NETWORK DETECTIVE™

USER GUIDE

Reporter

Fully Automate ongoing Report Generation & Delivery with Reporter

9/20/2021 2:47 PM

Contents

Introduction to Reporter

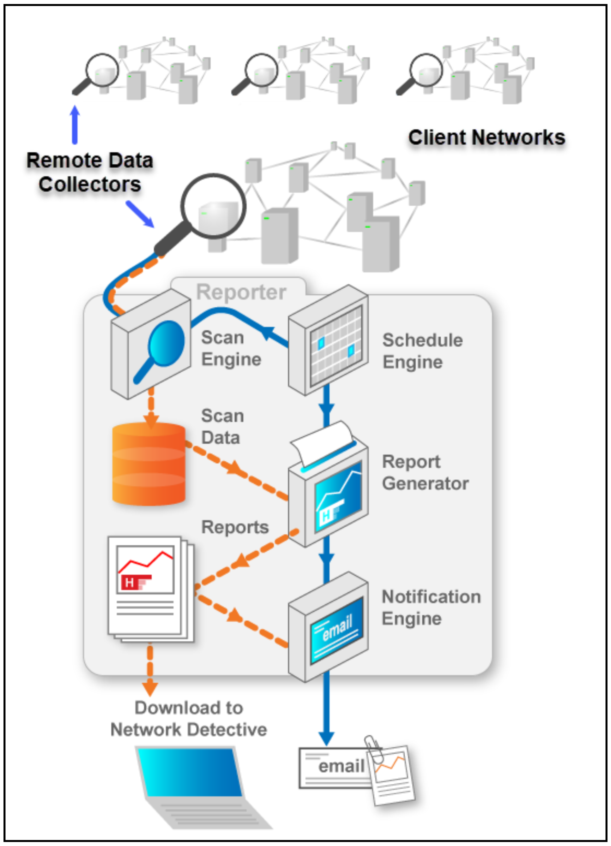
This section covers everything you need to know before getting started with **Reporter**.

Reporter Overview

Reporter allows you to automate, schedule, and deliver the assessment reports generated by Network Detective. Reporter can be used with each Network Detective 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. Reporter also includes our **InDoc** technology, which allows you to annotate network assets with your own notes and procedures.

Reporter Appliance

You can install **one** Reporter appliance on your company network, where it can generate automated reports for multiple client sites. Use the **Network Detective** application to manage the Reporter and to select which reports to generate and deliver on a pre-scheduled basis. Reporter also has the ability to schedule and automatically perform **External Vulnerability Scans**.



Remote Data Collector

The Reporter works in tandem with the Network Detective **Remote Data Collector** (RDC). The **RDC** is an automated data collector used to execute network and local computer scans necessary to perform Network, Security, Office 365/Exchange, SQL Server, HIPAA, and PCI assessments. The RDC is installed in under five minutes at each client site.

You manage the RDC from the Network Detective application, where you configure and schedule scans.

© 2021 RapidFire Tools, Inc. All rights reserved.

InDoc and the RapidFire Tools Portal

With your Reporter subscription, you can use **InDoc** and the **RapidFire Tools Portal** to dive deeper into the data you collect from your Reporter sites. With InDoc, you can supplement Reporter data with your own network documentation to make managing your client's assets a breeze. InDoc utilizes Reporter scan data to provide continually updated asset documentation that can be augmented with notes, procedures, and tags as well as being related to other assets.

About this User Guide

This guide is designed to provide an overview and specific steps required to:

- install and configure the **Reporter Software Appliance**
- install and configure the **Remote Data Collector** at each client site for which you wish to use Reporter
- schedule the collection of IT and Compliance assessment scan data for storage in the RapidFire Tools **Secure Cloud Storage Area** to automatically generate assessment reports
- use **InDoc** and the **RapidFire Tools Portal** to enhance your asset documentation for client sites with your own Notes and Procedures

Components of the Reporter

Reporter Component	Description
Reporter Appliance	This is the **Reporter** software application that operates on the MSP network. Specifically, you will install the **RapidFire Tools Server** Windows Service.
Remote Data Collector	You install the **Remote Data Collector** at each of your client's sites, where you configure it to perform unattended scans on the network.
Network Detective Application	This is the same **Network Detective** desktop application and report generator that is used with any other Network Detective modules. This application contains additional features to manage the **Reporter** remotely, including the **Client-Connector**.
InDoc and RapidFire Tools Portal	**InDoc** utilizes Reporter scan data to provide continually updated asset documentation that can be augmented with *Notes*, *Procedures*, and *Smart Tags*. You can also map *Relationships* between assets. You access InDoc for Sites through the **RapidFire Tools Portal**.
(Optional) Diagnostic Tool	The **Diagnostic Tool** is used for configuring and troubleshooting the **Reporter**. The Diagnostic Tool should be run on the same network as the **Reporter** to perform diagnostics checks such as for **Reporter** connectivity or for available updates.

© 2021 RapidFire Tools, Inc. All rights reserved.

Reporter Features

Reporter is designed to perform the following:

- Enable an MSP to remotely gather Network Detective scan data for multiple client networks to generate assessment reports. This eliminates the need to manually download scan data from the Secure Cloud Storage Area previously uploaded using the Network Detective **Client-Connector**.
- Automate the collection and consolidation of scan data using the Network Detective **Remote Data Collector** and automatically generate Assessment reports from the point-of-view of the client's internal network. This eliminates the need to manually generate assessment reports.
- Enable an MSP to operate a Reporter appliance on its local network to set up, manage, and perform automatic assessment report generation for multiple client Sites.
- Allow MSP support technicians and help desk personnel to easily access documentation and current asset information regarding a customer site to assist in addressing customer issues.

Automated Assessment Reporting

Automatic Report Generation enables you to use the **Reporter** to schedule and generate assessment reports for each Network Detective Assessment Module. This includes:

- Network Assessments
- Security Assessments
- SQL Server Assessments
- Microsoft Exchange Assessments (using the Exchange Data Collector)
- HIPAA Compliance Assessments
- PCI Compliance Assessments

Automated External Vulnerability Scanning

Reporter enables you to configure and schedule an External Vulnerability Scan to run at regular intervals.

External Vulnerability Scans are performed at the external “Network Edge” to check for security holes and weaknesses. The results can help you help make better network security decisions. The External Vulnerability Scan performed by **Reporter** includes a full NMap Scan which checks security holes, warnings, and informational items that can help you make better network security decisions. This is an essential scan and is a standard security check to ensure a viable security policy has been defined, implemented, and maintained to protect the network from outside attacks.

The External Vulnerability scans can be incorporate into Network Detective Security, HIPAA, and PCI Assessments.

Remote Updating of the Reporter

Reporter is easy to update remotely. Updates may include bug fixes, new features, and additional scans types. Updates can be configured to take place automatically.

InDoc and the RapidFire Tools Portal

With your Reporter subscription, you can use InDoc and the RapidFire Tools Portal to dive deeper into the data you collect from your Reporter sites. With InDoc, you can supplement Reporter data with your own network documentation to make managing your client's assets a breeze. With InDoc, you can:

- Annotate each asset on the client's network with your own Notes and Procedures.
- See relationships between assets by linking together Related Items.
- Safely share Confidential Notes, including passwords, in a secure storage area.
- Manage the Smart Tags associated with each network asset. Smart Tags are used to monitor network security with Cyber Hawk, our security service delivery system.

Tips for Automated Report Scheduling

Before you schedule report generation, be sure you take into account these tips:

Schedule Site Reports after Site Scans

Tip: Use **Reporter** to schedule reports to be generated at a time after the necessary scans have taken place on your customer networks using the Network Detective **Remote Data Collector**. This will ensure Reporter has access to the latest scan data before it generates and delivers the assessment reports.

Schedule Reports at Correct Time Intervals for Multiple Sites

Tip: Before it can generate reports, Reporter needs time to download Scan Data from the RapidFire Tools **Secure Cloud Storage Area**. Schedule Report generation tasks to take place 20-30 minutes apart for each of your Network Detective sites. This will ensure Reporter has enough time to download scans and generate reports for a site before it moves on to the next site.

Schedule External Vulnerability Reports after External Vulnerability Scan

Tip: External Vulnerability Scans may take several hours to complete for your Site. Schedule your External Vulnerability Report tasks at least 5 hours after your external scan for the site.

© 2021 RapidFire Tools, Inc. All rights reserved.

RapidFire Tools Server System Requirements

Below you can find the minimum requirements for the RapidFire Tools Server:

RapidFire Tools Server Type	Cyber Hawk	Compliance Manager	Reporter
Minimum Requirements	• Intel i5 processor • Windows 10 Pro or Windows 2016 Server and up • 2 GB Available RAM • 5 GB Disk Space • Network connectivity/Internet access	• Intel i5 processor • Windows 10 Pro or Windows 2016 Server and up • 2 GB Available RAM • 5 GB Disk Space • Network connectivity/Internet access	• Intel i5 processor • Windows 10 Pro or Windows 2016 Server and up • 4 GB Available RAM • 10 GB Disk Space Recommendation: +1 GB per client Site • Network connectivity/Internet access **Important:** Reporter is installed on the MSP network - NOT the client network.

Important: You can only install **one** RapidFire Tools server/appliance on a PC or endpoint at a time. If you need to install multiple server(s)/appliance(s), install each one on a separate endpoint on the network.

© 2021 RapidFire Tools, Inc. All rights reserved.

Reporter Prerequisites

The following components are required to operate the **Reporter Appliance**:

- a subscription to one or more Network Detective **IT** or **Compliance Assessment Modules**
- the **Network Detective Application**
- an Internet connection used to access the RapidFire Tools **Secure Cloud Storage Area**
- the **Remote Data Collector** configured and scheduled to perform unattended scans on your client’s network. These scans may include
    - Network and Security Scan Data Collection
    - Exchange and Office 365 Mail Scan Data Collection
    - SQL Server Data Collection
    - HIPAA Assessment Data Collection
    - PCI Assessment Data Collection
- a **Client-Connector** configured to operate with the **Remote Data Collector** to upload the scan data collected from the network at your client’s site to the RapidFire Tools **Secure Cloud Storage Area**.

Setting Up Reporter

Setting up your Reporter consists of these steps:

1. Install the Reporter appliance on your MSP network and associate it with Network Detective Sites
2. Install the Remote Data Collector on a network located at each physical client Site for which you wish to generate automated reports
3. Configure the Remote Data Collector to perform unattended scans at each client Site
4. Configure the Reporter appliance and schedule automated report generation

Initial Reporter Set Up

Step 1 — Install Reporter Appliance on MSP Network

Visit https://www.rapidfiretools.com/nd-downloads to download and install the Reporter Server on a Windows 10 PC operating within your MSP company's network.

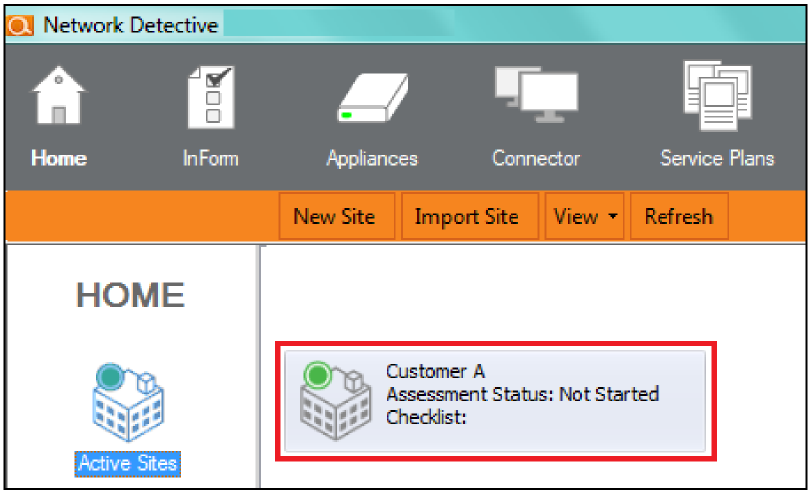
For more information about **installing the Reporter Server**, please download the Reporter Server Installation Guide.

Important: You can only install **one** RapidFire Tools server/appliance on a PC or endpoint at a time. If you need to install multiple server(s)/appliance(s), install each one on a separate endpoint on the network.

After successfully deploying the Reporter Server, visit https://www.rapidfiretools.com/nd-downloads to download and install the latest version of the **Network Detective Application**. Then run **Network Detective** and login with your credentials.

Step 2 — Open Existing Network Detective Site with an Active Assessment Project

1. Start the Network Detective application.
2. Select the **Site** that you want to use with the **Reporter Appliance**.



Customer A
Assessment Status: Not Started
Checklist:

3. To open the **Site**, double-click on the **Site** name.

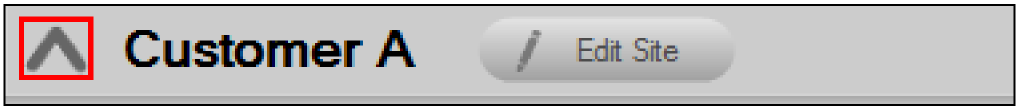
   If you do not have a **Site**, create a **New Site**.

4. Open an existing **Assessment Project** or **Start** a **New Assessment Project** to be used with the **Reporter Appliance**.

Step 3 — Associate Reporter with Sites

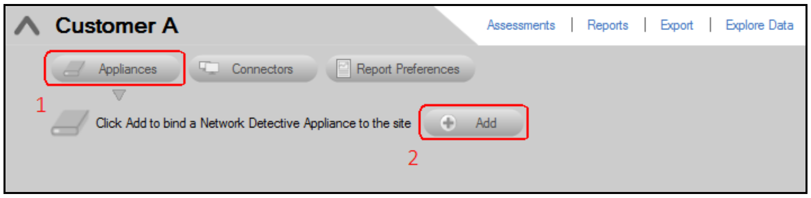
Before using the **Reporter**, the **Reporter** must be **Associated** with a **Site** in the **Network Detective Application**.

1. After creating a new Network Detective **Site**, or within an existing **Site**, in order to "**Associate**" a **Reporter** with the **Site** used for the **Assessment Project**, you must first select the ⌃ selector symbol to expand the **Site's** properties view.



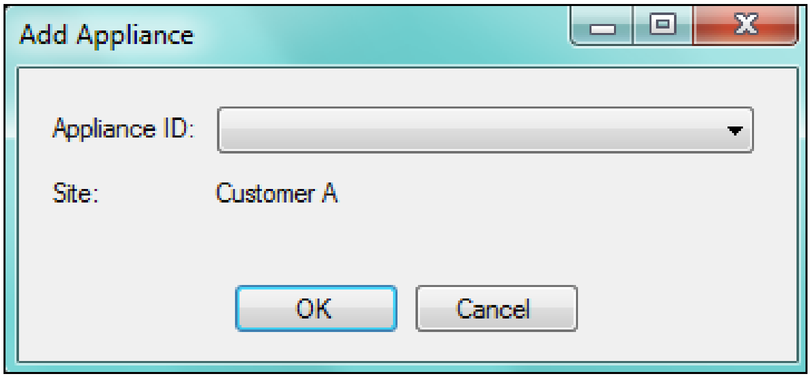
This action will expand the **Site**'s properties for you to view and to **Add** a **Software Appliance** to the **Site**.

2. To add an **Appliance** to **Site**, select the **Appliance** button, then the **Appliances Add** button.



Click Add to bind a Network Detective Appliance to the site

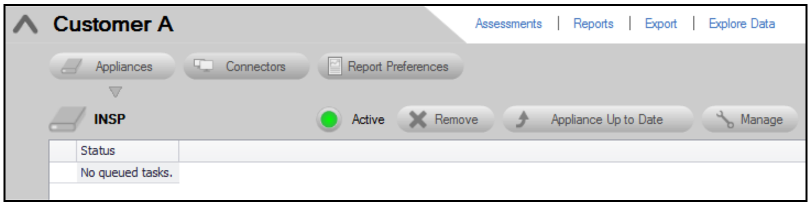
3. Select the **Appliance ID** of the **Appliance** from the drop down menu.



Appliance ID:

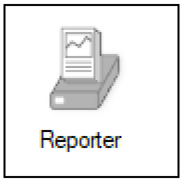
Site: Customer A

After successfully adding an **Appliance,** it will appear under the **Appliance** bar in the **Site Properties** window.

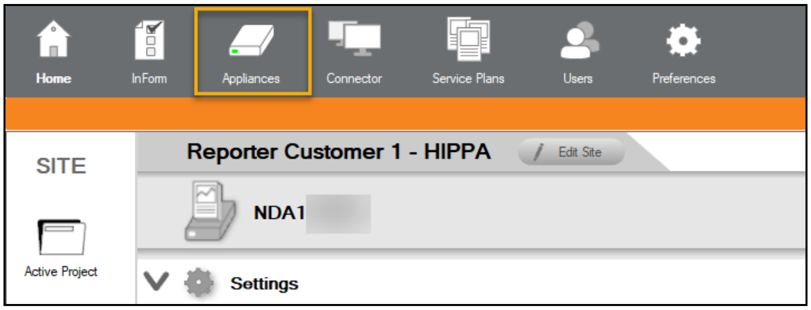


Status
No queued tasks.

The **Reporter** button will appear on the left-side bar when it is successfully associated with the Site.



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

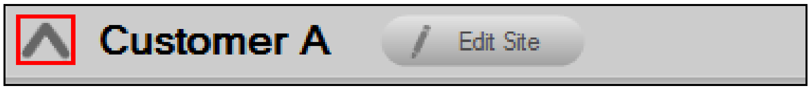


To return to the **Site** that you are using to perform your **Assessment**, click on the **Home** icon above and select the **Site** that you are using to perform your **Assessment**.

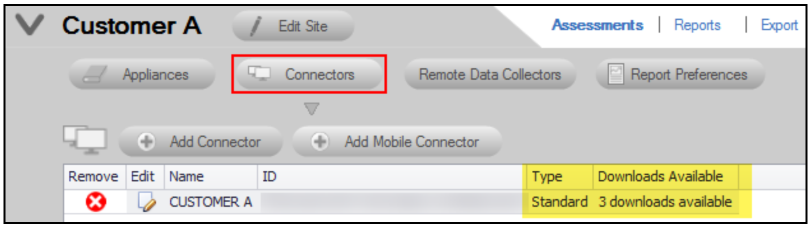
Step 4 — Add Client-Connector to the Site

1. Open the **Site** being used for your **Assessment** and **Reporter** configuration.

2. Select the ∧ **Selector** symbol to expand the **Site** properties view.



3. Select **Connector** button.

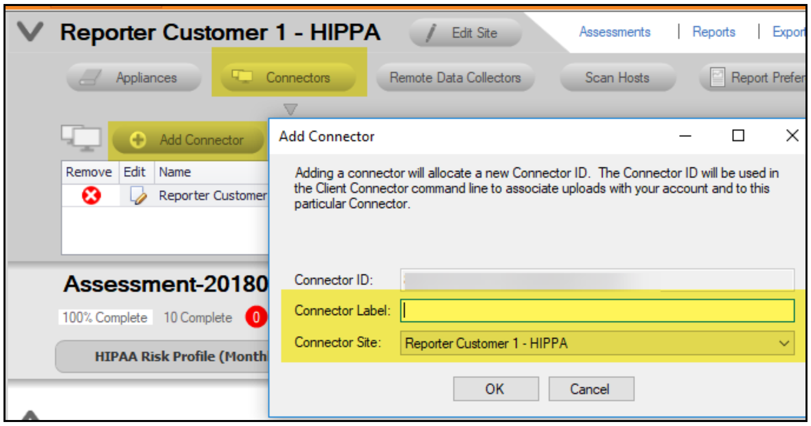


Remove	Edit	Name	ID	Type	Downloads Available
✖	✎	CUSTOMER A	[redacted]	Standard	3 downloads available

4. View the **Connectors** associated with the **Site**.

> **Note:** If a **Client-Connector** is not associated with a **Site** that is to be used with a **Reporter Appliance**, it will be necessary to **Add** a **Client-Connector** to the **Site**.

5. Click **Add Connector**. Enter a **Connector Label** and click **OK**.



Adding a connector will allocate a new Connector ID. The Connector ID will be used in the Client Connector command line to associate uploads with your account and to this particular Connector.

Connector ID: [redacted]

Connector Label:

Connector Site: Reporter Customer 1 - HIPPA

6. Close the **Site** properties by selecting the ∨ **Selector**.

When you complete these steps, proceed to "Initial Remote Data Collector Set Up" on the next page.

Initial Remote Data Collector Set Up

To perform the installation of the **Remote Data Collector**, please follow the instructions below.

Important: You will need Network Detective login credentials in order to install the Remote Data Collector.

Note: The Remote Data Collector is installed at the client's site.

Remote Data Collector System Requirements

The following is a list of computer and software system requirements that are necessary to operate the **Remote Data Collector**:

1. Subscriptions to the Reporter Appliance and any Network Detective Assessment modules relevant to the assessment reports you want to run.
2. A computer connected to your client's WMI enabled network running Windows 8.1 or 10.
3. A Client-Connector associated with the Reporter Site in Network Detective
4. Access to the Internet.

Network Prerequisites for RDC Scans

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 234 for configuration guidance for both Windows Active Directory and Workgroup environments.

Before setting up the RDC, be sure that you have the information detailed below on hand. 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.
- **External IP addresses** for the organisation to be used when setting up External Vulnerability Scans.
- **Network Detective Account Credentials**.

- For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IPaddress 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.

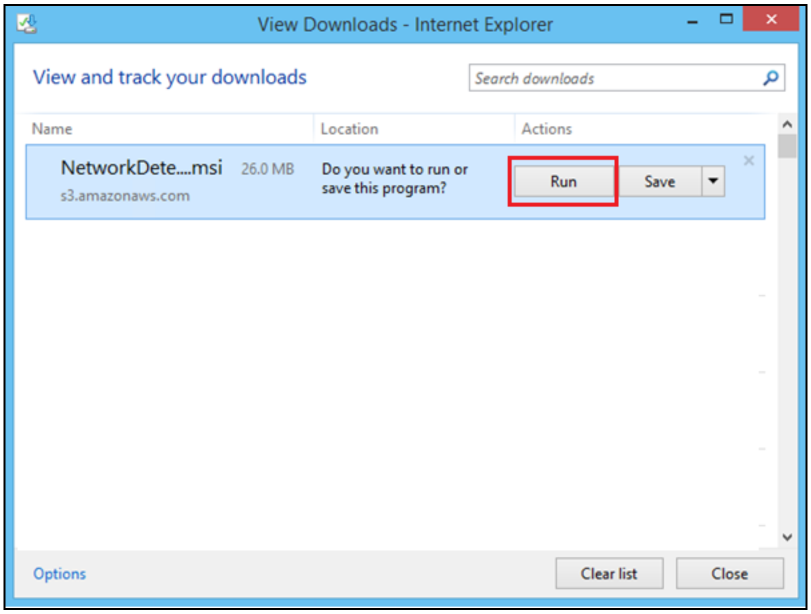
Remote Data Collector and Exchange Assessments

If you are installing the RDC to perform an Exchange assessment, you must install the RDC directly on the Exchange server itself. This is required in order for the RDC to communicate with the Exchange server using any required Exchange Shell utility available on the Exchange Server.

> **Note:** If you are scanning Office 365, you do not need to run the RDC on the server. You will only need to enter management credentials for Office 365.

Step 1 — Download and Install Remote Data Collector on Client Network

1. Visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd-downloads to download and run the **Remote Data Collector Installer** file. The **Installer** file is named **NetworkDetectiveRemoteDataCollector.msi**.

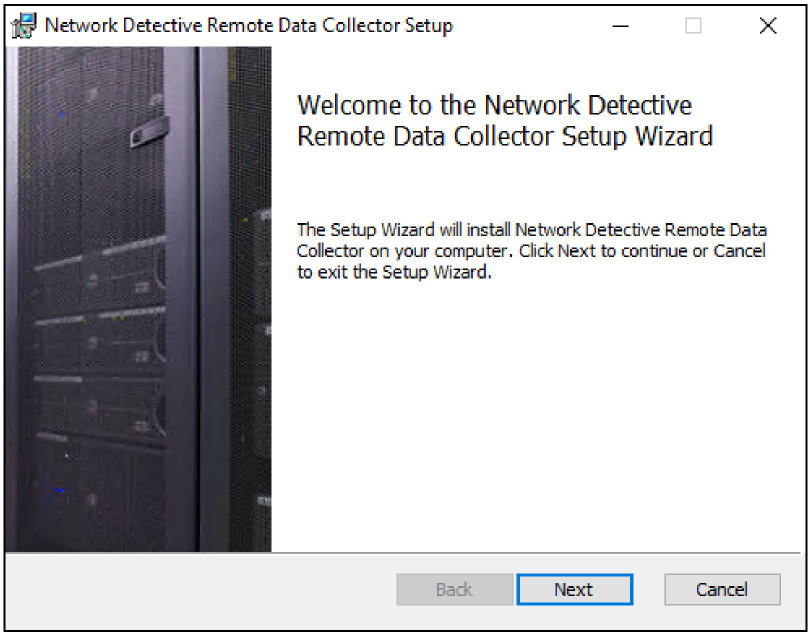


View Downloads - Internet Explorer

View and track your downloads

Name	Location	Actions
NetworkDete....msi 26.0 MB s3.amazonaws.com	Do you want to run or save this program?	Run Save

2. After downloading the **Installer**, **Run** the **Installer** to start the installation process.
3. After the Welcome Screen is displayed, click **Next** button to continue the installation process.

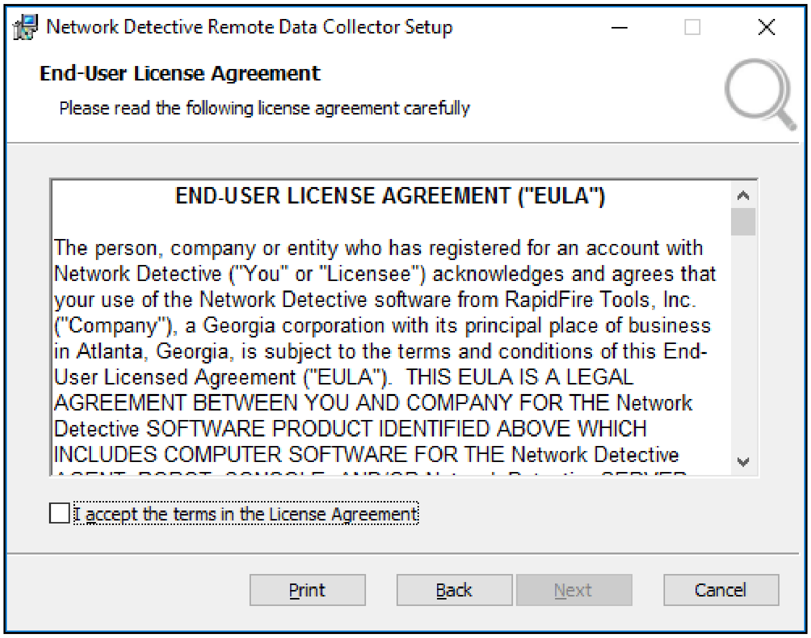


Network Detective Remote Data Collector Setup

Welcome to the Network Detective Remote Data Collector Setup Wizard

The Setup Wizard will install Network Detective Remote Data Collector on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Accept the terms of the **End User License Agreement** and click **Next**.


Network Detective Remote Data Collector Setup

End-User License Agreement

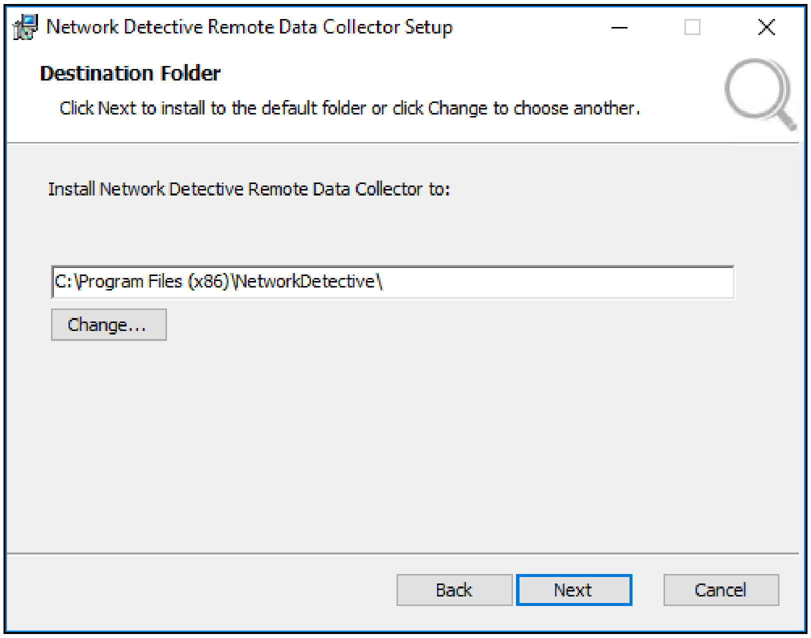
Please read the following license agreement carefully

END-USER LICENSE AGREEMENT ("EULA")

The person, company or entity who has registered for an account with Network Detective ("You" or "Licensee") acknowledges and agrees that your use of the Network Detective software from RapidFire Tools, Inc. ("Company"), a Georgia corporation with its principal place of business in Atlanta, Georgia, is subject to the terms and conditions of this End-User Licensed Agreement ("EULA"). THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND COMPANY FOR THE Network Detective SOFTWARE PRODUCT IDENTIFIED ABOVE WHICH INCLUDES COMPUTER SOFTWARE FOR THE Network Detective

□ I accept the terms in the License Agreement

5. Accept the default **Destination Folder** location for the Remote Data Collector's installation. Click **Next**.


Network Detective Remote Data Collector Setup

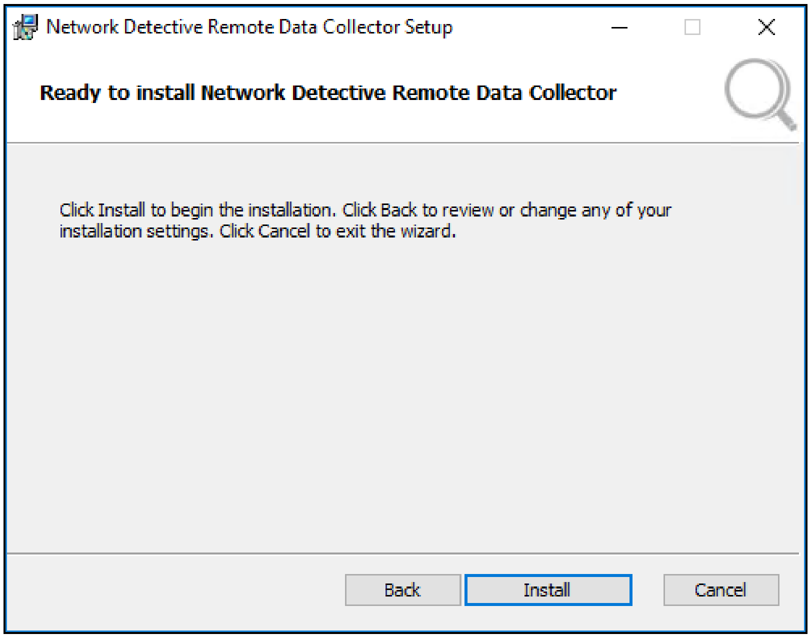
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Network Detective Remote Data Collector to:

C:\Program Files (x86)\NetworkDetective\

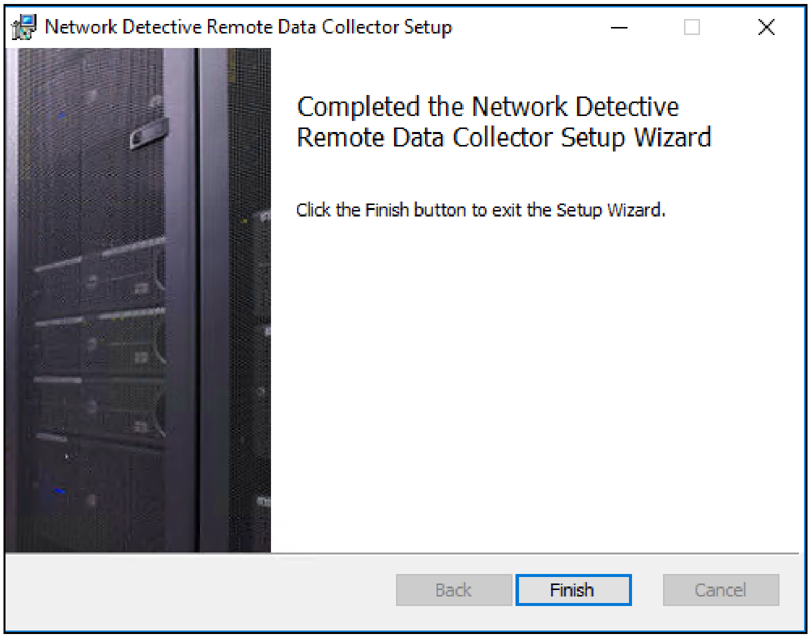
6. Click **Install** button to proceed with the installation and set up of the **Remote Data Collector**.



Ready to install Network Detective Remote Data Collector

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

7. When the install is complete, click **Finish**.

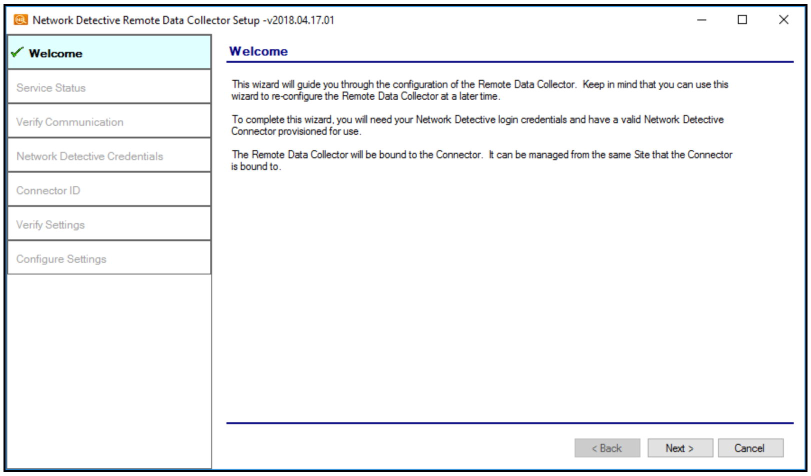


Completed the Network Detective Remote Data Collector Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 2 — Set Up Remote Data Collector on Client Network

1. When the install is complete, the Remote Data Collector setup window will then appear. Click **Next**.



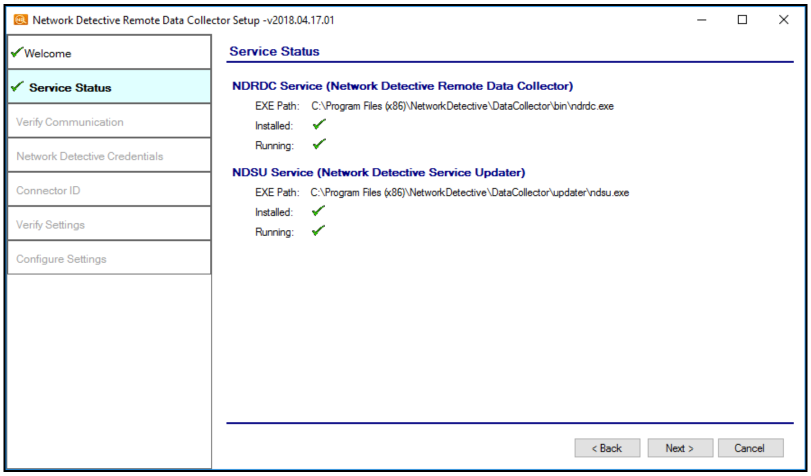
Welcome

This wizard will guide you through the configuration of the Remote Data Collector. Keep in mind that you can use this wizard to re-configure the Remote Data Collector at a later time.

To complete this wizard, you will need your Network Detective login credentials and have a valid Network Detective Connector provisioned for use.

The Remote Data Collector will be bound to the Connector. It can be managed from the same Site that the Connector is bound to.

2. During this step, the **Remote Data Collector** and **Service Updater** programs will be installed. Once the Installer confirms the installation of each program, click **Next**.



Service Status

NDRDC Service (Network Detective Remote Data Collector)

EXE Path: C:\Program Files (x86)\NetworkDetective\DataCollector\bin\ndrdc.exe

Installed: ✓

Running: ✓

NDSU Service (Network Detective Service Updater)

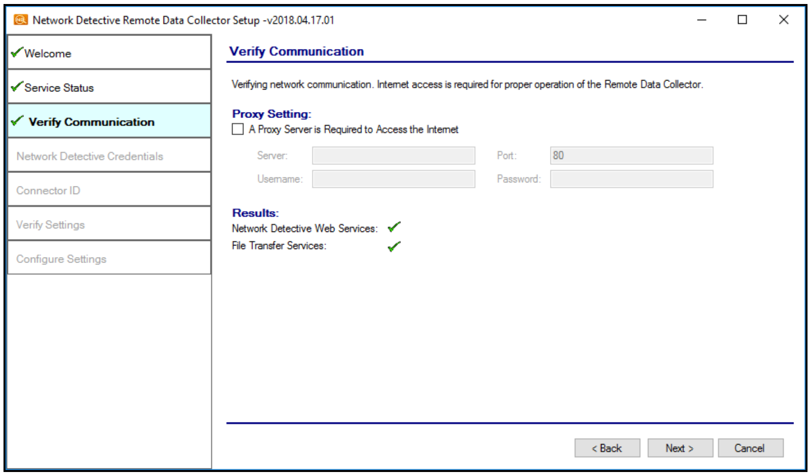
EXE Path: C:\Program Files (x86)\NetworkDetective\DataCollector\updater\ndsu.exe

Installed: ✓

Running: ✓

3. In this step, the RDC will verify that the computer that will host the data collector can communicate with the Network Detective web and file transfer services. Click **Next**.

Note: If you are using a proxy server, enter the required credentials and connection information.



Verify Communication

Verifying network communication. Internet access is required for proper operation of the Remote Data Collector.

Proxy Setting:

□ A Proxy Server is Required to Access the Internet

Server:

Port: 80

Username:

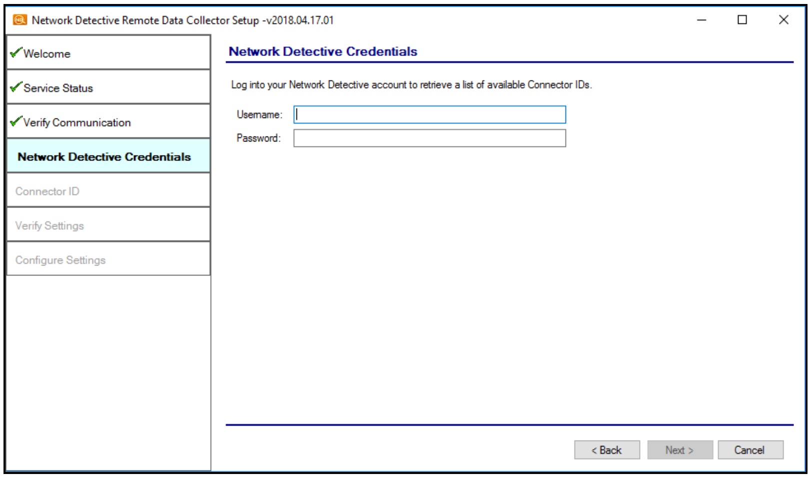
Password:

Results:

Network Detective Web Services: ✓

File Transfer Services: ✓

4. Next you will need to link the RDC to your chosen Site in Network Detective. To do this, first enter your Network Detective credentials and click **Next**.



Network Detective Credentials

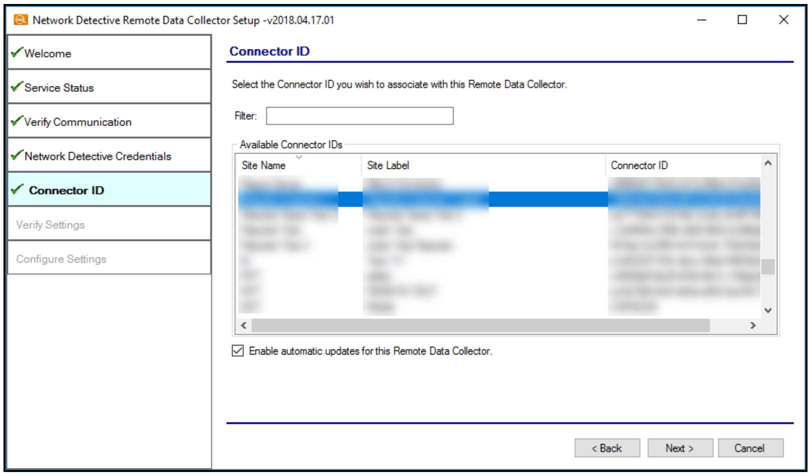
Log into your Network Detective account to retrieve a list of available Connector IDs.

Username:

Password:

5. Scroll through the list of **Sites** associated with your Network Detective account. Select the **Site/Connector ID** with which to associate the Data Collector. This will be the Reporter Site that will receive regular data from the RDC scans. Click **Next**.

> **Note:** You must set up a Client Connector in the Network Detective application before you can complete this step.



Connector ID

Select the Connector ID you wish to associate with this Remote Data Collector.

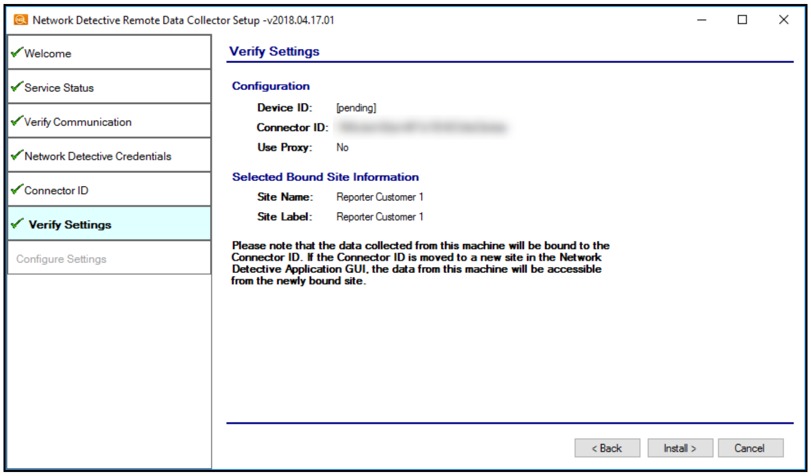
Filter:

Available Connector IDs

Site Name	Site Label	Connector ID
[redacted]	[redacted]	[redacted]

☑ Enable automatic updates for this Remote Data Collector.

6. Review the **Remote Data Collector's** configuration settings and verify they are correct.



Verify Settings

Configuration

Device ID: [pending]

Connector ID: [redacted]

Use Proxy: No

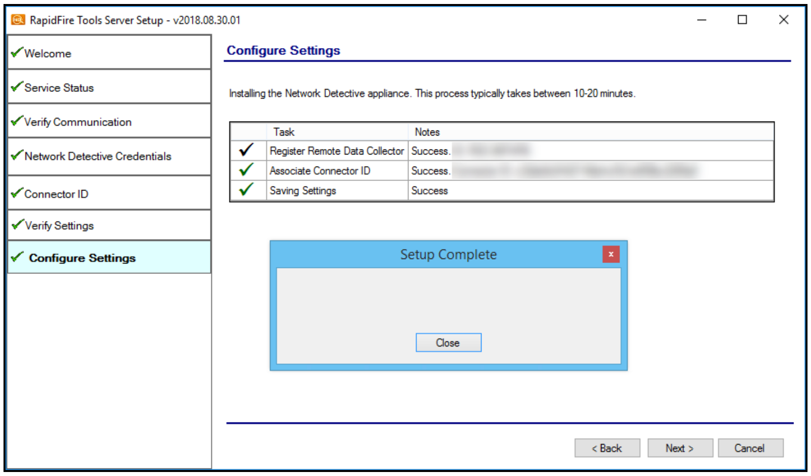
Selected Bound Site Information

Site Name: Reporter Customer 1

Site Label: Reporter Customer 1

Please note that the data collected from this machine will be bound to the Connector ID. If the Connector ID is moved to a new site in the Network Detective Application GUI, the data from this machine will be accessible from the newly bound site.

7. Select the **Back** button to correct any configuration issues, or click **Next** to finalize the setup.
8. After the **Remote Data Collector** (RDC) application is set up, you will be notified that the RDC is ready for use.



RapidFire Tools Server Setup - v2018.08.30.01

Configure Settings

Installing the Network Detective appliance. This process typically takes between 10-20 minutes.

	Task	Notes
✓	Register Remote Data Collector	Success. [redacted]
✓	Associate Connector ID	Success. [redacted]
✓	Saving Settings	Success

Setup Complete

When you complete these steps, proceed to "Configure Remote Data Collector to Perform Scan Tasks" on the next page.

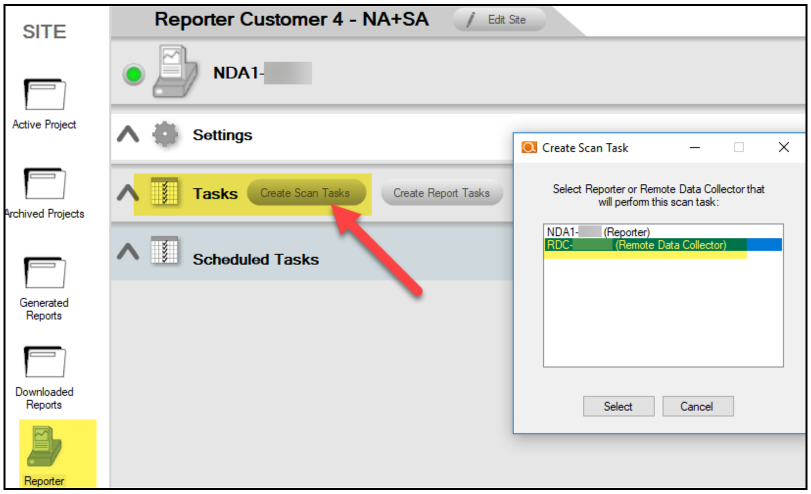
Configure Remote Data Collector to Perform Scan Tasks

In order to generate automated assessment reports using Reporter, you will need to configure the Remote Data Collector to perform scheduled scans on the client's network. This gives Reporter the data it needs to generate documentation.

To create scan tasks, perform the following steps:

1. Click on the **Reporter** button on the left side of the Site screen.

2. From the **Tasks** bar, click **Create Scan Tasks**.

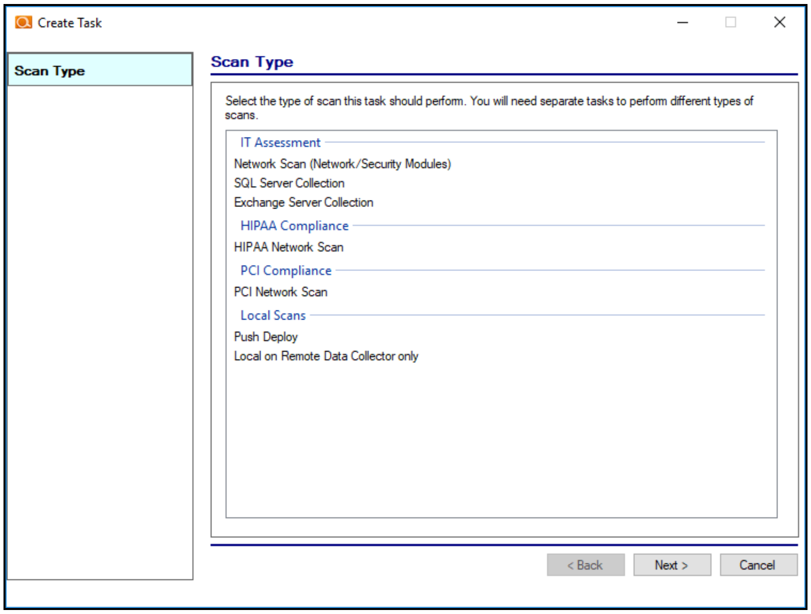


Select Reporter or Remote Data Collector that will perform this scan task:

NDA1-[redacted] (Reporter)
RDC-[redacted] (Remote Data Collector)

3. **Select** the **Remote Data Collector(s)** available for the Site. *If you don't see any RDCs, be sure you installed them correctly.*

   The **Create Task** window will be displayed.



Create Task

Scan Type

Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

IT Assessment

Network Scan (Network/Security Modules)
SQL Server Collection
Exchange Server Collection

HIPAA Compliance

HIPAA Network Scan

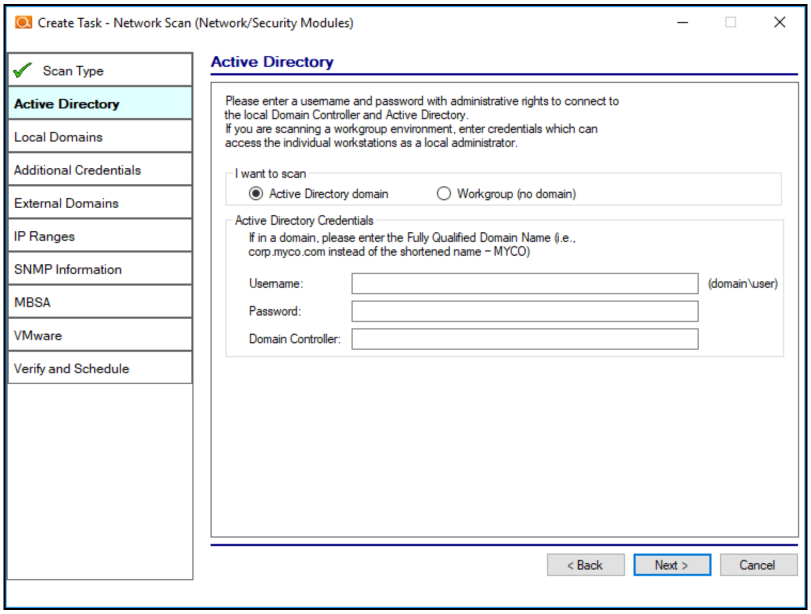
PCI Compliance

PCI Network Scan

Local Scans

Push Deploy
Local on Remote Data Collector only

4. Follow the wizard and enter the necessary scan settings. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for more details (Network, Security, HIPAA, PCI, Exchange, and SQL scans).



Create Task - Network Scan (Network/Security Modules)

Active Directory

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory.
If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.

I want to scan

● Active Directory domain ○ Workgroup (no domain)

Active Directory Credentials

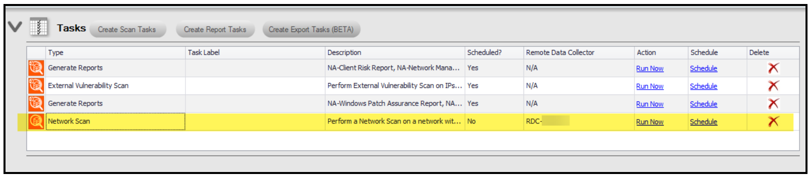
If in a domain, please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name – MYCO)

Username: (domain\user)

Password:

Domain Controller:

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

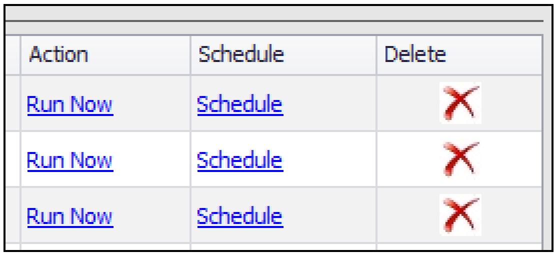


Tasks

Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Mana...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IPs...	Yes	N/A	Run Now	Schedule	✗
Generate Reports		NA-Windows Patch Assurance Report, NA...	Yes	N/A	Run Now	Schedule	✗
Network Scan		Perform a Network Scan on a network wit...	No	RDC-[redacted]	Run Now	Schedule	✗

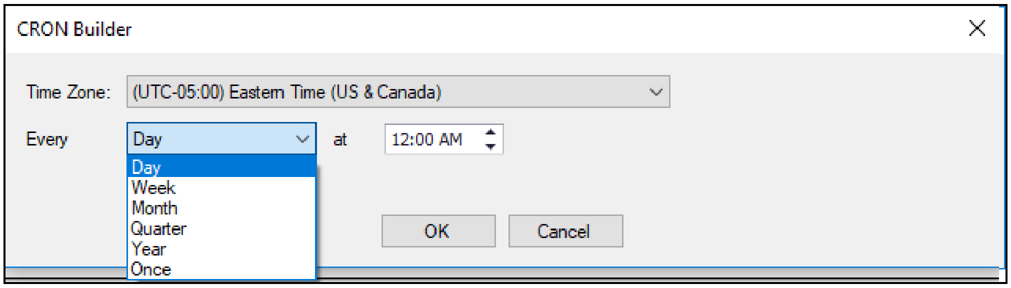
5. In order to initiate the scan, you will need to move the scan from the Task list into **Scheduled Tasks**. There are two ways to do this:

   a. Select the **Run Now** option link under the **Action** column to initiate the scan. This will place the scan directly into the **Scheduled Tasks** list, and *the scan will begin immediately*.



Action	Schedule	Delete
Run Now	Schedule	✗
Run Now	Schedule	✗
Run Now	Schedule	✗

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

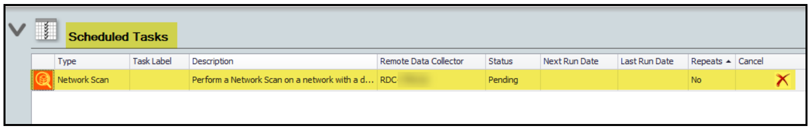


CRON Builder

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

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



Scheduled Tasks

Type	Task Label	Description	Remote Data Collector	Status	Next Run Date	Last Run Date	Repeats	Cancel
Network Scan		Perform a Network Scan on a network with a d...	RDC[redacted]	Pending			No	✗

Tip: Continue creating and scheduling scan tasks for the Site. You will need to create and schedule the correct scan tasks for the reports you wish to automate. If you don't perform the correct scans, your reports won't have the necessary information. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for specific instructions for setting up the various types of scans.

To continue setting up Reporter, proceed to "Configure Reporter to Access Scan Data and Generate Reports" on the next page.

Configure Reporter to Access Scan Data and Generate Reports

This section covers the last step in setting up Reporter: configuring Reporter to access the scan data provided by the Remote Data Collector to schedule, generate, and deliver automated reports.

Before proceeding, be sure that you have completed these earlier steps:

- "Initial Reporter Set Up" on page 16
- "Initial Remote Data Collector Set Up" on page 21
- "Configure Remote Data Collector to Perform Scan Tasks" on page 30

Note: Before proceeding, also be sure that you have completed a scan on the client's network using the Remote Data Collector (RDC). The steps below including verifying that the RDC scan data can be successfully uploaded to the Reporter in order to generate reports.

Then follow the steps below:

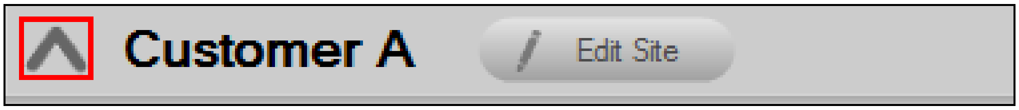
Step 1 — Verify connection to Remote Data Collector

Verify that the **Remote Data Collector scans** have been uploaded to the **Secure Cloud Storage Area** and can be accessed via the **Client-Connector**.

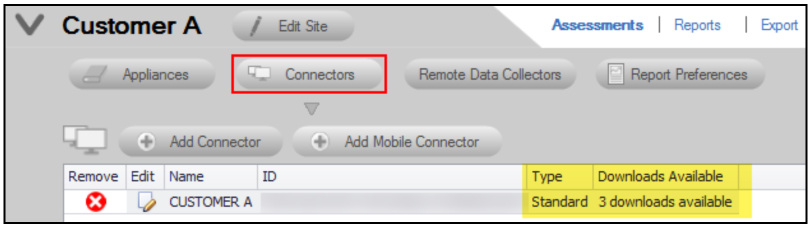
Tip: See "Client-Connector Diagram" on page 228 for a helpful picture of how this process works.

To do this:

1. If you have not done so already, run a test scan on your client’s network using the Remote Data Collector.
2. Open the Network Detective **Site** associated with the **Reporter**.
3. Click the selector ⌃ symbol to expand the **Site** properties view.



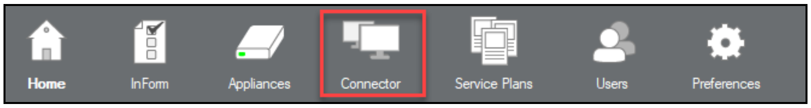
4. Click **Connectors**.
5. View the **Connectors** associated with the **Site**.
6. View the **Downloads Available** status indicator within the list of **Client-Connectors** associated with the **Site**. *If there are downloads available, this means the RDC is successfully uploading completed scans to Network Detective.*



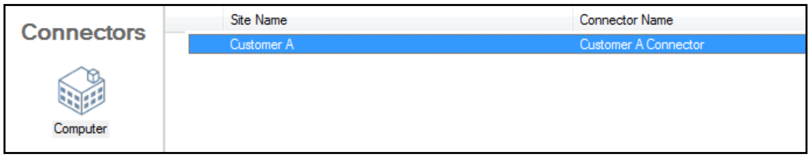
Remove	Edit	Name	ID	Type	Downloads Available
✖	✎	CUSTOMER A	[redacted]	Standard	3 downloads available

Alternatively, you can:

1. Click the **Connector** icon on the Network Detective menu bar. A list of available **Client-Connectors** will be presented.



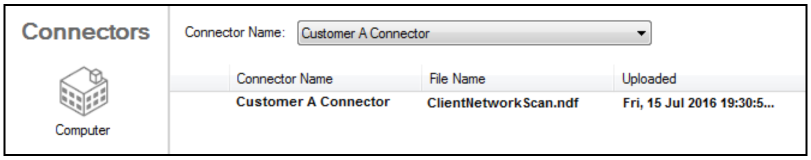
2. Double-click on the **Client-Connector** that is **Associated** with the **Site** you are using with the **Reporter Appliance**.



Site Name	Connector Name
Customer A	Customer A Connector

3. The list of scan files that have been uploaded to the **Secure Client Storage Area** for use by the **Reporter Appliance** will be listed for the **Client-Connector**

associated with your assessment's **Site**.



Connector Name: Customer A Connector

Connector Name	File Name	Uploaded
Customer A Connector	ClientNetworkScan.ndf	Fri, 15 Jul 2016 19:30:5...

Important: If you can't find scan data, be sure that:

- The Remote Data Collector is installed correctly
- You associated the RDC with the correct Site by selecting the correct Client-Connector during the installation process
- The Remote Data Collector is configured to perform scans on the client network

Step 2 — Schedule an External Vulnerability Scan (OPTIONAL)

The External Vulnerability Scan enhances your assessment reports by gathering information about the target network's external vulnerabilities.

The **External Vulnerability Scan** feature within **Reporter** can only be used with the following modules:

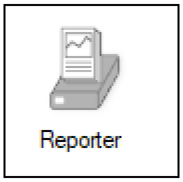
- Security Assessment Module
- HIPAA Compliance Assessment Module
- PCI Compliance Assessment Module

Note: You only need to create one External Vulnerability Scan task for each site and/or set of external IPs you wish to scan. Reporter can use this scan data to generate multiple sets of reports.

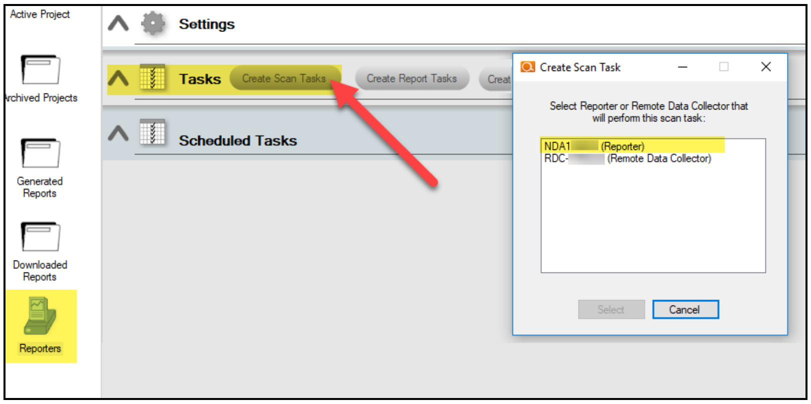
Important: You can schedule this scan to occur whenever you'd like. However, be sure to schedule the external vulnerability scan several hours BEFORE you assign Reporter to generate reports. This will ensure Reporter has the latest scan data to generate reports.

To create the External Vulnerability Scan task, perform the following steps:

1. Click on the **Reporter** button on the left side of the Site screen.



2. From the **Tasks** bar, click **Create Scan Tasks**.



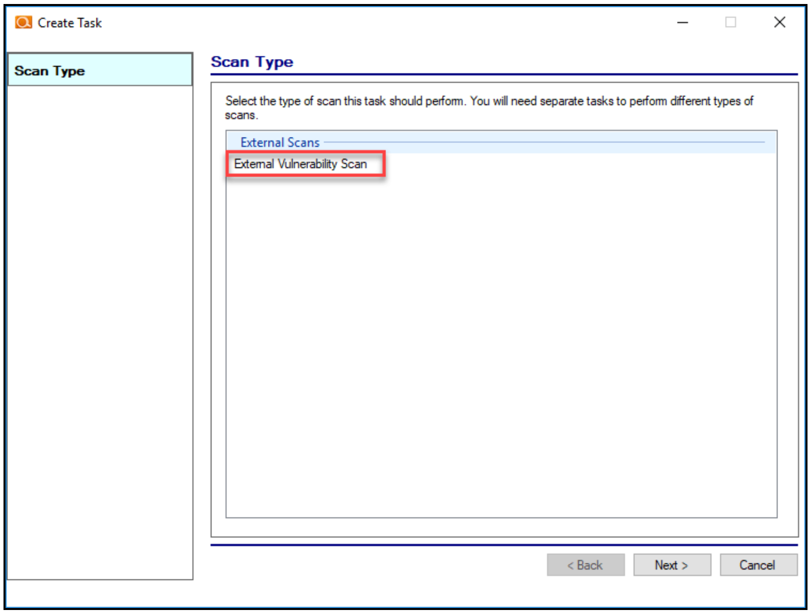
Select Reporter or Remote Data Collector that will perform this scan task:

NDA1[redacted] (Reporter)
RDC-[redacted] (Remote Data Collector)

3. **Select** the **Reporter** available for the Site.

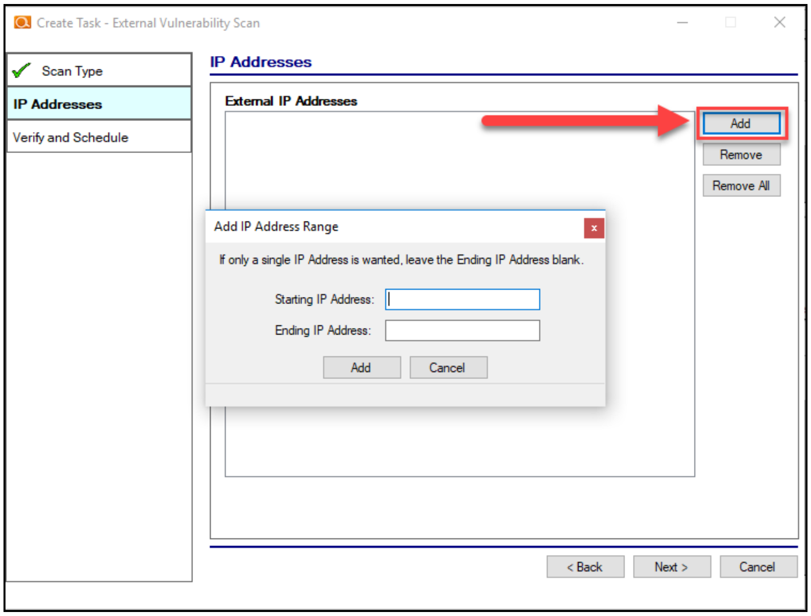
Set up the External Vulnerability Scan

1. Choose **External Vulnerability scan** from the wizard and click the **Next** button.



Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

2. Select the **Add** button in the **Create Task – External Vulnerability Scan** window to add the IP address range to be scanned.

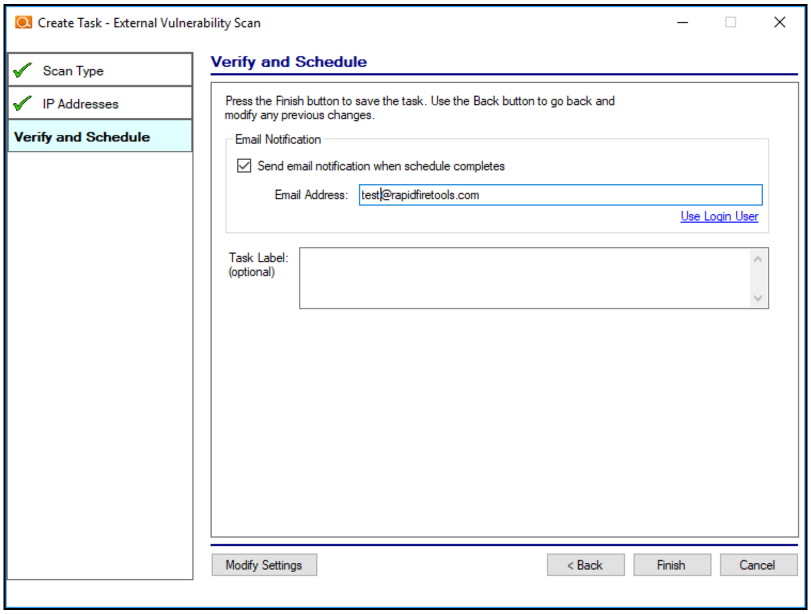


If only a single IP Address is wanted, leave the Ending IP Address blank.

Starting IP Address:

Ending IP Address:

3. Enter the IP address range and select the **Add** button to add the IP addresses to the **External IP Addresses** list.
4. Select the **Next** button to continue. The **Verify and Schedule** window will be displayed.



Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

☑ Send email notification when schedule completes

Email Address: test@rapidfiretools.com

Task Label: (optional)

5. If an **Email Notification** should be sent after the scan is complete, then:

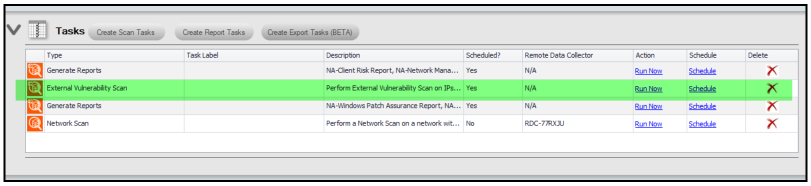
a. select the **Send Email Notification** option

b. type in the Email address for the recipient of the **Notification**

> **Note:** Scans can take several hours to complete. The designated recipient of scan completion notifications will receive an e-mail when the **External Vulnerability Scan** is complete.

6. Select the **Finish** button to complete the scan's configuration

7. The **External Vulnerability Scan** will now be listed in the **Manage Appliance** window within the **Task Library** list.



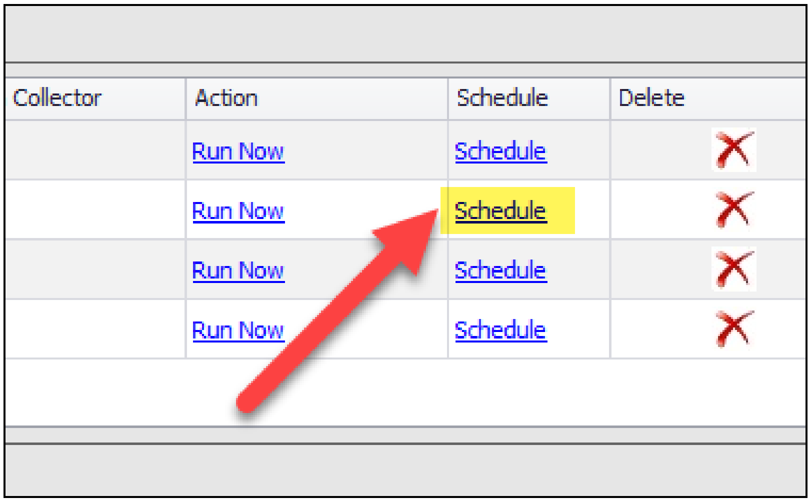
Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Mana...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IPs...	Yes	N/A	Run Now	Schedule	✗
Generate Reports		NA-Windows Patch Assurance Report, NA...	Yes	N/A	Run Now	Schedule	✗
Network Scan		Perform a Network Scan on a network wit...	No	RDC-77RXJU	Run Now	Schedule	✗

8. Next, click **Run Now** or **Schedule** to initialize the scan immediately - or at a regular scheduled time.

Schedule the External Vulnerability Scan

1. Click on **Schedule** link to open the **CRON Builder** window. The **CRON Builder** is used to schedule the running of scans.

