GROUND LABS

CARD RECON

User Guide

Card Recon 3.0.4

Table of Contents

CR DESKTOP / SERVER 3.0.4 RELEASE NOTES 4
NEW PLATFORM INTEGRATIONS 4
Scan and Remediate Newly Supported Windows Server and macOS Versions 4
IMPORTANT SECURITY ENHANCEMENTS 4
IMPORTANT NOTES 4
Upcoming End-of-Support Platforms and Features 4
CHANGELOG 4
What's New? 5
Enhancements 5
Bug Fixes 5
SUMMARY OF CHANGES 6
TARGETS 6
ABOUT CARD RECON 3.0.4 7
OVERVIEW 7
Who is Card Recon Suitable For 7
Additional Resources 7
FEATURES 7
DISCLAIMER 8
SYSTEM REQUIREMENTS 9
CERTIFIED OPERATING SYSTEMS 9
GETTING STARTED 11
SYSTEM REQUIREMENTS 11
DOWNLOAD CARD RECON 11
RUN YOUR FIRST SCAN 11
SET UP CARD RECON 12
WINDOWS GUI 12
LINUX SHELL 12
RUNNING CARD RECON AS A PORTABLE APPLICATION 12
RUNNING THE CARD RECON GUI 14
RUNNING THE CARD RECON CLI 17
RUNNING THE CARD RECON CLI ON WINDOWS 17
Method 1 17
Method 2 17
RUNNING THE CARD RECON CLI ON MACOS, LINUX AND UNIX-LIKE SYSTEMS 18
Enabling Full Disk Access in macOS Systems 18
Running the Card Recon CLI 19
Opening Compliance Reports 20
CARD RECON LICENSING 21
SUBSCRIPTION LICENSE 21
TARGETS 21
CARD RECON DESKTOP AND CARD RECON SERVER 21
Feature Comparison 22
HOW LICENSING WORKS 23
ASSIGNING LICENSES 24
ASSIGNING A LICENSE THROUGH THE GROUND LABS SERVICES PORTAL 24
OFFLINE LICENSES 25
ASSIGNING LICENSES THROUGH OTHER MEANS 25
GETTING HOST NAME AND MAC ADDRESS 27
WINDOWS SYSTEMS 27

UNIX-LIKE SYSTEMS (LINUX, UNIX, FREEBSD, OSX ETC.) 27
LOGGING INTO CARD RECON 29
ONLINE AUTHENTICATION 29
Ground Labs Services Login 30
Scan Token Login 30
OFFLINE AUTHENTICATION 31
Selecting Login with Offline License File 31
Using an Offline License File on the Windows GUI 31
Using an Offline License File on the CLI 32
Placing the Offline License File in the Same Folder as the Card Recon Executable 32
GENERATING AND USING SCAN TOKENS 33
GENERATING SCAN TOKENS 33
Identifying Scan Tokens 34
USING AND ACTIVATING SCAN TOKENS 34
SINGLE OR MULTIPLE-USE SCAN TOKENS 35
CONFIGURING SCANS FOR CARD RECON 37
CARD RECON GRAPHIC USER INTERFACE 38
SELECTING CARD DATA TYPES 39
SELECTING TARGET LOCATION 40
LOCAL STORAGE 41
ALL LOCAL FILES 41
ALL LOCAL SHADOW VOLUMES 42
ALL LOCAL FREE DISK SPACE 42
LOCAL MEMORY 43
SETTING RESOURCE USAGE 44
LIMIT CPU THROUGHPUT 44
LIMIT SEARCH THROUGHPUT 45
SUSPEND SEARCH SCHEDULE 45
SETTING CUSTOM SEARCH RULES 46
LIST OF SEARCH FILTERS 46
SETTING RESULTS DATABASE OPTIONS 49
RESULTS DATABASE LOCATION 50
RESULTS DATABASE SIZE 50
ENCRYPT DATABASE 51
SETTING COMPLIANCE REPORT SAVINGS OPTIONS 52
ONLINE REPORTING 52
SAVE COMPLIANCE REPORTS 53
SAVE AND LOAD OPTIONS 54
SAVING AND LOADING SEARCH CONFIGURATIONS 54
Load Search Configuration 54
Save Search Configuration 55
SAVING AND LOADING RESULTS DATABASE 55
Load Results Database 55
Save Results Database 55
SAVING MATCH LISTS 55
SAVING COMPLIANCE REPORTS 56
RESULTS AND REMEDIATION 57
COMPLIANCE REPORT 59
REMEDIATING AND MARKING MATCHES 63
CARD RECON COMMAND-LINE INTERFACE 64
GETTING STARTED WITH THE CLI 65
LOCATE CARD RECON CLI 65
RUNNING CARD RECON CLI 65
CARD RECON CLI OPTIONS 66

SETTING UP A WINDOWS VIRTUAL MACHINE 68
SYSTEM REQUIREMENTS 68
DOWNLOAD WINDOWS VM 68
INSTALLING THE VIRTUAL MACHINE 69
THIRD-PARTY SOFTWARE DISCLAIMER 71

CR DESKTOP / SERVER 3.0.4 RELEASE NOTES

The Release Notes provide information about new features, platforms, data types, enhancements, bug fixes and all the changes that have gone into **Card Recon 3.0.4**.

Contents:

1. Highlights
    - New Platform Integrations
    - Important Security Enhancements
2. Important Notes
    - Upcoming End-of-Support Platforms and Features
3. Card Recon 3.0.4 Changelog
    - What's New?
    - Enhancements
    - Bug Fixes

NEW PLATFORM INTEGRATIONS

Scan and Remediate Newly Supported Windows Server and macOS Versions

NEW With Card Recon 3.0.4, you can now scan Windows Server 2025 and macOS Sequoia environments. Scanning and remediation are supported for both newly added operating systems.

For more information, see Certified Operating Systems.

> **Note:** Remediating and marking matches are supported for Windows Server Targets through the Card Recon GUI only.

IMPORTANT SECURITY ENHANCEMENTS

This release of **Card Recon 3.0.4** brings updates to the TLS protocol library to enhance the overall security of the application.

IMPORTANT NOTES

Upcoming End-of-Support Platforms and Features

The following platforms and/or features will reach end of support and be removed in the upcoming **Card Recon 3.0.5** release:

- macOS System Targets
    - macOS Monterey 12

CHANGELOG

The Changelog is a complete list of all the changes in **Card Recon 3.0.4**.

What's New?

- New Platform Integrations:
  - NEW Windows Server 2025
  - NEW macOS Sequoia 15

Enhancements

- Improved Features:
  - Updated TLS protocol library for increased application security.

Bug Fixes

- File contents could not be decoded properly and would cause scans to stall when scanning certain types of compressed PDFs with repeated elements (e.g., images, tables, attachments).

Ensuring we are delivering the best technology for our customers is a core value at Ground Labs. If you are interested in future early builds of Card Recon with forthcoming features, please email your interest to product@groundlabs.com.

SUMMARY OF CHANGES

This section provides a summary of the **Card Recon 3.0.4** changes from **Card Recon 3.0.3**.

- Targets

TARGETS

Target / Component	Card Recon 3.0.4	Card Recon 3.0.3
macOS Workstation • macOS Sequoia 15 NEW	Supported.	-
Windows Server Target • Windows Server 2025 64-bit NEW	Supported.	-

ABOUT CARD RECON 3.0.4

OVERVIEW

Card Recon is a data discovery tool that scans storage media and systems that may hold cardholder data. Built on the Payment Card Industry Data Security Standard (PCI DSS ®), Card Recon can search documents, local database files, local email files, etc. in your systems to find more than 160 combinations of Personal Account Number (PAN) structures used in 10 major card brands across more than 200 countries.

Accurate and powerful, Card Recon is the PCI compliance tool of choice for more than 300 Qualified Security Accessors (QSAs), and trusted by over 2,500 merchants across 80 countries. Support for 7 operating systems means that Card Recon can cover the majority of common system types used by organizations.

Who is Card Recon Suitable For

Card Recon is ideal for security consultants and small businesses with a requirement to scan up to 5 systems. **Card Recon Desktop** is designed for scanning the contents of workstations, while **Card Recon Server** is designed for sample-based scanning of file servers.

For environments with 5 or more systems with a requirement to scan workstations, servers, database systems, emails, or cloud storage platforms, it is recommended that our Enterprise Recon solution be used due to its centralized design, support for a variety of platforms, ability to automate scanning, and capability to consolidate reporting data from multiple scans.

Additional Resources

1. Advanced support: https://www.groundlabs.com/submit-a-ticket/
2. Card Recon product page: https://www.groundlabs.com/card-recon/
3. Ground Labs home page: https://www.groundlabs.com
4. Card Recon End User License Agreement: https://www.groundlabs.com/eula/

FEATURES

- **Built for PCI Compliance**: Out-of-the-box cardholder data detection for 10 major card brands that can find 160+ combinations of PAN structures used across more than 200 countries.
- **Accurate and Powerful**: Our data discovery algorithms are extensively tested to produce fast and accurate search results. False positives are managed by a built-in detection algorithm that filters test results to keep your scans effective.
- **Search almost Anything**: This software searches a wide range of file types in offline locations for workstations and file servers [1].
- **PCI Compliance Reporting**: Generate comprehensive and easy-to-read compliance reports that are detailed and actionable. Reports can be saved to various formats (e.g. PDF, HTML, CSV etc.), making them highly portable.
- **Powerful Remediation**: When found, data security risks can be securely removed, quarantined, or masked by our powerful remediation tools without

leaving the software.

- **7 Platforms with No Installation Required** [1]: Card Recon can run, without installation, on any of the 7 supported platforms. It also can run from portable storage media.
- **Low CPU Usage**: Designed to minimize impact on users or production applications so that you can keep your systems secure without having to schedule downtime.

[1] : See System Requirements for more information on the platforms that are supported for Card Recon Desktop and Card Recon Server.

DISCLAIMER

It is important that you read and understand this document, which has been prepared for your gainful and reasonable use of Card Recon Desktop and Card Recon Server. Use of both Card Recon editions and these documents reasonably indicate that you have agreed to the terms outlined in this section.

Reasonable care has been taken to make sure that the information provided in this document is accurate and up-to-date; in no event shall the authors or copyright holders be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with these documents. If you have any questions about this documentation please contact our support team by sending an email to support@groundlabs.com.

Examples used are meant to be illustrative; users' experience with the software may vary.

No part of this document may be reproduced or transmitted in any form or by means, electronic or mechanical, for any purpose, without the express written permission of the authors or the copyright holders.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

SYSTEM REQUIREMENTS

Card Recon 3.0.4 is designed to use as few system resources as possible, and will run on most modern systems.

Min. Memory: 128 MB

CERTIFIED OPERATING SYSTEMS

Note:

- Ground Labs is unable to warrant full official support for Card Recon for the versions other than those listed in the Table 1: Certified Operating Systems.
- If your organization uses an environment not listed in the table below, please contact support@groundlabs.com.

Category	Operating Systems
Windows Desktop Environments (GUI and Command-Line)	• Windows 10 32-bit/64-bit • Windows 11 64-bit
macOS System Environments (Command-Line only)	• macOS Monterey 12 • macOS Ventura 13 • macOS Sonoma 14 • macOS Sequoia 15 **Note: Full disk access required for macOS Targets** Scanning macOS Target locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for the Terminal prior to the first scan of the macOS Target. Locations not granted full access will be logged as inaccessible locations. See Enabling Full Disk Access in macOS Systems for more information.
[S] Windows Server Environments (GUI and Command-Line)	• Windows Server 2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit • Windows Server 2025 64-bit

Category	Operating Systems
[S] Linux System Environments (Command-Line only)	• Debian 11+ 32-bit/64-bit • Oracle Linux 8+ 64-bit • RHEL 7+ 64-bit • Ubuntu 16 32-bit/64-bit • Ubuntu 18+ 64-bit **Note:** A minimum Linux Kernel version of 2.6 is required.
[S] UNIX System Environment (Command-Line only)	FreeBSD 13+ 32-bit/64-bit
[S] EBCDIC for Mainframes	Files copied from mid-range and mainframe systems such as AS/400, S/390 and iSeries encoded using IBM's Extended Binary Coded Decimal Interchange Code (EBCDIC).

[S] : Requires Card Recon Server

GETTING STARTED

Card Recon requires no installation to run scans.

SYSTEM REQUIREMENTS

Before you start, check your system requirements. For a list of certified operating systems, see System Requirements.

To check the version of the operating system you are running:

- **Windows**: See Microsoft's Which Windows operating system am I running?.
- **macOS**, **Linux and other UNIX-like operating systems**: Run the `uname-r` command to check the kernel you are running.

DOWNLOAD CARD RECON

If you have not obtained a licensed copy of Card Recon you can get a free trial, or purchase Card Recon from here.

Once you have obtained a trial or purchased license, you should receive an email containing instructions for validating and using your license. Your Ground Labs Services Portal user name and password will be sent to you via email.

> **Note:** If you have problems with your Ground Labs Services Portal user name and password, please contact the person managing your licensing details or Ground Labs support.

1. Go to Ground Labs Services Portal and log in.
2. On the dashboard, click to download the Card Recon version that matches your operating system
    - Card Recon Command-Line Interface (CLI) applications.
    - Card Recon Graphical User Interface (GUI) applications.

RUN YOUR FIRST SCAN

To run your first scan:

1. License your scan Target.
2. Scan.
3. Remediate/Report.

SET UP CARD RECON

Note: Administrator privileges are required for Card Recon to run.

Once downloaded, locate the **Card Recon** executable in your downloads folder. By default, Card Recon saves results, journal files, configuration files, and compliance reports in the same folder as the executable file.

To keep all these files in one place, create a folder called `cardrecon` and move your Card Recon executable into it.

WINDOWS GUI

To set up Card Recon with the Windows GUI:

1. Create a new folder in Windows Explorer
2. Move the Card Recon executable to the new folder

LINUX SHELL

In your terminal, run the following commands:

```
# In your downloads directory ~/Downloads/
mkdir cardrecon

# Moves the Card Recon executable to the ~/cardrecon/ directory
mv cr_linux26_x.x.x cardrecon

# Changes working directory to ~/cardrecon/
cd cardrecon
```

RUNNING CARD RECON AS A PORTABLE APPLICATION

Card Recon is a portable application. You can put Card Recon on a portable storage drive and run it on any authorized host system.

Info: For a list of certified operating systems and system requirements, see System Requirements.

To run Card Recon as a portable application:

1. Download the appropriate version of Card Recon for your system.
2. Download an Offline License File. See Offline Authentication.
3. Place the Offline License File in the same folder as your Card Recon executable.
4. Run Card Recon.

RUNNING THE CARD RECON GUI

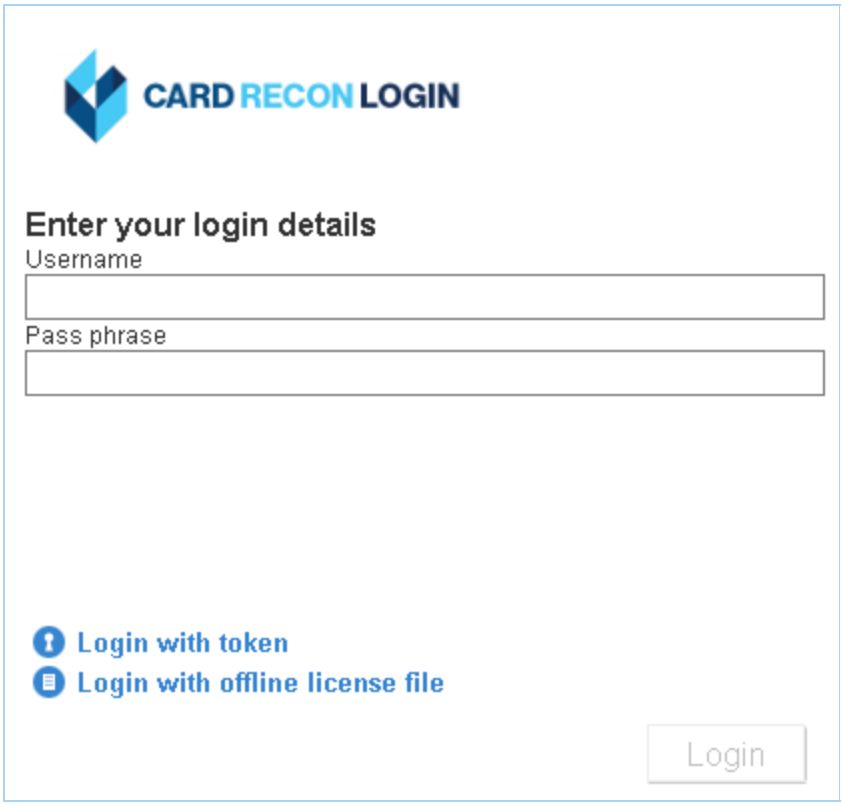
Info:
When the Card Recon runs, it looks for these files in its directory:

- `cardrecon.cfg` : default Card Recon configuration file.
- `<license-file-name>.li2` : Offline License File; Card Recon looks for any file ending with `.li2` .

