NETWORK DETECTIVE™

USER GUIDE

PCI Compliance Assessment Module with Inspector

Instructions to Perform a PCI Compliance Assessment

11/2/2023 4:58 PM

Contents

About the Network Detective PCI Compliance Assessment Module

The Payment Card Industry Data Security Standard (PCI DSS) is an actionable security framework that helps merchants that accept credit/debit cards prepare for, prevent, detect, and respond to security breaches.

Per PCI Requirement 12.2, an annual Risk Assessment is a key requirement that must be met to comply with PCI. The Risk Assessment must identify the vulnerabilities to the security of the Cardholder Data Environment (CDE) whereby threats that can act on IT system component and software application vulnerabilities, including the likelihood and the impact if that occurs.

Network Detective's PCI Compliance module is the first professional tool to combine and integrate automated data collection with a structured framework for collecting supplemental assessment information not available through automated tools.

The PCI Compliance module is the first solution to allow for the automatic generation of the key Evidence of Compliance documents that are necessary to demonstrate compliance with PCI requirements. This module includes comprehensive checklists that cover a number of the Administrative, Physical, and Technical safeguards defined within the PCI Requirements. The PCI module produces more than just the documents to satisfy a compliance requirement. Network Detective PCI module provides factual evidence, expert advice, and direction to individuals performing PCI Risk Assessments in order minimize or eliminate the risk of a data breach.

Key PCI Terms

Term	Definition
Cardholder Data	The full Primary Account Number (PAN) is the minimum. Cardholder data may consist of the full PAN, cardholder name, expiration data and/or the service/security code.
Cardholder Data Environment	The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
CDE	The acronym for Cardholder Data Environment.
Primary Account Number	Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Often times referred to as “Account Number”.
PAN	The acronym for Primary Account Number.

Introduction to PCI Compliance Assessment Module

This section covers everything you need to know before getting started with your PCI Compliance Assessment.

PCI Compliance Assessment Overview

Network Detective's PCI Compliance Assessment Module combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a PCI Compliance Assessment, you will:

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

What You Will Need

In order to perform a PCI Compliance Assessment, you will need the following components:

Note: You can access these at https://www.rapidfiretools.com/nd.

PCI Compliance Assessment Component	Description
Network Detective	The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
PCI Data Collector	The Network Detective PCI Data Collector is a windows application that performs the data collections (network, local 'quick', and local 'deep') for the PCI Compliance Module. Supports both Network and Computer scans.
Inspector Appliance	The Inspector Appliance is an appliance-based system used for performing scheduled IT assessment scans and deeper dive diagnostics. The Inspector performs scans from the point-of-view of the client's internal network.
Surveys and Worksheets	Surveys and worksheets contain questions that require investigation outside of an automated scan. You create and manage these documents directly from the Network Detective Application, where you can also import and export your responses to and from Word.

Risk Assessment vs. Risk Profile

There are two types of PCI Compliance Assessments that can be performed:

Assessment Type	Description
PCI Risk Assessment	A complete assessment that includes all worksheets and surveys. • Required at least annually • Recommended quarterly as part of a quarterly compliance review • Requires that all manual worksheets be completed **Important:** Allow for at least an entire day to perform the assessment on a typical 15 user network
PCI Risk Profile	Updates a Risk Assessment to show progress in avoiding and mitigating risks - and finds new ones that may have otherwise been missed. • Does NOT require worksheets • Requires selecting a prior Risk Assessment (will use existing worksheets) • Requires less than 1 hour for a typical 15 user network **Note:** You can only create a Risk Profile after you have first performed a Risk Assessment.

PCI Risk Profile Use for Ongoing PCI Compliance Assessments

A PCI Risk Analysis should be done no less than once a year. However, the Network Detective includes an abbreviated version of the PCI Risk Analysis assessment and reporting process within the Network Detective PCI Module. This process is called the PCI Risk Profile.

The PCI Risk Profile is designed to provide interim reporting in a streamlined and almost completely automated manner.

Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.

An important aspect of this abbreviated process is the need that the PCI Module has been already used to perform a PCI Risk Assessment of your customer's Cardholder Data Environment (CDE) on a previous occasion.

Choosing a PCI Risk Assessment Mode

When performing a PCI Risk Assessment with Network Detective, you can select from two different modes:

Mode	Assessment Value	Description
PCI Module with Inspector	*Highest*	Select this mode when you have the Network Detective **Inspector Appliance**. When you use Inspector alongside the PCI Module, your assessment can include an **Internal Vulnerability Scan** and a **Layer 2/3 Network Diagram**. These provide a more thorough assessment of a Merchant's IT-based Cardholder Data Environment (CDE), and are part of the PCI DSS requirements.
PCI Module (standalone)	*Basic*	Select this mode when you 1) do not have Inspector, and 2) are using other tools to perform an Internal Vulnerability Scan and produce a network diagram of the CDE. **Important:** As per PCI DSS requirements, an Internal Vulnerability scan must be performed on all devices within the CDE. This helps to identify and mitigate network vulnerabilities to prevent a security breach.

Planning the On-site Data Collection

There are various ways to collect data for a PCI Compliance Assessment. These methods can vary based on time, cost, client expectation, level of detail needed to identify remediation needs, etc. Here are some general guidelines to help you plan your on-site data collection.

PCI Risk Assessment

Collection Type	Procedure	When to Use
Quick Audit	• External Scan • Network Scan • Computer Scan on 1-3 computers • All worksheets	• When there isn't enough time for a full assessment • When a full assessment is not required • When you cannot access every computer on the network • When you need an initial risk assessment to make changes to the network before a complete audit
Full Audit	• External Scan • Network Scan • Computer Scan on all computers • All worksheets	• When you need to collect data from every device on the network • When you need to prepare complete PCI Compliance documentation

PCI Risk Profile

Note: You can only perform a PCI Risk Profile after you have completed at least one PCI Risk Assessment.

Collection Type	Procedure	When to Use
Quick Audit	• External Scan • Network Scan • Computer Scan on 1-3 computers • NO worksheets	• When there isn't enough time for a full assessment • When a full assessment is not required • When you cannot access every computer on the network • When you need an initial risk assessment to make changes to the network before a complete audit
Full Audit	• External Scan • Network Scan • Computer Scan on all computers • NO worksheets	• When you need to collect data from every device on the network • When you need to prepare complete PCI Compliance documentation

Automated Scans Performed During the PCI Assessment Process

The Initial Data Collection phase of the PCI Compliance Assessment consists of the following required and optional scans:

- External Vulnerability Scan
- Internal Vulnerability Scan (optional and requires the Network Detective Inspector)
- PCI Network and Layer 2/3 Discovery Scan (using Inspector)
- PCI Scans on Local Computers (using the Inspector to Push Local Scans for PCI and the PCI Data Collector for unreachable computers)
- Optional Local Computer Scans (using the PCI Data Collector)

The PCI Data Collector scans make use of multiple technologies/approaches for collecting information on the client network, including:

- Network Scan
- Active Directory
- WMI
- Remote Registry
- ICMP
- File System Scanning
- Windows Registry
- Windows Shares and Permissions
- Security Center

Using the Compensating Controls Worksheet to Address Compliance Lapses and False Positives

Sometimes you may get stuck in an assessment. This might happen for several reasons:

- You cannot resolve every single compliance issue identified in the assessment
- Your scan results differ from what you know is the reality on the target network
- You do not have enough information to enter accurate responses for every form question

If you encounter any of the above, you can always move ahead and complete your assessment using the **Compensating Controls Worksheet**. This worksheet becomes available near the end of your To Do list. It allows you to document explanations on suspect items. Your explanation can include why various discovered items are not true issues and indicate possible false positives. Additionally, you can explain why a certain compliance requirement should not apply to you – or an alternative way in which you have met the requirement.

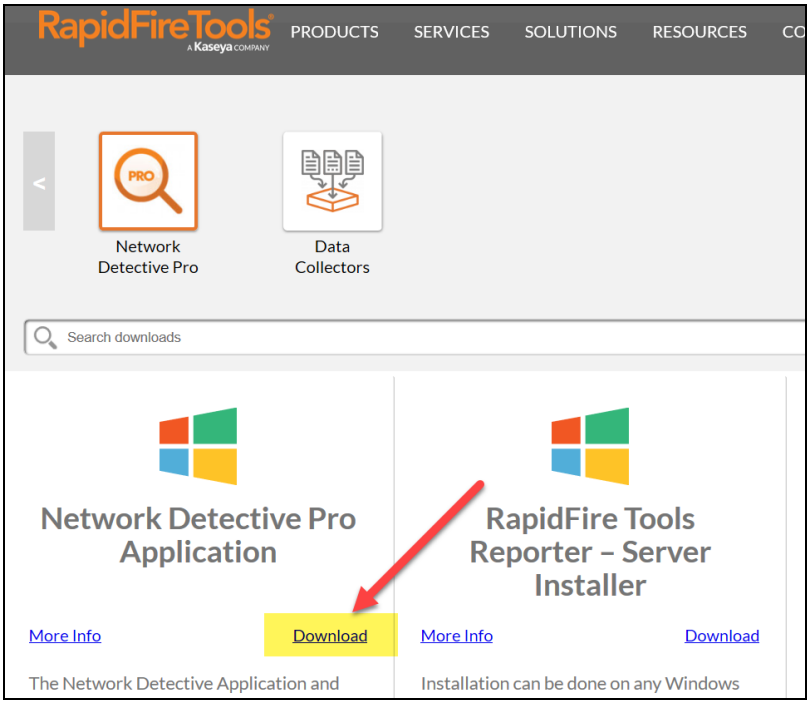
These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The **Compensating Controls Worksheet** does not alleviate the need for safeguards but allows for description of alternative means of mitigating the identified security risk.

Setting up your PCI Compliance Assessment Project

Download and Install the Network Detective Application

Visit https://www.rapidfiretools.com/nd. Download and install the Network Detective Application.

Important: Do not install the Network Detective Application on your client's network. Only the various **Data Collectors** are run on your client's network and computers.



Always accept the prompt to update Network Detective to the latest version.

When you run Network Detective for the first time, it will launch the Network Detective Wizard. You can dismiss the wizard and proceed to create a New Site. Sites are used to manage your customers' IT Assessment Projects.

Note: We recommend you use Sites to manage the assessments you perform for your clients. Sites help organize the scans you perform on your clients' networks and computers.

Create a New Site

The first step in the assessment is creating a “Site”. All Network Detective assessments are organized into Sites. A Site can be a physical location or a logical grouping, such as a customer account name.

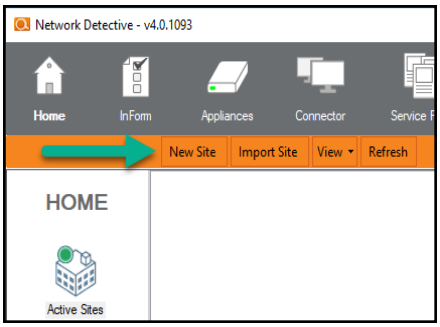
Before making a selection, you must decide on your assessment strategy. For example:

A. For a single location, create one Site.
B. For organizations with multiple locations, decide if you want one set of reports, or separate reports for each location.

> **Note:** Reports are generated on a Site by Site basis.

To create a new Site:

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



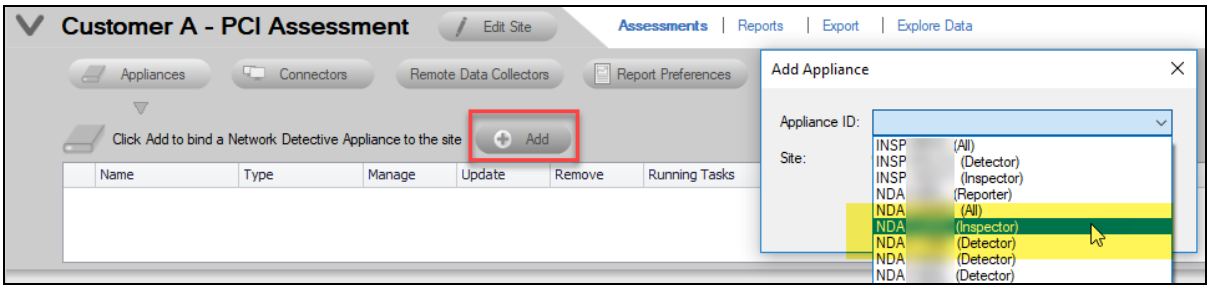
3. Enter a **Site Name** and click **OK**.

Add Inspector Appliance

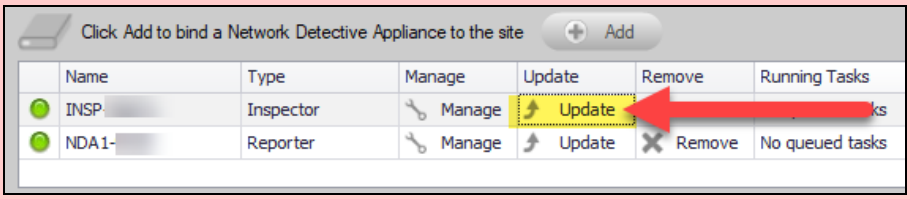
Next, associate an Inspector with the Site. To do this:

1. From within the newly created Site, click the chevron button to show the Site Configuration Options.

2. Next, click **Add**. The Add Appliance window will appear.
3. Use the drop-down menu to select the Appliance you wish to associate with the site.

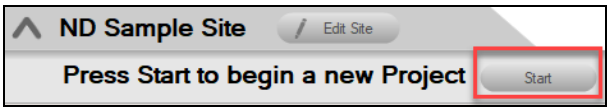


Important: Before starting your first assessment using the PCI Module, be sure to update your Inspector device to the latest version.

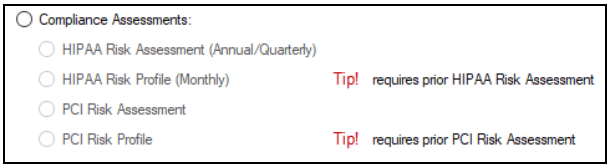


Start a PCI Compliance Assessment Project

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



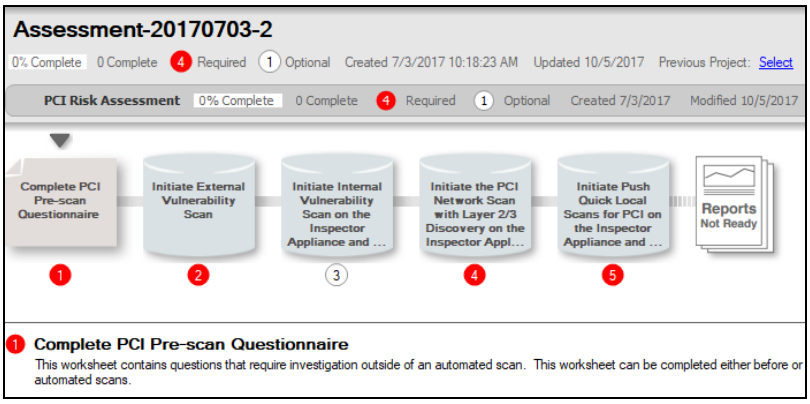
2. Next, select **Compliance Assessments**, and then select your chosen PCI Compliance Assessment.



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

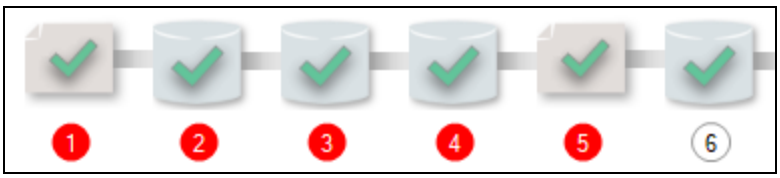
Use the PCI Compliance Assessment Checklist

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



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

When you complete a step, that item will be updated with a green check mark in the checklist.



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

Performing a PCI Compliance Assessment

To perform a PCI Compliance Assessment, complete the steps detailed in this guide.

Collect Initial PCI Compliance Assessment Data

Step 1 — Complete the Pre-Scan Questionnaire

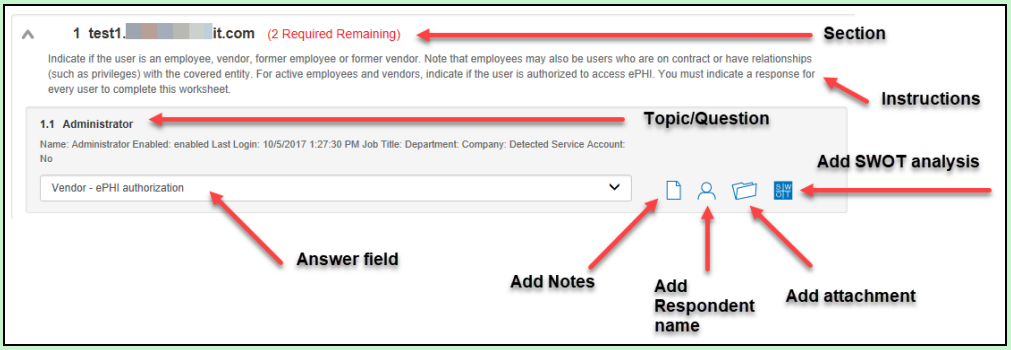
The **Pre-Scan Questionnaire** is the first part of the PCI Compliance Assessment process. To complete the pre-scan questionnaire:

1. Double click on the **Complete PCI Pre-scan Questionnaire** item within the checklist. Or you can click on the PCI Pre-Scan Questionnaire in the InForm Bar located at the bottom of the Assessment Window.
2. Complete each required item within the worksheet.

EXAMPLE:

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

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



ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.

iii. Enter the *Response*. There are three types of responses:

Response Type	Description	Example Use
Text Response	Free-form text response	"Describe the condition of the data center."
Multiple Choice	Multiple fixed responses	"Does the firewall have IPS?" (Yes/No)
Checklist Item	An item that is marked off if completed	"Check the security of the door locks."

Note: With few exceptions, you must respond to each form entry to complete the all of the surveys within the PCI Compliance Assessment process.

iv. (Optional) Enter any *Notes* relevant to the topic's response.

v. (Optional) Enter the name of *Respondent* (i.e. the person who provided you with the information, if applicable).

vi. (Optional) Add any relevant *Attachments*. See "Add Image Attachments to Surveys and Worksheets" on page 107 for more details.

Note: Only image attachments (.png, .jpg) are supported at this time.

vii. (Optional) Add a *SWOT Analysis*, examining Strengths, Opportunities, Weaknesses, and Threats. See "Add SWOT Analysis to Surveys and Worksheets" on page 107 for more details.

viii. Save your answers periodically and **Save** and **Close** when you are done.

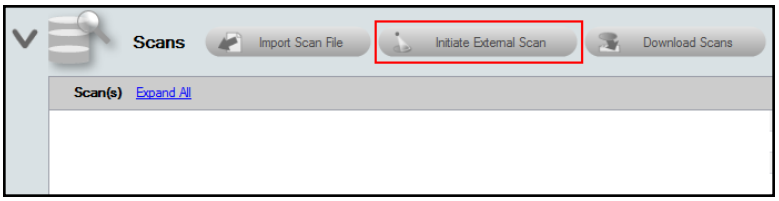
To return to the questionnaire, double click on the icon in the Checklist, or click on the item within the InForm Bar.

Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

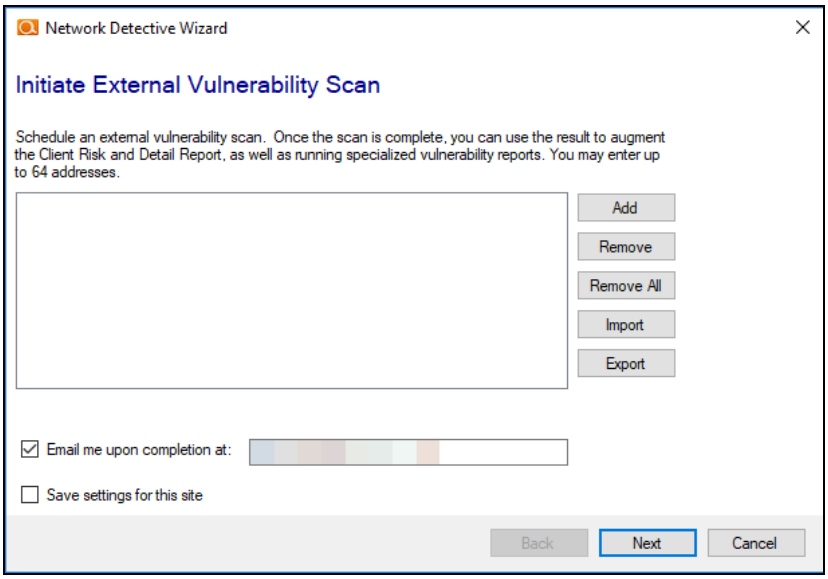
Step 2 — Initiate External Vulnerability Scan

To configure and start the External Vulnerability Scan:

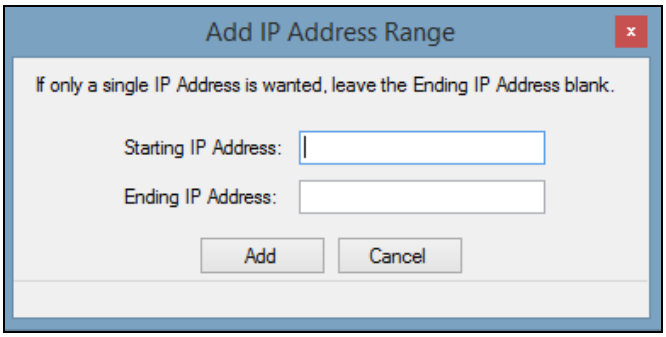
1. From the **Scans Bar** located at the bottom of the Assessment Window, click **Initiate External Scan**.



2. In the **Network Detective Wizard** window, enter the range of IP addresses you would like to scan. **You can enter up to 64 external addresses**.



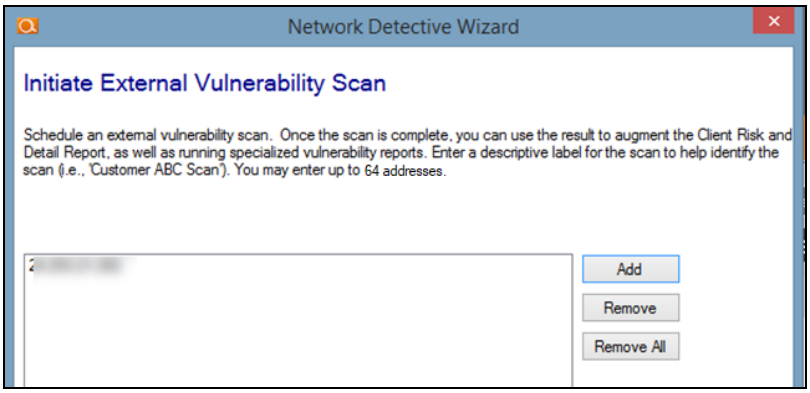
3. Click **Add** to add a range of external IP addresses to the scan.



Tip: If you do not know the external range, you can use websites such as whatismyip.com to determine the external IP address of a customer.

4. Enter the IP range for the scan. If only a single IP Address is wanted, leave the Ending IP Address blank.

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

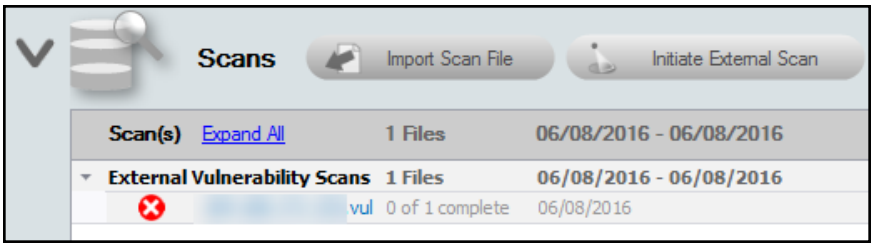


5. In the **Initiate External Vulnerability Scan** window, enter an email address to be notified when the scan is completed.
6. Click **Next** to send the request to the servers that will perform the scan.

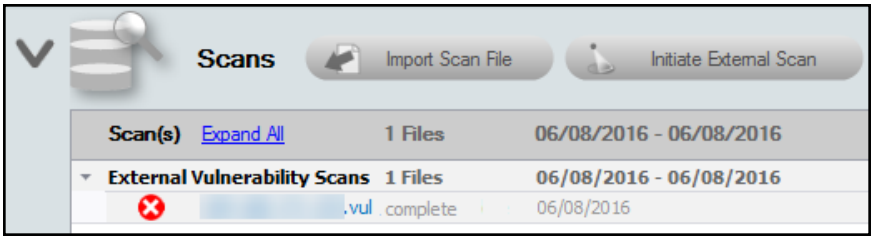
Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several

hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Scans can take several hours to complete. You will receive an e-mail when the scan is complete. Note that the **Assessment Window** will be updated to reflect the **External Vulnerability Scan** has been initiated. Refer to the list under the **Scans Bar** located within the **Assessment Window** as detailed in the figure below.



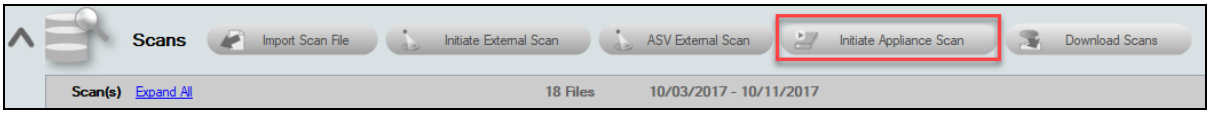
The scan's status of **0 of 1 complete** will be updated to **complete** once the scan is completed. You will also receive an email notification. The External Vulnerability Scan's **"complete"** status is shown below.



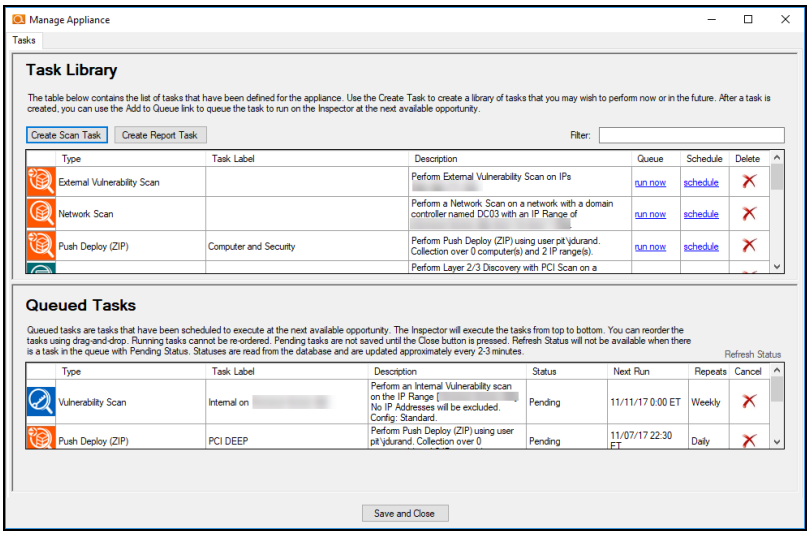
Step 3 — Initiate Internal Vulnerability Scan on the Inspector Appliance and Download Results (OPTIONAL)

The Internal Vulnerability Scan will enhance the risk assessment and risk reports by performing an internal scan looking for common vulnerabilities within the Cardholder Data Environment. The scan is initiated from the Network Detective Application. Please note that the scan may take several hours to complete.

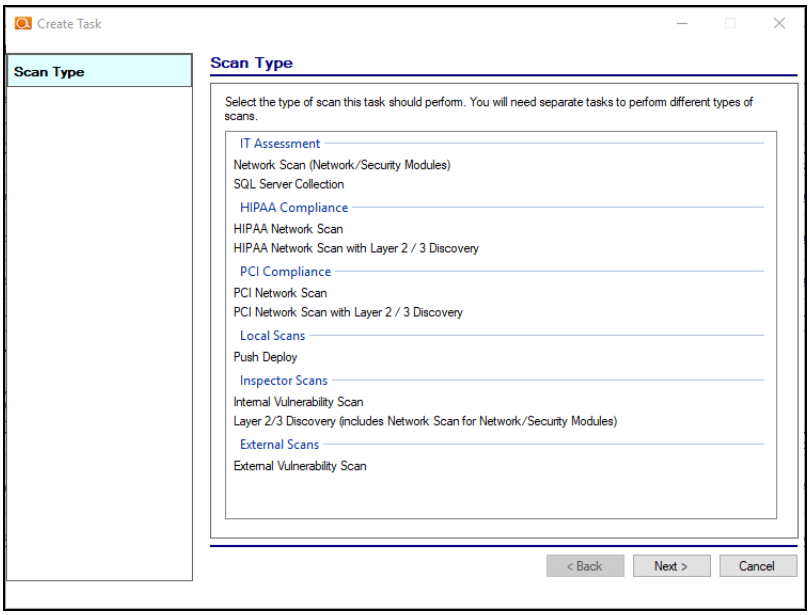
1. Click on the **Initiate Appliance Scan** button located on the Scans Bar.



