



USER GUIDE

Network Detective Pro

Contents

Introduction to Network Detective Pro	11
<u>Network Detective Pro Components</u>	11
Download and Install the Network Detective Pro Application	13
Set Up Network Detective Pro Reports	14
<u>Setting Report Branding and Customization Preferences</u>	14
Setting Reports Preferences at the Global or Site Level	14
Access and Set Reports Defaults Preferences at the Global Level	14
Access and Set Reports Defaults Preferences at the Site Level	15
Network Detective “Site”	15
Setting Reports Preferences	15
<u>Setting Reports Preferences</u>	16
<u>Set Reports Text Preferences</u>	16
<u>Set Reports Logo Preferences</u>	17
Adding the Cover Page Logo Image	17
Adding the Header Logo Image	18
<u>Set Reports Cover Page Styles and Themes Preferences</u>	19
Setting the Reports Cover Page Style	20
Setting the Module Color Scheme	20
Setting Document Style	21
Set Infographic Report Style	22
Assigning Custom Defined Color Schemes to Each Assessment Module	23
<u>Set Reports Cover Images Preferences</u>	24
<u>Configure Report Date Format in Network Detective Pro</u>	26
<u>Assigning the Global Reports Preferences to a Site</u>	27
Performing a Network Assessment	29
<u>Network Assessment Overview</u>	29
What You Will Need	29

Network Prerequisites for Network Detective Pro Scans	30
<u>Step 1 — Download and Install the Network Detective Pro app</u>	31
<u>Step 2 — Create a New Site</u>	31
<u>Step 3 — Start a Network Assessment</u>	32
<u>Step 4 — Perform Network Scan Data Collection</u>	33
Scanning an Active Directory Domain-based Network	34
Scanning a Workgroup Network	43
<u>Step 5 — Use the Push Deploy Tool to Collect Remaining Data</u>	51
<u>Step 6 — Import Scans into Network Detective Pro App</u>	56
<u>Step 7 — Run Dark Web Scan (Optional)</u>	58
<u>Step 8 — Generate Network Assessment Reports</u>	60
<u>Network Assessment Reports</u>	60
Standard Reports	60
Infographics	65
Change Reports	66
Performing a Security Assessment	67
<u>Security Assessment Overview</u>	67
What You Will Need	67
Network Prerequisites for Network Detective Pro Scans	69
<u>Step 1 — Download and Install the Network Detective Pro Application</u>	70
<u>Step 2 — Create a New Site</u>	70
<u>Step 3 — Start a Security Assessment</u>	71
<u>Step 4 — Initiate External Vulnerability Scan</u>	72
<u>Step 5 — Perform Security Scan Data Collection</u>	75
Scanning a Workgroup Network	83
<u>Step 6 — Use the Push Deploy Tool to Collect Remaining Data</u>	89
<u>Step 7 — Import Scans into Network Detective Pro App</u>	94
<u>Step 8 — Generate Security Assessment Reports</u>	96
<u>Security Assessment Reports</u>	96

Standard Reports	96
Infographics	100
Change Reports	101
Performing a Microsoft Cloud Assessment	103
<u>Microsoft Cloud Assessment Overview</u>	103
What Does the Microsoft Cloud Assessment Cover?	103
What Does the Microsoft Cloud Assessment Do?	103
What You Will Need	105
<u>Step 1 — Download and Install the Network Detective Pro Application</u>	107
<u>Step 2 — Create a New Site</u>	107
<u>Step 3 — Start a Microsoft Cloud Assessment Project</u>	107
Use the Microsoft Cloud Assessment Checklist	108
<u>Step 4 — Run the Cloud Data Collector</u>	109
Perform Scan Using Enterprise App	109
Perform Scan Using OAUTH Credentials	110
Scan in Progress	112
<u>Step 5 — (Optional) Document Compensating Controls</u>	114
<u>Step 6 — Generate Reports</u>	115
<u>Prerequisites to Perform Cloud Scan using Enterprise App</u>	118
Step 1 — Create Enterprise App in Azure Tenant to be Assessed	118
Step 2 — Grant API Permissions to Enterprise App	120
Step 3 — Create Secret Key for Enterprise App	122
Step 4 — Add App as Reader to Root Management Group	123
Step 5 — Gather Credentials and Perform Scan	129
<u>Microsoft Cloud Assessment Reports</u>	130
Performing an AWS Assessment	134
<u>AWS Assessment Overview</u>	134
What You Will Need	135
<u>Step 1 — Download and Install the Network Detective Pro app</u>	136
<u>Step 2 — Create a New Site</u>	136

<u>Step 3 — Start an AWS Assessment</u>	137
<u>Step 4 — Gather AWS Access Key and Secret Key</u>	138
4(A) — Create User and Assign API permissions	138
4(B) — Generate Access Key ID and Secret key	139
<u>Step 5 — Perform AWS Scan Data Collection</u>	141
<u>Step 6 — Generate AWS Assessment Reports</u>	142
<u>AWS Assessment Reports</u>	144
Standard Reports	144
Performing a Cyberattack Risk Assessment Scan	145
<u>Cyberattack Risk Assessment Overview</u>	145
<u>Step 1 — Download and Install the Network Detective Pro app</u>	145
<u>Step 2 — Create a New Site</u>	145
<u>Step 3 — Create Cyberattack Risk Assessment in Network Detective Pro</u>	146
<u>Step 4 — Access RapidFire Tools Portal and Customize Branding</u>	148
<u>Step 5 — Create and Distribute the Cyberattack Risk Assessment Computer Scanner</u>	149
<u>Step 6 — Users Downloads and Runs Cyberattack Risk Assessment Computer Scanner</u>	152
<u>Step 7 — Download Scans in Network Detective Pro Cyberattack Risk Assessment</u>	154
<u>Step 8 —(Optional) Run Dark Web ID Scan</u>	156
Set Up Dark Web ID Integration with Network Detective Pro	158
<u>Step 9 — Generate Reports</u>	159
<u>Cyberattack Risk Assessment Reports</u>	160
Standard Reports	160
Performing an Exchange Assessment	161
<u>Exchange Assessment Overview</u>	161
What You Will Need	162
<u>Step 1 — Download and Install the Network Detective Pro Application</u>	162

<u>Step 2 — Create a New Site</u>	162
<u>Step 3 — Start an Exchange Assessment</u>	163
<u>Step 4 — Perform Exchange Scan Data Collection</u>	164
<u>Step 5 — Generate Exchange Assessment Reports</u>	168
<u>Exchange Assessment Reports</u>	168
Standard Reports	168
Change Reports	171
Performing a SQL Server Assessment	173
<u>SQL Server Assessment Overview</u>	173
What You Will Need	174
<u>Step 1 — Download and Install the Network Detective Pro Application</u>	174
<u>Step 2 — Create a New Site</u>	174
<u>Step 3 — Start an SQL Server Assessment</u>	175
<u>Step 4 — Perform SQL Server Scan Data Collection</u>	176
<u>Step 5 — Generate SQL Server Assessment Reports</u>	179
Standard Reports	180
Change Reports	182
<u>SQL Server Assessment Reports</u>	182
Standard Reports	182
Change Reports	184
Performing a Combined Network and Security Assessment	185
<u>Network Assessment Overview</u>	185
<u>Security Assessment Overview</u>	185
What You Will Need	186
Network Prerequisites for Network Detective Pro Scans	187
<u>Step 1 — Download and Install the Network Detective Pro Application</u>	188
<u>Step 2 — Create a New Site</u>	188
<u>Step 3 — Start a Network and Security Assessment</u>	189
<u>Step 4 — Initiate External Vulnerability Scan</u>	190

<u>Step 5 — Collect Data using Data Collector</u>	194
<u>Step 6 — Use the Push Deploy Tool to Collect Remaining Data</u>	205
<u>Step 7 — Import Scans into Network Detective Pro App</u>	209
<u>Step 8 — Generate Assessment Reports</u>	213
Appendices	214
<u>Pre-Scan Network Configuration Checklist</u>	214
Checklist for Domain Environments	214
Checklist for Workgroup Environments	216
<u>Enable Discovery Agents for Local Data Collection (Network Detective Pro)</u>	219
Step 1 — Enable Discovery Agents via RapidFire Tools Portal	219
Step 2 — Install Discovery Agent(s)	222
Step 3 — Confirm Discovery Agent install for your Organization	225
Step 4 — (Optional) Enable Access for Site Admin and Technician Users	225
Step 5 — Assign Labels to Agents	226
Step 6 — Schedule scans for Discovery Agent	228
Step 7 — Download scan into assessment	229
<u>Silent Install for Discovery Agent</u>	230
<u>Install Linux and OSX Discovery Agents</u>	231
Default Scripted Linux Install	231
Default Scripted OSX Install	232
Install Script Options	233
<u>Scripts for Linux and OSX Manual Data Collection</u>	235
Linux X64 Collection	235
OSX ARM64 Collection	235
OSX X64 Collection	235
Optional Flags	235
<u>End-user Initiated Computer Scans</u>	237
Step 1 — Create a New Network Detective Pro Portal Site	237
Step 2 — Customize Portal Branding	237
Step 3 — Enable End-users Scans from RFT Portal	238
Step 3 — Send URL to End-users	238

Step 4 — End-user Runs Computer Scanner from URL	238
Step 5 — Download Scan(s) from Network Detective	240
For New Sites	240
Existing Sites	240
Download End-user Scans	241
Step 6 — Generate Reports	241
<u>Generate Commonly Used Report Sets</u>	242
<u>Document Exceptions with the Issue Exception Worksheet</u>	245
<u>Using a USB drive</u>	249
<u>Override Issues in Network Detective Pro Reports</u>	250
Override issues at the global level	250
Override issues at the site level	252
Affected Reports	254
<u>Adding a Connector to a Site</u>	255
<u>Adding an Inspector to a Site</u>	257
<u>Dark Web Scan Summary for Security Assessment Module</u>	259
How it Works	259
How to Perform Dark Web Scan as Part of Your Security Assessment	260
What to do if Compromised Passwords are Detected	262
<u>Set Up Full Dark Web ID Integration</u>	263
Step 1 — Contact Dark Web ID Support to Enable User API Access	263
Step 2 — Set Up Dark Web ID Integration with Network Detective Pro	263
Step 3 — Continue Assessment and Perform Scan	264
<u>Perform Datto Unified Continuity Scan</u>	265
Step 1 — Enable API Access in Datto Partner Portal	265
Step 2 — Enable Datto Unified Continuity Integration	266
Step 3 — Perform Network Assessment Scan	268
Step 4 — Perform Datto Unified Continuity Scan	268
Step 5 — Generate Reports	269
<u>Data Breach Liability Scanning and Reporting</u>	271
Steps to Perform Scans to Identify PII and Generate the Data Breach Liability Report ..	272

<u>Completing Worksheets and Surveys</u>	275
Entering Assessment Responses into Surveys and Worksheets	275
Add Image Attachments to Surveys and Worksheets	276
Add SWOT Analysis to Surveys and Worksheets	277
Time Savings Tip to Reduce Survey and Worksheet Data Input Time	278
Use the InForm Worksheet Tool Bar	278
Bulk Entry for InForm Worksheets	278
Create Word Response Form	281
Important Note on Working with Word Response Forms	282
Import Word Response Form	283
<u>Compiling Network Detective Data</u>	285
<u>Integrate Network Detective Pro with a PSA System</u>	287
Step 1 — Gather Credentials and Set Up your PSA System	287
Step 2 — Create a Connection Between Network Detective Pro and Target PSA	289
Export Configuration Items from Network Detective Pro to PSA	292
Export Exchange Contacts from Network Detective Pro to PSA	298
Create Tickets from Assessment Issues and Recommendations from Network Detective Pro to PSA	298
Set Up Autotask Integration	301
Set Up ConnectWise REST Integration	306
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	306
Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with	307
Create Minimum Permissions Security Role for API Member	307
Table Setup Configuration	308
Step 3 — Create an API Key in the ConnectWise Ticketing System	309
Step 4 — Configure Service Tables in ConnectWise	310
Step 5 — Remove "Disallow Saving" Flag from Company	311
Set Up ConnectWise SOAP Integration	315
Set Up Kaseya BMS Integration	317
<u>Export Network Detective Pro Reports to IT Glue</u>	319
Step 1 — Create API Key in IT Glue	319
Step 2 — Create Connection to IT Glue in Network Detective Pro	320

Step 3 — Export Reports to IT Glue	321
<u>Sign Out of Network Detective Pro</u>	324
<u>Network Detective Linux Computer Data Collector</u>	326
Download the Linux Computer Data Collector	326
Run the Linux Computer Data Collector	326
Scan Output and Import into Assessment	326
<u>Augment Reporting to Eliminate False Positives</u>	327
Use the Excel Export Spreadsheet to Find Display Names	329

Introduction to Network Detective Pro

Network Detective Pro is the indispensable tool for MSPs who want to maximize the value of each client relationship. Be in-the-know about every new network environment you touch, and every change that takes place on all the client networks you manage. Then transform that data into meaningful reports that you can use throughout the managed services lifecycle to work faster and create new revenue opportunities.

Network Detective Pro is quick and easy to use. To perform an assessment you follow four basic steps:

1. **Create a Site to Organize your Assessment:** Use **Sites** to manage 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:** Start a new project for your chosen assessment and use the guided checklist to collect data.
3. **Perform the Assessment and Data Collection:** Run scans as required for your chosen assessment. Use the assessment-specific Data Collector and/or the Push Deploy Tool. The output of the scans will be in .zip files based on assessment type (.ndf, .cdf, .sdf).
4. **Generate Assessment Reports:** Customize the reports to be presented to your customers by setting up your company's branding. Then generate a set of reports to accomplish your exact business purpose!

Once you complete an assessment, you can then use **Reporter**. Reporter to automate, schedule, and deliver the assessment reports generated by Network Detective Pro. Reporter can be used with each Network Detective Pro assessment type, and allows you to deliver emailed assessment reports to anyone on your distribution list, or store generated reports in a shared folder location on your internal network.

Network Detective Pro Components

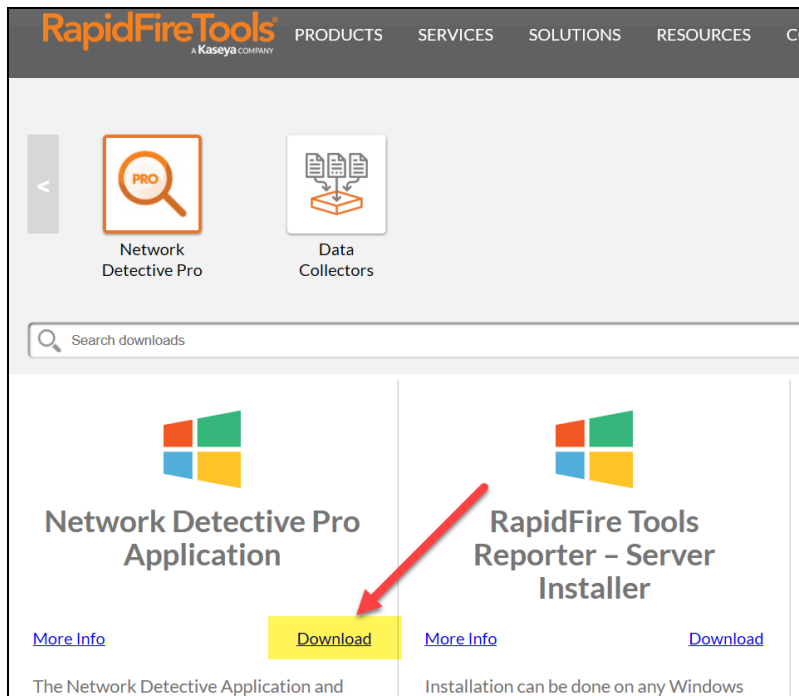
The Network Detective Pro application is composed of several components:

- **Network Detective Pro application:** create and manage your assessments, generate reports, detect external vulnerabilities for target sites, and scan the Microsoft Cloud

- **Data Collectors for various assessment types (Network, Security, Exchange, and SQL):** download and run the specified data collector to generate scan data to import into your assessment in Network Detective Pro
- **Push Deploy Tool:** save time and perform local computer scans from a centralized location on the target network to collect scan data
- **Reporter:** use in tandem with the Remote Data Collector to automate your assessment projects from beginning to end

Download and Install the Network Detective Pro Application

Visit <https://www.rapidfiretools.com/ndpro-downloads/>. Download and install the Network Detective Pro Application.



Set Up Network Detective Pro Reports

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

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

Setting Report Branding and Customization Preferences

Network Detective Pro 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.

Setting Reports Preferences at the Global or Site Level

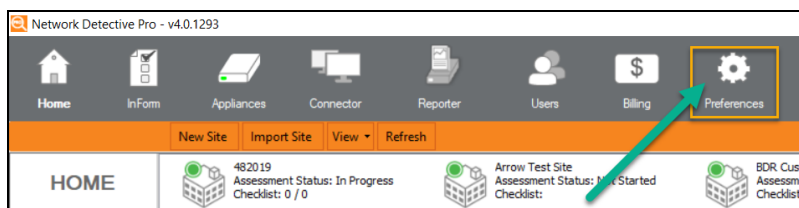
You can configure the report branding by configuring the **Report Defaults** settings at one of two levels:

- at the Global level (for all Sites) using the Network Detective Pro **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 Pro, 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 Pro 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 Pro**. 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 Pro, 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.

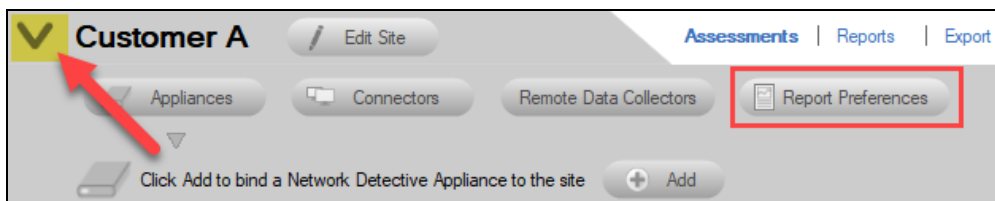
Setting Reports Preferences

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.



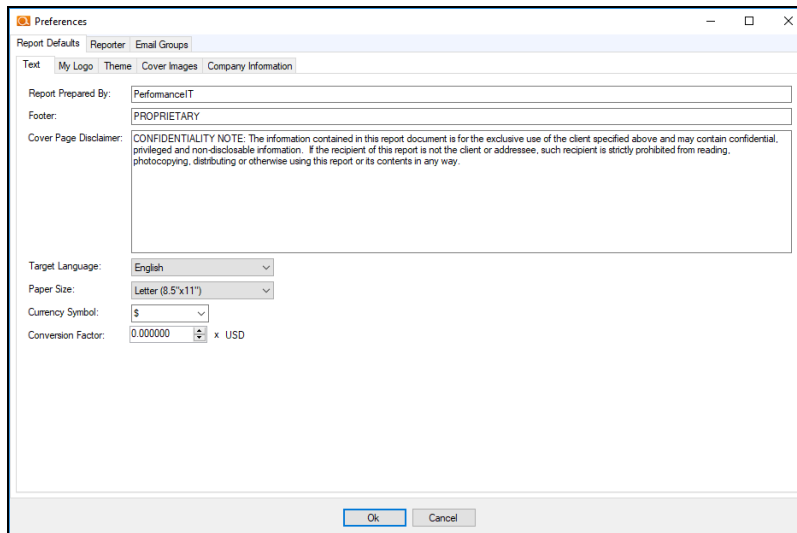
The **Site’s Preferences** will be displayed.



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**.

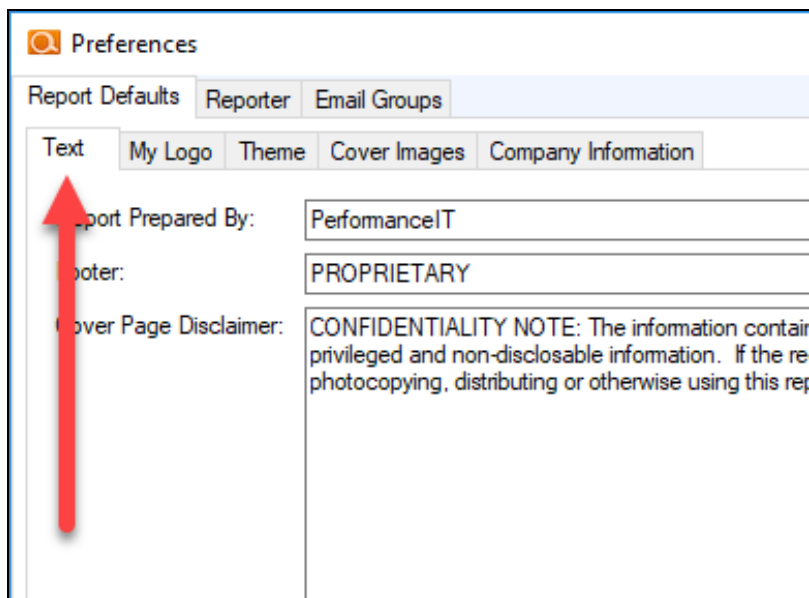
Setting Reports Preferences

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

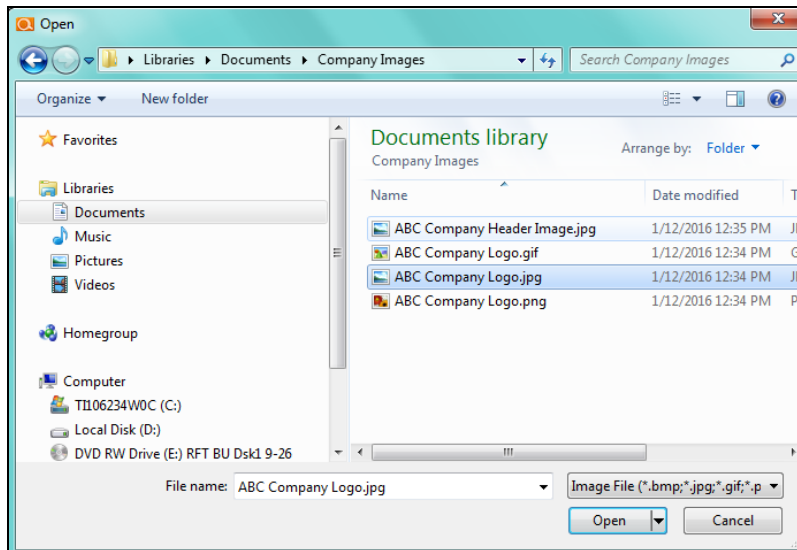
To incorporate your company's logos into the Reports generated by Network Detective, you must update the **My Logos Report Defaults** preferences to include your company's logo files.

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**.



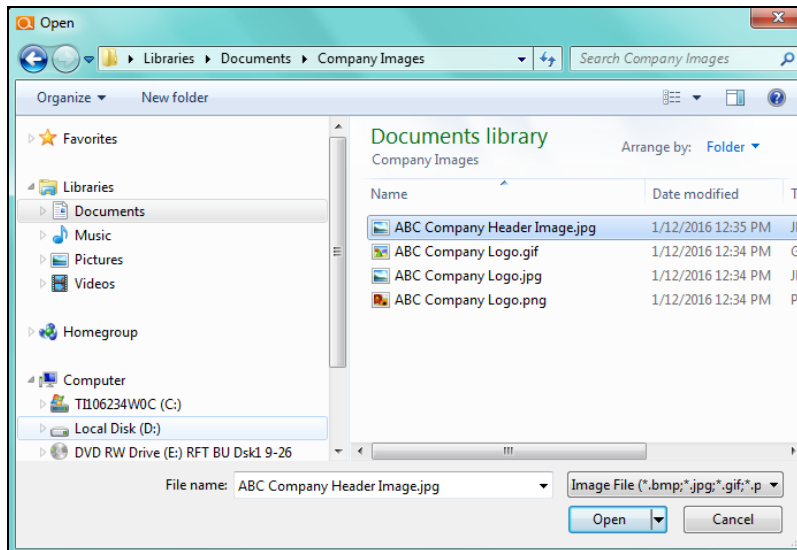
Select the image file to be used for the **Cover Logo Image** and select **Open** to complete the image upload process.

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

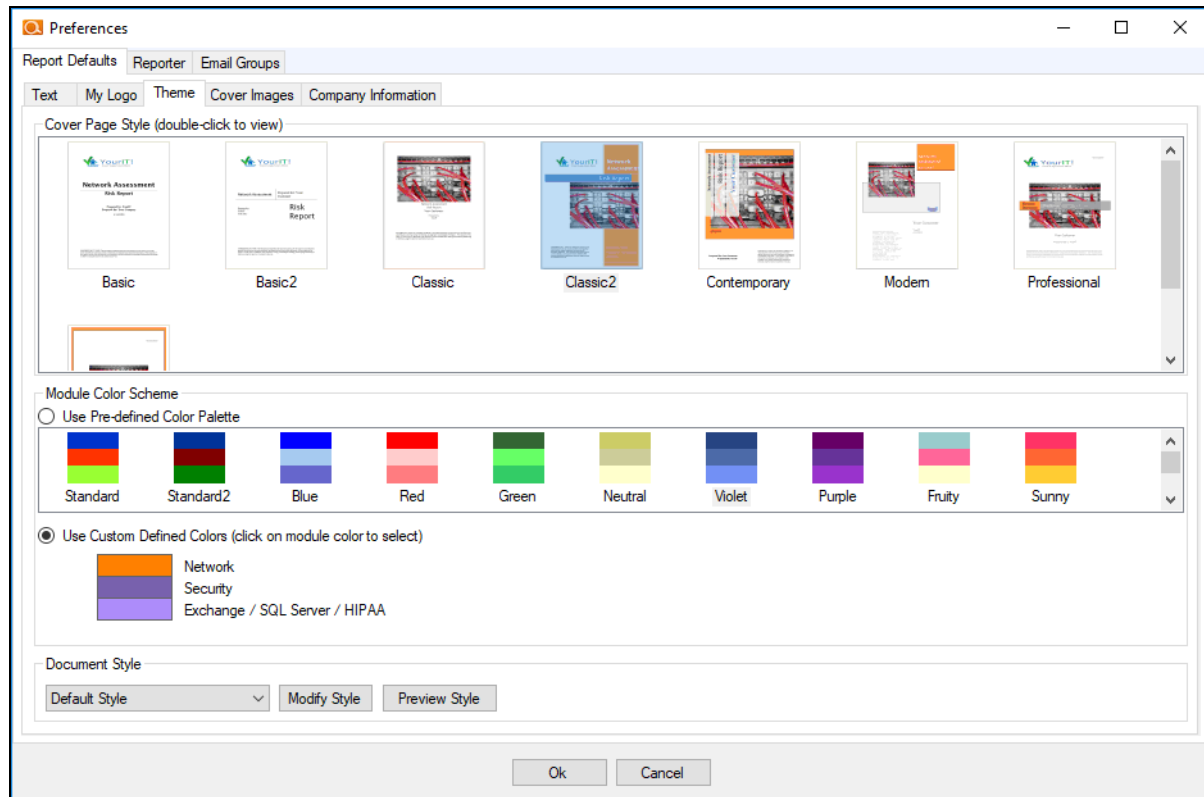
To save your **Cover Logo Image** and **Header Logo Image** settings, select the **Preferences Window Ok** button.

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).

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

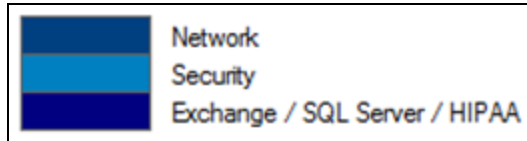
Select the **Cover Page Style** from the available **Cover Page** document styles. If no other **Reports Defaults** preferences are to be set, then select the **Preferences Window Ok** button. Otherwise, continue setting a **Color Scheme** for one or more Modules as detailed below.

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) for use during the report generation process.

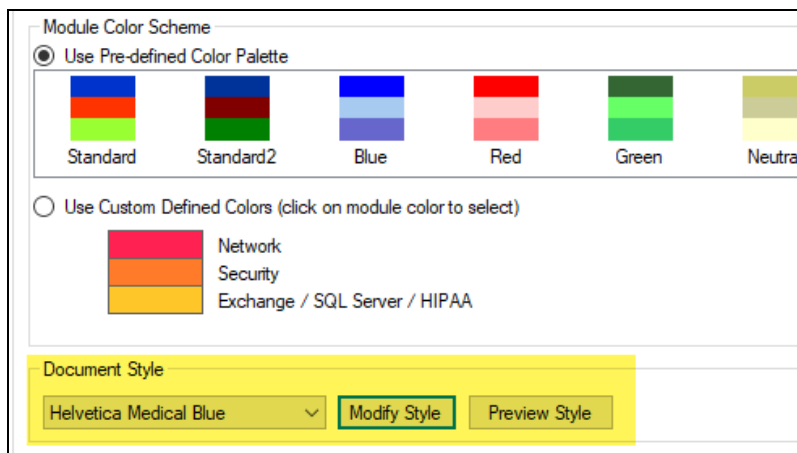
To use the **Module Color Scheme** option, select a color palette from the Pre-defined Color Palettes.

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.

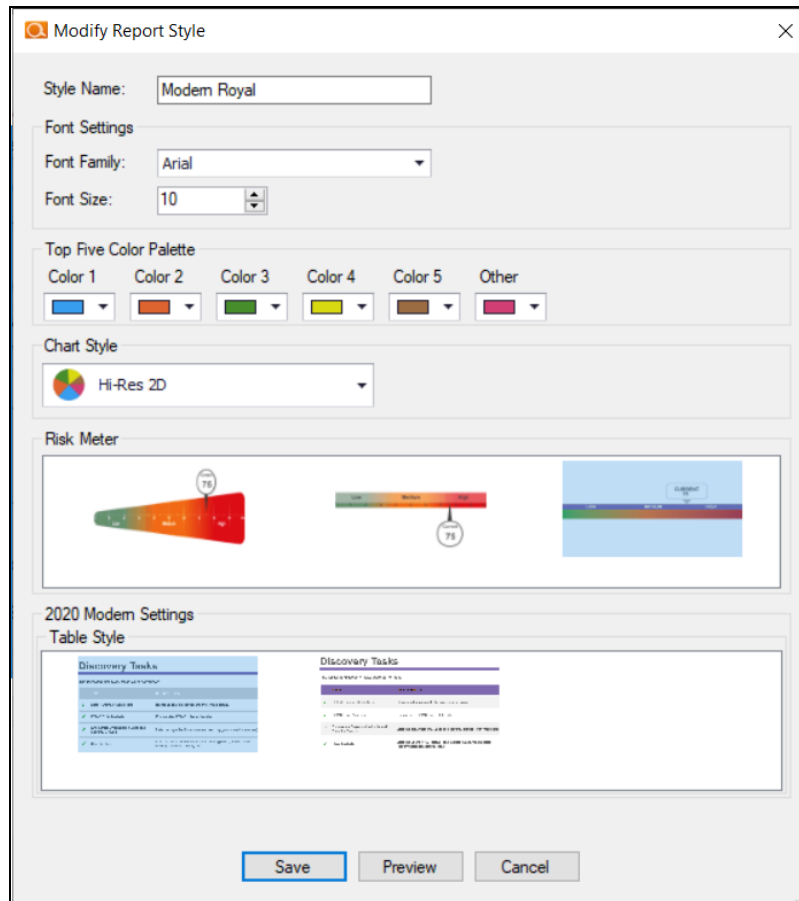


Setting Document Style

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



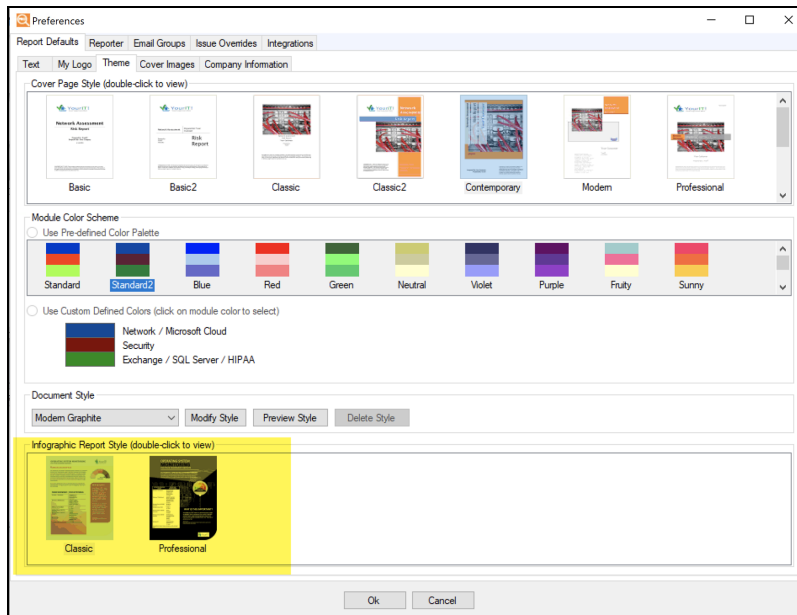
Click the **Modify Style** to make changes to the selected style.



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:

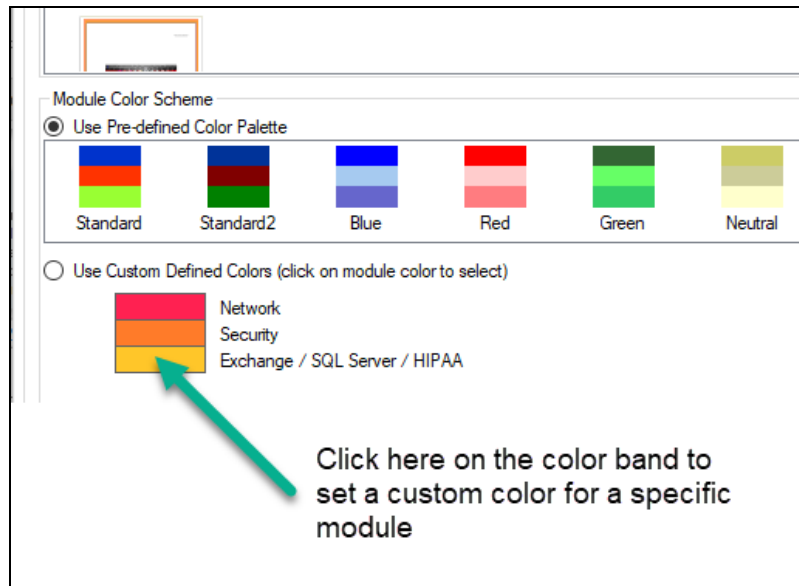
- Outdated Operating Systems Summary
- Outdated Malware Definitions Summary
- Password Policy Summary
- Data Breach Liability Summary
- Executive Summary
- Dark Web ID Summary

Assigning Custom Defined Color Schemes to Each Assessment Module

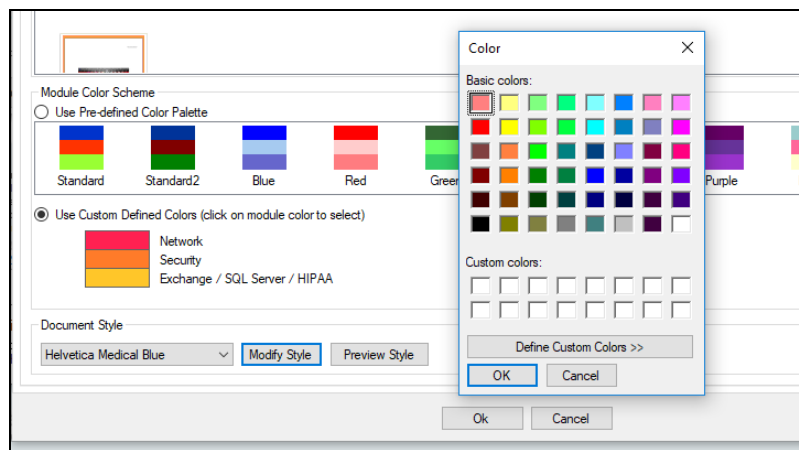
Note: Currently, you cannot define custom color schemes for the "Modern" report styles.

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.

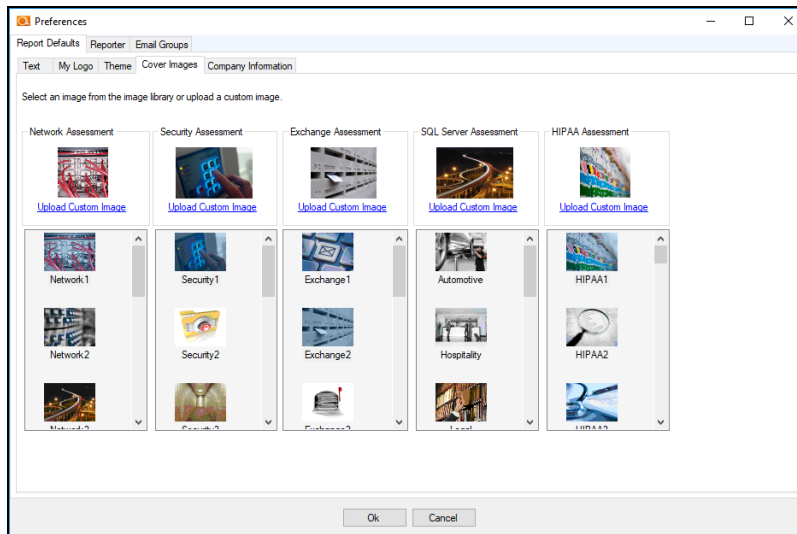


To save the color assignment for the Module's color band you selected, click on the **Preference Window Ok** button. Then set the colors for the other modules. To save your final Theme settings, select the **Preferences Window Ok** button.

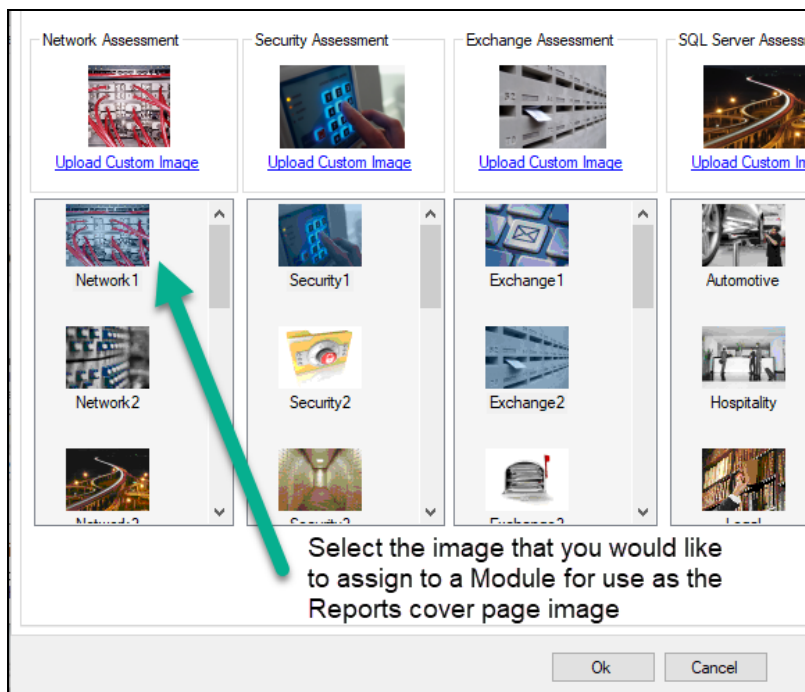
Set Reports Cover Images Preferences

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 Pro

You can configure the format for dates displayed in Network Detective Pro 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 Pro, 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.

Preferences

Report Defaults | Email Groups

Text | My Logo | Theme | Cover Images | Company Information

Report Prepared For:

Report Prepared By: RapidFire Tools Support

Footer: PROPRIETARY

Cover Page Disclaimer: CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Target Language: English

Date Format: dd-MMM-yyyy 19-Jun-2018

Paper Size: Letter (8.5"x11")

Currency Symbol: \$

Conversion Factor: 0.000000 x USD

Reset to Global Preferences

Ok Cancel

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

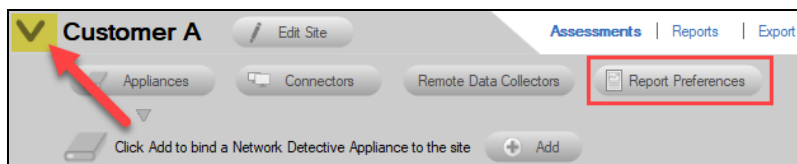
Assigning the Global Reports Preferences to a Site

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.

The screenshot shows the 'Preferences' dialog box with the 'Report Defaults' tab selected. The dialog contains several input fields and dropdown menus for configuring report settings. A green arrow points to a yellow button labeled 'Reset to Global Preferences' located at the bottom right of the dialog, above the 'Ok' and 'Cancel' buttons.

Report Defaults | Email Groups

Text | My Logo | Theme | Cover Images | Company Information

Report Prepared For:

Report Prepared By: PerformanceIT

Footer: PROPRIETARY

Cover Page Disclaimer: CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Target Language: English

Paper Size: Letter (8.5"x11")

Currency Symbol: \$

Conversion Factor: 0.000000 x USD

Reset to Global Preferences

Ok Cancel

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

Performing a Network Assessment

Network Assessment Overview

The Network Assessment Module gives you the broadest insights of any IT assessment module. The Network Assessment Module has many every day uses for your MSP, including:

- Conducting full, 'deep-dive' network assessments
- Documenting your customers' networks as part of regular "Technology Reviews"
- Generating change management reports for clients
- Conducting IT SWOT Analyses to help your clients make better and more informed business decisions

What You Will Need

Network Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
Network Detective Data Collector	The Network Detective Network Assessment Data Collector (NADC) is a windows application that performs the data collections for the Network Assessment Module.
Push Deploy Tool	The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.



Network Prerequisites for Network Detective Pro Scans

For a successful network scan:

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

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

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

Follow these steps to perform a Network Assessment.

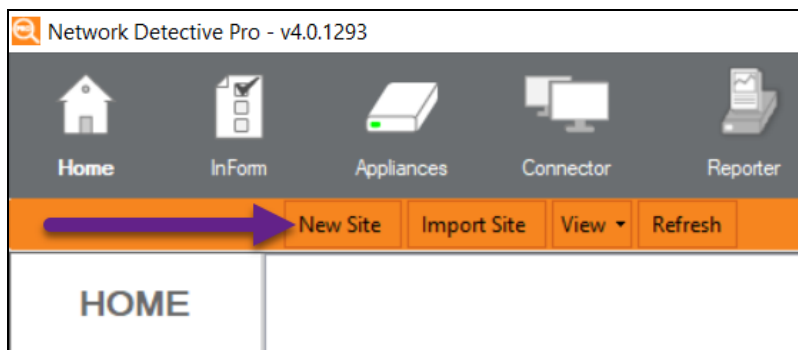
Step 1 — Download and Install the Network Detective Pro app

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

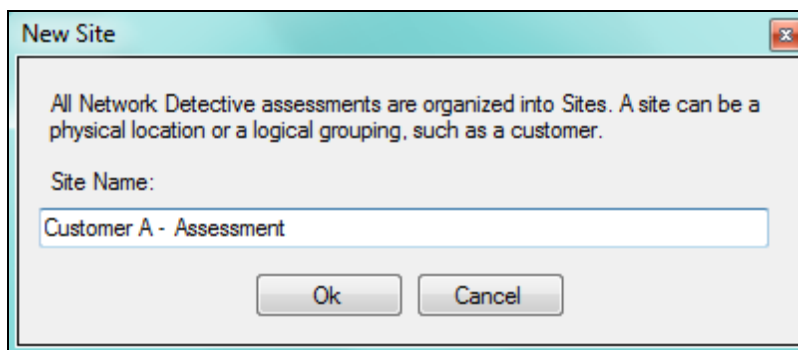
Step 2 — Create a New Site

To create a new site:

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



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

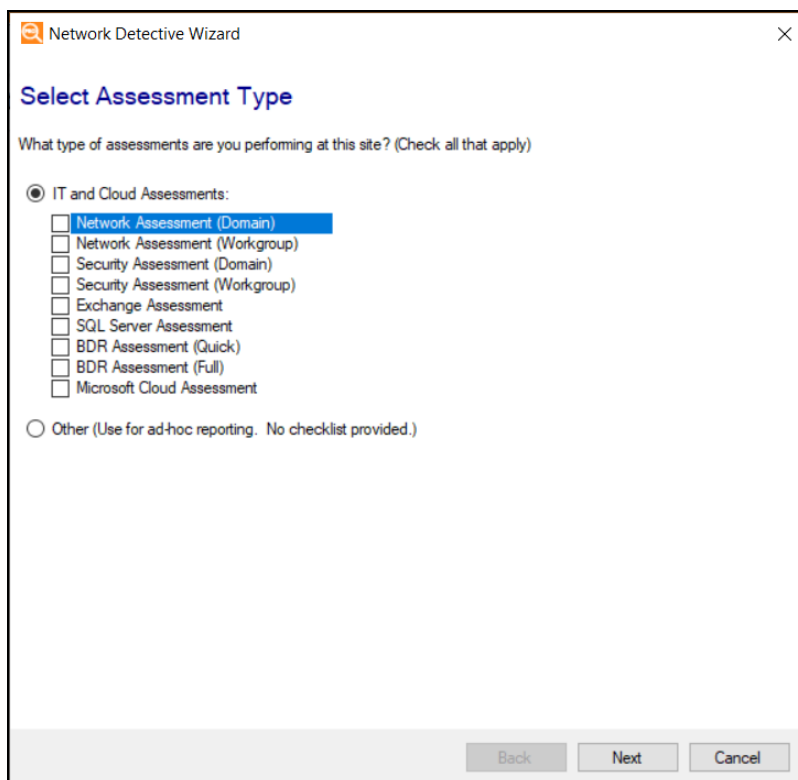


Step 3 — Start a Network Assessment

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

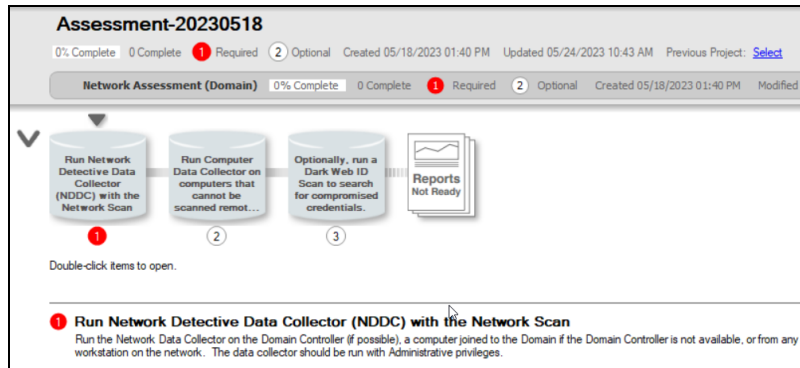


Next, select the **Network Assessment** option presented.



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

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



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

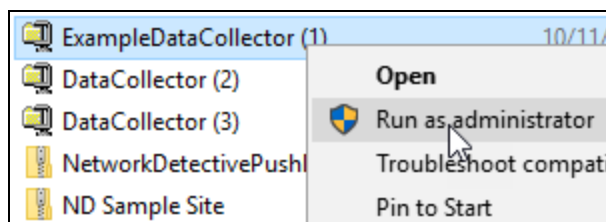
You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.



Step 4 — Perform Network Scan Data Collection

Download and run the **Network Detective Pro 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/ndpro-downloads/> 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.

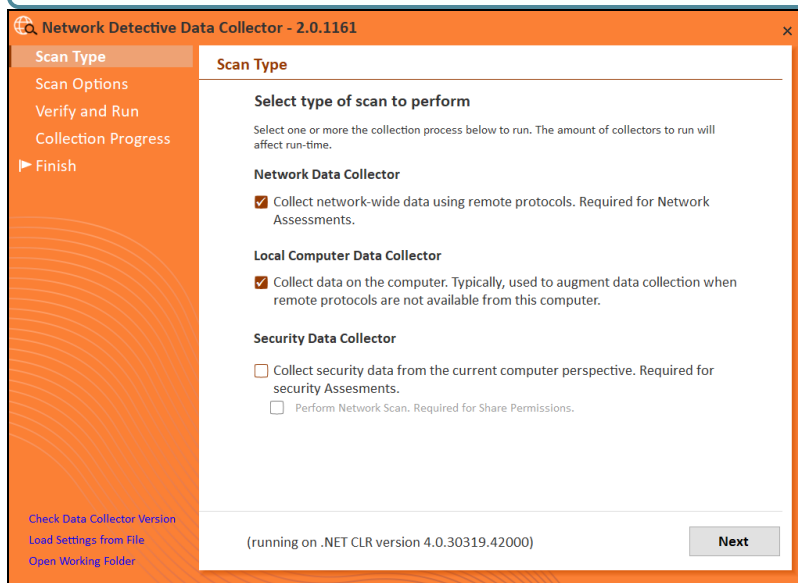
- Look here if you are ["Scanning an Active Directory Domain-based Network" below](#)
- Look here if you are ["Scanning a Workgroup Network" on page 43](#)

Scanning an Active Directory Domain-based Network

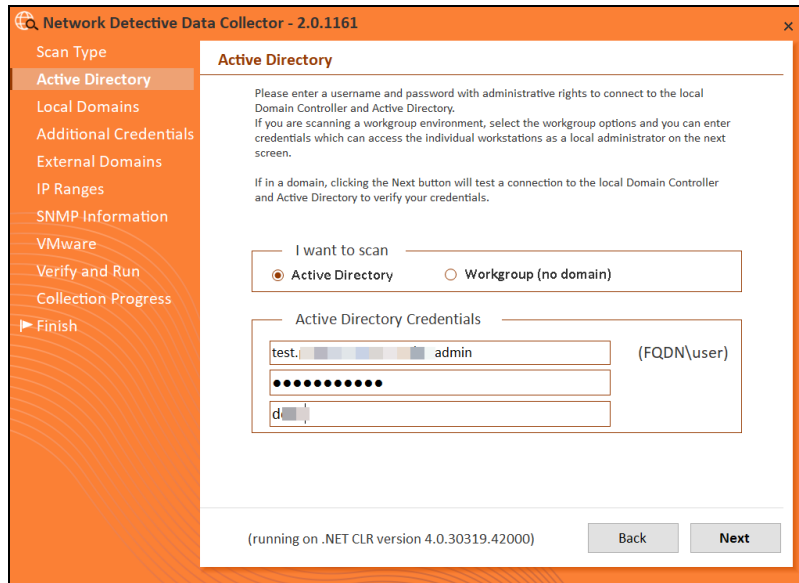
Once you run the Data Collector, the Scan Type screen will appear.

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.



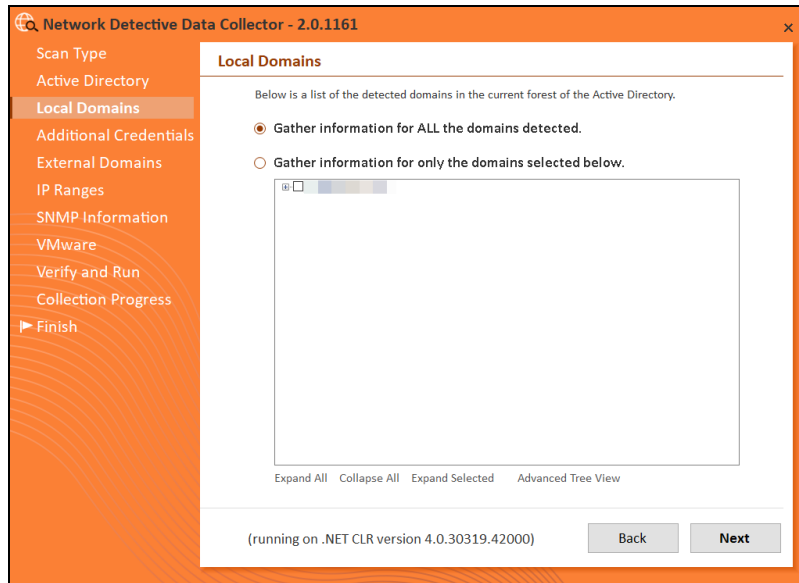
2. The **Active Directory** window will appear. Select the type of network you are scanning: *Active Directory domain*.



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.

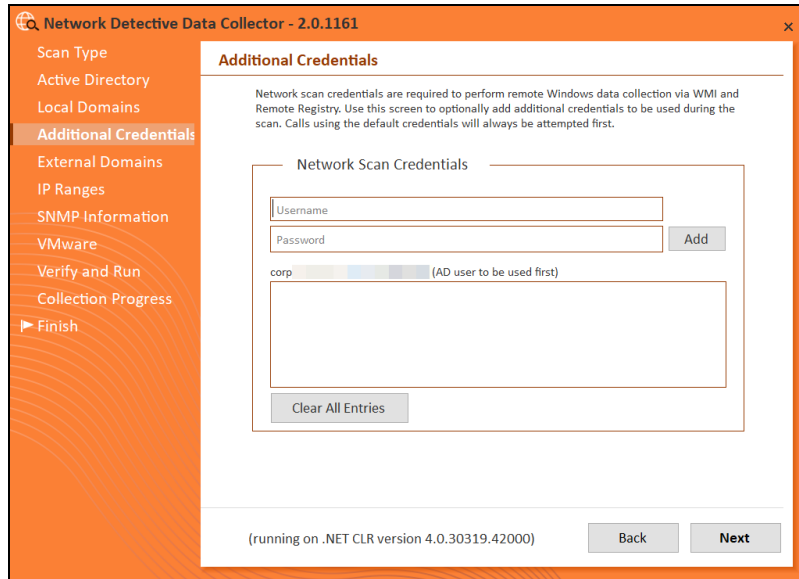
Note: For example: **corp.yourprospect.com\username**.

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**.

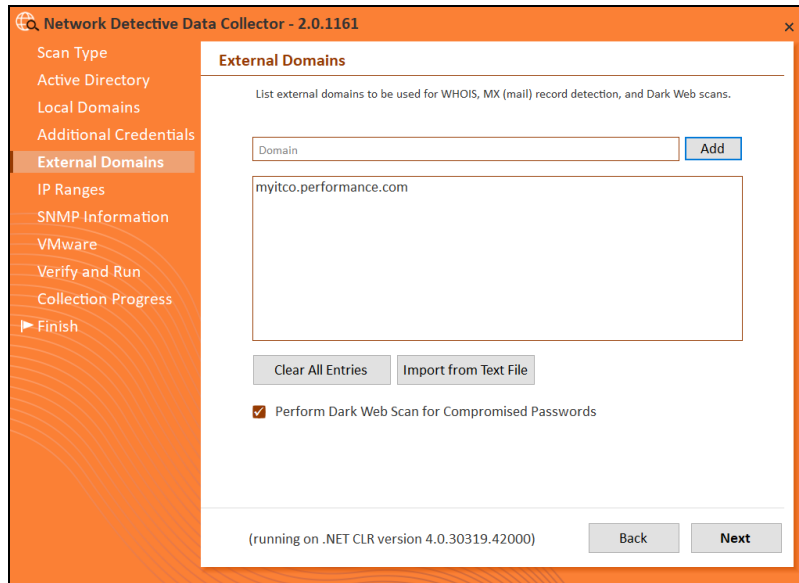


Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

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**.

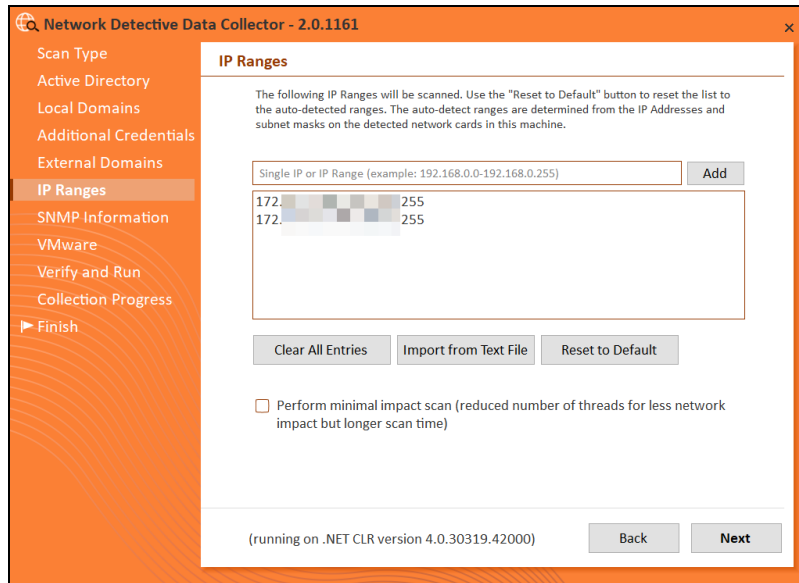


A Whois query and MX (mail) record detection will be performed on the external domains.

Note: Perform Dark Web Scan for Compromised Passwords*: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. This service will return the first 5 compromised passwords for each domain specified. If any compromised credentials exist for these domains, they will appear in your assessment reports for the **Security Assessment Module (SAM)**.

*To access the Dark Web Scan results, you must have a subscription to the Security Assessment Module and you must generate Security Assessment reports using your data. See also [Dark Web Scan Summary for Security Assessment Module](#).

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**.

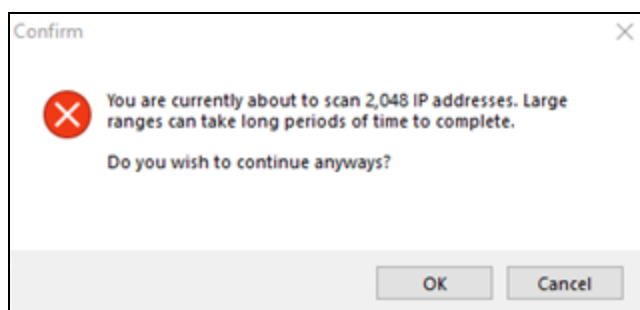


From this screen you can also:

- 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.

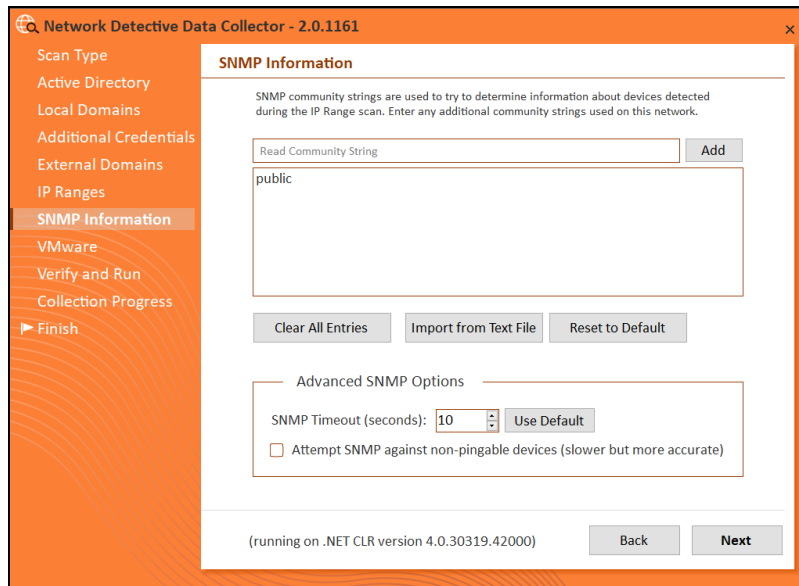
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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



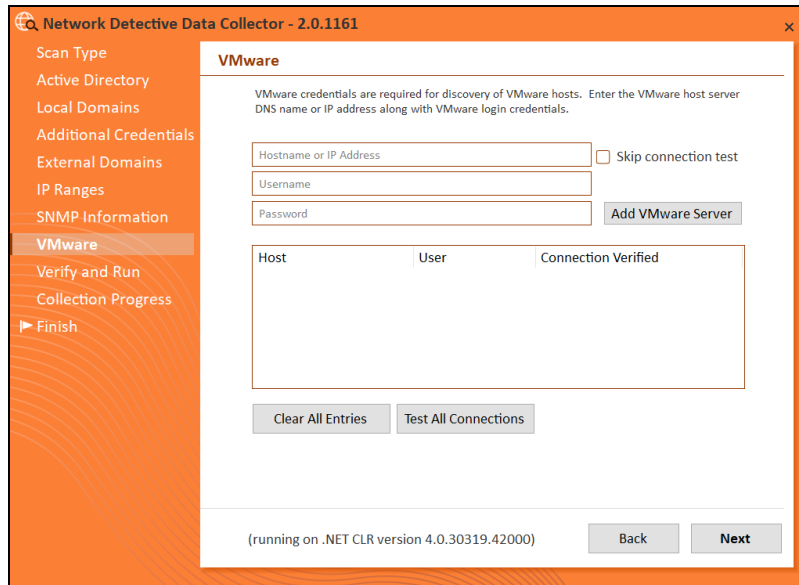
Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

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



Tip: Select **Attempt SNMP against non-pingable devices** to enhance Layer 2/3 data collection and reporting with Network Detective Pro. Note that this option may increase overall scan time.

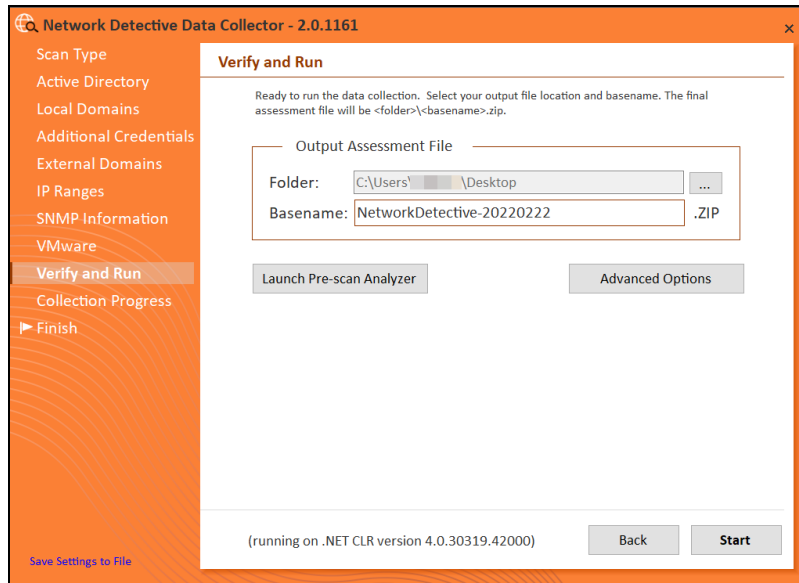
- The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next**.



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 **.NDF** file.

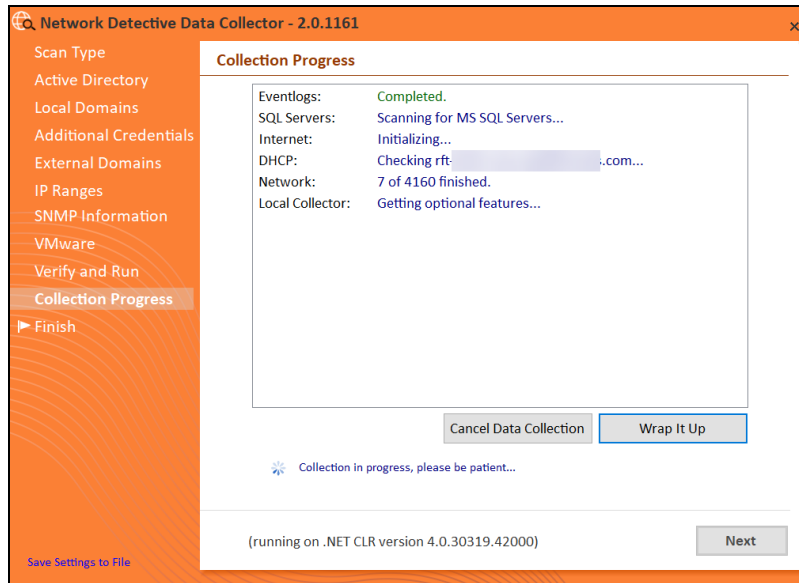


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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

Overview Result Summary Active Directory SQL Server Network Computers Push Deploy						
Pushing local data collectors to remote computers requires WMI, Admin\$ access, and .NET 3.5 or above.						
Showing: All Nodes						
Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01.CORP.RAPIDFIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORP.RAPL...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-095DFE1.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HM0E71.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4Q80.CORP...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORP.R...	10.236.83.1...	✓	?			Accessing WMI...
DESKTOP-7RF9K75.CORP.R...		✓	✗			WMI failed. The RPC server is unavailable.

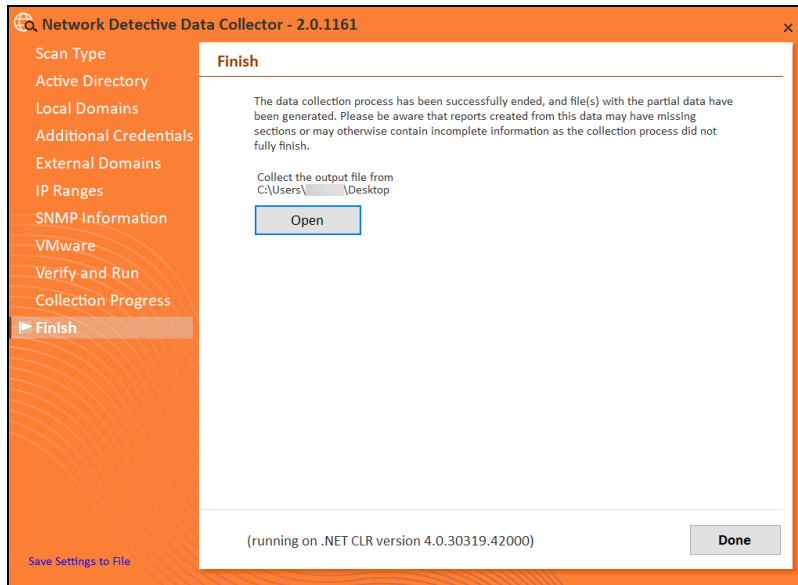
Enter any **Comments** and then click **Start**.

