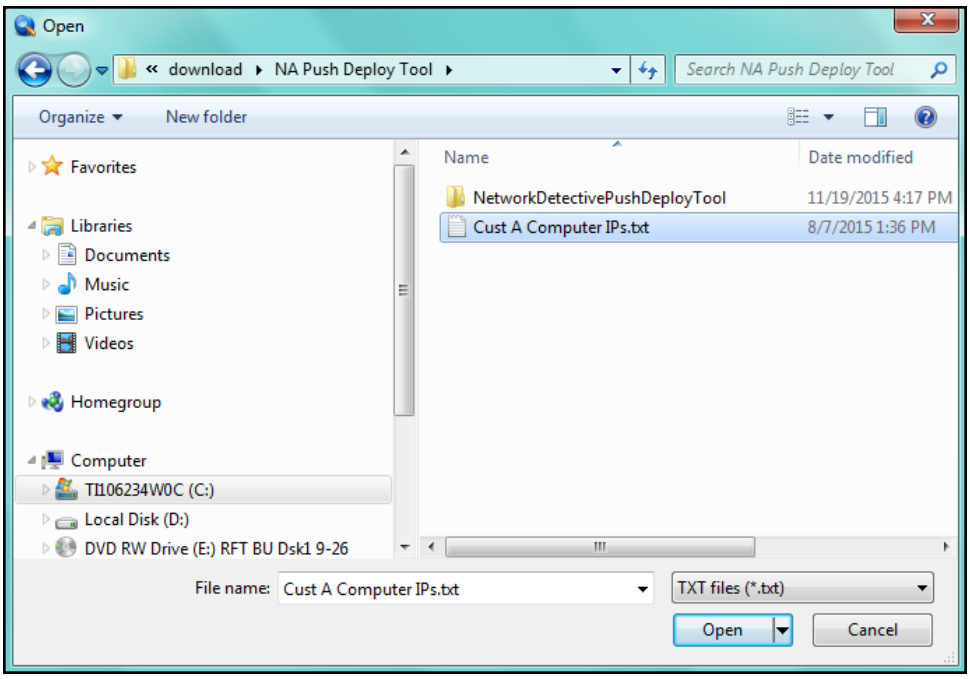
Method 1 - Add IP Entry for Computers to be Scanned

To use the **Add Entry** method to select computers to be scanned, type in the computer IP or IP Range address as shown below, then click on the **Add Entry** 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**.

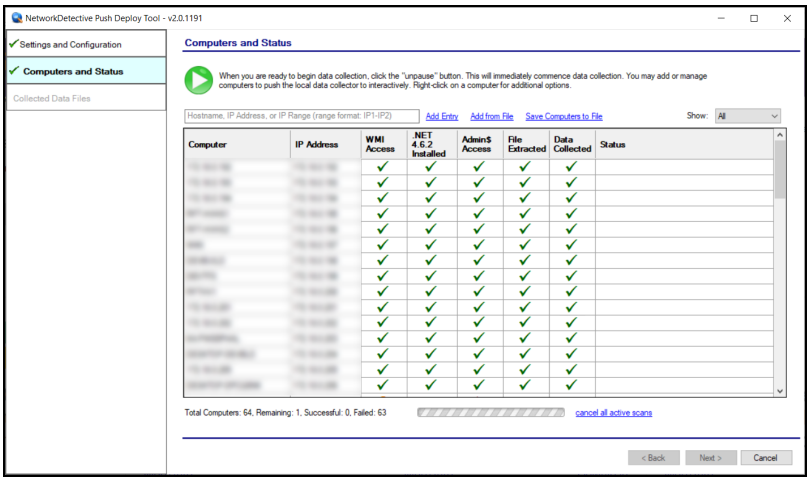
Upon the file's selection and opening the IP address and computer information will be imported into the **Push Deploy Tool** and presented in the **Computers and Collection Status** window for verification prior to starting the scan.

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 **Computer and Collection Status** window.

Step 4 – Initiating the Scan

After creating/adding a list of one or more computers to scan, start the scan either by selecting the "**unpause**" button in the **Computer and Status** window, or, by selecting the

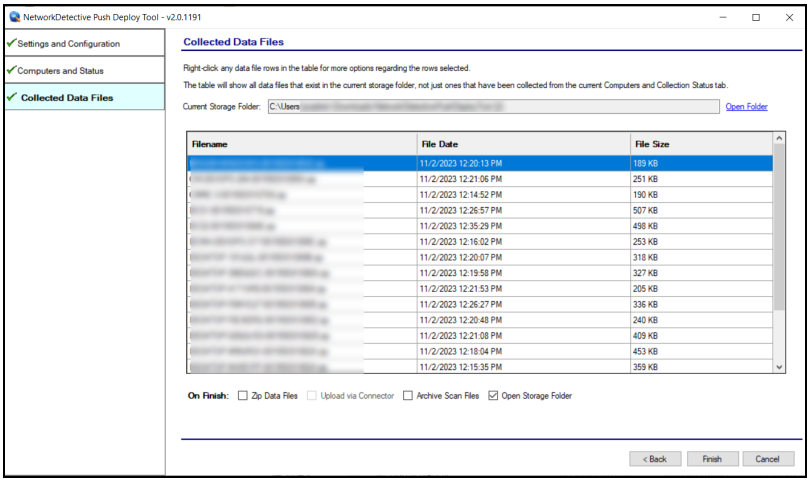
Next button in the **Computer and Status Window** and the scan will be initiated after you confirm that the scan should be started. The status of each computer's scan activity will be highlighted within the **Computers and Collection Status** window as presented below.



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**.

Step 5 – Verify that the Local Computer Scan Data has been Collected

To verify the inclusion of the scan data produced by the **Push Deploy Tool** within your assessment, select the Next button to view the **Collected Data Files** window.



Step 6 – Verify that Network Assessment Local Computer Scan Files are Available from Scan Process

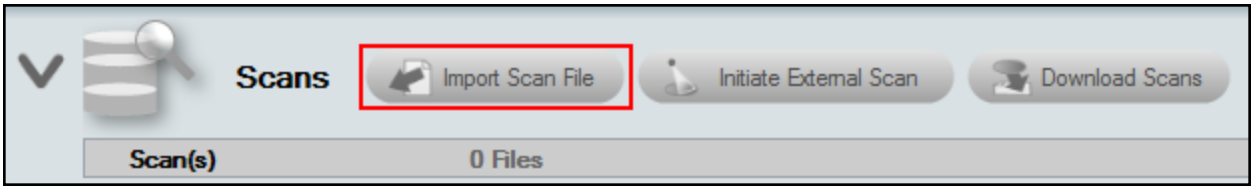
To review or access the files produced by the **Push Deploy Tool's** scans, select the **On Finish: Open Storage Folder** option in the **Collected Data Files** window and then select the **Finish** button.

After all of the Network Assessment's Local Computer Scans are complete for the computers that were selected to undergo this scan, the next phase in the process is to import the scan data files produced by the Local Scans into the current Network Assessment.

Importing the Local Computer Scan Data into the Network Assessment

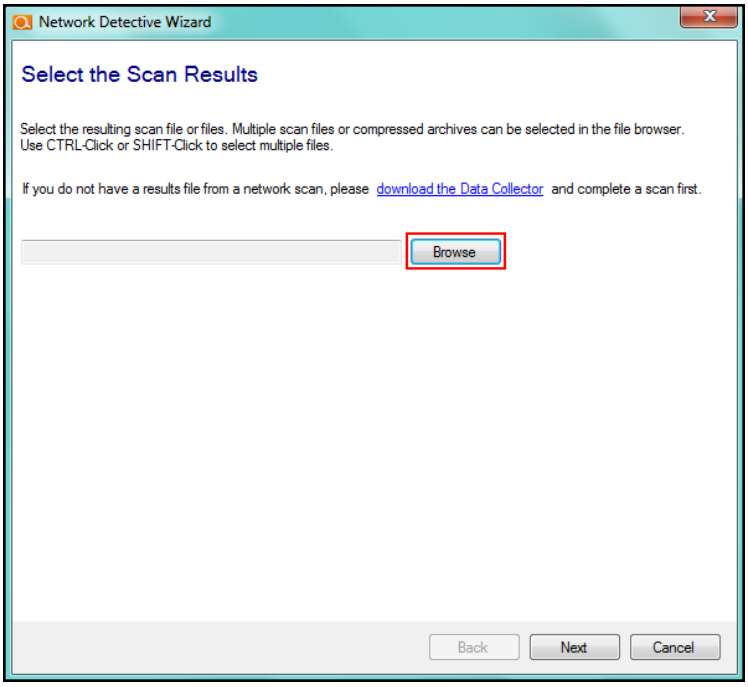
The final phase in this process is to import the data collected during the Computer Scans performed by the **Push Deploy Tool's** local computer scanner into the **Network Assessment** itself.

Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:

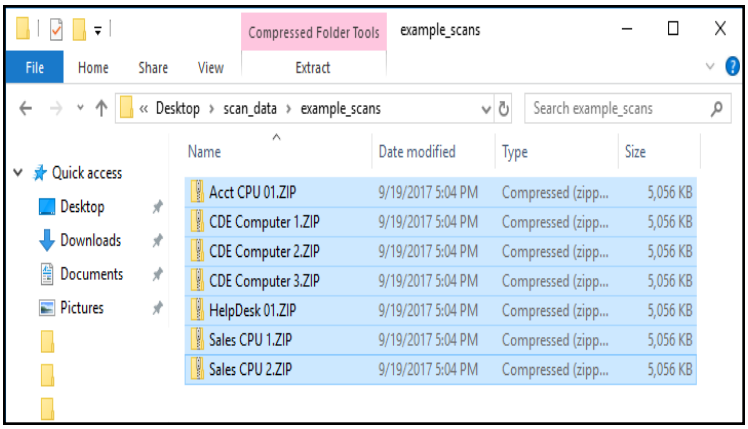


The following **Select the Scan Results** window will be displayed. This window enables you to **Browse**, select, and import the .ZIP scan files into the **Network Assessment**.

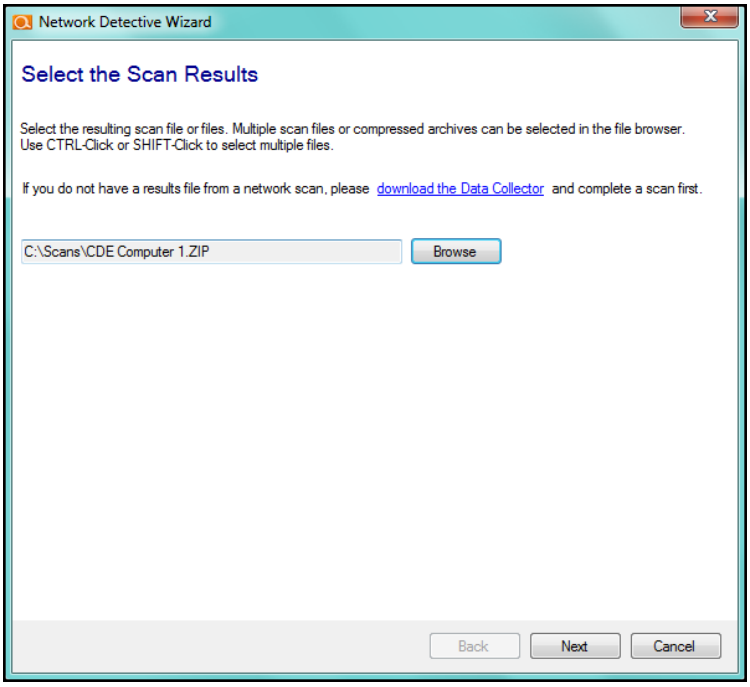
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP files produced by the **Push Deploy Tool** based **Local Computer Scans** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Local Computer Scan** data file.

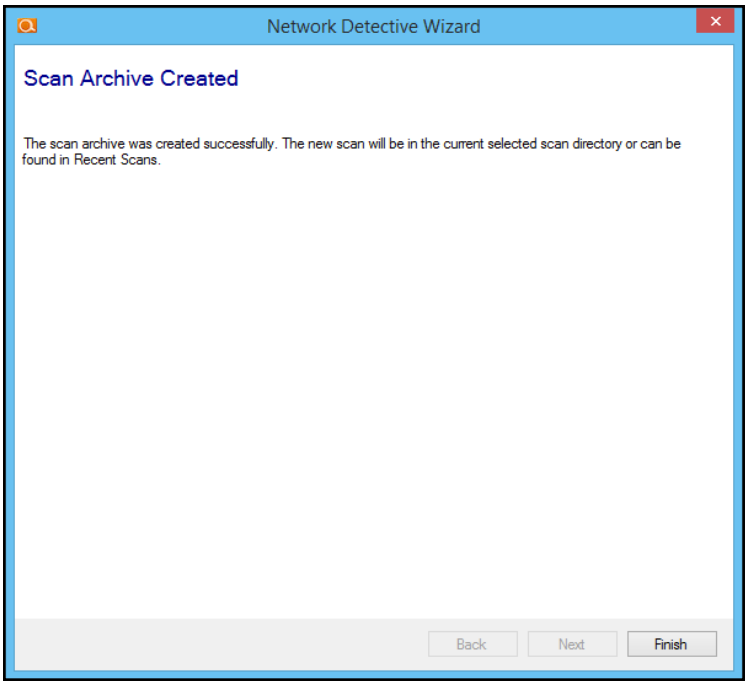


Then click the **Open** button to import the scan data. The following window will be presented.



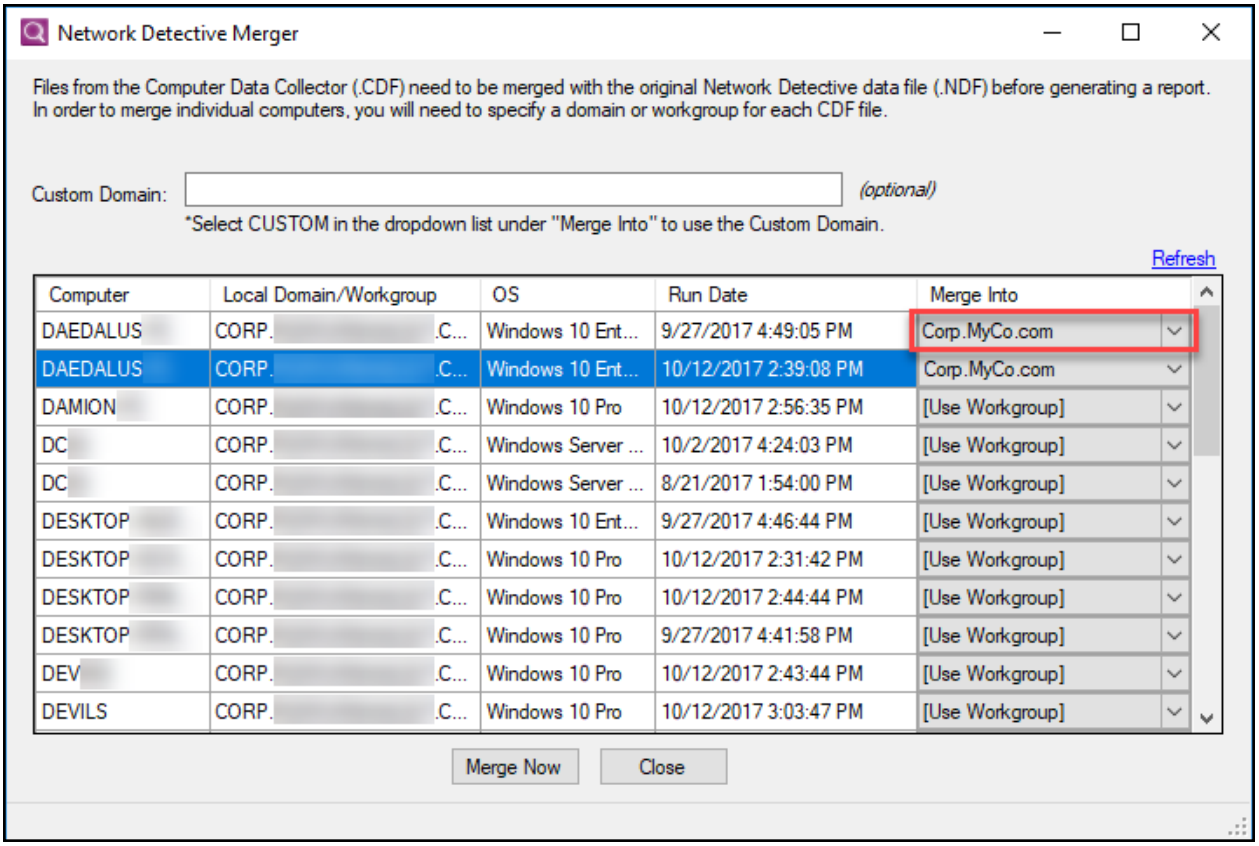
To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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



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

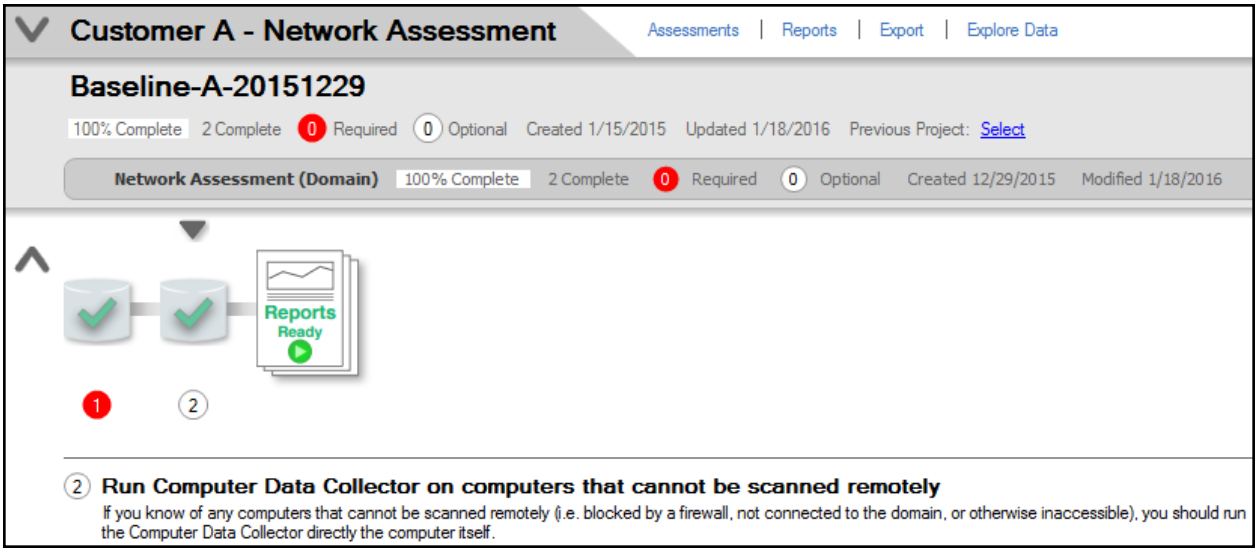
The **Merge Window** will appear.



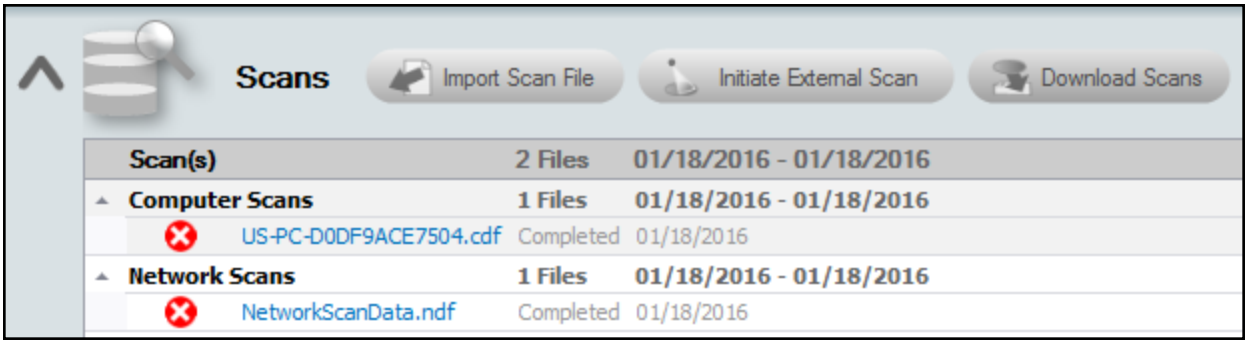
During the Merge process be sure to select a **Merge Into** option based on the type of scan you are performing. When performing local scans of computers available on the network that are within a domain by using the **Push Deploy Tool**, be sure to reference the domain name of the network being assessed from the **Merge Into** list within the **Merge Window**.

After the local computer scan's .ZIP file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Computer Scan** data under the **Scans** section of the **Assessment Window**.

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



After the **Local Computer** scans files are imported into the assessment, the **Scans** section of the **Assessment Window** will be updated to list the **Computer Scans** files imported into the assessment as seen below.



Task 3: Run the Computer Data Collector to Perform Local Scans on the Computers that were Unreachable during Push Deploy Tool Scanning (OPTIONAL)

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

Use the **Computer Data Collector** to run the **Local Scan** on selected computer systems manually.

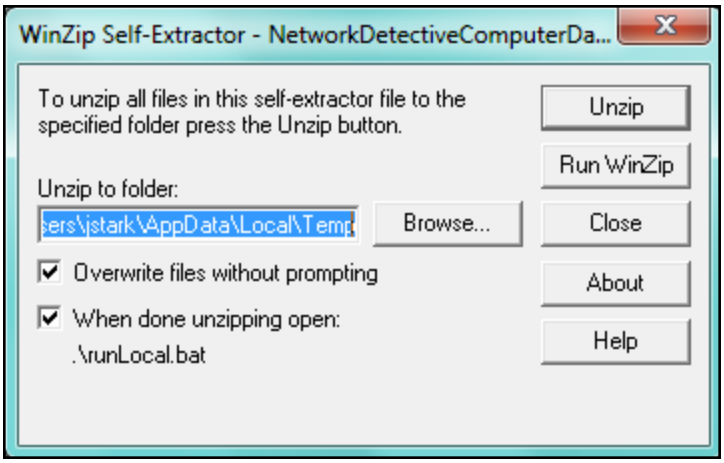
Running the Computer Data Collector to Perform Local Computer Scans

For computers that were unreachable during the **Local Scans** that were to be performed using the **Push Deploy Tool** and still require scanning, you will need to download and run the **Computer Data Collector** from the RapidFire Tools software download website to a folder on a local computer or a USB drive. The **Computer Data Collector** is a self-extracting .zip file named **NetworkDetectiveComputerDataCollector.exe** that executes as an ".EXE" and is completely non-invasive – it is not "installed" on the local computer being scanned or any other machine on the client's network, and does not make any changes to the system.

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

Always download the latest version of the Computer Data Collector. Visit the RapidFire Tools software download website and download and run the **Network Assessment Data Collector** file. This file is a self-extracting ZIP file that does not install on the client computer. Use the **Unzip** option to unzip the files into a temporary location and start the **Computer Data Collector**.

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



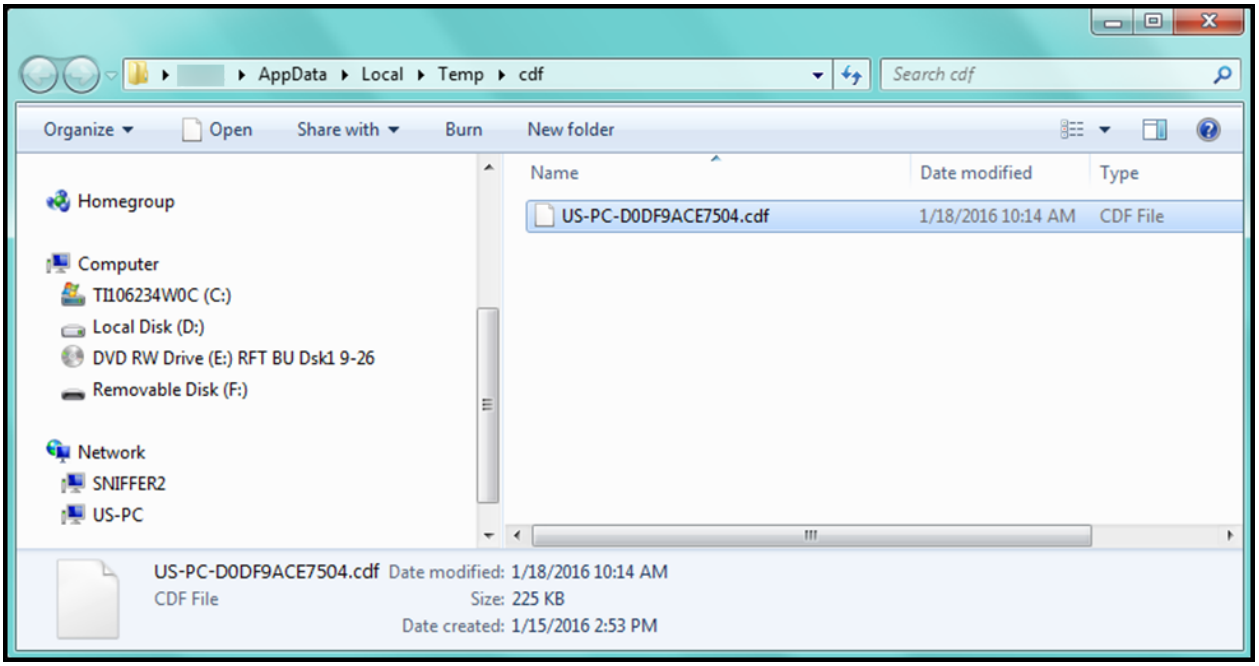
Note: Note that the Computer Data Collector will have to be downloaded and run on each local computer that is to be included in the Network Assessment that you are performing.

Step 2 – Starting the Computer Data Collector Scan on a Local Computer

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

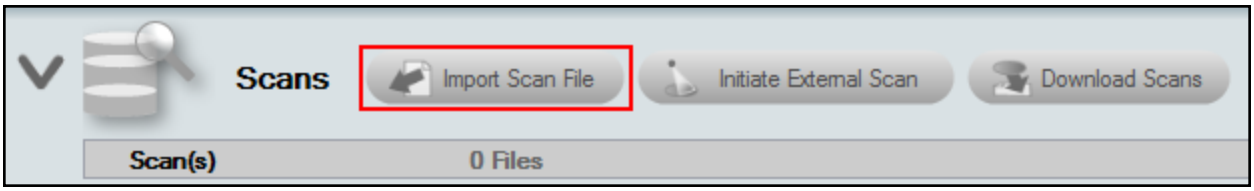
Step 3 – Review Local Scan File Location

Upon completion of the Local Computer Scan using the **Computer Data Collector**, a window will be presented to you displaying the location of the scan output file that has a file extension of .CDF. This .CDF file should be retrieved and imported into your assessment.

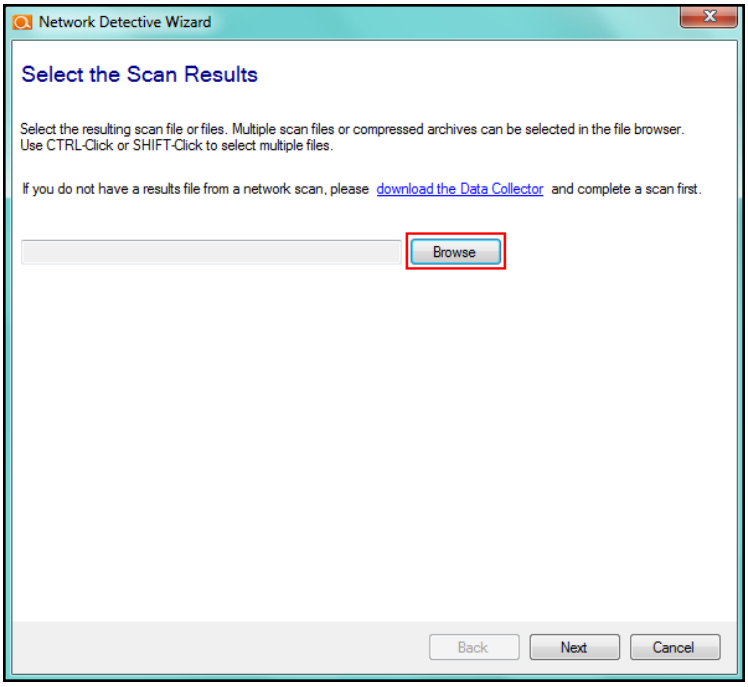


Importing the Local Scan Data

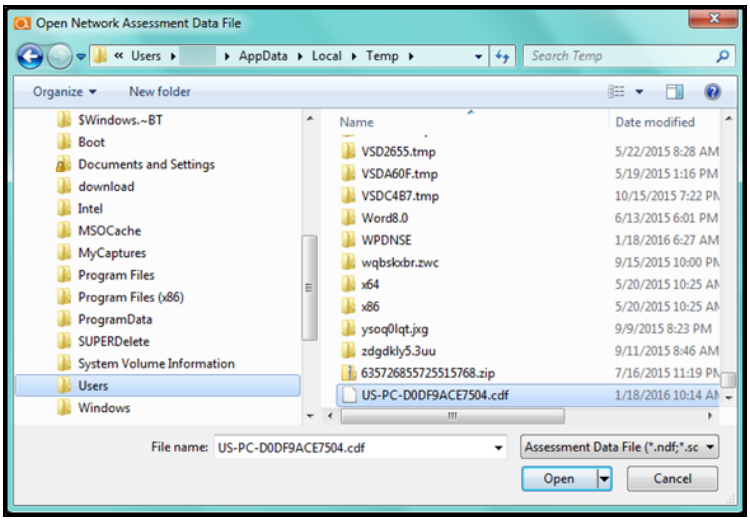
The final step in this process is to import the data collected during the **Local Scans performed** by the **Computer Data Collector** into the **Active** Network assessment. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment Window**:



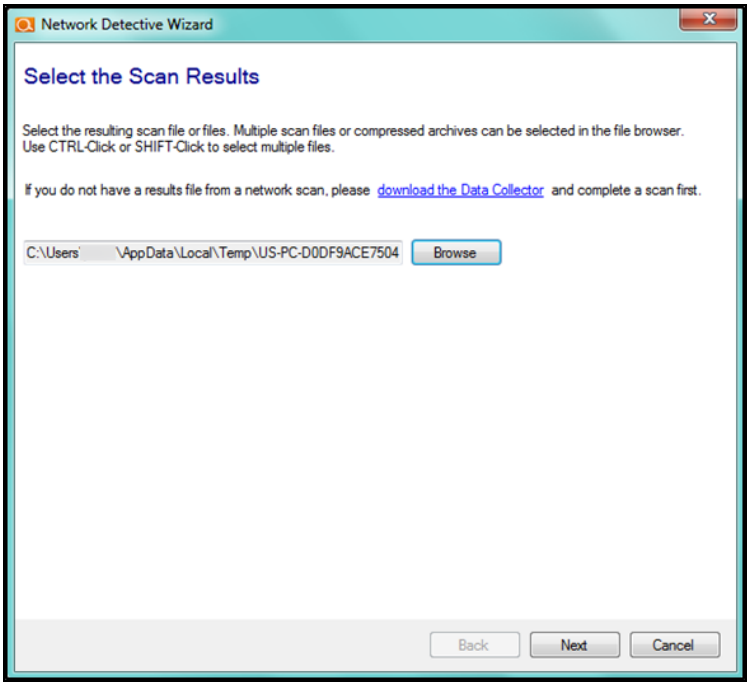
The **Select the Scan Results** window will be displayed thereby allowing you to import the .CDF file produced by the **Network Assessment Data Collector Network Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Network Scan** data file.

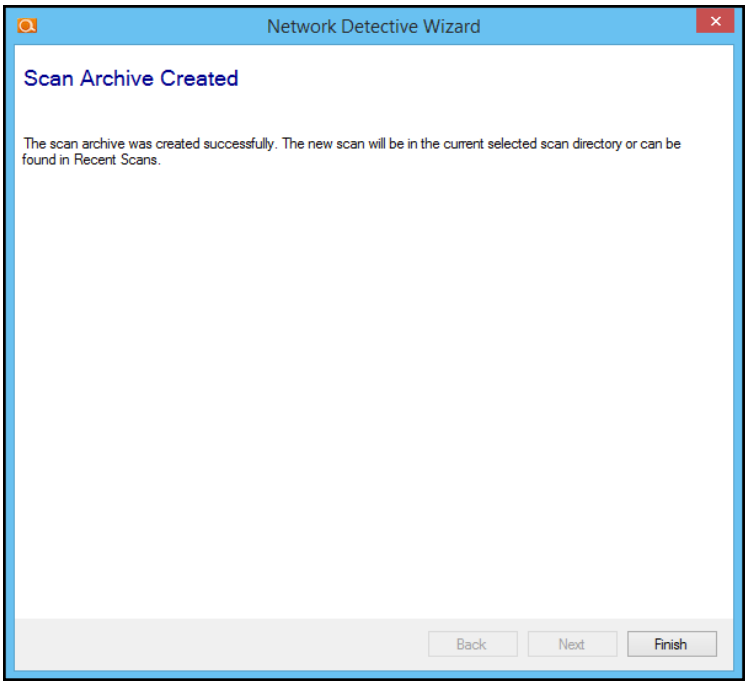


Then click the **Open** button to import the scan data. The following window will be presented.



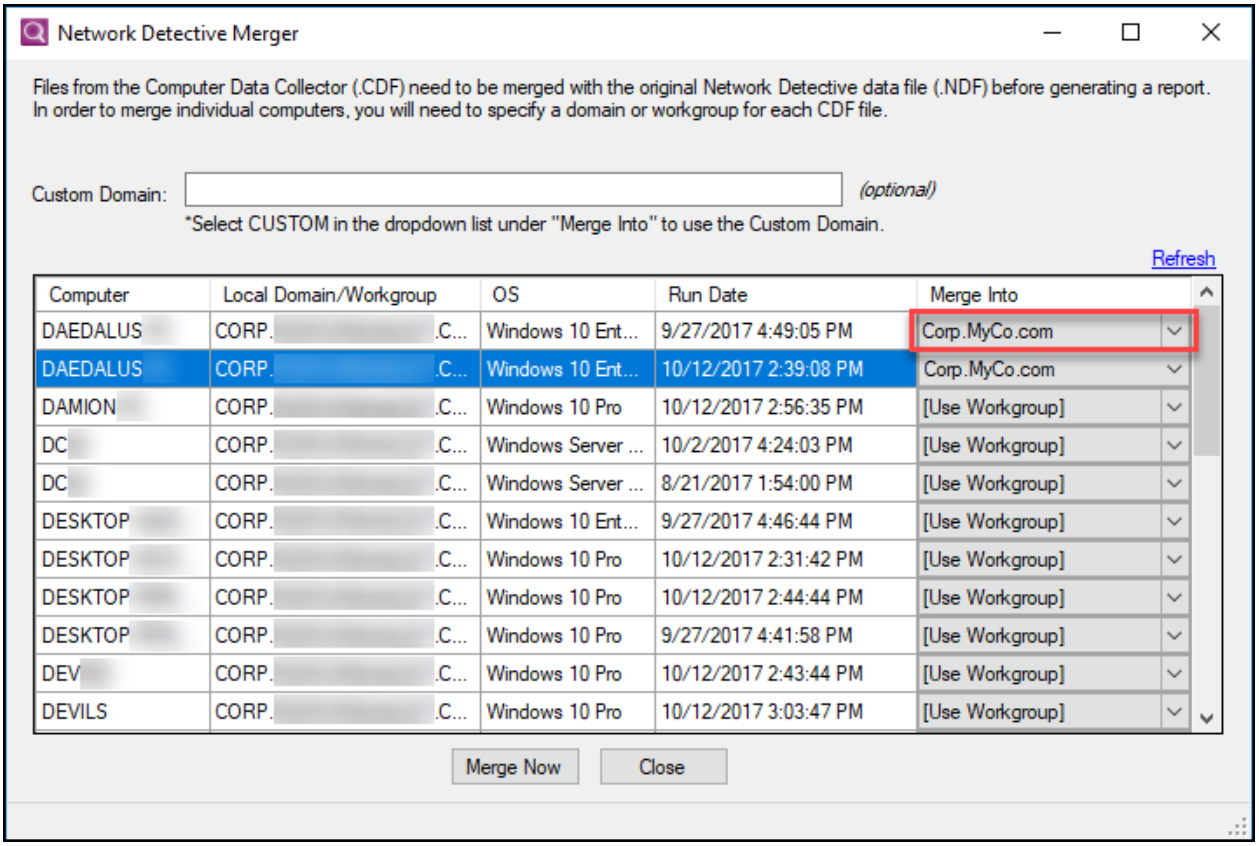
To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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



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

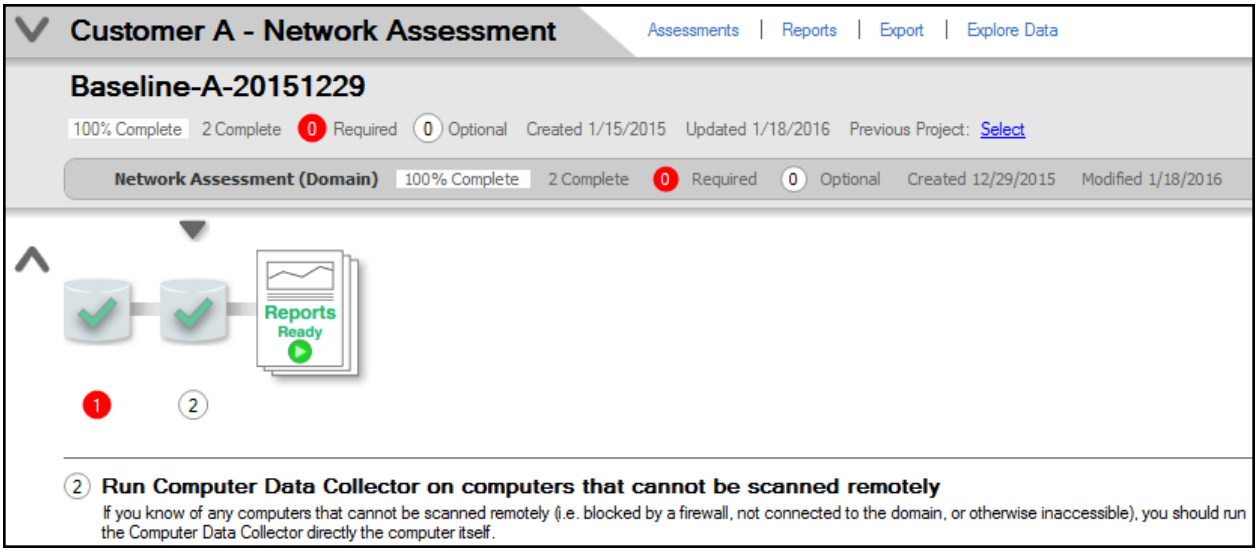
The **Merge Window** will appear.



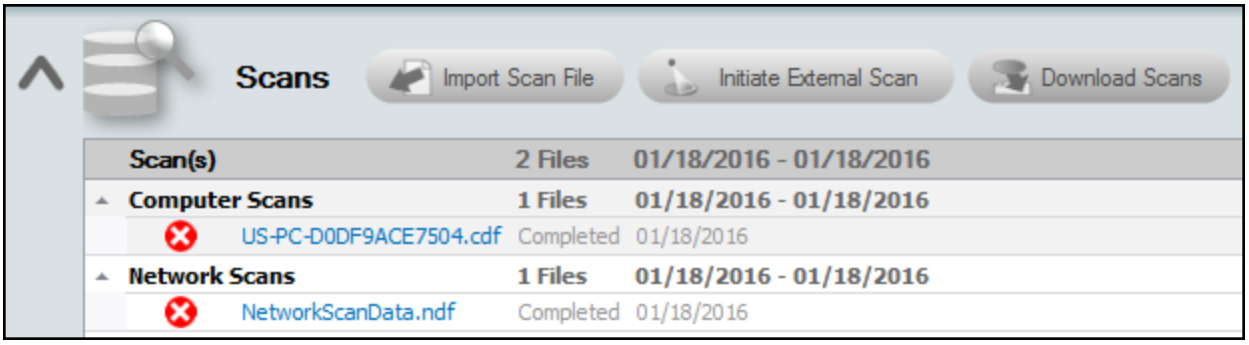
During the Merge process be sure to select a **Merge Into** option based on the type of scan you are performing. When performing local scans of unreachable computers that are within a domain by using the **Computer Data Collector,** be sure to reference the domain name of the network being assessed from the **Merge Into** list within the Merge Window.

After the local computer scan's .CDF file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Computer Scan** data under the **Scans** section of the **Assessment Window**.

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



After the **Local Computer** scans files are imported into the assessment, the **Scans** section of the **Assessment Window** will be updated to list the **Computer Scans** files imported into the assessment as seen below.



Task 4: Document Exceptions that Mitigate Identified Risks and Improve Risk Scoring

Complete the Issue Exception Worksheet (Optional)

The **Issue Exception Worksheet** is an **optional** worksheet that compiles the issues discovered by the Network Assessment Data Collector network scans, Push Deploy Tool Scans, and the Computer Data Collector used throughout the Network Assessment process.

This purpose of this worksheet is to enable the individual performing the assessment to document actions that remediate identified issues in order to mitigate the risks resulting from issues identified by the assessment process.

At the initial completion of an Assessment, you can generate a **Risk Report** to review the risk issues initially identified during the Assessment.

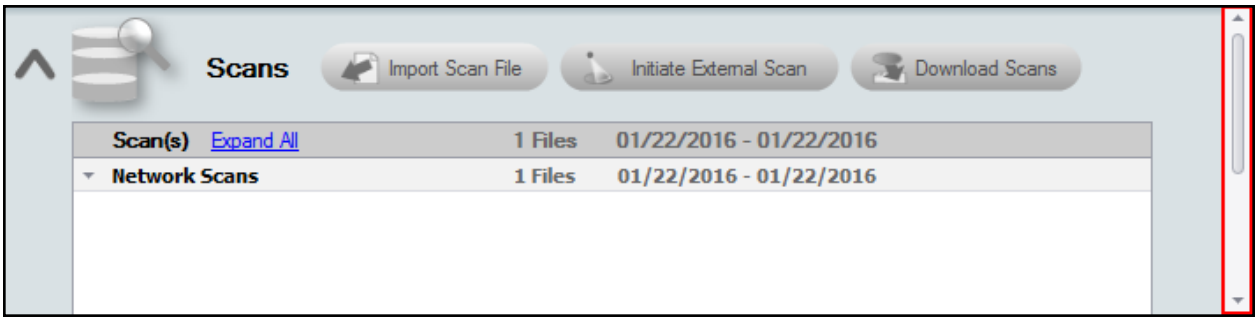
In the case that some of the issues presented in the **Risk Report** are being mitigated through some sort of compensating control, you can remove the risk identified during the assessment from the **Risk Report** through the use of the **Issue Exception Worksheet**.

The **Issue Exception Worksheet** is used to document **Issue Exceptions** along with compensating controls used to mitigate identified issues. The compensating controls document the actions that have been taken to mitigate the risks associated with a particular issue. Documenting these compensating controls will allow you to reduce the risk identified and the **Risk Score** calculated and presented in the **Risk Report**.

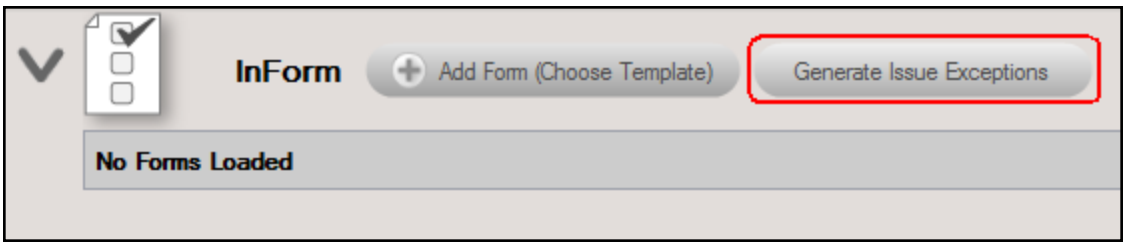
Upon viewing the **Issue Exceptions Worksheet** you will see that the Issues listed in the worksheet are the same risk issues are outlined in the **Risk Report**.

Process to Document Issue Exceptions

To access the **Issue Exception Worksheet** select, first, select the scroll bar next to the **Scans Bar** located at the bottom of the **Assessment Window**, and scroll down to the **InForm Bar**.

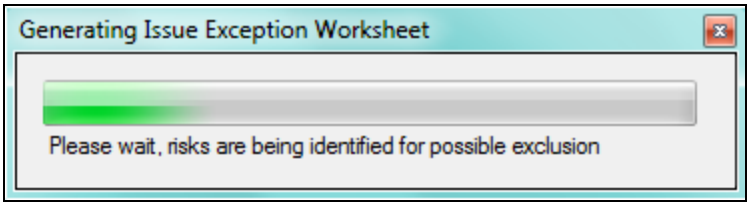


Then select the "**edit**" **Issue Exception Worksheet** option available on the **InForm Bar** located in the **Assessment Window** as presented below:

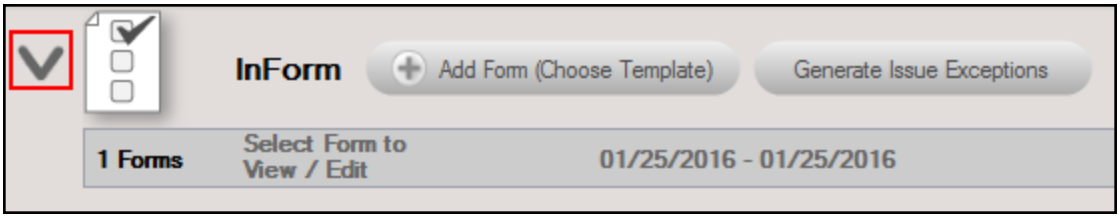


This action will result in an **Issues Exceptions Worksheet** being generated.

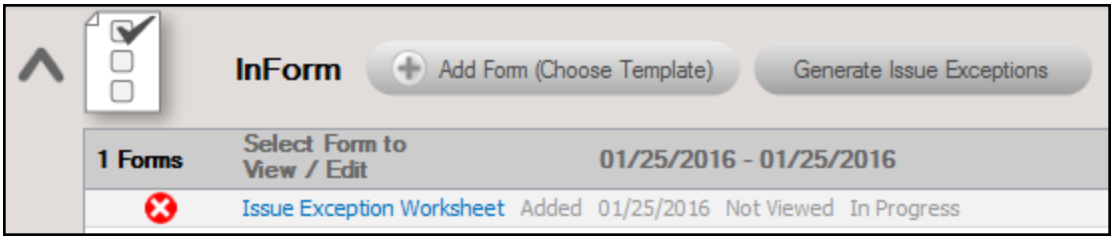
The **Generating Issue Exception Worksheet** status bar will be presented during the generation of the worksheet.



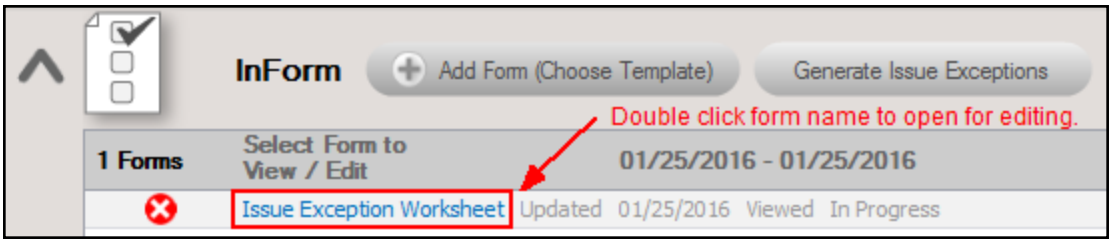
Once the **Issue Exception Worksheet** is generated, the **Issue Exception Worksheet** is added to the **InForm** section of the **Assessment Window**



To view and edit the **Issue Exception Worksheet**, select the down arrow located on the left side of the **InForm Bar** to expand the list of forms/worksheets available for viewing below the **InForm Bar**.

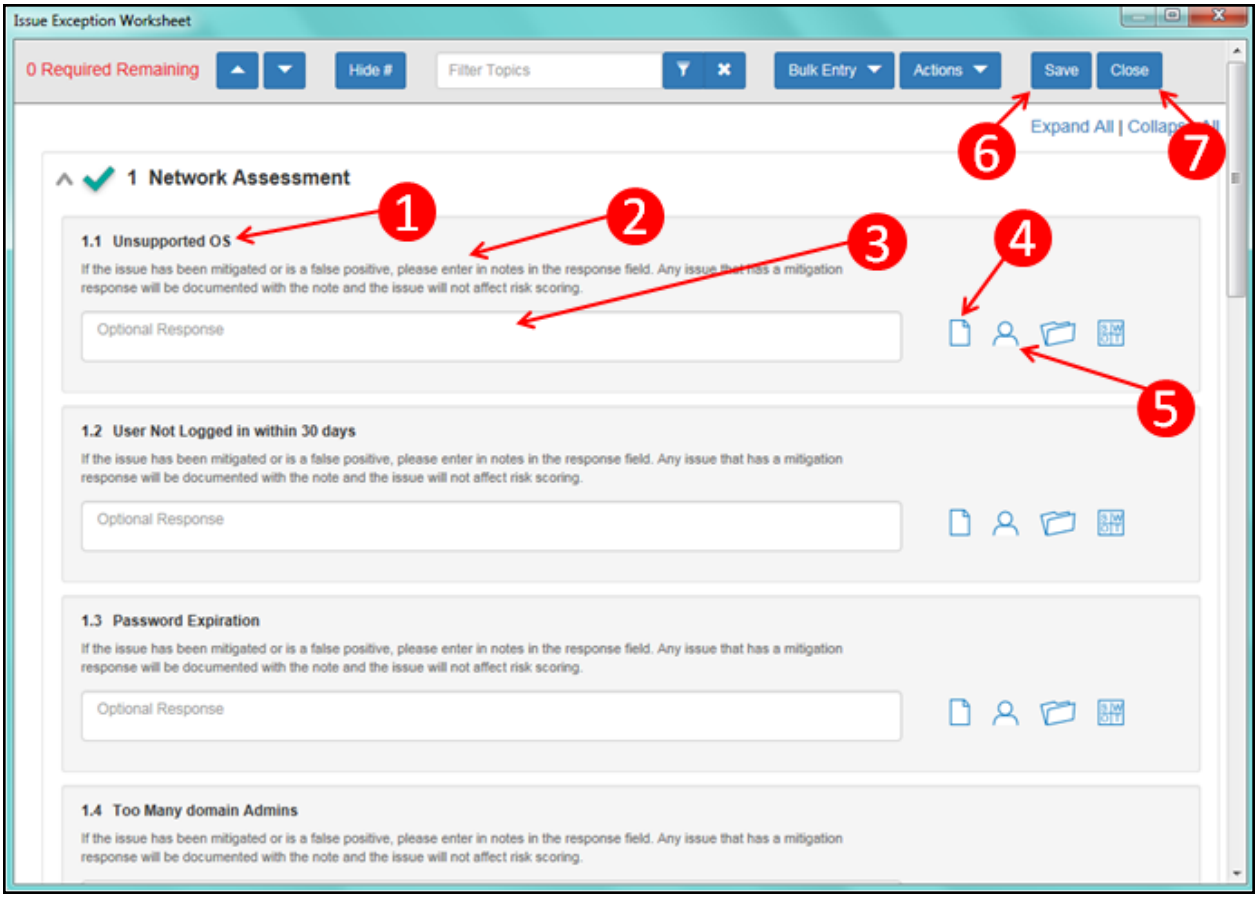


The **Issue Exception Worksheet** will become available for viewing and editing.



Double click on the **Issue Exception Worksheet** text denoted in Blue text to open the worksheet for viewing and editing.

Upon opening the **Issue Exception Worksheet**, the following window is presented:



Issues and their **Exceptions Responses** are listed in the Worksheet window to enable you to document "Responses" outlining the actions used to mitigate the **Issues** identified during the **Assessment**. Follow the steps below to review and document issue mitigation or clarification responses.

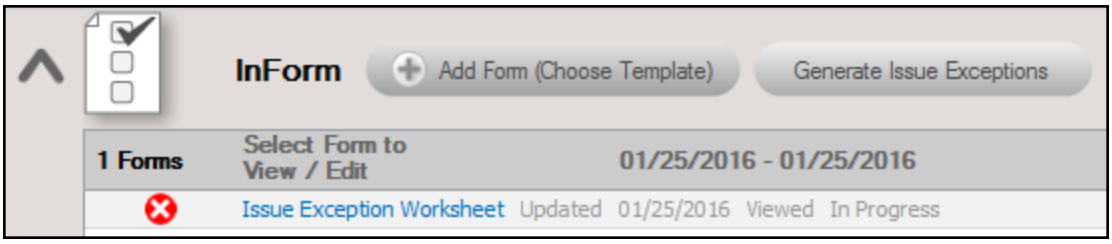
To document the "**responses**" to the Instructions/Questions presented in this worksheet:

1. Review the "**Topic Question**".
2. Review the "Instructions". Instructions provide guidance and are not included in the reports.
3. Enter the "**Response**" in the Response field. A **Response** must be given for each Issue entry to complete the worksheet if you want to remove these issues from the **Risk Report**.

> **Note: Please note that the Issue Exception Worksheet does not require a response for each and every topic**. Enter your **Response** if applicable, otherwise, leave the entry blank.

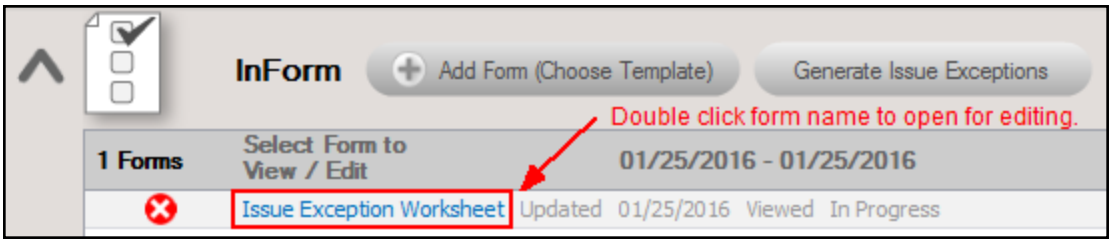
4. Select the **Notes** icon to enter any "Notes" relevant to a particular **Exception** mitigation action or explanation topic's Response.
5. Select the **Respondent** icon to enter the name of individual that responded or provided information to respond to the topic's question or requirement in the "Respondent" field.
6. Save your answers periodically and **Save** when you are done.
7. Select **Close** to close the worksheet when you are done.

Once the **Issue Exception Worksheet** is saved, it will be listed under the **InForm Bar** located in the **Assessment Window**. Click on the selector control on the left of the **InForm Bar** to access the **Issue Exception Worksheet's** entry in the **InForm** list.



Please note that the **Issue Exception Worksheet** status indicator to the right of the worksheet name shows that the worksheet has been **Updated**.

You can return to the **Issue Exception Worksheet** to make any modifications by Double clicking on the **Issue Exception Worksheet** text denoted in Blue text.

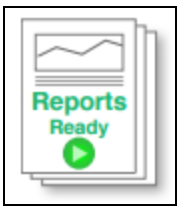


> **Tip:** To learn more about how to save time completing Surveys and Worksheets, please see "Completing Worksheets and Surveys" on page 263.

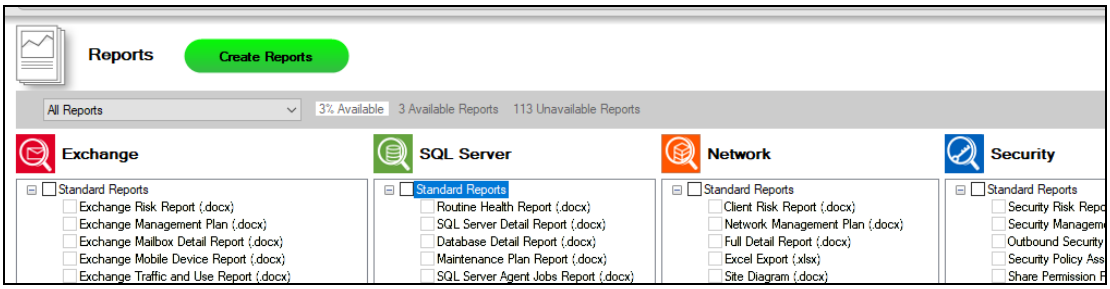
Phase 4 – Generating Network Assessment Reports

Steps to Generate Network Assessment Reports

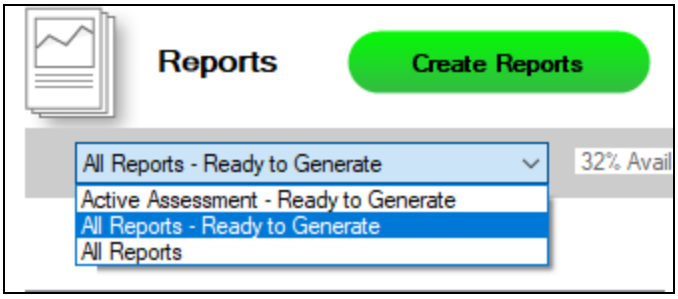
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



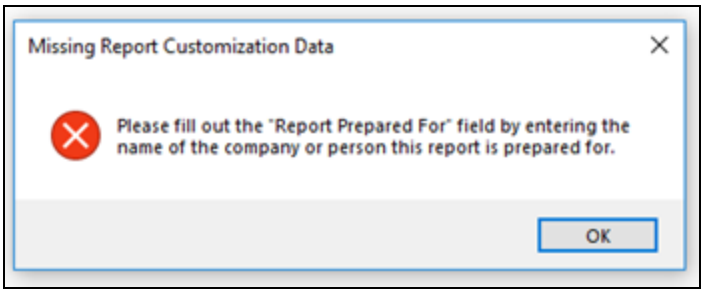
4. Select which of the Network Assessment reports that you want to generate.



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.

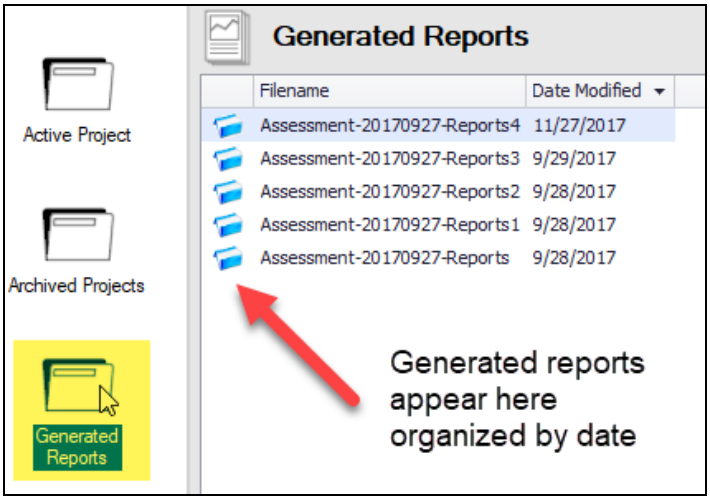


5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.
   i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



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.

Using Data Explorer with Network Assessment Scan Data to Create Custom Reports and Monitor Customer Metrics

This section describes how to use the Network Detective Data Explorer. The Data Explorer is a tool available to Network Detective subscribers. It enables the user to

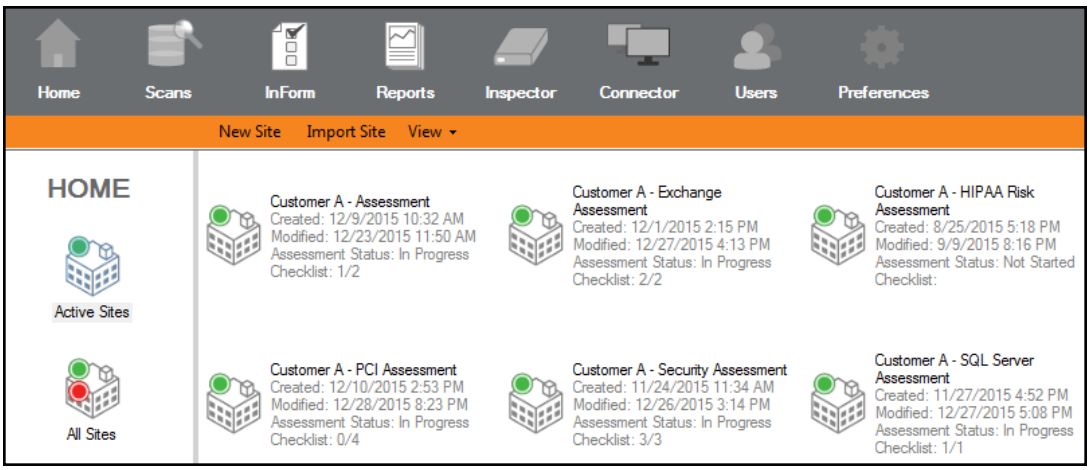
preview report data and continuously monitor customer metrics. Used with the Site Module, this is a powerful way to ensure that you get the most from Network Detective.

Requirements

- Network Detective Application
- Network Detective Subscription

Creating a Site

In order to use the Data Explorer, you must have a Network Detective Site associated with your customer.



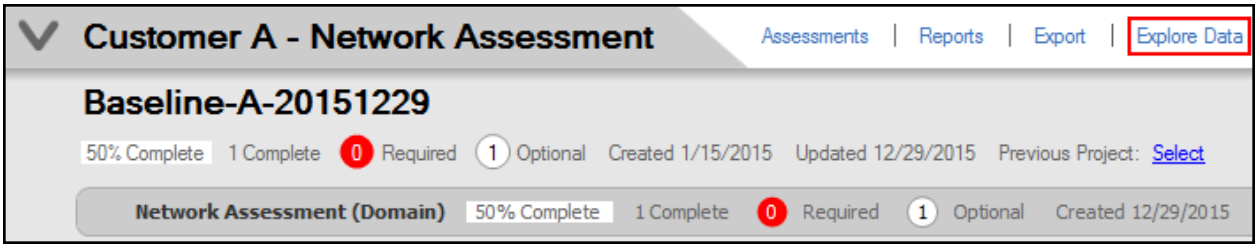
Creating a Site is simple, just click the **New Site** and follow the prompts to name your Site and start a Network Assessment project. If you have already collected data, the NDF/NDZ and InForm data can be easily imported into a Site's Assessment project.

Note that you must have Network Scan data in order to use the Data Explorer.

Opening the Data Explorer with an Active Network Assessment

After you have created a Site for your customer, performed a Network Assessment, and added Scan data, you can use the **Data Explorer** tool to preview graphs and charts that may be included in your Reports.

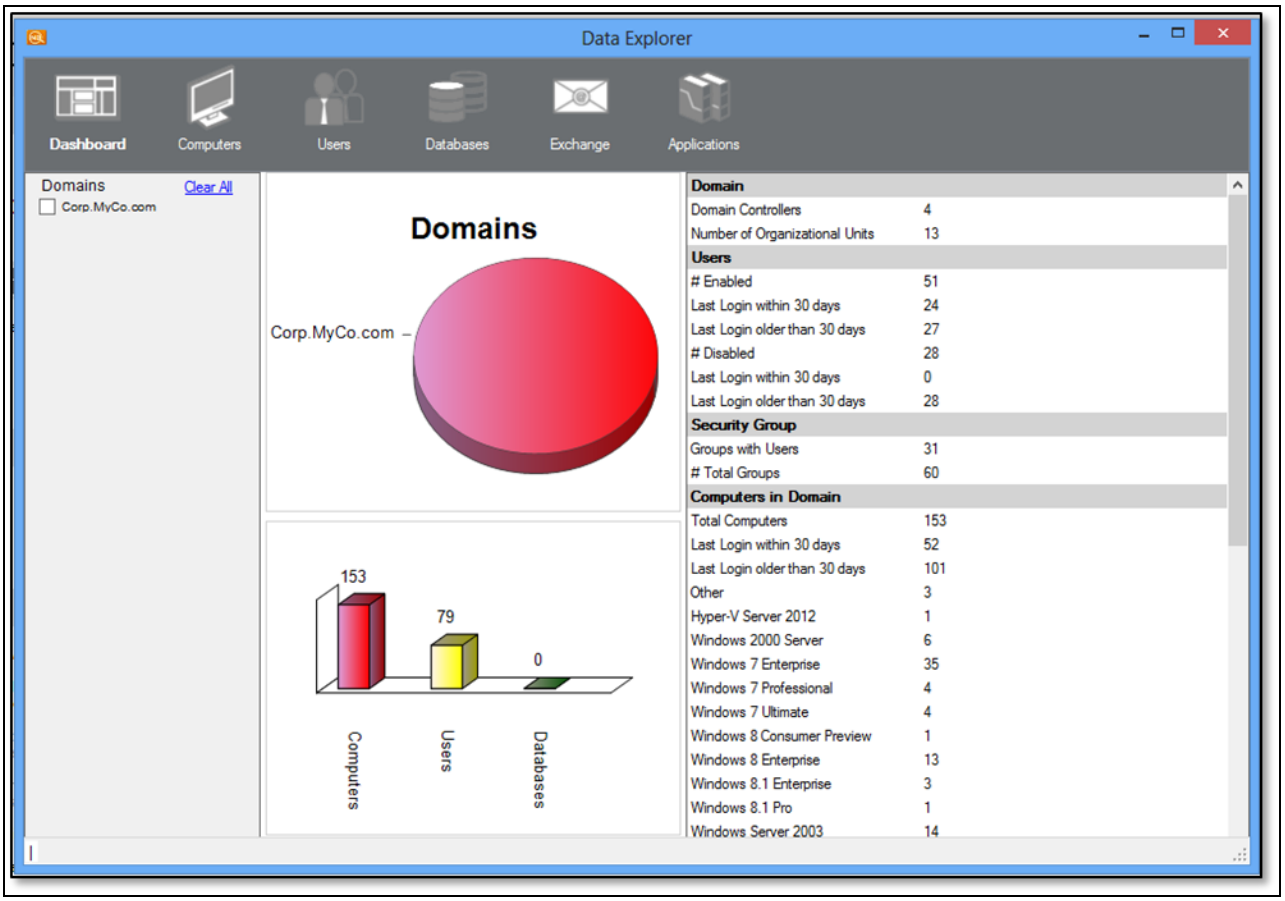
In the active Assessment Dashboard you can select the **Explore Data** Link to use Data Explorer.



This action will start the **Data Explorer**.

The Data Explorer Dashboard

When you open the **Data Explorer** the default view is the **Dashboard**, which summarizes all of the Scan data you have imported into the current Assessment.



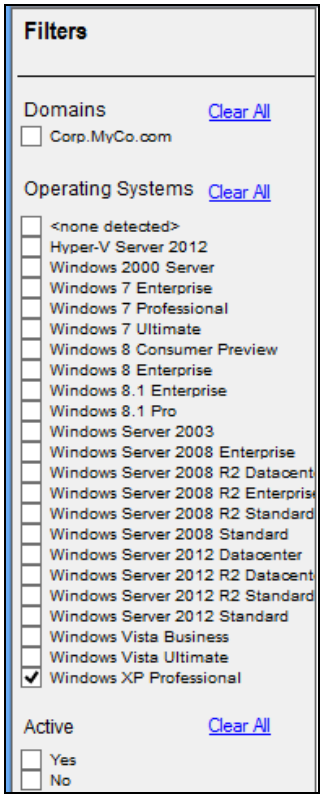
This screen is a condensed overview of the Network Assessment. All of the metrics in the Dashboard are current. As you import new data and continue with your **Assessment**, the figures will be updated.

The **Dashboard** can help you monitor a Site and track the progress of your **Assessment**. It is faster and more convenient than generating a report. In many cases, small changes such as if customer has added a Windows XP machine to the network, may not necessitate a full report.

Using Filters

After you have created a **Site** for your customer, performed a Network Assessment, and added Scan data, you can use the **Data Explorer** tool to view information about your customer's Network.

Note: The Network Assessment data can be viewed by a number of different "filter" categories. These Filters include: by Computers, by Users, by Databases, by Exchange Servers, or by Applications



Select the **Filter** that you want, (i.e. Computers, Users, Databases, Exchange, or Applications.)

To filter the data, click on a Filter icon at the top of the Data Explorer window. For example, click on the **Computers** icon to switch to a more specific view of your Customer's Network Assessment data by computer.

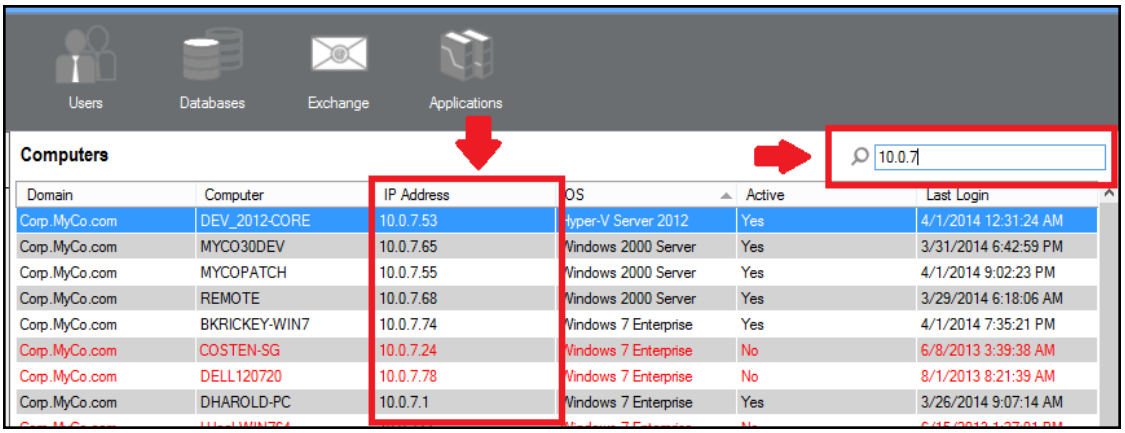
From here, you can also further filter the viewed data using the search box in the upper right-hand corner or the **Filters** menu on the left hand side.

Filter by criteria such as computers running a Windows Operating System, inactive computers, or computers on different domains.

In the Network Detective application, navigate to **Sites**, **Open** the **Site** and then go to an **Active Assessment**.

From the **Active Assessment**, click the **Explore Data** link in the **Assessment Window**. This action will start the Data Explorer.

Using the Search box, you can filter by other values, such as IP address.



You can also view additional details for each computer by double clicking on the row presented in the list.

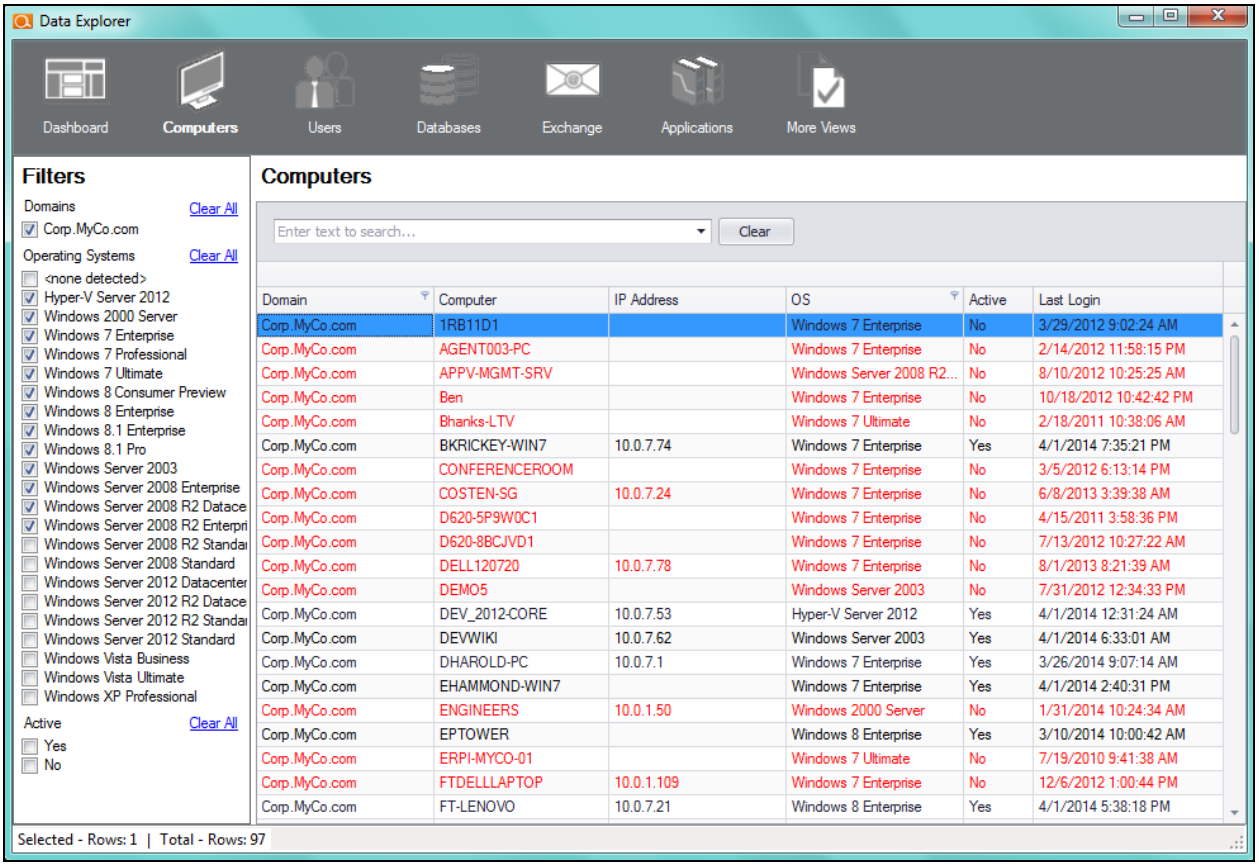
Creating Custom Reports

To create custom reports using Microsoft Excel or Word, you have the ability to copy unfiltered and filtered Network Assessment data into tabular form in each of these applications.

To create a custom report please following the steps below:

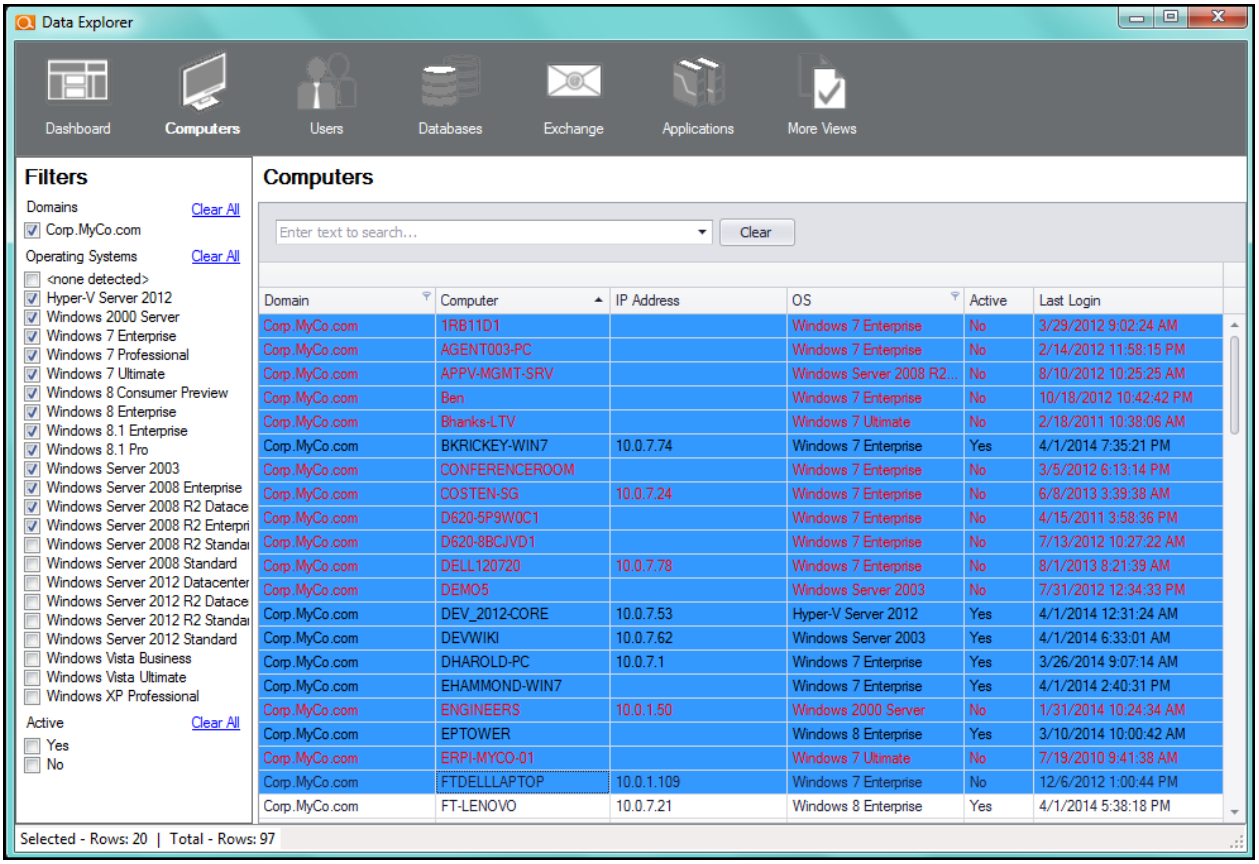
Step 1 – Filter the Network Assessment Scan Results Data in the Data Explorer Window

After opening Data Explorer, **Filter** the data using the **Filter** feature to create the scan data set that you would like to put into a custom report using Excel or Word.