2. The Manage Appliance window will appear. Click **Create Scan Task**.



3. The Create Task window will appear. Under Inspector Scans, select the **Internal Vulnerability Scan** option, and then click **Next**.



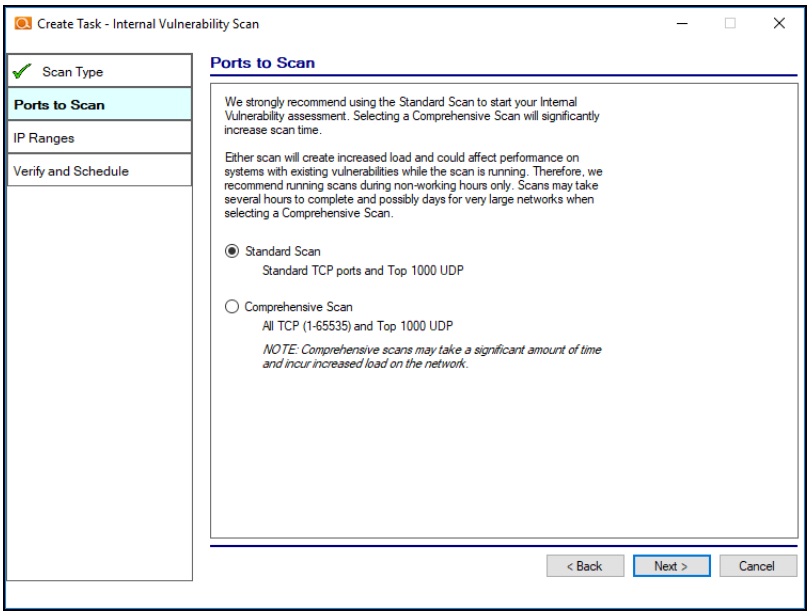
4. The Ports to Scan window will be displayed. The Ports to Scan setup option allows you to select one of two available scanning options.

   -

     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.

   - **Standard Scan** is used to scan Standard TCP ports and Top 1000 UDP ports.
   - **Comprehensive Scan** is used to execute a comprehensive scan of all TCP ports and Top 1000 UDP ports.

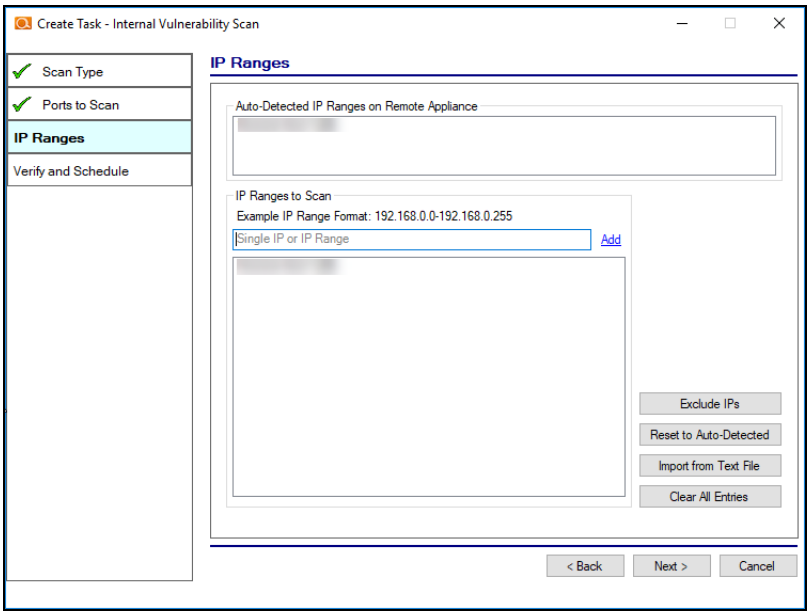
   To proceed, select the appropriate number of ports to scan for your assessment's purposes. Then click **Next**.



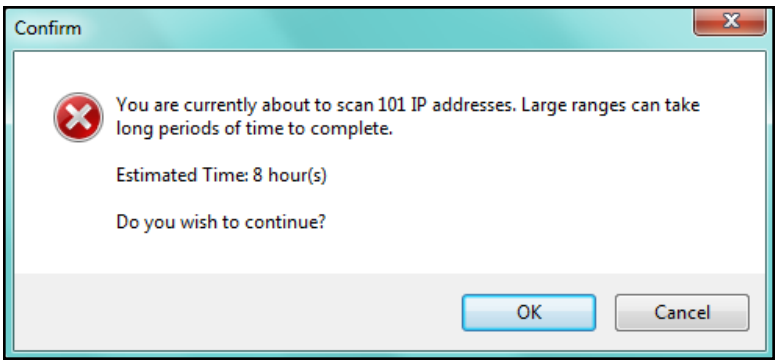
5. At this point the Network Detective PCI Module will connect with the Inspector appliance and Auto-Detect an IP address range that can be scanned. The IP Ranges screen will then be displayed. You can also manually set the IP address range that you would like to scan during the scheduled Internal Vulnerability Scan. Define the IP Range that you would like to scan and click **Next**.

Important: The Auto-Detect feature will identify the IP range of the internal subnet that is from the Inspector. This could result in a substantially larger number of IP addresses that will be scanned verses the actual number of workstations, servers, and other IP-based network components (which could be a far smaller number). If the internal vulnerability scan is configured to scan a large number of IP addresses that are not used by any device, the vulnerability scan may take much longer than necessary.

Note: To reduce the scan time, research the specific ranges of IP addresses used within the network to identify the smallest range to use for the scan.

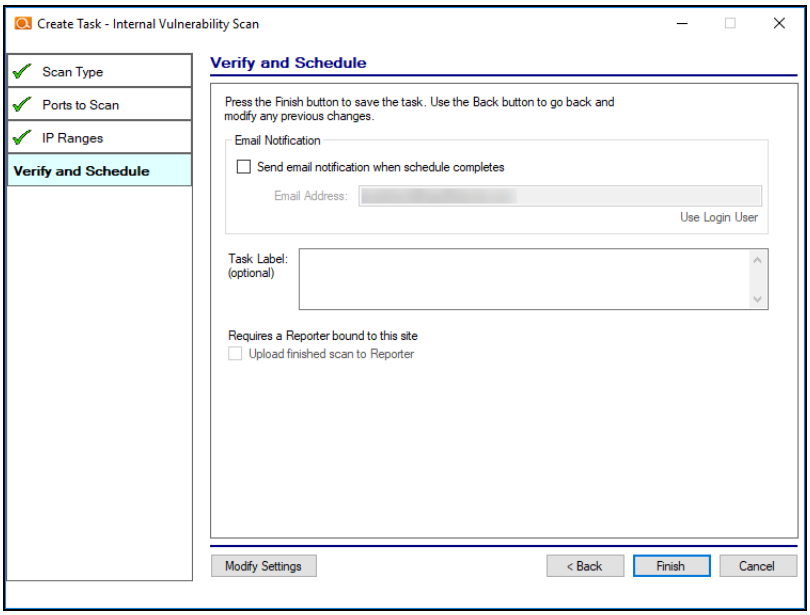


6. You will be then notified about the estimated amount of time necessary to perform the scan on the IP Range that you specified.



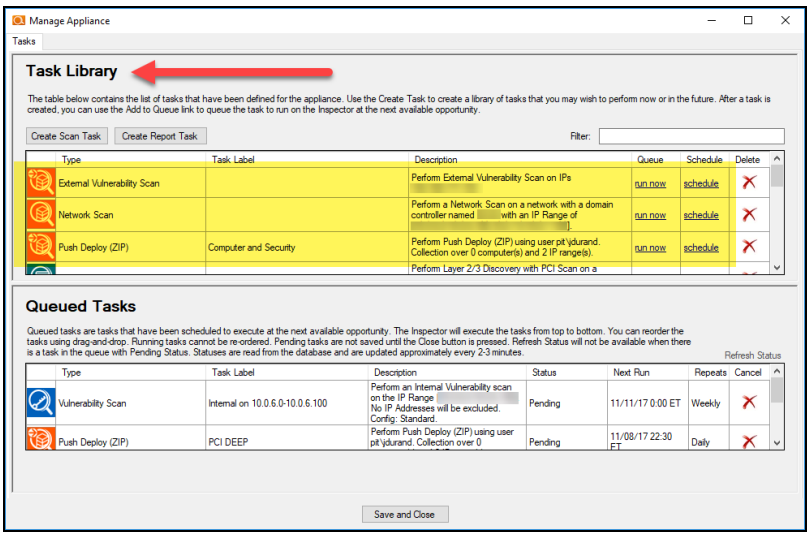
Before proceeding, be sure to note the time estimated within the Confirm Window. Click **OK**.

7. The Verify and Schedule window will be displayed. To have an Email Notification sent to you when the scan task completes, select the **Send email notification when schedule completes** option, and type in the email address where the notification should be sent.



8. Click **Finish**.

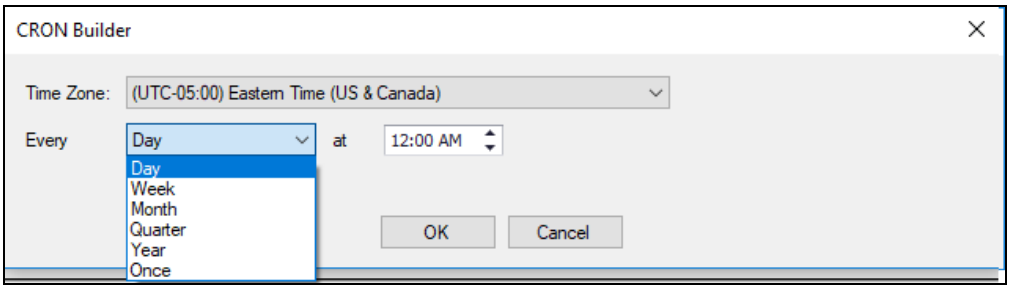
Once you create the scan task, it will appear as a task in the appliance Task Library.



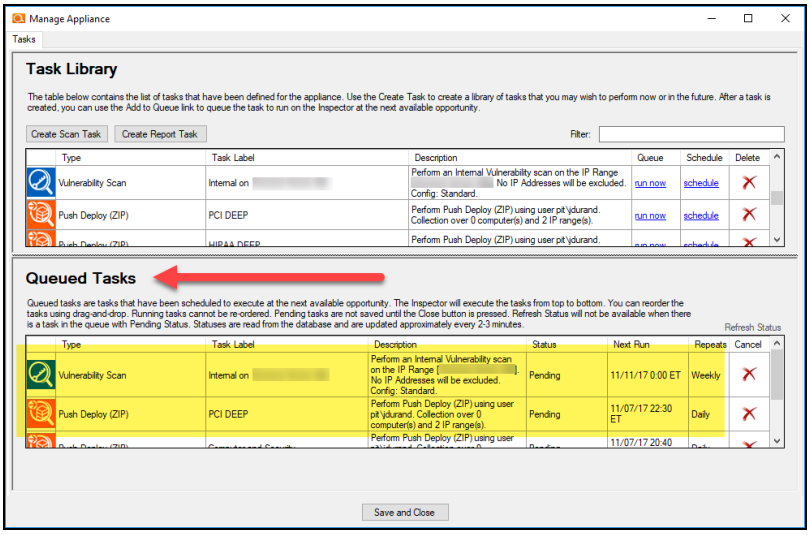
In order to initiate the scan, you will need to move the scan from the Task Library into the list of Queued Tasks. There are two ways to do this:

a. Select the **run now** option link under the Queue column to initiate the scan. This will place the scan directly into the Queued Tasks list.

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



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

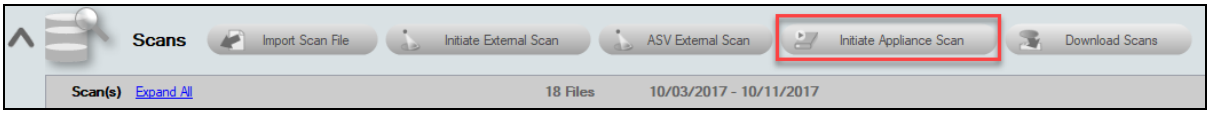


> **Tip:** Once you have placed the internal vulnerability scan task into the Queued Tasks list, you can continue on to Step 4 and Step 5 of this process. These steps allow you to and configure and schedule the required "PCI Network and Layer 2/3 Discovery Scan" and the "PCI Quick Local Collector Push Scan". After setting up and queueing the respective Step 4 and 5 scans, monitor the status of all of the scans to completion. Once the scheduled scans are completed, download each respective scan's data as instructed in this guide.

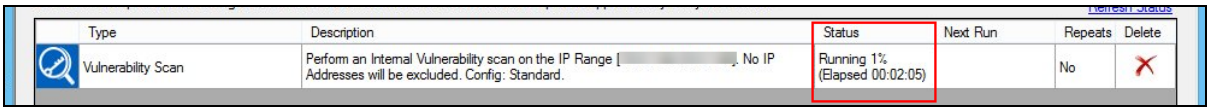
Checking Appliance Scan Execution Status

To check on the status of the scheduled appliance scan:

1. Click **Initiate Appliance Scan**.



2. View the Queued Tasks list to check the status of the scheduled scan.



The status of the scan may be set to Pending or Running along with a percentage of the task's performance completion as illustrated in the window below.

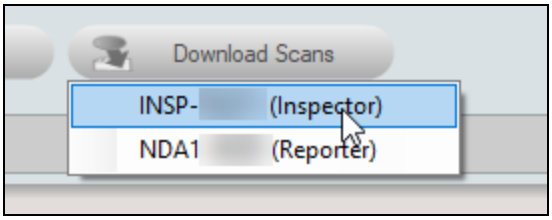
When the scan task is completed, the task will be removed from the Queued Tasks list. You can then download the scan and merge it into your assessment project.

Download Appliance Scans

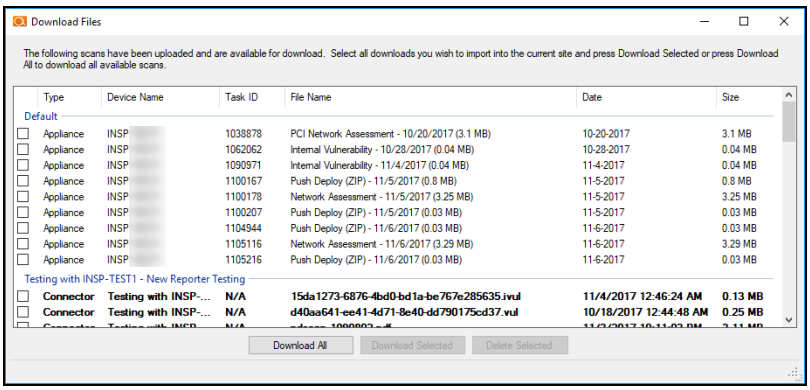
Once the scan is completed, download the scan and merge it into your assessment project. To do this:

1. Click **Download Scans** from the Scans bar.

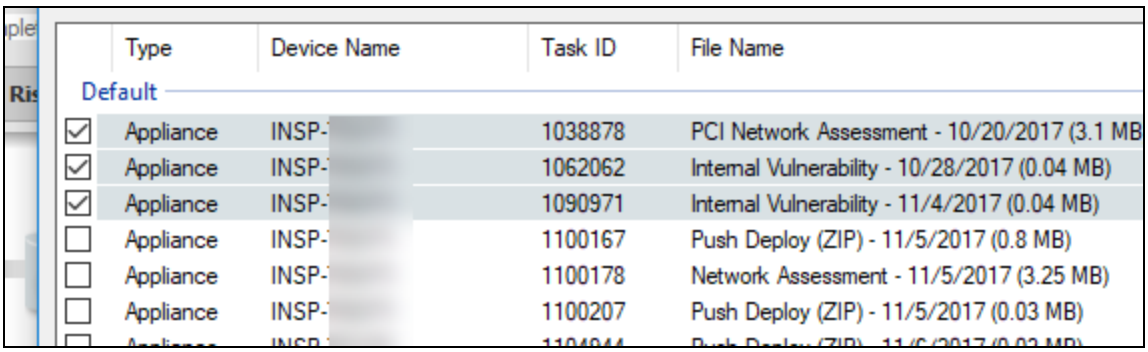
2. Select the appliance for which you would like to download scans.



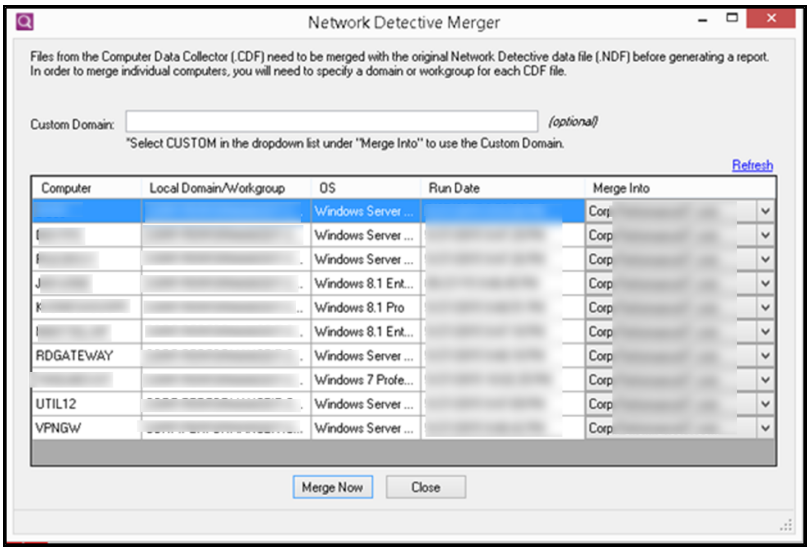
3. The Download Files window will appear. Here you can see a list all of the scans that an appliance has performed for a given Site.



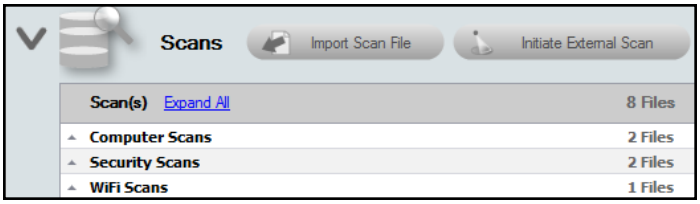
4. Select the check box next to the scan file you wish to download then select the **Download Selected** button. The file will then be downloaded and imported into the assessment.



5. If prompted, merge the scans into the assessment using the Network Detective Merger. Click **Merge Now** to perform the merge.



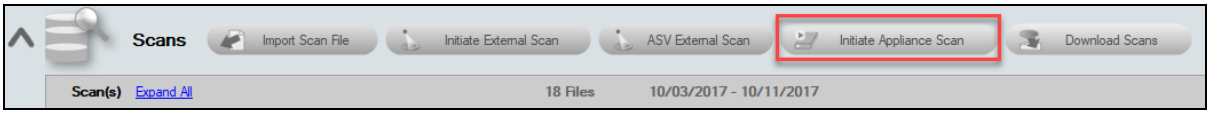
The imported scans will appear as files under the Scans bar.



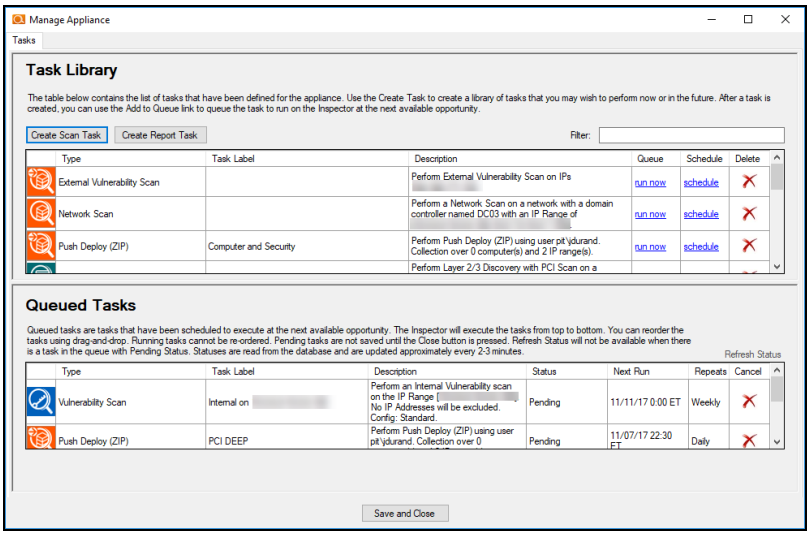
Step 4 — Initiate the PCI Network Scan with Layer 2/3 Discovery on the Inspector Appliance and Download Results

The PCI Network Scan with Layer 2/3 Discovery enhances the PCI risk assessment and risk reports by performing an internal scan looking for and identifying all network devices. The scan is initiated from the Network Detective Application. Please note that the scan may take several hours to complete.

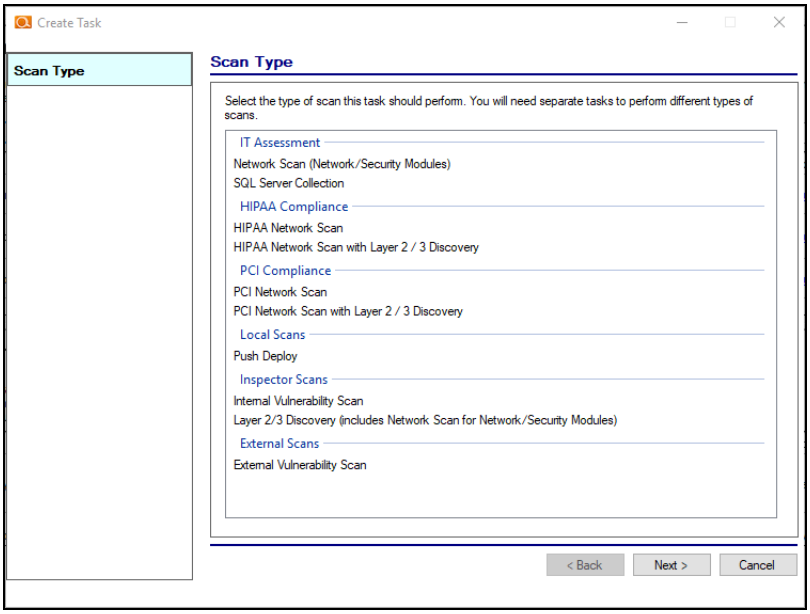
1. Click on the **Initiate Appliance Scan** button located on the Scans Bar.



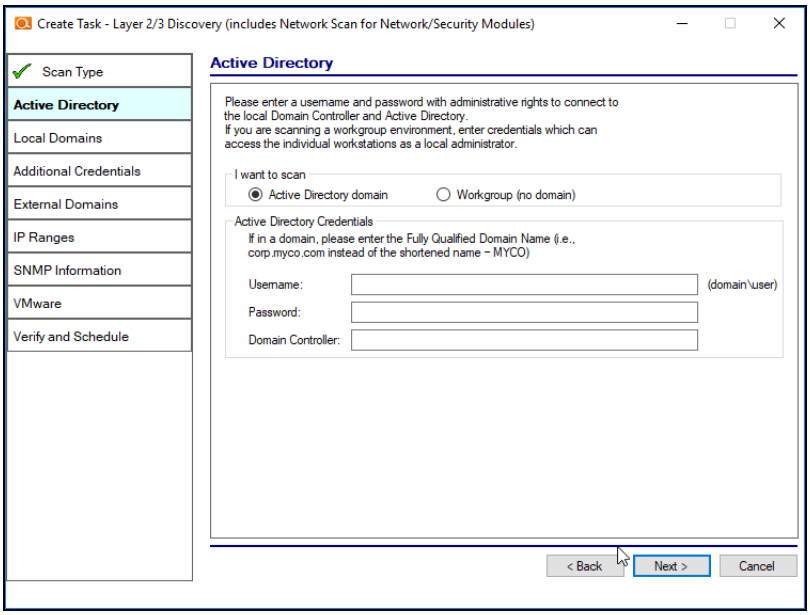
2. The Manage Appliance window will appear. Click **Create Scan Task**.



3. The Create Task window will appear. Under PCI Compliance Scans, select the **PCI Network Scan with Layer 2/3 Discovery** option, and then click **Next**.

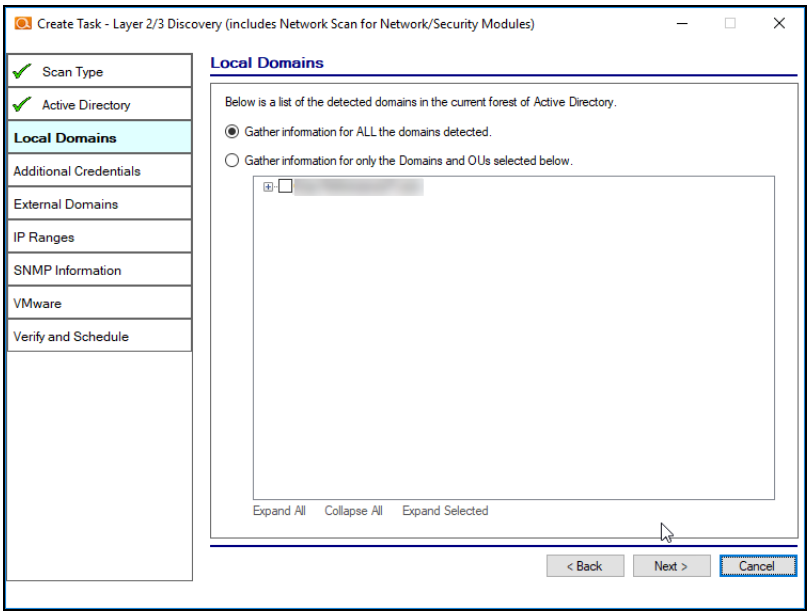


4. The Create Task window will be displayed in order to configure the Layer 2/3 scan's parameters. From the Active Directory window, **select the type of network you are scanning** (either an Active Directory domain or Workgroup). Then you can **enter the administrative credentials** necessary to access the network environment during the scanning process. Then click **Next**.

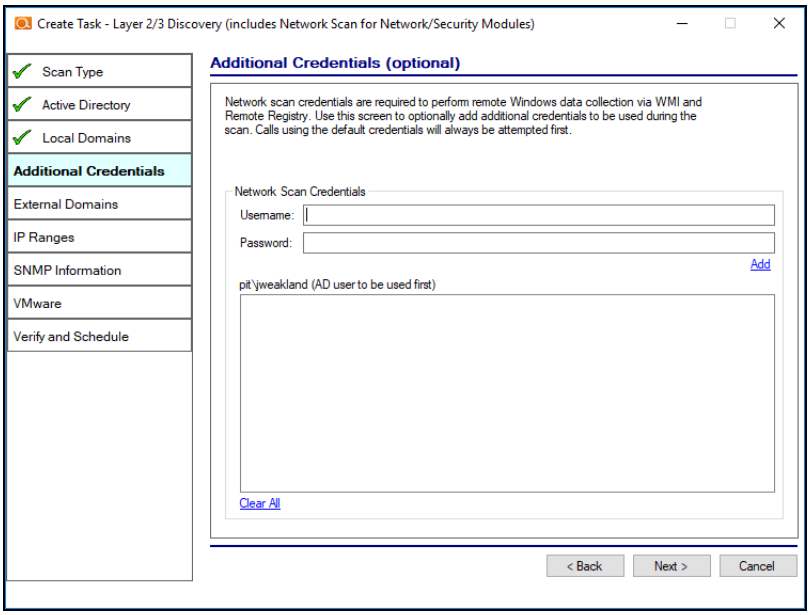


5. The Local Domains window will appear. Select to gather information from ALL domains detected or from Domains and OUs you select. Click **Next** and confirm your selection.