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



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

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



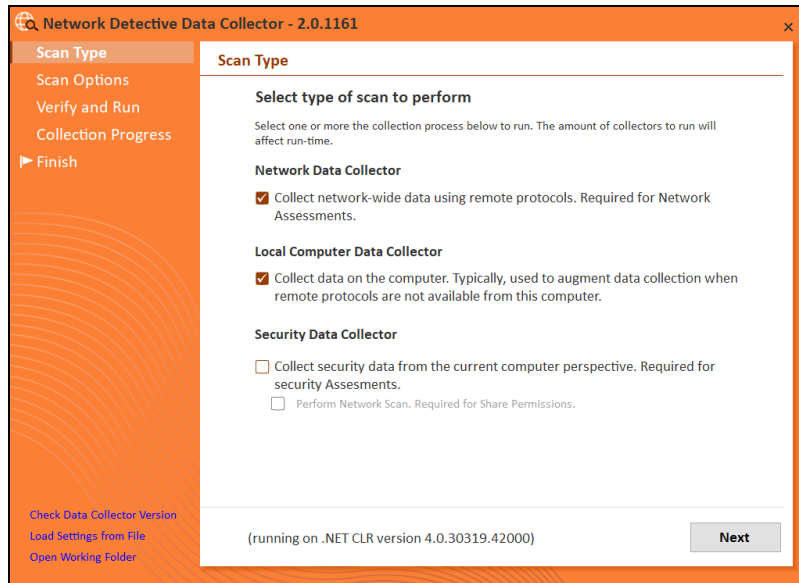
Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

Scanning a Workgroup Network

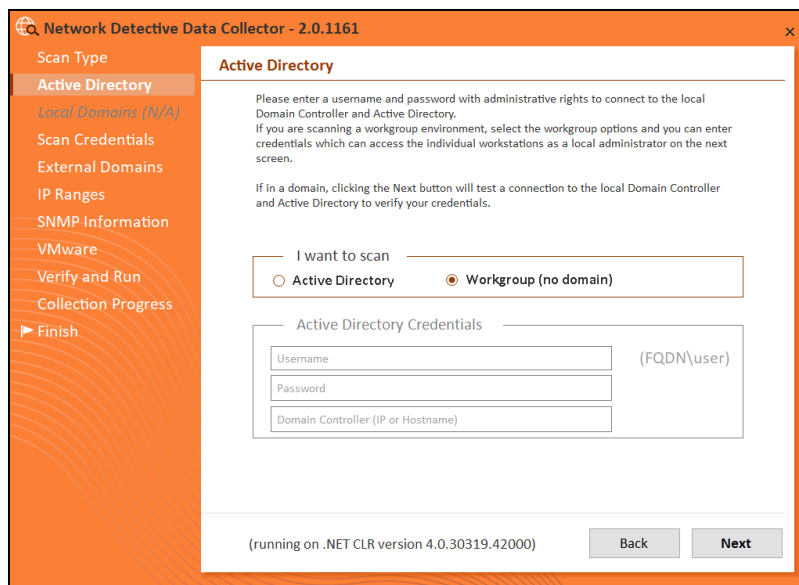
Once you run the Data Collector, the Scan Type screen will appear.

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: *Workgroup*).



3. 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**.

Network Detective Data Collector - 2.0.1161

Scan Type
Active Directory
Local Domains (N/A)
Scan Credentials
External Domains
IP Ranges
SNMP Information
VMware
Verify and Run
Collection Progress
▶ Finish

Scan Credentials

Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan.

Network Scan Credentials

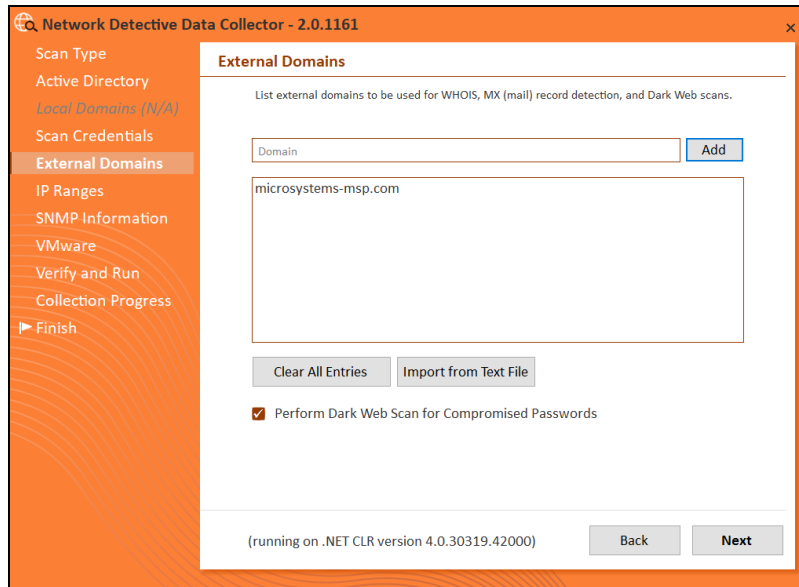
Username
Password Add

Clear All Entries

✖ At least one credential is required in a workgroup environment.

(running on .NET CLR version 4.0.30319.42000) Back Next

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

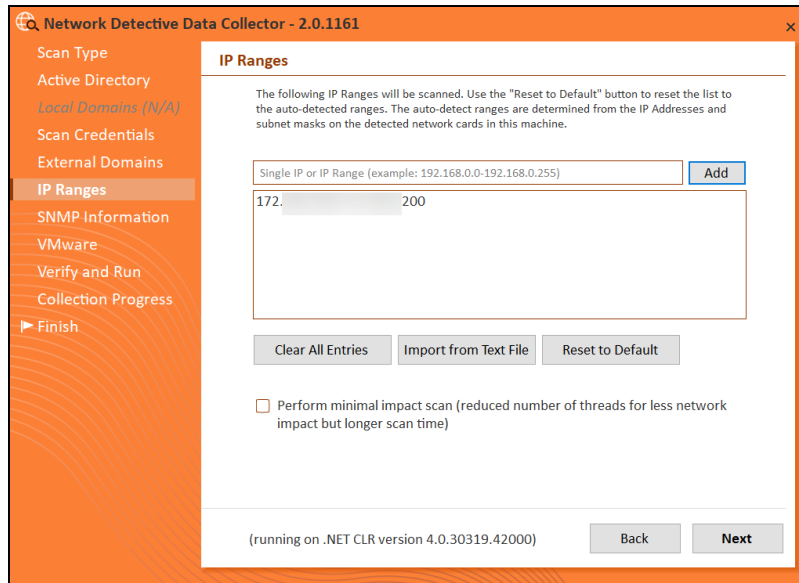


A Whois query and MX (mail) record detection will be performed on the external domains.

Note: Perform Dark Web Scan for Compromised Passwords*: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. This service will return the first 5 compromised passwords for each domain specified. If any compromised credentials exist for these domains, they will appear in your assessment reports for the **Security Assessment Module (SAM)**.

*To access the Dark Web Scan results, you must have a subscription to the Security Assessment Module and you must generate Security Assessment reports using your data. See also [Dark Web Scan Summary for Security Assessment Module](#).

5. 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**.

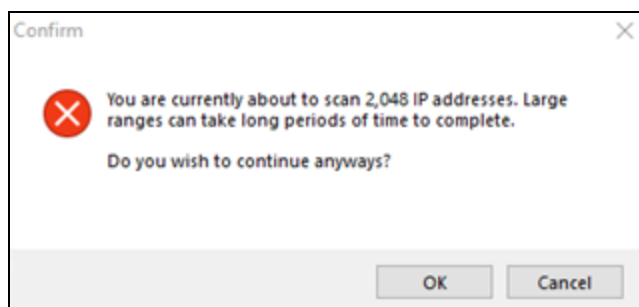


From this screen you can also:

- 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.

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

Network Detective Data Collector - 2.0.1161

Scan Type
Active Directory
Local Domains (N/A)
Scan Credentials
External Domains
IP Ranges
SNMP Information
VMware
Verify and Run
Collection Progress
Finish

SNMP Information

SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.

Read Community String Add

Clear All Entries Import from Text File Reset to Default

Advanced SNMP Options

SNMP Timeout (seconds): Use Default

☐ Attempt SNMP against non-pingable devices (slower but more accurate)

(running on .NET CLR version 4.0.30319.42000) Back 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). MBSA 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.

- 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**.

The screenshot shows the 'VMware' configuration window in the Network Detective Data Collector. The left sidebar contains a list of scan types: Scan Type, Active Directory, Local Domains (N/A), Scan Credentials, External Domains, IP Ranges, SNMP Information, VMware (selected), Verify and Run, Collection Progress, and Finish. The main area is titled 'VMware' and contains instructions: 'VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials.' Below this are three input fields: 'Hostname or IP Address', 'Username', and 'Password'. There is a checkbox for 'Skip connection test' and a button 'Add VMware Server'. A table with columns 'Host', 'User', and 'Connection Verified' is present. At the bottom are buttons 'Clear All Entries' and 'Test All Connections'. The status bar at the bottom indicates '(running on .NET CLR version 4.0.30319.42000)' and has 'Back' and 'Next' buttons.

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

The screenshot shows the 'Verify and Run' configuration window in the Network Detective Data Collector. The left sidebar is the same as the previous window, with 'Verify and Run' selected. The main area is titled 'Verify and Run' and contains instructions: 'Ready to run the data collection. Select your output file location and basename. The final assessment file will be <folder>\<basename>.zip.' Below this is the 'Output Assessment File' section with two input fields: 'Folder:' (containing 'C:\Users\...\Desktop') and 'Basename:' (containing 'NetworkDetective-20220222'). There are buttons 'Launch Pre-scan Analyzer' and 'Advanced Options'. The status bar at the bottom indicates '(running on .NET CLR version 4.0.30319.42000)' and has 'Back' and 'Start' buttons. A 'Save Settings to File' link is visible in the bottom left corner.

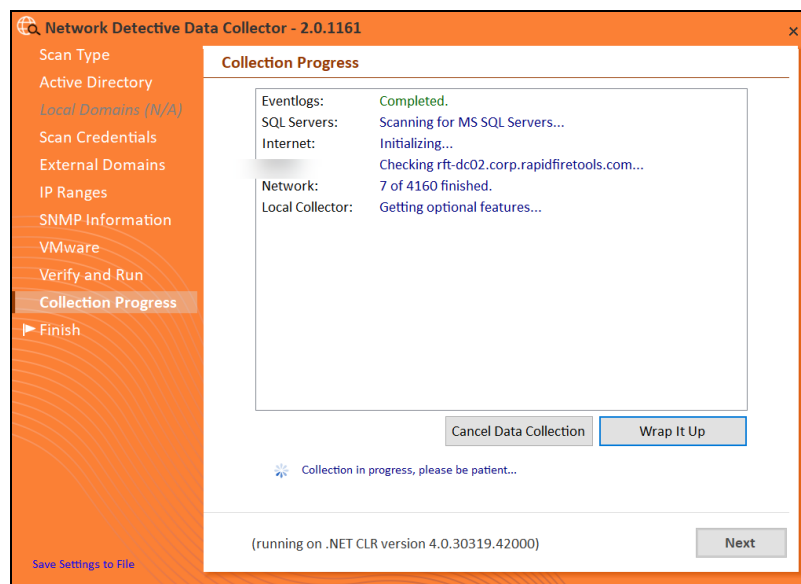
Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which

assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion of the pre-scan.

Overview Result Summary Active Directory SQL Server Network Computers Push Deploy						
Pushing local data collectors to remote computers requires WMI, Admin\$ access, and .NET 3.5 or above.						
Showing: All Nodes						
Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01-CORP-RAPIDFIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10-CORP-RAPL...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-9SSDFE1-CORP-R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-4HN0E7L-CORP-R...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4Q8O-CORP-R...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30-CORP-R...	10.236.83.1...	✓	?			Accessing WMI...
DESKTOP-7RF9K75-CORP-R...		✓	✗			WMI failed. The RPC server is unavailable.

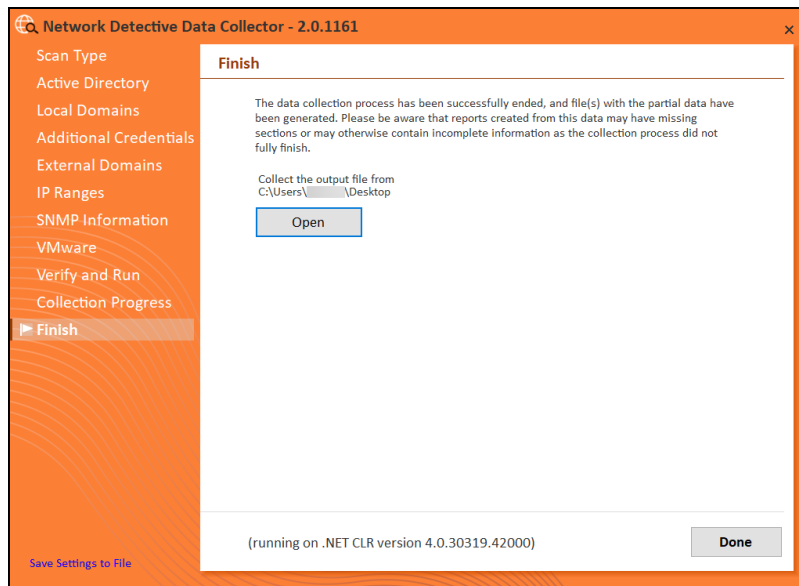
Enter any **Comments** and then click **Start**.

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



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

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



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

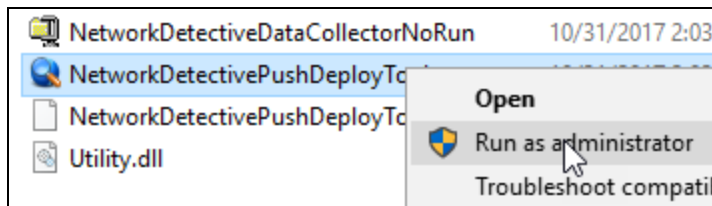
Step 5 — Use the Push Deploy Tool to Collect Remaining Data

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

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

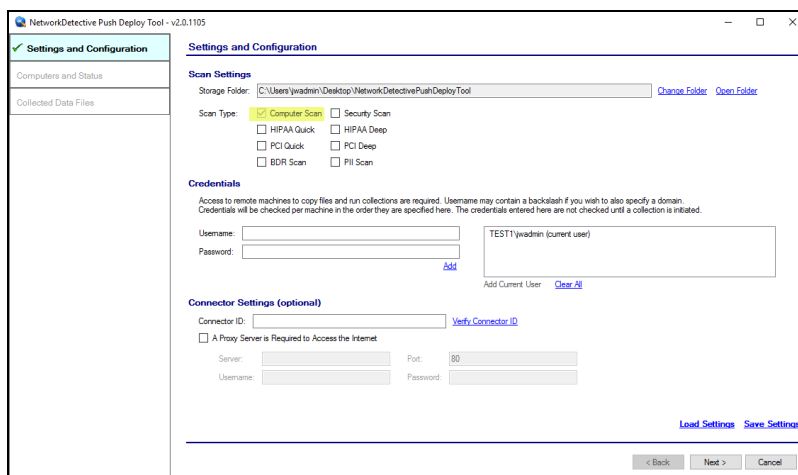
1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/ndpro-downloads/> and download the Push Deploy Tool.
2. **Unzip** the files onto a USB drive or directly onto any machine on the target network.

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



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

The Push Deploy Tool Settings and Configuration window will appear.



- Set the **Storage Folder location** and select the **Computer Scan** option.

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

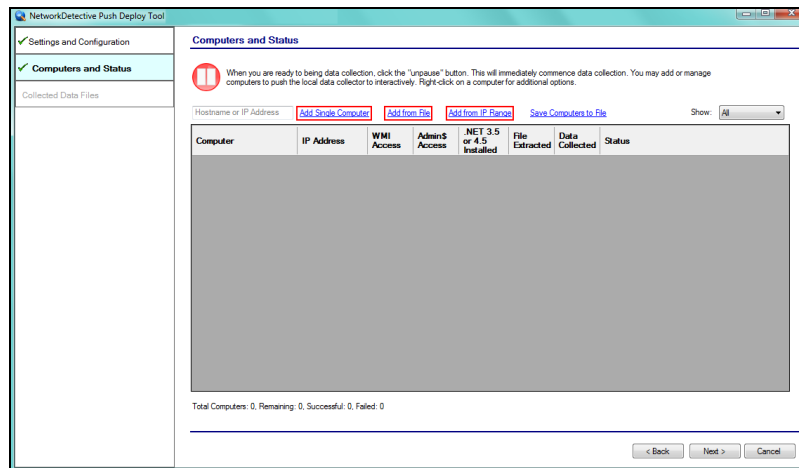
If additional credentials are required, type in the administrator level **Username** and **Password** necessary to access the local computers on the network to be scanned. Then click **Add**.

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

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

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

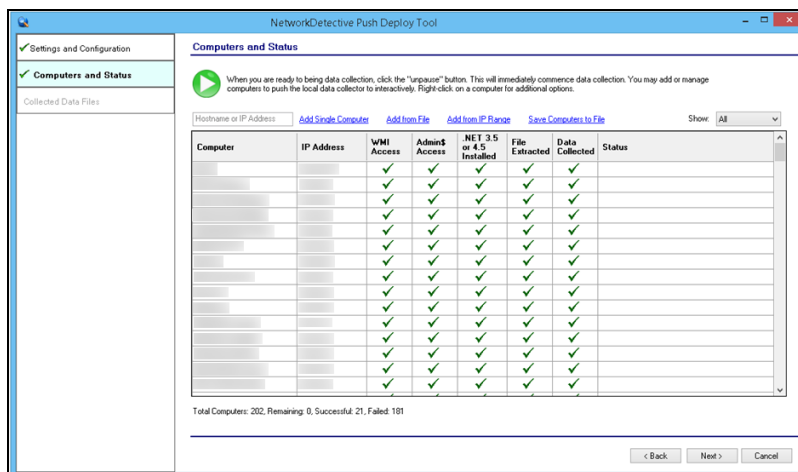
scanned again in future assessments



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

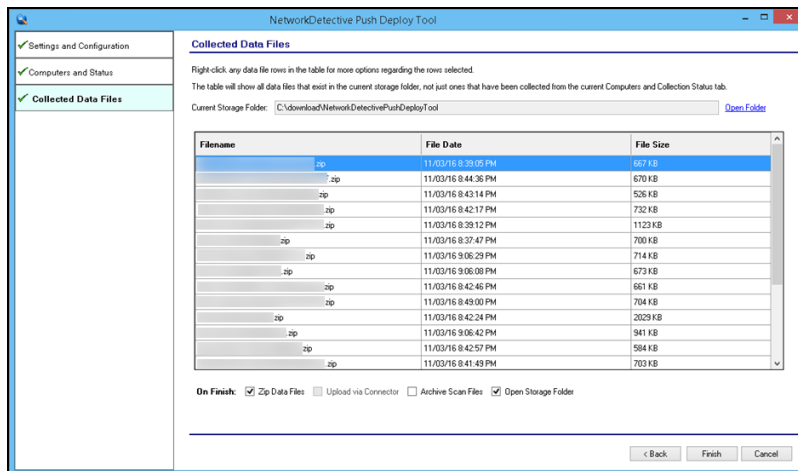
After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the **Computers and Status** window.

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



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

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



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

MORE INFO:

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

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

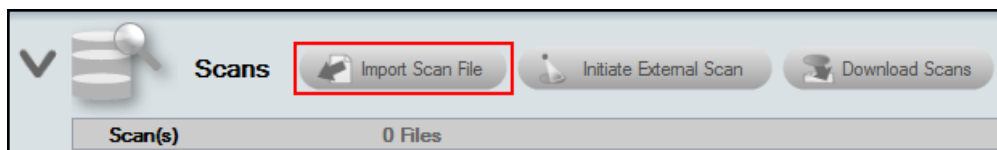
After all of the **Computer Scans** are complete, the next phase in the process is to import the scan data files produced by the **Computer Scan** into the current assessment.

Step 6 — Import Scans into Network Detective Pro App

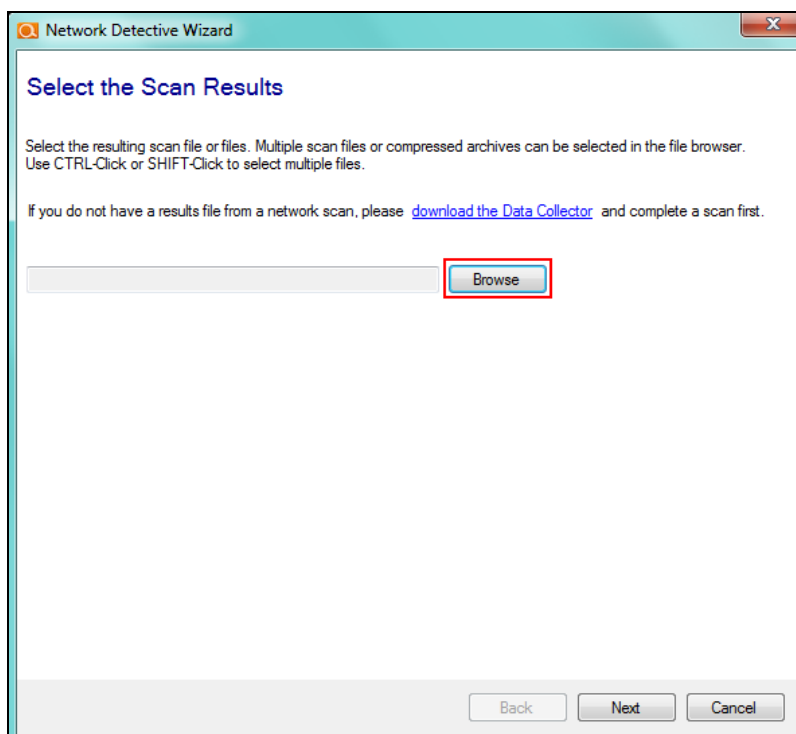
Tip: The **Push Deploy Tool** performs a localized scan on each workstation on the target network. **Perform this required step** to gather maximum data for the most detailed reports.

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

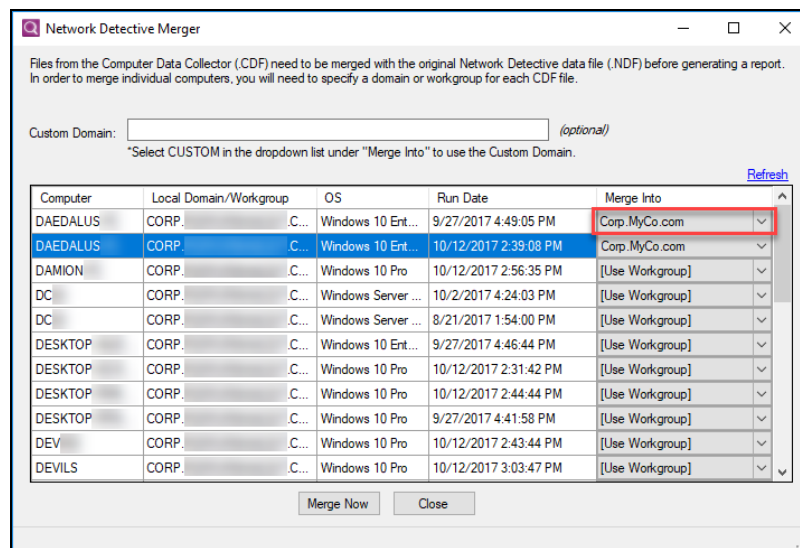
1. Click **Import Scan File** on the **Scans** bar in the Network Detective **Assessment** window.



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

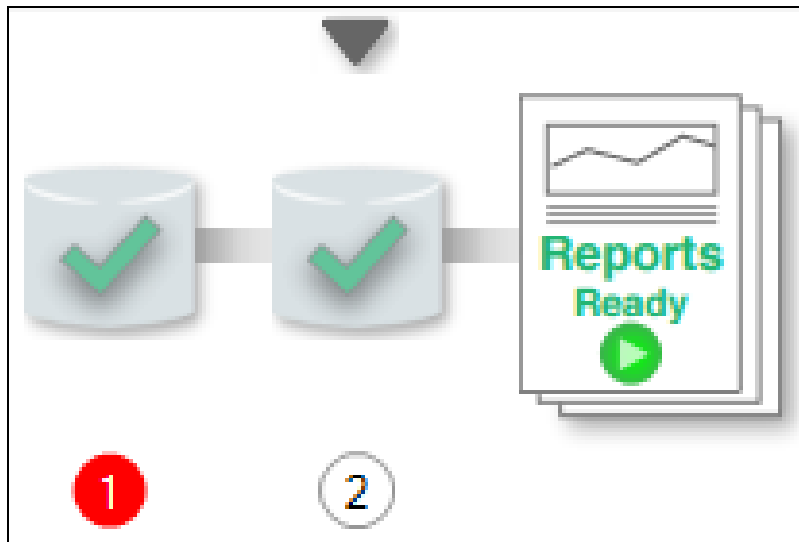


2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. Click **Open** button to import the scan data. Then click **Next**.
4. An archived copy of the scan will be created in the Network data directory. You can access this at **%APPDATA%\NetworkDetective** on your PC. Click **Finish**.
 - i. *If prompted*, use the **Network Detective Pro Merger** to merge the data file(s) into the assessment. Select the Domain into which the file will be merged. Click **Merge Now**.



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

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



Step 7 — Run Dark Web Scan (Optional)

In this step, you can optionally perform a Dark Web Scan to detect compromised credentials as part of your Network Assessment. This is a separate process from using the Dark Web Scan available in the data collector. You must subscribe to Dark Web ID to use this feature. Here's how it works:

1. Be sure you have completed a network scan and uploaded the results to Network Detective Pro.
2. Enable the Dark Web ID Integration from **Preferences > Integrations > Dark Web ID**. This first requires creating a support ticket with Kaseya support and the Dark Web ID Team to enable API access.

See also ["Set Up Full Dark Web ID Integration" on page 263](#).

Preferences

Report Defaults Reporter Email Groups Issue Overrides Integrations

Dark Web ID IT Glue Datto Unified Continuity

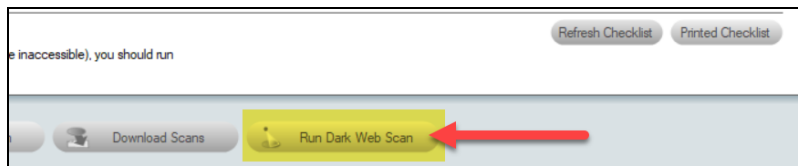
☒ Enable Dark Web ID Integration

Dark Web ID Username: @rapidfiretools.com

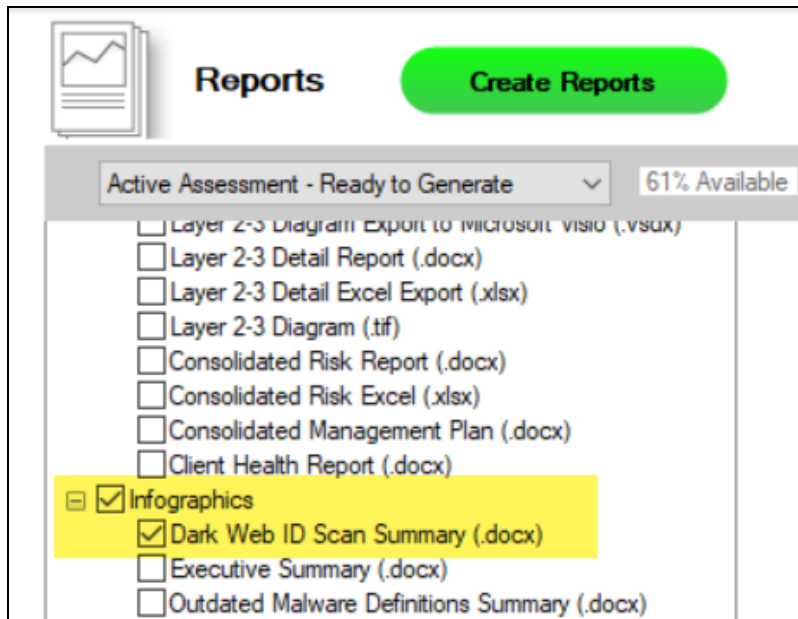
Dark Web ID Password:

Test Connection

- Click the **Run Dark Web Scan** button from the Scans bar. The scan will present a confirmation when complete.



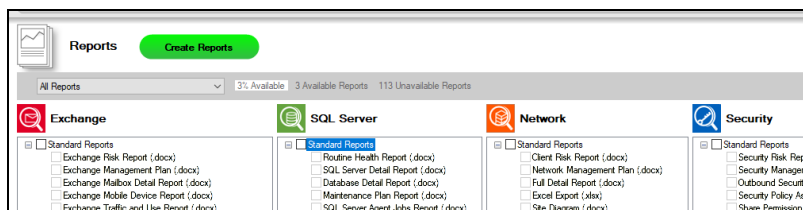
- You can then generate the **Dark Web ID Scan Summary** report.



Step 8 — Generate Network Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your Network Assessment, follow the steps below:

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



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

Network Assessment Reports

The **Network Assessment** module can 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 assets 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

Report Name	Description
	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. <i>Keep the Full Network Assessment in your hip pocket, and pull it out when your prospective new client asks how you came up with your findings!</i>
Computer Security Report Card	The Computer Security Report Card assesses individual computers at a high level based on various security criteria. The report card should be viewed as a relative measure as to how well a computer complies with security best practices. There may be specific reasons or compensating controls that may make it unnecessary to achieve an "A" in all categories to be considered secure. 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	We also give you the output of the Consolidated Risk Report and

Report Name	Description
Excel	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 assets 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 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 assets 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 assets 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.

Report Name	Description
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 computers 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 report show systems that were able to be accessed via SNMP and those that were not able to be accessed. Not all computers 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 assets discovered on the network that were accessible through Layer 2/3 discovery.
Layer 2-3 Diagram Export to Microsoft Visio	This Visio file helps you visualize all assets 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 assets 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

Report Name	Description
	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 computers, 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 assets 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 to Microsoft Visio	You have the option to export the Site Diagram to 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

Report Name	Description
	risk to the network.
Windows Service Account Report	This report details the Windows Service Accounts discovered in the target environment.

Infographics

Compliance Baseline Assessment Summary	This report provides a summary of baseline compliance for the site (requires Compliance Manager GRC subscription). The report details the current level of coverage in each rapid baselines assessment for each standard and variant, allowing readers to quickly understand where future planning is required.
Dark Web ID Summary	This visual report adds dark web monitoring to your assessment report. The presence of compromised account credentials represents a huge risk to the operations of your business. The longer a credential remains compromised, the higher the chance that sensitive information has been leaked to a threat.
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 computers 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 asset discovery.

Performing a Security Assessment

Security Assessment Overview

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

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

What You Will Need

Security Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
Security Assessment Data Collector	The Network Detective Security Assessment Data Collector (SADC) is a windows application that performs the data collections for the Security

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



Network Prerequisites for Network Detective Pro Scans

For a successful network scan:

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

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

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

Follow these steps to perform a Security Assessment.

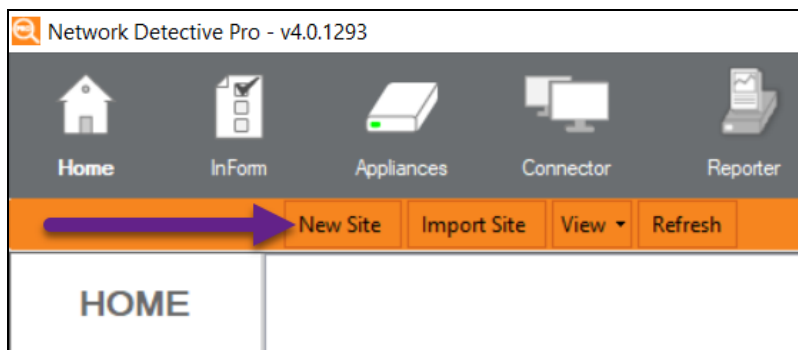
Step 1 — Download and Install the Network Detective Pro Application

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

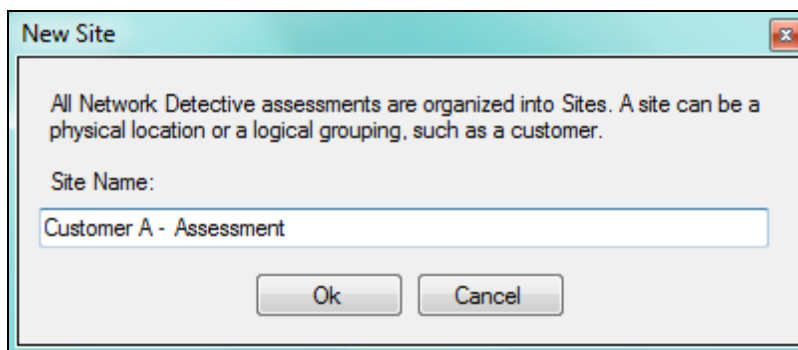
Step 2 — Create a New Site

To create a new site:

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



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

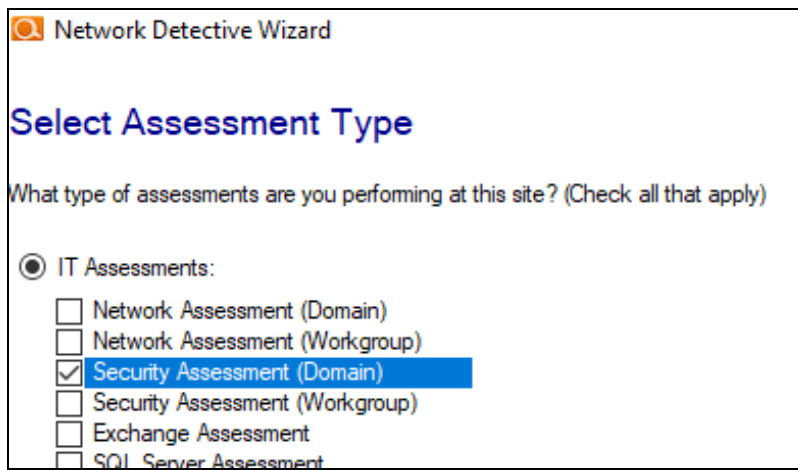


Step 3 — Start a Security Assessment

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

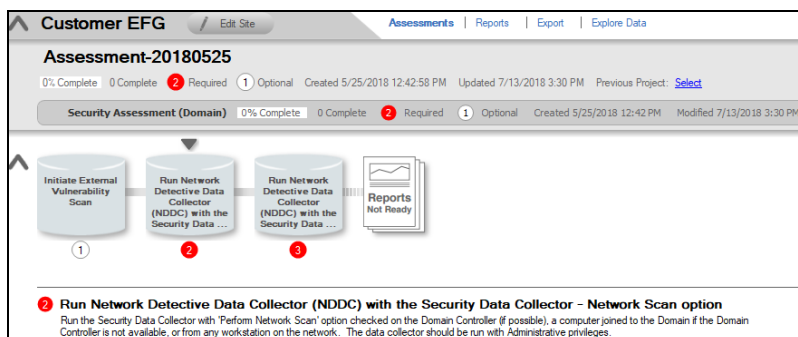


Next, select the **Security Assessment** option presented.



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

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



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

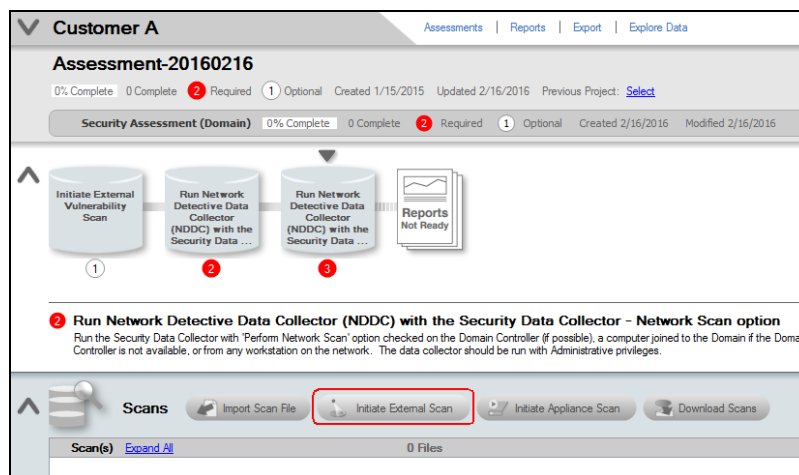
You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.



Step 4 — Initiate External Vulnerability Scan

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

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



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

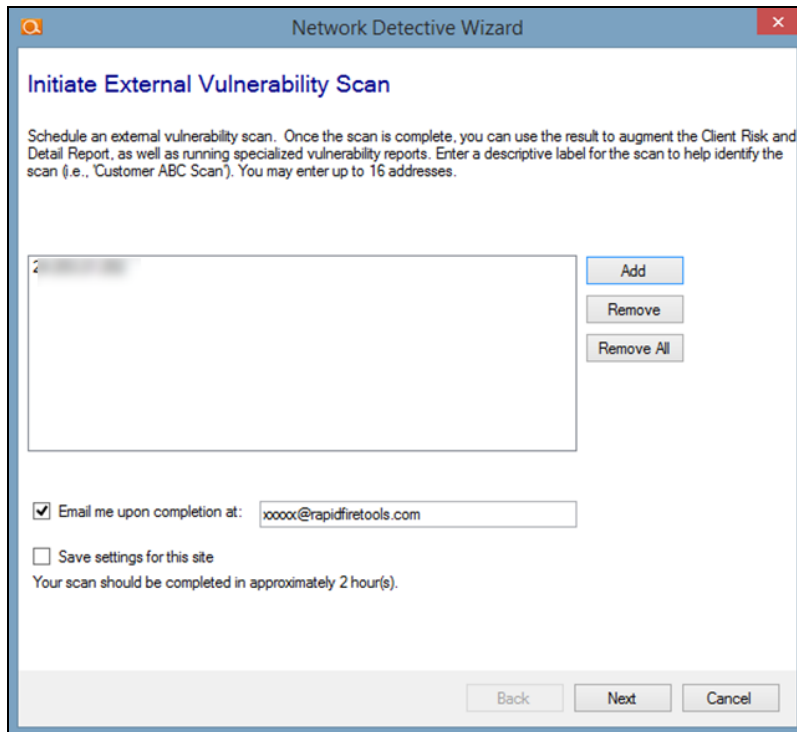
The screenshot shows a window titled "Network Detective Wizard" with a close button in the top right. The main heading is "Initiate External Vulnerability Scan". Below the heading is a paragraph of instructions: "Schedule an external vulnerability scan. Once the scan is complete, you can use the result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

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

The screenshot shows a dialog box titled "Add IP Address Range" with a close button in the top right. Inside the dialog, there is a line of text: "If only a single IP Address is wanted, leave the Ending IP Address blank." Below this text are two input fields. The first is labeled "Starting IP Address:" and the second is labeled "Ending IP Address:". Below these fields are two buttons: "Add" and "Cancel".

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

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



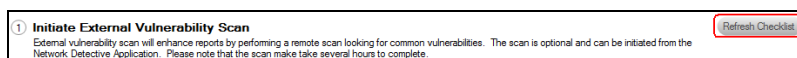
The screenshot shows a window titled "Network Detective Wizard" with a sub-header "Initiate External Vulnerability Scan". The main text explains that the scan can be used to augment reports and that up to 16 addresses can be entered. Below this is a large text input field with a small "2" in the top left corner. To the right of the field are three buttons: "Add", "Remove", and "Remove All". Below the input field, there is a checked checkbox for "Email me upon completion at:" followed by a text field containing "xxxxx@rapidfiretools.com". There is also an unchecked checkbox for "Save settings for this site". A note states "Your scan should be completed in approximately 2 hour(s)". At the bottom are "Back", "Next", and "Cancel" buttons.

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

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

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

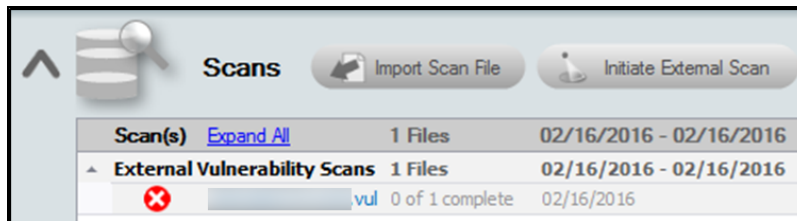
Next, select the **Refresh Checklist** option to update the status of the **External Vulnerability Scan** that is listed under the **Scans** bar.



The screenshot shows a status bar with a red circle containing a "1" next to the text "Initiate External Vulnerability Scan". Below this is a small text box explaining that the scan is optional and can be initiated from the Network Detective Application. To the right of the text box is a button labeled "Refresh Checklist".

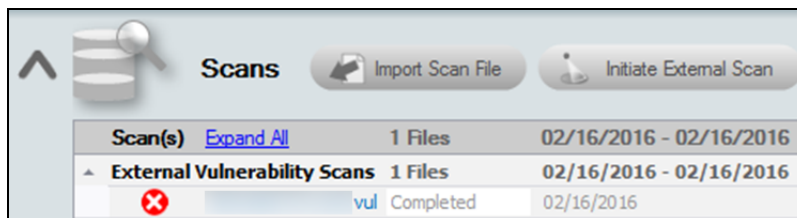
The **Assessment Window** and associated **Scans** listed under the **Scans** bar at the bottom of the **Assessment Window** will be updated to reflect the External Vulnerability Scan has been initiated and its completion is pending.

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



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

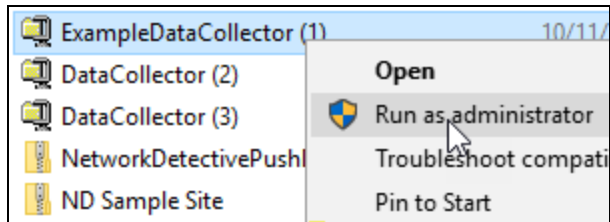
Upon the scan's completion, note that the **External Vulnerability Scan** with its **"Completed"** status will be listed as an imported scan under the **Scans** bar at the bottom of the **Assessment Window** as presented below.



Step 5 — Perform Security Scan Data Collection

Download and run the **Network Detective Pro 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/ndpro-downloads/> and download the **Network Detective Data Collector**.
2. Run the **Network Detective Data Collector** executable program as an Administrator (**right click>Run as administrator**).



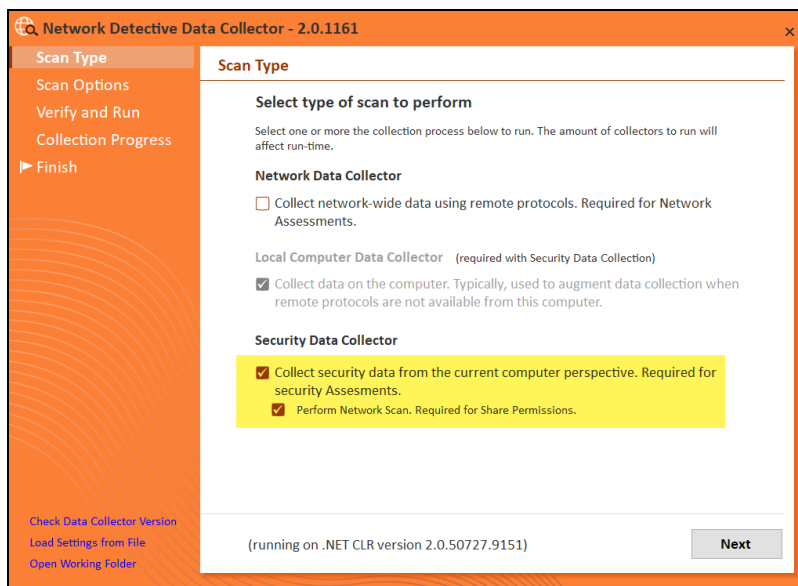
Important: For the most comprehensive scan, you **MUST** run the data collector as an **ADMINISTRATOR**.

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.

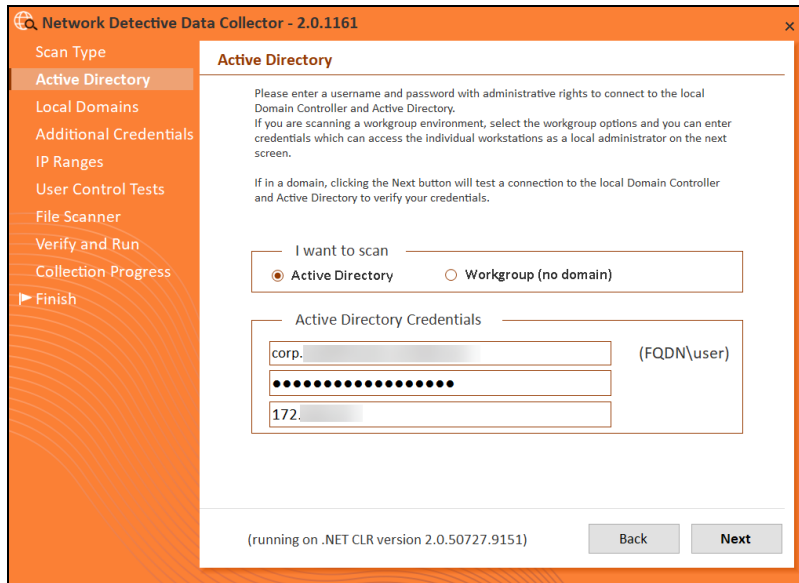
Configure the network scan using the wizard.

- Look here if you are ["Performing a Security Assessment" on page 67](#)
- Look here if you are ["Scanning a Workgroup Network" on page 83](#)

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*).



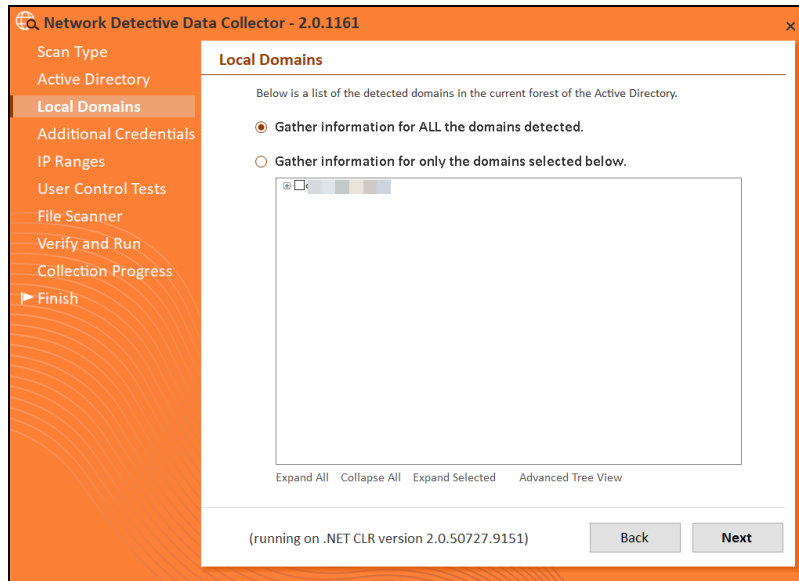
The screenshot shows the 'Network Detective Data Collector - 2.0.1161' window. On the left is a sidebar with a 'Scan Type' menu containing: Active Directory (selected), Local Domains, Additional Credentials, IP Ranges, User Control Tests, File Scanner, Verify and Run, Collection Progress, and Finish. The main area is titled 'Active Directory' and contains the following text: 'Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. If you are scanning a workgroup environment, select the workgroup options and you can enter credentials which can access the individual workstations as a local administrator on the next screen. If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.'

Below the text is a section 'I want to scan' with two radio buttons: 'Active Directory' (selected) and 'Workgroup (no domain)'. Below that is a section 'Active Directory Credentials' with three input fields: a domain field containing 'corp.' with '(FQDN\user)' to its right, a password field with masked characters, and an IP address field containing '172.'. At the bottom, it says '(running on .NET CLR version 2.0.50727.9151)' and has 'Back' and 'Next' buttons.

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.

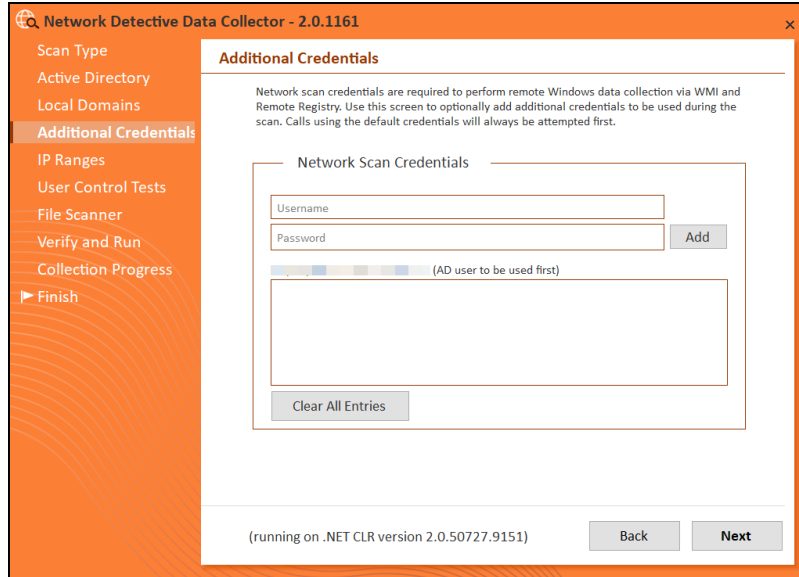
Note: For example: **corp.yourprospect.com\username**.

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**.



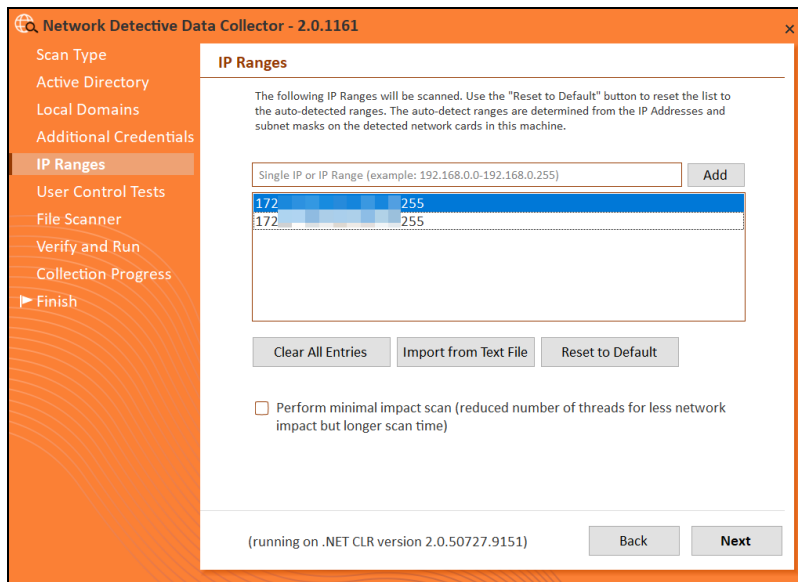
Confirm your selections if you opt to scan only specific Domains and OUs. Click **OK**.

- 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**.



- The **IP Ranges** screen will then appear. The Network Detective Data Collector will automatically suggest an IP Range for the scan. If you do not wish to scan the

default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

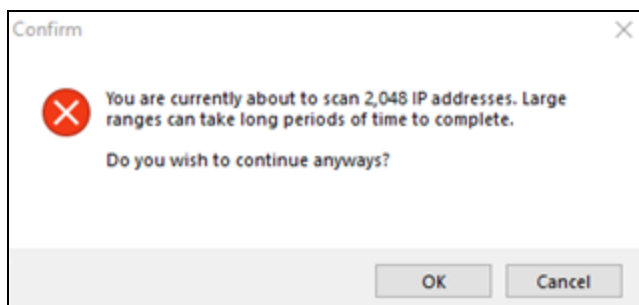


From this screen you can also:

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

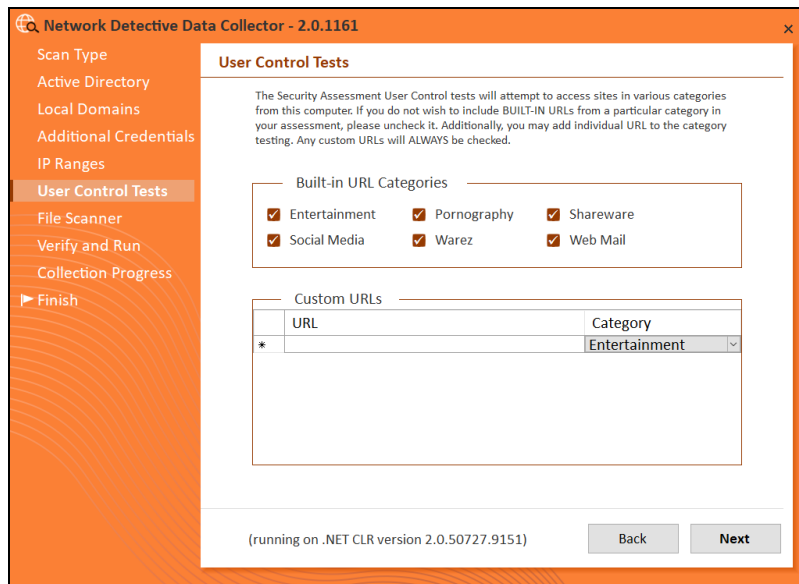
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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

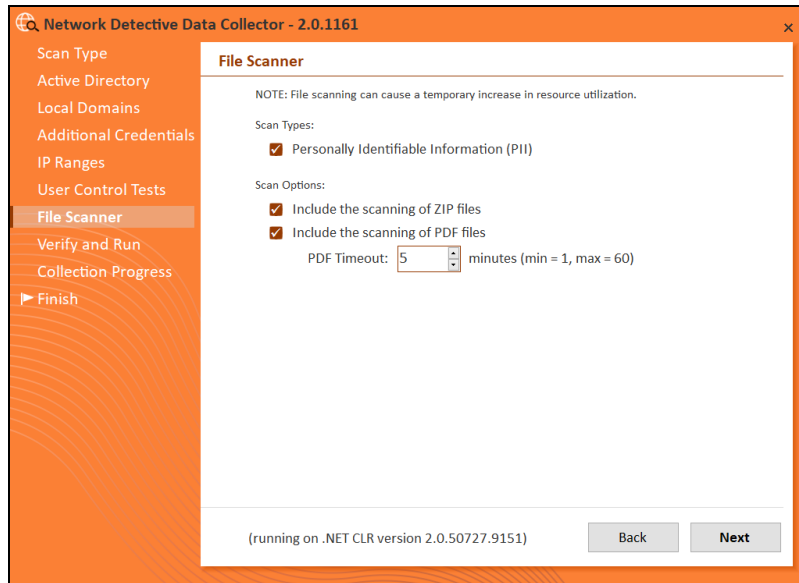


Important: If you are scanning a large number of IP addresses, confirm that you wish to continue.

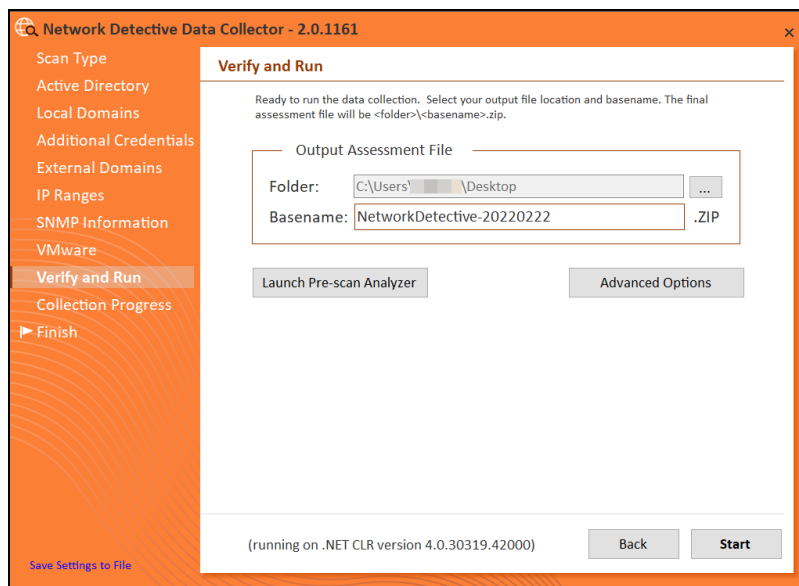
8. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your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



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



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



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

Overview Result Summary Active Directory SQL Server Network Computers **Push Deploy**

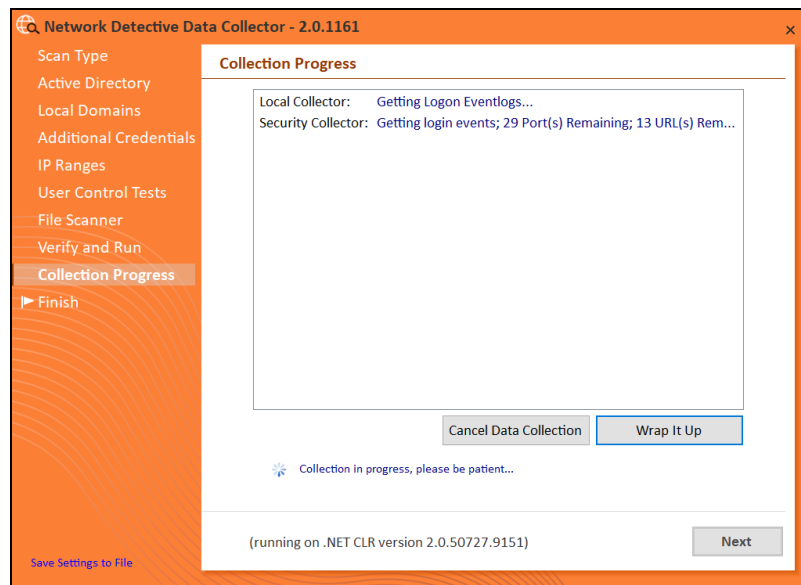
Pushing local data collectors to remote computers requires WMI, Admin\$ access, and .NET 3.5 or above.

Showing: All Nodes

Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01-CORPRAPIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORPRAPI...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-99SDFE1.CORP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HN0E7L.CORP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4080.CORP...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORP...	10.236.83.1...	?	?			Accessing WMI...
DESKTOP-7RF9K75.CORP...		✓	✗			WMI failed. The RPC server is unavailable.

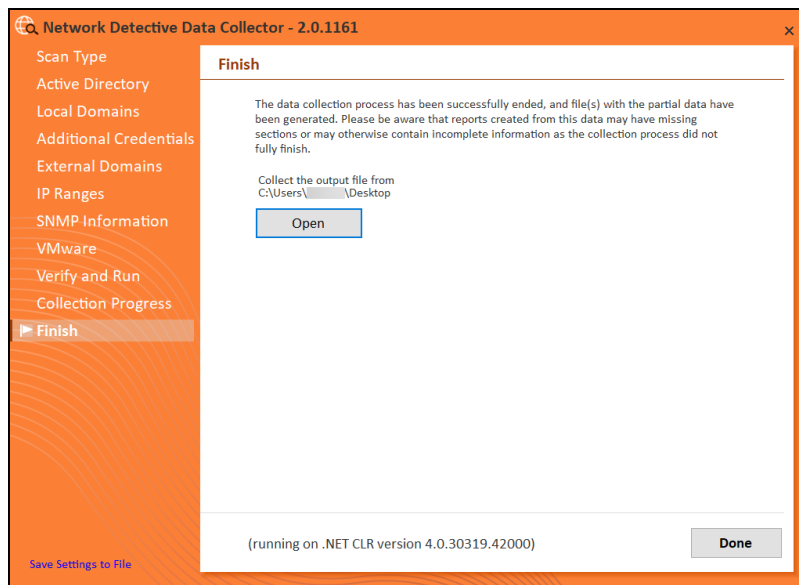
Enter any **Comments** and then click **Start**.

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



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

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



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

Scanning a Workgroup Network

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

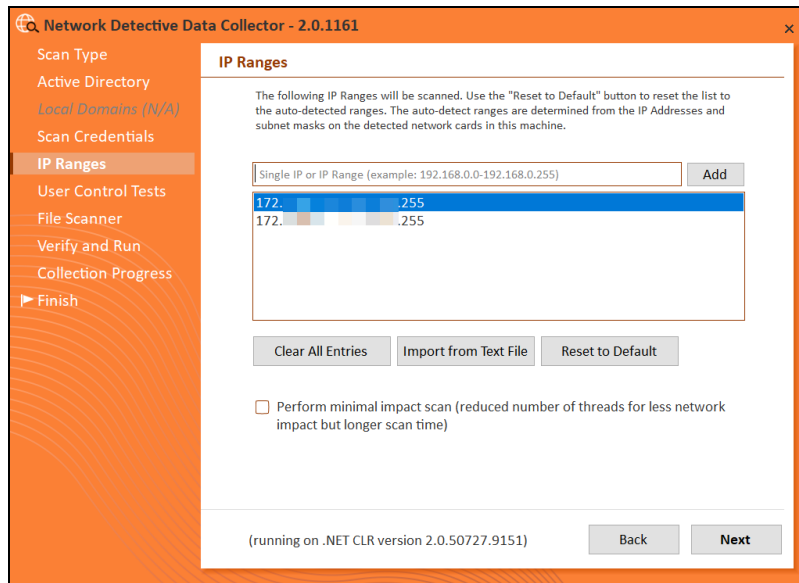
The screenshot shows the 'Active Directory' configuration window. On the left is a sidebar with navigation links: Scan Type, Active Directory (selected), Local Domains (N/A), Scan Credentials, IP Ranges, User Control Tests, File Scanner, Verify and Run, Collection Progress, and Finish. The main area has a title 'Active Directory' and instructions: 'Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. If you are scanning a workgroup environment, select the workgroup options and you can enter credentials which can access the individual workstations as a local administrator on the next screen. If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.' Below the instructions are two radio buttons: 'Active Directory' and 'Workgroup (no domain)', with the latter selected. Under 'Active Directory Credentials', there are three input fields: a domain field containing 'corp.', a password field with masked characters, and an IP field containing '172'. To the right of the password field is the label '(FQDN\user)'. At the bottom, it says '(running on .NET CLR version 2.0.50727.9151)' and has 'Back' and 'Next' buttons.

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.

The screenshot shows the 'Scan Credentials' configuration window. The sidebar is the same as the previous screen, with 'Scan Credentials' now selected. The main area has a title 'Scan Credentials' and instructions: 'Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan.' Below the instructions is a section titled 'Network Scan Credentials' containing a 'Username' field, a 'Password' field, and an 'Add' button. Below these is a list box showing a single entry with a masked icon and '.com'. At the bottom of this section is a 'Clear All Entries' button. At the very bottom of the window, it says '(running on .NET CLR version 2.0.50727.9151)' and has 'Back' and 'Next' buttons.

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**.

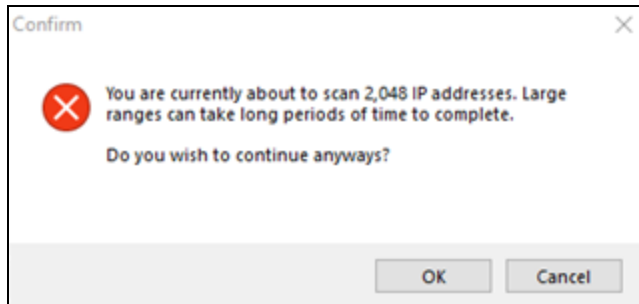


From this screen you can also:

- 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.

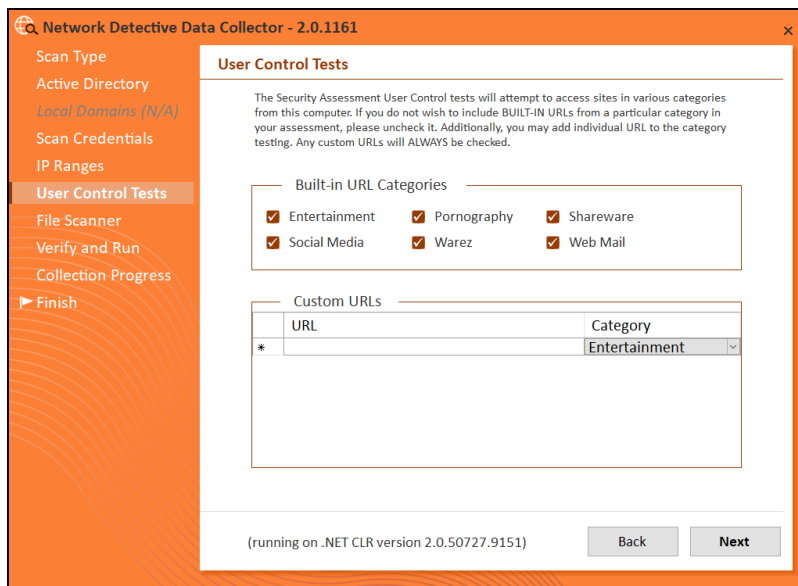
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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

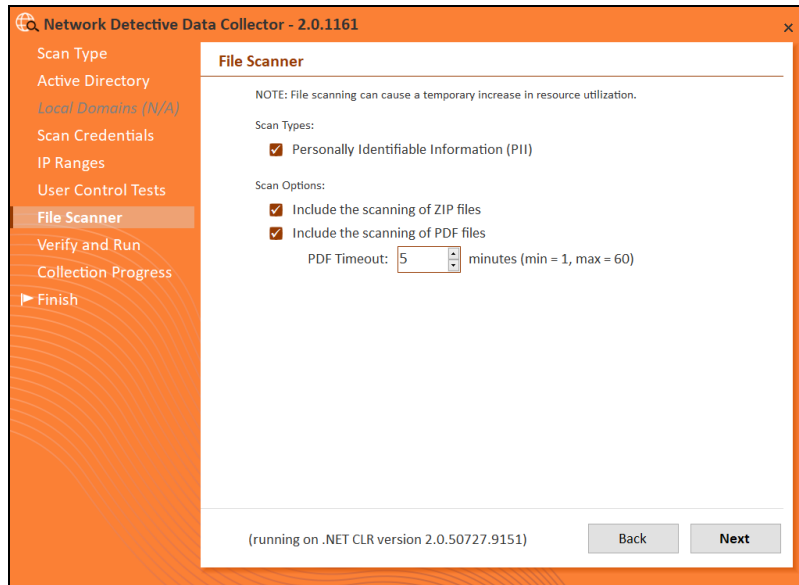


Important: If you are scanning a large number of IP addresses, confirm that you wish to continue. Consider performing multiple scans on smaller IP ranges. You can then upload each "batch" of scan files into the assessment, where they will be merged for complete results.

