



USER GUIDE

Reporter

Fully Automate ongoing Report Generation & Delivery with Reporter

Contents

Introduction to Reporter	9
<u>Reporter Overview</u>	9
Reporter Appliance	9
Remote Data Collector	9
InDoc and the RapidFire Tools Portal	10
About this User Guide	10
Components of the Reporter	11
<u>Reporter Features</u>	12
Automated Assessment Reporting	12
Automated External Vulnerability Scanning	12
Remote Updating of the Reporter	13
InDoc and the RapidFire Tools Portal	13
<u>Tips for Automated Report Scheduling</u>	14
Schedule Site Reports after Site Scans	14
Schedule Reports at Correct Time Intervals for Multiple Sites	14
Schedule External Vulnerability Reports after External Vulnerability Scan	14
<u>RapidFire Tools Server System Requirements</u>	15
Reporter Prerequisites	16
Setting Up Reporter	17
<u>Initial Reporter Set Up</u>	17
Step 1 — Install Reporter Appliance on MSP Network	17
Step 2 — Open Existing Network Detective Site with an Active Assessment Project	18
Step 3 — Associate Reporter with Sites	19
Step 4 — Add Client-Connector to the Site	21
<u>Initial Remote Data Collector Set Up</u>	22
Remote Data Collector System Requirements	22
Network Prerequisites for RDC Scans	22
Remote Data Collector and Exchange Assessments	23
Step 1 — Download and Install Remote Data Collector on Client Network	23

Step 2 — Set Up Remote Data Collector on Client Network	26
<u>Configure Remote Data Collector to Perform Scan Tasks</u>	31
<u>Configure Reporter to Access Scan Data and Generate Reports</u>	35
Step 1 — Verify connection to Remote Data Collector	35
Step 2 — Schedule an External Vulnerability Scan (OPTIONAL)	38
Set up the External Vulnerability Scan	39
Schedule the External Vulnerability Scan	41
Step 3 — Configure Automatic Report Generation	43
Setting Up Automatic Reports by Assessment Module	47
<u>Network Assessment Automatic Reports</u>	47
<u>Security Assessment Automatic Reports</u>	50
<u>SQL Server Assessment Automatic Reports</u>	53
<u>Exchange Assessments Automatic Reports – (Using the Exchange Data Collector and Windows Task Manager)</u>	56
<u>HIPAA Compliance Assessment Automatic Reports</u>	59
Step 1 — Finish and Upload Completed HIPAA Assessment Project to Reporter	59
Step 2 — Create HIPAA Scan Tasks	60
Step 3 — Create HIPAA Report Tasks	60
Step 4 — Review and Update HIPAA Exception Report and Update InForms	63
Step 5 — Finish and Upload Updated HIPAA Assessment Project to Reporter	64
<u>PCI Compliance Assessment Automatic Reports</u>	66
Step 1 — Finish and Upload Completed PCI Assessment Project to Reporter	66
Step 2 — Create PCI Scan Tasks	67
Step 3 — Create PCI Report Tasks	67
Step 4 — Review and Update PCI Exception Report and Update InForms	70
Step 5 — Finish and Upload Updated PCI Assessment Project to Reporter	71
<u>Synchronizing Assessment Projects with Reporter</u>	73
Finishing a Project: Upload Project to Appliance	73
Starting a Project: Sync New Assessment with Latest Appliance Scans	74
<u>Manually Download Reports (Reporter)</u>	75
Filter Reports by Days Back	77

<u>Copy Reports to External Network Share with Reporter</u>	79
<u>Automate Vulnerability Reports with VulScan</u>	81
Step 1 — Create Scan Tasks from VulScan Site	81
Create Internal Scan Task	81
Create External Scan Task	85
Step 2 — Create Vulnerability Report Tasks	88
Step 3 — Download Reports from VulScan Appliance in Network Detective	89
Remote Data Collector Scans	90
<u>Configuring Remote Data Collector Scans by Assessment Module</u>	90
Network and Security Assessment Scan	91
Scanning an Active Directory Domain Network	91
Scanning a Workgroup Network	98
Exchange Server Assessment Scan	106
SQL Server Assessment Scan	108
HIPAA Compliance Network Scan	109
PCI Compliance Network Scan	111
Push Deploy Local Computer Scans	113
Local Scan for a Computer Running the Remote Data Collector	117
<u>Configure the Local Data Scan Merges</u>	121
Step 1 — Select and Open the Site	121
Step 2 — Select Manage Appliance	121
Step 3 — Set Scan Data Merge Configuration	122
Step 4 — Set the Local Scan Merge Settings and Save Settings	122
InDoc and the RapidFire Tools Portal	124
<u>Requirements for using InDoc with Reporter</u>	125
<u>Using InDoc (RapidFire Tools Portal)</u>	128
<u>Explore Network Assets with InDoc</u>	130
View Data about Network Assets	131
Users	131
Computers	132
<u>Add a Note to an Asset (InDoc)</u>	133

Add and View Confidential Notes (InDoc)	136
Enable Confidential Information Protection for InDoc	138
Grant User Access to Confidential Notes	138
<u>Add a Procedure to an Asset (InDoc)</u>	140
Edit or Delete Procedures	142
<u>Add Related Items to a Network Asset (InDoc)</u>	143
<u>View Site Management Plan (InDoc)</u>	146
<u>Edit Smart Tags in InDoc</u>	148
<u>InDoc User Permissions</u>	151
How to Set Up User Permissions for InDoc	151
Privacy Permissions for Confidential Notes (InDoc)	152
<u>How Can my Team Use InDoc? Two Examples</u>	153
#1: Help Desk	153
#2: Tech at a Customer Site	153
<u>RapidFire Tools Portal Client View for Reporter</u>	154
Step 1 — Configure Reporter to Publish to the Client Portal	154
Configure Reporter Template to Publish to Client Portal	156
Step 2 — Ensure that the Site is Visible in the Client Portal	157
Step 3 — Add Client User to Site and Assign Client Role	158
Step 4 — Configure Client View in RapidFire Tools Portal	158
Access the Portal as a Client User	160
Appendices	162
<u>Reporter Templates</u>	163
<u>Create and Deploy Reporter Templates</u>	164
Step 1 — Create New Reporter Template	164
Step 2 — Assign Reports to Template	166
Step 3 — Set Delivery Method	168
Step 4 — Schedule the Report Task	169
Step 5 — Assign Template to Sites	170
Modifying Reporter Template Tasks at the Site Level	172
Step 6 — Configure Scans for Reporter Templates	172

Important Tips for Using Reporter Templates	173
Suggestions for Scheduling Report Tasks	173
How Long Does it Take for Reporter to Complete Report Tasks?	173
Preset Reporter Templates	173
Reload Preset Templates	174
<u>Custom Reports</u>	175
Create a Custom Report Template	175
Create a Report Generation Task using the Custom Full Detail Report Template	179
<u>Generate Client Progress Reports</u>	183
<u>Set Scan and Report Task Time Zone and Date Format</u>	187
At Site Level	187
At Global Level	188
<u>Automate Microsoft Cloud Assessment and Reports with Reporter</u>	189
Step 1 — Create MS Cloud Scan task	189
Step 2 — Create MS Cloud Report Task	192
Step 3 — Schedule Scan and Report Tasks	194
<u>Automate AWS Assessment and Reports with Reporter</u>	196
Step 1 — Create AWS Scan task	196
Step 2 — Create MS Cloud Report Task	199
Step 3 — Schedule Scan and Report Tasks	201
<u>Authenticate Exchange Scan using Enterprise App</u>	203
Step 1 — Register app in Azure Active Directory	203
Step 2 — Assign Exchange Administrator role to app	206
Step 3 — Install Required Exchange Online Management PowerShell Module	207
Step 4 — Generate self-signed certificate and attach to app	208
a) Name the certificate	208
b) Generate the certificate	208
c) Export the certificate	208
Step 5 — Add certificate to Enterprise App	209
Step 6 — Collect credentials to perform Exchange scan	210
<u>Integrate Reporter with a PSA System with Export Tasks</u>	212
Step 1 — Gather Credentials and Set Up your PSA System	212

Step 2 — Create Export Task with Reporter	214
Step 3 — Schedule/Run Export Task	221
Set Up Autotask Integration	223
Set Up ConnectWise REST Integration	228
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	228
Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with	228
Create Minimum Permissions Security Role for API Member	229
Step 3 — Create an API Key in the ConnectWise Ticketing System	230
Step 4 — Configure Service Tables in ConnectWise	230
Step 5 — Remove "Disallow Saving" Flag from Company	232
Set Up ConnectWise SOAP Integration	237
Set Up Kaseya BMS Integration	239
Set Up Network Detective to IT Glue Integration	241
Step 1 — Create Organization and API Key in IT Glue	241
Step 2 — Create a Reporter Export Task to IT Glue	242
Step 3 — Create Connection to IT Glue and Configure Asset Mapping	245
Step 4 — Continue Configuring Export Task	249
Step 5 — Access data in IT Glue after scan and export	252
Matching Criteria for Configurations and Contacts	254
Association Criteria for Flexible Assets	254
Key Fields	255
<u>Software Appliance Diagnostic Tool</u>	258
Available Commands	258
<u>Augment Reporting to Eliminate False Positives</u>	261
Use the Excel Export Spreadsheet to Find Display Names	263
<u>Updating a Software Appliance</u>	265
<u>Set Up Custom SMTP Server Support (Reporter)</u>	267
<u>Client-Connector Diagram</u>	271
<u>Using Reporter with Cyber Hawk</u>	272
Step 1 — Associate Reporter and Cyber Hawk with the same Site	272
Step 2 — Configure Cyber Hawk to Upload Scans for use by Reporter	273

Step 3 — Set up Reporter to Automatically Generate Reports	274
<u>Pre-Scan Network Configuration Checklist</u>	277
Checklist for Domain Environments	277
Checklist for Workgroup Environments	279

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.

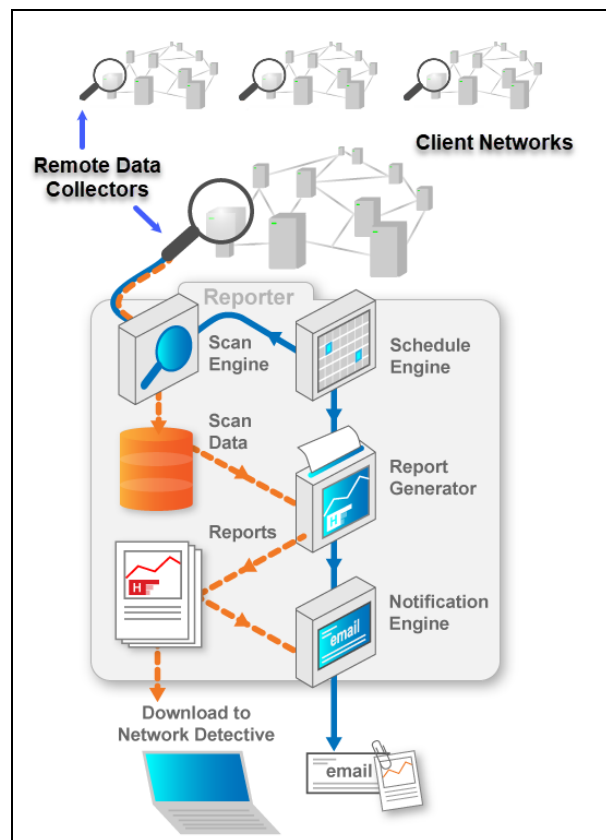
Reporter Appliance

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.



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 <i>Notes</i> , <i>Procedures</i> , and <i>Smart Tags</i> . You can also map <i>Relationships</i> 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.

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 incorporated 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.

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.

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. ["Initial Reporter Set Up" below](#)
2. ["Initial Remote Data Collector Set Up" on page 22](#)
3. ["Configure Remote Data Collector to Perform Scan Tasks" on page 31](#)
4. ["Configure Reporter to Access Scan Data and Generate Reports" on page 35](#)

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.

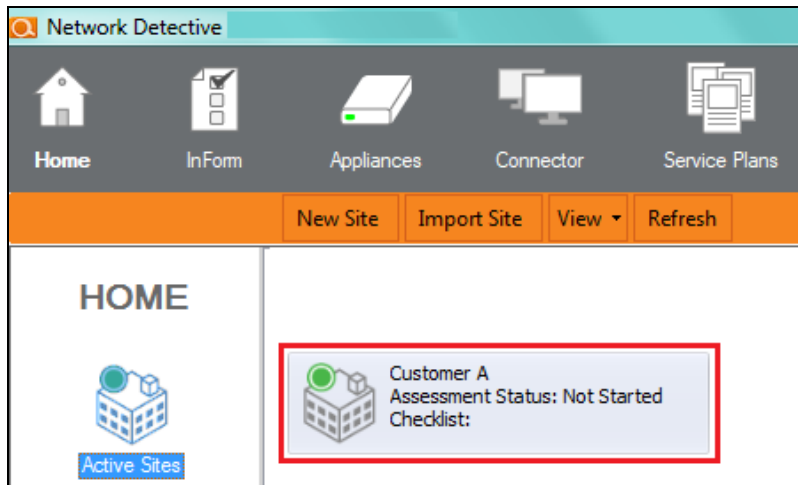
For more information about **installing the Reporter Server**, please download the [Reporter Server Installation Guide](#).

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**.



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

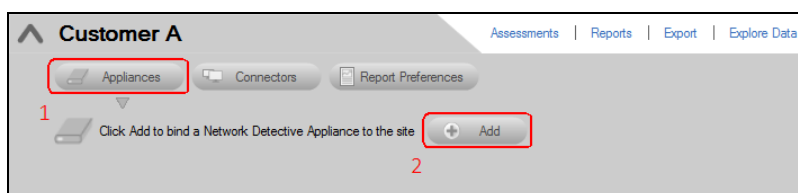
Before using the **Reporter**, the **Reporter** must be **Associated** with a **Site** in the **Network Detective Application**.

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.

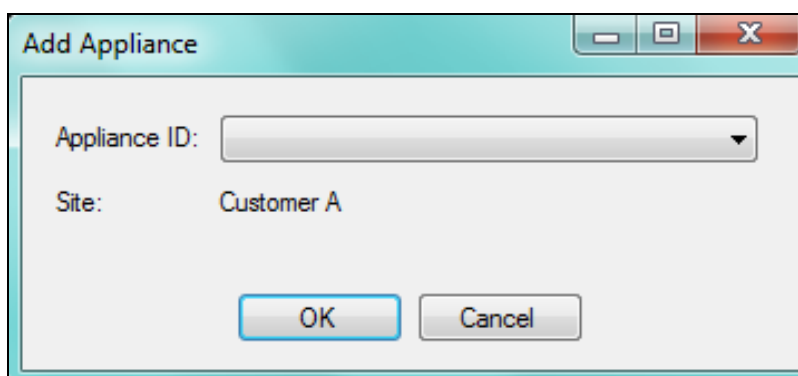


This action will expand the **Site’s** properties for you to view and to **Add** a **Software Appliance** to the **Site**.

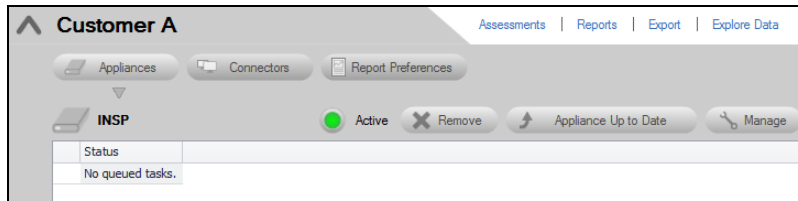
2. To add an **Appliance** to **Site**, select the **Appliance** button, then the **Appliances Add** button.



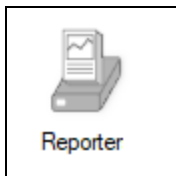
3. Select the **Appliance ID** of the **Appliance** from the drop down menu.



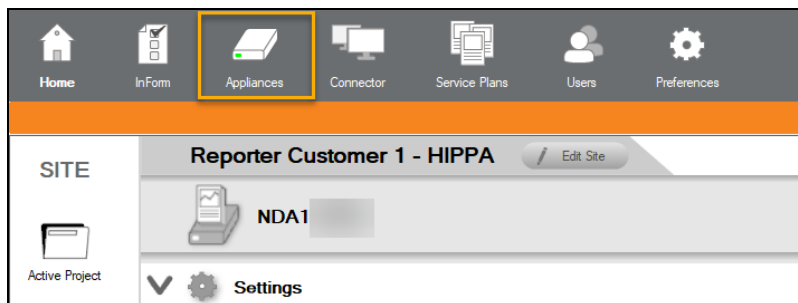
After successfully adding an **Appliance**, it will appear under the **Appliance** bar in the **Site Properties** window.



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**.

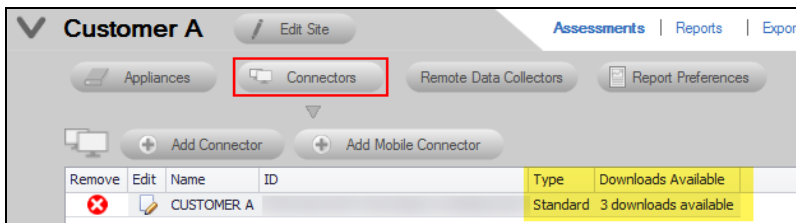
Step 4 — Add Client-Connector to the Site

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

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



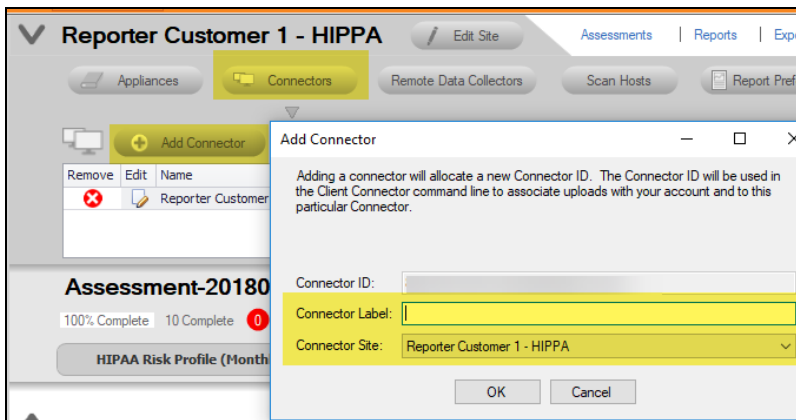
3. Select **Connector** button.



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**.



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

When you complete these steps, proceed to ["Initial Remote Data Collector Set Up" on the facing 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 277](#) 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.

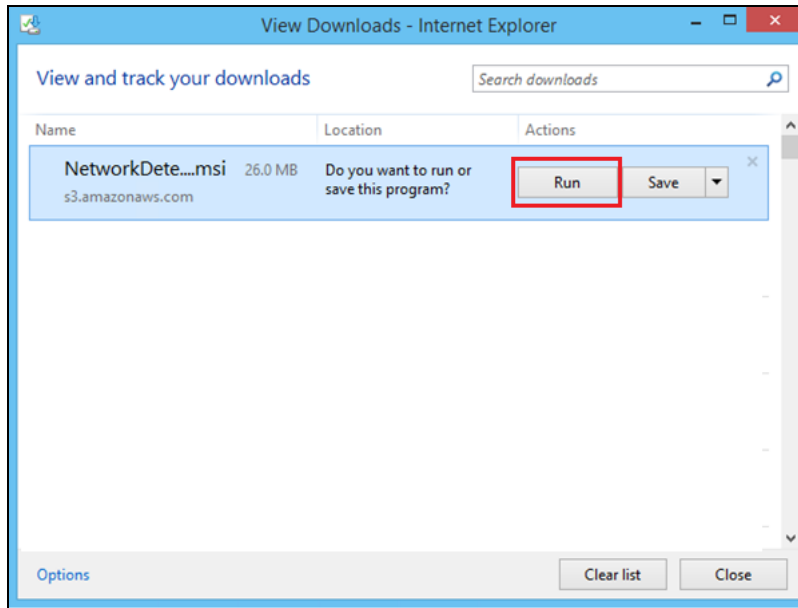
Remote Data Collector and Exchange Assessments

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.

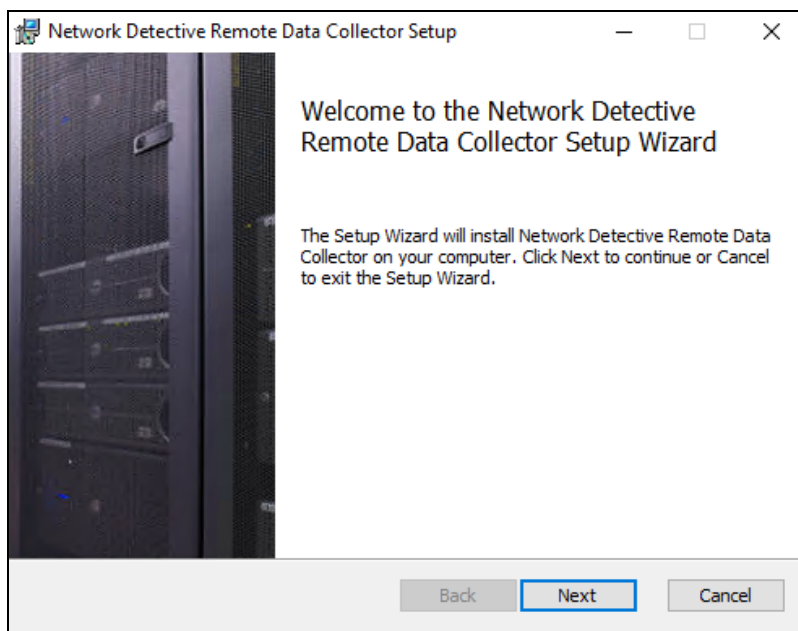
Note: If you are scanning Office 365, you do not need to run the RDC on the server. You will only need to enter management credentials for Office 365.

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

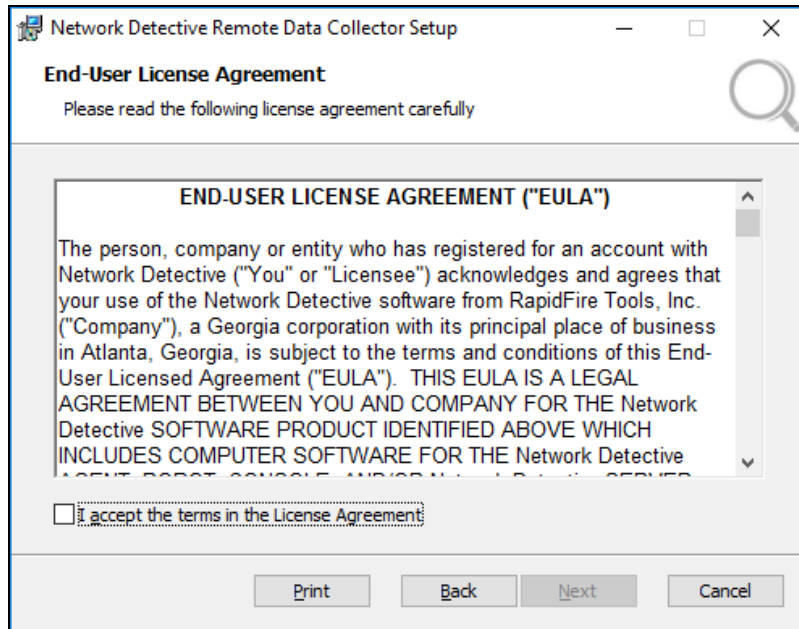
1. Visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/nd-downloads> to download and run the **Remote Data Collector Installer** file. The **Installer** file is named **NetworkDetectiveRemoteDataCollector.msi**.



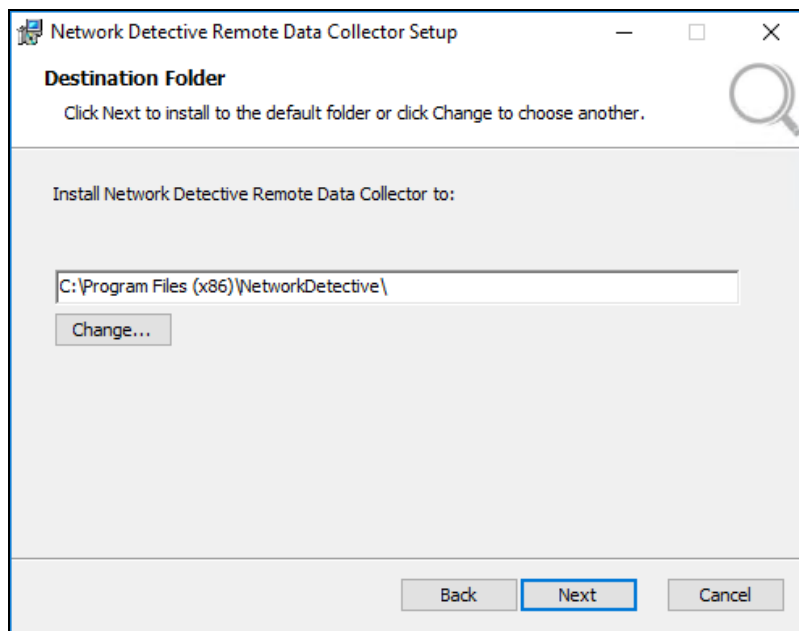
2. After downloading the **Installer**, **Run** the **Installer** to start the installation process.
3. After the Welcome Screen is displayed, click **Next** button to continue the installation process.



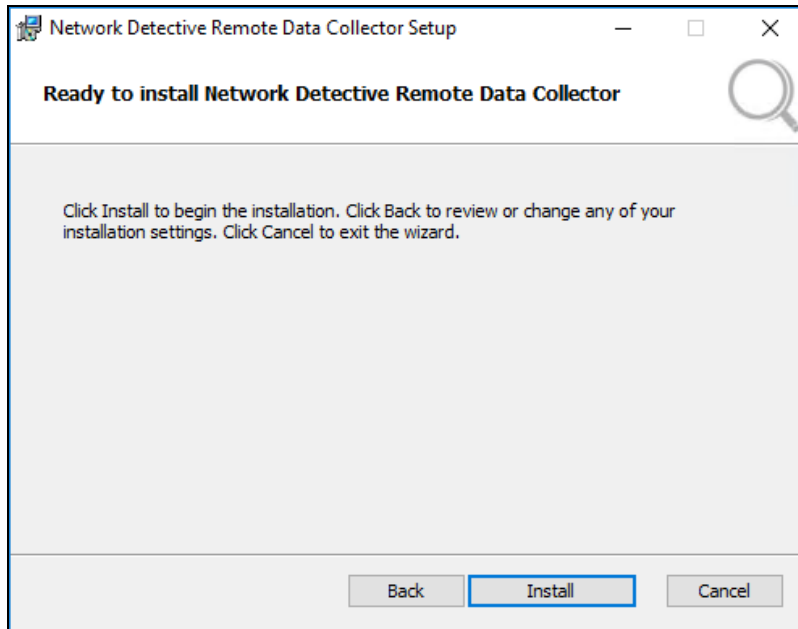
4. Accept the terms of the **End User License Agreement** and click **Next**.



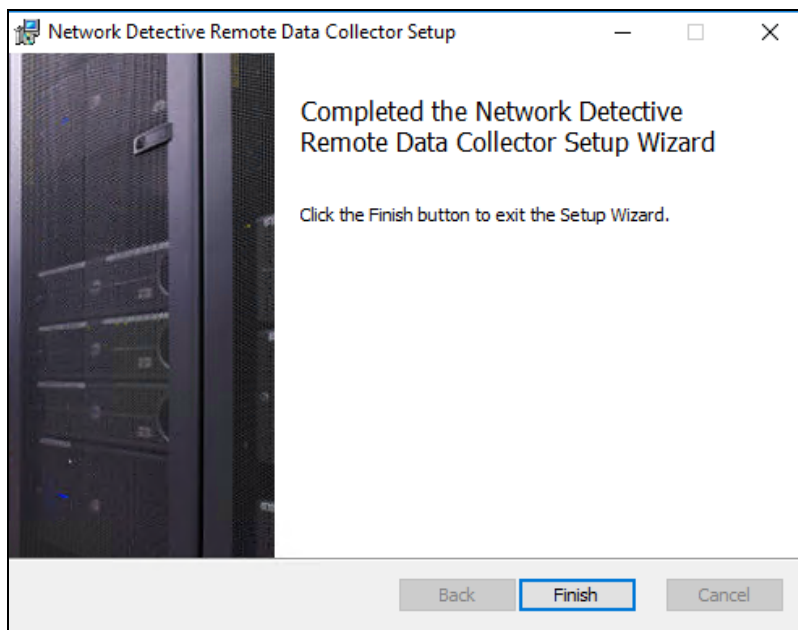
5. Accept the default **Destination Folder** location for the Remote Data Collector's installation. Click **Next**.



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

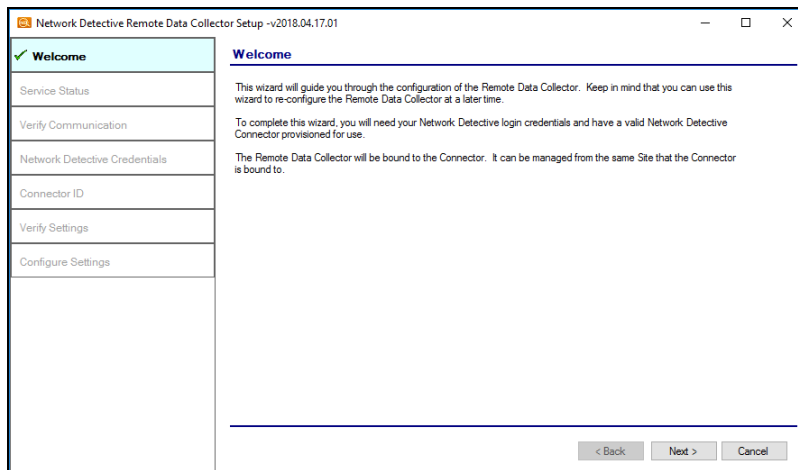


7. When the install is complete, click **Finish**.

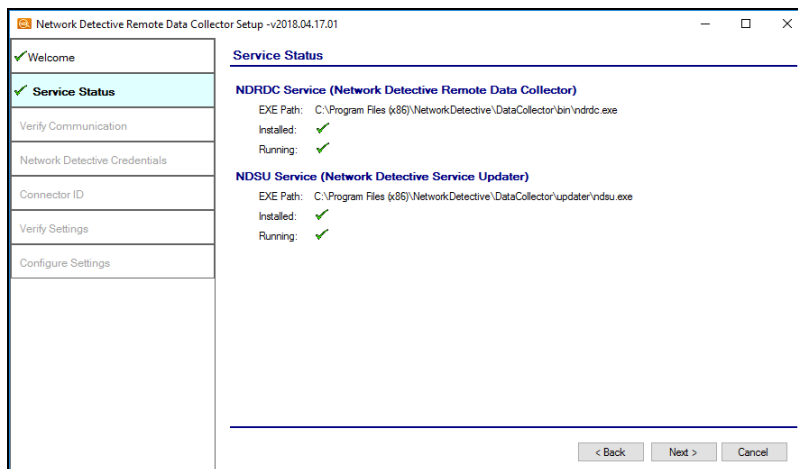


Step 2 — Set Up Remote Data Collector on Client Network

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

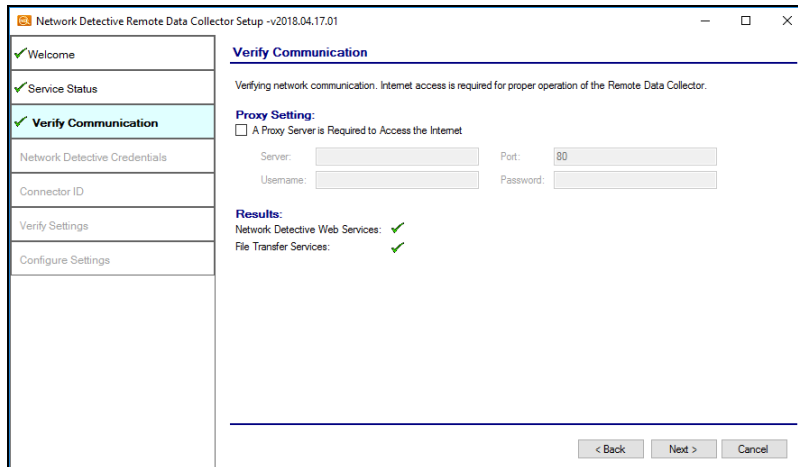


2. During this step, the **Remote Data Collector** and **Service Updater** programs will be installed. Once the Installer confirms the installation of each program, click **Next**.

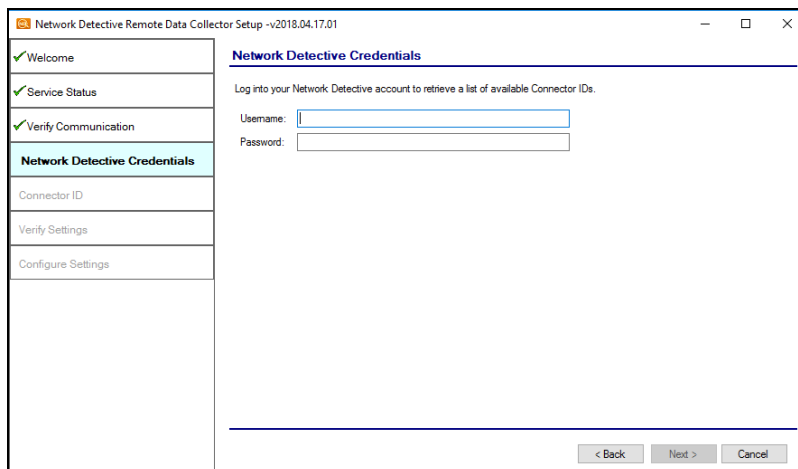


3. In this step, the RDC will verify that the computer that will host the data collector can communicate with the Network Detective web and file transfer services. Click **Next**.

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

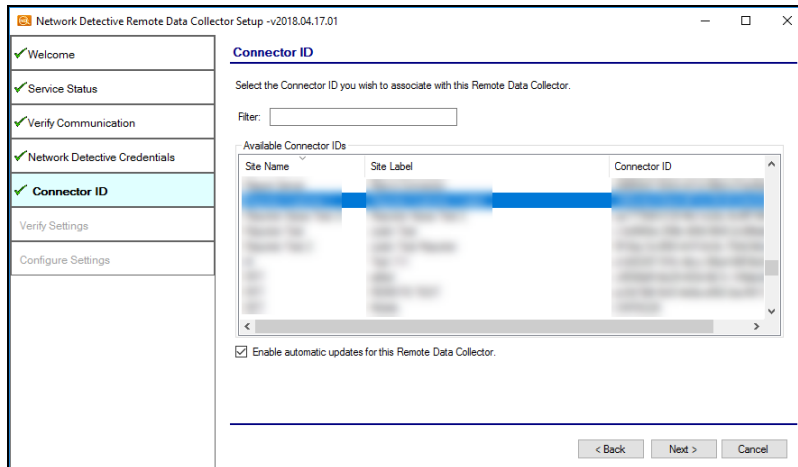


- Next you will need to link the RDC to your chosen Site in Network Detective. To do this, first enter your Network Detective credentials and click **Next**.

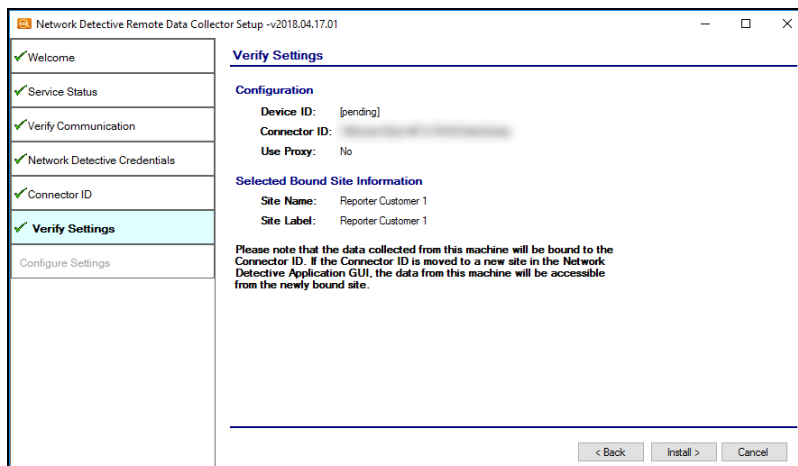


- Scroll through the list of **Sites** associated with your Network Detective account. Select the **Site/Connector ID** with which to associate the Data Collector. This will be the Reporter Site that will receive regular data from the RDC scans. Click **Next**.

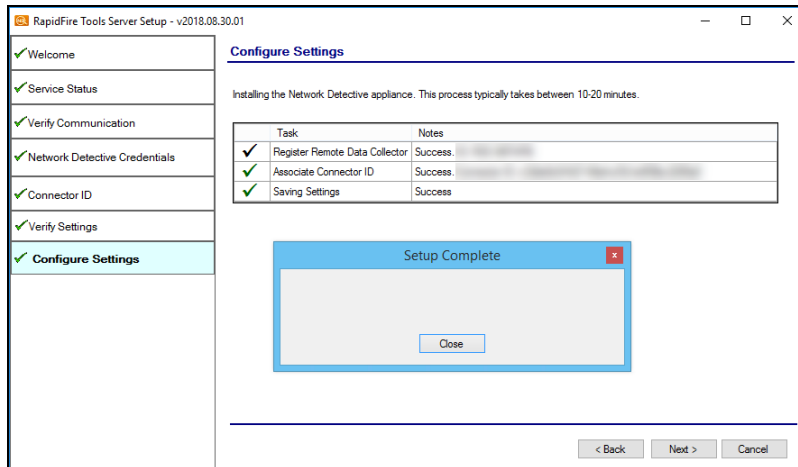
Note: You must set up a Client Connector in the Network Detective application before you can complete this step.



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



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.



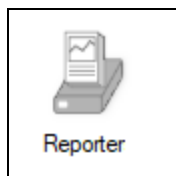
When you complete these steps, proceed to ["Configure Remote Data Collector to Perform Scan Tasks" on the next page.](#)

Configure Remote Data Collector to Perform Scan Tasks

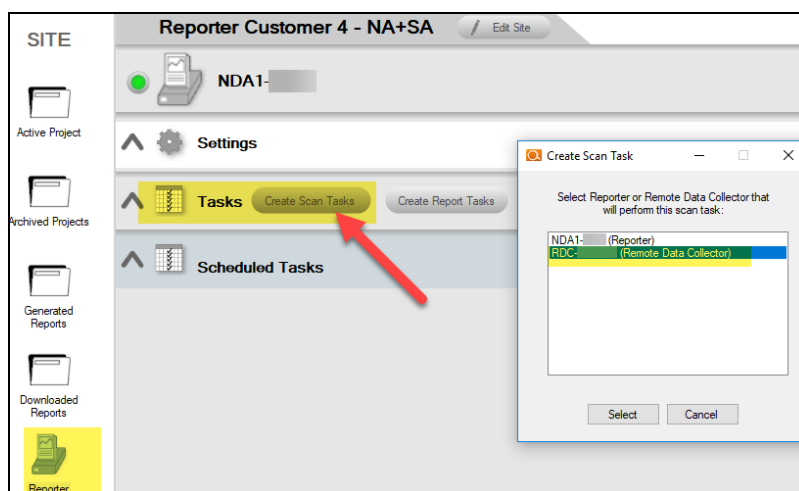
In order to generate automated assessment reports using Reporter, you will need to configure the Remote Data Collector to perform scheduled scans on the client's network. This gives Reporter the data it needs to generate documentation.

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**.



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.

The screenshot shows the 'Create Task' wizard window. On the left is a sidebar with a 'Scan Type' tab selected. The main area is titled 'Scan Type' and contains the instruction: 'Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.' Below this is a list of scan types: 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, and Local on Remote Data Collector only. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

4. Follow the wizard and enter the necessary scan settings. See ["Configuring Remote Data Collector Scans by Assessment Module" on page 90](#) for more details (Network, Security, HIPAA, PCI, Exchange, and SQL scans).

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' wizard window. On the left sidebar, 'Active Directory' is selected. The main area is titled 'Active Directory' and contains the instruction: '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.' Below this is a section 'I want to scan' with two radio buttons: 'Active Directory domain' (selected) and 'Workgroup (no domain)'. Underneath is a section 'Active Directory Credentials' with the instruction: 'If in a domain, please enter the Fully Qualified Domain Name (i.e., corp.mycorp.com instead of the shortened name - MYCO)'. It includes input fields for 'Username:' (with a hint '(domain\user)'), 'Password:', and 'Domain Controller:'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

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

Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Man...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IP...	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...	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

OK Cancel

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...	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 90](#) 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 17](#)
- ["Initial Remote Data Collector Set Up" on page 22](#)
- ["Configure Remote Data Collector to Perform Scan Tasks" on page 31](#)

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**.

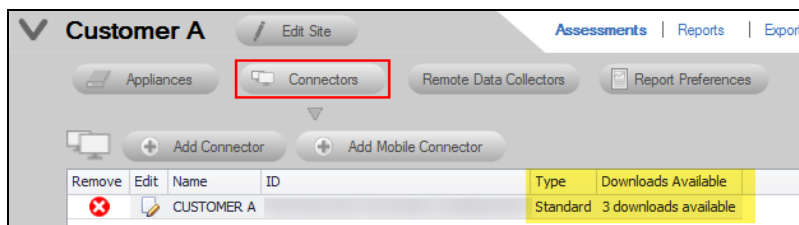
Tip: See ["Client-Connector Diagram" on page 271](#) for a helpful picture of how this process works.

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.

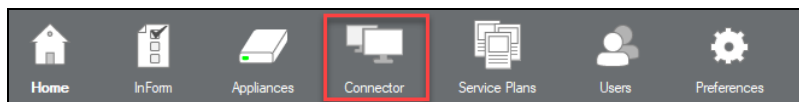


4. Click **Connectors**.
5. View the **Connectors** associated with the **Site**.
6. View the **Downloads Available** status indicator within the list of **Client-Connectors** associated with the **Site**. *If there are downloads available, this means the RDC is successfully uploading completed scans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

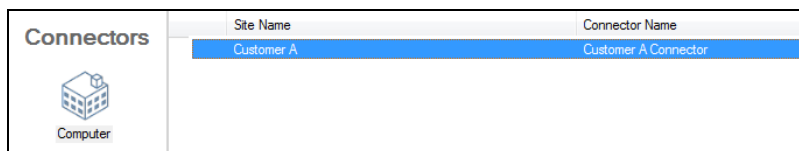


Alternatively, you can:

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**.



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**.

Connectors  Computer	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:

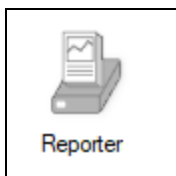
- Security Assessment Module
- HIPAA Compliance Assessment Module
- PCI Compliance Assessment Module

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.

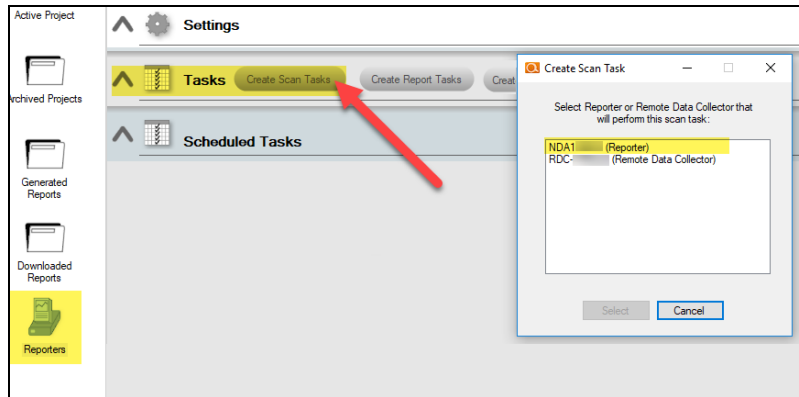
Important: You can schedule this scan to occur whenever you'd like. However, be sure to schedule the external vulnerability scan several hours BEFORE you assign Reporter to generate reports. This will ensure Reporter has the latest scan data to generate reports.

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.



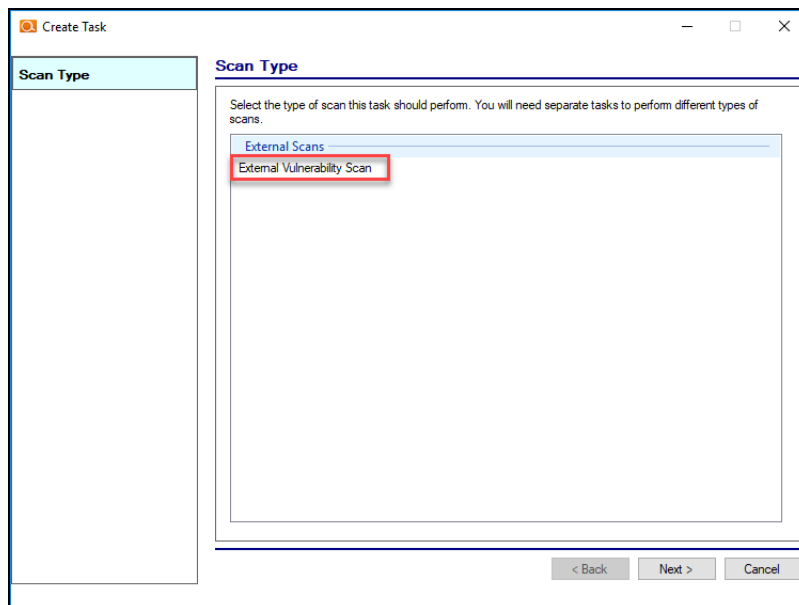
2. From the **Tasks** bar, click **Create Scan Tasks**.



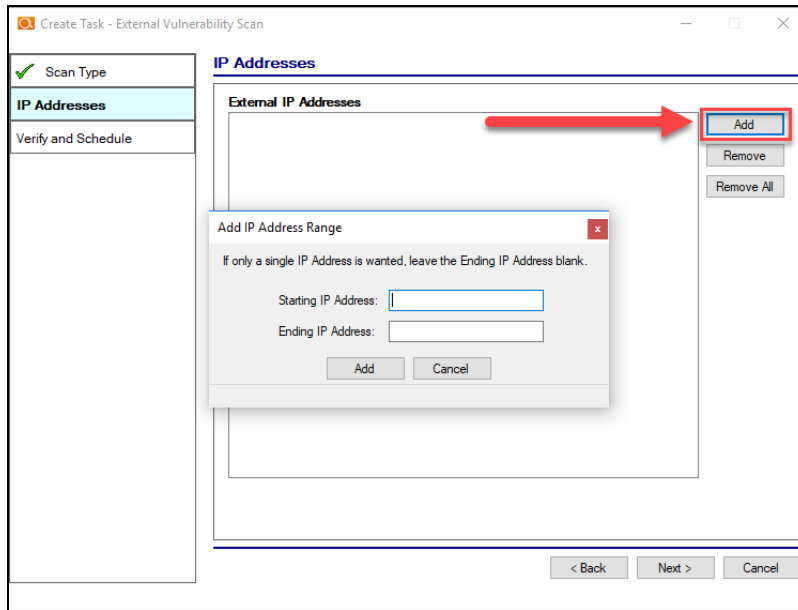
3. Select the **Reporter** available for the Site.

Set up the External Vulnerability Scan

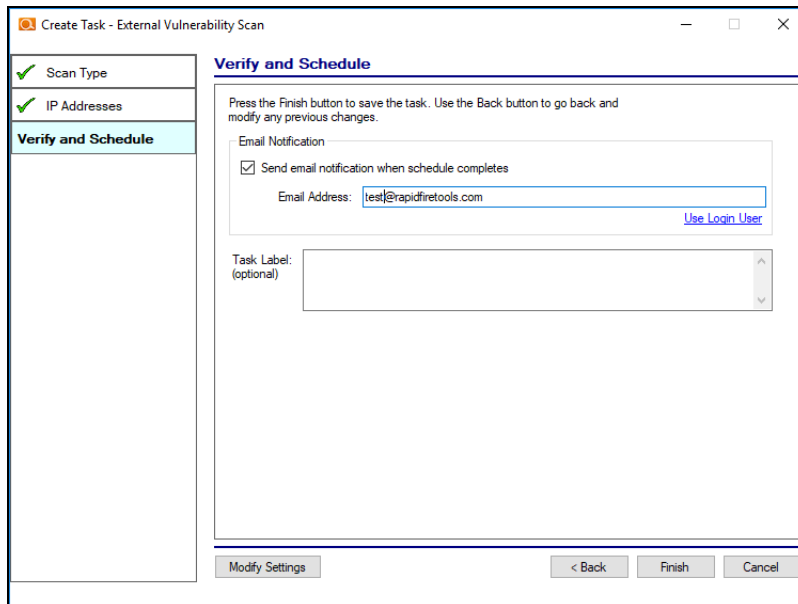
1. Choose **External Vulnerability scan** from the wizard and click the **Next** button.



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



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.

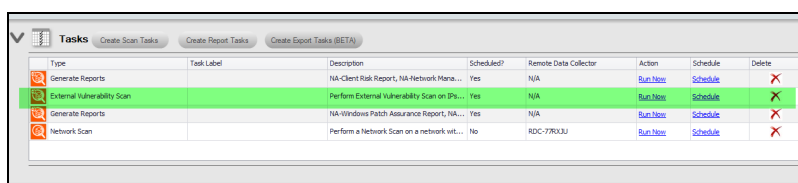


5. If an **Email Notification** should be sent after the scan is complete, then:

- 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 IP...	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 with...	No	RDC-770XU	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).

