

# CARD RECON

## User Guide

# CARD RECON

## Table of Contents

---

<b>CARD RECON 2.0.25 Release Notes</b>	1
New Data Types	1
New features	1
Bug fixes	1
Improvements	2
<b>About CARD RECON</b>	1
Overview	1
Who is Card Recon suitable for?	1
Additional Resources	1
Features	2
Disclaimer	2
<b>System Requirements</b>	4
Certified Operating Systems	4
<b>Getting Started</b>	6
System Requirements	6
Download CARD RECON	6
Run Your First Scan	6
<b>Set Up CARD RECON</b>	7
Windows GUI	7
Linux shell	7
Running CARD RECON as a Portable Application	7
<b>Running the CARD RECON GUI</b>	9
<b>Running the CARD RECON CLI</b>	12
Running the CARD RECON CLI on Windows	12
Method 1	12
Method 2	13
Running the CARD RECON CLI on Linux and UNIX-like systems	14
<b>Results and Remediation</b>	17
<b>Compliance Report</b>	19
Match detail	21
Match status	21
<b>Remediating and Marking Matches</b>	22
<b>CARD RECON Licensing</b>	24
Subscription License	24
Targets	24
CARD RECON Standard Edition and Advanced Edition	25
Feature Comparison	25
<b>How Licensing Works</b>	28
<b>Assigning Licenses</b>	29
Assigning a license through the Ground Labs Services Portal	29
Offline Licenses	30
Assigning licenses through other means	31

<b>Getting Host name and MAC Address</b>	32
Windows systems	32
UNIX-like systems (Linux, UNIX, FreeBSD, OSX etc.)	33
<b>Logging into CARD RECON</b>	34
Online authentication	34
Ground Labs Services login	34
SCAN TOKEN login	35
Offline authentication	36
Selecting Login with offline license file	36
Using an OFFLINE LICENSE FILE on the Windows GUI	37
Using an OFFLINE LICENSE FILE on the CLI	37
Placing the OFFLINE LICENSE FILE in the same folder as the CARD RECON executable	37
<b>Generating and Using Scan Tokens</b>	38
Generating SCAN TOKENS	38
Using and Activating SCAN TOKENS	40
Single or multiple-use SCAN TOKENS	41
<b>Configuring Scans for CARD RECON</b>	43
<b>CARD RECON Graphic User Interface</b>	44
<b>Selecting Card Data Types</b>	45
<b>Selecting Target Location</b>	47
<b>Local Storage</b>	49
All local files	50
All local shadow volumes	50
All local free disk space	50
<b>Local Memory</b>	51
<b>Network Storage</b>	52
Windows Share	53
UNIX File Share	53
Remote Access via SSH	53
<b>Databases</b>	55
File-based Scan	55
Live Database Scan	55
Supported Databases and Requirements	55
Remediating Matches	56
Add Credentials	56
Add Databases to Search Locations	57
Database Connection Options	58
<b>Email</b>	59
Google Mail (IMAP)	59
Requirements	59
Add Credentials	59
Add Search Location	60
2-Factor Authentication	60

---

Office 365 Mail (IMAP) .....	61
Requirements .....	61
Add Credentials .....	61
Add Search Location .....	62
Internet Mailbox .....	62
Requirements .....	63
Add Credentials .....	63
Add Search Location .....	64
Internet SSL Mailbox .....	64
Requirements .....	64
Add Credentials .....	64
Add Search Location .....	65
Lotus Notes .....	66
Requirements .....	66
Add Credentials .....	67
Add Search Location .....	67
Lotus Notes User Name .....	68
Locally Stored Email Data .....	68
Scanning Information Stores .....	68
<b>Websites</b> .....	<b>70</b>
Website search options .....	70
Maximum search depth .....	70
Follow external Website links .....	70
<b>Cloud Storage</b> .....	<b>71</b>
<b>Amazon S3</b> .....	<b>72</b>
Get AWS User Security Credentials .....	72
Add Credentials .....	73
Add Target .....	74
<b>Rackspace Cloud</b> .....	<b>76</b>
Get Rackspace API key .....	76
Add Credentials .....	76
Add Target .....	77
<b>Box</b> .....	<b>79</b>
Add Target .....	79
Obtain Access Code .....	80
Finish Adding Target .....	80
<b>Dropbox</b> .....	<b>81</b>
Add Target .....	81
Obtain Access Code .....	82
Finish Adding Target .....	82
<b>Google Apps</b> .....	<b>83</b>
Configure Google Apps Account .....	83
Select a project .....	83
Enable APIs .....	84

Create a Service Account .....	85
Set up Domain-Wide Delegation .....	86
Add Credentials .....	89
Add Target .....	90
<b>OneDrive</b> .....	<b>91</b>
Add Target .....	91
Obtain Access Code .....	92
Finish Adding Target .....	92
<b>Azure Storage</b> .....	<b>93</b>
Get Azure Account Access keys .....	93
Add Credentials .....	93
Add Target .....	94
<b>Setting Resource Usage</b> .....	<b>96</b>
Limit CPU Priority .....	97
Limit Search Throughput .....	97
Suspend Search Schedule .....	97
<b>Setting Credentials for Restricted Targets</b> .....	<b>98</b>
Search Target Credentials .....	98
Encrypt Credentials .....	98
<b>Setting Custom Search Rules</b> .....	<b>100</b>
List of Search Filters .....	100
<b>Setting Results Database Options</b> .....	<b>104</b>
Results Database Location .....	105
Results Database Size .....	105
Encrypt Database .....	106
<b>Setting Compliance Report Savings Options</b> .....	<b>107</b>
Online Reporting .....	108
Save Compliance Reports .....	108
<b>Save and Load Options</b> .....	<b>109</b>
Saving and Loading Search Configurations .....	109
Load search configuration .....	109
Save search configuration .....	110
Saving and Loading Results Databases .....	110
Load results database .....	110
Save results database .....	110
Saving Match Lists .....	110
Saving Compliance Reports .....	111
<b>CARD RECON Command-Line Interface</b> .....	<b>112</b>
<b>Getting Started with the CLI</b> .....	<b>113</b>
Locate CARD RECON CLI .....	113
Running CARD RECON CLI .....	113
<b>CARD RECON CLI Options</b> .....	<b>114</b>
<b>Setting Up a Windows Virtual Machine</b> .....	<b>116</b>
System Requirements .....	116

Download Windows VM .....	116
Installing the Virtual Machine .....	117

---

# CARD RECON 2.0.25 RELEASE NOTES

## NEW DATA TYPES

- New data type: TROY credit card numbers.

## NEW FEATURES

- Added: Ability to scan ALZ archives.
- Added: Ability to scan EGG archives.
- Added: Ability to scan Hangul Word Processor (HWP) files.
- Added: Ability to scan and mask XLS files.
- Added: Amazon S3 Bucket scans now support AWS regions that require requests to be signed with Amazon Signature Version 4.
- Added: Issue where JBIG2 encoded images in PDFs were not being decoded correctly.
- Added: Support for reporting composite keys. NOTE: This does not add support for scanning composite keys.

## BUG FIXES

- Fixed: Issue where Amazon S3 Bucket scans would appear to fail because of an incorrectly entered scan location.
- Fixed: Issue where Windows shared folder scans did not allow very long paths.
- Fixed: Issue where XLSX files containing multiple worksheets would need to be remediated more than once.
- Fixed: Issue where certain date formats contained in files would cause scan errors.
- Fixed: Issue where custom search filters would change unexpectedly when repeatedly modified.
- Fixed: Issue where file attribute custom search filters were not working for cloud Targets.
- Fixed: Issue where scanning blobs in MS SQL Server would fail.
- Fixed: Issue where scanning remote Targets that do not reside on a domain would fail.
- Fixed: Issue where scans could not access Amazon S3 Buckets with names that contain periods.
- Fixed: Issue where setting a date filter for Exchange scans would not work.
- Fixed: Issue where some files were not being scanned in Amazon S3 Buckets.

- Fixed: Issue where, in an XLS file, a series of adjacent cells containing digits would be detected incorrectly as credit card numbers.

## IMPROVEMENTS

- Improved: CSV reports contain more detail.
- Improved: Support for PST files.
- False positives: Removed false positives that occur in Windows configuration files and certain temporary internet files.
- False positives: Removed false positives that occur in python source files in Solaris SPARC systems.
- False positives: Removed false positives that occur in Libre Office LICENSE.fofd files.

# ABOUT CARD RECON

**Note:** This documentation is a work-in-progress and will be progressively updated.

## 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 emails, databases, documents, 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 Assessors \(QSAs\)](#), and trusted by over 2,500 merchants across 80 countries. Support for more than 7+ operating systems and the ability to scan cloud storage means that **CARD RECON** can cover the majority of common system types used by organisations.

## 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** Standard Edition is designed for scanning the contents of Workstations whilst **CARD RECON** Advanced Edition is designed for sample-based scanning of Servers.

For environments of 5 or more systems it is recommended that [Enterprise Recon](#) be used due to its centralised design and ability to automate scanning and consolidate reporting data from multiple scans.

## ADDITIONAL RESOURCES

Advanced support for **CARD RECON** can be found at: <https://support.groundlabs.com>

More information on **CARD RECON** can be found at: <https://www.groundlabs.com/software/card-recon>

More information on Ground Labs products can be found at: <https://www.groundlabs.com>

The **CARD RECON End User License Agreement** can be found at:  
<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 offline and online storage locations, including workstations, file servers, NAS and SAN devices, Gmail, Lotus Notes, Oracle, Amazon AWS Cloud.
- **PCI Compliance Reporting:** Generate comprehensive and easy to read compliance reports that are detailed and actionable; reports can be saved to 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:** CARD RECON can run, without installation, on any of the 7 supported platforms; it also can be run from portable storage media.
- **Low CPU Usage:** Designed to minimise impact on users or production applications so that you can keep your systems secure without having to schedule downtime.

## DISCLAIMER

It is important that you read and understand this document, which has been prepared for your gainful and reasonable use of CARD RECON. Use of CARD RECON 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](mailto: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** 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. However, Ground Labs will provide support for new versions as they are released to market once they have been completed appropriate testing and compliance procedures.
- If your organization uses an environment not listed in the table below, please contact [support@groundlabs.com](mailto:support@groundlabs.com).

Category	Operating Systems
Windows Desktop Environments (GUI and Command-Line)	<ul style="list-style-type: none"> <li>• Windows XP</li> <li>• XP Embedded</li> <li>• Windows Vista</li> <li>• Windows 7</li> <li>• Windows 8</li> <li>• Windows 8.1</li> <li>• Windows 10</li> </ul>
Windows Server Environments (GUI and Command-Line)	<ul style="list-style-type: none"> <li>• Windows Server 2003</li> <li>• Windows Server 2008</li> <li>• Windows Server 2012</li> <li>• Windows Server 2016</li> </ul>
Linux System Environments (Command-Line only)	<ul style="list-style-type: none"> <li>• Centos</li> <li>• Debian</li> <li>• Fedora</li> <li>• Redhat</li> <li>• Slackware</li> <li>• SUSE</li> <li>• Ubuntu</li> </ul>

Category	Operating Systems
	(A minimum Linux Kernel version of 2.4 is required.)
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).
UNIX System Environment (Command-Line only)	<ul style="list-style-type: none"> <li>• Solaris 9.x - 11.x (SPARC &amp; Intel x86)</li> <li>• AIX 6.1 - 7.1</li> <li>• FreeBSD 9+ (Intel x86)</li> <li>• HP UX 11.31+ (Intel Itanium)</li> <li>• Macintosh - OSX 10.5+ (Intel x86 &amp; PowerPC)</li> </ul>

# 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 \(page 4\)](#).

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

- **Windows:** See Microsoft's "[Which Windows operating system am I running?](#)"
- **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. This guide assumes that you are running CARD RECON on the host you wish to scan and that you are scanning the host's local storage.

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 cardrecon_linux26_2.0.xx ..../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 authorised host system.

**Info:** For a list of certified operating systems and system requirements, see [System Requirements \(page 4\)](#).

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 \(page 36\)](#).
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`.

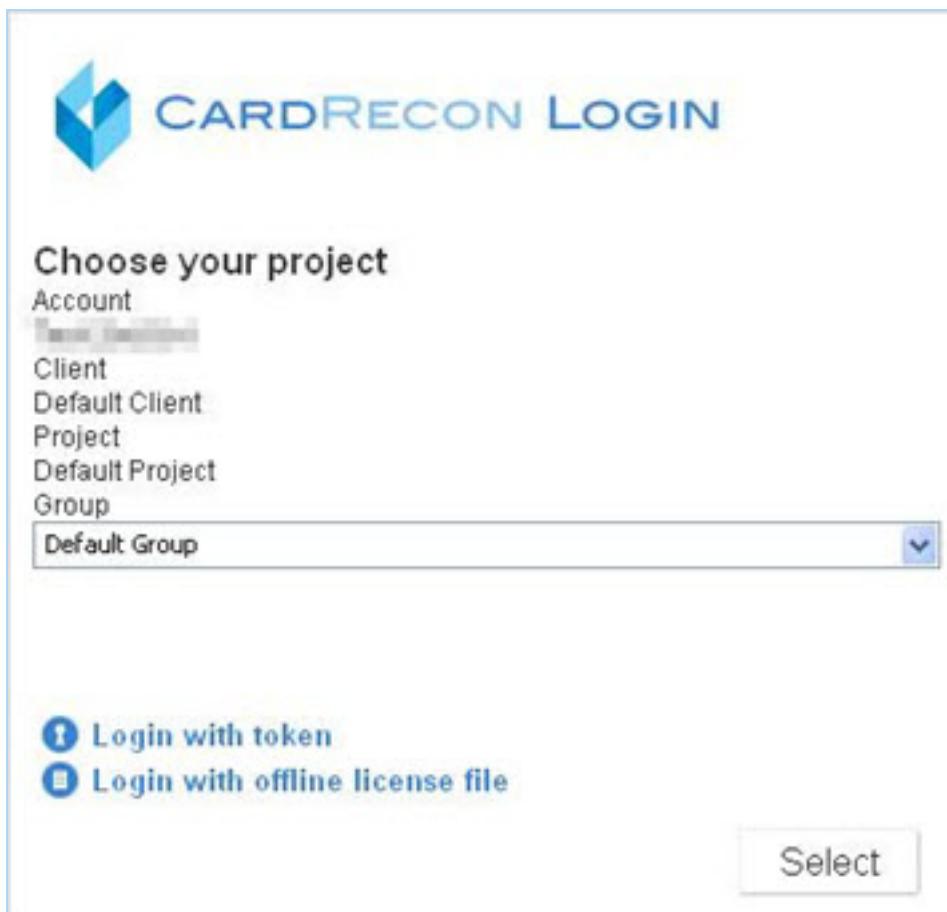
If it finds any of these files in the directory that the **CARD RECON** executable occupies, it will try to load them when the **CARD RECON** runs.

To run **CARD RECON**:

1. Double-click on the **CARD RECON** executable (e.g. `cardrecon_gui_2.0.xx.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**.



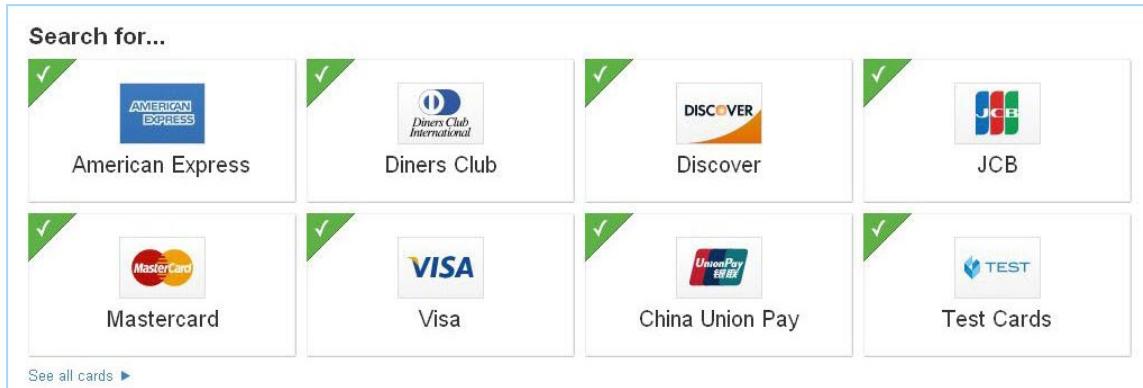
**Note: Managing licenses**

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.

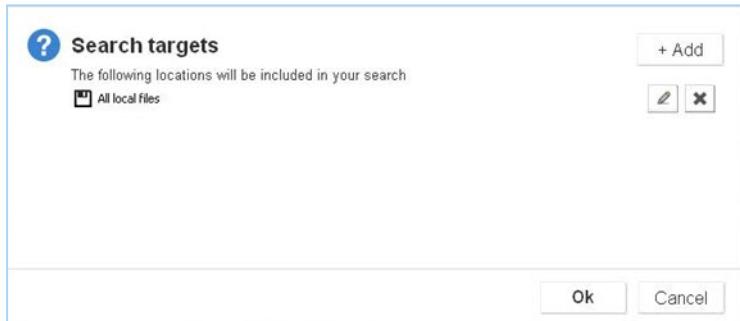
If you are not sure of which project or license group to use, contact your IT administrator or the licensee for more information. If you are the licensee, IT administrator, or the only user, you can choose **Default Project** or **Default Client**.

For more information on how to manage your licenses, please see [CARD RECON Licensing \(page 24\)](#).

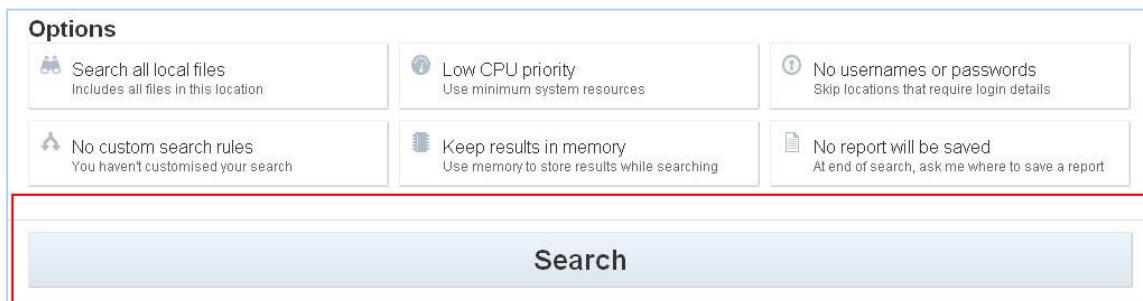
4. On the dashboard, select the card data types to include in your scan.



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 \(page 47\)](#) 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 \(page 17\)](#).

# RUNNING THE CARD RECON CLI

Running the **CARD RECON** CLI executable immediately attempts a scan.

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.

**Note:** 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 \(page 114\)](#).

## RUNNING THE CARD RECON CLI ON WINDOWS

Locate the Windows CLI executable :`cardrecon_2.0.xx.exe`

There are 2 ways to run the Windows CLI.

### METHOD 1

1. Locate `cardrecon_2.0.xx.exe` in Windows Explorer.
2. Right-click `cardrecon_2.0.xx.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 \(page 34\)](#) 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 with default settings - i.e. it scans all local storage with default search parameters (see [Selecting Card Data Types \(page 45\)](#) 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 journal file.
cardrecon_2.0.xx.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 \(page 34\)](#) 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.

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 \(page 17\)](#) ).

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

1. In the Terminal, locate the CARD RECON executable. E.g. `cardrecon_linux26_2.0.xx`.
2. Open your terminal and run `chmod u+x cardrecon_linux26_2.0.xx`.
3. Run the following command as root:

```
# Run a default scan, save a compliance report and an
# encrypted database journal file.
./cardrecon_linux26_64_2.0.xx -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 \(page 24\)](#).

5. Log in using one of the three methods (see [Logging into CARD RECON \(page 34\)](#) 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](#).

