

# **USER GUIDE**

**Network Detective Pro** 

10/19/2023 1:46 PM

# Contents

Network Detective Pro Components11
Download and Install the Network Detective Pro Application13
Set Up Network Detective Pro Reports14
Setting Report Branding and Customization Preferences
Setting Reports Preferences at the Global or Site Level
Access and Set Reports Defaults Preferences at the Global Level
Access and Set Reports Defaults Preferences at the Site Level
Network Detective "Site"
Setting Reports Preferences
Setting Reports Preferences 16
Set Reports Text Preferences 16
Set Reports Logo Preferences
Adding the Cover Page Logo Image
Adding the Header Logo Image
Set Reports Cover Page Styles and Themes Preferences19
Setting the Reports Cover Page Style
Setting the Module Color Scheme
Setting Document Style
Set Infographic Report Style
Assigning Custom Defined Color Schemes to Each Assessment Module23
Set Reports Cover Images Preferences
Configure Report Date Format in Network Detective Pro26
Assigning the Global Reports Preferences to a Site 27
Performing a Network Assessment 29
Network Assessment Overview 20
What You Will Need 29

Network Prerequisites for Network Detective Pro Scans	
Step 1 — Download and Install the Network Detective Pro app	
Step 2 — Create a New Site	
Step 3 — Start a Network Assessment	
Step 4 — Perform Network Scan Data Collection	
Scanning an Active Directory Domain-based Network	
Scanning a Workgroup Network	43
Step 5 — Use the Push Deploy Tool to Collect Remaining Data	51
Step 6 — Import Scans into Network Detective Pro App	
Step 7 — Run Dark Web Scan (Optional)	
Step 8 — Generate Network Assessment Reports	
Network Assessment Reports	60
Standard Reports	60
Infographics	65
Change Reports	66
Change Reports Performing a Security Assessment	66 67
Change Reports Performing a Security Assessment Security Assessment Overview	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site Step 3 — Start a Security Assessment	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site Step 3 — Start a Security Assessment Step 4 — Initiate External Vulnerability Scan	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site Step 3 — Start a Security Assessment Step 4 — Initiate External Vulnerability Scan Step 5 — Perform Security Scan Data Collection	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site Step 3 — Start a Security Assessment Step 4 — Initiate External Vulnerability Scan Step 5 — Perform Security Scan Data Collection Scanning a Workgroup Network	
Change Reports Performing a Security Assessment Security Assessment Overview What You Will Need Network Prerequisites for Network Detective Pro Scans Step 1 — Download and Install the Network Detective Pro Application Step 2 — Create a New Site Step 3 — Start a Security Assessment Step 4 — Initiate External Vulnerability Scan Step 5 — Perform Security Scan Data Collection Scanning a Workgroup Network Step 6 — Use the Push Deploy Tool to Collect Remaining Data	
Change Reports         Performing a Security Assessment         Security Assessment Overview         What You Will Need         Network Prerequisites for Network Detective Pro Scans         Step 1 — Download and Install the Network Detective Pro Application         Step 2 — Create a New Site         Step 3 — Start a Security Assessment         Step 4 — Initiate External Vulnerability Scan         Step 5 — Perform Security Scan Data Collection         Scanning a Workgroup Network         Step 6 — Use the Push Deploy Tool to Collect Remaining Data         Step 7 — Import Scans into Network Detective Pro App	
Change Reports         Performing a Security Assessment         Security Assessment Overview         What You Will Need         Network Prerequisites for Network Detective Pro Scans         Step 1 — Download and Install the Network Detective Pro Application         Step 2 — Create a New Site         Step 3 — Start a Security Assessment         Step 4 — Initiate External Vulnerability Scan         Step 5 — Perform Security Scan Data Collection         Scanning a Workgroup Network         Step 6 — Use the Push Deploy Tool to Collect Remaining Data         Step 7 — Import Scans into Network Detective Pro App         Step 8 — Generate Security Assessment Reports	

Standard Reports	96
Infographics	
Change Reports	
Performing a Microsoft Cloud Assessment	
Microsoft Cloud Assessment Overview	
What Does the Microsoft Cloud Assessment Cover?	
What Does the Microsoft Cloud Assessment Do?	
What You Will Need	105
Step 1 — Download and Install the Network Detective Pro Application	
Step 2 — Create a New Site	
Step 3 — Start a Microsoft Cloud Assessment Project	
Use the Microsoft Cloud Assessment Checklist	
Step 4 — Run the Cloud Data Collector	
Perform Scan Using Enterprise App	
Perform Scan Using OAUTH Credentials	110
Scan in Progress	112
Step 5 — (Optional) Document Compensating Controls	114
Step 6 — Generate Reports	
Prerequisites to Perform Cloud Scan using Enterprise App	118
Step 1 — Create Enterprise App in Azure Tenant to be Assessed	
Step 2 — Grant API Permissions to Enterprise App	
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	
Modify Report Privacy Options in Microsoft 365 Admin Center	
Microsoft Cloud Assessment Reports	
Performing an AWS Assessment	
AWS Assessment Overview	
What You Will Need	137
Step 1 — Download and Install the Network Detective Pro app	

Step 2 — Create a New Site	138
Step 3 — Start an AWS Assessment	139
Step 4 — Gather AWS Access Key and Secret Key	140
4(A) — Create User and Assign API permissions	140
4(B) — Generate Access Key ID and Secret key	142
Step 5 — Perform AWS Scan Data Collection	145
Step 6 — Generate AWS Assessment Reports	146
AWS Assessment Reports	148
Standard Reports	148
Performing a Cyberattack Risk Assessment Scan	. 149
Cyberattack Risk Assessment Overview	149
Step 1 — Download and Install the Network Detective Pro app	149
Step 2 — Create a New Site	149
Step 3 — Create Cyberattack Risk Assessment in Network Detective Pro	150
Step 4 — Access RapidFire Tools Portal and Customize Branding	152
Step 5 — Create and Distribute the Cyberattack Risk Assessment Computer Scanner	153
Step 6 — Users Downloads and Runs Cyberattack Risk Assessment Compute Scanner	<u>r</u> 156
Step 7 — Download Scans in Network Detective Pro Cyberattack Risk Assessment	158
Step 8 —(Optional) Run Dark Web ID Scan	160
Set Up Dark Web ID Integration with Network Detective Pro	162
Step 9 — Generate Reports	163
Cyberattack Risk Assessment Reports	164
Standard Reports	164
Performing an Exchange Assessment	165
Exchange Assessment Overview	165
What You Will Need	166

Step 1 — Download and Install the Network Detective Pro Application	
Step 2 — Create a New Site	
Step 3 — Start an Exchange Assessment	
Step 4 — Perform Exchange Scan Data Collection	
Step 5 — Generate Exchange Assessment Reports	
Exchange Assessment Reports	
Standard Reports	
Change Reports	
Performing a SQL Server Assessment	
SQL Server Assessment Overview	
What You Will Need	
Step 1 — Download and Install the Network Detective Pro Application	178
<u>Step 2 — Create a New Site</u>	
Step 3 — Start an SQL Server Assessment	
Step 4 — Perform SQL Server Scan Data Collection	
Step 5 — Generate SQL Server Assessment Reports	
Standard Reports	
Change Reports	
SQL Server Assessment Reports	
Standard Reports	
Change Reports	
Performing a Combined Network and Security Assessmen	t189
Network Assessment Overview	
Security Assessment Overview	
What You Will Need	190
Network Prerequisites for Network Detective Pro Scans	191
Step 1 — Download and Install the Network Detective Pro Application	
Step 2 — Create a New Site	
Step 3 — Start a Network and Security Assessment	

Step 4 — Initiate External Vulnerability Scan	194
Step 5 — Collect Data using Data Collector	198
Step 6 — Use the Push Deploy Tool to Collect Remaining Data	209
Step 7 — Import Scans into Network Detective Pro App	213
Step 8 — Generate Assessment Reports	217
ppendices	218
Pre-Scan Network Configuration Checklist	218
Checklist for Domain Environments	218
Checklist for Workgroup Environments	220
Enable Discovery Agents for Local Data Collection (Network Detective Pro)	223
Discovery Agent Firewall Requirements	
Step 1 — Enable Discovery Agents via RapidFire Tools Portal	
Step 2 — Install Discovery Agent(s)	226
Step 3 — Confirm Discovery Agent install for your Organization	
Step 4 — (Optional) Enable Access for Site Admin and Technician Users	
Step 5 — Assign Labels to Agents	
Step 6 — Schedule scans for Discovery Agent	
Step 7 — Download scan into assessment	
Remove Discovery Agents	
Silent Install for Discovery Agent	235
Install Linux and OSX Discovery Agents	237
Find and Copy Install Key for Discovery Agents	
Default Scripted Linux Install	238
Default Scripted OSX Install	
Install Script Options	239
Scripts for Linux and OSX Manual Data Collection	242
Linux X64 Collection	
OSX ARM64 Collection	242
OSX X64 Collection	
Optional Flags	243
End-user Initiated Computer Scans	

Step 1 — Create a New Network Detective Pro Portal Site	
Step 2 — Customize Portal Branding	
Step 3 — Enable End-users Scans from RFT Portal	245
Step 3 — Send URL to End-users	
Step 4 — End-user Runs Computer Scanner from URL	
Step 5 — Download Scan(s) from Network Detective	247
For New Sites	
Existing Sites	
Download End-user Scans	
Step 6 — Generate Reports	
Generate Commonly Used Report Sets	
Document Exceptions with the Issue Exception Worksheet	
Using a USB drive	
Override Issues in Network Detective Pro Reports	
Override issues at the global level	
Override issues at the site level	
Affected Reports	
Adding a Connector to a Site	
Adding an Inspector to a Site	
Dark Web Scan Summary for Security Assessment Module	
How it Works	
How to Perform Dark Web Scan as Part of Your Security Assessment	
What to do if Compromised Passwords are Detected	
Set Up Full Dark Web ID Integration	
Step 1 — Contact Dark Web ID Support to Enable User API Access	
Step 2 — Set Up Dark Web ID Integration with Network Detective Pro	
Step 3 — Continue Assessment and Perform Scan	271
Perform Datto Unified Continuity Scan	
Step 1 — Enable API Access in Datto Partner Portal	
Step 2 — Enable Datto Unified Continuity Integration	273
Step 3 — Perform Network Assessment Scan	275
Step 4 — Perform Datto Unified Continuity Scan	

	Step 5 — Generate Reports	. 276
D	ata Breach Liability Scanning and Reporting	.278
	Steps to Perform Scans to Identify PII and Generate the Data Breach Liability Report	. 279
C	ompleting Worksheets and Surveys	.282
	Entering Assessment Responses into Surveys and Worksheets	282
	Add Image Attachments to Surveys and Worksheets	283
	Add SWOT Analysis to Surveys and Worksheets	284
	Time Savings Tip to Reduce Survey and Worksheet Data Input Time	. 285
	Use the InForm Worksheet Tool Bar	285
	Bulk Entry for InForm Worksheets	. 285
	Create Word Response Form	288
	Important Note on Working with Word Response Forms	289
	Import Word Response Form	290
<u>C</u>	ompiling Network Detective Data	.292
Ir	tegrate Network Detective Pro with a PSA System	294
	Step 1 — Gather Credentials and Set Up your PSA System	294
	Step 2 — Create a Connection Between Network Detective Pro and Target PSA	296
	Export Configuration Items from Network Detective Pro to PSA	. 299
	Export Exchange Contacts from Network Detective Pro to PSA	305
	Create Tickets from Assessment Issues and Recommendations from Network Detective Pro to PSA	305
	Set Up Autotask Integration	308
	Set Up ConnectWise REST Integration	313
	Step 1 — Download and Install the ConnectWise Manage Internet Client	
	Application	313
	Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate	e 214
	Create Minimum Permissions Security Pole for API Member	21/
		215
	Step 3 Create an API Key in the ConnectWise Ticketing System	316
	Step 3 — Create an Ar rivey in the ConnectWise Recently System	317
	Step 5 — Remove "Disallow Saving" Flag from Company	318
	Set Up ConnectWise SOAP Integration	322
	Set Up Kaseva BMS Integration	324

Export Network Detective Pro Reports to IT Glue	
Step 1 — Create API Key in IT Glue	
Step 2 — Create Connection to IT Glue in Network Detective Pro	
Step 3 — Export Reports to IT Glue	
Sign Out of Network Detective Pro	331
Network Detective Linux Computer Data Collector	
Download the Linux Computer Data Collector	
Run the Linux Computer Data Collector	
Scan Output and Import into Assessment	
Augment Reporting to Eliminate False Positives	334
Use the Excel Export Spreadsheet to Find Display Names	

## 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

#### **RapidFireTools**<sup>\*</sup>

# Download and Install the Network Detective Pro Application

Visit <u>https://www.rapidfiretools.com/ndpro-downloads/</u>. 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.

	Intwork Detective Pro - v4.0.1293										
l				/ -		Į	•	2	\$		-
I	Home	InForm	Applia	ances Co	nnector	Rep	orter	Users	Billing	Preference	ces
			New Site	Import Site	View -	Refresh					
	HOME 482019 Assessment Status: In Progress Checklist: 0 / 0			ess		Arrow Test Site Assessment Status: Checklist:	c Started		BDR Custo Assessmer Checklist:		

#### **RapidFireTools**°

**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.

Customer A - Network Assessment

The Site's Preferences will be displayed.

V	Customer A	/ Edit Site	Asses	ssments   Reports   Export
	Appliances	Connectors	Remote Data Collectors	Report Preferences
	Click Add to bind a	Network Detective Applian	ice to the site 🔶 Add	

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**.

Preferences	- 0	×
Report Defaults Reporter	Email Groups	
Text My Logo Theme	e Cover Images Company Information	
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 confide proleged and non-disclosable information. If the requert 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.	rtial,
Target Language: Paper Size:	English ~ Letter (8.5%11') ~	
Currency Symbol: Conversion Factor:	IS ✓ 0.000000 ≑ x USD	
	Ok Cancel	

## 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.

Cover Logo Image: (600 x 150)	RapidFireTools	Network Assessment
Header Logo Image: (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 **Cover Page Logo**.

Open				
C V V Libraries > Documents >	Com	pany Images 👻 🐓	Search Company Images	ρ
Organize 🔻 New folder			:= - 🔟 📀	)
🔆 Favorites	Â	Documents library Company Images	Arrange by: Folder 🔻	
Contraction Contraction Contraction		Name	Date modified	ту
Documents	_	🔄 ABC Company Header Ima	age.jpg 1/12/2016 12:35 PM	JP
	Ε	MBC Company Logo.gif	1/12/2016 12:34 PM	GI
Videos		🖺 ABC Company Logo.jpg	1/12/2016 12:34 PM	JP
9 <u></u>		👪 ABC Company Logo.png	1/12/2016 12:34 PM	PI
🤣 Homegroup				
💻 Computer				
and TI106234W0C (C:)				
💼 Local Disk (D:)				
💿 DVD RW Drive (E:) RFT BU Dsk1 9-26	-	•		F
File name: ABC Compa	iny Lo	go.jpg 🔻	Image File (*.bmp;*.jpg;*.gif;*.p 🔻	
			Open 🔽 Cancel	

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

## Adding the Header Logo Image

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

Cover Logo Image: (600 x 150)	<b>RapidFireTools</b>	YouriT!	Network Assessment
Header Logo Image: (300 x 75 or 600 x 150)		tin in the second se	Risk Report
		Discovery 19515 The body discovery advances party on the first party of the first party of the discovery of the first party of the body of the first party of the discovery of the first party of the first discovery of the first party of the first party of the discovery of the first party of the first party of the first discovery of the first party of the first party of the first discovery of the first party of the first party of the first discovery of the first party of the first party of the first discovery of the first party of the first party of the first party of the first discovery of the first party of the first party of the first party of the first discovery of the first party of the first par	12 19(17) Steam (and 10) Steam (and 10) 19(17) Stea

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

Open				×
Cover the Libraries Documen	ts ▶ Comp	any Images 👻 😽	Search Company Images	٩
Organize 🔻 New folder			= - 1 (	2
🛚 🔆 Favorites	Î	Documents library Company Images	Arrange by: Folder 🔻	
✓ □ Libraries		Name	Date modified	Ту
		🔄 ABC Company Header Imag	ge.jpg 1/12/2016 12:35 PM	JP
Pictures	E	📧 ABC Company Logo.gif	1/12/2016 12:34 PM	GI
Videos		🔊 ABC Company Logo.jpg	1/12/2016 12:34 PM	JP
🗅 🍓 Homegroup		📭 ABC Company Logo.png	1/12/2016 12:34 PM	Pľ
4 🖳 Computer				
▷ 🏭 TI106234W0C (C:)				
Local Disk (D:)				
🛛 🕅 DVD RW Drive (E:) RFT BU Dsk1 9-2	- 26	•		•
File name: ABC Co	ompany Hea	der Image.jpg 🔹 👻	Image File (*.bmp;*.jpg;*.gif;*.p 🔻	
			Open 🔻 Cancel	]

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

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

## Set Reports Cover Page Styles and Themes Preferences

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

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.

O Preferences						- 0	×
Report Defaults Rep	oorter Email Groups						
Text My Logo	Theme Cover Images Compar	y Information					
Cover Page Style	(double-click to view)						
Network Assessment Bit Room With the set	Constant				A second se		^
Basic	Basic2	Classic	Classic2	Contemporary	Modern	Professional	
Module Color Sche	eme d Color Palette						~
		_					^
Standard	Standard2 Blue	Red Gre	en Neutral	Violet	Purple Fruity	Sunny	~
Use Custom De     Document Style	fined Colors (click on module color Network Security Exchange / SQL Server / H	or to select) IPAA					
Default Style	<ul> <li>✓ Modify Style</li> </ul>	e Preview Style					
			Ok Cance	ł			

#### 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.

Module Color So Use Pre-defir	cheme ned Color Palette				
Standard	Standard2	Blue	Red	Green	Neutral
O Use Custom	Defined Colors (clic) Network Security Exchange /	k on module cok SQL Server / H	or to select) IPAA		
Document Style	ical Blue	Modify Style	e Preview S	Style	

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

Modify Report Style	×
Style Name: Modern Royal	
Font Settings	
Font Family: Arial	
Font Size: 10	
Top Five Color Palette	
Color 1 Color 2 Color 3 Color 4 Color 5 Other	
Chart Style	
Hi-Res 2D 🗸	
Risk Meter	
2020 Modern Settings Table Style Discovery Teaks	
Save Preview Cancel	

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

## Set Infographic Report Style

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

#### **RapidFireTools**\*

Preferences										-	×
port Defaults	Reporter	Email Groups	Issue Overrides	Integrations							
ext My Log	o Theme	Cover Image	es Company Inf	ormation							
Cover Page S	tyle (doubl	e-click to view)									
Vertice Constraints	) 		E) Rink Report		*						^
Bas	c	Basi	c2	Classic	C	lassic2	Contemporary	Mod	lem	Professional	
) Use Pre-de	fined Colo	Palette									^
Standard	Star	idard2	Blue	Red	Green	Neutral	Violet	Purple	Fruity	Sunny	~
Document St Modern Grap	le hite	ecurity xchange / SQI	. Server / HIPAA Modify Style	Preview Style	Delete	Style					
Class	ic	(double-click to	o view)								

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.

#### **RapidFireTools**°

O Preferences		-		$\times$
Report Defaults Email Groups				
Text My Logo Theme Cov	er 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 co pavlinged, and non-actionable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopyin otherwise using this report or its contents in any way.	ntain com Ig, distribu	fidential, ting, or	
Target Language:	English v			
Date Format:	dd-MMM-yyyy v 19-Jun-2018			
Paper Size: Currency Symbol:	Letter (8.5%117) Select date format			
Conversion Factor:	0.000000 🚖 × 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 Assessment's name to access the **Report Preferences** setup option.

## Customer A - Network Assessment

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.

O Preferences		-		×
Report Defaults Email Gr	sups			
Text My Logo Then	e 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 privileged and non-diaclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from photocopying, distributing or otherwise using this report or its contents in any way.	contain c reading,	onfidentia	I.
Target Language: Paper Size: Currency Symbol: Conversion Factor:	Engleh ✓ Letter (8.5°×11") ✓ § ✓ 0.000000 (⊖ × USD			
	Rect	o Global	Preferenc	85
	Ok Cancel			

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

#### **RapidFireTools**\*

# 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 <u>Pre-Scan Network Configuration Checklist</u> 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.

#### **RapidFireTools**°

Follow these steps to perform a Network Assessment.

# Step 1 — Download and Install the Network Detective Pro app

Go to <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site	<b>E</b>
All Network Detective assessme physical location or a logical gro Site Name:	ents are organized into Sites. A site can be a ouping, such as a customer.
Customer A - Assessment	
Ok	Cancel

## 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**.

 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.

	Assessmer	nt-20230518						
	0% Complete 0 Complete 1 Required 2 Optional Created 05/18/2023 01:40 PM Updated 05/24/2023 10:43 AM Previous Project: Select							
	Network Asse	essment (Domain) 0	% Complete 0 Complete	e 🚺 Required	2 Optional	Created 05/18/	/2023 01:40 PM	Modified 0
	<b>V</b>							
~	Run Network Detective Data Collector (NDDC) with the Network Scan	Run Computer Data Collector on computers that cannot be scanned remot	Optionally, run a Dark Web ID Scan to search for compromised credentials.	Reports Not Ready				
	0	2	3					
	Double-click items to op	pen.						
				N				
	Run Network	k Detective Data Data Collector on the Dom e network. The data collector	Collector (NDDC) nain Controller (if possible), a ctor should be run with Adm	with the Net computer joined to inistrative privileges	work Scan the Domain if the	Domain Controller	ris not available, o	or from any

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.

- Visit the RapidFire Tools software download website at <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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 <u>"Scanning an Active Directory Domain-based Network" below</u>
- Look here if you are <u>"Scanning a Workgroup Network" on page 43</u>

### 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**.

🕲 Network Detective Da	ta Collector - 2.0.1161 ×				
Scan Type	Local Domains				
Active Directory	Below is a list of the detected domains in the current forest of the Active Directory.				
Local Domains	Gather information for ALL the domains detected.				
Additional Credentials					
External Domains	<ul> <li>Gather information for only the domains selected below.</li> </ul>				
IP Ranges					
SNMP Information					
VMware					
Verify and Run					
Collection Progress					
► Finish					
	Expand All Collapse All Expand Selected Advanced Tree View				
	(running on .NET CLR version 4.0.30319.42000) Back 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.

🛱 Network Detective Dat	ta Collector - 2.0.1161 x				
Scan Type	Additional Credentials				
Active Directory	Network scan credentials are required to perform remote Windows data collection via WMI and				
Local Domains	Neuronic 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.				
Additional Credentials					
External Domains	Network Scan Credentials				
IP Ranges	<u></u>				
SNMP Information	Username				
VMware	Password Add				
Verify and Run	corp (AD user to be used first)				
Collection Progress					
▶ Finish					
	Clear All Entries				
	(running on .NET CLR version 4.0.30319.42000) Back Next				

8. The **External Domains** screen will appear. Enter the name(s) of the organization's **External Domains**. Click **Next**.
| Scan Type  | External Domains   |
|--|--|
| Active Directory<br>Local Domains  | List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.  |
| Additional Credentials<br>External Domains   | Domain   |
| IP Ranges<br>SNMP Information<br>VMware<br>Verify and Run<br>Collection Progress<br>► Finish | myitco.performance.com         Clear All Entries         Import from Text File         Perform Dark Web Scan for Compromised Passwords |
|  | (running on .NET CLR version 4.0.30319.42000) Back 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 <u>Dark Web Scan Summary for Security</u> <u>Assessment Module</u>.

 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.

Scan Type	IP Ranges
Active Directory Local Domains	The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network cards in this machine.
External Domains	Single IP or IP Range (example: 192.168.0.0-192.168.0.255) Add
SNMP Information	172. 255 172. 255
VMware Verify and Run	
Collection Progress	
► Finish	Clear All Entries Import from Text File Reset to Default
▶ Finish	Clear All Entries Import from Text File Reset to Default Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)

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.



#### **RapidFireTools**<sup>®</sup>

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

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

🕀 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	SNMP Information
Active Directory	SNMP community strings are used to try to determine information about devices detected
Local Domains	during the IP Range scan. Enter any additional community strings used on this network.
Additional Credentials	Read Community String Add
External Domains	nublic
IP Ranges	public
SNMP Information	
VMware	
Verify and Run	
Collection Progress	
► Finish	Clear All Entries Import from Text File Reset to Default
	Advanced SNMP Options SNMP Timeout (seconds): 10  Attempt SNMP against non-pingable devices (slower but more accurate)
	(running on .NET CLR version 4.0.30319.42000) Back 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.

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

	VMware		
Local Domains	DNS name or IP addre	are required for discovery of VNW ass along with VMware login cred	are nosts. Enter the viviware host server entials.
Additional Credentials			
External Domains	Hostname or IP Addr	ess	Skip connection test
IP Ranges	Username		
SNMP Information	Password		Add VMware Server
VMware			
Verify and Run	Host	User	Connection Verified
Collection Progress			
Finish			
	Clear All Entries	s Test All Connections	
	Clear All Entrie	s Test All Connections	
	Clear All Entrie	s Test All Connections	
	Clear All Entrie	s Test All Connections	

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.

🛱 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Verify and Run
Active Directory	Ready to run the data collection. Select your output file location and basename. The final
Local Domains	assessment file will be <folder>\<basename>.zip.</basename></folder>
Additional Credentials	Output Assessment File
External Domains IP Ranges	Folder: C:\Users' Desktop
SNMP Information	Basename: NetworkDetective-20220222 .ZIP
VMware	
Verify and Run	Launch Pre-scan Analyzer Advanced Options
Collection Progress	
▶ Finish	
Save Settings to File	(running on .NET CLR version 4.0.30319.42000) Back Start

**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. Prescan results and recommendations are provided at the completion of the prescan.

Overview Result Sum	mary Act	ive Direc	tory S	QL Server	Network Compu	ters Push Deploy		
Pushing local data collect	ors to remote	e comput	ers require	es WMI, Adr	min\$ access, and .N	ET 3.5 or above.		
							Showing: All Nodes	
Computer	IP Address	In A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status		ľ
APP01.CORP.RAPIDFIRETO		<ul> <li>✓</li> </ul>	×			WMI failed. The RPC serv	er is unavailable.	
BROWN-WIN10.CORP.RAPI		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-09SDFE1.CORP.R		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-1HM0E7I.CORP.R		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-6ND4Q8O.CORP	172.18.0.207	✓	✓	✓	✓	Full access		
DESKTOP-7DBVA30.CORP.R	10.236.83.1	✓	?			Accessing WMI		
DESKTOR TREAKTE CORR.		1	×			WMI failed The RRC con-	or is unavailable	

Enter any Comments and then click Start.