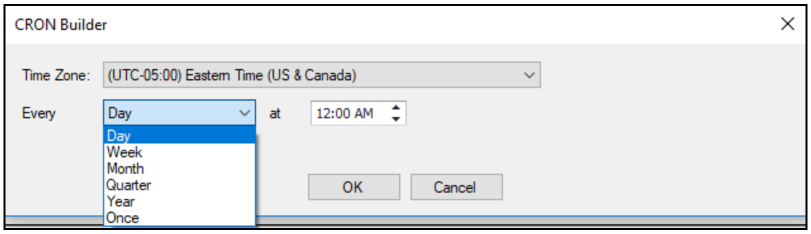
> **Important:** You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external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



Collector	Action	Schedule	Delete
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗

Scans can be set to run **daily**, **weekly**, **monthly**, **quarterly**, **annually**, or **just once**. You may also set the time of the day that the scan should be initiated.

Note: Please note that the time zone used for the CRON Builder time is Eastern Standard Time (EST).

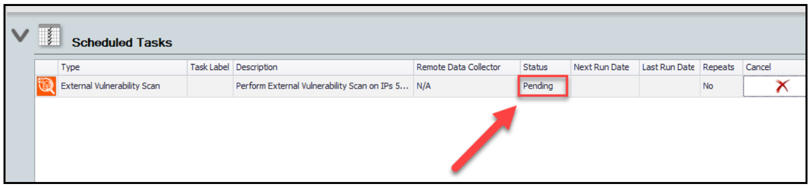


CRON Builder

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

2. Set the scan frequency by selecting one option from **Every** list (i.e. day, week, month, year, or once)
3. Next set the "**on the**" by selecting a day that the scan should be performed.
4. Then set the time of the day that the scan should run by setting the "**at**" time.



Scheduled Tasks

Type	Task Label	Description	Remote Data Collector	Status	Next Run Date	Last Run Date	Repeats	Cancel
External Vulnerability Scan		Perform External Vulnerability Scan on IPs 5...	N/A	Pending			No	✗

5. Click on **OK** to save the scan **Schedule**. The scheduled scan task will then be listed in the **Scheduled Tasks** list as a **Pending** task.

> **Note:** When the scan starts, the task **Status** will be set to **Running** within the **Scheduled Tasks** list.

Step 3 — Configure Automatic Report Generation

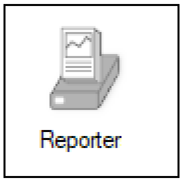
Below is an overview of the steps required to set up **Reporter** to enable **Automatic Report Generation** for the following Assessment types:

- Network Assessments
- Security Assessments
- SQL Server Assessments
- Microsoft Exchange and Office 365 Mail Assessments
- HIPAA Compliance Assessments
- PCI Compliance Assessments

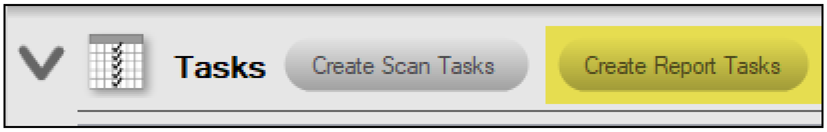
> **Tip:** If you want to quickly set up report tasks for multiple sites, you can use "Reporter Templates" on page 150.

To start setting up automated reports:

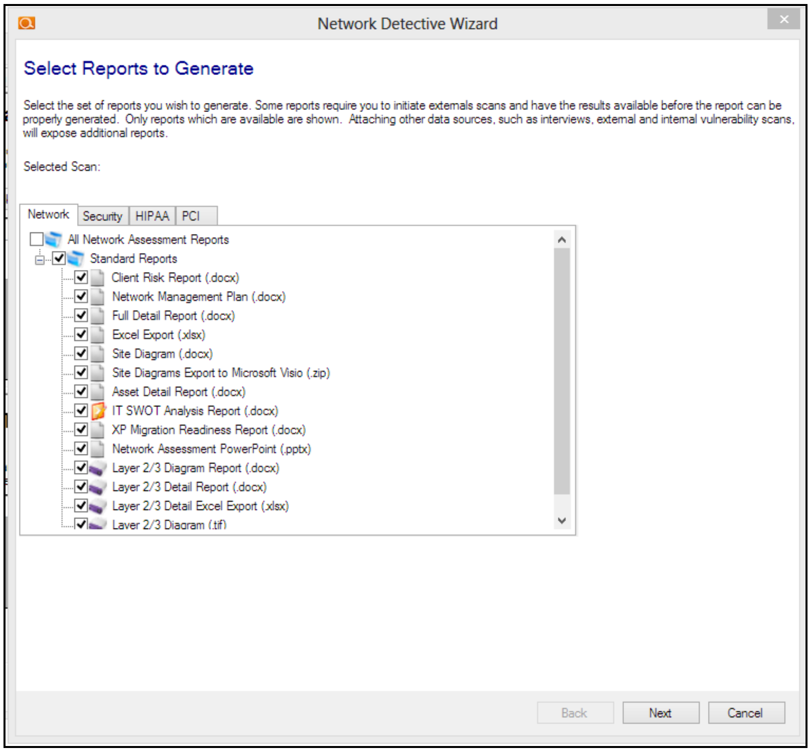
1. **Start** new **Assessment**, or, **Open** an **Archived Assessment** for use on your Reporter Site.
2. Click on the **Reporter** icon to open the Reporter dashboard.



3. Click **Create Report Tasks**.



4. Select the Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



Network Detective Wizard

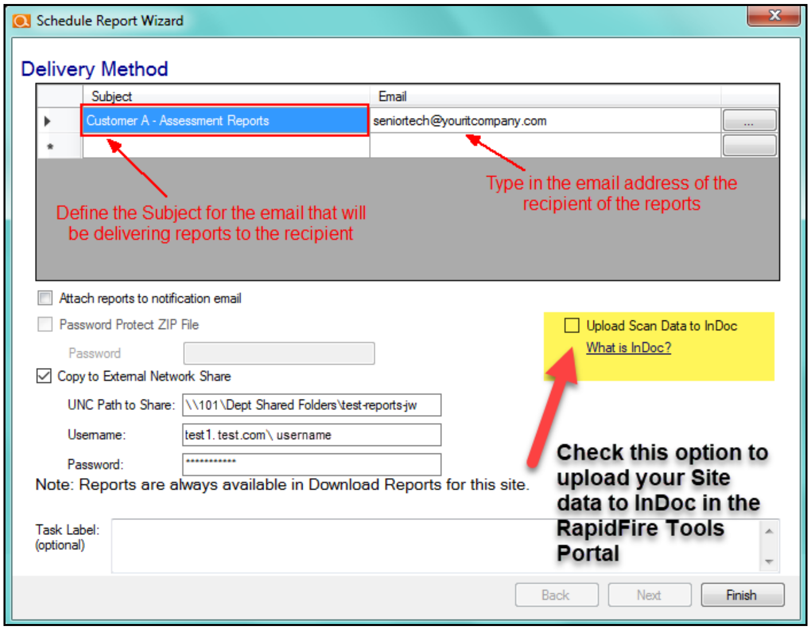
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- □ All Network Assessment Reports
  - ☑ Standard Reports
    - ☑ Client Risk Report (.docx)
    - ☑ Network Management Plan (.docx)
    - ☑ Full Detail Report (.docx)
    - ☑ Excel Export (.xlsx)
    - ☑ Site Diagram (.docx)
    - ☑ Site Diagrams Export to Microsoft Visio (.zip)
    - ☑ Asset Detail Report (.docx)
    - ☑ IT SWOT Analysis Report (.docx)
    - ☑ XP Migration Readiness Report (.docx)
    - ☑ Network Assessment PowerPoint (.pptx)
    - ☑ Layer 2/3 Diagram Report (.docx)
    - ☑ Layer 2/3 Detail Report (.docx)
    - ☑ Layer 2/3 Detail Excel Export (.xlsx)
    - ☑ Layer 2/3 Diagram (.tif)

5. Next, set the **Delivery Method** for the Reports. In this window you can:



Schedule Report Wizard

Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@youritcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

□ Attach reports to notification email

□ Password Protect ZIP File

Password:

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\ username

Password: ***********

Note: Reports are always available in Download Reports for this site.

□ Upload Scan Data to InDoc

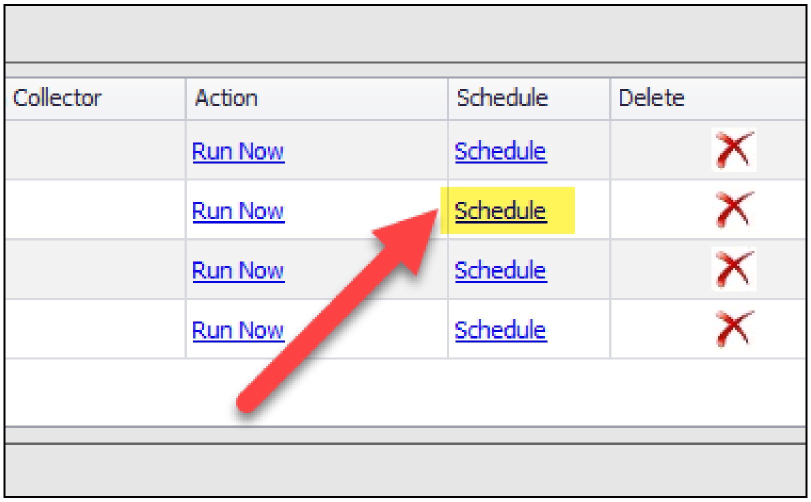
What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient
- set if you want to send the reports attached to the Report notification email message
- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

6. After defining the **Delivery Method** settings, click on the **Finish** button.
7. Click on the **Schedule** link in order to schedule the created **Report Task for a time which is certain to be after the scan is complete and uploaded to the Secure Cloud Storage Area by the Client-Connector**.



Collector	Action	Schedule	Delete
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗

Important: **Reporter's** automated report generation engine will use whatever data is available to the **Reporter** for downloading from the **Secure Cloud Storage Area** based on the most recent scan that has been completed and uploaded using the **Client-Connector**.

Therefore, if the scan of your client's network is not complete and uploaded to the **Secure Cloud Storage Area** using the **Client-Connector**, then the reports will not have the most recent scan's data either.

If the user has specified that reports be delivered by email, the specified email address should receive an email with a .zip file of the reports attached as long as the zip file **is less than 5 MB in size**.

Tip: See "Setting Up Automatic Reports by Assessment Module" on the next page for specific instructions on setting up reports for each assessment module (Network, Security, SQL, Exchange, HIPAA, and PCI).

Setting Up Automatic Reports by Assessment Module

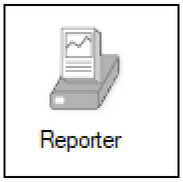
This section covers everything you need to know about setting up automatic reports using Reporter.

Network Assessment Automatic Reports

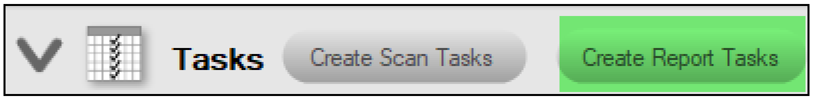
Note: Before you set up automated Network Assessment reports, be sure you set up recurring Network Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **Network/Security Assessment Scan**, 2) **Push Deploy Computer Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.

To set up automatically generated reports for the Network Assessment Module:

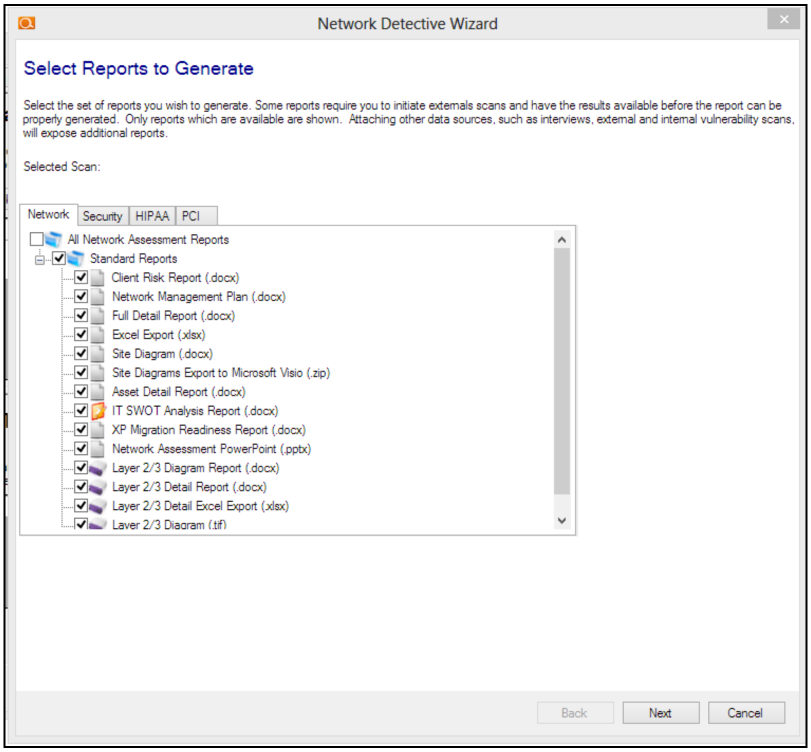
1. Click on the **Reporter** icon to open the Reporter dashboard.



2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the Network Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



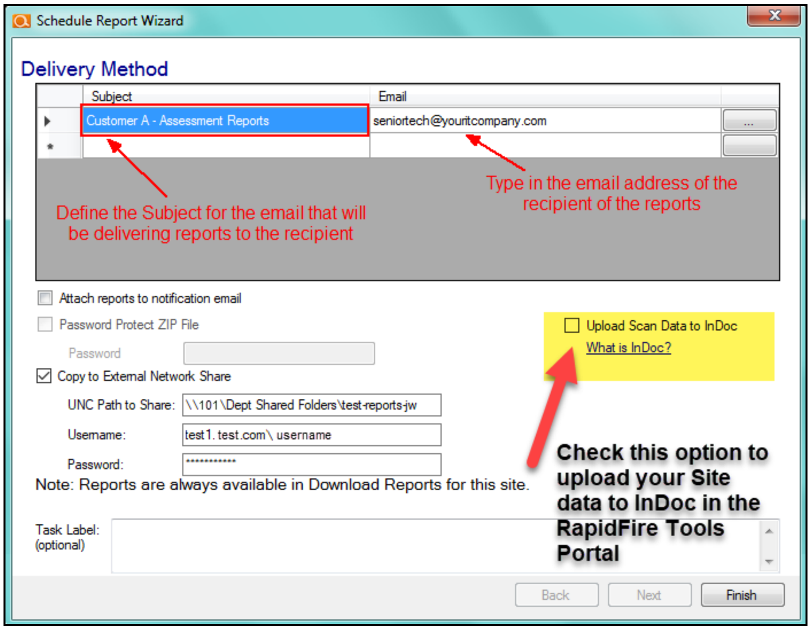
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- □ All Network Assessment Reports
  - ☑ Standard Reports
    - ☑ Client Risk Report (.docx)
    - ☑ Network Management Plan (.docx)
    - ☑ Full Detail Report (.docx)
    - ☑ Excel Export (.xlsx)
    - ☑ Site Diagram (.docx)
    - ☑ Site Diagrams Export to Microsoft Visio (.zip)
    - ☑ Asset Detail Report (.docx)
    - ☑ IT SWOT Analysis Report (.docx)
    - ☑ XP Migration Readiness Report (.docx)
    - ☑ Network Assessment PowerPoint (.pptx)
    - ☑ Layer 2/3 Diagram Report (.docx)
    - ☑ Layer 2/3 Detail Report (.docx)
    - ☑ Layer 2/3 Detail Excel Export (.xlsx)
    - ☑ Layer 2/3 Diagram (.tif)

4. Next, set the **Delivery Method** for the Reports. In this window you can:



Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@yourtcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

□ Attach reports to notification email

□ Password Protect ZIP File

Password

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\username

Password: ***********

□ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

Note: Reports are always available in Download Reports for this site.

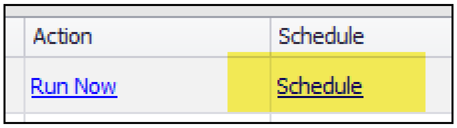
Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient

- set if you want to send the reports attached to the Report notification email message
- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

Tip: Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

5. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
6. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

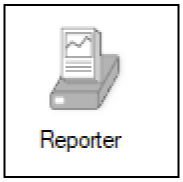
Important: You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

Security Assessment Automatic Reports

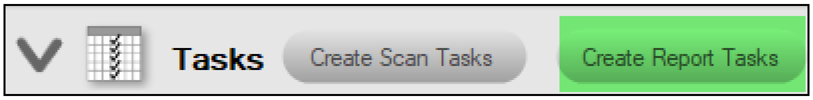
> **Note:** Before you set up automated Security Assessment reports, be sure you set up recurring Security Assessment scans using the Remote Data Collector and Reporter appliance. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **Network/Security Assessment Scan**, 2) **Push Deploy Security Scan**, 3) **External Vulnerability Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.

To set up automatically generated reports for the Security Assessment Module:

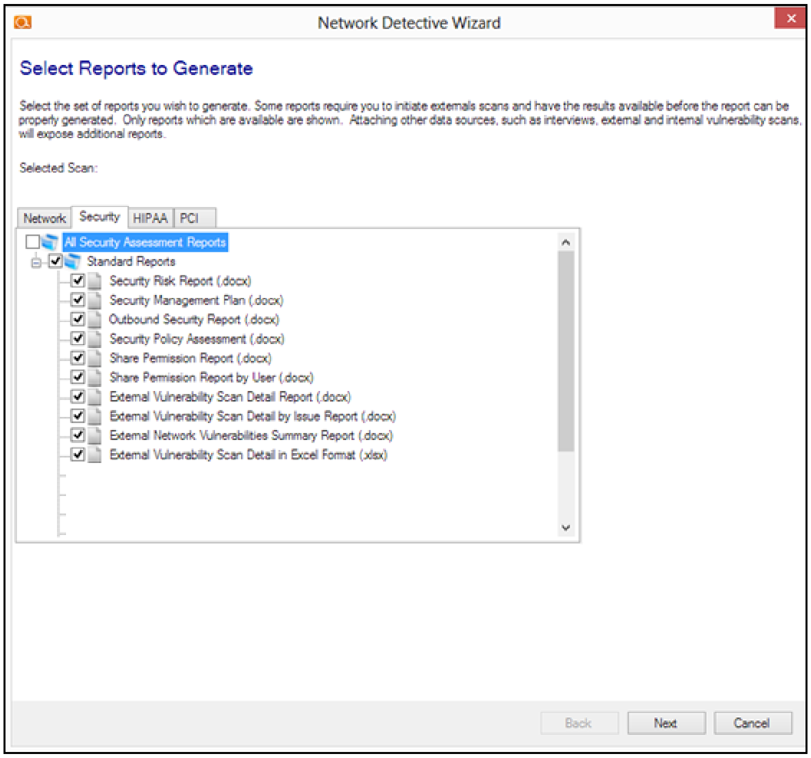
1. Click on the **Reporter** icon to open the Reporter dashboard.



2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the Network Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



Network Detective Wizard

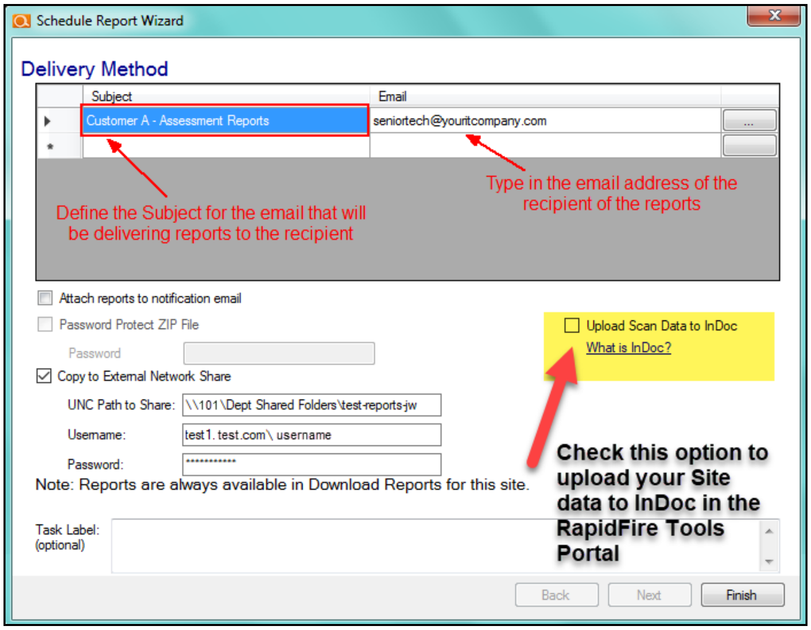
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- □ All Security Assessment Reports
  - ☑ Standard Reports
    - ☑ Security Risk Report (.docx)
    - ☑ Security Management Plan (.docx)
    - ☑ Outbound Security Report (.docx)
    - ☑ Security Policy Assessment (.docx)
    - ☑ Share Permission Report (.docx)
    - ☑ Share Permission Report by User (.docx)
    - ☑ External Vulnerability Scan Detail Report (.docx)
    - ☑ External Vulnerability Scan Detail by Issue Report (.docx)
    - ☑ External Network Vulnerabilities Summary Report (.docx)
    - ☑ External Vulnerability Scan Detail in Excel Format (.xlsx)

4. Next, set the **Delivery Method** for the Reports. In this window you can:



Schedule Report Wizard

Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@yourtcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

□ Attach reports to notification email

□ Password Protect ZIP File

Password:

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1. test.com\ username

Password: ***********

Note: Reports are always available in Download Reports for this site.

□ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

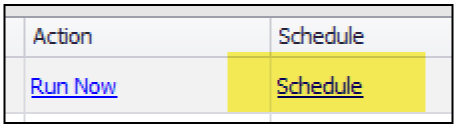
Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient

- set if you want to send the reports attached to the Report notification email message
- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

Tip: Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

5. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
6. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

Important: You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

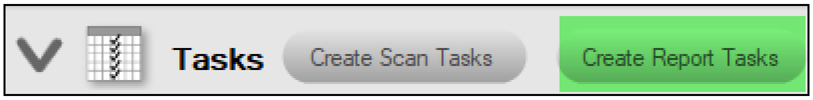
SQL Server Assessment Automatic Reports

Note: Before you set up automated SQL Server assessment reports, be sure you set up recurring SQL Server Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring **SQL Server Assessment Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.

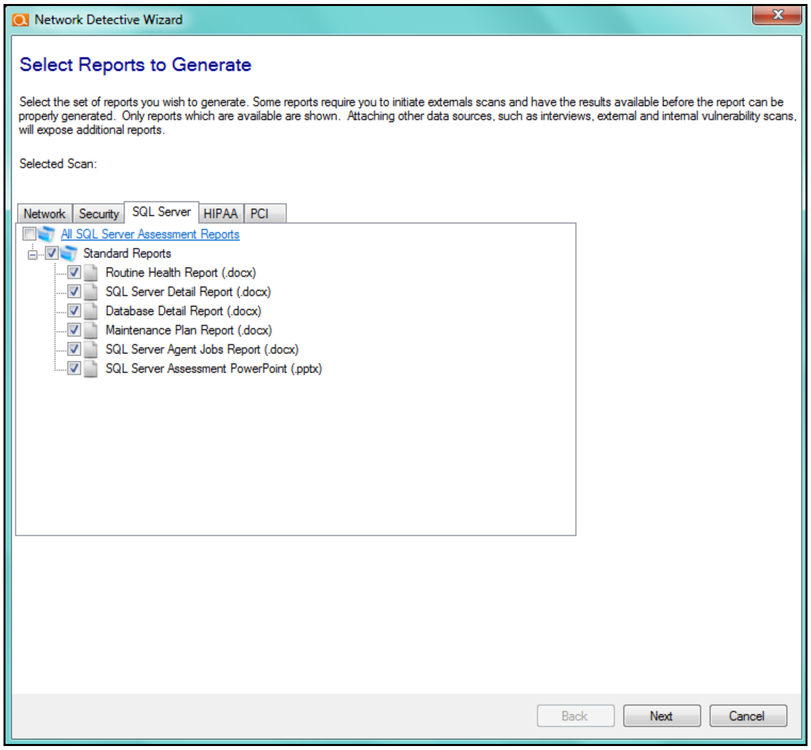
To set up automatically generated reports for the SQL Server Assessment Module:

1. Click on the **Reporter** icon to open the Reporter dashboard.

2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the SQL Server Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



Network Detective Wizard

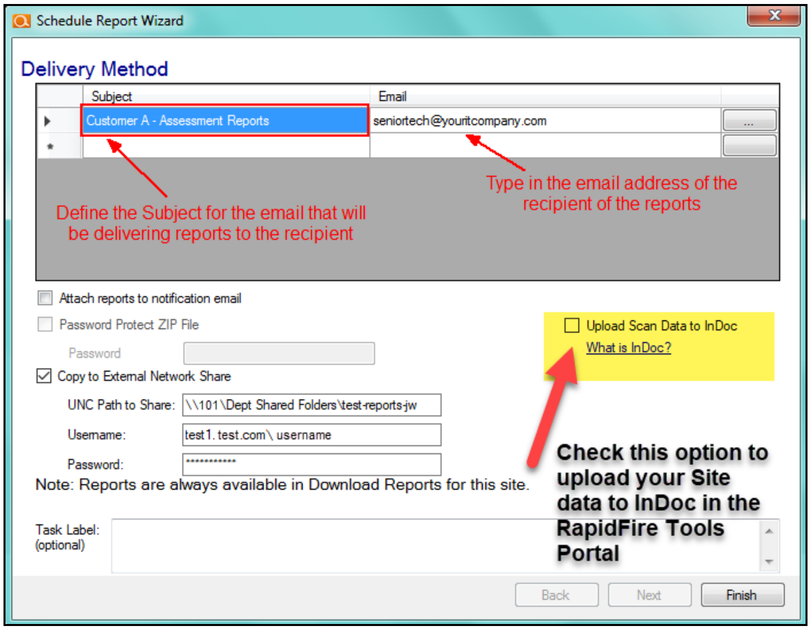
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- □ All SQL Server Assessment Reports
  - ☑ Standard Reports
    - ☑ Routine Health Report (.docx)
    - ☑ SQL Server Detail Report (.docx)
    - ☑ Database Detail Report (.docx)
    - ☑ Maintenance Plan Report (.docx)
    - ☑ SQL Server Agent Jobs Report (.docx)
    - ☑ SQL Server Assessment PowerPoint (.pptx)

4. Next, set the **Delivery Method** for the Reports. In this window you can:



Schedule Report Wizard

Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@youritcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

□ Attach reports to notification email

□ Password Protect ZIP File

Password:

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\username

Password: ***********

Note: Reports are always available in Download Reports for this site.

□ Upload Scan Data to InDoc

What is InDoc?

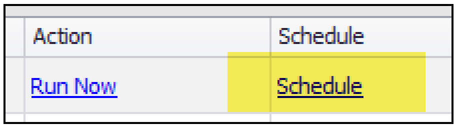
Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient
- set if you want to send the reports attached to the Report notification email message
- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

Tip: Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

5. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
6. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

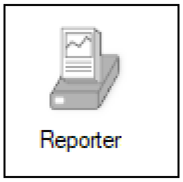
Important: You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

Exchange Assessments Automatic Reports – (Using the Exchange Data Collector and Windows Task Manager)

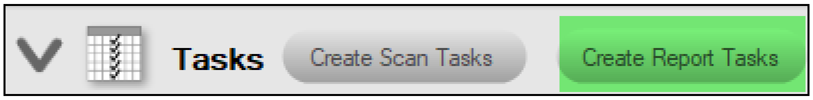
Note: Before you set up automated Exchange Assessment reports, be sure you set up recurring Exchange Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring **Exchange Assessment Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.

To set up automatically generated reports for the Exchange Assessment Module:

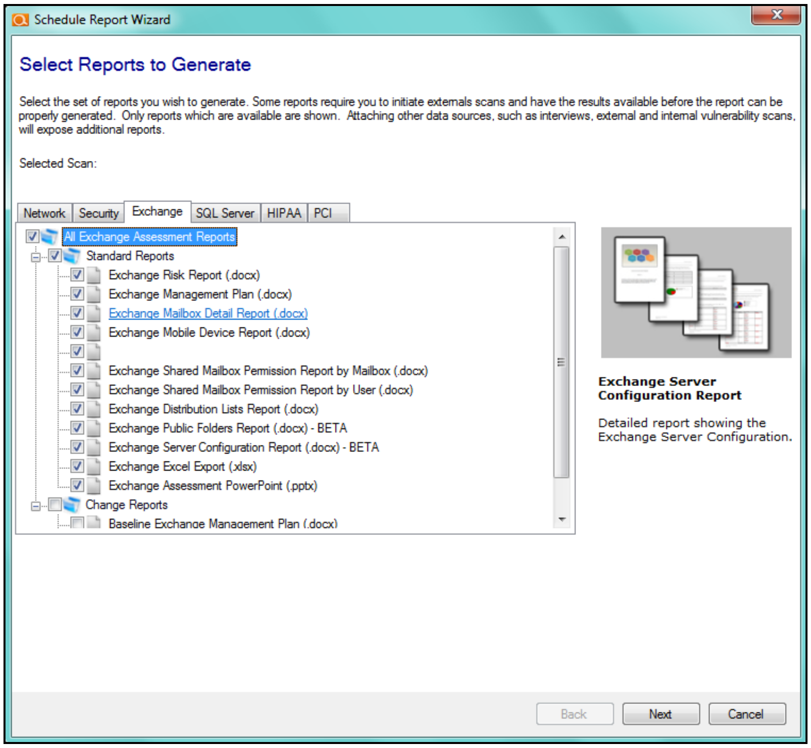
1. Click on the **Reporter** icon to open the Reporter dashboard.



2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the Exchange Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

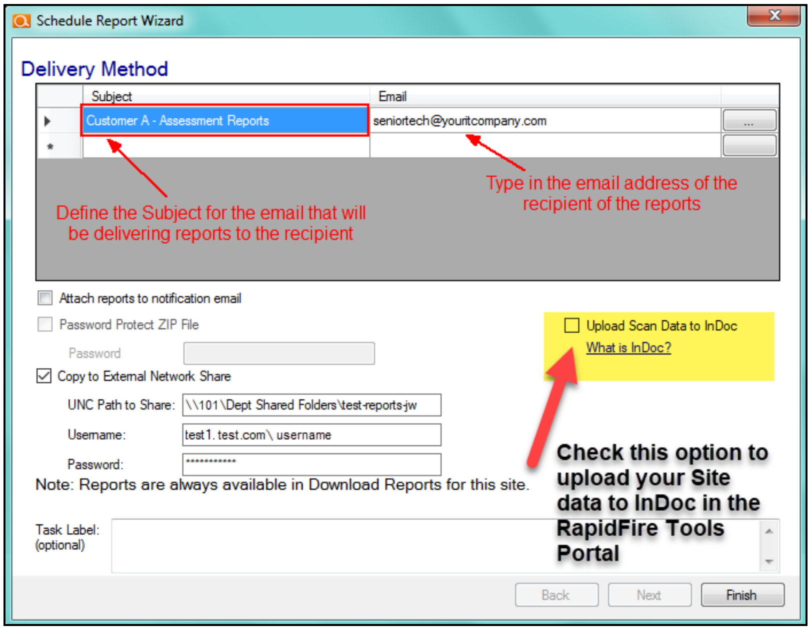
Selected Scan:

- ☑ All Exchange Assessment Reports
  - ☑ Standard Reports
    - ☑ Exchange Risk Report (.docx)
    - ☑ Exchange Management Plan (.docx)
    - ☑ Exchange Mailbox Detail Report (.docx)
    - ☑ Exchange Mobile Device Report (.docx)
    - ☑
    - ☑ Exchange Shared Mailbox Permission Report by Mailbox (.docx)
    - ☑ Exchange Shared Mailbox Permission Report by User (.docx)
    - ☑ Exchange Distribution Lists Report (.docx)
    - ☑ Exchange Public Folders Report (.docx) - BETA
    - ☑ Exchange Server Configuration Report (.docx) - BETA
    - ☑ Exchange Excel Export (.xlsx)
    - ☑ Exchange Assessment PowerPoint (.pptx)
  - □ Change Reports
    - □ Baseline Exchange Management Plan (.docx)

Exchange Server Configuration Report

Detailed report showing the Exchange Server Configuration.

4. Next, set the **Delivery Method** for the Reports. In this window you can:



Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@youritcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

□ Attach reports to notification email

□ Password Protect ZIP File

Password

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1. test.com\ username

Password: ************

Note: Reports are always available in Download Reports for this site.

□ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

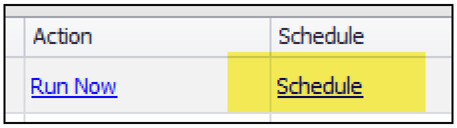
Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient

- set if you want to send the reports attached to the Report notification email message
- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

Tip: Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

5. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
6. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

Important: You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

HIPAA Compliance Assessment Automatic Reports

With Reporter, you can set up automatic HIPAA reports to produce regular, up-to-date compliance documentation. Once you set up automated scans and report tasks, you will only need to manually update your documentation in response to certain changes in the reporting environment, like new users or computers.

Before you set up automated HIPAA assessment reports, *you must first* complete a full HIPAA assessment that includes **external vulnerability scans**, **network scans**, **local push scans**, and the completion of all appropriate Inform-based **Surveys and Worksheets**. The user should be able to generate all **HIPAA Assessment Reports**. Once you've done this, here is the workflow for automating HIPAA compliance assessments with Reporter:

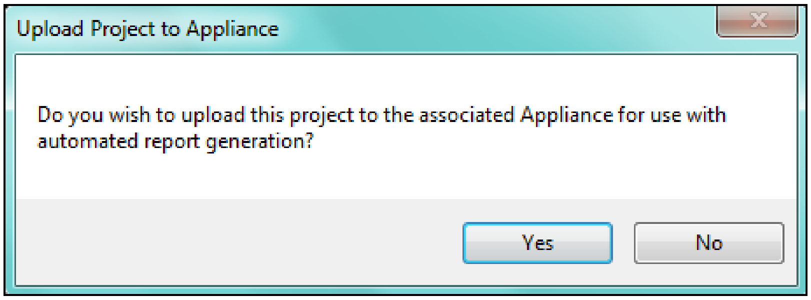
1. **Finish** the assessment, and then **Upload** the completed assessment with the Reporter appliance. This allows you use the finished assessment as the "baseline" for automated HIPAA reporting.
2. Set up recurring HIPAA assessment scans using the Remote Data Collector and Reporter. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **HIPAA Network Scan**, 2) **Push Deploy Computer Scan**, 3) **External Vulnerability Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.
3. Set up recurring HIPAA report tasks with Reporter.
4. Review exception report and update HIPAA worksheets.
5. Finish the updated HIPAA assessment and upload to Reporter.

Here are the steps with detailed instructions:

Step 1 — Finish and Upload Completed HIPAA Assessment Project to Reporter

The first step is to complete and finish a full HIPAA assessment. You should be able to generate all HIPAA assessment reports. Then:

1. Once satisfied with a complete **HIPAA Assessment**, press the “**Finish**” Assessment button.


Upload Project to Appliance

Do you wish to upload this project to the associated Appliance for use with automated report generation?

2. Confirm that you wish to **Upload Project to Appliance**(Reporter) to be used for automatic report generation. This allows you to use the finished assessment, including your completed worksheets, as the baseline for future assessments.

Step 2 — Create HIPAA Scan Tasks

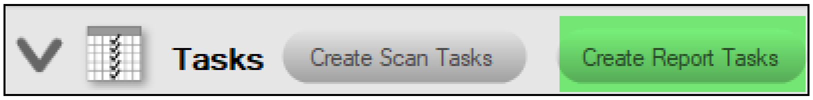
Now that you've completed the assessment and uploaded it to the appliance, it's time to create automatic scan tasks with Reporter and the Remote Data Collector. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for detailed instructions.

Step 3 — Create HIPAA Report Tasks

Next, you need to create automatic HIPAA report tasks with Reporter.

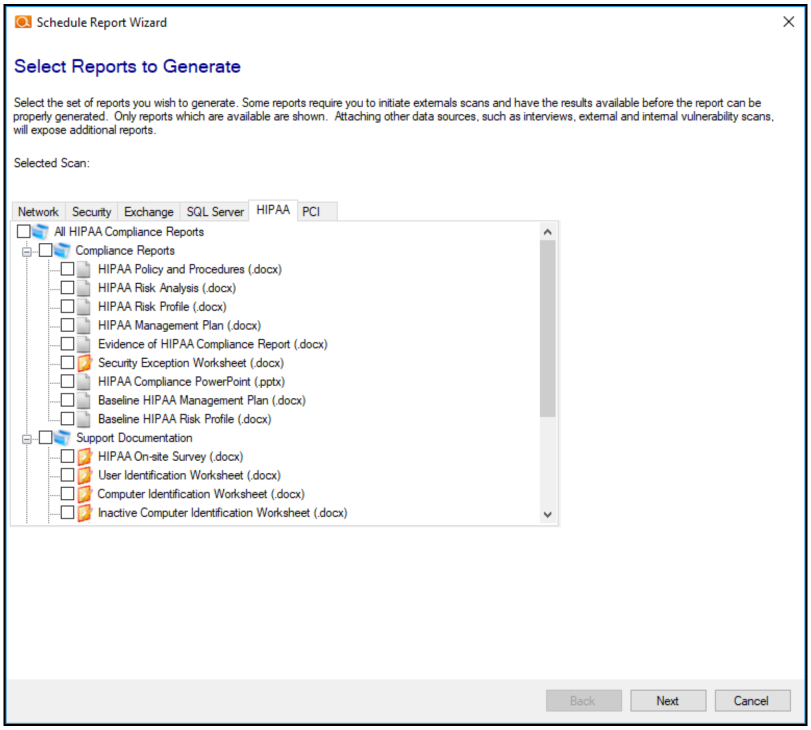
1. Click on the **Reporter** icon to open the Reporter dashboard.

2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the HIPAA Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.

4. From within the **Select Reports to Generate** window, select the **HIPAA Risk Profile Report** and any other **HIPAA Assessment** reports you would like to generate. Then select the **Next** button.



Schedule Report Wizard

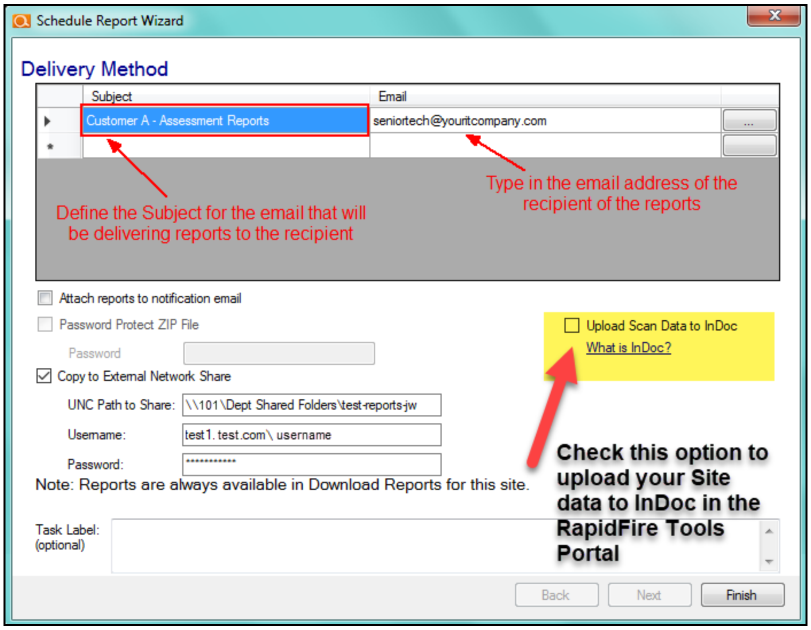
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- ☐ All HIPAA Compliance Reports
  - ☐ Compliance Reports
    - ☐ HIPAA Policy and Procedures (.docx)
    - ☐ HIPAA Risk Analysis (.docx)
    - ☐ HIPAA Risk Profile (.docx)
    - ☐ HIPAA Management Plan (.docx)
    - ☐ Evidence of HIPAA Compliance Report (.docx)
    - ☐ Security Exception Worksheet (.docx)
    - ☐ HIPAA Compliance PowerPoint (.pptx)
    - ☐ Baseline HIPAA Management Plan (.docx)
    - ☐ Baseline HIPAA Risk Profile (.docx)
  - ☐ Support Documentation
    - ☐ HIPAA On-site Survey (.docx)
    - ☐ User Identification Worksheet (.docx)
    - ☐ Computer Identification Worksheet (.docx)
    - ☐ Inactive Computer Identification Worksheet (.docx)

5. Next, set the **Delivery Method** for the Reports. In this window you can:



Schedule Report Wizard

Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@yourtcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

☐ Attach reports to notification email

☐ Password Protect ZIP File

Password:

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\ username

Password: ***********

Note: Reports are always available in Download Reports for this site.

☐ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

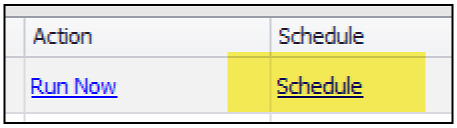
Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient
- set if you want to send the reports attached to the Report notification email message

- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

Tip: Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

6. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
7. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

Important: You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

Step 4 — Review and Update HIPAA Exception Report and Update InForms

After you finish your assessment and set up automatic HIPAA scanning and reporting, you will receive updated HIPAA documentation through email or whatever delivery method you choose.

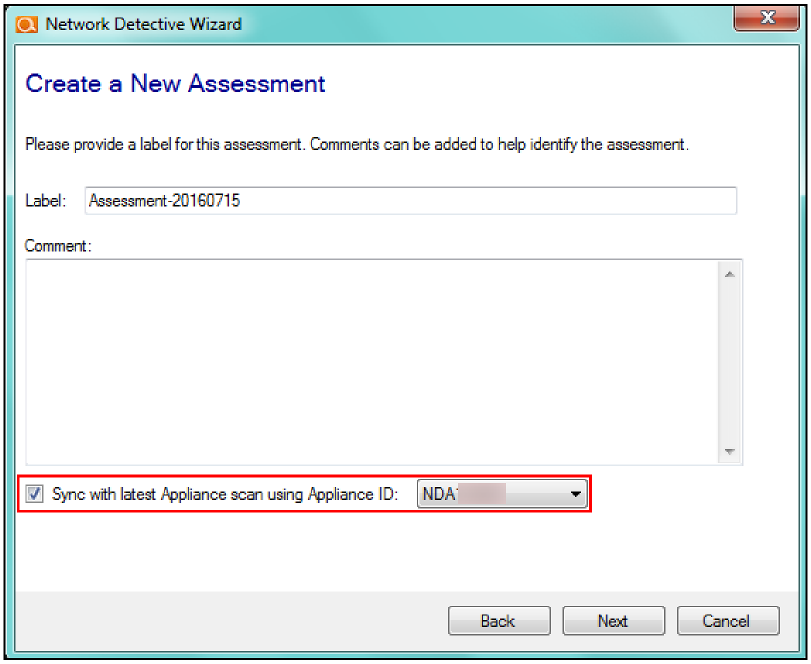
Tip: Refer to the HIPAA **Exception Report** to quickly identify where you need to manually update your HIPAA compliance documentation with notes or other information that cannot be drawn from automated scans.

1. Double click on the **Assessment** report's **Filename** to open and view the report.
2. If you can download an **Exception Report**, please proceed to the next section below to address the **Exceptions** identified.

   If no **Exception Report** is available, this means no **Exceptions** exist. Proceed by simply downloading the other reports that are available.

Note: The **Exception Report** summarizes where your worksheets may be missing information as a result of the new scan data being uploaded to the **Reporter**. When an **Exception Report** is generated, you need to manually update your worksheets with information that cannot be collected automatically. For example, if new users are added to your network, you will need to enter information about their role within the organization.

3. **Start** a new **HIPAA Risk Assessment**.



Network Detective Wizard

Create a New Assessment

Please provide a label for this assessment. Comments can be added to help identify the assessment.

Label: Assessment-20160715

Comment:

☑ Sync with latest Appliance scan using Appliance ID: NDA[redacted]

4. On the **Create New Assessment** Wizard Screen, select the checkbox to **Sync** the assessment with the **Reporter Appliance**.

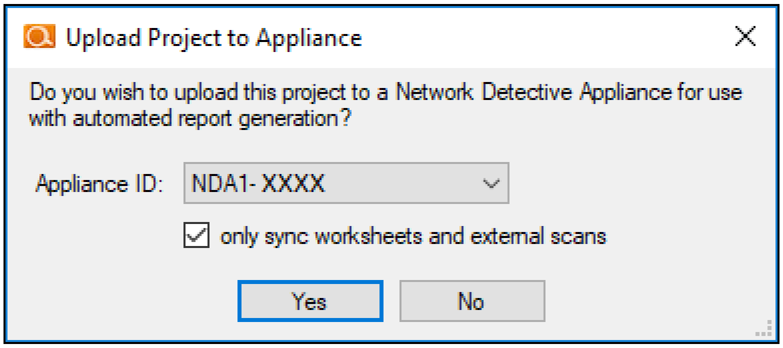
   The Reporter will synchronize the Site's previous assessment data with the new **HIPAA Assessment** you created.

5. Edit and update the **Worksheets** within the **Assessment** in the order presented in the **Checklist**. Perform **Worksheet** updates based on the missing information referenced within in the **Exception Report**.

Step 5 — Finish and Upload Updated HIPAA Assessment Project to Reporter

1. Once the updating of the **Worksheets** is complete, **Finish** the **Assessment** by selecting the **Finish** button in the **Assessment Window**.

2. When prompted to do so, synchronize the **HIPAA Assessment** with the **Reporter**. This will save the new worksheet responses you entered based on the **Exception Report**.



Upload Project to Appliance

Do you wish to upload this project to a Network Detective Appliance for use with automated report generation?

Appliance ID: NDA1- XXXX

☑ only sync worksheets and external scans

PCI Compliance Assessment Automatic Reports

With Reporter, you can set up automatic PCI reports to produce regular, up-to-date compliance documentation. Once you set up automated scans and report tasks, you will only need to manually update your documentation in response to certain changes in the reporting environment, like new users or computers.

Before you set up automated PCI assessment reports, *you must first* complete a full PCI assessment that includes **external vulnerability scans**, **network scans**, **local push scans**, and the completion of all appropriate Inform-based **Surveys and Worksheets**. The user should be able to generate all **PCI Assessment Reports**. Once you've done this, here is the workflow for automating PCI compliance assessments with Reporter:

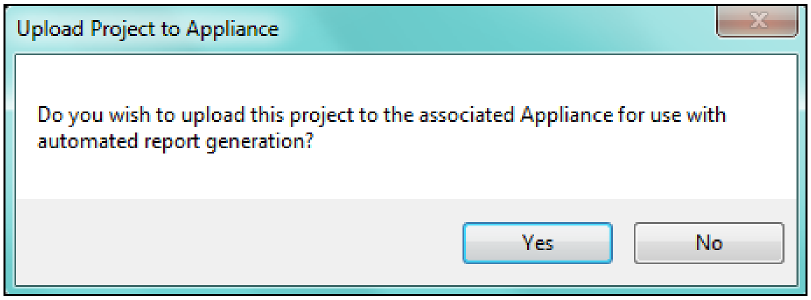
1. **Finish** the assessment, and then **upload/sync** the completed assessment with the Reporter appliance. This allows you use the finished assessment as the "baseline" for automated PCI reporting.
2. Set up recurring PCI assessment scans using the Remote Data Collector and Reporter. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **PCI Network Scan**, 2) **Push Deploy Computer Scan**, 3) **External Vulnerability Scan**. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for instructions.
3. Set up recurring PCI report tasks with Reporter.
4. Review exception report and update PCI worksheets.
5. Finish the updated PCI assessment and upload to Reporter.

Here are the steps with detailed instructions:

Step 1 — Finish and Upload Completed PCI Assessment Project to Reporter

The first step is to complete and finish a full PCI assessment. You should be able to generate all PCI assessment reports. Then:

1. Once satisfied with a complete **PCI Assessment**, press the “**Finish**” Assessment button.



Upload Project to Appliance

Do you wish to upload this project to the associated Appliance for use with automated report generation?

2. Confirm that you wish to **Upload Project to Appliance** (Reporter) to be used for automatic report generation. This allows you to use the finished assessment, including your completed worksheets, as the baseline for future assessments.

Step 2 — Create PCI Scan Tasks

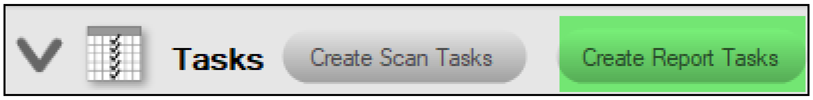
Now that you've completed the assessment and uploaded it to the appliance, it's time to create automatic scan tasks with Reporter and the Remote Data Collector. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78 for detailed instructions.

Step 3 — Create PCI Report Tasks

Next, you need to create automatic PCI report tasks with Reporter.

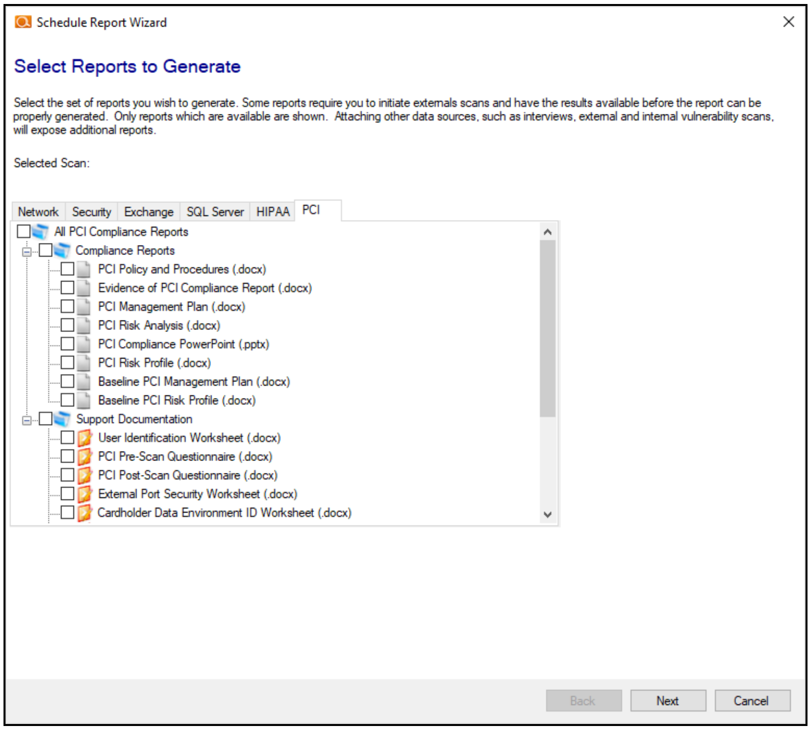
1. Click on the **Reporter** icon to open the Reporter dashboard.

2. From the **Tasks** bar, click **Create Report Tasks**.



3. Select the PCI Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.

4. From within the **Select Reports to Generate** window, select the **PCI Risk Profile Report** and any other **PCI Assessment** reports you would like to generate. Then select the **Next** button.



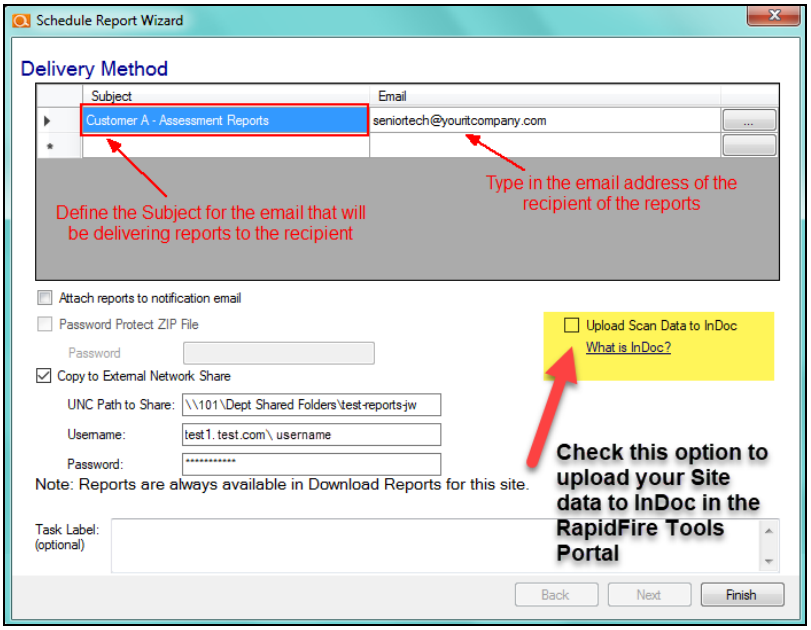
Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- ☐ All PCI Compliance Reports
  - ☐ Compliance Reports
    - ☐ PCI Policy and Procedures (.docx)
    - ☐ Evidence of PCI Compliance Report (.docx)
    - ☐ PCI Management Plan (.docx)
    - ☐ PCI Risk Analysis (.docx)
    - ☐ PCI Compliance PowerPoint (.pptx)
    - ☐ PCI Risk Profile (.docx)
    - ☐ Baseline PCI Management Plan (.docx)
    - ☐ Baseline PCI Risk Profile (.docx)
  - ☐ Support Documentation
    - ☐ User Identification Worksheet (.docx)
    - ☐ PCI Pre-Scan Questionnaire (.docx)
    - ☐ PCI Post-Scan Questionnaire (.docx)
    - ☐ External Port Security Worksheet (.docx)
    - ☐ Cardholder Data Environment ID Worksheet (.docx)

5. Next, set the **Delivery Method** for the Reports. In this window you can:



Delivery Method

Subject	Email
Customer A - Assessment Reports	seniortech@yourcompany.com

Define the Subject for the email that will be delivering reports to the recipient

Type in the email address of the recipient of the reports

☐ Attach reports to notification email

☐ Password Protect ZIP File

Password:

☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\ username

Password: ***********

Note: Reports are always available in Download Reports for this site.

☐ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

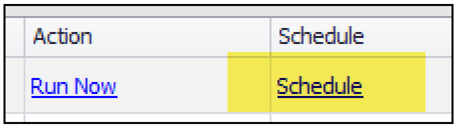
Task Label: (optional)

- define the Subject for the email to be sent and enter the email address of the Recipient
- set if you want to send the reports attached to the Report notification email message

- set password protection on the file that contains the reports
- "Copy Reports to External Network Share with Reporter" on page 76

> **Tip:** Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See "InDoc and the RapidFire Tools Portal" on page 111 for more on how to set up InDoc.

6. After defining the **Delivery Method** settings, click on the **Finish** button. The report task will be added to the list of **Tasks**.
7. Click **Schedule** to schedule the report task.



Action	Schedule
Run Now	Schedule

> **Important:** You must schedule the report task to occur AFTER your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after** your scan tasks are scheduled to begin.

Step 4 — Review and Update PCI Exception Report and Update InForms

After you finish your assessment and set up automatic PCI scanning and reporting, you will receive updated PCI documentation through email or whatever delivery method you choose.

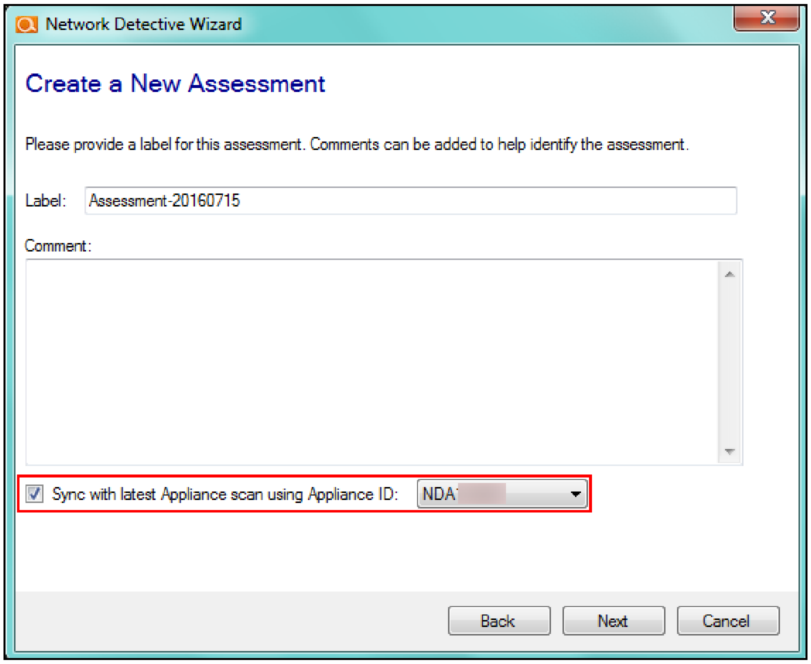
> **Tip:** Refer to the PCI **Exception Report** to quickly identify where you need to manually update your PCI compliance documentation with notes or other information that cannot be drawn from automated scans.

1. Double click on the **Assessment** report's **Filename** to open and view the report.
2. If you can download an **Exception Report**, please proceed to the next section below to address the **Exceptions** identified.

If no **Exception Report** is available, this means no **Exceptions** exist. Proceed by simply downloading the other reports that are available.

Note: The **Exception Report** summarizes where your worksheets may be missing information as a result of the new scan data being uploaded to the **Reporter**. When an **Exception Report** is generated, you need to manually update your worksheets with information that cannot be collected automatically. For example, if new users are added to your network, you will need to enter information about their role within the organization.

3. **Start** a new **PCI Risk Assessment**.



Network Detective Wizard

Create a New Assessment

Please provide a label for this assessment. Comments can be added to help identify the assessment.

Label: Assessment-20160715

Comment:

☑ Sync with latest Appliance scan using Appliance ID: NDA[redacted]

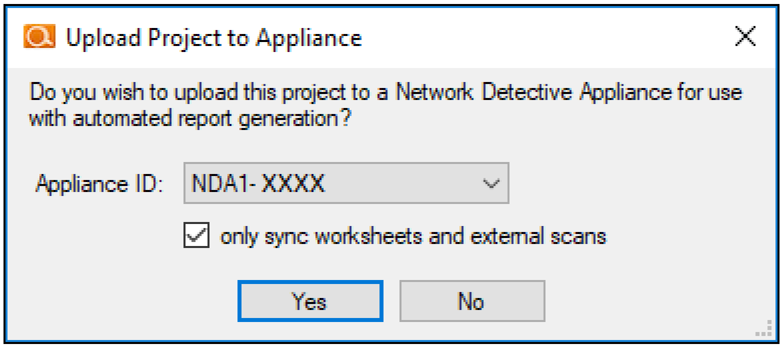
4. On the **Create New Assessment** Wizard Screen, select the checkbox to **Sync** the assessment with the **Reporter Appliance**.

   The Reporter will synchronize the Site's previous assessment data with the new **PCI Assessment** you created.

5. Edit and update the **Worksheets** within the **Assessment** in the order presented in the **Checklist**. Perform **Worksheet** updates based on the missing information referenced within in the **Exception Report**.

Step 5 — Finish and Upload Updated PCI Assessment Project to Reporter

1. Once the updating of the **Worksheets** is complete, **Finish** the **Assessment** by selecting the **Finish** button in the **Assessment Window**.
2. When prompted to do so, synchronize the **PCI Assessment** with the **Reporter**. This will save the new worksheet responses you entered based on the **Exception Report**.



Upload Project to Appliance

Do you wish to upload this project to a Network Detective Appliance for use with automated report generation?

Appliance ID: NDA1- XXXX

☑ only sync worksheets and external scans

Synchronizing Assessment Projects with Reporter

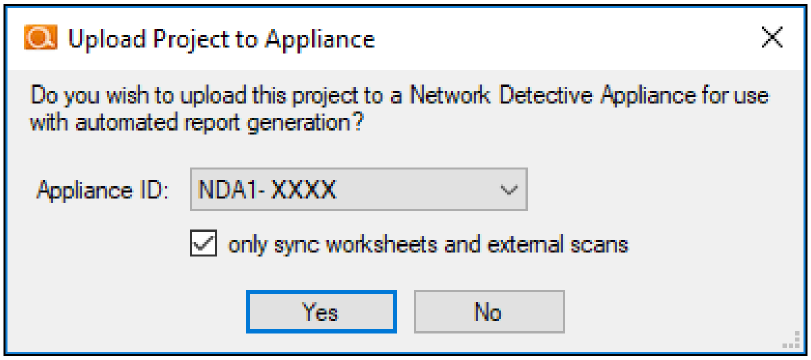
Reporter allows you to upload a finished project to the appliance in order to automate assessments and report generation. Uploading a project has several functions:

- Reuse worksheet data — when you upload worksheets to your reporter appliance, and start a new assessment, your worksheets will automatically be populated with the saved information
- Reuse external scan data — the results of your external scan data will be uploaded and available for later use
- Reuse network and computer scan data — the results of your network and computer scan data will be uploaded and available for later use

Finishing a Project: Upload Project to Appliance

To upload a project to an appliance:

1. When you have completed your assessment, click **Finish**. Confirm that you wish to wrap up the project.
2. The **Upload Project to Appliance** window will appear.
3. Select the Appliance to which to upload your completed assessment project.



Upload Project to Appliance

Do you wish to upload this project to a Network Detective Appliance for use with automated report generation?

Appliance ID: NDA1- XXXX

☑ only sync worksheets and external scans

4. Choose whether to **Only sync worksheets and external scans**.

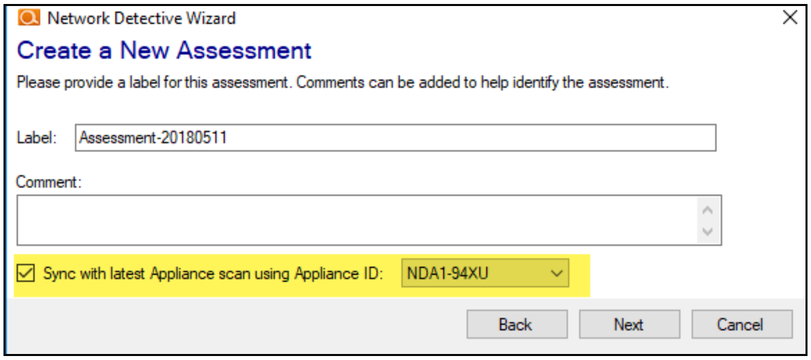
> **Note:** We recommended you keep this option selected unless you wish to include or remove specific scan files.

5. Click **Yes** to complete synchronizing the assessment with the appliance. Your assessment data will be copied to the appliance. It will be available to synch with a new assessment. See "Starting a Project: Sync New Assessment with Latest Appliance Scans" on the next page.

Starting a Project: Sync New Assessment with Latest Appliance Scans

When you start a new assessment, you can sync the newly created assessment with the data stored on the appliance. Your new assessment will then have the most current worksheets and scan data from the Reporter appliance. To do this:

1. Start a New Assessment.
2. From the Create a New Assessment window, check **Sync with latest Appliance scan using Appliance ID**.



Network Detective Wizard

Create a New Assessment

Please provide a label for this assessment. Comments can be added to help identify the assessment.

Label: Assessment-20180511

Comment:

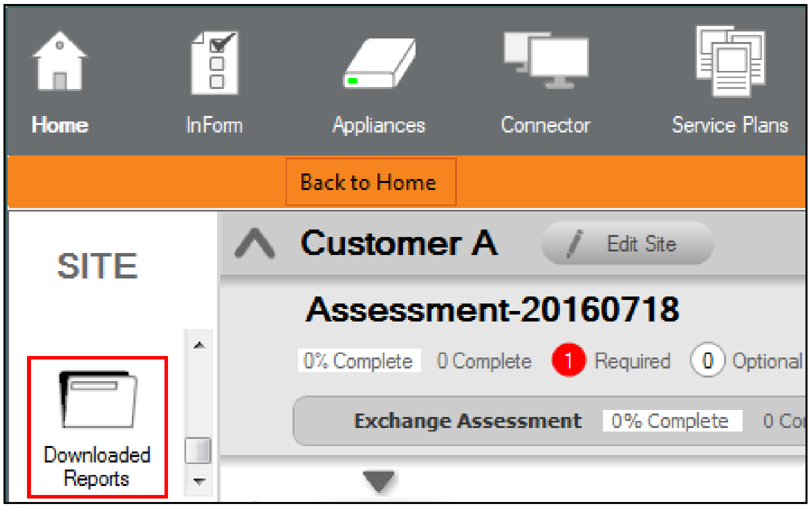
☑ Sync with latest Appliance scan using Appliance ID: NDA1-94XU

3. Select the Reporter **Appliance** from which to get the latest data
4. Click **Next** and continue creating the new assessment. Your new assessment will be pre-populated with the data from the appliance.

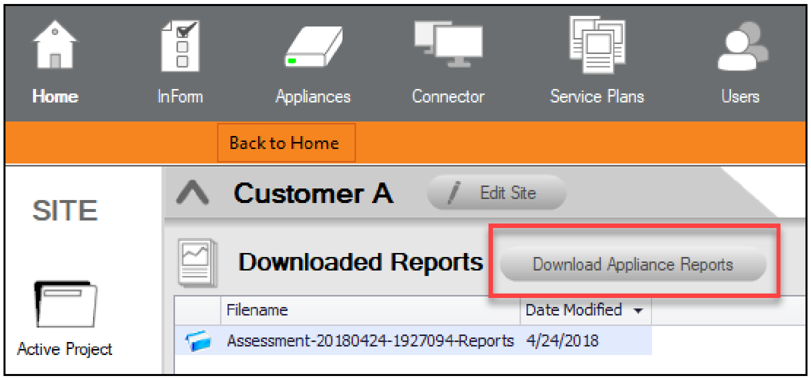
Manually Download Reports (Reporter)

After sufficient time has passed since the report generation task schedule time follow these steps to download and view the reports.

1. **Open** the **Site Associated** with **Reporter**.
2. Select the **Downloaded Reports** Icon on the left side of the Network Detective window to display the **Download Reports** button in the Network Detective window.



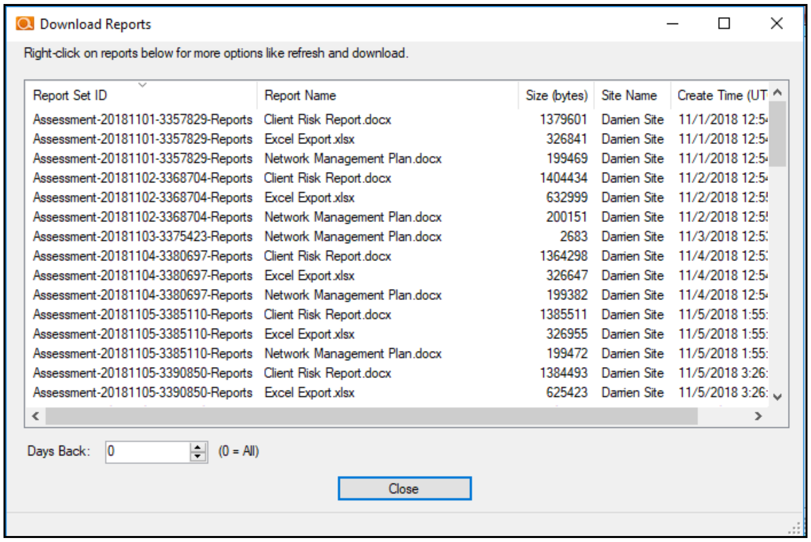
3. View the list of generated reports by selecting the **Download Appliance Reports** button that appeared at the top of the Network Detective window.



Filename	Date Modified
Assessment-20180424-1927094-Reports	4/24/2018

4. Upon selecting the **Download Reports** button, a window will appear with reports generated by the **Reporter**.

© 2021 RapidFire Tools, Inc. All rights reserved.

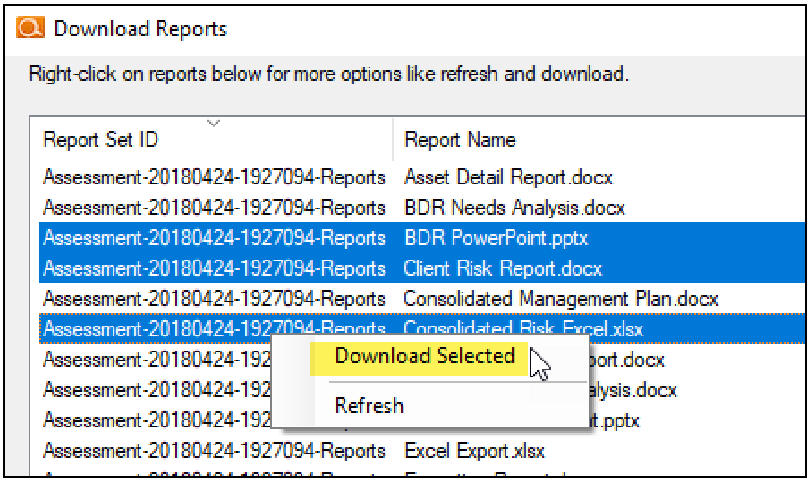


Download Reports

Right-click on reports below for more options like refresh and download.