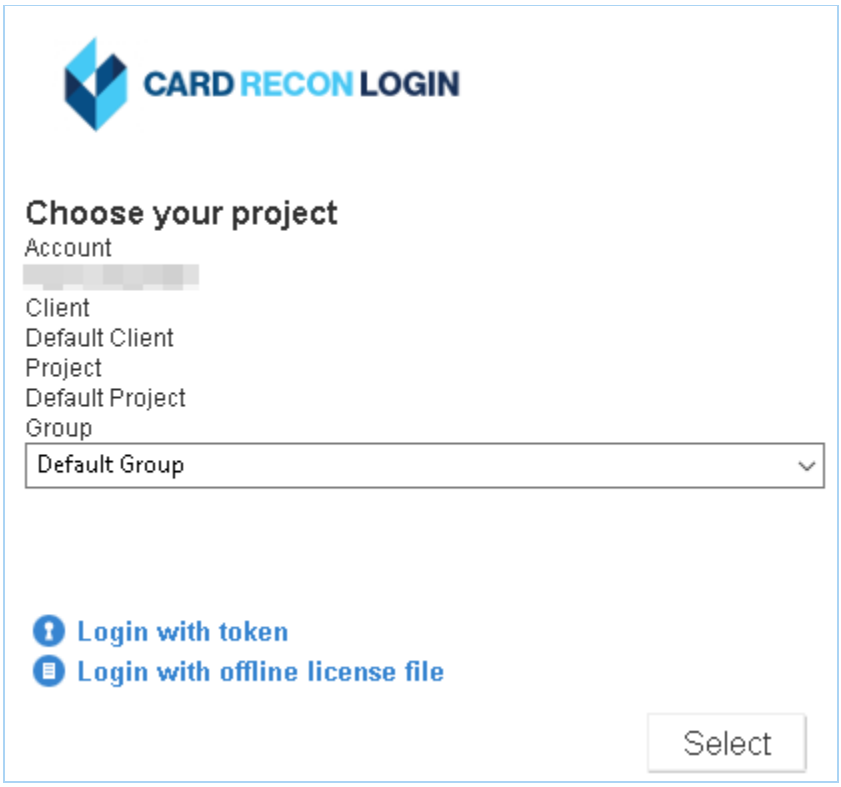
If it finds any of these files in the directory that the Card Recon executable occupies, it will try to load them when the Card Recon runs.

To run **Card Recon**:

1. Double-click on the Card Recon executable (e.g. `cr_gui_x.x.x.exe`) to run Card Recon.
2. In the Card Recon login window, enter your Ground Labs Services Portal user name and password.



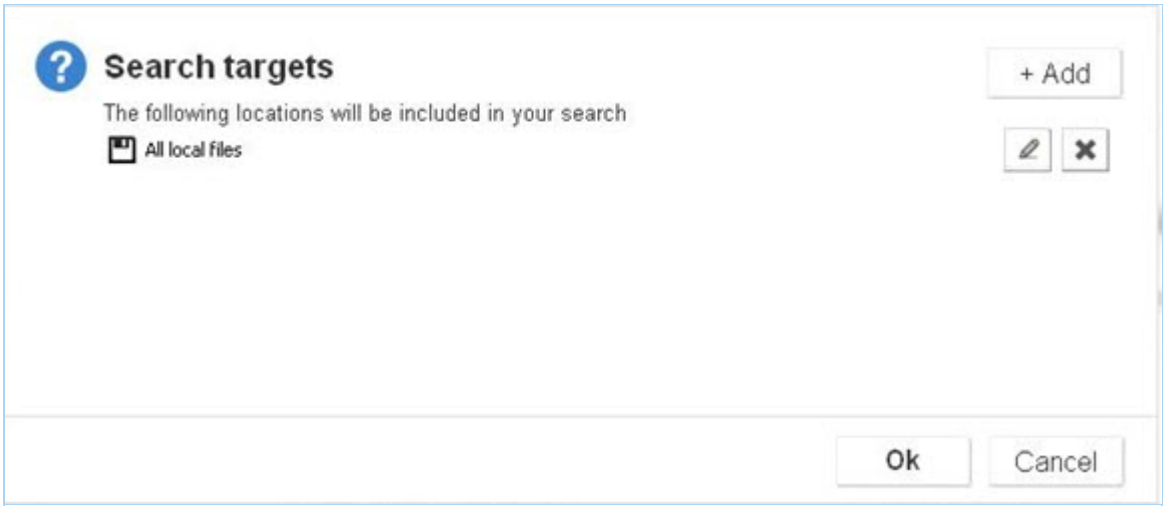
3. From the **Choose your project list**, select your project and click **Select**.



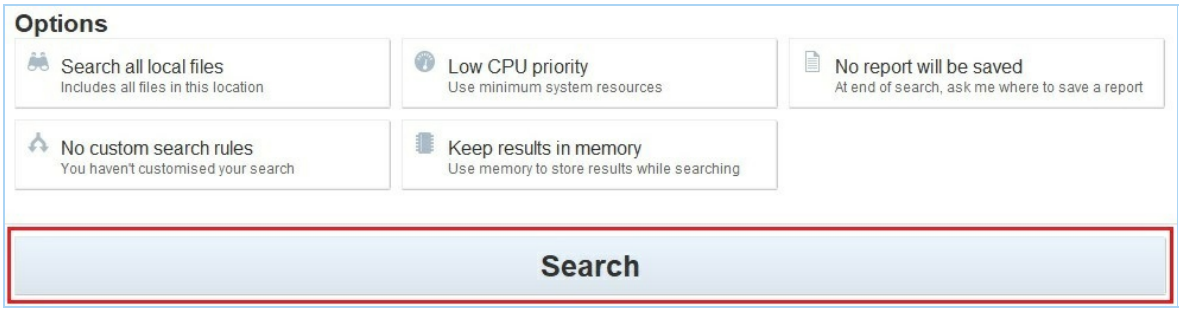
> **Note: Managing licenses**
> Project and license groups are usually used by the licensees or IT administrators who manage your software licenses to assign permissions to certain groups of users.
>
> If you are not sure of which project or license group to use, contact your IT administrator or the licensee for more information. If you are the licensee, IT administrator, or the only user, you can choose **Default Project** or **Default Client**.
>
> For more information on how to manage your licenses, please see Card Recon Licensing.

4. On the dashboard, select the card data types to include in your scan.

5. (Optional) Click **Search all local files** to change the Target that you want to scan (the default Target is the host's local storage). See Selecting Target Location for more information.



6. Click **Search** to start scanning.



When you click **Search**, Card Recon checks if you have valid licenses for the Targets that you wish to scan, and prompts you if you do not.

After a scan is completed, you can see the scan's results. For details, see Results and Remediation.

RUNNING THE CARD RECON CLI

Running the **Card Recon** CLI executable immediately attempts a scan.

> **Info:**
> When the Card Recon runs, it looks for these files in its directory:
>
> - `cardrecon.cfg` : default Card Recon configuration file.
> - `<license-file-name>.li2` : Offline License File; Card Recon looks for any file ending with `.li2` .
>
> If it finds any of these files in the directory that the Card Recon executable occupies, it will try to load them when the Card Recon runs.

The Card Recon CLI automatically loads `cardrecon.cfg` when run, altering your scan configuration. If your loaded `cardrecon.cfg` is set up for Card Recon to load a specific journal file, Card Recon loads that journal file when run with `cardrecon.cfg` .

If you do not want to load these files when you run the Card Recon CLI, use the `-c` and `-journal` flags OR remove these files from the directory.

For more information, see Card Recon CLI Options.

RUNNING THE CARD RECON CLI ON WINDOWS

Locate the Windows CLI executable: `cr_x.x.x.exe`

There are 2 ways to run the Windows CLI.

Method 1

1. Locate `cr_x.x.x.exe` in Windows Explorer.
2. Right-click `cr_x.x.x.exe` , select **Run as administrator** and enter the administrator password if prompted.
3. In the terminal, Card Recon will prompt you to validate your license.
4. Log in using one of the three methods (see Logging into Card Recon for more information):
    - Ground Labs Login.
    - Use an Online Token.
    - Use Offline License File.

> **Info:** Card Recon may ask you to select a Client and Project Group. If you are the only user or the licensee, select **Default Client** and **Default Project** when prompted . If not, check with your system administrator or the licensee.

Card Recon will run with default settings – i.e. it scans all local storage with default search parameters (see Selecting Card Data Types for more information).

Method 2

1. Click **Start** to open the Start Menu.
2. Enter `cmd` to search for `cmd.exe` , or find it in **Start** > **All Programs** > **Accessories** > **Command Prompt**.

3. Right-click `cmd.exe` or the Command Prompt program and select **Run as administrator**. Enter the administrator password if prompted.
4. In the newly-opened Command Prompt window, navigate to the folder where your Card Recon executable is located.

```
# If your Card Recon executable is in the Downloads folder
cd c:\User\username\Downloads\
```

5. To run the Card Recon executable with default settings, issue this command:

```
# Run a default scan, save a compliance report and an encrypted database jo
urnal file.
cr_x.x.x.exe -j journal-filename.jnl -password-inline password
```

> **Info:** Saving a database journal file allows you to inspect and remediate matches in the Card Recon GUI.

6. Card Recon prompts you to validate your license.
7. Log in using one of the three methods (see Logging into Card Recon for more information):
   - Ground Labs Login.
   - Use an Online Token.
   - Use Offline License file.

> **Info:** Card Recon may ask you to select a Client and Project Group. If you are the only user or the licensee, select **Default Client** and **Default Project** when prompted . If not, check with your system administrator or the licensee.

8. Once logged in, Card Recon runs a scan with default settings. When the scan completes, Card Recon automatically saves a compliance report.

> **Info:** To inspect and remediate matches found by Card Recon, load the database journal file (e.g. `journal-filename.jnl`) saved by the Card Recon CLI in the Card Recon GUI. See Results and Remediation.

RUNNING THE CARD RECON CLI ON MACOS, LINUX AND UNIX-LIKE SYSTEMS

> **Note: Full disk access required for macOS Targets**
> Scanning macOS Target locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for the Terminal prior to the first scan of the macOS Target. Locations not granted full access will be logged as inaccessible locations. See Enabling Full Disk Access in macOS Systems for more information.

Enabling Full Disk Access in macOS Systems

> **Info:** Instructions to enable the "Full Disk Access" feature may vary in different versions of macOS. For more information, see Change Privacy & Security settings on Mac.

For supported macOS systems, the macOS Terminal must have full disk access prior to performing the first scan.

To enable the Full Disk Access feature for the Terminal in macOS:

1. On the macOS Target, open **System Settings**.
2. Click **Privacy & Security** > **Full Disk Access**.
3. Select the toggle button for **Terminal** to enable full disk access.

Note: If the Full Disk Access feature is not enabled prior to the first scan of the macOS Target, you will be prompted during the scan process to allow macOS Terminal full access to each `/Users` folder being scanned. Locations not granted full access will be logged as inaccessible locations.

Running the Card Recon CLI

1. In the Terminal, locate the Card Recon executable. E.g. `cr_linux26_x.x.x`.
2. Open your terminal and run:

```
chmod u+x cr_linux26_x.x.x
```

3. Run the following command as root:

```
# Run a default scan, save a compliance report and an encrypted database jo
urnal file.
./cr_linux26_x.x.x -j journal-filename.jnl -password-inline password
```

4. Card Recon prompts you to validate your license.

   Note: Managing licenses
   Project and license groups are usually used by the licensees or IT administrators who manage your software licenses to assign permissions to certain groups of users.

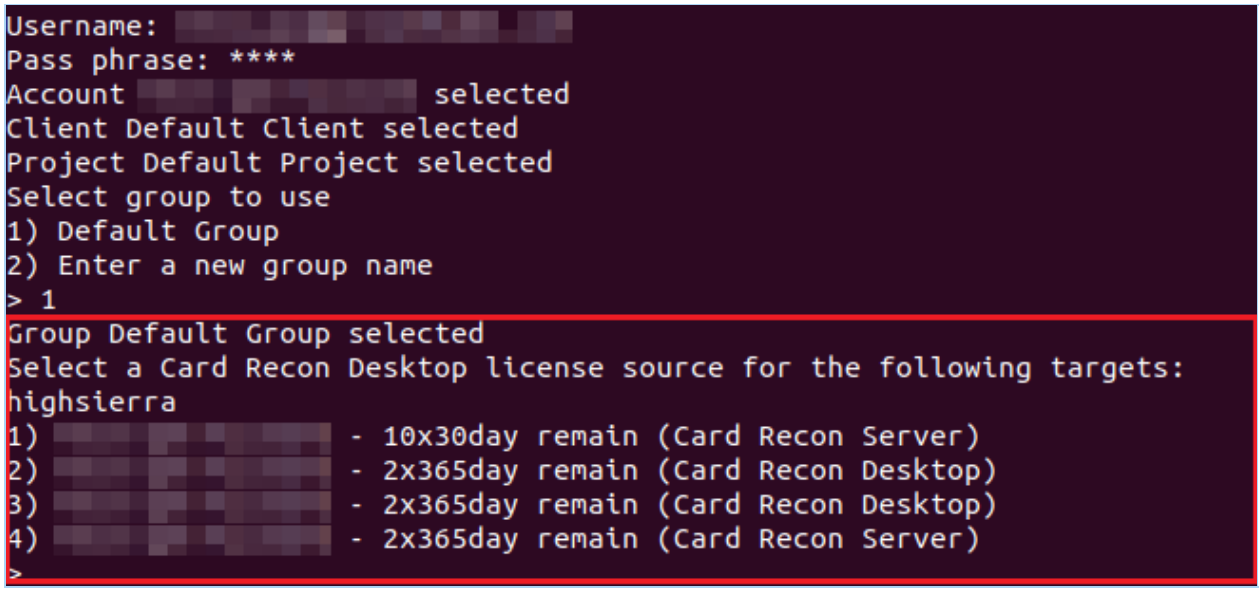
   If you are not sure of which project or license group to use, contact your IT administrator or the licensee for more information. If you are the licensee, IT administrator, or the only user, you can choose **Default Project** or **Default Client**.

   For more information on how to manage your licenses, please see Card Recon Licensing.

5. Log in using one of the three methods (see Logging into Card Recon for more information):
   - Ground Labs Login.
   - Use an Online Token.
   - Use Offline License File.

   Info: Card Recon may ask you to select a Client and Project Group. If you are the only user or the licensee, select **Default Client** and **Default Project** when prompted . If not, check with your system administrator or the licensee.

If you have not assigned a license to the current Target, Card Recon will return a list of licenses available in your Ground Labs Services Portal.



Card Recon should ask you to confirm authorization of the Target. For more information on Card Recon licensing, see Card Recon Licensing.

Card Recon starts scanning the Target with default settings.

Note: If the Full Disk Access feature is not enabled prior to the first scan of the macOS Target, you will be prompted during the scan process to allow macOS Terminal full access to each `/Users` folder being scanned. Locations not granted full access will be logged as inaccessible locations.

Info: To inspect and remediate matches found by Card Recon, load the database journal file (e.g. `journal-filename.jnl`) saved by the Card Recon CLI in the Card Recon GUI. See Results and Remediation.

Opening Compliance Reports

Once the scan is done, Card Recon automatically saves a compliance report. To open these files, issue the following command as administrator:

```
# Where <filename>.pdf is the file saved by Card Recon that you want to open.
chmod 644 <filename>.pdf
```

Info: If you are running the Card Recon CLI with `sudo`, then Card Recon saves files (configuration files, database journal files, and compliance reports) as root.

CARD RECON LICENSING

This section covers the following topics:

- Subscription License
- Targets
- Card Recon Desktop and Card Recon Server

SUBSCRIPTION LICENSE

Card Recon 3.0.4 is licensed to end-users on a per-Target basis.

Licenses typically last a year under the Subscription License model, and will cover standard technical support and updates for the licensed product throughout the term of the license.

More details about the Subscription License can be found in the Ground Labs EULA.

TARGETS

Target Type	License Assignment
Workstations	1 license per workstation (Windows and macOS).
[S] Servers	1 license per server. This allows you to run scans on the local file system and on the process memory. A server is a local computer running any of the following operating systems on a physical host machine or virtual machine: • Windows Server • FreeBSD • Linux

[S] : Requires Card Recon Server

CARD RECON DESKTOP AND CARD RECON SERVER

Card Recon is typically used to scan local storage on workstations for cardholder data.

To use Card Recon to scan servers and use advanced features, you would need to upgrade to a Card Recon Server license.

Feature Comparison

Platform or File Type	Card Recon Desktop [1]	Card Recon Server
Windows	✓	✓
macOS	✓	✓
Linux		✓
FreeBSD		✓
EBCDIC for Mainframes		✓
Note: Some features are not available on all supported operating systems.		
File Formats		
Text Files	✓	✓
Multiple Encoding types	✓	✓
Office Documents	✓	✓
Compressed Files	✓	✓
Local Database Files	✓	✓
Local Email Files	✓	✓
Audio Files		✓
Image File OCR		✓
Target Types		
Local Storage	✓	✓
Free Disk Space	✓	✓
Shadow Volumes	✓	✓
Process Memory	✓	✓
Classification and Remediation		
Mask Cardholder Data	✓	✓
Secure Quarantine	✓	✓
Permanent Delete	✓	✓
Content Inspection	✓	✓
Encryption	✓	✓

[1] To explore a feature-limited version of Card Recon Desktop, get a free Card Recon Trial.

HOW LICENSING WORKS

⚠ **Warning:** License assignment to a Target is **permanent**. You will not be able re-assign your licenses once they have been assigned to a Target. See our Ground Labs EULA for more information.

Before a scan can be run on a Target with **Card Recon**, the Target needs to be assigned a license. Each Target needs its own license. See Selecting Target Location for more details on what would be considered a Target.

Licenses are managed through the Ground Labs Services Portal.

For documentation on how to assign licenses, see Assigning Licenses.