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

Scan Type	Collection Progress
Active Directory Local Domains Additional Credentials External Domains IP Ranges SNMP Information VMware Verify and Run Collection Progress Finish	Eventlogs:       Completed.         SQL Servers:       Scanning for MS SQL Servers         Internet:       Initializing         DHCP:       Checking rft         Network:       7 of 4160 finished.         Local Collector:       Getting optional features
Save Settings to File	Cancel Data Collection Wrap It Up

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*).

Scan Type	Active Directory
	Domain Controller and Active Directory.
Scan Credentials	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.
IP Ranges	If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.
SNMP Information	
VMware	I want to scan
Verify and Run	<ul> <li>Active Directory</li> <li>Workgroup (no domain)</li> </ul>
Collection Progress	
	Active Directory Credentials
	Username (FQDN\user)
	Password
	Domain Controller (IP or Hostname)
	(running on .NET CLR version 4.0.30319.42000) Back Ne

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**.

ican Type	Scan Credentials
Active Directory	
Local Domains (N/A)	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 Credentials	scan.
External Domains	Network Scan Credentials
IP Ranges	
SNMP Information	Username
VMware	Password Add
Verify and Run	
Collection Progress	
Finish	
Finish	
Finish	
Finish	Clear All Entries
Finish	Clear All Entries
Finish	Clear All Entries
Finish	Clear All Entries  X At least one credential is required in a workgroup environment.
Finish	Clear All Entries  X At least one credential is required in a workgroup environment.

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

	External Domains
	List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.
Scan Credentials External Domains	Domain
IP Ranges SNMP Information VMware Verify and Run Collection Progress Finish	microsystems-msp.com         Clear All Entries         Import from Text File         Perform Dark Web Scan for Compromised Passwords
	(running on .NET CLR version 4.0.30319.42000) Back 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 <u>Dark Web Scan Summary for Security</u> <u>Assessment Module</u>.

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**.

🙃 Network Detective Da	ita Collector - 2.0.1161 ×
	IP Ranges
	The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to
	the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and
Scan Credentials	sublet masks on the detected network cards in this machine.
External Domains	Single IP or IP Range (example: 192.168.0.0-192.168.0.255) Add
IP Ranges	172. 200
SNMP Information	
VMware	
Verify and Run	
Collection Progress	
► Finish	
	Clear All Entries Import from Text File Reset to Default
	Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)
	(running on .NET CLR version 4.0.30319.42000) Back Next

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.

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

🚯 Network Detective Dat	ta Collector - 2.0.1161 x
Scan Type	SNMP Information
Active Directory	SNMP community strings are used to try to determine information about devices detected
Local Domains (N/A)	during the IP Range scan. Enter any additional community strings used on this network.
Scan Credentials	Read Community String
External Domains	nublic
IP Ranges	public
SNMP Information	
VMware	
Verify and Run	
Collection Progress	
► Finish	Clear All Entries Import from Text File Reset to Default
	Advanced SNMP Options SNMP Timeout (seconds): 10 : 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). 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.

7. 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**.

Scan Type	VMware	
	VMwara gradentials are required for discour	any of VMwara basts. Enter the VMwara bast same
	DNS name or IP address along with VMware	e login credentials.
Scan Credentials		
	Hostname or IP Address	Skip connection test
IP Ranges	Username	
SNMP Information	Password	Add VMware Server
Verify and Run	Host User	Connection Verified
Collection Progress		
Finish		
	Clear All Entries Test All Conr	nections

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.

🕀 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Verify and Run
Active Directory	Ready to run the data collection. Select your output file location and basename. The final
Local Domains (N/A)	assessment file will be <folder>\<basename>.zip.</basename></folder>
Scan Credentials	Output Assessment File
External Domains	Folder: C:\Users\ \Desktop
IP Ranges	Basename: NetworkDetective-20220222
SNIVIP Information	
Viviware	
Collection Progress	Launch Pre-scan Analyzer Advanced Options
▶ Finish	
Save Settings to File	(running on .NET CLR version 4.0.30319.42000) Back Start

**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. Prescan results and recommendations are provided at the completion of the prescan.

Overview Result Summ	nary Act	ive Direc	tory S	QL Server	Network Compu	ters Push Deploy		
Pushing local data collecto	rs to remote	comput	ers requir	es WMI, Adr	nin\$ access, and .N	ET 3.5 or above.		
						Showing: A	II Nodes	
							^	
Computer	Address	In A/D	Access	Adminş Access	above Installed	Status	-	
APP01.CORP.RAPIDFIRETO		$\checkmark$	×			WMI failed. The RPC server is unavailable.		
BROWN-WIN10.CORP.RAPI		<ul><li>✓</li></ul>	×			WMI failed. The RPC server is unavailable.		
DESKTOP-09SDFE1.CORP.R		<ul> <li>✓</li> </ul>	×			WMI failed. The RPC server is unavailable.		
DESKTOP-1HM0E7I.CORP.R		✓	×			WMI failed. The RPC server is unavailable.		
DESKTOP-6ND4Q8O.CORP	172.18.0.207	<ul> <li>✓</li> </ul>	✓	✓	✓	Full access		
	10.236.83.1	~	?			Accessing WMI		
DESKTOP-7DBVA30.CORP.R						WAAR Asthed, The DDC exercise to consultable		

Enter any Comments and then click Start.

9. 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.

🕲 Network Detective Dat	a Collector - 2.0.1161
Scan Type	Collection Progress
Active Directory	
Local Domains (N/A)	Eventlogs: Completed.
Scan Credentials	Internet: Initializing
External Domains	Checking rft-dc02.corp.rapidfiretools.com
IP Ranges	Network: 7 of 4160 finished.
SNMP Information	Local Collector: Getting optional features
VMware	
Verify and Run	
Collection Progress	
► Finish	
	Cancel Data Collection Wrap It Up
Save Settings to File	(running on .NET CLR version 4.0.30319.42000) Next

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**.

🕲 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Finish
Active Directory	
Local Domains	The data collection process has been successfully ended, and file(s) with the partial data have been generated. Please be aware that reports created from this data may have missing
Additional Credentials	sections or may otherwise contain incomplete information as the collection process did not fully finish.
External Domains	Callest the output file from
IP Ranges	C:\Users\ \Desktop
SNMP Information	Open
VMware	
Verify and Run	
Collection Progress	
🕨 Finish	
Save Settings to File	(running on .NET CLR version 4.0.30319.42000) Done

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.

- Visit the RapidFire Tools software download website at <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

RetworkDetective Push Deploy Tool	- v2.0.1105		-		×
✓ Settings and Configuration	Settings and Configuration				
Computers and Status	Scan Settings				
Collected Data Files	Storage Folder: C:\Uleens'\underschinn\Dedictop\NetworkDetectivePluehDeployTool C Scan Type: Computer Scan  Scan Type: Scan Scanty Scan	<u>Change Folder</u>	Open Fold	<u>ler</u>	
	HIPAA Gutek.   HIPAA Deep   PI Gutek.   PCI Deep   BOR Scan   PI Scan				
	Credentials Access to remote machines to copy files and run collections are required. Usersame may contain a backlash f you with to also specify a d Credential will be checked per machine in the order they are specified inter. The credentials extends here are not checked unit a collector	domain. n is initiated.			
	Username TESTT(wednin (curret use) Password:				
	Add Current User Clear All Connector Settings (optional)				
	Connector ID: Verfix Connector ID A Proop Server is Required to Access the Internet Server: Port. 80 Usemana: Password				
		Load Set	tings S	ave Se	ttings
	< Bar	ick Ner	xt >	Cance	el 👘

### 4. 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

RetworkDetective Push Deploy Tool							
✓ Settings and Configuration	Computers and Status	3					
Computers and Status     Collected Data Files	When you are ready computers to push the	to being data collection e local data collector to	n, click the "unpause" b interactively. Right-clic	utton. This will imme k on a computer for	ediately commence data coller r additional options.	tion. You may add or manage	
	Hostname or IP Address	Add Single Computer	Add from File	Add from IP Range	Save Computers to File	Show	Al 👻
	Computer	IP Address	WMI Admin\$ Access Access	.NET 3.5 or 4.5 Installed	File Data Stracted St	atus	
	Total Computers: 0, Remaining	0, Successful: 0, Faile	d: 0				
						< Back Ne	ext > Cancel

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.

Q	Net	workDetective I	Push Deplo	by Tool						- • ×
✓ Settings and Configuration	Computers and Stat	us								
✓ Computers and Status	When you are rear	dy to being data colle	tion, click the	"unpause" bu	tton. This will im	mediately com	mence data c	ollection. You may add	d or manage	
Collected Data Files	computers to push	the local data collect	or to interactive	ely. Right-click	on a computer	for additional of	options.		-	
	Hostname or IP Address	Add Single Comp	ter Add h	om File A	dd from IP Ranc	ze <u>Save C</u>	Computers to P	ie .	Show: All	~
	Computer	IP Address	WHI Access	Admin\$ Access	.NET 3.5 or 4.5 Installed	File Extracted	Data Collected	Status		^
			<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			✓	<ul> <li>✓</li> </ul>	✓	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			¥	4	¥	¥	¥			
			¥	¥	¥ 	¥ ✓	¥ √			
			· ·	· ·	· ·	· ·	~			
				· ·	· ·					
			~	1	✓	✓	~			
			<ul><li>✓</li></ul>	✓	<ul> <li>✓</li> </ul>	✓	✓			
			✓	✓	✓	✓	✓			
			✓	✓	✓	✓	✓			
			✓	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			×	×	✓	¥	<b>v</b>			
		_	¥	¥	¥	¥	¥			
			V,	¥.	₩.	V,	V,			*
	Total Computers: 282, Remai	ining: 0, Successful: 2	1, Failed: 181							
								< Back	Nest>	Cancel

### **RapidFireTools**°

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

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

<u>a</u>	NetworkDetective Push De	eploy Tool	-	×
✓ Settings and Configuration	Collected Data Files			
✓Computers and Status	Right-click any data file rows in the table for more options re	parding the rows selected.	the survey Course days and Collection Claims tak	
✓ Collected Data Files	Current Storage Folder: C:\download\NetworkDetectiveP	ge reider, nor just ones mar nave been collected non ishDeployTool	Open Fold	a
	Filename	File Date	File Size	^
	dz	11/03/16 8:39:05 PM	667 KB	
	zip	11/03/16 8:44:36 PM	670 KB	
	zip	11/03/16 8:43:14 PM	526 KB	
	zip	11/03/16 8:42:17 PM	732 KB	
	zip	11/03/16 8:39:12 PM	1123 KB	
	zip	11/03/16 8:37:47 PM	700 KB	
	zip	11/03/16 9:06:29 PM	714 KB	
	.zip	11/03/16 9:06:08 PM	673 KB	
	zip	11/03/16 8:42:46 PM	661 KB	
	zip	11/03/16 8:49:00 PM	704 KB	
	zip	11/03/16 8:42:24 PM	2029 KB	
	zip	11/03/16 9:06:42 PM	941 KB	
	zip	11/03/16 8:42:57 PM	584 KB	
	zip	11/03/16 8:41:49 PM	703 KB	~
	On Finish: 🗹 Zip Data Files 📃 Upload vis Connec	tor 🗌 Archive Scan Files 🗹 Open Storage Fol	der <back c.<="" finish="" td=""><td>ancel</td></back>	ancel

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

## **MORE INFO:**

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

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

After all of the **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.

V	Sca	ns Import Scan File	Initiate External Scan	Download Scans
	Scan(s)	0 Files		

The Select the Scan Results window will be displayed.

Network Detective Wizard
Select the Scan Results
Select the resulting scan file or files. Multiple scan files or compressed archives can be selected in the file browser. Use CTRL-Click or SHIFT-Click to select multiple files.
If you do not have a results file from a network scan, please download the Data Collector and complete a scan first.
Browse
Back Next Cancel

### **RapidFireTools**°

- 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**.

les from the Com order to merge in	puter Data Collector ( ndividual computers, ;	(.CDF) need to you will need to	be merged with the o pspecify a domain or	riginal Network Detective data workgroup for each CDF file.	a file (.NDF) before generat	ing a repo
ustom Domain:				(opti	ional)	
	Select CUS I OW IN 1	the dropdown i	ist under Merge Into	to use the Custom Domain.		Refre
Computer	Local Domain/V	Vorkgroup	OS	Run Date	Merge Into	
DAEDALUS	CORP.	.C	Windows 10 Ent	9/27/2017 4:49:05 PM	Corp.MyCo.com	~
DAEDALUS	CORP.	.C	Windows 10 Ent	10/12/2017 2:39:08 PM	Corp.MyCo.com	~
DAMION	CORP.	.C	Windows 10 Pro	10/12/2017 2:56:35 PM	[Use Workgroup]	~
DC	CORP.	.C	Windows Server	10/2/2017 4:24:03 PM	[Use Workgroup]	~
DC	CORP.	.C	Windows Server	8/21/2017 1:54:00 PM	[Use Workgroup]	~
DESKTOP	CORP.	.C	Windows 10 Ent	9/27/2017 4:46:44 PM	[Use Workgroup]	~
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:31:42 PM	[Use Workgroup]	~
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:44:44 PM	[Use Workgroup]	~
DESKTOP	CORP.	.C	Windows 10 Pro	9/27/2017 4:41:58 PM	[Use Workgroup]	~
DEV	CORP.	.C	Windows 10 Pro	10/12/2017 2:43:44 PM	[Use Workgroup]	~
DEVILS	CORP.	.C	Windows 10 Pro	10/12/2017 3:03:47 PM	[Use Workgroup]	~
	1					

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.
- 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.

S 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						

See also "Set Up Full Dark Web ID Integration" on page 270.

## **RapidFireTools**°

- Network Detective Pro User Guide
  - 3. Click the **Run Dark Web Scan** button from the Scans bar. The scan will present a confirmation when complete.



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

Reports Create Reports	
Active Assessment - Ready to Generate V 61% Availab	e
Layer 2-3 Diagram Export to Microsoft Visio (.vsdx)     Layer 2-3 Detail Report (.docx)     Layer 2-3 Detail Excel Export (.xlsx)     Layer 2-3 Diagram (tif)     Consolidated Risk Report (.docx)     Consolidated Risk Excel (.xlsx)     Consolidated Management Plan (.docx)     Client Health Report (.docx)     Client Health Report (.docx)     Orark Web ID Scan Summary (.docx)	
Executive Summary (.docx) Outdated Malware Definitions Summary (.docx)	

# 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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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.

Reports Create Reports			
All Reports ~ 3% Availa	ble 3 Available Reports 113 Unavailable Reports		
Exchange	SQL Server	Retwork	Security
Standard Reports	Standard Reports	Standard Reports	Standard Reports
Exchange Risk Report (.docx)	Routine Health Report (.docx)	Client Risk Report (.docx)	Security Risk Repo
Exchange Management Plan (.docx)	SQL Server Detail Report (.docx)	Network Management Plan (.docx)	Security Managem
Exchange Mailbox Detail Report (.docx)	Database Detail Report (.docx)	Full Detail Report (.docx)	Outbound Security
Exchange Mobile Device Report (.docx)	Maintenance Plan Report (.docx)	Excel Export (xlsx)	Security Policy Ass
Exchange Traffic and Use Report (.docx)	SQL Server Agent Jobs Report (.docx)	Site Diagram (.docx)	Share Permission F

- 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 allows you to generate the following reports:

## **Standard Reports**

Report Name	Description
Asset Detail Report	For each network scan, this report provides detailed information on each of the individual 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.

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

## What You Will Need

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.

## **RapidFireTools**\*

# Network Prerequisites for Network Detective Pro

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 <u>Pre-Scan Network Configuration Checklist</u> 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site	
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer. Site Name:	
Customer A - Assessment	
Ok Cancel	

### **RapidFireTools**<sup>®</sup>

# 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**.

 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.
0	Network Detective Wizard	×
Initiate External Vuln	erability Scan	
Schedule an external vulnerability s Detail Report, as well as running sp scan (i.e., 'Customer ABC Scan'). Ye	can. Once the scan is complete, you can use the re cialized vulnerability reports. Enter a descriptive lab u may enter up to 64 addresses.	sult to augment the Client Risk and el for the scan to help identify the
Email me upon completion at:     Save settings for this site	xxxxxx@rapidfiretools.com	Add Remove Remove All
	Back	Next 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.

Add IP Address Range
If only a single IP Address is wanted, leave the Ending IP Address blank.
Starting IP Address: Ending IP Address: Add 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.

Network Detective Wizard	×
Initiate External Vulnerability Scan	
Schedule an external vulnerability scan. Once the scan is complete, you can use the re Detail Report, as well as running specialized vulnerability reports. Enter a descriptive lab scan (i.e., 'Customer ABC Scan'). You may enter up to 16 addresses.	suit to augment the Client Risk and el for the scan to help identify the
2	Add
	Remove All
Email me upon completion at: xxxxxx@rapidfiretools.com	]
Save settings for this site Your scan should be completed in approximately 2 hour(s).	
Back	Next 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.

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.	

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.

- Visit the RapidFire Tools software download website at <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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 <u>"Performing a Security Assessment" on page 67</u>
- Look here if you are "Scanning a Workgroup Network" on page 83

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



#### **RapidFireTools**°

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

🚯 Network Detective Da	ta Collector - 2.0.1161 ×
Scan Type	Active Directory
Active Directory	Please enter a username and password with administrative rights to connect to the local
Local Domains	Domain Controller and Active Directory.
Additional Credentials	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
IP Ranges	screen.
User Control Tests	If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.
File Scanner	
Verify and Run	I want to scan
Collection Progress	Active Directory     O Workgroup (no domain)
▶ Finish	Active Directory Credentials corp. (FQDN\user) ••••••••••••••••••••••••••••••••••••
	(running on .NET CLR version 2.0.50727.9151) Back Next

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**.

🕲 Network Detective Da	ta Collector - 2.0.1161 x
Scan Type	Local Domains
Active Directory	Below is a list of the detected domains in the current forest of the Active Directory
Local Domains	below is a list of the detected domains in the carrent forest of the richter billeden p
Additional Credentials	Gather information for ALL the domains detected.
IP Ranges	<ul> <li>Gather information for only the domains selected below.</li> </ul>
User Control Tests	
File Scanner	
Verify and Run	
Collection Progress	
► Finish	
	Expand All Collapse All Expand Selected Advanced Tree View
	(running on .NET CLR version 2.0.50727.9151) Back Next

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

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

🛱 Network Detective Da	ta Collector - 2.0.1161 ×
Scan Type	Additional Credentials
Active Directory	Network scan credentials are required to perform remote Windows data collection via WMI and
Local Domains	Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Calle using the default credentials will always be attempted first
Additional Credentials	scan. Cans using the default credentials will always be attempted inst.
IP Ranges	Network Scan Credentials
User Control Tests	
File Scanner	Username
Verify and Run	Password Add
Collection Progress	(AD user to be used first)
▶ Finish	Clear All Entries
	(running on .NET CLR version 2.0.50727.9151) Back Next

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

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

Scan Type	IP Ranges
Active Directory Local Domains Additional Credentials	The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network cards in this machine.
IP Ranges	Single IP or IP Range (example: 192 168 0 0.192 168 0 255)
User Control Tests File Scanner	172         255           172         255
Verify and Run Collection Progress	
	Clear All Entries Import from Text File Reset to Default
	Clear All Entries Import from Text File Reset to Default Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)

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.

Confirm		$\times$
×	You are currently about to scan 2,048 IP addresses. Large ranges can take long periods of time to complete.	
	Do you wish to continue anyways?	
	OK Cancel	

**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**.

Scan Type	User Control Tests
Active Directory Local Domains Additional Credentials	The Security Assessment User Control tests will attempt to access sites in various categories from this computer. If you do not wish to include BUILT-IN URLs from a particular category in your assessment, please uncheck it. Additionally, you may add individual URL to the category testing. Any custom URLs will ALWAYS be checked.
IP Ranges User Control Tests	Built-in URL Categories
File Scanner	🇹 Entertainment 🛛 Pornography 🔽 Shareware
Verify and Run	🗹 Social Media 🗹 Warez 🗹 Web Mail
Collection Progress	
▶ Finish	Custom URLs URL Category      Entertainment
	(running on .NET CLR version 2.0.50727.9151) Back Next

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

#### **RapidFireTools**°

(C) Network Detective Dat	ta Collector - 2.0.1161	×
Scan Type	File Scanner	T
Active Directory	NOTE: File scanning can cause a temporary increase in resource utilization.	-
Local Domains	Scan Tunaci	
Additional Credentials	Personally Identifiable Information (PII)	
IP Ranges		
User Control Tests	Scan Options:	
File Scanner	Include the scanning of ZIP files	
Verify and Run	PDE Timeout: 5 minutes (min = 1 max = 60)	
Collection Progress	PDF filleout. 5 initiates (fille = 1, filax = 60)	
► Finish		
SHHHH		
	(running on .NET CLR version 2.0.50727.9151) Back Next	

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.

🛱 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Verify and Run
Active Directory	Poodu to sup the data collection. Select your output file location and bacaname. The final
Local Domains	assessment file will be <folder>\ basename&gt;.zip.</folder>
Additional Credentials	Output Assessment File
External Domains	
IP Ranges	Folder: C:\Users' Desktop
SNMP Information	Basename: NetworkDetective-20220222 .ZIP
VMware	
Verify and Run	Launch Pre-scan Analyzer Advanced Options
Collection Progress	
▶ Finish	
Save Settings to File	(running on .NET CLR version 4.0.30319.42000) Back Start

**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. Prescan results and recommendations are provided at the completion of the prescan.

Overview Result Sur	nmary Ac	tive Dire	ctory	SQL Server	Network Compu	ters Push Deploy		
Pushing local data collec	tors to remot	e compu	ters requir	es WMI, Adı	min\$ access, and .N	ET 3.5 or above.		
							Showing: All Nodes	
Computer	IP Address	ln A/D	WMI Access	Admin\$ Access	.NET v3.5 or above Installed	Status		
APP01.CORP.RAPIDFIRETO		<ul> <li>✓</li> </ul>	×			WMI failed. The RPC server is unavailable.		
BROWN-WIN10.CORP.RAPI.		✓	×			WMI failed. The RPC server is unavailable.		
DESKTOP-09SDFE1.CORP.R		✓	×			WMI failed. The RPC server is unavailable.		
DESKTOP-1HM0E7I.CORP.R.		✓	×			WMI failed. The RPC server is unavailable.		
DESKTOP-6ND4Q8O.CORP	. 172.18.0.207	✓	✓	~	✓	Full access		
DESKTOP-7DBVA30.CORP.R.	10.236.83.1	. 🗸	?			Accessing WMI		

Enter any Comments and then click Start.

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

🕀 Network Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Collection Progress
Active Directory	Local Collector: Getting Logon Eventlogs
Local Domains	Security Collector: Getting login events; 29 Port(s) Remaining; 13 URL(s) Rem
Additional Credentials	
IP Ranges	
User Control lests	
File Scanner	
Verity and Run	
Collection Progress	
	Cancel Data Collection Wrap It Up
Save Settings to File	(running on .NET CLR version 2.0.50727.9151) Next

#### **RapidFireTools**<sup>®</sup>

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**.

Retwork Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Finish
Active Directory	
Local Domains	The data collection process has been successfully ended, and file(s) with the partial data have been generated. Please be aware that reports created from this data may have missing
Additional Credentials	sections or may otherwise contain incomplete information as the collection process did not fully finish
External Domains	
IP Ranges	C:\Users\ \Desktop
SNMP Information	Open
VMware	
Verify and Run	
Collection Progress	
🕨 Finish	
	(running on .NET CLR version 4.0.30319.42000) Done
Save Settings to File	

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*).

🚯 Network Detective Da	ta Collector - 2.0.1161	×					
Scan Type	Active Directory						
Active Directory	Please enter a username and password with administrative rights to connect to the local						
Local Domains (N/A)	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						
Scan Credentials							
IP Ranges	screen.						
User Control Tests	If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.						
File Scanner							
Verify and Run	I want to scan						
Collection Progress	<ul> <li>Active Directory</li> <li>Workgroup (no domain)</li> </ul>						
▶ Finish	Active Directory Credentials       corp.     (FQDN\user)       ••••••••••••••••••••••••••••••••••••						
	(running on .NET CLR version 2.0.50727.9151) Back Next						

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.

Scan Type	Scan Credentials						
Active Directory	Network scan credentials are required to perform remote Windows data collection via WMI and						
Local Domains (N/A)	Remote Registry. Use this screen to optionally add additional credentials to be used during the						
Scan Credentials	scall.						
IP Ranges	Network Scan Credentials						
User Control Tests							
File Scanner	Username						
Verify and Run	Password Add						
Collection Progress							
▶ Finish	.com Clear All Entries						
	(running on .NET CLR version 2.0.50727.9151) Back Next						

#### **RapidFireTools**<sup>®</sup>

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**.

Scan Type       IP Ranges         Active Directory       Local Ourmente (N/A)         Scan Credentials       The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network cards in this machine.         IP Ranges       User Control Tests         File Scanner       Verify and Run         Collection Progress       The file or IP Range (example: 192.168.0.0-192.168.0.255)         Add       172         IP Range       255         IP Finish       Clear All Entries         Import from Text File       Reset to Default         Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)       (running on .NET CLR version 2.0.50727.9151)	🕲 Network Detective Da	ta Collector - 2.0.1161	×
Active Directory         Active Directory         Accel Directory         Accel Directory         Accel Directory         Scan Credentials         IP Ranges         User Control Tests         File Scanner         Verify and Run         Collection Progress         Finish         Clear All Entries         Import from Text File         Reset to Default         Operation         (running on .NET CLR version 2.0.50727.9151)         Back	Scan Type	IP Ranges	
Accel (Journaury (1974))         Scan Credentials         IP Ranges         User Control Tests         File Scanner         Verify and Run         Collection Progress         Finish         Clear All Entries         Import from Text File         Reset to Default         Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)         (running on .NET CLR version 2.0.50727.9151)         Back	Active Directory	The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to	
Scan Credentials       IP Ranges         User Control Tests       Single IP or IP Range (example: 192.168.0.0-192.168.0.255)         File Scanner       225         Verify and Run       2255         Collection Progress       172         Finish       Clear All Entries         Import from Text File       Reset to Default         Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)       (running on .NET CLR version 2.0.50727.9151)	Local Domains (N/A)	the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subpat marks on the detected activate cards in this machine.	
IP Ranges       Single IP or IP Range (example: 192.168.0.0-192.168.0.255)       Add         User Control Tests       IT2.       .255         File Scanner       Verify and Run       .255         Collection Progress       .255         ▶ Finish       Clear All Entries       Import from Text File         Reset to Default               Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)         (running on .NET CLR version 2.0.50727.9151)       Back	Scan Credentials	Sublict masks on the detected network cards in this machine.	
User Control Tests File Scanner Verify and Run Collection Progress Finish Clear All Entries Import from Text File Reset to Default Perform minimal impact scan (reduced number of threads for less network impact but longer scan time) (running on .NET CLR version 2.0.50727.9151) Back Next	IP Ranges	Single IP or IP Range (example: 192.168.0.0-192.168.0.255) Add	
File Scanner       172.       .255         Verify and Run       Collection Progress	User Control Tests	172	
Verify and Run Collection Progress Finish Clear All Entries Import from Text File Reset to Default Clear All Entries Import from Text File Reset to Default Perform minimal impact scan (reduced number of threads for less network impact but longer scan time) (running on .NET CLR version 2.0.50727.9151) Back Next	File Scanner	172	
Collection Progress  Finish  Clear All Entries Import from Text File Reset to Default  Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)  (running on .NET CLR version 2.0.50727.9151) Back Next	Verify and Run		
▶ Finish          Clear All Entries       Import from Text File       Reset to Default         □       Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)         (running on .NET CLR version 2.0.50727.9151)       Back       Next	Collection Progress		
Clear All Entries       Import from Text File       Reset to Default         Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)       Import from Text File       Reset to Default         (running on .NET CLR version 2.0.50727.9151)       Back       Next	► Finish		
(running on .NET CLR version 2.0.50727.9151) Back Next		Clear All Entries Import from Text File Reset to Default Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)	
		(running on .NET CLR version 2.0.50727.9151) Back Next	

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**.