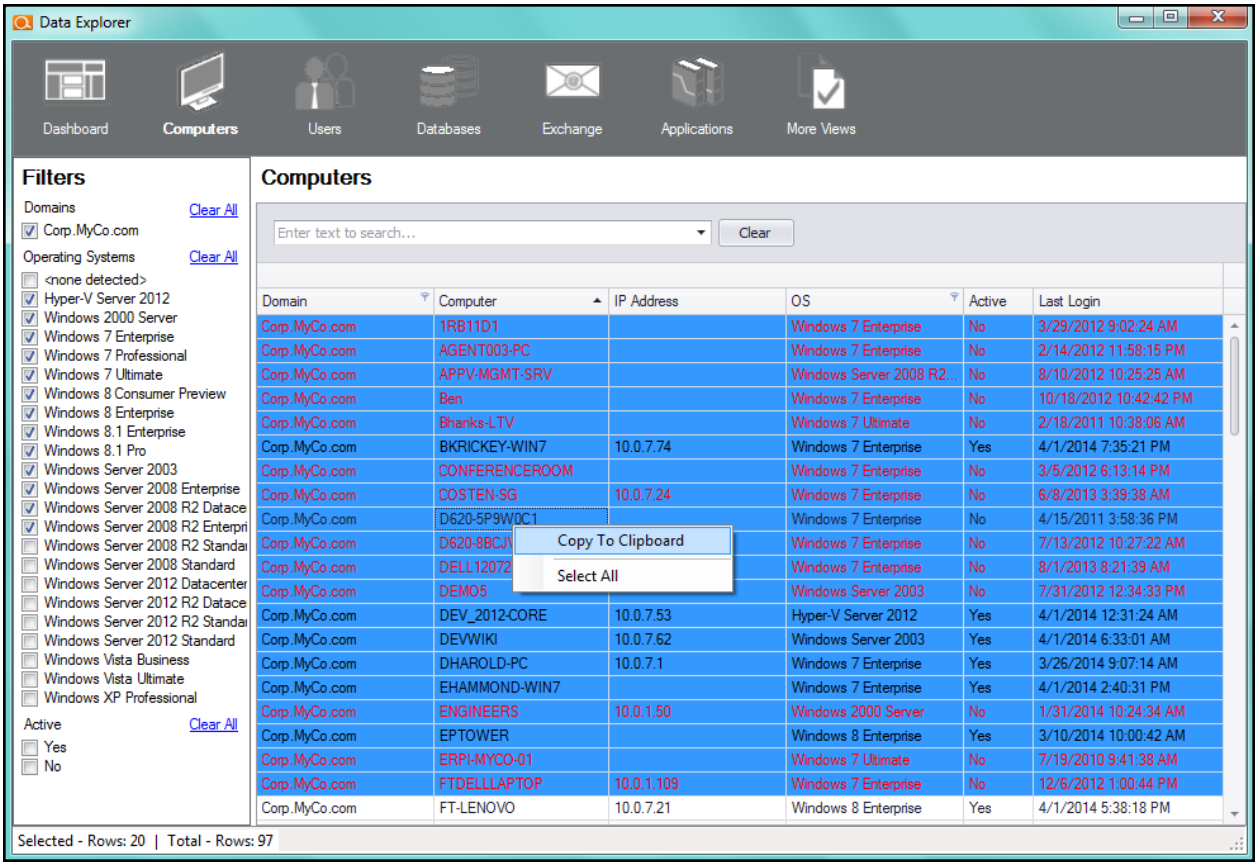
Step 2 – Select the Data to be Copied into Excel or Word

Next, select the rows of the filtered scan data that you would like to copy into a report.



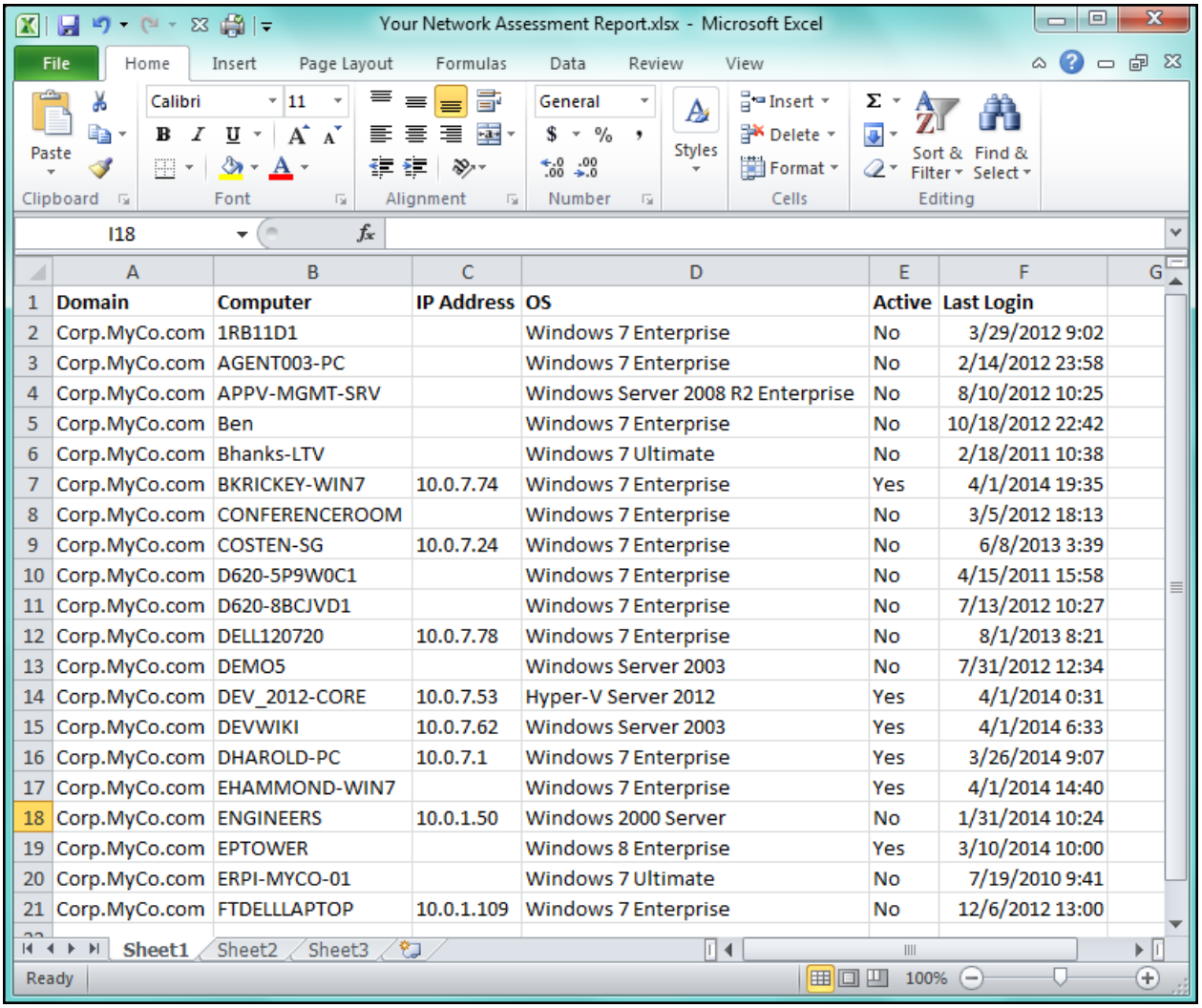
Step 3 – Copy the Selected Data

Right click on the selected data to activate the **Copy to Clipboard** menu. Then select **Copy to Clipboard** to copy the selected data to the **Clipboard**.



Step 4 – Paste the Data in Your Report

After starting Microsoft Excel or Word and creating a spreadsheet or document for your **Custom Report**, you can now paste the Filtered scan data into your report.



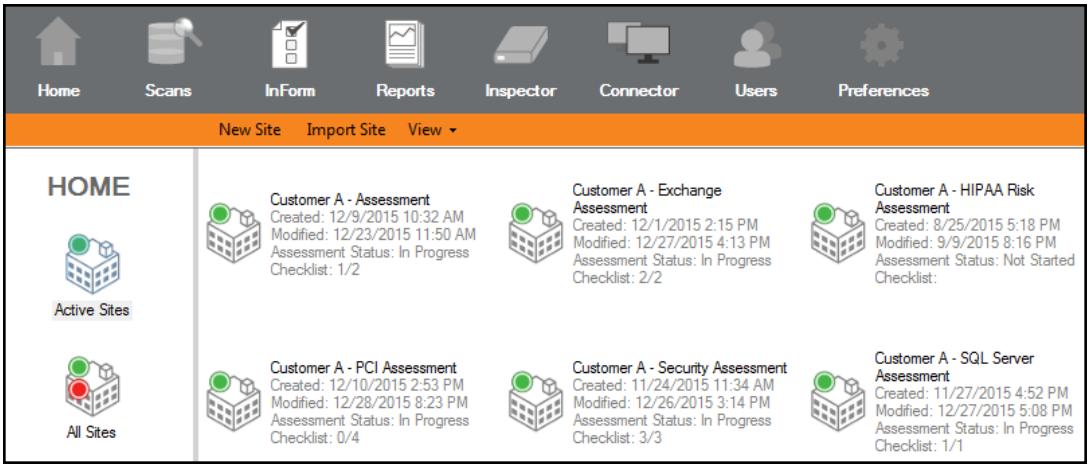
	A	B	C	D	E	F
1	Domain	Computer	IP Address	OS	Active	Last Login
2	Corp.MyCo.com	1RB11D1		Windows 7 Enterprise	No	3/29/2012 9:02
3	Corp.MyCo.com	AGENT003-PC		Windows 7 Enterprise	No	2/14/2012 23:58
4	Corp.MyCo.com	APPV-MGMT-SRV		Windows Server 2008 R2 Enterprise	No	8/10/2012 10:25
5	Corp.MyCo.com	Ben		Windows 7 Enterprise	No	10/18/2012 22:42
6	Corp.MyCo.com	Bhanks-LTV		Windows 7 Ultimate	No	2/18/2011 10:38
7	Corp.MyCo.com	BKRICKEY-WIN7	10.0.7.74	Windows 7 Enterprise	Yes	4/1/2014 19:35
8	Corp.MyCo.com	CONFERENCEROOM		Windows 7 Enterprise	No	3/5/2012 18:13
9	Corp.MyCo.com	COSTEN-SG	10.0.7.24	Windows 7 Enterprise	No	6/8/2013 3:39
10	Corp.MyCo.com	D620-5P9W0C1		Windows 7 Enterprise	No	4/15/2011 15:58
11	Corp.MyCo.com	D620-8BCJVD1		Windows 7 Enterprise	No	7/13/2012 10:27
12	Corp.MyCo.com	DELL120720	10.0.7.78	Windows 7 Enterprise	No	8/1/2013 8:21
13	Corp.MyCo.com	DEMO5		Windows Server 2003	No	7/31/2012 12:34
14	Corp.MyCo.com	DEV_2012-CORE	10.0.7.53	Hyper-V Server 2012	Yes	4/1/2014 0:31
15	Corp.MyCo.com	DEVWIKI	10.0.7.62	Windows Server 2003	Yes	4/1/2014 6:33
16	Corp.MyCo.com	DHAROLD-PC	10.0.7.1	Windows 7 Enterprise	Yes	3/26/2014 9:07
17	Corp.MyCo.com	EHAMMOND-WIN7		Windows 7 Enterprise	Yes	4/1/2014 14:40
18	Corp.MyCo.com	ENGINEERS	10.0.1.50	Windows 2000 Server	No	1/31/2014 10:24
19	Corp.MyCo.com	EPTOWER		Windows 8 Enterprise	Yes	3/10/2014 10:00
20	Corp.MyCo.com	ERPI-MYCO-01		Windows 7 Ultimate	No	7/19/2010 9:41
21	Corp.MyCo.com	FTDELLLAPTOP	10.0.1.109	Windows 7 Enterprise	No	12/6/2012 13:00

Enhancing Assessments by Adding an InForm Sheet to an Assessment Process

InForm surveys can be a valuable addition to **Site Assessments**. Information collected by a tech on-site or entered manually into a survey or worksheet template built using **InForm** will enable the tech to collect additional information during an assessment that can be compiled into the Network Detective Reports.

For more information, please review the section of this User Guide entitled "Using InForm to Build Questionnaire Worksheet and Survey Templates for Enhanced Assessment Data Collection" on page 235.

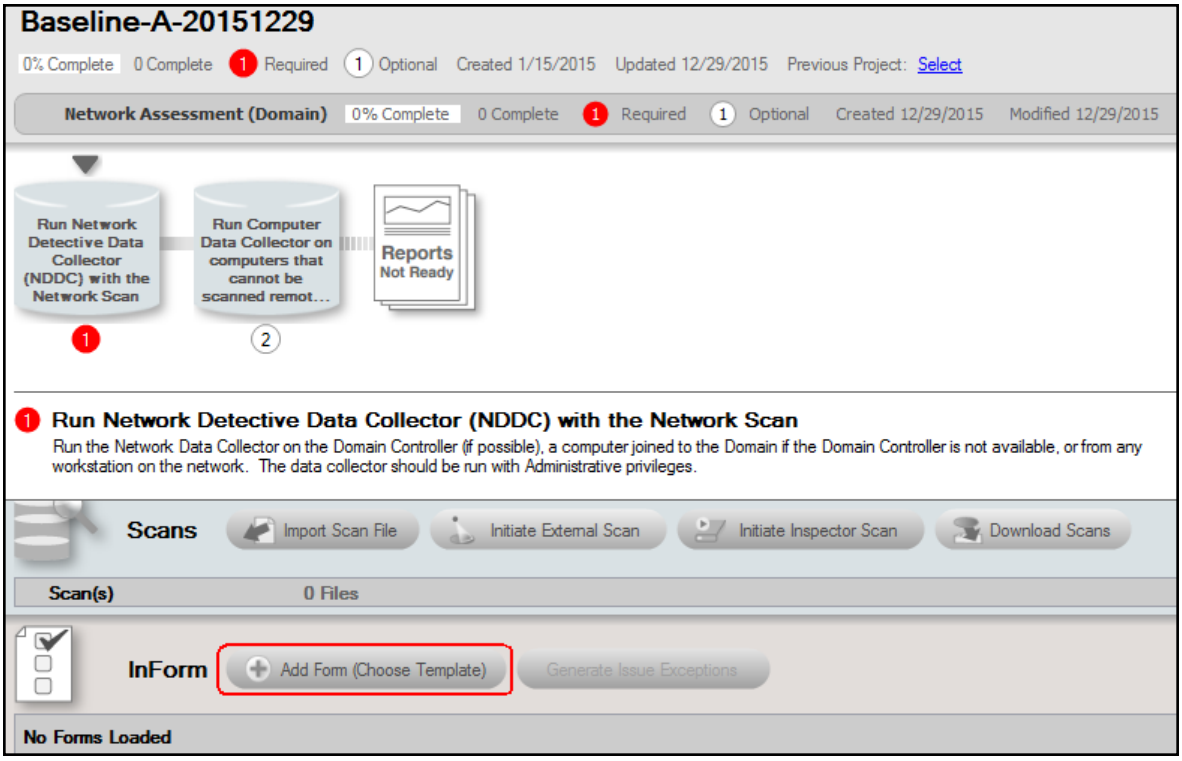
The Site Model allows you to create and edit InForm sheets from within the Assessment.



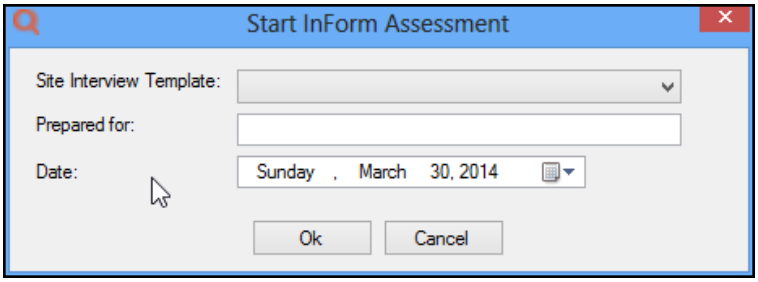
To add an **InForm** sheet to your **Assessment Project**, first navigate to the desired **Site** from the Home screen by double-clicking on its icon.

This will bring you to the Dashboard of the Site's current Assessment.

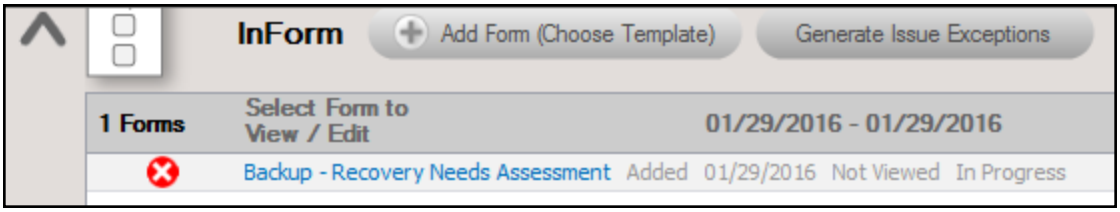
From the Assessment's Dashboard, select "**Add Form**" under the **InForm** bar.



Using the **Start InForm Assessment** dialog box, select your template, type in the name of your customer in the "Prepared for" field, and click "Ok."



The new template will be listed under the **InForm** bar. Click the Inform template name that is in Blue text link to open and use your template.



Performing Network Assessments Required to Generate Change Reports and Quarterly Business Review Reports

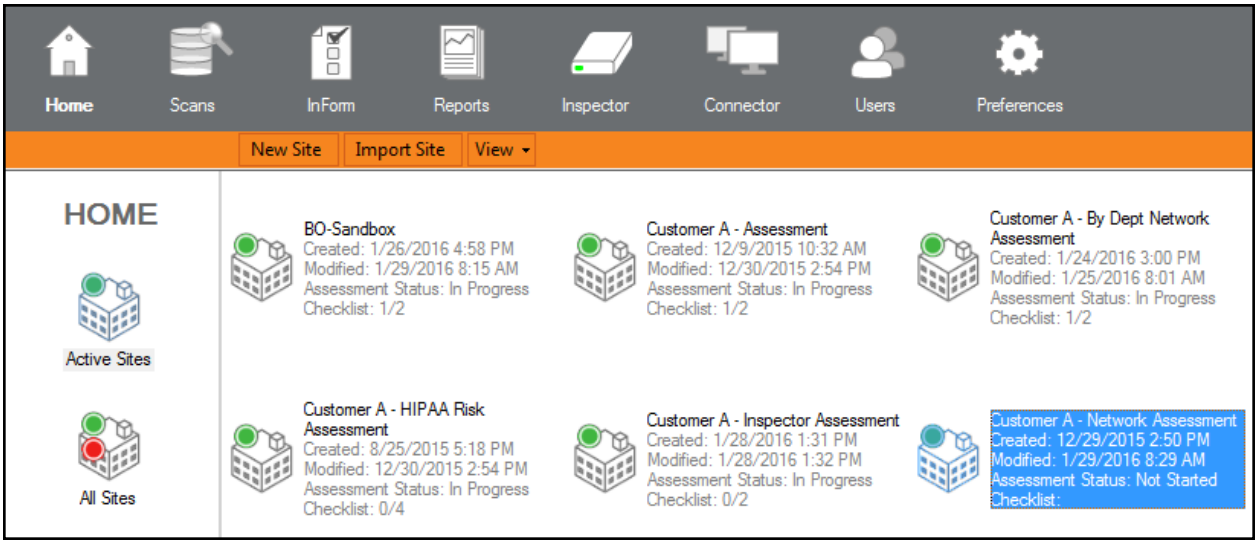
In order to use Network Detective to generate Network Assessment Change Reports and Quarterly Business Review reports it is necessary to **compare a past Network Assessment (i.e. Baseline Assessment) with the second (a new or more recent) Network Assessment**.

Based on the content presented in Change Reports and Quarterly Business Review reports, two assessments are required in order to identify changes to the network over the time period that took place between the two network assessments.

The steps to create a Network Assessment that enables the generation of Change and Quarterly Business Review reports are below.

Step 1 – Select and Open a Site that Contains a Completed and Archived Network Assessment Project

Open the **Site** containing an **Archived Network Assessment** by double clicking on the **Site**.

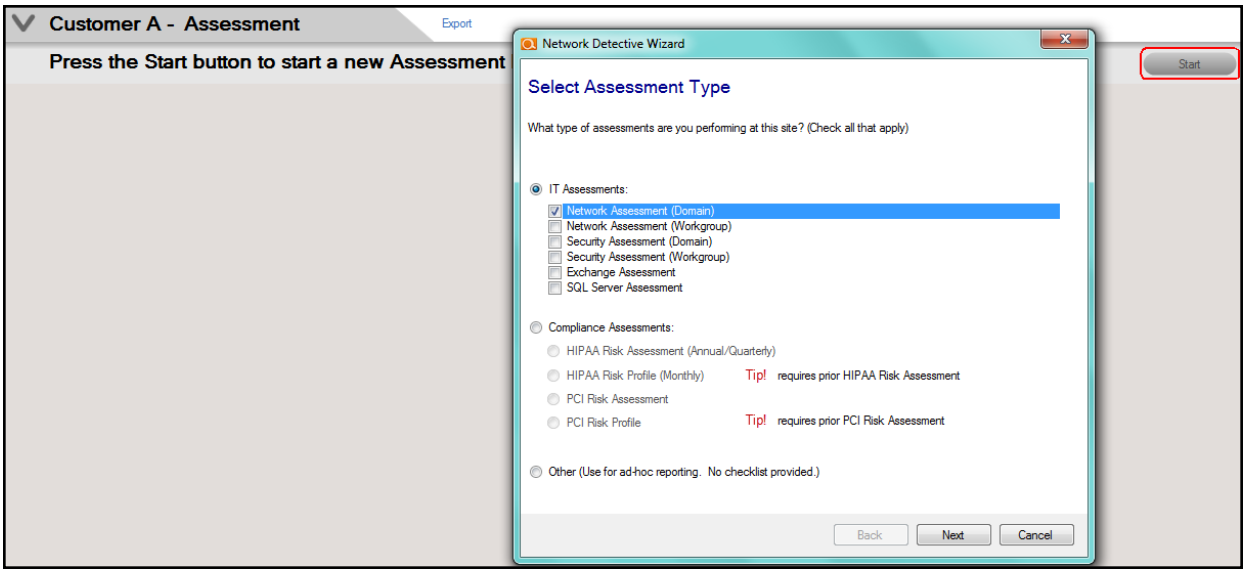


The **Start New Assessment** window will be displayed.

Step 2 – Create a new Network Assessment Project

If you already have a second Network Assessment Project to compare to the first "baseline" Network Assessment Project, then skip this step and go to step 3 below. If not, then proceed with Step 2 by performing the following actions.

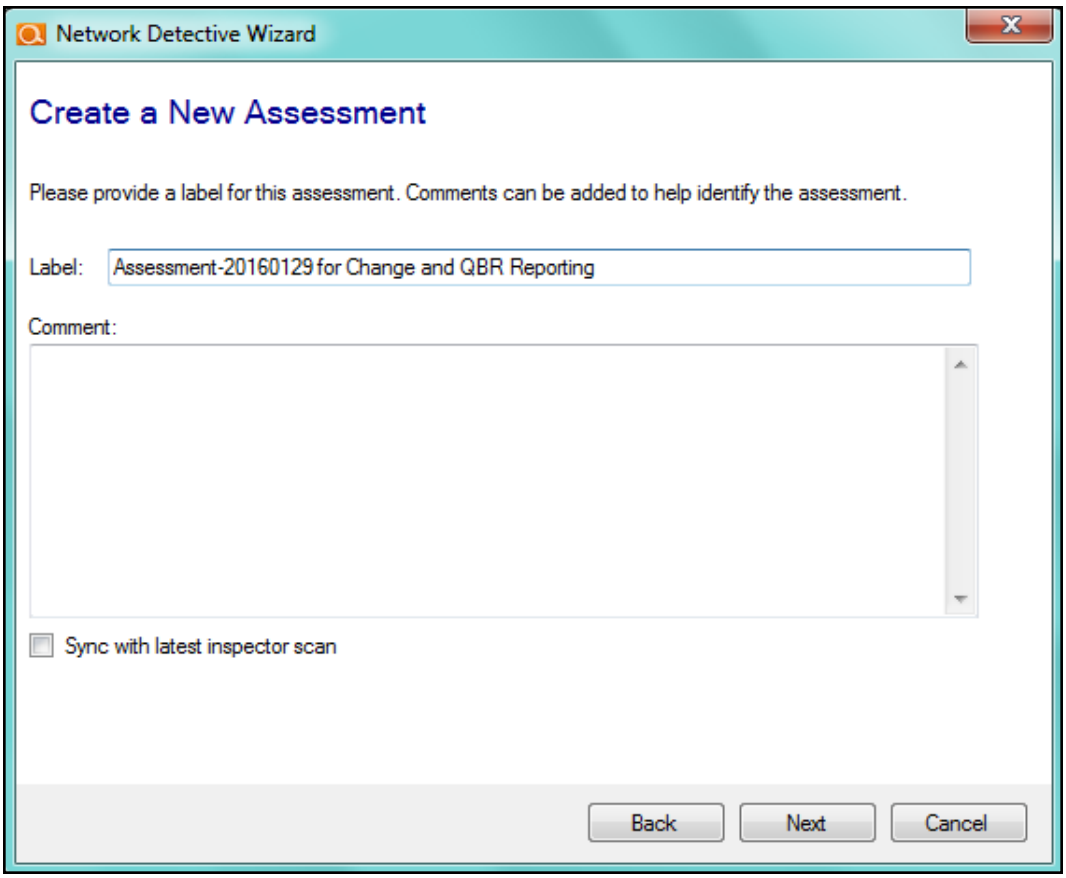
From the **Site's Dashboard**, click the "**Start**" button on the "**Active Assessment**" bar to start an **Assessment**.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more **Assessment Types**.

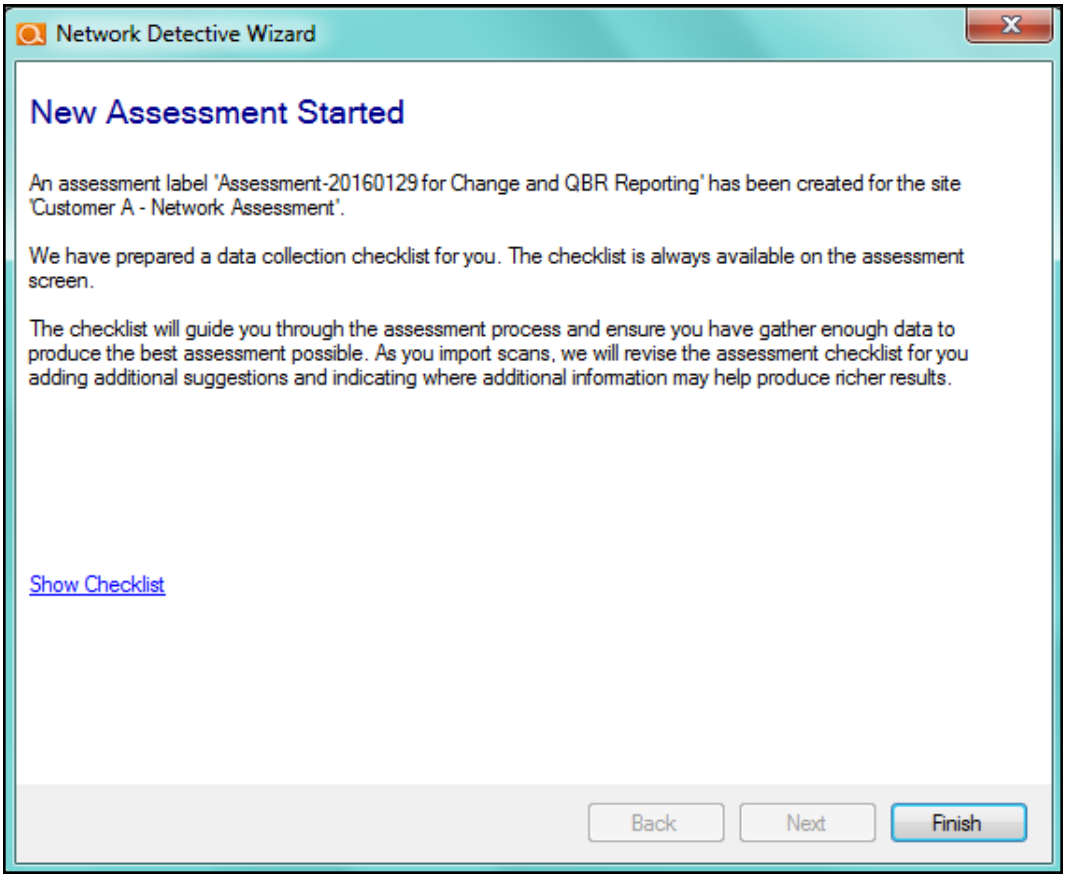
To create a Network Assessment Project, select the **Network Assessment** option and click on the **Next** button.



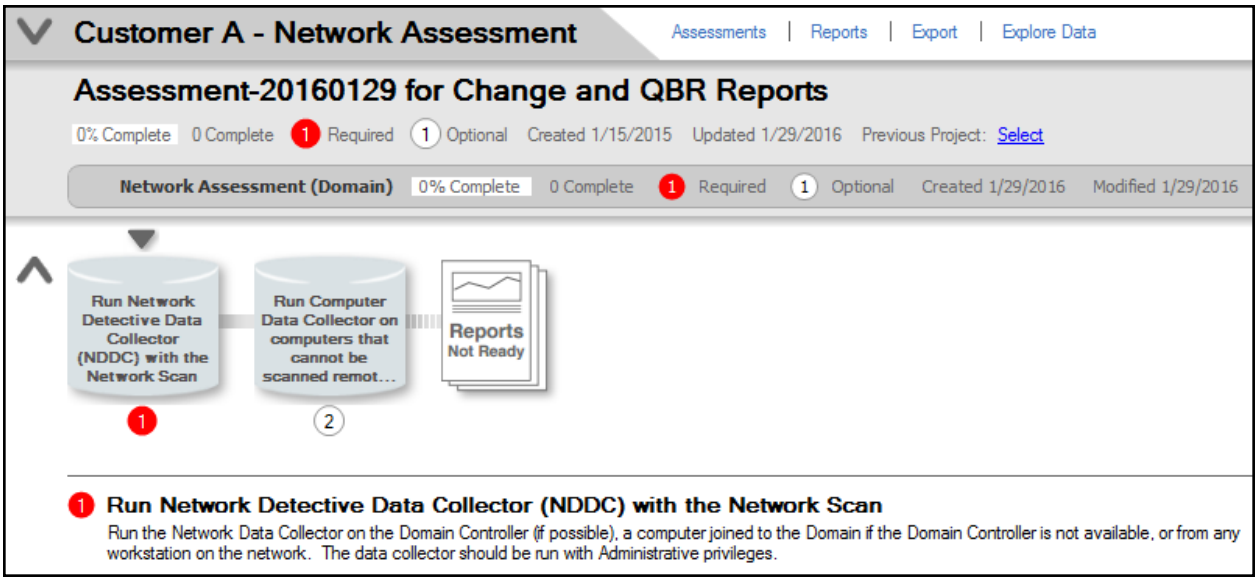
Enter a **Label** to identify the assessment.

Enter a **Comment** to help further identify the assessment.

Select the **Next** button to proceed to create/start the new assessment project.

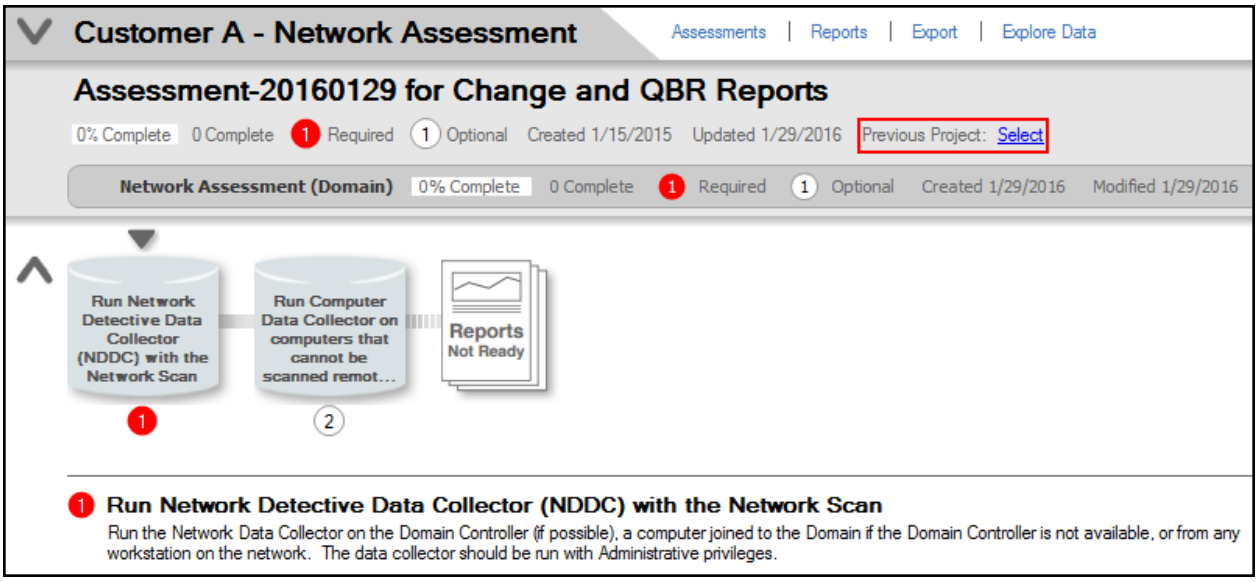


The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment** as displayed below.

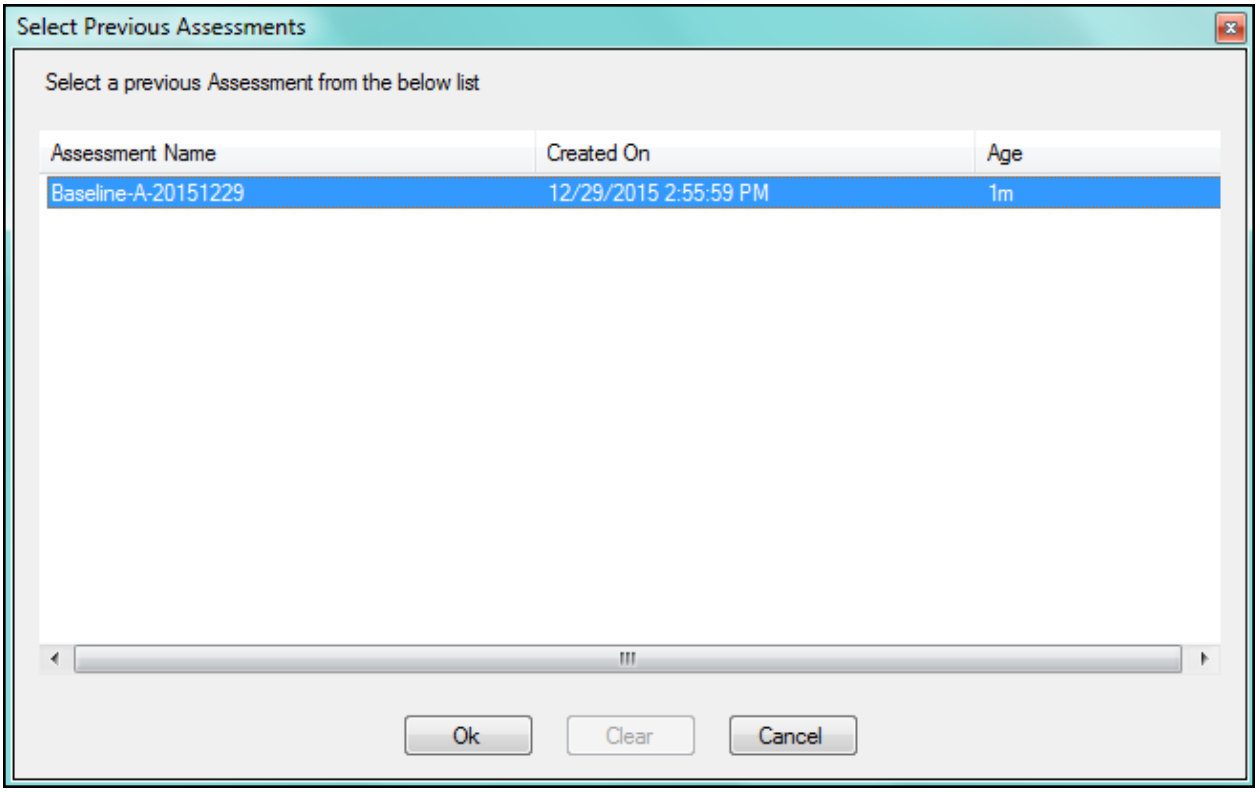


Step 3 – Select and Link a Previously Completed Network Assessment Project to the New Assessment Project for Comparison

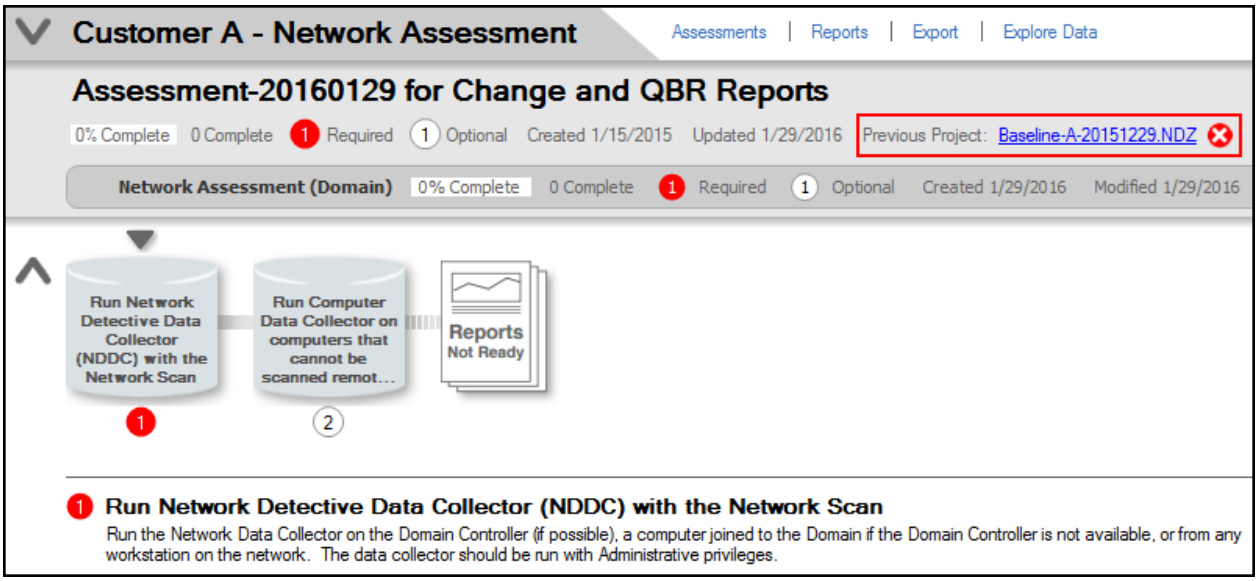
From within an **Active Assessment**, select the **Previous Project** link in order to select the previously completed **Network Assessment** from the **Archived**assessments associated with this **Site**.



This action will present the **Select Previous Assessments** window.



Select the previous **Assessment** from the list of assessments and click on the OK button to link the previous **Assessment** to the current **Assessment** for comparison and **Change Reporting** purposes.



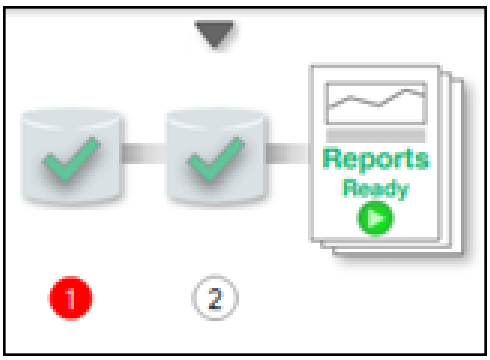
Step 4 – Perform Network and Local Computer Scans and Import Scan Data into the New Assessment Project

Based on the **Checklist**, perform the same Network and Local Computer scans that were performed in the **Previous Assessment Project** and import the scan data into this new **Network Assessment**.

These scans should include the:

- **Network Scan** Using the **Network Assessment Data Collector**
- **Scans on Local Computers** using the **Push Deploy Tool**
- **Local Computer Scans** using the **Computer Data Collector** for unreachable computers

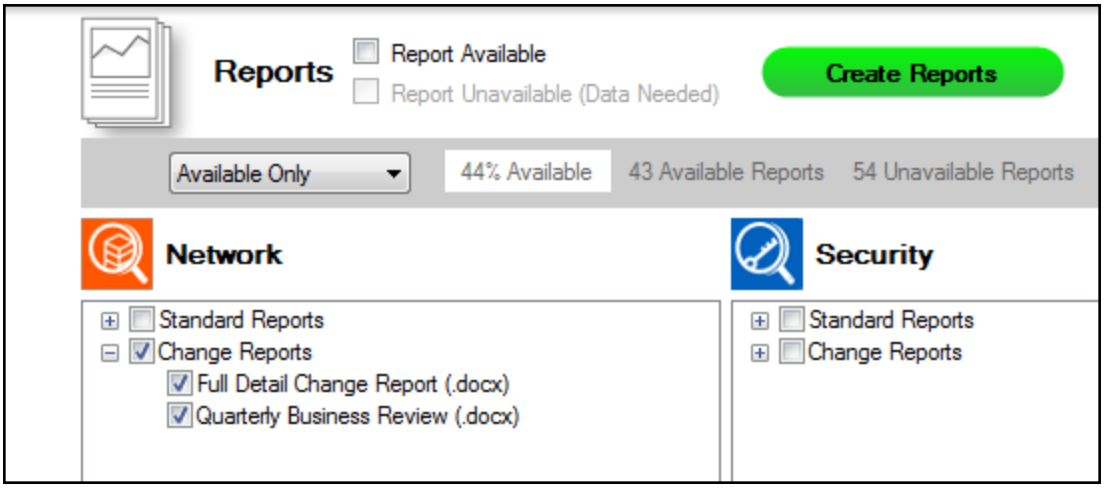
Once these scans are imported into the new **Network Assessment** the **Checklist** will indicate the **Reports** are ready to be generated.



Step 5 – Generate the Change Reports

Select the Reports link in the **Network Assessment** window to generate reports. This action will display the **Create Reports** window.

In the **Create Reports Window**, select the **Change Reports** you wish to generate by selecting the **Full Detail Change Report** and/or the **Quarterly Business Review Report**.



Then select the **Create Reports** button to produce the reports you have selected.

Performing a Security Assessment

To perform a Security Assessment, complete the four phases detailed in this guide.

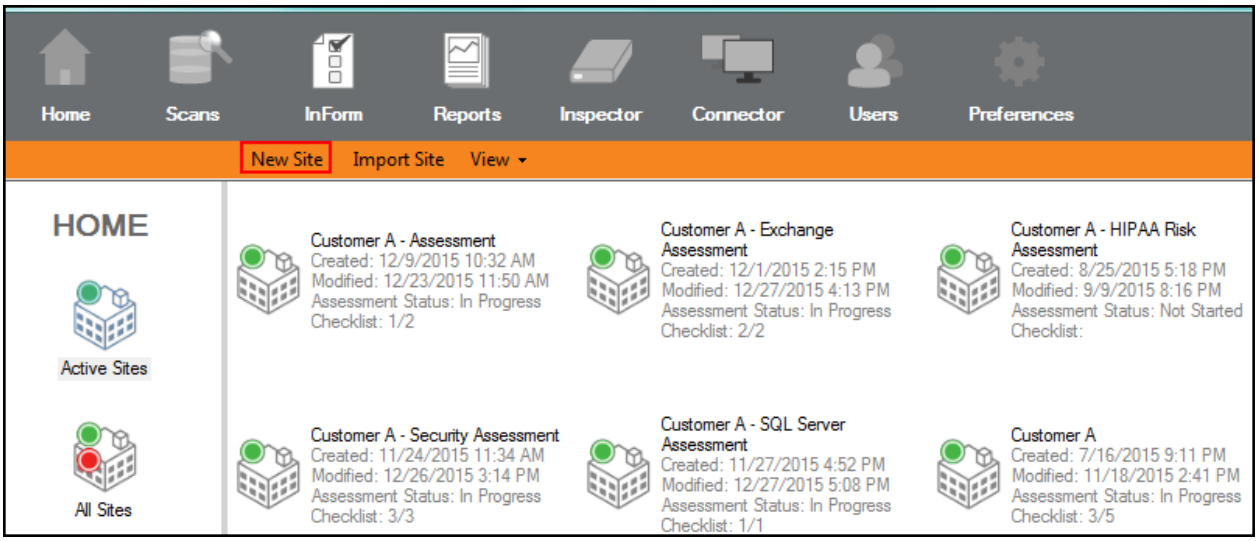
Phase 1 – Initial Security Assessment Project Setup

Creating a Site

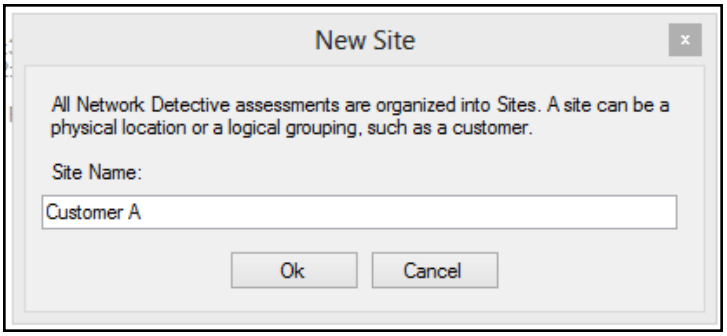
The first step in the assessment is creating a **"Site"**. All Network Detective assessment projects are organized into Sites. A **Site** can be a physical location or a logical grouping, such as a customer account name.

a. For a single location you will create one **Site**.

b. For organizations with multiple locations you must decide if you want one set of reports, or separate reports for each location.



Select **New Site**.



Enter the **Site Name**. For sites with multiple locations, enter a more detailed description.

Setting Report Branding for a Site

Reports produced by Network Detective can be “branded” with your company’s standards through the use of the **Reports Preference**s feature. Report Branding can be set at the **Global Level** (for all Sites), or at the **Site Level**. If you want to set the **Report Preferences** at the **Site Level**, please go to "Set Up Network Detective Reports" on page 16.

Adding a Connector to a Site

To add a Connector to a **Site**, please go to "Adding a Connector to a Site" on page 255.

> **Note:** Also see the Network Detective Remote Data Collector User Guide.

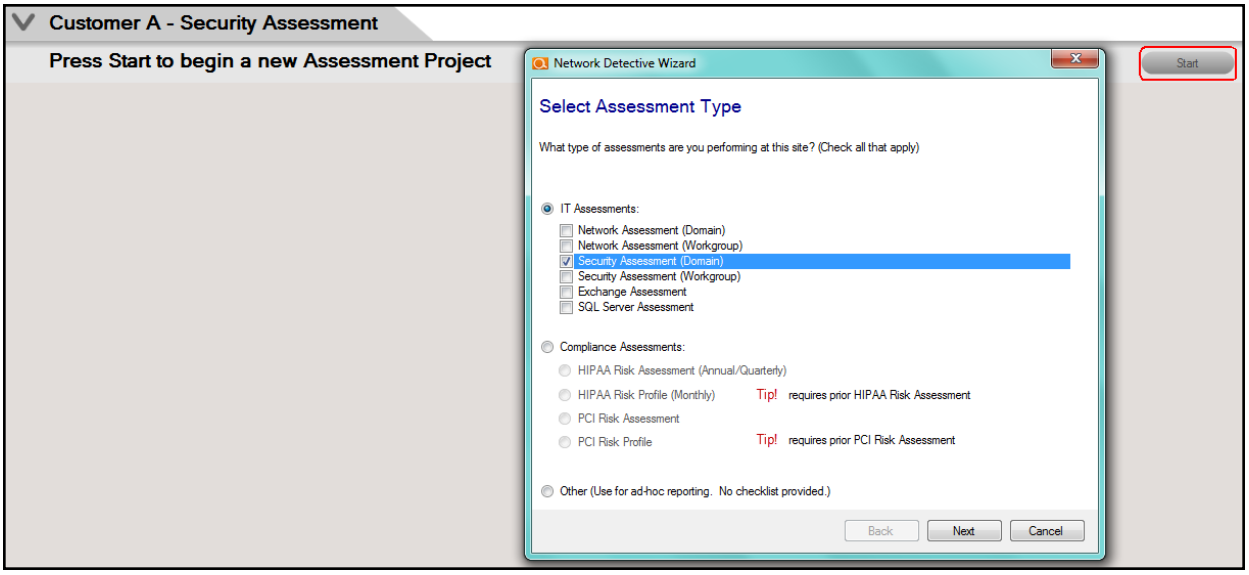
Adding an Inspector to a Site

To add an Inspector to a **Site**, please go to "Adding an Inspector to a Site" on page 257.

Phase 2 – Starting a Security Assessment Project

Starting a Security Assessment Project

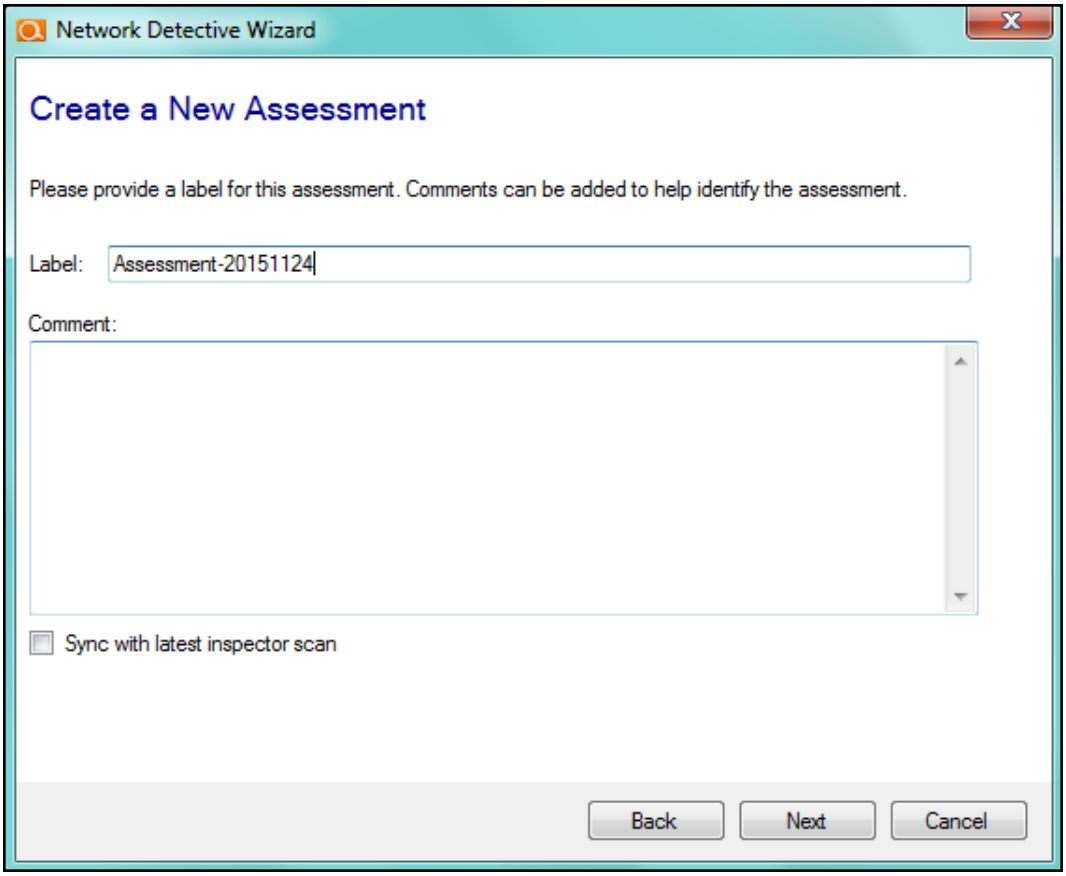
From the Site's Dashboard, click the "**Start**" button on the "**Assessment**" bar to start an Assessment project.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more Assessment Types.

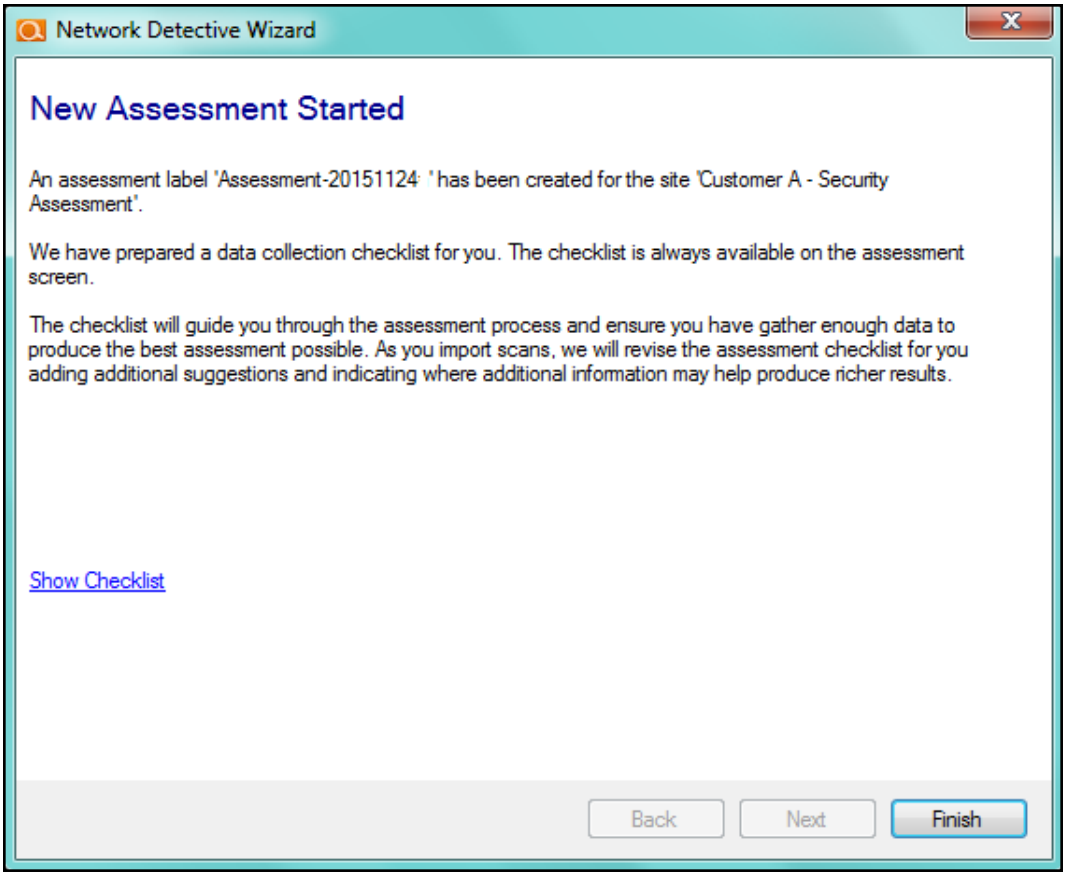
To create a Security Assessment project, select the Security Assessment option and click on the **Next** button.



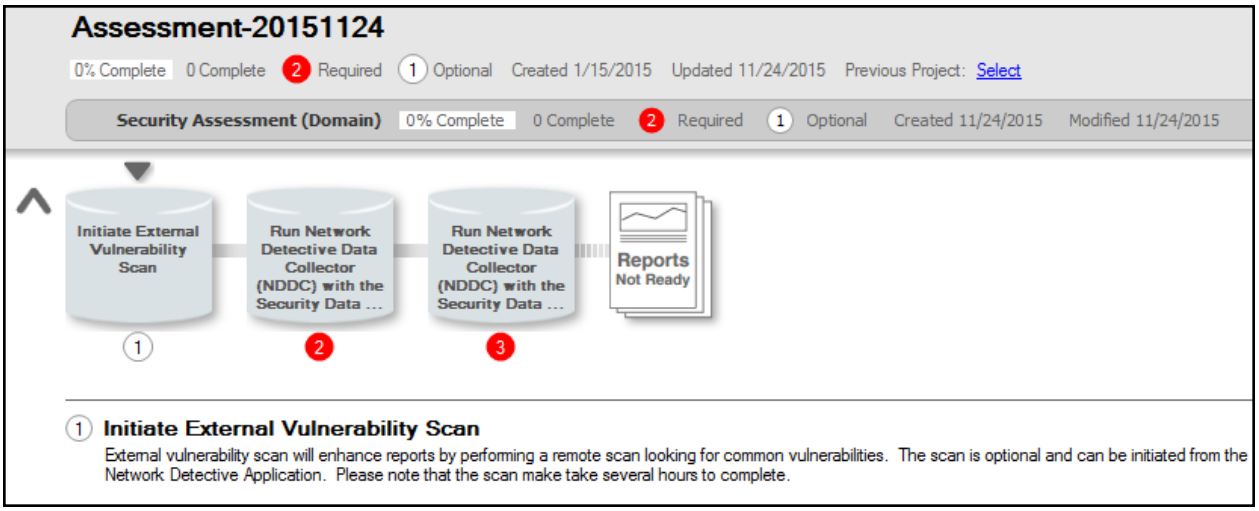
Enter a **Label** to identify the assessment.

Enter a **Comment** to help further identify the assessment.

Select the **Next** button to proceed to create/start the new assessment.



The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment**.



Planning the On-site Data Collection

There are various ways to collect data for a Security Assessment. These methods can vary based on time, cost, client expectation, level of detail needed to identify remediation needs, etc.

Initial Assessment

Types of collections:

Security Assessment

- Quick Assessment
  - Security Scan of the Network + Security Scans on Local Computers for 1-3 computers
- Full Assessment
  - Security Scan of Network + Security Scans on Local Computer Scans for all computers

Scans Performed During the Security Assessment Process

The Initial Data Collection phase of the Security Assessment consists of the following required and optional scans:

- **Security Scan of the Network** Using the **Network Assessment Data Collector**
- **Security Scans on Local Computers** using the **Push Deploy Tool**
- **Security Scans on Local Computers** on the unreachable computers using the **Network Assessment Data Collector's Security Data Collector** scan option

> **Note:** In order to complete this item within the Checklist, run Security Scans on two or more local computers.

The Security Assessment Data Collector scans make 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

See also: "Pre-Scan Network Configuration Checklist" on page 249.

Optional Local Scanning of Unreachable Computers and the Optional Internal Network Vulnerability Scan

Throughout the assessment process, "**Optional**" scans may need to be undertaken based on the availability of servers and workstations during automated and network scans, based on a need to sample scan machines outside of the network that you are assessing, or based on the need to more thoroughly scan for internal network vulnerabilities.

These scans would include:

Optional Scan Type	Description
Run Network Assessment Data Collector using the Security Data Collector scan option to perform a security can on local Computers that were unreachable *Refer to* "Task 4: Run the Network Assessment Data Collector selecting the Security Collector Scan on the Computers that were Unreachable during Security Assessment Push Deploy Tool Scanning (OPTIONAL)" on page 146	Run the "Local" Security Scan on any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible). Using the Network Assessment Data Collector to Run the Security Scan directly on the computer itself.
Internal Vulnerability Scan (requires Inspector) *(Refer to the Inspector User Guide for instructions on how to run this scan)*	An Inspector initiated scan that checks for Open Ports and Protocol Vulnerabilities that could be exploited ONCE a hacker is in your network – or by employees. Essentially "INSIDE attacking INSIDE". This scan complements the external vulnerability scan performed with the Security,

Optional Scan Type	Description
	HIPAA, and PCI modules, which finds weaknesses at the network “edge” that could be exploited by external sources.

Phase 3 – Performing the Assessment and Data Collection

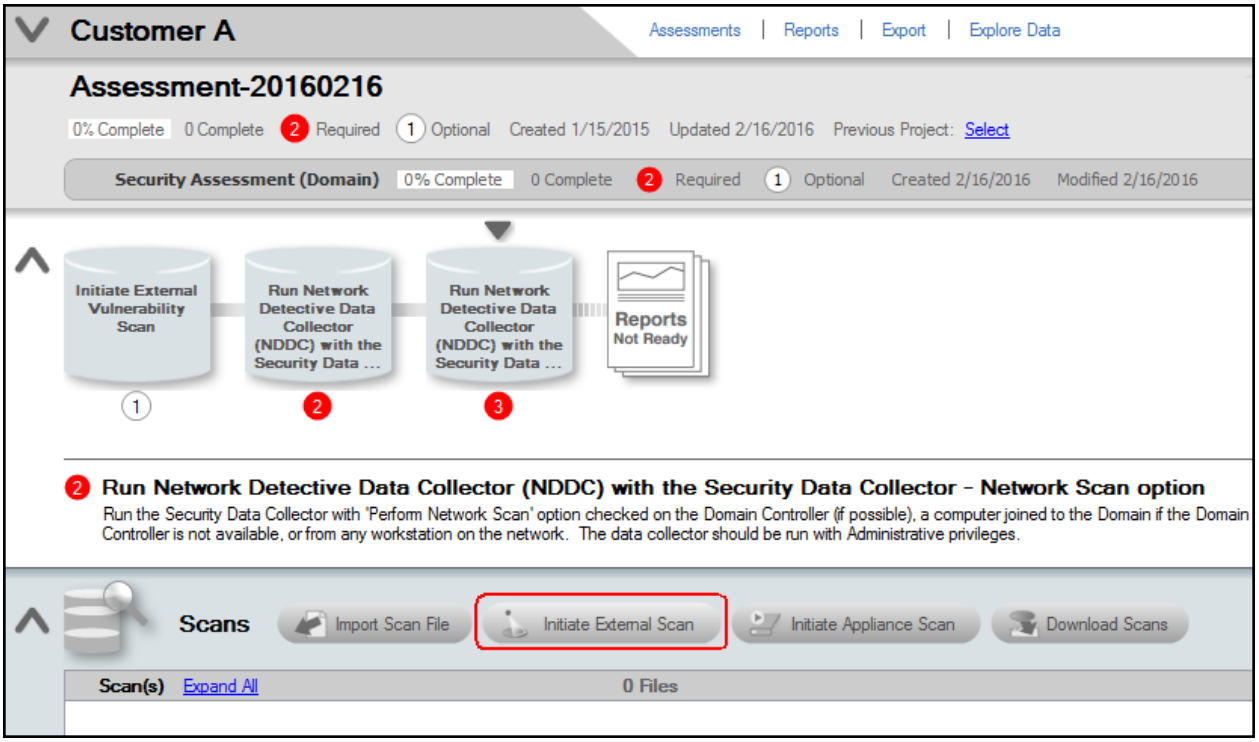
To perform the Security Assessment and the associated Data Collections, the following tasks must be performed:

- "Task 1: Initiate the External Vulnerability Scan (Optional)" below
- "Task 2: Initiate the Network Scan Using the Network Detective Data Collector and Import Scan Results" on page 118
- "Task 3: Use the Push Deploy Tool to Collect Remaining Data and Import Scan Results" on page 135
- "Task 4: Run the Network Assessment Data Collector selecting the Security Collector Scan on the Computers that were Unreachable during Security Assessment Push Deploy Tool Scanning (OPTIONAL)" on page 146
- "Task 5: Document Exceptions" on page 156

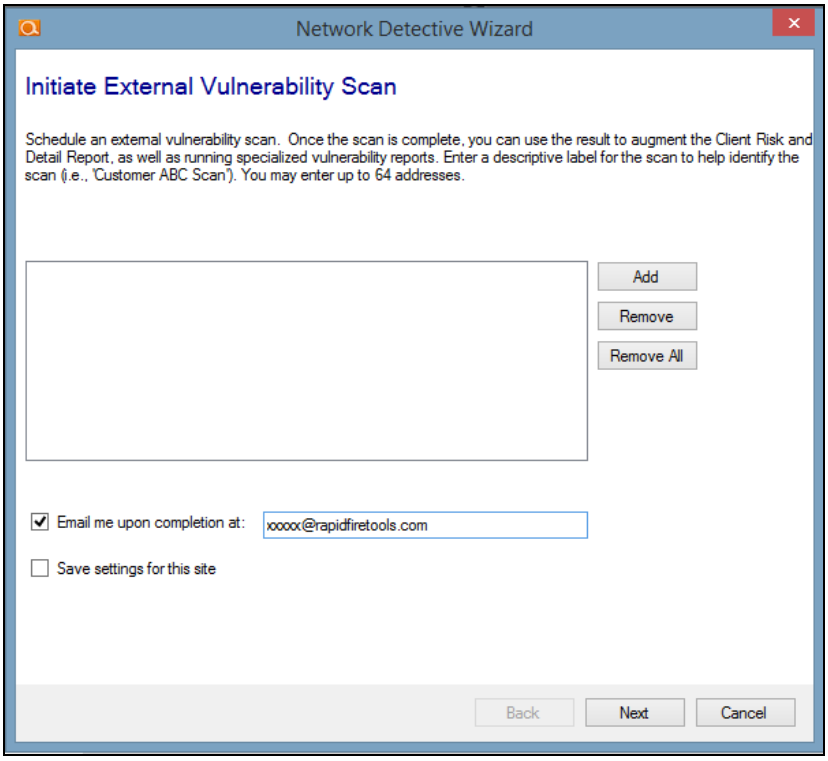
Task 1: Initiate the External Vulnerability Scan (Optional)

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

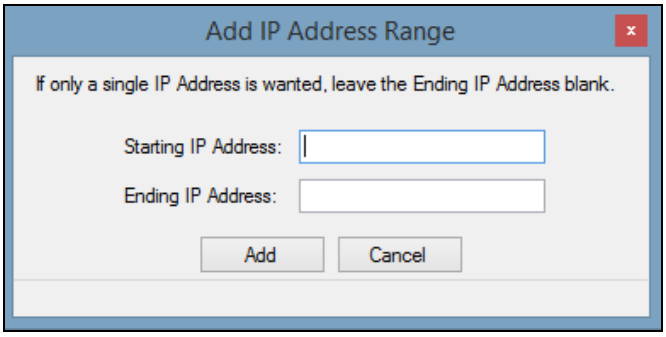
Select **Initiate External Scan** button to start an **External Vulnerability Scan**.



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

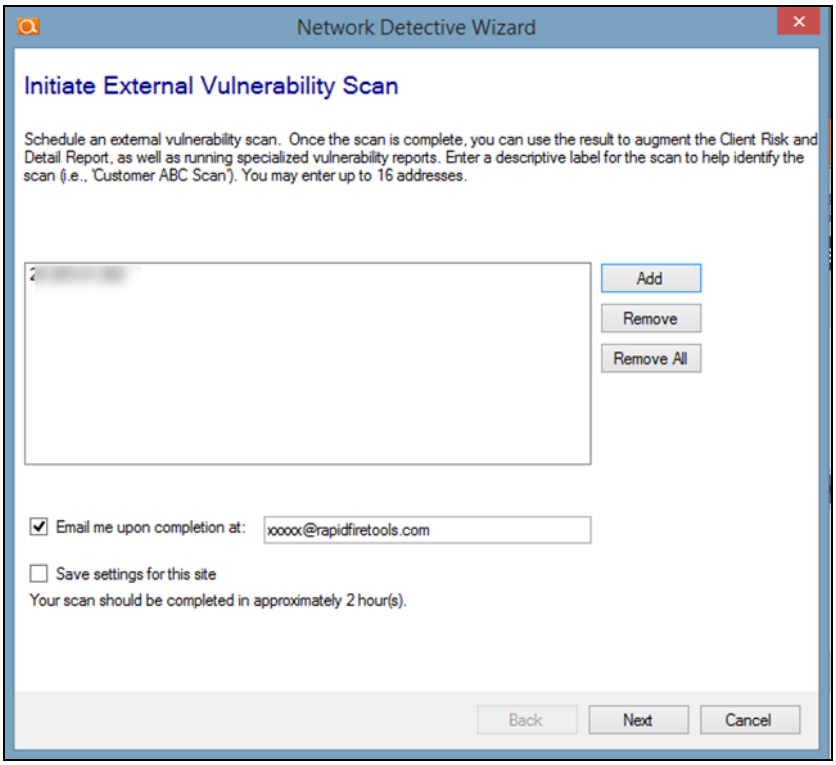


Select **Add** to add a range of external IP addresses to the scan. If you do not know the external range, you can use websites such as whatismyip.com to determine the external IP address of a customer.



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

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

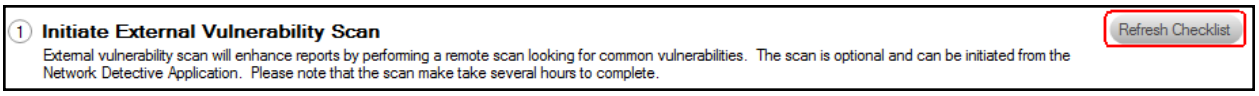


In the **Initiate External Vulnerability Scan** window, enter an email address to be notified when the scan is completed.

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

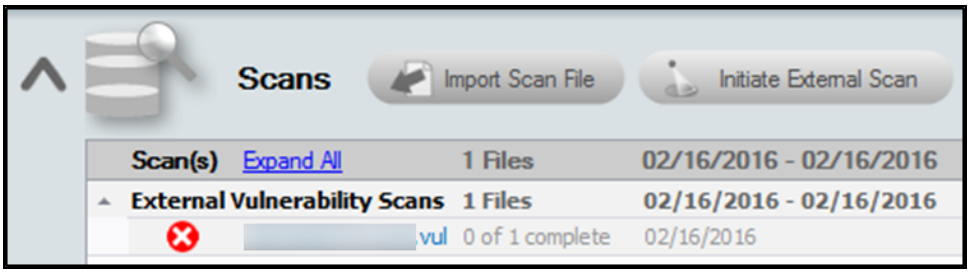
Scans can take several hours to complete. You will receive an e-mail when the External Vulnerability Scan is complete.

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



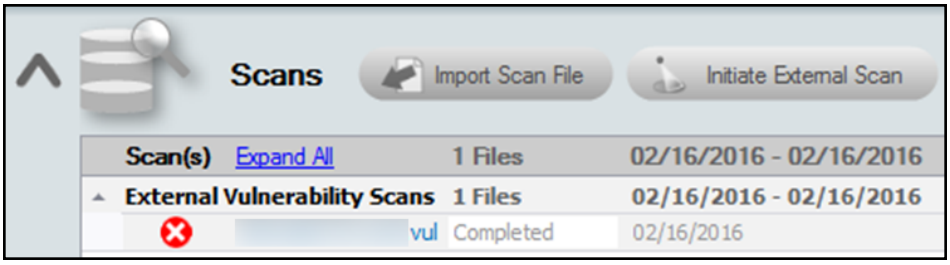
The **Assessment Window** and associated **Scans** listed under the **Scans** bar at the bottom of the **Assessment Window** will be updated to reflect the External Vulnerability Scan has been initiated and its completion is pending.

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



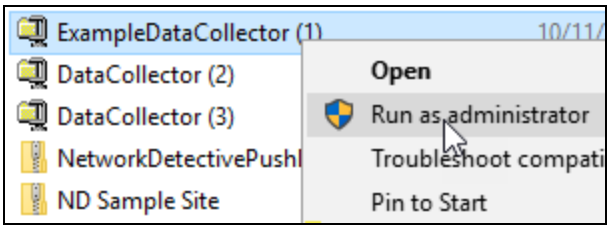
The scan's **pending** status of **"0 of 1 complete"** will be updated to **"Completed"** once the scan is completed. An email message stating that "the scan is complete" will also be sent to the person's email address that was specified when the scan was set up to be performed.

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



Task 2: Initiate the Network Scan Using the Network Detective Data Collector and Import Scan Results

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

1. Visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the Network Detective Data Collector.
2. Run the **Network Detective Data Collector** executable program as an Administrator (**right click>Run as administrator**).
3. 

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

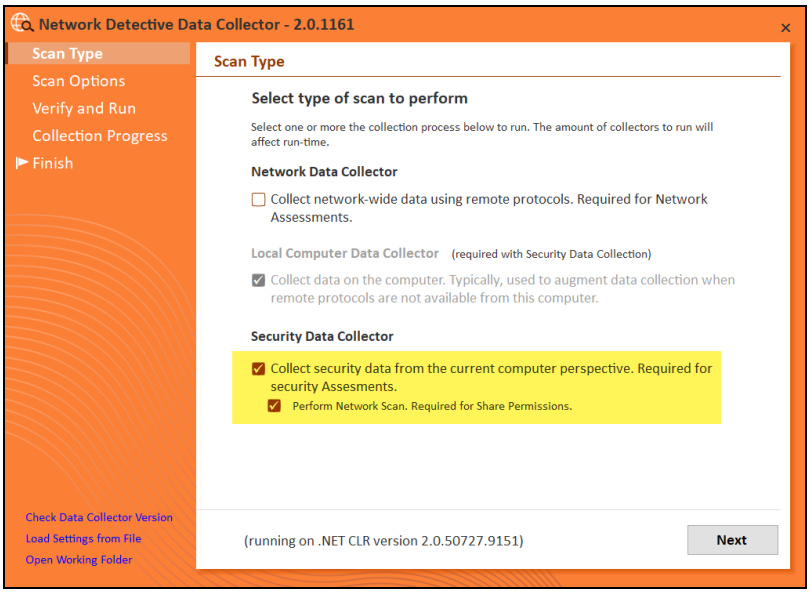
4. **Unzip** the files into a temporary location. The Network Detective Data Collector's self-extracting ZIP file does not install itself on the client computer.
5. The Network Detective Data Collector Scan Type window will appear.

Configure the network scan using the wizard.