ASSIGNING LICENSES

Assigning a license to the Target can be done through the Ground Labs Services Portal. You cannot scan a Target if it does not have a license assigned.

Info: Licenses can also be automatically assigned through online authentication if:

1. There are available licenses available for the project.
2. You have a Ground Labs Services Portal username and password
3. Or you have a Scan Token.

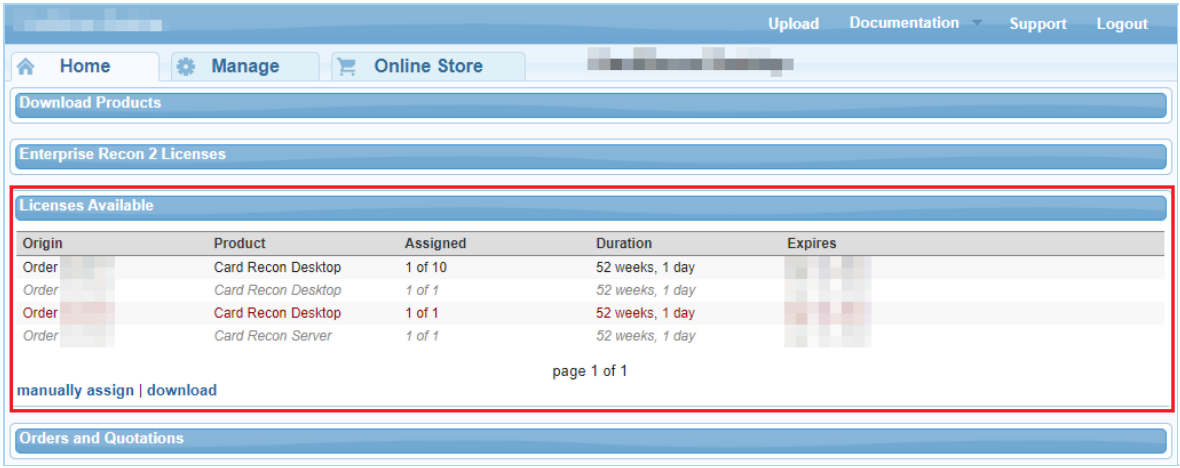
See Online Authentication for more information.

Warning: License assignment to a Target is **permanent**. You will not be able re-assign your licenses once they have been assigned to a Target. See our Ground Labs EULA for more information.

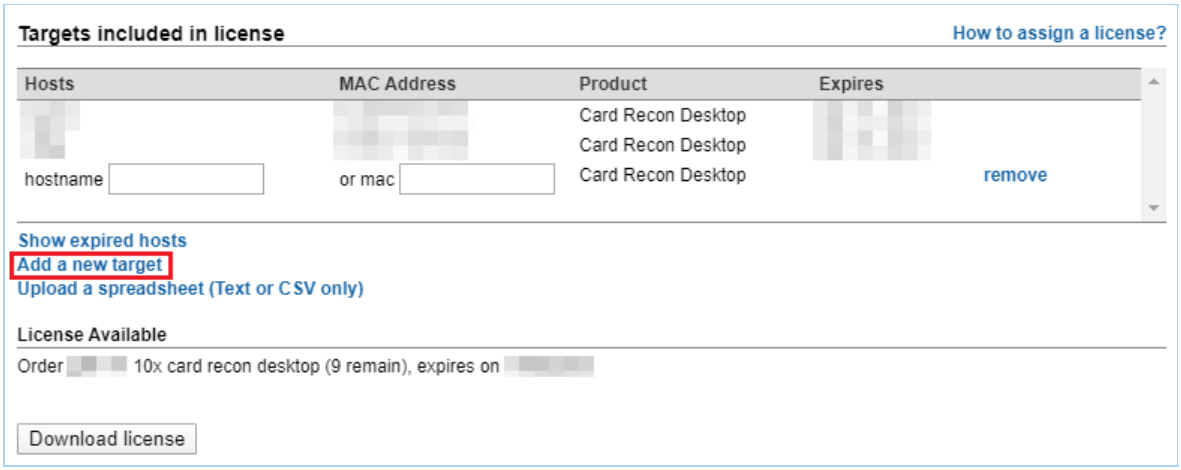
ASSIGNING A LICENSE THROUGH THE GROUND LABS SERVICES PORTAL

To assign a license to a Target:

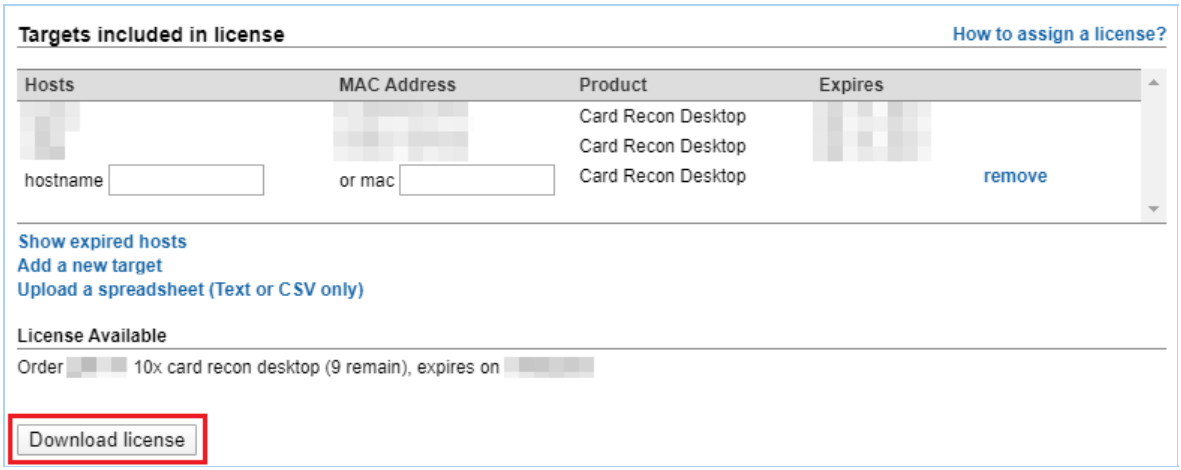
1. On to the Ground Labs Services Portal, go to the **Licenses Available** section to see a summary of the licenses that are associated with your account.



2. At **Licenses Available**, click **manually assign** to display the **Targets included in license** dialog.
3. In the **Targets included in license** dialog, click **Add a new target** to assign a license to a new Target.



4. Enter the `hostname` and/or MAC address of the Target.
5. Click **Download License** to confirm license assignment.



Info: To find the `hostname` or MAC address of your host, see Getting Host Name and MAC Address.

Warning: Make sure that the `hostname` and/or MAC address of the Target that you're assigning a license to is correct; Target assignment is permanent.

OFFLINE LICENSES

Downloading a license will put an Offline License File (`*.li2`) in your downloads folder. This license file can be used to authenticate your copy of Card Recon without an Internet connection.

For more information on using offline licenses, please see Logging into Card Recon.

ASSIGNING LICENSES THROUGH OTHER MEANS

You can also assign licenses through the Card Recon application itself.

To assign a license through the Card Recon application, you will either need a Ground Labs Services Portal account or a Scan Token. For details, see Generating and Using Scan Tokens.

Log into the Card Recon application using your Ground Labs Services Portal account or Scan Token.

When you attempt to scan an unlicensed Target, Card Recon will prompt you to assign an available license to that Target.

For more information on assigning licenses through other means, see Logging into Card Recon.

Info: When attempting to scan an unlicensed Target while logged in with a Scan Token, Card Recon will only prompt you to license the Target if your Scan Token is associated with unassigned licenses.

If all licenses associated with your Scan Token have been assigned, then Card Recon will return an “Insufficient available licenses” error and not allow you to assign additional licenses.

GETTING HOST NAME AND MAC ADDRESS

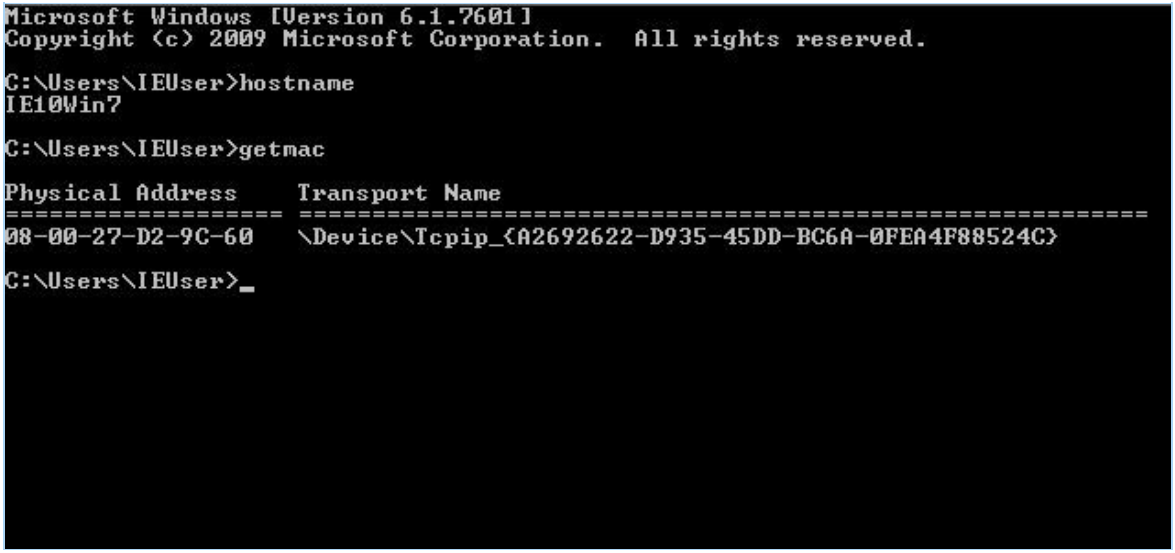
You will need either the `hostname` or the MAC address of the Target to assign it a license through the Ground Labs Services Portal.

For more information on how to assign licenses to Targets, see Assigning Licenses.

WINDOWS SYSTEMS

1. Open the command prompt by doing one of the following:
   - At the Start menu, enter `cmd` and press Enter to bring up the command Prompt
   - Go to **Start** > **All Programs** > **Accessories** > **Command Prompt**.
2. In the command prompt, enter:

```
hostname
getmac
```



   - `hostname` gets the command prompt to return your Windows machine's host name.
   - `getmac` gets the command prompt to return your machine's MAC address (also known as the machine's physical address).

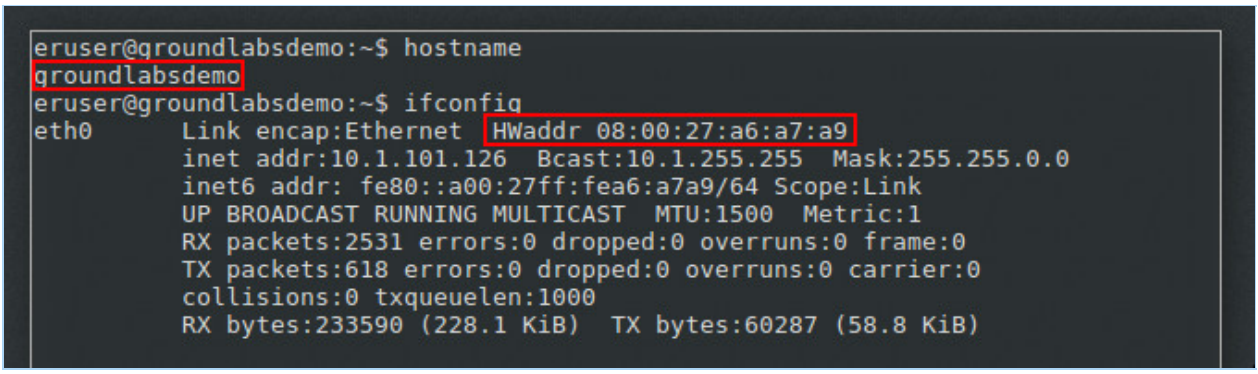
UNIX-LIKE SYSTEMS (LINUX, UNIX, FREEBSD, OSX ETC.)

Open the terminal and issue the following commands:

```
hostname
ifconfig -a
```

- `hostname` gets Terminal to return your machine's host name.
- `ifconfig -a` returns your machine's MAC address (also known as the machine's

physical address).



Info: `ifconfig -a` returns information on your system's network interfaces. The physical address or MAC address of your system's network adapter can either be found labeled as `HWaddre` or `ether`.

LOGGING INTO CARD RECON

You need to log into **Card Recon** before you can use the application. You can log into Card Recon through:

- Online Authentication
- Offline Authentication

> **Note:** Online Authentication requires a working Internet connection. This means that the host running Card Recon must have TCP port 80 open for outbound connections.
>
> If the host connects to the Internet through a proxy server, it must use a transparent proxy for Card Recon to authenticate online.

ONLINE AUTHENTICATION

Online Authentication requires a working Internet connection. This means that the host running Card Recon must have TCP port 80 open for outbound connections.

If the host connects to the Internet through a proxy server, it must use a transparent proxy for Card Recon to authenticate online.

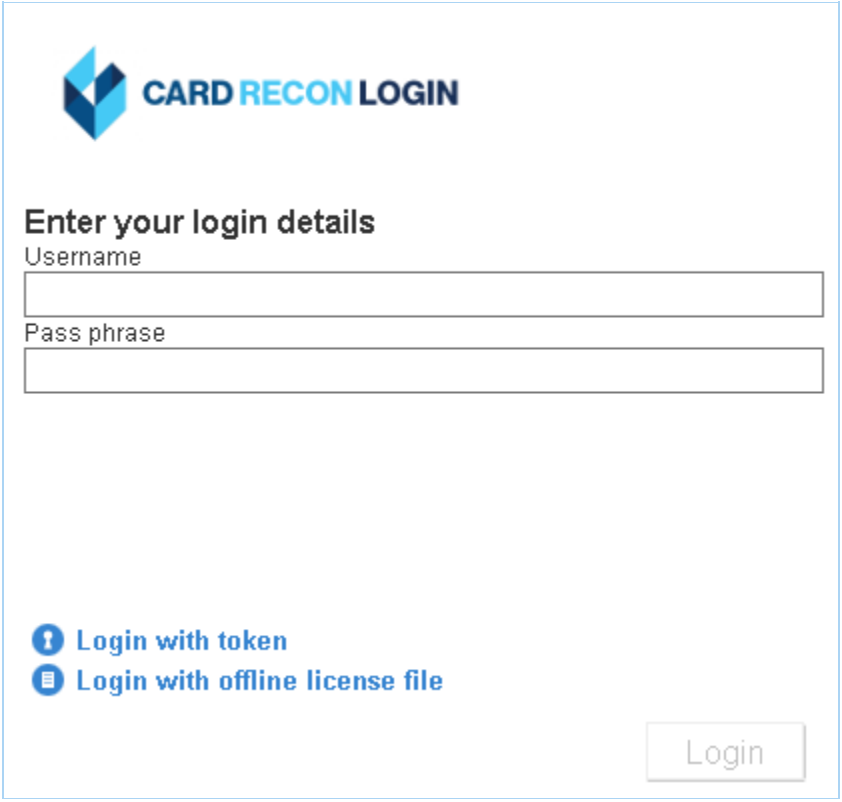
Card Recon will attempt to connect to Ground Labs authentication servers; if it cannot connect to the authentication servers, Card Recon will return a "Can’t connect to licensing system" error and will not allow you to continue using Card Recon.

You can authenticate online using:

- Your Ground Labs Services Portal login details.
- Generated Scan Tokens. See Generating and Using Scan Tokens.

Ground Labs Services Login

You can log into Card Recon using your Ground Labs Services Portal username and password.



Card Recon will connect to the Ground Labs authentication servers and verify your login details.

If you log in using your Ground Labs Services Portal account, Card Recon will use license information that is associated with that account. This means that information regarding available licenses and assigned Targets will be pulled from your Ground Labs Services Portal account.

If the Target is not already assigned a license under your account, Card Recon will prompt you to apply or purchase an appropriate license when trying to scan it.

Scan Token Login

Select "Login with token" to log into Card Recon with a Scan Token.

Using a Scan Token to log into Card Recon would mean that Card Recon would use licensing information associated with the Scan Token.

License assignment will be limited to the licenses associated with the Scan Token, and the number of activations allocated to it.

Logging in with a Scan Token will still draw information about licenses from the Scan Token's Ground Labs Services Portal parent account that have already been assigned to Targets.

