NETWORK DETECTIVE™

USER GUIDE

Inspector

Deep-Dive Scans Produce Special Reports for Added Network & Security Expertise

11/2/2023 5:00 PM

Contents

Introduction to Inspector **5**

Inspector Overview 5

Components of the Inspector Software Appliance 5

Inspector Software Appliance Features 7

Network Assessment Network Scan 7

Layer 2/3 Discovery of Network Devices (Exclusive to the Inspector) 7

Internal Vulnerability Scan (Exclusive to the Inspector) 7

HIPAA Compliance and Risk Assessment Scans 8

PCI Compliance and Risk Assessment Scans 8

External Vulnerability Scan 8

Automated Assessment Reporting 8

Remote Updating of the Inspector Software Appliance 9

Inspector Automated Scanning and Scheduling Best Practices 9

Inspector Appliance System Requirements 9

Setting Up Inspector **11**

Initial Inspector Set Up 11

Step 1 — Install Inspector Appliance on MSP Network 11

Step 2 — Open Existing Network Detective Site with an Active Assessment Project 13

Step 3 — Associate Inspector with a Site 14

Configure Inspector Scans 15

Inspector Scans **19**

Managing, Running, and Scheduling Scans (Inspector) 19

Scan Task Library versus Scan Tasks Queue 19

Manage the Scan Queue 19

Run a Scan On-Demand 20

Schedule a Scan 21

Cancel a Scan 23

Configuring Inspector Scans by Type/Assessment Module 25

Network/Security Scan 25
Scanning an Active Directory Domain Network 25
Scanning a Workgroup Network 34
Using the Run Now Option 42
HIPAA Compliance Network Scan 44
PCI Compliance Network Scan 46
Push Deploy Local Computer Scan for PCI 47
Push Deploy Local Computer Scan for HIPAA 51
Push Deploy (All Modules) 55
Internal Vulnerability Scan 56
Tips for Scheduling the Level 2 Scan 57
Layer 2/3 Discovery Scan 59
External Vulnerability Scan 60
Schedule the Running of the External Vulnerability Scan 62
Configuring the Local Data Scan Merges 65
Step 1 — Select and Open the Site 65
Step 2 — Select Manage Appliance 65
Step 3 — Set Scan Data Merge Configuration 66
Step 4 — Set the Local Scan Merge Settings and Save Settings 66
Setting Up Automatic Reports with Inspector 68
Network Assessments Automatic Reports 68
Security Assessments Automatic Reports 72
HIPAA Compliance Assessments Automatic Reports 75
Performing the Initial HIPAA Assessment Report Generation Set-up 75
PCI Compliance Assessments Automatic Reports 79
Performing the Initial PCI Assessment Report Generation Set-up 79
Manually Download Reports 83
Inspector Appendices 86
Pre-Scan Network Configuration Checklist 87
Checklist for Domain Environments 87
Checklist for Workgroup Environments 89

Updating a Software Appliance 91
Inspector Appliance Override 94
Set Scan and Report Task Time Zone and Date Format 96
At Site Level 96
At Global Level 97
Software Appliance Diagnostic Tool 98
Available Commands 98

Introduction to Inspector

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

Inspector Overview

The Inspector Software Appliance is an appliance-based system used for performing scheduled IT assessment scans and deep dive security diagnostics.

This guide is designed to provide an overview and specific steps required to install and configure the Inspector Software Appliance and schedule the collection of data to be used with other Network Detective modules, including:

- Network and Security assessment data
- SQL Server assessment data
- Internal Network Vulnerability assessment data
- Layer 2/3 Discovery and Network assessment data
- Local Login Anomaly assessment data
- HIPAA Compliance assessment data
- PCI Compliance assessment data

Components of the Inspector Software Appliance

Inspector Component	Description
Inspector Software Appliance	This is the Inspector software application that operates on either the **Network Detective Hardware Appliance** or on a user supplied Microsoft Hyper-V or VMware based system.
Optional Network Detective Hardware Appliance	This is an optional hardware component that can be purchased from RapidFire Tools to host and operate the **Inspector Software Appliance**. It is a small form factor computer server which plugs into the target network through an Ethernet connection.
Inspector Diagnostic Tool	This tool is used for configuring and troubleshooting the Inspector. The Diagnostic Tool should be run on the same network as the **Inspector** to perform diagnostics checks such as for Inspector connectivity or for available updates.
Network Detective	This is the same Network Detective desktop application and report

Inspector Component	Description
Application	generator that is used with any other Network Detective modules. This application contains additional features to manage the **Inspector** remotely.

Inspector Software Appliance Features

One key purpose of the **Inspector** is to perform scans from the point-of-view of the client's internal network.

Below is an overview of the scans that can be performed by the **Inspector Software Appliance**.

Network Assessment Network Scan

The full Network Assessment Scan from the point-of-view of the **Inspector Software Appliance**. The resulting scan can be used to generate reports from the Network Assessment module.

> **Note:** This feature requires the Network Assessment Module.

Layer 2/3 Discovery of Network Devices (Exclusive to the Inspector)

Run when the Network Assessment Network Scan is executed. Scans network devices for Layer 2 and Layer 3 connectivity information. The scans are used to generate Layer 2/3 diagram and detail reports.

Internal Vulnerability Scan (Exclusive to the Inspector)

This scan takes advantage of the point-of-view provided by being connected to the client's internal network. Data is collected about Open Ports and Protocol Vulnerability that would be exploited once a hacker is in the network. The Internal Vulnerability Scan analyzes the network from the inside, from the perspective of an attacker who is within the internal network. The External Vulnerability scan, on the other hand, checks for potential weak points on the outside edge of the network.

Internal vulnerability scans are similar to external vulnerability scans; however, they are performed from inside the target network. They look for vulnerabilities that are normally blocked externally by firewalls. Within a network, un-patched or vulnerable systems may exist that an external scan may not capture. This scan option performs a vulnerability scans with additional options which may be more intensive than the external equivalent.

Important: Please be aware that scans may be resource intensive. To minimize impact on the network, you may wish to run the scan during non-business hours; however, off-hour scans may miss computers which are offline during the time of the scans (i.e., turned-off desktops and mobile laptops).

HIPAA Compliance and Risk Assessment Scans

These network and local scans can be scheduled and executed by Inspector in order to identify ePHI, network vulnerabilities, security vulnerabilities, and local computer vulnerabilities necessary to perform a HIPAA IT Risk Assessment.

Note: This feature requires the HIPAA Assessment Module.

PCI Compliance and Risk Assessment Scans

These network and local scans can be scheduled and executed by Inspector in order to identify credit/debit card Primary Account Number (PAN) data, network vulnerabilities, security vulnerabilities, and local computer vulnerabilities necessary to perform a PCI Data Security Standard (DSS) Compliance and IT Risk Assessment.

Note: This feature requires the PCI Assessment Module.

External Vulnerability Scan

External Vulnerability scans are performed at the external “Network Edge” to check for security holes and weakness that can help you help make better network security decisions. The External Vulnerability Scan performed by Inspector 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

Automated Assessment Reporting

Automatic Report Generation enables you to use the Inspector to schedule and generate of a number of assessment reports associated with the following:

- Network Assessments
- Security Assessments
- SQL Server
- HIPAA Compliance Assessments
- PCI Compliance Assessments

Remote Updating of the Inspector Software Appliance

The **Inspector Software Appliance** is easy to update remotely. Updates include bug fixes, new features, and additional scans types.

Inspector Automated Scanning and Scheduling Best Practices

It is recommended that Network, Local Computer, External Vulnerability, Layer 2/3 Discovery and Network, and the Local Collector Push for Login Anomaly Reporting scans are scheduled to be performed on a weekly basis.

It is recommended that Internal Vulnerability scans are scheduled to be performed on a monthly basis or after any significant IT infrastructure change has taken place.

Inspector Appliance System Requirements

Below are the minimum requirements for installing and operating Inspector.

Please note the **Operational Requirements** that must be met after Inspector has been installed and deployed.

Hyper-V Install Requirements:

- Hyper-V Enabled Operating System (Windows 8.1+)
- 6 GB Available RAM
- 40 GB Hard Drive Space

VMware Install Requirements:

- ESXi 5.5+
- 6 GB Available RAM
- 40 GB Hard Drive Space

Operational Requirements:

- i5 Processor for dedicated use. Xeon server class processors for non-dedicated.
- 16 GB Available RAM
- 40 GB Hard Drive Space

Setting Up Inspector

Setting up your Inspector consists of these steps:

1. "Initial Inspector Set Up" below
2. "Configure Inspector Scans" on page 15

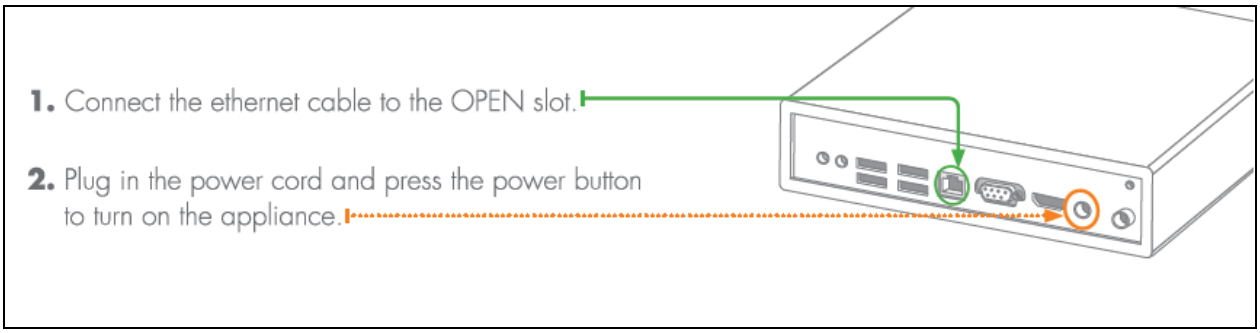
Initial Inspector Set Up

Step 1 — Install Inspector Appliance on MSP Network

Install the Inspector Appliance on your company's network by either:

A. *Connect the Inspector Appliance installed on the Small Form Factor Server Computer that you purchased from RapidFire Tools to your MSP Network.*

To set up the **Small Form Factor Computer Server** used to operate the **Inspector**, first go to the physical location of the target network. After finding a secure location for the device, connecting it to the network can be accomplished in two easy steps:



B. *Visit www.rapidfiretools.com/nd to download and install the Network Detective Virtual Appliance on a Hyper-V or VMware enabled computer operating within your MSP company's network.*

For more information about installing the Virtual Appliance, please download the Virtual Appliance Installation Guide.

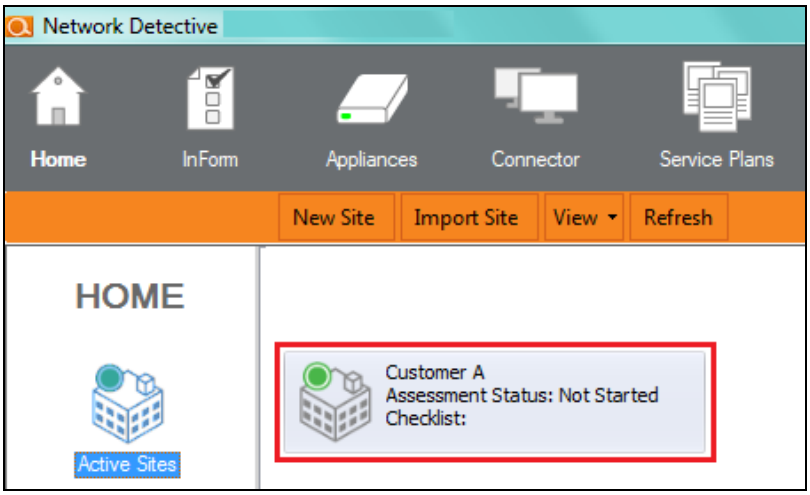
> **Note:** After the installation of the Inspector Appliance is complete, be sure to allocate the memory resources necessary to meet the minimum system Operational Requirements as detailed in "Inspector Appliance System Requirements" on page 9.

> **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 Inspector Appliance, visit www.rapidfiretools.com/nd 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 **Inspector 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 **Inspector Appliance** and a **Client-Connector**.

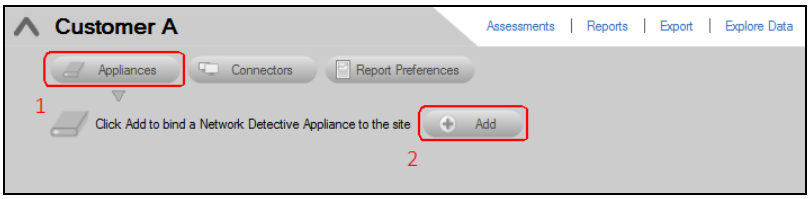
Step 3 — Associate Inspector with a Site

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

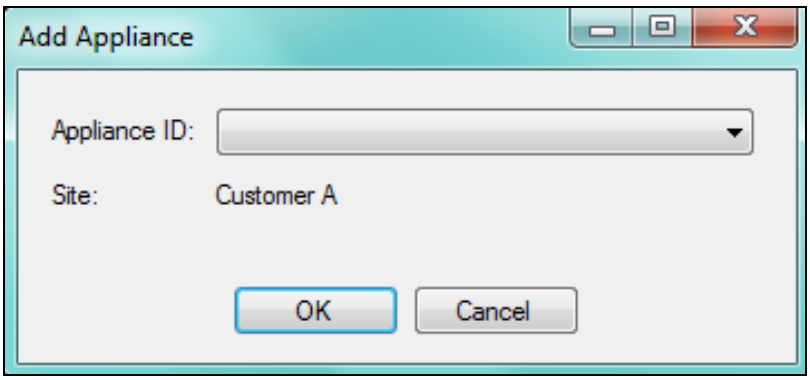
1. After creating a new Network Detective **Site**, or within an existing **Site**, in order to "**Associate**" a **Inspector** with the **Site** used for the **Assessment Project**, you must first select the  selector symbol to expand the **Site's** properties view.

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.

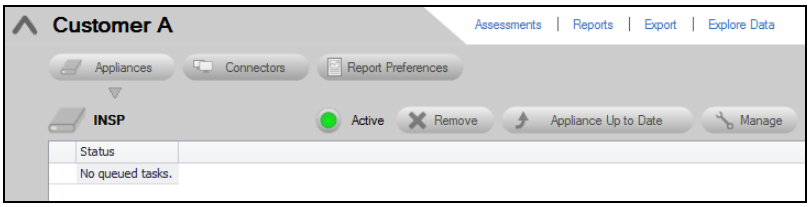


3. Select the **Appliance ID** of the **Inspector Appliance** from the drop down menu.

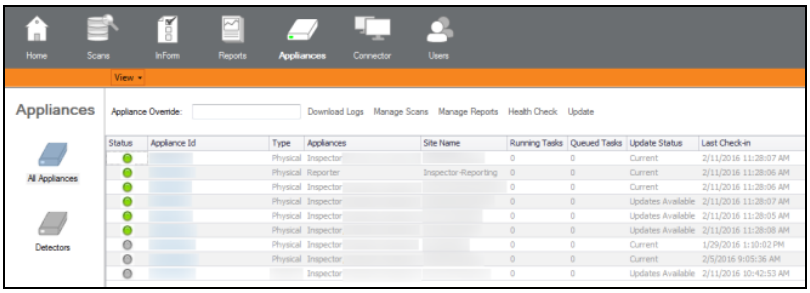


> **Note:** When users have purchased a **Small Form Factor Computer Server**, the **Appliance ID** can be found on a printed label on the **Hardware Appliance** itself.

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



4. To 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**.

Configure Inspector Scans

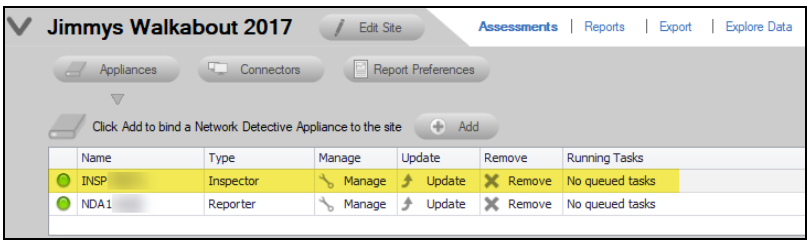
After associating an **Appliance** with a customer specific **Site** used for performing assessments, it is very simple to configure **Network Scans**, **Local Computer Scans**, **Internal Vulnerability Scans**, **Layer 2/3 Discovery and Network**, and the **Local Push Collector for Login Anomaly Reporting Scans** using the **Inspector Software Appliance** remotely from within the **Network Detective** desktop application.

With the **Inspector Software Appliance**, it is only necessary to go through the configuration and setup of a Network Scan one time. After completing the setup, the Scan

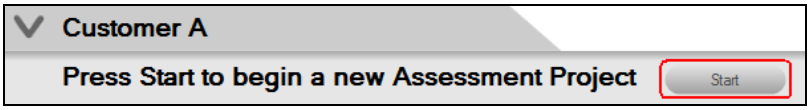
configurations will be stored and associated with the **Inspector Software Appliance** to be run either on-demand or on a set schedule.

To set up a scan, first, go to the target **Site's Assessment Window** and verify that an Inspector has been successfully associated with the **Site**.

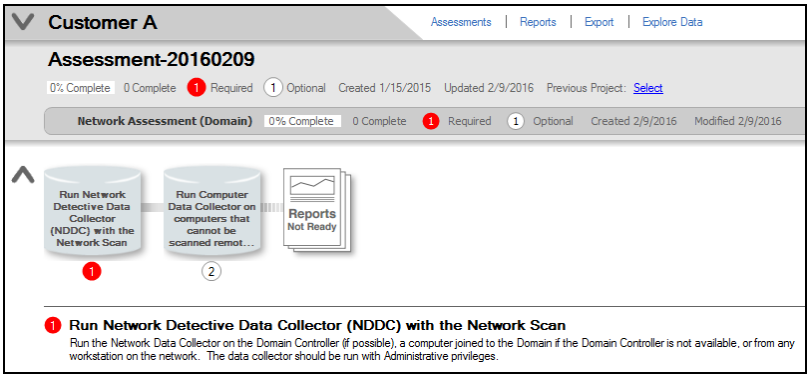
The Inspector(s) will appear under the **Appliances** bar.



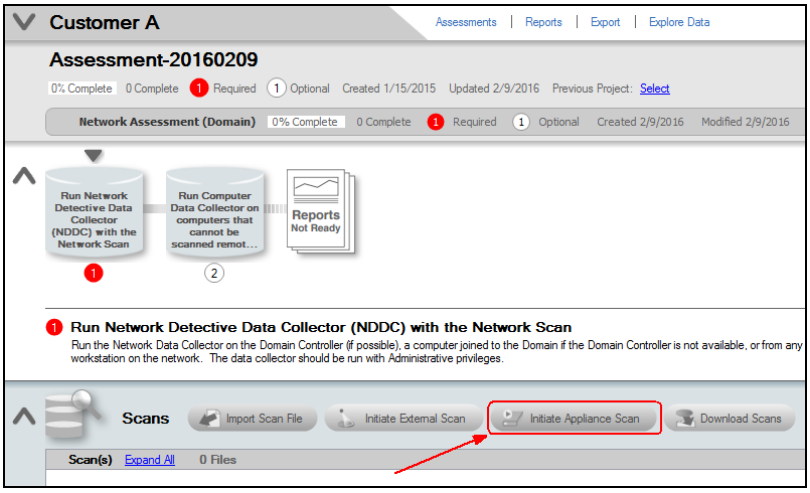
If the **Site** does not already have an active **Assessment**, start a new **Assessment** by clicking **Start** and following the prompts to choose the desired type of **Assessment**.



If an active **Assessment** is underway and available, the Assessment will be presented when the **Site** file is opened.

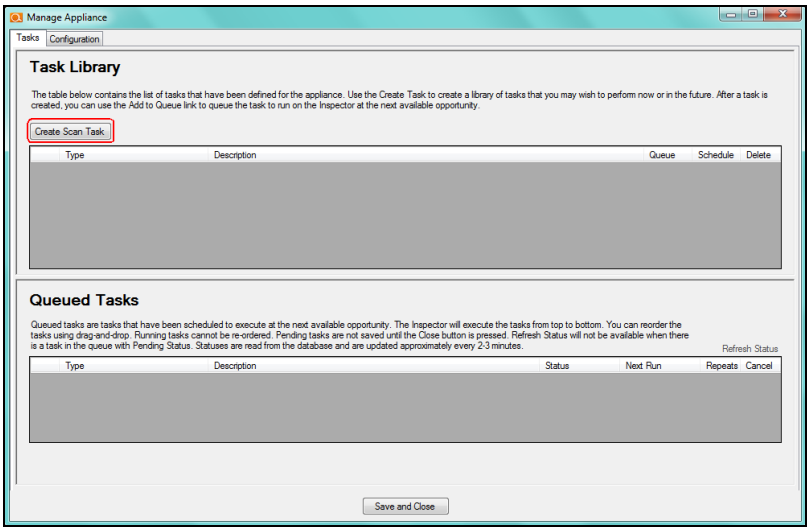


Upon selecting the **Active Assessment**, you will be directed to the assessment's **Assessment Window**.

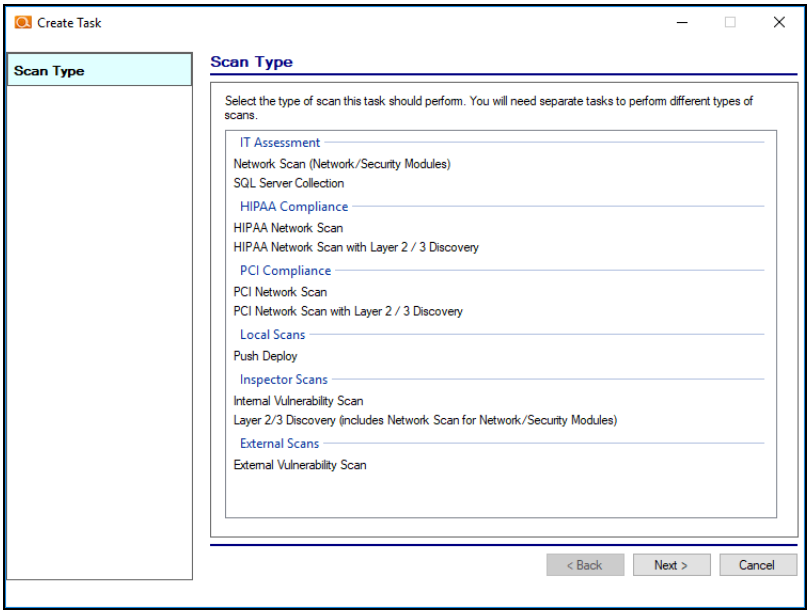


From the **Site's** active **Assessment**, select **Initiate Appliance Scan** from the **Scans** bar.

The **Manage Appliance Tasks** window will be displayed enabling you to select the IT or Compliance Assessment **scan** you want to perform, configure the scan task, and to store the scan task in the **Inspector Task Library** for either manual or scheduled execution.



If this is the first time a Scan has been initiated from the **Inspector Software Appliance**, follow the **Network Detective Data Collector's Create Task** prompts to configure the Scan.



Tip: See "Configuring Inspector Scans by Type/Assessment Module" on page 25 for detailed instructions on setting up Inspector scans.

Inspector Scans

This section covers everything you need to know about Inspector scans.