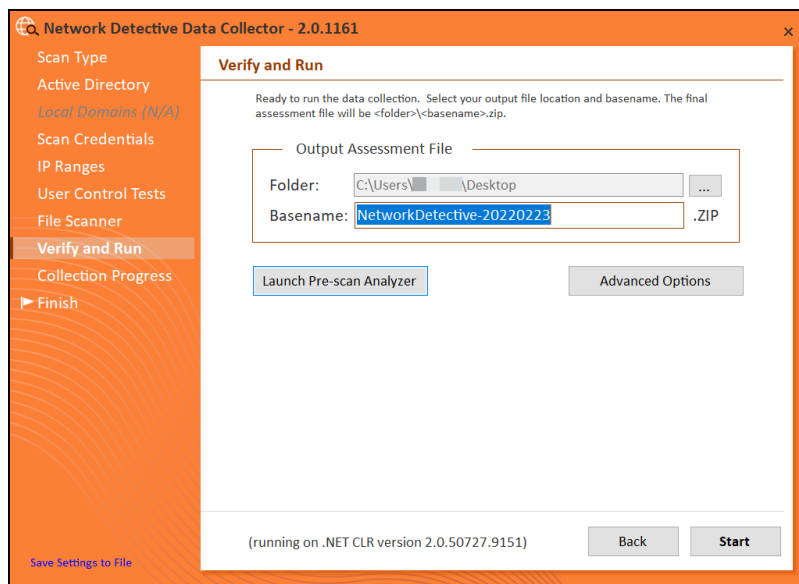
4. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your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

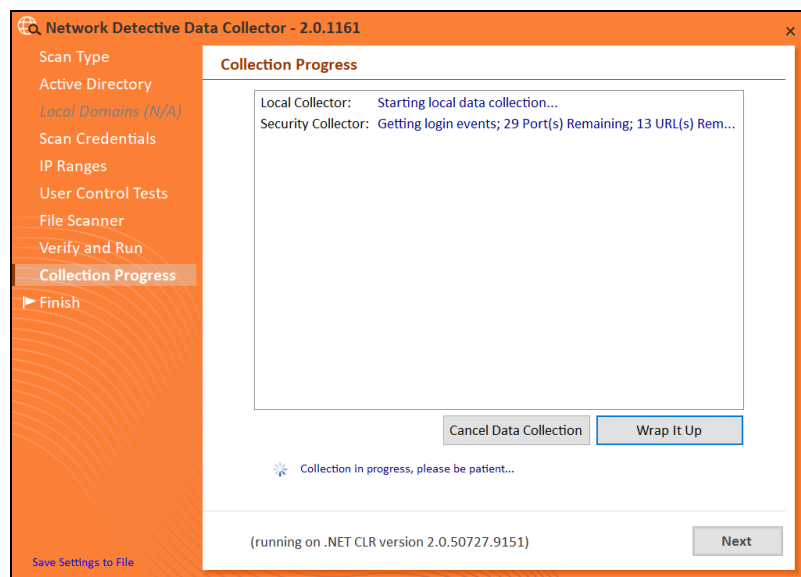


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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

Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01-CORPRAPIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORPRAPI...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-09S0F1.CORPRA...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HN0E71.CORPRA...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4080.CORPRA...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORPRA...	10.236.83.1...	✓	?			Accessing WMI...
DESKTOP-7RF9K75.CORPRA...		✓	✗			WMI failed. The RPC server is unavailable.

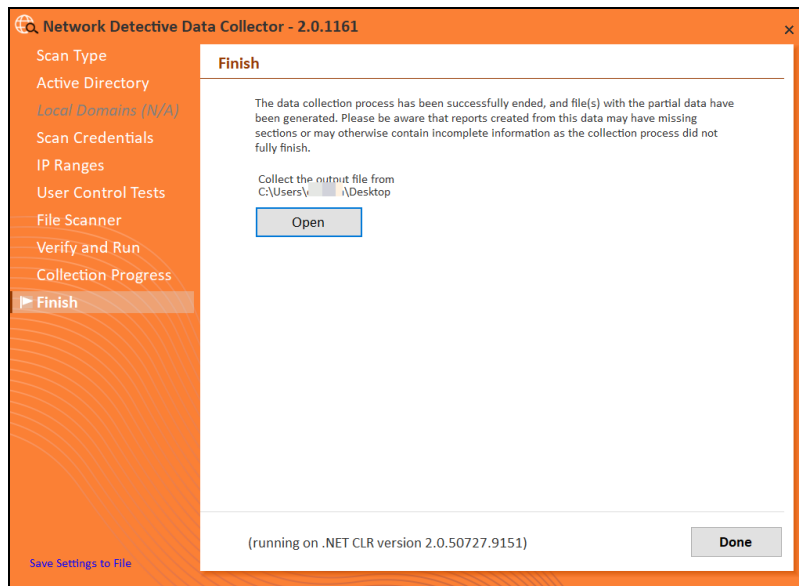
Enter any **Comments** and then click **Start**.

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



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

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



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

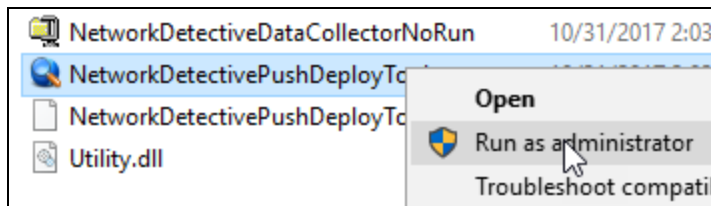
Step 6 — Use the Push Deploy Tool to Collect Remaining Data

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

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

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

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



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

The Push Deploy Tool Settings and Configuration window will appear.

4. Set the **Storage Folder location** and select the **Security Scan** option.

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

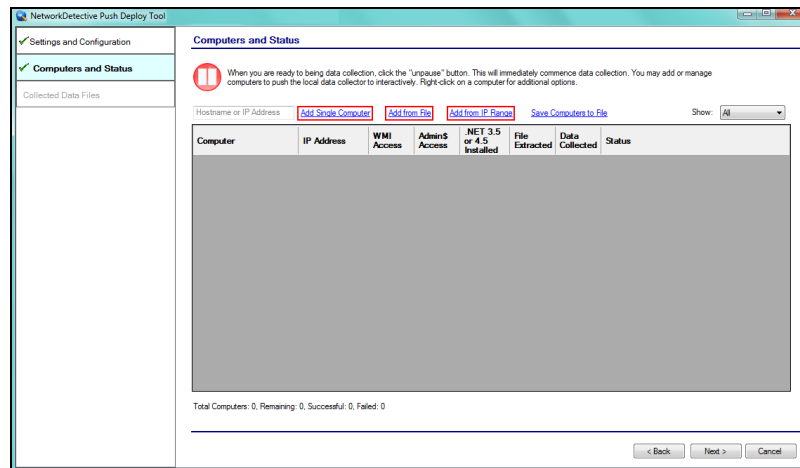
If additional credentials are required, type in the administrator level **Username** and **Password** necessary to access the local computers on the network to be scanned. Then click **Add**.

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

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

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

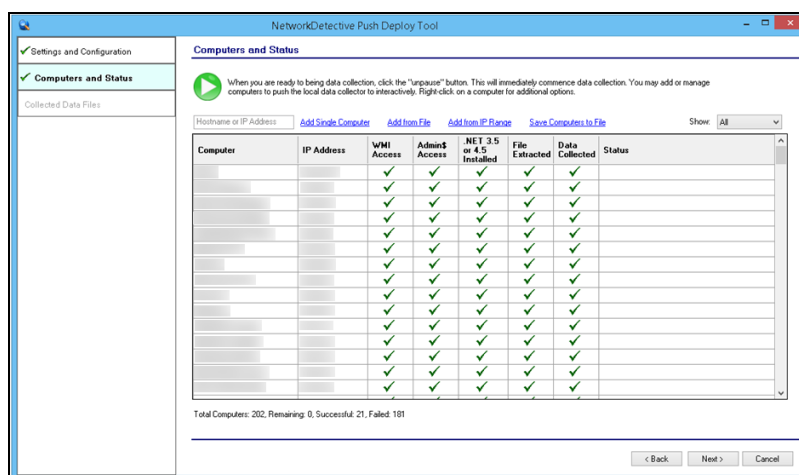
scanned again in future assessments



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

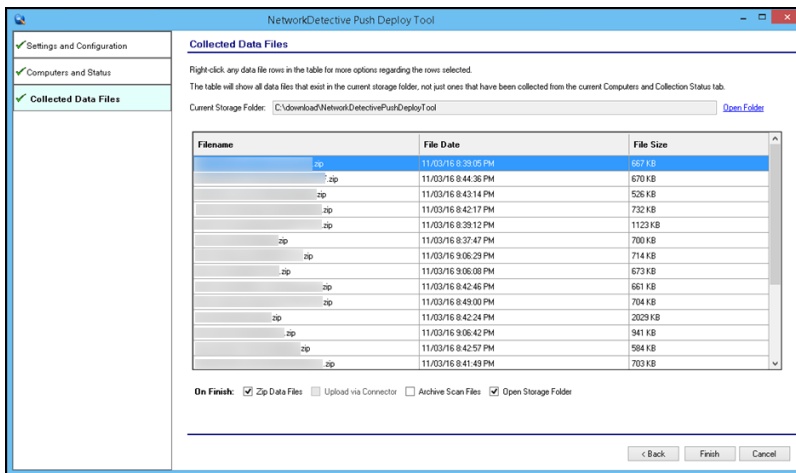
After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the **Computers and Status** window.

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



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

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



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

MORE INFO:

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

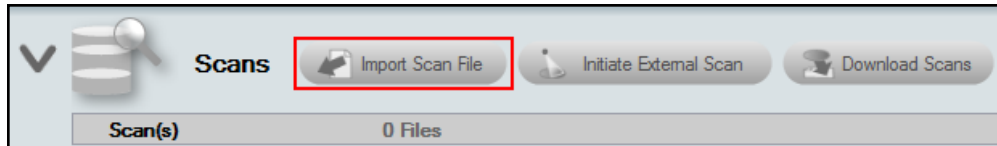
The output files (.ZIP, files) from the local scans can be stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.

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

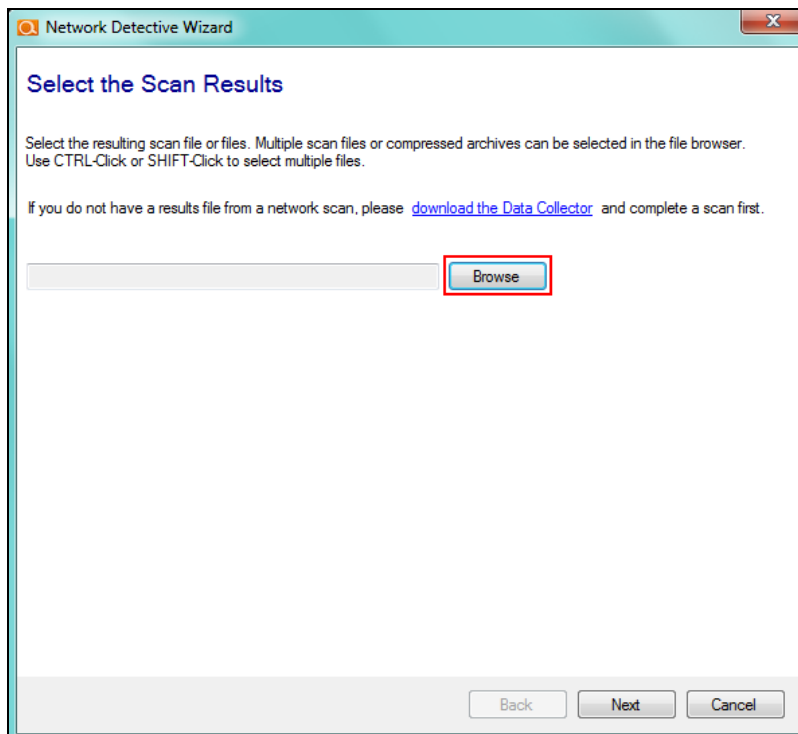
Step 7 — Import Scans into Network Detective Pro App

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

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

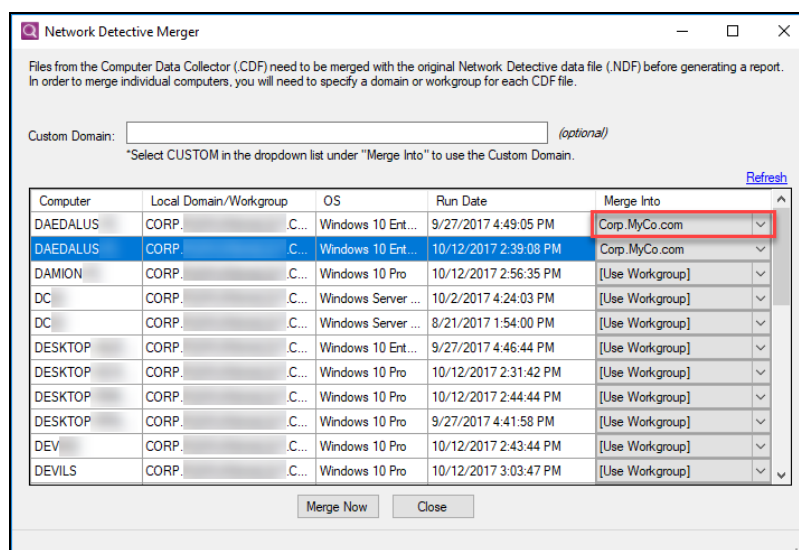


The **Select the Scan Results** window will be displayed.



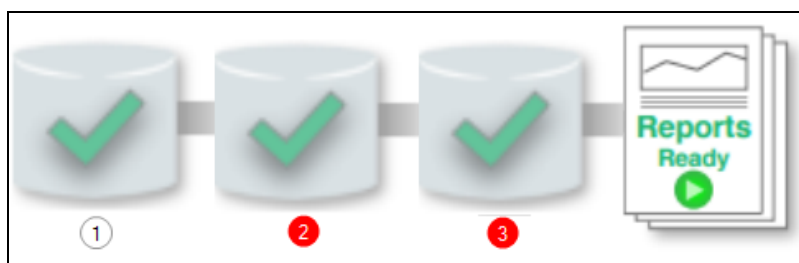
2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. For a Security Scan, these will be:

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



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

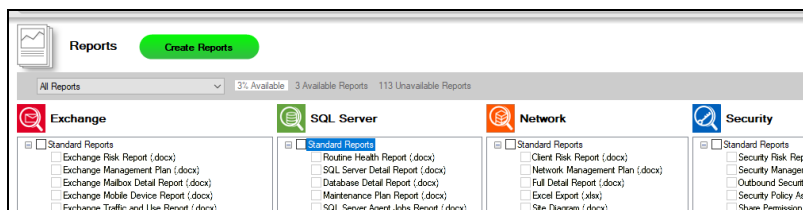
Once all of the scan data is imported into the **Assessment**, the assessment's **Checklist** will indicate that the **Reports** are ready to be generated.



Step 8 — Generate Security Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your Security Assessment, follow the steps below:

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



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

Security Assessment Reports

The **Security Assessment** module can generate the following reports:

Standard Reports

Report Name	Description
Anomalous Login Report	The Anomalous Login Report shows suspicious logins by user and computer based on various probability criteria. The includes: A) logins into specific computers users don't normally log into, and B) logins by users outside of their regular pattern (not only by day of week, but also by time of day).
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

Report Name	Description
	for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F'). The report card should be viewed as a relative measure as to how well a computer complies with security best practices. There may be specific reasons or compensating controls that may make it unnecessary to achieve an "A" in all categories to be considered secure.
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 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	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,

Report Name	Description
Report	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 assets, as well as several graphical breakdowns of the numerical disposition of issues on the target network. (*Requires Inspector)
Internal Vulnerability Scan Detail Excel*	Internal vulnerability breakdown in MS Excel format.
Internal Vulnerability Scan Detail Report*	This detailed report provides extensive data on each discovered internal vulnerability organized by each affected asset. This includes insight into the technical nature of each issue, a proposed solution, as well as several graphical breakdowns of the numerical disposition of issues on the target network. (*Requires Inspector)
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

Report Name	Description
	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 computers in the environment and helps point out commonalities in the sets and which users/computer combinations have the configurations applied. There are separate reports for both user settings and computer settings.
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 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

Report Name	Description
	security, along with a summary of the number of computers with issues. This powerful lead generation and sales development tool also reports on outbound protocols, System Control protocols, User Access Controls, as well as an external vulnerabilities summary list.
Share Permission Report	Comprehensive lists of all network “shares” by computer, detailing which users and groups have access to which devices and files, and what level of 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 computer 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 (computers) which they should not be.
User Permissions Report	Organizes permissions by user, showing all shared computers and files to which they have access.

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.

Report Name	Description
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.
Vulnerability Scan Assessment Summary	This report provides an assessment of internal and external vulnerabilities (requires VulScan subscription). The report details the highest severity vulnerabilities, allowing 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 Report	This report details the Risk Score for both the current and previous assessment, focusing in particular on security issues and vulnerabilities. At the same time, the report breaks down each issue and conveys whether the issue is increasing or decreasing in risk level. For example, are your computers missing more or fewer security patches since the previous assessment? This report will tell you.
Login Failures by Computer	Compares the results of the current and previous login failures report by computer.

Report Name	Description
Change Report	
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.

Performing a Microsoft Cloud Assessment

Microsoft Cloud Assessment Overview

Network Detective's **Microsoft Cloud Assessment Module** combines 1) automated data collection with 2) a structured framework for documenting your assessment. To perform a Microsoft Cloud Assessment, you will:

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

What Does the Microsoft Cloud Assessment Cover?

This module helps you manage and assess risk across your entire Microsoft Cloud Assessment deployment. It assesses and documents several components, including:

- Microsoft 365 Cloud Services
 - Office 365
 - Teams
 - SharePoint
 - OneDrive (does not scan file content)
 - Outlook/Exchange (does not scan email content)
- Microsoft Azure Cloud Services
 - Azure Active Directory
 - Azure Infrastructure Data Collection (applications, virtual machines, services)

What Does the Microsoft Cloud Assessment Do?

As the computing world steadily moves more resources into the Cloud, it's getting increasingly difficult for MSPs and other IT professionals to manage assets and configurations that are no longer physically present . . . and that they don't have complete

control over. By periodically running a full assessment on each Microsoft Cloud environment, MSPs can provide themselves, and their clients, with essential reports that will help control the flow, privacy, and security of the organization's data.

Having all this information, organized and at your fingertips, is essential for:

- A new technician who's trying to get a handle on the Microsoft Cloud environment
- A Cloud administrator who is trying to hunt down a misconfiguration that's causing problems
- An MSP who needs to scope a proposal for a prospective new client
- Curbing the sprawl and potential HR headaches of Teams, SharePoint, and OneDrive

What You Will Need

In order to perform a Microsoft Cloud Assessment, you will need the following components:

Note: You can access these at <https://www.rapidfiretools.com/ndpro-downloads/>.

Microsoft Cloud Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
Azure Environment Credentials (Enterprise Application method)	To assess the Microsoft 365 and Azure Active Directory environment at the same time, you must set up API permissions in the Azure portal. See "Prerequisites to Perform Cloud Scan using Enterprise App" on page 118 for a detailed walkthrough. This will allow you to gather the necessary credentials to perform the scan using the Enterprise Application collection method.
Admin Credentials for Microsoft 365 tenant to be assessed (OAUTH method)	You must have admin credentials for an admin role user who is a member of the Microsoft 365 tenant to be assessed. You will use these credentials to grant permission for Network Detective to connect to the Microsoft Graphs API. The following roles have been verified to work to create this connection: • Privileged role admin (Recommended) • Cloud application admin (Recommended) (Using one these roles will only grant permissions to the individual users who enter their credentials to perform the scan.) • Global admin (Using the Global admin role will grant scanning permissions to all non-admin users in the Microsoft 365 tenant who have access to the Site in Network Detective.) If you attempt to sign in with another type of admin role than those listed above, you will be unable to grant the necessary permissions.

Microsoft Cloud Assessment Component	Description
	See Assign Admin Roles in the Microsoft 365 documentation for more details.

Follow these steps to perform a Microsoft Cloud Assessment:

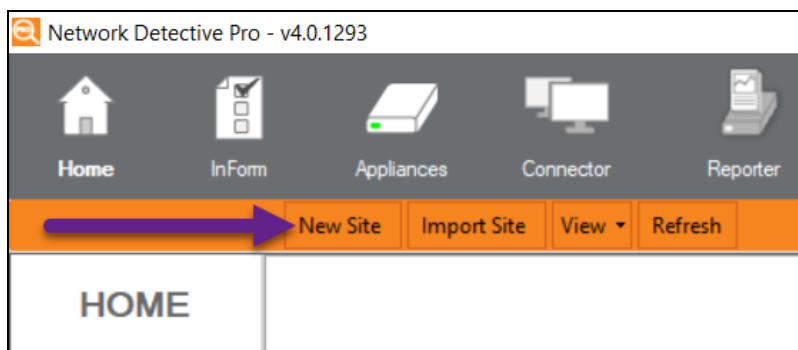
Step 1 — Download and Install the Network Detective Pro Application

1. Visit <https://www.rapidfiretools.com/ndpro-downloads/>. Download and install the Network Detective Pro Application.
2. Open the app and log in using your credentials.

Step 2 — Create a New Site

To create a new site:

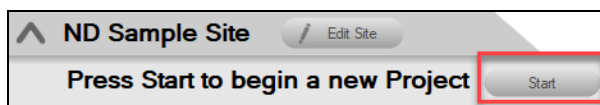
1. Click **New Site** to create a new Site for your assessment project.



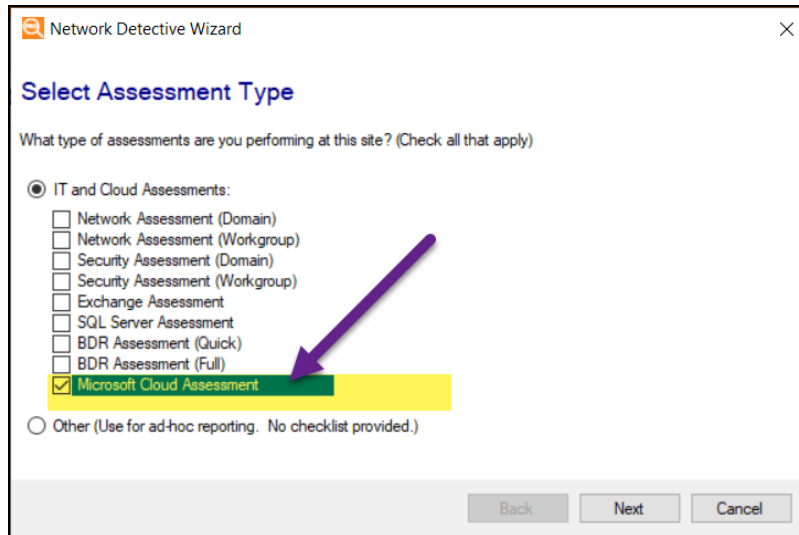
2. Enter a **Site Name** and click **OK**.

Step 3 — Start a Microsoft Cloud Assessment Project

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



2. Next, select **IT and Cloud Assessments**, and then select Microsoft Cloud Assessment.



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

Use the Microsoft Cloud Assessment Checklist

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



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

When you complete a step, that item will be updated with a green check mark  in the checklist. Different assessment types have a different number of steps to complete.



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



Step 4 — Run the Cloud Data Collector

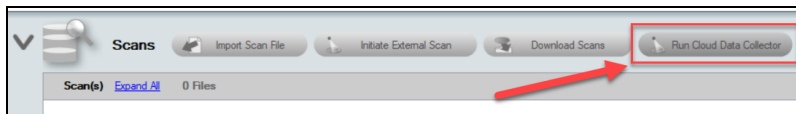
You can collect Microsoft Cloud Data in two different ways:

- ["Perform Scan Using Enterprise App" below](#): Allows you to collect data from both the MS Cloud and Azure environments using an Enterprise Application that you install via the MS Azure Portal.
- ["Perform Scan Using OAUTH Credentials" on the facing page](#): Allows you to collect data from the MS Cloud (Office 365, Teams, and so on) only and **DOES NOT INCLUDE** Azure Infrastructure data. This method requires only Office 365 credentials with the proper admin permissions.

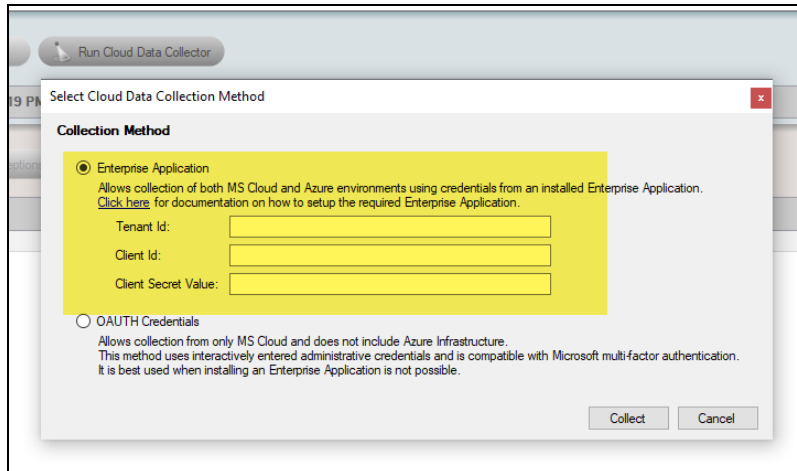
Perform Scan Using Enterprise App

Note: Before you can perform the cloud scan using this method, be sure you have set up the ["Prerequisites to Perform Cloud Scan using Enterprise App" on page 118](#).

1. To start your assessment, click **Run Cloud Data Collector** under Scans.



2. Select the **Enterprise Application** collection method. Enter the required values into the correct fields and click **Collect**. Refer to the table below for tips on finding the relevant credentials in the Microsoft Azure management portal.

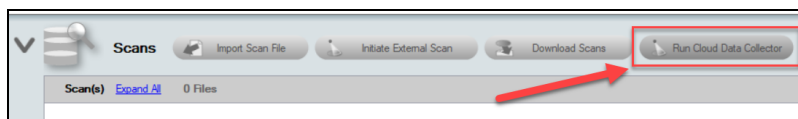


Credential	Where to find
Tenant ID	Services > Azure AD > Enterprise Apps > Your App > Overview
Client ID	Services > Azure AD > Enterprise Apps > Your App > Overview
Client Secret Value	Services > Azure AD > Enterprise Apps > Your App > Certificates & Secrets

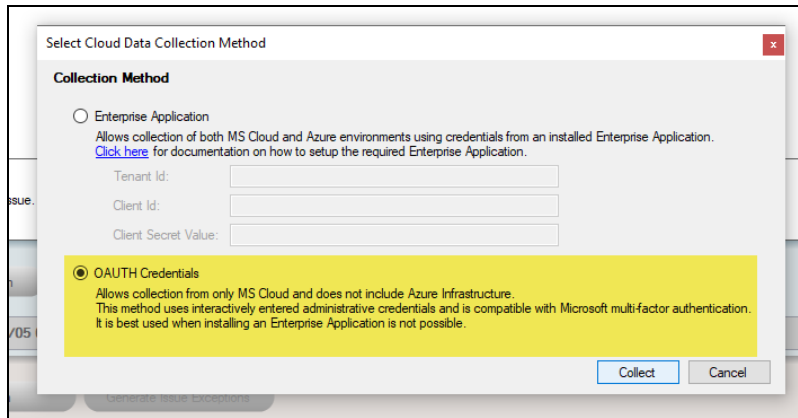
Perform Scan Using OAUTH Credentials

Note: Before you can Run the Cloud Data Collector, you need admin credentials for the Microsoft 365 tenant to be assessed.

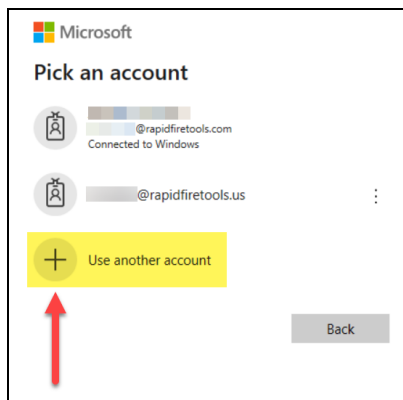
1. To start your assessment, click **Run Cloud Data Collector** under Scans.



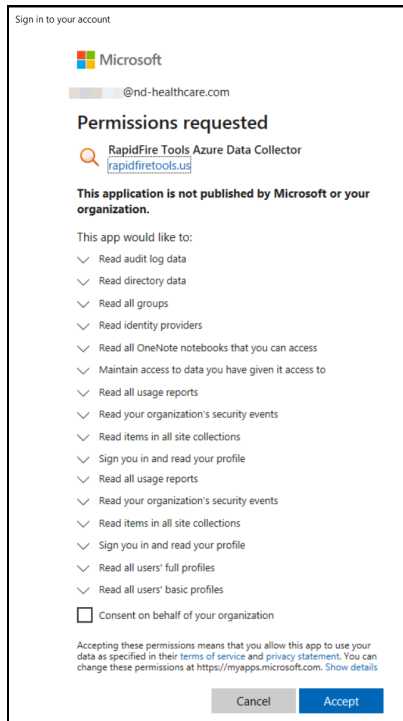
2. Select **OAUTH Credentials** and click **Collect**.



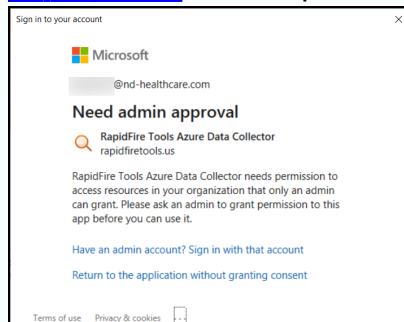
3. A Microsoft login window will appear. Enter admin credentials for the Microsoft Cloud environment to be assessed. To do this, click **Use Another Account**.



4. Consent to the permissions needed for Network Detective to scan the Microsoft Cloud environment. Check the box and click **Accept**.

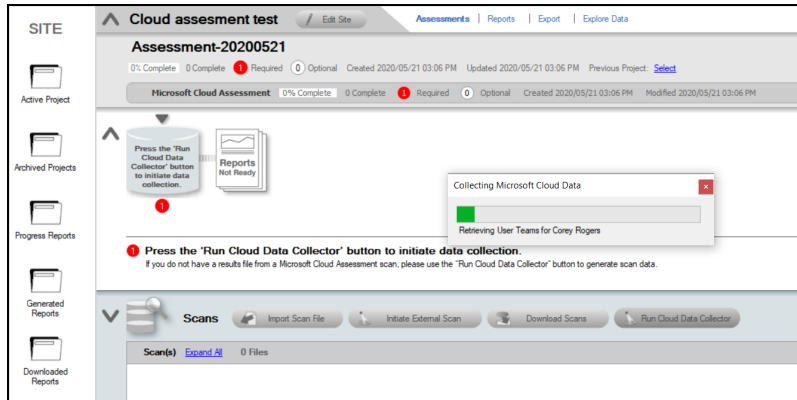


Note: If you attempt to sign in with an account that does not have the required admin access, you will be prompted to sign in with an admin account. See ["Admin Credentials for Microsoft 365 tenant to be assessed \(OAUTH method\)" on page 105](#) for the specific admin roles.

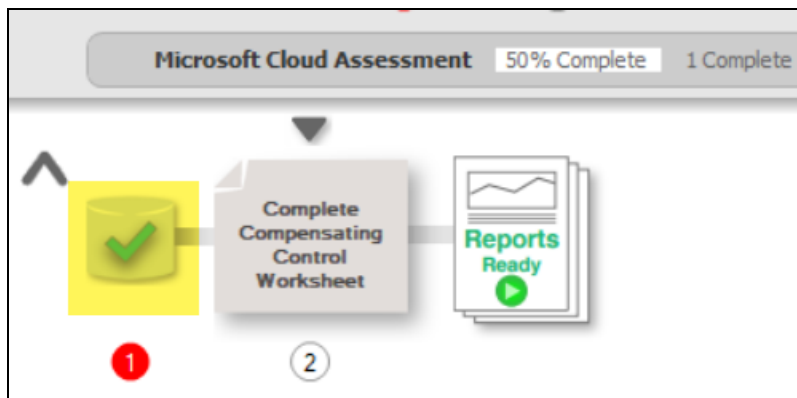


Scan in Progress

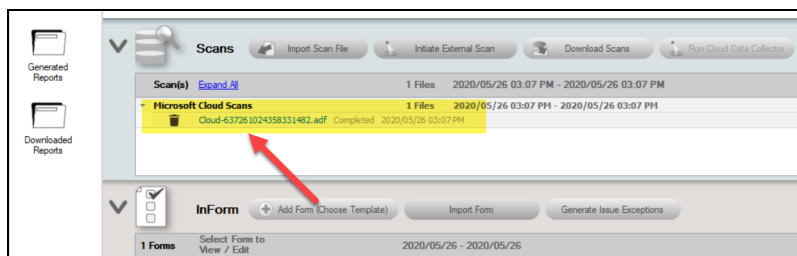
Once you initiate the scan using either method detailed above, the scan will begin and a progress window will appear. This process may take several minutes.



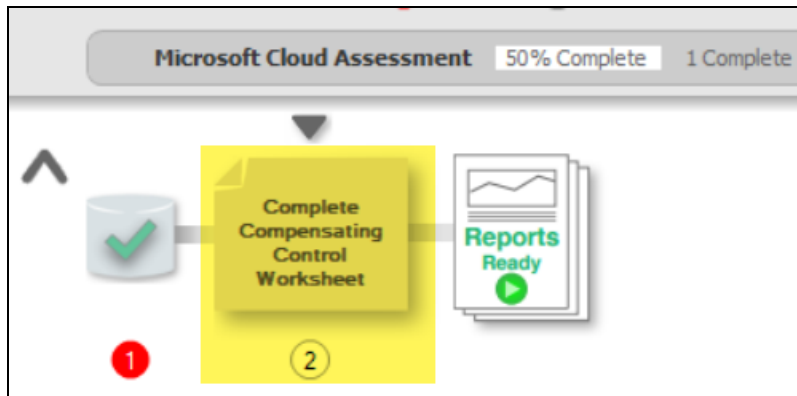
When the scan completes, the "Run Cloud Data Collector" step will be marked complete in the Checklist.



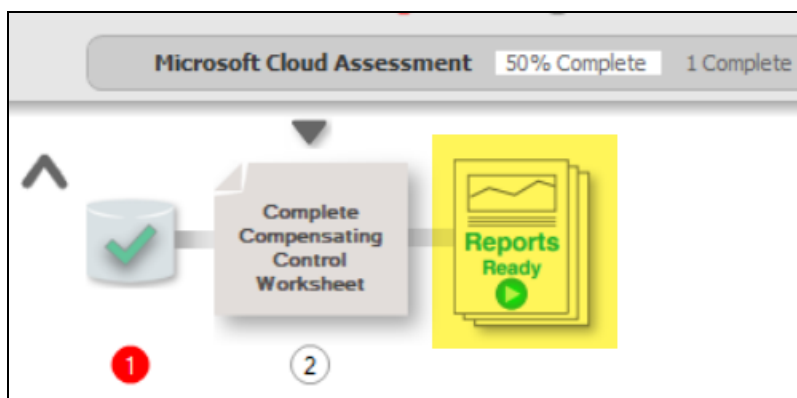
At the same time, the data file will appear in the Scans menu under Microsoft Cloud Scans.



The optional **Compensating Controls Worksheet** will then become available to complete.



Finally, you can choose to generate reports based on the current scan data without choosing to enter information on Compensating Controls.



Step 5 — (Optional) Document Compensating Controls

Next, complete the optional **Compensating Controls Worksheet** (CCW). While not necessary to generate reports, the CCW details security exceptions that will be (or have been) implemented to mitigate risks in the cloud environment. Here you can document and explain why various discovered items are not true issues and possible false positives.

1. Double click on the **Compensating Controls Worksheet** from the assessment checklist.

MS Cloud Compensating Control Worksheet

0 Required Remaining

Filter Topics

Bulk Entry Actions Save Close

Expand All | Collapse All

1 User Risk Policy Not Enabled

1.1 User Risk Policy Not Enabled

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Valid

2 Sign in Risk Policy Not Enabled

2.1 Sign in Risk Policy Not Enabled

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Valid

3 Self Service Password Reset Not Enabled

3.1 Self Service Password Reset Not Enabled

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

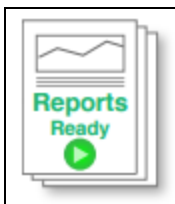
Valid

2. Ensure you save your changes to the form before you close it.
3. You may add notes, respondent names, SWOT details, responses, and file attachments.

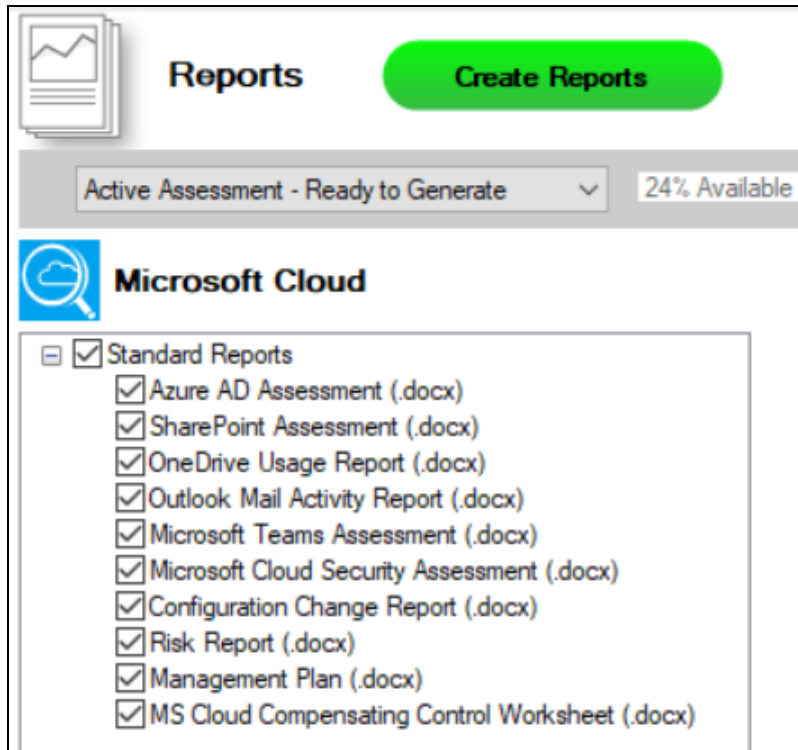
When you complete all of the fields, this step will appear as complete in the check list.

Step 6 — Generate Reports

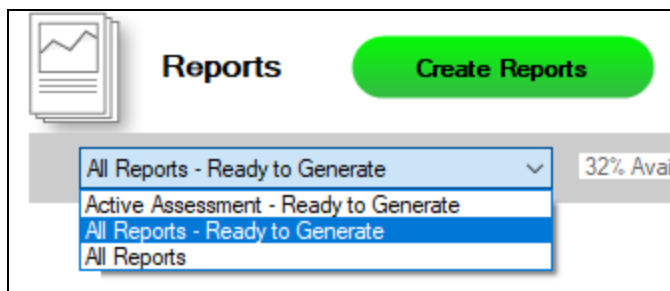
1. From your site, click the **Reports Ready** button at the end of the assessment checklist.



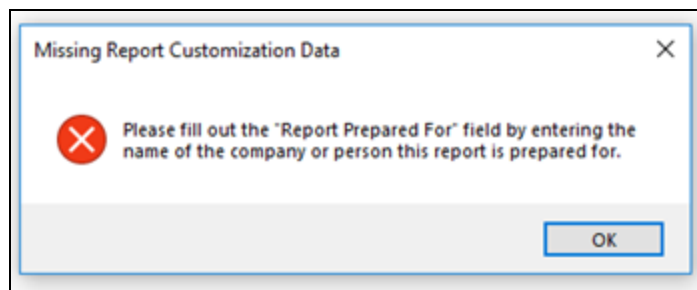
2. Select which of the Microsoft Cloud Assessment reports that you want to generate.



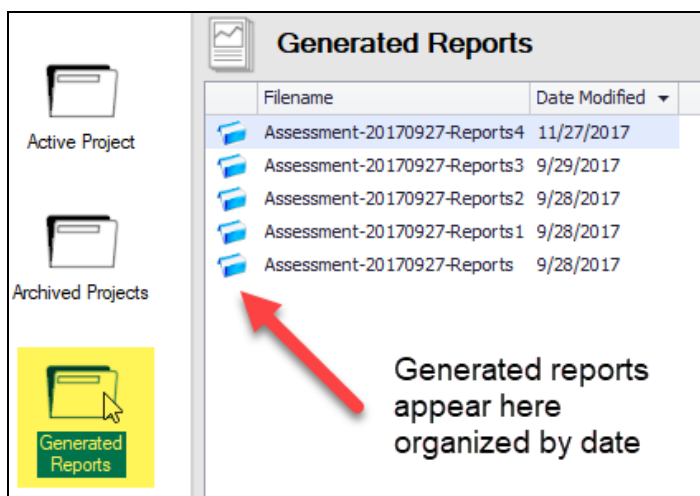
You can use the Reports drop-down menu to filter reports related to the active assessment project, reports that are ready to generate, or to browse all available reports.



3. 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.



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.



Prerequisites to Perform Cloud Scan using Enterprise App

The Cloud Scan – for both Network Detective Pro and Compliance Manager GRC – allows you to collect data from any Azure Active Directory environment. This includes Azure domains, virtual machines, and cloud services.

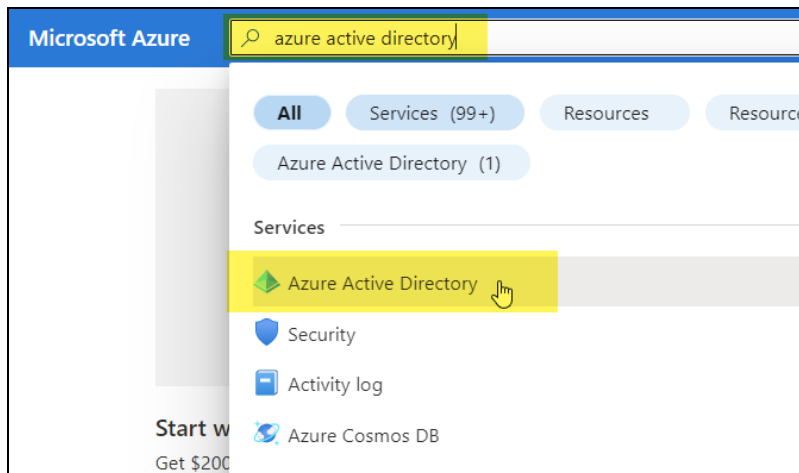
Before you can initiate the Cloud Scan, you must first set up an **Enterprise App** in the Microsoft Azure tenant to be assessed. The Enterprise App provides the credentials and permissions necessary to perform the scan. You may need to enlist the help of an on-site IT administrator to assist you.

Follow these steps to set up the Enterprise App in the Azure environment to be assessed. This walk-through covers how to do this using the Microsoft Azure Portal (portal.azure.com).

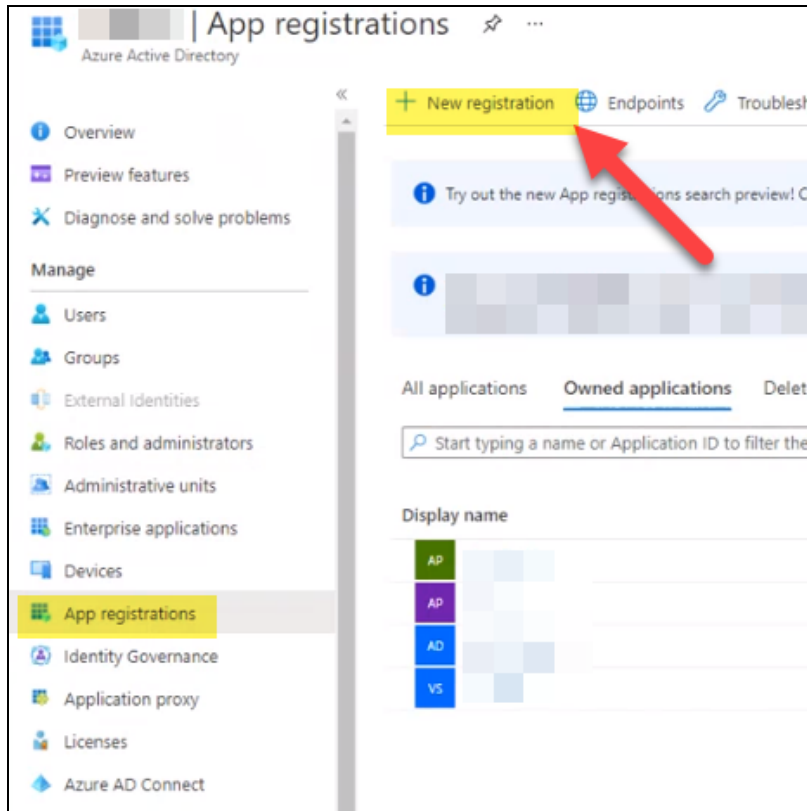
Note: Note that you must have an active Azure subscription in the Azure tenant to be assessed.

Step 1 — Create Enterprise App in Azure Tenant to be Assessed

1. From the Azure Portal home page, search for and open **Azure Active Directory**.



2. From the left screen, click **App Registrations**. Then click **New Registration**.



3. Enter a name for the application. Choose the **Supported account types** for the app. A **Redirect URL** is not required. Then click **Register**.

Register an application ...

* Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

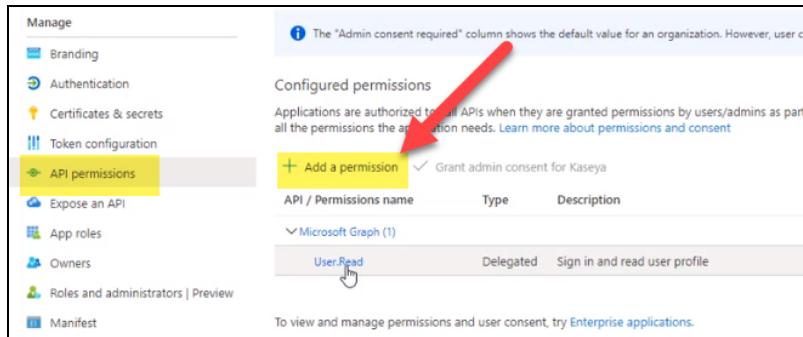
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

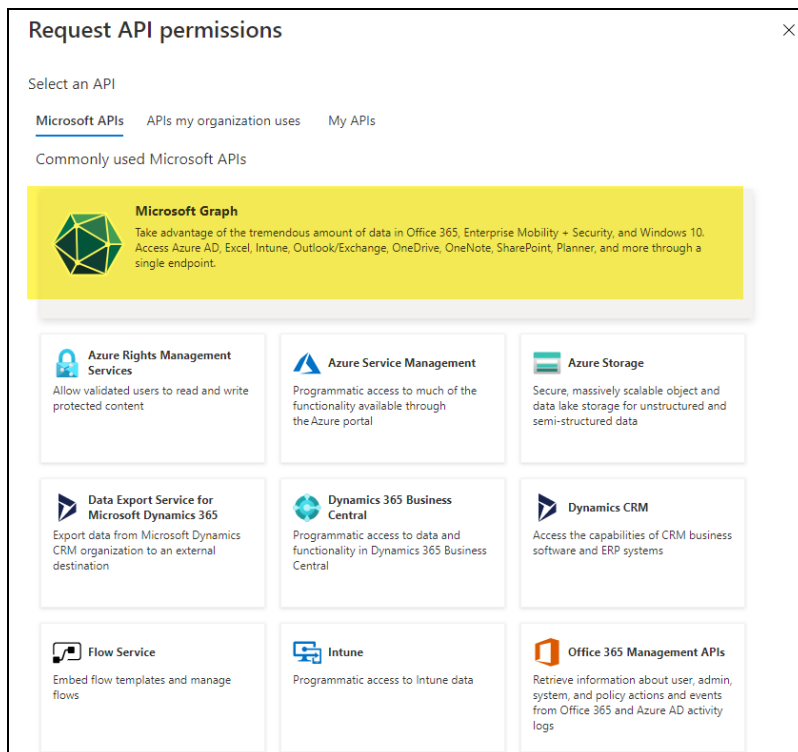
Web

Step 2 — Grant API Permissions to Enterprise App

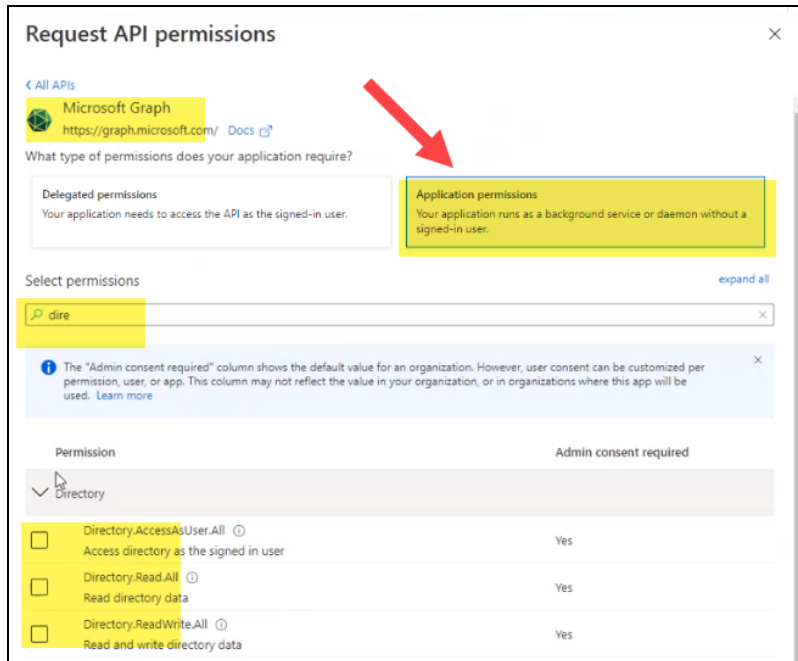
1. From your app, click **API permissions** from the left menu. Next click **Add a permission**.



2. From Microsoft APIs, choose the **Microsoft Graph API**.



3. From **Application Permissions**, select and assign the permissions detailed in the list below. When you are finished, click **Add Permissions**.



- AdministrativeUnit.Read.All
- AuditLog.Read.All
- Device.Read.All
- Directory.Read.All
- Domain.Read.All
- Group.Read.All
- GroupMember.Read.All
- IdentityProvider.Read.All
- Notes.Read.All
- Organization.Read.All
- Reports.Read.All
- SecurityEvents.Read.All
- Sites.Read.All
- User.Read.All
- Subscription.Read.All (***LOCATED UNDER DELEGATED PERMISSIONS**)
- User.ReadBasic.All (***LOCATED UNDER DELEGATED PERMISSIONS**)

Note: Select **Delegated Permissions** to access the two permissions above.

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

subscription.read.all

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
Subscription (1)	
☒ Subscription.Read.All ⓘ Read all webhook subscriptions	Yes

4. Finally, click **Grant admin consent** for the app permissions. Some permissions require admin consent to be added. Work with your on-site Azure administrator to grant admin consent.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by us all the permissions the application needs. [Learn more about permissions and con](#)

+ Add a permission ☒ Grant admin consent for

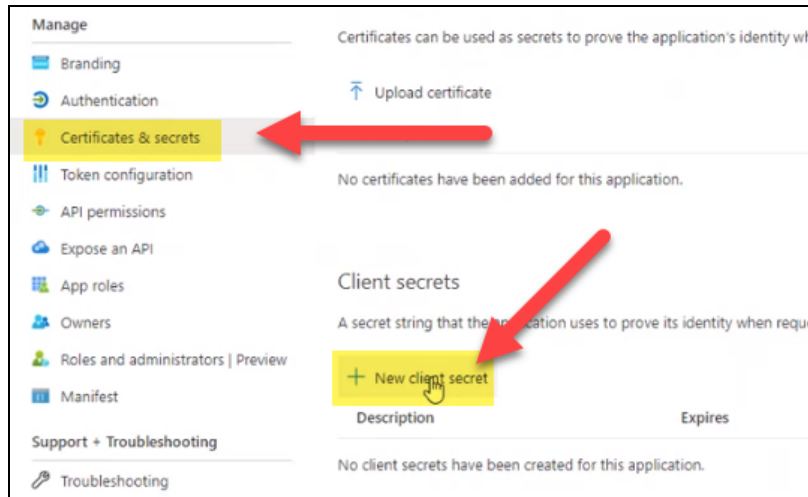
API / Permissions name Grant admin consent for

Microsoft Graph (10)

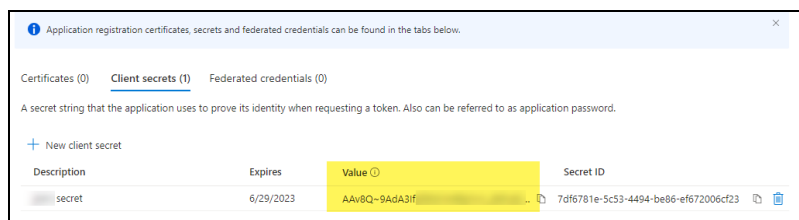
AuditLog.Read.All	Application	Read all audit log data
-------------------	-------------	-------------------------

Step 3 — Create Secret Key for Enterprise App

1. From your app, click **Certificates & Secrets** from the left-menu.
2. Click **New client secret**.

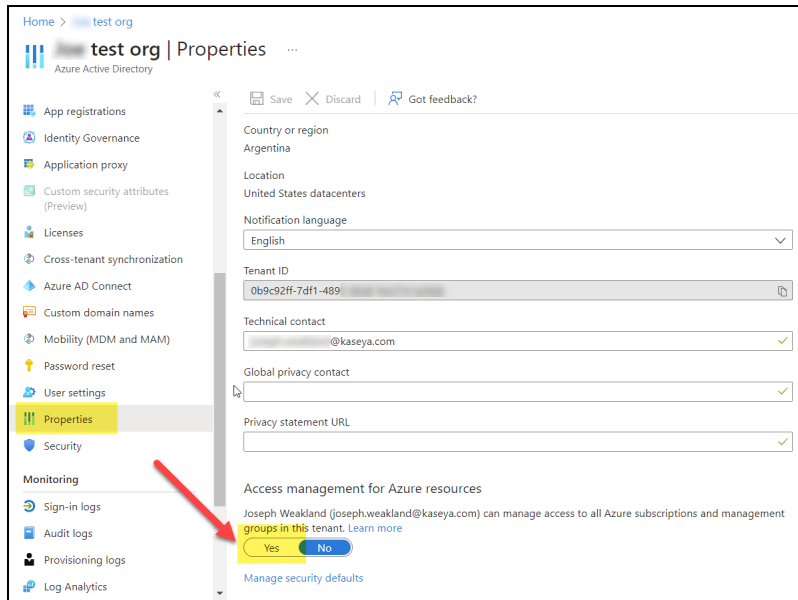


3. Enter a description for the secret and select an expiration period. Click **Add**.
4. Take note of the secret **Value**. You can copy it to your clipboard.

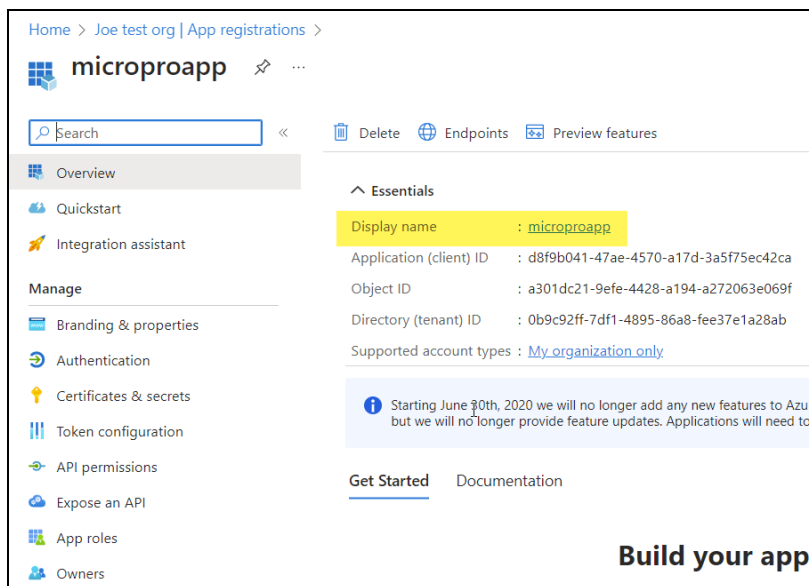


Step 4 — Add App as Reader to Root Management Group

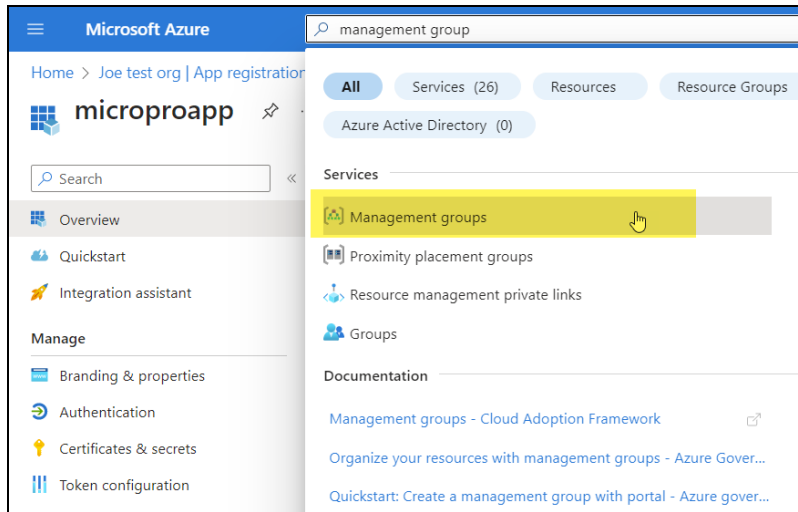
1. From your Azure tenant, navigate to **Azure Active Directory > Properties**. Switch **Access management for Azure resources** to **Yes**.



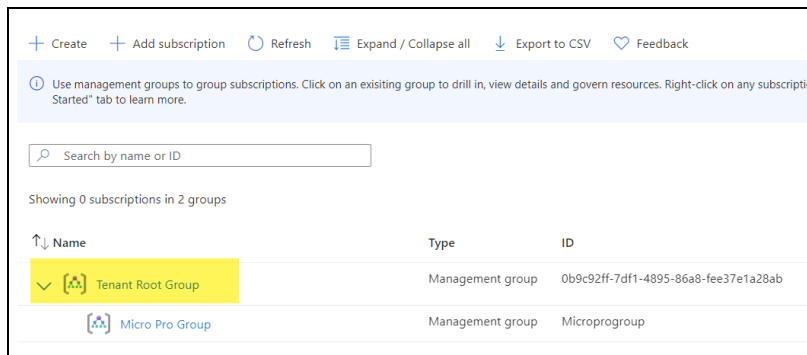
- Next, navigate to **Azure Active Directory > App registrations**. Find and click on the app you created earlier. Copy the complete display name of the app to your clipboard.



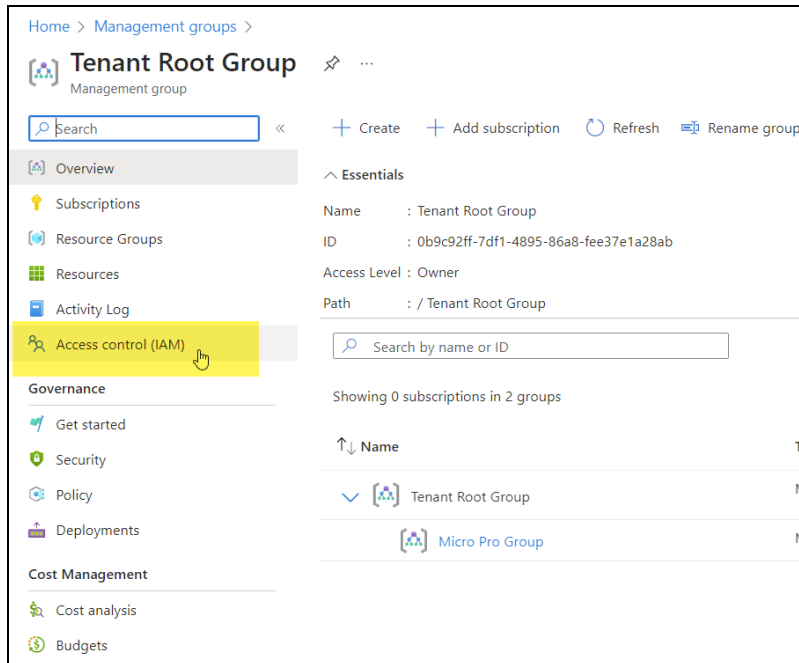
- From the search bar, search for and open **Management Groups**.



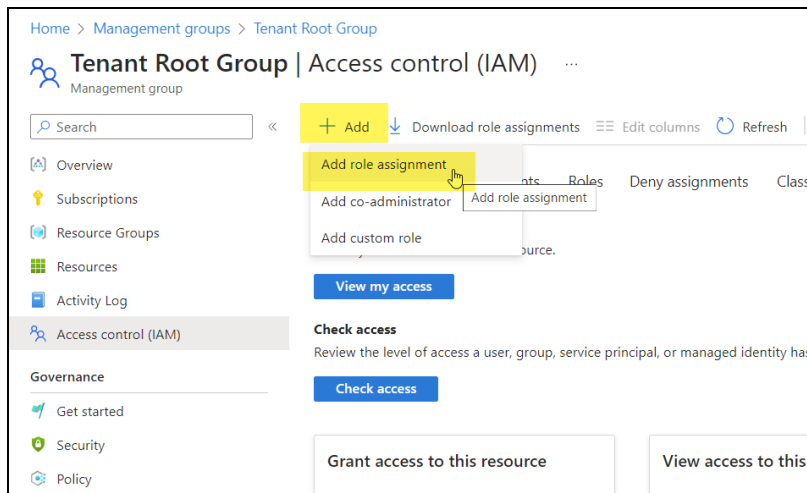
4. Click on and open the **Tenant Root Group**.



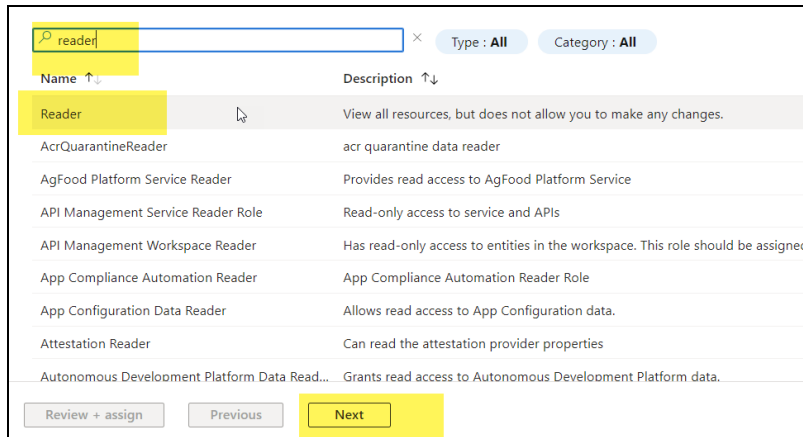
5. Select **Access Control (IAM)**.



6. Click on '+ Add' and 'Add role assignment'.



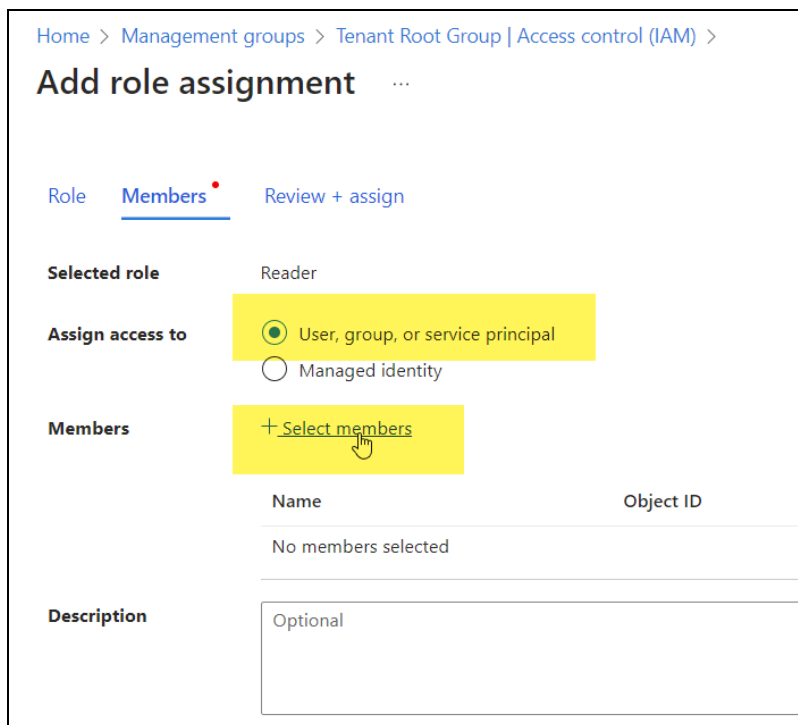
7. Select the 'Reader' role and then click on **Next**.



Name ↑↓	Description ↑↓
Reader	View all resources, but does not allow you to make any changes.
AcrQuarantineReader	acr quarantine data reader
AgFood Platform Service Reader	Provides read access to AgFood Platform Service
API Management Service Reader Role	Read-only access to service and APIs
API Management Workspace Reader	Has read-only access to entities in the workspace. This role should be assigned
App Compliance Automation Reader	App Compliance Automation Reader Role
App Configuration Data Reader	Allows read access to App Configuration data.
Attestation Reader	Can read the attestation provider properties
Autonomous Development Platform Data Read...	Grants read access to Autonomous Development Platform data.