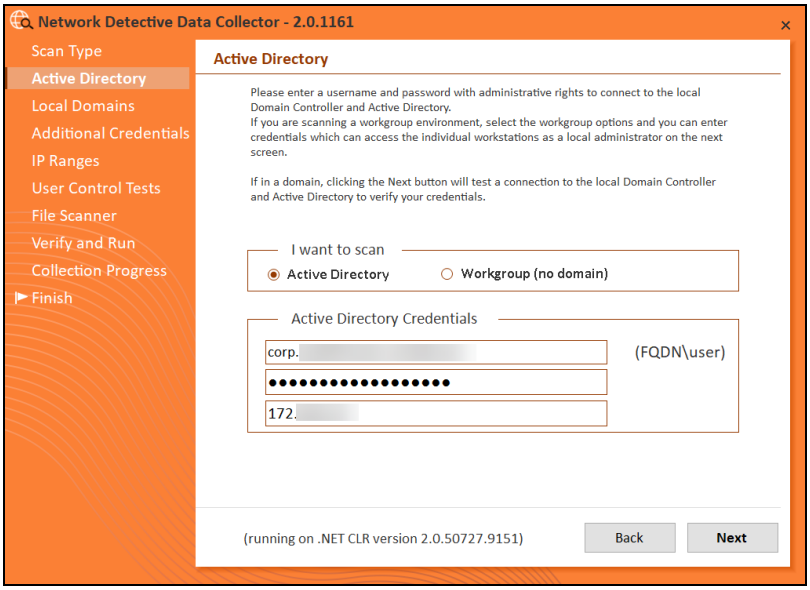
- Look here if you are "Scanning an Active Directory Domain-based Network" on the next page
- Look here if you are "Scanning a Workgroup Network" on page 125

Scanning an Active Directory Domain-based Network

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



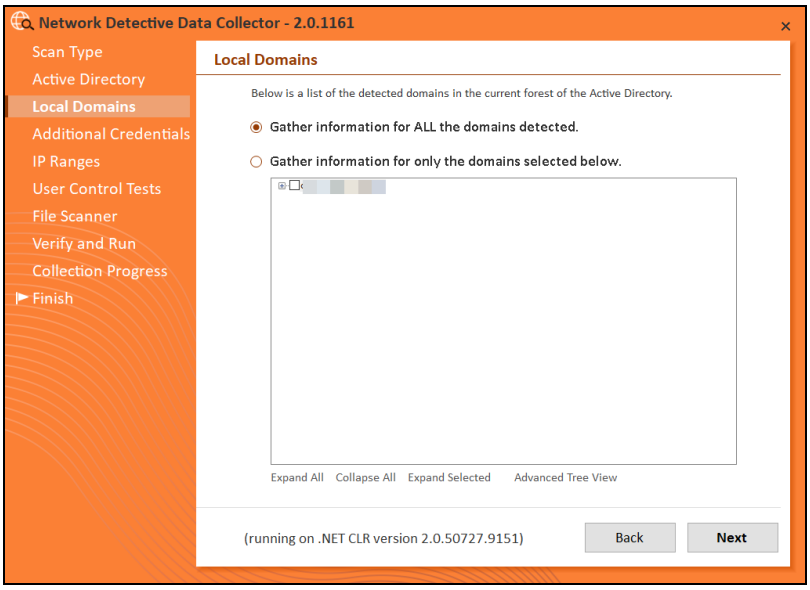
1. The **Active Directory** window will appear. Select the type of network you are scanning (*Active Directory domain*).



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

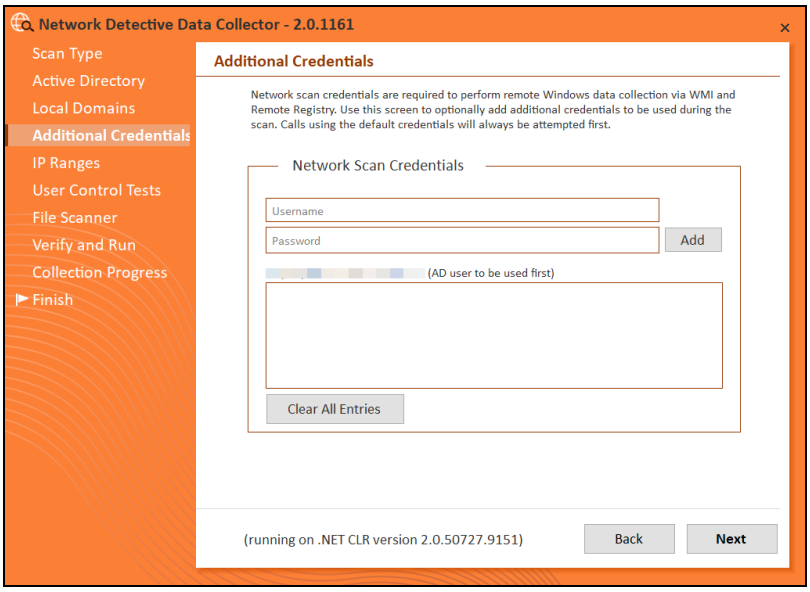
> **Note:** For example: **corp.yourprospect.com\username.**

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

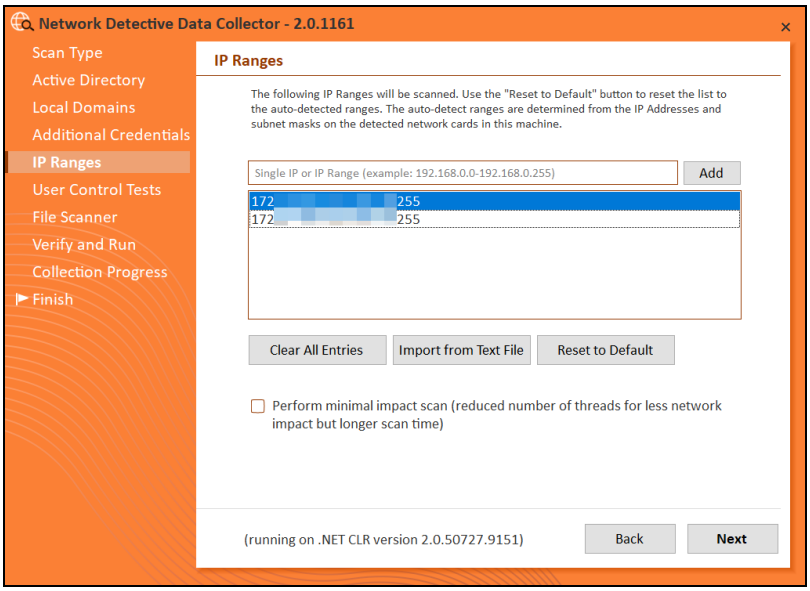


Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

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



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

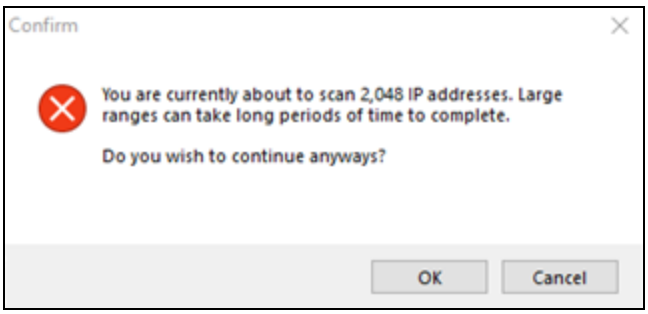


From this screen you can also:

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

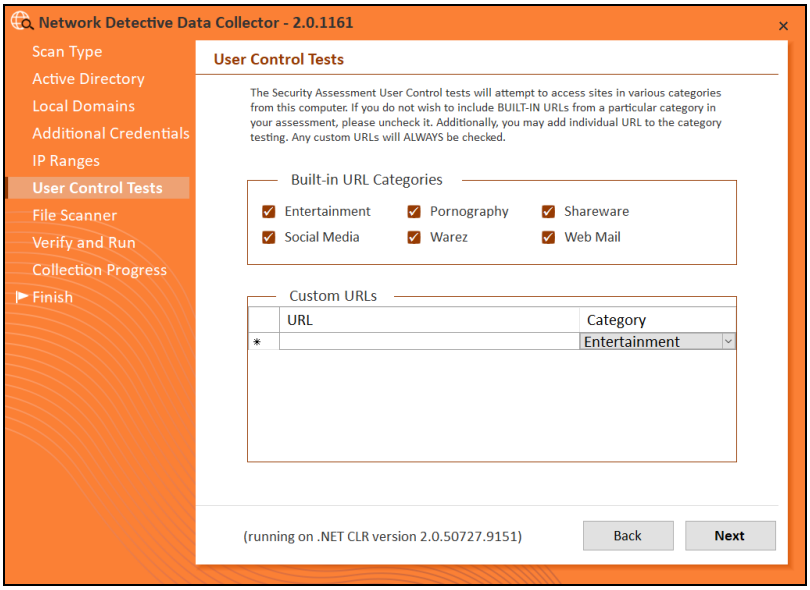
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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

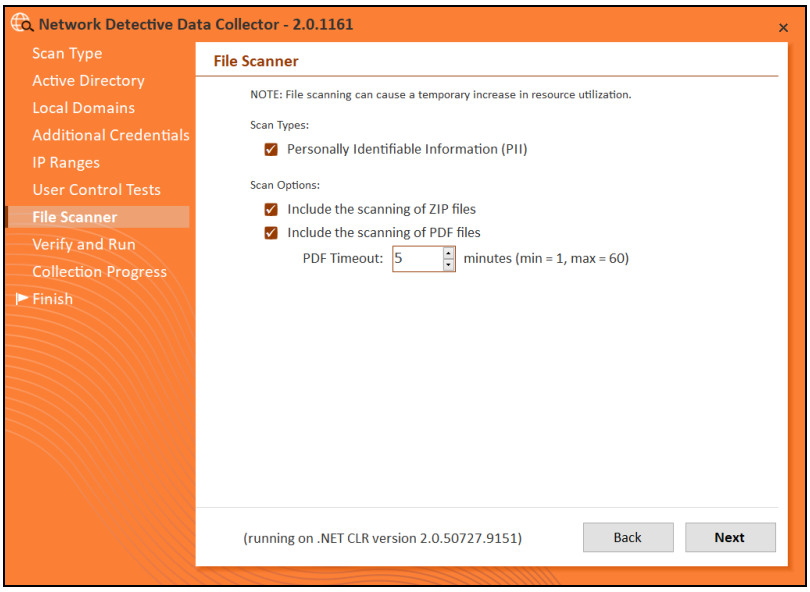


Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

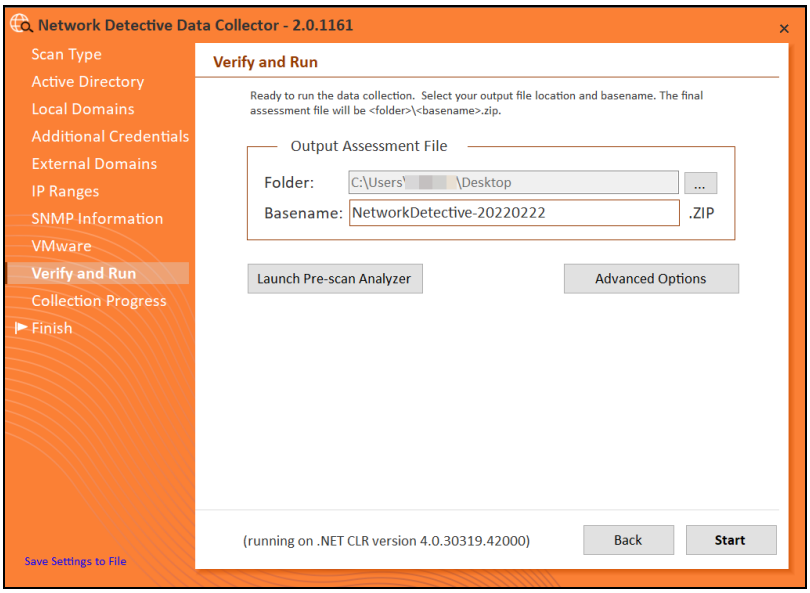
8. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your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



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

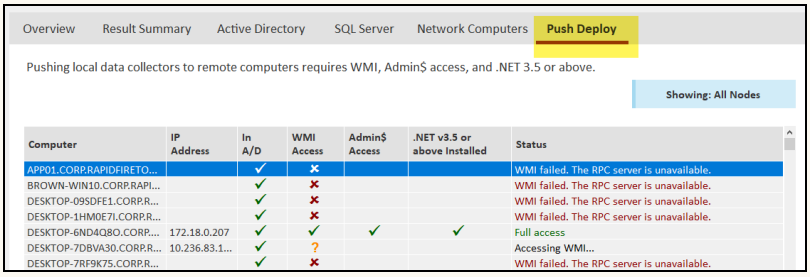


10. The **Verify and Run** window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan's **Output Assessment File Folder** location and **Basename** for the scan data. The file will be output as a **.PCI** file.



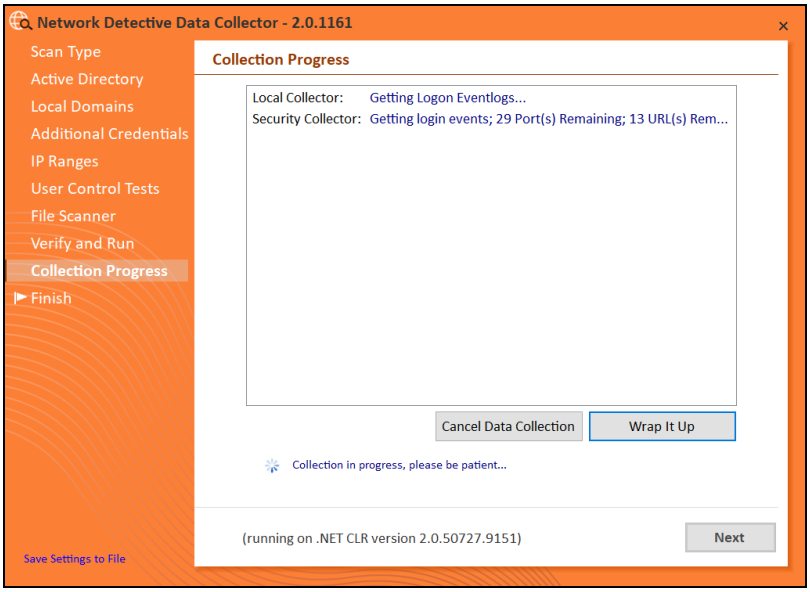
> **Tip:** Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which devices are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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

scan.



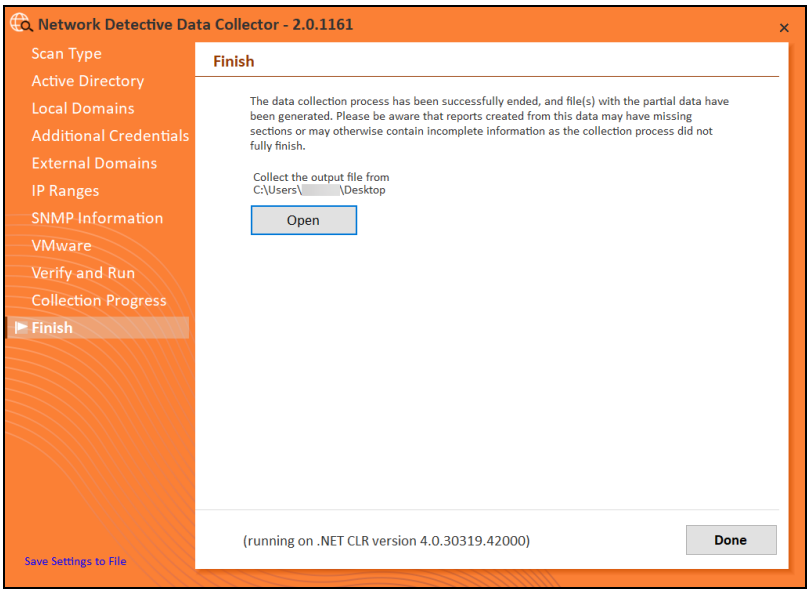
Enter any **Comments** and then click **Start**.

11. The **Collection Progress** window will appear. The **Network Scan's** status is detailed in the **Collection Progress** window. The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.



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

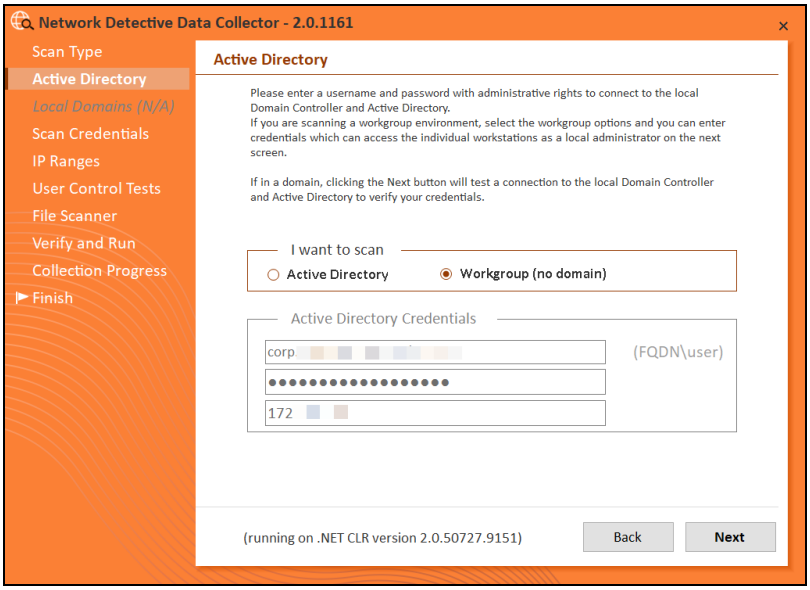
Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.



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

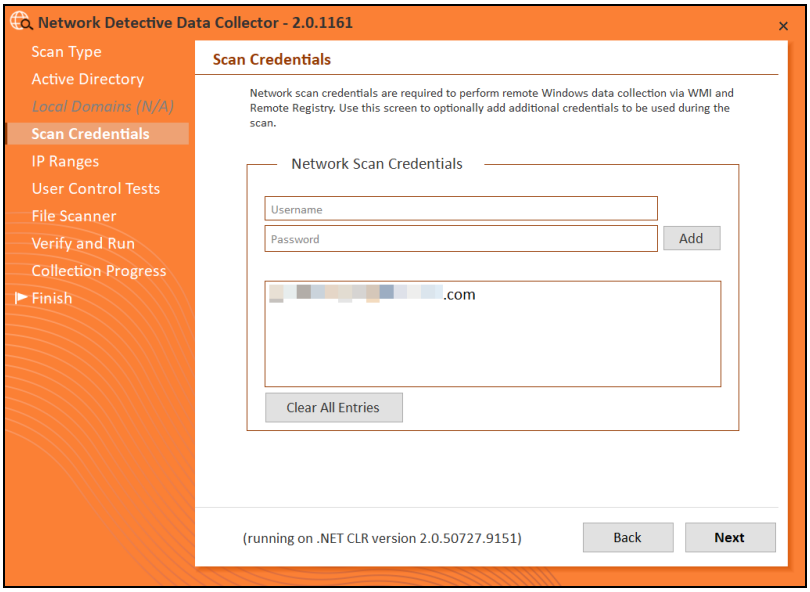
Scanning a Workgroup Network

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

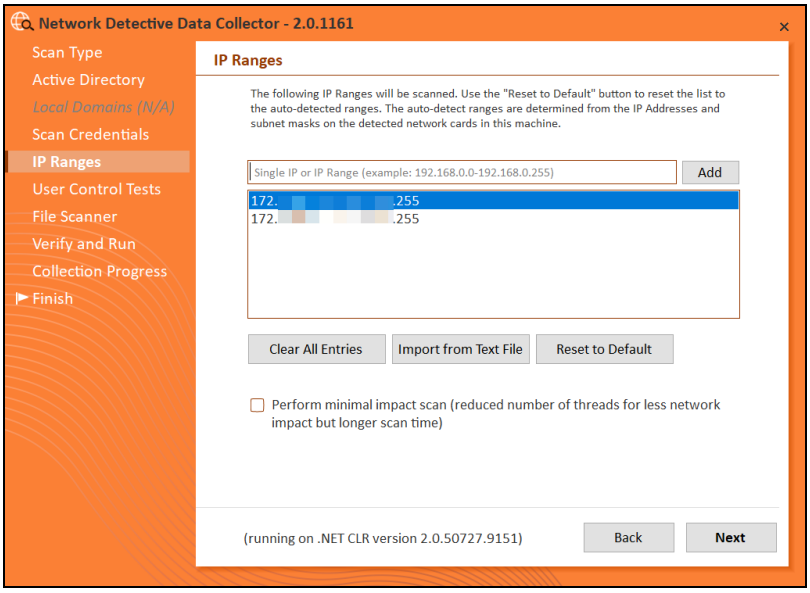


2. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator. Then click **Next**.

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



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

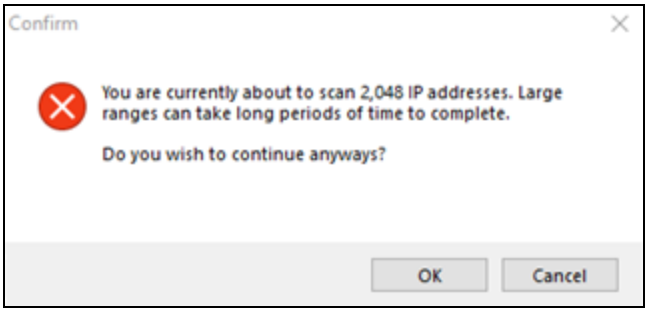


From this screen you can also:

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

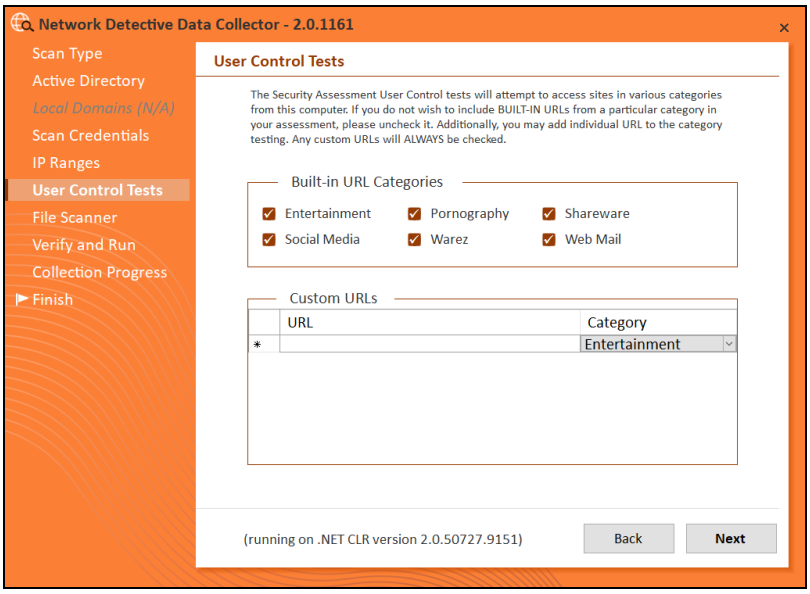
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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

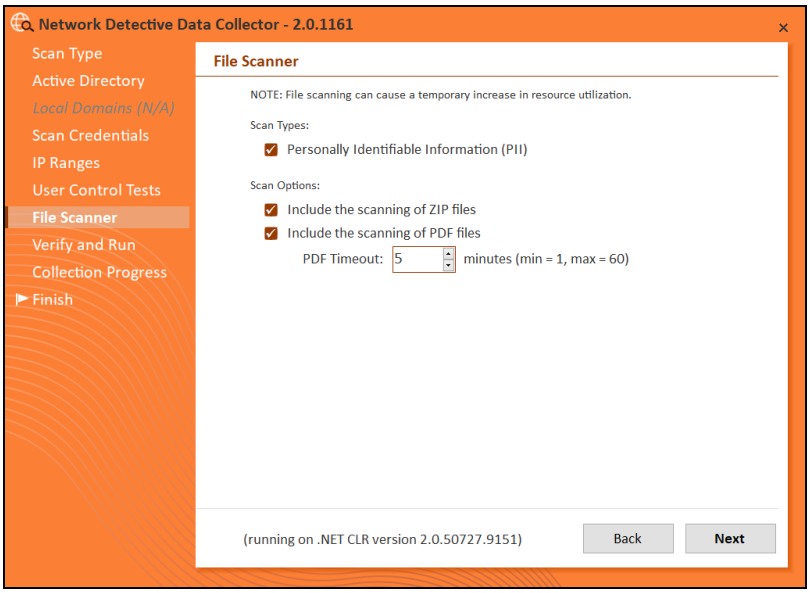


Important: If you are scanning a large number of IP addresses, confirm that you wish to continue. Consider performing multiple scans on smaller IP ranges. You can then upload each "batch" of scan files into the assessment, where they will be merged for complete results.

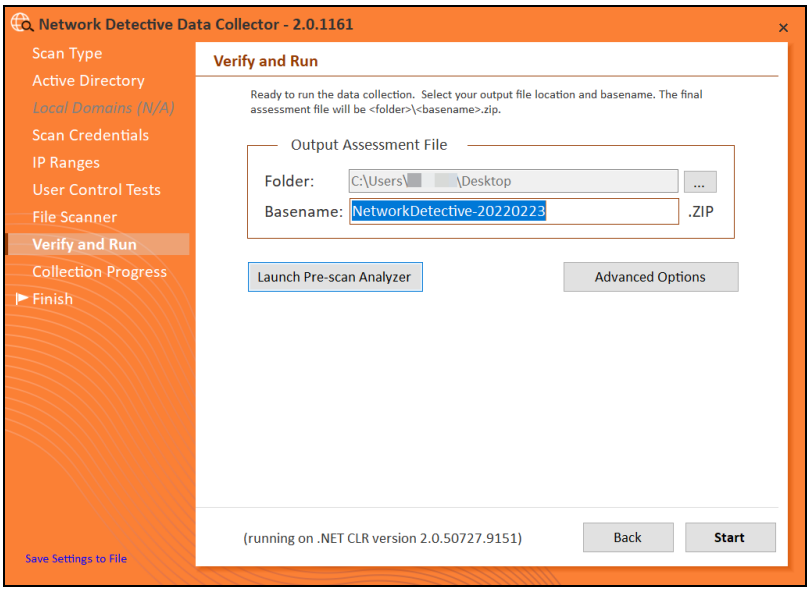
4. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your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



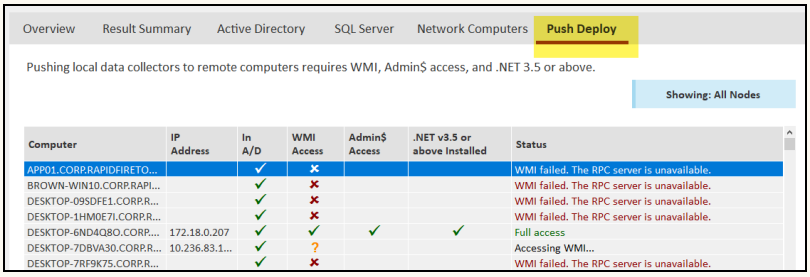
5. The **File Scanner** screen will appear. Choose whether to scan for PII (Personally Identifiable Information) and click **Next**.



6. 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 **.PCI** file.

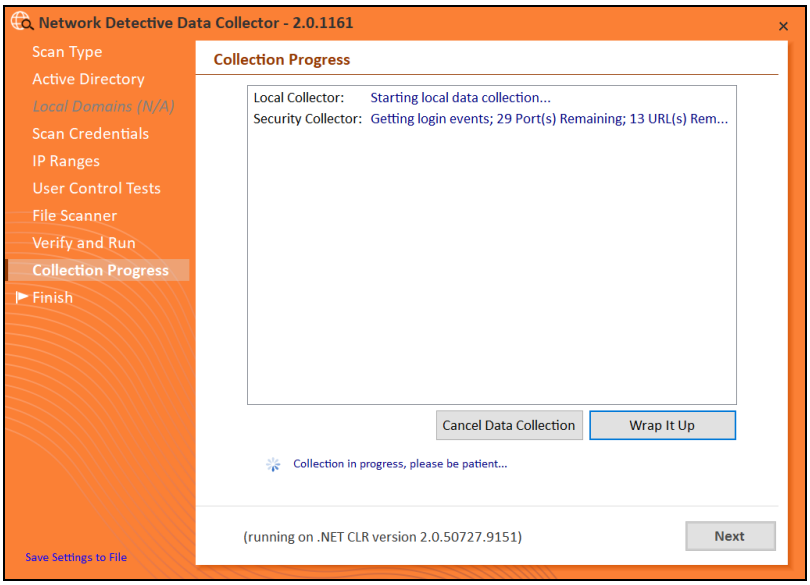


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which devices are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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



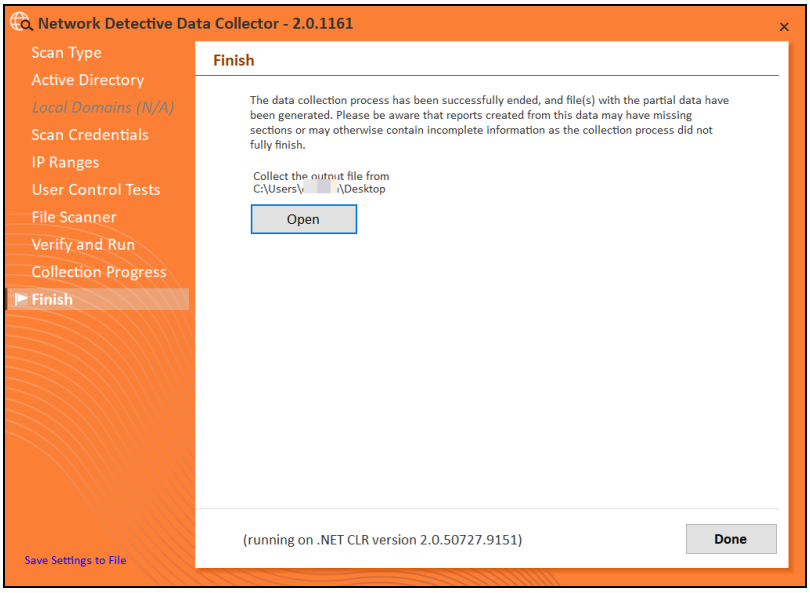
Enter any **Comments** and then click **Start**.

7. The **Collection Progress** window will appear. The **Network Scan's** status is detailed in the **Collection Progress** window. The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.



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

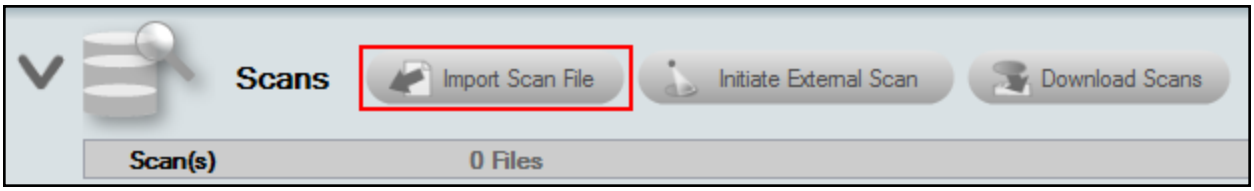
Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file's location and the scan's **Results Summary**.



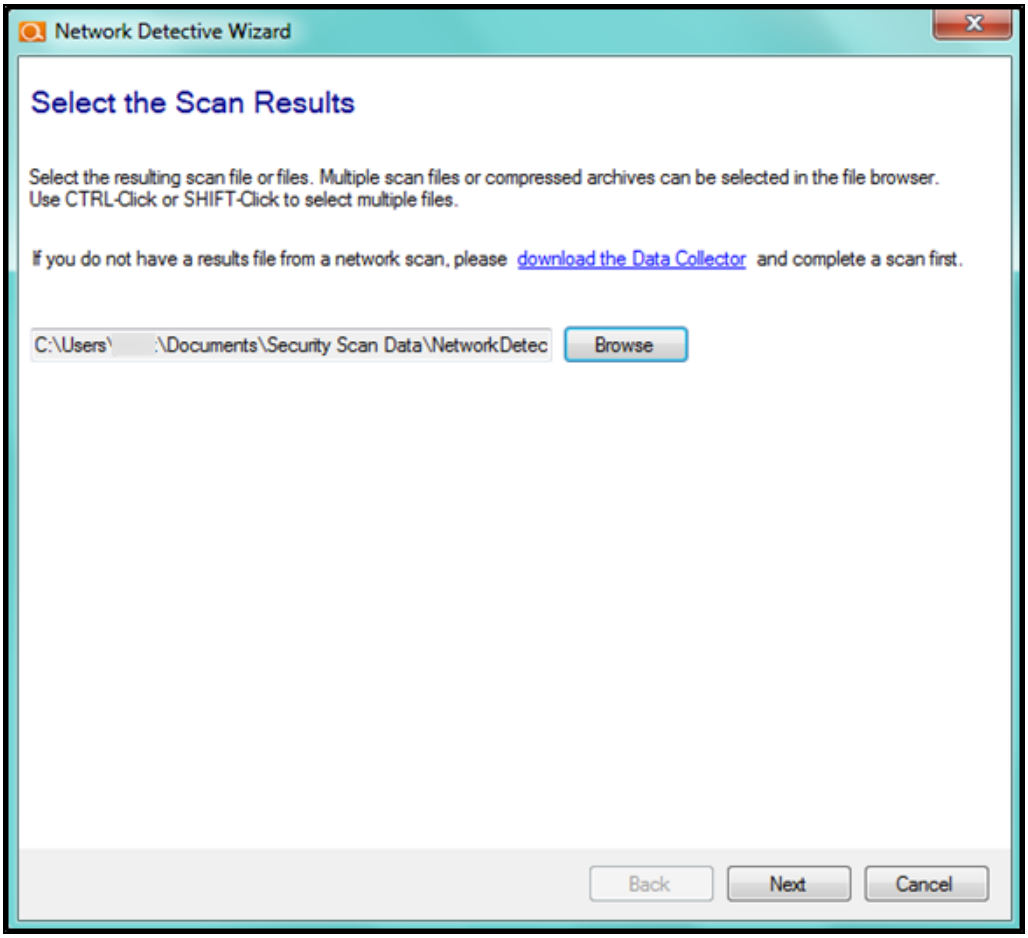
Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

Importing the Security Assessment Security Scan Data

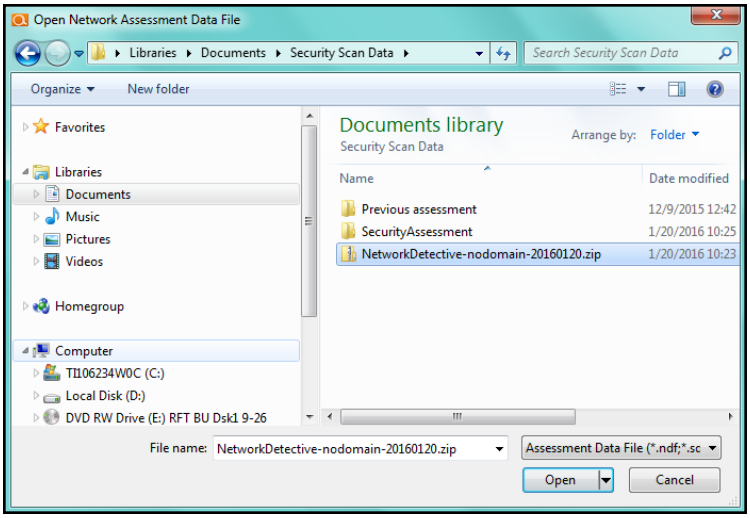
The final step in this process is to import the data collected during the **Security Assessment Security Scan** into the **Active Security Assessment**. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:



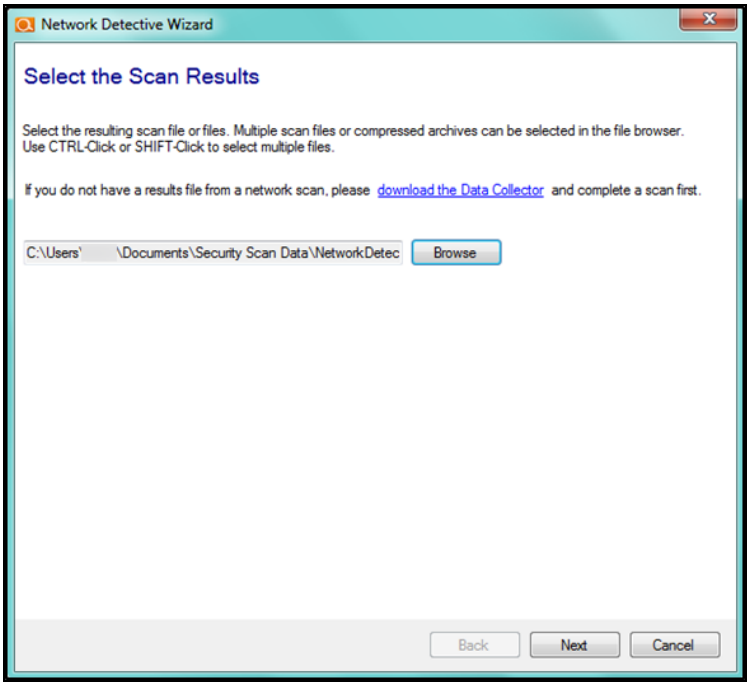
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP file produced by the **Network Assessment Data Collector Security Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Security Scan** data file.

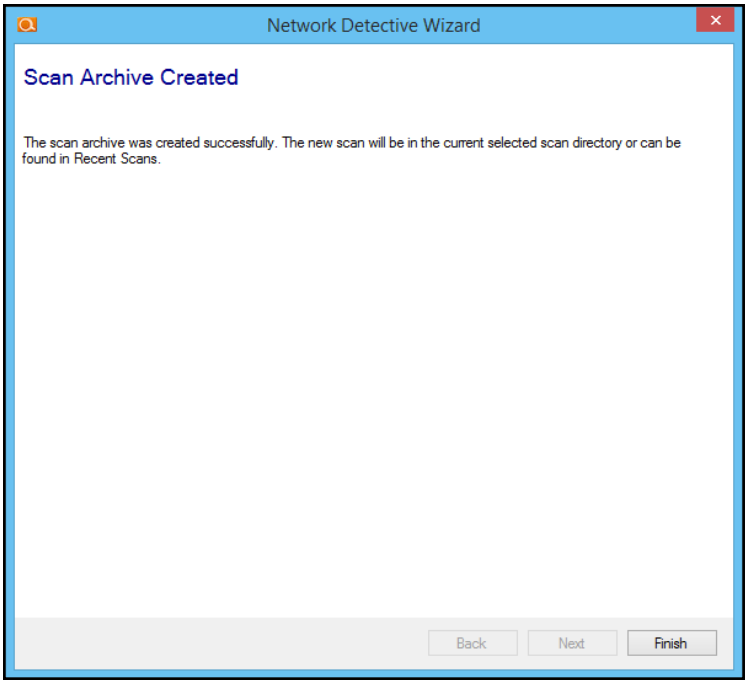


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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

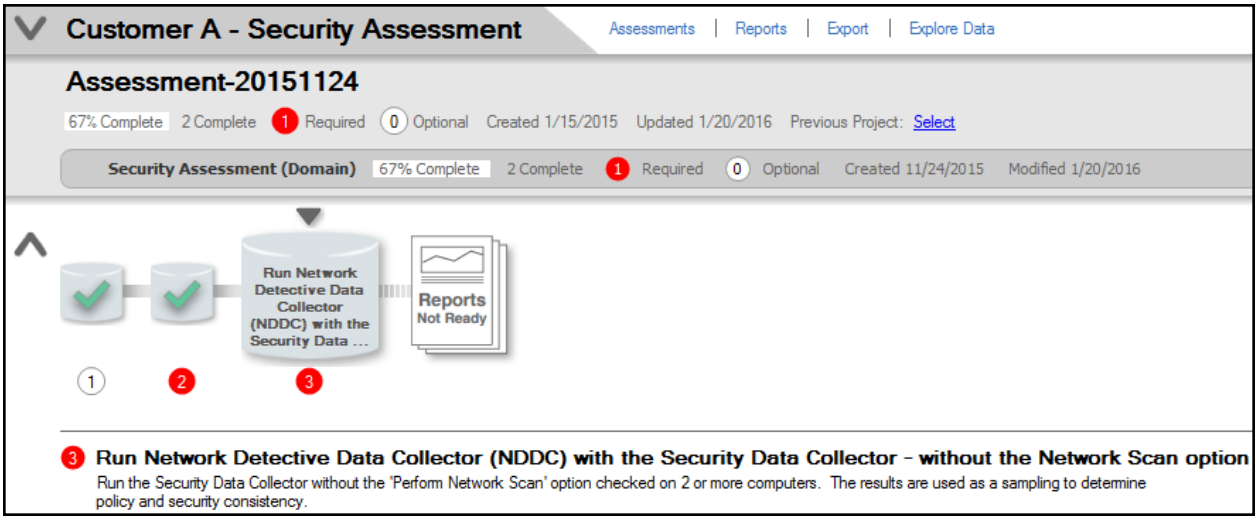


Select the **Finish** button to complete the scan file import process.

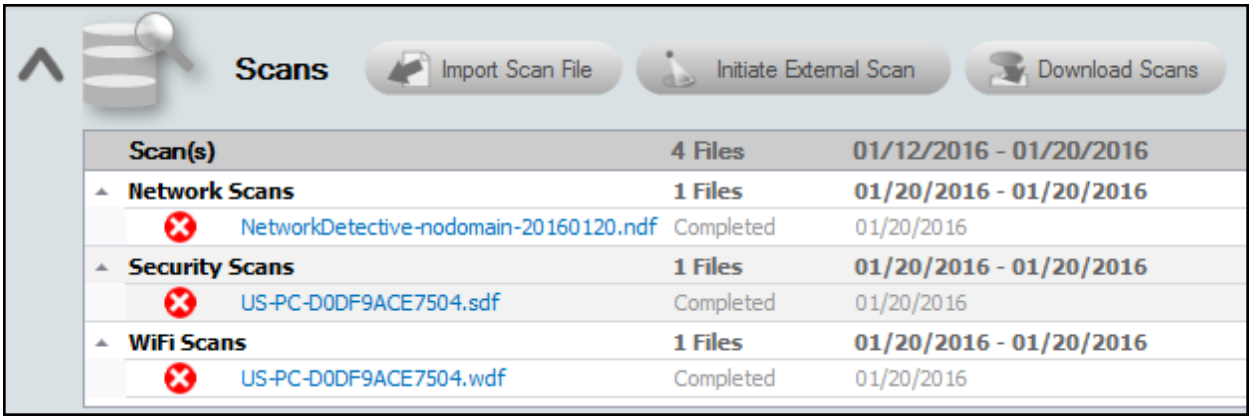
Scans List Updated Upon Completion of Imported Security Scan

After the Security Scan's file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Security Assessments Security Scan** data under the **Scans** section of the **Assessment Window**.

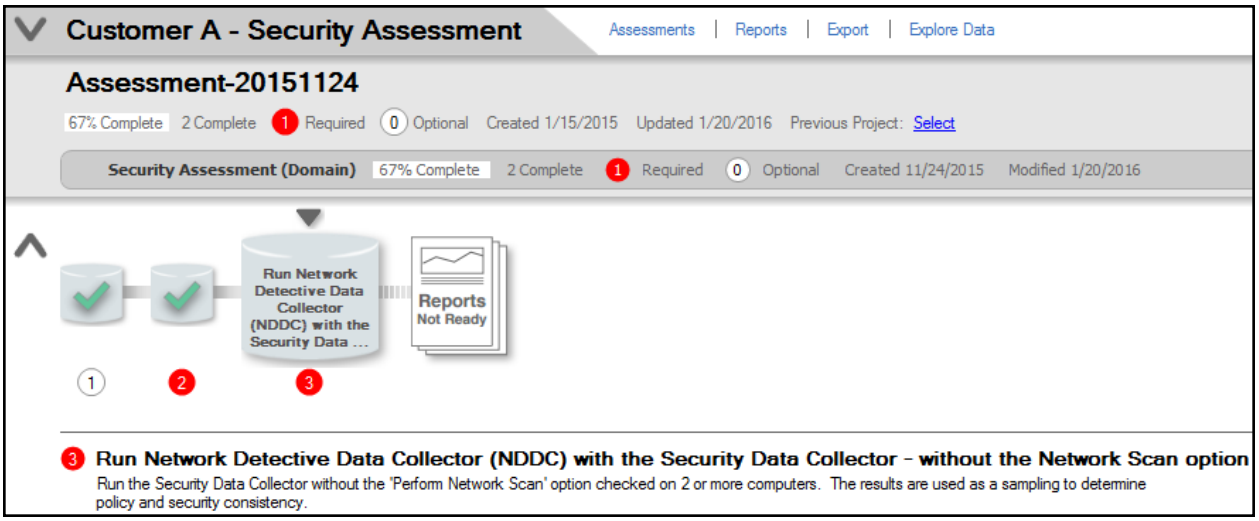
In addition, the **Status and Check List** information indicators will be updated to present the assessment's current status. Refer to the figure below.



After the **Security Scan file** is imported, the **Scans** section of the Assessment window will be updated to list the files imported into the assessment as seen below.



As illustrated in the **Checklist** below, the next step is to proceed with using the **Network Assessment Data Collector** to perform a second **Security Scan** without the "**Perform Network Scan**" option enabled on two (2) or more computers and import the resulting security scan data file into the assessment. The results of this second security scan are used as a sampling to determine policy and security consistency.



The Security Scan that must be performed on two or more computers, if not all of the computers on your customer's network can be accomplished through performing either:

- Use the Security Assessment Push Deploy Tool to Initiate Push of Local Computer Scans on Selected Systems and Import Scan Results

OR

- Run the Network Assessment Data Collector selecting the Security Collector Scan on the Computers that were Unreachable during Security Assessment Push Deploy Tool Scanning (OPTIONAL)

Task 3: Use the Push Deploy Tool to Collect Remaining Data and Import Scan Results

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

The Push Deploy Tool 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

Process to Run the Push Deploy Tool to Perform Local Computer Security Scans

During a Security Assessment, the **Push Deploy Tool** pushes the **Local Security Data Collector** to machines in a specified IP 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 within the network from a centralized location. **The Push Deploy Tool** is used to reduce or eliminate the need for you to spend time at each computer within the network to run a local computer security scan.

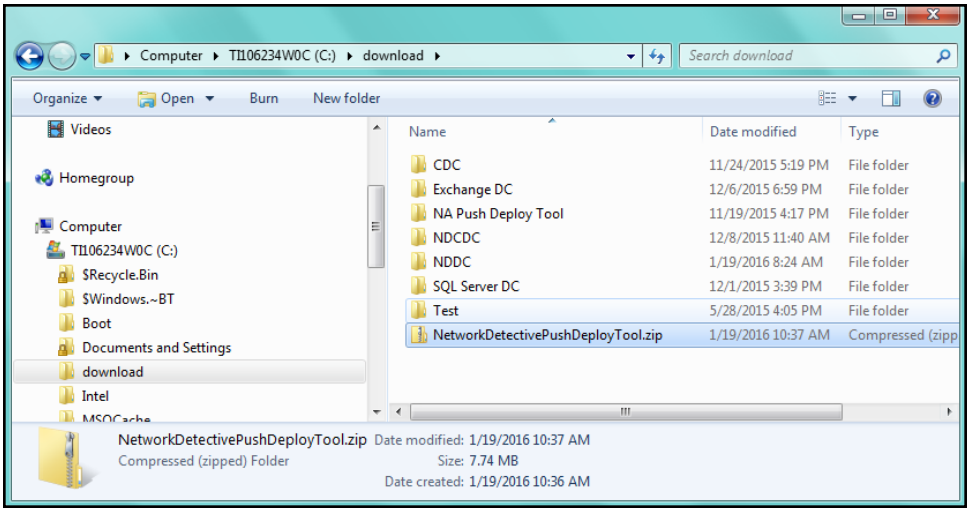
The output files (.ZIP files) from the local scans can either be:

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

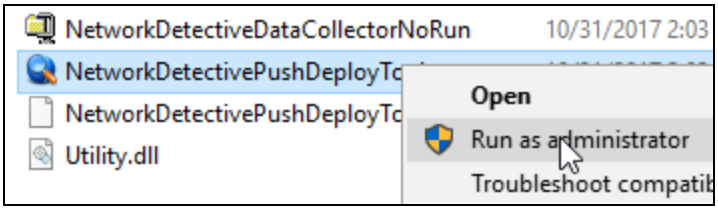
To use the Push Deploy Tool to perform security scans for computers within a network, please follow the steps detailed below.

Step 1 – Download and Run the Push Deploy Tool

To perform a Local Computer Security Scan, download the Push Deploy Tool from the RapidFire Tools download page at https://www.rapidfiretools.com/nd. Then extract the contents of the **Network Detective Push Deploy Tool** .ZIP file to a USB drive or directly to any machine on the target network.



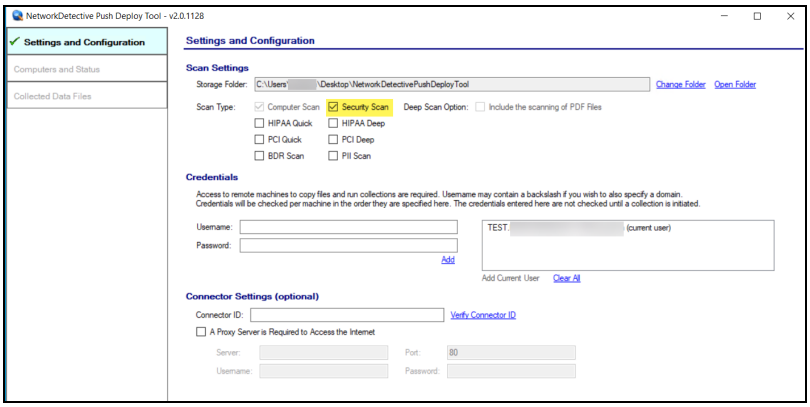
Then right click on the **NetworkDetectivePushDeployTool.exe** contained within the folder named **NetworkDetectivePushDeployTool** that was created by the .ZIP file extraction and select the **Run as Administrator** option to run the tool.



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

Step 2 – Configure the Push Deploy Tool to Perform Local Computer Security Scan and Add Credentials

Starting the **Push Deploy Tool** will present the following window.



First, select the **Security Scan** option.

Tip: If you wish to scan for additional data for more robust reporting, including PII (personally identifiable information), see "Data Breach Liability Scanning and Reporting" on page 259.

Next, set the **Storage Folder location** used to store the scan data collected from the computers scanned. **Note: This Storage Folder location can be located on a network share drive to centralize scan file storage.**

If the individual performing the **Push Deploy Tool-based** scans is logged into the network using Domain Administrator credentials, then the need to enter credentials as part of configuring the **Push Deploy Tool** scans may not be required as the **Domain Administrator** credentials may be entered in the Credentials list by default.

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

Note: For the Push Deploy Tool to push the local scans to computers throughout the network to perform local computer scans, you need to 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. Push/Deploy also relies on using the Admin$ share to copy and run the data collector locally. Admin$ must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan.

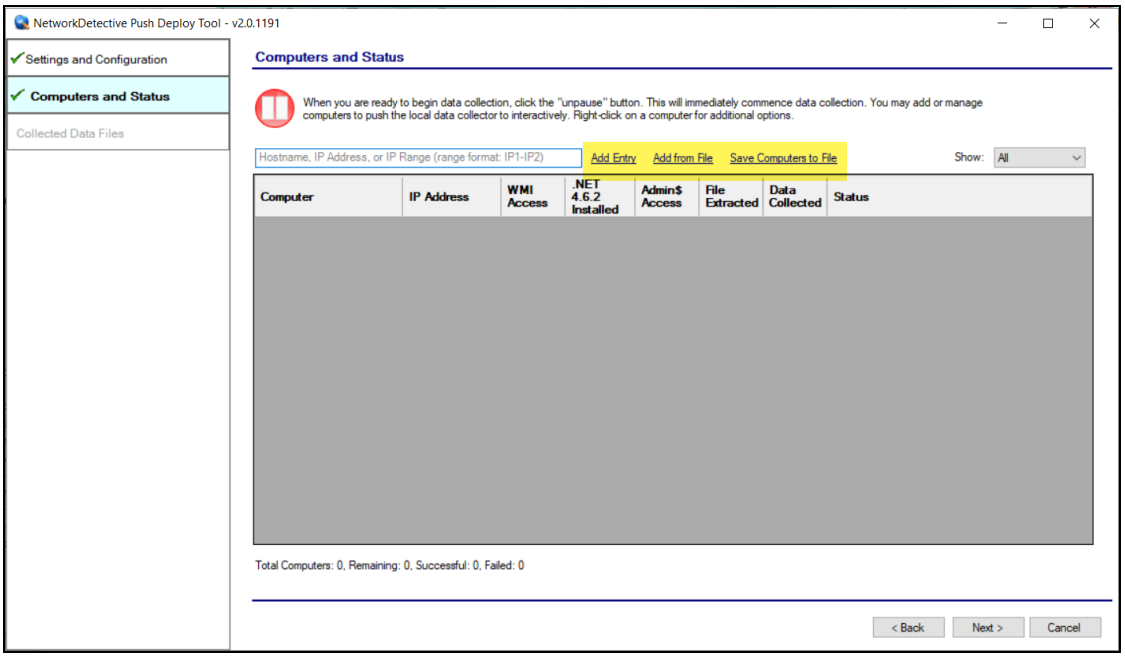
For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same. In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials.

Next, select the **Computers and Collection Status** tab.

Step 3 – Add the Computers to Scan

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

- **Add Entry** to be scanned (Add single IP or IP range)
- **Add** (computers) **from File** that are to be scanned
- Or **Save Computers to File** in order to export a list of computers to be scanned again in future assessments

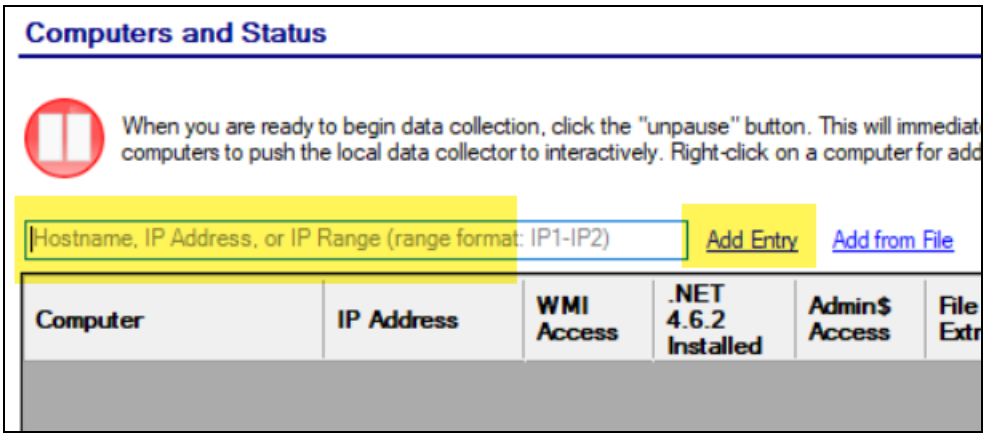


Scan Setup Process Methods used to Configure Computers to be Scanned

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

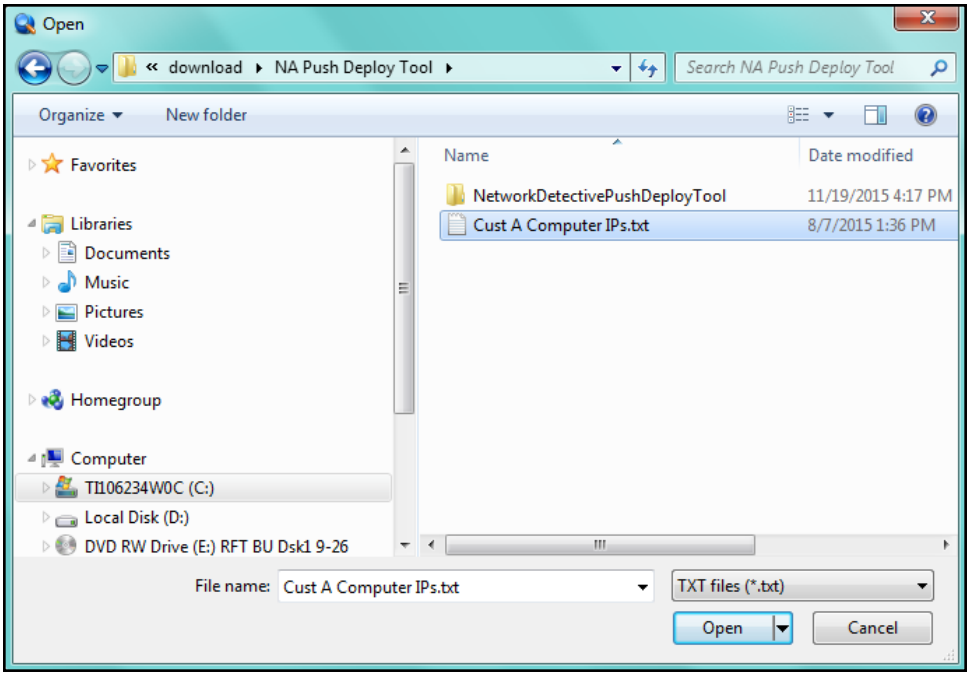
Method 1 - Add IP Entry for Computers to be Scanned

To use the **Add Entry** method to select computers to be scanned, type in the computer IP or IP Range address as shown below, then click on the **Add Entry** 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.

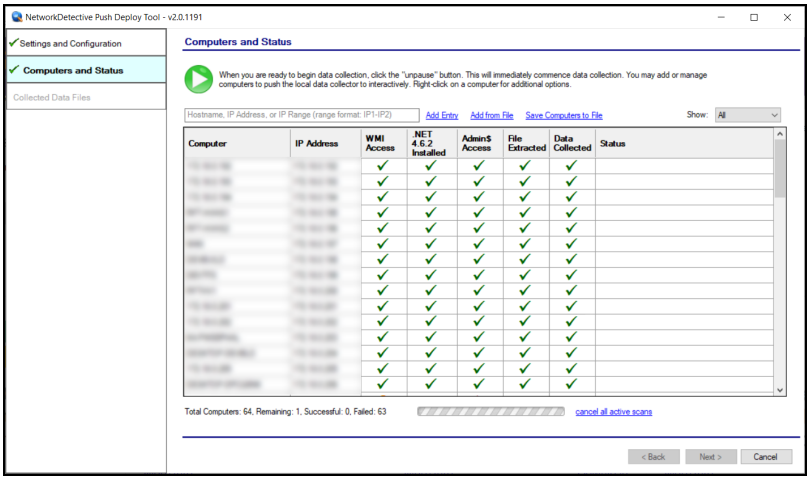
The file that contains the IP addresses can be created using the Push Deploy Tools' **Save Computers to File** feature, or created manually with a text editor using the required text formatting structure so that the IP addresses are recognized by the **Push Deploy Tool**.

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 Collection Status** window for verification prior to starting the scan.

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 **Computer and Collection Status** window.

Step 4 – Initiating the Scan

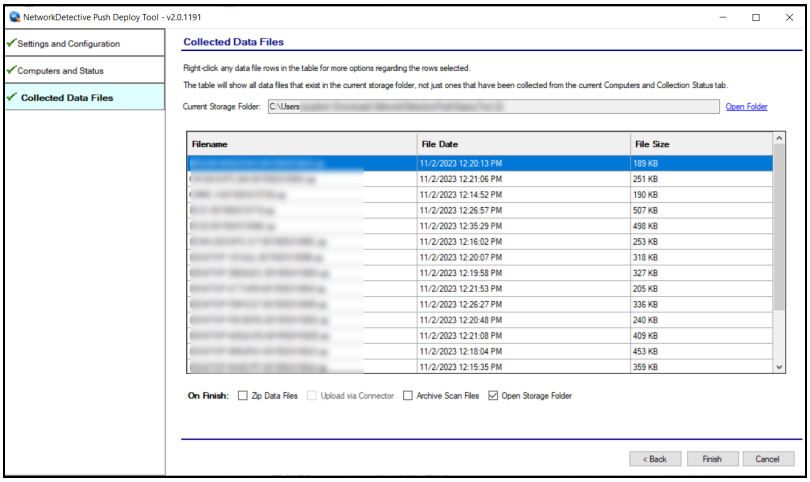
After creating/adding a list of one or more computers to scan, start the scan either by selecting the "**unpause**" button in the **Computer and Status** window, or, by selecting the **Next** button in the **Computer and Status Window** and the scan will be initiated after you confirm that the scan should be started. The status of each computer's scan activity will be highlighted within the **Computers and Collection 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**.

Step 5 – Verify that the Local Computer Security Scan Data has been Collected

To verify the inclusion of the scan data produced by the **Push Deploy Tool** within your assessment, select the Next button to view the **Collected Data Files** window**.**



Step 6 – Verify that Network Assessment Local Computer Security Scan Files are Available from Scan Process

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 and then

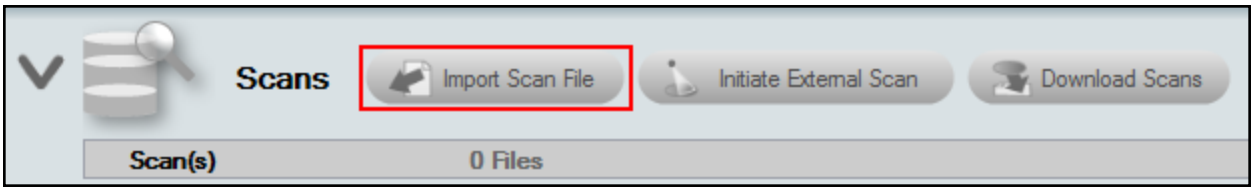
select the **Finish** button.

After all of the **Security Assessment's Local Computer Security Scans** are complete for the computers that were selected to undergo this scan, the next phase in the process is to import the scan data files produced by the **Local Scans** into the current **Security Assessment**.

Importing the Push Deploy Tool Local Computer Security Scan Data into the Security Assessment

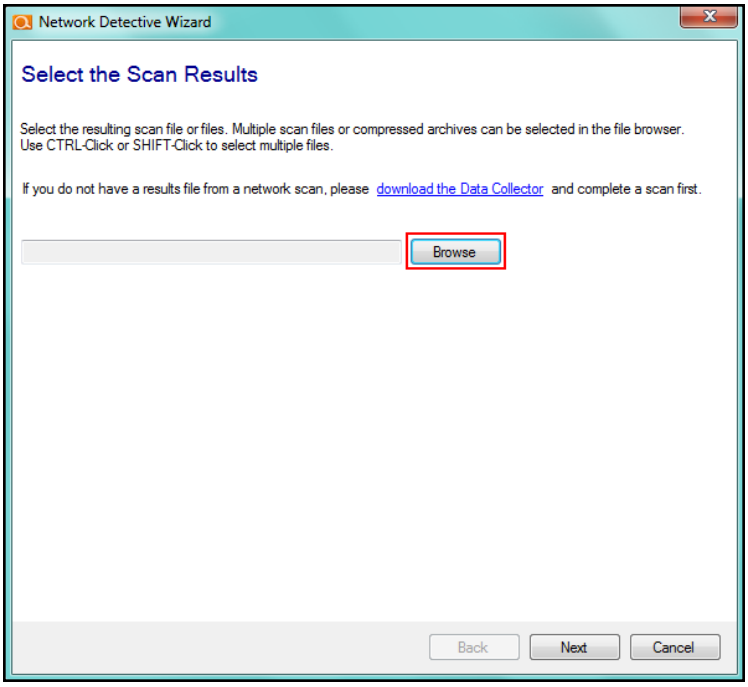
The final phase in this process is to import the data collected during the Security Scans performed by the **Push Deploy Tool's** local computer security scanner into the **Security Assessment** itself.

Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:

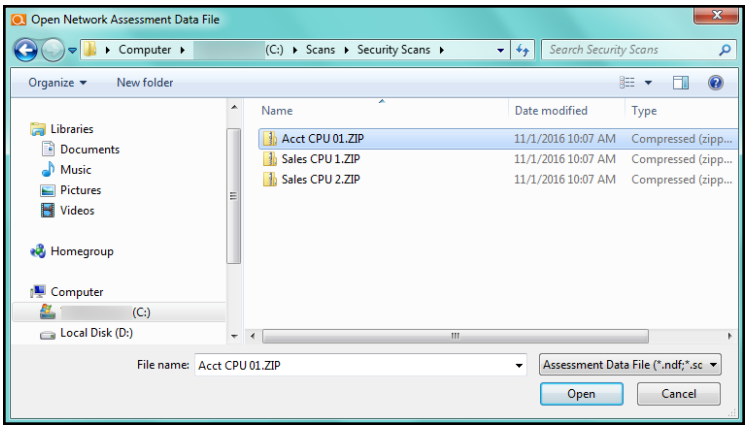


The following **Select the Scan Results** window will be displayed. This window enables you to **Browse**, select, and import the .ZIP scan files into the **Security Assessment**.

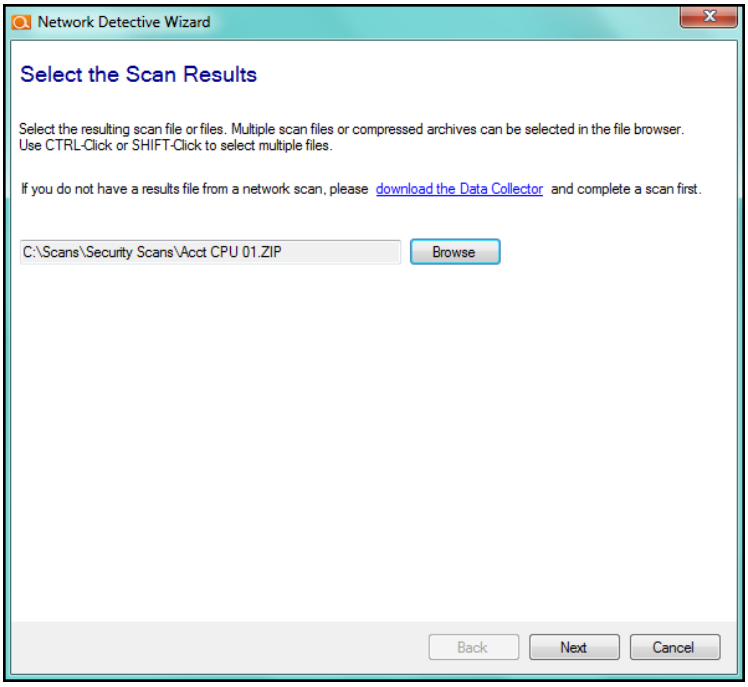
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP files produced by the **Push Deploy Tool** based **Local Computer Security Scans** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Local Computer Security Scan** data file.

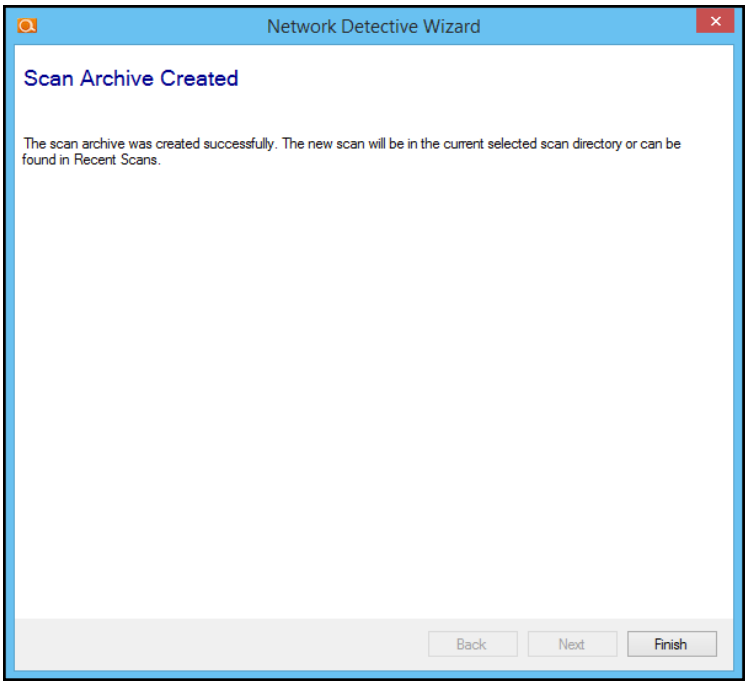


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

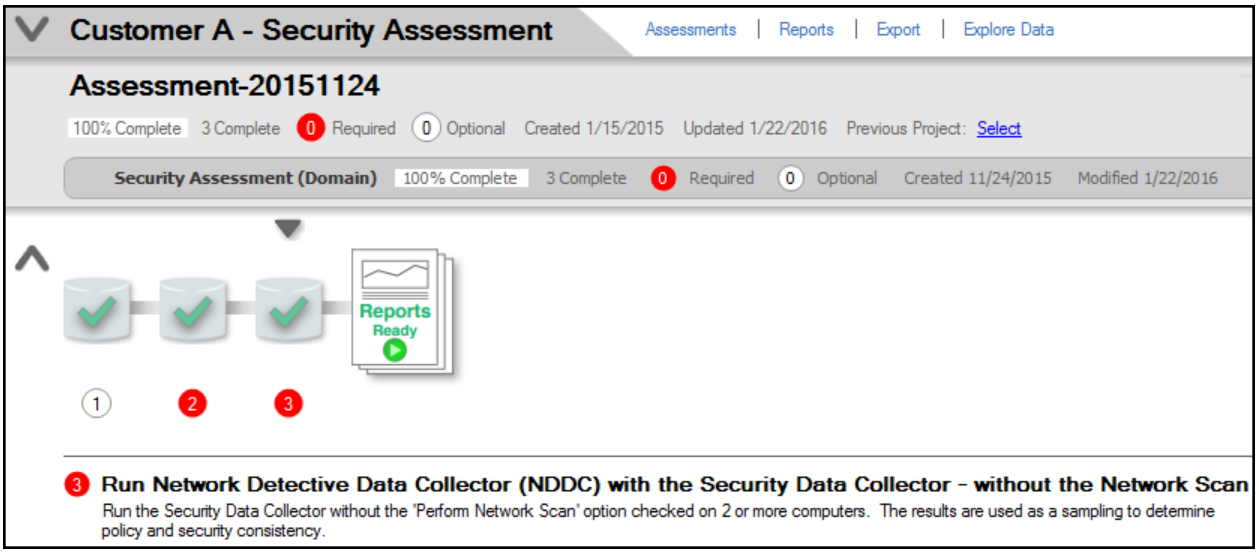
The success of the scan's import will be confirmed by the **Scan Archive Created** window being displayed as presented below.



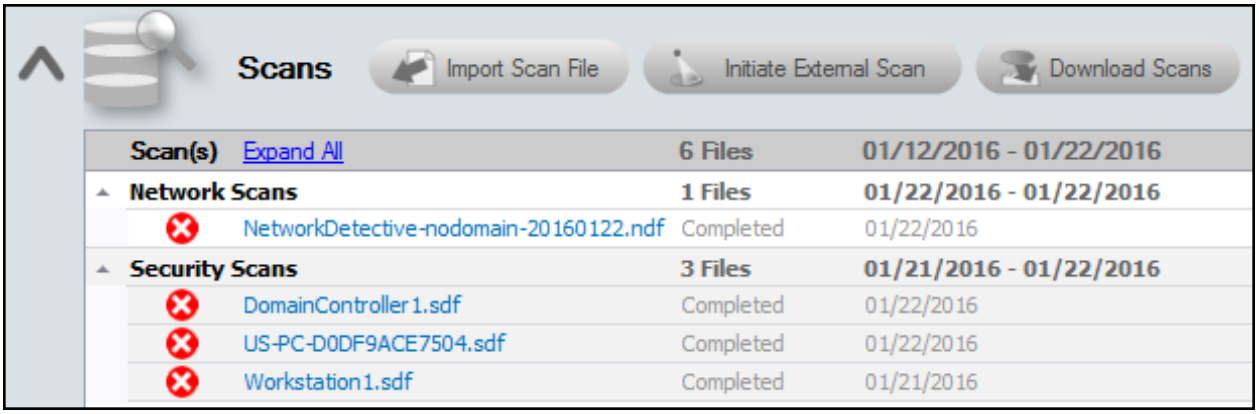
Select the **Finish** button to complete the scan file import process.

After the Local Computer Security Scan's .ZIP file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Security Scan** data under the **Scans** section of the **Assessment Window**.

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



After the **Local Computer Security Scan**s files are imported into the assessment, the **Scans** section of the **Assessment Window** will be updated to list the **Security Scans** files imported into the assessment as seen below.



Task 4: Run the Network Assessment Data Collector selecting the Security Collector Scan on the Computers that were Unreachable during Security Assessment Push Deploy Tool Scanning (OPTIONAL)

Process to Run the Network Assessment Data Collector to Perform a Security Scan on a Local Computer

The **Network Assessment 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 **Network Assessment 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

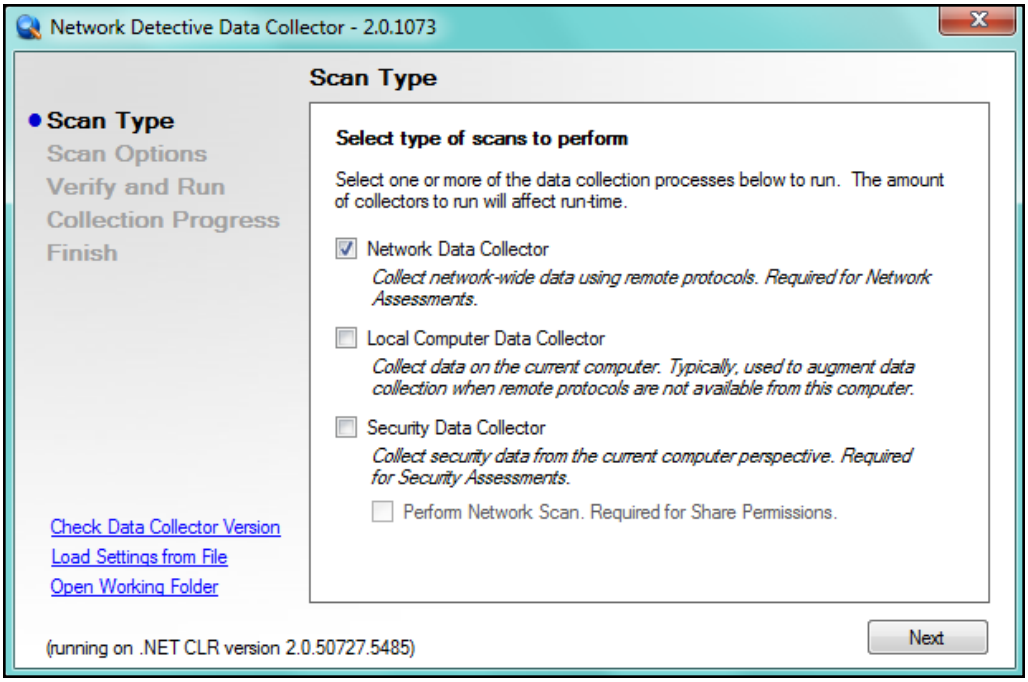
Step 1- Running the Network Assessment Data Collector to Perform a Security Scan on a Local Computer

Visit the RapidFire Tools software download website to download and then run the **Network Assessment Data Collector** file. It is a self-extracting ZIP file that does not install on the client computer. Use the **unzip** option to unzip the files into a temporary location and start the collector.