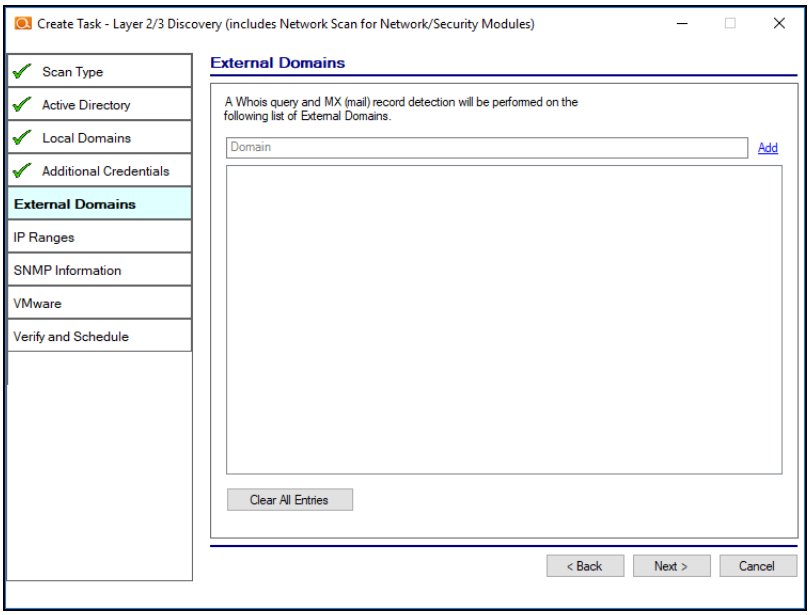
> **Note:** Note: If you select to scan a Workgroup, then the Local Domains select step in this process will be skipped.



6. The Additional Credentials window will appear. If necessary, enter the required additional credentials to perform remote Windows data collection via WMI and Remote Registry. **Click** Next.

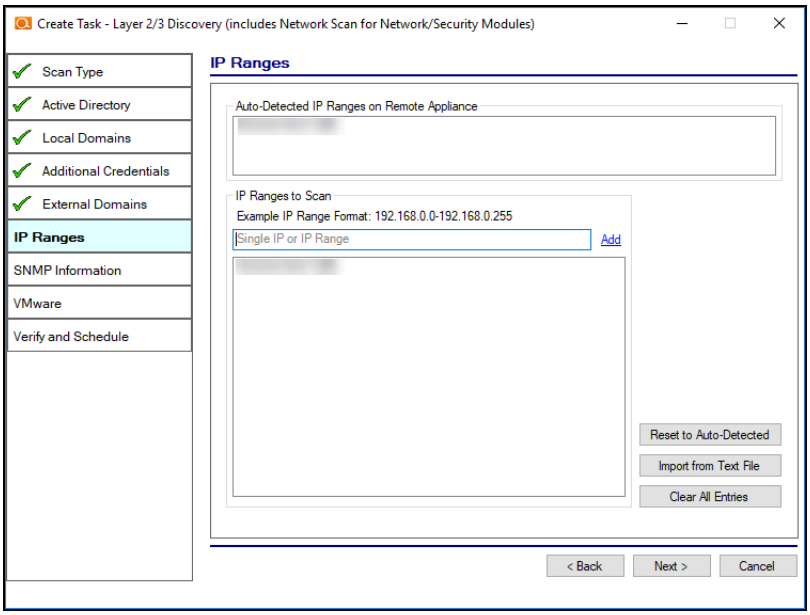


7. The External Domains screen will be presented. Enter the name(s) of the organization's external domains. A Whois query and MX (mail) record detection will be performed upon selecting the **Next** button.

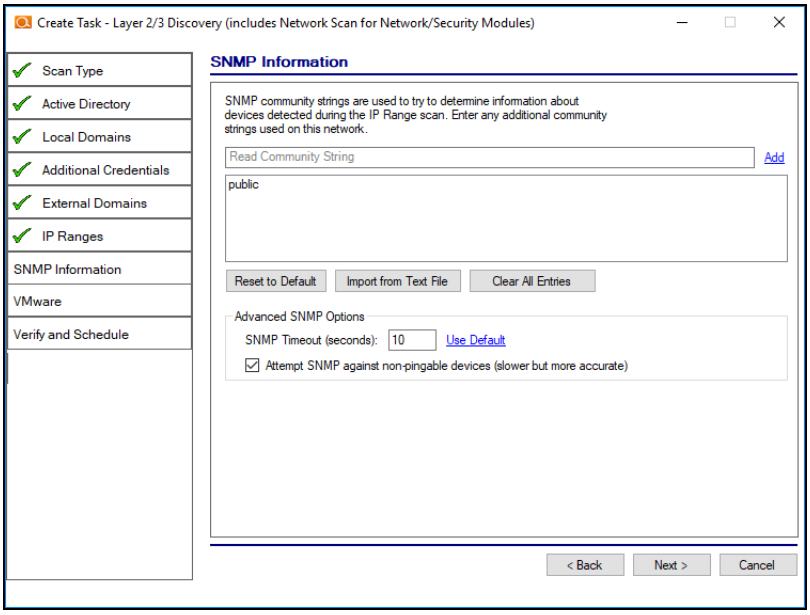


If you do not select any external domains, confirm that you wish to proceed.

8. Next, the IP Address Ranges screen will be presented. Enter the starting and ending IP addresses for the range(s) you want to scan in the Starting IP Address field and the Ending IP Address field under the IP Ranges to Scan list.

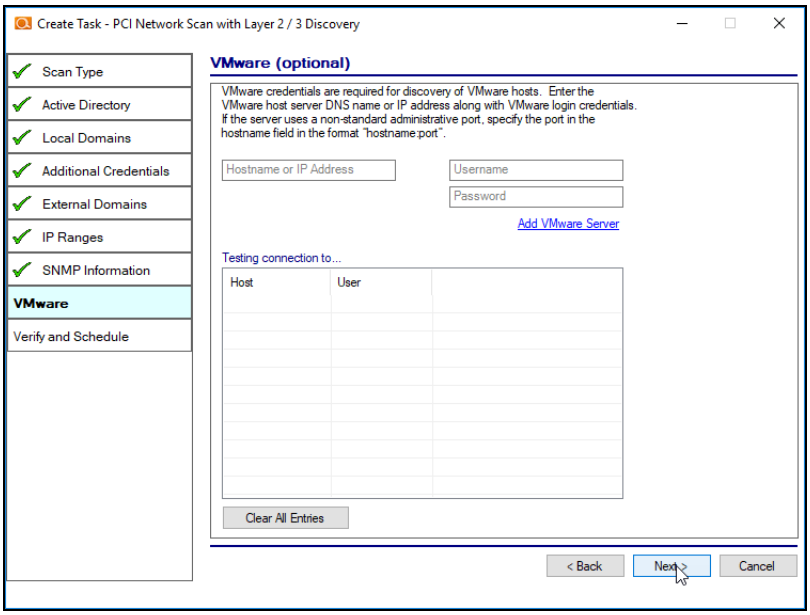


9. The SNMP Information screen will be presented. Enter any additional community strings used on the network. Then click on the **Next** button.

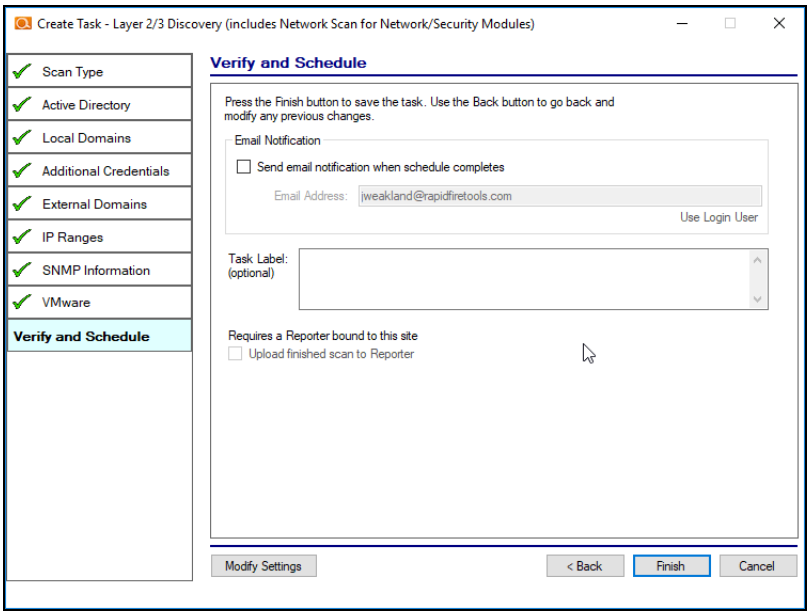


Important: As of 9/28/2018, the Microsoft Base Security Analyzer (MBSA) has been removed from the Data Collector. MBSA is in the process of being deprecated by Microsoft. Microsoft no longer supports MBSA in newer versions of Windows (i.e. v10 and Windows Server 2016). MSBA is only useful for earlier 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.

10. The VMWare credentials screen will appear. Enter the hostname or IP Address for the VMWare host. Then enter login credentials. Click **Add VMWare Server**. When you have finished adding VMWare servers, click **Next**.

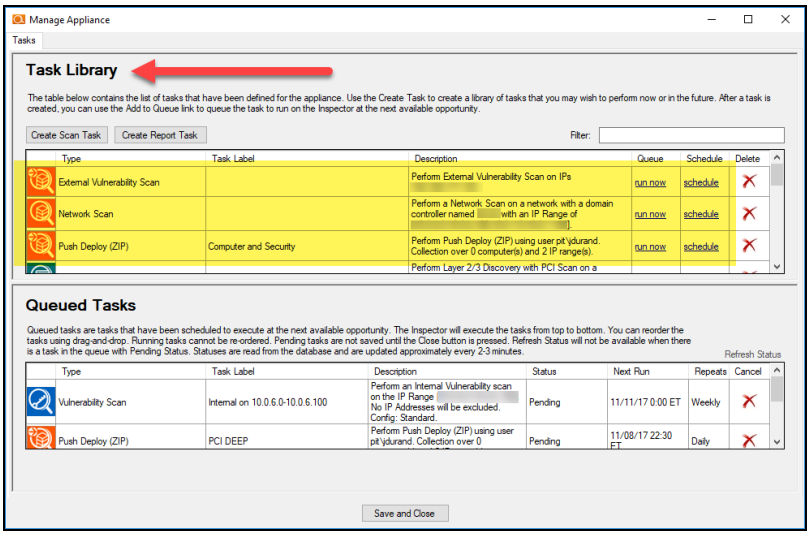


11. The Verify and Schedule window will appear. To have an Email Notification sent to you when the scan task completes, select the **Send email notification when schedule completes** option, and next type in the email address where the notification should be sent. Click on the Finish button to complete the scheduling of the PCI Network Scan with Layer 2/3 Discovery scan task.



12. Click **Finish**.

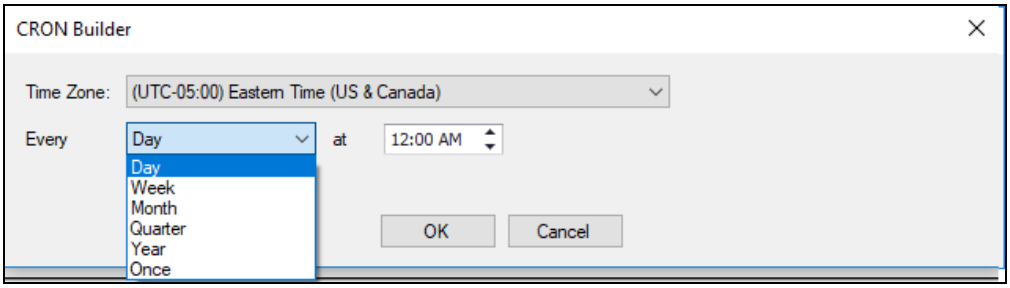
13. Once you create the scan task, it will appear as a task in the appliance Task Library.



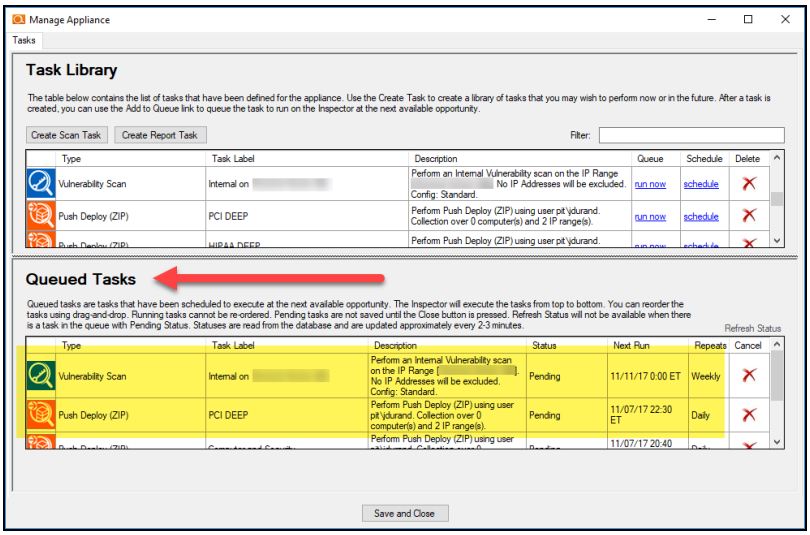
In order to initiate the scan, you will need to move the scan from the Task Library into the list of Queued Tasks. There are two ways to do this:

a. Select the **run now** option link under the Queue column to initiate the scan. This will place the scan directly into the Queued Tasks list.

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



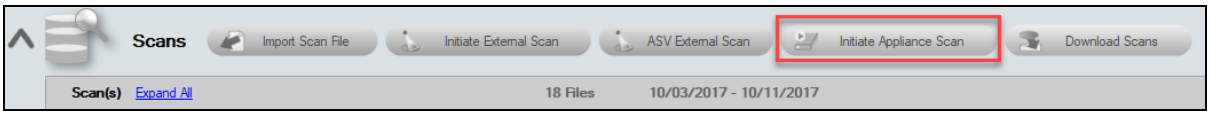
Whether you choose to run the scan now or schedule the scan to take place in the future, it will be added to the Queued Tasks list, where you can check its status. This is the final step in initiating (or scheduling) a scan.



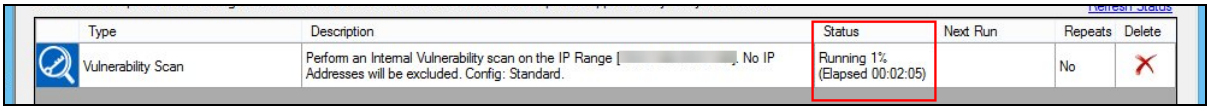
Checking Appliance Scan Execution Status

To check on the status of the scheduled appliance scan:

1. Click **Initiate Appliance Scan**.



2. View the Queued Tasks list to check the status of the scheduled scan.



The status of the scan may be set to Pending or Running along with a percentage of the task's performance completion as illustrated in the window below.

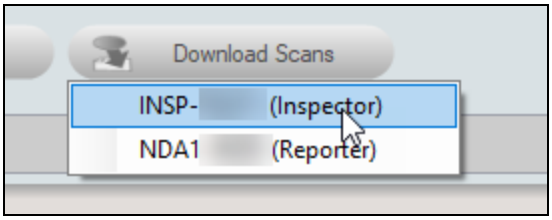
When the scan task is completed, the task will be removed from the Queued Tasks list. You can then download the scan and merge it into your assessment project.

Download Appliance Scans

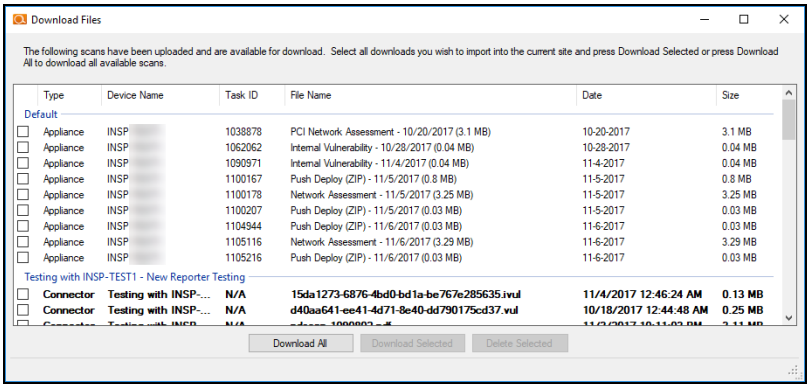
Once the scan is completed, download the scan and merge it into your assessment project. To do this:

1. Click **Download Scans** from the Scans bar.

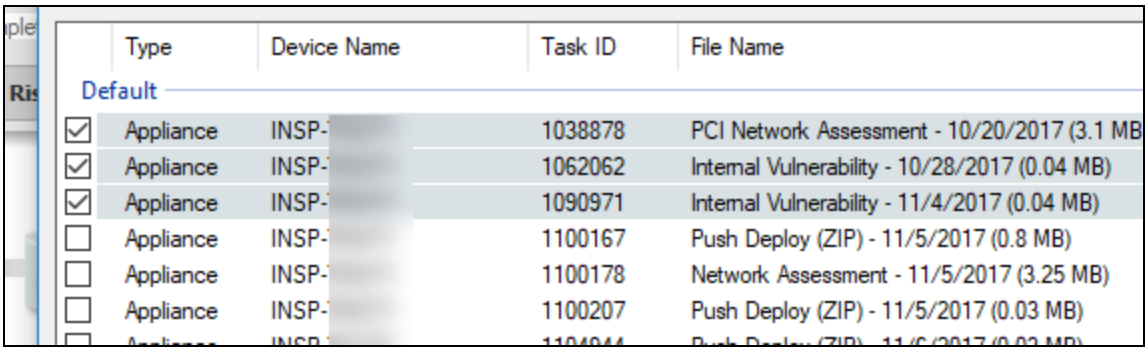
2. Select the appliance for which you would like to download scans.



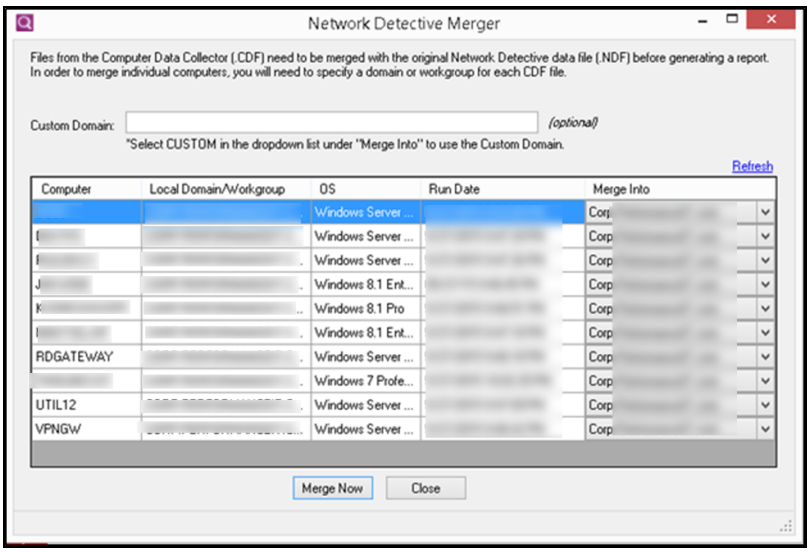
3. The Download Files window will appear. Here you can see a list all of the scans that an appliance has performed for a given Site.



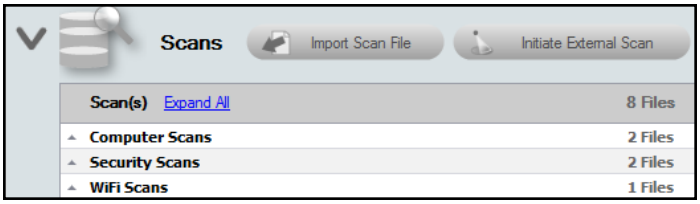
4. Select the check box next to the scan file you wish to download then select the **Download Selected** button. The file will then be downloaded and imported into the assessment.



5. If prompted, merge the scans into the assessment using the Network Detective Merger. Click **Merge Now** to perform the merge.



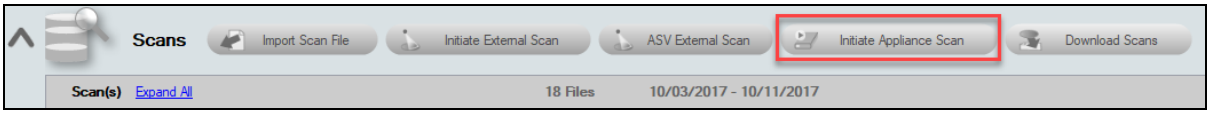
The imported scans will appear as files under the Scans bar.



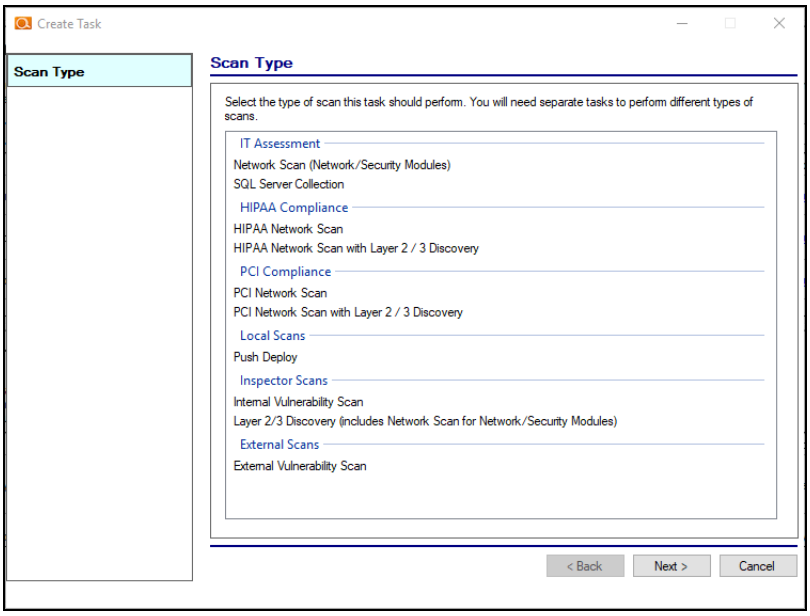
Step 5 — Initiate Push Quick Local Scans for PCI on the Inspector Appliance and Download Results

A full PCI assessment requires running the Local Computer Data Collector on all computers. Use the Inspector Appliance to Push Quick Local Scan for PCI to all devices within the cardholder data environment. This task is initiated from within the Network Detective Application. Please note that the scan may take several hours to complete.

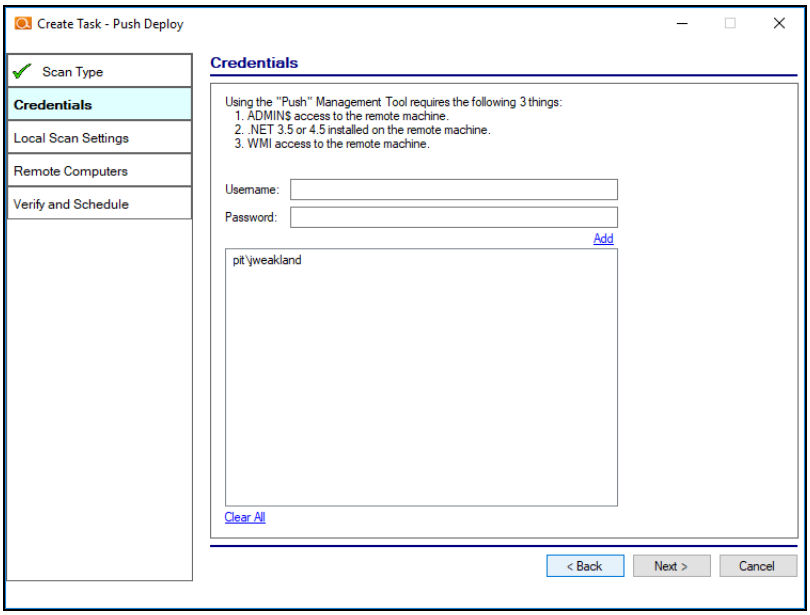
1. Click on the **Initiate Appliance Scan** button located on the Scans Bar to initiate the scheduling of Push Quick Local Scan(s) for PCI scan task.



2. The Create Task window will be displayed. Select the **Push Deploy** under Local Scans. Click **Next**.



3. The Credentials window will appear.



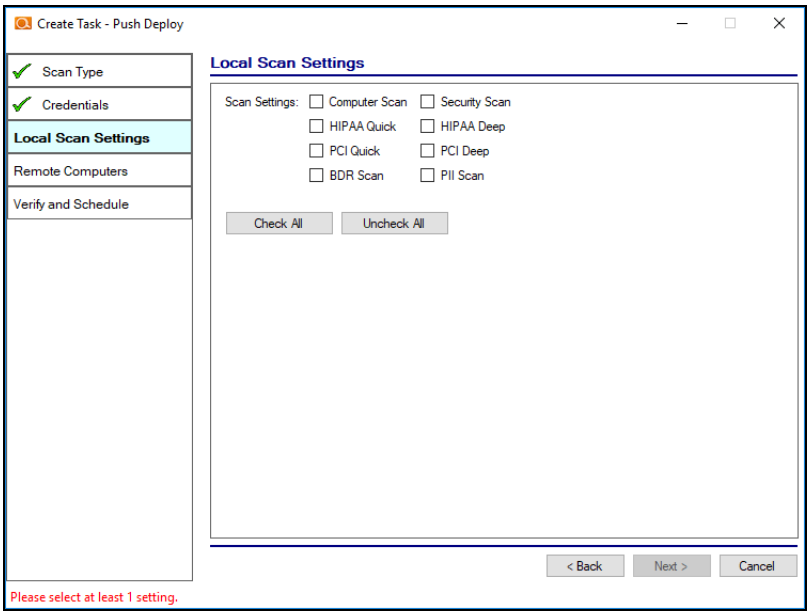
This window details the prerequisites and requirements that must be met to enable a Push Quick Local Scans for PCI task to be scheduled and executed successfully. Please note them carefully before you proceed.

These are:

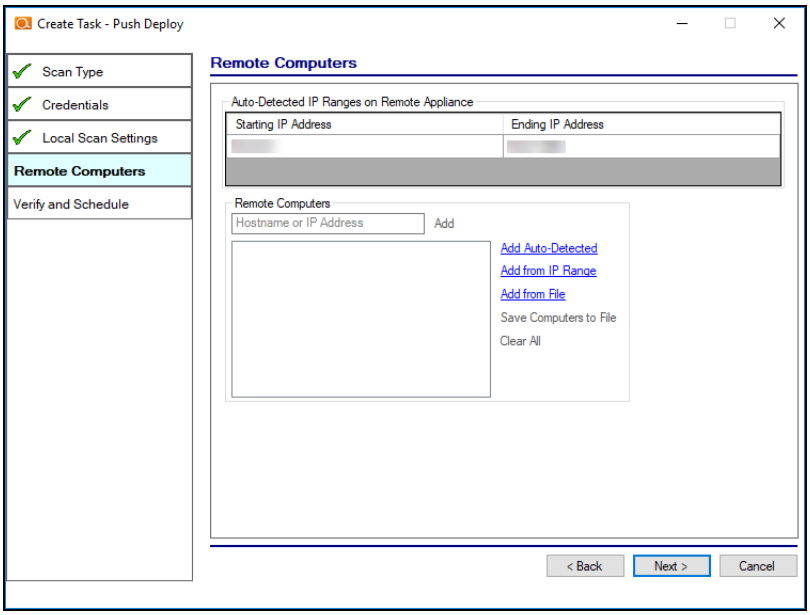
- ADMIN$ access to the remote machine
- .NET 4.6.2 installed on the remote machine
- WMI access to the remote machine

After validating that the “Push” Management Tool requirements have been met, enter credentials with administrative rights. Click **Next**.

4. From the Local Scan settings window, select PCI Quick Scan. Click **Next**.

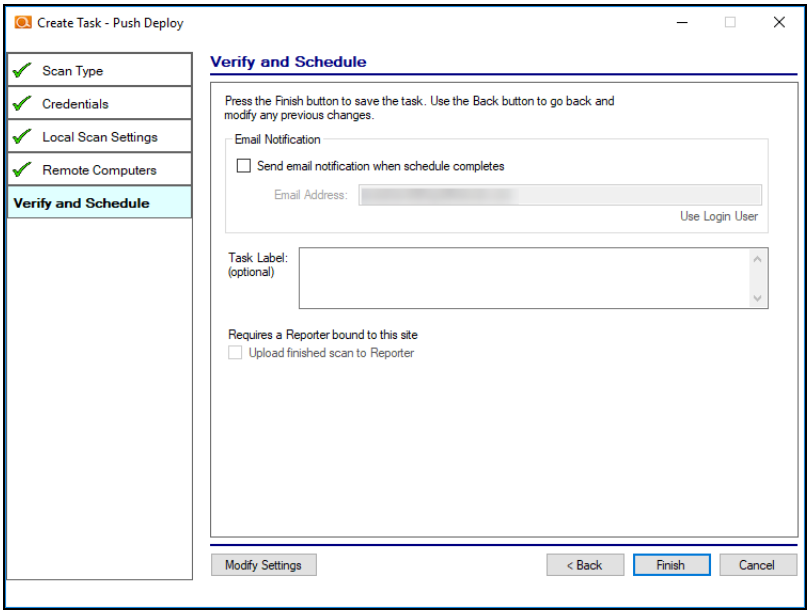


5. The Remote Computers screen will appear. Select **Add Auto-Detected**, **Add from IP Range**, or **Add from File** to add one or more computer Hostnames or IP addresses. Once the Remote Computers are identified and added, these computers will be listed in the list-box control. Click **Next**.