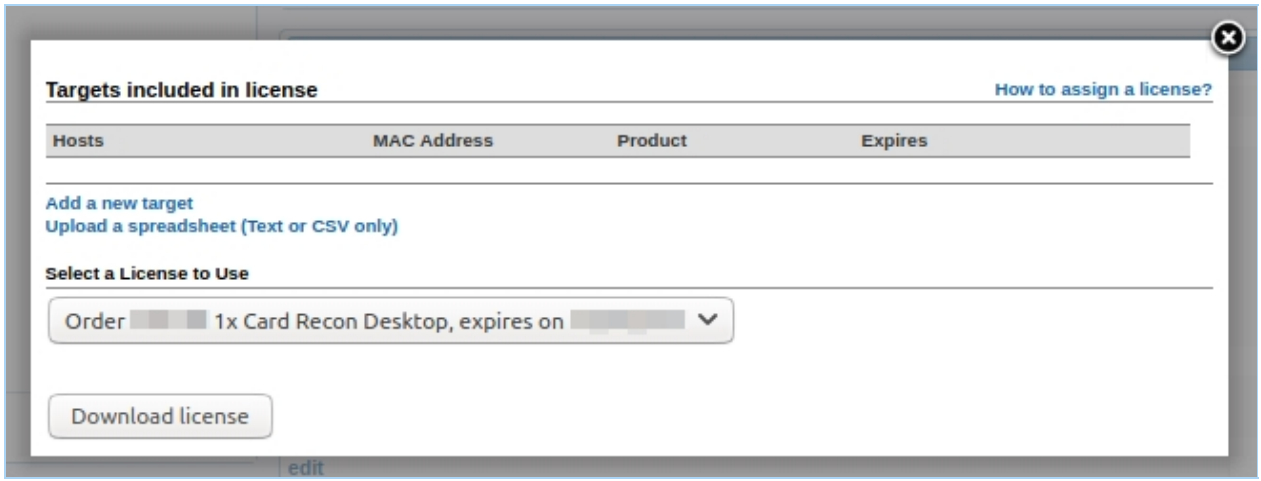
If the Target has a license already assigned to it, using a Scan Token will not use an additional license if the existing license and the Scan Token are from the same Ground Labs Services Portal parent account.

For more information on Scan Tokens, see Generating and Using Scan Tokens.

OFFLINE AUTHENTICATION

Authenticating offline is possible with Card Recon. If the Target is on a host without Internet access, or if your host has connectivity issues that prevent you from authenticating online, you can authenticate offline to perform a scan.

The Ground Labs Services Portal allows authorized users to download Offline License Files (`*.li2`).



You must assign at least one license to a Target before you can download an Offline License File.

Once you have assigned a license to a Target, you'll be able to download an Offline License File. If no Target has been assigned, the Ground Labs Services Portal will return an error.

Look for the "Licenses Available" section on the Ground Labs Services Portal dashboard. Click download to download the Offline License File.

There are 2 ways to use Offline License Files in the Card Recon CLI and GUI:

- Selecting the **Login with offline license file** option at the Card Recon login screen.
- Placing the Offline License File in the same folder as the Card Recon executable.

Selecting Login with Offline License File

Selecting **Login with offline license file** prompts you to locate an Offline License File on your disk.

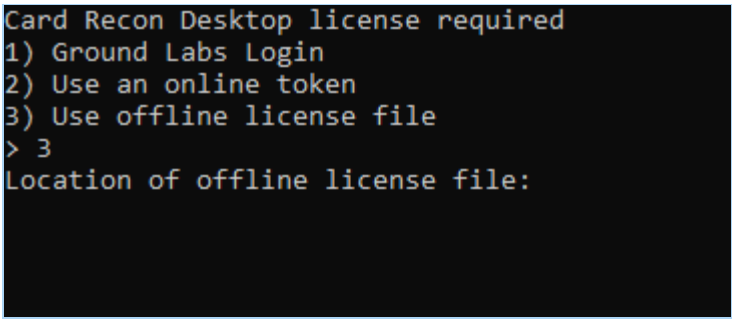
Using an Offline License File on the Windows GUI

On the Windows GUI, the **Login with offline license file** option can be found on the login screen.

Selecting that will get Card Recon to prompt you to locate your Offline License File on your disk.

Using an Offline License File on the CLI

On the Card Recon CLI, selecting the **Use offline license file** option will prompt you to locate your Offline License File on the disk.



If the license file you are using is outdated, or if it does not contain the appropriate license for the Target that you wish to scan, Card Recon will prompt you to authenticate online.

Placing the Offline License File in the Same Folder as the Card Recon Executable

The Card Recon CLI and GUI will check if there are any Offline License Files in the same directory as its executable.

If it finds an `.li2` file, it will check if the license contained in it matches the intended Target.

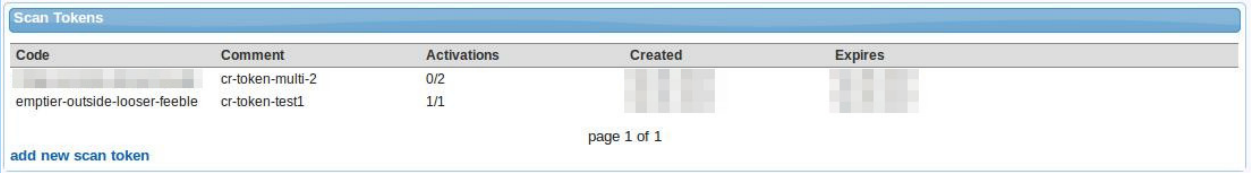
If it does not, Card Recon will prompt you to authenticate online.

GENERATING AND USING SCAN TOKENS

Scan Tokens are easy-to-remember passphrases that can be distributed to authorized users.

They can be used in place of a Ground Labs Services Portal user name and password for authenticating a user on **Card Recon**. This is useful when a user needs permission to run scans on a Target without having access to Ground Labs Services Portal user credentials.

You can manage and generate Scan Tokens at the Ground Labs Services Portal. Look for the "Scan Tokens" section on the dashboard.



Info: Scan Tokens are commonly used organizations where scan permissions and privileges need to be distributed to trusted users without giving them access to the organization's Ground Labs Services Portal account.

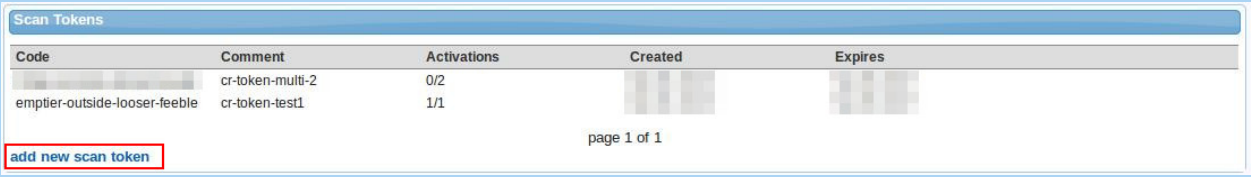
This allows users other than the owner of the Ground Labs Services Portal account to (among other things):

1. Assign licenses to Targets.
2. Scan targets.
3. Access Card Recon to create, modify, and save Card Recon configuration files for use on another host. For details, see Save and Load Options.

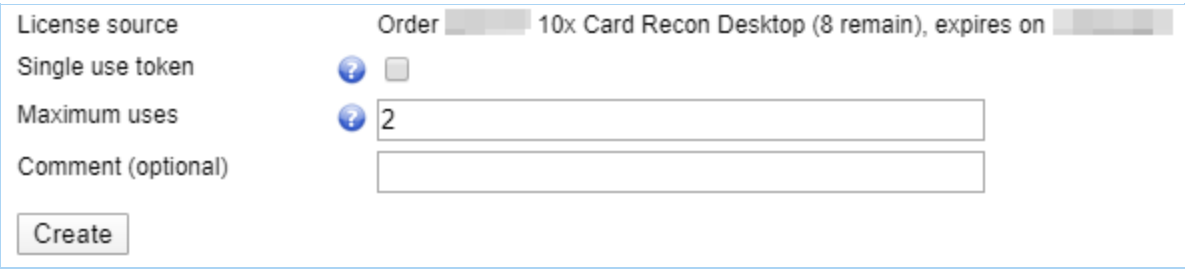
GENERATING SCAN TOKENS

Generate Scan Tokens at the Ground Labs Services Portal dashboard.

Look for the "Scan Tokens" panel, and click “add new scan token”.



Clicking on "add new scan token" will bring up its dialog window.



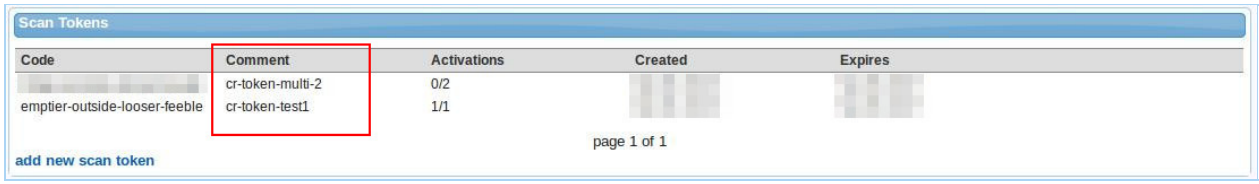
You will be asked to select your "License source" and the number of uses for your

token.

Select the appropriate license source for the Scan Token that you are generating, and click **Create**.

Identifying Scan Tokens

Comments can be added to your Scan Token to help you keep track of your Tokens in the "Comment" input box.

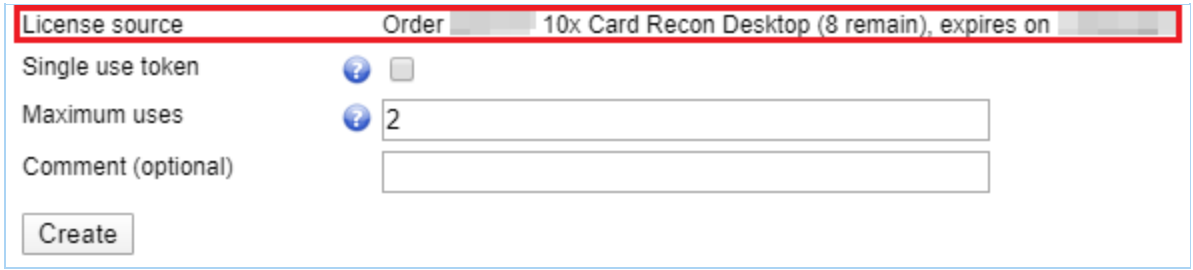


Comments can be used to help document:

- **Scan Token allocation**: If you have multiple workstation groups with different administrators, each administrator can be given a Scan Token with a license pool that they can draw from to assign to workstations in the group.
- **License allocation**: When allocated, the "Scan Tokens" section on the Ground Labs Services Portal only carries the Scan Token itself, the number of activations the Scan Token carries, its creation and expiry dates. It does not carry details on the licenses it is associated with.

Note: Make sure that you're selecting the correct license source that you want to associate the Scan Token(s) with.

USING AND ACTIVATING SCAN TOKENS

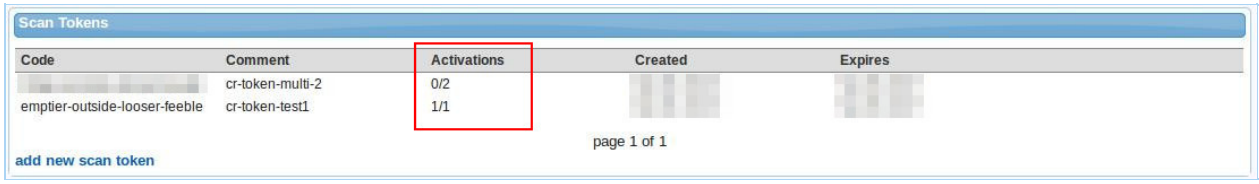


A Scan Token has a "license source" it is attached to.

A "license source" is the pool of licenses that the Scan Token can draw from when assigning licenses to new Targets.

A Scan Token can be used to log into an instance of Card Recon without assigning a license to the host.

When attempting to scan a new Target while logged into Card Recon using a Scan Token, Card Recon will draw from the "license source" that is attached to the Scan Token it is using to assign the a license to the new Target.



Scan Tokens are not "activated" when used to log into Card Recon.

They are "activated" when, after logging into Card Recon, a license that is attached to the Scan Token is assigned to a new Target.

If no licenses attached to the Scan Token are assigned to any Targets, then no activations are used.

This means a Scan Token can be used to assign licenses to new Targets as long as there are "activations" available.

If there are no more "activations" for the Scan Token, it can still be used to log into an instance of Card Recon, but cannot be used to assign licenses to new Targets, or scan Targets that do not come under the licenses that are attached to it.

Example: Scan Token A has 0/1 activations.
Scan Token A is used to log into Card Recon on host B, that contains Target B (local storage). No licenses are assigned yet, hence Scan Token A still has 0/1 activations used.

While logged in with Scan Token A, Card Recon runs a scan on Target B. A license is then assigned to Target B from Scan Token A's "license source". 1 license is assigned; Scan Token A now has 1/1 activations used.

Scan Token A can still be used to log into Card Recon.

But when that login instance is used to attempt a scan on Target Card Recon returns an "Insufficient available licenses" error.

This happens even if there are licenses available for assignment in your Ground Labs Services Portal account , but there are no more "activations" available for your Scan Token.

Note: Scan Tokens are not licenses, nor are they used in place of licenses. A license is not assigned to a Target when a Scan Token is used to log into a copy of Card Recon. A license is only assigned when a Scan Token is used to log into a copy of Card Recon, and a scan on a new Target is performed.

SINGLE OR MULTIPLE-USE SCAN TOKENS

When generating a Scan Token, you are asked if the Token should be a "Single use token" or otherwise.

- **"Single use token"**: A "Single use token" is a Scan Token that can be used to activate or assign one license to a Target.
- **Multiple-use**: If you choose to generate a multiple-use Scan Token, you can select the number of activations that the Scan Token can be used for.
  That Scan Token can be used to activate or assign licenses to Targets as long as there are activations left on the Scan Token.

You can generate as many Scan Tokens as you need as long as you have licenses available for assignment in your Ground Labs Services Portal account.

If you have assigned all your licenses to Targets, you will not be able to generate any

more Scan Tokens.

CONFIGURING SCANS FOR CARD RECON

Card Recon configuration can be done through either the

- Card Recon Command-Line Interface (CLI)
- Card Recon Graphic User Interface (GUI) (on supported Windows platforms only).

CARD RECON GRAPHIC USER INTERFACE

Card Recon is typically configured through the Card Recon Graphic User Interface (GUI) on Windows.

Once configured, scan options can be exported as `cfg` files and imported into other instances of the Card Recon GUI and CLI.

You can configure Card Recon through the following options on the Card Recon GUI dashboard:

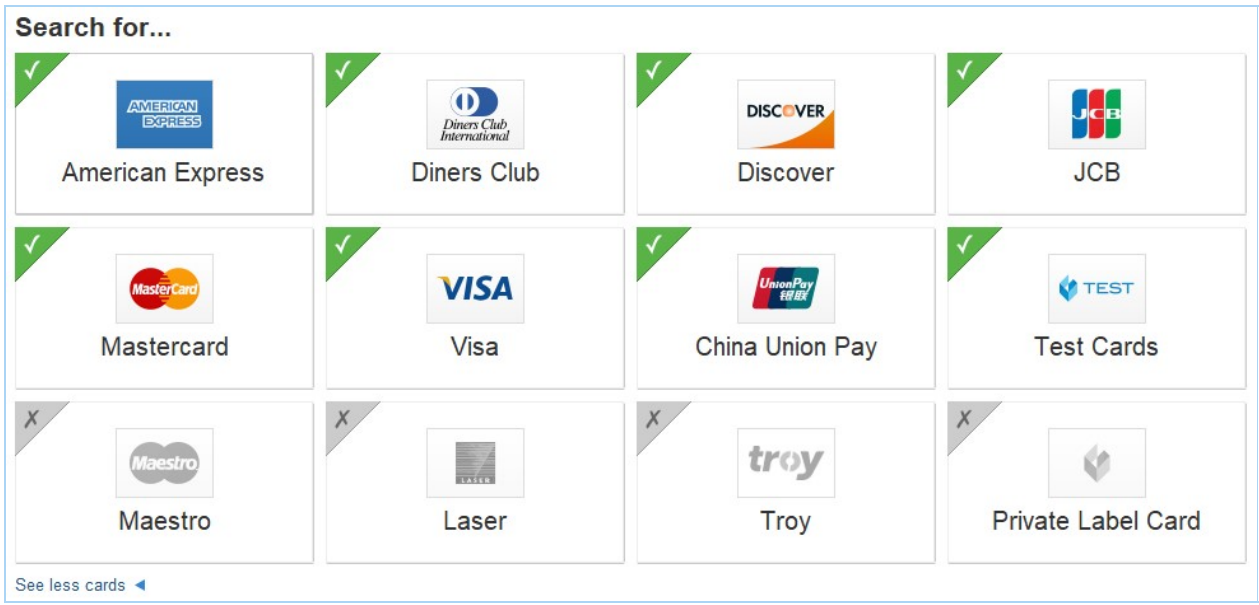
- Selecting Card Data Types
- Selecting Target Location
- Setting Resource Usage
- Setting Custom Search Rules
- Setting Results Database Options
- Setting Compliance Report Savings Options

Info: Card Recon can be configured through the CLI, but configuration features are limited. The Card Recon GUI can be run on a Windows VM to create and manage Card Recon configuration files that can be exported for use on the Card Recon CLI.

Note: You can log into Card Recon using your Ground Labs Services Portal user name and password or a Scan Token without needing to validate a license.

SELECTING CARD DATA TYPES

Card Recon can scan for 160+ combinations of PAN structures across 10 major card data types.



Info: Click on **See all cards** to see all available card data types.