Report Set ID	Report Name	Size (bytes)	Site Name	Create Time (UT
Assessment-20181101-3357829-Reports	Client Risk Report.docx	1379601	Darien Site	11/1/2018 12:5
Assessment-20181101-3357829-Reports	Excel Export.xlsx	326841	Darien Site	11/1/2018 12:5
Assessment-20181101-3357829-Reports	Network Management Plan.docx	199469	Darien Site	11/1/2018 12:5
Assessment-20181102-3368704-Reports	Client Risk Report.docx	1404434	Darien Site	11/2/2018 12:5
Assessment-20181102-3368704-Reports	Excel Export.xlsx	632999	Darien Site	11/2/2018 12:5
Assessment-20181102-3368704-Reports	Network Management Plan.docx	200151	Darien Site	11/2/2018 12:5
Assessment-20181103-3375423-Reports	Network Management Plan.docx	2683	Darien Site	11/3/2018 12:5
Assessment-20181104-3380697-Reports	Client Risk Report.docx	1364298	Darien Site	11/4/2018 12:5
Assessment-20181104-3380697-Reports	Excel Export.xlsx	326647	Darien Site	11/4/2018 12:5
Assessment-20181104-3380697-Reports	Network Management Plan.docx	199382	Darien Site	11/4/2018 12:5
Assessment-20181105-3385110-Reports	Client Risk Report.docx	1385511	Darien Site	11/5/2018 1:55:
Assessment-20181105-3385110-Reports	Excel Export.xlsx	326955	Darien Site	11/5/2018 1:55:
Assessment-20181105-3385110-Reports	Network Management Plan.docx	199472	Darien Site	11/5/2018 1:55:
Assessment-20181105-3390850-Reports	Client Risk Report.docx	1384493	Darien Site	11/5/2018 3:26:
Assessment-20181105-3390850-Reports	Excel Export.xlsx	625423	Darien Site	11/5/2018 3:26:

5. Select one or more reports. Right click and select Download Selected.



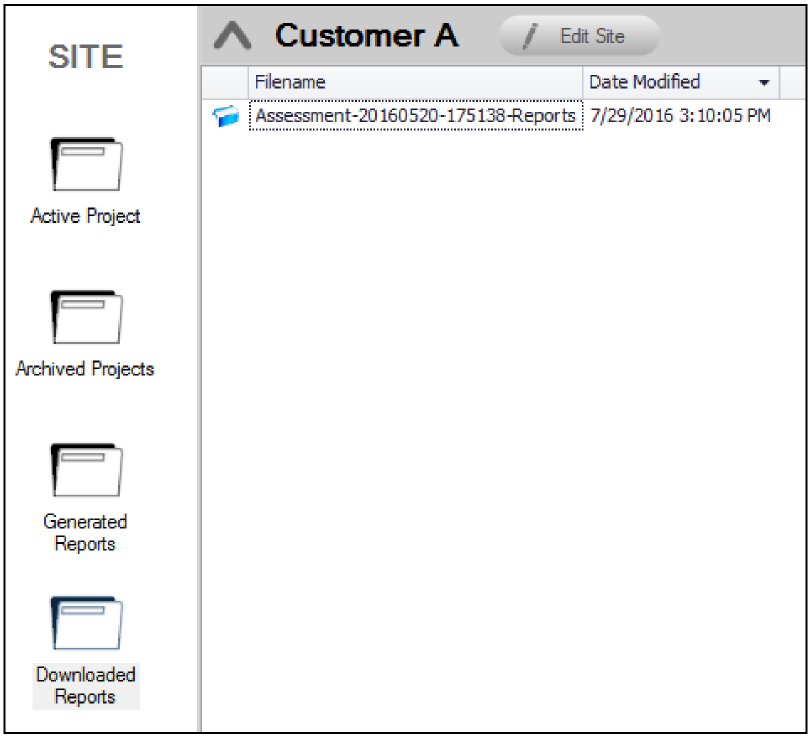
Download Reports

Right-click on reports below for more options like refresh and download.

Report Set ID	Report Name
Assessment-20180424-1927094-Reports	Asset Detail Report.docx
Assessment-20180424-1927094-Reports	BDR Needs Analysis.docx
Assessment-20180424-1927094-Reports	BDR PowerPoint.pptx
Assessment-20180424-1927094-Reports	Client Risk Report.docx
Assessment-20180424-1927094-Reports	Consolidated Management Plan.docx
Assessment-20180424-1927094-Reports	Consolidated Risk Excel.xlsx
Assessment-20180424-192	ort.docx
Assessment-20180424-192	alysis.docx
Assessment-20180424-192	t.pptx
Assessment-20180424-1927094-Reports	Excel Export.xlsx

6. You can hold **Shift** and click to select multiple reports at once.
7. Close the **Download Reports** window when you are finished selecting and downloading reports.

   The downloaded report(s) will now be available for viewing.



Filename	Date Modified
Assessment-20160520-175138-Reports	7/29/2016 3:10:05 PM

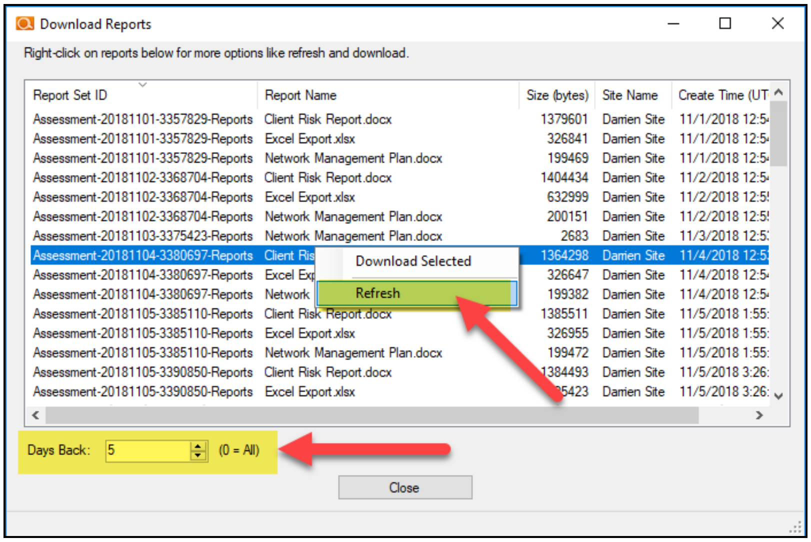
Double click on the **Assessment** report's **Filename** to open and view the report.

Filter Reports by Days Back

When browsing reports to download, you can filter all but the most recent reports. Use this option if you have a large number of reports and want to view only the most recent. To do this:

1. From the Download Reports screen, enter a number of **Days Back**. (The number "0" will reveal all available reports.)
2. Right click in the list of reports and select Refresh.

© 2021 RapidFire Tools, Inc. All rights reserved.



Download Reports

Right-click on reports below for more options like refresh and download.

Report Set ID	Report Name	Size (bytes)	Site Name	Create Time (UT
Assessment-20181101-3357829-Reports	Client Risk Report.docx	1379601	Darien Site	11/1/2018 12:5
Assessment-20181101-3357829-Reports	Excel Export.xlsx	326841	Darien Site	11/1/2018 12:5
Assessment-20181101-3357829-Reports	Network Management Plan.docx	199469	Darien Site	11/1/2018 12:5
Assessment-20181102-3368704-Reports	Client Risk Report.docx	1404434	Darien Site	11/2/2018 12:5
Assessment-20181102-3368704-Reports	Excel Export.xlsx	632999	Darien Site	11/2/2018 12:5
Assessment-20181102-3368704-Reports	Network Management Plan.docx	200151	Darien Site	11/2/2018 12:5
Assessment-20181103-3375423-Reports	Network Management Plan.docx	2683	Darien Site	11/3/2018 12:5
Assessment-20181104-3380697-Reports	Client Ris	1364298	Darien Site	11/4/2018 12:5
Assessment-20181104-3380697-Reports	Excel Exp	326647	Darien Site	11/4/2018 12:5
Assessment-20181104-3380697-Reports	Network	199382	Darien Site	11/4/2018 12:5
Assessment-20181105-3385110-Reports	Client Risk Report.docx	1385511	Darien Site	11/5/2018 1:55:
Assessment-20181105-3385110-Reports	Excel Export.xlsx	326955	Darien Site	11/5/2018 1:55:
Assessment-20181105-3385110-Reports	Network Management Plan.docx	199472	Darien Site	11/5/2018 1:55:
Assessment-20181105-3390850-Reports	Client Risk Report.docx	1384493	Darien Site	11/5/2018 3:26:
Assessment-20181105-3390850-Reports	Excel Export.xlsx	5423	Darien Site	11/5/2018 3:26:

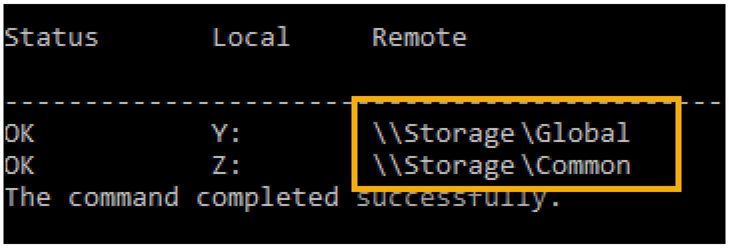
Days Back: 5 (0 = All)

The list of reports will then be limited to the specified number of days back.

Copy Reports to External Network Share with Reporter

To copy your reports to an external network share, be sure you meet these requirements:

1. You must enter the correct UNC path to the external share. On a computer that has access to the external share, open a command prompt and type "net use." A list of external network shares will appear. If you do not see your external share, be sure it is mapped correctly.

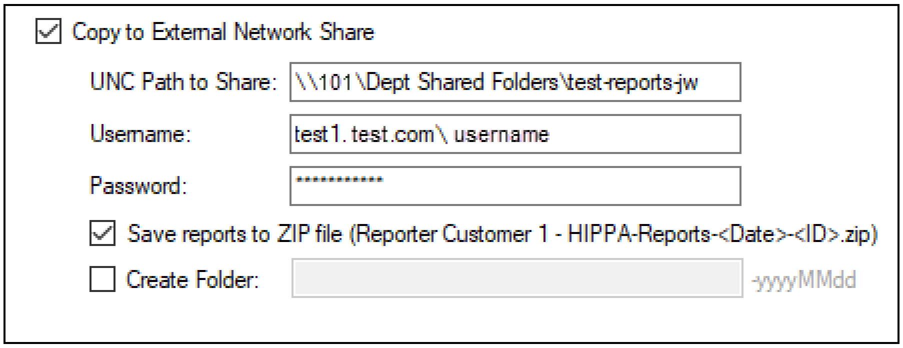


```
Status       Local     Remote

-----------------------------------------------------------
OK           Y:        \\Storage\Global
OK           Z:        \\Storage\Common
The command completed successfully.
```

> **Important:** If Reporter is installed on a separate domain, log into a computer on that domain and check the UNC path for your external share. You will need to use that UNC path instead.

2. The user credentials you enter must have the correct security permissions to access to the external network share. If you can view and open the external share in Windows using your credentials, then you likely have the correct permissions.
3. In the Schedule Report Wizard, enter the username in the format: **domain\user**. You can use the short domain name or the fully qualified domain name. Below is an example.



☑ Copy to External Network Share

UNC Path to Share: \\101\Dept Shared Folders\test-reports-jw

Username: test1.test.com\ username

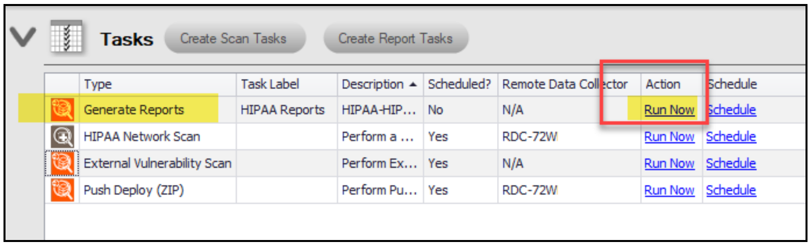
Password: ************

☑ Save reports to ZIP file (Reporter Customer 1 - HIPPA-Reports-<Date>-<ID>.zip)

☐ Create Folder: -yyyyMMdd

To test whether your reports can be copied to the external share, click **Run Now** on your report task.

© 2021 RapidFire Tools, Inc. All rights reserved.



Type	Task Label	Description ▲	Scheduled?	Remote Data Collector	Action	Schedule
Generate Reports	HIPAA Reports	HIPAA-HIP...	No	N/A	Run Now	Schedule
HIPAA Network Scan		Perform a ...	Yes	RDC-72W	Run Now	Schedule
External Vulnerability Scan		Perform Ex...	Yes	N/A	Run Now	Schedule
Push Deploy (ZIP)		Perform Pu...	Yes	RDC-72W	Run Now	Schedule

Then check whether your reports appear in the share. If they do not, check to be sure you entered the correct credentials and UNC path. Also check to be sure the user has the correct security permissions to access the share.

© 2021 RapidFire Tools, Inc. All rights reserved.

Remote Data Collector Scans

This section covers everything you need to know about using the Remote Data Collector with Reporter.

Configuring Remote Data Collector Scans by Assessment Module

In order to generate automated assessment reports using Reporter, you will need to configure the Remote Data Collector to perform the appropriate scheduled scans on the client's network:

Report Types	Necessary RDC Scans
Network Assessment	• Network Scan (Network/Security Assessment Modules) • Push Deploy Scan (selecting Computer Scan)
Security Assessment	• Network Scan (Network/Security Assessment Modules) • Push Deploy Scan (selecting Security Scan) • *External Vulnerability Scan (set up on the Reporter)
SQL Server Assessment	• SQL Server Collection
Exchange Assessment	• Exchange Server Collection
HIPAA Assessment	• HIPAA Network Scan • Push Deploy Scan (selecting HIPAA Deep Scan) • *External Vulnerability Scan (set up on the Reporter)
PCI Assessment	• PCI Network Scan • Push Deploy Scan (selecting PCI Deep Scan) • *External Vulnerability Scan (set up on the Reporter)

See below for specific instructions for setting up the various types of scans.

> **Tip:** If you haven't set up your Reporter appliance or Remote Data Collector yet, see "Setting Up Reporter" on page 16.

© 2021 RapidFire Tools, Inc. All rights reserved.

Network and Security Assessment Scan

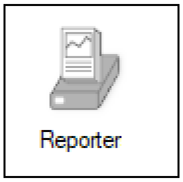
Set up a recurring Network/Security Assessment scan to collect data for automatic Network and Security Assessment reports.

Configure the network scan using the wizard.

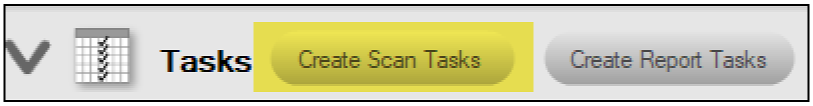
- Look here if you are "Scanning an Active Directory Domain Network" below
- Look here if you are "Scanning a Workgroup Network" on page 86

Scanning an Active Directory Domain Network

1. Open the **Reporter** dashboard.

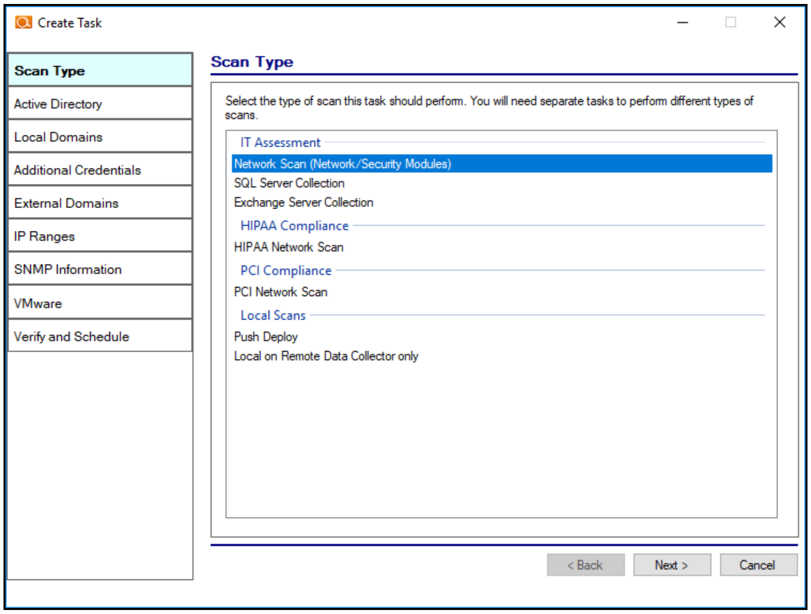


2. Click **Create Scan Tasks** and **select the RDC**.



3. Choose the **Network Scan (Network/Security Modules)** option from the wizard and click the **Next** button.

© 2021 RapidFire Tools, Inc. All rights reserved.



Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

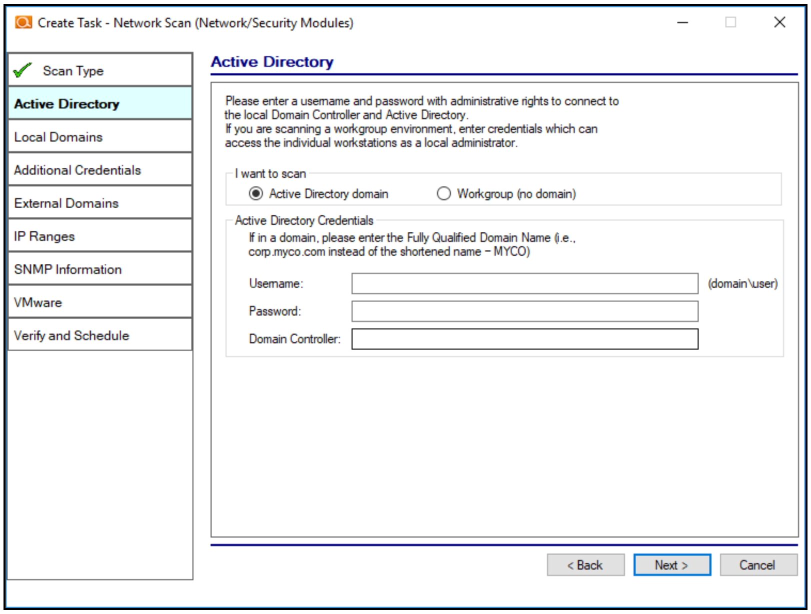
IT Assessment
- Network Scan (Network/Security Modules)
- SQL Server Collection
- Exchange Server Collection

HIPAA Compliance
- HIPAA Network Scan

PCI Compliance
- PCI Network Scan

Local Scans
- Push Deploy
- Local on Remote Data Collector only

4. Select the type of network you want to scan: **Active Directory Domain**.



Active Directory

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory.
If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.

I want to scan
● Active Directory domain ○ Workgroup (no domain)

Active Directory Credentials
If in a domain, please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name – MYCO)

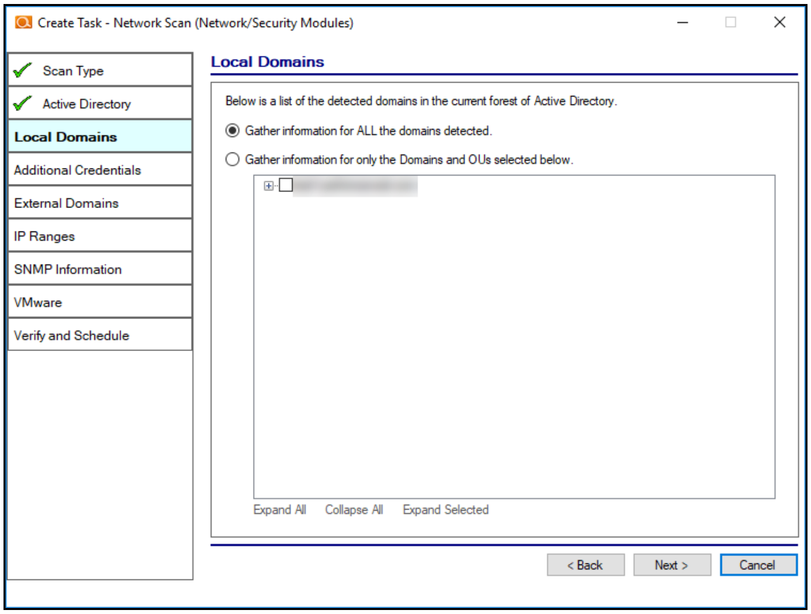
Username: (domain\user)
Password:
Domain Controller:

5. 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.

© 2021 RapidFire Tools, Inc. All rights reserved.

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

6. Enter the **name or IP address** of the **Domain Controller**.
7. Choose either to scan all **Domains** detected on the target network or to restrict the Scan to selected **Organizational Units** (OUs) and Domains.



Create Task - Network Scan (Network/Security Modules)

- ✓ Scan Type
- ✓ Active Directory
- **Local Domains**
- Additional Credentials
- External Domains
- IP Ranges
- SNMP Information
- VMware
- Verify and Schedule

Local Domains

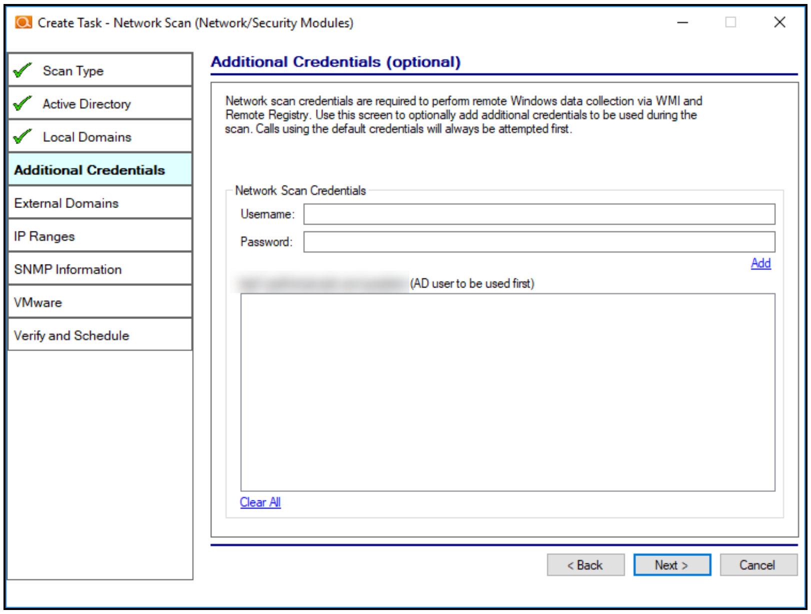
Below is a list of the detected domains in the current forest of Active Directory.

● Gather information for ALL the domains detected.

○ Gather information for only the Domains and OUs selected below.

⊞ □ [redacted]

8. Enter any **Additional Credentials** necessary to access endpoints during the scan. Enter the username and password and click **Add**. When you've finished, click **Next**.



Additional Credentials (optional)

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

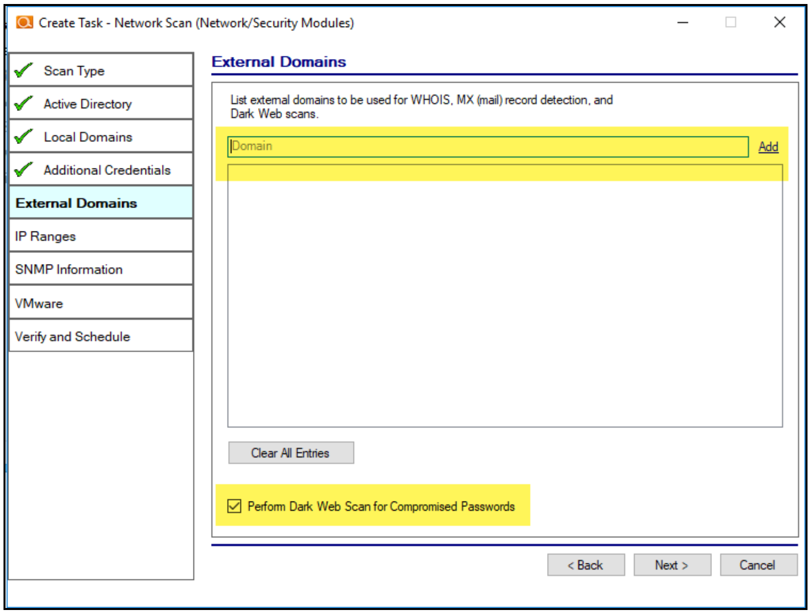
Network Scan Credentials

Username:

Password:

[redacted] (AD user to be used first)

9. 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



External Domains

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

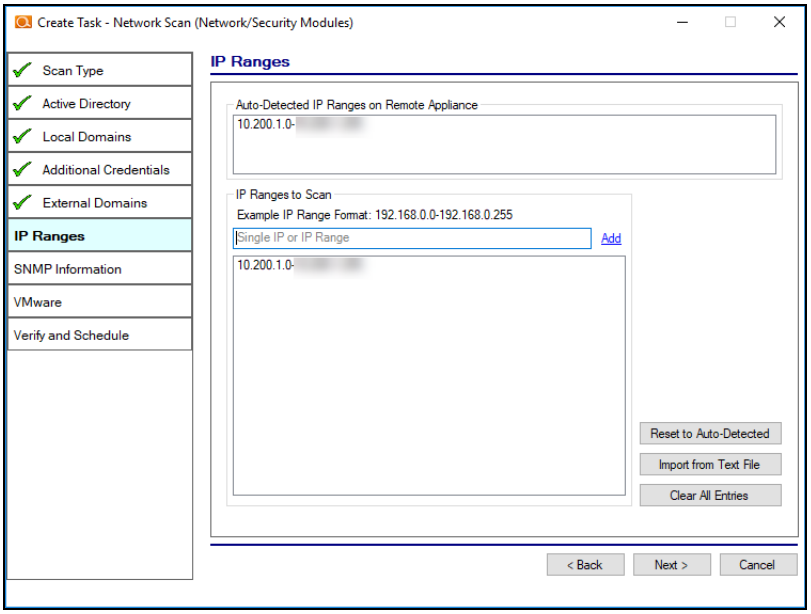
Domain

☑ Perform Dark Web Scan for Compromised Passwords

© 2021 RapidFire Tools, Inc. All rights reserved.

> **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 Security Assessment reports. This service will return the first 5 compromised passwords for each domain specified.

10. The **IP Ranges** from the target network will be auto-detected and included in the scan. To include additional subnets input them here.



IP Ranges

Auto-Detected IP Ranges on Remote Appliance: 10.200.1.0-[redacted]

IP Ranges to Scan

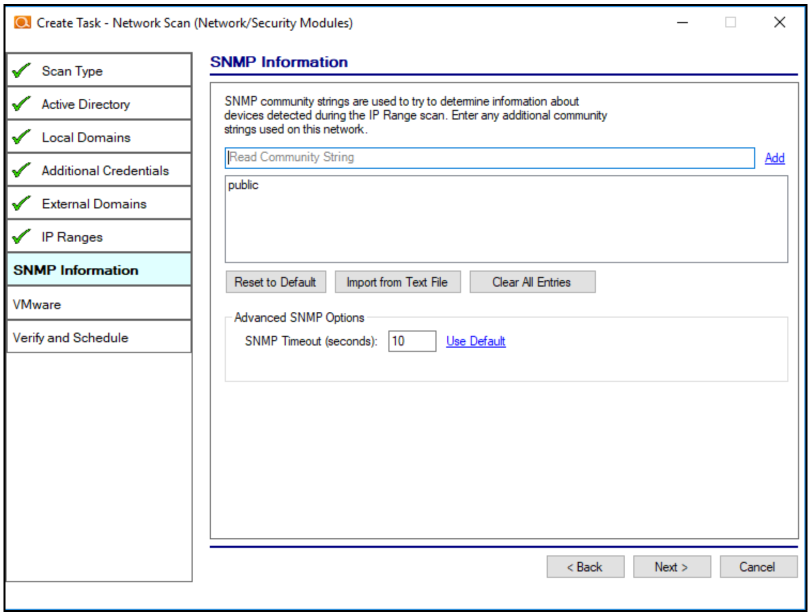
Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

10.200.1.0-[redacted]

11. 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.

© 2021 RapidFire Tools, Inc. All rights reserved.



SNMP Information

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

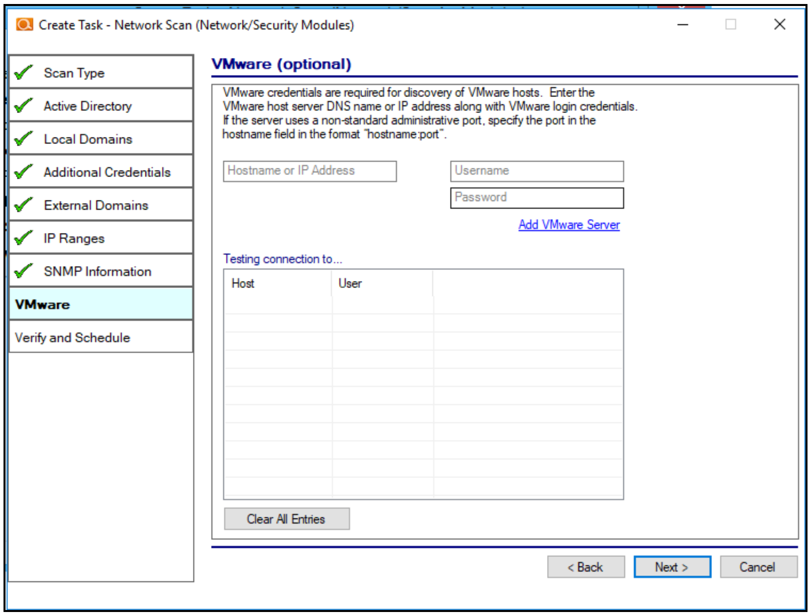
Read Community String

public

Advanced SNMP Options

SNMP Timeout (seconds): 10

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



VMware (optional)

VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname field in the format "hostname:port".

Hostname or IP Address

Username

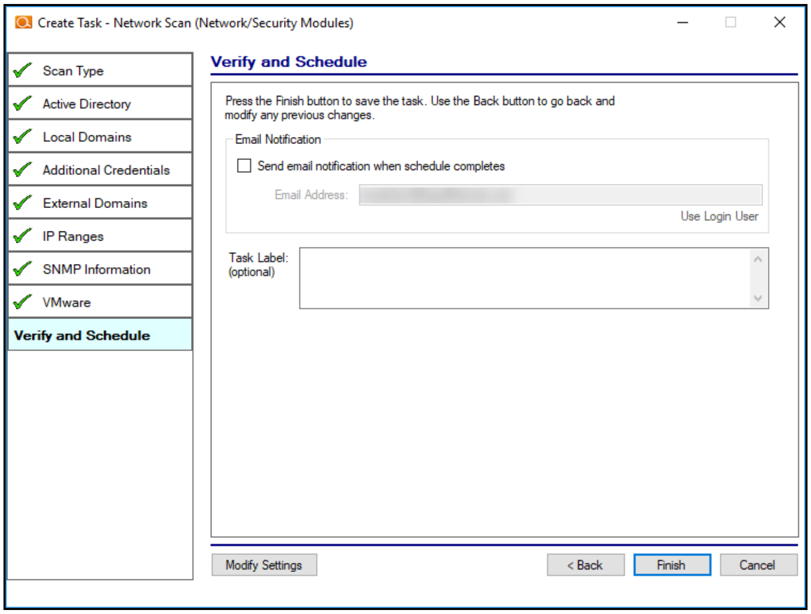
Password

Testing connection to...

Host	User

13. Check "**Send an email notification when schedule completes**" to notify an individual via email that the scan task is complete. The use of this option is

recommended as the time a scan takes to complete varies depending on the target network.



Verify and Schedule

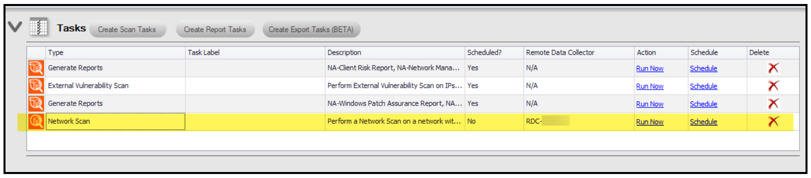
Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

Email Notification

□ Send email notification when schedule completes

Email Address: [redacted]

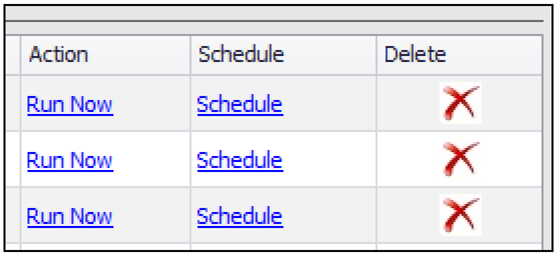
14. Click on the **Finish** button to complete the scheduling of the **Network Scan** task. The task will then be displayed in the **Tasks Library** window.



Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Mana...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IPs...	Yes	N/A	Run Now	Schedule	✗
Generate Reports		NA-Windows Patch Assurance Report, NA...	Yes	N/A	Run Now	Schedule	✗
Network Scan		Perform a Network Scan on a network wit...	No	RDC-[redacted]	Run Now	Schedule	✗

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

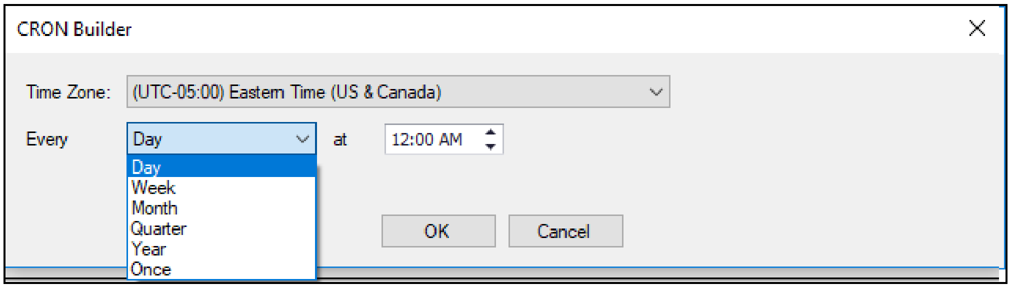
    a. Select the **Run Now** option link under the **Action** column to initiate the scan. This will place the scan directly into the **Scheduled Tasks** list.



Action	Schedule	Delete
Run Now	Schedule	✗
Run Now	Schedule	✗
Run Now	Schedule	✗

© 2021 RapidFire Tools, Inc. All rights reserved.

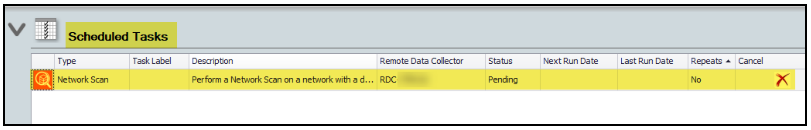
b. Or, click **Schedule** to execute the scan sometime in the future. When you click the **Schedule** link, the CRON Builder scheduler window is displayed and is used to set the scheduled action's execution time.


CRON Builder

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

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

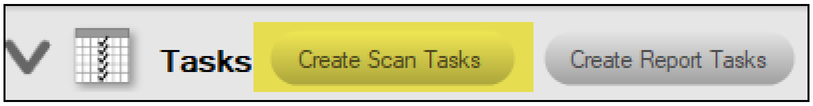

Scheduled Tasks

Type	Task Label	Description	Remote Data Collector	Status	Next Run Date	Last Run Date	Repeats	Cancel
Network Scan		Perform a Network Scan on a network with a d...	RDC [redacted]	Pending			No	✗

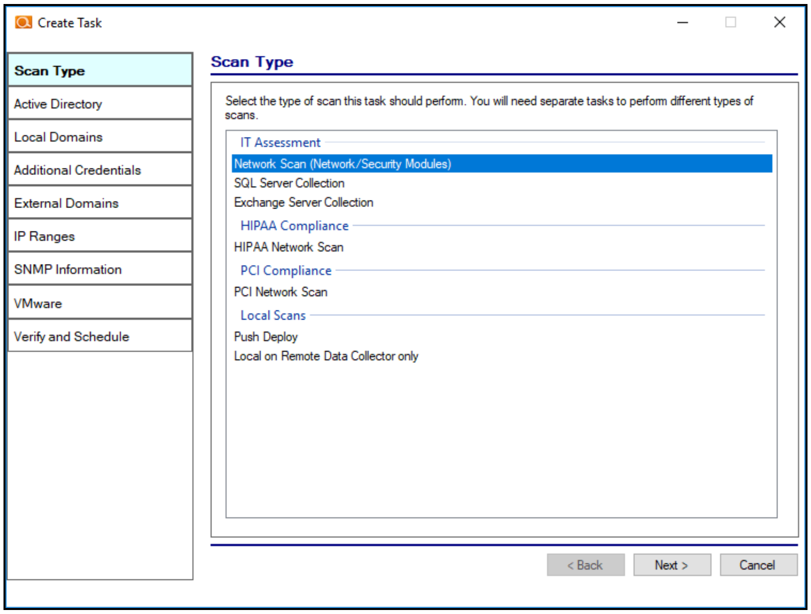
Scanning a Workgroup Network

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and **select the RDC**.



3. Choose the **Network Scan (Network/Security Modules)** option from the wizard and click the **Next** button.



Create Task

Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

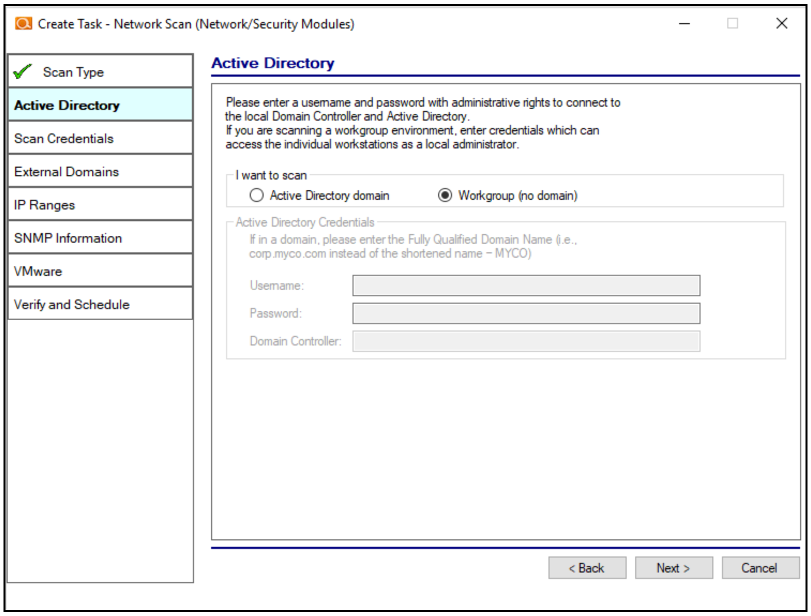
IT Assessment
- Network Scan (Network/Security Modules)
- SQL Server Collection
- Exchange Server Collection

HIPAA Compliance
- HIPAA Network Scan

PCI Compliance
- PCI Network Scan

Local Scans
- Push Deploy
- Local on Remote Data Collector only

4. Select the type of network you want to scan: **Workgroup (No domain)**.



Create Task - Network Scan (Network/Security Modules)

Active Directory

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory.
If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.

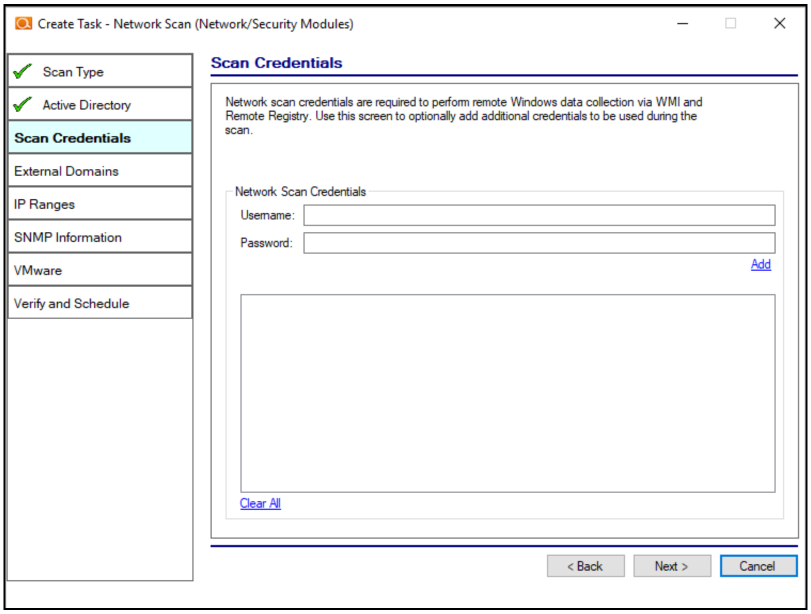
I want to scan
○ Active Directory domain ● Workgroup (no domain)

Active Directory Credentials
If in a domain, please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name - MYCO)

Username:
Password:
Domain Controller:

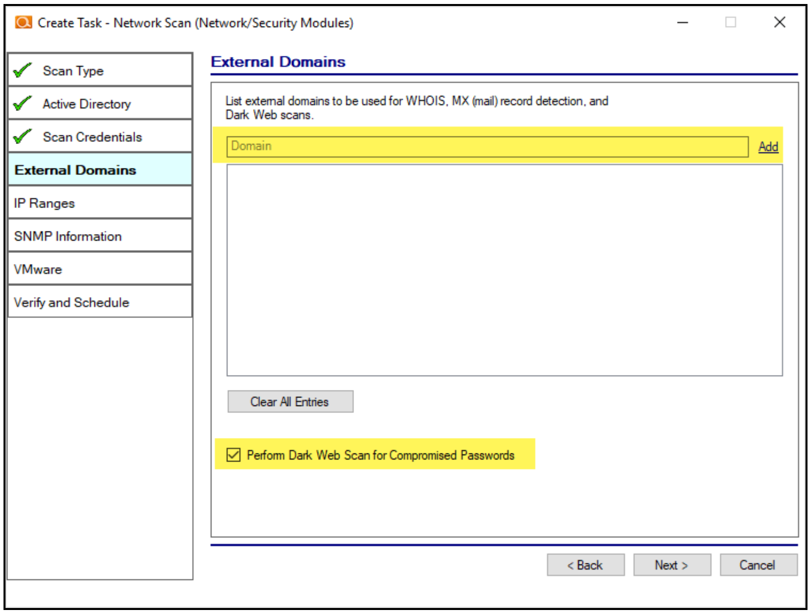
5. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator.

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.



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.

6. 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



External Domains

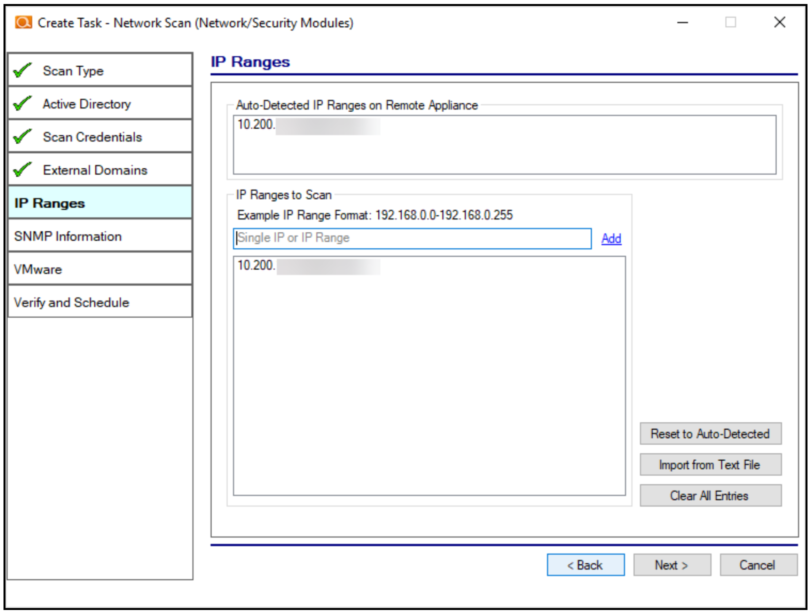
List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.

☑ Perform Dark Web Scan for Compromised Passwords

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 Security Assessment reports. This service will return the first 5 compromised passwords for each domain specified.

7. The **IP Ranges** from the target network will be auto-detected and included in the scan. To include additional subnets input them here.

© 2021 RapidFire Tools, Inc. All rights reserved.



IP Ranges

Auto-Detected IP Ranges on Remote Appliance

10.200.[redacted]

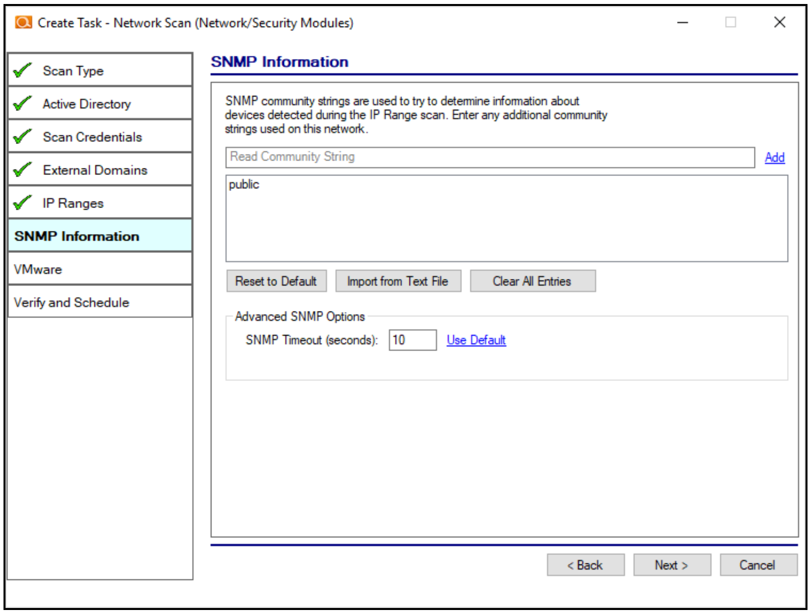
IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

10.200.[redacted]

8. 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.



SNMP Information

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

Read Community String

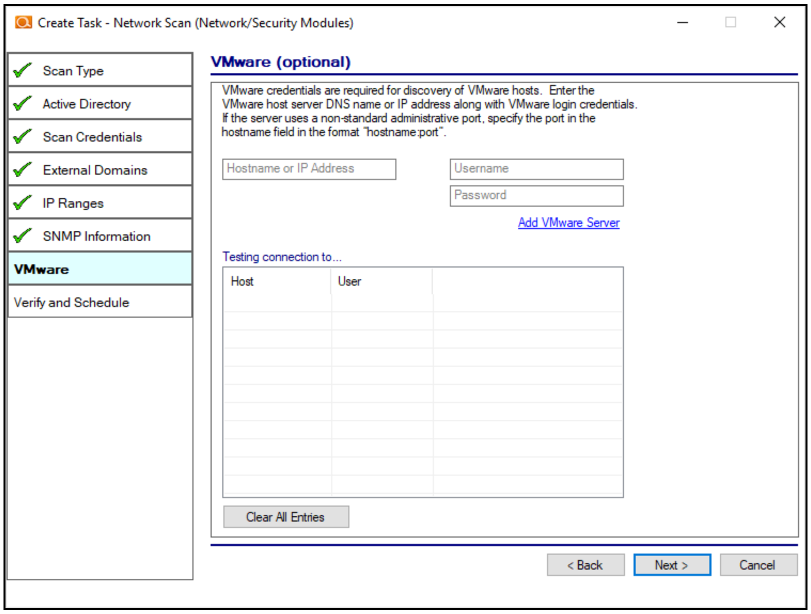
public

Advanced SNMP Options

SNMP Timeout (seconds): 10

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

© 2021 RapidFire Tools, Inc. All rights reserved.

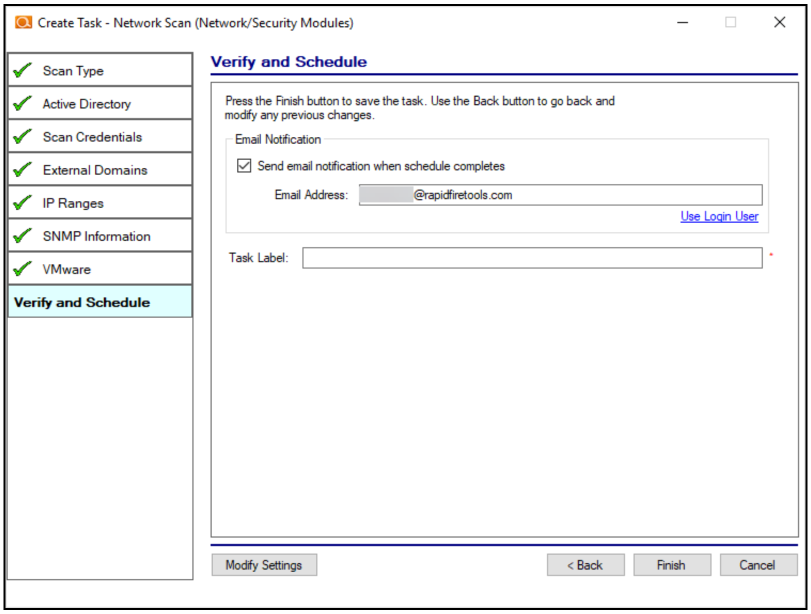


VMware (optional)

VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname field in the format "hostname:port".

Testing connection to...

10. Check "**Send an email notification when schedule completes**" to notify an individual via email that the scan task is complete. The use of this option is recommended as the time a scan takes to complete varies depending on the target network.



Verify and Schedule

Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

Email Notification

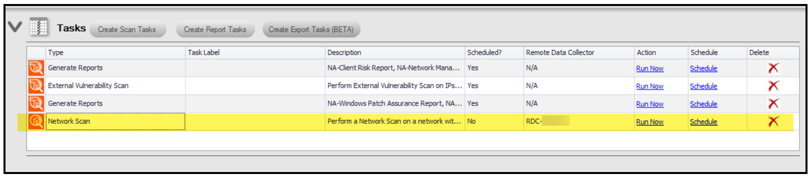
☑ Send email notification when schedule completes

Email Address: [redacted]@rapidfiretools.com

Task Label: *

11. Click on the **Finish** button to complete the scheduling of the **Network Scan** task. The task will then be displayed in the **Tasks Library** window.

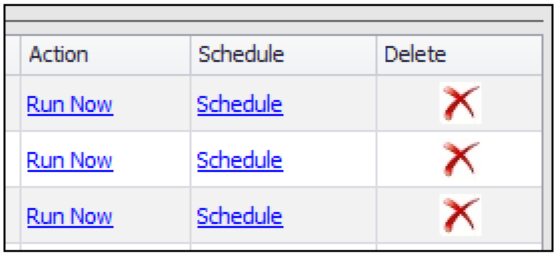
RapidFireTools® © 2021 RapidFire Tools, Inc. All rights reserved.



Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Mana...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IPs...	Yes	N/A	Run Now	Schedule	✗
Generate Reports		NA-Windows Patch Assurance Report, NA...	Yes	N/A	Run Now	Schedule	✗
Network Scan		Perform a Network Scan on a network wit...	No	RDC-[redacted]	Run Now	Schedule	✗

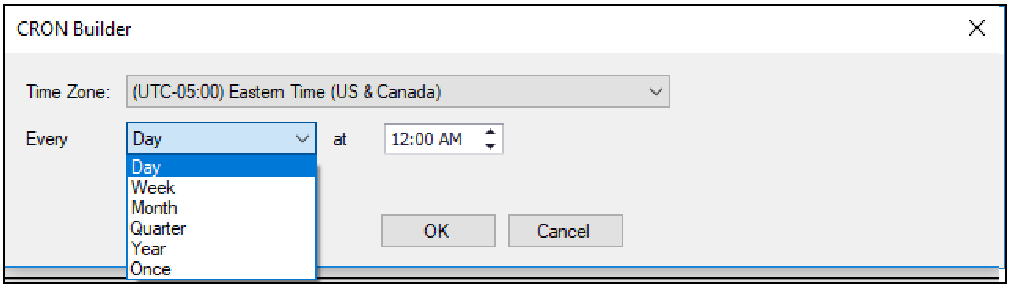
12. In order to initiate the scan, you will need to move the scan from the Task list into **Scheduled Tasks**. There are two ways to do this:

    a. Select the **Run Now** option link under the **Action** column to initiate the scan. This will place the scan directly into the **Scheduled Tasks** list.

Action	Schedule	Delete
Run Now	Schedule	✗
Run Now	Schedule	✗
Run Now	Schedule	✗

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

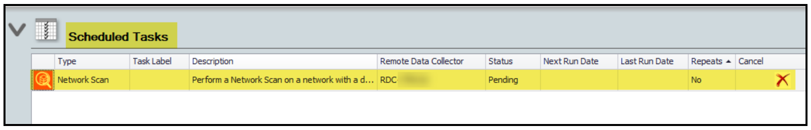
    

    CRON Builder

    Time Zone: (UTC-05:00) Eastern Time (US & Canada)

    Every Day at 12:00 AM

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



Type	Task Label	Description	Remote Data Collector	Status	Next Run Date	Last Run Date	Repeats ▲	Cancel
Network Scan		Perform a Network Scan on a network with a d...	RDC[redacted]	Pending			No	✗

© 2021 RapidFire Tools, Inc. All rights reserved.

To learn more about how to configure the scans related to a Network Assessment, please refer to the **Network Detective User Guide** at https://www.rapidfiretools.com/nd.

Note: Note that the Network Assessment Reports are only available as part of the Network Assessment module.

© 2021 RapidFire Tools, Inc. All rights reserved.

Exchange Server Assessment Scan

Set up a recurring Exchange Assessment scan to collect data for automatic Exchange Assessment reports. To create this scan task, perform the following steps:

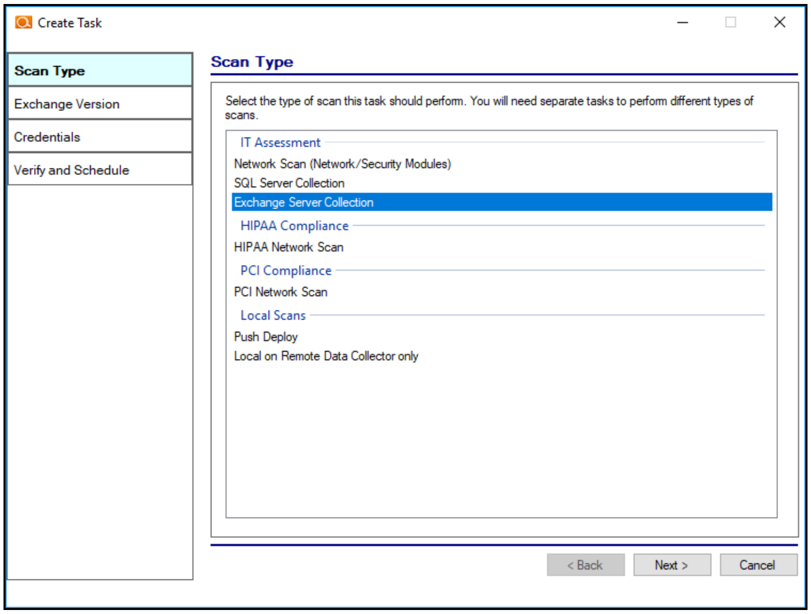
> **Note:** If you are installing the RDC to perform an Exchange assessment, you must install the RDC directly on the Exchange server itself. This is required in order for the RDC to communicate with the Exchange server using any required Exchange Shell utility available on the Exchange Server.
>
> If you are scanning Office 365, you do not need to run the RDC on the server. You will only need to enter management credentials for Office 365.

To create this scan task, perform the following steps:

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.
3. Select the **Exchange Server** option. Select the **Next** button.

© 2021 RapidFire Tools, Inc. All rights reserved.



Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

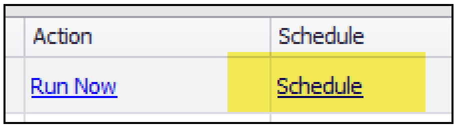
IT Assessment
Network Scan (Network/Security Modules)
SQL Server Collection
Exchange Server Collection

HIPAA Compliance
HIPAA Network Scan

PCI Compliance
PCI Network Scan

Local Scans
Push Deploy
Local on Remote Data Collector only

4. Follow the prompts to set-up the **Server**, **Port**, and **Credentials** for the SQL Server being scanned. Select the **Next** button.
5. Verify the settings, set-up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.
6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

To learn more about how to configure the scans related to a SQL Server Assessment, please refer to the **Network Detective User Guide** at https://www.rapidfiretools.com/nd.

Note: Note that the SQL Server Module's Assessment Reports are only available as part of the SQL Server Module subscription.

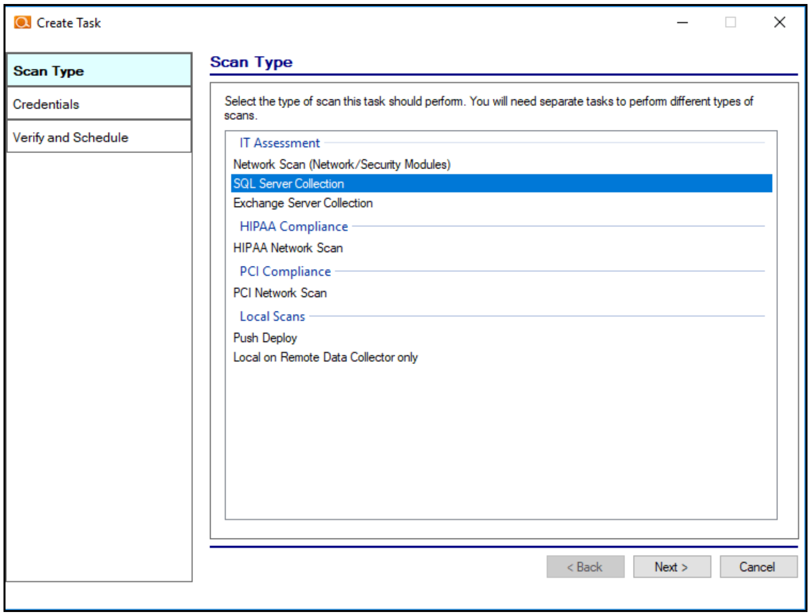
SQL Server Assessment Scan

To create this scan task, perform the following steps:

© 2021 RapidFire Tools, Inc. All rights reserved.

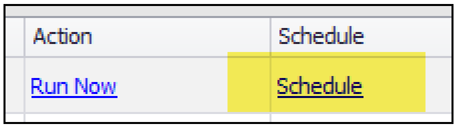
1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.
3. Select the **SQL Server** option. Select the **Next** button.



Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

4. Follow the prompts to set-up the **Server**, **Port**, and **Credentials** for the SQL Server being scanned. Select the **Next** button.
5. Verify the settings, set-up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.
6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

© 2021 RapidFire Tools, Inc. All rights reserved.

To learn more about how to configure the scans related to a SQL Server Assessment, please refer to the **Network Detective User Guide** at https://www.rapidfiretools.com/nd.

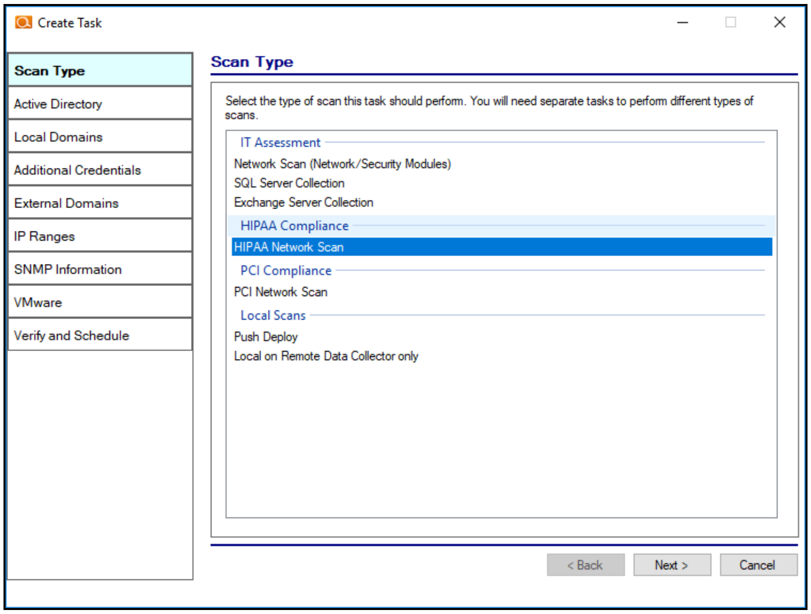
> **Note:** Note that the SQL Server Module's Assessment Reports are only available as part of the SQL Server Module subscription.

HIPAA Compliance Network Scan

To create this scan task, perform the following steps:

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.
3. Select the **HIPAA Network Scan** option. Select the **Next** button.



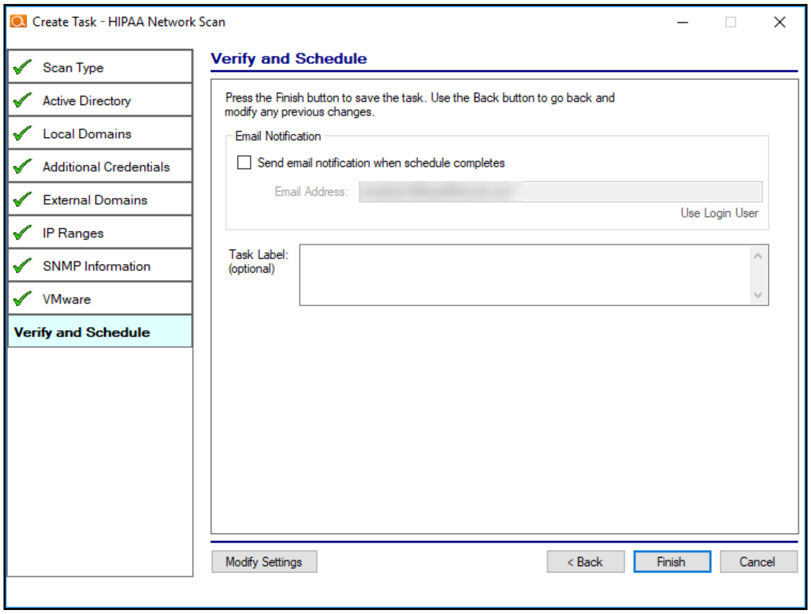
Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

IT Assessment
Network Scan (Network/Security Modules)
SQL Server Collection
Exchange Server Collection
HIPAA Compliance
HIPAA Network Scan
PCI Compliance
PCI Network Scan
Local Scans
Push Deploy
Local on Remote Data Collector only

4. Follow the prompts to set-up the Credentials, Local Domains, External Domains, IP Ranges, SNMP Information, Microsoft Base Security Analyzer (MBSA), and VMware (Optional) parameters.

RapidFireTools® © 2021 RapidFire Tools, Inc. All rights reserved.

5. Verify the settings, set up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.



Verify and Schedule

Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

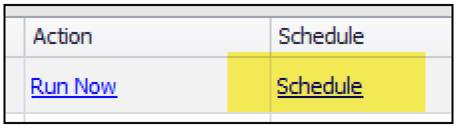
Email Notification

☐ Send email notification when schedule completes

Email Address:

Task Label: (optional)

6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

To learn more about how to configure the scans related to a HIPAA Compliance Assessment, please refer to the **HIPAA Module User Guide** at https://www.rapidfiretools.com/nd.

> **Note:** Note that the HIPAA Module's Assessment Reports are only available as part of the HIPAA Module subscription.

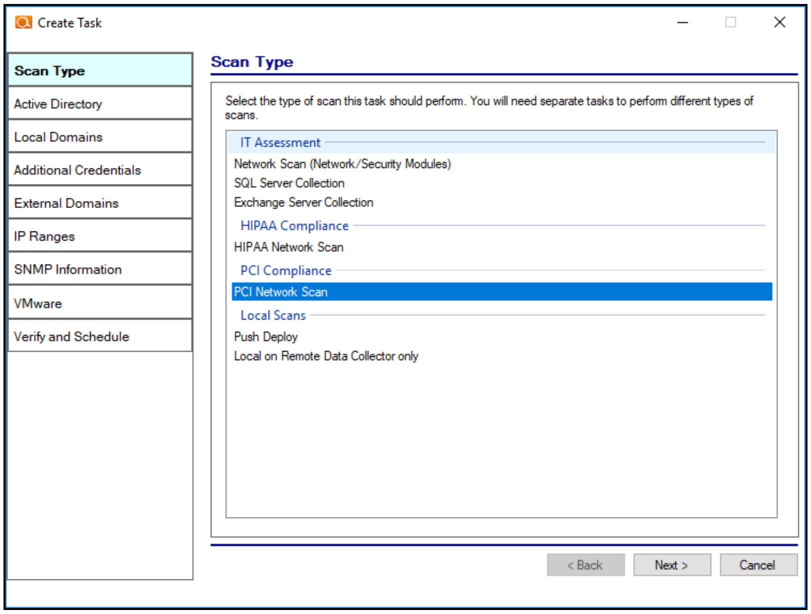
PCI Compliance Network Scan

To create this scan task, perform the following steps:

© 2021 RapidFire Tools, Inc. All rights reserved.

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.
3. Select the **PCI Network Scan** option. Select the **Next** button.



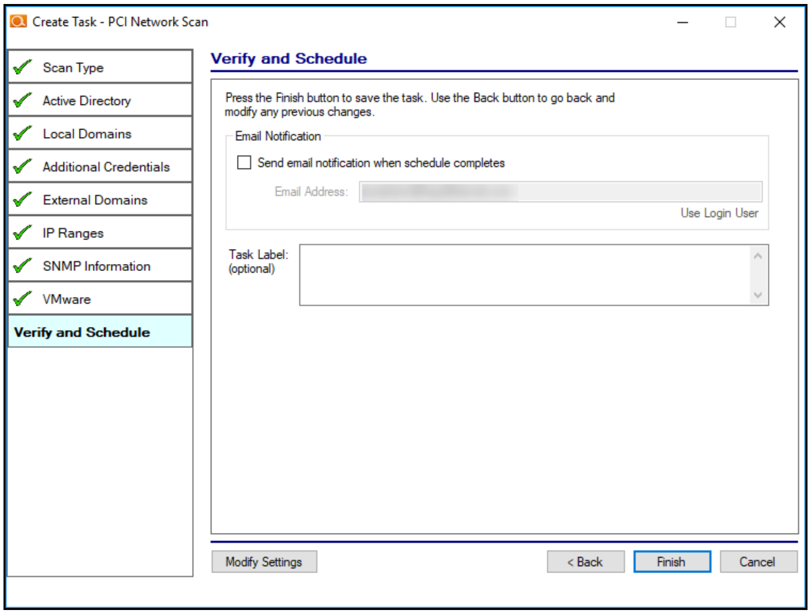
Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

IT Assessment
Network Scan (Network/Security Modules)
SQL Server Collection
Exchange Server Collection
HIPAA Compliance
HIPAA Network Scan
PCI Compliance
PCI Network Scan
Local Scans
Push Deploy
Local on Remote Data Collector only

4. Follow the prompts to set-up the Credentials, Local Domains, External Domains, IP Ranges, SNMP Information, Microsoft Base Security Analyzer (MBSA), and VMware (Optional) parameters.
5. Verify the settings, set up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.

© 2021 RapidFire Tools, Inc. All rights reserved.



Verify and Schedule

Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

Email Notification

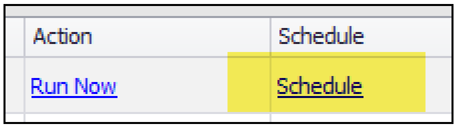
□ Send email notification when schedule completes

Email Address: [redacted]

Use Login User

Task Label: (optional)

6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

To learn more about how to configure the scans related to a PCI Compliance Assessment, please refer to the **PCI Module User Guide** at https://www.rapidfiretools.com/nd.

> **Note:** Note that the PCI Module's Assessment Reports are only available as part of the PCI Module subscription.

Push Deploy Local Computer Scans

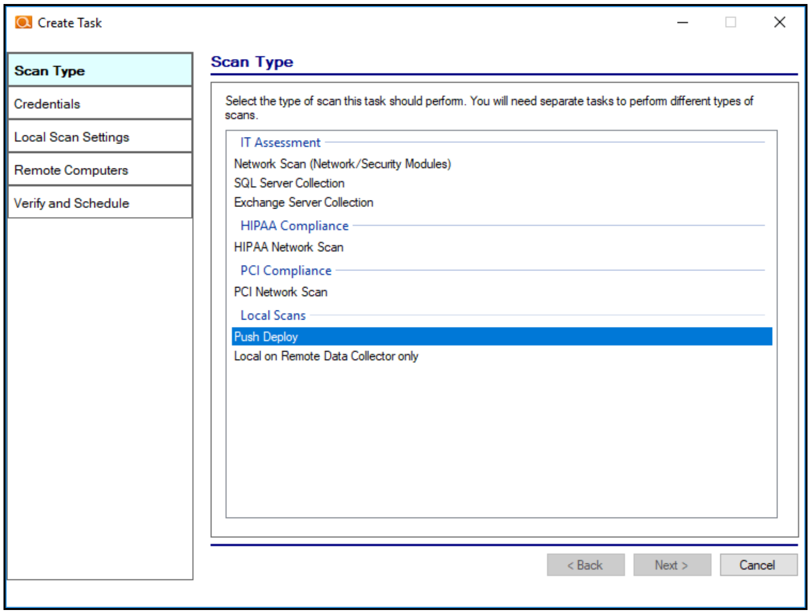
> **Note:** Use Push Deploy Local Computer Scans to gather detailed data for individual workstations. These can be used for all report types and are essential for a comprehensive assessment.