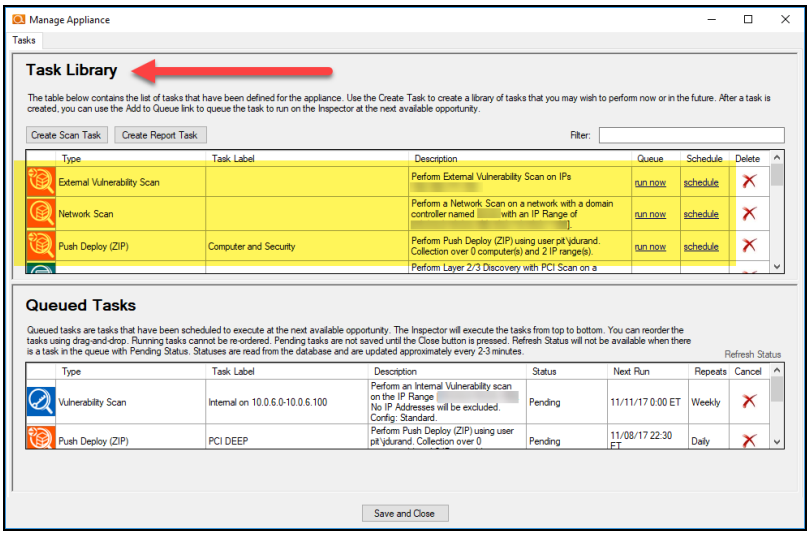


6. Verify and schedule the scan. To have an Email Notification sent to you when the push and scan task completes, select the “Send email notification when schedule

completes" option, and type in the email address where the notification should be sent. Click **Finish**.



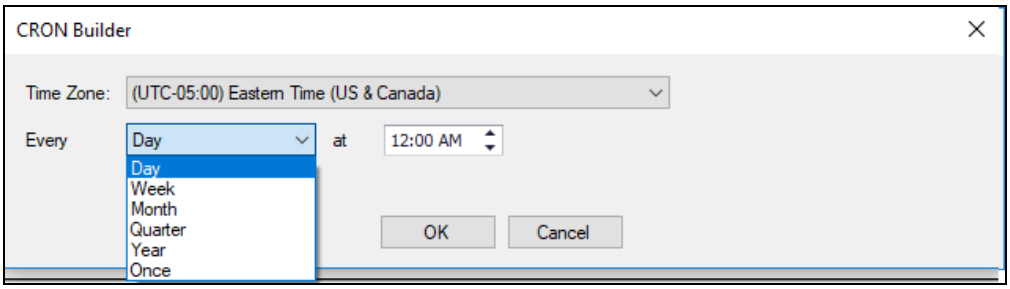
7. Once you create the scan task, it will appear as a task in the appliance Task Library.



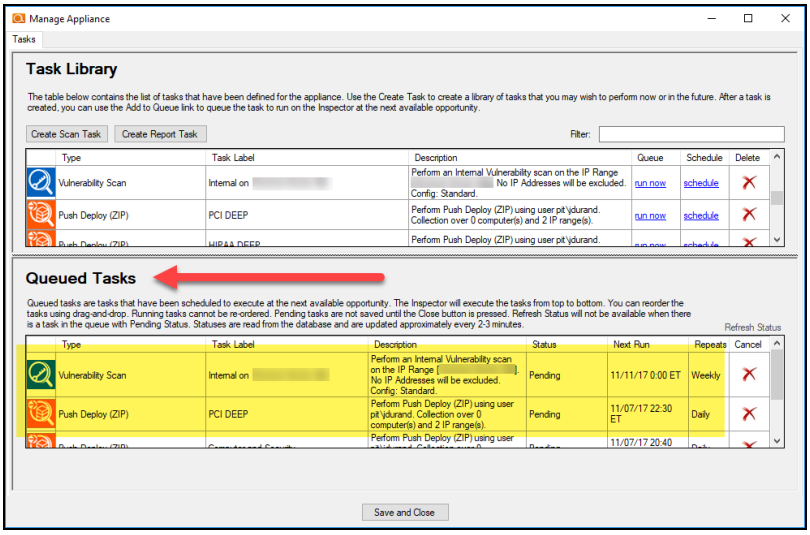
In order to initiate the scan, you will need to move the scan from the Task Library into the list of Queued Tasks. There are two ways to do this:

a. Select the **run now** option link under the Queue column to initiate the scan. This will place the scan directly into the Queued Tasks list.

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



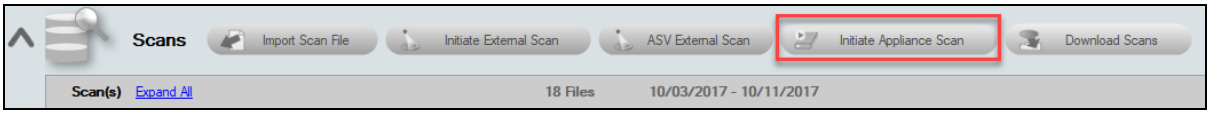
Whether you choose to run the scan now or schedule the scan to take place in the future, it will be added to the Queued Tasks list, where you can check its status. This is the final step in initiating (or scheduling) a scan.



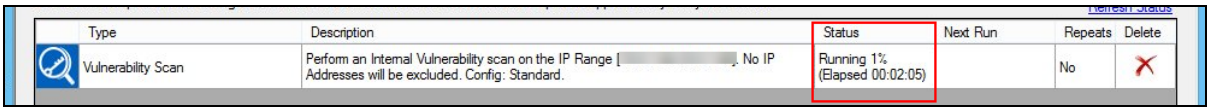
Checking Appliance Scan Execution Status

To check on the status of the scheduled appliance scan:

1. Click **Initiate Appliance Scan**.



2. View the Queued Tasks list to check the status of the scheduled scan.



The status of the scan may be set to Pending or Running along with a percentage of the task's performance completion as illustrated in the window below.

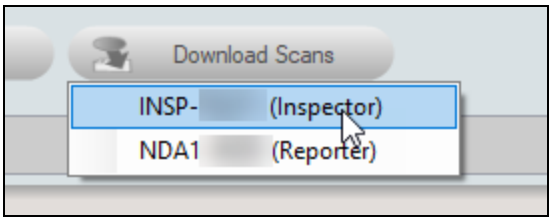
When the scan task is completed, the task will be removed from the Queued Tasks list. You can then download the scan and merge it into your assessment project.

Download Appliance Scans

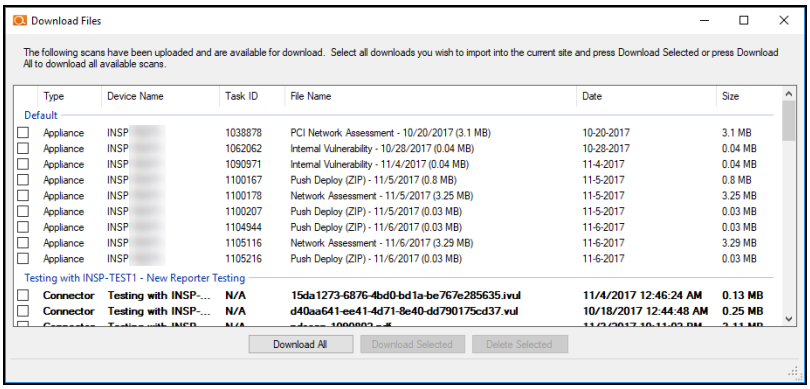
Once the scan is completed, download the scan and merge it into your assessment project. To do this:

1. Click **Download Scans** from the Scans bar.

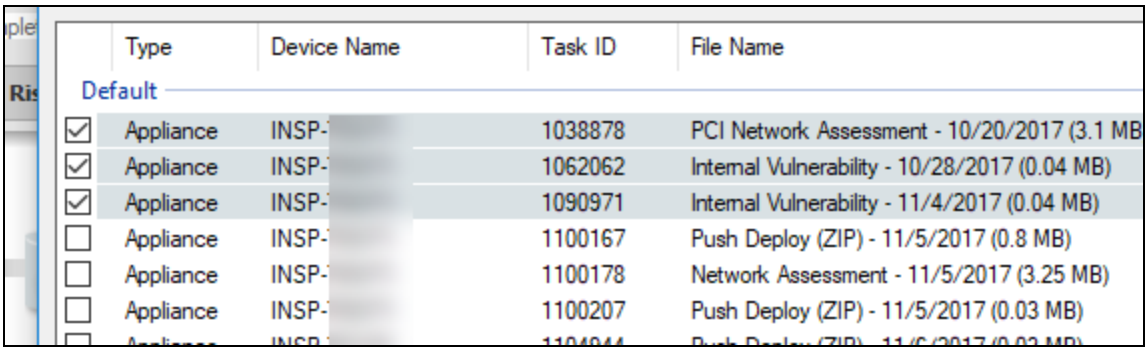
2. Select the appliance for which you would like to download scans.



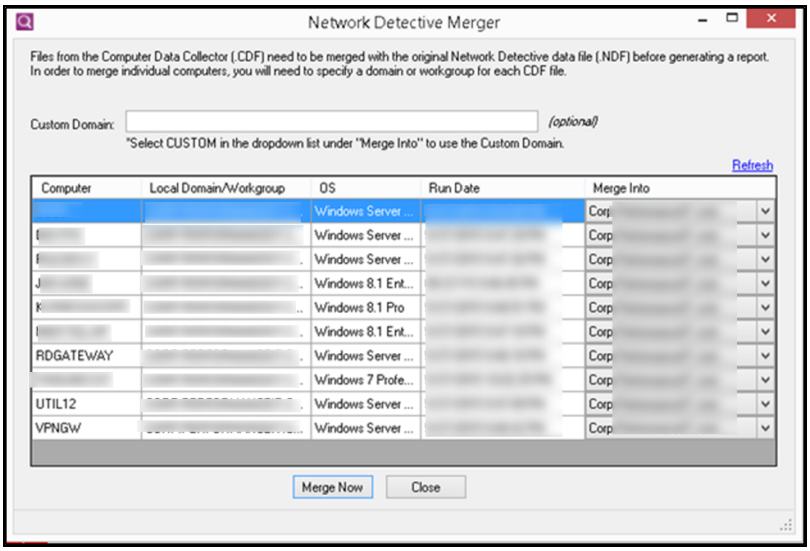
3. The Download Files window will appear. Here you can see a list all of the scans that an appliance has performed for a given Site.



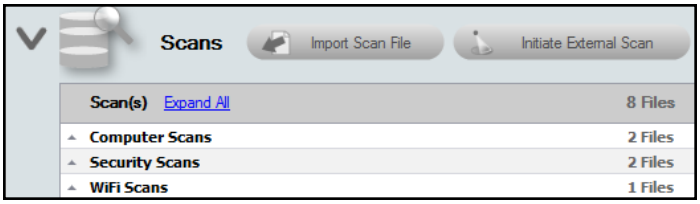
4. Select the check box next to the scan file you wish to download then select the **Download Selected** button. The file will then be downloaded and imported into the assessment.



5. If prompted, merge the scans into the assessment using the Network Detective Merger. Click **Merge Now** to perform the merge.



The imported scans will appear as files under the Scans bar.

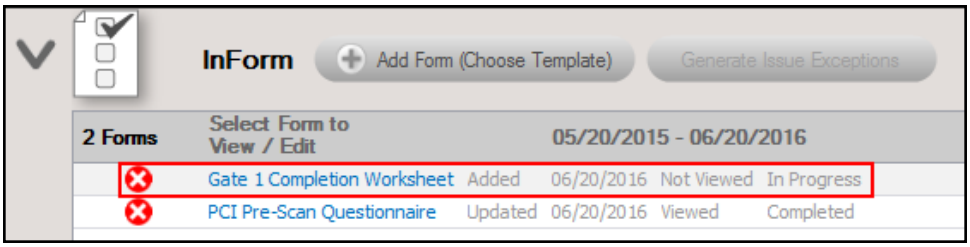


Step 6 — Gate 1 Completion Worksheet

After completing the initial phase of the PCI assessment process, the **Gate 1 Completion Worksheet** is added to the **InForm** section of the **Assessment Window**. The worksheet is listed below the **Inform Bar** at the bottom of the **Assessment Window**. The purpose of the **Gate 1 Completion Worksheet** is to confirm that the initial phase of the PCI assessment has been performed, including all optional scans, before proceeding to the next phase of the assessment process.

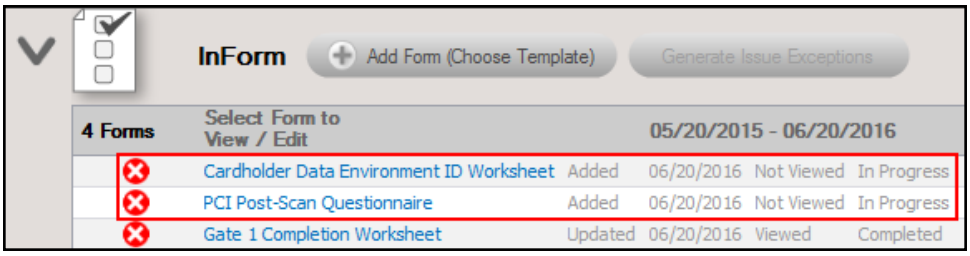
To open and complete the **Gate 1 Completion Worksheet**:

1. Click on the **name label** for the **Gate 1 Completion Worksheet** entry in the **InForm** Questionnaire/Worksheet list located below the **InForm Bar** at the bottom of the **Assessment** window.



2. If you are ready to proceed to the next step in the assessment process, complete this worksheet by selecting the **Yes** response in the **Response** field and **Save** the worksheet.

   The **Checklist** will then be updated to include the additional work items that must be completed.



Step 7 — Run PCI Data Collector selecting Quick Local Scan on the Computers that Were Unreachable (OPTIONAL)

Using the **PCI Data Collector**, run the local scan any computers that cannot be scanned remotely (i.e. blocked by a firewall, not connected to the domain, or otherwise inaccessible).

> **Note:** If you do not need to scan any computers that were unreachable, then skip this step.

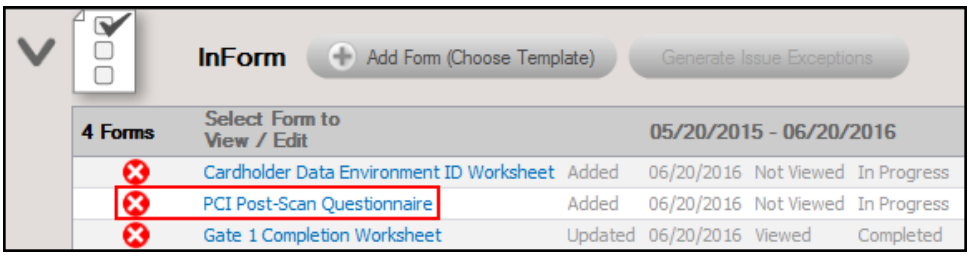
Use the **PCI Data Collector** to run the **PCI Quick Local Scan** on selected computer systems manually.

To use the PCI Data Collector to run the Quick Local Scan, please refer to "Run the PCI Computer Data Collector — “Quick” Local Computer Scan " on page 90.

Step 8 — Complete the PCI Post-Scan Questionnaire

The **PCI Post-Scan Questionnaire** contains questions that have been developed as a result of the PCI Data Collector's scans. These questions help build a comprehensive assessment. Your answers will be included in the appropriate reports.

To access the PCI Post-Scan Questionnaire, click on the **name label** for the PCI Post-Scan Questionnaire listed below the **Inform Bar** located at the bottom of the Assessment Window.



Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

Cardholder Data Environment (CDE) Deep Scan

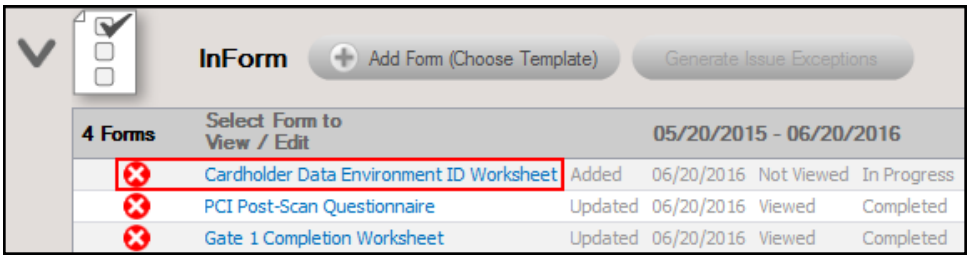
In this critical phase of the PCI assessment process, there are both Worksheets and Scans that must be completed and performed in order to accomplish the goal of assessing PCI compliance of the Cardholder Data Environment system components and computers.

Step 9 — Complete Cardholder Data Environment ID Worksheet

The **Cardholder Data Environment ID Worksheet** contains a list of the system components that have been identified during the network scan phase of the automated data collection. The system components identified are operating within a particular domain or workgroup and also include non-domain devices.

In this worksheet, you document the purpose of the equipment identified, if the equipment is part of the Cardholder Data Environment (CDE), and if the equipment is within the scope of PCI compliance requirements. Alternatively, you can confirm that the equipment components are not part of the CDE.

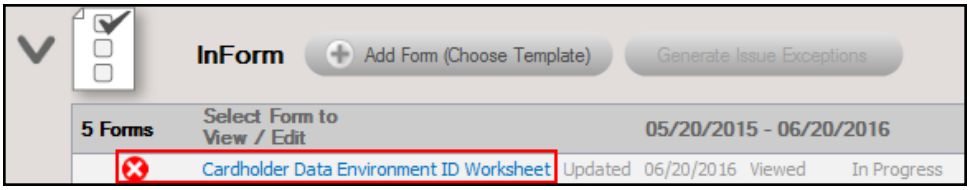
To access the Cardholder Data Environment ID Worksheet, click on the **name label** for the **Cardholder Data Environment ID Worksheet** listed below the InForm bar located at the bottom of the Assessment Window here:



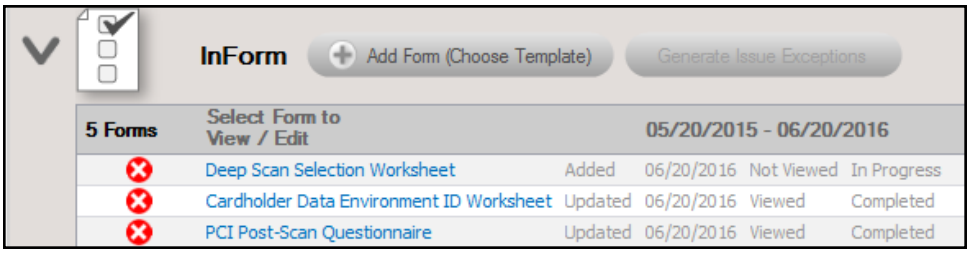
For each device, either the machine name or IP address of the device is displayed in the **Topic** column. Additional details about the devices listed in the worksheet are documented in the **Notes** field, including OS version, IP address, Description data, and possibly a CPU version.

> **Tip:** See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

You can return to the Cardholder Data Environment ID Worksheet by clicking on the name label for the Cardholder Data Environment ID Worksheet located under the InForm Bar at the bottom of the Assessment Window.



After saving the Cardholder Data Environment ID Worksheet, the list of questionnaires and worksheets in the InForm section of the Assessment Window is updated to include the Deep Scan Selection Worksheet.



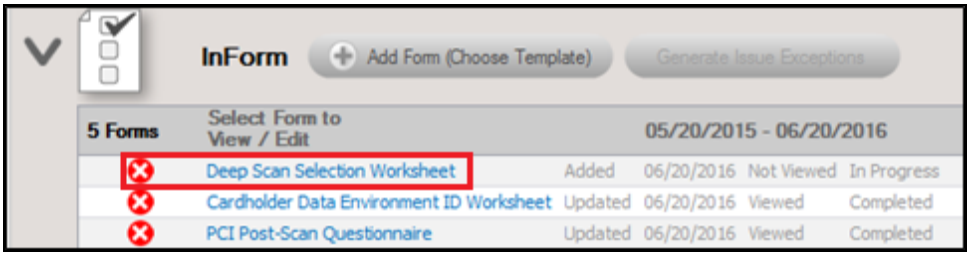
Step 10 — Complete Deep Scan Selection Worksheet

Use the Deep Scan Selection to worksheet to choose which computers to scan using the Push Deploy Tool.

The PCI “Deep Scan”, which includes a process to search for Primary Account Number (PAN) data (i.e. Cardholder Data) on workstations and servers, should be run on all computers in the Cardholder Data Environment (CDE) that can be accessed along with a sampling of computers outside of the CDE. The PCI Deep Scan determines if PAN data is potentially present on any IT system workstation or server.

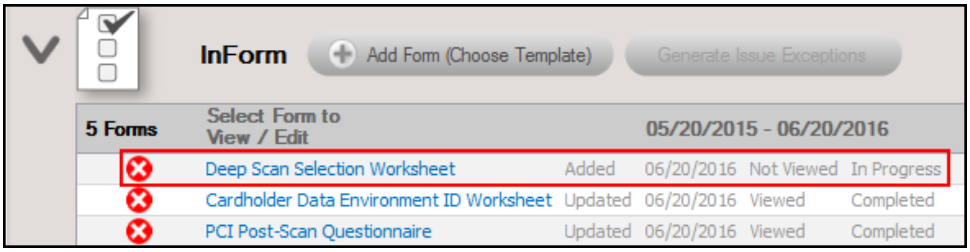
The Deep Scan Selection Worksheet helps you define the computers that should be referenced in the IP Range/Hostname field of the PCI Deep Scan process using the Push Deploy Tool detailed in the next step.

After completing the initial phase of the PCI assessment process, the **Deep Scan Selection Worksheet** is added to the **InForm** section of the **Assessment Window**.



Note: The computers selected in this worksheet will be scanned using the **PCI Data Collector Computer Scan** with the **Deep Scan** mode turned on so that a detailed search for files containing PAN data is undertaken during the scanning process.

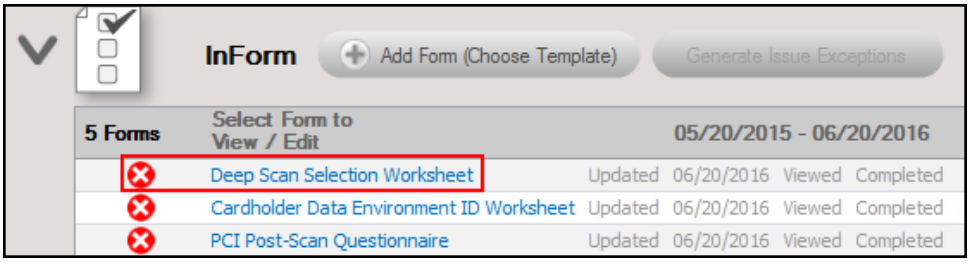
To select which systems are to be scanned by the **Deep Scan** process, click on the **name label** for the **Deep Scan Selection Worksheet** located under the Inform bar located at the bottom of the Assessment window here:



Save your answers periodically and **Save and Close** when you are done.

Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

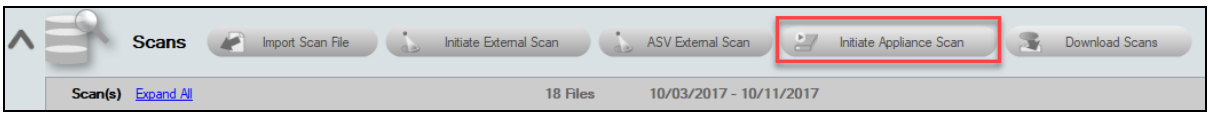
You can return to the **Deep Scan Selection Worksheet** by clicking on the **name label** for the **Deep Scan Selection Worksheet** located under the Inform bar at the bottom of the Assessment Window.



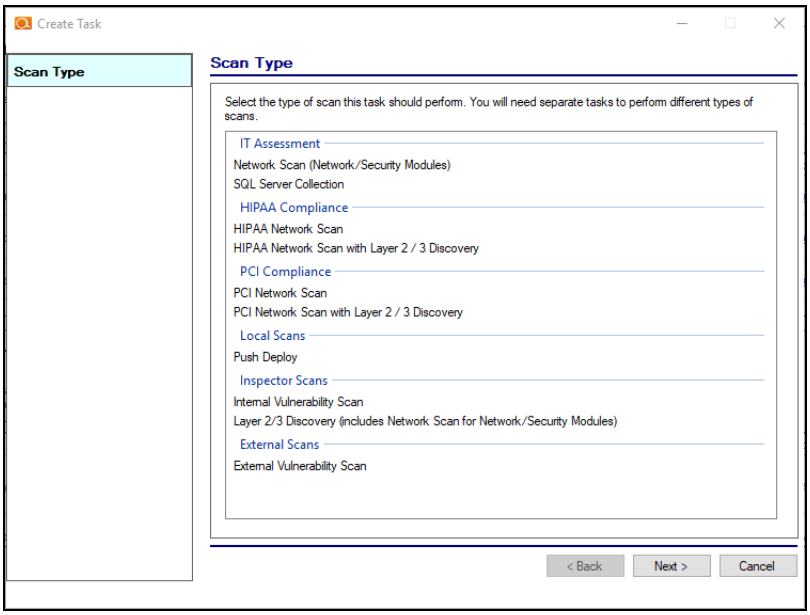
Step 11 — Initiate Push Deep Local Scans for PCI on the Inspector Appliance and Download Results

A full PCI assessment requires running the Local Computer Data Collector on all computers. Use the Inspector Appliance to Push Deep Local Scan for PCI to all devices within the cardholder data environment. This task is initiated from within the Network Detective Application. Please note that the scan may take several hours to complete.

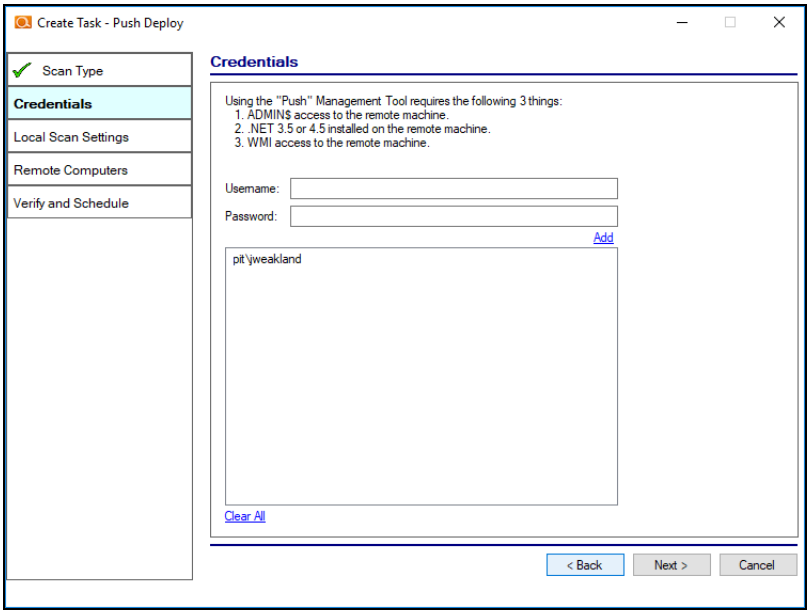
1. Click on the **Initiate Appliance Scan** button located on the Scans Bar to initiate the scheduling of Push Deep Local Scan(s) for PCI scan task.



2. The Create Task window will be displayed. Select the **Push Deploy** under Local Scans. Click **Next**.



3. The Credentials window will appear.



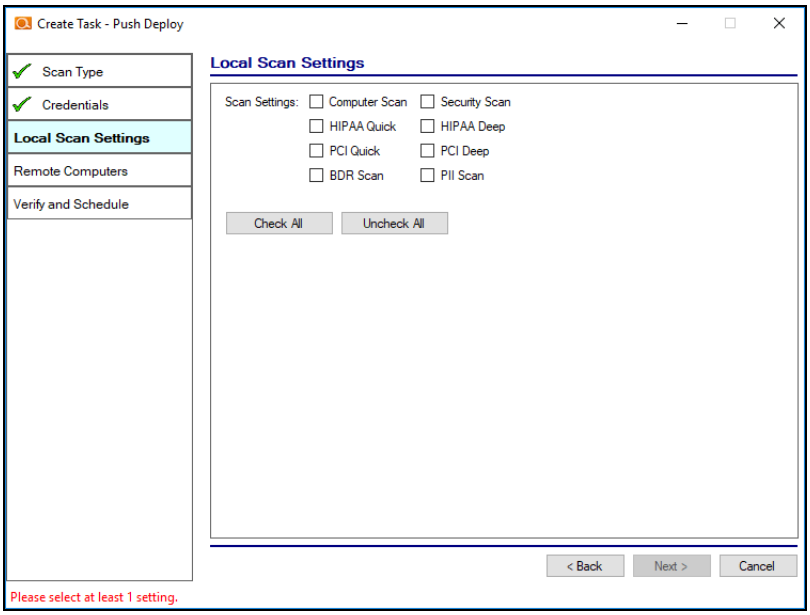
This window details the prerequisites and requirements that must be met to enable a Push Deep Local Scans for PCI task to be scheduled and executed successfully. Please note them carefully before you proceed.