```
Username: [REDACTED]
Pass phrase: *****
Account [REDACTED] selected
Client Default Client selected
Project Default Project selected
Select group to use
1) Default Group
2) Enter a new group name
> 1
Group Default Group selected
Select a Card Recon license source for the following targets:
localhost
1) [REDACTED] - 3x365day remain (Card Recon)
2) [REDACTED] - 9x365day remain (Card Recon Advanced)
3) [REDACTED] - 3x365day remain (Data Recon)
4) [REDACTED] - 2x365day remain (Data Recon Advanced)
>
```

CARD RECON should ask you to confirm authorisation of the TARGET. For more information on CARD RECON licensing, see [CARD RECON Licensing \(page 24\)](#)

CARD RECON starts scanning the TARGET with default settings.

Once done, CARD RECON automatically saves a compliance report. 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 \(page 17\)](#)).

To open these files, issue the following command as administrator:

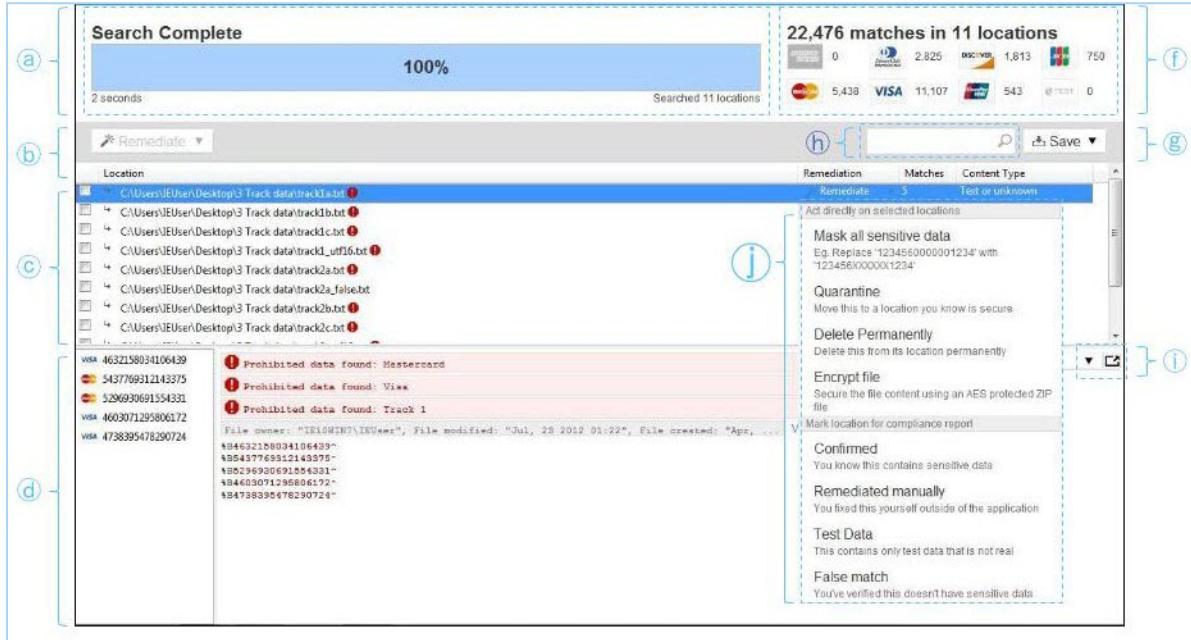
```
# Where <filename>.pdf is the file saved by CARD RECON that you
want to open.
chmod 644 <filename>.pdf
```

**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.

# 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)	<b>The scan progress bar</b>	Shows the progress of the currently running scan, and controls to stop, pause, or skip files during the current scan.
(b)	<b>Bulk remediate/mark</b>	Selecting one or more matches in the match list will allow you to remediate or mark matches in bulk. See <a href="#">Remediating and Marking Matches (page 22)</a> .
(c)	<b>Match list</b>	Shows list of matched data; selecting an item on this list will bring up its details on the Match Inspector.
(d)	<b>Match Inspector</b>	Shows specific match details.
(f)	<b>Match summary</b>	Shows a summary of match data found during the scan.
(g)	<b>Save results database/match list/compliance report</b>	Save options drop-down menu.
(h)	<b>Filter matches</b>	Type in search terms to quickly filter match results.
(i)	<b>Detach Match</b>	Clicking on the "detach" icon will detach the Match Inspector from the main window.

	Label	Description
	<b>Inspector/Change Match Inspector view</b>	CARD RECON window; the Match Inspector can display match details as text or as a hex file.
(J)	<b>Remediate/Mark matches</b>	For more information on how to remediate/mark matches, see <a href="#">Remediating and Marking Matches (page 22)</a> .

**Warning:** If you click **Back** to go to the dashboard, and start a new scan by clicking **Search**, your 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.

**CARDRECON REPORT**

**a** Results on **IE10WIN7**      13 Apr 2016 11:58PM - 14 Apr 2016 12:48AM

**b**

- 135,739 locations are clean  
No sensitive data was found in these locations
- 293,783 instances of cardholder data  
These should be encrypted or removed as soon as possible
- 210 instances of prohibited data  
This includes magnetic stripe data and must be removed immediately

**c** 0 search filters      7 card brands

**d**

Host IP	10.0.2.15	Card Recon 2.0.13 (Standard Edition)		
OS	Microsoft Windows 7 Enterprise Edition 32-bit	Licensed to Test Zed Ent		
Searched	11.77 GB (11,774,991,250 bytes)			

**e** 1 Search Target

Test	Prohibited	Cardholder	%
1,755	210	293,783	100.0

**f** 17 Inaccessible locations  
*Details at the bottom of the report*

**g** Search Summary

Total Match Locations	2,047
Total Matches	293,783

By Status	Prohibited	Cardholder	%
Unconfirmed Matches <i>You haven't confirmed that these contain match data.</i>	210	293,783	99.4
Confirmed Matches <i>You know these contain match data.</i>	0	0	none
Remediated using Card Recon (excluded from total) <i>You masked, quarantined, encrypted or deleted these using Card Recon.</i>	0	0	none

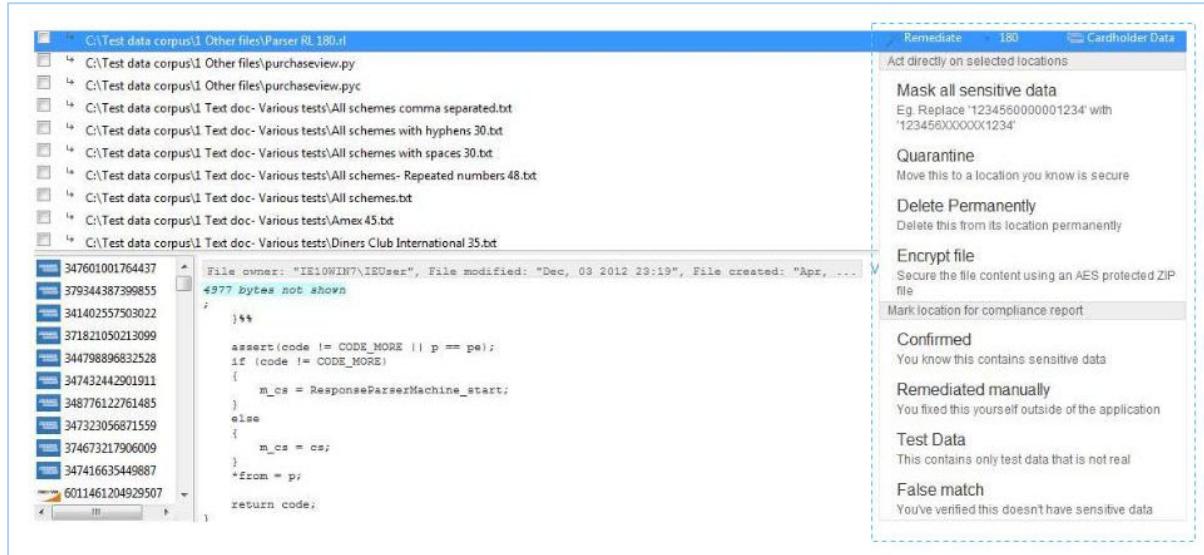
	Label	Description
(a)	Date and status of scan	Gives the host name of the host scanned, the date the scan started, and the date the scan was completed or stopped.  If the scan was canceled or stopped (you cannot generate a compliance report unless you complete or stop a scan), the report will state that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

	Label	Description										
	parameters	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 <b>CARD RECON</b> , and licensee details.										
(e)	Target summary	Shows the number of match locations and the number of matches, organised by targets.  Also shows the number of locations that cannot be accessed by <b>CARD RECON</b> .										
(f)	Search summary	<p>Shows a summary of all match details.</p> <table border="1"> <thead> <tr> <th>Search Summary Category</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Overview</td> <td> <p>Provides total number of non-compliant match locations and total number of non-compliant matches found during the scan.</p> <p>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.</p> <p>See the section below on "Match status".</p> </td> </tr> <tr> <td>"By Status"</td> <td>Shows matches organised by status. See the section below on "Match status".</td> </tr> <tr> <td>"By Card Brand"</td> <td>Shows matches organised by card brand; see <a href="#">6.2. Selecting Card Data Types</a></td> </tr> <tr> <td>"By Content Type"</td> <td> <p>Shows matches organised by file format types.</p> <p><b>CARD RECON</b> has native support for certain file formats, and will scan these files with the appropriate decoder.</p> <p>For formats that <b>CARD RECON</b> does not have native support for, <b>CARD RECON</b> will decode by brute force.</p> <p>Matches found in files that <b>CARD RECON</b> has scanned but does not have native support for will be reported as "Text or unknown" in the "By Content Type" category.</p> </td> </tr> </tbody> </table>	Search Summary Category	Description	Overview	<p>Provides total number of non-compliant match locations and total number of non-compliant matches found during the scan.</p> <p>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.</p> <p>See the section below on "Match status".</p>	"By Status"	Shows matches organised by status. See the section below on "Match status".	"By Card Brand"	Shows matches organised by card brand; see <a href="#">6.2. Selecting Card Data Types</a>	"By Content Type"	<p>Shows matches organised by file format types.</p> <p><b>CARD RECON</b> has native support for certain file formats, and will scan these files with the appropriate decoder.</p> <p>For formats that <b>CARD RECON</b> does not have native support for, <b>CARD RECON</b> will decode by brute force.</p> <p>Matches found in files that <b>CARD RECON</b> has scanned but does not have native support for will be reported as "Text or unknown" in the "By Content Type" category.</p>
Search Summary Category	Description											
Overview	<p>Provides total number of non-compliant match locations and total number of non-compliant matches found during the scan.</p> <p>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.</p> <p>See the section below on "Match status".</p>											
"By Status"	Shows matches organised by status. See the section below on "Match status".											
"By Card Brand"	Shows matches organised by card brand; see <a href="#">6.2. Selecting Card Data Types</a>											
"By Content Type"	<p>Shows matches organised by file format types.</p> <p><b>CARD RECON</b> has native support for certain file formats, and will scan these files with the appropriate decoder.</p> <p>For formats that <b>CARD RECON</b> does not have native support for, <b>CARD RECON</b> will decode by brute force.</p> <p>Matches found in files that <b>CARD RECON</b> has scanned but does not have native support for will be reported as "Text or unknown" in the "By Content Type" category.</p>											

	Label	Description												
(8)	Match detail and status	<p><b>MATCH DETAIL</b></p> <p>Match details are sorted into 3 columns:</p> <ul style="list-style-type: none"> <li>• "Test"</li> <li>• "Prohibited"</li> <li>• "Cardholder"</li> </ul>												
<table border="1" data-bbox="430 541 1389 905"> <thead> <tr> <th data-bbox="430 541 616 624">Match Severity</th><th data-bbox="616 541 1389 624">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="430 624 616 720">"Test"</td><td data-bbox="616 624 1389 720">The scanned locations that contain match test card patterns. These matches should not affect PCI compliance.</td></tr> <tr> <td data-bbox="430 720 616 840">"Prohibited"</td><td data-bbox="616 720 1389 840">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.</td></tr> <tr> <td data-bbox="430 840 616 905">"Cardholder"</td><td data-bbox="616 840 1389 905">The total number of match instances found during the scan.</td></tr> </tbody> </table>			Match Severity	Description	"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 Severity	Description													
"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.													
<p><b>MATCH STATUS</b></p> <p>Matches can be labelled with 6 different statuses. How a match is labelled will determine how it is reported in the compliance report.</p>														
<table border="1" data-bbox="430 1035 1389 2237"> <thead> <tr> <th data-bbox="430 1035 652 1080">Match Status</th><th data-bbox="652 1035 1389 1080">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="430 1080 652 1388">"Unconfirmed Matches"</td><td data-bbox="652 1080 1389 1388"> <p>"Unconfirmed" matches are data that match <b>CARD RECON's</b> search patterns, and are likely to contain non-compliant data.</p> <p>This data should be reviewed and marked as "confirmed", a "false match", or "test data".</p> <p>Matches found during an initial scans will by default be marked as "unconfirmed", and will require review by the user.</p> </td></tr> <tr> <td data-bbox="430 1388 652 1484">"Confirmed Matches"</td><td data-bbox="652 1388 1389 1484">"Confirmed" matches are matches that have been reviewed by the user and are found to contain non-compliant data.</td></tr> <tr> <td data-bbox="430 1484 652 1754">"Remediated using <b>CARD RECON</b>" *</td><td data-bbox="652 1484 1389 1754"> <p>Matches that have been marked as "Remediated using <b>CARD RECON</b>" are confirmed matches that have been remediated using <b>CARD RECON's</b> built-in remediation tools.</p> <p>Remediating matches with <b>CARD RECON's</b> built-in remediation tools will automatically mark them as "Remediated using <b>CARD RECON</b>".</p> </td></tr> <tr> <td data-bbox="430 1754 652 2091">"Remediated Manually" *</td><td data-bbox="652 1754 1389 2091"> <p>Matches that have been marked as "Remediated Manually" are confirmed matches that have been marked by a user as remediated with tools outside of <b>CARD RECON</b>.</p> <p>Marking matches as having been "Remediated Manually" will not alter existing data.</p> <p><b>CARD RECON</b> cannot guarantee that matches that have been marked as manually remediated have been effectively remediated to comply with PCI DSS.</p> </td></tr> <tr> <td data-bbox="430 2091 652 2237">"False Match" *</td><td data-bbox="652 2091 1389 2237">Matches that have been marked as a "False Match" are matches that have been reviewed and found to be false positives.</td></tr> </tbody> </table>			Match Status	Description	"Unconfirmed Matches"	<p>"Unconfirmed" matches are data that match <b>CARD RECON's</b> search patterns, and are likely to contain non-compliant data.</p> <p>This data should be reviewed and marked as "confirmed", a "false match", or "test data".</p> <p>Matches found during an initial scans will by default be marked as "unconfirmed", and will require review by the user.</p>	"Confirmed Matches"	"Confirmed" matches are matches that have been reviewed by the user and are found to contain non-compliant data.	"Remediated using <b>CARD RECON</b> " *	<p>Matches that have been marked as "Remediated using <b>CARD RECON</b>" are confirmed matches that have been remediated using <b>CARD RECON's</b> built-in remediation tools.</p> <p>Remediating matches with <b>CARD RECON's</b> built-in remediation tools will automatically mark them as "Remediated using <b>CARD RECON</b>".</p>	"Remediated Manually" *	<p>Matches that have been marked as "Remediated Manually" are confirmed matches that have been marked by a user as remediated with tools outside of <b>CARD RECON</b>.</p> <p>Marking matches as having been "Remediated Manually" will not alter existing data.</p> <p><b>CARD RECON</b> cannot guarantee that matches that have been marked as manually remediated have been effectively remediated to comply with PCI DSS.</p>	"False Match" *	Matches that have been marked as a "False Match" are matches that have been reviewed and found to be false positives.
Match Status	Description													
"Unconfirmed Matches"	<p>"Unconfirmed" matches are data that match <b>CARD RECON's</b> search patterns, and are likely to contain non-compliant data.</p> <p>This data should be reviewed and marked as "confirmed", a "false match", or "test data".</p> <p>Matches found during an initial scans will by default be marked as "unconfirmed", and will require review by the user.</p>													
"Confirmed Matches"	"Confirmed" matches are matches that have been reviewed by the user and are found to contain non-compliant data.													
"Remediated using <b>CARD RECON</b> " *	<p>Matches that have been marked as "Remediated using <b>CARD RECON</b>" are confirmed matches that have been remediated using <b>CARD RECON's</b> built-in remediation tools.</p> <p>Remediating matches with <b>CARD RECON's</b> built-in remediation tools will automatically mark them as "Remediated using <b>CARD RECON</b>".</p>													
"Remediated Manually" *	<p>Matches that have been marked as "Remediated Manually" are confirmed matches that have been marked by a user as remediated with tools outside of <b>CARD RECON</b>.</p> <p>Marking matches as having been "Remediated Manually" will not alter existing data.</p> <p><b>CARD RECON</b> cannot guarantee that matches that have been marked as manually remediated have been effectively remediated to comply with PCI DSS.</p>													
"False Match" *	Matches that have been marked as a "False Match" are matches that have been reviewed and found to be false positives.													

# REMEDIATING AND MARKING MATCHES

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 LICENSING

This section covers the following topics:

- [Subscription License \(page 24\)](#)
- [Targets \(page 24\)](#)
- [CARD RECON Standard Edition and Advanced Edition \(page 25\)](#)

## SUBSCRIPTION LICENSE

CARD RECON 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
Servers	<p><b>All servers:</b> 1 license per server. This allows you to run scans on the local file system, process memory, and on network storage.</p> <div style="background-color: #e0f2ff; padding: 10px;"> <p><b>Info:</b> The server on which the network storage device is hosted requires a license, but the host on which the network storage device is mounted does not.</p> </div> <p><b>Database servers:</b> 1 license per database server. Database servers are licensed individually. If using a clustered database, each node must also be individually licensed.</p> <p><b>Websites:</b> 1 license per domain name. No limit on sub-folders within the same domain. Sub-domains are licensed separately. For example, the following require a separate license each:</p> <ul style="list-style-type: none"> <li>• <code>example.com</code></li> <li>• <code>www.example.com</code></li> <li>• <code>subdomain.example.com</code></li> </ul>
OneDrive Personal	1 license per OneDrive Personal user.
Google Apps/ G Suite	1 license per user across Google Mail, Google Calendars, Google Tasks, and Google Drive storage.
Dropbox (for individuals)	1 license per Dropbox (for individuals) user.

Target Type	License Assignment
Box Enterprise	1 license per Box business user.
Amazon S3 Bucket	1 license per Bucket.
Azure Queues/Tables/BLOB	1 license per Queue. 1 license per Table. 1 license per BLOB.
Rackspace Cloud Files	1 license per Rackspace Cloud Files container.
Office 365 Mail or Microsoft Exchange	1 license per Office 365 or Microsoft Exchange user. Must have IMAP enabled.
Google Mail (Gmail)	See Google Apps/ G Suite for more information. Must have IMAP enabled.
Lotus Notes	1 license per Lotus Notes user.
IMAP/IMAPS Mailboxes	1 license per internet mailbox (IMAP/IMAPS).

## CARD RECON STANDARD EDITION AND ADVANCED EDITION

**CARD RECON** is typically used to scan local storage on host computers for cardholder data.

To use **CARD RECON** to scan advanced TARGETS such as databases and cloud storage, you would need to upgrade to a **CARD RECON** Advanced Edition license.

### FEATURE COMPARISON

Platform or File Type	Standard Edition	Advanced Edition
Windows	✓	✓
macOS	✓	✓
Linux	✓	✓
FreeBSD	✓	✓
Solaris		✓
HP-UX		✓
AIX		✓
EBCDIC for Mainframes		✓
<b>Note:</b> Some features are not available on all supported operating systems.		
File Formats		

Platform or File Type	Standard Edition	Advanced Edition
Text Files	✓	✓
Multiple Encoding types	✓	✓
Office Documents	✓	✓
Compressed Files	✓	✓
Databases (client side)	✓	✓
Databases (server side)		✓
Emails (client)	✓	✓
Emails (server)		✓
Audio Files		✓
Image File OCR		✓
<b>Target Types</b>		
Local Storage	✓	✓
Free Disk Space	✓	✓
Shadow Volumes	✓	✓
Process Memory	✓	✓
Websites	✓	✓
Network Storage		✓
Live Database Servers		✓
Live Email Servers		✓
Cloud Storage		✓
<b>Database Servers (Live)</b>		
IBM DB2		✓
Microsoft SQL Server		✓
MySQL		✓
Oracle		✓
PostgreSQL		✓
SAP Sybase		✓
<b>Email Servers</b>		
Office 365 (IMAP)*		✓
Microsoft Exchange (IMAP)*		✓

Platform or File Type	Standard Edition	Advanced Edition
Gmail (IMAP)*		✓
Generic IMAP*		✓
Lotus Notes*		✓
<b>Cloud Storage</b>		
Amazon AWS (S3)		✓
Google Apps		✓
Microsoft Azure		✓
Dropbox		✓
Box		✓
Microsoft OneDrive		✓
Rackspace		✓
<b>Classification and Remediation</b>		
Mask Cardholder Data	✓	✓
Secure Quarantine	✓	✓
Permanent Delete	✓	✓
Content Inspection	✓	✓
Encryption	✓	✓

\*Individual user credentials required for each unique mailbox. To scan multiple mailboxes using administrator credentials, use [Enterprise Recon](#).

# 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 [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 [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 \(page 29\)](#)

**Note:** By default, CARD RECON will assume that the local storage system of host (the computer that CARD RECON is running on) is the TARGET. If this should not be the case, you will need to change the TARGET. Please see [Configuring Scans for CARD RECON \(page 43\)](#)

**Info:** For more information about licensing, please refer to the [Subscription Licensing and Upgrades FAQ](#).

# 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.

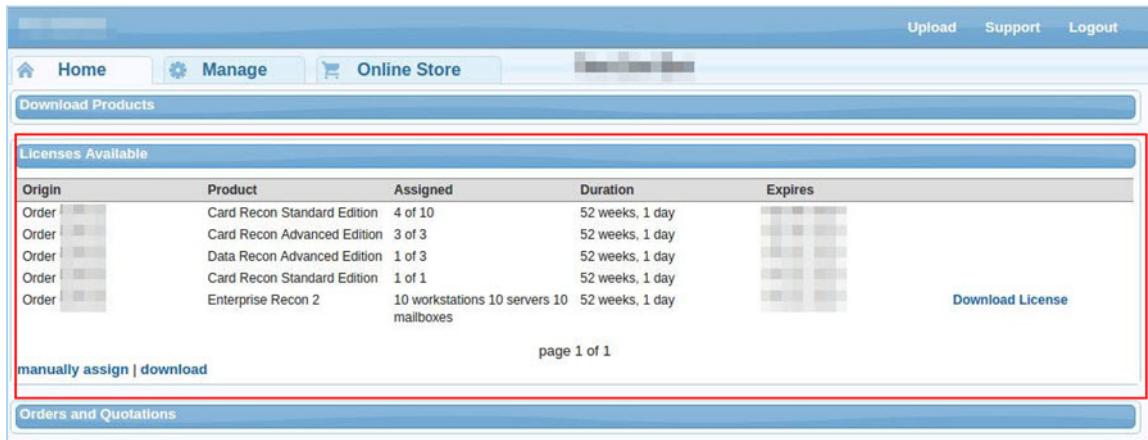
See [Online authentication \(page 34\)](#) for more information.

**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 [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.



Origin	Product	Assigned	Duration	Expires
Order 1	Card Recon Standard Edition	4 of 10	52 weeks, 1 day	
Order 1	Card Recon Advanced Edition	3 of 3	52 weeks, 1 day	
Order 1	Data Recon Advanced Edition	1 of 3	52 weeks, 1 day	
Order 1	Card Recon Standard Edition	1 of 1	52 weeks, 1 day	
Order 1	Enterprise Recon 2	10 workstations 10 servers 10 mailboxes	52 weeks, 1 day	

[Download License](#)

page 1 of 1

[manually assign](#) | [download](#)

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.

Targets included in license				How to assign a license?
Hosts	MAC Address	Product	Expires	
[REDACTED]	[REDACTED]	Card Recon Standard Edition	[REDACTED]	
[REDACTED]	[REDACTED]	Card Recon Standard Edition	[REDACTED]	
hostname [REDACTED]	or mac [REDACTED]	Card Recon Standard Edition	[REDACTED]	<a href="#">remove</a>
<a href="#">Add a new target</a> <small>Upload a spreadsheet (Text or CSV only)</small>				
<b>Select a License to Use</b> Order [REDACTED] 10x Card Recon Standard Edition (4 remain), expires on [REDACTED]				
<a href="#">Download license</a>				

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

Targets included in license				How to assign a license?
Hosts	MAC Address	Product	Expires	
[REDACTED]	[REDACTED]	Card Recon Standard Edition	[REDACTED]	
[REDACTED]	[REDACTED]	Card Recon Standard Edition	[REDACTED]	
hostname [REDACTED]	or mac [REDACTED]	Card Recon Standard Edition	[REDACTED]	<a href="#">remove</a>
<a href="#">Add a new target</a> <small>Upload a spreadsheet (Text or CSV only)</small>				
<b>Select a License to Use</b> Order [REDACTED] 10x Card Recon Standard Edition (4 remain), expires on [REDACTED]				
<a href="#">Download license</a>				

**Info:** To find the `hostname` or MAC address of your host, see [Getting Host name and MAC Address \(page 32\)](#).

**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 (`*.lic`) 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 \(page 34\)](#).

## 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 \(page 38\)](#).

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 \(page 34\)](#).

**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 \(page 29\)](#).

**Note:** This guide assumes that you are attempting to license a TARGET that is the local storage or local memory on a host machine.

## 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
```

```
Microsoft Windows [Version 6.1.7601]  
Copyright <c> 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\IEUser>hostname  
IE10Win7  
  
C:\Users\IEUser>getmac  
  
Physical Address      Transport Name  
=====  =====  
08-00-27-D2-9C-60    \Device\Tcpip_{A2692622-D935-45DD-BC6A-0FEA4F88524C}  
  
C:\Users\IEUser>
```

`hostname` gets the command prompt to return your Windows machine's host name, while `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).

```
eruser@groundlabsdemo:~$ hostname  
groundlabsdemo  
eruser@groundlabsdemo:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:a6:a7:a9  
          inet addr:10.1.101.126 Bcast:10.1.255.255 Mask:255.255.0.0  
          inet6 addr: fe80::a00:27ff:fea6:a7a9/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:2531 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:618 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:233590 (228.1 KiB) TX bytes:60287 (58.8 KiB)
```

**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 `HWaddr` 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's 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 \(page 38\)](#).

