

NETWORK DETECTIVE

by RapidFire Tools

PRO



QUICK START GUIDE

5/30/2024 10:51 PM

Cyberattack Risk Assessment Module

Instructions to Perform a Cyberattack Risk Assessment



+1-678-323-1300



[rapidfiretools.com](https://www.rapidfiretools.com)



support@rapidfiretools.com

Contents

Performing a Cyberattack Risk Assessment Scan	3
<u>Cyberattack Risk Assessment Overview</u>	3
<u>Step 1 — Download and Install the Network Detective Pro app</u>	3
<u>Step 2 — Create a New Site</u>	3
<u>Step 3 — Create Cyberattack Risk Assessment in Network Detective Pro</u>	4
<u>Step 4 — Access RapidFire Tools Portal and Customize Branding</u>	6
<u>Step 5 — Create and Distribute the Cyberattack Risk Assessment Computer Scanner</u>	7
<u>Step 6 — Users Downloads and Runs Cyberattack Risk Assessment Computer Scanner</u>	10
<u>Step 7 — Download Scans in Network Detective Pro Cyberattack Risk Assessment</u>	12
<u>Step 8 —(Optional) Run Dark Web ID Scan</u>	14
Set Up Dark Web ID Integration with Network Detective Pro	16
<u>Step 9 — Generate Reports</u>	17
Cyberattack Risk Assessment Reports	19
<u>Standard Reports</u>	19

Performing a Cyberattack Risk Assessment Scan

Cyberattack Risk Assessment Overview

A cyberattack risk assessment is a systematic examination of an organization's potential vulnerabilities to cyber-attacks and the likelihood of such attacks occurring. It involves identifying, analyzing, and prioritizing potential security threats, and evaluating the current security measures in place to mitigate those threats.

The goal of a cyberattack risk assessment is to identify areas of risk and recommend steps that can be taken to reduce the risk of a successful attack, thereby improving the overall security posture of an organization.

With Network Detective Pro you can engage end-users in performing a Cyberattack Risk Assessment. You can create a custom download page where users will download and run a simple data collector. You can then download the scan results and generate a Cyberattack Risk Assessment Report.

Follow these steps to perform a Cyberattack Risk Assessment:

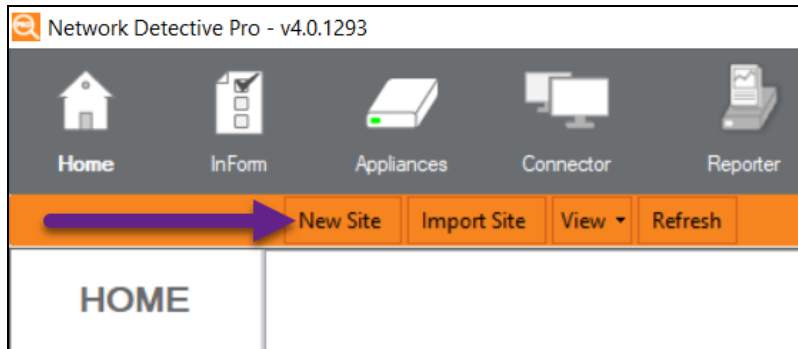
Step 1 — Download and Install the Network Detective Pro app

Go to <https://www.rapidfiretools.com/ndpro-downloads/> to download and install the Network Detective Pro application on a PC on the MSP network. Then run Network Detective Pro and log in with your credentials.

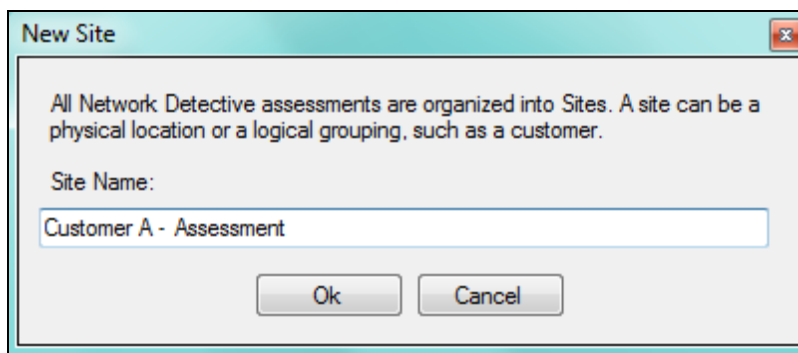
Step 2 — Create a New Site

To create a new site:

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



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

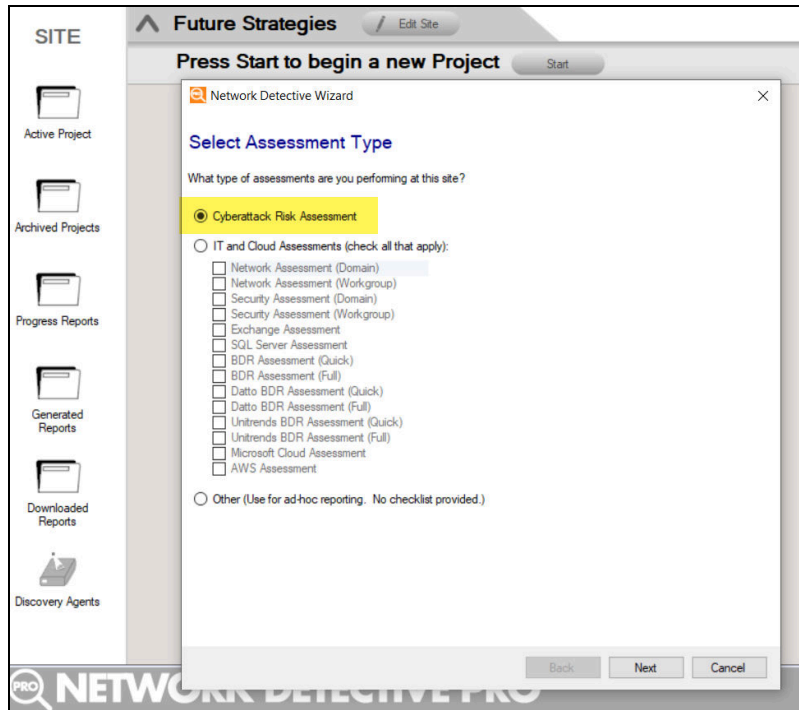


Step 3 — Create Cyberattack Risk Assessment in Network Detective Pro

1. From within the **Site Window**, select the **Start** button that is located on the far right side of the window to start the **Assessment**.

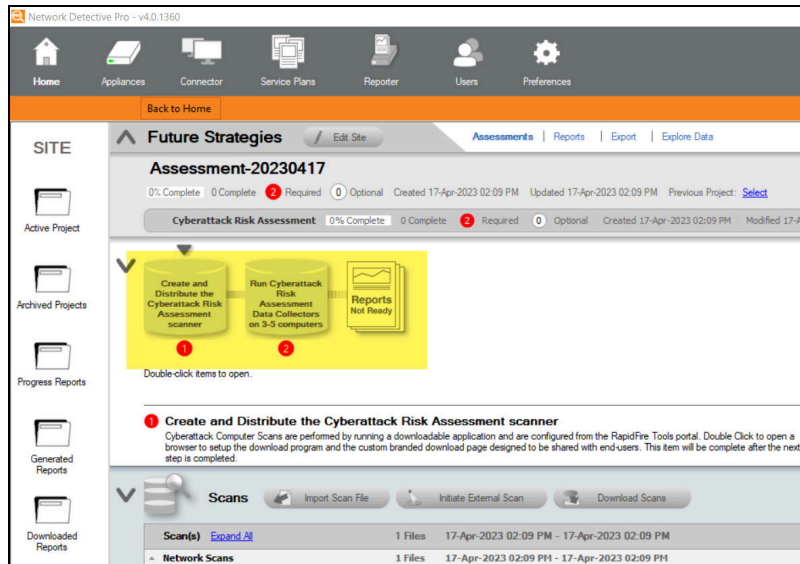


Next, select the **Cyberattack Risk Assessment**.



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

2. Once the new **Cyberattack Risk Assessment** is started, a “**Checklist**” is displayed in the **Assessment Window** presenting the “**Required**” and “**Optional**” steps that are to be performed during the assessment process. Below is the **Checklist** for a **Cyberattack Risk Assessment**.