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.

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	

- 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

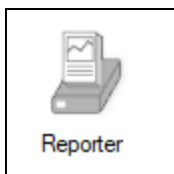
Below is an overview of the steps required to set up **Reporter** to enable **Automatic Report Generation** for the following Assessment types:

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

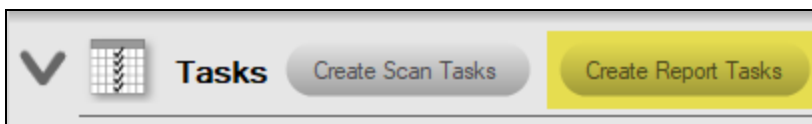
Tip: If you want to quickly set up report tasks for multiple sites, you can use ["Reporter Templates" on page 163](#).

To start setting up automated reports:

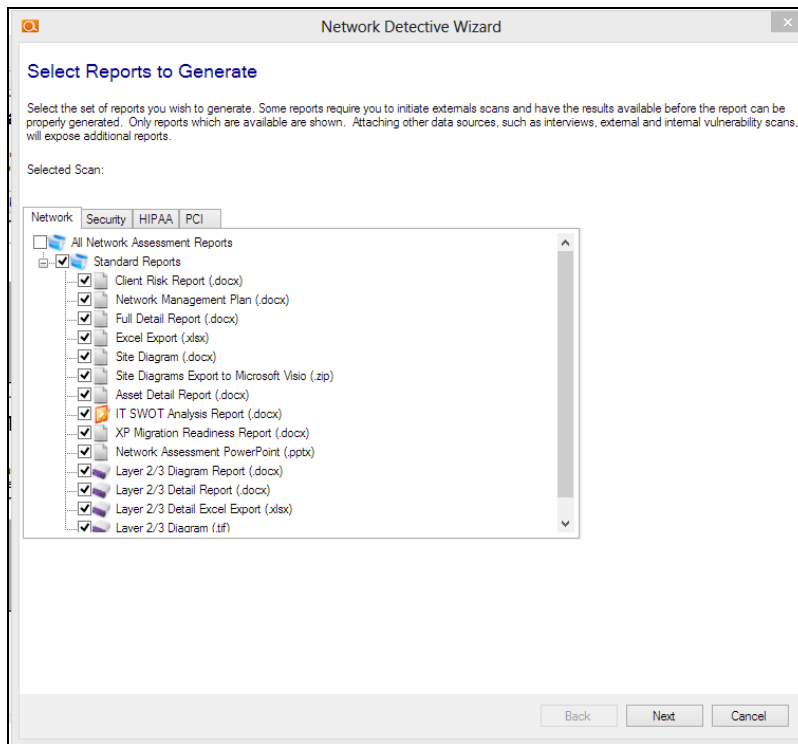
- Start** new **Assessment**, or, **Open** an **Archived Assessment** for use on your Reporter Site.
- Click on the **Reporter** icon to open the Reporter dashboard.



- 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.



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

Schedule Report Wizard

Delivery Method

1. Subject: Network Detective Notification Email

2. ☐ Attach reports to notification email

3. ☐ Copy to External Network Share

4. ☐ Upload Scan Data to InDoc [What is InDoc?](#)

5. ☐ Publish to Client Portal

6. ☐ Export to IT Glue [Choose Connection](#)

UNC Path to Share: Username: Password: Create Folder: yyyyMMdd

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

Task Label: NDHealth Cloud Reports

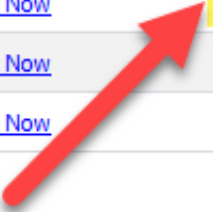
Back Next Finish

1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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

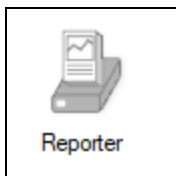
This section covers everything you need to know about setting up automatic reports using Reporter.

Network Assessment Automatic Reports

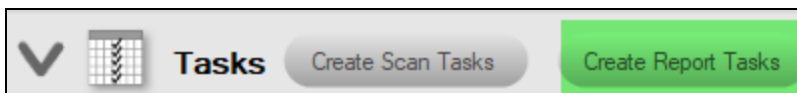
Note: Before you set up automated Network Assessment reports, be sure you set up recurring Network Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **Network/Security Assessment Scan**, 2) **Push Deploy Computer Scan**. See ["Configuring Remote Data Collector Scans by Assessment Module" on page 90](#) for instructions.

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

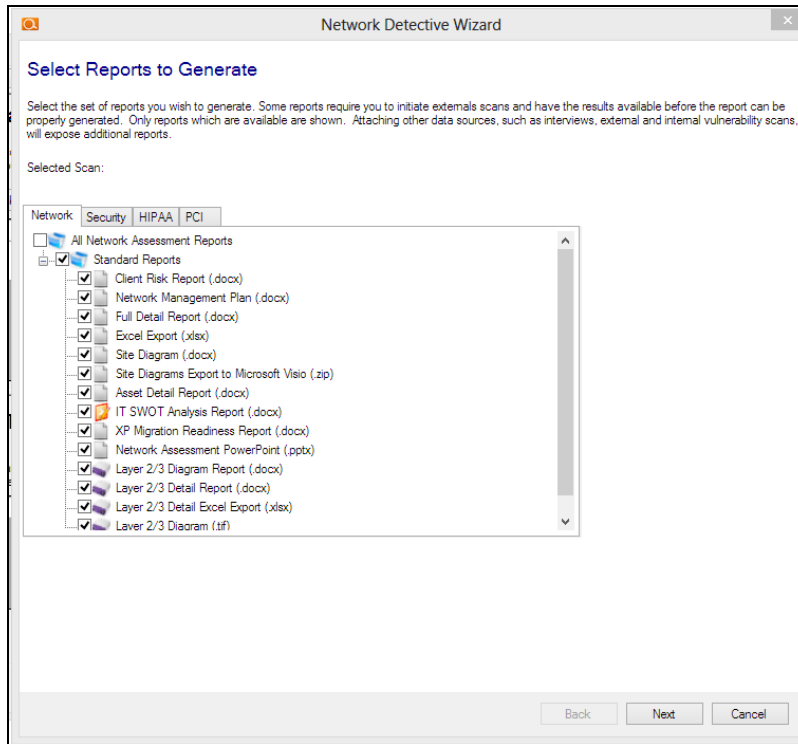
1. Click on the **Reporter** icon to open the Reporter dashboard.



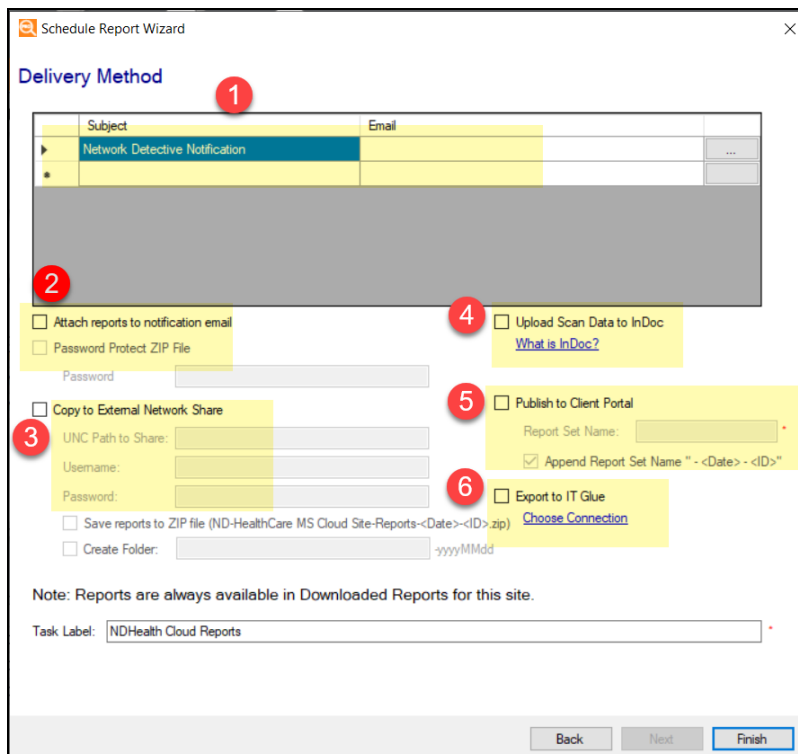
2. From the **Tasks** bar, click **Create Report Tasks**.



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



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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

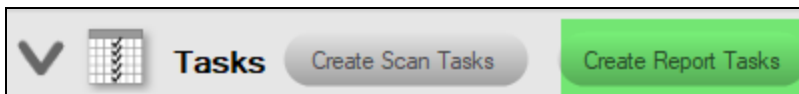
Note: Before you set up automated Security Assessment reports, be sure you set up recurring Security Assessment scans using the Remote Data Collector and Reporter appliance. This will provide the scan data for your reports. Specifically, you will need to set up a recurring: 1) **Network/Security Assessment Scan**, 2) **Push Deploy Security Scan**, 3) **External Vulnerability Scan**. See ["Configuring Remote Data Collector Scans by Assessment Module" on page 90](#) for instructions.

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

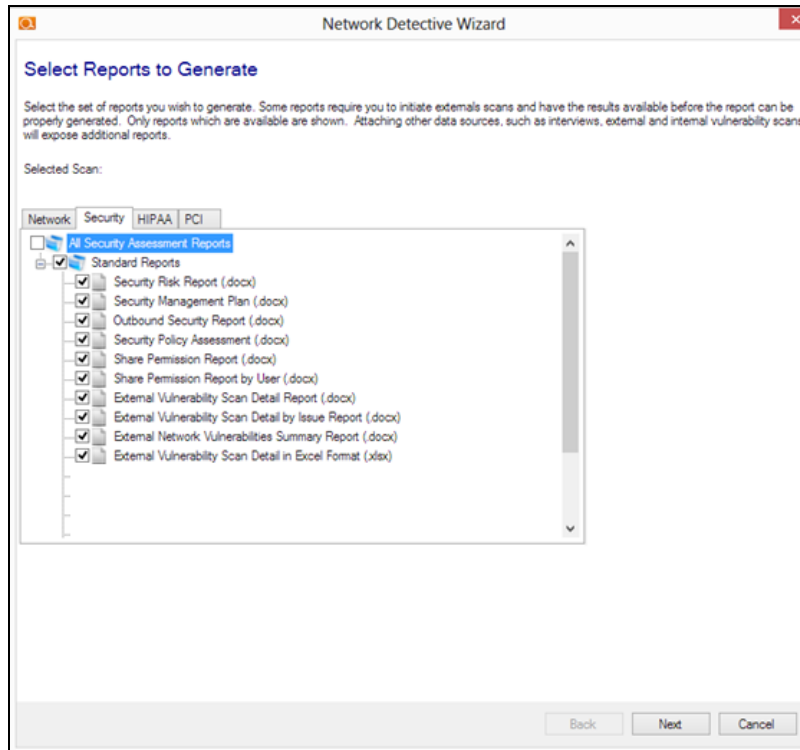
1. Click on the **Reporter** icon to open the Reporter dashboard.



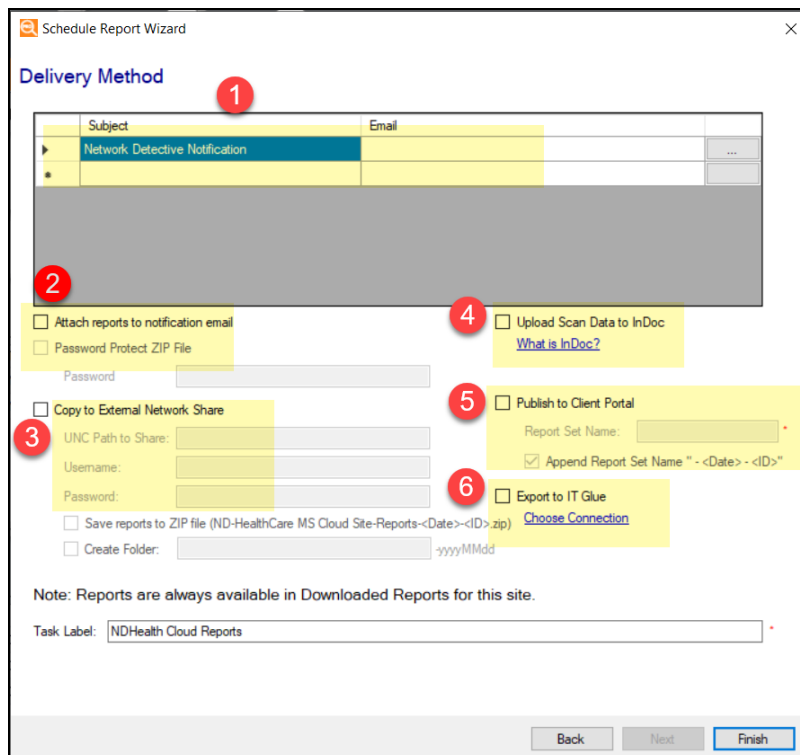
2. From the **Tasks** bar, click **Create Report Tasks**.



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



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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 124](#) 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

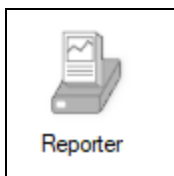
Important: You must schedule the report task to occur **AFTER** your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after**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

SQL Server Assessment Automatic Reports

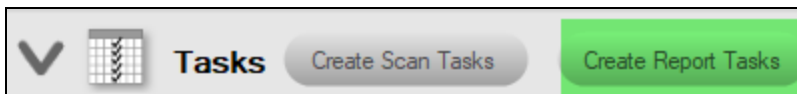
Note: Before you set up automated SQL Server assessment reports, be sure you set up recurring SQL Server Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring **SQL Server Assessment Scan**. See ["Configuring Remote Data Collector Scans by Assessment Module" on page 90](#) for instructions.

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

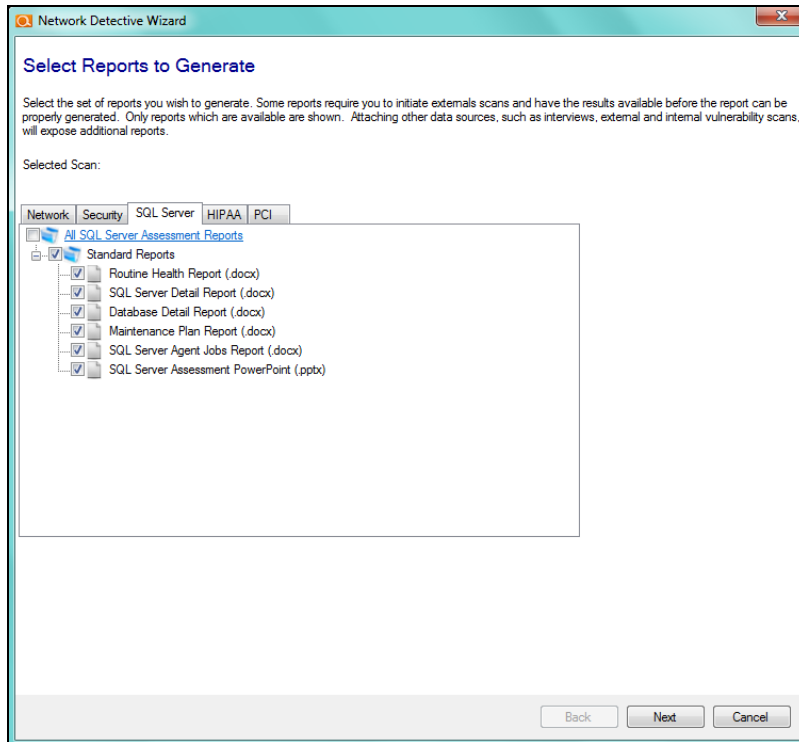
1. Click on the **Reporter** icon to open the Reporter dashboard.



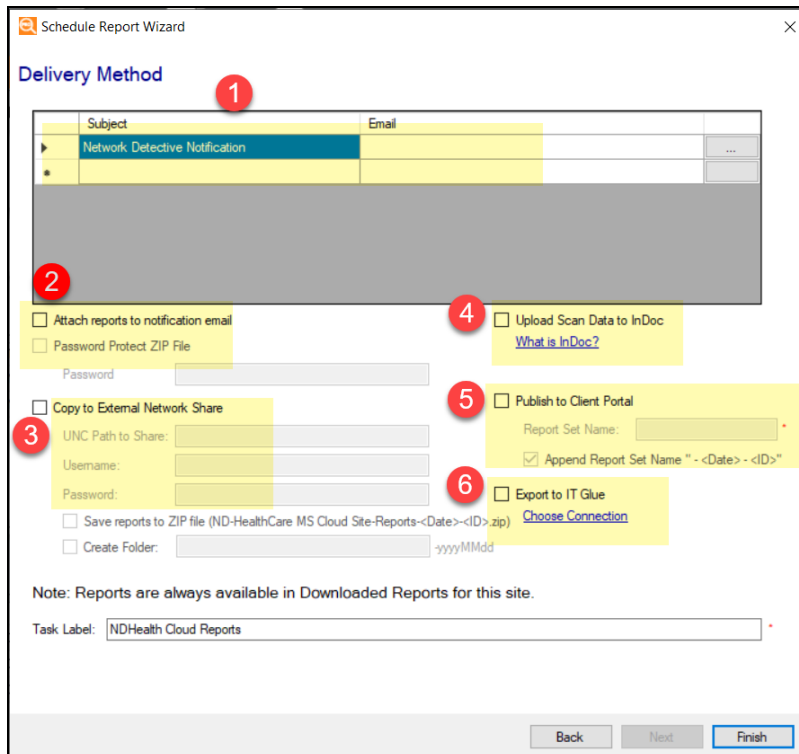
2. From the **Tasks** bar, click **Create Report Tasks**.



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.



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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 124](#) 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

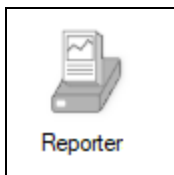
Important: You must schedule the report task to occur **AFTER** your scan tasks have completed. *This allows time for the Remote Data Collector to perform scans and upload them so that Reporter can use the latest scan data.* In general, we recommend you schedule your reports **3 or more hours after**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

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

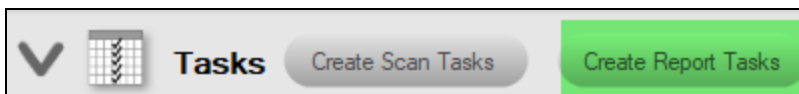
Note: Before you set up automated Exchange Assessment reports, be sure you set up recurring Exchange Assessment scans using the Remote Data Collector. This will provide the scan data for your reports. Specifically, you will need to set up a recurring **Exchange Assessment Scan**. See ["Configuring Remote Data Collector Scans by Assessment Module" on page 90](#) for instructions.

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

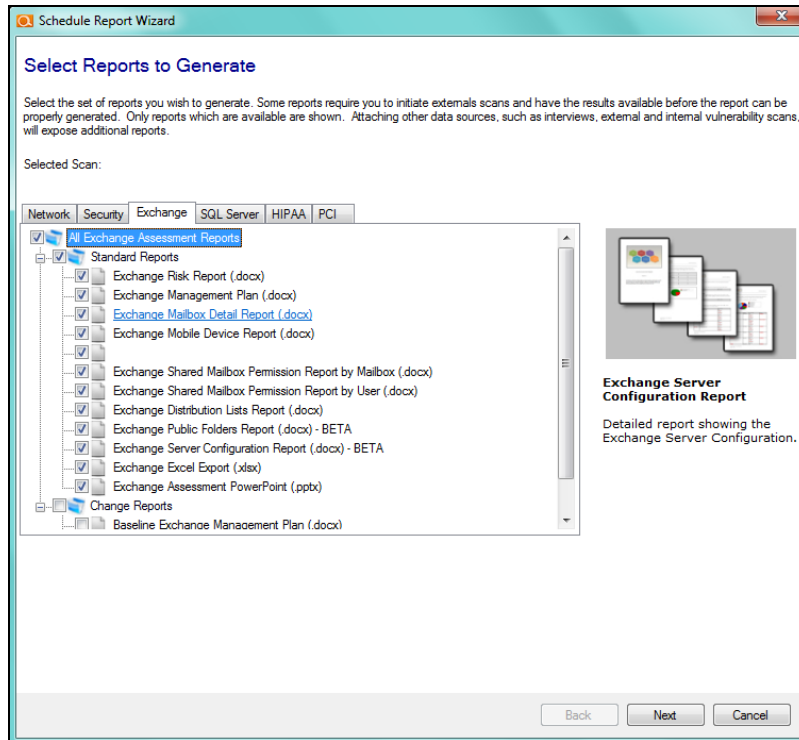
1. Click on the **Reporter** icon to open the Reporter dashboard.



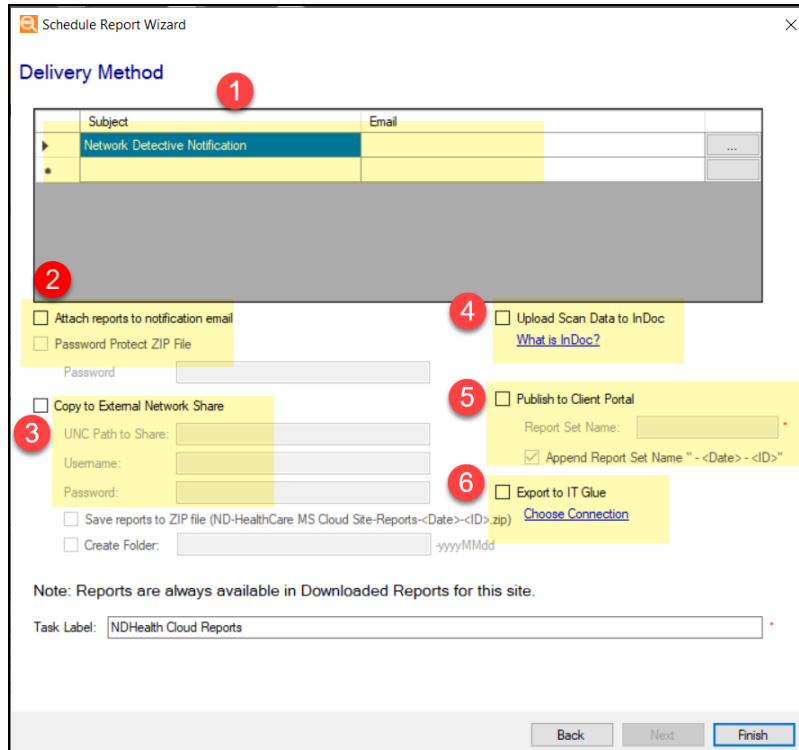
2. From the **Tasks** bar, click **Create Report Tasks**.



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



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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 124](#) 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:

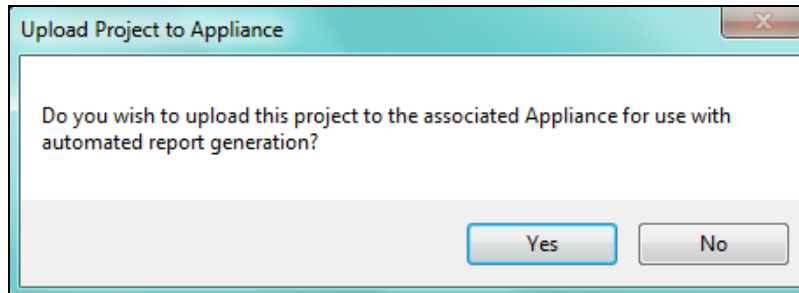
1. **Finish** the assessment, and then **Upload** the completed assessment with the Reporter appliance. This allows you use the finished assessment as the "baseline" for automated HIPAA reporting.
2. Set up recurring HIPAA assessment scans using the Remote Data Collector and Reporter. This will provide 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 90](#) 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.



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.

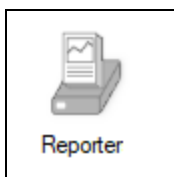
Step 2 — Create HIPAA Scan Tasks

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 90](#) for detailed instructions.

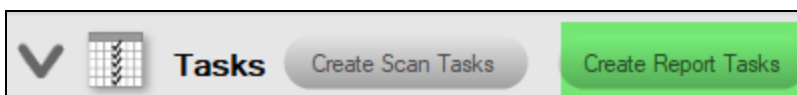
Step 3 — Create HIPAA Report Tasks

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

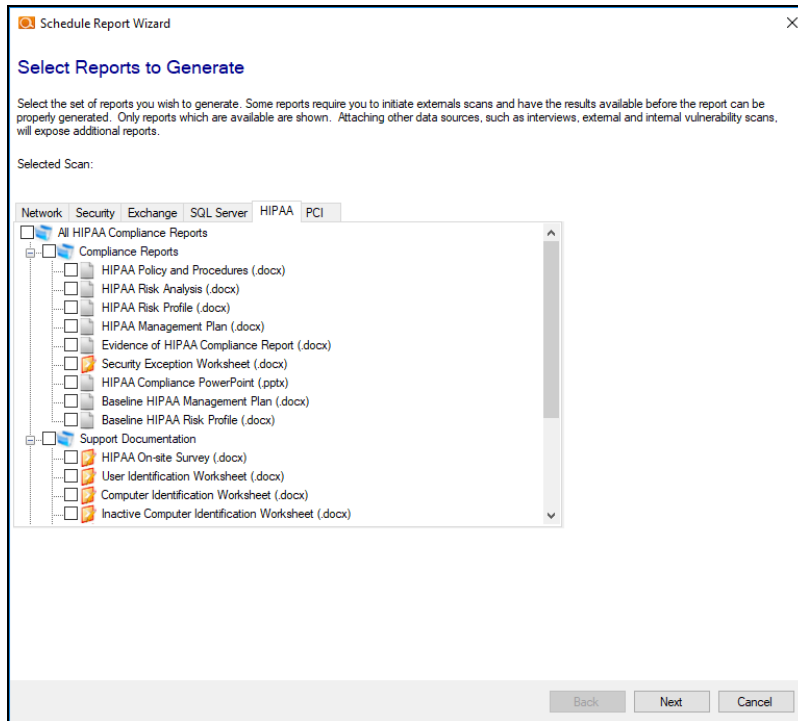
1. Click on the **Reporter** icon to open the Reporter dashboard.



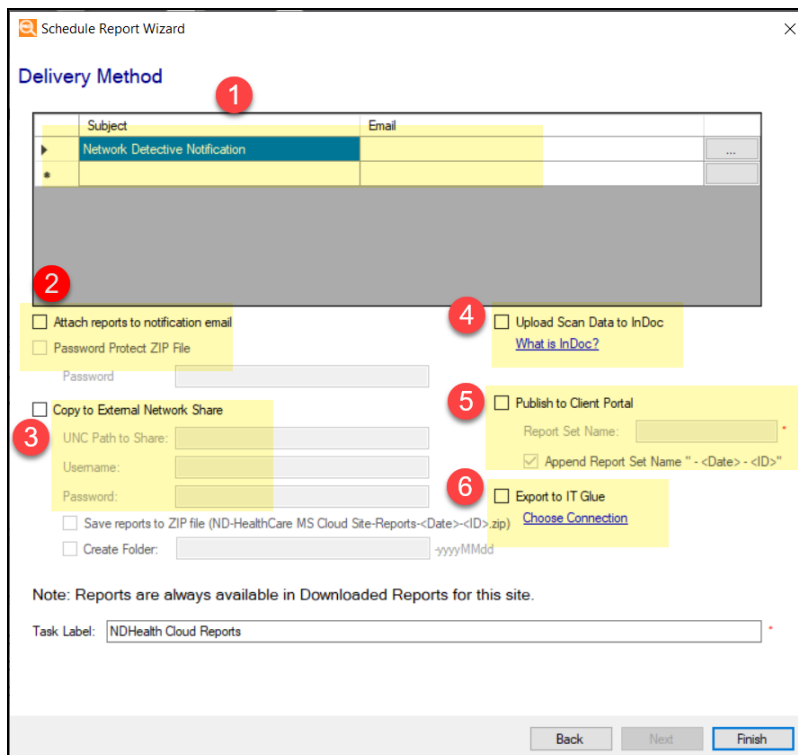
2. From the **Tasks** bar, click **Create Report Tasks**.



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.



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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 124](#) 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.

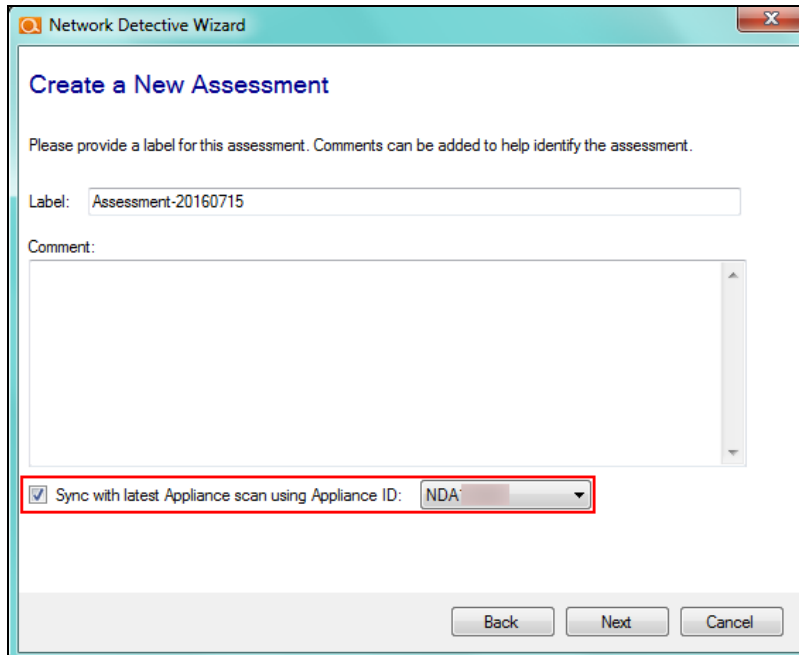
Tip: Refer to the HIPAA **Exception Report** to quickly identify where you need to manually update your HIPAA compliance documentation with notes or other information that cannot be drawn from automated scans.

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**.



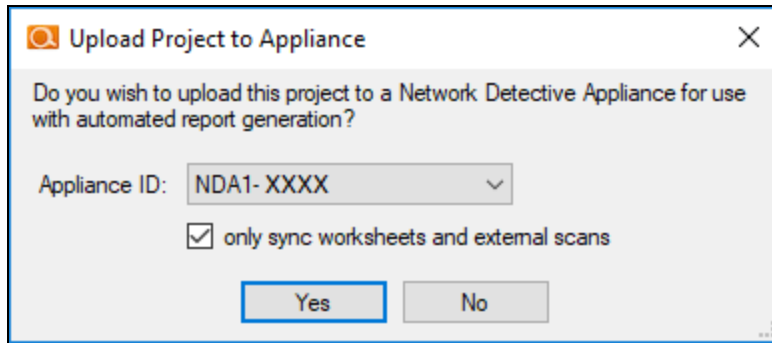
4. On the **Create New Assessment** Wizard Screen, select the checkbox to **Sync** the assessment with the **Reporter Appliance**.

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.

The screenshot shows a dialog box titled "Upload Project to Appliance" with a close button (X) in the top right corner. The main text asks, "Do you wish to upload this project to a Network Detective Appliance for use with automated report generation?". Below this, there is a label "Appliance ID:" followed by a dropdown menu showing "NDA1- XXXX" with a downward arrow. Underneath the dropdown is a checked checkbox with the text "only sync worksheets and external scans". At the bottom, there are two buttons: "Yes" and "No".

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:

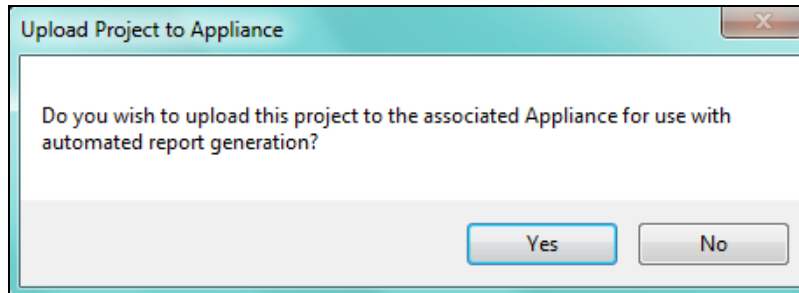
1. **Finish** the assessment, and then **upload/sync** the completed assessment with the Reporter appliance. This allows you use the finished assessment as the "baseline" for automated PCI reporting.
2. Set up recurring PCI assessment scans using the Remote Data Collector and Reporter. This will provide 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 90](#) 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.



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.

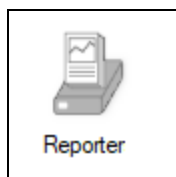
Step 2 — Create PCI Scan Tasks

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 90](#) for detailed instructions.

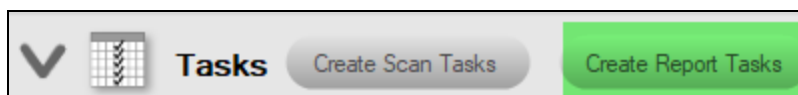
Step 3 — Create PCI Report Tasks

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

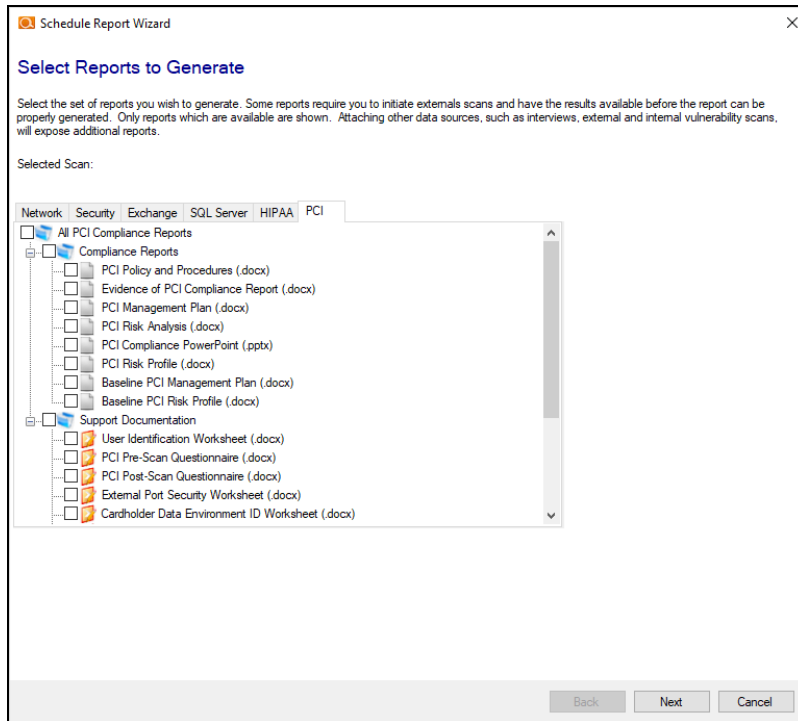
1. Click on the **Reporter** icon to open the Reporter dashboard.



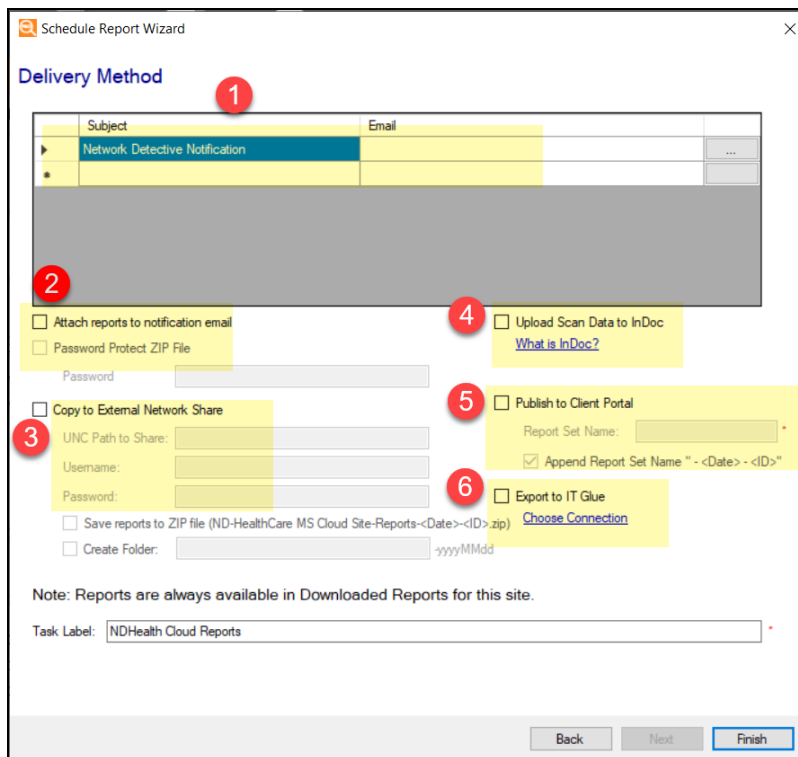
2. From the **Tasks** bar, click **Create Report Tasks**.



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.



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



1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. ["Copy Reports to External Network Share with Reporter" on page 79](#)
4. 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 124](#) for more on how to set up InDoc.
5. Publish documents to the Client Portal. See ["RapidFire Tools Portal Client View for Reporter" on page 154](#).
6. [Export Network Detective Report Tasks to IT Glue with Reporter](#)

Important: Note that some of these features are only available with Network Detective Pro.

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 124](#) 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.

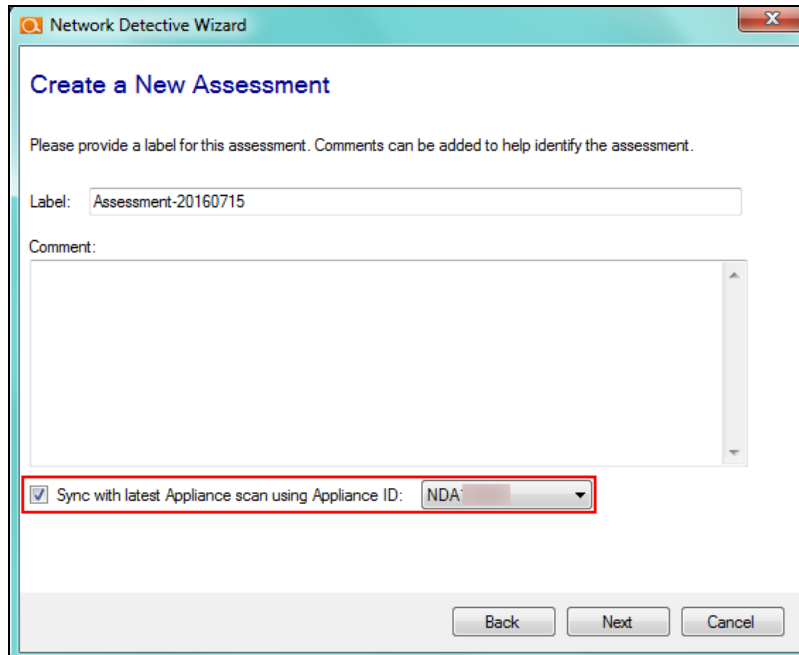
Tip: Refer to the PCI **Exception Report** to quickly identify where you need to manually update your PCI compliance documentation with notes or other information that cannot be drawn from automated scans.

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.**



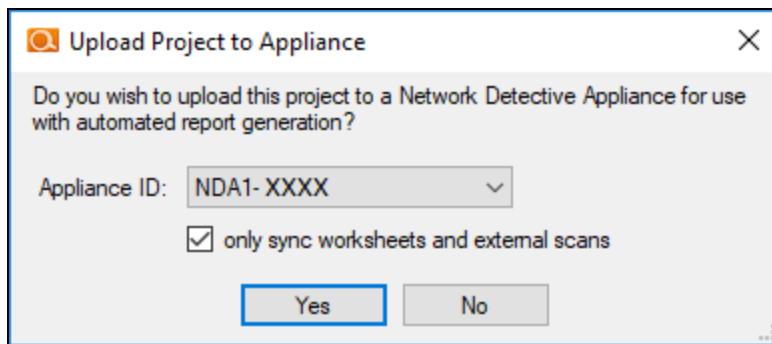
4. On the **Create New Assessment** Wizard Screen, select the checkbox to **Sync** the assessment with the **Reporter Appliance**.

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.

The screenshot shows a dialog box titled "Upload Project to Appliance" with a close button (X) in the top right corner. The main text asks: "Do you wish to upload this project to a Network Detective Appliance for use with automated report generation?". Below this, there is a label "Appliance ID:" followed by a dropdown menu showing "NDA1- XXXX" with a downward arrow. Underneath the dropdown is a checked checkbox with the text "only sync worksheets and external scans". At the bottom, there are two buttons: "Yes" and "No".

Synchronizing Assessment Projects with Reporter

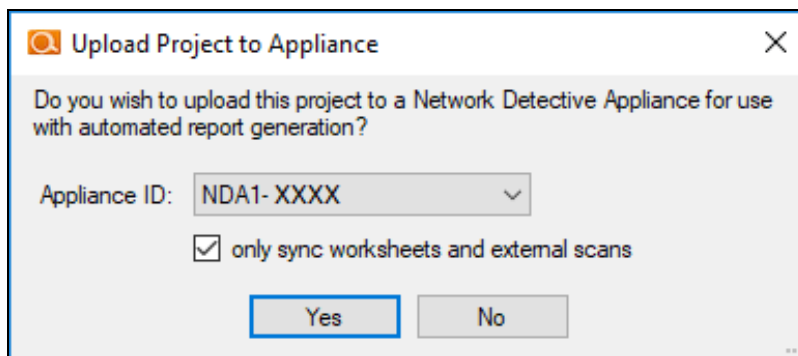
Reporter allows you to upload a finished project to the appliance in order to automate assessments and report generation. Uploading a project has several functions:

- 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.



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

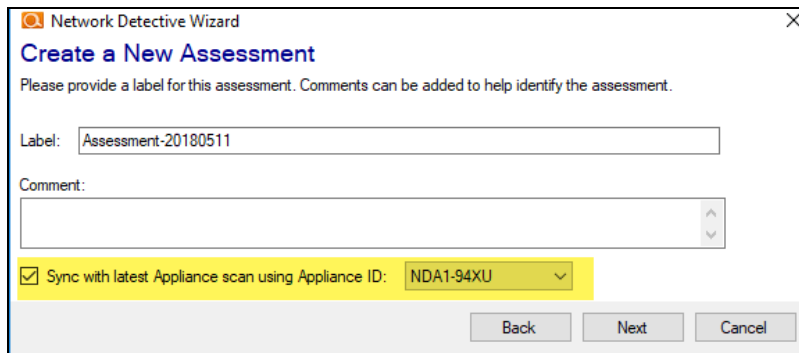
Note: We recommended you keep this option selected unless you wish to include or remove specific scan files.

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 facing 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**.

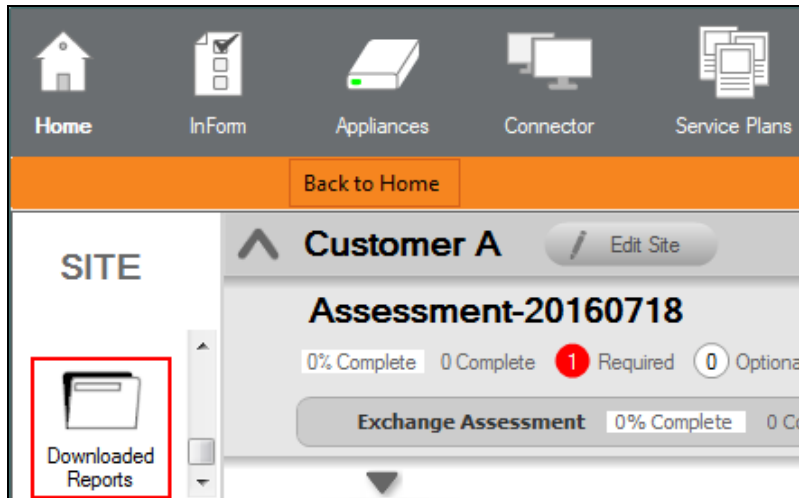


3. Select the Reporter **Appliance** from which to get the latest data
4. Click **Next** and continue creating the new assessment. Your new assessment will be pre-populated with the data from the appliance.

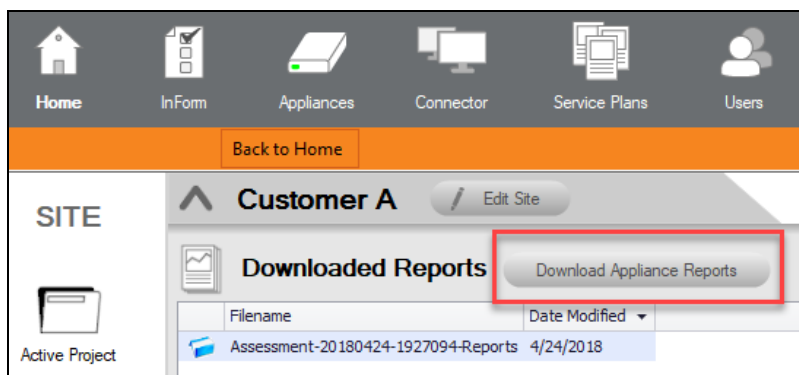
Manually Download Reports (Reporter)

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

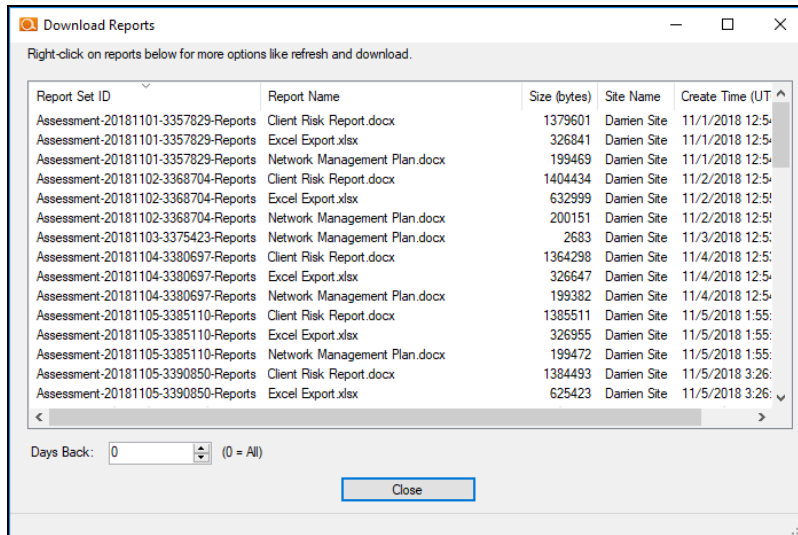
1. **Open the Site Associated with Reporter.**
2. Select the **Downloaded Reports** Icon on the left side of the Network Detective window to display the **Download Reports** button in the Network Detective window.



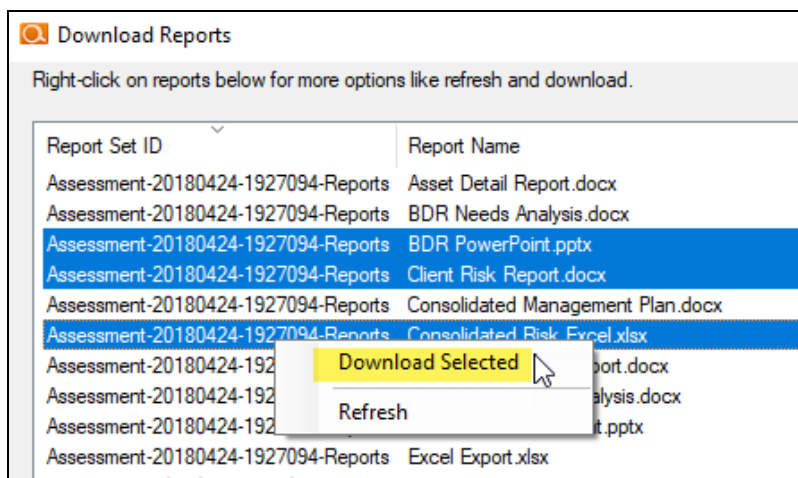
3. View the list of generated reports by selecting the **Download Appliance Reports** button that appeared at the top of the Network Detective window.



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

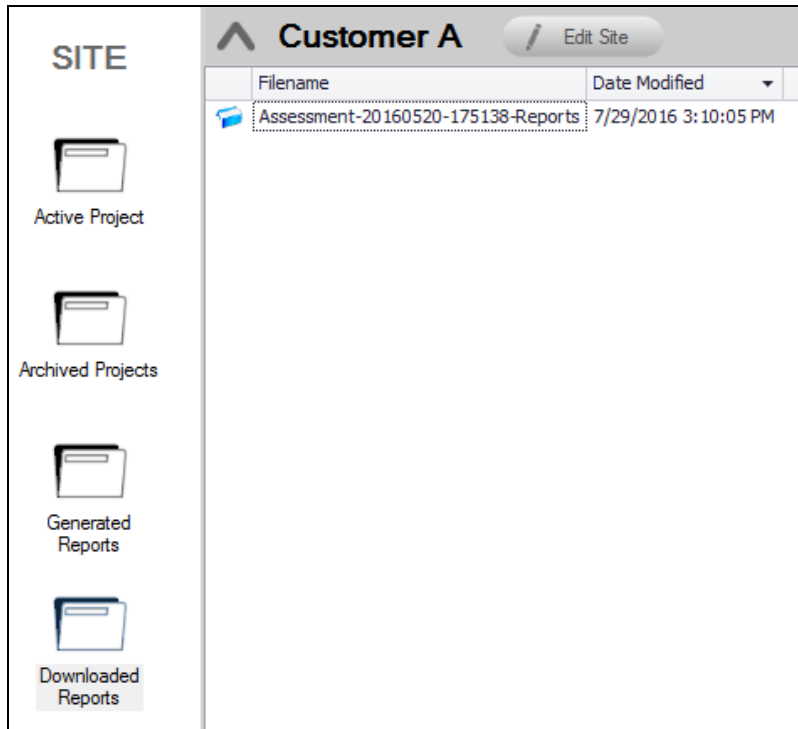


5. Select one or more reports. Right click and select Download Selected.



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.