[Review + assign](#) [Previous](#) [Next](#)

8. With **'User, group, or service principal'** selected, click on **'+ Select Members'**.



Home > Management groups > Tenant Root Group | Access control (IAM) >

Add role assignment ...

Role **Members** Review + assign

Selected role Reader

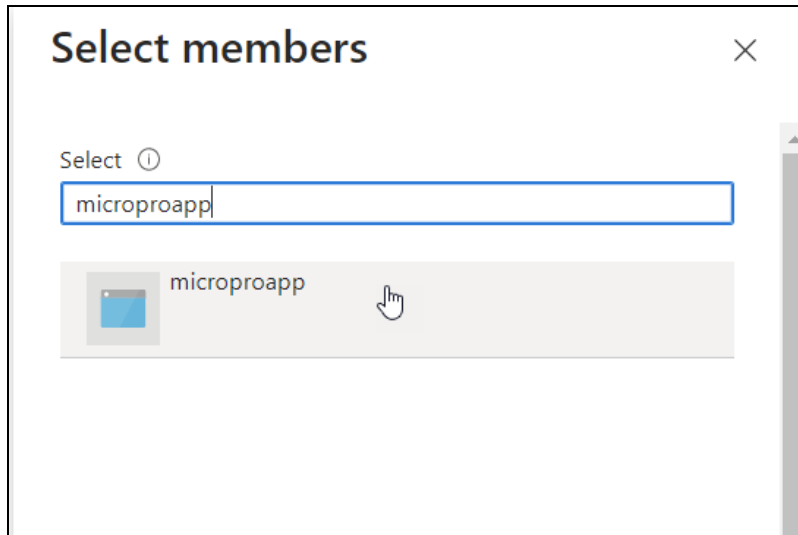
Assign access to ☒ User, group, or service principal ☐ Managed identity

Members [+ Select members](#)

Name	Object ID
No members selected	

Description Optional

9. In the **Select members** box, **paste the Display name of the app** that you copied earlier. Then click **Select**.



10. Click **Next** and then click **Review + assign**.

Name	Object ID	Type
microproapp	1811fd1f-8454-4703-8c50-608f7ae70e27	App

Description: Optional

Review + assign Previous Next

11. You can find the app that you added under **Role assignments**.

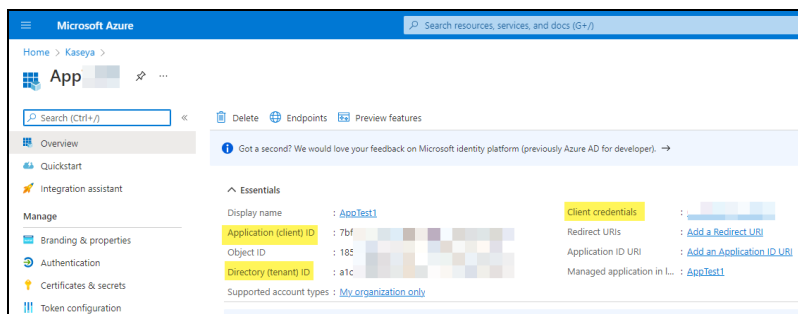
Name	Type	Role	Scope	Condition
Reader	App	Reader	This resource	None
User Access Administrator	User	User Access Administrator	Root (Inherited)	None

Step 5 — Gather Credentials and Perform Scan

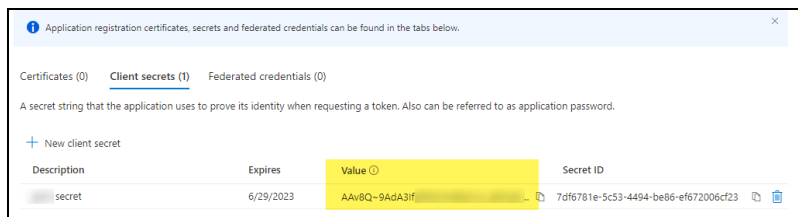
1. To perform a combined Microsoft Cloud and Azure Scan using Network Detective Pro or Compliance Manager GRC, you will need 3 separate credentials.

- **Tenant ID**
- **Client ID**
- **Client secret Value**

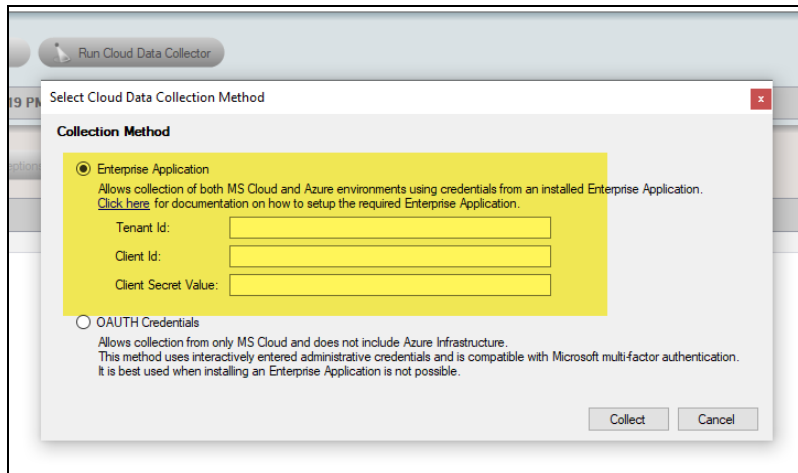
You can find these in the Azure Portal from [Your App] > **Overview**.



Copy the client secret **value** from **Certificates & secrets** > **Client secrets**.



2. **For Network Detective Pro:** Open **Network Detective Pro** and log in to your account. From your chosen Network Detective Pro Microsoft Cloud Assessment Site, click **Run Cloud Data Collector**. Enter these values into the correct fields and click **Collect**.



3. **For Compliance Manager GRC:** From **[Your Site] > Compliance Manager GRC > Data Collection > Cloud Scan**, click **Configure**. Enter the values into the correct fields. Then click **Save**.

The screenshot shows a "Configure Scan Settings" form. Under the heading "Azure AD Credentials", there are three input fields: "Client Id:", "Tenant Id:", and "Client Secret Value:". The "Client Id:" field is currently highlighted with a red border. At the bottom right of the form are "Cancel" and "Save" buttons.

Microsoft Cloud Assessment Reports

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

Report Name	Description
Azure AD Detail Report	The Azure AD Detail Report goes through the entire Azure Active Directory environment and documents all organizations, domains, and support services that are turned on for the AD environment. Every detail is presented in line-item fashion in an editable report document, including: installed special applications, web URLs to those apps, organizational contacts, distribution lists, proxy addresses, Microsoft

Report Name	Description
	service plans and SKUs being used, groups, users, permissions, devices, and more. The report is organized by section with a table of contents to help you locate the specific findings of interest, and problem areas are conveniently highlighted in red, making it easy to spot individual problems to be rectified.
Cloud Management Plan	The Cloud Management Plan takes issues identified in the Risk Report, organizes them by severity, and includes specific recommendations on how to remediate them. The report's information is pulled directly from the Microsoft controls from multiple Cloud components, including SharePoint, OneDrive, Teams, Azure AD itself. It also identifies other types of issues related to misconfigurations and operations.
Cloud Risk Report	The Cloud Risk Report, like the Risk Reports in all of our other Network Detective modules, spans all of the Microsoft Cloud components. It includes an overall Risk Score, an overall Issues Score, as well as a summary list of issues discovered. The issues come from both the Microsoft controls as well as other best practices. It identifies specific risks that are due to misconfigurations as well as risks created from turning on or off specific running components.
Compensating Control Worksheet	The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to mitigate risks in the cloud environment. Here you can explain document and explain why various discovered items are not true issues and possible false positives. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements. The Compensating Controls Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk.
Microsoft Cloud Configuration Change Report	The Microsoft Cloud Configuration Change Report is a very detailed technical report that identifies entity and configuration changes. The changes are grouped by properties, showing the old values vs. the new values, and then the changes are grouped together into bands called "Change Sets." This report gives you the ability to look at a group of changes together, as well as see how all the properties have changed for that particular time period. This is useful for change management and for capturing and documenting unwanted changes in the event you need to roll back those changes in the user interface.

Report Name	Description
Microsoft Cloud Security Assessment	The Microsoft Cloud Security Assessment report brings together all of the security aspects of Microsoft Cloud under one umbrella. It not only includes your own Microsoft Control Score and Secure Score from Microsoft; it also shows your trending against the average score of your peers.
Microsoft Teams Assessment Report	The Microsoft Teams Assessment Report provides detail about each team in the system, including who the owners are, what channels they have, and what kind of user identity audits have been conducted on the channels. There are individual entries that can be used for audits of the member settings, the guest settings, the message settings, the fun settings, the tab settings. This information goes beyond the Microsoft security score controls and includes other types of misconfigurations that might cause security problems, such as having guest members that are able to remove and delete channels.
OneDrive Assessment Report	The OneDrive Assessment Report provides a high-level summary report of all OneDrive usage. This is critical to know, since it includes every user the system has, all the Teams, and all the sites created by the client. This overview report gives you a solid handle on how the OneDrive platform is growing, and looks for spikes in that growth that need to be managed. It also looks for spikes in activity that may need to be investigated. The report provides trends over of 30-, 60-, and 90-day increments to give you a solid indicator of storage and bandwidth utilization.
Outlook Mail Activity Report	The Outlook Mail Activity Report is the perfect complement to the Network Detective Exchange Assessment module, which provides deep dive information about Office 365 usage. The Outlook Mail Activity Report provides a high-level summary of what emails are being sent and received by your top 10 active senders and active receivers for the reporting period. This report is meant to be run month-over-month to identify the power users who may need more capacity, and which mailboxes are not being read at all and likely represent recently inactive users that need to be cleaned up.
SharePoint Assessment Report	The SharePoint Assessment Report is a detailed assessment that shows the total number of sites started under management, how many active SharePoint sites there are, what storage requirements there are, and includes daily trends in the number of sites and storage usage. It then takes the site collections and breaks down all the individual sites so you can understand what is being published in each,

Report Name	Description
	how they are organized, and even what groups they contain. Among other things, the report helps understand growth trends and better predicts backup needs.

Performing an AWS Assessment

AWS Assessment Overview

The AWS (Amazon Web Services) Assessment module employs a specialized data collector to scan the Amazon Cloud. In this way, you can use Network Detective Pro to gather basic infrastructure data from AWS, including details from some of the most commonly used cloud services.

The AWS Module allows you to produce two editable, detailed reports about the following AWS services:

- **IAM** – AWS accounts are typically provisioned with a root account, but it is recommended to use the Identity Access Management (IAM) service to add additional users and assign permissions. This section shows the various groups and users that have been granted access.
- **VPC** – Network resources can be grouped in VPCs. VPCs represent network segmentation in the AWS world. VPNs can be established to VPCs allowing external access to cloud resources.
- **EC2** – This represents one of the most commonly used computer resources in AWS that can be used to run virtual machines. These are some of the first types of resources that MSPs are typically asked to manage in the AWS environment for their customers. In most cases, RMM agents can be placed on individual virtual machines that are part of EC2.
- **RDS** – This service is used to create relational databases in the cloud (like SQL Server and MySQL). Businesses typically have migrated their databases from on premise to RDS instances in AWS.
- **S3** – This service is used to store files in AWS for access by various other services, including EC2. Additional uses can be for downloads, uploads, and also to host websites.

With Network Detective Pro, you'll have access to all the data you need to prioritize your work based on risk and issue severity, and get the right things done at the right time.

What You Will Need

Network Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
AWS Credentials	Before you scan the AWS environment, you will need to following AWS credentials: • AWS Access Key ID • AWS Secret Key WORK WITH YOUR TECH TEAM TO GATHER THESE CREDENTIALS, AND TREAT THEM WITH THE APPROPRIATE SECURITY PRECAUTIONS!

Follow these steps to perform a AWS Assessment.

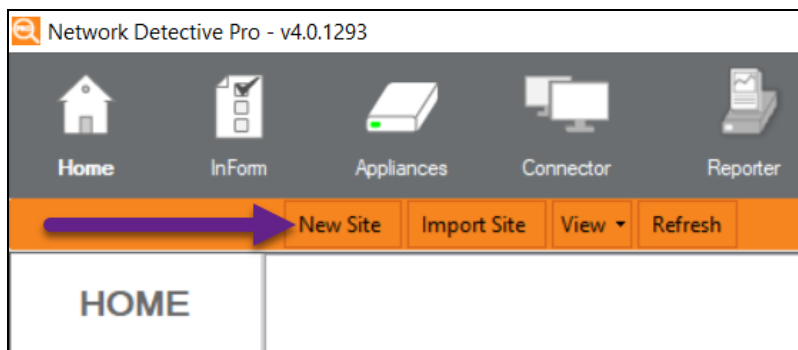
Step 1 — Download and Install the Network Detective Pro app

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

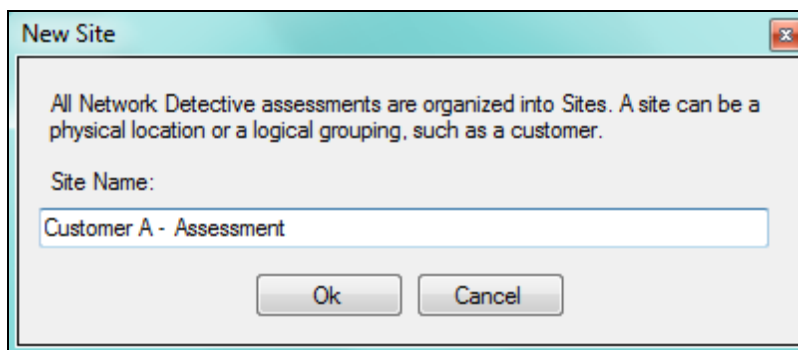
Step 2 — Create a New Site

To create a new site:

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



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

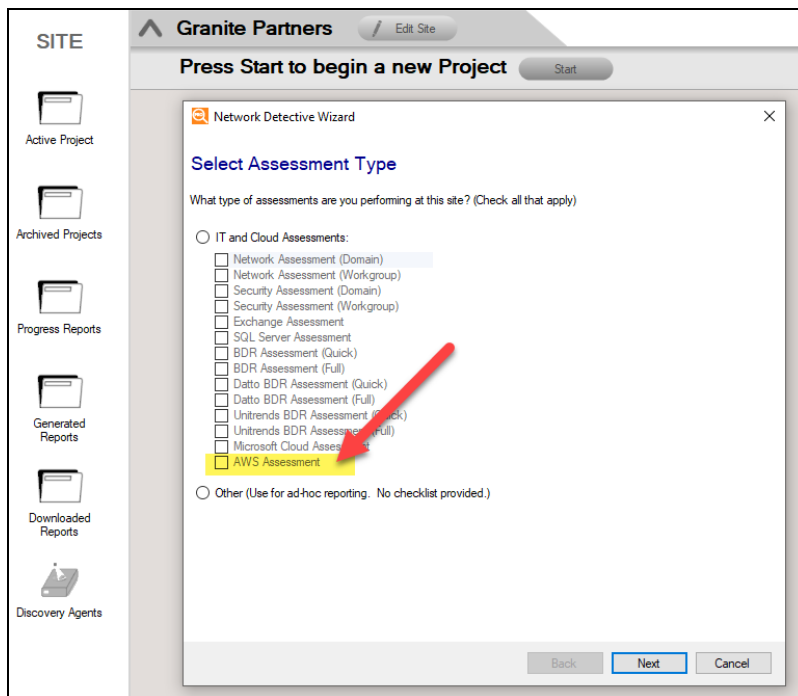


Step 3 — Start an AWS Assessment

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

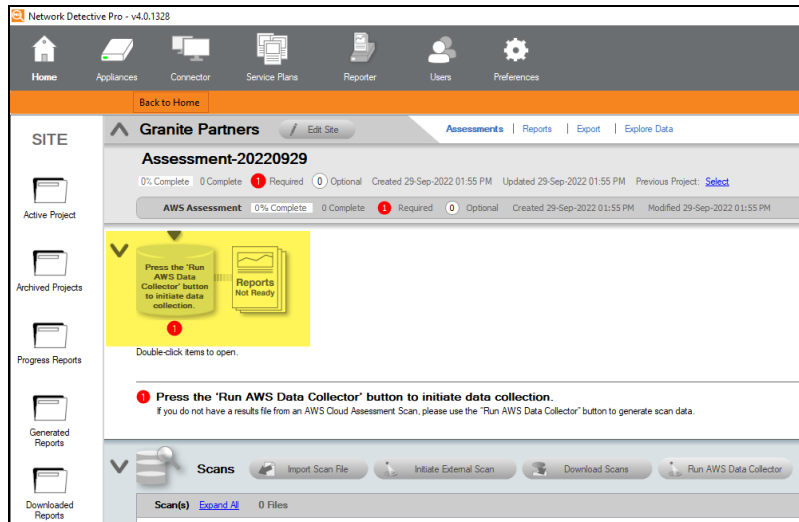


Next, select the **AWS Assessment** option presented.



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

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



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

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



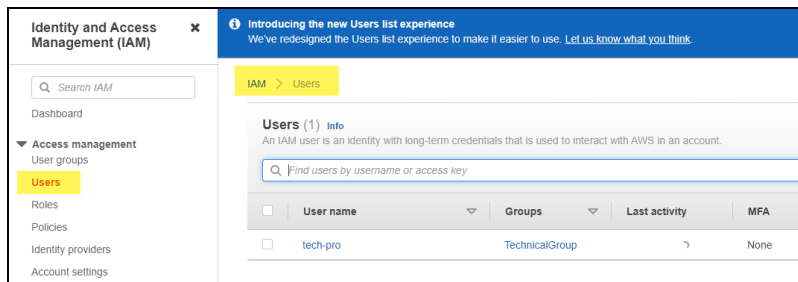
Step 4 — Gather AWS Access Key and Secret Key

Before you can begin the AWS scan, you must A) create an AWS user with the minimum API permissions to complete the AWS scan, and B) generate an **Access key ID** and **Secret key** for this user and copy them to your clipboard. Here's how this works:

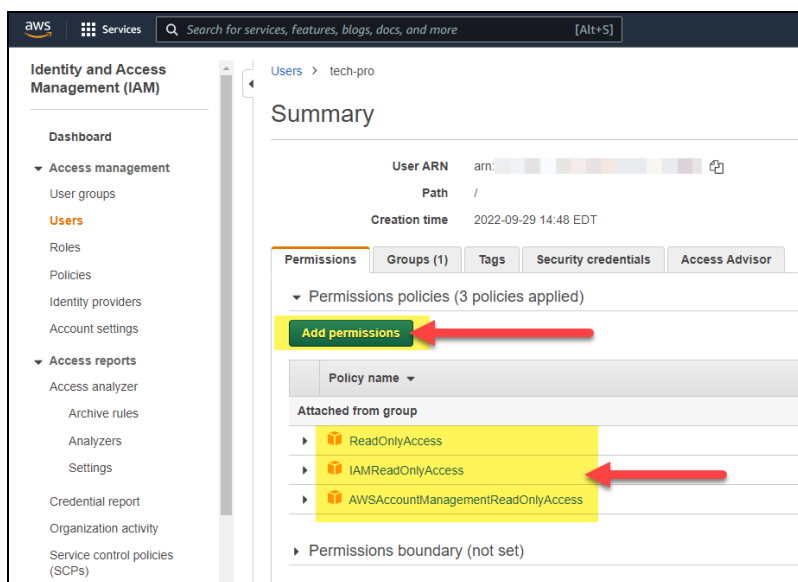
4(A) — Create User and Assign API permissions

Create a user in the AWS console and assign the user the appropriate API permissions to perform the AWS scan.

1. Navigate to **Identity and Access Management > Users**.



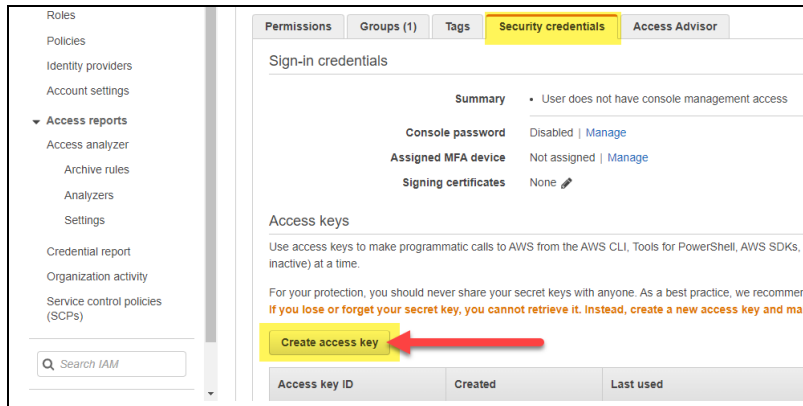
2. Create a new user or modify an existing user. Add the following **API permissions** to the user:



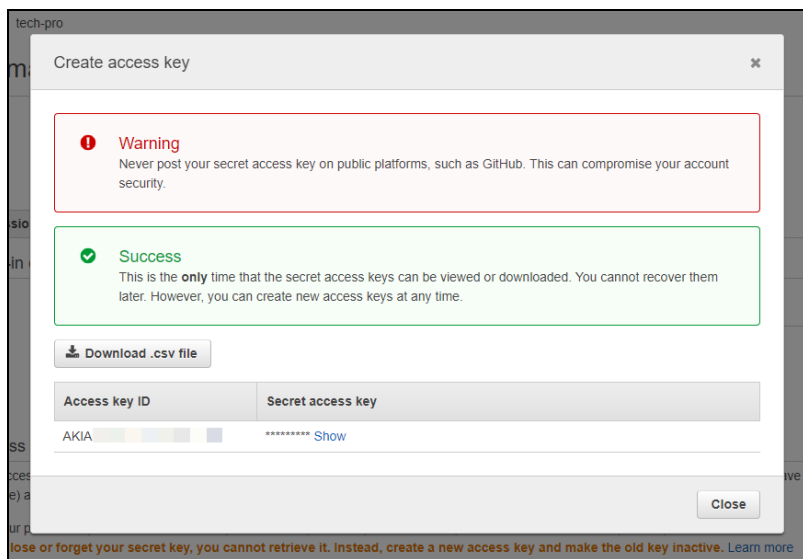
- **ReadOnlyAccess**
- **IAMReadOnlyAccess**
- **AWSAccountManagmentReadOnlyAccess**

4(B) — Generate Access Key ID and Secret key

1. Next, open the **Security credentials** tab for the user. Then click **Create access key**.



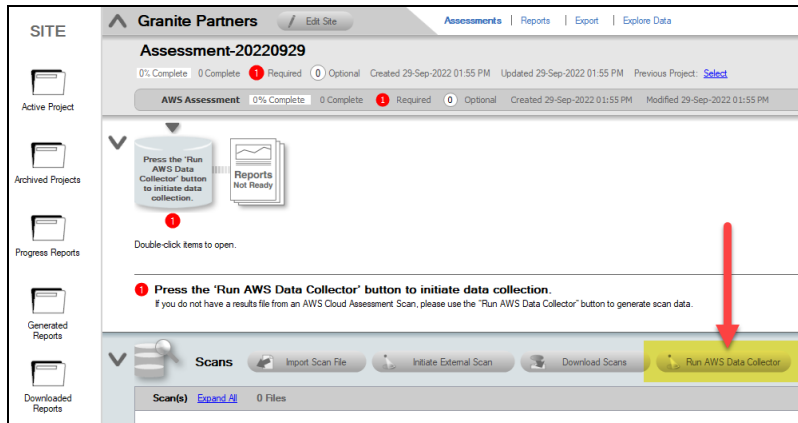
2. Copy the **Access key ID** and **Secret access key** to your clipboard. **TREAT THIS DATA WITH THE APPROPRIATE SECURITY PRECAUTIONS!**



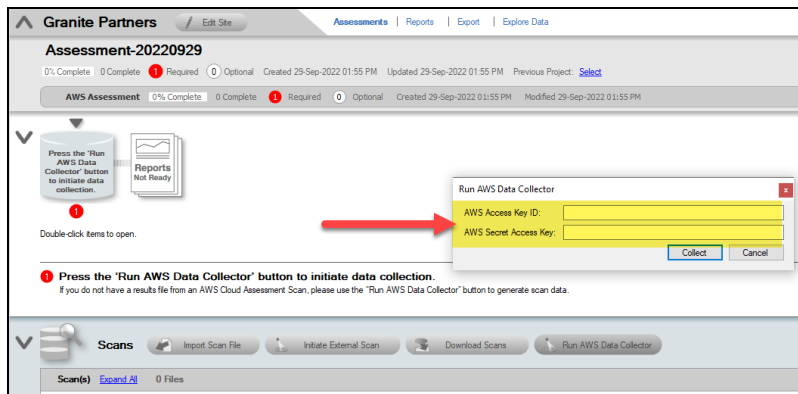
Step 5 — Perform AWS Scan Data Collection

To begin the AWS Cloud Scan, return to the Network Detective Pro app. From your active AWS assessment:

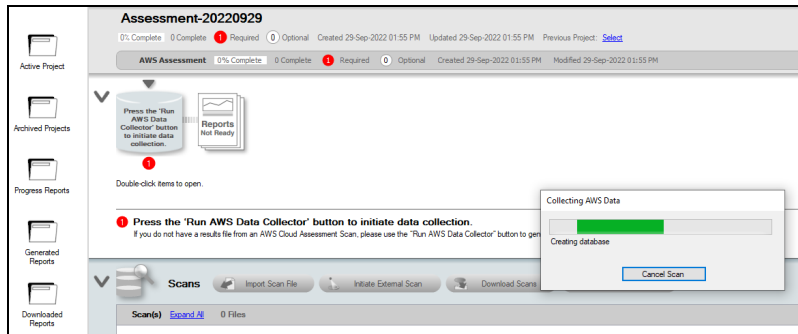
1. Click **Run AWS Data Collector** from the Scans panel.



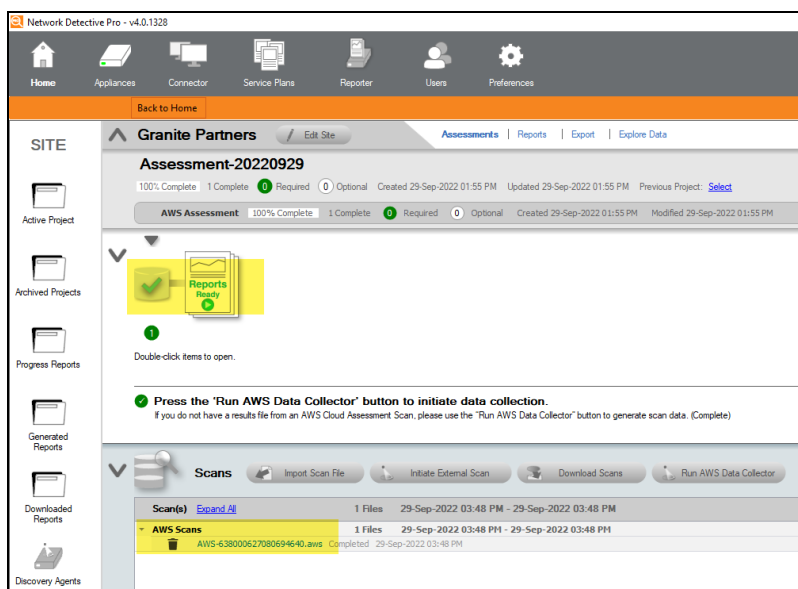
2. Enter the credentials you copied in the previous step. Then click **Collect**.



3. A progress bar indicates a successful connection to the AWS environment.



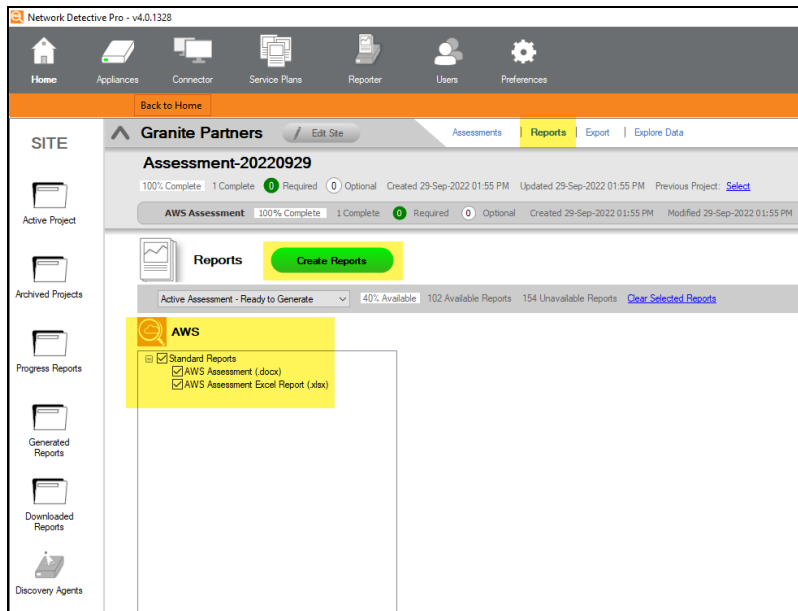
- When the AWS scan finishes, your checklist will be updated and the AWS scan file (.aws) will appear. You are now ready to generate reports.



Step 6 — Generate AWS Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your AWS Assessment, follow the steps below:

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



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

AWS Assessment Reports

The **AWS Assessment** module can generate the following reports:

Standard Reports

Report Name	Description
AWS Assessment	The AWS Assessment goes through the entire AWS environment and documents all services, account ID, EC2, RDS, and S3 that are found in the AWS environment. Every detail is presented in line-item fashion in an editable report document. The report is organized by section with a table of contents to help you locate the specific findings of interest.
AWS Assessment Change Report	The AWS Assessment Change Report is a very detailed technical report that identifies entity and configuration changes. The changes are grouped by properties, showing the old values vs. the new values, and then the changes are grouped together into bands called “Change Sets.” This report gives you the ability to look at a group of changes together, as well as see how all the properties have changed for that particular time period. This is useful for change management and for capturing and documenting unwanted changes in the event you need to roll back those changes in the user interface.
AWS Assessment Excel	Comprehensive lists of all AWS assets and services in MS Excel format.

Performing a Cyberattack Risk Assessment Scan

Cyberattack Risk Assessment Overview

A cyberattack risk assessment is a systematic examination of an organization's potential vulnerabilities to cyber-attacks and the likelihood of such attacks occurring. It involves identifying, analyzing, and prioritizing potential security threats, and evaluating the current security measures in place to mitigate those threats.

The goal of a cyberattack risk assessment is to identify areas of risk and recommend steps that can be taken to reduce the risk of a successful attack, thereby improving the overall security posture of an organization.

With Network Detective Pro you can engage end-users in performing a Cyberattack Risk Assessment. You can create a custom download page where users will download and run a simple data collector. You can then download the scan results and generate a Cyberattack Risk Assessment Report.

Follow these steps to perform a Cyberattack Risk Assessment:

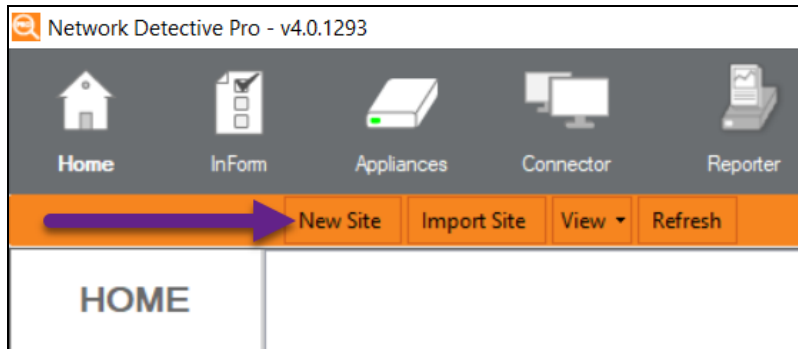
Step 1 — Download and Install the Network Detective Pro app

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

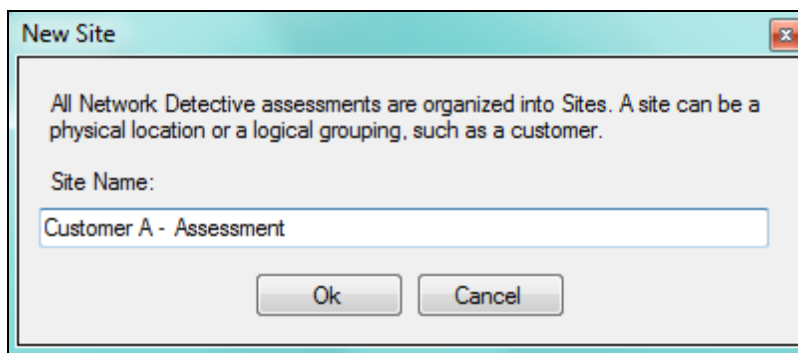
Step 2 — Create a New Site

To create a new site:

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



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

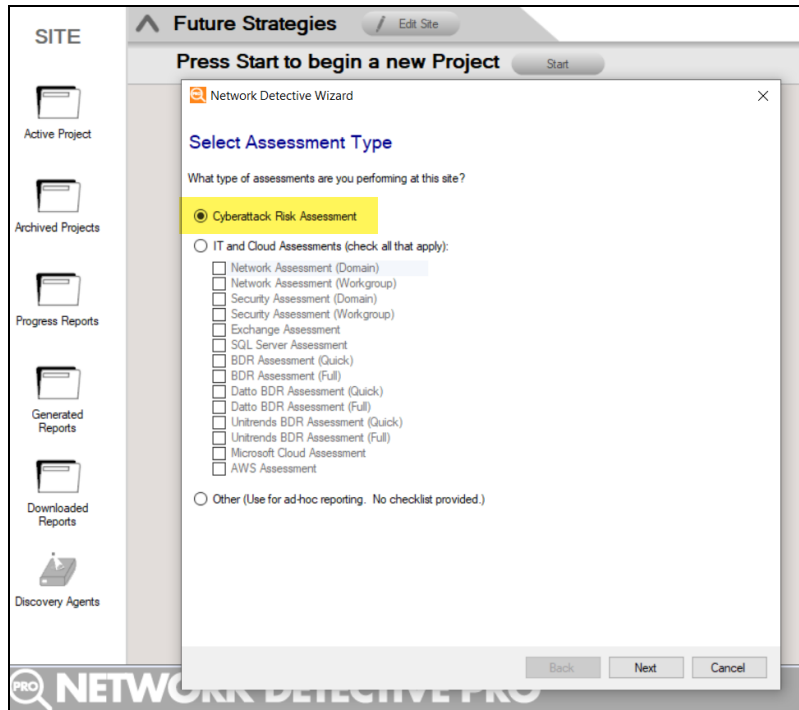


Step 3 — Create Cyberattack Risk Assessment in Network Detective Pro

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

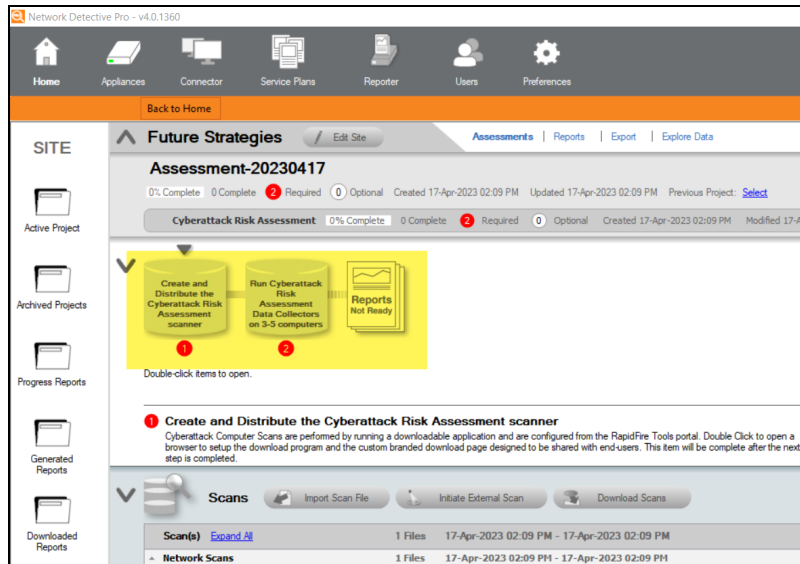


Next, select the **Cyberattack Risk Assessment**.



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

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



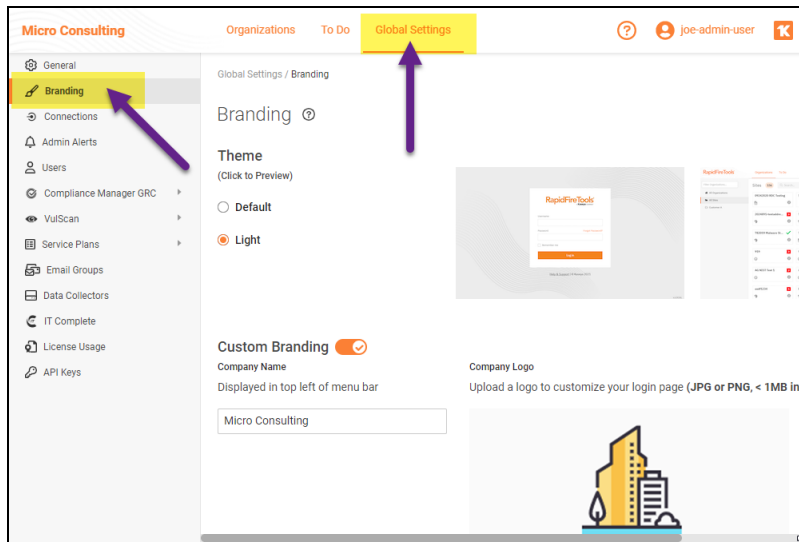
3. Complete the required **Checklist Items** and use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

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



Step 4 — Access RapidFire Tools Portal and Customize Branding

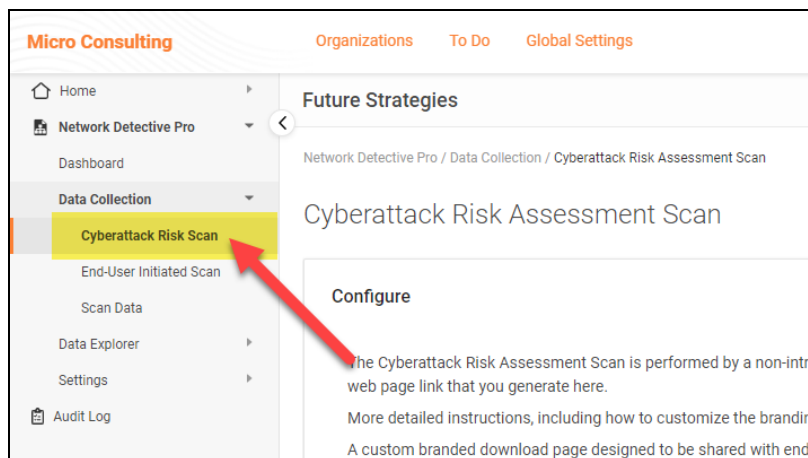
Access the RapidFire Tools Portal at <https://www.youritportal.com>. Then, customize the branding for the end-user download page. The download page is where end-users will access the computer scanner. It can be customized with your own company logo, for example. From the RapidFire Tools Portal, navigate to **Global Settings > Branding** and make your changes.



Step 5 — Create and Distribute the Cyberattack Risk Assessment Computer Scanner

Next, you will enable end-users to download and run the Cyberattack Risk Assessment Computer Scanner.

1. From the RapidFire Tools Portal, open your Network Detective Pro site and navigate to **Data Collection > Cyberattack Risk Scan**.



2. Click **Generate** from the Configure panel to create the URL for end-users to download and run the Cyberattack Risk Assessment Computer Scanner.

Cyberattack Risk Assessment Scan

Configure

The Cyberattack Risk Assessment Scan is performed by a non-intrusive scanning application that is downloaded from a site-specific, custom web page link that you generate here.

More detailed instructions, including how to customize the branding on the download page, are available [here](#).

A custom branded download page designed to be shared with end-users for local computer scans can be generated and managed below:

Click Generate to create a unique download page

Generate Delete Open Copy

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☒ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

3. **Copy the URL** and distribute the URL to end-users.

Configure

The Cyberattack Risk Assessment Scan is performed by a non-intrusive scanning application that is downloaded from a site-specific, custom web page link that you generate here.

More detailed instructions, including how to customize the branding on the download page, are available [here](#).

A custom branded download page designed to be shared with end-users for local computer scans can be generated and managed below:

<https://greystone.alert-central-staging.com/download/cybersecurity-computer-s> **Regenerate** Delete Open **Copy**

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☒ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

Save options Cancel

You can also configure several scan options. Uncheck optional scan items to reduce scan time.

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☐ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

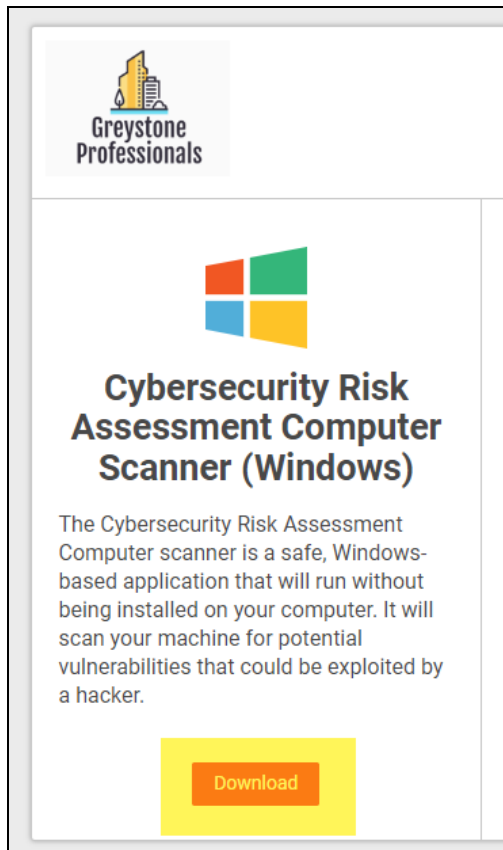
Save optionsCancel

Here's a breakdown of each scan option. When you change scan settings, the changes are applied to the next scan you perform.

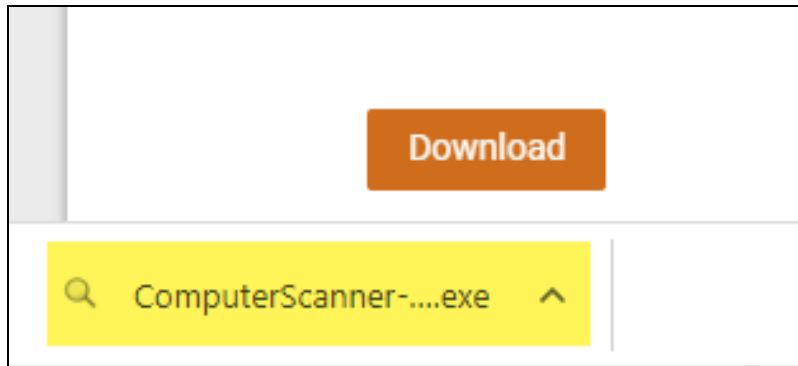
Perform Deep Scan for Sensitive Information	Scan for Personal Identifiable Information (PII) on the endpoint
Web Filtering Validation	Check to see if the endpoint can access websites that might pose a security risk
Malicious File Download Validation	Check to see if the endpoint can download files that might pose a security risk
External Vulnerability Scan	Perform a scan to detect potential external vulnerabilities
Detect Stored Browser Credentials	Check for cached users IDs and passwords

Step 6 — Users Downloads and Runs Cyberattack Risk Assessment Computer Scanner

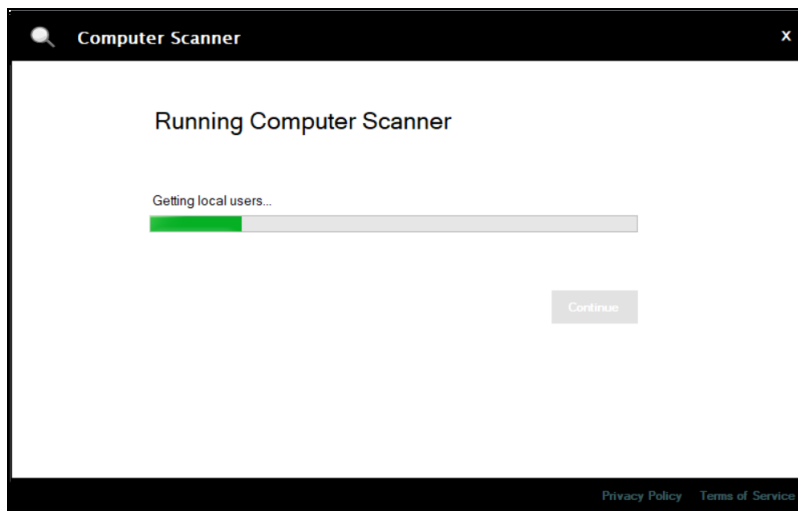
1. In this step, the end-user opens the URL that you provide. The end-user then clicks **Download** under the Cyberattack Risk Assessment Computer Scanner.



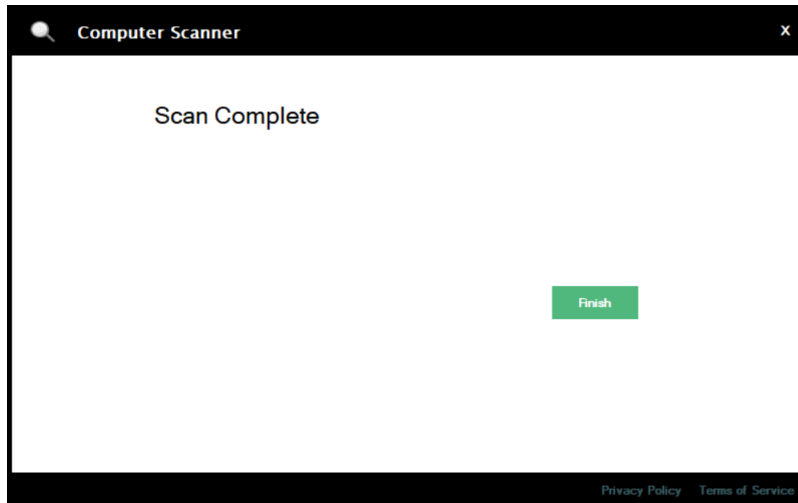
2. The end-user then opens the downloaded scanner.



3. The computer scanner will begin collecting data. This process will take a few minutes.



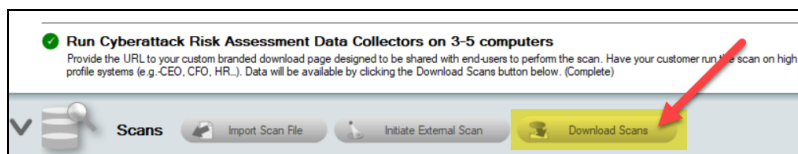
4. When the scan is complete, the end-user clicks Finish. The scan file will automatically be uploaded to Network Detective Pro and become available for you to download.



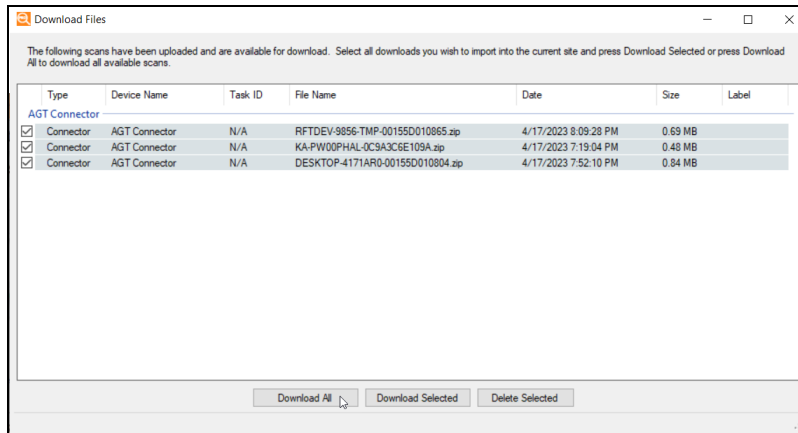
Note: You must run the Cyberattack Risk Assessment Computer Scanner on at least 3 devices in order to advance your assessment.

Step 7 — Download Scans in Network Detective Pro Cyberattack Risk Assessment

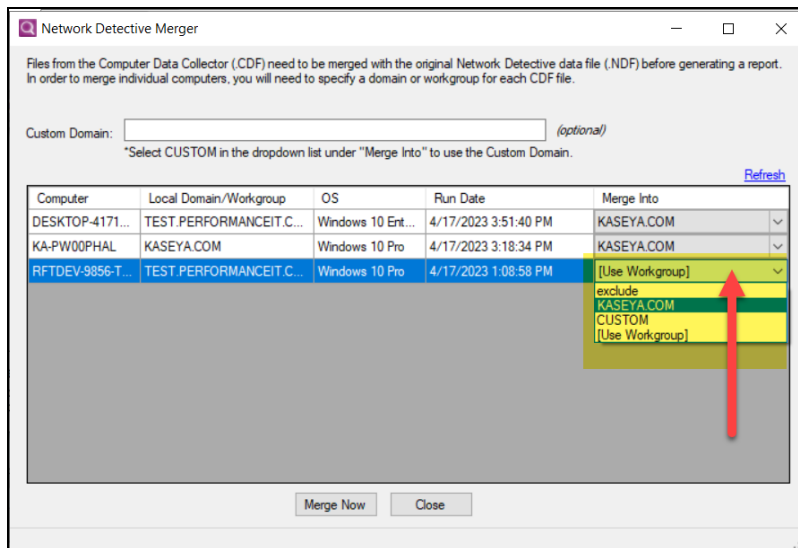
1. Next, return to Network Detective Pro and open your Cyberattack Risk Assessment project.
2. From the Scans bar, click **Download Scans**.



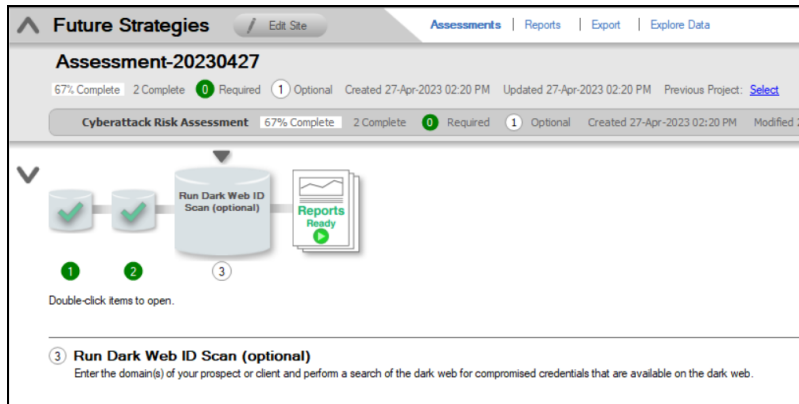
3. **Select and download** your Cyberattack Risk Assessment scans.



- For each scan file, **choose a merge option**. Select the domain or workgroup in which to merge the scan. This will determine how the scan data is organized in your reports. Then click **Merge Now**.



- Once you have downloaded and **merged at least 3 scan files into your assessment**, your checklist will be marked complete. You can now run the optional **Dark Web ID Scan**.

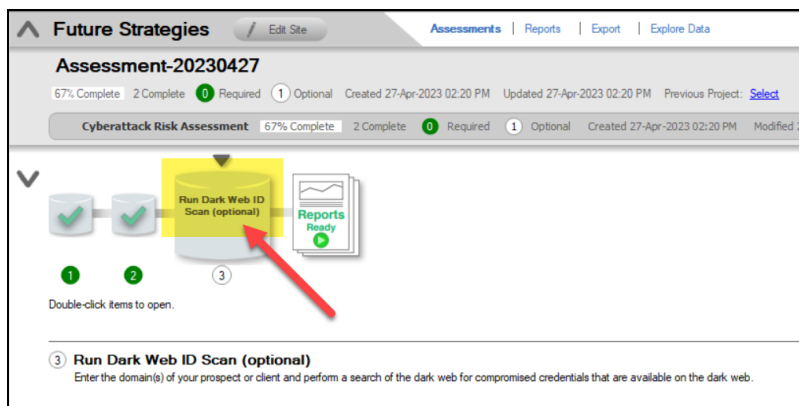


Step 8 —(Optional) Run Dark Web ID Scan

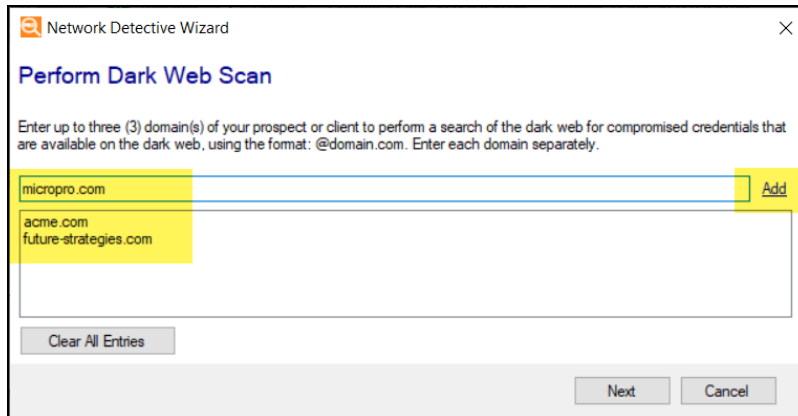
In this step, you can perform a **Dark Web Scan** for compromised usernames and passwords that may exist on the dark web. A sample of the results will appear in your assessment reports. You can ["Set Up Dark Web ID Integration with Network Detective Pro" on page 158](#) to retrieve the full list of compromised credentials.

To run the Dark Web Scan:

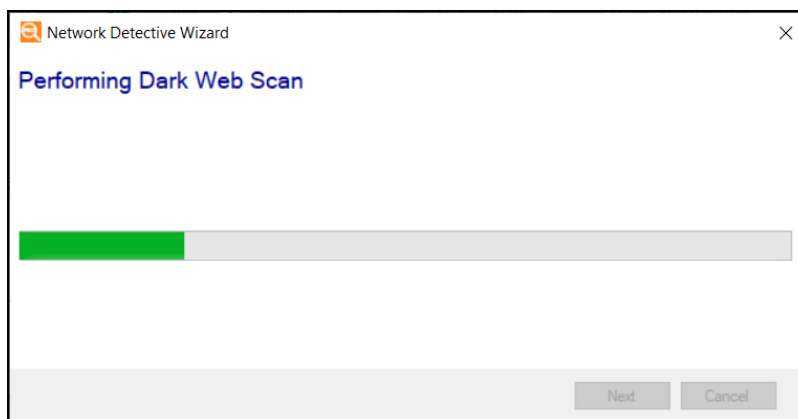
1. Double click on the **Run Dark Web ID Scan** to do item.



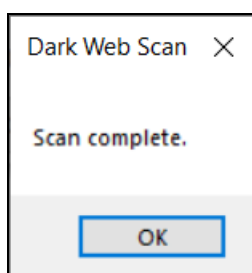
2. Enter a domain and click **Add**. **YOU CAN ENTER A MAXIMUM OF 3 DOMAINS**



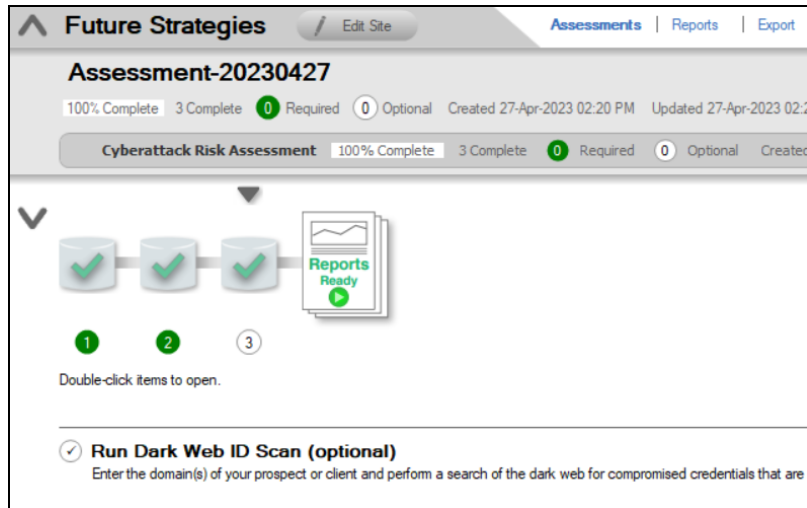
- When you finish entering domains to scan, click **Next**. The Dark Web Scan will begin.



- You will receive a notification when the scan is complete.



- The Run Dark Web ID Scan will be marked complete in your assessment To Do list.



Set Up Dark Web ID Integration with Network Detective Pro

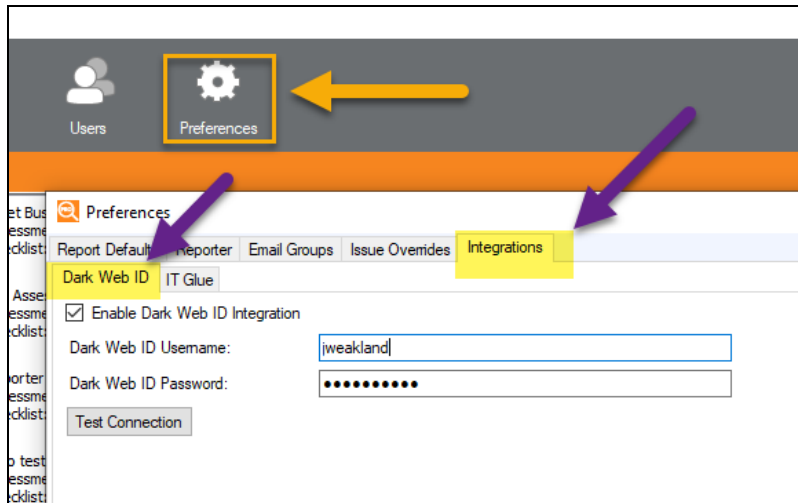
By default, the Dark Web Scan will only return the **first 5** compromised passwords identified for each domain you specify. However, **Dark Web ID** users (<https://www.idagent.com/>) can access full reporting for compromised passwords. To set this up:

First, contact Dark Web ID Support to Enable User API Access. To enable API Access, the Dark Web ID customer must open a ticket with Kaseya Support. The Dark Web ID team will grant the customer API access. Once the support ticket is closed, the user can successfully enter and test their credentials in Network Detective Pro. See also <https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-I-enable-API-access-for-ID-Agent->.

Once you enable Dark Web ID API access, you can set up the integration in Network Detective Pro. To do this:

1. In the Network Detective Pro app, click **Preferences** from the top menu.
2. Click the **Integrations** tab
3. From the **Dark Web ID** tab, **enable** the Dark Web ID Integration.
4. Then enter your Dark Web ID **Username** and **Password**.
5. Finally, click **Test Connection**. Once you verify the connection works, click **OK** to

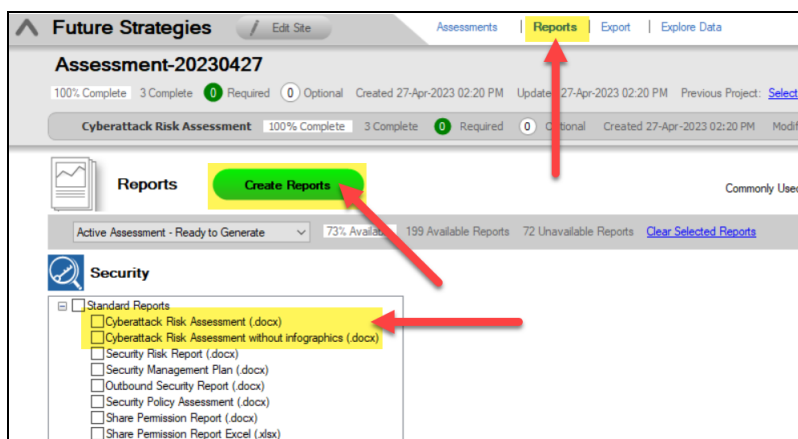
dismiss the Preferences menu.



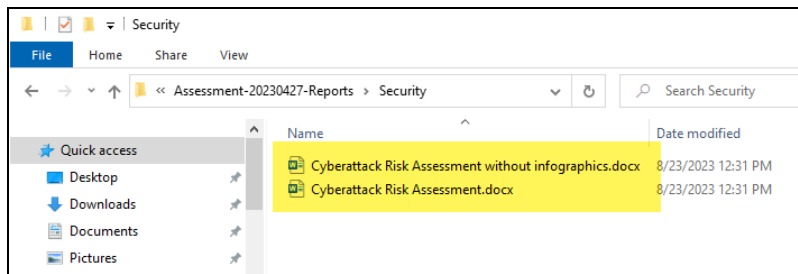
Step 9 — Generate Reports

To generate reports:

1. Open **Reports**.
2. Select the **Cyberattack Risk Assessment report**. You can choose to generate the report with or without infographics.
3. Click **Create Reports**.



4. The **Cyberattack Risk Assessment Report** will then become available in Windows Explorer.



Cyberattack Risk Assessment Reports

In addition to the standard Security assessment reports, the **Cyberattack Risk Assessment** module can generate the following additional reports:

Standard Reports

Report Name	Description
Cyberattack Risk Assessment Report	The Cyberattack Risk Assessment Report is a systematic examination of your organization's potential vulnerabilities to cyber-attacks and the likelihood of such attacks occurring. It involves identifying, analyzing, and prioritizing potential security threats, and evaluating the current security measures in place to mitigate those threats. This graphically-rich report includes an overall risk score, executive summary, and detailed findings.
Cyberattack Risk Assessment Report without infographics	You can generate the Cyberattack Risk Assessment Report without infographics.

Performing an Exchange Assessment

Exchange Assessment Overview

The Network Detective **Exchange Assessment Module** is composed of:

- the **Exchange Assessment Data Collector** used to assess the integrity of the Exchange email system being scanned
- the **Network Detective Pro application** used to manage Sites and generate assessment reports

The Network Detective **Exchange Assessment Module** is quick and easy to use. There are just a few basic steps:

1. Download and Install the Network Detective Pro application

Visit <https://www.rapidfiretools.com/ndpro-downloads/> to download and install the Network Detective Pro application.

2. Create a New Site

Create Site files 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 Exchange assessment — or any other assessment type.

3. Start an Exchange Assessment

Once the **Site** is created, start a **New Assessment** and perform the Exchange assessment data collection process using the guided **Checklist**.

4. Perform Exchange Scan Data Collection

Run the Exchange Assessment Data Collector on the target server. The output of the Exchange scan will be an .EDF used to generate reports via Network Detective. **Be sure that you document the name of the folder used to store scan data to import into your assessment.** When the Exchange Scan is complete, import the scan file into the assessment in Network Detective.

5. Generate Exchange Assessment Reports

Customize your reports by setting up your company's branding of the report to be generated with your logos and client information, and run the reports. The Network Detective Report Wizard will step you through this process.

What You Will Need

Exchange Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
Exchange Assessment Data Collector	The Network Detective Exchange Assessment Data Collector (EADC) is a windows application that performs the data collections for the Exchange Assessment Module.

Follow these steps to perform an Exchange Assessment.

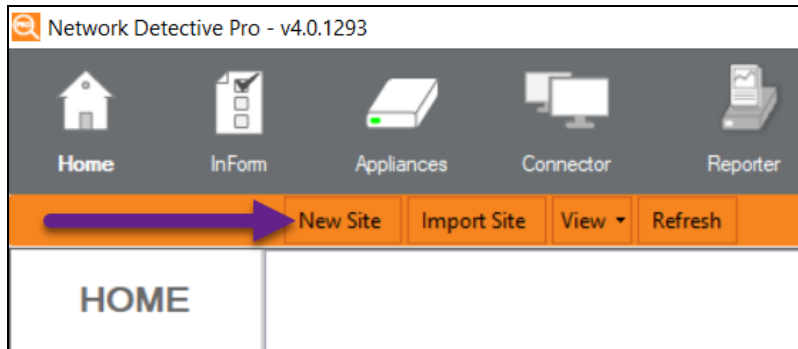
Step 1 — Download and Install the Network Detective Pro Application

Go to <https://www.rapidfiretools.com/ndpro-downloads/> to download and install the Network Detective Pro application. Then run Network Detective Pro and log in with your credentials.

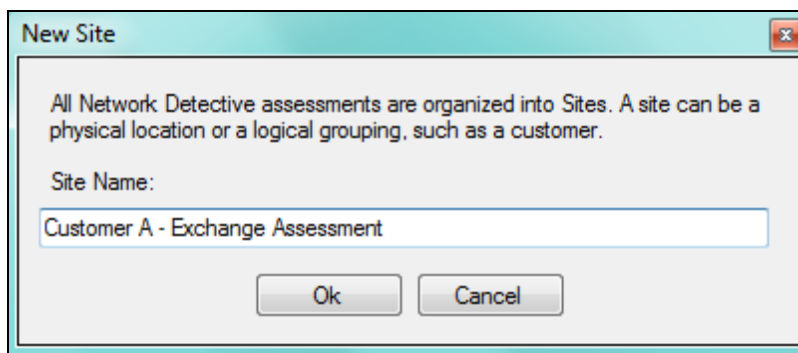
Step 2 — Create a New Site

To create a new site:

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



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

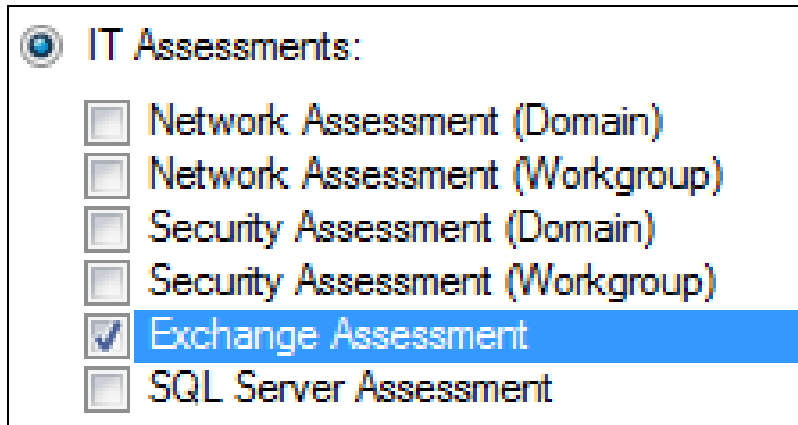


Step 3 — Start an Exchange Assessment

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

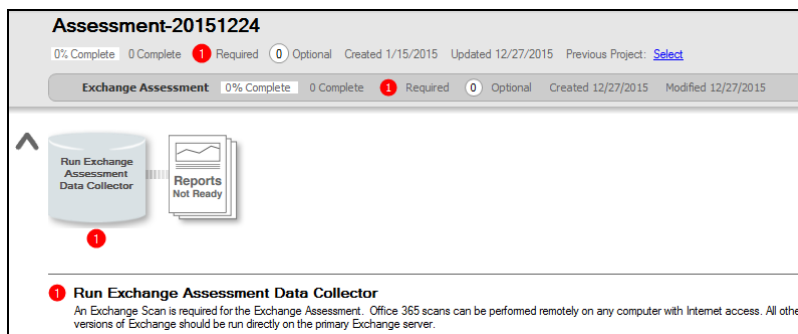


Next, select the **Exchange Assessment** option presented.