3. Complete the required **Checklist Items** and use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

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

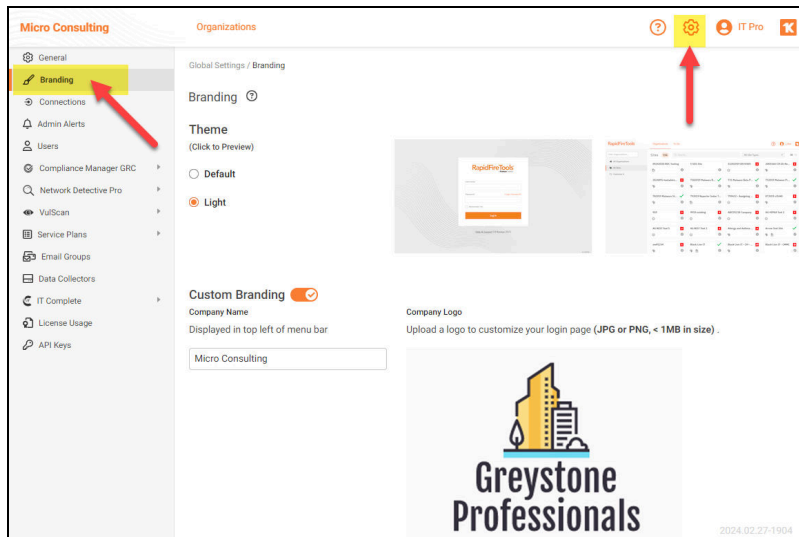


Step 4 — Access RapidFire Tools Portal and Customize Branding

Access the RapidFire Tools Portal at <https://www.youritportal.com>. Then, customize the branding for the end-user download page. The download page is where end-users will access the computer scanner. It can be customized with your own company logo, for

example. From the RapidFire Tools Portal, navigate to global **Settings (Admin)** > **Branding** and make your changes.

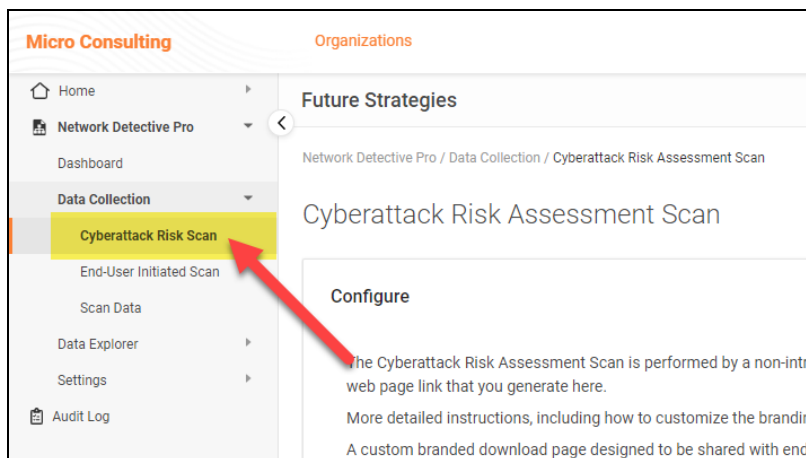




Step 5 — Create and Distribute the Cyberattack Risk Assessment Computer Scanner

Next, you will enable end-users to download and run the Cyberattack Risk Assessment Computer Scanner.

1. From the RapidFire Tools Portal, open your Network Detective Pro site and navigate to **Data Collection > Cyberattack Risk Scan**.



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

Cyberattack Risk Assessment Scan

Configure

The Cyberattack Risk Assessment Scan is performed by a non-intrusive scanning application that is downloaded from a site-specific, custom web page link that you generate here.

More detailed instructions, including how to customize the branding on the download page, are available [here](#).

A custom branded download page designed to be shared with end-users for local computer scans can be generated and managed below:

Click Generate to create a unique download page

Generate Delete Open Copy

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☒ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

3. **Copy the URL** and distribute the URL to end-users.

Configure

The Cyberattack Risk Assessment Scan is performed by a non-intrusive scanning application that is downloaded from a site-specific, custom web page link that you generate here.

More detailed instructions, including how to customize the branding on the download page, are available [here](#).

A custom branded download page designed to be shared with end-users for local computer scans can be generated and managed below:

<https://greystone.alert-central-staging.com/download/cybersecurity-computer-s> **Regenerate** Delete Open **Copy**

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☒ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

Save options Cancel

You can also configure several scan options. Uncheck optional scan items to reduce scan time.

Select Scan Options:

Uncheck optional scan items to reduce scan time.