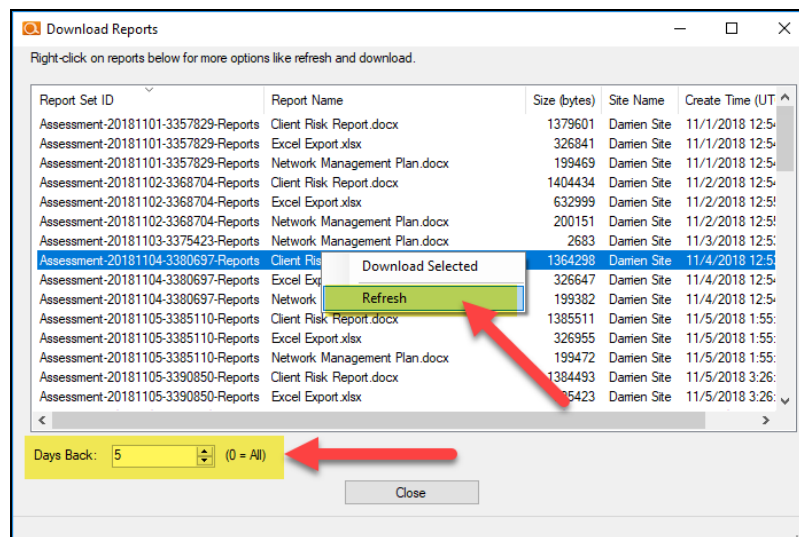


Double click on the **Assessment** report's **Filename** to open and view the report.

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.

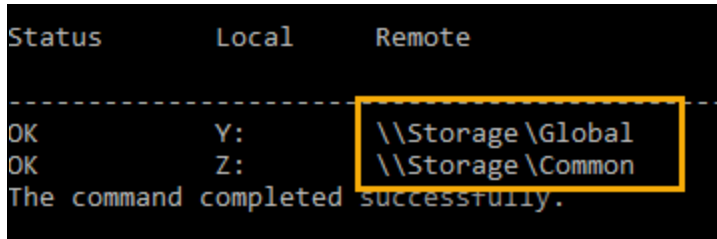


The list of reports will then be limited to the specified number of days back.