Managing, Running, and Scheduling Scans (Inspector)

Scan Task Library versus Scan Tasks Queue

The **Scan Task Library** contains saved Scan configurations which can be run on demand or on a schedule to conduct a number of scans that can be performed by the Inspector appliance. The advantage of the **Scan Task Library** is that the Scan configurations can be reused and run on-demand or on a schedule. There is no need to repeatedly enter the same information (such as the IP Range) each time a data collection is performed using this model. The scans **Tasks Queue** lists the scans that are pending.

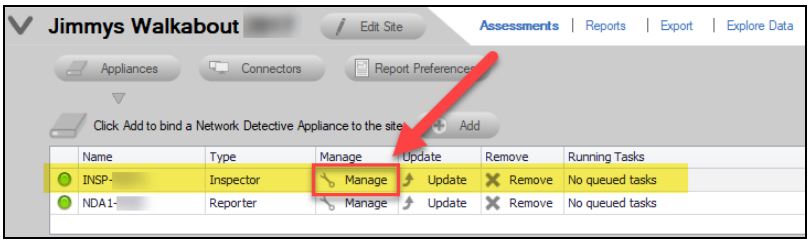
Manage the Scan Queue

After going through the steps to **Associate** the **Software Appliance** with a **Site**, configuring the **Scan tasks** , and storing the tasks in the **Task Library**, it is a simple process to run either an immediate or scheduled Data Collection scan on the target network.

Note that the Scan configuration process must only be completed one time and the resulting configuration will be stored for future use. The storing of this configuration information simplifies both automated and remote execution of scan tasks.

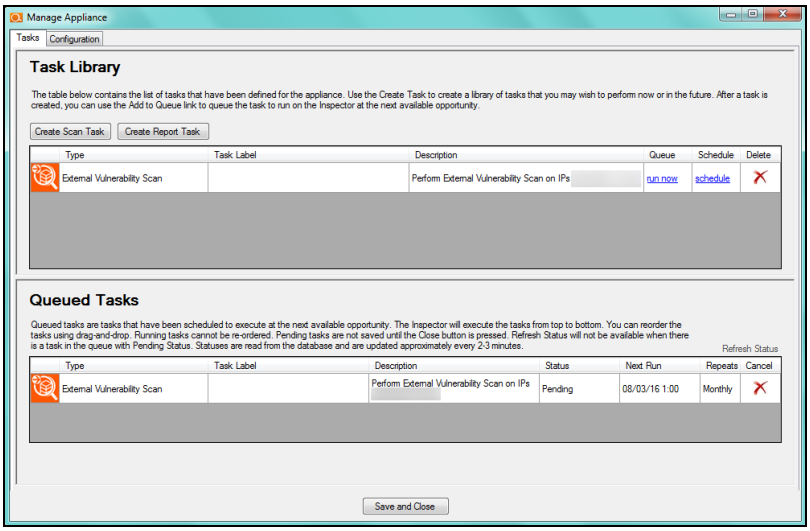
1. Open the **Site** that is being used with the **Inspector Appliance**.
2. Then navigate to the target **Site's Assessment Window**.
3. After starting a new assessment, or within an existing assessment, in order to "**Manage**" an Appliance within the Assessment Project, you must first select the  **Selector** symbol to expand the assessment properties view.

This action will expand the **Site's** properties for you to view and to add an Appliance to the **Site**.



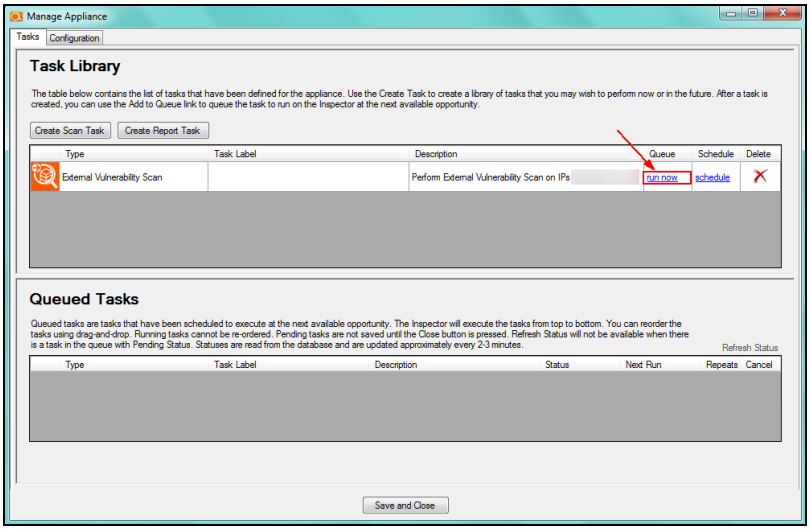
4. Under the **Appliances** bar in the **Site's Properties** window select the **Manage** button.

   This action will display the **Manage Appliance** window and present the **Task Library** along with the **Queued Tasks** previously set up on the **Appliance** for the specific **Site** you created the tasks to execute.



Run a Scan On-Demand

Scans can be executed immediately through the use of the **Run Now** feature.

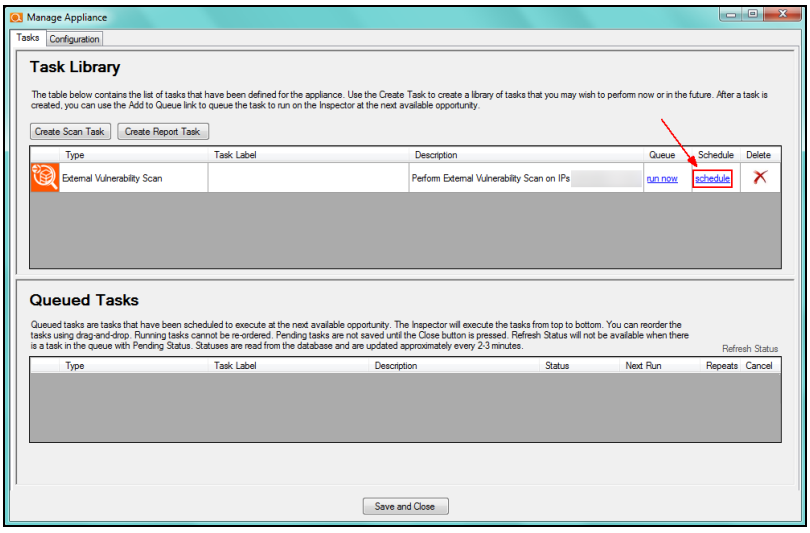


To run a Scan configuration, locate the task in the **Task Library** and select **Run Now**.

After the task has been queued, it will run as soon as resources are available. A Scan that is run on-demand (i.e. instead of on a schedule) will have no value in the table under the **Next Run** column in the **Queued Tasks** list.

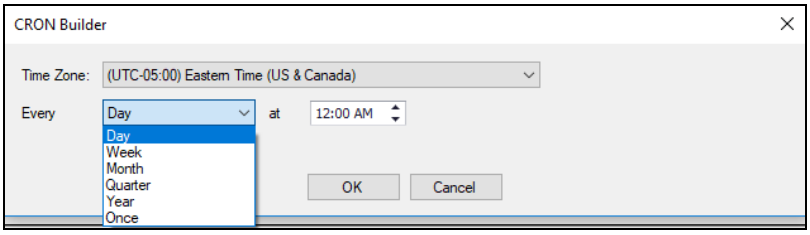
Schedule a Scan

1. To schedule a scan, click on **Schedule** link to open the **CRON Builder** window. The **CRON Builder** is used to schedule the running of scans.

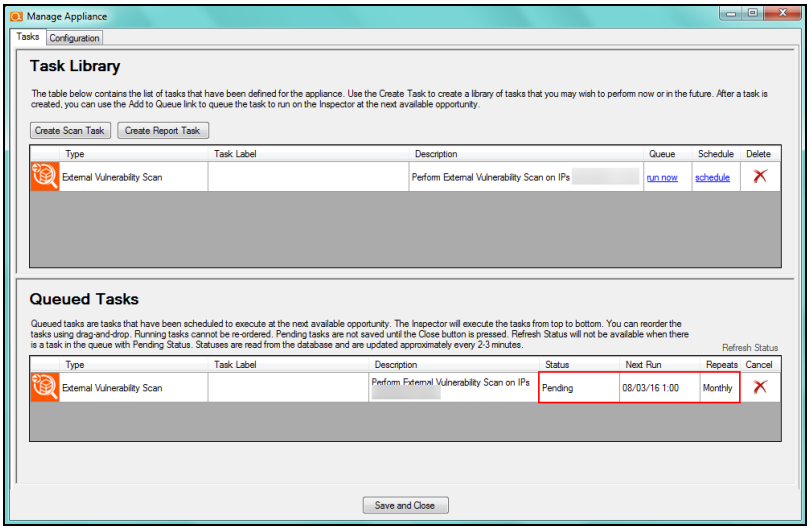


Scans can be set to run **daily**, **weekly**, **monthly**, **annually**, or **just once**. You may also set the time of the day that the scan should be initiated.

2. Set the scan frequency by selecting one option from the **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.



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

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

6. Select the **Save & Close** button in the **Manage Appliance** window to save the **Schedule settings**.

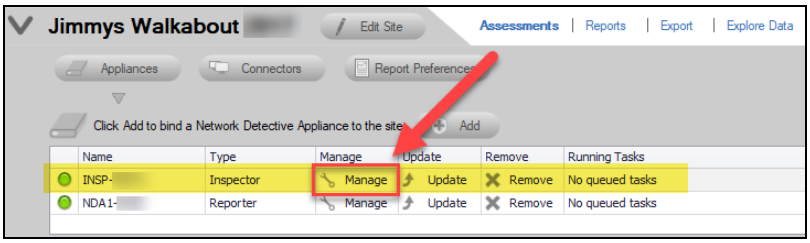
> **Note:** Please note that the time zone used for the CRON Builder time is Eastern Standard Time (EST).

Cancel a Scan

1. After starting a new assessment, or within an existing assessment, in order to "**Manage**" an **Appliance** within the Assessment Project, you must first select the  **Selector** symbol to expand the assessment properties view.

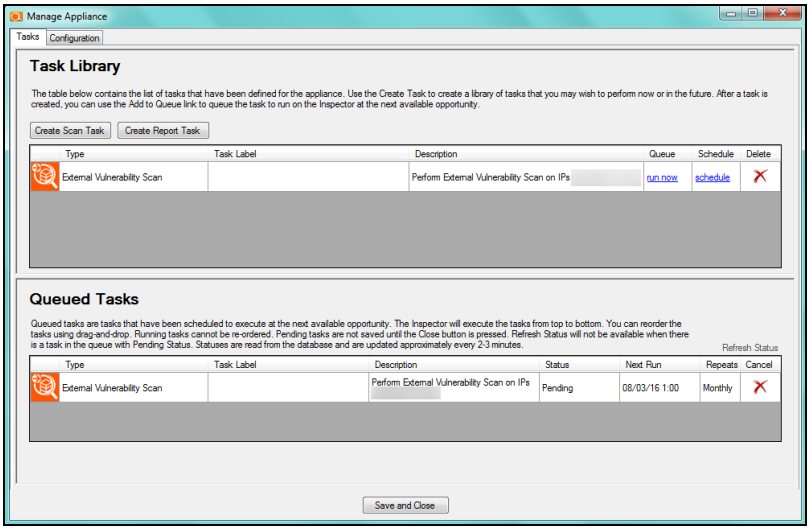
This action will expand the **Site's** properties for you to view and to add an Appliance to the **Site**.

2. Under the **Appliances** bar in the **Site's Properties** window select the **Manage** button.



This action will display the **Manage Appliance** window and present the **Task Library** and the **Queued Tasks** previously set up on the **Appliance**.

Then view the **Queued Tasks** located within the **Manage Appliance** window.



3. From **Queued Tasks**, click the **Delete** button for the Scan.

This action will only delete the Scan from the **Queue**. So, the scan will not be run until it has been re-scheduled. The Scan's configuration will still be stored in the **Task Library**.

Configuring Inspector Scans by Type/Assessment Module

In order to automate scans and reports using Inspector, you will need to configure Inspector to perform scheduled scans on the client's network. See below for specific instructions for setting up the various types of scans.

Network/Security Scan

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

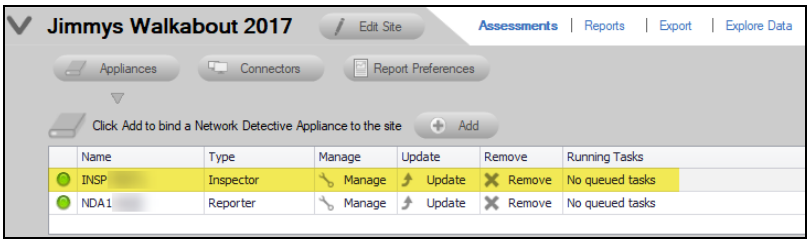
Configure the network scan using the wizard.

- Look here if you are "Scanning an Active Directory Domain Network" below
- Look here if you are "Scanning a Workgroup Network" on page 34

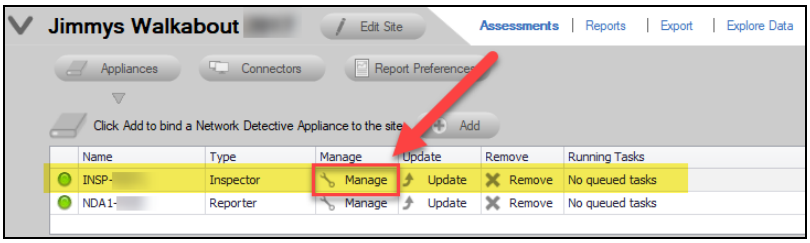
Scanning an Active Directory Domain Network

1. To view the **Inspector** associated with a **Network Detective Site**, select the  **selector** to access the **Site's** properties.

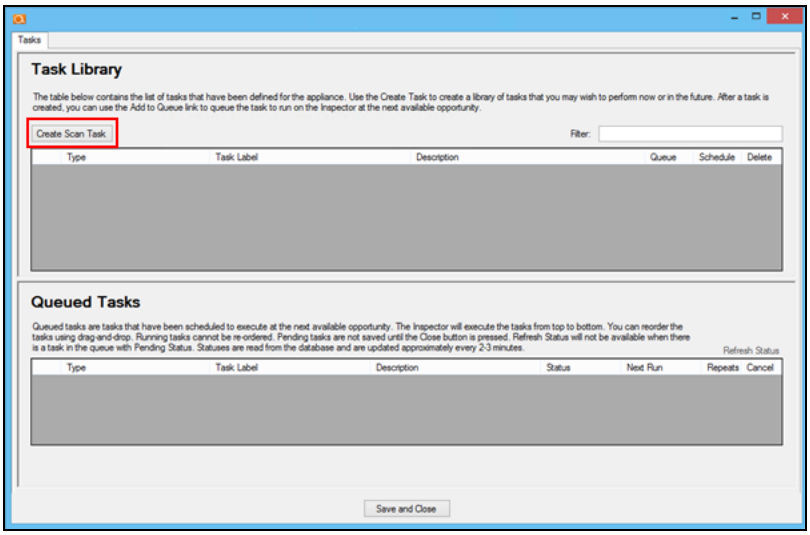
2. In the **Site** properties window, click on the **Appliances** button to view the available **Appliances**.



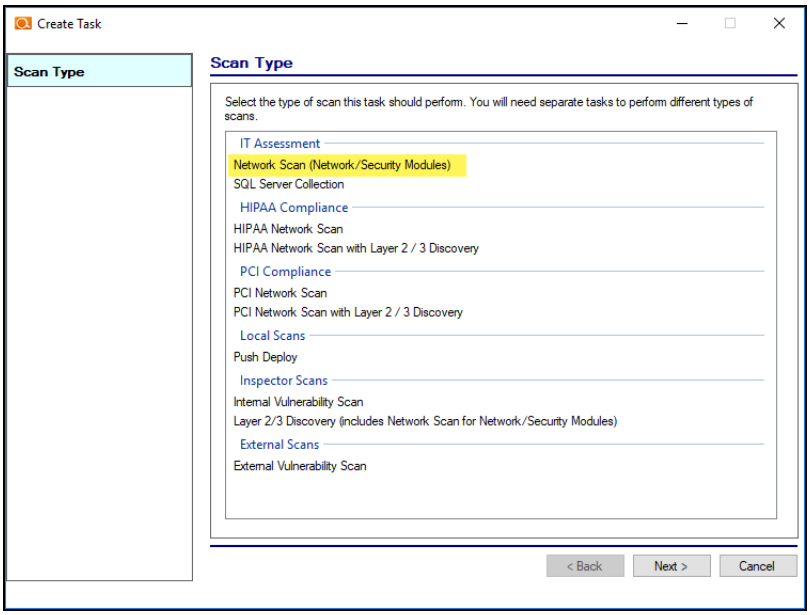
3. Any available **Inspectors** set up for use with the **Site** will appear within the **Appliances** list window.
4. Select the **Manage** button for the **Inspector** that you want to use to schedule or run a scan task.



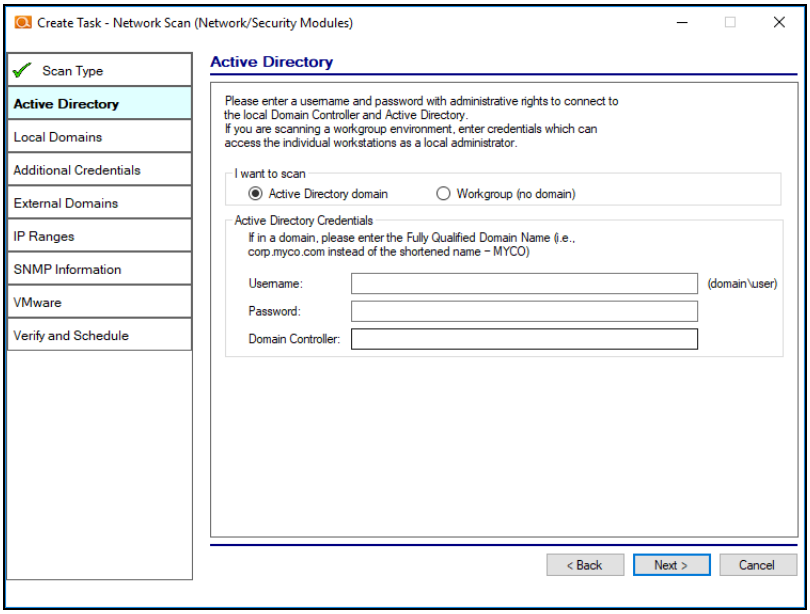
5. To create a **Scan Task**, select the **Create Scan Task** button.



6. The **Manage Appliance** window will be displayed.
7. Choose **Network Scan** option from the wizard and click the **Next** button.



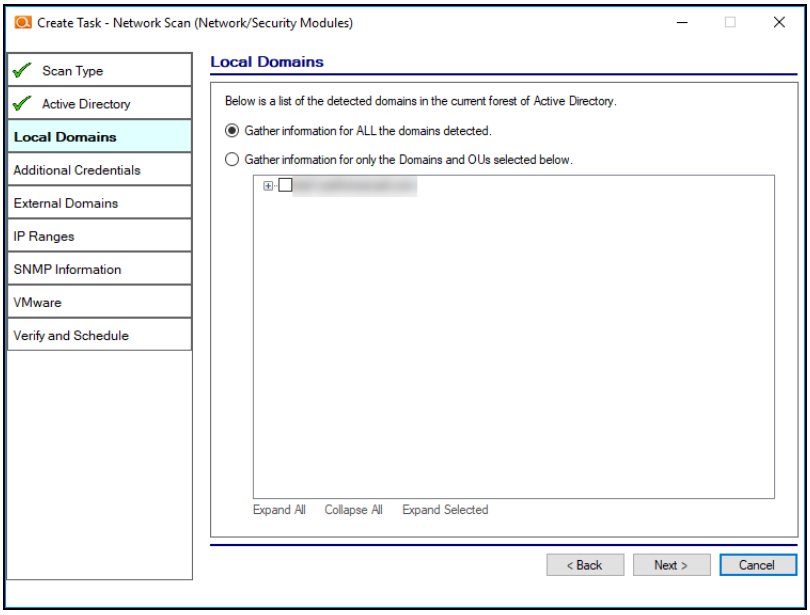
8. Select the type of network you want to scan: **Active Directory Domain**.



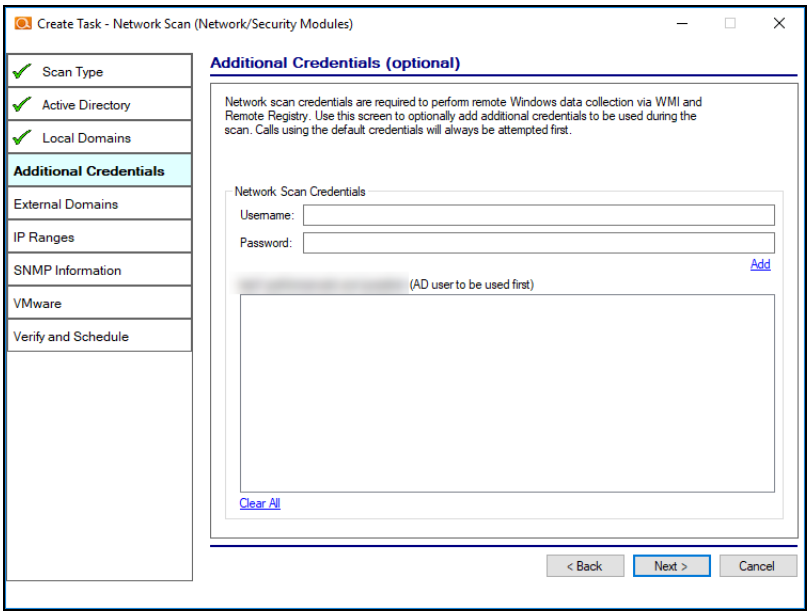
9. Next enter the network's **Fully Qualified Domain Name** along with a **username** and **password** with administrative rights to connect to the local Domain Controller and Active Directory.

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

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



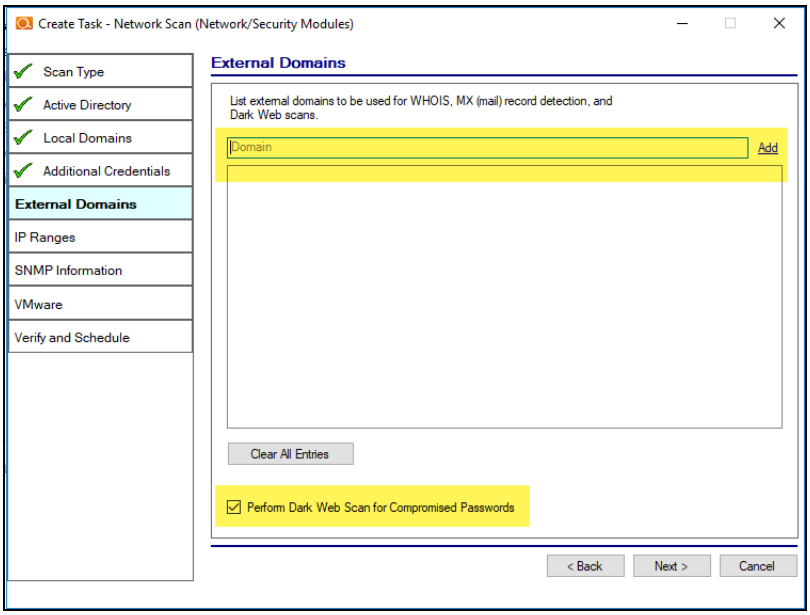
12. Enter any **Additional Credentials** necessary to access endpoints during the scan. Enter the username and password and click **Add**. When you've finished, click **Next**.