### GROUND LABS SERVICES LOGIN

You can log into CARD RECON using your [Ground Labs Services Portal](#) username and password.

The image shows the CARD RECON login interface. At the top left is the CARD RECON logo. Below it, the text "CARDRECON LOGIN" is displayed. A section titled "Enter your login details" contains two input fields: "Username" and "Pass phrase". Below these fields are two links: "Login with token" and "Login with offline license file". At the bottom right of the interface is a "Login" button.

**CARD RECON** will connect to Ground Labs's 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.

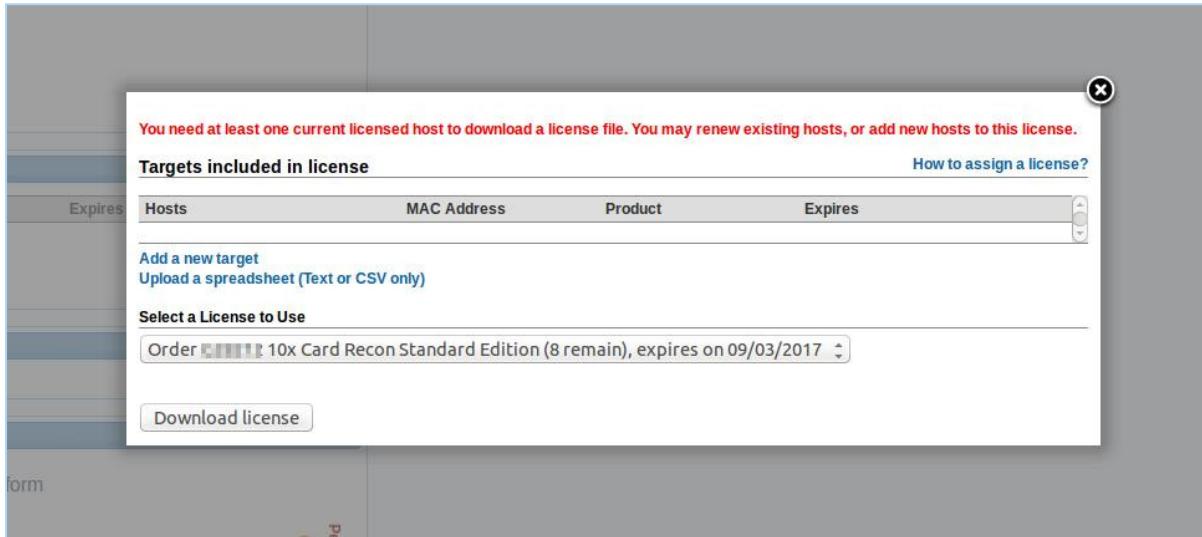
If the TARGET has a license already assigned to it, using a SCAN TOKEN will not use an additional license if the existing license and the SCAN TOKEN are from the same [Ground Labs Services Portal](#) parent account.

For more information on SCAN TOKENS, see [Generating and Using Scan Tokens \(page 38\)](#).

## 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 authorised 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.

```
C:\Users\Public>cardrecon_x64_2.0.21.exe
Card Recon license required
1) Ground Labs Login
2) Use an online token
3) Use offline license file
> 3
Location of offline license file:
```

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 pass-phrases that can be distributed to authorised 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.

Scan Tokens				
Code	Comment	Activations	Created	Expires
emptier-outside-looser-feeble	cr-token-multi-2 cr-token-test1	0/2 1/1		
page 1 of 1				

[add new scan token](#)

**Info:** SCAN TOKENS are commonly used organisations where scan permissions and privileges need to be distributed to trusted users without giving them access to the organisation's [Ground Labs Services Portal](#) account.

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

- Assign licenses to TARGETS.
- Scan targets.
- Access **CARD RECON** to create, modify, and save **CARD RECON** configuration files for use on another host. For details, see [Save and Load Options \(page 109\)](#).

## 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".

Scan Tokens				
Code	Comment	Activations	Created	Expires
emptier-outside-looser-feeble	cr-token-multi-2 cr-token-test1	0/2 1/1		
page 1 of 1				

[add new scan token](#)

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

License source	<input type="text" value="Order G28212 10x Card Recon Standard E"/>
Single use token	<input checked="" type="checkbox"/>
Maximum uses	<input type="text" value="2"/>
Comment (optional)	<input type="text"/>
<input type="button" value="Create"/>	

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**.

#### Info:

Comments can be added to your SCAN TOKEN to help you keep track of your TOKENS in the "Comment" input box.

Scan Tokens				
Code	Comment	Activations	Created	Expires
emptier-outside-looser-feeble	cr-token-multi-2 cr-token-test1	0/2 1/1		
page 1 of 1				

[add new scan token](#)

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

License source: Order G28212 10x Card Recon Standard E

Single use token:

Maximum uses: 2

Comment (optional):

**Create**

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 a license to the new TARGET.

Scan Tokens				
Code	Comment	Activations	Created	Expires
cr-token-multi-2	cr-token-multi-2	0/2		
emptier-outside-looser-feeble	cr-token-test1	1/1		

add new scan token

page 1 of 1

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 \(page 112\)](#) (CLI)
- [CARD RECON Graphic User Interface \(page 44\)](#) (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 \(page 45\)](#)
- [Selecting Target Location \(page 47\)](#)
- [Setting Resource Usage \(page 96\)](#)
- [Setting Credentials for Restricted Targets \(page 98\)](#)
- [Setting Custom Search Rules \(page 100\)](#)
- [Setting Results Database Options \(page 104\)](#)
- [Setting Compliance Report Savings Options \(page 107\)](#)

**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.

**Search for...**

 American Express	 Diners Club	 Discover	 JCB
 Mastercard	 Visa	 China Union Pay	 Test Cards
 Maestro	 Laser	 Private Label Card	

See less cards ▲

**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.

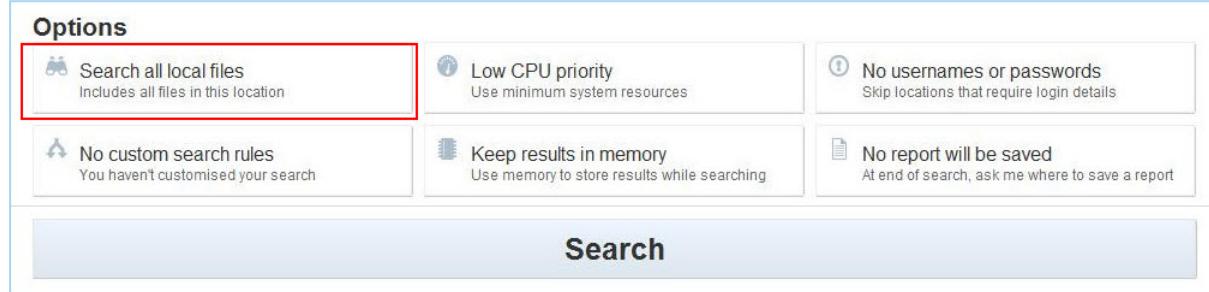
You can select 3 additional card data types:

- Maestro
- Laser

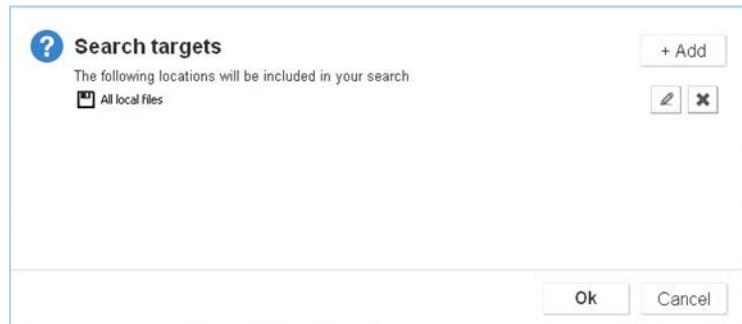
- Private Label Cards

# 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 \(page 49\)](#).
- [Local Memory \(page 51\)](#).
- [Network Storage \(page 52\)](#).
- [Databases \(page 55\)](#).
- [Email \(page 59\)](#).
- [Websites \(page 70\)](#).
- [Cloud Storage \(page 71\)](#).

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 \(page 24\)](#).

**Warning:** Scanning a new TARGET will have CARD RECON prompt you to assign a new license.

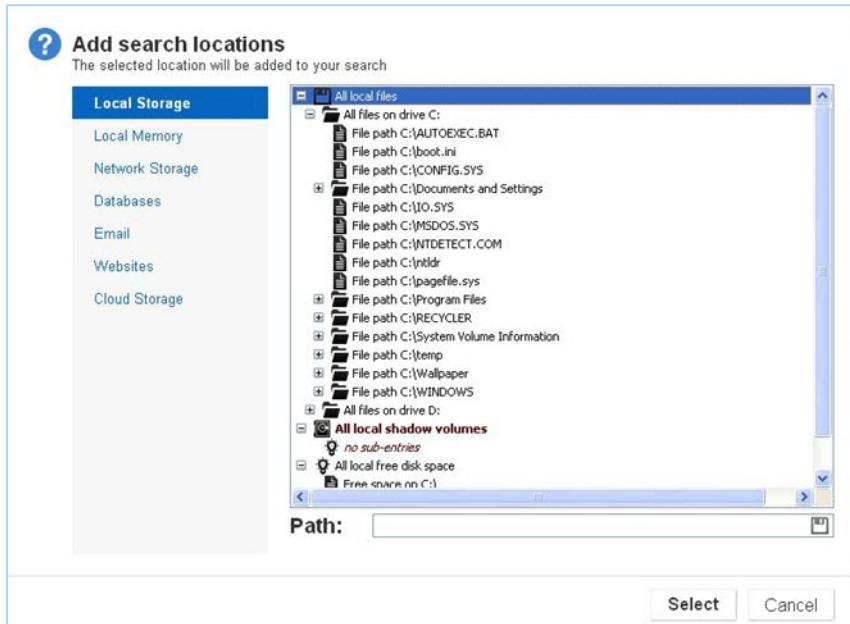
# LOCAL STORAGE

**CARD RECON** can scan local storage for sensitive data.

Local storage for a host would include the contents of local physical storage drives, and the contents of removable media (e.g. USB drives) mounted on the host.

Within the "Local Storage" tab, you can manage the locations on local storage that **CARD RECON** will scan.

Removable media will also appear here.



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 (page 50)
- All local shadow volumes (page 50)
- All local free disk space (page 50)

## 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>

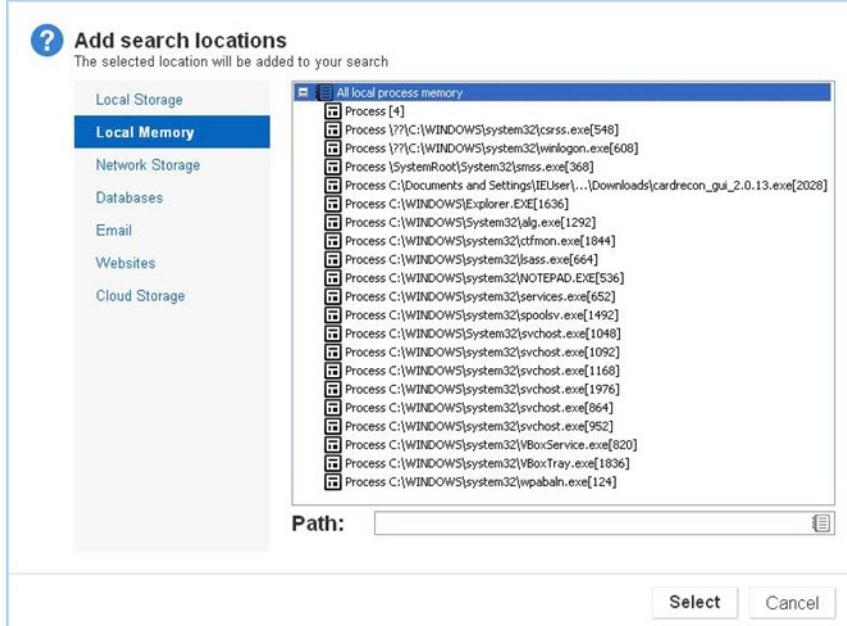
## ALL LOCAL FREE DISK SPACE

(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.



# NETWORK STORAGE

CARD RECON can scan network storage media for sensitive data.

This would include being able to scan remote file servers, Storage Area Networks (SAN) devices, and Network-Attached Storage (NAS) devices.

You can scan the following Network Storage types:

- [Windows Share \(page 53\)](#)
- [UNIX File Share \(page 53\)](#)
- [Remote Access via SSH \(page 53\)](#)

**Warning:** Scanning network storage devices transmits data to-and-from CARD RECON across the network, increasing your PCI footprint and network load.

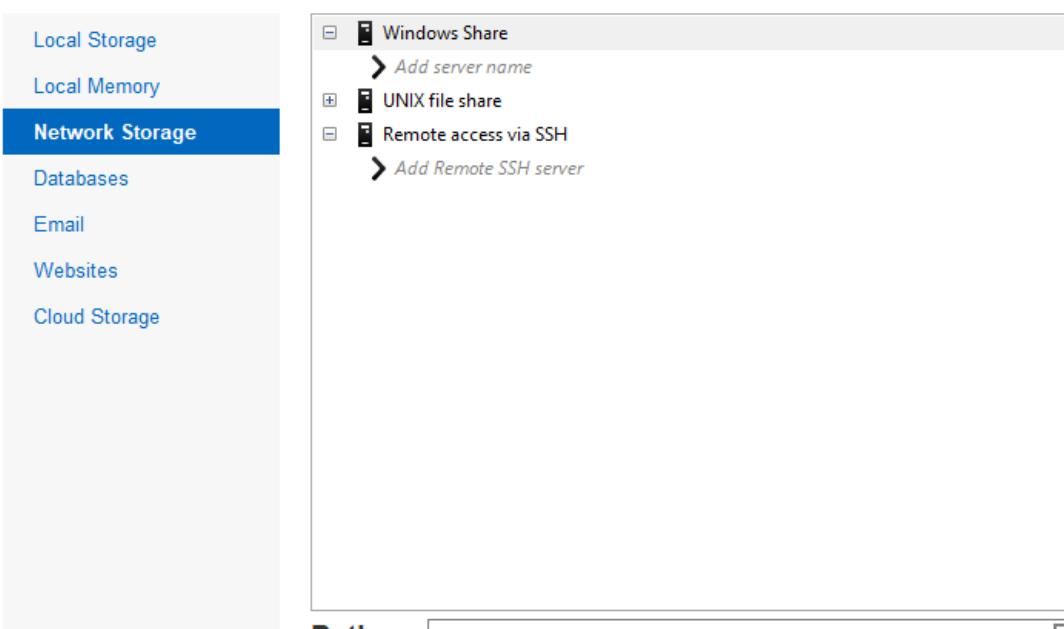
To avoid increasing your PCI footprint and network slowdowns, run a [Local Storage \(page 49\)](#) scan instead.

**Add search locations**  
The selected location will be added to your search

Local Storage  
Local Memory  
**Network Storage**  
Databases  
Email  
Websites  
Cloud Storage

Path:

**Select** **Cancel**

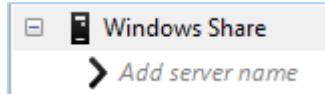


## WINDOWS SHARE

Add a Windows share by clicking on the + to expand the **Windows Share** option.

**CARD RECON** displays the Windows shares available on the network. You can also add a Windows share TARGET by typing the host name or IP address of a Windows share server in the "Add share name" field.

You will be prompted for access credentials if the selected Windows share requires it.



You can also scan a specific share on a Windows share server by typing the share name in the "Add share name" field.



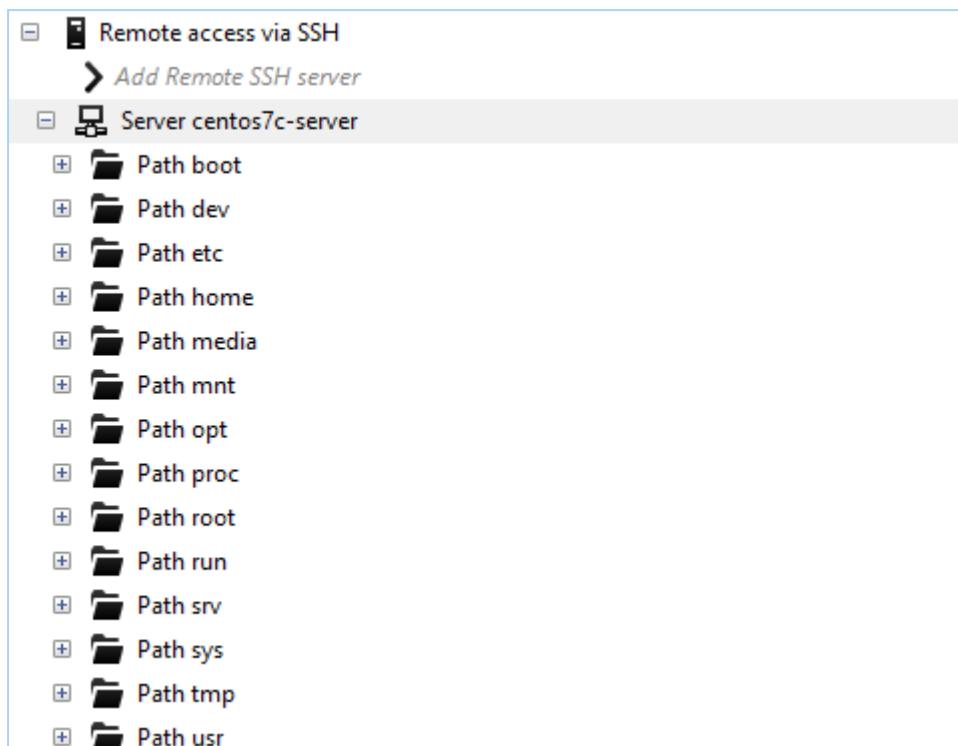
## UNIX FILE SHARE

Add a UNIX file share as a TARGET by typing the host name or IP address of the UNIX file share (NFS).

## REMOTE ACCESS VIA SSH

**CARD RECON** will allow you to scan TARGETS via SSH.

To scan a TARGET via SSH, enter the host name or IP address of the TARGET server, and enter your credentials when prompted. The TARGET must have an SSH server running.



# DATABASES

---

Databases can be scanned in two ways:

- [File-based Scan \(page 55\)](#)
- [Live Database Scan \(page 55\)](#)

## FILE-BASED SCAN

(Not recommended) The data storage files of a database can be scanned directly. Performing a [Local Storage \(page 49\)](#) scan on a database server automatically picks up data storage files and scans them for sensitive data.

Scanning data storage files may run into the following issues:

- Matches from ghost records or slack space may be found, instead of only data that can be queried from the database.
- The data storage files may be locked by a database that is running.

To avoid these issues, perform a live database scan.

## LIVE DATABASE SCAN

A live database scan is run by querying the database directly to search for sensitive data.

### SUPPORTED DATABASES AND REQUIREMENTS

The following databases are supported:

Database	Requirements
MySQL	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> </ul>
Microsoft SQL Server 2005 and above	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> </ul>
PostgreSQL 9.5 and above	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> </ul>
Oracle Database 9 and above	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> <li>• <a href="#">Oracle Instant Client</a> installed on host</li> </ul>
IBM DB2 11.1 and above	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> <li>• <a href="#">Data Server Driver for ODBC and CLI</a> installed on host</li> </ul>
Sybase/SAP Adaptive Server Enterprise (ASE) 15.7 and above	<ul style="list-style-type: none"> <li>• <b>CARD RECON</b> Advanced Edition</li> <li>• <a href="#">Sybase/SAP ASE client</a> installed on host</li> </ul>

## REMEDIATING MATCHES

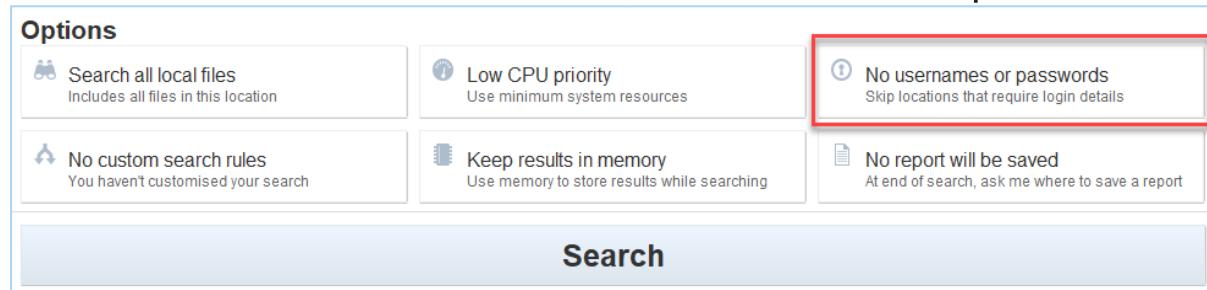
**CARD RECON** does not modify data in the databases it scans. As a result, direct remedial action is unavailable for matches found in a live database scan.

You can, however, mark matches for manual remedial action. See [Remediating and Marking Matches \(page 22\)](#) for more information.

## ADD CREDENTIALS

Your database credentials must have SELECT (data reader) access to the database resources to be scanned.

To add credentials for a database search location, click on **No usernames or passwords**:



In the **Search target credentials** dialog box:

- Click **+ Add** and select one of the following:
  - MySQL
  - Oracle
  - Microsoft SQL
  - IBM DB2
  - PostgreSQL
  - Sybase
- Fill in the following fields:
  - Target location:** Enter the database server `hostname`.
  - Username:** Enter your user name.
  - Password:** Enter your password.
- (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.

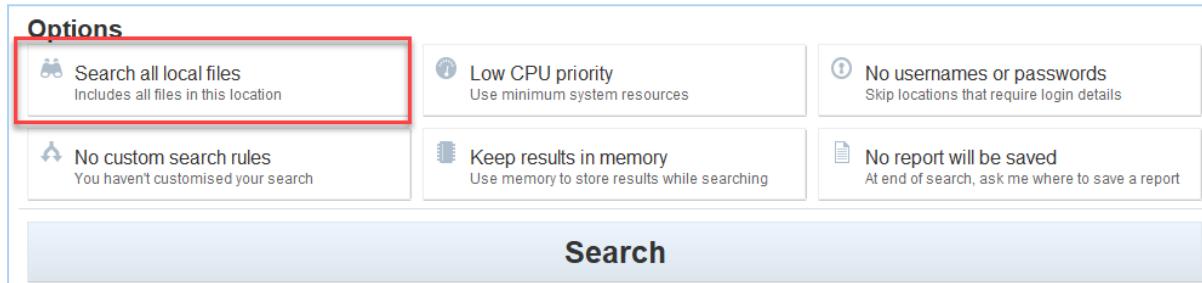
**Tip:** Credentials are only saved if:

- Search configuration is saved. See [Save and Load Options \(page 109\)](#) for more information.
- The results database is saved. See [Setting Results Database Options \(page 104\)](#) for more information.