Copy Reports to External Network Share with Reporter

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

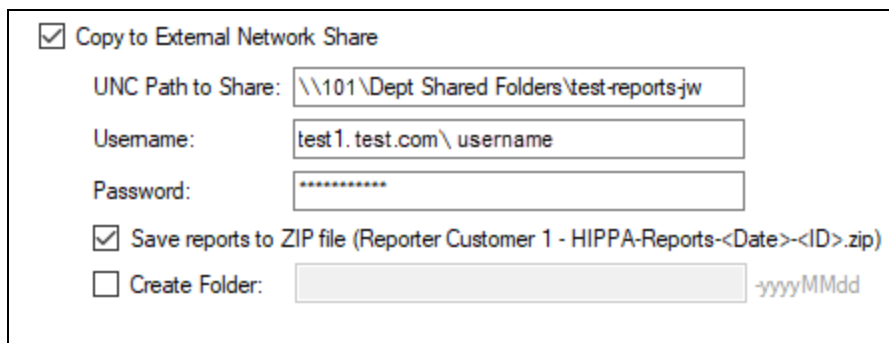
1. You must enter the correct UNC path to the external share. On a computer that has access to the external share, open a command prompt and type "net use." A list of external network shares will appear. If you do not see your external share, be sure it is mapped correctly.



```
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:

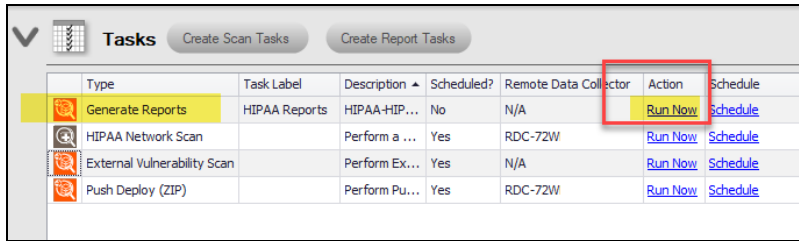
Username:

Password:

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

☐ Create Folder:

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



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.

Automate Vulnerability Reports with VulScan

With VulScan and Reporter, you can automate your internal and external vulnerability reporting. This requires that you have several components setup and running. These are:

- VulScan site with internal and/or external scan appliance
- Network Detective site with associated VulScan and Reporter appliance

Follow these steps to enable automated vulnerability reports:

- ["Step 1 — Create Scan Tasks from VulScan Site" below](#)
- ["Step 2 — Create Vulnerability Report Tasks" on page 88](#)
- ["Step 3 — Download Reports from VulScan Appliance in Network Detective" on page 89](#)

Step 1 — Create Scan Tasks from VulScan Site

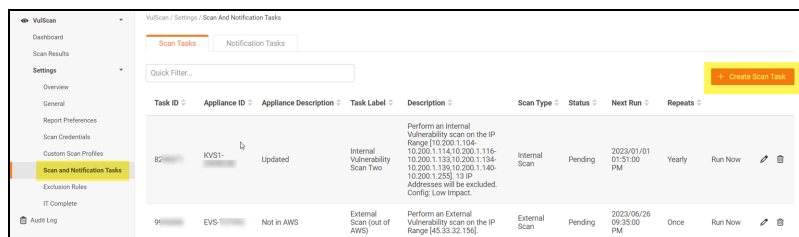
First be sure that your VulScan scan tasks are set up and scheduled to run. You can automate reporting for both internal and external vulnerabilities.

- ["Create Internal Scan Task" below](#)
- ["Create External Scan Task" on page 85](#)

Create Internal Scan Task

In order to collect vulnerability data from the target network, you need to set up scan tasks. Follow these steps to create an internal vulnerability scan task with VulScan:

1. From your site, go to **Vulnerability Scanner > Settings > Scan and Notification Tasks**.
2. From the **Scan Tasks** tab, click **Create Scan Task**.



3. From Scan Type, select **Internal Vulnerability Scan** and click next.

Create Scan Task

Select Scan Type

Select the type of scan to be scheduled.

☒ Internal Vulnerability Scan

☐ External Vulnerability Scan

Cancel Previous Next

4. Select the Appliance from the drop-down menu and click **Next**.

Create Scan Task

Vulnerability Scanner Appliance

Select Appliance for this Scan Task.

NDA1-96

NDA1-97 Primary IP Scanner - Main Office

Cancel Previous Next

5. Select the **Scan Profile**.

Create Scan Task

Select Scan Profile

We strongly recommend using the Low Impact or Standard Scan to start your Internal Vulnerability assessment. Selecting a Comprehensive Scan will significantly increase scan time.

Any scan will create increased load and could affect performance on systems with existing vulnerabilities while the scan is running. For minimal impact, we recommend selecting Low Impact and running scans during non-working hours. Scans may take several hours to complete and possibly days for very large networks when selecting a Comprehensive Scan.

☒ **Low Impact Scan**
Standard TCP ports and Top 1000 UDP. Does not include brute force login attempts.

☐ **Standard Scan**
Standard TCP ports and Top 1000 UDP

☐ **Comprehensive Scan**
All TCP (1-65535) and Top 1000 UDP
NOTE: Comprehensive scans may take a significant amount of time and incur increased load on the network.

☐ **Custom**
Scan Profile: Select a Custom Scan Profile Create Profile Refresh

Cancel Previous Next

The available options are in the table below. Click **Next**.

Scan Profile	Description	Notes
Low Impact Scan	Standard TCP ports and Top 1000 UDP	Does not include brute force login attempts
Standard Scan	Standard TCP	

Scan Profile	Description	Notes
	ports and Top 1000 UDP	
Comprehensive Scan	All TCP (1-65535) and Top 1000 UDP	Comprehensive scans may take a significant amount of time and incur increased load on network

6. Next select **IP ranges**. The VulScan appliance will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

Important: Do not use multiple appliances to scan the same subnet or IP range. This may produce errors in your scan results.

From this screen you can also:

- Click **Reset to Auto-detected** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

Note: Key network component IP addresses should be excluded in order to prevent scans being performed from impacting the performance of a device when it is being scanned. For example, a company might want to exclude the IP Address range for their voice over IP telephone system if they are performing a scan during business hours.

Tip: If you are using multiple appliances to perform internal vulnerability scans for a site, define a sub-set of the IP range for the scan task. Create multiple scan tasks to distribute the work between the available appliances.

7. Click **Next Page** once you have configured the IP ranges for the scan.
8. From the **Verify and Schedule** menu, configure the scan task:

The screenshot shows a web form titled "Create Scan Task" with a sub-section "Verify and Schedule". The form contains the following fields and options:

- Email Notification:** A checkbox labeled "Send email notification when schedule completes" is unchecked. Below it is a text input field for "Email Address".
- Task Label:** A text input field.
- Time Zone:** A dropdown menu currently showing "(UTC-05:00) Eastern Time (US & Canada)".
- Schedule:** A section with a dropdown set to "Every", a "Select interval" input field, the word "at", and a time picker set to "12:00 AM".
- Vulnerability Scan Setting:** Two checkboxes: "Enable Scan Task" (checked) and "Skip devices with all ports filtered" (unchecked).
- Buttons:** "Cancel", "Previous", and "Save" buttons are at the bottom right.

- a. Select whether to send an **email notification** when the scan completes — then enter an email recipient for the notification.
 - b. Enter a **task label** to describe the scan task.
 - c. Select the **time zone** from the drop-down menu.
 - d. Next choose a day and time to **schedule** the scan.
 - e. Choose whether to **skip devices that have all ports filtered**.
9. Click **Save**.

The internal vulnerability Scan Task will be created. You can see the details for the task in the scan tasks table.

Task ID	Appliance ID	Appliance Description	Task Label	Description	Scan Type	Status	Next Run	Repeats
8298471	KVS1	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10.200.1.104-10.200.1.133] 13 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Queued	01/01/2024 11:51:00 AM	Yearly Run Now

Create External Scan Task

Note: Before you can create an external vulnerability scan task, you first need to provision and install an external vulnerability scan appliance.

Follow these steps to create an external vulnerability scan task with VulScan:

1. From your site, go to **Vulnerability Scanner > Settings > Scan and Notification Tasks**.
2. From the **Scan Tasks** tab, click **Create Scan Task**.

Task ID	Appliance ID	Appliance Description	Task Label	Description	Scan Type	Status	Next Run	Repeats
8298471	KVS1	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10.200.1.104-10.200.1.133] 13 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Pending	2023/01/01 01:51:00 PM	Yearly Run Now
9100000	EVS1	Not in AWS	External Vulnerability Scan (out of AWS)	Perform an External Vulnerability scan on the IP Range [45.83.35.156]	External Scan	Pending	2023/06/26 09:35:00 PM	Once Run Now

3. From Scan Type, select **External Vulnerability Scan** and click **Next**.

Create Scan Task

Select Scan Type

Select the type of scan to be scheduled.

☐ Internal Vulnerability Scan

☒ External Vulnerability Scan

Cancel Previous Next

4. Select the Appliance from the drop-down menu and click **Next**.



Create Scan Task

Vulnerability Scanner Appliance

Select Appliance for this Scan Task.

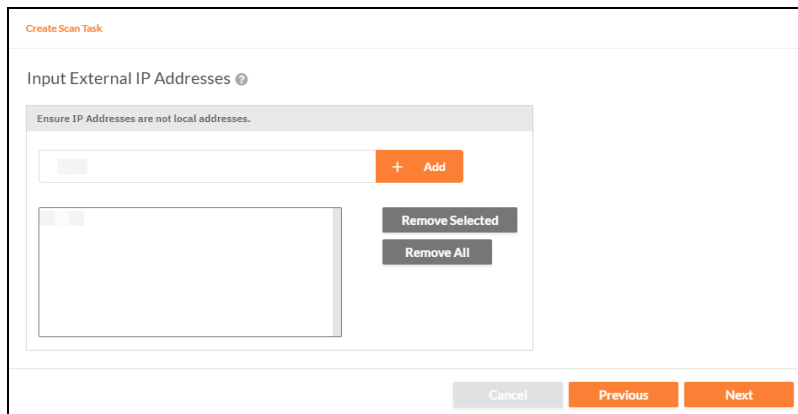
EVS-FFLW76

Cancel Previous Next

5. Enter the IP addresses for the external vulnerability scan. Click **Next Page**.

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.

Note: IP ranges for the external vulnerability scan are not supported at this time. Please enter individual IPs for the external scan.



Create Scan Task

Input External IP Addresses ⓘ

Ensure IP Addresses are not local addresses.

+ Add

Remove Selected

Remove All

Cancel Previous Next

6. From the **Verify and Schedule** menu, configure the scan task:

Create Scan Task

Verify and Schedule

Email Notification

☐ Send email notification when schedule completes

Email Address

Task Label

Time Zone

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

Schedule

Every at 12:00 AM 🕒

Vulnerability Scan Setting

☒ Enable Scan Task

☐ Skip devices with all ports filtered

Cancel Previous Save

- Select whether to send an **email notification** when the scan completes — then enter an email recipient for the notification.
- Enter a **task label** to describe the scan task.
- Select the **time zone** from the drop-down menu.
- Next choose a day and time to **schedule** the scan.

7. Click **Save**.

The external vulnerability Scan Task will be created. You can see the details for the task in the scan tasks table.

Vulnerability Scanner > Settings > Scan And Notification Tasks

Scan Tasks Notification Tasks

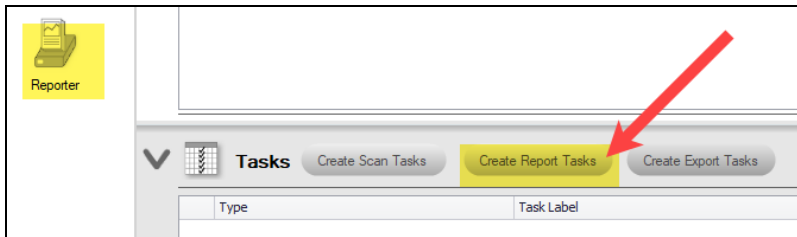
Quick Filter...

+ Create Scan Task

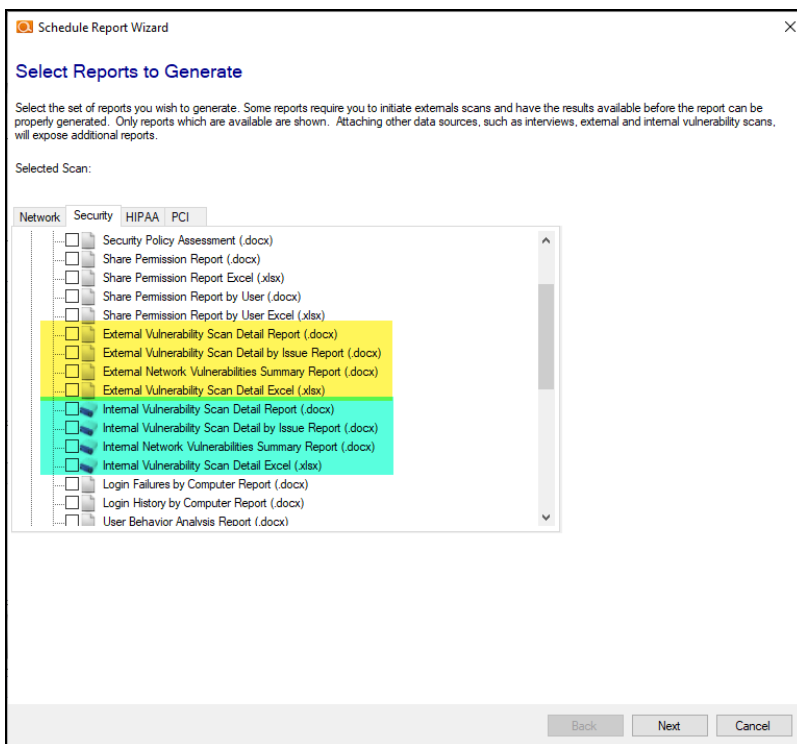
Task ID	Appliance ID	Appliance Description	Task Label	Description	Scan Type	Status	Next Run	Frequency	Actions
			Standard External Vulnerability Scan	Perform an External Vulnerability scan on the IP Range. No IP Addresses will be excluded. Config: Low Impact.	External Scan	Pending	09-Sep-2021 12:00:00 AM	Daily	Run Now ✎ ⌵

Step 2 — Create Vulnerability Report Tasks

1. From your Network Detective site, open the Reporter console and click **Create Report Tasks**.



2. From the **Security** tab, select the internal and/or external reports that you wish to automate. Click Next.



3. Configure the delivery method and schedule the reports to begin a few hours after your internal or external scan will have finished.

Step 3 — Download Reports from VulScan Appliance in Network Detective

Once your report tasks finish, open the Reporter console for your site and ["Manually Download Reports \(Reporter\)" on page 75](#).

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 17](#).

Network and Security Assessment Scan

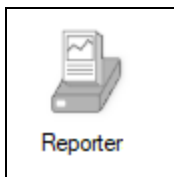
Set up a recurring Network/Security Assessment scan to collect data for automatic Network and Security Assessment reports.

Configure the network scan using the wizard.

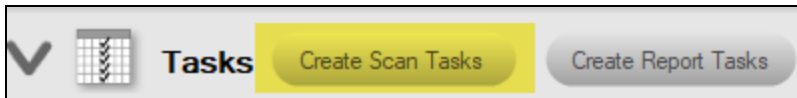
- Look here if you are ["Scanning an Active Directory Domain Network" below](#)
- Look here if you are ["Scanning a Workgroup Network" on page 98](#)

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.

The 'Create Task' dialog box is shown with the 'Scan Type' tab selected. On the left is a vertical list of scan types: Active Directory, Local Domains, Additional Credentials, External Domains, IP Ranges, SNMP Information, VMware, and Verify and Schedule. The main area on the right is titled 'Scan Type' and contains a list of scan types under the heading 'IT Assessment'. The 'Network Scan (Network/Security Modules)' option is highlighted in blue. Other options include SQL Server Collection, Exchange Server Collection, HIPAA Compliance, HIPAA Network Scan, PCI Compliance, PCI Network Scan, Local Scans, Push Deploy, and Local on Remote Data Collector only. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

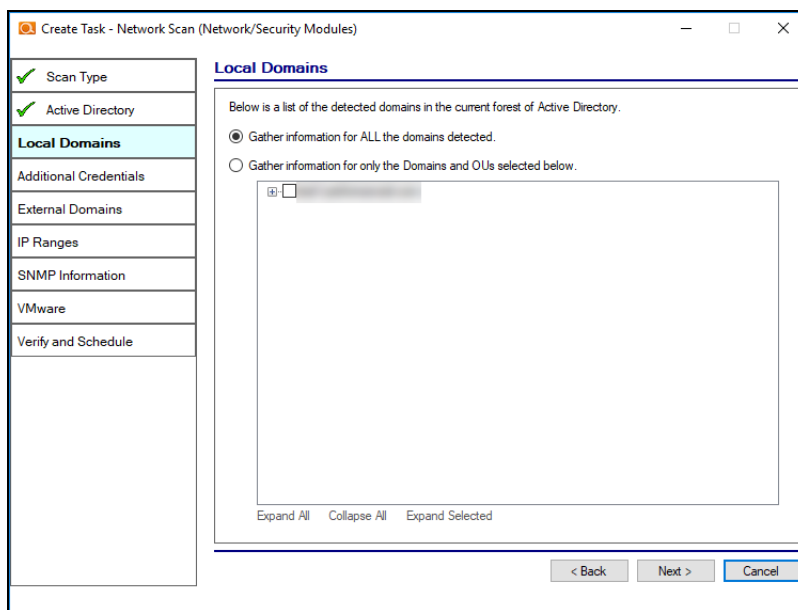
4. Select the type of network you want to scan: **Active Directory Domain**.

The 'Create Task - Network Scan (Network/Security Modules)' dialog box is shown with the 'Active Directory' tab selected. On the left is a vertical list of scan types: Scan Type (checked), Active Directory (highlighted), Local Domains, Additional Credentials, External Domains, IP Ranges, SNMP Information, VMware, and Verify and Schedule. The main area on the right is titled 'Active Directory' and contains instructions: 'Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.' Below this are two radio buttons: 'Active Directory domain' (selected) and 'Workgroup (no domain)'. Under the 'Active Directory Credentials' section, there is a note: 'If in a domain, please enter the Fully Qualified Domain Name (i.e., corp.mycorp.com instead of the shortened name - MYCORP)'. There are three input fields: 'Username:' (with a placeholder '(domain\user)'), 'Password:', and 'Domain Controller:'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

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.

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.



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**.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window. On the left is a sidebar with a list of modules: Scan Type, Active Directory, Local Domains, Additional Credentials (highlighted), External Domains, IP Ranges, SNMP Information, VMware, and Verify and Schedule. The main area is titled 'Additional Credentials (optional)' and contains a text box explaining that network scan credentials are required for remote Windows data collection via WMI and Remote Registry. Below this is a form for 'Network Scan Credentials' with fields for 'Username:' and 'Password:', an 'Add' button, and a note '(AD user to be used first)'. At the bottom of the main area is a 'Clear All' button. At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

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

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window with the 'External Domains' tab selected. The sidebar on the left is the same as in the previous screenshot. The main area is titled 'External Domains' and contains a text box explaining that external domains are used for WHOIS, MX (mail) record detection, and Dark Web scans. Below this is a form with a 'Domain' input field and an 'Add' button. At the bottom of the main area is a 'Clear All Entries' button. At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

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.

The screenshot shows a software window titled "Create Task - Network Scan (Network/Security Modules)". On the left is a sidebar with a list of modules: "Scan Type", "Active Directory", "Local Domains", "Additional Credentials", "External Domains", "IP Ranges" (which is highlighted in blue), "SNMP Information", "VMware", and "Verify and Schedule". The main area of the window is titled "IP Ranges". It contains two text boxes: "Auto-Detected IP Ranges on Remote Appliance" and "IP Ranges to Scan". The "Auto-Detected" box contains the text "10.200.1.0-". The "IP Ranges to Scan" box has a header "Example IP Range Format: 192.168.0.0-192.168.0.255" and a sub-header "Single IP or IP Range" with an "Add" button next to it. Below this, the same text "10.200.1.0-" is entered. To the right of the "IP Ranges to Scan" box are three buttons: "Reset to Auto-Detected", "Import from Text File", and "Clear All Entries". At the bottom of the window are three navigation buttons: "< Back", "Next >", and "Cancel".

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.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window. On the left, a sidebar lists modules with checkboxes: Scan Type, Active Directory, Local Domains, Additional Credentials, External Domains, IP Ranges, **SNMP Information** (highlighted), VMware, and Verify and Schedule. The main panel is titled 'SNMP Information' and contains instructions: '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.' Below this is a text area with 'public' and an 'Add' button. There are also buttons for 'Reset to Default', 'Import from Text File', and 'Clear All Entries'. Under 'Advanced SNMP Options', there is a 'SNMP Timeout (seconds):' field with '10' and a 'Use Default' link. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window with the 'VMware (optional)' tab selected. The sidebar is the same as in the previous screenshot. The main panel is titled 'VMware (optional)' and contains instructions: 'VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname field in the format "hostname:port".' Below this are input fields for 'Hostname or IP Address', 'Username', and 'Password', along with an 'Add VMware Server' link. A section titled 'Testing connection to...' contains a table with columns 'Host' and 'User'. Below the table is a 'Clear All Entries' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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.

✓ Scan Type

✓ Active Directory

✓ Local Domains

✓ Additional Credentials

✓ External Domains

✓ IP Ranges

✓ SNMP Information

✓ VMware

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:

Use Login User

Task Label:
(optional)

Modify Settings

< Back

Finish

Cancel

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.

Tasks

Create Scan Tasks

Create Report Tasks

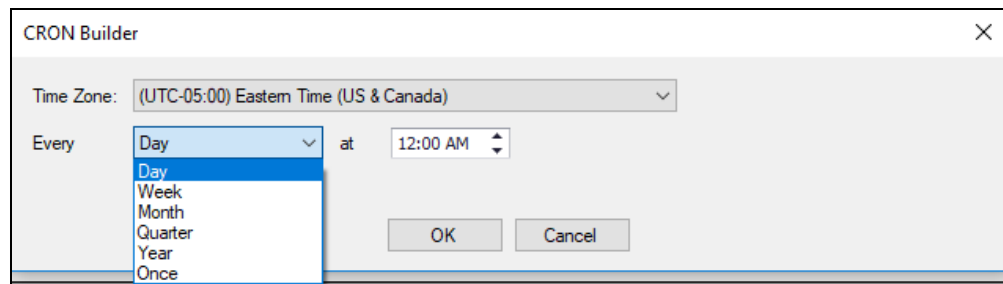
Create Export Tasks (BETA)

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 IP...	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	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	✗

- 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.

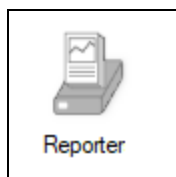


16. Whether you choose to run the scan now or schedule the scan to take place in the future, it will be added to the **Scheduled Tasks** list, where you can check its status. This is the final step in initiating (or scheduling) a scan.

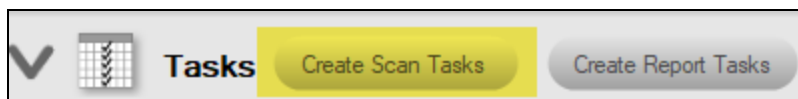
Type	Task Label	Description	Remote Data Collector	Status	Next Run Date	Last Run Date	Repeats	Cancel
Network Scan		Perform a Network Scan on a network with a d...	RDC	Pending			No	X

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.

The 'Create Task' dialog box is shown with the 'Scan Type' tab selected. The left sidebar lists various scan types: Active Directory, Local Domains, Additional Credentials, External Domains, IP Ranges, SNMP Information, VMware, and Verify and Schedule. The main area, titled 'Scan Type', contains a list of scan types: IT Assessment, Network Scan (Network/Security Modules) (highlighted), SQL Server Collection, Exchange Server Collection, HIPAA Compliance, HIPAA Network Scan, PCI Compliance, PCI Network Scan, Local Scans, Push Deploy, and Local on Remote Data Collector only. Navigation buttons at the bottom are '< Back', 'Next >', and 'Cancel'.

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

The 'Create Task - Network Scan (Network/Security Modules)' dialog box is shown with the 'Active Directory' tab selected. The left sidebar lists various scan types: Scan Type (checked), Active Directory (highlighted), Scan Credentials, External Domains, IP Ranges, SNMP Information, VMware, and Verify and Schedule. The main area, titled 'Active Directory', contains instructions: 'Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.' Below this, there are two radio buttons: 'Active Directory domain' and 'Workgroup (no domain)' (selected). Under the 'Active Directory Credentials' section, there are three text input fields: 'Username:', 'Password:', and 'Domain Controller:'. Navigation buttons at the bottom are '< Back', 'Next >', and 'Cancel'.

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.

The screenshot shows a window titled "Create Task - Network Scan (Network/Security Modules)". On the left is a sidebar with a list of modules: "Scan Type" (checked), "Active Directory" (checked), "Scan Credentials" (selected), "External Domains", "IP Ranges", "SNMP Information", "VMware", and "Verify and Schedule". The main area is titled "Scan Credentials" and contains the following text: "Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan." Below this text are two input fields: "Username:" and "Password:". To the right of the "Password:" field is a blue "Add" link. Below these fields is a large empty rectangular box. At the bottom left of this box is a blue "Clear All" link. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

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

Create Task - Network Scan (Network/Security Modules)

✓ Scan Type

✓ Active Directory

✓ Scan Credentials

External Domains

IP Ranges

SNMP Information

VMware

Verify and Schedule

External Domains

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

Domain Add

Clear All Entries

☒ Perform Dark Web Scan for Compromised Passwords

< Back Next > Cancel

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.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window with the 'IP Ranges' tab selected. On the left, a sidebar lists modules: Scan Type, Active Directory, Scan Credentials, External Domains, IP Ranges (highlighted), SNMP Information, VMware, and Verify and Schedule. The main area is titled 'IP Ranges' and contains two text boxes: 'Auto-Detected IP Ranges on Remote Appliance' with the value '10.200.' and 'IP Ranges to Scan' with the value '10.200.'. An example IP range format is provided: 'Example IP Range Format: 192.168.0.0-192.168.0.255'. Below the text boxes are buttons for 'Reset to Auto-Detected', 'Import from Text File', and 'Clear All Entries'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- 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.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window with the 'SNMP Information' tab selected. The sidebar is the same as in the previous screenshot, but 'SNMP Information' is now highlighted. The main area is titled 'SNMP Information' and contains a text box for 'Read Community String' with the value 'public'. Below this are buttons for 'Reset to Default', 'Import from Text File', and 'Clear All Entries'. There is also an 'Advanced SNMP Options' section with a text box for 'SNMP Timeout (seconds):' with the value '10' and a 'Use Default' link. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

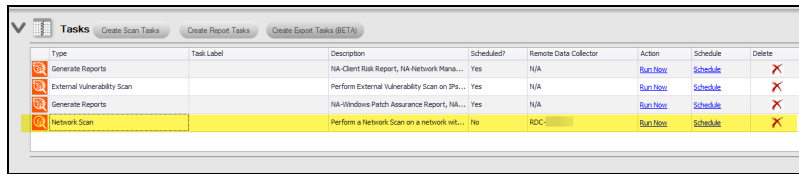
- Input the **Hostname** or **IP Address** and **Credentials** of the VMware Servers that you would like to include in the scanning process.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window. On the left, a list of modules is shown with checkboxes: Scan Type, Active Directory, Scan Credentials, External Domains, IP Ranges, SNMP Information, VMware (selected), and Verify and Schedule. The main area is titled 'VMware (optional)' and contains instructions: 'VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname field in the format "hostname.port".' Below this are input fields for 'Hostname or IP Address', 'Username', and 'Password'. A link 'Add VMware Server' is present. A table titled 'Testing connection to...' has columns 'Host' and 'User'. At the bottom are buttons '< Back', 'Next >', and 'Cancel'.

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.

The screenshot shows the 'Create Task - Network Scan (Network/Security Modules)' window, now on the 'Verify and Schedule' tab. The left sidebar shows the 'Verify and Schedule' tab selected. The main area contains instructions: 'Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.' Below this is an 'Email Notification' section with a checkbox 'Send email notification when schedule completes' which is checked. An 'Email Address' field contains '@rapidfiretools.com'. A link 'Use Login User' is present. A 'Task Label' field is empty. At the bottom are buttons 'Modify Settings', '< Back', 'Finish', and 'Cancel'.

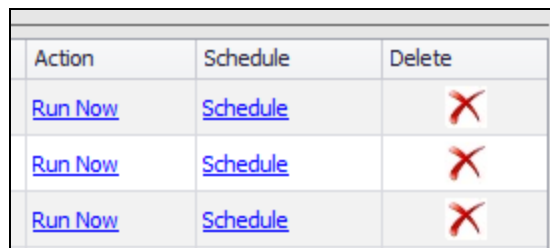
11. Click on the **Finish** button to complete the scheduling of the **Network Scan** task. The task will then be displayed in the **Tasks Library** window.



Type	Task Label	Description	Scheduled?	Remote Data Collector	Action	Schedule	Delete
Generate Reports		NA-Client Risk Report, NA-Network Man...	Yes	N/A	Run Now	Schedule	✗
External Vulnerability Scan		Perform External Vulnerability Scan on IP...	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 with...	No	RDC...	Run Now	Schedule	✗

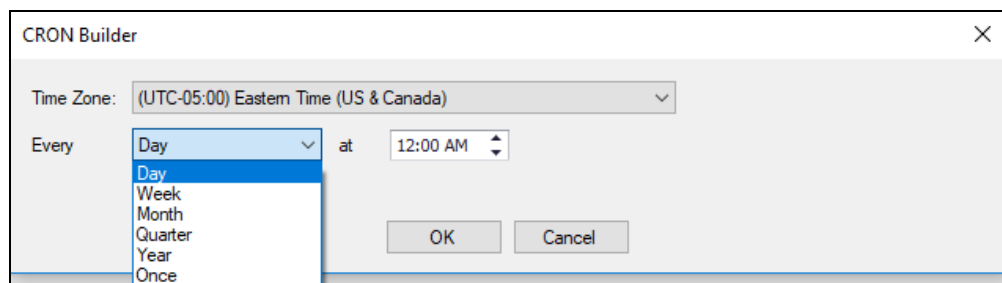
12. In order to initiate the scan, you will need to move the scan from the Task list into **Scheduled Tasks**. There are two ways to do this:

- 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.

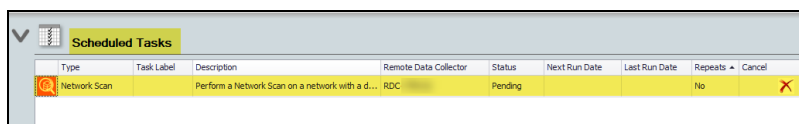


CRON Builder

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...	Pending			No	✗

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.

Exchange Server Assessment Scan

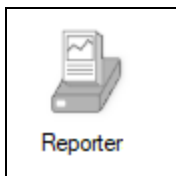
Set up a recurring Exchange Assessment scan to collect data for automatic Exchange Assessment reports. To create this scan task, perform the following steps:

Note: If you are installing the RDC to perform an Exchange assessment for an on-premise server, 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.

The screenshot shows the 'Create Task' window with the 'Scan Type' tab selected. The left sidebar contains a list of steps: 'Scan Type' (highlighted), 'Exchange Version', 'Credentials', and 'Verify and Schedule'. The main area is titled 'Scan Type' and contains the instruction: 'Select the type of scan this task should perform. You will need separate tasks to perform different types of scans.' Below this is a list of scan types: 'IT Assessment', 'Network Scan (Network/Security Modules)', 'SQL Server Collection', 'Exchange Server Collection' (highlighted), 'HIPAA Compliance', 'HIPAA Network Scan', 'PCI Compliance', 'PCI Network Scan', 'Local Scans', 'Push Deploy', and 'Local on Remote Data Collector only'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

4. Next, select the credentials/authentication method to use:

- **Use Legacy Credentials:** Enter a user name and password to connect to the target Office 365 environment.

The screenshot shows the 'Create Task - Exchange Server Collection' window with the 'Credentials' tab selected. The left sidebar shows the progress: 'Scan Type' and 'Exchange Version' are completed (checked), 'Credentials' is the current step (highlighted), and 'Verify and Schedule' is next. The main area is titled 'Credentials' and contains the instruction: 'Enter your Exchange Online for Office 365 management credentials below. These credentials will be used to connect to your particular instance of Office 365 to perform the scan. Clicking Next will test requirements and your credentials. This can take up to a minute in some cases.' Below this are two radio button options: 'Use Legacy Credentials' (selected) and 'Use Enterprise Application Credentials'. Under 'Use Legacy Credentials' are input fields for 'User Name:' and 'Password:'. Under 'Use Enterprise Application Credentials' are input fields for 'Organization:', 'App ID:', and 'Thumbprint:'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