- ☒ Perform Deep Scan for Sensitive Information
 - ☒ Only Scan Documents and Download Folders
- ☒ Web Filtering Validation
- ☒ Malicious File Download Validation
- ☐ External Vulnerability Scan
- ☒ Detect Stored Browser Credentials

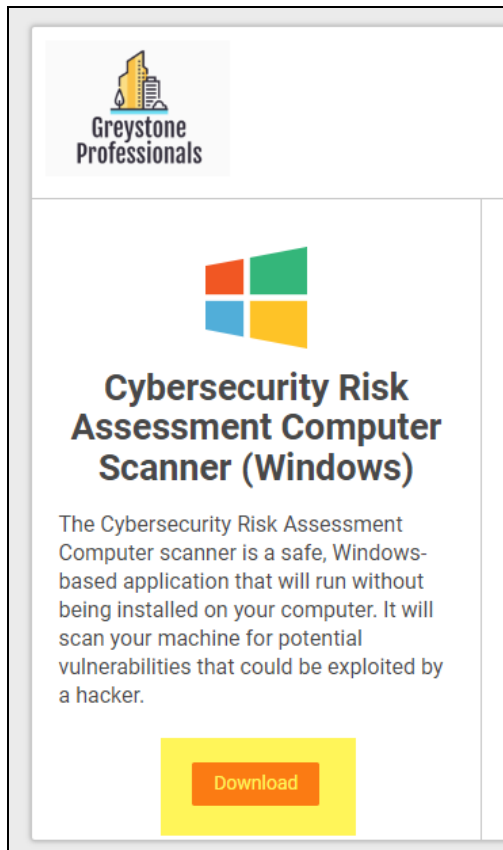
Save optionsCancel

Here's a breakdown of each scan option. When you change scan settings, the changes are applied to the next scan you perform.

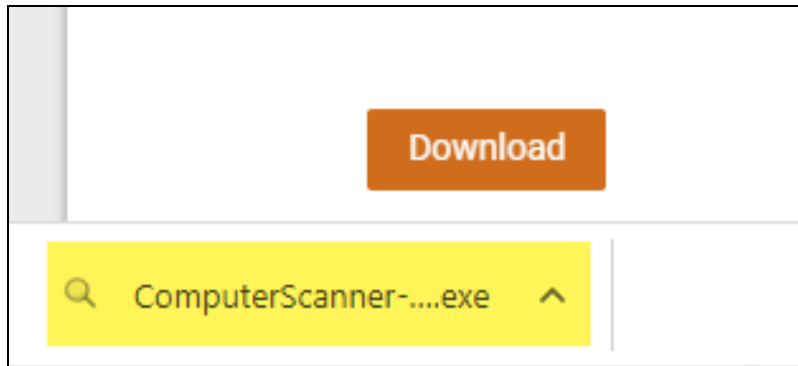
Perform Deep Scan for Sensitive Information	Scan for Personal Identifiable Information (PII) on the device
Web Filtering Validation	Check to see if the device can access websites that might pose a security risk
Malicious File Download Validation	Check to see if the device can download files that might pose a security risk
External Vulnerability Scan	Perform a scan to detect potential external vulnerabilities
Detect Stored Browser Credentials	Check for cached users IDs and passwords

Step 6 — Users Downloads and Runs Cyberattack Risk Assessment Computer Scanner

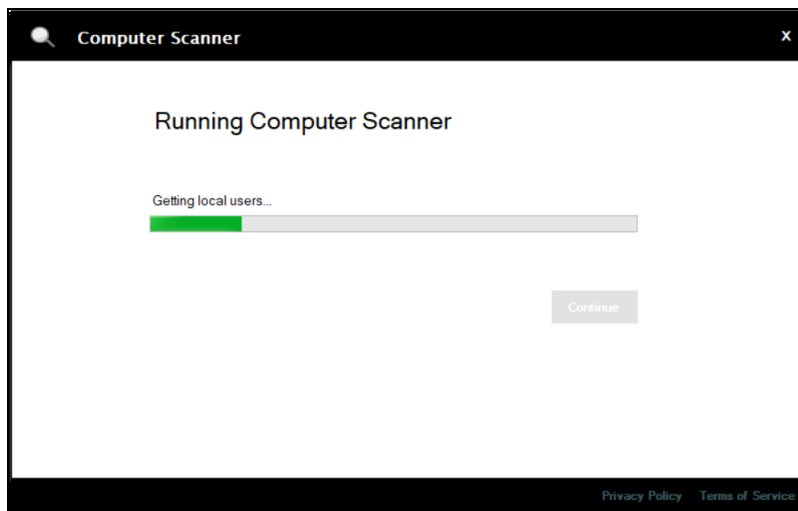
1. In this step, the end-user opens the URL that you provide. The end-user then clicks **Download** under the Cyberattack Risk Assessment Computer Scanner.