Retwork Detective Da	ta Collector - 2.0.1161	×
Scan Type	User Control Tests	
Active Directory	The Security Assessment User Control tests will attempt to access sites in various categories	-
Local Domains (N/A)	from this computer. If you do not wish to include BUILT-IN URLs from a particular category in	
Scan Credentials	testing. Any custom URLs will ALWAYS be checked.	
IP Ranges		
User Control Tests	Built-in URL Categories	
File Scanner	🗹 Entertainment 🛛 Pornography 🔽 Shareware	
Verify and Run	🗹 Social Media 🛛 🗹 Warez 🗳 Web Mail	
Collection Progress		
► Finish	Custom URLs	
	URL Category	
	* Entertainment V	
	(running on .NET CLR version 2.0.50727.9151) Back Next	

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

🚯 Network Detective Da	ta Collector - 2.0.1161	×
Scan Type	File Scanner	
Active Directory	NOTE: File scanning can cause a temporary increase in resource utilization.	
Local Domains (N/A)	Sean Tunger	
Scan Credentials	Personally Identifiable Information (PII)	
IP Ranges		
User Control Tests	Scan Options:	
File Scanner	Include the scanning of ZIP files	
Verify and Run	DDE Timesente E miguetes (min 1 man 60)	
Collection Progress	PDF limeout:	
► Finish		
		_
	(running on .NET CLR version 2.0.50727.9151) Back Next	

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.

Retwork Detective Dat	ta Collector - 2.0.1161	×
Scan Type	Verify and Run	
Active Directory	Poodu to run the data collection. Select your output file location and baconame. The final	-
Local Domains (N/A)	assessment file will be <folder>\ basename&gt;.zip.</folder>	
Scan Credentials	Output Assessment File	
IP Ranges		
User Control Tests	Folder: C:\Users\ Desktop	
File Scanner	Basename: NetworkDetective-20220223 .ZIP	
Verify and Run		
Collection Progress	Launch Pre-scan Analyzer Advanced Options	
► Finish		
SEENER		
		_
	(running on .NET CLR version 2.0.50727.9151) Back Start	
Save Settings to 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. Prescan results and recommendations are provided at the completion of the prescan.

Overview Result Sur	nmary Ac	tive Dire	ctory	SQL Server	Network Compu	ters Push Deploy	
Pushing local data collec	tors to remot	e compu	ters requir	es WMI, Adı	min\$ access, and .N	ET 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		<ul> <li>✓</li> </ul>	×			WMI failed. The RPC server is unavailable.	
BROWN-WIN10.CORP.RAPI.		<ul><li>✓</li></ul>	×			WMI failed. The RPC server is unavailable.	
DESKTOP-09SDFE1.CORP.R		✓	×			WMI failed. The RPC server is unavailable.	
DESKTOP-1HM0E7I.CORP.R.		✓	×			WMI failed. The RPC server is unavailable.	
DESKTOP-6ND4Q8O.CORP	. 172.18.0.207	<ul><li>✓</li></ul>	✓	~	✓	Full access	
DESKTOP-7DBVA30.CORP.R.	10.236.83.1	. 🗸	?			Accessing WMI	

Enter any Comments and then click Start.

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

🛱 Network Detective Da	ta Collector - 2.0.1161 ×
Scan Type	Collection Progress
Active Directory	Local Collectory Starting local data collection
Local Domains (N/A)	Security Collector: Getting login events; 29 Port(s) Remaining; 13 URL(s) Rem
Scan Credentials	
IP Ranges	
User Control Tests	
File Scanner	
Verify and Run	
Collection Progress	
▶ Finish	
	Cancel Data Collection Wrap It Up
Save Settings to File	(running on .NET CLR version 2.0.50727.9151) Next

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**.

🛱 Network Detective Da	ta Collector - 2.0.1161 ×
Scan Type	Finish
Active Directory	
Local Domains (N/A)	The data collection process has been successfully ended, and file(s) with the partial data have been generated. Please be aware that reports created from this data may have missing
Scan Credentials	sections or may otherwise contain incomplete information as the collection process did not fully finish
IP Ranges	
User Control Tests	Collect the output file from C:\Users\v \\Desktop
File Scanner	Open
Verify and Run	
Collection Progress	
🕨 Finish	
	(running on .NET CLR version 2.0.50727.9151) Done
Save Settings to File	

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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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

RetworkDetective Push Deploy Tool							
✓ Settings and Configuration	Computers and Status						
Computers and Status     Collected Data Files	When you are ready t computers to push the	o being data collection local data collector to	, click the "unpause" bi interactively. Right-click	tton. This will imm t on a computer fo	ediately commence data c r additional options.	ollection. You may add or mana	ige
	Hostname or IP Address	Add Single Computer	Add from File	dd from IP Range	Save Computers to F	ile Sho	w: Al 👻
	Computer	IP Address	WMI Admin\$ Access Access	.NET 3.5 or 4.5 Installed	File Data Extracted Collected	Status	
	Total Computers: 0, Remaining:	0, Successful: 0, Failed	d: 0				
						< Back	Next > Cancel

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.

Q	Net	workDetective I	Push Deplo	by Tool						- • ×
✓ Settings and Configuration	Computers and Stat	us								
✓ Computers and Status	When you are rear	dy to being data colle	tion, click the	"unpause" bu	tton. This will im	mediately com	mence data c	ollection. You may add	d or manage	
Collected Data Files	computers to push	the local data collect	or to interactive	ely. Right-click	on a computer	for additional of	options.		-	
	Hostname or IP Address	Add Single Comp	ter Add h	om File A	dd from IP Ranc	ze <u>Save C</u>	Computers to P	ie .	Show: All	~
	Computer	IP Address	WHI Access	Admin\$ Access	.NET 3.5 or 4.5 Installed	File Extracted	Data Collected	Status		^
			<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			✓	<ul> <li>✓</li> </ul>	✓	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			¥	4	¥	¥	¥			
			¥	¥	¥ 	¥ ✓	¥ √			
			· ·	· ·	· ·	· ·	~			
				· ·	· ·					
			~	1	✓	✓	~			
			<ul><li>✓</li></ul>	✓	<ul> <li>✓</li> </ul>	✓	✓			
			✓	✓	✓	✓	✓			
			✓	✓	✓	✓	✓			
			✓	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			×	×	✓	×	<b>v</b>			
		_	¥	¥	¥	¥	¥			
			V,	¥.	₩.	V,	V,			*
	Total Computers: 282, Remai	ining: 0, Successful: 2	1, Failed: 181							
								< Back	Nest>	Cancel

#### **RapidFireTools**°

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

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

<u>a</u>	NetworkDetective Push De	eploy Tool	-	×
✓ Settings and Configuration	Collected Data Files			
✓Computers and Status	Right-click any data file rows in the table for more options re	parding the rows selected.	the survey Course days and Collection Claims tak	
✓ Collected Data Files	Current Storage Folder: C:\download\NetworkDetectiveP	ge reider, nor just ones mar nave been collected non ishDeployTool	Open Fold	a
	Filename	File Date	File Size	^
	dz	11/03/16 8:39:05 PM	667 KB	
	zip	11/03/16 8:44:36 PM	670 KB	
	zip	11/03/16 8:43:14 PM	526 KB	
	zip	11/03/16 8:42:17 PM	732 KB	
	zip	11/03/16 8:39:12 PM	1123 KB	
	zip	11/03/16 8:37:47 PM	700 KB	
	zip	11/03/16 9:06:29 PM	714 KB	
	.zip	11/03/16 9:06:08 PM	673 KB	
	zip	11/03/16 8:42:46 PM	661 KB	
	zip	11/03/16 8:49:00 PM	704 KB	
	zip	11/03/16 8:42:24 PM	2029 KB	
	zip	11/03/16 9:06:42 PM	941 KB	
	zip	11/03/16 8:42:57 PM	584 KB	
	zip	11/03/16 8:41:49 PM	703 KB	~
	On Finish: 🗹 Zip Data Files 📃 Upload vis Connec	tor 🗌 Archive Scan Files 🗹 Open Storage Fol	der <back c.<="" finish="" td=""><td>ancel</td></back>	ancel

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

#### **MORE INFO:**

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

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

After all of the **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.

Network Detective Wizard
Select the Scan Results
Select the resulting scan file or files. Multiple scan files or compressed archives can be selected in the file browser. Use CTRL-Click or SHIFT-Click to select multiple files.
If you do not have a results file from a network scan, please download the Data Collector and complete a scan first.
Browse
Back Next Cancel

- 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:

#### **RapidFireTools**<sup>®</sup>

- .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**.

Network Det	ective Merger				-		>
Files from the Computer Data Collector (.CDF) need to be merged with the original Network. Detective data file (.NDF) before generating a report. In order to merge individual computers, you will need to specify a domain or workgroup for each CDF file.							
Custom Domain:	*Select CUSTOM in t	the dropdown I	ist under "Merge Into	(op. " to use the Custom Domain.	tional)		
Constant	Local Density (I		00	D = D to	Marrielate	<u>Refr</u>	rest
	COPP	vorkgroup	US Windows 10 Ent	RUN Date	Com McCo.com		1
	CORP.	 C	Windows 10 Ent	10/12/2017 2:39:08 PM	Corp.MyCo.com	- v	۲
DAMION	CORP	 C	Windows 10 Pro	10/12/2017 2:56:35 PM	[Use Workgroup]	-	1
DC	CORP	с.	Windows Server	10/2/2017 4:24:03 PM	[Use Workgroup]		1
DC	CORP.	C	Windows Server	8/21/2017 1:54:00 PM	[Use Workgroup]	~	ſ
DESKTOP	CORP.	.C	Windows 10 Ent	9/27/2017 4:46:44 PM	[Use Workgroup]	~	1
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:31:42 PM	[Use Workgroup]	~	1
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:44:44 PM	[Use Workgroup]	~	1
DESKTOP	CORP.	.C	Windows 10 Pro	9/27/2017 4:41:58 PM	[Use Workgroup]	~	1
DEV	CORP.	.C	Windows 10 Pro	10/12/2017 2:43:44 PM	[Use Workgroup]	~	1
DEVILS	CORP.	.C	Windows 10 Pro	10/12/2017 3:03:47 PM	[Use Workgroup]	~	1,
DEVILS	CORP.	.C	Windows 10 Pro lerge Now	10/12/2017 3:03:47 PM	[Use Workgroup]	~	-

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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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.

Reports Create Reports			
All Reports ~ 3% Availa	ble 3 Available Reports 113 Unavailable Reports		
Exchange	SQL Server	Retwork	Security
Standard Reports	Standard Reports	Standard Reports	Standard Reports
Exchange Risk Report (.docx)	Routine Health Report (.docx)	Client Risk Report (.docx)	Security Risk Repo
Exchange Management Plan (.docx)	SQL Server Detail Report (.docx)	Network Management Plan (.docx)	Security Managem
Exchange Mailbox Detail Report (.docx)	Database Detail Report (.docx)	Full Detail Report (.docx)	Outbound Security
Exchange Mobile Device Report (.docx)	Maintenance Plan Report (.docx)	Excel Export (xlsx)	Security Policy Ass
Exchange Traffic and Use Report (.docx)	SQL Server Agent Jobs Report (.docx)	Site Diagram (.docx)	Share Permission F

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

## Security Assessment Reports

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

#### **Standard Reports**

Report Name	Description
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.

#### **RapidFireTools**\*

## 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

#### **RapidFireTools**°

#### What You Will Need

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

Note: You can acces	s 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 <u>"Prerequisites to Perform Cloud Scan using Enterprise App" on page 118</u> 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:
	<ul> <li>Privileged role admin (Recommended)</li> <li>Cloud application admin (Recommended)</li> <li>(Using one these roles will only grant permissions to the individual users who enter their credentials to perform the scan.)</li> <li>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.)</li> </ul>
	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 <u>Assign Admin Roles</u> in the Microsoft 365 documentation for more details.

#### **RapidFireTools**\*

Follow these steps to perform a Microsoft Cloud Assessment:

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

- 1. Visit <u>https://www.rapidfiretools.com/ndpro-downloads/</u>. 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.

Q Network Detect	tive Pro	- v4.0.1293				
Ê			/ '	<u>.</u>	2	
Home	InForm	Applia	ances C	onnector	Rej	porter
		New Site	Import Site	View 🕶	Refresh	
HOME						

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.

Q Network Detective Wizard			×
Select Assessment Type			
What type of assessments are you performing at this site? (Check all	that apply)		
IT and Cloud Assessments:			
<ul> <li>Network Assessment (Domain)</li> <li>Network Assessment (Workgroup)</li> <li>Security Assessment (Workgroup)</li> <li>Exchange Assessment</li> <li>SQL Server Assessment</li> <li>BDR Assessment (Quick)</li> <li>BDR Assessment (Full)</li> <li>✓ Microsoft Cloud Assessment</li> </ul>			
Other (Use for ad-hoc reporting. No checklist provided.)			
	Back	Next	Cancel

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** and **Optional** 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.

	Assessment-20200526
	0% Complete 0 Complete 1 Required 0 Optional Created 2020/05/26 09:37 AM Updated 2020/05/26 09:37 AM Previous Project: Select
	Microsoft Cloud Assessment 0% Complete 0 Complete 0 Required 0 Optional Created 2020/05/26 09:37 AM Modified 2020/05/26 09:37 AM
^	Press the TRun Cloud Data Collector' buttom to initiate data collection.
	Press the 'Run Cloud Data Collector' button to initiate data collection. If you do not have a results file from a Microsoft Cloud Assessment scan, please use the 'Run Cloud Data Collector' button to generate scan data.

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:

- <u>"Perform Scan Using Enterprise App" below</u>: 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.
- <u>"Perform Scan Using OAUTH Credentials" on the facing page</u>: Allows you to collect data from the MS Cloud (Office 365, Teams, and so on) only and <u>DOES NOT INCLUDE</u> Azure Infrastructure data. This method requires only Office 365 credentials with the proper admin permissions.

See <u>"Modify Report Privacy Options in Microsoft 365 Admin Center" on page 130</u> to troubleshoot issues with how data appears in your reports.

### 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.



 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. RapidFire Tools, Inc. All rights reserved.

ele	ect Cloud Data Collection N	lethod						
Co	ection Method							
	Enterprise Application     Allows collection of both	MS Cloud and A	zure environme	nts using crede	entials from an	installed Ent	erprise Appli	cation.
	Click here for documenta	tion on how to s	setup the requin	ed Enterprise A	pplication.	_		
	Tenant Id:							
	Client Id:							
	Client Secret Value:							
	O OAUTH Credentials							
	Allows collection from on This method uses interact	y MS Cloud and tively entered ad	does not includ ministrative cre	de Azure Infrast dentials and is	ructure. compatible wit	h Microsoft r	nulti-factor a	uthentication.

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.

#### **RapidFireTools**<sup>®</sup>

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**.

your acc	punt
	Microsoft
	@nd-healthcare.com
Pe	ermissions requested
С	RapidFire Tools Azure Data Collector
Thi org	s application is not published by Microsoft or your anization.
Thi	s app would like to:
$\sim$	Read audit log data
$\sim$	Read directory data
$\sim$	Read all groups
$\sim$	Read identity providers
$\sim$	Read all OneNote notebooks that you can access
$\sim$	Maintain access to data you have given it access to
$\sim$	Read all usage reports
$\sim$	Read your organization's security events
$\sim$	Read items in all site collections
$\sim$	Sign you in and read your profile
$\sim$	Read all usage reports
$\sim$	Read your organization's security events
$\sim$	Read items in all site collections
$\sim$	Sign you in and read your profile
$\sim$	Read all users' full profiles
$\sim$	Read all users' basic profiles
	Consent on behalf of your organization
Acci data char	epting these permissions means that you allow this app to use your as specified in their terms of service and privacy statement. You can ge these permissions at https://myapps.microsoft.com. Show details
	Cancel 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.

Sign in	i to your account	×
	Microsoft	
	@nd-healthcare.com	
	Need admin approval	
	Q RapidFire Tools Azure Data Collector rapidfiretools.us	
	RapidFire Tools Azure Data Collector needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.	
	Have an admin account? Sign in with that account	
	Return to the application without granting consent	
Te	erms of use Privacy & cookies	

#### 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	×
0 Required Remaining 🔺 💌 Hide # Filter Topics 🍸 🗙 Bulk Entry 💌 Actions 💌	Save	Close	^
	Expand	1 All   Collapse	All
A ✔ 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 miligated through a compensating control.	-	10 M	
	Ø	OT	
∧ ✓ 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 Valid	D	SW	
∧ ✔ 3 Self Service Password Reset Not Enabled			
3.4 Solf Sonies Dareword Dorot Not Enabled			
Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.			
Valid Valid	P	SW	
	-		

- 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.

Reports Create Reports	
Active Assessment - Ready to Generate V 24% Avail	able
Microsoft Cloud	
<ul> <li>Standard Reports</li> <li>Azure AD Assessment (.docx)</li> <li>SharePoint Assessment (.docx)</li> <li>OneDrive Usage Report (.docx)</li> <li>Outlook Mail Activity Report (.docx)</li> <li>Microsoft Teams Assessment (.docx)</li> <li>Microsoft Cloud Security Assessment (.docx)</li> <li>Microsoft Cloud Security Assessment (.docx)</li> <li>Configuration Change Report (.docx)</li> <li>Risk Report (.docx)</li> <li>Management Plan (.docx)</li> <li>MS Cloud Compensating Control Worksheet (.docx)</li> </ul>	

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.

	Reports	Create	Repo	rts
AL	leports - Ready to Ger	nerate	~	32% Avail
Activ All R All R	re Assessment - Read eports - Ready to Ger eports	ly to Generate nerate		

- 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.

	Generated Reports	;
	Filename	Date Modified 🔻
Active Project	Assessment-20170927-Reports4	11/27/2017
	Assessment-20170927-Reports3	9/29/2017
	Assessment-20170927-Reports2	9/28/2017
	Assessment-20170927-Reports1	9/28/2017
	Assessment-20170927-Reports	9/28/2017
Archived Projects	Generated appear he organized	d reports ere by date

# 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 Microsoft Entra ID 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 Microsoft Entra ID.

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

Azure Active Directory	ations 🖈 …
»	+ New registration 🕀 Endpoints 🧷 Troublesh
<ul> <li>Overview</li> </ul>	
Preview features	The put the new App regist pape search preview! C
X Diagnose and solve problems	Ty out the new App regime the scale preview of
Manage	0
🚨 Users	
A Groups	
External Identities	All applications Owned applications Delet
👃 Roles and administrators	$\sim$ Start typing a name or Application ID to filter the
Administrative units	
Enterprise applications	Display name
Devices	AP
III, App registrations	A0
(A) Identity Governance	
Application proxy	<b>V5</b>
Licenses	
Azure AD Connect	

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 applicatio	on …
* Name	
The user-facing display name for this ap	plication (this can be changed later).
Supported account types	
Who can use this application or access t	his API?
<ul> <li>Accounts in this organizational dire</li> </ul>	ctory only only - Single tenant)
<ul> <li>Accounts in any organizational dire</li> </ul>	ctory (Any Azure AD directory - Multitenant)
<ul> <li>Accounts in any organizational dire</li> </ul>	ctory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft accounts only	
Help me choose	
Redirect URI (optional)	l>
We'll return the authentication response changed later, but a value is required fo	to this URI after successfully authenticating the user. Providing this now is optional and it can be r most authentication scenarios.

### Step 2 — Grant API Permissions to Enterprise App

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

Manage		The "Admin consent reas	uired" column shows th	e default value for an organization. However, user co
	Branding			
Э	Authentication	Configured permissions		
+	Certificates & secrets	Applications are authorized to	all APIs when they a	are granted permissions by users/admins as part
111	Token configuration	all the permissions the at	tion needs. Learn mo	re about permissions and consent
	API permissions	+ Add a permission </th <th>Grant admin consent</th> <th>for Kaseya</th>	Grant admin consent	for Kaseya
6	Expose an API	API / Permissions name	Туре	Description
12	App roles	∽ Microsoft Graph (1)		
24	Owners	User.Read	Delegated	Sign in and read user profile
4	Roles and administrators   Preview	0		
0	Manifest	To view and manage permissio	ons and user consent,	try Enterprise applications.

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**.

Request API permissions	×
C All APIs Microsoft Graph https://graph.microsoft.com/ Docs @* What type of permissions does your application require?	i
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
₽ dire	×
The "Admin consent required" column shows the default value for a permission, user, or app. This column may not reflect the value in yo used. Learn more	in organization. However, user consent can be customized per $$\times$$ our organization, or in organizations where this app will be
Permission	Admin consent required
Directory.AccessAsUser.All ① Access directory as the signed in user	Yes
Directory.Read All ① Read directory data	Yes
Directory.ReadWrite.All      Read and write directory data	Yes

- 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.

Delegated permissions	Application permissions
our application needs to access the API as the signed-in user.	Your application runs as a background service or daemon without a signed-in user.
ct permissions	expand all
subscription.read.all	×
	^ 
The "Admin consent required" column shows the default we permission, user, or app. This column may not reflect the vused. <u>Learn more</u>	value for an organization. However, user consent can be customized per Xalue in your organization, or in organizations where this app will be
<ul> <li>The "Admin consent required" column shows the default v permission, user, or app. This column may not reflect the v used. Learn more</li> <li>Permission</li> </ul>	value for an organization. However, user consent can be customized per Xalue in your organization, or in organizations where this app will be Admin consent required
The "Admin consent required" column shows the default v permission, user, or app. This column may not reflect the v used. Learn more Permission Subscription (1)	value for an organization. However, user consent can be customized per alue in your organization, or in organizations where this app will be Admin consent required

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 cor						
+ Add a permission	✓ Grant admin consent for					
API / Permissions ne	Grant admin consent for					
∽ Microsoft Grann (10)						
Audit tog.Read.All	Application Read all audit log data					
<u> </u>						

- Step 3 Create Secret Key for Enterprise App
  - 1. From your app, click **Certificates & Secrets** from the left-menu.
  - 2. Click New client secret.

#### **RapidFireTools**<sup>®</sup>

Manage		Certificates can be used as secrets to prove the application's identity wh		
	Branding			
Э	Authentication	Upload certificate		
Ŷ.	Certificates & secrets			
111	Token configuration	No certificates have been added for	this application.	
-@-	API permissions			
4	Expose an API			
14	App roles	Client secrets		
24	Owners	A secret string that the presention	uses to prove its identity when reque	
2,	Roles and administrators   Preview	all New effect execut		
0	Manifest	- New client secret	Factor.	
Sup	port + Troubleshooting	Description	Expires	
Þ	Troubleshooting	No client secrets have been created	for this application.	

- 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.

Application registration certificates, secrets and federated credentials can be found in the tabs below.						
Certificates (0) Client secrets (1) Federated credentials (0) A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.						
Description Expires Value 🛈 Secret ID						
secret	6/29/2023	AAv8Q~9AdA3If [	7df6781e-5c53-4494-be86-ef672006cf23	D	١	

## Step 4 — Add App as Reader to Root Management Group

1. From your Azure tenant, navigate to **Microsoft Entra ID > Properties**. Switch **Access management for Azure resources** to **Yes**.

Home > test org	
Azure Active Directory	erties …
«	Save X Discard   R Got feedback?
Identity Governance	Country or region Argentina
Application proxy	location
Custom security attributes (Preview)	United States datacenters
Licenses	Notification language
Cross-tenant synchronization	English
Azure AD Connect	Tenant ID
📮 Custom domain names	
Ø Mobility (MDM and MAM)	lechnical contact ©kaseya.com ✓
📍 Password reset	Global privacy contact
🎒 User settings	
Properties	Privacy statement URL
Security	✓
Monitoring	Access management for Azira recourses
Sign-in logs	Access management for Azure resources
Audit logs	groups in this tenant. Learn more
Provisioning logs	Yes No
P Log Analytics	Manage security defaults

2. Next, navigate to **Microsoft Entra ID** > **App registrations**. Find and click on the app you created earlier. Copy the complete display name of the app to your clipboard.