- **Use Enterprise Application Credentials:** Enter credentials to authenticate using an Enterprise App that you configure in the target environment. See ["Authenticate Exchange Scan using Enterprise App" on page 203](#).

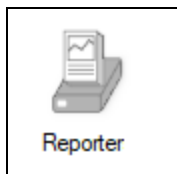
5. Verify the settings, set-up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.
6. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*

Action	Schedule
Run Now	Schedule

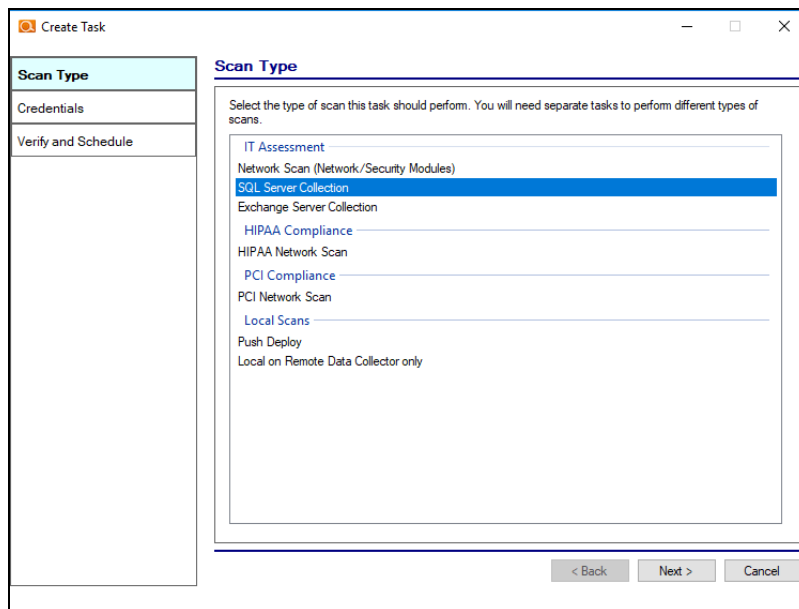
SQL Server Assessment Scan

To create this scan task, perform the following steps:

1. Open the **Reporter** dashboard.



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



- Follow the prompts to set-up the **Server**, **Port**, and **Credentials** for the SQL Server being scanned. Select the **Next** button.
- 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.
- 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.

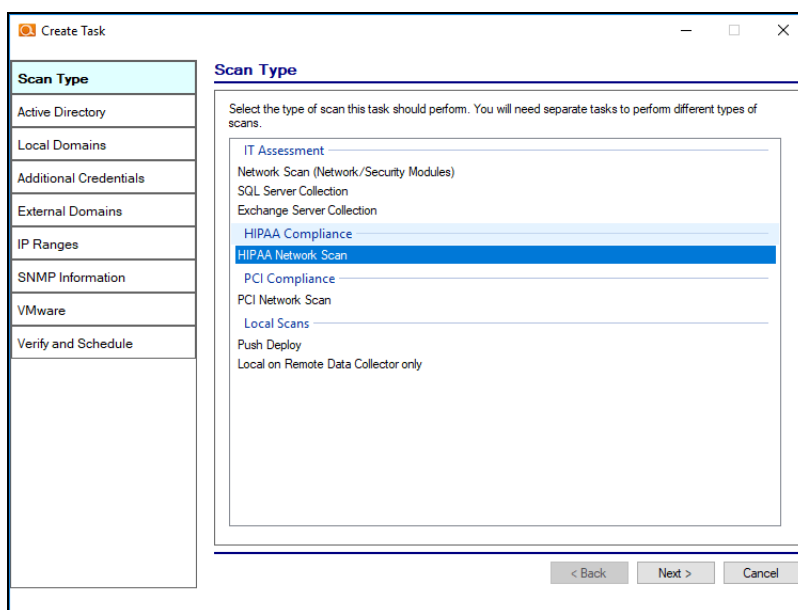
HIPAA Compliance Network Scan

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.



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.

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.

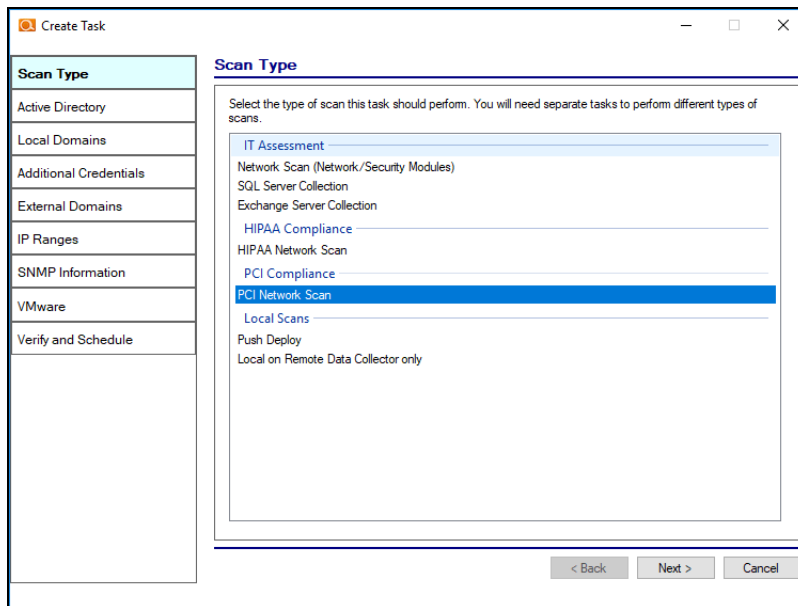
PCI Compliance Network Scan

To create this scan task, perform the following steps:

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.



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.

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

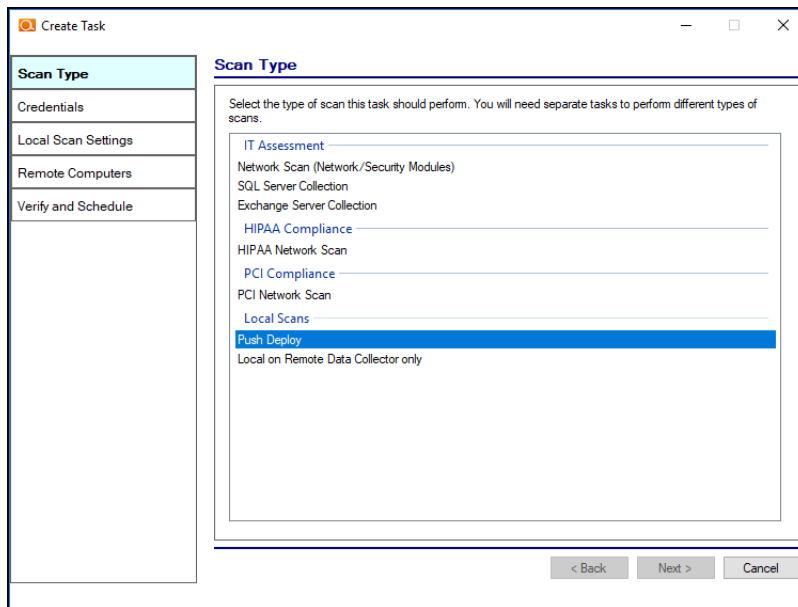
Note: Use Push Deploy Local Computer Scans to gather detailed data for individual workstations. These can be used for all report types and are essential for a comprehensive assessment.

To create this scan task, perform the following steps:

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.



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

Select the **Next** button.

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

The screenshot shows the 'Create Task - Push Deploy' window with the 'Credentials' tab selected. The left sidebar contains a list of steps: 'Scan Type' (checked), 'Credentials' (selected), 'Local Scan Settings', 'Remote Computers', and 'Verify and Schedule'. The main area is titled 'Credentials' and contains the following text: '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.' Below this text are input fields for 'Username:' and 'Password:'. A red message 'Please add at least one Credential.' is displayed, with an 'Add' link next to it. Below the message is a large empty rectangular box. At the bottom left of the main area is a 'Clear All' link. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

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.

The screenshot shows the 'Create Task - Push Deploy' window with the 'Local Scan Settings' tab selected. The left sidebar is the same as in the previous screenshot, but 'Local Scan Settings' is now selected. The main area is titled 'Local Scan Settings' and contains the following text: 'Scan Settings: ☒ Computer Scan ☐ Security Scan'. Below this are four rows of checkboxes: 'HIPAA Quick' and 'HIPAA Deep', 'PCI Quick' and 'PCI Deep', 'BDR Scan' and 'PII Scan'. At the bottom of the main area are two buttons: 'Check All' and 'Uncheck All'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

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.

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

Select the **Next** button.

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.

The screenshot shows a window titled "Create Task - Push Deploy" with a sidebar on the left containing a list of steps: Scan Type, Credentials, Local Scan Settings, Remote Computers, and Verify and Schedule (which is highlighted). The main area is titled "Verify and Schedule" and contains the following elements:

- A message: "Press the Finish button to save the task. Use the Back button to go back and modify any previous changes."
- An "Email Notification" section with a checkbox labeled "Send email notification when schedule completes". Below it is an "Email Address:" text field and a "Use Login User" button.
- A "Task Label: (optional)" text field.
- At the bottom, there are three buttons: "Modify Settings", "< Back", and "Finish" (highlighted in blue), and a "Cancel" button.

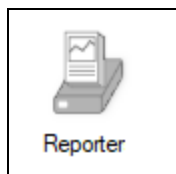
8. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*

Action	Schedule
Run Now	Schedule

Local Scan for a Computer Running the Remote Data Collector

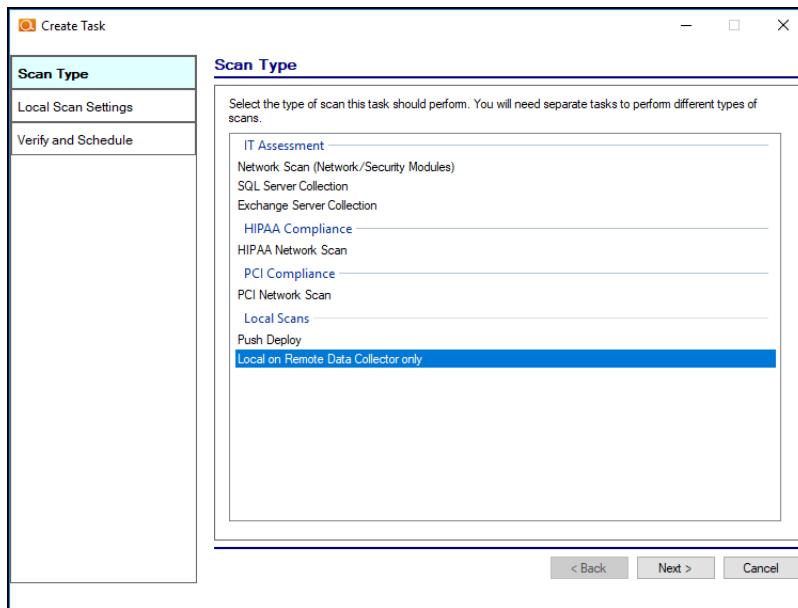
This scan will collect data only on the computer running the RDC. To create this scan task, perform the following steps:

1. Open the **Reporter** dashboard.



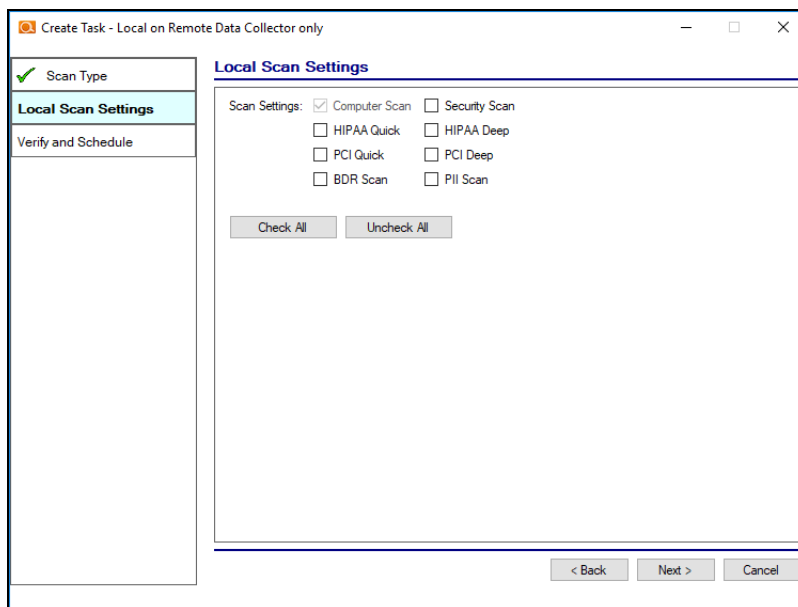
2. Click **Create Scan Tasks** and select the RDC.

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.



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.



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.

Create Task - Local on Remote Data Collector only

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:

Use Login User

Task Label: (optional)

Modify Settings < Back Finish Cancel

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

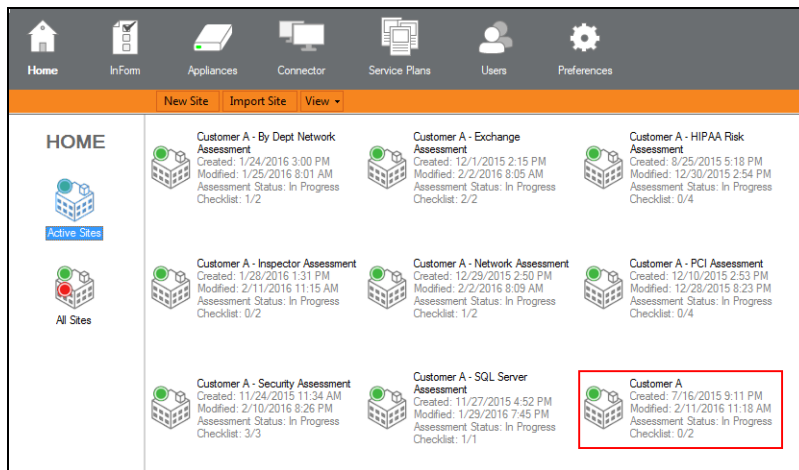
Configure the Local Data Scan Merges

When local scans are performed by the Network Detective **Data Collectors, Appliance,** or **Discovery Agents**, 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.

With **Discovery Agents**, you can also select the appropriate **Labels** for local scans to be merged into your assessment.

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.



Step 1 — Select and Open the Site

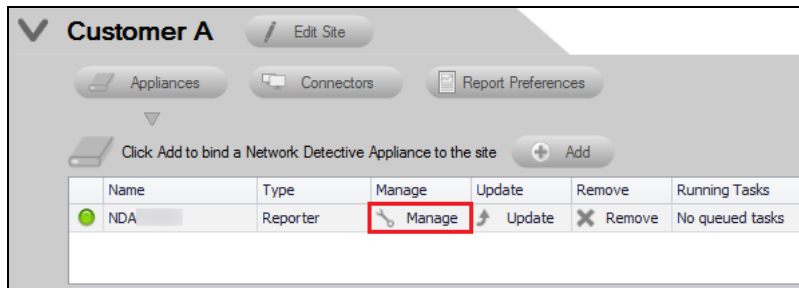
First, open your Reporter site and access your active project.

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**.



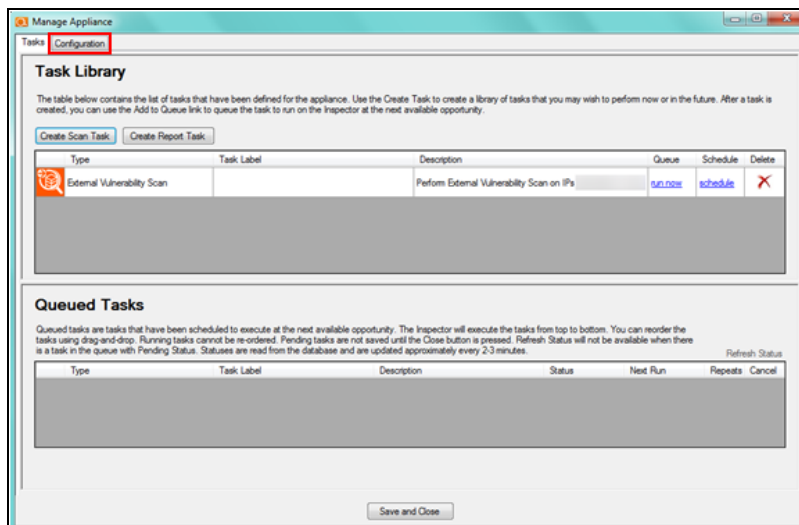
Then select the **Manage** option presented for the Reporter **Appliance** listed.



The Manage Reporter window will be displayed.

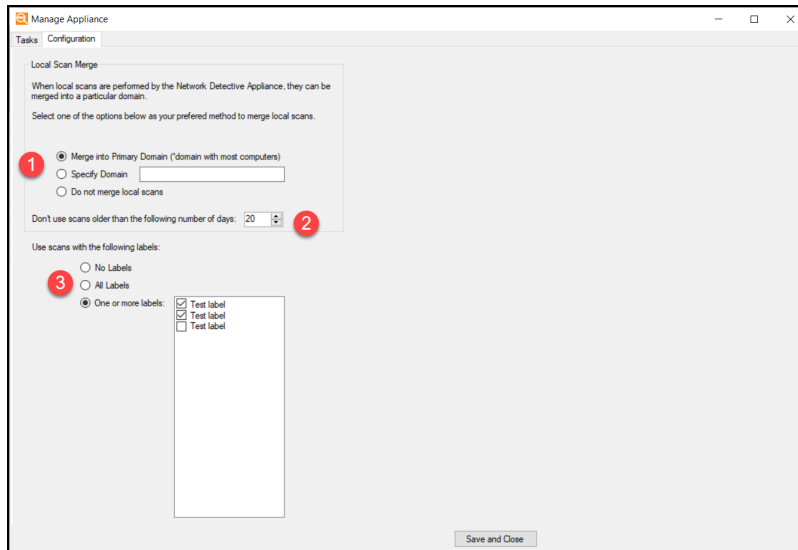
Step 3 — Set Scan Data Merge Configuration

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



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

1. 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. Finally, if you are using Discovery Agents, choose the labels you wish to use for your scans. You can select
 - **No Labels**
 - **All Labels**
 - **One or more Labels** (make your individual selections from the list)

Note: See the help topic "Enable Discovery Agents for Local Data Collection" in the Network Detective User Guide for a complete walk through on deploying and labeling Discovery Agents.

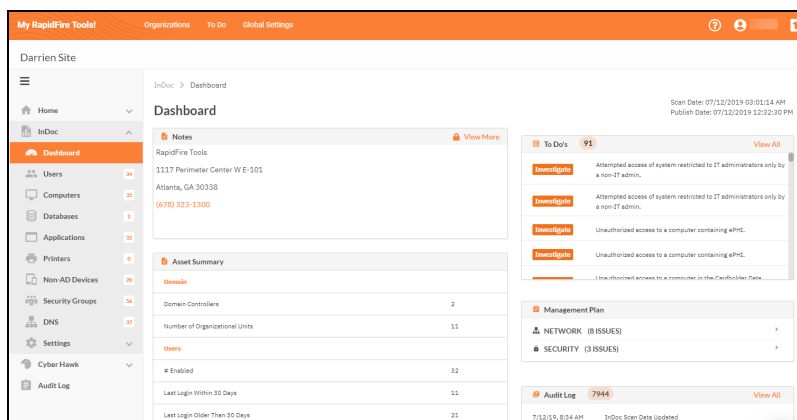
4. Then select the Save and Close button to store the **Scan Merge Settings**.

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>.



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.

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 17](#) 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.

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 (Reporter Customer 1 - HIPPA-Reports-<Date>-<ID>.zip)
☐ Create Folder: -yyyyMMdd

☒ Upload Scan Data to InDoc
[What is InDoc?](#)

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

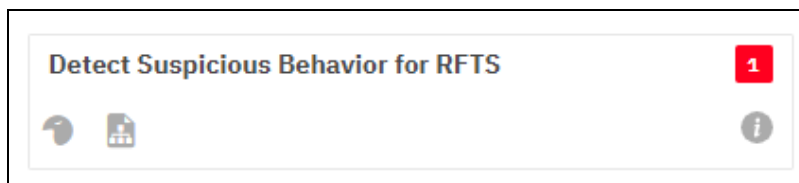
Task Label (optional):

Back Next Finish

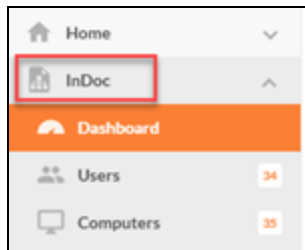
6. Users who wish to access InDoc in the RapidFire Tools Portal must have the correct **Global** and **Site-specific Role** permissions. User Roles are configured in the Portal. See ["InDoc User Permissions" on page 151](#).
7. Your reports must have successfully generated.

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**.

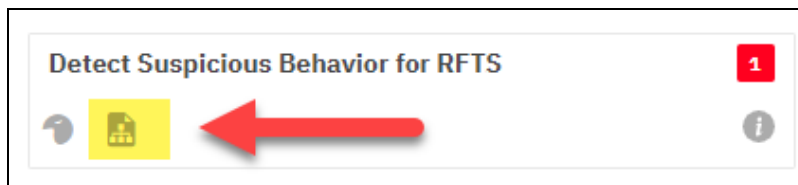


Using InDoc (RapidFire Tools Portal)

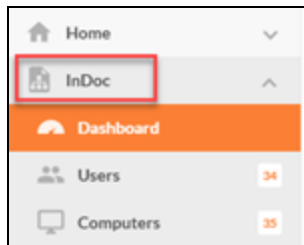
Once you set up Reporter for automated reporting and data collection, you can begin using InDoc in the RapidFire Tools Portal. (See ["Requirements for using InDoc with Reporter" on page 125](#)). Each time scans are performed and reports successfully generated, InDoc will be updated with the latest data. 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.

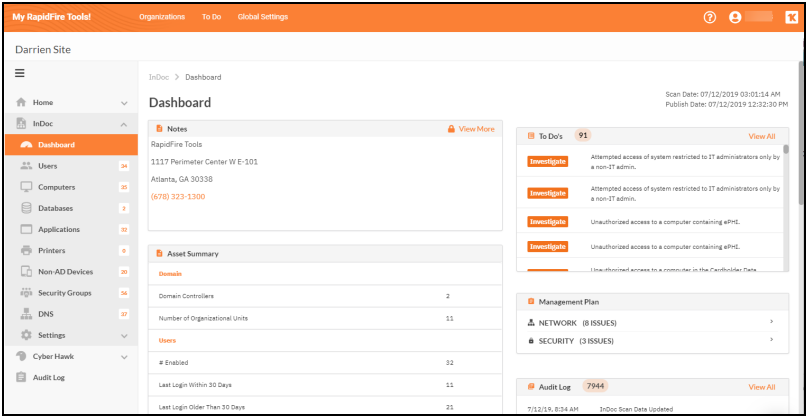


3. Click on the **InDoc tab > Dashboard**.



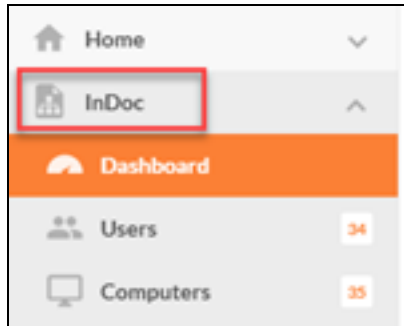
From here you can view details about network assets taken from the latest scan data — and you can begin adding your own supplementary documentation. The InDoc dashboard gives you a high level overview of the activity at the Site, including

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

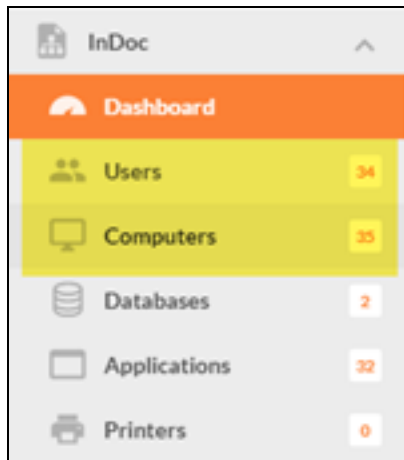


Explore Network Assets with InDoc

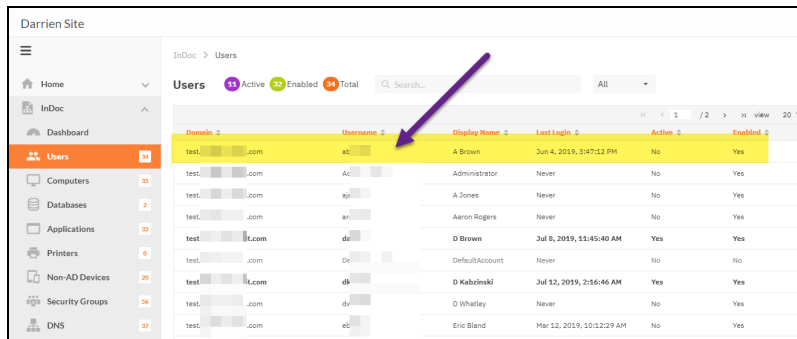
InDoc uses the stream of data from Reporter to help your team find, manage, and document everything at a Site. You access InDoc for your Sites in the RapidFire Tools Portal at <https://www.youritportal.com>. From the **InDoc tab** > **Overview**, you can view detailed information about network assets.



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.



The screenshot shows the 'Users' page in the RapidFire Tools portal. The left sidebar contains navigation links: Home, InDoc, Dashboard, Users (selected), Computers, Databases, Applications, Printers, Non-AD Devices, Security Groups, and DNS. The main content area displays a table of users. A purple arrow points to the 'Display Name' column header. The table has columns for Domain, Username, Display Name, Last Login, Active, and Enabled. The first row is highlighted in yellow.

Domain	Username	Display Name	Last Login	Active	Enabled
test. .com	ad. .com	A. Brown	Jun 4, 2019, 3:47:12 PM	No	Yes
test. .com	Administrator	Administrator	Never	No	Yes
test. .com	A. Jones	A. Jones	Never	No	Yes
test. .com	Aaron Rogers	Aaron Rogers	Never	No	Yes
test. .com	D. Brown	D. Brown	Jul 6, 2019, 11:45:40 AM	Yes	Yes
test. .com	DefaultAccount	DefaultAccount	Never	No	No
test. .com	D. Kukulinski	D. Kukulinski	Jul 12, 2019, 2:16:46 AM	Yes	Yes
test. .com	D. Whalley	D. Whalley	Never	No	Yes
test. .com	Eric Bland	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.

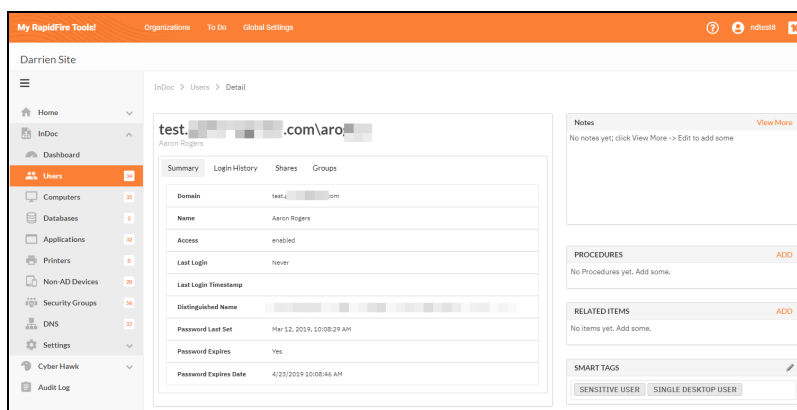
View Data about Network Assets

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.



The screenshot shows the 'Users' details page in the RapidFire Tools portal. The left sidebar contains navigation links: Home, InDoc, Dashboard, Users (selected), Computers, Databases, Applications, Printers, Non-AD Devices, Security Groups, and DNS. The main content area displays the details for a user named 'test. .com\aro. .com'. The details are organized into sections: Summary, Login History, Shares, and Groups. The Summary section includes fields for Domain, Name, Access, Last Login, Last Login Timestamp, Distinguished Name, Password Last Set, Password Expires, and Password Expires Date. The right sidebar contains sections for Notes, Procedures, Related Items, and Smart Tags.

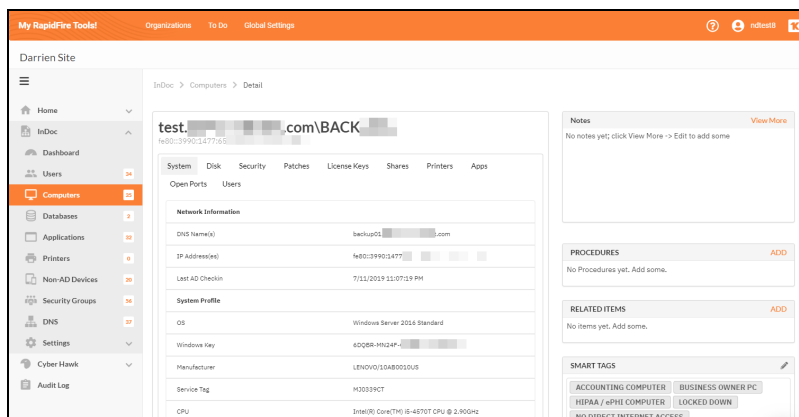
Summary	Login History	Shares	Groups
Domain test. .com	Name Aaron Rogers	Access enabled	Last Login Never
Last Login Timestamp [Timestamp]	Distinguished Name [Distinguished Name]	Password Last Set Mar 12, 2019, 10:02:29 AM	Password Expires Yes
Password Expires Date 4/23/2019 10:02:29 AM			

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.



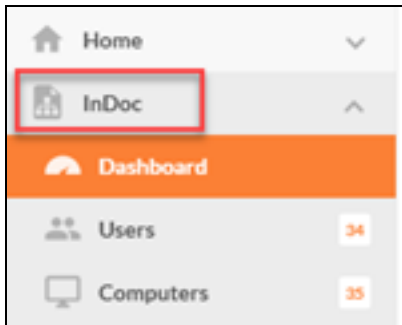
For each computer, you can also add Notes, Procedures, Related Items, and/or Smart Tags for the user. For example:

- 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

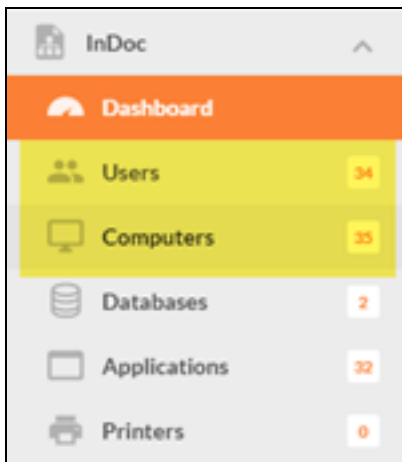
Add a Note to an Asset (InDoc)

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.

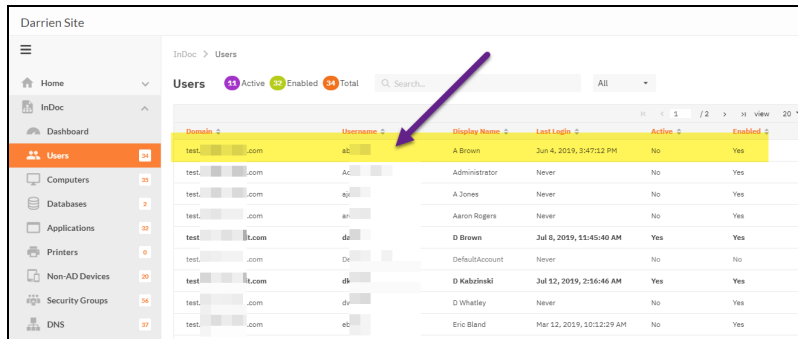
1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc tab > Overview**.



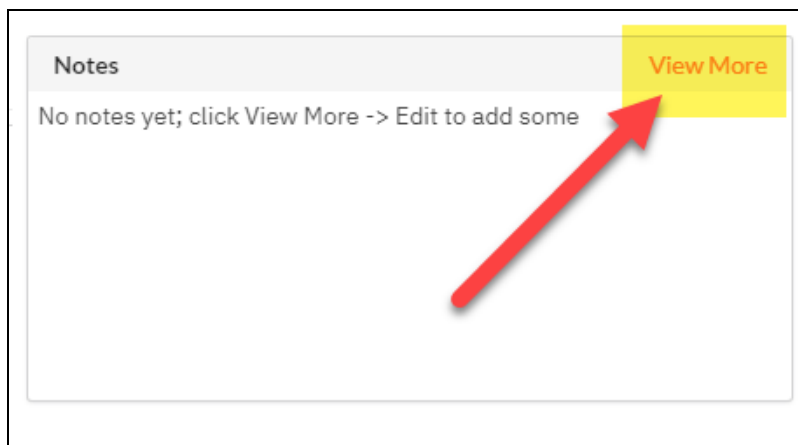
3. Choose an asset category ("Users" or "Computers," for example).



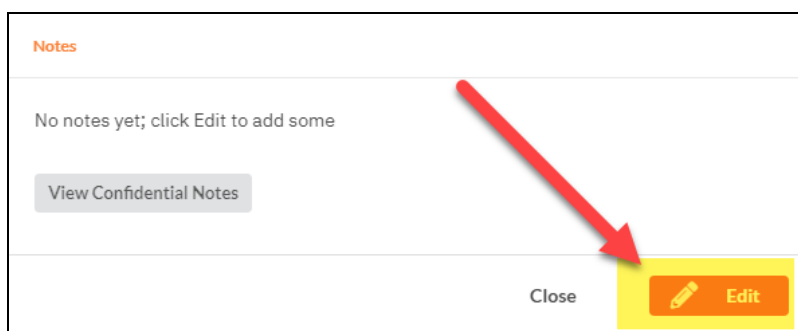
4. The list of detected assets will appear. Click on a specific asset from the list.



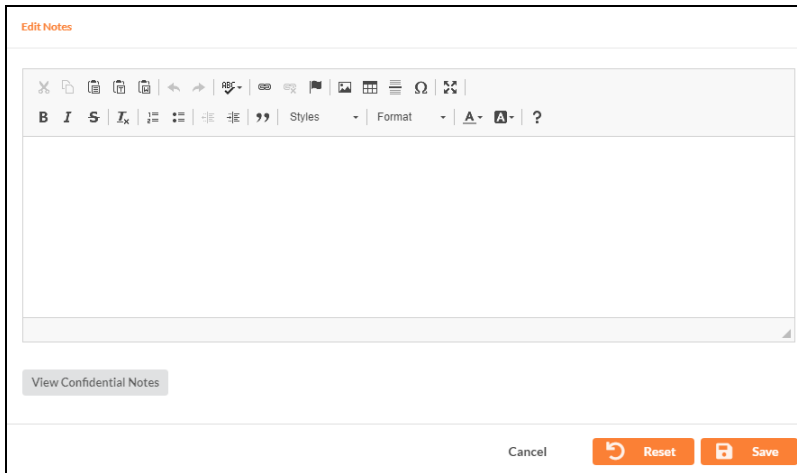
5. Next to the **Notes** panel, click **View More**.



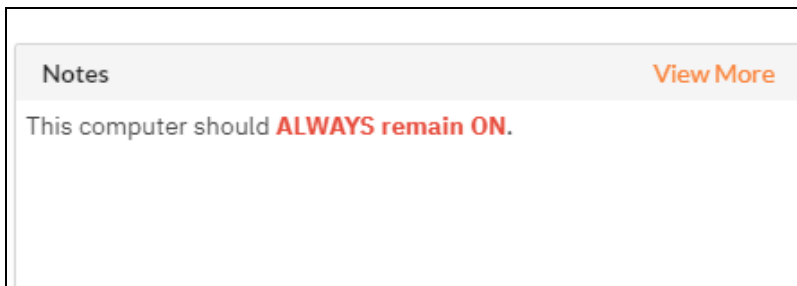
6. Click **Edit**.



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



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

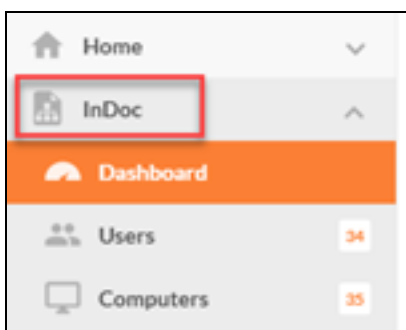


Add and View Confidential Notes (InDoc)

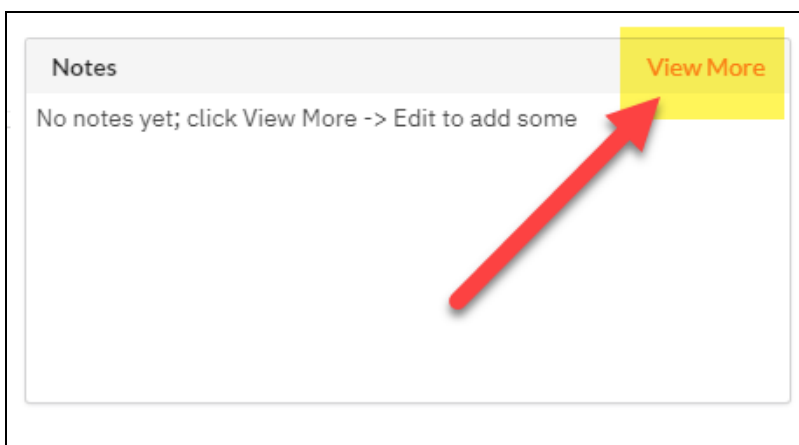
Note: Before you can add or view confidential notes with InDoc, you first need to ["Enable Confidential Information Protection for InDoc" on page 138](#). You will also need to be granted confidential access by a Master or Admin user.

To create or view confidential notes with InDoc:

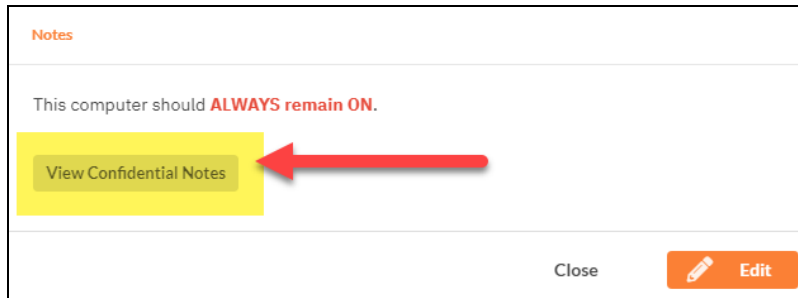
1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the **InDoc tab > Overview**.



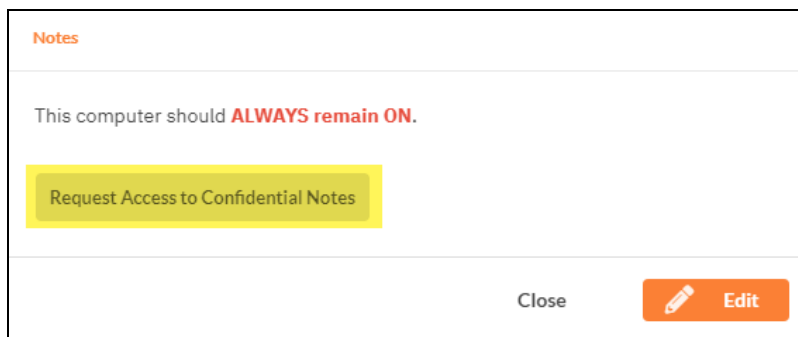
3. Choose an asset category ("Users" or "Computers," for example). The list of detected assets will appear.
4. Click on a specific asset from the list.
5. Next to the **Notes** panel, click **View More**.



6. Click **View Confidential Notes**.



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](#)).



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**.

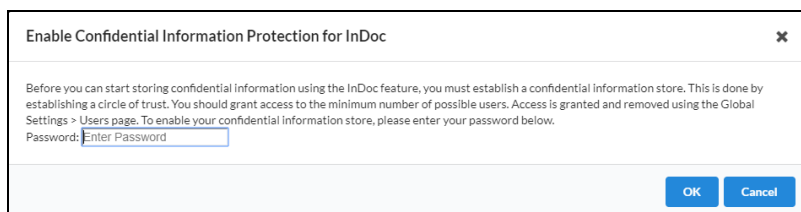
Note: You will need to re-enter your password to view or change confidential notes.

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.

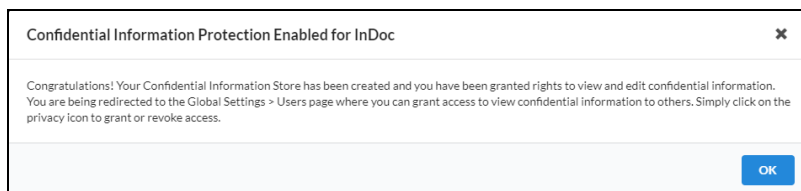
This task will be performed by a Global Master user when they first log in to the portal after you set up InDoc. Here's how it works:

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**.



The dialog box is titled "Enable Confidential Information Protection for InDoc" and has a close button (X) in the top right corner. The main text reads: "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." Below this text is a password input field with the placeholder text "Enter Password". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

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



The dialog box is titled "Confidential Information Protection Enabled for InDoc" and has a close button (X) in the top right corner. The main text reads: "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." At the bottom right of the dialog is a single button: "OK".

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@raj [redacted]	Jones	Admin	All / -TestAutoTask ()	No	No
another-example-user@u [redacted]	[redacted]	Site Restricted		No	No
BakeCDNotesTestin [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?

Cancel

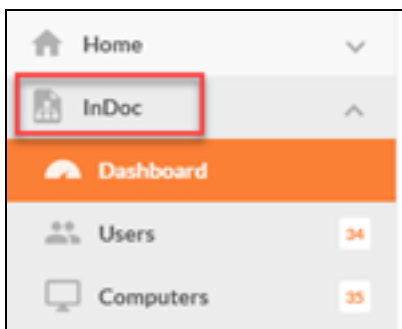
Allow

Add a Procedure to an Asset (InDoc)

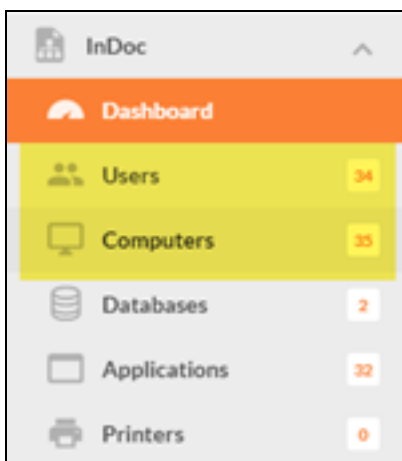
You can use InDoc to document **Procedures** and associate them directly with the relevant network assets.

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.

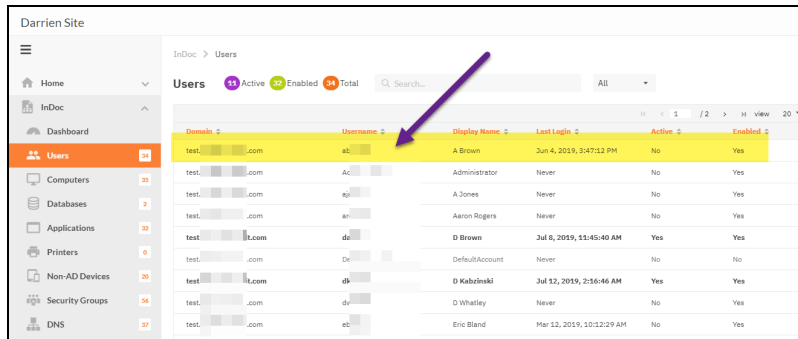
1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc** tab > **Overview**.



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



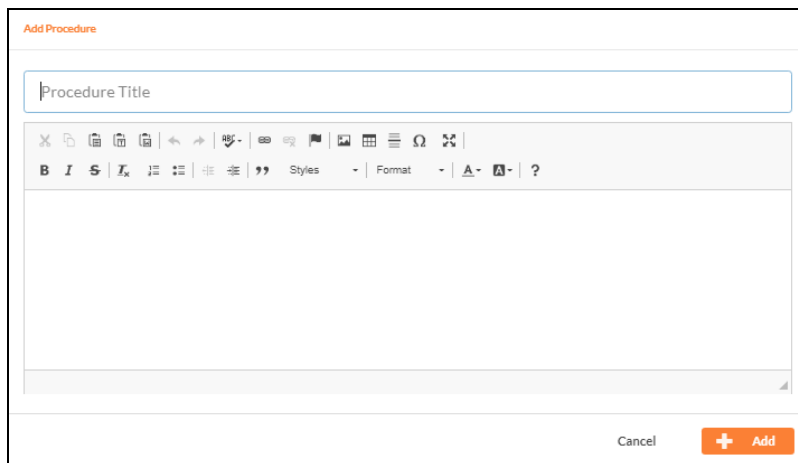
4. The list of detected assets will appear. Click on a specific asset from the list.



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

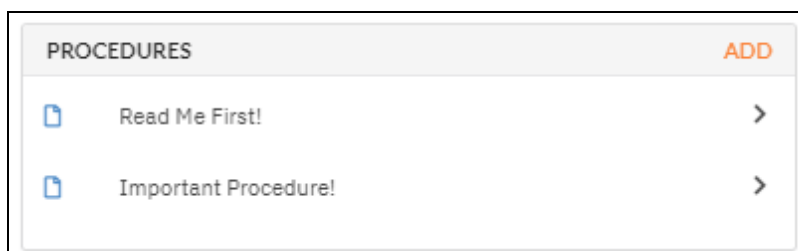


6. Use the editor to write or edit your Procedure.



7. Click **Save**.

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



Edit or Delete Procedures

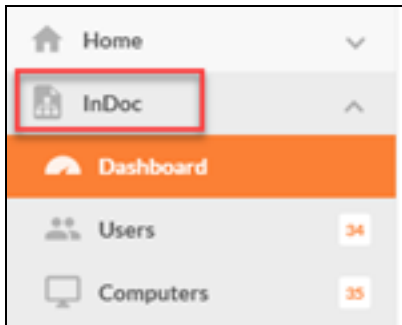
Whenever you need to change a procedure:

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**.

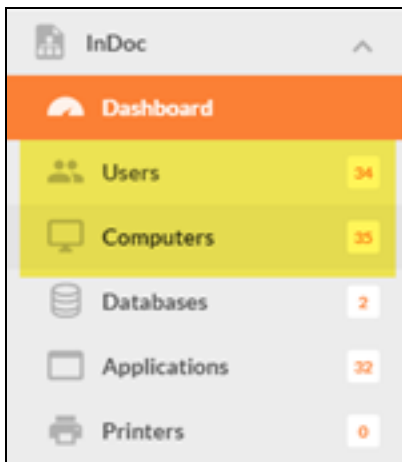
Add Related Items to a Network Asset (InDoc)

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:

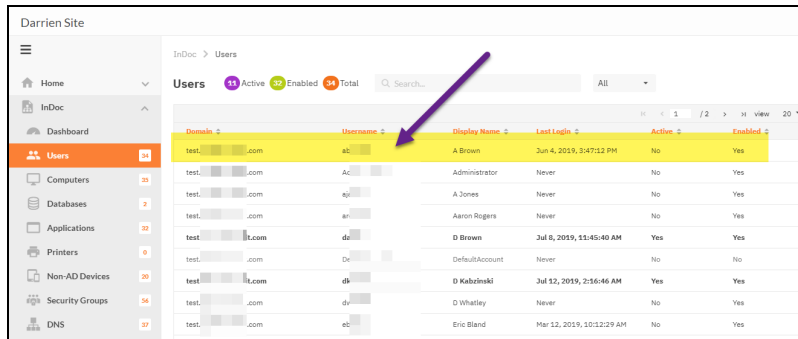
1. Open the Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc** tab > **Overview**.



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



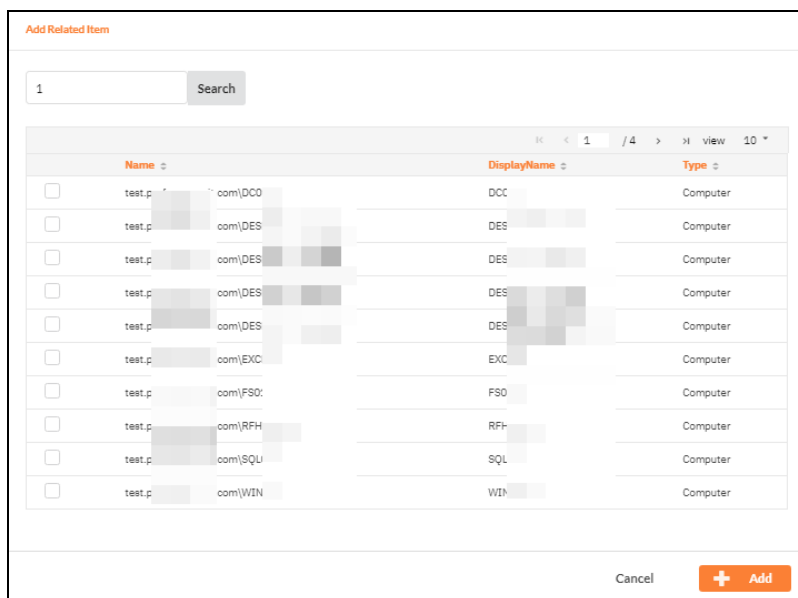
4. The list of detected assets will appear. Click on a specific asset from the list.



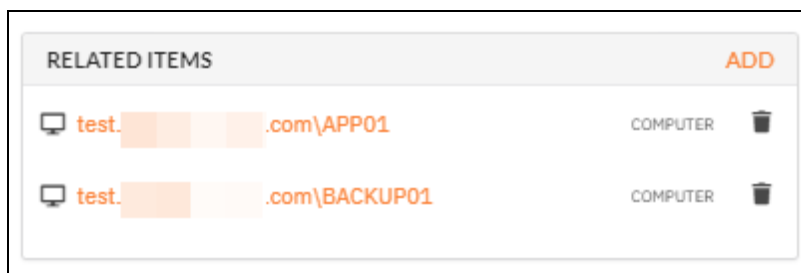
- From the **Related Items** tab, click **Add**.



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



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

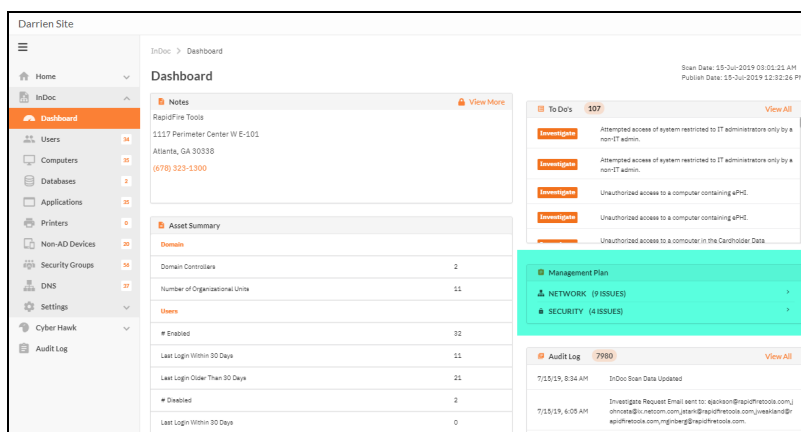


Note: To remove a related item from an asset, click on the  icon. The related item will be removed.

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.



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
 Anti-virus not installed	94
 Anti-spyware not installed	94
 Anti-virus not up to date	90
 Anti-spyware not up to date	90
 Few Security patches missing on computers.	75
 Significantly high number of Domain Administrators	35
 User password set to never expire	30
 Operating system in Extended Support	20
 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.

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

High Risk | User Password Set To Never Expire

Risk Score	Recommendations	Severity	Probability
80	Investigate all accounts with passwords set to never expire and configure them to expire regularly. ☐ TEST1.IT.COM\abadmin / ABrown Admin ☐ TEST1.IT.COM\ldadmin / Darrien Brown ☐ TEST1.IT.COM\ldkadmin / DK Admin ☐ TEST1.IT.COM\jadmin / 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		

Close

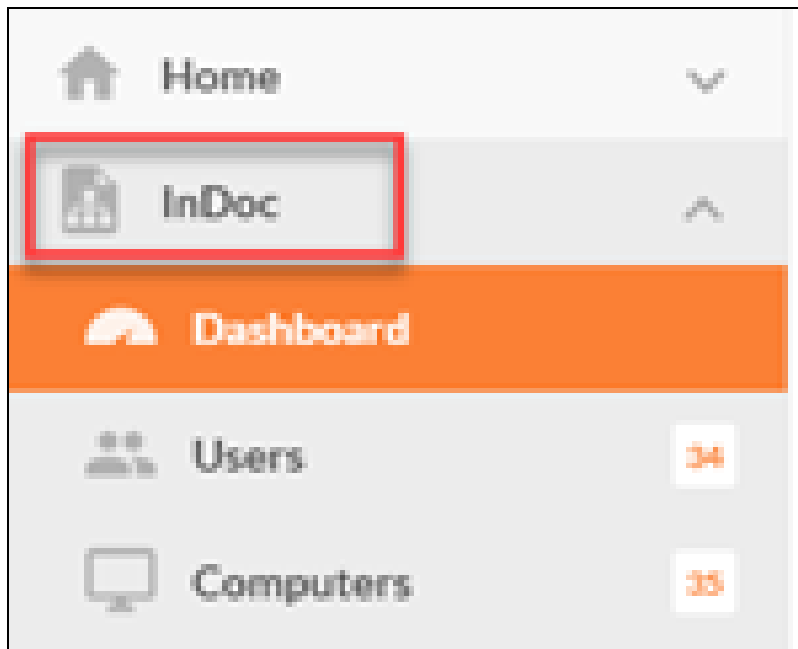
Tip: For more detailed information on the issues identified, **review the latest Management Plan report** for that specific module. You can **download Reporter documents in the Network Detective application**.

Edit Smart Tags in InDoc

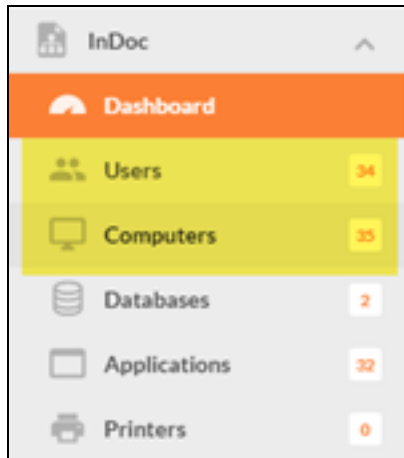
Cyber Hawk, our security alerting system, incorporates a proprietary feature called **Smart Tags**. Smart Tags allow you to adapt Cyber Hawk to each client's unique IT environment to detect network Anomalies, Changes, and Threats (ACT). Smart Tags allow you to add information about specific users, assets, 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:

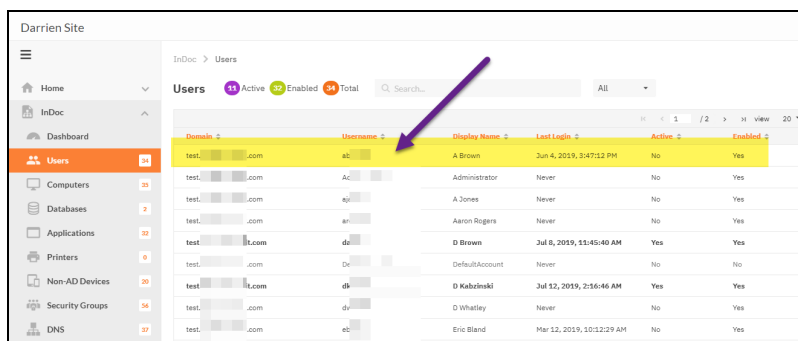
1. Open the InDoc Site in the RapidFire Tools Portal.
2. Navigate to the Site **InDoc** tab > **Overview**.



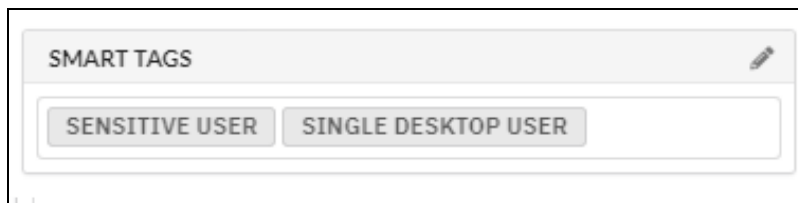
3. Choose an asset category ("Users" or "Computers," for example).



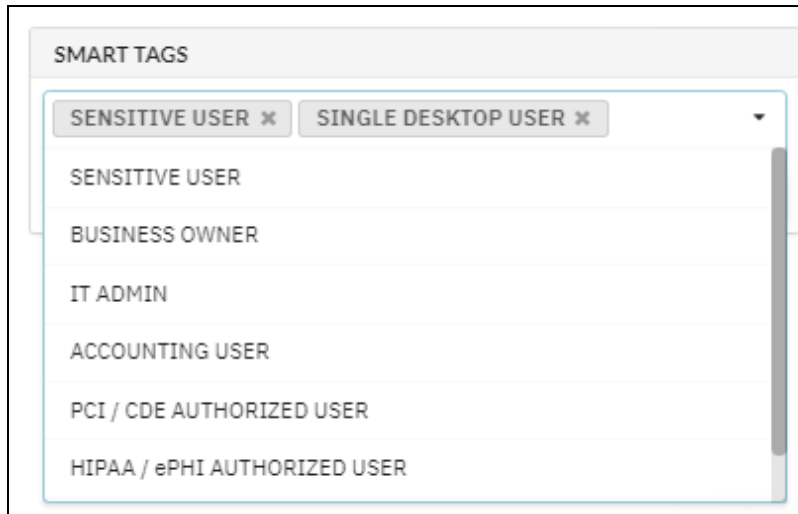
4. The list of detected assets will appear. Click on a specific asset from the list.



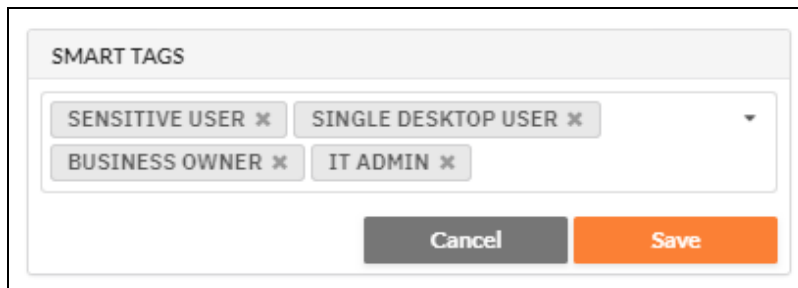
5. From the **Smart Tags** panel, click the pen icon .



6. Choose your Smart Tags from the available list.



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



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.

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 138](#).
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 138](#).

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 125](#)

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.

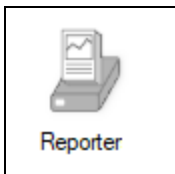
Tip: The *Client Portal* is the same as the RapidFire Tools Portal – just limited to only what clients need to see.

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)	

- 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 125](#)

- 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.

The screenshot shows the 'Schedule Report Wizard' window, specifically the 'Delivery Method' tab. At the top, there is a table with columns 'Subject' and 'Email'. The first row has 'Network Detective Notification' in the 'Subject' column. Below the table, there are several options: 'Attach reports to notification email' (unchecked), 'Password Protect ZIP File' (unchecked), 'Copy to External Network Share' (unchecked), 'Save reports to ZIP file (Site Name-Reports-<Date>-<ID>.zip)' (unchecked), and 'Create Folder' (unchecked). There are also checkboxes for 'Upload Scan Data to InDoc (BETA)' (checked) and 'Publish to Client Portal' (unchecked). The 'Publish to Client Portal' section is highlighted in yellow and includes a 'Report Set Name' field and an 'Append Report Set Name " - <Date> - <ID>"' checkbox (checked). A 'Task Label' field is at the bottom. The window has 'Back', 'Next', and 'Cancel' buttons at the bottom right.

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:

Back Next Cancel

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:

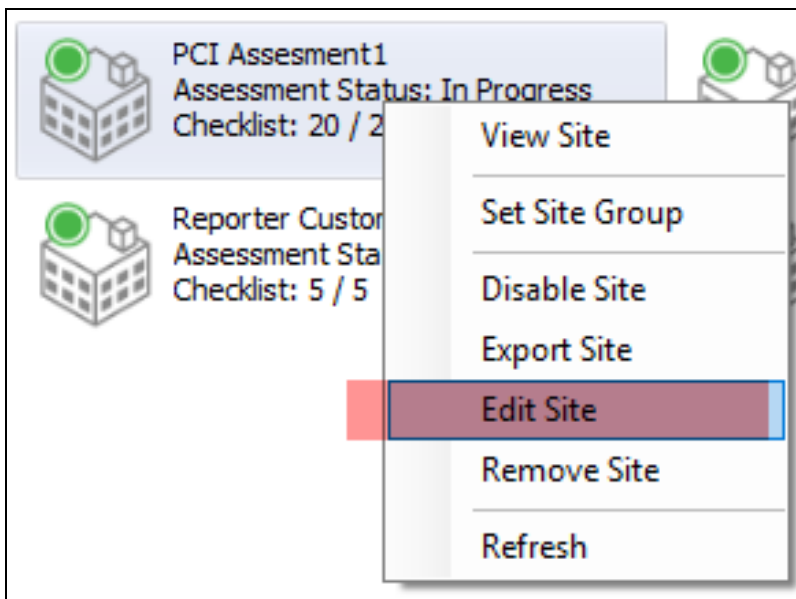
1. Click on **Reporter** from the **Network Detective top ribbon**.
2. Click **Edit** on the **Reporter Template** you wish to modify.
3. **Double click on the Report Task** you wish to modify.
4. Click **Next** to go to the **Delivery Method** screen, and check **Publish to Client Portal**.
5. Complete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

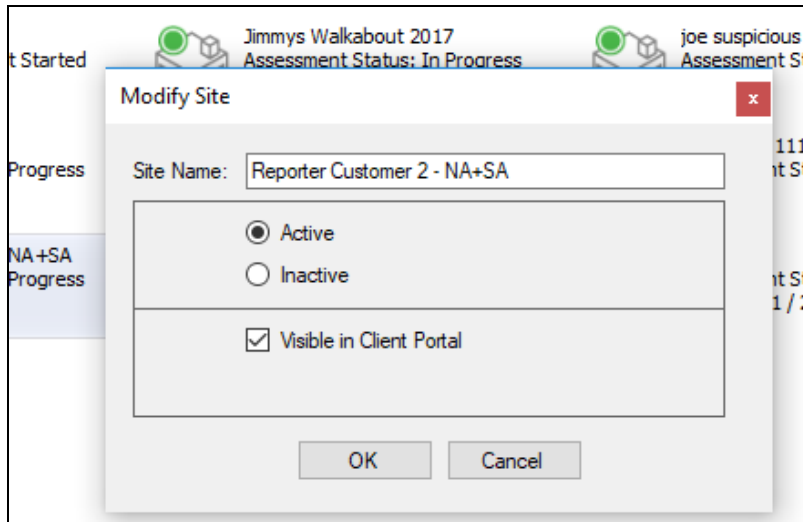
Step 2 — Ensure that the Site is Visible in the Client Portal

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**.



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



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.

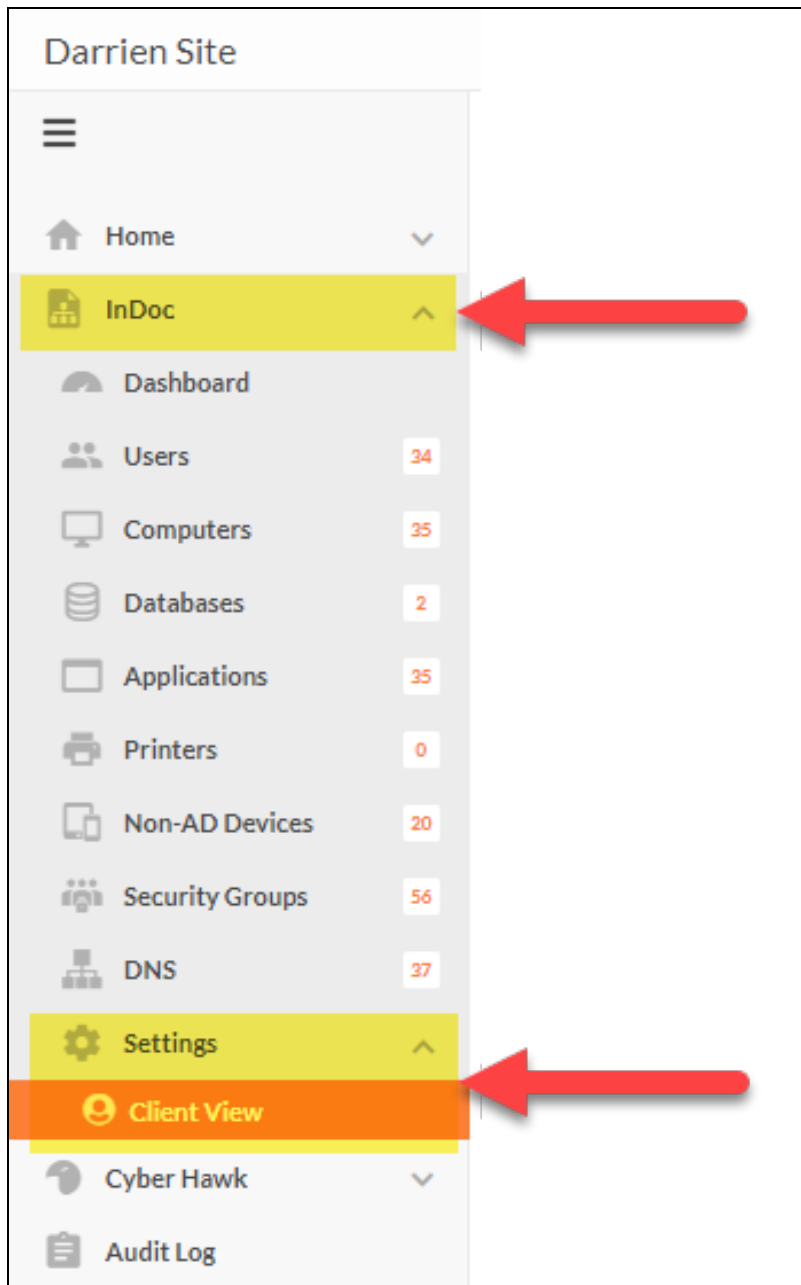
4. Now you need to add the new user to the Client Role. Go to **Home > Roles**.
5. Click **Add User** next to the **Client View** Role. Select the User. Then click **Add**.

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.

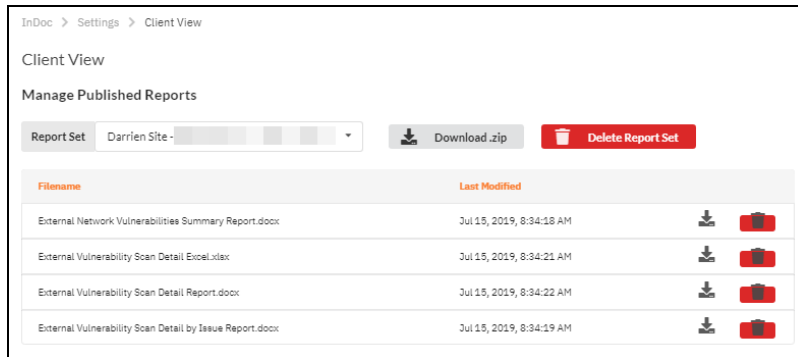
Step 4 — Configure Client View in RapidFire Tools Portal

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.



- 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:

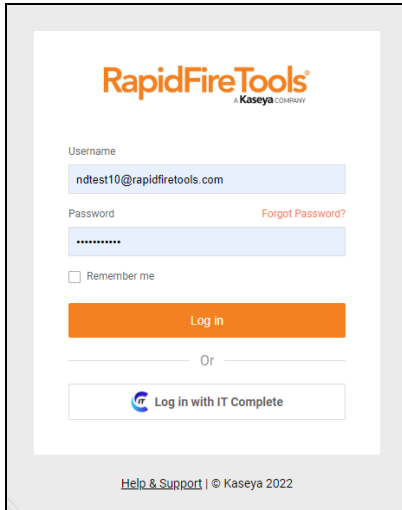
- Deleting reports or report sets will remove them from the Client View, but not from Network Detective.
- You cannot restore reports to the Client View once you have deleted them. You will have to republish them from Network Detective.

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 154](#) 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
A Kaseya COMPANY

Username
ndtest10@rapidfiretools.com

Password [Forgot Password?](#)

☐ Remember me

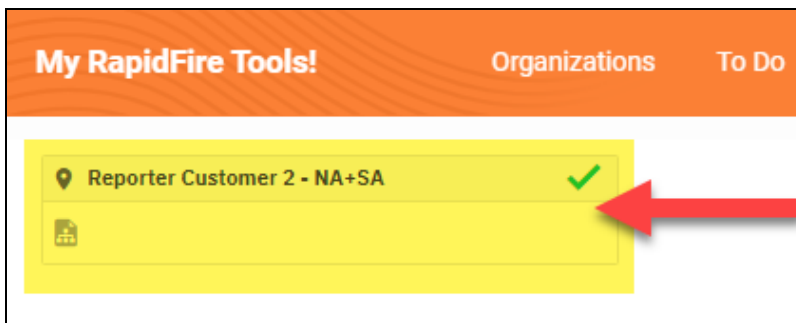
Log in

Or

 Log in with IT Complete

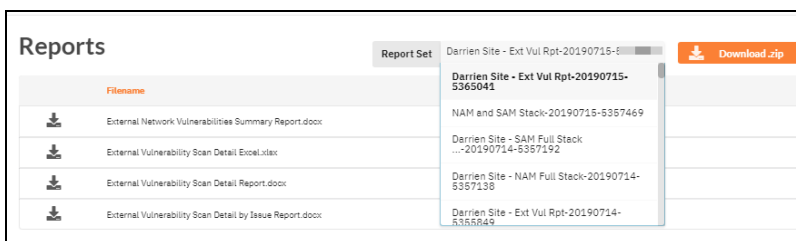
[Help & Support](#) | © Kaseya 2022

- 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.



- If necessary, click on the **Reports** tab.
- 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 **download reports together as a .zip file**. The reports will be in MS Word format.



Appendices

This section contains other helpful topics related to Reporter:

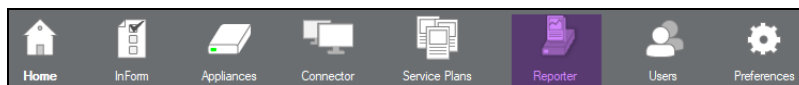
<u>Reporter Templates</u>	163
<u>Create and Deploy Reporter Templates</u>	164
<u>Custom Reports</u>	175
<u>Generate Client Progress Reports</u>	183
<u>Set Scan and Report Task Time Zone and Date Format</u>	187
<u>Automate Microsoft Cloud Assessment and Reports with Reporter</u>	189
<u>Automate AWS Assessment and Reports with Reporter</u>	196
<u>Authenticate Exchange Scan using Enterprise App</u>	203
<u>Integrate Reporter with a PSA System with Export Tasks</u>	212
<u>Software Appliance Diagnostic Tool</u>	258
<u>Augment Reporting to Eliminate False Positives</u>	261
<u>Updating a Software Appliance</u>	265
<u>Set Up Custom SMTP Server Support (Reporter)</u>	267
<u>Client-Connector Diagram</u>	271
<u>Using Reporter with Cyber Hawk</u>	272
<u>Pre-Scan Network Configuration Checklist</u>	277

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!

Create and Deploy Reporter Templates

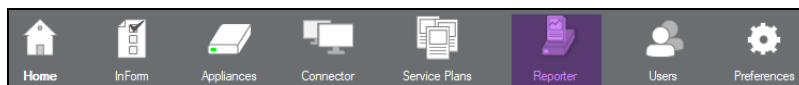
Reporter Templates allow you to create re-usable sets of report tasks for multiple Reporter Sites at the same time.

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 17](#).

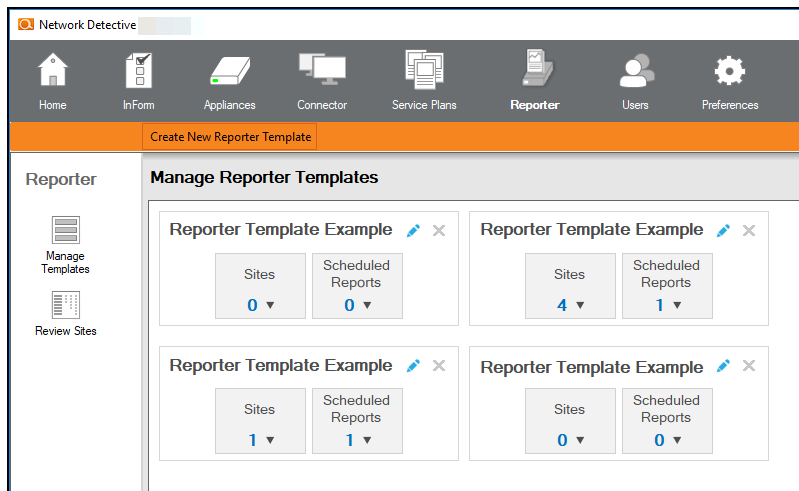
To create and deploy a Reporter Template, follow these steps:

Step 1 — Create New Reporter Template

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



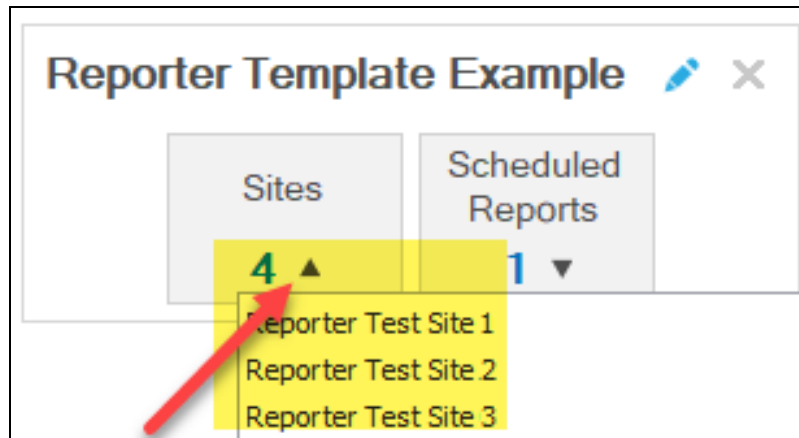
The **Manage Reporter Templates** screen will appear.



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

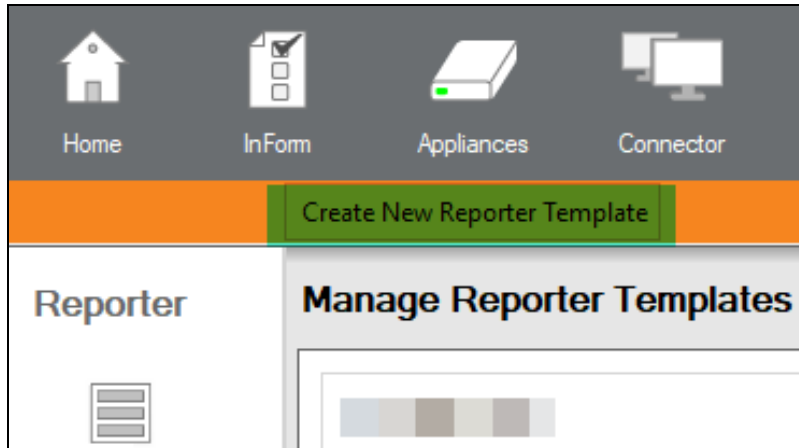
- **Number of Sites** template has been applied to
- **Number of Scheduled Reports** included in the template

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

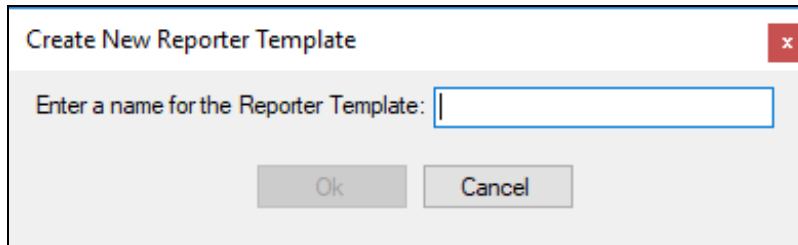


Note: Here you can also see the "preset" Reporter Templates available for you to configure. If you want to get started with one of the preset templates, click the Edit icon  on the template, and go to ["Step 2 — Assign Reports to Template" on the next page.](#)

- Click **Create New Reporter Template**.

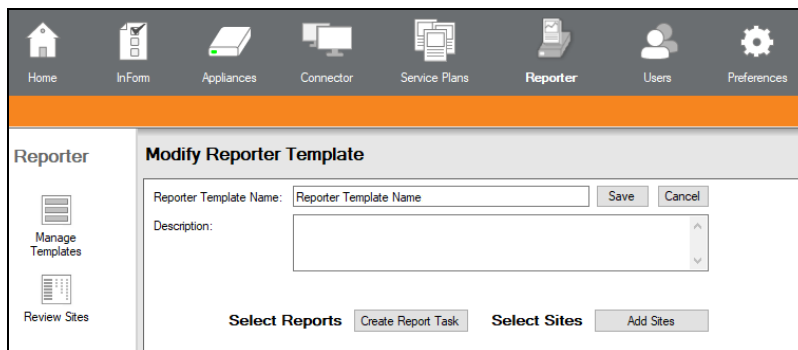


- Enter a name** for the Reporter Template.



A dialog box titled "Create New Reporter Template" with a red close button in the top right corner. It contains a text input field with the placeholder text "Enter a name for the Reporter Template:". Below the input field are two buttons: "Ok" and "Cancel".

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



The "Modify Reporter Template" screen is displayed within the Network Detective application. The top navigation bar includes icons for Home, InForm, Appliances, Connector, Service Plans, Reporter (highlighted), Users, and Preferences. The left sidebar shows "Reporter" with sub-options "Manage Templates" and "Review Sites". The main content area is titled "Modify Reporter Template" and contains a form with the following fields and buttons:

- "Reporter Template Name:" with a text input field and "Save" and "Cancel" buttons.
- "Description:" with a large text area.
- At the bottom, there are four buttons: "Select Reports", "Create Report Task", "Select Sites", and "Add Sites".

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.

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

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

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

Type	Task Label	Description	End
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... notification to be sent to lwrenn@rapidfiretools.com. InDoc upload enabled.	

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

Collector (RDC). Reporter and all RDCs must be set up properly for each Site. See ["Setting Up Reporter" on page 17](#).

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 79](#).
 - 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 125](#).
 - 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](#)

[View for Reporter" on page 154.](#)

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: ~yyyMMdd

☒ 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:

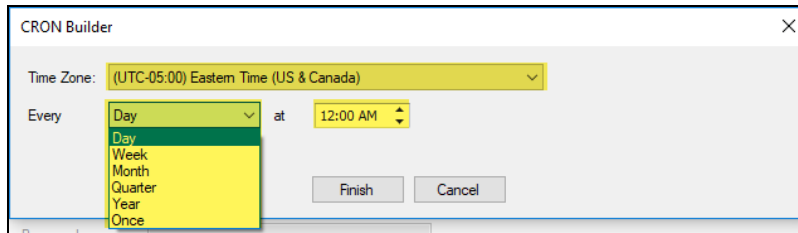
Back Next Cancel

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.