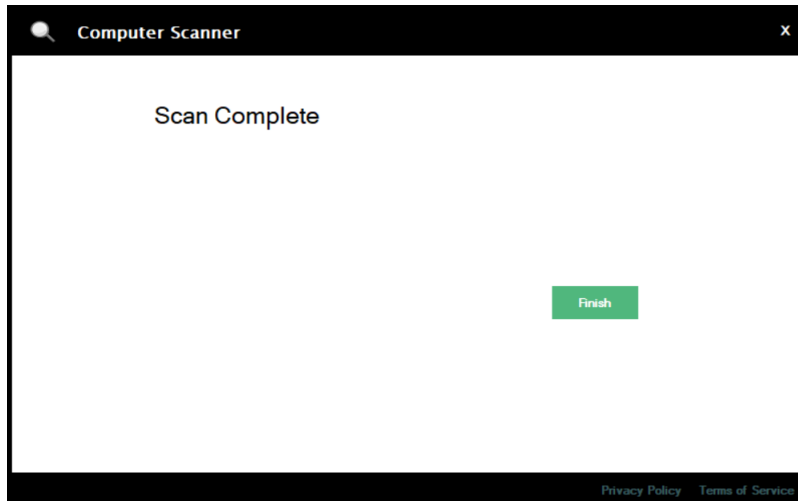
2. The end-user then opens the downloaded scanner.



3. The computer scanner will begin collecting data. This process will take a few minutes.



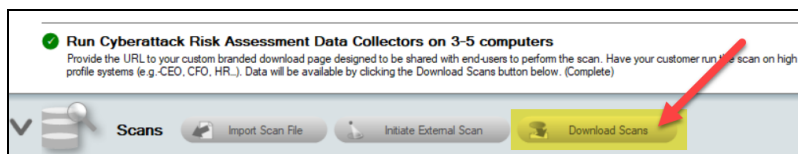
4. When the scan is complete, the end-user clicks Finish. The scan file will automatically be uploaded to Network Detective Pro and become available for you to download.



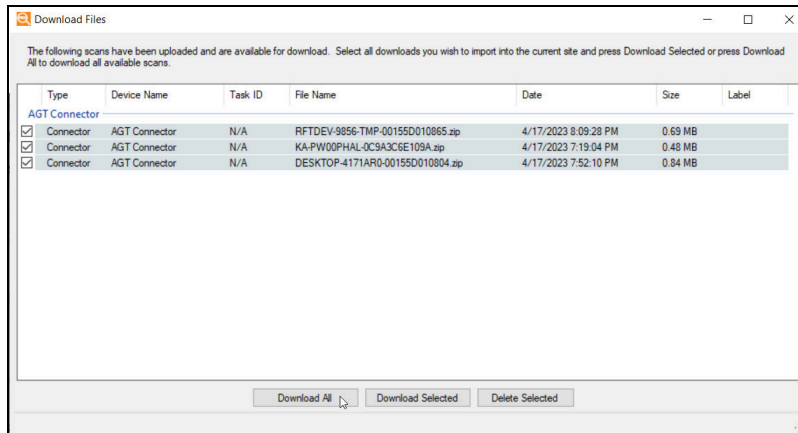
Note: You must run the Cyberattack Risk Assessment Computer Scanner on at least 3 devices in order to advance your assessment.

Step 7 — Download Scans in Network Detective Pro Cyberattack Risk Assessment

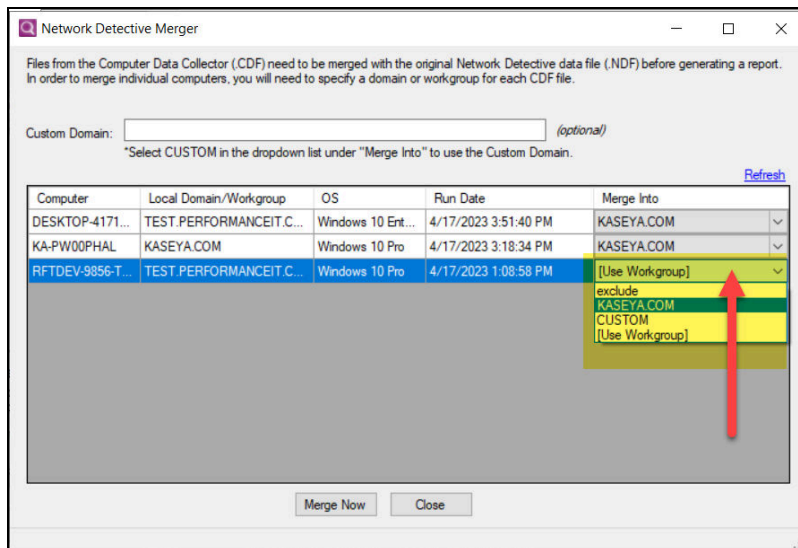
1. Next, return to Network Detective Pro and open your Cyberattack Risk Assessment project.
2. From the Scans bar, click **Download Scans**.