These are:

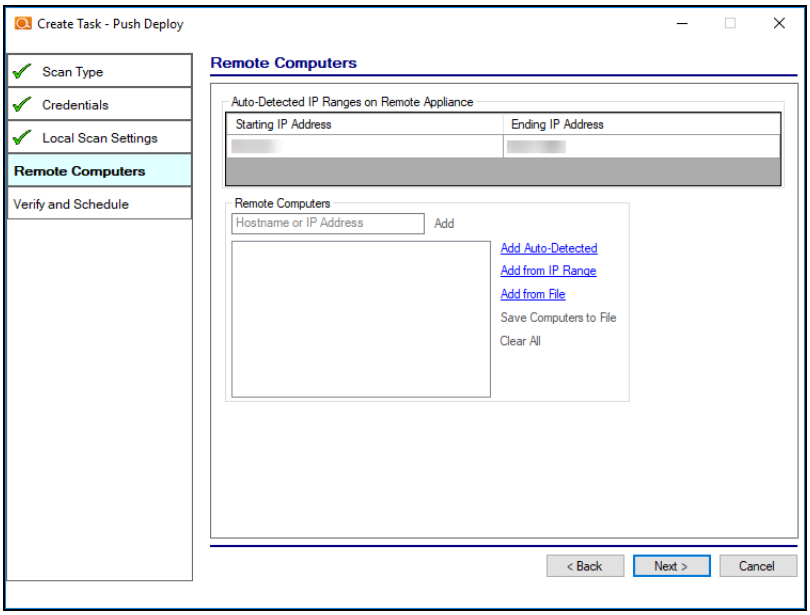
- ADMIN$ access to the remote machine
- .NET 4.6.2 installed on the remote machine
- WMI access to the remote machine

After validating that the “Push” Management Tool requirements have been met, enter credentials with administrative rights. Click **Next**.

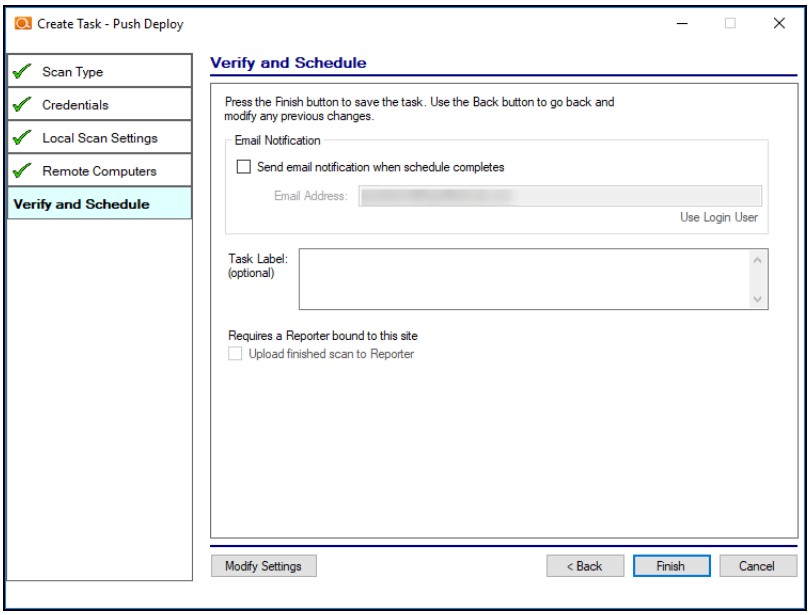
4. From the Local Scan settings window, select PCI Deep Scan. Click **Next**.



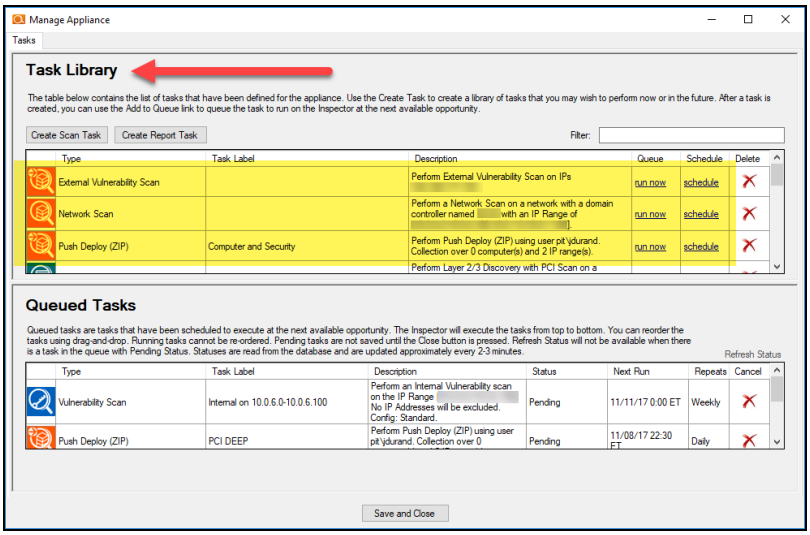
5. The Remote Computers screen will appear. Select **Add Auto-Detected**, **Add from IP Range**, or **Add from File** to add one or more computer Hostnames or IP addresses. Once the Remote Computers are identified and added, these computers will be listed in the list-box control. Click **Next**.



6. Verify and schedule the scan. To have an Email Notification sent to you when the push and scan task completes, select the “Send email notification when schedule completes” option, and type in the email address where the notification should be sent. Click **Finish**.



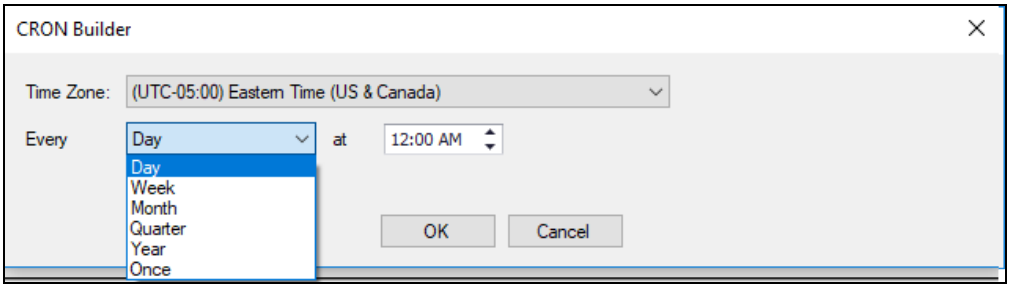
7. Once you create the scan task, it will appear as a task in the appliance Task Library.



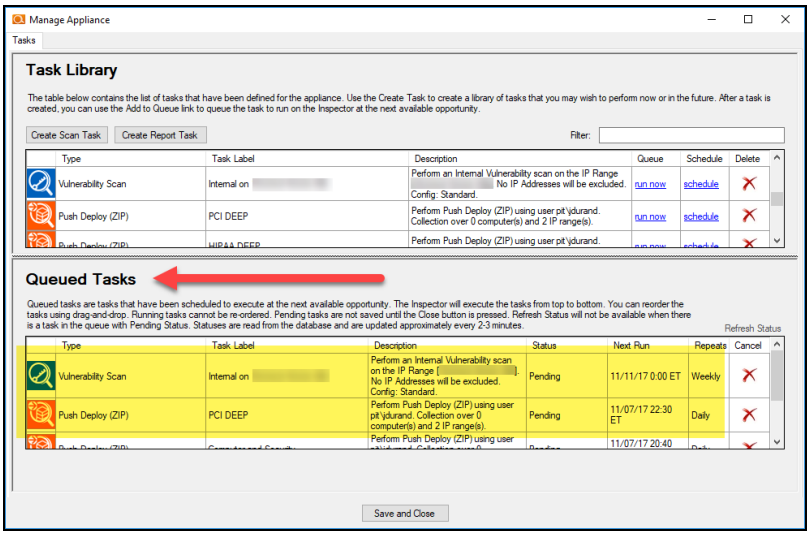
In order to initiate the scan, you will need to move the scan from the Task Library into the list of Queued Tasks. There are two ways to do this:

a. Select the **run now** option link under the Queue column to initiate the scan. This will place the scan directly into the Queued Tasks list.

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



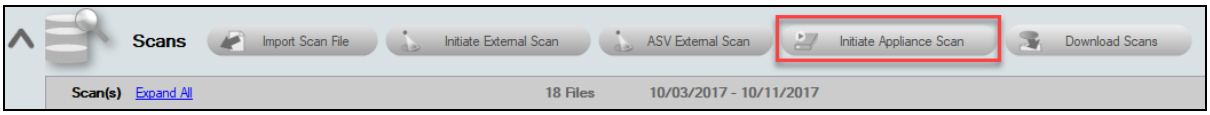
Whether you choose to run the scan now or schedule the scan to take place in the future, it will be added to the Queued Tasks list, where you can check its status. This is the final step in initiating (or scheduling) a scan.



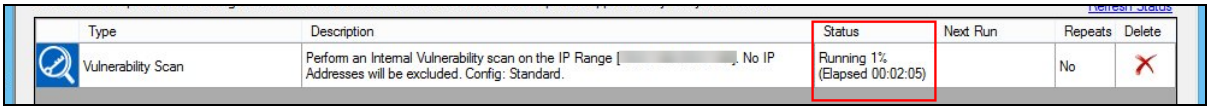
Checking Appliance Scan Execution Status

To check on the status of the scheduled appliance scan:

1. Click **Initiate Appliance Scan**.



2. View the Queued Tasks list to check the status of the scheduled scan.



The status of the scan may be set to Pending or Running along with a percentage of the task's performance completion as illustrated in the window below.

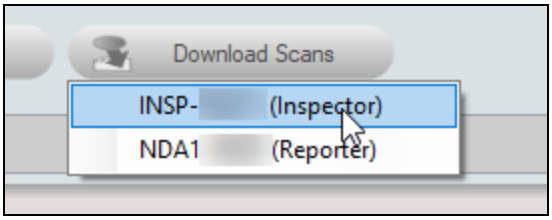
When the scan task is completed, the task will be removed from the Queued Tasks list. You can then download the scan and merge it into your assessment project.

Download Appliance Scans

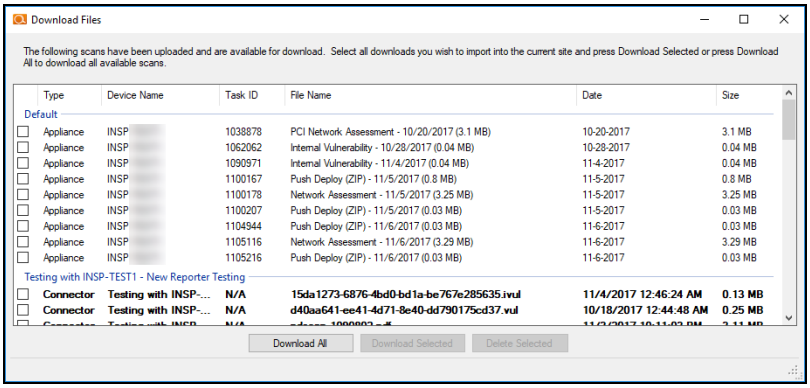
Once the scan is completed, download the scan and merge it into your assessment project. To do this:

1. Click **Download Scans** from the Scans bar.

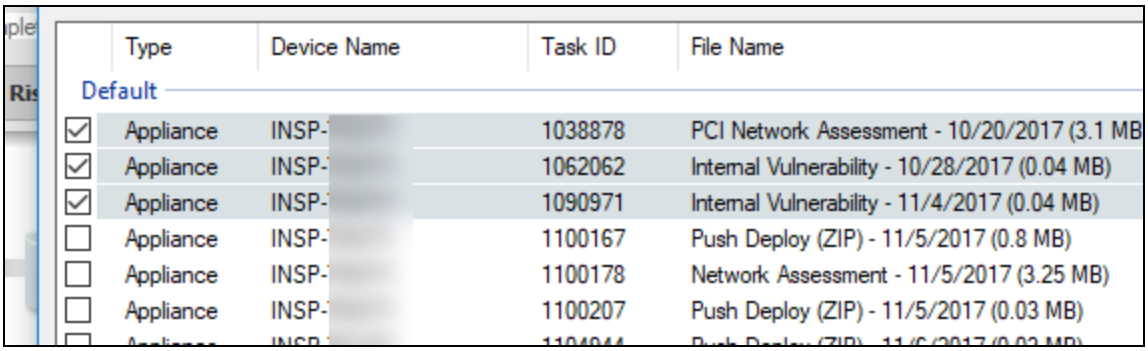
2. Select the appliance for which you would like to download scans.



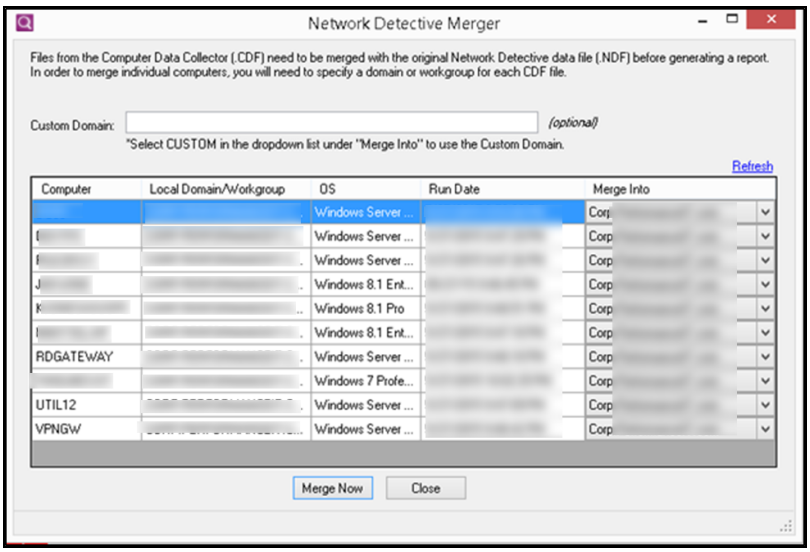
3. The Download Files window will appear. Here you can see a list all of the scans that an appliance has performed for a given Site.



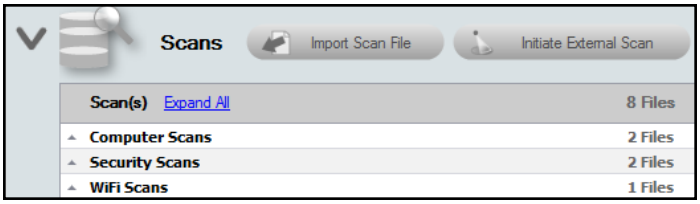
4. Select the check box next to the scan file you wish to download then select the **Download Selected** button. The file will then be downloaded and imported into the assessment.



5. If prompted, merge the scans into the assessment using the Network Detective Merger. Click **Merge Now** to perform the merge.



The imported scans will appear as files under the Scans bar.

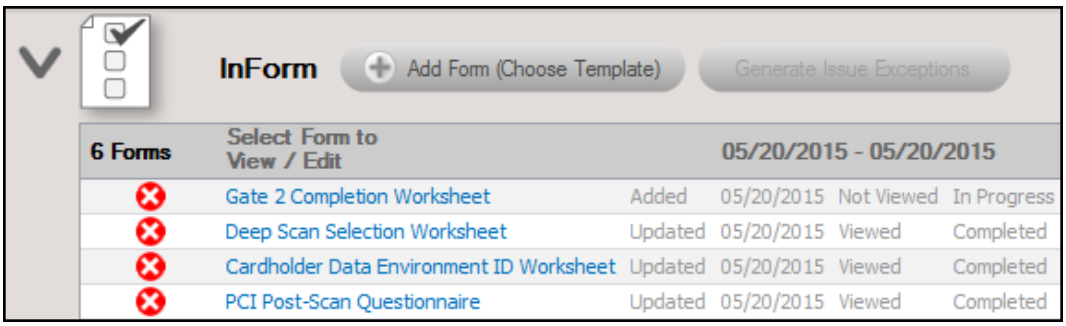


Step 12 — Complete the Gate 2 Completion Worksheet

The purpose of the **Gate 2 Completion Worksheet** is for you to confirm that you have completed all PCI Deep scans you wish to perform and include within the PCI

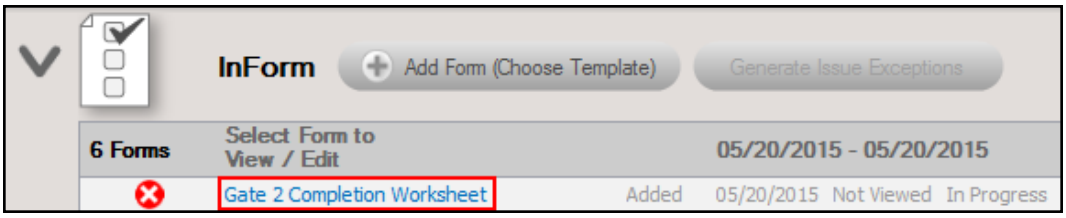
assessment process.

After completing the “deep” scanning phase of the PCI assessment process, the **Gate 2 Completion Worksheet** is added to the **InForm** section of the **Assessment Window**.

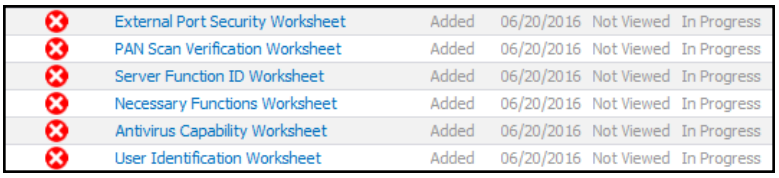


The completion of the **Gate 2 Completion Worksheet** confirms that the second phase of the PCI assessment has been performed before proceeding to the next phase of the assessment process.

To complete the **Gate 2 Completion Worksheet**, click on the **name label** for the **Gate 2 Completion Worksheet** available listed below the **InformBar** located at the bottom of the **Assessment Window** here:



Completing the **Gate 2 Worksheet** will also add several new worksheets to the **InForm** section of the **Assessment Window.** These new worksheets represent the next steps in the PCI assessment process.



These new worksheets will include

- User ID Worksheet.
- Antivirus Capability Worksheet
- Necessary Functions Worksheet
- Server Function ID Worksheet
- PAN Scan Verification Worksheet
- External Port Security Worksheet

Step 13 — Run the PCI Deep Scan on the Selected Systems Manually (OPTIONAL)

It may be necessary to collect PCI Deep Scan data from any computers that were unavailable during the PCI Deep Scan process. This case may occur because a computer was offline or in a remote location inaccessible by the Push Deploy Tool.

If necessary, use the **PCI Data Collector** to run the **PCI Deep Scan** on selected computer systems manually.

For more information, see "Run the PCI Computer Data Collector — “Deep” Local Computer Scan " on page 95.

> **Note:** If you do not need to scan any computers that were unreachable, then proceed to the next step.

Collect Secondary PCI Compliance Assessment Data

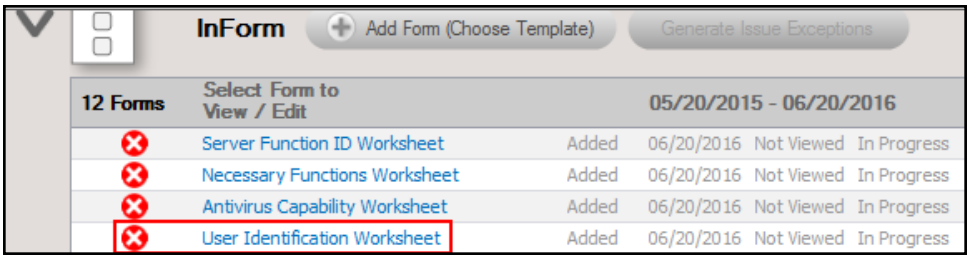
Step 14 — Complete the User ID Worksheet

The User ID Worksheet enables you to identify each user and document if they are authorized to access the Cardholder Data Environment (CDE) that you are assessing.

The **User ID Worksheet** contains a list of users that have been identified as having network/system access rights during the network scan phase of the automated data collection.

In this worksheet, you document **the type of user account** (for example: Employee CDE access, Employee no CDE access, General Account, Vendor CDE access, Vendor no CDE access, etc.).

To access the **User Identification Worksheet** click on the **name label** for the **User Identification Worksheet** available listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



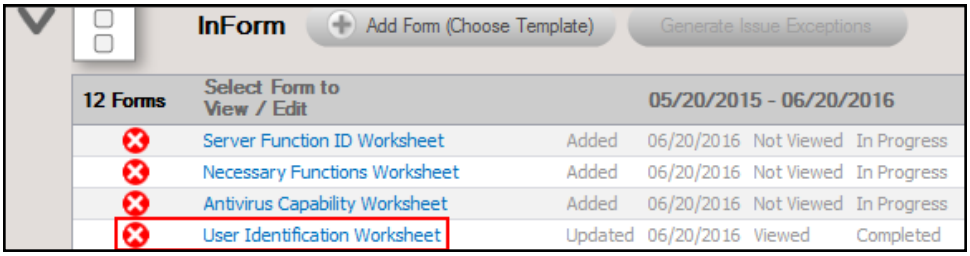
From the **Assessment Window**, **edit** the **User Identification Worksheet**.

For each user you can select the **Response** field and change the default response to the response required.

The **Remote Access to CDE** topic enables to you document employees and/or vendors that have the rights necessary to remotely access the CDE.

Save your answers periodically and **Save and Close** when you are done.

You can return to the **User Identification Worksheet** by selecting the **worksheet's name label**.

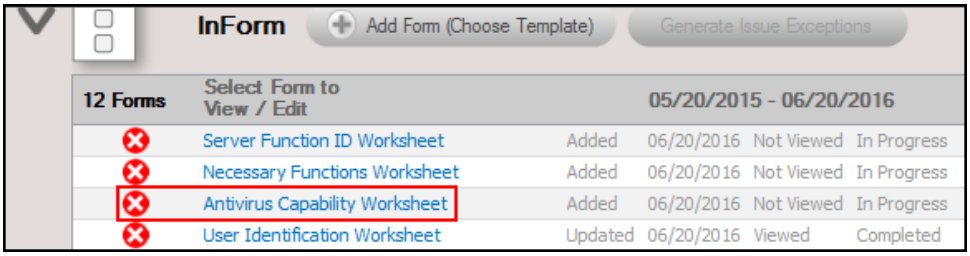


Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

Step 15 — Complete the Anti-Virus Capability Worksheet

The Anti-Virus Capability Worksheet is used to assess and document the PCI compliant features that are contained in any Anti-Virus and/or Anti-Spyware software installed on servers and workstations operating within the environment scanned by the PCI Module.

To access the **Antivirus Capability Worksheet** click on the **name label** for the **Antivirus Capability Worksheet** available listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:

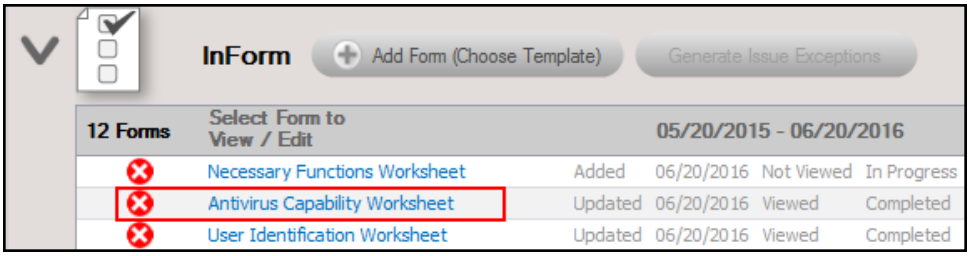


The **Antivirus Capability Worksheet** presents a list of the Anti-Virus and Anti-Spyware applications installed within the assessed IT environment. These Anti-Virus and Anti-Spyware applications are listed in the worksheet to enable you to document an examination of the features contained within the applications. The final **Antivirus Capability** assessment will be a result of responses to a series of questions used to document the features of each of these Anti-Virus and Anti-Spyware applications.

Note: Answer each instruction/question with “Yes”, if the Anti-Virus/Anti-Spyware meets the each of the criteria detailed within this survey worksheet.

Save your answers periodically and **Save and Close** when you are done.

You can return to the **Antivirus Capability Worksheet** by selecting the **worksheet's name label**.

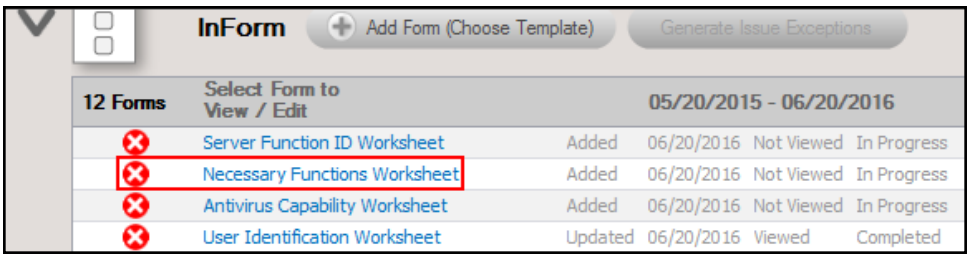


Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

Step 16 — Complete the Necessary Functions Identification Worksheet

The **Necessary Functions Identification Worksheet** is used to assess, validate, and document the need of services, drivers, and features that are installed and/or running on servers and workstations that are operating within the CDE scanned by the PCI Module.

To access the **Necessary Functions Identification Worksheet** click on the **name label** for the **Necessary Functions Identification Worksheet** available listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



Upon editing the **Necessary Functions Worksheet**, the following window is presented:

This worksheet presents the process used to document the **services**, **drivers**, and **features** installed and operating on each server and/or workstation within the assessed IT environment.

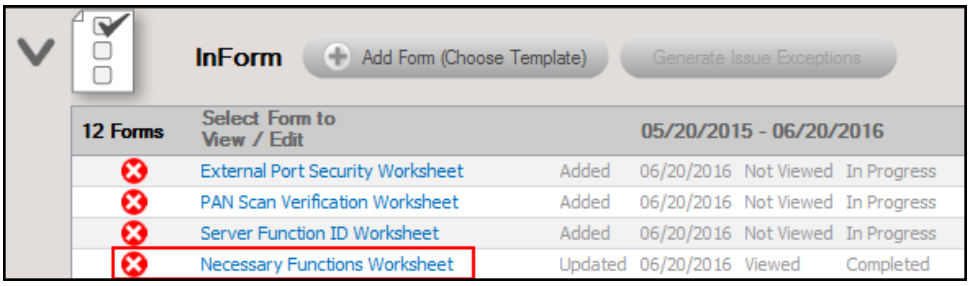
The equipment that has been identified is listed in the worksheet to enable you to answer if a **service**, **driver**, or **feature** that is operating on a given server or workstation is necessary.

To save you time, by default, the "**Response**" is set to "**Yes**", to indicate that the **service**, **driver**, or **feature** is necessary. If the item listed is not required, then, you should change the response to "No".

> **Note:** Answer each instruction/question with the documented purpose/function of each service, driver, or feature that is operating on a given server or workstation in an effort to document the applications, drivers, and services that are operating on system components within the Cardholder Data Environment (CDE) per the PCI requirements.

Save your answers periodically and **Save and Close** when you are done.

You can return to the **Necessary Functions Worksheet** by selecting the **worksheet's name label.**

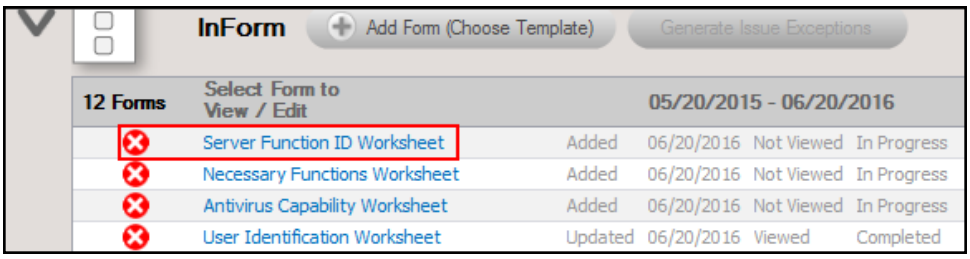


> **Tip:** See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

Step 17 — Complete the Server Function ID Worksheet

The Server Function Identification Worksheet is used to assess and document the "function" that a server operating within the Cardholder Data Environment (CDE) performs.