The CRON Builder dialog box is shown. It has a title bar with a close button. The 'Time Zone' dropdown is set to '(UTC-05:00) Eastern Time (US & Canada)'. The 'Every' dropdown is open, showing options: Day, Day, Week, Month, Quarter, Year, and Once. The 'at' dropdown is set to '12:00 AM'. There are 'Finish' and 'Cancel' buttons at the bottom right.

CRON Builder

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

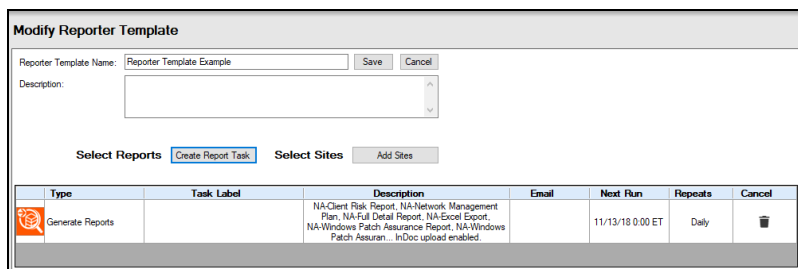
Every: Day at 12:00 AM

Finish Cancel

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 173](#) for more details.

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

The Modify Reporter Template dialog box is shown. It has a title bar. The 'Reporter Template Name' field contains 'Reporter Template Example' and has 'Save' and 'Cancel' buttons. The 'Description' field is empty. Below the fields are buttons for 'Select Reports', 'Create Report Task', 'Select Sites', and 'Add Sites'. At the bottom is a table with columns: Type, Task Label, Description, Email, Next Run, Repeats, and Cancel.

Modify Reporter Template

Reporter Template Name: Reporter Template Example Save Cancel

Description:

Select Reports Create Report Task Select Sites Add Sites

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 Assurance - 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:

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

Modify Reporter Template

Reporter Template Name:

Reporter Template Example

Save

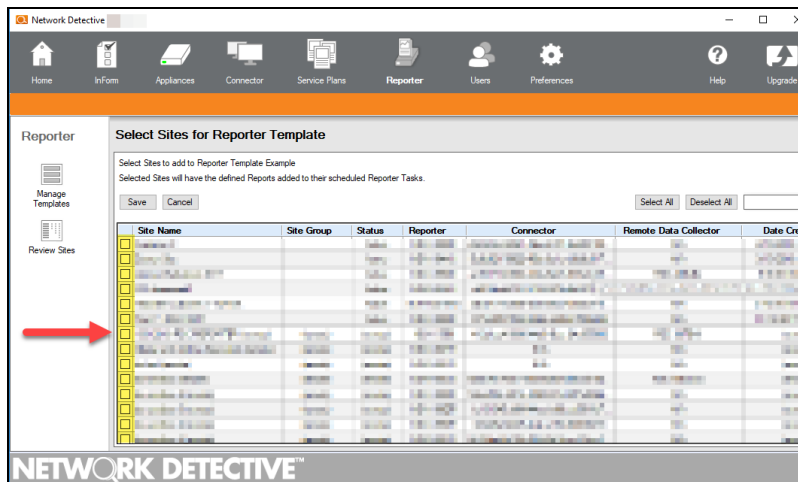
Cancel

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.



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:

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 Assurance - InDoc upload enabled.		11/15/18 0:00 ET	Daily	

Site	Modified	Remove
	No	

The Reporter Template Tasks will also appear on the Reporter dashboard on each Site that you applied it to:

Tasks

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.

Tasks

Type	Task ...	Description	Scheduled?	Remote Data Colle...	Reporter Template
Generate ...		NA-Client Risk Report, N...	Yes	N/A	Reporter Template Example (Modified)
Generate ...		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 90](#).

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

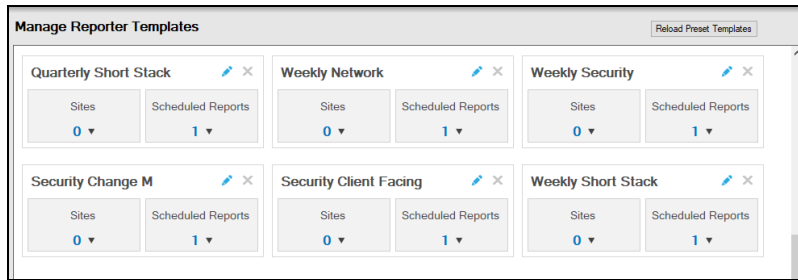
Particularly large tasks for multiple sites could take several hours to complete. Keep this in mind when scheduling Report Tasks for your Sites using Reporter Templates.

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.

- There are also both client-facing and in-house reporting presets.

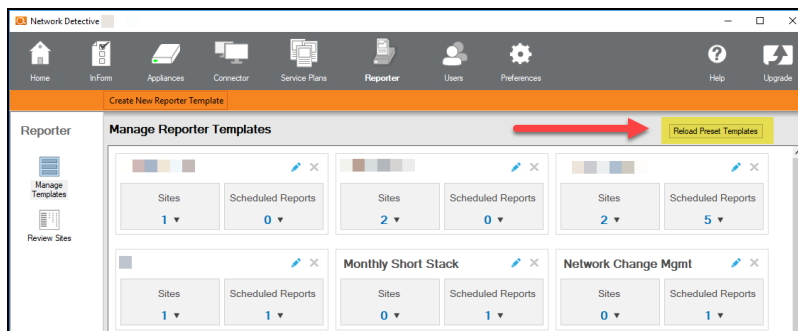


Reload Preset Templates

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.



Custom Reports

You can use the Reporter Custom Reports feature to create a custom Network Assessment Module Full Detail Report.

Prerequisites:

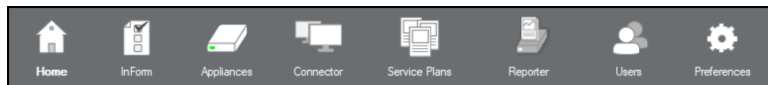
- Customer must subscribe to the Network Assessment Module
- Customer must subscribe to the Reporter
- Customer must have updated their Network Detective application installation to the latest version of ND
- Customer must have updated their Reporter to the latest version of Reporter
- Customer must 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:

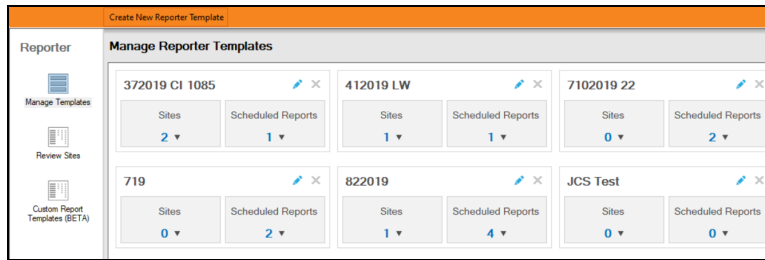
- ["Create a Custom Report Template" below](#)
- ["Create a Report Generation Task using the Custom Full Detail Report Template" on page 179](#)

Create a Custom Report Template

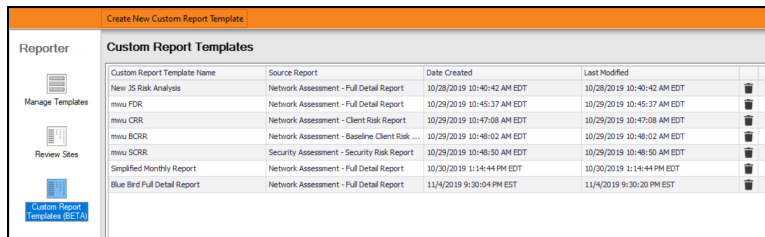
1. Log in to Network Detective.
2. Open a Network Detective **Site** associated with Reporter.
3. Select the **Reporter** icon on the Network Detective top ribbon bar.



The **Manager Reporter Templates** window is displayed.

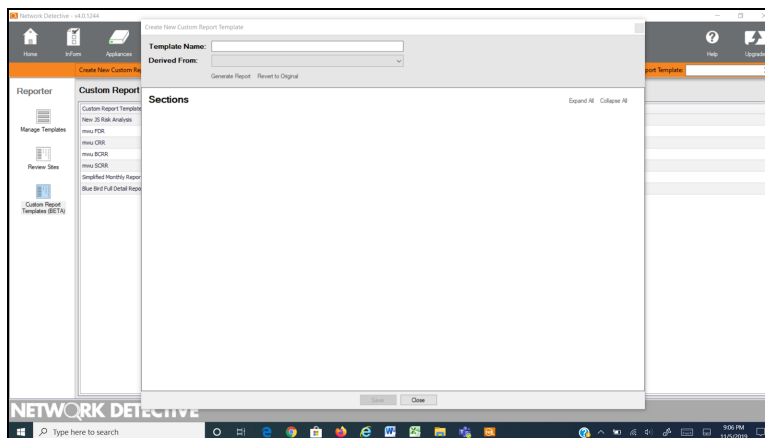


4. Select the Custom Reports Templates icon in the left hand ribbon bar.

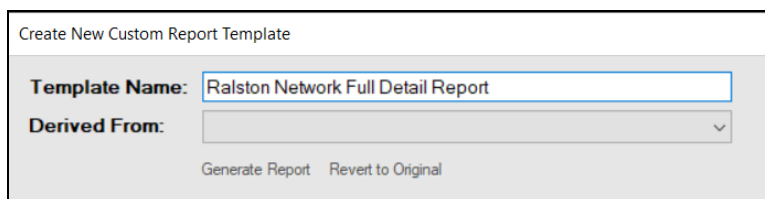


This Custom Reports window is displayed.

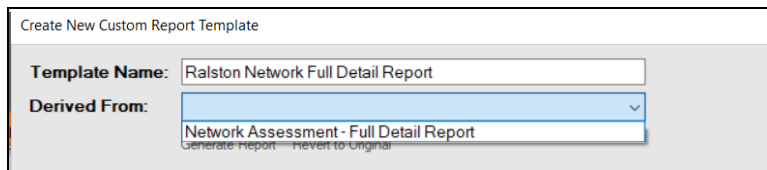
5. Select the **Create New Customer Report Template** button.
6. The Create New Custom Report Template window is displayed.



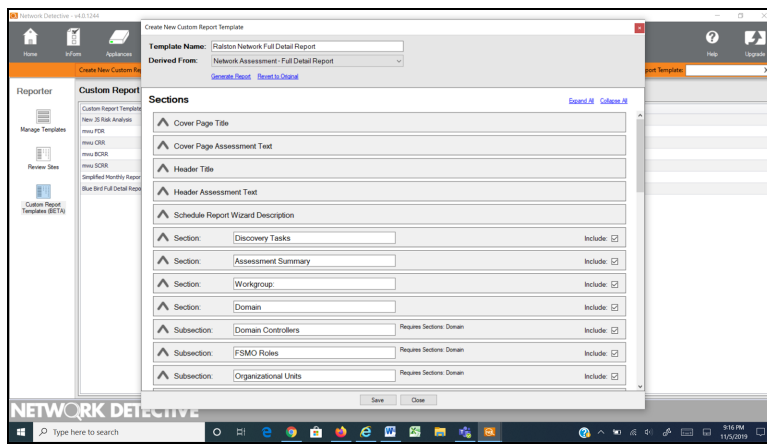
7. Type in the name of the new Custom Report Template.



8. Select the Network Assessment - Full Detail Assessment option from the Derived From list.

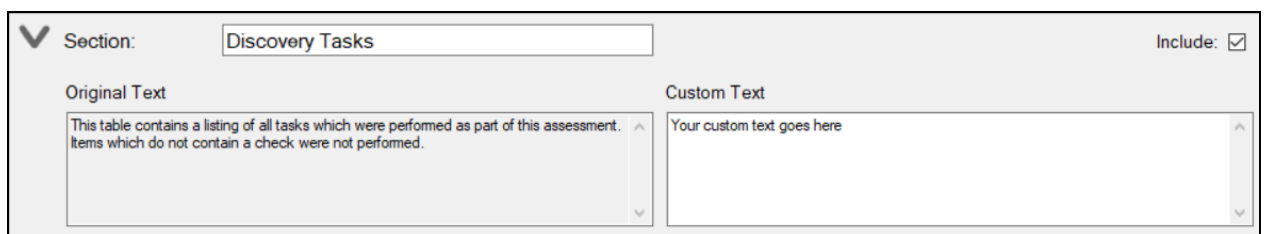


9. The Sections of the Full Detail Report that can be customized are presented in the Create New Custom Report Template window.



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.



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.

Template Name: Ralston Network Full Detail Report

Derived From: Network Assessment - Full Detail Report

Generate Report Revert to Original

Sections

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

Generate Report Revert to Original

Sections

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.

Subsection: Domain Controllers Requires Section: Domain Include: ☒

Subsection: FSMO Roles Requires Section: Domain Include: ☒

Subsection: Cross-Organizational Links Requires Section: Domain Include: ☒

Save Close

13. The following information will be displayed in the Create New Custom Report Template window.

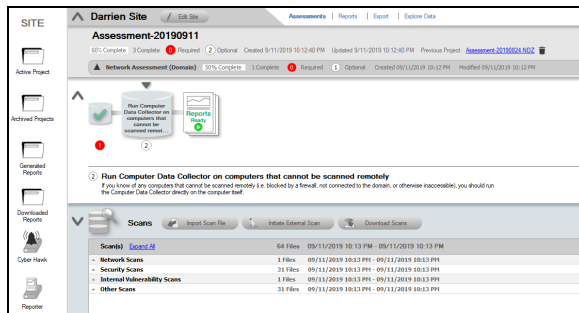
Date Created: 11/5/2019 10:01:27 PM EST by jstark@rapidfiretools.com

Last Modified: 11/5/2019 10:01:31 PM EST by jstark@rapidfiretools.com

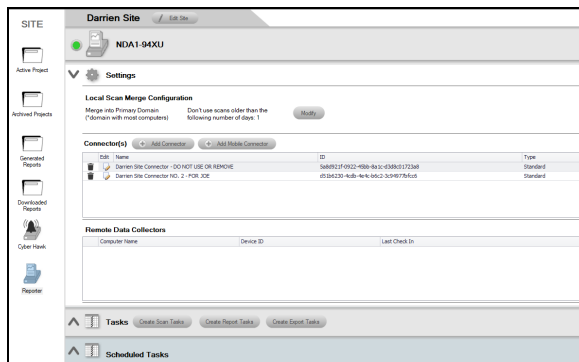
14. Select the Close button to close the Create New Custom Report Template window.

Create a Report Generation Task using the Custom Full Detail Report Template

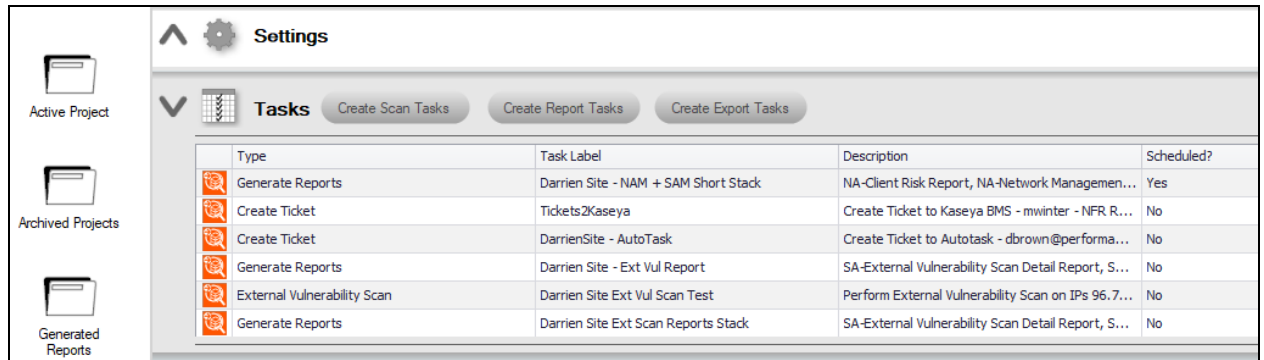
1. Log into Network Detective.
2. Open the Network Detective Site associated with the Reporter.
3. Select the Reporter icon on the left hand ribbon bar.



The Reporter UI will be displayed.

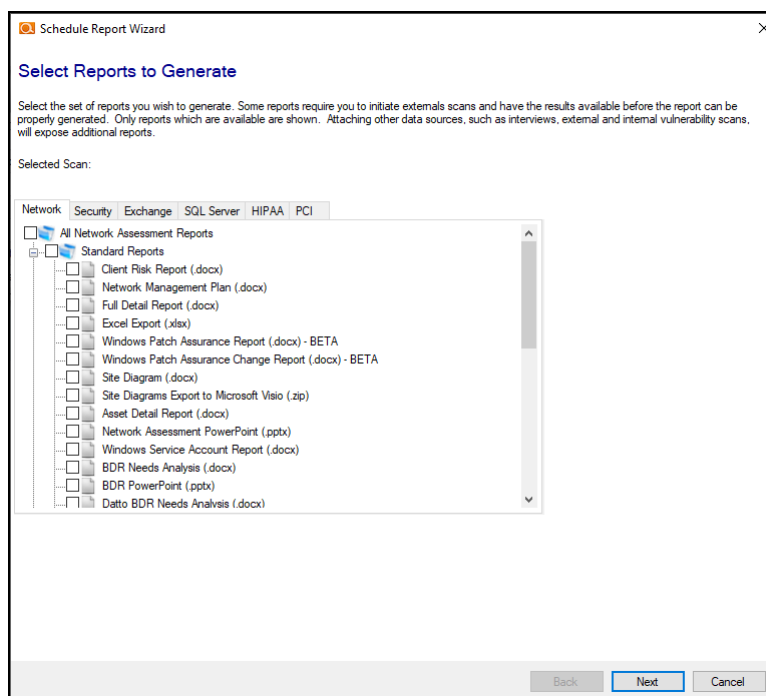


4. Click on the Tasks  Selector to expand the Reporter Tasks list.
5. The Tasks list is expanded.



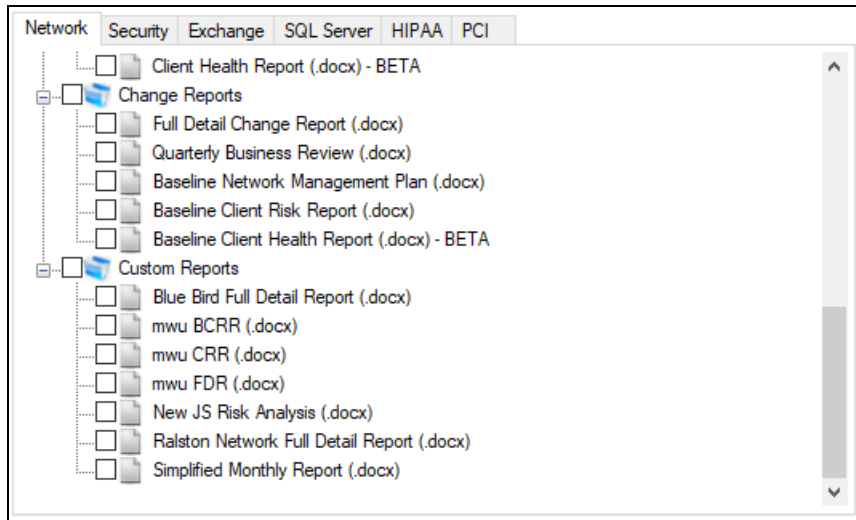
6. Select the Create Report Tasks button

The Schedule Reports Window is displayed.

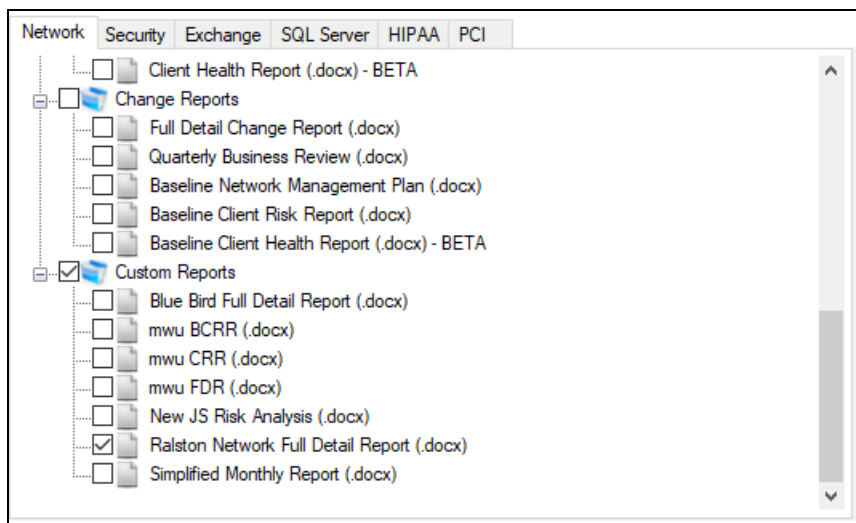


7. Select the Network Tab to display the Reports list of the Network Assessment Module.

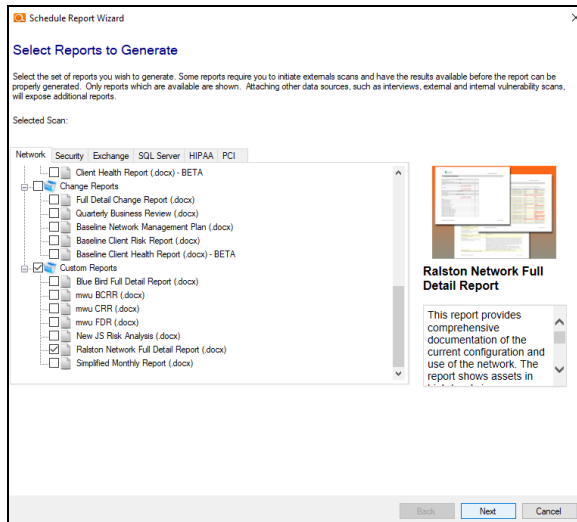
8. Scroll to the bottom of the Network Assessment Module Reports List to view the available customer Reports. (Note that the "Ralston Network Full Detail Report" created as a Custom Report Template is available on the Custom Reports list).



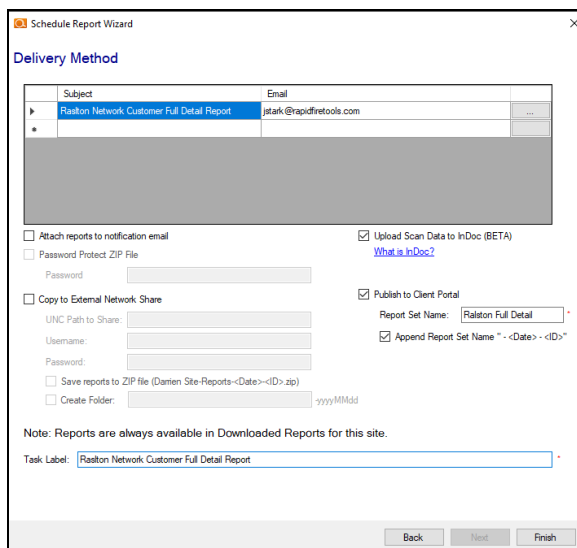
9. Select the Custom Report that is to be generated by the Report Task being created.



10. Select the Next button to proceed in creating the Report Task.



11. Set up the Delivery Method for the Report Task.



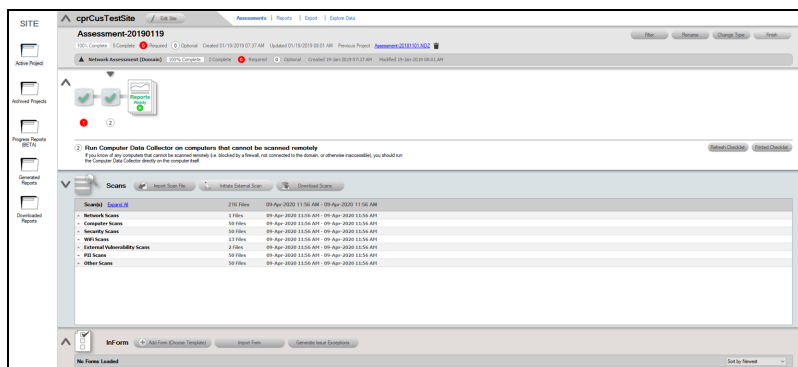
12. Select the Finish button to complete the creation of the Report Task for the Custom Report.
13. Either select the newly created Custom Report Task's "Run Now" link to generate the report, or schedule the report to the generated at a schedule Day and Time.

Generate Client Progress Reports

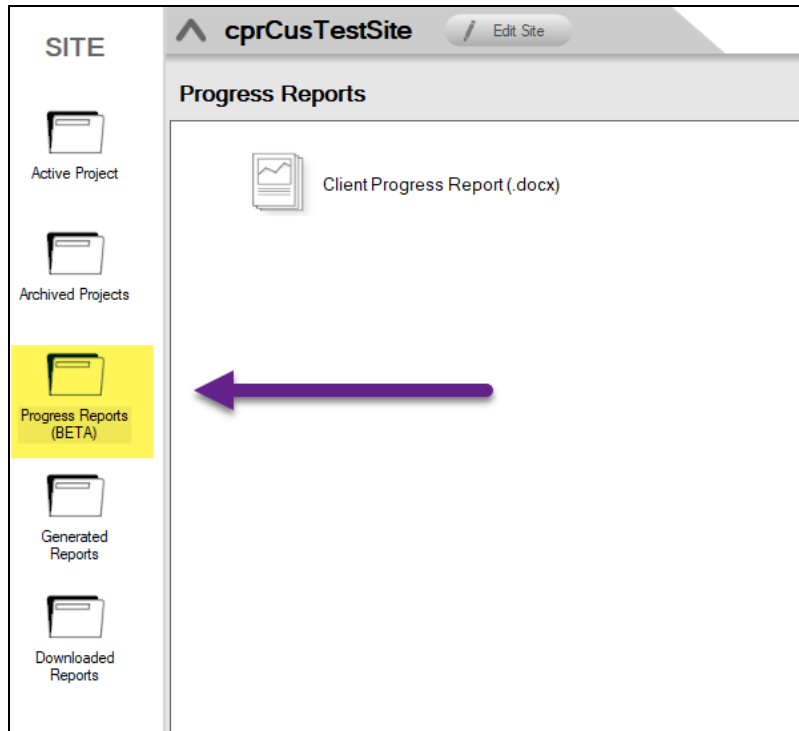
The **Client Progress Report** is designed to be generated after you have completed several Network and Security Assessments. You can find an example here. This report compares key areas over time and display trending changes with charts and graphs. Computers are given a letter grade ('A' through 'F').

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.

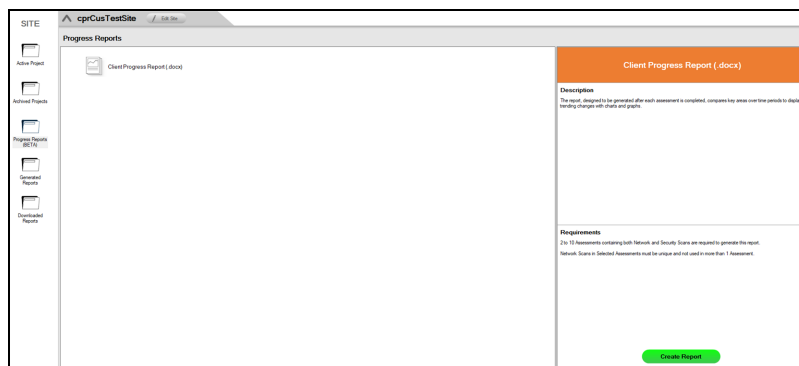
1. Open a Reporter site with two or more archived assessments containing both Network and Security Scans. These assessments can be archived. A current assessment is not required.



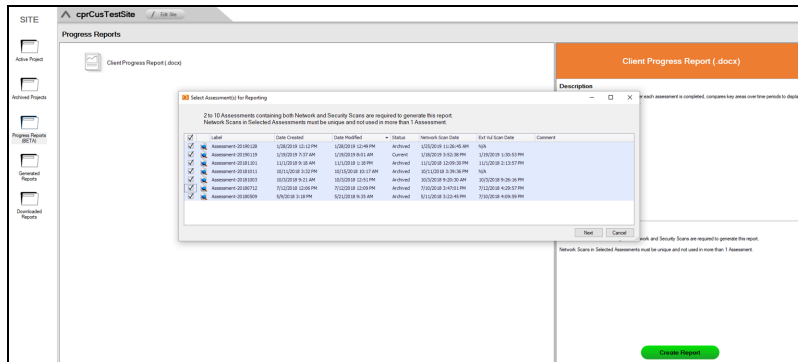
2. On the left-hand site menu, click **Progress Reports (BETA)**.



3. Click **Client Progress Reports (.docx)**. From the side panel, you can find report details and requirements.

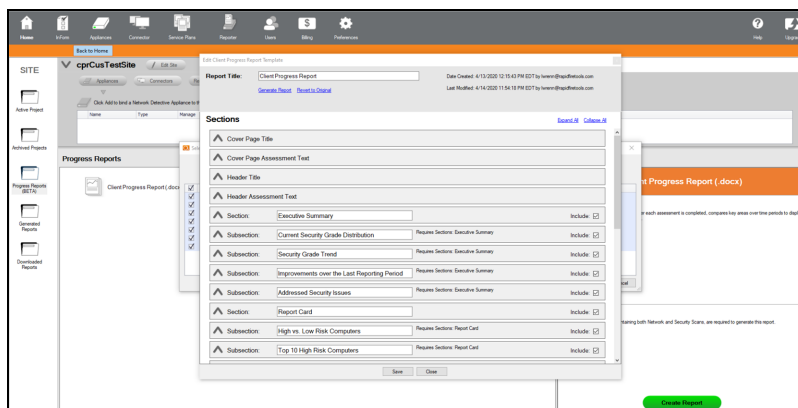


4. From the side panel, click **Create Reports**.
5. Select which assessments to include in the report (minimum of 2). All assessments are included in the report by default (up to 10). Then click **Next**.

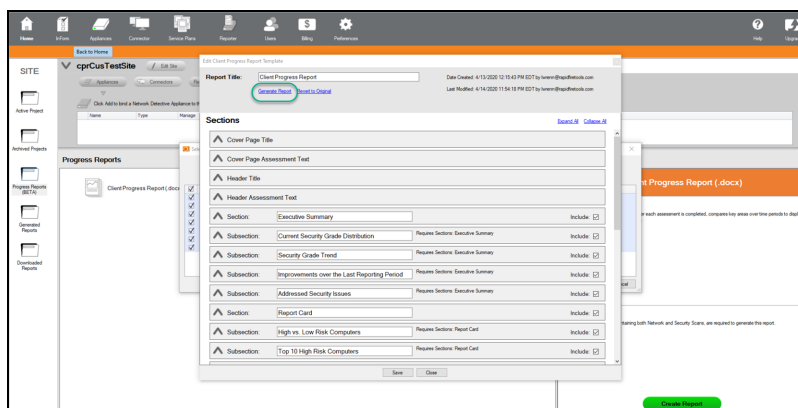


- From the **Edit Client Progress Reports** screen, you can change and edit the text of the report, including its title and subsections. You can likewise add custom text to each section and decide to exclude certain sections, if you choose.

Note: Click **Save** to keep a record of your edits to the report. Date Created and Date Modified are displayed on the form.



- When you are ready, click **Generate Report**. After the report is built, it will appear in Windows File Explorer.



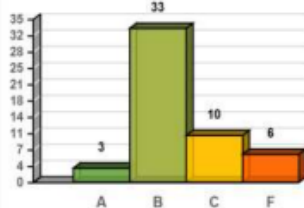
[You can find an example Client Progress Report here.](#)

Executive Summary

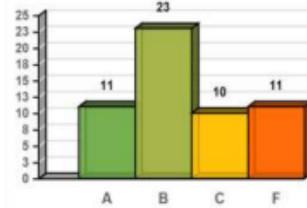
As part of our ongoing services to ensure the health of your business IT, we regularly scan the environment collecting large amounts of data. We use the data to perform network and security assessments to evaluate both overall health of the network as well as individual computers.

Computers are given a letter grade ('A' through 'F'). Below is the current computer security score breakdown of the IT environment.

Current Security Grade Distribution
(19-Jan-2019 7:37 AM)

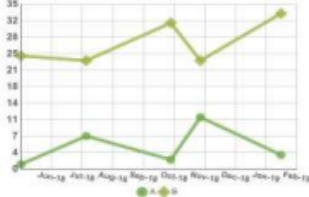


Previous Security Grade Distribution
(01-Nov-2018 9:18 AM)

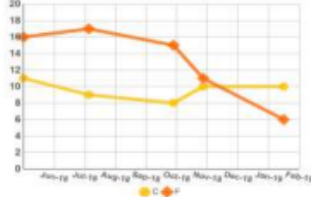


Our goal is "peak performance" of all your computers. To objectively measure how well we are doing, we try to increase the number of computers receiving an 'A' grade over time. Certain factors, like the introduction of new systems, failed updates, or misconfigurations can cause issues and lower scores.

Security Grade Trend - Low Risk Computers



Security Grade Trend - High Risk Computers



Set Scan and Report Task Time Zone and Date Format

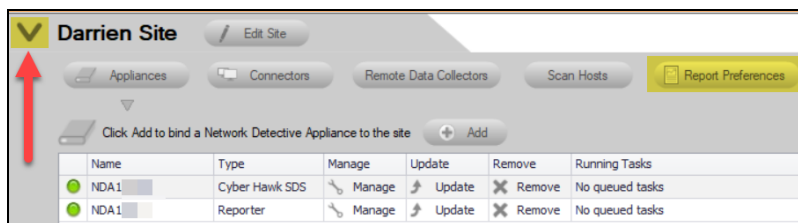
You can configure the time zones and dates that appear next to your Site's scan and report tasks. This feature applies to both **Reporter** and **Inspector** for Network Detective.

- 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.

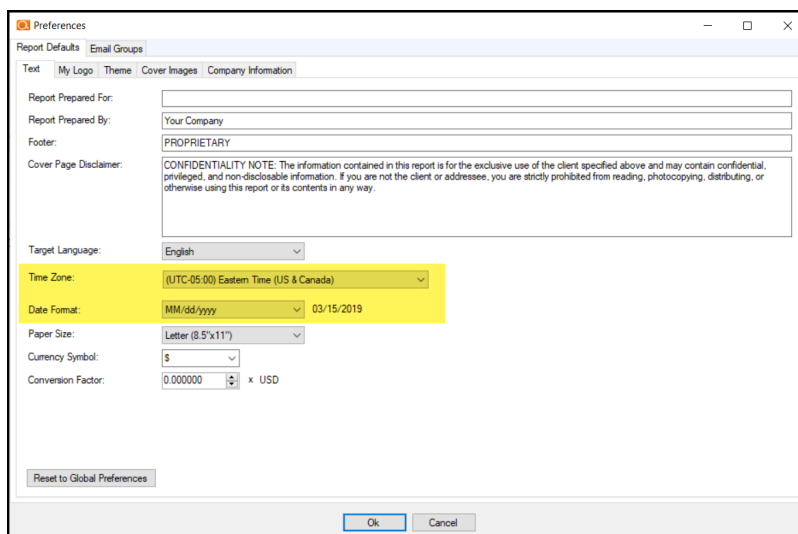
To set preferences:

At Site Level

1. Open your **Reporter** or **Inspector** Site in Network Detective.
2. Open the Site Settings and click **Report Preferences**.



3. From **Report Defaults > Text**, select your desired **Time Zone** and **Date Format**. Click **OK**.

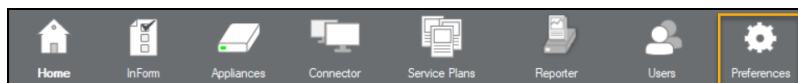


Your scheduled scan and report tasks will now appear with your preferred time zone and date format for just this site.

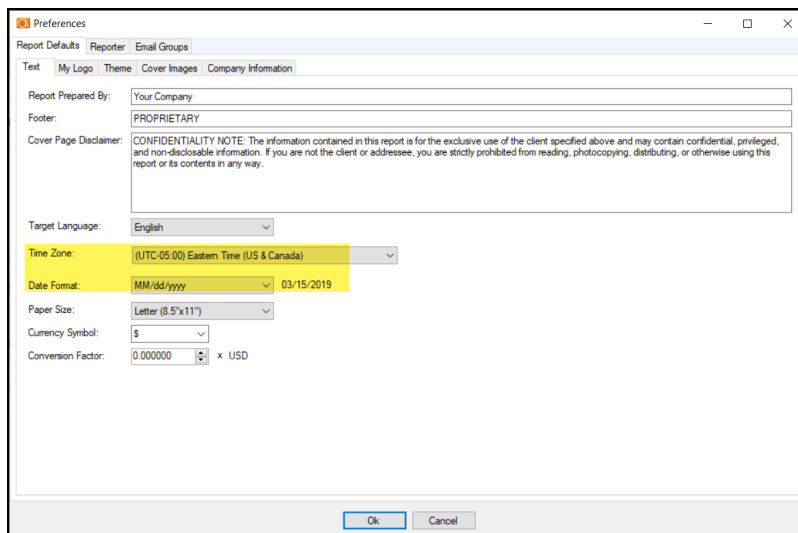
Status	Next Run Date	Last Run Date	Repeats
Pending	03/08/2020 4:30 PM ADT		No
Pending	03/15/2019 10:05 PM ADT	03/14/2019	Daily
Pending	03/16/2019 7:30 PM ADT	03/15/2019	Daily

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**.



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.

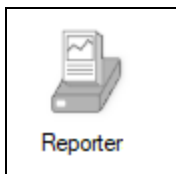
Automate Microsoft Cloud Assessment and Reports with Reporter

You can **automate** your Microsoft Cloud Assessment using **Reporter**. This allows you to perform scheduled scans and generate Microsoft Cloud Assessment reports for your sites at whatever interval you choose.

To automate your Microsoft Cloud Assessment:

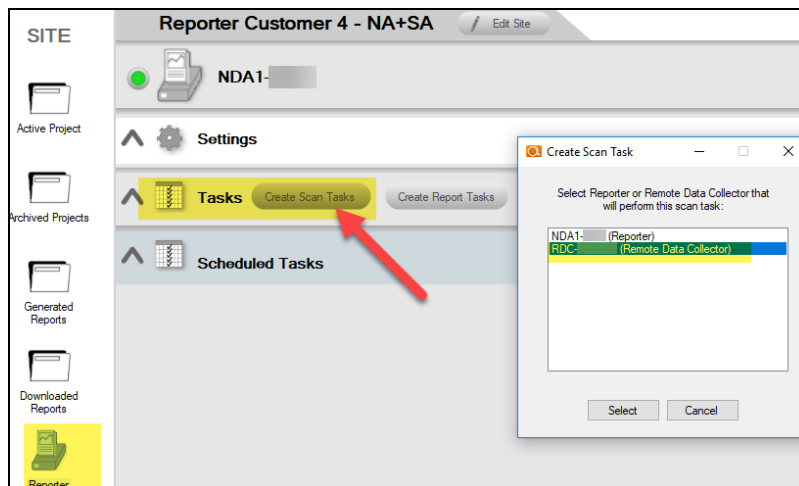
Step 1 — Create MS Cloud Scan task

1. First, ensure you have set up the [Prerequisites to Perform Cloud Scan using Enterprise App](#). To create the automatic Microsoft Cloud scan task, you must have the **Tenant ID**, **Client ID**, and **Client Secret Value** for the Microsoft Cloud/Azure tenant to be assessed.
2. Second, ensure you have set up **Reporter** and assigned the appliance to your Microsoft Cloud Assessment site. This includes the **Remote Data Collector** and **Connector**. See the Reporter User Guide at <https://www.rapidfiretools.com/nd-downloads> for a complete walkthrough.
3. Once you have Reporter set up, navigate to your Microsoft Cloud Assessment site.
4. Click the **Reporter** icon from the left-hand menu to open the Reporter console.

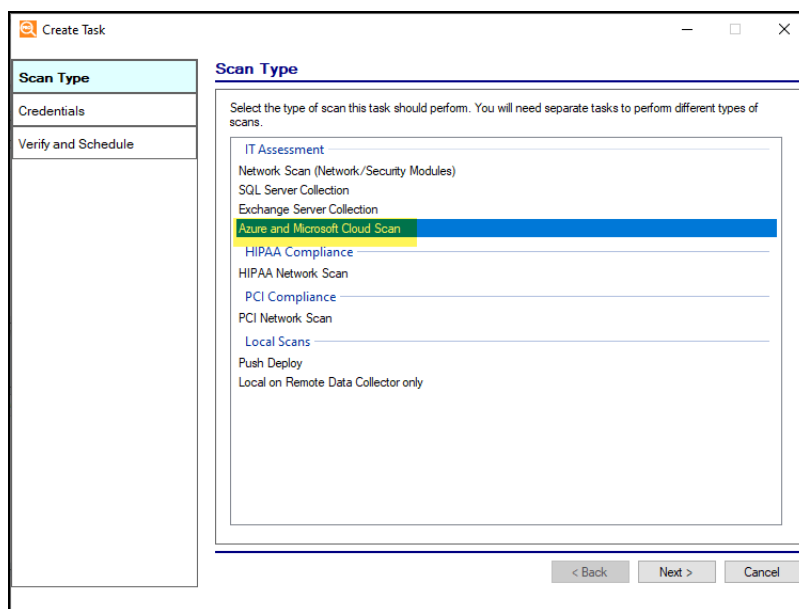


Tip: Verify that your **Reporter appliance** and **Remote Data Collector** are online from the **Settings** panel.

5. Click **Create Scan Task** and choose the **Remote Data Collector**. Click **Select**.



6. Choose **Azure and Microsoft Cloud Scan** and click **Next**.



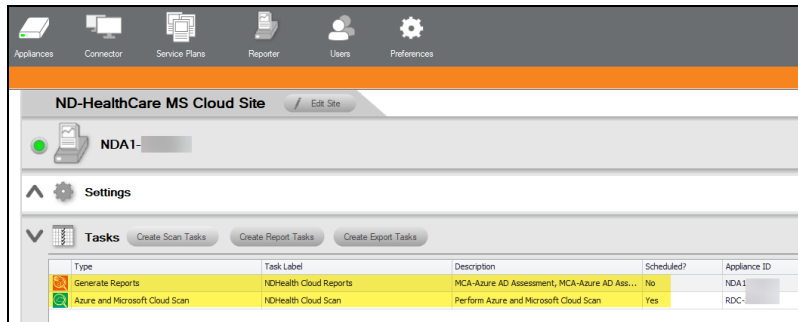
7. Enter the **Tenant ID**, **Client ID**, and **Client Secret Value** for the Microsoft Cloud/Azure tenant to be assessed.

The screenshot shows the 'Create Task - Azure and Microsoft Cloud Scan' window. On the left, a sidebar contains three steps: 'Scan Type' (checked), 'Credentials' (highlighted), and 'Verify and Schedule'. The main area is titled 'Credentials' and contains the text 'Enterprise Application Credentials' and a link 'Click here for documentation on how to setup the required Enterprise Application.' Below this, there are three input fields: 'Tenant Id:', 'Client Id:', and 'Client SecretValue:'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8. Enter a **Task Label** and optionally configure an email notification for when the scan completes. Click **Finish**.

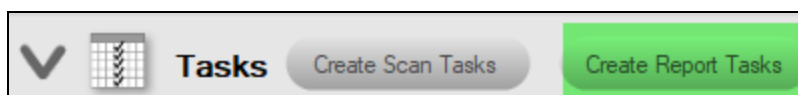
The screenshot shows the 'Create Task - Azure and Microsoft Cloud Scan' window. On the left, a sidebar contains three steps: 'Scan Type' (checked), 'Credentials' (checked), and 'Verify and Schedule' (highlighted). The main area is titled 'Verify and Schedule' and contains the text 'Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.' Below this, there is an 'Email Notification' section with a checkbox 'Send email notification when schedule completes' and an 'Email Address:' input field. To the right of the email address field is a link 'Use Login User'. Below the email notification section is a 'Task Label:' input field. At the bottom left, there is a 'Modify Settings' button. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Your new Cloud Scan task will appear in the Tasks library for this site.

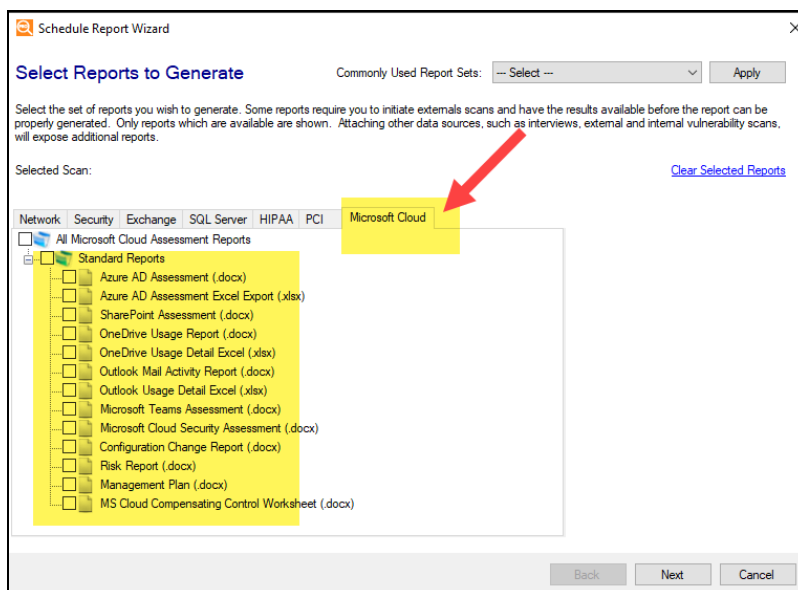


Step 2 — Create MS Cloud Report Task

1. Next, you need to create a Report Task to transform your scan data into automated Microsoft Cloud Assessment reports.
2. Click **Create Report Tasks**.



3. Select the **Microsoft Cloud** tab. Then select the Microsoft Cloud Assessment reports that you want to generate.



4. Click **Next**.

- From the **Delivery Method** screen, configure how and where to publish your report. You can also simply download the reports from the appliance when the report job finishes. Enter a task label and click **Finish**.

Schedule Report Wizard

Delivery Method

Subject	Email
Network Detective Notification	

☐ Attach reports to notification email
 ☐ Upload Scan Data to InDoc
[What is InDoc?](#)

☐ Password Protect ZIP File
 Password:

☐ Copy to External Network Share
 ☐ Publish to Client Portal
 UNC Path to Share: Report Set Name:

Username:
☒ Append Report Set Name " - <Date> - <ID>"

Password:

☐ Save reports to ZIP file (ND-HealthCare MS Cloud Site-Reports-<Date>-<ID>.zip)

☐ Create Folder: -yyyyMMdd

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

Task Label:

Back Next Finish

- See the Reporter User Guide at <https://www.rapidfiretools.com/nd-downloads> for more details regarding how to configure Reporter delivery methods.

Your new Cloud Scan report task will appear in the Tasks library for this site.

Type	Task Label	Description	Scheduled?	Appliance ID
Generate Reports	NDHealth Cloud Reports	MCA-Azure AD Assessment, MCA-Azure AD Ass...	No	NDA1
Azure and Microsoft Cloud Scan	NDHealth Cloud Scan	Perform Azure and Microsoft Cloud Scan	Yes	RDC-

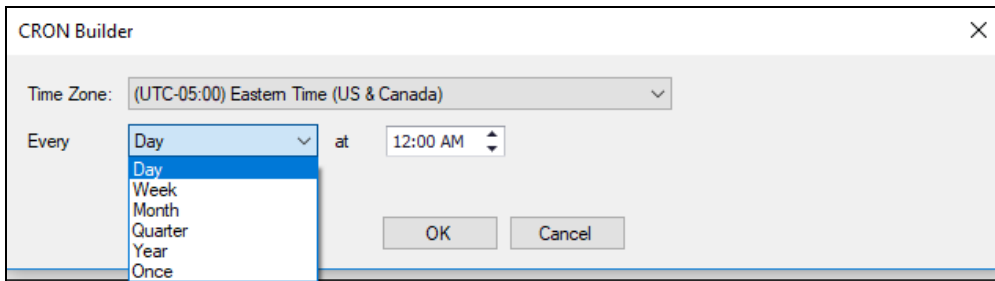
Step 3 — Schedule Scan and Report Tasks

Once you create both the scan and report task, it's time to schedule the tasks.

1. First, schedule the Scan Task. Next to the Microsoft Cloud task, click **Schedule**.

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

2. Assign an interval to the scan task then click **OK**.



CRON Builder

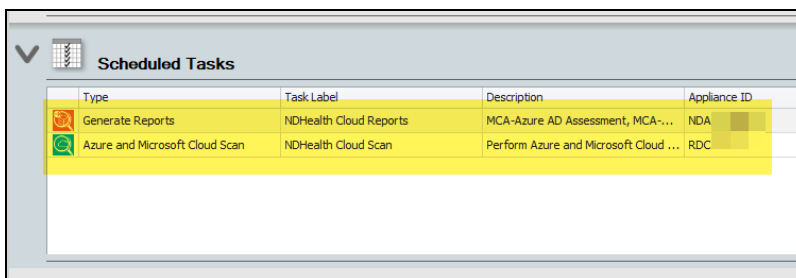
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Every Day at 12:00 AM

OK Cancel

Important: Be sure to schedule the Microsoft Cloud scan task to begin several hours **BEFORE** your report task. This will ensure your reports contain the latest data from the complete scan.

3. The Microsoft Cloud Scan will then appear in the queue of scheduled scan tasks. Alternatively, you can click **Run Now** from the scan task library to begin the scan immediately.



Type	Task Label	Description	Appliance ID
 Generate Reports	NDHealth Cloud Reports	MCA-Azure AD Assessment, MCA-...	NDA
 Azure and Microsoft Cloud Scan	NDHealth Cloud Scan	Perform Azure and Microsoft Cloud ...	RDC

4. Finally, schedule the Microsoft Cloud Assessment report task. To the right of the report task, click **Schedule**. Assign an interval to the report task then click **OK**.

Important: Be sure to schedule the Microsoft Cloud report task to begin a few hours **AFTER** the scan task. This will ensure your reports contain the latest data from the complete scan.

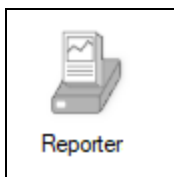
Automate AWS Assessment and Reports with Reporter

You can **automate** your AWS Assessment using **Reporter**. This allows you to perform scheduled scans and generate AWS Assessment reports for your sites at whatever interval you choose.

To automate your AWS Assessment:

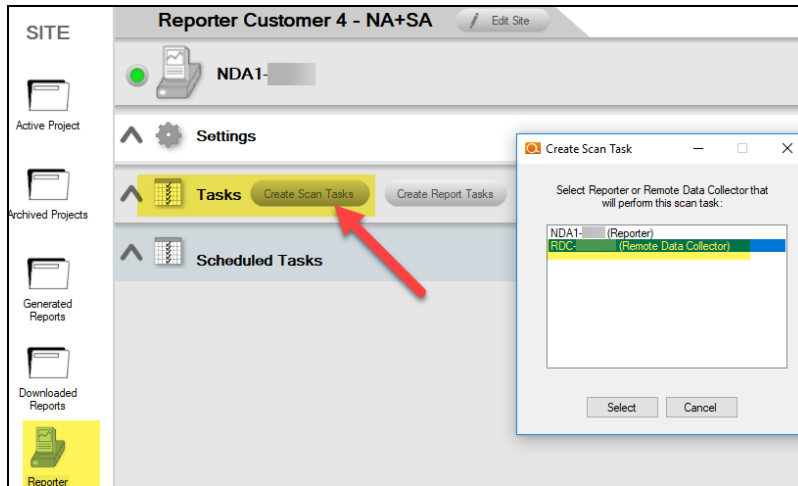
Step 1 — Create AWS Scan task

1. First, ensure you have gathered the **AWS Access Key** and **Secret Key** for the target environment. See the AWS Quick Start Guide at <https://www.rapidfiretools.com/nd-downloads> for a complete walkthrough.
2. Second, ensure you have set up **Reporter** and assigned the appliance to your AWS Assessment site. This includes the **Remote Data Collector** and **Connector**. See the Reporter User Guide at <https://www.rapidfiretools.com/nd-downloads> for a complete walkthrough.
3. Once you have Reporter set up, from your site click the **Reporter** icon from the left-hand menu to open the Reporter console.

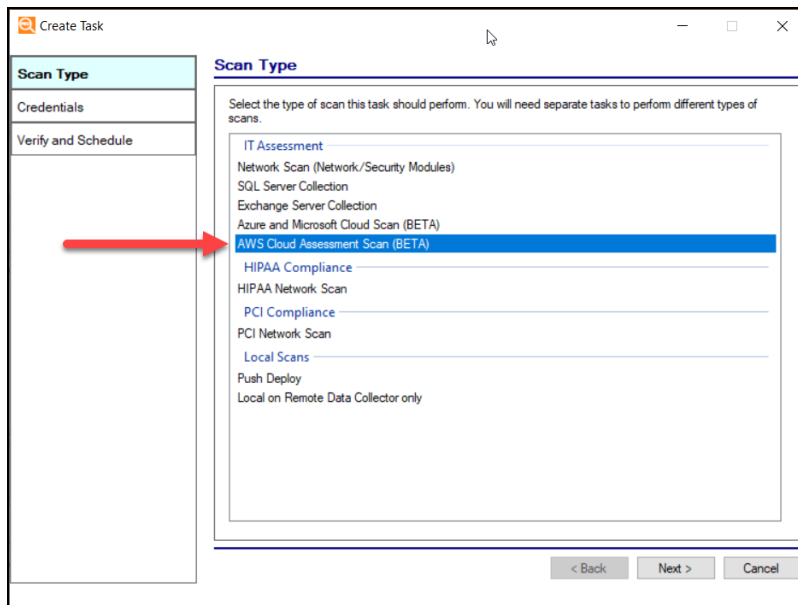


Tip: Verify that your **Reporter appliance** and **Remote Data Collector** are online from the **Settings** panel.

4. Click **Create Scan Task** and choose the **Remote Data Collector**. Click **Select**.



5. Choose **AWS Scan** and click **Next**.



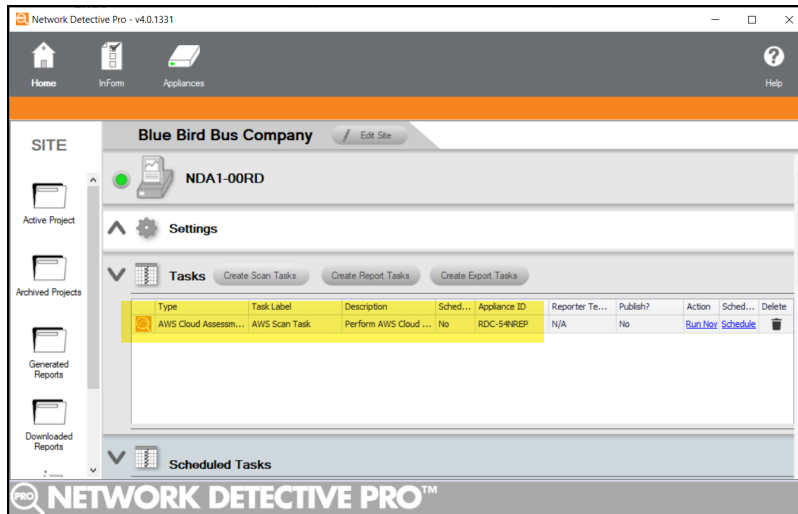
6. Enter the **AWS Access Key** and **Secret Key** for the AWS tenant to be assessed.

The screenshot shows the 'Create Task - AWS Cloud Assessment Scan (BETA)' window. On the left, a sidebar contains three steps: 'Scan Type' (checked), 'Credentials' (highlighted in light blue), and 'Verify and Schedule'. The main area is titled 'Credentials' and contains the text 'Amazon Web Services Credentials' and a link 'Click here for documentation on how to setup the required AWS credentials.' Below this are two input fields: 'AWS Access Key ID:' and 'AWS Secret Access Key:'. Both fields are highlighted in yellow. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted in blue), and 'Cancel'.

7. Enter a **Task Label** and optionally configure an email notification for when the scan completes. Click **Finish**.

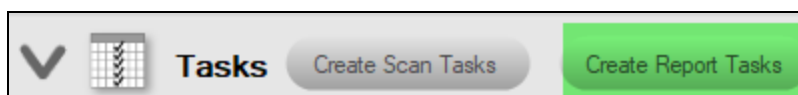
The screenshot shows the 'Create Task - AWS Cloud Assessment Scan (BETA)' window. On the left, a sidebar contains three steps: 'Scan Type' (checked), 'Credentials' (checked), and 'Verify and Schedule' (highlighted in light blue). The main area is titled 'Verify and Schedule' and contains the text 'Press the Finish button to save the task. Use the Back button to go back and modify any previous changes.' Below this is an 'Email Notification' section with a checkbox 'Send email notification when schedule completes' and an 'Email Address' field containing 'jweakland@rapidfiretools.com'. There is a 'Use Login User' link. Below the email section is a 'Task Label' field. At the bottom left, there is a 'Modify Settings' button. At the bottom right, there are three buttons: '< Back', 'Finish' (highlighted in blue), and 'Cancel'.

Your new AWS scan task will appear in the Tasks library for this site.

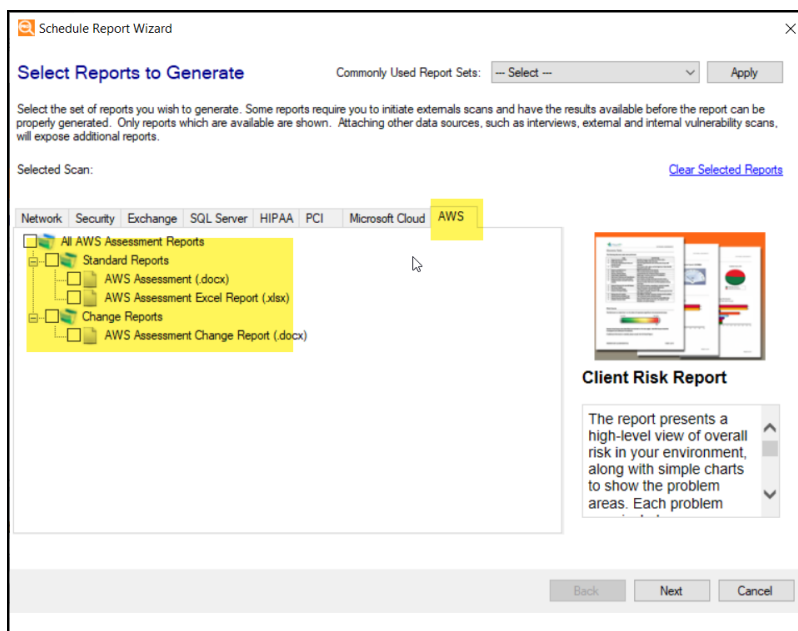


Step 2 — Create MS Cloud Report Task

1. Next, you need to create a Report Task to transform your scan data into automated AWS Assessment reports.
2. Click **Create Report Tasks**.



3. Select the **AWS** tab. Then select the AWS reports that you want to generate.



4. Click **Next**.
5. From the **Delivery Method** screen, configure how and where to publish your report. You can also simply download the reports from the appliance when the report job finishes. Enter a task label and click **Finish**.

Schedule Report Wizard

Delivery Method

Subject	Email
Network Detective Notification	

☐ Attach reports to notification email ☒ Upload Scan Data to InDoc

☐ Password Protect ZIP File

Password:

☐ Copy to External Network Share ☐ Publish to Client Portal

UNC Path to Share: Report Set Name:

Username: ☒ Append Report Set Name " - <Date> - <ID> "

Password: ☐ Export to IT Glue [Choose Connection](#)

☐ Save reports to ZIP file (Blue Bird Bus Company-Reports-<Date>-<ID>.zip)

☐ Create Folder: -yyyyMMdd

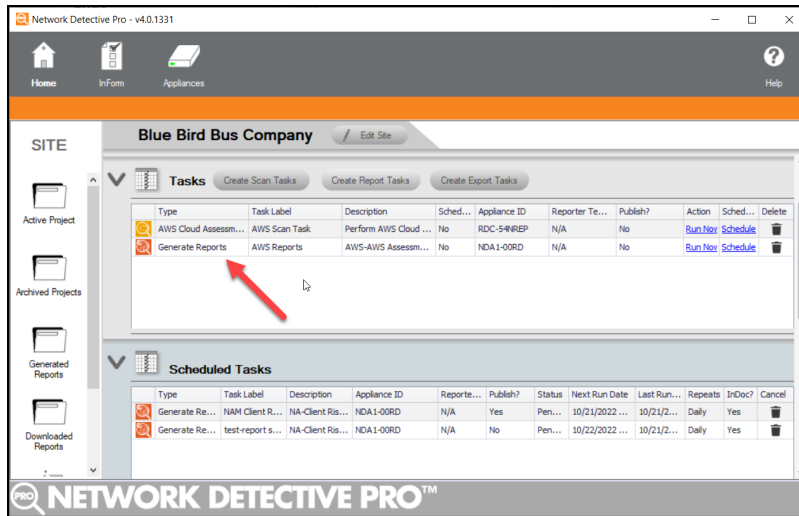
Note: Reports are always available in Downloaded Reports for this site.

Task Label:

Back Next Finish

6. See the Reporter User Guide at <https://www.rapidfiretools.com/nd-downloads> for more details regarding how to configure Reporter delivery methods.

Your new AWS report task will appear in the Tasks library for this site.



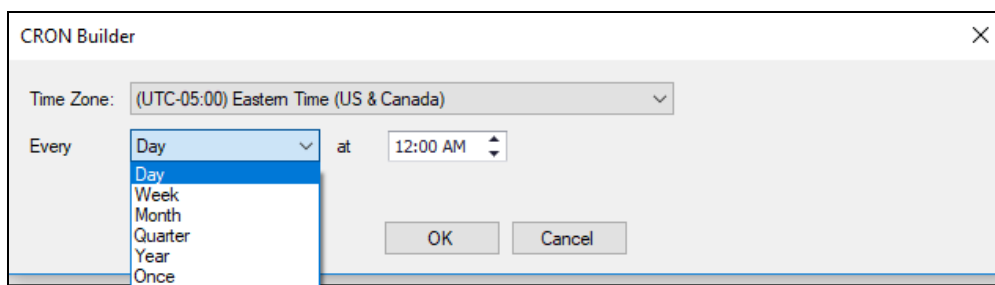
Step 3 — Schedule Scan and Report Tasks

Once you create both the scan and report task, it's time to schedule the tasks.

1. First, schedule the Scan Task. Next to the AWS scan task, click **Schedule**.

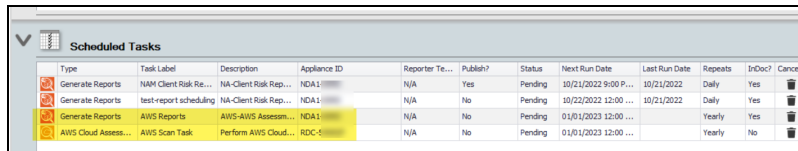
Action	Schedule	Delete
Run Now	Schedule	
Run Now	Schedule	
Run Now	Schedule	

2. Assign an interval to the scan task then click **OK**.



Important: Be sure to schedule the AWS scan task to begin several hours **BEFORE** your report task. This will ensure your reports contain the latest data from the complete scan.

- The AWS scan task will then appear in the queue of scheduled scan tasks. Alternatively, you can click **Run Now** from the scan task library to begin the scan immediately.



Type	Task Label	Description	Appliance ID	Reporter Te...	Publsh?	Status	Next Run Date	Last Run Date	Repeats	InDoc?	Cancel
Generate Reports	NAM Client Risk Re...	NA-Client Risk Rep...	NDA1	N/A	Yes	Pending	10/21/2022 9:00 P...	10/21/2022	Daily	Yes	
Generate Reports	test-report scheduling	NA-Client Risk Rep...	NDA1	N/A	No	Pending	10/22/2022 12:00 ...	10/21/2022	Daily	Yes	
Generate Reports	AWS Reports	AWS-AWS Assesse...	NDA1	N/A	No	Pending	01/01/2023 12:00 ...		Yearly	Yes	
AWS Cloud Assess...	AWS Scan Task	Perform AWS Cloud...	RDC-5	N/A	No	Pending	01/01/2023 12:00 ...		Yearly	No	

- Finally, schedule the AWS Assessment report task. To the right of the report task, click **Schedule**. Assign an interval to the report task then click **OK**.

Important: Be sure to schedule the AWS report task to begin a few hours **AFTER** the scan task. This will ensure your reports contain the latest data from the complete scan.

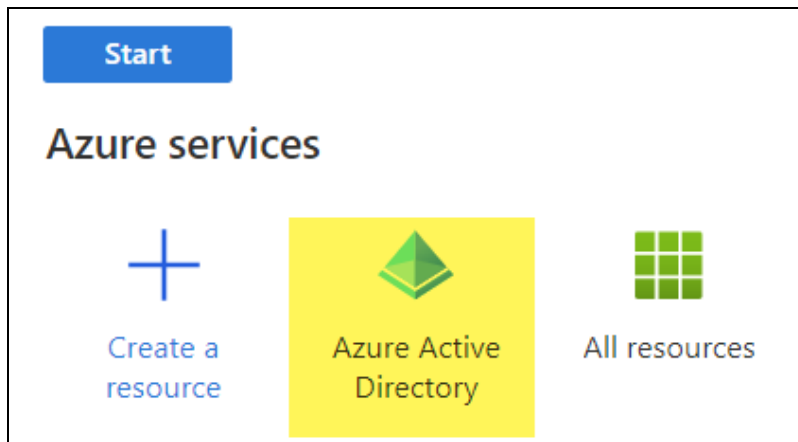
Authenticate Exchange Scan using Enterprise App

This topic covers how to authenticate your Exchange Scan using an Enterprise Application that you will create in the target Azure environment. This method requires that you complete these steps:

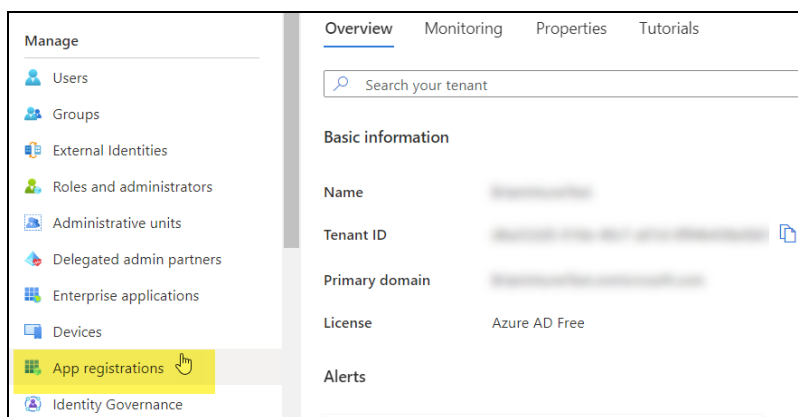
Step 1 — Register app in Azure Active Directory

In this step, you will create a new app in the target Azure environment and assign it the appropriate API permissions.

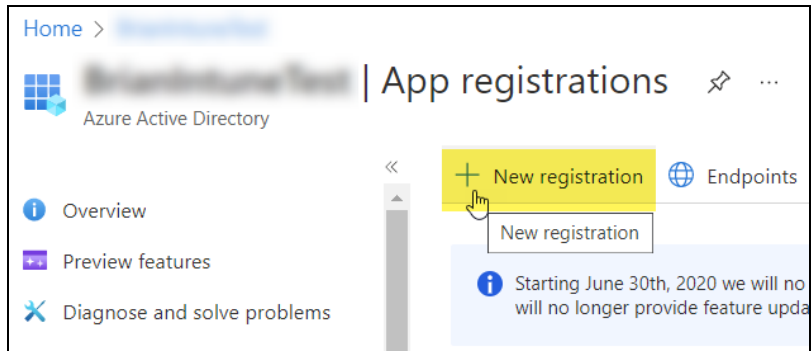
1. Access the Azure Portal at portal.azure.com and log in. Then navigate to **Azure Active Directory**.



2. From the left menu, click **App registrations**.

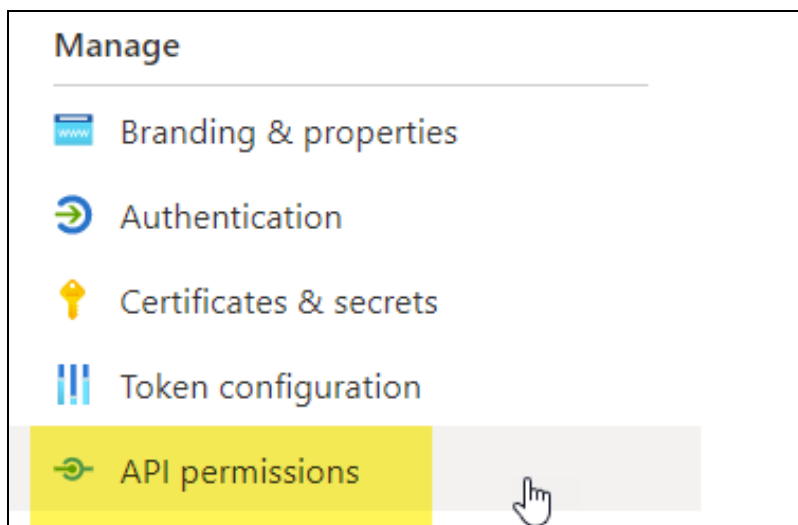


3. Then click **New registration**.

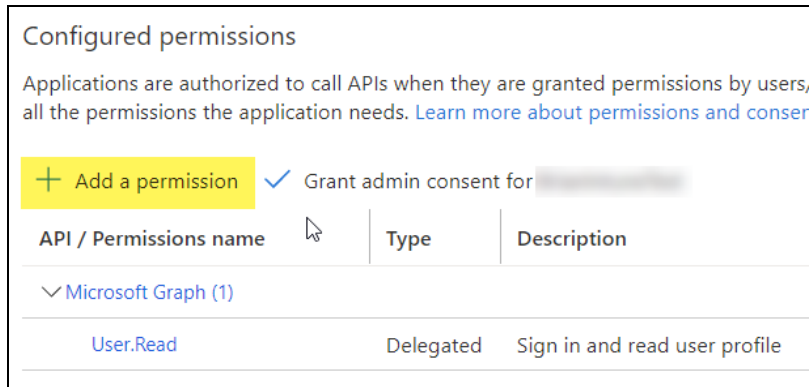


4. Enter a **name** for the app. Ignore the other settings and click **Register**.

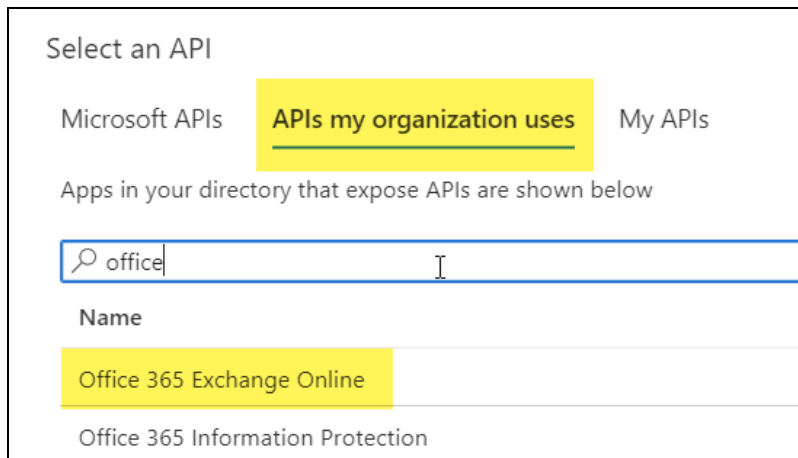
5. From your new app, click **API permissions**.



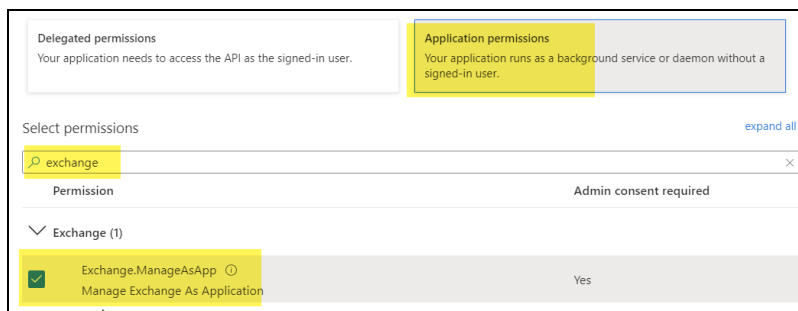
6. Click **Add a permission**.



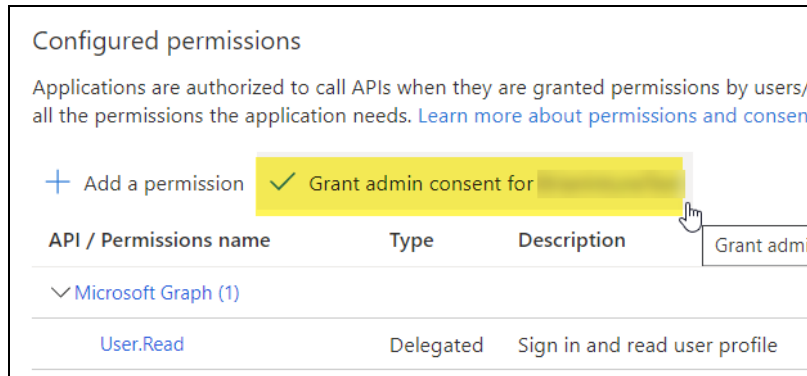
7. Select **APIs my organization uses**, and then search for and select **Office 365 Exchange Online**.



8. Next, choose **Application permissions**.
9. Search for **Exchange**, and then select **Exchange.ManageAsApp**. Then click **Add permissions**.

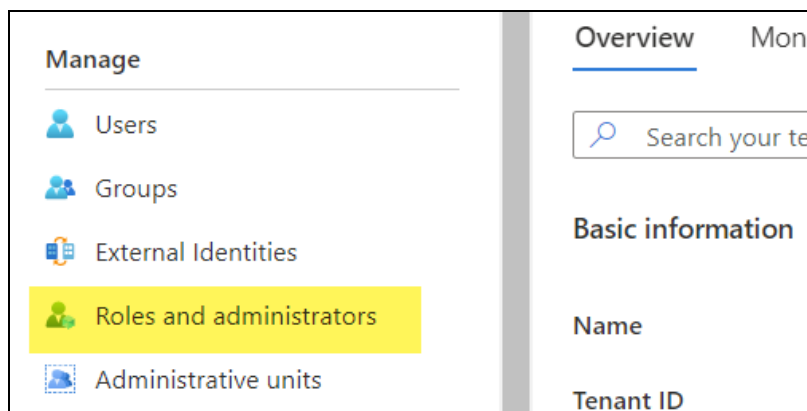


10. Next, from Configured permissions, click **Grant admin consent for [organization]**.

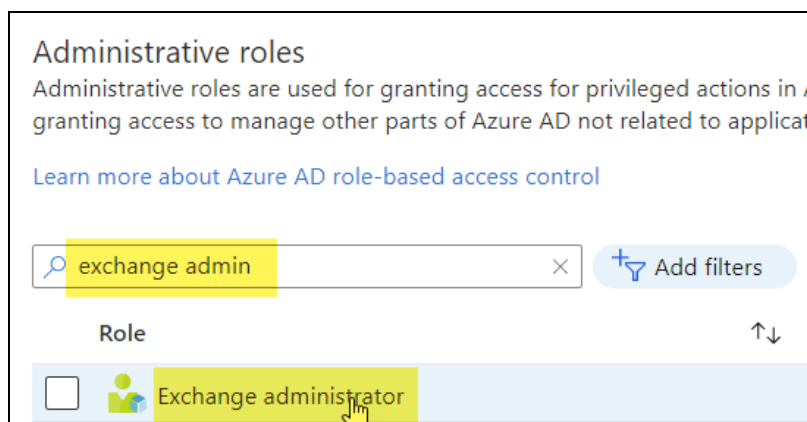


Step 2 — Assign Exchange Administrator role to app

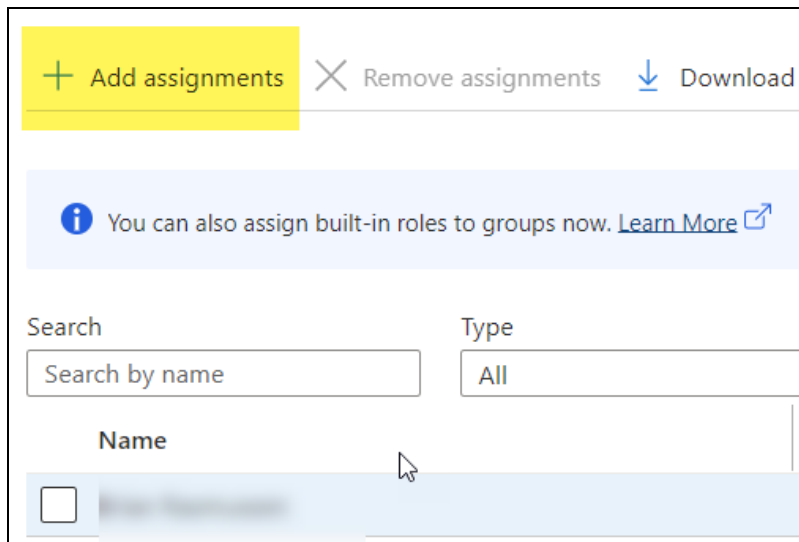
1. Return to the Azure Active Directory **Overview** (also called "Home") page.
2. From the left menu, click **Roles and administrators**.



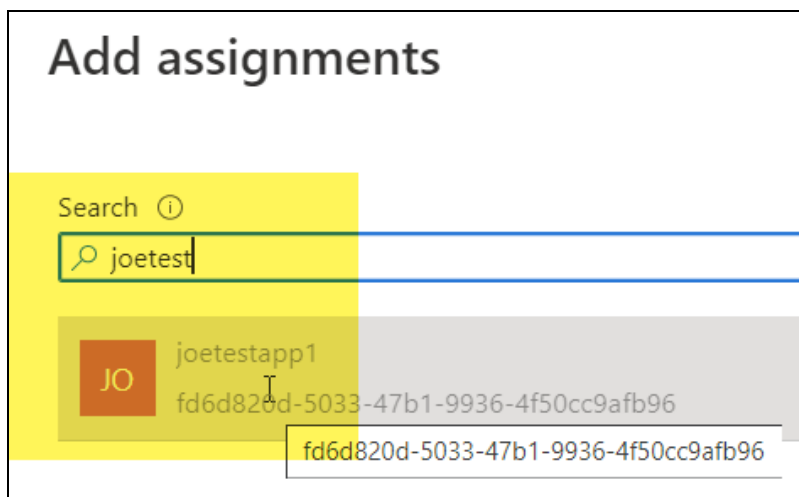
3. Search for **Exchange administrator** from the list of roles, and then **click on it** (do not click on the check box).



4. Click **Add assignments**.



5. Search for and **select the app you created** in Step 1.
6. Then click **Add**. You will have then assigned the Exchange admin role to the app.



Step 3 — Install Required Exchange Online Management PowerShell Module

This step is performed on the local machine on the target network that will host the Remote Data Collector (RDC). This must be the same endpoint where you will generate a certificate in ["Step 4 — Generate self-signed certificate and attach to app" on the next page](#).

On this endpoint, **install the Exchange Online Management module**. **YOU MUST RUN POWERSHELL AS AN ADMINISTRATOR** when you run these commands:

1. `Install-Module -Name MSOnline -Scope AllUsers`
2. `Install-Module -Name ExchangeOnlineManagement -Scope AllUsers`
3. `Install-Module -Name PowerShellGet -Scope AllUsers -Force`

Step 4 — Generate self-signed certificate and attach to app

Before you can begin your Exchange scan, you must generate a self-signed certificate on the local machine from which the scan will be performed. You will then attach this certificate to the enterprise app you created in Step 1.

Note: If you are using the Remote Data Collector (RDC) to perform the Exchange scan, generate the certificate from the endpoint that hosts the RDC.

To generate the self-signed certificate, **RUN WINDOWS POWERSHELL AS AN ADMINISTRATOR**. Then run the 3 commands below:

a) Name the certificate

Replace "{certificateName}" with a name for the certificate