4. Click **Ok**.

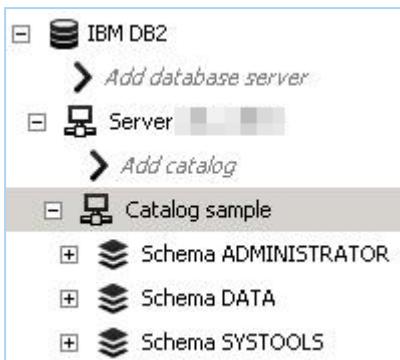
## ADD DATABASES TO SEARCH LOCATIONS

In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click **+ Add**.
2. Select **Databases**.
3. Select one of the following and click **+** to expand the selection:
  - MySQL
  - Oracle
  - Microsoft SQL
  - IBM DB2
  - PostgreSQL
  - Sybase
4. In the **Add database server** field, enter the database server host name as: `hostname[:port]`  
Specify a port if the database server is not using a default port. For more options, see [Database Connection Options \(page 58\)](#) below.
5. Press **Enter** to add the specified database server as a search location.
6. (Optional) Click **+** to expand the added database server and select specific resources to scan.



7. Click **Select** and then **Ok** to finish adding the location.

## DATABASE CONNECTION OPTIONS

Some databases may require you to specify additional parameters to connect to them:

Database	Connection Options
Oracle Database	<p><b>Connect using a fully qualified domain name (FQDN)</b></p> <p>When adding an Oracle Database as a search location, you may need to enter the FQDN of the database server instead of its host name.</p> <p><b>Oracle 12x/TNS: protocol adapter error</b></p> <p>If you are using Oracle 12x, or if the Oracle database displays a "TNS: protocol adapter error", you must specify a <code>SERVICE_NAME</code>.</p> <p>Add the service name to the database server host name:</p> <pre>&lt;hostname (SERVICE_NAME=&lt;SID&gt;) [:port]&gt;[/catalog[/table]]</pre> <p>For example: <code>db_server (SERVICE_NAME=GLAB) /catalog_A/table_1</code></p>
Microsoft SQL Server	<p>Scan a specific SQL Server instance (where multiple are running):</p> <pre>&lt;hostname(instance=&lt;instance_name&gt;) [:port]&gt;</pre> <p>For example: <code>db_server(instance=mssql_instance_1)</code></p>
Sybase/SAP ASE	<p>Scan a specific Sybase instance (where multiple are running):</p> <pre>&lt;hostname(instance=&lt;instance_name&gt;) [:port]&gt;</pre> <p>For example: <code>db_server(instance=sybase_instance_1)</code></p>

# EMAIL

CARD RECON can scan the following email locations:

- [Google Mail \(IMAP\) \(page 59\)](#)
- [Office 365 Mail \(IMAP\) \(page 61\)](#)
- [Internet Mailbox \(page 62\)](#)
- [Internet SSL Mailbox \(page 64\)](#)
- [Lotus Notes \(page 66\)](#)
- [Locally Stored Email Data \(page 68\)](#)

If your email platform is not listed here, you can still scan your mailbox by:

1. Enabling IMAP.
2. Adding your mailbox as an [Internet Mailbox \(page 62\)](#) or [Internet SSL Mailbox \(page 64\)](#) (recommended) Target.

**Info:** Individual user credentials are required for each unique mailbox. To scan multiple mailboxes using administrator credentials, use [Enterprise Recon](#).

## GOOGLE MAIL (IMAP)

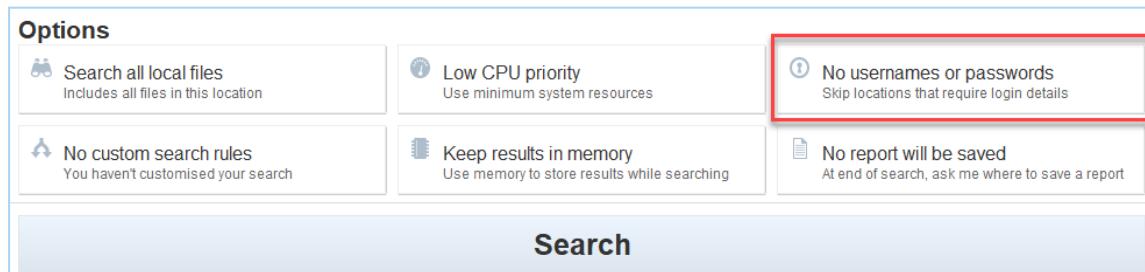
### REQUIREMENTS

Target Google Mail accounts must be a Google Apps or G Suite account. Enable IMAP to scan Google Mail accounts.

### ADD CREDENTIALS

Add credentials for the Google Mail Target:

1. Click on **No usernames or passwords**.

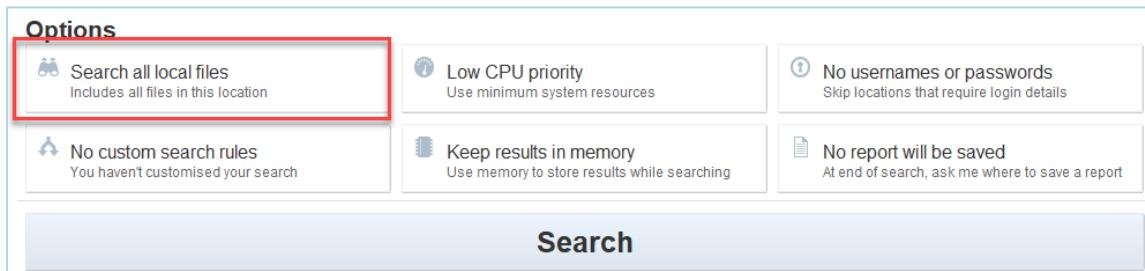


2. In the **Search target credentials** dialog box, click **+ Add** and select **Google Mail**.
3. Fill in the fields:
  - **Target location:** Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.
  - **Username:** Enter the email address of the target mailbox. For example, `user@example.com`
  - **Password:** Enter your mailbox password. If you have 2-factor authentication enabled, create an app password and enter it here. See [2-Factor Authentication \(page 60\)](#) for more information.
4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

## ADD SEARCH LOCATION

Add a Google Mail account as a search location:

1. Click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and select **Email**.
3. Select and expand **Google Mail**.
4. Select the **Add Google Apps domain** field. Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.
5. Select the "Domain" Target that appears below the **Add Google Apps domain** field.
6. (Optional) Select individual folders and emails to scan.
7. Click **Select** to finish adding the Google Mail Target.

## 2-FACTOR AUTHENTICATION

To access Google Mail accounts with 2-factor authentication enabled:

1. On your browser, sign into Google Mail.
2. In Google Mail, navigate to **My Account > Sign-in & security**
3. Under the "Password & sign-in method" section, click on **App passwords**.
4. In the "App passwords" page, go to the **Select the app and device for which you want to generate the app password** section.
5. Click on **Select app**, select **Other (Custom name)** and enter "Scan". Click **GENERATE**
6. Google then displays a 16 character "App password". Use the app password in place of your Google Mail password when entering credentials into **CARD RECON**.

## OFFICE 365 MAIL (IMAP)

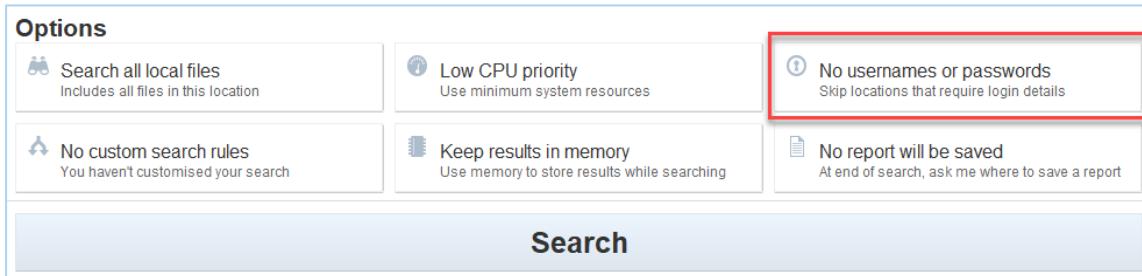
### REQUIREMENTS

Enable IMAP to scan Office 365 Mail accounts.

### ADD CREDENTIALS

Add credentials for the Office 365 Mail Target:

1. Click on **No usernames or passwords**.



2. In the **Search target credentials** dialog box, click **+ Add** and select **Microsoft Office 365 Exchange Web Services (EWS)**.
3. Fill in the fields:
  - **Target location:** Enter the target mailbox as `<domain/email_address>`. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.
  - **Username:** Enter the email address of the target mailbox. For example, `user@example.com`
  - **Password:** Enter your mailbox password. If you have 2-factor authentication enabled, create an app password and enter it here.

**Info: 2-Factor Authentication**

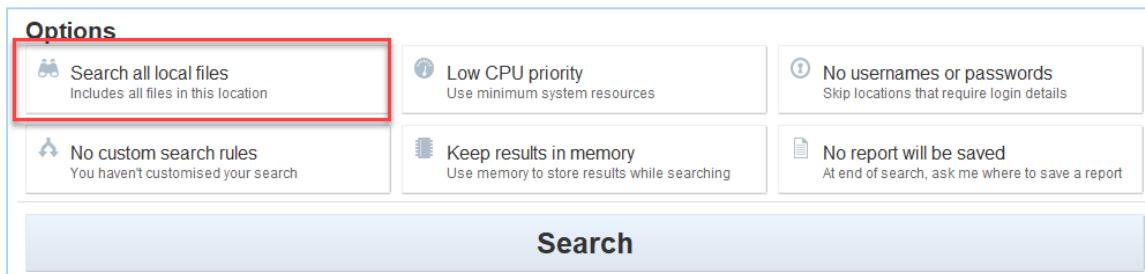
If you have 2-factor authentication enabled for your Office 365 account, you must create an app password for use with **CARD RECON**. See [Microsoft: Create an app password for Office 365](#) for more information.

4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

**ADD SEARCH LOCATION**

Add an Office 365 Mail account as a search location:

1. Click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and select **Email**.
3. Select and expand **Office 365 Mail**.
4. Select the field that appears underneath. Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.
5. Select the "Domain" Target that appears.
6. (Optional) Select individual folders and emails to scan.
7. Click **Select** to finish adding the Office 365 Mail Target.

**INTERNET MAILBOX****Note: Internet SSL Mailbox Target**

(Recommended) Scan Internet Mailboxes using SSL to keep traffic between **CARD RECON** and the mail server encrypted. See [Internet SSL Mailbox \(page 64\)](#) for more information.

Additionally, some email services do not allow you to connect without using SSL. If you are getting a "Username or password incorrect" error while trying to add an Internet Mailbox Target, try adding an Internet SSL Mailbox Target instead.

## REQUIREMENTS

The [Internet Mailbox \(page 62\)](#) Target allows you to add general email accounts as Targets.

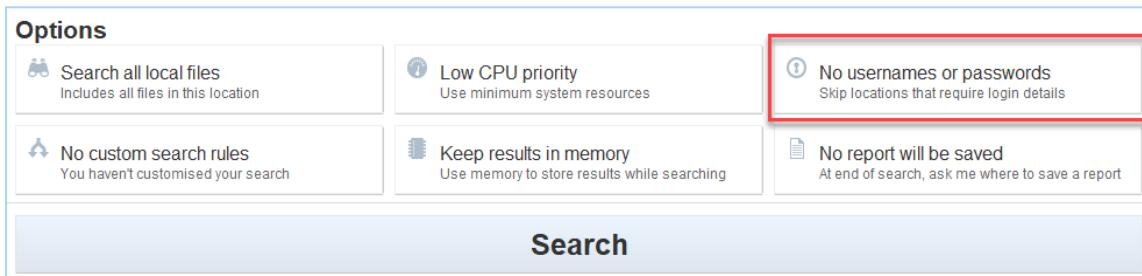
To add a general email account as an Internet Mailbox Target, the email account must:

- Have IMAP enabled.
- Use the default port for IMAP: 143

## ADD CREDENTIALS

Add credentials for the Internet Mailbox Target:

1. Click on **No usernames or passwords**.



2. In the **Search target credentials** dialog box, click **+ Add** and select **Internet Mailbox (IMAP)**.
3. Fill in the fields:

- **Target location**: Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.

**Note:** Check with your email service provider for information on what to enter as the IMAP/S target <domain>. For example, to scan Gmail with IMAP/S, enter `imap.gmail.com` as <domain>.

- **Username**: Enter the email address of the target mailbox. For example, `user@example.com`
- **Password**: Enter your mailbox password. If you have 2-factor authentication enabled, create an app password and enter it here.

### Info: 2-factor authentication

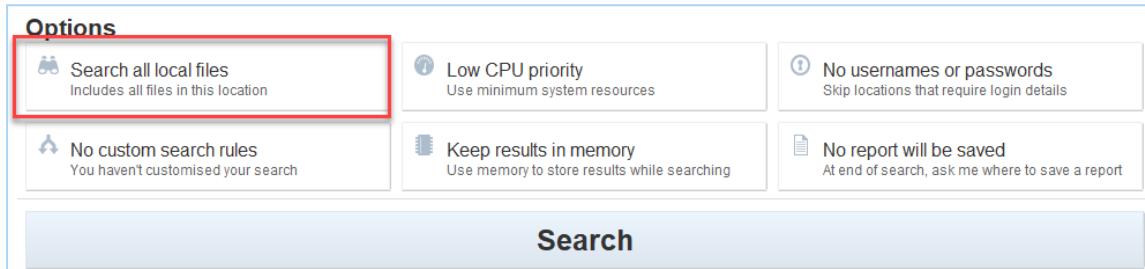
2-factor authentication is not supported. To access Internet Mailbox accounts that require 2-factor authentication, you must set up an app password for use with **CARD RECON**. Create and use the app password instead of your account password.

4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

## ADD SEARCH LOCATION

Add an Internet Mailbox account as a search location:

1. Click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and select **Email**.
3. Select and expand **Internet Mailbox**.
4. Select the **Add imap host** field. Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.

**Note:** Check with your email service provider for information on what to enter as the IMAP/S target <domain>. For example, to scan Gmail with IMAP/S, enter `imap.gmail.com` as <domain>.

5. Select the "Domain" Target that appears.
6. (Optional) Select individual folders and emails to scan.
7. Click **Select** to finish adding the Internet Mailbox Target.

## INTERNET SSL MAILBOX

### REQUIREMENTS

The [Internet SSL Mailbox \(page 64\)](#) Target allows you to add general email accounts as Targets.

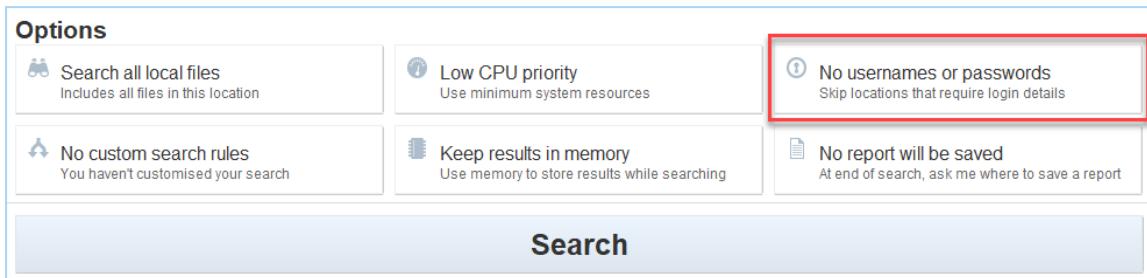
To add a general email account as an Internet SSL Mailbox Target, the email account must:

- Have IMAP enabled.
- Use the default port for IMAP SSL: 993

### ADD CREDENTIALS

Add credentials for the Internet SSL Mailbox Target:

1. Click on **No usernames or passwords**.



2. In the **Search target credentials** dialog box, click **+ Add** and select **Secure Internet Mailbox (IMAPS)**.
3. Fill in the fields:

- **Target location**: Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.

**Note:** Check with your email service provider for information on what to enter as the IMAP/S target <domain>. For example, to scan Gmail with IMAP/S, enter `imap.gmail.com` as <domain>.

- **Username**: Enter the email address of the target mailbox. For example, `user@example.com`
- **Password**: Enter your mailbox password. If you have 2-factor authentication enabled, create an app password and enter it here.

#### Info: 2-factor authentication

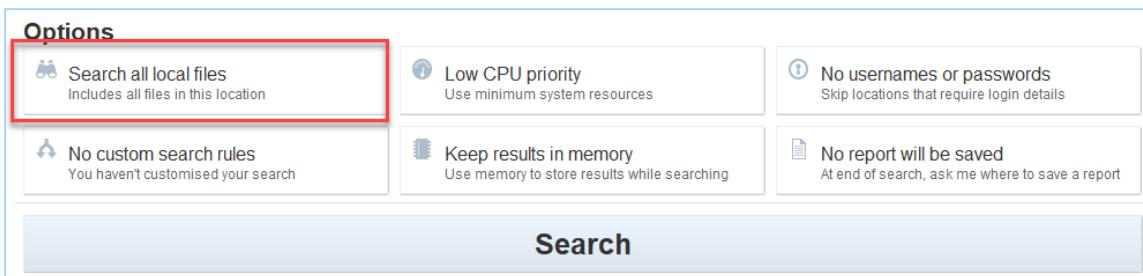
2-factor authentication is not supported. To access Internet SSL Mailbox accounts that require 2-factor authentication, you must set up an app password for use with **CARD RECON**. Create and use the app password instead of your account password.

4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

## ADD SEARCH LOCATION

Add an Internet SSL Mailbox account as a search location:

1. Click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and select **Email**.
  3. Select and expand **Internet SSL Mailbox**.
  4. Select the **Add imap host** field. Enter the target mailbox as <domain/email\_address>. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, enter `example.com/user@example.com`.
- Note:** Check with your email service provider for information on what to enter as the IMAP/S target <domain>. For example, to scan Gmail with IMAP/S, enter `imap.gmail.com` as <domain>.
5. Select the "Domain" Target that appears.
  6. (Optional) Select individual folders and emails to scan.
  7. Click **Select** to finish adding the Internet SSL Mailbox Target.

## LOTUS NOTES

### REQUIREMENTS

The Lotus Notes client must be installed on the host running **CARD RECON**. Scans works best with a single-user installation of the Lotus Notes client.

You must use the 32-bit version of **CARD RECON**.

Supported Lotus Notes clients:

- Lotus Notes client 8.5.3
- Lotus Notes client 9.0.1

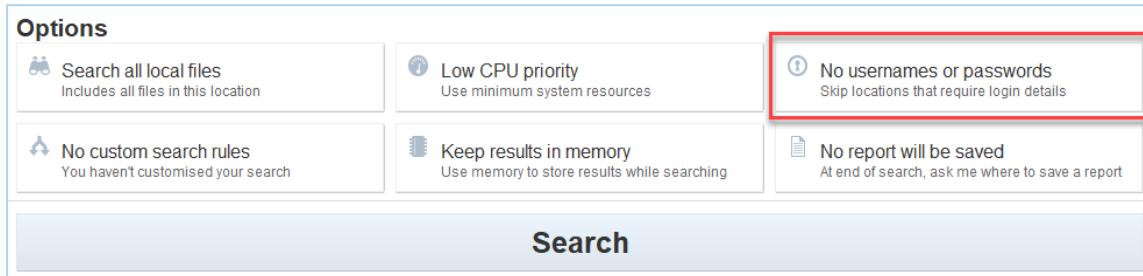
To see which versions of Lotus Domino these clients support, see the following links:

- [IBM Support: Supported configurations for Notes/Domino 8.0.x and 8.5.x](#)
- [IBM Support: Supported configurations for IBM Notes and Domino 9.x](#)

## ADD CREDENTIALS

Add credentials for the Lotus Notes Target:

1. Click on **No usernames or passwords**.

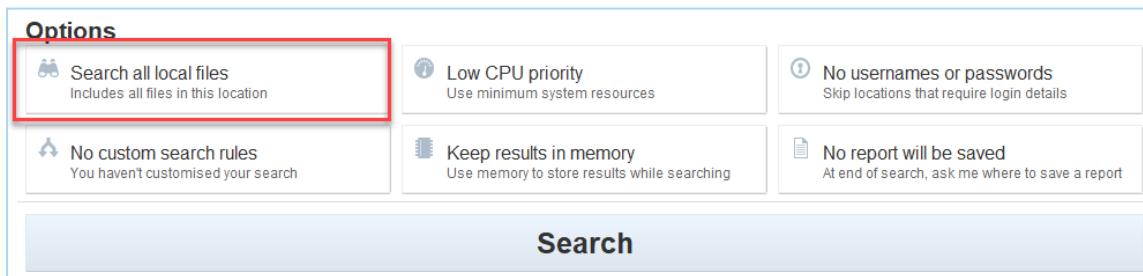


2. In the **Search target credentials** dialog box, click **+ Add** and select **Lotus Notes**.
3. Fill in the fields:
  - Target location:** Enter the Lotus Domino server domain name.
  - Username:** Enter a Lotus Notes User Name to scan that user's mailbox. This should be in the format <User\_name/lotus\_domain>. See [Lotus Notes User Name \(page 68\)](#) for more information.
  - Password:** Enter the user's password.
4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

## ADD SEARCH LOCATION

Add a Lotus Notes account as a search location:

1. Click on **Search all local files**.



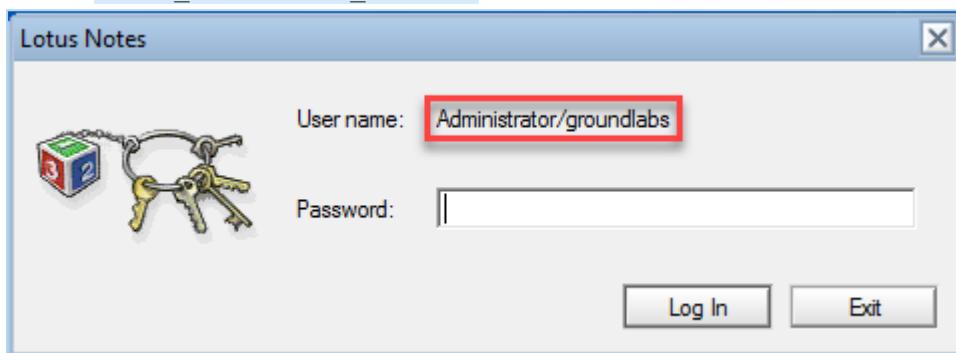
2. In the **Search targets** dialog box, click **+ Add** and select **Email**.
3. Select and expand **Lotus Notes**.
4. Enter your Lotus Domino server domain and press enter.
5. Select the "Domain" Target that appears below.

6. (Optional) Select individual folders and emails to scan.
7. Click **Select** to finish adding the Lotus Notes Target.