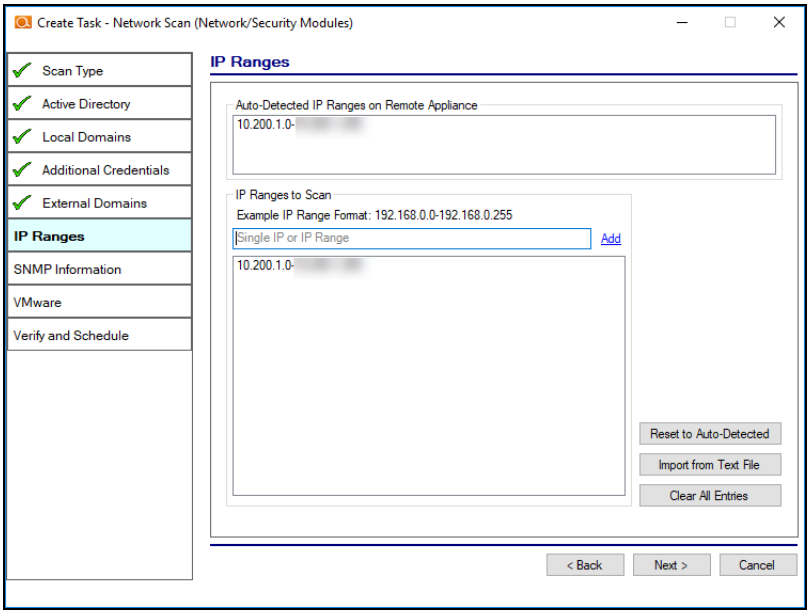
13. **External Domain** names allow others to visit the target site and facilitate services, such as email. Input the **External Domains** here to include them as part of the data collection.

    Examples of **External Domains** include:

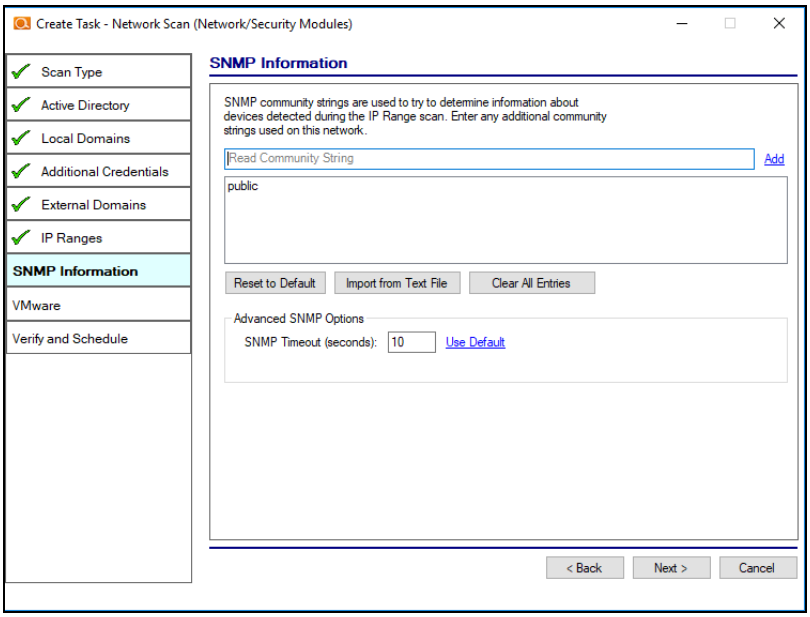
    - example.com
    - mycompany.biz



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

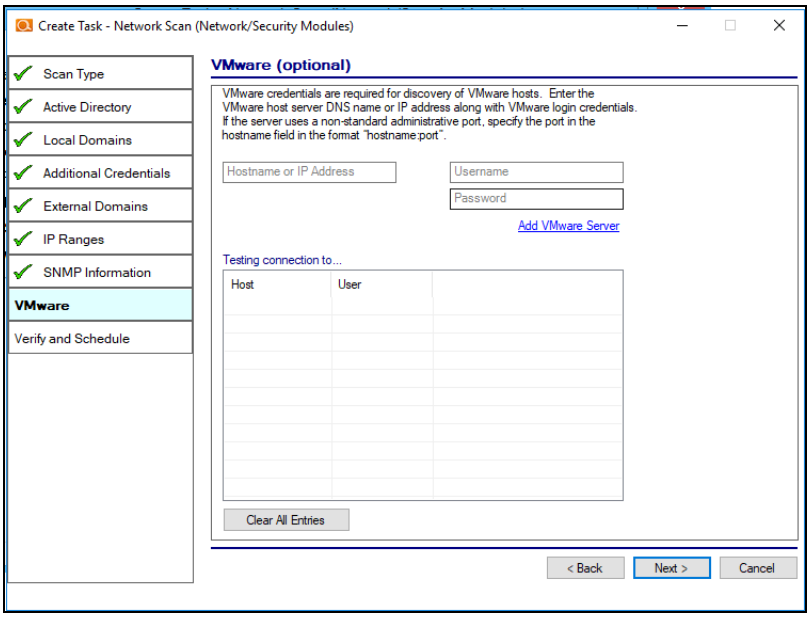


15. By default, the appliance will retrieve data from devices with the community string “public.” If desired, define an additional community string (such as “private”) and enter it here.

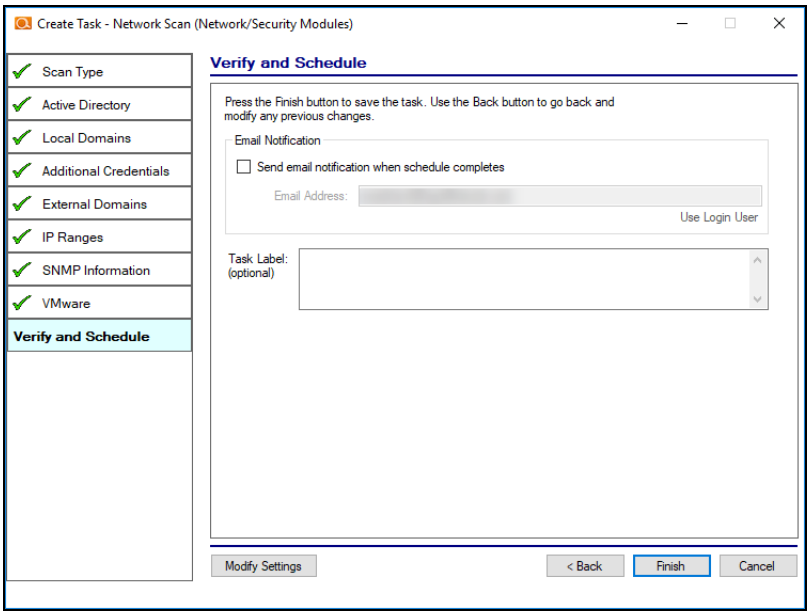


Important: As of 9/28/2018, the Microsoft Base Security Analyzer (MBSA) has been removed from the Data Collector. MBSA is in the process of being deprecated by Microsoft. Microsoft no longer supports MBSA in newer versions of Windows (i.e. v10 and Windows Server 2016). MSBA is only useful for earlier versions of Windows (Windows 7, Windows 8, 8.1, and Windows Server 2008, Windows Server 2008 R2, Windows 2012, and Windows 2012 R2). Follow the steps in this guide and **use the Push Deploy Tool as instructed**. This will collect information such as Patch Analysis for all Windows operating systems.

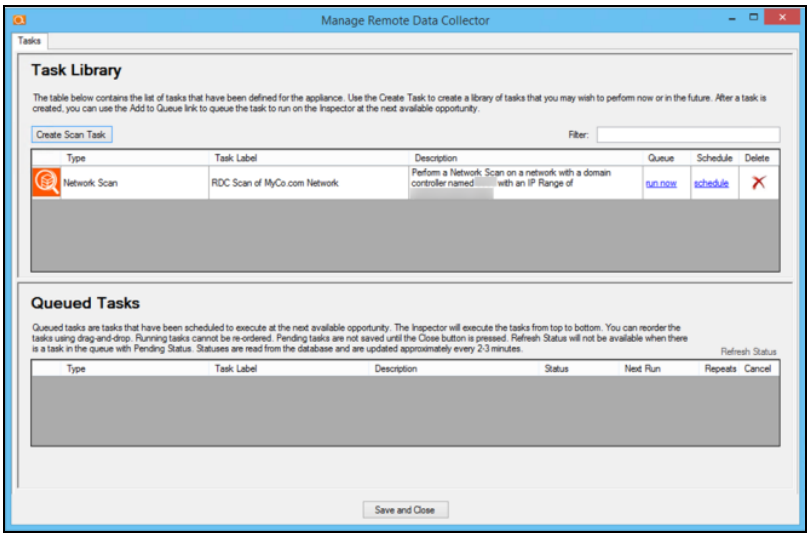
16. Input the **Hostname** or **IP Address** and **Credentials** of the VMware Servers that you would like to include in the scanning process.



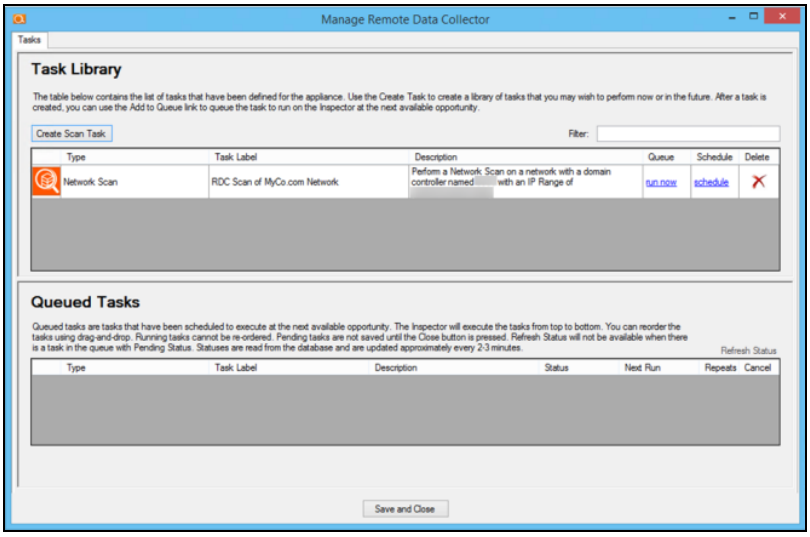
17. Check “**Send an email notification when schedule completes**" to notify an individual via email that the scan task is complete. The use of this option is recommended as the time a scan takes to complete varies depending on the target network.



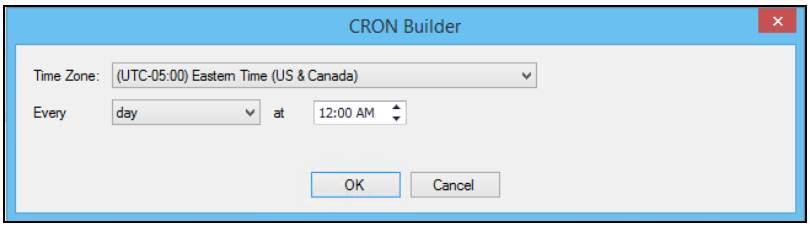
18. Click on the **Finish** button to complete the scheduling of the **Network Scan** task. The task will then be displayed in the **Appliance Tasks and Queue** window.
19. The added **Network Scan task** can be confirmed by its presence in the **Task Library** list



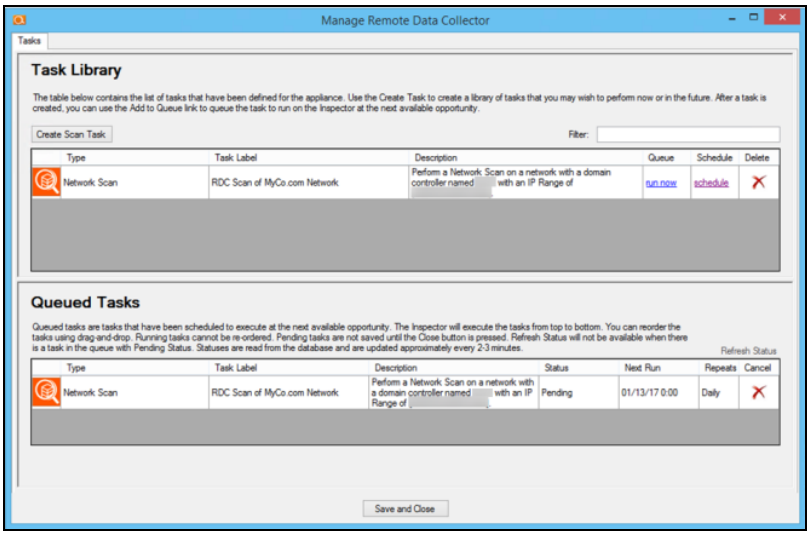
20. Upon viewing the scan task, you can click on **schedule** link to execute the scan sometime in the future by selecting the interval (daily, weekly, monthly, annually, or just once) option and the time that the scan should be scheduled to run.



21. When you click the **schedule** link, the **CRON Builder** scheduler window is displayed and is used to set the schedule action's execution time.



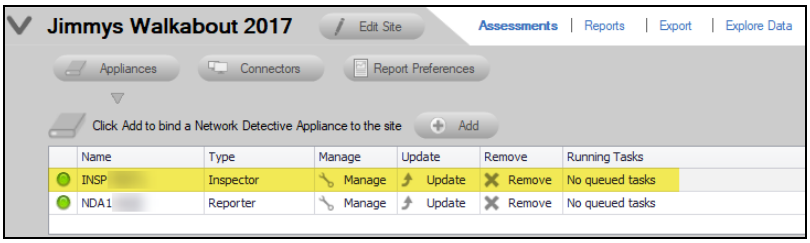
22. When scheduling the scan, set the **Time Zone**, **Frequency**, and **Time** you want the appliance to execute the scan and select the **OK** button.
23. After selecting the **OK** button in the **Cron Builder**, a **Pending** scan task will be present in the **Queued Task** list.



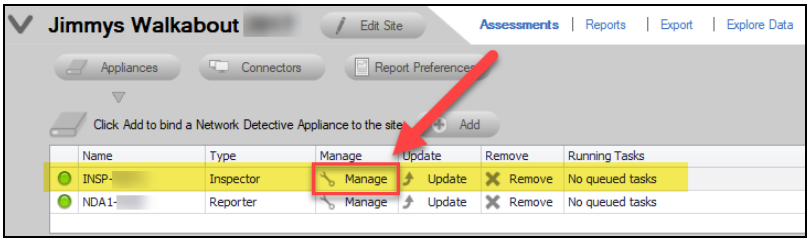
Scanning a Workgroup Network

1. To view the **Inspector** associated with a **Network Detective Site**, select the  **selector** to access the **Site's** properties.

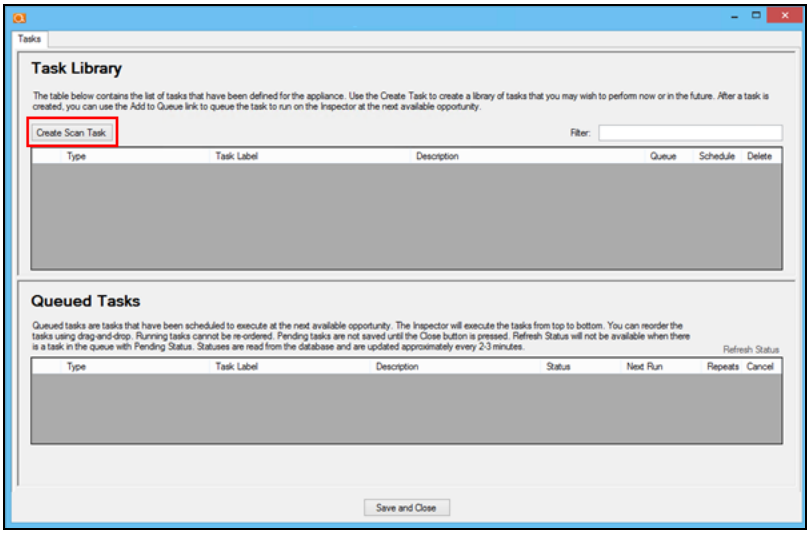
2. In the **Site** properties window, click on the **Appliances** button to view the available **Appliances**.



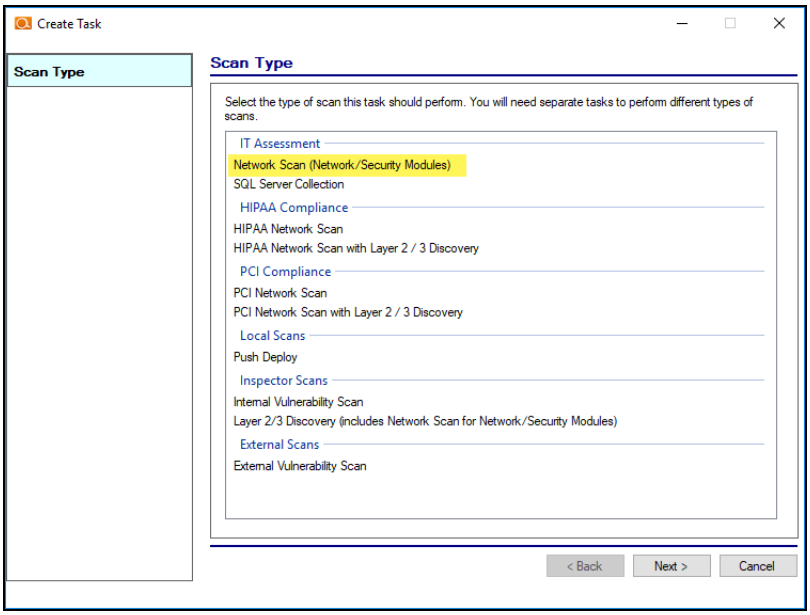
3. Any available **Inspectors** set up for use with the **Site** will appear within the **Appliances** list window.
4. Select the **Manage** button for the **Inspector** that you want to use to schedule or run a scan task.



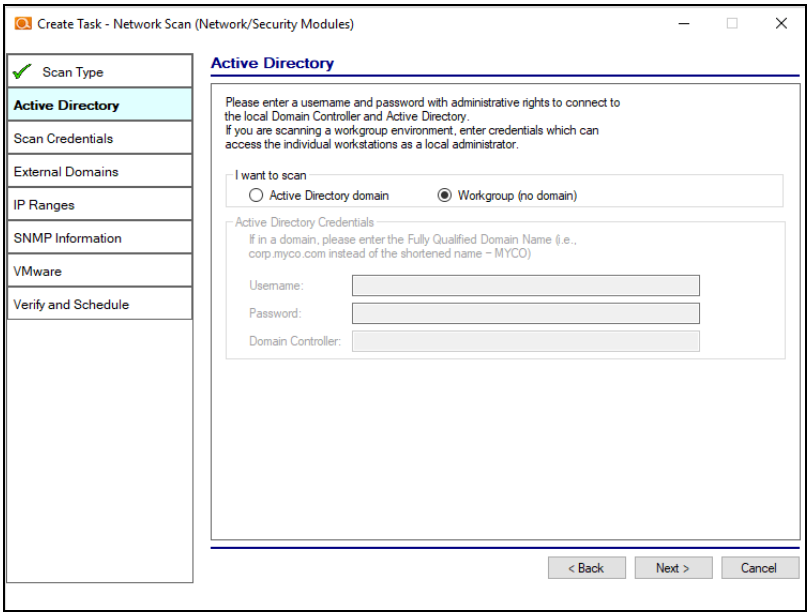
5. To create a **Scan Task**, select the **Create Scan Task** button.



6. The **Manage Appliance** window will be displayed.
7. Choose **Network Scan** option from the wizard and click the **Next** button.

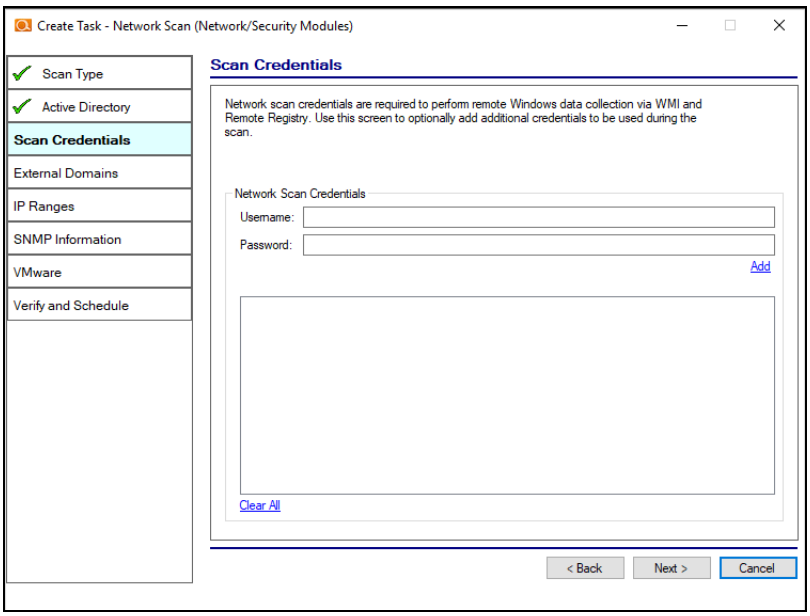


8. Select the type of network you want to scan: **Workgroup (No domain)**.

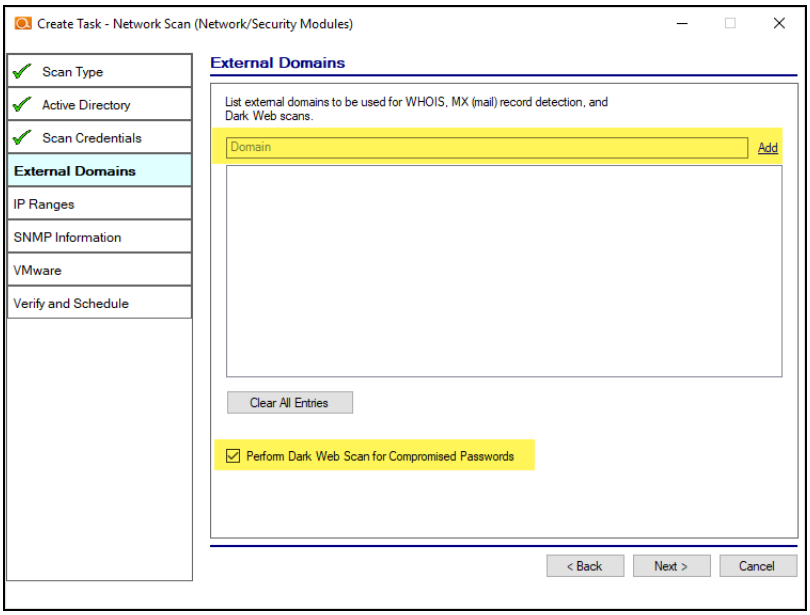


9. The **Scan Credentials** screen will appear. Enter additional credentials which can access the individual workstations as a local administrator.

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.