8 card data types are enabled by default:

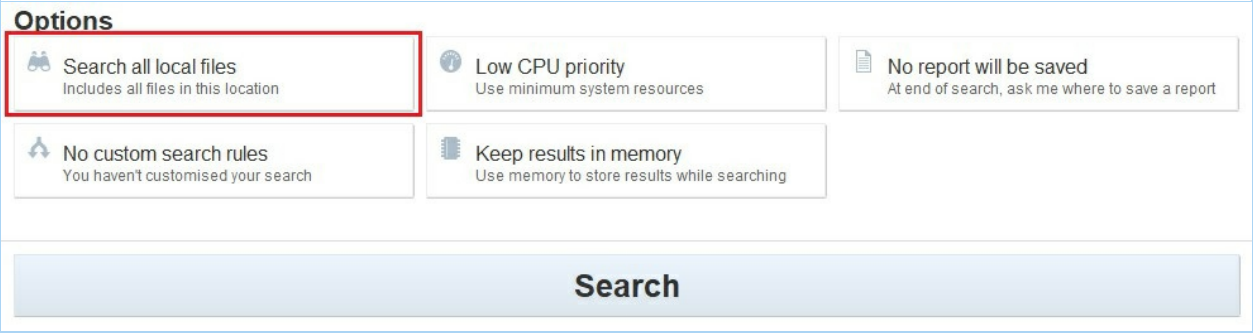
- American Express.
- Diners Club.
- Discover.
- JCB.
- MasterCard.
- Visa.
- China Union Pay.
- Test Cards.

You can select 4 additional card data types:

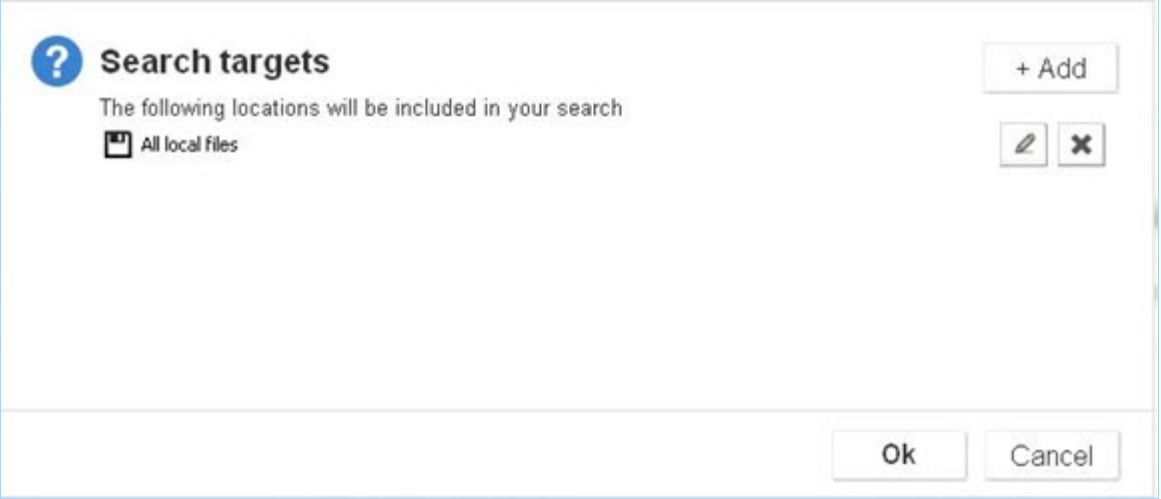
- Maestro.
- Laser.
- Troy.
- Private Label Cards.

SELECTING TARGET LOCATION

You can select search locations with the **Card Recon** GUI. To begin selecting search locations, look for the "Search all local files" button on the dashboard.



Click **Search all local files** to bring up the "Search targets" dialog.



Card Recon can scan the following Target types for sensitive data:

- Local Storage
- Local Memory

To add one or more search locations to your next scan, click **+Add** at the "Search targets" dialog

You can also add search locations by typing the details of the location (specific to the Target type; see individual sections below for details) in the "Path" field and pressing the **Enter** key.

Note: A list of Targets and how they are licensed can be found at Card Recon Licensing.

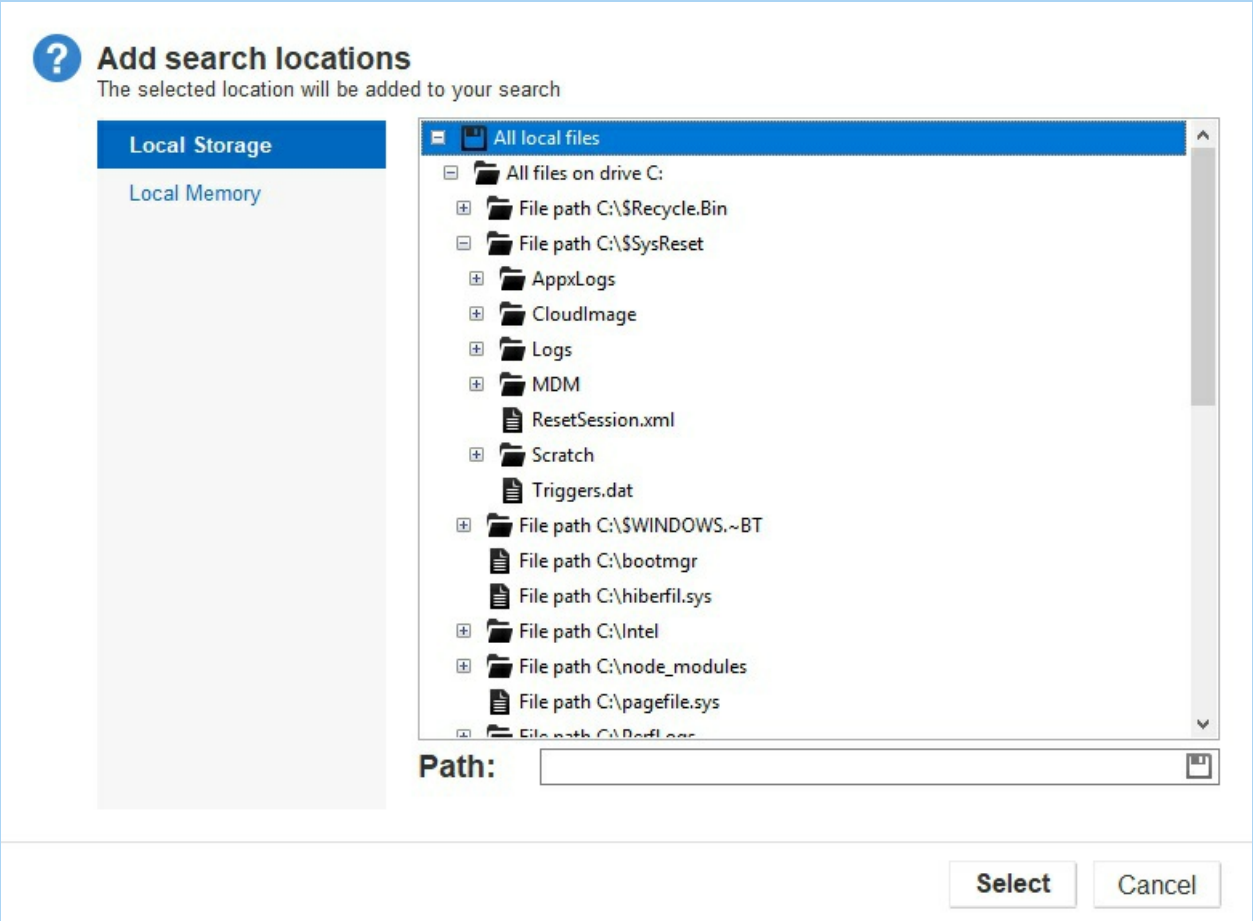
Warning: Scanning a new Target will have Card Recon prompt you to assign a new license.

LOCAL STORAGE

Card Recon can scan local storage for sensitive data.

Local storage for a host includes the contents of local physical storage drives mounted on the host.

Within the "Local Storage" tab, you can manage the locations on local storage that Card Recon will scan.



Scan specific directories by typing the full path for the location you want to scan in the "Path" field. For example:

```
# Example path for Windows systems
c:\filePathName\

# Example path for Unix-like systems
~/filePathName/
```

You can scan the following local storage types:

- All local files
- All local shadow volumes
- All local free disk space

ALL LOCAL FILES

By default, Card Recon scans all local files on local storage drives.

You can select which paths on your local storage drives that you want to include and exclude in a scan.

ALL LOCAL SHADOW VOLUMES

(Windows only) Shadow volumes are a feature of computers that use Windows NTFS as their filesystem. Shadow volumes (also known as Shadow Copies) are part of Microsoft's Volume Shadow Copy Service, and are typically used by Windows systems for Windows backup services or for creating System Restore Points.

For more information about shadow volumes, please see:
https://technet.microsoft.com/en-us/magazine/2006.01.rapidrecovery.aspx

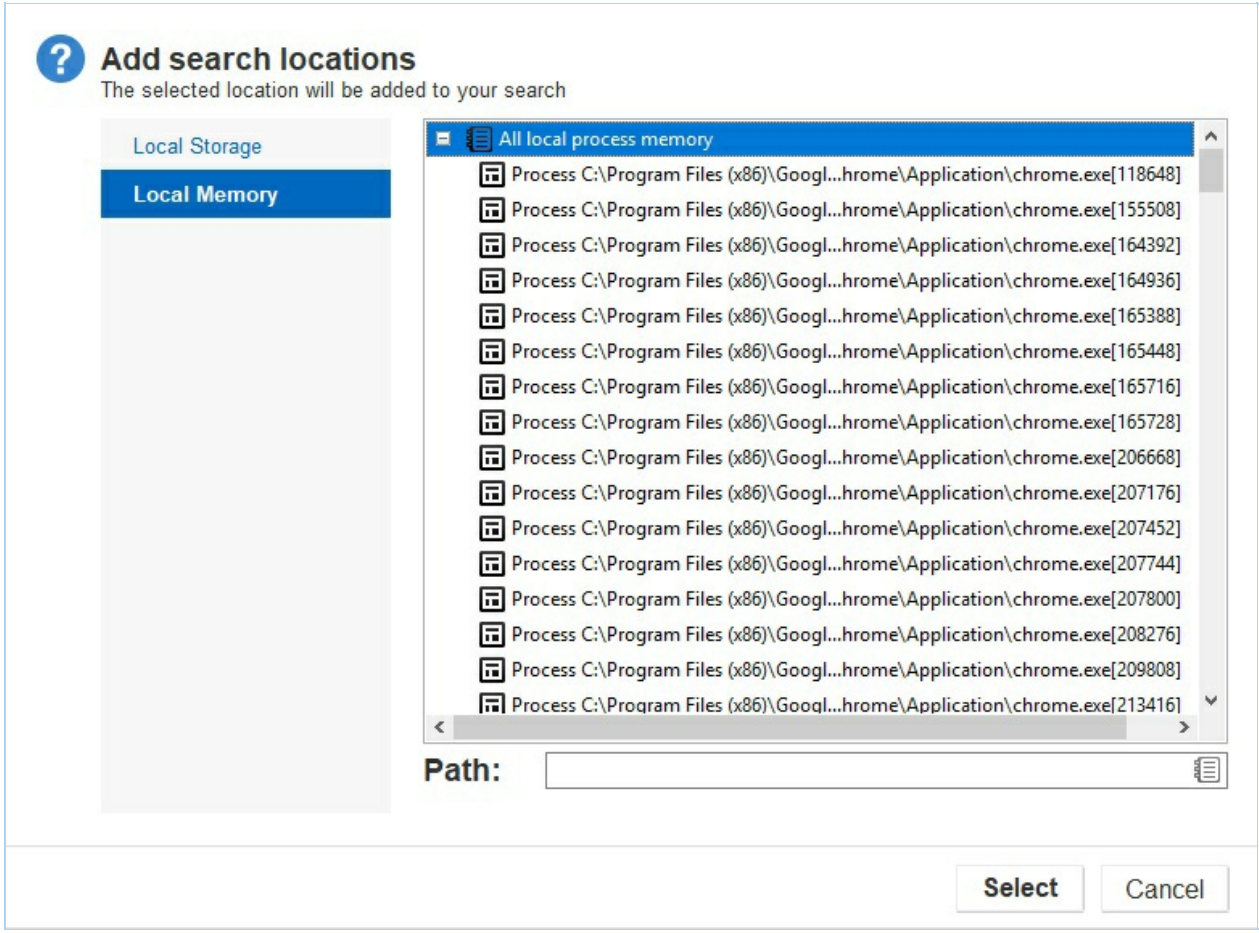
ALL LOCAL FREE DISK SPACE

(Windows only) Deleting files from a file system may not remove all traces of them; in some cases, sensitive data may remain in disk space freed-up by deleting files. Scanning local free disk space makes sure that traces of data left behind by deleted files do not contain sensitive data.

LOCAL MEMORY

Card Recon can scan for sensitive data that may be stored in the host machine's system memory (RAM).

The "Local Memory" tab allows you to select from processes that are currently running.

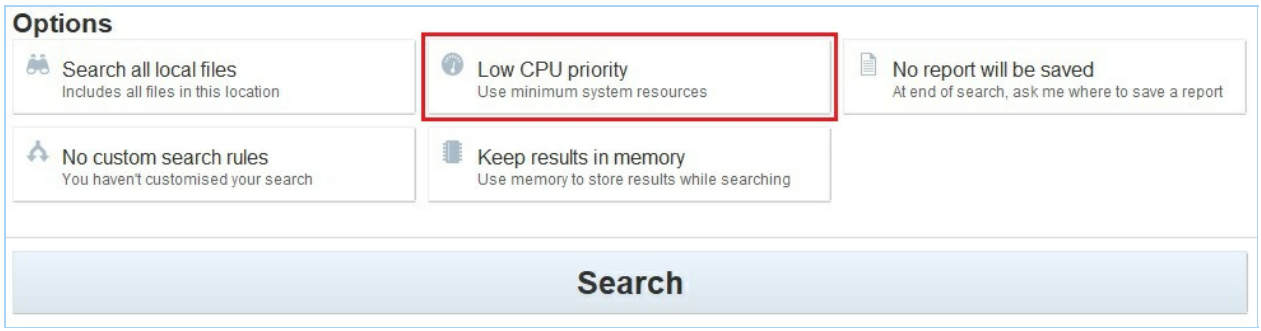


SETTING RESOURCE USAGE

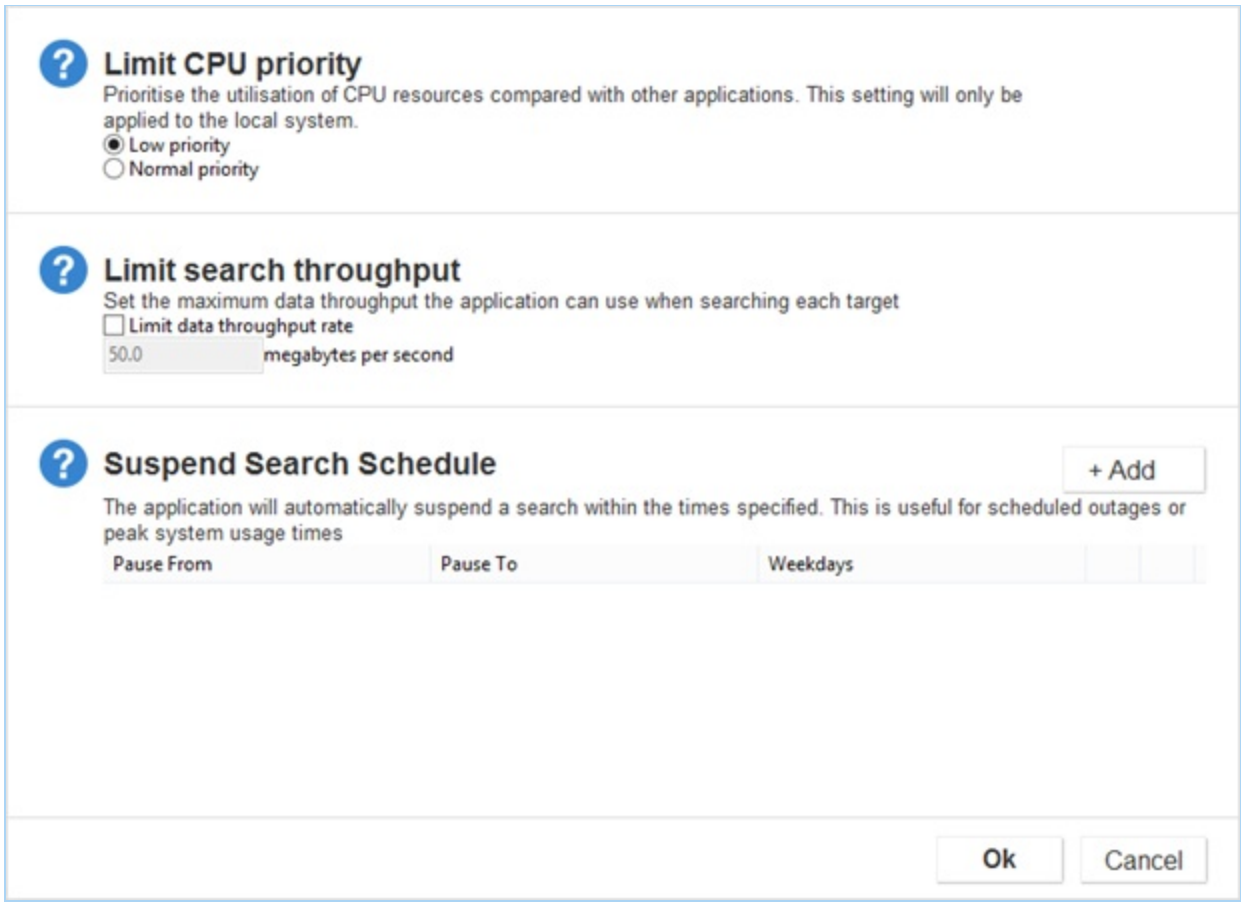
Card Recon allows you to manage how resource intensive running its scans will be.