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

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



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

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

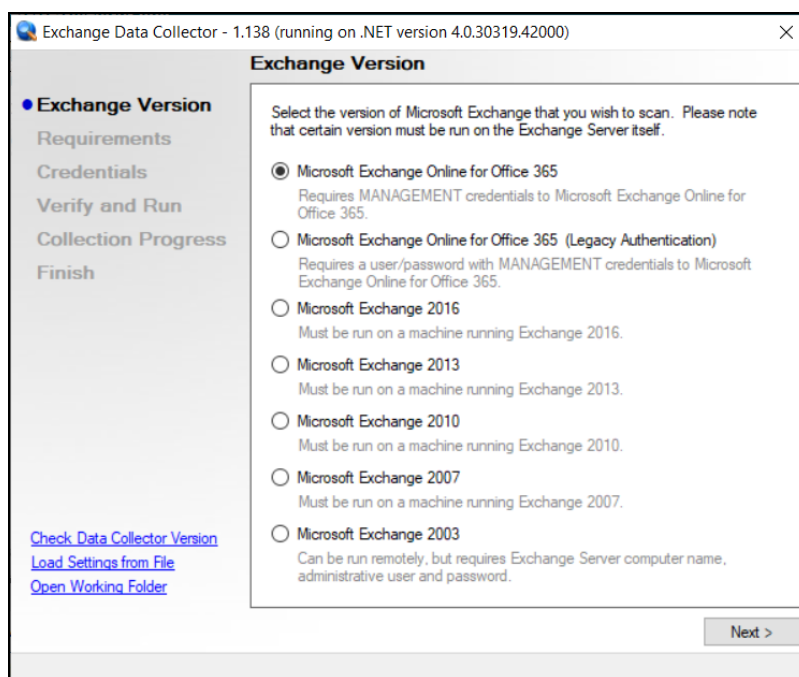


Step 4 — Perform Exchange Scan Data Collection

1. On the target network, log in to the local machine with **Administrator** privileges.
2. Download the **latest Exchange Assessment Data Collector** program from <https://www.rapidfiretools.com/ndpro-downloads/> and save onto any machine that can connect to the Exchange server. You can also save the program to a USB drive and run it on the machine.

Note: This download is a self-extracting zip file and does not require installation when run on client systems. You may extract the Exchange Data Collector files to a folder on either a machine that can connect to the Exchange server or a USB drive. Then you can run "RunExchangeDataCollector.exe" to launch the GUI.

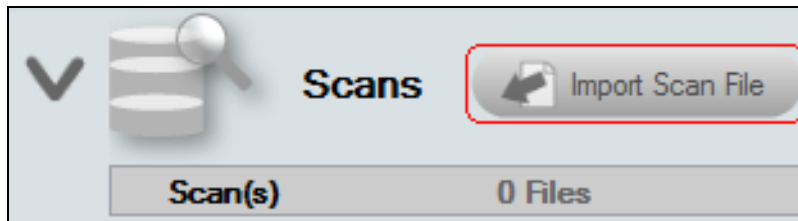
3. Right-click on the downloaded file and **run-as administrator** to ensure you are running with elevated credentials.
4. Next, after starting the **Exchange Assessment Data Collector**, select the version of Exchange that you are performing your scan on. Then proceed with using the necessary credentials while following the remaining wizard-driven prompts.



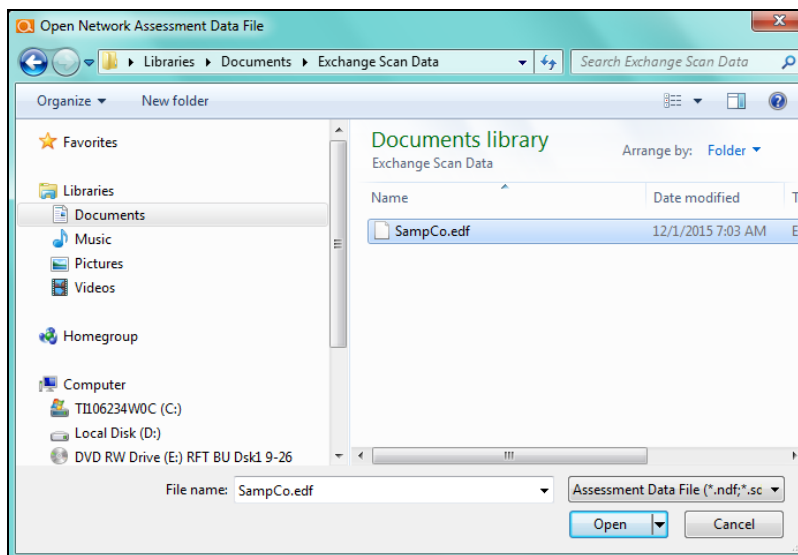
5. After the **Exchange Scan** is complete, either save the scan results file to a USB drive for later importing of the results into the assessment or email the file for later

access. **Make sure the USB has sufficient free space to extract and save the Data Collector files and to store the scan results data files.**

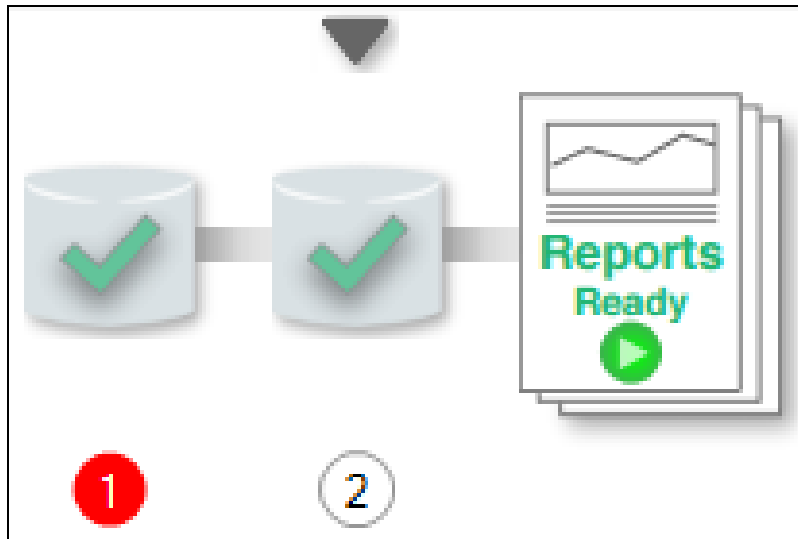
6. **Importing the Exchange Scan file into your Assessment:** From within the **Scans** section of the **Assessment Window**, select the **Import Scan File** button.



7. Then, browse for the folder storing the Exchange Scan results data file generated by the Exchange Data Collector, select the file, and then **Open** the file to import the scan results into your assessment.

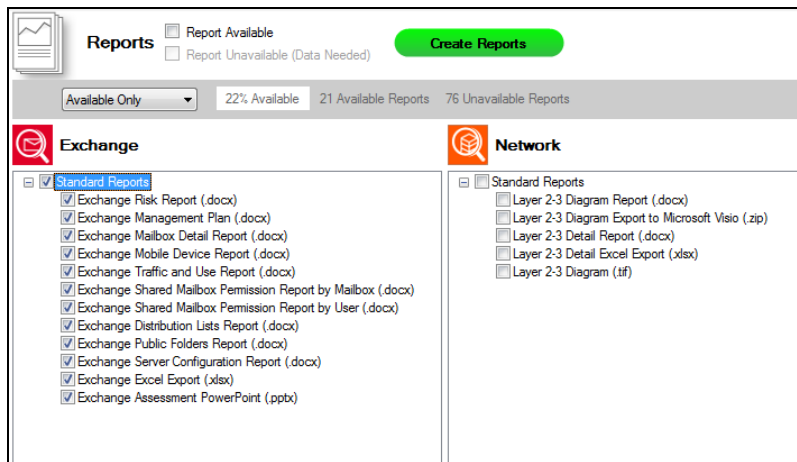


8. Once all of the scan data is imported into the **Assessment**, the assessment's **Checklist** will indicate that the **Reports** are ready to be generated.



Step 5 — Generate Exchange Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your Exchange Assessment, follow the steps below:



1. Run Network Detective Pro and log in with your credentials.
2. Then select the **Site**, go to the **Active Assessment**, and then select the **Reports** link to the center of the **Assessment Window** in order select the reports you want to generate.
3. Select the **Create Reports** button and follow the prompts to generate the reports you selected.
4. At the end of the report generation process, the generated reports will be made available for you to open and review.

Exchange Assessment Reports

The **Exchange Assessment** module can generate the following reports:

Standard Reports

Report Name	Description
Exchange Assessment	Use our generated PowerPoint presentation as a basis for conducting a meeting presenting your findings from the Network Detective. General

Report Name	Description
PowerPoint	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 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.

Report Name	Description
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 computers, 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 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

Report Name	Description
	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.

Performing a SQL Server Assessment

SQL Server Assessment Overview

The Network Detective **SQL Server Assessment Module** is composed of:

- the **SQL Server Assessment Data Collector** used to assess the integrity of the SQL Server database being scanned
- the **Network Detective Pro application** used to manage Sites and generate assessment reports

The Network Detective **SQL Server Assessment Module** is quick and easy to use. There are just a few basic steps:

1. Download and install the Network Detective Pro application

Visit <https://www.rapidfiretools.com/ndpro-downloads/> to download and install the Network Detective Pro application.

2. Create a New Site

Create Site files 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 SQL Server Assessment — or any other assessment type.

3. Start a New SQL Server Assessment

Once the **Site** is created, start a **New Assessment** and perform the SQL assessment data collection process using the guided **Checklist**.

4. Perform SQL Server Scan Data Collection

Run the SQL Server Assessment Data Collector on the target server. The output of the SQL scan will be an .DDF used to generate reports via Network Detective. **Be sure that you document the name of the folder used to store scan data to import into your assessment.** When the SQL Scan is complete, import the scan file into the assessment in Network Detective.

5. Generate SQL Server Assessment Reports

Customize your reports by setting up your company's branding of the report to be generated with your logos and client information, and run the reports. The Network Detective Report Wizard will step you through this process.

What You Will Need

SQL Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
SQL Assessment Data Collector	The Network Detective SQL Server Assessment Data Collector is a windows application that performs the data collections for the SQL Server Assessment Module.

Follow these steps to perform a SQL Server Assessment.

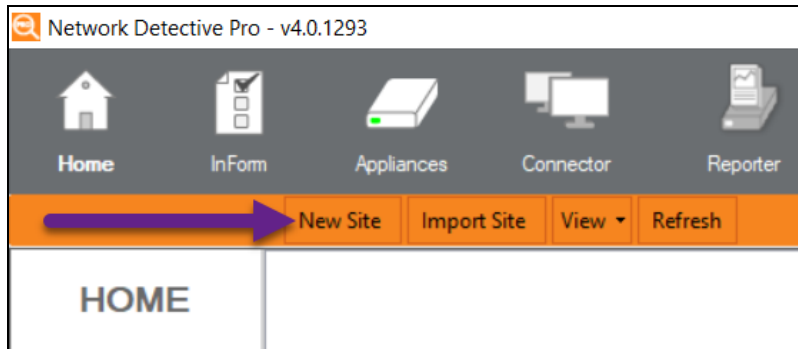
Step 1 — Download and Install the Network Detective Pro Application

Go to <https://www.rapidfiretools.com/ndpro-downloads/> to download and install the Network Detective Pro application. Then run Network Detective Pro and log in with your credentials.

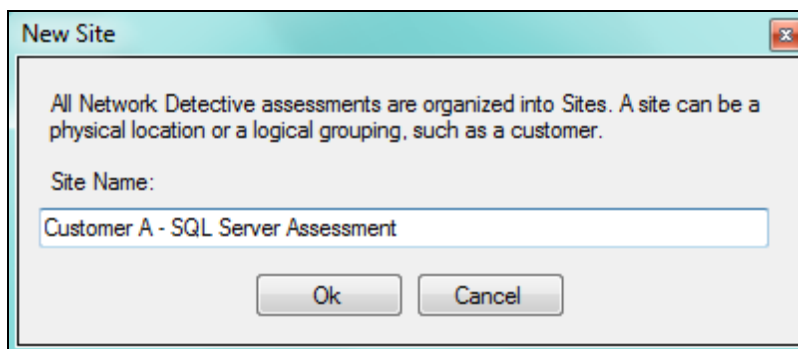
Step 2 — Create a New Site

To create a new site:

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

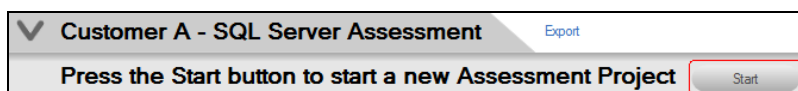


3. Enter a **Site Name** and click **OK**.

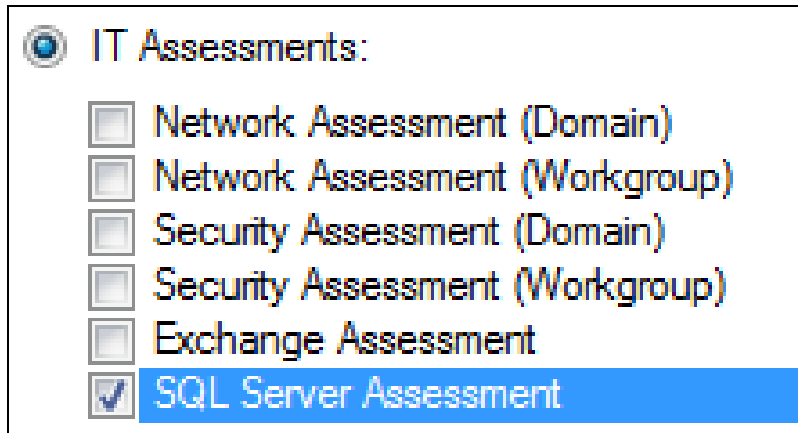


Step 3 — Start an SQL Server Assessment

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

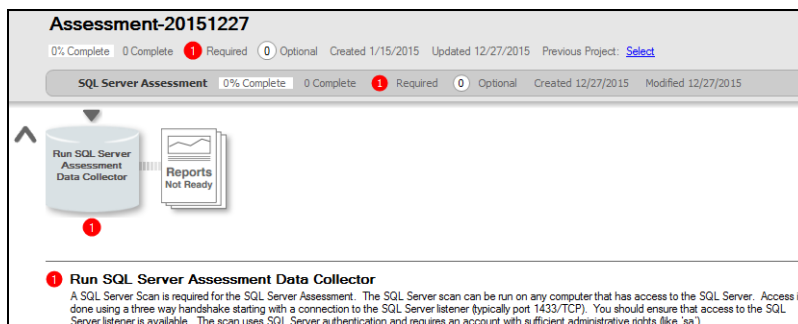


Next, select the **SQL Server Assessment** option presented.



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

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



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

Step 4 — Perform SQL Server Scan Data Collection

1. On the target network, log in to the local machine with **Administrator** privileges.
2. Download the **latest SQL Server Data Collector** program from <https://www.rapidfiretools.com/ndpro-downloads/> and save onto any machine that can connect to the SQL Server. You can also save the program to a USB drive and run it on the machine.

Note: This download is a self-extracting zip file and does not require installation when run on client systems. You may extract the SQL Server Data Collector files to a folder on either a machine that can connect to the SQL Server or a USB drive. Then you can run “RunSqlServerDataCollector.exe” to launch the GUI.

3. Right-click on the downloaded file and **run-as administrator** to ensure you are running with elevated credentials. (This is a self-extracting zip file and is completely non-invasive – it is not installed on any other machine on the client’s network.)
4. Next, after starting the **SQL Server Data Collector** enter the necessary credentials and follow the remaining wizard-driven prompts. You can use either:
 - **SQL Server credentials**, or:

SQL Server Data Collector - 1.11 (running on .NET version 2.0.50727.5485)

Credentials

The SQL Server Assessment Data Collector can use either Windows Authentication or SQL Server Authentication. SQL Server Authenticated account should have sufficient administrative privileges to collect data (i.e., 'sa').

Clicking Next will test your credentials and detect the version of SQL Server that is running. This can take up to 30 seconds in some cases.

Server:

Port: [default](#)

Authentication:

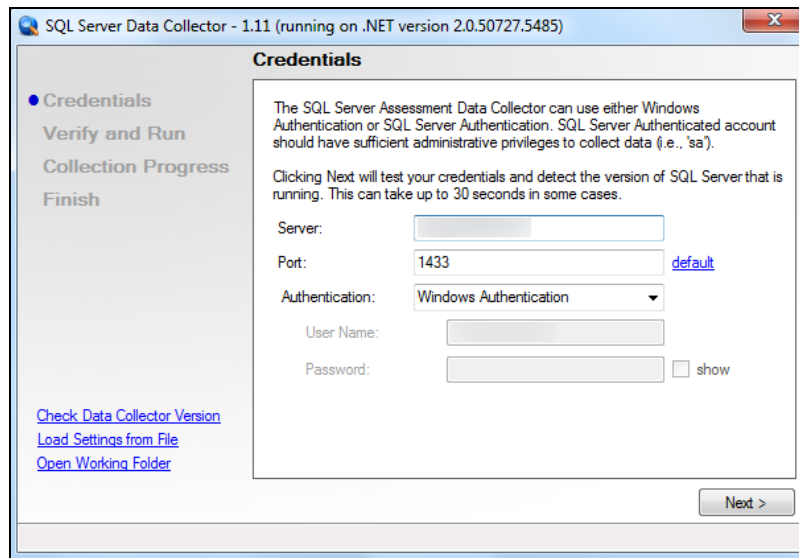
User Name:

Password: ☐ show

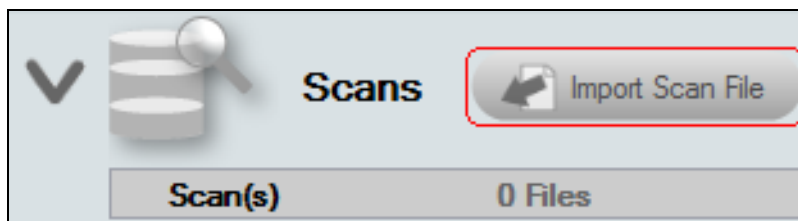
[Check Data Collector Version](#)
[Load Settings from File](#)
[Open Working Folder](#)

[Next >](#)

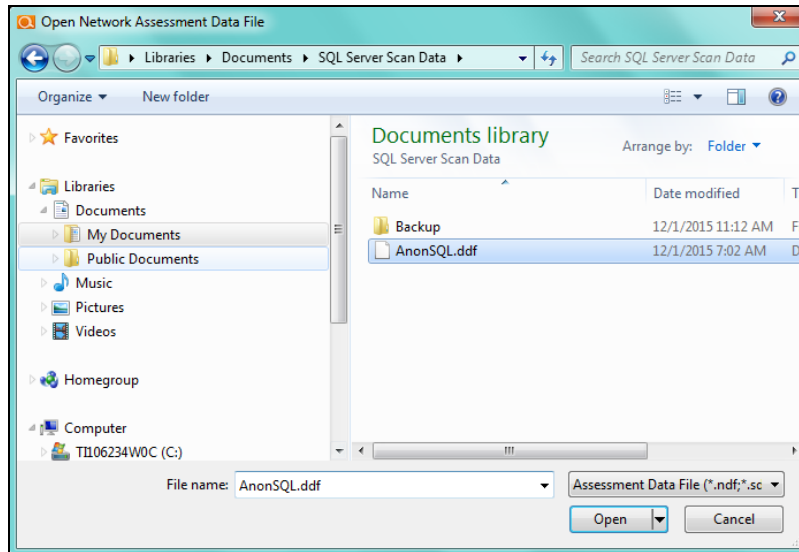
- **Windows Authentication** credentials.



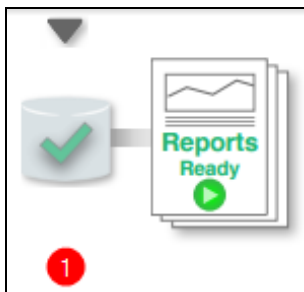
5. After the **SQL Server Scan** is complete, either save the scan results file to a USB drive for later importing of the results into the assessment or email the file for later access. **Make sure the USB has sufficient free space to extract and save the Data Collector files and to store the scan results data files.**
6. **Importing the SQL Server Scan file into your Assessment:** From within the **Scans** section of the **Assessment Window**, select the **Import Scan File** button.



7. Then, browse the folder storing the SQL Server Scan results data file generated by the SQL Server Data Collector, select the file, and then **Open** the file to import the scan results into your assessment.



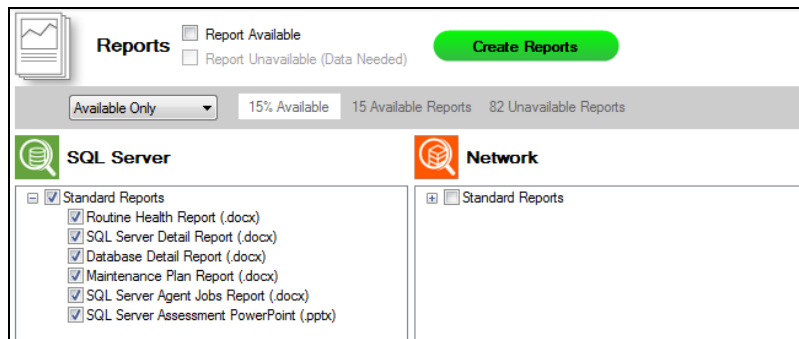
8. Once all of the scan data is imported into the **Assessment**, the assessment's **Checklist** will indicate that the **Reports** are ready to be generated.



Step 5 — Generate SQL Server Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your SQL Server Assessment, follow the steps below:

1. Run Network Detective Pro and login with your credentials.



2. Then select the **Site**, go to the **Active Assessment**, and then select the **Reports** link to the center of the **Assessment Window** in order select the reports you want to generate.
3. Select the **Create Reports** button and follow the prompts to generate the reports you selected.
4. At the end of the report generation process, the generated reports will be made available for you to open and review.

The **SQL Server Assessment** module can 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

Report Name	Description
	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.
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

Report Name	Description
	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.

SQL Server Assessment Reports

The **SQL Server Assessment** module can 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

Report Name	Description
	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.
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

Report Name	Description
	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.

Performing a Combined Network and Security Assessment

This quick start guide covers how use the **Network** and **Security** Assessment Modules to perform both assessments at the same time. You will save time and effort by collecting scan data to complete two checklists simultaneously. At the end, you will be able to generate both Network Assessment and Security Assessment reports.

Network Assessment Overview

The Network Assessment Module gives you the broadest insights of any IT assessment module. The Network Assessment Module has many every day uses for your MSP, including:

- Conducting full, 'deep-dive' network assessments
- Documenting your customers' networks as part of regular "Technology Reviews"
- Generating change management reports for clients
- Conducting IT SWOT Analyses to help your clients make better and more informed business decisions

Security Assessment Overview

The Security Assessment Module allows you to deliver IT security assessment services to your client – even if you aren't an IT security expert. The Security Assessment Module has many uses for your MSP, including:

- Generate executive-level reports that include a proprietary Security Risk Score and Data Breach Liability Report along with summary charts, graphs and an explanation of the risks found in the security scans.
- Identify network "share" permissions by user and computer. Provide comprehensive lists of all network shares, detailing which users and groups have access to which devices and files, and what level of access they have.
- Catalog external vulnerabilities including security holes, warnings, and informational items that can help you make better network security decisions. This is an essential item for many standard security compliance reports.
- Methodically analyze login history from the security event logs. The report uses mathematical modeling and proprietary pattern recognition to highlight potential

unauthorized users who log into machines they normally do not access and at times they normally do not log in.

What You Will Need

Security Assessment Component	Description
Network Detective Pro	The Network Detective Pro Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Pro Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
Network/Security Data Collector	The Network Detective Network/Security Data Collector is a windows application that performs the data collections for both the Network and Security Assessment Module.
Push Deploy Tool	The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.



Network Prerequisites for Network Detective Pro Scans

For a successful network scan:

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

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

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

Follow these steps to perform a combined Network and Security Assessment.

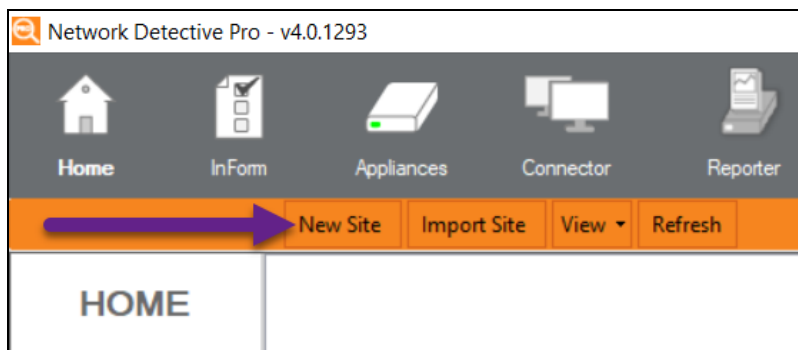
Step 1 — Download and Install the Network Detective Pro Application

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

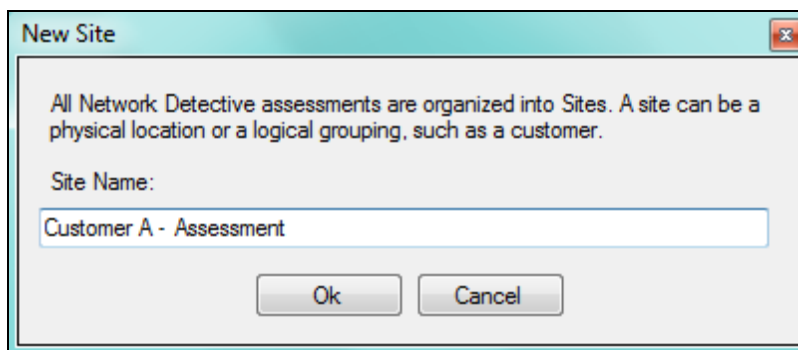
Step 2 — Create a New Site

To create a new site:

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



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

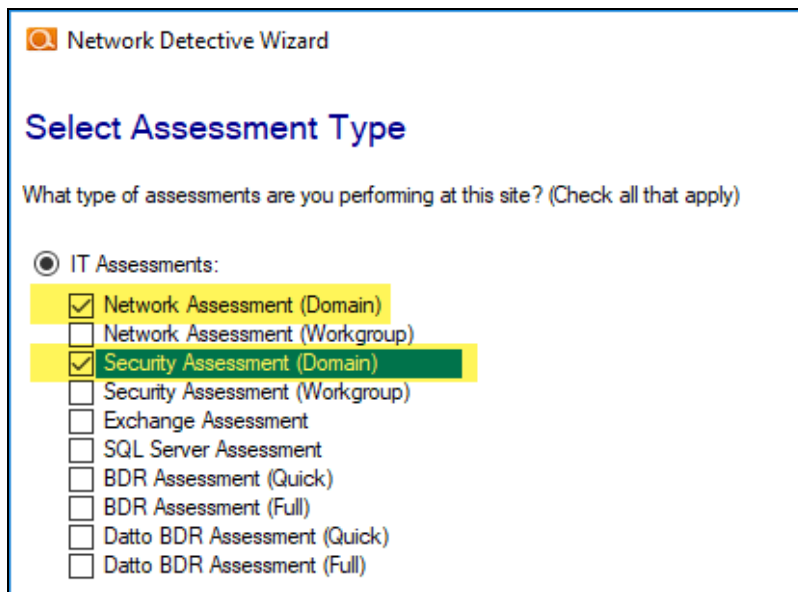


Step 3 — Start a Network and Security Assessment

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



Next, select both the **Network Assessment** and **Security Assessment** options presented.



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

2. Once the new assessments are started, a “**Checklist**” is displayed in the **Assessment Window** presenting the “**Required**” and “**Optional**” steps that are to be performed during the assessment process. Below is the **Checklist** for a **Network Assessment**.
3. You can switch between the Network and Security Assessment, as in the images below:

See Active Assessments and Completion Status

Click the triangle button to expand the list of assessments in the active project

Customer 1 Test / Edit Site | Assessments | Reports | Export

Assessment-20180430
0% Complete | 0 Complete | 3 Required | 2 Optional | Created 30-Apr-2018 03:12 PM | Updated 22-Oct-2018 12:03

Assessment	0% Complete	0 Complete	3 Required	2 Optional	Created	Updated
Network Assessment (Domain)	0% Complete	0 Complete	1 Required	1 Optional	Created	
Security Assessment (Domain)	0% Complete	0 Complete	2 Required	1 Optional	Created	

1 Run Network Detective Data Collector (NDDC) with the Network Scan

2 Run Computer Data Collector on computers that cannot be scanned remotely

Reports Not Ready

You can see a progress indicator and tasks completed for both assessments

1 Run the Network Detective Data Collector (NDDC) with the Network Scan
Run the Network Data Collector on the Domain Controller (if possible), a computer joined to the Domain if the Domain Controller is not available, or from any workstation on the network. The data collector should be run with Administrative privileges.

Switch Between Active Assessment Checklists

Click on an assessment to swap between checklists

Customer 1 Test / Edit Site | Assessments | Reports

Assessment-20180430
0% Complete | 0 Complete | 3 Required | 2 Optional | Created 30-Apr-2018 03:12 PM | Updated 22-Oct-2018 12:03

Assessment	0% Complete	0 Complete	3 Required	2 Optional	Created	Updated
Network Assessment (Domain)	0% Complete	0 Complete	1 Required	1 Optional	Created	
Security Assessment (Domain)	0% Complete	0 Complete	2 Required	1 Optional	Created	

The selected assessment checklist will appear

1 Initiate External Vulnerability Scan

2 Run Network Detective Data Collector (NDDC) with the Security Data ...

3 Run Network Detective Data Collector (NDDC) with the Security Data ...

Reports Not Ready

2 Run Network Detective Data Collector (NDDC) with the Security Data ...
Run the Security Data Collector with 'Perform Network Scan' option checked on the Domain Controller (if possible), a computer joined to the Domain if the Domain Controller is not available, or from any workstation on the network. The data collector should be run with Administrative privileges.

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

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

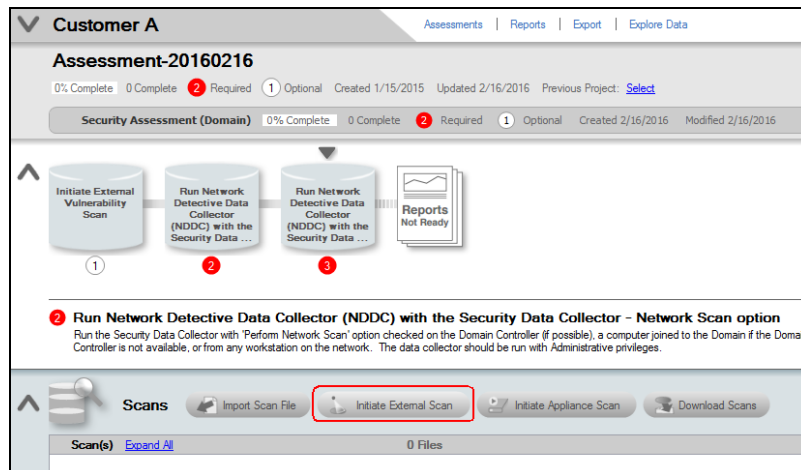


Step 4 — Initiate External Vulnerability Scan

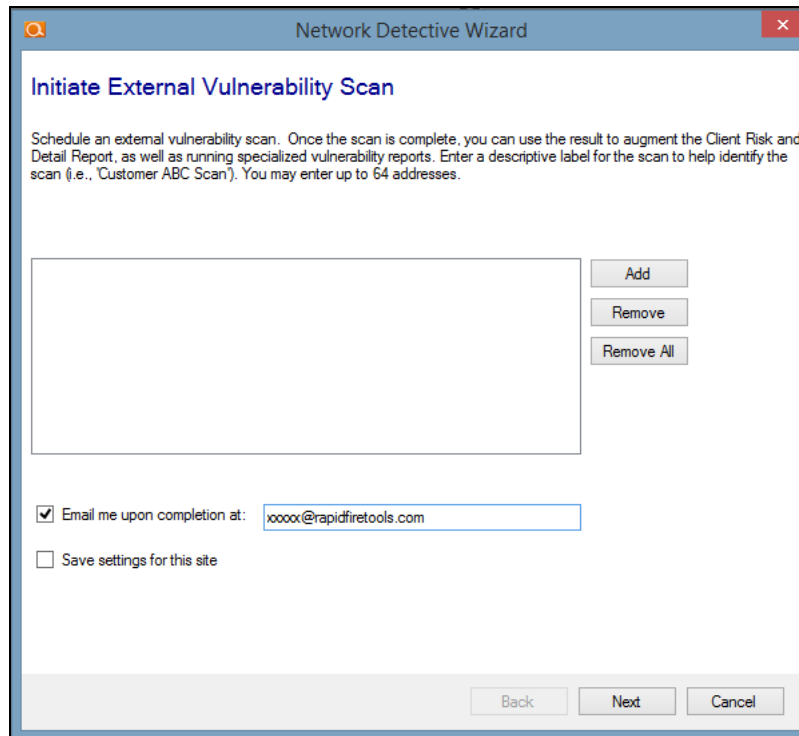
Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same

external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

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

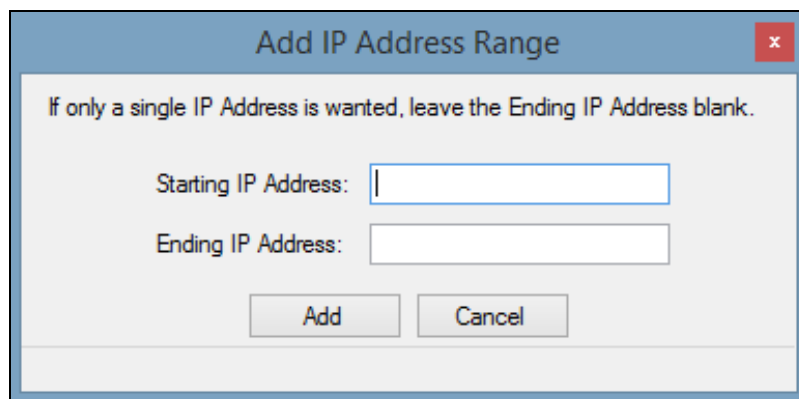


Enter the range of IP addresses you would like to scan. **You may enter up to 64 external addresses.**



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

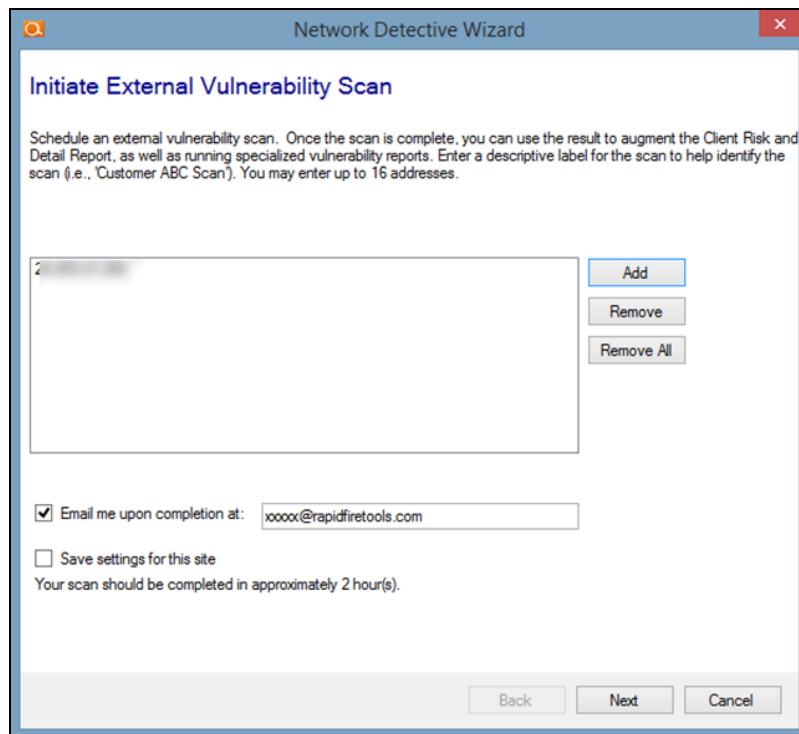
Select **Add** to add a range of external IP addresses to the scan. If you do not know the external range, you can use websites such as whatismyip.com to determine the external IP address of a customer.



The screenshot shows a dialog box titled "Add IP Address Range" with a close button in the top right. It contains the instruction: "If only a single IP Address is wanted, leave the Ending IP Address blank." Below this are two input fields: "Starting IP Address:" and "Ending IP Address:". At the bottom are two buttons: "Add" and "Cancel".

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

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



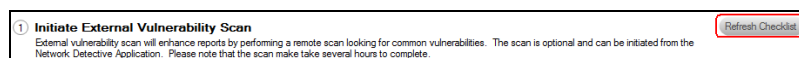
The screenshot shows a window titled "Network Detective Wizard" with a sub-header "Initiate External Vulnerability Scan". The text inside reads: "Schedule an external vulnerability scan. Once the scan is complete, you can use the result to augment the Client Risk and Detail Report, as well as running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

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

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

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

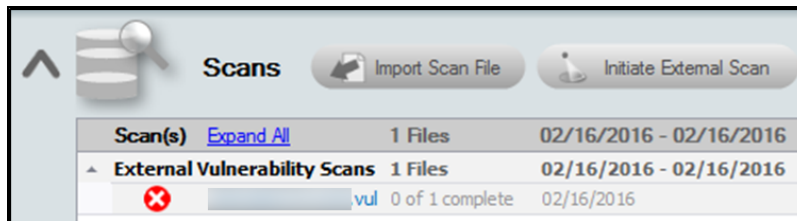
Next, select the **Refresh Checklist** option to update the status of the **External Vulnerability Scan** that is listed under the **Scans** bar.



The screenshot shows a status bar with a red circle containing a '1' next to the text "Initiate External Vulnerability Scan". Below this text is a small paragraph: "External vulnerability scan will enhance reports by performing a remote scan looking for common vulnerabilities. The scan is optional and can be initiated from the Network Detective Application. Please note that the scan make take several hours to complete." To the right of this text is a button labeled "Refresh Checklist".

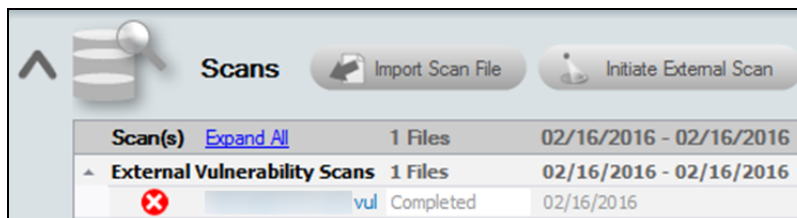
The **Assessment Window** and associated **Scans** listed under the **Scans** bar at the bottom of the **Assessment Window** will be updated to reflect the External Vulnerability Scan has been initiated and its completion is pending.

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



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

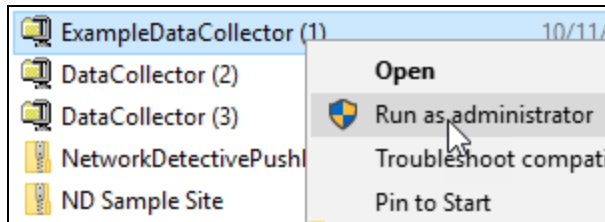
Upon the scan's completion, note that the **External Vulnerability Scan** with its **"Completed"** status will be listed as an imported scan under the **Scans** bar at the bottom of the **Assessment Window** as presented below.



Step 5 — Collect Data using Data Collector

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

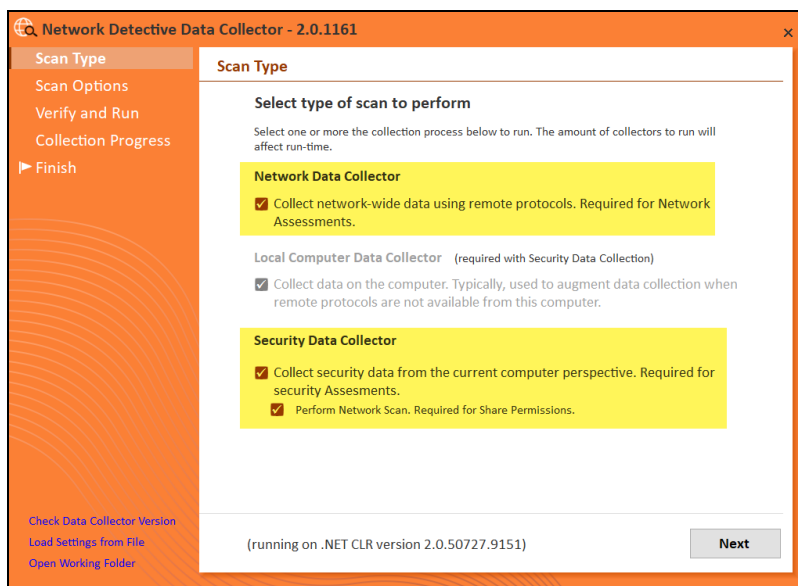
1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/ndpro-downloads/> and download the Network Detective Data Collector.
2. Run the **Network Detective Data Collector** executable program as an Administrator (**right click>Run as administrator**).



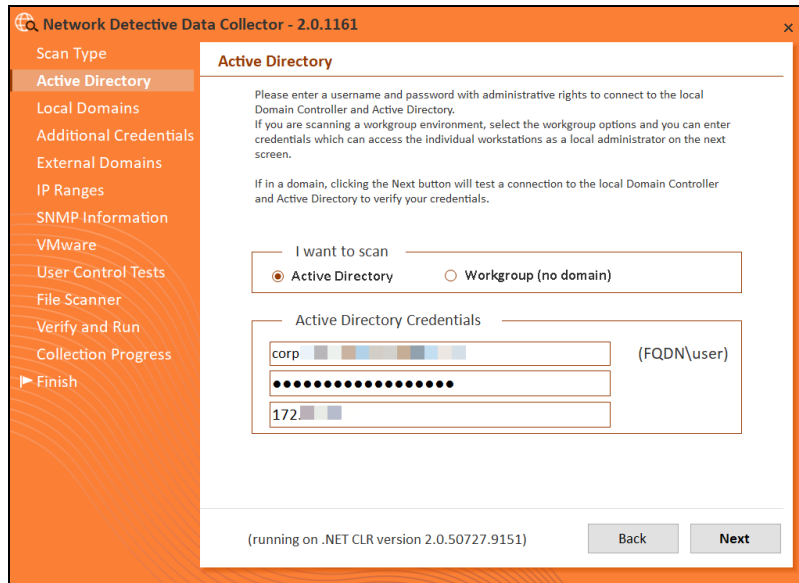
Important: For the most comprehensive scan, you **MUST** run the data collector as an **ADMINISTRATOR**.

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.

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



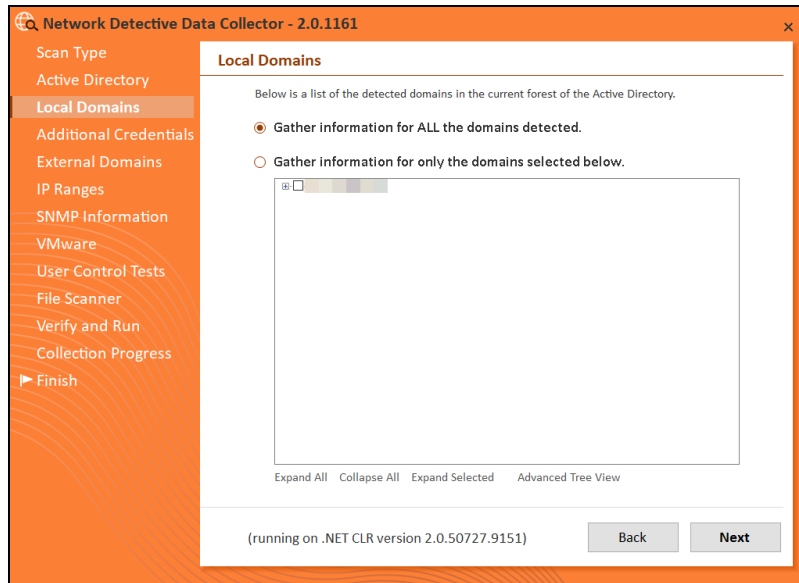
5. The **Active Directory** window will appear. Select the type of network you are scanning (*Active Directory domain* or *Workgroup*).



Next enter the required administrative credentials to access the network during the scan.

- If in a domain, enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. Click **Next** to test a connection to the local Domain Controller and Active Directory to verify your credentials.
 - If you are scanning a Workgroup environment, select Workgroup, click **OK**, and skip to #7.
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**.

Note: If you select to scan a Workgroup, the Network Detective Data Collector will skip this step.



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. Click **Next**.

Note: If you selected Workgroup on the Active Directory window, enter credentials which can access the individual workstations as a local administrator.

Network Detective Data Collector - 2.0.1161

Scan Type
Active Directory
Local Domains
Additional Credentials
External Domains
IP Ranges
SNMP Information
VMware
User Control Tests
File Scanner
Verify and Run
Collection Progress
▶ Finish

Additional Credentials

Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

Username
Password Add

corp. (AD user to be used first)

Clear All Entries

(running on .NET CLR version 2.0.50727.9151) Back Next

8. Input the **External Domains** here to include them as part of the data collection. **External Domain** names allow others to visit the target site and facilitate services, such as email. Examples of **External Domains** include:

- example.com
- mycompany.biz

Network Detective Data Collector - 2.0.1161

Scan Type
Active Directory
Local Domains
Additional Credentials
External Domains
IP Ranges
SNMP Information
VMware
User Control Tests
File Scanner
Verify and Run
Collection Progress
▶ Finish

External Domains

List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.

Domain Add

Clear All Entries Import from Text File

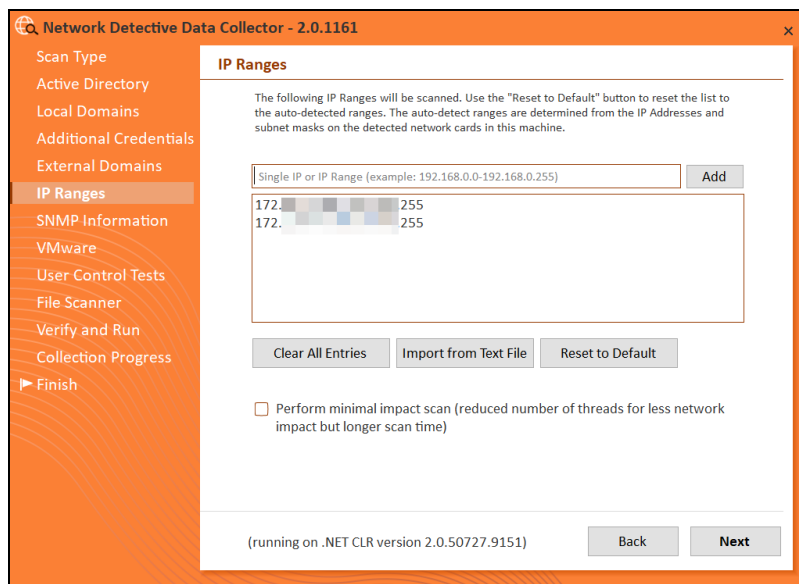
☒ Perform Dark Web Scan for Compromised Passwords

Please enter 1 or more external domains for the Dark Web scan.

(running on .NET CLR version 2.0.50727.9151) Back Next

Note: Perform Dark Web Scan for Compromised Passwords: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. If any compromised credentials exist for these domains, they will appear in your assessment reports. This service will return the first 5 compromised passwords for each domain specified.

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**.

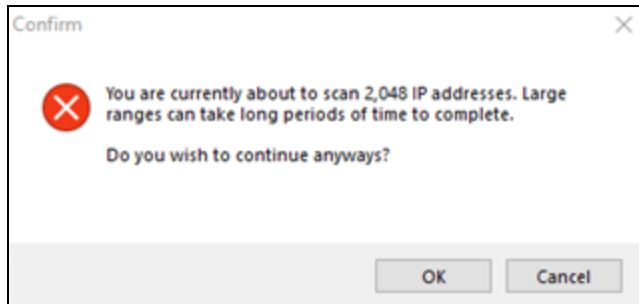


From this screen you can also:

- 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.

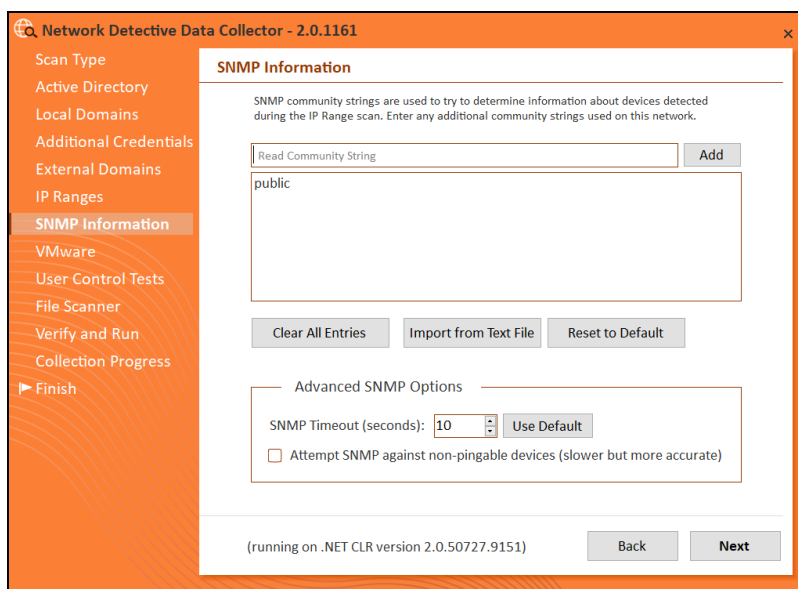
Important: Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

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** screen will appear. By default, the software will retrieve data from devices with the community string “public.” If desired, define an additional community string (such as “private”) and enter it here.



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

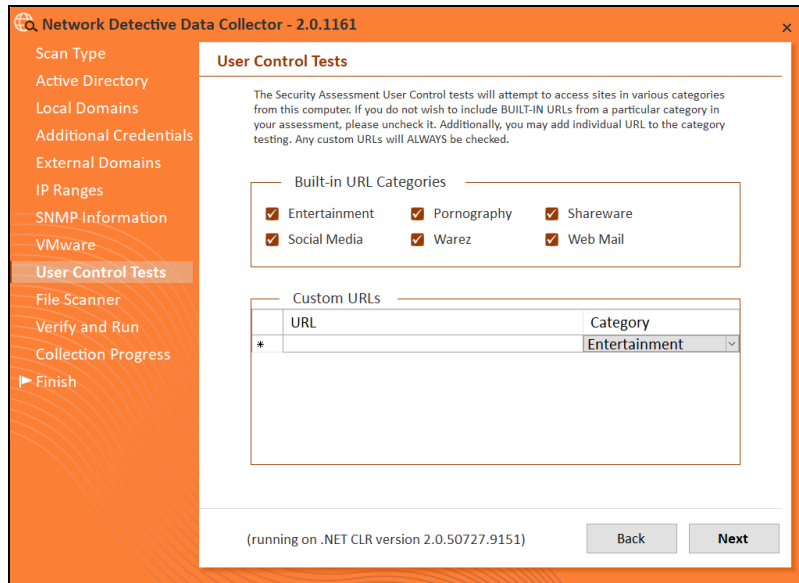
steps in this guide and **use the Push Deploy Tool as instructed**. This will collect information such as Patch Analysis for all Windows operating systems.

11. Input the **Hostname** or **IP Address** and **Credentials** of the VMware Servers that you would like to include in the scanning process.

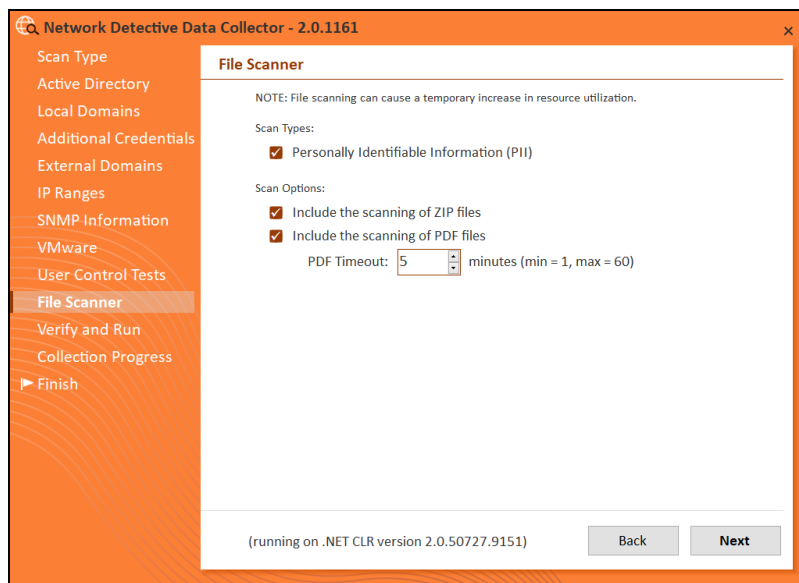
The screenshot shows the 'VMware' configuration window in the 'Network Detective Data Collector - 2.0.1161' application. The left sidebar contains a list of options: Scan Type, Active Directory, Local Domains, Additional Credentials, External Domains, IP Ranges, SNMP Information, VMware (selected), User Control Tests, File Scanner, Verify and Run, Collection Progress, and Finish. The main panel has a title bar 'VMware' and a subtitle 'VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials.' Below this are three input fields: 'Hostname or IP Address', 'Username', and 'Password'. To the right of the 'Hostname or IP Address' field is a checkbox labeled 'Skip connection test'. Below the input fields is an 'Add VMware Server' button. A table with three columns, 'Host', 'User', and 'Connection Verified', is shown below the buttons. At the bottom of the main panel are 'Clear All Entries' and 'Test All Connections' buttons. The footer of the window displays '(running on .NET CLR version 2.0.50727.9151)' and 'Back' and 'Next' buttons.

Host	User	Connection Verified
------	------	---------------------

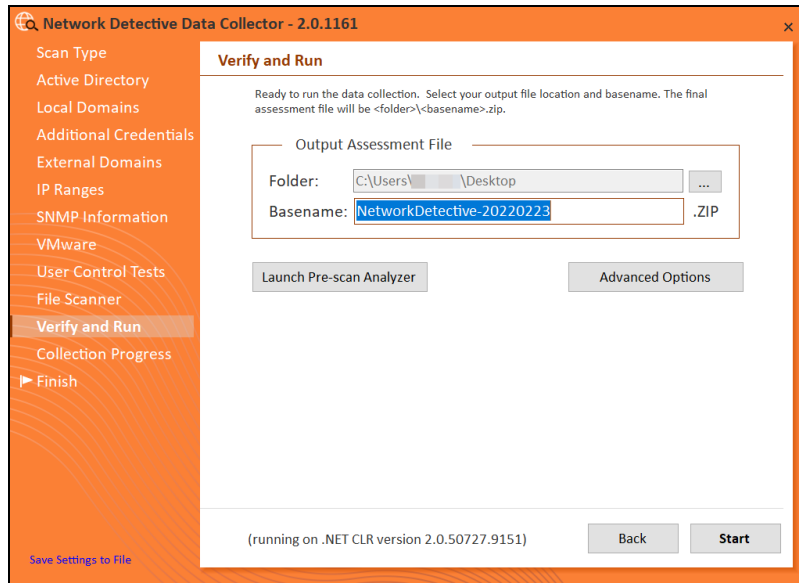
12. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter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



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



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

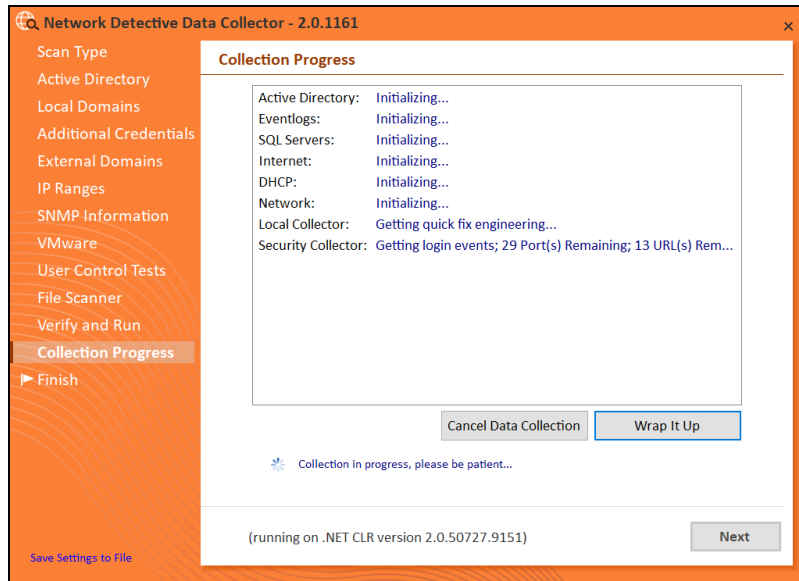


Tip: Use the **Pre-scan Analyzer** to identify and correct any configuration issues prior to running the Network Scan. The **Push Deploy** tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion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

Overview Result Summary Active Directory SQL Server Network Computers Push Deploy						
Pushing local data collectors to remote computers requires WMI, Admin\$ access, and .NET 3.5 or above.						
Showing: All Nodes						
Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status
APP01.CORP.RAPIDFIRETO...		✓	✗			WMI failed. The RPC server is unavailable.
BROWN-WIN10.CORP.RAP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-095DFE1.CORP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-1HM0E71.CORP...		✓	✗			WMI failed. The RPC server is unavailable.
DESKTOP-6ND4Q80.CORP...	172.18.0.207	✓	✓	✓	✓	Full access
DESKTOP-7DBVA30.CORP...	10.236.83.1...	?	?			Accessing WMI...
DESKTOP-7RF9K75.CORP...		✓	✗			WMI failed. The RPC server is unavailable.

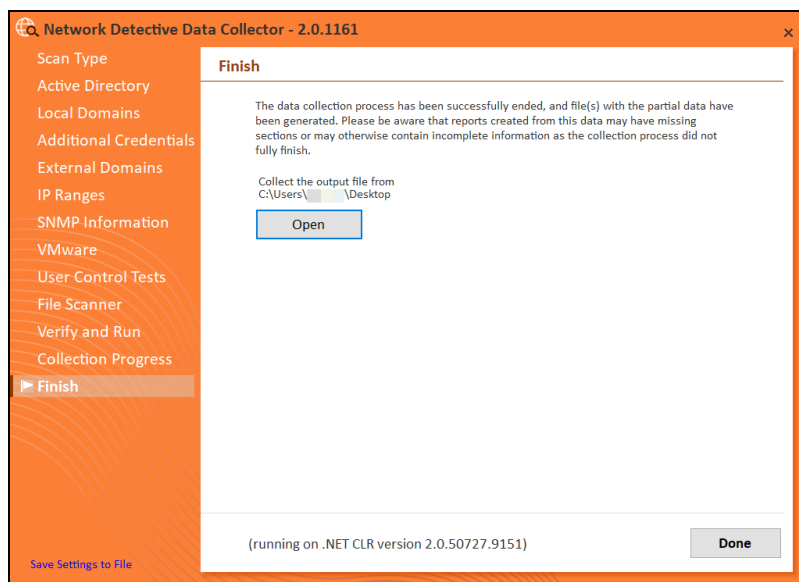
Enter any **Comments** and then click **Start**.

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



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

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

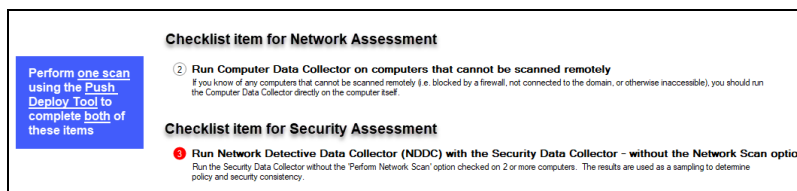


Click **Done** to close the **Network Detective Data Collector** window. Note the location where the scan's output file is stored.

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

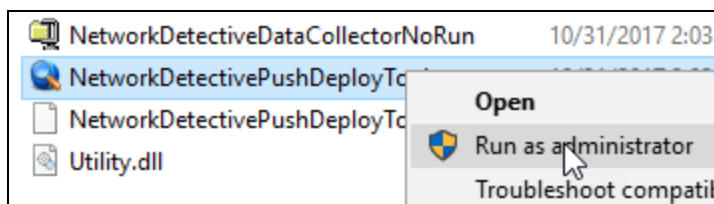
Tip: The **Push Deploy Tool** performs a localized scan on each workstation on the target network. **Perform this required step** to gather maximum data for the most detailed reports.

We recommend using the Push Deploy Tool to complete your remaining assessment tasks for both the Network and Security Assessments. These tasks appear in the guided checklist and are pictured below:



Download and run the Push Deploy Tool on a PC on the target network. It can quickly perform local data scans on all computers without the need to run the Data Collector on each computer separately. To do this:

1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/ndpro-downloads/> and download the Push Deploy Tool.
2. **Unzip** the files onto a USB drive or directly onto any machine on the target network.
3. From within the unzipped folder, run the **NetworkDetectivePushDeployTool.exe** executable program as an Administrator (**right click>Run as administrator**).



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

The Push Deploy Tool Settings and Configuration window will appear.

4. Set the **Storage Folder location** and select the **Security Scan** option.

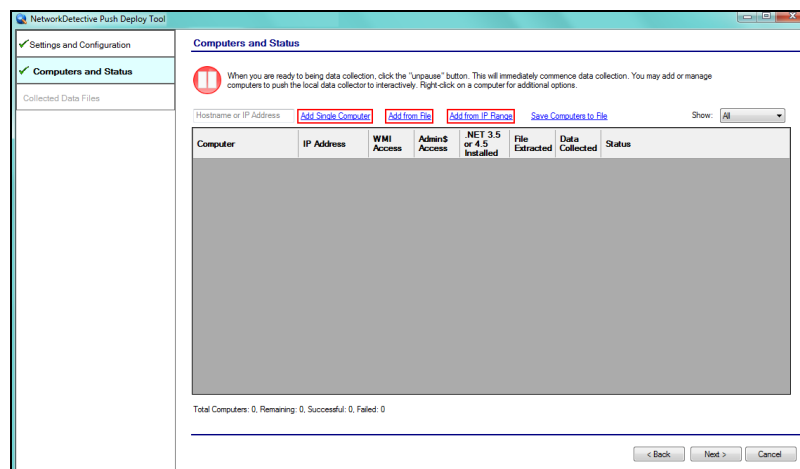
Tip: For your convenience, create a shared network folder to centralize and store all scan results data files created by the **Push Deploy Tool**. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

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

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

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

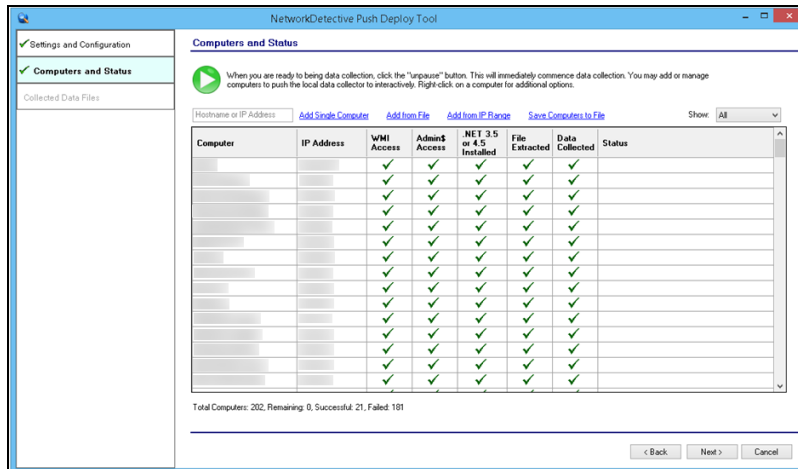
5. Click **Next** after you have configured the Push Deploy Tool.
6. The **Computers and Status** window will appear. From here you can:
 - **Add a Single Computer** to be scanned
 - **Add (computers) from File** that are to be scanned
 - **Add (computers) from IP Range** that are to be scanned
 - Or **Save Computers to File** in order to export a list of computers to be scanned again in future assessments



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

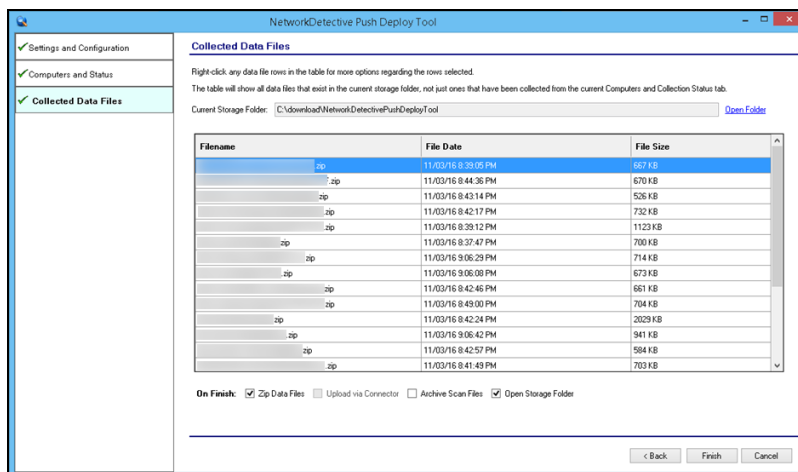
After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the **Computers and Status** window.