To create this scan task, perform the following steps:

© 2021 RapidFire Tools, Inc. All rights reserved.

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.
3. Select the **Local Scans Push Deploy** option to push scans to individual computers on the Network.



Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

IT Assessment
Network Scan (Network/Security Modules)
SQL Server Collection
Exchange Server Collection

HIPAA Compliance
HIPAA Network Scan

PCI Compliance
PCI Network Scan

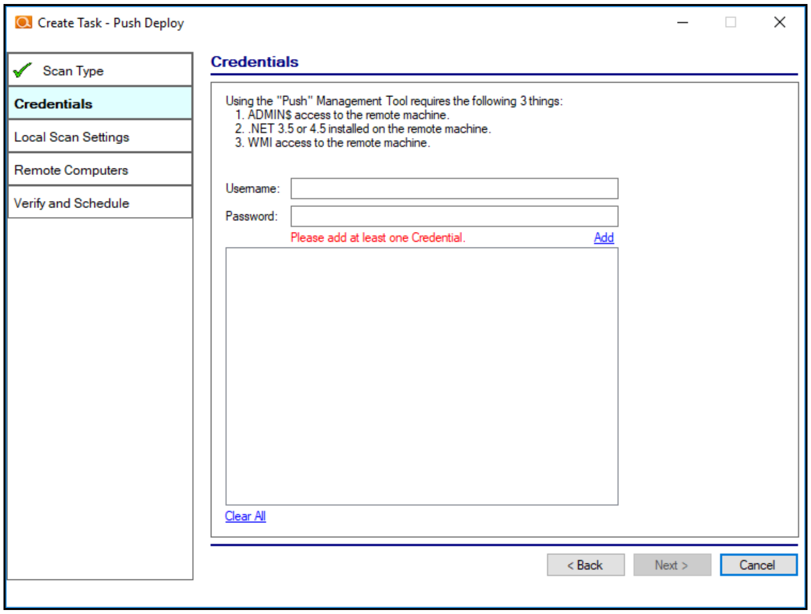
Local Scans
Push Deploy
Local on Remote Data Collector only

Note: WMI must be available and operational on your network.

Select the **Next** button.

4. Follow the prompts to set-up the **Credentials**.

© 2021 RapidFire Tools, Inc. All rights reserved.



Credentials

Using the "Push" Management Tool requires the following 3 things:
1. ADMIN$ access to the remote machine.
2. .NET 3.5 or 4.5 installed on the remote machine.
3. WMI access to the remote machine.

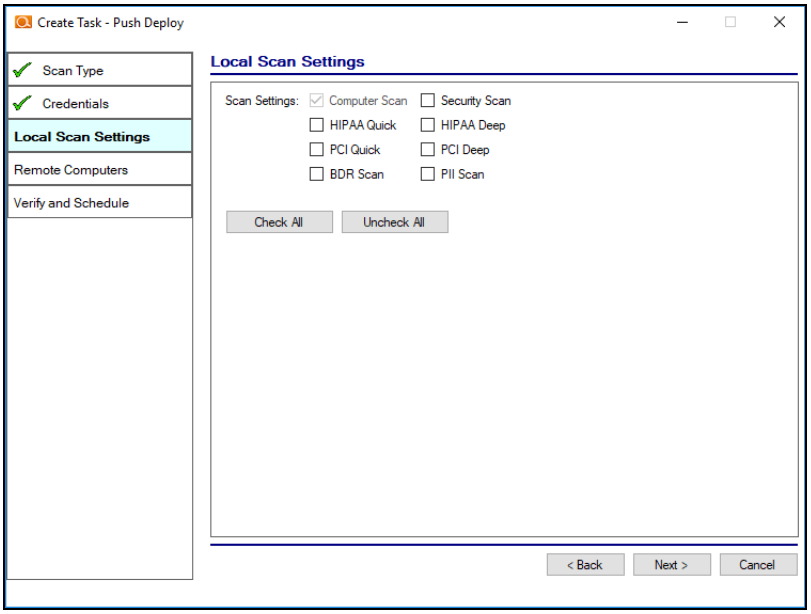
Username:

Password:

Please add at least one Credential.

Select the **Next** button.

5. The selection of the **Local Scan Settings** depends on the type of IT or Compliance Assessment Reports that you are generating with the Reporter.



Local Scan Settings

Scan Settings: ☑ Computer Scan ☐ Security Scan
☐ HIPAA Quick ☐ HIPAA Deep
☐ PCI Quick ☐ PCI Deep
☐ BDR Scan ☐ PII Scan

© 2021 RapidFire Tools, Inc. All rights reserved.

Select the **Scan Settings** to collect the scan data required to produce the reports that you want to generate. Below are the **Scan Settings** required for each assessment type.

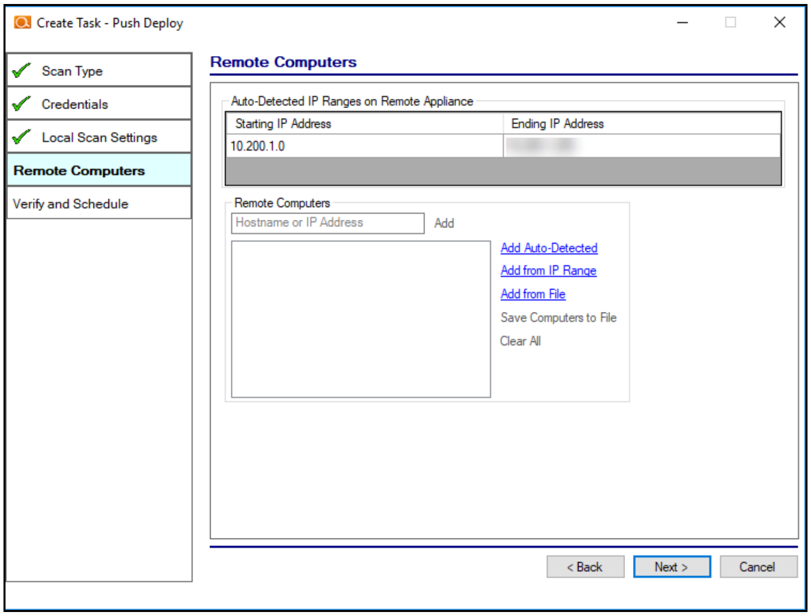
Assessment Report Type	Select these Scan Settings
Network Assessment	Computer Scan
Security Assessment	Computer and Security Scans
HIPAA Assessment	HIPAA Deep*
PCI Assessment	PCI Deep*

Note: The “Quick” version of this scan can be used instead of the “Deep” scan in order to reduce scan time. Use of the ‘Quick” scans may result in instances of ePHI or Cardholder Data not being identified.

Select the **Next** button.

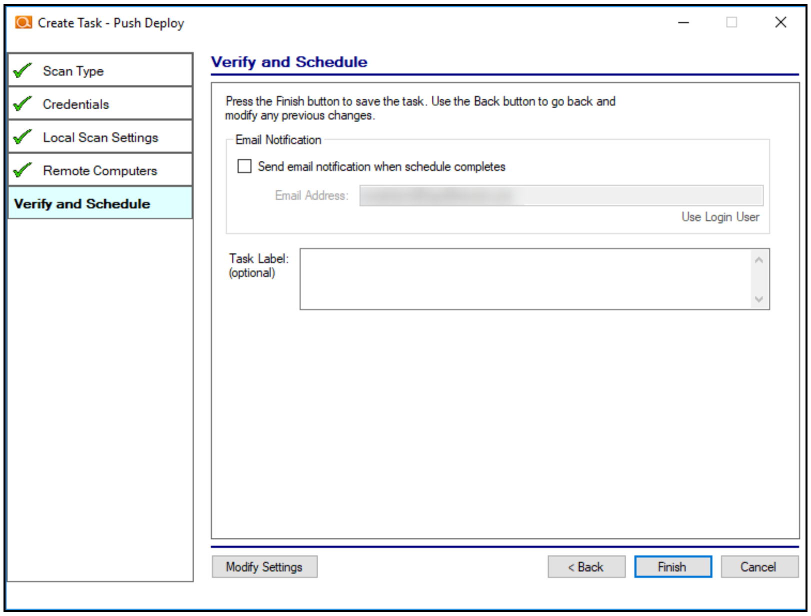
6. Define the **Remote Computer** IP addresses for the computers being scanned.

Select the **Next** button.



Starting IP Address	Ending IP Address
10.200.1.0	[redacted]

7. Verify the settings, set up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.



Create Task - Push Deploy

- ✓ Scan Type
- ✓ Credentials
- ✓ Local Scan Settings
- ✓ Remote Computers
- Verify and Schedule

Verify and Schedule

Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

Email Notification

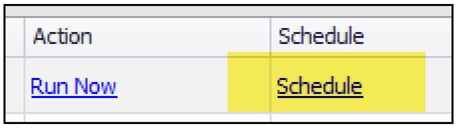
□ Send email notification when schedule completes

Email Address: [redacted]

Use Login User

Task Label: (optional)

8. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

Local Scan for a Computer Running the Remote Data Collector

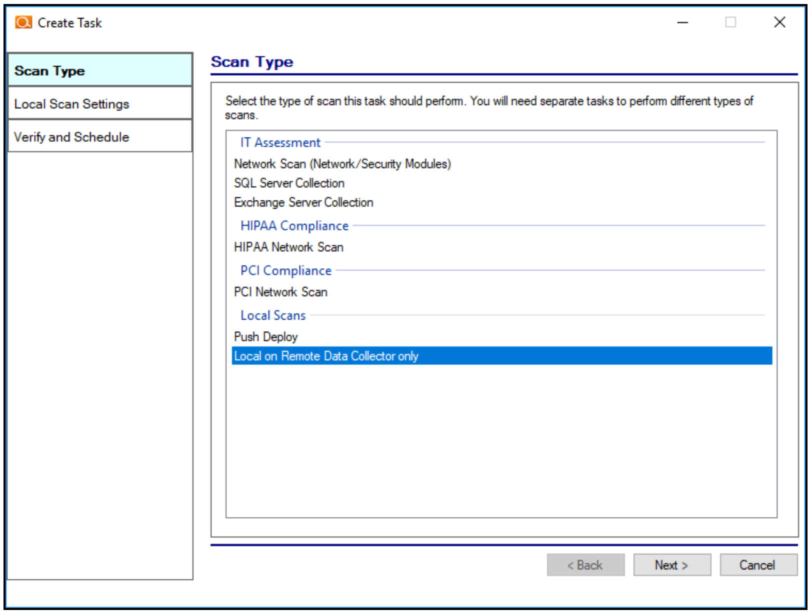
This scan will collect data only on the computer running the RDC. To create this scan task, perform the following steps:

1. Open the **Reporter** dashboard.

2. Click **Create Scan Tasks** and select the RDC.

© 2021 RapidFire Tools, Inc. All rights reserved.

3. Select the **Local on Remote Data Collector Only** scan option to perform a local scan on the computer used to run the Remote Data Collector.



Create Task

Scan Type

Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.

IT Assessment
- Network Scan (Network/Security Modules)
- SQL Server Collection
- Exchange Server Collection

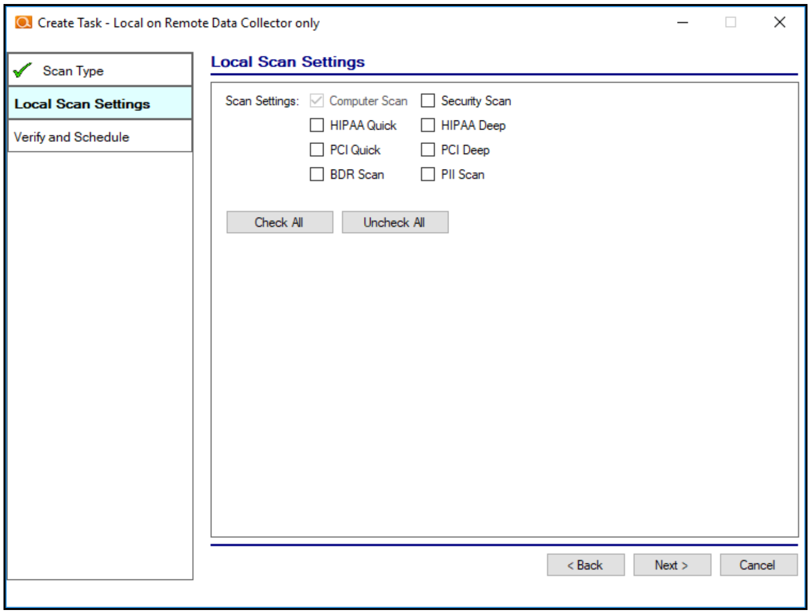
HIPAA Compliance
- HIPAA Network Scan

PCI Compliance
- PCI Network Scan

Local Scans
- Push Deploy
- Local on Remote Data Collector only

Select the **Next** button.

4. The selection of the **Local Scan Settings** depends on the type of IT or Compliance Assessment Reports that you are generating with the Reporter.



Create Task - Local on Remote Data Collector only

Local Scan Settings

Scan Settings: ☑ Computer Scan ☐ Security Scan
☐ HIPAA Quick ☐ HIPAA Deep
☐ PCI Quick ☐ PCI Deep
☐ BDR Scan ☐ PII Scan

© 2021 RapidFire Tools, Inc. All rights reserved.

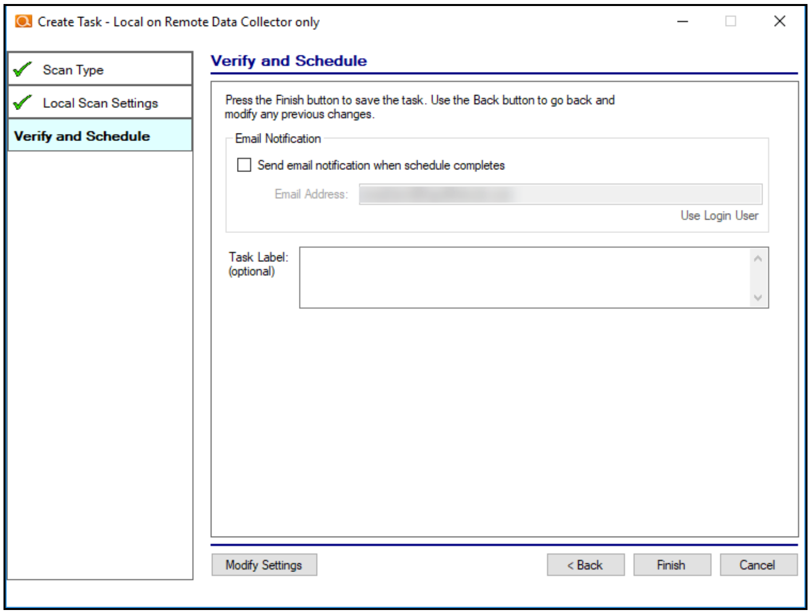
Select the **Scan Settings** to collect the scan data required to produce the reports that you want to generate. Below are the **Scan Settings** required for each assessment type.

Assessment Report Type	Select these Scan Settings
Network Assessment	Computer Scan
Security Assessment	Computer and Security Scans
HIPAA Assessment	HIPAA Deep*
PCI Assessment	PCI Deep*

> **Note:** The “Quick” version of this scan can be used instead of the “Deep” scan in order to reduce scan time. Use of the ‘Quick” scans may result in instances of ePHI or Cardholder Data not being identified.

Select the **Next** button.

5. Verify the settings, set up an **Email Notification** to be sent once the scan is completed, and select the **Finish** button to create the scan task.



Verify and Schedule

Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.

Email Notification

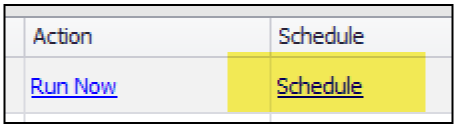
□ Send email notification when schedule completes

Email Address: [redacted]

Use Login User

Task Label: (optional)

6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Action	Schedule
Run Now	Schedule

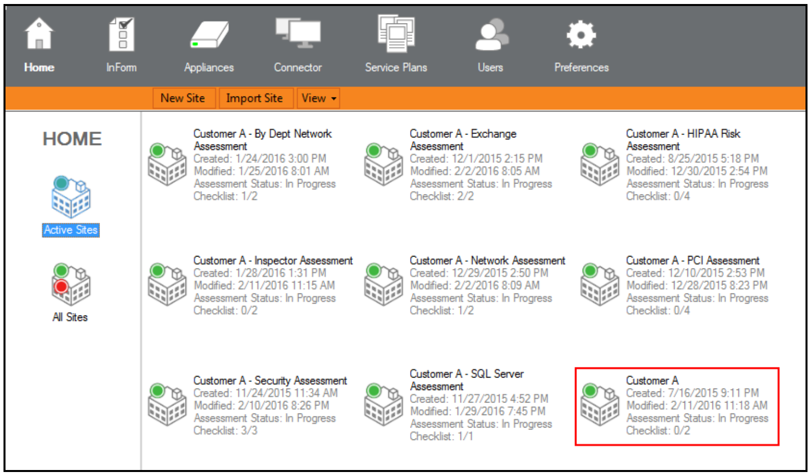
© 2021 RapidFire Tools, Inc. All rights reserved.

Configuring the Local Data Scan Merges

When local scans are performed the Network Detective **Data Collectors** or by an **Appliance**, the scan files can be merged into a particular domain data set. The **Configuration of Local Scan Merges** feature allows you to select which method you prefer to use when merging local scans.

This setting will impact Automated Report Generation.

To select the process to be used by the **Appliance** to **Merge** any **Local Scan Data** into a primary domain data set, perform the following steps.



Customer A - By Dept Network Assessment
Created: 1/24/2016 3:00 PM
Modified: 1/25/2016 8:01 AM
Assessment Status: In Progress
Checklist: 1/2

Customer A - Exchange Assessment
Created: 12/1/2015 2:15 PM
Modified: 2/2/2016 8:05 AM
Assessment Status: In Progress
Checklist: 2/2

Customer A - HIPAA Risk Assessment
Created: 8/25/2015 5:18 PM
Modified: 12/30/2015 2:54 PM
Assessment Status: In Progress
Checklist: 0/4

Customer A - Inspector Assessment
Created: 1/28/2016 1:31 PM
Modified: 2/11/2016 11:15 AM
Assessment Status: In Progress
Checklist: 0/2

Customer A - Network Assessment
Created: 12/29/2015 2:50 PM
Modified: 2/2/2016 8:09 AM
Assessment Status: In Progress
Checklist: 1/2

Customer A - PCI Assessment
Created: 12/10/2015 2:53 PM
Modified: 12/28/2015 8:23 PM
Assessment Status: In Progress
Checklist: 0/4

Customer A - Security Assessment
Created: 11/24/2015 11:34 AM
Modified: 2/10/2016 8:26 PM
Assessment Status: In Progress
Checklist: 3/3

Customer A - SQL Server Assessment
Created: 11/27/2015 4:52 PM
Modified: 1/29/2016 7:45 PM
Assessment Status: In Progress
Checklist: 1/1

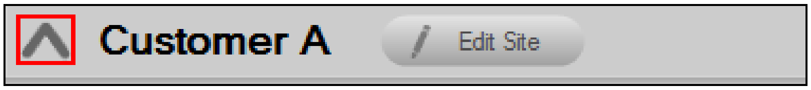
Customer A
Created: 7/16/2015 9:11 PM
Modified: 2/11/2016 11:18 AM
Assessment Status: In Progress
Checklist: 0/2

Step 1 — Select and Open the Site

Double click your mouse pointer on the **Site** that you are configuring to use the **Reporter** Appliance.

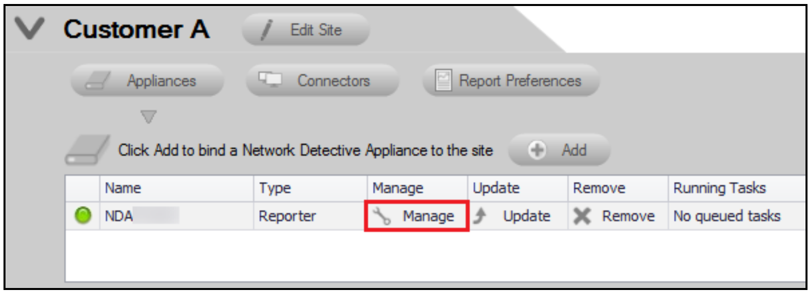
Step 2 — Select Manage Appliance

After the **Site** has been opened, select the **Selector** symbol to expand the **Site** properties to view any **Appliances** associated with the **Site**.



Then select the **Manage** option presented for the **Appliance** listed.

© 2021 RapidFire Tools, Inc. All rights reserved.



Customer A

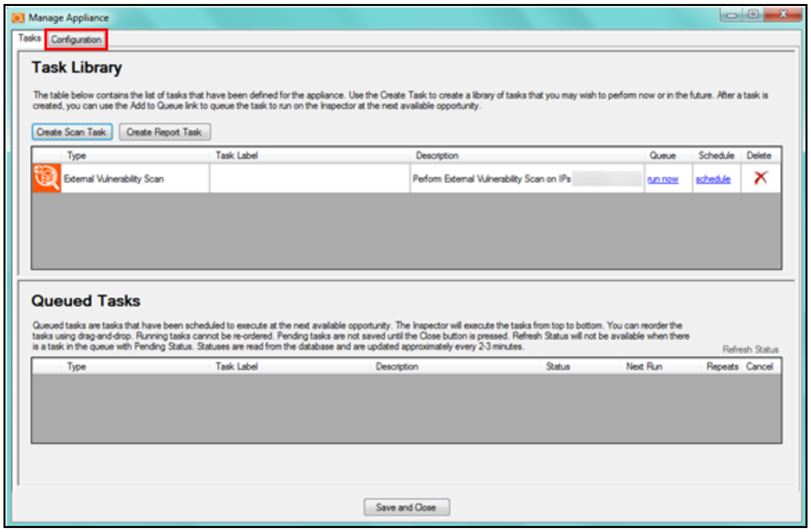
Click Add to bind a Network Detective Appliance to the site

	Name	Type	Manage	Update	Remove	Running Tasks
●	NDA [redacted]	Reporter	Manage	Update	✗ Remove	No queued tasks

The Manage Reporter window will be displayed.

Step 3 — Set Scan Data Merge Configuration

Select the **Configuration** tab in the **Manage Appliance** to view the **Local Scan Merge** settings.



Manage Appliance

Task Library

The table below contains the list of tasks that have been defined for the appliance. Use the Create Task to create a library of tasks that you may wish to perform now or in the future. After a task is created, you can use the Add to Queue link to queue the task to run on the Inspector at the next available opportunity.

	Type	Task Label	Description	Queue	Schedule	Delete
	External Vulnerability Scan		Perform External Vulnerability Scan on IPs [redacted]	run now	schedule	✗

Queued Tasks

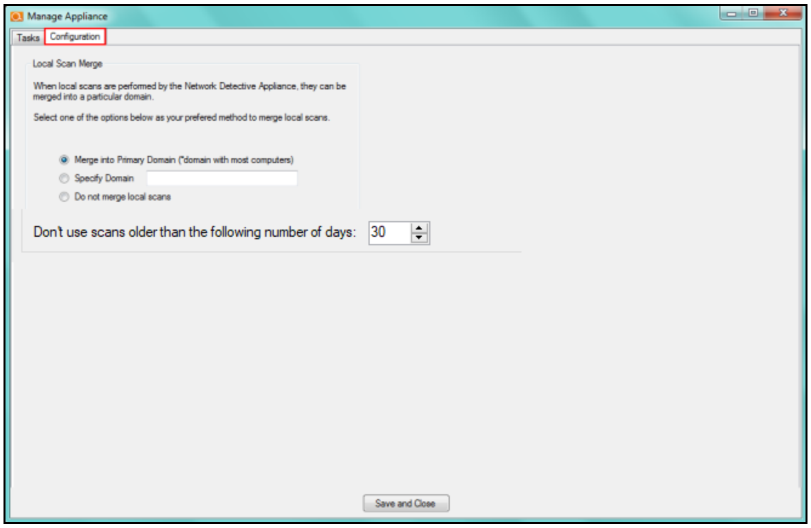
Queued tasks are tasks that have been scheduled to execute at the next available opportunity. The Inspector will execute the tasks from top to bottom. You can reorder the tasks using drag-and-drop. Running tasks cannot be re-ordered. Pending tasks are not saved until the Close button is pressed. Refresh Status will not be available when there is a task in the queue with Pending Status. Statuses are read from the database and are updated approximately every 2-3 minutes.

	Type	Task Label	Description	Status	Next Run	Repeats	Cancel

Step 4 — Set the Local Scan Merge Settings and Save Settings

1. Select the preferred **Local Scan Merge** method, or select, **Do Not Merge Local Scans**.

© 2021 RapidFire Tools, Inc. All rights reserved.



Local Scan Merge

When local scans are performed by the Network Detective Appliance, they can be merged into a particular domain.

Select one of the options below as your prefered method to merge local scans.

● Merge into Primary Domain (*domain with most computers)
○ Specify Domain
○ Do not merge local scans

Don't use scans older than the following number of days: 30

For example, you may wish to perform local scans manually on computers that are not connected to an Active Directory domain. From the **Local Scan Merge** screen, you can decide how these local scans fit into your reports:

- **Merge into Primary Domain**: This will merge local scans into the primary Active Directory Domain (the Domain with the most computers)
- **Specify Domain**: The computers scanned will be associated with this Domain in the reports you generate.
- **Do not merge local scans**: The local scans for computers will appear separately in the reports you generate (they will not be associated with a Domain).

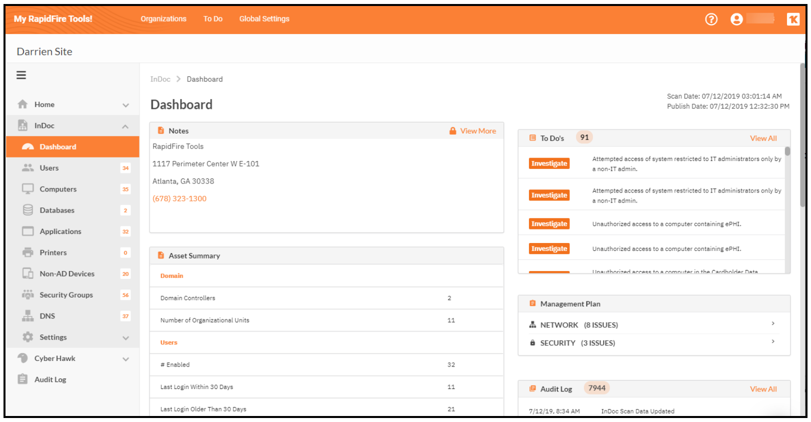
2. Next, set the option to prevent using scans that are older than a specified number of days.
3. Then select the Save and Close button to store the **Scan Merge Settings**.

© 2021 RapidFire Tools, Inc. All rights reserved.

InDoc and the RapidFire Tools Portal

InDoc uses the stream of data from Reporter to help your team find, manage, and document everything at a Site.

With your Reporter subscription, you can use **InDoc** and the RapidFire Tools Portal to dive deeper into the data you collect from your Reporter sites. With InDoc, you can supplement Reporter data with your own network documentation to make managing your client's assets a breeze. Access the RapidFire Tools Portal at https://www.youritportal.com.



Darrien Site

Dashboard

Scan Date: 07/12/2019 03:01:14 AM
Publish Date: 07/12/2019 12:32:30 PM

Notes

RapidFire Tools
1117 Perimeter Center W E-101
Atlanta, GA 30338
(678) 323-1300

Asset Summary

Domain	
Domain Controllers	2
Number of Organizational Units	11
Users	
# Enabled	32
Last Login Within 30 Days	11
Last Login Older Than 30 Days	21

To Do's 91

- Investigate — Attempted access of system restricted to IT administrators only by a non-IT admin.
- Investigate — Attempted access of system restricted to IT administrators only by a non-IT admin.
- Investigate — Unauthorized access to a computer containing ePHI.
- Investigate — Unauthorized access to a computer containing ePHI.
- Unauthorized access to a computer in the Cardholder Data

Management Plan

- NETWORK (8 ISSUES)
- SECURITY (3 ISSUES)

Audit Log 7944

7/12/19, 8:34 AM InDoc Scan Data Updated

With InDoc, you can:

- **Explore and view data** from all network assets discovered during the latest scan and take immediate action.
- See **To Do** items and **Risk Management Plan** issues for the Site.
- Annotate each asset on the client's network with your own **Notes** and **Procedures**.
- See relationships between assets by linking together **Related Items**.
- Safely share **Confidential Notes**, including passwords, in a secure storage area.
- Manage the **Smart Tags** associated with each network asset. Smart Tags are used to monitor network security with Cyber Hawk, our security service delivery system.

© 2021 RapidFire Tools, Inc. All rights reserved.

Requirements for using InDoc with Reporter

Using InDoc with Reporter is easy — but you need to have Reporter set up first. Review the requirements for using InDoc with Reporter below.

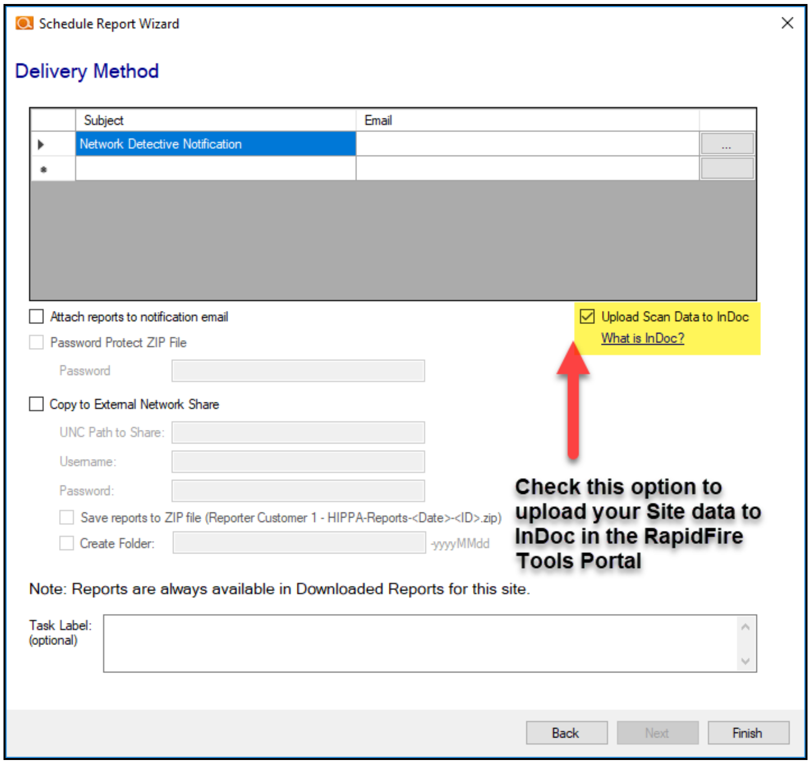
1. You must have a subscription to the Network Assessment Module and Reporter.
2. Reporter must be installed on the MSP network and associated with one or more Sites in Network Detective. You can only use InDoc with Sites that have an associated Reporter in Network Detective.
3. One or more Remote Data Collectors (RDC) must be installed on the client network (s) and associated with the Reporter Sites using Connector(s).
4. The RDC must be configured to perform scans on the network. The RDC must also have performed a scan and uploaded it to the Network Detective Site through the Connector.

   Note: See "Setting Up Reporter" on page 16 for detailed instructions.

5. You must have automated report tasks set up, and select **Upload Scan Data to InDoc** when configuring your report tasks.

   Note: **Upload Scan Data to InDoc** is selected by default, and will be retroactively applied to your previously-created report jobs.

© 2021 RapidFire Tools, Inc. All rights reserved.



Delivery Method

	Subject	Email
▶	Network Detective Notification	
*		

□ Attach reports to notification email

□ Password Protect ZIP File

Password

□ Copy to External Network Share

UNC Path to Share:

Username:

Password:

□ Save reports to ZIP file (Reporter Customer 1 - HIPPA-Reports-<Date>-<ID>.zip)

□ Create Folder: -yyyyMMdd

☑ Upload Scan Data to InDoc

What is InDoc?

Check this option to upload your Site data to InDoc in the RapidFire Tools Portal

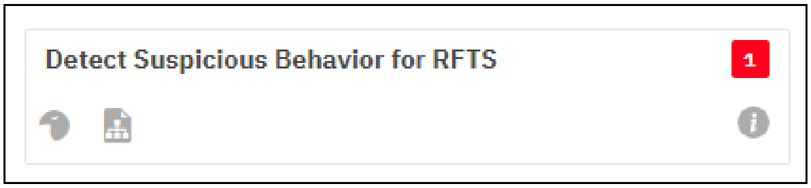
Note: Reports are always available in Downloaded Reports for this site.

Task Label: (optional)

6. Users who wish to access InDoc in the RapidFire Tools Portal must have the correct **Global** and **Site**-specific **Role** permissions. User Roles are configured in the Portal. See "InDoc User Permissions" on page 138.
7. Your reports must have successfully generated.

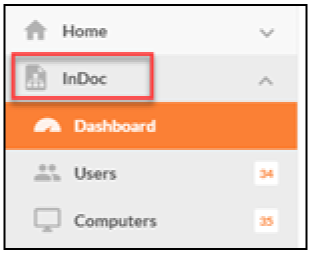
Once you set up InDoc with these steps, your **InDoc** Site will appear in the RapidFire Tools Portal.

Tip: If you are using Reporter with Cyber Hawk, you can access both tools from the same Site.



Click on the Site to view the **InDoc** tab to see the InDoc **Dashboard**.

© 2021 RapidFire Tools, Inc. All rights reserved.

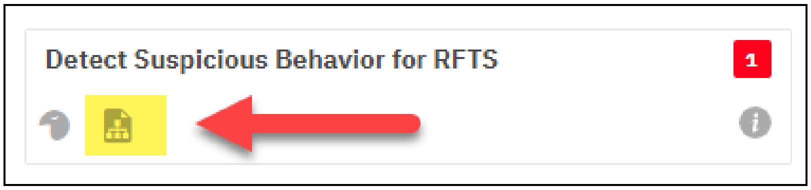

Home
InDoc
Dashboard
Users
34
Computers
35

Using InDoc (RapidFire Tools Portal)

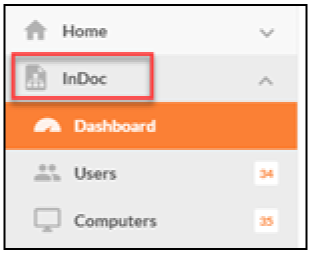
Once you set up Reporter for automated reporting and data collection, you can begin using InDoc in the RapidFire Tools Portal. (See "Requirements for using InDoc with Reporter" on page 112). Each time scans are performed and reports successfully generated, InDoc will be updated with the latest data. To access InDoc:

1. Log in to the RapidFire Tools Portal with your Network Detective account credentials.
2. Open the Site for which you would like to use InDoc. You can only use InDoc with Sites that have an associated Reporter in Network Detective.

   Note: InDoc Sites are marked with an InDoc site badge.

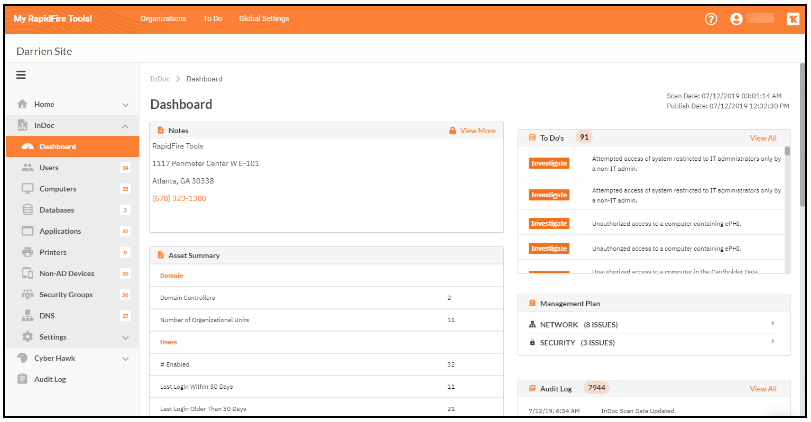
3. Click on the **InDoc tab** > **Dashboard**.

   From here you can view details about network assets taken from the latest scan data — and you can begin adding your own supplementary documentation. The InDoc dashboard gives you a high level overview of the activity at the Site, including

© 2021 RapidFire Tools, Inc. All rights reserved.

pending **To Do** items, an **Asset Summary**, and **Notes** from your tech group.



Dashboard

Scan Date: 07/12/2019 03:01:14 AM
Publish Date: 07/12/2019 12:32:30 PM

Notes

RapidFire Tools

1117 Perimeter Center W E-101

Atlanta, GA 30338

(678) 323-1300

Asset Summary

Domain	
Domain Controllers	2
Number of Organizational Units	11
Users	
# Enabled	32
Last Login Within 30 Days	11
Last Login Older Than 30 Days	21

To Do's 91

- Investigate — Attempted access of system restricted to IT administrators only by a non-IT admin.
- Investigate — Attempted access of system restricted to IT administrators only by a non-IT admin.
- Investigate — Unauthorized access to a computer containing ePHI.
- Investigate — Unauthorized access to a computer containing ePHI.
- Unauthorized access to a computer in the Cardholder Data

Management Plan

NETWORK (8 ISSUES)
SECURITY (3 ISSUES)

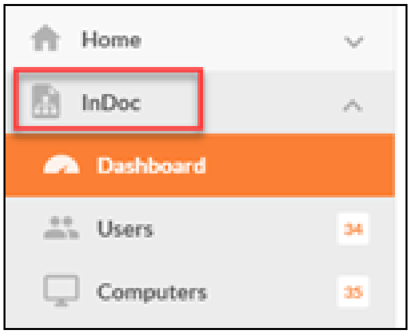
Audit Log 7944

7/12/19, 8:34 AM InDoc Scan Data Updated

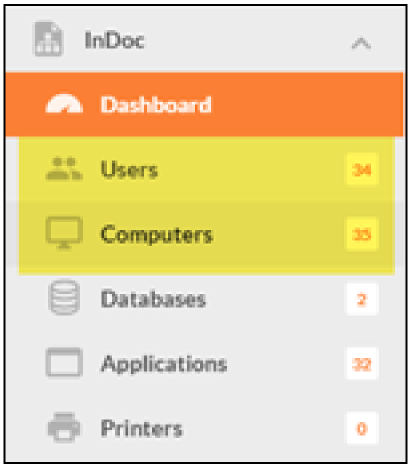
© 2021 RapidFire Tools, Inc. All rights reserved.

Explore Network Assets with InDoc

InDoc uses the stream of data from Reporter to help your team find, manage, and document everything at a Site. You access InDoc for your Sites in the RapidFire Tools Portal at https://www.youritportal.com. From the **InDoc tab** > **Overview**, you can view detailed information about network assets.

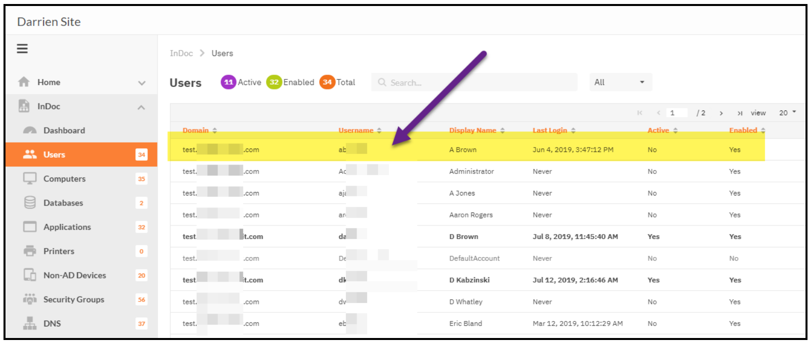


The available asset categories appear below the Dashboard button. These assets are divided into categories, such as **Users** and **Computers**. Click on an asset category to view a list of assets detected on the network during the most recent scan.



Click on a specific asset from the list for a detailed view showing information specific to the asset type. This information is dynamically updated by Reporter.

© 2021 RapidFire Tools, Inc. All rights reserved.



Domain	Username	Display Name	Last Login	Active	Enabled
test.[redacted].com	ab[redacted]	A Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test.[redacted].com	Ac[redacted]	Administrator	Never	No	Yes
test.[redacted].com	aj[redacted]	A Jones	Never	No	Yes
test.[redacted].com	ar[redacted]	Aaron Rogers	Never	No	Yes
test[redacted]it.com	**da[redacted]**	**D Brown**	**Jul 8, 2019, 11:45:40 AM**	**Yes**	**Yes**
test.[redacted].com	De[redacted]	DefaultAccount	Never	No	No
test[redacted]it.com	**dk[redacted]**	**D Kabzinski**	**Jul 12, 2019, 2:16:46 AM**	**Yes**	**Yes**
test.[redacted].com	dv[redacted]	D Whatley	Never	No	Yes
test.[redacted].com	eb[redacted]	Eric Bland	Mar 12, 2019, 10:12:29 AM	No	Yes

Note: Currently, you can explore details for **Users** and **Computers**. More categories will be added in the future.

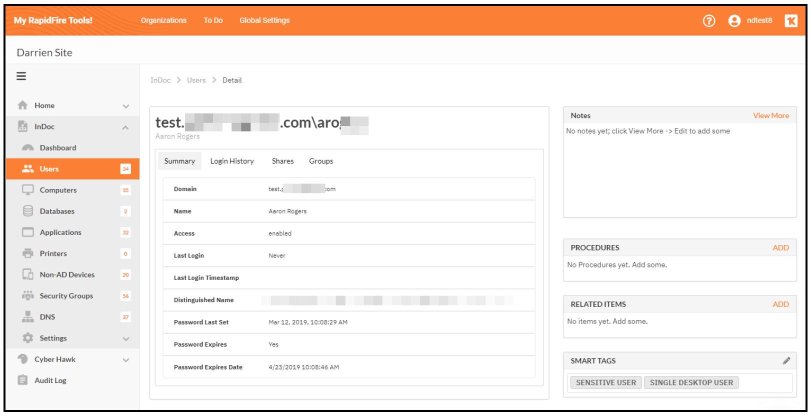
View Data about Network Assets

To view data about particular assets:

1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the **InDoc tab** > **Overview**.
3. Choose an asset category ("Users" or "Computers," for example). The list of detected assets will appear.
4. Click on a specific asset from the list. From here you can add your own **Notes**, **Procedures**, **Related Items**, and **Smart Tags** to the asset.

Users

The **Users** details page shows information such as domain, last login, password expiration, login history, and groups.



test.[redacted].com\aro[redacted]

Aaron Rogers

Domain	test.[redacted]om
Name	Aaron Rogers
Access	enabled
Last Login	Never
Last Login Timestamp	
Distinguished Name	[redacted]
Password Last Set	Mar 12, 2019, 10:08:29 AM
Password Expires	Yes
Password Expires Date	4/23/2019 10:08:46 AM

No notes yet; click View More -> Edit to add some

No Procedures yet. Add some.

No items yet. Add some.

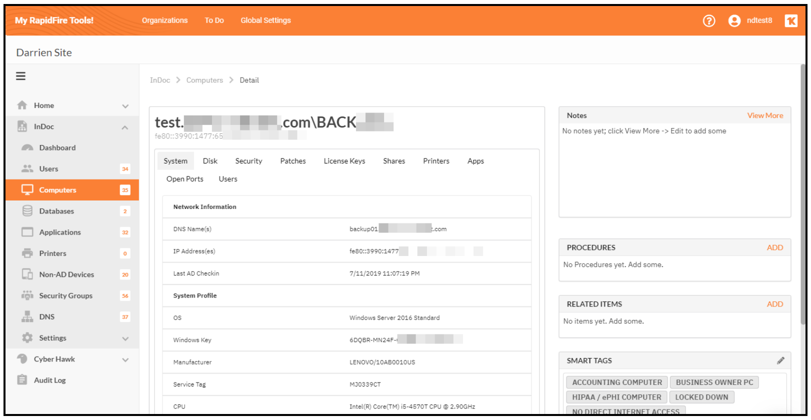
© 2021 RapidFire Tools, Inc. All rights reserved.

You can also view or add Notes, Procedures, Related Items, and/or Smart Tags for the user. For example:

- Assign **Related Items** to help your team know which network assets are the user's, such as PCs or printers.
- Assign **Smart Tags** to the User, such as Business Owner, Accounting User, or IT Admin.

Computers

The **Computers** details page shows information such as IP address, operating system, Windows keys, service tags, CPU, RAM, Disk, Applications, and associated printers. Up to date information on assets can be provided to Technicians on demand.



test.[redacted].com\BACK[redacted]
fe80::3990:1477:65[redacted]

Network Information	
DNS Name(s)	backup01[redacted].com
IP Address(es)	fe80::3990:1477[redacted]
Last AD Checkin	7/11/2019 11:07:19 PM
System Profile	
OS	Windows Server 2016 Standard
Windows Key	6DQBR-MN24F-[redacted]
Manufacturer	LENOVO/10AB0010US
Service Tag	MJ0339CT
CPU	Intel(R) Core(TM) i5-4570T CPU @ 2.90GHz

Notes View More
No notes yet; click View More -> Edit to add some

PROCEDURES ADD
No Procedures yet. Add some.

RELATED ITEMS ADD
No items yet. Add some.

SMART TAGS
ACCOUNTING COMPUTER
BUSINESS OWNER PC
HIPAA / ePHI COMPUTER
LOCKED DOWN
NO DIRECT INTERNET ACCESS

For each computer, you can also add Notes, Procedures, Related Items, and/or Smart Tags for the user. For example:

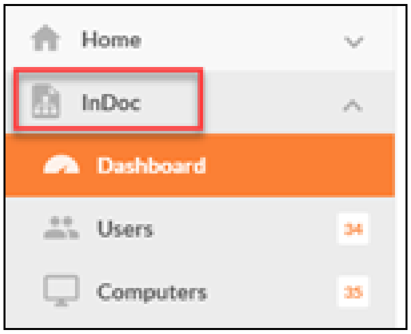
- Add a **Procedure** to a computer to help your team troubleshoot known issues specific to that computer
- Add a **Related Item** to help your team see which users log on to the PC
- Add a **Smart Tag** to a sensitive computer, such as ACCOUNTING or PCI/HIPAA

© 2021 RapidFire Tools, Inc. All rights reserved.

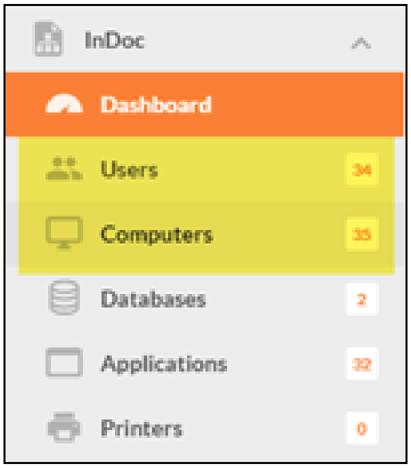
Add a Note to an Asset (InDoc)

You can use InDoc to write your own notes and associate them with specific network assets. This is great for labeling and keeping track of important assets. Use Notes to help your tech group understand the purpose and function of each machine on the network.

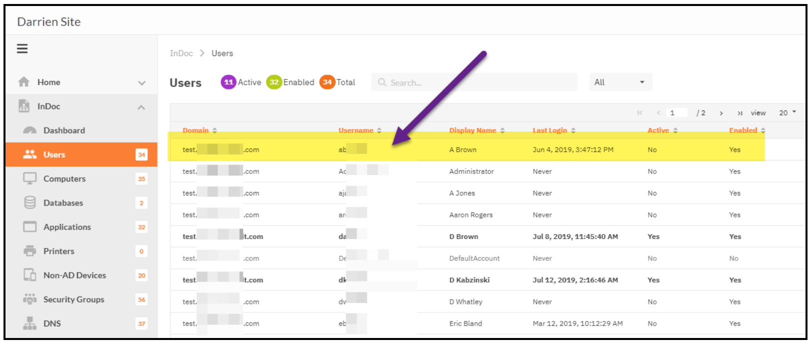
1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc tab** > **Overview**.



3. Choose an asset category ("Users" or "Computers," for example).

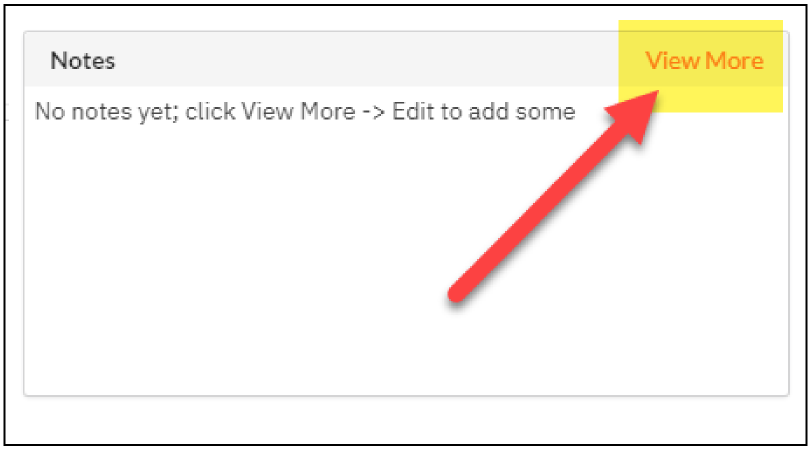


4. The list of detected assets will appear. Click on a specific asset from the list.



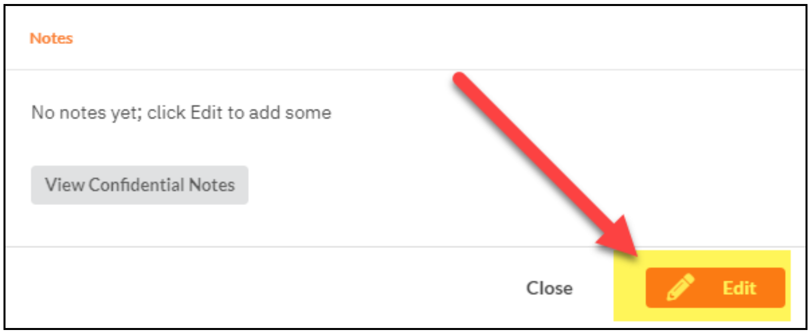
Domain	Username	Display Name	Last Login	Active	Enabled
test.[redacted].com	ab[redacted]	A Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test.[redacted].com	Ac[redacted]	Administrator	Never	No	Yes
test.[redacted].com	aj[redacted]	A Jones	Never	No	Yes
test.[redacted].com	ar[redacted]	Aaron Rogers	Never	No	Yes
test[redacted]t.com	**da[redacted]**	**D Brown**	**Jul 8, 2019, 11:45:40 AM**	**Yes**	**Yes**
test.[redacted].com	De[redacted]	DefaultAccount	Never	No	No
test[redacted]t.com	**dk[redacted]**	**D Kabzinski**	**Jul 12, 2019, 2:16:46 AM**	**Yes**	**Yes**
test.[redacted].com	dv[redacted]	D Whatley	Never	No	Yes
test.[redacted].com	eb[redacted]	Eric Bland	Mar 12, 2019, 10:12:29 AM	No	Yes

5. Next to the **Notes** panel, click **View More**.



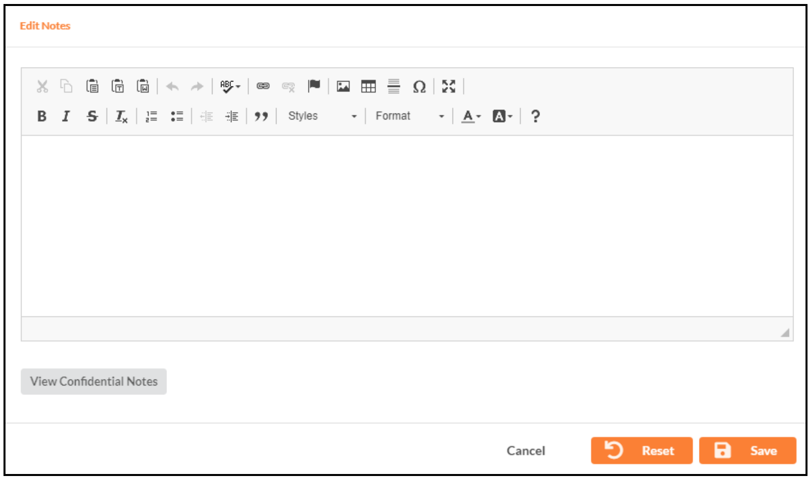
No notes yet; click View More -> Edit to add some

6. Click **Edit**.

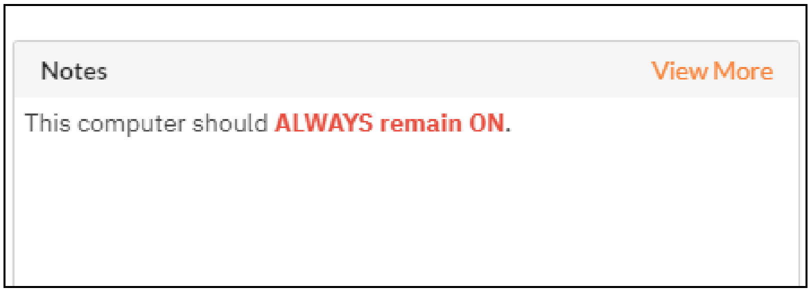


No notes yet; click Edit to add some

7. Use the editor to add or change your notes.



8. Click **Save**. Your Note will appear under the Notes panel.



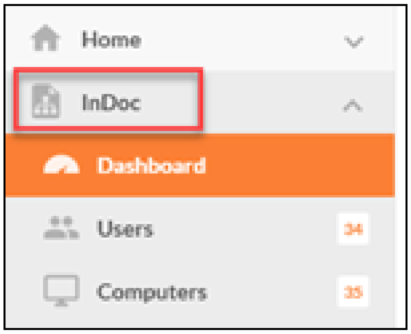
This computer should **ALWAYS remain ON**.

Add and View Confidential Notes (InDoc)

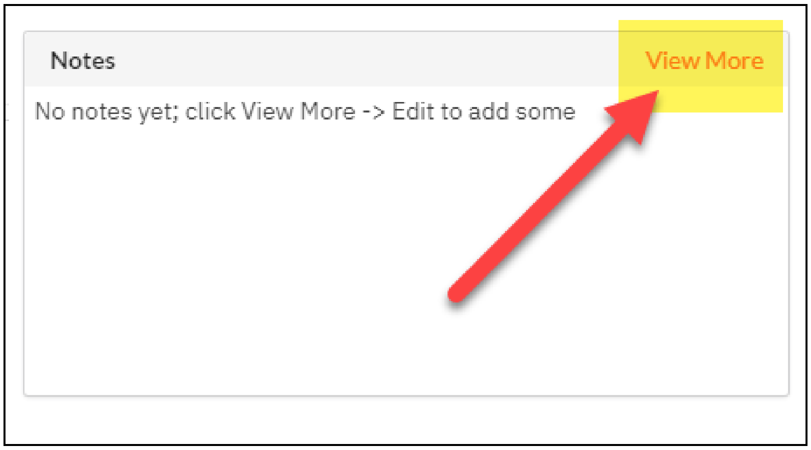
Note: Before you can add or view confidential notes with InDoc, you first need to "Enable Confidential Information Protection for InDoc" on page 125. You will also need to be granted confidential access by a Master or Admin user.

To create or view confidential notes with InDoc:

1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the **InDoc tab** > **Overview**.

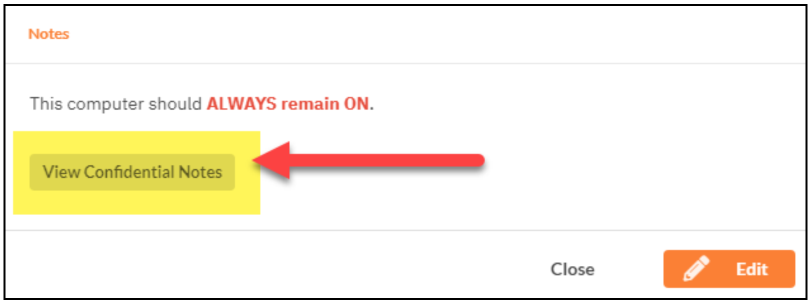


3. Choose an asset category ("Users" or "Computers," for example). The list of detected assets will appear.
4. Click on a specific asset from the list.
5. Next to the **Notes** panel, click **View More**.



No notes yet; click View More -> Edit to add some

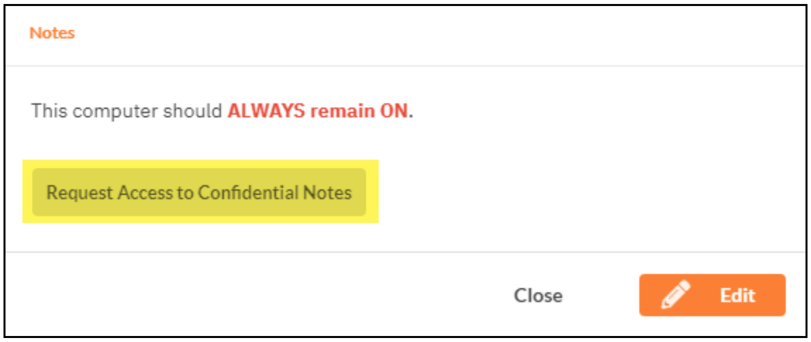
6. Click **View Confidential Notes**.



Notes

This computer should **ALWAYS remain ON.**

If you do not have permission to view confidential notes, you can click **Request Access**. An Admin will then receive an email notification and can choose to log in to the Portal and give you access from **Global Settings** > **Users**. (See "Grant User Access to Confidential Notes" on the next page).



Notes

This computer should **ALWAYS remain ON.**

7. Enter your RapidFire Tools Portal/Network Detective password when prompted.
8. Use the text editor to add or change your confidential notes. Click **Save**.

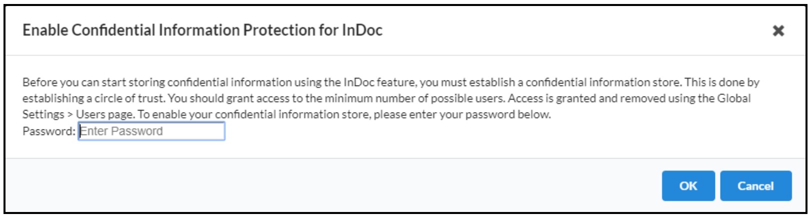
> **Note:** You will need to re-enter your password to view or change confidential notes.

Enable Confidential Information Protection for InDoc

With InDoc, you can securely write and share confidential notes that you place on network assets. This is perfect for managing passwords or other sensitive information about the client's network. Before you use this feature, you will need to set up a secure "circle of trust" for using confidential notes with InDoc.

This task will be performed by a Global Master user when they first log in to the portal after you set up InDoc. Here's how it works:

1. Once you set up InDoc, log in to the Portal as a user with **Master** rights.
2. If you have not done so already, you will be prompted to create a confidential information Store. Enter your portal password and click **OK**.

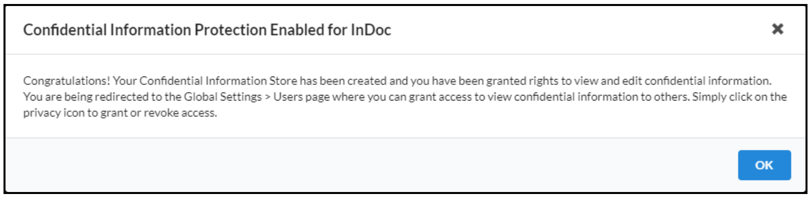


Enable Confidential Information Protection for InDoc

Before you can start storing confidential information using the InDoc feature, you must establish a confidential information store. This is done by establishing a circle of trust. You should grant access to the minimum number of possible users. Access is granted and removed using the Global Settings > Users page. To enable your confidential information store, please enter your password below.

Password: Enter Password

3. You will now have access to create and view confidential notes and associate them with network assets.



Confidential Information Protection Enabled for InDoc

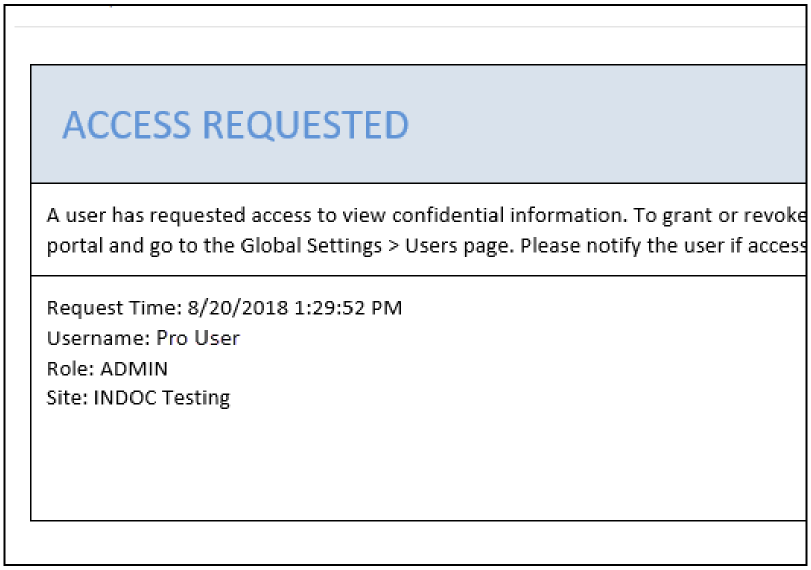
Congratulations! Your Confidential Information Store has been created and you have been granted rights to view and edit confidential information. You are being redirected to the Global Settings > Users page where you can grant access to view confidential information to others. Simply click on the privacy icon to grant or revoke access.

4. You will then be redirected to the **Global Settings** > **Users** page where you can grant access to view confidential information to others.

Grant User Access to Confidential Notes

Note: Before you can add or view confidential notes with InDoc, you first need to "Enable Confidential Information Protection for InDoc" above.

Users with access to InDoc can request access to confidential notes. Master users with privacy permission will receive an email when a user requests access to a confidential note.



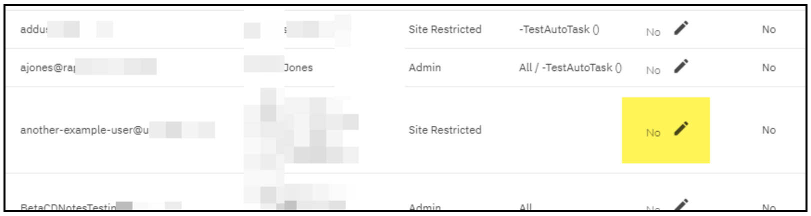
ACCESS REQUESTED

A user has requested access to view confidential information. To grant or revoke
portal and go to the Global Settings > Users page. Please notify the user if access

Request Time: 8/20/2018 1:29:52 PM
Username: Pro User
Role: ADMIN
Site: INDOC Testing

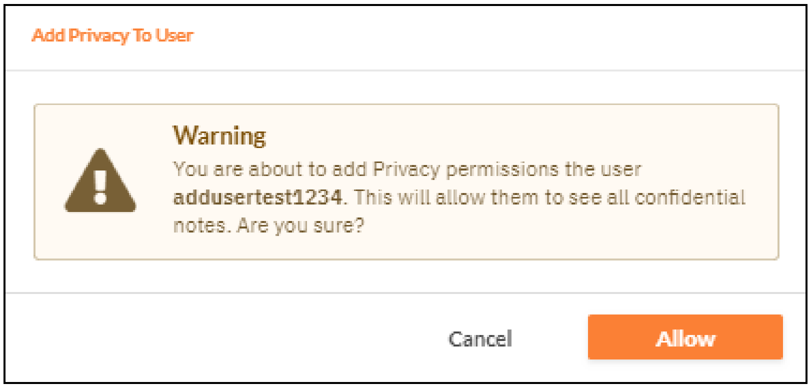
To grant privacy access to the user:

1. Log in to the RapidFire Tools Portal.
2. Navigate to **Global Settings** > **Users**.
3. Under the **Access Confidential** field, click **No** to edit the confidential access for the appropriate user.



addu[redacted]	[redacted]	Site Restricted	-TestAutoTask ()	No ✎	No
ajones@ra[redacted]	[redacted]Jones	Admin	All / -TestAutoTask ()	No ✎	No
another-example-user@u[redacted]	[redacted]	Site Restricted		No ✎	No
BetaCDNotesTestin[redacted]	[redacted]	Admin	All	No ✎	No

4. Confirm that you wish to grant the user Privacy permissions. The user will then be able to view confidential notes.



Add Privacy To User

Warning

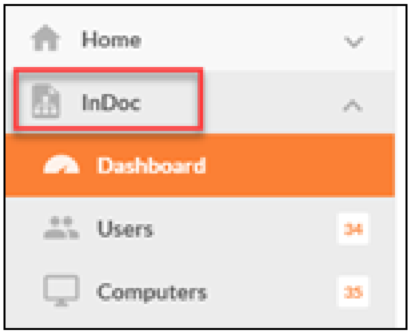
You are about to add Privacy permissions the user **addusertest1234**. This will allow them to see all confidential notes. Are you sure?

Add a Procedure to an Asset (InDoc)

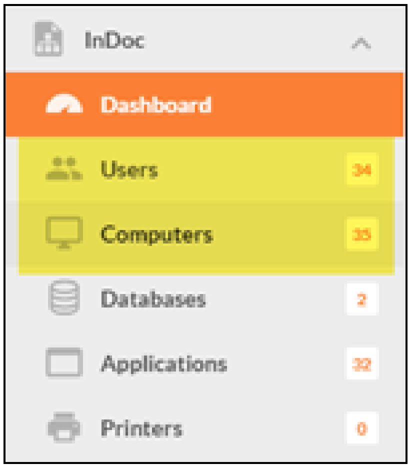
You can use InDoc to document **Procedures** and associate them directly with the relevant network assets.

> Tip: Procedures are handy for managing instructions or settings that apply to specific assets on the network, like a Domain Controller. This puts the information right at your tech team's fingertips.

1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc tab** > **Overview**.

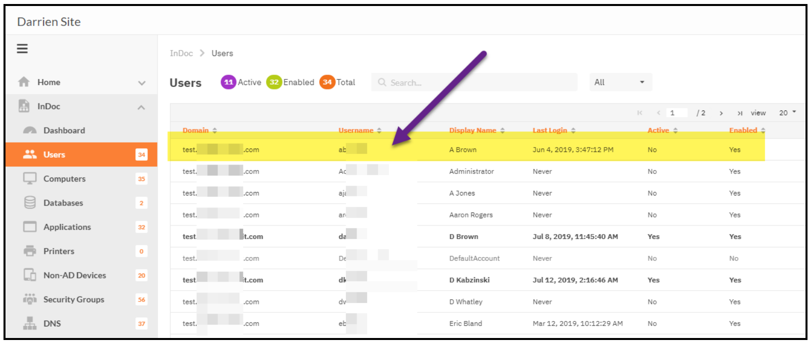


3. Choose an asset category ("Users" or "Computers," for example).



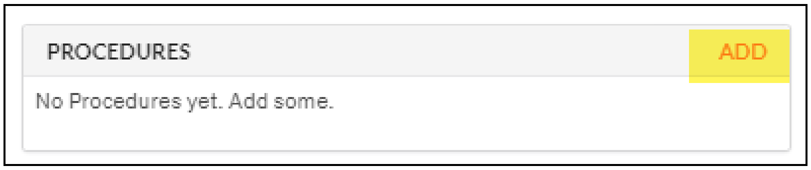
4. The list of detected assets will appear. Click on a specific asset from the list.

© 2021 RapidFire Tools, Inc. All rights reserved.