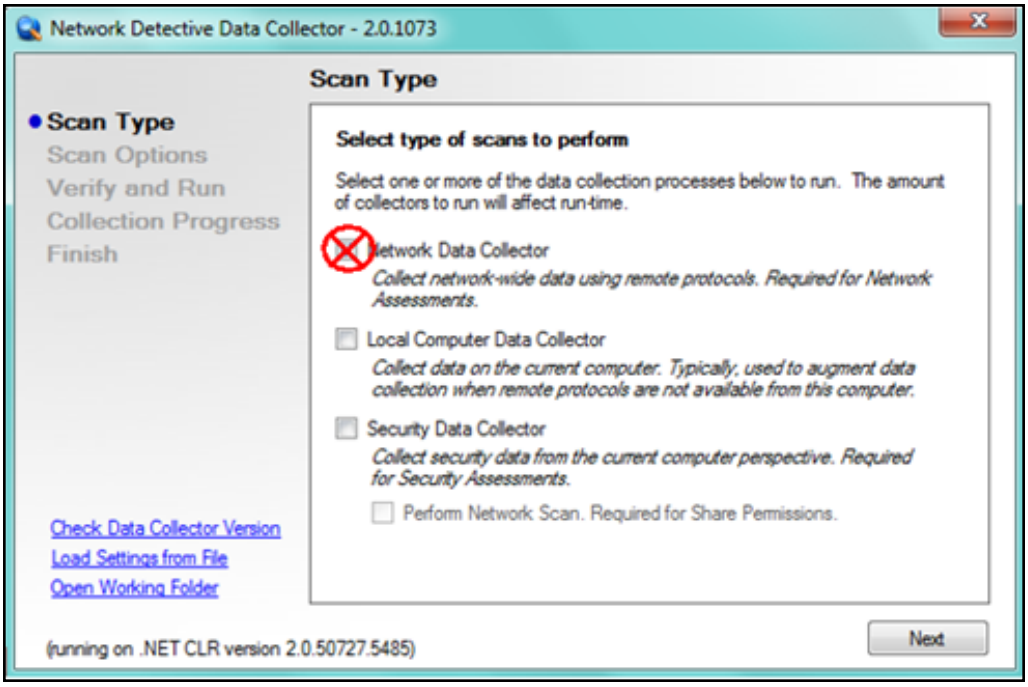
Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

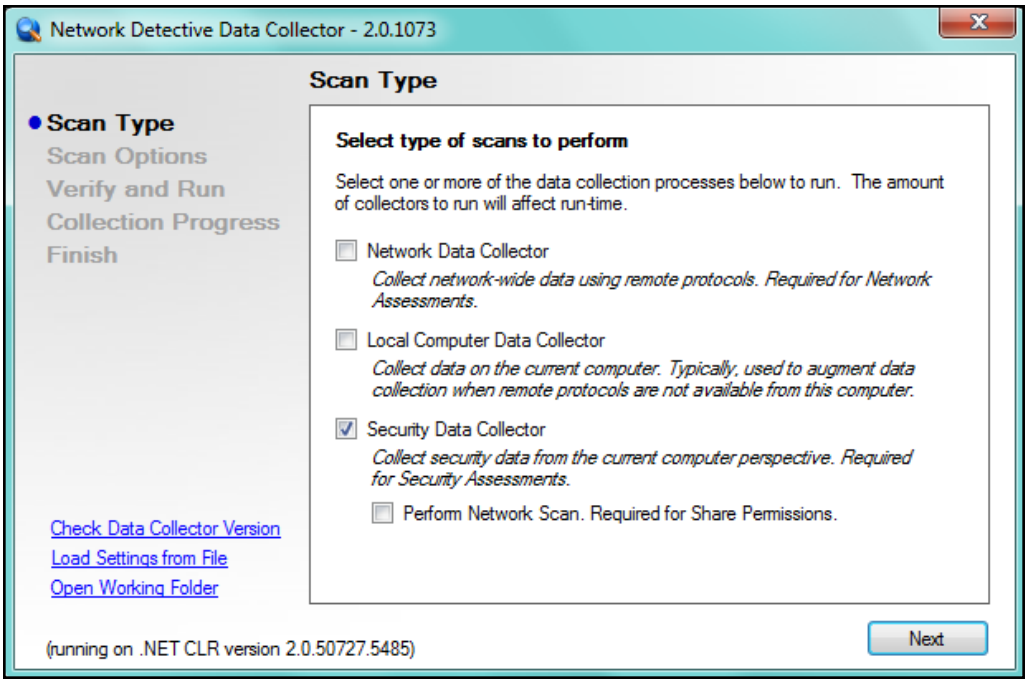
Step 2 – Configure the Network Assessment Data Collector to Perform the Security Scan

Starting the **Network Assessment Data Collector** application will present the following screen.



If you are running on a computer in the network, such as the domain controller, to run a Security Scan, **deselect the Network Data Collector option** and then select the **Security Data Collector** option. Do not select the **Perform Network Scan** option.



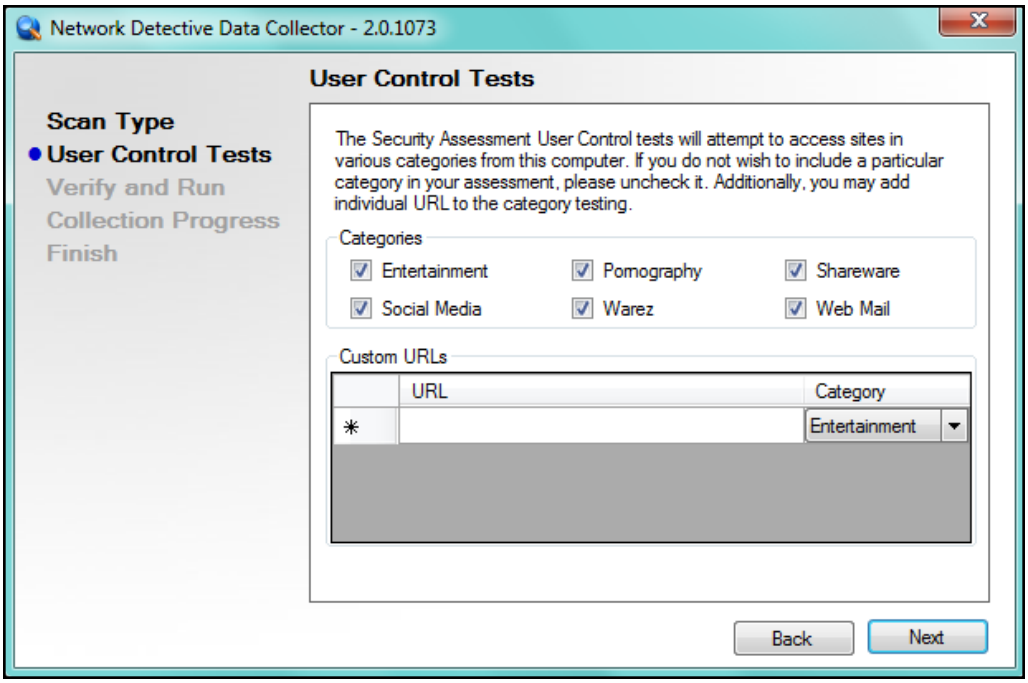


Only the Security Data Collector option should be selected.

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

Step 3 – User Control Tests

Select the **Categories** of sites that User Control and access tests should be performed upon.

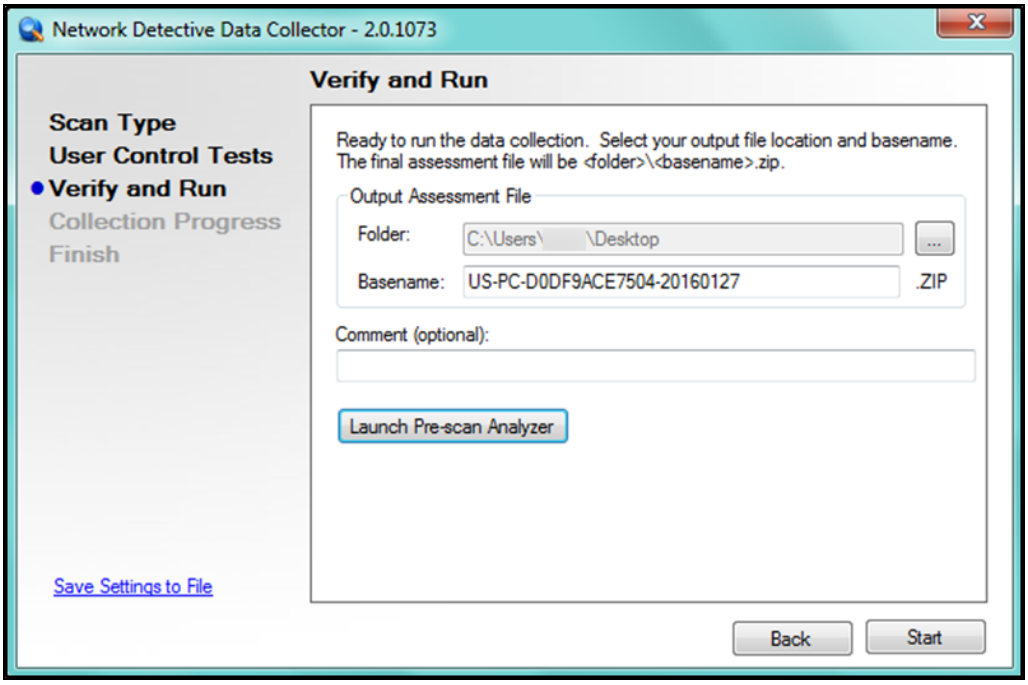


Then click on the **Next** button.

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

Step 4 – Verify and Run the Scan

Select the folder that you want to store the scan data file in after the scan is completed.



You may change the scan's **Output Assessment File Folder** location and **Basename** for the scan data.

Starting the Security Scan

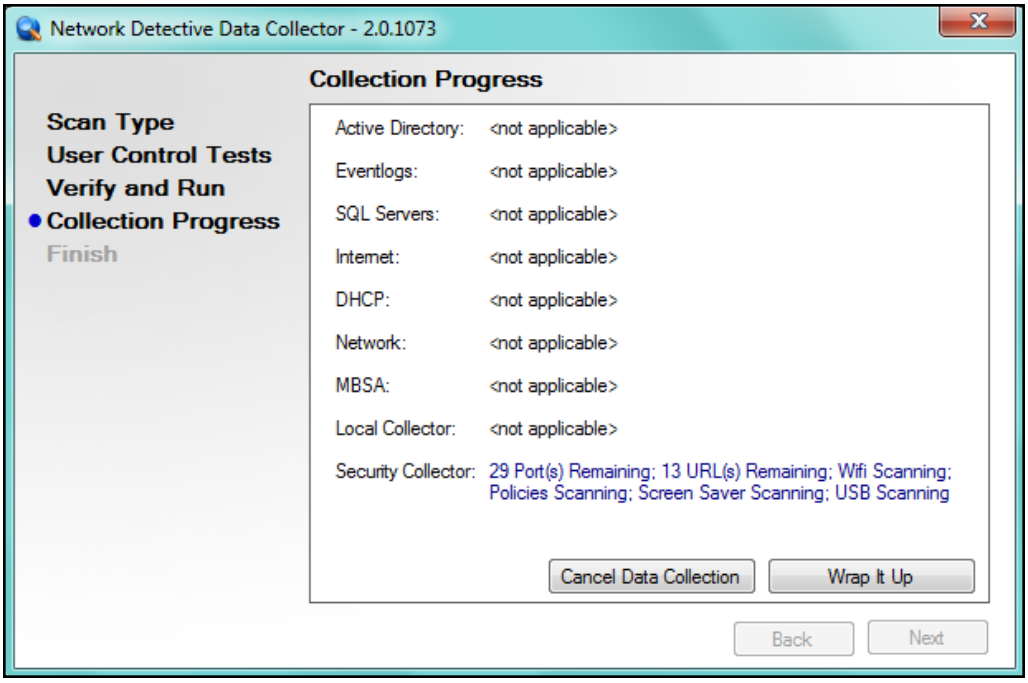
Once the **Assessment File Folder** location and **Basename** for the scan data has been specified, enter any **Comments,** and then select the **Start** button to initiate the scan**.**

Once the scan is started, the scan's **Collection Progress** window will then be displayed.

Step 5 – Monitor the Security Scan's Collection Progress

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

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

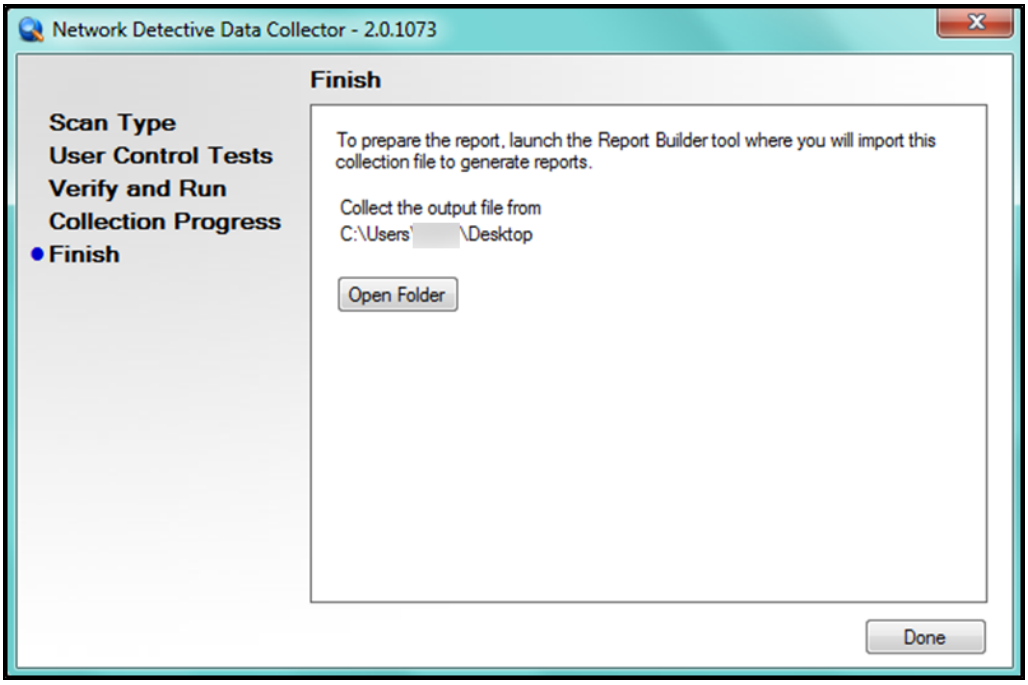


At any time you can **Cancel Data Collection** which will not save any data. By selecting **Wrap It Up** you can terminate the scan and generate reports using the incomplete data collected.

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

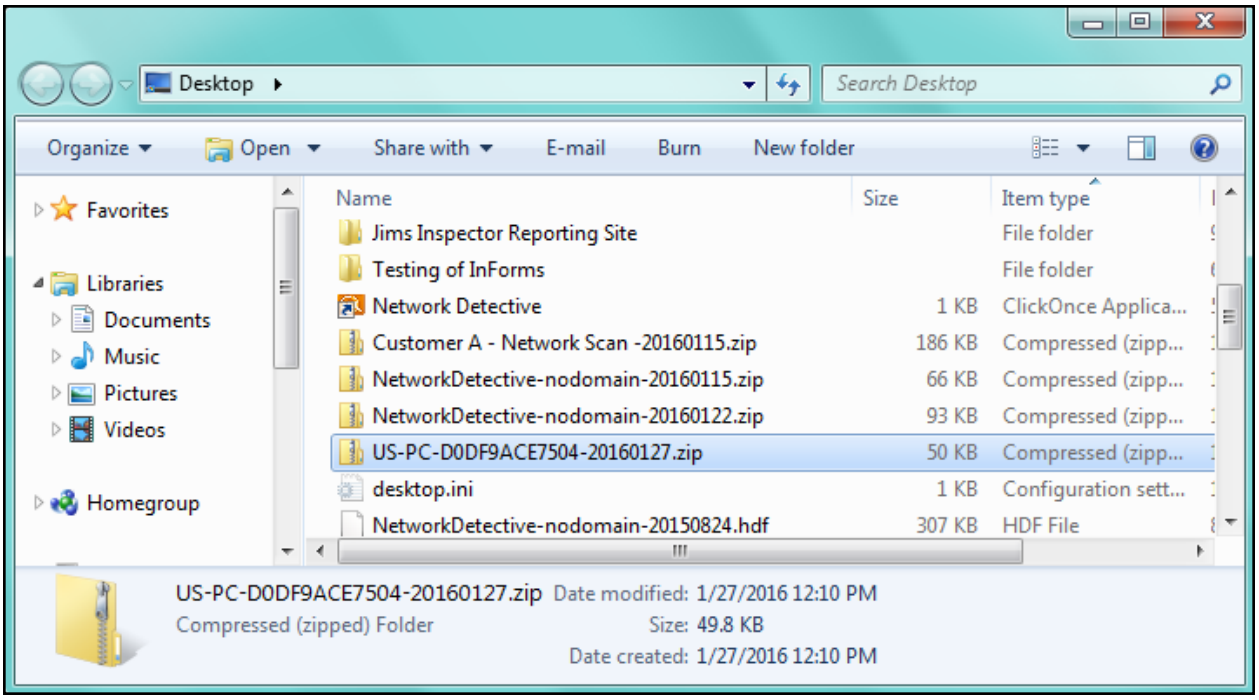
Step 6 – Complete the Network Assessment Data Collector Security Scan Process

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



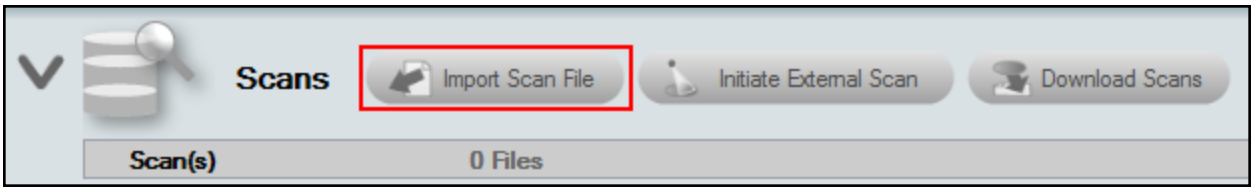
Click on **Done button** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

You can also view the file's location by selecting the **Open Folder** option.

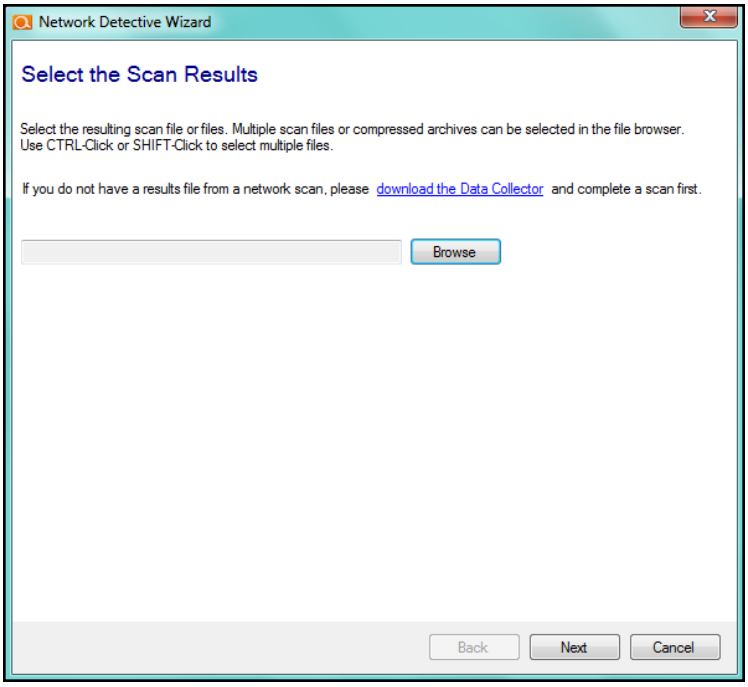


Importing the Security Assessment Security Scan Data

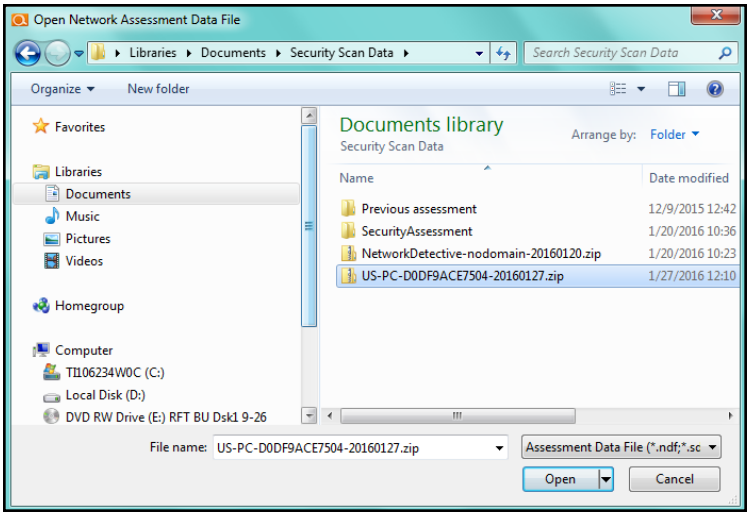
The final step in this process is to import the data collected during the **Security Assessment Security Scan** into the **Active Security Assessment**. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:



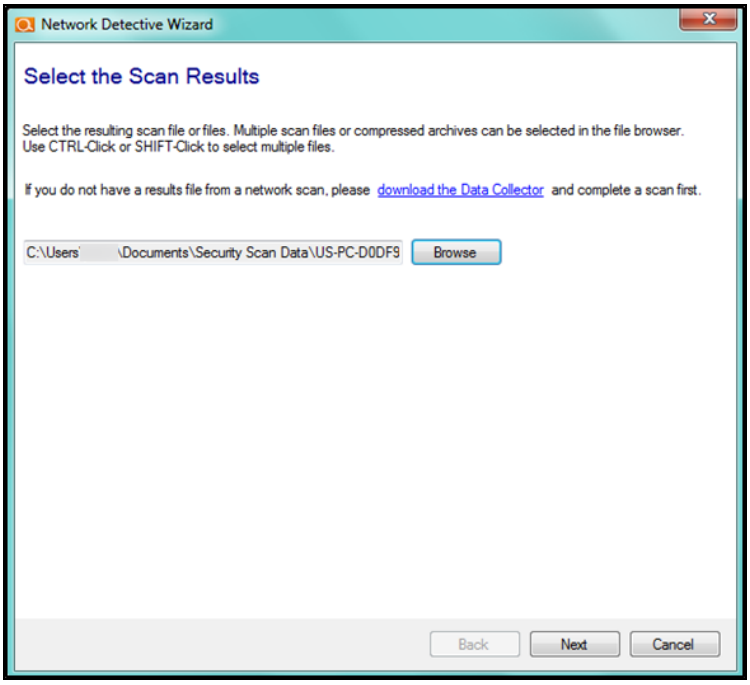
The **Select the Scan Results** window will be displayed thereby allowing you to import the .ZIP file produced by the **Network Assessment Data Collector Security Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Security Scan** data file.

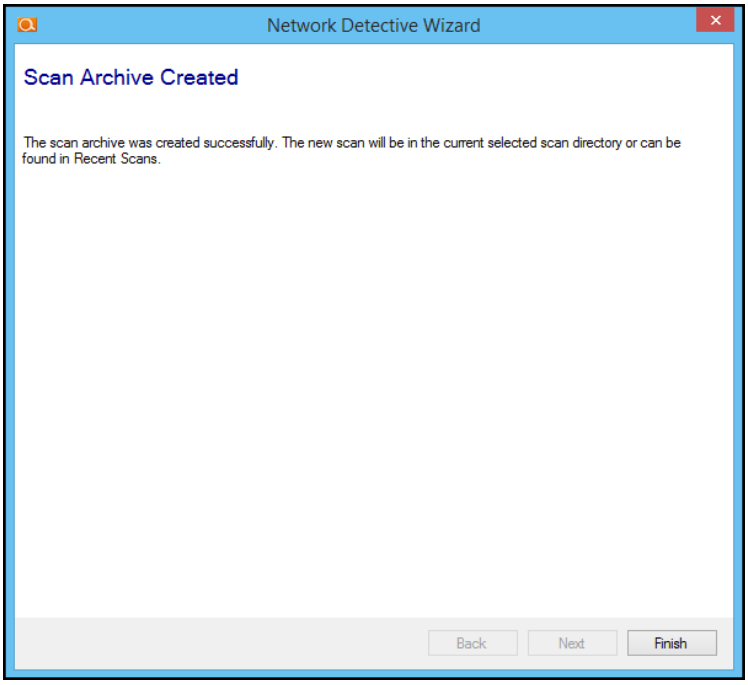


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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

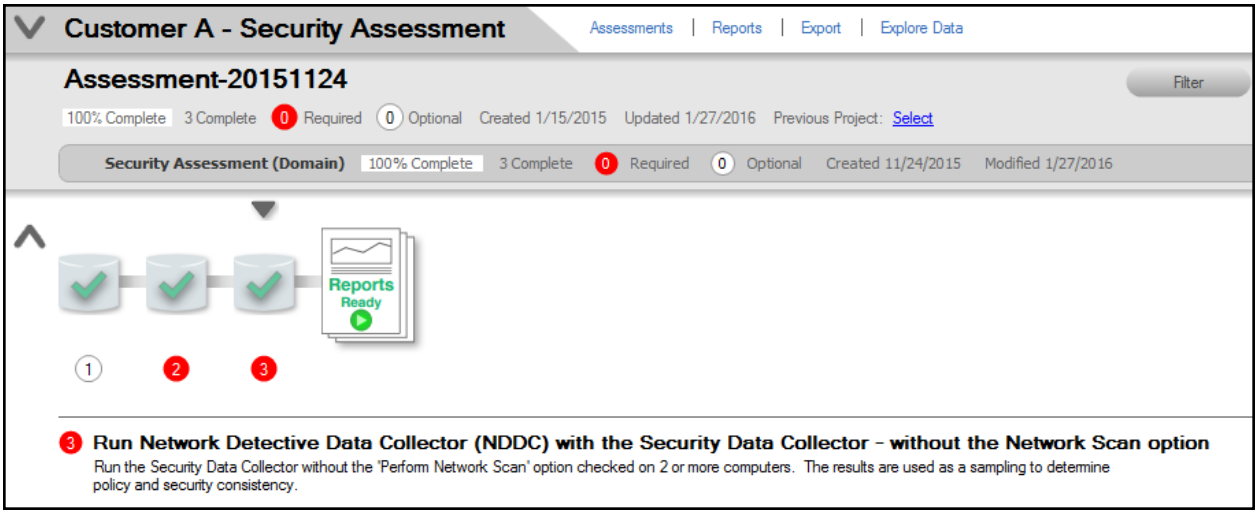


Select the **Finish** button to complete the scan file import process.

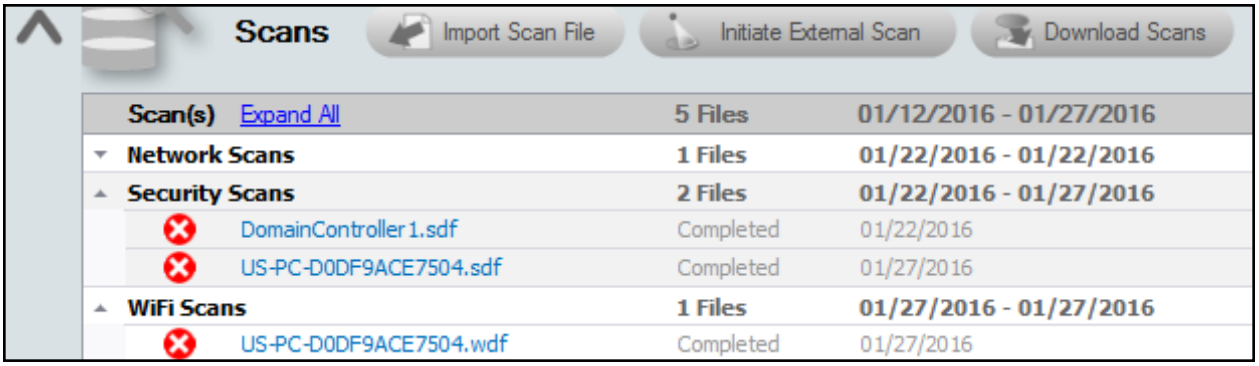
Scans List Updated Upon Completion of Imported Security Scan

After the Security Scan's .SDF file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Security Assessments Security Scan** data under the **Scans** section of the **Assessment Window**.

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



After the **Security Scan file** is imported, the **Scans** section of the Assessment window will be updated to list the files imported into the assessment as seen below.



Task 5: Document Exceptions

Complete the Issue Exception Worksheet (Optional)

The **Issue Exception Worksheet** is an **optional** worksheet that compiles the issues discovered by the Network Assessment Data Collector network and security scans, Security Assessment Push Deploy Tool Scans, and the Local Security Scan using the Data Collector all used throughout the Security Assessment process.

This purpose of this worksheet is to enable the individual performing the assessment to document actions that remediate identified issues in order to mitigate the risks resulting from issues identified by the assessment process.

At the initial completion of an Assessment, you can generate a **Risk Report** to review the risk issues initially identified during the Assessment.

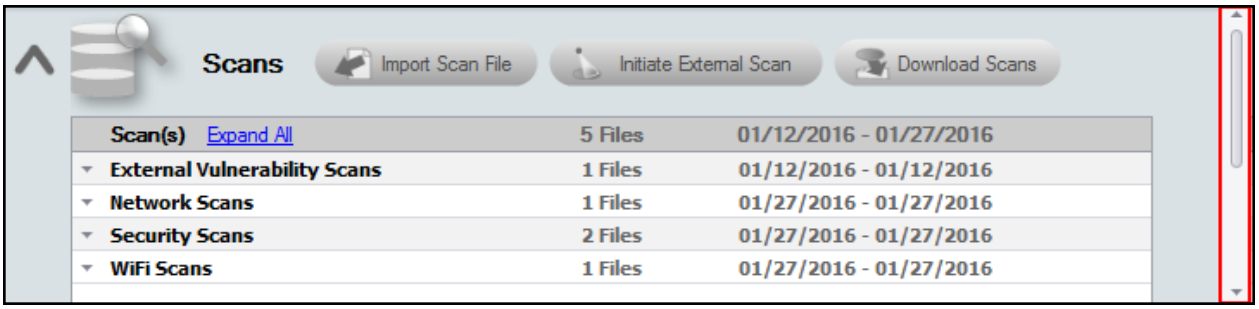
In the case that some of the issues presented in the **Risk Report** are being mitigated through some sort of compensating control, you can remove the risk identified during the assessment from the **Risk Report** through the use of the **Issue Exception Worksheet**.

The **Issue Exception Worksheet** is used to document **Issue Exceptions** along with compensating controls used to mitigate identified issues. The compensating controls document the actions that have been taken to mitigate the risks associated with a particular issue. Documenting these compensating controls will allow you to reduce the risk identified and the **Risk Score** calculated and presented in the **Risk Report**.

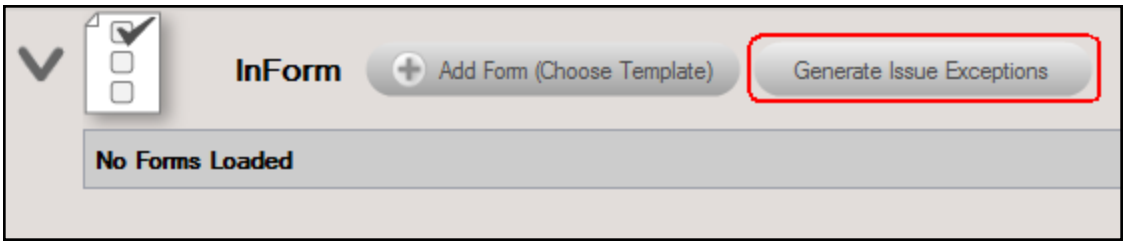
Upon viewing the **Issue Exceptions Worksheet** you will see that the Issues listed in the worksheet are the same risk issues are outlined in the **Risk Report**.

Process to Document Issue Exceptions

To access the **Issue Exception Worksheet** select, first, select the scroll bar next to the **Scans Bar** located at the bottom of the **Assessment Window**, and scroll down to the **InForm Bar**.

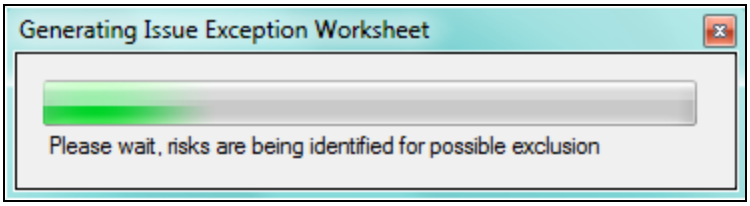


Then select the **Generate Issue Exception worksheet** option available on the **InForm Bar** located in the **Assessment Window** as presented below:

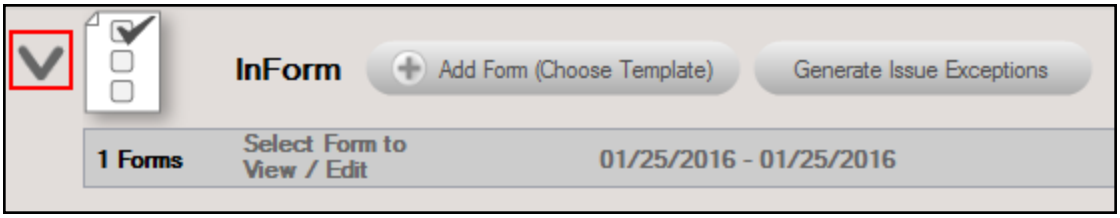


This action will result in an **Issues Exceptions Worksheet** being generated.

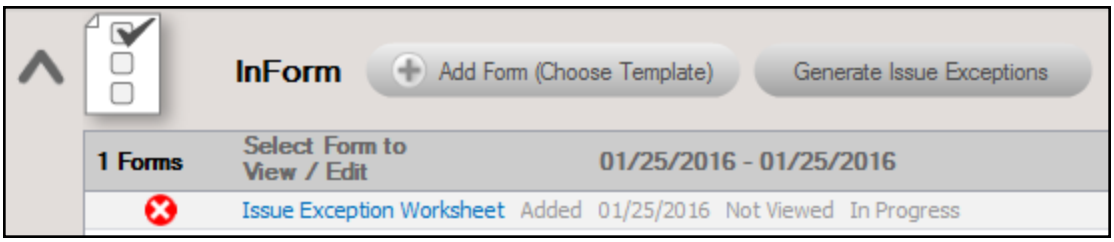
The **Generating Issue Exception Worksheet** status bar will be presented during the generation of the worksheet.



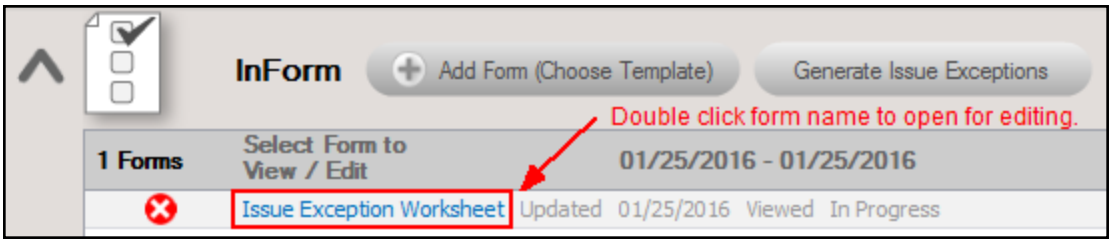
Once the **Issue Exception Worksheet** is generated, the **Issue Exception Worksheet** is added to the **InForm** section of the **Assessment Window.** Click on the selector control on the left of the **InForm Bar** to access the Issue **Exception Worksheet's** entry in the **InForm** list.



To view and edit the **Issue Exception Worksheet**, select the down arrow located on the left side of the **InForm Bar** to expand the list of forms/worksheets available for viewing below the **InForm Bar**.

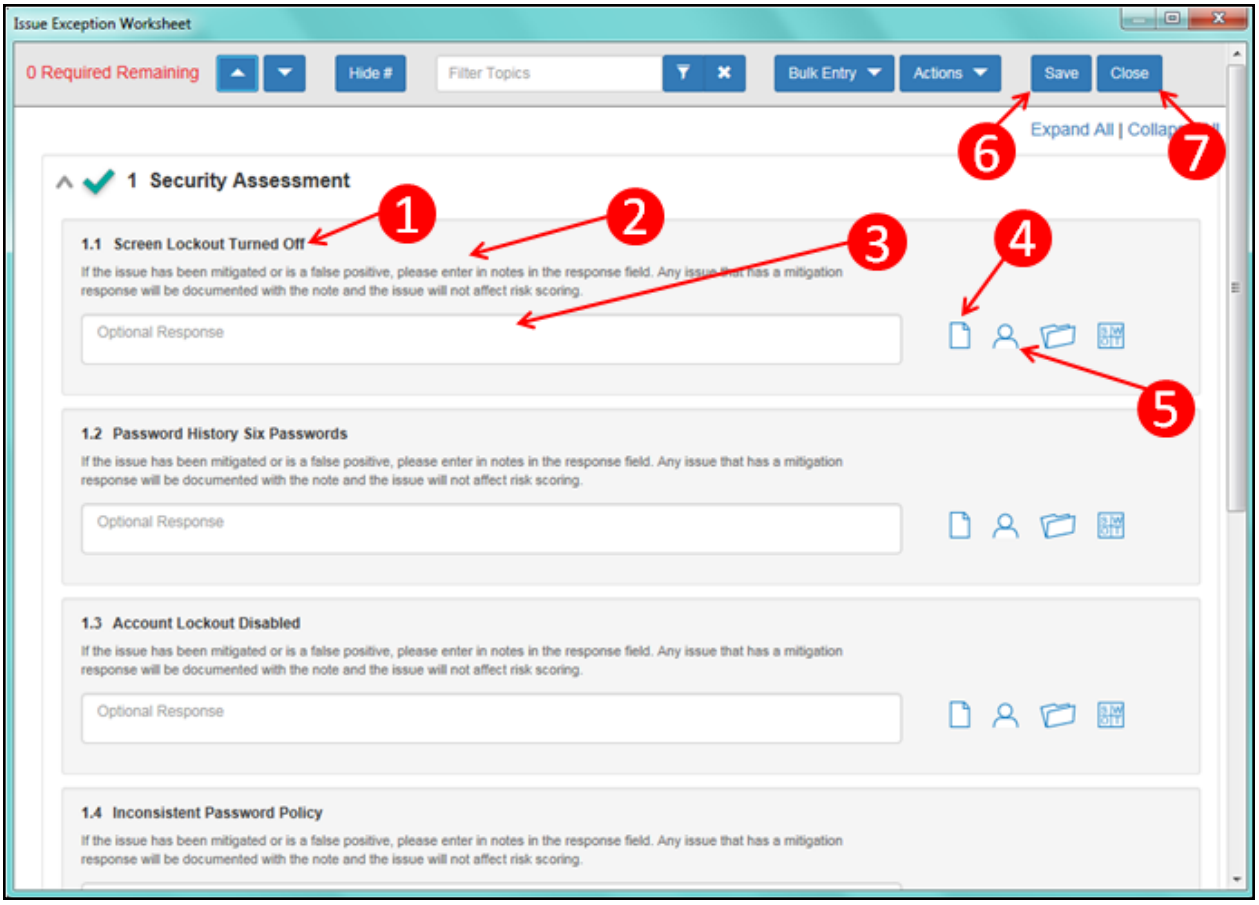


The **Issue Exception Worksheet** will become available for viewing and editing.



Double click on the **Issue Exception Worksheet** text denoted in Blue text to open the worksheet for viewing and editing.

Upon opening the **Issue Exception Worksheet**, the following window is presented:



Issues and their **Exception Responses** are listed in the Worksheet window to enable you to document "Responses" outlining the actions used to mitigate the **Issues** identified during the **Assessment**. Follow the steps below to review and document issue mitigation or clarification responses.

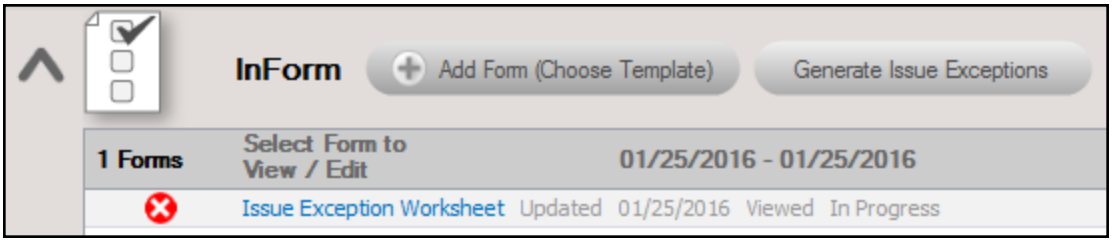
To document the "**responses**" to the Instructions/Questions presented in this worksheet:

1. Review the "**Topic Question**".
2. Review the "Instructions". Instructions provide guidance and are not included in the reports.
3. Enter the "**Response**" in the Response field. A **Response** must be given for each Issue entry to complete the worksheet if you want to remove these issues from the **Risk Report**.

> Note: **Please note that the Issue Exception Worksheet does not require a response for eachand every topic.** Enter your **Response** if applicable, otherwise, leave the entry blank.

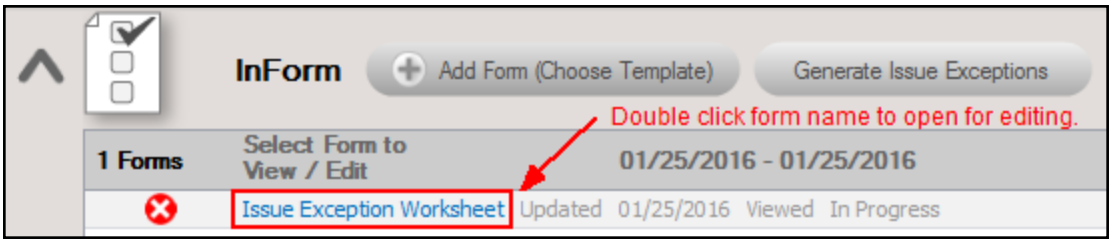
4. Select the **Notes** icon to enter any “Notes” relevant to a particular **Exception** mitigation action or explanation topic’s Response.
5. Select the **Respondent** icon to enter the name of individual that responded or provided information to respond to the topic’s question or requirement in the “Respondent” field.
6. Save your answers periodically and **Save** when you are done.
7. Select **Close** to close the worksheet when you are done.

Once the **Issue Exception Worksheet** is saved, it will be listed under the **InForm Bar** located in the **Assessment Window**. Click on the selector control on the left of the **InForm Bar** to access the Issue **Exception Worksheet’s** entry in the **InForm** list.



Please note that the **Issue Exception Worksheet** status indicator to the right of the worksheet name shows that the worksheet has been **Updated**.

You can return to the **Issue Exception Worksheet** to make any modifications by Double clicking on the **Issue Exception Worksheet** text denoted in Blue text.

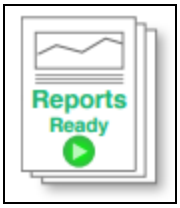


Tip: To learn more about how to save time completing Surveys and Worksheets, please see "Completing Worksheets and Surveys" on page 263.

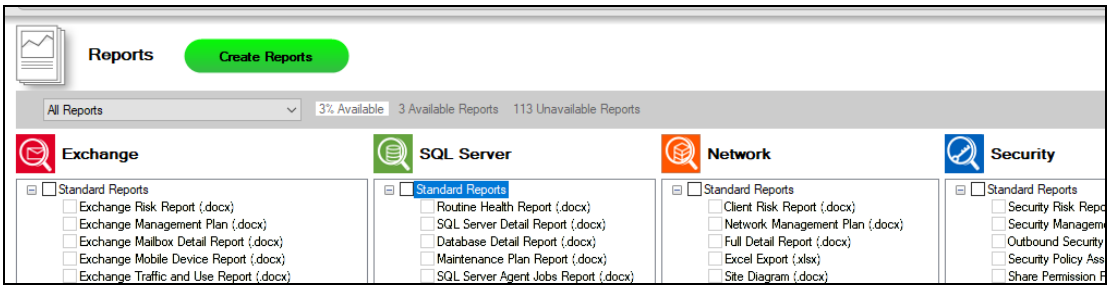
Phase 4 – Generating Security Assessment Reports

Steps to Generate Security Assessment Reports

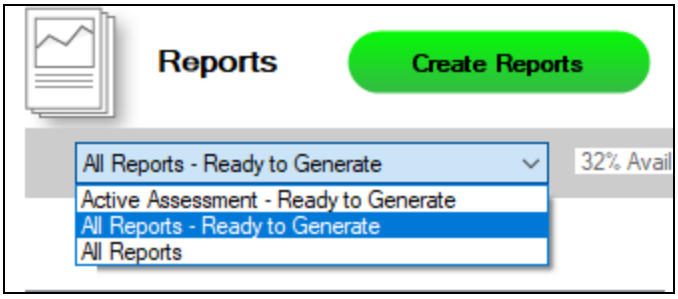
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



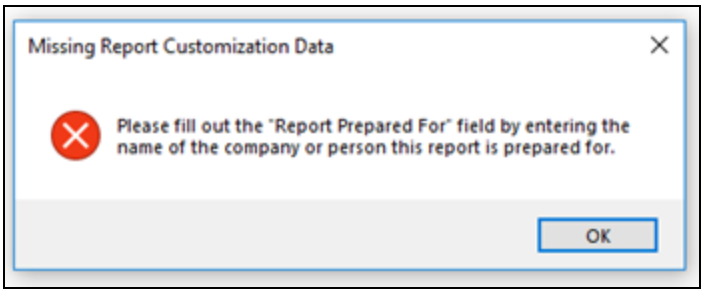
4. Select which of the Security Assessment reports that you want to generate.



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.

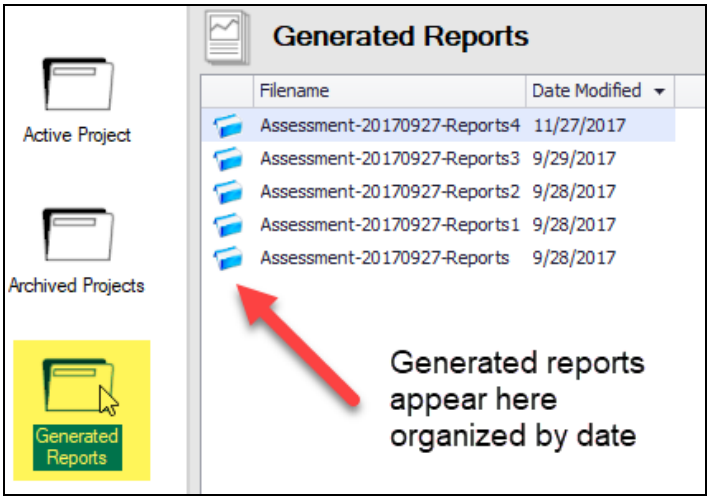


5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.
   i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



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.

Performing Security Assessments Required to Generate Change Reports and Quarterly Business Review Reports

In order to use Network Detective to generate Security Assessment Change Reports it is necessary to compare a past Security Assessment (i.e. Baseline Assessment) with the

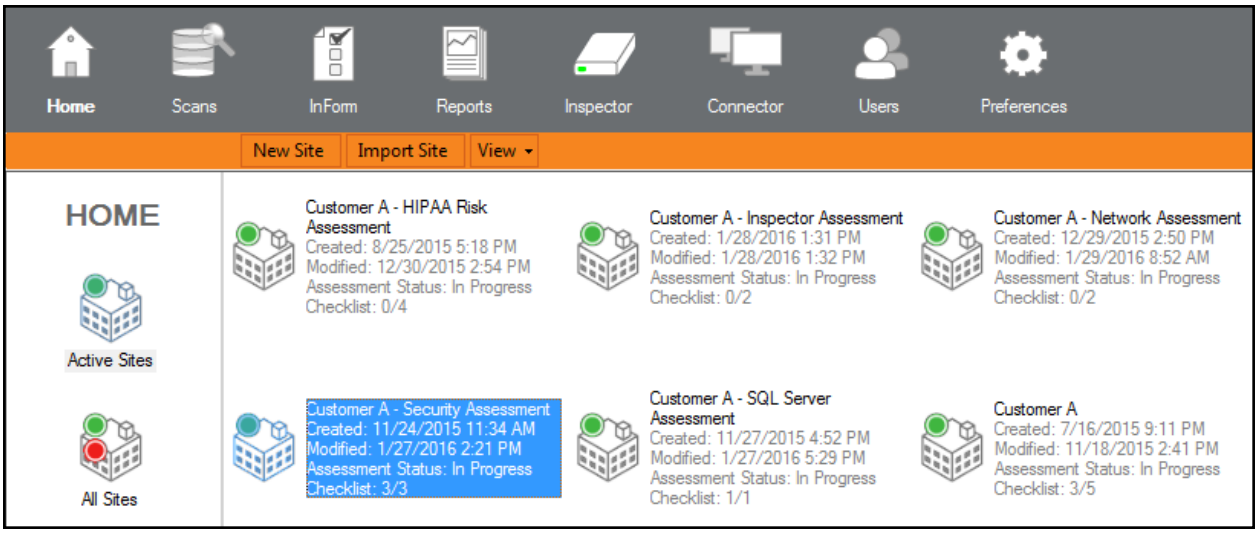
second (a new or more recent) Security Assessment.

Based on the content presented in the Security Assessment Change reports, two assessments are required in order to identify changes to the network over the time period that took place between the two assessments.

The steps to create a Security Assessment that enables the generation of Change Reports are below.

Step 1 – Select and Open a Site that Contains a Completed and Archived Security Assessment Project

Open the **Site** containing an **Archived Security Assessment** by double clicking on the **Site**.

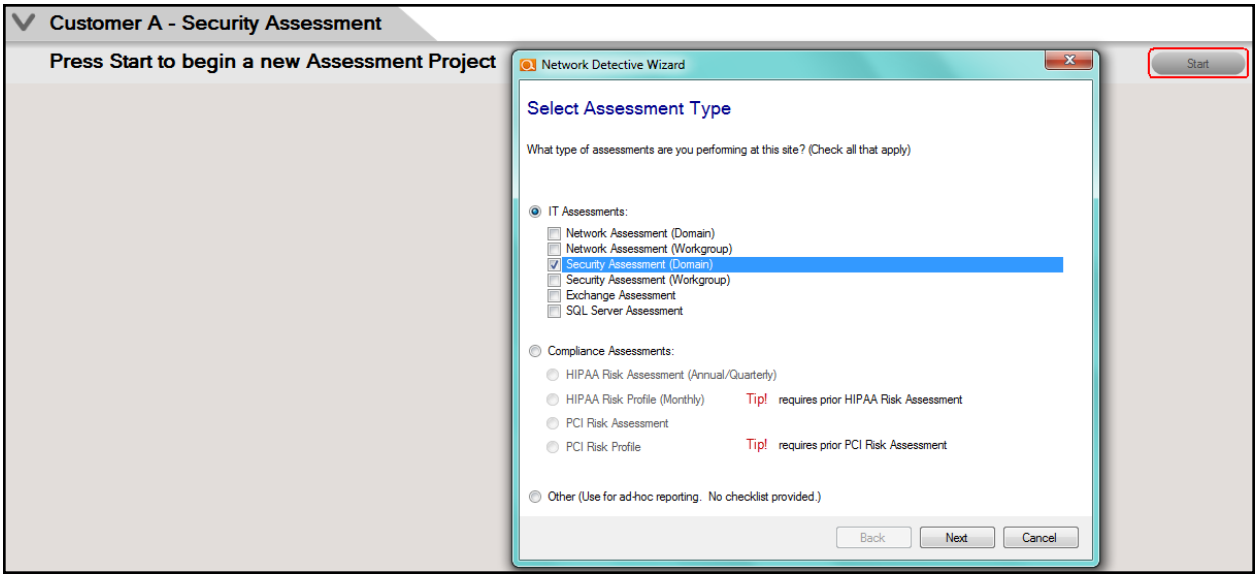


The **Start New Assessment** window will be displayed.

Step 2 – Create a new Security Assessment Project

If you already have a second Security Assessment Project to compare to the first "baseline" Security Assessment Project, then skip this step and go to step 3 below. If not, then proceed with Step 2 by performing the following actions.

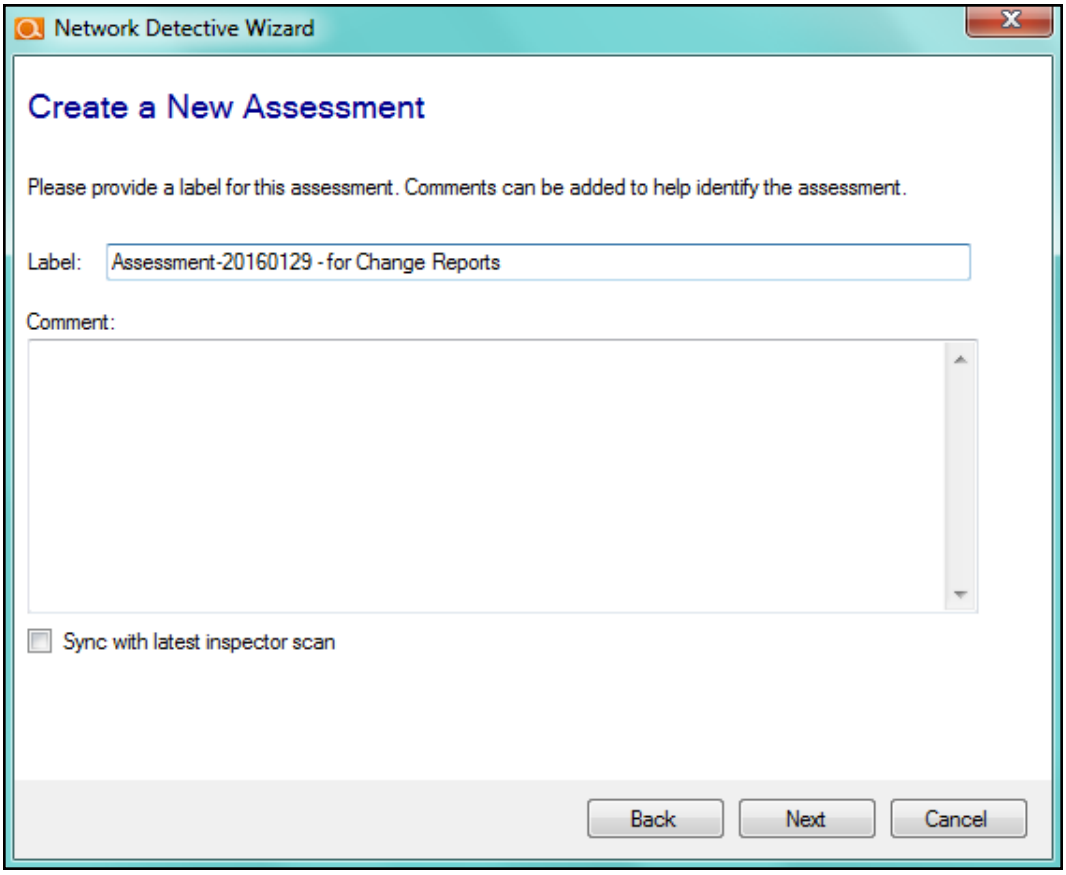
From the Site's Dashboard, click the "Start" button on the "Active Assessment" bar to start an Assessment project.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more Assessment Types.

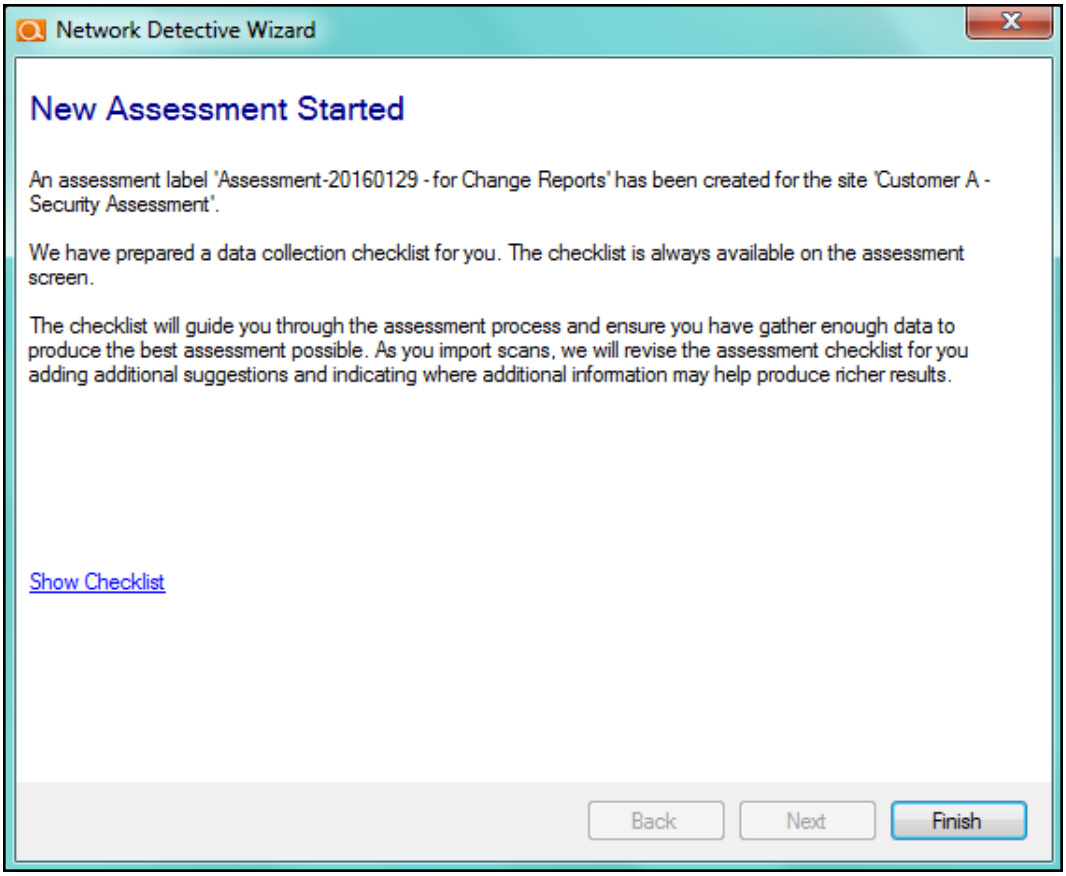
To create a Security Assessment Project, select the Security Assessment option and click on the **Next** button.



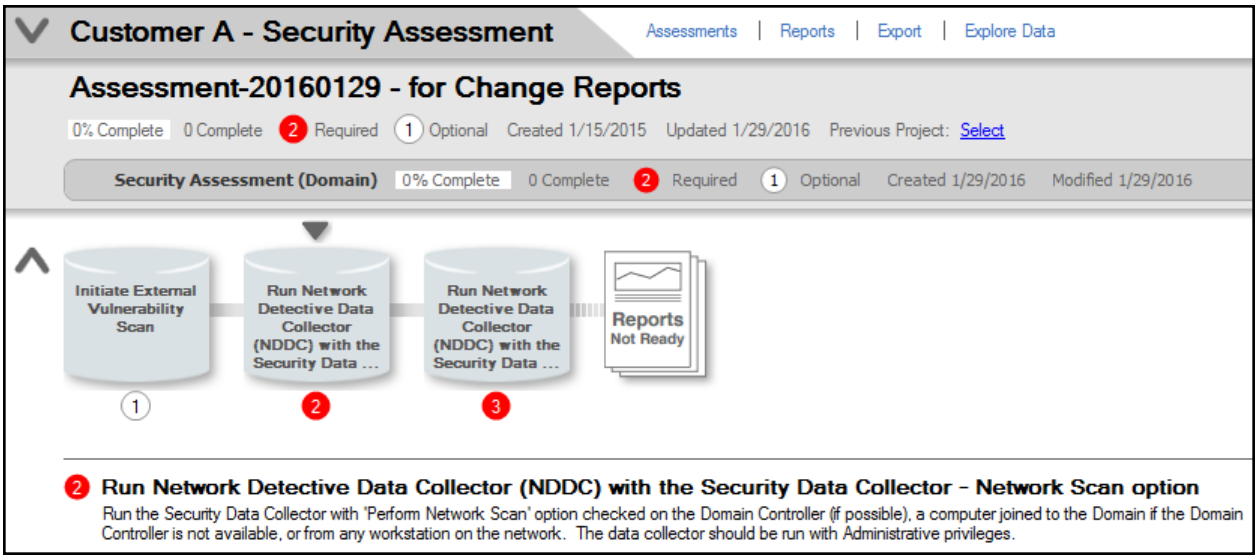
Enter a **Label** to identify the assessment.

Enter a **Comment** to help further identify the assessment.

Select the **Next** button to proceed to create/start the new Assessment.

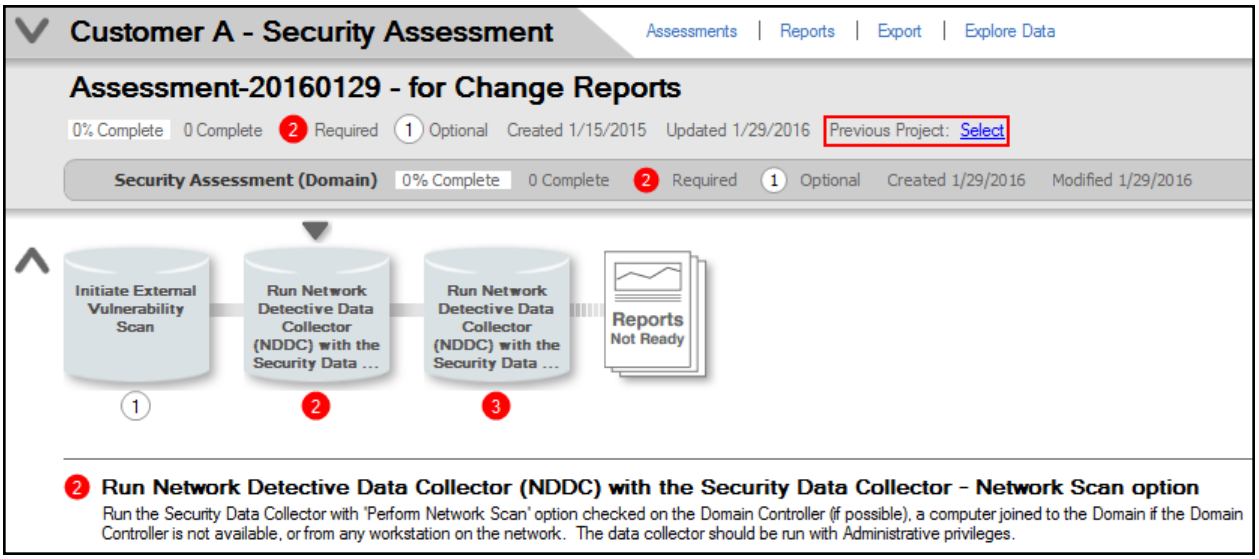


The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment**.

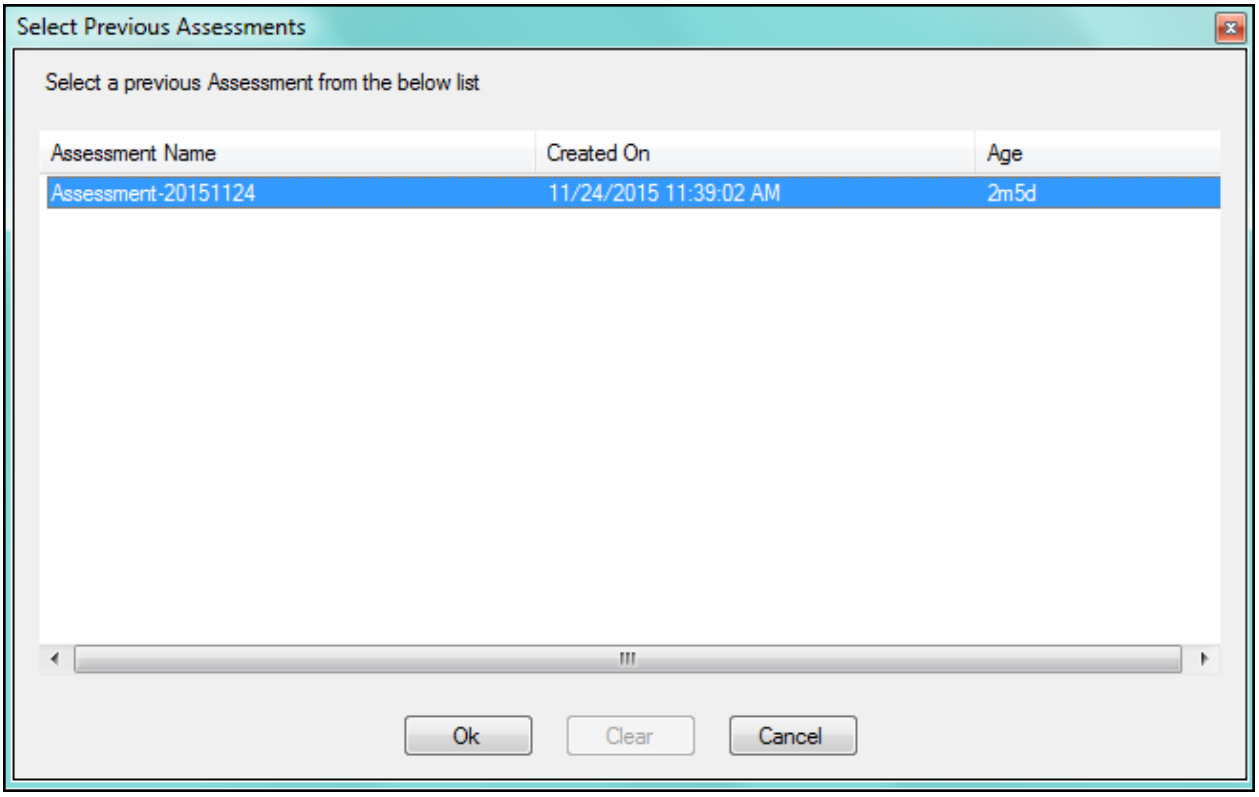


Step 3 – Select and Link a Previously Completed Security Assessment Project to the New Assessment Project for Comparison

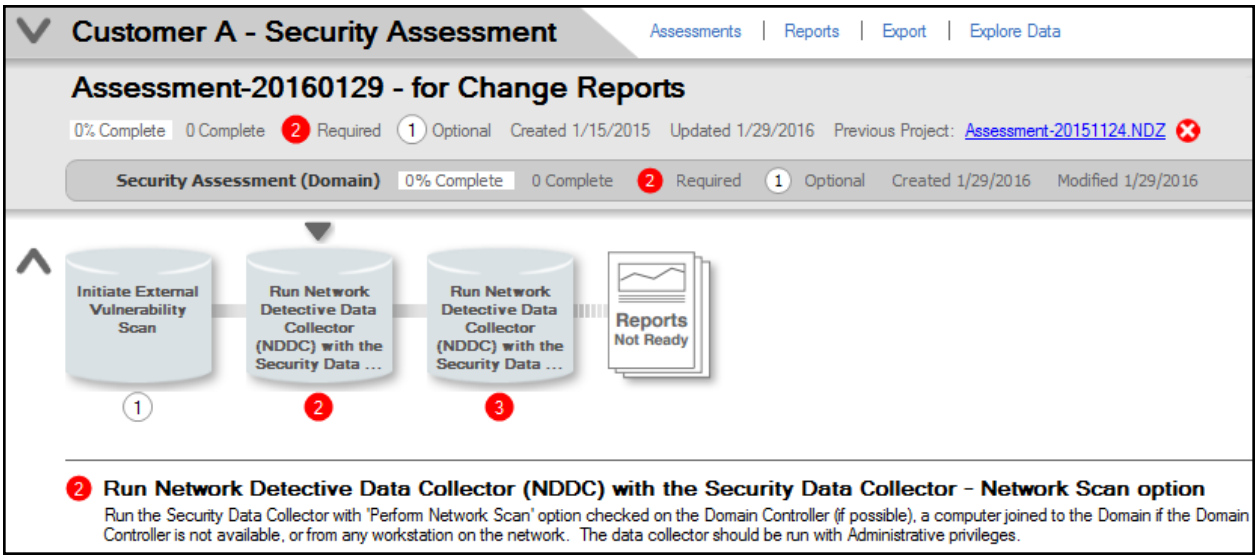
From within an **Active Assessment**, select the **Previous Project** link in order to select the previously completed **Security Assessment** from the **Archived** assessments associated with this **Site**.



This action will present the **Select Previous Assessments** window.



Select the previous **Assessment** from the list of assessments and click on the OK button to link the previous **Assessment** to the current **Assessment** for comparison and **Change Reporting** purposes.

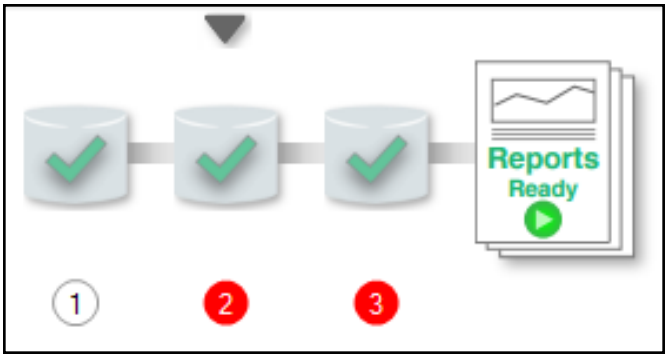


Step 4 – Perform Security Scans on the Network and Local Computers and Import Scan Data into the New Assessment Project

Based on the **Checklist**, perform the same scans that were performed in the **Previous Assessment Project** and import the scan data into this new **Security Assessment**.

These scans should include a **Security Scan** of the network and any security scans done on 2 or more local computers either using the **Push Deploy Tool** or the **Network Assessment Data Collector's Security Data Collector** scan option.

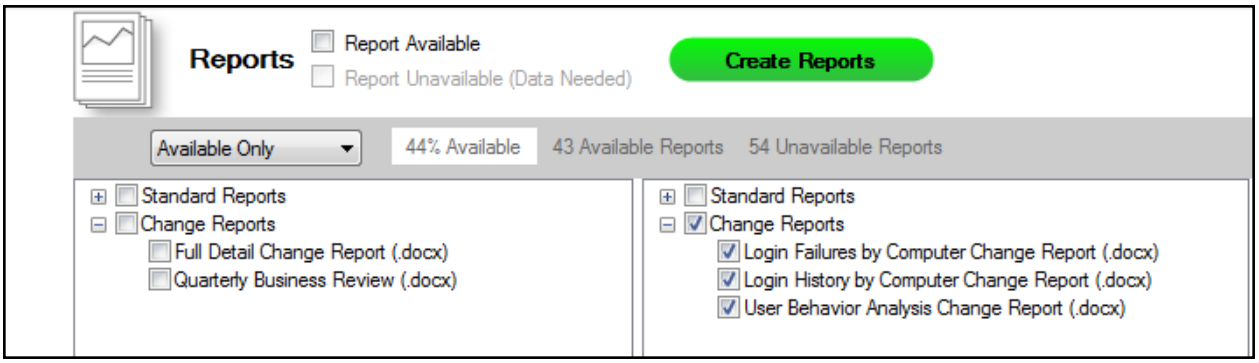
Once these scans are imported into the new **Security Assessment** the **Checklist** will indicate the **Reports** are ready to be generated.



Step 5 – Generate the Change Reports

Select the Reports link in the **Security Assessment** window to generate reports. This action will display the **Create Reports** window.

In the **Create Reports Window**, select the **Change Reports** you wish to generate by selecting the **Full Login Failures by Computer Change Report**, **the Login History by Computer Change Report**, and/or the **User Behavior Analysis Change Report**.



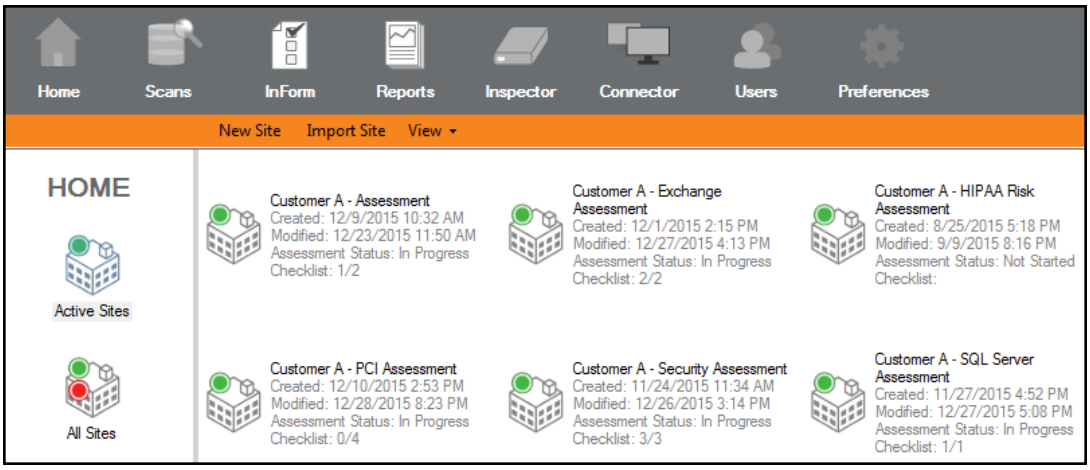
Then select the **Create Reports** button to produce the reports you have selected.

Enhancing Assessments by Adding an InForm Sheet to an Assessment Process

InForm surveys can be a valuable addition to **Site Assessments**. Information collected by a tech on-site or entered manually into a survey or worksheet template built using **InForm** will enable the tech to collect additional information during an assessment that can be compiled into the Network Detective Reports.

For more information, please review the section of this User Guide entitled "Using InForm to Build Questionnaire Worksheet and Survey Templates for Enhanced Assessment Data Collection" on page 235.

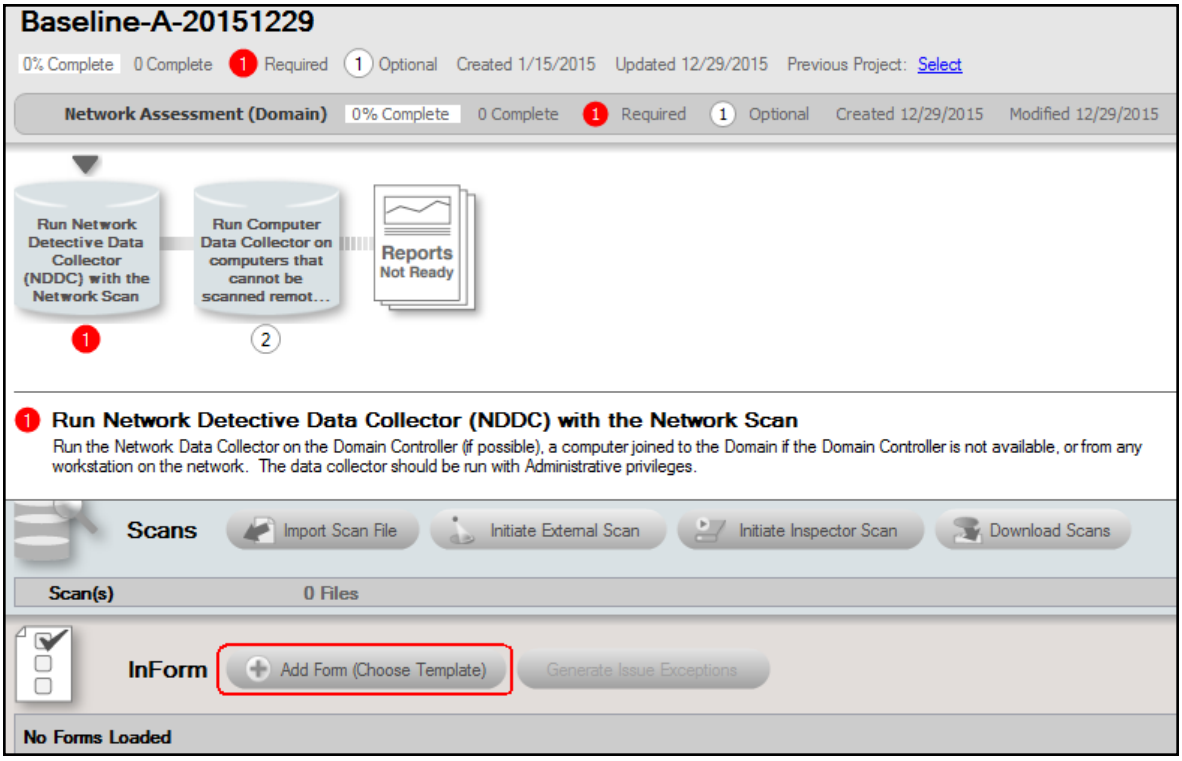
The Site Model allows you to create and edit InForm sheets from within the Assessment.