Configuring resource usage allows you to manage Card Recon's impact on system resources, especially on production systems.

To begin setting resource usage for Card Recon, look for the button labeled "Low CPU priority" on the dashboard.



Click on "Low CPU priority" to bring up the **Resource Usage Management** dialog.



LIMIT CPU THROUGHPUT

Card Recon will scan Targets in "Low priority" mode by default.

This keeps Card Recon’s impact on host systems low so that it can be safely run on production machines.

Selecting "Normal priority" will run Card Recon at a higher CPU priority, which may cause performance issues on the host system.

Info: Running Card Recon in "Low priority" mode is recommended.

LIMIT SEARCH THROUGHPUT

You can limit the rate at which Card Recon scans data. By default, Card Recon will scan data at the highest rate that your system's hardware will allow.

Limiting the rate at which Card Recon scans data will reduce the disk I/O load for the system running Card Recon. If Card Recon is scanning files outside of local storage, limiting search throughput will also reduce both the disk I/O load for the system being scanned and the stress put on the network.

Info: The speed at which Card Recon reads data is also dependent on the hardware it is stored on, as well as how complex the data being read is.

SUSPEND SEARCH SCHEDULE

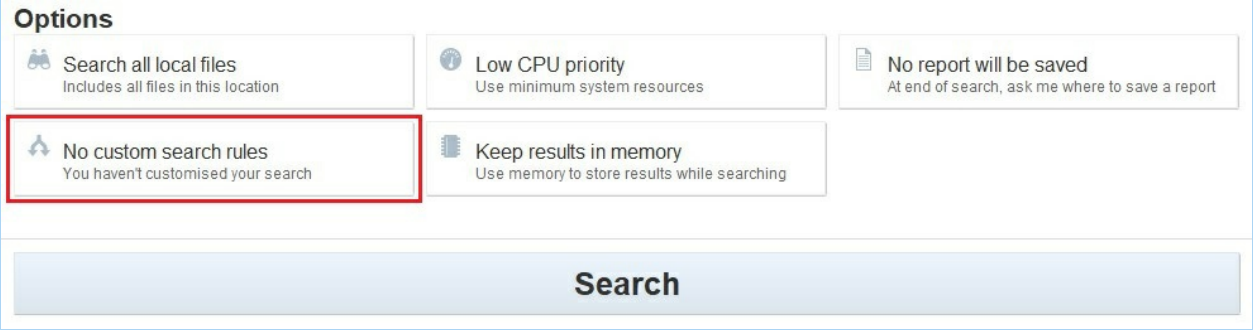
You can schedule a pause in a scan schedule.

This allows users to begin a scan and schedule it to pause during specific periods when system resources need to be freed up for production or critical use.

SETTING CUSTOM SEARCH RULES

You can set up custom search filters to tell **Card Recon** to search for specific types of data.

To begin setting up custom search filters, look for the button labeled "No custom search rules" on the Card Recon dashboard.



In the **Search Filters** dialog, click **+ Add**. It should bring up a drop-down menu of all the search filters that you can add search rules for.

LIST OF SEARCH FILTERS

Search Filter Name	Usage
[S] Enable OCR	OCR (Optical Character Recognition) scans images and detects text data. Enabling this will tell Card Recon to scan images for text data. This is a resource intensive feature.
[S] Enable Voice Recognition	Enables voice recognition when scanning WAV and MP3 files. Voice recognition is a resource-heavy feature. ⚠ **Warning:** Support for voice recognition should be considered preliminary at this time. The feature is generically tuned and is limited to the English language only. Voice recognition accuracy will be particularly low in situations where an accent may exist.
Exclude location by prefix	Excludes search locations whose paths begin with a given string. This can be used to exclude entire folder trees. For example, `c:\windows\system32` will exclude all files and folders in the `c:\windows\system32` folder, and all the files and folders whose paths start with `c:\windows\system32`.
Exclude location by suffix	Excludes search locations whose paths end with a given string. This is usually used to exclude files that end with a given string. For example, `led.jnl` will exclude all files and folders that end with the string led.jnl from the scan.

Search Filter Name	Usage
Exclude locations by expression	Excludes search locations by expression. The syntax of this expression is as follows: • `?` : A wildcard character that matches *exactly one* character `???` matches 3 characters. If placed at the end of a file or directory name, will also match zero characters. E.g.: `c:\V???` will match `c:\V123` and `c:\V1` , but will not match `c:\V1234` . • `*` : A wildcard character that *matches zero or more* characters in a search string. ◦ `*` matches all files in the directory. ◦ `*.txt` matches all `txt` files in the directory.
Include locations within modification date	Includes search locations that have been modified within a given range of dates. Card Recon will prompt you to select a start date and an end date. Files and folders that fall outside of the range set by the selected start and end date will not be scanned.
Include locations modified recently	Includes search locations that have been modified within a given number of days from the current date. Card Recon will prompt you to select the number of days within which a file is modified. E.g.: Setting the number of days to `14` will exclude files and folders that have been modified more than 14 days before the current date.
Exclude locations greater than filesize (MB)	Excludes files that are larger than a given file size (in MB).
Ignore exact match	Ignore matches that match a given string exactly. E.g.: Setting this to `4419123456781234` will ignore matches found during scans that match the given string `4419123456781234` exactly.
Ignore match by prefix	Ignore matches that begin with a given string. E.g.: Setting this to `4419` will ignore matches found during scans that begin with `4419` .

Search Filter Name	Usage
Ignore match by expression	Ignore matches found during scans if they match a given expression. The syntax of this expression is as follows: • `?` : A wildcard character that matches *exactly one* character `???` matches 3 characters. If placed at the end of an expression, will also match zero characters. E.g.: `c:\V???` will match `c:\V123` and `c:\V1`, but will not match `c:\V1234`. • `*` : A wildcard character that *matches zero or more* characters in a search string. ◦ `*` will ignore all matches ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`.
Add test data	Report match as test data if it matches a given string exactly. E.g.: Setting this to `4419123456781234` will report matches found during scans that match the given string `4419123456781234` exactly as test data.
Add test data prefix	Reports matches that begin with a given string as test data. E.g.: Setting this to `4419` will report matches found during scans that begin with `4419` as test data.
Add test data expression	Report matches found during scans as test data if they match a given expression. The syntax of this expression is as follows: • `?` : A wildcard character that matches *exactly one* character `???` matches 3 characters. If placed at the end of an expression, will also match zero characters. E.g.: `c:\V???` will match `c:\V123` and `c:\V1`, but will not match `c:\V1234`. • `*` : A wildcard character that *matches zero or more* characters in a search string. ◦ `*` will ignore all matches ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`.
[S] Enable EBCDIC mode	Enables scanning Extended Binary Coded Decimal Interchange Code (EBCDIC). EBCDIC is a character encoding scheme that is typically used by older IBM mainframe systems.
Suppress Test Data	Test data will not be displayed in scan report.

[S] : Requires Card Recon Server

SETTING RESULTS DATABASE OPTIONS

A results database is used by **Card Recon** to save and track scan progress.

Card Recon uses one results database per scan. When you start a new scan, Card Recon will begin using a new results database and lose the previous one.

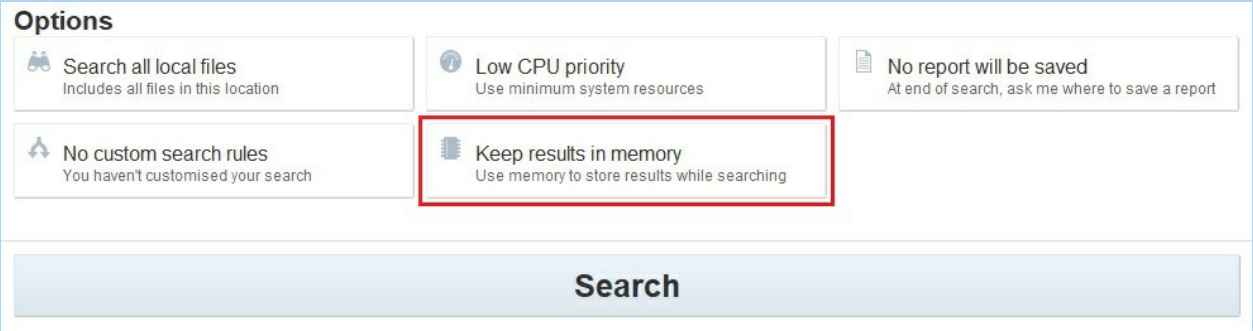
By default, this results database is stored in your system's memory. This means that when you close and re-open Card Recon, your previous results database (and scan/remediation progress) will be lost.

Info: You can also save your results database as a results database file (`*.jnl`) by picking "Save results database" in Card Recon's "Tools" drop-down menu. See Save and Load Options.

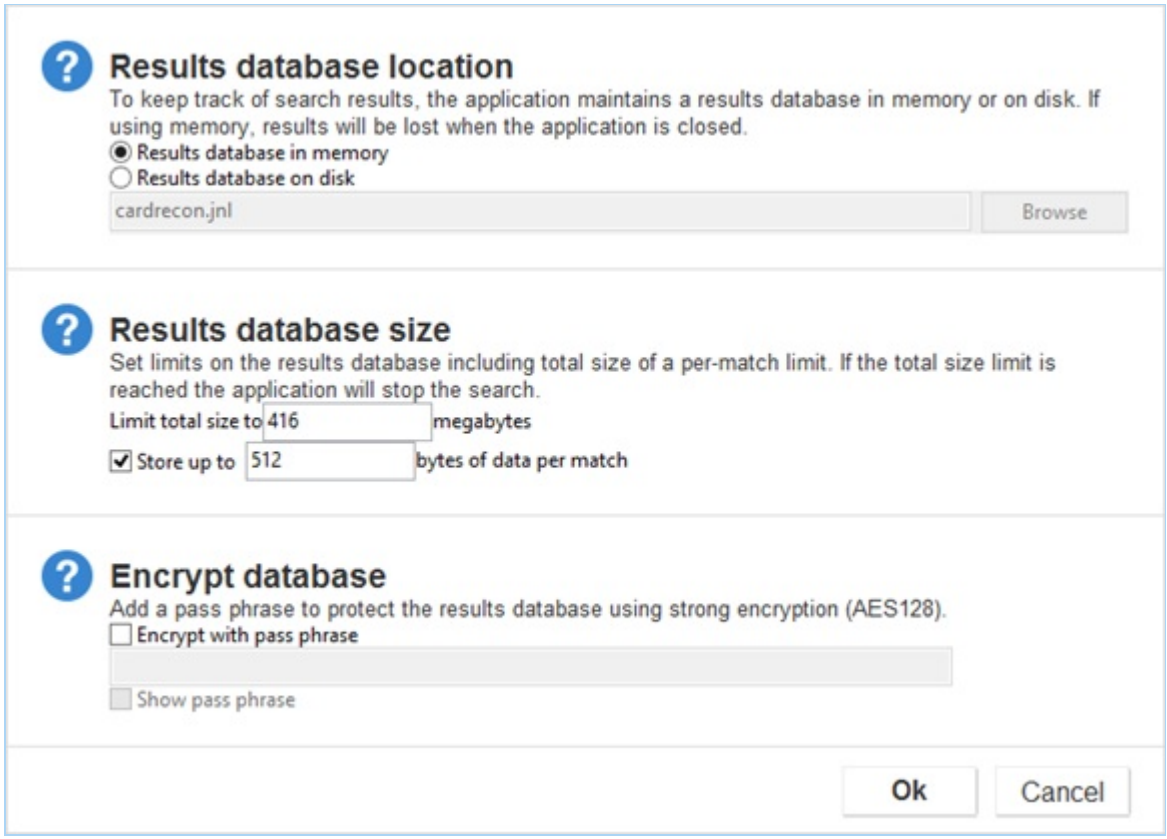
Configuring the how the results database is saved will allow you to:

- Change the default location where Card Recon stores its results database.
- Change the maximum size of the results database.
- Set a password to encrypt the database.

To begin configuring, click Keep results in memory on the Card Recon dashboard.



Clicking it should bring up the dialog for configuring how the results database is saved.



RESULTS DATABASE LOCATION

By default, the results database is kept in system memory.

To tell Card Recon to save the results database to disk:

1. Select the "Results database on disk" option.
2. Type the path and file name of the results database file that you want to save to OR click **Browse** to set the location of the results database file.

Info: Entering `cardrecon.jnl` in the "Results database on disk" field will save the results database as `cardrecon.jnl` in the same folder as the Card Recon executable.

RESULTS DATABASE SIZE

The size of the results database is limited to limit its impact on system resources.

The default max size of the results database is 416 MB.

Card Recon will store a given amount of contextual data per match. This data is the contextual match information that Card Recon displays when matches are found.

By default, the size of this match data is 512 bytes.

Warning: Card Recon will display an error when the size of the results database or the limit on contextual data per match is exceeded.

ENCRYPT DATABASE

Card Recon can encrypt a saved database journal file.

Click the "Encrypt with pass phrase" checkbox and enter a pass phrase to encrypt the database journal file.

Note: The database journal file may contain sensitive data if matches were found during the scan. Encrypting the file keeps this data in the database journal file secure.

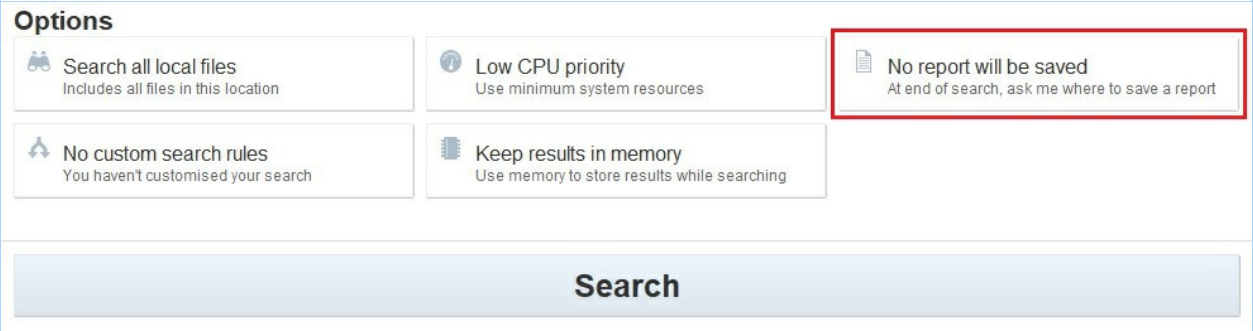
Warning: If you lose your pass phrase, Card Recon cannot load the database journal file. Please keep your passphrase in a secure location.

SETTING COMPLIANCE REPORT SAVINGS OPTIONS

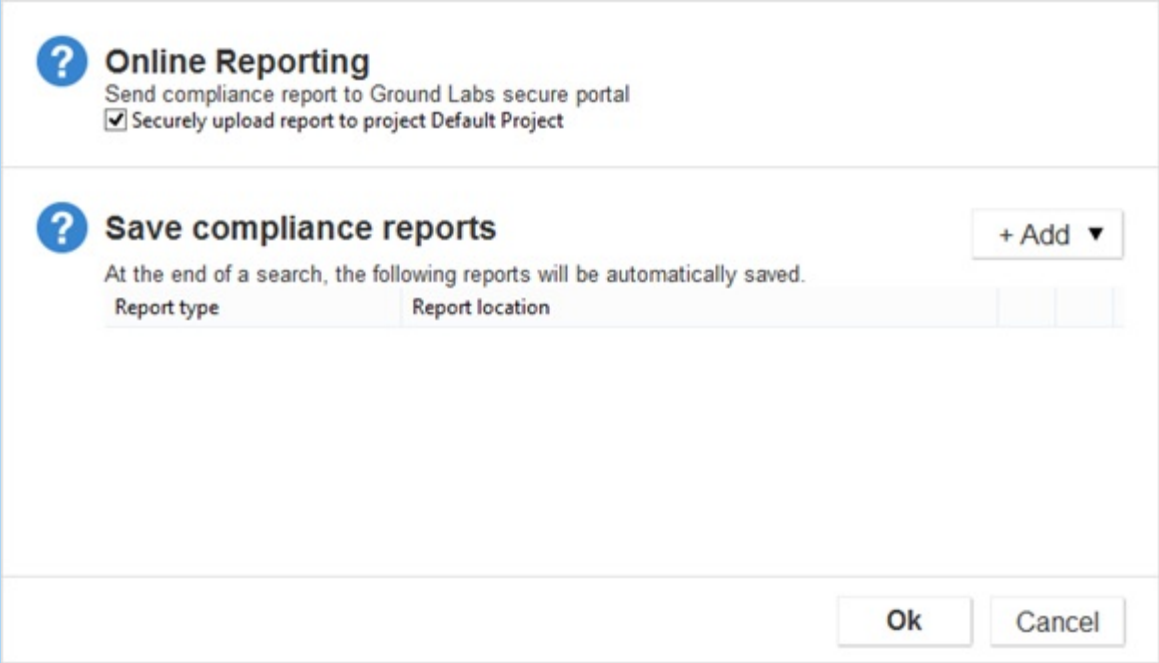
By default, compliance reports will not be saved or securely uploaded to the Ground Labs Services Portal.

See Compliance Report for more information.

To configure how **Card Recon** saves reports, click the button labeled "No report will be saved" on the dashboard.



The brings up the dialog for configuring how the compliance reports are saved.



ONLINE REPORTING

By default, Card Recon will not attempt to upload the results of each scan to the Ground Labs Services Portal once the scan is complete.

To turn this on, select the "Securely upload report" check box.