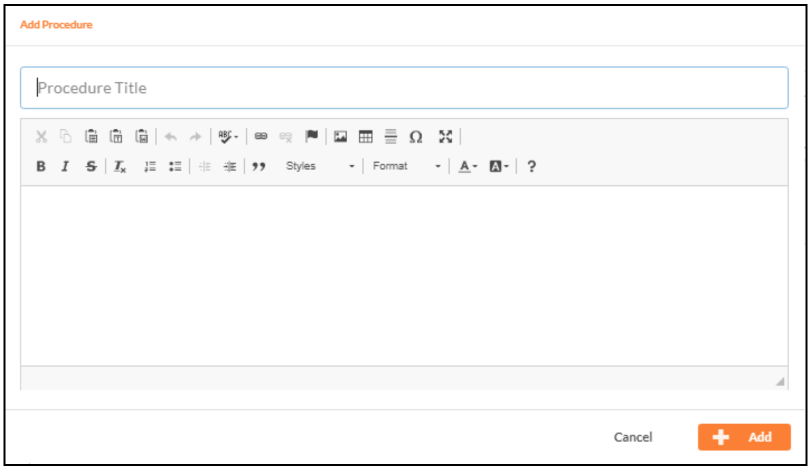
Domain	Username	Display Name	Last Login	Active	Enabled
test.[redacted].com	ab[redacted]	A Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test.[redacted].com	Ac[redacted]	Administrator	Never	No	Yes
test.[redacted].com	aj[redacted]	A Jones	Never	No	Yes
test.[redacted].com	ar[redacted]	Aaron Rogers	Never	No	Yes
test[redacted]t.com	da[redacted]	D Brown	Jul 8, 2019, 11:45:40 AM	Yes	Yes
test.[redacted].com	De[redacted]	DefaultAccount	Never	No	No
test[redacted]t.com	dk[redacted]	D Kabzinski	Jul 12, 2019, 2:16:46 AM	Yes	Yes
test.[redacted].com	dv[redacted]	D Whatley	Never	No	Yes
test.[redacted].com	eb[redacted]	Eric Bland	Mar 12, 2019, 10:12:29 AM	No	Yes

5. Next to the **Procedures** panel, click **Add**.



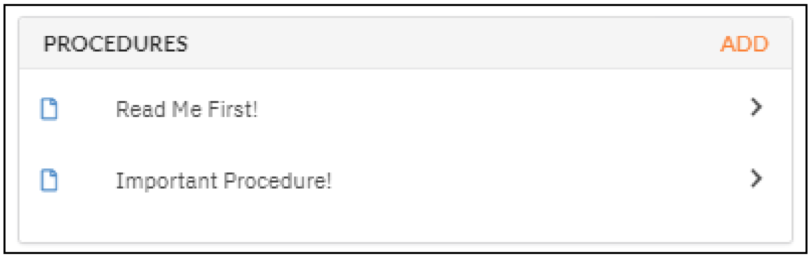
No Procedures yet. Add some.

6. Use the editor to write or edit your Procedure.



7. Click **Save**.

You can then see your list of procedures for the asset in the Procedures panel.



Read Me First!

Important Procedure!

© 2021 RapidFire Tools, Inc. All rights reserved.

Edit or Delete Procedures

Whenever you need to change a procedure:

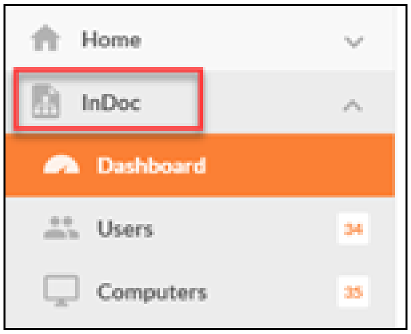
1. Open the **Procedure** from the panel.
2. Click **Edit**. (You can also click **Delete** to remove the procedure).
3. Make any changes you wish using the editor.
4. Click **Save**.

© 2021 RapidFire Tools, Inc. All rights reserved.

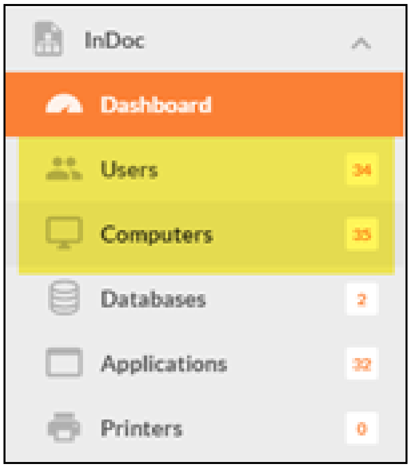
Add Related Items to a Network Asset (InDoc)

Use InDoc's relationship mapping feature to help keep track of important related items on the client's network. This includes relationships like which users regularly log in to which computers. To assign related items to an asset:

1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc** tab > **Overview**.

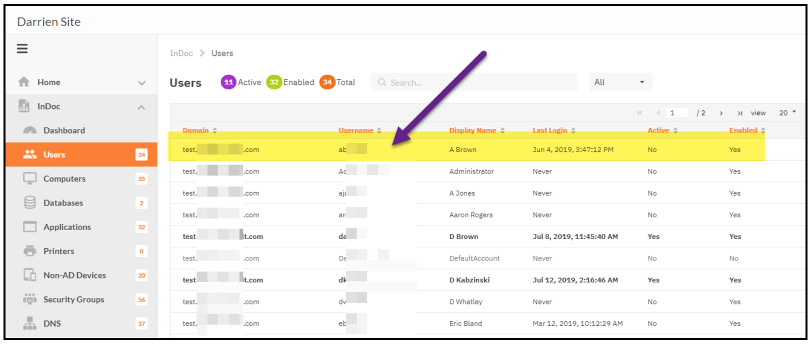


3. Choose an asset category ("Users" or "Computers," for example).



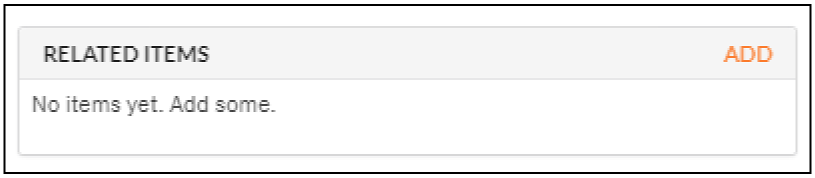
4. The list of detected assets will appear. Click on a specific asset from the list.

© 2021 RapidFire Tools, Inc. All rights reserved.



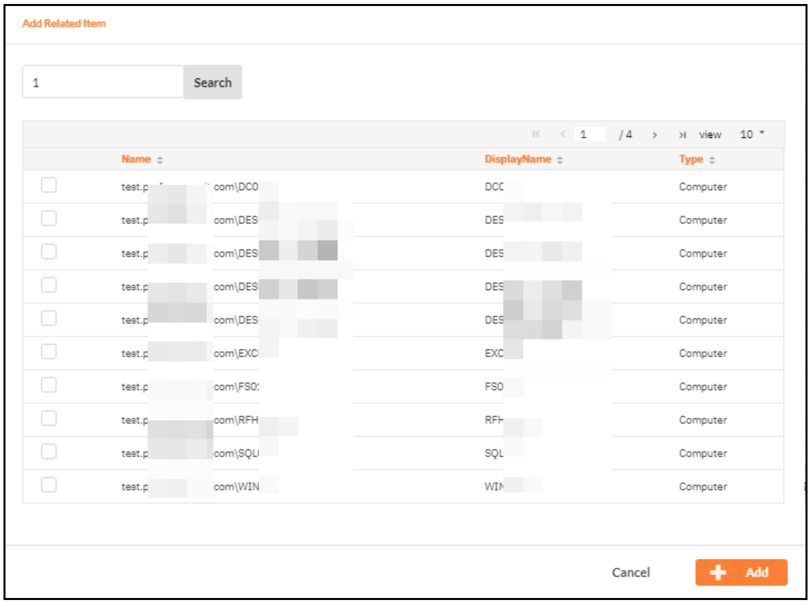
Domain	Username	Display Name	Last Login	Active	Enabled
test.[redacted].com	ab[redacted]	A Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test.[redacted].com	Ad[redacted]	Administrator	Never	No	Yes
test.[redacted].com	aj[redacted]	A Jones	Never	No	Yes
test.[redacted].com	ar[redacted]	Aaron Rogers	Never	No	Yes
test[redacted]t.com	**da[redacted]**	**D Brown**	**Jul 8, 2019, 11:45:40 AM**	**Yes**	**Yes**
test.[redacted].com	De[redacted]	DefaultAccount	Never	No	No
test[redacted]t.com	**dk[redacted]**	**D Kabzinski**	**Jul 12, 2019, 2:16:46 AM**	**Yes**	**Yes**
test.[redacted].com	dw[redacted]	D Whatley	Never	No	Yes
test.[redacted].com	eb[redacted]	Eric Bland	Mar 12, 2019, 10:12:29 AM	No	Yes

5. From the **Related Items** tab, click **Add**.


RELATED ITEMS

No items yet. Add some.

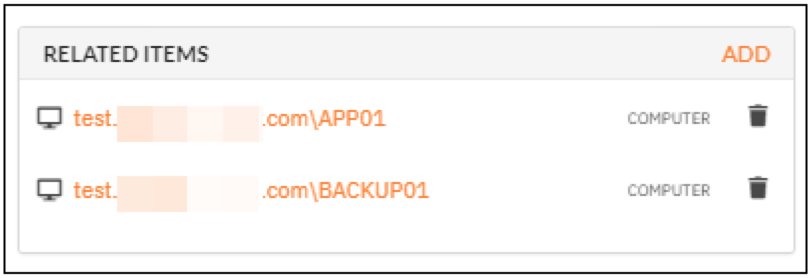
6. Scroll down the list of items, or search for it using the search bar.


Add Related Item

1

	Name	DisplayName	Type
□	test.p[redacted]com\DC0[redacted]	DC[redacted]	Computer
□	test.p[redacted]com\DES[redacted]	DES[redacted]	Computer
□	test.p[redacted]com\DES[redacted]	DES[redacted]	Computer
□	test.p[redacted]com\DES[redacted]	DES[redacted]	Computer
□	test.p[redacted]com\DES[redacted]	DES[redacted]	Computer
□	test.p[redacted]com\EXC[redacted]	EXC[redacted]	Computer
□	test.p[redacted]com\FS0[redacted]	FS0[redacted]	Computer
□	test.p[redacted]com\RFH[redacted]	RFH[redacted]	Computer
□	test.p[redacted]com\SQL[redacted]	SQL[redacted]	Computer
□	test.p[redacted]com\WIN[redacted]	WIN[redacted]	Computer

7. Click the **Check Box** for each item you want to associate with the asset.
8. Click **Add**. The related items will appear in the panel. Other users can then click on the Related Items to view more about them.



test.[redacted].com\APP01 COMPUTER

test.[redacted].com\BACKUP01 COMPUTER

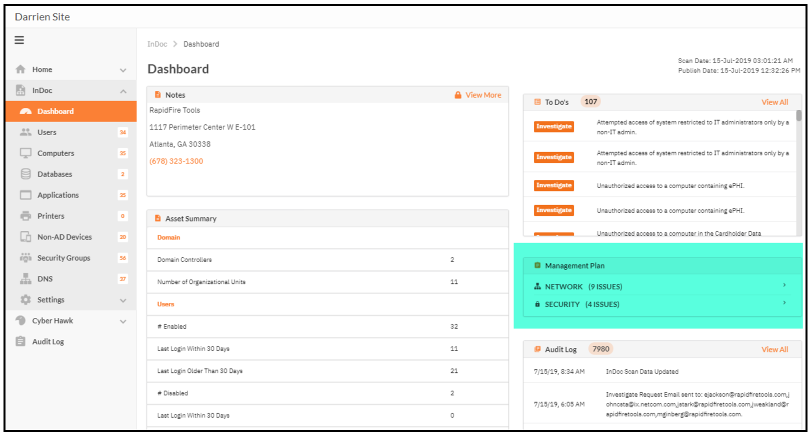
Note: To remove a related item from an asset, click on the 🗑 icon. The related item will be removed.

© 2021 RapidFire Tools, Inc. All rights reserved.

View Site Management Plan (InDoc)

On a Site's **InDoc tab**, you and your team can access a quick overview of the site **Management Plan**. This provides a concise overview of the Management Plan document that you can generate with Reporter. To use this feature:

1. Open the **InDoc** tab > **Overview** for the Site.



Scan Date: 15-Jul-2019 03:01:21 AM
Publish Date: 15-Jul-2019 12:32:26 PM

Notes

RapidFire Tools
1117 Perimeter Center W E-101
Atlanta, GA 30338
(678) 323-1300

Asset Summary

Domain	
Domain Controllers	2
Number of Organizational Units	11
Users	
# Enabled	32
Last Login Within 30 Days	11
Last Login Older Than 30 Days	21
# Disabled	2
Last Login Within 30 Days	0

To Do's 107

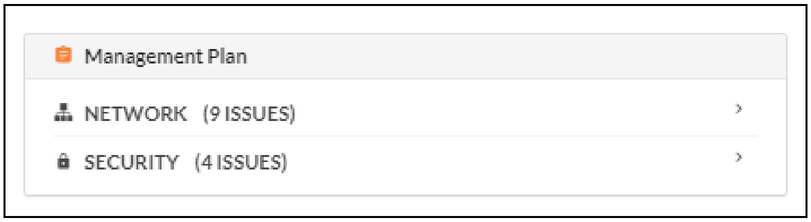
Investigate	Attempted access of system restricted to IT administrators only by a non-IT admin.
Investigate	Attempted access of system restricted to IT administrators only by a non-IT admin.
Investigate	Unauthorized access to a computer containing ePHI.
Investigate	Unauthorized access to a computer containing ePHI.
	Unauthorized access to a computer in the Cardholder Data

Management Plan
NETWORK (9 ISSUES)
SECURITY (4 ISSUES)

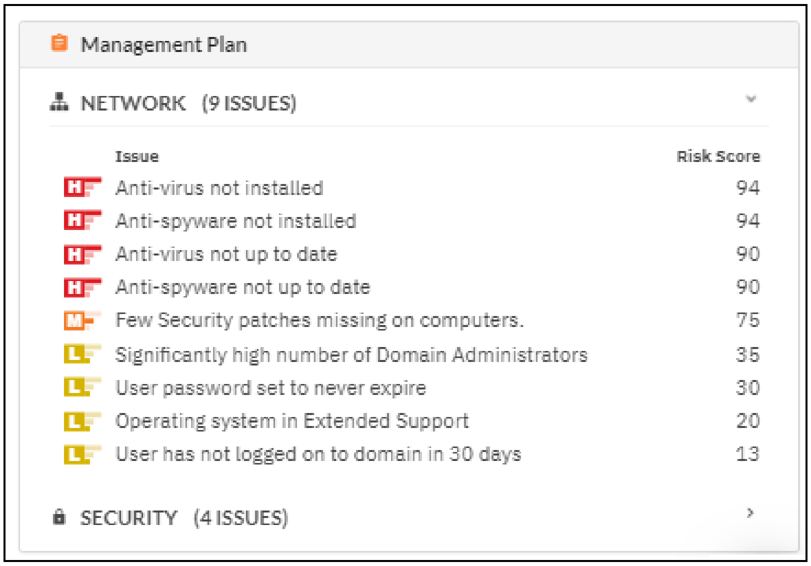
Audit Log 7980

7/15/19, 8:34 AM	InDoc Scan Data Updated
7/15/19, 6:05 AM	Investigate Request Email sent to: ejackson@rapidfiretools.com,johncsta@ix.netcom.com,jstark@rapidfiretools.com,jweakland@rapidfiretools.com,mginberg@rapidfiretools.com.

2. Under the **Management Plan** panel, you can see the Network Detective modules to which you are subscribed.



3. Click on a module to open up a short list of the issues identified on the Site network.



Management Plan

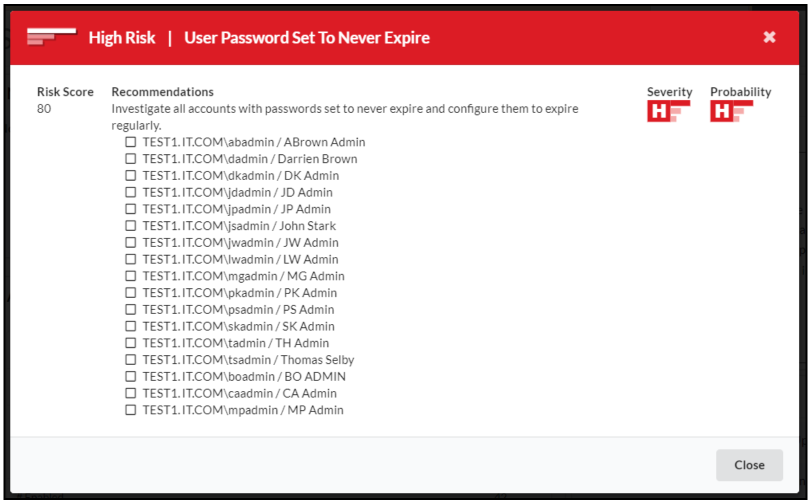
NETWORK (9 ISSUES)

	Issue	Risk Score
H	Anti-virus not installed	94
H	Anti-spyware not installed	94
H	Anti-virus not up to date	90
H	Anti-spyware not up to date	90
M	Few Security patches missing on computers.	75
L	Significantly high number of Domain Administrators	35
L	User password set to never expire	30
L	Operating system in Extended Support	20
L	User has not logged on to domain in 30 days	13

SECURITY (4 ISSUES)

Next to each issue you can see the **Risk Score** (100-1). High Risk issues should be addressed first.

4. Click on a specific issue to open up a brief description and remediation instructions.



High Risk | User Password Set To Never Expire

Risk Score
80

Recommendations
Investigate all accounts with passwords set to never expire and configure them to expire regularly.

- ☐ TEST1.IT.COM\abadmin / ABrown Admin
- ☐ TEST1.IT.COM\dadmin / Darrien Brown
- ☐ TEST1.IT.COM\dkadmin / DK Admin
- ☐ TEST1.IT.COM\jdadmin / JD Admin
- ☐ TEST1.IT.COM\jpadmin / JP Admin
- ☐ TEST1.IT.COM\jsadmin / John Stark
- ☐ TEST1.IT.COM\jwadmin / JW Admin
- ☐ TEST1.IT.COM\lwadmin / LW Admin
- ☐ TEST1.IT.COM\mgadmin / MG Admin
- ☐ TEST1.IT.COM\pkadmin / PK Admin
- ☐ TEST1.IT.COM\psadmin / PS Admin
- ☐ TEST1.IT.COM\skadmin / SK Admin
- ☐ TEST1.IT.COM\tadmin / TH Admin
- ☐ TEST1.IT.COM\tsadmin / Thomas Selby
- ☐ TEST1.IT.COM\boadmin / BO ADMIN
- ☐ TEST1.IT.COM\caadmin / CA Admin
- ☐ TEST1.IT.COM\mpadmin / MP Admin

Severity: H

Probability: H

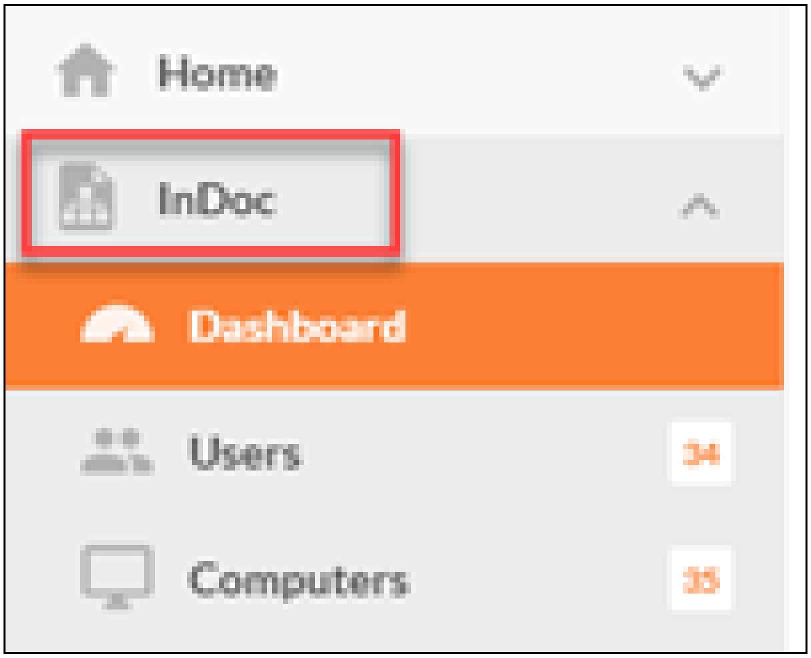
Tip: For more detailed information on the issues identified, **review the latest Management Plan report** for that specific module. You can **download Reporter documents in the Network Detective application**.

Edit Smart Tags in InDoc

Cyber Hawk, our security alerting system, incorporates a proprietary feature called **Smart Tags**. Smart Tags allow you to adapt Cyber Hawk to each client's unique IT environment to detect network Anomalies, Changes, and Threats (ACT). Smart Tags allow you to add information about specific users, assets, and settings that helps Cyber Hawk get "smarter" about what it is finding. That means more potential threats identified with fewer false positives.

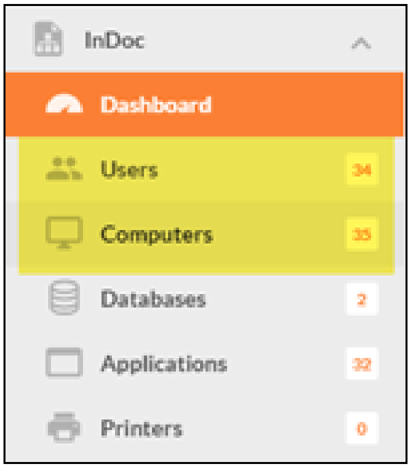
InDoc allows you to manage and assign Smart Tags to network assets. (Note that you can also do this from within the Cyber Hawk dashboard in the Network Detective application.) To manage Smart Tags in InDoc:

1. Open the InDoc Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc** tab > **Overview**.

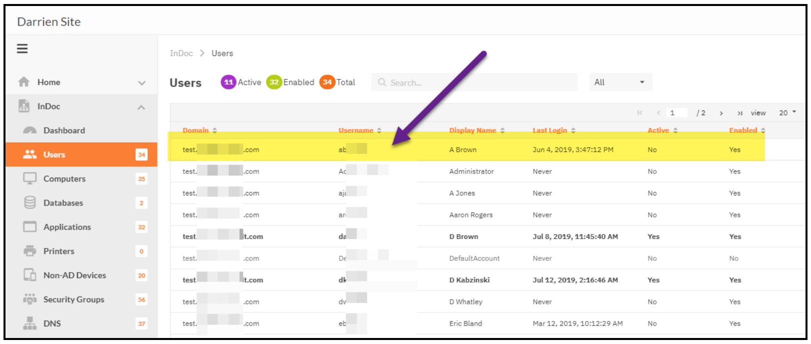


3. Choose an asset category ("Users" or "Computers," for example).

© 2021 RapidFire Tools, Inc. All rights reserved.

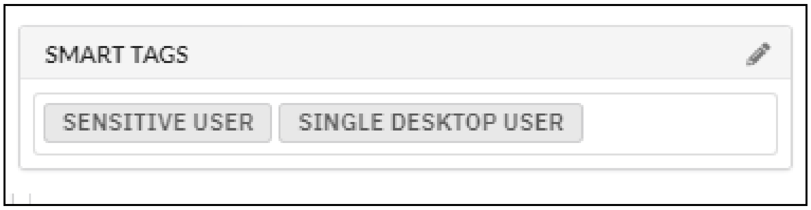


4. The list of detected assets will appear. Click on a specific asset from the list.

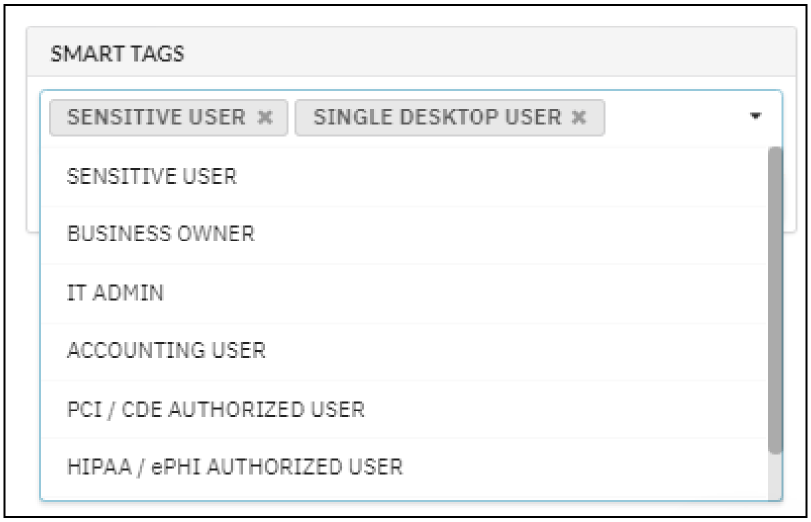


Domain	Username	Display Name	Last Login	Active	Enabled
test.[redacted].com	ab[redacted]	A Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test.[redacted].com	Ad[redacted]	Administrator	Never	No	Yes
test.[redacted].com	aj[redacted]	A Jones	Never	No	Yes
test.[redacted].com	ar[redacted]	Aaron Rogers	Never	No	Yes
test[redacted]t.com	**da[redacted]**	**D Brown**	**Jul 8, 2019, 11:45:40 AM**	**Yes**	**Yes**
test.[redacted].com	De[redacted]	DefaultAccount	Never	No	No
test[redacted]t.com	**dk[redacted]**	**D Kabzinski**	**Jul 12, 2019, 2:16:46 AM**	**Yes**	**Yes**
test.[redacted].com	dv[redacted]	D Whatley	Never	No	Yes
test.[redacted].com	eb[redacted]	Eric Bland	Mar 12, 2019, 10:12:29 AM	No	Yes

5. From the **Smart Tags** panel, click **the pen icon** .

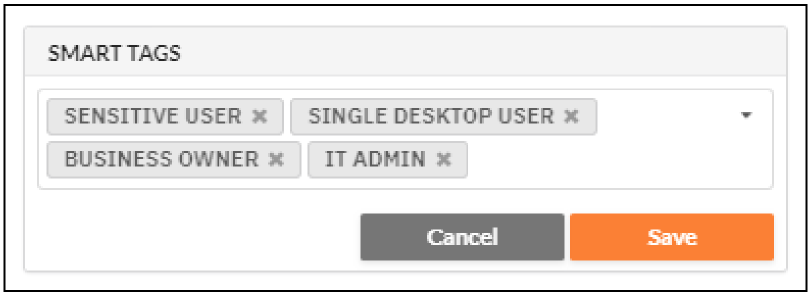


6. Choose your Smart Tags from the available list.



SMART TAGS

7. Click **Save**. Your **Smart Tags** for the asset will appear under the Smart Tags panel.



SMART TAGS

To remove a Smart Tag from the asset, click the **X** on the tag.

Note: Changes to **Smart Tags** will be reflected in the Network Detective application. See the Cyber Hawk User Guide for more information.

© 2021 RapidFire Tools, Inc. All rights reserved.

InDoc User Permissions

You will need to configure your MSP team users correctly in order for them to access InDoc. Only users with the correct **Global** and **Site**-specific **Roles** can see InDoc data in the RapidFires Tools Portal. See "How to Set Up User Permissions for InDoc" below for step-by-step instructions.

The following matrix shows which types of users can see InDoc information.

Global Roles

- Master/All
- Admin
- Restricted (the Global Role of Restricted – typically an MSP technician)

Site Roles

- Site Admin
- Technician

Important: A user must have both a Global Role *AND* a Site Role to access InDoc.

All other users cannot see the InDoc tab. However, they can see there is a Badge for InDoc on the main site tile.

- You can set *Global Roles* from **Global Settings** > **Users**.
- You can set *Site Roles* from **[Your InDoc Site]** > **Home** > **Roles**. You will first need to add the users to your Site from **[Your InDoc Site]** > **Home** > **Users**.

How to Set Up User Permissions for InDoc

You must assign users the correct Global and Site-specific project Roles in order for them to have access to InDoc. You can do this quickly and easily:

1. Log in to the RapidFire Tools Portal.
2. Go to **Global Settings** > **Users**. All of the users associated with your Network Detective account will appear in the list.
3. If you wish to create new users, click **Add New**. Otherwise, make sure your previous (or new) users who wish to use InDoc have the correct **Global Access Level** (Master/All, Admin, or Restricted).
4. Navigate back to the home page and click on your InDoc Site.

5. Go to **[Your InDoc Site]** > **Home** > **Users**. Click **Add User** and select your **Existing User(s)**. Click **Add**.

   Important: Do not create a new user from Site Settings. This user will not have the correct Global Access Level.

6. Go to **[Your InDoc Site]** > **Home** > **Roles**. Assign your users to the correct **Site Role(s)** (Site Admin or Technician).
7. If necessary, be sure to give these users their username and password. They can then log in to the Portal and begin working with InDoc!

Privacy Permissions for Confidential Notes (InDoc)

InDoc allows your team to create and view confidential notes assigned to assets at a Site. In order to create or view these notes, you must have privacy permissions.

You can manage privacy permissions for InDoc confidential notes from **Global Settings** > **Users**. The process works like this:

1. The first **Master/Admin** user who logs into InDoc will gain the ability to assign Privacy access to other users. See "Enable Confidential Information Protection for InDoc" on page 125.
2. This user can navigate to **Global Settings** > **Users** to grant other users Privacy access. This includes the ability to create and view confidential notes, as well as to assign Privacy access to other users. See "Grant User Access to Confidential Notes" on page 125.

How Can my Team Use InDoc? Two Examples

InDoc allows MSP support technicians and help desk personnel to easily access documentation and current asset information regarding a customer site to assist in addressing customer issues. Here are two examples:

EXAMPLE:

#1: Help Desk

1. A support call comes in. A customer says they are having problems with their computer and printing.
2. You ask for the customer’s user name and company.
3. Using **InDoc**, you drill into the customer’s site and find the user.
4. You bring up the user’s details, look at **Related Items**, and see both “DESKTOP5” (a PC) and “My HP Printer” (a printer) are associated with the user.
5. You ask, “Are you having issues with the printer called 'My HP Printer' which I see is an HP OfficeJet 8710?"
6. When you bring up the printer, you see a **Procedure** called "HP Printer Reattachment" with step-by-step instructions on how to remove and re-attach the printer. Apparently, they've had this problem before.
7. After reading the **Procedure**, you know the computer to remotely connect to, and the printer and model for which to download drivers, all of which facilitates the quick resolution of the problem.

#2: Tech at a Customer Site

1. You arrive on-site and are told there is a permission problem. You need to get on the domain controller.
2. You’ve never been at this site, but you quickly access **InDoc** from the **RapidFire Tools Portal**.
3. You open the **Site** and use **InDoc** to see if there are any **Notes** or **Procedures** you should be aware of on the DC's before working with them.
4. There are 3 domain controllers, but one has a **Note** that says "Legacy DC – No longer in use" allowing you to avoid spending time working on a computer that is no longer in use.

RapidFire Tools Portal Client View for Reporter

With **Reporter**, **InDoc**, and the **RapidFire Tools Portal**, you can make IT and Compliance assessment reports available for clients to view and download.

Note: Before you can use the Client View, you need to enable InDoc for your Reporter Site in the RapidFire Tools Portal. See "Requirements for using InDoc with Reporter" on page 112

Here's a quick overview:

- First **set up your Report Tasks** to publish to the Client Portal.
- Then **assign clients the Client Role** for a Site, and configure their access to the Client Portal and reports.
- Clients can then log into a restricted version of the portal (the "Client Portal") to access and download reports.

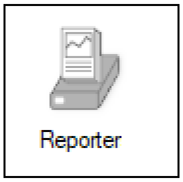
Tip: The *Client Portal* is the same as the RapidFire Tools Portal – just limited to only what clients need to see.

Here's how you set things up for clients to access reports:

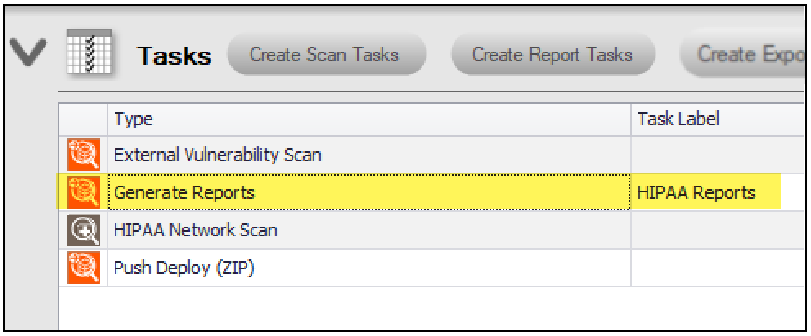
Step 1 — Configure Reporter to Publish to the Client Portal

First you need to configure one or more of your existing report jobs to publish to the Client Portal. To do this:

1. In the **Network Detective** app, open your Reporter Site.
2. Click on **Reporter** button (lower left-hand side of the screen) to open the Reporter dashboard for the Site.



3. Under Tasks, **double click on the report task** you wish to publish to the Client Portal.



Type	Task Label
External Vulnerability Scan	
Generate Reports	HIPAA Reports
HIPAA Network Scan	
Push Deploy (ZIP)	

4. Click **Next** to go to the Delivery Method screen.

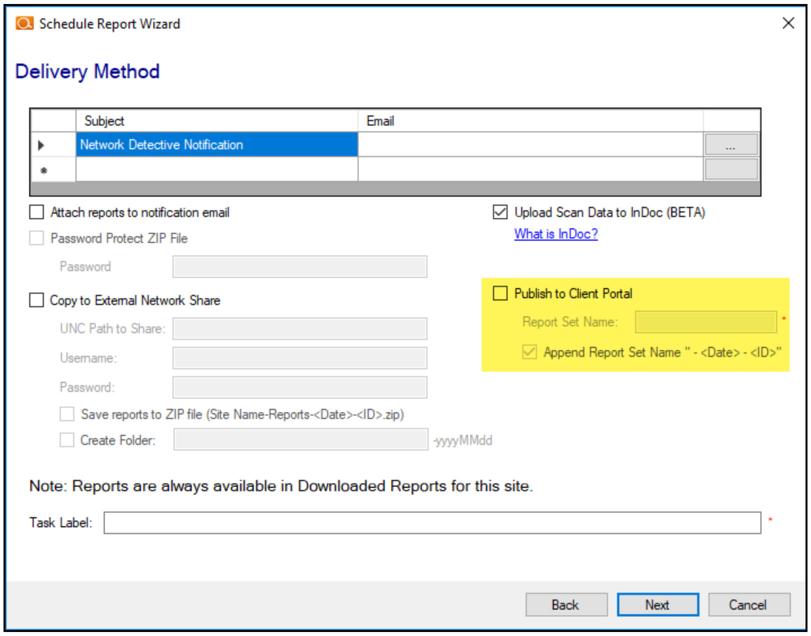
> **Note:** Before you can use the Client View, you need to enable InDoc for your Reporter Site in the RapidFire Tools Portal. See "Requirements for using InDoc with Reporter" on page 112

5. Check the **Publish to Client Portal** box.

   - Enter a **Report Set Name** that will appear in the Portal for the client to access.
   - You can also choose to **Append the Report Set Name** with the **Date** and an **ID**.

   > **Note:** This is useful to help distinguish between multiple report sets with

the same name.



Schedule Report Wizard

Delivery Method

	Subject	Email
▶	Network Detective Notification	
*		

□ Attach reports to notification email

□ Password Protect ZIP File

Password:

□ Copy to External Network Share

UNC Path to Share:

Username:

Password:

□ Save reports to ZIP file (Site Name-Reports-<Date>-<ID>.zip)

□ Create Folder: -yyyyMMdd

☑ Upload Scan Data to InDoc (BETA)

What is InDoc?

□ Publish to Client Portal

Report Set Name: *

☑ Append Report Set Name " - <Date> - <ID>"

Note: Reports are always available in Downloaded Reports for this site.

Task Label: *

6. Click **Next**.
7. **Schedule** the task if you have not already done so.
8. Click **Finish**.

Configure Reporter Template to Publish to Client Portal

If you modify a report task associated with an existing Reporter Template, you can save time by changing all of your report tasks for multiple sites at once. To do this:

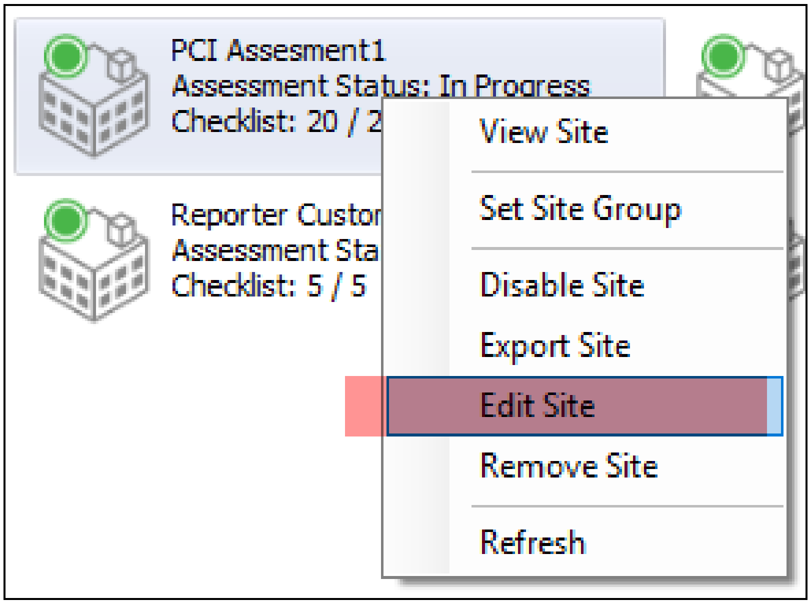
1. Click on **Reporter** from the **Network Detective top ribbon**.
2. Click **Edit** on the **Reporter Template** you wish to modify.
3. **Double click on the Report Task** you wish to modify.
4. Click **Next** to go to the **Delivery Method** screen, and check **Publish to Client Portal**.
5. Complete the remaining prompts and save your edited task.

Note: All of your Reporter Sites that have this task will publish their reports to the Client Portal. However, you still need to complete the remaining steps below.

Step 2 — Ensure that the Site is Visible in the Client Portal

Next you need to configure the Site to make it visible in the Client Portal:

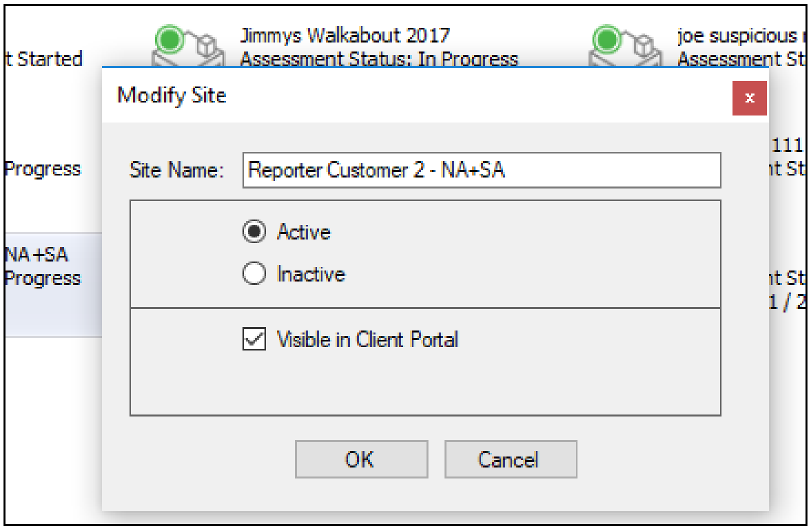
1. From within the **Network Detective** app, navigate to the **Home** screen.
2. Right click on the Site you want to appear in the Portal and click **Edit Site**.



PCI Assesment1
Assessment Status: In Progress
Checklist: 20 / 2

Reporter Custor
Assessment Sta
Checklist: 5 / 5

3. Check the **Visible in Client Portal** box.



Modify Site

Site Name: Reporter Customer 2 - NA+SA

● Active
○ Inactive

☑ Visible in Client Portal

4. Repeat this for each Site that you wish to make visible to clients.

Step 3 — Add Client User to Site and Assign Client Role

1. Log in to the **RapidFire Tools Portal** (https://www.youritportal.com).
2. Navigate to the Site, then to **Home** > **Users**.
3. Click **Add User**. Then choose **New User**. Add the client user to the Site. You will need their email address and name. Create a password for the user.

   Important: You will need to send these credentials, including the password, to the client user.

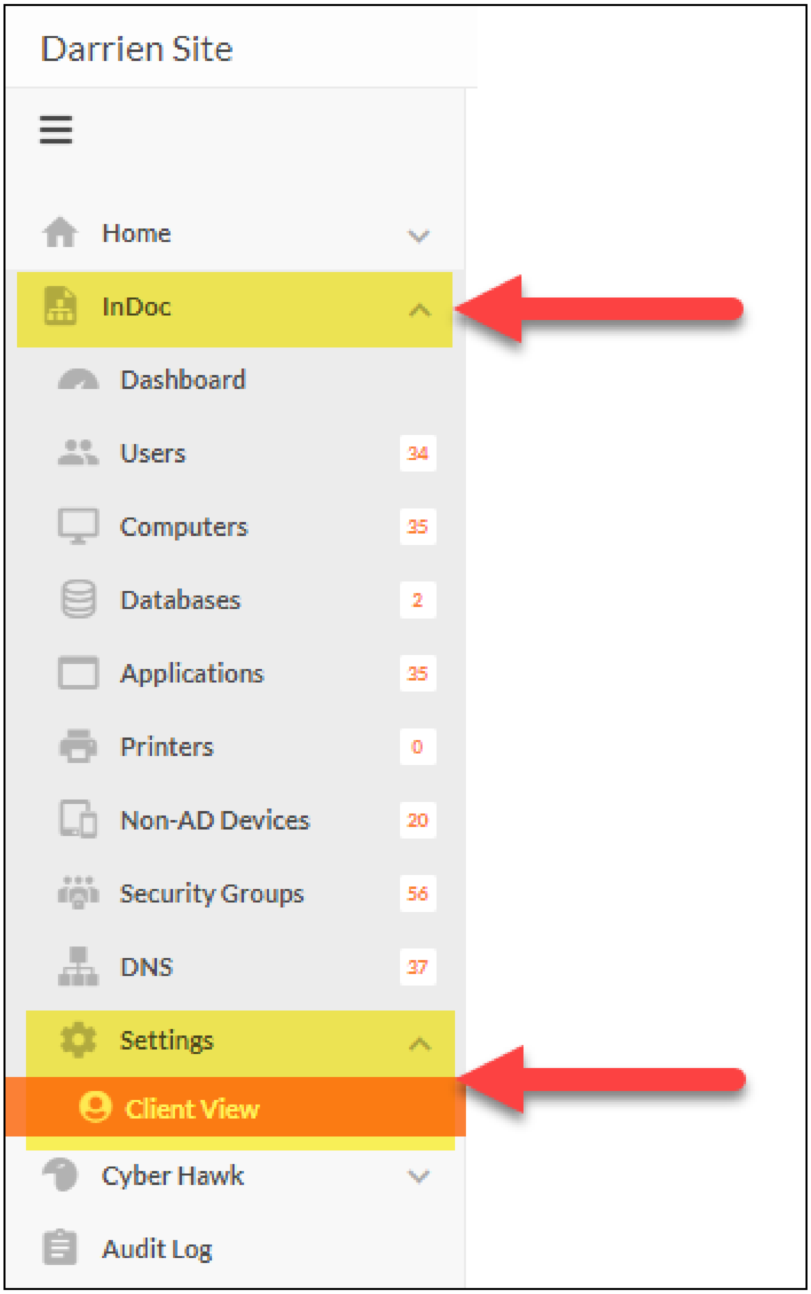
4. Now you need to add the new user to the Client Role. Go to **Home** > **Roles**.
5. Click **Add User** next to the **Client View** Role. Select the User. Then click **Add**.

   The user will be added to the client role and will be able to access a restricted version of the Site. Create additional users and assign them to the client role if needed.

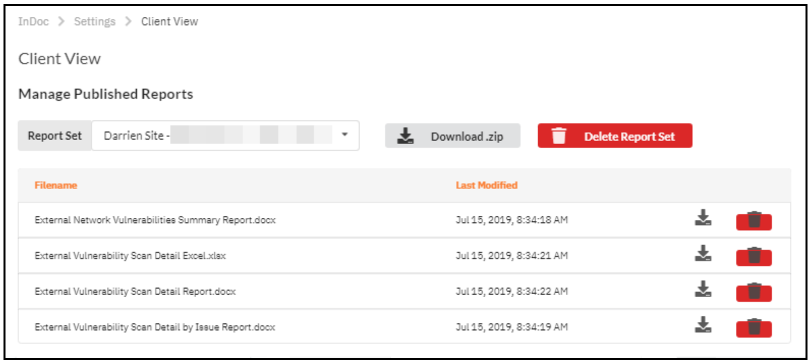
Step 4 — Configure Client View in RapidFire Tools Portal

Configure the **Client View**. This consists of deleting any reports you wish to remove from a report set.

1. From the Portal, access the Site and go to **InDoc** > **Settings** > **Client View**.



2. Review the list of reports published to the site. Choose from various published **Report Sets** using the drop down menu.



InDoc > Settings > Client View

Client View

Manage Published Reports

Filename	Last Modified		
External Network Vulnerabilities Summary Report.docx	Jul 15, 2019, 8:34:18 AM	⭳	🗑
External Vulnerability Scan Detail Excel.xlsx	Jul 15, 2019, 8:34:21 AM	⭳	🗑
External Vulnerability Scan Detail Report.docx	Jul 15, 2019, 8:34:22 AM	⭳	🗑
External Vulnerability Scan Detail by Issue Report.docx	Jul 15, 2019, 8:34:19 AM	⭳	🗑

- If you want to delete a report, click the 🗑 icon next to the report you want to delete.
- If you want to delete an entire Report Set, click **Delete Report Set**.

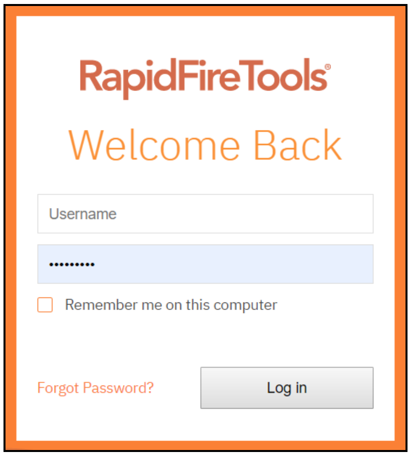
> **Important:**
> • Deleting reports or report sets will remove them from the Client View, but not from Network Detective.
> • You cannot restore reports to the Client View once you have deleted them. You will have to republish them from Network Detective.

Access the Portal as a Client User

> **Important:** Before clients can access the portal, an admin will need to set up access on their behalf. See "RapidFire Tools Portal Client View for Reporter" on page 141 for detailed instructions.

Clients can view assessment reports that have been published to the Portal. To do this:

1. Navigate to the portal using the URL provided by the MSP.
2. Enter the login credentials provided by the MSP.



RapidFireTools

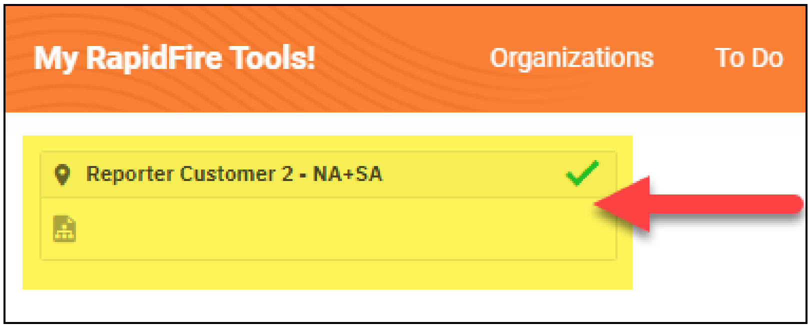
Welcome Back

Username

•••••••••

□ Remember me on this computer

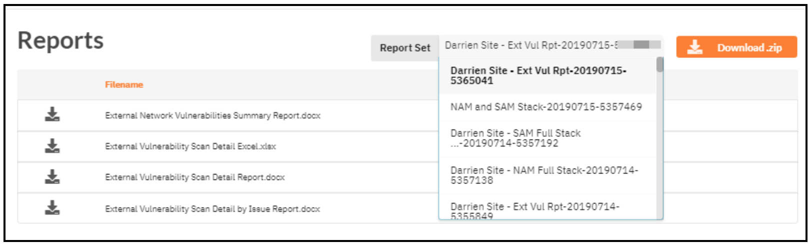
3. The MSP will have granted you access to one or more sites to view reports. Click on the **Site** for which you wish to view/download reports.



Reporter Customer 2 - NA+SA ✓

4. If necessary, click on the **Reports** tab.
5. **Select the report set** from the drop-down menu. Also **select a target language** if the reports have been published in multiple languages.

   Click the download button next to a report to **download reports individually**, or click the Download .zip button to to **download reports together as a .zip file**. The reports will be in MS Word format.



Reports

Report Set: Darrien Site - Ext Vul Rpt-20190715-5

- **Darrien Site - Ext Vul Rpt-20190715-5365041**
- NAM and SAM Stack-20190715-5357469
- Darrien Site - SAM Full Stack ...-20190714-5357192
- Darrien Site - NAM Full Stack-20190714-5357138
- Darrien Site - Ext Vul Rpt-20190714-5355849

	Filename
⤓	External Network Vulnerabilities Summary Report.docx
⤓	External Vulnerability Scan Detail Excel.xlax
⤓	External Vulnerability Scan Detail Report.docx
⤓	External Vulnerability Scan Detail by Issue Report.docx

Appendices

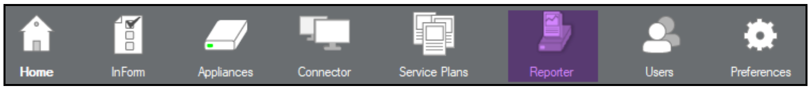
This section contains other helpful topics related to Reporter:

Reporter Templates

Instead of configuring report tasks for each Site one by one, you can use **Reporter Templates** to set up automated report tasks for all of your sites simultaneously. **Reporter Templates** allow you to create and deploy report tasks quickly and easily. With Reporter Templates you can:

- Select reports to generate from each of your Network Detective module subscriptions and choose from a variety of report scheduling options
- Specify where to publish your reports, including emailing recipients and/or copying reports to a network share
- Choose to upload scan data to **InDoc** in the **RapidFire Tools Portal**
- Once your template is configured, deploy it to multiple Reporter Sites at once

You can Manage Reporter Templates from the **Reporter button** located on the **Network Detective** top ribbon.



Tip: Reporter Templates also include several "preset" templates that you can use to get started right away!

© 2021 RapidFire Tools, Inc. All rights reserved.

Create and Deploy Reporter Templates

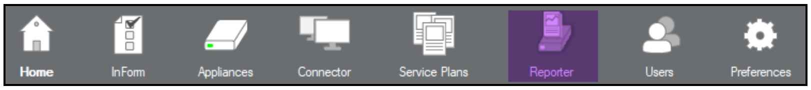
Reporter Templates allow you to create re-usable sets of report tasks for multiple Reporter Sites at the same time.

Note: Before you can use Reporter Templates, you need to have Reporter set up and associated with each Site you wish to use. See "Setting Up Reporter" on page 16.

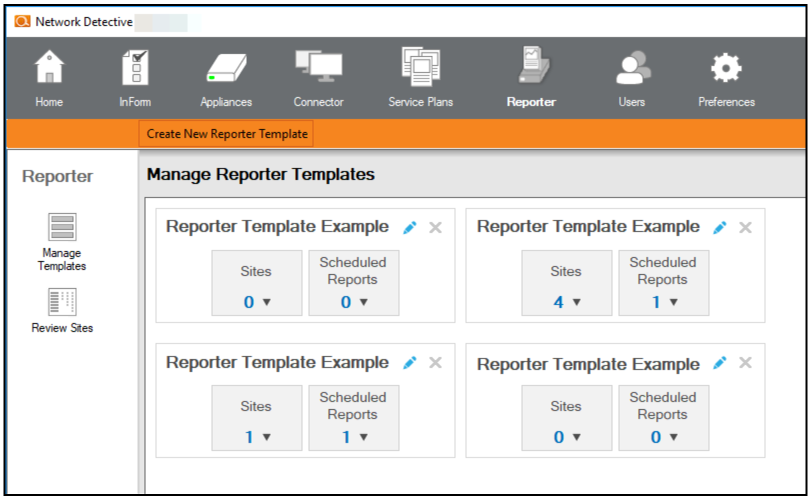
To create and deploy a Reporter Template, follow these steps:

Step 1 — Create New Reporter Template

1. Click on the **Reporter button** located on the Network Detective top ribbon.



The **Manage Reporter Templates** screen will appear.

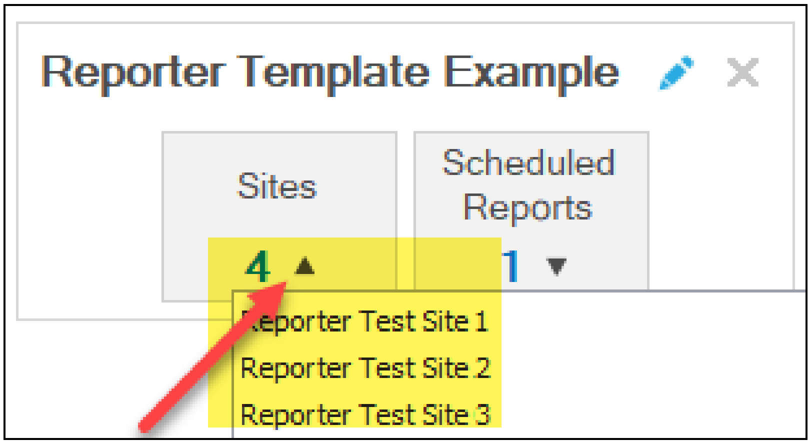


Here you can see all of the templates you created previously. For each template, you can also see:

- **Number of Sites** template has been applied to
- **Number of Scheduled Reports** included in the template

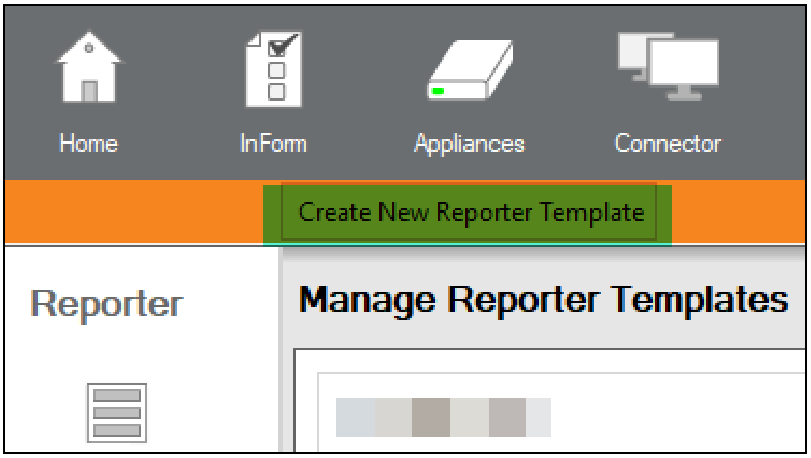
© 2021 RapidFire Tools, Inc. All rights reserved.

- Click on the arrow button ▼ to quickly see this information in a drop-down



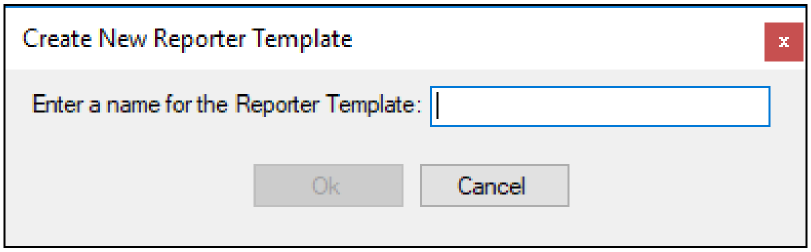
Note: Here you can also see the "preset" Reporter Templates available for you to configure. If you want to get started with one of the preset templates, click the Edit icon on the template, and go to "Step 2 — Assign Reports to Template" on the next page.

2. Click **Create New Reporter Template**.



3. **Enter a name** for the Reporter Template.

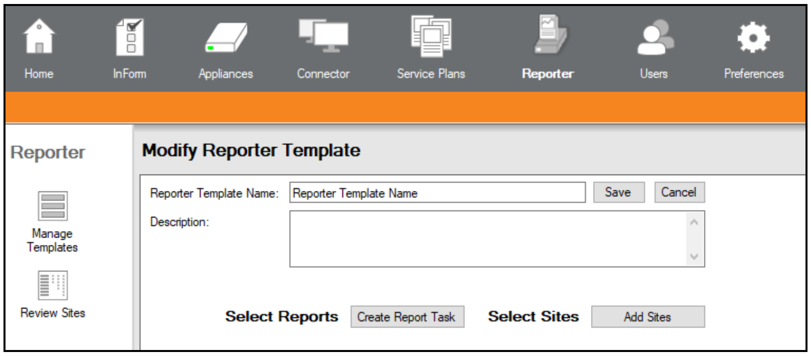
© 2021 RapidFire Tools, Inc. All rights reserved.



Create New Reporter Template

Enter a name for the Reporter Template:

The **Modify Reporter Template** screen will appear.



Modify Reporter Template

Reporter Template Name: Reporter Template Name

Description:

4. Enter a **Description** for the Reporter Template.

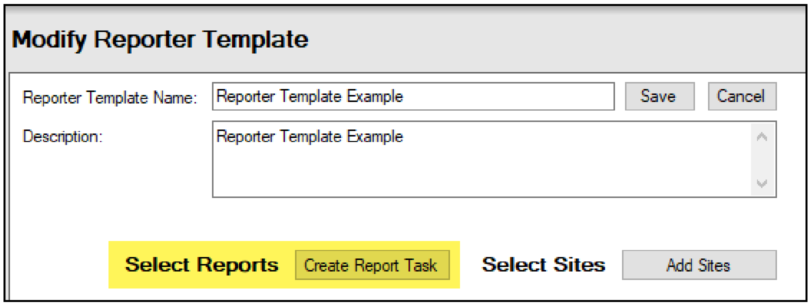
> **Note:** Your description should include notes that explain the template to other Network Detective users. For example:
> • *What report tasks does the template contain?*
> • *To which Sites is it applied?*
> • *What is the schedule?*

Step 2 — Assign Reports to Template

Next assign the reports that will be part of the Reporter Template.

© 2021 RapidFire Tools, Inc. All rights reserved.

1. Next to **Select Reports**, click **Create Report Task**.

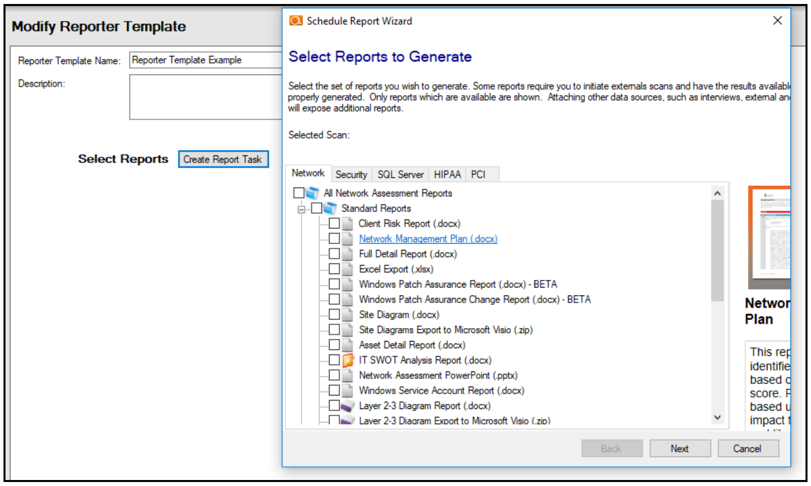


Modify Reporter Template

Reporter Template Name: Reporter Template Example

Description: Reporter Template Example

2. From the **Select Reports to Generate** screen, check the reports for each module that you wish to include as part of the report task.



Modify Reporter Template

Reporter Template Name: Reporter Template Example

Description:

Schedule Report Wizard

Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results availabl
properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external an
will expose additional reports.

Selected Scan:

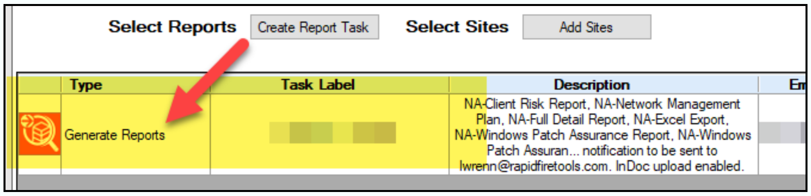
Network | Security | SQL Server | HIPAA | PCI

- □ All Network Assessment Reports
  - □ Standard Reports
    - □ Client Risk Report (.docx)
    - □ Network Management Plan (.docx)
    - □ Full Detail Report (.docx)
    - □ Excel Export (.xlsx)
    - □ Windows Patch Assurance Report (.docx) - BETA
    - □ Windows Patch Assurance Change Report (.docx) - BETA
    - □ Site Diagram (.docx)
    - □ Site Diagrams Export to Microsoft Visio (.zip)
    - □ Asset Detail Report (.docx)
    - □ IT SWOT Analysis Report (.docx)
    - □ Network Assessment PowerPoint (.pptx)
    - □ Windows Service Account Report (.docx)
    - □ Layer 2-3 Diagram Report (.docx)
    - □ Layer 2-3 Diagram Export to Microsoft Visio (.zip)

**Networ
Plan**

This rep
identifie
based o
score. F
based u
impact t

Note: If you want to configure an existing Report Task, double click on it from the list of tasks.



Type	Task Label	Description	Em
Generate Reports	[redacted]	NA-Client Risk Report, NA-Network Management Plan, NA-Full Detail Report, NA-Excel Export, NA-Windows Patch Assurance Report, NA-Windows Patch Assuran... notification to be sent to lwrenn@rapidfiretools.com. InDoc upload enabled.	[redacted]

Important: The selected reports will be generated whenever the report task is scheduled to run and when there is available scan data from the Remote Data

© 2021 RapidFire Tools, Inc. All rights reserved.

Collector (RDC). Reporter and all RDCs must be set up properly for each Site. See "Setting Up Reporter" on page 16.

3. Click **Next**.

Step 3 — Set Delivery Method

1. Next you need to configure how you wish to deliver and/or publish the reports for the template. Reporter gives you several options:

   A. To send the generated reports by email, enter an email **Subject** line and each recipient's **Email** address. Then check the **Attach reports to notification** email box.

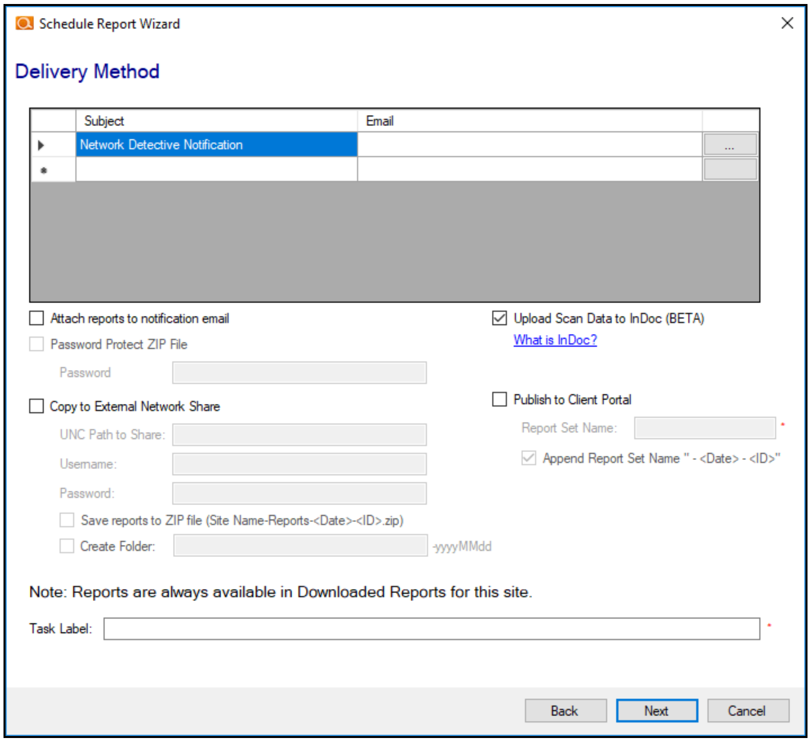
   B. Select **Copy to External Network Share** to publish the reports to a network drive. See also "Copy Reports to External Network Share with Reporter" on page 76.

   C. If you wish to upload scan data to InDoc in the RapidFire Tools Portal, check **Upload Scan Data to InDoc**. See also "Requirements for using InDoc with Reporter" on page 112.

   D. Check **Publish to Client Portal** to make the reports available for the client to view in the RapidFire Tools Portal. See also "RapidFire Tools Portal Client

© 2021 RapidFire Tools, Inc. All rights reserved.

View for Reporter" on page 141.



Schedule Report Wizard

Delivery Method

	Subject	Email	
▸	Network Detective Notification		...
*			

☐ Attach reports to notification email

☐ Password Protect ZIP File

Password

☐ Copy to External Network Share

UNC Path to Share:

Username:

Password:

☐ Save reports to ZIP file (Site Name-Reports-<Date>-<ID>.zip)

☐ Create Folder: -yyyyMMdd

☑ Upload Scan Data to InDoc (BETA)

What is InDoc?

☐ Publish to Client Portal

Report Set Name: *

☑ Append Report Set Name " - <Date> - <ID>"

Note: Reports are always available in Downloaded Reports for this site.

Task Label: *

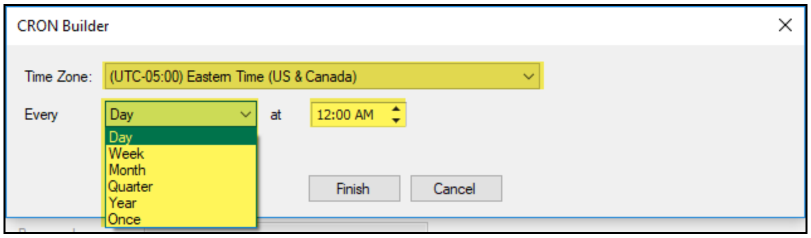
2. Enter a **Task Label** for the report task. Click **Next**.

> **Note:** A Reporter Template can contain several individual Report Tasks, so enter a label to help you distinguish it from other tasks within the template. For example, enter a label based on the module (Security, HIPAA) or the reporting schedule.

Step 4 — Schedule the Report Task

1. The **CRON Builder** (Scheduler) window will appear. Set the time and frequency for which to generate reports.

© 2021 RapidFire Tools, Inc. All rights reserved.



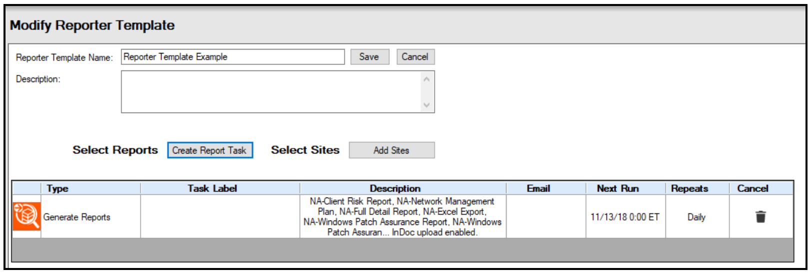
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

2. Click **Finish**.

Important: The time it takes to generate reports will vary depending on the volume of reports you are generating. A large report job for many sites using one Reporter appliance could take several hours. *Keep this in mind when scheduling report tasks*. See "Important Tips for Using Reporter Templates" on page 160 for more details.

3. Your Reporter Task will then appear in the list of tasks associated with your Report Template.



Reporter Template Name: Reporter Template Example

Description:

	Type	Task Label	Description	Email	Next Run	Repeats	Cancel
	Generate Reports		NA-Client Risk Report, NA-Network Management Plan, NA-Full Detail Report, NA-Excel Export, NA-Windows Patch Assurance Report, NA-Windows Patch Assuran... InDoc upload enabled.		11/13/18 0:00 ET	Daily	🗑

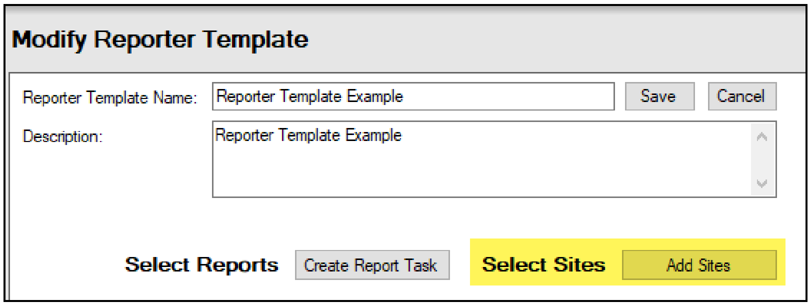
4. Continue adding Report Tasks until you have all of the tasks you want for the Reporter Template.

Step 5 — Assign Template to Sites

Next you will assign the Reporter Template to one or more Sites. To do this:

© 2021 RapidFire Tools, Inc. All rights reserved.