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



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

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



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

MORE INFO:

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

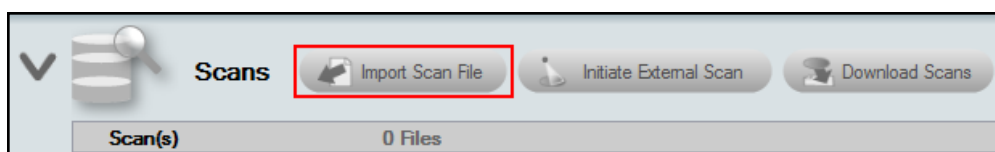
The output files (.ZIP, files) from the local scans can be stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.

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

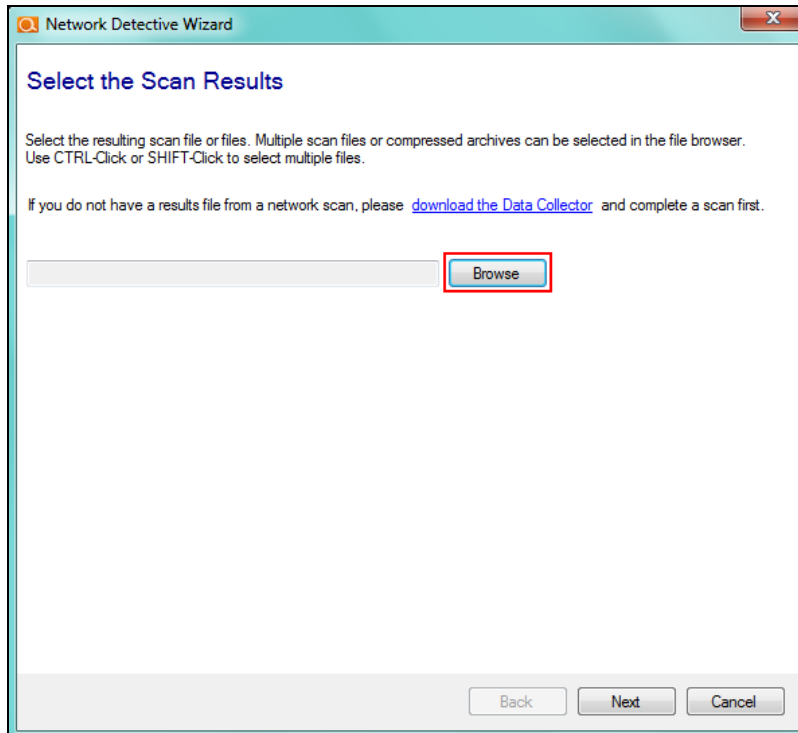
Step 7 — Import Scans into Network Detective Pro App

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

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



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

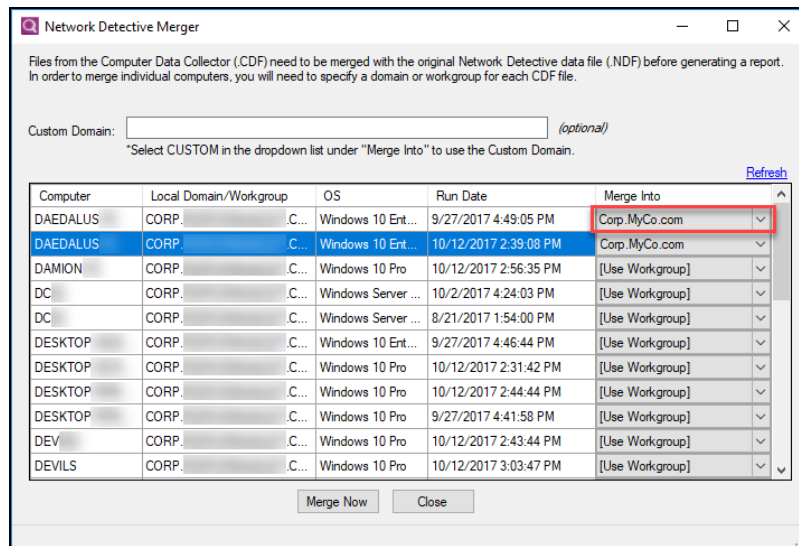


2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.

Tip: You do not need to unzip the files. You can also upload multiple files at once!

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

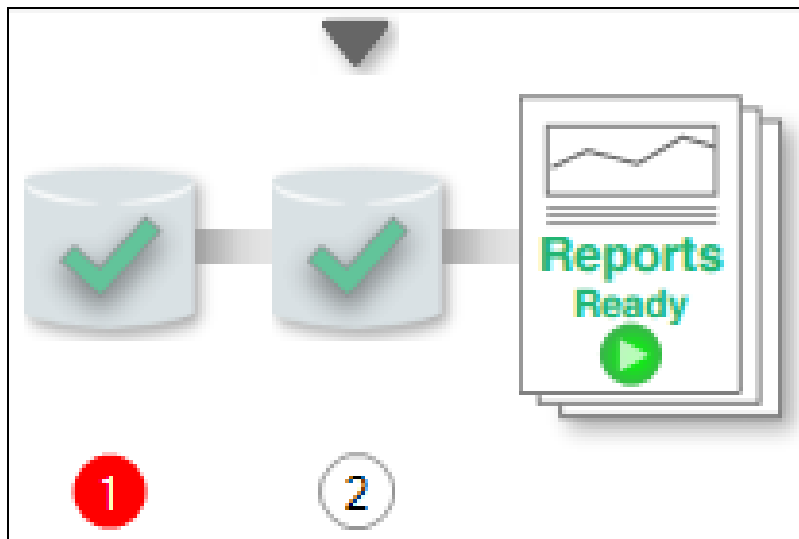
Click **Merge Now**.



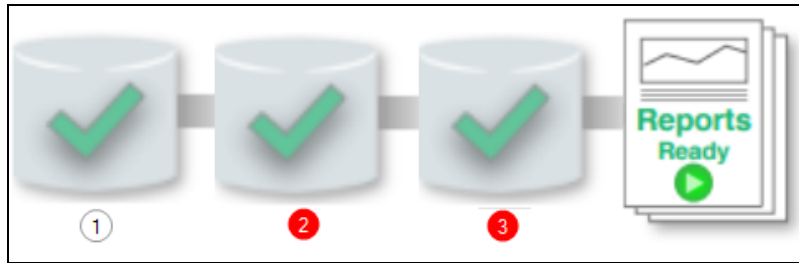
The **Scans** bar will be updated with the imported scan files.

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

Completed Checklist for Network Assessment



Completed Checklist for Security Assessment



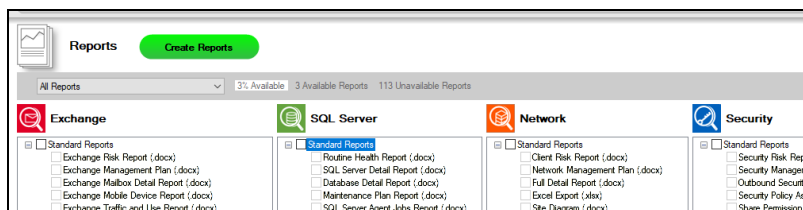
The status for both assessments will also appear as 100 percent complete:

Assessment-20180430					
100% Complete	5 Complete	0 Required	0 Optional	Created 30/04/2018 03:12 PM	Updated 24/10/2
▼ Network Assessment (Domain)	100% Complete	2 Complete	0 Required	0 Optional	
Security Assessment (Domain)	100% Complete	3 Complete	0 Required	0 Optional	

Step 8 — Generate Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective Pro should be installed on your workstations or laptop. Install Network Detective Pro from <https://www.rapidfiretools.com/ndpro-downloads/> if you have not already done so. To generate the reports for your Security Assessment, follow the steps below:

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



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

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 3.5 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 <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
☐	Allow <i>File and printer sharing</i> 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 <i>Remote Registry</i> “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 <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: - operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices - to send ICMP echo reply messages in response to an ICMP echo request Note: ICMP requests are used to detect active Windows computers and network devices to scan.
GPO Configuration for Windows Services	
☐	<i>Windows Management Instrumentation (WMI)</i> Startup Type: Automatic
☐	<i>Windows Update Service</i> Startup Type: Automatic
☐	<i>Remote Registry</i> Startup Type: Automatic
☐	<i>Remote Procedure Call</i> Startup Type: Automatic

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

Complete?	Workgroup Configuration
<input data-bbox="284 294 324 336" type="checkbox"/>	Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request Note: ICMP requests are used to detect active Windows computers and network devices to scan.

Enable Discovery Agents for Local Data Collection (Network Detective Pro)

The Discovery Agent for is a lightweight, streamlined option for collecting local data from specific network endpoints. Discovery Agents generate local scan files that are passed to your site via a secure connection. You can install any number of Discovery Agents for an organization, where they will perform local scans on the days of the week you designate.

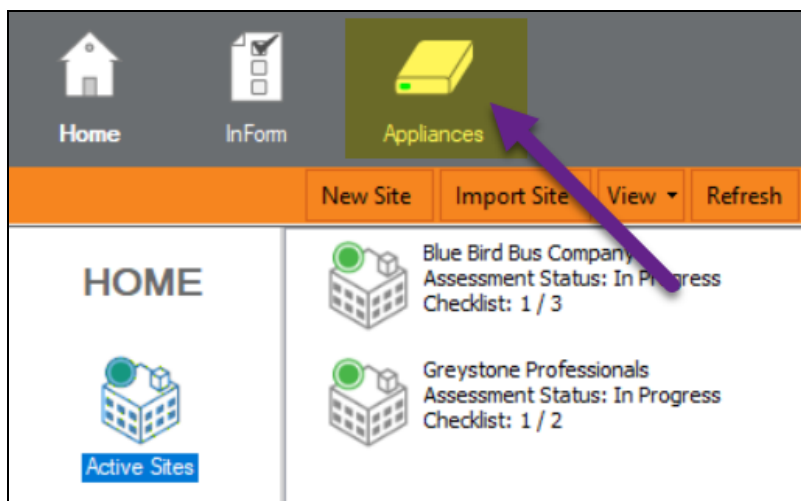
By assigning labels to your Agents, you can filter the scan data that you import into your assessment projects. Finally, you can combine Discovery Agents with other data collectors to customize your IT assessment for your exact purpose.

Follow the steps below to enable Discovery Agents for your site and use them to perform local scans:

Step 1 — Enable Discovery Agents via RapidFire Tools Portal

In the first step, enable Discovery Agents at the organization level using the RapidFire Tools Portal.

1. From the Network Detective Pro app, click **Appliances** from the top menu.



2. Click **Discovery Agents** from the left menu.

Reporters Remote Data Collectors Discovery Agents		NDA: [redacted]	Virtual	Cyber Hawk SDS
		NDA: [redacted]	Virtual	All
		NDA: [redacted]	Virtual	Compliance Manager
		EVS: [redacted]	Virtual	Vulnerability Scan...
		NDA: [redacted]	Virtual	Vulnerability Scan...
		PVS: [redacted]	Virtual	Vulnerability Scan...
		NDA: [redacted]	Virtual	Cyber Hawk SDS
		NDA: [redacted]	Server	All
		NDA: [redacted]	Virtual	Inspector
		NDA: [redacted]	Server	Cyber Hawk SDS
		NDA: [redacted]	Server	Cyber Hawk SDS
		NDA: [redacted]	Physical	Inspector
		NDA: [redacted]	Virtual	Inspector

- Open the "**Click here to log in to the RapidFire Tools Portal**" link.

Discovery Agents are managed at the Organization level and can be managed in the RapidFire Tools Portal

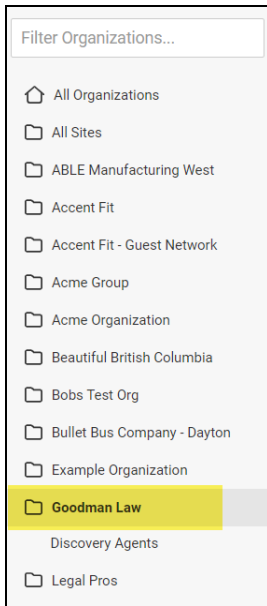
[Click here to log in to the RapidFire Tools Portal](#)

Learn more from the video below.

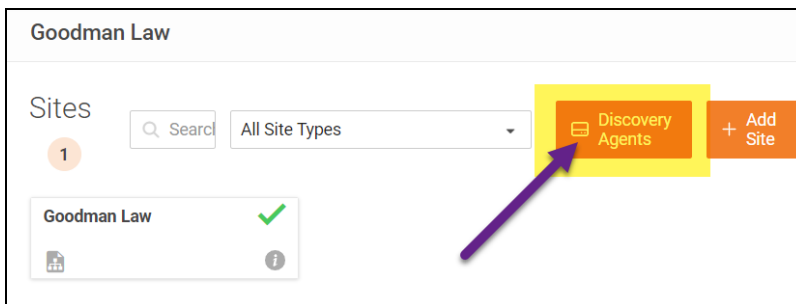
ORGANIZATION DISCOVERY AGENTS (NETWORK DETECTIVE PRO)

- Sites that you create in Network Detective Pro are also created in the RapidFire Tools Portal. The sites will appear in an organization with the same name as your site.
- From the left menu, find the organization with the same name as your site. **Click on the org.**

Note: You can later rename orgs or move sites between orgs whenever you choose.

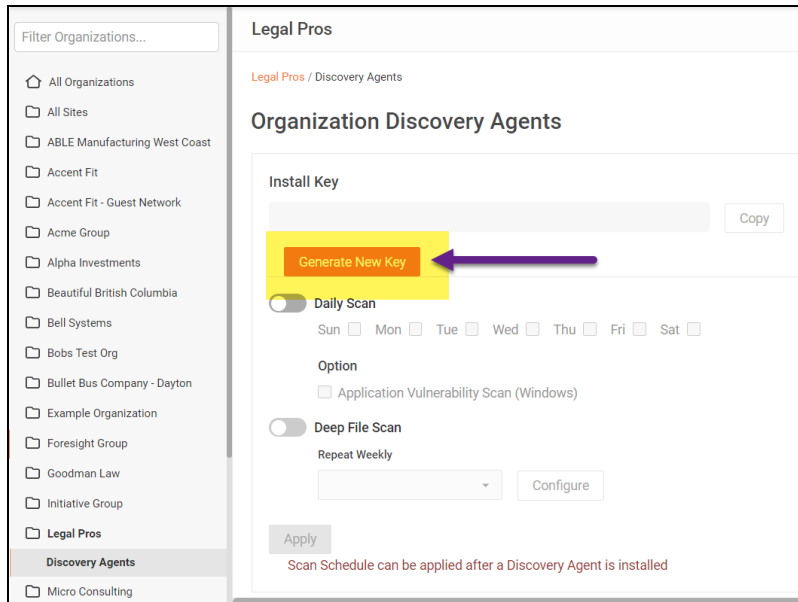


6. Click **Discovery Agents** from the right page.



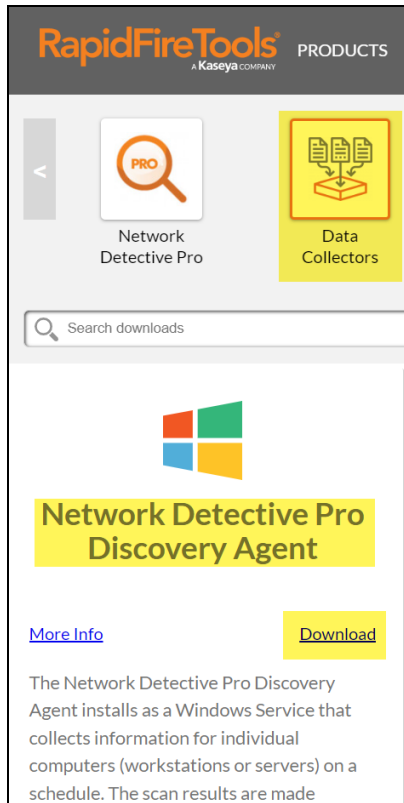
Note: The organization must contain at least one site for you to access to Discovery Agents.

7. From the Organization Discovery Agents page, click **Generate New Key**. Copy the **Install Key** to your clipboard. You will use this to install Discovery Agents for this organization.



Step 2 — Install Discovery Agent(s)

1. Download the Discovery Agent from <https://www.rapidfiretools.com/ndpro-downloads/>. You can download the Agent installer from **Data Collectors** > **Network Detective Pro Discovery Agent**.

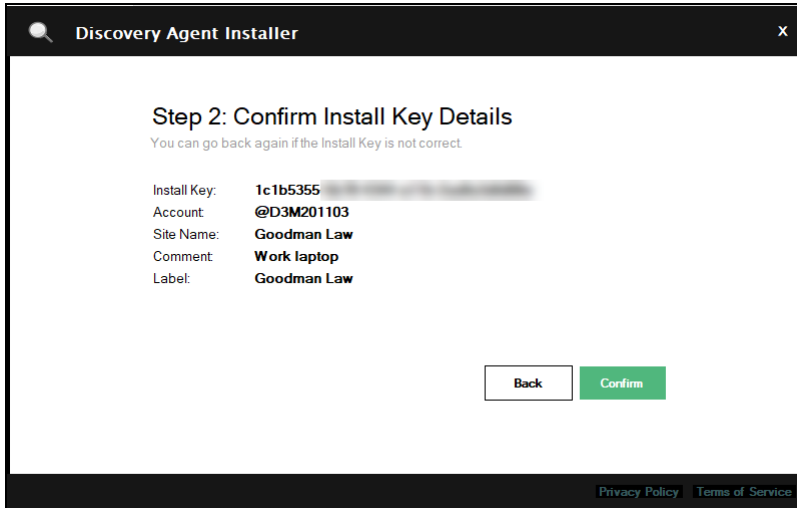


2. Open the app, proceed through the setup prompts, and click **Install**.
3. Confirm that you want to allow the Discovery Agent to make changes to your device. Once you finish the wizard, the Discovery Agents Installer will open.
4. **Enter the install key** that you generated in the previous step. Also **enter a "label"** to help you identify the endpoint on which the agent is installed. You will later use the label to import the correct scan data into your assessment projects.

The screenshot shows the "Discovery Agent Installer" window. The title bar includes a search icon, the text "Discovery Agent Installer", and a close button. The main content area is titled "Step 1: Enter Install Key". It contains three input fields: "Enter the Install Key for this Installation" with the value "1c1b5355-5b78", "Enter a comment to help identify this computer (optional)" with the value "Work laptop", and "Enter a 'label' to make it easier to select and use Discovery Agents (optional)" with the value "Goodman Law". A green "Continue" button is located at the bottom right. At the bottom of the window, there are links for "Privacy Policy" and "Terms of Service".

Finally, **enter an optional comment** to help identify the PC hosting the Agent.

5. Next, **Confirm** the site and key details for the Discovery Agent.



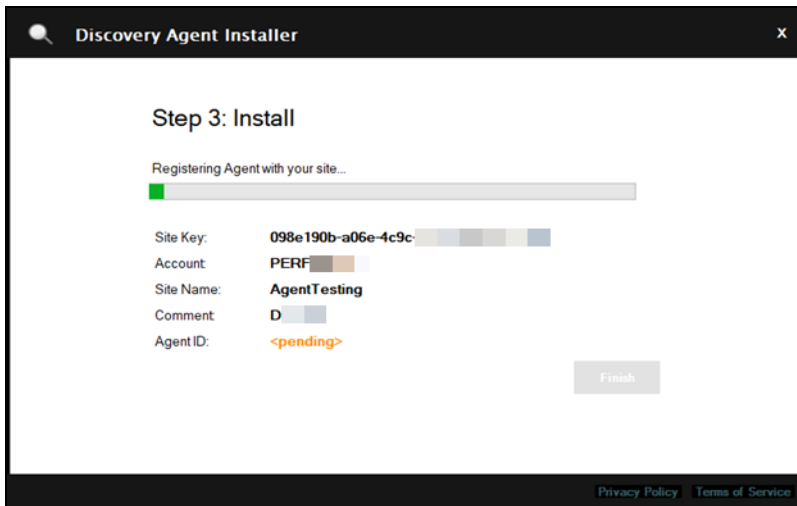
The screenshot shows the 'Discovery Agent Installer' window at Step 2: Confirm Install Key Details. The title bar includes a magnifying glass icon, the text 'Discovery Agent Installer', and a close button 'x'. The main content area has the heading 'Step 2: Confirm Install Key Details' and a subtext 'You can go back again if the Install Key is not correct.' Below this, the following details are listed: Install Key: 1c1b5355, Account: @D3M201103, Site Name: Goodman Law, Comment: Work laptop, and Label: Goodman Law. At the bottom right, there are 'Back' and 'Confirm' buttons. The footer contains links for 'Privacy Policy' and 'Terms of Service'.

Install Key:	1c1b5355
Account:	@D3M201103
Site Name:	Goodman Law
Comment:	Work laptop
Label:	Goodman Law

Back Confirm

Privacy Policy Terms of Service

6. The installer will begin registering the Agent for your organization.



The screenshot shows the 'Discovery Agent Installer' window at Step 3: Install. The title bar includes a magnifying glass icon, the text 'Discovery Agent Installer', and a close button 'x'. The main content area has the heading 'Step 3: Install' and a progress bar labeled 'Registering Agent with your site...'. Below the progress bar, the following details are listed: Site Key: 098e190b-a06e-4c9c, Account: PERF, Site Name: AgentTesting, Comment: D, and Agent ID: <pending>. A 'Finish' button is located at the bottom right. The footer contains links for 'Privacy Policy' and 'Terms of Service'.

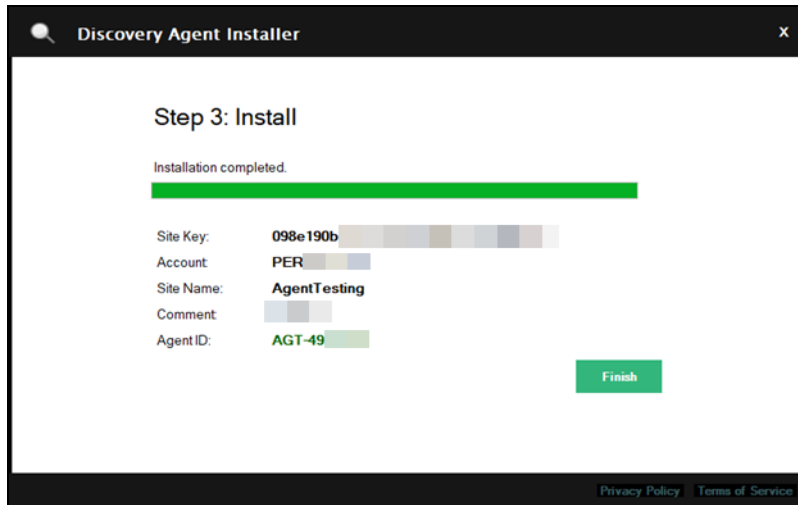
Registering Agent with your site...

Site Key:	098e190b-a06e-4c9c
Account:	PERF
Site Name:	AgentTesting
Comment:	D
Agent ID:	<pending>

Finish

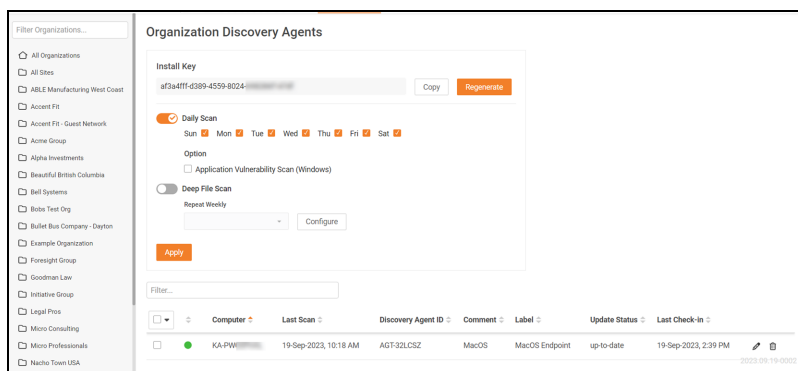
Privacy Policy Terms of Service

7. Click **Finish** when complete.



Step 3 — Confirm Discovery Agent install for your Organization

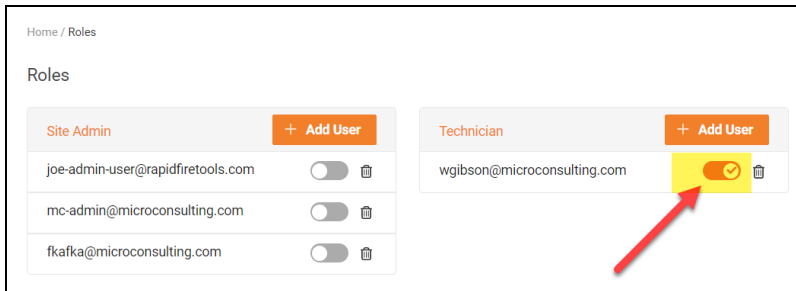
1. Once you've installed the Agent(s) on the target network, return to the portal and navigate to **[Your Organization] > Discovery Agents**.
2. Under installed Discovery Agents, you will see the new Agent.
3. The appliance status will appear as green once the Agent checks in with the RapidFire Tools Portal.



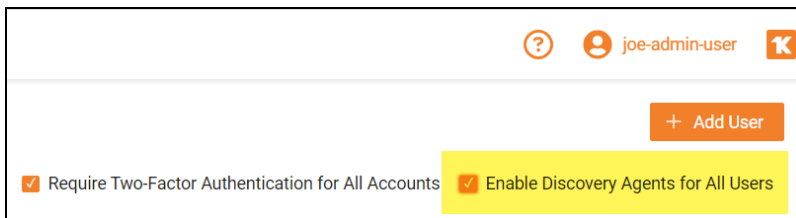
Step 4 — (Optional) Enable Access for Site Admin and Technician Users

Next, you can optionally enable your Site Admin and Technician portal users to manage the Discovery Agents that you deploy. You can do this in two ways:

1. From your site, access **Roles**. Next to your Site Admin and/or Technician users, **turn on the slider**. These users can then access and manage Discovery Agents for the organization that contains the site.



2. Alternatively, if you want to enable access to Discovery Agents for all Site Admin and/or Technician Users in the portal, navigate to **Global Settings > Users**. From the top-right page, select **Enable Discovery Agents for All Users**. All site-restricted Site Admin and Technician users can then manage Discovery Agents for their assigned organizations and sites.



Step 5 — Assign Labels to Agents

If you didn't assign a label to your agent(s), be sure to do so now. To assign labels to agents:

1. Navigate to **[Your Organization] > Discovery Agents**.
2. **Select the agents** where you want to add or edit labels.

Option

☒ Application Vulnerability Scan (Windows)

☐ Deep File Scan

Repeat Weekly

Configure

Apply

Filter...

☒	Computer	Last Scan	Discovery Agent ID	Comment
☒	DESKTOP-	19-Sep-2023, 4:18 PM	AGT-23	10.200.1.140
☒	DESKTOP-	19-Sep-2023, 4:18 PM	AGT-76	DevTest Network VulScan Agent

Showing 1 - 2 of 2 Items

3. Click the **Select All** button, and then click **Update Label**.

☒	Computer	Last Scan	Discovery Agent ID	Comment	Label
1 Selected	W	03-Feb-2023, 3:02 PM	AGT-37B	Work laptop	Goodman Law

- Run Scan Now
- Update Now
- Cancel Scans
- Remove Agents
- Update Comment
- Update Label

4. Enter your label and click **Save**.

Discovery Agents Label

Add label for Discovery Agents.

Goodman Law offsite

Cancel Save

5. The label will be updated for the select agent(s).

10 rows per page1 of 1

Computer

Last Scan

Discovery Agent ID

Comment

Label

KA-PW

NEVER

AGT-01A

work laptop

Goodman Law offsite

Step 6 — Schedule scans for Discovery Agent

1. From the **RapidFire Tools Portal**, navigate to **[Your Org] > Discovery Agents**.
2. From **Scan Schedule**, select one or more days of the week for the agent(s) to perform scans. Then click **Apply**.

Note: The **Deep File Scan** is only used with Compliance Manager GRC.

Note: The **Application Vulnerability Scan** is only used with VulScan.

Organization Discovery Agents

Install Key

af3a4fff-d389-4559-8024-698

Copy

Regenerate

☒ Daily Scan

Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒

Option

☐ Application Vulnerability Scan (Windows)

☐ Deep File Scan

Repeat Weekly

Configure

Apply

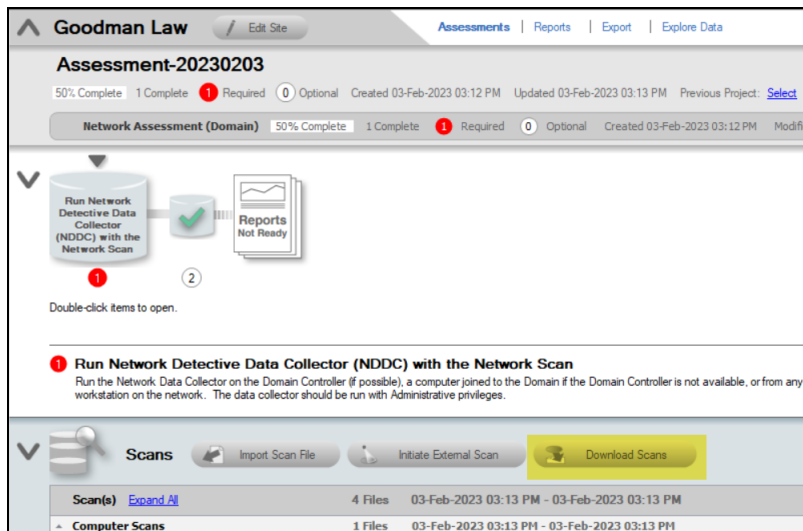
Filter...

Note: To avoid disruption during normal business hours, Agent scans begin at 2:00am on the selected days.

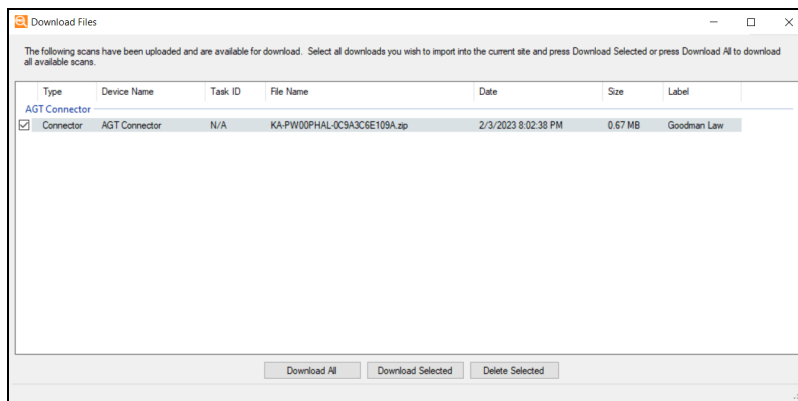
Step 7 — Download scan into assessment

To import Agent scans into your active assessment project:

1. Open your Network Detective Pro site. This site should be in the same organization where you installed discovery agents.
2. From your active assessment project, click **Download Scans** from the Scans bar.



3. Agent scans are organized under the **Agent Connector (AGT)** header.
4. Sort scans using the **Label** field. Using labels, you can select which scans to import into your assessment.



5. Select the scan files you wish to import, and then click **Download Selected**.
6. The local computer data files (.cdf) will be merged into your assessment.

Silent Install for Discovery Agent

Use the commands below in a batch file, Powershell Script, or similar, to perform a silent install for the Discovery Agent. You can combine these commands with others you may use for your agent deployments.

1. First, download the agent on the target endpoint. You can use this URL:
<https://download.rapidfiretools.com/download/DiscoveryAgent.msi>
2. Save the agent installer in the same location where you will run the batch file.
3. Next, use the following two commands.

To install the agent:

```
msiexec /qn /i DiscoveryAgent.msi /L*V install-silent.log
```

To bind the agent to your site:

```
"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\register-device.exe" -installkey <your key> (without the < >)
```

You can also append a **label** and **comment** to the command above. Example:

```
"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\register-device.exe" -installkey <your key> -label "Your Label" -comment "Your Comment" (without the < >)
```

Install Linux and OSX Discovery Agents

The help topic below demonstrates how to use scripts to deploy the Discovery Agent in Linux and OSX environments. The first section provides the default installation scripts. The second section provides a more detailed walkthrough for scripting the Linux and OSX installation.

Note: In order to deploy the Agent with the scripts below, you will need the **Install Key** for the Discovery Agent. Copy the Install Key to your clipboard. The exact Install Key should be inserted in place of the `<install_key>` tag in the scripts below.

Note: Commands must be executed by a user with super user privileges (i.e., root) or using the 'sudo' command.

Default Scripted Linux Install

```
curl -O
https://download.rapidfiretools.com/download/discoveryagent-
install-linux.tar.gz

tar xzf discoveryagent-install-linux.tar.gz

./discoveryagent-install-linux --install

/opt/discoveryagent/discoveryagent -register -installkey
<install_key> -comment "my comment" -label "my label"
```

Note: Do not use the `<` and `>` characters when you enter the install key. For the optional comment and label, only use quotation marks if your entry is two or more words.

System Requirements

Hardware	Less than 20 MB disk space
Software	• Linux Operating System that employs Systemd (system daemon) for service management. (Note that most modern Linux distributions employ this method by default.) • YUM, APT, or ZIPPY installed for package management. • .NET 6.0 Runtime The following software packages. (The app will install these packages if

System Requirements	
	they are not already present.) o curl o unzip
Other prereqs	Install Key for Discovery Agent.

Default Scripted OSX Install

```
curl -O
https://download.rapidfiretools.com/download/discoveryagent-
install-osx.tar.gz

tar xzf discoveryagent-install-osx.tar.gz

./discoveryagent-install-osx --install

/opt/discoveryagent/discoveryagent -register -installkey
<install_key> -comment "my comment" -label "my label"
```

Note: Do not use the < and > characters when you enter the install key. For the optional comment and label, only use quotation marks if your entry is two or more words.

System Requirements	
Hardware	Less than 20 MB disk space
Software	• macOS 10.15 "Catalina" or higher • .NET 6.0 Runtime The following software packages. (The app will install these packages if they are not already present.) - o curl - o unzip
Other prereqs	Install Key for Discovery Agent.

Install Script Options

Note: Replace `discoveryagent-install-linux` with `discoveryagent-install-osx` on OSX.

```
./discoveryagent-install-linux --help
```

Syntax: `discoveryagent-install-linux [command] [options]`

commands:

```
--version|-v
```

```
--help|-h
```

```
--check-prereqs|-c
```

```
--install-missing-pkgs
```

Note: `--install` will do this automatically. Only use this option to install the pkgs without doing the full install.

```
--download-bundle
```

```
--url [url]
```

Overrides the URL used for downloading the install bundle.

```
--install
```

```
--install-dir [install dir]
```

Defaults to `/opt/discoveryagent`

```
--url [url]
```

Overrides the URL used for downloading the install bundle.

```
--bundle [install bundle zip file]
```

Use an install bundle already on the local machine.

```
--verify-install
```

```
--uninstall
```

Options:

```
--force
```

Non-interactive mode. Does not prompt for confirmation.

Scripts for Linux and OSX Manual Data Collection

Note: With the default run, the resulting CDF data file will be called <computer name>-<mac address>.cdf.

Linux X64 Collection

```
curl -O
https://download.rapidfiretools.com/download/computerscanner-
linux-x64.tar.gz

tar xzf computerscanner-linux-x64.tar.gz

./computerscanner
```

OSX ARM64 Collection

```
curl -O
https://download.rapidfiretools.com/download/computerscanner-osx-
arm64.tar.gz

tar xzf computerscanner-osx-arm64.tar.gz

./computerscanner
```

OSX X64 Collection

```
curl -O
https://download.rapidfiretools.com/download/computerscanner-osx-
x64.tar.gz

tar xzf computerscanner-osx-x64.tar.gz

./computerscanner
```

Optional Flags

- **Switch:** -outbase <basename>
 - **Details:** The basename of the outfile.
 - **Default:** <COMPUTERNAME>-<MAC ADDRESS>

- **Switch:** `-outdir <directory>`
 - **Details:** The directory to produce the outfile. Defaults to the current directory.

End-user Initiated Computer Scans

With the RapidFire Tools Portal, you can enlist end-users in scanning their own devices. With a couple of clicks, end-users download and run the computer scanner. The scan files will then be uploaded to your Network Detective Pro assessment project, where you can download them. Here's how to get started:

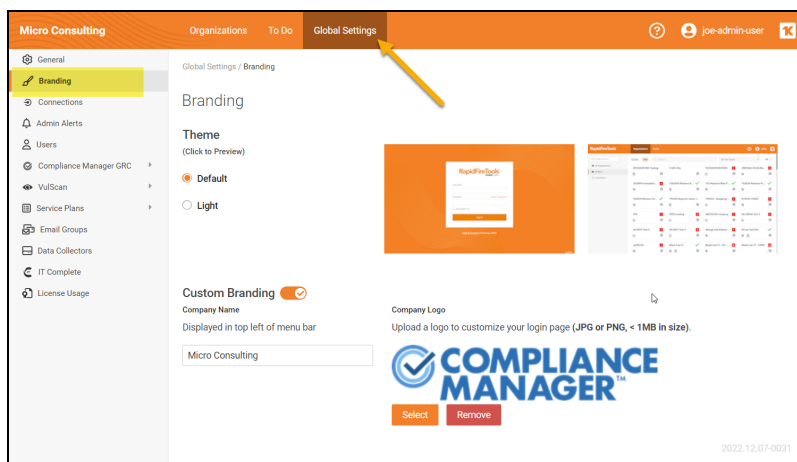
Step 1 — Create a New Network Detective Pro Portal Site

You can enable end-user scans for both **new** and **existing** Network Detective Pro sites.

- **New sites:** Create a new Network Detective Pro site in the RapidFire Tools Portal. Then proceed to ["Step 2 — Customize Portal Branding" below](#).
- **Existing Sites:** You can enable end-user scans for existing Network Detective Pro sites in the Portal. These sites must have a corresponding site in the Network Detective Pro desktop app that is publishing data to the RapidFire Tools Portal via Reporter. See "InDoc and the RapidFire Tools" Portal in the [Reporter User Guide](#).

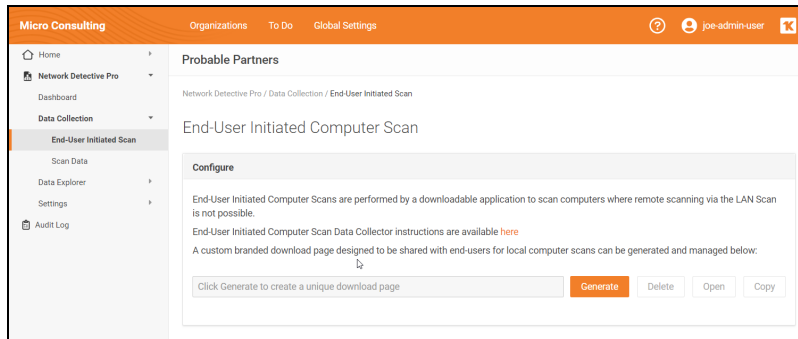
Step 2 — Customize Portal Branding

Next, customize the branding for the end-user download page. The download page is where end-users will access the computer scanner. It can be customized with your own company logo, for example. From the RapidFire Tools Portal, navigate to **Global Settings > Branding** and make your changes.

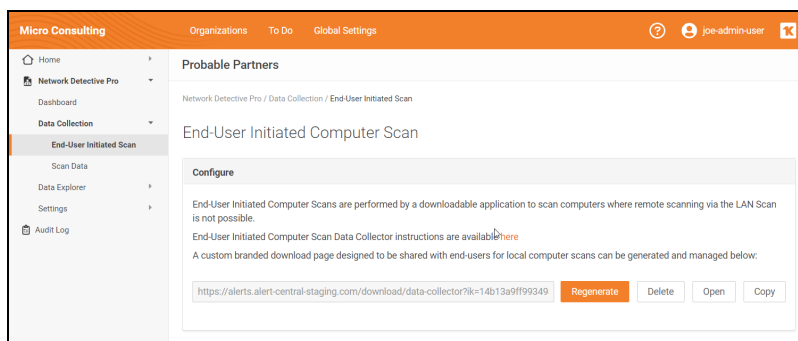


Step 3 — Enable End-users Scans from RFT Portal

1. From your Network Detective Pro site, navigate to **Data Collection > End-user Initiated Scan**.



2. Click **Generate** to create a URL for end-users to download and run the computer scanner. Copy the URL to your clipboard.

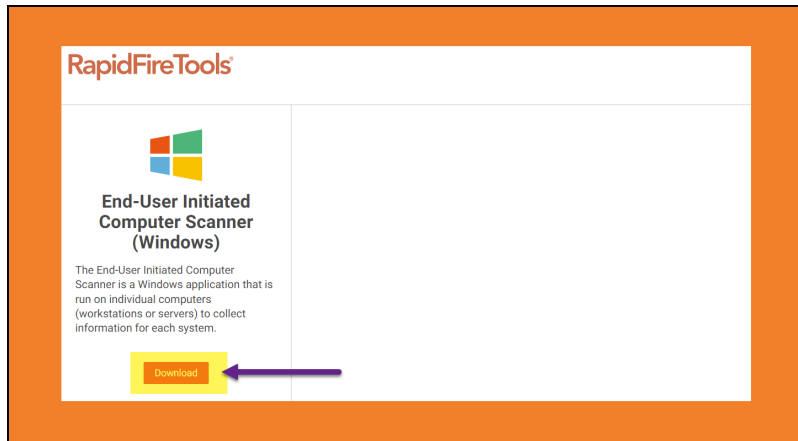


Step 3 — Send URL to End-users

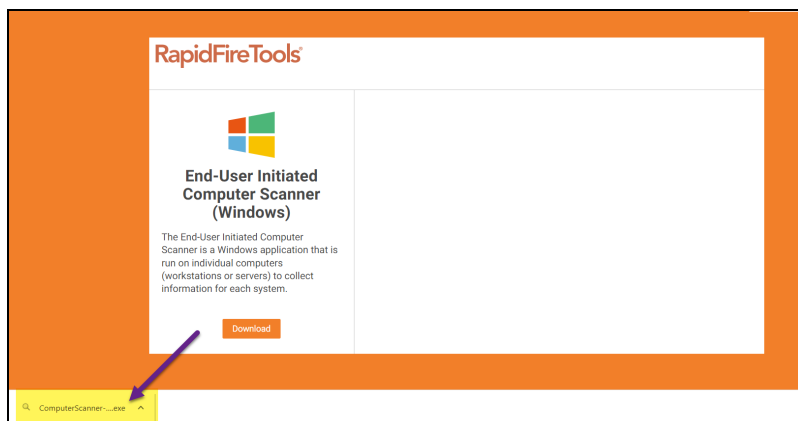
Once you generate the URL, send it to your end-users. You can do this with a simple email — or whatever method you choose.

Step 4 — End-user Runs Computer Scanner from URL

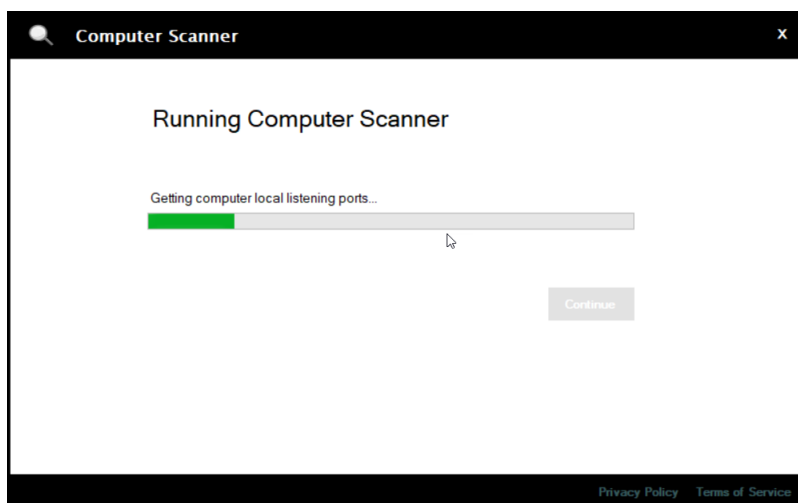
1. With the URL, the end-user opens the download page for the computer scanner and clicks **Download**.



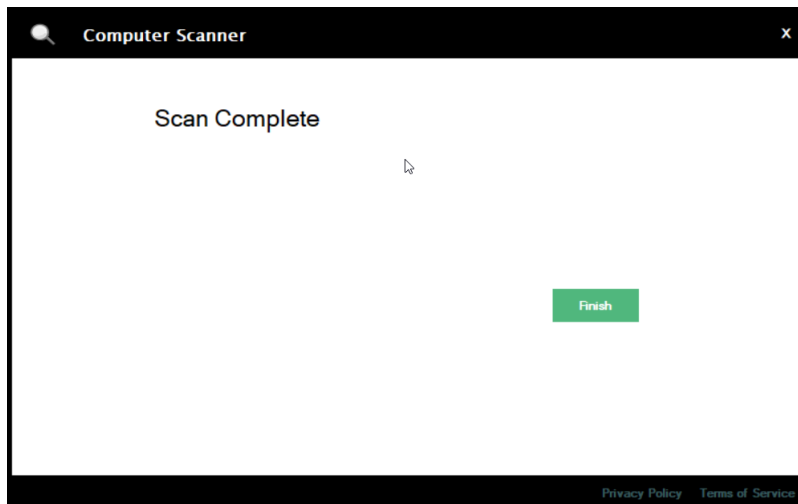
2. The end-user next opens and runs the computer scanner.



3. The computer scanner will immediately begin the scan. The user can continue using their device while the scan runs.



4. When the scan completes, the end-user clicks **Finish**.



Step 5 — Download Scan(s) from Network Detective

Once the end-user performs the scan, the scan file is uploaded and becomes available to download in Network Detective Pro.

For New Sites

If you created a new site in the RapidFire Tools Portal for end-user scans, follow these steps:

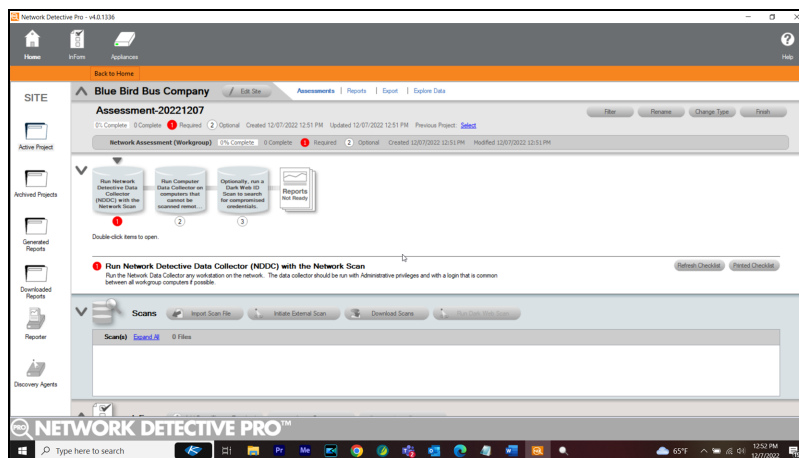
1. Open the Network Detective Pro app, and log in with the same account as your RapidFire Tools portal account. This should be the same account that contains your portal site.
2. From the Network Detective Pro app, click **New Site**.
3. For your **site name**, enter the exact site name of your corresponding Network Detective Pro site in the RapidFire Tools Portal. The names must match exactly. Then continue to ["Download End-user Scans" on the facing page](#).

Existing Sites

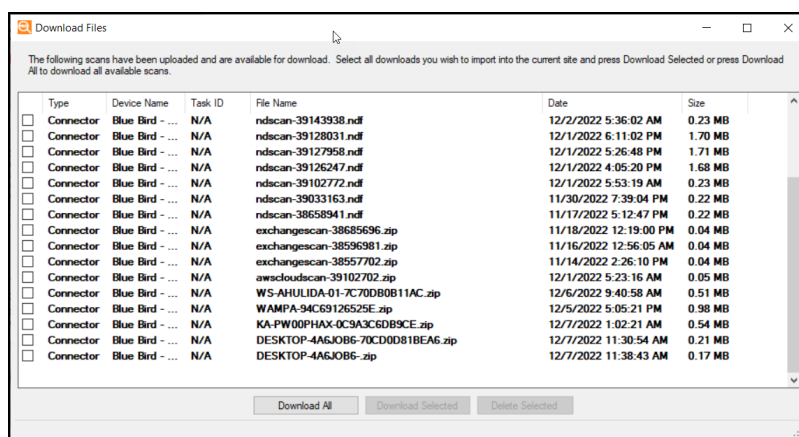
If you already have a site in the Network Detective Pro app that is publishing data to your portal site via Reporter, continue to ["Download End-user Scans" on the facing page](#).

Download End-user Scans

1. From your Network Detective Pro site, click **Download Scans** from the scans bar.



2. The end-user scans will appear by device name. Select them and click **Download**.



Step 6 — Generate Reports

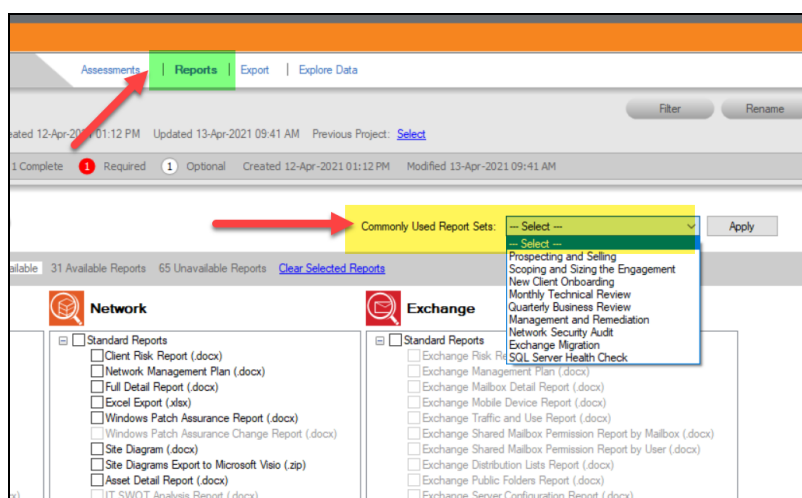
Once you download the scans, you can generate assessment reports.

Use the blank network data file (.ndf) to generate reports that would otherwise require a network scan. You can download the blank .ndf in the [web version of this help topic here](#).

Generate Commonly Used Report Sets

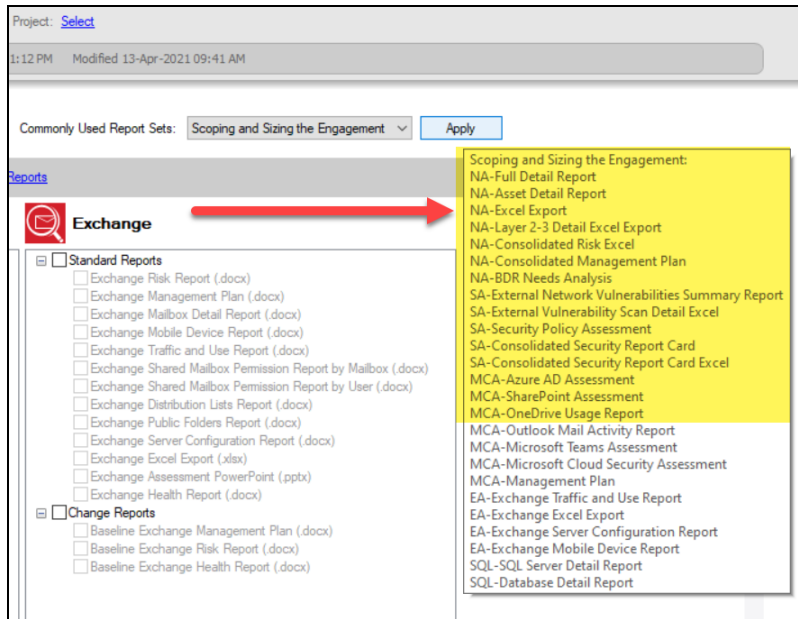
Network Detective Pro makes it easy for you to generate a set of reports to accomplish your chosen business purpose. For example, you can select a set of reports geared toward prospecting and selling, onboarding a new client, or performing a monthly technical review. To use this feature:

1. Once you have completed your assessment and are ready to generate reports, go to **Reports** from your assessment dashboard. Then open the **Commonly Used Report Sets** drop-down menu.

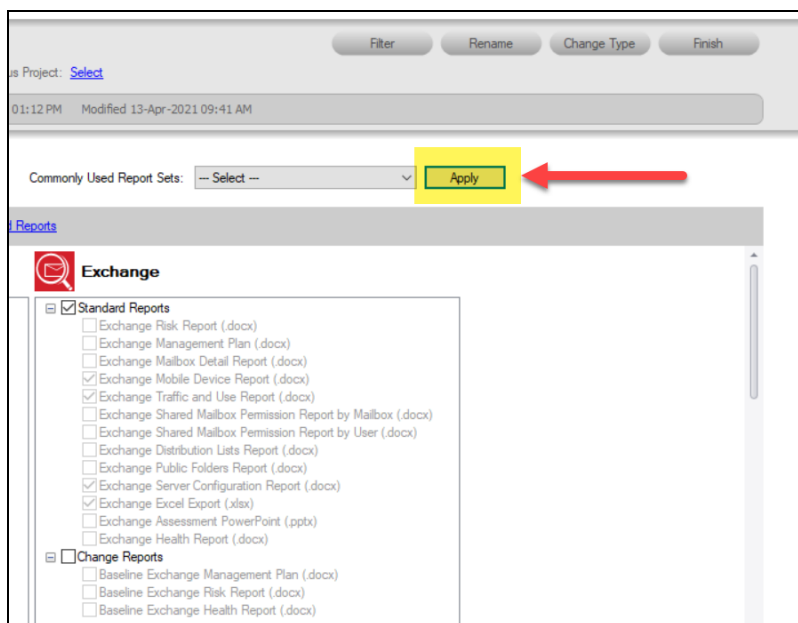


2. Select a report set from the drop-down menu. The report sets represent the various business functions for your IT assessments and can help convey the value of your managed service to both prospective and current clients.

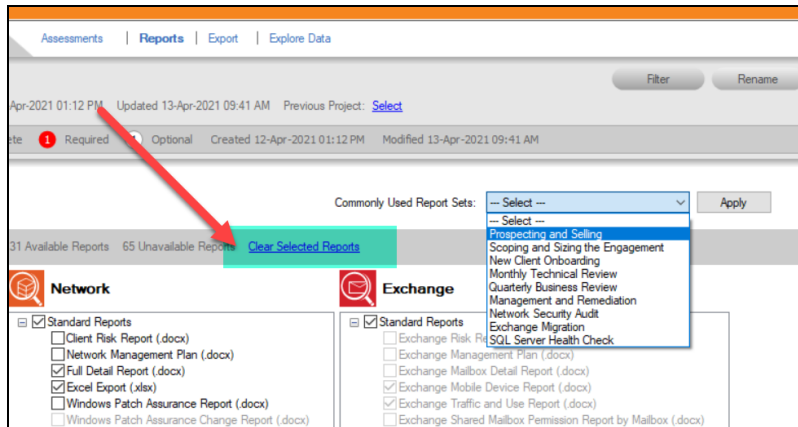
Note: When you select a report set, you can hover your mouse over the Apply button to see a pop-up list of reports contained in each set.



- Once you select a report set, click **Apply**. The associated reports will be selected in the Reports console. You can continue to select and apply common report sets as you wish.



Note: If you want to clear your report selections and start over, click **Clear Selected Reports**.



4. Once you select your reports, click **Create Reports** to generate your assessment documentation.

Document Exceptions with the Issue Exception Worksheet

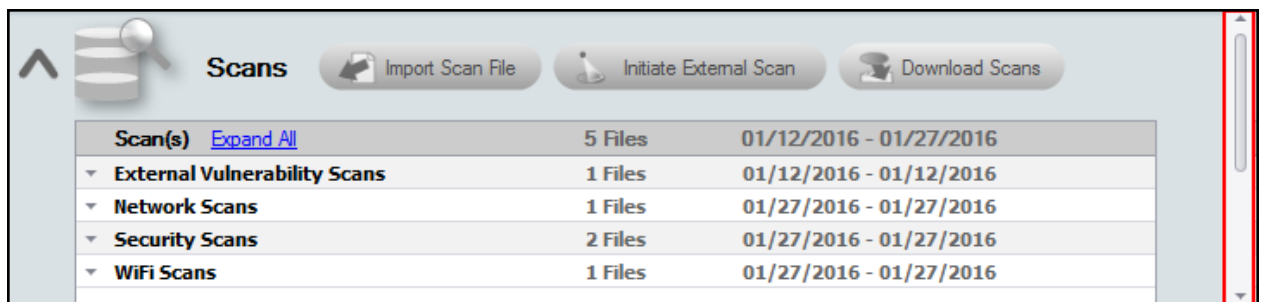
The **Issue Exception Worksheet** compiles the issues discovered during the assessment process. Depending on the assessment type, these can be technical issues identified during the scanning process, or issues that result from your answers to security worksheets and surveys.

The Issue Exception Worksheet allows you to document your response to each of these issues. For example, you can explain why the issue is false positive, or alternatively, you can outline the measures you've taken to mitigate the issue.

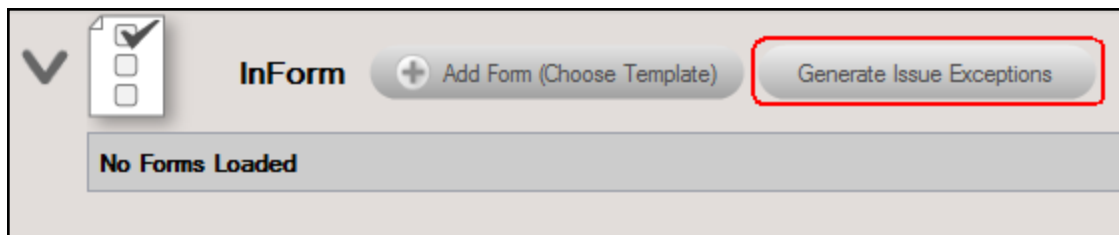
In this way, the Issue Exception Worksheet brings the human element back into the assessment and allows an auditor to document explanations for suspect items. Of course, the worksheet does not alleviate the need for safeguards, but it does but allows provide you with an alternative means of mitigating assessment issues.

Here's how you can employ the Issue Exception worksheet in your projects:

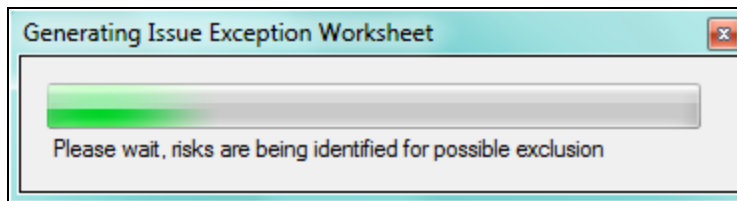
1. First, **open one of your Network Detective Pro sites**. Before you can generate the worksheet, you should first have completed your assessment checklist. This includes completing any required scans or responding to any worksheets or surveys that are part of the assessment.
2. Mouse over or scroll down to the InForm panel near the bottom of the Network Detective site interface.



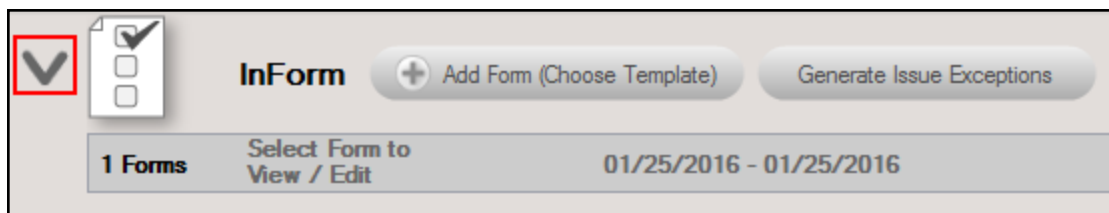
3. Next click **Generate Issue Exceptions**.



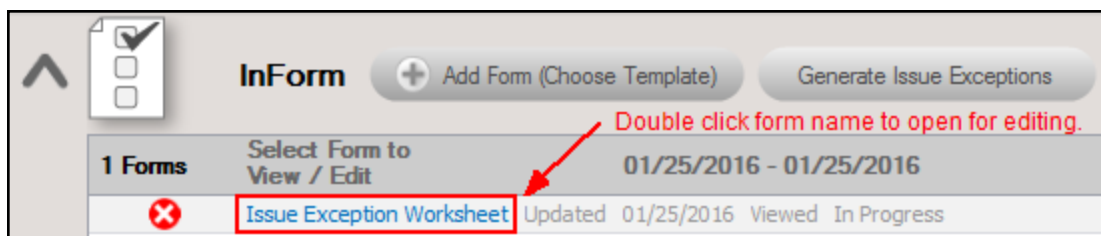
4. A status bar will appear while the worksheet is being created. Once it's finished, the Issue Exception Worksheet will become available for viewing and editing.



5. 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.



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



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 these steps to review and document issue mitigation or clarification responses.

0 Required Remaining

Filter Topics

Bulk Entry Actions Save Close

Expand All | Collapse All

1 Network Assessment

1.1 Unsupported OS
If the issue has been mitigated or is a false positive, please enter in notes in the response field. Any issue that has a mitigation response will be documented with the note and the issue will not affect risk scoring.
identified as false positive

1.2 User Not Logged in within 30 days
If the issue has been mitigated or is a false positive, please enter in notes in the response field. Any issue that has a mitigation response will be documented with the note and the issue will not affect risk scoring.
Issue has been mitigated through technical means

1.3 Password Expiration
If the issue has been mitigated or is a false positive, please enter in notes in the response field. Any issue that has a mitigation response will be documented with the note and the issue will not affect risk scoring.
Issue not relevant to client

1.4 Too Many domain Admins
If the issue has been mitigated or is a false positive, please enter in notes in the response field. Any issue that has a mitigation response will be documented with the note and the issue will not affect risk scoring.
Optional Response

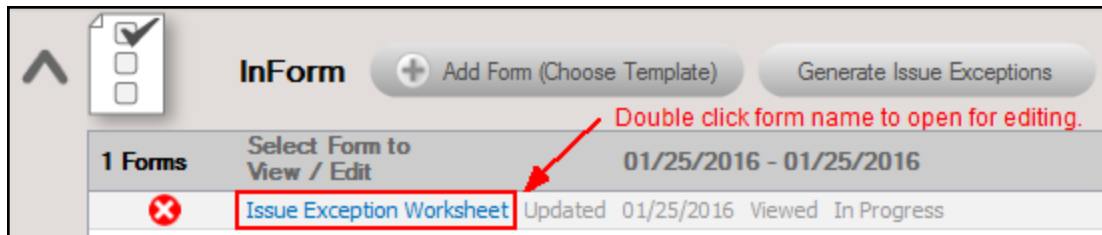
7. First review the **topic** for each issue.
8. Then review the **issue description**. Most descriptions contain additional detail that explains the issue and how you can resolve it. In some worksheets, Exceptions are grouped by a number of exception types that may include Firewall, Office Environment, Business Associate Agreements, and so on.
9. Next, **enter a response** for the issue. How you respond is up to you. As we alluded to earlier, there are a few categories for how you might respond to the issue:
 - You can explain how the issue is a false positive and does not affect the assessment environment
 - Or you can explain that while the issue detected is real, it does not pose a risk because you have measures in place to mitigate the issue
 - Further yet, you could explain that you wish to exclude the issue simply because it isn't relevant to your client or service
10. Some worksheets might employ a drop down menu where you select from multiple responses. If this is the case, you can use the Notes icon to enter any "Notes" relevant to a particular exception.
11. Select the **Respondent** icon to enter the name of individual that provided information for the response. These can be the name of the auditor themselves or of an SME who explained the exception.

Note: The Exception Worksheet does not require a response for each and every topic. Enter your Response if applicable, otherwise, leave the entry blank.

12. **Save your answers** periodically and Save when you are done. When you're finished, click Save and Close.

Once the Issue Exception Worksheet is saved, it will be listed under the InForm Bar located in the Assessment Window.

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.

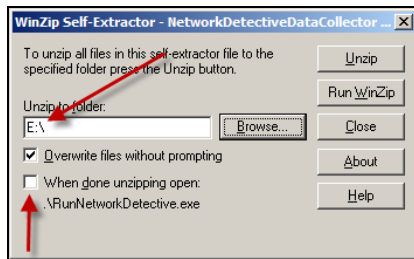


When you mark issues as exceptions, the overall risk score and other areas in your assessment documentation will change. Specifically, the documented exceptions will be removed from the risk score.

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.

Override Issues in Network Detective Pro Reports

Network Detective Pro gives you the option to ignore certain detected issues in your assessment reports. This can be helpful if you are having trouble with false positives, or if you wish to ignore certain issues that are not relevant to your assessment purpose or the client's needs. Further, you can override values for each issue, such as **Severity**, **Probability**, and **Score**.

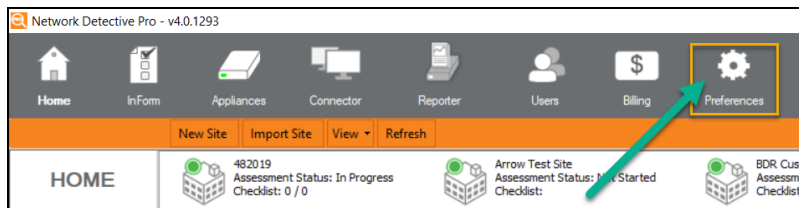
These customization options give you flexibility in how you choose to present issues to your stakeholders.

You can still view ignored issues in the **Issue Exception Worksheet**.