SAVE COMPLIANCE REPORTS

Card Recon will prompt you to save a compliance report after each scan.

To configure Card Recon to automatically save a compliance report without prompting you:

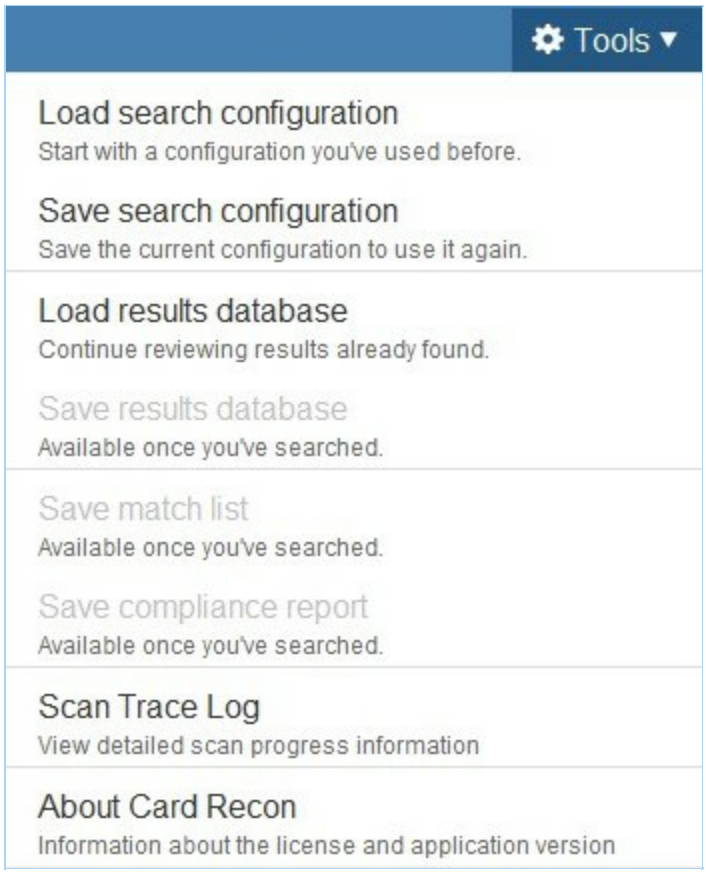
1. Click **+Add** to display a drop-down list of the report formats Card Recon can use.
2. Select your preferred report format from the drop-down list.
3. Type the file path and file name where Card Recon will save the compliance report.

You can save multiple reports in different locations.

Info: Card Recon will automatically append the appropriate file extension to the file name entered (e.g. `cardrecon.pdf` for PDF reports).

SAVE AND LOAD OPTIONS

You can import and save scan options with **Card Recon** using the "Tools" menu.



SAVING AND LOADING SEARCH CONFIGURATIONS

Card Recon's search configuration files (`*.cfg`) allow you to save and load your Card Recon's scan options.

Use the Card Recon GUI to save search configuration files. The Card Recon CLI cannot save search configuration files.

These configuration files may be loaded by both the Card Recon GUI and the Card Recon CLI.

Load Search Configuration

When you click on "Load search configuration", Card Recon prompts you to locate the configuration file that you wish to load.

Locate the appropriate configuration file on your computer and click **Open** to load the configuration file.

Info: If Card Recon cannot start, your configuration file may be corrupted. Remove the configuration file from the directory Card Recon is placed in and start Card Recon.

Save Search Configuration

Clicking on "Save search configuration" will prompt you to decide where you want to save your current Card Recon search configuration.

SAVING AND LOADING RESULTS DATABASE

Card Recon uses database journal files (`*.jnl`) to record scan and remediation progress. See Setting Results Database Options for more information.

Load Results Database

When you click on "Load results database", Card Recon prompts you to locate the results database file that you wish to load.

Loading a saved results database file will load the scan results of that particular scan, as well as any remediation done.

Loading a saved results database file will allow the user to continue remediating matches that were found in the saved results database.

Save Results Database

Clicking on "Save results database" will prompt you to decide where you want to save the current results database.

Note: Database journal files only save the results of a completed or incomplete scan. Loading a saved database journal file with the Card Recon GUI will not allow you to continue a previously paused or stopped scan.

Info: You can only save a results database after you've completed, paused, or stopped a scan.

SAVING MATCH LISTS

Once a scan has stopped running, Card Recon will allow you to save a list of all the matches found in the current session.

When saving a match list, Card Recon will automatically mask matched data.

A saved match list will contain:

- Matched data (masked).
- File path of file containing matched data.
- Type of match.
- Remedial action taken.
- Format of file containing matched data.

SAVING COMPLIANCE REPORTS

On completing a scan, Card Recon will ask if you want to save a compliance report if Card Recon is not already configured to save compliance reports.

By default, compliance reports are saved as PDFs.

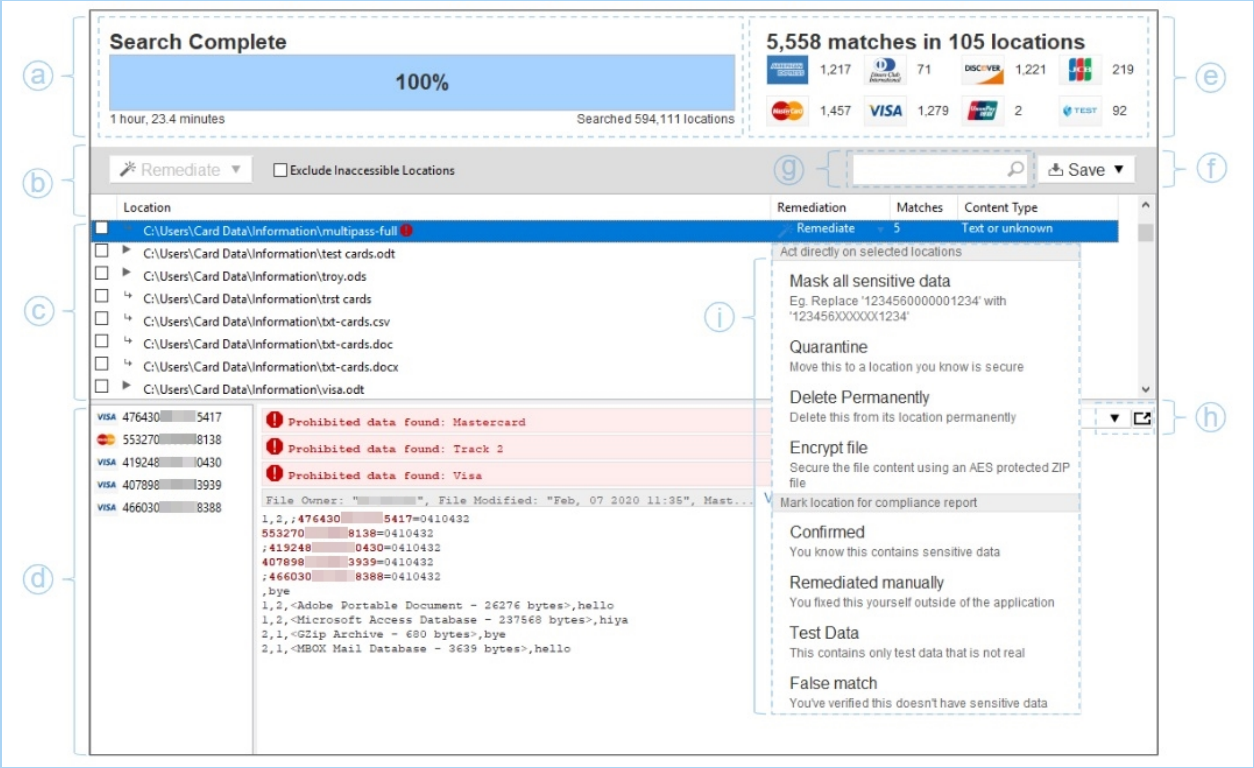
You can save compliance reports as:

- Adobe PDFs (`*.pdf`).
- Spreadsheets (`*.csv`).
- HTML (`*.html`).
- Text (`*.txt`).
- Ground Labs offline report files (`*.crr`).

RESULTS AND REMEDIATION

Beginning a scan on the **Card Recon** GUI will take you to the Card Recon Results screen.

The Results screen displays a summary of the current scan, which will help you decide how to manage non-compliant data found during the scan.



Label		Description
a	**The scan progress bar**	Shows the progress of the currently running scan, and controls to stop, pause, or skip files during the current scan.
b	**Bulk remediate/mark**	Selecting one or more matches in the match list will allow you to remediate or mark matches in bulk. See Remediating and Marking Matches.
c	**Match list**	Shows list of matched data. Selecting an item on this list will bring up its details on the Match Inspector.
d	**Match Inspector**	Shows specific match details.
e	**Match summary**	Shows a summary of match data found during the scan.
f	**Save results database/match list/compliance report**	Save options drop-down menu.
g	**Filter matches**	Type in search terms to quickly filter match results.

h	**Detach Match Inspector/Change Match Inspector view**	Clicking on the "detach" icon will detach the Match Inspector from the Card Recon window; the Match Inspector can display match details as text or as a hex file.
i	**Remediate/Mark matches**	For more information on how to remediate/mark matches, see Remediating and Marking Matches. **Note:** Remediating and marking matches are supported for Windows Server Targets through the Card Recon GUI only.

Warning: If you click **Back** to go to the dashboard, and start a new scan by clicking **Search**, you current scan progress will be lost.

Once Card Recon completes a scan, it will ask if you want to save a compliance report.

If you have already configured Card Recon to save a compliance report, Card Recon will not prompt you about report saving.

COMPLIANCE REPORT

The **Card Recon** compliance report summarizes all of Card Recon's findings from a given scan.

Label		Description
a	**Date and status of scan**	Gives the host name of the host scanned, the date the scan started, and the date the scan was completed or stopped. If the scan was canceled or stopped (you cannot generate a compliance report unless you complete or stop a scan), the report will state that the scan was "(canceled)".
b	**Compliance summary**	Summary of clean locations, match instances, and locations that contain prohibited matches.
c	**Scan parameters**	Summary of parameters applied to the scan, such as search filters and types of card data.

d	**Host and scan configuration**	Gives the host's IP address, the host's operating system, the total size of the data scanned, the version of Card Recon, and licensee details.
e	**Target summary**	Shows the number of match locations and the number of matches, organized by targets. Also shows the number of locations that cannot be accessed by Card Recon.
f	**Search Summary**	Shows a summary of all match details. • **Overview** Provides total number of non-compliant match locations and total number of non-compliant matches found during the scan. Remediating and marking matches as "Remediated Manually", "False Match", and "Test Data" will reduce the number of non-compliant matches added to this match overview. See the section below on "Match status". • **"By Status"** Shows matches organized by status. See the section below on "Match status". • **"By Card Brand"** Shows matches organized by card brand; see Selecting Card Data Types. • **"By Content Type"** Shows matches organized by file format types. Card Recon has native support for certain file formats, and will scan these files with the appropriate decoder. For formats that Card Recon does not have native support for, Card Recon will decode by brute force. Matches found in files that Card Recon has scanned but does not have native support for will be reported as "Text or unknown" in the "By Content Type" category.
g	**Match detail and status**	**MATCH DETAIL** Match details are sorted into 3 columns: • **"Test"** The scanned locations that contain match test card patterns. These matches should not affect PCI compliance. • **"Prohibited"** The number of scanned locations that contain non-compliant match data. These locations should be checked and remediated for non-compliance as soon as possible. • **"Cardholder"** The total number of match instances found during the scan. **MATCH STATUS** Matches can be labeled with 6 different statuses. How a match is labeled will determine how it is reported in the compliance report. • **"Unconfirmed Matches"**

"Unconfirmed" matches are data that match Card Recon's search patterns, and are likely to contain non-compliant data.
This data should be reviewed and marked as "confirmed", a "false match", or "test data".
Matches found during an initial scans will by default be marked as "unconfirmed", and will require review by the user.

- **"Confirmed Matches"**
  "Confirmed" matches are matches that have been reviewed by the user and are found to contain non-compliant data.
- **"Remediated using Card Recon"** *
  Matches that have been marked as "Remediated using Card Recon" are confirmed matches that have been remediated using Card Recon's built-in remediation tools.
  Remediating matches with Card Recon's built-in remediation tools will automatically mark them as "Remediated using Card Recon".
- **"Remediated Manually"** *
  Matches that have been marked as "Remediated Manually" are confirmed matches that have been marked by a user as remediated with tools outside of Card Recon.
  Marking matches as having been "Remediated Manually" will not alter existing data.
  Card Recon cannot guarantee that matches that have been marked as manually remediated have been effectively remediated to comply with PCI DSS.

- **"False Match"** *
  Matches that have been marked as a "False Match" are matches that have been reviewed and found to be false positives.

  When marking a match as a false match, Card Recon will ask if you would like to:
  - **"Send encrypted false match samples to Ground Labs for permanent resolution"**: This would securely send data that you mark as false matches to Ground Labs so that future scans can be improved.
  - **"Update configuration to exclude identical matches from future searches"**: This would update Card Recon's current search filters for the current session, and save a configuration file that contains a custom search filter to exclude the data marked as a false match from future searches. (For more information, see Save and Load Options).

  Note: Search filters for the current session will only update if you check the "Update configuration to exclude identical matches from future searches" option before clicking **Okay** to confirm that the selected match is a false match.

- **"Test Data"** *
  Matches that have been marked as "Test Data" are matches

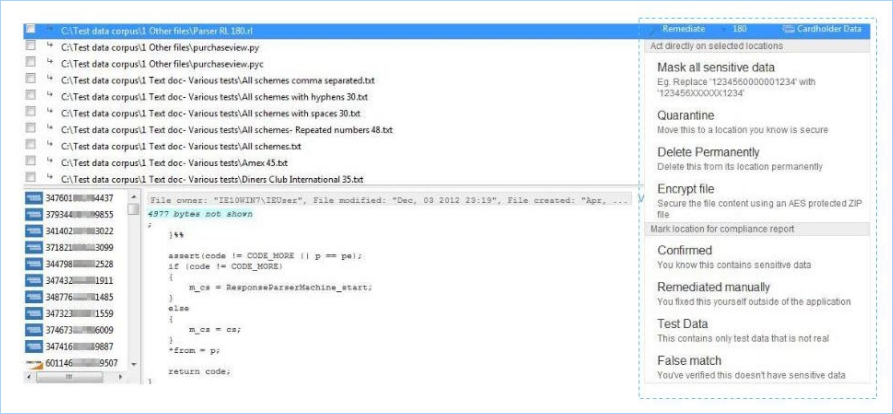
		that have been reviewed and found to match data that are from test data sets. When marking a match as test data Card Recon will ask if you would like to: ◦ **"Update configuration to exclude identical matches from future searches"**: This would update Card Recon's current search filters for the current session, and save a configuration file that contains a custom search filter to exclude the data marked as a false match from future searches. (For more information, see Save and Load Options). **Note:** Search filters for the current session will only update if you check the "Update configuration to exclude identical matches from future searches" option before clicking **Okay** to confirm that the selected match is a false match.

Note: * Matches that are marked as "Remediated using Card Recon", "Remediated Manually", "False Match", or "Test Data" will be excluded from the "Total Match Locations" and "Total Matches" in the "Search summary" section (f).

REMEDIATING AND MARKING MATCHES

Note: Remediating and marking matches are supported for Windows Server Targets through the Card Recon GUI only.

Match data found during a scan should be reviewed to verify if the match has uncovered genuinely non-compliant data. Selecting a match in the match list will allow you to select remediative action for it .



Card Recon allows you to take the following remedial actions on a match:

- **"Act directly on selected locations"**: Actions that will alter files such that the resulting data is PCI compliant
  - **"Mask all sensitive data"**: Writes over match data in match locations with masking characters so that the data is no longer non-compliant.
  - **"Quarantine"**: Moves the non-compliant file to another location; this should be used to move non-compliant files to a secure location.
  - **"Delete Permanently"**: Delete the non-compliant file from its location securely.
  - **"Encrypt file"**: Packs the non-compliant file into an encrypted ZIP file.
- **"Mark location for compliance report"**: Mark locations after reviewing them.
  - **"Confirmed"**: Confirm that the match contains sensitive data, and mark it for further action.
  - **"Remediated Manually"**: Confirm that the match contains sensitive data, and that it has been remediated with tools outside of Card Recon.
  - **"Test Data"**: Mark the match as test data; match does not contain sensitive data.
  - **"False match"**: Mark the match as a false positive; match does not contain sensitive data.

Saving a new compliance report will show changes made by remediating and marking the matches with Card Recon.

CARD RECON COMMAND-LINE INTERFACE

The **Card Recon 3.0.4** Command-Line Interface (CLI) allows you to run Card Recon on supported systems. For details, see System Requirements.

While it is possible to configure and run scans for Card Recon using the CLI, the Card Recon Graphical User Interface (GUI) offers more configuration options. See Card Recon Graphic User Interface.

Info: If you have no access to a Windows machine to run an instance of the Card Recon GUI, read about Setting Up a Windows Virtual Machine to run the Card Recon GUI.

GETTING STARTED WITH THE CLI

Download the appropriate version of the **Card Recon** CLI from the Ground Labs Services Portal.

> **Info:** Card Recon should be run with administrator privileges. Use `runas` in the Command Prompt and `sudo` in Terminal.

For more details, see Running the Card Recon CLI.