1. Click **Add Sites** next to **Select Sites**.



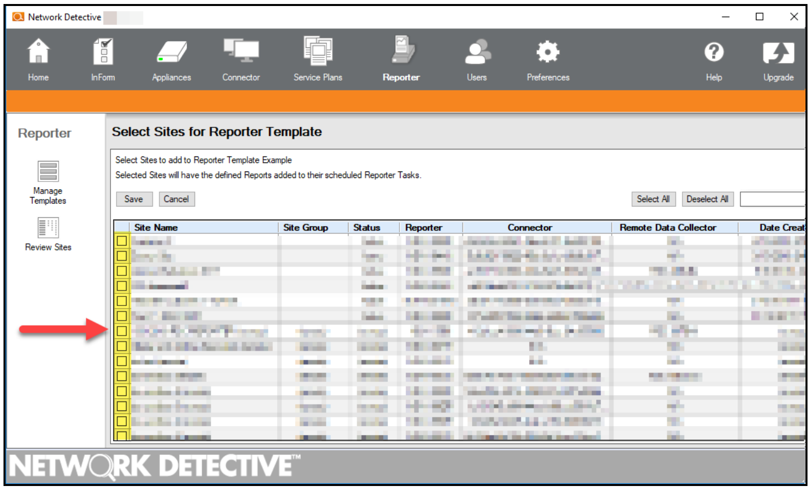
Modify Reporter Template

Reporter Template Name: Reporter Template Example

Description: Reporter Template Example

The list of Sites for your account will appear. Here you can see each Site's assigned Reporter, RDC, and other relevant details.

2. Check the box next to each Reporter Site to which you wish to deploy the template you created.



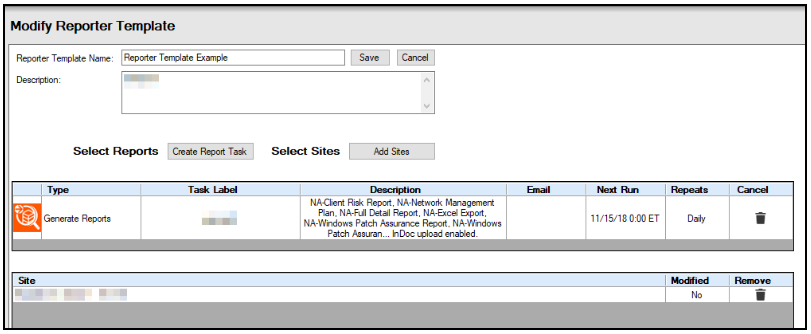
Select Sites for Reporter Template

Select Sites to add to Reporter Template Example

Selected Sites will have the defined Reports added to their scheduled Reporter Tasks.

3. Click **Save**.

The Sites that you applied the template to will appear on the Modify Reporter template page.



Modify Reporter Template

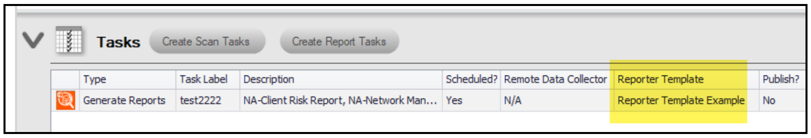
Reporter Template Name: Reporter Template Example

Description: [redacted]

Type	Task Label	Description	Email	Next Run	Repeats	Cancel
Generate Reports	[redacted]	NA-Client Risk Report, NA-Network Management Plan, NA-Full Detail Report, NA-Excel Export, NA-Windows Patch Assurance Report, NA-Windows Patch Assuran... InDoc upload enabled.		11/15/18 0:00 ET	Daily	🗑

Site	Modified	Remove
[redacted]	No	🗑

The Reporter Template Tasks will also appear on the Reporter dashboard on each Site that you applied it to:

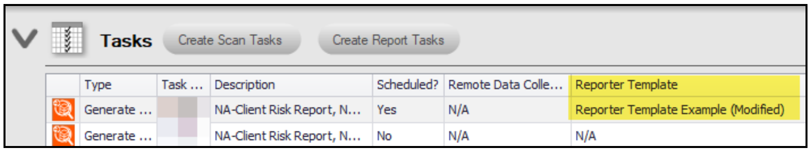


Type	Task Label	Description	Scheduled?	Remote Data Collector	Reporter Template	Publish?
Generate Reports	test2222	NA-Client Risk Report, NA-Network Man…	Yes	N/A	Reporter Template Example	No

From a Site's Reporter Dashboard, you can see if a Report Task is associated with a template. The name of the template will appear in the **Reporter Template field** in the Tasks window.

Modifying Reporter Template Tasks at the Site Level

On a Site level, if you modify a task associated with a Reporter Template, the task will be marked as "Modified" and will no longer be linked to the template.



Type	Task …	Description	Scheduled?	Remote Data Colle…	Reporter Template
Generate …	[redacted]	NA-Client Risk Report, N…	Yes	N/A	Reporter Template Example (Modified)
Generate …	[redacted]	NA-Client Risk Report, N…	No	N/A	N/A

Step 6 — Configure Scans for Reporter Templates

If you have not done so already, you must set up **Remote Data Collector scans** to gather the data from the target networks necessary to generate reports. See "Configuring Remote Data Collector Scans by Assessment Module" on page 78.

Note: We recommend you schedule scans to occur a few hours before your reports are scheduled to be generated.

Important Tips for Using Reporter Templates

Suggestions for Scheduling Report Tasks

- You should schedule your reports to be generated several hours AFTER your Remote Data Collector (RDC) scan tasks.
- If you are managing multiple sites with multiple RDCs, be sure you schedule your report tasks at a time when you know all of your sites will have the most recent scan data. This should be less critical for *monthly* or *quarterly* reports, but is worth considering for *daily* or *weekly* reporting.

How Long Does it Take for Reporter to Complete Report Tasks?

The time it takes to generate reports can vary, depending on factors such as:

- Amount of scan data Reporter needs to process
- Number of Report Tasks assigned to one Reporter at a given time
- Number of Reports selected for a single Report Task
- Number of Sites for which you are generating Reports at a given time

Particularly large tasks for multiple sites could take several hours to complete. Keep this in mind when scheduling Report Tasks for your Sites using Reporter Templates.

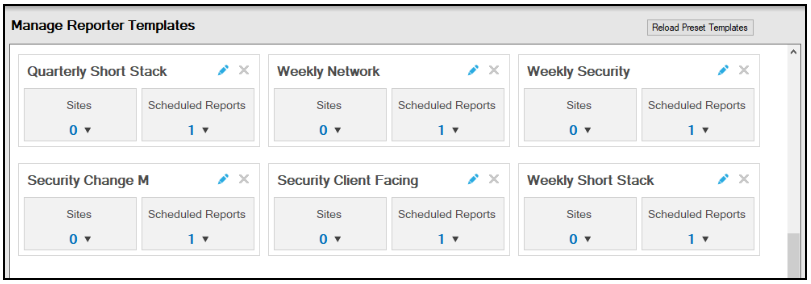
Preset Reporter Templates

You can choose from several preset Reporter Templates from the Manage Reporter Templates screen. You can use these to get started with deploying report tasks to your Sites right away.

- These Preset Templates are for use with the Network and Security Assessment Modules.
- There are presets for Weekly, Monthly, and Quarterly reporting.

© 2021 RapidFire Tools, Inc. All rights reserved.

- There are also both client-facing and in-house reporting presets.



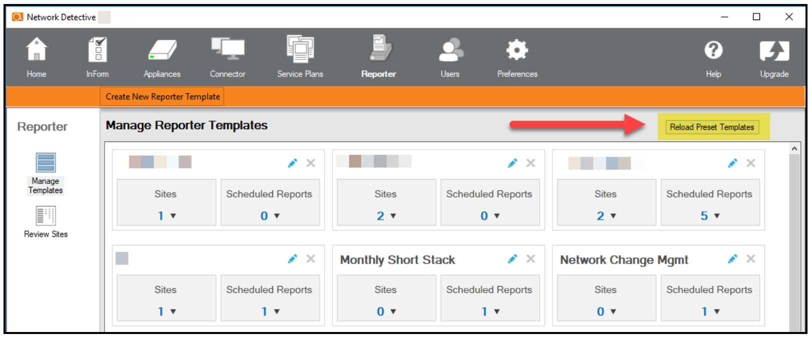
Quarterly Short Stack — Sites 0, Scheduled Reports 1
Weekly Network — Sites 0, Scheduled Reports 1
Weekly Security — Sites 0, Scheduled Reports 1
Security Change M — Sites 0, Scheduled Reports 1
Security Client Facing — Sites 0, Scheduled Reports 1
Weekly Short Stack — Sites 0, Scheduled Reports 1

Reload Preset Templates

To restore the factory preset templates:

1. Click on the **Reporter** icon to go to the **Manage Reporter Templates** screen.
2. Click **Reload Preset Templates** to restore the factory Preset Templates that have been deleted.

> **Note:** This will NOT overwrite your own modified Preset Templates. It will only restore Preset Templates that have been deleted.



Sites 1, Scheduled Reports 0
Sites 2, Scheduled Reports 0
Sites 2, Scheduled Reports 5
Sites 1, Scheduled Reports 1
Monthly Short Stack — Sites 0, Scheduled Reports 1
Network Change Mgmt — Sites 0, Scheduled Reports 1

© 2021 RapidFire Tools, Inc. All rights reserved.

Custom Reports

You can use the Reporter Custom Reports feature to create a custom Network Assessment Module Full Detail Report.

Prerequisites:

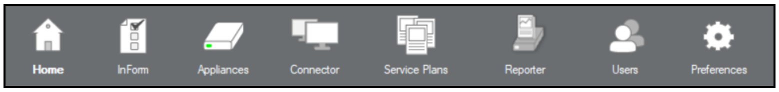
- Customer must subscriber to the Network Assessment Module
- Customer must subscribe to the Reporter
- Customer must have updated their Network Detective application installation to the latest version of ND
- Customer must have updated their Reporter to the latest version of Reporter
- Customer must have installed the Remote Data Collector on a network (Active Directory Based or Workgroup Based)
- Customer must have used the Reporter UI to schedule a 1) Network Scan, 2) A Push Local computer Scan Task, and 3) Set Reporter “Merge” settings to enable these scans to be used for automated report generation

This topic covers two uses for custom reports:

- "Create a Custom Report Template" below
- "Create a Report Generation Task using the Custom Full Detail Report Template" on page 166

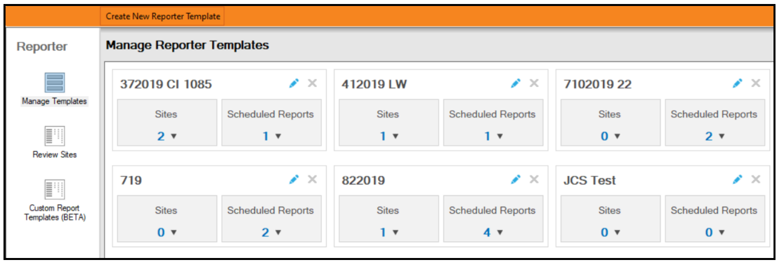
Create a Custom Report Template

1. Log in to Network Detective.
2. Open a Network Detective **Site** associated with Reporter.
3. Select the **Reporter** icon on the Network Detective top ribbon bar.



The **Manager Reporter Templates** window is displayed.

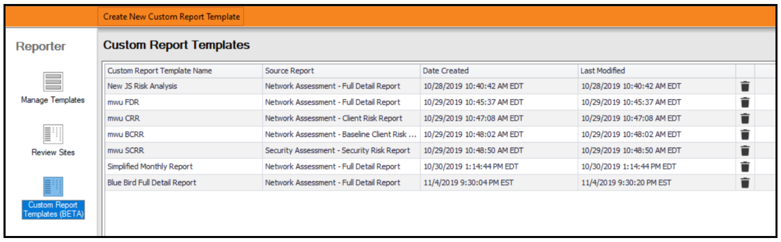
© 2021 RapidFire Tools, Inc. All rights reserved.



Manage Reporter Templates

Template	Sites	Scheduled Reports
372019 CI 1085	2	1
412019 LW	1	1
7102019 22	0	2
719	0	2
822019	1	4
JCS Test	0	0

4. Select the Custom Reports Templates icon in the left hand ribbon bar.

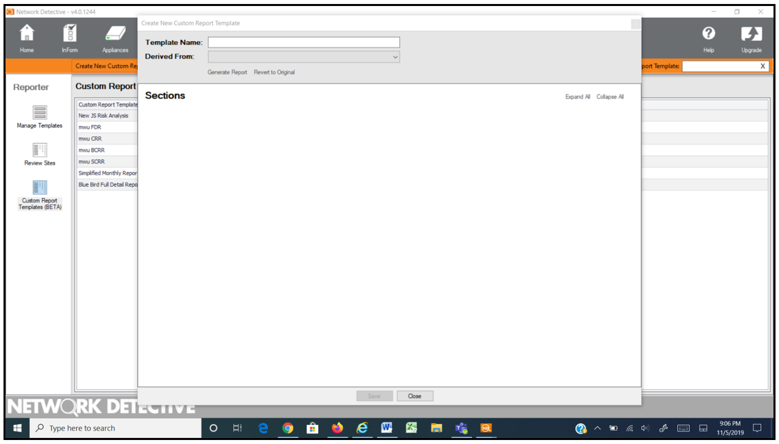

Create New Custom Report Template
Reporter
Manage Templates
Review Sites
Custom Report Templates (BETA)

Custom Report Templates

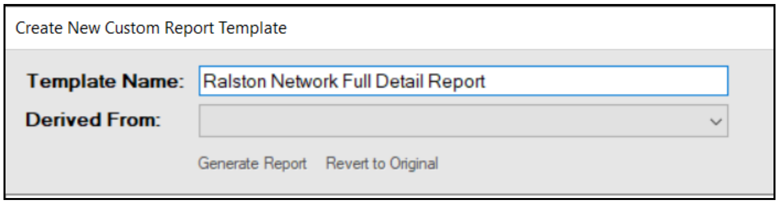
Custom Report Template Name	Source Report	Date Created	Last Modified
New JS Risk Analysis	Network Assessment - Full Detail Report	10/28/2019 10:40:42 AM EDT	10/28/2019 10:40:42 AM EDT
mwu FDR	Network Assessment - Full Detail Report	10/29/2019 10:45:37 AM EDT	10/29/2019 10:45:37 AM EDT
mwu CRR	Network Assessment - Client Risk Report	10/29/2019 10:47:08 AM EDT	10/29/2019 10:47:08 AM EDT
mwu BCRR	Network Assessment - Baseline Client Risk ...	10/29/2019 10:48:02 AM EDT	10/29/2019 10:48:02 AM EDT
mwu SCRR	Security Assessment - Security Risk Report	10/29/2019 10:48:50 AM EDT	10/29/2019 10:48:50 AM EDT
Simplified Monthly Report	Network Assessment - Full Detail Report	10/30/2019 1:14:44 PM EDT	10/30/2019 1:14:44 PM EDT
Blue Bird Full Detail Report	Network Assessment - Full Detail Report	11/4/2019 9:30:04 PM EST	11/4/2019 9:30:20 PM EST

This Custom Reports window is displayed.

5. Select the **Create New Customer Report Template** button.
6. The Create New Custom Report Template window is displayed.



7. Type in the name of the new Custom Report Template.

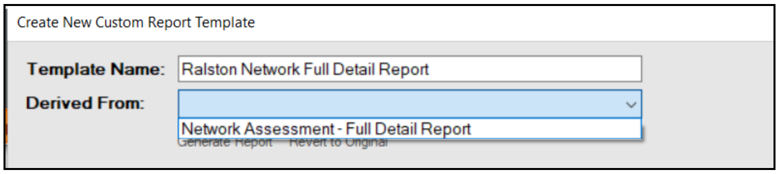


Template Name: Ralston Network Full Detail Report

Derived From:

© 2021 RapidFire Tools, Inc. All rights reserved.

8. Select the Network Assessment - Full Detail Assessment option from the Derived From list.

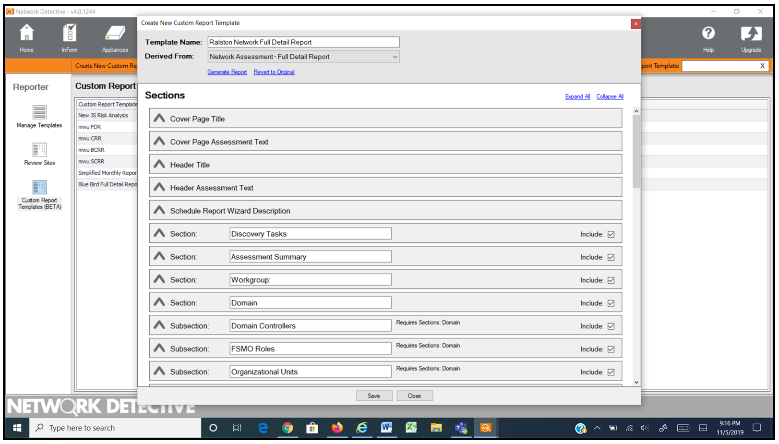


Create New Custom Report Template

Template Name: Ralston Network Full Detail Report

Derived From: Network Assessment - Full Detail Report

9. The Sections of the Full Detail Report that can be customized are presented in the Create New Custom Report Template window.



Create New Custom Report Template

Template Name: Ralston Network Full Detail Report

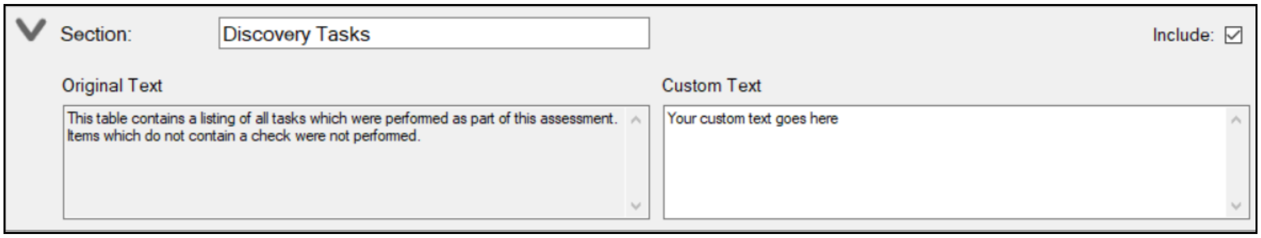
Derived From: Network Assessment - Full Detail Report

Sections

Cover Page Title			
Cover Page Assessment Text			
Header Title			
Header Assessment Text			
Schedule Report Wizard Description			
Section:	Discovery Tasks		Include: ☑
Section:	Assessment Summary		Include: ☑
Section:	Workgroup:		Include: ☑
Section:	Domain		Include: ☑
Subsection:	Domain Controllers	Requires Sections: Domain	Include: ☑
Subsection:	FSMO Roles	Requires Sections: Domain	Include: ☑
Subsection:	Organizational Units	Requires Sections: Domain	Include: ☑

Customization Features include:

- Include Feature – This feature enables inclusion or removal sections from the Full Detail Report.
- Custom Text – This feature enables the modification of the Full Detail Report's Original Text contained in the report describing each report Section's findings.



Section: Discovery Tasks Include: ☑

Original Text

This table contains a listing of all tasks which were performed as part of this assessment. Items which do not contain a check were not performed.

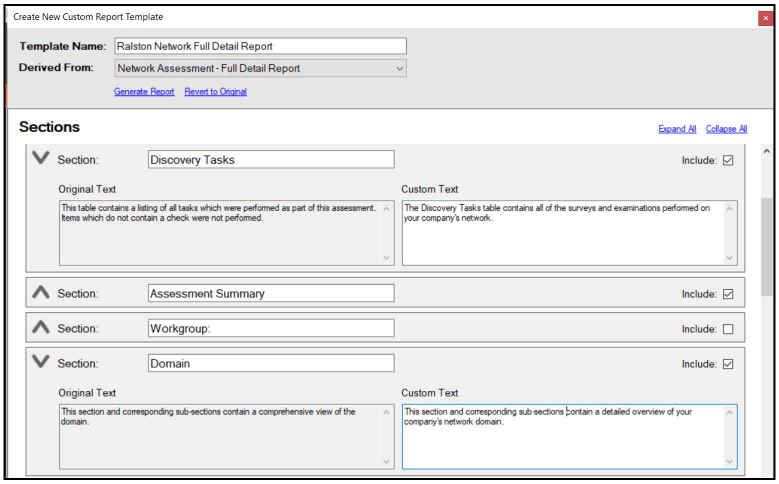
Custom Text

Your custom text goes here

10. Select all of the Sections that should be "Included" in the Custom Full Detail report.

11. For all of the sections to be included in the report, add Custom Text that will replace the original text contain in the Full Detail report.

© 2021 RapidFire Tools, Inc. All rights reserved.



Template Name: Ralston Network Full Detail Report
Derived From: Network Assessment - Full Detail Report

Section: Discovery Tasks Include: ☑

Original Text: This table contains a listing of all tasks which were performed as part of this assessment. Items which do not contain a check were not performed.

Custom Text: The Discovery Tasks table contains all of the surveys and examinations performed on your company's network.

Section: Assessment Summary Include: ☑

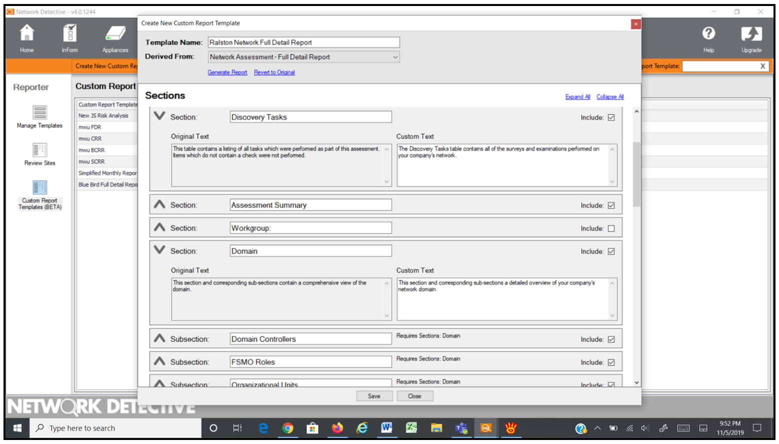
Section: Workgroup: Include: □

Section: Domain Include: ☑

Original Text: This section and corresponding sub-sections contain a comprehensive view of the domain.

Custom Text: This section and corresponding sub-sections contain a detailed overview of your company's network domain.

12. Select the Save Button to save your Custom Full Detail Report template that can be used by all of the Network Detective Sites associated with the Reporter.



Template Name: Ralston Network Full Detail Report
Derived From: Network Assessment - Full Detail Report

Section: Discovery Tasks Include: ☑

Original Text: This table contains a listing of all tasks which were performed as part of this assessment. Items which do not contain a check were not performed.

Custom Text: The Discovery Tasks table contains all of the surveys and examinations performed on your company's network.

Section: Assessment Summary Include: ☑

Section: Workgroup: Include: □

Section: Domain Include: ☑

Original Text: This section and corresponding sub-sections contain a comprehensive view of the domain.

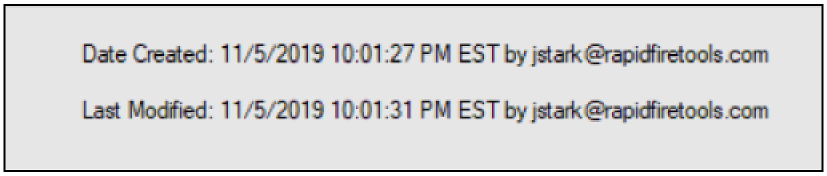
Custom Text: This section and corresponding sub-sections a detailed overview of your company's network domain.

Subsection: Domain Controllers Requires Sections: Domain Include: ☑

Subsection: FSMO Roles Requires Sections: Domain Include: ☑

Subsection: Organizational Units Requires Sections: Domain Include: ☑

13. The following information will be displayed in the Create New Custom Report Template window.



Date Created: 11/5/2019 10:01:27 PM EST by jstark@rapidfiretools.com

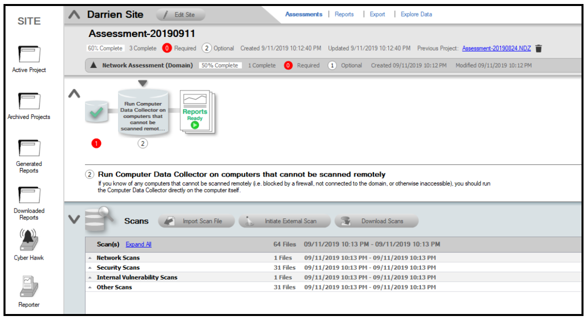
Last Modified: 11/5/2019 10:01:31 PM EST by jstark@rapidfiretools.com

14. Select the Close button to close the Create New Custom Report Template window.

© 2021 RapidFire Tools, Inc. All rights reserved.

Create a Report Generation Task using the Custom Full Detail Report Template

1. Log into Network Detective.
2. Open the Network Detective Site associated with the Reporter.
3. Select the Reporter icon on the left hand ribbon bar.



Assessment-20190911

60% Complete 3 Complete 0 Required 2 Optional Created 9/11/2019 10:12:40 PM Updated 9/11/2019 10:12:40 PM Previous Project: Assessment-20190824.NDZ

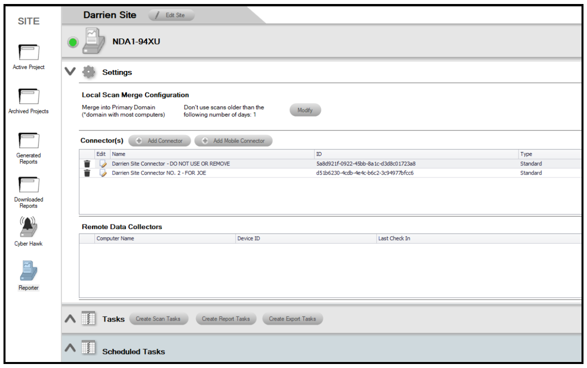
Network Assessment (Domain) 50% Complete 1 Complete 0 Required 1 Optional Created 09/11/2019 10:12 PM Modified 09/11/2019 10:12 PM

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

If you know of any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible), you should run the Computer Data Collector directly on the computer itself.

Scan(s) Expand All	64 Files	09/11/2019 10:13 PM - 09/11/2019 10:13 PM
Network Scans	1 Files	09/11/2019 10:13 PM - 09/11/2019 10:13 PM
Security Scans	31 Files	09/11/2019 10:13 PM - 09/11/2019 10:13 PM
Internal Vulnerability Scans	1 Files	09/11/2019 10:13 PM - 09/11/2019 10:13 PM
Other Scans	31 Files	09/11/2019 10:13 PM - 09/11/2019 10:13 PM

The Reporter UI will be displayed.



NDA1-94XU

Local Scan Merge Configuration

Merge into Primary Domain (*domain with most computers)

Don't use scans older than the following number of days: 1

Connector(s)

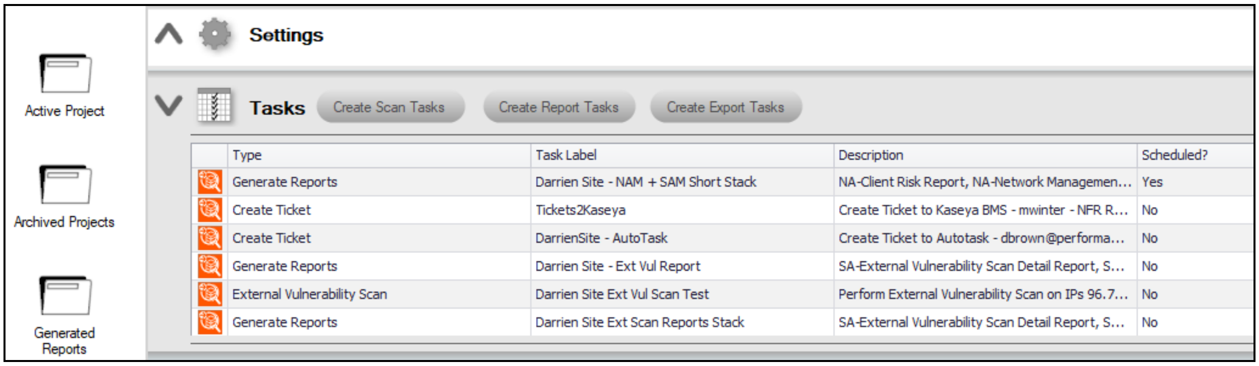
Edit	Name	ID	Type
	Darrien Site Connector - DO NOT USE OR REMOVE	5a8d921f-0922-45bb-8a1c-d3d8c01723a8	Standard
	Darrien Site Connector NO. 2 - FOR JOE	d51b6230-4cdb-4e4c-b6c2-3c94977bfcc6	Standard

Remote Data Collectors

Computer Name	Device ID	Last Check In

4. Click on the Tasks ^ Selector to expand the Reporter Tasks list.
5. The Tasks list is expanded.

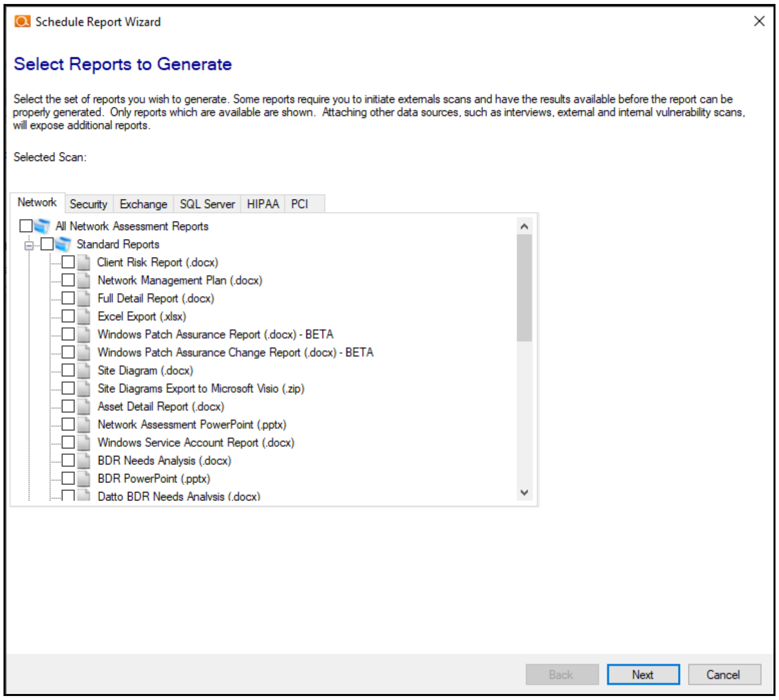
© 2021 RapidFire Tools, Inc. All rights reserved.



Type	Task Label	Description	Scheduled?
Generate Reports	Darrien Site - NAM + SAM Short Stack	NA-Client Risk Report, NA-Network Managemen...	Yes
Create Ticket	Tickets2Kaseya	Create Ticket to Kaseya BMS - mwinter - NFR R...	No
Create Ticket	DarrienSite - AutoTask	Create Ticket to Autotask - dbrown@performa...	No
Generate Reports	Darrien Site - Ext Vul Report	SA-External Vulnerability Scan Detail Report, S...	No
External Vulnerability Scan	Darrien Site Ext Vul Scan Test	Perform External Vulnerability Scan on IPs 96.7...	No
Generate Reports	Darrien Site Ext Scan Reports Stack	SA-External Vulnerability Scan Detail Report, S...	No

6. Select the Create Report Tasks button

   The Schedule Reports Window is displayed.



Select Reports to Generate

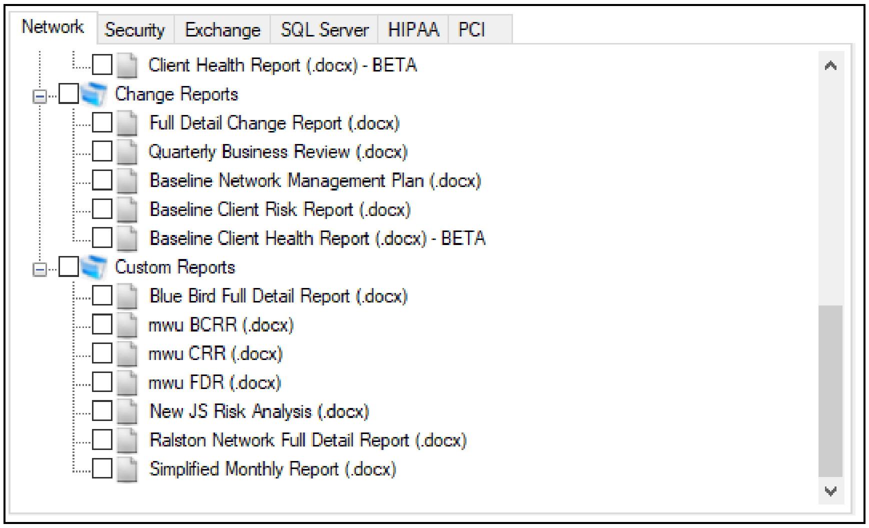
Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

Selected Scan:

- □ All Network Assessment Reports
  - □ Standard Reports
    - □ Client Risk Report (.docx)
    - □ Network Management Plan (.docx)
    - □ Full Detail Report (.docx)
    - □ Excel Export (.xlsx)
    - □ Windows Patch Assurance Report (.docx) - BETA
    - □ Windows Patch Assurance Change Report (.docx) - BETA
    - □ Site Diagram (.docx)
    - □ Site Diagrams Export to Microsoft Visio (.zip)
    - □ Asset Detail Report (.docx)
    - □ Network Assessment PowerPoint (.pptx)
    - □ Windows Service Account Report (.docx)
    - □ BDR Needs Analysis (.docx)
    - □ BDR PowerPoint (.pptx)
    - □ Datto BDR Needs Analysis (.docx)

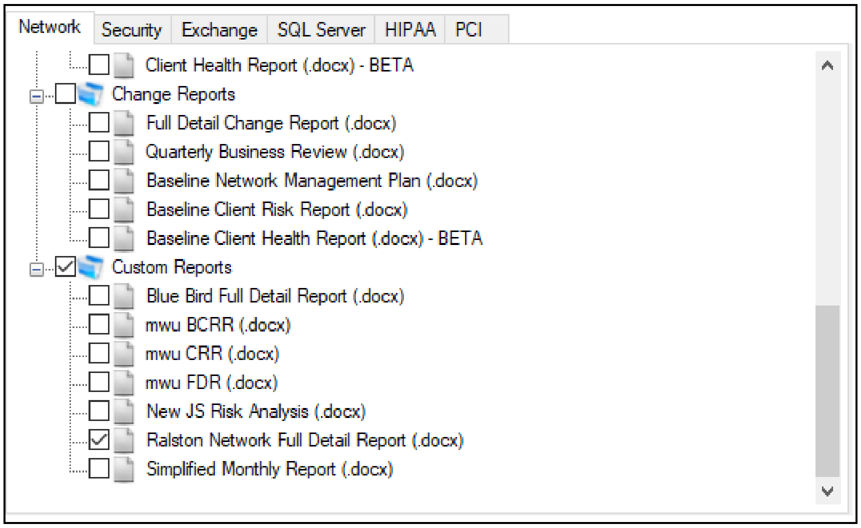
7. Select the Network Tab to display the Reports list of the Network Assessment Module.
8. Scroll to the bottom of the Network Assessment Module Reports List to view the available customer Reports. (Note that the "Ralston Network Full Detail Report" created as a Custom Report Template is available on the Custom Reports list).

© 2021 RapidFire Tools, Inc. All rights reserved.



- □ Client Health Report (.docx) - BETA
- □ Change Reports
  - □ Full Detail Change Report (.docx)
  - □ Quarterly Business Review (.docx)
  - □ Baseline Network Management Plan (.docx)
  - □ Baseline Client Risk Report (.docx)
  - □ Baseline Client Health Report (.docx) - BETA
- □ Custom Reports
  - □ Blue Bird Full Detail Report (.docx)
  - □ mwu BCRR (.docx)
  - □ mwu CRR (.docx)
  - □ mwu FDR (.docx)
  - □ New JS Risk Analysis (.docx)
  - □ Ralston Network Full Detail Report (.docx)
  - □ Simplified Monthly Report (.docx)

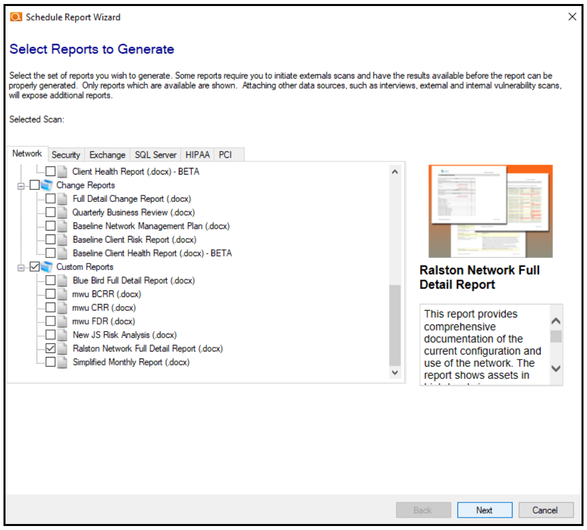
9. Select the Custom Report that is to be generated by the Report Task being created.



- □ Client Health Report (.docx) - BETA
- □ Change Reports
  - □ Full Detail Change Report (.docx)
  - □ Quarterly Business Review (.docx)
  - □ Baseline Network Management Plan (.docx)
  - □ Baseline Client Risk Report (.docx)
  - □ Baseline Client Health Report (.docx) - BETA
- ☑ Custom Reports
  - □ Blue Bird Full Detail Report (.docx)
  - □ mwu BCRR (.docx)
  - □ mwu CRR (.docx)
  - □ mwu FDR (.docx)
  - □ New JS Risk Analysis (.docx)
  - ☑ Ralston Network Full Detail Report (.docx)
  - □ Simplified Monthly Report (.docx)

10. Select the Next button to proceed in creating the Report Task.

© 2021 RapidFire Tools, Inc. All rights reserved.



Schedule Report Wizard

Select Reports to Generate

Select the set of reports you wish to generate. Some reports require you to initiate externals scans and have the results available before the report can be properly generated. Only reports which are available are shown. Attaching other data sources, such as interviews, external and internal vulnerability scans, will expose additional reports.

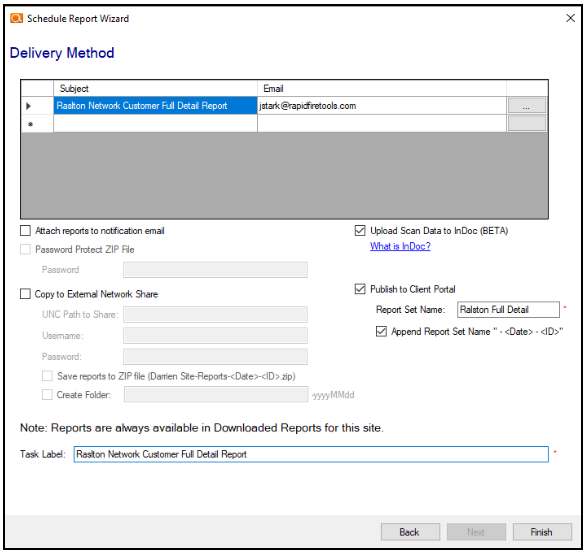
Selected Scan:

- □ Client Health Report (.docx) - BETA
- □ Change Reports
  - □ Full Detail Change Report (.docx)
  - □ Quarterly Business Review (.docx)
  - □ Baseline Network Management Plan (.docx)
  - □ Baseline Client Risk Report (.docx)
  - □ Baseline Client Health Report (.docx) - BETA
- ☑ Custom Reports
  - □ Blue Bird Full Detail Report (.docx)
  - □ mwu BCRR (.docx)
  - □ mwu CRR (.docx)
  - □ mwu FDR (.docx)
  - □ New JS Risk Analysis (.docx)
  - ☑ Ralston Network Full Detail Report (.docx)
  - □ Simplified Monthly Report (.docx)

Ralston Network Full Detail Report

This report provides comprehensive documentation of the current configuration and use of the network. The report shows assets in

11. Set up the Delivery Method for the Report Task.



Schedule Report Wizard

Delivery Method

	Subject	Email
▶	Rasiton Network Customer Full Detail Report	jstark@rapidfiretools.com
*		

□ Attach reports to notification email

□ Password Protect ZIP File

Password

□ Copy to External Network Share

UNC Path to Share:

Username:

Password:

□ Save reports to ZIP file (Damien Site-Reports-<Date>-<ID>.zip)

□ Create Folder: -yyyyMMdd

☑ Upload Scan Data to InDoc (BETA)

What is InDoc?

☑ Publish to Client Portal

Report Set Name: Ralston Full Detail *

☑ Append Report Set Name " - <Date> - <ID>"

Note: Reports are always available in Downloaded Reports for this site.

Task Label: Rasiton Network Customer Full Detail Report *

12. Select the Finish button to complete the creation of the Report Task for the Custom Report.

13. Either select the newly created Custom Report Task's "Run Now" link to generate the report, or schedule the report to the generated at a schedule Day and Time.

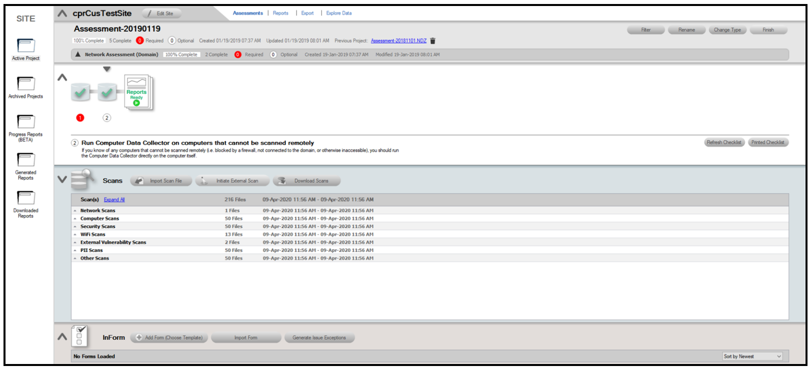
© 2021 RapidFire Tools, Inc. All rights reserved.

Generate Client Progress Reports

The **Client Progress Report** is designed to be generated after you have completed several Network and Security Assessments. This report compares key areas over time and display trending changes with charts and graphs. Computers are given a letter grade ('A' through 'F').

Important: The Client Progress Report requires a minimum of 2 assessments, containing both Network and Security Scans. The report will compare a maximum of 10 total assessments. Network Detective will notify you if the Site does not meet these requirements.

1. Open a Reporter site with two or more archived assessments containing both Network and Security Scans. These assessments can be archived. A current assessment is not required.



Assessment-20190119

100% Complete 5 Complete 0 Required 0 Optional Created 01/19/2019 07:37 AM Updated 01/19/2019 08:01 AM Previous Project: Assessment-20181101.NDZ

Network Assessment (Domain) 100% Complete 2 Complete 0 Required 0 Optional Created 19-Jan-2019 07:37 AM Modified 19-Jan-2019 08:01 AM

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

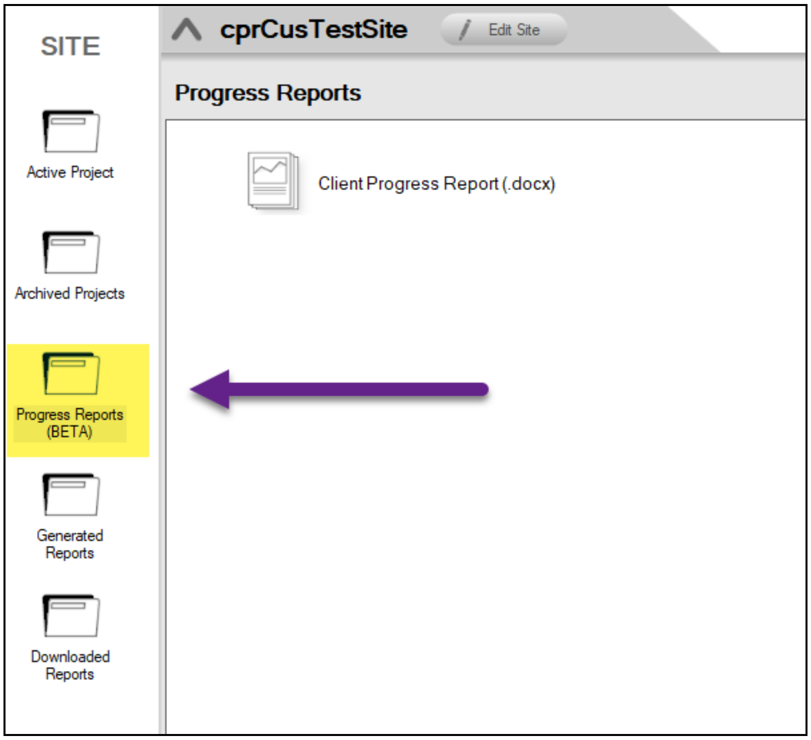
If you know of any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible), you should run the Computer Data Collector directly on the computer itself.

Scan(s) Expand All	216 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
Network Scans	1 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
Computer Scans	50 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
Security Scans	50 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
WiFi Scans	13 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
External Vulnerability Scans	2 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
PII Scans	50 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM
Other Scans	50 Files	09-Apr-2020 11:56 AM - 09-Apr-2020 11:56 AM

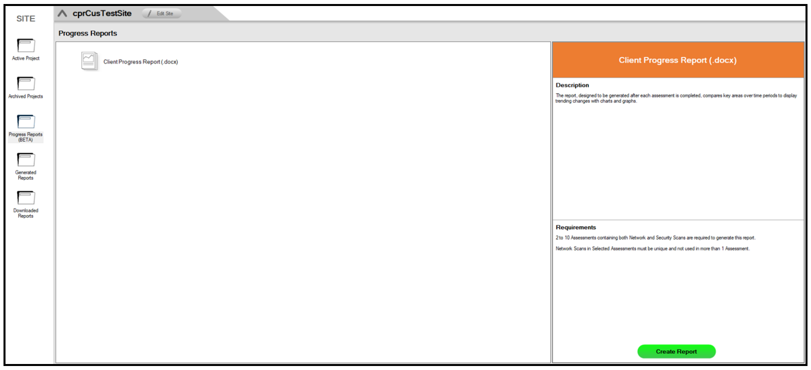
No Forms Loaded

2. On the left-hand site menu, click **Progress Reports (BETA)**.

© 2021 RapidFire Tools, Inc. All rights reserved.



3. Click **Client Progress Reports** (.docx). From the side panel, you can find report details and requirements.



Description

The report, designed to be generated after each assessment is completed, compares key areas over time periods to display trending changes with charts and graphs.

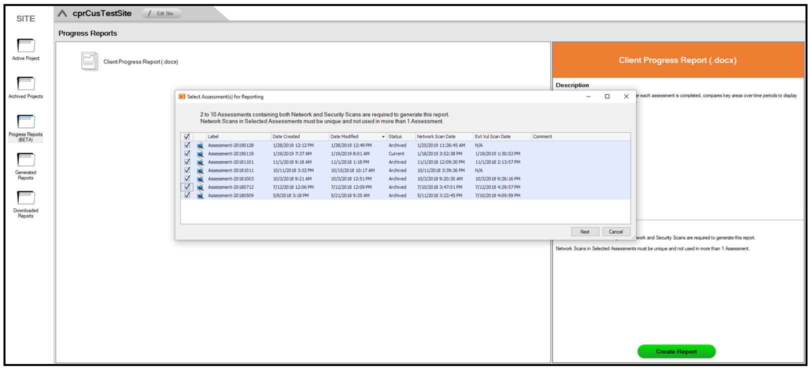
Requirements

2 to 10 Assessments containing both Network and Security Scans are required to generate this report.

Network Scans in Selected Assessments must be unique and not used in more than 1 Assessment.

4. From the side panel, click **Create Reports**.
5. Select which assessments to include in the report (minimum of 2). All assessments are included in the report by default (up to 10). Then click **Next**.

© 2021 RapidFire Tools, Inc. All rights reserved.



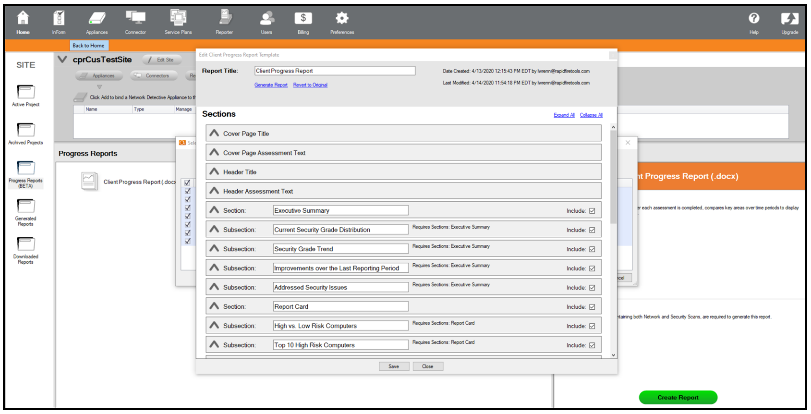
Select Assessment(s) for Reporting

2 to 10 Assessments containing both Network and Security Scans are required to generate this report.
Network Scans in Selected Assessments must be unique and not used in more than 1 Assessment.

☑	Label	Date Created	Date Modified	Status	Network Scan Date	Ext Vul Scan Date	Comment
☑	Assessment-20190128	1/28/2019 12:12 PM	1/28/2019 12:49 PM	Archived	1/25/2019 11:26:45 AM	N/A	
☑	Assessment-20190119	1/19/2019 7:37 AM	1/19/2019 8:01 AM	Current	1/18/2019 3:52:38 PM	1/19/2019 1:30:53 PM	
☑	Assessment-20181101	11/1/2018 9:18 AM	11/1/2018 1:18 PM	Archived	11/1/2018 12:09:30 PM	11/1/2018 2:13:57 PM	
☑	Assessment-20181011	10/11/2018 3:32 PM	10/15/2018 10:17 AM	Archived	10/11/2018 3:39:36 PM	N/A	
☑	Assessment-20181003	10/3/2018 9:21 AM	10/3/2018 12:51 PM	Archived	10/3/2018 9:20:30 AM	10/3/2018 9:26:16 PM	
☑	Assessment-20180712	7/12/2018 12:06 PM	7/12/2018 12:09 PM	Archived	7/10/2018 3:47:01 PM	7/12/2018 4:29:57 PM	
☑	Assessment-20180509	5/9/2018 3:18 PM	5/21/2018 9:35 AM	Archived	5/11/2018 3:22:45 PM	7/10/2018 4:09:59 PM	

6. From the **Edit Client Progress Reports** screen, you can change and edit the text of the report, including its title and subsections. You can likewise add custom text to each section and decide to exclude certain sections, if you choose.

> **Note:** Click **Save** to keep a record of your edits to the report. Date Created and Date Modified are displayed on the form.



Edit Client Progress Report Template

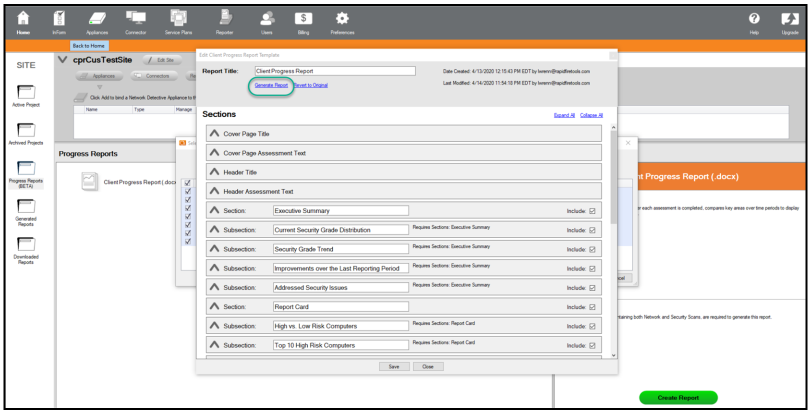
Report Title: Client Progress Report

Date Created: 4/13/2020 12:15:43 PM EDT by lwrenn@rapidfiretools.com
Last Modified: 4/14/2020 11:54:18 PM EDT by lwrenn@rapidfiretools.com

Sections

Cover Page Title			
Cover Page Assessment Text			
Header Title			
Header Assessment Text			
Section:	Executive Summary		Include: ☑
Subsection:	Current Security Grade Distribution	Requires Sections: Executive Summary	Include: ☑
Subsection:	Security Grade Trend	Requires Sections: Executive Summary	Include: ☑
Subsection:	Improvements over the Last Reporting Period	Requires Sections: Executive Summary	Include: ☑
Subsection:	Addressed Security Issues	Requires Sections: Executive Summary	Include: ☑
Section:	Report Card		Include: ☑
Subsection:	High vs. Low Risk Computers	Requires Sections: Report Card	Include: ☑
Subsection:	Top 10 High Risk Computers	Requires Sections: Report Card	Include: ☑

7. When you are ready, click **Generate Report**. After the report is built, it will appear in Windows File Explorer.



Edit Client Progress Report Template

Report Title: Client Progress Report

Date Created: 4/13/2020 12:15:43 PM EDT by lwrenn@rapidfiretools.com
Last Modified: 4/14/2020 11:54:18 PM EDT by lwrenn@rapidfiretools.com

Sections

Cover Page Title
Cover Page Assessment Text
Header Title
Header Assessment Text
Section: Executive Summary Include: ☑
Subsection: Current Security Grade Distribution Requires Sections: Executive Summary Include: ☑
Subsection: Security Grade Trend Requires Sections: Executive Summary Include: ☑
Subsection: Improvements over the Last Reporting Period Requires Sections: Executive Summary Include: ☑
Subsection: Addressed Security Issues Requires Sections: Executive Summary Include: ☑
Section: Report Card Include: ☑
Subsection: High vs. Low Risk Computers Requires Sections: Report Card Include: ☑
Subsection: Top 10 High Risk Computers Requires Sections: Report Card Include: ☑

© 2021 RapidFire Tools, Inc. All rights reserved.

Set Scan and Report Task Time Zone and Date Format

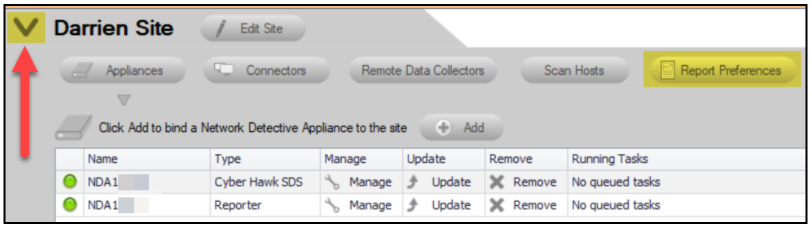
You can configure the time zones and dates that appear next to your Site's scan and report tasks. This feature applies to both **Reporter** and **Inspector** for Network Detective.

- You can use this feature from **Global Preferences** to ensure all of your NEWLY CREATED sites display scan and report task times in your own local time zone.
- Alternatively, if you are responsible for several sites in different time zones, you can use **Site Preferences** to change the time zone for each site. This can help you more easily determine when a task will occur with sites in different time zones.

To set preferences:

At Site Level

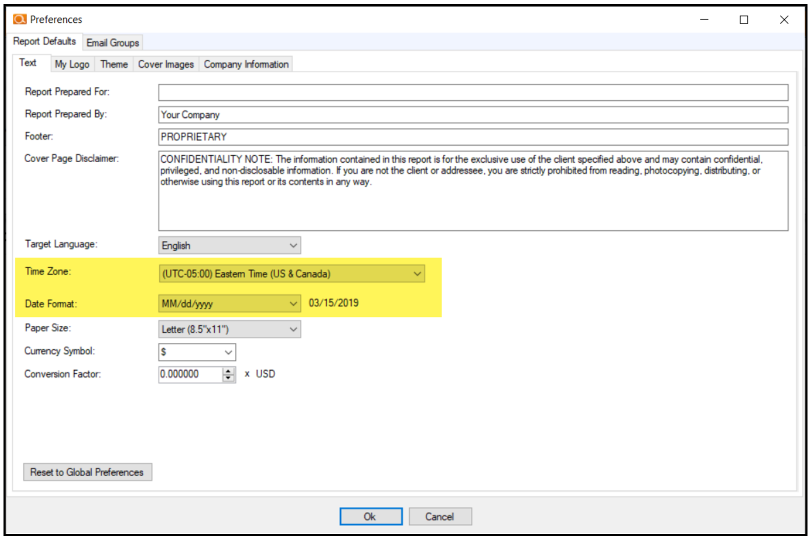
1. Open your **Reporter** or **Inspector** Site in Network Detective.
2. Open the Site Settings and click **Report Preferences**.



Click Add to bind a Network Detective Appliance to the site

	Name	Type	Manage	Update	Remove	Running Tasks
●	NDA1 [redacted]	Cyber Hawk SDS	Manage	Update	Remove	No queued tasks
●	NDA1 [redacted]	Reporter	Manage	Update	Remove	No queued tasks

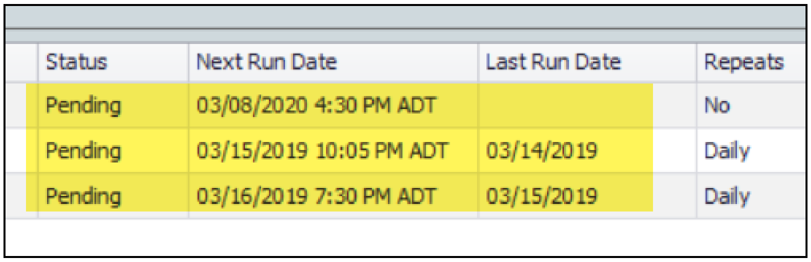
3. From **Report Defaults** > **Text**, select your desired **Time Zone** and **Date Format**. Click **OK**.



Report Prepared For:	
Report Prepared By:	Your Company
Footer:	PROPRIETARY
Cover Page Disclaimer:	CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.
Target Language:	English
Time Zone:	(UTC-05:00) Eastern Time (US & Canada)
Date Format:	MM/dd/yyyy 03/15/2019
Paper Size:	Letter (8.5"x11")
Currency Symbol:	$
Conversion Factor:	0.000000 x USD

© 2021 RapidFire Tools, Inc. All rights reserved.

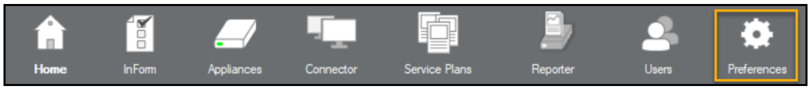
Your scheduled scan and report tasks will now appear with your preferred time zone and date format for just this site.



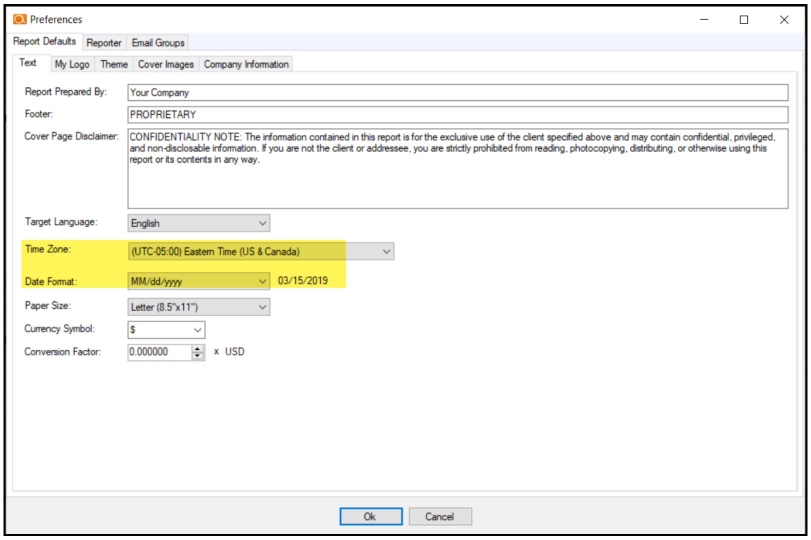
Status	Next Run Date	Last Run Date	Repeats
Pending	03/08/2020 4:30 PM ADT		No
Pending	03/15/2019 10:05 PM ADT	03/14/2019	Daily
Pending	03/16/2019 7:30 PM ADT	03/15/2019	Daily

At Global Level

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



2. From **Report Defaults** > **Text**, select your desired **Time Zone** and **Date Format**. Click **OK**.



Report Prepared By: Your Company

Footer: PROPRIETARY

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

Target Language: English

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Date Format: MM/dd/yyyy 03/15/2019

Paper Size: Letter (8.5"x11")

Currency Symbol: $

Conversion Factor: 0.000000 x USD

Unless you have adjusted your preferences at the Site level, your NEWLY CREATED Site's scheduled scan and report tasks will now appear with your preferred time zone and date format.

> **Note:** New *Reporter Templates* you create and apply will also use your Global **Time Zone** and **Date Format** preferences.

© 2021 RapidFire Tools, Inc. All rights reserved.

Integrate Reporter with a PSA System with Export Tasks

With Reporter and Network Detective, you can *automatically* export important information uncovered during your scans into your preferred Professional Services Automation (PSA) system with **Export Tasks**. 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 Reporter with your chosen PSA System.

Step 1 — Gather Credentials and Set Up your PSA System

Before you begin, you will need:

- Valid Login Credentials for Network Detective
- A Network Detective "Site" for which you wish to export items or create tickets in your PSA
- Valid Login Credentials for your PSA system account (if you wish to integrate Network Detective with multiple PSA accounts, gather credentials for each PSA account)
- A Reporter associated with your Site, as well as the Remote Data Collector that has collected scan data. See also "Setting Up Reporter" on page 16.
- Other prerequisites specific to your chosen PSA system (refer to the table below).

PSA System	PSA Prerequisites
Autotask®	• Autotask Username • Autotask Password
REST ConnectWise™	• ConnectWise REST Public Key • ConnectWise REST Private Key • ConnectWise Company ID • ConnectWise PSA URL **Note:** You must configure ConnectWise correctly before you can integrate with Network Detective. See also "Set Up ConnectWise REST Integration" on

© 2021 RapidFire Tools, Inc. All rights reserved.

PSA System	PSA Prerequisites
	page 191
SOAP ConnectWise™	- ConnectWise Username - ConnectWise Password - ConnectWise Company ID - ConnectWise PSA URL **Note:** You must configure ConnectWise correctly before you can integrate with Network Detective. See also "Set Up ConnectWise SOAP Integration" on page 195
Tigerpaw® SOFTWARE	- Tigerpaw Username - Tigerpaw Password - Tigerpaw API URL
BMS™ by Kaseya	- Kaseya Username - Kaseya Password **Note:** The Kaseya User must be in the Kaseya Administrator Role. See also "Set Up Kaseya BMS Integration" on page 197. - Kaseya Tenant (i.e. company name) - Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

© 2021 RapidFire Tools, Inc. All rights reserved.

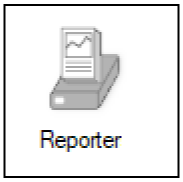
PSA System	PSA Prerequisites
ITGlue	- **Works with Export Configurations ONLY** - IT Glue API URL **Note:** For the API URL, use **https://api.itglue.com**. If your IT Glue account is in the EU Data Center, use **https://api.eu.itglue.com.** - IT Glue API Key **Note:** You will generate the API Key in the IT Glue application.

Step 2 — Create Export Task with Reporter

1. **Start Network Detective** and log in with your credentials.
2. Open the Reporter **Site** for which you wish to create tickets in the target PSA.

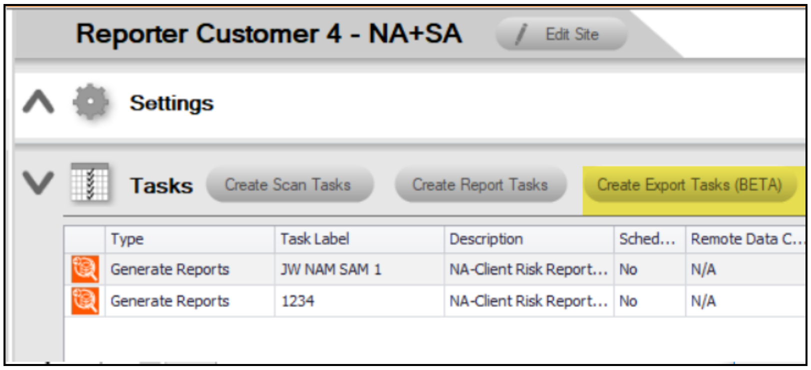
   > **Note:** You must have scan data and must have generated reports in order to create tickets.

3. Click the **Reporter** icon in the bottom left of the screen to open the Reporter dashboard.



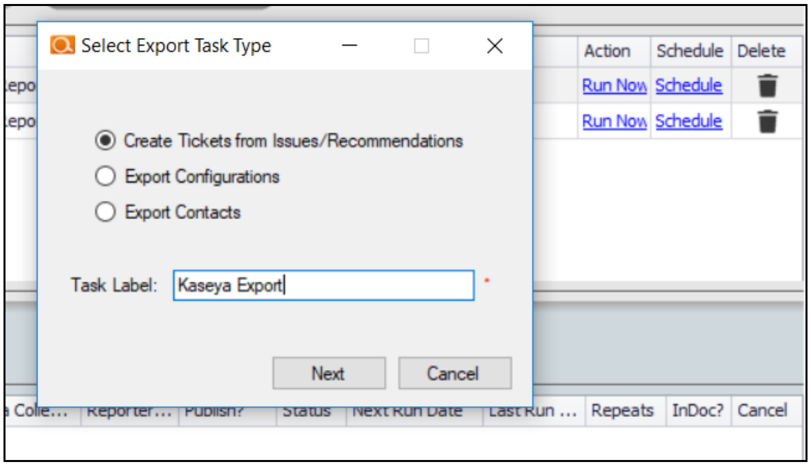
4. From the Reporter dashboard, click **Create Export Tasks**.

© 2021 RapidFire Tools, Inc. All rights reserved.



	Type	Task Label	Description	Sched…	Remote Data C…
	Generate Reports	JW NAM SAM 1	NA-Client Risk Report…	No	N/A
	Generate Reports	1234	NA-Client Risk Report…	No	N/A

5. Choose an **Export Task Type** from the drop-down menu.



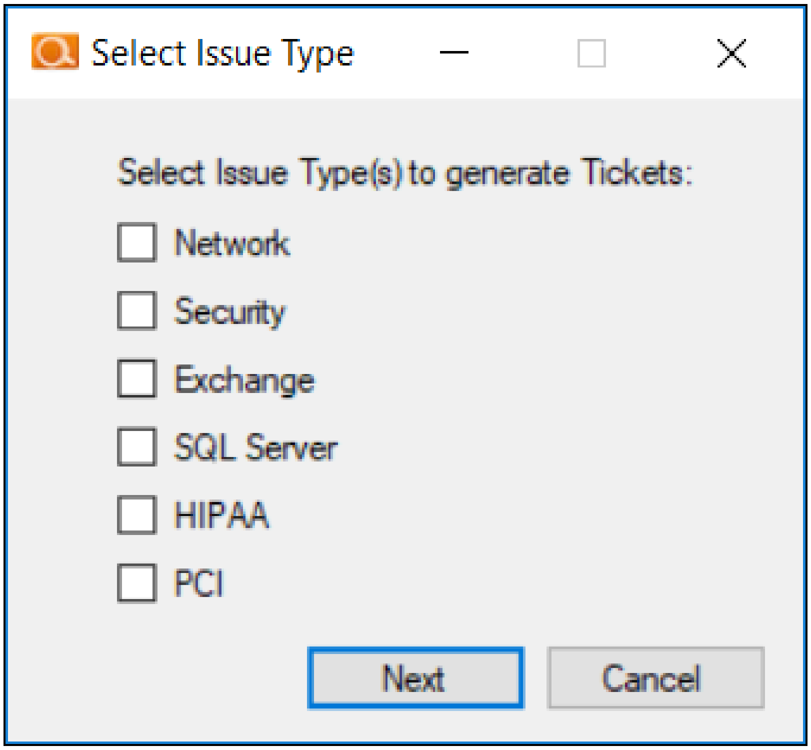
● Create Tickets from Issues/Recommendations
○ Export Configurations
○ Export Contacts

Task Label: Kaseya Export *

> **Note:**
> a) **Create Tickets** – Automatically create tickets in your company's PSA/Ticketing System.
> b) **Export Configurations** – Export Configurations (hardware information, etc.) into Autotask, Kaseya BMS, ConnectWise, Tiger Paw, or ITGlue.
> c) **Export Contacts** – Export Contacts identified by the Exchange Assessment Module into Autotask, Kaseya BMS, ConnectWise, or Tiger Paw.

6. Select the module/type of issues for which to generate tickets.

© 2021 RapidFire Tools, Inc. All rights reserved.



Select Issue Type

Select Issue Type(s) to generate Tickets:

□ Network

□ Security

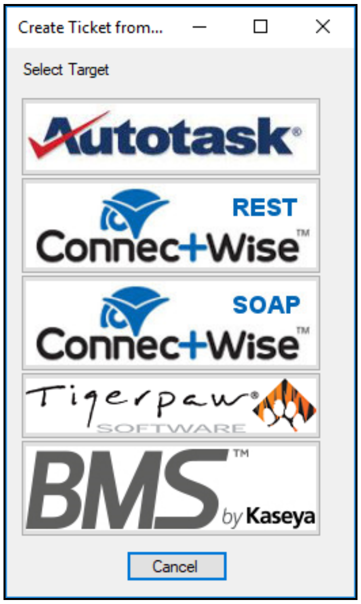
□ Exchange

□ SQL Server

□ HIPAA

□ PCI

7. **Select your Target** Ticketing/PSA system from the list of supported options.