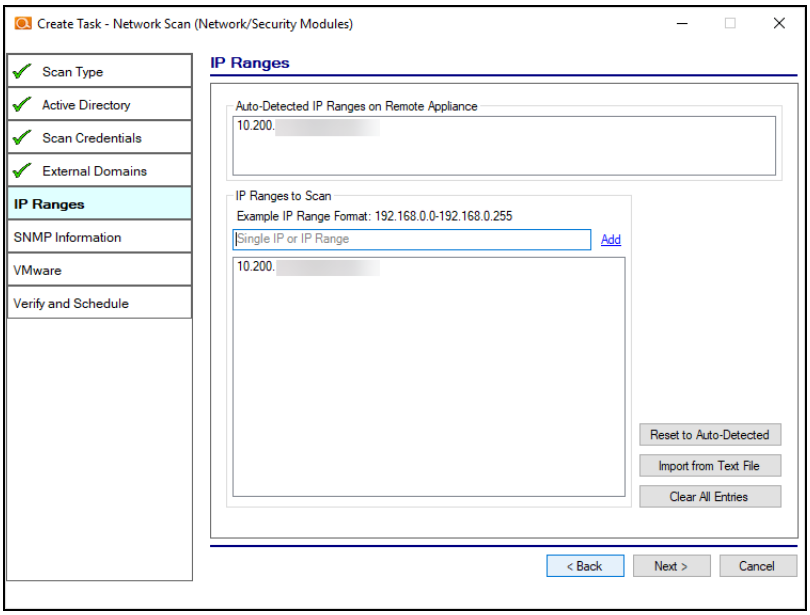


10. Input the **External Domains** here to include them as part of the data collection. **External Domain** names allow others to visit the target site and facilitate services, such as email. Examples of **External Domains** include:
    - example.com
    - mycompany.biz

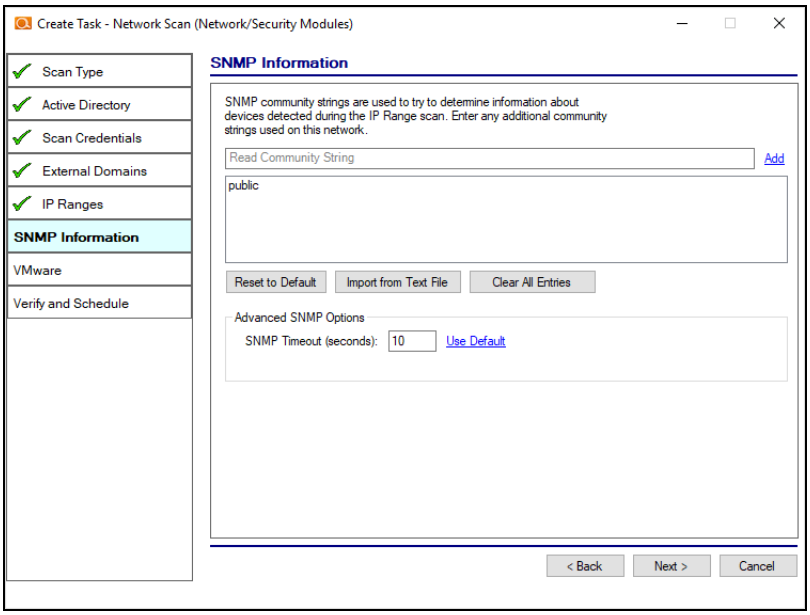


> **Note:** **Perform Dark Web Scan for Compromised Passwords**: Select this option to check the domains you enter for compromised usernames/passwords on the dark web. If any compromised credentials exist for these domains, they will appear in your Security Assessment reports. This service will return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

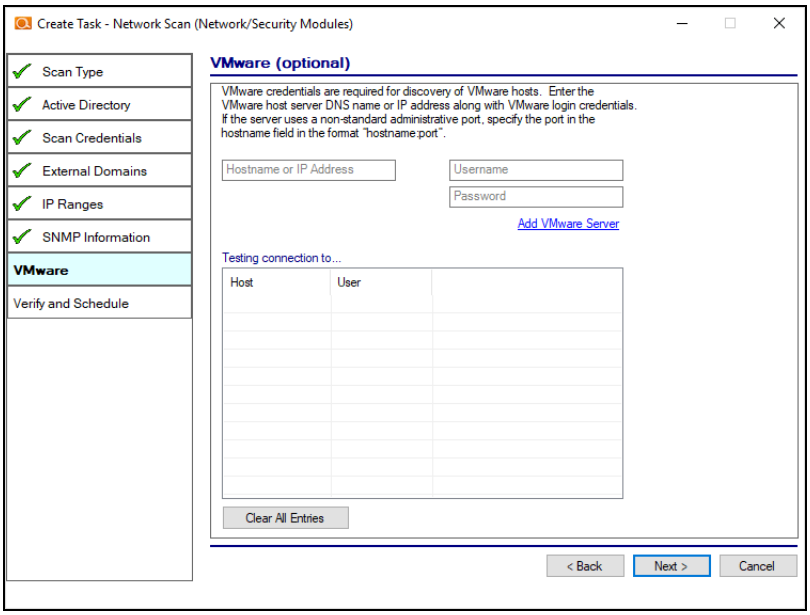
11. The **IP Ranges** from the target network will be auto-detected and included in the scan. To include additional subnets input them here.



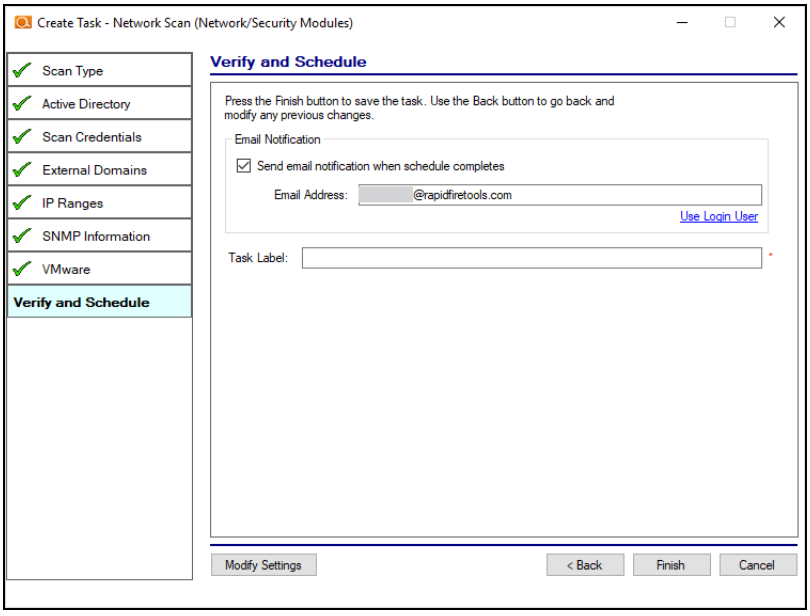
12. By default, the software will retrieve data from devices with the community string “public.” If desired, define an additional community string (such as “private”) and enter it here.



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

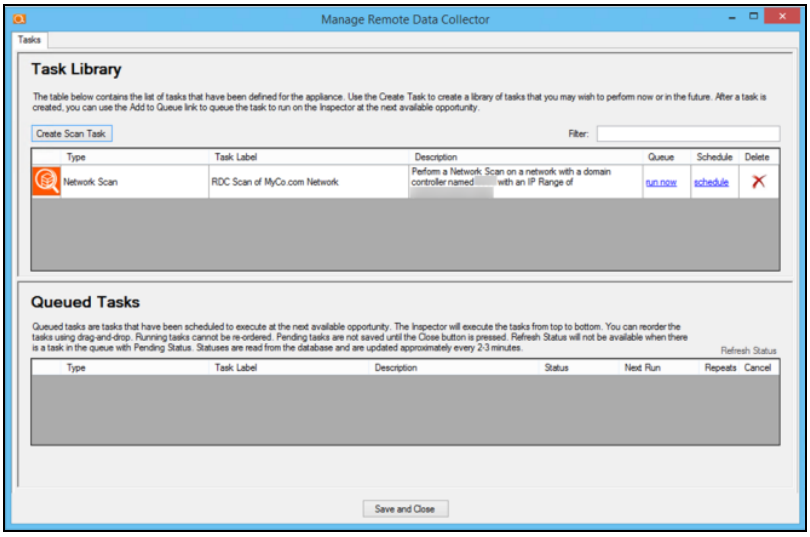


14. Check "**Send an email notification when schedule completes**" to notify an individual via email that the scan task is complete. The use of this option is recommended as the time a scan takes to complete varies depending on the target network.

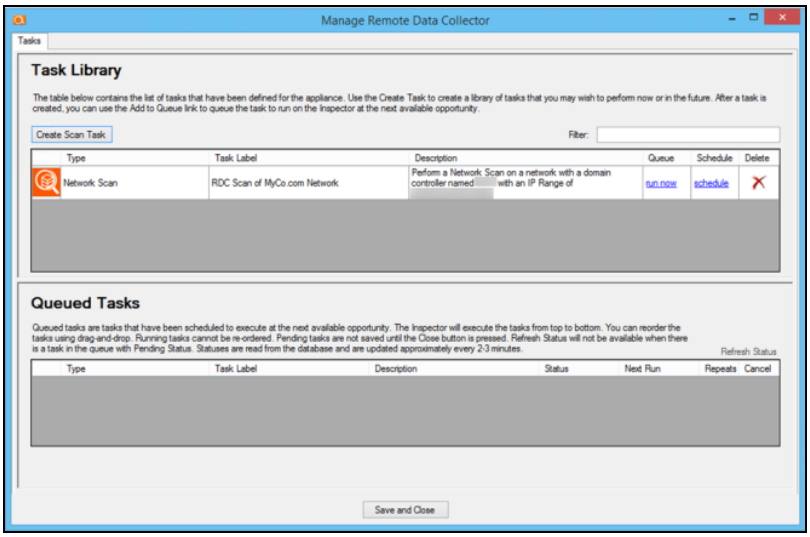


15. Click on the **Finish** button to complete the scheduling of the **Network Scan** task. The task will then be displayed in the **Appliance Tasks and Queue** window.

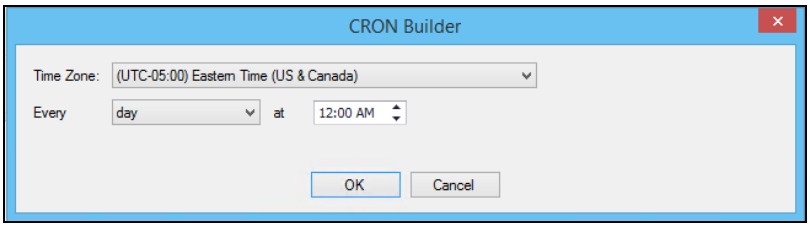
16. The added **Network Scan task** can be confirmed by its presence in the **Task Library** list



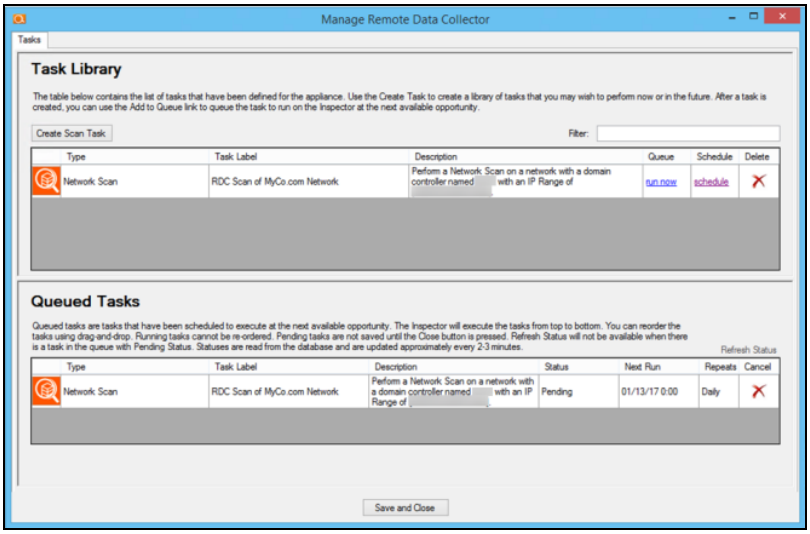
17. Upon viewing the scan task, you can click on **schedule** link to execute the scan sometime in the future by selecting the interval (daily, weekly, monthly, annually, or just once) option and the time that the scan should be scheduled to run.



18. When you click the **schedule** link, the **CRON Builder** scheduler window is displayed and is used to set the schedule action's execution time.

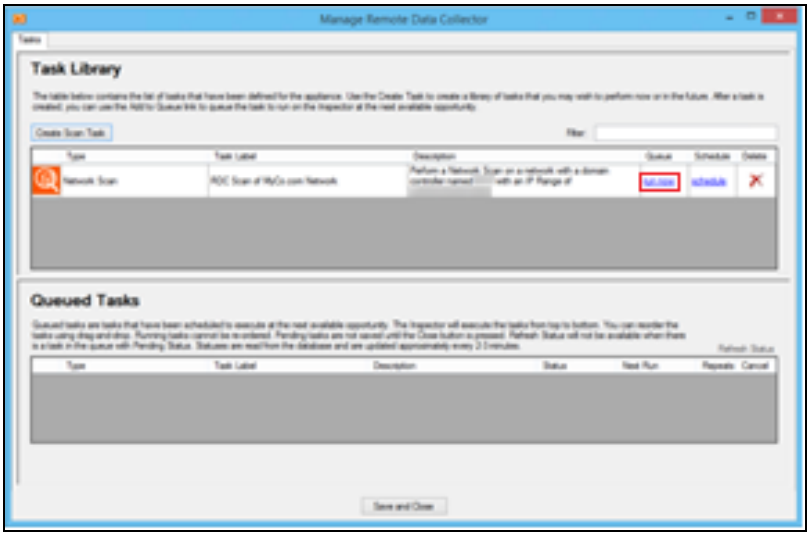


19. When scheduling the scan, set the **Time Zone**, **Frequency**, and **Time** you want the appliance to execute the scan and select the **OK** button.
20. After selecting the **OK** button in the **Cron Builder**, a **Pending** scan task will be present in the **Queued Task** list.



Using the Run Now Option

To immediately start a scan task, select the "**run now**" option link under the **Queue** column. The **run now** option will initiate the scan and place the scan task into the **Queued Tasks** list for execution.



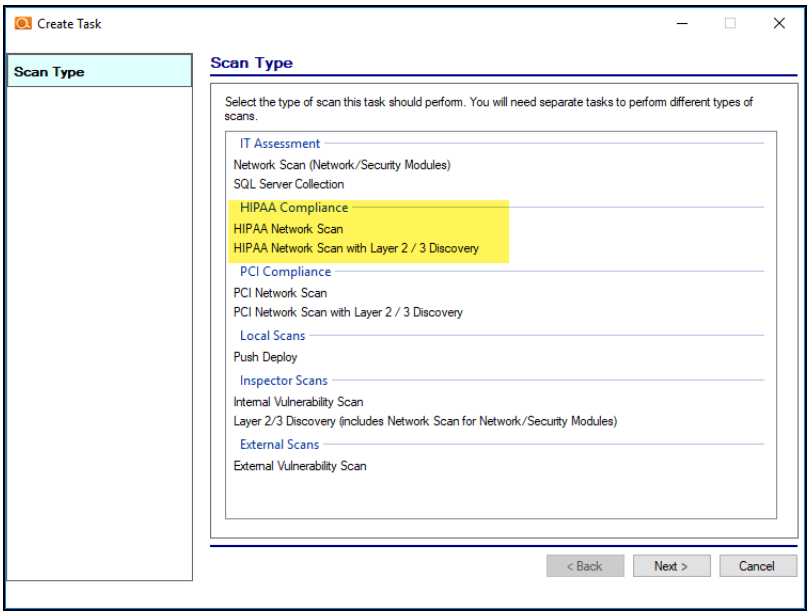
To learn more about how to configure the scans related to a Network Assessment, please refer to the **Network Detective User Guide**.

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

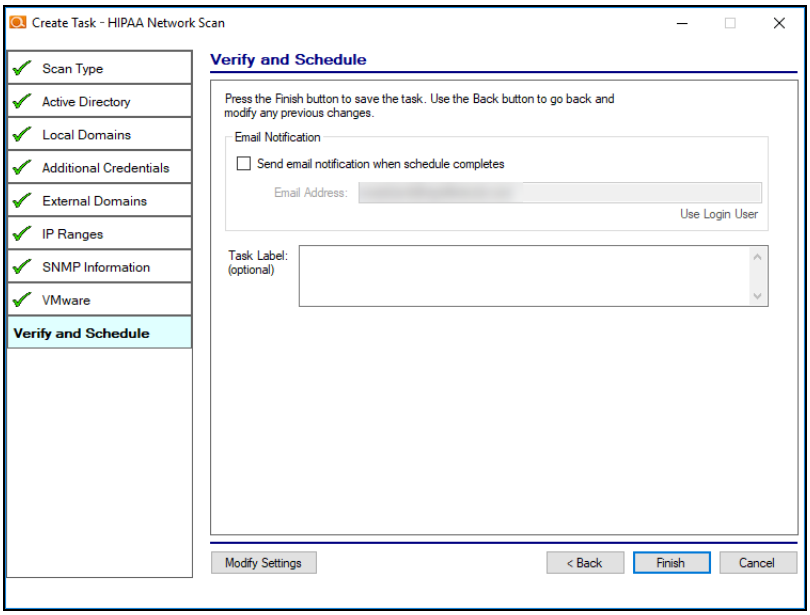
HIPAA Compliance Network Scan

To create this scan task, perform the following steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **HIPAA Network Scan** option. You can also choose HIPAA Network Scan with Layer 2/3 Discovery. Select the **Next** button.



6. 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.
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.



8. Schedule the scan listed in the **Manage Appliance** window's **Task Library**.

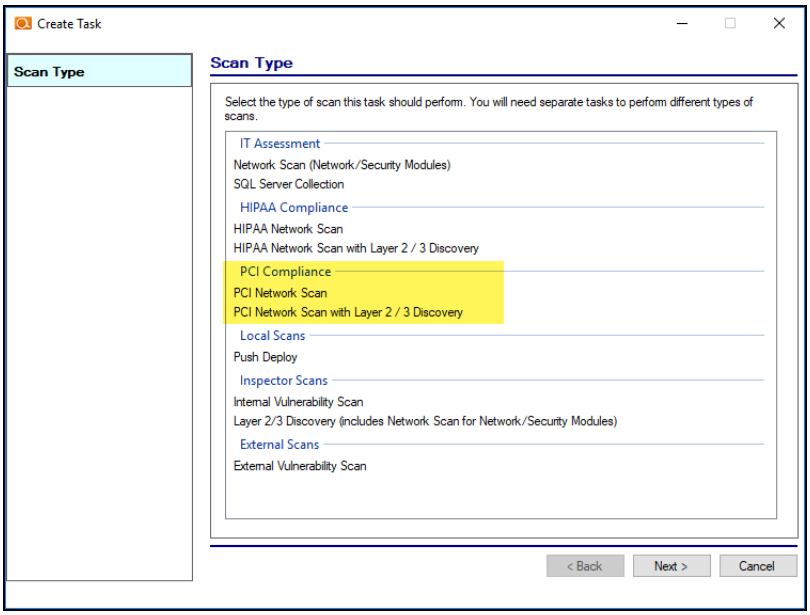
To learn more about how to configure the scans related to a HIPAA Compliance Assessment, please refer to the **HIPAA Module User Guide** at www.rapidfiretools.com/nd.

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

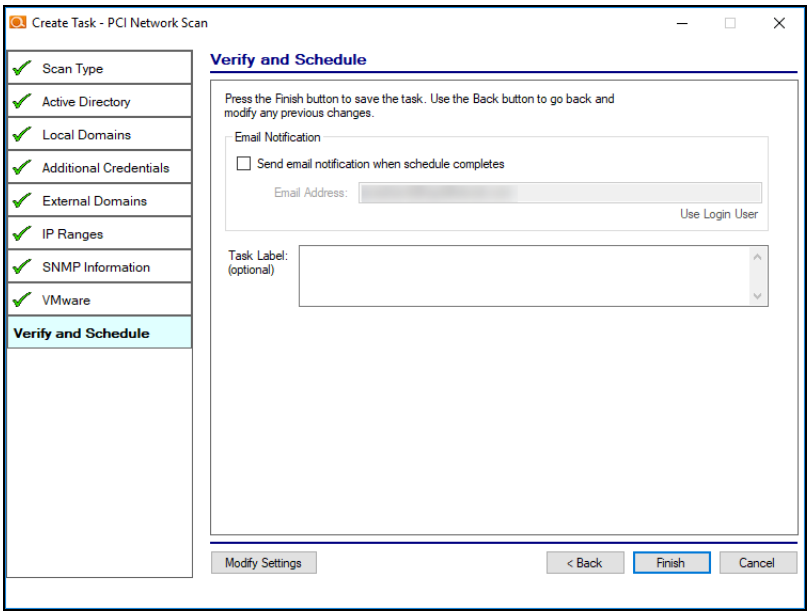
PCI Compliance Network Scan

To create this scan task, perform the following steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **PCI Network Scan** option. You can also choose PCI Network Scan with Layer 2/3 Discovery. Select the **Next** button.



6. 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.
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.



8. Schedule the scan listed in the **Manage Appliance** window's **Task Library**.

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

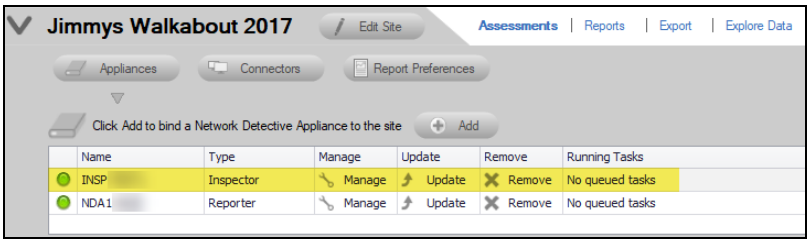
Note that the PCI Module's Assessment Reports are only available as part of the PCI Module subscription.

Push Deploy Local Computer Scan for PCI

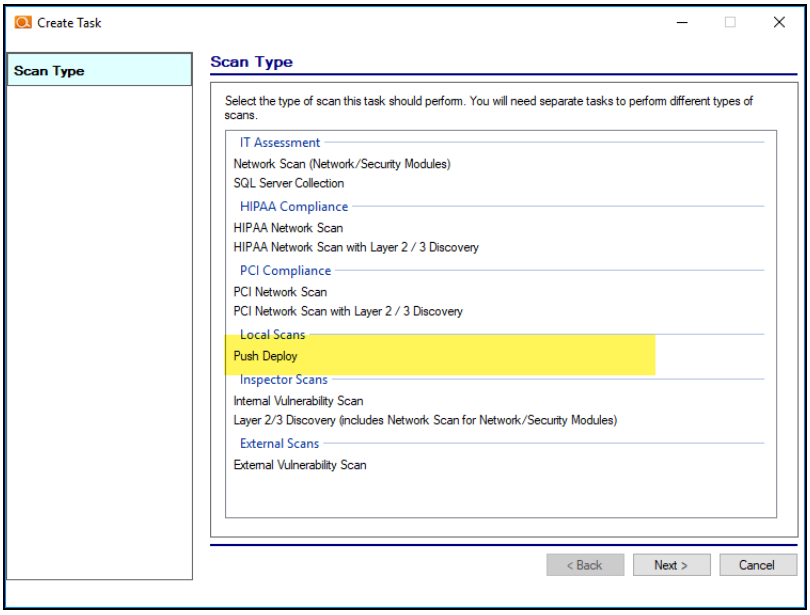
> **Note:** Use Push Deploy Local Computer Scans to gather detailed data for individual workstations. These can be used for all report types and are essential for a comprehensive assessment.