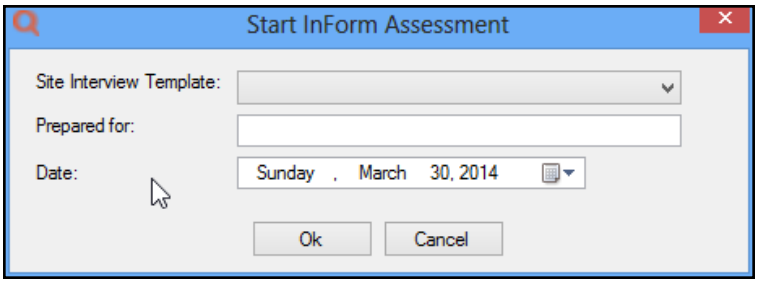
To add an **InForm** sheet to your **Assessment Project**, first navigate to the desired **Site** from the Home screen by double-clicking on its icon.

This will bring you to the Dashboard of the Site's current Assessment.

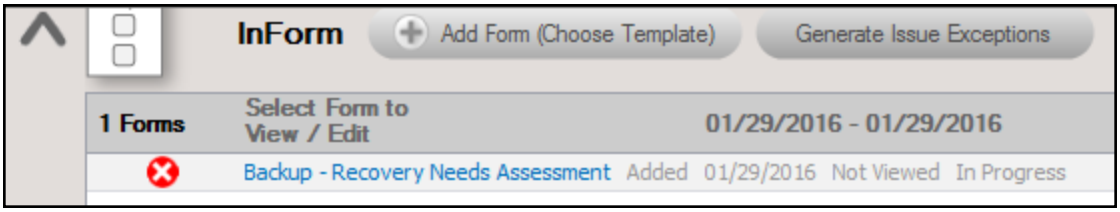
From the Assessment's Dashboard, select "**Add Form**" under the **InForm** bar.



Using the **Start InForm Assessment** dialog box, select your template, type in the name of your customer in the “Prepared for” field, and click “Ok.”



The new template will be listed under the **InForm** bar. Click the Inform template name that is in Blue text link to open and use your template.



Performing an Exchange Assessment

To perform a Exchange Assessment, complete the four phases detailed in this guide.

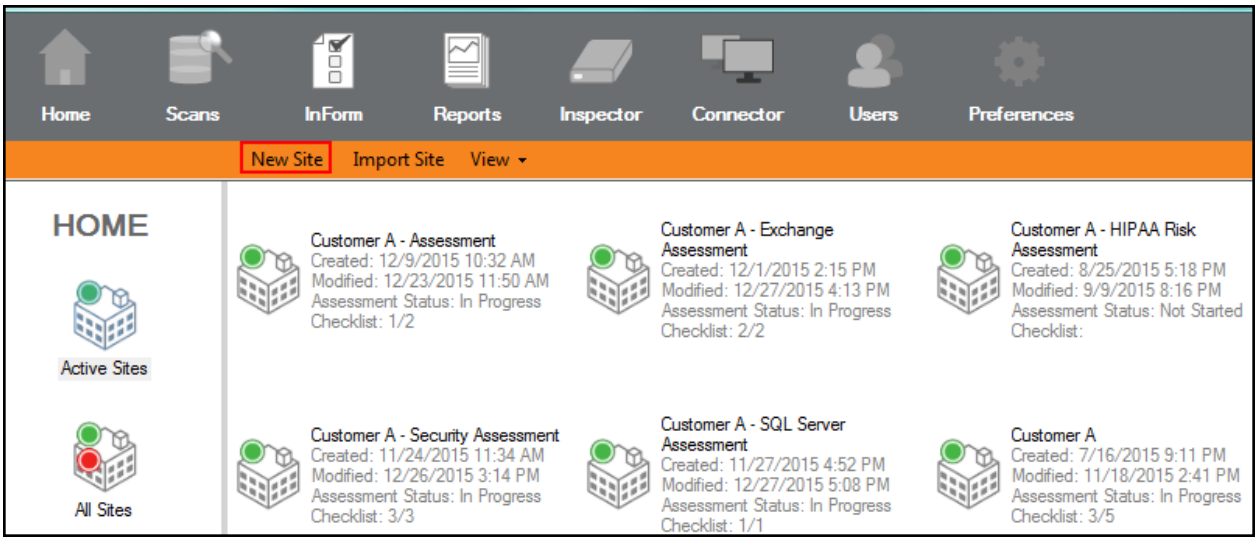
Phase 1 – Initial Exchange Assessment Project Setup

Creating a Site

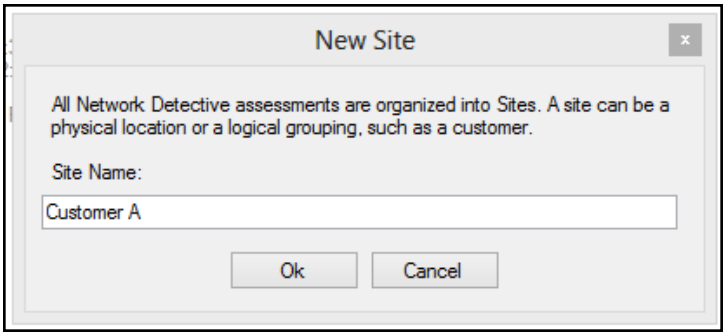
The first step in the assessment is creating a **"Site"**. All Network Detective assessment projects are organized into Sites. A **Site** can be a physical location or a logical grouping, such as a customer account name.

a. For a single location you will create one **Site**.

b. For organizations with multiple locations you must decide if you want one set of reports, or separate reports for each location.



Select **New Site**.



Enter the **Site Name**. For sites with multiple locations, enter a more detailed description.

Setting Report Branding for a Site

Reports produced by Network Detective can be “branded” with your company’s standards through the use of the **Reports Preference**s feature. Report Branding can be set at the **Global Level** (for all Sites), or at the **Site Level**. If you want to set the **Report Preferences** at the **Site Level**, please go to "Set Up Network Detective Reports" on page 16.

Adding a Connector to a Site

To add a Connector to a **Site**, please go to "Adding a Connector to a Site" on page 255.

Note: Also see the Network Detective Remote Data Collector User Guide.

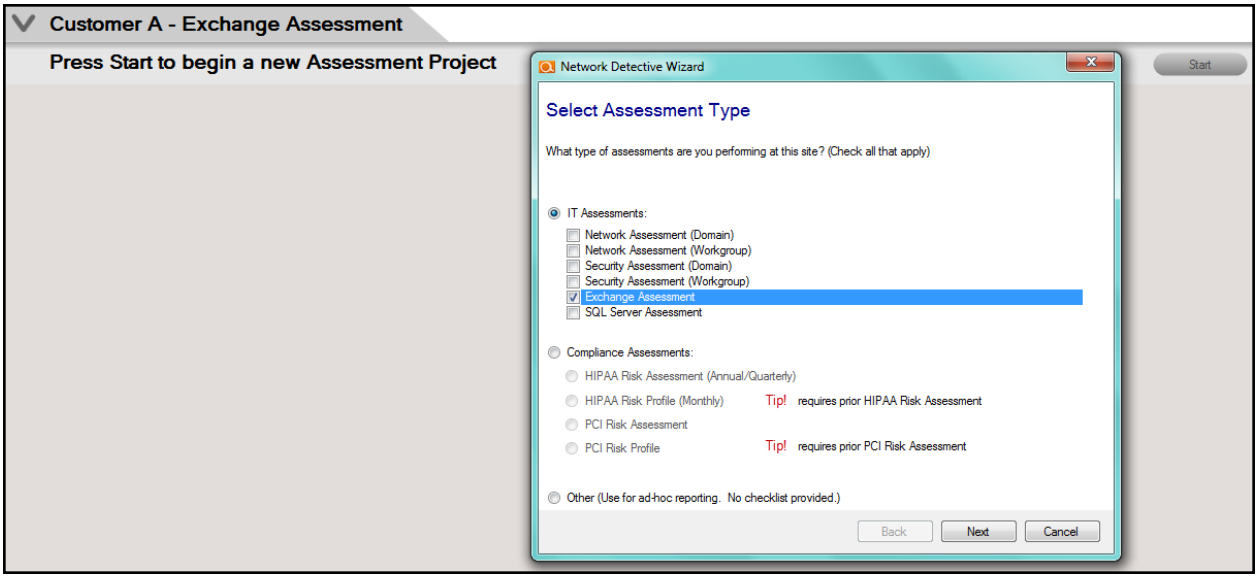
Adding an Inspector to a Site

To add an Inspector to a **Site**, please go to "Adding an Inspector to a Site" on page 257.

Phase 2 – Starting an Exchange Assessment Project

Starting an Exchange Assessment Project

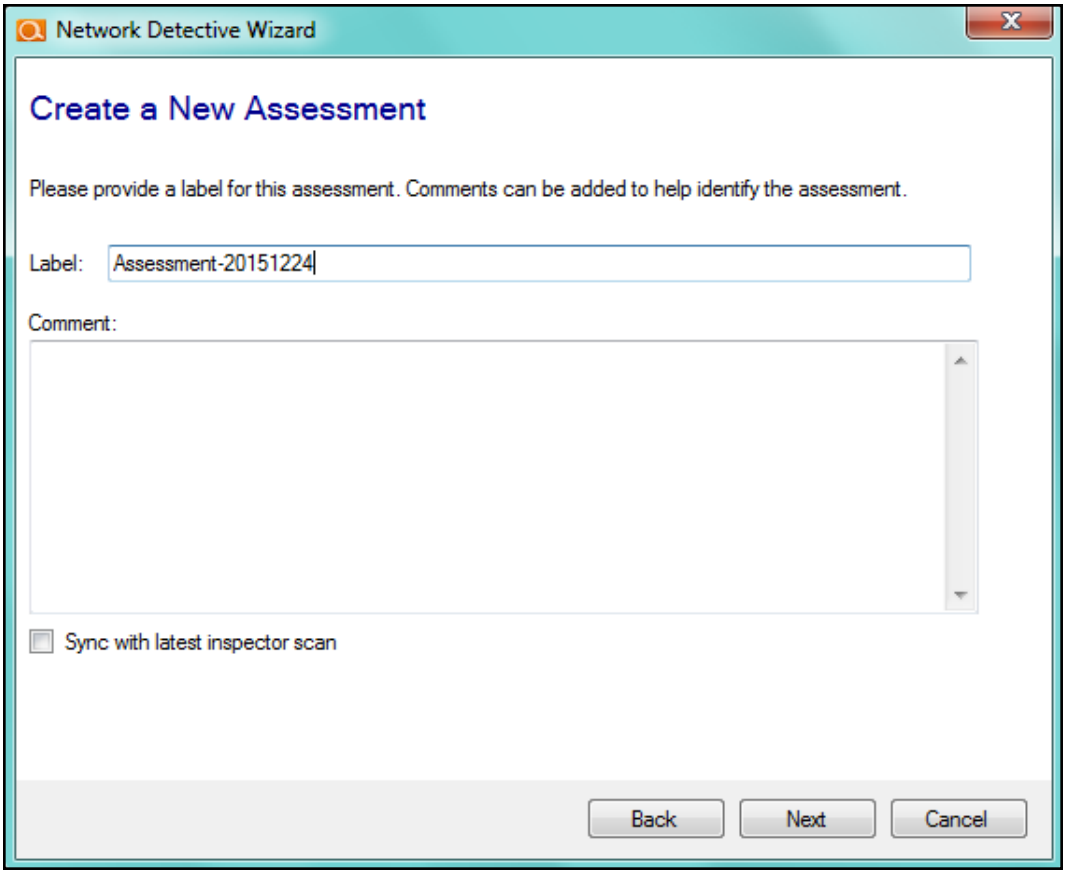
From the Site's Dashboard, click the "Start" button on the "Active Assessment" bar to start an Assessment.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more **Assessment** types.

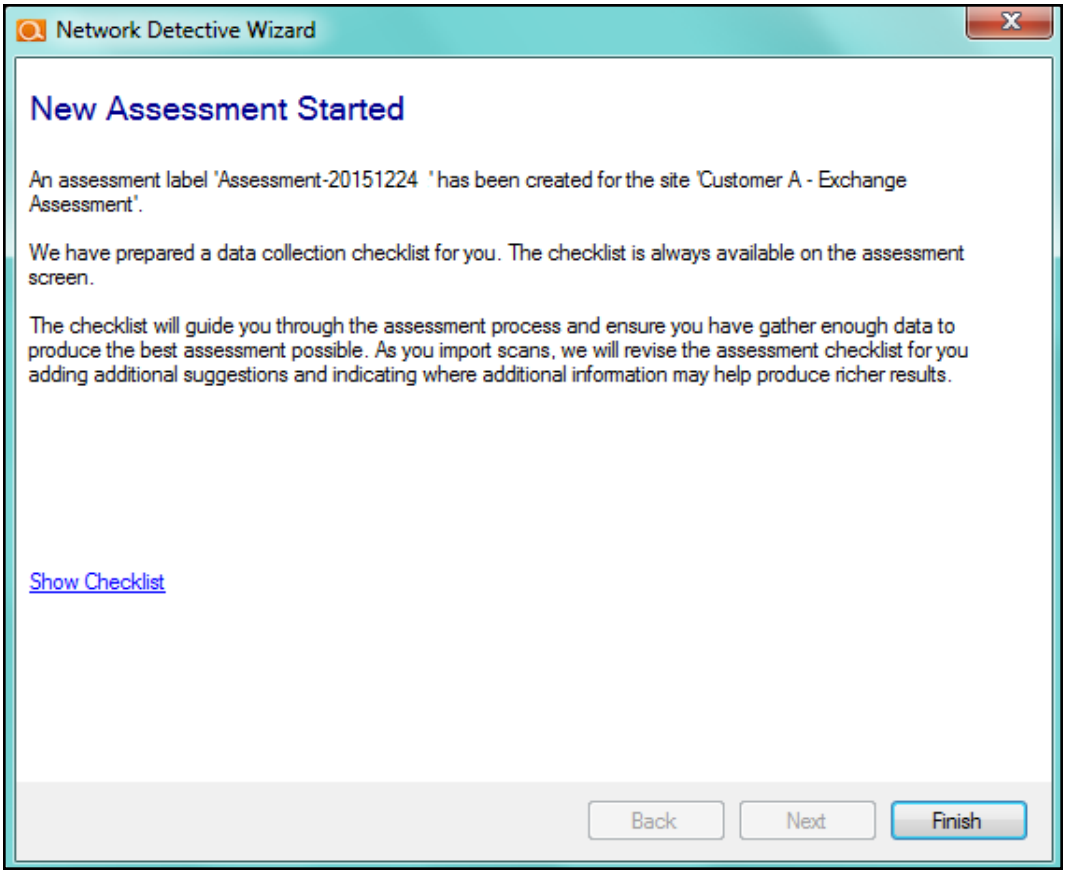
To create an Exchange Assessment Project, select the Exchange Assessment option and click on the **Next** button.



Enter a **Label** to identify the assessment.

Enter a **Comment** to help further identify the assessment.

Select the **Next** button to proceed to create/start the new Assessment.



The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment**.

Phase 3 – Performing the Assessment and Data Collection

Process to Run the Exchange Server Scan Using the Exchange Assessment Data Collector and Import Scan Results

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

The Data Collector makes use of multiple technologies/approaches for collecting information on the Microsoft Exchange environment depending on the version of Exchange. Remote protocols are used to access Office 365 environments, while the use of local PowerShell and CmdLets that are specific for Microsoft Exchange are used for local scans.

In most cases, the Microsoft Exchange server will already have PowerShell and the proper CmdLets installed. During the scan start phase, the Exchange Assessment Data Collector will check for pre-requisites before performing its scan.

For local Exchange 2003, 2007, 2010, 2013, and 2016 installations, the Exchange Assessment Data Collector must be run on the server running Exchange.

Step 1 – Running the Exchange Assessment Data Collector to Perform an Exchange Scan

Visit the RapidFire Tools software download website to download and then run the Exchange Data Collector file.

The Exchange Assessment Data Collector is a self-extracting zip file that executes an ".EXE". Use the **Unzip** option to unzip the files into a temporary location, or a location more convenient for you to access if needed and start the collector.

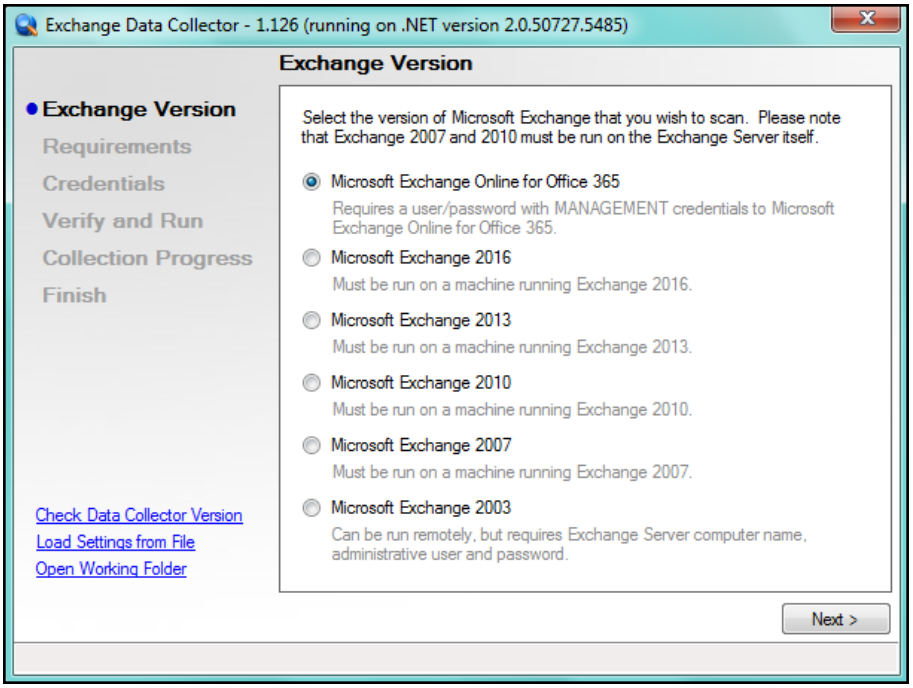
Note: Please note: When installing the Exchange Data Collector it is recommended that you do not use the default folder (directory) name the Data Collector recommends. Please create and use a Folder name that is similar to the following: Drive Letter:\Download\Exchange Assessment

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

Using this folder name or another folder name that is easy for you to access may be helpful in case you are asked to provide log files produced by the Exchange Data Collector to the RapidFire Tools Help Desk Team. The log files are stored in the folder that you use to run the Exchange Data Collector.

Step 2 – Configure the Exchange Data Collector to Perform the Microsoft Exchange Scan

Starting the **Exchange Data Collector** application will present the following screen.



Next, select the version of Microsoft Exchange that you need to scan.

Note: Note: The scan for Microsoft Exchange Online for Office 365 can be done from any Internet connected PC; however, the scans on Microsoft Exchange 2003, 2007, 2010, 2013, and 2016 systems must be run from the actual server Microsoft Exchange is running on from an account with administrative credentials.

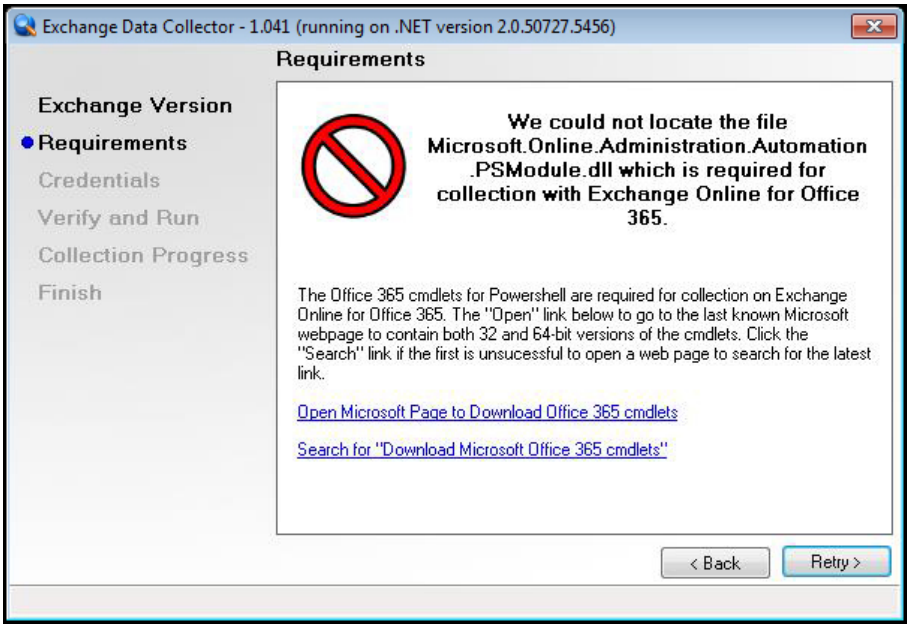
Select the **Next** button and the **Credentials** window will be presented.

Step 3 – Verify Required Files are Present to Perform the Scan

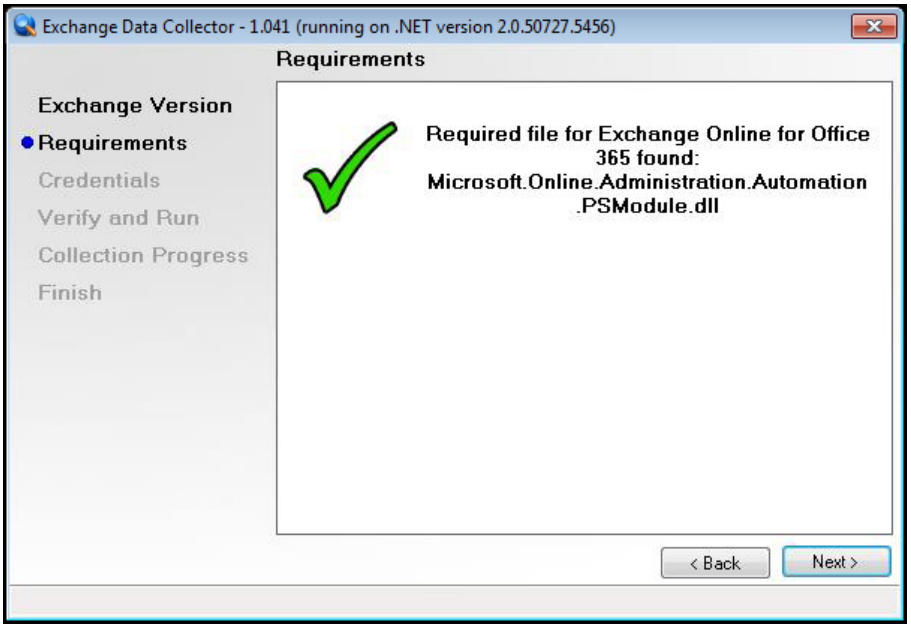
Prior to a scan taking place, the Exchange Data Collector checks for the presence of files that are required to enable the scan to be performed.

Microsoft Exchange Online for Office 365

Office 365 requires a file named **Microsoft.Online.Administration.Automation.PSModule.dll** to be present. If the wizard cannot find this file, the following error message will displayed.

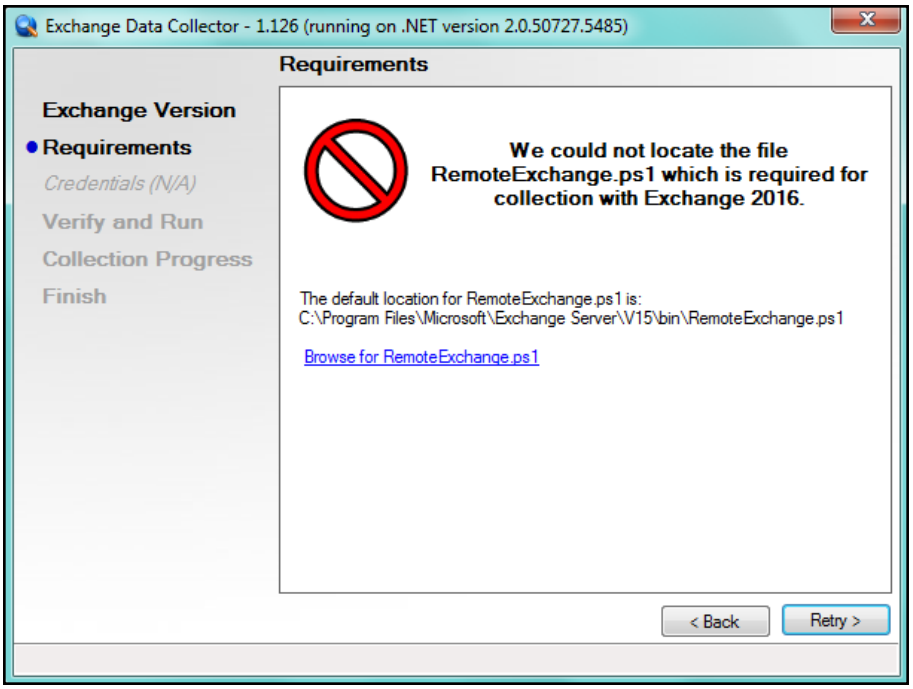


If the wizard can successfully discover the file, the following confirmation screen will be displayed:

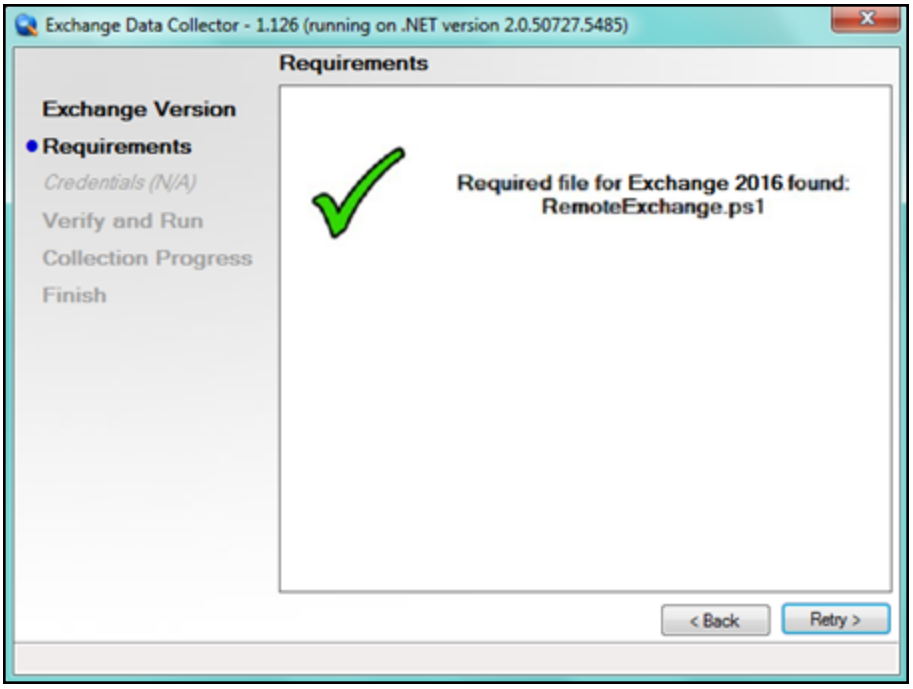


Microsoft Exchange 2016

Exchange 2016 requires a file named **RemoteExchange.ps1** to be present. If the wizard cannot find this file, the following error message will be displayed:

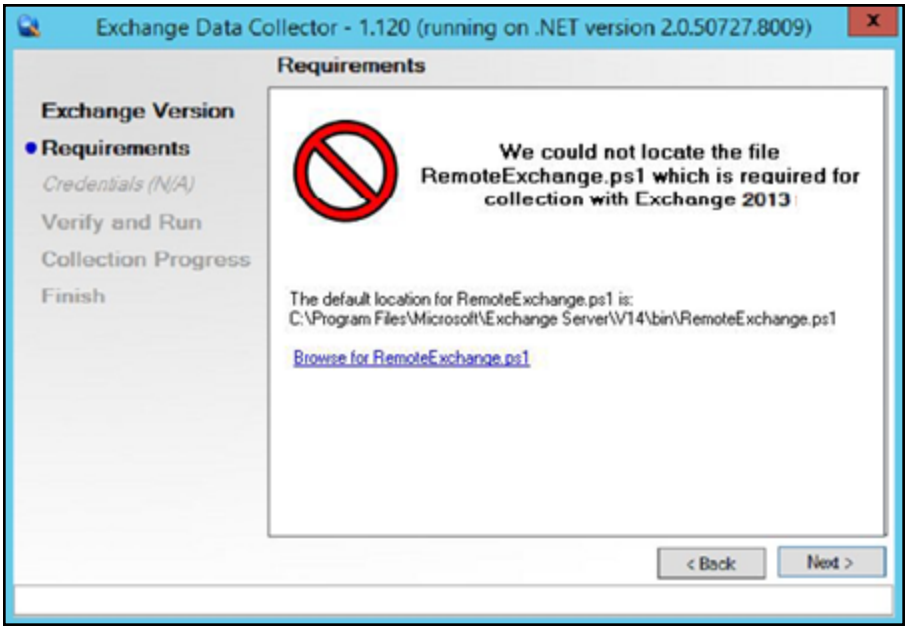


If the wizard can successfully discover the file, the following confirmation screen will be displayed:

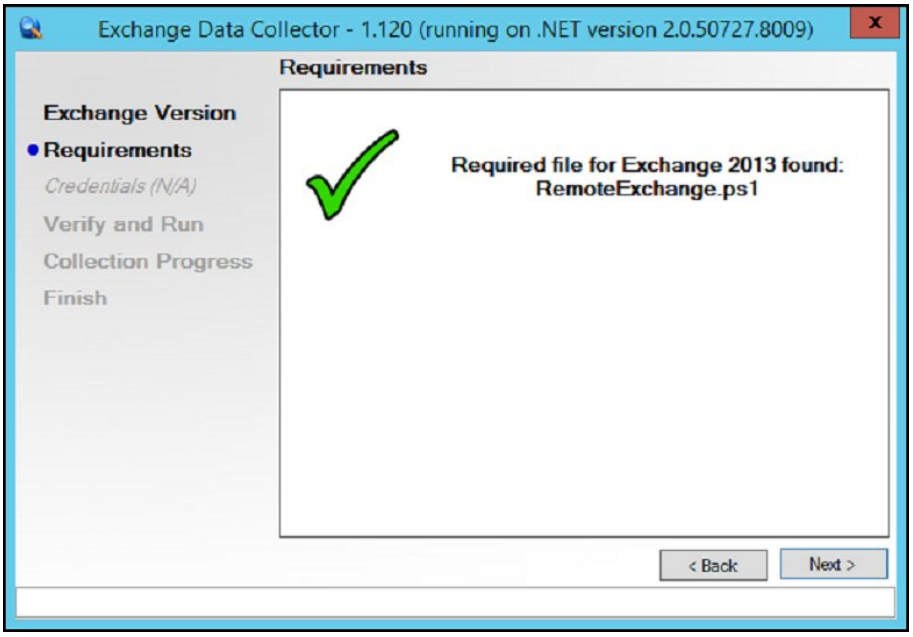


Microsoft Exchange 2013

Exchange 2013 requires a file named **RemoteExchange.ps1** to be present. If the wizard cannot find this file, the following error message will be displayed:

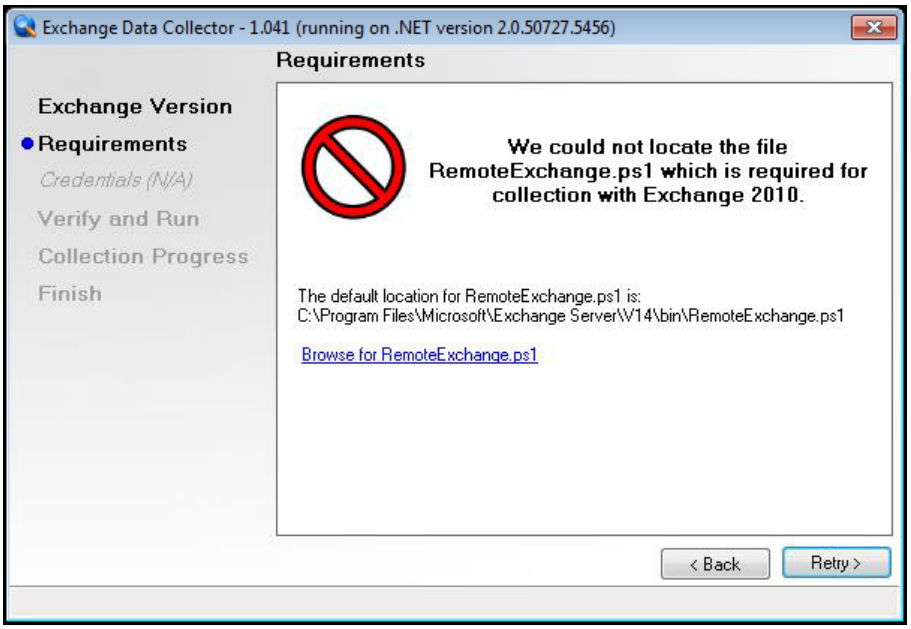


If the wizard can successfully discover the file, the following confirmation screen will be displayed:

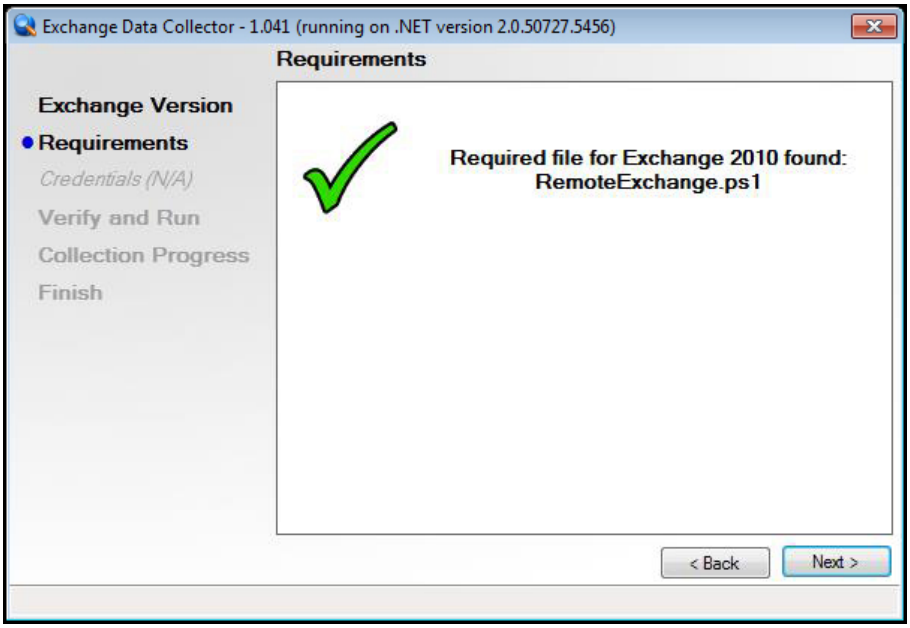


Microsoft Exchange 2010

Exchange 2010 requires a file named RemoteExchange.ps1 to be present. If the wizard cannot find this file, the following error message will be displayed:

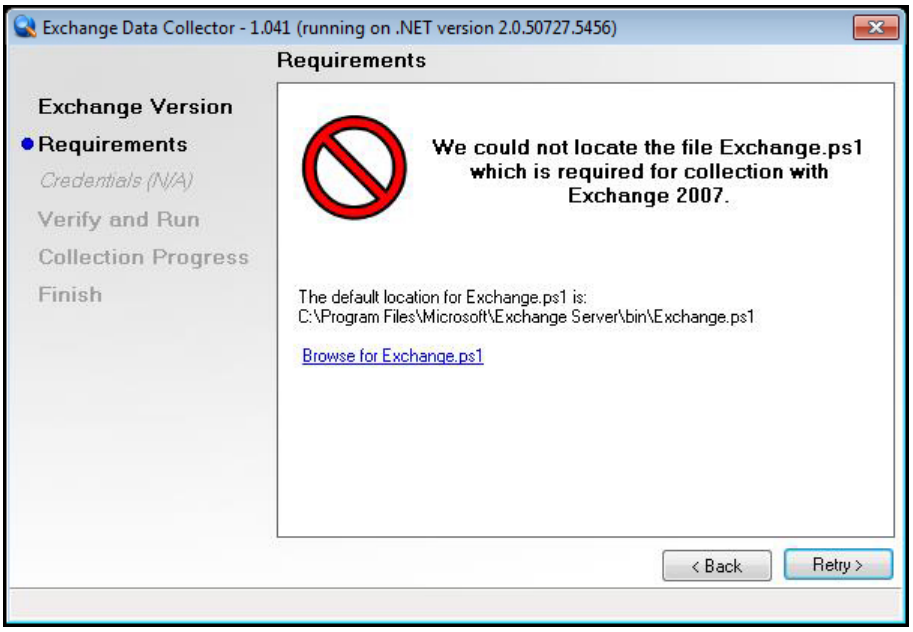


If the wizard can successfully discover the file, the following confirmation screen will be displayed:

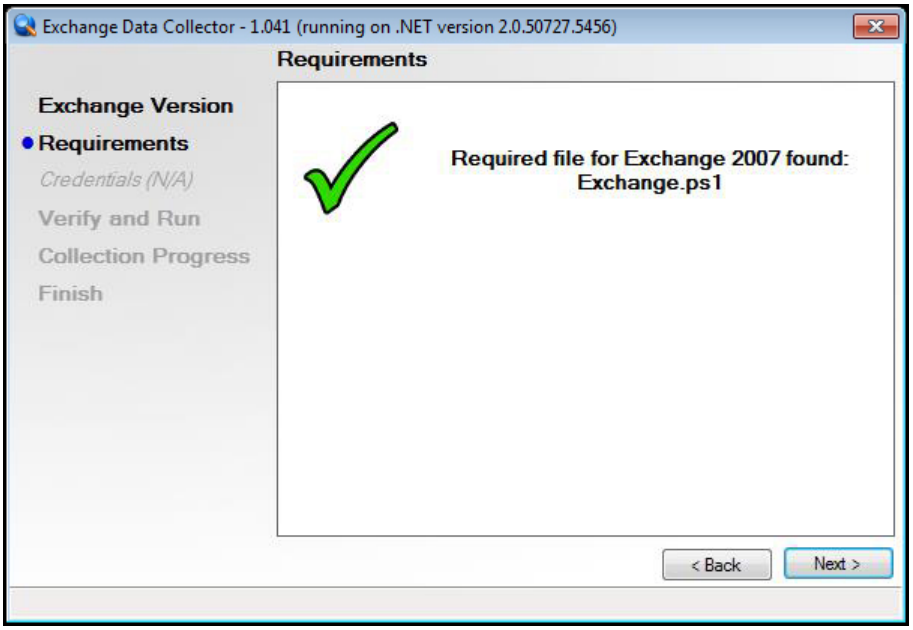


Microsoft Exchange 2007

Exchange 2007 requires a file named **Exchange.ps1** to be present. If the wizard cannot find this file, the following error message will be displayed:



If the wizard can successfully discover the file, the following confirmation screen will be displayed:

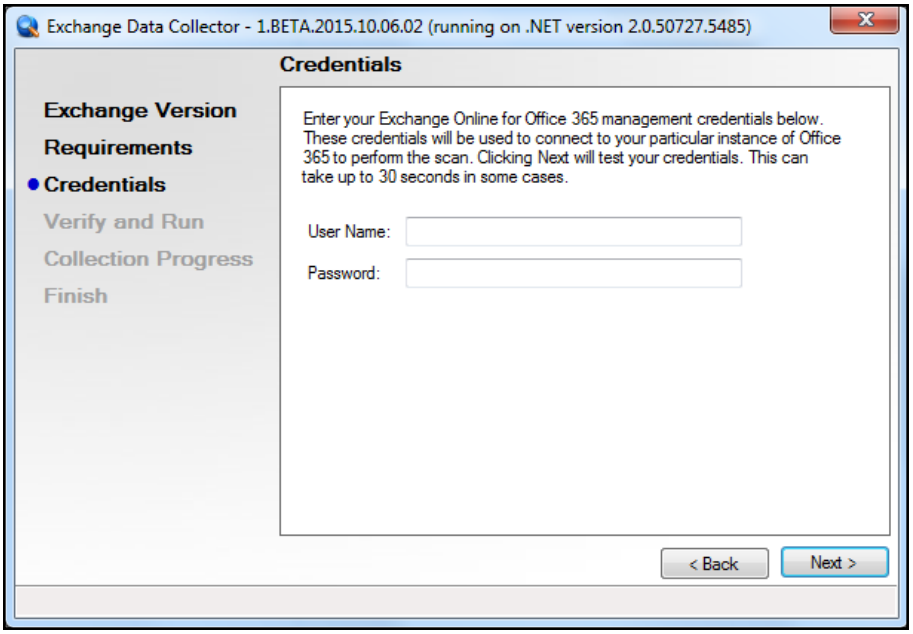


Microsoft Exchange 2003

When the Exchange Data Collector successfully initializes the scan process, you will be required to input the Credentials for the Exchange Server as detailed in Step 4 below.

Step 4 – Input Credentials

The **Credentials** window will be displayed to enable you to input your credentials for **Office 365.** (If you selected **Microsoft Exchange 2016**, **2013**, **2010**, or **2007** in Step 2, this step will be grayed out and the wizard will skip to Step 5.)



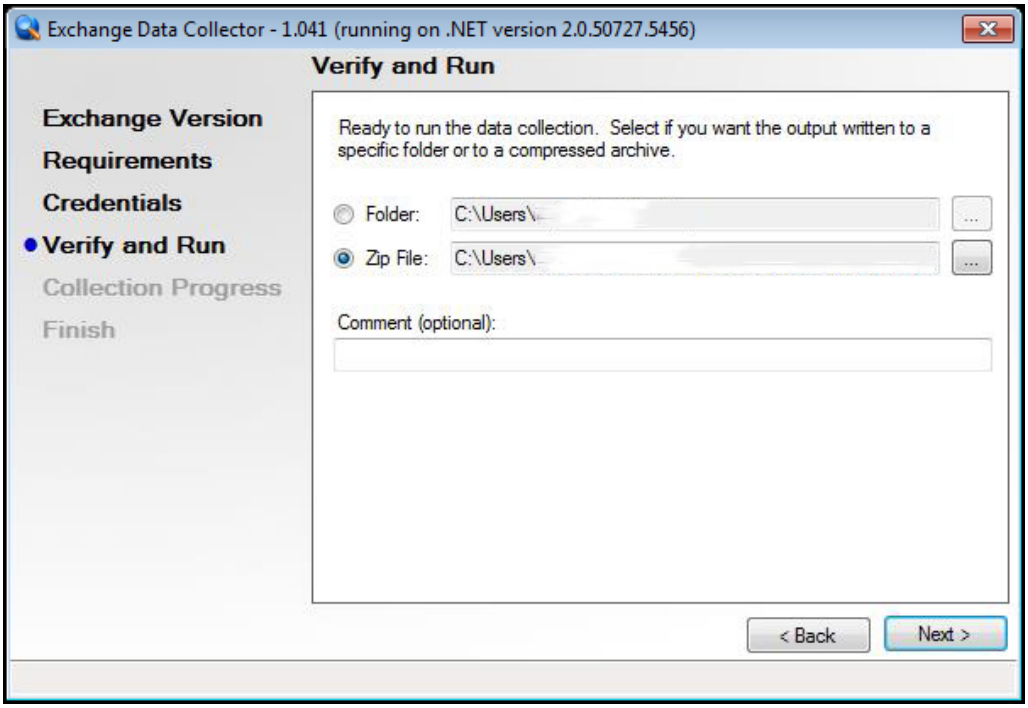
Enter the **Credentials** by performing these steps:

1. Enter a username and password for **Office 365** or the **Exchange Server** you are scanning.
2. Select the **Next** button.
3. Enter a username and password for **Office 365** or the **Exchange Server** you are scanning.

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

Step 5 – Verify and Run the Scan

Select the folder that you want to store the scan data file in after the scan is completed.



This page asks you to specify a destination for the output files of your scan. You have the option of outputting to a folder, or you can output to a compressed .zip file.

Starting the Exchange Assessment Scan

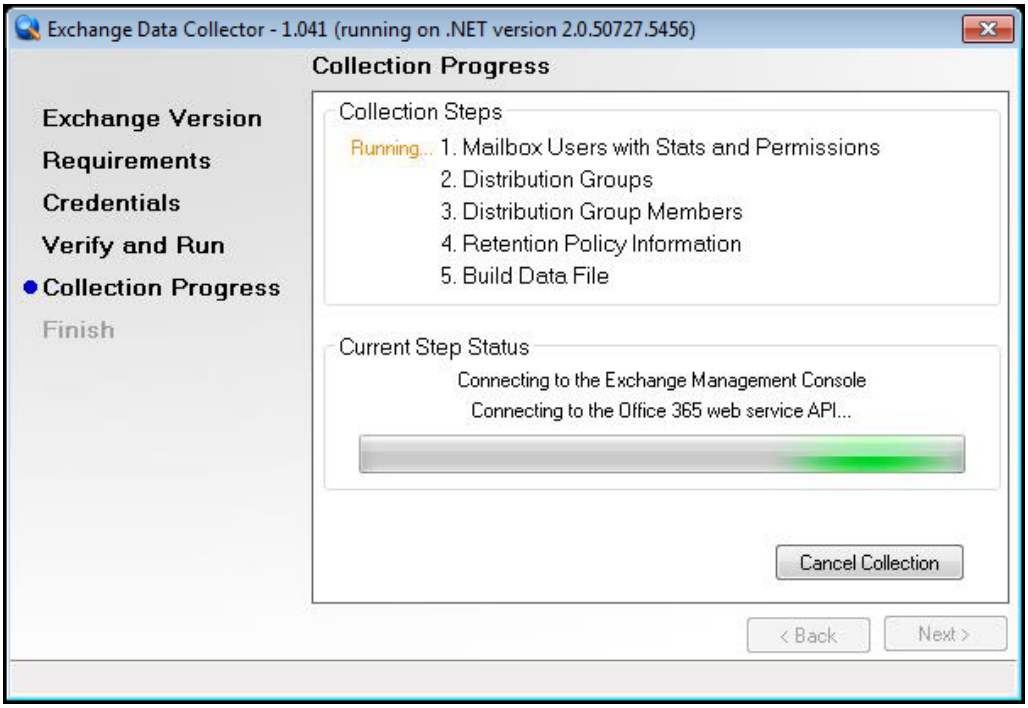
Once the **File Folder** location or the **.ZIP file** location for the scan data has been specified, enter any **Comments**, and then select the **Next** button to initiate the scan.

Once the scan is started, the scan's **Collection Progress** window will then be displayed.

Step 6 – Monitor the Exchange Assessment Scan's Collection Progress

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

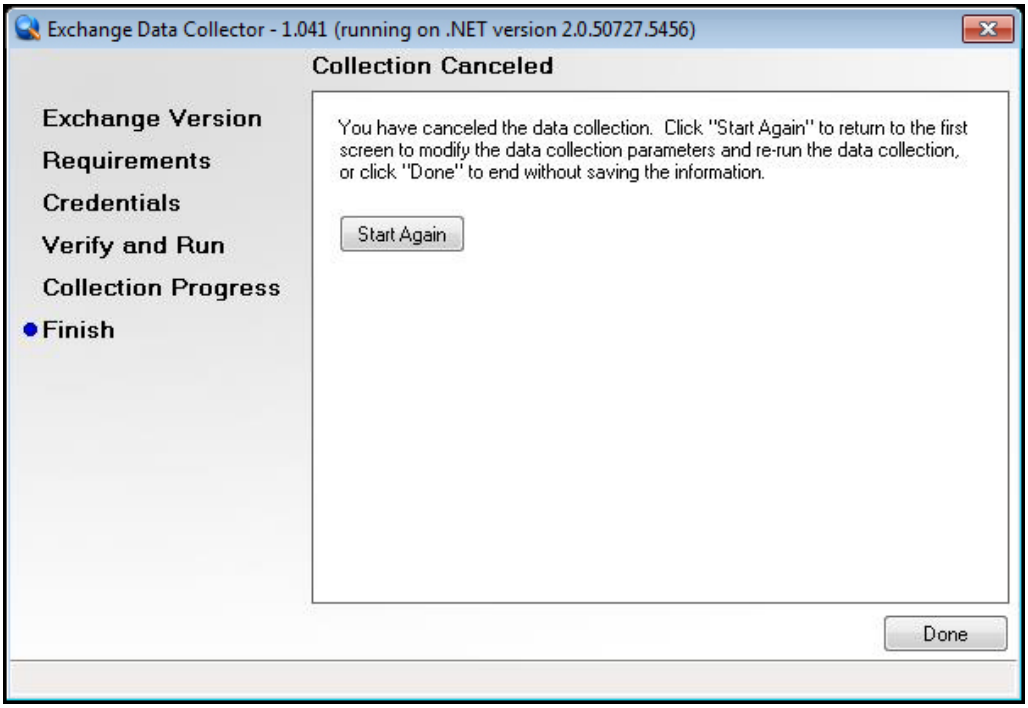
The **Collection Progress** window presents the progress status of a number of scanning processes that are undertaken.



This page charts the progress of your scan.

At any time you can **Cancel Data Collection** which will not save any data.

Canceling the Exchange Data Collection process will display the following window.

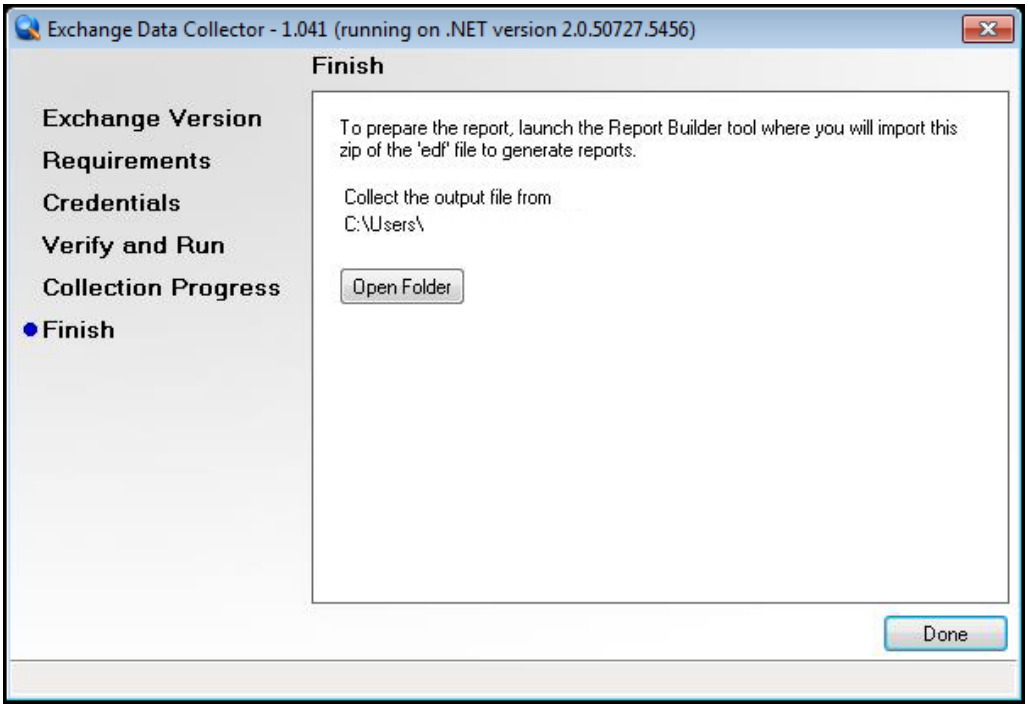


If the scan cancellation was done in error, you have the option to “Start Again.”

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

Step 7 – Complete the Exchange Data Collector Scan Process

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

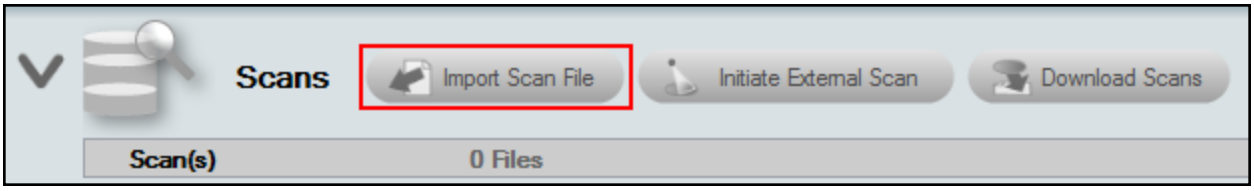


Click on **Done** button to close the **Exchange Data Collector** window. Note the location where the scan’s output file is stored.

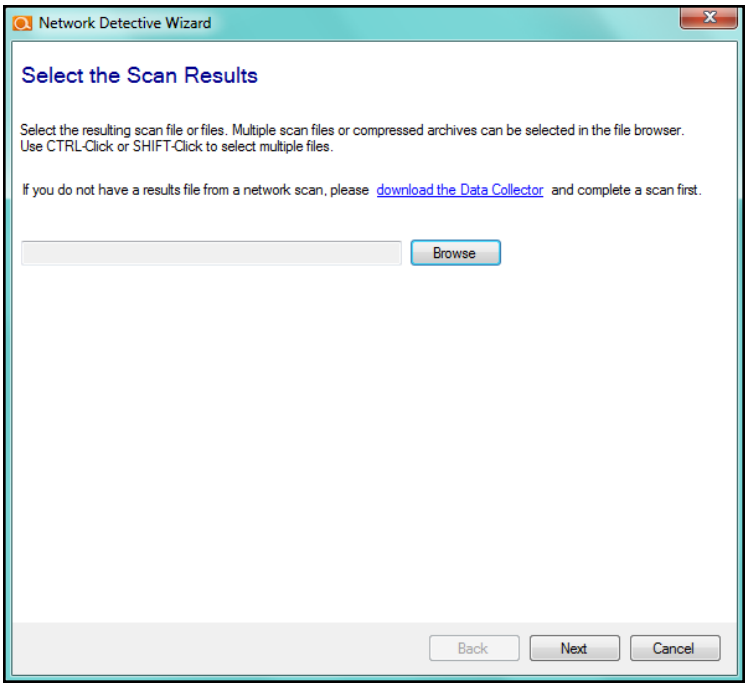
You can also view the file’s location by selecting the **Open Folder** option.

Importing the Exchange Assessment Scan Data

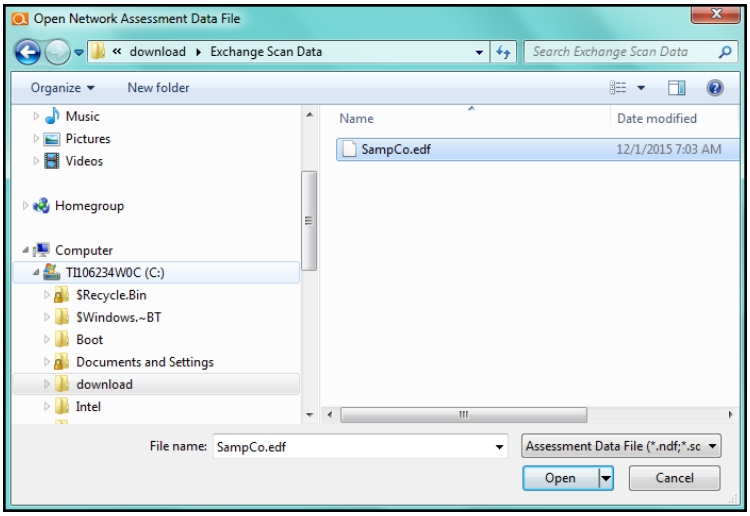
The final step in this process is to import the data collected during the **Exchange Assessment Scan** into the **Active Exchange Assessment** itself. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:



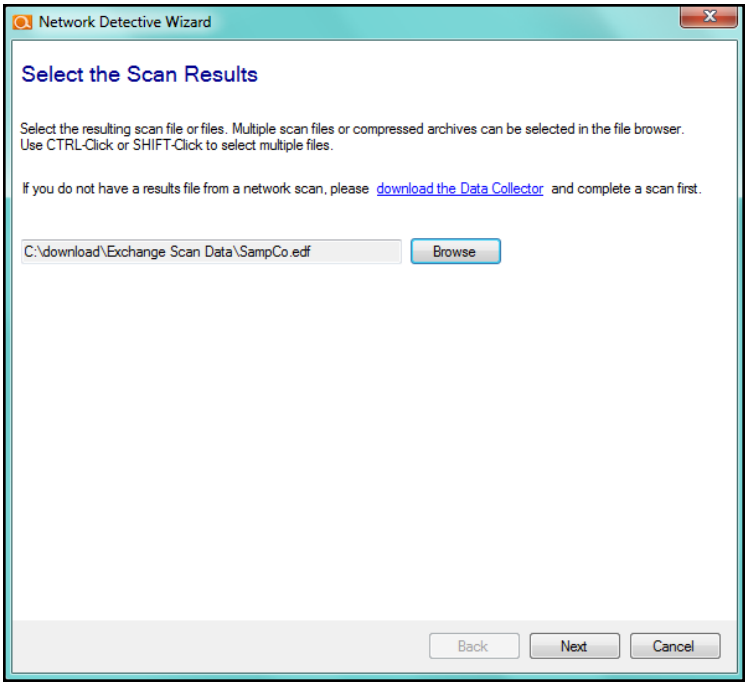
The **Select the Scan Results** window will be displayed thereby allowing you to import the .EDF or .ZIP file produced by the **Exchange Assessment Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **Exchange Scan** data file.

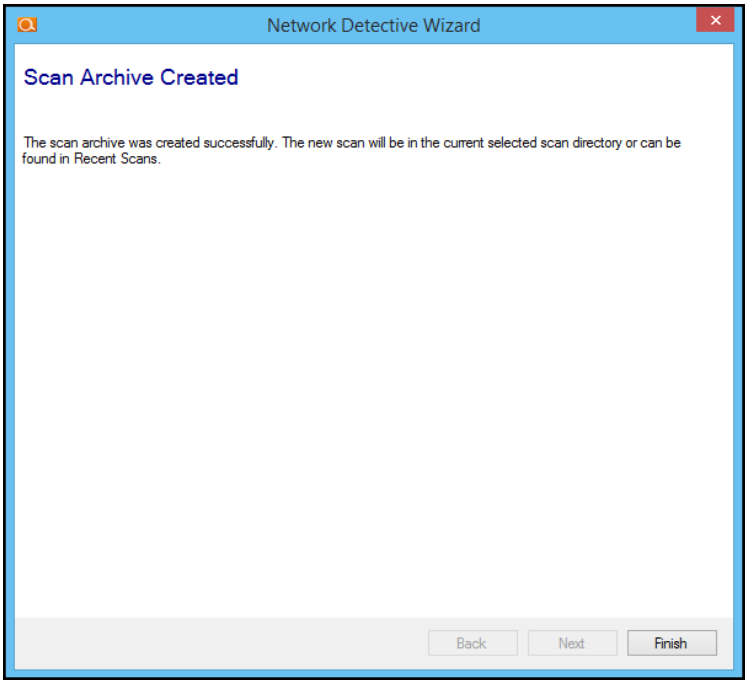


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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

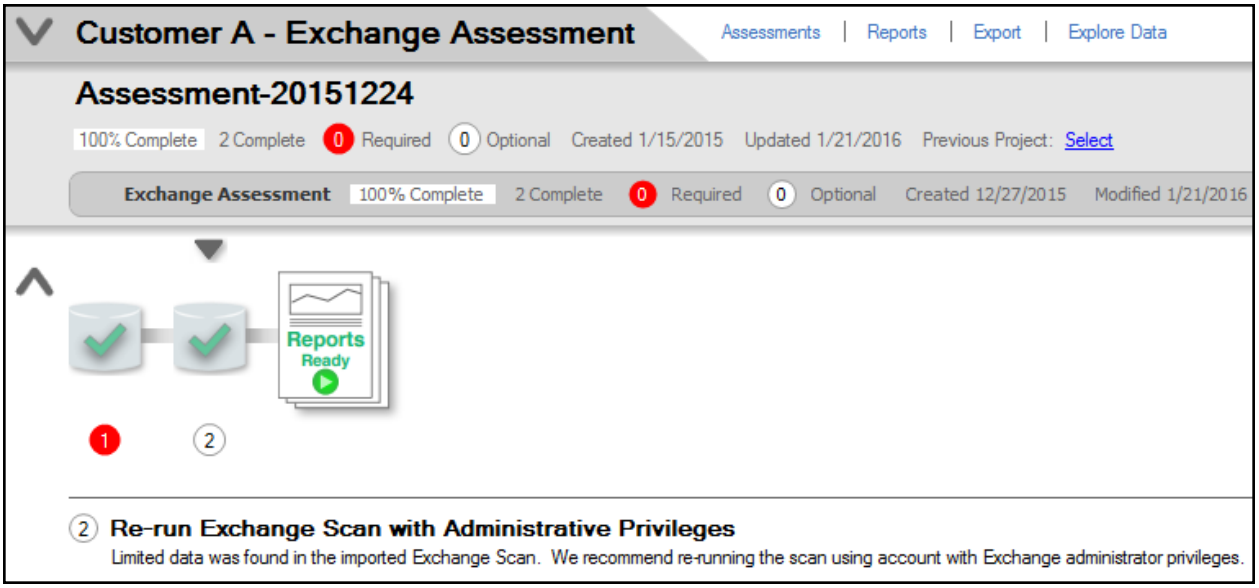


Select the **Finish** button to complete the scan file import process.

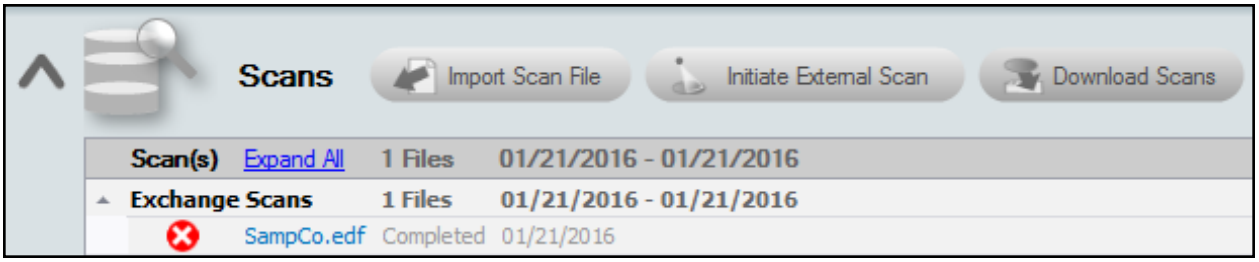
Scans List Updated Upon Completion of Imported Exchange Scan

After the Exchange Scan's .EDF file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **Exchange Assessment's Scan** data under the **Scans** section of the **Assessment Window**.

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



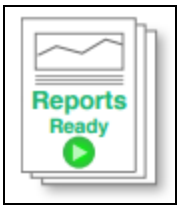
After the **Exchange Scan file** is imported, the **Scans** section of the **Assessment Window** will be updated to list the files imported into the assessment as seen below.



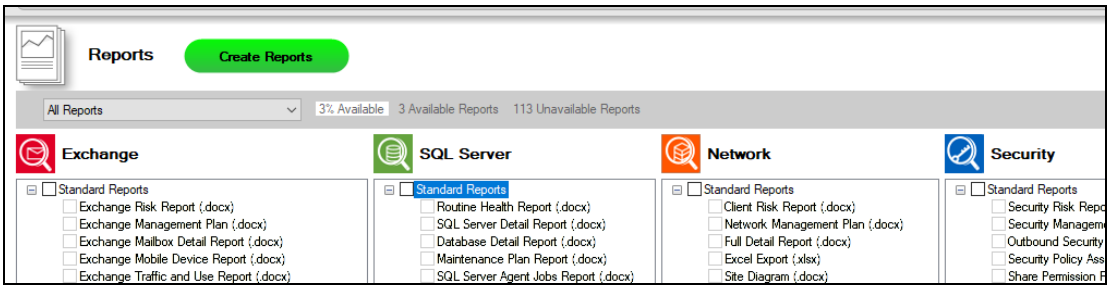
Phase 4 – Generating Exchange Assessment Reports

Steps to Generate Exchange Assessment Reports

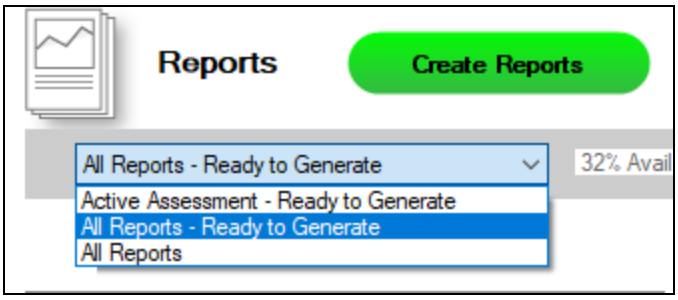
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



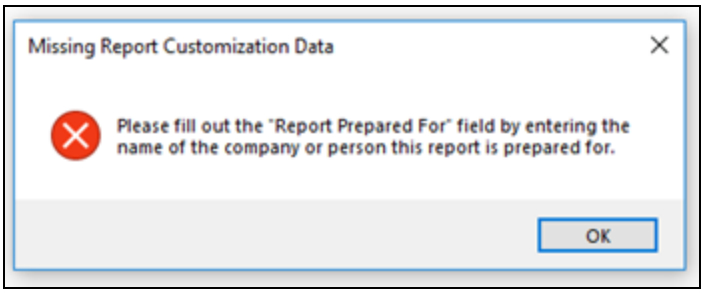
4. Select which of the Exchange Assessment reports that you want to generate.



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.

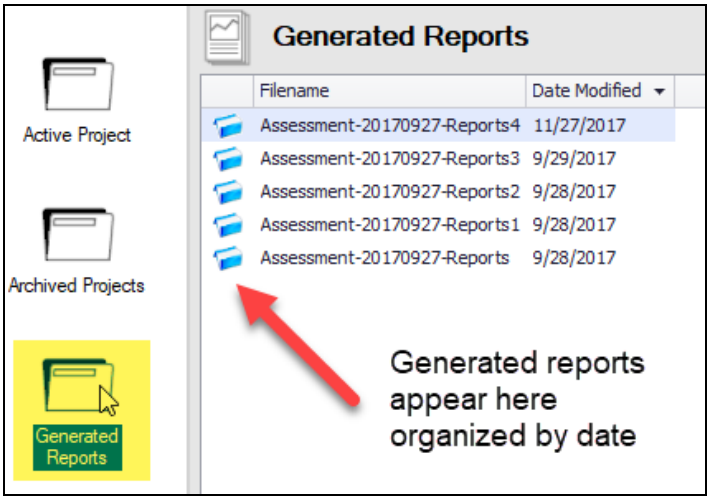


5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.
   i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



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.

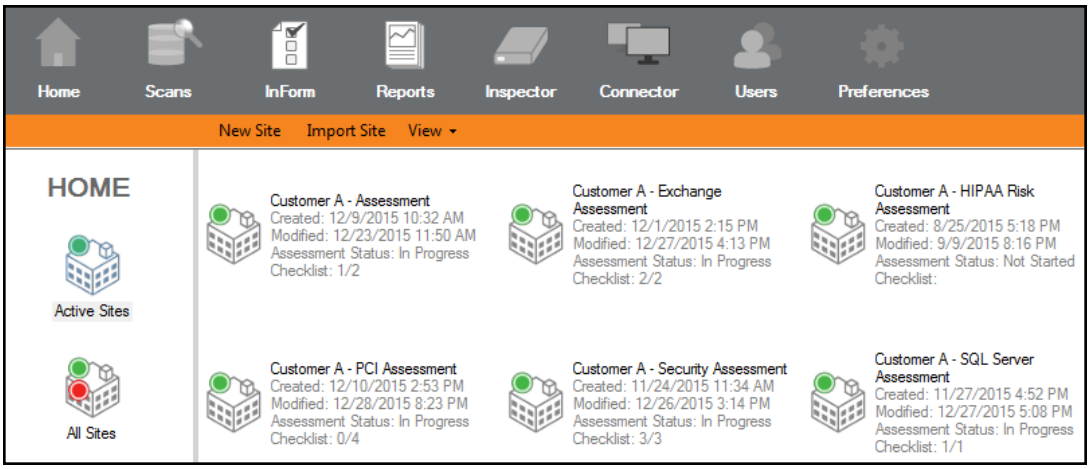
Enhancing Assessments by Adding an InForm Sheet to an Assessment Process

InForm surveys can be a valuable addition to **Site Assessments**. Information collected by a tech on-site or entered manually into a survey or worksheet template built using

InForm will enable the tech to collect additional information during an assessment that can be compiled into the Network Detective Reports.

For more information, please review the section of this User Guide entitled "Using InForm to Build Questionnaire Worksheet and Survey Templates for Enhanced Assessment Data Collection" on page 235.

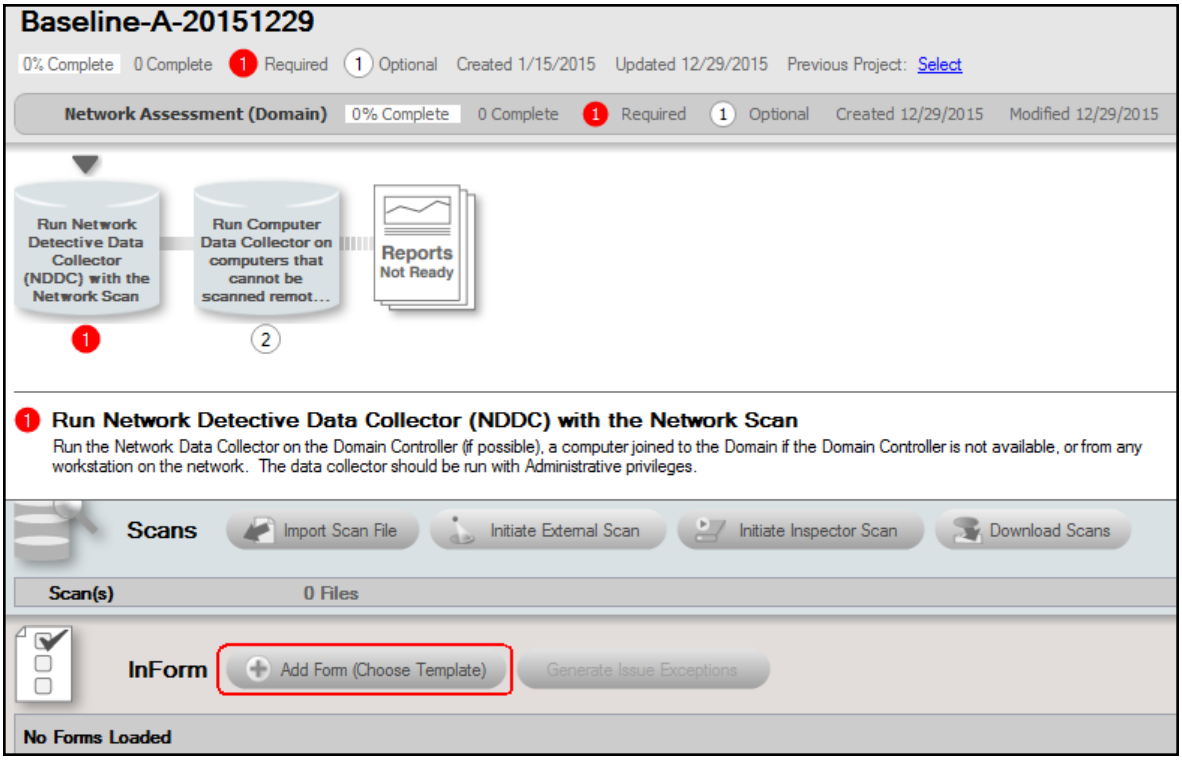
The Site Model allows you to create and edit InForm sheets from within the Assessment.



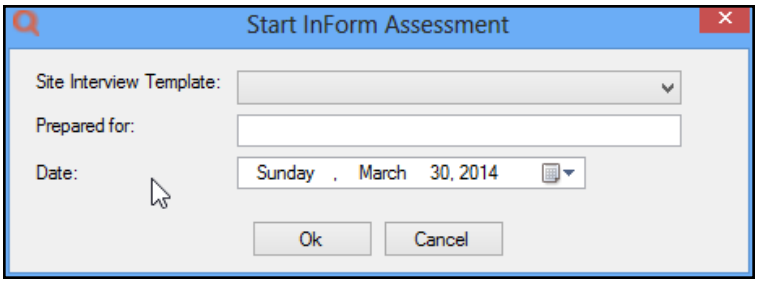
To add an **InForm** sheet to your **Assessment Project**, first navigate to the desired **Site** from the Home screen by double-clicking on its icon.

This will bring you to the Dashboard of the Site's current Assessment.

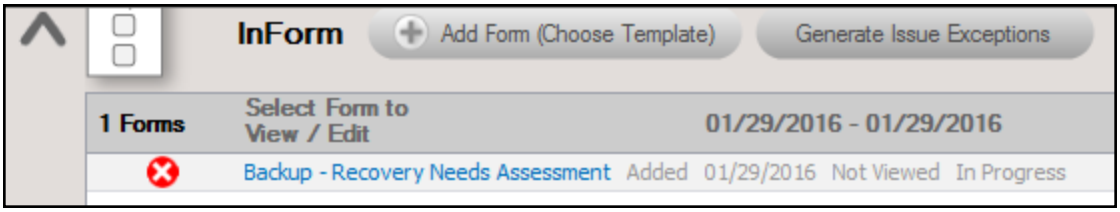
From the Assessment's Dashboard, select "**Add Form**" under the **InForm** bar.



Using the **Start InForm Assessment** dialog box, select your template, type in the name of your customer in the “Prepared for” field, and click “Ok.”



The new template will be listed under the **InForm** bar. Click the Inform template name that is in Blue text link to open and use your template.



Perfoming an SQL Server Assessment

To perform a SQL Server Assessment, complete the four phases detailed in this guide.

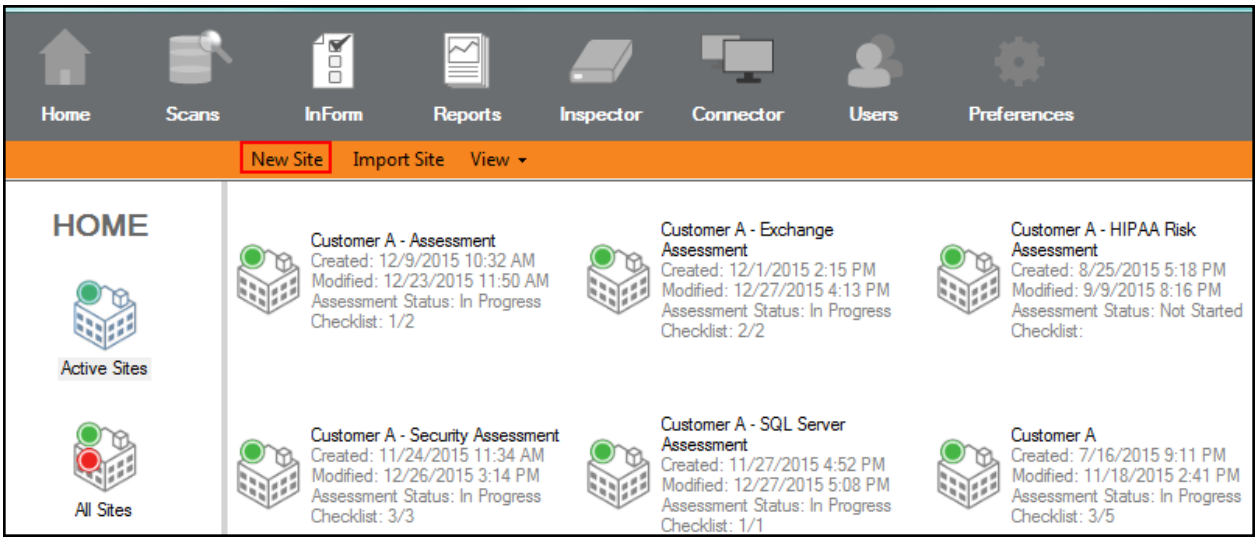
Phase 1 – Initial SQL Server Assessment Project Setup

Creating a Site

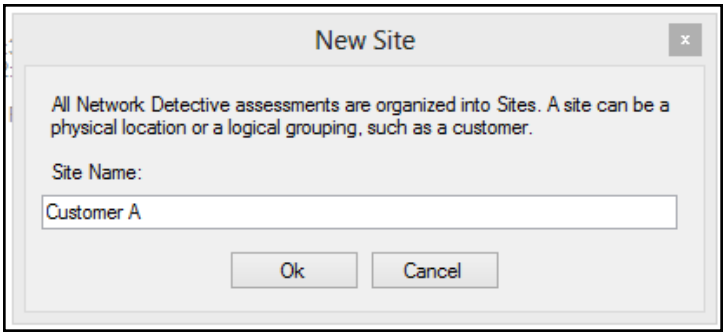
The first step in the assessment is creating a **"Site"**. All Network Detective assessment projects are organized into Sites. A **Site** can be a physical location or a logical grouping, such as a customer account name.

a. For a single location you will create one **Site**.

b. For organizations with multiple locations you must decide if you want one set of reports, or separate reports for each location.