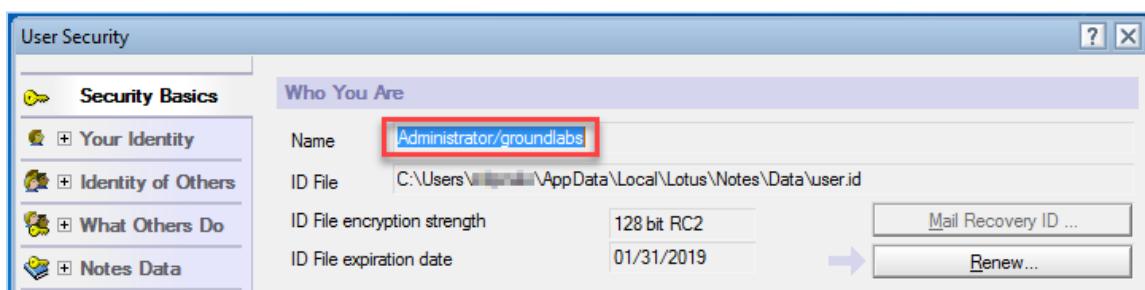
## LOTUS NOTES USER NAME

To find your Lotus Notes user name:

1. Open the Lotus Notes client.
2. From the menu bar, select **File > Security > User Security**.
3. A password prompt opens. In the prompt, your Lotus Notes user name is displayed in the format `<User_name/lotus_domain>`.



4. If no password prompt opens, find your Lotus Notes user name in the **User Security** screen.



## LOCALLY STORED EMAIL DATA

(Not recommended) You can scan locally stored email data by running a [Local Storage \(page 49\)](#) scan on the data storage files for that particular email client or server.

Scanning locally stored email data instead of running an Internet Mailbox scan runs the risk of finding false positives in places not accessible through querying the email server itself, such as ghost records or slack space.

## SCANNING INFORMATION STORES

Email servers store data in information stores that can be accessed when performing a [Local Storage \(page 49\)](#) scan. For instance, Microsoft Exchange servers store data in Microsoft

Exchange Information Store files (EDB and STM files). Do not run a scan on an information store currently in use by an email server. Instead:

1. Make a backup of the information store files.
2. Run a [Local Storage \(page 49\)](#) scan on the backup information store files.

**Note: Remediate matches found in Information Stores**

Remediation is limited for matches found in information stores, as modifying an information store may cause irreversible loss of data. For Microsoft Exchange Information Stores, the following remediation options are disabled:

- Mask matches
- Deleting individual matches (attempting to delete matches will permanently erase the Microsoft Exchange Information Store file being remediated)

# WEBSITES

**CARD RECON** can crawl the contents of a given website to search for sensitive data. **CARD RECON** can scan public-facing websites, intranets, and other web-based content that can be accessed via a HTTP or HTTPS URL.

To search a website:

1. Locate the "Websites" tab on the "Add search locations" dialog.
2. Enter the URL that you wish to scan.
3. Click **Select**

**Note:** If the URL that you wish to scan is a HTTPS URL, then you are attempting to scan an "SSL Web site". Enter the URL of the domain that you wish to scan in the appropriate field.

If you need credentials to access restricted parts of the website:

1. Open the "Search target credentials" dialog.
2. Click **+Add** and select the "Website (HTTPS)" or "Website (HTTP)" option, whichever is appropriate.
3. Enter your credentials. Click **Ok** to save your credentials.

## WEBSITE SEARCH OPTIONS

**CARD RECON** allows you to modify your website searches:

### MAXIMUM SEARCH DEPTH

The "maximum search depth" limits the link-depth that **CARD RECON** will search. Link-depth is the number of links or clicks a given web page is away from a given URL.

Setting a maximum search depth prevents **CARD RECON** from endlessly crawling links on the given website.

### FOLLOW EXTERNAL WEBSITE INKS

Allows you to add external website links that the licensed domain links to, but does not reside in the licensed domain.

# CLOUD STORAGE

---

You can add the following cloud storage Target types to CARD RECON:

- [Amazon S3 \(page 72\)](#)
- [Azure Storage \(page 93\)](#)
- [Box \(page 79\)](#)
- [Dropbox \(page 81\)](#)
- [Google Apps \(page 83\)](#)
- [OneDrive \(page 91\)](#)
- [Rackspace Cloud \(page 76\)](#)

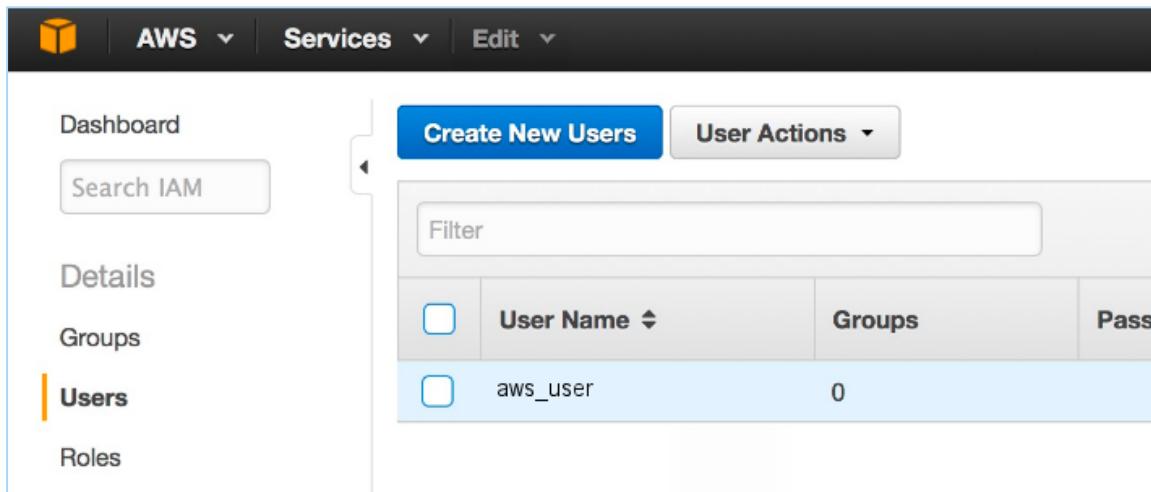
# AMAZON S3

To add Amazon S3 as a cloud Target:

1. [Get AWS User Security Credentials \(page 72\)](#)
2. [Add Credentials \(page 73\)](#)
3. [Add Target \(page 74\)](#)

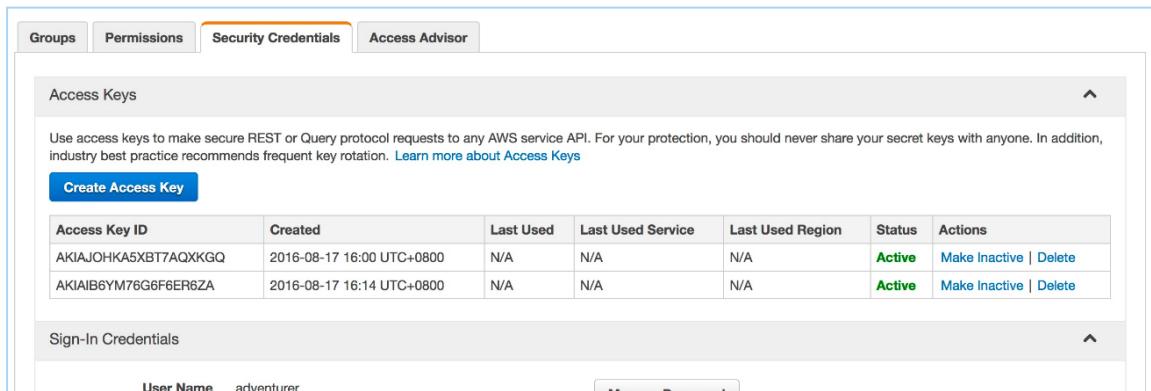
## GET AWS USER SECURITY CREDENTIALS

1. Log into the [AWS IAM console](#).
2. On the left of the page, click **Users** and select an IAM user with full access to the Target Amazon S3 Bucket.



The screenshot shows the AWS IAM service interface. In the top navigation bar, 'AWS' and 'Services' are visible. On the left sidebar, 'Dashboard', 'Search IAM', 'Details', 'Groups', and 'Users' are listed; 'Users' is currently selected and highlighted with an orange border. In the main content area, there is a 'Create New Users' button and a 'User Actions' dropdown. Below these are two tabs: 'Filter' and 'User Name'. A table lists one user: 'aws\_user' with '0' groups. The 'aws\_user' row is highlighted with a light blue background.

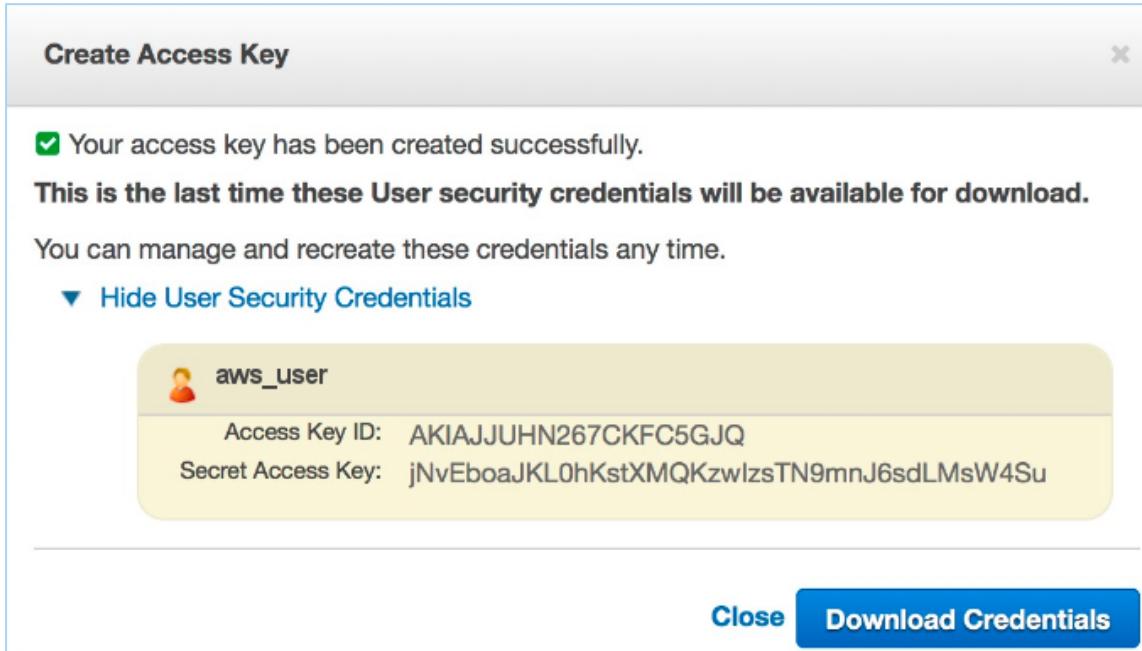
3. On the **User** page, click on the **Security Credentials** tab. The tab displays the user's existing Access Keys.



The screenshot shows the 'Security Credentials' tab for the 'aws\_user' user. At the top, there are tabs for 'Groups', 'Permissions', 'Security Credentials' (which is active and highlighted in orange), and 'Access Advisor'. Below the tabs, there is a section titled 'Access Keys' with a sub-instruction: 'Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation.' A 'Create Access Key' button is present. A table lists two access keys: 'AKIAJOHKA5XBT7AQXKGQ' and 'AKIAIB6YM76G6F6ER6ZA', both of which are marked as 'Active'. At the bottom, there is a 'Sign-In Credentials' section and a note about managing password.

4. Click **Create Access Key**. A dialog box appears, displaying a new set of User security credentials. This consists of an **Access Key ID** and a **Secret Access Key**.

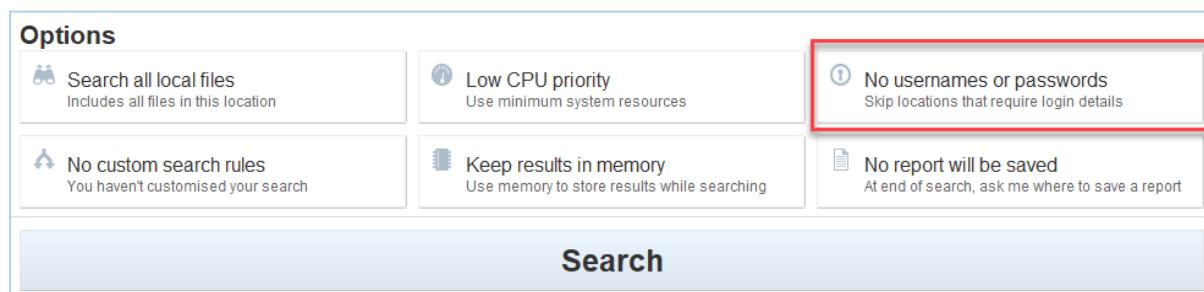
- Click **Download Credentials** to save the User security credentials in a secure location, or write it down in a safe place. You cannot access this set of credentials once the dialog box is closed.



**Note:** Save your new Access Key set. Once this window is closed, you cannot access this Secret Access Key.

## ADD CREDENTIALS

In the main menu, click on **No usernames or passwords**:



In the **Search target credentials** dialog box:

1. Click + Add and select one of the following:

**Note:** Use Amazon S3 (HTTPS) credentials for Amazon S3 (SSL) Bucket Targets.

- (Recommended) **Amazon S3 (HTTPS)**
- **Amazon S3 (HTTP)**

2. Fill in the following fields:

- **Target location:** Enter the Amazon S3 Bucket name.
- **Username:** Enter the Access Key ID obtained in [Get AWS User Security Credentials \(page 72\)](#)
- **Password:** Enter the Secret Access Key obtained in [Get AWS User Security Credentials \(page 72\)](#)

3. (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.

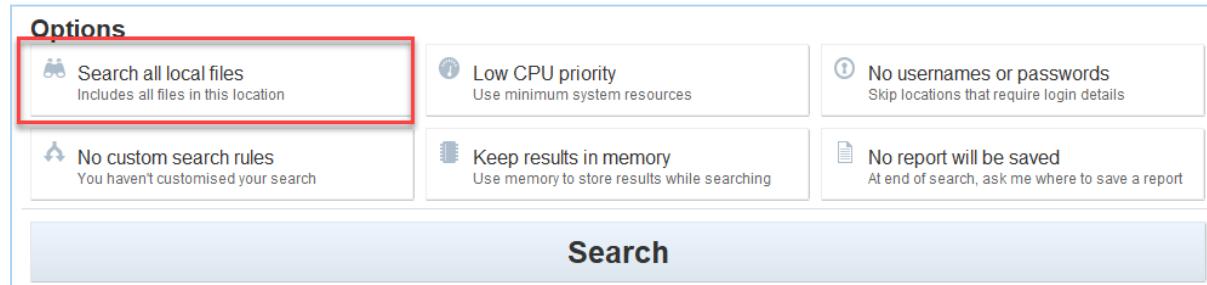
**Tip:** Credentials are only saved if:

- Search configuration is saved. See [Save and Load Options \(page 109\)](#) for more information.
- The results database is saved. See [Setting Results Database Options \(page 104\)](#) for more information.

4. Click Ok.

## ADD TARGET

In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click + Add.
2. Select Cloud Storage.

3. Select one of the following and click + to expand the selection:
    - (Recommended) **Amazon S3 (SSL) Bucket**
- Note:** To scan Amazon S3 Buckets secured with AWS KMS, you must use the **Amazon S3 (SSL) Bucket** Target type.
- **Amazon S3 Bucket**
4. In the Add S3 storage bucket field, enter the Bucket name.
  5. Press **Enter** to add the specified Amazon S3 Bucket as a Target.
  6. (Optional) Click + to expand the added Target and select specific objects to scan.
  7. Click **Select** and then **Ok** to finish adding the Target.

# RACKSPACE CLOUD

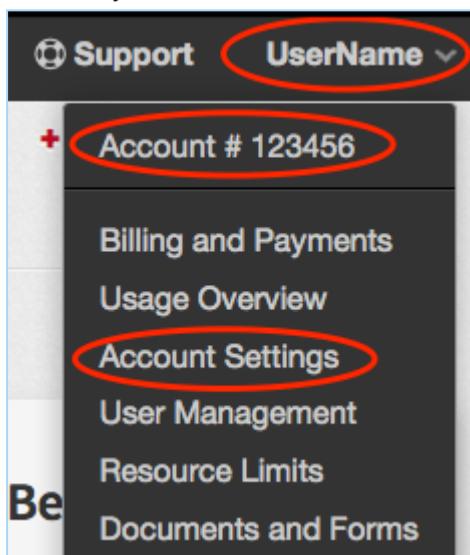
Support for Rackspace services is currently limited to Cloud File Storage only.

To add Rackspace Cloud File Storage as a cloud Target:

1. [Get Rackspace API key \(page 76\)](#)
2. [Add Credentials \(page 76\)](#)
3. [Add Target \(page 77\)](#)

## GET RACKSPACE API KEY

1. Log into your Rackspace account.
2. Click on your **Username**, and then click **Account Settings**.



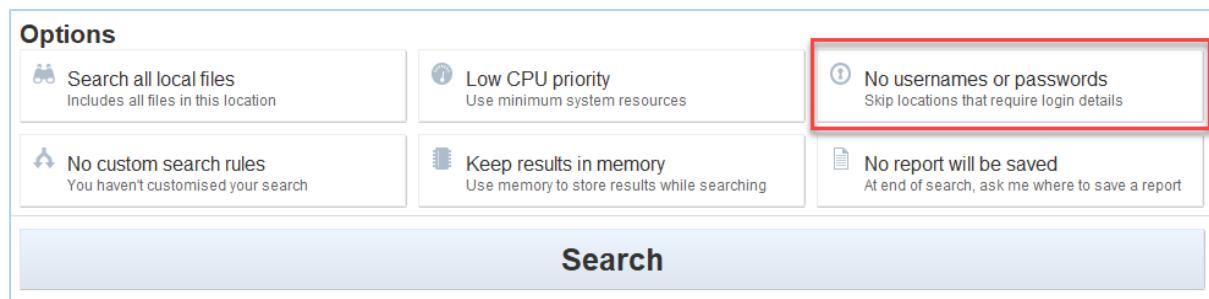
3. In the Account Settings page, go to **API Key** and click **Show**.

Email Address	<input type="text" value="support@rackspace.com"/>	
Security Question	What is the location of a dream vacation?	
API Key	<input type="text" value="....."/>	

4. Write down your Rackspace account **API Key**.

## ADD CREDENTIALS

In the main menu, click on **No usernames or passwords**:



In the **Search target credentials** dialog box:

1. Click + Add and select **Rackspace Cloud Files (HTTPS)**.
2. Fill in the following fields:
  - **Target location**: Enter the Rackspace account name.
  - **Username**: Enter the Rackspace account name.
  - **Password**: Enter the API key obtained in [Get Rackspace API key \(page 76\)](#).
3. (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.

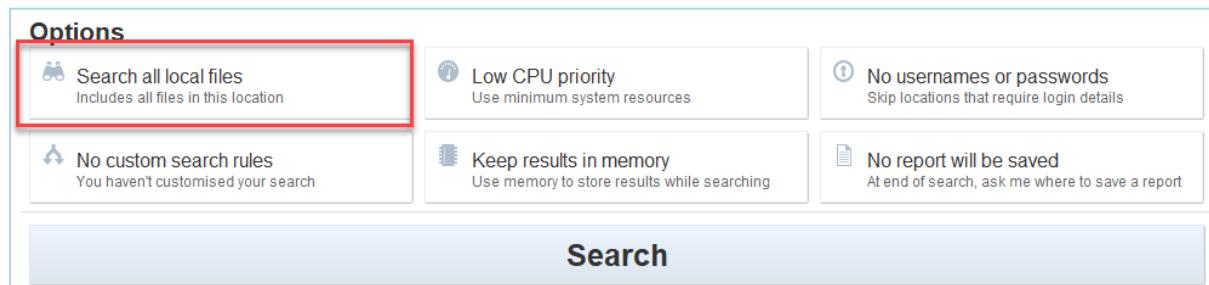
**Tip:** Credentials are only saved if:

- Search configuration is saved. See [Save and Load Options \(page 109\)](#) for more information.
- The results database is saved. See [Setting Results Database Options \(page 104\)](#) for more information.

4. Click Ok.

## ADD TARGET

In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click **+ Add**.
2. Select **Cloud Storage**.
3. Select **Rackspace Cloud Files** and click **+** to expand the selection.
4. In the **Add Rackspace Account Name** field, enter the Rackspace account name.
5. Press **Enter** to add the specified Rackspace account as a Target.
6. (Optional) Click **+** to expand the added Target and select specific objects to scan.
7. Click **Select** and then **Ok** to finish adding the Target.

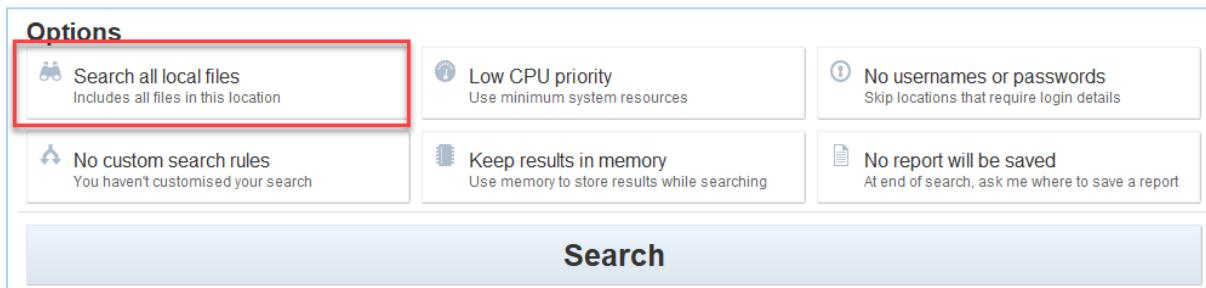
# BOX

To add Box as a cloud Target:

- [Add Target \(page 79\)](#)
- [Obtain Access Code \(page 80\)](#)
- [Finish Adding Target \(page 80\)](#)

## ADD TARGET

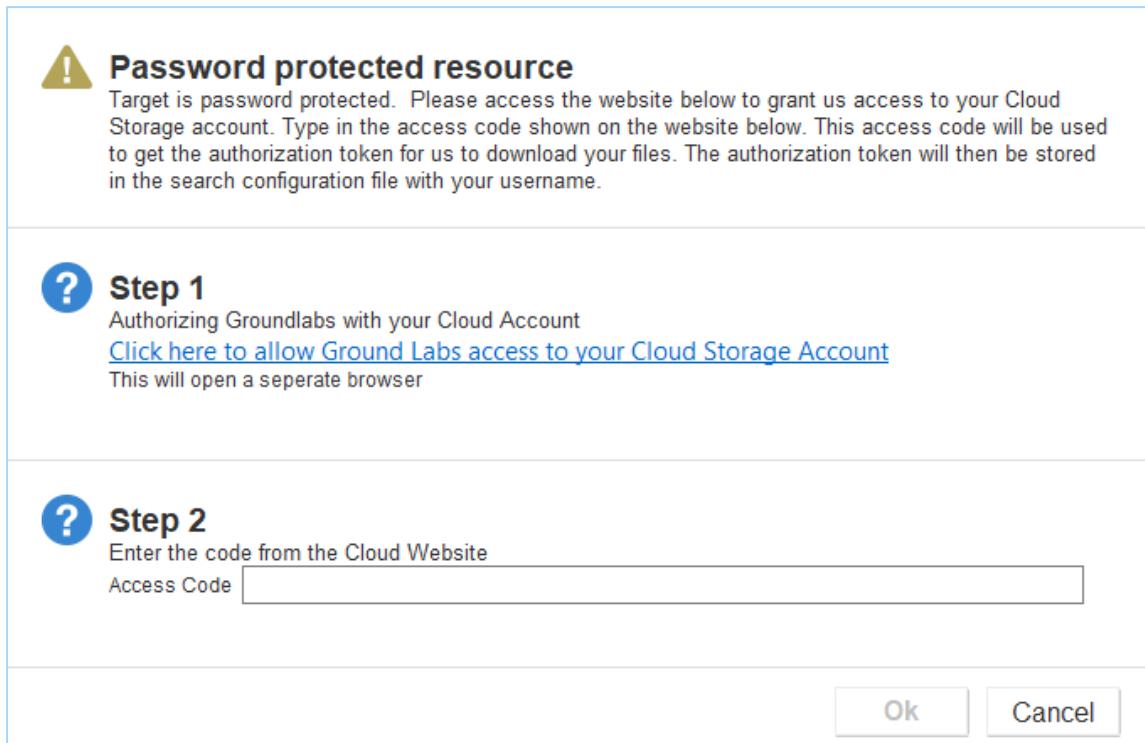
In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click **+ Add**.
2. Select **Cloud Storage**.
3. Select **Box.Net Location** and click **+** to expand the selection.
4. In the **Add Box Account Name** field, enter the Box account name.
5. Press **Enter** to add the specified Box account as a Target.