To create this scan task, perform the following steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.



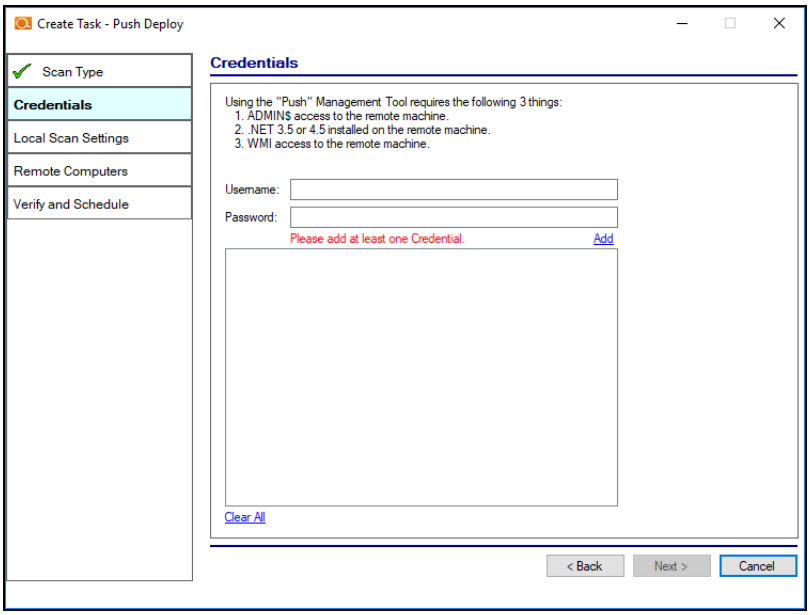
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **Push Deploy** option. Select the **Next** button.



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

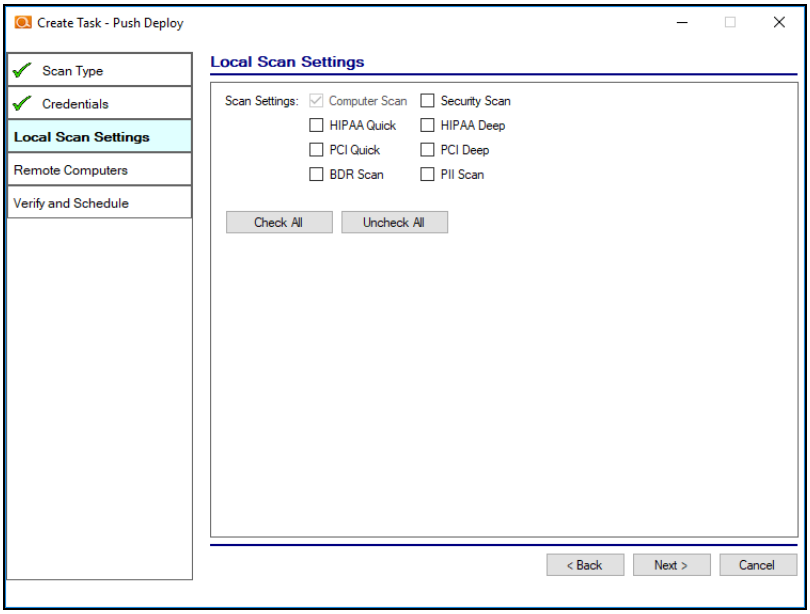
Select the **Next** button.

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



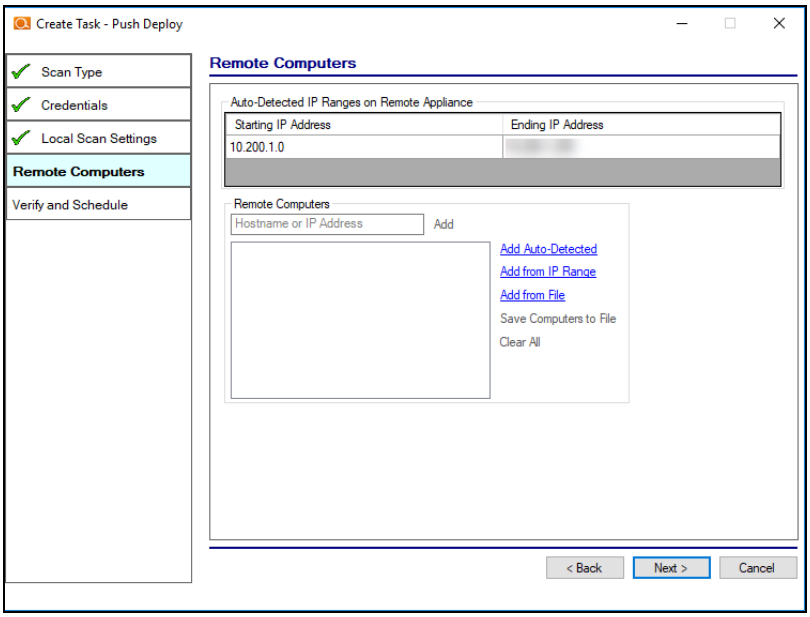
Select the **Next** button.

7. From the Local Scan Settings screen, select **PCI Deep Scan** and click **Next**.

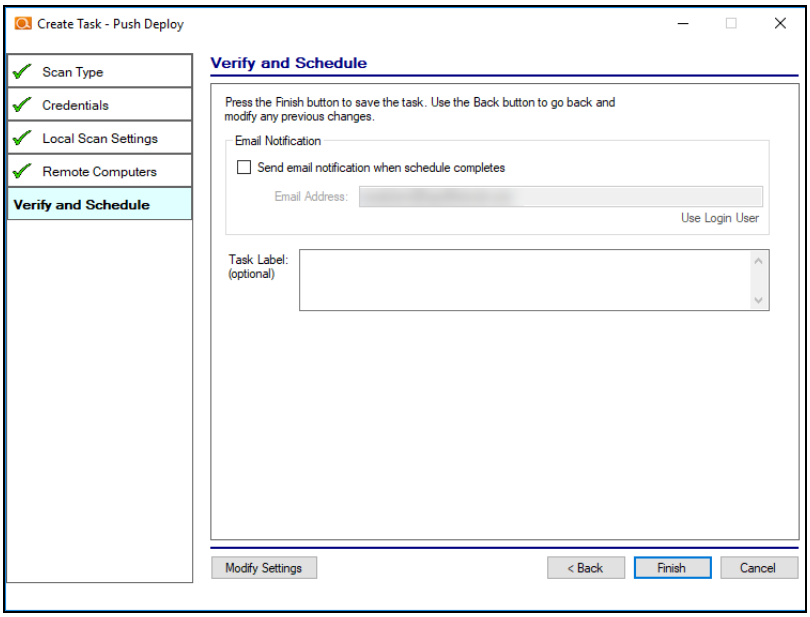


8. Define the **Remote Computer** IP addresses for the computers being scanned.

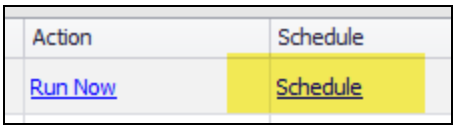
   Select the **Next** button.



9. 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.



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

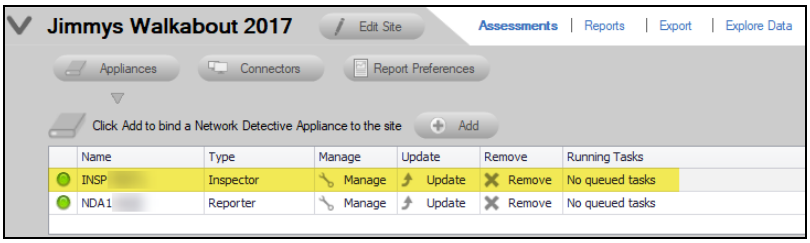


Push Deploy Local Computer Scan for HIPAA

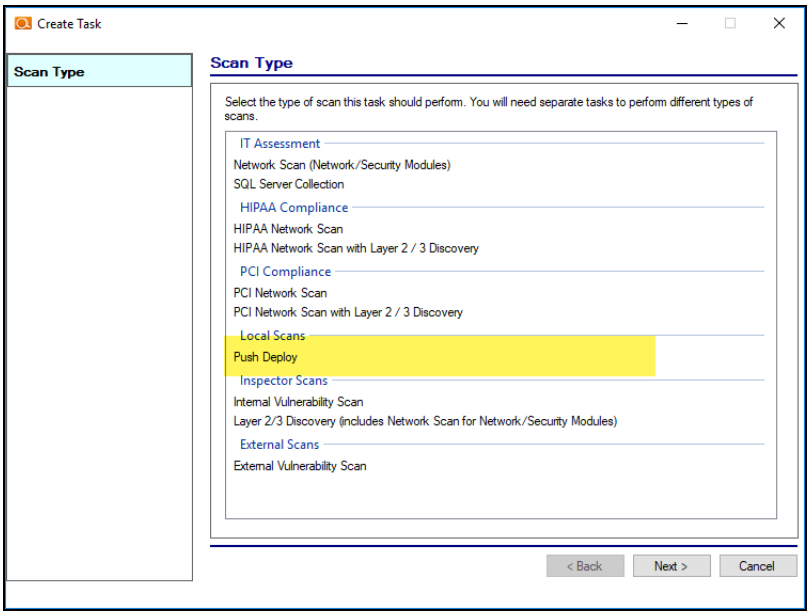
Note: Use Push Deploy Local Computer Scans to gather detailed data for individual workstations. These can be used for all report types and are essential for a comprehensive assessment.

To create this scan task, perform the following steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.



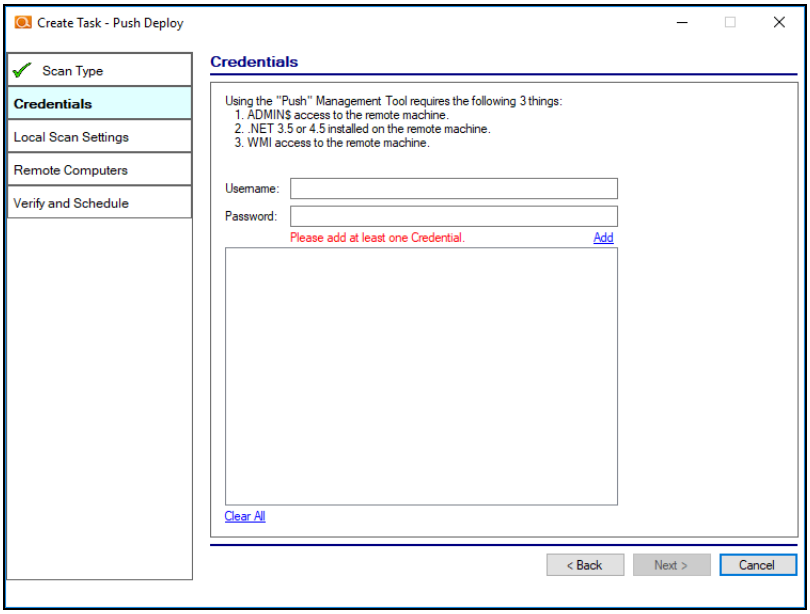
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **Push Deploy** option. Select the **Next** button.



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

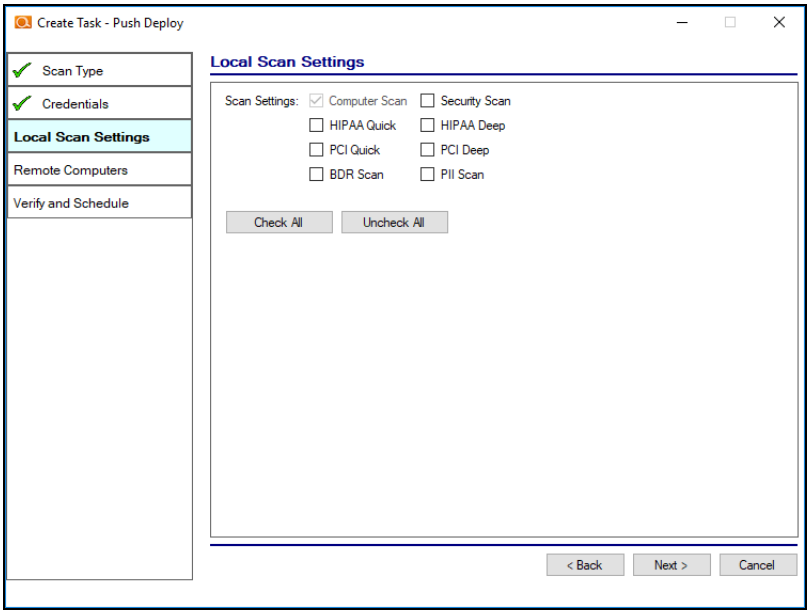
Select the **Next** button.

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



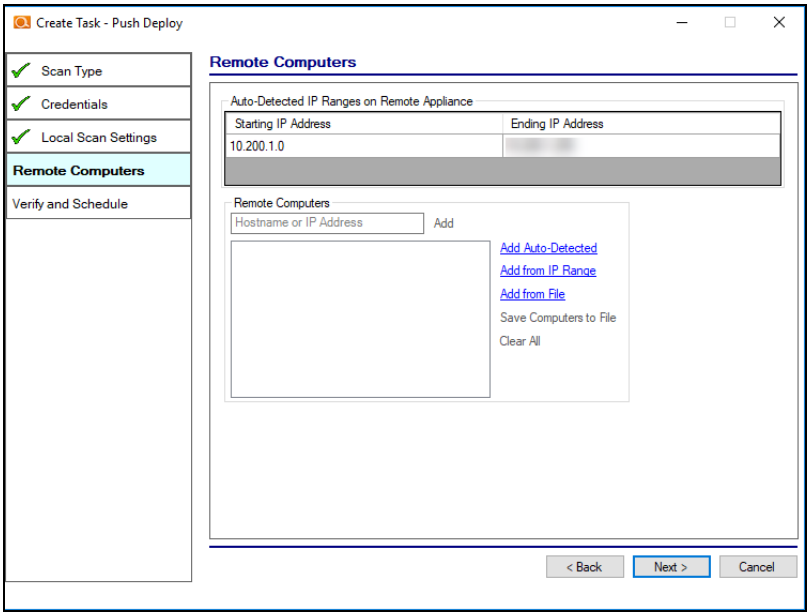
Select the **Next** button.

7. From the Local Scan Settings screen, select **HIPAA Deep Scan** and click **Next**.

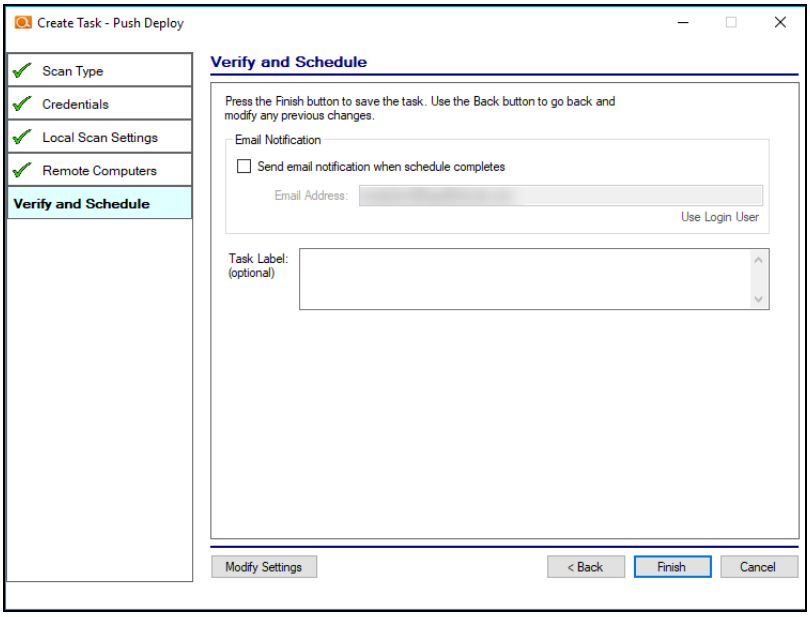


8. Define the **Remote Computer** IP addresses for the computers being scanned.

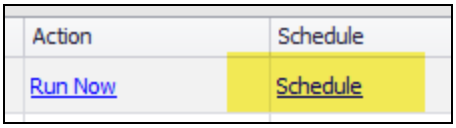
   Select the **Next** button.



9. 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.



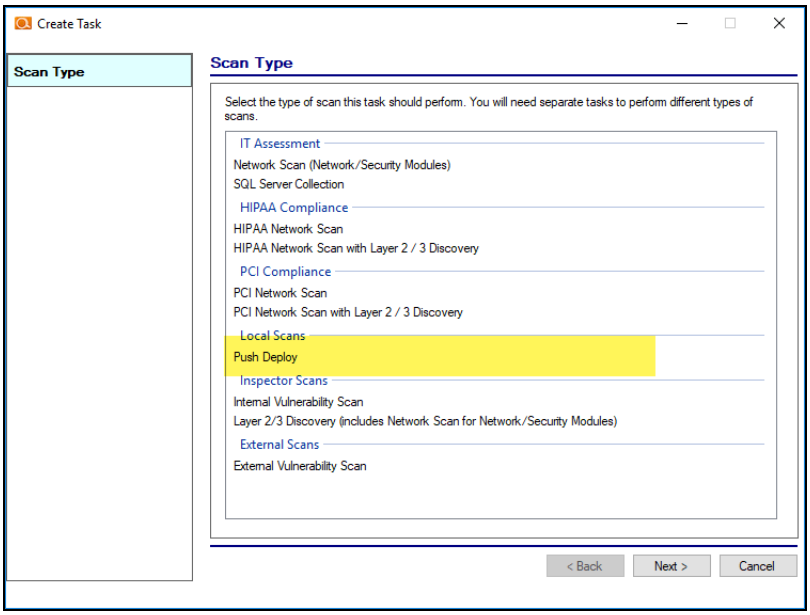
10. **Schedule** the scan from the Task window. *Be sure to schedule the scan a few hours before your report jobs.*



Push Deploy (All Modules)

To create a Push Deploy scan task for any assessment module, follow these general steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **Push Deploy** option. Select the **Next** button.

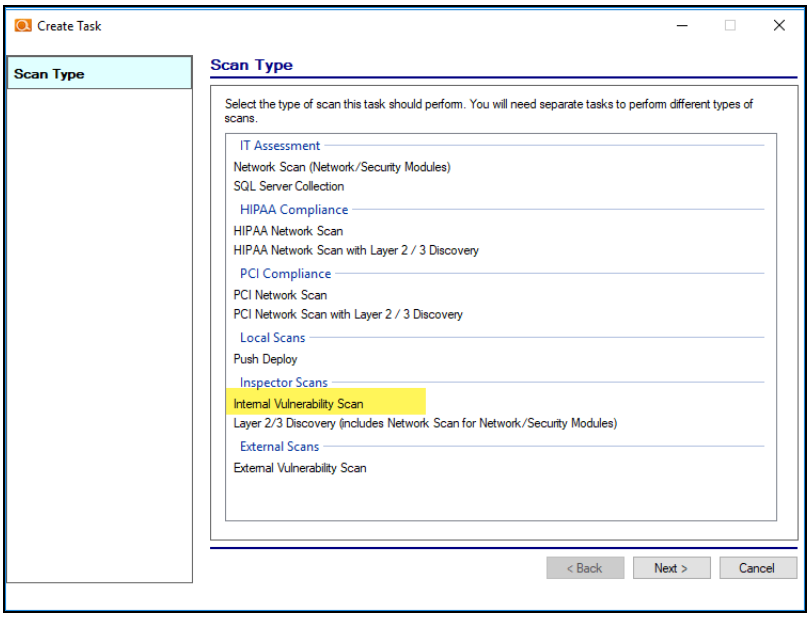


6. Verify the settings, set-up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.
7. Schedule the scan listed in the **Manage Appliance** window's **Task Library**.

Internal Vulnerability Scan

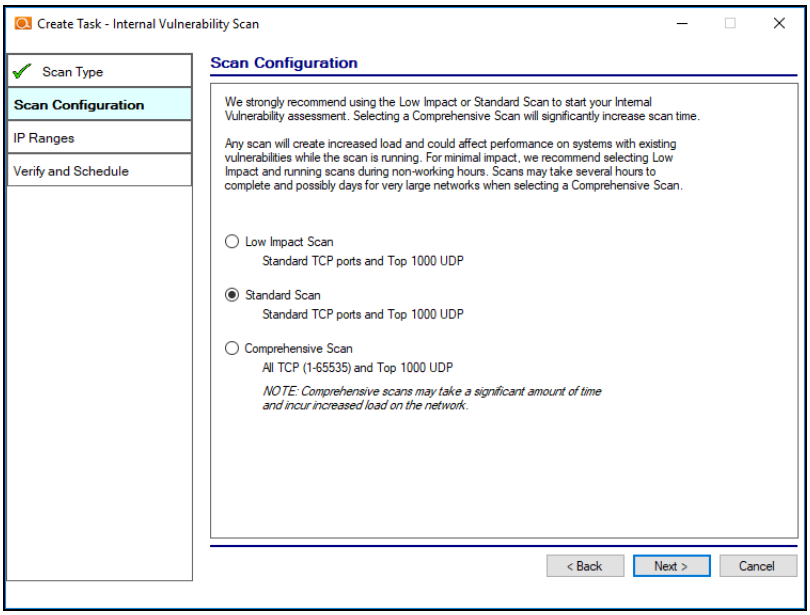
To create this scan task, perform the following steps:

1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **Internal Vulnerability Scan** option. Select the **Next** button.



6. Follow the prompts to set-up the Internal Vulnerability Scan. Select the **Next** button.

> **Note:** The **Low Impact Scan** is the same as the standard scan, but does not include *brute force* and *default password* checks. Use this option if you are having trouble with the Standard scan on your network, such as users being locked out of their accounts.



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.
8. Schedule the scan listed in the **Manage Appliance** window's **Task Library**.

> **Important:** We recommended you review the "Tips for Scheduling the Level 2 Scan" below below to avoid affecting network performance.

Tips for Scheduling the Level 2 Scan

Inspector's Level 2 Scan (Weekly) functionality relies on the use of an Internal Network Vulnerability scanner process to perform this scan. Internal Network Vulnerability scans are intentionally designed to be aggressive and comprehensive in nature. At Internal Network Vulnerability scan run time, there are instances where these scans can impact network performance and access to computer endpoints by network users during the time a scheduled Internal Network Vulnerability scan is being performed.

It is recommended that:

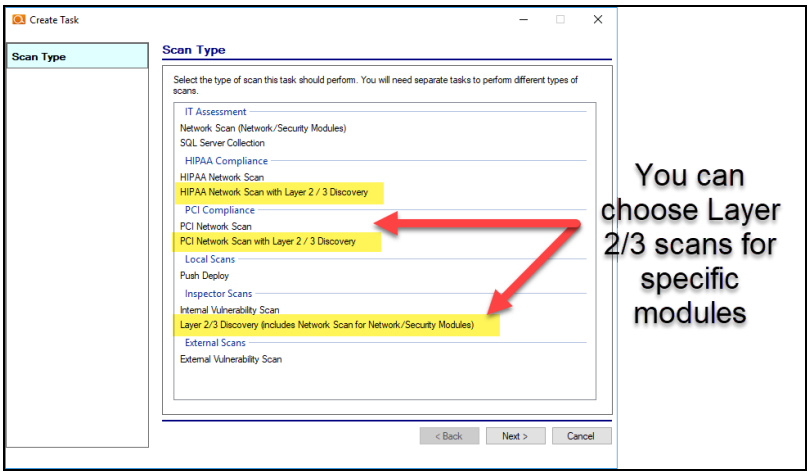
- Level 2 scans are scheduled and performed at times when the network is not in use by network users, back-up processes, or any other system or process that requirements unimpeded network access.