Select **New Site**.



Enter the **Site Name**. For sites with multiple locations, enter a more detailed description.

Setting Report Branding for a Site

Reports produced by Network Detective can be “branded” with your company’s standards through the use of the **Reports Preference**s feature. Report Branding can be set at the **Global Level** (for all Sites), or at the **Site Level**. If you want to set the **Report Preferences** at the **Site Level**, please go to "Set Up Network Detective Reports" on page 16.

Adding a Connector to a Site

To add a Connector to a **Site**, please go to "Adding a Connector to a Site" on page 255.

> **Note:** Also see the Network Detective Remote Data Collector User Guide.

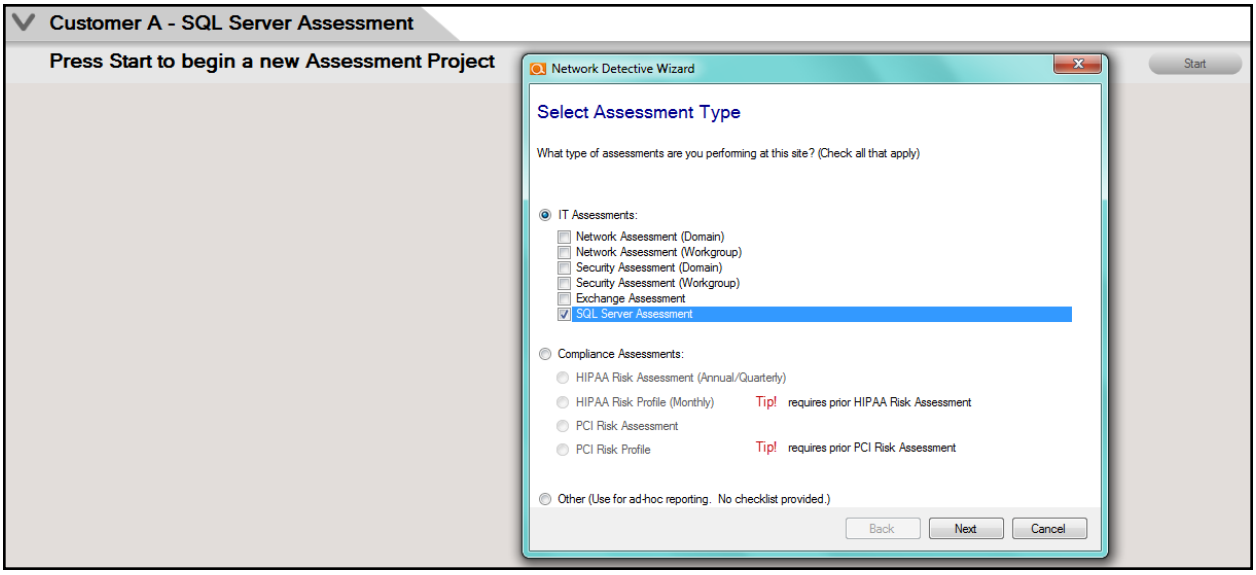
Adding an Inspector to a Site

To add an Inspector to a **Site**, please go to "Adding an Inspector to a Site" on page 257.

Phase 2 – Starting an SQL Server Assessment Project

Starting an SQL Server Assessment Project

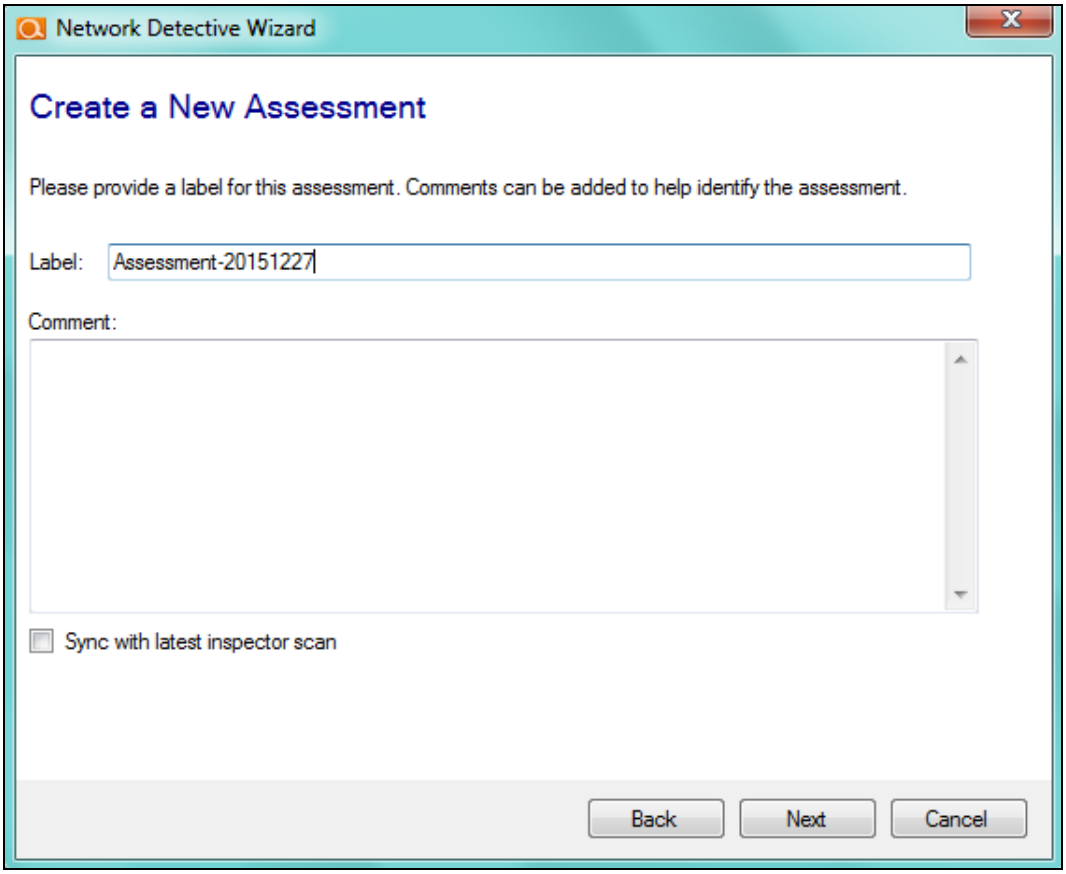
From the Site's Dashboard, click the "**Start**" button on the "Active Assessment" bar to start an **Assessment**.



This will open the **Assessment** setup wizard.

First, you will be prompted to choose one or more **Assessment** types.

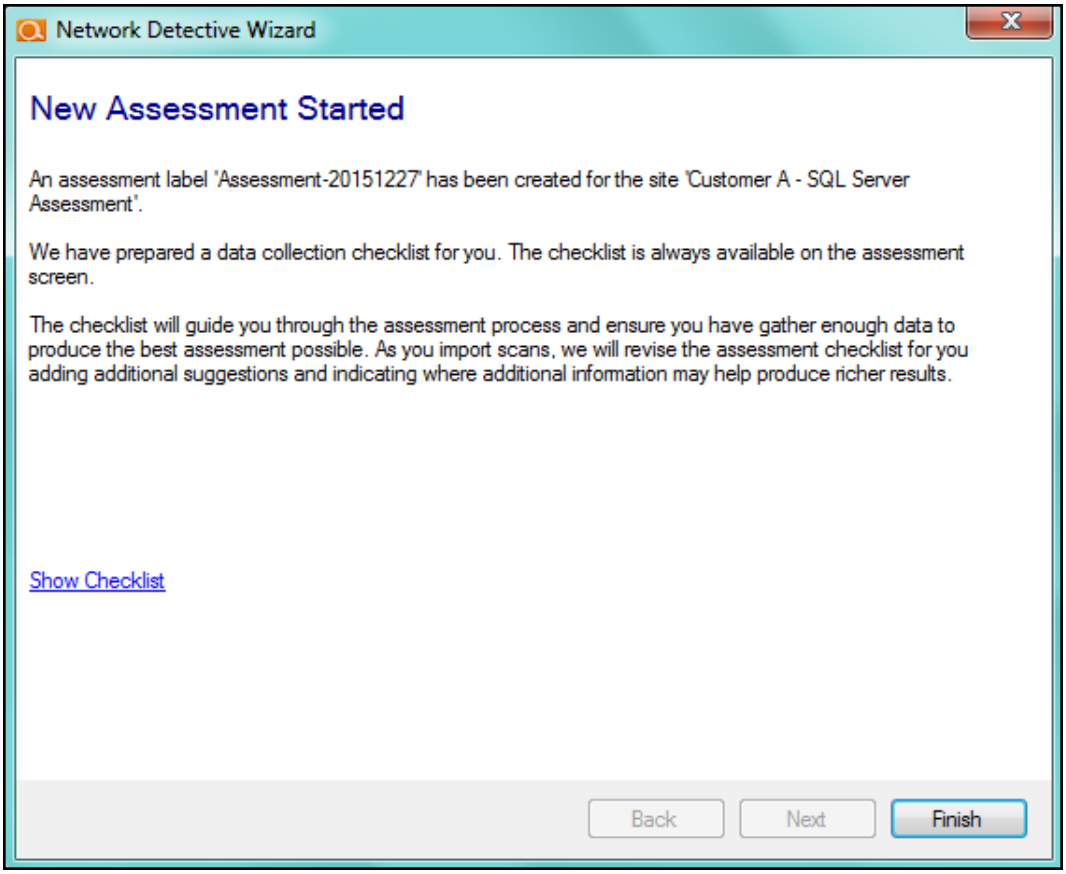
To create an SQL Server Assessment Project, select the **SQL Server Assessment** option and click on the **Next** button.



Enter a **Label** to identify the assessment.

Enter a **Comment** to help further identify the assessment.

Select the **Next** button to proceed to create/start the new Assessment.



The final window of the setup wizard summarizes the new **Assessment** and provides a link to the **Checklist**, which you can use to track the progress of your **Assessment**.

Planning the On-site Data Collection

There are various ways to collect data for a SQL Server Assessment. These methods can vary based on time, cost, client expectation, level of detail needed to identify remediation needs, etc.

Initial Assessment

Types of collections:

SQL Server Assessment

- Quick Assessment
    - SQL Server Scans on 1-2 databases

- Full Assessment
  - SQL Server Scans on all databases

Scans Performed During the SQL Server Assessment Process

The Data Collection phase of the SQL Server Assessment consists of a **Server Database Scan** using the **SQL Server Assessment Data Collector**.

Phase 3 – Performing the Assessment and Data Collection

Initiate the SQL Server Scan Using the SQL Server Assessment Data Collector and Import Scan Results

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

The Data Collector makes use of multiple various protocols to scan a SQL Server instance and can be done remotely.

The SQL Server Assessment Data Collector can be used to inspect any SQL Server on the LAN or hosted at a remote location so long as it can be accessed using SQL Server Authentication (the same as Management Studio).

Step 1 – Running the SQL Server Assessment Data Collector to Perform an SQL Server Scan

Visit the RapidFire Tools software download website to download and then run the SQL Server Data Collector file.

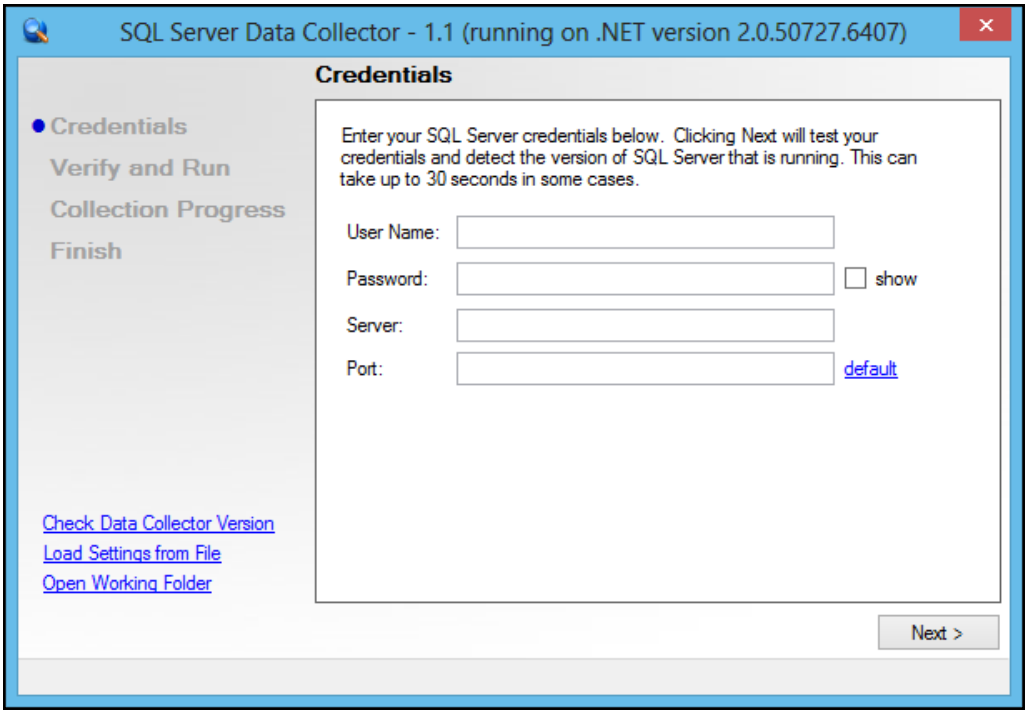
The SQL Server Assessment Data Collector is a self-extracting zip file that executes an ".EXE". Use the **Unzip** option to unzip the files into a temporary location and start the collector.

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

Step 2 – Input Credentials

Starting the **SQL Server Data Collector** application will present the following screen.

The **Credentials** window will be displayed to enable you to input the SQL Server credentials necessary to access the SQL Server database that you are attempting to scan.



Enter the **Credentials** by performing these steps:

1. Enter a username and password for the SQL Server that you intend to scan**.**
2. Enter the Server name and Port value

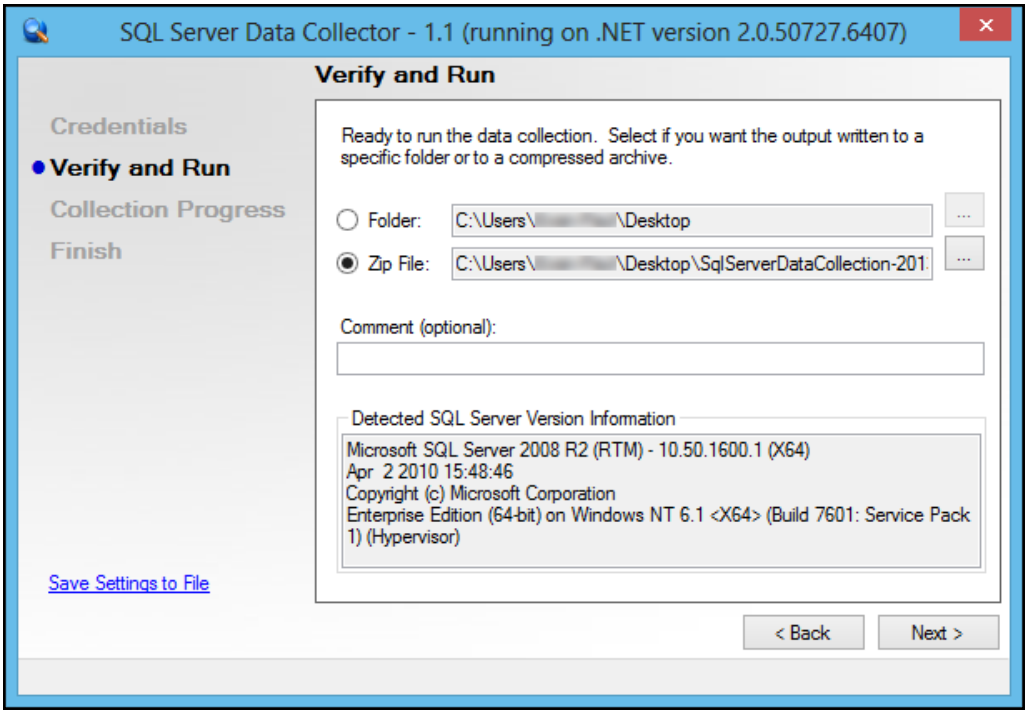
   Note: Please Note: If there is more than 1 instance, the Server name format needs to be: server\<instance name>

3. Select the **Next** button.

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

Step 3 – Verify and Run the Scan

Select the folder that you want to store the scan data file in after the scan is completed.



This page asks you to specify a destination for the output files of your scan. You have the option of outputting to a folder, or the SQL Server Data Collector can output to a compressed .zip file.

Starting the SQL Server Scan

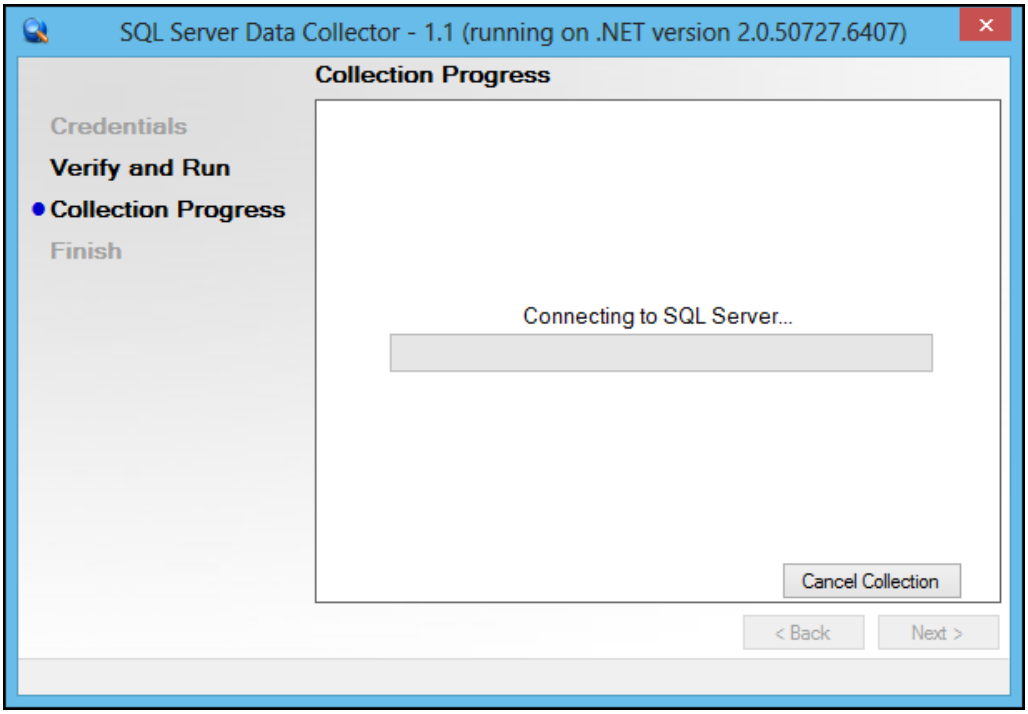
Once the **File Folder** location or the **.ZIP file** location for the scan data has been specified, enter any **Comments,** and then select the **Next** button to initiate the scan**.**

Once the scan is started, the scan's **Collection Progress** window will then be displayed.

Step 4 – Monitor the SQL Server Assessment Scan's Collection Progress

The **SQL Server 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.



This page charts the progress of your scan.

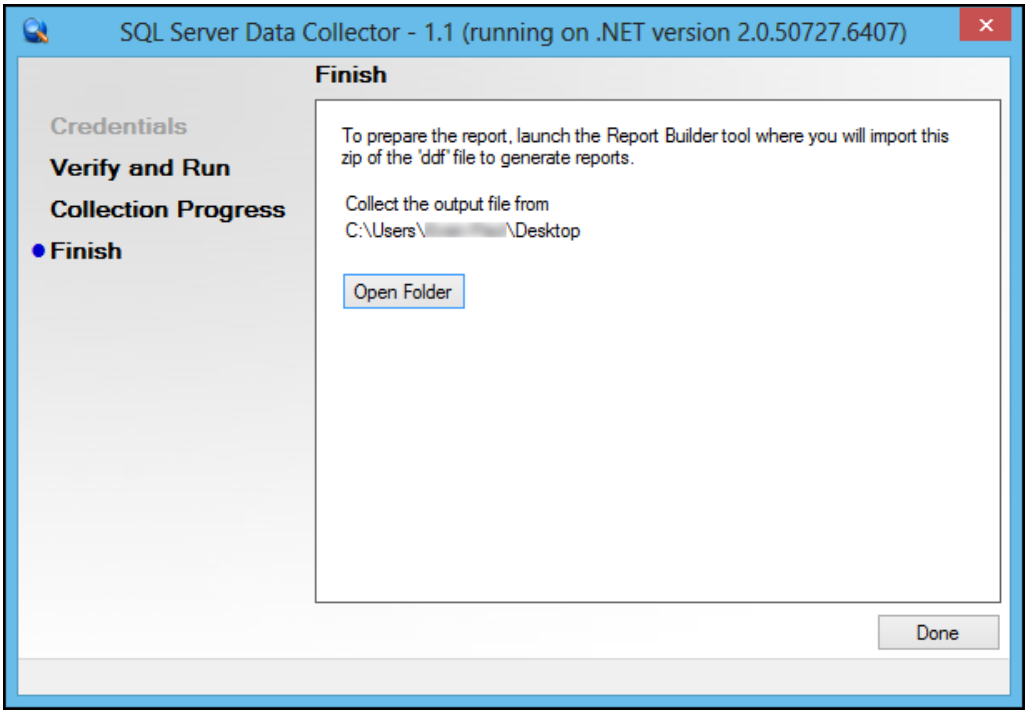
At any time you can **Cancel Data Collection** which will not save any data.

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

Step 5 – Complete the SQL Server Data Collector Scan Process

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

The wizard shows the output destination, and allows you to open that folder and review the results of your completed scan.

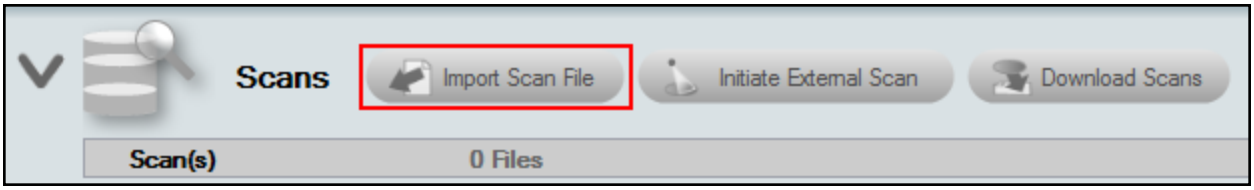


Click on **Done button** to close the **SQL Server Data Collector** window. Note the location where the scan's output file is stored.

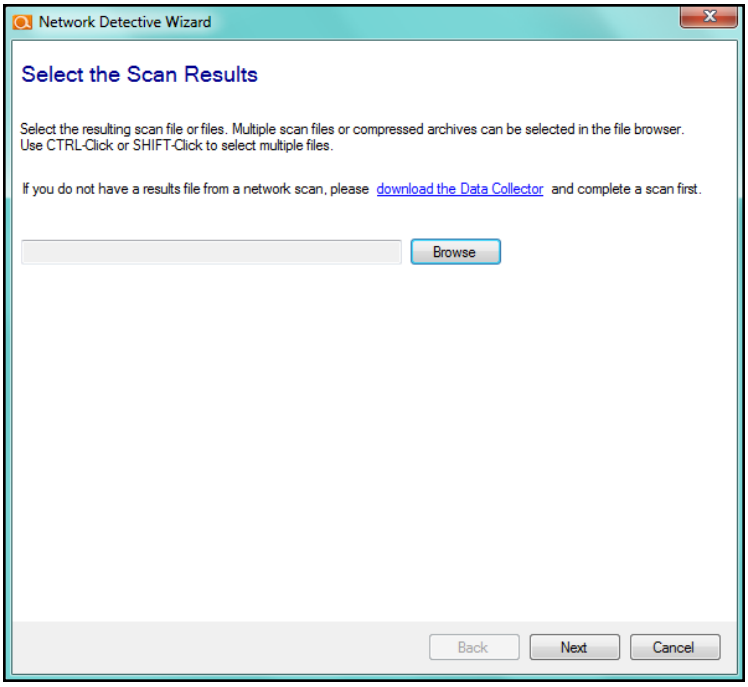
You can also view the file's location by selecting the **Open Folder** option.

Importing the SQL Server Scan Data in the SQL Server Assessment

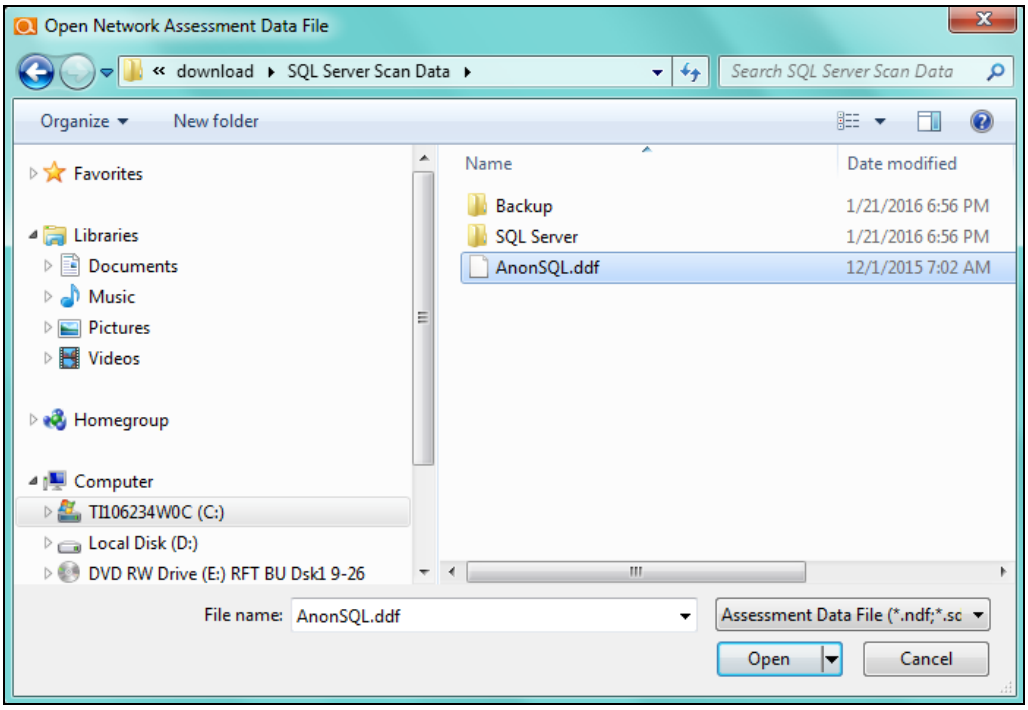
The final step in this process is to import the data collected during the **SQL Server Assessment Scan** into the **Active SQL Server Assessment** itself. Click on the **Import Scan File** button located on the **Scans** bar in the Network Detective **Assessment** window:



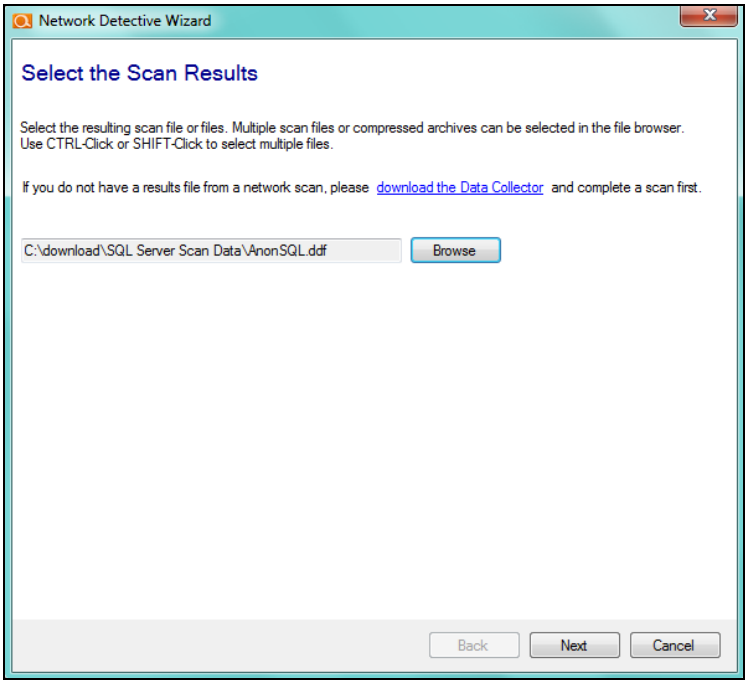
The **Select the Scan Results** window will be displayed thereby allowing you to import the .DDF or .ZIP file produced by the **SQL Server Assessment Scan** into the **Assessment**.



Select **Browse** in the **Scan Results** window and select the **SQL Server Scan** data file.

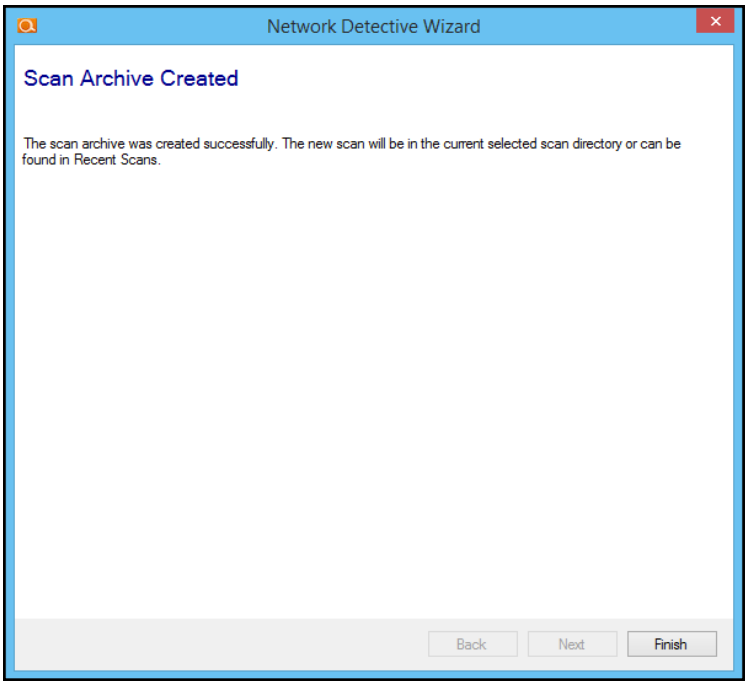


Then click the **Open** button to import the scan data. The following window will be presented.



To continue the scan import process, click on the **Next** button in the **Scan Results** window.

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

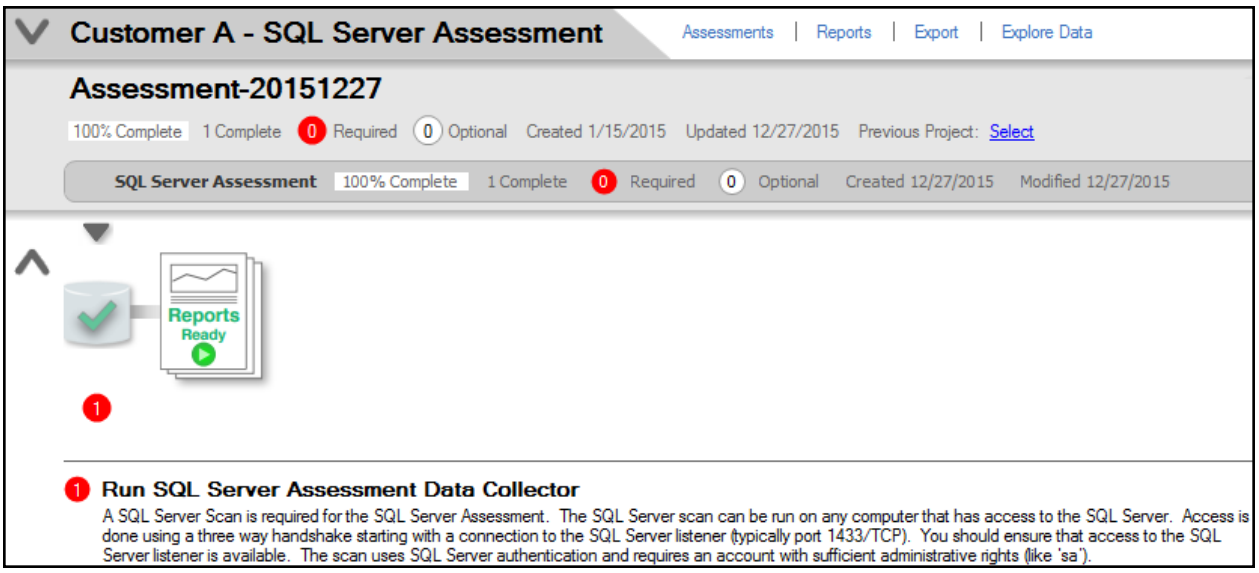


Select the **Finish** button to complete the scan file import process.

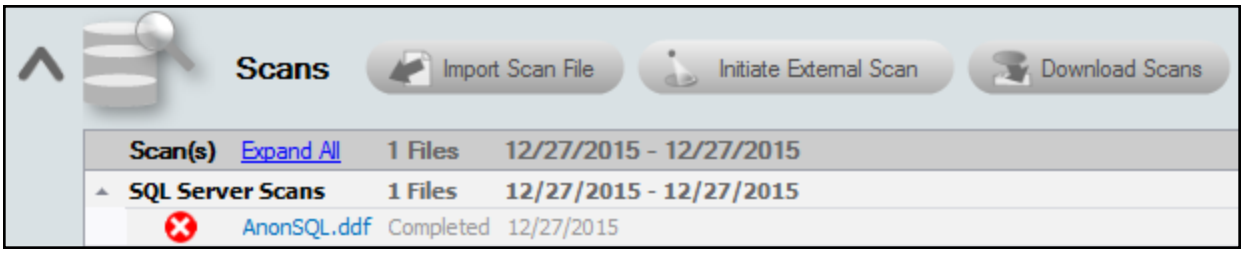
Scans List Updated Upon Completion of Imported SQL Server Scan

After the SQL Server Scan's .DDF file is imported, the **Scans Dashboard** within the **Assessment Window** will be updated to reflect the addition of the **SQL Server Assessment's Scan** data under the **Scans** section of the **Assessment Window**.

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



After the **SQL Server Scan file** is imported, the **Scans** section of the **Assessment Window** will be updated to list the files imported into the assessment as seen below.



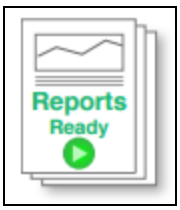
SQL Server Assessments in Environments Using Multiple Databases

Note: Please Note: When performing SQL Server assessments for companies that have more than one SQL Server database, you can have multiple Server scan files (i.e. .DDF files) imported into the assessment. In this case, when Generating Reports, a report will be produced for each individual SQL Server database that is included within the assessment.

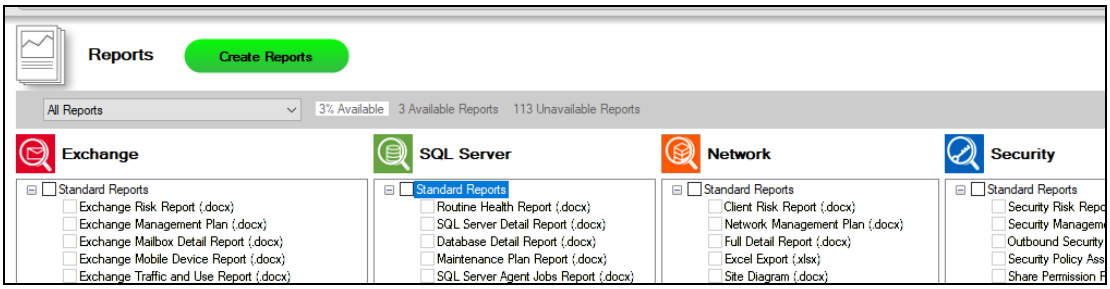
Phase 4 – Generating SQL Server Assessment Reports

Steps to Generate SQL Server Assessment Reports

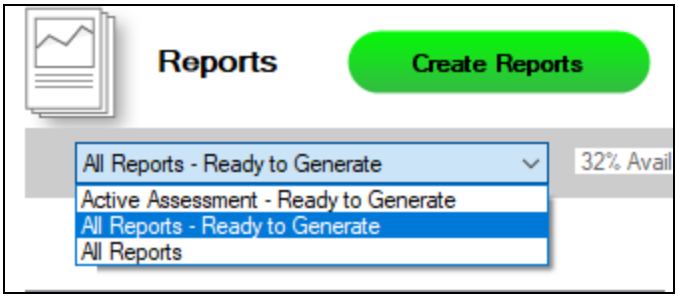
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



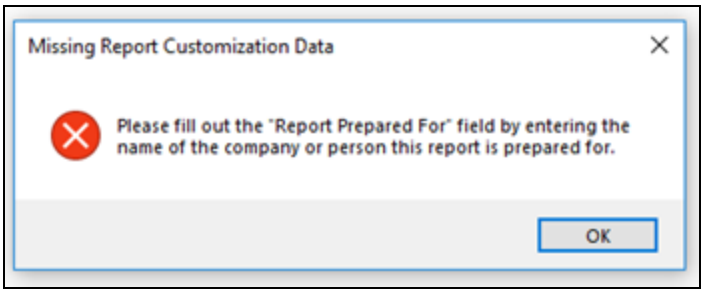
4. Select which of the SQL Server Assessment reports that you want to generate.



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.

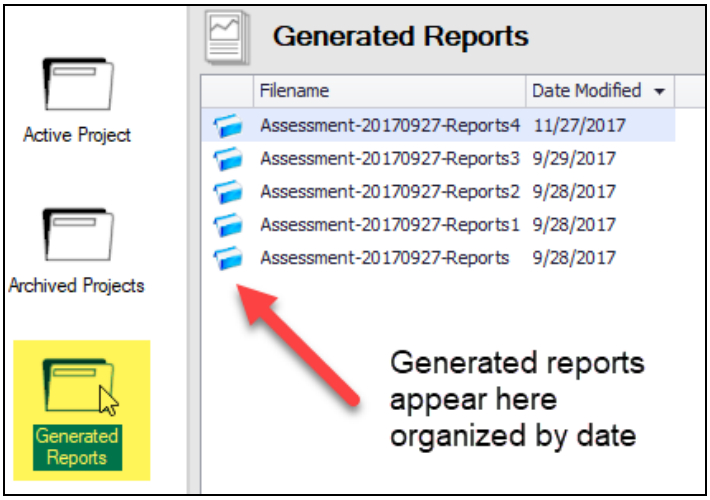


5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.
   i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



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.

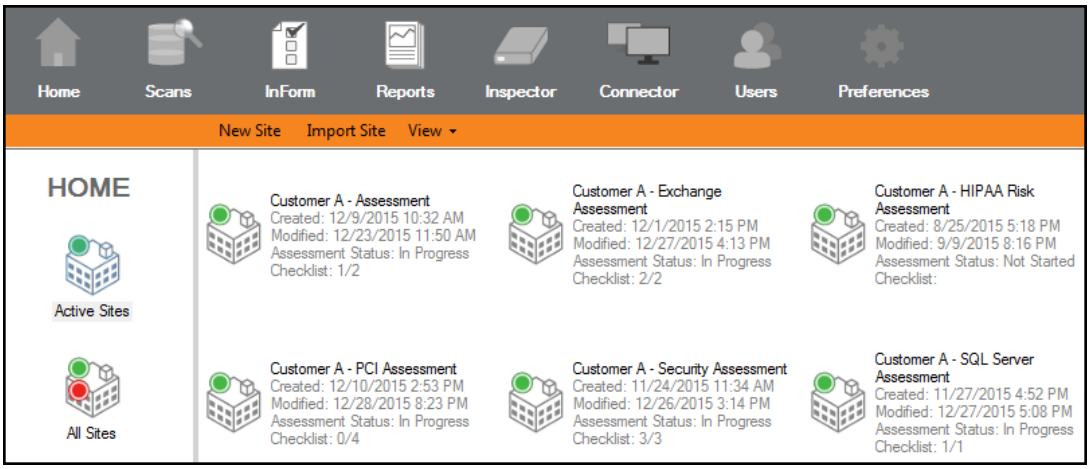
Enhancing Assessments by Adding an InForm Sheet to an Assessment Process

InForm surveys can be a valuable addition to **Site Assessments**. Information collected by a tech on-site or entered manually into a survey or worksheet template built using

InForm will enable the tech to collect additional information during an assessment that can be compiled into the Network Detective Reports.

For more information, please review the section of this User Guide entitled "Using InForm to Build Questionnaire Worksheet and Survey Templates for Enhanced Assessment Data Collection" on page 235.

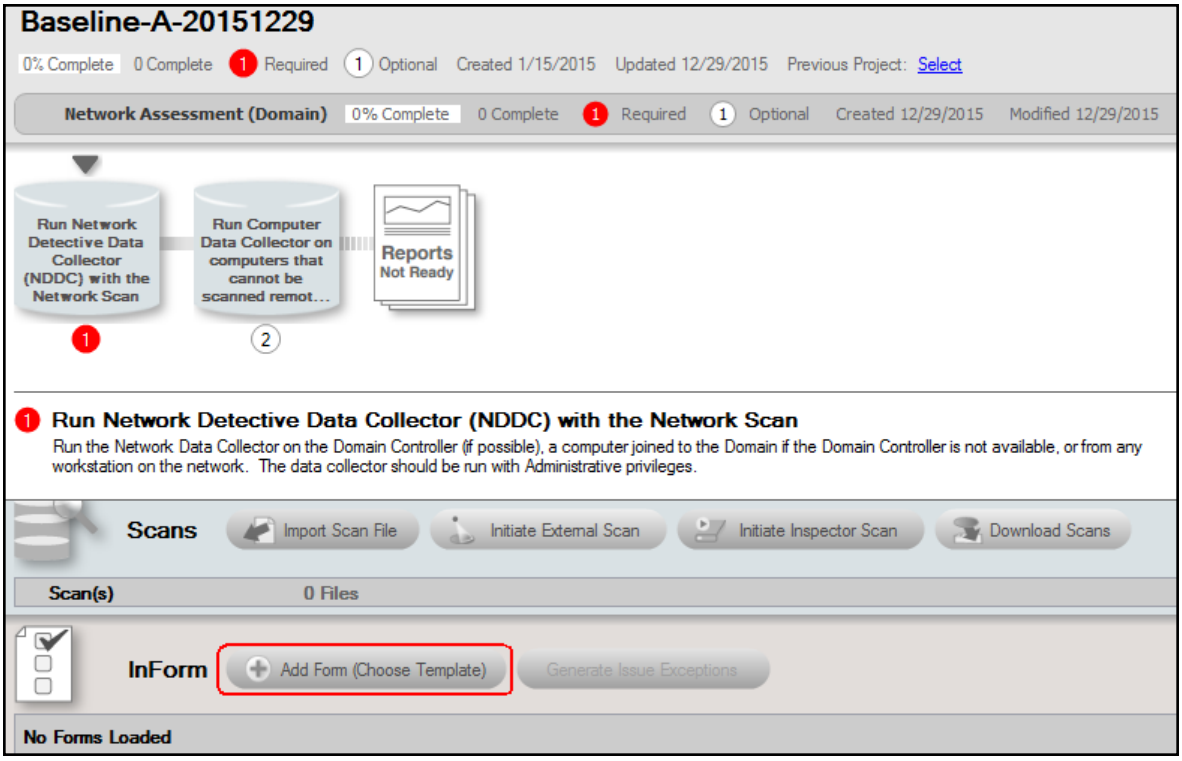
The Site Model allows you to create and edit InForm sheets from within the Assessment.



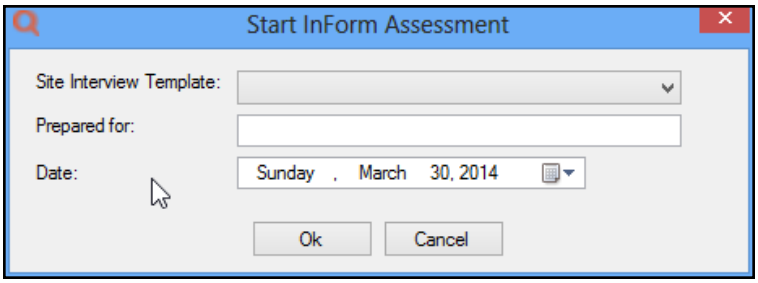
To add an **InForm** sheet to your **Assessment Project**, first navigate to the desired **Site** from the Home screen by double-clicking on its icon.

This will bring you to the Dashboard of the Site's current Assessment.

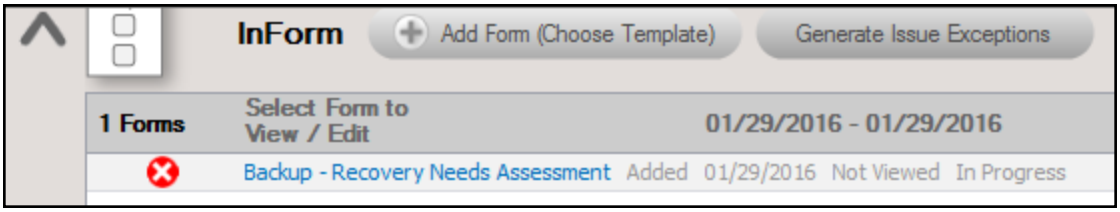
From the Assessment's Dashboard, select "**Add Form**" under the **InForm** bar.



Using the **Start InForm Assessment** dialog box, select your template, type in the name of your customer in the “Prepared for” field, and click “Ok.”



The new template will be listed under the **InForm** bar. Click the Inform template name that is in Blue text link to open and use your template.



Network Detective Reports Overview

This section covers everything you need to know about Network Detective Reports.

Network Assessment Reports

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

Standard Reports

Report Name	Description
Asset Detail Report	For each network scan, this report provides detailed information on each of the individual devices discovered by Network Detective. The report is ideal for cataloging and documenting the complete settings and configurations for individual workstations and servers.
BDR Needs Analysis	An analysis of the backup needs for servers, workstations, and cloud applications on the network.
BDR PowerPoint	PowerPoint presentation showing a summary of the backup needs for servers, workstations, and cloud applications on the network.
Client Health Report	The Client Health Report details the overall risk to the assessment environment. The Health Score represents the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur. Unresolved issues are detailed item by item and are organized by risk score.
Client Risk Report	This is the "money" report for you. The report presents your client with a summary of their overall risk score based on your scan, along with simple charts to show the problem areas. Each problem area represents an opportunity for you to present a proposed solution and pitch your services. The purpose of this report is for you to use as a "discussion document" to aid you in having a conversation with your customer about the specific risk areas you found, what they mean, and how you can help. *Keep the Full Network Assessment in your hip pocket, and pull it out*

Report Name	Description
	when your prospective new client asks how you came up with your findings!
Computer Security Report Card	The Computer Security Report Card assesses individual devices at a high level based on various security criteria. The report card should be viewed as a relative measure as to how well a device complies with security best practices. There may be specific reasons or compensating controls that may make it unnecessary to achieve an "A" in all categories to be considered secure. Devices discovered on the network are assigned an overall score, as well as a specific score for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F').
Consolidated Management Plan	The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.
Consolidated Risk Excel	We also give you the output of the Consolidated Risk Report and export it into an Excel file format.
Consolidated Risk Report	The Consolidated Risk Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Consolidated Risk Score and a high-level overview of the health and security of the network. The report details the scan tasks undertaken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security, Exchange, SQL Server) and compliance assessments (HIPAA and PCI) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis. At the end of the report, you can find a summary of the devices discovered on the network, in addition to other useful information organized by assessment type.
Datto BDR Needs Analysis	An analysis of the backup needs for servers, workstations, and cloud applications on the network.
Datto BDR Powerpoint	PowerPoint presentation showing a summary of the backup

Report Name	Description
	needs for servers, workstations, and cloud applications on the network.
Datto Unified Continuity Report	This report details the status of your Datto BCDR, Cloud Continuity for PCs, Datto Continuity for Microsoft Azure, and SaaS Protection accounts.
Excel Export	We also give you the ability to output all of the devices and configurations uncovered by our scan, and export it into an Excel file format. Once in Excel, you'll be able to take the data and import it into your favorite Service Desk or PSA system, or simply create your own custom sorts, analyses, reports and graphs inside of Excel. Add columns of new data such as location info, emergency phone numbers, and customer instructions to make this report even more valuable.
Full Detail Report	This report provides comprehensive documentation of the current configuration and use of the network. The report shows devices in high-level views, allowing you to easily get an overall assessment of the entire network. Discovered issues are highlighted, making it easy to spot individual problems.
IT SWOT Analysis	Embellish your IT assessments with site photos, policies, and additional information you collect from client interviews & on-site inspections. The Network Detective In-Form tool is included with all Module subscriptions. Use it to create IT check-lists, questionnaires, and IT SWOT Analyses.
Layer 2-3 Detail Excel Export	This Excel report show systems that were able to be accessed via SNMP and those that were not able to be accessed. Not all devices need to be accessible via SNMP, but all primary network devices should be to get the best complete picture. The report requires detection of at least one Layer 2/3 device (i.e., a router or a switch).
Layer 2-3 Detail Report	This report show systems that were able to be accessed via SNMP and those that were not able to be accessed. Not all devices need to be accessible via SNMP, but all primary network devices should be to get the best complete picture. The report requires detection of at least one Layer 2/3 device (i.e., a router or a switch).
Layer 2-3 Diagram (.tif)	This .tif image helps you visualize all devices discovered on the

Report Name	Description
	network that were accessible through Layer 2/3 discovery.
Layer 2-3 Diagram Export to Microsoft Visio	This Visio file helps you visualize all devices discovered on the network that were accessible through Layer 2/3 discovery. Specifically, you can export the Layer 2-3 Diagram to Visio, Microsoft's diagramming software. This allows you to access the diagram in the Visio app.
Layer 2-3 Diagram Report	This Word doc helps you visualize all devices discovered on the network that were accessible through Layer 2/3 discovery. Specifically, it breaks down the graphic into several "zones" or sub-graphics that make larger networks easier to visualize piece by piece.
Network Assessment Change Report	Everyone knows that a computer network is a dynamic environment and as such is constantly changing. And a Network Assessment is only a snapshot of the network status at the time the assessment is run. That's why we include a valuable Network Assessment Comparison Report. Every time you run an assessment on a given network, the software generates a unique encrypted data file containing all the findings. Network Detective allows you to generate a report that compares the results of any two network scans, and highlights everything that has changed.
Network Assessment PowerPoint	PowerPoint presentation showing details of the environment scanned, risk and issue score, issue overview, and next steps.
Network Management Plan	This report will help prioritize issues based on the issue's risk score. A listing of all affected devices, users, or sub-systems is provided along with recommended actions.
Response Report	Response Reports can be generated from any InForm form. These reports allow you to present data entered into InForm from the pre-built forms or from your own forms.
Site Diagram	Once you sign up for Network Detective and run a scan, you'll have the option to generate a site diagram which breaks down and categorizes all of the devices available on the network. The schematic shows the basic network structure, with convenient drill downs into each group of like workstations. Each device is annotated with important identifying configuration information and is color-coded based on its status.
Site Diagrams Export	You have the option to export the Site Diagram to Visio,

Report Name	Description
to Microsoft Visio	Microsoft's diagramming software. This allows you to access the site network diagram in the Visio app.
Windows Patch Assurance Change Report	The Windows Patch Assurance Change Report uses scan data from both the previous assessment and the current assessment to help verify the effectiveness of the client's patch management program over time. The Summary section provides a high-level overview of missing security updates and service packs across the entire network. After the Summary, you can find more detailed missing patch information for each individual workstation. Use this information to apply critical patches to reduce the overall security risk to the network.
Windows Patch Assurance Report	The Windows Patch Assurance Report helps verify the effectiveness of the client's patch management program. The report uses scan data to detail which patches are missing on the network. The Summary section provides a high-level overview of missing security updates and service packs across the entire network. After the Summary, you can find more detailed missing patch information for each individual workstation. Use this information to apply critical patches to reduce the overall security risk to the network.
Windows Service Account Report	This report details the Windows Service Accounts discovered in the target environment.

Infographics

Executive Summary	This report provides a holistic risk assessment of systems present on the network and summarizes actionable issues into 9 categories. This allows readers to quickly understand where immediate action is required.
Outdated Malware Definitions Summary	This visual report report adds malware definition monitoring to your assessment report. Up to date anti-spyware and antivirus definitions are required to properly prevent the spread of malicious software
Outdated Operating System Summary	This visual report adds operating system (OS) monitoring to your assessment report. Unsupported OSes no longer receive vital security patches and present an inherent risk.

Server Aging Infographic Report	The age of hardware in your environment can directly affect your availability and performance. As hardware gets older, the risk of failure increases. During our assessment of your environment, we analyzed the age of servers in the environment.

Change Reports

Baseline Client Health Report	The report shows how the Health Score has changed between the updated and previous assessment. Likewise, the report contains a list of Resolved Issues between the current and previous assessment organized by risk severity.
Baseline Client Risk Report	This report details the Risk Score for both the current and previous assessment. At the same time, the report breaks down each issue and conveys whether the issue is increasing or decreasing in risk level. For example, are your devices missing more or fewer security patches since the previous assessment? This report will tell you.
Baseline Network Management Plan	The Baseline Network Management Plan compares the results of a previous assessment with the latest assessment. Items that have been fixed or remediated are crossed out.
Full Detail Change Report	A computer network is a dynamic environment and as such is constantly changing. While the Network Assessment Full Detail report is a snapshot of the network status at the time the assessment is run, the Network Assessment Change report focuses on only the add, removes, and changes in the network.
Quarterly Business Review Report	This report compares one time period to a previous one forming the basis for a Quarterly Business Review centered on changes and overall trending rather than detailed documentation and device discovery.

Security Assessment Reports

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

Standard Reports

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

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

Report Name	Description
Scan Detail Excel*	
Internal Vulnerability Scan Detail Report*	This detailed report provides extensive data on each discovered internal vulnerability organized by each affected device. This includes insight into the technical nature of each issue, a proposed solution, as well as several graphical breakdowns of the numerical disposition of issues on the target network. (*Requires Inspector)
Login Failures by Computer Report	This report provides a list of systems that have had failed interactive and network login attempts along with a count of the number of failed logins over the past 1, 7 and 30 days. Use this to identify an employee who has forgotten their credentials. In an extreme scenario, the report may help you detect a hacker trying to enter the network through an employee's legitimate account, or an attempt to access a highly sensitive system such as the CEO's workstation.
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.
Outbound Security Report	Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet content accessibility.
Resulting Set of Policies Reports	This report analyzes the various Resulting Sets of Policy (RSOP) based on user settings on devices in the environment and helps point out commonalities in the sets and which users/device combinations have the configurations applied. There are separate reports for both user settings and device settings.
Security Assessment 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.
Security Health Report	This report measures the overall risk to the environment by the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a

Report Name	Description
	security, availability, or performance related incident will occur. This report will also compare the results of a previous assessment with the current assessment.
Security Management Plan	Network Management Plan This report will help prioritize issues based on the issue's risk score. A listing of all security related risks are provided along with recommended actions.
Security Policy Assessment Report	A detailed overview of the security policies which are in place on both a domain wide and local machine basis.
Security Risk Report	This report includes a proprietary Security Risk Score and chart showing the relative health (on a scale of 1 to 10) of the network security, along with a summary of the number of devices with issues. This powerful lead generation and sales development tool also reports on outbound protocols, System Control protocols, User Access Controls, as well as an external vulnerabilities summary list.
Share Permission Report	Comprehensive lists of all network “shares” by device, detailing which users and groups have access to which devices and files, and what level of access they have.
Share Permission Report by User	Comprehensive lists of all network “shares” by user. Each subsection details the share and file system permissions granted to each user account within the above domain.
Share Permission Report by User Excel	Comprehensive lists of all network “shares” by user in MS Excel format.
Share Permission Report Excel	Comprehensive lists of all network “shares” by devices in MS Excel format.
User Behavior Analysis Report	Shows all logins, successful and failure, by user. Report allows you to find service accounts which are not properly configured (and thus failing to login) as well as users who may be attempting (and possibly succeeding) in accessing resources (devices) which they should not be.
User Permissions	Organizes permissions by user, showing all shared devices and files to which they have access.

Report Name	Description
Report	

Infographics

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

Change Reports

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

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

Exchange Assessment Reports

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

Standard Reports

Report Name	Description
Exchange Assessment 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.
Exchange Distribution Lists Report	Most organizations routinely create email distribution groups - both for internal communications and for routing incoming emails to multiple individuals at the same time. The problem is that over time, many companies lose track of which groups they've created and who's included in them. Obviously, with a migration you'd want to be able to accurately replicate all of these groups. But how about all those situations when employees turn over or change positions? Each time this happens individual emails need to be systematically added and removed from groups. This report identifies and lists all distribution groups as well as which end-users or other groups are to receive any emails.
Exchange Excel Export	We also give you the ability to output all of the Exchange data configurations uncovered by our scan, and export it into an Excel file format. Once in Excel, you'll be able to take the data and import it into your favorite Service Desk or PSA system, or simply create your own custom sorts, analyses, reports and graphs inside of Excel.
Exchange Health Report	This report measures the overall risk to the environment by the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur.
Exchange Mailbox Detail Report	Without this tool, it would be a daunting task to ask someone to document all known and available information for every mailbox in an Exchange environment. With the Exchange Assessment module, it's quick and painless. Simply run the non-invasive scan on the target Exchange Server, and Network Detective does the rest. This report gives you a mailbox-by-mailbox catalog of information, including everything from mailbox display name to quotas to a listing of

Report Name	Description
	folders/sizes for each mailbox (and more). Whether documenting regular use, planning ahead, or preparing for a migration - knowledge is power and, in this case, knowledge can be money as well. This report will allow you to better prepare for a migration by knowing all mailbox settings, ensure that display names, etc., are standardized, quotas are set appropriately, and also trouble-shoot issues with specific mailboxes.
Exchange Mailbox Permissions Report by Mailbox	Sometimes there's a need to give one or more individuals permission to access either someone else's mailbox, or a group mailbox, on a temporary basis - vacations, leaves of absence, and terminations are all examples of this situation. For security purposes, best practices suggest a periodic review of all mailboxes This report will identify on a mailbox-by-mailbox basis which groups or which individuals have access to the mailbox and at what level.
Exchange Mailbox Permissions Report by User	A separate companion report inverts the information to show you on a user-by-user basis which users have access to which mailboxes. This report is a great way to document individual access rights.
Exchange Management Plan	This report will help prioritize issues based on the issue's risk score. A listing of all affected devices, users, or sub-systems is provided along with recommended actions.
Exchange Mobile Device Report	Whether users are provided with a company sanctioned mobile device or are given the ability to "bring their own device", it is important to know all the details of the network's techno-diversity. This report provides a detailed listing of every mobile device used by employees to access their organization's mailbox. The report indicates the names and specific types of mobile devices that are accessing the Exchange server, as well as the operating systems and even the number of folders that are being updated. This report will help optimize employee connectivity/productivity and plan appropriately for system changes/upgrades. The report is also useful to present to clients as an aid to support your case as for system changes (such as setting up a SharePoint portal, moving to Exchange 2016, etc.).
Exchange Public Folders Report	Public folders give Outlook users access to common folders in order to share information. Access is determined by the Exchange administrator. Public folders can be available to everyone within a

Report Name	Description
	select organization, or to a specific group. This report gives you a quick run down of the public folders in the Exchange environment. This can be useful for determining whether users have access to public folders that they shouldn't - or if certain folders should not be made public in the Exchange environment.
Exchange Risk Report	While the Exchange Assessment module will automatically generate the detailed reports you need to manage a full migration project - or deliver an on-going security and maintenance service - you might not want to share all that information with your clients. Instead, show them a branded high-level report. Designed specifically to be a customer-facing document, this report provides a polished overview of any issues identified in the more detailed reports. Corresponding charts and graphs clearly communicate issues and serve as a graphical aide to help suggest remedial steps. This is the perfect report to prepare for your account reviews for current customers to show that you are properly handling their Exchange environments. And, it's a fabulous report to run for new prospects to show potential deficiencies and risks that you can help cure and manage.
Exchange Server Configuration Report	This report details the technical configuration and details of the Exchange Server. This information can be hard to consolidate or visualize without this report. This report can be useful for the Exchange administrator in order to quickly take in the configuration and overall health of the Exchange environment.
Exchange Traffic and Use Report	Managing individual and aggregate mailbox sizes is a real challenge for most organizations. It's obviously important to understand the total organizational email traffic and usage in order to prepare for a migration project. But the report is equally useful on an ongoing basis to help manage individual mailbox size limits based on usage needs, and to identify individuals who may be misusing or abusing their mailboxes. This report will show you the status of all mailboxes - their size limits, percentage used, and percentage free. This report is extremely useful when planning a migration or for growth planning to ensure that systems will continue to run without interruption.

Change Reports

Baseline Exchange Management Plan	This management report will also compare the results of a previous assessment with the current assessment.
Baseline Exchange Risk Report	This risk report will compare the results of a previous assessment with the current assessment.
Baseline Exchange Health Report	This report measures the overall risk to the environment by the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur. This report will also compare the results of a previous assessment with the current assessment.

SQL Server Assessment Reports

The **SQL Server Assessment** allows you to generate the following reports:

Standard Reports

Report Name	Description
Database Detail Report	This report details the settings and health of individual databases that reside on the scanned SQL Server. It lists the database properties, potentially missing indexes, locks, statistics, fragmentation, and existing indexes. Without this tool, it would be a daunting task to collect all this information. Because this report documents each database individually, it can be run ad-hoc when specific database performance problems arise. But best practice is not to wait and react to these problems but plan to run this report on a regular basis (quarterly or monthly, depending upon the how critical the application is). This report will help identify opportunities to improve performance and accumulate trending data that will help you anticipate problems before they occur. The report is also a great way to document your work for both internal and external uses.
Maintenance Plan Report	This report details all maintenance plans and their sub-plans. Maintenance plans perform routine tasks on your SQL Server. Not all maintenance plans are active and in-use, and you can use the report to document what's in place and if adequate automation of maintenance and backups are being performed.
Routine Health Report	This report assesses the health of the SQL Server using three major categories. These include settings, file, and resources. Setting health looks for configuration issues that may go against prescribed best practices. File health looks at how the database interacts with the file system, looking for adequate space and compares the current configuration versus best practices. Resource health looks to ensure adequate resources are available to operate the SQL Server optimally and looks for indicators pointing to performance issues. Resource health comprises of three sub-categories – wait health, task health, and memory health. Wait health deals with issues with database processing waits and delays. Task health validates that scheduled tasks and jobs are working optimally. Memory health looks to ensure adequate memory is available to run the SQL Server properly.

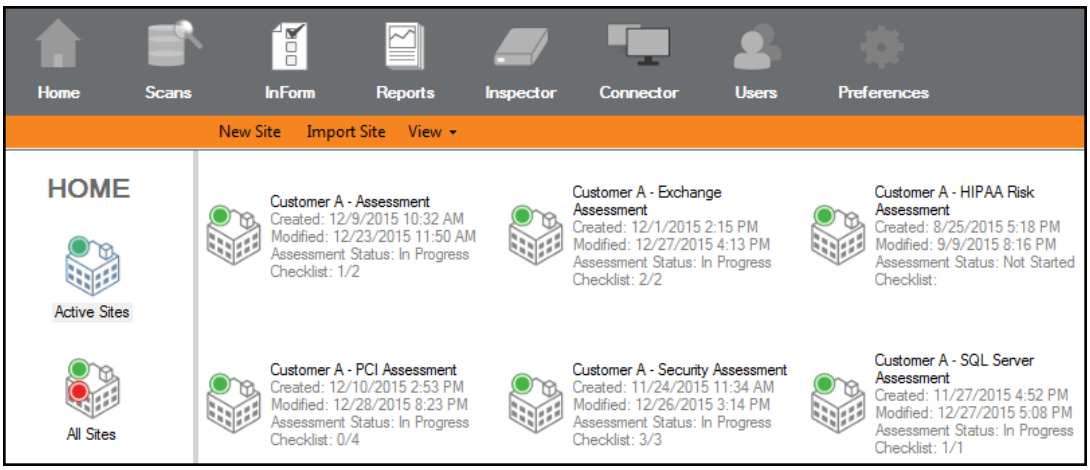
Report Name	Description
SQL Server Agent Jobs Report	This report details all jobs (active and inactive) for the SQL Server agent. Some jobs may be maintenance plans and can be seen in detail in the Maintenance Plan Detail report (see above). Look in the Job History section of this report for entries in RED or that do not say "success" and see what jobs are causing errors and why. This report is so simple to generate, even non-DBA tech can use it to check for errors in jobs. And since some Remote Monitoring and Management (RMM) tools do not delve into the actual database level, it makes sense to run this report monthly to supplement your RMM tool, and also to keep it "honest."
SQL Server Assessment PowerPoint	A PowerPoint version of the SQL Server Assessment, including key assessment details.
SQL Server Detail Report	This report details the settings and health of the SQL Server as a whole. It looks at settings, configuration, performance, and backup. Information and detailed breakdown of databases can be found in the Database Detail report.
SQL Server Health Report	The SQL Server Report details the overall risk to the assessment environment. The Health Score represents the number of issues detected. An ideal environment would have a Health Score of 0 (indicating no risks found). The higher the score, the more likely a security, availability, or performance related incident will occur. Unresolved issues are detailed item by item and are organized by risk score.

Change Reports

Report Name	Description
Baseline SQL Server Health Report	The Health Report details the overall risk to the assessment environment. It compares the results of the current assessment with the previous.

Downloading Scans with Client Connector

Downloading Scans using the Site Model is done on a Site-by-Site basis. In order to download Scans, you must first set up a Connector to associate with your Site.

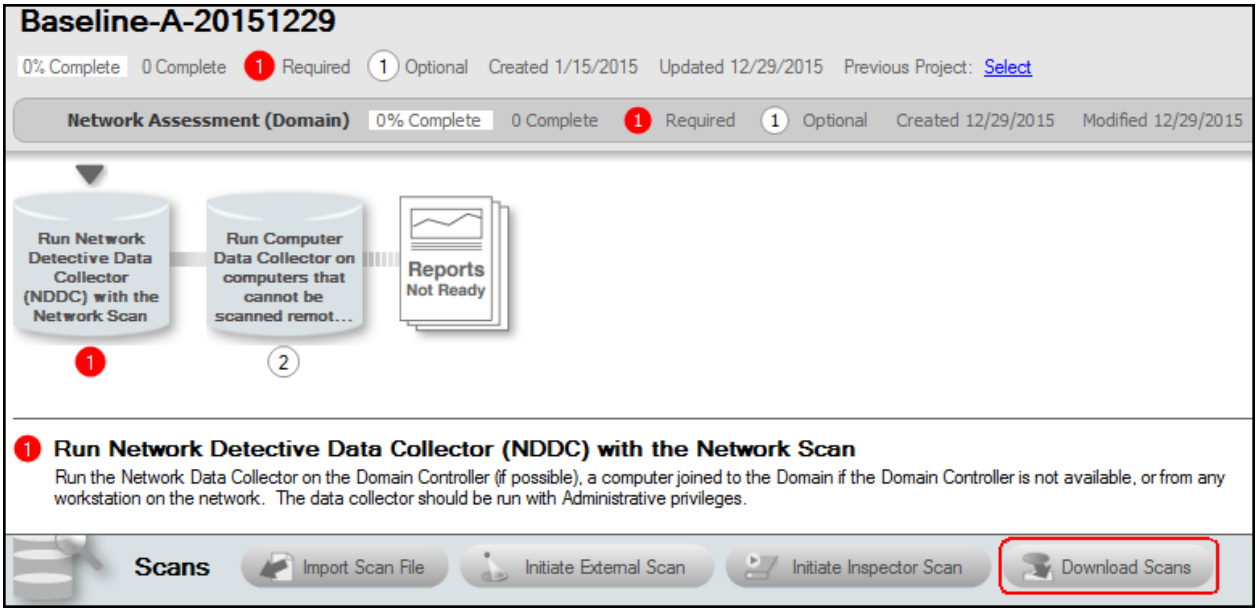


First, navigate to the desired Site from the Home screen by double-clicking on its icon.

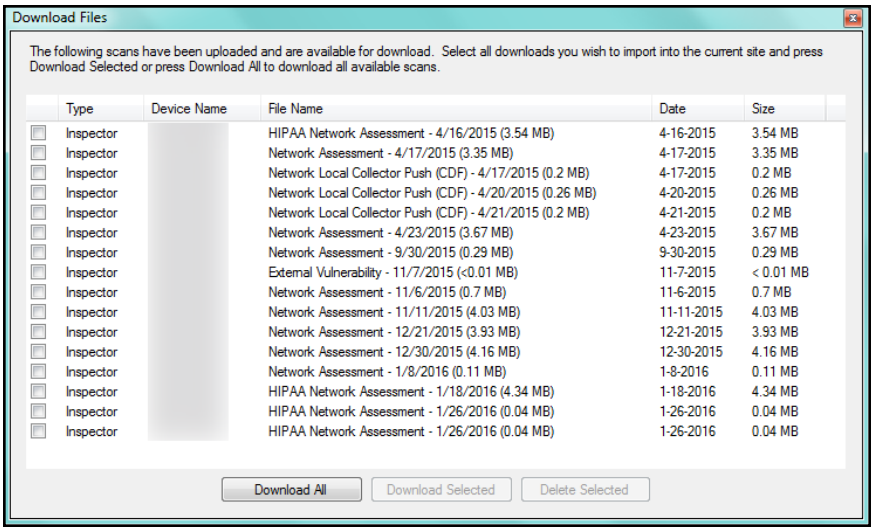
This will bring you to the Dashboard of the Site's current Assessment.

From the Site's Dashboard, you can view the Site's associated Connectors under the "Connectors" bar.

Here you can also view whether or not your Connectors have downloads available.



When the Assessment's Dashboard opens, click "Download Scans" from the "Scans" bar.



This will open a dialog box which will allow you to browse the Scans available from the Connector. You can select specific scans or use the "Download All" option.

After your Scans have finished downloading, they will be listed under the "Imported Scans" bar and you can use them to generate Reports.

Using InForm to Build Questionnaire Worksheet and Survey Templates for Enhanced Assessment Data Collection

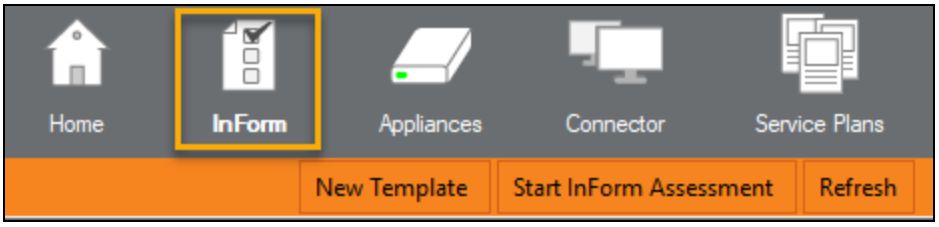
InForm allows you to create custom forms to gather information about a client and their site and generate reports. Your Interviews could focus on anything from purely technical information – server room security, cable management, etc. – to policies like BYOD.

Templates

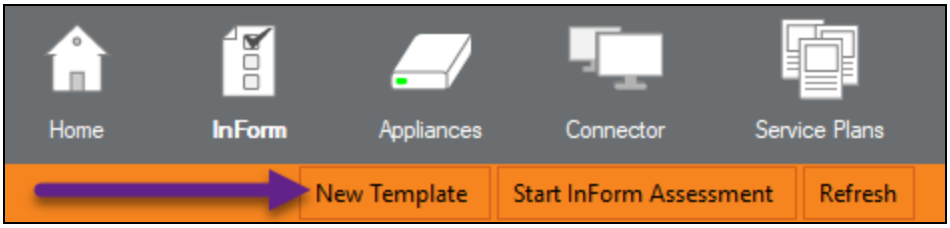
Templates represent a re-usable form design. Templates contain the list of Categories and Topics. You can have multiple templates for different types of clients (e.g. – Managed Services, Prospect, IT Site Survey etc.) or services (e.g. – Security Audit).

Creating a New Template

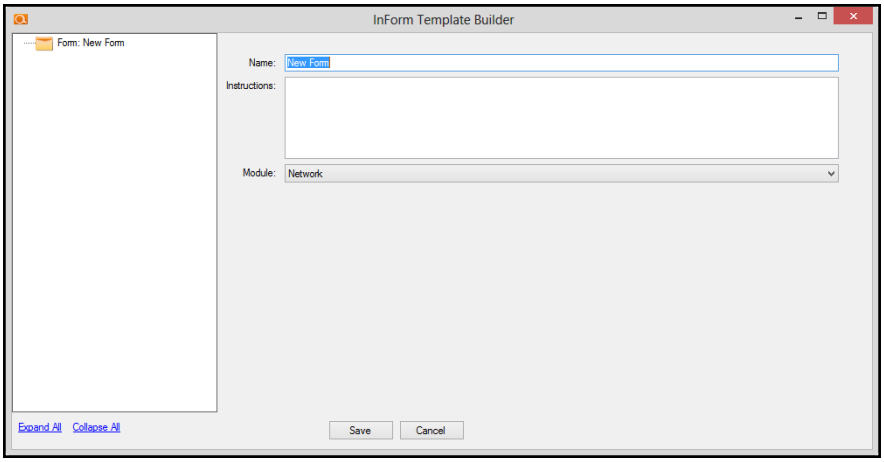
From the Network Detective Home screen, click on the InForm icon to start the Inform Template builder.



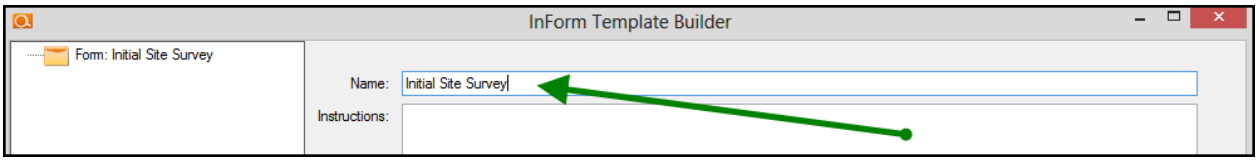
Selecting **New Template** will start the Inform template builder.



This action will start the Inform Template Builder as displayed below.