Home > Joe test org   App registrations >	
職 microproapp 🛷 …	
✓ Search «	📋 Delete 🜐 Endpoints 🐱 Preview features
Overview	A Freedile
🗳 Quickstart	> Essentiais
💋 Integration assistant	Display name : <u>microproapp</u>
	Application (client) ID : d8f9b041-47ae-4570-a17d-3a5f75ec42ca
Manage	Object ID : a301dc21-9efe-4428-a194-a272063e069f
🔤 Branding & properties	Directory (tenant) ID : 0b9c92ff-7df1-4895-86a8-fee37e1a28ab
Authentication	Supported account types : <u>My organization only</u>
📍 Certificates & secrets	Starting June 20th 2020 we will be langer add any new featurer to Aru
Token configuration	but we will no longer provide feature updates. Applications will need to
- API permissions	Col Statul - Decementation
🙆 Expose an API	Get started Documentation
App roles	Ruild your app
A Owners	Build your app

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

$\equiv$ Microsoft Azure				
Home > Joe test org   App registration	All Services (26) Resources Resource Groups Azure Active Directory (0)			
✓ Search	Services			
Overview	🖎 Management groups 🖉			
📣 Quickstart	EB Proximity placement groups			
🚀 Integration assistant	👍 Resource management private links			
Manage	A Groups			
Branding & properties	Documentation			
Authentication	Management groups - Cloud Adoption Framework			
📍 Certificates & secrets	Organize your resources with management groups - Azure Gover			
Token configuration	Quickstart: Create a management group with portal - Azure gover			

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

+ Create + Add subscription	Č) Refresh 🛛 🗍 Exp	pand / Collapse all	↓ Export to CSV	/ 💛 Feedback	
Use management groups to group su Started" tab to learn more.	ubscriptions. Click on an ex	isiting group to drill in,	, view details and go	vern resources. Right-o	click on any subscription
Showing 0 subscriptions in 2 groups					
$\uparrow \downarrow$ Name		Туре	ID		
🤝 🖍 Tenant Root Group		Managem	ent group 0b9c	92ff-7df1-4895-86a8	3-fee37e1a28ab
Micro Pro Group		Managem	ent group Micr	oprogroup	

5. Select Access Control (IAM).

Home > Management groups >	
Anagement group	\$ ···
	+ Create $+$ Add subscription 💍 Refresh 🛋 Rename group
(A) Overview	$\wedge$ Essentials
Subscriptions	Name : Tenant Root Group
Resource Groups	ID : 0b9c92ff-7df1-4895-86a8-fee37e1a28ab
Resources	Access Level : Owner
Activity Log	Path : / Tenant Root Group
ති Access control (IAM)	
Governance	Showing 0 subscriptions in 2 groups
🌱 Get started	
Security	T↓ Name Ty
Policy	🗸 🕅 Tenant Root Group M
📩 Deployments	(🕅) Micro Pro Group M
Cost Management	
颖 Cost analysis	
Budgets	

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

Home > Management groups > Tenant Root Group						
PR         Tenant Root Group   Access control (IAM)            Management group						
₽ Search «	+ Add ↓ Download role assignments 🗉 Edi	t columns 💍 Refresh 🛛				
(A) Overview	Add role assignment	any assignments Class				
📍 Subscriptions	Add co-administrator Add role assignment	eny assignments Class				
Resource Groups	Add custom role					
Resources	View my access					
Activity Log	view my access					
Access control (IAM)	Check access	aal or managod identity bar				
Governance Check access						
🍯 Get started						
Security	Grant access to this recourse	View access to this				
Policy	Grant access to this resource	view access to this				

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

	× Type : All Category : All
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	+ <u>Select members</u>		
	Name	Object ID	
	No members selected		
Description			
Description	Optional		

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

Select members		
Select ①	-	•
microproapp		

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

Members	+ Select members		
	Name	Object ID	Туре
	microproapp	1811fd1f-8454-4703-8c50-608f7ae70e27	Арр
Description	Optional		
Review + assign	Previous Next		

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

+ Add ↓ Download role assignments	☷ Edit columns 💍 Refresh   ≻	🤇 Remove 📗 🔗 Feedback		
Check access Role assignments Role	es Deny assignments Classic a	dministrators		
	Type : All Role : All Sco	ope : All scopes Group by : Role		
2 items (1 Users, 1 Service Principals) Name	Туре	Role	Scope	Condition
∨ Reader				
microproapp	App	Reader ①	This resource	None
✓ User Access Administrator				
kaseya.com#	User	User Access Administrator ①	Root (Inherited)	None

#### **RapidFireTools**\*

## 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**.

		₽ Search res	ources, services, and docs (G+/)	
Home > Kaseya >				
🜉 App 👘 💉 🗠				
	🗊 Delete 🕀 Endpoint	s 🐱 Preview features		
Overview	Got a second? We would be a second?	Ild love your feedback on Microsoft ide	entity platform (previously Azure AD for developer). $\rightarrow$	
🗳 Quickstart				
🚀 Integration assistant				
Manage	Display name	: AppTest1	Client credentials	:
Branding & properties	Application (client) ID	: 7bf	Redirect URIs	: Add a Redirect URI
	Object ID	: 185	Application ID URI	: Add an Application ID URI
Authentication	Directory (tenant) ID	: a1c	Managed application in I	: AppTest1
📍 Certificates & secrets	Supported account type	es : My organization only		
Token configuration				

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

Application registration certificates, secrets and	federated credentials	can be found in the tabs below.		×
Certificates (0) Client secrets (1) Federal A secret string that the application uses to prove it	ted credentials (0) ts identity when req	uesting a token. Also can be referred to as appli	cation password.	
+ New client secret				
Description	Expires	Value 🕕	Secret ID	
secret	6/29/2023	AAv8Q~9AdA3If 🕅	7df6781e-5c53-4494-be86-ef672006cf23	۵

# Modify Report Privacy Options in Microsoft 365 Admin Center

By default, the Microsoft Cloud will conceal user information such as usernames, groups, and sites for certain reports. This can affect how data is presented in your Microsoft Cloud Assessment reports. If you are missing details in your reports, follow these steps to resolve the issue:

- 1. From your browser, access the Microsoft 365 admin center at admin.microsoft.com.
  - .... Microsoft 365 admin center  $\equiv$ ND-Solutions ŵ Home 8 Users 묘 Devices የድ Teams & groups Billing Þ Setup Show all
- 2. From the home page, click **Show all** from the side menu.

3. Then click Settings.

#### **RapidFireTools**<sup>®</sup>



4. Then open Org settings.



5. From the list of Services, scroll down and click Reports.

1	Settings	^	9	
	Domains		1	Office Scripts
	Search & intelligence		100	Productivity Score
	Org settings		1.7	Reports
	Integrated apps			
	Partner relationships		B	SharePoint
Þ	Setup		S	Sway
k	Reports	$\sim$		User consent to anns
$\otimes$	Health	$\sim$	A 33	oser consent to apps
			Ô	User owned apps and services
Adr	nin centers		$\overline{a}$	What's new in Office
۲	Security		2	Whiteboard

6. From the right-hand menu, **DESELECT** the **Display concealed user, group, and site names in all reports** option. Then click **Save**. Disabling this option will ensure your Microsoft Cloud Assessment reports have more detailed data.

		Ł		ŵ	?	W
6.68						×
	Reports					
<b>N</b>	Reports found in the Microsoft 365 admin center pro organization's usage data. Your organization's data i security and privacy safeguards.	ovide in s manag	formation ged by f	on abou rusted o	t your cloud	
Description	By default, reports conceal user information such as You can decide to display concealed information if y organization's policies require it.	usernar ou pref	nes, gro er or if y	ups, an our	d sites.	
Manage multi-factor authentication settings for our users. Choose how news about your organization and industry then	This setting applies to Microsoft 365 usage reports i Microsoft Graph and Power BI and the usage report: center.	n Micro s in Micr	soft 365 rosoft Ti	admin eams ad	center, min	
Choose how often users get feature updates and the Office ap	Display concealed user, group, and site names i	n all rep	orts			
Let users open files stored in third-party storage services in O						
Let users automate their tasks in Office on the web.	Microsoft 365 usage analytics Usage data is analyzed and used to make charts and	l graphs	to help	you un	derstar	id
Manage data privacy controls for Productivity Score.	your organization's use of apps and services. Report Microsoft 365 admin center and in Power BI. Learn h	s can be low to g	e found let start	in the ed with	Power I	81
Manage data privacy controls for Admin Center reports	Make report data available to Microsoft 365 usa	ige anal	ytics fo	Power	BI	
Control external sharing.						
Manage sharing and content sources allowed for Sway.	Save					

# **Microsoft Cloud Assessment Reports**

The Microsoft Cloud Assessment allows you to 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

Report Name	Description
	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 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

Report Name	Description
	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.
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	The SharePoint Assessment Report is a detailed assessment that

Report Name	Description
Assessment Report	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, 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.

#### **RapidFireTools**°

## 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	<ul> <li>Before you scan the AWS environment, you will need to following AWS credentials:</li> <li>AWS Access Key ID</li> <li>AWS Secret Key</li> <li>WORK WITH YOUR TECH TEAM TO GATHER THESE CREDENTIALS, AND TREAT THEM WITH THE APPROPRIATE SECURITY PRECAUTIONS!</li> </ul>

Follow these steps to perform a AWS Assessment.

# Step 1 — Download and Install the Network Detective Pro app

Go to <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer. Site Name:
Customer A - Assessment
Ok Cancel

#### **RapidFireTools**°

# 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.

SITE	Granite Partners / Edt Ste      Press Start to begin a new Project Start		
Active Project	Network Detective Wizard		
	Select Assessment Type		
	What type of assessments are you performing at this site? (Check all that apply)		
Archived Projects	O IT and Cloud Assessments:		
Progress Reports	Network Assessment (Domain)     Network Assessment (Domain)     Securty Assessment (Workgroup)     Securty Assessment (Workgroup)     Solution Assessment     SQL Server Assessment     DR Assessment (Quick)     BDR Assessment (Quick)		
Generated Reports	Datio BDR Assessment (Culler)     Datio BDR Assessment (Culler)     Unitrends BDR Assessment (Culler)     Microsoft Cloud Assessment     Other (Use for ad-hoc reporting. No checklist provided.)		
Downloaded Reports			
i de la companya de l			
Discovery Agents			
	Back Next Cancel		

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

 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.

I Network Detectiv	e Pro - v4.0.1328
Ê	🖉 🖷 🖺 🔺 🌣
Home A	ppliances Connector Service Plans Reporter Users Preferences
	Back to Home
SITE	Assessments   Reports   Export   Explore Data
	Assessment-20220929
	0% Complete 0 Complete 0 Required 0 Optional Created 29-Sep-2022 01:55 PM Updated 29-Sep-2022 01:55 PM Previous Project: Select
Active Project	AWS Assessment 0% Complete 0 Complete 0 Required 0 Optional Created 29-Sep-2022 01:55 PM Modified 29-Sep-2022 01:55 PM
Archived Projects	Press the 'Ran Collector Julian collector.
Progress Reports	Double-click items to open.
Generated	Press the 'Run AWS Data Collector' button to initiate data collection. If you do not have a results life from an AWS Doud Assessment Scan, please use the 'Run AWS Data Collector' button to generate scan data.
Heports	V Scans 🖉 Inport Scan File 👔 Initiate External Scan 🖉 Download Scans 👔 Run AWS Data Collector
Downloaded Reports	Scan(s) Expand Al 0 Files

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.

Refresh Checklist	Printed Checklist

# 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 (IAM) > Users.



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

Permissions         Groups (1)         Tags (3)         Security credentials         Access Advisor					
Permissions policies (3) C Remove Add permissions v					
	Filter by Type				
Q Sec	Q. Search         All types         ▼         < 1 >         ⊘				
	Policy	name 🖸 🔺	Туре	▼ Attached via [2]	
0	٠	AWSAccountManagementReadOnlyAc	AWS managed	Group TechnicalG	iroup
0	٠	IAMReadOnlyAccess	AWS managed	Group Technical	Group
	٠	ReadOnlyAccess	AWS managed - job function	Group TechnicalG	iroup

- ReadOnlyAccess
- IAMReadOnlyAccess
- AWSAccountManagmentReadOnlyAccess

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

1. Next, open the Security credentials tab for the user.



2. Then click Create access key.



3. If prompted, select the Third party-service use case and click **Next**.



4. Enter a description for the key and click Create Access Key.

<b>Set description tag – optional Info</b> The description for this access key will be attached to this user as a tag and shown alongside the access key.		
Description tag value Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.		
Network Detective Online AWS Scan		
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: : / = + - @		
Cancel Previous Create access key		

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

Retrieve access keys Info		
Access key If you lose or forget your secret according to the old key and make the old key an	ess key, you cannot retrieve it. Instead, create a 29 inactive.	
Access key	Secret access key	
AKIAQLOSGIZXY2DHLHNF	•**************** <u>Show</u>	
4	•	

#### **RapidFireTools**\*
## 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**.

🔨 Gran	nite Partners / Edit Ste Assessments   Reports   Export   Explore Data					
Ass 0% Com	Assessment-20220929           D1: Complete 0 Complete 0 Required 0 Optional Created 23-Sep-2022 01:55 FM lipidated 23-Sep-2022 01:55 FM Previous Project: Select					
A	WS Assessment 0% Complete 0 Complete 0 Required 0 Optional Created 29-Sep-2022 01:55 PM Modified 29-Sep-2022 01:55 PM					
Press AW: Collect to init oolil Double-c	Press the 'Run AWS Data Collector' button to initiate data collection  Press the 'Run AWS Data Collector' button to initiate data collection.  Provide rate areads file from an AWS Obd Assessment Scan, please use the 'Run AWS Data Collector' button to generate scan data.					
<b>~</b> B	Scans 🖉 Inpot Scan File 👔 Initiale External Scan 💽 Download Scans 👔 Run AWS Data Collector					
Sca	n(s) Expand Al 0 Files					

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



4. 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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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 allows you to 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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**.

New Site 🛛 💌
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer.
Customer A - Assessment
Ok Cancel

# 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.

Refresh Checklist	Printed Checklist
-------------------	-------------------

# Step 4 — Access RapidFire Tools Portal and Customize Branding

Access the RapidFire Tools Portal at <u>https://www.youritportal.com</u>.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.

Micro Consulting	Organizations To Do	Global Settings	?	9 joe-admin-user Ҟ
General	Global Settings / Branding	-		
🖌 Branding	orosa octango, pranang			
<ul> <li>Connections</li> </ul>	Branding @			
🗘 Admin Alerts	Thomas			
2 Users	(Click to Preview)			Reptification
Compliance Manager GRC	> Default		RapidFireTooks	the second
<ul> <li>VulScan</li> </ul>	) Delault			1
E Service Plans	Light		C marks	9 0 0 9 0 0
Email Groups			Making (House 10)	And a second sec
Data Collectors				
C IT Complete				
License Usage	Custom Branding	$\odot$		
🖉 API Keys	Company Name	Co	company Logo	
	Displayed in top left of me	nu bar U	Ipload a logo to customize your log	in page (JPG or PNG, < 1MB in
	Micro Consulting		4	
				3
			Ψ :	

# 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**.



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



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.
Peform 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.



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.

Q C	Computer Scanner	x
	Running Computer Scanner	
	Getting local users	
	Privacy Policy Terms	of Service

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.

#### **RapidFireTools**<sup>®</sup>

୍	Download File	25				-		×
TI Al	ne following sca I to download al	ns have been uploaded I available scans.	l and are available for	r download. Select all downloads you wish to ir	nport into the current site and press Do	wnload Selected o	r press Down	oad
	Туре	Device Name	Task ID	File Name	Date	Size	Label	
A	GT Connector							- 1
	Connector	AGT Connector	N/A	RFTDEV-9856-TMP-00155D010865.zip	4/17/2023 8:09:28 PM	0.69 MB		
	Connector	AGT Connector	N/A	KA-PW00PHAL-0C9A3C6E109A.zip	4/17/2023 7:19:04 PM	0.48 MB		
	Connector	AGT Connector	N/A	DESKTOP-4171AR0-00155D010804.zip	4/17/2023 7:52:10 PM	0.84 MB		
					Data Science			
				6				

4. 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**.

Q Network Detec	tive Merger			-		×
Files from the Compo In order to merge inc	uter Data Collector (.CDF) need to dividual computers, you will need to	be merged with the o specify a domain or	riginal Network Detectiv workgroup for each CDI	e data file (.NDF) before gene Ffile.	rating a rej	port.
Custom Domain:	Select CUSTOM in the dropdown li	ist under "Merge Into	" to use the Custom Don	<i>(optional)</i> nain.		
					<u>Re</u>	resh
Computer	Local Domain/Workgroup	OS	Run Date	Merge Into		
DESKTOP-4171	TEST.PERFORMANCEIT.C	Windows 10 Ent	4/17/2023 3:51:40 PM	KASEYA.COM		$\sim$
KA-PW00PHAL	KASEYA.COM	Windows 10 Pro	4/17/2023 3:18:34 PM	KASEYA.COM		$\sim$
RFTDEV-9856-T	TEST.PERFORMANCEIT.C	Windows 10 Pro	4/17/2023 1:08:58 PM	[Use Workgroup]		~
	м	lerge Now C	lose	exclude KASEYACOM CUSTOM [Use Workgroup]	Î	
						.:

5. 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 <u>"Set Up Dark Web ID Integration with Network Detective Pro" on page 162</u> 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

#### **RapidFireTools**<sup>®</sup>



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



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



5. 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 (<u>https://www.idagent.com/</u>) 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 <a href="https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-l-enable-API-access-for-ID-Agent-">https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-l-enable-API-access-for-ID-Agent-</a>.

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

#### **RapidFireTools**°

dismiss the Preferences menu.

	Users Preferences					
et Bus	Preferences					
cklist	Report Default Reporter Email Groups Issue Overrides Integrations					
Acco	Dark Web ID IT Glue					
essme	Enable Dark Web ID Integration					
CKIIST	Dark Web ID Usemame: jweakland					
orter	Dark Web ID Password:					
essme cklist:	Test Connection					
o test						
essme cklist:						

## 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.

I     Image: Security       File     Home       Share     View						
← → × ↑ 📜 « Assessment	20230427-Reports > Security ~ 0	Search Security				
t Ouishaanna	^ Name	Date modified				
	Cyberattack Risk Assessment without infographics.docx	8/23/2023 12:31 PM				
📃 Desktop 🛛 🖈	Cyberattack Risk Assessment docy	8/23/2023 12:31 PM				
🐥 Downloads 🛛 🖈		0,20,2020 12:01111				
🗄 Documents 💉						
📰 Pictures 🧳						

## 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer.
Site Name:
Customer A - Exchange Assessment
Ok Cancel

## 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

**RapidFireTools**<sup>®</sup>

- 1. On the target network, log in to the local machine with Administrator privileges.
- 2. Download the **latest Exchange Assessment Data Collector** program from <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

Open Network Assessment Data File		×
COO - Libraries > Documents > E	xchange Scan Data 🔹 🔸	Search Exchange Scan Data 👂
Organize 🔻 New folder		≣ ▼ 🔟 🔞
🔆 Favorites	Documents library     Exchange Scan Data	Arrange by: Folder 🔻
Cibraries	Name	Date modified Ty
Documents     Music	SampCo.edf	12/1/2015 7:03 AM EC
Pictures		
🤣 Homegroup		
r∰ Computer		
DVD RW Drive (E:) RFT BU Dsk1 9-26	<b>▼</b>	•
File name: SampCo.edf	•	Assessment Data File (*.ndf;*.sc Open Cancel

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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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 allows you to 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.

#### **RapidFireTools**\*

## 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer. Site Name:
Customer A - SQL Server Assessment
Ok Cancel

## 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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 ve	ersion 2.0.50727.5485)	×
	Credentials		
Credentials     Verify and Run     Collection Progress     Finish	The SQL Server Asse Authentication or SQL should have sufficient Clicking Next will test running. This can take	essment Data Collector can use eith . Server Authentication. SQL Serve administrative privileges to collect your credentials and detect the ver e up to 30 seconds in some cases.	er Windows r Authenticated account data (i.e., 'sa'). sion of SQL Server that is
	Server: Port: Authentication: User Name: Password:	1433 SQL Server Authentication sa	default ▼
Check Data Collector Version Load Settings from File Open Working Folder			Next >

• Windows Authentication credentials.

SQL Server Data Collector - 1.	11 (running on .NET	version 2.0.50727.5485)	×
	Credentials		
<ul> <li>Credentials</li> <li>Verify and Run</li> <li>Collection Progress</li> </ul>	The SQL Server Ass Authentication or SQ should have sufficier Clicking Next will test	essment Data Collector can use e L Server Authentication. SQL Se t administrative privileges to colle	either Windows rver Authenticated account ct data (i.e., 'sa'). version of SQL Server that is
Finish	running. This can tak	e up to 30 seconds in some case	95.
	Server:		
	Port:	1433	default
	Authentication:	Windows Authentication	-
	User Name:		
	Password:		show
Check Data Collector Version Load Settings from File Open Working Folder			Next >

- 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.

Open Network Assessment Data File									X
CO V Libraries > Documents > S	QL S	Ser	erver Scan Data 🕨 🔻	•	<del>fy</del>	Search SQ	L Server S	ican Data	٩
Organize 🔻 New folder							:==		?
🛛 🔆 Favorites			Documents libra SQL Server Scan Data	ar	у	Arra	ange by:	Folder 🔻	
⊿ 🧊 Libraries			Name				Date m	odified	Ту
Documents	=		퉬 Backup				12/1/20	15 11:12 AN	И Fil
Public Documents			AnonSQL.ddf				12/1/20	15 7:02 AM	DI
🖻 🎝 Music									
Pictures									
Videos									
> 🤣 Homegroup									
Commuter									
→ 🚰 TI106234W0C (C:)	-	•	•						F
File name: AnonSOL ddf					•	Assessment	Data File	(*.ndf:*.sc	•
Allohoge.uur						Open		Cancel	

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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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:

•	
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

### Standard Reports

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 allows you to generate the following reports:

## **Standard Reports**

Report Name	Description
Database Detail Report	This report details the settings and health of individual databases that reside on the scanned SQL Server. It lists the database properties, potentially missing indexes, locks, statistics, fragmentation, and existing indexes. Without this tool, it would be a daunting task to collect all this information. Because this report documents each database individually, it can be run ad-hoc when specific database performance problems arise. But best practice is not to wait and react to these problems but plan to run this report on a regular basis (quarterly or monthly, depending upon the how critical the application is). This report will help

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

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 <u>Pre-Scan Network Configuration Checklist</u> 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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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.

New Site
All Network Detective assessments are organized into Sites. A site can be a physical location or a logical grouping, such as a customer. Site Name:
Customer A - Assessment
Ok Cancel

#### **RapidFireTools**<sup>®</sup>

## 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**.

- 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



#### Switch Between Active Assessment Checklists



4. 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.

Refresh Checklist	Printed Checklist
-------------------	-------------------

## 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.

$\mathbf{\vee}$	Custome	ər A			Assessmen	ts Reports	Export Explore	Data	
	Assessment-20160216								
	0% Complete (	0 Complet	e 2 Required	1 Optional Created	1/15/2015 Updated	1 2/16/2016 Prev	vious Project: Select		
	Security	Assessi	ment (Domain)	0% Complete 0 Con	nplete 🛛 2 Require	ed 1 Optiona	Created 2/16/2016	5 Modified 2/16/2016	
^	Initiate Externa Vulnerability Scan	al	Run Network Detective Data Collector (NDDC) with the Security Data 2	Run Network Detective Data Collector (NDDC) with the Security Data	Reports Not Ready				
	Run Network Detective Data Collector (NDDC) with the Security Data Collector - Network Scan option 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 Dor Controller is not available, or from any workstation on the network. The data collector should be run with Administrative privileges.							<b>work Scan option</b> and to the Domain if the Domain	
^		Scans	Import S	ican File	ate External Scan	Initiate Ap	pliance Scan	Download Scans	
	Scan(s)	Expand A	1		0 Files				

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

	Network Detective Wizard		×	
Initiate External Vuln	erability Scan			
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.				
		Add		
		Remove		
		Remove All		
Email me upon completion at:	xxxxx@rapidfiretools.com	]		
Save settings for this site				
	Back	Next	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.

Add IP Address Range
If only a single IP Address is wanted, leave the Ending IP Address blank.
Starting IP Address: Ending IP Address: Add 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.

Network Detective Wizard	×			
Initiate External Vulnerability Scan 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.				
2	Add Remove Remove All			
Email me upon completion at: xxxxxx@rapidfiretools.com     Save settings for this site     Your scan should be completed in approximately 2 hour(s).				
Back	Next 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.

1 Initiate External Vulnerability Scan	Refresh Checklist
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.	

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.

- Visit the RapidFire Tools software download website at <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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**.

Scan Type	Scan Type
Scan Options Verify and Run Collection Progress	Select type of scan to perform Select one or more the collection process below to run. The amount of collectors to run will affect run-time.
► Finish	Network Data Collector Collect network-wide data using remote protocols. Required for Network Assessments.
	<ul> <li>Local Computer Data Collector (required with Security Data Collection)</li> <li>Collect data on the computer. Typically, used to augment data collection when remote protocols are not available from this computer.</li> </ul>
	Security Data Collector         Collect security data from the current computer perspective. Required for security Assesments.         Perform Network Scan. Required for Share Permissions.
Check Data Collector Version	(running on .NET CLR version 2.0.50727.9151) Next

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

Scan Type	Active Directory
Active Directory	Please onter a username and password with administrative rights to connect to the local
Local Domains	Domain Controller and Active Directory.
Additional Credentials	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
External Domains	screen.
P Ranges	If in a domain, clicking the Next button will test a connection to the local Domain Controller and Active Directory to verify your credentials.
SNMP Information	
VMware	I want to scan
User Control Tests	Active Directory     O Workgroup (no domain)
File Scanner	
Verify and Run	Active Directory Credentials
Collection Progress	corp (FQDN\user)
Einish	•••••
	172
	(running on .NET CLR version 2.0.50727.9151) Back Next

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.

	ta Collector - 2.0.1161 ×			
Scan Type	Local Domains			
Active Directory	Below is a list of the detected domains in the current forest of the Active Directory.			
Local Domains				
Additional Credentials	Gather Information for ALL the domains detected.			
External Domains	<ul> <li>Gather information for only the domains selected below.</li> </ul>			
IP Ranges				
SNMP Information				
VMware				
User Control Tests				
File Scanner				
Verify and Run				
Collection Progress				
► Finish				
	Expand All Collapse All Expand Selected Advanced Tree View			
	(running on .NET CLR version 2.0.50727.9151) Back 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. Click **Next**.

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

Scan Type	Additional Credentials
Active Directory Local Domains	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
Additional Credentials	scan. Calls using the default credentials will always be attempted first.
External Domains	Network Scan Credentials
IP Ranges	
SNMP Information	Username
VMware	Password Add
User Control Tests	corp. (AD user to be used first)
File Scanner	
Verify and Run	
Collection Progress	
Einish	
	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 Da	ta Collector - 2.0.1161	×
Scan Type	External Domains	
Active Directory	List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.	
Local Domains		
Additional Credentials	Domain Add	
External Domains		
IP Ranges		
SNMP Information		
VMware		
User Control Tests		
File Scanner		
Verify and Run		
Collection Progress	Class All Estring	
Finish	Clear All Entries Import from lext File	
	Perform Dark Web Scan for Compromised Passwords	
	X Please enter 1 or more external domains for the Dark Web scan.	
	(running on .NET CLR version 2.0.50727.9151) Back Next	

#### **RapidFireTools**<sup>\*</sup>

**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**.

🕀 Network Detective Dat	ta Collector - 2.0.1161 x
Scan Type	IP Ranges
Active Directory	The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to
Local Domains	the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network cards in this machine.
Additional Credentials	
External Domains	Single IP or IP Range (example: 192.168.0.0-192.168.0.255) Add
IP Ranges	172. 255
SNMP Information	172. 255
VMware	
User Control Tests	
File Scanner	
Verify and Run	
Collection Progress	Clear All Entries Import from lext File Reset to Default
Finish	Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)
	(running on .NET CLR version 2.0.50727.9151) Back Next

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.