- any routers, switches, computers, industrial devices connected to the network, security devices, and other network devices that should not be interfered with in any way during day to day network operation or must be operational and accessible to network systems and users on a 24x7x365 basis, that these IP addresses of the aforementioned devices should be excluded from the Inspector's IP Range settings contained within the Inspector's Scan Settings.

Layer 2/3 Discovery Scan

To create this scan task, perform the following steps:

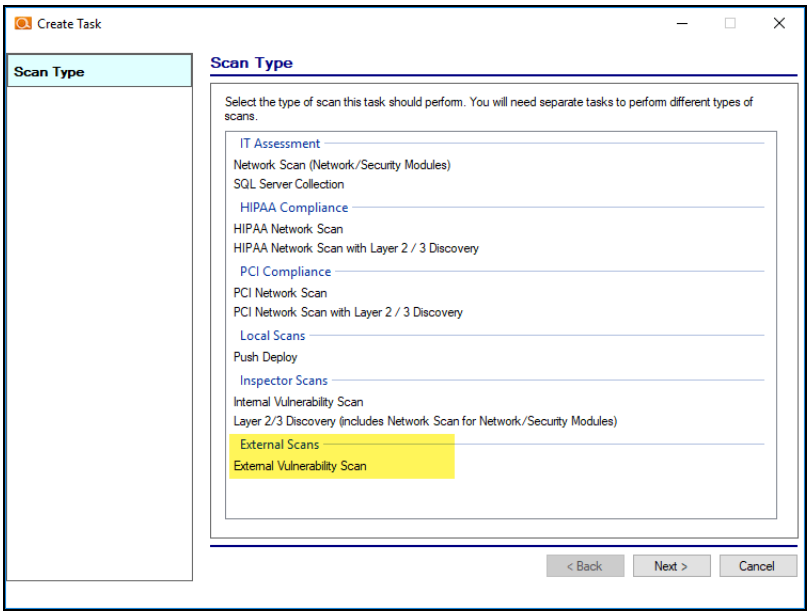
1. Select the **Site Preferences**.
2. Click on the **Appliances** button.
3. Select the Appliance's **Manage** option to display the **Manage Appliance** window.
4. Click on the **Create Task** button in the **Manage Appliance** window to display the **Create Task** window.
5. Select the **Layer 2/3** option. Select the **Next** button.



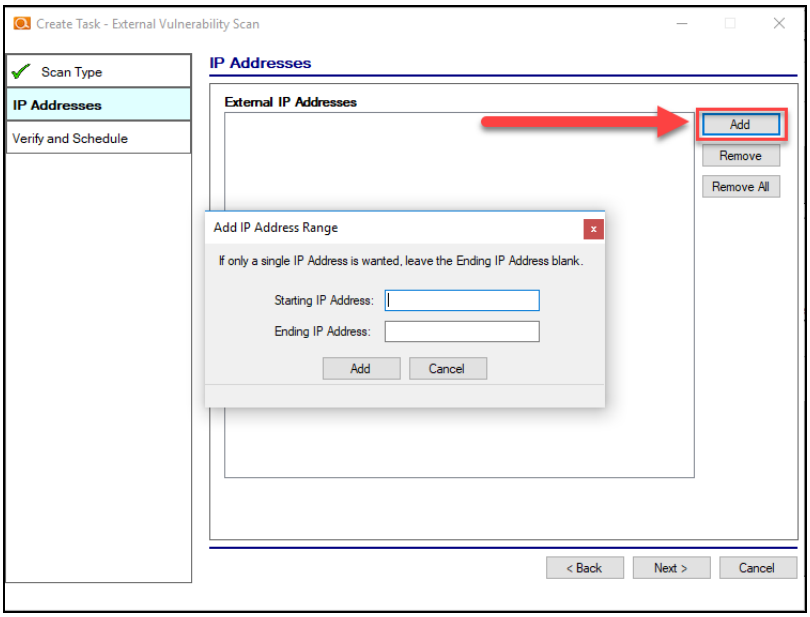
6. Follow the prompts to set-up the Push Deploy scan. Select the **Next** button.
7. Verify the settings, set-up an Email Notification to be sent once the scan is completed, and select the **Finish** button to create the scan task.
8. Schedule the scan listed in the **Manage Appliance** window's **Task Library**.

External Vulnerability Scan

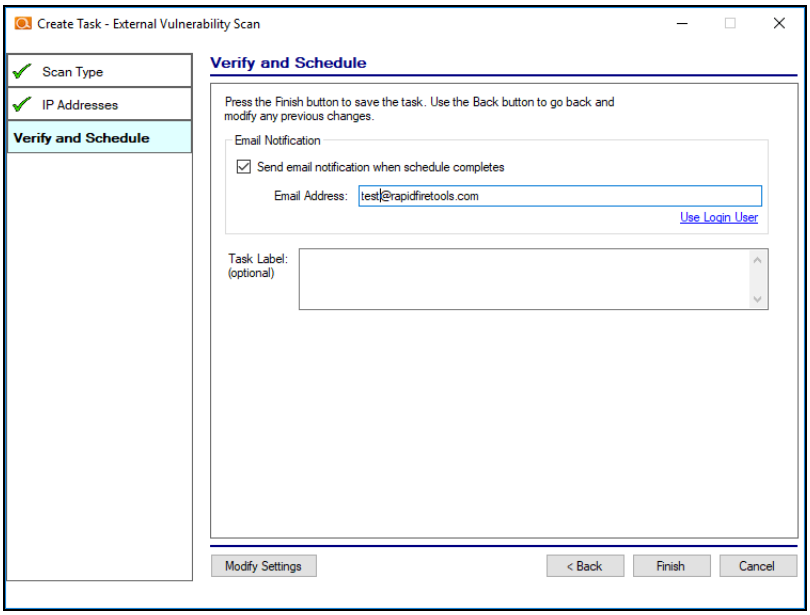
1. Choose **External Vulnerability scan** from the wizard and click the **Next** button.



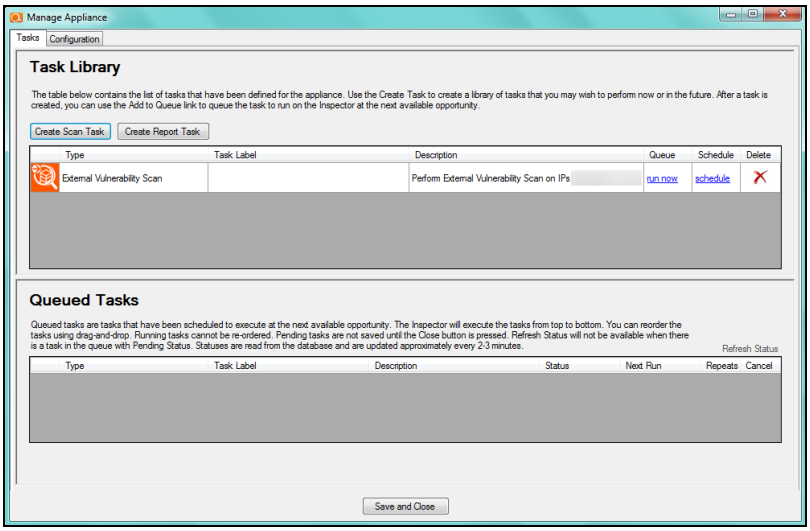
2. Select the **Add** button in the **Create Task – External Vulnerability Scan** window to add the IP address range to be scanned.



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**
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.



Proceed to the next step to **Schedule** the automated running of the scan.

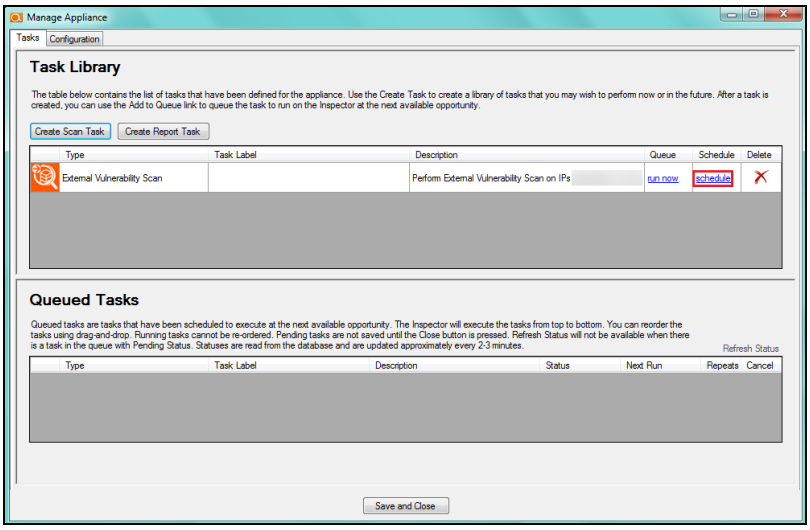
Upon viewing the scan task, you can select the **Run Now** option link under the **Queue** column to initiate the scan. Selecting **Run Now** will place the scan into the **Queued Tasks** list.

> **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.

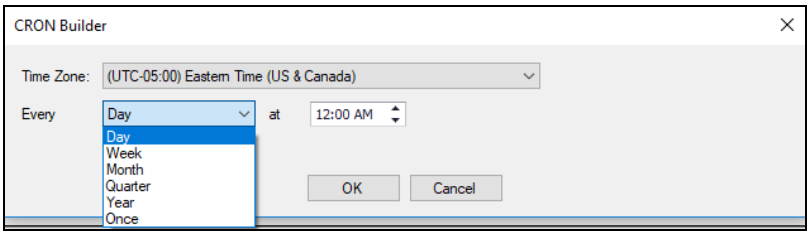
Schedule the Running of the External Vulnerability Scan

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

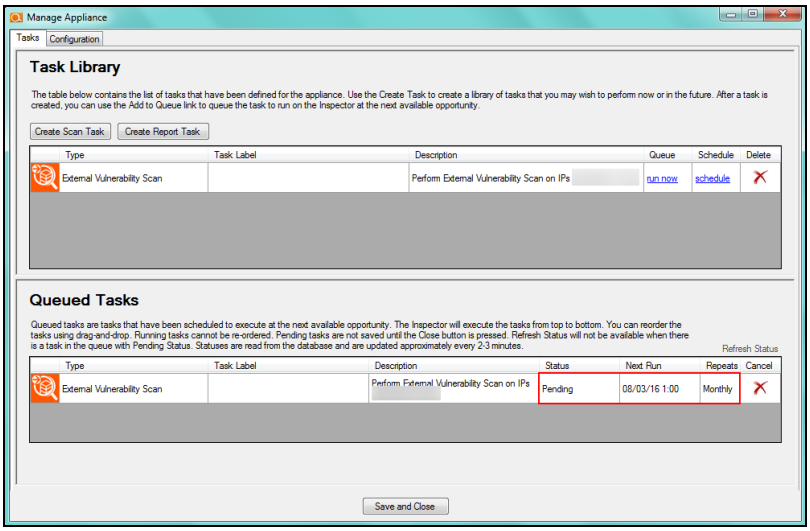
1. Click on **Schedule** link to open the **CRON Builder** window. The **CRON Builder** is used to schedule the running of scans.



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



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.



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

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

6. Select the **Save & Close** button in the **Manage Appliance** window to save the **Schedule settings**.

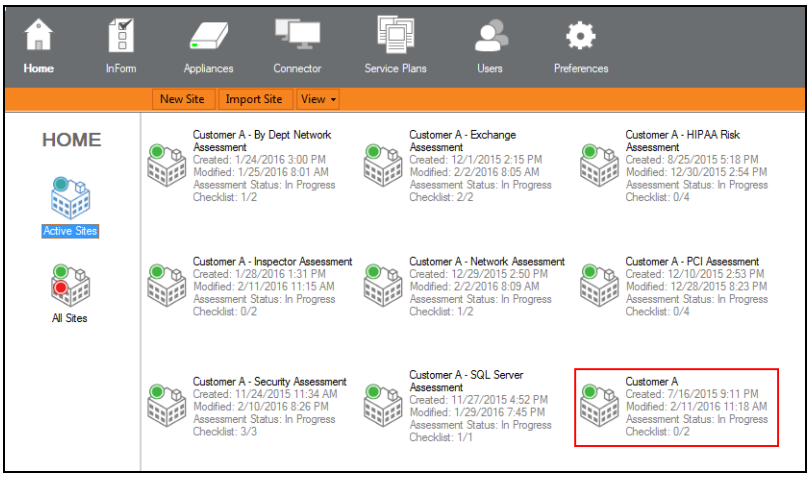
> **Note:** Please note that the time zone used for the CRON Builder time is Eastern Standard Time (EST).

Configuring the Local Data Scan Merges

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

This setting will impact Automated Report Generation.

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



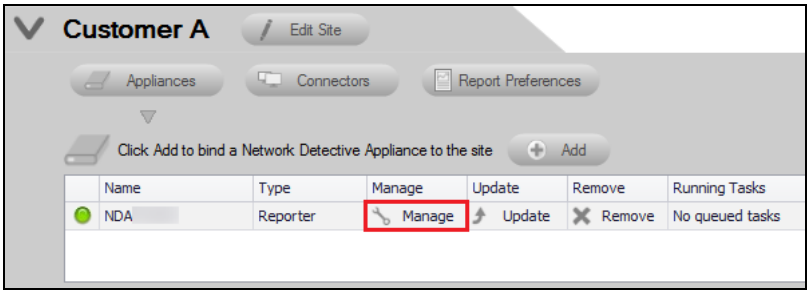
Step 1 — Select and Open the Site

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

Step 2 — Select Manage Appliance

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

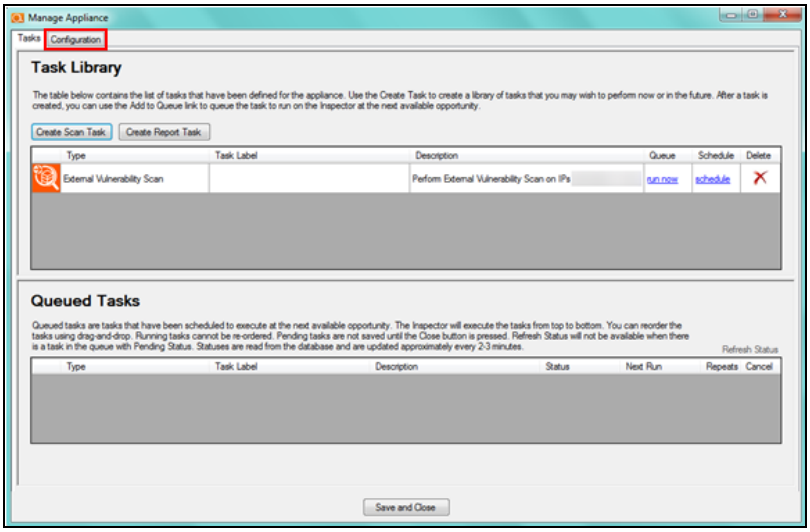
Then select the **Manage** option presented for the **Appliance** listed.



The Manage Inspector window will be displayed.

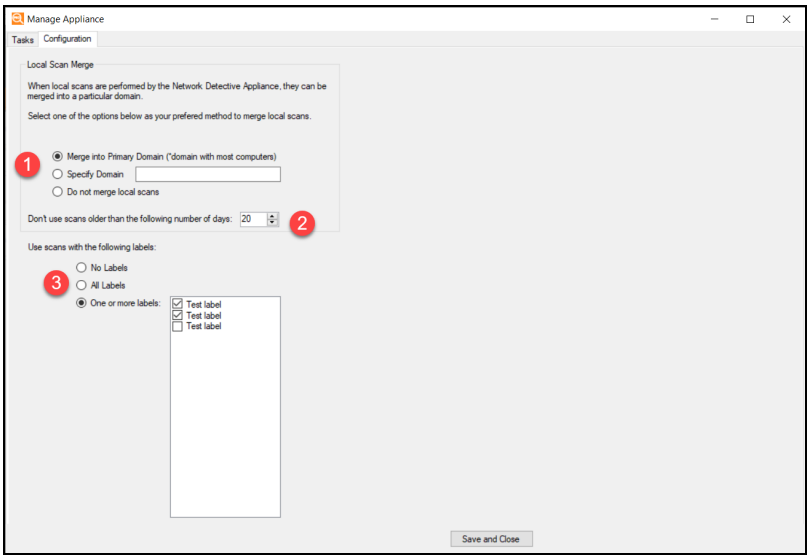
Step 3 — Set Scan Data Merge Configuration

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



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

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

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

Setting Up Automatic Reports with Inspector

This section covers everything you need to know about setting up automatic reports with Inspector.

Network Assessments Automatic Reports

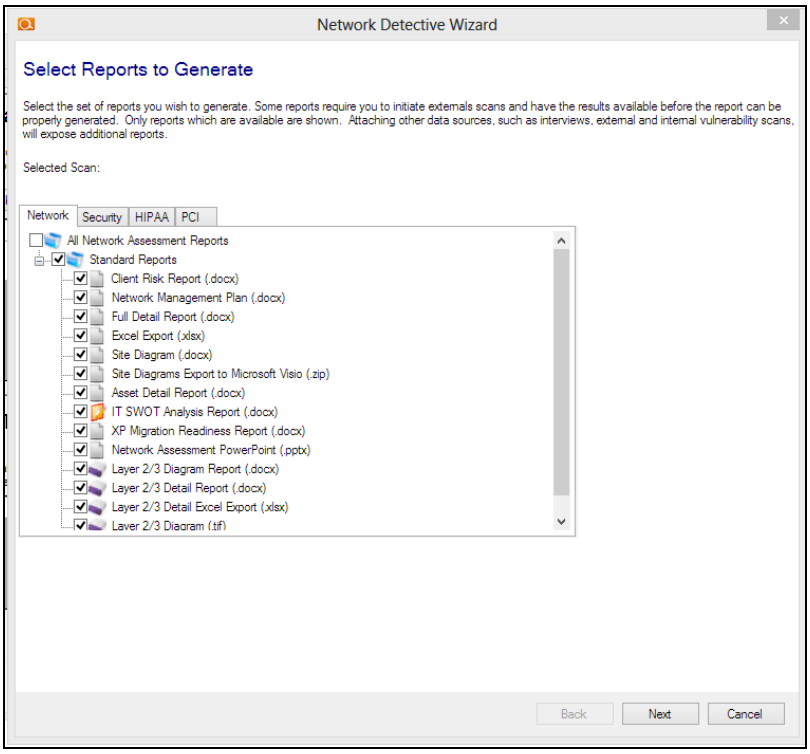
Automatic report generation for the Network Assessment Module requires that the scans be run by the Inspector before a report can be generated.

The following are the steps necessary to set up automatically generated reports for the Network Assessment Module:

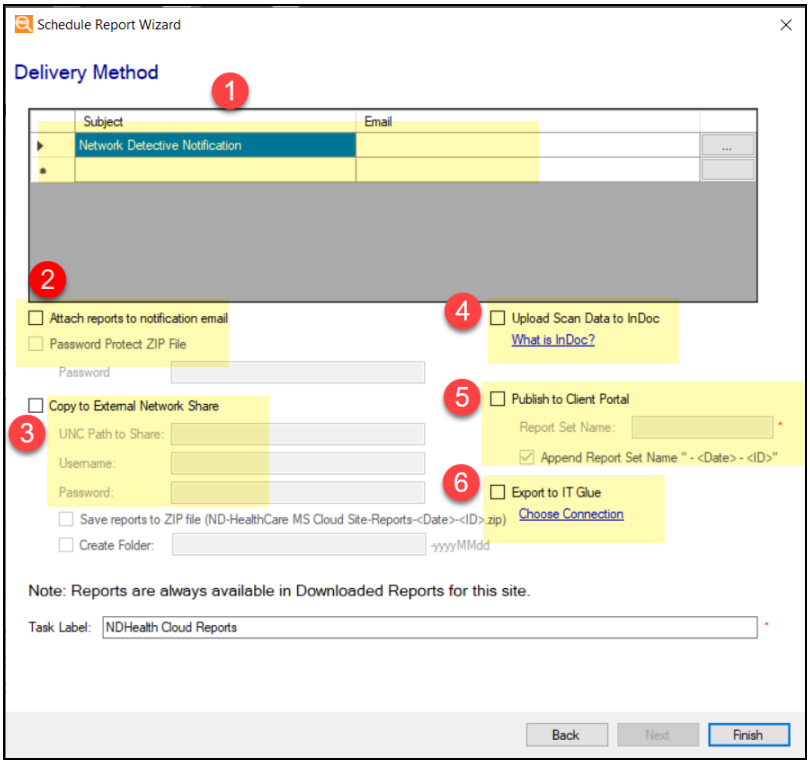
1. Using the **Manage Inspector** feature and the **Manage Appliance Window**, create a **Report Task** that specifies desired reports from the **Network Assessment Module**.

   Keep in mind that reports for specific **Assessment** types can only be produced after the Scans required for a specific **Assessment** type have been performed.

2. In the **Manage Appliance Window**, create a **Report Task** and select the Network Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.



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

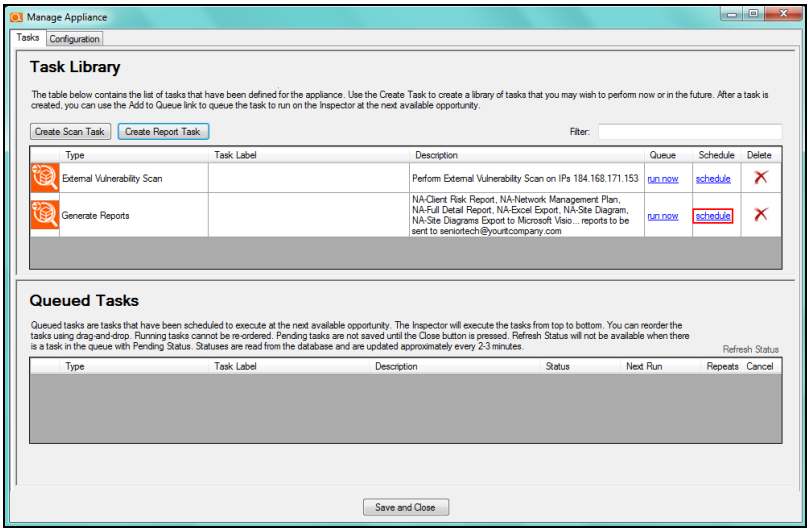


1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. Copy Reports to External Network Share with Reporter
4. Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See InDoc and the RapidFire Tools Portal for more on how to set up InDoc.
5. Publish documents to the Client Portal. See RapidFire Tools Portal Client View for Reporter.
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.

After defining the **Delivery Method** settings, click on the **Finish** button.

4. 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**.



Inspector's automated report generation engine will use whatever data is available to the **Inspector** for downloading from the appliance.