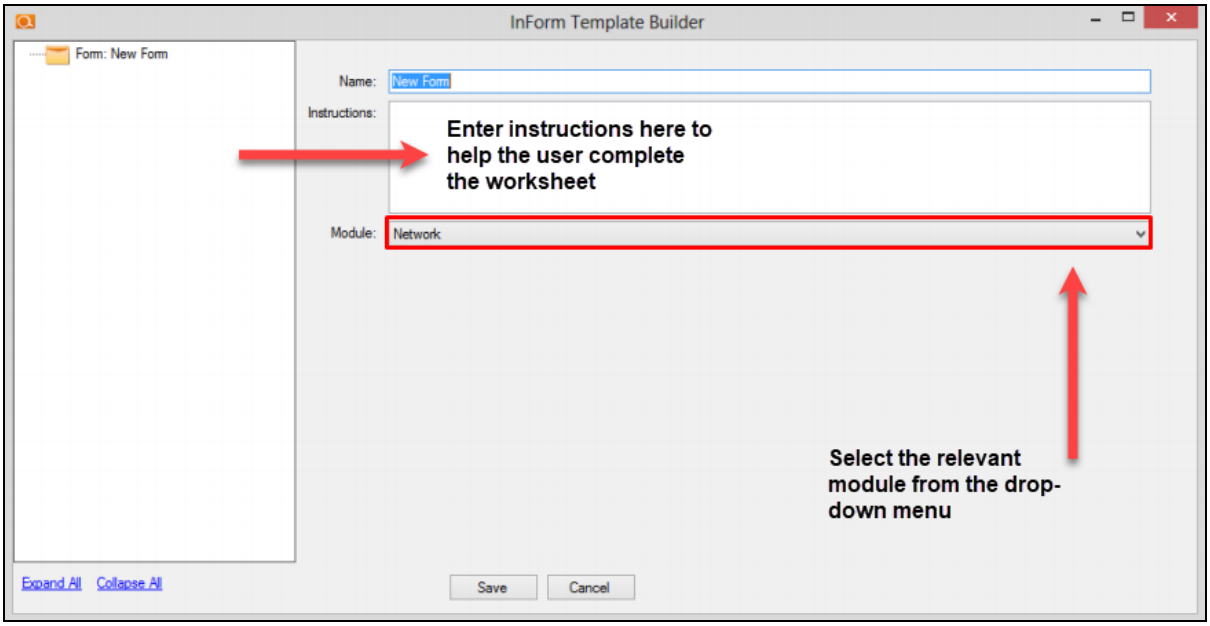


Change the name of the form. This will also change the filename for the template description file.

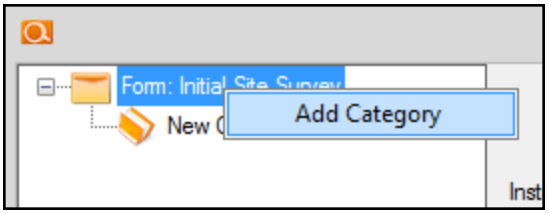


Include any instructions that would be helpful for the completion of this InForm, and select the relevant Network Detective module for this form.

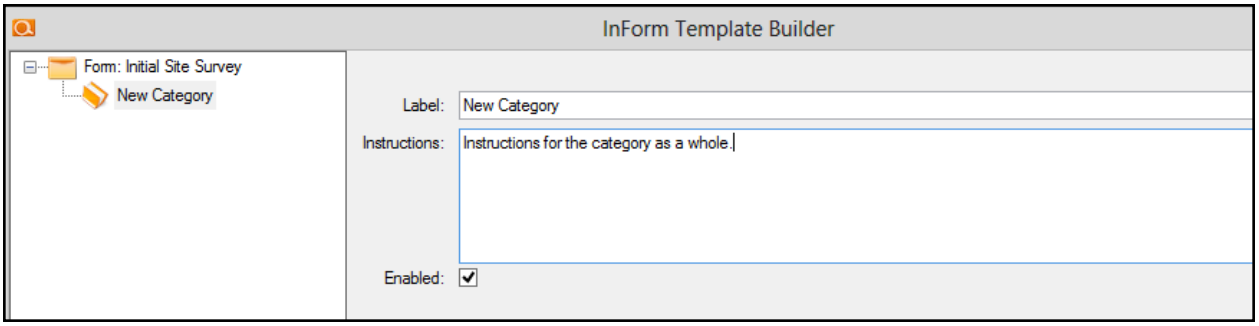
> **Note:** Any custom issues will only be applied to the documentation generated for the module selected in this dropdown.



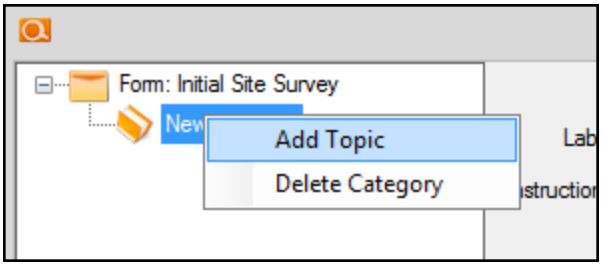
Right-click on the Form header or any other node to bring up the context menu. From this menu, you can Add New Categories. Categories are used to group various topics together.



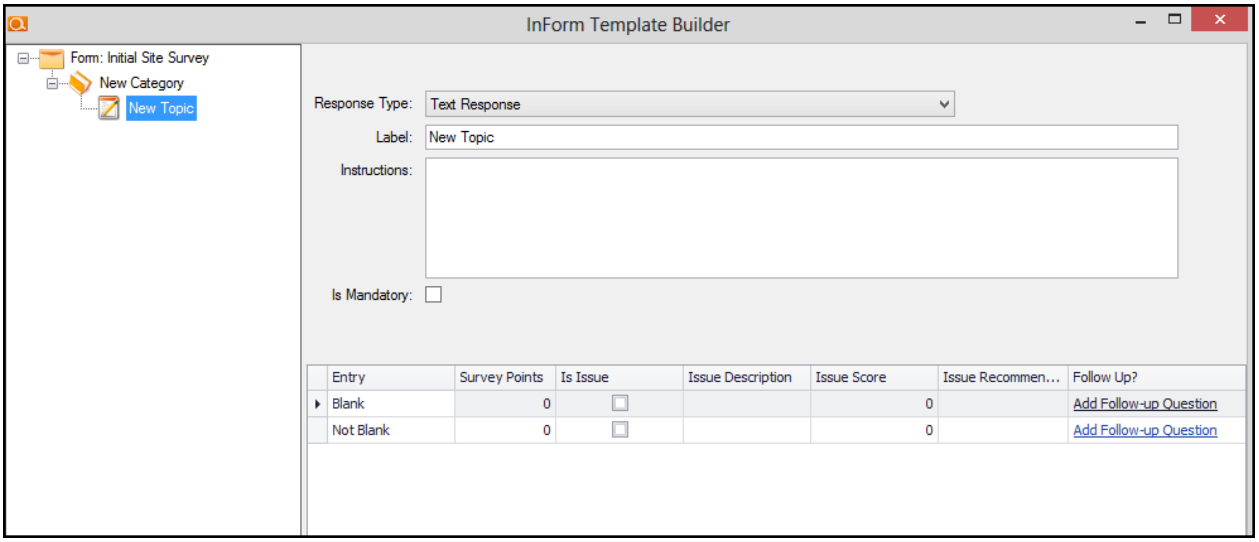
Use the category editor to change the label of the category and add instructions for the category as a whole.



Select the Category and right-click to add individual topics.



Use the topic editor to select the type of response, change the label for the topic, and add instructions for the topic.



Response Types

InForm supports 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 • Cannot Determine

Response Type	Description	Example Use
Checklist Item	An item that is marked off if done	Check the security of the door locks

Follow-ups

Follow-ups are Topics that will appear if a particular response to a question is chosen. You can add multiple follow-ups for a particular response by using the Add Follow-up Question link next to a particular response.

Issues

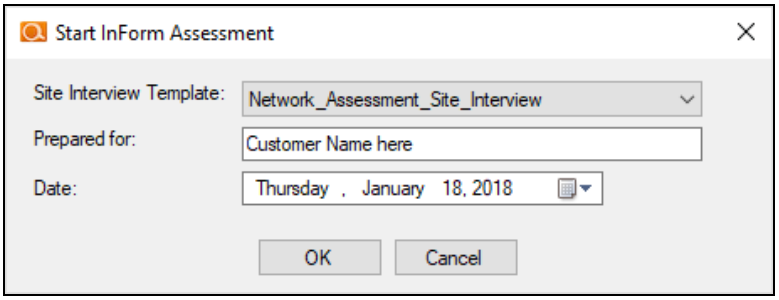
The selection of any response can be marked as an Issue. Issues must have the Issue Description, Issue Score, and Issue Recommendation completed. If a response is selected that is marked as an issue, the issue will be added to the Risk Analysis, Management Plan, and Power Point issue section. In this way, you can create forms that affect the risk and issue scores.

Response Forms

Response forms can be added to any assessment from the InForm section.

Creating a Response Form

From the InForm section, press the 'Add' button to add an InForm response form to the assessment.

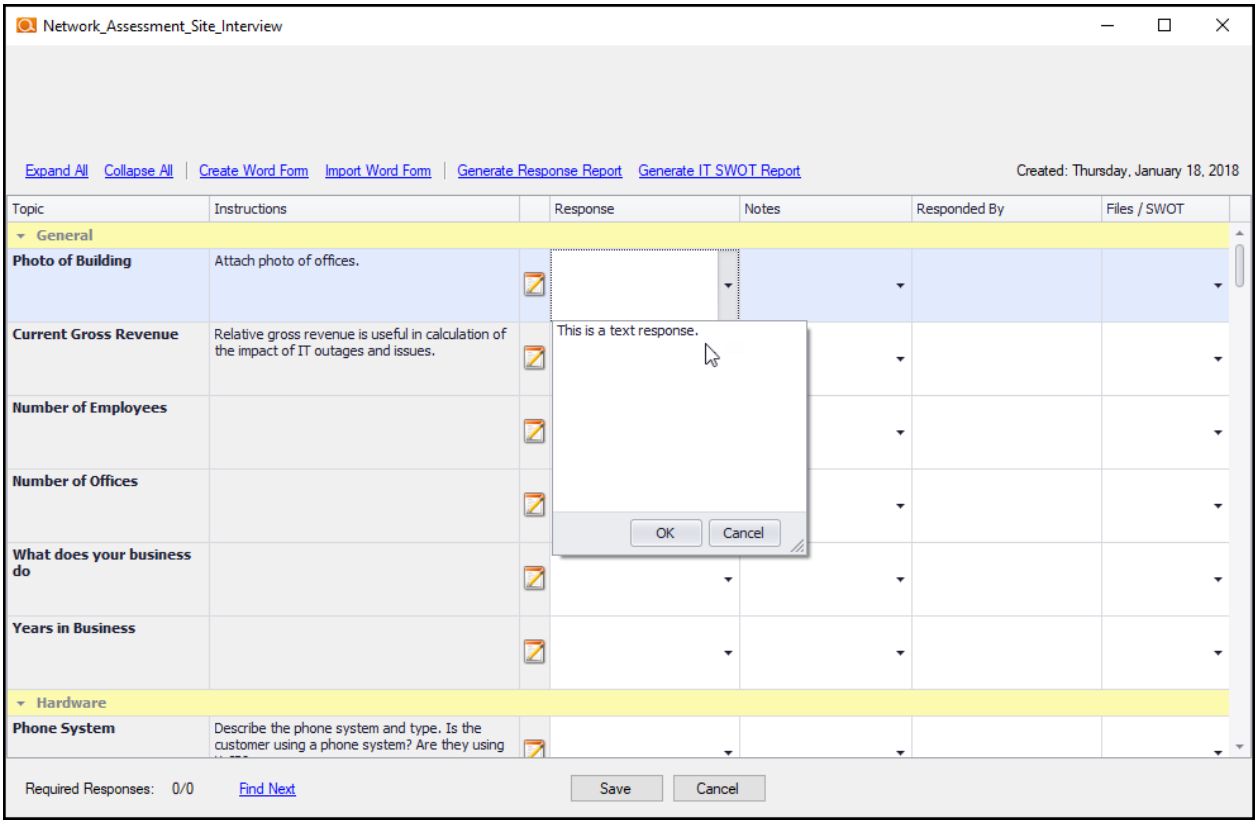


Click on the visit link to open up the response form.

Entering Responses

Use the response column to enter your answers for the various topics. Notes are used to augment or supplement the information in the responses. Files and SWOT are used to

attach pictures and other files, as well as specify strengths, weakness, opportunities, and threat entries.



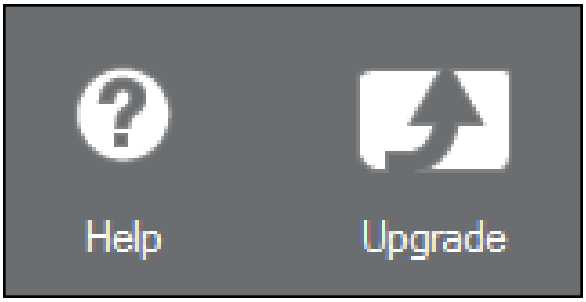
Generating Marketing Collateral and Sample Legal Forms

Network Detective makes available a series of **Videos**, **Recorded Webinars**, **Marketing Collateral**, and **Sample Legal Forms** to support your company's efforts to learn how to use Network Detective and support your company's efforts to offer of IT and Compliance Assessment services.

Generating Marketing Collateral

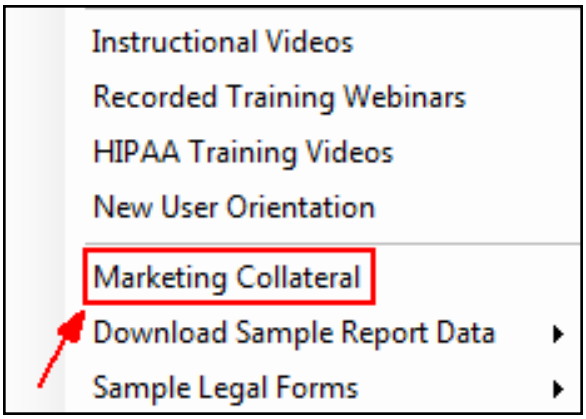
Follow these steps to generate **Marketing Collateral**:

1. Select the Network Detective Help icon.

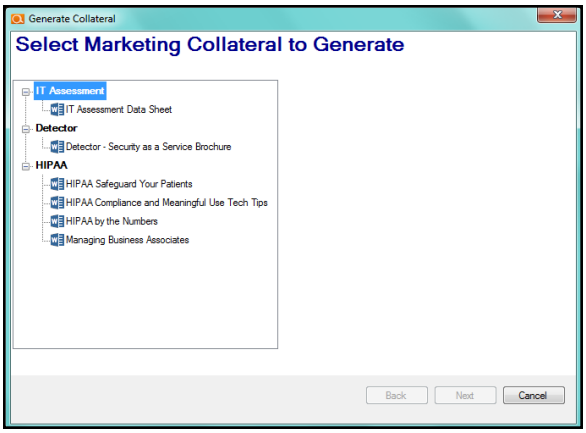


A menu will be displayed with a number of options to access videos and documents for your use.

2. Select the **Marketing Collateral** Menu option.



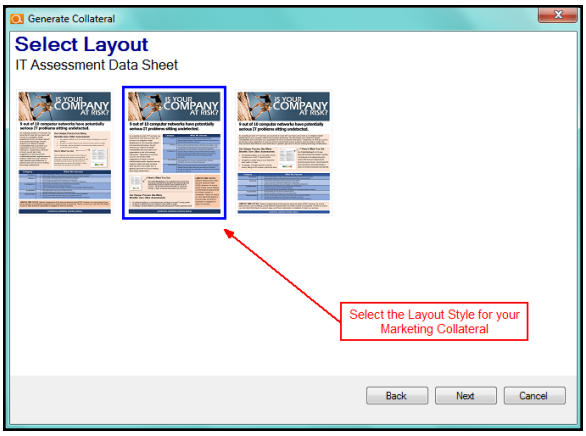
3. Select the **Marketing Collateral** document that you would like to **Generate**.



Select the **Next** button to continue.

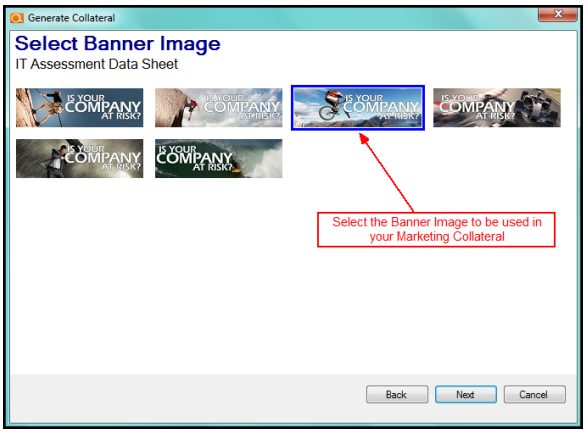
4. Select the **Layout** for the brochure you want to **Generate**. With some **Marketing Collateral** selections, the **Select Layout** option step may not be presented.

   Then select the **Next** button to continue.

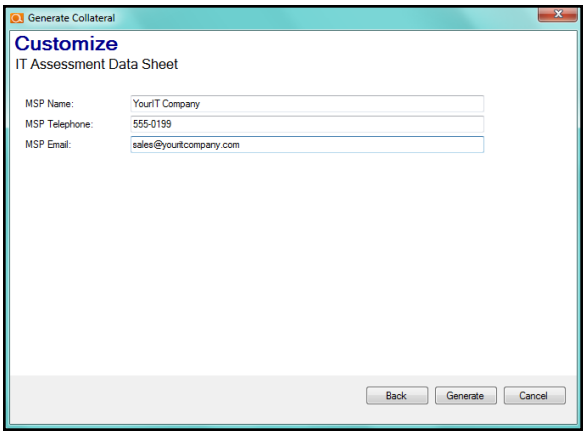


5. Select the **Banner Image** for your **Marketing Collateral**.

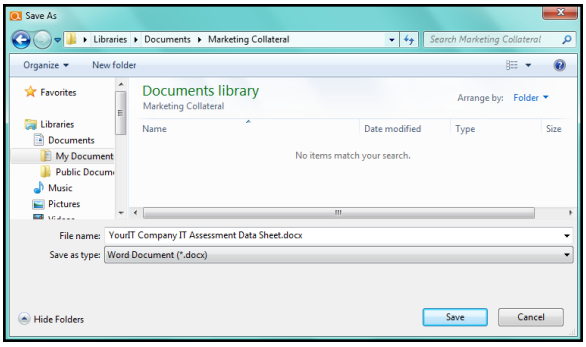
   Then select the **Next** button to continue.



6. Enter in your **Company Name**, **Telephone Number**, and **Email** address for placement into the **Marketing Collateral** to be generated.

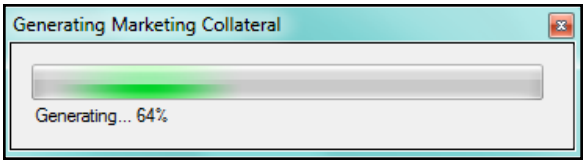


7. Select the **Generate** button to generate the **Marketing Collateral** document.
8. Before generating the actual **Marketing Collateral** document, you will be prompted for the location where your **Marketing Collateral** will be saved.

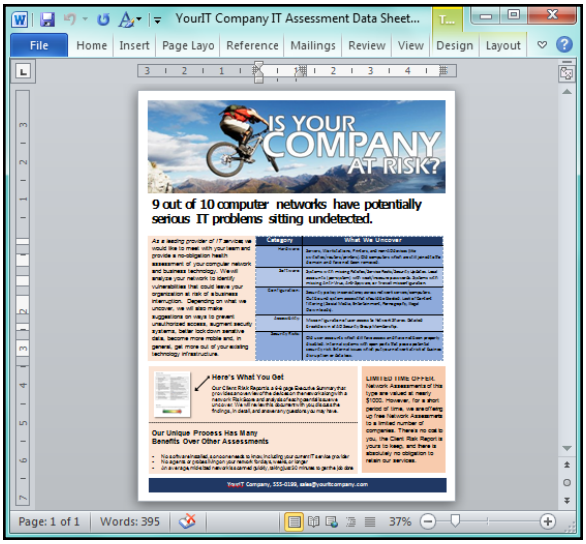


Select the location where the document should be stored and select the **Save** button.

9. The **Marketing Collateral** document will be generated.



10. After the **Marketing Collateral** document is generated and saved to the location you specified, the document will be opened and displayed in Microsoft Word.



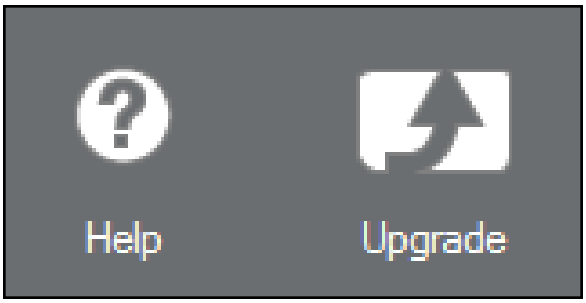
Downloading Sample Legal Forms

> **Note:** Disclaimer: RapidFire Tools provides sample Managed Services agreements, Business Associate agreements, legal templates and other self-help services as a convenience with your subscription. RapidFire Tools is not a law firm or substitute for an attorney. You should consult with your law firm and have them review and evaluate any legal document before using.

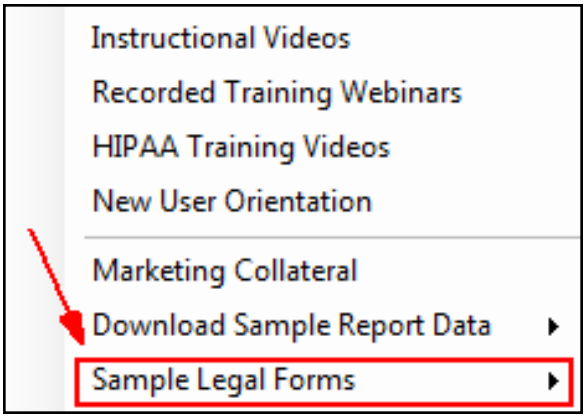
Follow these steps to download **Sample Legal Forms**:

1. Select the Network Detective **Help** icon.

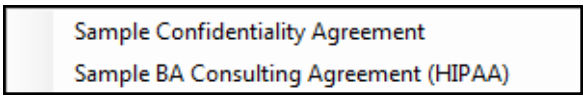
   A menu will be displayed with a number of options to access videos and documents for your use.



2. Select the **Sample Legal Forms** Menu option.

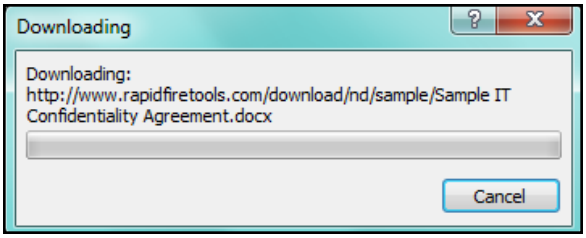


3. Select either the **Sample Confidentiality Agreement** or the **Sample Business Associate Consulting Agreement** in order to download the selected **Sample Agreement** for your use.

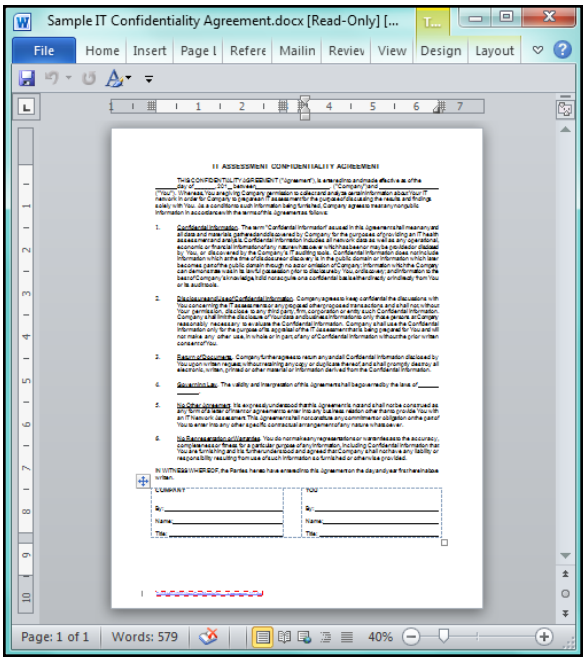


For illustration purposes, the **Sample Confidentiality Agreement** has been selected.

4. After selecting the **Sample Agreement** of your choice, Network Detective will prompt you to define a location to save the Sample Agreement document, then it will proceed with downloading the document file.



After the **Sample Agreement** document is downloaded, it will then be automatically opened by Microsoft Word for your use.



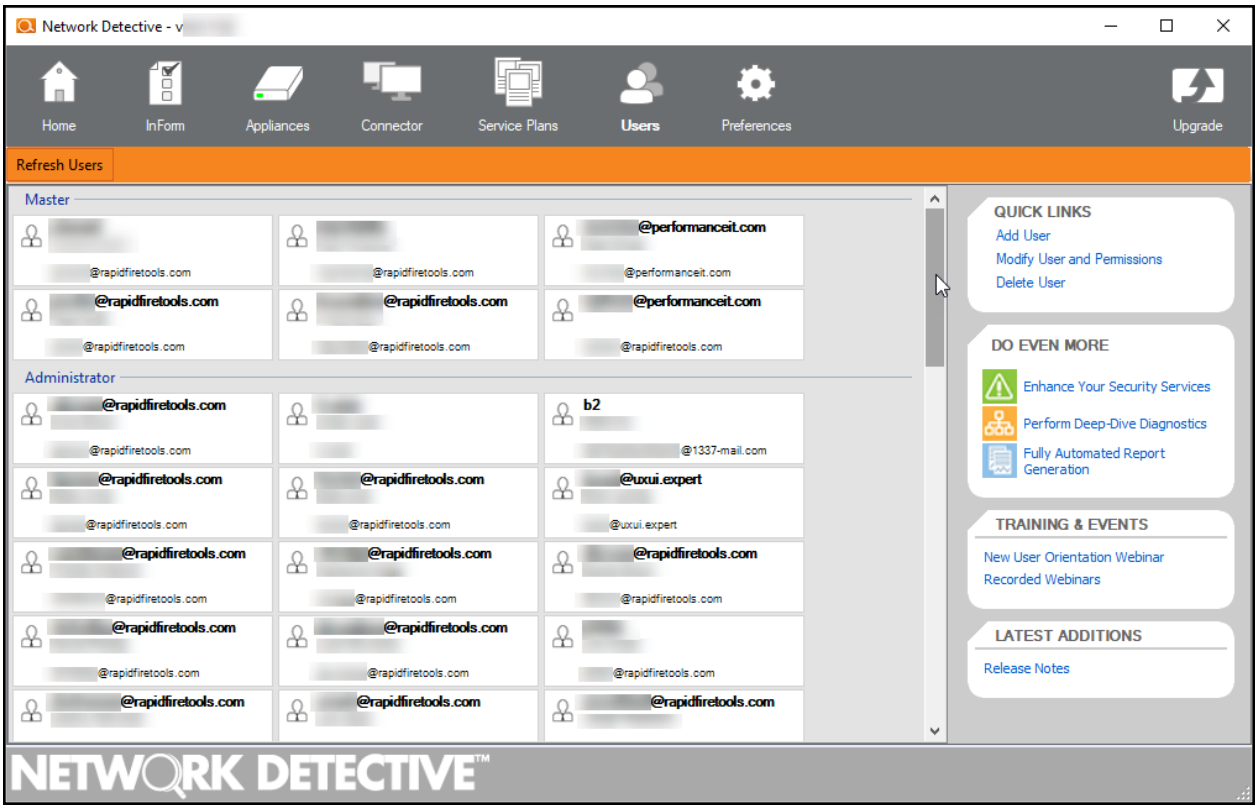
5. Save the document for your use.

Managing Network Detective Users

Use the manage Users option to add or remove users from your company's Network Detective subscription.

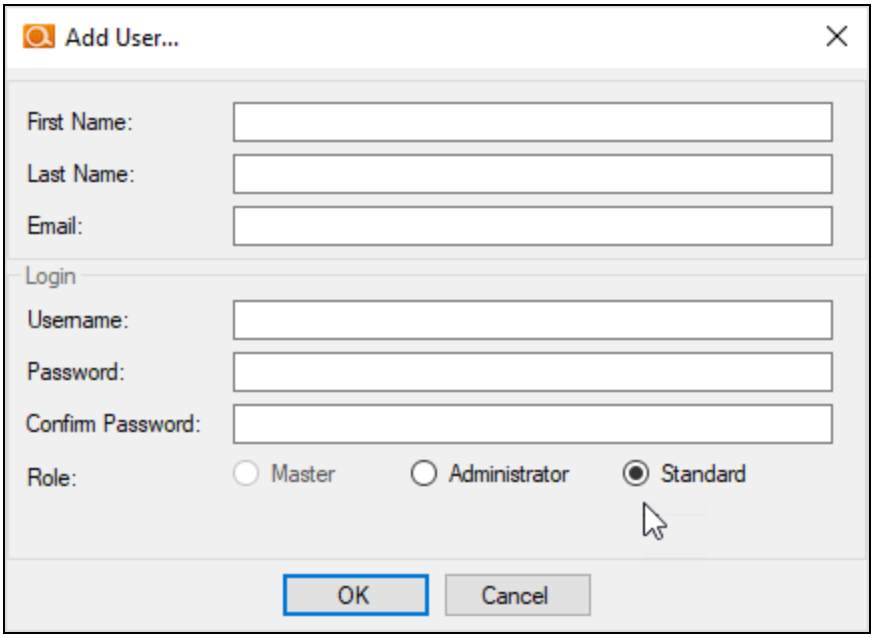
Access the manage Users option by selecting the User icon on the Network Detective bar.

You can add users to the account so that they can run reports. Upon selecting the **Users** option, the following screen will be displayed:



Click **Add User** in the top right corner to add a new user.

Then enter the information and credentials for the user.



Finally, select the type of Role the new user should have. The Role determines the user's level of access:

- **Standard Users** *cannot access* Manage Users, Preferences, and Billing
- **Admin Users** *can access* Manage users and Preferences, *but not* Billing
- **Master Users** can manage Users, Preferences, and Billing

Appendices

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)

Complete	Domain Configuration
	• File and Printer Sharing (NB-Session-In)
☐	Enable *Remote Registry* "read only" access on computers targeted for scanning. **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

Complete	Domain Configuration
	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)
	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:

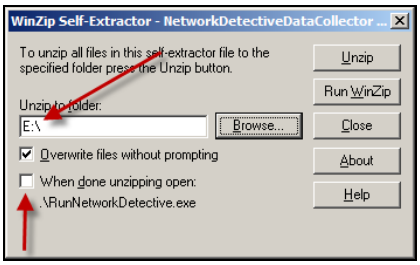
Complete?	Workgroup Configuration
	Network Settings
☐	• *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
☐	• *File and printer sharing* must be enabled on the computers you wish to scan
☐	• *Ensure the Windows Services below 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.

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

Using a USB drive

It is often handy to use a USB drive so that you are not downloading anything onto the client or prospect machine. And it is extremely useful when using the Local Data Collector.

To setup the USB drive, simply download and run NetworkDetectiveDataCollector.exe, and unzip it directly to the USB drive (uncheck “When done unzipping…”).



To run a scan from the USB, run any of:

RunNetworkDetective.exe – runs the interactive Data Collector. This is the same as downloading and unzipping/running the Data Collector from the download site.

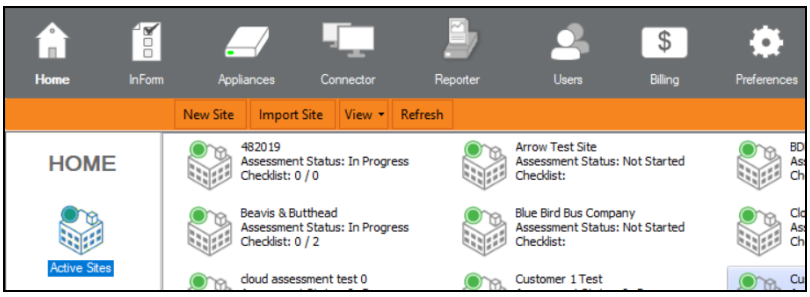
runLocal.bat – runs the Data Collector to perform a Local Data Collection, and will pop up a dialog with the folder containing the CDF file once complete. Note that the CDF file output is stored on the root of USB and in the “CDF” folder that will be created. This way all CDFs from multiple machines are in one folder.

runLocalSilent.bat – runs the Data Collector to perform a Local Data Collection, but does not pop open a dialog box. Note that the CDF file output is stored on the root of USB and in the “CDF” folder that will be created. This way all CDFs from multiple machines are in one folder.

Adding a Connector to a Site

As an alternative to importing Scans from a local source, Scans can be downloaded remotely via the Network Detective Client Connector service.

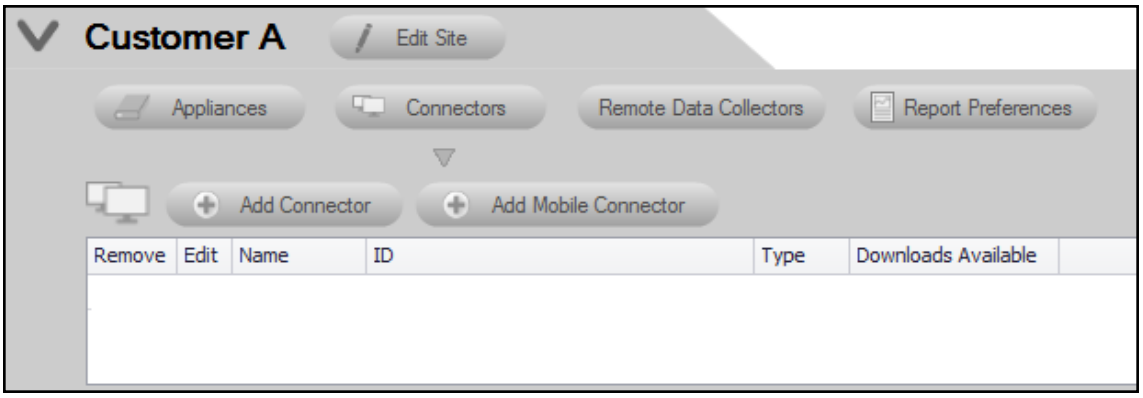
Preferences for Client Connectors are configured on a Site-by-Site basis and can be customized for each individual site.



To add a Connector to a Site, first navigate to the desired Site from the Home screen by double-clicking on its icon.

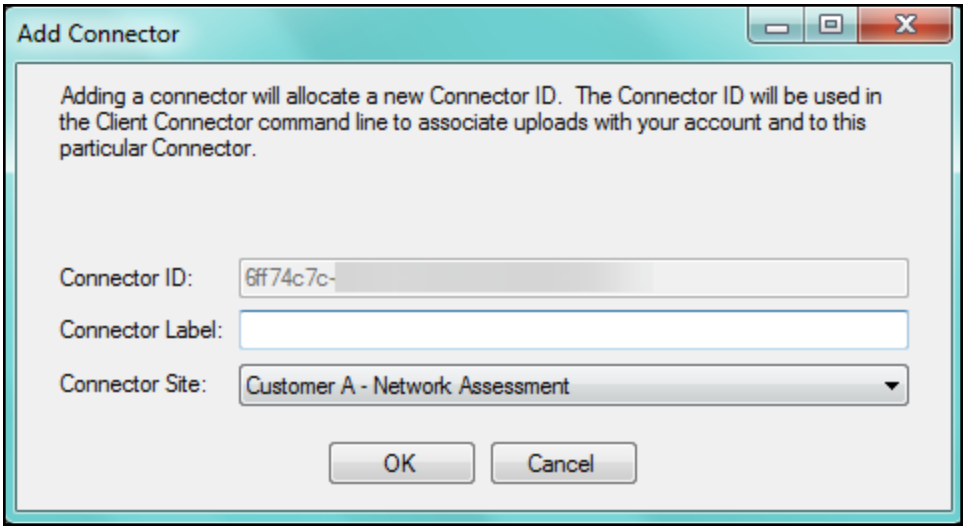
This will open the Site's Dashboard.

From the Site's Dashboard, select the selector control to the left of the Assessment's name to access the **Connector** setup option.



By selecting the **Connectors** option, then the **Add Connector** button you will be prompted with a wizard to configure the Connector. Enter a unique label for the Connector. If you wish, the label can be identical to the **Site Name**.

Note: Note that the Connector ID is randomly generated and will be used to configure the Connector.



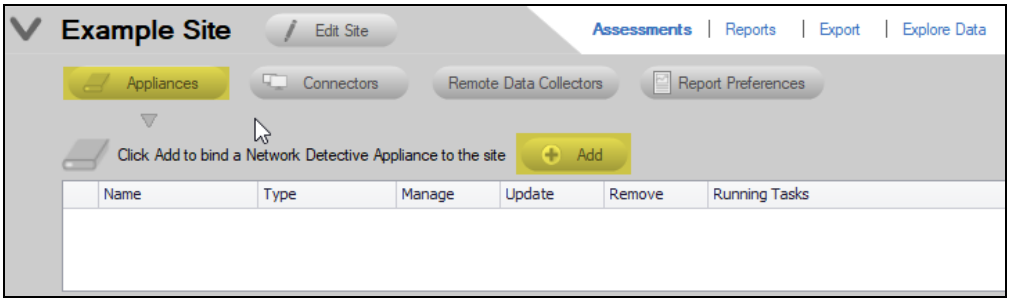
Next, configure your Connector.

You can now use your Connector to download Scans and associate them with your Assessments.

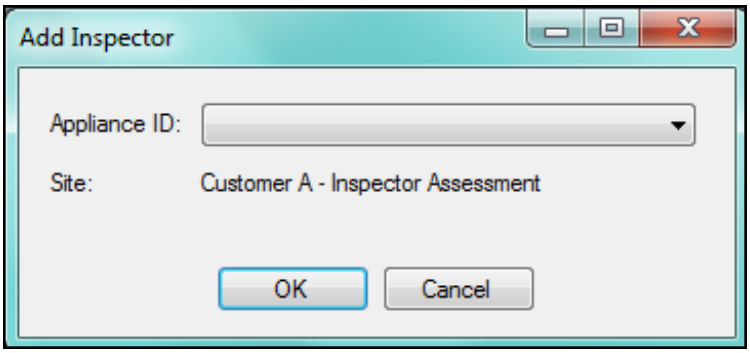
Adding an Inspector to a Site

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.

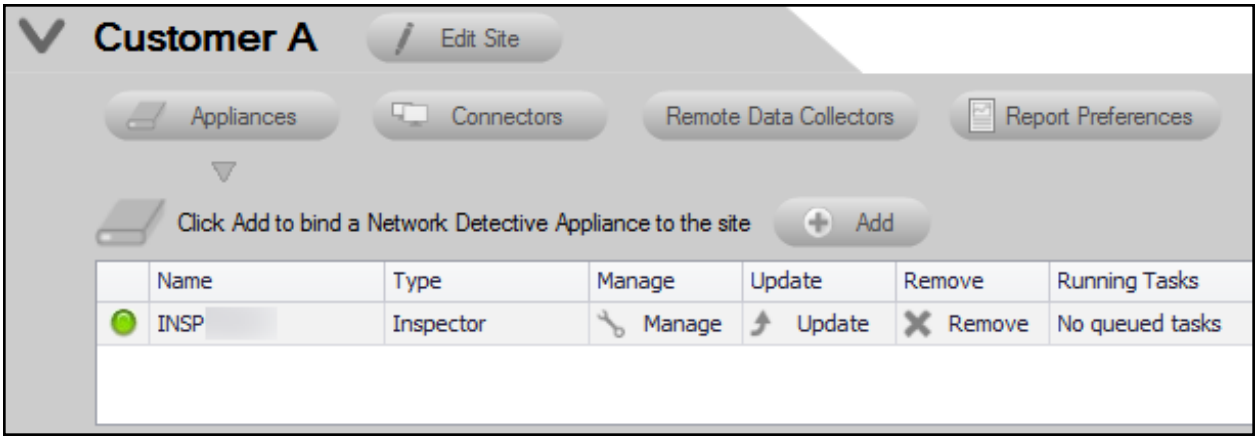


To add an Inspector to an Assessment, from the Assessment’s dashboard select the **Inspector** button, then the **Inspector Add** button as noted above.

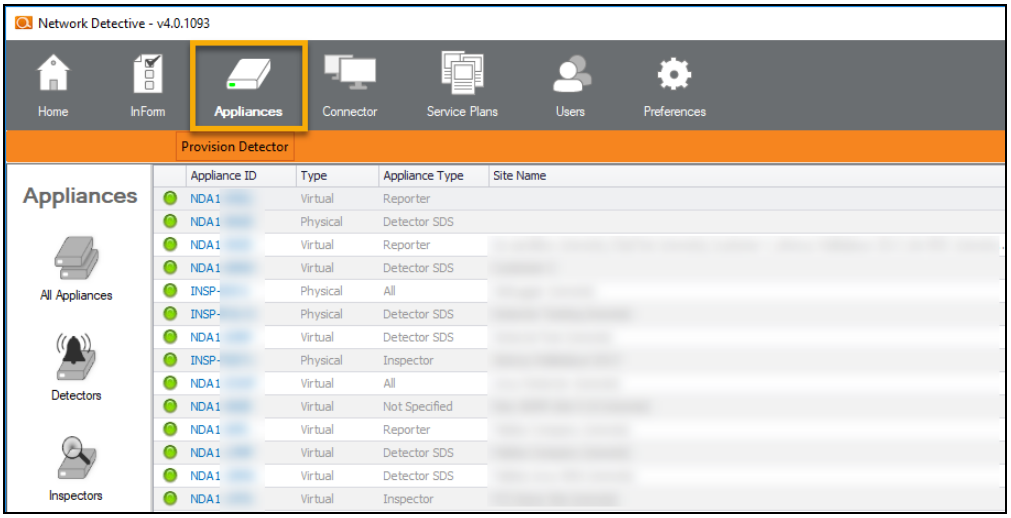


Select the **Inspector ID** of the Inspector from the drop down menu. Note that the Inspector ID can be found on a printed label on the Inspector Appliance.

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



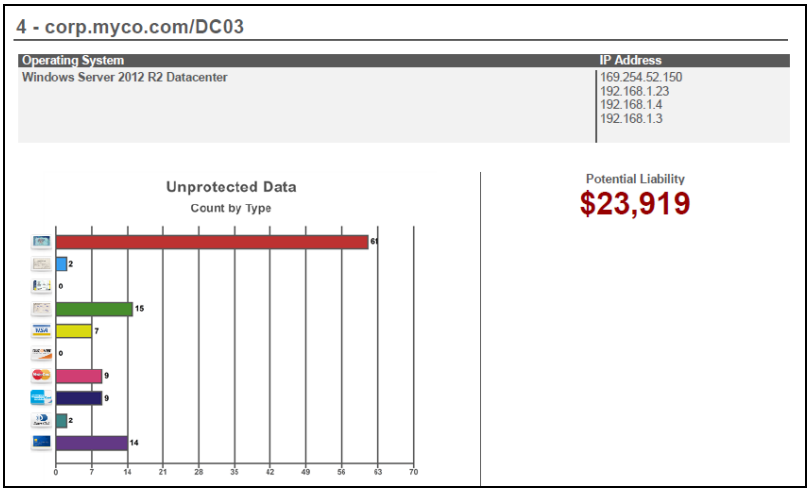
To view a list of all Inspectors and their associated Sites, navigate to the **Appliances** tab from the top bar of the Network Detective Home screen. This will show a summary of all Inspectors, their activity status, and other useful information.



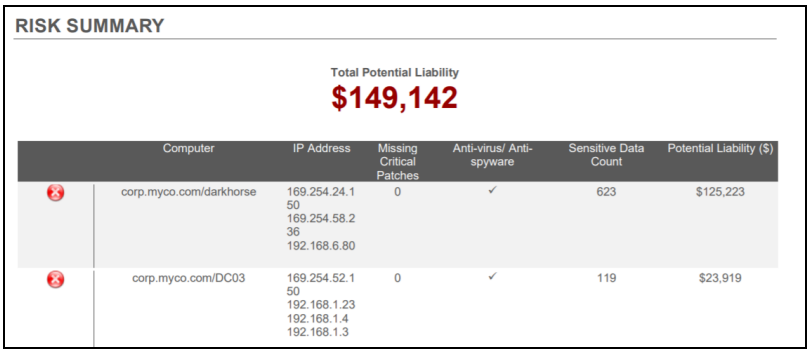
To return to the **Site** that you are using to perform your assessment, click on Home above and select the Site that you are using to perform your assessment.

Data Breach Liability Scanning and Reporting

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



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



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

- Visa card
- Mastercard
- Discover Card
- Diners Club United States & Canada
- Mastercard Diners Club Alliance

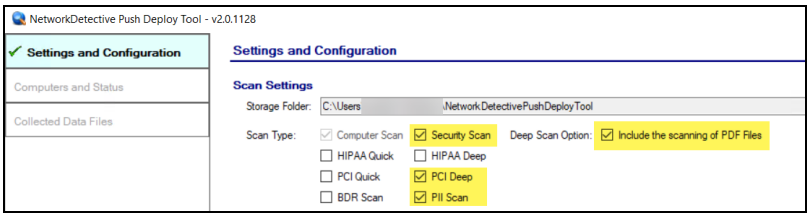
- American Express
- Date of Birth
- SSN
- Drivers License
- ACH (bank transfer information)

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

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

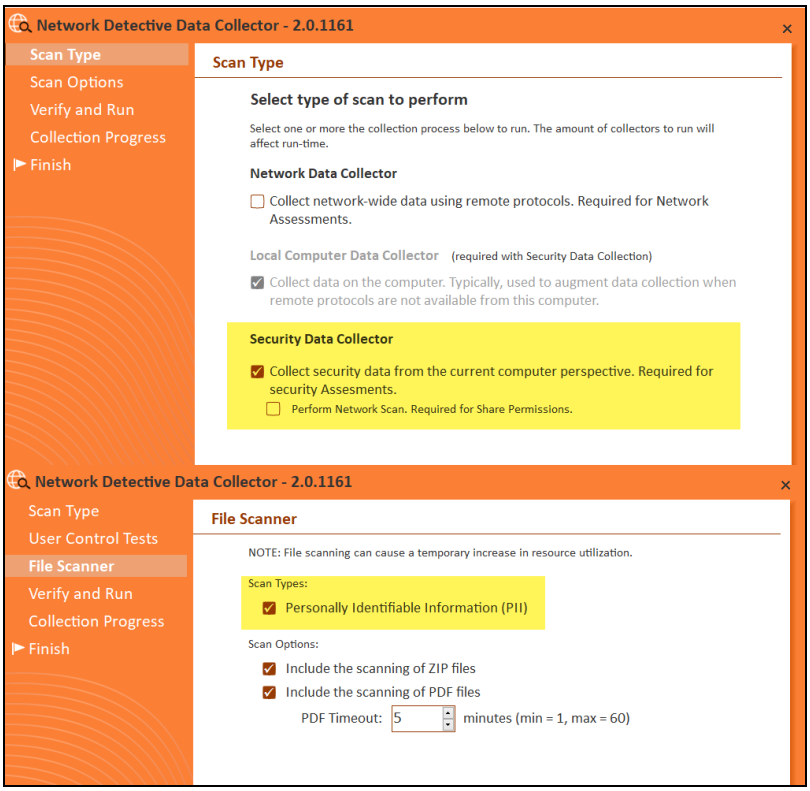
You can perform the extra scans needed for a complete Data Breach Liability Report as part of a normal Security Assessment. To do this:

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

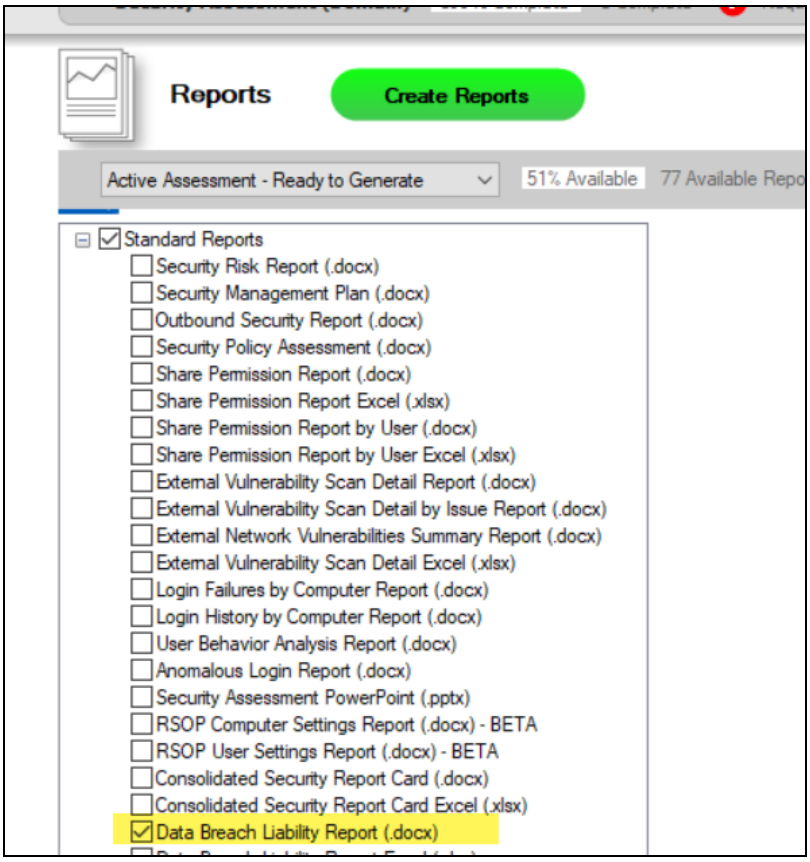


> **Note:** Also select whether you want to scan PDF files. Note that this may significantly increase total scan time.

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



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


Reports
Create Reports
Active Assessment - Ready to Generate
51% Available
77 Available Repo
Standard Reports
Security Risk Report (.docx)
Security Management Plan (.docx)
Outbound Security Report (.docx)
Security Policy Assessment (.docx)
Share Permission Report (.docx)
Share Permission Report Excel (.xlsx)
Share Permission Report by User (.docx)
Share Permission Report by User Excel (.xlsx)
External Vulnerability Scan Detail Report (.docx)
External Vulnerability Scan Detail by Issue Report (.docx)
External Network Vulnerabilities Summary Report (.docx)
External Vulnerability Scan Detail Excel (.xlsx)
Login Failures by Computer Report (.docx)
Login History by Computer Report (.docx)
User Behavior Analysis Report (.docx)
Anomalous Login Report (.docx)
Security Assessment PowerPoint (.pptx)
RSOP Computer Settings Report (.docx) - BETA
RSOP User Settings Report (.docx) - BETA
Consolidated Security Report Card (.docx)
Consolidated Security Report Card Excel (.xlsx)
Data Breach Liability Report (.docx)

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

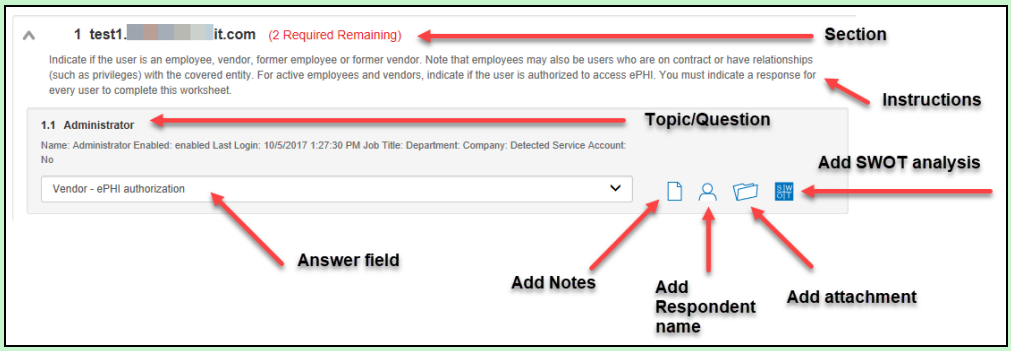
Entering Assessment Responses into Surveys and Worksheets

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 Network Assessment process.

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

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

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

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

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

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

Add Image Attachments to Surveys and Worksheets

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

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

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

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

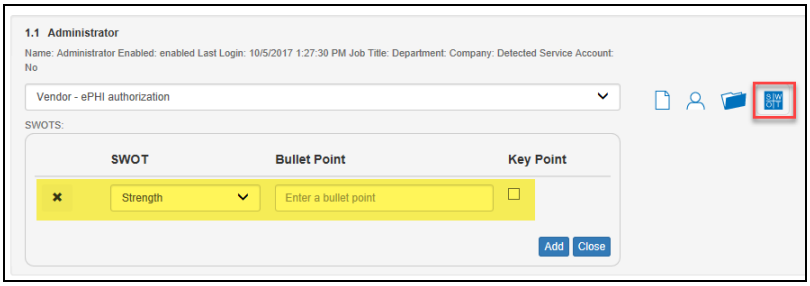
> **Note:** Once you complete your assessment and generate reports, your attached images will appear alongside the form item in the published report and/or supporting document.

Add SWOT Analysis to Surveys and Worksheets

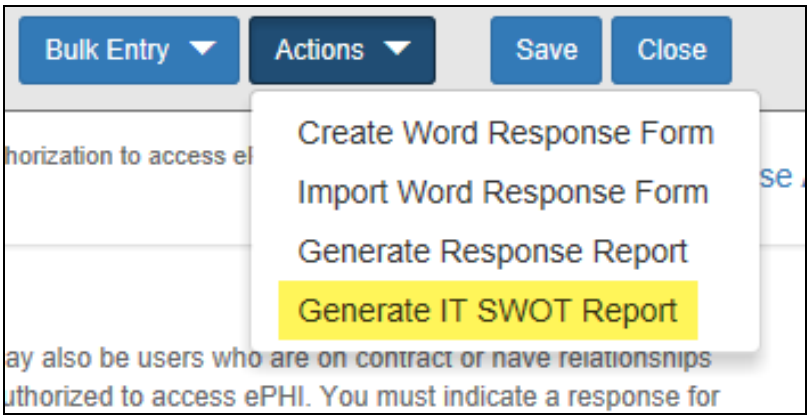
The IT SWOT analysis is a structured method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats affecting an IT network. The analysis involves identifying internal and external issues that are favorable and unfavorable to increasing the overall network health and security of the environment.

To add SWOT to your inform items:

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



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

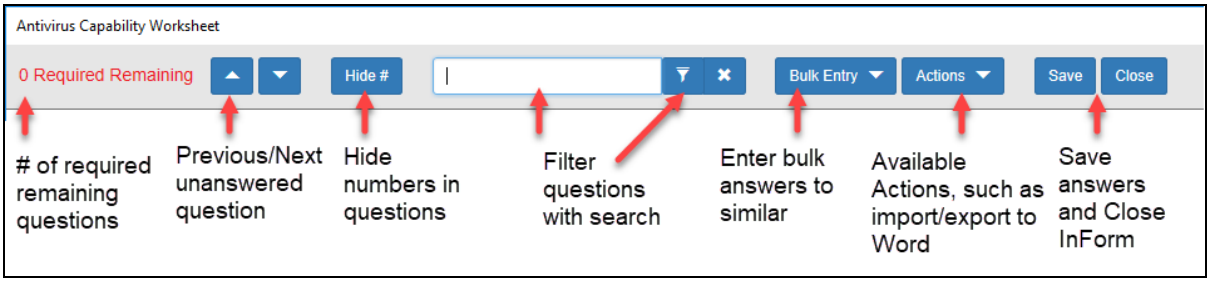


Note: A folder will open with your generated IT SWOT Report. You must generate this report separately for each InForm in your assessment.

Time Savings Tip to Reduce Survey and Worksheet Data Input Time

Use the InForm Worksheet Tool Bar

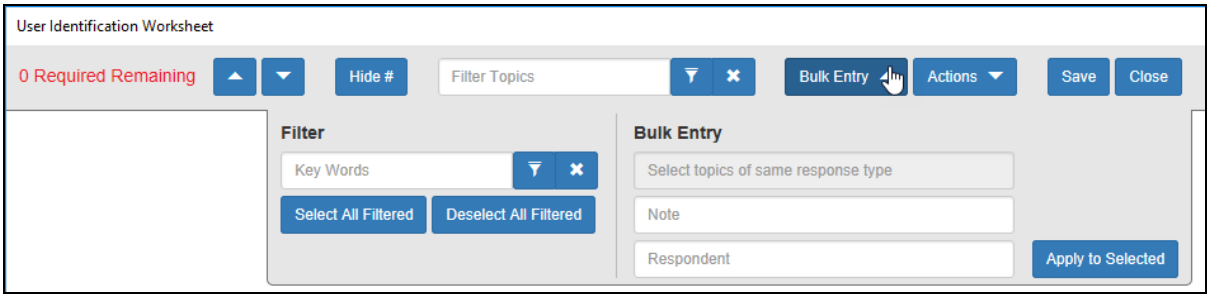
Use the InForm tool bar to save time when completing worksheets.



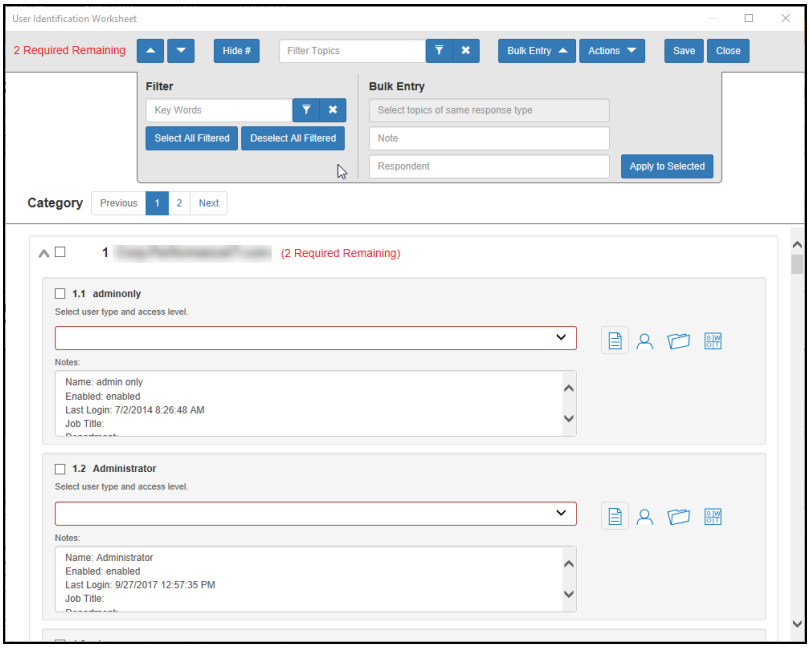
Bulk Entry for InForm Worksheets

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

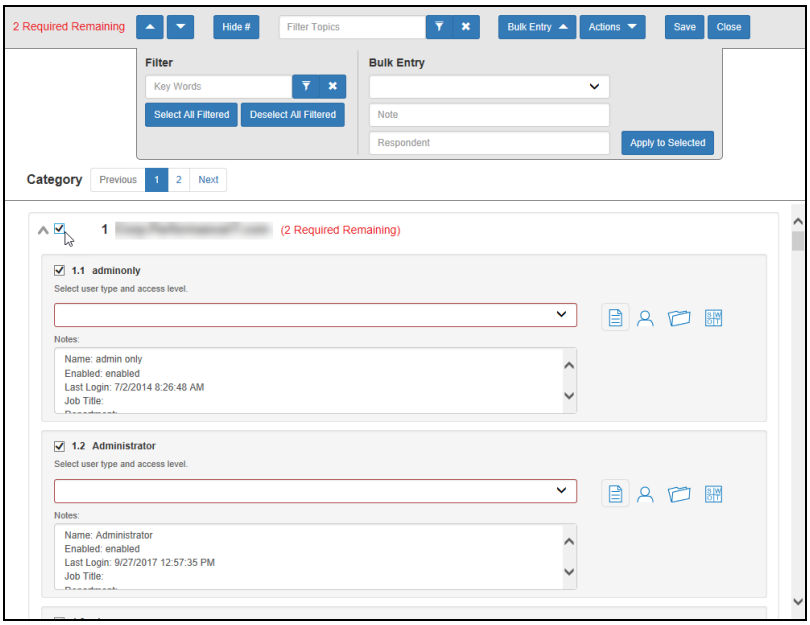
1. Click **Bulk Entry** from the Inform tool bar.



Check boxes will appear next to the response topics.

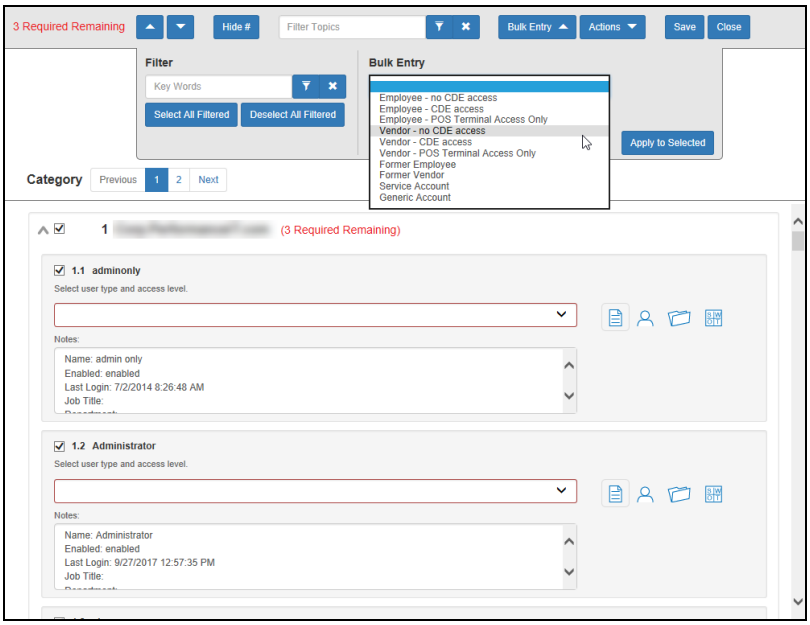


2. Select the check boxes for the topics for which you wish to enter bulk responses.

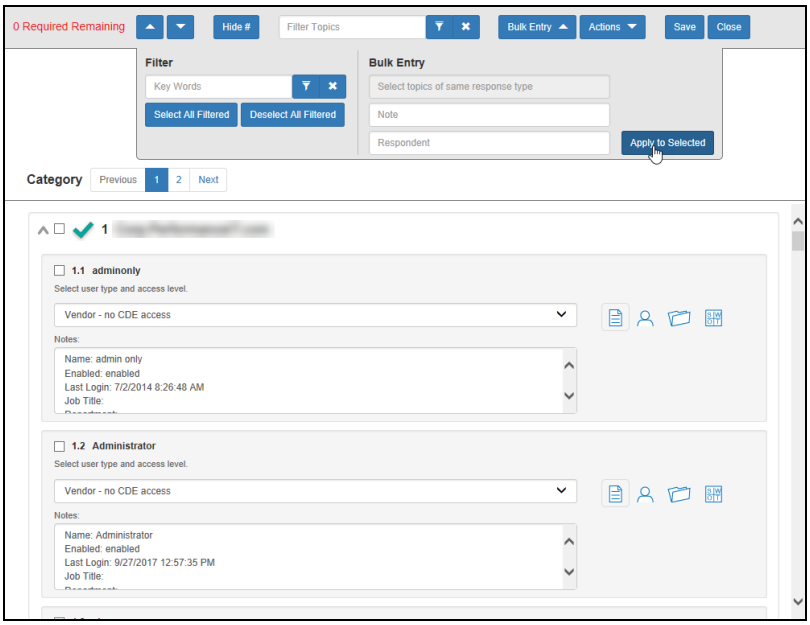


Note: You can select individual topics, or you can click the check box next to the section heading to select all topics within the section. You can also **Filter** topics using terms like "Admin." Note that each topic within the section must require the same types of responses in order to enter bulk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

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



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



Your chosen response will be entered into the selected topics.

Create Word Response Form

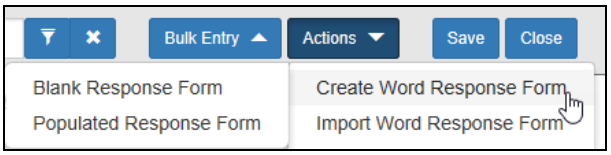
You can export InForm worksheets in your assessment project to Word. This allows you or others to complete worksheets without using Network Detective. For example, you can create a Word response form and send it to a client at a site. The client can then help you gather the required information and enter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

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

To create a Word response Form:

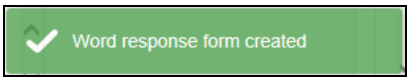
1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
    a. Click **Blank Response Form** to generate a Word document with blank fields ready for data entry.
    b. Click **Populated Response Form**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

responses already entered using InForm.



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

   A confirmation message will appear.



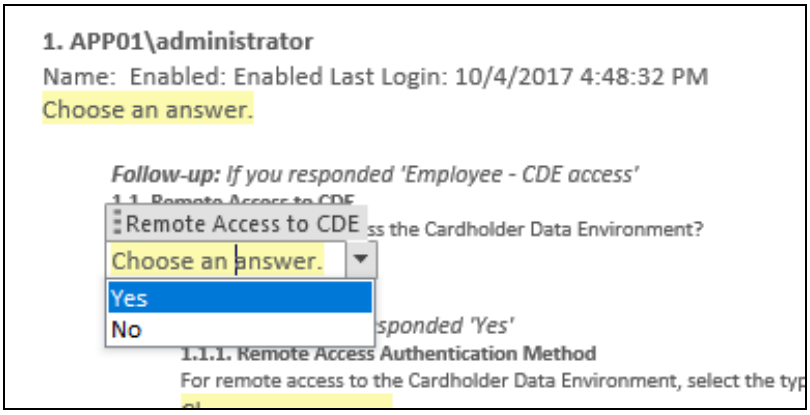
Important Note on Working with Word Response Forms

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

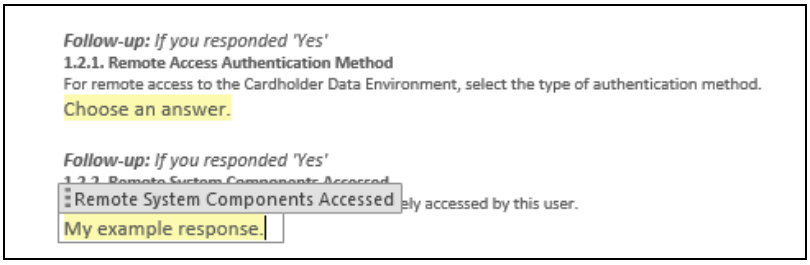
- **DO NOT DELETE** the field controls embedded in the response form! The response fields appear in the images below for your reference:

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

  Multiple choice response field



  Text response field



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

Import Word Response Form

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

EXAMPLE:

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

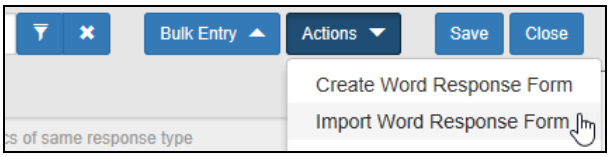
Step 2: Send it to a client to enter additional information about the site using Word.

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

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

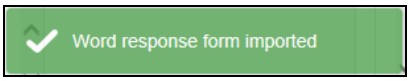
To import a Word response form:

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



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

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



Mac Data Collector

The Mac Data Collector may be run via a .cmd (command), or through Terminal (Macintosh's Command Prompt).

Running As .cmd

After downloading the .zip file containing the Mac Data Collector, double click to extract it to a directory (jump drive, desktop, etc.).

This outputs a file called NetworkDetectiveMacCollector.cmd.

Double click the .cmd, and the collection will run. When complete, a .cdf is produced in the directory the scan was initiated from.

Scripting

If scripting, download and extract as above. You may then add the following optional arguments to change the output directory or filename:

Argument	Result
-f	Specifies filename for .cdf
-d	Specifies output directory for .cdf

Troubleshooting

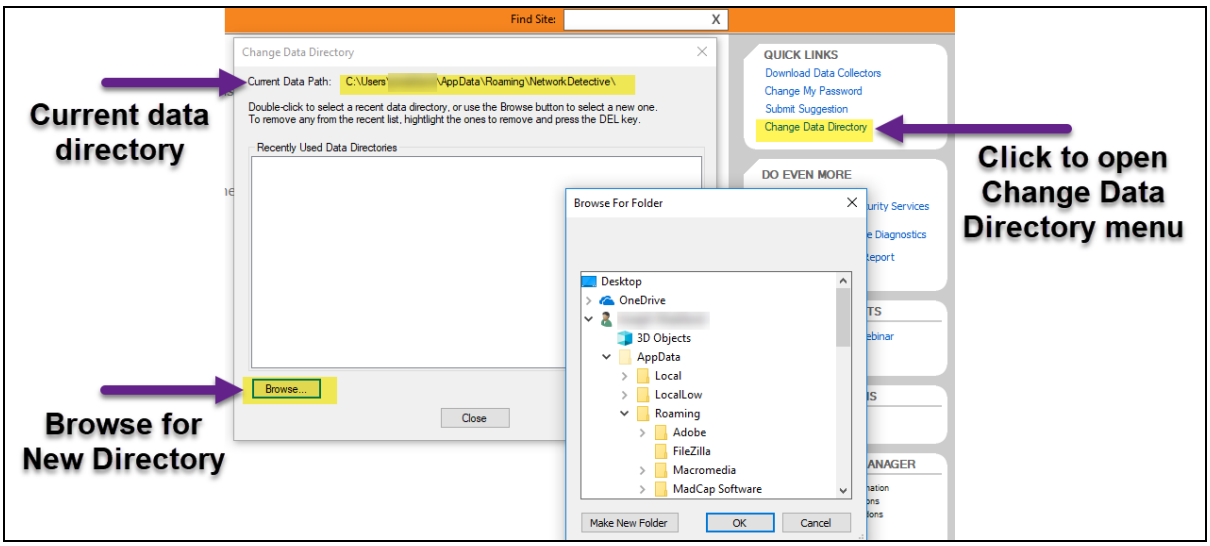
If double-clicking the .cmd does not produce a .cdf, try deliberately running the .cmd from Terminal.

Right click the .cmd and select **Open With**, then navigate to Terminal.

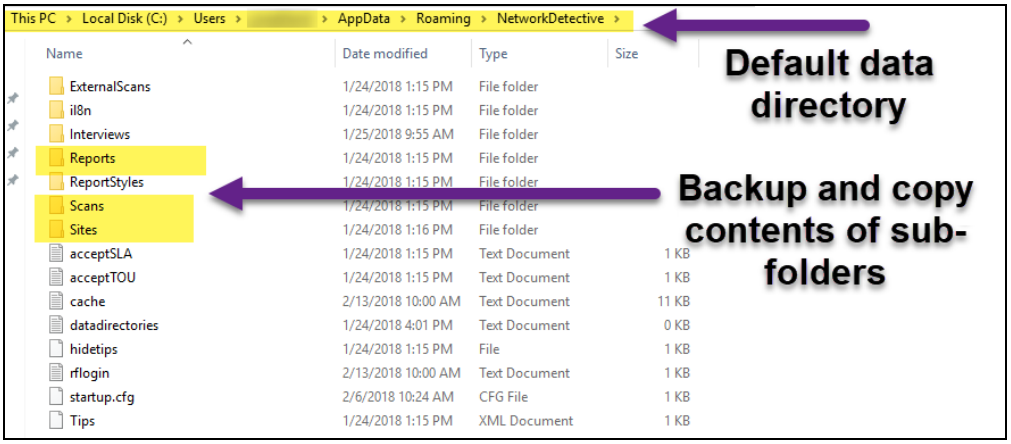
Compiling Network Detective Data

In order to share sites, scans and reports between all Network Detective users, use the **Change Data Directory** quick link from the home screen.

You can set this as a network share, Dropbox, Cloud Sync, One Drive or however you would like as long as all users have access to this directory.

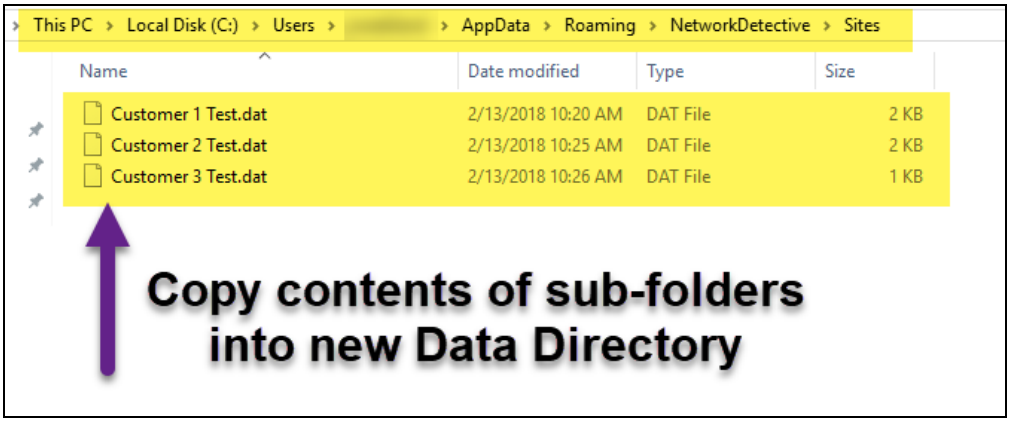


Changing the directory will automatically create a new Network Detective folder along with all of the corresponding subfolders. Any data already created locally will not migrate automatically. To retain this data, navigate to the **C:\Users\[User]\AppData\Roaming\NetworkDetective** folder (you may need to enable hidden file viewing) and copy the relevant contents of any subfolders you wish to retain.

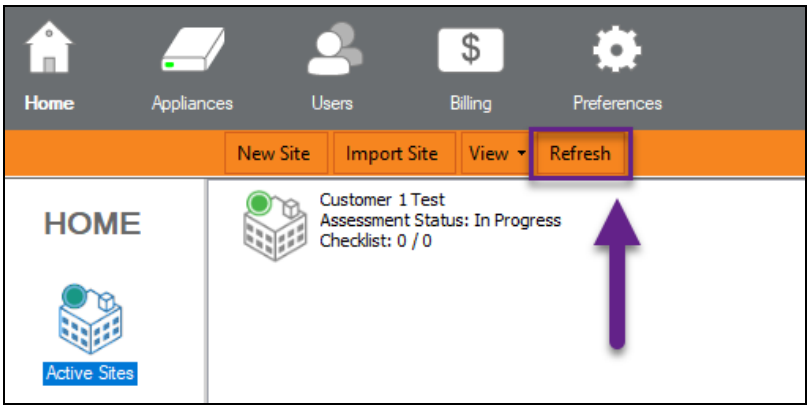


Most importantly, copy the contents of the **Reports**, **Scans**, and **Sites** subfolders over to corresponding subfolders of the new directory.

Important: We recommend that you backup any important data before transferring.



Once this has been completed, select the refresh button from the Homescreen of the Network Detective Application to view all of the previously created sites, which will contain all of their relevant data.



Integrate Network Detective with a PSA System

With Network Detective, you can export important information uncovered during your assessment into your preferred Professional Services Automation (PSA) system. This includes technical information on computer assets discovered on the network, contact information for network users, and issues for remediation. This topic covers how to integrate Network Detective with your chosen PSA System.

Step 1 — Gather Credentials and Set Up your PSA System

Before you begin, you will need:

- Valid Login Credentials for Network Detective
- A Network Detective "Site" for which you wish to export items or create tickets in your PSA
- Valid Login Credentials for your PSA system account (if you wish to integrate Network Detective with multiple PSA accounts, gather credentials for each PSA account)
- Other prerequisites specific to your chosen PSA system (refer to the table below)

PSA System	PSA Prerequisites
Autotask®	**Note:** To set up a connection between the Network Detective application and the Autotask system, you will need to create an API User in Autotask. See "Set Up Autotask Integration" on page 290. • Autotask API Username • Autotask API Password
REST ConnectWise™	• ConnectWise REST Public Key • ConnectWise REST Private Key • ConnectWise Company ID • ConnectWise PSA URL **Note:** You must configure ConnectWise correctly before you can integrate with Network Detective. See "Set Up ConnectWise REST Integration" on page 295 for detailed instructions.