6. Click + to bring up the **Password protected resource** dialog box.



## OBTAI ACCESS CODE

In the **Password protected resource** dialog box:

1. Under **Step 1**, click on **Click here to allow Ground Labs access to your Cloud Storage Account** to open a browser window.
2. Follow the on-screen instructions to give **CARD RECON** permissions to access files on your cloud storage service and obtain an **OAuth Access Code**.
3. In **CARD RECON**, enter the **Access Code** under **Step 2**.
4. Click **Ok** to close the **Password protected resource** dialog box.

**CARD RECON** will display the contents of your cloud storage account in the list of Targets in the **Add search locations** dialog box.

## FINISH ADDING TARGET

1. (Optional) In the expanded contents of the cloud Target, select specific objects to scan.
2. Click **Select** and then **Ok** to finish adding the Target.

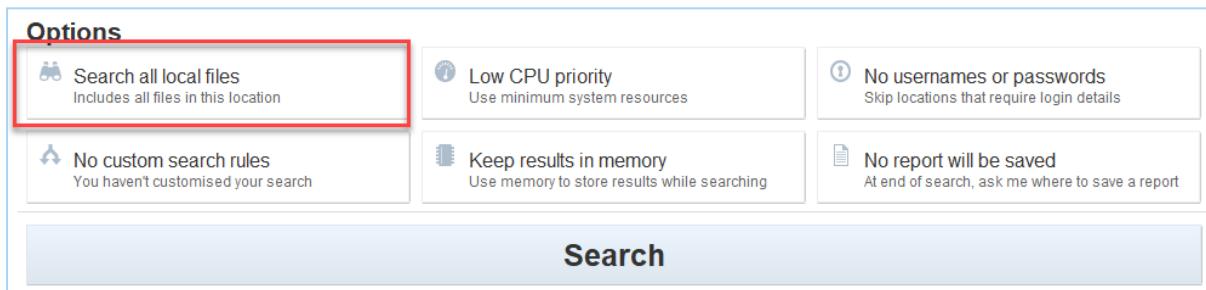
# DROPBOX

To add Dropbox as a cloud Target:

- [Add Target \(page 81\)](#)
- [Obtain Access Code \(page 82\)](#)
- [Finish Adding Target \(page 82\)](#)

## ADD TARGET

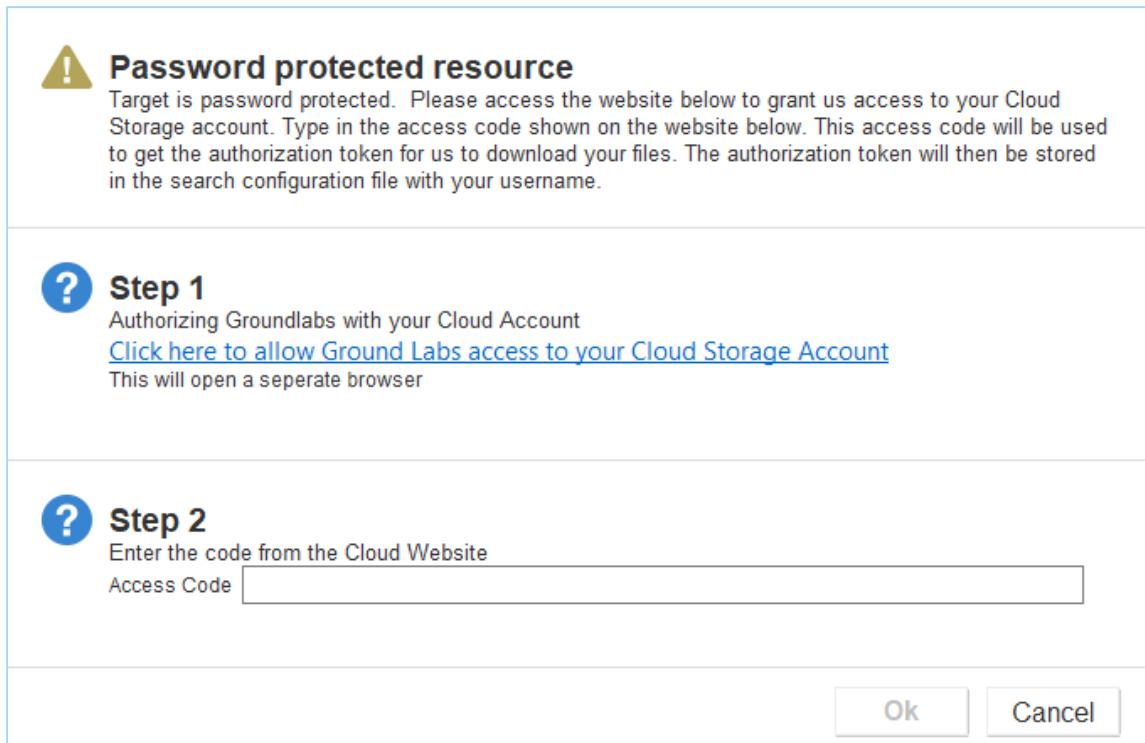
In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click **+ Add**.
2. Select **Cloud Storage**.
3. Select **Dropbox Location** and click **+** to expand the selection.
4. In the **Add Dropbox Account Name** field, enter the Dropbox account name.
5. Press **Enter** to add the specified Dropbox account as a Target.

6. Click + to bring up the **Password protected resource** dialog box.



## OBTAI ACCESS CODE

In the **Password protected resource** dialog box:

1. Under **Step 1**, click on **Click here to allow Ground Labs access to your Cloud Storage Account** to open a browser window.
2. Follow the on-screen instructions to give **CARD RECON** permissions to access files on your cloud storage service and obtain an **OAuth Access Code**.
3. In **CARD RECON**, enter the **Access Code** under **Step 2**.
4. Click **Ok** to close the **Password protected resource** dialog box.

**CARD RECON** will display the contents of your cloud storage account in the list of Targets in the **Add search locations** dialog box.

## FINISH ADDING TARGET

1. (Optional) In the expanded contents of the cloud Target, select specific objects to scan.
2. Click **Select** and then **Ok** to finish adding the Target.

# GOOGLE APPS

The instructions here work for setting up the following Google Apps products as Targets:

- Google Docs
- Google Tasks
- Google Calendars

To add Google Apps as cloud Targets:

1. [Configure Google Apps Account \(page 83\)](#)
2. [Add Credentials \(page 89\)](#)
3. [Add Target \(page 90\)](#)

## CONFIGURE GOOGLE APPS ACCOUNT

Before you add Google Apps products as Targets, you must have:

- A Google Apps administrator account for the Target Google Apps domain.
- The Target must be a Google Apps account. Personal Google accounts are not supported.

**Info:** Setting up a Google Apps account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using CARD RECON.

To set up a Google Apps account for scanning, you must:

1. [Select a project \(page 83\)](#)
2. [Enable APIs \(page 84\)](#)
3. [Create a Service Account \(page 85\)](#)
4. [Set up Domain-Wide Delegation \(page 86\)](#)

### SELECT A PROJECT

1. Log into the [Google Developers console](#).
2. Click on **Select a project ▼**. The **Select** dialog box opens and displays a list of existing projects.

In the **Select** dialog box, you can:

- Select an existing project.
- (Recommended) Create a new project.

The screenshot shows a 'Select' dialog box with a search bar at the top. Below the search bar are two tabs: 'Recent' (which is selected) and 'All'. A list of projects follows, each with a name, ID, and a small icon. The project 'adventure' is selected, indicated by a blue checkmark next to its name.

Name	ID
✓ adventure	adventure-140700
gdrive	14-140700

To select an existing project:

1. Click on a project.
2. Click **OPEN**.

To create a new project:

1. Click on **+**.
2. In the **New Project** page, enter your **Project name** and click **Create**.

## ENABLE APIs

To scan a specific Google Apps product, enable the API for that product in your project.

To enable Google Apps APIs:

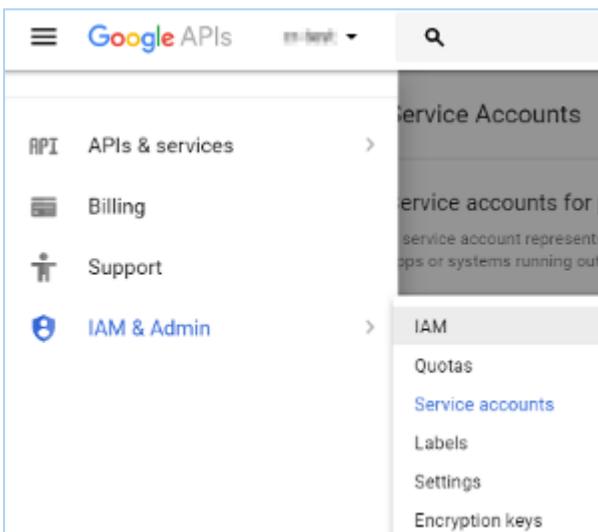
1. [Select a project \(page 83\)](#).
2. In the project Dashboard, click **+ ENABLE APIs AND SERVICES**. This displays the API Library.
3. Enable the **Admin SDK API**.
  - a. Under G Suite APIs, click **Admin SDK**.
  - b. Click **ENABLE**.
4. Repeat to enable the following APIs:

Target Google Apps Product	API Library
Google Docs	Google Drive API
Google Tasks	Tasks API
Google Calendar	Google Calendar API

## CREATE A SERVICE ACCOUNT

Create a service account for CARD RECON:

1. Click on the  menu on the upper-left corner of the [Google Developers Console](#).
2. Go to **IAM & Admin > Service accounts.**



3. Click **+ CREATE SERVICE ACCOUNT**.

 **CREATE SERVICE ACCOUNT**

4. In the **Create service account** dialog box, enter the following:

Field	Description
Service account name	Enter a descriptive label.
Role	Select <b>Project &gt; Owner</b> .
Service account ID:	Enter a name for your service account, or click the refresh button to generate a service account ID. An example service account ID: <code>service-account-634@project_name-1272.iam.gserviceaccount.com</code>
Furnish a new private	1. Select <b>Furnish a new private key</b> .

Field	Description
key	2. Select P12.
Enable G Suite Domain-wide Delegation	Select <b>Enable G Suite Domain-wide Delegation</b> .

**Note:** If prompted, enter a product name for the OAuth consent screen and save your OAuth consent screen settings. The product name should describe your project. For example: "CARD RECON".

5. Click **CREATE**. The **Service account and key created** dialog box displays, and a P12 key is saved to your computer. Keep the P12 key in a secure location.

**Info:** The dialog box displays the private key's password: `notasecret`. **CARD RECON** does not need you to remember this password.

6. Click **Close**.
7. Write down the newly created service account's **Service account ID** and **Key ID**.

## SET UP DOMAIN-WIDE DELEGATION

**Note:** Set up domain-wide delegation with the administrator account used in [Enable APIs \(page 84\)](#).

The following is a guide for setting up domain-wide delegation for existing service accounts.

To allow **CARD RECON** to access your Google Apps domain with the Service Account, you must set up and enable domain-wide delegation for your Service Account.

To set up domain-wide delegation:

1. In the [Google Developer's Console](#), click on the  menu.
2. Go to **API Manager > Credentials**.
3. On the **Credentials** page, under **OAuth 2.0 client IDs**, go to the entry for your service account and take note of the **Client ID**.

Credentials

Credentials OAuth consent screen Domain verification

Create credentials  Delete

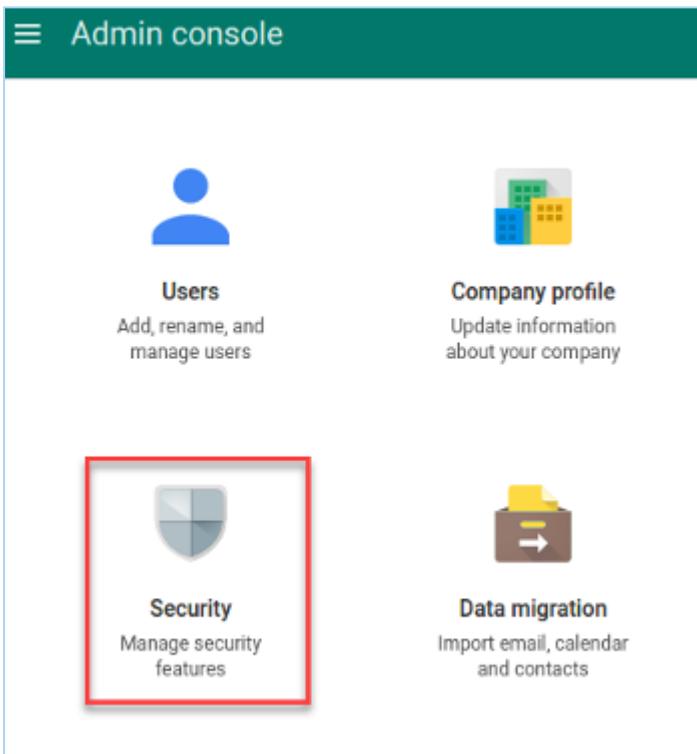
Create credentials to access your enabled APIs. Refer to the API documentation for details.

OAuth 2.0 client IDs

<input type="checkbox"/> Name	Creation date	Type	Client ID
Client for service-account-name-14	19 Aug 2016	Service account client	116877825065678775170

**Note:** The Client ID is required when assigning DwD to your Service Account.

4. Go to the [Google Apps Admin console](#). In the **Admin Console**, click on **Security**.



5. On the **Security** page, click **Show more**.
6. Click on **Advanced settings** to expand it.
7. Under **Authentication**, click **Manage API client access**.

### ^ Advanced settings

#### Authentication

##### [Manage OAuth domain key](#)

Allows admins to access all user data without needing login credentials. [?](#)

##### [Manage API client access](#)

Allows admins to control access to user data by applications that use OAuth protocol.

8. In **Manage API client access**, enter:

- Client Name:** Your Service account Client ID (For example, [116877825065678775170](#)).
- One or More API Scopes:** For each Google Apps product that you wish to scan, you must apply a different API Scope.

The following is a list of API Scopes required for CARD RECON to work with each Google Apps service:

Google Apps service	API Scope
All (required)	<a href="https://www.googleapis.com/auth/admin.directory.user.readonly">https://www.googleapis.com/auth/admin.directory.user.readonly</a>
Google Docs	<a href="https://www.googleapis.com/auth/drive.readonly">https://www.googleapis.com/auth/drive.readonly</a>
Google Tasks	<a href="https://www.googleapis.com/auth/tasks.readonly">https://www.googleapis.com/auth/tasks.readonly</a>
Google Calendar	<a href="https://www.googleapis.com/auth/calendar.readonly">https://www.googleapis.com/auth/calendar.readonly</a>

**Info:** You can apply multiple API Scopes by separating them with commas. For example,

<https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.googleapis.com/auth/drive.readonly>

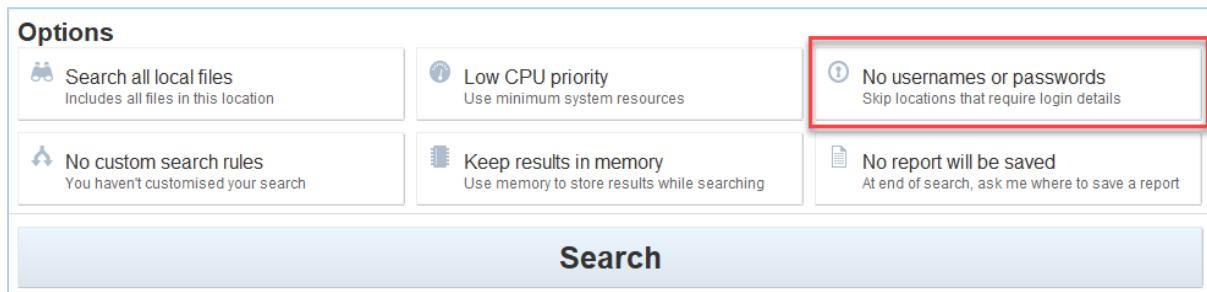
**Note: Copying and pasting**

Copying and pasting formatted text into **Manage API client access** may cause it to display an error. Instead, manually enter the API Scopes as shown above.

- c. Click **Authorize**.

## ADD CREDENTIALS

In the main menu, click on **No usernames or passwords**:



In the **Search target credentials** dialog box:

**Note:** You must add two credential sets per Google Apps Target. Follow the instructions below carefully.

1. Click **+ Add** and select one of the following Target types:
  - **Google Docs**
  - **Google Tasks**
  - **Google Calendars**
2. Fill in the following fields:
  - **Target location**: Enter the Google Apps domain.
  - **Username**: Enter a Google Apps domain administrator email address.

**Note:** Use the same administrator account used to [Enable APIs \(page 84\)](#) and [Set up Domain-Wide Delegation \(page 86\)](#).

  - **Password**: Leave blank.
3. Click **+ Add** again, and select the same Target type.
4. Fill in the following fields:
  - **Target location**: Enter the Google Apps domain used in step 2.
  - **Username**: Enter the service account name obtained in [Create a Service Account](#).
  - **Password**: Enter the file name of the P12 key obtained in [Create a Service Account \(page 85\)](#). The P12 key must be saved in the same folder as the **CARD RECON** executable.

- (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.

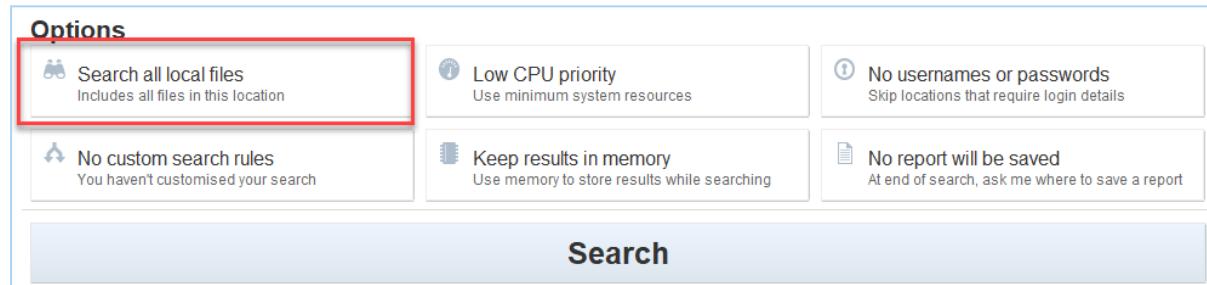
**Tip:** Credentials are only saved if:

- Search configuration is saved. See [Save and Load Options \(page 109\)](#) for more information.
- The results database is saved. See [Setting Results Database Options \(page 104\)](#) for more information.

- Click **Ok**.

## ADD TARGET

In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

- Click **+ Add**.
- Select **Cloud Storage**.
- Select one of the following and click **+** to expand the selection.:
  - Google Docs
  - Google Tasks
  - Google Calendars
- In the **Add Google Apps domain** field, enter the Google Apps domain name.

**Example:** If your Google Apps administrator email is `admin@domain.com`, your Google Apps domain is `domain.com`.

- Press **Enter** to add the specified Google Apps domain as a Target.
- (Optional) Click **+** to expand the added Target and select specific objects to scan.



- Click **Select** and then **Ok** to finish adding the Target.