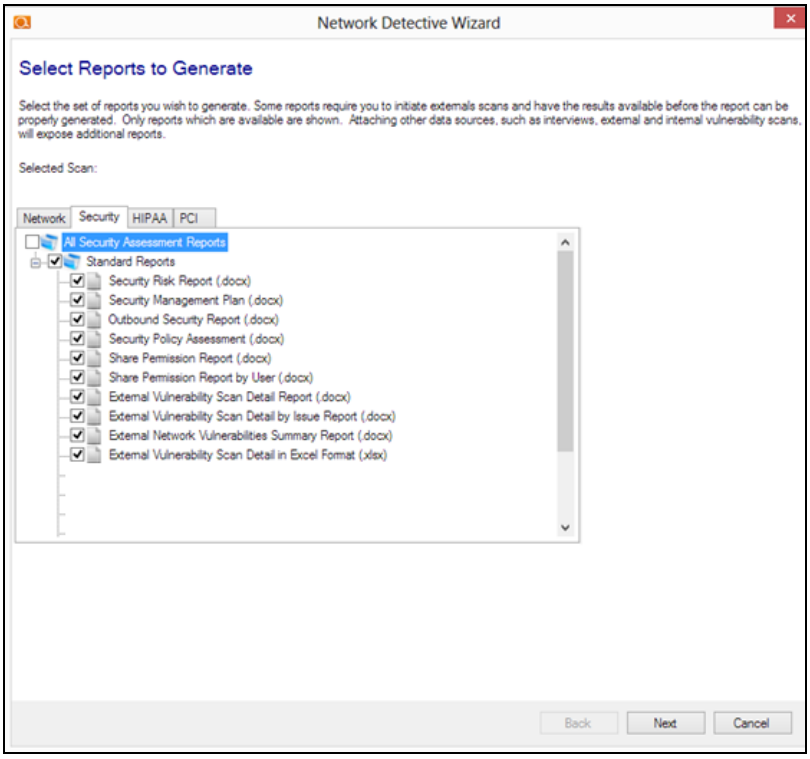
5. If the user has specified that reports be delivered by email, the specified email should receive an email with a .zip file of the reports attached as long as the zip file is less than 5 MB in size.

Security Assessments Automatic Reports

Automatic report generation for the Security Assessment Module requires that a **Scheduled Scan** be run on your client's network and the resulting scan file(s) automatically uploaded to the Inspector Appliance before a report can be generated.

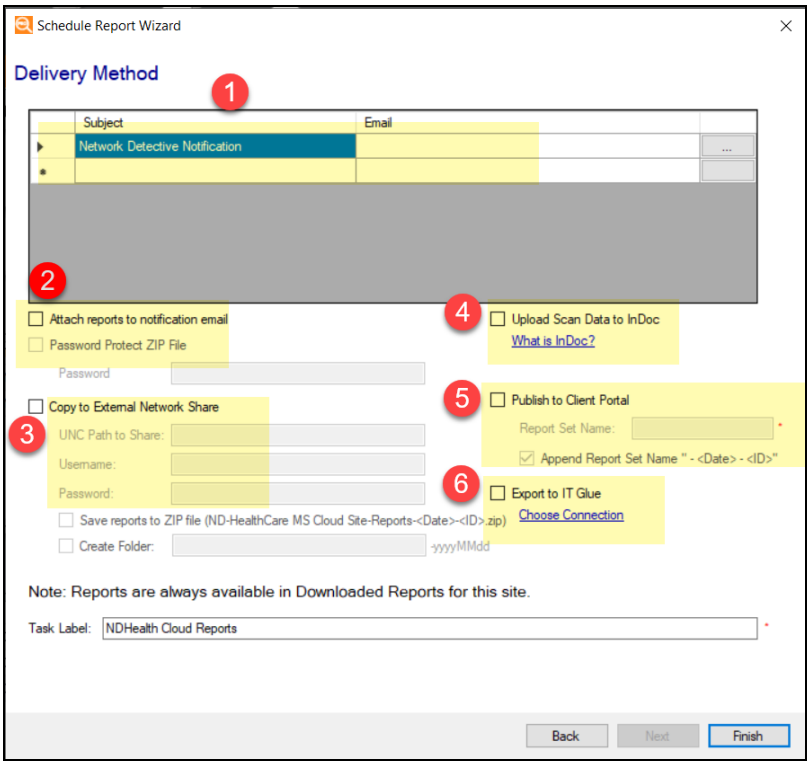
The following are the steps necessary to set up automatically generated reports for the Security Assessment Module:

1. Using the **Manage Appliance** feature and the **Manage Appliance Window**, create a **Report Task** that specifies desired reports from the **Security Assessment Module**.



   Keep in mind that reports for specific **Assessment** types can only be produced after the Scans required for a specific **Assessment** type have been performed and uploaded to the **appliance**.

2. In the **Manage Appliance Window,** create a **Report Task** and select the Security Assessment reports you would like to generate from within the **Select Reports to Generate** window. Then select the **Next** button.
3. Next, set the **Delivery Method** for the Reports. In this window you can:

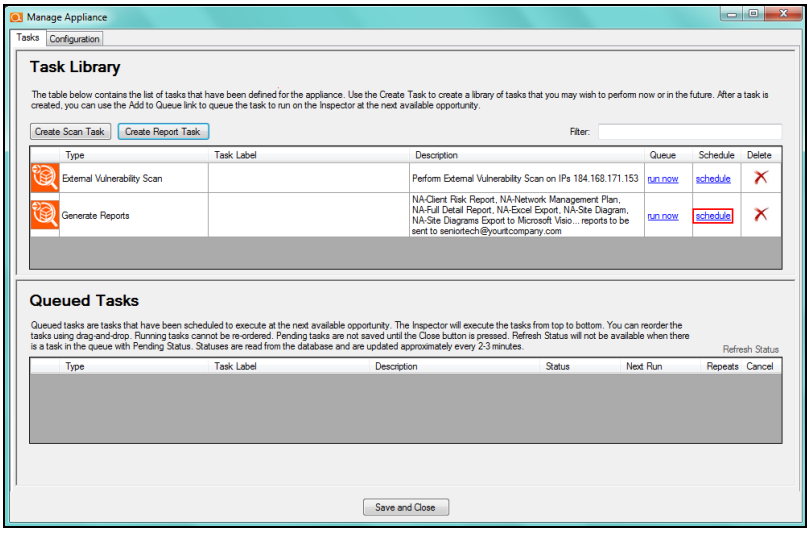


1. Define the Subject for the email to be sent and enter the email address of the Recipient
2. Set if you want to send the reports attached to the Report notification email message
3. Copy Reports to External Network Share with Reporter
4. Select **Upload Scan Data to InDoc** to send your Site information to InDoc in the RapidFire Tools Portal, where you can explore, manage, and document network assets. See InDoc and the RapidFire Tools Portal for more on how to set up InDoc.
5. Publish documents to the Client Portal. See RapidFire Tools Portal Client View for Reporter.
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.

After defining the **Delivery Method** settings, click on the **Finish** button.

4. Click on the **Schedule** link in order to schedule the running of the created **Report Task for a time which is certain to be after the scan is complete and uploaded to the appliance**.



5. If the user has specified that reports be delivered by email, the specified email 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.

HIPAA Compliance Assessments Automatic Reports

Automatic report generation for the HIPAA Compliance Module requires that a full assessment that includes scans, worksheets and surveys be completed and **uploaded to the Inspector** before reports can be generated.

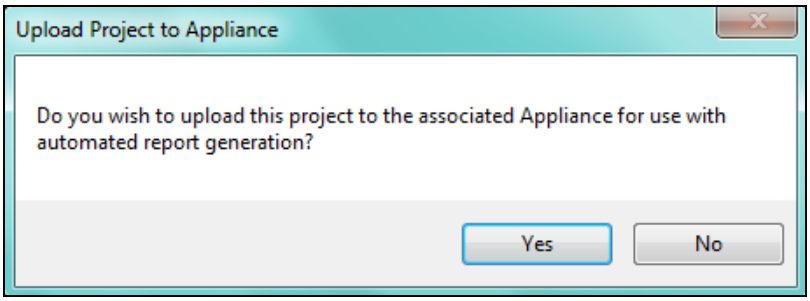
This is the only way for user completed worksheets and questionnaire data to be transferred to the **Inspector**.

Once the assessment is complete and synced, new scans can be automatically performed on the client's network using the **HIPAA Scans available from the Inspector**. Then, at the scheduled time, the **Inspector** will retrieve the scan data and new reports will be generated using the data collected from the **Inform-based Surveys** and **Worksheets** from your initial **Assessment** that was previously uploaded to the **Inspector Appliance**.

Performing the Initial HIPAA Assessment Report Generation Set-up

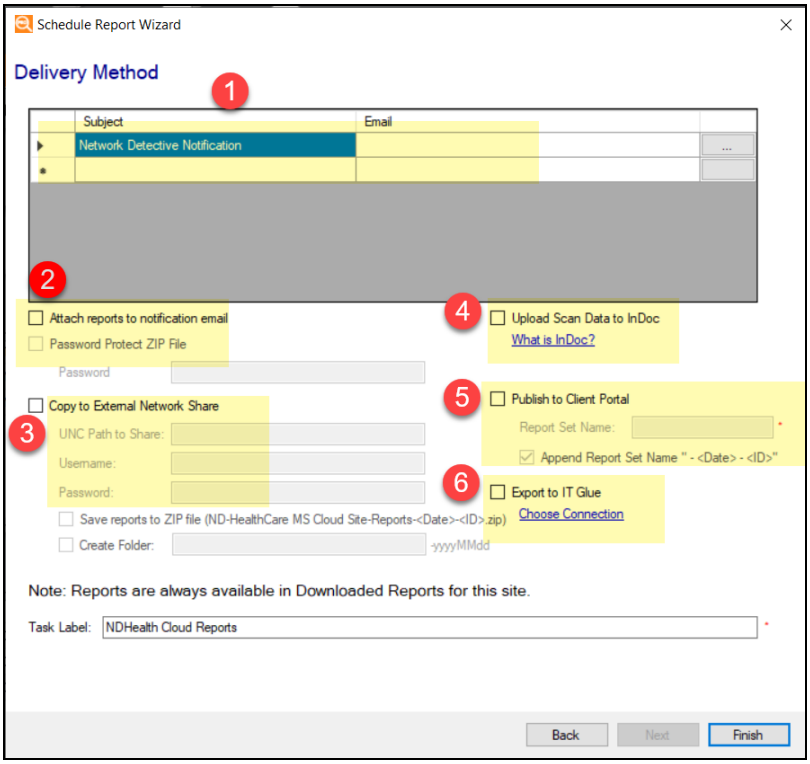
The following are the steps necessary to set up automatically generated reports for the HIPAA Compliance Module:

1. Using Network Detective, create a new assessment that is of the type **HIPAA Risk Assessment**.
2. **Associate** your **Inspector** with the **Site** that this new **HIPAA Assessment** is created within.
3. Complete all the requirements for a successful **HIPAA Risk Assessment** within this new assessment. This includes external vulnerability scans, network scans, local scans, and the completion of all appropriate Inform-based **Surveys and Worksheets**. When this step is complete, the user should be able to generate all **HIPAA Assessment** reports.
4. Generate the **HIPAA Assessment** reports to verify that the assessment was performed correctly.
5. Once satisfied with a complete **HIPAA Assessment**, press the "**Finish**" Assessment button.



Confirm that you wish to upload the **Assessment Project** data to the **Inspector** to be used for automatic report generation.

6. After the upload is complete, access the **Manage Appliance Window** and select the **Create Report Task** option.
7. 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.
8. Next, set the **Delivery Method** for the Reports. In this window you can:



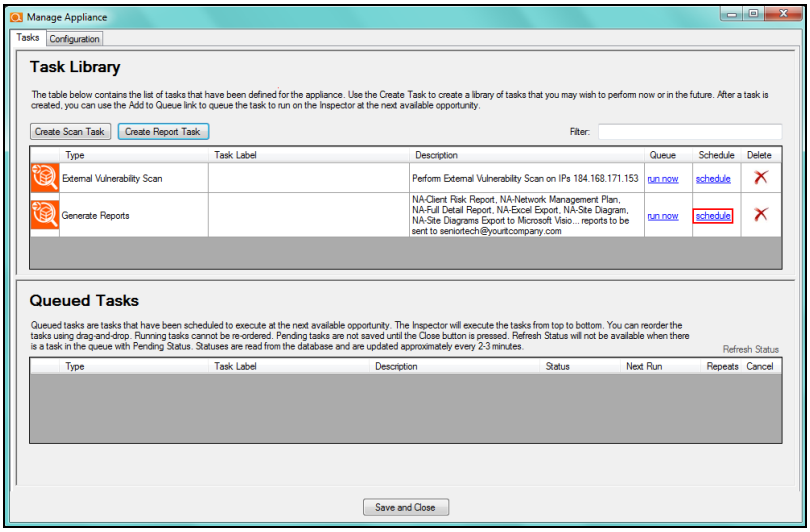
1. Define the Subject for the email to be sent and enter the email address of the Recipient

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
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 for more on how to set up InDoc.
5. Publish documents to the Client Portal. See RapidFire Tools Portal Client View for Reporter.
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.

After defining the **Delivery Method** settings, click on the **Finish** button.

9. Click on the **Schedule** link in order to schedule the running of the created **Report Task for a time which is certain to be after the scan is complete and uploaded to the appliance**.



Inspector's automated report generation engine will use whatever data is available to the **Inspector** for downloading based on the most recent scan that has been completed. Therefore, if the scan of your client's network is not complete, then the reports will not have the most recent scan's data either.

> **Note:** Keep in mind that reports for specific Assessment types can only be produced after the Scans required for a specific Assessment type have been performed.

10. If the user has specified that reports be delivered by email, the specified email recipient 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. Reports over 5MB must be manually downloaded using the **Download Reports** feature detailed below.

    If you receive an **Exception Report** via email:

    a. Note any missing elements present in the Exception report (if present)
    b. Update Inform forms in currently active Assessment to reflect that data desired.
    c. If current Informs do not contain the topics that are noted as missing:
        i. Press the “Finish” button for the currently active Assessment.
        ii. DO NOT agree to the question which asks if you would like to sync the datato the Inspector.
        iii. Start a new active Assessment. Check the checkbox which says “Sync with latest Inspector scan”
        iv. New assessment with latest data from Inspector will be created. Update Inform as appropriate.
    d. Press “Finish” button for currently active Assessment
    e. DO agree to sync the data to the Inspector.

PCI Compliance Assessments Automatic Reports

Automatic report generation for the PCI Compliance Module requires that a full assessment that includes scans, worksheets and surveys be completed and **uploaded to the Inspector** before reports can be generated.

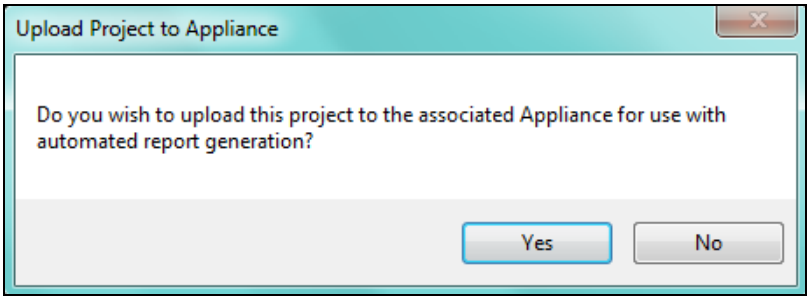
This is the only way for user completed worksheets and questionnaire data to be transferred to the **Inspector**.

Once the assessment is complete and synced, new scans can be automatically performed on the client's network using the **PCI Scans available from the Inspector**. Then, at the scheduled time, the **Inspector** will retrieve the scan data and new reports will be generated using the data collected from the **Inform-based Surveys** and **Worksheets** from your initial **Assessment** that was previously uploaded to the **Inspector Appliance**.

Performing the Initial PCI Assessment Report Generation Set-up

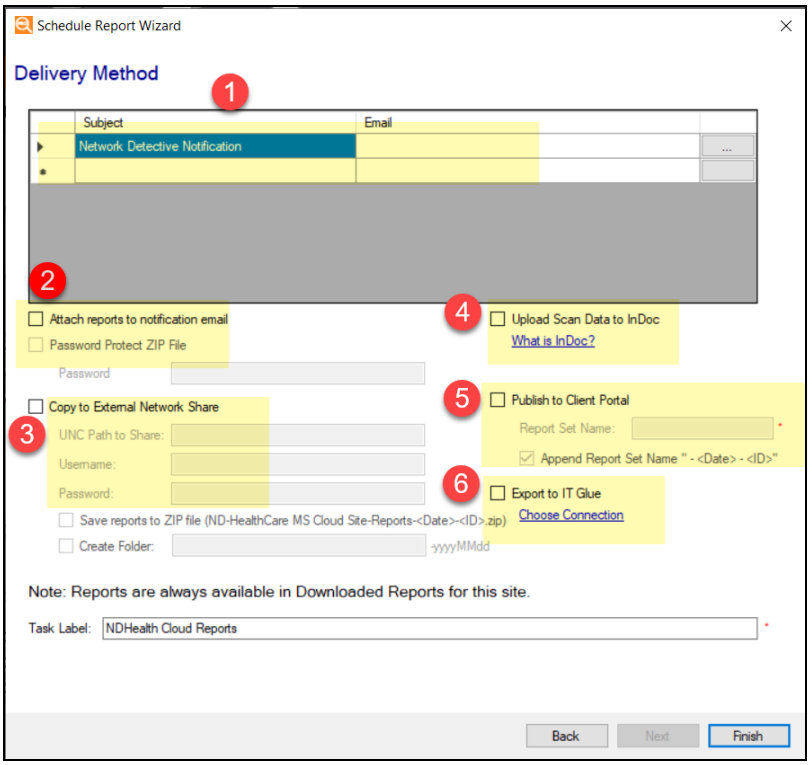
The following are the steps necessary to set up automatically generated reports for the PCI Compliance Module:

1. Using Network Detective, create a new assessment that is of the type **PCI Risk Assessment**.
2. **Associate** your **Inspector** with the **Site** that this new **PCI Assessment** is created within.
3. Complete all the requirements for a successful **PCI Risk Assessment** within this new assessment. This includes external vulnerability scans, network scans, local scans, and the completion of all appropriate inform-based **Surveys and Worksheets**. When this step is complete, the user should be able to generate all **PCI Assessment** reports.
4. Generate the **PCI Assessment** reports to verify that the assessment was performed correctly.
5. Once satisfied with a complete **PCI Assessment**, press the "**Finish**" Assessment button.



Confirm that you wish to upload the **Assessment Project** data to the **Inspector** to be used for automatic report generation.

6. After the upload is complete, access the **Manage Appliance Window** and select the **Create Report Task** option.
7. 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.



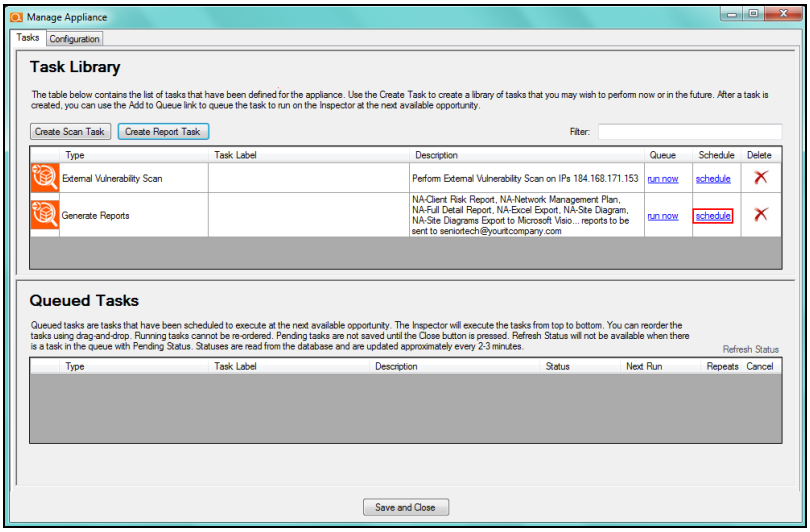
8. Next, set the **Delivery Method** for the Reports. In this window you can:
    1. Define the Subject for the email to be sent and enter the email address of the Recipient
    2. Set if you want to send the reports attached to the Report notification email message
    3. Copy Reports to External Network Share with Reporter
    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 for more on how to set up InDoc.

5. Publish documents to the Client Portal. See RapidFire Tools Portal Client View for Reporter.
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.

After defining the **Delivery Method** settings, click on the **Finish** button.

9. Click on the **Schedule** link in order to schedule the running of the created **Report Task for a time which is certain to be after the scan is complete and uploaded to the appliance**.



Inspector's automated report generation engine will use whatever data is available to the **Inspector** for downloading based on the most recent scan that has been completed. Therefore, if the scan of your client's network is not complete, then the reports will not have the most recent scan's data either.

Note: Keep in mind that reports for specific Assessment types can only be produced after the Scans required for a specific Assessment type have been performed.

10. If the user has specified that reports be delivered by email, the specified email recipient 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. Reports over 5 MB must be manually downloaded using the **Download Reports** feature detailed below.

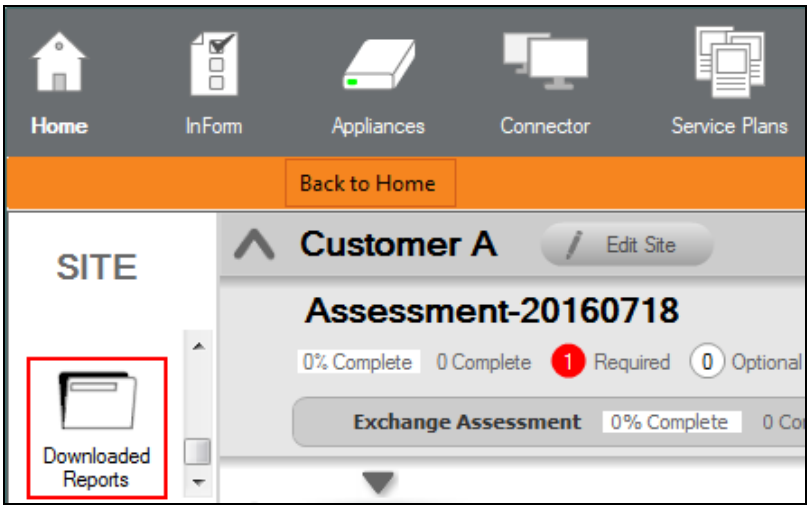
If you receive an **Exception Report** via email:

a. Note any missing elements present in the Exception report (if present)
b. Update Inform forms in currently active Assessment to reflect that data desired.
c. If current Informs do not contain the topics that are noted as missing:
    i. Press the “Finish” button for the currently active Assessment.
    ii. DO NOT agree to the question which asks if you would like to sync the datato the Inspector.
    iii. Start a new active Assessment. Check the checkbox which says “Sync with latest Inspector scan”
    iv. New assessment with latest data from Inspector will be created. Update Inform as appropriate.
d. Press “Finish” button for currently active Assessment
e. DO agree to sync the data to the Inspector.