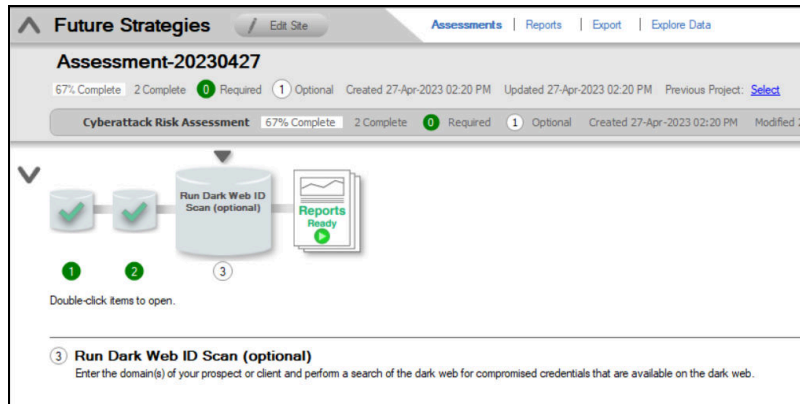
3. **Select and download** your Cyberattack Risk Assessment scans.



- For each scan file, **choose a merge option**. Select the domain or workgroup in which to merge the scan. This will determine how the scan data is organized in your reports. Then click **Merge Now**.



- Once you have downloaded and **merged at least 3 scan files into your assessment**, your checklist will be marked complete. You can now run the optional **Dark Web ID Scan**.

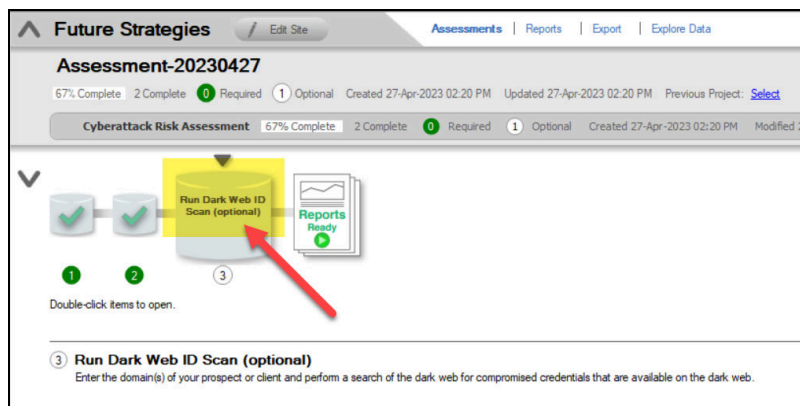


Step 8 —(Optional) Run Dark Web ID Scan

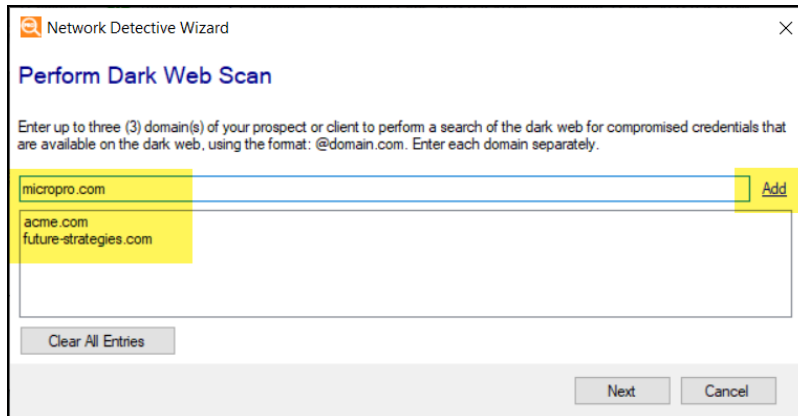
In this step, you can perform a **Dark Web Scan** for compromised usernames and passwords that may exist on the dark web. A sample of the results will appear in your assessment reports. You can ["Set Up Dark Web ID Integration with Network Detective Pro" on page 16](#) to retrieve the full list of compromised credentials.