🕀 Network Detective Dat	ta Collector - 2.0.1161	×
Scan Type	SNMP Information	
Active Directory	SNMP community strings are used to try to datarmine information about davises datasted	_
Local Domains	during the IP Range scan. Enter any additional community strings used on this network.	
Additional Credentials	Read Community String	
External Domains	Public Public	
IP Ranges	public	
SNMP Information		
VMware		
User Control Tests		
File Scanner		
Verify and Run	Clear All Entries Import from Text File Reset to Default	
Collection Progress		
► Finish	Advanced SNMP Options	
	SNMP Timeout (seconds): 10 IIse Default	
	Attempt SNMD against non ningable devices (slower but more accurate)	
	Attempt swine against non-pingable devices (slower but more accurate)	
	(running on .NET CLR version 2.0.50727.9151) 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). 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.

	VMware			
	VMware credentials are	a required for discovery of VMw	vare hosts. Enter the VMware host server	
	DNS name or IP address	s along with VMware login cred	lentials.	
Additional Credentials				
External Domains	Hostname or IP Addres	iS	Skip connection test	
IP Ranges	Username			
SNMP Information	Password		Add VMware Server	
	Uest	Llear	Connection Varified	
User Control Tests	nost	User	connection vernied	
File Scanner				
Verify and Run				
Collection Progress				
► Finish				
	Clear All Entries	Test All Connections		
	(running on NET CLR	Version 2.0.50727.9151)	Back Next	

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**.

Scan Type	User Control Tests							
	The Security Assessment User Control tests will attempt to access sites in various categories							
Local Domains	from this computer. If you do not wish to include BUILT-IN URLs from a particular category in							
Additional Credentials	your assessment, please uncheck it. Additionally, you may add individual URL to the category testing. Any custom URLs will ALWAYS be checked.							
External Domains								
IP Ranges	Built-in URL Categories							
SNMP Information	🗹 Entertainment 🗹 Pornography 🗹 Shareware							
VMware	🗹 Social Media 🗹 Warez 🗹 Web Mail							
User Control Tests								
File Scanner	Custom URLs							
Verify and Run	URL Category							
Collection Progress	* Entertainment ~							
► Finish								

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

Scan Type	File Scanner	
Active Directory Local Domains Additional Credentials External Domains IP Ranges SNMP Information VMware User Control Tests File Scanner Verify and Run Collection Progress Finish	File Scanner         NOTE: File scanning can cause a temporary increase in resource utilization.         Scan Types:         Personally Identifiable Information (PII)         Scan Options:         Include the scanning of ZIP files         Include the scanning of PDF files         PDF Timeout:         f	
	(running on .NET CLR version 2.0.50727.9151) Back 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.

🛱 Network Detective Dat	ta Collector - 2.0.1161	×
Scan Type	Verify and Run	
Active Directory	Ready to run the data collection. Select your output file location and basename. The final	_
Local Domains	assessment file will be <folder>\<basename>.zip.</basename></folder>	
Additional Credentials	Output Assessment File	
External Domains		
IP Ranges	Folder: C:\Users\ \Desktop	
SNMP Information	Basename: NetworkDetective-20220223 .ZIP	
VMware		
User Control Tests	Launch Pre-scan Analyzer Advanced Options	
File Scanner		
Verify and Run		
Collection Progress		
▶ Finish		
aan ah		
Save Settings to File	(running on .NET CLR version 2.0.50727.9151) Back Start	
oute vertings to the		

**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. Prescan results and recommendations are provided at the completion of the prescan.

Overview Result Sum	nmary Act	ive Direc	ctory S	SQL Server	Network Compu	iters Push Deploy		
Pushing local data collect	tors to remote	e comput	ers requir	es WMI, Adı	min\$ access, and .N	IET 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		<ul> <li>✓</li> </ul>	×			WMI failed. The RPC serv	er is unavailable.	
BROWN-WIN10.CORP.RAPI		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-09SDFE1.CORP.R		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-1HM0E7I.CORP.R		✓	×			WMI failed. The RPC serv	er is unavailable.	
DESKTOP-6ND4Q8O.CORP	172.18.0.207	✓	✓	✓	✓	Full access		
DESKTOP-7DBVA30.CORP.R	10.236.83.1	✓	?			Accessing WMI		
		1	×			WMI failed The RRC con-	or is unavailable	

Enter any Comments and then click Start.

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

Scan Type	Collection Progress
Active Directory Local Domains Additional Credentials External Domains IP Ranges SNMP Information VMware User Control Tests File Scanner Verify and Run Collection Progress Finish	Active Directory:       Initializing         Eventlogs:       Initializing         SQL Servers:       Initializing         Internet:       Initializing         DHCP:       Initializing         Network:       Initializing         Local Collector:       Getting quick fix engineering         Security Collector:       Getting login events; 29 Port(s) Remaining; 13 URL(s) Rem
Save Settings to file	Cancel Data Collection Wrap It Up  Collection in progress, please be patient (running on .NET CLR version 2.0.50727.9151) Next

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**.

Retwork Detective Dat	ta Collector - 2.0.1161 ×
Scan Type	Finish
Active Directory	
Local Domains	The data collection process has been successfully ended, and file(s) with the partial data have been generated. Please be aware that reports created from this data may have missing
Additional Credentials	sections or may otherwise contain incomplete information as the collection process did not fully finish.
External Domains	Collect the output file from
IP Ranges	C:\Users\\Desktop
SNMP Information	Open
VMware	
User Control Tests	
File Scanner	
Verify and Run	
Collection Progress	
🕨 Finish	
Save Settings to File	(running on .NET CLR version 2.0.50727.9151) Done
sare settings to the	

#### **RapidFireTools**<sup>\*</sup>

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 <u>https://www.rapidfiretools.com/ndpro-downloads/</u> 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

RetworkDetective Push Deploy Tool										
✓ Settings and Configuration	Computers and State	IS								
✓ Computers and Status	When you are read	lv to being data collectio	on, click the '	'unpause" bu	tton. This will imr	nediately com	mence data ci	election. You may	add or manage	
Collected Data Files	computers to push	the local data collector	to interactive	ly. Right-click	on a computer f	or additional o	ptions.			
	Hostname or IP Address	Add Single Compute	Add fro	m File	dd from IP Rang	e Save C	omputers to F	le i	Show:	Al 👻
	Computer	IP Address	WMI Access	Admin\$ Access	.NET 3.5 or 4.5	File Extracted	Data Collected	Status		
			1		a la carcia					
	Total Computers: 0, Remainin	g: 0, Successful: 0, Fai	led: 0							
								- P	anta Ner	t Const
								< B	sox Nex	t >   Cancel

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.

2	Ne	tworkDetective P	ush Deplo	y Tool						×
Settings and Configuration	Computers and Sta	tus								
Computers and Status	When you are rea	ady to being data collec	tion, click the	"unpause" bu	tton. This will in	mediately com	mence data c	ollection. You may a	dd or manage	
Collected Data Files	computers to pus	h the local data collecti	or to interactive	ely. Right-click	on a computer	for additional of	options.			
001000000000000000000000000000000000000	Hostname or IP Address	Add Single Compu	ter Add h	om File A	dd from IP Ran	ge <u>Save</u> (	Computers to F	le	Show: All	v
	Computer	IP Address	WHI Access	Admin\$ Access	.NET 3.5 or 4.5 Installed	File Extracted	Data Collected	Status		^
			<ul><li>✓</li></ul>	✓	<ul><li>✓</li></ul>	<ul><li>✓</li></ul>	✓			
			✓	<ul> <li>✓</li> </ul>	✓	✓	✓			
			<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>			
			✓	✓	✓	✓	✓			_
			✓	✓	✓	✓	✓			
			×	×	¥	¥	¥			
		_	•	¥ (	•	•	•			
			¥	¥	•	•	•			
			-	-	¥	· ·	· ·			
						· ·	-			
				· ·		· •				
			×	×	×	<ul> <li>✓</li> </ul>	1			
			1	1	1	~	1			
			✓	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	✓	✓			
	Total Computers: 202, Rem	aining: 0, Successful: 2	1, Failed: 181		1	,	1			
								< Bac	k Next>	Cancel

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

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

Collected Data Files	The table will show all data files that exist in the current sto Current Storage Folder: C:\download\NetworkDetective	rage folder, not just ones that have been collected from PushDeployTool	the current Computers and Collection Status ta	ab. <u>Open Folder</u>
	Filename	File Date	File Size	,
	źó	11/03/16 8:39:05 PM	667 KB	_
	.zip	11/03/16 8:44:36 PM	670 KB	
	zip	11/03/16 8:43:14 PM	526 KB	
	zip	11/03/16 8:42:17 PM	732 KB	
	zip	11/03/16 8:39:12 PM	1123 KB	
	zp	11/03/16 8:37:47 PM	700 KB	
	zip	11/03/16 9:06:29 PM	714 KB	
	.zip	11/03/16 9:06:08 PM	673 KB	
	zip	11/03/16 8:42:46 PM	661 KB	
	zip	11/03/16 8:49:00 PM	704 KB	
	zip	11/03/16 8:42:24 PM	2029 KB	
	.zp	11/03/16 9:06:42 PM	941 KB	
	zip	11/03/16 8:42:57 PM	584 KB	
	.zp	11/03/16 8:41:49 PM	703 KB	

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

#### MORE INFO:

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

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

After all of the **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.

Network Detective Wizard
Select the Scan Results
Select the resulting scan file or files. Multiple scan files or compressed archives can be selected in the file browser. Use CTRL-Click or SHIFT-Click to select multiple files.
If you do not have a results file from a network scan, please download the Data Collector and complete a scan first.
Browse
Back Next Cancel

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.

#### **RapidFireTools**<sup>®</sup>

#### Click Merge Now.

Network Detective Merger —							Х
Files from the Con In order to merge	nputer Data Collector (.CD individual computers, you	F) need to t will need to	be merged with the o specify a domain or	riginal Network Detective dat workgroup for each CDF file.	a file (.NDF) before gene	rating a rep	oort.
Custom Domain:	(optional) "Select CUSTOM in the dropdown list under "Merge Into" to use the Custom Domain.						
Computer	Local Domain/Work	aroup	OS	Bun Date	Merge Into	Ref	resh ∧
DAEDALUS	CORP.	.C	Windows 10 Ent	9/27/2017 4:49:05 PM	Corp.MyCo.com	~	
DAEDALUS	CORP.	.C	Windows 10 Ent	10/12/2017 2:39:08 PM	Corp.MyCo.com	~	
DAMION	CORP.	.C	Windows 10 Pro	10/12/2017 2:56:35 PM	[Use Workgroup]	~	
DC	CORP.	.C	Windows Server	10/2/2017 4:24:03 PM	[Use Workgroup]	~	·
DC	CORP.	.C	Windows Server	8/21/2017 1:54:00 PM	[Use Workgroup]	~	
DESKTOP	CORP.	.C	Windows 10 Ent	9/27/2017 4:46:44 PM	[Use Workgroup]	~	
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:31:42 PM	[Use Workgroup]	~	·
DESKTOP	CORP.	.C	Windows 10 Pro	10/12/2017 2:44:44 PM	[Use Workgroup]	~	·
DESKTOP	CORP.	.C	Windows 10 Pro	9/27/2017 4:41:58 PM	[Use Workgroup]	~	
DEV	CORP.	.C	Windows 10 Pro	10/12/2017 2:43:44 PM	[Use Workgroup]	~	
DEVILS	CORP.	.C	Windows 10 Pro	10/12/2017 3:03:47 PM	[Use Workgroup]	~	· 🗸
	1	М	erge Now C	lose			

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:



#### **RapidFireTools**<sup>®</sup>
# 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 <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a> 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.

Reports Create Reports			
All Reports V 3% Availab	ble 3 Available Reports 113 Unavailable Reports		
Exchange	SQL Server		Security
Standard Reports	Standard Reports	Standard Reports	Standard Reports
Exchange Risk Report (.docx)	Routine Health Report (.docx)	Client Risk Report (.docx)	Security Risk Repo
Exchange Management Plan (docx) SQL Server Detail Report (docx) Network Management Plan (docx) Security Ma			Security Managem
Exchange Mailbox Detail Report (.docx)	Database Detail Report (.docx)	Full Detail Report (.docx)	Outbound Security
Exchange Mobile Device Report (docx) Maintenance Plan Report (docx) Excel Export (xlsx) Security Polic			Security Policy Ass
Exchange Traffic and Use Report (.docx)	SQL Server Agent Jobs Report (.docx)	Site Diagram (.docx)	Share Permission F

- 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 the Windows Firewall						
	This includes the following rules:					
	Windows Management Instrumentation (ASync-In)					
	<ul> <li>Windows Management Instrumentation (WMI-In)</li> </ul>					
	Windows Management Instrumentation (DCOM-In)					
	Allow File and printer sharing to operate through Windows Firewall					
	This includes the following rules:					
	File and Printer Sharing (NB-Name-In)					
	File and Printer Sharing (SMB-In)					

#### **RapidFireTools**<sup>®</sup>

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 I request messages and ICMP echo reply messages to be sent and received Windows computers and network devices.	
	Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:
	<ul> <li>operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li> </ul>
	• to send ICMP echo reply messages in response to an ICMP echo request
	Note: ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
	Windows Management Instrumentation (WMI) • Startup Type: Automatic
	Windows Update Service • Startup Type: Automatic
	Remote Registry  • Startup Type: Automatic
	Remote Procedure Call  • Startup Type: Automatic

Complete	Domain Configuration			
	Network Shares			
	• Admin\$ must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)			
	3rd Party Firewalls			
	Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist.     Note: This is a requirment for both Active Directory and Workgroup Networks.			

## Checklist for Workgroup Environments

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

1. reg add

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\syst
em /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-accountcontrol-and-remote-restrictions-in-windows

 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-wmiremotely-starting-with-vista

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

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

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

You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

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

Complete?	Workgroup Configuration			
	Enable the <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:			
	<ul> <li>operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li> </ul>			
	<ul> <li>to send ICMP echo reply messages in response to an ICMP echo request</li> </ul>			
	Note: ICMP requests are used to detect active Windows computers and network devices to scan.			

#### **RapidFireTools**\*

# 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:

## **Discovery Agent Firewall Requirements**

IT admins and end customers using RapidFire Tools products should configure the firewall rules on their networks to enable access to the following RapidFire Tools URLs.

- gatekeeper.rapidfiretools.com
- go.rapidfiretools.com
- au.rapidfiretools.com
- go-eu.rapidfiretools.com
- go-au.rapidfiretools.com
- · wcflb.rapidfiretools.com
- wcflb-eu.rapidfiretools.com
- wcflb-au.rapidfiretools.com
- api.ndglue.com
- networkdetective.s3.amazonaws.com
- download.rapidfiretools.com

The RapidFire Tools Server and Discovery Agent requires access to port 443.

## 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.

	-		
	O NDA:	Virtual	Cyber Hawk SDS
	O NDA:	Virtual	All
Reporters	O NDA:	Virtual	Compliance Manager
-	O EVS-	Virtual	Vulnerability Scan
	O NDA:	Virtual	Vulnerability Scan
Remote Data Collectors	PVS-	Virtual	Vulnerability Scan
	O NDA:	Virtual	Cyber Hawk SDS
	O NDA:	Server	All
	NDA:	Virtual	Inspector
ÁZ/	NDA:	Server	Cyber Hawk SDS
	NDA:	Server	Cyber Hawk SDS
Discovery Agents	NDA:	Physical	Inspector
	NDA:	Virtual	Inspector

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



- 4. 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.
- 5. 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.

Goodman Law					
Sites	All Site Types	Discover     Agents	y + Add Site		
Goodman Law	$\checkmark$				
<b></b>	0				

**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.

Filter Organizations	Legal Pros
<ul> <li>All Organizations</li> <li>All Sites</li> </ul>	Legal Pros / Discovery Agents Organization Discovery Agents
ABLE Manufacturing West Coast	
C Accent Fit	Install Key
Accent Fit - Guest Network	Conv
🗋 Acme Group	
Alpha Investments	Generate New Key
🗅 Beautiful British Columbia	Daily Scan
D Bell Systems	Sun Mon Tue Wed Thu Fri Sat
D Bobs Test Org	Ontion
🗋 Bullet Bus Company - Dayton	Option
Example Organization	
D Foresight Group	Deep File Scan
🗅 Goodman Law	Repeat Weekly
D Initiative Group	✓ Configure
🗅 Legal Pros	Apply
Discovery Agents	Scan Schedule can be applied after a Discovery Agent is installed
Micro Consulting	

# Step 2 — Install Discovery Agent(s)

Download the Discovery Agent from <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/ndpro-downloads/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/">https://www.rapidfiretools.com/ndpro-downloads/</a>. You can download the Agent installer from Data Collectors <a href="https://www.rapidfiretools.com/">https://www.rapidfiretools.com/</a>. You can download the Agent installer from Data Collectors <a href="https://ww

	PRODUCTS		
Network Detective Pro	Data Collectors		
Q Search downloads			
Network Detective Pro Discovery Agent			
More Info	<u>Download</u>		
The Network Detective Pro Discovery Agent installs as a Windows Service that collects information for individual computers (workstations or servers) on a schedule. The scan results are made			

- 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.

Discovery Agent Installer	x
Step 1: Enter Install Key	
Enter the Install Key for this Installation	
1c1b5355-5b78	
Enter a comment to help identify this computer (optional)	
Work laptop	
Enter a "label" to make it easier to select and use Discovery Agents (optional)	
Goodman Law	
Conti	nue
Priva	cy Policy 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.

٩	Discovery Agent In	istaller				×
	Step 2: You can go ba Install Key: Account Site Name: Comment Label:	Confirm Install ck again if the Install Key 1c1b5355 @D3M201103 Goodman Law Work Iaptop Goodman Law	I Key Deta	ails Back	Confirm	
					Privacy Policy	Terms of Service

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

•	Discove	ry Agent Ins	taller		×
		Step 3: In	stall		
		Registering Age	nt with your site		
		Site Key:	098e190b-a06e-4c9c		
		Account	PERF		
		Site Name:	AgentTesting		
		Comment	D		
		Agent ID:	<pre><pending></pending></pre>		
				Privacy Policy Terms of S	ervice

7. Click Finish when complete.

Q Discovery	Agent Ins	taller		x
S	Step 3: In	<b>stall</b> leted.		
S A S C A	Site Key: Account Site Name: Comment Agent ID:	098e190b PER AgentTesting AGT-49	Finish	
			Privacy Policy T	erms of Service

# 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.

Filter Organizations	Organization Discovery Agents
All Organizations	
All Sites	Install Key
ABLE Manufacturing West Coast	af3a4fff-d389-4559-8024- Copy Regenerate
C Accent Fit	
Accent Fit - Guest Network	C Daily Scan
Acme Group	Sun Di Mon Ki Tue Ki Wed Ki Thu Ki Fn Ki Sat Ki
Alpha Investments	Option
Beautiful British Columbia	Application Vulnerability Scan (Windows)
🗅 Bell Systems	O Deep File Scan
🗅 Bobs Test Org	Repeat Weekly
🗈 Bullet Bus Company - Dayton	- Configure
Example Organization	
C Foresight Group	Appy
🗅 Goodman Law	
D Initiative Group	Filter_
Legal Pros	
Micro Consulting	Comparer s cars scars unscovery agent to s comment a Ladel 5 Update status a Last Check-in 6
Micro Professionals	🗌 🕚 KA-PW 💷 19-Sep-2023, 10:18 AM AGT-32LCSZ MacOS MacOS Endpoint up-to-date 19-Sep-2023, 2:39 PM 🥒 📋
D Nacho Town USA	

# 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.

Home / Roles			
Roles			
Site Admin	+ Add User	Technician + Add User	
joe-admin-user@rapidfiretools.com	<b>D</b>	wgibson@microconsulting.com	
mc-admin@microconsulting.com			
fkafka@microconsulting.com	<b>D</b>		

 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 siterestricted Site Admin and Technician users can then manage Discovery Agents for their assigned organizations and sites.

	?	g joe-admin-user	K
		+ Add Us	er
✓ Require Two-Factor Authentication for All Accounts	🗹 Enable Dise	covery Agents for All Us	ers

## 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 Ap Deep F Repeat	n plication Vulnerability i <b>le Scan</b> Weekly	y Scan (Windows)		
Арр	ly		- Configure		
Filter					
	\$	Computer 🔶	Last Scan ≑	Discovery Agent ID $\updownarrow$	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	2 Items			

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

•	¢	Computer ≑	Last Scan ≑	Discovery Agent ID $\mbox{\ensuremath{}}$	Comment ≑	Label ≑
1 Select	ed	w	03-Feb-2023, 3:02 PM	AGT-37B	Work laptop	Goodman Law
Run Sc	an Now					
Update	e Now					
Cancel	Scans					
Remov	ve Agents	;				
Update	e Comme	nt				
Update	e Label 🧶	ŋ				

4. Enter your label and click Save.

8	Discovery Agents Label
	Add label for Discovery Agents. Goodman Law offsite
	Cancel
net i	Scan  Discovery Agent ID  Comment

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



## 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.

^	Goodman Law / Edt Ste Assessments   Reports   Export   Explore Data	
	Assessment-20230203	
	50% Complete 1 Complet	ject: <u>Select</u>
	Network Assessment (Domain) 50% Complete 1 Complete 1 Required 0 Optional Created 03-Feb-2023 03:12	PM Modifie
~	Run Network Collector (NDDC) with the Network Scan (2) Double-click items to open.	
	Run Network Detective Data Collector (NDDC) with the Network Scan Run the Network Data Collector on the Domain Controller (# possible), a computer joined to the Domain if the Domain Controller is not available workstation on the network. The data collector should be run with Administrative privileges.	e, or from any
V	Scans 🖉 Import Scan File 🚺 Initiate External Scan	
	Scan(s)         Expand Al         4 Files         03-Feb-2023         03:13 PM - 03-Feb-2023         03:13 PM	
	▲ Computer Scans 1 Files 03-Feb-2023 03:13 PM - 03-Feb-2023 03:13 PM	

- 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.

Q	Download File	5					-		×
	The following scar all available scans	is have been uploaded and a	are available for	download. Select all downloads you wish to import into	the current site and press Downlo	ad Selected or	press Download All to	o downloa	ıd
	Type AGT Connector	Device Name	Task ID	File Name	Date	Size	Label		
E	Connector	AGT Connector	N/A	KA-PW00PHAL-0C9A3C6E109A.zip	2/3/2023 8:02:38 PM	0.67 MB	Goodman Law		
Ŀ									
				Download All Download Selected	Delete Selected				

- 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.

## **Remove Discovery Agents**

To remove Discovery Agents:

- 1. Access the Organization Discovery Agent page and ensure that the Discovery Agent to be removed is online. You cannot remove an Organization Discovery Agent that is offline.
- 2. **Select the checkbox** on the left of the Discovery Agent Appliance ID that is to be removed.
- 3. Select the Remove Agents menu option.

	ation Witnesshifts	· Coop (Windows)							
Applica	Cases	y Scan (windows)							
Beneat Wer	ekty								
		- Configure							
		Conrigure							
_									
Apply									
er									
er									
er						t de la			
ter • • C	Computer ≑	Last Scan $\diamondsuit$	Discovery Agent ID 👙	Comment $\Rightarrow$		Label 💠	Update Status 💠	Last Check-in $\diamondsuit$	
er • c Selected	Computer 🗢	Last Scan 🗘	Discovery Agent ID 💠	Comment \$		Label 0	Update Status 🗘	Last Check-in 🗘	
er ♥	Computer 🗢 3-test-a	Last Scan ¢ 18-Oct-2023, 11:43 PM	Discovery Agent ID AGT-29GPKN	Comment ¢	Pizza Cafe Computer Endpoint	Label 🗘	Update Status 🗘 up-to-date	Last Check-in 0	PM 🖉 🕯
	Computer 🗢	Last Scan © 18-0et-2023, 11:43 PM	Discovery Agent ID AGT-29GPKN	Comment ¢ DCMA BU of Alfredos	Pizza Cafe Computer Endpoint	Label ¢	Update Status ¢ up-to-date	Last Check-in 19-Oct-2023, 3:09	PM 🖉 🗊
	Computer 🗢 3-test-a N-VMS	Last Scan © 18-Oct-2023, 11:43 PM NEVER	Discovery Agent ID AGT-29GPKN AGT-22HAZX	Comment © DCMA BU of Alfredos 10.200.1.80	Pizza Cafe Computer Endpoint	Label 🗘 APC Atlanta	Update Status up-to-date up-to-date	Last Check-in 19-0ct-2023, 3:09 15-Dec-2022, 3:28	PM Ø
	Computer 🗢 3-test-a UN-VMS	Last Scan 18-Oct-2023, 11:43 PM NEVER	Discovery Agent ID AGT-29GPKN AGT-22HAZX	Comment ¢ DCMA BU of Alfredos 10.200.1.80	Pizza Cafe Computer Endpoint	Label 🗘 APC Atlanta	Update Status up-to-date up-to-date	Last Check-in 19-0ct-2023, 3:09 15-Dec-2022, 3:28	PM 🖉 🕯 PM 🍵
er	Computer 🔶 >-test-a N-VMS	Last Scan © 18-Oct-2023, 11:43 PM NEVER	Discovery Agent ID AGT-29GPKN AGT-22HAZX	Comment © DCMA BU of Alfredos 10.200.1.80	Yizza Cafe Computer Endpoint	Label 🗘 APC Atlanta	Update Status up-to-date up-to-date	Last Check-in 19-Oct-2023, 3:09 15-Dec-2022, 3:28	PM 🖉 🗊 PM 🝵
	Computer 🔶 -test-a IN-VMS	Last Scan © 18-Oct-2023, 11:43 PM NEVER	Discovery Agent ID AGT-29GPKN AGT-22HAZX	Comment ¢ DCMA BU of Alfredos 10.200.1.80	Yizza Cafe Computer Endpoint	Label 🗘 APC Atlanta	Update Status up-to-date up-to-date	Last Check-in 19-0ct-2023, 3:09 15-Dec-2022, 3:28 ( 1 ) 25	PM PM
er  Celected  Selected  In Scan Now  date Now  innoel Scans  imove Agents  date Comment  edate Lond	Computer 🔶 Intestra IN-VMS	Last Scan © 18-Oct-2023, 11:43 PM NEVER	Discovery Agent ID AGT-29GPKN AGT-22HAZX	Comment © DCMA BU of Alfredos 10.200.1.80	Pizza Cafe Computer Endpoint	Label 🗘 APC Atlanta	Update Status up-to-date up-to-date	Last Check-in © 19-Oct-2023, 3.09 15-Dec-2022, 3.28 (1) > 25	PM PM

- 4. The Discovery Agent will be removed from the Organization Discovery Agent Page.
- 5. Finally, uninstall the Discovery Agent app from the computer endpoint.

You cannot remove an Organization Discovery Agent that is offline. You will receive the error message pictured below.