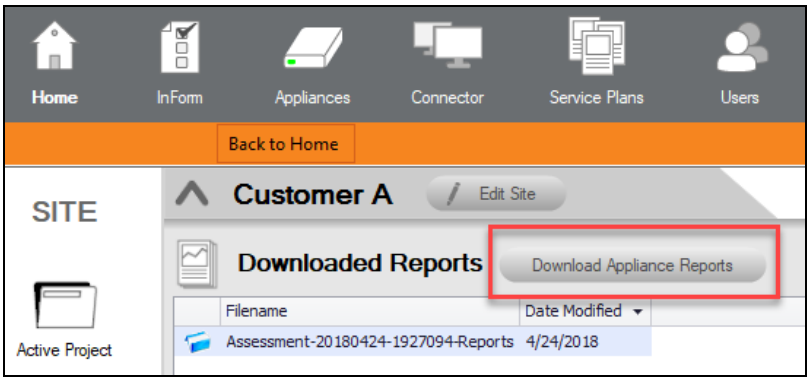
Manually Download Reports

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

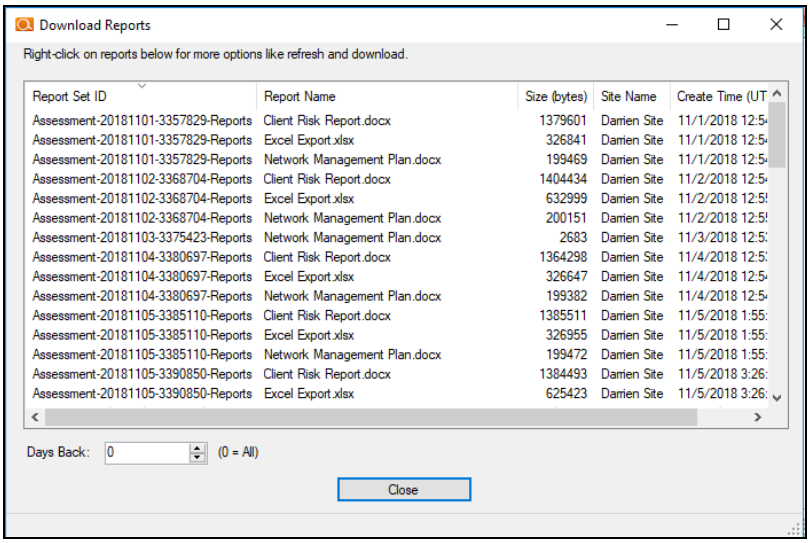
1. **Open** the **Site Associated** with **Inspector**.
2. Select the **Downloaded Reports** Icon on the left side of the Network Detective window to display the **Download Reports** button in the Network Detective window.



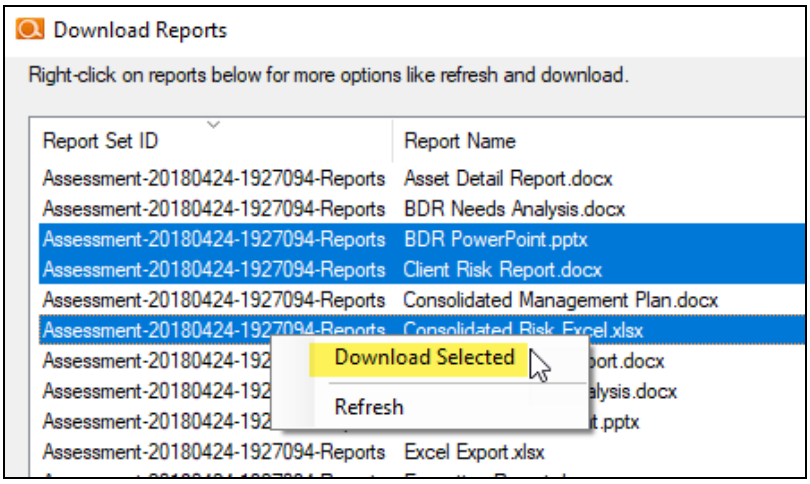
3. View the list of generated reports by selecting the **Download Appliance Reports** button that appeared at the top of the Network Detective window.



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

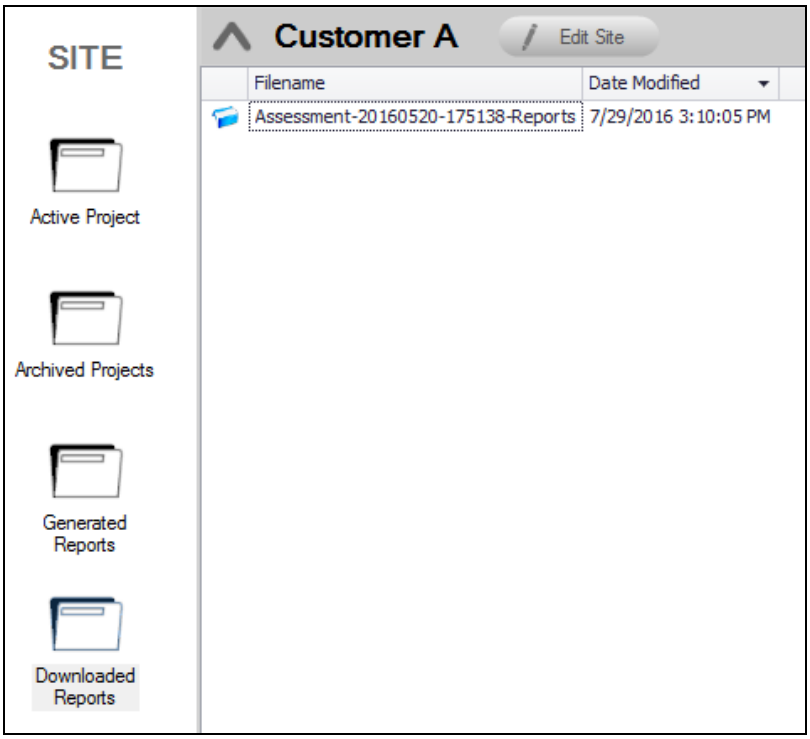


5. Select one or more reports. Right click and select Download Selected.



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.

8. 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.

Inspector Appendices

This section contains other helpful topics related to Inspector:

Pre-Scan Network Configuration Checklist 87

Updating a Software Appliance 91

Inspector Appliance Override 94

Set Scan and Report Task Time Zone and Date Format 96

Software Appliance Diagnostic Tool 98

Pre-Scan Network Configuration Checklist

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

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

> **Note:** You must have the .NET 4.6.2 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

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

Complete	Domain Configuration
	GPO Configuration for Windows Firewall (Inbound Rules)
☐	Allow *Windows Management Instrumentation (WMI)* service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
☐	Allow *File and printer sharing* to operate through Windows Firewall This includes the following rules: • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
☐	Enable *Remote Registry* "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 *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request **Note:** ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
☐	*Windows Management Instrumentation (WMI)* • Startup Type: Automatic
☐	*Windows Update Service* • Startup Type: Automatic
☐	*Remote Registry* • Startup Type: Automatic
☐	*Remote Procedure Call* • Startup Type: Automatic
	Network Shares
☐	• *Admin$* must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

Complete	Domain Configuration
	3rd Party Firewalls
☐	• Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. **Note:** This is a requirment for both Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

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

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

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

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

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

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

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

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

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

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

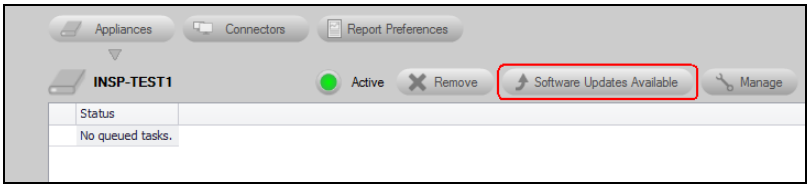
You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

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

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.

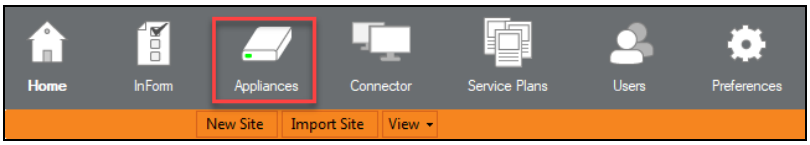
Updating a Software Appliance

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.

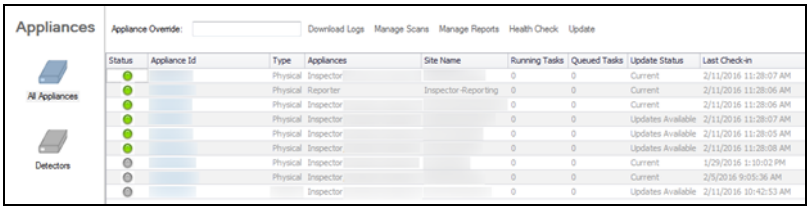


Updates may include bug fixes, new features, and additional scans types.

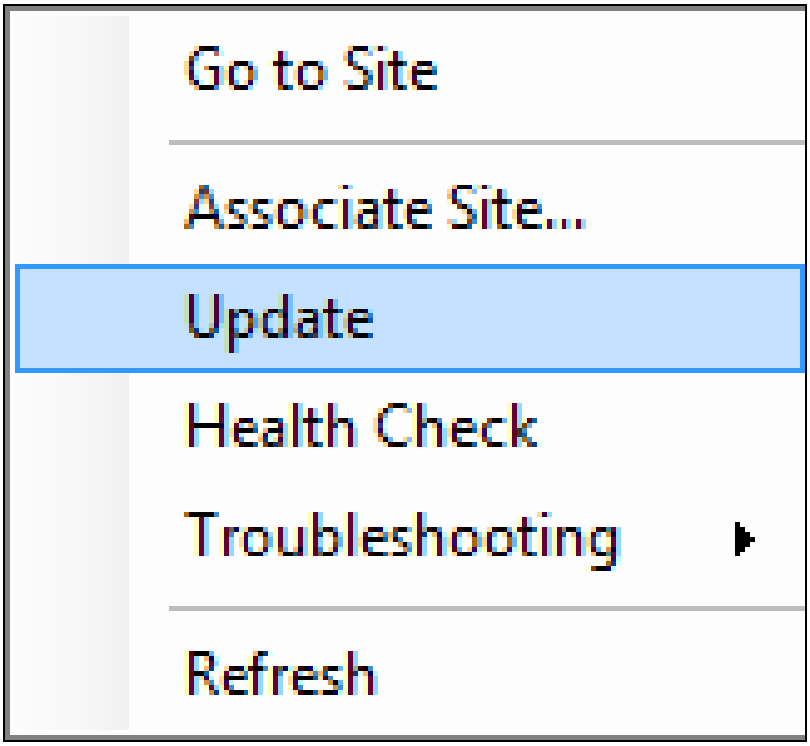
In the **Network Detective Application**, navigate to **Network Detective** ribbon bar and select the **Appliances** icon.



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



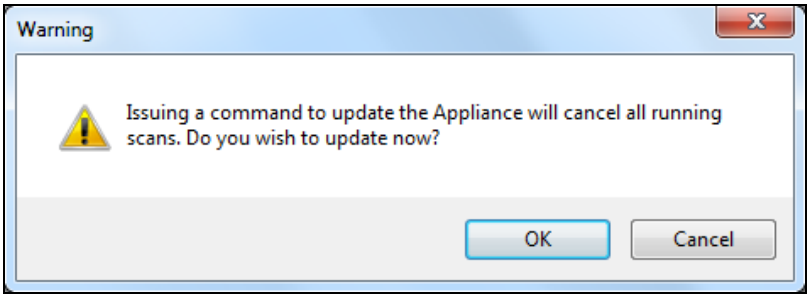
To update the selected **Software Appliance,** right click on the **Appliance's** name, and select the **Update** menu option presented as displayed.



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.

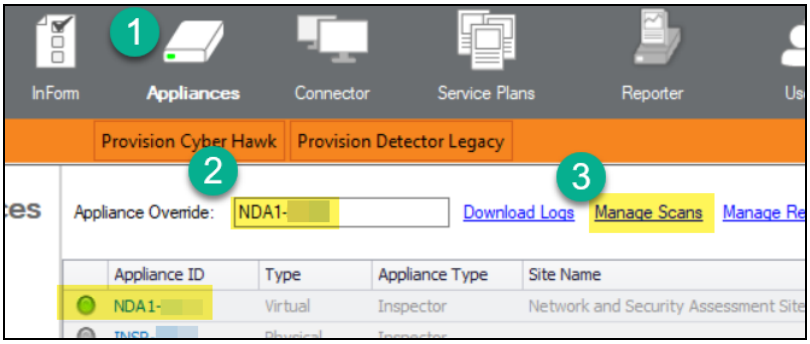


A window will appear confirming the request for a software update.

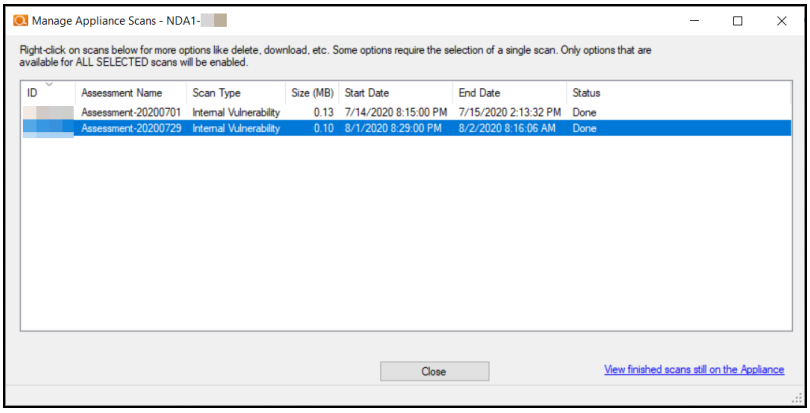
Inspector Appliance Override

From the **Appliances** screen, you have additional options to manage, cancel, and download Inspector Appliance scans. To do this:

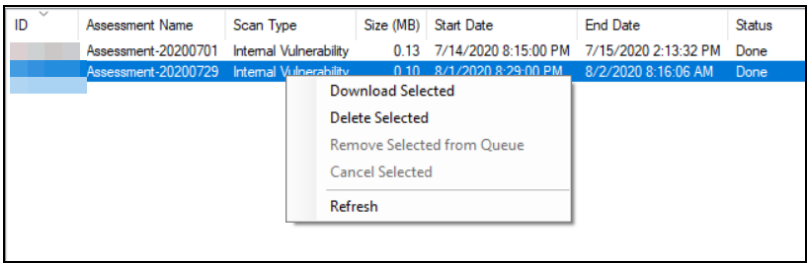
1. Click on **Appliances** from the top menu.
2. In the **Appliance Override** field, enter the full ID for the Inspector Appliance. For example, "NDA1-XXXX."
3. Click **Manage Scans**.



The **Manage Appliance Scans** window will appear. Here you can see your recent scan activity, including active and queued scans.

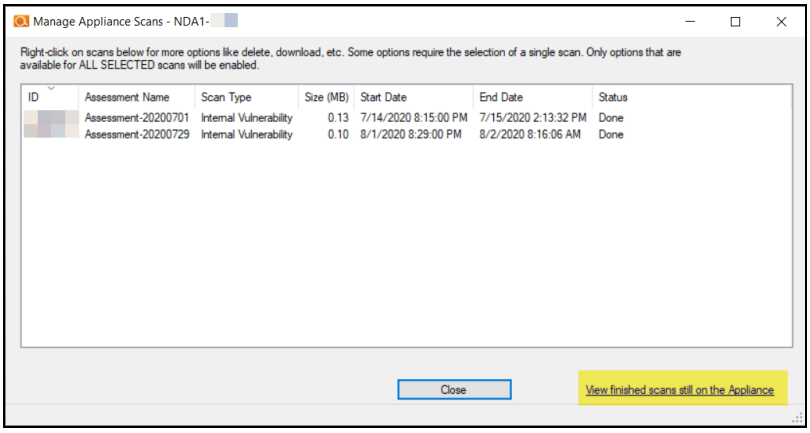


4. Right click on a scan to access several options:

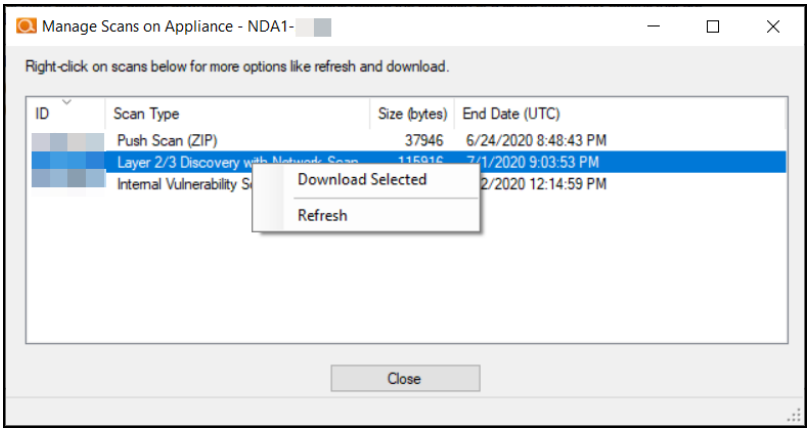


- Download selected scan
- Delete scan
- Cancel scan in progress
- Remove scan from queue

5. Likewise, you can click **View finished scans still on the Appliance** to download older completed scans.



6. Right click on a scan to download it.



Set Scan and Report Task Time Zone and Date Format

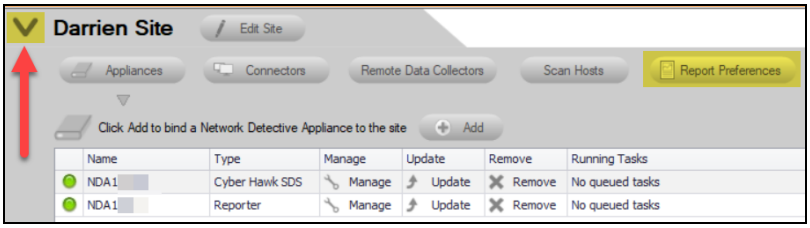
You can configure the time zones and dates that appear next to your Site's scan and report tasks. This feature applies to both **Reporter** and **Inspector** for Network Detective.

- 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.

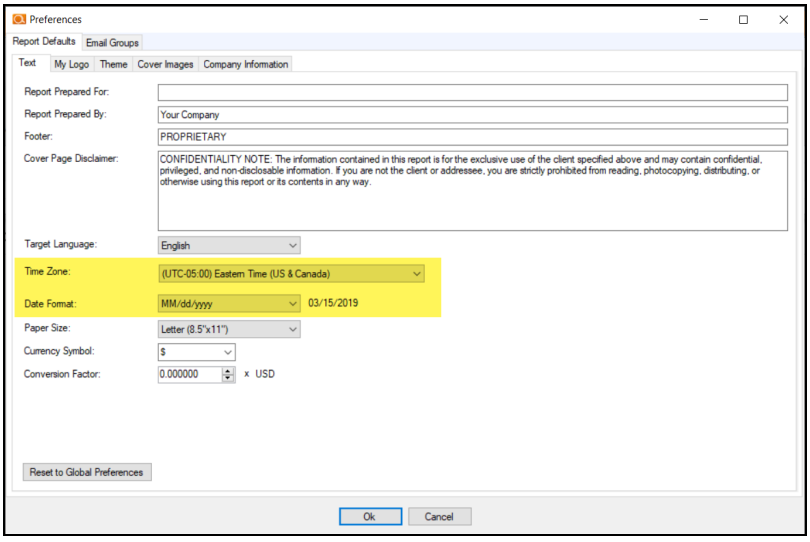
To set preferences:

At Site Level

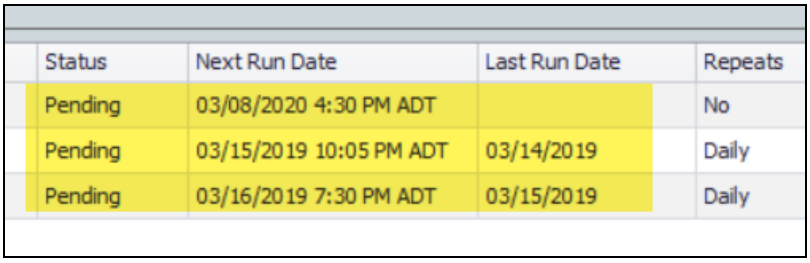
1. Open your **Reporter** or **Inspector** Site in Network Detective.
2. Open the Site Settings and click **Report Preferences**.



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.

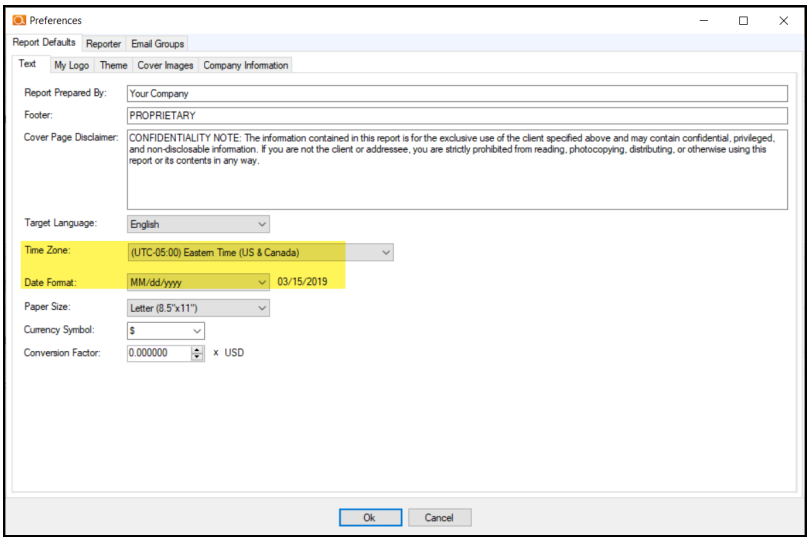


Status	Next Run Date	Last Run Date	Repeats
Pending	03/08/2020 4:30 PM ADT		No
Pending	03/15/2019 10:05 PM ADT	03/14/2019	Daily
Pending	03/16/2019 7:30 PM ADT	03/15/2019	Daily

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**.

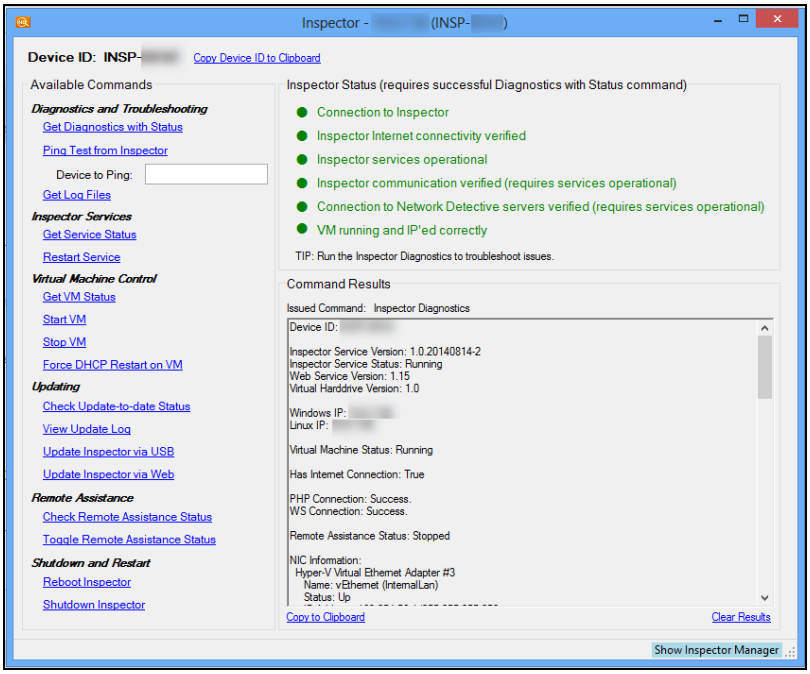


Unless you have adjusted your preferences at the Site level, your NEWLY CREATED Site's scheduled scan and report tasks will now appear with your preferred time zone and date format.

> **Note:** New *Reporter Templates* you create and apply will also use your Global **Time Zone** and **Date Format** preferences.

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.