Override issues at the global level

You can configure overrides at the global level to ignore certain issues in reporting for all of your Network Detective Pro sites. To do this:

1. Click **Preferences** from the **Network Detective** top-menu.



Note: Note that you must be an admin user in order to set preferences, including issue overrides, at the global level.

2. From Preferences, select the **Issue Overrides** tab.

Preferences

Report Defaults | Email Groups | **Issue Overrides**

Text | My Logo | Theme | Cover Images | Company Information

Report Prepared For:

Report Prepared By:

Footer:

Cover Page Disclaimer:

Target Language:

Time Zone:

Date Format:

Paper Size:

Currency Symbol:

Conversion Factor:

[Reset to Global Preferences](#)

Ok Cancel

- A list of the most commonly detected issues will appear.

Preferences

Report Defaults | Reporter | Email Groups | **Issue Overrides** | Integrations

The most commonly detected issues are listed below. Uncheck an issue to ignore the issue completely during report generation. Scores can be overridden with a number between 1-100. Changes to Global Preferences will affect all Sites unless overridden at the Site level. Ignored issues will still appear in the Issue Exception Worksheet.

[Reset all Severity, Probability, and Score](#) [Select All](#) [Unselect All](#)

Enabled	Module	Issue	Severity	Probability	Score
☒	BDR Assessment	Critical servers not backed up	High	High	100
☒	BDR Assessment	Critical workstations not backed up	High	High	95
☒	BDR Assessment	Insufficient network speed for offsite backup	High	High	80
☒	BDR Assessment	No successful backup was ever successfully performed	High	High	100
☒	BDR Assessment	On-Premises Exchange Server not backed up	High	High	80
☒	BDR Assessment	On-Premises Exchange Server not backed up successfully in 30 days	Medium	Medium	70
☒	BDR Assessment	Recent backup failures	High	High	90
☒	BDR Assessment	Significantly aged hardware	Medium	Medium	70
☒	BDR Assessment	SQL Server not backed up	High	High	75
☒	BDR Assessment	SQL Server not backed up successfully in 30 days	Medium	Medium	65
☒	Exchange Assessment	Disabled Mailboxes	High	High	100
☒	Exchange Assessment	Empty Distribution Lists	Low	Low	20
☒	Exchange Assessment	Mailbox Size versus Quota (>50%)	High	Low	35
☒	Exchange Assessment	Mailbox Size versus Quota (>75%)	High	Medium	65
☒	Exchange Assessment	Mailbox Size versus Quota (>90%)	High	High	90
☒	Exchange Assessment	Mailbox without Quota	Low	Low	20
☒	Microsoft Cloud Assessment	Admin Multi-Factor Authentication	High	High	90
☒	Microsoft Cloud Assessment	Admin Role Overlap	High	High	90
☒	Microsoft Cloud Assessment	Adobe Reader Flash Content Rendering	High	High	90
☒	Microsoft Cloud Assessment	Advanced Audit Policy Alert	High	High	90
☒	Microsoft Cloud Assessment	Anonymous Access Restricted To Named Pipes	High	High	90
☒	Microsoft Cloud Assessment	Authentication of Remote Desktop Connections	High	High	90
☒	Microsoft Cloud Assessment	Azure ATP Sensor	High	High	90
☒	Microsoft Cloud Assessment	BitLocker Additional Authentication	High	High	90

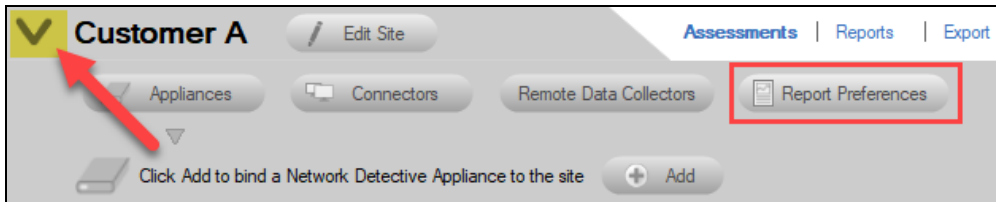
Ok Cancel

- Uncheck an issue to ignore the issue** completely during report generation. You can also override the issue **Severity**, **Probability**, and **Score** for issues that appear in reports that include this data. These settings will change how Network Assessment displays these issues in their associated reports.
- When you are finished making changes, click **OK**. The issues will then be omitted for future reports for all sites.

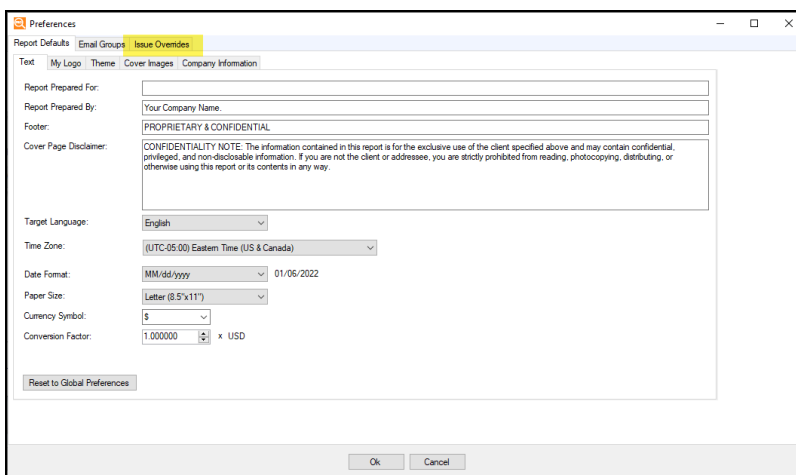
Note: Note that if you have previously set issue overrides at the site level, these sites will be unaffected by subsequent changes to global issue overrides.

Override issues at the site level

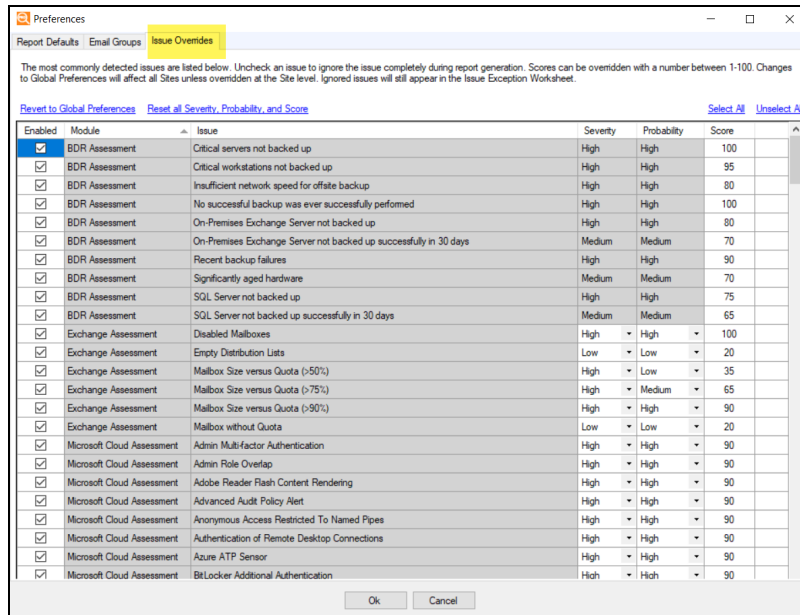
1. Open the Site Preferences from the top-left chevron button. Then click **Report Preferences**.



2. From Preferences, select the **Issue Overrides** tab.

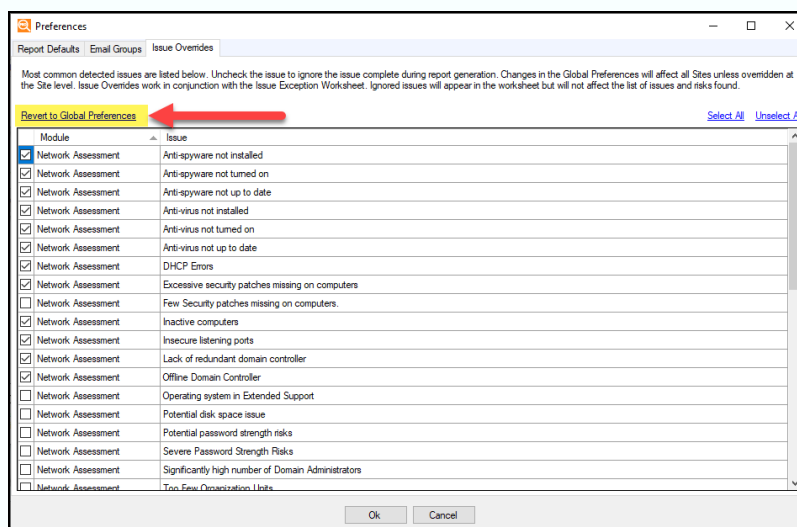


3. A list of the most commonly detected issues will appear.



4. **Uncheck an issue to ignore the issue** completely during report generation. You can also override the issue **Severity**, **Probability**, and **Score** for issues that appear in reports that include this data.
5. When you are finished making changes, click **OK**. The issues will then be omitted for future reports for this site only.

Note: Note that once you set issue overrides at the site level, these sites will be unaffected by subsequent changes to global issue overrides. To revert the site overrides to the global configuration, click **Revert to Global Preferences**.



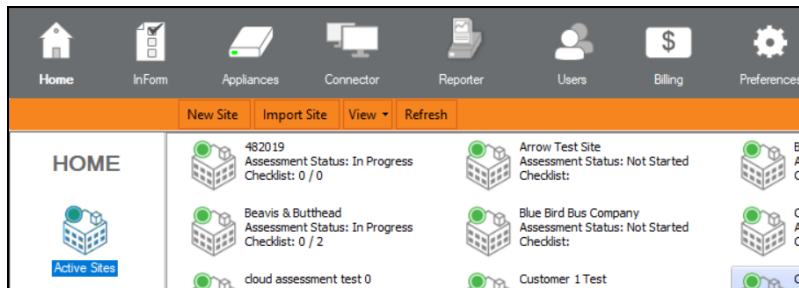
Affected Reports

Network Assessment	Security Assessment
Client Risk Report	Security Risk Report
Network Management Plan	Security Management Plan
Consolidated Risk Report	Consolidated Security Report Card
Consolidated Risk Excel	Consolidated Security Report Card Excel
Consolidated Management Plan	Security Health Report
Baseline Network Management Plan	Baseline Security Management Plan*
Baseline Client Risk Report	Baseline Security Risk Report*
Baseline Client Health Report	Baseline Security Health Report*
Asset Detail Report*	Security Assessment PowerPoint
Network Assessment PowerPoint	

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 Pro Client Connector service.

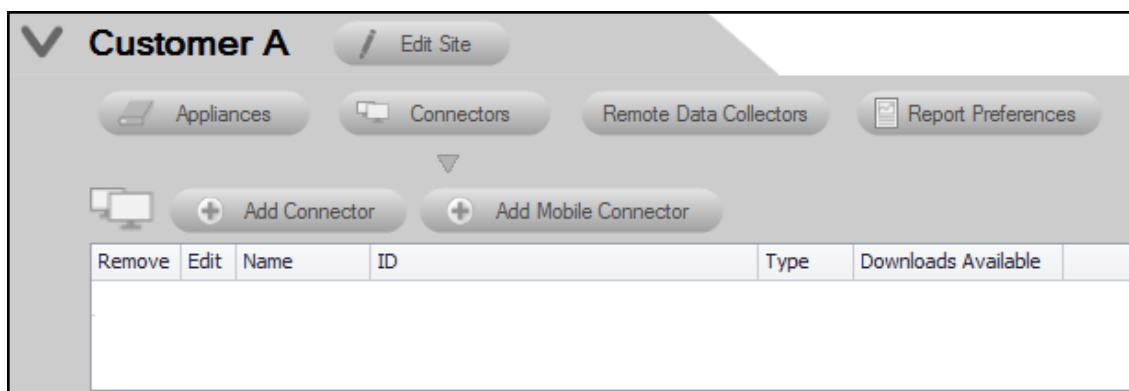
Preferences for Client Connectors are configured on a Site-by-Site basis and can be customized for each individual site.



To add a Connector to a Site, first navigate to the desired Site from the Home screen by double-clicking on its icon.

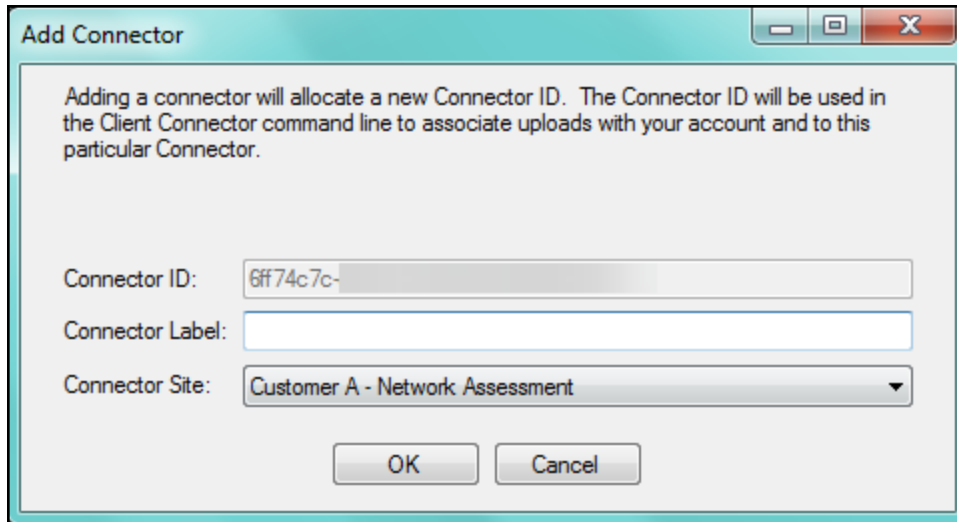
This will open the Site's Dashboard.

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.



The image shows a Windows-style dialog box titled "Add Connector". It has a light blue header bar with standard window controls (minimize, maximize, close). The main content area is white and contains the following text: "Adding a connector will allocate a new Connector ID. The Connector ID will be used in the Client Connector command line to associate uploads with your account and to this particular Connector." Below this text are three input fields: "Connector ID:" with a text box containing "6ff74c7c-", "Connector Label:" with an empty text box, and "Connector Site:" with a dropdown menu showing "Customer A - Network Assessment". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Next, configure your Connector.

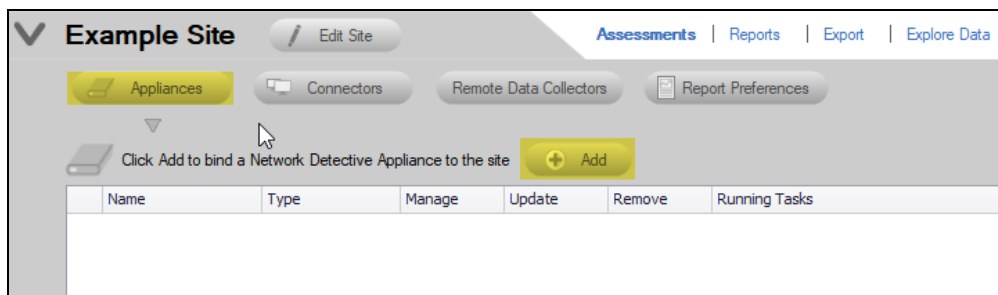
You can now use your Connector to download Scans and associate them with your Assessments.

Adding an Inspector to a Site

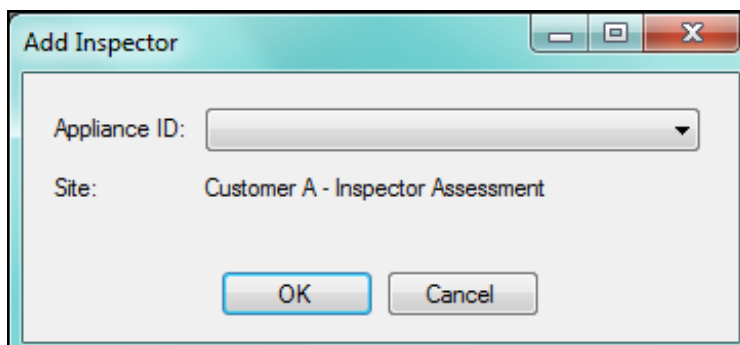
After starting a new assessment, or within an existing assessment, in order to “Associate” and Inspector Appliance with the Assessment Project, you must first select the **V** symbol to expand the assessment properties view.



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

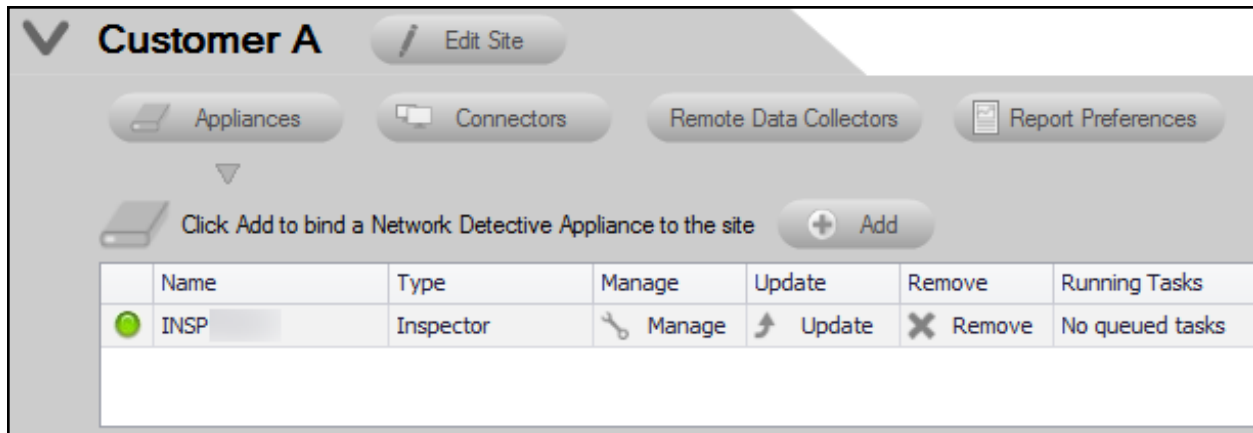


To add an Inspector to an Assessment, from the Assessment’s dashboard select the **Inspector** button, then the **Inspector Add** button as noted above.

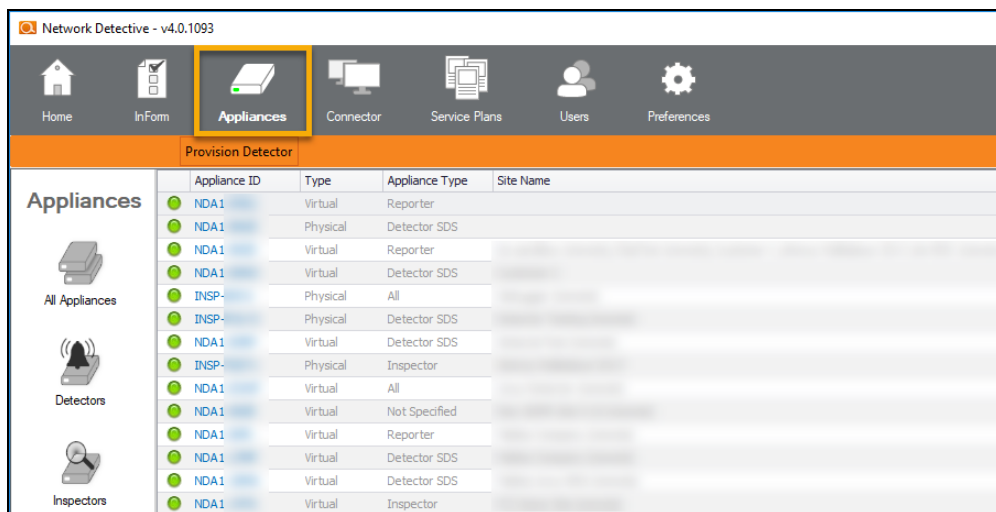


Select the **Inspector ID** of the Inspector from the drop down menu. Note that the Inspector ID can be found on a printed label on the Inspector Appliance.

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 Pro 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.

Dark Web Scan Summary for Security Assessment Module

We provide a **Dark Web Scan** for compromised passwords as part of the Security Assessment Module (SAM) and reports. This feature can quickly and dramatically convey to clients the security risks that exist on their network and why they need MSP security services.

How it Works

We offer a Dark Web scan that shows 5 returned results for each domain identified within the assessment. When you specify one or more domains, the scan searches the Dark Web for compromised login credentials (usernames and passwords). This feature is available in several SAM reports and deliverables, including:

- Security Risk Report
- Security Management Plan
- Consolidated Risk Report
- Consolidated Management Plan

Compromised passwords will appear as an issue in these reports as in the example below:

High Risk			
Risk Score	Recommendation	Severity	Probability
100	Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess. ☐ elmatador@example.com password: 12345***** ☐ manutdace@example.com password: gepar***** ☐ nha@example.com password: 11052***** ☐ samco_619@example.com password: samet***** ☐ soasta_fight_3789@example.com password: soast***** ☐ mohenchao@gmail.com password: 86420***** ☐ moonislah786@gmail.com password: 51711***** ☐ mores12088@gmail.com password: shing***** ☐ mountain11060722@gmail.com password: sky12***** ☐ mppinvest@gmail.com password: wbgvc***** ☐ akumar@performanceit.com password: anish***** ☐ dwillis@performanceit.com password: sunny***** ☐ flasilmi@performanceit.com password: aaron***** ☐ klino@performanceit.com password: myron***** ☐ kmorris@performanceit.com password: proit*****	H	H
77	Enable account lockout for all users.	H	H
72	Enable automatic screen lock on the specified computers. ☐ DC01	M	M

EXAMPLE:

Here is an example of how the results will appear in the *Baseline Security Risk Report*.

1500	Compromised Passwords found on the Dark Web (100 pts each)
	<i>Current Score:</i> 100 pts x 15 = 1500: 90.96%
	<i>Previous Score:</i> 100 pts x 15 = 1500: 90.96%
	<i>Issue:</i> A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2018. <i>Recommendation:</i> Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess.

Issue: Compromised Passwords found on the Dark Web

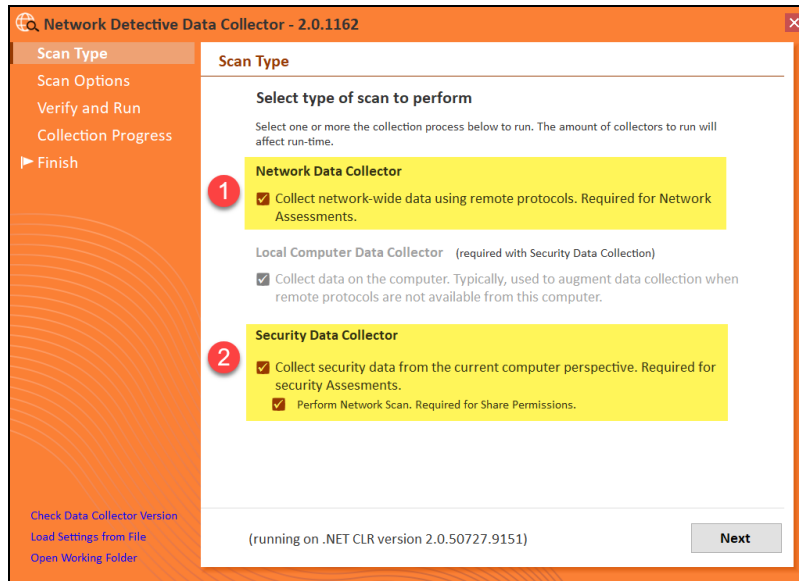
Description: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2018.

Recommendation: Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess.

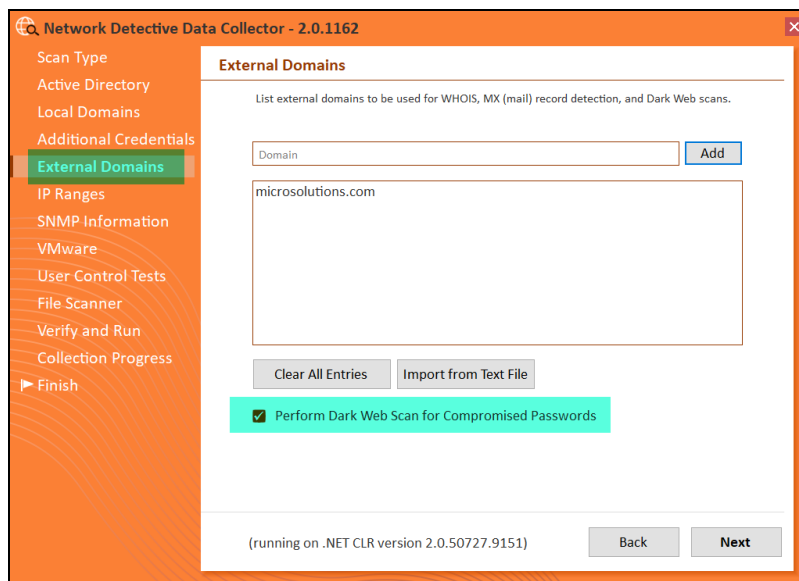
How to Perform Dark Web Scan as Part of Your Security Assessment

You can perform a **Dark Web Scan** for compromised passwords as part of a Security Assessment. You can opt into this feature when configuring your scan for the **Network Detective Data Collector**. Here's how it works:

1. First, run the **Network Detective Data Collector** and select both the **Network** and **Security Data Collector** options when first configuring the scan.



2. Continue through the wizard and enter the required network information and user credentials to configure the scan.
3. When you reach the **External Domains** screen, be sure that **Perform Dark Web Scan for Compromised Passwords** is selected.
4. Before you click **Next**, enter each external domain that you would like to scan for compromised passwords. Click **Add** to enter the domain in the list of domains to be scanned.



5. Complete all steps in the wizard and perform the scan. Then upload the results into your assessment in Network Detective Pro. See [Performing a Security Assessment](#)

for complete instructions.

Any compromised passwords will appear as security issues identified in your assessment reports and documentation.

Important: Note that the Dark Web Scan will only return the **first 5** compromised passwords identified for each domain you specify.

What to do if Compromised Passwords are Detected

The Dark Web Scan searches for compromised login credentials for each of the domains entered during the scan. It only returns the 5 most recently compromised logins for each domain.

If the scan reveals compromised logins, consider these actions:

- Force users to change their passwords or implement multi-factor authentication.
- Deliver reports on a regular basis to keep on top of possible new breaches.

Note: It is not always necessary to get the complete list of compromised credentials, as older entries may not lead to increased security due to password expiration.

Set Up Full Dark Web ID Integration

By default, the Dark Web Scan will only return the **first 5** compromised passwords identified for each domain you specify. However, **Dark Web ID** users (<https://www.idagent.com/>) can access full reporting for compromised passwords. To set this up:

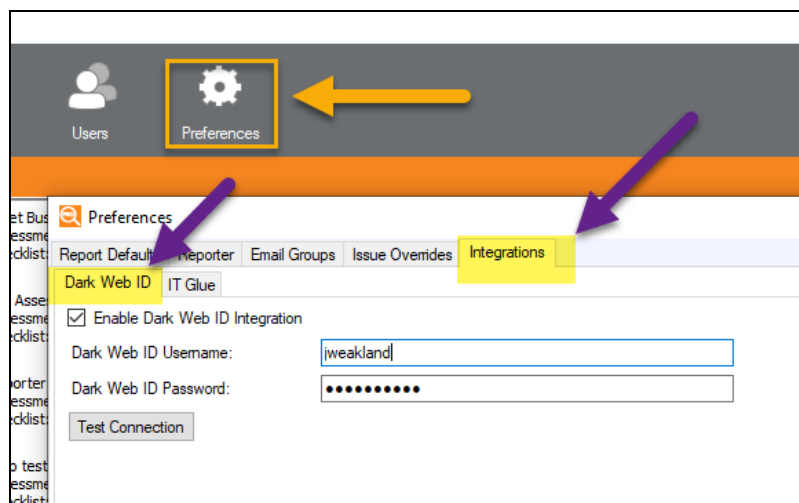
Step 1 — Contact Dark Web ID Support to Enable User API Access

To enable API Access, the Dark Web ID customer must open a ticket with Kaseya Support. The Dark Web ID team will grant the customer API access. Once the support ticket is closed, the user can successfully enter and test their credentials in Network Detective Pro. See also <https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-I-enable-API-access-for-ID-Agent->.

Step 2 — Set Up Dark Web ID Integration with Network Detective Pro

Once you enable Dark Web ID API access, you can set up the integration in Network Detective Pro. To do this:

1. In the Network Detective Pro app, click **Preferences** from the top menu.
2. Click the **Integrations** tab
3. From the **Dark Web ID** tab, **enable** the Dark Web ID Integration.
4. Then enter your Dark Web ID **Username** and **Password**.
5. Finally, click **Test Connection**. Once you verify the connection works, click **OK** to dismiss the Preferences menu.



Step 3 — Continue Assessment and Perform Scan

- Once you enable the Dark Web ID Integration, complete your assessment.
- See ["How to Perform Dark Web Scan as Part of Your Security Assessment" on page 260](#).
- Your assessment documentation will feature complete data regarding compromised passwords.

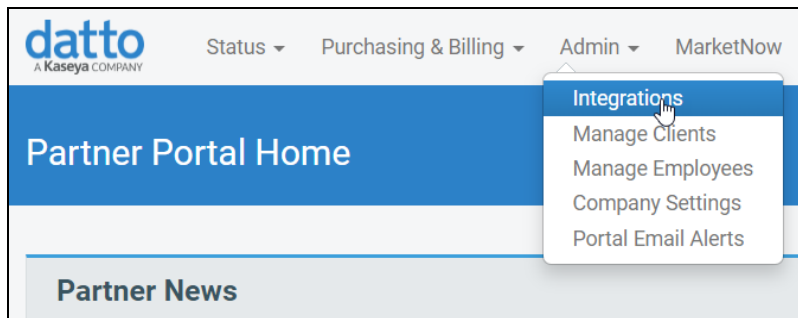
Perform Datto Unified Continuity Scan

During the Network Assessment, you can optionally perform a Datto Unified Continuity Scan. This will retrieve data from your Datto BCDR, Cloud Continuity for PCs, Datto Continuity for Microsoft Azure, and SaaS Protection accounts. This topic covers how to perform the Datto Unified Continuity Scan as you perform a Network Assessment.

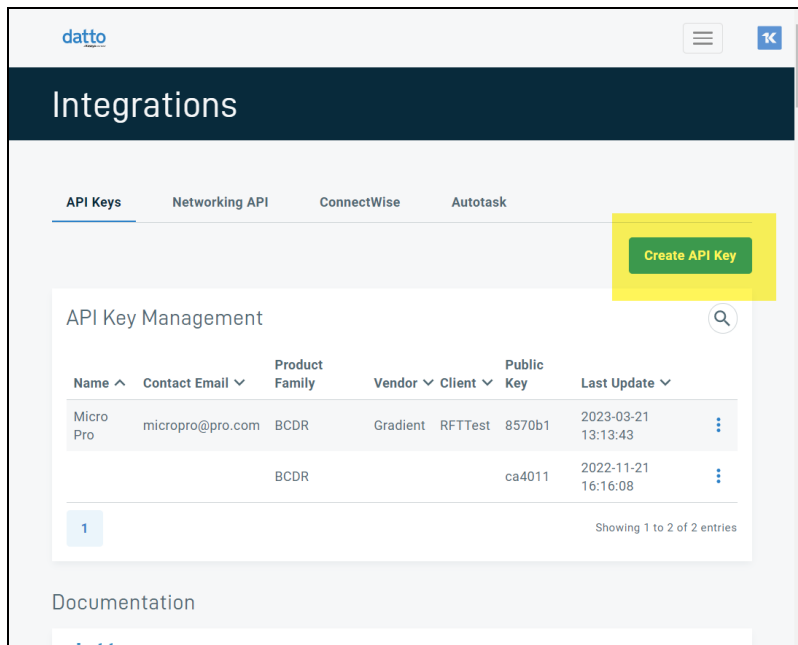
Step 1 — Enable API Access in Datto Partner Portal

First, you need to **generate Datto API credentials** for use with Network Detective Pro. To do this:

1. From the Datto Partner Portal, navigate to **Admin > Integrations**.

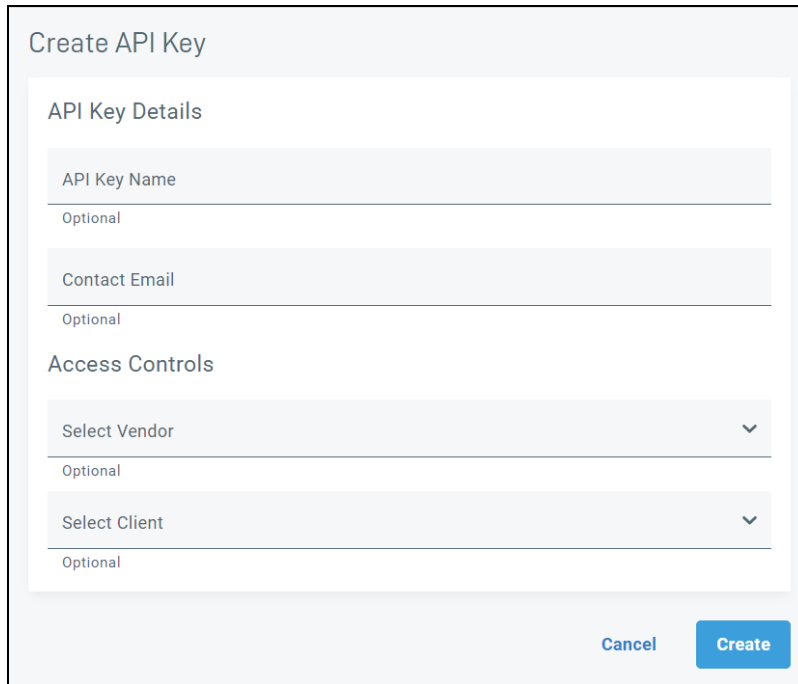


2. Click **Create API Key**.



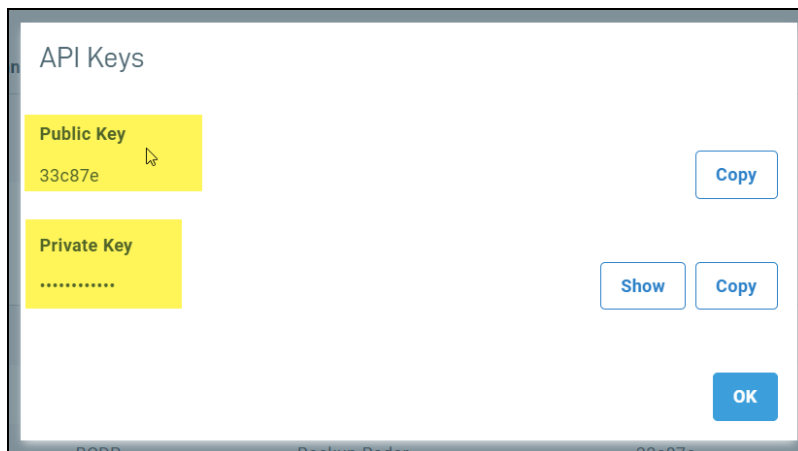
3. Complete the fields for the API Key and click **Create**.

- Enter an optional **Name** and **Contact Email** for the API Key.
- Select the optional **Vendor** and **Client**. The vendor and/or client should match the Datto organization from where you want to collect data.



The 'Create API Key' dialog box is shown. It has a title bar 'Create API Key'. Below it is a section 'API Key Details' with two input fields: 'API Key Name' and 'Contact Email', both marked as 'Optional'. Below that is a section 'Access Controls' with two dropdown menus: 'Select Vendor' and 'Select Client', both marked as 'Optional'. At the bottom right are 'Cancel' and 'Create' buttons.

4. Copy the **Public Key** and **Private Key** for use later.

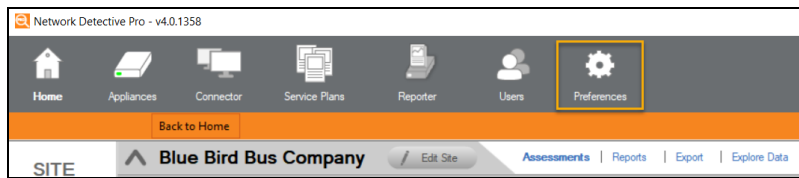


The 'API Keys' dialog box is shown. It has a title bar 'API Keys'. Below it are two yellow boxes: 'Public Key' with the value '33c87e' and 'Private Key' with a masked value '.....'. To the right of the 'Public Key' box is a 'Copy' button. To the right of the 'Private Key' box are 'Show' and 'Copy' buttons. At the bottom right is an 'OK' button.

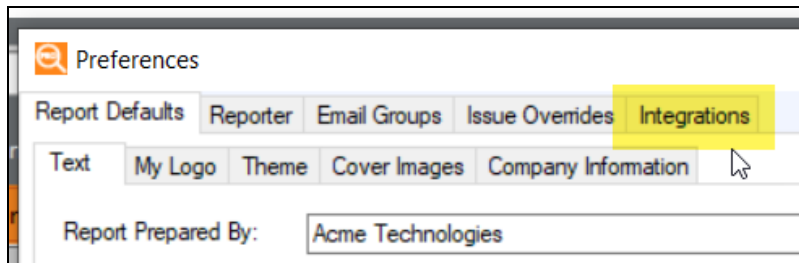
Step 2 — Enable Datto Unified Continuity Integration

Next enable the integration from Network Detective Pro:

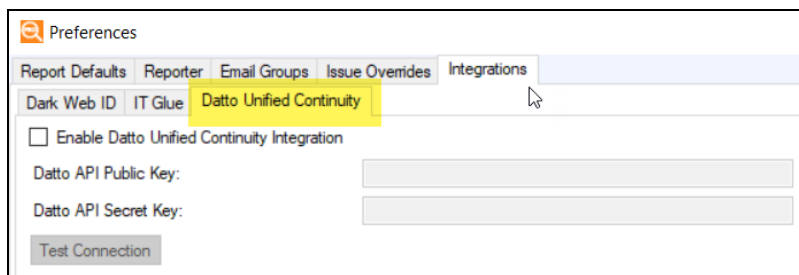
1. From the top menu, open **Preferences**.



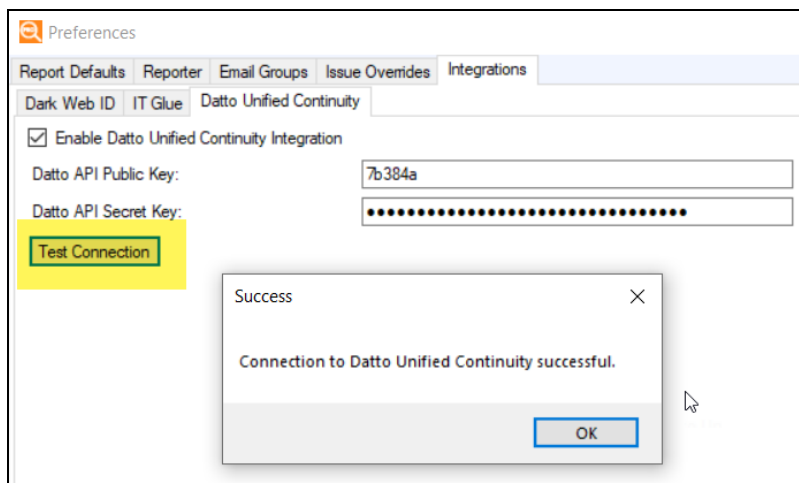
2. Open **Integrations**.



3. Open the **Datto Unified Continuity** tab.



4. Enter the API credentials and click **Test Connection**. A success notification will appear.

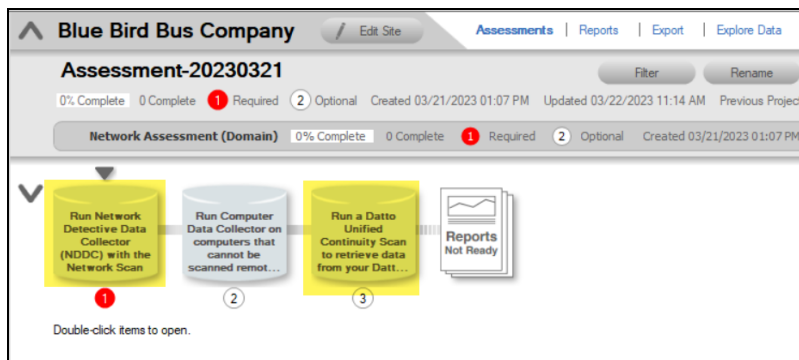


Step 3 — Perform Network Assessment Scan

Before you can perform a Datto Unified Continuity Scan, you must first:

1. **Create a Network Assessment project.**
2. **Perform a Network Scan.** Perform the Network Scan on the same environment where you want to collect Datto Continuity data.

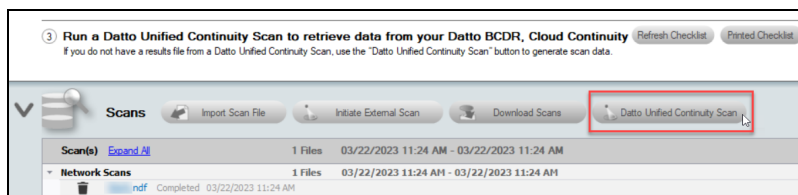
After you complete ["Step 2 — Enable Datto Unified Continuity Integration" on page 266](#), the "Run a Datto Unified Continuity Scan" task will appear in your checklist.



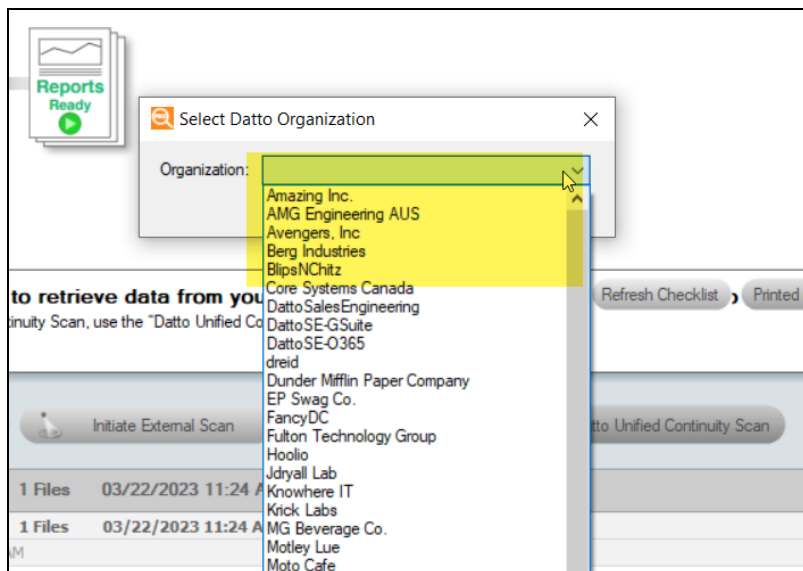
Step 4 — Perform Datto Unified Continuity Scan

Once you perform a network scan, you can then perform the Datto Unified Continuity Scan.

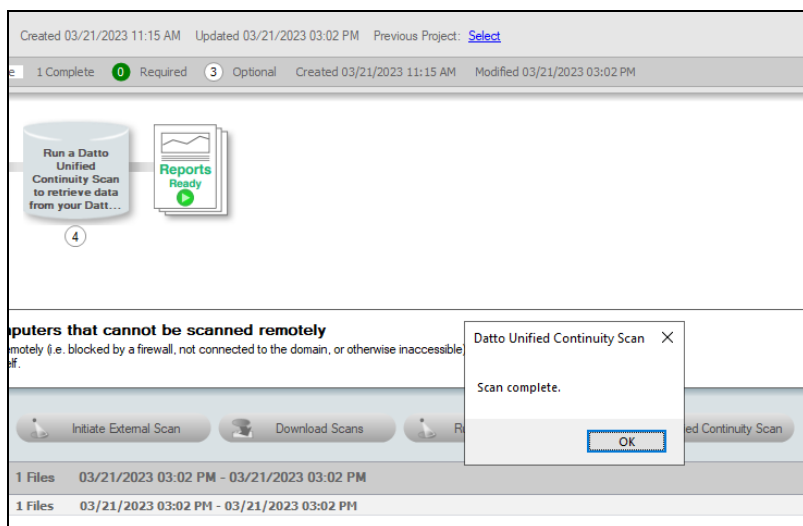
1. From the Scans bar, click **Datto Unified Continuity Scan**.



2. Choose the Datto **Organization** from the drop-down menu and click **Scan**.



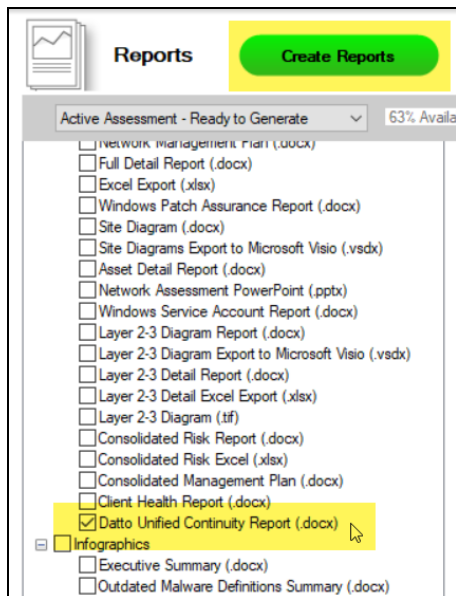
3. You will receive a success notification when the scan completes.



Step 5 — Generate Reports

Once you perform the Datto Unified Continuity Scan, you can generate the **Datto Unified Continuity Report**.

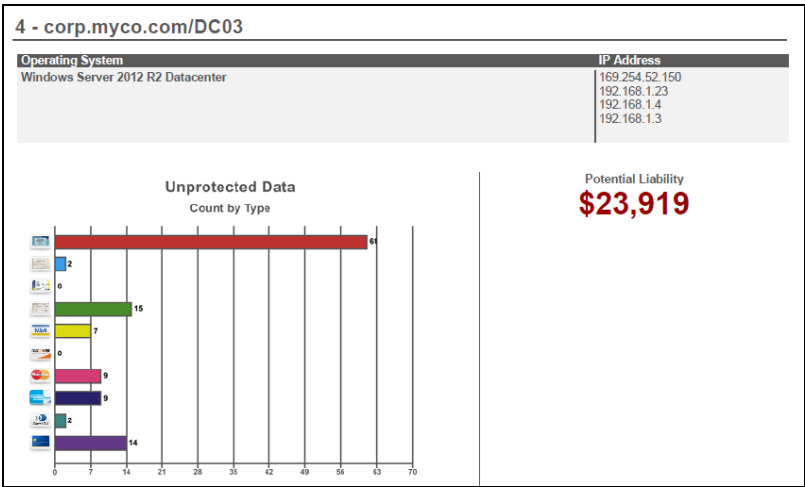
1. From your Network Detective Pro site, navigate to **Reports**.



2. From Network Assessment reports, **check the Datto Unified Continuity Report**.
3. Then click **Create Reports**. The Datto Unified Continuity Report will then be available for your review.

Data Breach Liability Scanning and Reporting

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



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

RISK SUMMARY					
Total Potential Liability					
\$149,142					
Computer	IP Address	Missing Critical Patches	Anti-virus/ Anti-spyware	Sensitive Data Count	Potential Liability (\$)
	corp.myco.com/darkhorse	0	✓	623	\$125,223
	169.254.24.1				
	50				
	169.254.58.2				
	corp.myco.com/DC03	0	✓	119	\$23,919
	169.254.52.1				
	50				
	192.168.1.23				
	192.168.1.4				
	192.168.1.3				

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**.

NetworkDetective Push Deploy Tool - v2.0.1128

Settings and Configuration

Computers and Status

Collected Data Files

Settings and Configuration

Scan Settings

Storage Folder: C:\Users\...\.NetworkDetectivePushDeployTool

Scan Type:

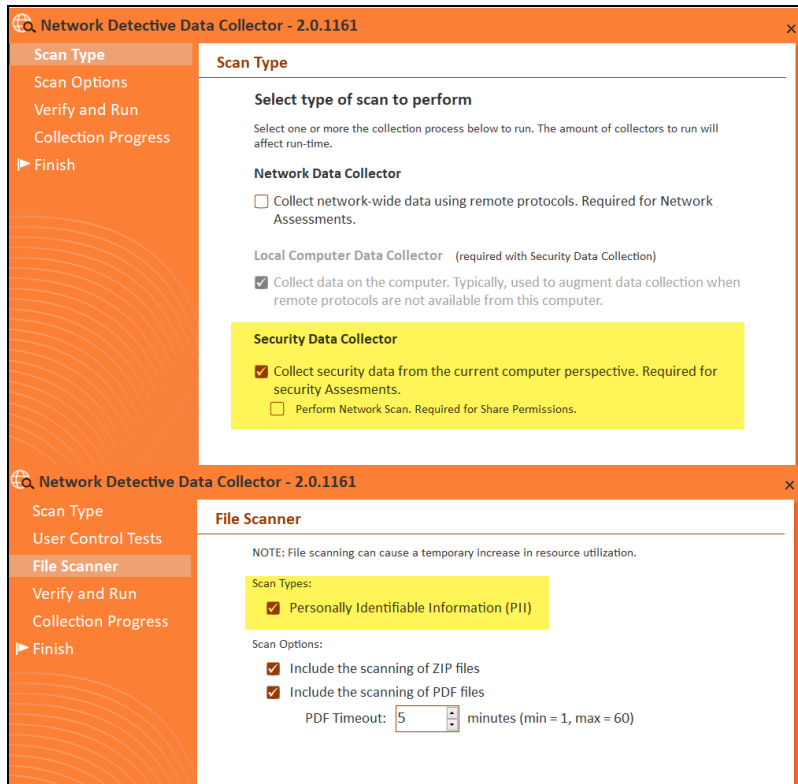
- ☒ Computer Scan
- ☒ Security Scan
- ☐ HIPAA Quick
- ☐ HIPAA Deep
- ☐ PCI Quick
- ☒ PCI Deep
- ☐ BDR Scan
- ☒ PII Scan

Deep Scan Option:

- ☒ Include the scanning of PDF Files

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 Reports

☒ 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 through 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:

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

The screenshot shows a web-based form interface. At the top, it displays '1 test1. it.com (2 Required Remaining)' with a red arrow pointing to the 'Section' label. Below this is a paragraph of instructions, with a red arrow pointing to the 'Instructions' label. The main content area is titled '1.1 Administrator' and 'Topic/Question'. It contains a dropdown menu with 'Vendor - ePHI authorization' selected, with a red arrow pointing to the 'Answer field' label. To the right of the dropdown are four icons: a document, a person, a folder, and a blue square. Red arrows point from these icons to labels: 'Add Notes' (document), 'Add Respondent name' (person), and 'Add attachment' (folder). A red arrow points from the blue square icon to the 'Add SWOT analysis' label.

- Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.
- 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 Pro.
2. Underneath an InForm item, click on the folder icon.



1.1 Administrator
Name: Administrator Enabled: enabled Last Login: 10/5/2017 1:27:30 PM Job Title: Department: Company: Detected Service Account:
No
Vendor - ePHI authorization
Add

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

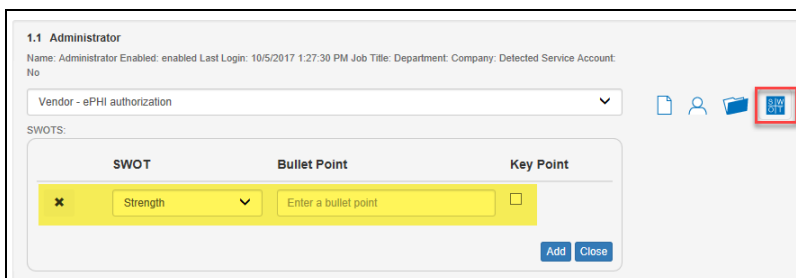
Note: Once you complete your assessment and generate reports, your attached images will appear alongside the form item in the published report and/or supporting document.

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.

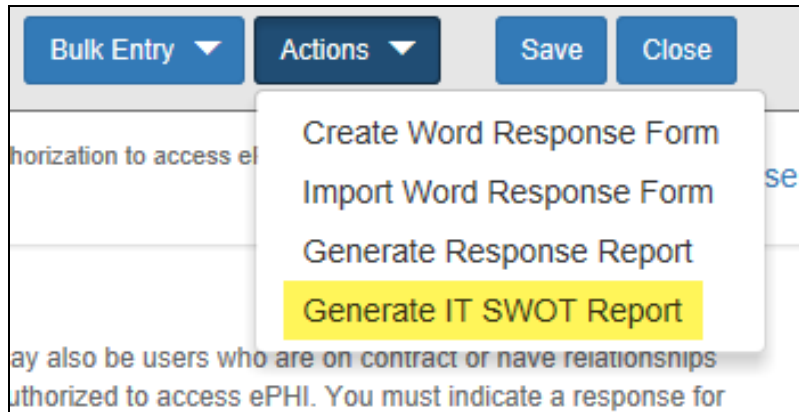
To add SWOT to your inform items:

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



1.1 Administrator
Name: Administrator Enabled: enabled Last Login: 10/5/2017 1:27:30 PM Job Title: Department: Company: Detected Service Account:
No
Vendor - ePHI authorization
Add
SWOTS:
SWOT Bullet Point Key Point
x Strength Enter a bullet point
Add Close

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**.

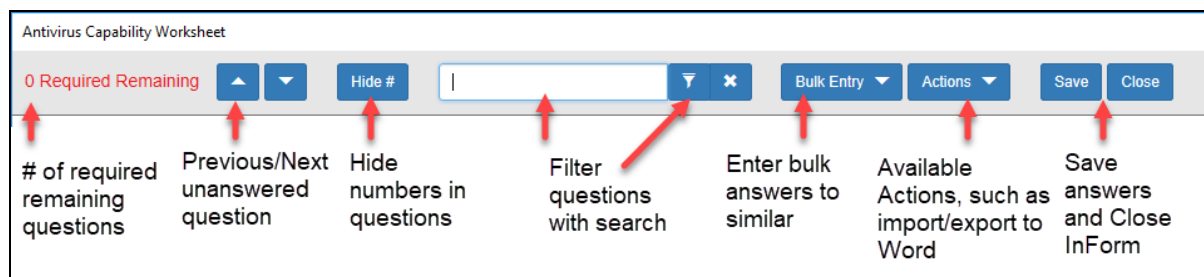


Note: A folder will open with your generated IT SWOT Report. You must generate this report separately for each InForm in your assessment.

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.

The screenshot shows the 'User Identification Worksheet' interface. At the top, there's a status bar with '0 Required Remaining', navigation arrows, a 'Hide #' button, a 'Filter Topics' search bar, and buttons for 'Bulk Entry', 'Actions', 'Save', and 'Close'. The 'Bulk Entry' button is highlighted with a mouse cursor. Below the status bar, there are two main sections: 'Filter' and 'Bulk Entry'. The 'Filter' section includes a 'Key Words' input field, a dropdown arrow, a close button, and 'Select All Filtered' and 'Deselect All Filtered' buttons. The 'Bulk Entry' section includes a 'Select topics of same response type' dropdown, a 'Note' input field, a 'Respondent' input field, and an 'Apply to Selected' button.

Check boxes will appear next to the response topics.

The screenshot shows the 'User Identification Worksheet' interface with the 'Bulk Entry' section expanded. The status bar now shows '2 Required Remaining'. The 'Filter' section is still visible. The 'Bulk Entry' section includes a 'Select topics of same response type' dropdown, a 'Note' input field, a 'Respondent' input field, and an 'Apply to Selected' button. Below the 'Bulk Entry' section, there's a 'Category' section with 'Previous', '1', '2', and 'Next' buttons. The main content area shows a list of response topics with checkboxes. The first topic is '1.1 adminonly' with a checkbox. Below it, there's a 'Notes' section with a dropdown menu and a list of details: Name: admin only, Enabled: enabled, Last Login: 7/2/2014 8:26:48 AM, and Job Title: Administrator. The second topic is '1.2 Administrator' with a checkbox. Below it, there's a 'Notes' section with a dropdown menu and a list of details: Name: Administrator, Enabled: enabled, Last Login: 9/27/2017 12:57:35 PM, and Job Title: Administrator.

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

2 Required Remaining

Filter Topics

Key Words

Select All Filtered Deselect All Filtered

Bulk Entry

Note

Respondent

Apply to Selected

Category Previous 1 2 Next

1.1 adminonly

Select user type and access level.

Notes:

Name: admin only
Enabled: enabled
Last Login: 7/2/2014 8:26:48 AM
Job Title:

1.2 Administrator

Select user type and access level.

Notes:

Name: Administrator
Enabled: enabled
Last Login: 9/27/2017 12:57:35 PM
Job Title:

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.

3 Required Remaining

Filter Topics

Key Words

Select All Filtered Deselect All Filtered

Bulk Entry

Employee - no CDE access
Employee - CDE access
Employee - POS Terminal Access Only
Vendor - no CDE access
Vendor - CDE access
Vendor - POS Terminal Access Only
Former Employee
Former Vendor
Service Account
Generic Account

Apply to Selected

Category Previous 1 2 Next

1.1 adminonly

Select user type and access level.

Notes:

Name: admin only
Enabled: enabled
Last Login: 7/2/2014 8:26:48 AM
Job Title:

1.2 Administrator

Select user type and access level.

Notes:

Name: Administrator
Enabled: enabled
Last Login: 9/27/2017 12:57:35 PM
Job Title:

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

0 Required Remaining

Filter Topics

Bulk Entry

Actions

Save

Close

Filter

Key Words

Select All Filtered

Deselect All Filtered

Bulk Entry

Select topics of same response type

Note

Respondent

Apply to Selected

Category

Previous

1

2

Next

1.1 adminonly

Select user type and access level.

Vendor - no CDE access

Notes:

Name: admin only

Enabled: enabled

Last Login: 7/2/2014 8:26:48 AM

Job Title:

1.2 Administrator

Select user type and access level.

Vendor - no CDE access

Notes:

Name: Administrator

Enabled: enabled

Last Login: 9/27/2017 12:57:35 PM

Job Title:

Your chosen response will be entered into the selected topics.

Create Word Response Form

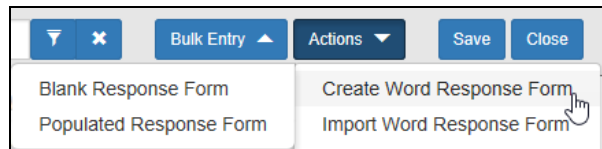
You can export InForm worksheets in your assessment project to Word. This allows you or others to complete worksheets without using Network Detective. For example, you can create a Word response form and send it to a client at a site. The client can then help you gather the required information and enter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

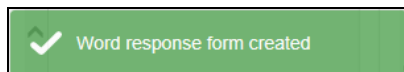
1. From the Active Assessment screen in Network Detective Pro, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
 - a. Click **Blank Response Form** to generate a Word document with blank fields ready for data entry.
 - b. Click **Populated Response Form**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



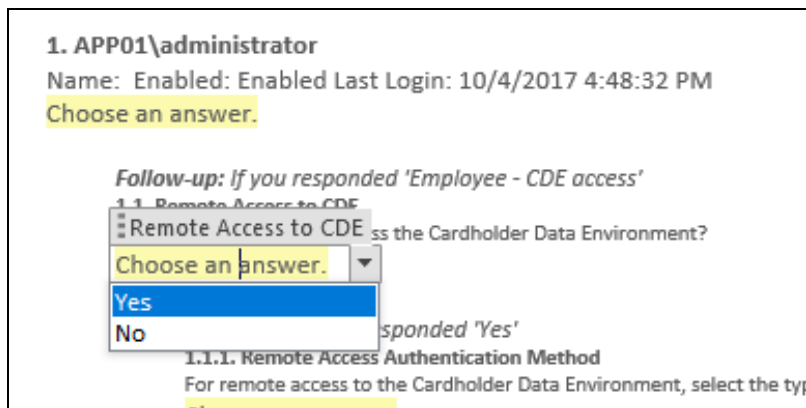
Important Note on Working with Word Response Forms

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

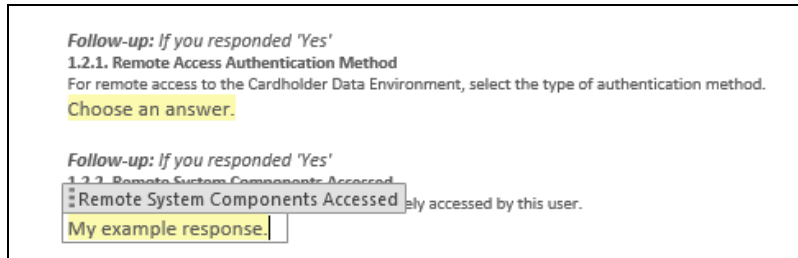
- **DO NOT DELETE** the field controls embedded in the response form! The response fields appear in the images below for your reference:

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

Multiple choice response field



Text response field



Follow-up: If you responded 'Yes'

1.2.1. Remote Access Authentication Method

For remote access to the Cardholder Data Environment, select the type of authentication method.

Choose an answer.

Follow-up: If you responded 'Yes'

1.2.2. Remote System Components Accessed

Remote System Components Accessed

My example response.

- 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.

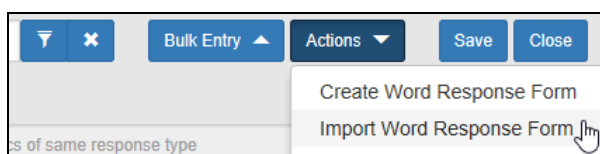
Step 2: Send it to a client to enter additional information about the site using Word.

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.

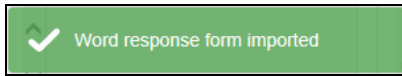
To import a Word response form:

1. From the Active Assessment screen in Network Detective Pro, 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**.

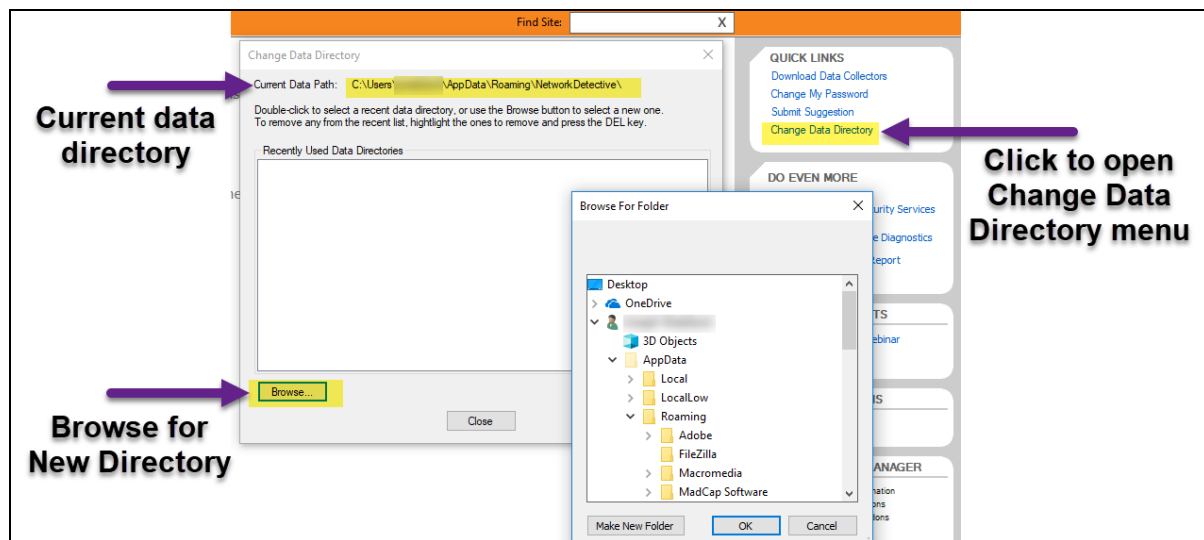
A confirmation message will appear. The InForm worksheet fields will be updated with the imported responses.



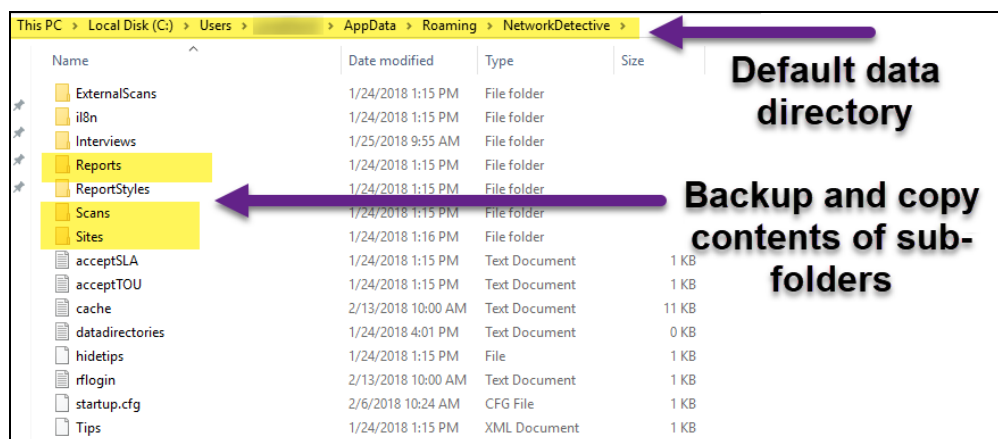
Compiling Network Detective Data

In order to share sites, scans and reports between all Network Detective Pro 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.