To run the Dark Web Scan:

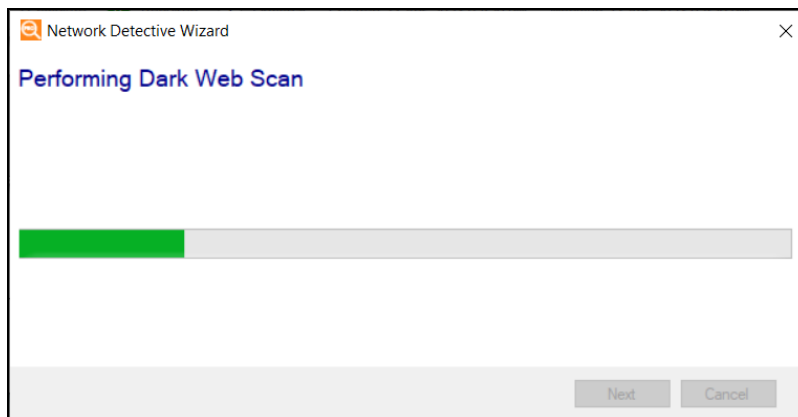
1. Double click on the **Run Dark Web ID Scan** to do item.



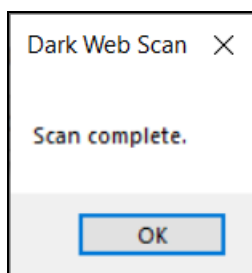
2. Enter a domain and click **Add**. **YOU CAN ENTER A MAXIMUM OF 3 DOMAINS**



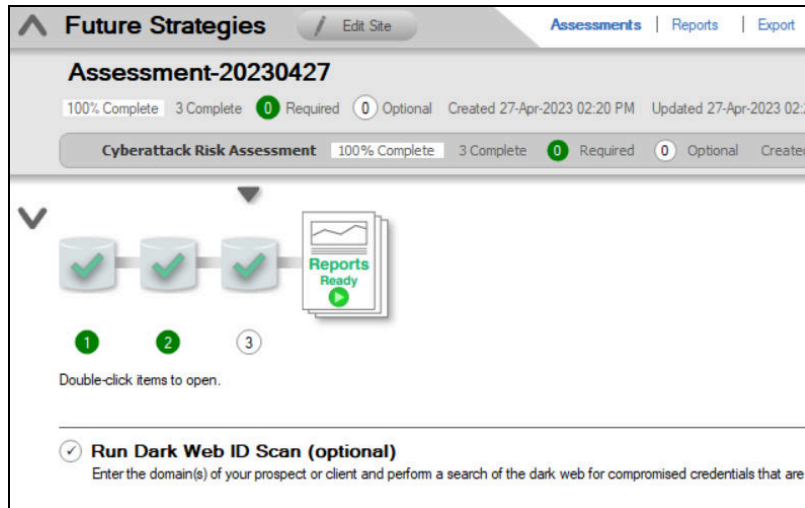
- When you finish entering domains to scan, click **Next**. The Dark Web Scan will begin.



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



- The Run Dark Web ID Scan will be marked complete in your assessment To Do list.



Set Up Dark Web ID Integration with Network Detective Pro

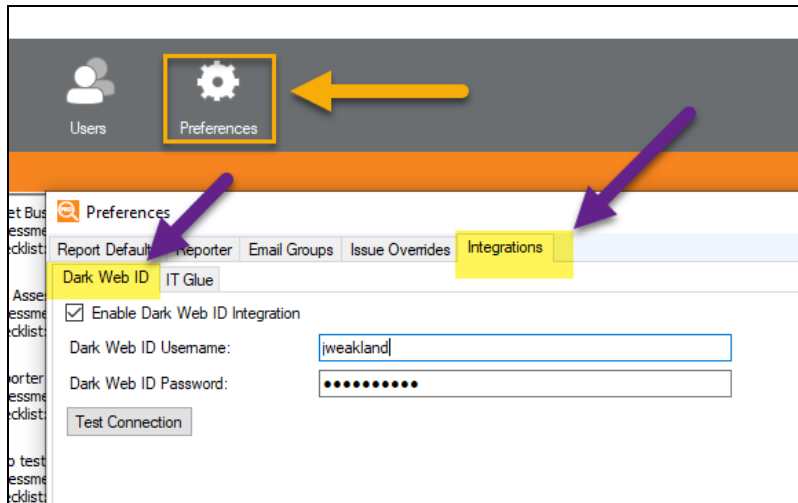
By default, the Dark Web Scan will only return the **first 5** compromised passwords identified for each domain you specify. However, **Dark Web ID** users (<https://www.idagent.com/>) can access full reporting for compromised passwords. To set this up:

First, contact Dark Web ID Support to Enable User API Access. To enable API Access, the Dark Web ID customer must open a ticket with Kaseya Support. The Dark Web ID team will grant the customer API access. Once the support ticket is closed, the user can successfully enter and test their credentials in Network Detective Pro. See also <https://helpdesk.kaseya.com/hc/en-gb/articles/4407392147345-How-can-I-enable-API-access-for-ID-Agent->.

Once you enable Dark Web ID API access, you can set up the integration in Network Detective Pro. To do this:

1. In the Network Detective Pro app, click **Preferences** from the top menu.
2. Click the **Integrations** tab
3. From the **Dark Web ID** tab, **enable** the Dark Web ID Integration.
4. Then enter your Dark Web ID **Username** and **Password**.
5. Finally, click **Test Connection**. Once you verify the connection works, click **OK** to

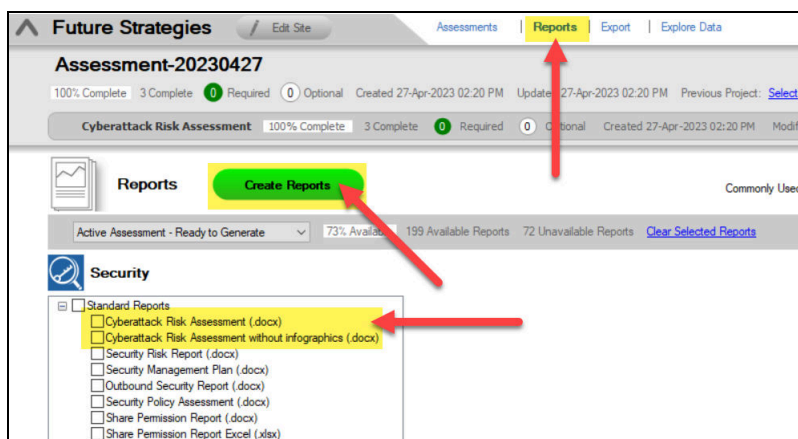
dismiss the Preferences menu.



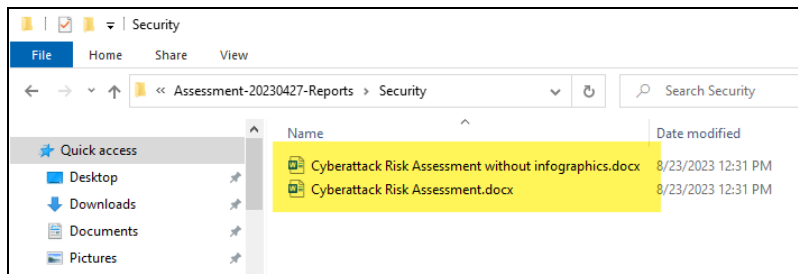
Step 9 — Generate Reports

To generate reports:

1. Open **Reports**.
2. Select the **Cyberattack Risk Assessment report**. You can choose to generate the report with or without infographics.
3. Click **Create Reports**.



4. The **Cyberattack Risk Assessment Report** will then become available in Windows Explorer.



Cyberattack Risk Assessment Reports

In addition to the standard Security assessment reports, the **Cyberattack Risk Assessment** module can generate the following additional reports:

Standard Reports

Report Name	Description
Cyberattack Risk Assessment Report	The Cyberattack Risk Assessment Report is a systematic examination of your organization's potential vulnerabilities to cyber-attacks and the likelihood of such attacks occurring. It involves identifying, analyzing, and prioritizing potential security threats, and evaluating the current security measures in place to mitigate those threats. This graphically-rich report includes an overall risk score, executive summary, and detailed findings.
Cyberattack Risk Assessment Report without infographics	You can generate the Cyberattack Risk Assessment Report without infographics.