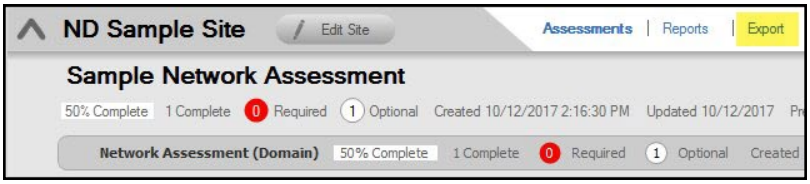
PSA System	PSA Prerequisites
	• ConnectWise Username • ConnectWise Password • ConnectWise Company ID • ConnectWise PSA URL **Note:** You must configure ConnectWise correctly before you can integrate with Network Detective. See "Set Up ConnectWise SOAP Integration" on page 304 for detailed instructions.
	• Tigerpaw Username • Tigerpaw Password • Tigerpaw API URL
	• Kaseya Username • Kaseya Password **Note:** The Kaseya User must be in the Kaseya Administrator Role. See for "Set Up Kaseya BMS Integration" on page 306 detailed instructions. • Kaseya Tenant (i.e. company name) • Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

Step 2 — Create a Connection Between Network Detective and Target PSA

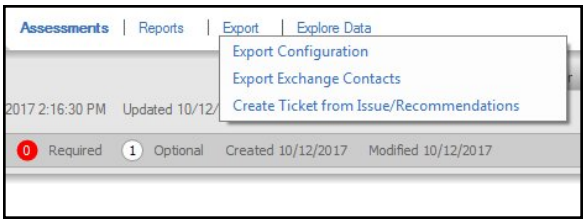
1. If you have not already done so, visit https://www.rapidfiretools.com/nd-downloads to **download and install Network Detective**.
2. **Start Network Detective** and log in with your credentials.
3. Open the **Site** for which you wish to create tickets in the target PSA.

> **Note:** You must have completed your assessment project and must have reports ready to generate in order to create tickets.

4. Within the Assessment window, click **Export**.

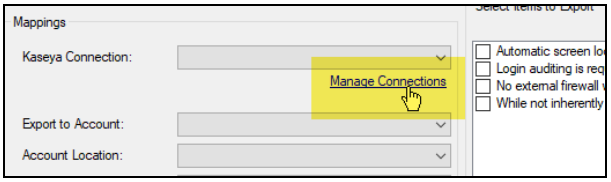


5. Choose an export option from the drop-down menu.

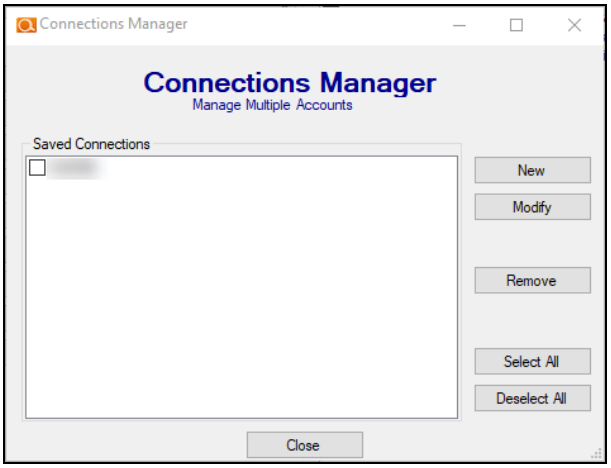


6. **Select your Target** Ticketing/PSA system from the list of supported options.

7. Click **Manage Connections**.

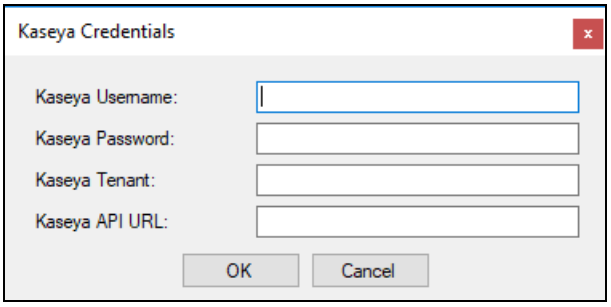


The Connections Manager window will be displayed.



8. Select the **New** button in the Connections Manager window to create a new PSA connection.

   The PSA Credentials window will be displayed



9. Enter the credentials for chosen PSA.

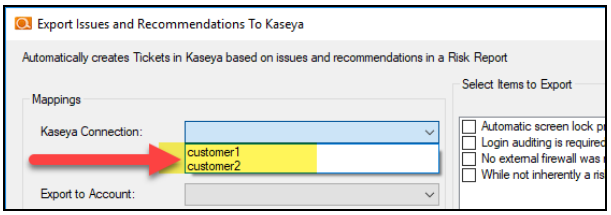
   Important: To generate login credentials for ConnectWise REST, see "Set Up ConnectWise REST Integration" on page 295. To generate login credentials for ConnectWise SOAP, see "Set Up ConnectWise SOAP Integration" on page 304.

10. Click **OK**.

    The new Connection will be listed in the Saved Connections list in the Connections Manager window.

    Tip: If you wish to export items to multiple, separate PSA accounts, repeat this process and add Connections for each account.

11. Click **Close** to dismiss the Connection Manager.
12. From the Export screen, verify the connection by selecting it from the drop-down menu.



> **Note:** If the connection is successful, some of the Mappings fields should automatically populate with values from the PSA system.

13. Proceed to export information to your PSA. Refer to the instructions below.

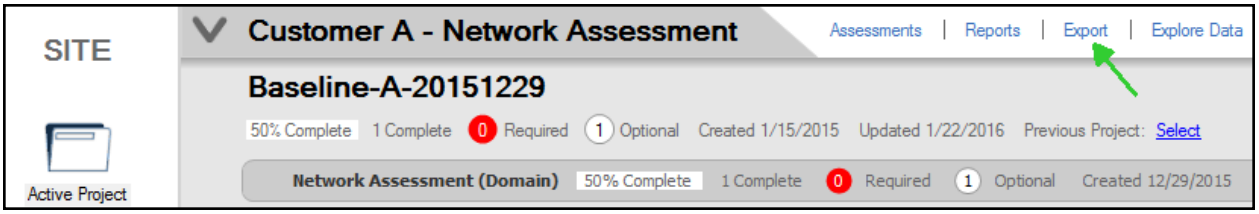
Once you have created the connection, you can then use the **Export** features:

- "Export Configuration Items from Network Detective to PSA" below
- "Export Exchange Contacts from Network Detective to PSA" on page 287
- "Create Tickets from Assessment Issues and Recommendations from Network Detective to PSA" on page 287

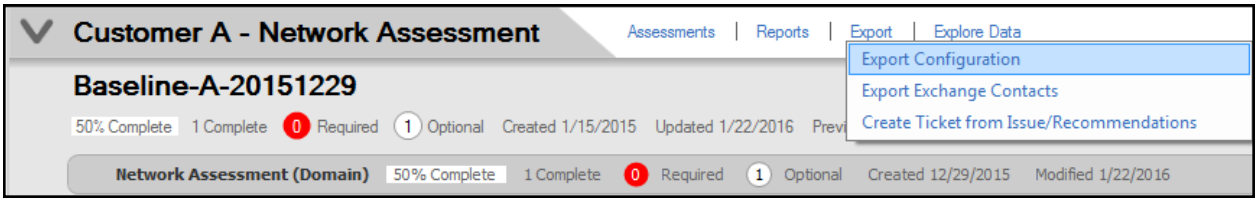
Export Configuration Items from Network Detective to PSA

You can use Network Detective to export data to configuration items within your preferred PSA/CRM or Ticketing Systems such as Autotask, ConnectWise, and Tigerpaw. To do this:

1. Open the **Site** and **Assessment Project** for which you wish to create tickets.
2. Within the Assessment window, click **Export**.

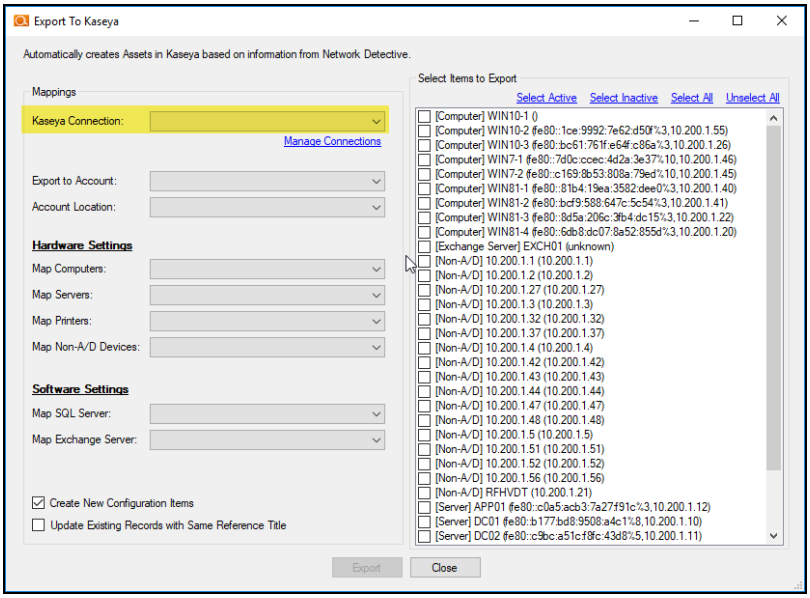


3. Click **Export Configuration**.



4. Select the **Target PSA** from the menu.

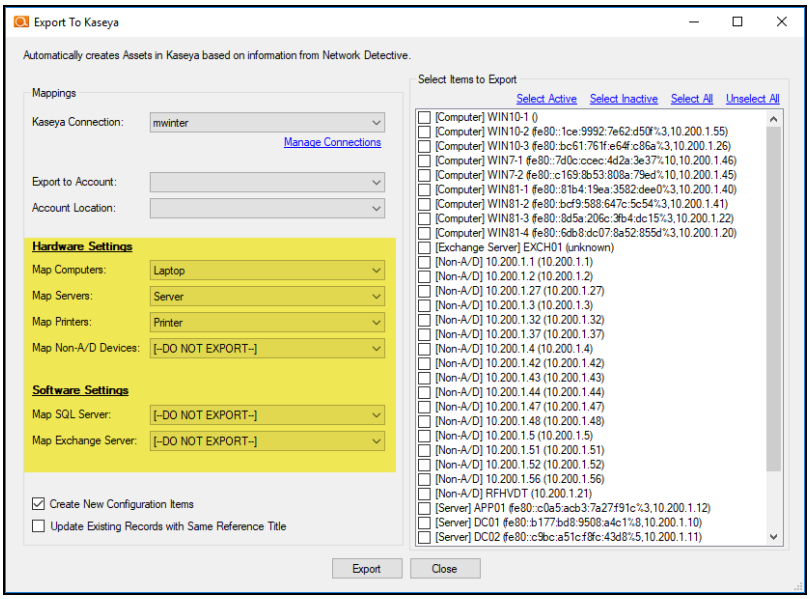
5. The **Export Issues/Recommendations** window will appear.
6. Select a **Connection** from the drop-down menu. The Connection determines the specific PSA account to which the tickets will be exported.



Important: If you have not yet created a connection, see "Integrate Network Detective with a PSA System" on page 275 and follow the instructions there. Then return to this help topic.

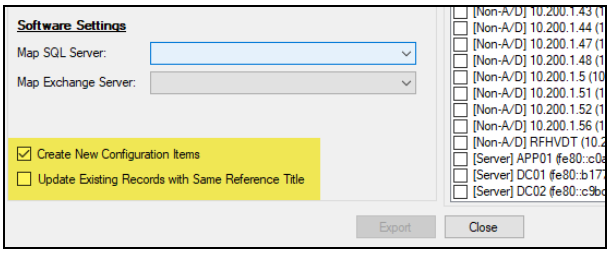
Note: When the Connection between Network Detective and the PSA is established, some of the fields in the Mapping menu will automatically populate. This may take up to 60 seconds.

7. Map the issues to service ticket fields in your PSA. These mappings allow you to configure how the items will be mapped within your PSA.



Important: You configure the values for the mapping fields in your PSA system. Ensure the values are correctly configured in your PSA before continuing.

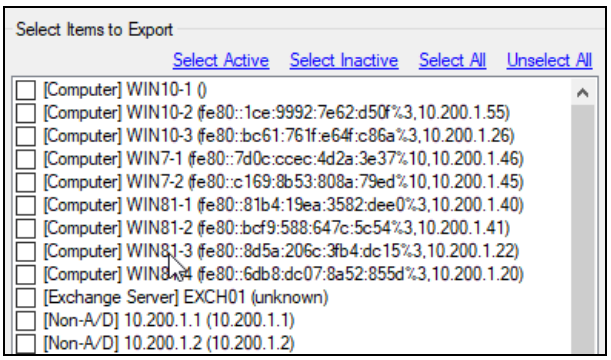
8. Choose whether to **Create New Configuration Items**. This will create new items in your PSA, even the items already exist.



9. Select **Update Existing Records with Same Reference Title** if you want to update existing configuration items with information from Network Detective.

> **Tip:** You can perform this operation multiple times with different "Selected Items" to map each group to different Product types. For example, if different sets of "Non-A/D devices need to get mapped to different elements (e.g. - some to Switches, other to Printers), select appropriate items, set the mapping and repeat with different settings as necessary.

10. From the list, **Select Items to Export**.



11. Click **Export**. Confirm that you wish to export the issues.

    After the export is complete, an Export Complete status window will be displayed indicating the number of items created in the PSA.

> **Note:** You can then log in to your PSA and confirm that your items have been created.

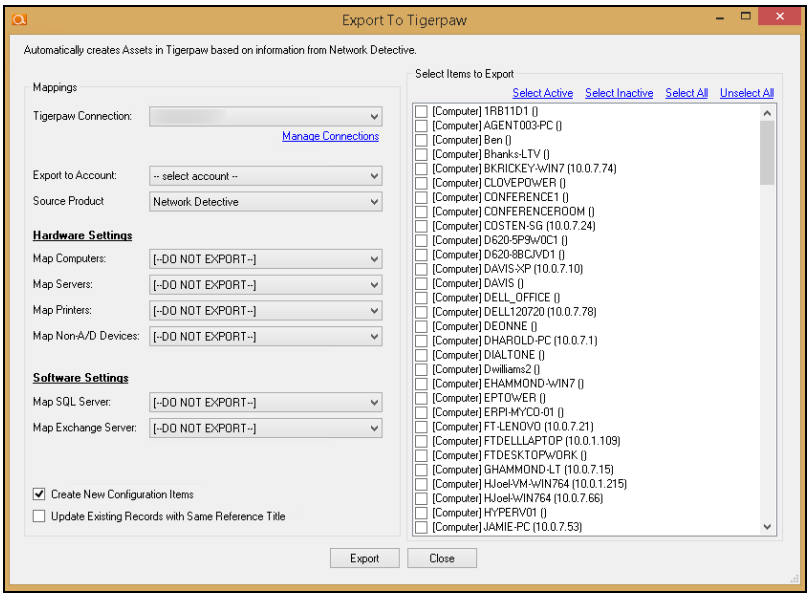
Export fields for Autotask

When exporting to Autotask, Network Detective will set the following fields in each Configuration item:

- Product (mapped as per step 4 above)
- Reference Title (from the machine name)
- Notes (information on the device, including O/S, CPU, RAM, IP, etc. – as available from scan)

Export fields for Tigerpaw

Once you have created and established a connection to Tigerpaw, Network Detective will populate the Export to Account field and Source Product drop down list.



Select the account from the Source Product list that you want to export your Configuration Fields to within Tigerpaw. Once the account is selected, elect the Hardware Settings and Software Settings that you want to export.

Then complete the Export by selecting the Export button.

At that point, “Assets” will be created within the Tigerpaw system for management under the Tigerpaw “Managed Assets” process.

Export fields for ConnectWise

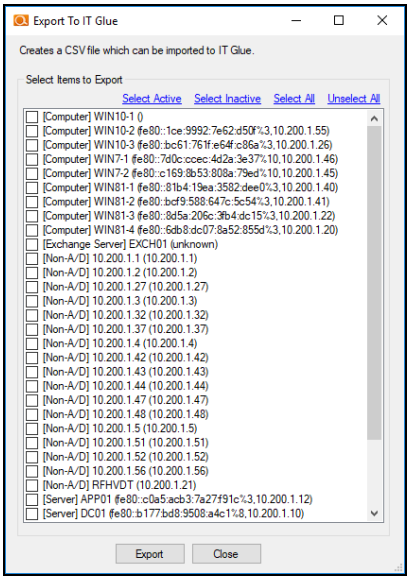
When exporting to ConnectWise, you can use any existing Configuration Types that you have setup. In this case, Network Detective will populate the standard fields, and the Notes field will be set with the information for that system (CPU, Memory, etc.). If there was information in the Notes field, it will be overwritten by Network Detective.

There is also the option to use a Configuration Type specific to Network Detective for each of Computers, Servers, Printers, etc. These will be in the appropriate drop-down with "(ND)" as the suffix - for example "Computer (ND)" and "Server (ND)." These will automatically be created by Network Detective. If you use this Configuration Type, Network Detective will create and set custom Configuration Questions relevant to the Configuration type. For example, for Computers (ND), the Configuration Questions include: Computer Name, Operating System, CPU, etc. The full list of information will also be entered into the Configuration Question: Misc.

Export Configuration Items to IT Glue

To Export Configuration Items to IT Glue:

1. **Select the items to export** from the list.



2. Click **Export**.
3. Enter a name for the CSV file. Click **Open**.
4. Network Detective will then create a CSV file. Import the file into IT Glue.

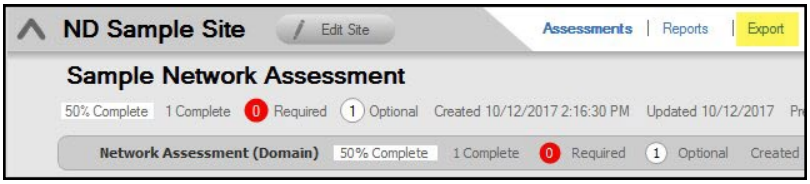
Export Exchange Contacts from Network Detective to PSA

Help topic coming soon!

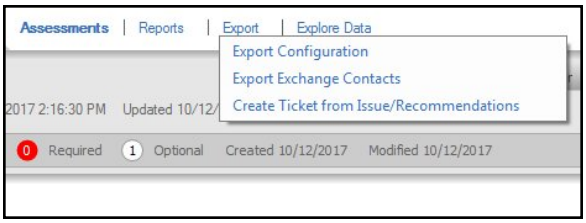
Create Tickets from Assessment Issues and Recommendations from Network Detective to PSA

Network Detective allows you to create tickets from Issues and Recommendations identified during the assessment. To create and export tickets to your preferred PSA system:

1. Open the **Site** and **Assessment Project** for which you wish to create tickets.
2. Within the Assessment window, click **Export**.

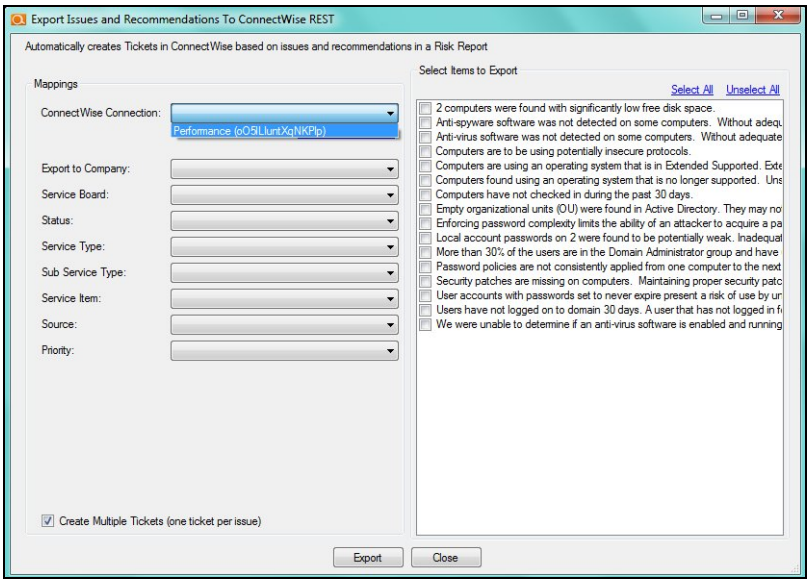


3. Click **Create Ticket from Issues/Recommendations**.



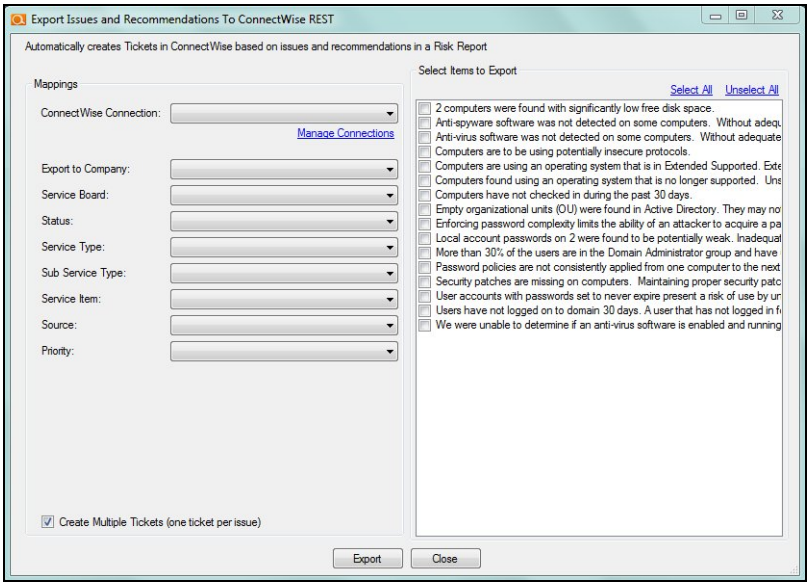
4. Select your preferred **Target** PSA from the menu.

5. The **Export Issues/Recommendations** window will appear.
6. Select a **Connection** from the drop-down menu. The Connection determines the specific PSA account to which the tickets will be exported.



Important: If you have not yet created a connection, see "Integrate Network Detective with a PSA System" on page 275 and follow the instructions there. Then return to this help topic.

> **Note:** When the Connection between Network Detective and the PSA is established, some of the fields in the Mapping menu will automatically populate. This may take up to 60 seconds.

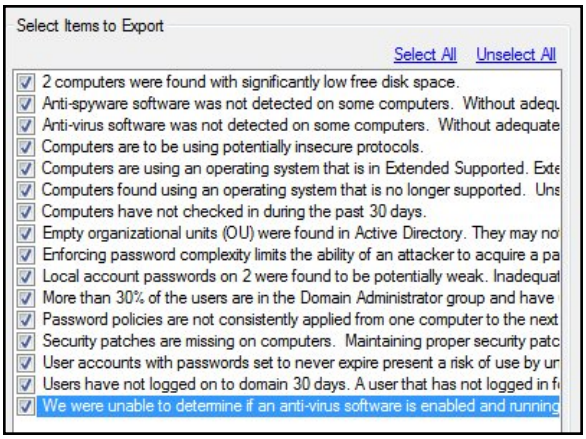


7. Map the issues to service ticket fields in your PSA. These mappings allow you to configure how the issues in Network Detective are created as tickets in your PSA.

> **Important:** You configure the values for the mapping fields in your PSA system. Ensure the values are correctly configured in your PSA before continuing.

> **Note:** In the **Export Issues and Recommendations** window select the **Create Multiple Tickets** option to create a ticket for each Issue and Recommendation contained within the Items to Export list. Unselect this option to create a single ticket with all of the issues.

8. From the list, **Select Items to Export** to the PSA.



9. Click **Export**. Confirm that you wish to export the issues.

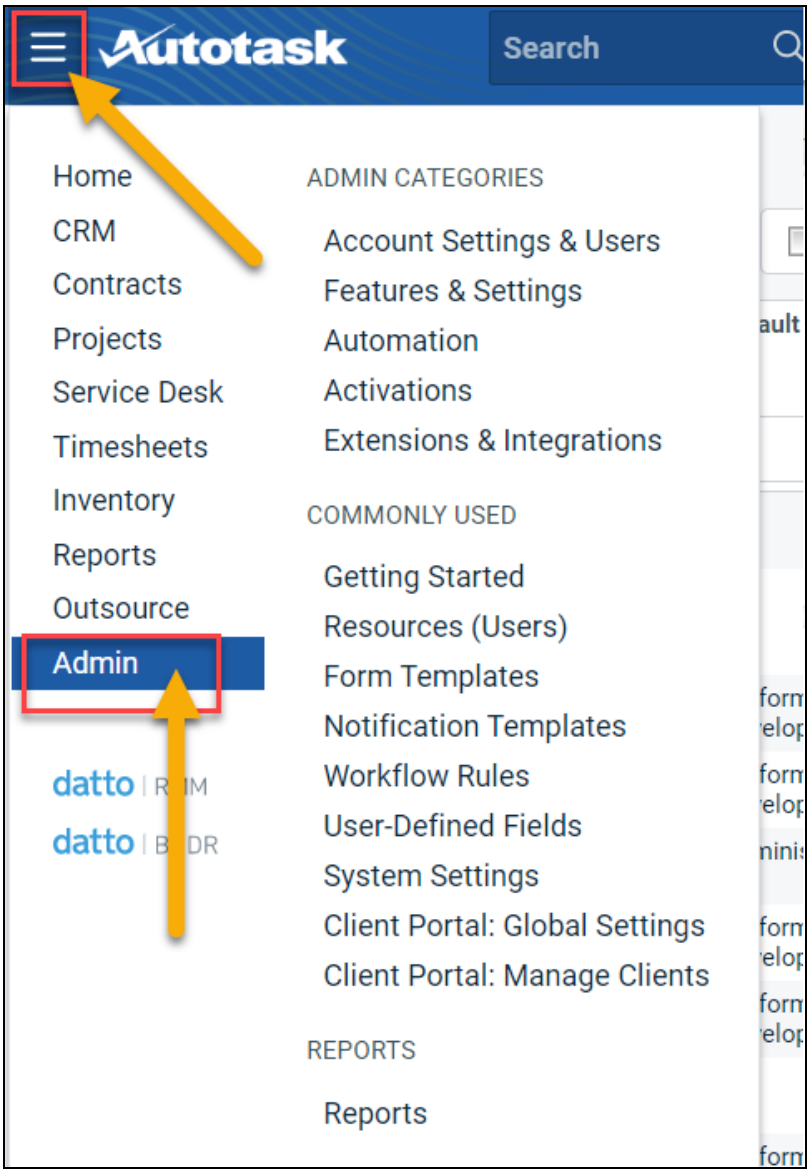
   After the export is complete, an Export Complete status window will be displayed indicating the number of Issues tickets created in the PSA.

> **Note:** You can then log in to your PSA and confirm that your tickets have been created.

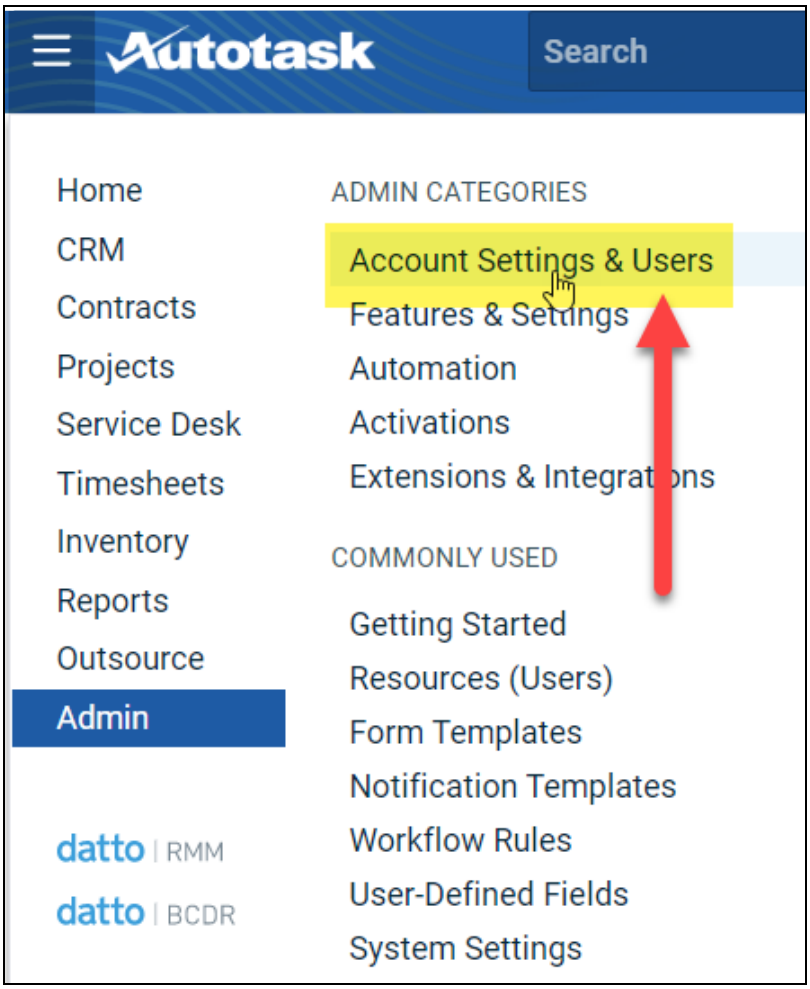
Set Up Autotask Integration

To set up a connection with the Autotask system, you will need to **create an API User in Autotask**. To do this:

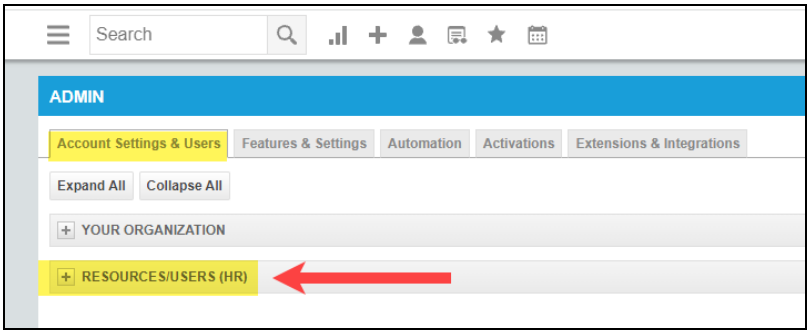
1. Log in to Autotask with your admin user credentials.
2. Click on the **Autotask home** button on the left, then click **Admin**.



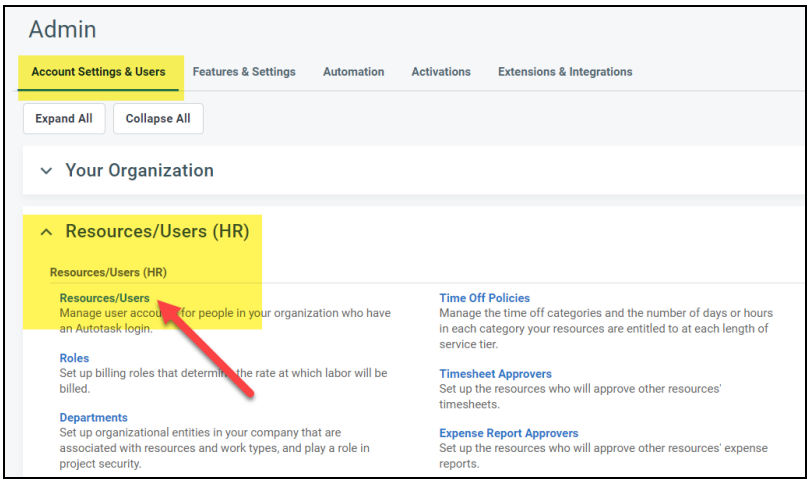
3. From the **Admin** menu, click **Account Settings & Users**.



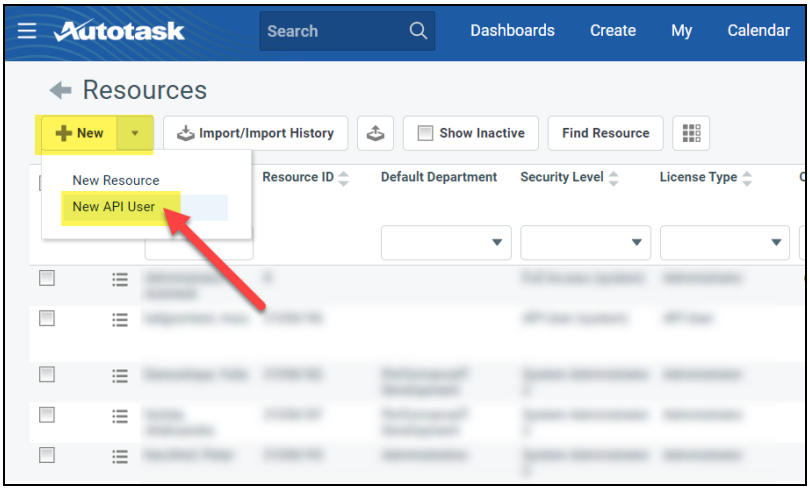
4. Next, click **Resources/Users (HR)** to expand the menu.



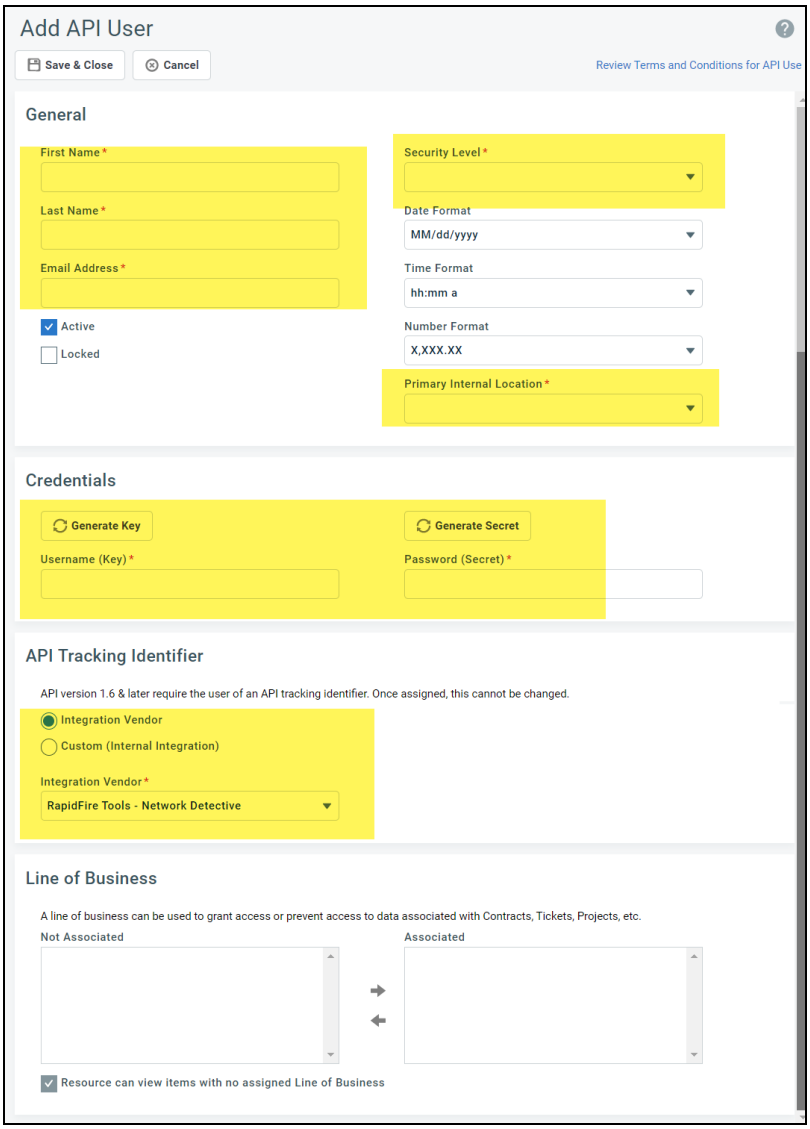
5. Then click **Resources/Users**.



6. Hover your mouse over the drop-down menu to the right of the **New** button, then select **New API User**.



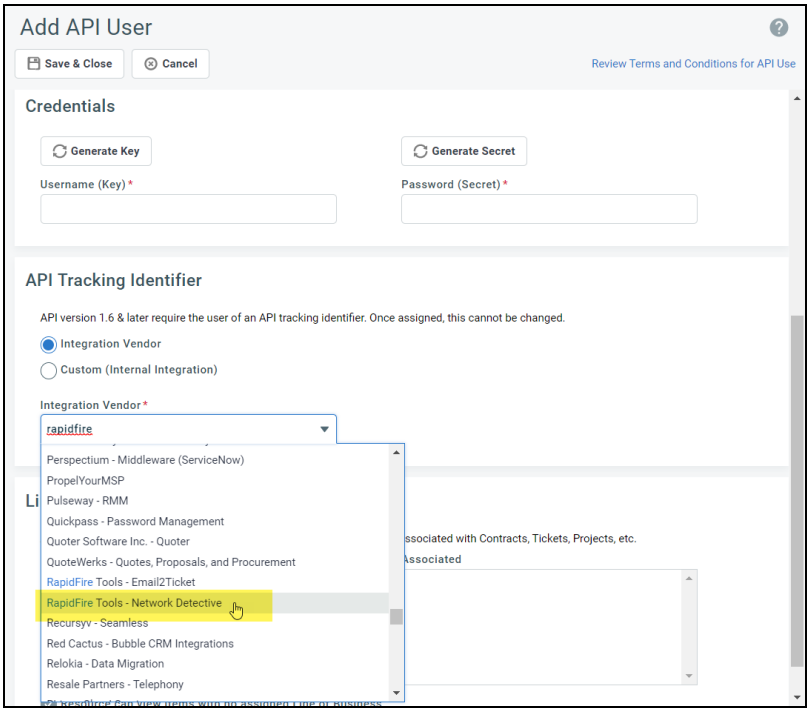
7. Enter information about the API user. Autotask will prompt you to enter the mandatory fields.



- Enter a **first and last name** for the API user.
- Enter an **email address** for the API user.
- From **Security Level**, select **API User (system)**.
- Select a **Primary Internal Location** for the API user.
- Enter/generate a **username** for the API user, then enter/generate a **password**.

> **Note:** Take note of these credentials as you will enter these in Network Detective to enable the API integration.

- Under **API Tracking Identifier**, select **Integration Vendor**. Then select **RapidFire Tools — Network Detective**.



8. When you are finished configuring the new API user, click **Save & Close**. The new user will appear in the list.

Set Up ConnectWise REST Integration

To set up a connection to ConnectWise Ticketing system using the REST API you will be required to:

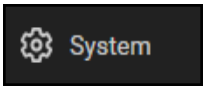
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

To enable the integration, you will need to use the ConnectWise Manage Internet Client application. Download and install the app from http://university.connectwise.com/install/. Then log in using your credentials.

If you are using the ConnectWise Manage web app, you can continue to use the web app after you have completed the steps in this guide and enabled the integration.

Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with

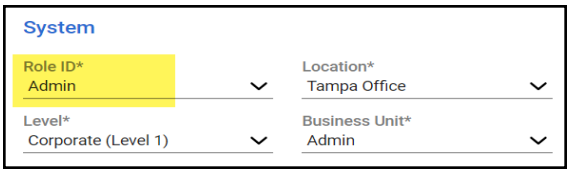
1. From the ConnectWise dashboard, click **System** from the side menu.



2. Next, click **Members**.
3. Click on **API Members Tab**. The API Members screen will appear.

   Note that the API Members Tab may not show by default and may need to be added. You can add this tab from the Tab Configuration menu on the Members page ⚙.

4. Click on the + button to create a new API Member. Fill in all required information.
5. Confirm that the API Member has been assigned Admin rights by checking the member's **Role ID** under **System**.



> **Important:** By default, the API Member must have **Admin** rights for the integration to function correctly. However, we provide a "least privilege" custom solution for the API Member Role ID below. See "Create Minimum Permissions Security Role for API Member" below.

Create Minimum Permissions Security Role for API Member

If you do not wish to assign the API member full Admin rights, create this custom security role and assign it to the API member:

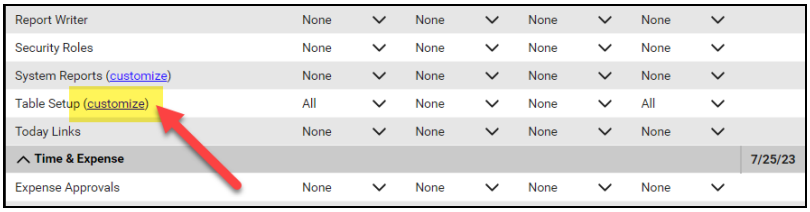
1. Go to **System** > **Security Roles**.
2. Click the + button to create a new security role.

3. Set the permissions for the Role as detailed in the table below and click **Save**.
4. Assign this custom Security Role to the API Member instead of full Admin.

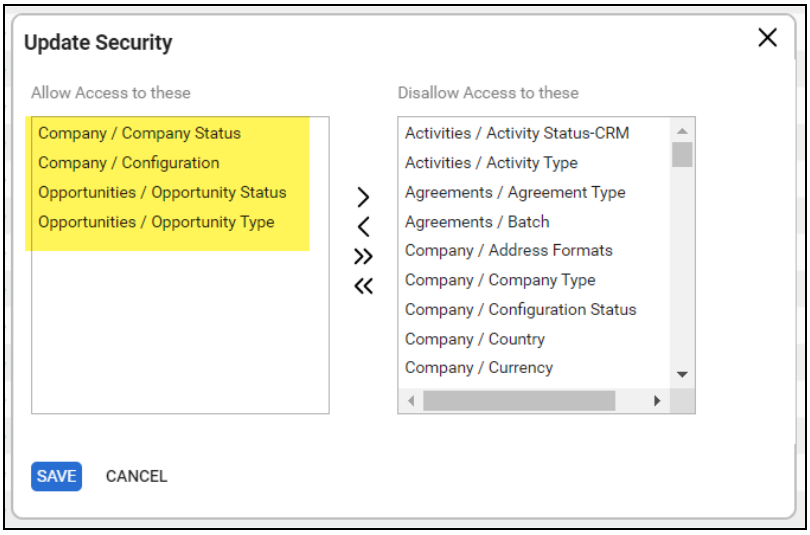
Module		Add Level	Edit Level	Delete Level	Inquire Level
Companies					
	Company Maintenance				All
	Configurations	All	All		All
	Contacts	All	All		All
Service Desk					
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup* *Customized Table Setup: Allow Company / Company Status, Company / Configuration, Opportunities / Opportunity Status, Opportunities / Opportunity Type (See "Table Setup Configuration" below below for an extended explanation)	All			All

Table Setup Configuration

From Table Setup, click **customize**.



Allow access to the items listed in the table above under **Table Setup**. You can also refer to the image below.

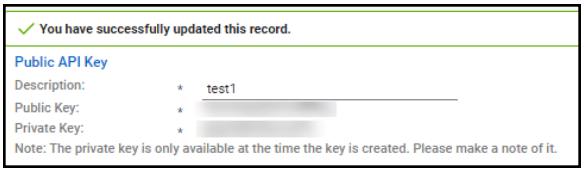


Step 3 — Create an API Key in the ConnectWise Ticketing System

1. Select the API Member that you created previously.
2. From the API Member details screen, click **API Keys**.

3. Click the + button.
4. Enter a **Description** for the API Key.
5. Click **Save**.
6. The newly generated API Key will appear.
7. Write down or take a screen shot of the Member's Public and Private API Key strings. This information will be required to set up the integration with ConnectWise.

Important: Note that the Private Key is only available at the time the key is created. Be sure to copy the keys for your records.



Step 4 — Configure Service Tables in ConnectWise

In order to export issues as tickets in ConnectWise, you will need to configure several **Service Tables** in ConnectWise. These tables ensure that the issues are “mapped” correctly to the tickets created within ConnectWise. You must configure the Service Tables correctly in order to establish the connection with ConnectWise.

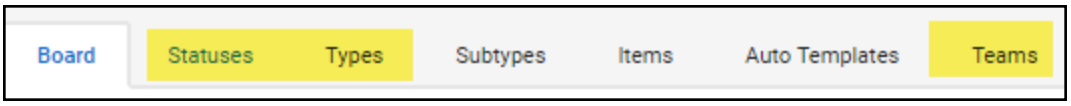
You can configure the Service Tables in ConnectWise from **System > Setup Tables > Category > Service**. Configure the Service Tables as detailed below:

1. **Service Board**

   You must have a Service Board created within ConnectWise. In addition, within the Service Board, you must create values for the following fields. You can create values for these fields from the Service Board page:

   a. **Statuses**
   b. **Types**
   c. **Teams**

   You must create at least one value for each of these fields.



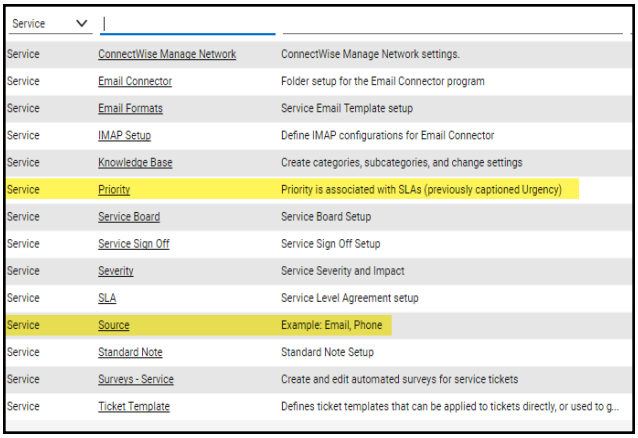
   In addition, you must define values for two additional Service Tables:

2. **Source**

   You must include at least one Source.

3. **Priority**

   You must include at least one Priority level.



Service		
Service	ConnectWise Manage Network	ConnectWise Manage Network settings.
Service	Email Connector	Folder setup for the Email Connector program
Service	Email Formats	Service Email Template setup
Service	IMAP Setup	Define IMAP configurations for Email Connector
Service	Knowledge Base	Create categories, subcategories, and change settings
Service	Priority	Priority is associated with SLAs (previously captioned Urgency)
Service	Service Board	Service Board Setup
Service	Service Sign Off	Service Sign Off Setup
Service	Severity	Service Severity and Impact
Service	SLA	Service Level Agreement setup
Service	Source	Example: Email, Phone
Service	Standard Note	Standard Note Setup
Service	Surveys - Service	Create and edit automated surveys for service tickets
Service	Ticket Template	Defines ticket templates that can be applied to tickets directly, or used to g...

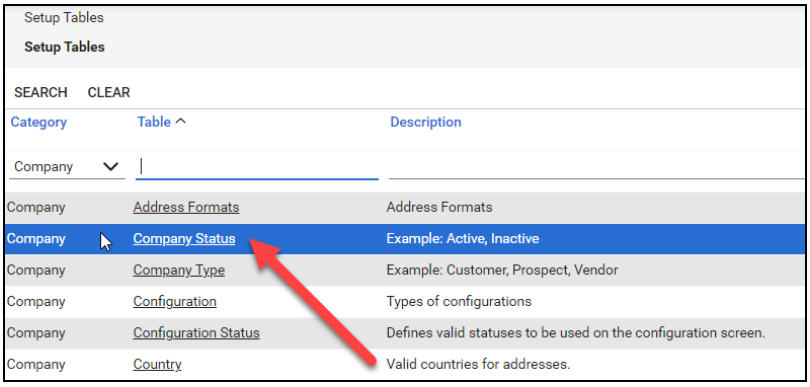
   If your existing Service Tables already contain values for the fields listed above, you do not need to create new values.

Step 5 — Remove "Disallow Saving" Flag from Company

The final step is to ensure your companies are able to save data such as tickets. By default, your company may have the "**Disallow Saving**" option flag enabled; this will prevent you from exporting tickets to the company.

Here's how to remove the "Disallow Saving" flag:

1. Navigate to **Setup Tables** > **Category** > **Company** > **Company Status**.



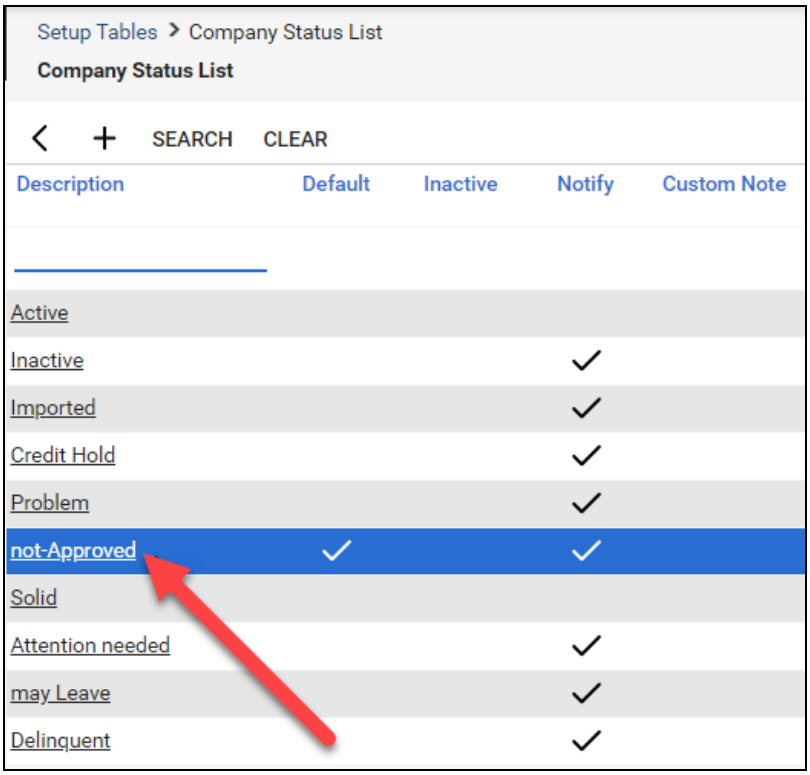
Setup Tables

Setup Tables

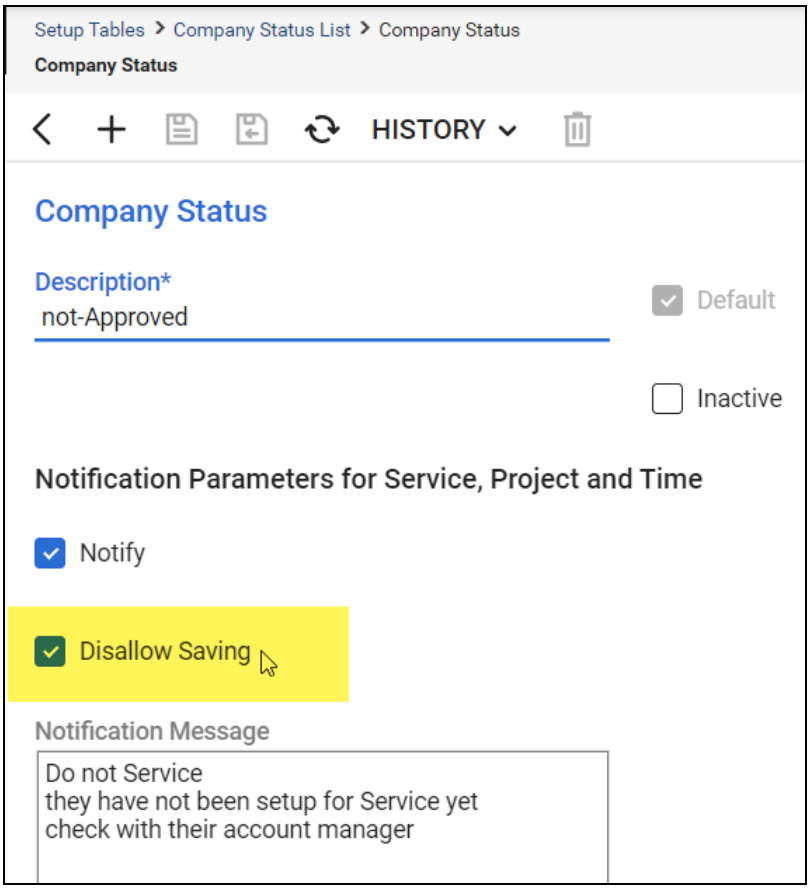
SEARCH CLEAR

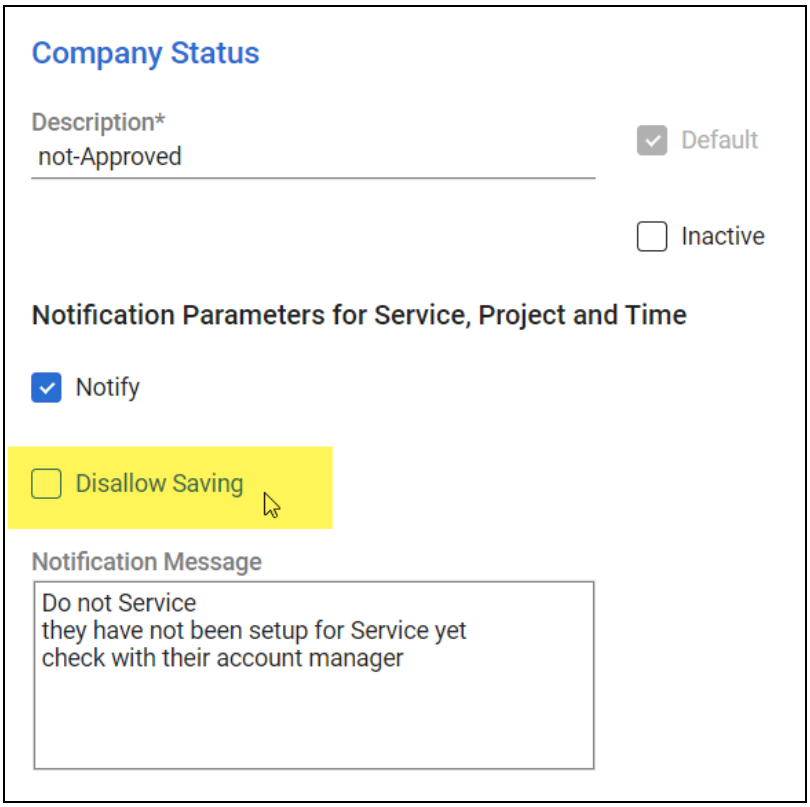
Category	Table	Description
Company	Address Formats	Address Formats
Company	Company Status	Example: Active, Inactive
Company	Company Type	Example: Customer, Prospect, Vendor
Company	Configuration	Types of configurations
Company	Configuration Status	Defines valid statuses to be used on the configuration screen.
Company	Country	Valid countries for addresses.

2. From Company Status, open the **not Approved** field.

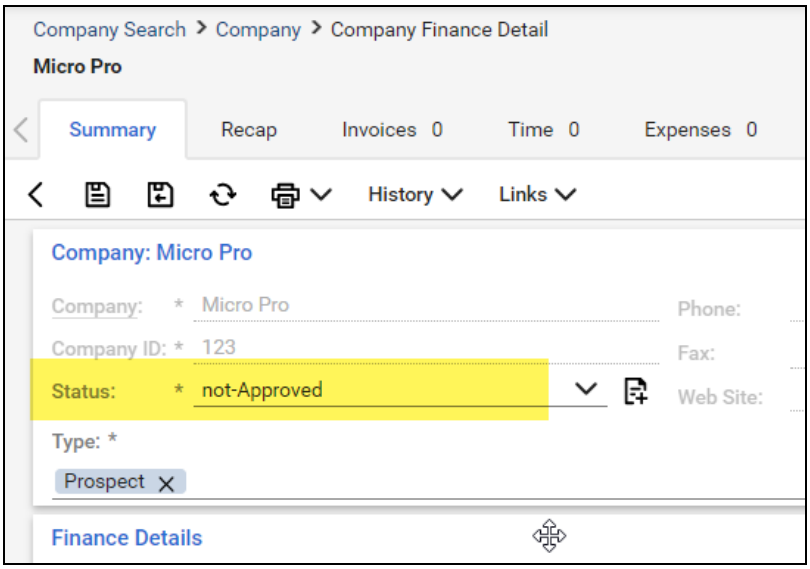


3. Uncheck the **Disallow Saving** flag.





4. This will allow you to export tickets to companies with the **not Approved** status. Alternatively, you can set the company itself to a different status that allows saving before attempting the ticket export.



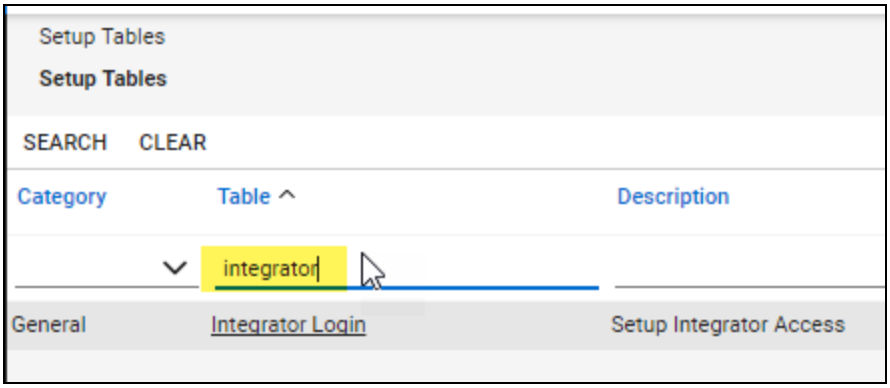
Set Up ConnectWise SOAP Integration

This topic covers how to integrate Network Detective with ConnectWise via the ConnectWise SOAP API.

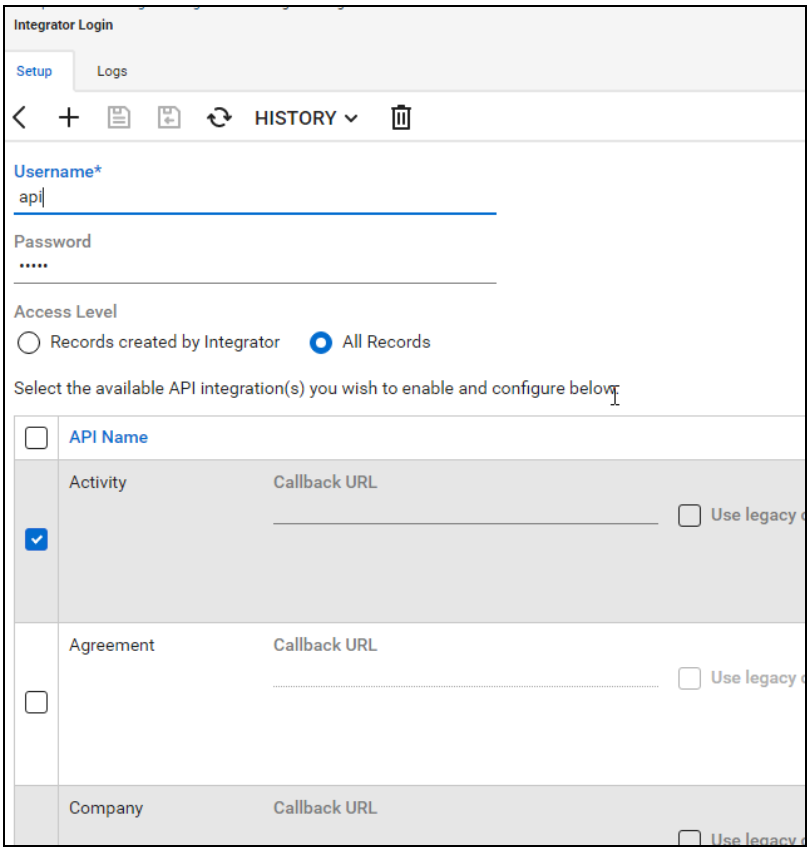
Important: The ConnectWise SOAP API is in the process of being deprecated by ConnectWise. We recommend that you use the ConnectWise REST API instead.

To set up the ConnectWise SOAP integration:

1. Navigate to **System**-> **Setup Tables**.
2. Type "**Integrator**" into the Table lookup and hit Enter.
3. Click the **Integrator Login** link.



4. Click the “**New**” Icon to bring up the New Integrator login screen as shown on the right.
5. Enter and record **Username** and **Password** values which you will need later on when creating a connection in Network Detective.
6. Set the Access Level to “**All Records**.”
7. Using the ConnectWise Enable Available APIs function, **enable the following APIs**:
    - ServiceTicketApi
    - TimeEntryApi
    - ContactApi
    - CompanyApi
    - ActivityApi
    - OpportunityApi
    - MemberApi
    - ReportingApi
    - SystemApi
    - ConfigurationApi



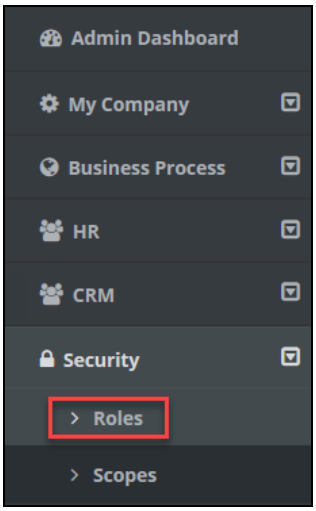
8. Click the **Save** icon to save this Integrator Login.

> **Note:** If you already have an Integrator Login configured, you may use it as long as the Company and Configuration APIs are enabled.)

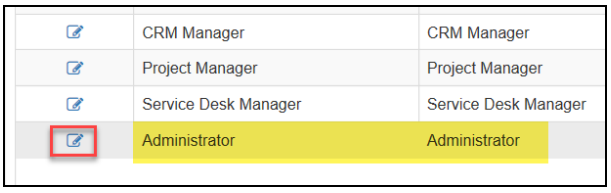
Set Up Kaseya BMS Integration

To export items to Kaseya BMS, you will need Administrator credentials in Kaseya BMS. To assign a Kaseya user to the Administrator role, follow these steps:

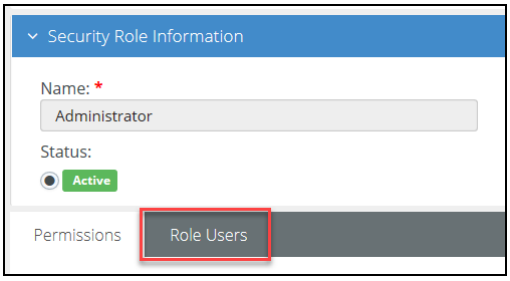
1. Log in to Kaseya BMS.
2. Go to **Security** > **Roles**.



3. Click **Open/Edit** on the Administrator Role.



4. Click the **Role Users** tab.

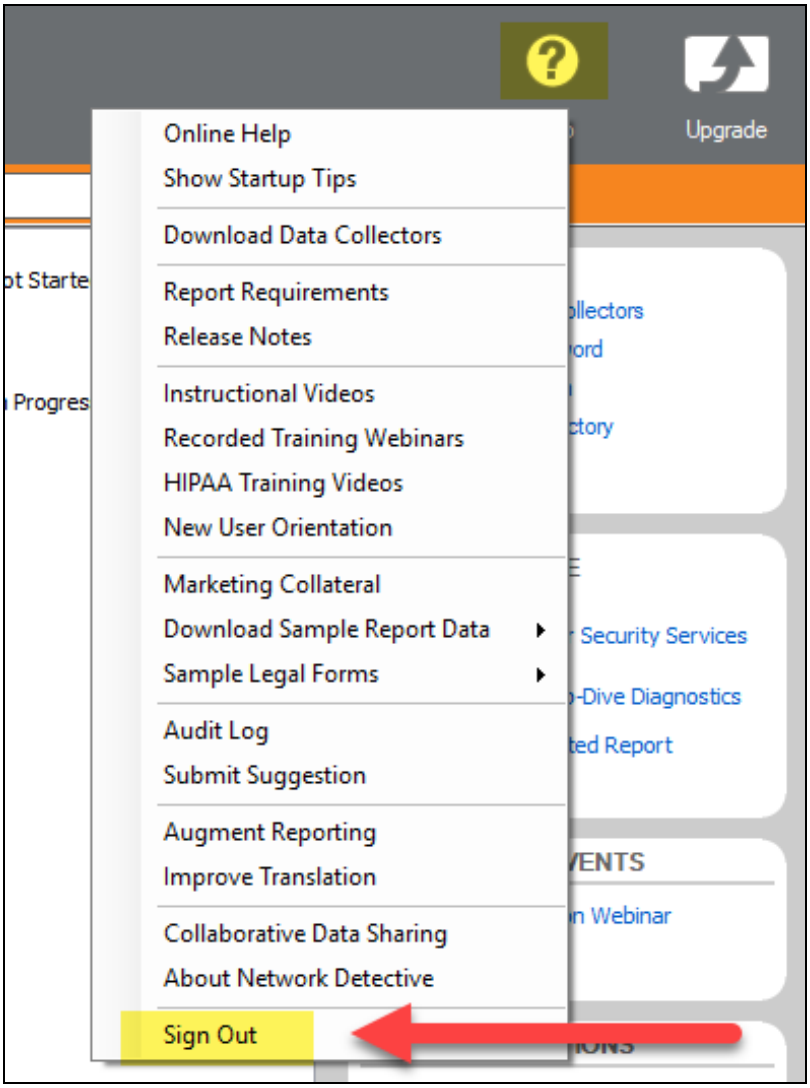


5. Click **Add**.
6. Search for the user to who will become a Kaseya Administrator and **Select** that user.
7. Click **OK**. This user can now invoke the Kaseya BMS API.

Sign Out of Network Detective

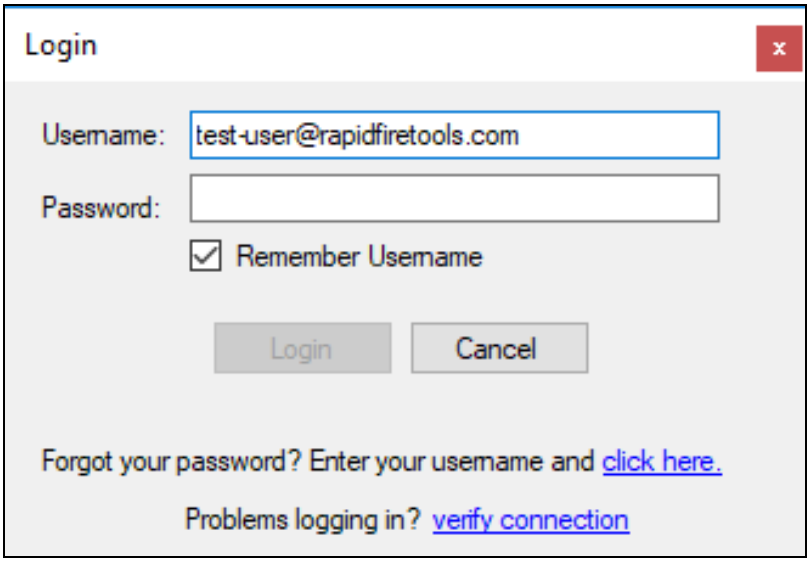
To sign out of Network Detective:

1. Click the **Help** button in the top right corner.



2. Click **Sign Out** at the bottom of the menu.

You will return to the Login screen where you can sign in using a different account.



Network Detective Linux Computer Data Collector

The Linux Computer Data Collector is a Linux application (works on most modern Linux versions) that is run on individual computers (workstations or servers) to collect information for that system. Use this to collect computer information from Linux systems to be merged into the network data collection.

This data collector is a version of computer data collector only and cannot perform Security Assessments or Network Data Collection.

Download the Linux Computer Data Collector

Download the Linux Computer Data Collector here:

https://download.rapidfiretools.com/download/NetworkDetectiveLinuxCollector.tar.gz

Run the Linux Computer Data Collector

This Linux Computer Data Collector download is a tar gzip file and does not require installation. Unzip it, then launch the application using the command below:

tar zxf NetworkDetectiveLinuxCollector.tar.gz | ./NetworkDetectiveLinuxCollector

Scan Output and Import into Assessment

Scan output is a ".cdf" file with the filename -.cdf. Copy this file for merging with the ZIP/NDF file when importing into the Network Detective application.

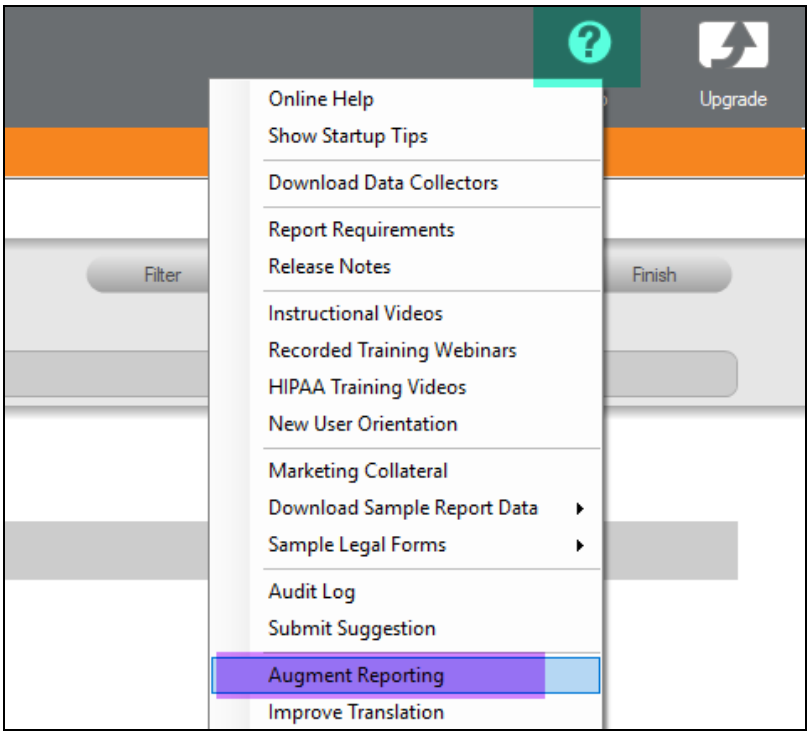
Augment Reporting to Eliminate False Positives

Occasionally, your customer may have a service installed that was not detected by Network Detective. With services such as antivirus and antispyware, new products are constantly being introduced to the market. Also, your customer may have a very old or very new release of an existing product. Since Network Detective is a very general-use product, reports may not always reflect a complete picture of your customer's unique circumstances.

The Augment Reports feature allows you to customize Network Detective's data analysis to better suit each of your customers. If a service is not listed in our database, you may add it through the Network Detective application. Then, re-generate the reports and the service will be properly included and displayed.

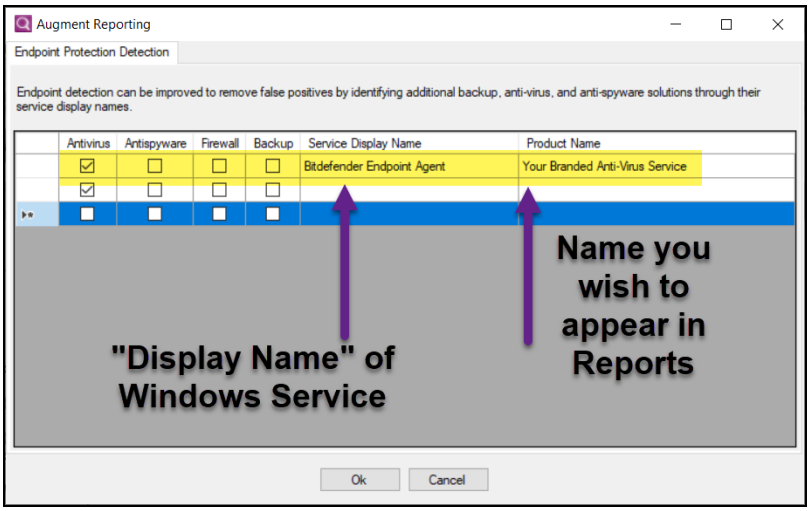
To augment your reports:

1. In Network Detective, go to **Help** > **Augment Reporting**.



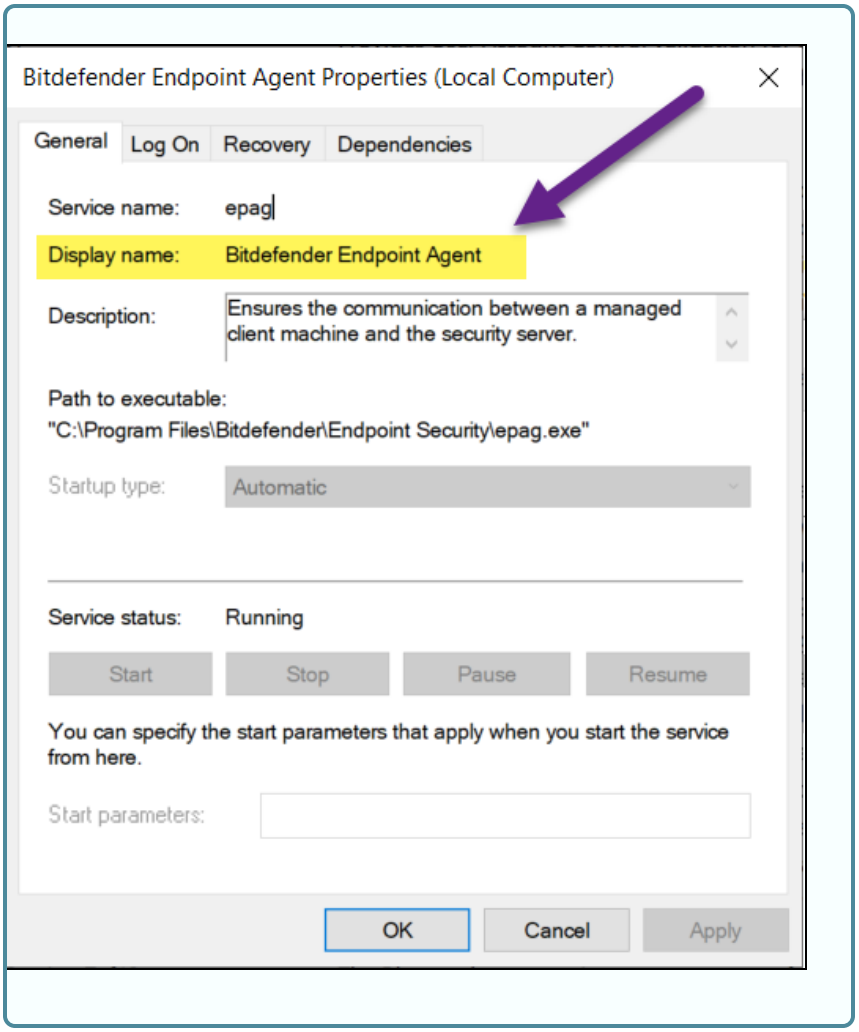
   The **Endpoint Protection Detection** screen will appear.

2. For each application you wish to add to your reports, select the type of application: *Antivirus*, *Antispyware, Firewall*, and/or *Backup*.



3. Then enter the *Display Name* for the Windows Service.

> **Note:** You can find the *Display Name* by opening the Windows Services app from your desktop. **Right click** on the service and click **Properties**. See "Use the Excel Export Spreadsheet to Find Display Names" on the facing page for an easy way to find display names for all Windows services.



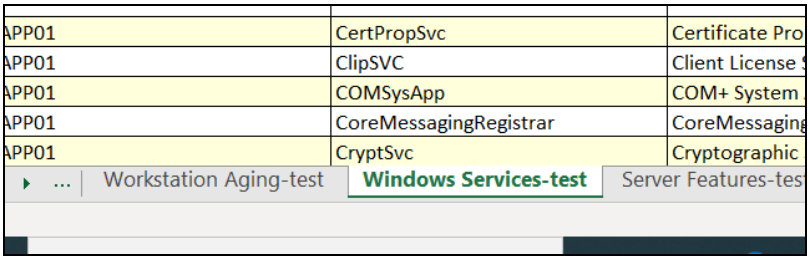
4. Next enter the **Product Name** for use with reporting. You can choose any name you wish for the Product Name for your Reports.
5. Repeat these steps for each app you wish to add to your reports.
6. Click **OK**.

   When 1) you next collect data on the target endpoints and 2) generate reports, your new reports will feature information on the apps you included.

Use the Excel Export Spreadsheet to Find Display Names

You can use the **Excel Export** from the Network Assessment Module to find Display Names for Windows Services. This might be helpful if you want to enter several apps into the Augment Reporting tool.

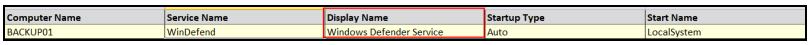
1. Generate the Excel Export Report from a NAM Assessment.
2. Open the report and navigate in Excel to the Windows Services worksheet.



APP01	CertPropSvc	Certificate Pro
APP01	ClipSVC	Client License S
APP01	COMSysApp	COM+ System
APP01	CoreMessagingRegistrar	CoreMessaging
APP01	CryptSvc	Cryptographic

... Workstation Aging-test | **Windows Services-test** | Server Features-tes

3. View the service entry for the *Antivirus*, *Antispyware,Firewall*, and/or *Backup* software installed on the computer and include this in the Augment Reporting tool.



Computer Name	Service Name	Display Name	Startup Type	Start Name
BACKUP01	WinDefend	Windows Defender Service	Auto	LocalSystem