```
$certname = "{certificateName}" ## Replace {certificateName}
```

b) Generate the certificate

```
$cert = New-SelfSignedCertificate -Subject "CN=$certname" -  
CertStoreLocation "Cert:\LocalMachine\My" -KeyExportPolicy  
Exportable -KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -  
HashAlgorithm SHA256
```

c) Export the certificate

Set the location to export the certificate by changing parameter after -FilePath

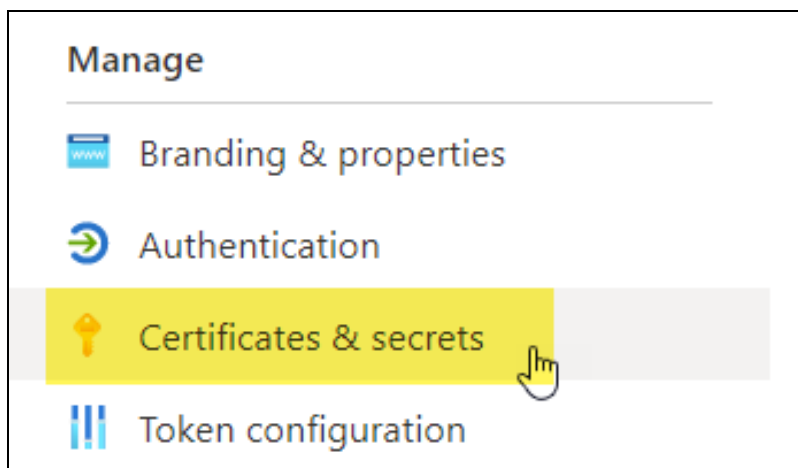
```
Export-Certificate -Cert $cert -FilePath  
"C:\Users\admin\Desktop\${certname}.cer" ## Specify your preferred location
```

Important: When you generate a certificate on a local machine, that certificate's Thumbprint can only be used for collection from that exact machine. Generate and

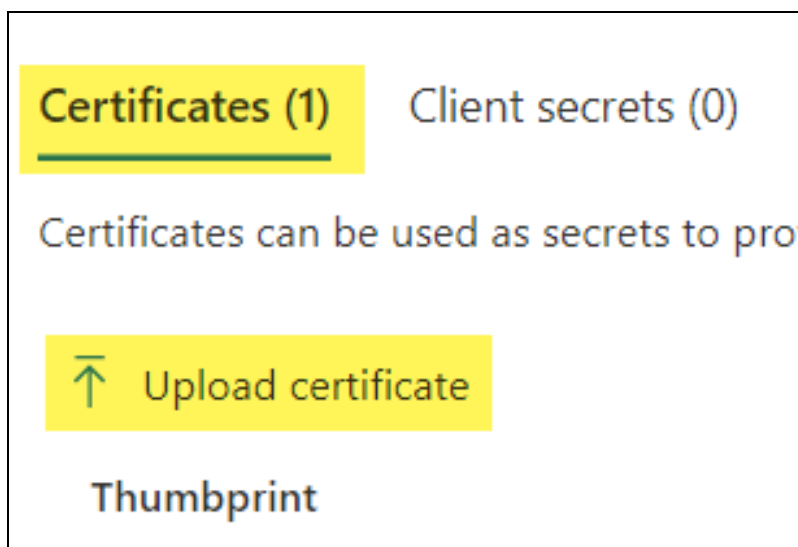
upload a new certificate for each additional endpoint where you want to perform the scan, as in "[Step 5 — Add certificate to Enterprise App](#)" below.

Step 5 — Add certificate to Enterprise App

1. Return to the Azure Portal at portal.azure.com and open **Azure Active Directory**.
2. Click **App registrations**.
3. Find and click on the app you created in Step 1.
4. Click **Certificates & secrets** from the left menu.



5. Open **Certificates**. Then click **Upload certificate**.



6. Select the certificate and click **Add**.

Upload certificate

×

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt *

Select a file

Description

Enter a description for this certificate

7. Copy the certificate **Thumbprint** for later use.

Certificates (1)

Client secrets (0)

Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when

↑ Upload certificate

Thumbprint	Description
86193	

Note: The column can be expanded by dragging the column separator between **Thumbprint** and **Description**.

Step 6 — Collect credentials to perform Exchange scan

To perform the scan, you need three credentials: **Organization**, **App ID**, and **Thumbprint**. The table below contains the location of each credential in the Azure portal. Once you have these credentials, you can proceed to ["Exchange Server Assessment Scan" on page 106](#).

Credential	Location
Organization	From the Azure Portal, navigate to Azure Active Directory . Under Basic information , take the value next to Primary domain .
Application ID	Navigate to Azure Active Directory > App Registrations > [YourApp] . Under the Essentials field, copy the value next to Application (client) ID .

Credential	Location
Thumbprint	Navigate to Azure Active Directory > App Registration > [YourApp] > Certificates & secrets. Find the corresponding Certificate and copy the complete Thumbprint.

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 17](#).
- Other prerequisites specific to your chosen PSA system (refer to the table below).

PSA System	PSA Prerequisites
	• Autotask Username • Autotask Password
	• 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

PSA System	PSA Prerequisites
	page 228
	• 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 237
	• Tigerpaw Username • Tigerpaw Password • Tigerpaw API URL
	• Kaseya Username • Kaseya Password Note: The Kaseya User must be in the Kaseya Administrator Role. See also "Set Up Kaseya BMS Integration" on page 239. • 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)

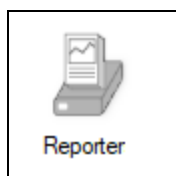
PSA System	PSA Prerequisites
	• Works with Export Configurations ONLY • IT Glue API URL Note: For the API URL, use https://api.itglue.com. If your IT Glue account is in the EU Data Center, use https://api.eu.itglue.com. • IT Glue API Key Note: You will generate the API Key in the IT Glue application.

Step 2 — Create Export Task with Reporter

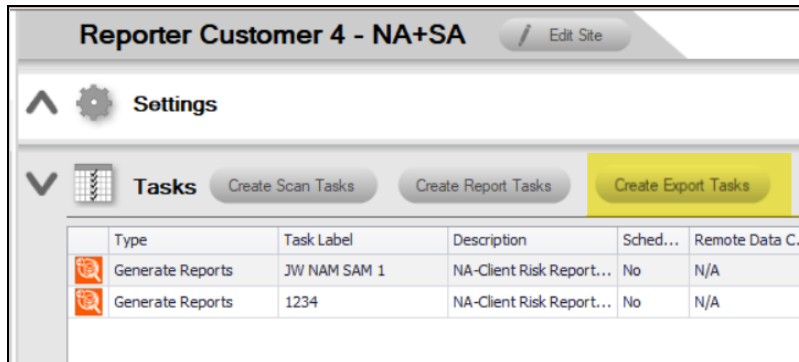
1. **Start Network Detective** and log in with your credentials.
2. Open the Reporter **Site** for which you wish to create tickets in the target PSA.

Note: You must have scan data and must have generated reports in order to create tickets.

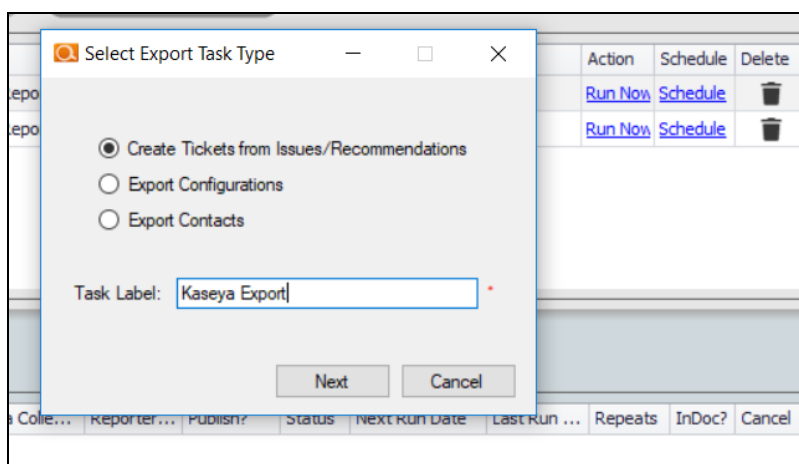
3. Click the **Reporter** icon in the bottom left of the screen to open the Reporter dashboard.



4. From the Reporter dashboard, click **Create Export Tasks**.



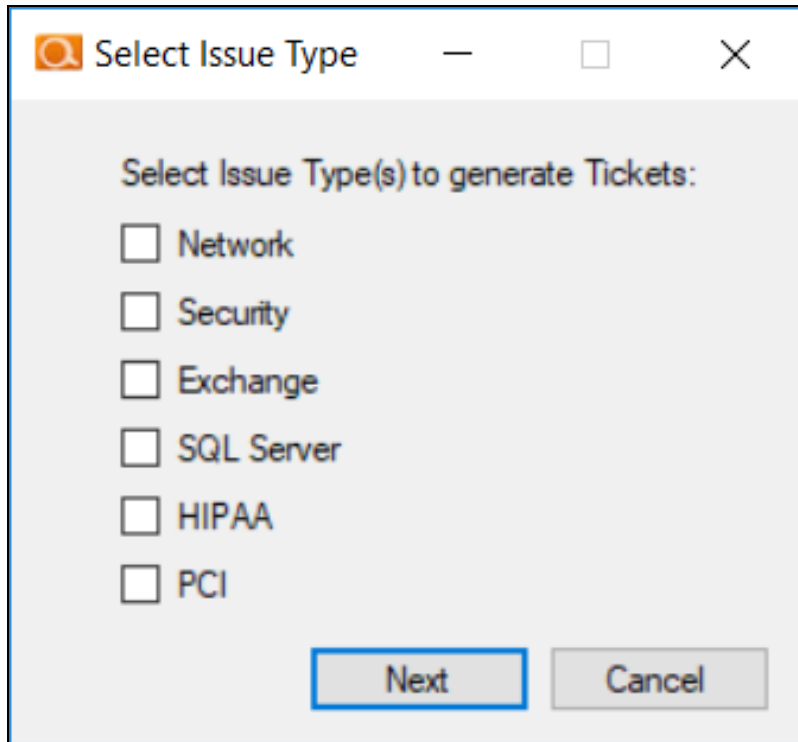
5. Choose an **Export Task Type** from the drop-down menu.



Note:

- Create Tickets** – Automatically create tickets in your company's PSA/Ticketing System.
- Export Configurations** – Export Configurations (hardware information, etc.) into Autotask, Kaseya BMS, ConnectWise, Tiger Paw, or ITGlue.
- 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.



7. **Select your Target** Ticketing/PSA system from the list of supported options.



8. The Export Issues window will appear. Click **Manage Connections**.

Export Issues and Recommendations To Kaseya

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

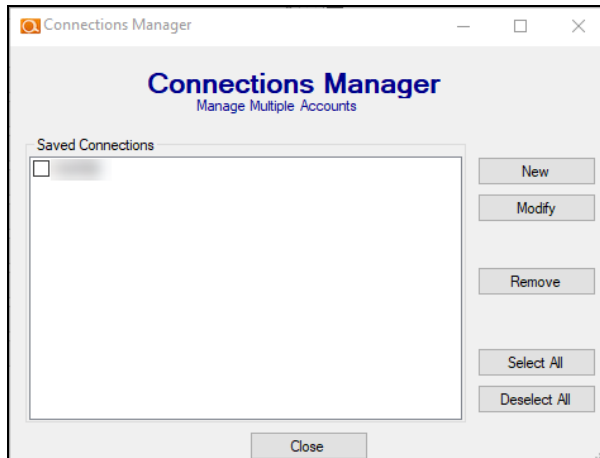
Queue: Level Four Support

Primary Assignee: Mark Winter

☒ Create Multiple Tickets (one ticket per issue)

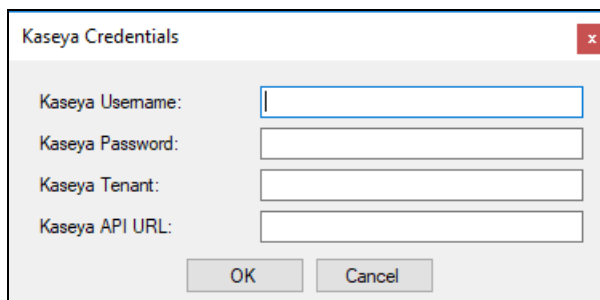
Update Close

The Connections Manager window will be displayed.



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
mwinter
RFTTest1
mwutest

Export to Account:

Account Location:

Contact:

Ticket Source:

Ticket Type:

Priority:

Status:

Queue:

Primary Assignee:

☒ Create Multiple Tickets (one ticket per issue)

Update Close

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.

Export Issues and Recommendations To Kaseya

Automatically creates Tickets in Kaseya based on issues and recommendations in a Risk Report

Mappings

Kaseya Connection: RFTTest1 [Manage Connections](#)

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)

Update Close

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.

Tasks					
		Create Scan Tasks	Create Report Tasks	Create Export Tasks (BETA)	
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.

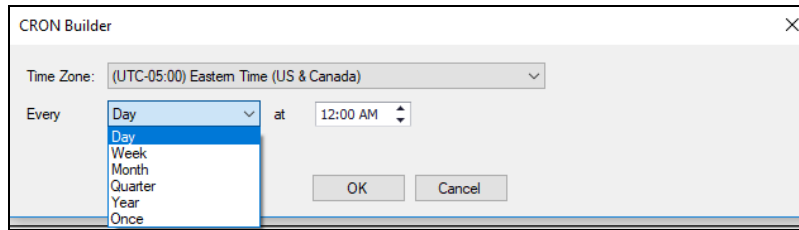
Step 3 — Schedule/Run Export Task

- 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).

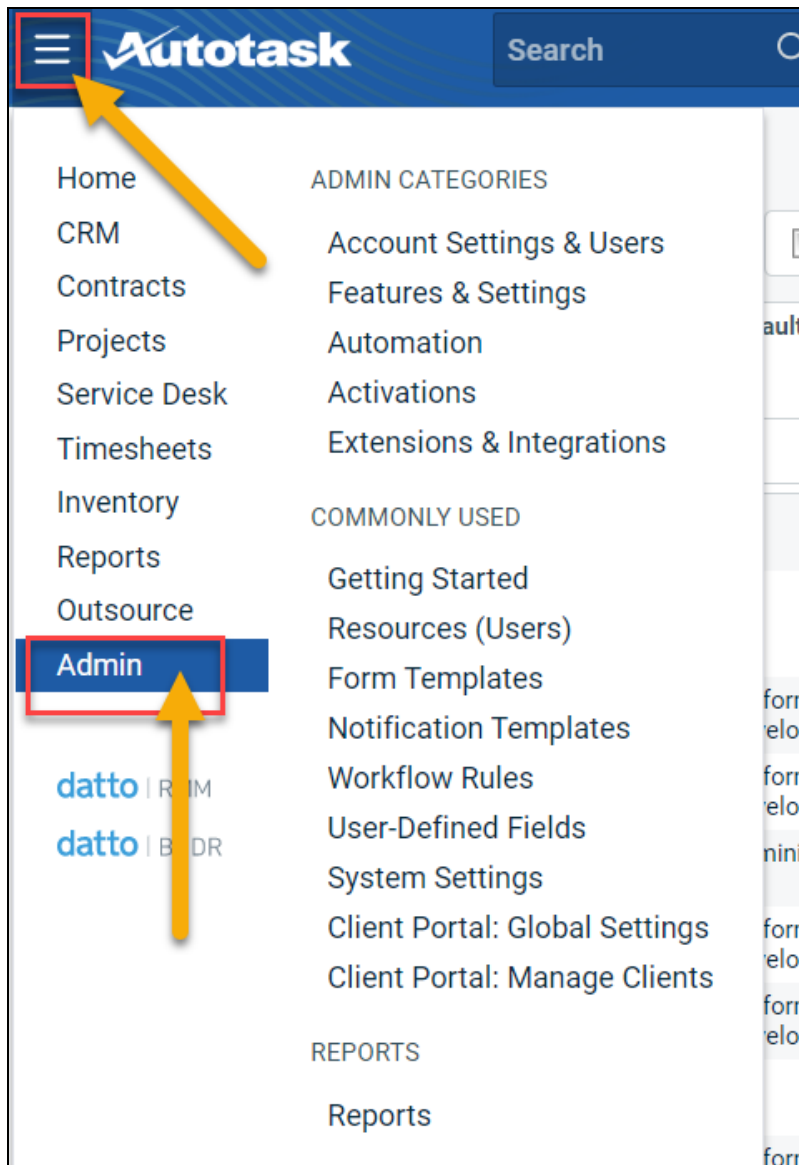


2. Set the export frequency by selecting one option from **Every** list (i.e. day, week, month, year, or once)
3. Next set the “**on the**” by selecting a day that the export should be performed.
4. Then set the time of the day that the export should run by setting the “**at**” time.
5. Click **OK** to save the Export task. It will run at the specified time and export items into your chosen PSA system.

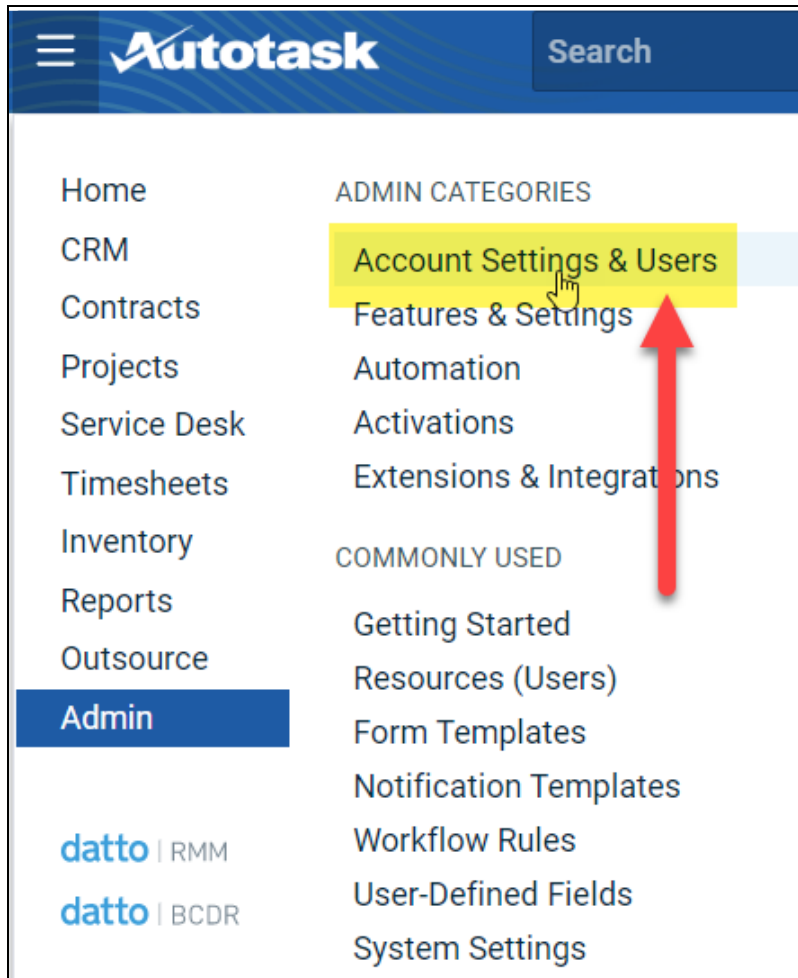
Set Up Autotask Integration

To set up a connection with the Autotask system, you will need to **create an API User in Autotask**. To do this:

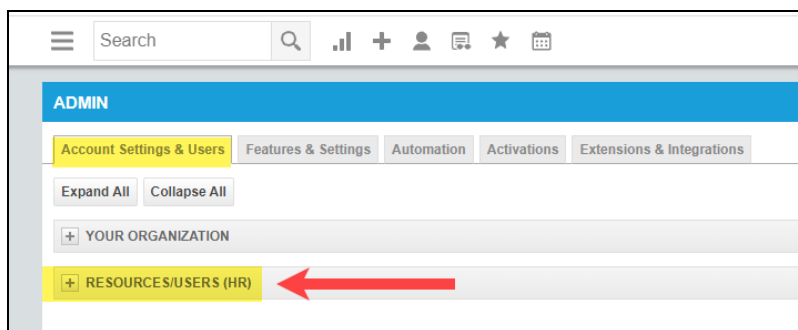
1. Log in to Autotask with your admin user credentials.
2. Click on the **Autotask home** button on the left, then click **Admin**.



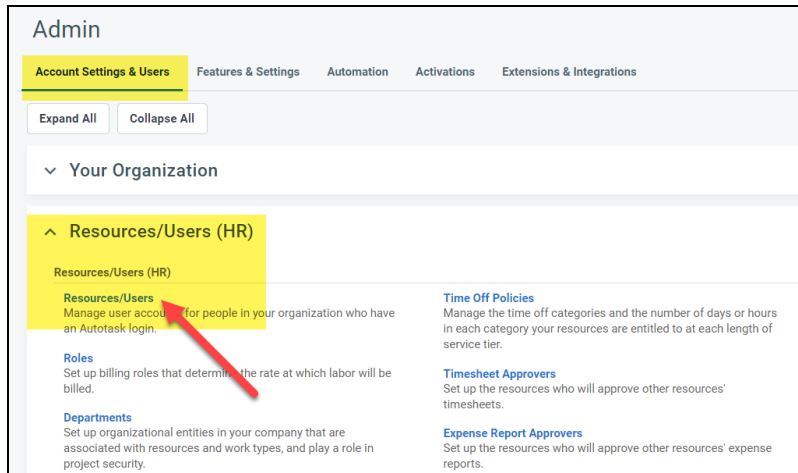
3. From the **Admin** menu, click **Account Settings & Users**.



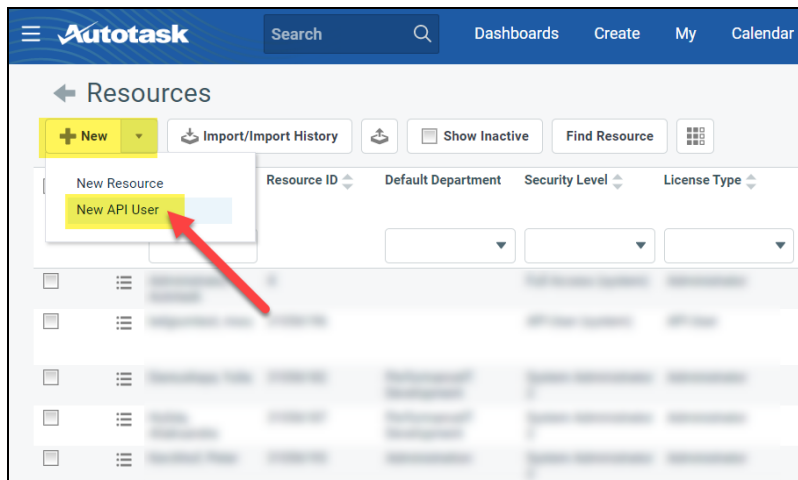
4. Next, click **Resources/Users (HR)** to expand the menu.



5. Then click **Resources/Users**.



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



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

Add API User

[Review Terms and Conditions for API Use](#)

General

First Name *

Last Name *

Email Address *

☒ Active
☐ Locked

Security Level *

Date Format
MM/dd/yyyy

Time Format
hh:mm a

Number Format
X,XXX.XX

Primary Internal Location *

Credentials

[Generate Key](#) [Generate Secret](#)

Username (Key) *

Password (Secret) *

API Tracking Identifier

API version 1.6 & later require the user of an API tracking identifier. Once assigned, this cannot be changed.

☒ Integration Vendor
☐ Custom (Internal Integration)

Integration Vendor *

RapidFire Tools - Network Detective

Line of Business

A line of business can be used to grant access or prevent access to data associated with Contracts, Tickets, Projects, etc.

Not Associated

Associated

☒ Resource can view items with no assigned Line of Business

- Enter a **first and last name** for the API user.
- Enter an **email address** for the API user.
- From **Security Level**, select **API User (system)**.
- Select a **Primary Internal Location** for the API user.
- Enter/generate a **username** for the API user, then enter/generate a **password**.

Note: Take note of these credentials as you will enter these in Network Detective to enable the API integration.

- Under **API Tracking Identifier**, select **Integration Vendor**. Then select **RapidFire Tools — Network Detective**.

The screenshot shows the 'Add API User' form. At the top, there are buttons for 'Save & Close' and 'Cancel', and a link to 'Review Terms and Conditions for API Use'. Below this is the 'Credentials' section with 'Generate Key' and 'Generate Secret' buttons, and input fields for 'Username (Key) *' and 'Password (Secret) *'. The 'API Tracking Identifier' section follows, with a note that API version 1.6 and later require an identifier. Two radio buttons are present: 'Integration Vendor' (selected) and 'Custom (Internal Integration)'. Below the radio buttons is a dropdown menu for 'Integration Vendor *' with 'rapidfire' entered. The dropdown list is open, showing various vendors. 'RapidFire Tools - Network Detective' is highlighted in yellow. Other vendors in the list include Perspectium - Middleware (ServiceNow), PropelyYourMSP, Pulseway - RMM, Quickpass - Password Management, Quoter Software Inc. - Quoter, QuoteWerks - Quotes, Proposals, and Procurement, RapidFire Tools - Email2Ticket, Recursyv - Seamless, Red Cactus - Bubble CRM Integrations, Relokia - Data Migration, and Resale Partners - Telephony. To the right of the dropdown, there is a text area with the placeholder 'associated with Contracts, Tickets, Projects, etc.' and a label 'Associated'.

8. When you are finished configuring the new API user, click **Save & Close**. The new user will appear in the list.

Set Up ConnectWise REST Integration

To set up a connection to ConnectWise Ticketing system using the REST API you will be required to:

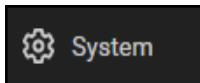
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

To enable the integration, you will need to use the ConnectWise Manage Internet Client application. Download and install the app from <http://university.connectwise.com/install/>. Then log in using your credentials.

If you are using the ConnectWise Manage web app, you can continue to use the web app after you have completed the steps in this guide and enabled the integration.

Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with

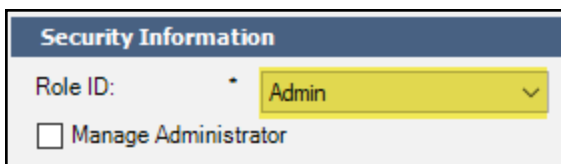
1. From the ConnectWise dashboard, click **System** from the side menu.



2. Next, click **Members**.
3. Click on **API Members Tab**. The API Members screen will appear.

Note that the API Members Tab may not show by default and may need to be added. You can add this tab from the Tab Configuration menu on the Members page .

4. Click on the  button to create a new API Member. Fill in all required information.
5. Confirm that the API Member has been assigned Admin rights by checking the member's Role ID under Security Information.

A screenshot of a form titled "Security Information" with a blue header. Below the header, there is a label "Role ID:" followed by a yellow dropdown menu showing "Admin" with a downward arrow. Below that is a checkbox labeled "Manage Administrator".

Security Information	
Role ID:	Admin
☐	Manage Administrator

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				

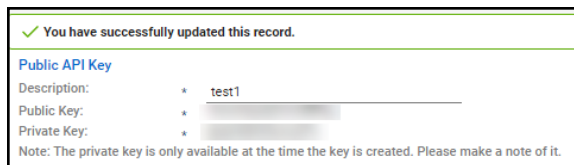
Step 3 — Create an API Key in the ConnectWise Ticketing System

1. Select the API Member that you created previously.
2. From the API Member details screen, click **API Keys**.



3. Click the  button.
4. Enter a **Description** for the API Key.
5. Click **Save**. 
6. The newly generated API Key will appear.
7. Write down or take a screen shot of the Member's Public and Private API Key strings. This information will be required to set up the integration with ConnectWise.

Important: Note that the Private Key is only available at the time the key is created. Be sure to copy the keys for your records.



Step 4 — Configure Service Tables in ConnectWise

In order to export issues as tickets in ConnectWise, you will need to configure several **Service Tables** in ConnectWise. These tables ensure that the issues are “mapped” correctly to the tickets created within ConnectWise. You must configure the Service Tables correctly in order to establish the connection with ConnectWise.

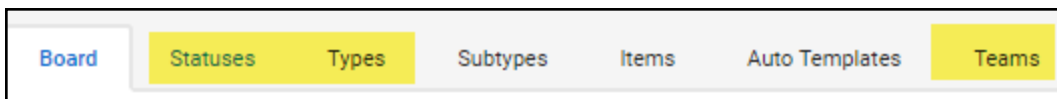
You can configure the Service Tables in ConnectWise from **System > Setup Tables > Category > Service**. Configure the Service Tables as detailed below:

1. **Service Board**

You must have a Service Board created within ConnectWise. In addition, within the Service Board, you must create values for the following fields. You can create values for these fields from the Service Board page:

- a. **Statuses**
- b. **Types**
- c. **Teams**

You must create at least one value for each of these fields.



In addition, you must define values for two additional Service Tables:

2. Source

You must include at least one Source.

3. Priority

You must include at least one Priority level.

Service	▼	
Service	ConnectWise Manage Network	ConnectWise Manage Network settings.
Service	Email Connector	Folder setup for the Email Connector program
Service	Email Formats	Service Email Template setup
Service	IMAP Setup	Define IMAP configurations for Email Connector
Service	Knowledge Base	Create categories, subcategories, and change settings
Service	Priority	Priority is associated with SLAs (previously captioned Urgency)
Service	Service Board	Service Board Setup
Service	Service Sign Off	Service Sign Off Setup
Service	Severity	Service Severity and Impact
Service	SLA	Service Level Agreement setup
Service	Source	Example: Email, Phone
Service	Standard Note	Standard Note Setup
Service	Surveys - Service	Create and edit automated surveys for service tickets
Service	Ticket Template	Defines ticket templates that can be applied to tickets directly, or used to g...

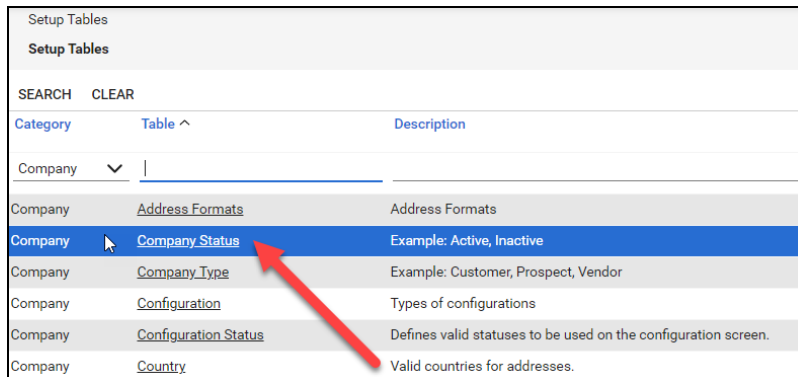
If your existing Service Tables already contain values for the fields listed above, you do not need to create new values.

Step 5 — Remove "Disallow Saving" Flag from Company

The final step is to ensure your companies are able to save data such as tickets. By default, your company may have the **"Disallow Saving"** option flag enabled; this will prevent you from exporting tickets to the company.

Here's how to remove the "Disallow Saving" flag:

1. Navigate to **Setup Tables > Category > Company > Company Status**.



The screenshot shows the 'Setup Tables' interface. At the top, there are 'SEARCH' and 'CLEAR' buttons. Below them is a table with columns 'Category', 'Table ^', and 'Description'. The 'Category' column has a dropdown menu currently showing 'Company'. The table lists several setup tables. The 'Company Status' table is highlighted in blue, and a red arrow points to it. The other tables listed are 'Address Formats', 'Company Type', 'Configuration', 'Configuration Status', and 'Country'.

Category	Table ^	Description
Company	Address Formats	Address Formats
Company	Company Status	Example: Active, Inactive
Company	Company Type	Example: Customer, Prospect, Vendor
Company	Configuration	Types of configurations
Company	Configuration Status	Defines valid statuses to be used on the configuration screen.
Company	Country	Valid countries for addresses.

2. From Company Status, open the **not Approved** field.

Setup Tables > Company Status List

Company Status List

< + SEARCH CLEAR

Description	Default	Inactive	Notify	Custom Note
Active				
Inactive			✓	
Imported			✓	
Credit Hold			✓	
Problem			✓	
not-Approved	✓		✓	
Solid				
Attention needed			✓	
may Leave			✓	
Delinquent			✓	

3. Uncheck the **Disallow Saving** flag.

Setup Tables > Company Status List > Company Status

Company Status

     HISTORY 

Company Status

Description*
not-Approved

☒ Default

☐ Inactive

Notification Parameters for Service, Project and Time

☒ Notify

☒ Disallow Saving

Notification Message

Do not Service
they have not been setup for Service yet
check with their account manager

Company Status

Description*
not-Approved

☒ Default

☐ Inactive

Notification Parameters for Service, Project and Time

☒ Notify

☐ Disallow Saving

Notification Message

Do not Service
they have not been setup for Service yet
check with their account manager

4. This will allow you to export tickets to companies with the **not Approved** status. Alternatively, you can set the company itself to a different status that allows saving before attempting the ticket export.

Company Search > Company > Company Finance Detail

Micro Pro

< Summary

Recap

Invoices 0

Time 0

Expenses 0

<

<

History <

Links <

Company: Micro Pro

Company: * Micro Pro

Phone:

Company ID: * 123

Fax:

Status: * not-Approved

<

Web Site:

Type: *

Prospect X

Finance Details

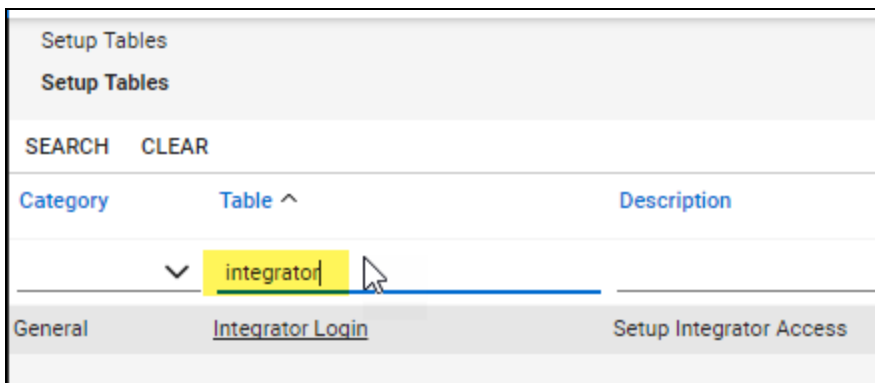
Set Up ConnectWise SOAP Integration

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.



The screenshot shows the 'Setup Tables' interface. At the top, there's a 'Setup Tables' header. Below it, a search bar with 'SEARCH' and 'CLEAR' buttons. A table with columns 'Category', 'Table ^', and 'Description' is displayed. The 'Table ^' column has a dropdown menu with 'Integrator' selected. Below the table, there's a 'General' tab and a link 'Integrator Login' which is highlighted. To the right of the link is '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

- MemberApi
- ReportingApi
- SystemApi
- ConfigurationApi

Integrator Login

Setup Logs

< + [List Icon] [Refresh Icon] HISTORY ▾ [Trash Icon]

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		☐ Use legacy
		Company		☐ Use legacy

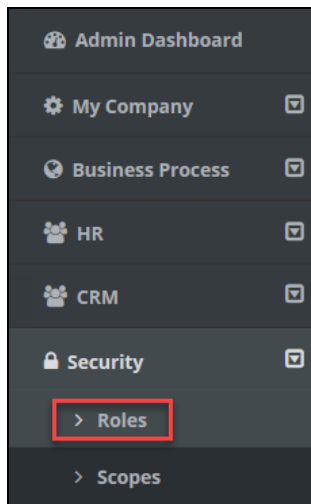
8. Click the **Save** icon to save this Integrator Login.

Note: If you already have an Integrator Login configured, you may use it as long as the Company and Configuration APIs are enabled.)

Set Up Kaseya BMS Integration

To export items to Kaseya BMS, you will need Administrator credentials in Kaseya BMS. To assign a Kaseya user to the Administrator role, follow these steps:

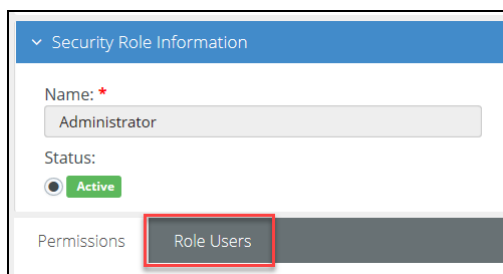
1. Log in to Kaseya BMS.
2. Go to **Security > Roles**.



3. Click **Open/Edit** on the Administrator Role.

	CRM Manager	CRM Manager
	Project Manager	Project Manager
	Service Desk Manager	Service Desk Manager
	Administrator	Administrator

4. Click the **Role Users** tab.

A screenshot of the 'Security Role Information' form. The form has a blue header with a dropdown arrow and the text 'Security Role Information'. Below the header, there is a 'Name:' field with a red asterisk, containing the text 'Administrator'. Below that is a 'Status:' section with a radio button selected for 'Active'. At the bottom, there are two tabs: 'Permissions' and 'Role Users'. The 'Role Users' tab is highlighted with a red rectangular box.

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.

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 ["Matching Criteria for Configurations and Contacts" on page 254](#) 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 17](#))
- 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 22](#) and ["Configure Remote Data Collector to Perform Scan Tasks" on page 31](#))

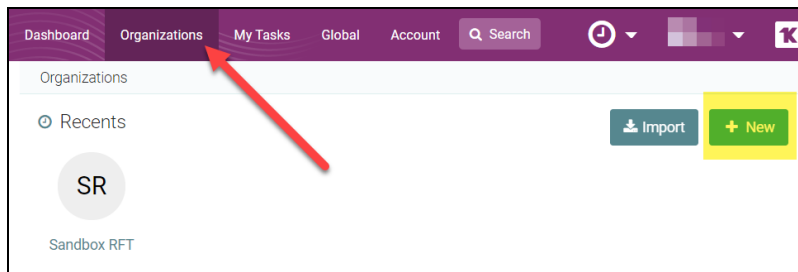
Note: See ["Setting Up Reporter" on page 17](#) for detailed instructions on installing and configuring Reporter.

Important: Currently, you can only export configuration items for Active Directory environments, and NOT Workgroups.

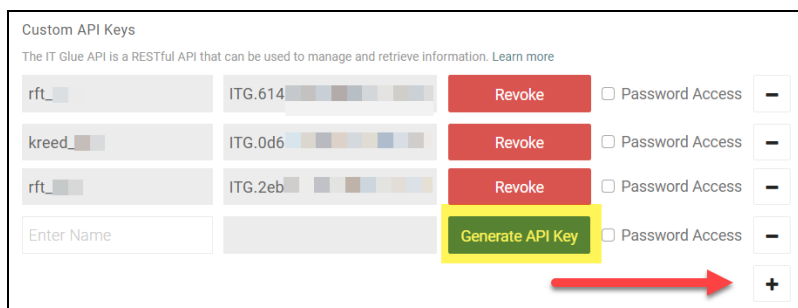
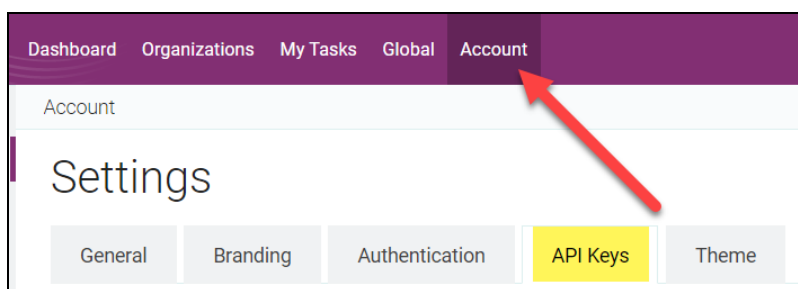