To access the **Server Function Identification Worksheet** click on the **name label** for the **Server Function Identification Worksheet** listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



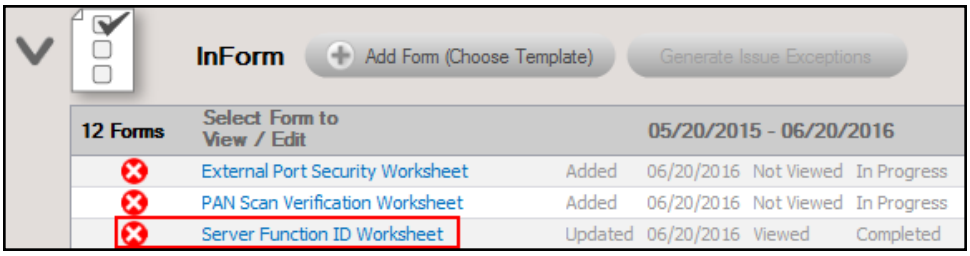
This worksheet presents the process used to document the role of each server operating within the assessed IT environment.

The equipment that has been identified is listed in the worksheet to enable you to answer a series of questions to document the “function” and purpose of each server that is specifically operating within your customer’s IT Environment.

Note: Answer each instruction/question with the documented purpose/function of each server in an effort to ensure that each server is only performing the number of IT “functions” allowed within the Cardholder Data Environment (CDE) as per the PCI specification.

Save your answers periodically and **Save and Close** when you are done.

You can return to the **Server Function ID Worksheet** by selecting the **worksheet’s name label**.



Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

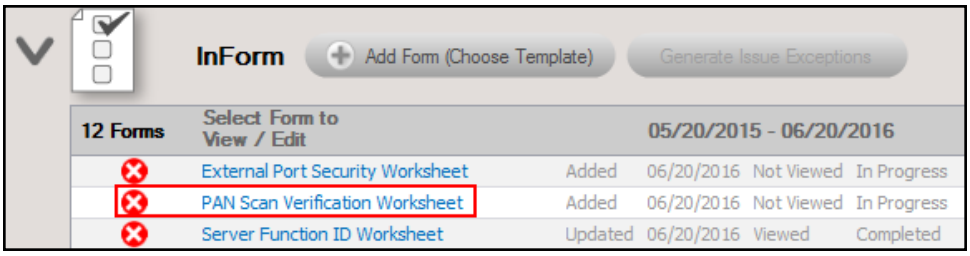
Step 18 — Complete the PAN Scan Verification Worksheet

The deep scan performed by the PCI Data Collector and Push Deploy Tool searches for Primary Account Number (PAN) data within the assessment environment.

The Primary Account Number (PAN) Scan Verification Worksheet contains a list of the locations where files containing what appears to be Cardholder Data have been identified as being stored on a workstation or a server.

In this step, you are to view this list of file locations and the actual documents themselves to determine whether or not the files do or do not contain Cardholder Data. Any "**False Positives**" should be documented.

To access the **PAN Scan Verification Worksheet**, click on the **name label** for the **PAN Scan Verification Worksheet** available listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



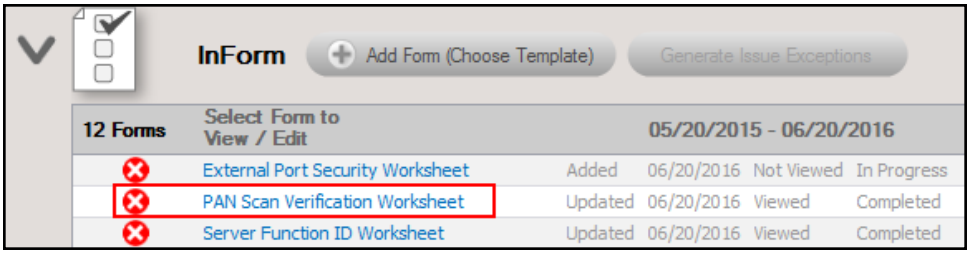
At this point in the process, the worksheet may present a list of files that are stored on a number of servers and workstations that are suspected of containing PAN data. These files were identified during a **deep scan** PAN search. Any files that the PAN scanner deems as containing cardholder data are logged. The locations of the file suspected of containing PAN data and the suspected PAN itself is documented and logged.

The file locations of the files suspected of containing PAN data that have been identified on one or more workstations and/or servers are listed in the **PAN Scan Verification** worksheet. The PCI risk assessment process requires that each of the identified files and associated PAN data are to be inspected. You then can document whether the suspected PAN data is an actual card number or a “false positive”.

This process can be accomplished by responding with a “Yes” or a “No” to a question asking if the file found on a particular workstation or server contains “Primary Account Numbers” (i.e. PANs).

Save your answers periodically and **Save and Close** when you are done.

You can return to the **PAN Scan Verification Worksheet** by selecting the **worksheet’s name label**.

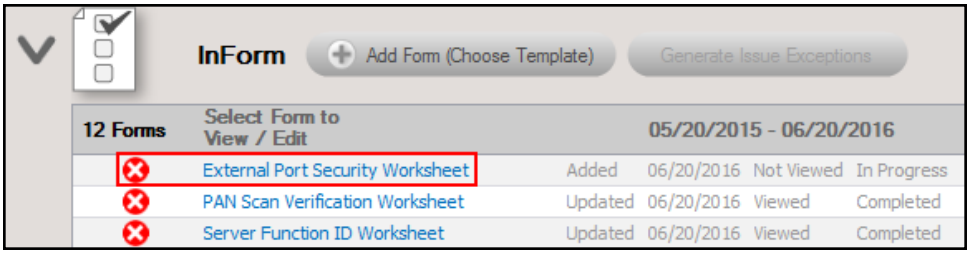


Step 19 — Complete the External Port Security Worksheet

The **External Port Security Worksheet** contains a list of the External Ports that have been identified during the External Vulnerability Scan phase of the automated data collection.

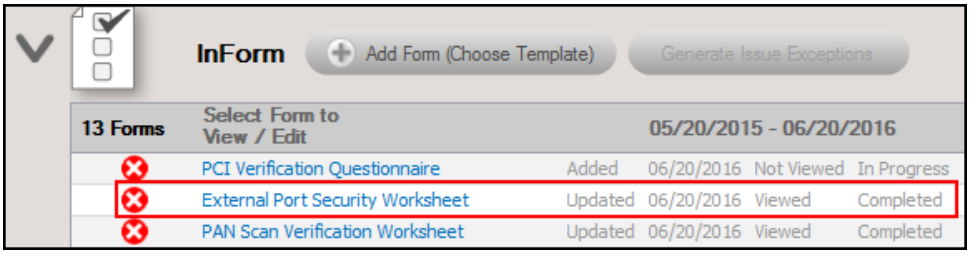
In the Worksheet, you document the business justification for each external port’s usage and document whether or not the port is considered an insecure port.

To access the **External Port Security Worksheet**, click on the **name label** for the **External Port Security Worksheet** listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



Save your answers periodically and **Save and Close** when you are done.

You can return to the **External Port Security Worksheet** by selecting the **worksheet's name label**.



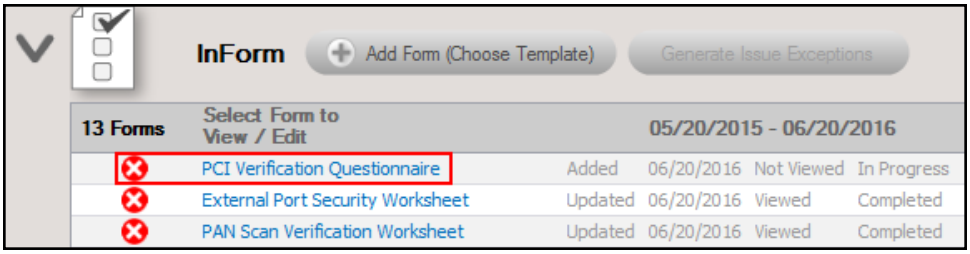
Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

Step 19 — Complete the PCI Verification Worksheet

The **PCI Verification Worksheet** contains a list of PCI compliance assessment issues flagged by the PCI Module. In this worksheet you identify risks and/or establish that system components, security measures, and software are PCI compliant.

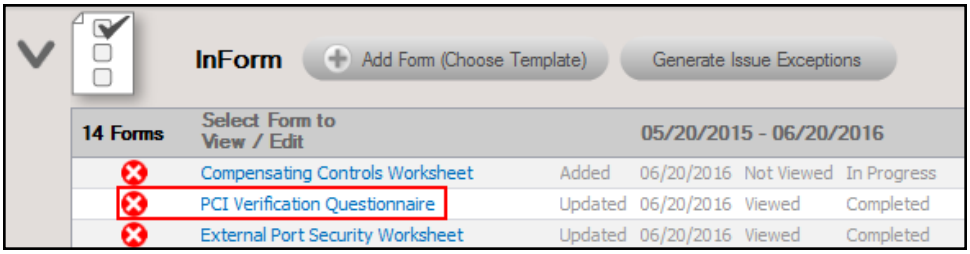
Some of the issues may include: Web-based management interfaces and security, cardholder data environment (CDE) firewall configuration, network diagram verification, security features associated with the use of insecure protocols, and anti-virus verification to just name a few.

To access the **PCI Verification Worksheet**, click on the **name label** for the **PCI Verification Worksheet** listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



Save your answers periodically and **Save and Close** when you are done.

You can return to the **PCI Verification Worksheet** by selecting the **worksheet's name label**.

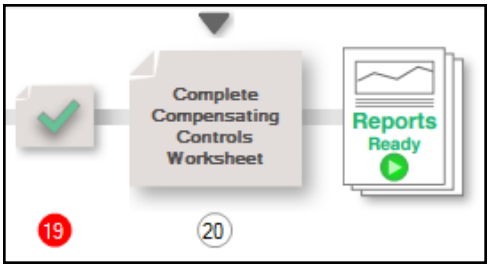


Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

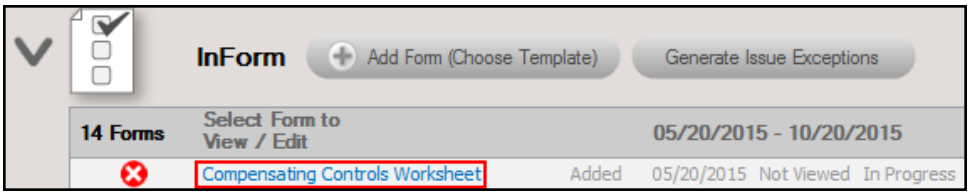
Next, document exceptions by completing the Compensating Controls Worksheet:

Step 21 — Complete the Compensating Controls Worksheet (Optional)

The Compensating Controls Worksheet is an **optional** worksheet that compiles the issues discovered by the PCI Data Collector, Questionnaires, and Assessment Worksheets used throughout the PCI assessment process. It enables you to document security exceptions along with Compensating Controls to manage the exceptions.



To access the **Compensating Controls Worksheet**, click on the **name label** for the **Compensating Controls Worksheet** listed below the **Inform Bar** located at the bottom of the **Assessment Window** here:



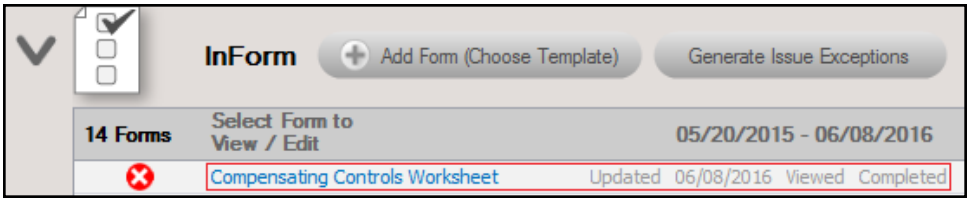
Exceptions are grouped by PCI Data Security Standard Requirement (PCI DSS) category.

> **Note:** Please note that the Compensating Controls Worksheet is the only worksheet that does not require a response for each and every topic.

Enter your **Response** if applicable, otherwise, leave the entry blank.

Click Save or **Save and Close** when you are done.

You can return to the **Compensating Controls Worksheet** by selecting the **worksheet's name label**.



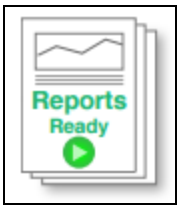
Tip: See "Time Savings Tip to Reduce Survey and Worksheet Data Input Time" on page 108 for helpful time-saving features when using InForm.

When you are finished with this worksheet, you can then generate PCI Compliance Assessment reports.

Generate PCI Compliance Assessment Reports

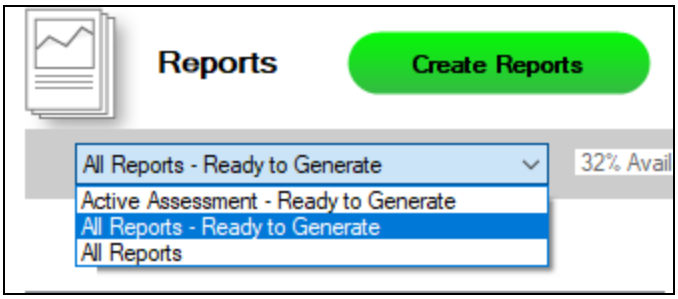
Once the assessment is complete, you can generate reports and supporting documentation. To do this:

1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



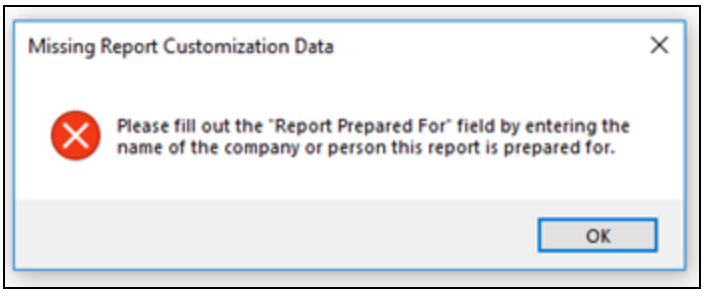
4. Select which of the PCI Compliance Assessment reports that you want to generate.

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



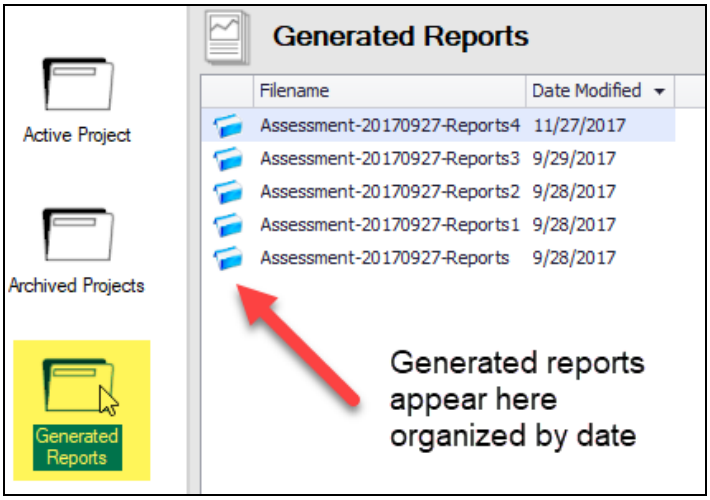
5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.

    i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



> **Tip:** See the Network Detective User Guide for instructions on how to customize your reports with your company's branding.

Click **Generated Reports** from the left-hand Site menu to access previously generated reports. Double click a set of assessment reports to open the folder in Windows Explorer.



Note on Time to Generate Reports

> **Important:** Larger data sets will require more time to generate reports. If the data set is especially large — in the range of several thousand users, for example — a full set of reports may take several hours to complete.

PCI Assessment Reports

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

Compliance Reports

These reports show where you are in achieving PCI compliance. In addition, these documents identify and prioritize issues that must be remediated to address PCI related security vulnerabilities through ongoing managed services.

Report Name	Description
Cardholder Data Environment (CDE) Network Diagram and Details Report*	This report allows you to completely visualize how system components are connected within the Cardholder Data Environment (CDE) being assessed. This high-level report shows a layer 2/3 diagram and mapping with section blow-ups that list all major network devices, and segmented diagrams of connected devices. Additional information is also provided to identify which operating systems and device types were found. CDE details include a list of all discovered computers and network devices including those that we were unable to find connectivity information (denoted in gray text within the report). Devices where connectivity information is unavailable may be due to a lack of responsiveness of the computer itself or other "hidden" network devices (i.e., network devices that did not respond to SNMP requests). ***Requires the Network Detective Inspector appliance.**
Evidence of PCI Compliance	Just performing PCI-compliant tasks is not enough. Audits and investigations require evidence that compliance tasks have been carried out and completed. Documentation must be kept for six years. The Evidence of Compliance includes log-in files, patch analysis, user & computer information, and other source material to support your compliance activities. When all is said and done, the proof to proper documentation is accessibility and the detail to satisfy an auditor or investigator included in this report.
PCI Policies & Procedures Document	The Policy and Procedures are the best practices that our industry experts have formulated to comply with the technical requirements of the PCI DSS. The policies spell out what your

Report Name	Description
	organization will do while the procedures detail how you will do it. In the event of a PCI Compliance audit, the first things an auditor will inspect are the Policies and Procedures documentation. This is more than a suggested way of doing business. The Policies and Procedures have been carefully thought out and vetted, referencing specific sections in the PCI DSS Requirements and supported by the other reports include with the PCI Compliance module.
PCI Post-Scan Questionnaire	The Post-Scan Questionnaire contains the documented responses to list of questions that were formulated based on the results of scans that have been performed.
PCI Pre-scan Questionnaire	This questionnaire contains a list of questions about physical and technical security that cannot be gathered automatically. The survey includes questions ranging from how facility controls access, firewall information, application development, to authentication and change management standards.
PCI Compliance PowerPoint	This PowerPoint slide deck presents a visual overview of the PCI assessment.
PCI Risk Analysis Report	PCI is a risk-based security framework and the production of a Risk Analysis is one of primary requirements for PCI compliance. In fact, a Risk Analysis is the foundation for the entire security program. It identifies the locations of electronic stores of, and/or the transmission of Cardholder Data and vulnerabilities to the security of the data, threats that might act on the vulnerabilities, and estimates both the likelihood and the impact of a threat acting on a vulnerability. The Risk Analysis helps Card Processing Merchants and their 3rd party Service Providers to identify the components of the Cardholder Data Environment (CDE), how the data moves within, and in and out of the organization. It identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of Cardholder Data at rest and/or during its transmission. The Risk Analysis must be run or updated at least annually, more often if anything significant changes that could affect one or more system components in the

Report Name	Description
	CDE itself.

Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
Antivirus Capability Identification Worksheet	This worksheet enables the PCI readiness specialist to inspect and document the features and capabilities Antivirus Software deployed on computers throughout network both in and out of the Cardholder Data Environment (CDE).
Cardholder Data Environment ID Worksheet	The Cardholder Data Environment Worksheet takes the list of computers gathered by the Data Collector and lets you identify those that store or access Cardholder Data. This is an effective tool in developing data management strategies including secure storage and encryption.
Compensating Controls Worksheet	The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to enable PCI compliance. This worksheet allows the PCI Compliance readiness specialist to document explanations on suspect items. The readiness specialist is enabled to document and explain why various discovered items are not true issues and possible false positives. These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The Compensating Control Worksheet compiles the issues discovered by the PCI Compliance Data Collection including the completion of the questionnaires and worksheets. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements. The Compensating Controls Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk. The process is consistent with industry standard PCI assessment and risk management processes.
Deep Scan Selection Worksheet	The PCI Deep Scan, which includes a Primary Account Number (PAN) scanner used to identify files that are suspected of

Report Type	Description
	containing Cardholder Data. This scan should be run on all computers in the Cardholder Data Environment (CDE) that can be accessed along with a sampling of computers outside the CDE. This worksheet enables the documentation of the computers that should be scanned with the PCI Deep Scan.
External Network Vulnerability Scan Detail by Issue	Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.
External Port Security Worksheet	This worksheet allows you to document business justifications for all of the allowed ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.
Internal Network Vulnerability Scan* by Details	Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from inside the target network. Closing internal vulnerabilities helps prevent external attackers, once inside a network, and internal users from exploiting weaknesses typically protected by external firewalls. ***Requires the Network Detective Inspector appliance.**
Necessary Functions Worksheet	For each server in the Cardholder Data Environment (CDE), this worksheet presents startup applications, services, and other functions, allowing you to identify functions which are unnecessary for the server to fulfill its primary function.
PAN Scan Verification Worksheet	The Deep Scan includes a Personal Account Number (PAN) scanner. The results of the PAN scan are presented in this worksheet, allowing you the opportunity to investigate and verify if the detected numbers are truly an identifying account number/credit card.
PCI Layer 2/3 Diagram*	This diagram shows the various components discovered along with their Layer 2 and Layer 3 connections. Systems and devices that are part of the Cardholder Data Environment (CDE) are highlighted. Having a representation of the components in the CDE along with their connectivity to the global network is a requirement of PCI. ***Requires the Network Detective Inspector.**

Report Type	Description
PCI Verification Questionnaire	The PCI Verification Worksheet contains a list of PCI compliance assessment issues that were flagged by the PCI Module throughout the assessment process as concerns that required additional information to be documented. This additional documentation was necessary to address risks that were identified or to establish that system components, security measures, and software are PCI compliant. Some of the issues may include: Web-based management interfaces and security, cardholder data environment (CDE) firewall configuration, network diagram verification, security features associated with the use of insecure protocols, and anti-virus verification to just name a few.
Server Function ID Worksheet	Per PCI DSS Requirement 2.1.1, only one function per server can be implemented in order to prevent functions that require different security levels from co-existing on the same server. The Service Function Identification worksheet enables you to document server roles (web server, database server, DNS server, etc.) and the functions activated on each server (real/physical or virtual) within the Cardholder Data Environment (CDE).
User Identification Worksheet	The User Identification Worksheet takes the list of users gathered by the Data Collector and lets you identify whether they are an employee or vendor. Users who should have been terminated and should have had their access terminated can also be identified. This is an effective tool to determine if unauthorized users have access to protected information. It also is a good indicator of the efforts the organization goes to so terminated employees and vendors have their access quickly disabled. Another benefit is that you can review the user list to identify generic logons, such as Admin, Billing Office, etc., which are not allowed by PCI since each user is required to be uniquely identified.

Change Reports

Report Name	Description
Baseline PCI Management Plan	Based on the findings in the Risk Analysis, the organization must create a Risk Management Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, Network Detective provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Management plan defines the strategies and tactics the organization will use to address its risks.
Baseline PCI Risk Profile	A Risk Analysis is a snapshot in time, while compliance is an ongoing effort. The Network Detective PCI Risk Profile updates a Risk Analysis to show progress in avoiding and mitigating risks. Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.

Appendices

Refer to the appendices listed below for the supplementary information referenced in this user guide:

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. **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

Complete	Domain Configuration
	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)
	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

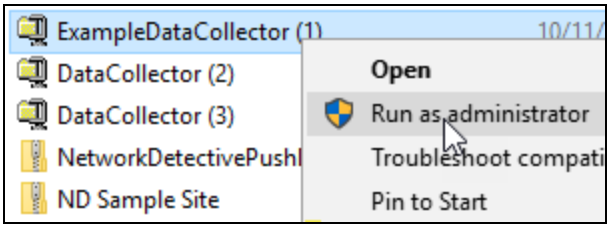
Complete?	Workgroup Configuration
☐	• *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
☐	• *File and printer sharing* must be enabled on the computers you wish to scan
☐	• *Ensure the Windows Services below are running and 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: • 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.

Run the PCI Computer Data Collector — “Quick” Local Computer Scan

A full PCI assessment requires running the Local Computer Data Collector on all computers. When computers are unreachable during the Push Quick Local Scan process undertaken using Inspection, the PCI Data Collector should be used to perform the scan on each of these computers.

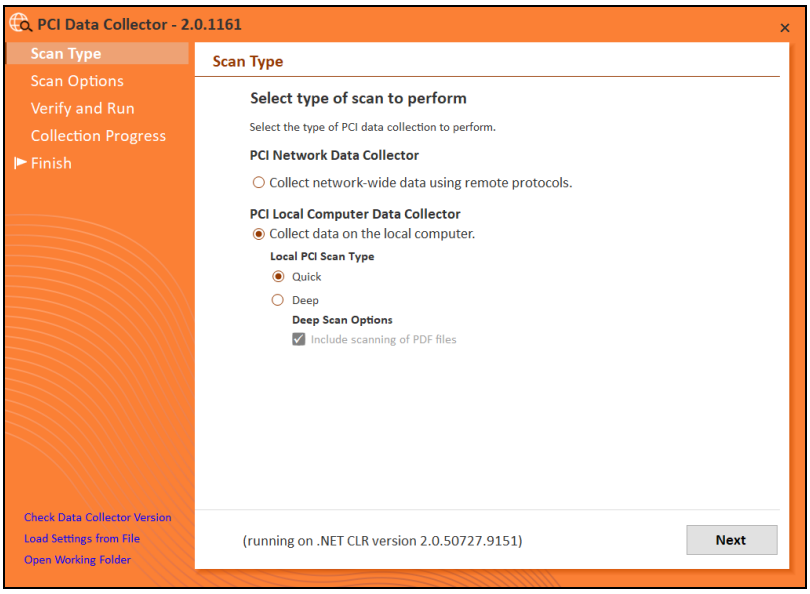
Note: This local computer scanning process using the PCI Data Collector running on the local machine is only used when Inspector is used with the PCI Module and on unreachable computers.

1. If you have not done so already, visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the PCI Data Collector.
2. Run the **PCI Data Collector** executable program as an Administrator (**right click>Run as administrator**).



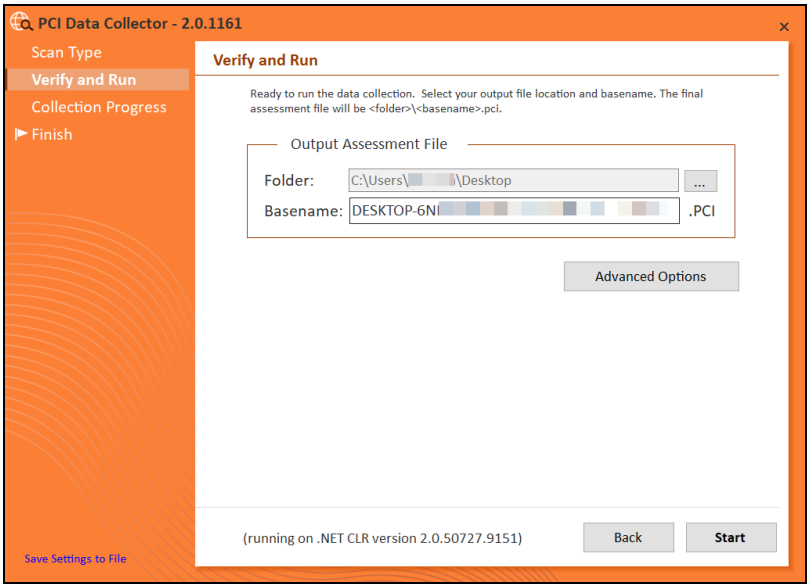
Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

3. **Unzip** the files into a temporary location. The PCI Data Collector’s self-extracting ZIP file does not install itself on the client computer.
4. The PCI Data Collector Scan Type window will appear.



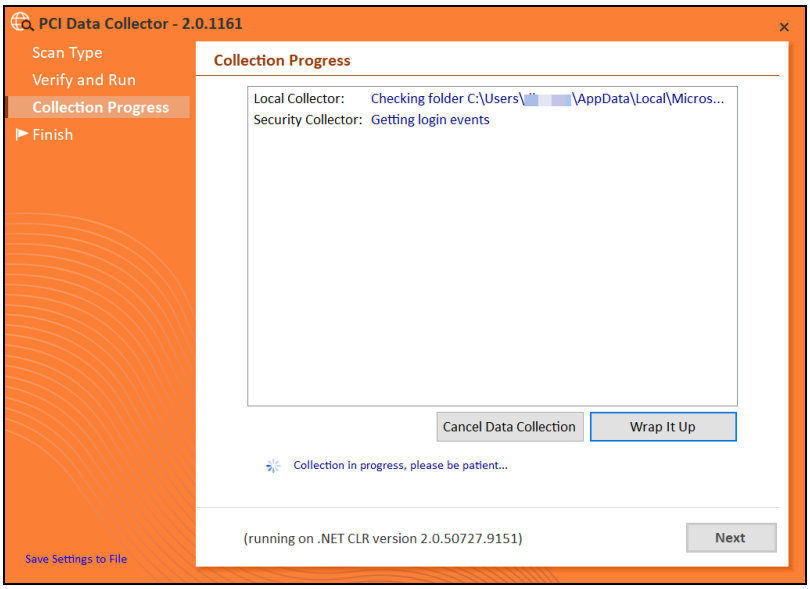
5. Select the **PCI Network Data Collector** option. **PCI Local Computer Data Collector** option and set the **Local PCI Scan Type** to **PCI Quick Scan**. Click **Next**.