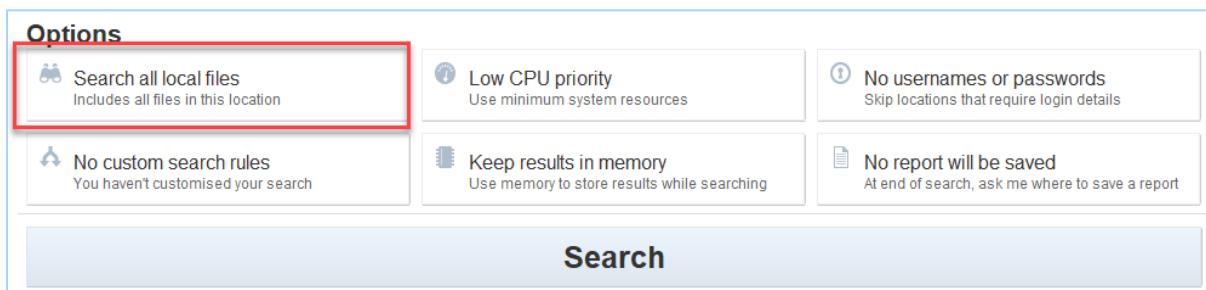
# ONEDRIVE

To add OneDrive as a cloud Target:

- [Add Target \(page 91\)](#)
- [Obtain Access Code \(page 92\)](#)
- [Finish Adding Target \(page 92\)](#)

## ADD TARGET

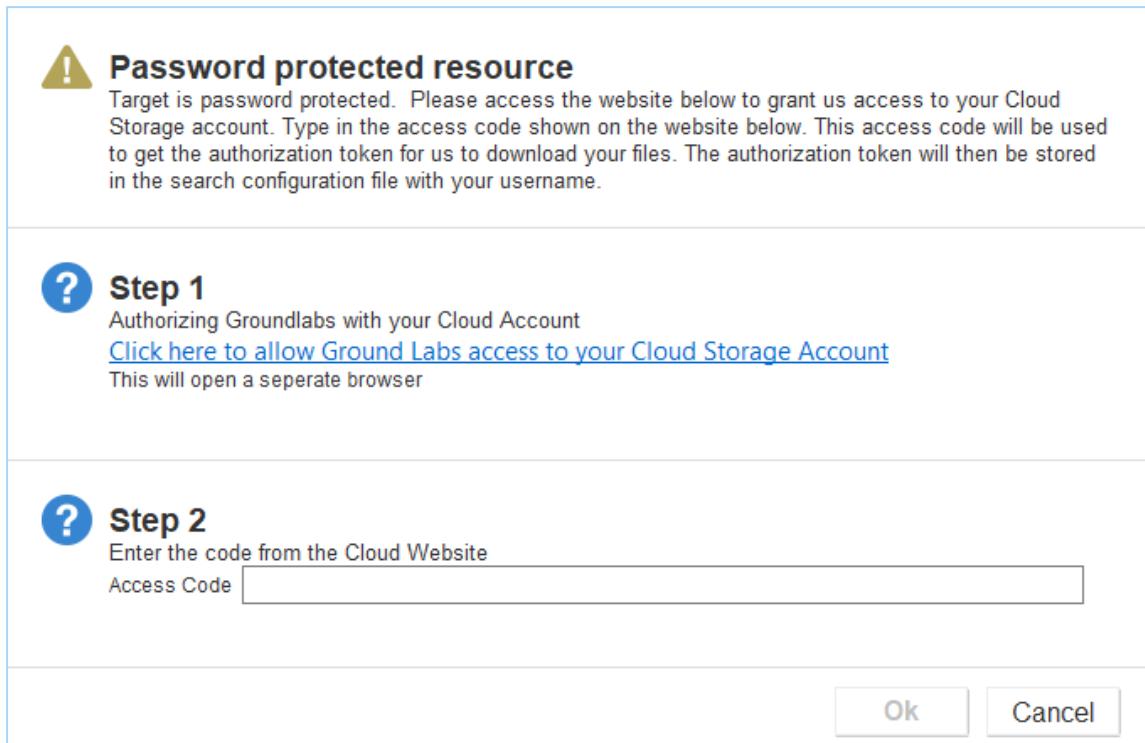
In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

1. Click **+ Add**.
2. Select **Cloud Storage**.
3. Select **OneDrive Location** and click **+** to expand the selection.
4. In the **Add OneDrive Account Name** field, enter the OneDrive account name.
5. Press **Enter** to add the specified OneDrive account as a Target.

6. Click + to bring up the **Password protected resource** dialog box.



## OBTAIACCESS CODE

In the **Password protected resource** dialog box:

1. Under **Step 1**, click on **Click here to allow Ground Labs access to your Cloud Storage Account** to open a browser window.
2. Follow the on-screen instructions to give **CARD RECON** permissions to access files on your cloud storage service and obtain an **OAuth Access Code**.
3. In **CARD RECON**, enter the **Access Code** under **Step 2**.
4. Click **Ok** to close the **Password protected resource** dialog box.

**CARD RECON** will display the contents of your cloud storage account in the list of Targets in the **Add search locations** dialog box.

## FINISH ADDING TARGET

1. (Optional) In the expanded contents of the cloud Target, select specific objects to scan.
2. Click **Select** and then **Ok** to finish adding the Target.

# AZURE STORAGE

The following instructions apply to:

- Azure Blobs
- Azure Queues
- Azure Tables

To add an Azure Storage account as a cloud Target:

1. [Get Azure Account Access keys \(page 93\)](#)
2. [Add Credentials \(page 93\)](#)
3. [Add Target \(page 94\)](#)

## GET AZURE ACCOUNT ACCESS KEYS

1. Log into your **Azure** account
2. Go to **Storage accounts > [storage-account-name] > Access keys.**

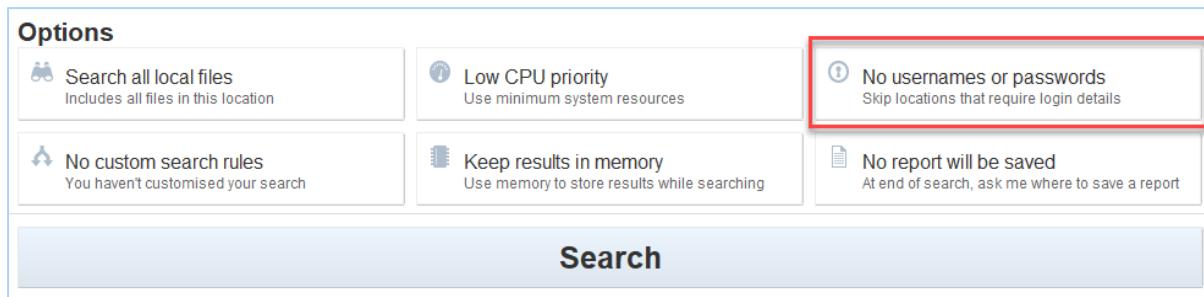
NAME	KEY
key1	jibfohktfln7eW37hBZVvpc6rU2f7Kta3nX/6LENVCRqQbsOTQfIC
key2	s6M85uEtzfppe3AfM/LX50PnGKSek1DBfDVEBClarpxOU5906cLi

3. Note down **key1** and **key2** which are your primary and secondary access keys respectively. Use the active access key to connect CR to your Azure Storage account.

**Info:** Only one access key can be active at a time. The primary and secondary access keys are used to make rolling key changes. Ask your Azure Storage account administrator which access key is currently active, and use that key with CR.

## ADD CREDENTIALS

In the main menu, click on **No usernames or passwords:**



In the **Search target credentials** dialog box:

1. Click **+ Add** and select one of the following:

**Note:** Use **Azure (HTTPS)** credentials for **Azure (SSL)** Targets.

- (Recommended) **Azure Blobs (HTTPS)**
- **Azure Blobs (HTTP)**
- (Recommended) **Azure (SSL) Queues (HTTPS)**
- **Azure Queues (HTTP)**
- (Recommended) **Azure (SSL) Tables (HTTPS)**
- **Azure Tables (HTTP)**

2. Fill in the following fields:

- **Target location:** Enter the Azure Storage account name.
- **Username:** Enter the Azure Storage account name.
- **Password:** Enter the Access Key obtained in [Get Azure Account Access keys \(page 93\)](#)

3. (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.

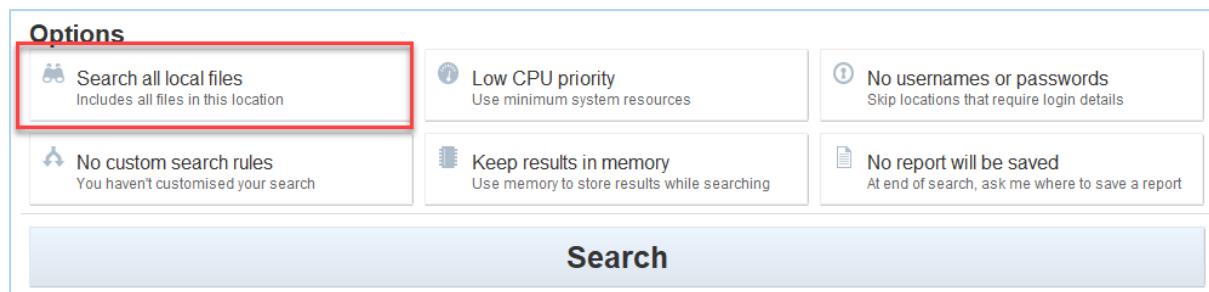
**Tip:** Credentials are only saved if:

- Search configuration is saved. See [Save and Load Options \(page 109\)](#) for more information.
- The results database is saved. See [Setting Results Database Options \(page 104\)](#) for more information.

4. Click **Ok**.

## ADD TARGET

In the main menu, click **Search all local files**:



In the **Search targets** dialog box:

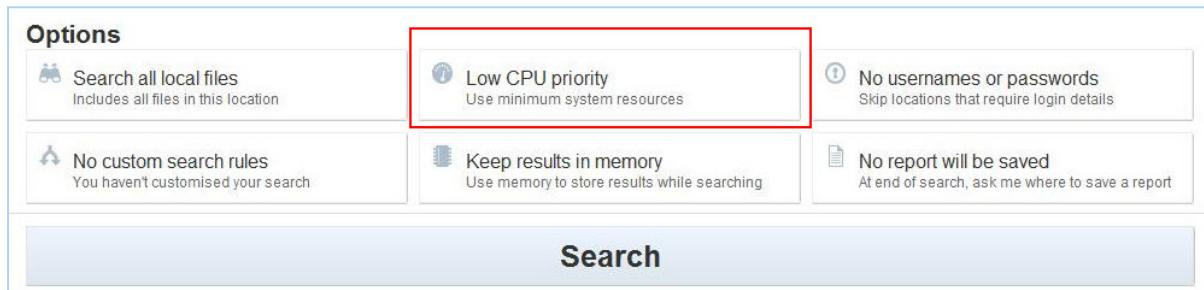
1. Click + Add.
2. Select **Cloud Storage**.
3. Select one of the following and click + to expand the selection:
  - (Recommended) **Azure (SSL) Blobs**
  - **Azure Blobs**
  - (Recommended) **Azure (SSL) Queues**
  - **Azure Queues**
  - (Recommended) **Azure (SSL) Tables**
  - **Azure Tables**
4. In the **Add Azure Storage Account Name** field, enter the Azure storage account name.
5. Press **Enter** to add the specified Azure Storage account as a Target.
6. (Optional) Click + to expand the added Target and select specific objects to scan.
7. Click **Select** and then **Ok** to finish adding the Target.

# SETTING RESOURCE USAGE

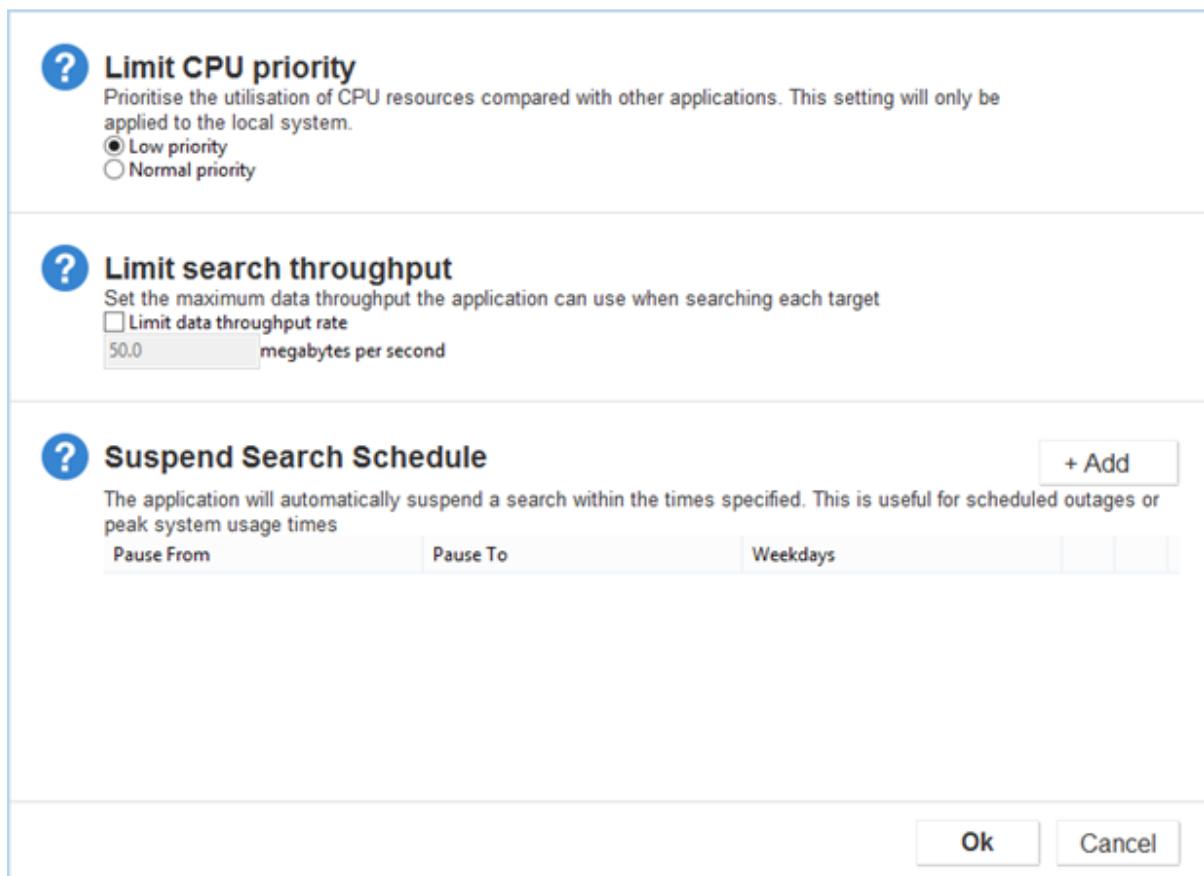
**CARD RECON** allows you to manage how resource intensive running its scans will be.

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 PRIORITY

**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 CREDENTIALS FOR RESTRICTED TARGETS

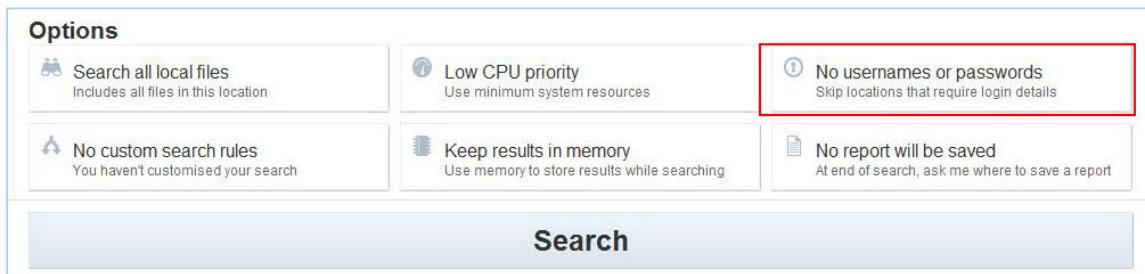
CARD RECON needs valid user credentials before it can scan certain TARGETS.

**Note:** See [Selecting Target Location \(page 47\)](#) for specific TARGET requirements.

## SEARCH TARGET CREDENTIALS

To set user credentials for restricted TARGETS:

1. Locate the button labeled "No usernames or passwords" on the CARD RECON GUI dashboard; clicking it will bring you to the "Search target credentials" dialog.



2. Click **+ Add** and select the TARGET type for which you would like to add user credentials for.
3. Fill the fields accordingly.

## ENCRYPT CREDENTIALS

Saving a configuration file or a results database will store your user credentials in the saved configuration or journal file. See [Setting Results Database Options \(page 104\)](#).

Adding a password here will encrypt the credentials saved in these files.

**?** **Search target credentials**

Enter login credentials for search targets that require authentication

Target Type	Target location	Username	Password

Show passwords

**?** **Encrypt credentials**

Add a master password to protect credentials using strong encryption (AES128). Credentials will only be stored if a configuration file or results database is saved.

<input type="password"/>
--------------------------

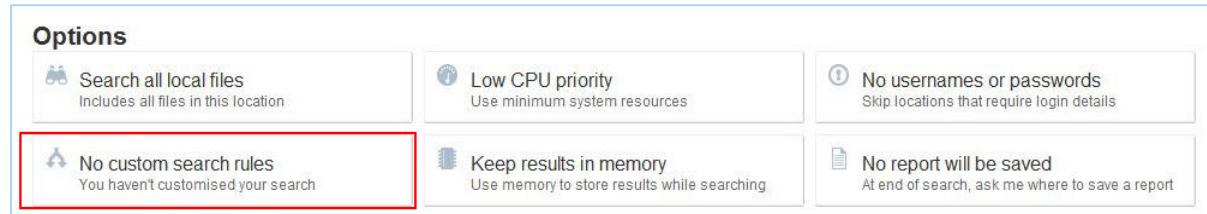
Show password

**Ok** **Cancel**

# 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
Enable OCR*	OCR (Optical Character Recognition) scans images and detects text data. Enabling this will tell <b>CARD RECON</b> to scan images for text data. This is a resource intensive feature.
Enable Voice Recognition	Enables voice recognition when scanning WAV and MP3 files. Voice recognition is a resource-heavy feature.  <b>Warning:</b> Support for voice recognition should be considered preliminary at this time.
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, <code>c:\windows\system32</code> will exclude all files and folders in the <code>c:\windows\system32</code> folder, and all the files and folders whose paths start with <code>c:\windows\system32</code> .
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. E.g. <code>led.jnl</code> will exclude all files and folders that end with the string <code>led.jnl</code> from the scan.

Search Filter Name	Usage						
Exclude locations by expression	<p>Excludes search locations by expression. The syntax of this expression is as follows:</p> <table border="1"> <thead> <tr> <th>Key</th><th>Function</th></tr> </thead> <tbody> <tr> <td>?</td><td>A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of a file or directory name, will also match zero characters.  E.g. <code>c:\v???</code> will match <code>c:\v123</code> and <code>c:\v1</code>, but will not match <code>c:\v1234</code>.</td></tr> <tr> <td>*</td><td>A wildcard character that <i>matches zero or more</i> characters in a search string.  <code>\*</code> matches all files in the directory. <code>\*.txt</code> matches all <code>txt</code> files in the directory.</td></tr> </tbody> </table>	Key	Function	?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of a file or directory name, will also match zero characters.  E.g. <code>c:\v???</code> will match <code>c:\v123</code> and <code>c:\v1</code> , but will not match <code>c:\v1234</code> .	*	A wildcard character that <i>matches zero or more</i> characters in a search string.  <code>\*</code> matches all files in the directory. <code>\*.txt</code> matches all <code>txt</code> files in the directory.
Key	Function						
?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of a file or directory name, will also match zero characters.  E.g. <code>c:\v???</code> will match <code>c:\v123</code> and <code>c:\v1</code> , but will not match <code>c:\v1234</code> .						
*	A wildcard character that <i>matches zero or more</i> characters in a search string.  <code>\*</code> matches all files in the directory. <code>\*.txt</code> matches all <code>txt</code> files in the directory.						
Include locations within modification date	<p>Includes search locations that have been modified within a given range of dates.</p> <p><b>CARD RECON</b> 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.</p>						
Include locations modified recently	<p>Includes search locations that have been modified within a given number of days from the current date.</p> <p><b>CARD RECON</b> will prompt you to select the number of days within which a file is modified.</p> <p>E.g.: Setting the number of days to <code>14</code> will exclude files and folders that have been modified more than 14 days before the current date.</p>						
Exclude locations greater than filesize (MB)	Excludes files that are larger than a given file size (in MB).						
Ignore exact match	<p>Ignore matches that match a given string exactly.</p> <p>E.g.: Setting this to <code>4419123456781234</code> will ignore matches found during scans that match the given string <code>4419123456781234</code> exactly.</p>						
Ignore match by prefix	<p>Ignore matches that begin with a given string.</p> <p>E.g.: Setting this to <code>4419</code> will ignore matches found during scans that begin with <code>4419</code>.</p>						

Search Filter Name	Usage						
Ignore match by expression	<p>Ignore matches found during scans if they match a given expression.</p> <p>The syntax of this expression is as follows:</p> <table border="1"> <thead> <tr> <th>Key</th><th>Function</th></tr> </thead> <tbody> <tr> <td>?</td><td>A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of an expression, will also match zero characters.   <code>V???</code> will match <code>V123</code> and <code>V1</code>, but will not match <code>V1234</code>.</td></tr> <tr> <td>*</td><td>A wildcard character that <i>matches zero or more</i> characters in a search string. <ul style="list-style-type: none"> <li><code>*</code> will ignore all matches</li> <li><code>*123</code> matches all expressions that end with <code>123</code>.</li> <li><code>123*</code> matches all expressions that begin with <code>123</code>.</li> </ul> </td></tr> </tbody> </table>	Key	Function	?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of an expression, will also match zero characters.  <code>V???</code> will match <code>V123</code> and <code>V1</code> , but will not match <code>V1234</code> .	*	A wildcard character that <i>matches zero or more</i> characters in a search string. <ul style="list-style-type: none"> <li><code>*</code> will ignore all matches</li> <li><code>*123</code> matches all expressions that end with <code>123</code>.</li> <li><code>123*</code> matches all expressions that begin with <code>123</code>.</li> </ul>
Key	Function						
?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters. If placed at the end of an expression, will also match zero characters.  <code>V???</code> will match <code>V123</code> and <code>V1</code> , but will not match <code>V1234</code> .						
*	A wildcard character that <i>matches zero or more</i> characters in a search string. <ul style="list-style-type: none"> <li><code>*</code> will ignore all matches</li> <li><code>*123</code> matches all expressions that end with <code>123</code>.</li> <li><code>123*</code> matches all expressions that begin with <code>123</code>.</li> </ul>						
Add test data	<p>Report match as test data if it matches a given string exactly.</p> <p>E.g.: Setting this to <code>4419123456781234</code> will report matches found during scans that match the given string <code>4419123456781234</code> exactly as test data.</p>						
Add test data prefix	<p>Reports matches that begin with a given string as test data.</p> <p>E.g.: Setting this to <code>4419</code> will report matches found during scans that begin with <code>4419</code> as test data.</p>						
Add test data expression	<p>Report matches found during scans as test data if they match a given expression.</p> <p>The syntax of this expression is as follows:</p> <table border="1"> <thead> <tr> <th>Key</th><th>Function</th></tr> </thead> <tbody> <tr> <td>?</td><td>A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters.   If placed at the end of an expression, will also match zero characters.   <code>V???</code> will match <code>V123</code> and <code>V1</code>, but will not match <code>V1234</code>.</td></tr> <tr> <td>*</td><td>A wildcard character that <i>matches zero or more</i> characters in a search string.  <code>*</code> will ignore all matches  <code>*123</code> matches all expressions that end with <code>123</code>.  <code>123*</code> matches all expressions that begin with <code>123</code>.</td></tr> </tbody> </table>	Key	Function	?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters.  If placed at the end of an expression, will also match zero characters.  <code>V???</code> will match <code>V123</code> and <code>V1</code> , but will not match <code>V1234</code> .	*	A wildcard character that <i>matches zero or more</i> characters in a search string. <code>*</code> will ignore all matches <code>*123</code> matches all expressions that end with <code>123</code> . <code>123*</code> matches all expressions that begin with <code>123</code> .
Key	Function						
?	A wildcard character that matches <i>exactly one</i> character; <code>???</code> matches 3 characters.  If placed at the end of an expression, will also match zero characters.  <code>V???</code> will match <code>V123</code> and <code>V1</code> , but will not match <code>V1234</code> .						
*	A wildcard character that <i>matches zero or more</i> characters in a search string. <code>*</code> will ignore all matches <code>*123</code> matches all expressions that end with <code>123</code> . <code>123*</code> matches all expressions that begin with <code>123</code> .						
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.						