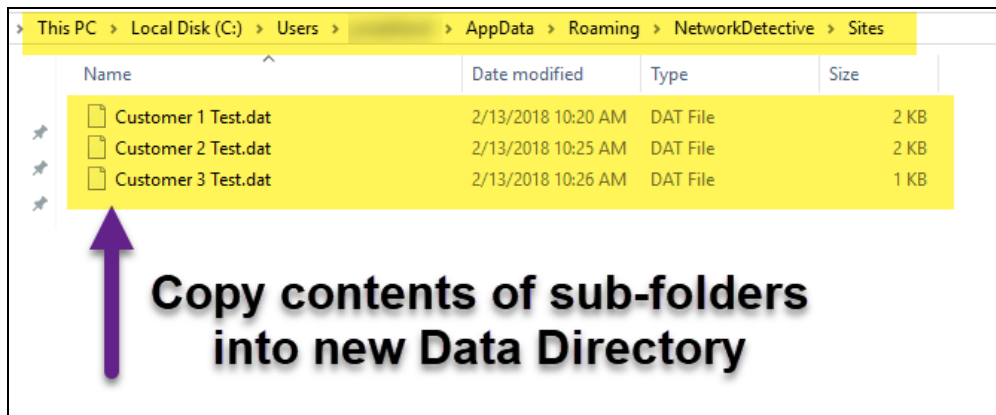


Changing the directory will automatically create a new Network Detective folder along with all of the corresponding subfolders. Any data already created locally will not migrate automatically. To retain this data, navigate to the **C:\Users\[User]\AppData\Roaming\NetworkDetective** folder (you may need to enable hidden file viewing) and copy the relevant contents of any subfolders you wish to retain.

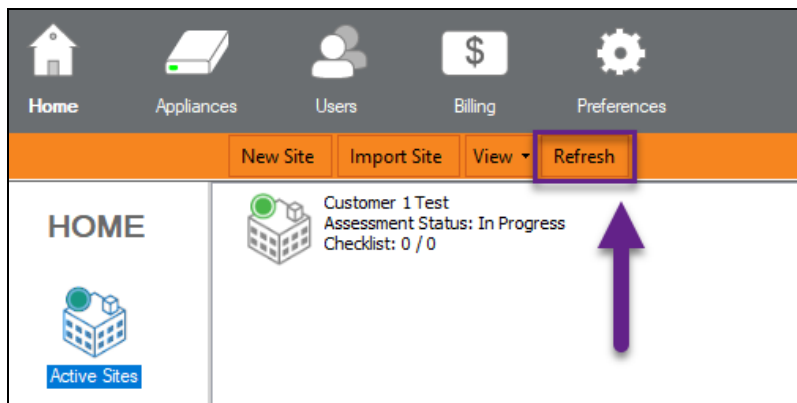


Most importantly, copy the contents of the **Reports**, **Scans**, and **Sites** subfolders over to corresponding subfolders of the new directory.

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 Pro with a PSA System

With Network Detective Pro, 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 Pro 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 Pro
- A Network Detective Pro "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 Pro 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
	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 301. • Autotask API Username • Autotask API Password
	• ConnectWise REST Public Key • ConnectWise REST Private Key • ConnectWise Company ID • ConnectWise PSA URL

PSA System	PSA Prerequisites
	Note: You must configure ConnectWise correctly before you can integrate with Network Detective Pro. See "Set Up ConnectWise REST Integration" on page 306 for detailed instructions.
	• ConnectWise Username • ConnectWise Password • ConnectWise Company ID • ConnectWise PSA URL Note: You must configure ConnectWise correctly before you can integrate with Network Detective Pro. See "Set Up ConnectWise SOAP Integration" on page 315 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 317 detailed instructions. • Kaseya Tenant (i.e. company name) • Kaseya API URL, example: "https://bms.kaseya.com" (you

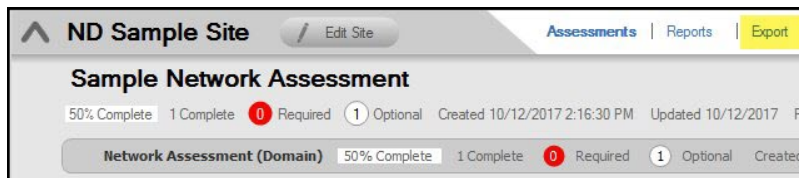
PSA System	PSA Prerequisites
	should receive the exact URL in an email from Kaseya)

Step 2 — Create a Connection Between Network Detective Pro and Target PSA

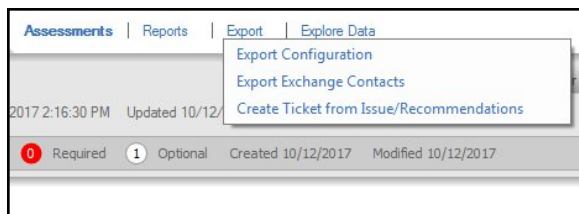
1. If you have not already done so, visit <https://www.rapidfiretools.com/ndpro-downloads/> to **download and install Network Detective Pro**.
2. **Start Network Detective Pro** and log in with your credentials.
3. Open the **Site** for which you wish to create tickets in the target PSA.

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**.



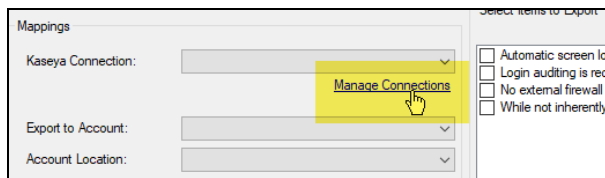
5. Choose an export option from the drop-down menu.



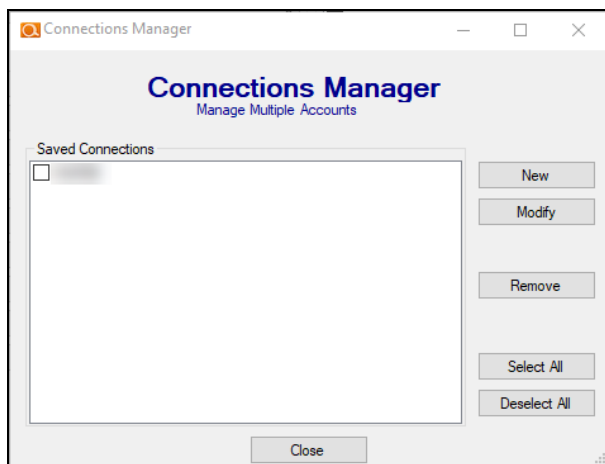
6. **Select your Target** Ticketing/PSA system from the list of supported options.



7. Click **Manage Connections**.

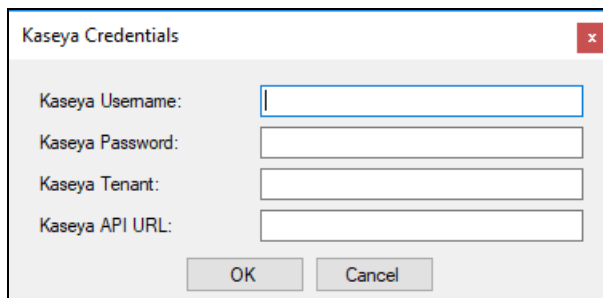


The Connections Manager window will be displayed.



8. Select the **New** button in the Connections Manager window to create a new PSA connection.

The PSA Credentials window will be displayed

A screenshot of the 'Kaseya Credentials' dialog box. It has a title bar with a close button (X). Inside, there are four labeled text input fields: 'Kaseya Username:', 'Kaseya Password:', 'Kaseya Tenant:', and 'Kaseya API URL:'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

9. Enter the credentials for chosen PSA.

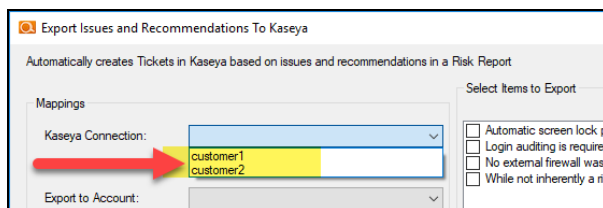
Important: To generate login credentials for ConnectWise REST, see ["Set Up ConnectWise REST Integration" on page 306](#). To generate login credentials for ConnectWise SOAP, see ["Set Up ConnectWise SOAP Integration" on page 315](#).

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.

A screenshot of the 'Export Issues and Recommendations To Kaseya' dialog box. The title bar includes a Kaseya logo and the text 'Export Issues and Recommendations To Kaseya'. Below the title bar, it says 'Automatically creates Tickets in Kaseya based on issues and recommendations in a Risk Report'. There are two main sections: 'Mappings' on the left and 'Select Items to Export' on the right. In the 'Mappings' section, there is a 'Kaseya Connection:' dropdown menu with 'customer1' and 'customer2' as options; a red arrow points to this dropdown. Below it is an 'Export to Account:' dropdown menu. In the 'Select Items to Export' section, there are four checkboxes: 'Automatic screen lock p', 'Login auditing is required', 'No external firewall was', and 'While not inherently a r'.

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.

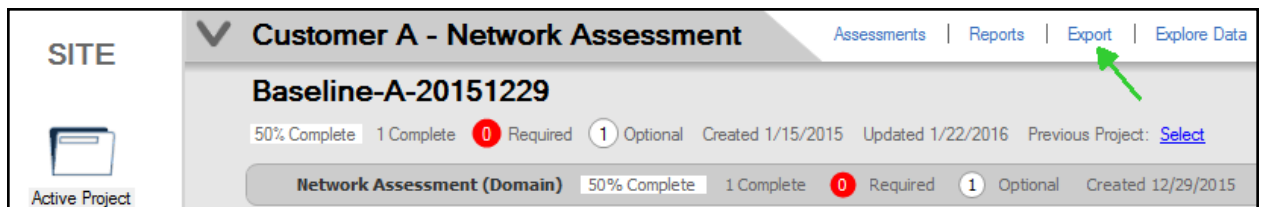
Once you have created the connection, you can then use the **Export** features:

- ["Export Configuration Items from Network Detective Pro to PSA" below](#)
- ["Export Exchange Contacts from Network Detective Pro to PSA" on page 298](#)
- ["Create Tickets from Assessment Issues and Recommendations from Network Detective Pro to PSA" on page 298](#)

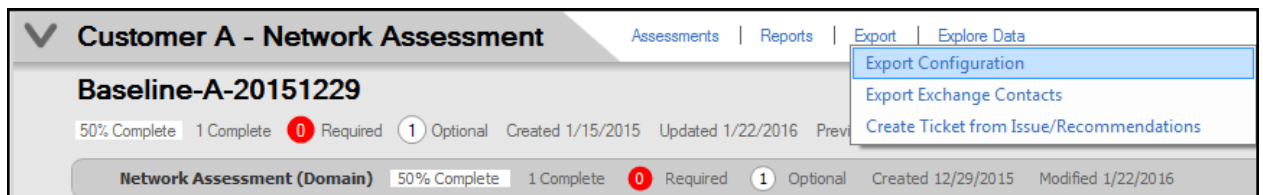
Export Configuration Items from Network Detective Pro to PSA

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:

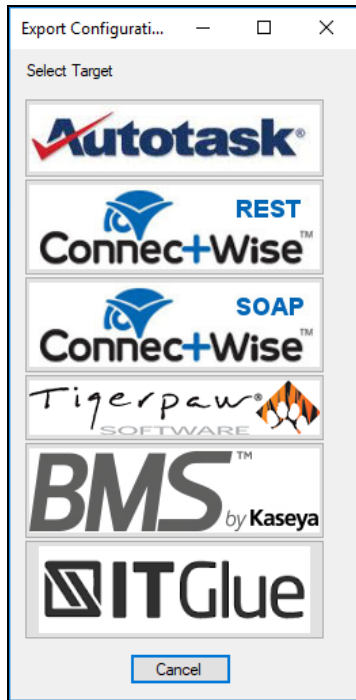
1. Open the **Site** and **Assessment Project** for which you wish to create tickets.
2. Within the Assessment window, click **Export**.



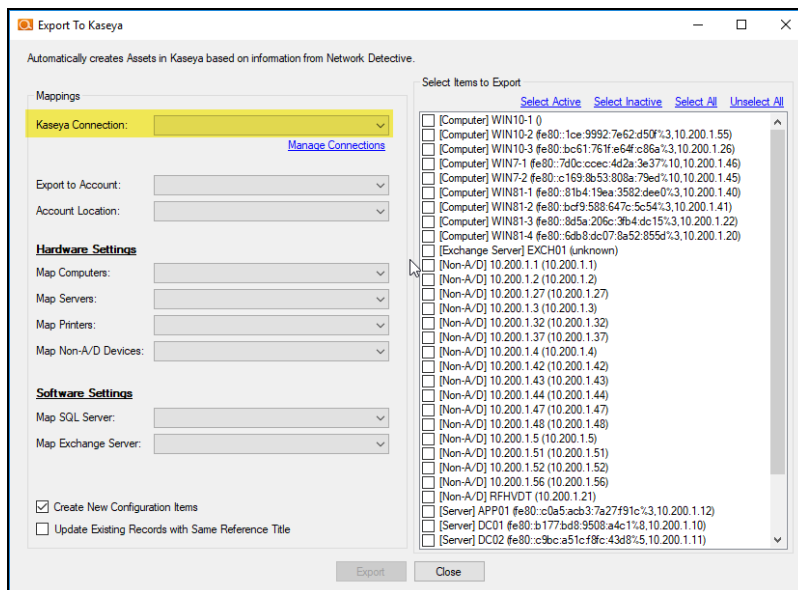
3. Click **Export Configuration**.



4. Select the **Target PSA** from the menu.



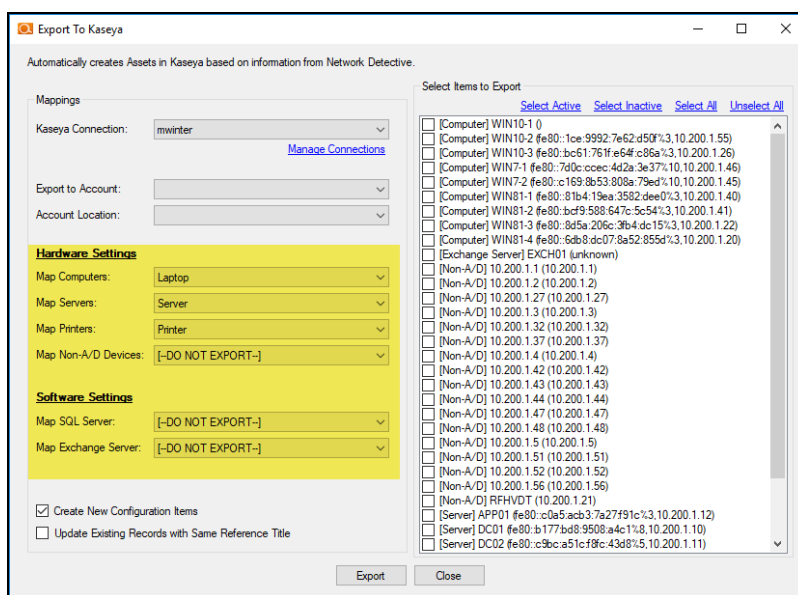
5. The **Export Issues/Recommendations** window will appear.
6. Select a **Connection** from the drop-down menu. The Connection determines the specific PSA account to which the tickets will be exported.



Important: If you have not yet created a connection, see ["Integrate Network Detective Pro with a PSA System"](#) on page 287 and follow the instructions there. Then return to this help topic.

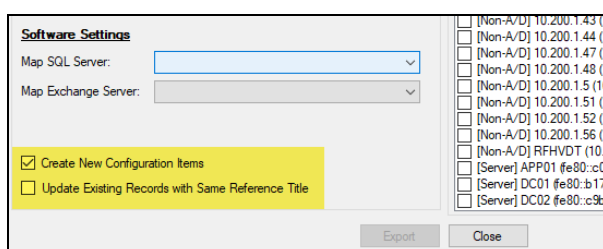
Note: When the Connection between Network Detective Pro and the PSA is established, some of the fields in the Mapping menu will automatically populate. This may take up to 60 seconds.

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.

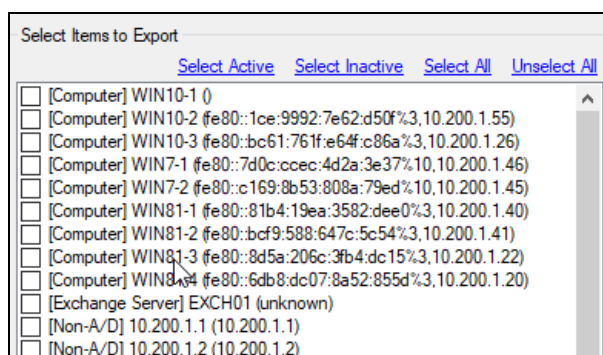
8. Choose whether to **Create New Configuration Items**. This will create new items in your PSA, even the items already exist.



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.

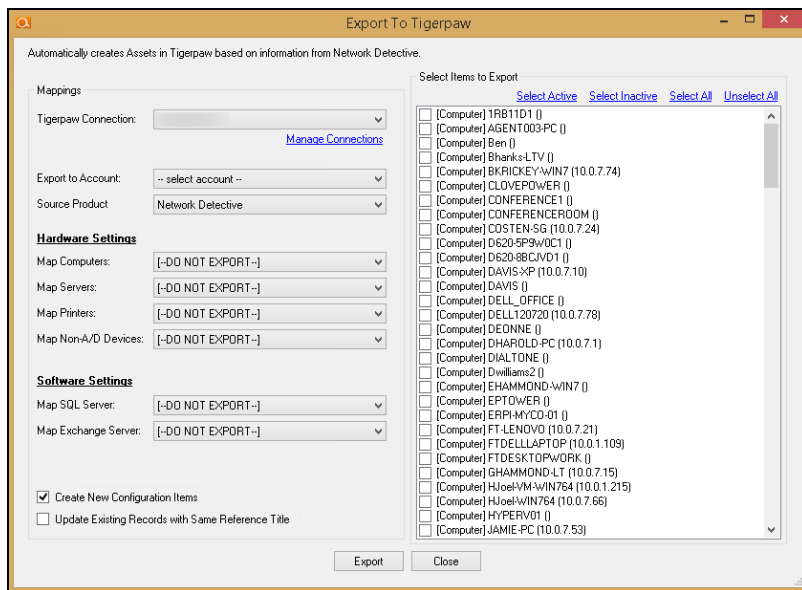
Export fields for Autotask

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

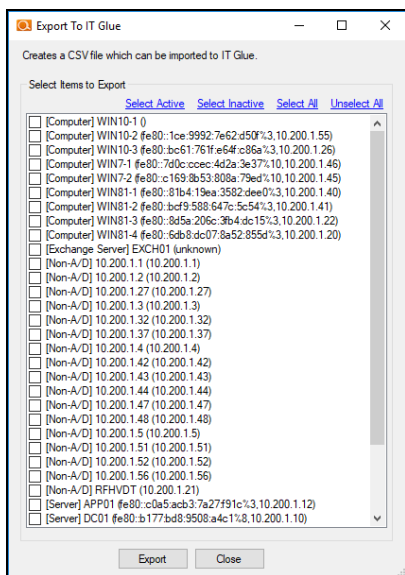
When exporting to ConnectWise, you can use any existing Configuration Types that you have setup. In this case, Network Detective will populate the standard fields, and the Notes field will be set with the information for that system (CPU, Memory, etc.). If there was information in the Notes field, it 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 Pro will then create a CSV file. Import the file into IT Glue.

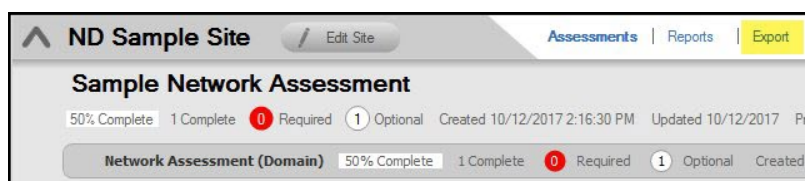
Export Exchange Contacts from Network Detective Pro to PSA

Help topic coming soon!

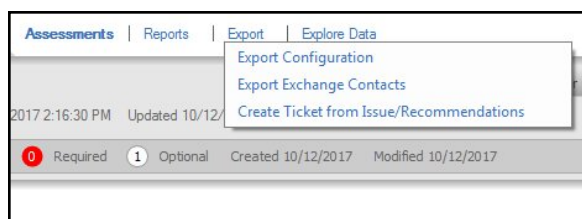
Create Tickets from Assessment Issues and Recommendations from Network Detective Pro to PSA

Network Detective Pro 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**.



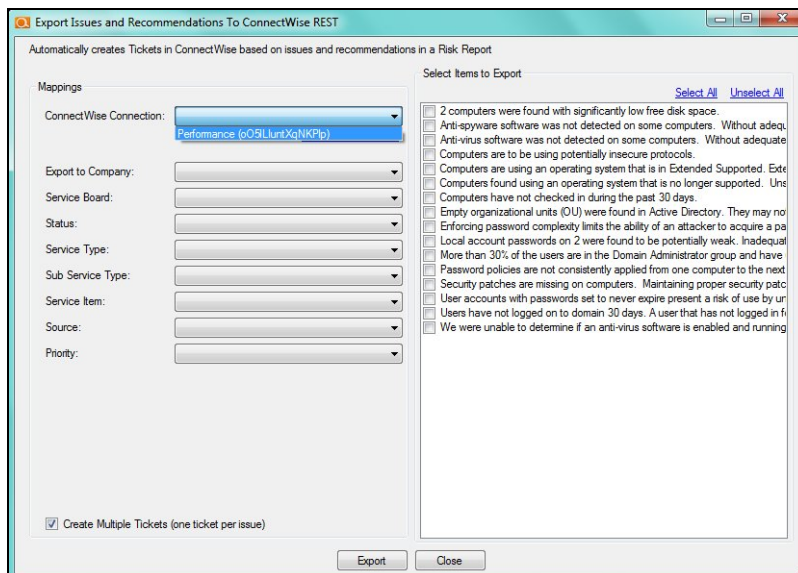
3. Click **Create Ticket from Issues/Recommendations**.



4. Select your preferred **Target** PSA from the menu.

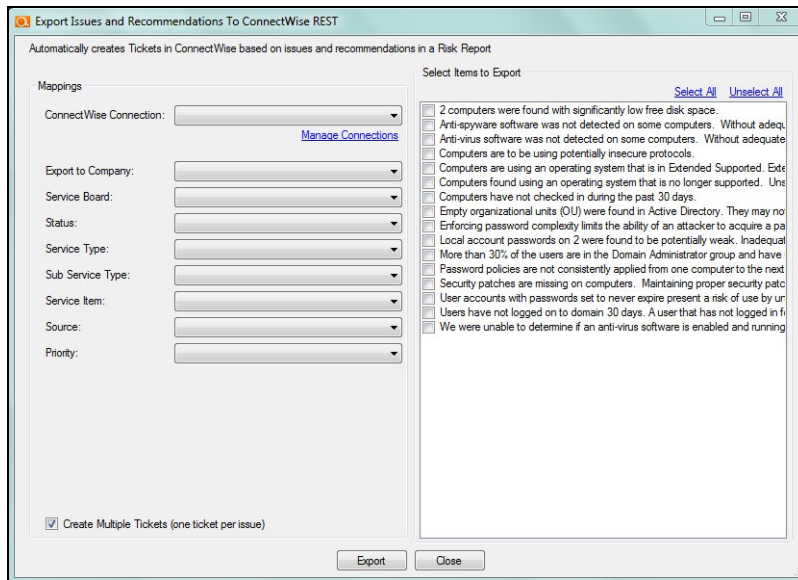


5. The **Export Issues/Recommendations** window will appear.
6. Select a **Connection** from the drop-down menu. The Connection determines the specific PSA account to which the tickets will be exported.



Important: If you have not yet created a connection, see ["Integrate Network Detective Pro with a PSA System"](#) on page 287 and follow the instructions there. Then return to this help topic.

Note: When the Connection between Network Detective Pro and the PSA is established, some of the fields in the Mapping menu will automatically populate. This may take up to 60 seconds.

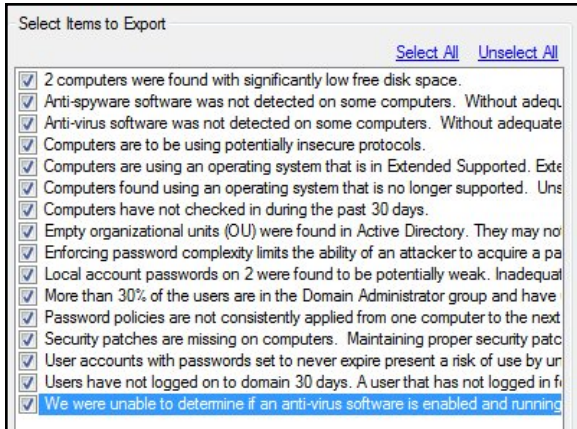


7. Map the issues to service ticket fields in your PSA. These mappings allow you to configure how the issues in Network Detective Pro are created as tickets in your PSA.

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.

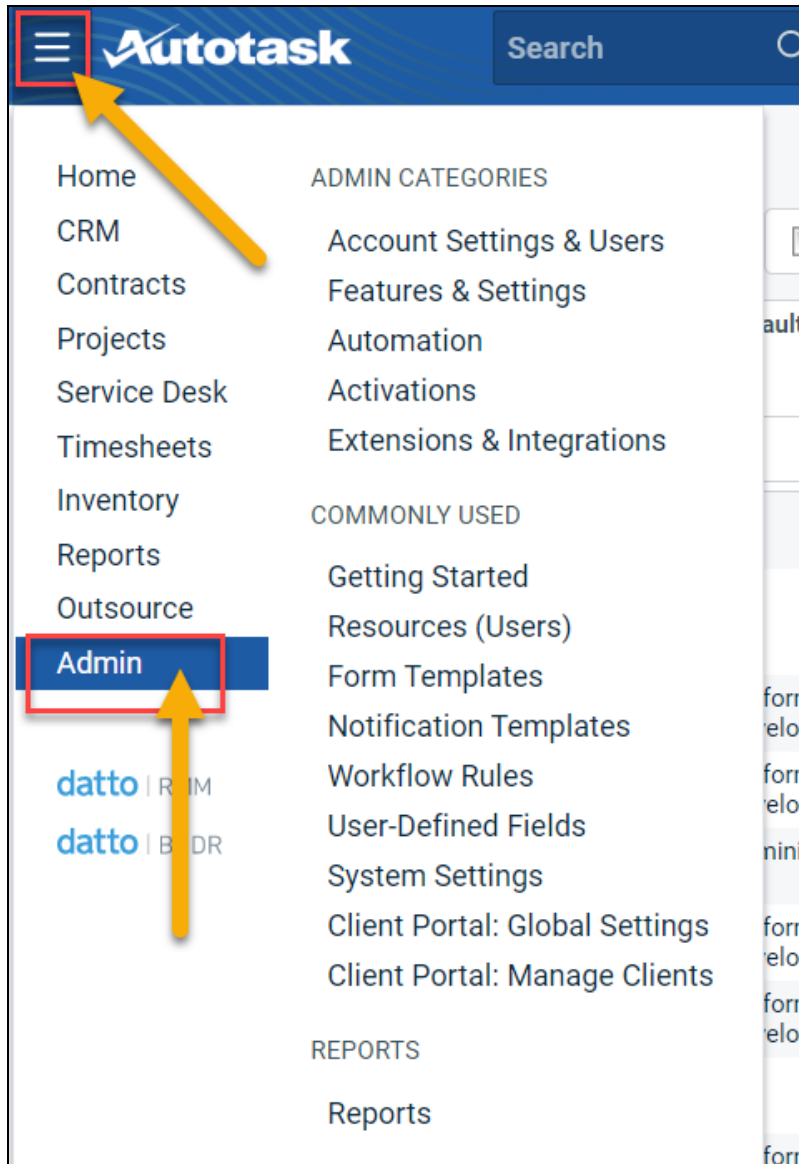
After the export is complete, an Export Complete status window will be displayed indicating the number of Issues tickets created in the PSA.

Note: You can then log in to your PSA and confirm that your tickets have been created.

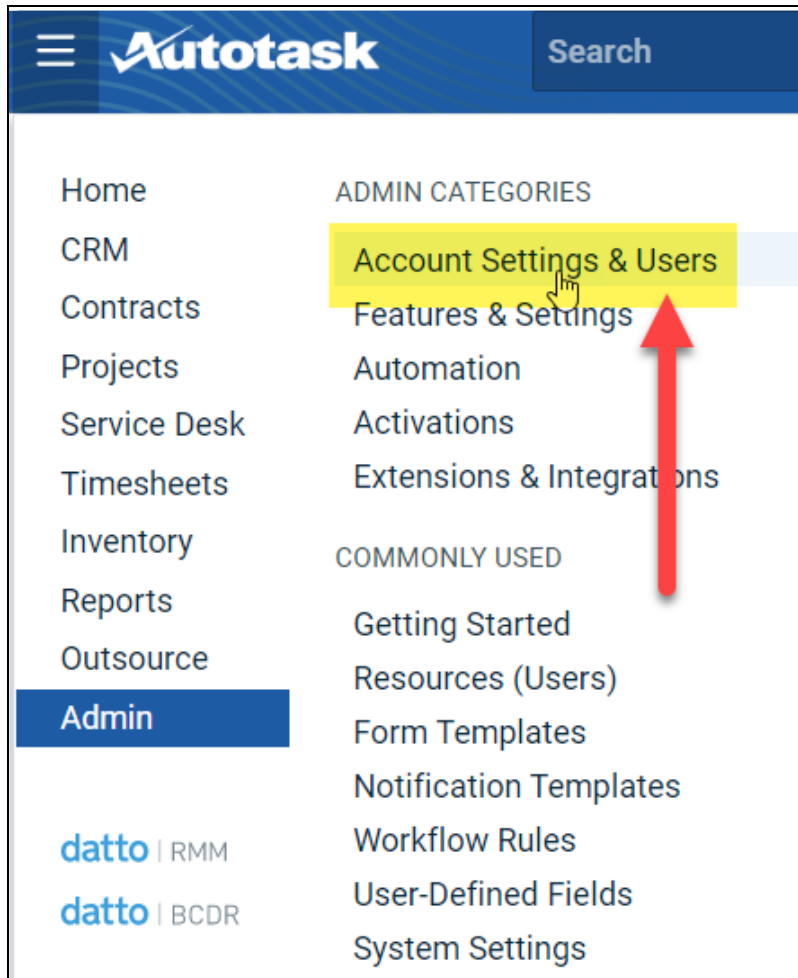
Set Up Autotask Integration

To set up a connection with the Autotask system, you will need to **create an API User in Autotask**. To do this:

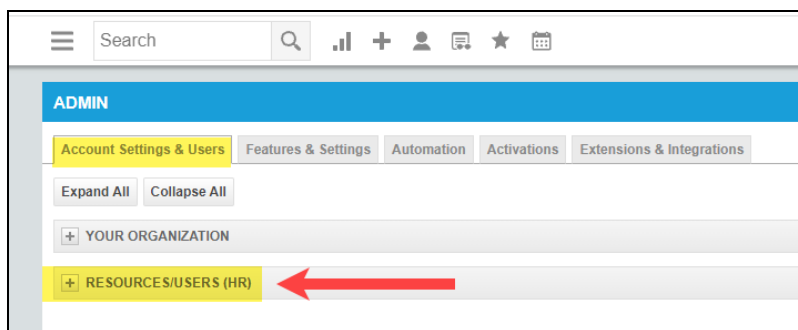
1. Log in to Autotask with your admin user credentials.
2. Click on the **Autotask home** button on the left, then click **Admin**.



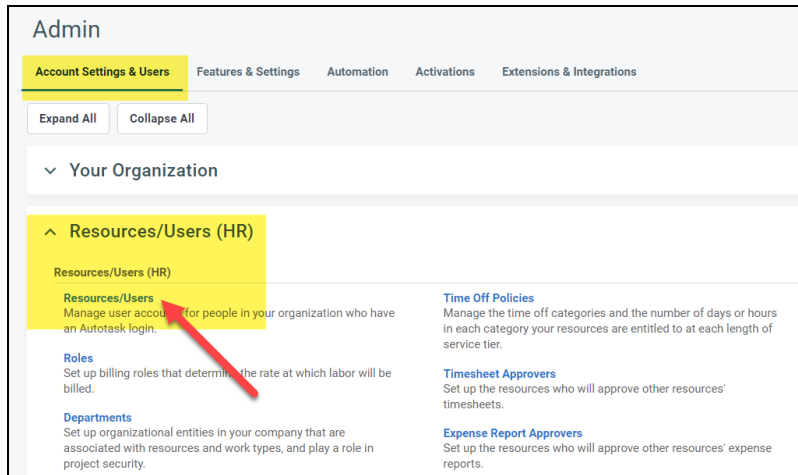
3. From the **Admin** menu, click **Account Settings & Users**.



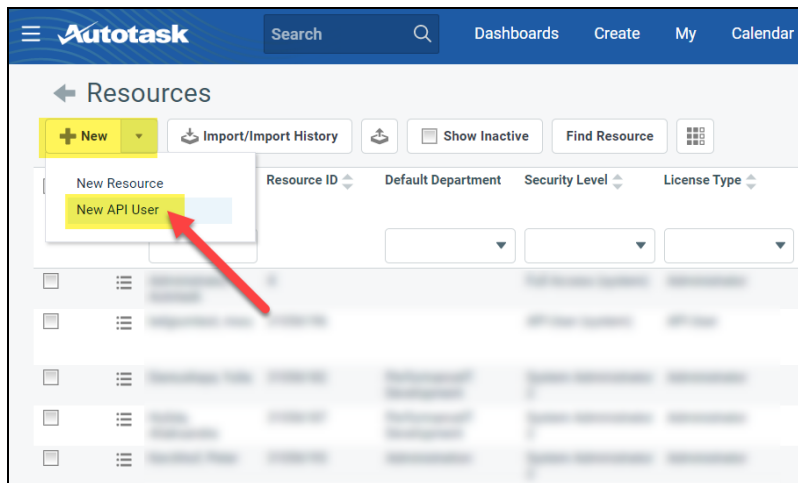
4. Next, click **Resources/Users (HR)** to expand the menu.



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.

Add API User
?

Save & Close
Cancel
[Review Terms and Conditions for API Use](#)

General

First Name *
Last Name *
Email Address *

Security Level *
Date Format
MM/dd/yyyy
Time Format
hh:mm a
Number Format
X,XXX.XX
Primary Internal Location *

☒ Active
☐ Locked

Credentials

Generate Key
Generate Secret

Username (Key) *
Password (Secret) *

API Tracking Identifier

API version 1.6 & later require the user of an API tracking identifier. Once assigned, this cannot be changed.

☒ Integration Vendor
☐ Custom (Internal Integration)

Integration Vendor *
RapidFire Tools - Network Detective

Line of Business

A line of business can be used to grant access or prevent access to data associated with Contracts, Tickets, Projects, etc.

Not Associated
Associated

☒ Resource can view items with no assigned Line of Business

- 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:

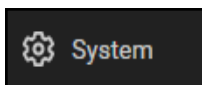
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

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**.

System			
Role ID*		Location*	
Admin	▼	Tampa Office	▼
Level*		Business Unit*	
Corporate (Level 1)	▼	Admin	▼

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.

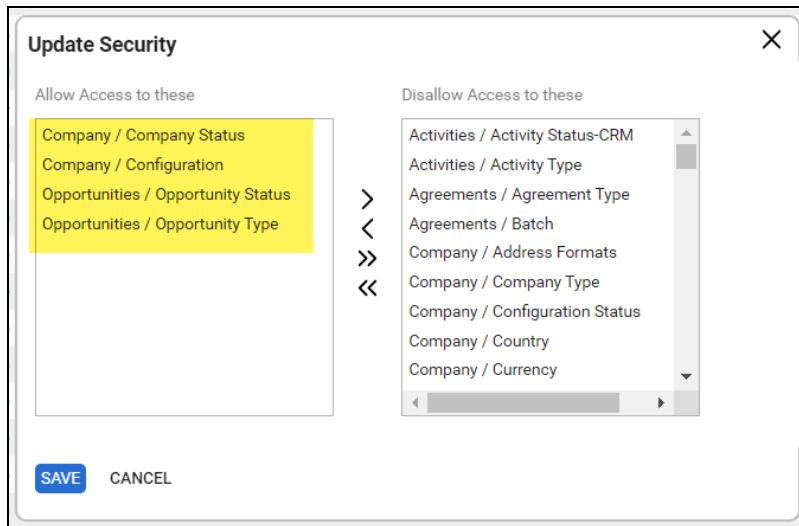
Module		Add Level	Edit Level	Delete Level	Inquire Level
Companies					
	Company Maintenance				All
	Configurations	All	All		All
	Contacts	All	All		All
Service Desk					
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup*	All			All
	*Customized Table Setup: Allow Company / Company Status, Company / Configuration, Opportunities / Opportunity Status, Opportunities / Opportunity Type (See "Table Setup Configuration" below below for an extended explanation)				

Table Setup Configuration

From Table Setup, click **customize**.

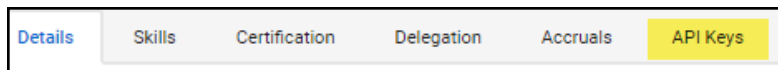
Report Writer	None	▼	None	▼	None	▼	None	▼
Security Roles	None	▼	None	▼	None	▼	None	▼
System Reports (customize)	None	▼	None	▼	None	▼	None	▼
Table Setup (customize)	All	▼	None	▼	None	▼	All	▼
Today Links	None	▼	None	▼	None	▼	None	▼
^ Time & Expense								7/25/23
Expense Approvals	None	▼	None	▼	None	▼	None	▼

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

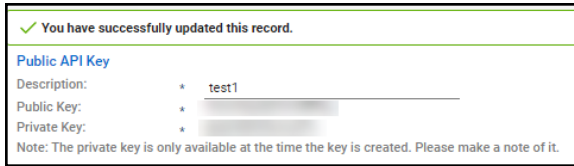
1. Select the API Member that you created previously.
2. From the API Member details screen, click **API Keys**.



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.



A screenshot of a web interface showing a confirmation message at the top: "✓ You have successfully updated this record." Below this is a section titled "Public API Key". It contains three fields: "Description:" with the value "test1", "Public Key:" with a masked value, and "Private Key:" with a masked value. At the bottom of this section is a note: "Note: The private key is only available at the time the key is created. Please make a note of it."

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.

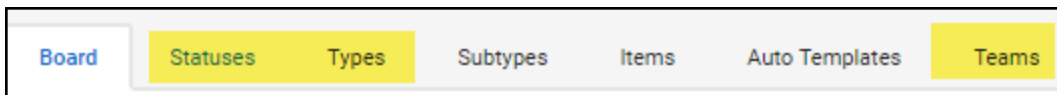
You can configure the Service Tables in ConnectWise from **System > Setup Tables > Category > Service**. Configure the Service Tables as detailed below:

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.



A screenshot of a navigation bar for the Service Board. It contains several tabs: "Board" (highlighted in blue), "Statuses" (highlighted in yellow), "Types" (highlighted in yellow), "Subtypes", "Items", "Auto Templates", and "Teams" (highlighted in yellow).

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	▼	
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.

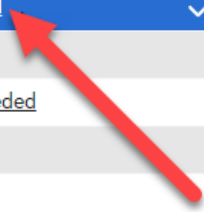
2. From Company Status, open the **not Approved** field.

Setup Tables > Company Status List

Company Status List

< + SEARCH CLEAR

Description	Default	Inactive	Notify	Custom Note
<u>Active</u>				
<u>Inactive</u>			✓	
<u>Imported</u>			✓	
<u>Credit Hold</u>			✓	
<u>Problem</u>			✓	
<u>not-Approved</u>	✓		✓	
<u>Solid</u>				
<u>Attention needed</u>			✓	
<u>may Leave</u>			✓	
<u>Delinquent</u>			✓	



- Uncheck the **Disallow Saving** flag.

Setup Tables > Company Status List > Company Status

Company Status

< +   ↺ HISTORY ▾ 

Company Status

Description*

not-Approved

☒ Default

☐ Inactive

Notification Parameters for Service, Project and Time

☒ Notify

☒ Disallow Saving

Notification Message

Do not Service
they have not been setup for Service yet
check with their account manager

Company Status

Description*

not-Approved

☒ Default

☐ Inactive

Notification Parameters for Service, Project and Time

☒ Notify

☐ Disallow Saving

Notification Message

Do not Service
they have not been setup for Service yet
check with their account manager

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.

Company Search > Company > Company Finance Detail

Micro Pro

Summary | Recap | Invoices 0 | Time 0 | Expenses 0

< | [Icon] | [Icon] | [Icon] | [Icon] | History | Links

Company: Micro Pro

Company: * Micro Pro Phone: _____

Company ID: * 123 Fax: _____

Status: * not-Approved [Dropdown Arrow] [Icon] Web Site: _____

Type: *

Prospect X

Finance Details [Icon]

Set Up ConnectWise SOAP Integration

This topic covers how to integrate Network Detective Pro 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.

Setup Tables

Setup Tables

SEARCH CLEAR

Category	Table ^	Description
	integrator	
General	<u>Integrator Login</u>	Setup Integrator Access

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 Pro.
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

Integrator Login

Setup Logs

< + HISTORY ▾

Username*
api

Password
....

Access Level
☐ Records created by Integrator
 ☒ All Records

Select the available API integration(s) you wish to enable and configure below:

☐	API Name	Callback URL	☐ Use legacy
☒	Activity		☐ Use legacy
☐	Agreement		☐ Use legacy
☐	Company		☐ Use legacy

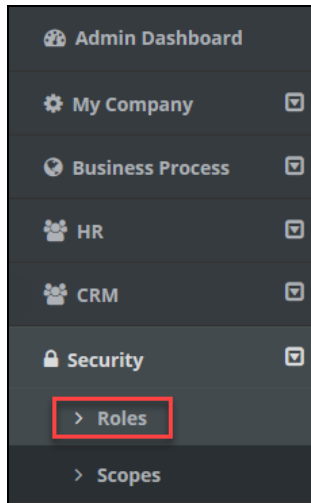
8. Click the **Save** icon to save this Integrator Login.

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.

	CRM Manager	CRM Manager
	Project Manager	Project Manager
	Service Desk Manager	Service Desk Manager
	Administrator	Administrator

4. Click the **Role Users** tab.

Security Role Information

Name: *

Administrator

Status:

☒ Active

Permissions

Role Users

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.

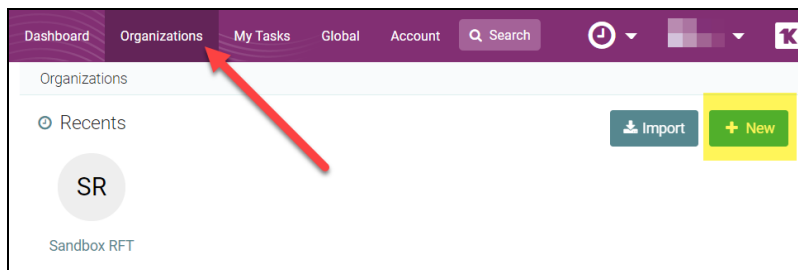
Export Network Detective Pro Reports to IT Glue

Network Detective Pro allows you to export your reports as documents in **IT Glue**, the Kaseya IT documentation product. Once you complete your IT assessment project and generate reports, you can easily share your IT documentation for a site with team members or others using IT Glue. Here's how the export works:

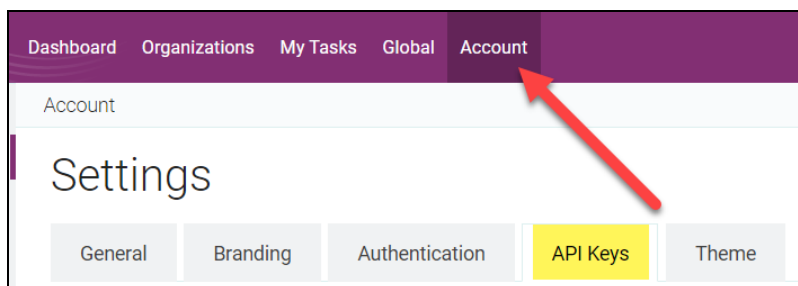
Step 1 — Create API Key in IT Glue

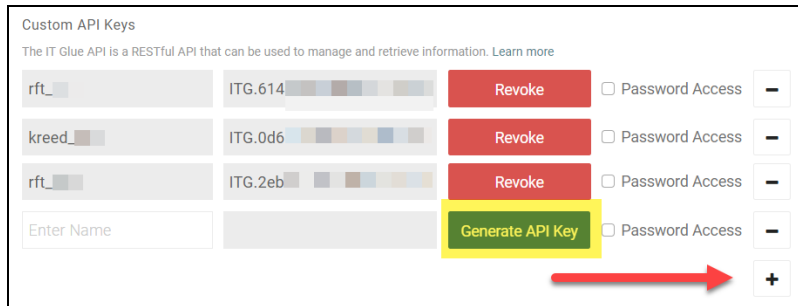
Before you can export reports, you need to integrate IT Glue with Network Detective Pro. From within your IT Glue account:

1. Create one or more **Organizations** in IT Glue. You will later select one of these orgs to send your data to the right place. You create new Organizations from the **Organizations** tab in IT Glue.



2. Create an IT Glue API Key for your use during integration and set up. You can do this from **Account > API Keys**.



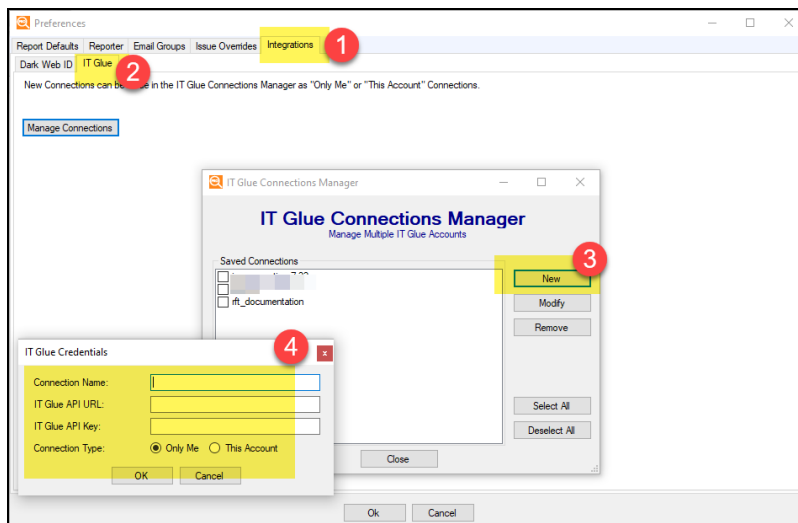


Important: For your reference, save a copy of the API key outside of IT Glue.

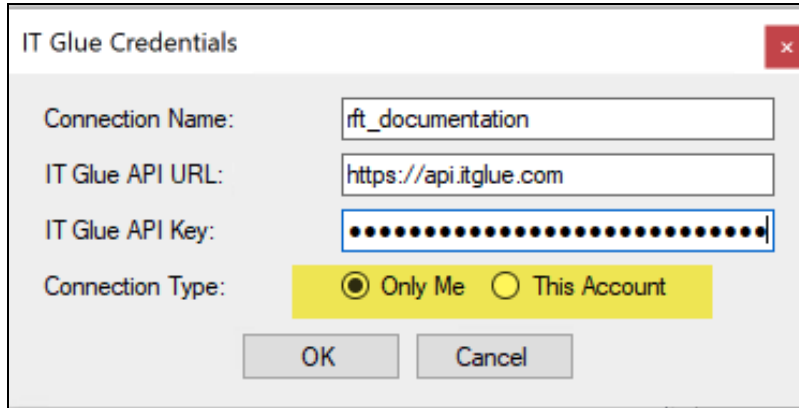
Step 2 — Create Connection to IT Glue in Network Detective Pro

Next, use your IT Glue API key to create a connection in Network Detective Pro.

1. First, open **Preferences** from the Network Detective Pro top menu, then click **Integrations**.
2. Click **IT Glue**, then click **Manage Connections**.



3. Then click **New** from the Connections Manager.
4. Enter the details for the connection, including the **API URL** and **API Key**.
5. Finally, choose whether to **enable this connection** only for the **current user**, or for the **entire account**. Then click **OK**.



IT Glue Credentials

Connection Name:

IT Glue API URL:

IT Glue API Key:

Connection Type: ☒ Only Me ☐ This Account

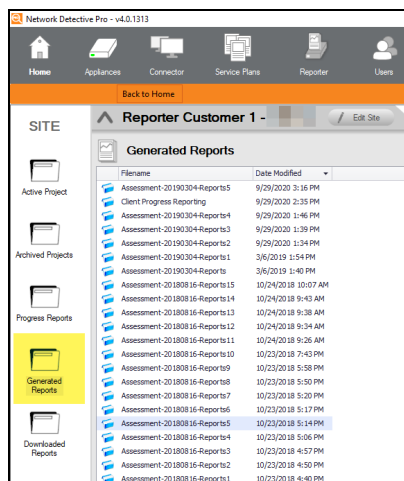
Note:

- For the API URL, use **https://api.itglue.com**
- If your IT Glue account is in the EU Data Center, use **https://api.eu.itglue.com**
- If your IT Glue account is in the AU Data Center, use **https://api.au.itglue.com**

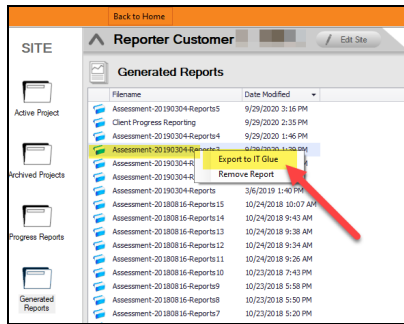
Step 3 — Export Reports to IT Glue

To export reports to IT Glue:

1. From your Site, open **Generated Reports** from the left-side menu.

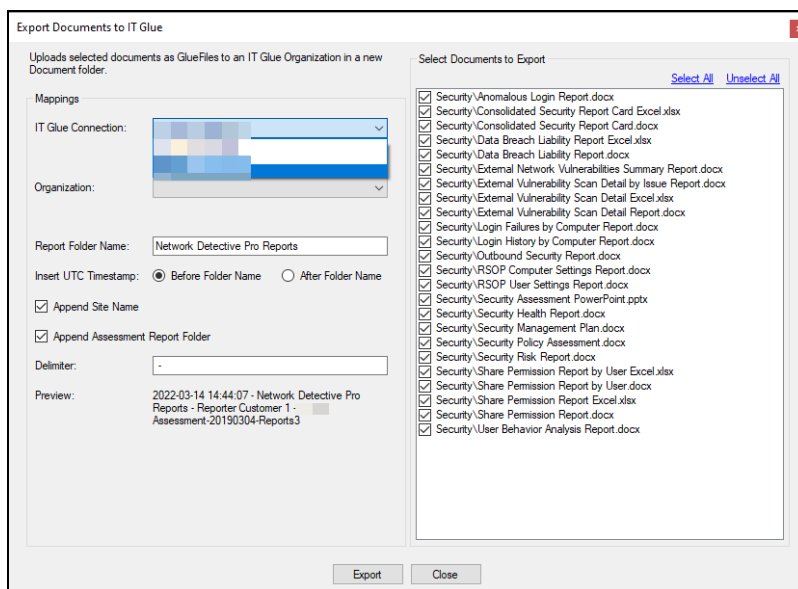


2. Choose the assessment reports you want to export, then **right click** and select **Export to IT Glue**.

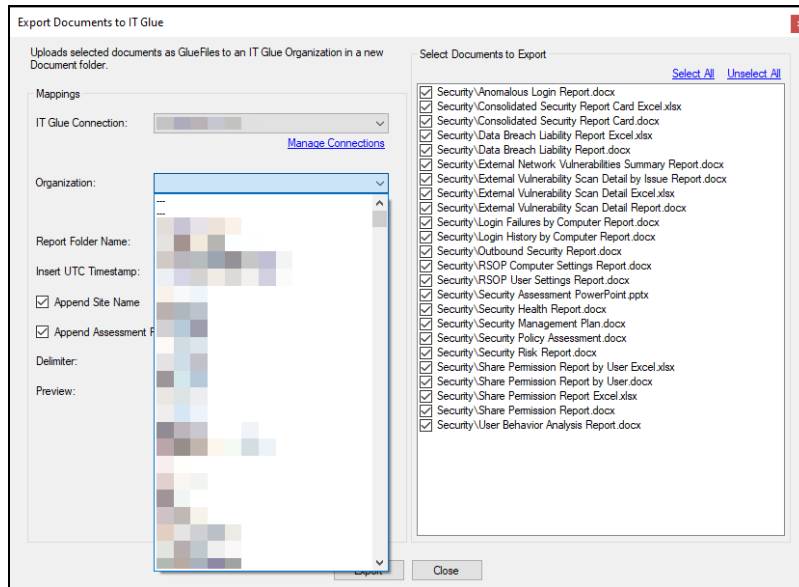


3. From the Export Documents to IT Glue menu, select the **IT Glue Connection** from the drop-down menu.

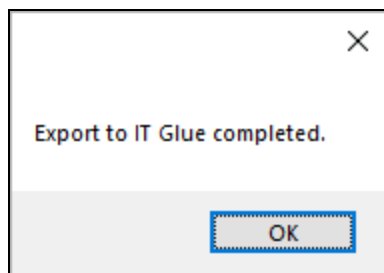
Note: If you are working with multiple IT Glue accounts, you can create and select from among several connections to ensure your documents go to the right place.



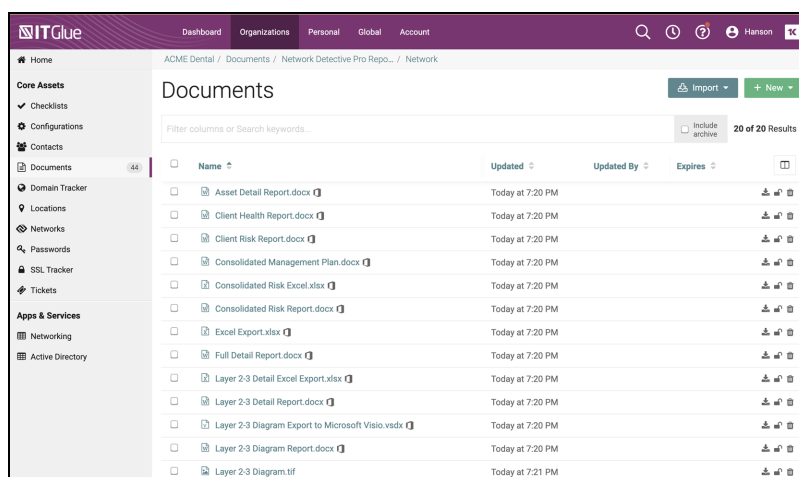
4. Then select the **Organization**. This list will include your available IT Glue orgs.



- Continue configuring the export. When you are ready, click **Export**. A confirmation will appear when the job is complete.



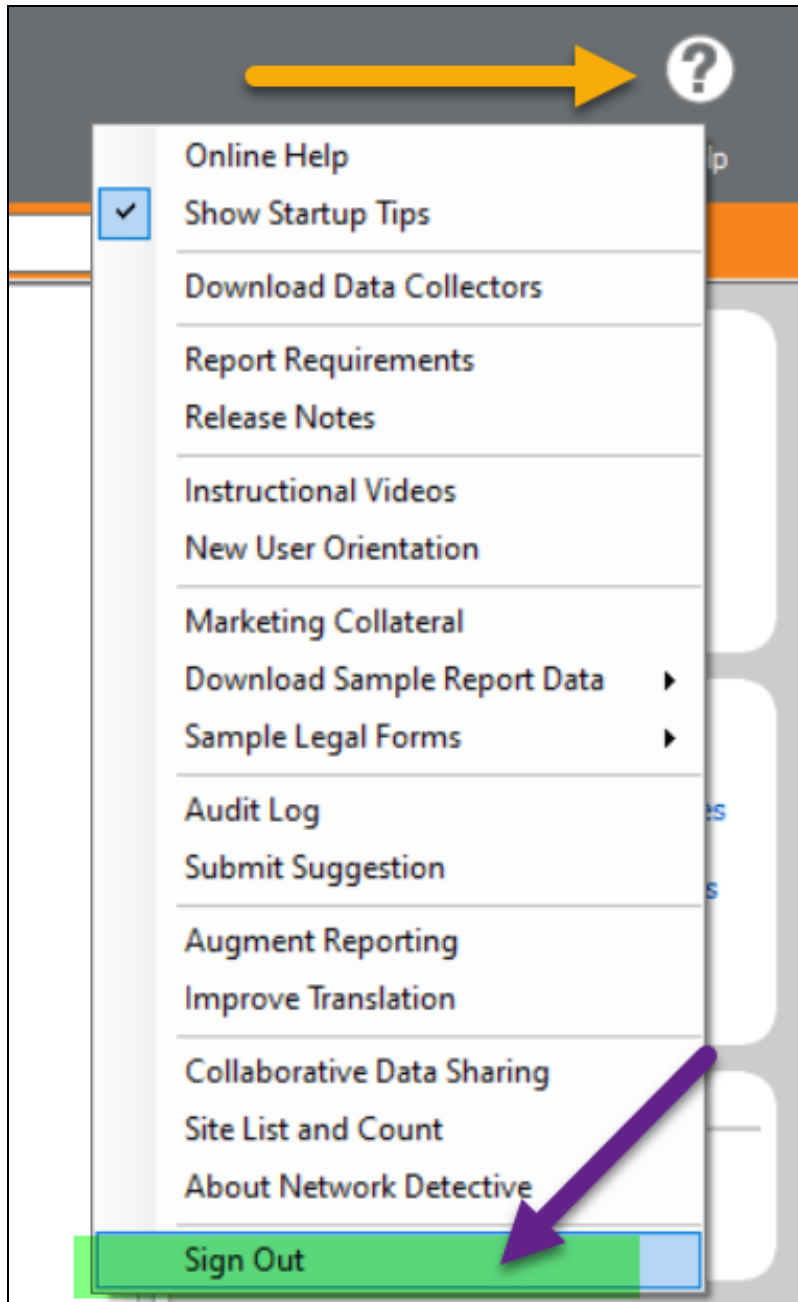
- You can then find your exported documents in IT Glue under the organization you selected.



Sign Out of Network Detective Pro

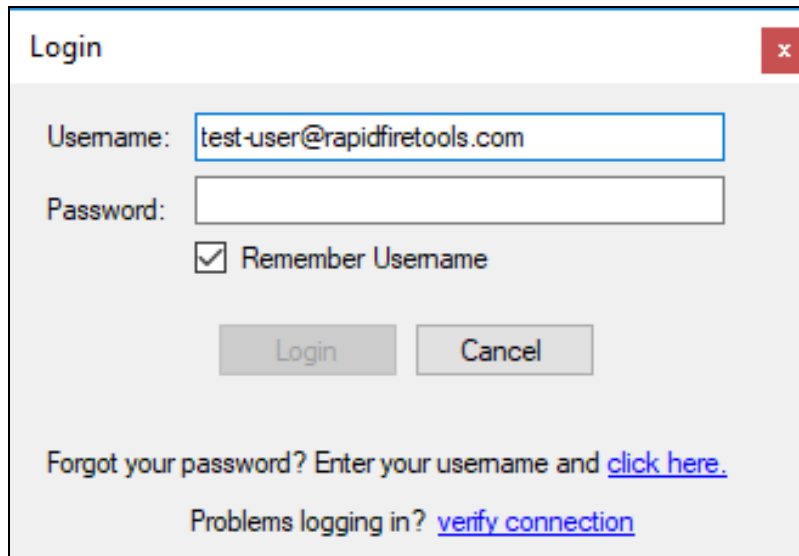
To sign out of Network Detective Pro:

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.

A screenshot of a 'Login' dialog box. The dialog has a title bar with the word 'Login' and a red close button with an 'x' icon. Inside the dialog, there is a 'Username:' label followed by a text input field containing 'test-user@rapidfiretools.com'. Below that is a 'Password:' label followed by an empty password input field. Under the password field is a checked checkbox labeled 'Remember Username'. At the bottom of the input section are two buttons: 'Login' and 'Cancel'. Below the buttons, there is a line of text: 'Forgot your password? Enter your username and [click here.](#)'. At the very bottom, it says 'Problems logging in? [verify connection](#)'.

Login

Username: test-user@rapidfiretools.com

Password:

☒ Remember Username

Login Cancel

Forgot your password? Enter your username and [click here.](#)

Problems logging in? [verify connection](#)

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):

<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 xzf 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 Pro application.

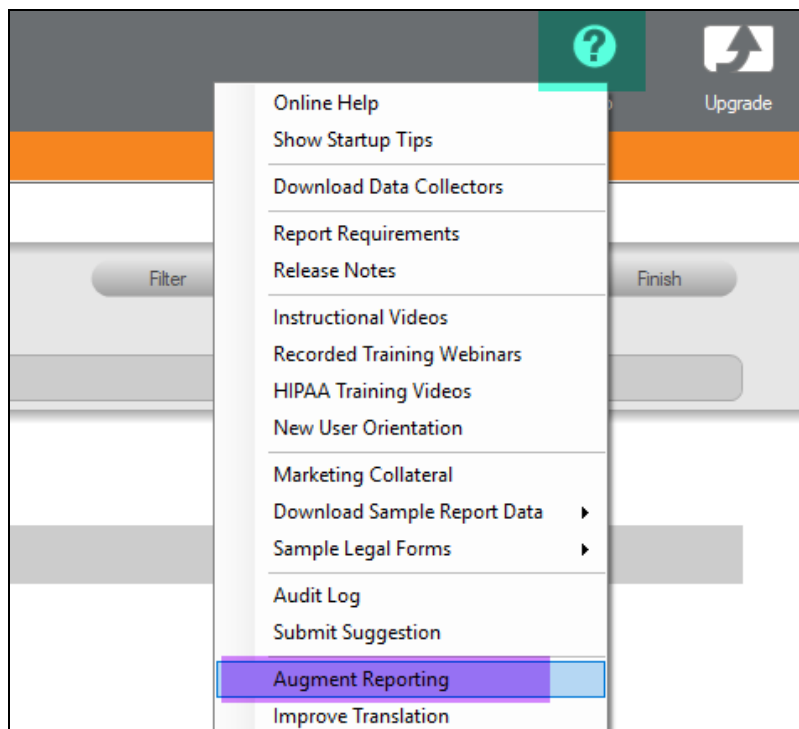
Augment Reporting to Eliminate False Positives

Occasionally, your customer may have a service installed that was not detected by Network Detective Pro. 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 Pro 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 Pro'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 Pro application. Then, re-generate the reports and the service will be properly included and displayed.

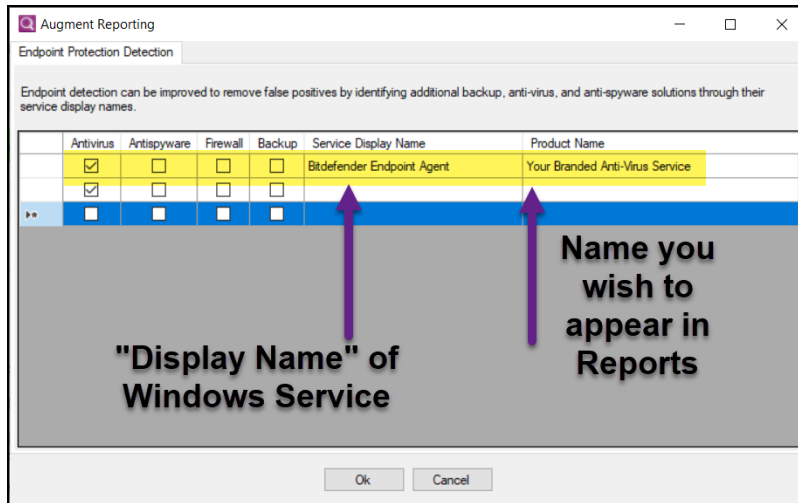
To augment your reports:

1. In Network Detective Pro, go to **Help > Augment Reporting**.



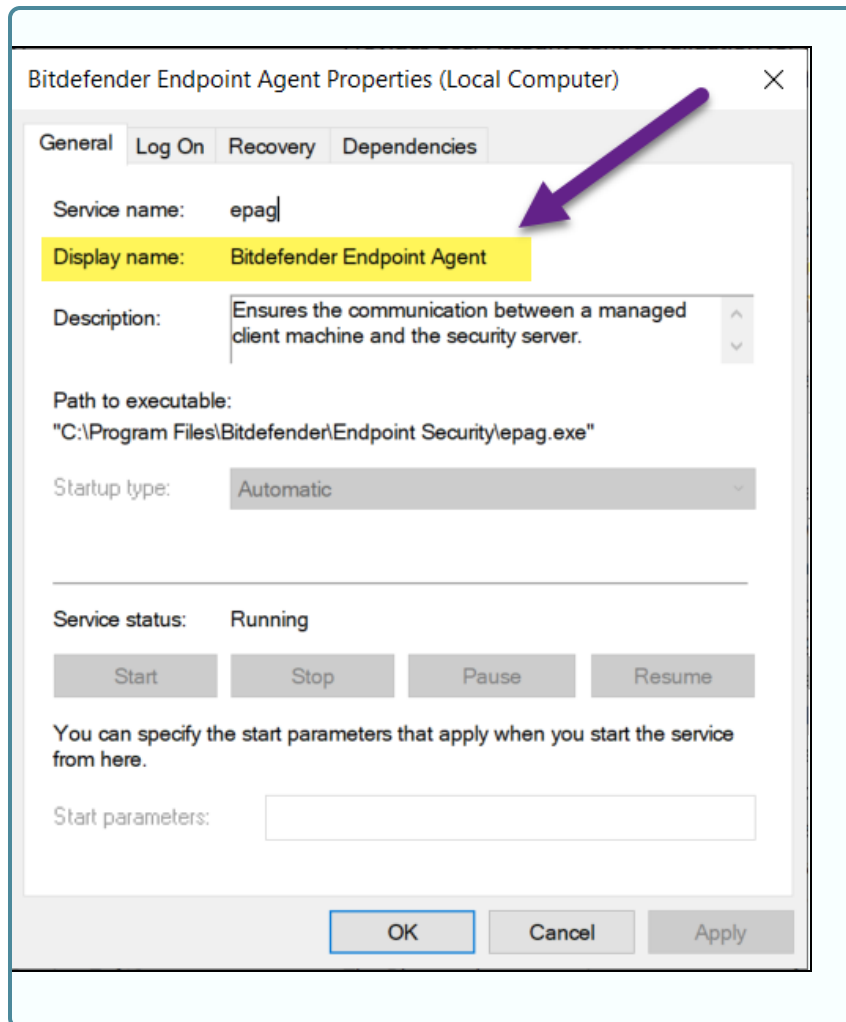
The **Endpoint Protection Detection** screen will appear.

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
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