   The Verify and Run window will be displayed. The **Verify and Run** window enables you to change the output location for the scan data, change the name of the file, and add comments.



6. After setting the **Output Assessment File**'s **folder location**, the **Basename** of the scan's output file, and adding **a Comment**, select **Start** to initiate the scan.

   The **Collection Progress** window will be displayed during the scan process.

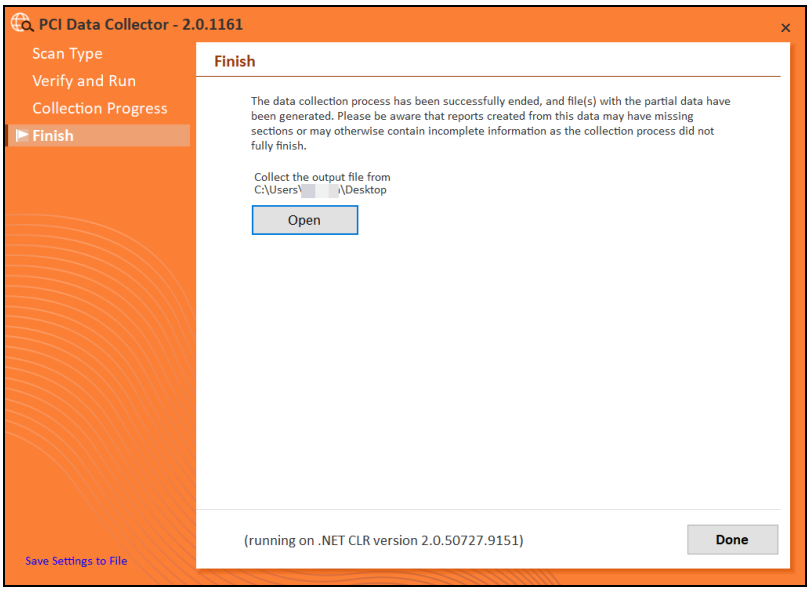


Track the scan's progress through the **Collection Progress** window.

At any time you may **Cancel Data Collection** without saving any data.

You may select **Wrap It Up** to stop a scan and use the incomplete data that was collected.

Upon the completion of the scan, the **Finish** window will be displayed.

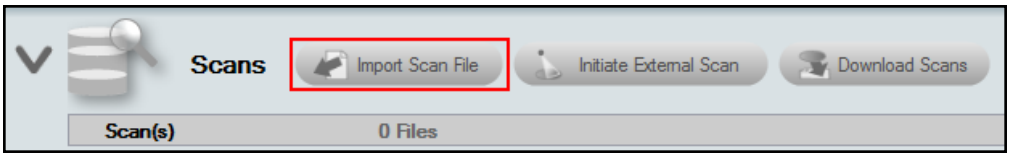


Note the scan **output file's** location and click on the **Done** button to complete the process.

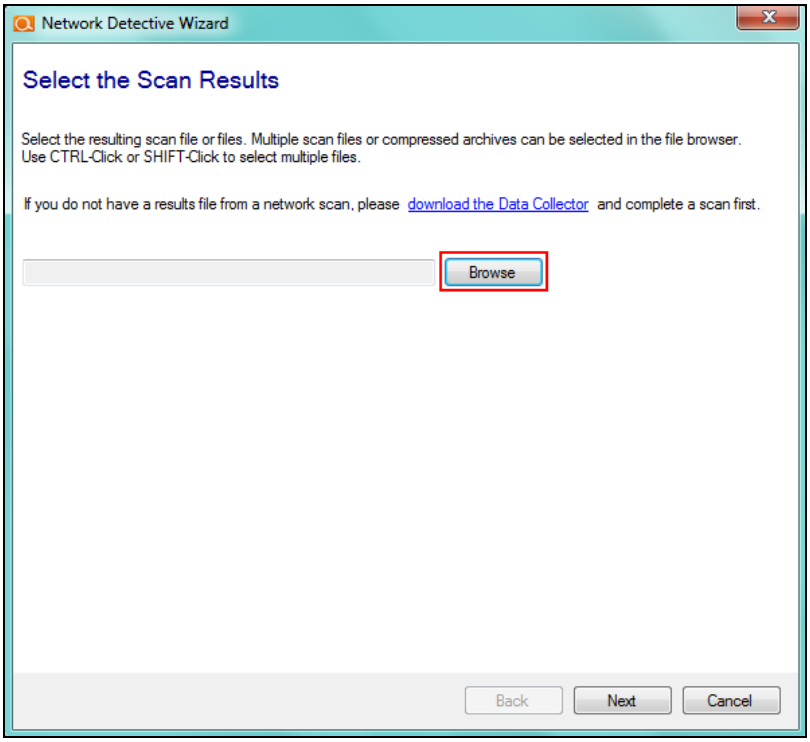
Import the Scan Data from Data Collector into the PCI Compliance Assessment Project

Now import the data collected by the Data Collector into the PCI Compliance Assessment.

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



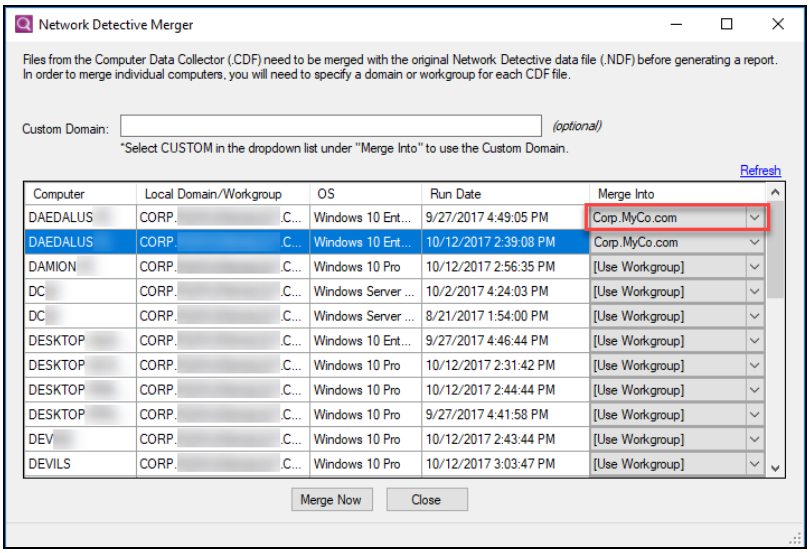
The **Select the Scan Results** window will be displayed.



2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.
3. Click **Open** button to import the scan data. Then click **Next**.

4. An archived copy of the scan will be created in the Network data directory. You can access this at **%APPDATA%\NetworkDetective** on your PC. Click **Finish**.

   i. *If prompted*, use the **Network Detective Merger** to merge the data file(s) into the assessment. Select the Domain into which the file will be merged. Click **Merge Now**.

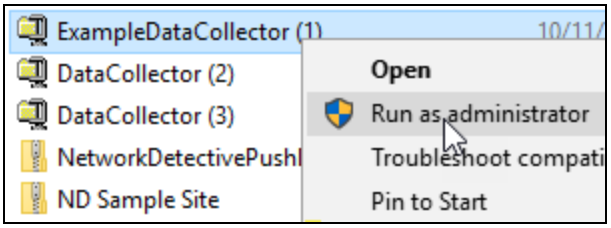


The **Scans** bar will be updated with the imported scan files.

Run the PCI Computer Data Collector — “Deep” Local Computer Scan

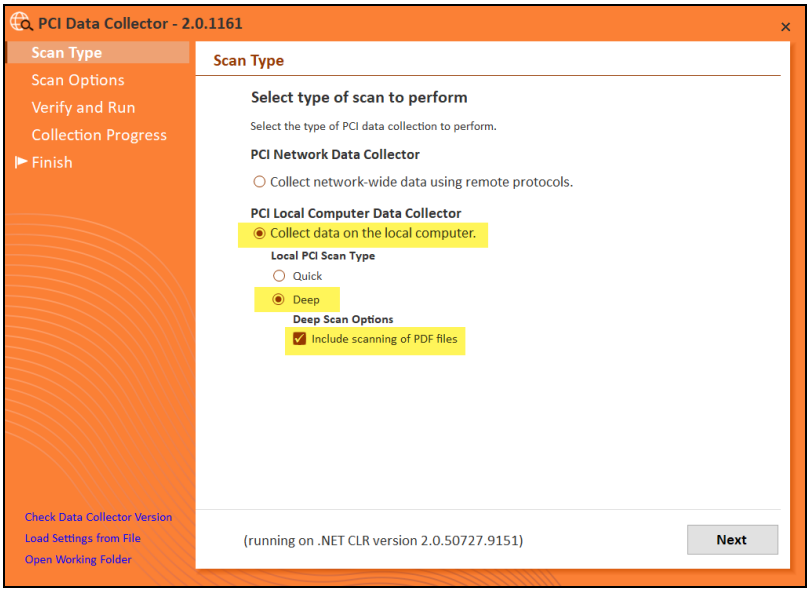
A full PCI Deep Scan assessment requires running the Local Computer Data Collector on all computers in **Deep** mode.

1. If you have not done so already, visit the RapidFire Tools software download website at https://www.rapidfiretools.com/nd and download the PCI Data Collector.
2. Run the **PCI Data Collector** executable program as an Administrator (**right click>Run as administrator**).



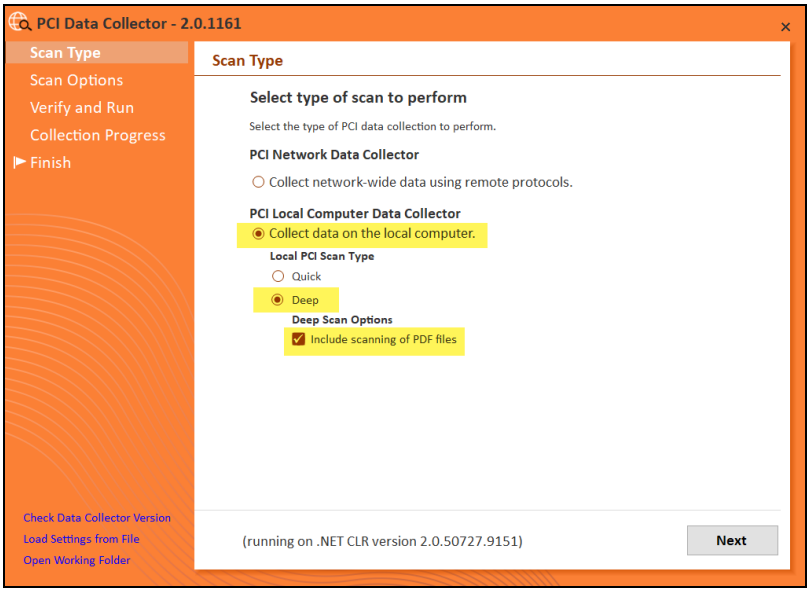
Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

3. **Unzip** the files into a temporary location. The PCI Data Collector’s self-extracting ZIP file does not install itself on the client computer.
4. The PCI Data Collector Scan Type window will appear.

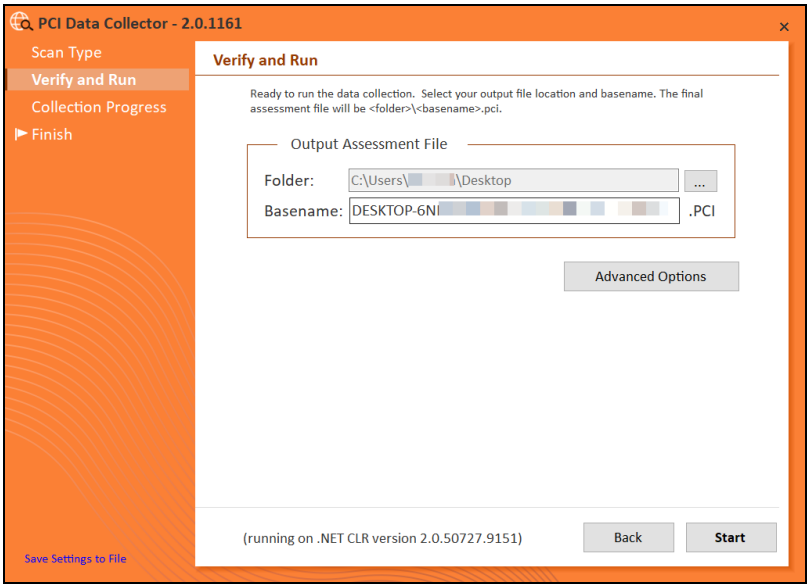


5. Select the **PCI Network Data Collector** option. **PCI Local Computer Data Collector** option and set the **Local PCI Scan Type** to **PCI Deep Scan**. Click **Next**.

   For the Deep Scan, select also whether you wish to perform a PDF scan. Note this may increase total scan time.

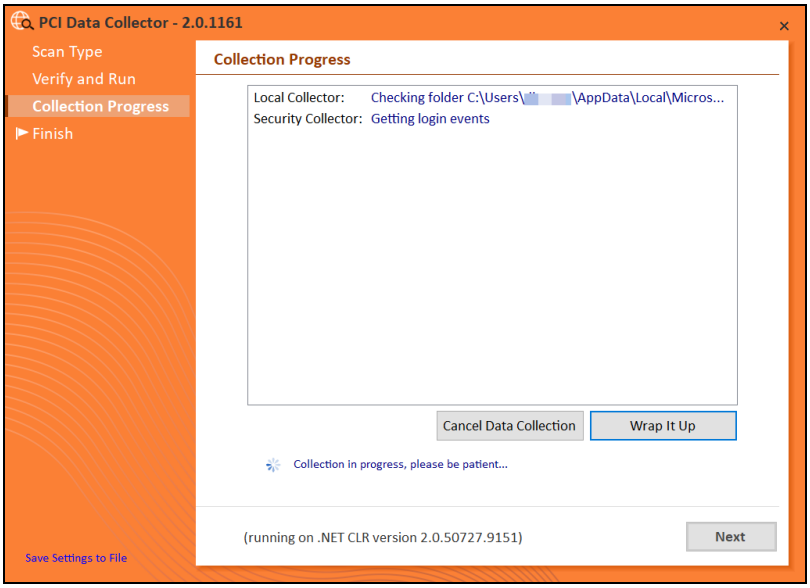


The Verify and Run window will be displayed. The **Verify and Run** window enables you to change the output location for the scan data, change the name of the file, and add comments.



6. After setting the **Output Assessment File**'s **folder location**, the **Basename** of the scan's output file, and adding **a Comment**, select **Start** to initiate the scan.

   The **Collection Progress** window will be displayed during the scan process.

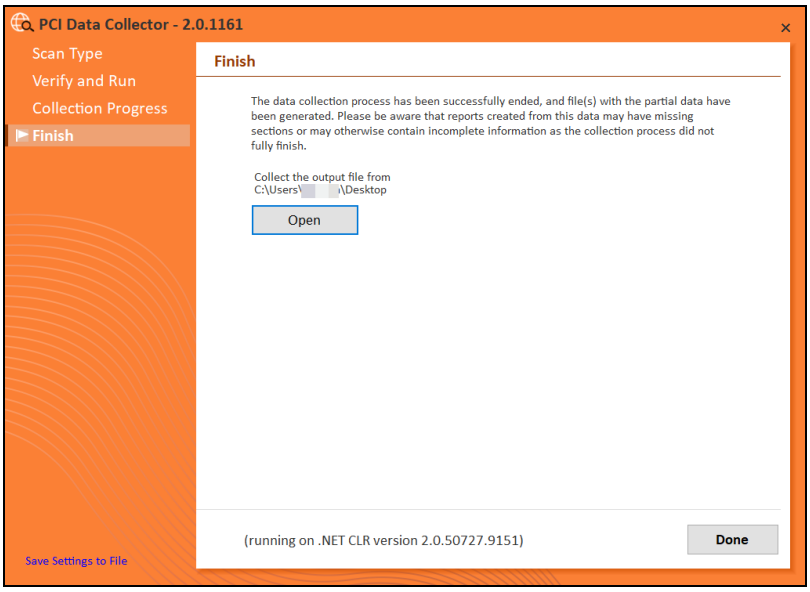


   Track the scan's progress through the **Collection Progress** window.

   At any time you may **Cancel Data Collection** without saving any data.

   You may select **Wrap It Up** to stop a scan and use the incomplete data that was collected.

   Upon the completion of the scan, the **Finish** window will be displayed.

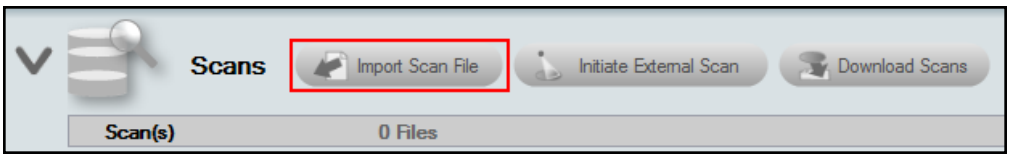


Note the scan **output file's** location and click on the **Done** button to complete the process.

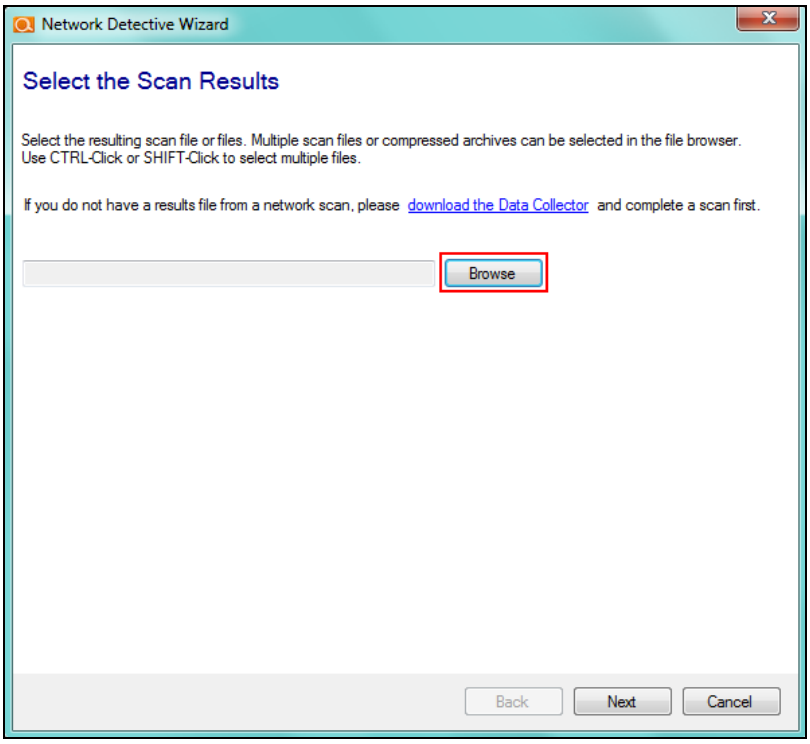
Import the Scan Data from Data Collector into the PCI Compliance Assessment Project

Now import the data collected by the Data Collector into the PCI Compliance Assessment.

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

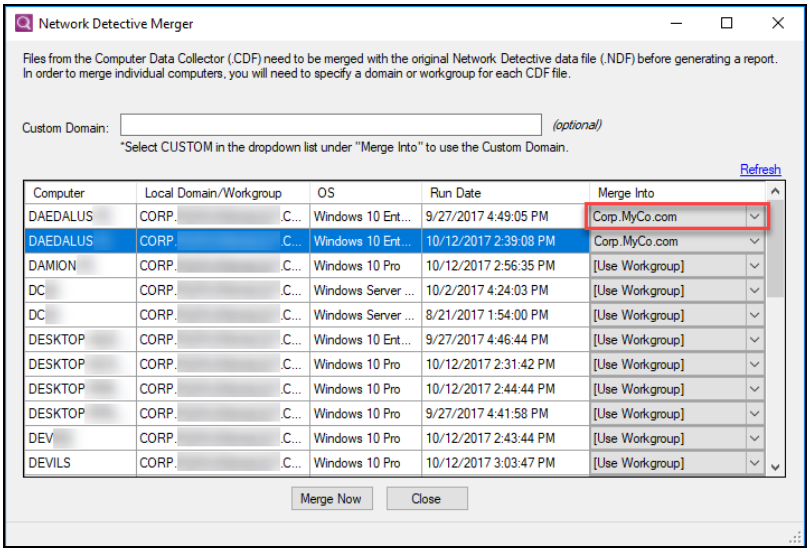


The **Select the Scan Results** window will be displayed.



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

Merge Now.

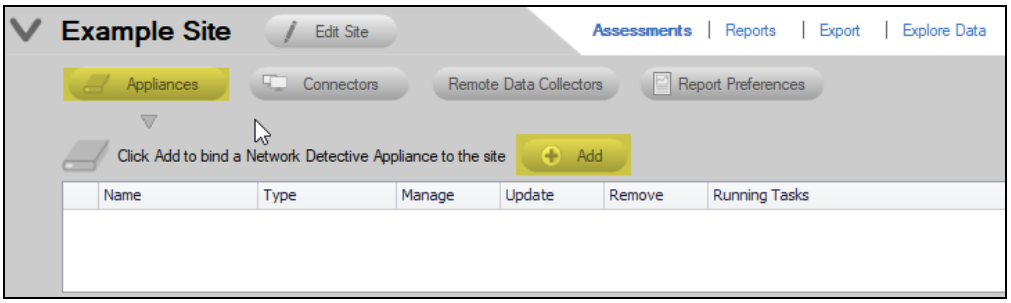


The **Scans** bar will be updated with the imported scan files.

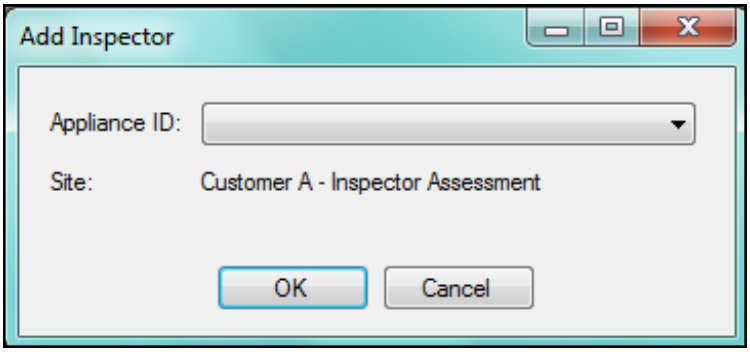
Adding an Inspector to a Site

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

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

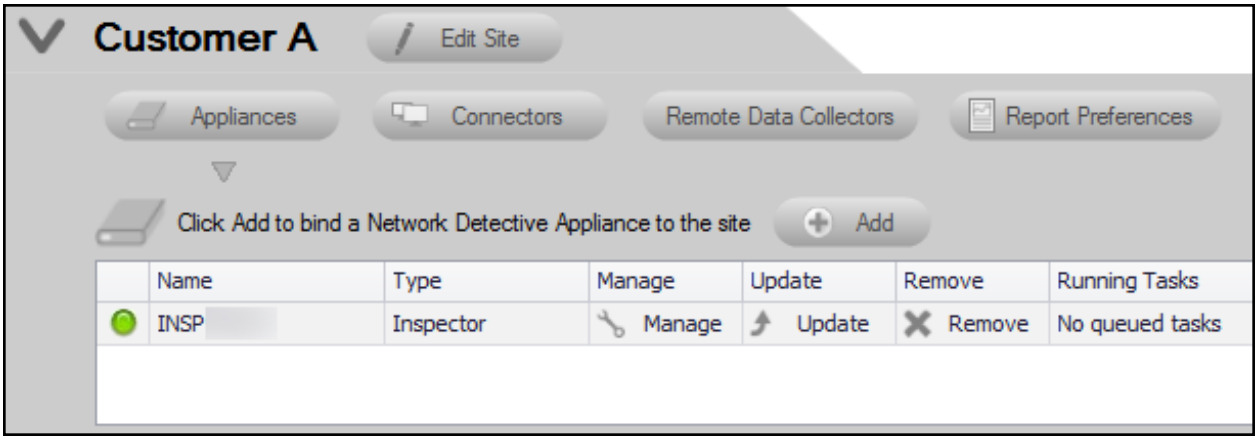


To add an Inspector to an Assessment, from the Assessment’s dashboard select the **Inspector** button, then the **Inspector Add** button as noted above.

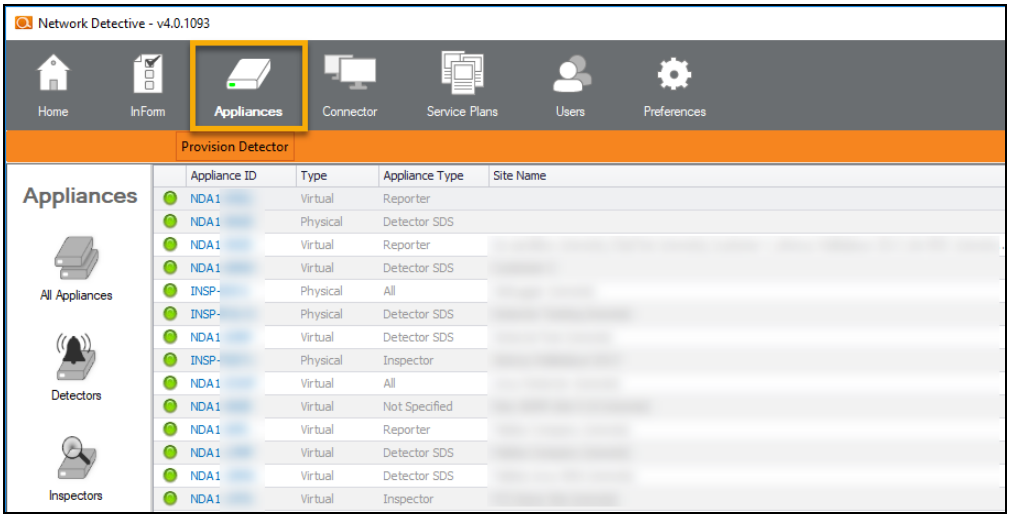


Select the **Inspector ID** of the Inspector from the drop down menu. Note that the Inspector ID can be found on a printed label on the Inspector Appliance.

After successfully adding an Inspector it will appear under the **Inspector** bar in the Assessment's dashboard.



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



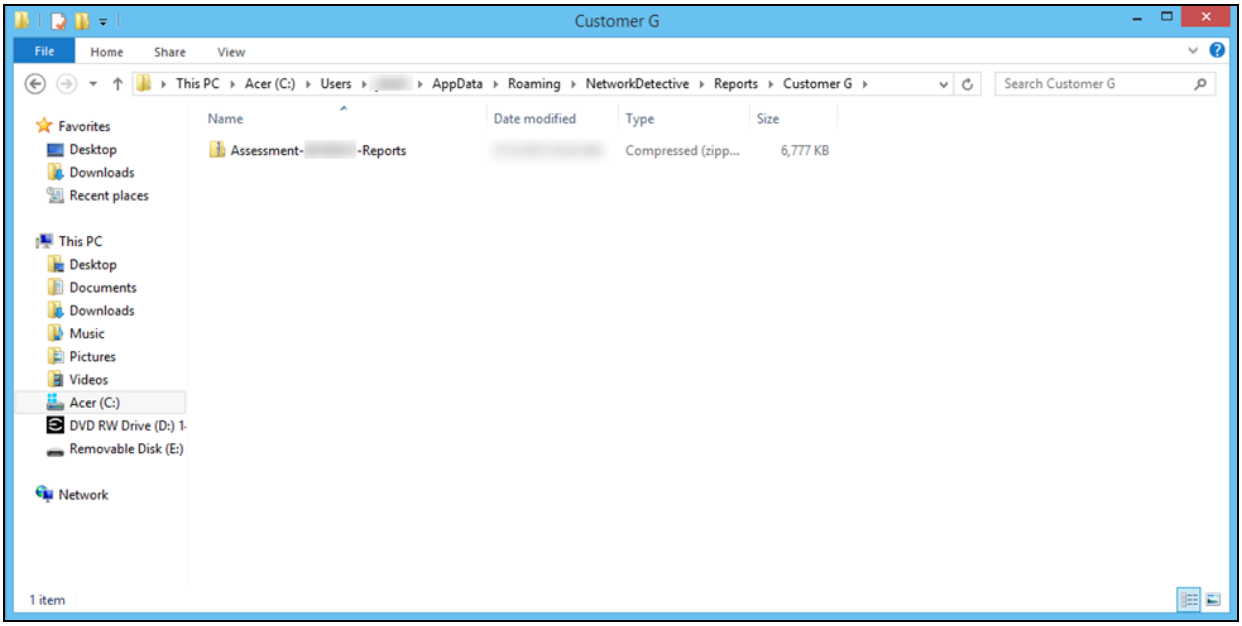
To return to the **Site** that you are using to perform your assessment, click on Home above and select the Site that you are using to perform your assessment.