**Search Filter**    **Usage**  
**Name**

\*Requires CARD RECON Advanced Edition

# 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.

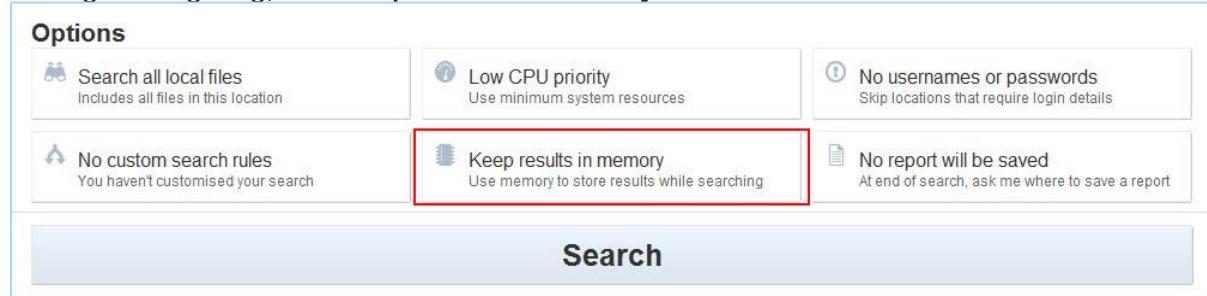
By default, this results database is stored in your system's memory. This means that when you close and re-open **CARD RECON**, your previous results database (and scan/remediation progress) will be lost.

**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 \(page 109\)](#).

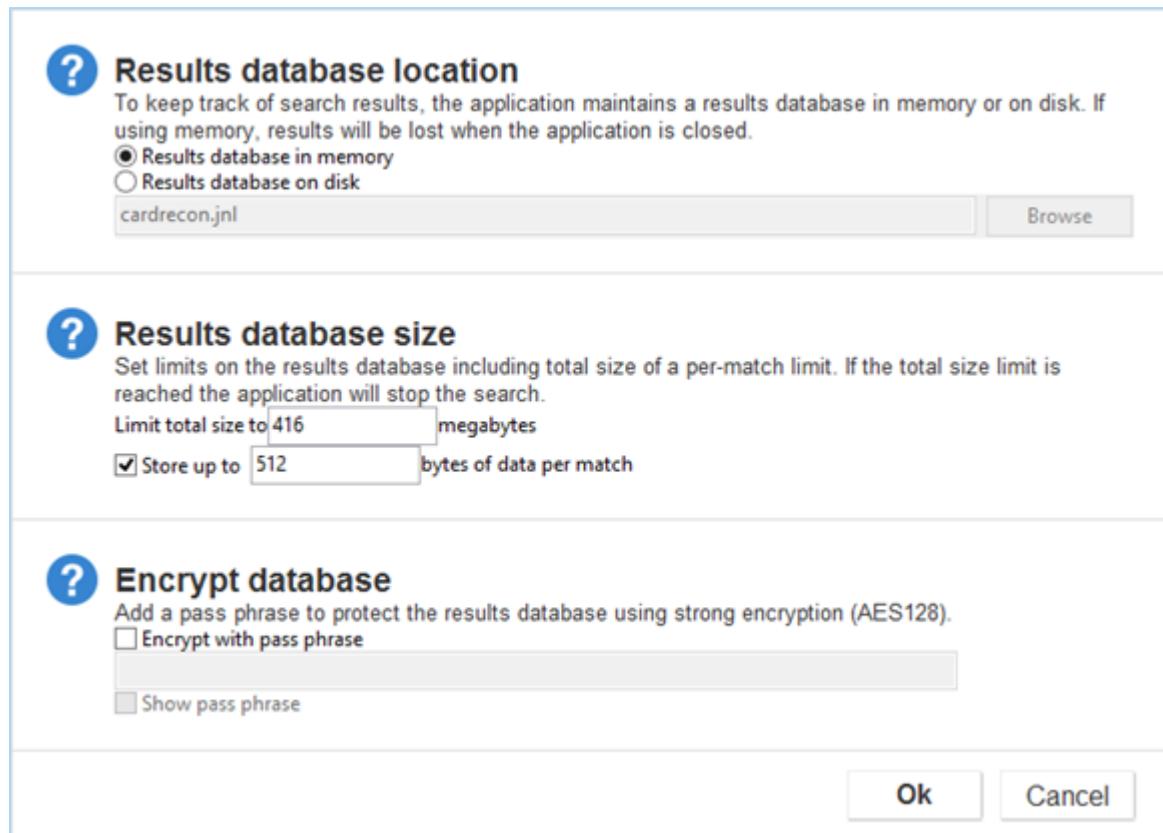
Configuring the how the results database is saved will allow you to:

- 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.

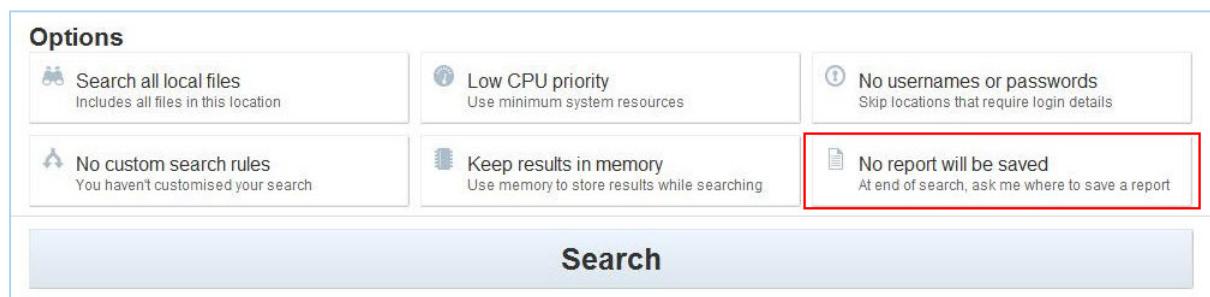
# SETTING COMPLIANCE REPORT SAVINGS OPTIONS

By default, compliance reports:

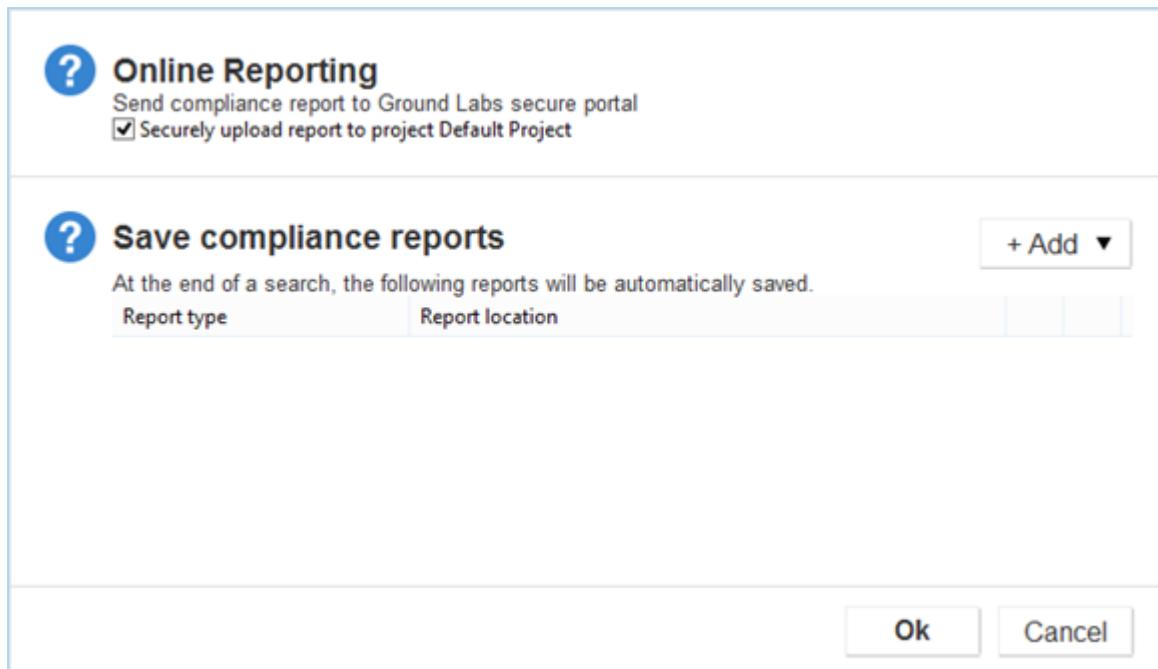
- Will not be saved.
- Will be securely uploaded to the [Ground Labs Services Portal](#).

See [Compliance Report \(page 19\)](#) for more information.

To configure how CARD RECON saves reports, click the button labeled "No report will be saved" on the dashboard.



The dialog for configuring how the compliance reports are saved displays.



## ONLINE REPORTING

By default, **CARD RECON** will attempt to upload the results of each scan to the [Ground Labs Services Portal](#) once the scan is complete.

To turn this off, clear 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:

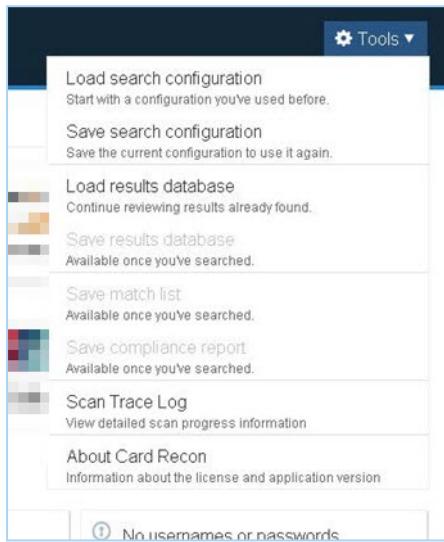
1. Click **+Add** to display a drop-down list of the report formats **CARD RECON** can use.
2. Select your preferred report format from the drop-down list.
3. Type the file path and file name where **CARD RECON** will save the compliance report.

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 DATABASES

**CARD RECON** uses database journal files (\*.jnl) to record scan and remediation progress. See [Setting Results Database Options \(page 104\)](#) 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).

# CARD RECON COMMAND-LINE INTERFACE

---

The CARD RECON Command-Line Interface (CLI) allows you to run CARD RECON on supported systems. For details, see [System Requirements \(page 4\)](#).

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 \(page 44\)](#).

**Info:** If you have no access to a Windows machine to run an instance of the CARD RECON GUI, you can set up a [Setting Up a Windows Virtual Machine \(page 116\)](#) 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](#).

Open the Command Prompt (on Windows) or Terminal (on UNIX-like platforms).

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

## 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  
cardrecon_2.0.xx.exe
```

In Terminal:

```
# Where <cardrecon_linux26_2.0.xx> is the file name of the  
CARD RECON executable  
chmod +x cardrecon_linux26_2.0.xx  
../cardrecon_linux26_2.0.xx
```

# CARD RECON CLI OPTIONS

Command Line Flags	Function
<code>-c, -config, -configuration &lt;path&gt;</code>	<p>Runs <b>CARD RECON</b> using a specified configuration file.</p> <p><b>Info:</b> This configuration file can be generated by the <b>CARD RECON GUI</b>. For details, see <a href="#">Configuring Scans for CARD RECON (page 43)</a>.</p>
<code>--export &lt;path&gt;</code>	<p>Sets the location where a list of matches will be saved. Export formats:</p> <ul style="list-style-type: none"> <li>• PDF</li> <li>• TXT</li> <li>• CSV</li> <li>• XML</li> </ul>
<code>-h, -help</code>	Displays all the command-line options available.
<code>-j, -journal &lt;file&gt;</code>	<p>Specify the location to save the database journal file.</p> <p>If specified database journal file exists, <b>CARD RECON</b> will load the file.</p> <p>See <a href="#">Save and Load Options (page 109)</a>.</p>
<code>-journal-overwrite</code>	Overwrite the database journal file specified with the <code>-journal</code> option if the database journal file already exists.
<code>-journal-resume</code>	<p>Use the data specified with the <code>-journal</code> option to recover and resume an interrupted search.</p> <p>Upon resuming, <b>CARD RECON</b> retries the location which was being searched at the time of interruption.</p>
<code>-journal-skip</code>	<p>Use the results database specified with the <code>-journal</code> option to recover and resume an interrupted search.</p> <p>Upon resuming, <b>CARD RECON</b> will skip the file which was being searched when the search was interrupted.</p>
<code>-l, -license &lt;path&gt;</code>	Sets the location of the OFFLINE LICENSE FILE. See <a href="#">Offline Licenses (page 30)</a> .
<code>-o, -output &lt;path&gt;</code>	<p>Sets the location where the compliance report will be saved. Output formats:</p> <ul style="list-style-type: none"> <li>• PDF.</li> <li>• TXT.</li> <li>• CSV.</li> <li>• CRR*.</li> </ul>

	<p><b>Info:</b> Multiple entries may be used to save several copies of the compliance report in different formats.</p>
-p, -password	Encrypt the saved database journal file; <b>CARD RECON</b> will prompt you to select a password.
-password- inline <password>	Encrypt the saved database journal file; user sets the password in-line, e.g.: <pre>./cardrecon_linux26_2.0.13 -j journalfile.jnl -password- inline PASSWORD</pre>
-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	<p>Turn on 'extra verbose' mode.</p> <p><b>Tip:</b> You can save the output from 'verbose' or 'extra verbose' mode for debugging.</p> <p>To do so, you first have to be using an OFFLINE LICENSE FILE. See <a href="#">Offline Licenses (page 30)</a>. Then, issue the following command:</p> <pre>./cardrecon_linux26_2.0.13 -vv &gt;&gt; output.txt</pre>

# 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 **VirtualBox's 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](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/microsoft-edge/tools/vms/>

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.

Select a download

Virtual machine

IE8 on Win7 (x86) ▾

Select platform

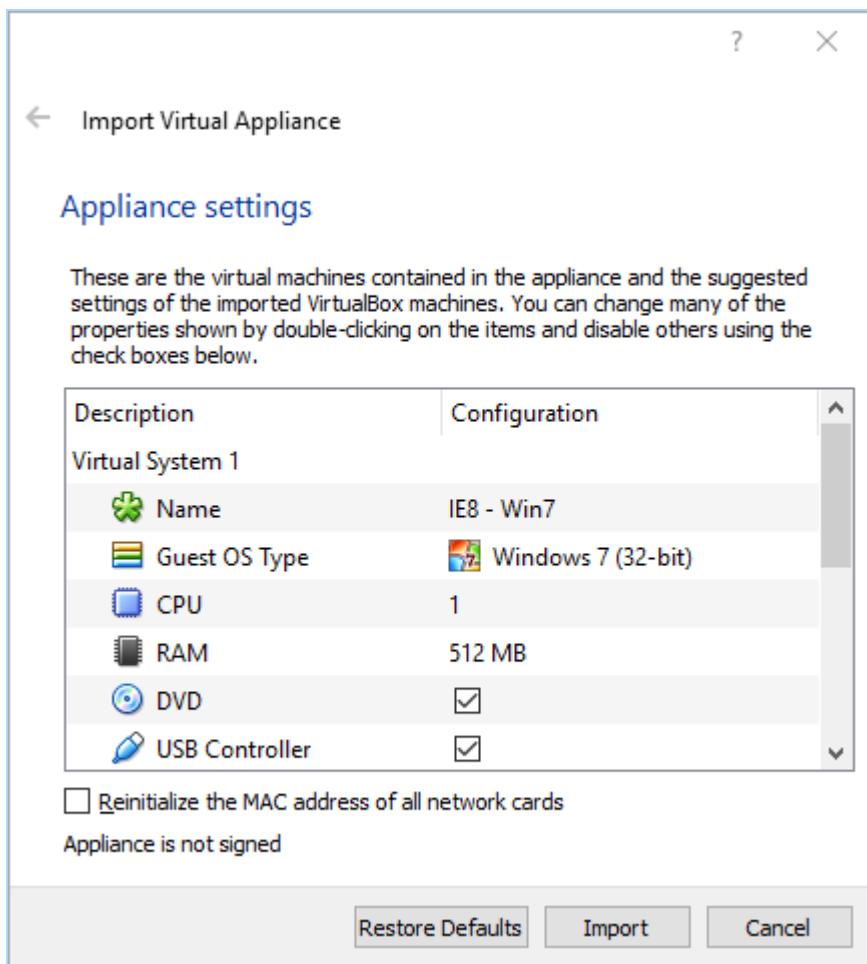
VirtualBox ▾

**DOWNLOAD .ZIP >**



## INSTALLING THE VIRTUAL MACHINE

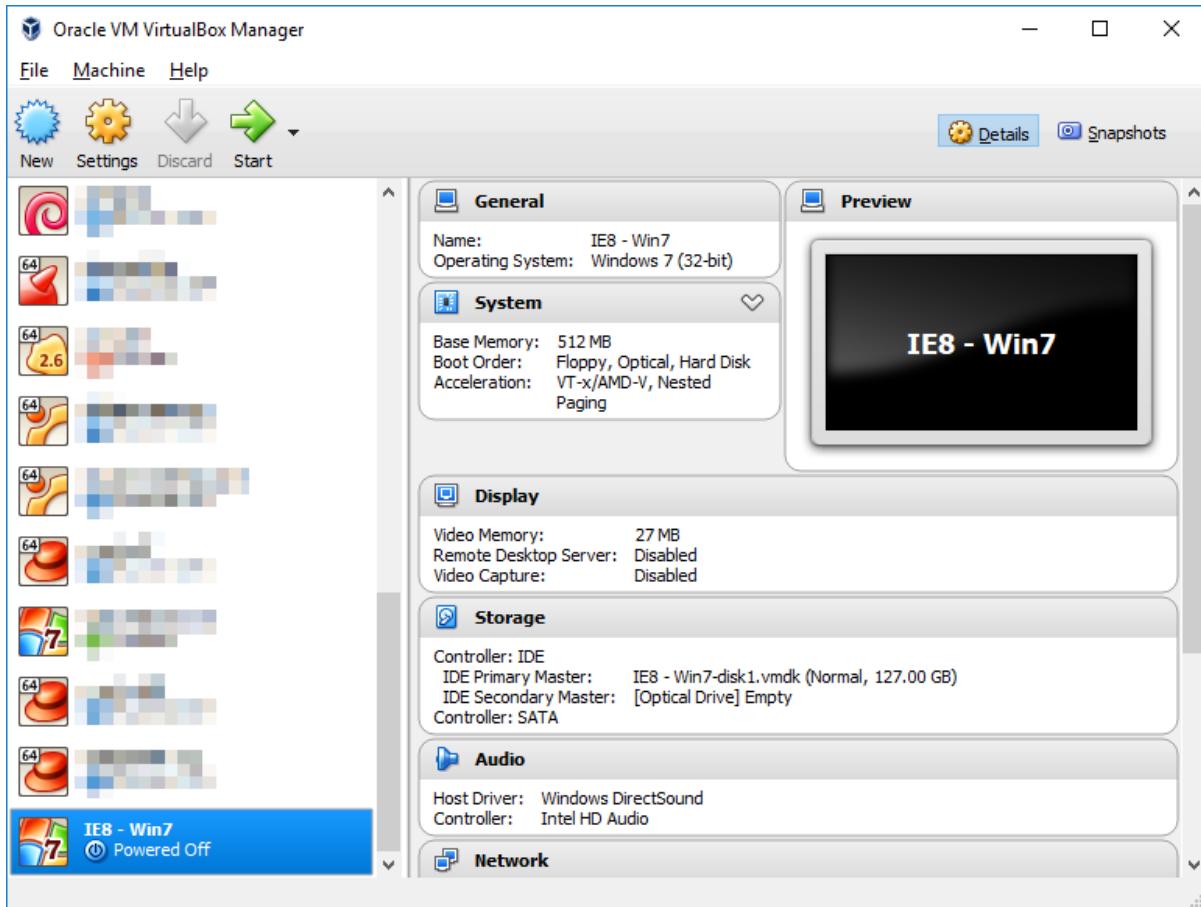
1. Make sure that [VirtualBox](#) is installed.
2. Locate the downloaded Windows VM [\\*.zip](#) file. Extract the virtual appliance file.
3. Double-click the extracted virtual appliance file ([\\*.ova](#)).  
[VirtualBox](#) opens and displays the "Import Virtual Appliance" dialog.



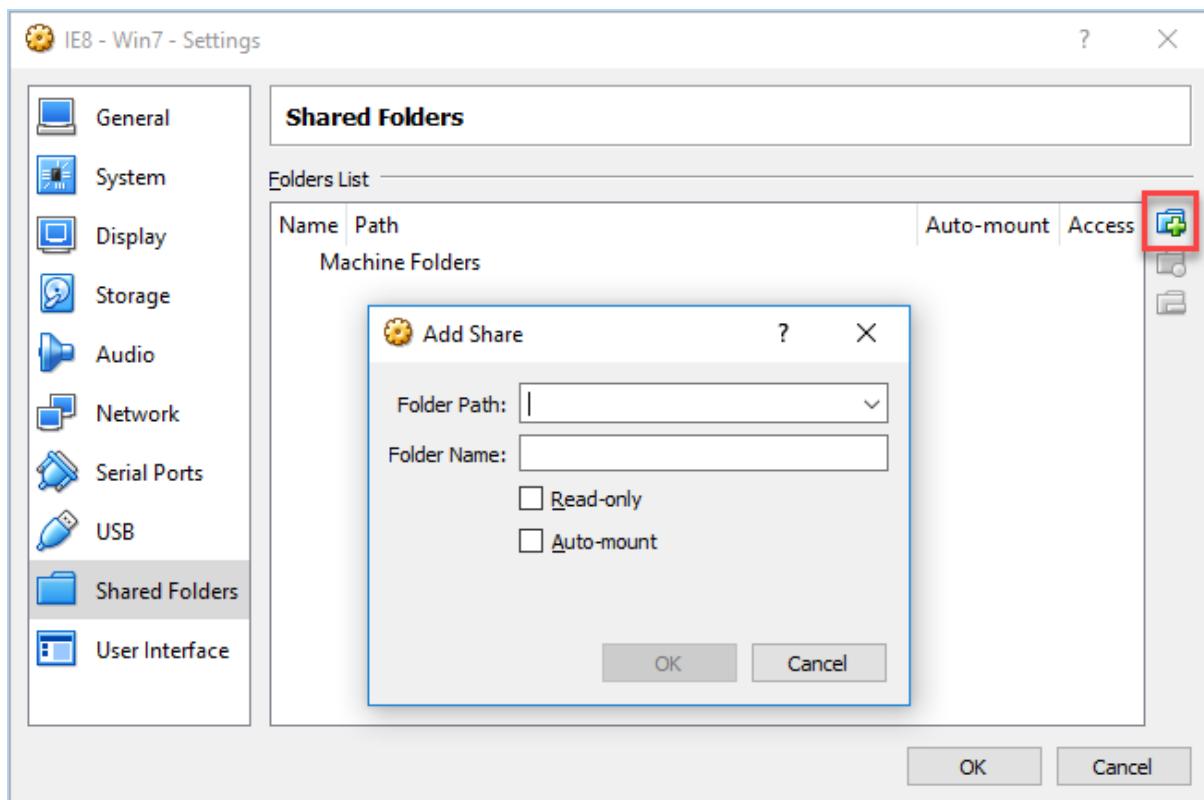
4. Click **Import** to start building the Windows VM.

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.