YourIT	Organizations To Do Global Settings		(?) Sindtest6
State     S	Outy Son     Son S Non S Tar S West B Tar     Organ     Organ     Organ     Organ     Organ     Organ     Organ     Organ      Organ	Remove Selected The following Discovery Agents cannot be remove. Either was for the Discovery Agents to compare compare AGT22042X	
	🖀 👻 🔿 Computer 🗢 Last Scan 🗘	Discovery Agent ID © Comment ©	Label 0 Update Status 0 Last Check-in 0
	<ul> <li>rft-dcma-test-a</li> <li>18-Oct-2023, 11:43 PM</li> </ul>		APC up to-date 19-0ct-2023, 3:09 PM 🥜 📋
	VULSCAN-VIMS NEVER		Atlanta up-to-date 15-Dec-2022, 3:28 PM 🝵

# 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, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.



2. Generate and copy the Install Key.

Bell Systems		
Bell Systems / Discovery Agents		
Organization Discovery Agents		
Install Key		
ebbb74a6-2b25-41f2-9b6a-4333	Сору	Regenerate
<ul> <li>Daily Scan</li> <li>Sun Mon Tue Wed Thu Fri Sat</li> <li>Option</li> <li>Application Vulnerability Scan (Windows)</li> <li>Deep File Scan</li> <li>Repeat Weekly</li> <li>Configure</li> </ul>		

- 3. Next, download the agent on the target endpoint. You can use this URL: https://download.rapidfiretools.com/download/DiscoveryAgent.msi
- 4. Save the agent installer in the same location where you will run the batch file.
- 5. Next, use the following two commands. Replace <your key> with the value for the Install Key that you copied earlier.

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.

## Find and Copy Install Key for Discovery Agents

In order to deploy the Agent with the scripts below, you will need the **Install Key** for the Discovery Agent.

1. First, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.



2. **Generate** and **copy** the Install Key. The exact Install Key should be inserted in place of the <install\_key> tag in the scripts below.



#### **RapidFireTools**<sup>®</sup>

## **Default Scripted Linux Install**

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

```
curl -0
https://download.rapidfiretools.com/download/discoveryagent-
install-linux.tar.gz
```

```
tar zxf 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 Re	equirements
Hardware	Less than 20 MB disk space
Software	<ul> <li>Linux Operating System that employs Systemd (system daemon) for service management. (Note that most modern Linux distributions employ this method by default.)</li> <li>YUM, APT, or ZIPPY installed for package management.</li> <li>.NET 6.0 Runtime The following software packages. (The app will install these packages if they are not already present.)</li> <li>o curl</li> <li>o unzip</li> </ul>
Other prereqs	Install Key for Discovery Agent.

## **Default Scripted OSX Install**

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

```
curl -0
https://download.rapidfiretools.com/download/discoveryagent-
install-osx.tar.gz
```

```
tar zxf 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 Re	equirements
Hardware	Less than 20 MB disk space
Software	<ul> <li>macOS 10.15 "Catalina" or higher</li> <li>.NET 6.0 Runtime</li> <li>The following software packages. (The app will install these packages if they are not already present.)</li> <li>o curl</li> <li>o unzip</li> </ul>
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
```

#### **RapidFireTools**<sup>®</sup>

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.

#### **RapidFireTools**\*

# 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 -0
https://download.rapidfiretools.com/download/computerscanner-
linux-x64.tar.gz
```

```
tar zxf computerscanner-linux-x64.tar.gz
```

./computerscanner

## **OSX ARM64 Collection**

```
curl -0
https://download.rapidfiretools.com/download/computerscanner-osx-
arm64.tar.gz
```

tar zxf computerscanner-osx-arm64.tar.gz

./computerscanner

System Requiremen	its
Hardware	20 MB disk space
Software	<ul> <li>macOS 10.15 "Catalina" or higher</li> <li>.NET 6.0 Runtime</li> <li>The following software packages.</li> <li>o curl</li> <li>o unzip</li> </ul>

## **OSX X64 Collection**

```
curl -0
https://download.rapidfiretools.com/download/computerscanner-osx-
x64.tar.gz
```

tar zxf computerscanner-osx-x64.tar.gz

#### ./computerscanner

System Requiremen	nts
Hardware	20 MB disk space
Software	<ul> <li>macOS 10.15 "Catalina" or higher</li> <li>.NET 6.0 Runtime</li> <li>The following software packages.</li> <li>o curl</li> <li>o unzip</li> </ul>

## **Optional Flags**

- Switch: -outbase <basename>
  - <sup>o</sup> 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 <u>"Step 2 — Customize Portal Branding" below</u>.
- 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 <u>Reporter</u> 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.

Micro Consulting		Organizations To Do	Global Settings	? 🕒 joe-admin-user 🔣
lo General		Global Settings / Branding	, , , , , , , , , , , , , , , , , , ,	
🖌 Branding		orona octango / branang		
Connections		Branding		
🗘 Admin Alerts		Thomas		
2 Users		(Click to Preview)		RydPitchak syname as O O /m D
Compliance Manager GRC	•	S Defect		
VulScan	•	Derault		
Service Plans	•	<ul> <li>Light</li> </ul>		Normality         Normality <t< td=""></t<>
Email Groups				Automotives and a second
Data Collectors				unter ■ Analari √ Analarito. ■ Analarito ■ 5 + 55 = 5 + 5 = 1
C IT Complete				
License Usage		Custom Branding		
		Company Name	ar	Company Logo
		Displayed in top left of menu b	di	opioau a logo to custornize your login page (JFG OFFRG, < THID IT Size).
		Micro Consulting		
				2022.12.07-0031

## Step 3 — Enable End-users Scans from RFT Portal

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

Micro Consulting		Organizations To Do Global Settings	?	🤰 joe-admin-user	ĸ
	+	Probable Partners			
Network Detective Pro	-				
Dashboard		Network Detective Pro / Data Collection / End-User Initiated Scan			
Data Collection	*	End-User Initiated Computer Scon			
End-User Initiated Scan		End-osei finitiated computer Scan			
Scan Data		Configure			
Data Explorer	Þ				
Settings	÷	End-User Initiated Computer Scans are performed by a downloadable application to scan computers where n is not possible.	emote s	canning via the LAN Sc	an
🛱 Audit Log		End-User Initiated Computer Scan Data Collector instructions are available here			
		A custom branded download page designed to be shared with end-users for local computer scans can be get $\cap{b}$	nerated	and managed below:	
		Click Generate to create a unique download page Generate	Delete	e Open Co	ру

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

Micro Consulting		Organizations To Do Global Settings 🧿 🧿 joe-admin-user 👔	
Home	÷	Probable Partners	
Network Detective Pro Dashboard	Ť	Network Detective Pro / Data Collection / End-User Initiated Scan	
Data Collection	*	End-User Initiated Computer Scan	
End-User Initiated Scan			
Scan Data		Configure	
Data Explorer	•		
Settings	•	End-User Initiated Computer Scans are performed by a downloadable application to scan computers where remote scanning via the LAN Scan is not possible.	
Audit Log		End-User Initiated Computer Scan Data Collector instructions are availablehere	
		A custom branded download page designed to be shared with end-users for local computer scans can be generated and managed below.	
		https://alerts.alert-central-staging.com/download/data-collector?ik=14b13a9ff99349 Regenerate Delete Open Copy	

## 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**.

End-User Initiated Computer Scanner	
(Windows)	
The End-User Initiated Computer Scanner is a Windows application that is	
run on individual computers (workstations or servers) to collect	
information for each system.	

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.

O,	Computer Scanner	x
	Dunning Computer Sconner	
	Getting computer local listening ports	
	L <sub>2</sub>	

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 <u>"Download End-user Scans" on the next page</u>.

### **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 <u>"Download End-user Scans" on the next page</u>.

#### **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**.

Туре	Device Name	Task ID	File Name	Date	Size	
Connector	Blue Bird	N/A	ndscan-39143938.ndf	12/2/2022 5:36:02 AM	0.23 MB	
Connector	Blue Bird	N/A	ndscan-39128031.ndf	12/1/2022 6:11:02 PM	1.70 MB	
Connector	Blue Bird	N/A	ndscan-39127958.ndf	12/1/2022 5:26:48 PM	1.71 MB	
Connector	Blue Bird	N/A	ndscan-39126247.ndf	12/1/2022 4:05:20 PM	1.68 MB	
Connector	Blue Bird	N/A	ndscan-39102772.ndf	12/1/2022 5:53:19 AM	0.23 MB	
Connector	Blue Bird	N/A	ndscan-39033163.ndf	11/30/2022 7:39:04 PM	0.22 MB	
Connector	Blue Bird	N/A	ndscan-38658941.ndf	11/17/2022 5:12:47 PM	0.22 MB	
Connector	Blue Bird	N/A	exchangescan-38685696.zip	11/18/2022 12:19:00 PM	0.04 MB	
Connector	Blue Bird	N/A	exchangescan-38596981.zip	11/16/2022 12:56:05 AM	0.04 MB	
Connector	Blue Bird	N/A	exchangescan-38557702.zip	11/14/2022 2:26:10 PM	0.04 MB	
Connector	Blue Bird	N/A	awscloudscan-39102702.zip	12/1/2022 5:23:16 AM	0.05 MB	
Connector	Blue Bird	N/A	WS-AHULIDA-01-7C70DB0B11AC.zip	12/6/2022 9:40:58 AM	0.51 MB	
Connector	Blue Bird	N/A	WAMPA-94C69126525E.zip	12/5/2022 5:05:21 PM	0.98 MB	
Connector	Blue Bird	N/A	KA-PW00PHAX-0C9A3C6DB9CE.zip	12/7/2022 1:02:21 AM	0.54 MB	
Connector	Blue Bird	N/A	DESKTOP-4A6JOB6-70CD0D81BEA6.zip	12/7/2022 11:30:54 AM	0.21 MB	
	Divo Dird	N/A	DESKTOP-4A6JOB6zip	12/7/2022 11:38:43 AM	0.17 MB	

## 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 <u>web version of this help topic here</u>.

# 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:

 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.



3. 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.

Filter Rename Change Type	Finish
us Project: Select	
01:12 PM Modified 13-Apr-2021 09:41 AM	
Commonly Used Report Sets:	
Reports	
Exchange Standard Repots  Standard Repot  Standard Repot  Standard Repot  Standard Repot  Standard Repot  Standard Repot  Standard Relation  Stand	Ĵ
Charge Reports     Baseline Exchange Management Plan (docx)     Baseline Exchange Risk Report (docx)     Baseline Exchange Health Report (docx)	

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

Assessments   Reports   Export   Explore Data			
Apr-2021 01:12 PM_Updated 13-Apr-2021 09:41 AM_Previous F	<sup>p</sup> roject: <u>Select</u>	Filter	Rename
te 🚺 Required 🔪 Optional Created 12-Apr-2021 01:	:12 PM Modified 13-Apr-202	1 09:41 AM	
Commonly Used Report Sets: 31 Available Reports 65 Unavailable Reports <u>Clear Selected Reports</u>		Select Select Prospecting and Selling Scoping and Sizing the Engagement	Apply
	Exchange	New Client Onboarding Monthly Technical Review Quarterly Business Review Management and Remediation	
Standard Reports	🖃 🗹 Standard Reports	Network Security Audit Exchange Migration	
Client Risk Report (.docx)	Exchange Risk R	SQL Server Health Check	
Network Management Plan (.docx)	Exchange Manag	ement Plan (.docx)	-
Full Detail Report (.docx)	Exchange Mailbo	x Detail Report (.docx)	
Excel Export (xlsx)	Exchange Mobile	Device Report (.docx)	
Windows Patch Assurance Report (.docx)	Exchange Traffic	and Use Report (.docx)	()
Windows Patch Assurance Change Report (.docx)	Exchange Shared	Mailbox Permission Report by Mailbox (.c	locx)

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.

	Scans Import Scan File	e initiate Ext	emal Scan
Scan(s)	Expand All	5 Files	01/12/2016 - 01/27/2016
<ul> <li>External</li> </ul>	l Vulnerability Scans	1 Files	01/12/2016 - 01/12/2016
<ul> <li>Network</li> </ul>	Scans	1 Files	01/27/2016 - 01/27/2016
<ul> <li>Security</li> </ul>	Scans	2 Files	01/27/2016 - 01/27/2016
<ul> <li>WiFi Sca</li> </ul>	ns	1 Files	01/27/2016 - 01/27/2016

3. Next click Generate Issue Exceptions.

V		InForm	Add Form (Choose Template)	(	Generate Issue Exceptions
	No Forms	Loaded			

#### **RapidFireTools**<sup>®</sup>
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.

Generating Issue Exception Worksheet	<b>E</b>
Please wait, risks are being identified for possible exclusion	

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.

		InForm	Add Form (Choose Template) Generate Issue Exceptions
1	Forms	Select Form to View / Edit	01/25/2016 - 01/25/2016

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

^		InForm Add Form (Choose Template) Generate Issue Exceptions Double click form name to open for editing.
	1 Forms	Select Form to View / Edit 01/25/2016 - 01/25/2016
	8	Issue Exception Worksheet Updated 01/25/2016 Viewed In Progress

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.



- 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...").

WinZip Self-Extractor - NetworkDetectiveData	Collector 🗙
To unzip all files in this self-extractor file to the specified folder presente Unzip button.	Unzip
Unzinte folder	Run <u>W</u> inZip
E:\ Browse	<u>C</u> lose
Verwrite files without prompting	About
When done unzipping open:	Help

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.

Q Preferences		-	×
Report Defaults Email Groups	Issue Overrides		
Text My Logo Theme Co	ver Images Company Information		
Report Prepared For:			
Report Prepared By:	Your Company Name.		
Footer:	PROPRIETARY & CONFIDENTIAL		
Cover Page Disclaimer:	CONFIDETINUTT NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, phyloged, and non-disclosable information. If you are not the client or addressee, you are sticity prohibited from reading, phylocopping, distributing, or otherwise using this report or its contents in any way.		
Target Language:	Engleh V		
Time Zone:	(UTC-05:00) Eastern Time (US & Canada) V		
Date Format:	MM/dd/yyyy v 01/06/2022		
Paper Size:	Letter (8.5"x11") ~		
Currency Symbol:	\$ ~		
Conversion Factor:	1.000000 🖨 x USD		
Reset to Global Preferences	]		
	Ok Cancel		

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

eport Defa	ults Reporter	Email Groups	Issue Overrides	Integrations							
The most c o Global Pi	ommonly detect references will a	ed issues are lis ffect all Sites ur	ted below. Unchec less overridden at f	k an issue to ignore the the Site level. Ignored i	e issue completely during report generation ssues will still appear in the Issue Exception	<ol> <li>Scores can be ov on Worksheet.</li> </ol>	emdden	with a numb	er bet	ween 1-100	. Changes
Reset all Se	everity, Probabil	ty, and Score								Select All	Unselect
Enabled	Module	-	Issue			Sev	erity	Probabilit	у	Score	
	BDR Assessme	nt	Critical servers not	t backed up		High		High		100	
	BDR Assessme	nt	Critical workstation	ns not backed up		High		High		95	
	BDR Assessme	nt	Insufficient networ	rk speed for offsite bac	kup	High		High		80	
$\checkmark$	BDR Assessme	nt	No successful bac	ckup was ever success	fully performed	High		High		100	
$\checkmark$	BDR Assessme	nt	On-Premises Exch	ange Server not backe	ed up	High		High		80	
	BDR Assessme	nt	On-Premises Exch	ange Server not backe	ed up successfully in 30 days	Med	ium	Medium		70	
$\checkmark$	BDR Assessme	nt	Recent backup fa	alures		High		High		90	
$\checkmark$	BDR Assessme	nt	Significantly aged	hardware		Med	Medium			70	
$\checkmark$	BDR Assessme	nt	SQL Server not be	SQL Server not backed up				High		75	
$\checkmark$	BDR Assessme	nt	SQL Server not ba	SQL Server not backed up successfully in 30 days				Medium		65	
$\checkmark$	Exchange Asse	ssment	Disabled Mailboxe	HS		High		High	-	100	
$\checkmark$	Exchange Asse	ssment	Empty Distribution	Lists		Low	•	Low	•	20	
$\checkmark$	Exchange Asse	ssment	Mailbox Size versu	us Quota (>50%)		High		Low	-	35	
$\checkmark$	Exchange Asse	ssment	Mailbox Size versu	us Quota (>75%)		High	•	Medium	•	65	
$\checkmark$	Exchange Asse	ssment	Mailbox Size versu	us Quota (>90%)		High		High	-	90	
$\checkmark$	Exchange Asse	ssment	Mailbox without Q	uota		Low	-	Low	-	20	
$\square$	Microsoft Cloud	Assessment	Admin Multi-factor	Authentication		High		High	-	90	
$\checkmark$	Microsoft Cloud	Assessment	Admin Role Overla	ар		High	•	High	•	90	
$\checkmark$	Microsoft Cloud	Assessment	Adobe Reader Fla	ish Content Rendering		High	•	High	*	90	
$\checkmark$	Microsoft Cloud	Assessment	Advanced Audit P	olicy Alert		High		High	-	90	
$\checkmark$	Microsoft Cloud	Assessment	Anonymous Acces	ss Restricted To Name	d Pipes	High	•	High	*	90	
$\checkmark$	Microsoft Cloud	Assessment	Authentication of	Remote Desktop Conn	ections	High	-	High	•	90	
$\checkmark$	Microsoft Cloud	Assessment	Azure ATP Senso	r		High	•	High	-	90	
	Microsoft Cloud	Assessment	BitLocker Addition	al Authentication		Hiat		Hiah	*	90	

- 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. These settings will change how Network Assessment displays these issues in their associated reports.
- 5. 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.

<b>Q</b> Preferences		-	×
leport Defaults Email Groups	Issue Overrides		
Text My Logo Theme Co	ver Images Company Information		
Report Prepared For:			
Report Prepared By:	Your Company Name.		
Footer:	PROPRIETARY & CONFIDENTIAL		
Cover Page Disclaimer:	COMEDENTAUTY NOTE: The exformation constanted in this report is for the socialise use of the client specified above and may contain confidential, pervinged, and non-discolable information. How 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 V		
Time Zone:	(UTC-05:00) Eastern Time (US & Canada) $\vee$		
Date Format:	MM/dd/yyyy v 01/06/2022		
Paper Size:	Letter (8.5"x11") ~		
Currency Symbol:	\$ ~		
Conversion Factor:	1.00000 🐳 x USD		
Reset to Global Preferences			
	Ok Cancel		

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

Q Prefere	ences						- 0	X L
Report Defa	aults Email Groups Issue Ov	errides						
The most of to Global F	commonly detected issues are lis references will affect all Sites u	sted below. Uncheck an issue to ignore the issue completely during report generation. Inless overridden at the Site level. Ignored issues will still appear in the Issue Exception	Scores can be overrido Worksheet.	den w	ith a numbe	er be	ween 1-100	. Changes
Revert to (	<u>Bobal Preferences</u> Reset all S	Severity, Probability, and Score					Select All	Unselect Al
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	٠	High	-	90	
	Exchange Assessment	Mailbox without Quota	Low	•	Low	•	20	
	Microsoft Cloud Assessment	Admin Multi-factor Authentication	High	•	High	-	90	
$\checkmark$	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	BtLocker Additional Authentication	High	-	Hiah	-	90	
M	Microsoft Cloud Assessment	BitLocker Additional Authentication Ok Cancel	Hiah	·	Hiah	•	90	

- 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**.

Rep Mo	ort Defaults Email Groups I	ssue Overrides	Sites unle	ss over	idden at	
the	Site level. Issue Overrides wo	k in conjunction with the Issue Exception Worksheet. Ignored issues will appear in the worksheet but will not affect the list of issues and	risks four	d.		
Re	vert to Global Preferences	<b></b>	Select	AII L	Inselect	All
	Module 4	sue			1	^
$\checkmark$	Network Assessment	Anti-spyware not installed				
$\checkmark$	Network Assessment	Anti-spyware not turned on				
$\checkmark$	Network Assessment	Anti-spyware not up to date				
$\checkmark$	Network Assessment	Anti-virus not installed				
$\checkmark$	Network Assessment	Anti-virus not turned on				
$\checkmark$	Network Assessment	Anti-virus not up to date				
$\checkmark$	Network Assessment	DHCP Errors				
$\checkmark$	Network Assessment	Excessive security patches missing on computers				
	Network Assessment	Few Security patches missing on computers.				
$\checkmark$	Network Assessment	Inactive computers				
$\checkmark$	Network Assessment	Insecure listening ports				
$\checkmark$	Network Assessment	Lack of redundant domain controller				
$\checkmark$	Network Assessment	Offine Domain Controller				
	Network Assessment	Operating system in Extended Support				
	Network Assessment	Potential disk space issue				
	Network Assessment	Potential password strength risks			_	
	Network Assessment	Severe Password Strength Fisks				
	Network Assessment	Significantly high number of Domain Administrators				
	Network Assessment	Too Few Organization Units				~

#### **RapidFireTools**<sup>®</sup>

## 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 Assessment's name to access the **Connector** setup option.

Customer A - Network Assessment
---------------------------------

V	Custom	er A 🚽	Edit Site				
	Applia	ances	Connectors	Remote Data Colle	ectors	Report Preferences	s
			$\nabla$				
	- <u>-</u>	Add Connecto	r 🕒 Add Mobi	le Connector			
	Remove Edit	Name	ID		Туре	Downloads Available	

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.

Add Connector	
Adding a connect the Client Connect particular Connect	or will allocate a new Connector ID. The Connector ID will be used in or command line to associate uploads with your account and to this or.
Connector ID:	6ff74c7c-
Connector Label:	
Connector Site:	Customer A - Network Assessment
	OK 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.

Example Site / Edit Site Assessments   Reports   Export   Explore Data
--

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

V	Example Site	/ Edit Site		A	ssessments	Reports	Export	Explore Data	
	Appliances	Connectors	Remote	Data Collectors	Rep	ort Preference	es		
	Click Add to bind a Network Detective Appliance to the site								
	Name	Туре	Manage	Update	Remove	Running Tas	sks		
		·	^	^	^	•			

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

Add Inspector	
Appliance ID: Site:	Customer A - Inspector Assessment
	OK Cancel

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.

V	Cu	stomer A	/ Edit Site				
		Appliances	Connectors	Remote	Data Collectors	Rep	ort Preferences
		$\nabla$					
		Click Add to bind a	Network Detective App	pliance to the sit	e 🕀 Add		
		Name	Туре	Manage	Update	Remove	Running Tasks
	0	INSP	Inspector	∿ Manage	🗲 Update	🗙 Remove	No queued tasks
		,		•	,	,	

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.

O Network Detective -	v4.0.1093					
Home InFo	m Appliances	s Connec	tor Service P	ans Users	Preferences	
	Provision Detecto	or				
	Appliance ID	Туре	Appliance Type	Site Name		
Appliances	O NDA1	Virtual	Reporter			
	O NDA1	Physical	Detector SDS			
( In	O NDA1	Virtual	Reporter			
	O NDA1	Virtual	Detector SDS			
All Appliances	INSP-	Physical	All			
	INSP-	Physical	Detector SDS			
	NDA1	Virtual	Detector SDS			
	INSP-	Physical	Inspector			
Detector	NDA1	Virtual	All			
Delectors	O NDA1	Virtual	Not Specified			
	O NDA1	Virtual	Reporter			
	O NDA1	Virtual	Detector SDS			
	O NDA1	Virtual	Detector SDS			
Inspectors	O NDA1	Virtual	Inspector			

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.   elimatador@example.com password: 12345************************************		
77	Enable account lockout for all users.	H	HE
72	Enable automatic screen lock on the specified computers.	MF	MF

#### **RapidFireTools**<sup>®</sup>

#### EXAMPLE:

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



**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.

Scall Type	an Type
Scan Options Verify and Run Collection Progress Finish	Select type of scan to perform Select one or more the collection process below to run. The amount of collectors to run will affect run-time. Network Data Collector
	Collect network-wide data using remote protocols. Required for Network Assessments.
	Collect data on the computer. Typically, used to augment data collection when remote protocols are not available from this computer.
2	<ul> <li>Security Data Collector</li> <li>Collect security data from the current computer perspective. Required for security Assesments.</li> <li>Perform Network Scan. Required for Share Permissions.</li> </ul>

- 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.

🕲 Network Detective Da	ta Collector - 2.0.1162	×
Scan Type	External Domains	
Active Directory	List avternal domains to be used for WHOIS_MY (mail) reserve detection, and Dark Web scores	_
Local Domains	List external domains to be used for writels, why (many record detection, and bark web scans.	
Additional Credentials		
External Domains	Domain	
IP Ranges	microsolutions.com	
SNMP Information		
VMware		
User Control Tests		
File Scanner		
Verify and Run		
Collection Progress		
Finish	Clear All Entries Import from Text File	
	Desfere Deal Web Case for Comparing Decayants	
	Perform Dark web scan for compromised Passwords	
		_
	(running on .NET CLR version 2.0.50727.9151) Back Next	
		-

5. Complete all steps in the wizard and perform the scan. Then upload the results into your assessment in Network Detective Pro. See <u>Performing a Security Assessment</u>

**RapidFireTools**<sup>\*</sup>

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 (<u>https://www.idagent.com/</u>) 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 <u>https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-I-enable-API-access-for-ID-Agent-</u>.

# 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.

	Users P	reference			-	
		0				
et Bus	Q Preferences					
cklist	Report Default	eporter	Email Group	s Issue Overrides	Integrations	
	Dark Web ID IT C	Glue				
essme	🗹 Enable Dark W	/eb ID Int	tegration			
Childe	Dark Web ID User	mame:	i	weakland		
orter essme	Dark Web ID Pass	sword:		•••••		]
cklist:	Test Connection					
o test essme						
cklist						

© 2023 RapidFire Tools, Inc. All rights reserved.

**RapidFireTools**\*

### 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 267.
- 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.

псу	rations						
API Keys	Networking API	Conne	ectWise	Autotas	k		
						Create	API Key
API Key	y Management						٩
Name 🔨	Contact Email 🗸	Product Family	Vendor 🗸	Client 🗸	Public Key	Last Update 🗸	
Micro Pro	micropro@pro.com	BCDR	Gradient	RFTTest	8570b1	2023-03-21 13:13:43	:
		BCDR			ca4011	2022-11-21 16:16:08	:
1						Showing 1 to 2 of	2 entries

3. Complete the fields for the API Key and click Create.

© 2023 RapidFire Tools, Inc. All rights reserved.

- 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.

Create API Key		
API Key Details		
API Key Name		
Optional		
Contact Email		
Optional		
Access Controls		
Select Vendor		~
Optional		
Select Client		~
Optional		
	Cancel	Create

4. Copy the **Public Key** and **Private Key** for use later.

API Keys		
Public Key		Сору
Private Key	Show	Сору
		ок
DCDD	Dookup Dodor 22007a	

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.