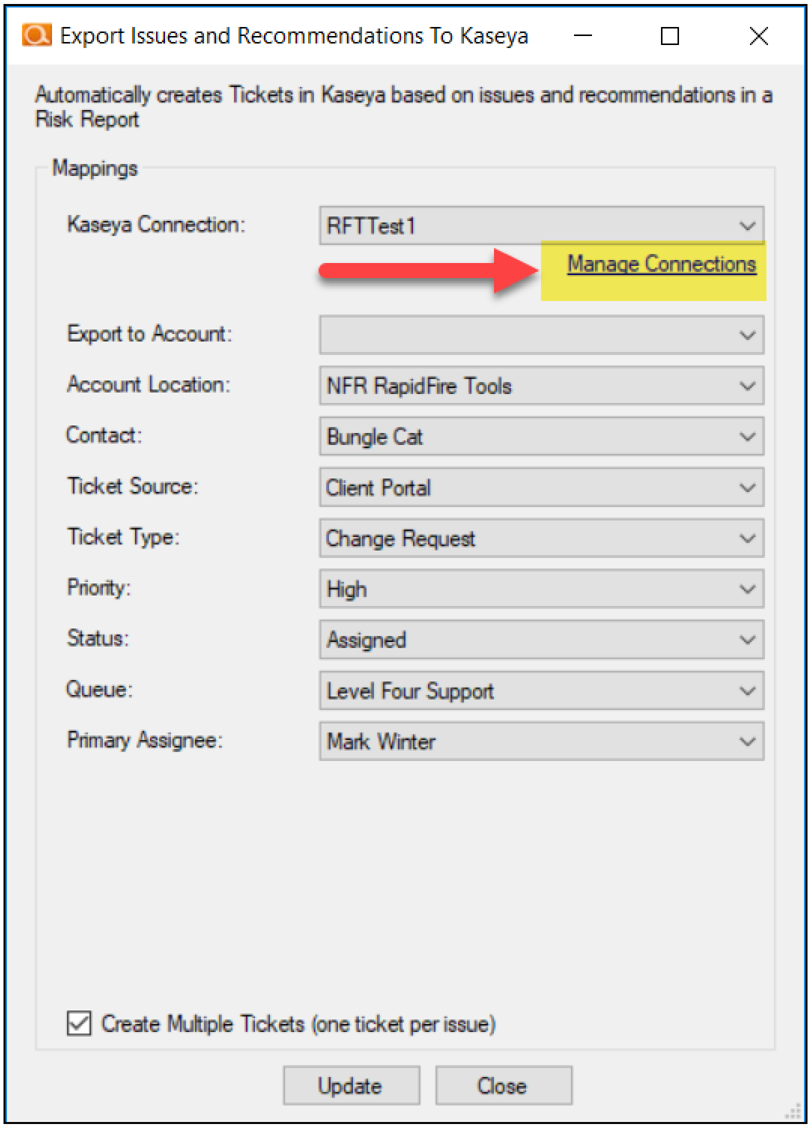


Create Ticket from...

Select Target

8. The Export Issues window will appear. Click **Manage Connections**.

© 2021 RapidFire Tools, Inc. All rights reserved.



Automatically creates Tickets in Kaseya based on issues and recommendations in a Risk Report

Mappings

Kaseya Connection: RFTTest1

Export to Account:

Account Location: NFR RapidFire Tools

Contact: Bungle Cat

Ticket Source: Client Portal

Ticket Type: Change Request

Priority: High

Status: Assigned

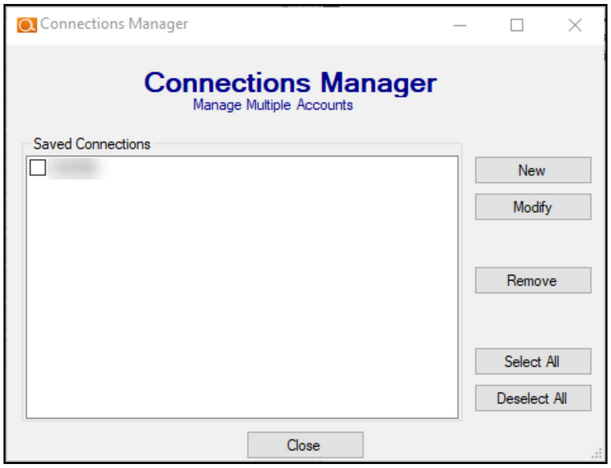
Queue: Level Four Support

Primary Assignee: Mark Winter

☑ Create Multiple Tickets (one ticket per issue)

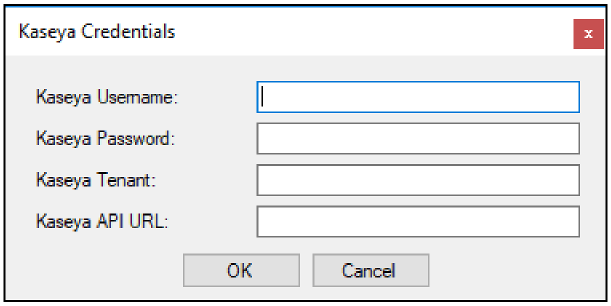
The Connections Manager window will be displayed.

© 2021 RapidFire Tools, Inc. All rights reserved.



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

   The PSA Credentials window will be displayed

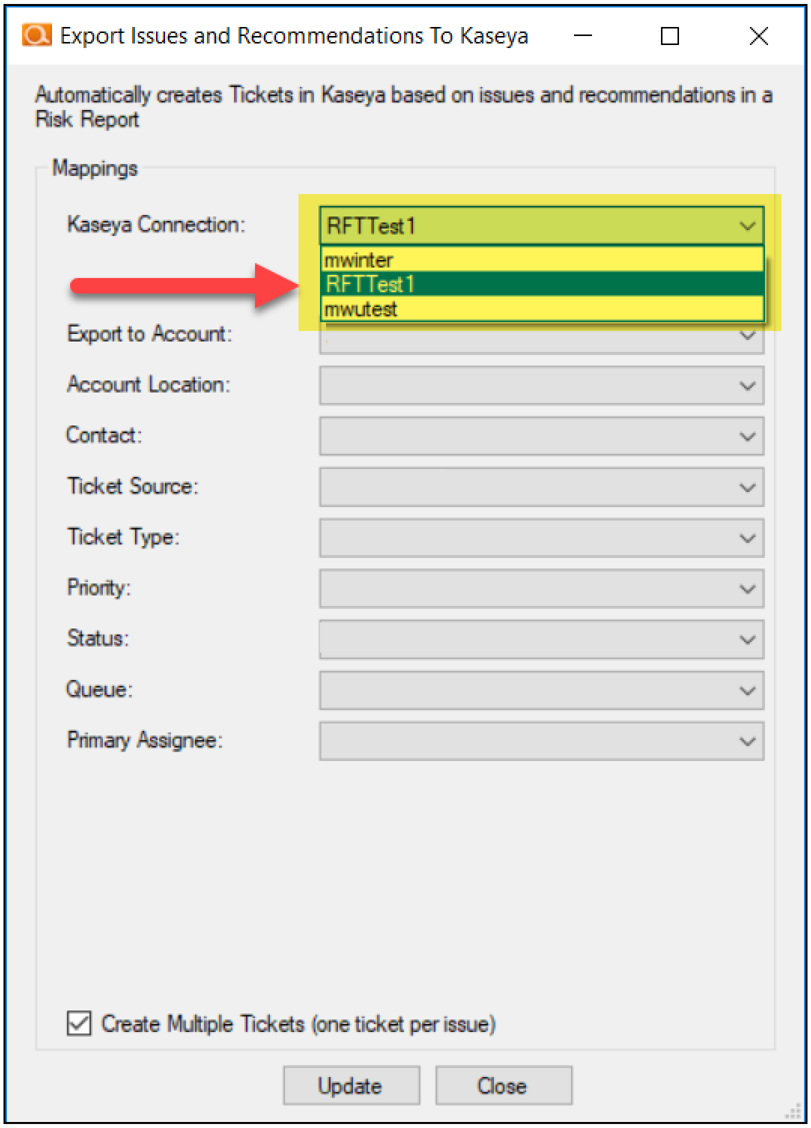


10. Enter the credentials for your chosen PSA.
11. Click **OK**.

    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.

12. Click **Close** to dismiss the Connection Manager.
13. From the Export screen, verify the connection by selecting it from the drop-down menu.



Export Issues and Recommendations To Kaseya

Automatically creates Tickets in Kaseya based on issues and recommendations in a Risk Report

Mappings

Kaseya Connection: RFTTest1

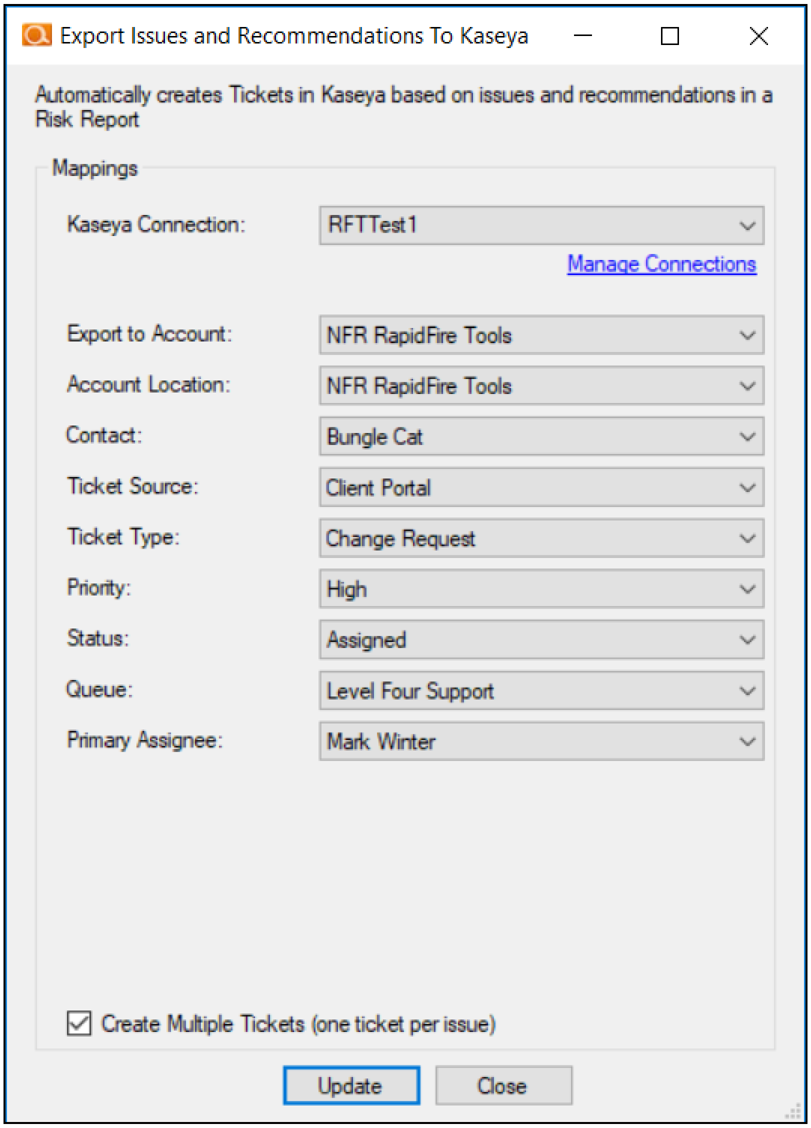
☑ Create Multiple Tickets (one ticket per issue)

Note: If the connection is successful, some of the Mappings fields should automatically populate with values from the PSA system.

14. Proceed to export information to your PSA. Refer to the instructions below.

Note: When the Connection between Network Detective and the PSA is established, some of the fields in the Mapping menu will automatically populate. This may take up to 60 seconds.

© 2021 RapidFire Tools, Inc. All rights reserved.



Automatically creates Tickets in Kaseya based on issues and recommendations in a Risk Report

Mappings

Kaseya Connection:	RFTTest1
Export to Account:	NFR RapidFire Tools
Account Location:	NFR RapidFire Tools
Contact:	Bungle Cat
Ticket Source:	Client Portal
Ticket Type:	Change Request
Priority:	High
Status:	Assigned
Queue:	Level Four Support
Primary Assignee:	Mark Winter

☑ Create Multiple Tickets (one ticket per issue)

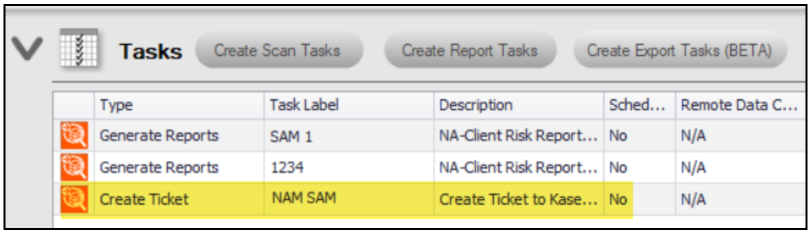
15. Map the issues to service ticket fields in your PSA. These mappings allow you to configure how the issues in Network Detective are created as tickets in your PSA.

    Important: You configure the values for the mapping fields in your PSA system. Ensure the values are correctly configured in your PSA before continuing.

16. When you are finished, click Update.

    The Export Task will appear in the tasks list.

© 2021 RapidFire Tools, Inc. All rights reserved.

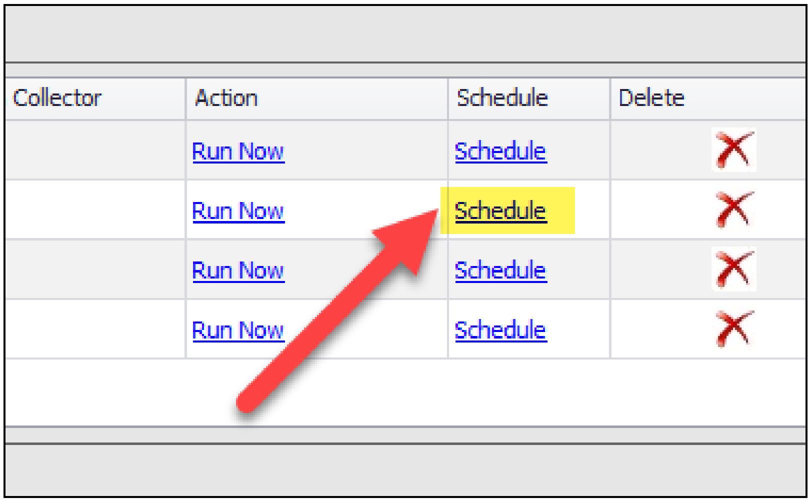


Type	Task Label	Description	Sched...	Remote Data C...
Generate Reports	SAM 1	NA-Client Risk Report...	No	N/A
Generate Reports	1234	NA-Client Risk Report...	No	N/A
Create Ticket	NAM SAM	Create Ticket to Kase...	No	N/A

Next, you must schedule the task to export.

Step 3 — Schedule/Run Export Task

1. Next to the Export Task, click on **Schedule** link to open the **CRON Builder** window. The **CRON Builder** is used to schedule the running of your Reporter task.

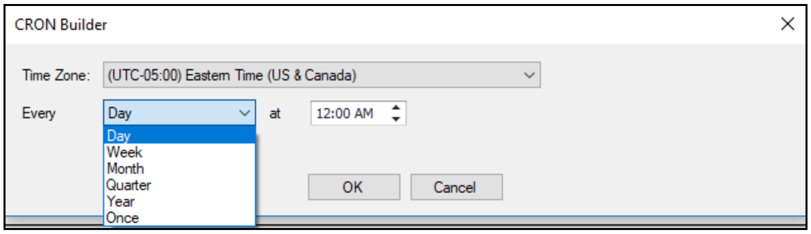


Collector	Action	Schedule	Delete
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗
	Run Now	Schedule	✗

Exports can be set to run **daily**, **weekly**, **monthly**, **quarterly**, **annually**, or **just once**. You may also set the time of the day that the scan should be initiated.

Note: Please note that the time zone used for the CRON Builder time is Eastern Standard Time (EST).

© 2021 RapidFire Tools, Inc. All rights reserved.



Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

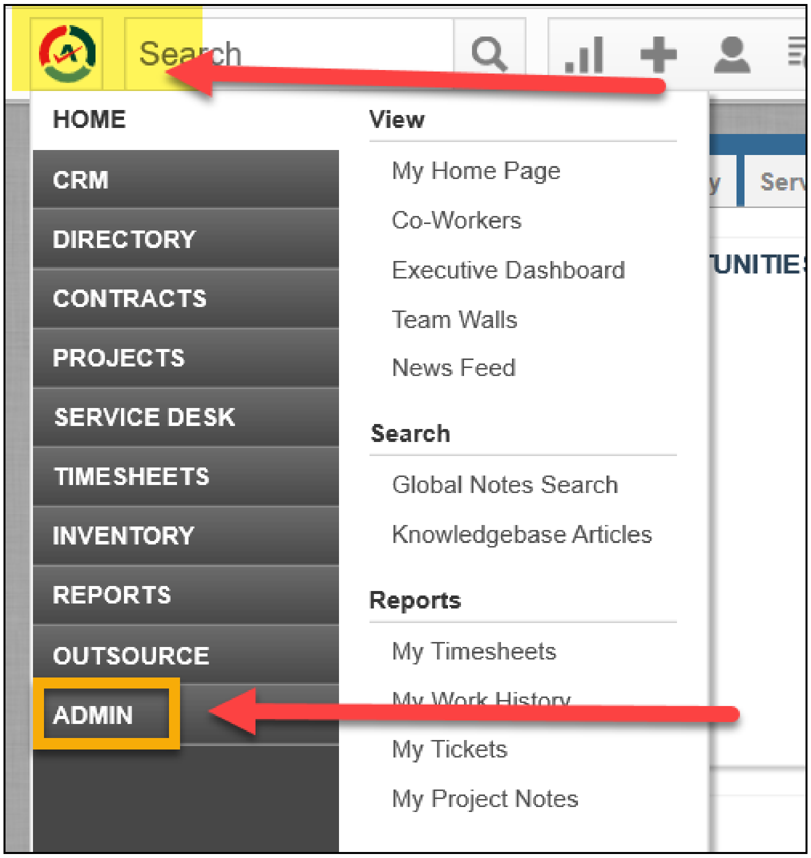
2. Set the export frequency by selecting one option from **Every** list (i.e. day, week, month, year, or once)
3. Next set the "**on the**" by selecting a day that the export should be performed.
4. Then set the time of the day that the export should run by setting the "**at**" time.
5. Click **OK** to save the Export task. It will run at the specified time and export items into your chosen PSA system.

© 2021 RapidFire Tools, Inc. All rights reserved.

Set Up Autotask Integration

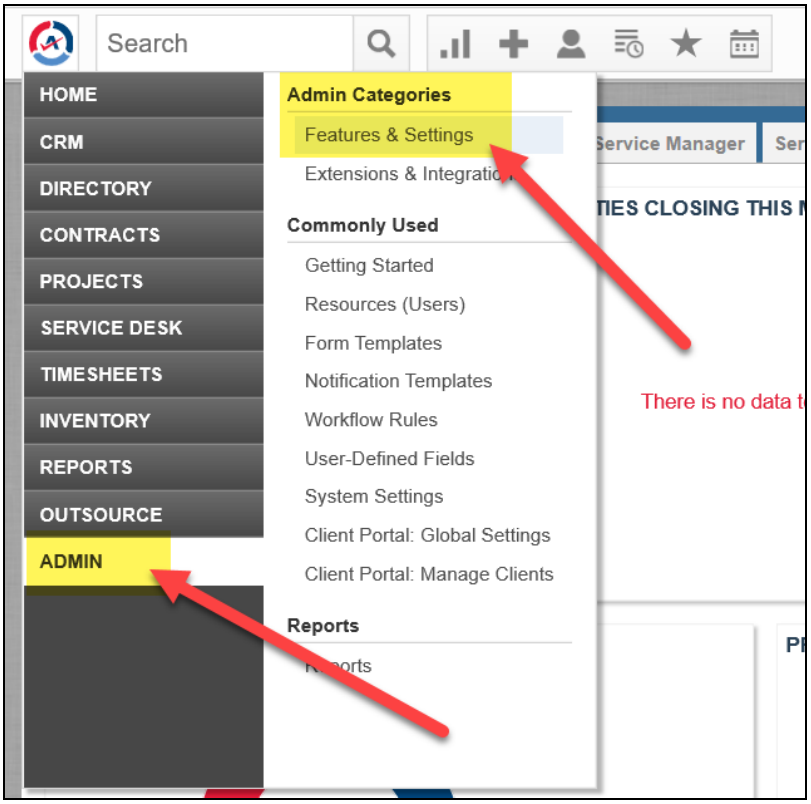
To set up a connection with the Autotask system, you will need to **create an API User in Autotask**. To do this:

1. Log in to Autotask with your admin user credentials.
2. Click on the **Autotask home** button on the left, then click **Admin**.

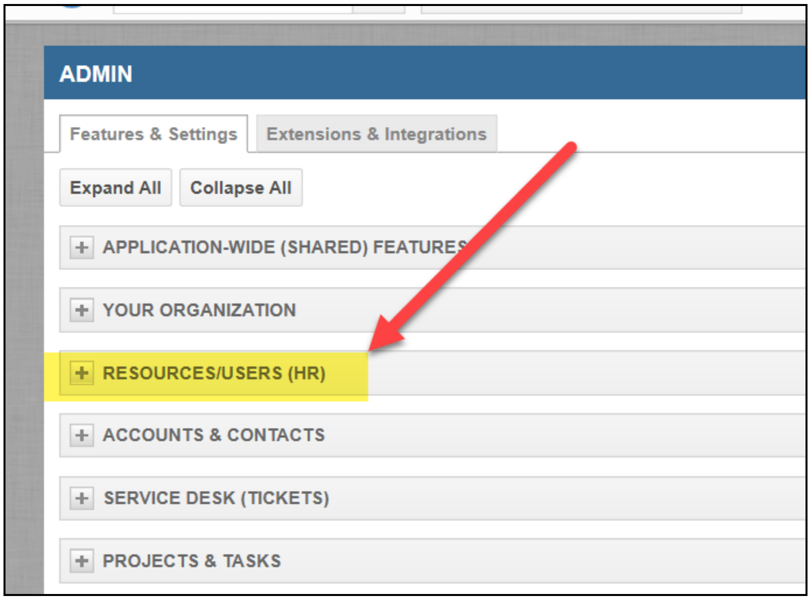


3. From the Admin menu, click **Features & Settings**.

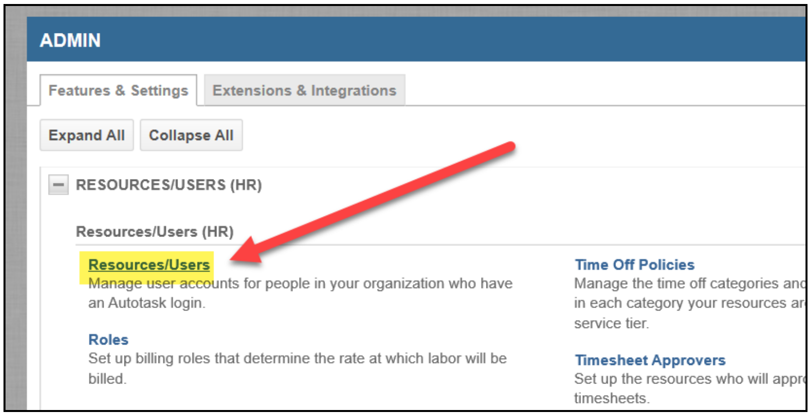
© 2021 RapidFire Tools, Inc. All rights reserved.



4. Next click **Resources/Users (HR)** from the Features & Settings menu.



5. Click **Resources/Users**.



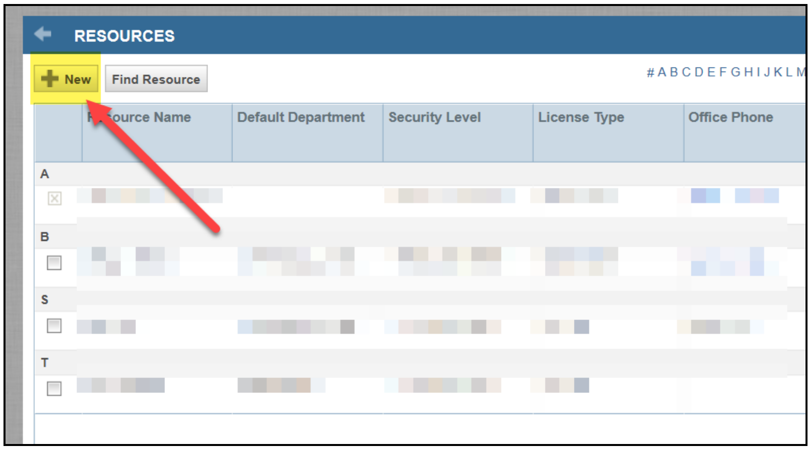
Resources/Users
Manage user accounts for people in your organization who have an Autotask login.

Roles
Set up billing roles that determine the rate at which labor will be billed.

Time Off Policies
Manage the time off categories and in each category your resources ar service tier.

Timesheet Approvers
Set up the resources who will appr timesheets.

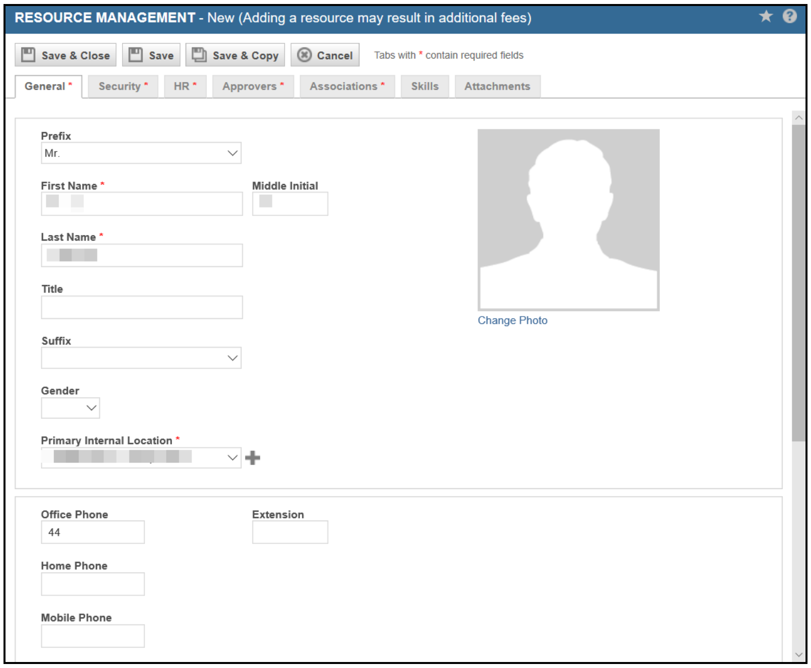
6. Click **New** to begin creating a new API user.



Resource Name	Default Department	Security Level	License Type	Office Phone

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

© 2021 RapidFire Tools, Inc. All rights reserved.



RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees)

Prefix: Mr.

First Name *: [redacted]

Middle Initial: [redacted]

Last Name *: [redacted]

Title

Suffix

Gender

Primary Internal Location *: [redacted]

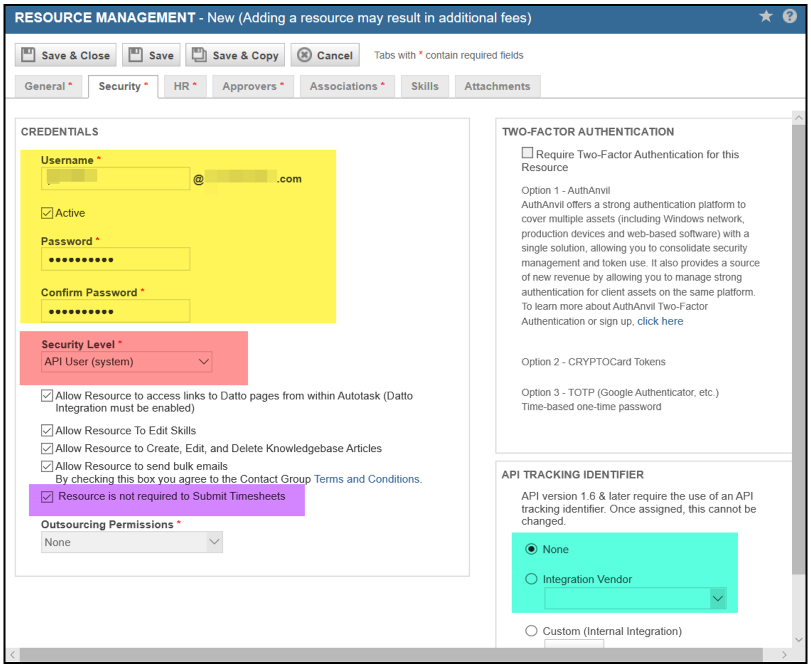
Office Phone: 44

Extension

Home Phone

Mobile Phone

8. On the **Security** tab, enter the user credentials and save these for use later.



RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees)

CREDENTIALS

Username *: [redacted] @[redacted].com

☑ Active

Password *: ••••••••••

Confirm Password *: ••••••••••

Security Level *: API User (system)

☑ Allow Resource to access links to Datto pages from within Autotask (Datto Integration must be enabled)

☑ Allow Resource To Edit Skills

☑ Allow Resource to Create, Edit, and Delete Knowledgebase Articles

☑ Allow Resource to send bulk emails
By checking this box you agree to the Contact Group Terms and Conditions.

☑ Resource is not required to Submit Timesheets

Outsourcing Permissions *: None

TWO-FACTOR AUTHENTICATION

☐ Require Two-Factor Authentication for this Resource

Option 1 - AuthAnvil
AuthAnvil offers a strong authentication platform to cover multiple assets (including Windows network, production devices and web-based software) with a single solution, allowing you to consolidate security management and token use. It also provides a source of new revenue by allowing you to manage strong authentication for client assets on the same platform. To learn more about AuthAnvil Two-Factor Authentication or sign up, click here

Option 2 - CRYPTOCard Tokens

Option 3 - TOTP (Google Authenticator, etc.)
Time-based one-time password

API TRACKING IDENTIFIER

API version 1.6 & later require the use of an API tracking identifier. Once assigned, this cannot be changed.

● None

○ Integration Vendor

○ Custom (Internal Integration)

9. While still on the Security tab, you must also:

    a. Select **API User** from the **Security Level** drop-down menu (pictured above)

    b. Select **None** under **API Tracking Identifier**.

© 2021 RapidFire Tools, Inc. All rights reserved.

    c. You can also optionally select **Resource is not required to Submit Timesheets**.

10. Complete any remaining prompts required by Autotask to create the user or to comply with your company's user and security policies.
11. When you are finished, click **Save & Close**. The new user will appear in the list.

© 2021 RapidFire Tools, Inc. All rights reserved.

Set Up ConnectWise REST Integration

To set up a connection to ConnectWise Ticketing system using the REST API you will be required to:

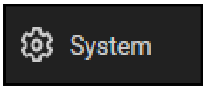
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

To enable the integration, you will need to use the ConnectWise Manage Internet Client application. Download and install the app from http://university.connectwise.com/install/. Then log in using your credentials.

If you are using the ConnectWise Manage web app, you can continue to use the web app after you have completed the steps in this guide and enabled the integration.

Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with

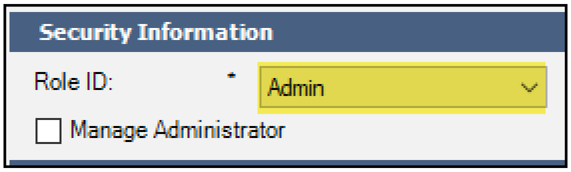
1. From the ConnectWise dashboard, click **System** from the side menu.



2. Next, click **Members**.
3. Click on **API Members Tab**. The API Members screen will appear.

   Note that the API Members Tab may not show by default and may need to be added. You can add this tab from the Tab Configuration menu on the Members page ⚙.

4. Click on the + button to create a new API Member. Fill in all required information.
5. Confirm that the API Member has been assigned Admin rights by checking the member’s Role ID under Security Information.



Security Information

Role ID: * Admin

□ Manage Administrator

© 2021 RapidFire Tools, Inc. All rights reserved.

Important: By default, the API Member must have **Admin** rights for the integration to function correctly. However, we provide a "least privilege" custom solution for the API Member Role ID below. See "Create Minimum Permissions Security Role for API Member" below.

Create Minimum Permissions Security Role for API Member

If you do not wish to assign the API member full Admin rights, create this custom security role and assign it to the API member:

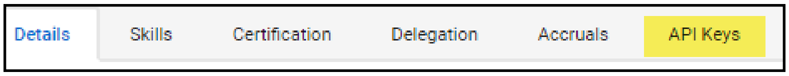
1. Go to **System** > **Security Roles**.
2. Click the + button to create a new security role.
3. Set the permissions for the Role as detailed in the table below and click **Save**.
4. Assign this custom Security Role to the API Member instead of full Admin.

Module		Add Level	Edit Level	Delete Level	Inquire Level
Companies					
	Company Maintenance				All
	Configurations	All	All		All
	Contacts	All	All		All
Service Desk					
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup	All			All
	Customized Table Setup: Allow Company / Configuration, Opportunities / Opportunity Status, Opportunities / Opportunity Type				

© 2021 RapidFire Tools, Inc. All rights reserved.

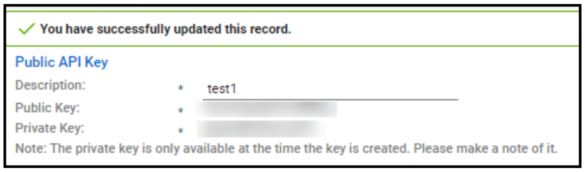
Step 3 — Create an API Key in the ConnectWise Ticketing System

1. Select the API Member that you created previously.
2. From the API Member details screen, click **API Keys**.



3. Click the + button.
4. Enter a **Description** for the API Key.
5. Click **Save**. 💾
6. The newly generated API Key will appear.
7. Write down or take a screen shot of the Member's Public and Private API Key strings. This information will be required to set up the integration with ConnectWise.

Important: Note that the Private Key is only available at the time the key is created. Be sure to copy the keys for your records.



✓ You have successfully updated this record.

Public API Key

Description: * test1

Public Key: * [redacted]

Private Key: * [redacted]

Note: The private key is only available at the time the key is created. Please make a note of it.

Step 4 — Configure Service Tables in ConnectWise

In order to export issues as tickets in ConnectWise, you will need to configure several **Service Tables** in ConnectWise. These tables ensure that the issues are "mapped" correctly to the tickets created within ConnectWise. You must configure the Service Tables correctly in order to establish the connection with ConnectWise.

You can configure the Service Tables in ConnectWise from **System>Setup Tables>Category>Service**. Configure the Service Tables as detailed below:

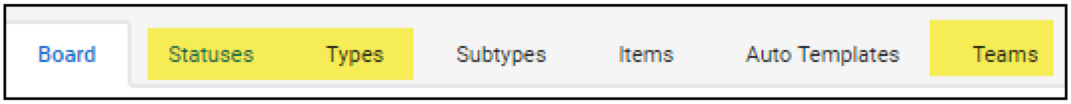
1. **Service Board**

© 2021 RapidFire Tools, Inc. All rights reserved.

You must have a Service Board created within ConnectWise. In addition, within the Service Board, you must create values for the following fields. You can create values for these fields from the Service Board page:

a. **Statuses**
b. **Types**
c. **Teams**

You must create at least one value for each of these fields.



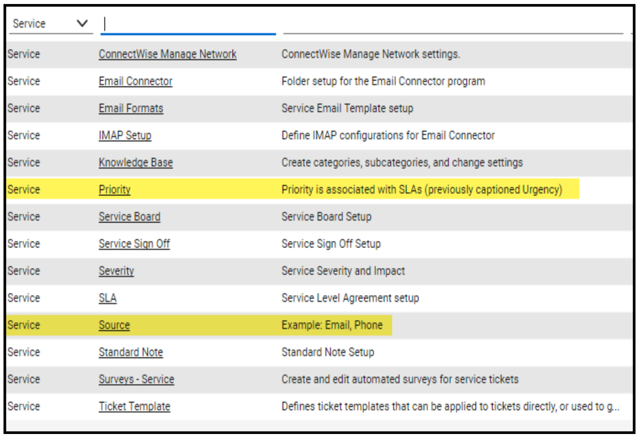
In addition, you must define values for two additional Service Tables:

2. **Source**

   You must include at least one Source.

3. **Priority**

   You must include at least one Priority level.



Service		
Service	ConnectWise Manage Network	ConnectWise Manage Network settings.
Service	Email Connector	Folder setup for the Email Connector program
Service	Email Formats	Service Email Template setup
Service	IMAP Setup	Define IMAP configurations for Email Connector
Service	Knowledge Base	Create categories, subcategories, and change settings
Service	Priority	Priority is associated with SLAs (previously captioned Urgency)
Service	Service Board	Service Board Setup
Service	Service Sign Off	Service Sign Off Setup
Service	Severity	Service Severity and Impact
Service	SLA	Service Level Agreement setup
Service	Source	Example: Email, Phone
Service	Standard Note	Standard Note Setup
Service	Surveys - Service	Create and edit automated surveys for service tickets
Service	Ticket Template	Defines ticket templates that can be applied to tickets directly, or used to g...

If your existing Service Tables already contain values for the fields listed above, you do not need to create new values.

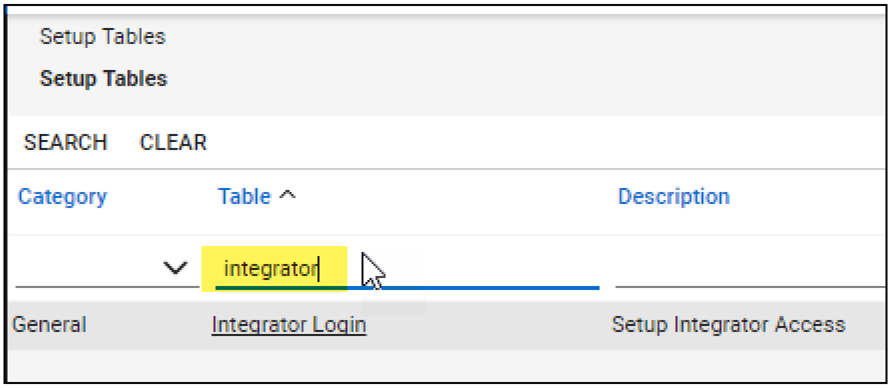
Set Up ConnectWise SOAP Integration

This topic covers how to integrate Network Detective with ConnectWise via the ConnectWise SOAP API.

Important: The ConnectWise SOAP API is in the process of being deprecated by ConnectWise. We recommend that you use the ConnectWise REST API instead.

To set up the ConnectWise SOAP integration:

1. Navigate to **System**-> **Setup Tables**.
2. Type "**Integrator**" into the Table lookup and hit Enter.
3. Click the **Integrator Login** link.



Setup Tables

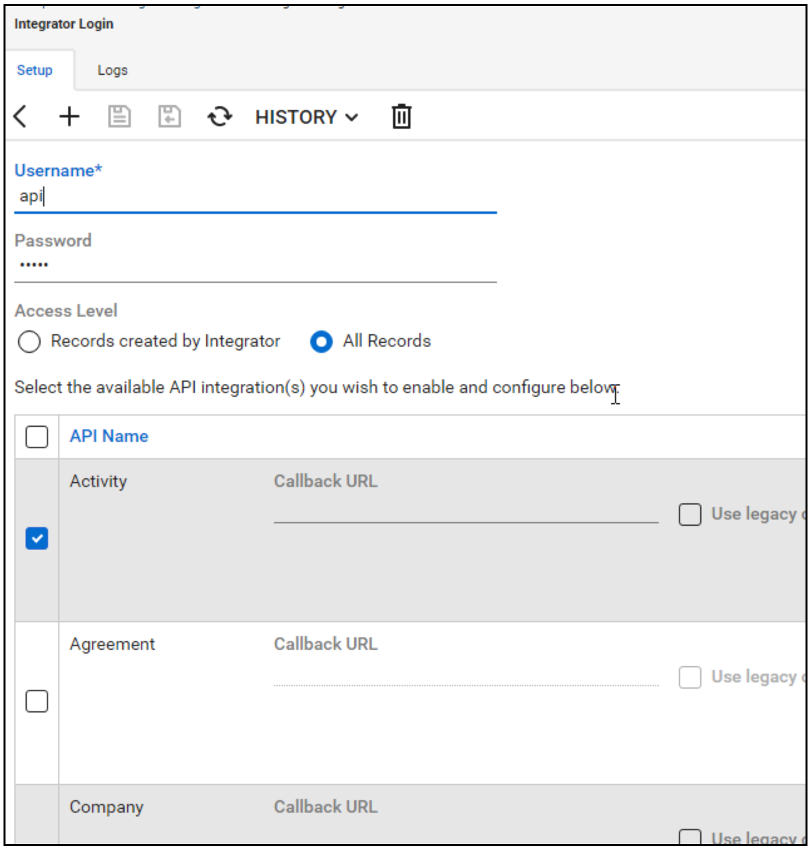
Setup Tables

Category	Table ^	Description
	integrator	
General	Integrator Login	Setup Integrator Access

4. Click the "**New**" Icon to bring up the New Integrator login screen as shown on the right.
5. Enter and record **Username** and **Password** values which you will need later on when creating a connection in Network Detective.
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

© 2021 RapidFire Tools, Inc. All rights reserved.

- MemberApi
- ReportingApi
- SystemApi
- ConfigurationApi



Username* api

Password •••••

Access Level
○ Records created by Integrator ● All Records

Select the available API integration(s) you wish to enable and configure below

□	API Name		
☑	Activity	Callback URL	□ Use legacy
□	Agreement	Callback URL	□ Use legacy
	Company	Callback URL	□ Use legacy

8. Click the **Save** icon to save this Integrator Login.

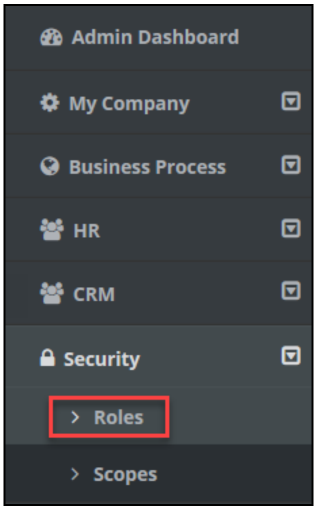
> **Note:** If you already have an Integrator Login configured, you may use it as long as the Company and Configuration APIs are enabled.)

© 2021 RapidFire Tools, Inc. All rights reserved.

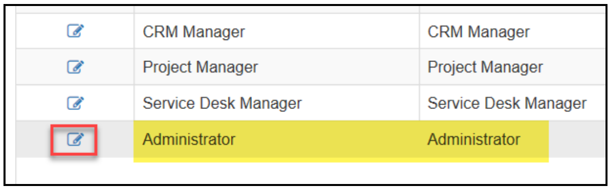
Set Up Kaseya BMS Integration

To export items to Kaseya BMS, you will need Administrator credentials in Kaseya BMS. To assign a Kaseya user to the Administrator role, follow these steps:

1. Log in to Kaseya BMS.
2. Go to **Security** > **Roles**.

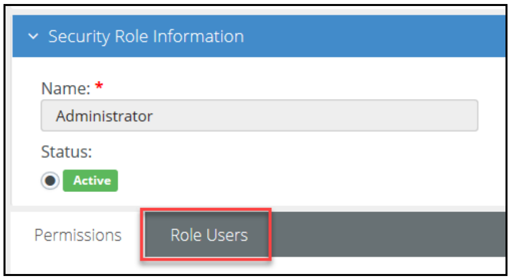


3. Click **Open/Edit** on the Administrator Role.



✎	CRM Manager	CRM Manager
✎	Project Manager	Project Manager
✎	Service Desk Manager	Service Desk Manager
✎	Administrator	Administrator

4. Click the **Role Users** tab.



Name: *
Administrator
Status:
● Active

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.

© 2021 RapidFire Tools, Inc. All rights reserved.

Set Up Network Detective to IT Glue Integration

This topic covers how to integrate Reporter with IT Glue, the Kaseya IT documentation product. This integration uses Reporter to discover assets, computers, servers, applications, and services such as Active Directory, DNS, DHCP, and more. Once you export this data to IT Glue, the IT Glue system automatically builds the relationships between these assets. This provides you with great visibility of the site's IT environment.

Important: This is a powerful integration that can create thousands of assets in IT Glue. We highly recommend that you review your settings carefully as the data created cannot be mass deleted. This integration has unique matching criteria to prevent duplicates. Please review the Matching Criteria for Configurations section of IT Glue's integration documentation to prevent duplication of data.

There are several **prerequisites needed** before you can create a **Reporter Export Task** to IT Glue:

- Partners must be **subscribed to the IT Glue Enterprise Plan** as the integration requires the IT Glue API.
- You must have the **Network Detective application** installed
- You must have a **Reporter scan server** installed on your MSP Network. (See "Initial Reporter Set Up" on page 16)
- You must have a **Remote Data Collector** (and its associated **Client-Connector**) set up with a Reporter Site configured to perform regular scan tasks. (See "Initial Remote Data Collector Set Up" on page 21 and "Configure Remote Data Collector to Perform Scan Tasks" on page 30)

  Note: See "Setting Up Reporter" on page 16 for detailed instructions on installing and configuring Reporter.

  Important: Currently, you can only export configuration items for Active Directory environments, and NOT Workgroups.

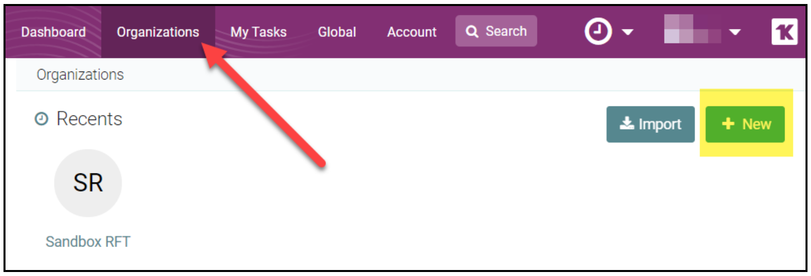
Once these prerequisites are met, you can then:

Create Organization and API Key in IT Glue

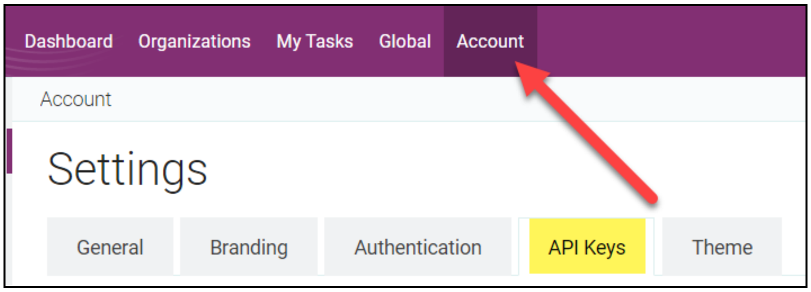
1. Create one or more **Organizations** in IT Glue. You will later select these to receive the exported data from Reporter. You create new Organizations from the

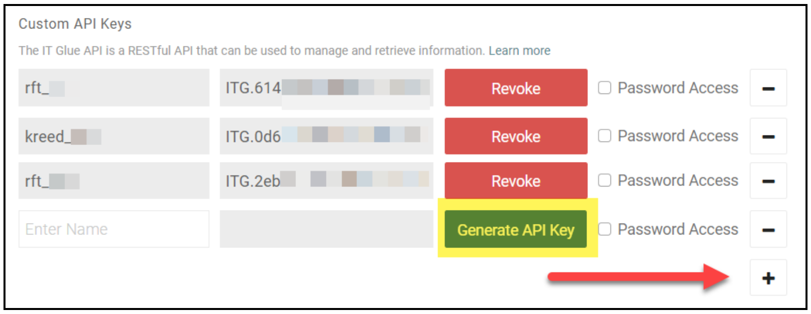
© 2021 RapidFire Tools, Inc. All rights reserved.

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 API that can be used to manage and retrieve information. Learn more

rft_[redacted]	ITG.614[redacted]	Revoke	□ Password Access	−
kreed_[redacted]	ITG.0d6[redacted]	Revoke	□ Password Access	−
rft_[redacted]	ITG.2eb[redacted]	Revoke	□ Password Access	−
Enter Name		Generate API Key	□ Password Access	−
				+

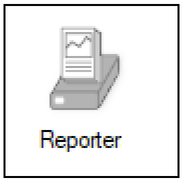
Important: For your reference, save a copy of the API key outside of IT Glue.

You can then use the instructions below to create a **Reporter Export Task** to IT Glue in the **Network Detective** application.

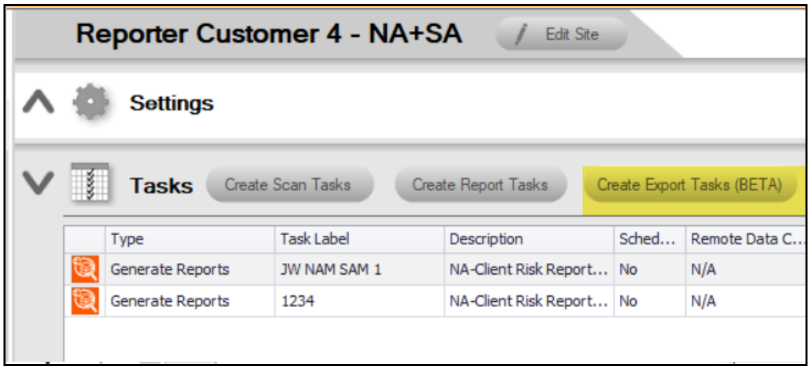
Create a Reporter Export Task to IT Glue

To set up a connection between the Network Detective application and IT Glue, you will:

1. In the **Network Detective** app, open the **Site** used to manage the Reporter. Click on the **Reporter icon** on the bottom left side of the Site screen.

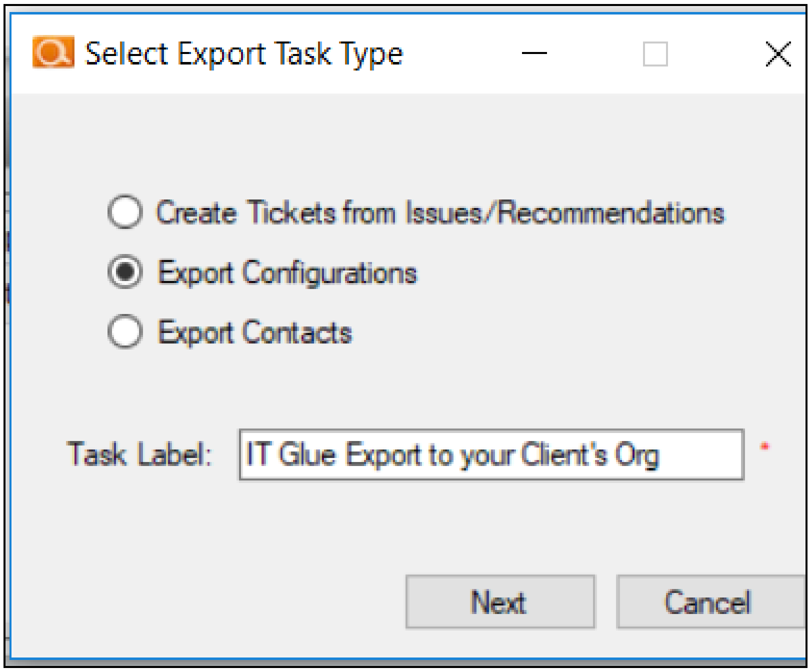


2. Click **Create Export Tasks**.



Type	Task Label	Description	Sched…	Remote Data C…
Generate Reports	JW NAM SAM 1	NA-Client Risk Report…	No	N/A
Generate Reports	1234	NA-Client Risk Report…	No	N/A

3. The Select Export Task Type window is displayed. Select the **Export Configuration** option and assign a **Task Label**.



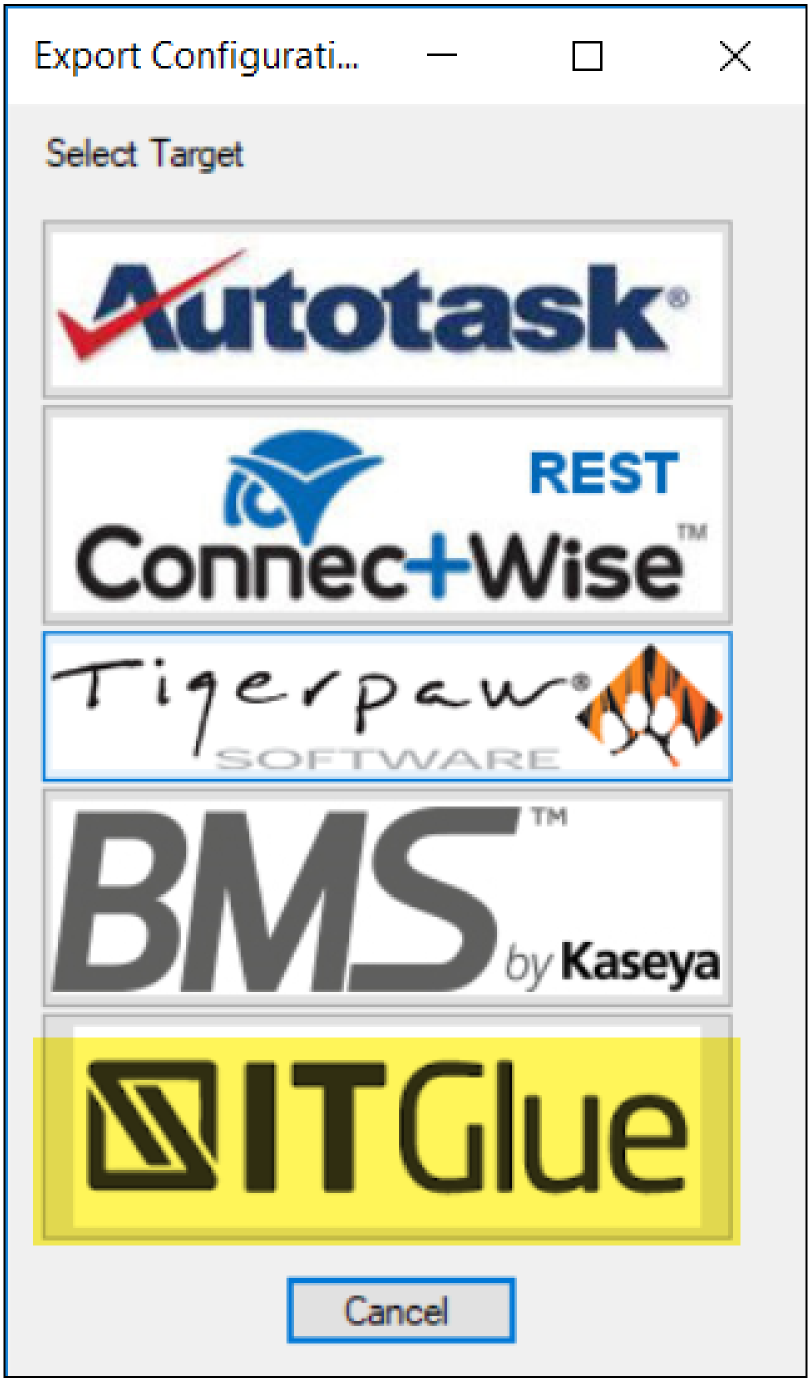
○ Create Tickets from Issues/Recommendations

● Export Configurations

○ Export Contacts

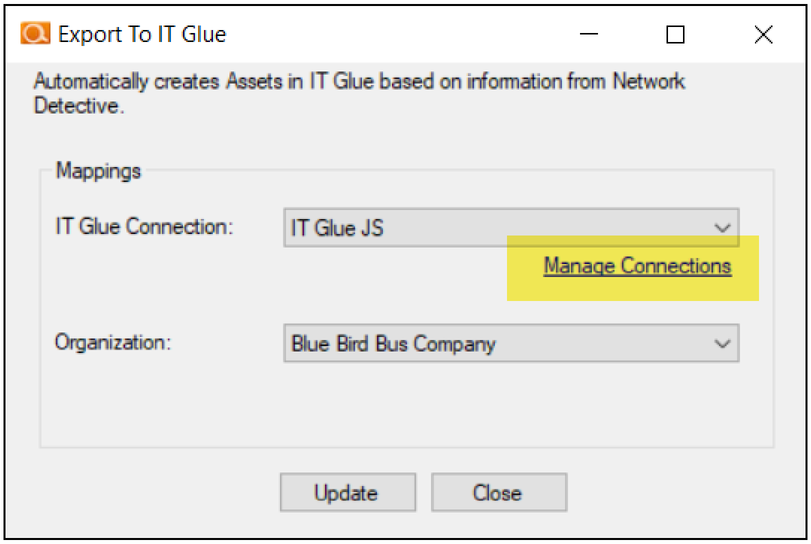
Task Label: IT Glue Export to your Client's Org *

4. Click **Next**. Select **IT Glue** from the available integrations.



5. Next, select the IT Glue **Mapping** and **Organization**. First, click **Manage Connections**.

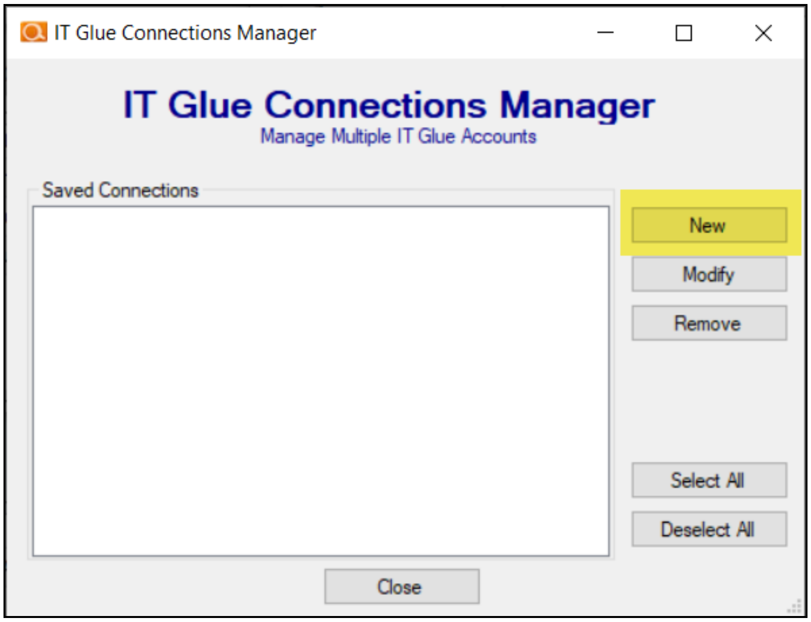
© 2021 RapidFire Tools, Inc. All rights reserved.



Export To IT Glue

Automatically creates Assets in IT Glue based on information from Network Detective.

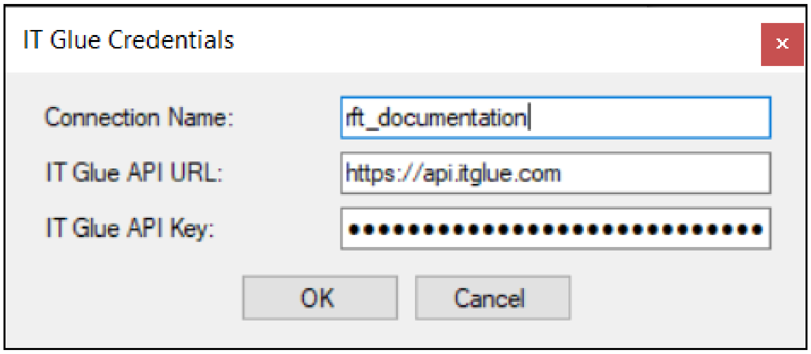
6. Click **New**.



IT Glue Connections Manager

7. Enter a **Connection Name**. Then enter your **IT Glue API** credentials. Click **OK**.

© 2021 RapidFire Tools, Inc. All rights reserved.



IT Glue Credentials

Connection Name: rft_documentation

IT Glue API URL: https://api.itglue.com

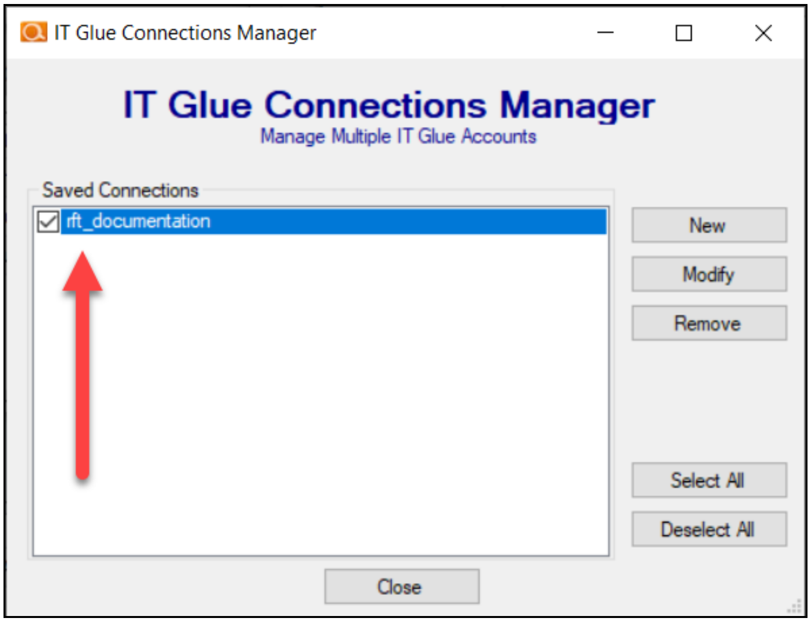
IT Glue API Key: ••••••••••••••••••••••••••••

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**

Important: The IT Glue API Key must be generated from within the ITGlue system. See "Create Organization and API Key in IT Glue" on page 199

8. The Connection will appear in the list of Saved Connections. Select the connection and click **Close**.



IT Glue Connections Manager

IT Glue Connections Manager

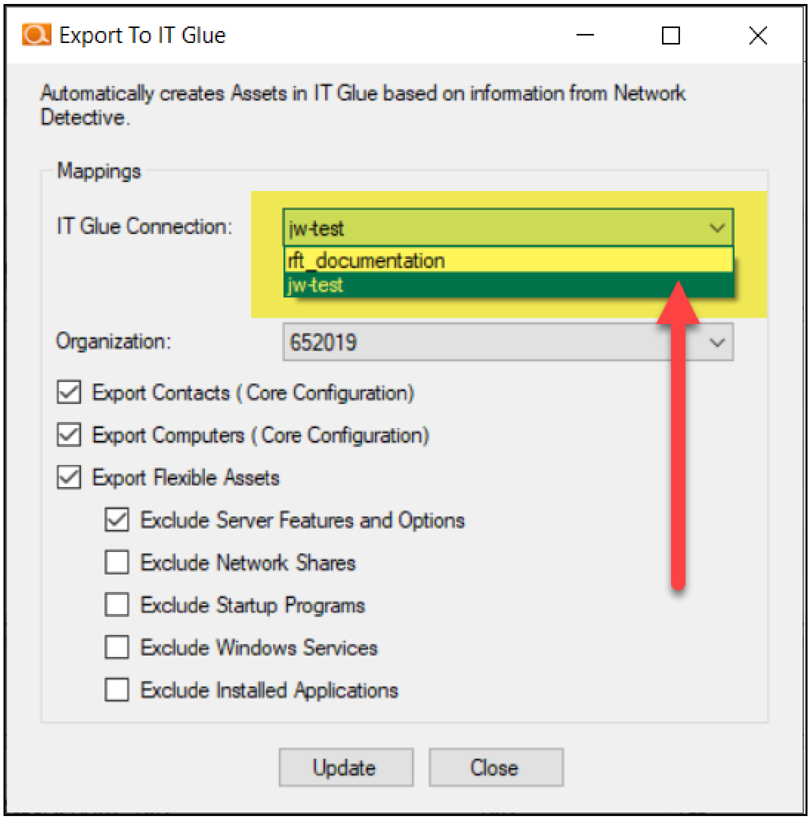
Manage Multiple IT Glue Accounts

Saved Connections

☑ rft_documentation

9. Next, select the **IT Glue Connection** from the drop-down menu.

© 2021 RapidFire Tools, Inc. All rights reserved.



Export To IT Glue

Automatically creates Assets in IT Glue based on information from Network Detective.

Mappings

IT Glue Connection: jw-test

Organization: 652019

☑ Export Contacts (Core Configuration)

☑ Export Computers (Core Configuration)

☑ Export Flexible Assets

☑ Exclude Server Features and Options

□ Exclude Network Shares

□ Exclude Startup Programs

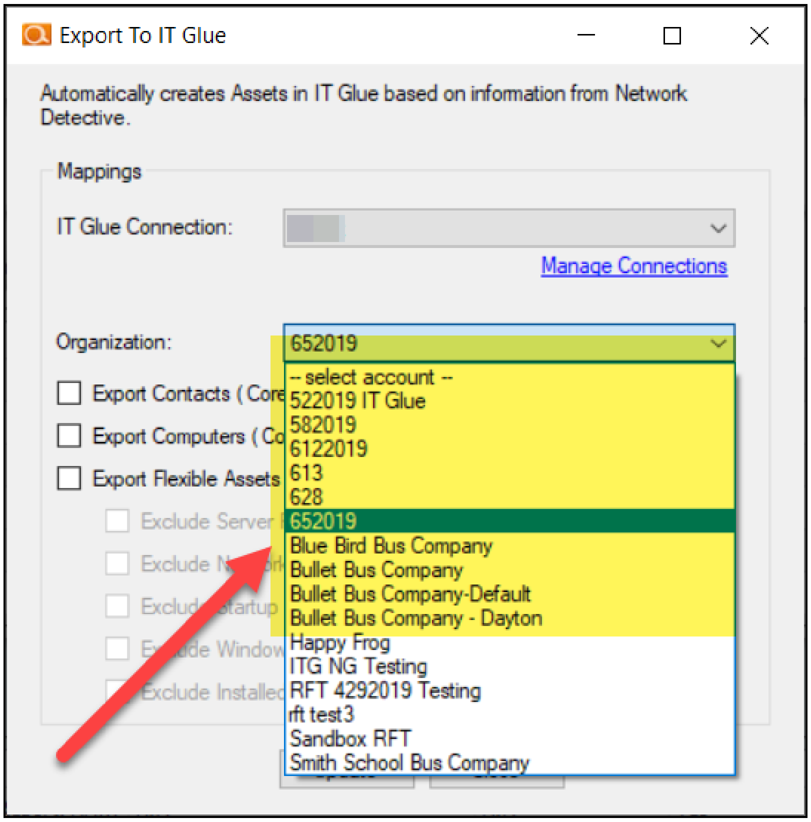
□ Exclude Windows Services

□ Exclude Installed Applications

10. Select the **Organization** to receive the exported configuration items.

> **Note:** If successful, you should see your IT Glue Organizations populate in the Organizations drop-down menu.

© 2021 RapidFire Tools, Inc. All rights reserved.



Export To IT Glue

Automatically creates Assets in IT Glue based on information from Network Detective.