LOCATE CARD RECON CLI

In the command prompt:

```
# Where c:\Users\<username>\Downloads\ is the directory where the Card Recon CLI executable is located
cd %userprofile%\Downloads\
```

In Terminal:

```
cd ~/Downloads
# Where /<username>/Downloads is the directory where the Card Recon CLI executable is located.
```

RUNNING CARD RECON CLI

In the command prompt:

```
# To run the Card Recon CLI
cr_x.x.x.exe
```

In Terminal:

```
# Where <cr_linux26_x.x.x> is the file name of the Card Recon executable
chmod +x cr_linux26_x.x.x
./cr_linux26_x.x.x
```

> **Note: Full disk access required for macOS Targets**
> Scanning macOS Target locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for the Terminal prior to the first scan of the macOS Target. Locations not granted full access will be logged as inaccessible locations. See Enabling Full Disk Access in macOS Systems for more information.

CARD RECON CLI OPTIONS

Command Line Flags	Function
`-c,-config,-configuration <path>`	Runs **Card Recon** using a specified configuration file. **Info:** This configuration file can be generated by the Card Recon GUI. For details, see Configuring Scans for Card Recon.
`-export <path>`	Sets the location where a list of matches will be saved. Export formats: • PDF • TXT • CSV • XML
`-h,-help`	Displays all the command-line options available.
`-j,-journal <file>`	Specify the location to save the database journal file. If specified database journal file exists, Card Recon will load the file. See Save and Load Options.
`-journal-overwrite`	Overwrite the database journal file specified with the `-journal` option if the database journal file already exists.
`-journal-resume`	Use the data specified with the `-journal` option to recover and resume an interrupted search. Upon resuming, Card Recon retries the location which was being searched at the time of interruption.
`-journal-skip`	Use the results database specified with the `-journal` option to recover and resume an interrupted search. Upon resuming, Card Recon will skip the file which was being searched when the search was interrupted.
`-l, -license <path>`	Sets the location of the Offline License File. See Offline Licenses.
`-o,-output <path>`	Sets the location where the compliance report will be saved. Output formats: • PDF • TXT • CSV • CRR* **Info:** Multiple entries may be used to save several copies of the compliance report in different formats.

Command Line Flags	Function
`-p, -password`	Encrypt the saved database journal file; Card Recon will prompt you to select a password.
`-password-inline <password>`	Encrypt the saved database journal file; user sets the password in-line, e.g.: `./cr_linux26_x.x.x -j journalfile.jnl -password-inline PASSWORD`
`-q,-quiet`	Runs in 'quiet' mode.
`-r <path>`	Sets the root directory for the search.
`-v, -verbose`	Runs in 'verbose' mode.
`-version`	Displays software version.
`-vv, -very-verbose`	Turn on 'extra verbose' mode. **Tip:** You can save the output from 'verbose' or 'extra verbose' mode for debugging. To do so, you first have to be using an Offline License File. See Offline Licenses. Then, issue the following command: `./cr_linux26_x.x.x -vv >> output.txt`

SETTING UP A WINDOWS VIRTUAL MACHINE

Setting up a Windows virtual machine (VM) will allow you to run the **Card Recon** GUI to create and save configuration files for use on the Card Recon CLI.

To begin setting up a Windows VM, you will need to run virtualization software.

Go to VirtualBox's downloads section to download a copy of VirtualBox: https://www.virtualbox.org/wiki/Downloads

Install VirtualBox by running the installer and following the on-screen instructions.

For more information on installing VirtualBox, please consult the VirtualBox end-user documentation.

SYSTEM REQUIREMENTS

To run VirtualBox, your host machine will need:

- A recent Intel or AMD processor.
- At least 1GB RAM.
- 8GB free disk space.
- A host operating system that is supported by VirtualBox.
- A supported guest operating system (in this case, Windows).

Info: For more information on VirtualBox's system requirements, please see: https://www.virtualbox.org/wiki/End-user_documentation.

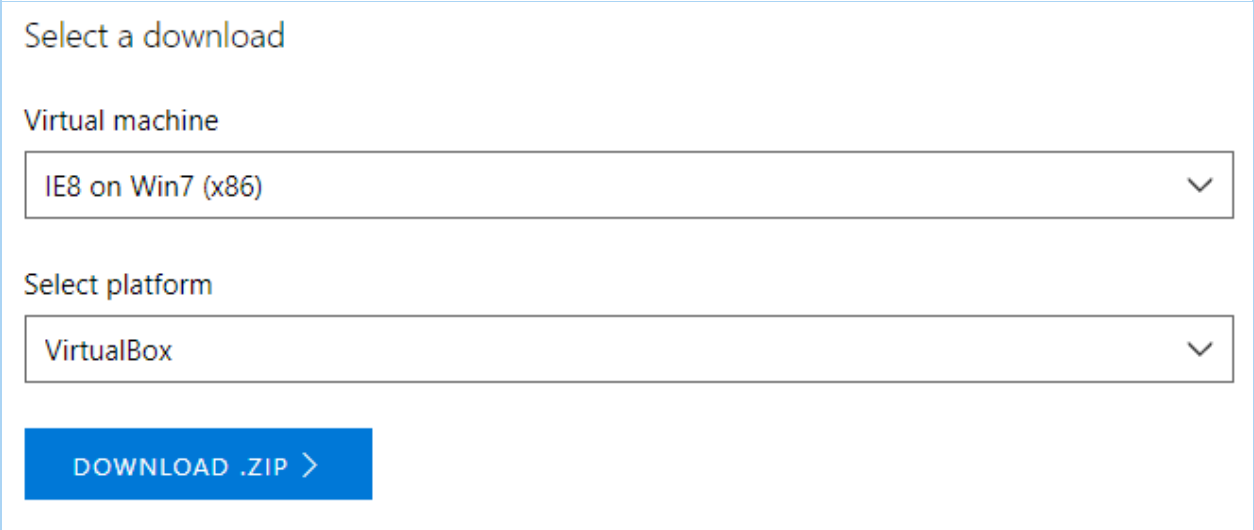
DOWNLOAD WINDOWS VM

Microsoft makes its platforms available as VMs for testing purposes here: https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

On Microsoft's "Download virtual machines page" :

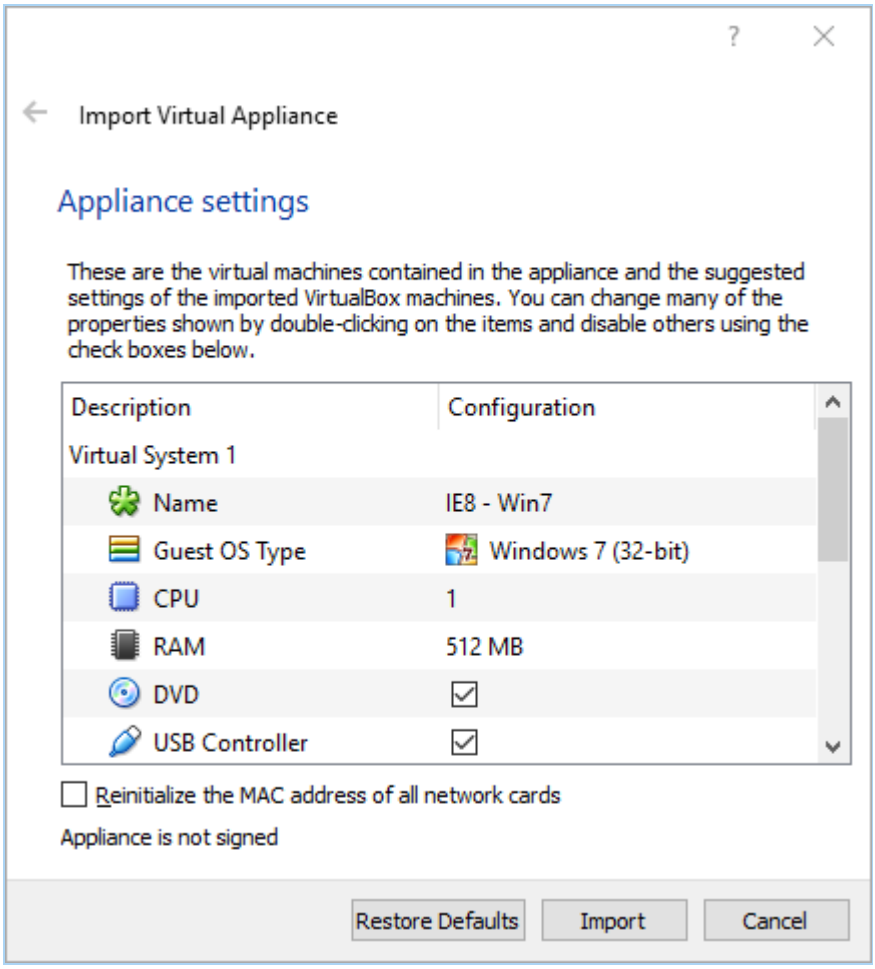
1. Select an appropriate version of Windows to run the Card Recon GUI on.
2. Select the appropriate platform (the virtualization software that the VM will run on, i.e. VirtualBox).

Click on the **Download .zip** button that appears on the right.



INSTALLING THE VIRTUAL MACHINE

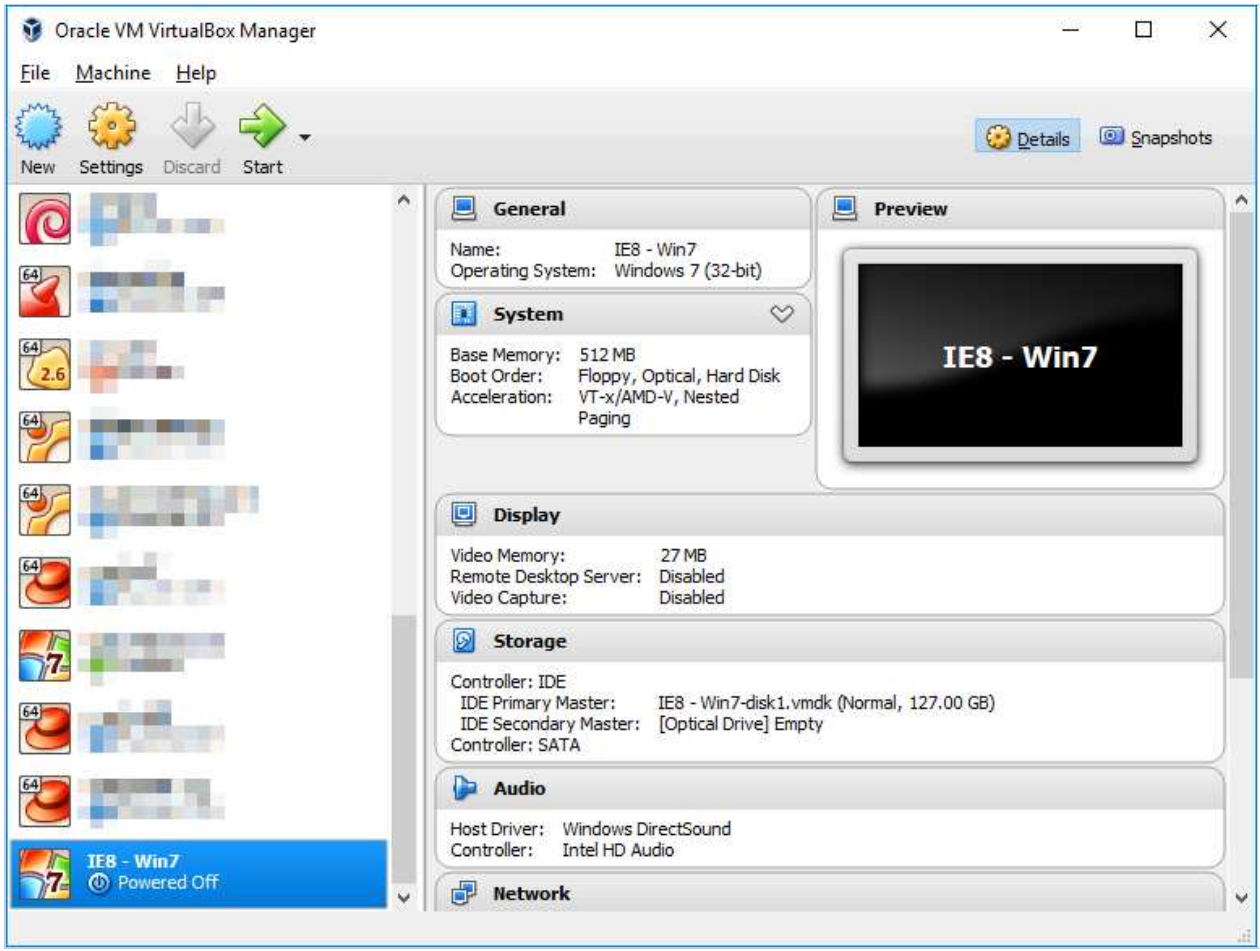
1. Make sure that VirtualBox is installed.
2. Locate the downloaded Windows VM `*.zip` file. Extract the virtual appliance file.
3. Double-click the extracted virtual appliance file (`*.ova`).
   VirtualBox opens and displays the "Import Virtual Appliance" dialog.



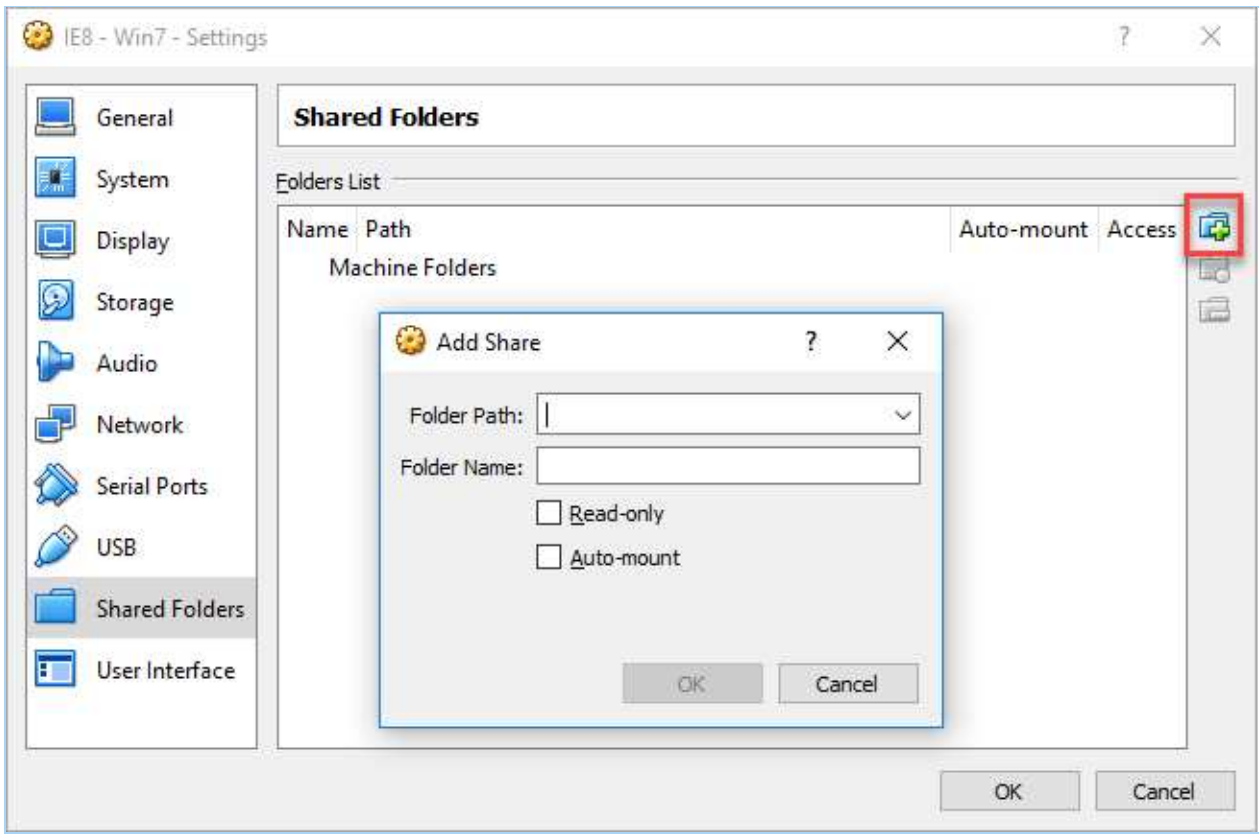
4. Click **Import** to start building the Windows VM.

When VirtualBox is done building the Windows VM, the "Import Virtual Appliance" dialog will automatically close.

The Windows VM will display in the Oracle VM VirtualBox Manager.



To share folders between your host machine and the Windows VM, right-click the Windows VM in the Oracle VM VirtualBox Manager and select **Settings**.



Select Shared Folders in the left panel. Click on the **Add shared folder** button on the right of the window

Enter the path of a folder on your host machine to share with the Windows VM.

Click **Start** to start the Windows VM.

Download and run the Card Recon GUI on the Windows VM to begin creating and managing your configuration files.

THIRD-PARTY SOFTWARE DISCLAIMER

Any links to third-party software available on this website are provided "as is" without warranty of any kind, either expressed or implied and such software is to be used at your own risk.

The use of the third-party software links on this website is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your computer system or loss of data that results from such activities. Ground Labs will not be liable for any damages that you may suffer with downloading, installing, using, modifying or distributing such software. No advice or information, whether oral or written, obtained by you from us or from this website shall create any warranty for the software.

Ground Labs does not provide support for these third-party products. If you have a question regarding the use of any of these items, which is not addressed by the documentation, you should contact the respective third-party item owner.