Q Preferences	5				
Report Defaults	Reporter	Email Groups	Issue Overrides	s Integrations	
Dark Web ID	IT Glue	atto Unified Cor	ntinuity	$\searrow$	
Enable Dat	to Unified C	Continuity Integra	ition		
Datto API Publ	ic Key:				
Datto API Secr	ret Key:				
Test Connecti	ion				

4. Enter the API credentials are click **Test Connection**. A success notification will appear.

Report Defaults       Reporter       Email Groups       Issue Overrides       Integrations         Dark Web ID       IT Glue       Datto Unified Continuity         Image: Superstand Structure       7b384a         Datto API Secret Key:       Image: Success in the second structure         Success       X         Connection to Datto Unified Continuity successful.       Image: Success in the second structure	Q Preferences					
Dark Web ID       IT Glue       Datto Unified Continuity         Image: Enable Datto Unified Continuity Integration       Image: Tob384a         Datto API Secret Key:       Image: Tob384a         Image: Test Connection       Image: Tob384a         Success       X         Connection to Datto Unified Continuity successful.       Image: Tob384a         Image: OK       Image: Tob384a	Report Defaults Reporter	Email Groups Issue	Overrides	Integrations		
Enable Datto Unified Continuity Integration   Datto API Public Key:   Datto API Secret Key:     Test Connection     Success   Connection to Datto Unified Continuity successful.     OK	Dark Web ID IT Glue Da	tto Unified Continuity				
Datto API Public Key:          Datto API Secret Key:       ••••••••••••••••••••••••••••••••••••	Enable Datto Unified Co	ntinuity Integration				
Datto API Secret Key: Test Connection Success Connection to Datto Unified Continuity successful. OK	Datto API Public Key:		7b384a			
Test Connection         Success         Connection to Datto Unified Continuity successful.         OK	Datto API Secret Key:		•••••	•••••	•••••	••••
Success × Connection to Datto Unified Continuity successful.	Test Connection					
Connection to Datto Unified Continuity successful.		Success			×	
ОК		Connection to D	atto Unifie	d Continuity	successful.	
					ОК	12

**RapidFireTools**<sup>\*</sup>

## 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 <u>"Step 2 — Enable Datto Unified Continuity Integration" on page 273</u>, 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**.

Reports Ready	Select Dat	to Organization	×
to retrieve d inuity Scan, use th	Organization: lata from you e "Datto Unified C	Amazing Inc. AMG Engineering AUS Avengers, Inc Berg Industries BipsNChitz Core Systems Canada Datto SIedesEngineering Datto SIedesEngineering Datto SIEdSLite Datto SIEdSLite Datto SIEdSLite Datto SIEdSLite	Refresh Checklist , Printed (
1 Files 03/2 1 Files 03/2	External Scan 22/2023 11:24 22/2023 11:24	Dunder Mifflin Paper Company EP Swag Co. FancyDC Fulton Technology Group Hoolio Jdryall Lab Knowhere IT Krick Labs MG Beverage Co.	tto Unified Continuity Scan
M		Motley Lue Moto Cafe	

3. You will receive a success notification when the scan completes.

Created 03/21/2023 11:15 AM Updated 03/21/2023 03:02 PM Previous Project:	<u>Select</u>	
e 1 Complete D Required 3 Optional Created 03/21/2023 11:15 AM	Modified 03/21/2023 03:02 PM	
Run a Datio Unified Continuity Scan to retrieve data from your Datt		
puters that cannot be scanned remotely motely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible	Datto Unified Continuity Scan 🛛 🗙	
n.	Scan complete.	
Initiate External Scan Download Scans 💦 R	ОК	ed Continuity Scan
1 Files 03/21/2023 03:02 PM - 03/21/2023 03:02 PM		
1 Files 03/21/2023 03:02 PM - 03/21/2023 03:02 PM		

## 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 SL	JMMARY					
		Total \$1	Potential Lial	bility		
	Computer	IP Address	Missing Critical Patches	Anti-virus/ Anti- spyware	Sensitive Data Count	Potential Liability (\$)
8	corp.myco.com/darkhorse	169.254.24.1 50 169.254.58.2 36 192.168.6.80	0	4	623	\$125,223
8	corp.myco.com/DC03	169.254.52.1 50 192.168.1.23 192.168.1.4 192.168.1.3	0	~	119	\$23,919

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

- Visa card
- Mastercard
- Discover Card
- Diners Club United States & Canada
- Mastercard Diners Club Alliance

- American Express
- Date of Birth
- SSN
- Drivers License
- ACH (bank transfer information)

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

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

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

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

RetworkDetective Push Deploy Tool	v2.0.1128				
<ul> <li>Settings and Configuration</li> </ul>	Settings and	Configuration			
Computers and Status	Scan Settings				
0 H + 10 + 51	Storage Folder:	C:\Users	Network Dete	ectivePushDeployTool	
Collected Data Files	Scan Type:	Computer Scan	Security Scan	Deep Scan Option:	Include the scanning of PDF Files
		HIPAA Quick	HIPAA Deep		
		PCI Quick	PCI Deep		
		BDR Scan	Pll Scan		

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

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



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

	•
Reports Create Reports	
Active Assessment - Ready to Generate V 51% Available	77 Available Repo
Standard Reports         Security Risk Report (.docx)         Security Management Plan (.docx)         Outbound Security Report (.docx)         Share Permission Report (.docx)         Share Permission Report by User (.docx)         Share Permission Report by User Excel (.xlsx)         Share Permission Report by User Excel (.xlsx)         External Vulnerability Scan Detail Report (.docx)         External Vulnerability Scan Detail Beport (.docx)         External Vulnerability Scan Detail Excel (.xlsx)         External Vulnerability Scan Detail Excel (.xlsx)         Login Failures by Computer Report (.docx)         Login Failures by Computer Report (.docx)         Login History by Computer Report (.docx)         Manomalous 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 (.docx)         Data Breach Liability Report Card Excel (.xlsx)	

# **Completing Worksheets and Surveys**

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

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

Assessment response data is collected through:

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

#### Entering Assessment Responses into Surveys and Worksheets

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

#### EXAMPLE:

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

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



- ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.
- iii. Enter the *Response*. There are three types of responses:

#### **RapidFireTools**<sup>®</sup>

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."			
complete the all of the surveys within the Network Assessment process.					
		etwork Assessment process.			
. (Optional) Ente	r any <i>Notes</i> relevant to the top r the name of <i>Respondent</i> (i.e	ic's response.			
<ul> <li>(Optional) Enter</li> <li>(Optional) Enter</li> <li>with the information</li> </ul>	r any <i>Notes</i> relevant to the top r the name of <i>Respondent</i> (i.e ation, if applicable).	ic's response. . the person who provided you			
<ul> <li>(Optional) Enter</li> <li>(Optional) Enter</li> <li>with the information of the informa</li></ul>	r any <i>Notes</i> relevant to the top r the name of <i>Respondent</i> (i.e ation, if applicable). any relevant <i>Attachments</i> . Se <u>orksheets" below</u> for more det	ic's response. . the person who provided you e <u>"Add Image Attachments to</u> rails.			
<ul> <li>(Optional) Ente</li> <li>(Optional) Ente</li> <li>with the information (Optional) Add a</li> <li>Surveys and Ward</li> <li>Note: Only improved the information of the informat</li></ul>	r any <i>Notes</i> relevant to the top r the name of <i>Respondent</i> (i.e ation, if applicable). any relevant <i>Attachments</i> . Se <u>orksheets" below</u> for more del nage attachments (.png, .jpg) a	ic's response. . the person who provided you e <u>"Add Image Attachments to</u> rails. are supported at this time.			

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.	
10	
Vendor - ePHI authorization	0 8 🖾 🎟

- 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 Admini Name: Admin No	strator istrator Enabled: enabled La:	st Login: 10/5/2017 1:27:30 PM Job Title: Departmer	nt: Company: Detected Service Account:	
Vendor - e SWOTS:	PHI authorization		~	DA 📁 📰
	SWOT	Bullet Point	Key Point	
×	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**.

Bulk Entry 🔻	Actions 🔻	Save	Close	
horization to access el	Create Wor Import Word	d Respons I Respons	se Form se Form	se
	Generate R	esponse F	Report	ŀ
	Generate IT	SWOT R	eport	
ay also be users who uthorized to access ef	are on contract of PHI. You must in	or nave reia dicate a res	tionsnips ponse for	

**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.

User Identification Worksheet			
0 Required Remaining	Hide # Filter Topics	🔻 🗙 Bulk Entry 🕁 Actions 🕶	Save Close
	Filter	Bulk Entry	
	Key Words 🔻 🗙	Select topics of same response type	
	Select All Filtered Deselect All Filtered	Note	
		Respondent	Apply to Selected

Check boxes will appear next to the response topics.

	et				
quired Remaining	▲ ▼ Hide #	Filter Topics	<b>▼</b> ×	Bulk Entry 🔺 Actions	▼ Save Close
	Filter		Bulk Entry		
	Key Words	<b>Y X</b>	Select topics of same res	ponse type	
	Select All Filtered	Deselect All Filtered	Note		
		N	Respondent		Apply to Selected
ategory Previou	us 1 2 Next	L∂			
∧□ 1	a falanana" -	(2 Required F	Remaining)		
1.1 adminor	niv				
Select user type an	nd access level				
				× [	8 🕫 🎟
Notes:				~	2 🕫 🖩
Notes: Name: admin o	only			<b>~</b>	2 10 11
Notes: Name: admin o Enabled: enabl	only led			~	8 🗗 🖼
Notes: Name: admin o Enabled: enabl Last Login: 7/2	nly led /2014 8:26:48 AM				8 🗇 🖩
Notes: Name: admin o Enabled: enabl Last Login: 7/2 Job Title:	only led I/2014 8:26:48 AM			~ [	
Notes: Name: admin o Enabled: enabl Last Login: 7/2 Job Title:	nly led I2/014 8:26:48 AM			· [	8 🗂 🖩
Notes: Name: admin d Enabled: enabl Last Login: 7/2 Job Title:	only led /2014 8:26:48 AM				A 🗗 🖩
Notes: Name: admin d Enabled: enable Last Login: 7/2 Job Title: Dutte: Dutte: Select user type an	only led IZO14 8.26-48 AM strator nd access level.			~ [	8 🗇 🖩
Notes: Name: admin of Enabled: enable Last Login: 7/2 Job Title: Job Title: Select user type an	unhy led (2014 8.26.48 AM strator d access level.				
Notes: Name: admin c Enabled: enabl Last Login: 7/2 Job Title: Select user type an	unity led 1/2014 8:26:48 AM strator d access level.			· [	
Notes: Name: admin c Enabled: enable Last Login: 7(2) Job The: C Last Login: 7(2) Last Logi	nhy ed (22014 8:26.48 AM strator d access level.				A 12 III
Notes: Name: admin o Enabled: enable Last Login: 7/2 Job Tille: De Tille: Select user type an Select user type an Notes: Name: Adminis	only led izota 8.26.48.AM strator istrator				A 17 III
Notes: Name: admin of Enabled: enable Last Login: 7/2 Job Title: Notes: Name: Adminis Enabled: Enabled: Enabled:	inhy edd 14 8:26.48 AM strator id access level.				
Notes: Name: admin o Enabled: enable Last Login: 7/2 Job Tille: De Tille: Select user type an Select user type an Notes: Name: Adminis Enabled: enable	only led 2/2014 8:26:48 AM strator di access level. :trator led itrator				
Notes: Name: admin t EasLogin: 7/2 Job Title: Notes: Nate: Notes: Nate: Adminis Eanabied: enabl Last Login: 9/2 Job Title:	Inly ed ad strator d access level.				A 17 III

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

#### **RapidFireTools**\*

	Hide #	Filter Topics	<b>T X</b>	Bulk Entry Actions	Save Close
	Filter		Bulk Entry		
	Key Words	<b>T</b> ×		~	
	Select All Filtered De	select All Filtered	Note		
			Respondent	A	oply to Selected
Previou	is 1 2 Next				
<b>2</b> 1	a fatoranati sa	(2 Required Re	emaining)		
Notes: Name: admin on Enabled: enable Last Login: 7/2/ Job Title:	nly ad access level. nly ad 2014 8:26:48 AM			<ul> <li></li> <li></li> <li></li> </ul>	S 🗂 🖩
✓ 1.2 Adminis	trator d access level.				0 🖂 💵
Select user type an					
Select user type an Notes:					

**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.

	Filter	_					
egory Previous	Key Words Select All Filtered E	T     X       Deselect All Filtered     X	Employee - no CDE access Employee - CDE access Employee - CDE access Vendor - CDE access Vendor - CDE access Vendor - CDE access Vendor - CDE access Former Employee Former Fundor Service Account Genetic Account	ß	Apply	r to Selected	
✓ 1	a fatoreau a constante a co	(3 Required Ren	naining)				
Notes: Name: admin on Enabled: enable Last Login: 7/2/2 Job Title:	ly d 1014 8:26:48 AM			<b>&gt;</b>			
Notes: Name: admin on Enabled: enable Last Login: 7/2/2 Job Title: Select user type and	ly d 014 8:26:48 AM rator access level.			<b>&gt;</b>			
Notes: Name: admin on Enabled: enable Last Login: 7/2/2 Job Title: Select user type and	ily d 1014 8:26:48 AM rator access level.			· ·			# **
Notes: Name: admin or Enabled: enable Last Login: 7/2/2 Job Title: Select user type and Notes:	ily 014 8-26-48 AM rator access level.						

4. Then click Apply to Selected.

ired Remaining	▲ ▼ Hide #	Filter Topics	▼ X Bulk Entry ▲ Actions ▼ Save Clos	e
	Filter		Bulk Entry	_
	Key Words	<b>▼ ×</b>	Select topics of same response type	
	Select All Filtered	Deselect All Filtered	Note	
			Respondent Apply to Selected	
egory Previous	1 2 Next			
🗆 🗸 1	And an article of the	-		
1.1 adminonly     Select user time and	/			
Select user type and	000033 10401.			
Vendor - no CDE	access		► S D III	
Notes:				
Name: admin onl	у			
Enabled: enabled				
Last Login: 7/2/20	014 8:26:48 AM			
Job Title:			*	
1.2 Administr	ator			
Select user type and	access level.			
Vendor - no CDE	access		A C III     A	
Notes:				
Name: Administra	ator			
Enabled: enabled			^	
Last Login: 9/27/2	2017 12:57:35 PM			
Job Title:			$\checkmark$	
Description				

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 <u>"Important Note on Working with Word</u> <u>Response Forms" on the next page</u> 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.

Word response form created

### Important Note on Working with Word Response Forms

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

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

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

### Multiple choice response field



Text response field



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

### Import Word Response Form

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

EXAMPLE:
Step 1: Create/export a Word response form for one of the worksheets in your assessment.
Step 2: Send it to a client to enter additional information about the site using Word.
Step 3: The client can then send you the worksheet as an email attachment.
<i>Step 4:</i> 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.

<b>▼</b> ×	Bulk Entry 🔺	Actions 🔻	Save	Close	
	Create Word Response Form				
s of same respor	ise type	Import Wo	ord Respons	e Form	

4. Select the file to import. Click Open.

### **RapidFireTools**<sup>®</sup>

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

Vord response form imported

## **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.

Thi	s PC	→ Local Disk (C:) →	Users > >	AppData > Roaming	<ul> <li>NetworkDetective</li> </ul>	
	Na	ame		Date modified	Туре	Size Default data
		ExternalScans		1/24/2018 1:15 PM	File folder	
<i>"</i>		il8n		1/24/2018 1:15 PM	File folder	directory
×		Interviews		1/25/2018 9:55 AM	File folder	
*		Reports		1/24/2018 1:15 PM	File folder	
*		ReportStyles		1/24/2018 1:15 PM	File folder	Backup and conv
		Scans		1/24/2018 1:15 PM	File folder	Buckup und copy
		Sites		1/24/2018 1:16 PM	File folder	contents of sub-
		acceptSLA		1/24/2018 1:15 PM	Text Document	1 KB
		acceptTOU		1/24/2018 1:15 PM	Text Document	1 KB TOIGETS
		cache		2/13/2018 10:00 AM	Text Document	11 KB
		datadirectories		1/24/2018 4:01 PM	Text Document	0 KB
		hidetips		1/24/2018 1:15 PM	File	1 KB
		flogin		2/13/2018 10:00 AM	Text Document	1 KB
		startup.cfg		2/6/2018 10:24 AM	CFG File	1 KB
	_	] Tips		1/24/2018 1:15 PM	XML Document	1 KB

### **RapidFireTools**<sup>®</sup>

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.

> This	PC > Local Disk (C:) > Users > >	AppData > Roaming	NetworkDetective	<ul> <li>Sites</li> </ul>	
	Name	Date modified	Туре	Size	
* *	Customer 1 Test.dat	2/13/2018 10:20 AM 2/13/2018 10:25 AM 2/13/2018 10:26 AM	DAT File DAT File DAT File	2 KB 2 KB 1 KB	
Copy contents of sub-folders					
into new Data Directory					

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
Autotask	Note: To set up a connection between the Network Detective application and the Autotask system, you will need to create an API User in Autotask. See <u>"Set Up Autotask</u> Integration" on page 308.
	Autotask API Password
REST CONNEC-+Wise <sup>™</sup>	<ul> <li>ConnectWise REST Public Key</li> <li>ConnectWise REST Private Key</li> <li>ConnectWise Company ID</li> <li>ConnectWise PSA URL</li> </ul>

PSA System	PSA Prerequisites
	Note: You must configure ConnectWise correctly before you can integrate with Network Detective Pro. See <u>"Set Up</u> <u>ConnectWise REST Integration" on</u> <u>page 313</u> for detailed instructions.
SOAP Connec+Wise	<ul> <li>ConnectWise Username</li> <li>ConnectWise Password</li> <li>ConnectWise Company ID</li> <li>ConnectWise PSA URL</li> </ul>
	Note: You must configure ConnectWise correctly before you can integrate with Network Detective Pro. See <u>"Set Up</u> <u>ConnectWise SOAP Integration" on</u> <u>page 322</u> for detailed instructions.
Tigerpaw	<ul> <li>Tigerpaw Username</li> <li>Tigerpaw Password</li> <li>Tigerpaw API URL</li> </ul>
BASS by Kaseya	<ul> <li>Kaseya Username</li> <li>Kaseya Password</li> <li>Note: The Kaseya User must be in the Kaseya Administrator Role. See for <u>"Set Up Kaseya BMS Integration" on</u> page 324 detailed instructions.</li> <li>Kaseya Tenant (i.e. company name)</li> <li>Kaseya API URL, example: "https://bms.kaseya.com" (you</li> </ul>

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 <u>https://www.rapidfiretools.com/ndpro-</u>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.

Mappings		Jelect items to Export
Kaseya Connection:	Manage Connections	Automatic screen lo Login auditing is rec No external firewall While not inherently
Export to Account:	×	
Account Location:	~	

The Connections Manager window will be displayed.

Connections Manager	_		$\times$
Connections Manager Manage Multiple Accounts			
Saved Connections	_		
		New	
		Modify	r
		Remov	e
		Select /	Ali
Close			.:1

8. Select the **New** button in the Connections Manager window to create a new PSA connection.

Kaseya Credentials	×
Kaseya Usemame: Kaseya Password: Kaseya Tenant: Kaseya API URL:	
	OK Cancel

The PSA Credentials window will be displayed

9. Enter the credentials for chosen PSA.

**Important:** To generate login credentials for ConnectWise REST, see <u>"Set Up</u> <u>ConnectWise REST Integration" on page 313</u>. To generate login credentials for ConnectWise SOAP, see <u>"Set Up ConnectWise SOAP Integration" on</u> <u>page 322</u>.

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.

<b>Q</b> Export Issues and Recomm	nendations To Kaseya		
Automatically creates Tickets in	Kaseya based on issues and reco	mmendations in a F	lisk Report
Mappings Kaseya Connection:	customer1 customer2	~	Select Items to Export  Automatic screen lock p  Login auditing is required No external firewall was i  While not inherently a ris
Export to Account:		$\sim$	

**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:

- <u>"Export Configuration Items from Network Detective Pro to PSA" below</u>
- <u>"Export Exchange Contacts from Network Detective Pro to PSA" on page 305</u>
- <u>"Create Tickets from Assessment Issues and Recommendations from</u> Network Detective Pro to PSA" on page 305

## 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.

Export To Kaseya	-		×
Automatically creates Assets in Kaseya based on information from Network Detective.			
Select Items to Export			
Mappings Select Active Select Inactive	Select All	Unselec	t All
Kaseya Connection: Computer] WIN10-10 Manage Connections Manage Connections (Computer) WIN10-3 fe80::tbc61761fre6#c88a%	3,10.200.1.5 3,10.200.1.2	5) 26)	^
Computer WIN71 fe80:730cccec.442a.3e37     Export to Account:     Computer WIN72 fe80:730cccec.442a.3e37     Computer WIN81-fe80:81b4.19ea.3582.dee0     Computer WIN81-fe80:81b4.19ea.3582.dee0     Computer WIN81-fe80:82b5.20ec.39b4.de157     Computer WIN81-fe80:82b5.20ec.39b4.de157	10,10.200.1 10,10.200.1 %3,10.200.1 3,10.200.1.4 %3.10.200.1.	.46) .45) .40) .1) 22)	
Hardware Settings Hardware Settings Map Computers Map Comp	43,10.200.1	.20)	
Map Servers:			
Map Printers:			
Map Non-A/D Devices: [ [Non-A/D] 10 2001.13 /( 10.2001.3)			
Software Settings         [Non-A/D] 10.200.143 (10.200.143)           Map SQL Server:         [Non-A/D] 10.200.147 (10.200.147)			
Map Exchange Server: [ [Non-A/O] 10.200.15 (10.200.15) [Non-A/O] 10.200.151 (10.200.151) [Non-A/O] 10.200.152 (10.200.152) [Non-A/O] 10.200.156 (10.200.156)			
Inon-Avg InHMD1 (1020121)     Iserver APP01 (1680)::063;acb3:7827/91cV3.10     Iserver APP01 (1680)::063;acb3:7827/91cV3.10     Iserver AP01 (1680)::063;acb3:7827/91cV3.10     Iserver DC01 (680)::b177/bd8:9508;a4c1%8,102     Iserver DC02 (fe80)::c96c:a51cf3fc:4348%5,102	.200.1.12) 00.1.10) 00.1.11)		~
Export Close			

**Important:** If you have not yet created a connection, see <u>"Integrate</u> <u>Network Detective Pro with a PSA System" on page 294</u> 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.

💽 Export To Kase	eya							-		×
Automatically crea	ates Assets	s in Kaseya based on information from 1	Network Detective							
Mappings				Select Item	s to Export	t Active	Select Inactive	Select All	Unsele	ect All
Kaseya Connect	tion:	mwinter Manage	~ Connections	Compu Compu Compu	ter] WIN10-1 () ter] WIN10-2 (fe ter] WIN10-3 (fe ter] WIN7-1 (fe8	80::1ce:9 80::bc61 30::7d0c:c	1992:7e62:d50f% 761f:e64f:c86a% :cec:4d2a:3e37%	3,10.200.1.5 3,10.200.1. 10,10.200.1	55) 26) I.46)	Î
Export to Account	unt:		~	Compu	ter] WIN 7-2 (fe8 ter] WIN 81-1 (fe	30::c169:8 e80::81b4	b53:808a:79ed% 19ea:3582:dee0	10,10.200.1%3,10.200.1	1.45) 1.40)	
Account Locatio	on:		~	Compu	ter] WIN81-2 (fe ter] WIN81-3 (fe ter] WIN81-4 (fe	80::bcf9: 80::8d5a	588:647c:5c54% 206c:3fb4:dc15% dc07:8a52:855d	3,10.200.1.4 \$3,10.200.1 \$3,10.200.1	11) .22) 1.20)	
Hardware Set	ttings			Exchar	nge Server] EXC	CH01 (unk	nown)			
Map Computers:		Laptop	~	Non-A	/D] 10.200.1.1 ( /D] 10.200.1.2 (	10.200.1. 10.200.1.	1) 2)			
Map Servers:		Server	~	Non-A	/D] 10.200.1.27 /D] 10.200.1.3 (	(10.200.1	.27) 3)			
Map Printers:		Printer	~	[Non-A	/D] 10.200.1.32	(10.200.1	.32)			
Map Non-A/D D	Devices:	[-DO NOT EXPORT]	~	[Non-A [Non-A [Non-A	/D] 10.200.1.3/ /D] 10.200.1.4 ( /D] 10.200.1.42	(10.200.1 10.200.1 (10.200.1	.37) 4) .42)			
Software Sett	<u>tings</u>			[Non-A	/D] 10.200.1.43 /D] 10.200.1.44 /D] 10.200.1.47	(10.200.1	.43) .44)			
Map SQL Server	er:	[-DO NOT EXPORT]	$\sim$	Non-A	/D] 10.200.1.48	(10.200.1	.47)			
Map Exchange	Server:	[-DO NOT EXPORT-]	~	[Non-A	/D] 10.200.1.5 ( /D] 10.200.1.51	10.200.1. (10.200.1	5) .51)			
				[Non-A	/D] 10.200.1.52 /D] 10.200.1.56	(10.200.1 (10.200.1	.52) .56)			
Create New	Configura	tion Items		[Non-A	/D] REHVD I (10 1 APP01 ffe80c	0.200.1.2 •0a5:ach?	1) 1·7a27f91c%3 10	200 1 12)		
Update Exist	sting Reco	rds with Same Reference Title		Server	] DC01 (fe80::b1 ] DC02 (fe80::c9	177:bd8:9 bc:a51c1	508:a4c1%8,10.2 8fc:43d8%5.10.2	00.1.10)		<b>~</b>
			Export	Close						

**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.

Select Items to Ex	port			
	Select Active	Select Inactive	Select All	Unselect All
Computer] WI	N10-1 ()			~
Computer] WI	N10-2 (fe80::1ce:	9992:7e62:d50f%3	3,10.200.1.5	5)
Computer] WI	N10-3 (fe80::bc61	:761f:e64f:c86a%	3,10.200.1.2	26)
Computer] WI	N7-1 (fe80::7d0c:c	cec:4d2a:3e37%	10,10.200.1	.46)
Computer] WI	N7-2 (fe80::c169:8	3b53:808a:79ed%	10,10.200.1	.45)
Computer] WI	N81-1 (fe80::81b4	:19ea:3582:dee0%	%3,10.200.1	.40)
Computer] W	N81-2 (fe80::bcf9:	588:647c:5c54%3	3,10.200.1.4	1)
Computer] W	N81-3 (fe80::8d5a	:206c:3fb4:dc15%	3,10.200.1.	22)
Computer] WI	N81x34 (fe80::6db8	:dc07:8a52:855d*	%3,10.200.1	.20)
Exchange Se	rver] EXCH01 (unk	(nown)		
[Non-A/D] 10.	200.1.1 (10.200.1.	1)		
[Non-A/D] 10.	200.1.2 (10.200.1.	2)		

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.