Mappings

IT Glue Connection: [redacted]

Manage Connections

Organization: 652019

- -- select account --
- 522019 IT Glue
- 582019
- 6122019
- 613
- 628
- 652019
- Blue Bird Bus Company
- Bullet Bus Company
- Bullet Bus Company-Default
- Bullet Bus Company - Dayton
- Happy Frog
- ITG NG Testing
- RFT 4292019 Testing
- rft test3
- Sandbox RFT
- Smith School Bus Company

☐ Export Contacts (Core

☐ Export Computers (Co

☐ Export Flexible Assets

☐ Exclude Server

☐ Exclude N

☐ Exclude Startup

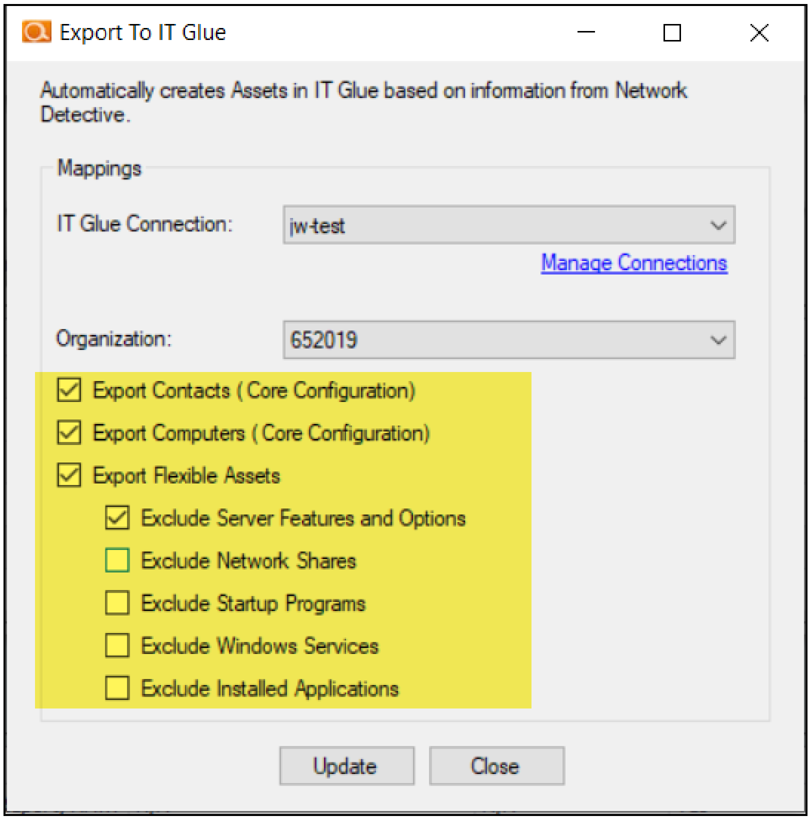
☐ Exclude Window

☐ Exclude Installed

11. Finally, select which configuration items to export.

> **Important:** Warning! If you have other integrations creating Contacts and/or Configurations in IT Glue such as a PSA and RMM, **DO NOT select the Export Contacts and Export Computers options** as they will create unwanted duplicates.
>
> We strongly recommend that you at least select the following check-boxes. These are enabled by default:
>
> - **'Exclude Server Features and Options'**
> - **'Exclude Startup Programs'**
> - **'Exclude Windows Services'**
>
> If you do not select these options, the Reporter will detect and add all of these items to IT Glue which may clutter search and navigation.

© 2021 RapidFire Tools, Inc. All rights reserved.



Export To IT Glue

Automatically creates Assets in IT Glue based on information from Network Detective.

Mappings

IT Glue Connection: jw-test

Manage Connections

Organization: 652019

☑ Export Contacts (Core Configuration)

☑ Export Computers (Core Configuration)

☑ Export Flexible Assets

☑ Exclude Server Features and Options

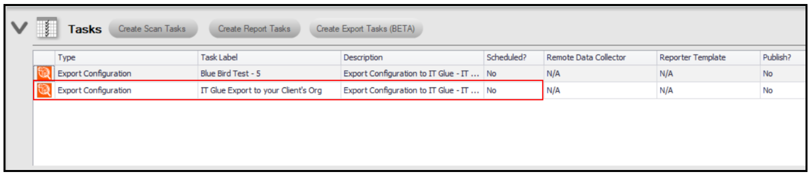
□ Exclude Network Shares

□ Exclude Startup Programs

□ Exclude Windows Services

□ Exclude Installed Applications

12. Again, **review the configuration items that you have selected to exclude** in the step above.
13. Once you set up the Connection, click **Update** to complete the creation of the task. The **Export Task** will appear in the **Tasks List**.



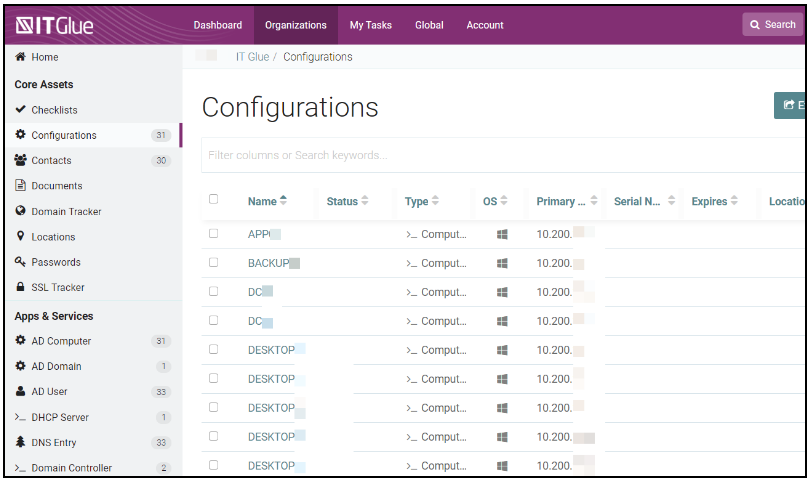
Type	Task Label	Description	Scheduled?	Remote Data Collector	Reporter Template	Publish?
Export Configuration	Blue Bird Test - 5	Export Configuration to IT Glue - IT ...	No	N/A	N/A	No
Export Configuration	IT Glue Export to your Client's Org	Export Configuration to IT Glue - IT ...	No	N/A	N/A	No

14. Click **Schedule** to run the Task at a specified time. Alternatively, click **Run Now** to run the task one time immediately.

    If the Export is successful, your Configuration items will appear in IT Glue.

Important: Note that once the export begins, it will be placed in the API queue. It may take up to **3 hours** for your results to appear in IT Glue.

© 2021 RapidFire Tools, Inc. All rights reserved.



	Name	Status	Type	OS	Primary ...	Serial N...	Expires	Locatio
□	APP		>_ Comput...	⊞	10.200.			
□	BACKUP		>_ Comput...	⊞	10.200.			
□	DC		>_ Comput...	⊞	10.200.			
□	DC		>_ Comput...	⊞	10.200.			
□	DESKTOP		>_ Comput...	⊞	10.200.			
□	DESKTOP		>_ Comput...	⊞	10.200.			
□	DESKTOP		>_ Comput...	⊞	10.200.			
□	DESKTOP		>_ Comput...	⊞	10.200.			
□	DESKTOP		>_ Comput...	⊞	10.200.			

Accessing data in IT Glue after scan and export

1. Log into your IT Glue account and navigate to the Organization main page.
2. Click on a newly updated item in the **Apps & Services** section in the left-hand menu. The Flexible Asset types are:
   - AD Domain
   - Domain Controller
   - FSMO Role
   - AD Computer
   - AD User
   - Security Group
   - Group Policy
   - DNS Entry
   - Windows Services
   - Enabled Server Feature
   - Enabled Optional Feature
   - Startup Programs
   - Non-AD Device
   - Microsoft SQL Server
   - Web Server
   - Time Server
   - Exchange Server

- DHCP Server
- Hyper-V Server
- Hyper-V Guest
- Printer (Attached)
- Printer (Networked)
- Printer (Share)
- Network Share
- Installed Application
- License key
- Missing Windows Patch

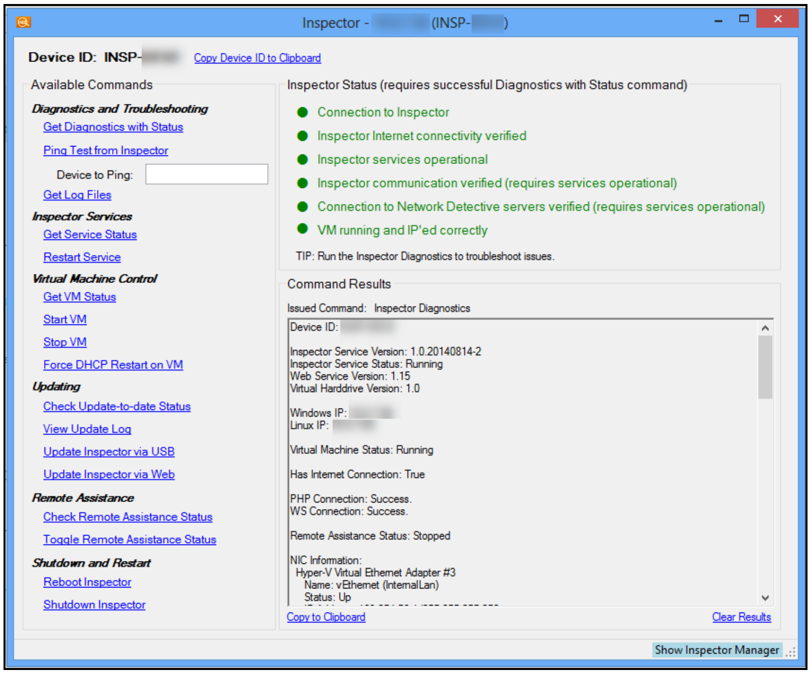
3. Open an item to see how the Reporter has automatically built relationships between the assets.
4. Active Directory users are added as IT Glue Contacts.

> **Note:** See also Matching Criteria for Configurations for more details on how the system avoids creating duplicate assets.

© 2021 RapidFire Tools, Inc. All rights reserved.

Software Appliance Diagnostic Tool

The Diagnostic Tool is used to gather relevant diagnostic information, test connectivity, manage updates, and allow remote support to the Appliance.



Device ID: INSP-[redacted]

- ● Connection to Inspector
- ● Inspector Internet connectivity verified
- ● Inspector services operational
- ● Inspector communication verified (requires services operational)
- ● Connection to Network Detective servers verified (requires services operational)
- ● VM running and IP'ed correctly

TIP: Run the Inspector Diagnostics to troubleshoot issues.

Issued Command: Inspector Diagnostics

```
Device ID: [redacted]

Inspector Service Version: 1.0.20140814-2
Inspector Service Status: Running
Web Service Version: 1.15
Virtual Harddrive Version: 1.0

Windows IP: [redacted]
Linux IP: [redacted]

Virtual Machine Status: Running

Has Internet Connection: True

PHP Connection: Success.
WS Connection: Success.

Remote Assistance Status: Stopped

NIC Information:
 Hyper-V Virtual Ethernet Adapter #3
   Name: vEthernet (InternalLan)
   Status: Up
```

Available Commands

There are a number of commands available within the Appliance Manager.

Location and Information

- *Locate Network Detective Appliance*

  Re-initialize the Appliance discovery process and attempts to retrieve the Device ID number and other diagnostic information.

- *Get Appliance Device ID*

  Display the Software Appliance's Device ID, used when associating the Software Appliance with a Site in the Network Detective Application.

Diagnostics and Troubleshooting

© 2021 RapidFire Tools, Inc. All rights reserved.

- *Appliance Diagnostics*

  Queries the Software Appliance for diagnostic information used to verify running status, software, connectivity, and NIC Information.

- *Ping Test from Appliance*

  Performs a ping test directed at a specified host or IP address from the point of view of the Software Appliance itself.

  Note: Network connectivity is required for the Appliance to operate properly.

- *Get Log Files*

  Retrieves diagnostics logs from the Appliance. Returns a link to download a .zip file containing run log information which may be used for further troubleshooting.

Service Control

- *Appliance Service Status*

  Queries the Software Appliance to return its current status. The possible statuses are as follows:

  - **Idle:** The Software Appliance is online, but performing no action.
  - **Queued:** The Software Appliance is online and performing no action. A schedule is active and queued to run.
  - **Running:** The Software Appliance is online and currently running a schedule.

- *Appliance Service Restart*

  Requests a Service Restart from the Software Appliance. Exercise caution when using this command because it may interrupt any running Scan.

Updating via USB

- *Update Appliance via USB*

  Requests the Software Appliance to update via USB. Attempts to detect a USB device. If a USB device is detected containing the necessary files is found to be connected to the Software Appliance an update will be performed.

© 2021 RapidFire Tools, Inc. All rights reserved.

> **Note:** Please ensure that a USB stick containing the update is plugged into the USB port of the system hosting the Software Appliance.

- *Check USB Update Status*

  Returns the current status of a running update. Also attempts to detect any USB device with available updates.

Remote Assistance

- *Toggle Remote Assistance Status*

  Instructs the Software Appliance to make itself available for Remote Assistance and to allow a technician to access the device for support.

- *Check Remote Assistance Status*

  Return the current status of Remote Assistance.

- *Shutdown and Restart*

  Restarts the Software Appliance.

- *Shutdown Appliance*

  Shuts down the Software Appliance.

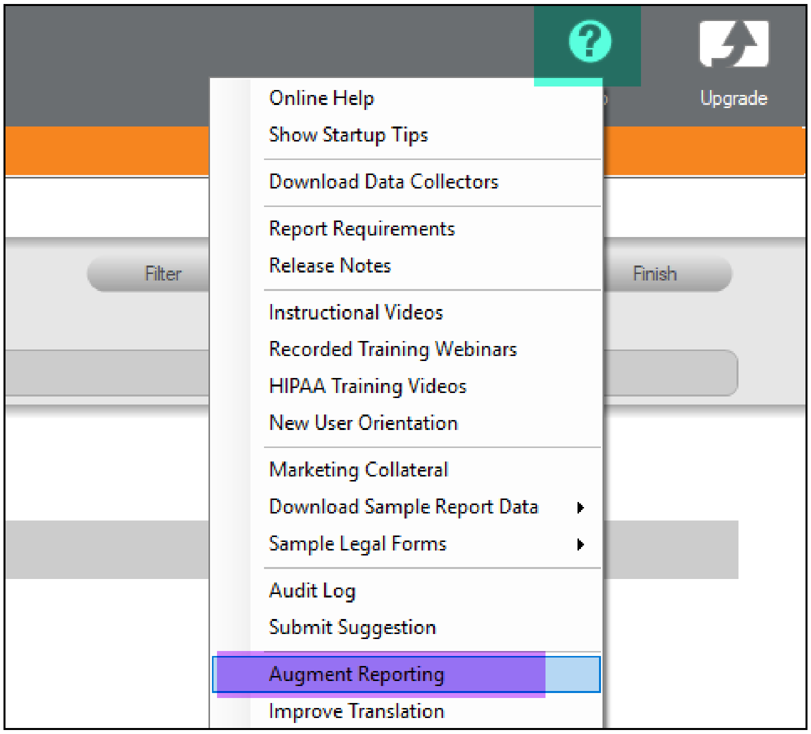
Augment Reporting to Eliminate False Positives

Occasionally, your customer may have a service installed that was not detected by Network Detective. With services such as antivirus and antispyware, new products are constantly being introduced to the market. Also, your customer may have a very old or very new release of an existing product. Since Network Detective is a very general-use product, reports may not always reflect a complete picture of your customer's unique circumstances.

The Augment Reports feature allows you to customize Network Detective's data analysis to better suit each of your customers. If a service is not listed in our database, you may add it through the Network Detective application. Then, re-generate the reports and the service will be properly included and displayed.

To augment your reports:

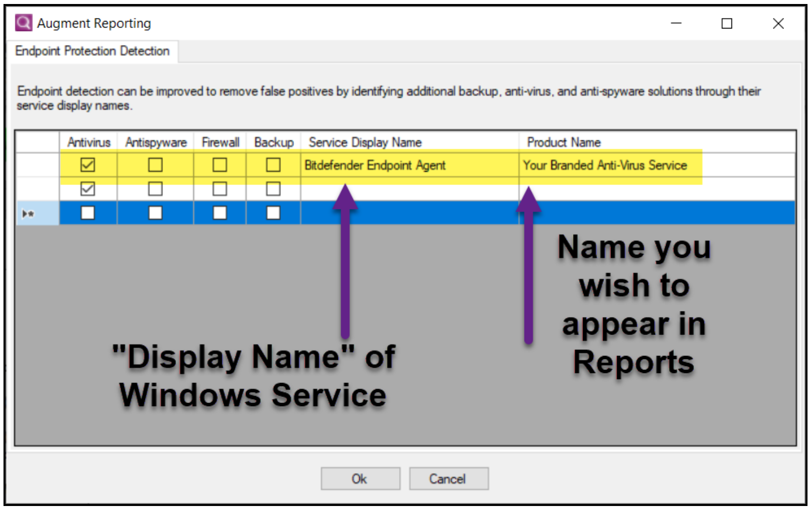
1. In Network Detective, go to **Help** > **Augment Reporting**.



   The **Endpoint Protection Detection** screen will appear.

2. For each application you wish to add to your reports, select the type of application: *Antivirus*, *Antispyware, Firewall*, and/or *Backup*.

© 2021 RapidFire Tools, Inc. All rights reserved.


Augment Reporting
Endpoint Protection Detection
Ok
Cancel
"Display Name" of Windows Service
Name you wish to appear in Reports

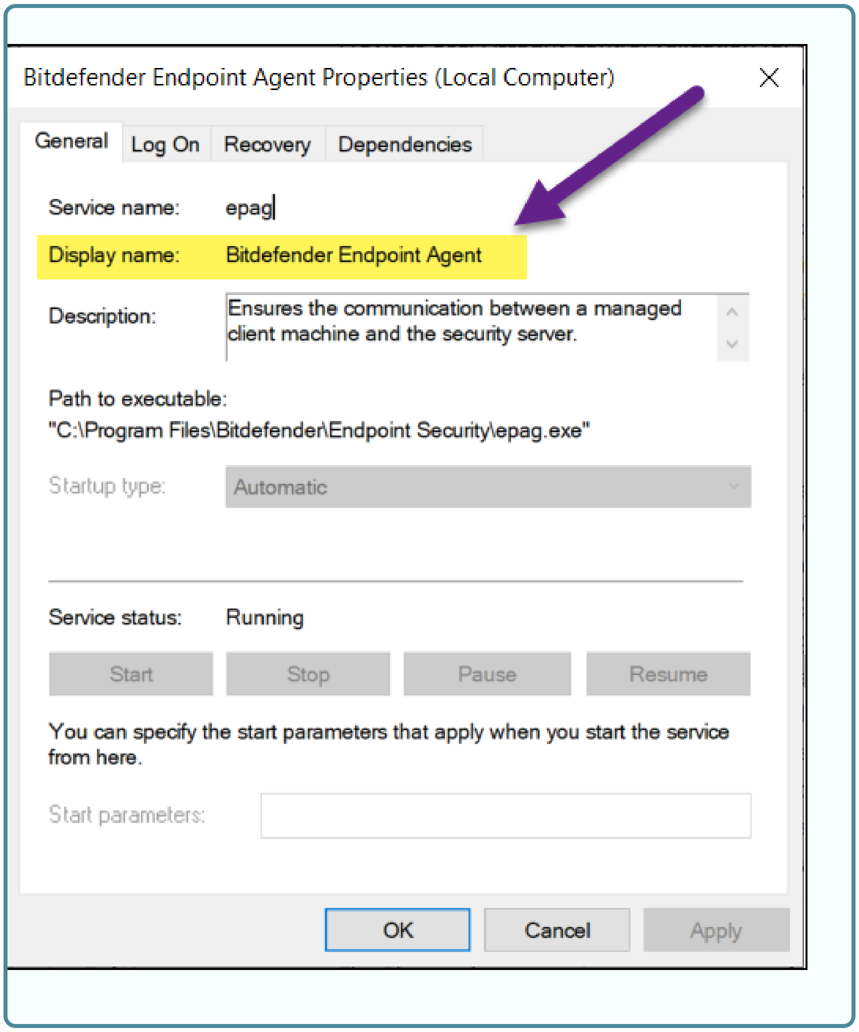
Endpoint detection can be improved to remove false positives by identifying additional backup, anti-virus, and anti-spyware solutions through their service display names.

	Antivirus	Antispyware	Firewall	Backup	Service Display Name	Product Name
	☑	☐	☐	☐	Bitdefender Endpoint Agent	Your Branded Anti-Virus Service
	☑	☐	☐	☐		
▸*	☐	☐	☐	☐		

3. Then enter the *Display Name* for the Windows Service.

> **Note:** You can find the *Display Name* by opening the Windows Services app from your desktop. **Right click** on the service and click **Properties**. See "Use the Excel Export Spreadsheet to Find Display Names" on the next page for an easy way to find display names for all Windows services.

© 2021 RapidFire Tools, Inc. All rights reserved.



Bitdefender Endpoint Agent Properties (Local Computer)

Service name: epag

Display name: Bitdefender Endpoint Agent

Description: Ensures the communication between a managed client machine and the security server.

Path to executable:
"C:\Program Files\Bitdefender\Endpoint Security\epag.exe"

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

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**.

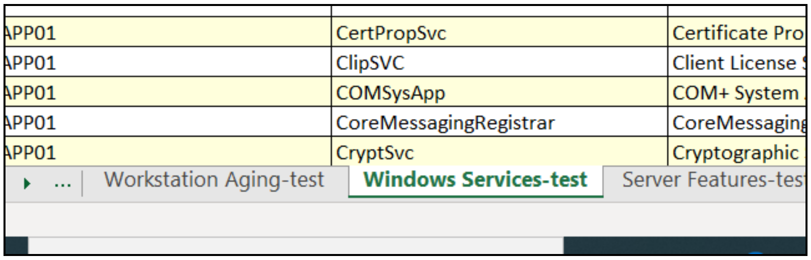
   When 1) you next collect data on the target endpoints and 2) generate reports, your new reports will feature information on the apps you included.

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.

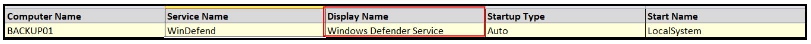
© 2021 RapidFire Tools, Inc. All rights reserved.

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

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.

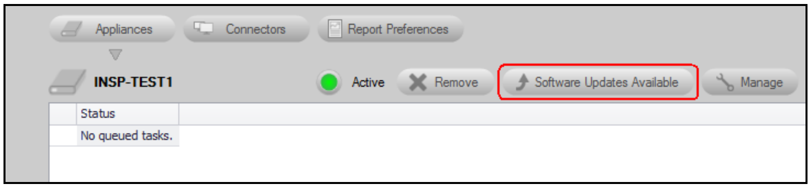


Computer Name	Service Name	Display Name	Startup Type	Start Name
BACKUP01	WinDefend	Windows Defender Service	Auto	LocalSystem

© 2021 RapidFire Tools, Inc. All rights reserved.

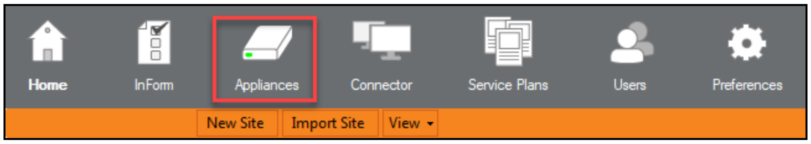
Updating a Software Appliance

After installing a **Software Appliance** at the **Site's** physical location and associating the **Software Appliance** with a **Site** in the **Network Detective Application**, it's important to regularly update the **Appliance** to get the most out of the features available on the **Software Appliance** you are using.

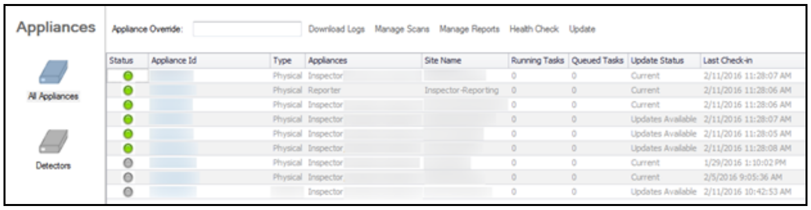


Updates may include bug fixes, new features, and additional scans types.

In the **Network Detective Application**, navigate to **Network Detective** ribbon bar and select the **Appliances** icon.



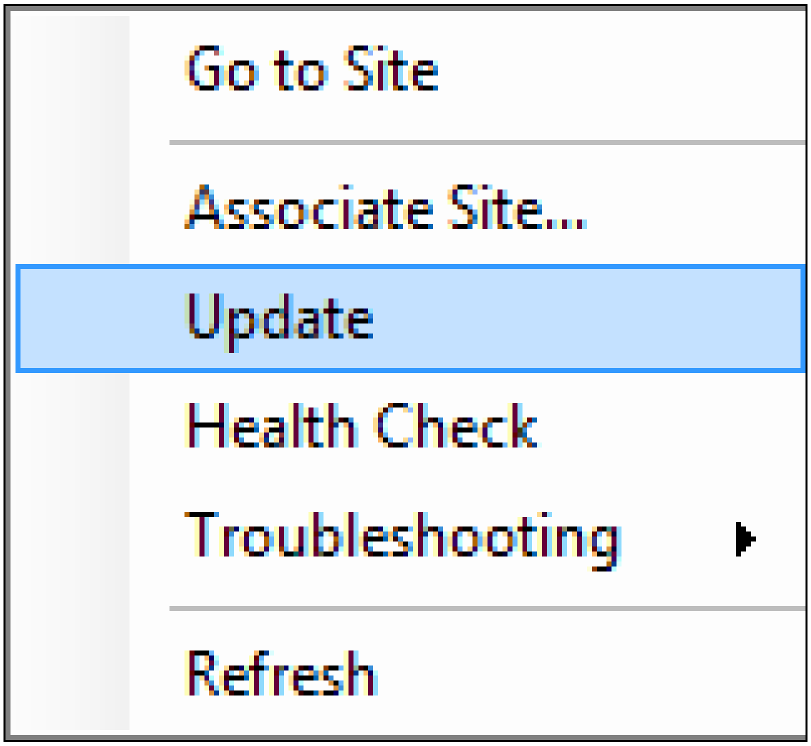
This action will display the **Software Appliances** window that lists all of the **Appliances** that are available for use from within **Network Detective**.



Status	Appliance Id	Type	Appliances	Site Name	Running Tasks	Queued Tasks	Update Status	Last Check-in
●	[redacted]	Physical	Inspector	[redacted]	0	0	Current	2/11/2016 11:28:07 AM
●	[redacted]	Physical	Reporter	Inspector-Reporting	0	0	Current	2/11/2016 11:28:06 AM
●	[redacted]	Physical	Inspector	[redacted]	0	0	Current	2/11/2016 11:28:06 AM
●	[redacted]	Physical	Inspector	[redacted]	0	0	Updates Available	2/11/2016 11:28:07 AM
●	[redacted]	Physical	Inspector	[redacted]	0	0	Updates Available	2/11/2016 11:28:05 AM
●	[redacted]	Physical	Inspector	[redacted]	0	0	Updates Available	2/11/2016 11:28:08 AM
○	[redacted]	Physical	Inspector	[redacted]	0	0	Current	1/29/2016 1:10:02 PM
○	[redacted]	Physical	Inspector	[redacted]	0	0	Current	2/5/2016 9:05:36 AM
○	[redacted]	[redacted]	Inspector	[redacted]	0	0	Updates Available	2/11/2016 10:42:53 AM

To update the selected **Software Appliance,** right click on the **Appliance's** name, and select the **Update** menu option presented as displayed.

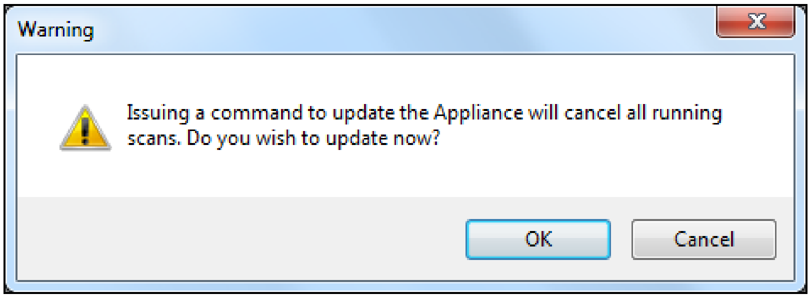
© 2021 RapidFire Tools, Inc. All rights reserved.



Note that the **Update** menu will only be visible if software updates are available.

IMPORTANT: The **Appliance Update Now** feature, when activated to update the **Software Appliance**, will shut down any tasks that are currently running on the **Software Appliance**. Before updating the **Software Appliance** either stop any currently running tasks listed in the

Manage Appliance Window Queued Tasks list, or perform the update after running tasks are completed.



Issuing a command to update the Appliance will cancel all running scans. Do you wish to update now?

A window will appear confirming the request for a software update.

© 2021 RapidFire Tools, Inc. All rights reserved.

Two-Factor Authentication for RapidFire Tools Portal

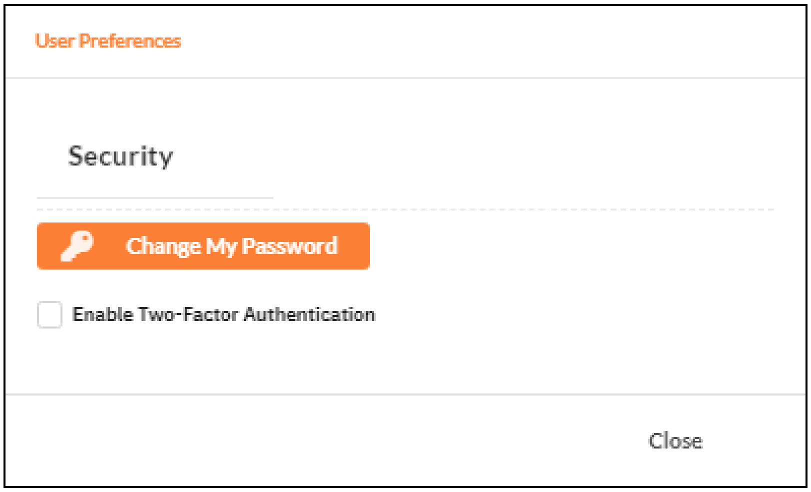
You can increase the security of your RapidFire Tools Portal account by enabling **Two-Factor Authentication (2FA)**. When 2FA is enabled, you will enter a second authenticator in addition to your password when you log into the Portal.

Note: **2FA** is enabled on a user-by-user basis. It is NOT account wide.

Enable Two-Factor Authentication

Follow the steps below to set up **2FA** in the RapidFire Tools Portal:

1. Download and install **Google Authenticator** on your phone. Visit **Google Play** or **Apple Store** and search for "Google Authenticator."
2. In the **RapidFire Tools Portal**, open your user options from 👤 and choose **User Preferences**.
3. Check **Enable Two-Factor Authentication**.



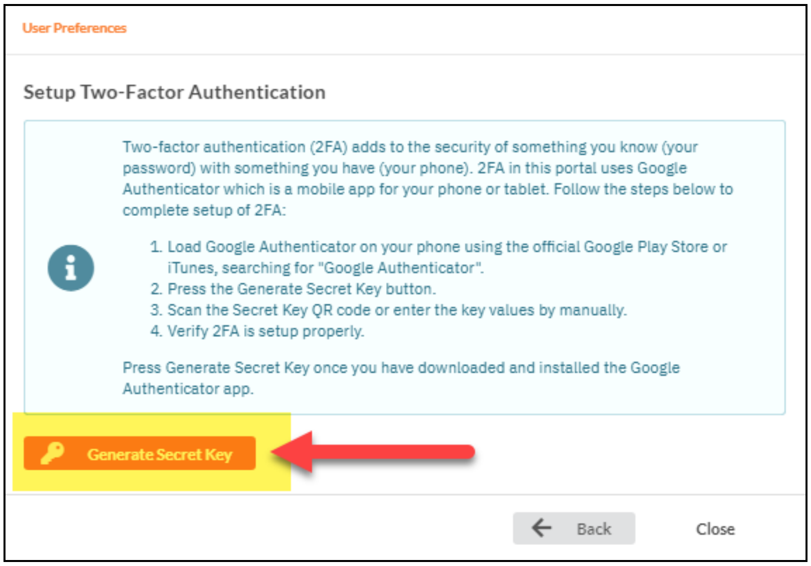
User Preferences

Security

□ Enable Two-Factor Authentication

4. Click **Generate Secret Key**.

© 2021 RapidFire Tools, Inc. All rights reserved.



User Preferences

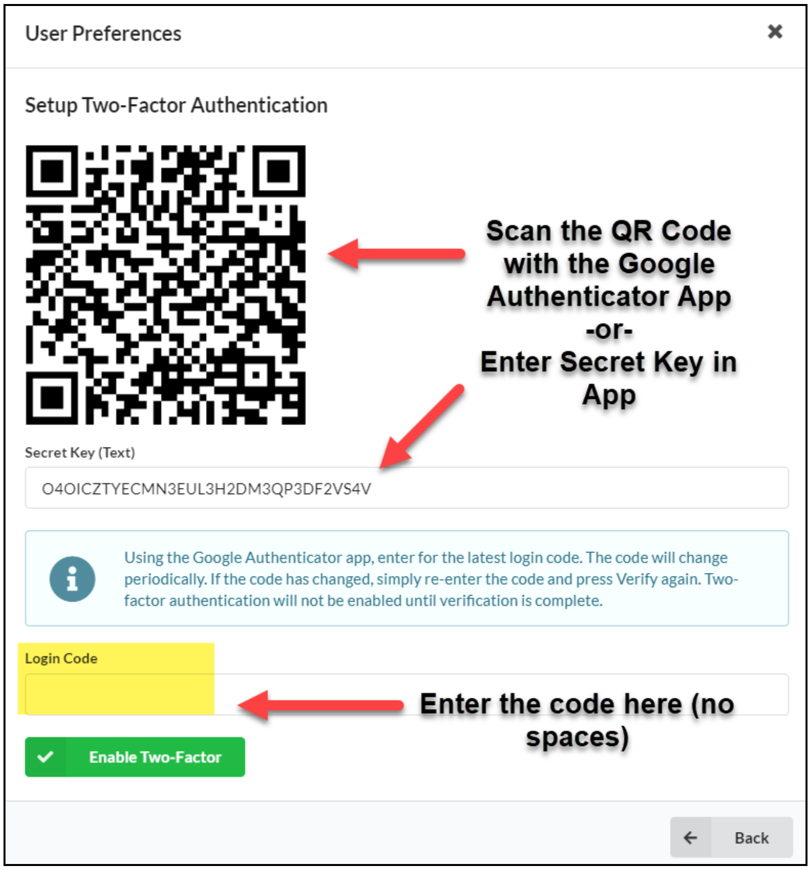
Setup Two-Factor Authentication

Two-factor authentication (2FA) adds to the security of something you know (your password) with something you have (your phone). 2FA in this portal uses Google Authenticator which is a mobile app for your phone or tablet. Follow the steps below to complete setup of 2FA:

1. Load Google Authenticator on your phone using the official Google Play Store or iTunes, searching for "Google Authenticator".
2. Press the Generate Secret Key button.
3. Scan the Secret Key QR code or enter the key values by manually.
4. Verify 2FA is setup properly.

Press Generate Secret Key once you have downloaded and installed the Google Authenticator app.

5. Using your Google Authenticator app on your phone, **scan the QR Code** on your computer screen or enter the Secret Key (Text) manually within the app.



User Preferences

Setup Two-Factor Authentication

Scan the QR Code with the Google Authenticator App -or- Enter Secret Key in App

Secret Key (Text)

O4OICZTYECMN3EUL3H2DM3QP3DF2VS4V

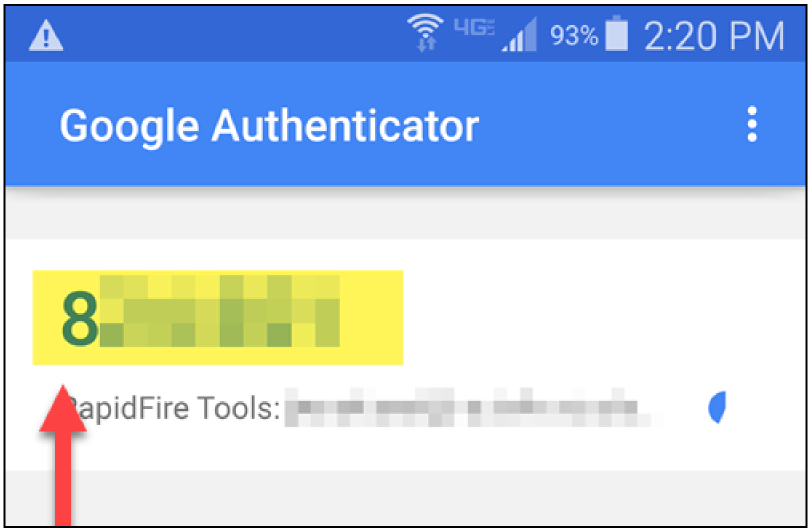
Using the Google Authenticator app, enter for the latest login code. The code will change periodically. If the code has changed, simply re-enter the code and press Verify again. Two-factor authentication will not be enabled until verification is complete.

Login Code

Enter the code here (no spaces)

© 2021 RapidFire Tools, Inc. All rights reserved.

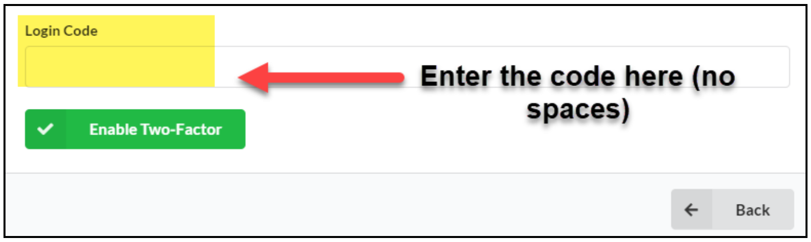
6. On your phone, a new Google Authenticator code will appear for your **RapidFire Tools account**.



8[redacted]

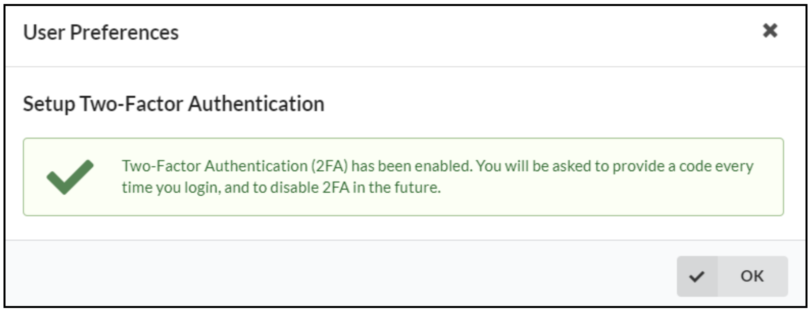
apidFire Tools: [redacted]

7. Enter the Google Authenticator code (**WITHOUT spaces**) in the **Login Code** field (pictured above). Then click **Enable Two-Factor**.



Enter the code here (no spaces)

If successful, the prompt below will appear:



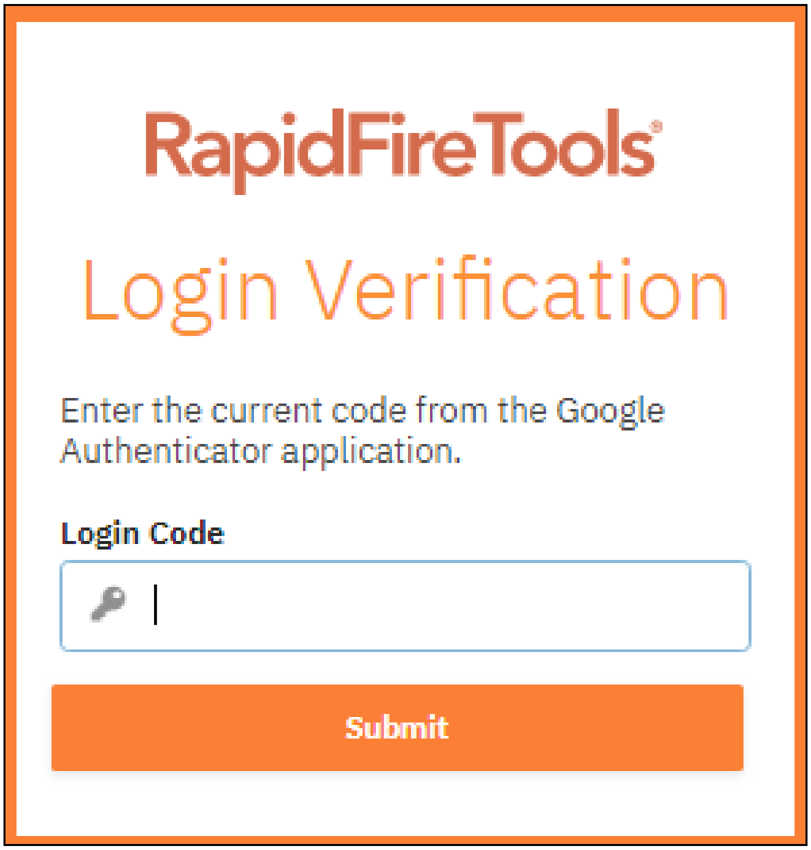
Setup Two-Factor Authentication

Two-Factor Authentication (2FA) has been enabled. You will be asked to provide a code every time you login, and to disable 2FA in the future.

Important: If you receive an error message, wait until the **Google Authenticator** code refreshes and enter the new code.

© 2021 RapidFire Tools, Inc. All rights reserved.

When you next log in to the Portal, you will be prompted to enter the Google Authenticator code after you enter your username and password:



RapidFireTools®

Login Verification

Enter the current code from the Google Authenticator application.

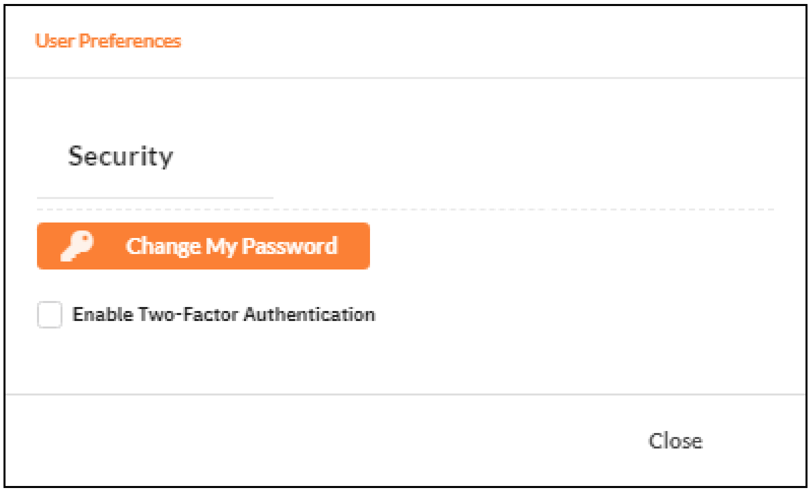
Login Code

Disable 2FA

If you wish to disable 2FA, follow these steps:

1. In the RapidFire Tools Portal, open your user options from 👤 and choose **User Preferences**.
2. Un-check **Enable Two-Factor Authentication**.

© 2021 RapidFire Tools, Inc. All rights reserved.

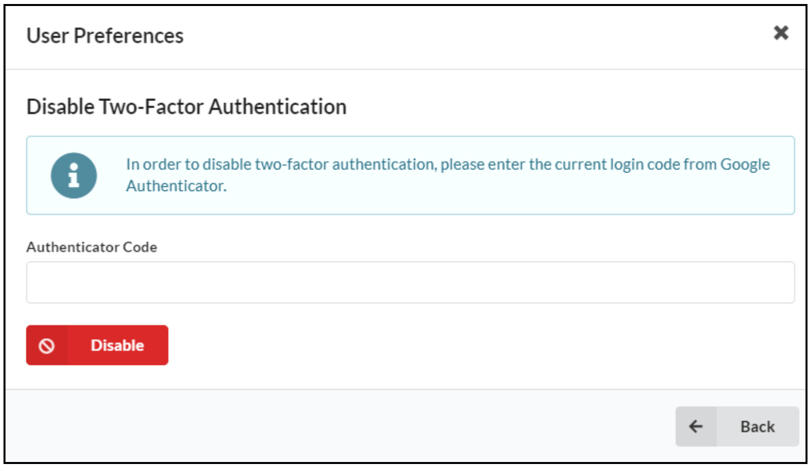


User Preferences

Security

□ Enable Two-Factor Authentication

3. Enter your authenticator code and click **Disable**. 2FA will then be disabled for your user.



User Preferences

Disable Two-Factor Authentication

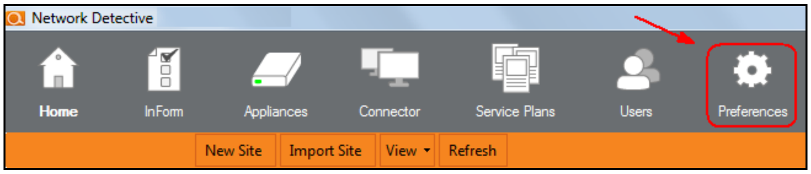
In order to disable two-factor authentication, please enter the current login code from Google Authenticator.

Authenticator Code

Set Up Custom SMTP Server Support (Reporter)

The steps below outline how to set up the use of your own SMTP Email Server to enable Reporter to send “**Reports are Ready for Download”** notifications by email.

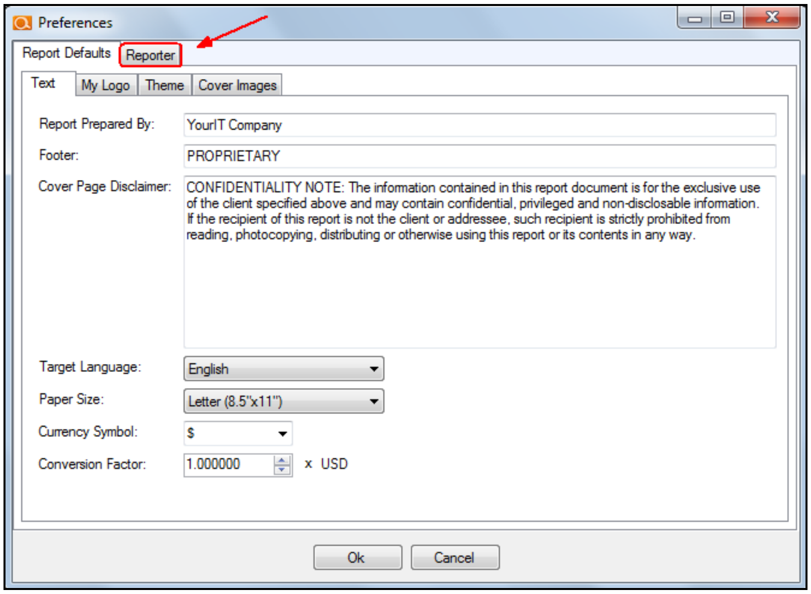
Follow these steps to set up the Reporter Custom SMTP **Email Server Configuration**.



1. In the Network Detective window, select the **Preferences** icon to access the **Preferences** window for access to the **Report Branding** and **Reporter Customer SMTP Server Configuration** options.

   The **Preferences** window will be displayed**.**

2. Select the **Reporter tab** within the **Preferences** window to access the Reporter’s **Custom SMTP Server** settings.



Report Prepared By: YourIT Company

Footer: PROPRIETARY

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

Target Language: English

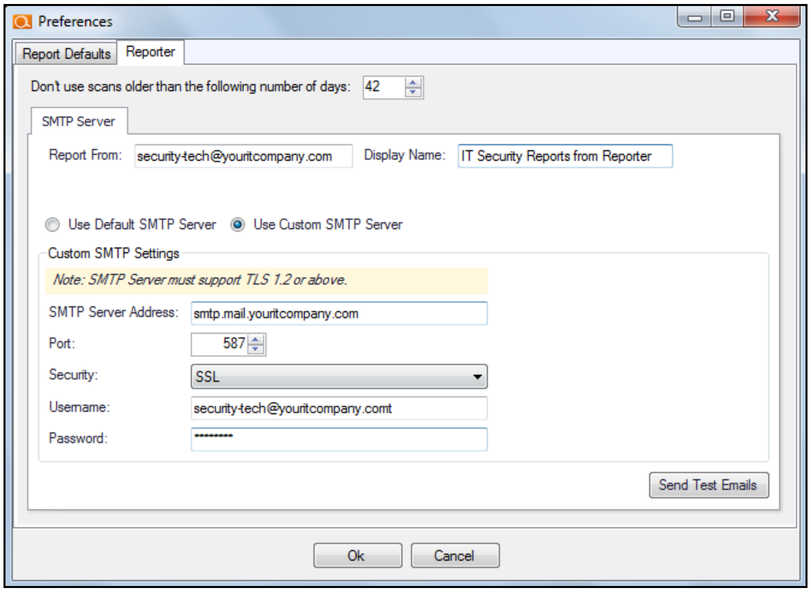
Paper Size: Letter (8.5"x11")

Currency Symbol: $

Conversion Factor: 1.000000 x USD

3. Configure the following to set up your **Custom SMTP Server** to relay email **Notifications** sent from Reporter:

© 2021 RapidFire Tools, Inc. All rights reserved.



Preferences

Report Defaults | Reporter

Dont use scans older than the following number of days: 42

SMTP Server

Report From: security-tech@yourtcompany.com Display Name: IT Security Reports from Reporter

○ Use Default SMTP Server ● Use Custom SMTP Server

Custom SMTP Settings

Note: SMTP Server must support TLS 1.2 or above.

SMTP Server Address: smtp.mail.yourtcompany.com

Port: 587

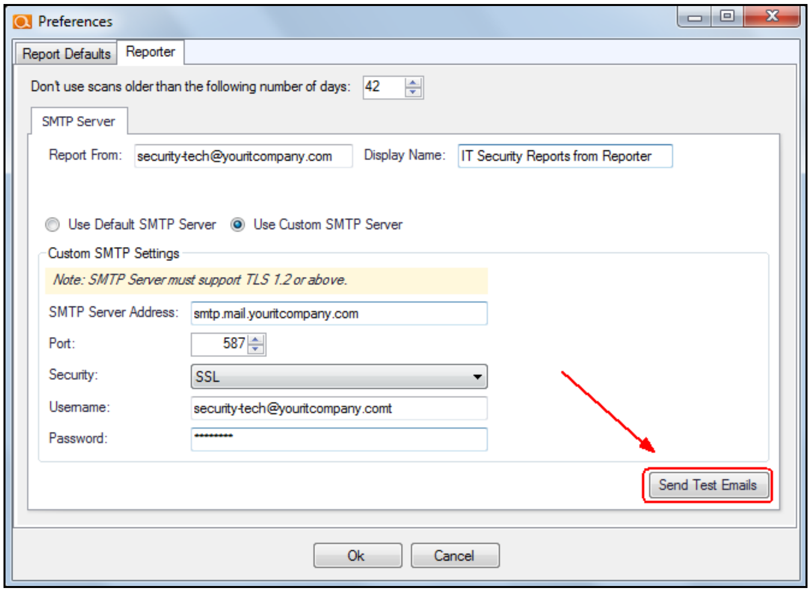
Security: SSL

Username: security-tech@yourtcompany.comt

Password: ********

- **Report From** email address
- **Display Name**
- **SMTP Server Address**
- **Port Number**
- **Security** Method
- **SMTP Server** Username and Password

4. Select the **Send Test Email** button to test the **Custom SMTP Server** configuration and email addresses.



Preferences

Report Defaults | Reporter

Dont use scans older than the following number of days: 42

SMTP Server

Report From: security-tech@yourtcompany.com Display Name: IT Security Reports from Reporter

○ Use Default SMTP Server ● Use Custom SMTP Server

Custom SMTP Settings

Note: SMTP Server must support TLS 1.2 or above.

SMTP Server Address: smtp.mail.yourtcompany.com

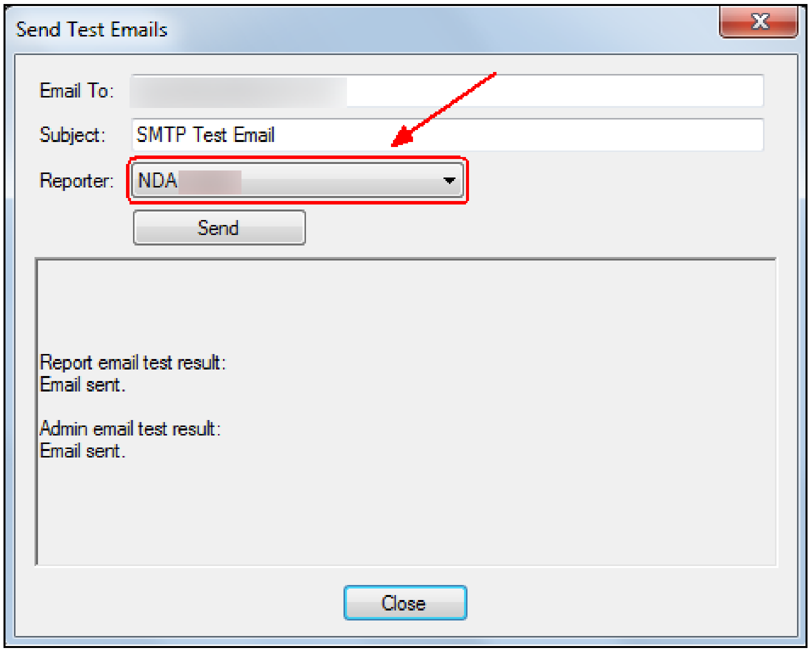
Port: 587

Security: SSL

Username: security-tech@yourtcompany.comt

Password: ********

5. Select your Reporter ID from the Reporter ID list.



Send Test Emails

Email To: [redacted]

Subject: SMTP Test Email

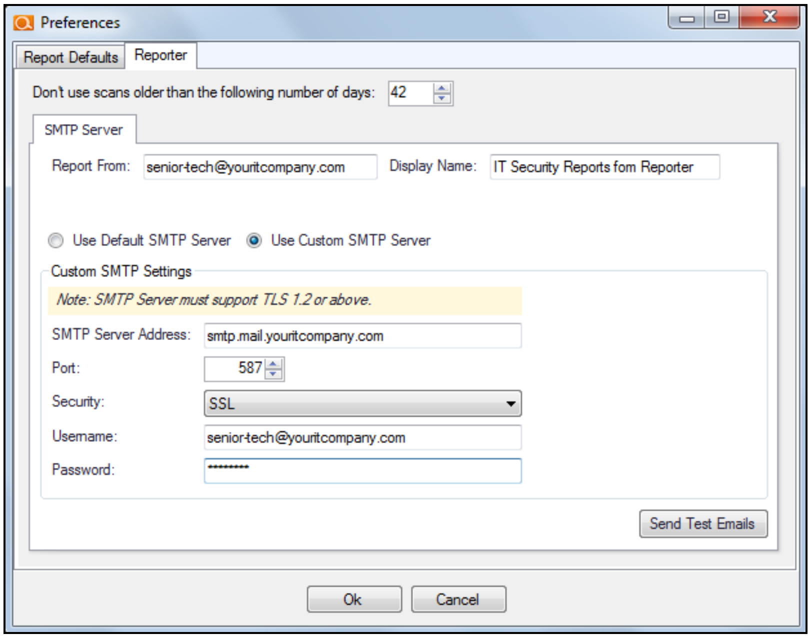
Reporter: NDA [redacted]

Report email test result:
Email sent.

Admin email test result:
Email sent.

Next, select the **Send** button in **the Send Test Emails** window.

The status of the send email test is displayed in the **Send Test Emails** window.



Preferences

Dont use scans older than the following number of days: 42

Report From: senior-tech@yourtcompany.com Display Name: IT Security Reports fom Reporter

○ Use Default SMTP Server ● Use Custom SMTP Server

Custom SMTP Settings

Note: SMTP Server must support TLS 1.2 or above.

SMTP Server Address: smtp.mail.yourtcompany.com

Port: 587

Security: SSL

Username: senior-tech@yourtcompany.com

Password: *********

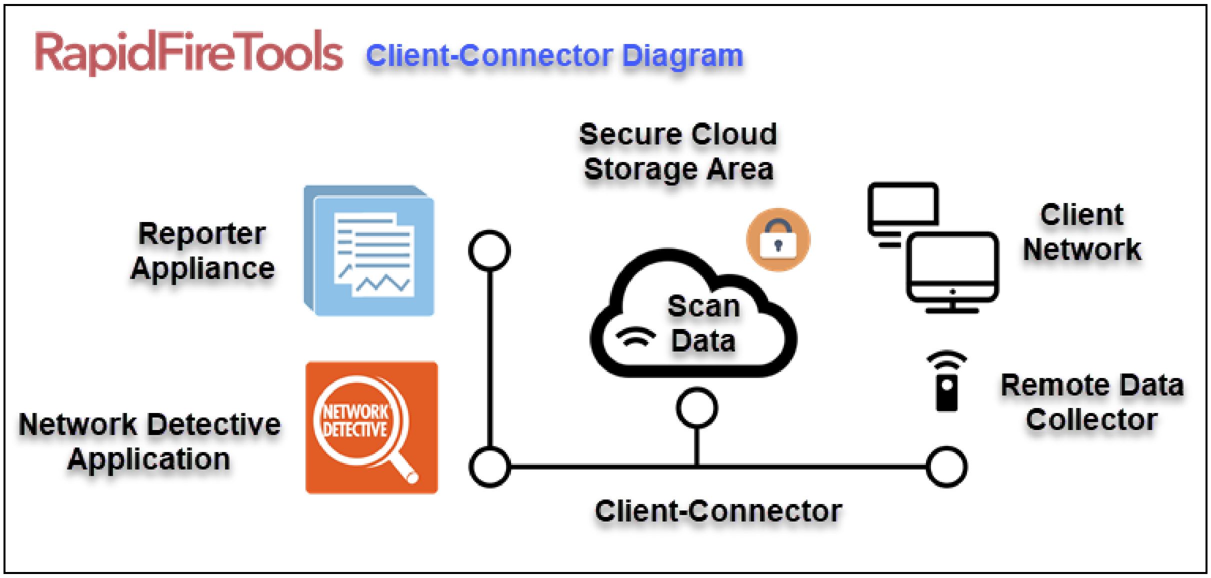
6. After a successful test has been completed, close the **Send Test Emails** window.

Next, select the **OK** button in the P**references** window to save the **Custom SMTP Server's Email Configuration** settings.

© 2021 RapidFire Tools, Inc. All rights reserved.

Client-Connector Diagram

The Remote Data Collector uploads scans to Secure Cloud Storage Area using the Client-Connector. You can download the scans from the Network Detective application. Likewise, the Reporter appliance will automatically download the scans in order to generate scheduled assessment reports.



© 2021 RapidFire Tools, Inc. All rights reserved.

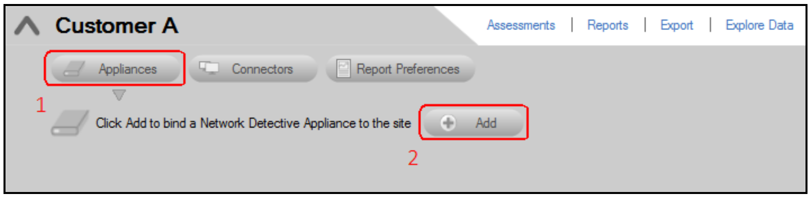
Using Reporter with Cyber Hawk

You can use Reporter with Scan Data collected by the Cyber Hawk Appliance to generate Network and Security Assessment Reports. In addition, when using the Security Assessment Module, you can generate an Internal Vulnerabilities Summary Report that uses the internal network vulnerability scan performed by the Cyber Hawk Appliance. To do this:

Step 1 — Associate Reporter and Cyber Hawk with the same Site

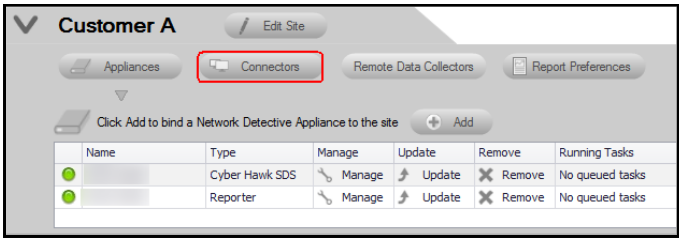
You will first need to make sure your Site has both a **Reporter and Cyber Hawk** appliance associated with it. To bind an appliance to a Site:

1. Open your active assessment project and click the selector icon ^.
2. Click **Appliances**.
3. Click **Add**. Choose the appliances to add.



Click Add to bind a Network Detective Appliance to the site

4. Once you add the Reporter and Cyber Hawk appliances, select the **Connectors** button to add a Connector to the Site. The Connectors list window will be displayed.



Click Add to bind a Network Detective Appliance to the site

	Name	Type	Manage	Update	Remove	Running Tasks
●	[redacted]	Cyber Hawk SDS	Manage	Update	✕ Remove	No queued tasks
●	[redacted]	Reporter	Manage	Update	✕ Remove	No queued tasks

> **Note:** The Connector is required to enable the Cyber Hawk to transport its scan files to the RapidFire Tools Secure Storage Area for access by the Reporter during the scheduled report generation time. You will assign the Connector to the site as part of the normal Reporter set up process.

© 2021 RapidFire Tools, Inc. All rights reserved.

5. Assign a Connector Label that specifically references the name of the Site that is going to be using the Connector. Next select the OK button to finish adding the Connector to the Site.

> **Note:** You must have first purchased and installed the appliance on the target network before you can bind it to a site. Note also that, unlike Reporter, Cyber Hawk appliance is installed on the client's network.

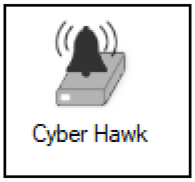
See also:

- "Setting Up Cyber Hawk" in the Cyber Hawk documentation at https://www.rapidfiretools.com/nd
- Setting Up Reporter

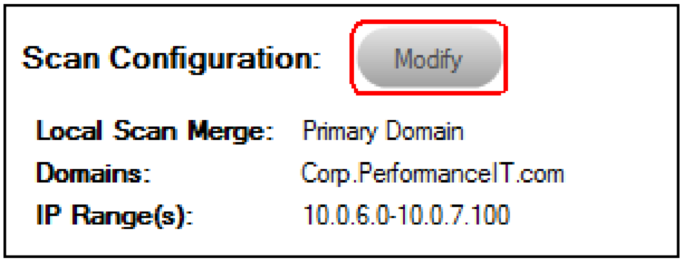
Step 2 — Configure Cyber Hawk to Upload Scans for use by Reporter

Next set up your Cyber Hawk scans to work with your Reporter. To do this:

1. Open Cyber Hawk from your Site.



2. Click **Modify** next to Scan Configuration.



Scan Configuration:

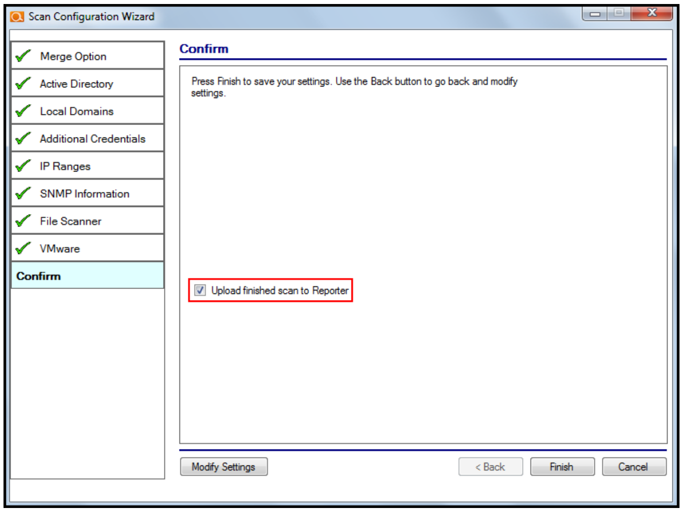
Local Scan Merge: Primary Domain

Domains: Corp.PerformanceIT.com

IP Range(s): 10.0.6.0-10.0.7.100

3. Configure your scan. In the Scan Configuration Wizard window, select the option “**Upload finished scan to Reporter**”.

© 2021 RapidFire Tools, Inc. All rights reserved.



Confirm

Press Finish to save your settings. Use the Back button to go back and modify settings.

☑ Upload finished scan to Reporter

4. (OPTIONAL) Next, configure your Remote Data Collector Scan Tasks. See Configure Remote Data Collector Scans for more details.

> **Note:** You can generate **Network Assessment** and **Security Assessment** reports using Cyber Hawk. Use Cyber Hawk to enhance your reports with an **Internal Vulnerability Scan**.
>
> However, for **SQL**, **Exchange**, **HIPAA**, and **PCI** assessments, you will need to use the Remote Data Collector.

> **Important:** Schedule your Cyber Hawk and Remote Data Collector scan tasks a few hours BEFORE your Reporter tasks. This will ensure your automated reports always contain the latest and best data.

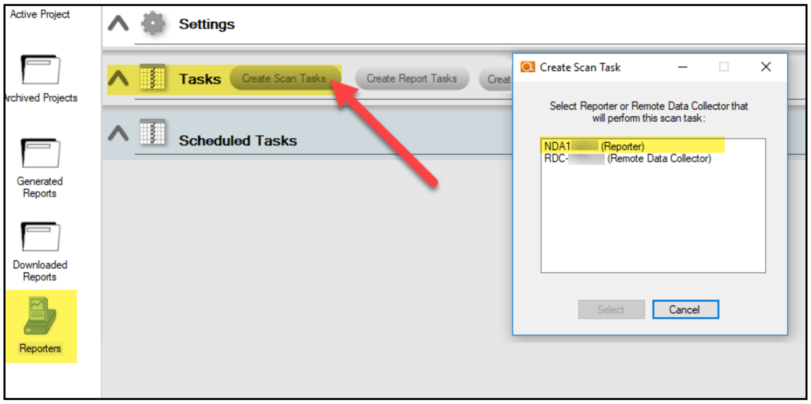
Step 3 — Set up Reporter to Automatically Generate Reports

The last step is to configure your Reporter tasks for automated reports.

1. Open your active assessment project and click the **Reporter** icon.

© 2021 RapidFire Tools, Inc. All rights reserved.

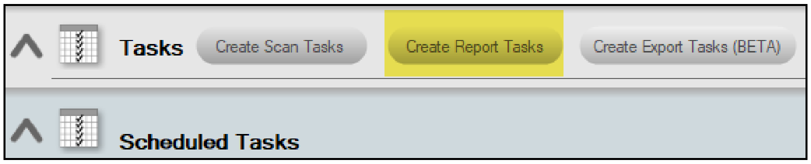
2. (Optional) If you want to set up an automated *External Vulnerability Scan*, click the **Create Scan Task** button and select the **Reporter** (*NOT* the Remote Data Collector). Then configure your External Vulnerability Scan.



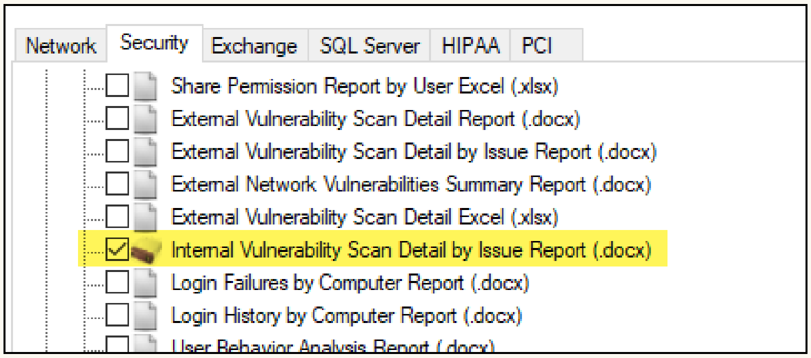
Select Reporter or Remote Data Collector that will perform this scan task:

NDA1[redacted] (Reporter)
RDC-[redacted] (Remote Data Collector)

3. Once you've created your optional external vulnerability scan, click **Create Report Tasks**. Use the wizard to create your report tasks.



Tip: Use the Internal Vulnerability Scan performed by Cyber Hawk to generate an automated **Internal Vulnerability Scan Report**.



☐ Share Permission Report by User Excel (.xlsx)
☐ External Vulnerability Scan Detail Report (.docx)
☐ External Vulnerability Scan Detail by Issue Report (.docx)
☐ External Network Vulnerabilities Summary Report (.docx)
☐ External Vulnerability Scan Detail Excel (.xlsx)
☑ Internal Vulnerability Scan Detail by Issue Report (.docx)
☐ Login Failures by Computer Report (.docx)
☐ Login History by Computer Report (.docx)
☐ User Behavior Analysis Report (.docx)

Note: Once you create scan and report tasks, click **Schedule** to set a time and day for them to regularly occur.

See also:

© 2021 RapidFire Tools, Inc. All rights reserved.

- Configure Reporter to Access Scan Data and Generate Reports
- Setting Up Automatic Reports by Assessment Module

RapidFireTools®

© 2021 RapidFire Tools, Inc. All rights reserved.

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 *Windows Management Instrumentation (WMI)* service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
□	Allow *File and printer sharing* to operate through Windows Firewall This includes the following rules: • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
□	Enable *Remote Registry* “read only” access on computers targeted for scanning.

© 2021 RapidFire Tools, Inc. All rights reserved.

Complete	Domain Configuration
	Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request **Note:** ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
□	*Windows Management Instrumentation (WMI)* • Startup Type: Automatic
□	*Windows Update Service* • Startup Type: Automatic
□	*Remote Registry* • Startup Type: Automatic
□	*Remote Procedure Call* • Startup Type: Automatic
	Network Shares
□	• *Admin$* must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

© 2021 RapidFire Tools, Inc. All rights reserved.

Complete	Domain Configuration
	3rd Party Firewalls
□	• Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. **Note:** This is a requirment for both Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

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

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

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

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

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

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

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

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

© 2021 RapidFire Tools, Inc. All rights reserved.

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

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

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

Complete?	Workgroup Configuration
	Network Settings
□	• *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
□	• *File and printer sharing* must be enabled on the computers you wish to scan
□	• *Ensure the Windows Services below are running and allowed to communicate through Windows Firewall*: • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
□	• Workgroup computer administrator user account credentials. **Note:** Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) adminstrator user account credentials for entry into the scan settings wizard.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:

© 2021 RapidFire Tools, Inc. All rights reserved.

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

© 2021 RapidFire Tools, Inc. All rights reserved.