Site Assessment Reports and Supporting Documents Locations

The reports document files produced by the PCI Module are stored in a compressed folder located on the hard disk of the computer operating the PCI Module.

For example, the figure below illustrates the location of the Assessment Report folder a PCI assessment for a site named "**Customer G**".

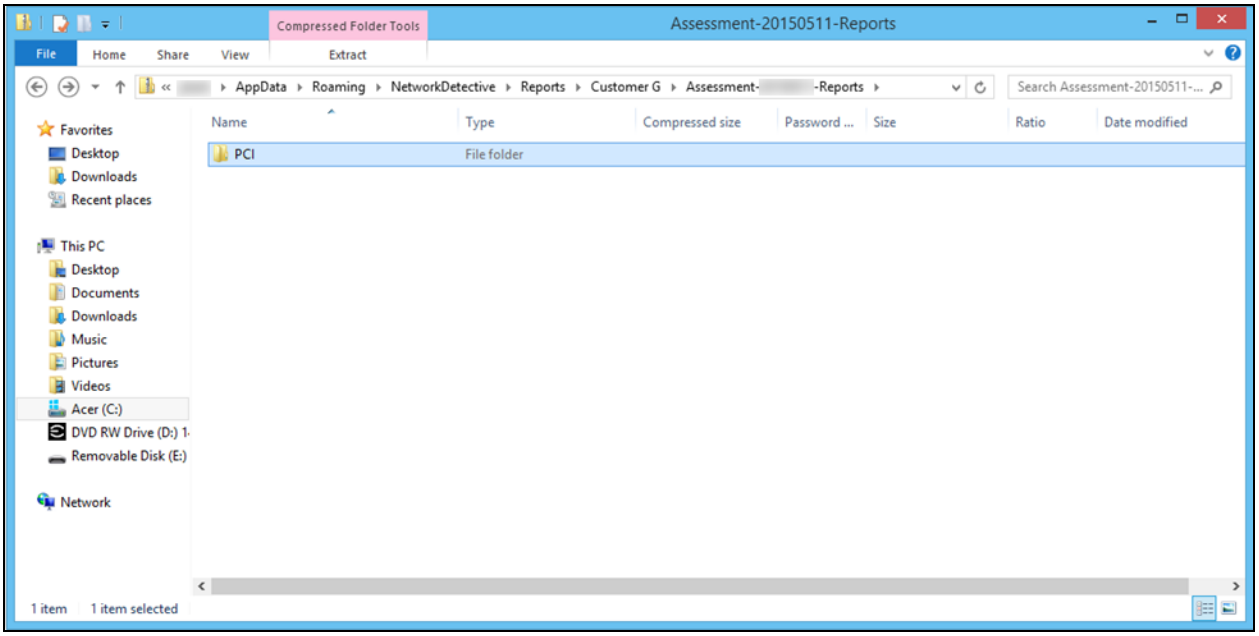
In the folder path referenced in the Windows Explorer folder window displayed below, the reference to "**Customer G**" is a reference to the PCI assessment's "Site Name" associated with the actual assessment.



To access the reports, you would double click on the assessment reports folder which is a "Compressed" folder (aka "zipped" folder).

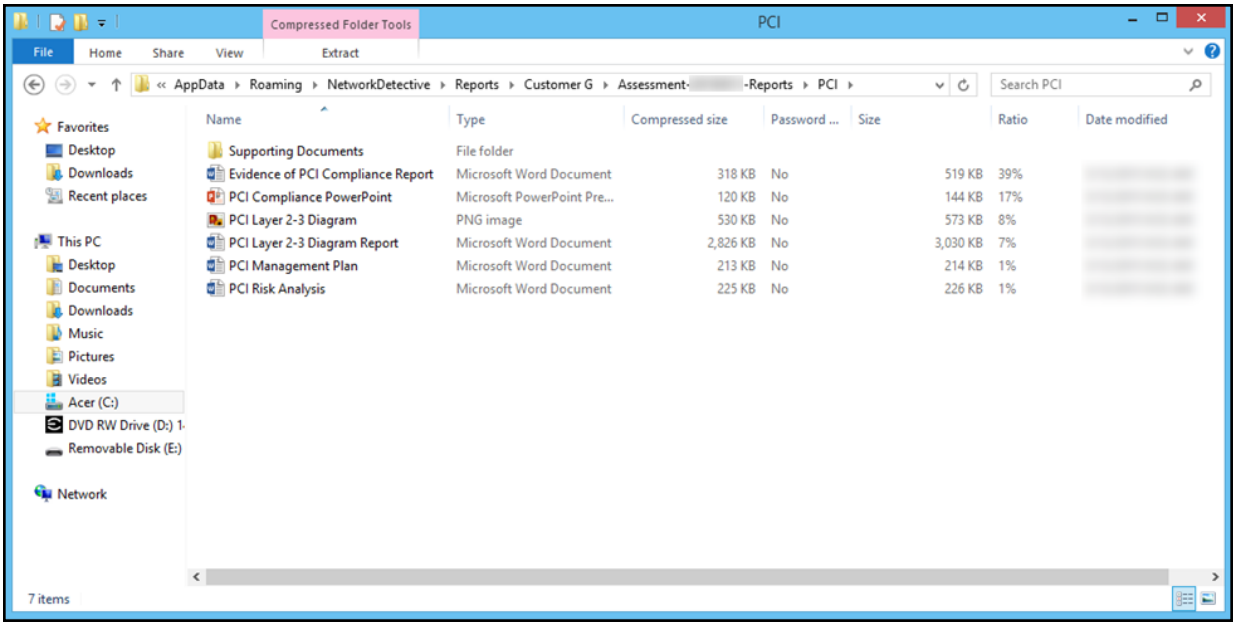
In this example the assessment reports folder is named: **Assessment 20149511-Reports**.

Windows Explorer will then display folder named "**PCI**" as shown below.

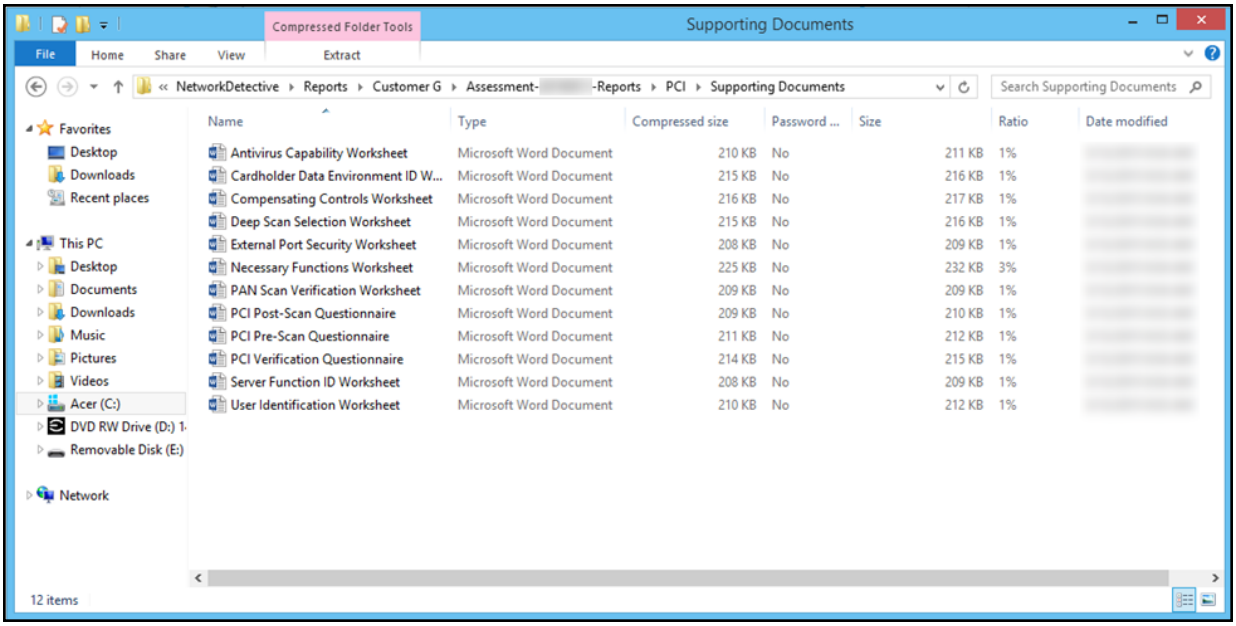


The "**PCI" folder** is the location where the PCI assessment's report documents, PCI Evidence of Compliance, and supporting questionnaire and worksheet documents are stored.

Upon doubling clicking the "**PCI" folder** in Windows Explorer, the reports and supporting documents for the assessment are available for viewing and editing.



Opening the "**Supporting Documents**" folder will enable access to all of the supporting documents as seen below.



Completing Worksheets and Surveys

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

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

Assessment response data is collected through:

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

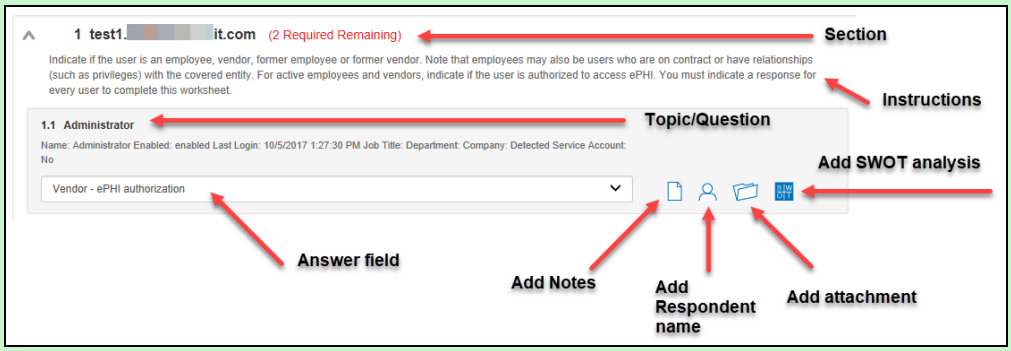
Entering Assessment Responses into Surveys and Worksheets

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

EXAMPLE:

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

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



ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.

iii. Enter the *Response*. There are three types of responses:

Response Type	Description	Example Use
Text Response	Free-form text response	"Describe the condition of the data center."
Multiple Choice	Multiple fixed responses	"Does the firewall have IPS?" (Yes/No)
Checklist Item	An item that is marked off if completed	"Check the security of the door locks."

Note: With few exceptions, you must respond to each form entry to complete the all of the surveys within the PCI Compliance Assessment process.

iv. (Optional) Enter any *Notes* relevant to the topic's response.

v. (Optional) Enter the name of *Respondent* (i.e. the person who provided you with the information, if applicable).

vi. (Optional) Add any relevant *Attachments*. See "Add Image Attachments to Surveys and Worksheets" on the next page for more details.

Note: Only image attachments (.png, .jpg) are supported at this time.

vii. (Optional) Add a *SWOT Analysis*, examining Strengths, Opportunities, Weaknesses, and Threats. See "Add SWOT Analysis to Surveys and Worksheets" below for more details.

viii. Save your answers periodically and **Save** and **Close** when you are done.

Add Image Attachments to Surveys and Worksheets

You can add images to worksheets and surveys. You might include pictures of key personnel or diagrams that explain certain security exceptions.

Attachments can be added to each item or question listed in a worksheet. To do this:

1. Open the InForm in your assessment in Network Detective.
2. Underneath an InForm item, click on the folder icon.

3. Click **Add**.
4. Select the attachment from your computer and click **Open**.
5. Continue adding attachments until you are finished.

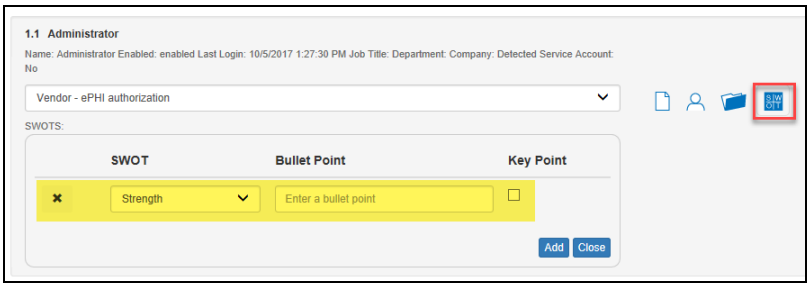
> **Note:** Once you complete your assessment and generate reports, your attached images will appear alongside the form item in the published report and/or supporting document.

Add SWOT Analysis to Surveys and Worksheets

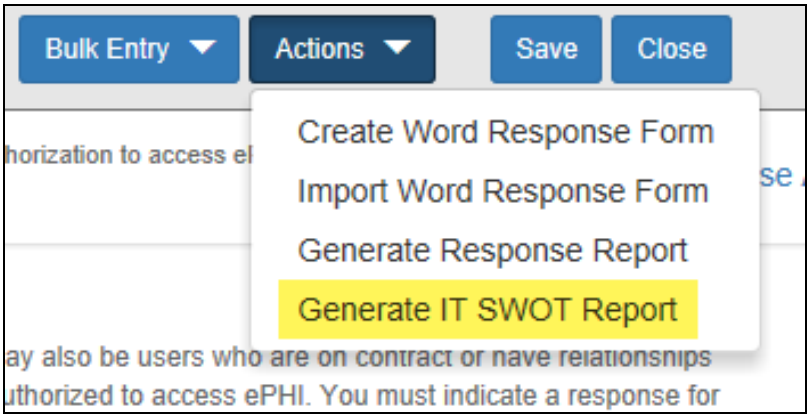
The IT SWOT analysis is a structured method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats affecting an IT network. The analysis involves identifying internal and external issues that are favorable and unfavorable to increasing the overall network health and security of the environment.

To add SWOT to your inform items:

1. Open the InForm in your active assessment in Network Detective.
2. Underneath an InForm item, click on the SWOT icon.



3. Fill in the required fields for each SWOT entry:
   - **Bullet Point**: Enter a short description of the issue here.
   - **Key Point**: Check this to make the entry appear in the SWOT table in the report. Otherwise, it will appear with the rest of the issues in the SWOT list in the report.
4. When you have finished entering all SWOT items for an InForm, click **Actions** and select **Generate IT SWOT Report**.

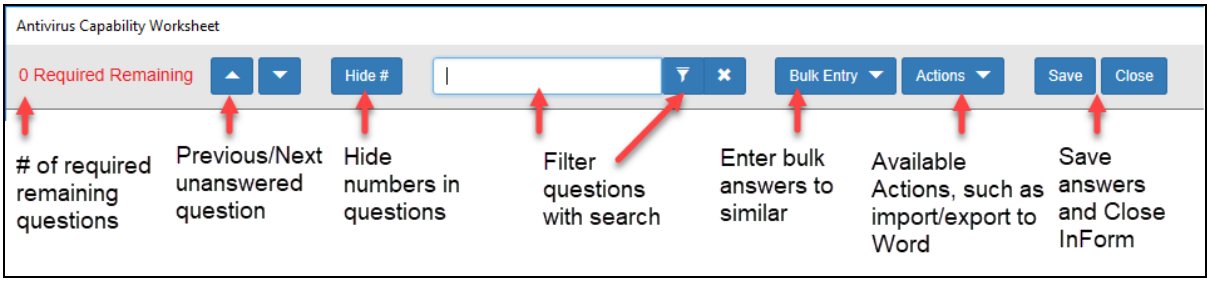


> **Note:** A folder will open with your generated IT SWOT Report. You must generate this report separately for each InForm in your assessment.

Time Savings Tip to Reduce Survey and Worksheet Data Input Time

Use the InForm Worksheet Tool Bar

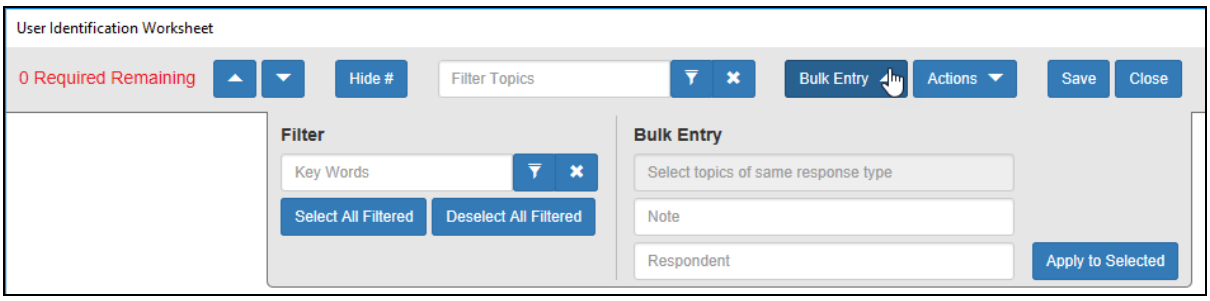
Use the InForm tool bar to save time when completing worksheets.



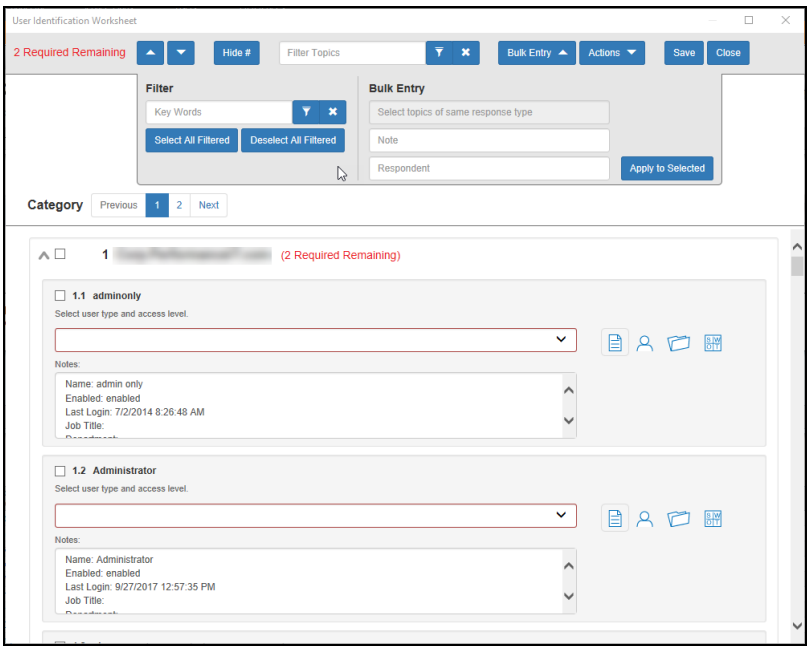
Bulk Entry for InForm Worksheets

InForm allows you to enter bulk responses for worksheet questions. Note that you can only enter bulk responses for questions that require the same types of responses. To use the bulk entry feature:

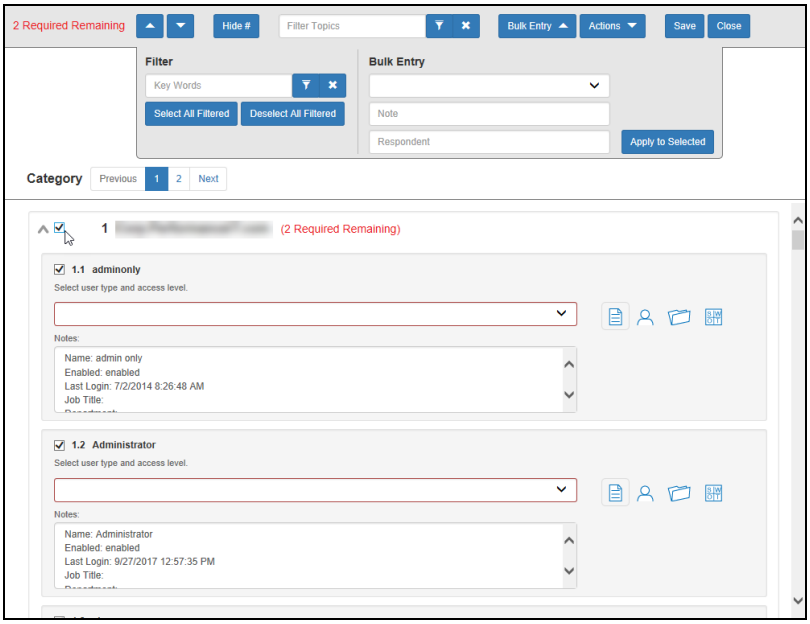
1. Click **Bulk Entry** from the Inform tool bar.



Check boxes will appear next to the response topics.

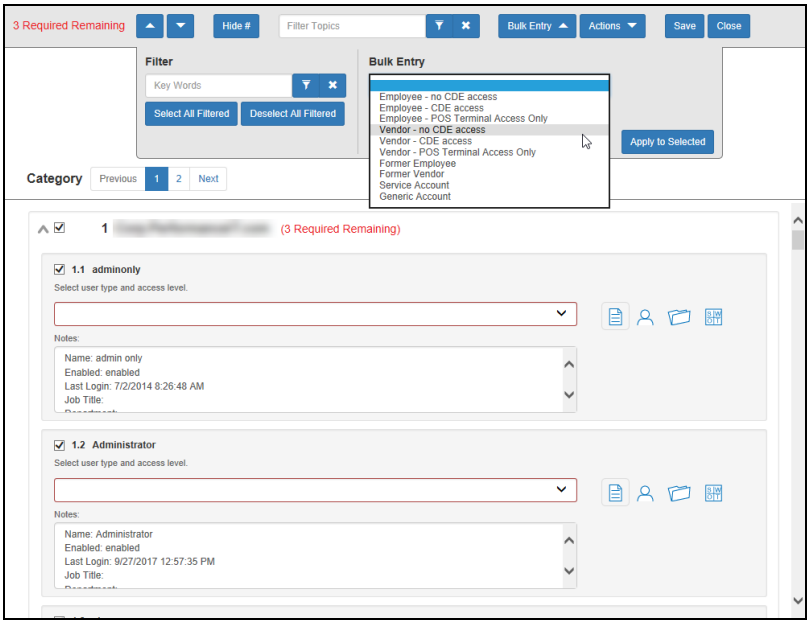


2. Select the check boxes for the topics for which you wish to enter bulk responses.

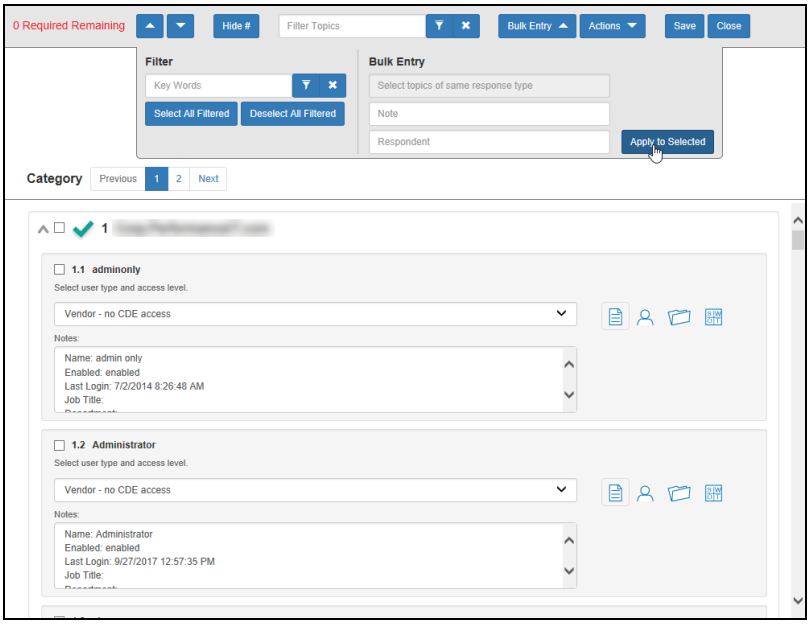


> **Note:** You can select individual topics, or you can click the check box next to the section heading to select all topics within the section. You can also **Filter** topics using terms like "Admin." Note that each topic within the section must require the same types of responses in order to enter bulk responses.

3. Select the response from the Bulk Entry menu. You can likewise enter any relevant notes or the name of a respondent.



4. Then click **Apply to Selected**.



Your chosen response will be entered into the selected topics.

Create Word Response Form

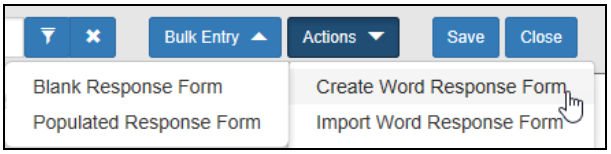
You can export InForm worksheets in your assessment project to Word. This allows you or others to complete worksheets without using Network Detective. For example, you can create a Word response form and send it to a client at a site. The client can then help you gather the required information and enter it in the response form.

Important: In order to import your data, you must enter your responses in the fields contained in the Word document. See "Important Note on Working with Word Response Forms" on the facing page for detailed instructions.

To create a Word response Form:

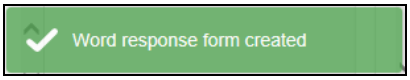
1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
   a. Click **Blank Response Form** to generate a Word document with blank fields ready for data entry.

b. Click **Populated Response Form** to generate a Word document with the responses already entered using InForm.



3. Select the location to save the file. Click **Save**.

   A confirmation message will appear.



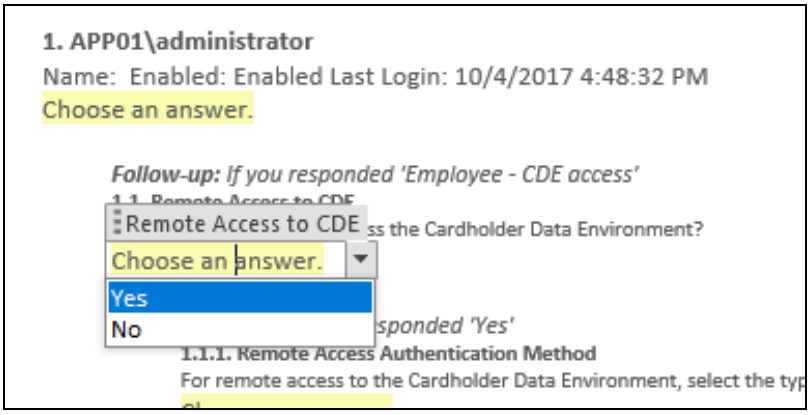
Important Note on Working with Word Response Forms

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

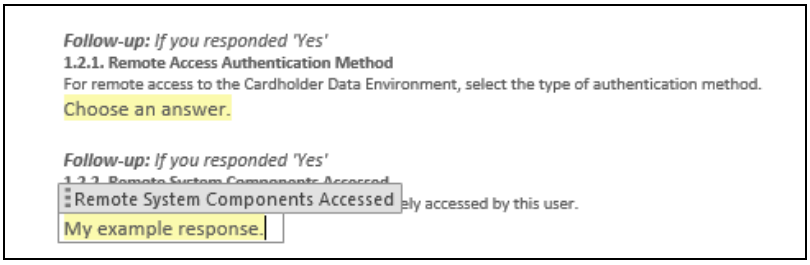
- **DO NOT DELETE** the field controls embedded in the response form! The response fields appear in the images below for your reference:

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

  Multiple choice response field



  Text response field



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

Import Word Response Form

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

EXAMPLE:

Step 1: Create/export a Word response form for one of the worksheets in your assessment.

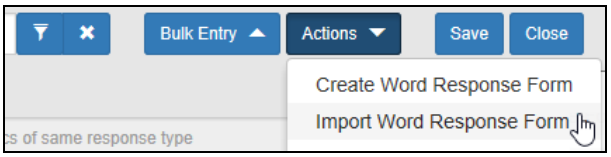
Step 2: Send it to a client to enter additional information about the site using Word.

Step 3: The client can then send you the worksheet as an email attachment.

Step 4: Import the Word document back into your assessment with the client's responses and make any final changes to the worksheet.

To import a Word response form:

1. From the Active Assessment screen in Network Detective, open the worksheet that you want to export to Word.
2. From the InForm tool bar, click **Actions**.
3. Click **Import Word Response Form**.



4. Select the file to import. Click **Open**.

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