Once these prerequisites are met, you can then:

Step 1 — Create Organization and API Key in IT Glue

1. Create one or more **Organizations** in IT Glue. You will later select one of these orgs to send your data to the right place. You create new Organizations from the

Organizations tab in IT Glue.

2. Create an IT Glue API Key for your use during integration and set up. You can do this from **Account > API Keys**.



Important: For your reference, save a copy of the API key outside of IT Glue.

You can then use the instructions below to create a **Reporter Export Task** to IT Glue in the **Network Detective** application.

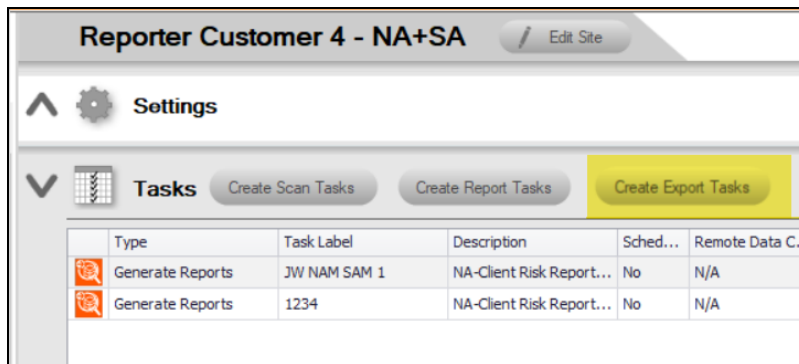
Step 2 — Create a Reporter Export Task to IT Glue

To set up a connection between the Network Detective application and IT Glue, you will:

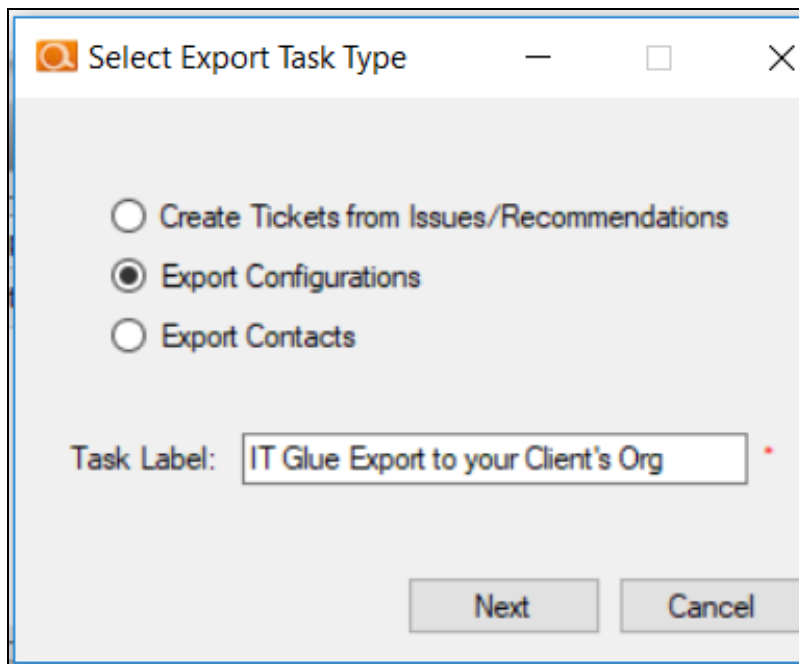
1. In the **Network Detective** app, open the **Site** used to manage the Reporter. Click on the **Reporter icon** on the bottom left side of the Site screen.



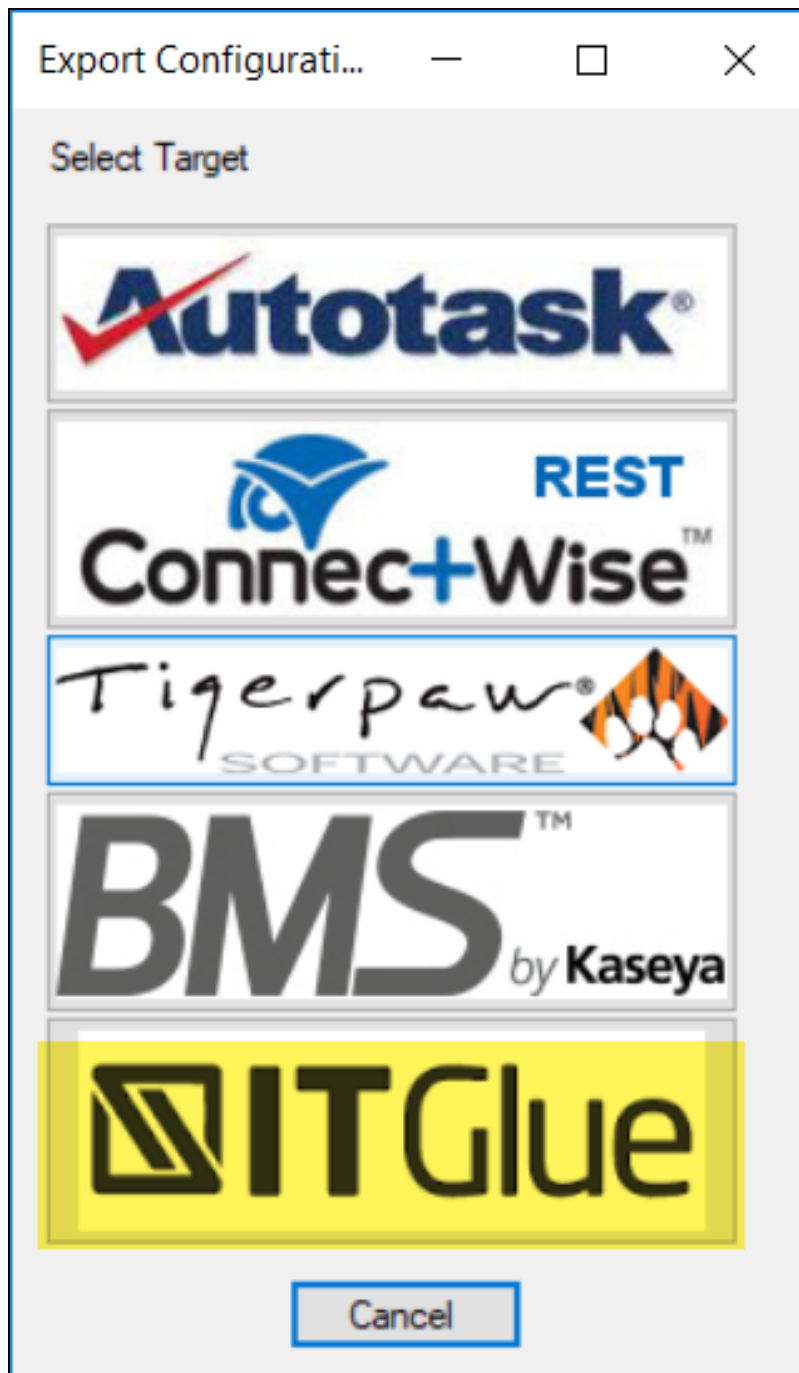
2. Click **Create Export Tasks**.



3. The Select Export Task Type window is displayed. Select the **Export Configuration** option and assign a **Task Label**.

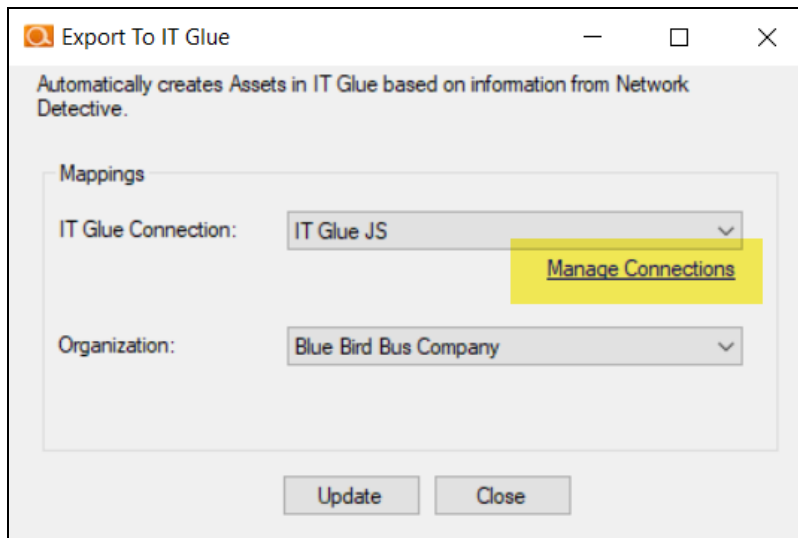


4. Click **Next**. Select **IT Glue** from the available integrations.

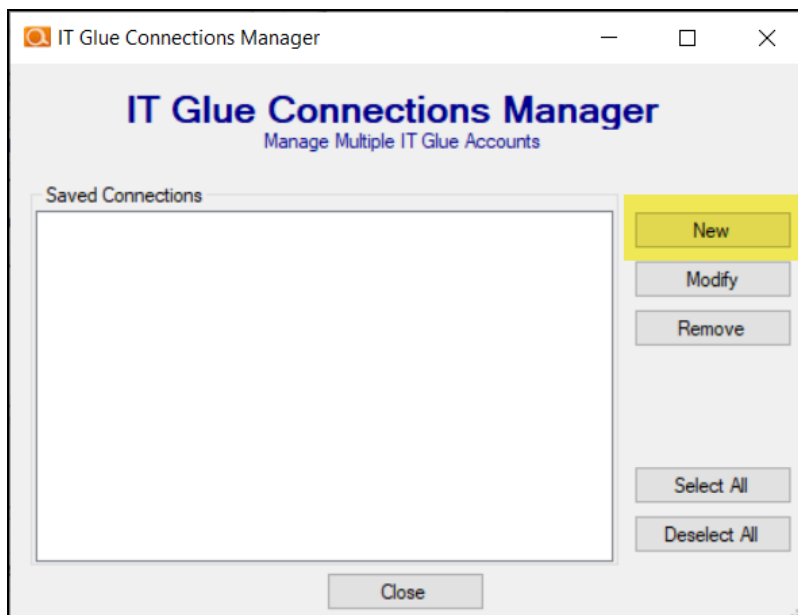


Step 3 — Create Connection to IT Glue and Configure Asset Mapping

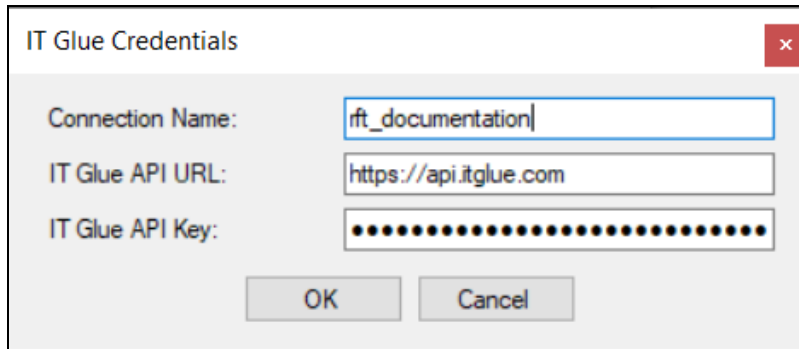
1. Click **Manage Connections**.



2. Click **New** from the IT Glue Connections Manager.



3. Enter a **Connection Name**. Then enter your **IT Glue API** credentials. Click **OK**.



IT Glue Credentials

Connection Name: rft_documentation

IT Glue API URL: https://api.itglue.com

IT Glue API Key:

OK Cancel

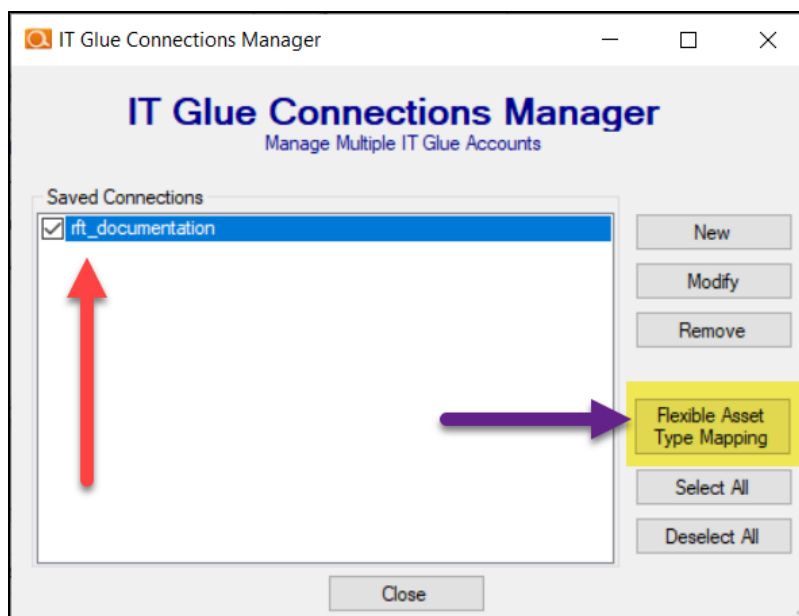
Note:

- For the API URL, use **https://api.itglue.com**
- If your IT Glue account is in the EU Data Center, use **https://api.eu.itglue.com**
- If your IT Glue account is in the AU Data Center, use **https://api.au.itglue.com**

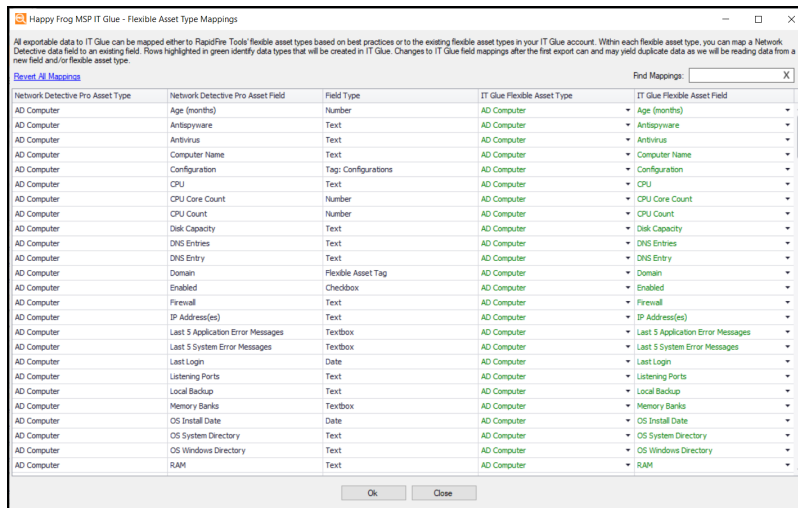
Important: The IT Glue API Key must be generated from within the ITGlue system. See ["Step 1 — Create Organization and API Key in IT Glue" on page 241](#)

The Connection will appear in the list of Saved Connections.

4. **OPTIONAL:** If you want greater control of how Network Detective data is exported to IT Glue, select your connection and click **Flexible Asset Type Mapping**.



The Flexible Asset Type Mappings wizard will load for your chosen connection.

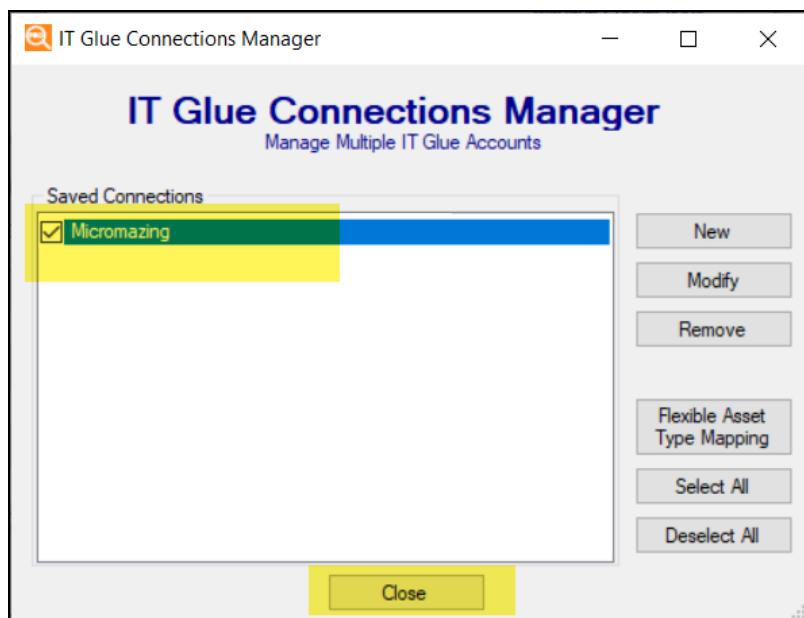


Note: Data that you export to IT Glue can be mapped to Network Detective's flexible asset types or to existing asset types in your IT Glue account. For each flexible asset type, you can choose to map a Network Detective data field to an existing IT Glue data field. Rows highlighted in green identify new data types that will be created in IT Glue. After the first export, changes to IT Glue field mappings may yield duplicate data. New fields and/or new asset types will be read as new data.

Review the available asset mappings. By default, the export will populate IT Glue with Network Detective's own asset types. However, you can choose to map each Network Detective asset to an existing asset in IT Glue. This is useful if you want to preserve your custom asset types in IT Glue.

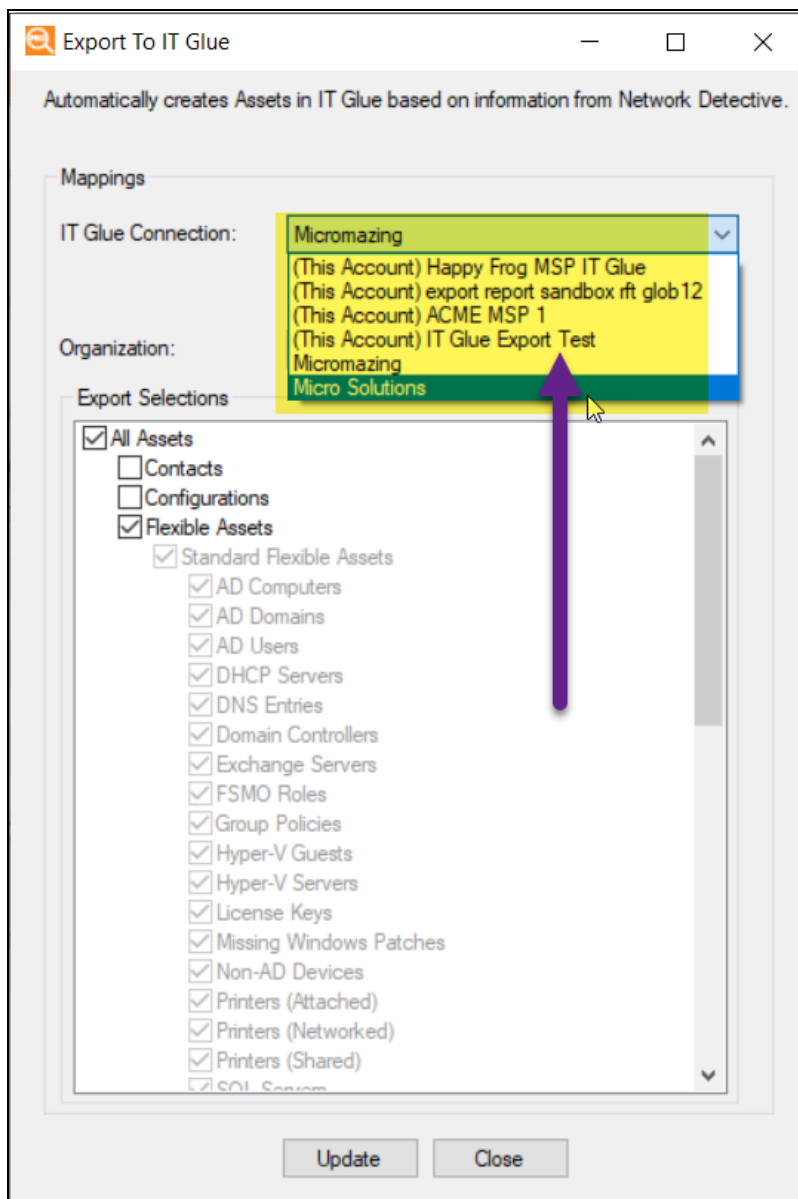
When you are finished configuring the mapping, click **OK**.

5. Select the connection and click **Close**.



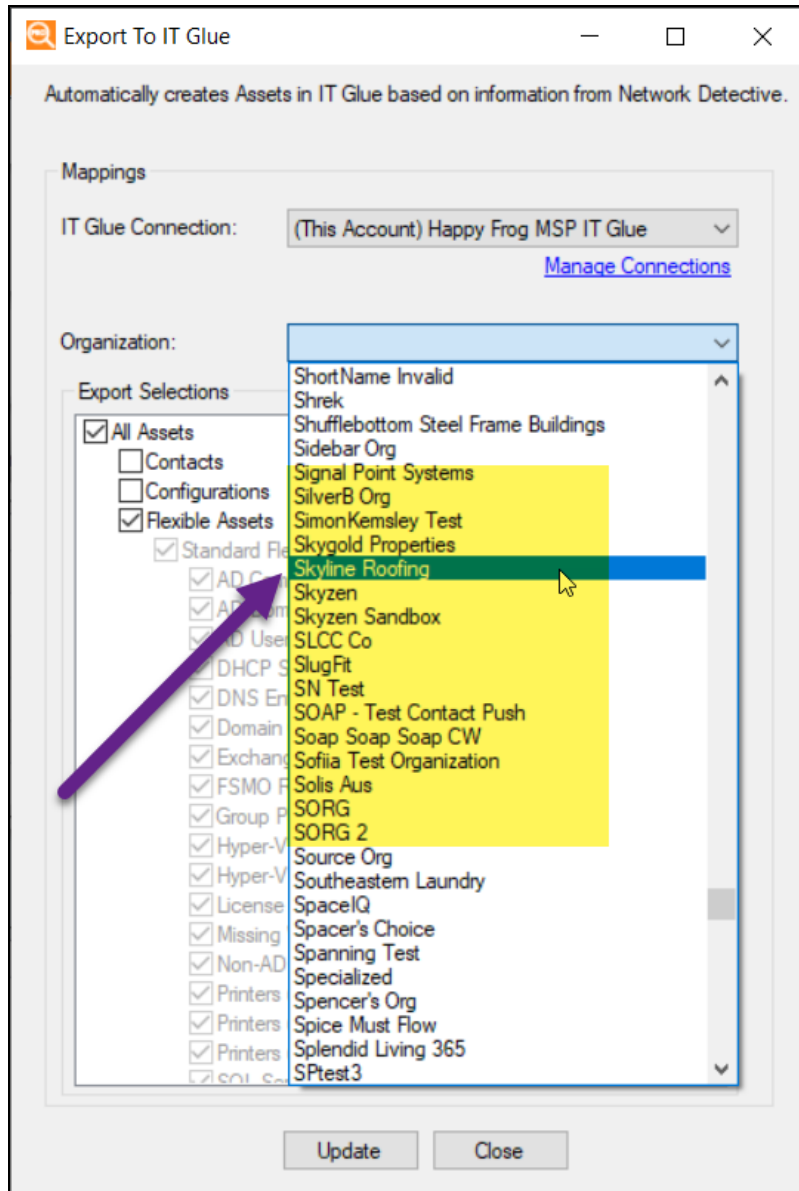
Step 4 — Continue Configuring Export Task

1. Next, select the **IT Glue Connection** you created from the drop-down menu.



2. 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.



3. Finally, select which configuration items to export.

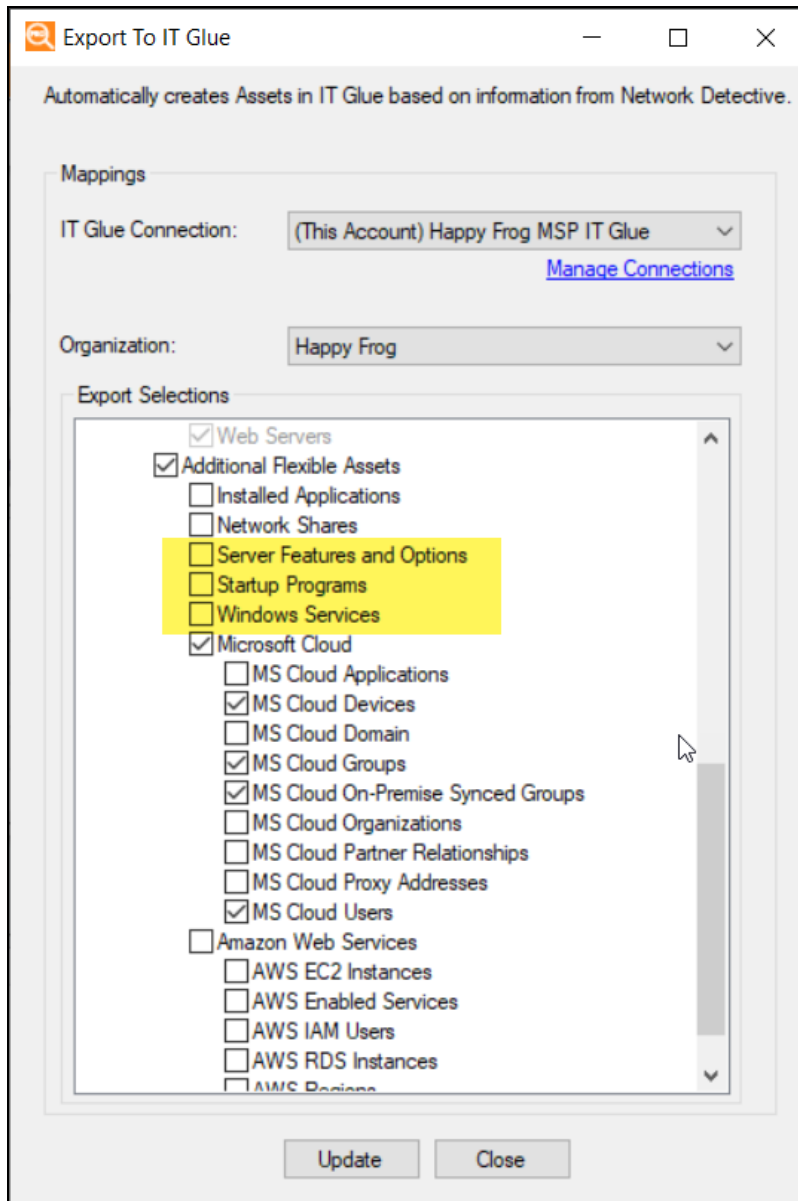
Important: Warning! If you have other integrations creating Contacts and/or Configurations in IT Glue such as a PSA and RMM, **DO NOT select the Export Contacts and Export Configurations options** as they will create unwanted duplicates.

We strongly recommend that you at least leave the following items unchecked. These are disabled by default:

- 'Server Features and Options'

- 'Startup Programs'
- 'Windows Services'

If you do select these options, the Reporter will detect and add all of these items to IT Glue which may clutter search and navigation.



4. 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

- 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.

Name	Status	Type	OS	Primary	Serial N	Expires	Location
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...			

Step 5 — Access data in IT Glue after scan and export

- Log into your IT Glue account and navigate to the Organization main page.
- Click on a newly updated item in the **Apps & Services** section in the left-hand menu. The Flexible Asset types are:
 - AD Computer
 - AD Domain
 - AD User
 - AWS EC2
 - AWS Enabled Services
 - AWS RDS
 - AWS Regions

- AWS S3
- AWS VPC
- DHCP Server
- DNS Entry
- Domain Controller
- Enabled Optional Feature
- Enabled Server Feature
- Exchange Server
- FSMO Role
- Group Policy
- Hyper-V Guest
- Hyper-V Server
- Installed Application
- License key
- Microsoft SQL Server
- Missing Windows Patch
- MS Cloud Applications
- MS Cloud Devices
- MS Cloud Domains
- MS Cloud Groups
- MS Cloud On-Premise Synced Groups
- MS Cloud Organizations
- MS Cloud Partner Relationships
- MS Cloud Proxy Addresses
- MS Cloud Users
- Network Share
- Non-AD Device
- Printer (Attached)
- Printer (Networked)
- Printer (Share)
- Security Group

- Startup Programs
 - Time Server
 - Web Server
 - Windows Services
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 and Contacts" below](#) for more details on how the system avoids creating duplicate assets.

Matching Criteria for Configurations and Contacts

The Reporter Appliance will always attempt to make a match according to the criteria in existing IT Glue Configurations and Contacts as listed in the table below.

In the case that there is no match, Reporter will create a new IT Glue Configuration and Contact. The matching logic for IT Glue Configurations and Contacts is similar to that of a PSA and RMM.

Rule for match on association	Association matches on
IT Glue Configurations	• Exact match on primary MAC address and serial number. ◦ If there is no match on <i>both</i> of these fields, the exact match is on the primary MAC address. ◦ If there is no match on that field, the exact match is on the serial number.
IT Glue Contacts	• Exact match both on a first and last name.

Association Criteria for Flexible Assets

New Flexible Assets created by the Reporter integration will always attempt to automatically associate to IT Glue assets (i.e. Configurations and Contacts) based on the table below:

Rule for match on association	Association matches on
IT Glue Configurations	- Exact match on primary MAC address and serial number. - If there is no match on both of these fields, the exact match is on the primary MAC address. - If there is no match on that field, the exact match is on the serial number.
IT Glue Contacts	- Exact match both on a first and last name. - If there is no match on these fields, the exact match is on the email address (not case sensitive).
IT Glue Domains	Domain name

Key Fields

What is a Key Field? Each Flexible Asset created by the Reporter integration has specific fields that it uses to associate data to. Please see the table below for all Key Fields.

Important: After the initial scan by the Reporter Appliance, **DO NOT** edit the content in these fields within IT Glue. **Doing so will create duplicates in your IT Glue account.** If you edit the fields after the initial scan, the fields will not match again in subsequent scans and the integration will create a new, duplicate asset.

Flexible Asset Type	Key Fields
AD Domain	Domain Name
Domain Controller	Computer*, Domain
FSMO Role	Domain, Role, Domain Controller
AD Computer	Domain, Configuration
AD User	Domain, Username
Security Group	Domain, Group Name

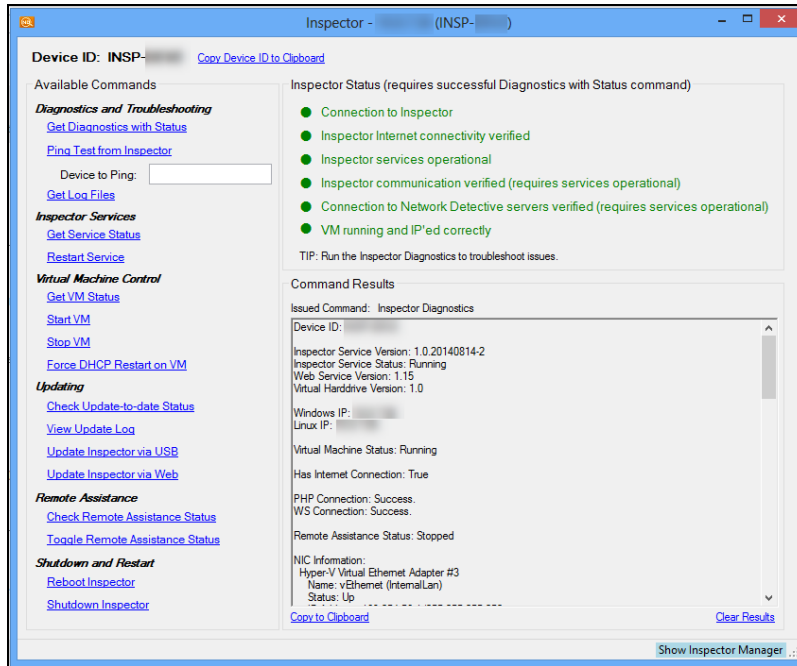
Flexible Asset Type	Key Fields
Group Policy	Domain, Policy Name
DNS Entry	IP Address
Windows Service	Computer*, Service Name
Enabled Server Feature	Computer*, Feature
Enabled Optional Server	Computer*, Feature
Startup Programs	Computer*, Startup Item
Non-AD Device	IP Address, Computer Name
Microsoft SQL Server	Sever Name, Instance
Web Server	Computer Name
Time Server	Server Name
Exchange Server	Server Name
DHCP Server	Server Name
Hyper-V Server	Hostname
Hyper-V Guest	Host, Guest Name
Printer (Attached)	IP Address, Printer Name
Printer (Networked)	IP Address, Printer Name
Printer (Share)	Shared Printer
Network Share	Hose, Share UNC

Flexible Asset Type	Key Fields
Installed Application	Computer*, Application Name
License Key	Computer*, Application Name
Missing Window Patch	Computer*, Issue

* IT Glue Configuration

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.



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

- *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.

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.

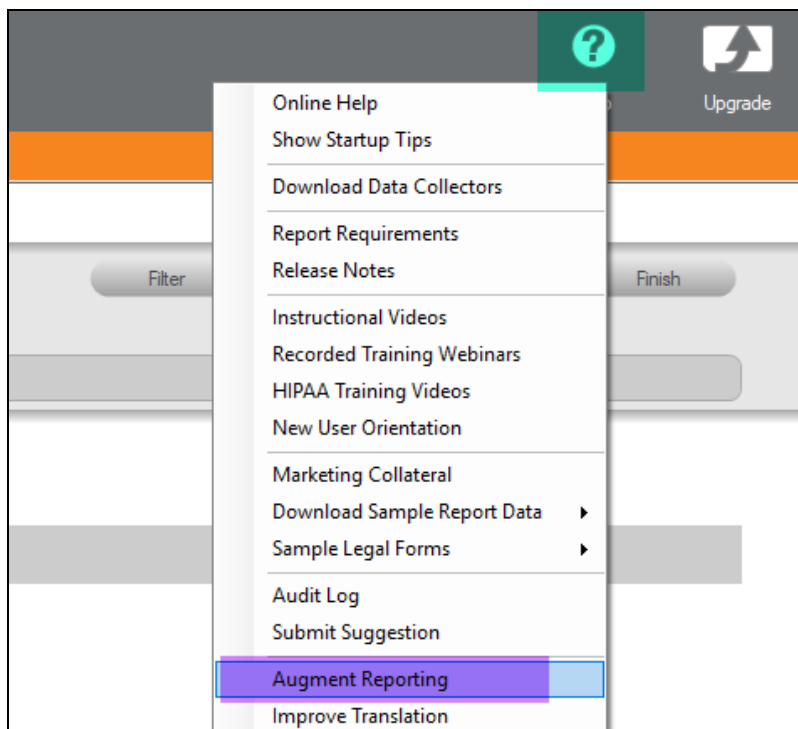
Augment Reporting to Eliminate False Positives

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.

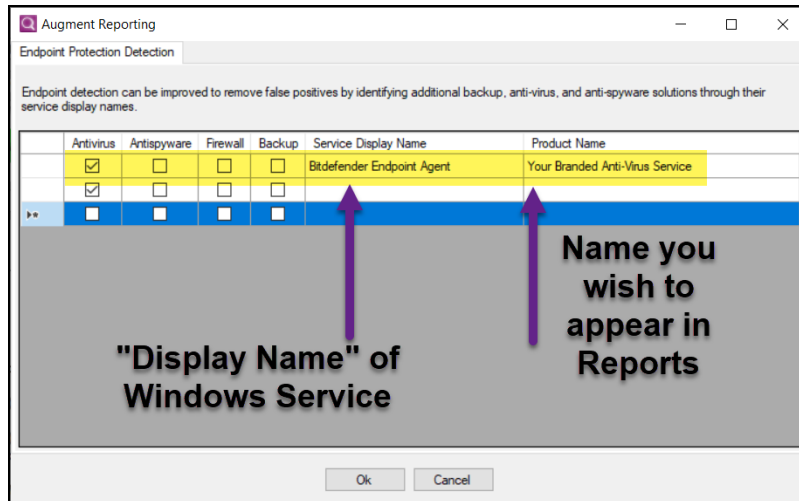
To augment your reports:

1. In Network Detective, go to **Help > Augment Reporting**.



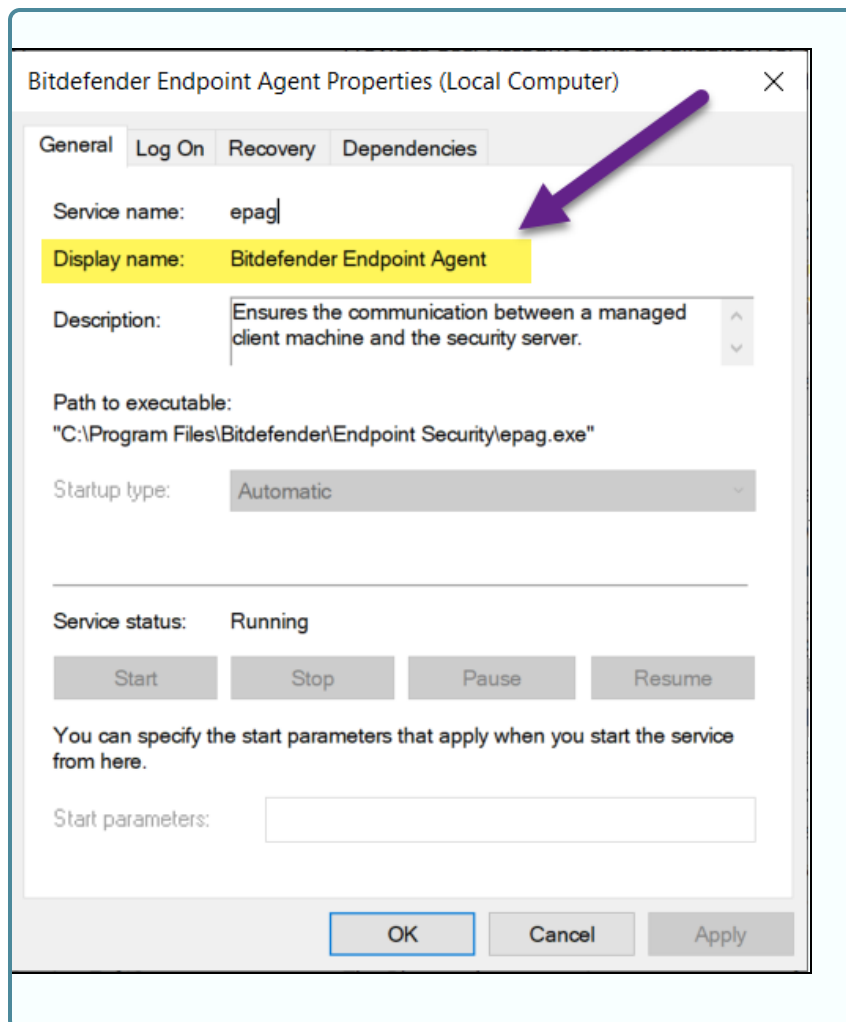
The **Endpoint Protection Detection** screen will appear.

2. For each application you wish to add to your reports, select the type of application: *Antivirus, Antispyware, Firewall, and/or Backup*.



3. Then enter the *Display Name* for the Windows Service.

Note: You can find the *Display Name* by opening the Windows Services app from your desktop. **Right click** on the service and click **Properties**. See ["Use the Excel Export Spreadsheet to Find Display Names" on the facing page](#) for an easy way to find display names for all Windows services.



4. Next enter the **Product Name** for use with reporting. You can choose any name you wish for the Product Name for your Reports.
5. Repeat these steps for each app you wish to add to your reports.
6. Click **OK**.

When 1) you next collect data on the target endpoints and 2) generate reports, your new reports will feature information on the apps you included.

Use the Excel Export Spreadsheet to Find Display Names

You can use the **Excel Export** from the Network Assessment Module to find Display Names for Windows Services. This might be helpful if you want to enter several apps into the Augment Reporting tool.

- 1. Generate the Excel Export Report from a NAM Assessment.
- 2. Open the report and navigate in Excel to the Windows Services worksheet.

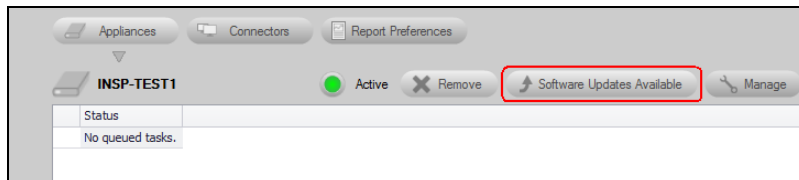
APP01	CertPropSvc	Certificate Pro
APP01	ClipSVC	Client License
APP01	COMSysApp	COM+ System
APP01	CoreMessagingRegistrar	CoreMessaging
APP01	CryptSvc	Cryptographic
▶ ... Workstation Aging-test Windows Services-test Server Features-tes		

- 3. View the service entry for the *Antivirus, Antispyware, Firewall, and/or Backup* software installed on the computer and include this in the Augment Reporting tool.

Computer Name	Service Name	Display Name	Startup Type	Start Name
BACKUP01	WinDefend	Windows Defender Service	Auto	LocalSystem

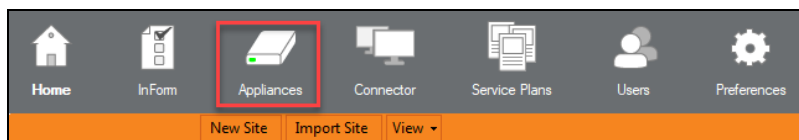
Updating a Software Appliance

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.

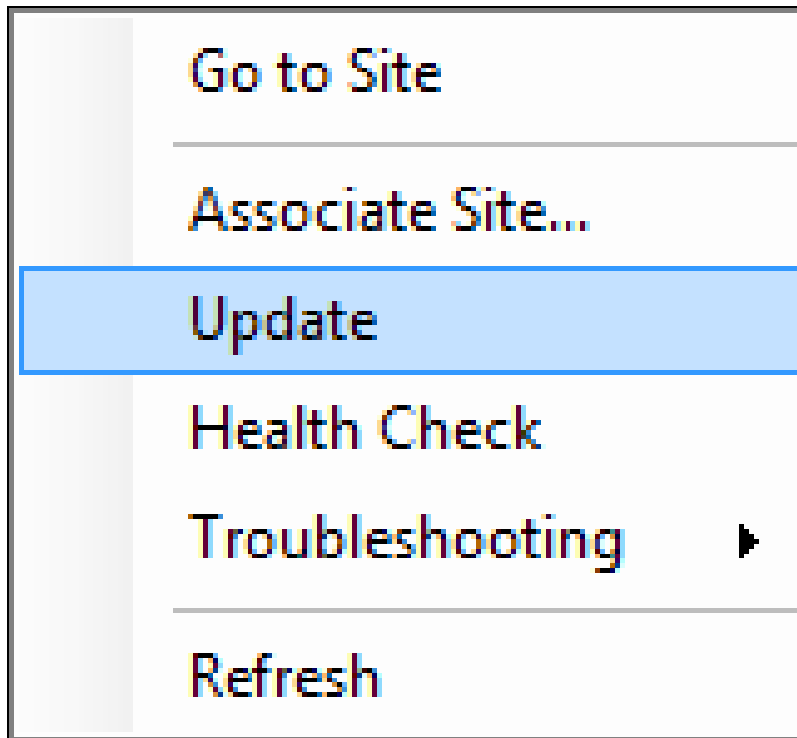
In the **Network Detective Application**, navigate to **Network Detective** ribbon bar and select the **Appliances** icon.



This action will display the **Software Appliances** window that lists all of the **Appliances** that are available for use from within **Network Detective**.

Appliances		Appliance Overview: Download Logs Manage Scans Manage Reports Health Check Update						
Status	Appliance Id	Type	Appliances	Site Name	Running Tasks	Queued Tasks	Update Status	Last Check-in
		Physical	Inspector		0	0	Current	2/11/2016 11:28:07 AM
		Physical	Reporter	Inspector Reporting	0	0	Current	2/11/2016 11:28:06 AM
		Physical	Inspector		0	0	Current	2/11/2016 11:28:06 AM
		Physical	Inspector		0	0	Updates Available	2/11/2016 11:28:07 AM
		Physical	Inspector		0	0	Updates Available	2/11/2016 11:28:05 AM
		Physical	Inspector		0	0	Updates Available	2/11/2016 11:28:08 AM
		Physical	Inspector		0	0	Current	1/29/2016 1:10:02 PM
		Physical	Inspector		0	0	Current	2/5/2016 9:05:36 AM
		Physical	Inspector		0	0	Updates Available	2/11/2016 10:42:53 AM

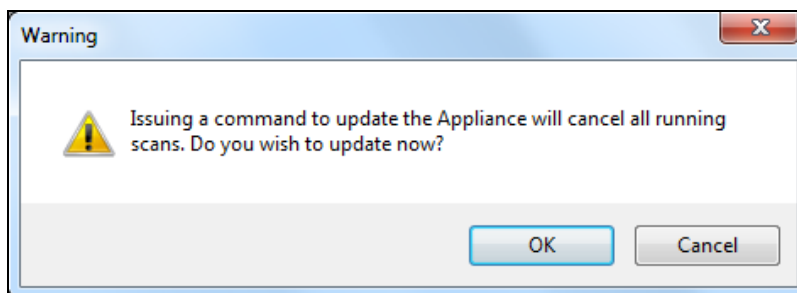
To update the selected **Software Appliance**, right click on the **Appliance's** name, and select the **Update** menu option presented as displayed.



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.

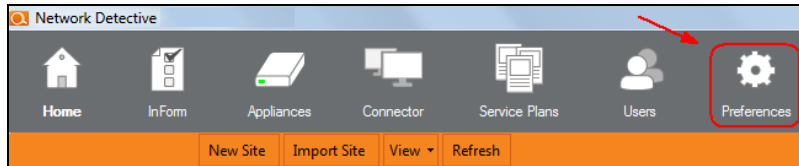


A window will appear confirming the request for a software update.

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.

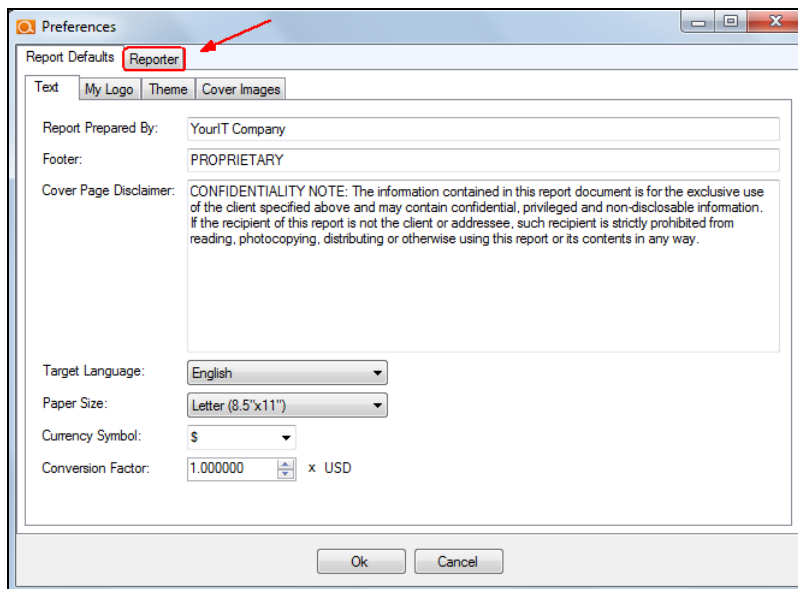
Follow these steps to set up the Reporter Custom SMTP **Email Server Configuration**.



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.



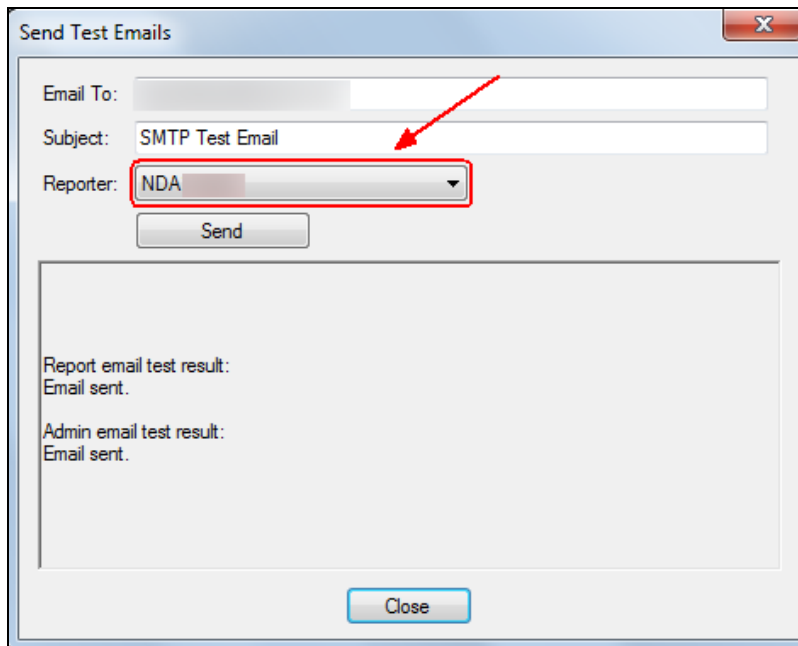
3. Configure the following to set up your **Custom SMTP Server** to relay email **Notifications** sent from Reporter:

The screenshot shows the 'Reporter' tab of the 'Preferences' dialog box. At the top, there's a section for 'Don't use scans older than the following number of days:' with a value of 42. Below this is the 'SMTP Server' section. It contains two input fields: 'Report From:' with the value 'security-tech@youritcompany.com' and 'Display Name:' with the value 'IT Security Reports from Reporter'. There are two radio buttons: 'Use Default SMTP Server' (unselected) and 'Use Custom SMTP Server' (selected). Below the radio buttons is a section titled 'Custom SMTP Settings' with a yellow note: 'Note: SMTP Server must support TLS 1.2 or above.' This section contains several input fields: 'SMTP Server Address:' with 'smtp.mail.youritcompany.com', 'Port:' with '587', 'Security:' with a dropdown menu set to 'SSL', 'Username:' with 'security-tech@youritcompany.com', and 'Password:' with a masked field '*****'. A 'Send Test Emails' button is located at the bottom right of the 'Custom SMTP Settings' section. At the very bottom of the dialog are 'Ok' and 'Cancel' buttons.

- **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.

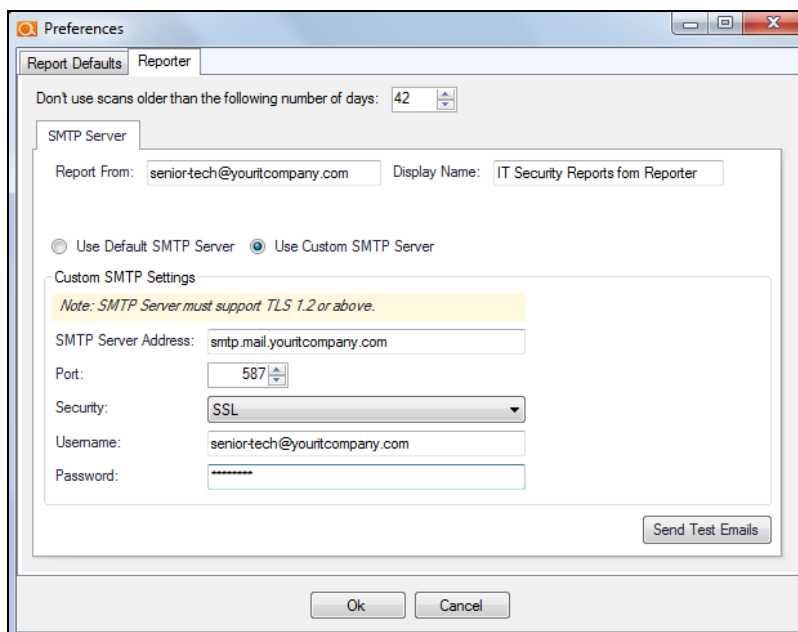
This screenshot is identical to the one above, showing the 'Reporter' tab of the 'Preferences' dialog box. The configuration for the 'Custom SMTP Server' is the same. A red arrow points from the right side of the dialog to the 'Send Test Emails' button, which is highlighted with a red rectangular box. The 'Ok' and 'Cancel' buttons are at the bottom.

5. Select your Reporter ID from the Reporter ID list.



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.

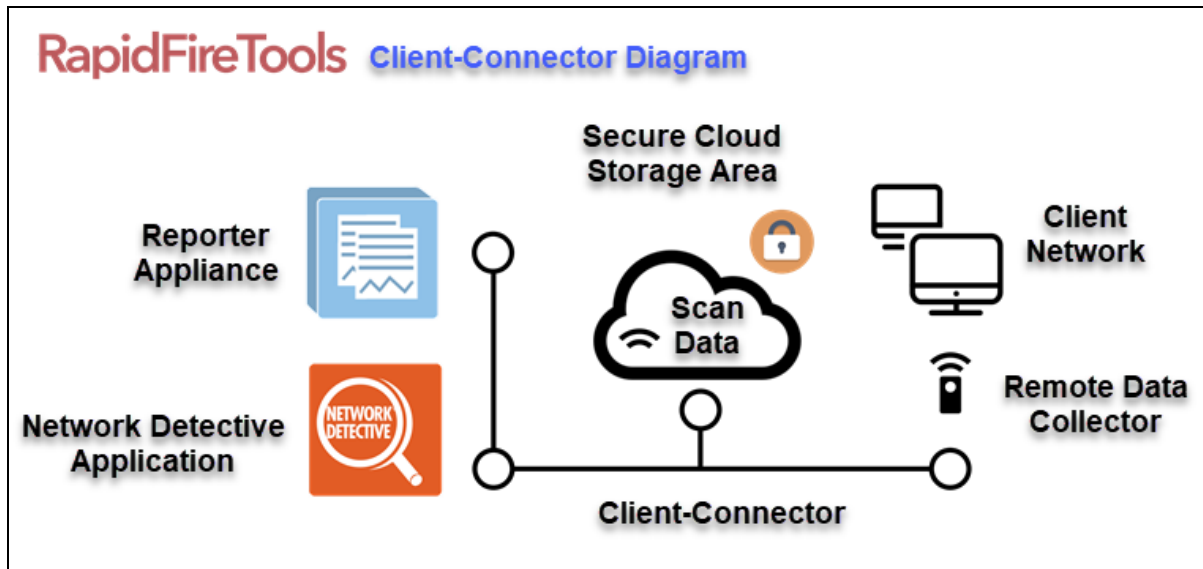


6. After a successful test has been completed, close the **Send Test Emails** window.

Next, select the **OK** button in the **Preferences** window to save the **Custom SMTP Server's Email Configuration** settings.

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.



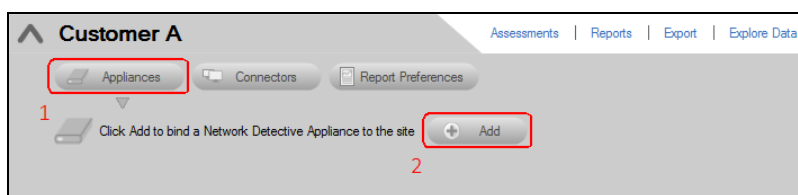
Using Reporter with Cyber Hawk

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:

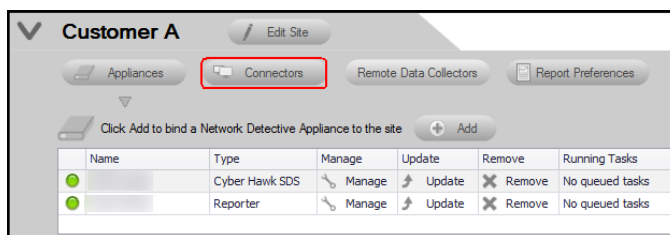
Step 1 — Associate Reporter and Cyber Hawk with the same Site

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.



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.



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.

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](#)

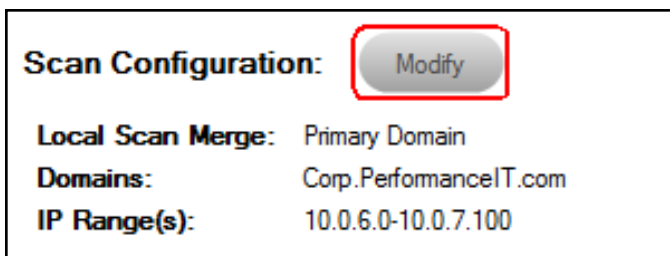
Step 2 — Configure Cyber Hawk to Upload Scans for use by Reporter

Next set up your Cyber Hawk scans to work with your Reporter. To do this:

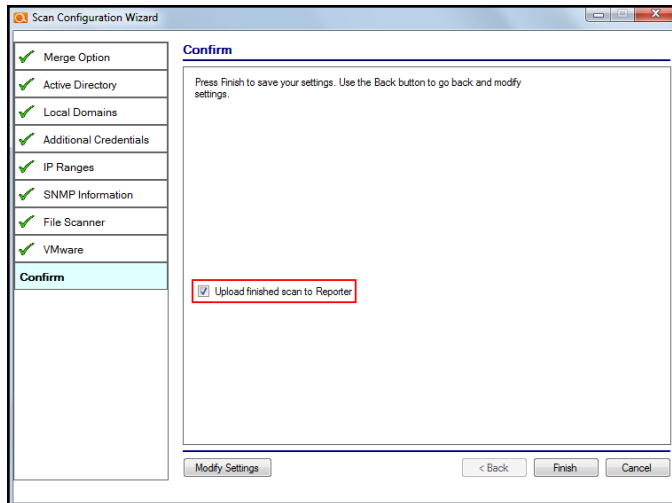
1. Open Cyber Hawk from your Site.



2. Click **Modify** next to Scan Configuration.



3. Configure your scan. In the Scan Configuration Wizard window, select the option **"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**.

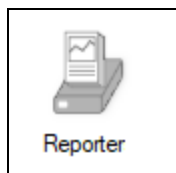
However, for **SQL**, **Exchange**, **HIPAA**, and **PCI** assessments, you will need to use the Remote Data Collector.

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.

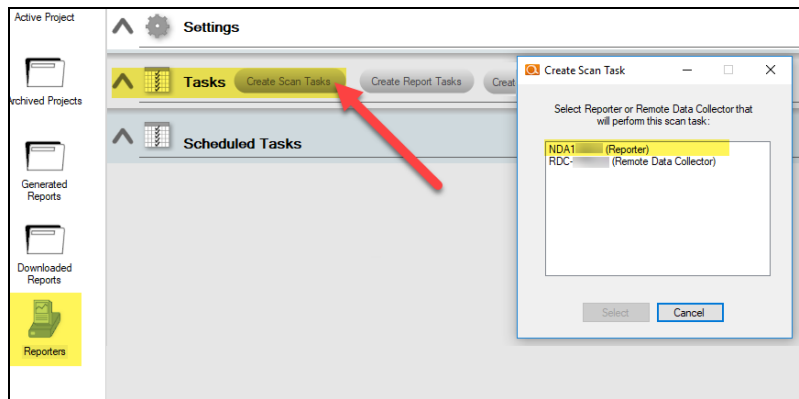
Step 3 — Set up Reporter to Automatically Generate Reports

The last step is to configure your Reporter tasks for automated reports.

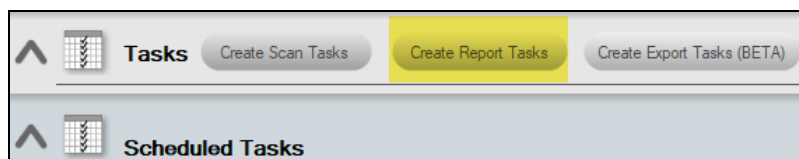
1. Open your active assessment project and click the **Reporter** icon.



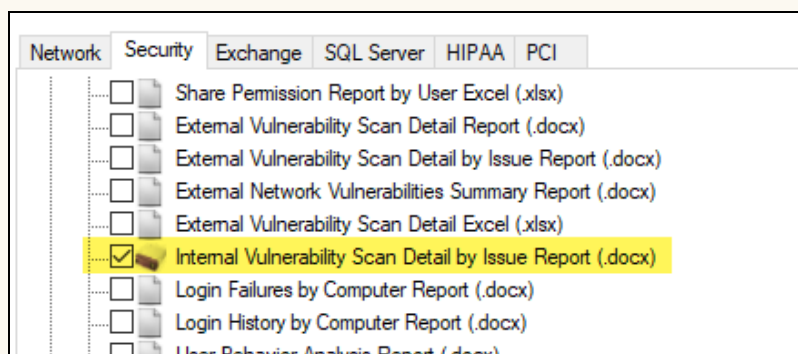
- (Optional) If you want to set up an automated *External Vulnerability Scan*, click the **Create Scan Task** button and select the **Reporter** (NOT the Remote Data Collector). Then configure your External Vulnerability Scan.



- 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**.



Note: Once you create scan and report tasks, click **Schedule** to set a time and day for them to regularly occur.

See also:

- [Configure Reporter to Access Scan Data and Generate Reports](#)
- [Setting Up Automatic Reports by Assessment Module](#)

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation – and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

Note: You must have the .NET 3.5 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
GPO Configuration for Windows Firewall (Inbound Rules)	
☐	Allow <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
☐	Allow <i>File and printer sharing</i> to operate through Windows Firewall This includes the following rules: • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
☐	Enable <i>Remote Registry</i> “read only” access on computers targeted for scanning.

Complete	Domain Configuration
	Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.
☐	Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request Note: ICMP requests are used to detect active Windows computers and network devices to scan.
GPO Configuration for Windows Services	
☐	<i>Windows Management Instrumentation (WMI)</i> • Startup Type: Automatic
☐	<i>Windows Update Service</i> • Startup Type: Automatic
☐	<i>Remote Registry</i> • Startup Type: Automatic
☐	<i>Remote Procedure Call</i> • Startup Type: Automatic
Network Shares	
☐	• <i>Admin\$</i> must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

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 requirement for both Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

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

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

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

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

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

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

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

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

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

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

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

Complete?	Workgroup Configuration
	Network Settings
☐	• <i>Admin\$</i> must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
☐	• <i>File and printer sharing</i> must be enabled on the computers you wish to scan
☐	• <i>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</i> • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
☐	• Workgroup computer administrator user account credentials. Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard.
☐	Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:

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.