2	Export To	o Tigerpaw 🚽 🗖 💌
Automatically creates Asse	ts in Tigerpaw based on information from Network Detec	tive.
		Select Items to Export
Mappings		Select Active Select Inactive Select All Unselect All
Tigerpaw Connection:	Manage Connections	[Computer] IRB11D1 0     [Computer] AGENT003-PC 0     [Computer] Ben 0     [Computer] Ben 0     [Computer] Ben 0
Export to Account:	select account V	Computer) BKRICKEY-WIN7 (10.0.7.74) (Computer) CLOVEPOWER ()
Source Product	Network Detective V	Computer) CONFERENCE1 ()
Hardware Settings		Computer] CDNFERENCERUDM () Computer] CDSTEN-SG (10.0.7.24) Computer] D520-5P9W0C1 ()
Map Computers:	[-DO NOT EXPORT]	Computer] D620-8BCJVD1 ()
Map Servers:	[-DO NOT EXPORT] V	Computer DAVIS XP (10.0.7.10)
Map Printers:	[-DO NOT EXPORT]	Computer] DELL120720 (10.0.7.78)
Map Non-A/D Devices:	[-DO NOT EXPORT] V	Computer] DEDNNE () Computer] DHARDLD-PC (10.0.7.1)
Software Settings		Computer] Dwilliams2 () Computer] EHAMMOND-WIN7 ()
Map SQL Server:	[-DO NOT EXPORT-]	Computer] EPTOWER ()
Map Exchange Server:	[-DO NOT EXPORT-]	[Computer] ERPI-MYCD-01 [)     [Computer] FT-LENOV0 [10.0.7.21]     [Computer] FTDELLAPTOP [10.0.1.109]     [Computer] FTDELSKTOPWORK [)
✓ Create New Configur Update Existing Rec	ation Items ords with Same Reference Title	□ (Computer) GHAMMOND-LT (10.0.7.15)           □ (Computer) HoteHVMIN764 (10.0.1.215)           □ (Computer) HoteHVMIN764 (10.0.7.56)           □ (Computer) HOTEHVMI764 (10.0.7.53)
	Export	Close

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.

🔍 Export To IT Glue	_		×
Creates a CSV/file which can be imported to IT Glue			
cleates a CSV file which can be imported to 11 Gide.			
Select Items to Export			
Select Active Select Inactive S	Select All	Unsele	<u>± Al</u>
Computer] WIN10-1 () [Computer] WIN10-2 (fe80::1ce:9992:7e62:d50f%3.1	0.200.1.5	5)	^
[Computer] WIN10-3 (fe80::bc61:761f:e64f:c86a%3,	10.200.1.2	26)	
[Computer] WIN7-1 (#e80::7d0c:ccec:4d2a:3e37%10	,10.200.1	.46)	
[Computer] WIN/-2 (te80::c169:8b53:808a:/9ed%10 [Computer] WINP1 1 (fe90::P1b4:19ea:2592:dea0%2	10.200.1	.45)	
[Computer] WIN81-1 (e606104.1564.5562.0660.5	0.200.1.4	.40)	
[Computer] WIN81-3 (fe80::8d5a:206c:3fb4:dc15%3)	10.200.1	22)	
[Computer] WIN81-4 (fe80::6db8:dc07:8a52:855d%3	,10.200.1	.20)	
Exchange Server] EXCH01 (unknown)			
[Non-A/D] 10.200.1.1 (10.200.1.1)			
[Non-A/D] 10.200.1.27 (10.200.1.27)			
[Non-A/D] 10.200.1.3 (10.200.1.3)			
[Non-A/D] 10.200.1.32 (10.200.1.32)			
[Non-A/D] 10.200.1.37 (10.200.1.37)			
[Non-A/D] 10.200.1.4 (10.200.1.4) [Non-A/D] 10.200.1.42 (10.200.1.42)			
[Non-A/D] 10.200.1.43 (10.200.1.43)			
[Non-A/D] 10.200.1.44 (10.200.1.44)			
[Non-A/D] 10.200.1.47 (10.200.1.47)			
[Non-A/D] 10.200.1.48 (10.200.1.48)			
[Non-A/D] 10.200.1.5 (10.200.1.5)			
[Non-A/D] 10.200.1.52 (10.200.1.51)			
[Non-A/D] 10.200.1.56 (10.200.1.56)			
[Non-A/D] RFHVDT (10.200.1.21)			
[Server] APP01 (fe80::c0a5:acb3:7a27f91c%3,10.20	00.1.12)		
[] [Server] DC01 (results 177:bd8:9508:a4c1%8,10.200	. 1. 10)		*
Export Close			

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.

	Select Items to Export
appings	Select All Unselect A
ConnectWise Connection:	Computers were found with significantly low free disk space.     Arti-spyware software was not detected on some computers. Without addet     Arti-spyware software was not detected on some computers. Without addet     Computers are to be using potentially insecure protocols.     Computers are to be using potentially insecure protocols.     Computers found using an operating system that is in Edended Supported. Ex     Computers found using an operating system that is not endered with the endered on some computers.     Computers found using an operating system that is not endered supported. U     Computers have unable complexity limits the bally of an attacket to acquire as provide and the the ability of an attacket to acquire as provide that so the vector of the town and minister or group and the text of a spice of the users are in the bally of an attacket to acquire as provide that so the than 30% of the text as a the users are in the users are in the users are in the sensing on computer. Ministraining proper security pathese are mising on computers. Ministraining proper security pathese are have not logged on to domain 30 days. Auser that has not logged in the spice of the spice proves that should be provide to determine if an arti-virus software is enabled and runnin     ve

**Important:** If you have not yet created a connection, see <u>"Integrate</u> <u>Network Detective Pro with a PSA System" on page 294</u> 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.

	Select Items to Export
Mappings	Select All Unselect A
ConnectWise Connection:	Computers were found with significantly low free disk space.     Anti-spyware software was not detected on some computers. Without adequa     Computers are to be using potentially insecure protocols.     Computers are using an operating system that is in Datended Supported. B     Computers found using an operating system that is in Datended Supported. B     Computers have not checked in during the past 30 days.     Friorcing password complexty limits the ability of an attacker to aquire a j     Local account passwords on 2 were found to be potentially weak. Inadequ     More than 30% of the users are inte Domain Administrator group and have     Password policies are not consistently applied from one computer to the ne     Security patches are missing on computers. Maintaining proper security pa
Source:	Users have not logged on to doman 30 days. A user that has not logged in     We were unable to determine if an anti-virus software is enabled and runnin

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.

	sk Search		
Home	ADMIN CATEGORIES		
CRM	Account Settings & Users		
Contracts	Features & Settings		
Projects	Automation		
Service Desk	Activations Extensions & Integrations		
Timesheets			
Inventory	COMMONLY USED		
Reports	Getting Started		
Outsource	Resources (Users)		
Admin	Form Templates		
	Notification Templates		
datto   RMM	Workflow Rules		
datto   BCDR	User-Defined Fields		
	System Settings		

4. Next, click **Resources/Users (HR)** to expand the menu.



5. Then click Resources/Users.

Admin	
Account Settings & Users Features & Settings Automation	Activations Extensions & Integrations
Expand All Collapse All	
<ul> <li>Your Organization</li> </ul>	
A Resources/Users (HR)	
Resources/Users (HR)	
Resources/Users Manage user accoul for people in your organization who have an Autotask login.	Time Off Policies Manage the time off categories and the number of days or hours in each category your resources are entitled to at each length of service tier.
Koles Set up billing roles that determine the rate at which labor will be billed.	Timesheet Approvers Set up the resources who will approve other resources' timesheets.
Departments Set up organizational entitles in your company that are associated with resources and work types, and play a role in project security.	Expense Report Approvers Set up the resources who will approve other resources' expense reports.

6. Hover your mouse over the drop-down menu to the right of the **New** button, then select **New API User**.

≡ <i>A</i> utotask	Search	Q Dast	nboards Create	My Calend	lar
<ul> <li>Resources</li> </ul>					
+ New 🔹 Import/In	mport History	🕹 📃 Show Inac	tive Find Resource		
New Resource	Resource ID 🚖	Default Department	Security Level 🚔	License Type 🔷	c
		•			•
	1000		AT 144 (1998)	100.000	

7. Enter information about the API user. Autotask will prompt you to enter the mandatory fields.

	0
	<b>U</b>
Save & Close (x) Cancel	Review Terms and Conditions for API Use
General	
First Name *	Security Level *
	▼
Last Name*	Date Format
	MM/dd/yyyy
Email Address*	Time Format
	hh:mm a 🔻
✓ Active	Number Format
Locked	x,xxx.xx •
	Primary Internal Location *
Credentials	
C Generate Key	C Generate Secret
Username (Key) *	Password (Secret)*
API Tracking Identifier	
API version 1.6 & later require the user of an API tracking identifier. Or	nce assigned, this cannot be changed.
Custom (Internal Integration)	
Untegration Vendor*	
RapidFire Tools - Network Detective	
Line of Rusiness	
Line of Dusiliess	
A line of business can be used to grant access or prevent access to d Not Associated	ata associated with Contracts, Tickets, Projects, etc. Associated
A	A
→	•
•	
Ŧ	*
Resource can view items with no assigned Line of Business	3

- 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.

Add API User	0
🖹 Save & Close 🛞 Cancel	Review Terms and Conditions for API Use
Credentials	-
⊖ Generate Key	⊖ Generate Secret
Username (Key) *	Password (Secret) *
API Tracking Identifier API version 1.6 & later require the user of an API tracking ide Integration Vendor Custom (Internal Integration) Integration Vendor*	ntifier. Once assigned, this cannot be changed.
rapidfire •	
Perspectium Middleware (ServiceNow) PropelYourMSP Li Pulseway RMM Quickpass - Password Management Quoter Software Inc Quoter QuoteWerks - Quotes, Proposals, and Procurement RapidFire Tools Mail Toket RapidFire Tools Network Detective Recursy- Seamless Red Cactus - Bubble CRM Integrations Relokia - Data Migration	ssociated with Contracts, Tickets, Projects, etc. Associated
Resale Partners - Telephony	susues v

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 <u>http://university.connectwise.com/install/</u>. 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* Admin	~	Location* Tampa Office	~
Level* Corporate (Level 1)	~	Business Unit* 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 <u>"Create Minimum Permissions</u> <u>Security Role for API Member" below</u>.

### 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 Des	k				
	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 <u>"Table Setup Configuration"</u> below below for an extended				
	explanation)				

## Table Setup Configuration

From Table Setup, click **customize**.

Report Writer	None	$\sim$	None	$\sim$	None	$\sim$	None	$\sim$	
Security Roles	None	$\sim$	None	$\sim$	None	$\sim$	None	$\sim$	
System Reports (customize)	None	$\sim$	None	$\sim$	None	$\sim$	None	$\sim$	
Table Set <mark>up (<u>customize</u>)</mark>	All	$\sim$	None	$\sim$	None	$\sim$	All	$\sim$	
Today Links	None	$\sim$	None	$\sim$	None	$\sim$	None	$\sim$	
∧ Time & Expense									7/25/23
Expense Approvals	None	~	None	$\sim$	None	~	None	~	

Allow access to the items listed in the table above under **Table Setup**. You can also refer to the image below.

llow Access to these		Disallow Access to these		
Company / Company Status		Activities / Activity Status-CRM		
Company / Configuration		Activities / Activity Type		
Opportunities / Opportunity Status	>	Agreements / Agreement Type		
Opportunities / Opportunity Type	<	Agreements / Batch		
	>>	Company / Address Formats		
	"	Company / Company Type		
		Company / Configuration Status		
		Company / Country		
		Company / Currency		-
		4	►	

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

You have successfully updated this record.						
Public API Key						
Description:	*	test1				
Public Key:	*					
Private Key:	*					

### 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.

		_				_
Board	Statuses	Types	Subtypes	Items	Auto Templates	Teams

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 🗸	<u> </u>	
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	<u>SLA</u>	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 $\ensuremath{g}\xspace.$

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 Ta	bles		
Setup Ta	bles		
0540011	01 5 4 5		
SEARCH	CLEAR	c	
Category		Table ^	Description
Company	$\sim$		
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			
	_						
Active							
Inactive			$\checkmark$				
Imported			$\checkmark$				
Credit Hold			$\checkmark$				
Problem			$\checkmark$				
not-Approved	$\checkmark$		$\checkmark$				
Solid							
Attention needed			~				
may Leave			$\checkmark$				
Delinquent			$\checkmark$				

3. 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 an	d Time							
Votify								
✓ 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 a	nd 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.

C N	Company Search > Company > Company Finance Detail Micro Pro							
<	Summary	Recap	Invoices 0	Time 0	Expenses 0			
<	8	� 骨∖	✓ History ✓	Links 🗸				
	Company: Mic	ro Pro						
	Company: *	Micro Pro			Phone:			
	Company ID: *	123			Fax:			
	Status: *	not-Approved	1	~	🛱 Web Site:			
	Type: *							
	Prospect X							
	Finance Detail	s		÷				

### 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 <u>ConnectWise REST API</u> 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 个	Description		
	🗸 integrator			
General	Integrator Login	Setup Integrator Access		

- 4. Click the "**New**" lcon 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				
<	+ 🗄 🗄 🕹 H	HISTORY 🗸 🔟			
Username* api					
Password					
Access Level					
Select the available API integration(s) you wish to enable and configure below:					
API Name					
	Activity	Callback URL	Use legacy		
	Agreement	Callback URL			
	Company	Callback URL			

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.

ľ	CRM Manager	CRM Manager	
ß	Project Manager	Project Manager	
ß	Service Desk Manager	Service Desk Mana	ger
ß	Administrator	Administrator	

4. Click the Role Users tab.

✓ Security Ro	le Information	
Name: *	tor	
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**.



Custom API Keys The IT Glue API is a RESTful AI	PI that can be used to manage and retrieve info	ormation. Learn more						
rft_	ITG.614	Revoke	Password Access	-				
kreed_	ITG.0d6	Revoke	Password Access	-				
rft_	ITG.2eb	Revoke	Password Access	-				
Enter Name		Generate API Key	Password Access	-				
		_		+				
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.

Preferences     Report Enail Groups Issue Ovendes     Megrations     Dark Web ID     If Glue     Connections Manager as 'Only Me' or 'This Account' Connections.      Manage Connections     If Glue Connections Manager	×
Report Defaults     Report     Email Groups     Issue Overrides     Integrations       Dark Web ID     IT Give     This Account* Connections         New Connections         Image Connections         Image Connections	
Dark Web ID IT Give Connections Manager as "Only Me" or "This Accourt" Connections.  Manage Connections  IT Glue Connections Manager	
New Connections can be the IT Glue Connections Manager as "Only Me" or "This Account" Connections.  Manage Connections	
Manage Connections	
Manage Connections       It Glue Connections Manager     —     —     ×	
🛛 IT Glue Connections Manager – – ×	
🔁 11 Glue Connections Manager — 🗆 🗙	
🝳 IT Glue Connections Manager — 🗆 🗙	
IT Glue Connections Manager	
Manage Multiple IT Glue Accounts	
Saved Connections	
New 1	
ff_documentation Modify	
Permus	
IT Glue Credentials	
Connection Name:	
IT Glue API URL	
T Chus ARI Kan	
Deselect All	
Connection Type: O Unity Me O This Account Close	
OK Cancel	
9	
Ok Cancel	

- 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:	rft_documentation
IT Glue API URL:	https://api.itglue.com
IT Glue API Key:	••••••
Connection Type:	Only Me
	OK Cancel

#### 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.

Q Network Detect	tive Pro - 1	4.0.1313		
Ê			1 🗳	2
Home	Appliance	s Connector Service	Plans Reporter	Users
		Back to Home		
SITE	$\wedge$	Reporter Customer	·1-	/ Edit Ste
		Generated Reports		
		Filename	Date Modified 🔹 👻	
Active Project	1	Assessment-20190304-Reports5	9/29/2020 3:16 PM	
	1	Client Progress Reporting	9/29/2020 2:35 PM	
	1	Assessment-20190304-Reports4	9/29/2020 1:46 PM	
	1	Assessment-20190304-Reports3	9/29/2020 1:39 PM	
	1	Assessment-20190304-Reports2	9/29/2020 1:34 PM	
Archived Projects	1	Assessment-20190304-Reports1	3/6/2019 1:54 PM	
	1	Assessment-20190304-Reports	3/6/2019 1:40 PM	
	1	Assessment-20180816-Reports15	10/24/2018 10:07 AM	
	1	Assessment-20180816-Reports14	10/24/2018 9:43 AM	
Progress Reports	1	Assessment-20180816-Reports13	10/24/2018 9:38 AM	
1 togetas reports	1	Assessment-20180816-Reports12	10/24/2018 9:34 AM	
	1	Assessment-20180816-Reports11	10/24/2018 9:26 AM	
	1	Assessment-20180816-Reports10	10/23/2018 7:43 PM	
	1	Assessment-20180816-Reports9	10/23/2018 5:58 PM	
Generated	1	Assessment-20180816-Reports8	10/23/2018 5:50 PM	
Heports	1	Assessment-20180816-Reports7	10/23/2018 5:20 PM	
	1	Assessment-20180816-Reports6	10/23/2018 5:17 PM	
	5	Assessment-20180816-Reports5	10/23/2018 5:14 PM	
Developeded	1	Assessment-20180816-Reports4	10/23/2018 5:06 PM	
Reports	1	Assessment-20180816-Reports3	10/23/2018 4:57 PM	
	6	Assessment-20180816-Reports2	10/23/2018 4:50 PM	
	6	Assessment-20180816-Reports1	10/23/2018 4:40 PM	

2. Choose the assessment reports you want to export, then **right click** and select **Export to IT Glue**.

		Back to Home			
SITE	^	Reporter Cust	omer		/ Edit Ste
		Generated Rep	orts		
		Filename		Date Modified	*
Active Project	6	Assessment-20190304-Rep	orts5	9/29/2020 3:16 PM	
	1	Client Progress Reporting		9/29/2020 2:35 PM	L. C.
	1	Assessment-20190304-Rep	orts4	9/29/2020 1:46 PM	
	6	Assessment-20190304-Ren	orte 2	9/20/2020 1-20 04	1
	6	Assessment-20190304-R	Export	t to IT Glue	
Archived Projects	1	Assessment-20190304-R	Remo	ve Report	
	1	Assessment-20190304-Rep	orts	3/6/2019 1:40 PM	
	1	Assessment-20180816-Rep	orts 15	10/24/2018 10:07	AM
	1	Assessment-20180816-Rep	orts14	10/24/2018 9:43 A	м
Persona Persona	1	Assessment-20180816-Rep	orts13	10/24/2018 9:38 A	м
riogress riepoits	1	Assessment-20180816-Rep	orts 12	10/24/2018 9:34 A	м
	1	Assessment-20180816-Rep	orts11	10/24/2018 9:26 A	м
	6	Assessment-20180816-Rep	orts 10	10/23/2018 7:43 P	м
	1	Assessment-20180816-Rep	orts9	10/23/2018 5:58 P	м
Generated	6	Assessment-20180816-Rep	orts8	10/23/2018 5:50 PI	м
Reports	1	Assessment-20180816-Rep	orts7	10/23/2018 5:20 P	м

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.

ploads selected documents as G ocument folder.	lueFiles to an IT Glue Organization in a new	Select Documents to Export	
ocument folder. Mappings T Glue Connection: Drganization: Report Folder Name: Netwo nsert UTC Timestamp: ● Bet ☑ Append Ste Name ☑ Append Assessment Report fo Delimiter: Preview: 2022.0 Preview: 2022	k Detective Pro Reports ore Folder Name After Folder Name Folder 3-14 14:44:07 - Network Detective Pro s- Reporter Customer 1 - nert-20190304-Reports 3	Security-Vormalous Login Report docx Security-Vormalous Login Report docx Security-Vormalous Login Report docx Security-Vormalous Heaven View Report Card docx Security-Votate Breach Lability Report Security-Wate Breach Lability Report docx Security-Votate Breach Lability Report docx Security-Votate Breach Lability Report docx Security-Votate Breach Lability Scan Detail Puese Report docx Security-Votatemal Winerability Scan Detail Puese Report docx Security-Votatemal Winerability Scan Detail Puese Lability Security-Votatiourd Security Report docx Security-Votatiourd Security Report docx Security-Votatiourd Security Report docx Security-Votatiourd Security Report docx Security-Security Health Report docx Security-Security Meangement Raccx Security-Security Puese Report docx Security-Security Puese Report Securits Security-Security Pues	<u>t All</u>

4. Then select the **Organization**. This list will include your available IT Glue orgs.

ploads selected documents as GlueFiles to an IT Glue Organization in a nev ocument folder.	Select Documents to Export
oloads selected documents as GlueFiles to an IT Glue Organization in a new ocument folder. Mappings T Glue Connection: Drganization: Report Folder Name: a Append Site Name Append Site Name Append Assessment F Delimiter: Preview:	Select Documents to Export     Security-Venomialous Login Report docx     Security-Venomialous Beauty Report Card Excel Max     Security-Consolidated Security Report Card Excel Max     Security-Consolidated Security Report Card docx     Security-Data Breach Liability Report Security Report docx     Security-External Networkship Scan Detail Isoci Max     Security-External Networkship Scan Detail Isoci Max     Security-External Networkship Scan Detail Isoci Max     Security-External Networkship Scan Detail Report docx     Security-External Networkship Scan Detail Report docx     Security-External Networkship Scan Detail Report docx     Security-Losin Failures by Computer Report docx     Security-Roter Settings Report docx     Security-Roter Settings Report docx     Security-Security Health Report docx     Security-Security Failes Report Bealt Report Beal

5. Continue configuring the export. When you are ready, click **Export**. A confirmation will appear when the job is complete.

	×
Export to IT Glue	completed.
	OK

6. You can then find your exported documents in IT Glue under the organization you selected.

⊠ITGlue		Da	shboard	Organizations	Personal	Global	Account		Q	0	?	🛃 Hanson 🔽
# Home		ACME	Dental / D	ocuments / Netv	vork Detective	e Pro Repo.	. / Network					
Core Assets ✓ Checklists		Do	cum	ents						소	Import	▼ + New ▼
Configurations										0	Include archive	20 of 20 Results
Contacts												
Documents	44		Name 🕈					Updated 🗘	Updated By 🗘	Exq	oires 🗘	
Obmain Tracker			🗟 Ass	et Detail Report.de	ocx 🗊			Today at 7:20 PM				200
♀ Locations			Clier	nt Health Report.c	locx 🗊			Today at 7:20 PM				* - 0
Networks			Clier	nt Risk Report.doo	x (]			Today at 7:20 PM				20
A SSI Tracker			🗟 Con	solidated Manage	ment Plan.do	icx 🗊		Today at 7:20 PM				* <b>*</b> *
<ul> <li>Sac macker</li> <li>Tickets</li> </ul>			Con	solidated Risk Exc	cel.xlsx 🚺			Today at 7:20 PM				200
Apps & Services			🗟 Con	solidated Risk Rej	port.docx 🖪			Today at 7:20 PM				20
I Networking			Exce	el Export.xlsx 🗊				Today at 7:20 PM				200
Active Directory			🗟 Full	Detail Report.doc	×đ			Today at 7:20 PM				200
			🖻 Laye	er 2-3 Detail Excel	Export.xlsx 🕻	1		Today at 7:20 PM				* - 0
			🗟 Laye	er 2-3 Detail Repor	t.docx 🗊			Today at 7:20 PM				20
			🗹 Laye	er 2-3 Diagram Exp	port to Micros	oft Visio.v	sdx 🗊	Today at 7:20 PM				200
			🗟 Laye	er 2-3 Diagram Re	port.docx 🐧			Today at 7:20 PM				200
			🗟 Laye	er 2-3 Diagram.tif				Today at 7:21 PM				20

© 2023 RapidFire Tools, Inc. All rights reserved.

**RapidFireTools**<sup>\*</sup>

## 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.

Login	×						
Usemame: test-user@raj	pidfiretools.com						
Password:							
🗹 Remembe	er Usemame						
Login	Cancel						
Forgot your password? Enter your usemame and click here.							
Problems logging in? verify connection							

#### **RapidFireTools**\*

## Network Detective Linux Computer Data Collector

The Linux Computer Data Collector is a Linux application (works on most modern Linux versions) that is run on individual computers (workstations or servers) to collect information for that system. Use this to collect computer information from Linux systems to be merged into the network data collection.

This data collector is a version of computer data collector only and cannot perform Security Assessments or Network Data Collection.

#### Download the Linux Computer Data Collector

Download the Linux Computer Data Collector here:

https://download.rapidfiretools.com/download/NetworkDetectiveLinuxCollector.tar.gz

## Run the Linux Computer Data Collector

This Linux Computer Data Collector download is a tar gzip file and does not require installation. Unzip it, then launch the application using the command below:

tar zxf NetworkDetectiveLinuxCollector.tar.gz | ./NetworkDetectiveLinuxCollector

## Scan Output and Import into Assessment

Scan output is a ".cdf" file with the filename -.cdf. Copy this file for merging with the ZIP/NDF file when importing into the Network Detective 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 generaluse 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.

	<b>e</b>	
	Online Help	) Upgrade
	Show Startup Tips	
	Download Data Collectors	
	Report Requirements	
Filter	Release Notes	Finish
	Instructional Videos	
	Recorded Training Webinars	
	HIPAA Training Videos	
	New User Orientation	
	Marketing Collateral	
	Download Sample Report Data	
	Sample Legal Forms	
	Audit Log	
	Submit Suggestion	
	Augment Reporting	
	Improve Translation	

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*.

q	🛛 Augment Reporting — 🗆 🗙										
End	Endpoint Protection Detection										
En	Endpoint detection can be improved to remove false positives by identifying additional backup, anti-virus, and anti-spyware solutions through their service display names.										
		Antivirus	Antispyware	Firewall	Backup	Service	e Display Name	P	Product Name		
		$\checkmark$				Bitdefen	der Endpoint Agent	Ye	Your Branded Anti-Virus Service		
		$\checkmark$				- 7					
Þ	,										
	"Display Name" of Windows Service							Name yo wish to appear in Reports	น า		
	Ok Cancel										

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 <u>"Use</u> <u>the Excel Export Spreadsheet to Find Display Names" on the facing page</u> for an easy way to find display names for all Windows services.

Bitdefend	der Endpo	oint Agent	Properties (I	Local Comput	er)	$\times$		
General	Log On	Recovery	Dependenc	ies				
Service	name:	epag						
Display	name:	Bitdefende	er Endpoint Ag	gent				
Descrip	Description: Ensures the communication between a managed client machine and the security server.							
Path to "C:\Pro	executabl gram Files	e: \Bitdefender	\Endpoint Sec	curity\epag.exe				
Startup	type:	Automatic				~		
		<b></b>				_		
Service	status:	Running				_ 1		
\$	Start	Stop	þ	Pause	Resume			
You ca from he	n specify ti re.	he start para	meters that a	pply when you	start the servi	ce		
Start pa	arameters:							
			OK	Cance	I Ap	pply		

- 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	Serve	er 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